+++ title = "About users and permissions" aliases = ["docs/sources/manage-users/_index.md", "docs/sources/administration/manage-users-and-permissions/about-users-and-permissions.md", "/docs/grafana/latest/permissions/overview/", "docs/sources/permissions/_index.md", "docs/sources/permissions/organization_roles.md"] weight = 100 +++

About users and permissions

A *user* is defined as any individual who can log in to Grafana. Each user is associated with a *role* that includes *permissions*. Permissions determine the tasks a user can perform in the system. For example, the **Admin** role includes permissions for an administrator to create and delete users.

You can assign a user one of three types of permissions:

- Grafana server administrator permissions: Manage Grafana server-wide settings and resources
- Organization permissions: Manage access to dashboards, alerts, plugins, teams, playlists, and other resources for an entire organization. The available roles are Viewer, Editor, and Admin.
- Dashboard and folder permission: Manage access to dashboards and folders

> ***Note**: If you are running Grafana Enterprise, you can also control access to data sources and use fine-grained access control to grant read and write permissions for specific resources. For more information about access control options available with Grafana Enterprise, refer to Grafana Enterprise user permissions features.*

Grafana server administrators

A Grafana server administrator manages server-wide settings and access to resources such as organizations, users, and licenses. Grafana includes a default server administrator that you can use to manage all of Grafana, or you can divide that responsibility among other server administrators that you create.

A server administrator can perform the following tasks:

- Manage users and permissions
- Create, edit, and delete organizations
- View server-wide settings defined in the [Configuration]({{< relref "../../administration/configuration.md" >}}) file
- View Grafana server statistics, including total users and active sessions
- Upgrade the server to Grafana Enterprise.

> ***Note:** The server administrator role does not exist in Grafana Cloud.*

Organization users and permissions

All Grafana users belong to at least one organization. An organization is an entity that exists within your instance of Grafana.

Permissions assigned to a user within an organization control the extent to which the user has access to and can update the following organization resources:

- dashboards and folders
- alerts
- playlists
- users within that organization
- data sources
- teams

- organization and team settings
- plugins
- annotations
- library panels
- API keys

Organization roles

Organization role-based permissions are global, which means that each permission level applies to all Grafana resources within an given organization. For example, an editor can see and update *all* dashboards in an organization, unless those dashboards have been specifically restricted using [dashboard permissions]({{< relref "manage-dashboard-permissions/_index.md">}}).

Grafana uses the following roles to control user access:

- **Organization administrator**: Has access to all organization resources, including dashboards, users, and teams.
- **Editor**: Can view and edit dashboards, folders, and playlists.
- **Viewer**: Can view dashboards and playlists.

The following table lists permissions for each role.

Permission	Organization administrator	Editor	Viewer
View dashboards	x	x	x
Add, edit, delete dashboards	x	x	
Add, edit, delete folders	x	x	
View playlists	x	x	x
Add, edit, delete playlists	x	x	
Create library panels	x	x	
View annotations	x	x	x
Add, edit, delete annotations	x	x	
Access Explore	x	x	
Add, edit, delete data sources	x		
Add and edit users	x		
Add and edit teams	x		
Change organizations settings	x		
Change team settings	x		
Configure application plugins	x		

Dashboard permissions

When you want to extend a viewer's ability to edit and save dashboard changes or limit an editor's permission to modify a dashboard, you can assign permissions to dashboards and dashboard folders. For example, you might want a certain viewer to be able to to edit a dashboard. While that user can *see* all dashboards, you can grant them access to *update* only one of them.

> *Important: The dashboard permissions you specify override the organization permissions you assign to the user for the selected entity.*

You can specify the following permissions to dashboards and folders.

- **Admin**: Can create, edit, or delete a dashboard or folder. Administrators can also change dashboard and folder permissions.
- **Edit**: Can create and edit dashboards. Editors *cannot* change folder or dashboard permissions, or add, edit, or delete folders.
- **View**: Can only view dashboards and folders.

For more information about assigning dashboard folder permissions, refer to [Grant dashboard folder permissions]({{< relref "./manage-dashboard-permissions/_index.md#grant-dashboard-folder-permissions" >}}).

For more information about assigning dashboard permissions, refer to [Grant dashboard permissions]({{< relref "./manage-dashboard-permissions/_index.md#grant-dashboard-permissions" >}}).

Editors with administrator permissions

If you have access to the Grafana server, you can modify the default editor role so that editors can use administrator permissions to manage dashboard folders, dashboards, and teams that they create.

> ***Note**: This permission does not allow editors to manage folders, dashboards, and teams that they do not create.*

This setting can be used to enable self-organizing teams to administer their own dashboards.

For more information about assigning administrator permissions to editors, refer to [Grant editors administrator permissions]({{< relref "./manage-server-users/grant-editor-admin-permissions.md" >}}).

Viewers with dashboard preview and Explore permissions

If you have access to the Grafana server, you can modify the default viewer role so that viewers can:

- Edit and preview dashboards, but cannot save their changes or create new dashboards.
- Access and use [Explore]({{< relref "../../explore/_index.md" >}}).

Extending the viewer role is useful for public Grafana installations where you want anonymous users to be able to edit panels and queries, but not be able to save or create new dashboards.

For more information about assigning dashboard preview permissions to viewers, refer to [Enable viewers to preview dashboards and use Explore]({{< relref "./manage-dashboard-permissions/_index.md#enable-viewers-to-preview-dashboards-and-use-explore" >}}).

Teams and permissions

A team is a group of users within an organization that have common dashboard and data source permission needs. For example, instead of assigning five users access to the same dashboard, you can create a team that consists of those users and assign dashboard permissions to the team. A user can belong to multiple teams.

You can assign a team member one of the following permissions:

- **Member**: Includes the user as a member of the team. Members do not have team administrator privileges.
- **Admin**: Administrators have permission to manage various aspects of the team, including team membership, permissions, and settings.

Because teams exist inside an organization, the organization administrator can manage all teams. When the `editors_can_admin` setting is enabled, editors can create teams and manage teams that they create. For more information about the `editors_can_admin` setting, refer to [Grant editors administrator permissions]({{< relref "./manage-server-users/grant-editor-admin-permissions.md" >}}).

Grafana Enterprise user permissions features

While Grafana OSS includes a robust set of permissions and settings that you can use to manage user access to server and organization resources, you might find that you require additional capabilities.

Grafana Enterprise provides the following permissions-related features:

- Data source permissions
- Fine-grained access control

Data source permissions

By default, a user can query any data source in an organization, even if the data source is not linked to the user's dashboards.

Data source permissions enable you to restrict data source query permissions to specific **Users** and **Teams**. For more information about assigning data source permissions, refer to [Data source permissions]({{< relref "../../enterprise/datasource_permissions.md" >}}).

Fine-grained access control

Fine-grained access control provides you a way of granting, changing, and revoking user read and write access to Grafana resources, such as users, reports, and authentication.

For more information about fine-grained access control, refer to [Fine-grained access control]({{< relref "../../enterprise/access-control" >}}).

Learn more

Want to know more? Complete the Create users and teams tutorial to learn how to set up users and teams.