Assign eDiscovery permissions in the Security & Compliance Center

To view contributors to this article access the link below

https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide

In this article

If you want people to use any of the eDiscovery-related tools in the Security & Compliance Center in Office 365 or the Microsoft 365 compliance center, you have to assign them the appropriate permissions. The easiest way to do this is to add the person the appropriate role group on the **Permissions** page in the Security & Compliance Center. This topic describes the permissions required to perform eDiscovery-and Content Search-related tasks using the Security & Compliance Center.

The primary eDiscovery-related role group in Security & Compliance Center is called **eDiscovery Manager**. There are two subgroups within this role group.

- **eDiscovery Managers** - An eDiscovery Manager can use the Content Search tool in the Security & Compliance Center 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 eDiscovery cases and Advanced eDiscovery cases, 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 can't access or manage cases created by other eDiscovery Managers.
- **eDiscovery Administrators** - 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 that are listed on the **eDiscovery** and **Advanced eDiscovery** pages in the Security & Compliance Center.
    - Access case data in Advanced eDiscovery for any case in the organization.
    - Manage any eDiscovery case after they add themselves as a member of the case.

    See the More information section for reasons why you might want eDiscovery Administrators in your organization.

Note

To analyze a user's data using Advanced eDiscovery, the user (the custodian of the data) must be assigned an Office 365 E5 or Microsoft E5 license. Alternatively, users with an E1 or E3 license can be assigned an E5 add-on license. Administrators, compliance officers, or legal personnel who are assigned to cases as members and use Advanced eDiscovery to collect, view, and analyze data don't need an E5 license. For more information about licensing, see Microsoft 365 licensing guidance for security & compliance.

Before you begin

- You have to be a member of the Organization Management role group or be assigned the Role Management role to assign eDiscovery permissions in the Security & Compliance Center.
- You can use the Add-RoleGroupMember cmdlet in Security & Compliance Center PowerShell to add a mail-enabled security group as a member of the eDiscovery Managers subgroup in the eDiscovery Manager role group. However, you can't add a mail-enabled security group to the eDiscovery Administrators subgroup. For details, see the More information section.

Assign eDiscovery permissions in the Security & Compliance Center

1. Go to https://protection.office.com.
2. Sign in to Office 365 using your work or school account.
3. In the left pane of the security and compliance center, select **Permissions**, and then select the checkbox next to **eDiscovery Manager**.
4. On the **eDiscovery Manager** flyout page, do one of the following based on the eDiscovery permissions that you want to assign.

   To make a user an eDiscovery Manager: Next to **eDiscovery Manager**, select **Edit**. In the **Choose eDiscovery Manager** section, select the **Choose eDiscovery Manager** hyperlink, and then select **+Add**. Select the user (or users) you want to add as an eDiscovery manager, and then select **Add**. When you're finished adding users, select **Done**. Then, on the **Editing Choose eDiscovery Manager** flyout page, select **Save** to save the changes to the eDiscovery Manager membership.

   To make a user an eDiscovery Administrator: Next to **eDiscovery Manager**, select **Edit**. In the **Choose eDiscovery Administrator** section, Under **eDiscovery Administrators**, select **Choose eDiscovery Administrator**, select **Edit**, and then select **+Add**. Select the user (or users) you want to add as an **eDiscovery Administrator**, and then **Add**. When you're finished adding users, select **Done**. Then, on the **Editing Choose eDiscovery Administrator** flyout page, select **Save** to save the changes to the eDiscovery Administrator membership.

Note

You can also use the **Add-eDiscoveryCaseAdmin** cmdlet to make a user an eDiscovery Administrator. However, the user must be assigned the Case Management role before you can use this cmdlet to make them an eDiscovery Administrator. For more information, see Add-eDiscoveryCaseAdmin.

On the **Permissions** page in the Security & Compliance Center, you can also assign users eDiscovery-related permissions by adding them to the Compliance Administrator, Organization Management, and Reviewer role groups. For a description of the eDiscovery-related RBAC roles assigned to each of these role groups, see the RBAC roles related to eDiscovery section.

RBAC roles related to eDiscovery

The following table lists the eDiscovery-related RBAC roles in the Security & Compliance Center, and indicates the built-in role groups that each role is assigned to by default.

Table 1

Role	Compliance Administrator	eDiscovery Manager & Administrator	Organization Management	Reviewer
Case Management	✓	✓	✓	
Compliance Search	✓	✓	✓	
Export		✓		
Hold	✓	✓	✓	
Preview		✓		
Review		✓		✓
RMS Decrypt		✓		
Search And Purge			✓	

The following sections describe each of the eDiscovery-related RBAC roles listed in the previous table.

Case Management

This role lets users create, edit, delete, and control access to eDiscovery and Advanced eDiscovery cases in the Security & Compliance Center. As previously explained, a user must be assigned the Case Management role before you can use the **Add-eDiscoveryCaseAdmin** cmdlet to make them an eDiscovery Administrator.

Compliance Search

This role lets users run the Content Search tool in the Security & Compliance Center to search mailboxes and public folders, SharePoint Online sites, OneDrive for Business sites, Skype for Business conversations, Office 365 Groups, and Microsoft Teams, and Yammer groups. This role allows a user to get an estimate of the search results and create export reports, but additional roles are needed to initiate content search actions such as previewing, exporting, or deleting search results.

Users who are assigned the Compliance Search role but don't have the Preview role can preview the results of a search in which the preview action has been initiated by a user who is assigned the Preview role. The user without the Preview role can preview results for up to two weeks after the initial preview action was created.

Similarly, users who are assigned the Compliance Search role but don't have the Export role can download the results of a search in which the export action was initiated by a user who is assigned the Export role. The user without the Export role can download the results of a search for up to two weeks after the initial export action was created. After that, they can't download the results unless someone with the Export role restarts the export.

For more information, see Content search in Office 365.

Export

The role lets users export the results of a Content Search to a local computer. It also lets them prepare search results for analysis in Advanced eDiscovery.

For more information about exporting search results, see Export search results from Security & Compliance Center.

Hold

This role lets users place content on hold in mailboxes, public folders, sites, Skype for Business conversations, and Office 365 groups. When content is on hold, content owners can still modify or delete the original content, but the content will be preserved until the hold is removed or until the hold duration expires.

For more information about holds, see:

- eDiscovery cases
- Advanced eDiscovery

Preview

This role lets users view a list of items that were returned from a Content Search. They can also open and view each item from the list to view its contents.

Review

This role lets users access case data in Advanced eDiscovery (classic) (also know as *Advanced eDiscovery v1*). The primary purpose of this role is to give users access to Advanced eDiscovery (classic). Users who are assigned this role can see and open the list of cases on the **eDiscovery** page in the Security & Compliance Center that they're members of. After the user accesses a case in the Security & Compliance Center, they can select **Switch to Advanced eDiscovery** to access and analyze the case data in Advanced eDiscovery (classic). This role doesn't allow the user to preview the results of a content search that's associated with the case or do other content search or case management tasks.

Note

At this time, users who are assigned the Review role (or is a member of the Reviewer role group) can't access data in Advanced eDiscovery in Microsoft 365 (also known as *Advanced eDiscovery v2*). To add members to a case in Advanced eDiscovery v2 so that they can review case data, a user must be a member of the eDiscovery Manager role group.

RMS Decrypt

This role lets users decrypt rights-protected email messages when exporting search results or preparing search results for analysis in Advanced eDiscovery. For more information about decrypting search results during export, see Export Content search results.

Search And Purge

This role lets users perform bulk removal of data matching the criteria of a content search. For more information, see Search for and delete email messages in your Office 365 organization.

More information

- **Why create an eDiscovery Administrator?** As previously explained, an eDiscovery Administrator is member of the eDiscovery Manager role group who can view and access all eDiscovery cases in your organization. This ability to access all the eDiscovery cases has two important purposes:
    - If a person who is the only member of an eDiscovery case leaves your organization, no one (including members of the Organization Management role group or another member of the eDiscovery Manager role group) can access that eDiscovery case because they aren't a member of a case. In this situation, there would be no way to access the data in the case. But because an eDiscovery Administrator can access all eDiscovery cases in the organization, they can view the case and add themselves or another eDiscovery manager as a member of the case.
    - Because an eDiscovery Administrator can view and access all eDiscovery and Advanced eDiscovery cases, they can audit and oversee all cases and associated compliance searches. This can help to prevent any misuse of compliance searches or eDiscovery cases. And because eDiscovery Administrators can access

potentially sensitive information in the results of a compliance search, you should limit the number of people who are eDiscovery Administrators.

- **Can I add a group as a member of the eDiscovery Manager role group?** As previously explained, you can add a mail-enabled security group as a member of the eDiscovery Managers subgroup in the eDiscovery Manager role group by using the **Add-RoleGroupMember** cmdlet in Security & Compliance Center PowerShell. For example, you can run the following command to add a mail-enabled security group to the eDiscovery Manager role group.

  PowerShell

```
Add-RoleGroupMember "eDiscovery Manager" -Member <name of security group>
```

Exchange distribution groups and Office 365 groups aren't supported. You must use a mail-enabled security group, which you can create in Exchange Online PowerShell by using the `New-DistributionGroup -Type Security` command. You can also create a mail-enabled security group (and add members) in the Exchange admin center or in the Microsoft 365 admin center. It might take up to 60 minutes after you create it for a new mail-enabled security to be available to add to the eDiscovery Managers role group.

Also as previously stated, you can't make a mail-enabled security group an eDiscovery Administrator by using the **Add-eDiscoveryCaseAdmin** cmdlet in Security & Compliance Center PowerShell. You can only add individual users as eDiscovery Administrators.

You also can't add a mail-enabled security group as a member of a case.