Advanced eDiscovery in Microsoft 365

Use the following guide to learn more about the latest Advanced eDiscovery solution and how to configure these solution elements for your organization. Getting started is easy, and this guide will help you prioritize your first steps in meeting internal policy, reducing risk, and ultimately increase efficiency using Microsoft 365.

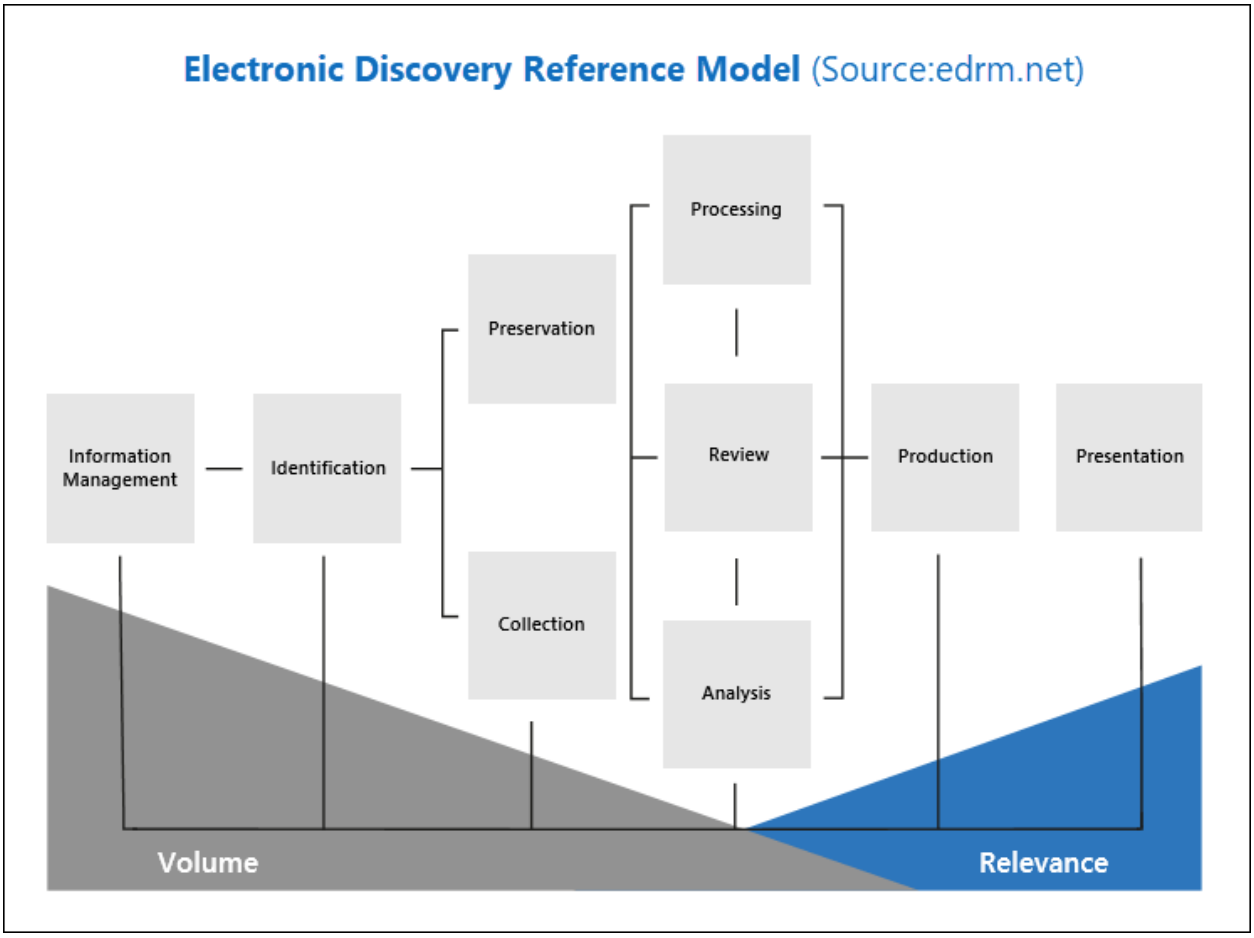
Prepared by:
Microsoft 365 Security & Compliance team

Advanced eDiscovery solution in Microsoft 365: Overview

The Advanced eDiscovery solution in Microsoft 365 builds on the existing eDiscovery and analytics capabilities in Office 365. This new solution, called *Advanced eDiscovery*, provides an end-to-end workflow to preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations. It also lets legal teams manage the entire legal hold notification workflow to communicate with custodians involved in a case.

Alignment with EDRM

The built-in workflow of Advanced eDiscovery aligns with the eDiscovery process outlined by the Electronic Discovery Reference Model (EDRM).



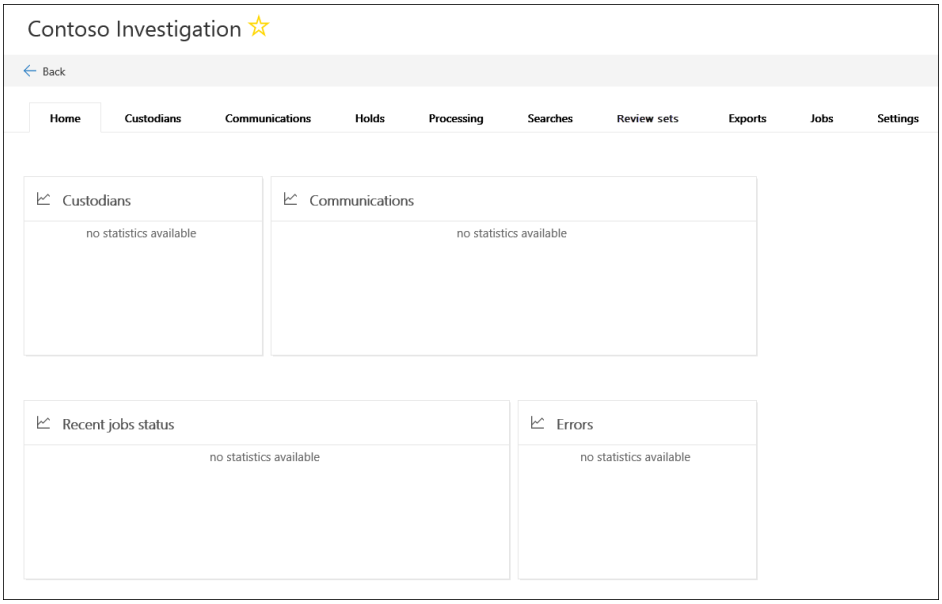
At a high level, here's how Advanced eDiscovery supports the EDRM workflow:

I. **Identification.** After you identify potential persons of interest in an investigation, you can add them as custodians to an Advanced eDiscovery case. After users are added as custodians, it's easy to preserve, collect, and review custodian documents.
II. **Preservation.** Advanced eDiscovery lets you place a legal hold on the data sources associated with the custodians in a case. You can also place non-custodial data on hold. Advanced eDiscovery also has a built-in communications workflow so you can send legal hold notifications to custodians and track their acknowledgments.
III. **Collection.** After you identified (and preserved) the data sources relevant to the investigation, you can use the built-in search tool in Advanced eDiscovery search for and collect live data from the custodial data sources (and non-custodial data sources, if applicable) that may be relevant to the case.
IV. **Processing.** After you've collected all data relevant to the case, the next step is process it for further review and analysis. In Advanced eDiscovery, the in-place data that you identified in the collection phase is copied to an Azure Storage location (called a *review set*), which provides you with a static view of the case data.
V. **Review.** After data has been added to a review set, you can view specific documents and run another queries to reduce the data to what is most relevant to the case. Also, can annotate and tag specific documents.
VI. **Analysis.** Advanced eDiscovery provides integrated analytics tool that helps you further cull data from the review set that you determine isn't relevant to the investigation. In addition to reducing the volume of relevant data, Advance eDiscovery also helps you save legal review costs by letting you organize content to make the review process easier and more efficient.
VII. **Production** and **Presentation.** When you're ready, you can export documents from a review set for legal review. You can export documents in their native format or in an EDRM-specified format so they can be imported into third-party review applications.

Getting started: create a new case

Go to https://protection.office.com.

1. Sign into Office 365 using your work or school account.
2. In the Security & Compliance Center, click **eDiscovery > Advanced eDiscovery**.
3. On the **Advanced eDiscovery** page, click **Create a case**.
4. On the **New eDiscovery case** flyout page, give the case a name (required), and then type an optional case number and description. Note that the case name must be unique in your organization.
5. Under **Do you want to configure additional settings after creating this case?** do one of the following:
    - Click **Yes** to create the case and display the **Settings** page in the new case. This allows you to add members to the case.
    - Click **No** to just create the case and display it in the list of cases on the **Advanced eDiscovery** page. If you choose this option, you will be added as the only member of the case and the default search and analytics settings will be used. You can add members or change settings any time after the case is created.
6. Click **Save** to create the case. The new case is displayed in the list of cases on the **Advanced eDiscovery** page.
7. To open a case, click the name of the case. The **Home** tab for the case is displayed. For example, here's a new case named *Contoso Investigation*.



I. Identification

Work with custodians

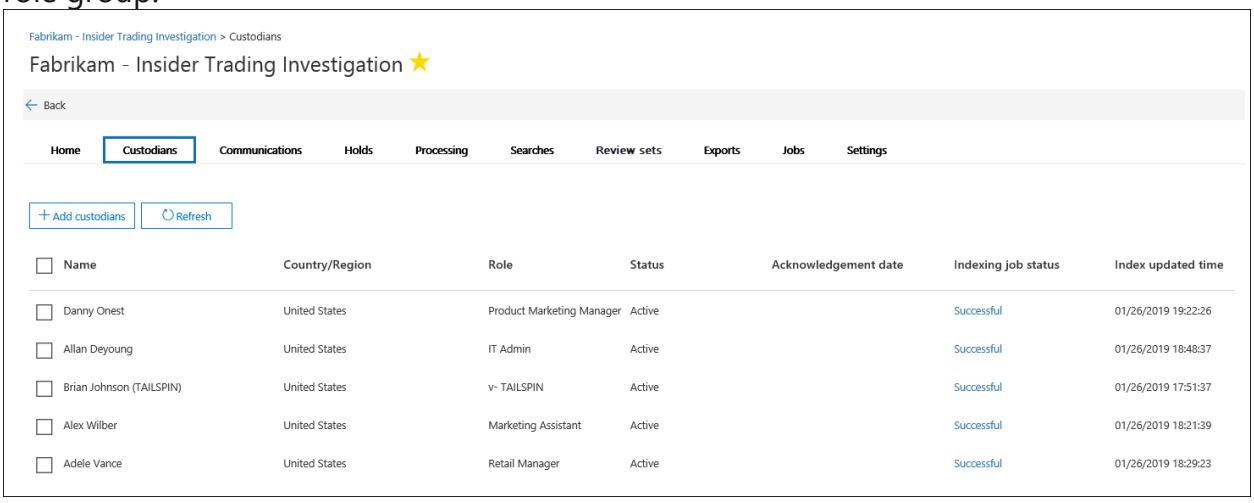
When an organization responds to a legal investigation, the workflow around identifying, preserving, and collecting potentially relevant content is based on the people in the organization who are the custodians of relevant data. In eDiscovery, these individuals are called *data custodians* (or just *custodians*) and are defined as "persons having administrative control of a document or electronic file". For example, the custodian of an email message could be the owner of the mailbox that contains the relevant message.

By using the built-in custodian management tool in Advanced eDiscovery, organizations can secure electronically stored information from inadvertent (or intentional) deletion. This lets you eliminate the time-consuming and error-prone process of manually having to perform the legal hold processes.

Add custodians to an Advanced eDiscovery case

Use the built-in custodian management tool in Advanced eDiscovery to coordinate your workflows around managing custodians and identifying relevant, custodial data sources associated with a case. When you add a custodian, the system can automatically identify and place a hold on their Exchange mailbox and OneDrive for Business account.

Use the following workflow to add and manage custodians in Advanced eDiscovery cases. To add custodians to a case, you must be a member of the eDiscovery Manager role group:



Step 1: Add potential custodians
The first step is to identify and add custodians to the case.

Step 2: Select custodian data sources
After adding custodians, the custodian tool will help you identify the primary data sources owned by each custodian; specifically, these data locations are the custodian's Exchange mailbox and OneDrive account.

Step 3: Associate additional data sources to a custodian
Depending on the case you're investigating, you may also need to search (and preserve content in) mailboxes that a specific custodian may have accessed, Office 365 groups that a custodian is currently a member of, or sites that a custodian has also accessed.

Step 4: Place custodians on hold
After you've finalized the custodians and data sources to add to the case, you can optionally place some or all of the custodians on hold.

View additional step-by-step guides to manage custodians in an Advanced eDiscovery case and view custodian activity.

II. Preservation

Work with communications

Advanced eDiscovery 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.

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

With Advanced eDiscovery, legal teams can create and customize their legal hold notification workflow. The custodian communications tool lets legal teams to configure the following notices and workflows:

- Issuance notice
- Re-Issuance notice
- Release notice
- Reminders and escalations

Role groups and permissions

Legal teams can control and segregate their case activity using eDiscovery-related role groups and permissions in the Security & Compliance Center. To create and manage legal hold notifications, a user must be part of the eDiscovery Manager or eDiscovery Administrator role groups.

View the step-by-step guide for creating a legal hold notice and managing hold notifications.

Communications editor

As you define the content of your portal content, legal hold notifications, and related reminders/escalations, you can leverage the Communications Editor to format and dynamically customize your content by using the rich text editor and merge field variables.

Manage hold notifications

After you have initiated your legal hold notification workflow, you can leverage Advanced eDiscovery to track the status of your communications. The Communications Tab showcases all of the hold notifications within your Advanced eDiscovery case. Here, you can see details, such as the number of custodians that have been assigned or have acknowledged the notice. You can also:

- **View communication details:** track and preview acknowledgements
- **Take action on existing communications:** re-send a hold notice or edit a communication by updating requirements, notifications, or settings

Acknowledge a hold notification

When responding to a regulatory request or investigation, you may be required to inform custodians of their obligation to preserve electronically stored information (ESI) as well as any material that may be relevant to an active or imminent legal matter. Once sent, legal teams must know that each custodian has received, read, and understood, and agreed to comply with the given instructions.

Manage holds in Advanced eDiscovery

You can use an Advanced eDiscovery case to create holds to preserve content that might be relevant to your case. 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.

View hold statistics: After some time, information about the new hold is displayed in the details pane on the **Holds** tab for the selected hold. This information includes the number of mailboxes and sites on hold and statistics about the content that was placed on hold. These hold statistics help you identify how much content that's related to the eDiscovery case is being held.

You can also perform actions like apply a query to your custodian-based hold. For more information about creating a hold query and using conditions, see Keyword queries and search conditions for Content Search.

Manage non-custodial holds
When you create a hold, you have the following options to scope the content that is held in the specified content locations:

- You create an infinite hold where all content is placed on hold. Alternatively, you can create a query-based hold where only content that matches a search query is placed on hold.
- You can specify a date range to hold only the content that was sent, received, or created within that date range. Alternatively, you can hold all content regardless of when it was sent, received, or created.

III. Collection

Collect data for a case in Advanced eDiscovery

Once you have identified custodians and data sources that are of interest for your case, it's time to identify the set of documents to delve into. You can use the Search tool in Advanced eDiscovery to identify these from custodial and non-custodial locations in Office 365.

After you run a search, you will be able to view statistics on the retrieved items such as the locations that had the most items that matched the search query. You can also

preview a subset of the results. When you've identified the set of documents that want to further examine, you can add the search results to a review set to collect and process.

Once you collect data, you'll be able to create a search, build search queries, view search results and statistics, and add search results to a review set.

IV. Processing

Work with processing errors

Processing is the process of file identification, expansion of embedded documents and attachments, text extraction, OCR (Optical Character Recognition) of image files and indexing of that content.

Advanced indexing of custodian data
When a custodian is added to an Advanced eDiscovery case, any content in Office 365 that was deemed as partially indexed is re-processed to make it fully searchable. This process is called *Advanced indexing*. Content can be partially indexed for a number of reasons including the existence of images, unsupported file types or when indexing file size limits are encountered.

Error remediation when processing data
Error remediation allows eDiscovery administrators the ability to rectify data issues that prevent Advanced eDiscovery from properly processing the content. For example, files that are password protected can't be processed since the files are locked or encrypted. Using error remediation, eDiscovery administrators can download files with such errors, remove the password protection, and then upload the remediated files.

View the entire workflow to remediate files with errors in Advanced eDiscovery cases here.

Single item error remediation
Error remediation gives Advanced eDiscovery users the ability to rectify data issues that prevent Advanced eDiscovery from properly processing the content. A new feature called *single item error remediation* gives eDiscovery managers the ability to view the metadata of files with a processing error and if necessary remediate the error directly in the review set.

V. Review

Manage review sets

Review sets are a static set of documents where you can analyze, query, view, tag, and export data in a case. For more information about performing these tasks, see:

- Analyze data in a review set
- Query the data in a review set
- View documents in a review set
- Tag documents in a review set
- Export case data

Not all documents that you need to analyze in Advanced eDiscovery are located in Office 365. With the non-Office 365 data import feature in Advanced eDiscovery, you can upload documents that aren't located in Office 365 to a review set. The article here shows you how to bring your non-Office 365 documents into Advanced eDiscovery for analysis.

Add data to a review set from another review set
In some cases, it may be necessary to select documents from one review set and work with them individually in another review set. This is especially useful if you've culled content in a review set and want to run analytics on the subset of data. Follow the workflow in this article to add content from one review set to another.

Set up attorney-client privilege detection
A major and costly aspect of the review phase of any eDiscovery process is reviewing documents for privileged content. Advanced eDiscovery provides machine learning-based detection of privileged content to make this process more efficient. This feature is called *attorney-client privilege detection*. **NOTE**: You must opt in to the attorney-client privilege detection model before you can use it.

When attorney-client privilege detection is enabled, all documents in a review set will be processed by the attorney-client privilege detection model when you analyze the data in the review set. The model looks for privileged content and participants.

View the step-by-step setup instructions here.

VI. Analysis

Analyze data in a review set

When the number of collected documents is large, it can be difficult to review them all. Advanced eDiscovery provides several tools to analyze the documents to reduce the volume of documents to be reviewed without any loss in information, and to help you organize the documents in a coherent manner. To learn more about these capabilities, see:

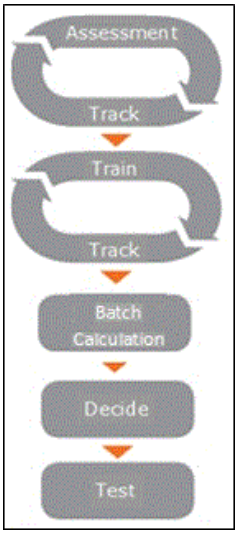
- Near duplicate detection
- Email threading
- Themes

Use the Relevance module to analyze data

In Advanced eDiscovery, the Relevance module includes the Relevance training and review of files related to a case. In order to use the Relevance workflow, go to Manage review set within a review set and click on Show Relevance. There are a couple of steps you need to complete before you can start the workflow:

- Process: each load set added to the review set will show up as a "container" here. You need to process these documents before you can add them to Relevance module; this is also where you can mark them as seed or pre-tagged for a specific issue.
- Add to Relevance: under Relevance > Loads, you can add documents that have been processed to Relevance to make them available for training.

The Relevance workflow is shown and described as follows:



VII. Production, Presentation, and Additional Resources

Export case data

There are three ways to export data from a review set:

Download – Use to download (by using a browser) a small set of native files. This is the quickest was to export a small set of data.

- Download offers a simple way to download content from a review set in Native format. It leverages the browser's data transfer features so a browser prompt will appear once a download is ready.
- To download content from a review set, start by selecting the files you want to download then select "Download" under the Actions menu.

Export – Use to customize what data is exported, including the export of metadata files, native files, text files, and redacted documents that have been saved to a PDF file. After exported data is uploaded Azure storage location, you have to download it to a local computer.

When you export documents from a review set in an Advanced eDiscovery case, the documents are uploaded to a Microsoft-provided Azure Storage location or to an Azure Storage location managed by your organization. The type of Azure Storage location used depends on which option was selected when the documents were exported.

This article provides instructions for how to use the Microsoft Azure Storage Explorer to connect to an Azure Storage location to browse and download the exported documents. For more information about Azure Storage Explorer, see QuickStart: Use Azure Storage Explorer.

Additional Resources:

- What's new in Advanced eDiscovery
- Limits in Advanced eDiscovery
- Supported file types
- Document metadata fields
- Conversation review sets
- Troubleshoot AzCopy