# Get started with Core eDiscovery

To view contributors to this article access the link below

*https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide*

## In this article



Core eDiscovery in Microsoft 365 provides a basic eDiscovery tool that organizations can use to search and export content in Microsoft 365 and Office 365. You can also use Core eDiscovery to place an eDiscovery hold on content locations, such as Exchange mailboxes, SharePoint sites, OneDrive accounts, and Microsoft Teams. Nothing is needed to deploy Core eDiscovery, but there are some prerequisite tasks that an IT admin and eDiscovery manager have to complete before your organization can start using Core eDiscovery to search, export, and preserve content.

This article discusses the steps necessary to set up Core eDiscovery. This includes ensuring the proper licensing required to access Core eDiscovery and place an eDiscovery hold on content locations, as well as assigning permissions to your IT, legal, and investigation team so they can access and manage cases. This article also provides a high-level overview of using cases to search for and export content.

## Step 1: Verify and assign appropriate licenses

Licensing for Core eDiscovery requires the appropriate organization subscription and per-user licensing.

- **Organization subscription:** To access Core eDiscovery in the Microsoft 365 compliance center or the Office 365 Security & Compliance Center and use the hold and export features, your organization must have a Microsoft 365 E3 or Office 365 E3 subscription or higher.
- **Per-user licensing:** To place an eDiscovery hold on user mailboxes, that user must be assigned one of the following licenses, depending on your organization subscription:
    - A Microsoft 365 E3 or Office 365 E3 license or higher
    - A Microsoft 365 E1 or Office 365 E1 license with an Exchange Online Plan 2 or Exchange Online Archiving add-on license

    For information about how to assign licenses, see Assign licenses to users.

For information about Microsoft 365 and Office 365 licensing, download and see the "Discover & Respond" solution in the Microsoft 365 Compliance Licensing Comparison.

**Step 2: Assign eDiscovery permissions**

To access Core eDiscovery or be added as a member of a Core eDiscovery case, a user must be assigned the appropriate permissions. Specifically, a user must be added as a member of the eDiscovery Manager role group in the Office 365 Security & Compliance Center. Members of this role group can create and manage Core eDiscovery cases. They can add and remove members, place an eDiscovery hold on users, create and edit searches, and export content from a Core eDiscovery case.

Complete the following steps to add users to the eDiscovery Manager role group:

1. Go to https://protection.office.com/permissions and sign in using the credentials for an admin account in your Microsoft 365 or Office 365 organization.
2. On the **Permissions** page, select the **eDiscovery Manager** role group.
3. On the eDiscovery Manager flyout page, click **Edit** next to the **eDiscovery Manager** section.
4. On the **Choose eDiscovery Manager** page in the edit role group wizard, click **Choose Discovery Manager**.
5. Click **Add** then select the checkbox for all users you want to add to the role group.
6. Click **Add** to add the selected users, and then click **Done**.
7. Click **Save** to add the users to the role group, and then click **Close** to complete the step.

**More information about the eDiscovery Manager role group**

There are two subgroups in the eDiscovery Manager role group. The difference between these subgroups is based on scope.

- **eDiscovery Manager:** Can view and manage the Core eDiscovery cases they create or are a member of. If another eDiscovery Manager creates a case but doesn't add a second eDiscovery Manager as a member of that case, the second eDiscovery Manager won't be able to view or open the case on the Core eDiscovery page in the compliance center. In general, most people in your organization can be added to the eDiscovery Manager subgroup.

- **eDiscovery Administrator:** Can perform all case management tasks that an eDiscovery Manager can do. Additionally, an eDiscovery Administrator can:
    - View all cases that are listed on the Core eDiscovery page.
    - Manage any case in the organization after they add themselves as a member of the case.
    - Access and export case data for any case in the organization.

  Because of the broad scope of access, an organization should have only a few admins who are members of the eDiscovery Administrators subgroup.

For more information about eDiscovery permissions and a description of each role that's assigned to the eDiscovery Manager role group, see Assign eDiscovery permissions.

**Step 3: Create a Core eDiscovery case**

The next step is to create a case and start using Core eDiscovery. Complete the following steps to create a case and add members. The user who creates the case is automatically added as a member.

1. Go to https://compliance.microsoft.com and sign in using the credentials for a user account that has been assigned the appropriate eDiscovery permissions. Members of the Organization Management role group can also create Core eDiscovery cases.
2. In the left navigation pane of the Microsoft 365 compliance center, click **Show all**, and then click **eDiscovery > Core**.
3. On the **Core eDiscovery** page, click **Create a case**.

4. On the **New case** flyout page, give the case a name (required), and then type an optional case number and description. The case name must be unique in your organization.
5. Click **Save** to create the case.

   The new case is created and displayed on the Core eDiscovery page. You may have to click **Refresh** to display the new case.

**Step 4 (optional): Add members to a Core eDiscovery case**

If you create a case in Step 3 and you're the only person who will use the case, then you don't have to perform this step. You can start using the case to create eDiscovery holds, search for content, or export search results. Perform this step if you want to give other users (or roles group) access to the case.

1. On the **Core eDiscovery** page in the Microsoft 365 compliance center, click the name of the case that you want to add members to.
2. On the **Manage this case** flyout page, under **Manage members**, click **Add** to add members to the case.

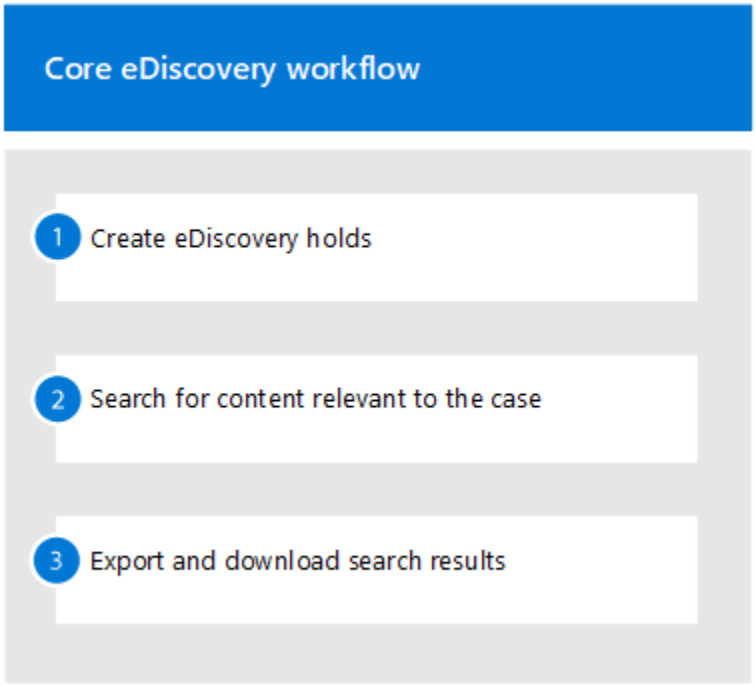
   You can also choose to add role group as members of a case. Under **Manage role groups**, click **Add**. You can only assign the role groups that you are a member of to a case. That's because role groups control who can assign members to an eDiscovery case.

3. In the list of people or role groups that can be added as members of the case, click the check box next to the names of the people (or role groups) that you want to add. If you have a large list of people who can added as members, use the **Search** box to search for a specific person in the list.

4. After you select the people or role groups to add as members of the case, click **Add**.
5. Click **Save** to save the new list of case members.

**Explore the Core eDiscovery workflow**

To get you started using core eDiscovery, here's a simple workflow of creating eDiscovery holds for people of interest, searching for content that relevant to your investigation, and then exporting that data for further review. In each of these steps, we'll also highlight some extended Core eDiscovery functionality that you can explore.




1. **Create an eDiscovery hold**. The first step after creating a case is placing a hold (also called an *eDiscovery hold*) on the content locations of the people of interest in your investigation. Content locations include Exchange mailboxes, SharePoint sites, OneDrive accounts, as well as the mailboxes

and sites associated with Microsoft Teams and Office 365 Groups. While this step is optional, creating an eDiscovery hold preserves content that may be relevant to the case during the investigation. When you create an eDiscovery hold you can preserve all content in specific content locations or you can create a query-based hold to preserve only the content that matches a hold query. In addition to preserving content, another good reason to create eDiscovery holds is to quickly search the content locations on hold (instead of having to select each location to search) when you create and run searches in the next step. After you complete your investigation, you can release any hold that you created.

2. **Search for content**. After you create eDiscovery holds, use the built-in search tool to search the content locations on hold. You can also search other content locations for data that may be relevant to the case. You can create and run different searches that are associated with the case. You use keywords, properties, and conditions to build search queries that return search results with the data that's most likely relevant to the case. You can also:
    - View search statistics that may help you refine a search query to narrow the results.
    - Preview the search results to quickly verify whether the relevant data is being found.
    - Revise a query and rerun the search.
3. **Export and download search results**. After you search for and find data that's relevant to your investigation, you can export it out of Office 365 for review by people outside of the investigation team. Exporting data is a two-step process. The first step is to export the results of a search in the case out of Office 365. This is accomplished by copying the results of a search to a

Microsoft-provided Azure Storage location. The next step is to use the eDiscovery Export tool to download the content to a local computer. In addition to the exported data files, the contains of the export package also contains an export report, a summary report, and an error report.