+++ title = "Fine-grained access control" description = "Grant, change, or revoke access to Grafana resources" keywords = ["grafana", "fine-grained-access-control", "roles", "permissions", "enterprise"] weight = 100 +++

Fine-grained access control

> ***Note:*** *Fine-grained access control is in beta, and you can expect changes in future releases.*

Fine-grained access control provides a standardized way of granting, changing, and revoking access when it comes to viewing and modifying Grafana resources, such as users and reports. Fine-grained access control works alongside the current Grafana permissions, and it allows you granular control of users' actions. For more information about Grafana permissions, refer to [About users and permissions]({{< relref "../../administration/manage-users-and-permissions/about-users-and-permissions.md" >}}).

To learn more about how fine-grained access control works, refer to [Roles]({{< relref "./roles.md" >}}) and [Permissions]({{< relref "./permissions.md" >}}). To use the fine-grained access control system, refer to [Fine-grained access control usage scenarios]({{< relref "./usage-scenarios.md" >}}).

Access management

Fine-grained access control considers a) *who* has an access (`identity`), and b) *what they can do* and on which *Grafana resource* (`role`).

You can grant, change, or revoke access to *users* (`identity`). When an authenticated user tries to access a Grafana resource, the authorization system checks the required fine-grained permissions for the resource and determines whether or not the action is allowed. Refer to [Fine-grained permissions]({{< relref "./permissions.md" >}}) for a complete list of available permissions.

Refer to [Assign roles]({{< relref "./roles.md#assign-roles" >}}) to learn about grant or revoke access to your users.

Resources with fine-grained permissions

Fine-grained access control is available for the following capabilities:

- [Use Explore mode]({{< relref "../../explore/_index.md" >}})
- [Manage users]({{< relref "../../administration/manage-users-and-permissions/manage-server-users/_index.md" >}})
- [Manage LDAP authentication]({{< relref "../../auth/ldap/_index.md" >}})
- [Manage data sources]({{< relref "../../datasources/_index.md" >}})
- [Manage data source permissions]({{< relref "../datasource_permissions.md" >}})
- [Manage a Grafana Enterprise license]({{< relref "../license/_index.md" >}})
- [Provision Grafana]({{< relref "../../administration/provisioning/_index.md" >}})
- [Manage reports]({{< relref "../reporting.md" >}})
- [View server information]({{< relref "../../administration/view-server/_index.md" >}})

To learn about specific endpoints where you can use fine-grained access control, refer to [Permissions]({{< relref "./permissions.md" >}}) and to the relevant [API]({{< relref "../../http_api/_index.md" >}}) documentation.

Enable fine-grained access control

Fine-grained access control is available behind the `accesscontrol` feature toggle in Grafana Enterprise 8.0+. You can enable it either in a [config file]({{< relref "../../administration/configuration.md#config-file-locations" >}}) or by

[configuring an environment variable]({{< relref "../../administration/configuration/#configure-with-environment-variables" >}}).

Enable in config file

In your [config file]({{< relref "../../administration/configuration.md#config-file-locations" >}}), add `accesscontrol` as a [feature_toggle]({{< relref "../../administration/configuration.md#feature_toggle" >}}).

```
[feature_toggles]
# enable features, separated by spaces
enable = accesscontrol
```

Enable with an environment variable

You can use `GF_FEATURE_TOGGLES_ENABLE = accesscontrol` environment variable to override the config file configuration and enable fine-grained access control.

Refer to [Configuring with environment variables]({{< relref "../../administration/configuration.md#configure-with-environment-variables" >}}) for more information.

Verify if enabled

You can verify if fine-grained access control is enabled or not by sending an HTTP request to the [Check endpoint]({{< relref "../../http_api/access_control.md#check-if-enabled" >}}).