Microsoft Purview eDiscovery Premium

eDiscovery Playbook

November 2023

legalsolutions@epiqglobal.com

www.epiqglobal.com

Contents

Document Notes ... 3
Introduction ... 3
  What is Microsoft Purview? ... 3
  eDiscovery Tools in Purview ... 3
  Key Features in Premium eDiscovery ... 4
    Advanced Indexing ... 4
    Custodian Management ... 5
    Email Threading ... 5
    Near Duplicate Detection ... 5
    Conversation Threading ... 6
    Hold (Preservation) Management ... 6
    Communications ... 6
    Cloud Attachments ... 7
    Reporting ... 7
    Optical Character Recognition ... 8
Permissions in Purview ... 8
  Purview eDiscovery Group Roles ... 8
Premium eDiscovery Case Management ... 9
  Creating a Case ... 9
  Settings ... 14
    Case Information ... 15
    Access & Permissions ... 15
    Search & Analytics ... 16
    Review Sets ... 16
  Closing and Deleting Cases ... 16
  Data Sources ... 17
    Custodians ... 17
      Bulk Import Custodians ... 20

Non-Custodial Data Locations 22
Teams as Data Sources 24
Where Teams Stores Data 25
Teams as Custodial Sources 26
Teams as Non-Custodial Sources 27
Update Data Sources 28
Hold 28
Understanding Preservation in Microsoft Purview 29
Preservation for Mailboxes 29
Preservation for SharePoint 29
Manually Creating a Hold 30
Optional: Limit a Hold with a Query 30
Communications (Issue a Legal Hold) 31
Create a Communication from Scratch 32
Monitor and Report on Communication Acknowledgements 37
Create a Communication from a Template 38
Collections 39
Create a Collection 39
Select Custodial Sources for Collection 40
Select Non-Custodial Sources for a Collection 41
Select Additional Locations to Search in a Collection 41
Additional Location Searches: Exchange 42
Additional Location Searches in SharePoint 43
Define your Search Query 44
Use the New Query Builder to build a Query 45
Use the Condition Card Builder to build a Query 1
Use the KQL Editor to build a Query 3
Use KQL Editor to Build a Query 4
Review Collection Progress and Estimates 5
Review Collection Search Statistics 7

Review a Sample of Collection Results 7
Committing a Collection to Review Set 8
Other Review Set Actions 8
Items on the Collection Actions Button (Figure 61) 9
Review Sets 10
Committing to a review set options: 10
Retrieval Options: 11
Collection ingestion scale: 11
Run Analytics in a Review Set 14
Filter a Review Set 14
Grouping 16
Tags 17
Processing 20
Exports 21
Jobs Report 26
Advanced Topics 28
Compliance Boundaries 28
Automation 28
Converting Standard eDiscovery Cases to Premium eDiscovery Cases 29
Premium eDiscovery Settings 30

Document Notes

Throughout this document there are several text boxes that have been used to draw attention to important considerations when using eDiscovery Premium. The following is a key to these tables:

	Note *Note boxes call your attention to something specific in the document and give some additional context to the section.*

!	***Important Note*** *Important Note boxes note points you need to be fully aware of when making decisions regarding how to use Microsoft Purview eDiscovery Premium. Skipping recommendations in the important note boxes may limit your access to the full functionality of eDiscovery Premium.*

	Tip *Tip boxes highlight Epiq's best practice recommendations for Purview eDiscovery.*

	Note *Microsoft is continually improving all M365 products, including eDiscovery. Because of this there are frequent small, and sometimes significant, changes to the interface. Rather than including a voluminous number of screen shots in this document, we frequently link to Microsoft's documentation which will include up to date images and descriptions of the features discussed here.*

Introduction

What is Microsoft Purview?

In April of 2022, Microsoft rebranded and gathered all of the compliance products in both M365 and Azure as Microsoft Purview. Microsoft's eDiscovery tools (Standard and Premium) are part of the Purview Platform. eDiscovery "adjacent" solutions in Purview include Data Lifecycle Management (retention and records management,) and Audit Log.

The Microsoft Purview Compliance Portal can be found at: https://compliance.microsoft.com/ .

	Note To access any of the solutions on the portal you must be granted permission. See Permissions in Purview later in this document for more information.

To Learn More about Purview See: What is Microsoft Purview? | Microsoft Learn

eDiscovery Tools in Purview

Microsoft Purview contains three solutions that allow authorized users to search across M365 content and collect data as evidence in legal matters and other investigations. Content search includes the ability to search M365 content using Microsoft's standard index and export the results. Standard eDiscovery adds the ability to organize searches by case and place location holds to preserve M365 data in place.

Premium eDiscovery adds Advanced Indexing, Optical Character Retention, Custodian management, and a growing list of features as detailed in the chart below. Content search and Standard eDiscovery are included in all Enterprise, Government, and Education license levels of M365. Premium eDiscovery requires that each custodian and users that receive the benefit of using Premium eDiscovery have an elevated license known as "E5" (or G5 or A5.)

For more information on M365 licensing see: Compare Microsoft 365 Enterprise Plans | Microsoft 365

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

See: Microsoft Purview eDiscovery solutions | Microsoft Learn

Key Features in Premium eDiscovery

Compared to Standard eDiscovery, Premium eDiscovery has a number of advanced features.

Advanced Indexing

Premium eDiscovery's Advanced Indexing combined with OCR (see Optical Character Recognition) greatly reduces the number of unsearchable or partially searchable items when compared to Microsoft's basic Content Search and Standard eDiscovery platforms. In addition, Premium eDiscovery Review Sets and reporting tools gives eDiscovery practitioners more insight into why items, like password protected files, are not searchable.

The word "index" has multiple meanings in technology, the legal world, and eDiscovery. When we refer to the index in Purview eDiscovery and M365, we are referring to the tools that make content searchable. When you do a search in Outlook or SharePoint, to find content you utilize the Exchange Online and SharePoint indices. Purview's Content Search and Standard eDiscovery also use the Exchange and SharePoint indices.

Microsoft optimizes its Exchange and SharePoint indices for speed and not completeness. Because of this, M365 items may not be completely searchable when using Content Search and Standard eDiscovery. Microsoft has documented the limitations of these indices here: Partially indexed items in Content Search | Microsoft Learn

Premium eDiscovery builds on the standard M365 indexing with Advanced Indexing. When data sources are added to a Premium eDiscovery case, Premium eDiscovery examines the existing indices for the data sources, identifies any partially indexed items and reindexes the items.

See: Advanced indexing of custodian and non-custodial data sources | Microsoft Learn

Custodian Management

In a Premium eDiscovery case, legal teams can add individuals in their organization as custodians and identify and preserve custodial data sources such as Exchange mailboxes, OneDrive accounts, SharePoint, and Teams sites. Identification of custodial sources initiates the advance indexing process in the locations. eDiscovery Holds, which secure information from inadvertent (or intentional) deletion by preserving data in place, can be placed on all custodial sources by checking a single checkbox. During the collection phase, all custodial data sources may be sourced all at once or individually.

See: Custodian Management | Learn

Email Threading

Consider an email conversation that has been going on for a while. In most cases, the last message in the email thread will include the contents of all the preceding messages. Therefore, reviewing the last message will give complete context of the conversation that happened in the thread. Email threading identifies such messages so that reviewers can review a fraction of collected documents without losing any context. Email threading parses each email thread and deconstructs it to individual messages. Each email thread is a chain of individual messages. Microsoft Purview eDiscovery Premium analyzes all email messages in the review set to determine whether an email message has unique content or if the chain (parent messages) is wholly contained in the final message in the email thread.

See: Email Threading | Learn

Near Duplicate Detection

Consider a set of documents to be reviewed in which a subset is based on the same template and has mostly the same boilerplate language, with a few differences here and there. If a reviewer could identify this subset, review one of them thoroughly, and review the differences for the rest, they would not miss any unique information while taking only a fraction of the time it would have taken them to read all the documents cover to cover. Near duplicate detection groups textually similar documents together to help you make your review process more efficient. When near duplicate detection is run, the system parses every document with text. Then, it compares every document against each other to determine whether their similarity is greater than the threshold set in the case. If it is, the documents are grouped together.

Once all documents have been compared and grouped, a document from each group is marked as the "pivot"; in reviewing your documents, you can review a pivot first and review the other documents in the same near duplicate set, focusing on the difference between the pivot and the document that is in review.

See: Near Duplicate Detection | Learn

Conversation Threading

Instant messaging is a convenient way to ask questions, share ideas, or quickly communicate across large audiences. As instant messaging platforms, like Microsoft Teams and Viva Engage groups, become core to enterprise collaboration, organizations must evaluate how their eDiscovery workflow addresses these new forms of communication and collaboration.

The conversation reconstruction feature in Microsoft Purview eDiscovery Premium is designed to help you identify contextual content and produce distinct conversation views. This capability allows you to efficiently and rapidly review complete instant message conversations (also called threaded conversations) that are generated in platforms like Microsoft Teams.

With conversation reconstruction, you can use built-in capabilities to reconstruct, review, and export threaded conversations. Use Premium eDiscovery conversation reconstruction to:

- Preserve unique message-level metadata across all messages within a conversation.
- Collect contextual messages around your search results.
- Review, annotate, and redact threaded conversations.
- Export individual messages or threaded conversations.

See: Conversation Threading | Learn

Hold (Preservation) Management

You can use a Microsoft Purview eDiscovery Premium case to create holds to preserve content that might be relevant to your case. Using the Premium eDiscovery hold capabilities, you can place holds on custodians and their data sources. Additionally, you can place a non-custodial hold on mailboxes and OneDrive for Business sites. You can also place a hold on the group mailbox, SharePoint site, and OneDrive for Business site for a Microsoft 365 group. Similarly, you can place a hold on the mailbox and site that are associated with Microsoft Teams. When you place content locations on hold, content is held until you release the custodian, remove a specific data location, or delete the hold policy entirely.

See: Hold (Preservation) Management

Communications

Microsoft Purview eDiscovery Premium allows legal departments to simplify their processes around tracking and distributing legal hold notifications. The custodian communications tool enables legal departments to manage and automate the entire legal hold process, from initial notifications, to reminders, and to escalations, all in one location.

See: Communications | Learn

Cloud Attachments

Cloud attachments, a.k.a. modern attachments, are email and Teams[1] attachments that link to documents on the sender's OneDrive or a SharePoint site. the attachment rather than including a copy of a file. Traditional email attachments are embedded in an email and collected when the message is collected. Most email archive platforms and Purview *Standard* eDiscovery do not collect cloud attachments. Premium eDiscovery provides multiple tools to assist with collection and review of modern attachments.

When collecting the results from a Premium eDiscovery collection search you have to the option of including the target of the cloud attachment. When the collection is processed into a review set, the parent child relationship between the message and its attachment will be preserved and the group can be viewed as a message family. Premium eDiscovery continues to preserve the parent child relationship when the files are exported using Premium eDiscovery's condensed directory export.

!

Important Note

SharePoint and OneDrive create a new version of a file each time the file is saved. Premium eDiscovery collects the latest version of the file and not the version shared. It is possible retain and collect shared versions of files if an organization has enabled the auto application of retention labels to cloud attachments. To utilize the auto application of labels in eDiscovery workflows, the feature ***must*** *be enabled before files are shared.*

See: Cloud Attachments | Learn

Reporting

When collecting data, managing holds, and managing cases, running reports to validate data and understand issues are essential. Premium eDiscovery provides multiple validation and reporting tools. These include:

- Top locations and search term reports which provide collection search estimated counts prior to collecting data.
- Collection statistics report shows counts on the number of items retrieved from locations during a collection. The report includes total item count along with counts by item type, duplicate counts, and retrieval exceptions.
- Processing statistics show the total count of expanded items processed into a review set.
- eDiscovery job reports in a case and across your M365 tenant. The reports show details on long running jobs and identifies if there are any issues. The tenant-wide jobs dashboard allows eDiscovery Administrators to view activities in both Premium and Standard eDiscovery and determine if your organization has jobs queued because too many concurrent jobs are running.
- Review Set Export report contains processed and aggregated metadata from all or selected documents in a review set. This includes information on item sources and any errors encountered when processing data.
- Using automation for reports. As noted in the automation section of this document, custom reports on cases, custodians, holds, collections, review sets, and more may be generated using the Graph API and the Security and Compliance PowerShell module.

[1] All Teams attachments are cloud attachments.

See: Collection statistics and reports | Learn

See: Manage jobs in eDiscovery | Learn

See: eDiscovery limits | Learn

See: Premium eDiscovery Exports | Learn

See: Document metadata fields in Premium eDiscovery | Learn

Optical Character Recognition

OCR converts images of text into searchable text. When OCR is enabled in a Premium eDiscovery case, Microsoft OCRs images found in the case data sources during the advanced indexing process.

See: Optical Character Recognition

Permissions in Purview

Along with the eDiscovery tools, multiple solutions within Microsoft Purview allow administrators to access content like email and documents without an account owner's knowledge or permission. Because of this, permissions to access Purview solutions must be granted explicitly through the Purview compliance portal. This differs from most M365 administrative roles which are set in Entra (Azure Active Directory.)

Global Administrators or members of the Organizational Management role assign Purview permissions through role groups. Role groups are groups of granular permissions to complete Purview actions. For example, there is a "Hold" permission that allows the ability to place a hold on a location in an eDiscovery case and a separate "Export" permission that grants the ability to export data from an eDiscovery case.

For more information see: Permissions in the Microsoft Purview Compliance Portal | Microsoft Learn

Purview eDiscovery Group Roles

Microsoft provides two default role groups that enable an eDiscovery practitioner to have full control and visibility of eDiscovery cases:

- **eDiscovery Manager -** An eDiscovery Manager can use eDiscovery search tools to search content locations in the organization and perform various search-related actions such as preview and export search results. Members can also create and manage cases in Microsoft Purview eDiscovery Standard and Microsoft Purview eDiscovery Premium, add and remove members to a case, create case holds, run searches associated with a case, and access case data. eDiscovery Managers can only access and manage the cases they create. They cannot access or manage cases created by other eDiscovery Managers unless granted access to those cases.
- **eDiscovery Administrator -** An eDiscovery Administrator is a member of the eDiscovery Manager role group and can perform the same content search and case management-related tasks that an eDiscovery Manager can perform. Additionally, an eDiscovery Administrator can:
    - Access all cases listed on the Standard eDiscovery and Premium eDiscovery pages in the compliance portal.
    - Access case data in any Standard or Premium eDiscovery case in the organization.

- Manage any eDiscovery case, including managing who may access the case
- Manage Premium eDiscovery global settings for their organization.
- Access reports on eDiscovery processes (jobs) running across their organization.

It is possible to create custom eDiscovery role groups should your organization require them. Customizing roles enables the ability to refine the permissions assigning the least number of privileges possible. For example, you may have multiple eDiscovery Teams in your organization where:

- Only Team A is permitted to create a case and include custodians.
- Only Team B is permitted to create collections and review, interact, and tag data.
- Only Team C is permitted to conduct a final review and export the data.

Another example of creating customized eDiscovery Role Groups would be to limit visibility of cases to only investigators within a specific region. This can be useful when an organization operates from different geographical regions and needs to align with Data Sovereignty Laws. For example, if your organization operates in the Americas, Europe, and Asia Pacific regions, you can create customized eDiscovery roles for each region. This approach helps to maintain compliance with data privacy laws and regulations. For example,

- Only AMER investigators can create, manage, and view cases within this region.
- Only EMEA investigators can create, manage, and view cases within this region.
- Only APAC investigators can create, manage, and view cases within this region.

Premium eDiscovery Case Management

Creating a Case

To create a case in Premium eDiscovery we need to navigate to ***eDiscovery Premium > Cases and Create a Case.*** Figure 1 - Create a Case

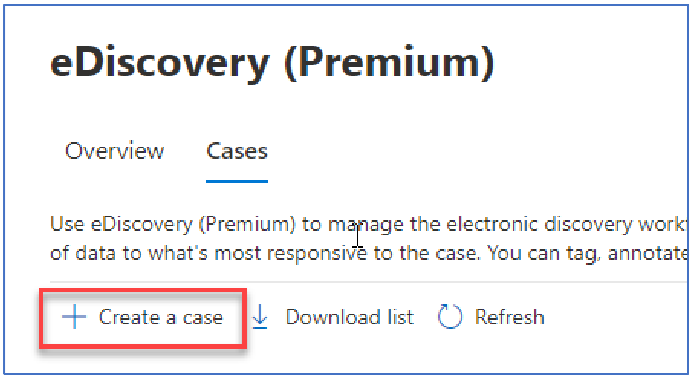


Figure 1 - Create a Case

The case creation wizard will launch. On the first page of the wizard, you will be prompted for the following:

1. **Name** – The unique name of the case. This property is required.

2. **Description** – A text field you may use to help other eDiscovery users understand this case. When exporting a list of cases, this field appears as a column. This property is optional.
3. **Number** – The name here is deceptive. This is also a text field. The intent of the filed is to provide a docket number or other identifier associated with the case. This optional property also appears as a column when exporting a list of cases. We find that organizations that choose to use this field often use it to categorize cases. For example, use the word "Investigation" to identify cases related to internal investigations.
4. **Case Format** – This is another deceptively named field. It implies a choice, but the only option available to choose is "New." This property is an example of Microsoft's continual evolution of the Premium eDiscovery platform. In 2022, Microsoft introduced a new underlying format for cases to better accommodate larger data sets and Teams data. For a brief period, an eDiscovery operator could select either the New or Classic case format, but Microsoft quickly transitioned to the advanced features and stability of the "New" case format.

The completed configuration is shown in Figure 2 - Case Information

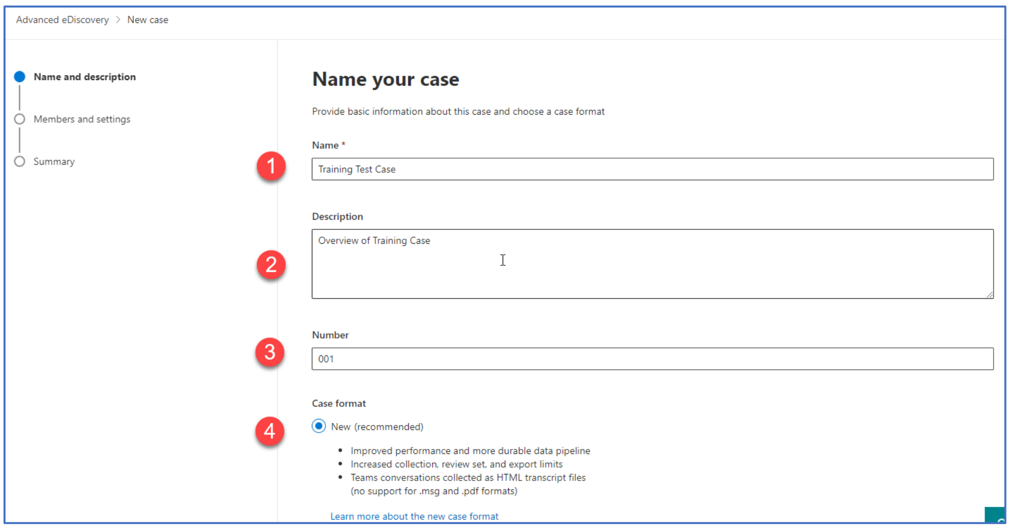


Figure 2 - Case Information

Tip
Case names must be unique across all Premium eDiscovery and Standard eDiscovery cases. This include cases you may not see because you have not been assigned to the case. We recommend companies create naming conventions to ensure case names are unique.

After entering the basic case information, click the ***Next*** button to move to the second page of the case creation wizard, ***'Add Team Members and Configure Settings'.*** On this page you will define who initially has access to the case, analytics options, and OCR options. All elements on this page are optional and can later be changed in the Settings menu for the case.

1. ***Users*** – Use this search interface to select individuals who need access to the case. For example, in Figure 3 – Case Setup, Aaron Bellamy will be granted access to the case. Purview permissions assigned to Aaron limit their abilities in the case. See Permissions in this document for more information.

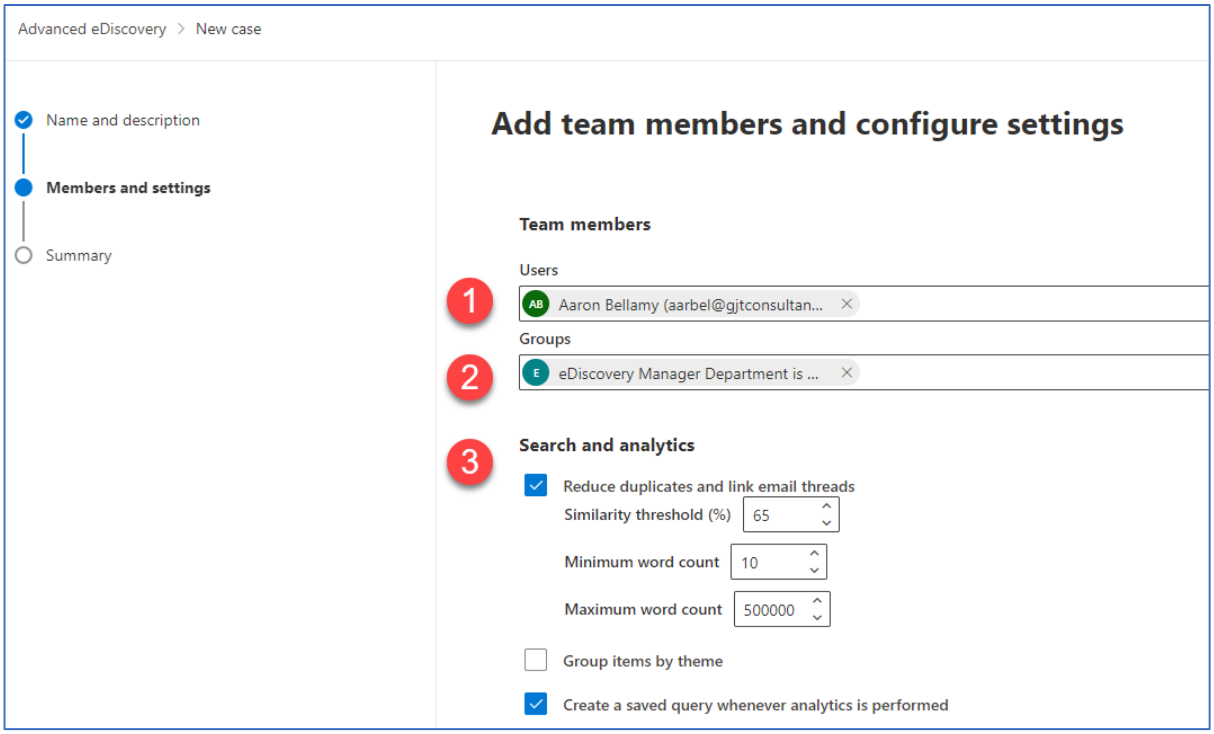


Figure 3 – Case Setup

Note
Adding users at this stage does not add the users as case custodians

Tip
People will not receive an automated notification when assigned to an eDiscovery case. The case will appear in their list of available cases the next time they access Premium eDiscovery. We recommend your case creation workflows include notifying people that they have access to a new case.

2. **Groups** – Use this search box to select Purview role groups that may access the case. The eDiscovery permissions assigned to the role group control what the members can and cannot do within the case. For example, if the group has just 'Review' permissions then the group members will only be able to review case content. See the Permissions section of this document for more information.

3. ***Search and Analytics*** – The settings in this area define how Premium eDiscovery will behave when it detects similar data while analyzing data in review sets. The settings currently include:

    a. **Similarity Threshold** -Premium eDiscovery uses this percentage to determine near duplicates documents and email threads. Microsoft's default threshold is 65%. This means if the text of two documents is 65% or greater identical, then the documents are identified near duplicates ("near dupes".) During document review, items in the review set may be grouped and filtered by duplicates, near duplicates, and email threads, thus making the review more efficent.

Premium eDiscovery also uses the simularity threshold while anayzing email to identify email threads. Forwarded and replied to emails typically contain the text of previous messages. That text is taken into account while constucting email threads.

	Tip While it is possible to change the similarity threshold, we recommend customers leave the settings at the default of 65%. If you feel that near-duplicates are over identified in a review set, the threshold may be increased and analytics re-run.

b. **Group items by Theme** – When themes is enabled and analytics run in a review set, Premium eDiscovery parses out common ideas and phrases that appear across all the documents in the review set. Premium eDiscovery then assigns those themes to the documents in which they appear. Documents may be associated with multiple themes but when themes is enabled, a dominant theme will be assigned and the reviewers may then filter and group items by theme**.**

The last two settings which are configurable at the new case creation stage are:

1. ***Text to Ignore*** – Repetitive text in collected content may skew results generated by Premium eDiscovery Analytics. For example, if every email contains the text "Please consider the environment before printing" then analytics would return themes related to the environment and printing in lieu of other, more relevant themes. Ignoring repetitive text yields more accurate analytics results.
2. ***Optical Character Recognition (OCR)*** – OCR converts images of text into searchable text. When OCR is enabled in a Premium eDiscovery case, Microsoft OCRs images found in the case data sources during the advanced indexing process.

This can be seen in the example Figure 4 – Case Setup Cont'd – Text to ignore and OCR

	Tip We recommend that OCR be enabled in Premium eDiscovery cases. Note that OCR is not available in Standard eDiscovery, you may notice your results will contain items Microsoft identifies as partially indexed or unsearchable. These unsearchable results include images that have not been OCRed. The number of unsearchable items is greatly reduced and frequently eliminated when using Premium eDiscovery because of OCR and Advanced Indexing.

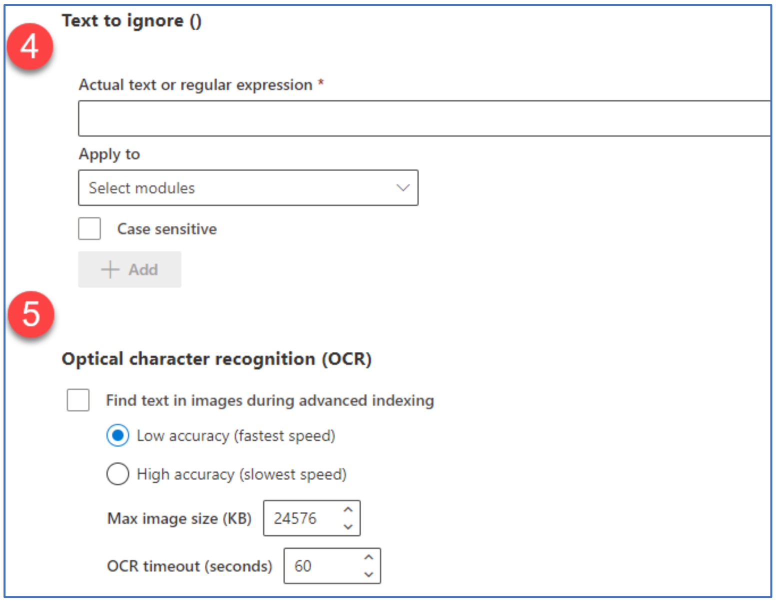


Figure 4 – Case Setup Cont'd – Text to ignore and OCR

After you have assigned users and groups to the case, and configured analytics options, click ***Next*** to move to the last page of the wizard. The last page summarizes settings configured in the case creation wizard. Review the settings and then choose ***Submit*** *to* create the case.

Premium eDiscovery will take a moment to create the case. After the case is created, your browser will open to the Overview page for the case. Note the case menu, highlighted in red on Figure 5 – Premium eDiscovery Case Overview Page. We will review the options available in each menu tab in the following sections of this document.

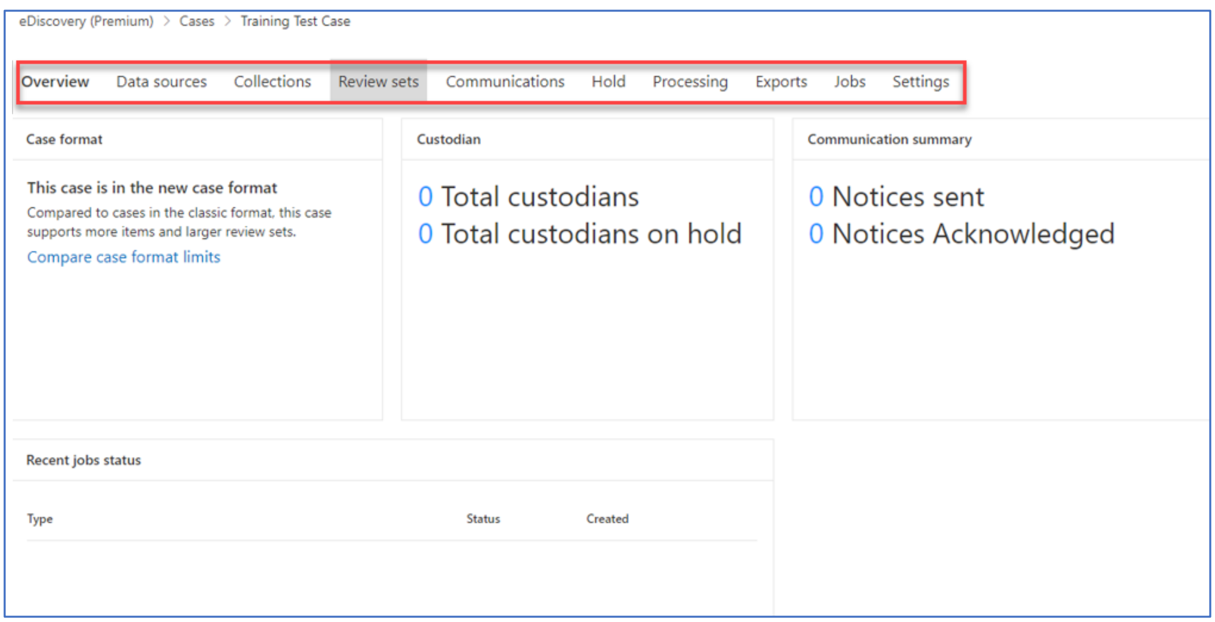


Figure 5 – Premium eDiscovery Case Overview Page

Settings

All the settings configured in the case creation wizard may be changed at any time by visiting the ***Settings*** tab on the case menu. As shown in the blow Figure 6 - Premium eDiscovery Case Settings

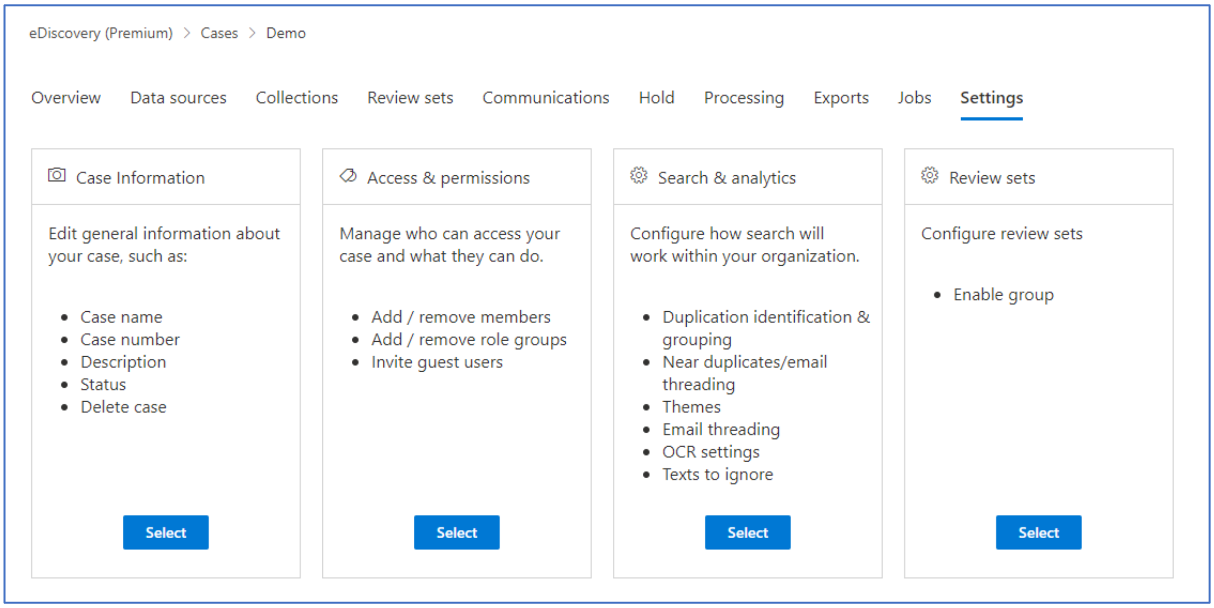


Figure 6 - Premium eDiscovery Case Settings

At this writing, there are four tiles on the settings page.

Case Information

Changing the case name, number, and description that were set during the case creation process is possible on the panel that pops-up when clicking the ***Select*** button on this tile. Whenever you make a change, you must choose **Save** from the ***Actions*** button on the Case Information panel as displayed in Figure 8 – Add Custodian.

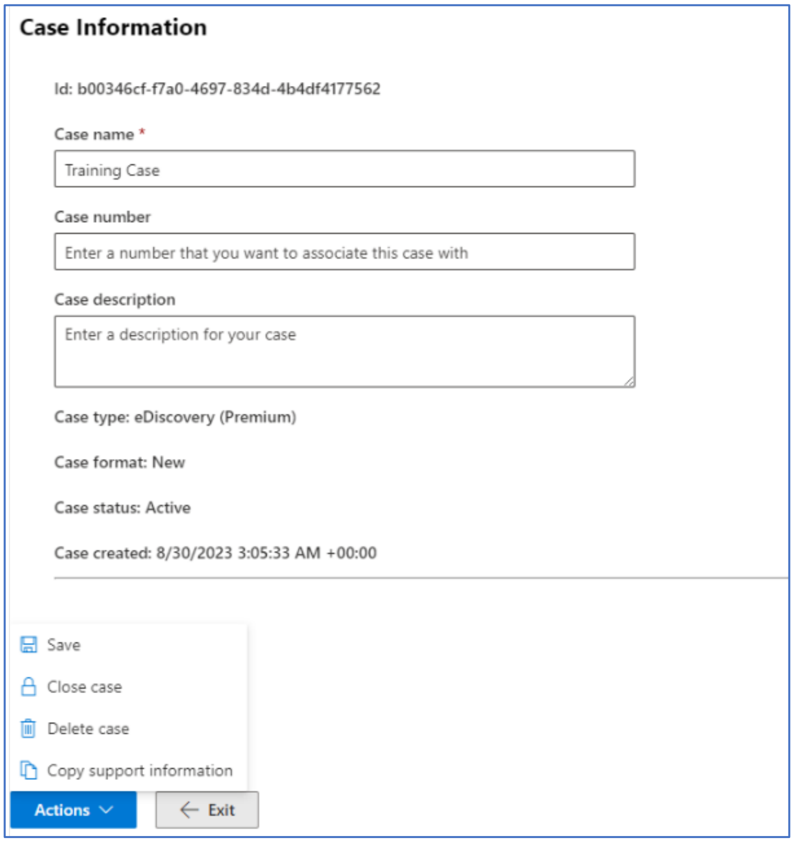


Figure 7 - Case information settings

Other actions on the Case Information panel include Closing and Deleting a case. We will discuss these actions further in the Closing and Deleting cases section below.

Finally, the actions on the button include **Copy support information.** As in any other software product, things sometimes go wrong, and you may need to open a support ticket with Microsoft. Copy support information copies information about your case to your clipboard. This information should be included in support tickets sent to Microsoft.

Access & Permissions

Along with modifying what team members may access a case, guest reviewers may also be invited to a case within this section. Microsoft introduced guest reviewers to Premium eDiscovery in May of 2023. The intent of this functionality is to allow organizations to grant outside counsel and other trusted external advisors review access to a case.

Before eDiscovery Managers and Administrators may invite a guest user to a case, an eDiscovery Administrator must enable Guest Access for your organization in the Premium eDiscovery Settings dashboard.

To learn more about Guest access see: [Guest access in eDiscovery (Premium) | Microsoft Learn]

Search & Analytics

Analytics settings like the similarity threshold that was set during case creation can be changed at any time in the search and analytics section. If you missed enabling OCR for a case, that can be enabled in this section as well.

> **! *Important Note***
> *If you enable OCR in a case after adding data sources to a case, you will need to update the index for the data source(s) to initialize OCR in the data sources.*

> **! *Important Note***
> *If you change analytic settings like the similarity threshold, you will need to rerun analytics in your review set(s) to see the changes reflected.*

Review Sets

In March of 2023, Microsoft introduced new options for grouping email threads, attachments, Teams and Viva Engage (Yammer) conversations in review sets. Prior to March of 2023, Premium eDiscovery allowed reviewers to view review sets grouped by families or by Teams or Viva Engage conversations. Grouping by families shows items like emails with attachments nested below. Grouping by conversations groups messages in Teams and Viva Engage - conversations together with attachments nested below.

For cases created on or after March 2023, you have the option to enable new grouping options. Conversation groupings now include email threads along with Teams conversations, and Viva Engage, attachments to conversations are nested in the conversations. Grouping by family groups files with embedded files. For example, all files from withing a Zip file are grouped together.

For more information Configure review set grouping settings for eDiscovery (Premium) cases | Microsoft Learn and Group and view documents in a review set in eDiscovery (Premium) | Microsoft Learn

Closing and Deleting Cases

As noted in the Case Information section of Case Settings, there is Close Case and Delete Case on the actions button in case settings. These options are also available on the case list.

Closing a case releases all holds in a case and marks a case as closed in case listing. Closed cases can be edited, and data can still be collected and exported from closed cases. Closed cases can also be reopened.

Deleting a case deletes all case components, like review sets, and the case is removed from the list of cases. Before a case may be deleted all holds must be removed from the case. This can be done by closing the case, releasing holds on data sources, or deleting holds.

> ***Note***
> *Deleting a case does not delete items in M365. For example, if a message collected into a review set from a mailbox and still exists in the mailbox, the message won't be deleted from the mailbox.*

Data Sources

A data source is a person or data location we may need to preserve (aka place on hold,) search against, and collect from during the lifecycle of a matter. There are two types of Premium eDiscovery case data sources: custodians, and non-custodial data locations.

Multiple things happen when we add a data source to a case:

1. Microsoft performs advanced indexing on the data source location(s).

> ***Tip***
> *To take advantage of Premium eDiscovery's Advanced Indexing you must add the locations you plan on searching as case data sources.*

2. If OCR is enabled for the case, non-searchable images in the data sources will be analyzed and if the image represents text, searchable text will be created.

> ***Tip***
> *OCR is enabled at the case level when you create a case. If you missed enabling it, you can enable it anytime and update the data sources to OCR images in the locations.*

3. Optionally, the location(s) will be placed on hold.
4. If the data source is a custodian, items collected from custodial locations are associated with the custodian in the review set.

Custodians

A custodian is an individual or entity who hold, or have the right to control, records and information[2]. In M365 this includes an account's mailbox and OneDrive by default but can include additional mailbox and SharePoint locations. For example, we may associate a custodian with a mailbox and a primary SharePoint site for a Microsoft Team where the custodian is a member.

There are three ways to add custodians to case. 1) You may add custodians interactively, 2) via bulk custodian import, or 3) use automation to programmatically add custodians (see Automation in this document for more information). Adding custodians interactively is the most frequently used option and accomplished through the "Add new custodians" option on the "Add data source" menu. As shown in Figure 8 – Add Custodian

[2] https://edrm.net/wiki/edrm-processing-glossary/.

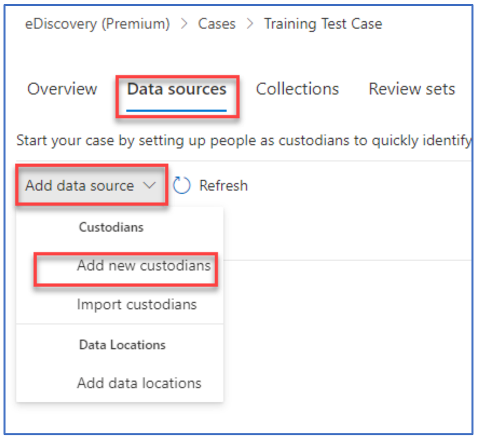


Figure 8 – Add Custodian

"Add new custodians" launches a wizard where you search for custodians and then associate them with data locations. In the example below, three custodians added by searching for and then selecting the custodian names in the "identify new custodian" search box. As displayed in Figure 9 – Selecting Custodians

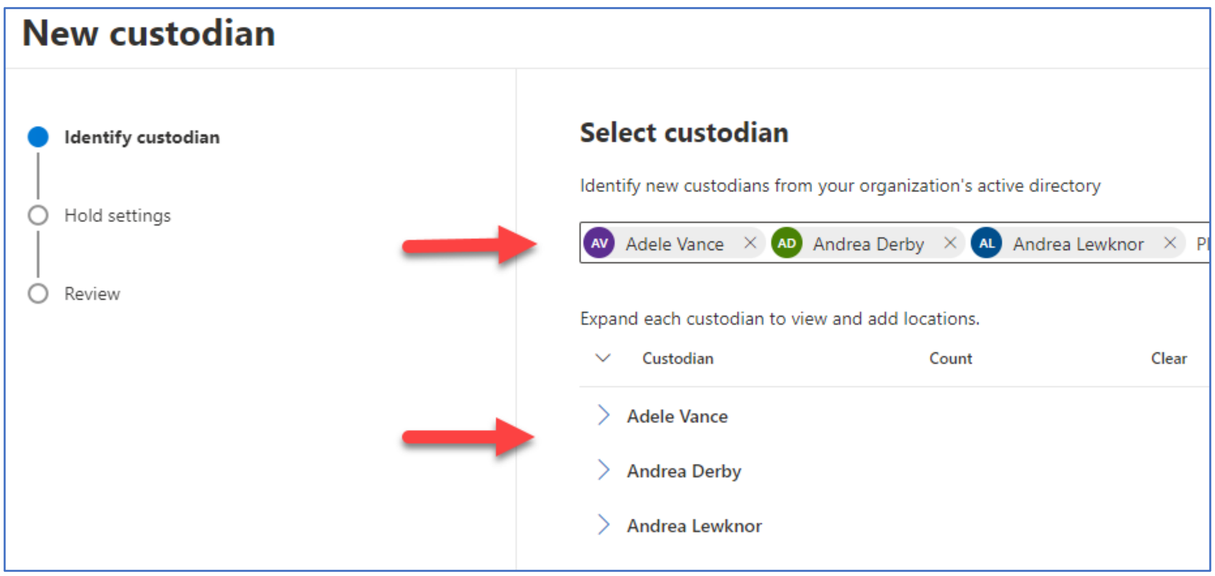


Figure 9 – Selecting Custodians

Tip
When searching for custodians to add to your case, Premium eDiscovery searches across active and inactive accounts in your M365 tenant. Inactive accounts are accounts that had a hold in place, or a retention policy applied when the mailbox license was removed. These accounts usually represent former employees. For more information on Inactive Accounts see: [Create and manage inactive mailboxes | Microsoft Learn]

When you select a custodian, their name appears in the list of custodians below the search box. Clicking the expansion arrow to the left of a custodian's name presents a list of locations that may be associated with a custodian. By default, as shown Figure 10 - Selecting Custodian Hold, a custodian will be associated with their mailbox and OneDrive. You may associate the custodian with additional locations by selecting the appropriate workload. For example, to identify a person as the custodian for a SharePoint site, click the edit link in the SharePoint row and search for the site on the resulting search interface.

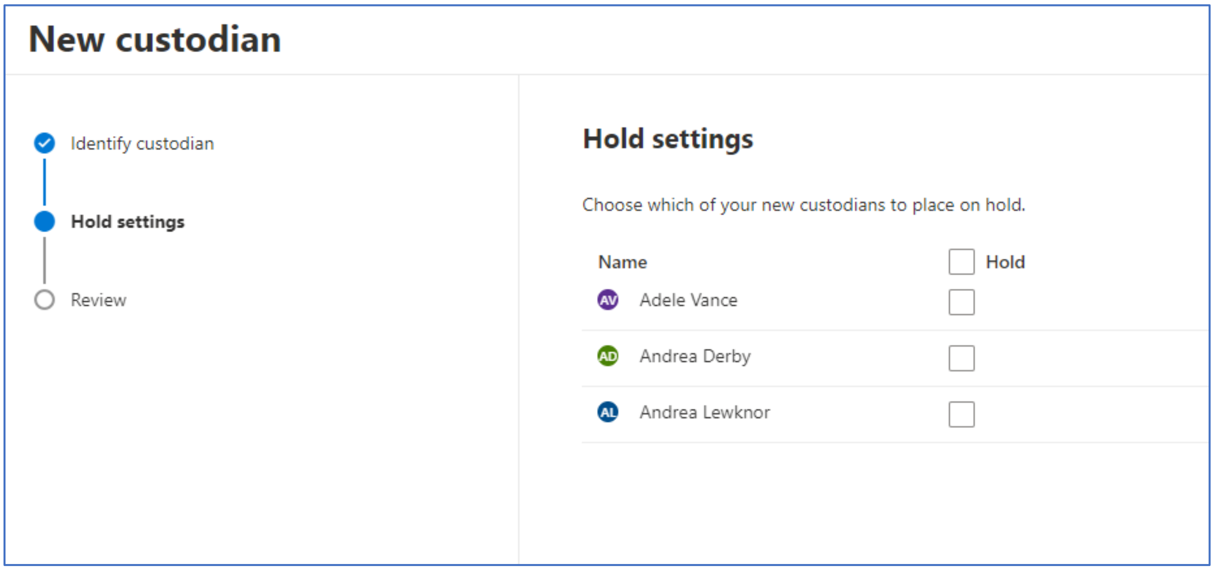


Figure 10 - Selecting Custodian Hold

After associating the custodians with the appropriate locations click '***Next'*** to move to the next page of the wizard. Checking the box to the right of the custodian's name will place all locations associated with the custodian on hold, as shown in Figure 11 – Place Custodian Locations on Hold.

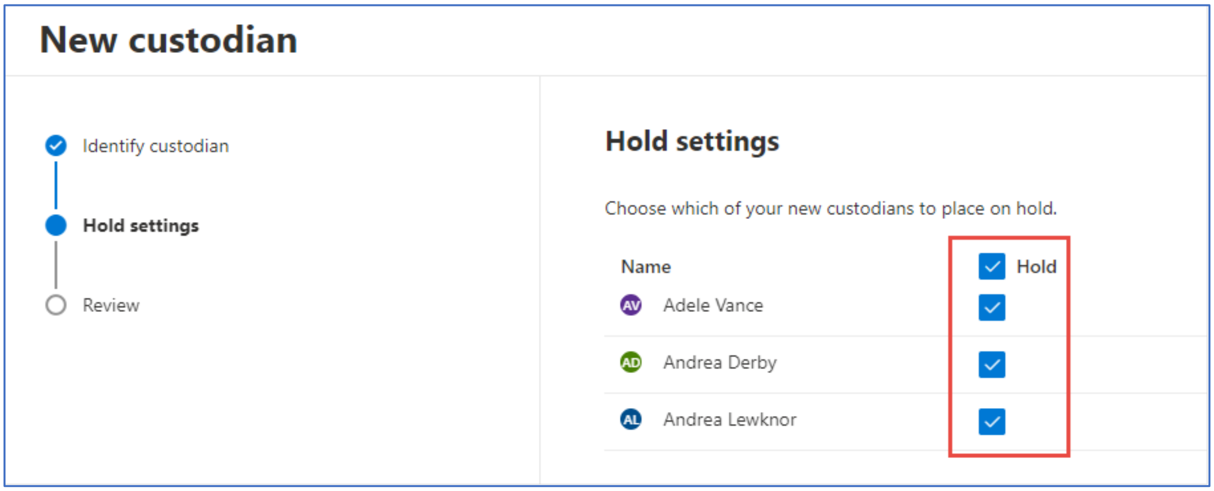


Figure 11 – Place Custodian Locations on Hold

After the wizard completes, you will be returned to the list of case data sources, as displayed in Figure 12 – Added Custodians.

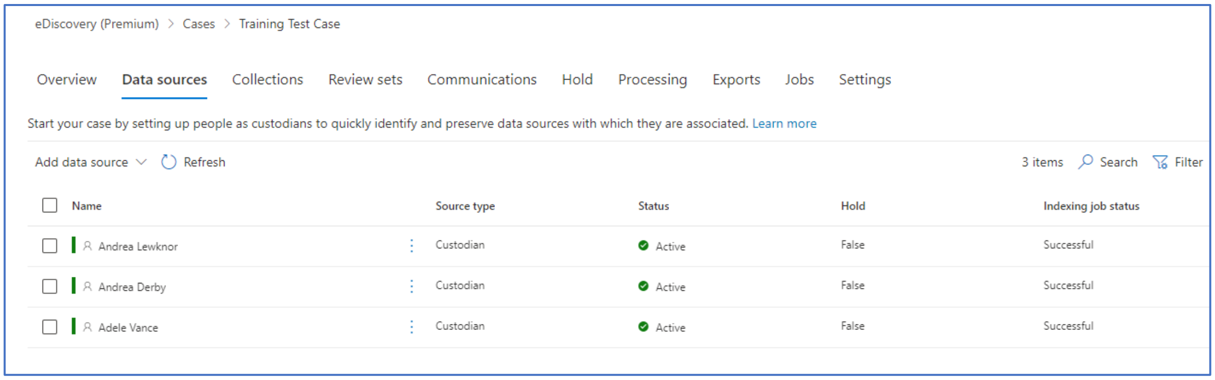


Figure 12 – Added Custodians

Tip
To get the full benefit of advanced indexing, wait for the indexing job status to change to Successful before starting a collection search of a data source.

Bulk Import Custodians

In addition to using the wizard to add new custodians as shown in Figure 13 – Import Custodians, it is possible to import up to 500 custodians at once into a case using the 'import custodian' feature.

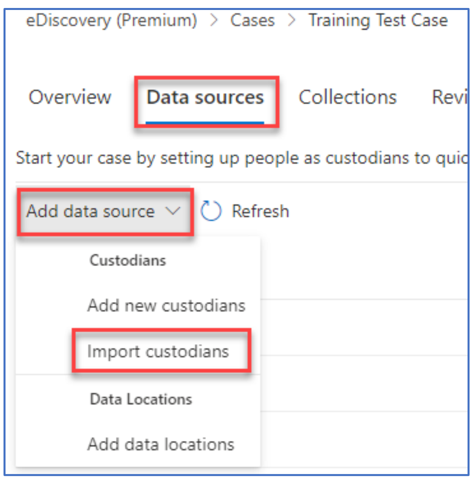


Figure 13 – Import Custodians

This selection allows the download of a CSV file template provided by Microsoft to import multiple custodians at one time to a case, as demostrated inFigure 14 – CSV Wizard.

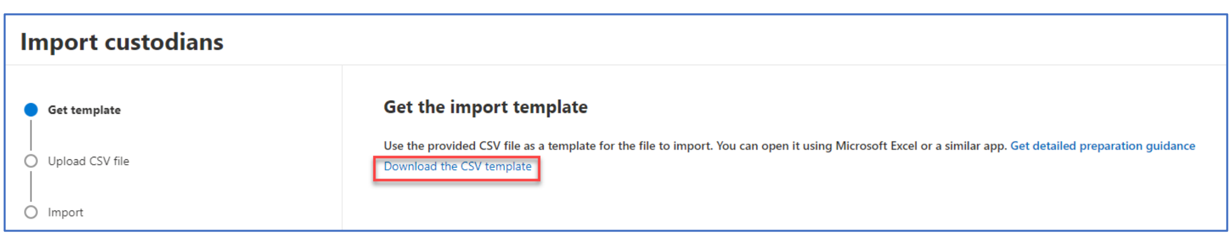


Figure 14 – CSV Wizard

The CSV template contains the following columns and can be seen in Figure 15 – Example CSV Import:

1. **Custodian contactEmail** - The email address of the custodian. This field is required.
2. **Exchange Enabled -** If the custodian's mailbox should be included as a custodial data source, the value in this column should be **TRUE**. Otherwise, enter **FALSE**. This field is required.
3. **OneDrive Enabled** – If the custodian's OneDrive should be included as a custodial data source, the value in this column should be **TRUE**. Otherwise, enter **FALSE**. This field is required.
4. **Is OnHold -** If the custodian should be placed on hold, enter **TRUE,** otherwise enter **FALSE.** This field is required.
5. & 6. **Workload1 Type** and **Workload1 Location** - Up to 99 additional locations can be associated with the custodian using the workload columns. The Workload type columns are used to specify what type of locations is being added (Exchange or SharePoint.) The Workload Location column should contain the email address or URL for the location to be added.

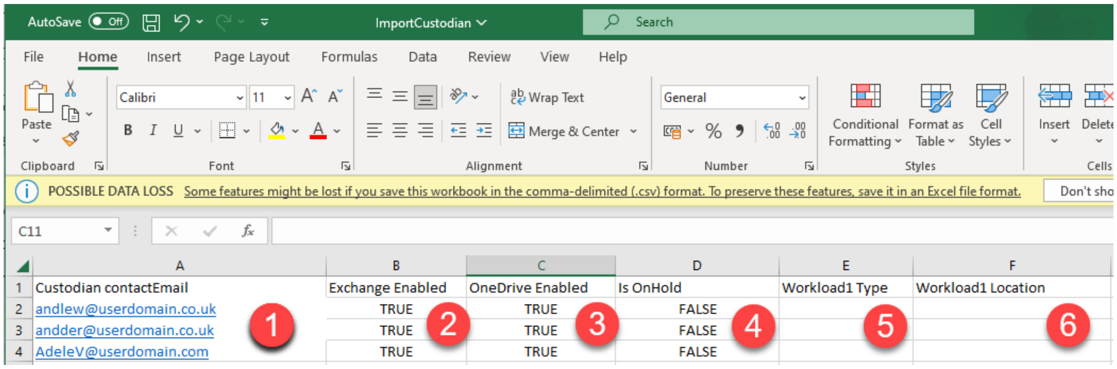


Figure 15 – Example CSV Import

See: Import custodians to an Premium eDiscovery case | Microsoft Learn for more information on bulk importing custodians.

Non-Custodial Data Locations

Non-custodial data sources are Exchange mailboxes and SharePoint sites that need to be searched in a case and (optionally) placed on hold but is not related to just one or a small number of custodians. As shown in Figure 16 – Add Data Locations

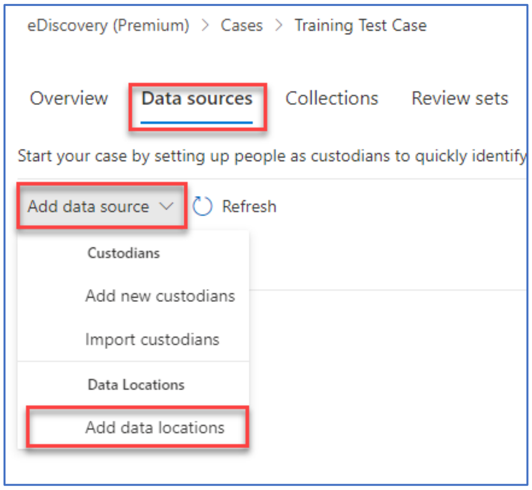


Figure 16 – Add Data Locations

The non-custodial wizard shows the four different data sources that can be ingested into an eDiscovery Case. This is also displayed in Figure 17 – Non-Custodial Data Locations.

1. **SharePoint** – Choose from a list of SharePoint sites.
2. **Exchange** – Choose from a list of shared mailboxes or distribution groups.
3. **M365 Connected Apps** – While still in the early days, M365 connected apps will utilize Microsoft Graph connectors for search to allow the search and collections of non-M365 data. See: Microsoft Graph connectors overview for Microsoft Search | Microsoft Learn for more information.

> ***Note***
> *M365 Connected Apps should not be confused with Purview data connectors – which allow you to archive data from third-party applications in M365 mailboxes. See Use data connectors to import and archive third-party data in Microsoft 365 | Microsoft Learn*

4. **Teams (preview)** – Microsoft added Teams as non-custodial data source option as a preview feature in September 2023. See Teams as data sources for more information.

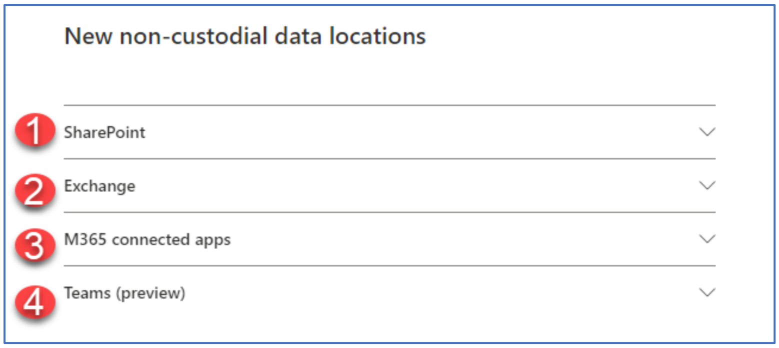


Figure 17 – Non-Custodial Data Locations.

The method to add non-custodial Exchange and SharePoint locations is similar to adding custodial data sources as seen in Figure 18 – Search for a Non-custodial location. You first search for the site and select from a list of search results.

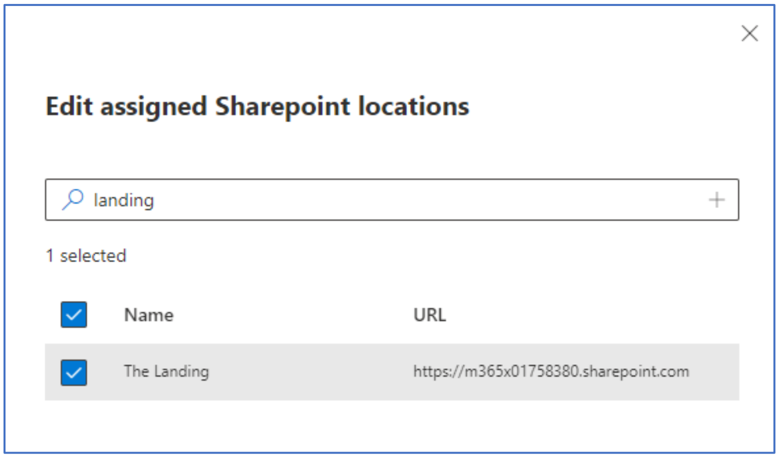


Figure 18 – Search for a Non-custodial location

Once the sites to add are selected click the '***Add***' button. You will be presented with a list of selected sites as displayed in Figure 19 – Non-custodial locations. You may place the sites on hold by leaving the blue checkbox to the right of the site names checked.

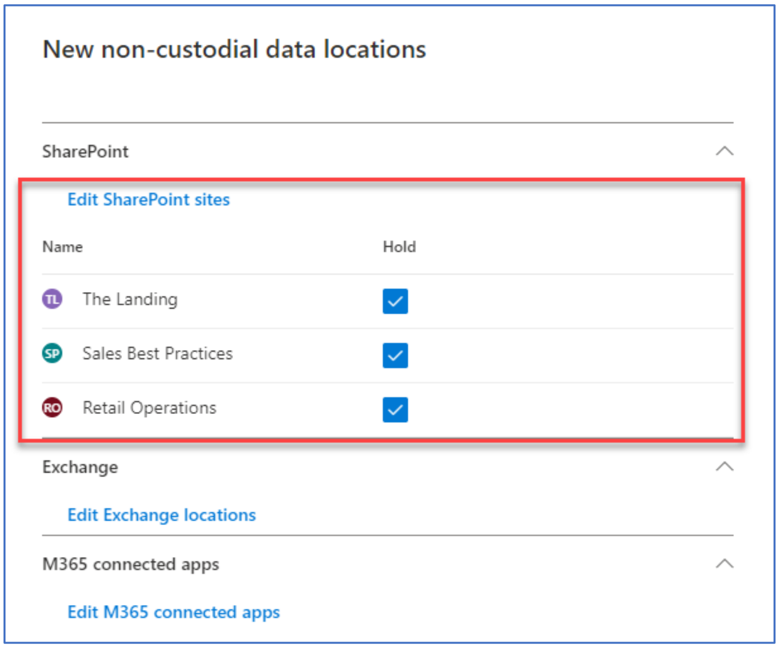


Figure 19 – Non-custodial locations

Once the non-custodial locations are added, the locations will appear in the list of Data Sources for the case.

Teams as Data Sources

Microsoft Teams is a multi-faceted, communication and collaboration platform. Along with commonly used features like 1:1 Chats and Meetings, Teams includes channel conversations, file sharing, integration with other M365 applications like Whiteboard, Planner, Forms and more.

Tip

We have observed that corporate legal departments and law firms may use a limited set of Teams features when compared to broader groups of corporate knowledge workers. This lack of understanding impacts workflow when identifying potentially relevant data sources in a case. Compounding this issue is the fact that Microsoft is continually enhancing Teams and is adding new features.

To fully understand what is being saved by Teams, technologist and attorneys should work together to ensure everyone understands what locations may be relevant in legal matters. Microsoft's Microsoft Teams help & learning is a great place to learn about the Teams user experience.

Legal groups should consider partnering with their organization's Teams administrators to better understand how Teams is being used. The Teams administration counsel includes reports that will show both what Teams features are being used in the environment along with what other applications are being used with Teams. See: Microsoft Teams analytics and reporting - Microsoft Teams | Microsoft Learn

Where Teams Stores Data

When a Microsoft Team is created, at least two underlying locations are created for the Team, a mailbox where Teams channel discussions are stored and a SharePoint site where documents and lists created and shared by the Team are stored. In addition to the primary mailbox and SharePoint site, additional SharePoint sites are created for a Team when Private or Shared Channels are created.

Teams Feature	How Feature is Used	Where Teams Saves this Data
Teams 1:X chats	Messages between two or more individuals	Messages in 1:X chats are stored in the Exchange Online mailbox of all chat participants.
Files shared in chats	Teams automatically uploads files shared in a chat into the sharer's OneDrive. Teams sends a link to the file to the recipients rather than a copy of the file. Microsoft refers to these files as Modern or Cloud attachments.	Files shared in a 1:X chat are stored in the OneDrive for Business account of the person who shared the file.
Teams channel messages	A Team is a digital workspace for a group of people who need to collaborate to get something done. Teams divide their workspaces into channels. Each channel is dedicated to a specific topic, department, or project. Team members post discussion topics, called channel messages, and share files in the channels. Most Teams channels are "standard" channels, that all team members can access.	All standard channel messages and posts are stored in the Exchange Online mailbox associated with the team
Teams channel files		Files shared in a standard channel are stored in the SharePoint Online site associated with the team.
Teams private channel messages	While all members of a Team have access to the Teams' standard channels, private channels may be access by a subset of Team members.	Messages sent in a private channel are stored in the Exchange Online mailboxes of all members of the private channel.
Teams private channel files		Files shared in a private channel are stored in a dedicated SharePoint Online site associated with the private channel.
Teams shared channel messages	Shared channels may be accessed by all members of a Team and can also be shared with additional individual or other Teams.	Messages sent in a shared channel are stored in a system mailbox associated with the shared channel.
Teams shared channel files		Files shared in a shared channel are stored in a dedicated SharePoint Online site associated with the shared channel.
Teams meetings chats – recorded meetings	When enabled, participants in a meeting may post chat messages in the meeting and share files in the chats.	Chats in recorded meetings are stored in the OneDrive for Business account for the user recording the Teams meeting.
Teams meetings recordings and transcripts	When enabled, the video, audio, and screen shares in a meeting will be recorded and saved as MP4 files.	Meeting recordings are stored in the OneDrive for Business account for the user recording the Teams meeting.
Teams channel meetings chats	Along with scheduling Teams meetings in their Outlook or Teams calendar, Team members may schedule meetings in a standard Teams channel. All members of	Channel meeting chats are stored in the Exchange Online mailbox associated with the team. Files shared in chats are saved in the SharePoint site for the Team.

Teams Feature	How Feature is Used	Where Teams Saves this Data
Teams channel meetings recordings and transcripts	the Team will see the meeting on their calendar and be able to join.	Meeting recordings are stored in the in the SharePoint site for the Team.
Teams reactions	Use emojis to react to Teams chats and Channel Posts.	Information about the reaction such as who reacted to the message and when they reacted are stored in the message metadata.
Teams gifs and stickers	Microsoft includes a large library of animated GIFs that Team users may use to add personality and fun to Teams messages. Stickers are images with customized text that users may share in messages.	Gifs and the image components of stickers are stored on Microsoft's servers. When Teams messages are collected by the Microsoft eDiscovery tools, the images are not collected. Instead links to the images are included in the collected text.

Note
In June of 2023, Microsoft enhanced the options for reviewing the video of recorded meetings and the associated transcripts. For more information see, eDiscovery (Premium) workflow for content in Microsoft Teams | Microsoft Learn

For more and up to date information on where Teams data is stored see: Where Teams content is stored | Microsoft Learn

Teams as Custodial Sources

Custodians may be associated with Teams where they have current memberships. Like other custodial data sources, Teams locations will go through the deep indexing and OCR processes. You will also have the option to put the Teams locations on hold. When adding a custodian, choose the '**Edit'** link to see a list of all the custodian's Teams, as see in Figure 20 – Select Teams for a Custodian.

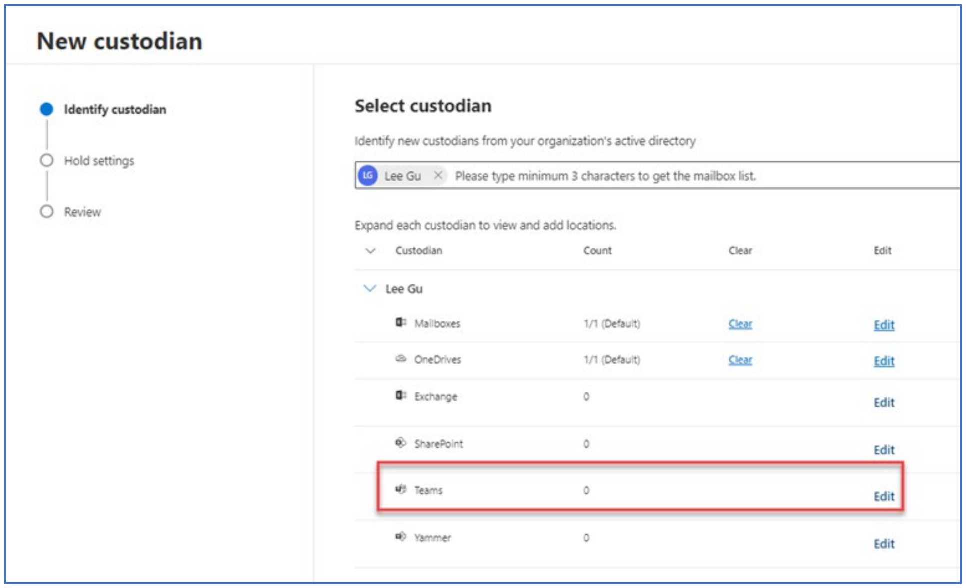


Figure 20 – Select Teams for a Custodian

The list of teams will include two entries. One for the Team mailbox and the other for the Team SharePoint site. These locations include the channel discussions and files shared in the standard channels in the Team.

As demonstrated in Figure *21* - Select Custodial Teams, both the Mailbox and SharePoint site have been selected. We could select all the custodian's teams by checking the box to the left of the "name" column heading.

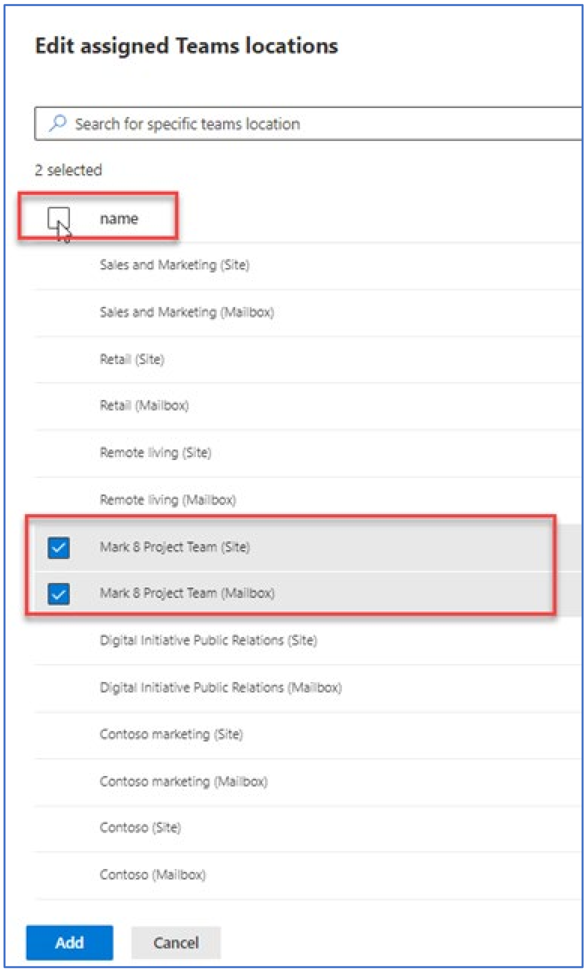


Figure 21 - Select Custodial Teams

> ***Note***
> *Selecting all Teams for a custodian selects just the Teams where the custodian has a current membership. If the custodian joins other Teams in the future, the Teams will not be added automatically to the case.*

Teams as Non-Custodial Sources

In September 2023, Microsoft added the ability to add Teams locations as non-custodial data sources. As of this writing the feature is still in preview and the functionality may evolve over the coming months.

Adding Teams as non-custodial sources allows you to search across all Teams within the M365 tenant and add the primary Mailbox and SharePoint site as data sources for the case. The tool also identifies

Private and Shared channels allowing you to add the sites for these channels as data sources. Finally, add Teams as data sources will identify users that are members of private channels and add their mailboxes as non-custodial data sources.

For more information on adding non-custodial data sources see: [Add non-custodial data sources to an eDiscovery (Premium) case | Microsoft Learn]

Update Data Sources

When a data source is first added to a case, Premium eDiscovery preforms advanced indexing and will OCR images in the specified locations if OCR is enabled for the case. New data added to locations is not automatically indexed for the case. In addition, if OCR is enabled in a case after a source is added, OCR is not automatically preformed on the locations. Updating the index on a data source will index any new items and OCR images after OCR is enabled.

To update the index on just one data source, select the vertical ellipse to the right of the data source in the data sources listing and choose update index as seen in Figure *22* - Update Data Source Index. To update the index on multiple locations, select the sources from the list and choose update index from the menu above the listing.

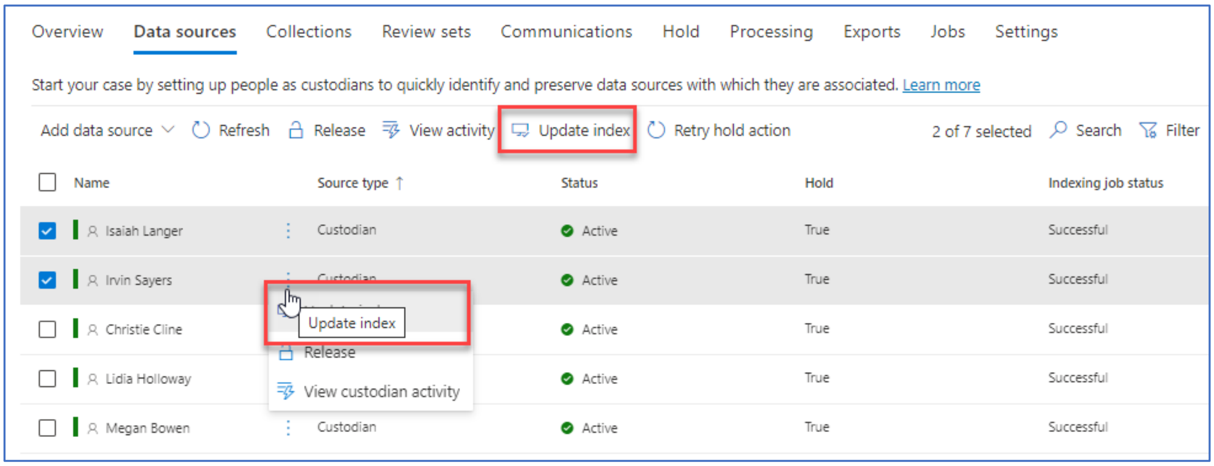


Figure 22 - Update Data Source Index

Hold

Important Note

If you have been asked to place an account or location on hold, your first impulse may be to go to the Hold tab in the Premium eDiscovery menu or to go into the Exchange administration console and place a hold there. Typically, these are not the best approaches. Instead, you should head to the Data Sources tab in the Premium eDiscovery menu. When you add an account as a custodian in a case or add other locations as non-custodial data source, you have the option to enable preservation on the locations AND enable deep indexing and OCRing of the locations.

In both Microsoft Purview eDiscovery Standard and Premium, a hold is a policy that contains multiple locations where preservation is required in the case at hand. When you add data sources to a case and place them on hold, a hold policy will automatically be added to the case and Microsoft will automatically manage the hold locations. You may also manually create hold policies in a case.

Understanding Preservation in Microsoft Purview

Unlike third party archive or backup systems, which make copies of data for preservation and store those copies elsewhere, Microsoft uses preservation in place. If a user deletes or modifies an item in a location on hold, Microsoft preserves the original file in that location. No one can delete or modify the preserved copies until all holds on the location are lifted.

Preservation for Mailboxes

Traditionally, Exchange Administrators manage mailbox holds through the Exchange Administration Console litigation hold feature. In Exchange, A litigation hold is a yes/no switch on a mailbox. It is either on hold or not on hold. Nothing in the Exchange Administration Console allows the administrator to note why a mailbox is on hold. If a mailbox needed to be preserved for multiple matters, the company would need to manually track why the mailbox was on hold.

Unfortunately, companies would lose track of why a mailbox had litigation hold enabled and never release holds in fear of violating their obligation to preserve. This led to the over retention of email.

To differentiate traditional exchange litigation holds, Microsoft calls the holds in Standard and Premium cases eDiscovery Holds. With eDiscovery Holds, a location may have preservation enabled in multiple cases. The holds are managed independently of each other. This means you may lift a hold in one case when the need for preservation is over without impacting holds in other cases.

The underlying method of preservation is the same for mailboxes when placed with Exchange or the Purview eDiscovery platforms. Exchange saves deleted and modified mailbox items in a hidden folder (what Microsoft calls a substrate folder) in the recoverable items folder. For a deeper dive into how Microsoft preserves mailbox see: Recoverable Items folder in Exchange Online | Microsoft Learn

> **! *Important Note***
> *Microsoft plans on eventually retiring the ability to place holds in the Exchange Administration console. After the feature is disabled, holds will need to be managed in either Purview Standard or Premium eDiscovery.*

Preservation for SharePoint

When holds are managed by Exchange Administrators in the Exchange Administration Console, preservation is not enabled for SharePoint and OneDrive locations. In the past, many companies relied on business units to preserve SharePoint data by making copies of files which were then turned over to the requesting legal team. Both Standard eDiscovery and Premium eDiscovery allow you to manage preservation for SharePoint and OneDrive centrally along with Exchange.

When a user deletes or modifies an item in a SharePoint or OneDrive location on hold, the item is retained in the preservation hold library for the site. The preservation hold library is a hidden system location. It is not designed to be used interactively but does contribute to the total storage size for a site. For a more in depth explanation into how Microsoft retains and preserves SharePoint data see: Learn about retention for SharePoint and OneDrive | Microsoft Learn

Manually Creating a Hold

Important Note

Keep in mind that when you manually create a hold, advanced indexing will not be enabled on the location on hold.

Navigate to the ‘Hold’ tab shown in Figure 23 – Create a Manual Holdand press ‘**Create**’.

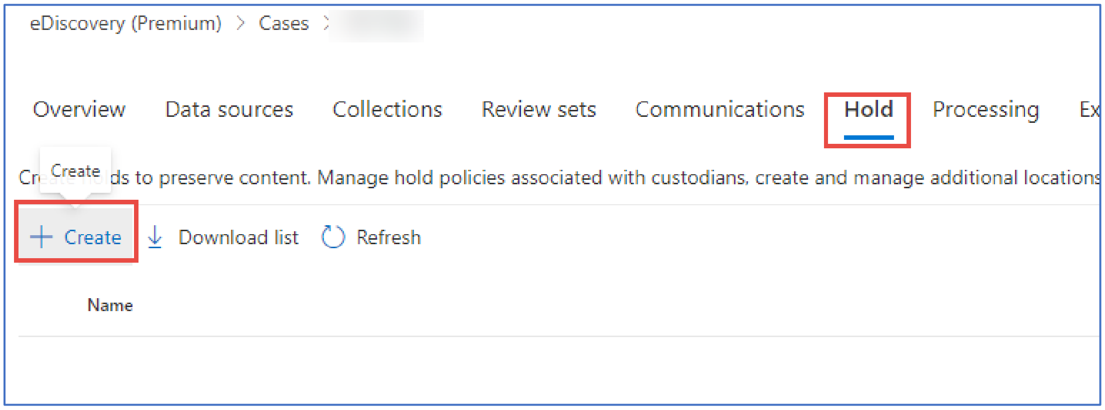


Figure 23 – Create a Manual Hold

Choose locations as demonstrated in Figure 24 - Choose Locations for Manual Hold. Choose the content locations that you want to place on hold. You can place Exchange mailboxes, SharePoint sites (which includes OneDrive), and Exchange public folders on hold.

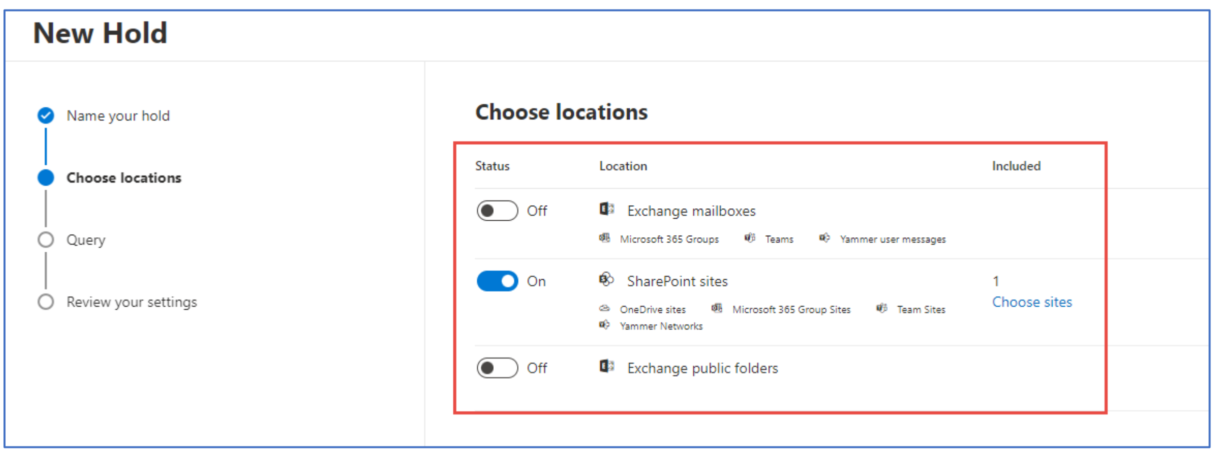


Figure 24 - Choose Locations for Manual Hold

Optional: Limit a Hold with a Query

You can limit a hold, rather than placing an entire location on hold, by using a query (as displayed in Figure 25 – Enter Queries for Hold. The query can specify keywords, message properties, or document properties, such as file names. You may also use broader properties such as a date range to limit the hold (as shown in Figure 26 – Condition card builder for Holds.).

Even though Microsoft allows you to use key words to limit a hold, we generally do not recommend doing so. There are two reasons for this:

1. Legal matters frequently evolve. What is believed to be the key terms at the start of a matter may expand by the end of a matter. If preservation was limited to smaller sets of key terms, potentially relevant data may be lost.
2. If the total characters of all hold queries placed on a location is greater than 10,000 characters, the queries will be ignored and everything in the location will be preserved.

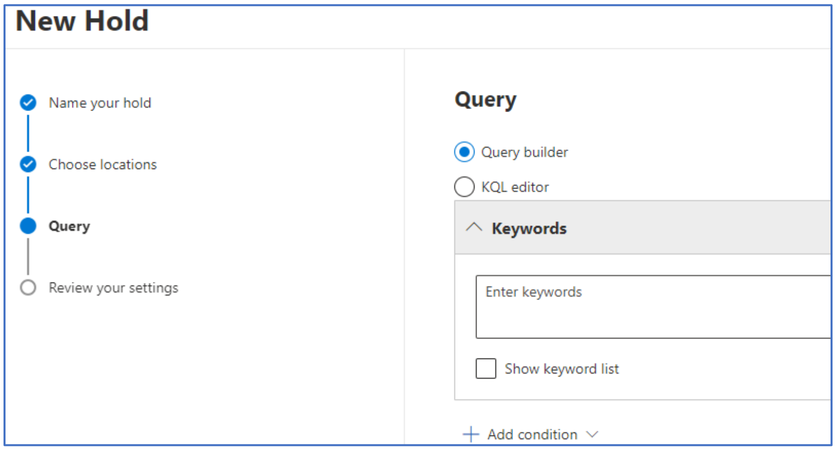


Figure 25 – Enter Queries for Hold

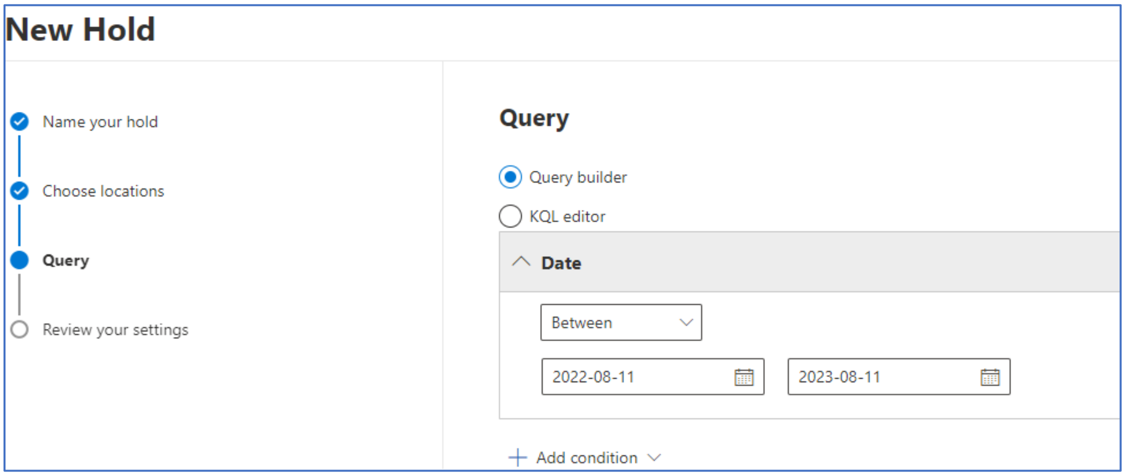


Figure 26 – Condition card builder for Holds.

Microsoft recently announced the ability to use PowerShell to

Communications (Issue a Legal Hold)

Microsoft Purview eDiscovery Premium allows legal departments to simplify their processes around tracking and distributing legal hold notifications. The custodian communications tool enables legal departments to manage and automate the entire legal hold process, from initial notifications, to reminders, and escalations, all in one location.

Create a Communication from Scratch

1. From the main case screen, select the **Communications** tab and click **+New communication.** As demonstrated below in Figure 27 - New Communication.

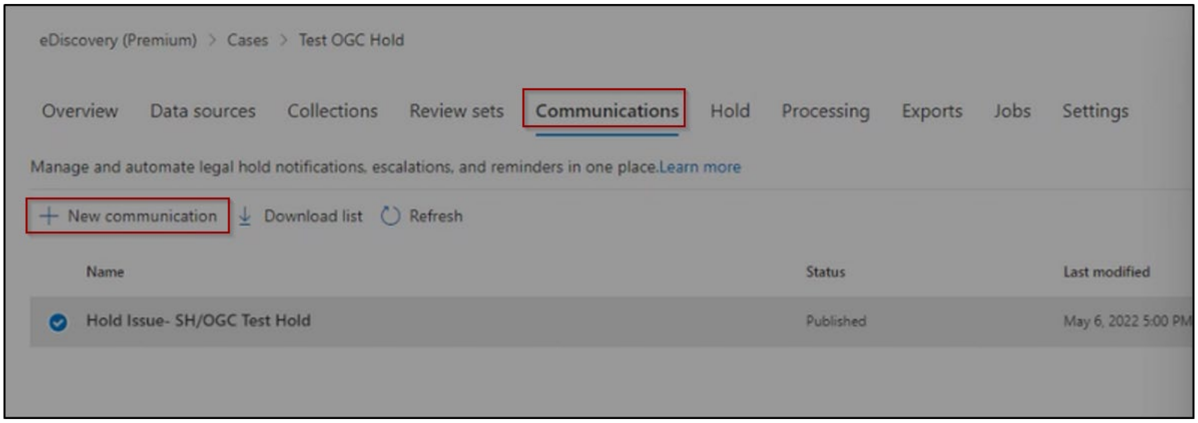


Figure 27 - New Communication

2. Enter a name for the communication, then select the "Issuing officer", and click **Next**, as displayed in Figure 28 - New Communication, Issuing Officer

> ***Note***
> *When you or others create a hold notification or other type of communication that is sent to a user who is a custodian in the case, you must specify an issuing officer. The notification is sent to the custodian on behalf of the specified issuing officer. For example, a paralegal in your organization might be responsible for creating and sending hold notifications to custodians in a case. In this scenario, the paralegal can specify an attorney in the organization as the issuing officer.*

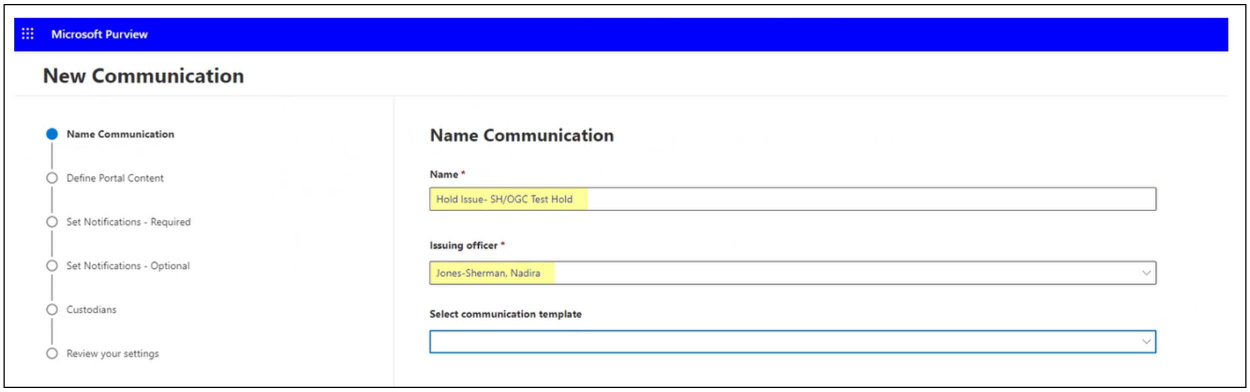


Figure 28 - New Communication, Issuing Officer

> ***Note***
> *Note: Custodians will receive hold notification emails that appear to be from the "Issuing officer". This individual will also be named in the Communication Portal and issuance / release emails when the "Issuing officer email" merge variable is used....*

3. **Define Portal Content**: The portal content will contain the **primary** language for the hold parameters and issuance. The full text will be provided in all notification emails as well as in a centralized portal for each custodian that tracks each of the custodian's cases with hold obligations, as shown in Figure 29 - Define Portal Content.

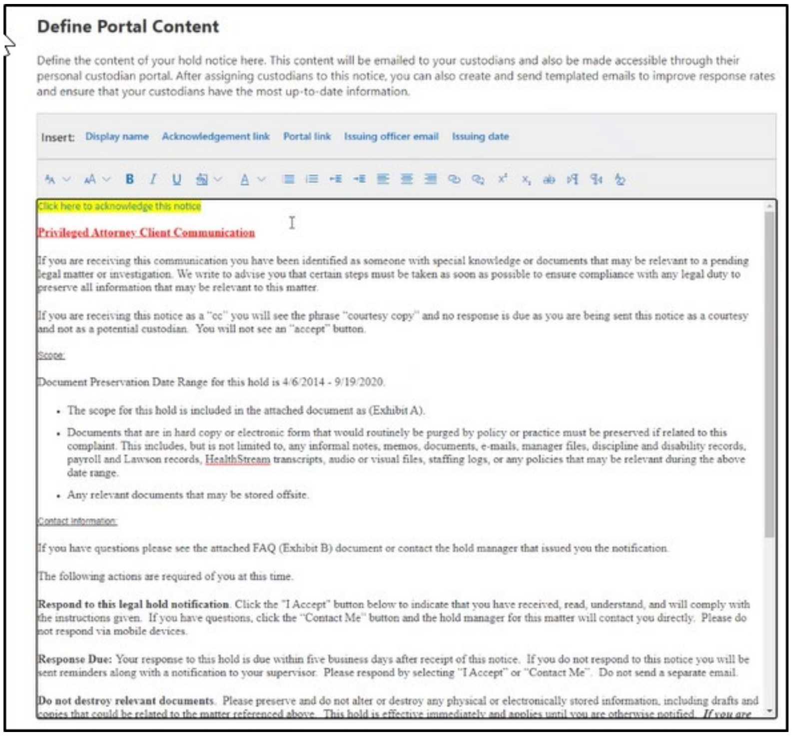


Figure 29 - Define Portal Content

There are three "merge variables" and two "links" available for insertion into the portal language. Merge variables do not change and can be retained and reused in boiler plate hold language. Links **must** be replaced during the initial portal content creation within each case.

a. **Display name:** Custodian name with merge variable in the format of {{DisplayName}}

b. **Acknowledgement link**: It is **crucial** that this link must be placed during this initial process of developing the portal content by placing the cursor within the document at the appropriate location and clicking **Acknowledgement Link** at the top. Failure to do so will prohibit custodians from the ability to acknowledge notices.

c. **Portal link:** To avoid confusion, and to help ensure custodians utilize the acknowledgement link, we do not recommend using the portal link on the Portal Page.

d. **Issuing officer email:** The email address of the individual selected in step #2 above with merge variable in the format of {{IssuingOfficerEmail}}.

e. **Issuing date:** The date that the custodian first received notice of the hold as a result of this process (when Send Notice is selected at the end of this section). This is formatted as {{IssuingDate}}.

4. Once the portal content is complete, click the **Next** button to move to the next page in the wizard.

5. **Set Notifications – Required**: This area, depicted in Figure 30, contains three sections, all of which must contain language before proceeding with this process. To avoid duplicating language presented to custodians and prevent potential confusion, we recommend keeping issuance / reissuance language to a minimum. Select '**Edit'** for each appropriate section.

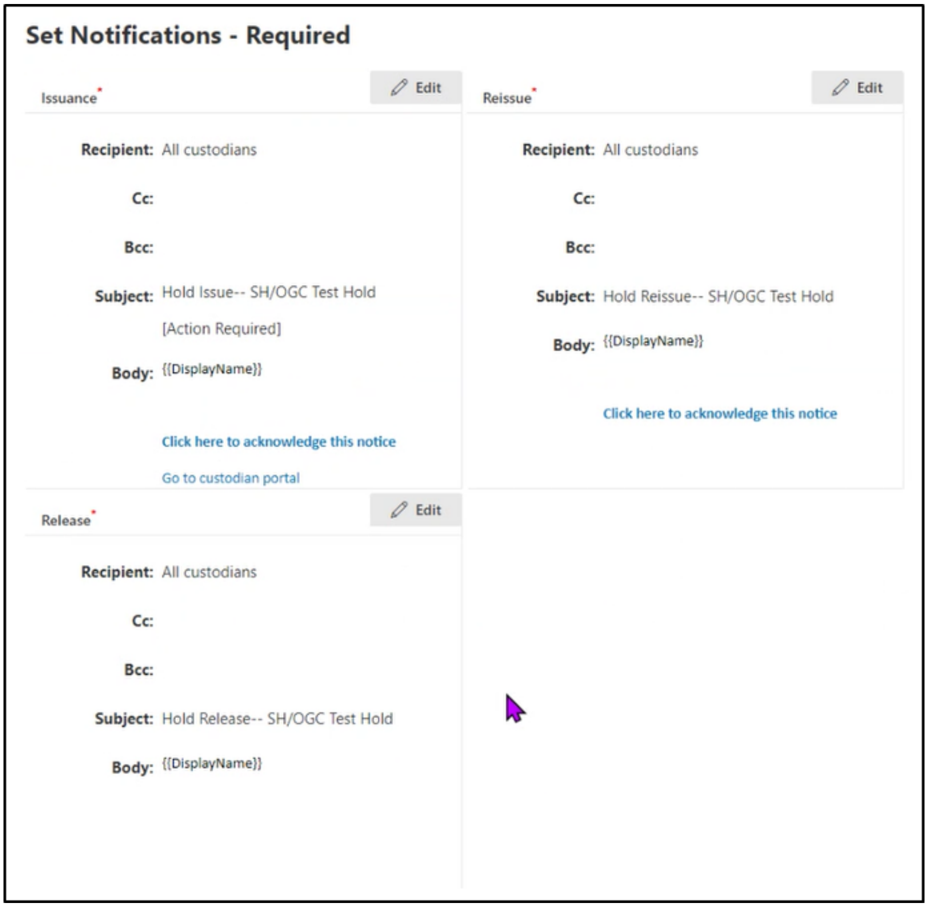


Figure 30 - Set Notifications

a. **Issuance:** The issuance email is sent to the selected custodians when the communication is first published. The portal content will be appended to the body of this email. Ensure that the subject line & body contains appropriate language as it relates to this matter and click '**Save'.**

b. **Reissue**: When the Portal Content is changed in any way due to the changing parameters of a case and the resultant hold, the language of this reissuance email will automatically go to the selected custodians with the portal content appended to the message. Acknowledgements of the reissued communication will be tracked. tracked. Click ‘**Save’** after customizing the subject line & body.

c. **Release**: Upon closing of the case or the lifting of a hold from a custodian, the language placed in the body of this section will be emailed to the custodian(s). Click ‘**Save’** after customizing the subject line and body.

> ***Tip***
> Because portal content is not included for release emails, consider including the full legal hold release language including acknowledgement link, in the Release email as shown should be provided here as shown below in Figure 31.

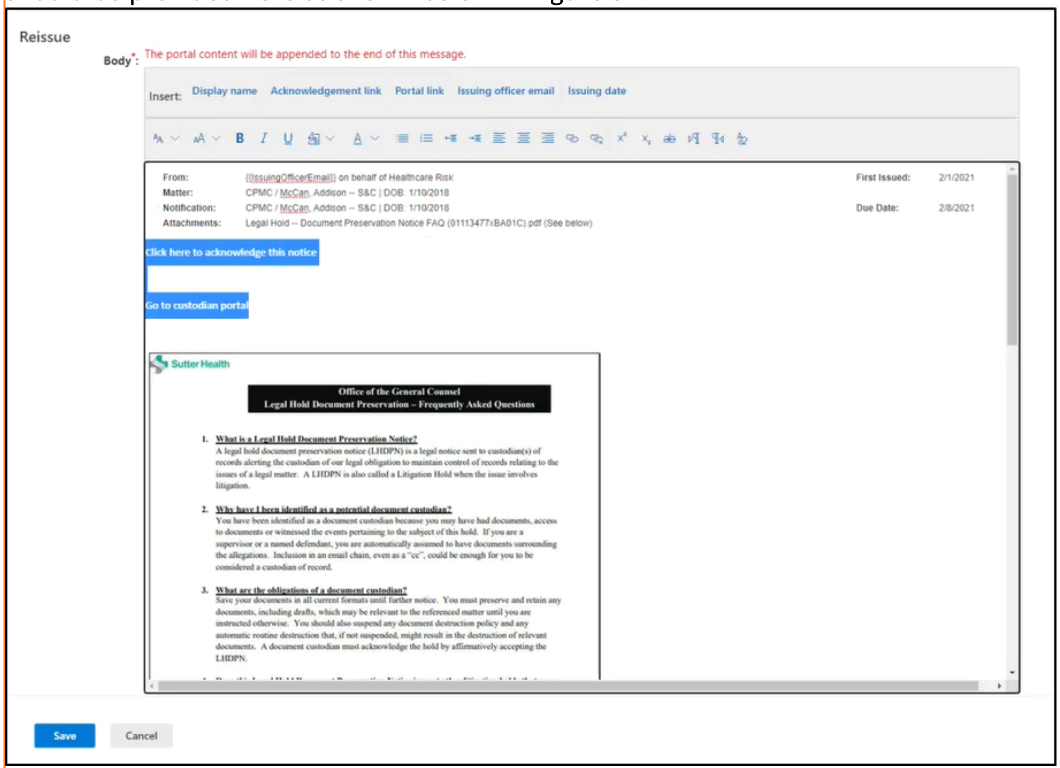


Figure 31- Release Email

6. Ensure that all three notification sections are populated and select ‘Next’ to move to the Optional Notifications page.

7. **Set Notifications – Optional**: This section provides the ability to send reminder and escalation emails when custodians have not acknowledged the issuance or reissuance communications. These communications are optional. To enable either message, select ‘**Edit’** on each of the two sections:

   a. **Reminder**: These emails will be sent automatically on a schedule and count of your choosing. Toggle the status switch to ‘**On’** to enable the reminder, enter reminder interval and number of reminders, subject, email body, and select ‘**Save’**. As displayed in Figure 32 - Notification Reminders

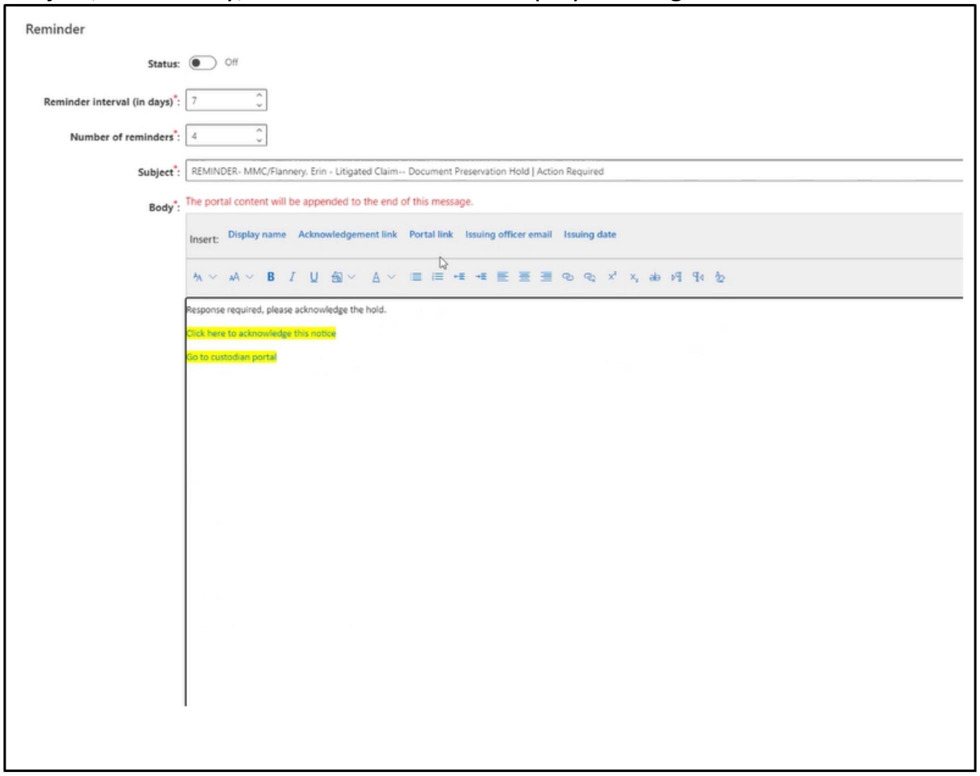


Figure 32 - Notification Reminders

b. **Escalation**: If desired, escalation emails can be automatically sent to a custodian and their manager if the custodian still has not acknowledged the communication once the reminder emails have exhausted their schedule. Configuration of the escalation emails is identical to the reminder messages. Click the **Next** button to move to the **“Choose custodians you want to notify”** of the communication wizard.

> ***Note***
> *For a custodian’s manager to be included in escalation emails, the custodians account properties in Entra (formerly known as, Azure Active Directory,) must include their manager.*

8. To select the custodians to receive the communication, choose **Select custodians**, as illustrated in Figure 33, and select the appropriate custodians from the resulting list. Click the **Add** button to add the custodians to the custodians to notify list. When your selections are complete, click the **Next** button to move to the **Review your settings page.**

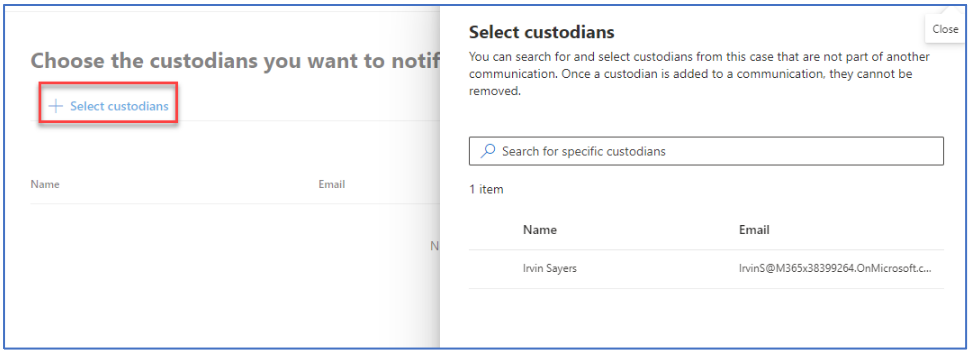


Figure 33- Select Custodians to Notify

Tip
In some matters, for example an investigation into the actions of some case custodians, not sending a communication to all custodians is prudent. Premium eDiscovery supports these scenarios. if you do not publish a communication to a custodian, they will never receive a hold notice and will not receive a notice when the hold is lifted, or the case is closed..

9. Review your settings: You will be presented with a summary of the content entered during steps 1 through 8 above. This will be your final opportunity to ensure no errors are present prior emails being sent to the selected custodian(s). If you find changes to make, clicking the edit links within the summary will take you to page in the communication wizard to make the change.

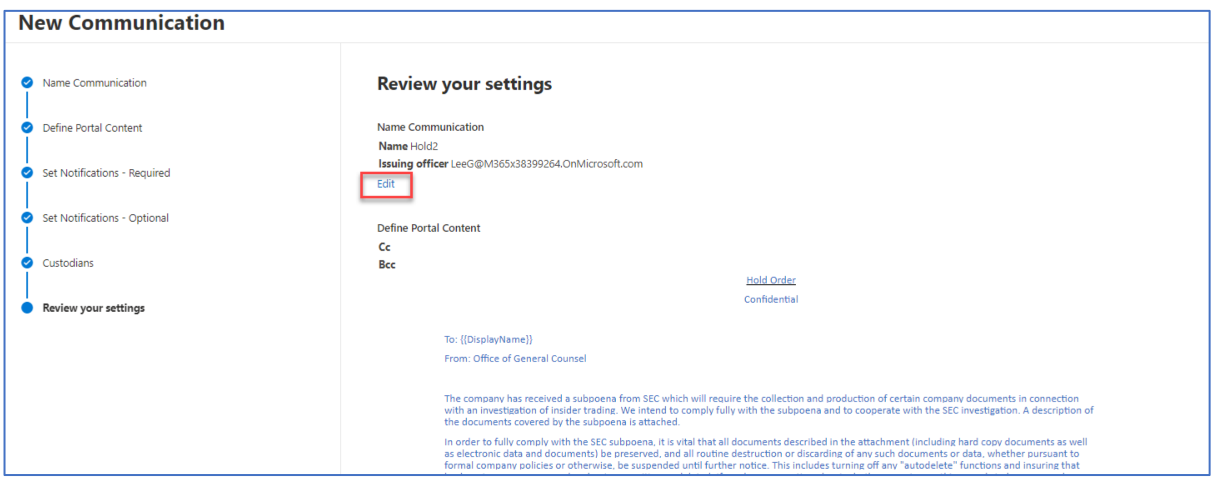


Figure 34- Communication Summary

10. Once you have confirmed the Communication is correct, click the **Submit** to publish the communication to the custodians.

Monitor and Report on Communication Acknowledgements

Selecting the communication from the list on the ‘**Communications’** tab, as shown in Figure 35 – Hold, opens a panel where the acknowledgment status of each custodian may be monitored.

Note
As of this writing, the Acknowledged metrics provided under the Communications panel on the Home tab may be out of sync.

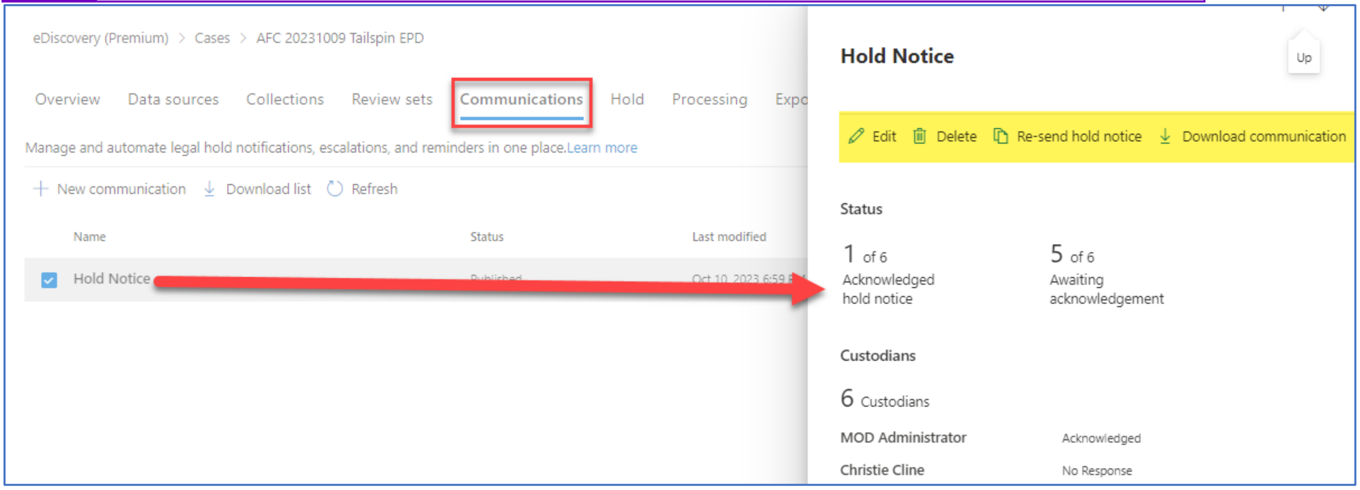


Figure 35 – Hold Notice Panel

Through the menu at the top of the Hold Notice panel (highlighted in yellow in Figure 35,) the communication may edited, deleted, or reissued. A report including the current portal content, notification language, and acknowledgment status may also be printed through the **Download Communication** menu option.

Important Note
Custodians will NOT receive a release notification if the communication is deleted. Release notifications are sent is a hold is lifted on a custodian or a case is closed.

Tip
Many legal teams regularly print the communication report to PDF to include in their case files and share with outside counsel.

Create a Communication from a Template

As detailed in the Create a Communication from Scratch section above, the creation of a communication is a multi-step process. To help streamline the workflow and ensure language consistency across communications, Premium eDiscovery allows eDiscovery Administrators to build communication templates that eDiscovery case managers may use to create communications.

Templates are created in the Premium eDiscovery Settings menu. The process to create a template is almost identical to the instructions in Create a Communication from Scratch. The only differences being you do not select an issuing officer or publish the template to custodians.

To create a new communication based on a template, follow the instructions in steps 1 through 3 in in Create a Communication from a Template but choose a communication template as shown in Figure 36

- New Communication. The new communication will pre-populated with the portal content and notifications from the template. These can then be customized for the case and published to custodians.

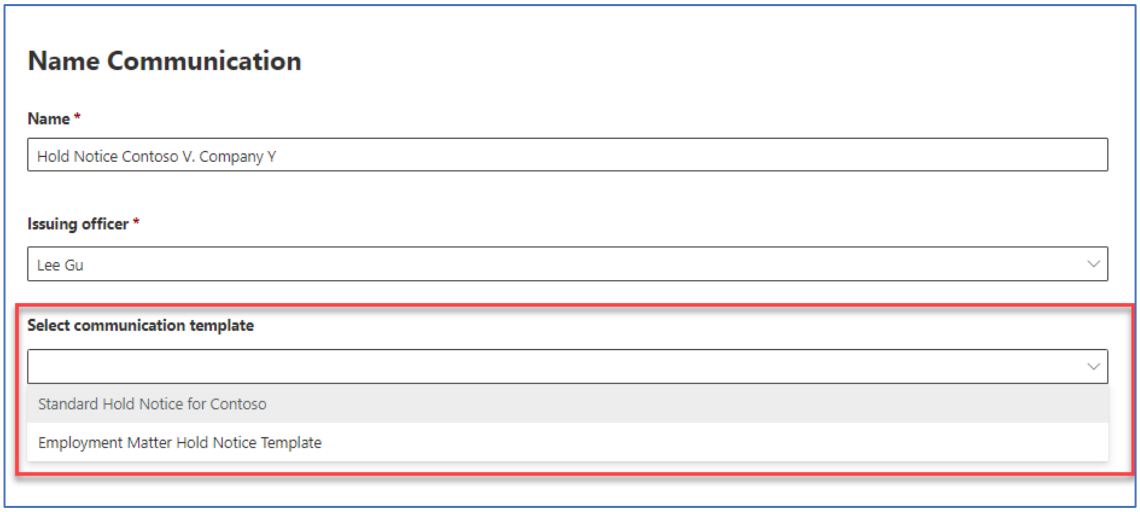


Figure 36 - New Communication from a Template

> ***Tip***
> *If a preview or draft of the notice content is required prior to sending notices to custodians, the notice can be saved (submitted) with no custodians selected. The communication will be saved as a "draft." If a snapshot PDF of the entire notice settings and text is desired, select the notice name (anywhere on the name except the check box), and the blade on the right will open. Select 'Download Communications' and print the preview to PDF*

Collections

Once the case is created and custodians are added, the next stage is to search for the data that will be relevant to the investigation. In the Collection phase, Premium eDiscovery enables you to collect data from the M365 workloads in a forensically sound manner, ensuring that the integrity and authenticity of the data are maintained. You can export emails, documents, chats, and other forms of Electronically Stored Information (ESI) to a secure location for further processing and review. The Collection phase allows you to reduce the volume of data that needs to be processed and reviewed by applying filters such as date range, file type, keywords, etc. You can also preview the estimated results of your collection before exporting them to a review set. By focusing on the most relevant and responsive data for your case, the Collection phase helps you save time and costs.

Collections allow the collation of all the data sources for an investigation. A search can be run against this data providing an estimate of how much data will be collected before committing the data to a review set for further analysis.

More information on collections can be found here: eDiscovery collections | Microsoft Learn

Create a Collection

To create a new collection for a case, select '**Collections**', and then select '**New Collection**' as displayed in Figure 37 - Create a Collection.

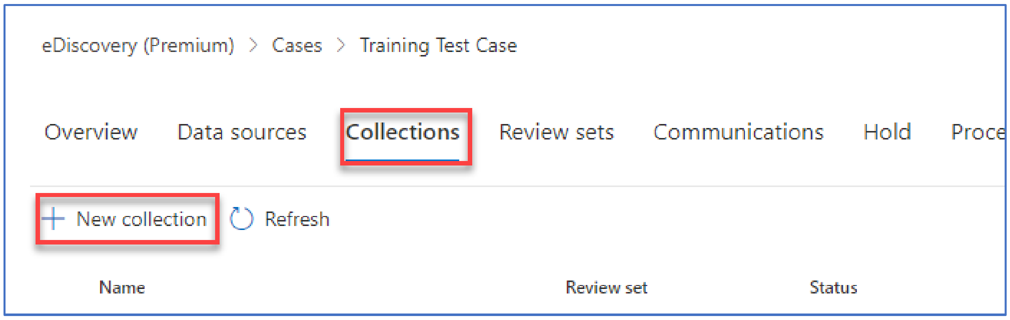


Figure 37 - Create a Collection

The wizard will first ask you to name the collection and provide a description, as shown in Figure 38 - New Collection.

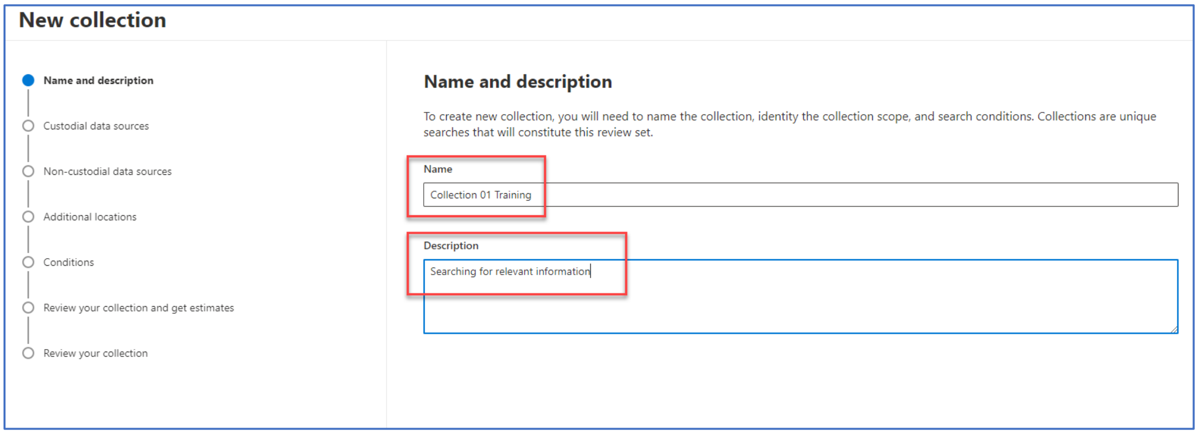


Figure 38 - New Collection

At the next stage select which custodians will be a part of this investigation. Custodians selected here will have their data sets searched, and thereafter, be added to the case for review.

Select Custodial Sources for Collection

The Collection option '**Select Custodians**' (item 1 in Figure 39) opens the dialog in Figure 40, displaying all case custodians. Through this interface you may choose a subset of the case custodians to include in the search. Enabling the '**Select All**' slider (item 2in Figure 39) adds all available custodians and all custodial locations as data sources for the collection search.

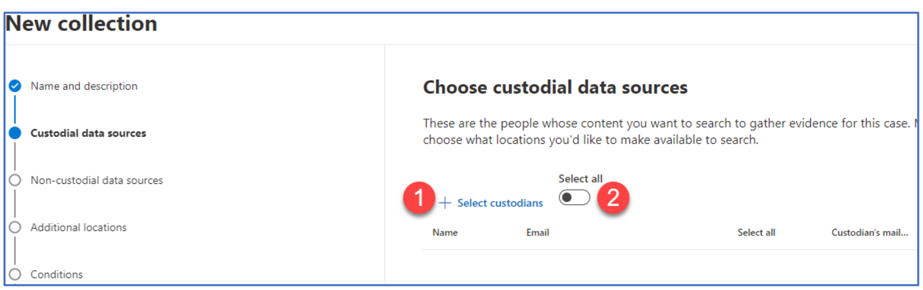


Figure 39 - Choose Custodial Data Sources

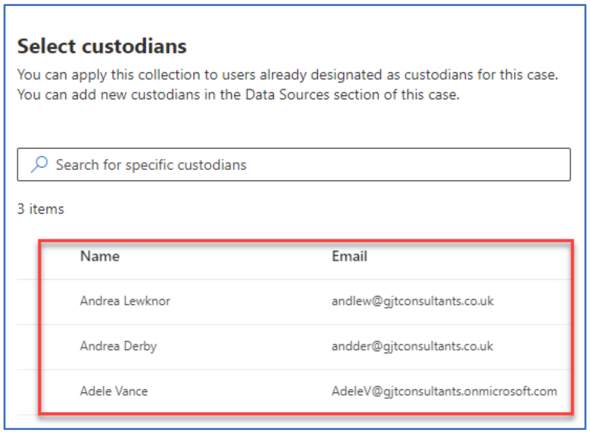


Figure 40 - Select Custodian Sources

Select Non-Custodial Sources for a Collection

Non-custodial data such as sites and groups can be added to this collection. The process of selecting a '**non-custodial source**' or '**Select All**' as highlighted in Figure 41 - Add non-custodial data sources is identical to the custodian selection behavior above.

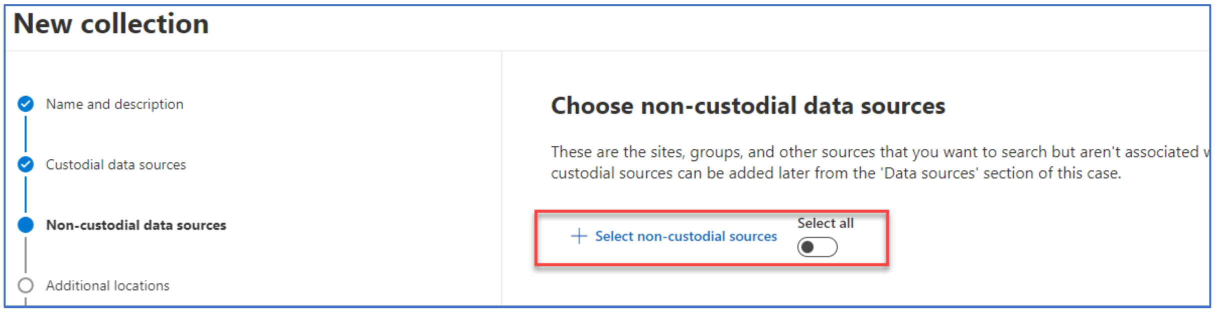


Figure 41 - Add non-custodial data sources

Select Additional Locations to Search in a Collection

Along with searching the data sources identified in a case, collections may search across other M365 locations. There are multiple scenarios where you may find yourself needing to search places other than the indexed case data sources. For example:

1. You do not know who your custodians are. Take an instance where anyone who communicated with joe@fictionalcompany.com is a potential case custodian. An exploratory search of all user mailboxes will identify who communicated with Joe. The people identified can then be added to the case as custodial data sources.

2. You have identified your custodians and added the custodian mailboxes and OneDrives as custodial data sources. Your need to identify SharePoint sites where the custodian has created and modified files. Counsel plans interviewing the custodians about the locations where they saved files to determine if the locations should be preserved and collected from.

Important Note

*Additional Location searches do **NOT** use Premium eDiscovery's advanced indexing or OCR. Because of this, additional location queries based on keywords may not return all* *responsive documents. Searches based on metadata like Date or email sender will return accurate results..*

Important Note

Depending on the size of your environment, additional location searches on all locations in your environment may take multiple hours to complete while searches based on data sources will take minutes, even when searching hundreds or thousands of data sources. . Avoid ALL location searches unless necessary.

Additional Location Searches: Exchange

Sliding the '**Exchange mailboxes'** slider to on as shown in Figure 42 enables searching mailboxes. By default, Premium eDiscovery will select "All" active mailboxes in the environment. You may narrow the locations to search by clicking the **"Choose users, groups, teams."**

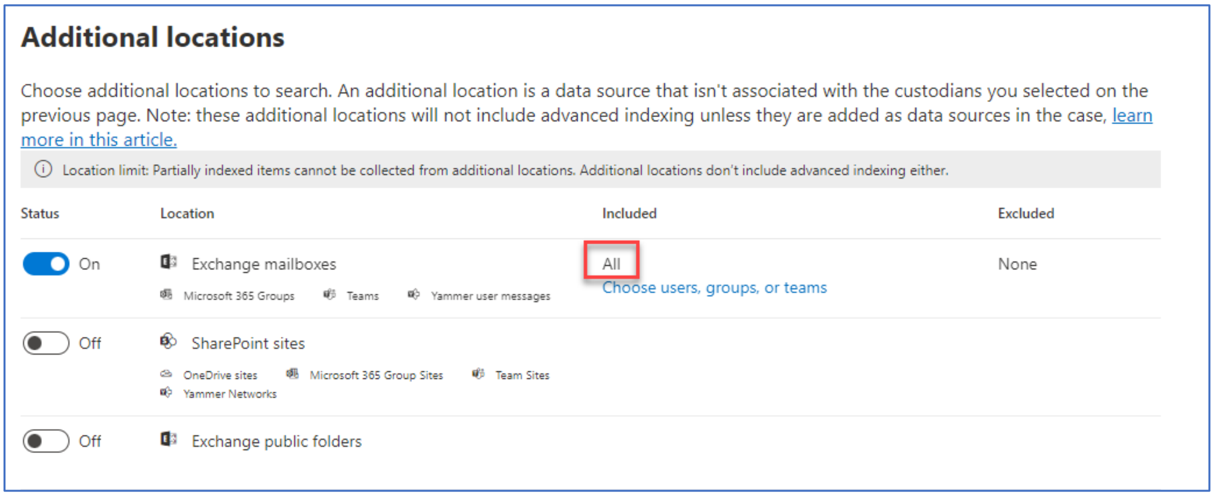


Figure 42- Additional Locations Exchange

Simultaneously searching all mailboxes in a tenant is slow and may cause performance issues in busy email systems. To speed up "All**"** searches and give you more granular control over what is searched, Microsoft introduced options to scope the "All" locations in June of 2023. When the Exchange mailboxes left to the default of "All", the search options listed in Figure 43 are enabled in the **"Additional search options"** section at the bottom of the page.

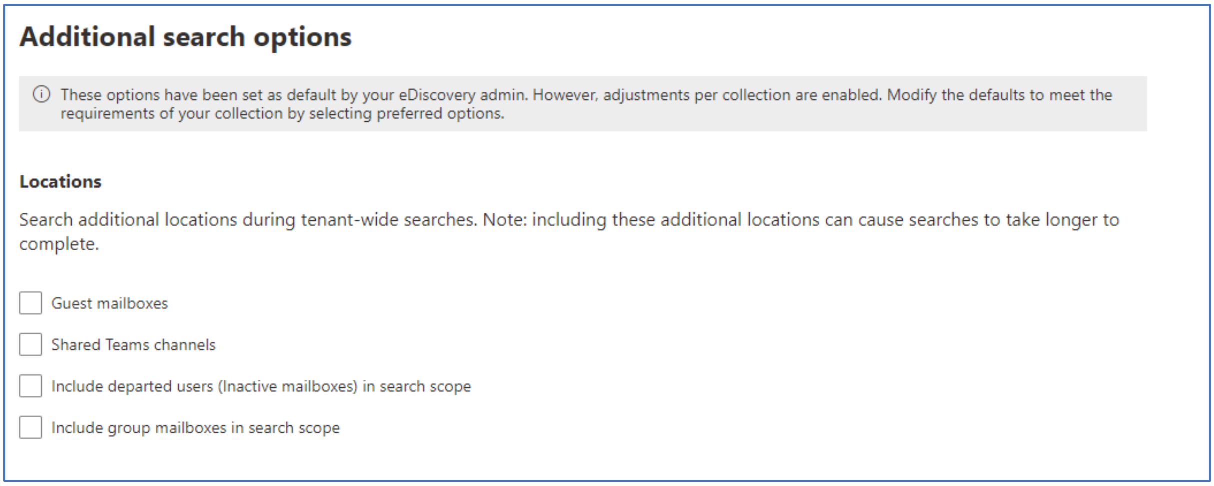


Figure 43- Search Options for Exchange "All" search

The "Additional search options" dialog includes these options:

1. **Guest Mailboxes**: When an external user is invited as a guest in an organization's M365 environment, a shadow mailbox is created for the guest user. Items like Teams chat messages sent by the guests while logged into the host environment are stored in the guest mailboxes. Checking this checkbox will include all guest mailboxes in your search. See [Guest access in Microsoft Teams - Microsoft Teams | Microsoft Learn] for more information on guest access in Teams.
2. **Shared Teams channels**: Compliance copies of messages posted in a Teams shared channel are saved in a shadow mailbox tied to the Team's primary mailbox. To include messages posted in all Shared channels check this box. To learn more about Shared channels see: [What is a shared channel in Microsoft Teams? - Microsoft Support].
3. **Include departed users (Inactive mailboxes) in search scope**: Inactive accounts are accounts that had a hold in place, or a retention policy applied when the mailbox license was removed. These accounts usually represent former employees. To include Inactive mailboxes in the search, check this box. For more information on Inactive Accounts see*:* [Create and manage inactive mailboxes | Microsoft Learn]
4. **Include group mailboxes in scope**: Microsoft Groups is a membership service that serves as the base for applications like Teams. When a Microsoft Team is created, a group mailbox is also created. Group mailboxes may also be created independently from Teams. To include Teams channel discussions and other group mailbox messages in search check this checkbox. To learn more about Microsoft groups see: [Microsoft 365 Groups and Microsoft Teams - Microsoft Teams | Microsoft Learn]

Additional Location Searches in SharePoint

Like the Exchange mailbox slider in the Additional locations dialog, sliding the **SharePoint** sites slider to on will default to searching all SharePoint sites. This includes all SharePoint, Teams, Yammer (Viva Engage), Groups, and OneDrive sites. You may search for and select indvidual SharePoint sites as shown in **Error! Reference source not found.** rather than searching against all of SharePoint. Keep three things in mind when selecting SharePoint sites in this dialog.

1. You cannot search for OneDrivesusinging this dialog but can paste in the URL for a user's OneDrive. See View the list of OneDrive URLs for users in your organization - SharePoint in

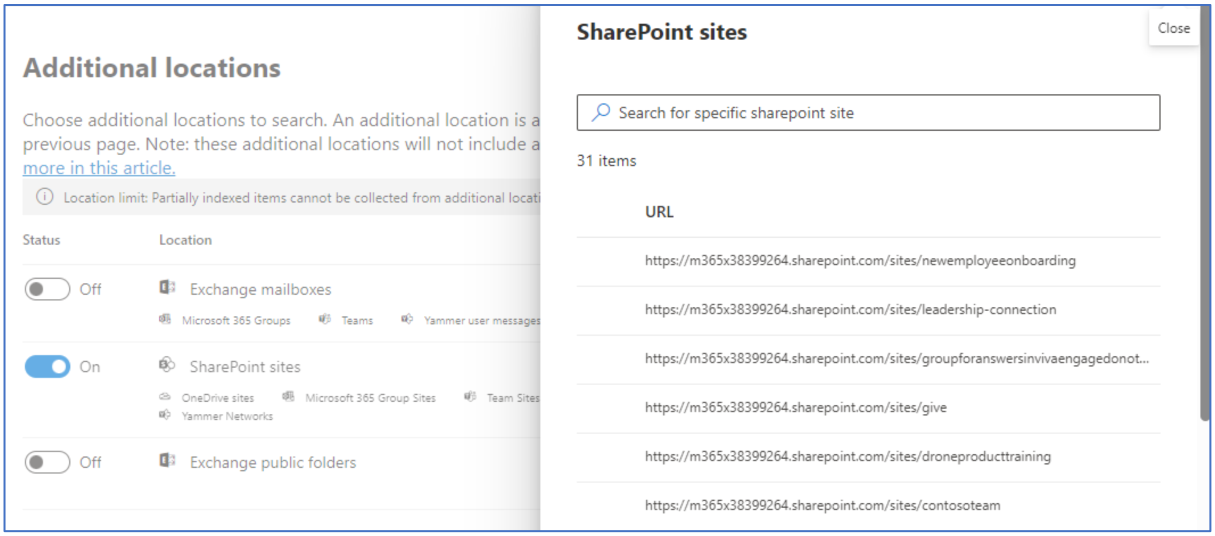


Figure 44 - Additional SharePoint Locations

   Microsoft 365 | Microsoft Learn for more information regarding detemine a user's OneDrive URL.

2. You may search by both site name and ite URL. However, if you cannot typically access a SharePoint site, you will not ba able to search by site name. You will still be able to select sites if the URL is known and collecect results from the site.
3. Keep in mind that SharePoiny selections are at the site level. You cannot choose an indvidual document library or folder.

Define your Search Query

The search query defines the conditions used to retrieve specific items from the selected custodian data sources, non-custodial data sources, and additional locations selected in the collection wizard. Premium eDiscovery provides three interfaces to build queries: 1) The New Query Builder, the Condition Card Builder, and 3) the Keyword Query Language (KQL) editor.

Both the New Query Builder, which was introduced in May of 2023, and the Condition Card Builder allow you to graphically build KQL queries using the most used search filters. The New Query builder allows you to build more complex queries compared to the traditional Condition Card builder with AND/OR conditions and query condition groups. The KQL editor assists you with drafting KQL queries by suggesting properties you may want to search as you type your query.

All three interfaces build queries using Microsoft's Keyword Query Language (KQL). KQL is used in Premium eDiscovery in both collection queries and review set filters. Premium eDiscovery includes many search features like keywords, metadata, analytics, and Boolean, proximity, and connector operators along with wildcard searches. For more information Premium eDiscovery search options see: Keyword queries and search conditions for eDiscovery | Microsoft Learn

Use the New Query Builder to build a Query

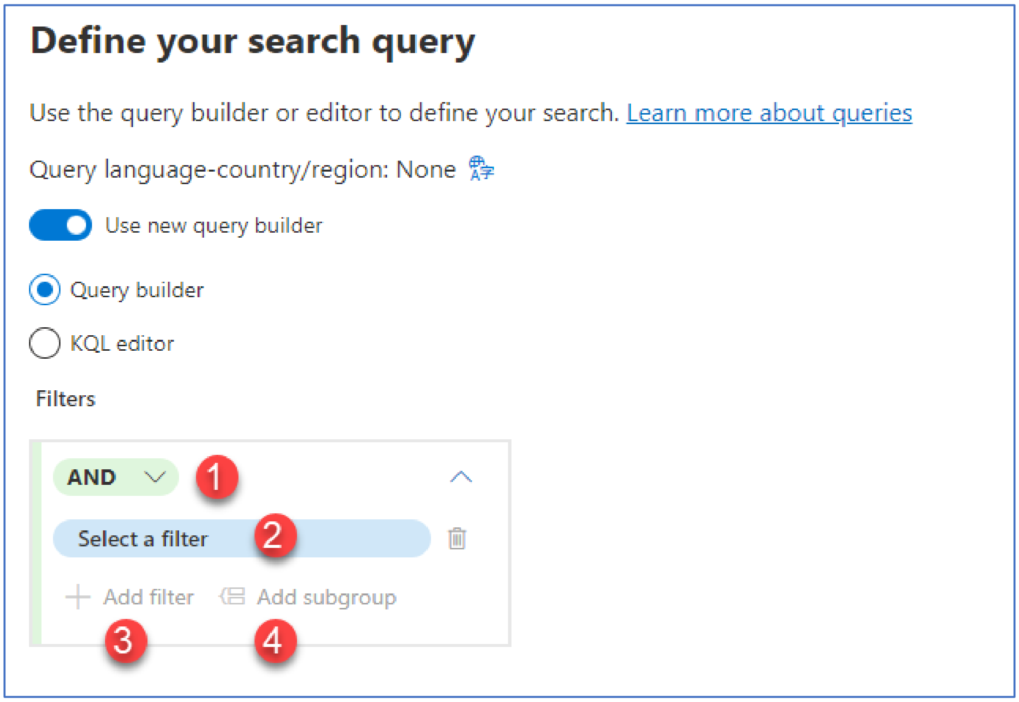


Figure 45 - New Collection Query Builder

The query builder, pictured in Figure 45, includes the following elements:

1. **AND/OR:** Conditional operators allow you to select the query condition that applies to specific filters and filter subgroups. The operators allow you to build subgroups connected to a primary filter.
2. **Select a filter:** Allows you to select properties to use as filters in the query. At this writing, this includes the following 21 properties:

Keywords	Participants	To
Date	Type *(Outlook Item Type)*	Author
Sender/Author	Received	Title
Size (in bytes)	Recipients	Created
Subject/Title	Sender	Last modified
Retention label	Sent	File type
Message kind	Subject	Sensitive Type

> ***Tip***
> *If you plan on using the Keywords filter in your search, choose it first. After any other filter is chosen, Keywords will no longer appear in the list of available filters. Unlike other filters, Keywords may be chosen just once.*

3. **Add filter:** Allows you to add multiple filters to your query after you've defined at least one query filter.

4. **Add subgroup:** After you've defined a filter, you can add a subgroup to refine the results returned by the filter. You can also add a subgroup to a subgroup for multi-layered query refinement.

5. **Select an operator:** As shown in, Figure 46, the operators compatible for the filter are available to select. The operators available depend on the filter type.

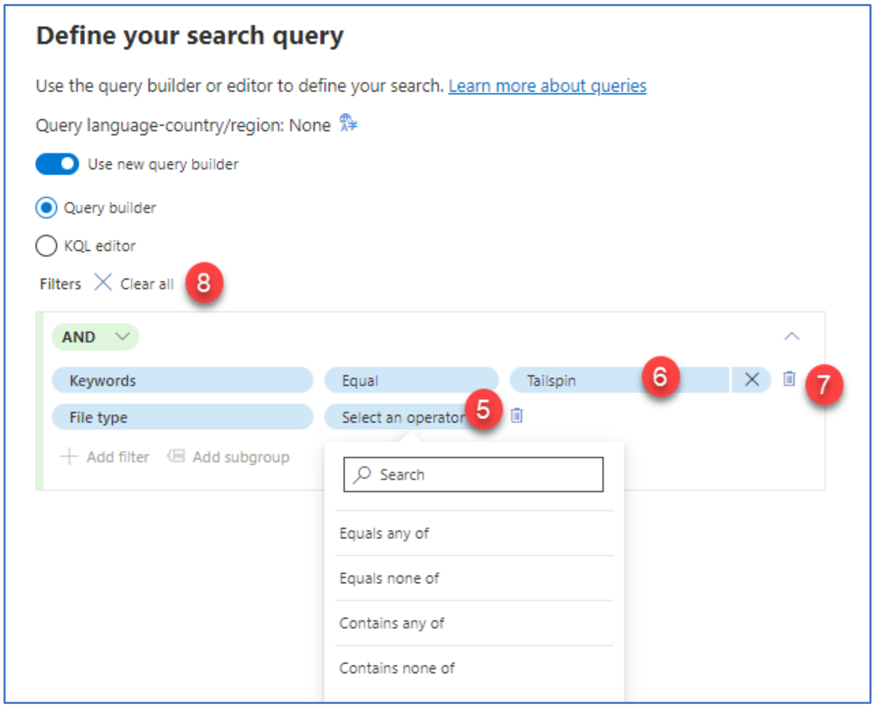


Figure 46- Select an Operator

6. **Value:** As shown in, Figure 46, depending on the selected filter, the values compatible for the filter are available. Additionally, some filters support multiple values and some filters support one specific value.

7. **Remove a filter condition:** As shown in, Figure 46, to remove an individual filter or subgroup, select the remove icon to the right of each filter line or subgroup.

8. **Clear all:** As shown in, Figure 46, to clear the entire query of all filters and subgroups, select Clear all.

Use the Condition Card Builder to build a Query

The Condition Card Builder can be used as shown below:

1. Select '**Condition card build**er.'

2. Type in the keywords that will narrow your search results to specific content as displayed in Figure 47 - Condition Card Builder.

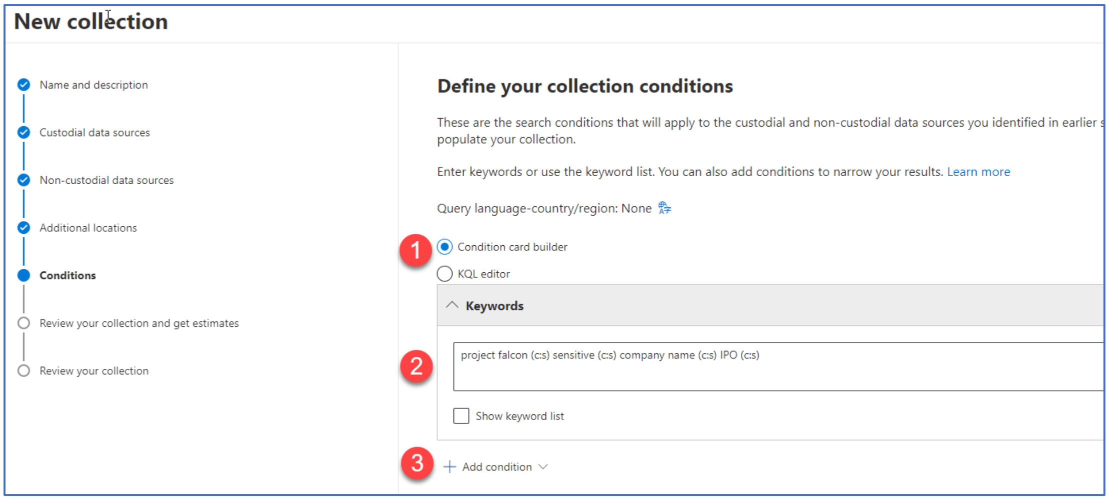


Figure 47 - Condition Card Builder

3. The third option is to select ‘Add condition’ to add additional conditions to further limit the search as shown in Figure 48 - Choose Conditions.

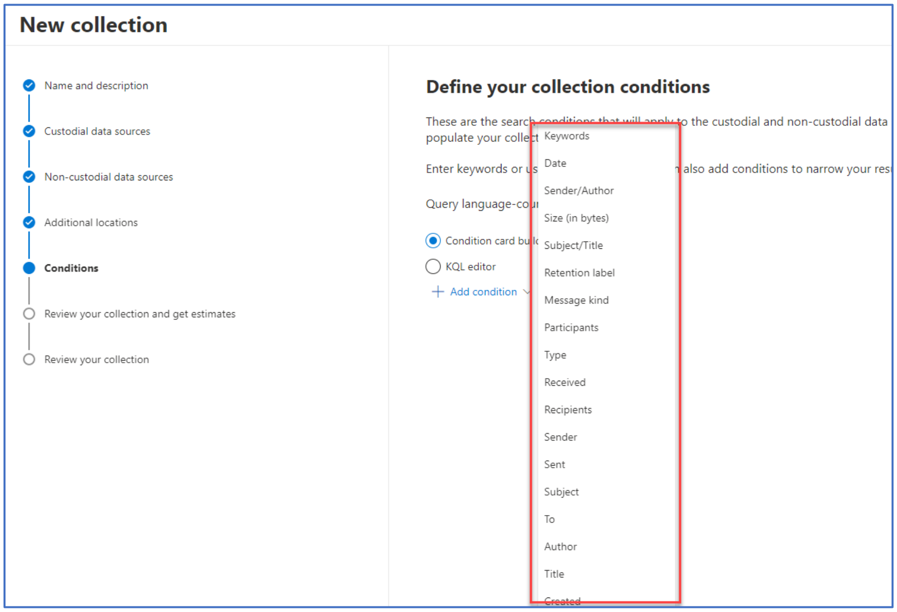


Figure 48 - Choose Conditions

As displayed in Figure 49 - Condition Card Example for all email messages between January 1, 2022 and December 12, 2022. is an example of using the ‘**Add condition**’ option to create a search for all email messages between January 1, 2022, and December 12, 2022.

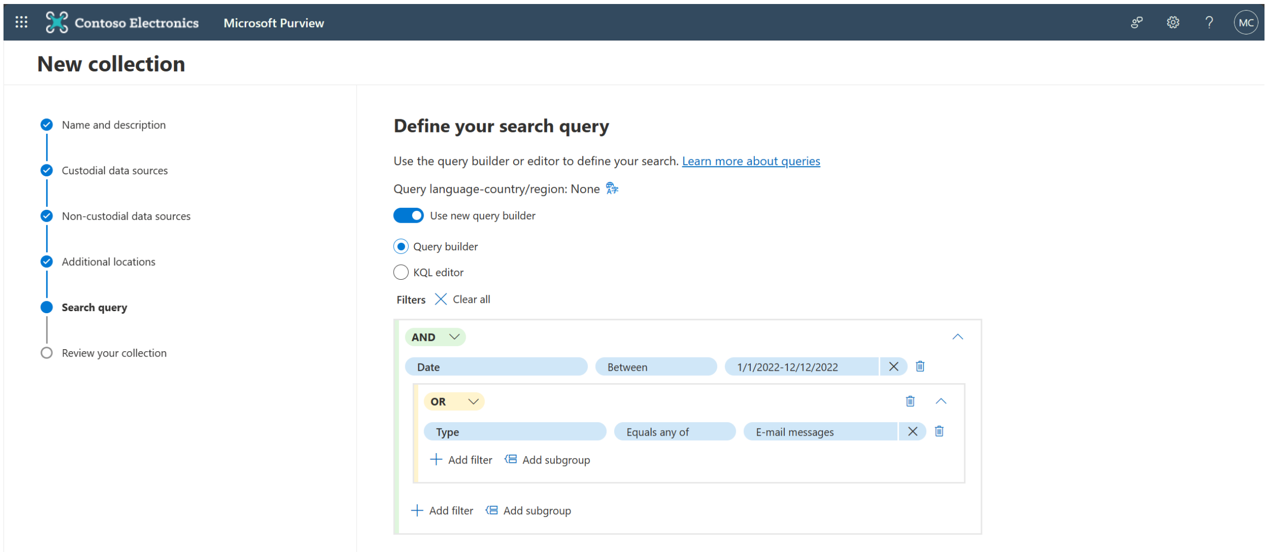


Figure 49 - Condition Card Example for all email messages between January 1, 2022 and December 12, 2022.

Use the KQL Editor to build a Query

The KQL editor is the second option in the condition wizard. This is the more advanced option where queries are inputted into the editor, as shown in Figure 50 - KQL Editor. Here queries can be written which are more granular and specific for the search.

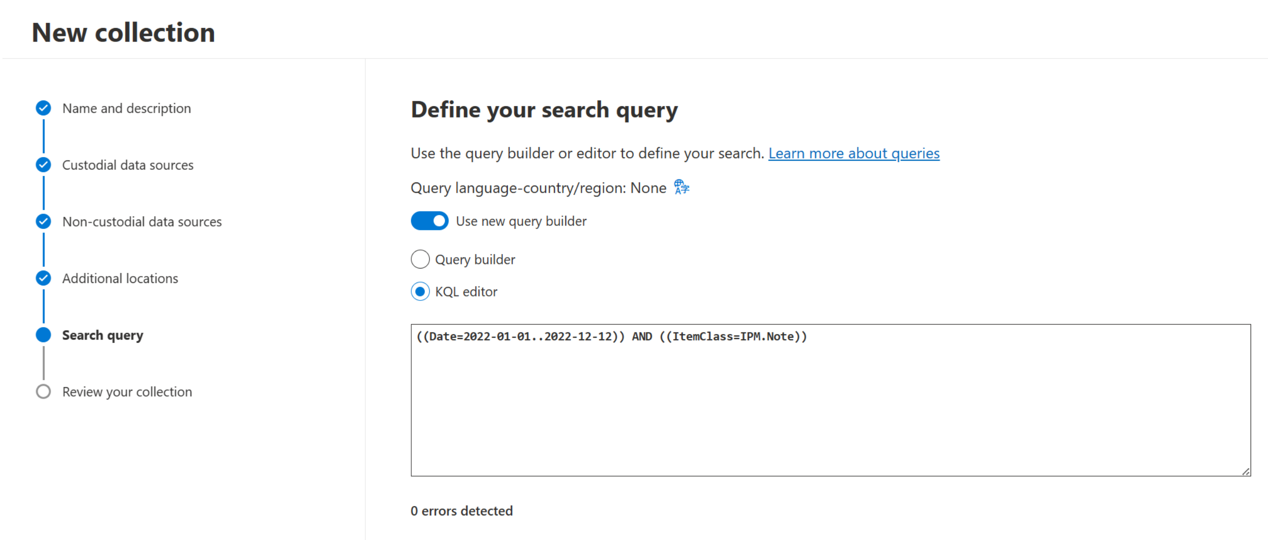


Figure 50 - KQL Editor

To create a KQL editor query the wizard will assist you by attempting to autocomplete the defined condition and suggesting which operators can be used to further enhance the query. As the below deomstrates in Figure 51 - KQL Auto Fill the date condition in the editor, the autocomplete box will suggest the operators which can be used with date such as (equals, not equal or contains).

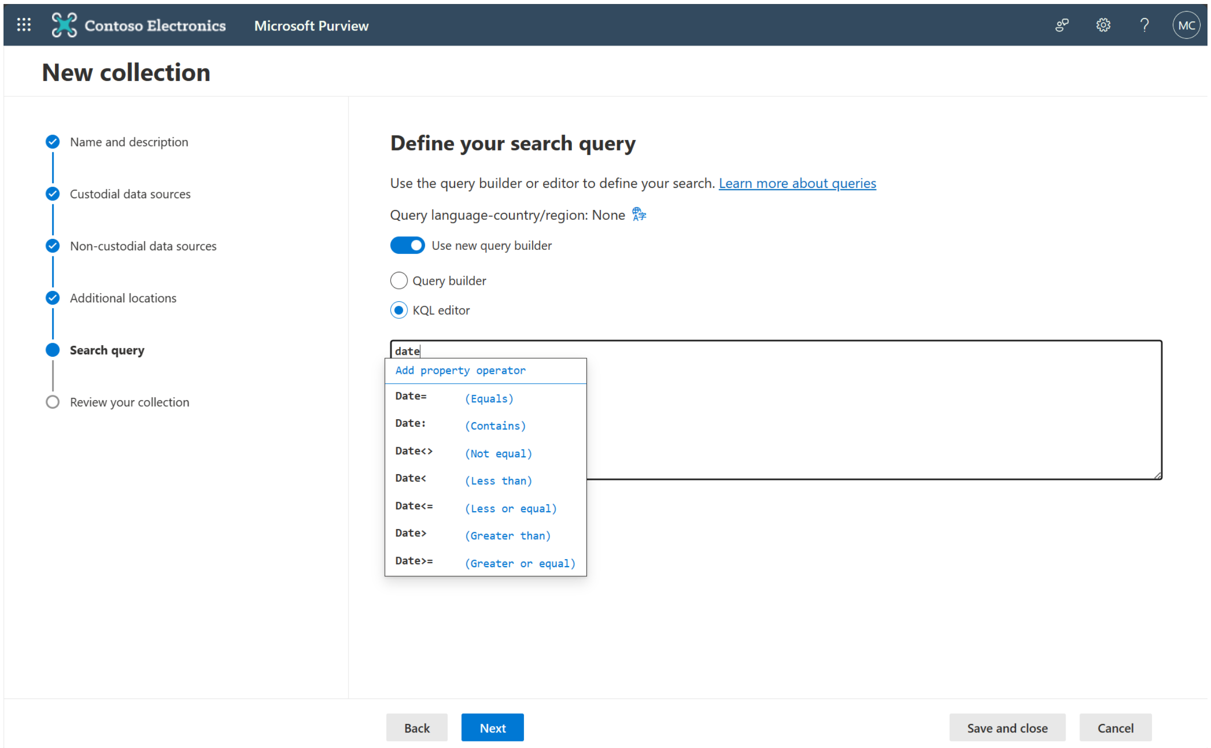


Figure 51 - KQL Auto Fill

Use KQL Editor to Build a Query

A complete KQL editor query is shown in the wizard which will search for all emails from January 1, 2022 to December 12, 2022, as displayed in Figure 52 - Example KQL Query

Example query: ***(date=2022-01-01..2022-12-08)(kind=email)***

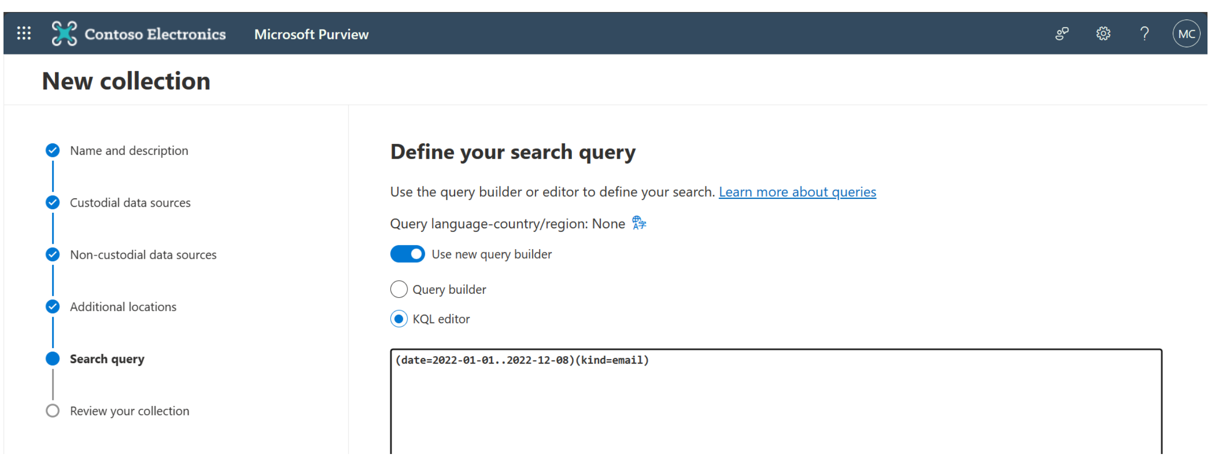


Figure 52 - Example KQL Query

Tip

We've found that customers that use the KQL editor keep "cheat sheets" of commonly used search queries in a OneNote notebook or text file. The eDiscovery teams use these as shared reference material.

[Use the KQL editor to build search queries | Microsoft Learn]

The end of the collection wizard is when custodians have been supplied and a search query completed as displayed in Figure 53 - Collection Review. Premium eDiscovery will now retrieve the data and provide an estimate of what will be collected.

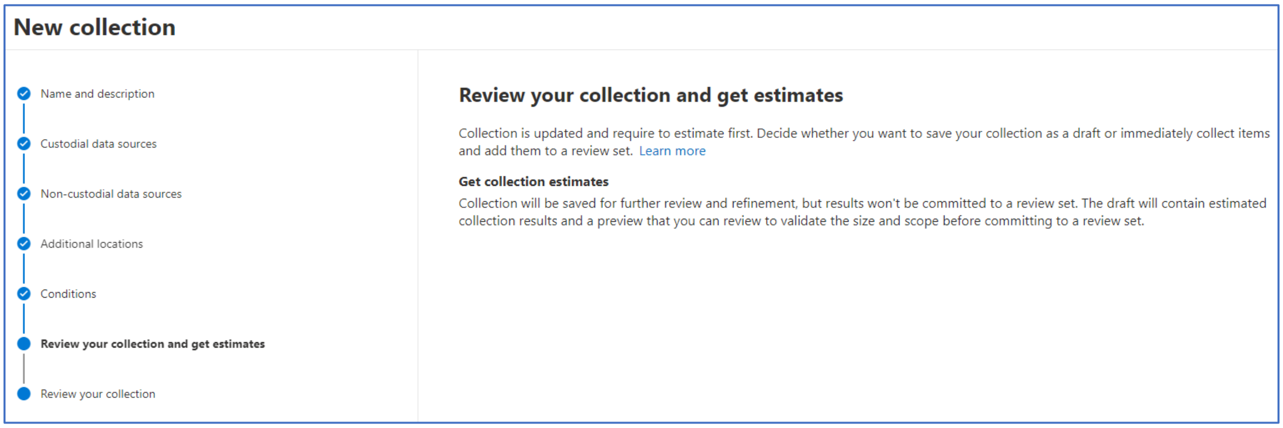


Figure 53 - Collection Review

At Ignite 2024, Microsoft announced the ability to **use Natural Language to generate search queries**. Read more in the Blog: https://aka.ms/eDiscoveryblog/Ignite23

Review Collection Progress and Estimates

To view the progress of the the collected data it is possible to access the newly created Collection which now appears in the '**Collections**' blade as demonstrated in Figure 54 - Collection Status. From this view it can be seen that an estimation is currently in progress.

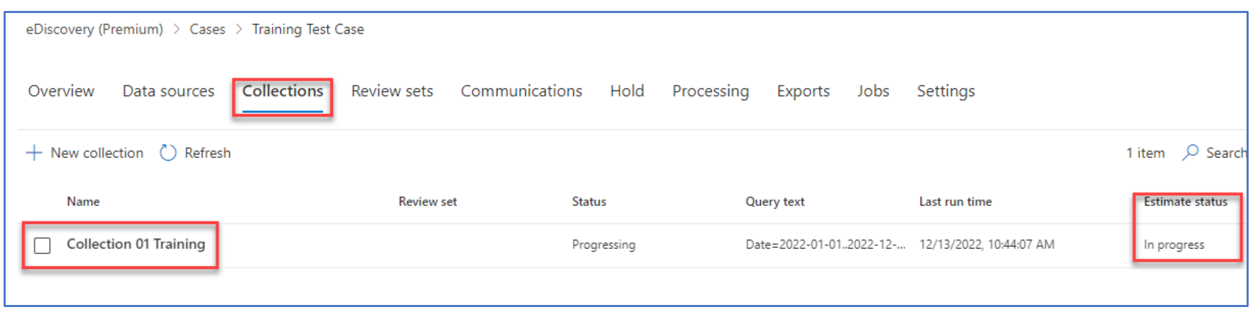


Figure 54 - Collection Status

Opening the collection wizard will default to the '**Summary**' tab which will show the query progress while search is running, as shown in Figure 55. When the search completes, pre-collections estimates will be displayes as shoiwn in Figure 56.

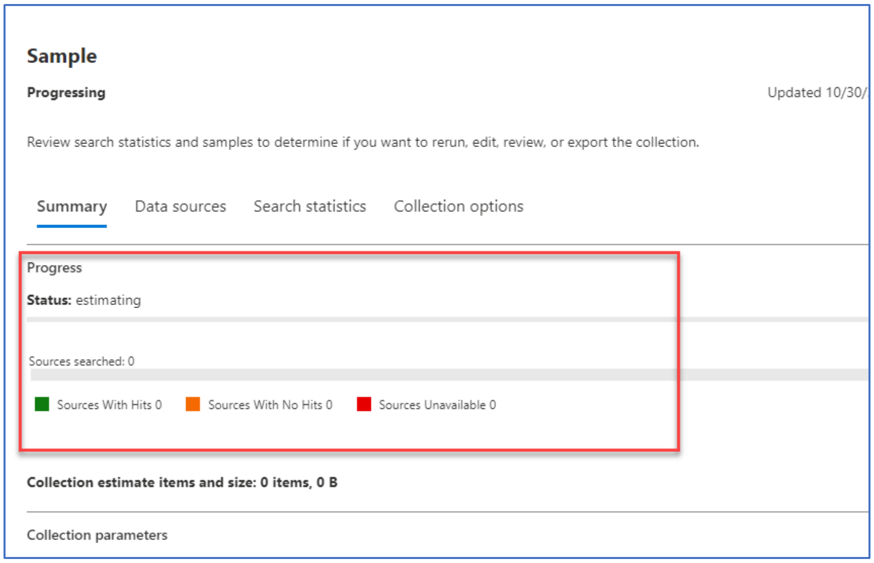


Figure 55- Collection Summary - Progress

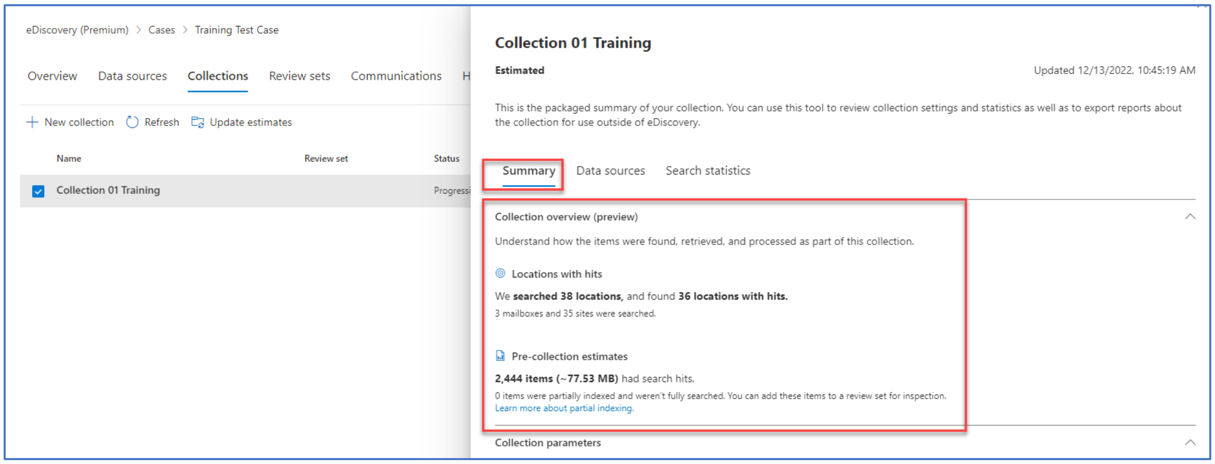


Figure 56 - Collection Summary - Estimate

Important Note

Until the collection query results are processed into a review set, the Premium eDiscovery can only provide an estimate of how many items will be collected. When items are collected into a review set, Microsoft performs eDiscovery processing on the data. This breaks each collected item down into its individual components. For example, an email message with five attachments will be counted as one item in the estimates but six items in the review set.

See Collection statistics and reports | Microsoft Learn for more information.

Review Collection Search Statistics

The ‘**Search statistics**’ tab will also present further estimation information such as which locations consumed the most data storage for the collection. Information on which locations contained the most items found during the search is also provided, as shown in Figure 57 - Collection Statistics.

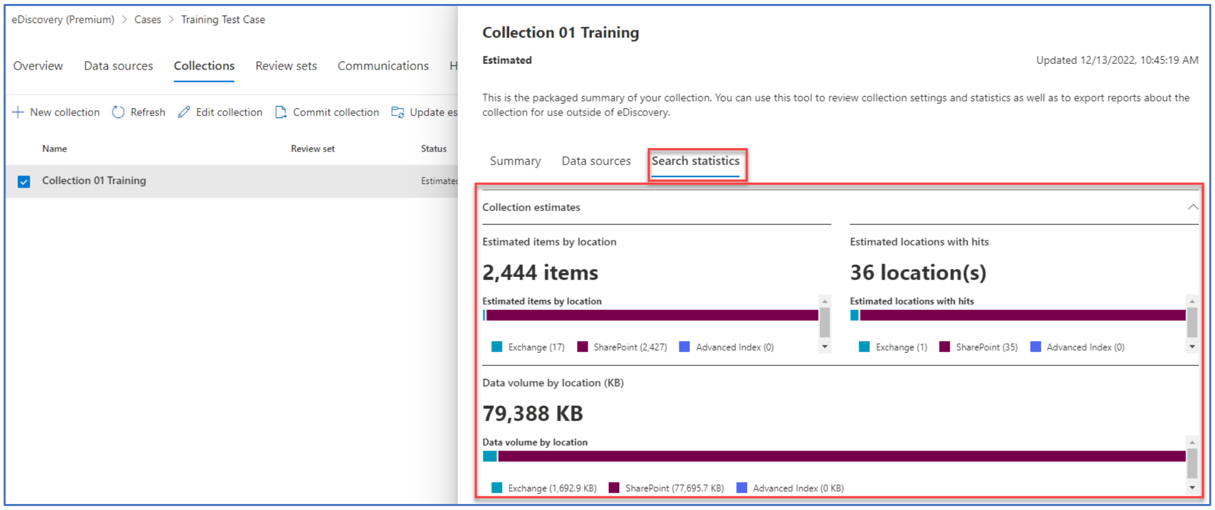


Figure 57 - Collection Statistics

[Collection statistics and reports | Microsoft Learn]

Review a Sample of Collection Results

Once the estimation has been completed it is highly recommended to review a sample of the content for accuracy.

The ‘View Sample’ option will take you to a new window as displayed in Figure 58 - View Collection Sample

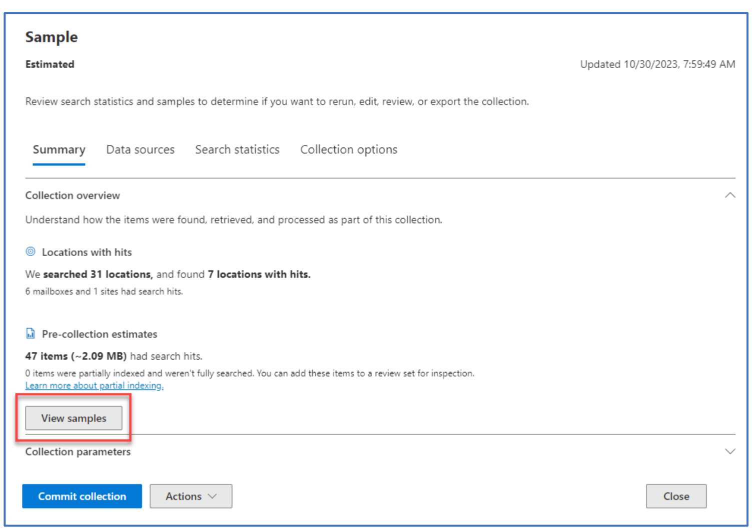


Figure 58 - View Collection Sample

The collection sample area will show documents found during the collection phase. Selecting one of the sample documents will show a preview of the document in the right hand window, as demonstrated in Figure 59 - Collection Sample. This allows for verification that the content is accurate and ready to be commited to a review set.

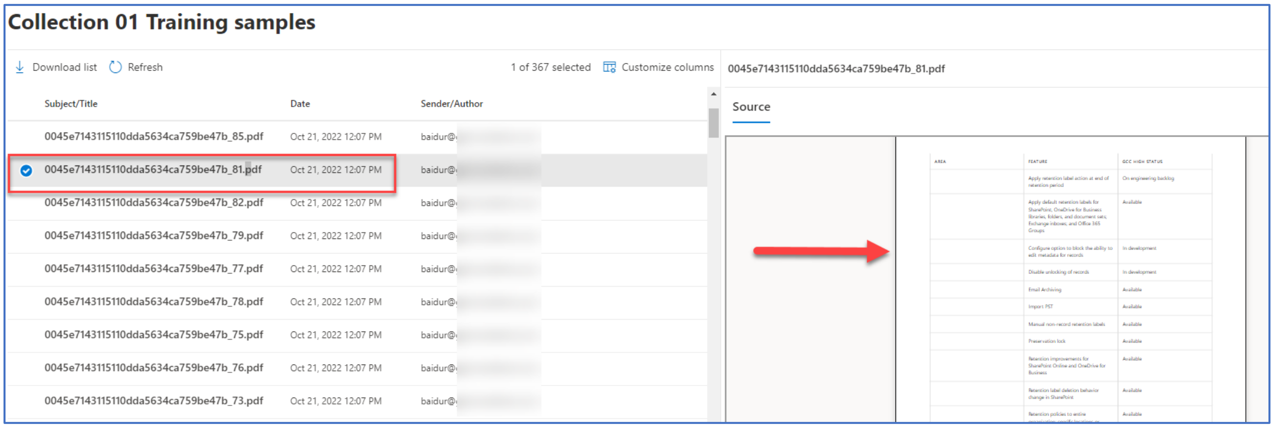


Figure 59 - Collection Sample

Committing a Collection to Review Set

Once sample documents have been verified for their accuracy, typically . the next step is committing a collection to a review set by clicking the Commit collection as shown in Figure 60. Follow the steps in Committing to a review set options: to complete the process of committing the collection.

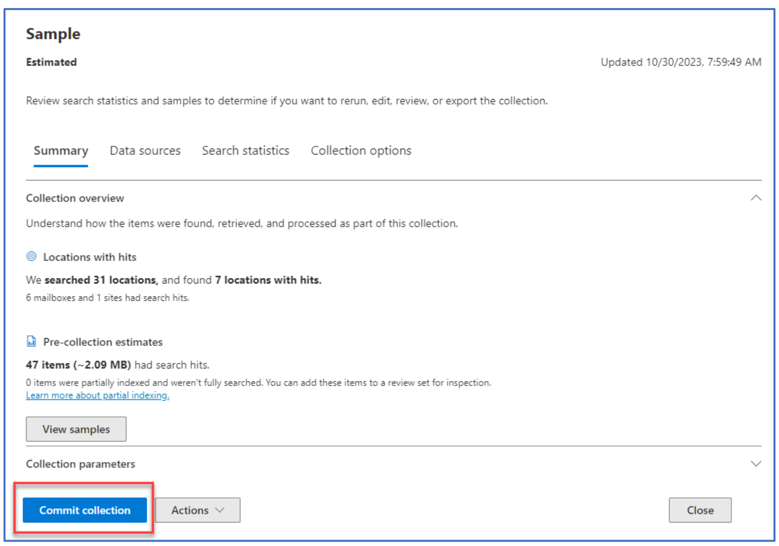


Figure 60- Commit Collection

Other Review Set Actions

To the right of the Commit collection button (see Figure 60,) is the action button. Clicking the actions button yields the pop-up action menu. The options on the action's menu depend on whether the collection has been committed. As shown in Figure 61, the options on the actions button shrink after a collection is committed. After a collection is committed, it becomes read-only to memorialize what locations were searches, the search terms and number of pre-collection results.

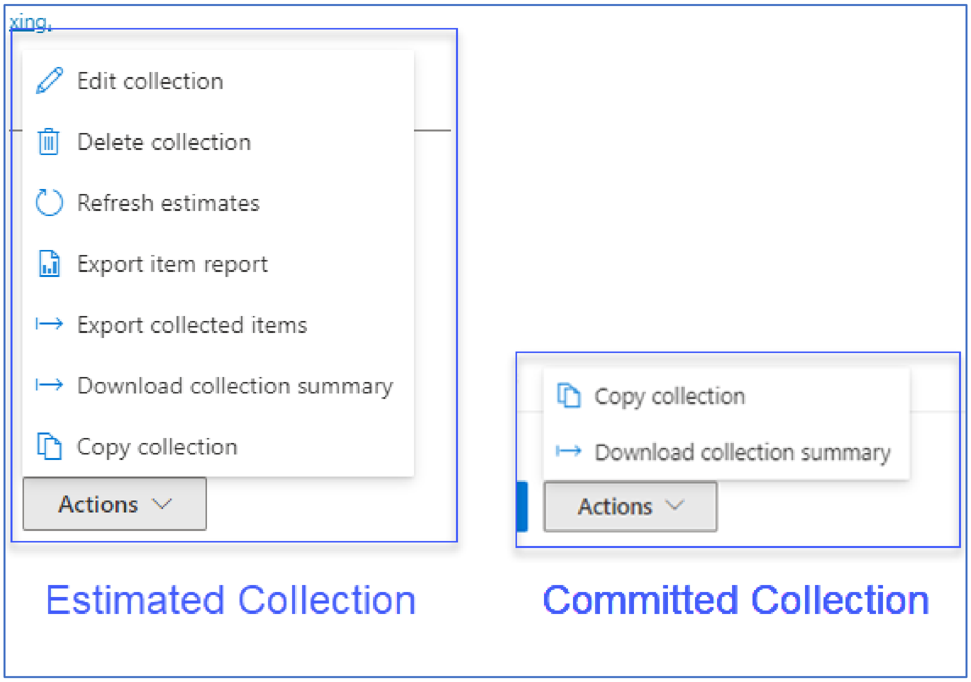


Figure 61- Collection Actions Button

Items on the Collection Actions Button (Figure 61)

1. **Edit Collection:** Choose this option to edit any of the settings in the collection, including the query and search locations.
2. **Delete Collection:** Deletes the collection estimate.
3. **Refresh Estimates**: Rerun the query (against the data sources) specified in the collection estimate to update the search estimates and statistics.

> ***Tip***
> *If some time has passed since estimates have been run for the collection, the estimates may have changed. For example, when searching across locations without holds places, items response to the collection may have been deleted. Consider refreshing the estimate to get updated search statistics before committing. You may also consider copying the collection and rerunning the search in the new collection. You may then compare search statics between the two estimates to determine if estimates have changed.*

4. **Export Item Report**: Added in June of 2023, this report is an item level CSV file on included pre-processed metadata on all items found in collection. Since the report is on pre-processed data, information on parent child relationships, will not be included. For example, if a ZIP file is collected, the report will not list all files contained in the Zip file in the report.

> ***Important Note***
> *The item report is not a single report. Instead, it is a collection of CSV files. Each location with responsive items will be generated.*

> ***Note***
> *Although .the report will not detail traditional email attachments in the report, you may to include information on attachments in the report.*

See Export Items Report | Microsoft Lear for more information.

5. **Export Collected Items:** Premium eDiscovery's traditional workflow has been collecting items to a review set and then exporting the processed from the review set. Export collected items allows you to skip processing into the review set and export in native format. This may be useful when the plan is to process the data in another eDiscovery platform. While you do lose the benefit of Premium eDiscovery review sets when using collect to export, you are still able to leverage the power of advanced indexing in collections.

> **!**
> ***Important Note***
> *At this writing, the Export to Collected items export does not include any sort of chain of custody or verification report. For example, a report indicating how many items were included from each location. When using the Export Collected items report, we suggest you download both the Export Items report and the collection search statistics report an use these to validate export reports.*

See Export Collected Items | Microsoft Learn for more information

6. **Download Collection Summary**: This report provides a high-level summary of the items count, size and source for each location being committed.
7. **Copy Collection**: Select this option provides the ability to create a copy of the collection settings and search logic.

Review Sets

When a collection has been verified for accuracy and commited the next stage is to create a review set for this content.

When a collection is commited you will be presented with the screen shot below.

Committing to a review set options:

Commit to a new or existing review set.

1. ***Add to new Review Set*** – The collected data will be moved into a newly created review set with the name specified in the name box.
2. ***Add to existing Review Set –*** The collected data can be merged and added to an existing review set to support an ongoing review.

> ***Tip***
> *When adding to an existing review set, the system will not create duplicate entries of the exact same item from the same location. For example, if you load a collection search of energy terms to a review set and then search the term "solar", only net new*

	items with solar will be added, anything that contained solar + one of the previous terms would not be added.

Retrieval Options:

Retrieval options allow you to specify additional connected items to be added to the collection results.

1. ***Teams and Yammer Conversations -*** Collect up to 12 hours of related conversations when a message matches a search.

2. ***Cloud Attachments -*** Collect items from links to SharePoint or OneDrive.

3. ***All Document Versions -*** Collect all versions of SharePoint documents. If not selected, only current versions are collected.

4. ***Partially Indexed Items -*** Collect unsearchable items that might be relevant.

Collection ingestion scale:

Select if the entire collection search results should be committed or if a sampling of the results would be necessary for further validation. Sampling can be set as either a confidence level or a percent to be reviewed.

The '**Commit**' button will then apply the collected data to a review set based on the selection above and as displayed below in Figure 62 - Create a Review Set.

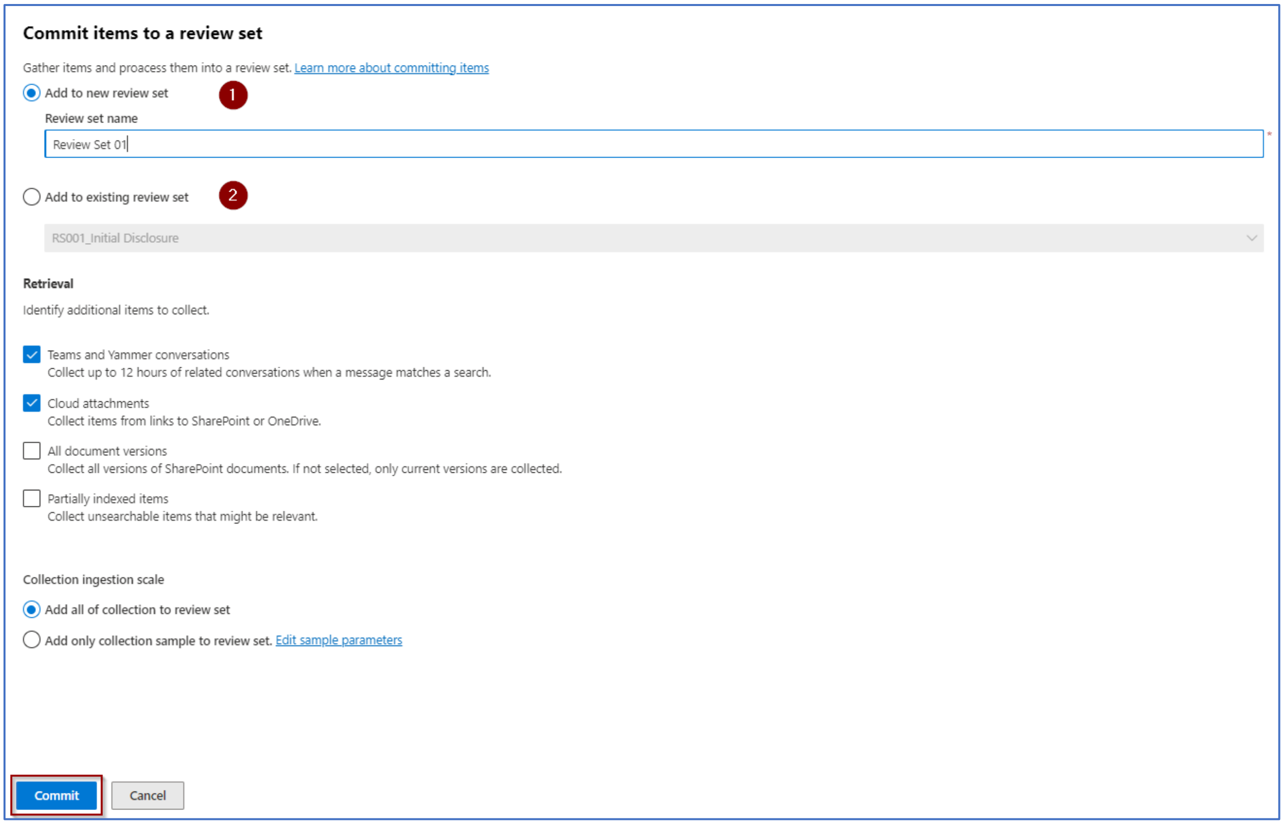


Figure 62 - Create a Review Set

A committed Review set will then appear under the ‘Review sets’ tab as demonstrated in *Figure 63 - Current Review Set*. A job will run in the background to add the items to the review set which may take some time depending on the size of the content. Initially, the ‘Size’ column will show as not available until the items are added.

During the commit stage, the data is being processed. This includes the following:

- Extracting attachments and embedded objects which will be captured as a family relationship within the review set.
- Extraction of compressed (e.g. ZIP) files as individual items.
- Extraction of fielded metadata which will be filterable and quarriable within the review set.
- Extraction of document text.
- Logging of processing errors with remediation steps within the review set.

If review set functionality is not necessary for a collection, the Export Collected Items option will allow a direct to export function which bypasses processing and building a review set. However, the enhanced features of the review set with filters, queries, culling, tagging, native redactions, selective exports, condensed (load ready) exports, and all the analytic features: exact deduplication, near-deduplication, email threading, and themes, will not be available.

Figure 63 - Current Review Set

When the review set is ready the ‘Size’ column will show a calculation of the items stored in the review set. The review set can now be selected, and its items can be reviewed in a new window as displayed in Figure 64 - Review Set ready for review.

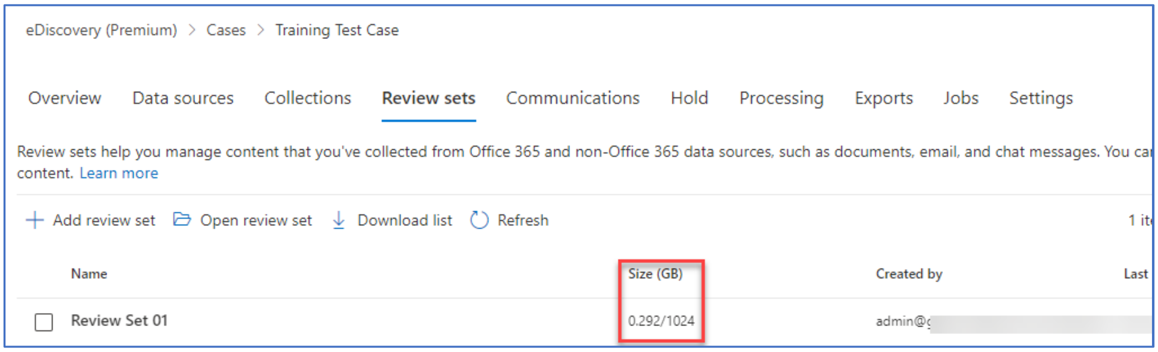


Figure 64 - Review Set ready for review

The Review set area will show documents that have been added to this Review set. Selecting a document will show a preview of the document in the right-hand window as demonstrated in *Figure 65 - Open Review Set*.

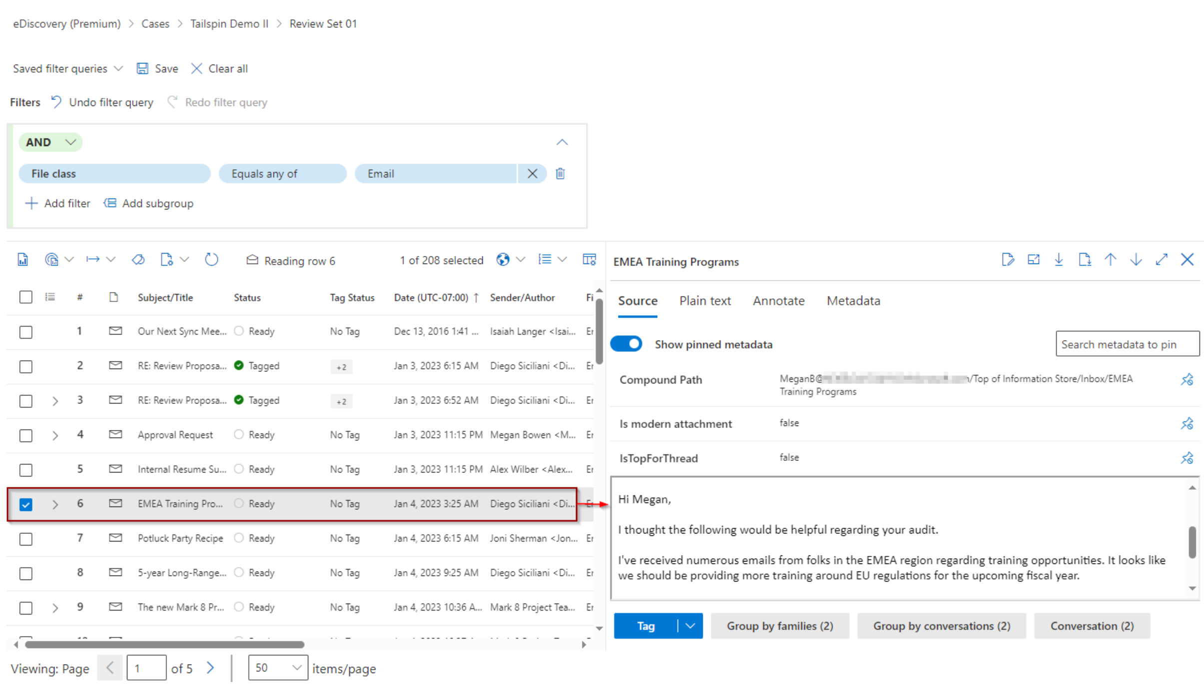


Figure 65 - Open Review Set

When many items are held in the Review set it makes reviewing the data tougher. Because of this, Microsoft offers Analytics, allowing items to be analyzed, queried, viewed, tagged, and exported.

Tip
Review sets are where advanced features are made available to provide enhanced review efficiencies through the analytics process.

Run Analytics in a Review Set

To Analyze data in a review set, select the **Analytics** icon highlighted in Figure 66 – Run Document & email Analytics and the '**Run Document & email analytics**'. This will create an analysis job where the data will be parsed into an Analytic Graph for simplicity of identifying what data has been returned and the count of each data set.

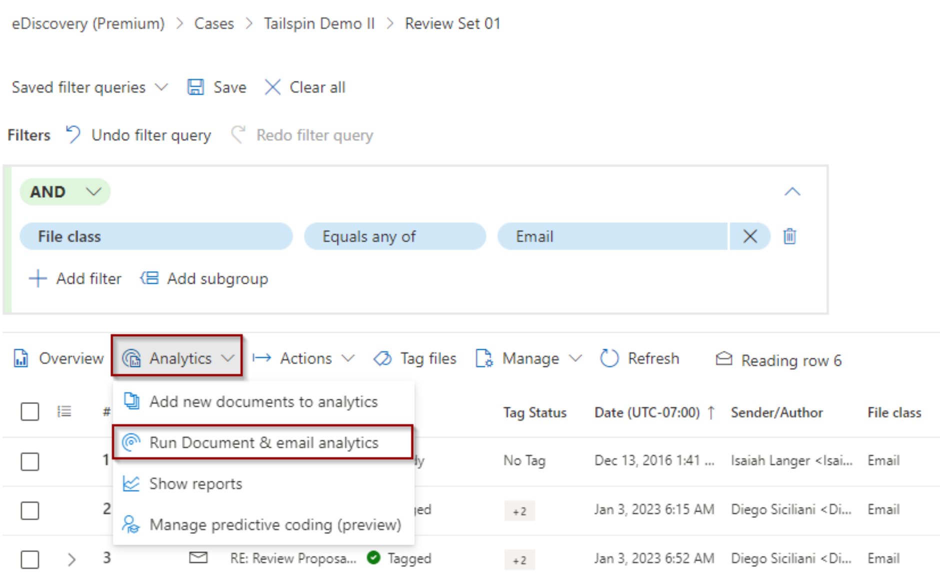


Figure 66 – Run Document & email Analytics

[Analyze data in a review set in eDiscovery (Premium) | Microsoft Learn]()

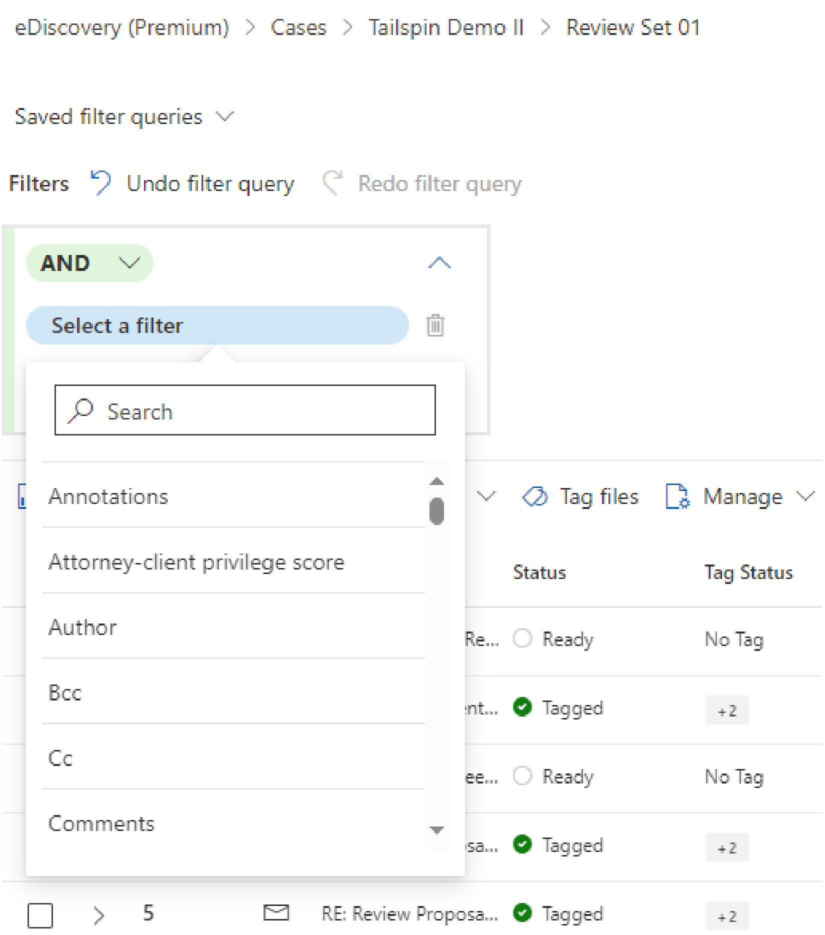
Filter a Review Set

As displayed below in Figure 67 - Query Review Set to Query data in a review set you can do the following:

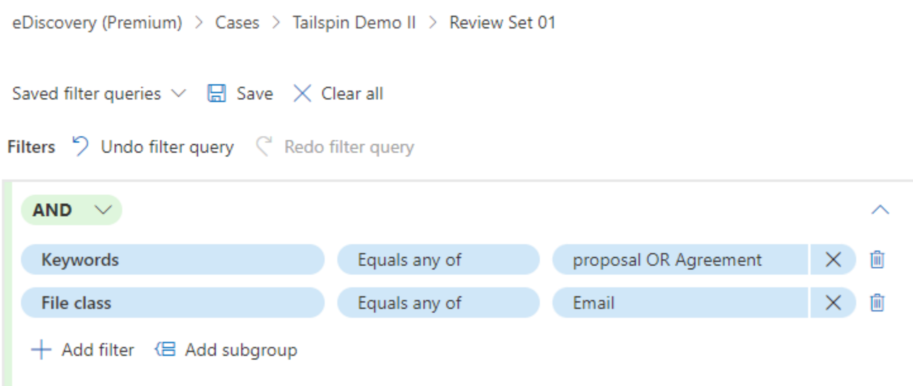
1. Select a field to filter by clicking on Select a Filter.

2. Add additional filters utilizing AND or OR logic.
3. Apply subgroups to further build distinct logic to be processed together

Select a Filter



Add multiple fields to a filter



Create a filter subgroup

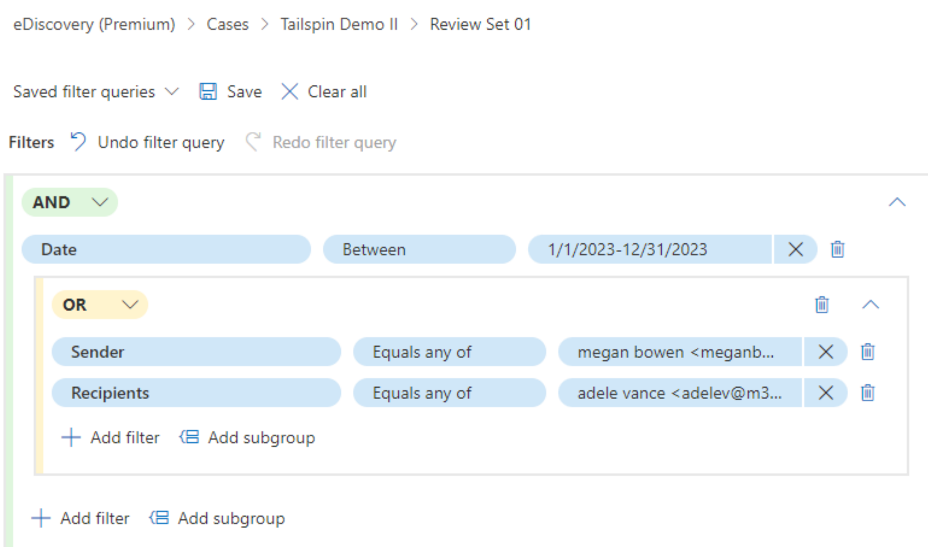


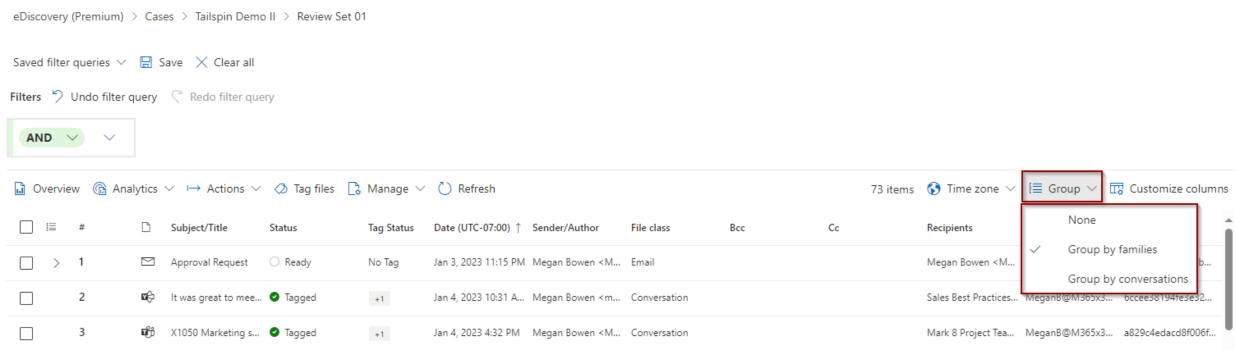
Figure 67 - Query Review Set

Grouping

Three options for grouping are provided on the review set menu. Groupings can be set to none, group by families, and group by conversations. If the Review Sets Grouping tile under settings has been enabled, the following grouping options are the default view.

- **Group by families**: All items related to a specific file are grouped together using the same Group ID. For example, if you have a PowerPoint file in the review set that includes imbedded images or .zip files, these images and files are grouped with the PowerPoint file and shown as nested items with the file in the item list view.
- **Group by conversations**: All email messages, Teams conversations, and Viva Engage conversations are grouped using the same Thread ID and appear as nested items. Additionally,

all associated content for these messages and conversations is also grouped together. For example, if you have an email conversation that includes several email messages, some of which include attachments and some that include embedded images, all of the email messages, attachments, and images are grouped together in the review set list view under an applicable item.



Tags

Tagging data in a review set is useful when there is a need to differentiate specific data. For example, to create tags to define what content is considered sensitive or not sensitive. When an item is tagged as such it can then be filtered to be included or excluded from a view.

Tags can be located by selecting the below **Manage** icon inside a review set and selecting '**Tags**' as displayed in Figure 68 - Select Tags

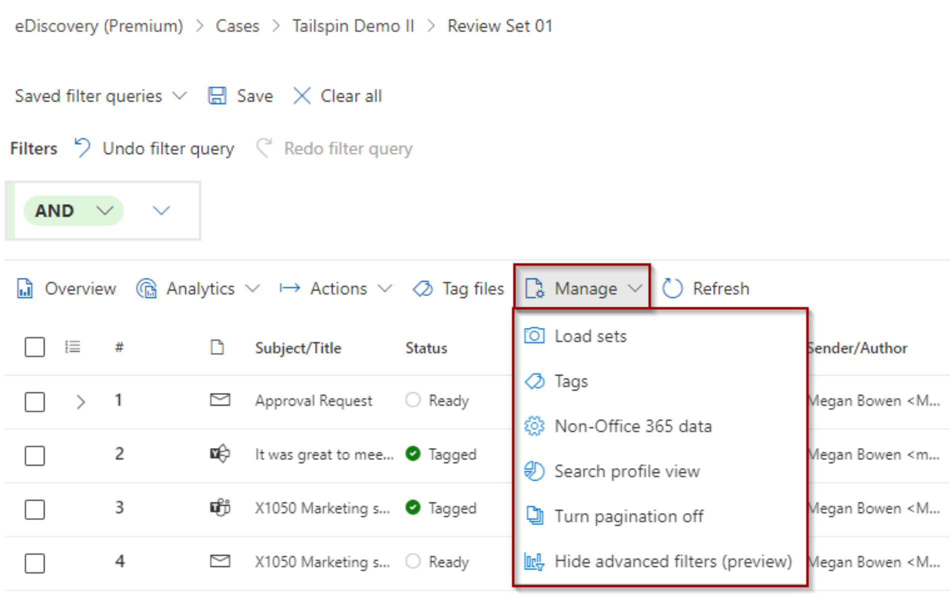


Figure 68 - Select Tags

New tags will need to be created before they are visible in a review set. Note, Tags can be created directly inside a Case Review Set, or a tag template can be created which can be made available to all cases.   Tags created in a review set will apply to all review sets within that case. When a template is used, the tags can be adjusted per case to meet specific needs. To create a tag, it is necessary to add both a Tag Group and a Tag Name.

When the tagging panel opens, create the tags by adding a tag group, and then adding a tag.

When adding tags, the following tag type options are available.

- Option (Radio Button) = can only have one selection from that tag group.
- Check Box = can have multiple selected tags from the same tag grouping.

Nested or sub-tags can be added to any tag selections for further definition within a tagging group.

Details for Tag Templates can be found at the following link: [Tag Templates (preview)]

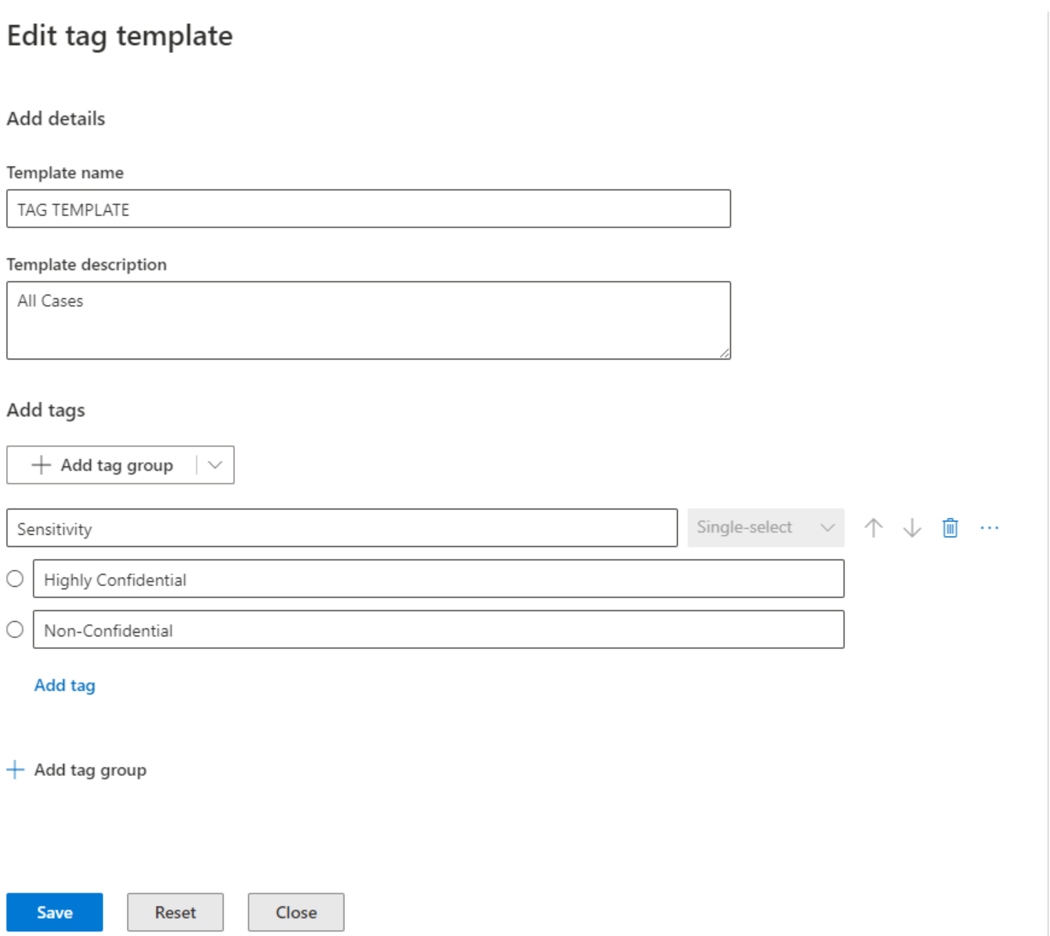


Figure 69 - Create New Tags

As demonstrated below in Figure 70 - Tag an Item to tag an item in a review set do the following:

1. Select an item from the review set.
2. In the item preview, select the ‘**Tag**’ Button.
3. In the ‘**Tag files**’ window locate ‘**Assign Tags**’ and apply the relevant tag.
4. Select ‘**Apply Tags**’ to save the change and commit the tag to the item.

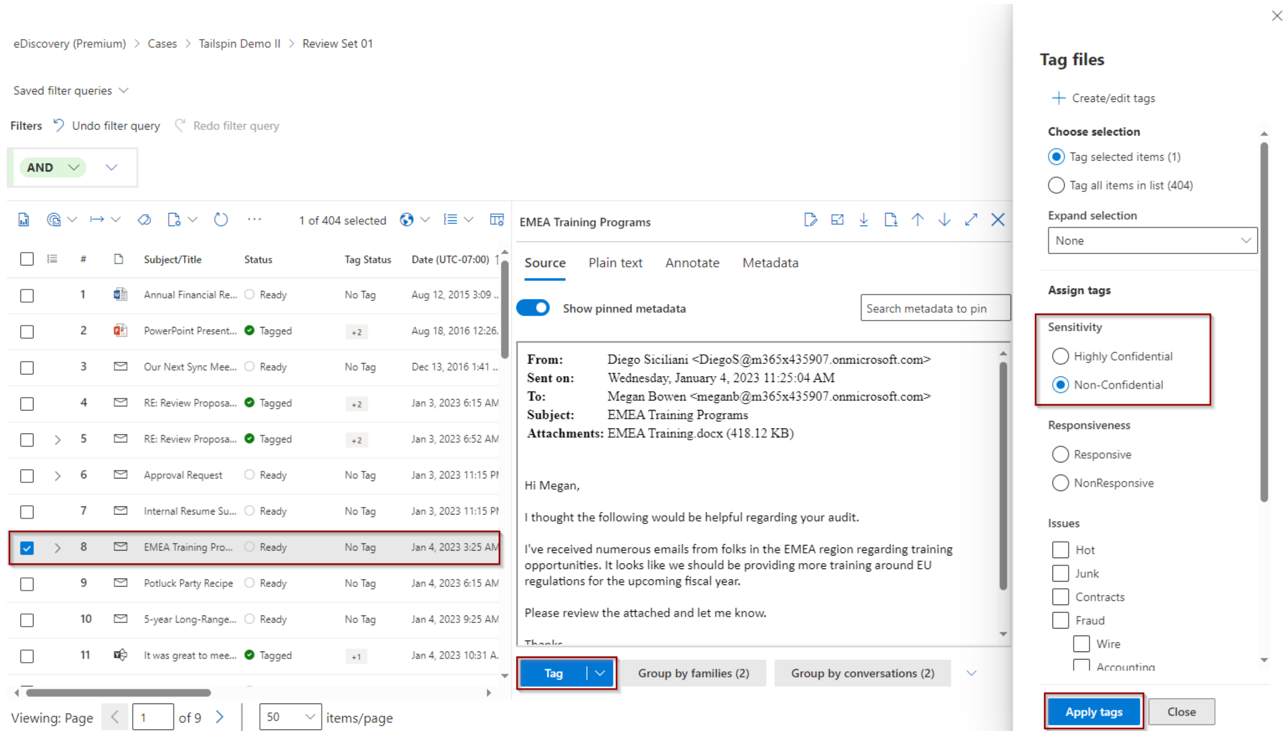


Figure 70 - Tag an Item

Further tagging details can be found at the following link: [Tag documents in a review set | Microsoft Learn]

Once items are tagged, they can be filtered based on the tag assigned. As demonstrated below Figure 71 - Tag Filter shows a filtered view displaying emails tagged with the non-confidential tag.

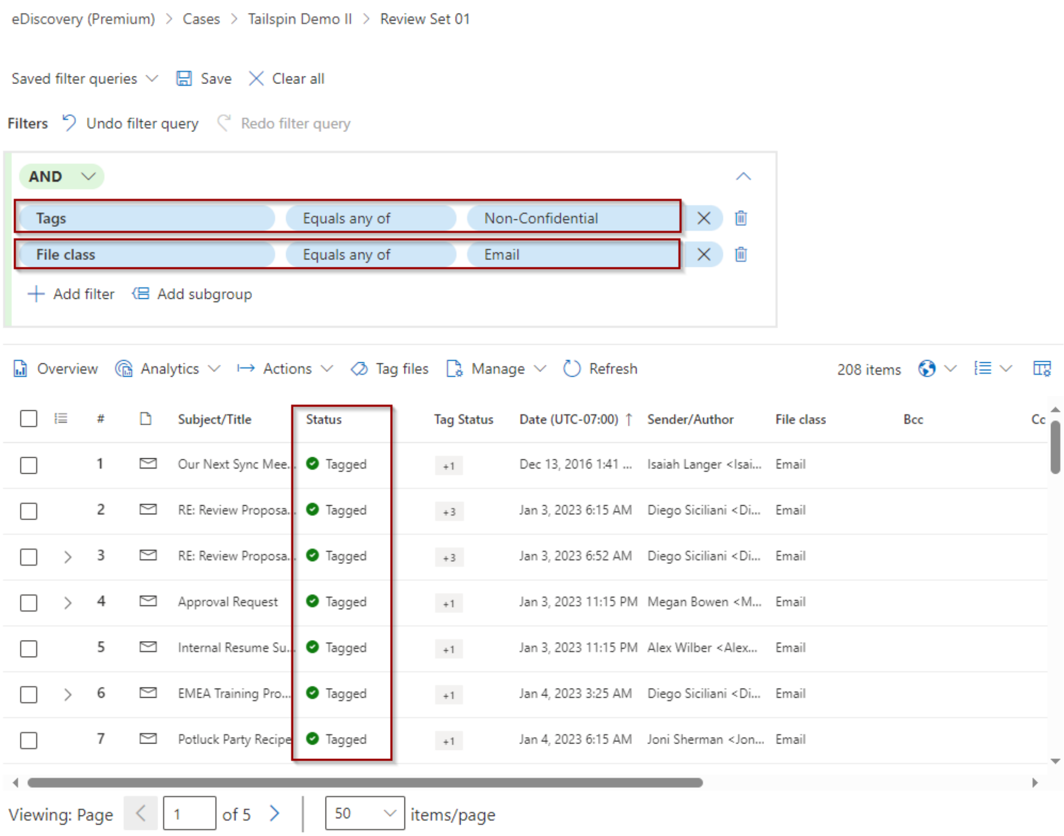


Figure 71 - Tag Filter

Processing

Processing provides visibility into Advanced Custodian Indexing and is where it is possible to address processing errors with file identification, expansion of embedded documents and attachments, and text extraction.

When adding custodians and non-custodian data sources to a case on the '**Sources tab**', all partially indexed items from M365 are processed to make them fully searchable. Likewise, when content is added to a review set from both M365 and non-M365 data sources, this content is also processed.

Exports & Downloads

Premium eDiscovery includes three options for getting data out of a case, 1) The collect to Export option detailed in the collections section of this document, 2) downloads for exporting single items or small collections, and 3) Exports for the bulk port of data for import into other systems.

Downloads

There may be scenarios where you need to quickly extract small amounts of data from a Premium eDiscovery review set. For example, your reviewers find an email thread stating primary facts of the case that outside counsel should review while developing case strategy.

To download items from the review set, first select the items to download in the review set and then choose **Download** from the actions menu as shown in Figure 72**.** The results will download in a zip file as shown in Figure 73.

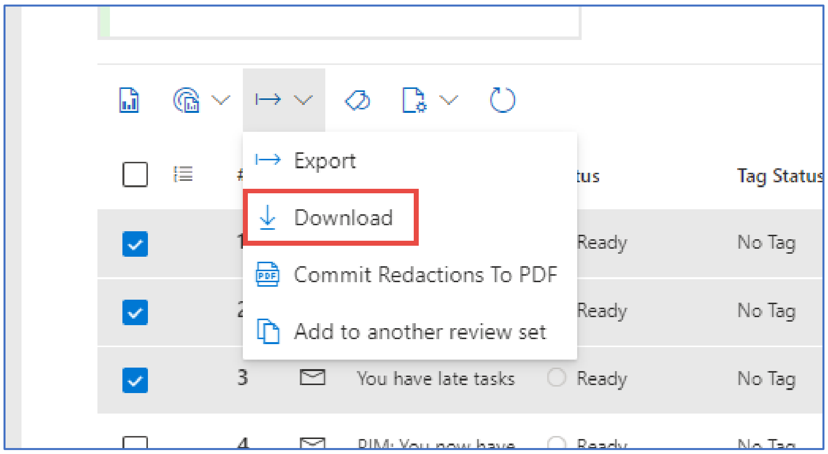


Figure 72 - Download Files Option

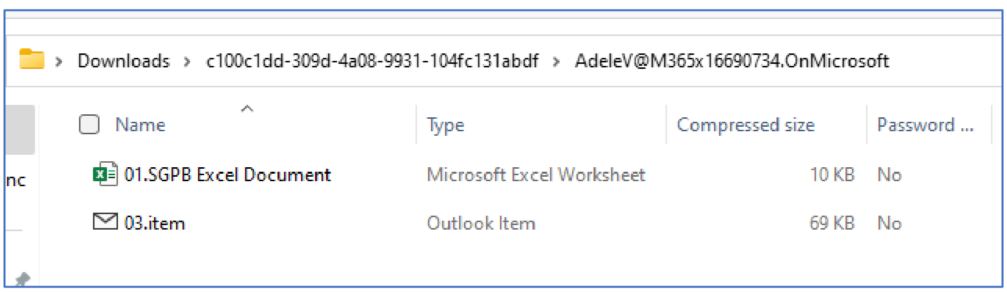


Figure 73 - Downloaded Files

You may also download items individually through the document viewer. As shown in Figure 74, click the arrow icon to download the file in its native format. Choose the page icon to download the item as a PDF.

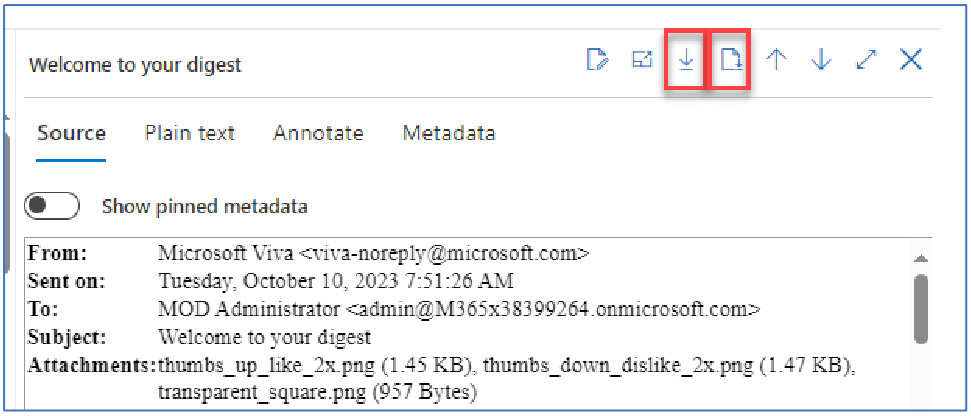


Figure 74- Download Individual Item

Exports

	Tip *Microsoft's documentation on exports can be found here: [Export documents from a review set in eDiscovery (Premium) | Microsoft Learn] if you are new to exports or infrequently use the features, we recommend you review the documentation along with our guidance below.*

Like downloads, the exports option is found on the Actions tab of the review set menu. The Exports feature is used to gather up to 5 million items or a total 500GB files. Premium eDiscovery includes four export formats as shown in Figure 75:

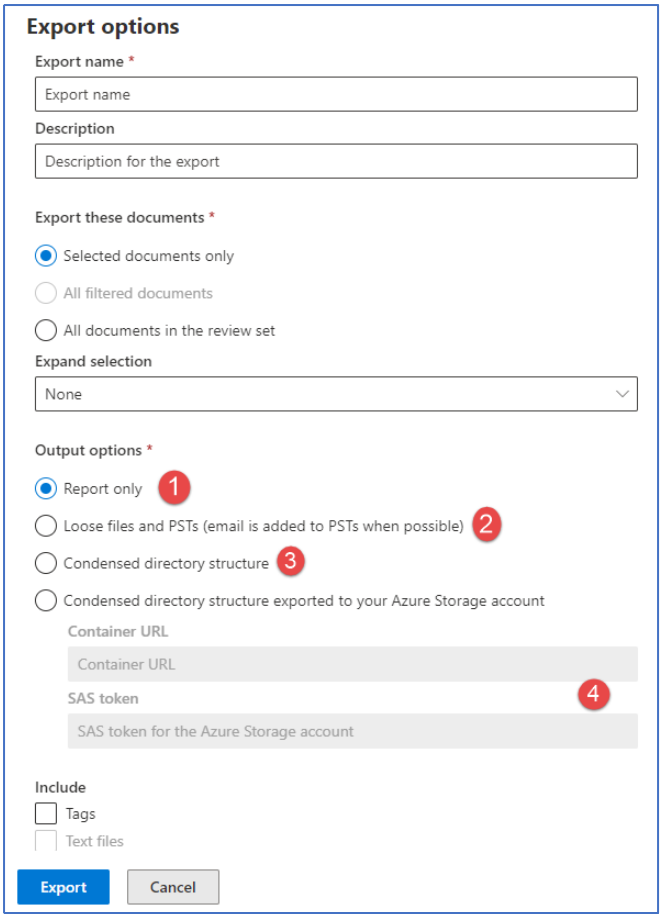
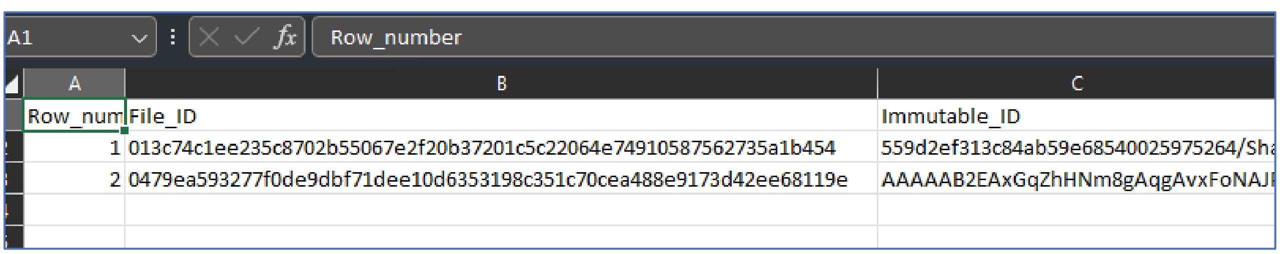


Figure 75 - Export Options

1. **Report Only:** With this option, a summary of the selected data is downloaded as a CSV file as demonstrated in Figure 76. The CSV includes the metadata for each item as detailed in the exported field name column in [Document metadata fields in eDiscovery (Premium) | Microsoft Learn](#)



A1 | Row_number

A	B	C
Row_num	File_ID	Immutable_ID
1	013c74c1ee235c8702b55067e2f20b37201c5c22064e74910587562735a1b454	559d2ef313c84ab59e68540025975264/Sha
2	0479ea593277f0de9dbf71dee10d6353198c351c70cea488e9173d42ee68119e	AAAAAB2EAxGqZhHNm8gAqgAvxFoNAJ

Figure 76 - Report Only File

2. **Loose files and PSTs:** You may find that this is the most frequently requested option when exporting for hand off to an eDiscovery vendor or outside counsel. The party receiving the files will typically reprocess the files using another eDiscovery platform other than Premium eDiscovery. The export includes the same report file included in the “report only: export and three folders:

- **Exchange:** Any emails included in the export will be included in PST files in this folder. A PST file, named for the primary email address for the mailbox, will be created for each mailbox.

- **SharePoint:** Files exported from SharePoint sites and OneDrive will be included in this folder.
- **Conversations:** Transcripts of Teams and Yammer (Viva engage) will be found here as html files.

! ***Important Note***

As mentioned above, the Loose files and PST export is the most frequently request format. In traditional eDiscovery workflows, that typically focused just on email, this format made sense. As the types of data included in M365 has grown, relying on just the Loose files and PST export may cause some issues. Why planning exports, consider how the following will be handled in systems consuming the export:

1. ***Cloud attachments****. (AKA modern attachments) are* ***not*** *included in the PST file when the file was attached to an email. Similarly, attachments to Teams conversations will not be saved in the folder with the HTML transcripts of the conversations. Instead, the files are exported in the SharePoint folder, in a folder structure that represents where the file was found on SharePoint or OneDrive.*

   This is an issue because the party receiving your export may not know how to pair the cloud attachments with the parent communications or may be using software that does not support this functionality.

2. ***Teams and Yammer Transcripts:*** *As notes above, Teams conversations are exported as HTLM files. These files are easy to read and load quickly in review platforms. However, if a party receiving the files processes these conversations as HTML files, key metadata about the conversation like dates and conversation participants will be lost.*

   The report included with the export contains metadata about the Teams conversations. The parties receiving the data must be aware that the report includes this information and know how to parse it out of the file.

3. **Condensed Directory Structure:** The condensed directory structure exports each individual file from the export set in one directory named “Native files.” Each file is renamed with a unique identifier as shown in Figure 77. Searchable text may also be included in the export in a directory named “Extracted Text.” The text files are named with the same unique identifier as the native files. The report file included with the export can be used to load the files into another eDiscovery review platform along with the processed metadata Premium eDiscovery generated.

   Unlike the loose files and PSTs format, the Condensed directory export format preserves parent cloud relationships for cloud attachments in a format that is ready to load into a database.

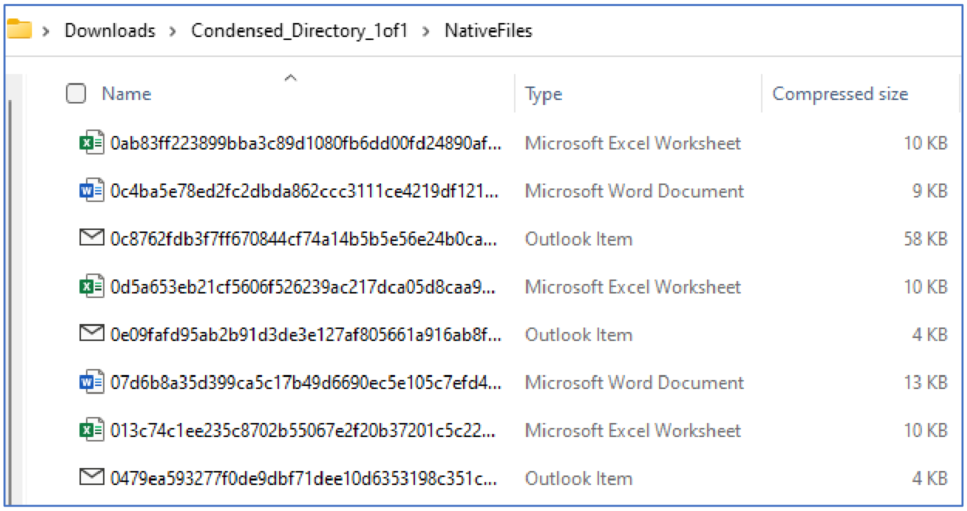


Figure 77 - Native File View

4. Condensed Directory Structure exported to Azure Storage

The final export option in Premium eDiscovery is to export to Azure Storage. This option works well with Compliance Boundaries where you can restrict the search area across regions. Because of this you may want to have the exported data within that search exported to the same locations. Exporting to Azure Secure Blob Storage provides that.

Tip

Customers frequently ask us the best format is best to use for exports. The chart below shows examples of different formats to choose when dealing with different scenarios.

Note that you may find yourself using a hybrid format when the bulk of email and loose files are exported using the loose files and PST format but Teams data and emails with cloud attachments are exported using the condensed directory format.

Knowing what type of data is included in your export set before you export will help you decide what format to choose. For example, if your data does not include modern attachments, then you will not need to consider how those parent child relationships will be handled downstream. Using the following review set filters will give insight into what is being exported:

Is Modern Attachment: *Searching for documents where this value is True will return files that are cloud attachments to emails and Teams conversations.*

File Class: *Searching for items where the value is "Conversation" will return Teams and Yammer conversations.*

Export Setting	Export Content	Reason

Condensed	Teams Conversations	HTML Transcripts of Teams Conversation; Attachments to the Teams Conversation are treated as family documents and included when possible.
Condensed	Data Set export for delivery to 3rd party review tool import	eDiscovery / Legal Services load file ready export
Condensed	Redactions	Export PDF redacted versions is only available with Condensed Directory export
Loose / PSTs	Native Files and PSTs	PSTs can only be exported when using the Loose / PSTs option. The system will generate one PST per custodian or unique data source. PSTs over 10 GB will be span into multiple PST files. SharePoint and OneDrive files will export in a folder mapping similar to the Online folder creation.
Condensed + Loose / PSTs (Hybrid)	Native Files and PSTs + Redactions	Export PDF redacted + Loose File PSTs

Jobs Report

The '**Jobs**' tab shows the progress of specific user-initiated tasks that occur within a Premium eDiscovery case. When job tasks are initiated eDiscovery Managers and Admins can view the progress of these actions is shown in the 'Jobs' tab as displayed in Figure 78 - eDiscovery Jobs overview for eDiscovery Manager.

Learn more: Manage jobs in eDiscovery (Premium) | Microsoft Learn

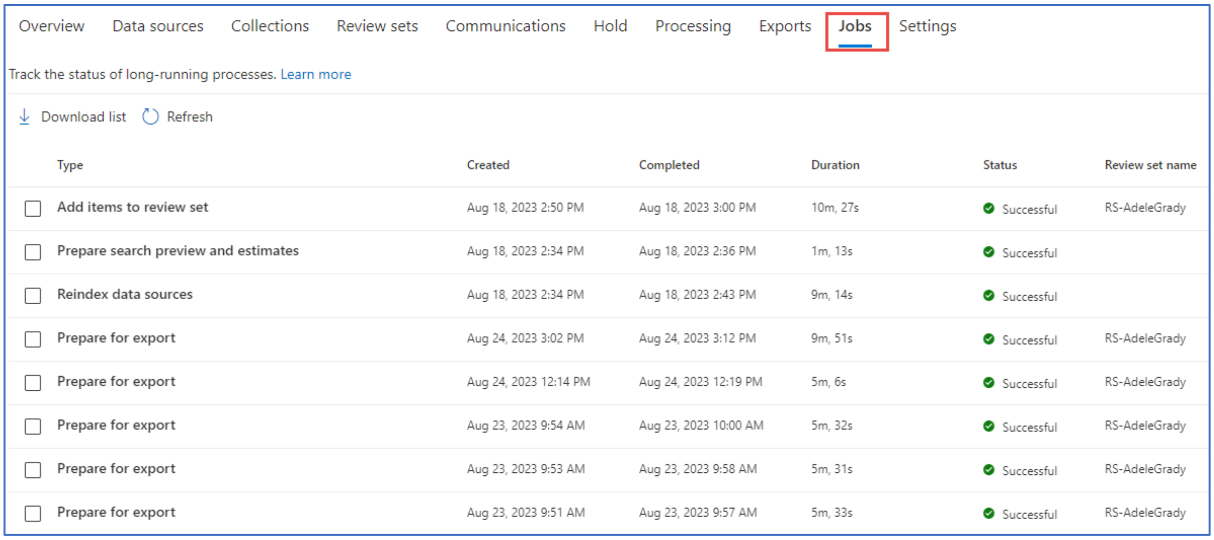


Figure 78 - eDiscovery Jobs overview for eDiscovery Manager

Under the Reports tab, eDiscovery Administrators can view, filter and group job tasks across all cases for activity for the past 30 days as demonstrated in Figure 79 - eDiscovery Jobs overview for eDiscovery Administrators.

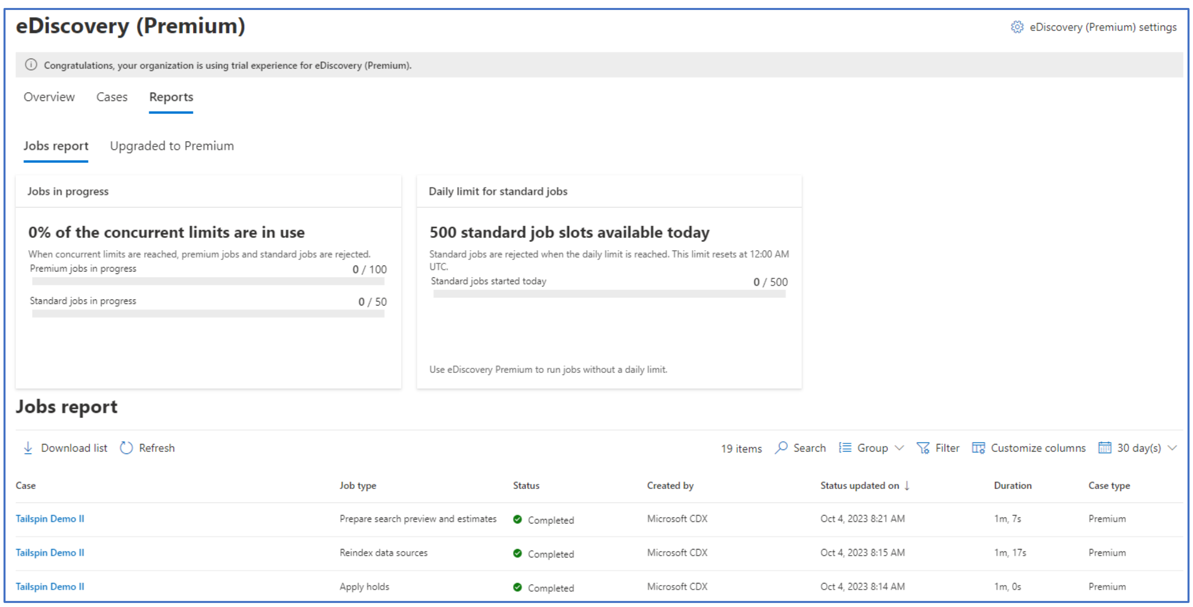


Figure 79 - eDiscovery Jobs overview for eDiscovery Administrators

From the screenshots above, there are several examples of running jobs. The table below explains what these specific jobs do. A full list of job types and descriptions can be found at the following link: https://learn.microsoft.com/en-us/purview/ediscovery-managing-jobs#job-types-and-descriptions

Job type	Description
Adding data to a review set	A user adds a collection to a review set. This job consists of two s–b jobs: • **Export** - A list of items in the collection is generated.

	• **Ingestion & Indexing** - The items in the collection that match the search query are copied to an Azure Storage location (in a process called *ingestion*) and then those items in the Azure Storage location are reindexed. This new index is used when querying and analyzing items in the data set.
Preparing search preview	After a user creates and runs a new draft collection (or reruns an existing draft collection), the search tool prepares a sample subset of items (that match the search query) that can be previewed. Previewing search results helps you determine the effectiveness of the search.
Re-indexing custodian data	When you add a custodian to a case, all partially indexed items 'n the custodian's selected data sources are reindexed by a process called *Advanced indexing*. This job is also triggered when you click '**Update index**' on the '**Processing**' tab of a case, and when you update the index for a specific custodian on the custodian properties flyout page.
Preparing data for export	A user exports documents from a review set. When the export process is complete, they can download the exported data to a local computer.

Advanced Topics

Compliance Boundaries

Compliance Boundaries is a solution that enables businesses to create technical boundaries within which eDiscovery Managers and eDiscovery Administrators can search for content, preview search results, export search results, and purge items (soft delete by default). This solution is based on Roles Based Access Control (RBAC) Groups and Security Permissions Filtering. The RBAC Groups manage the eDiscovery permissions of those who can access a Compliance Boundary. The Security Permissions Filtering controls the content locations that can be searched within the configured Compliance Boundary.

Organizations use Compliance Boundaries to meet regulatory requirements by dividing their eDiscovery landscape into separate geographical investigation areas. By creating custom Permissioned Groups for each region, investigators can only search for custodians within their operating regions. For instance, if your organization operates in the Americas, Europe, and Asia Pacific regions, you can configure a Compliance Boundary for each region (AMER, EMEA, and APAC). This will ensure that only the respective teams can search for data within their respective regions by filtering the visibility. This approach helps to maintain compliance with relevant data privacy laws and regulations.

Set up compliance boundaries for eDiscovery investigations | Microsoft Learn

Automation

As the volume of eDiscovery activities increases and organizations continue to mature, they typically look to take advantage of automation capabilities to increase efficiency and reduce the risk associated with ad-hoc manual processes. For example, some organizations leverage automation options to integrate Premium eDiscovery with their case management systems – creating Premium eDiscovery cases when a case is created in the management system. Organizations also use automation options to generate custom reports on their portfolio of eDiscovery cases and holds.

The Microsoft Graph APIs for eDiscovery provide functionality for automation. The commands, part of the Security namespace, include both generally available and beta eDiscovery commands. Microsoft also provides some options for managing eDiscovery cases using the Security & Compliance PowerShell commands in the Exchange Online PowerShell module.

Visit the following links for more information on automating Premium eDiscovery:

- Use the Microsoft Graph API - Microsoft Graph | Microsoft Learn
- Use the Microsoft Graph security API - Microsoft Graph beta | Microsoft Learn
- Policy & Compliance eDiscovery - PowerShell | Learn

Tip
Using automation to create cases will help ensure settings like enabling OCR and setting permissions are consistent across the cases in your organization.

Converting Standard eDiscovery Cases to Premium eDiscovery Cases

eDiscovery Administrators may convert Standard eDiscovery cases to Premium by selecting the Actions options for a case from the Standard eDiscovery case listing and choosing '**Upgrade case to Premium**' from the resulting menu as demonstrated in Figure 80 - Upgrade Standard eDiscovery Case.

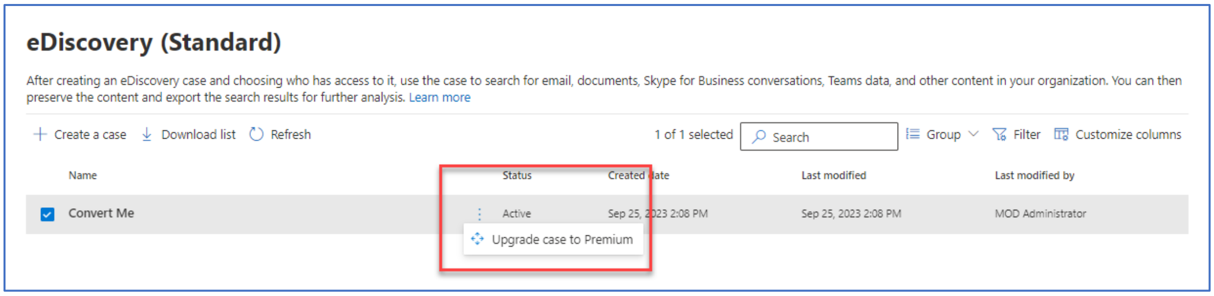


Figure 80 - Upgrade Standard eDiscovery Case

The following happens when a case is converted:

1. Once a case is upgraded, searches are available under the 'Collections section' in the Premium eDiscovery case.
2. Information for jobs created in the Standard eDiscovery case are maintained after the upgrade and appear in the Jobs menu for the Premium eDiscovery case.
3. Holds in the Standard case are maintained in the upgraded Premium case. No holds are removed or recreated during the upgrade process.
4. The search conditions from the Standard case are copied to a collection in the new Premium case. You can refresh/rerun the estimates, however this replaces all previous search statistics for the search.

Along with upgrading cases, eDiscovery Administrators may view a report of upgraded cases in the report's menu for Premium eDiscovery as shown in Figure 81 - Upgraded Case Report.

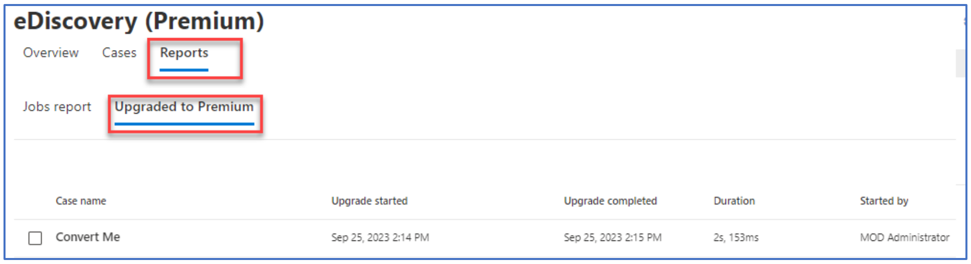


Figure 81 - Upgraded Case Report

See: [Upgrade a Standard eDiscovery case to Premium | Microsoft Learn]

Premium eDiscovery Settings

eDiscovery Administrators may manage global Premium eDiscovery settings through the eDiscovery (Premium) settings menu on the Premium eDiscovery overview page as displayed in Figure 82 - Premium eDiscovery Settings.

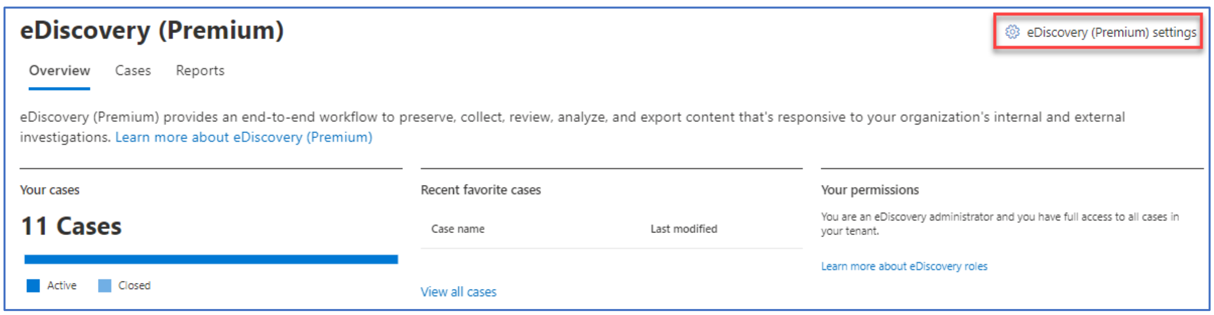


Figure 82 - Premium eDiscovery Settings

At this writing, the Premium eDiscovery settings page includes seven categories as shown in Figure 83 - Premium eDiscovery Settings.

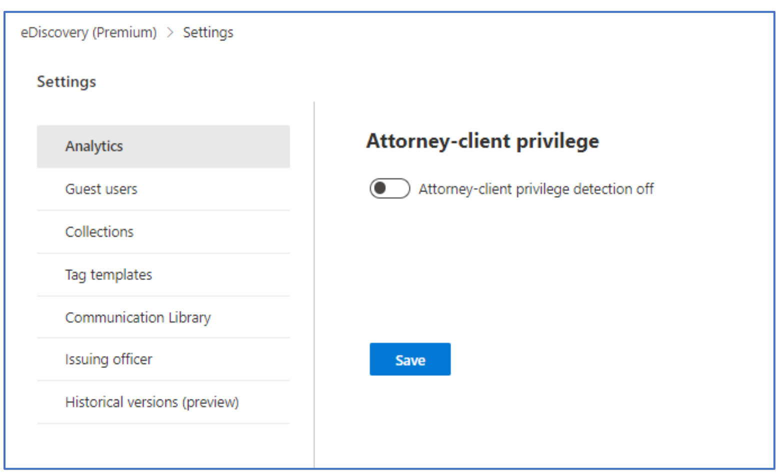


Figure 83 - Premium eDiscovery Settings

1. Analytics: If you have worked with review set analytics you may expect this section to relate to defaults for near duplicates and other analytic features. It does not. Instead, this is where detection for potentially privileged communications across all cases is configured.

See: Set up attorney-client privilege detection in Premium eDiscovery | Learn

2. Guest users: Introduced as a preview feature in May of 2023, guest access allows eDiscovery Managers to invite external users to a case. An eDiscovery Administrator must enable the feature here before any invites can be sent. An eDiscovery Administrator must approve each invite in the guest user panel and may monitor usage and revoke access at any time.

   See: Guest access in eDiscovery | Learn

3. Collections: Introduced in summer of 2023, the collection settings allow eDiscovery Administrators to set organization default options for collection searches, retrieval, and processing. To ensure consistency across an organization, these options may be enforced. Options include:

   a. Customization: To lock the selection on this page, uncheck this box.

   b. Locations: When doing an additional locations collection search, users will search all active user, shared, and resource mailboxes by default. To include inactive mailboxes, groups (Teams), Teams Shared channel mailboxes, and guest mailboxes, the eDiscovery practitioner must select these additional locations.

   c. Retrieval: Retrieval options that can be changed include, collecting Teams and Yammer conversations as transcript, collecting cloud attachments, collecting all versions of a document, and collecting unindexed items.

4. Tag Templates: Introduced in September of 2023, Tag templates are tag groups that can be reused across multiple review sets and cases.

5. Communication Library: eDiscovery Administrators create and edited Communication templates here.

6. Issuing Officers: Communications may be sent on behalf of these M365 accounts by eDiscovery managers.

7. Historical Versions (preview): SharePoint versioning allows for tracking the activity of an item, which can help in providing an audit trail. 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.

Figure 1 - Create a Case 9
Figure 2 - Case Information 10
Figure 3 – Case Setup 11
Figure 4 – Case Setup Cont'd – Text to ignore and OCR 13
Figure 5 – Premium eDiscovery Case Overview Page 13
Figure 6 - Premium eDiscovery Case Settings 14
Figure 7 - Case information settings 15
Figure 8 – Add Custodian 18
Figure 9 – Selecting Custodians 18
Figure 10 - Selecting Custodian Hold 19
Figure 11 – Place Custodian Locations on Hold 19
Figure 12 – Added Custodians 20
Figure 13 – Import Custodians 20
Figure 14 – CSV Wizard 20
Figure 15 – Example CSV Import 21
Figure 16 – Add Data Locations 22
Figure 17 – Non-Custodial Data Locations. 23
Figure 18 – Search for a Non-custodial location 23
Figure 19 – Non-custodial locations 24
Figure 20 – Select Teams for a Custodian 26
Figure 21 - Select Custodial Teams 27
Figure 22 - Update Data Source Index 28
Figure 23 – Create a Manual Hold 30
Figure 24 - Choose Locations for Manual Hold 30
Figure 25 – Enter Queries for Hold 31
Figure 26 – Condition card builder for Holds. 31
Figure 27 - New Communication 32
Figure 28 - New Communication, Issuing Officer 32
Figure 29 - Define Portal Content 33
Figure 30 - Set Notifications 34
Figure 31- Release Email 35
Figure 32 - Notification Reminders 36
Figure 33- Select Custodians to Notify 37
Figure 34- Communication Summary 37
Figure 35 – Hold Notice Panel 38
Figure 36 - New Communication from a Template 39
Figure 37 - Create a Collection 40
Figure 38 - New Collection 40

Figure 39 - Choose Custodial Data Sources........40
Figure 40 - Select Custodian Sources........41
Figure 41 - Add non-custodial data sources........41
Figure 42- Additional Locations Exchange........42
Figure 43- Search Options for Exchange "All" search........43
Figure 44 - Additional SharePoint Locations........44
Figure 45 - New Collection Query Builder........45
Figure 46- Select an Operator........1
Figure 47 - Condition Card Builder........2
Figure 48 - Choose Conditions........2
Figure 49 - Condition Card Example for all email messages between January 1, 2022 and December 12, 2022.........3
Figure 50 - KQL Editor........3
Figure 51 - KQL Auto Fill........4
Figure 52 - Example KQL Query........4
Figure 53 - Collection Review........5
Figure 54 - Collection Status........5
Figure 55- Collection Summary - Progress........6
Figure 56 - Collection Summary - Estimate........6
Figure 57 - Collection Statistics........7
Figure 58 - View Collection Sample........7
Figure 59 - Collection Sample........8
Figure 60- Commit Collection........8
Figure 61- Collection Actions Button........9
Figure 62 - Create a Review Set........12
Figure 63 - Current Review Set........13
Figure 64 - Review Set ready for review........13
Figure 65 - Open Review Set........13
Figure 66 – Run Document & email Analytics........14
Figure 67 - Query Review Set........16
Figure 68 - Select Tags........17
Figure 69 - Create New Tags........18
Figure 70 - Tag an Item........19
Figure 71 - Tag Filter........20
Figure 72 - Export Overview........**Error! Bookmark not defined.**
Figure 73 - Export Items........**Error! Bookmark not defined.**
Figure 74 - Export Items to Review Set........**Error! Bookmark not defined.**
Figure 75 - Download Files Option........21
Figure 76 - Downloaded Files........21

Figure 77 - Export Options 23
Figure 78 - Report Only .... **Error! Bookmark not defined.**
Figure 79 - Report Only File 23
Figure 80 - PST Export .... **Error! Bookmark not defined.**
Figure 81 - PST Export .... **Error! Bookmark not defined.**
Figure 82 - Condensed Directory .... **Error! Bookmark not defined.**
Figure 83 - Native File View 25
Figure 84 - eDiscovery Jobs overview for eDiscovery Manager 27
Figure 85 - eDiscovery Jobs overview for eDiscovery Administrators 27
Figure 86 - Upgrade Standard eDiscovery Case 29
Figure 87 - Upgraded Case Report 30
Figure 88 - Premium eDiscovery Settings 30
Figure 89 - Premium eDiscovery Settings 30