

Delegate permissions to use
eDiscovery

Assign eDiscovery permissions

+

Go to the [Microsoft 365 compliance center](#) and sign in using an account that can assign permissions.

+

In the left pane, select **Permissions**.

On the **Permissions & Roles** page, under **Compliance center**, click **Roles**.

On the **Compliance center roles** page, select **eDiscovery Manager**.

+

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**. On the **Choose eDiscovery Manager** wizard page, click **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** wizard page, select **Save** to save the changes to the eDiscovery Manager membership.

To make a user an eDiscovery Administrator: Next to **eDiscovery Administrator**, select **Edit**. On the **Choose eDiscovery Administrator** page, click **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** wizard page, select **Save** to save the changes to the eDiscovery Administrator membership.

Microsoft 365 admin center

Search

Contoso

Admin centers

- Security
- Compliance 
- Endpoint Manager
- Azure Active Directory
- Exchange
- SharePoint
- Teams
- All admin centers
- Show pinned

Install Office

Add domain

Add users

Connect

+ Add cards

Microsoft 365 compliance

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions 
- Trials

Solutions

- Catalog

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions**
- Trials

Solutions

Permissions & roles

Admin roles give users permission to view data and complete tasks in the Microsoft 365 compliance center. Give users only the access they need by assigning the least-permissive role.

Notice something different? Welcome to your one-stop-shop for managing compliance permissions. In addition to being able to view Azure AD roles, you can now manage roles for performing solution-specific tasks in the compliance center. 2 items

Name	Description
Azure AD (1)	
Roles	View and manage Azure AD roles used to perform tasks i...
Compliance center (1)	
Roles	View and manage roles used to perform solution-specific

Compliance center roles

Admin roles give users permission to view data and complete tasks in the the Microsoft 365 compliance center. Give users only the access they need by assigning the least-permissive role.

[Learn more](#)

To assign permissions for archiving and auditing, [go to the Exchange admin center](#).

To assign permissions for document deletion policies, [go to the Document Deletion Policy Center](#).

<input type="checkbox"/>	Name	Last modified 
<input type="checkbox"/>	Organization Management	March 19, 2022
<input type="checkbox"/>	Security Administrator	March 19, 2022
<input type="checkbox"/>	Billing Administrator	March 19, 2022
<input type="checkbox"/>	eDiscovery Manager	March 19, 2022
<input type="checkbox"/>	Compliance Administrator	March 19, 2022
<input type="checkbox"/>	Insider Risk Management	March 19, 2022
<input type="checkbox"/>	Insider Risk Management Admins	March 19, 2022

eDiscovery Manager

 Edit role group

 Delete role group

 Copy role group

Role group name

eDiscovery Manager

Description

[Edit](#)

Perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations.

Assigned roles

eDiscovery Manager

[Edit](#)

An eDiscovery Manager can only view and edit cases to which he or she has access.

None

eDiscovery Administrator

[Edit](#)

An eDiscovery Administrator can view and edit all cases regardless of permissions.

None

Close

Editing Choose eDiscovery Administrator

Choose the eDiscovery Administrator you want to include in this role group.

The list is currently empty.

[Choose eDiscovery Administrator](#)

Members (0)

Choose eDiscovery Administrator

<input type="checkbox"/> Name	Email address
<input checked="" type="checkbox"/> Isaiah Langer	IsaiahL@M365x81883120.OnMicrosoft.com
<input type="checkbox"/> Joni Sherman	JoniS@M365x81883120.OnMicrosoft.com
<input type="checkbox"/> Microsoft Service Account	ms-serviceaccount@M365x81883120.OnMicrosoft.com
<input type="checkbox"/> Lynne Robbins	LynneR@M365x81883120.OnMicrosoft.com
<input type="checkbox"/> Alex Wilber	AlexW@M365x81883120.OnMicrosoft.com
<input type="checkbox"/> Patti Fernandez	PattiF@M365x81883120.OnMicrosoft.com
<input type="checkbox"/> MOD Administrator	admin@M365x81883120.onmicrosoft.com
<input type="checkbox"/> Diego Siciliani	DiegoS@M365x81883120.OnMicrosoft.com
<input type="checkbox"/> Megan Bowen	MeganB@M365x81883120.OnMicrosoft.com
<input type="checkbox"/> Allan Deydung	AllanD@M365x81883120.OnMicrosoft.com

Choose eDiscovery Administrator

+ Add

- Remove



1 member added

Search

^ Members (1)

Isaiah Langer

IsaiahL@M365x81883120.OnMicrosoft.com

Done



Edit role group

Role group name

Choose roles

Choose eDiscovery Manager

Choose eDiscovery Administrator

Editing Choose eDiscovery Administrator

Choose the eDiscovery Administrator you want to include in this role group.

Selected eDiscovery Administrators

Isaiah Langer

[Edit](#)

[Save](#)

[Cancel](#)

eDiscovery Manager



 Edit role group

 Delete role group

 Copy role group

eDiscovery Manager

[Edit](#)

An eDiscovery Manager can only view and edit cases to which he or she has access.

None

eDiscovery Administrator

[Edit](#)

An eDiscovery Administrator can view and edit all cases regardless of permissions.

 [Close](#)

