

+++ title = "Datasource Permissions HTTP API " description = "Data Source Permissions API" keywords = ["grafana", "http", "documentation", "api", "datasource", "permission", "permissions", "acl", "enterprise"] aliases = ["/docs/grafana/latest/http\_api/datasourcepermissions/"] +++

# Data Source Permissions API

*The Data Source Permissions is only available in Grafana Enterprise. Read more about [Grafana Enterprise]({{< relref "../enterprise" >}}).*

*If you are running Grafana Enterprise and have [Fine-grained access control]({{< relref "../enterprise/access-control/\_index.md" >}}) enabled, for some endpoints you would need to have relevant permissions. Refer to specific resources to understand what permissions are required.*

This API can be used to enable, disable, list, add and remove permissions for a data source.

Permissions can be set for a user or a team. Permissions cannot be set for Admins - they always have access to everything.

The permission levels for the permission field:

- 1 = Query

## Enable permissions for a data source

POST /api/datasources/:id/enable-permissions

Enables permissions for the data source with the given `id`. No one except Org Admins will be able to query the data source until permissions have been added which permit certain users or teams to query the data source.

### Required permissions

See note in the [introduction]({{< ref "#data-source-permissions-api" >}}) for an explanation.

Action	Scope
datasources.permissions:write	datasources:* datasources:id:* datasources:id:1 (single data source)

### Examples

#### Example request:

```
POST /api/datasources/1/enable-permissions
Accept: application/json
Content-Type: application/json
Authorization: Bearer eyJrIjoiT0tTcG1pU1Y2RnVKZTFVaDFsNFZXdE9ZWmNrMkZYbk

{ }
```

#### Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 35

{"message":"Datasource permissions enabled"}
```

Status codes:

- **200** - Ok
- **400** - Permissions cannot be enabled, see response body for details
- **401** - Unauthorized
- **403** - Access denied
- **404** - Datasource not found

## Disable permissions for a data source

```
POST /api/datasources/:id/disable-permissions
```

Disables permissions for the data source with the given `id`. All existing permissions will be removed and anyone will be able to query the data source.

### Required permissions

See note in the [introduction]({{< ref "#data-source-permissions-api" >}}) for an explanation.

Action	Scope
datasources.permissions:write	datasources:* datasources:id:* datasources:id:1 (single data source)

### Examples

#### Example request:

```
POST /api/datasources/1/disable-permissions
Accept: application/json
Content-Type: application/json
Authorization: Bearer eyJrIjoiT0tTcG1pU1Y2RnVKZTFVaDFsNFZXdE9ZWmNrMkZYbk

{ }
```

#### Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 35

{"message":"Datasource permissions disabled"}
```

Status codes:

- **200** - Ok
- **400** - Permissions cannot be disabled, see response body for details
- **401** - Unauthorized
- **403** - Access denied
- **404** - Datasource not found

## Get permissions for a data source

```
GET /api/datasources/:id/permissions
```

Gets all existing permissions for the data source with the given `id`.

### Required permissions

See note in the [introduction]({{< ref "#data-source-permissions-api" >}}) for an explanation.

Action	Scope
<code>datasources.permissions:read</code>	<code>datasources:*</code> <code>datasources:id:*</code> <code>datasources:id:1</code> (single data source)

### Examples

#### Example request:

```
GET /api/datasources/1/permissions HTTP/1.1
Accept: application/json
Content-Type: application/json
Authorization: Bearer eyJrIjoit0tTcG1pU1Y2RnVKZTFVaDFsNFZXdeE9ZWmNrMkZYbk
```

#### Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 551

{
  "datasourceId": 1,
  "enabled": true,
  "permissions":
  [
    {
      "id": 1,
      "datasourceId": 1,
      "userId": 1,
      "userLogin": "user",
      "userEmail": "user@test.com",
      "userAvatarUrl": "/avatar/46d229b033af06a191ff2267bca9ae56",
      "permission": 1,
      "permissionName": "Query",
      "created": "2017-06-20T02:00:00+02:00",
```

```

      "updated": "2017-06-20T02:00:00+02:00",
    },
    {
      "id": 2,
      "datasourceId": 1,
      "teamId": 1,
      "team": "A Team",
      "teamAvatarUrl": "/avatar/46d229b033af06a191ff2267bca9ae56",
      "permission": 1,
      "permissionName": "Query",
      "created": "2017-06-20T02:00:00+02:00",
      "updated": "2017-06-20T02:00:00+02:00",
    }
  ]
}

```

Status codes:

- **200** - Ok
- **401** - Unauthorized
- **403** - Access denied
- **404** - Datasource not found

## Add permission for a data source

POST /api/datasources/:id/permissions

Adds a user permission for the data source with the given `id`.

### Required permissions

See note in the [introduction]({{< ref "#data-source-permissions-api" >}}) for an explanation.

Action	Scope
datasources.permissions.write	datasources:* datasources.id:* datasources.id:1 (single data source)

### Examples

#### Example request:

```

POST /api/datasources/1/permissions
Accept: application/json
Content-Type: application/json
Authorization: Bearer eyJrIjoiT0tTcG1pU1Y2RnVKZTFVaDFsNFZXde9ZWmNrMkZYbk

{
  "userId": 1,
  "permission": 1
}

```

**Example response:**

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 35

{"message":"Datasource permission added"}
```

Adds a team permission for the data source with the given `id` .

**Example request:**

```
POST /api/datasources/1/permissions
Accept: application/json
Content-Type: application/json
Authorization: Bearer eyJrIjoiT0tTcG1pU1Y2RnVKZTFVaDFsNFZXdE9ZWmNrMkZYbk

{
  "teamId": 1,
  "permission": 1
}
```

**Example response:**

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 35

{"message":"Datasource permission added"}
```

Status codes:

- **200** - Ok
- **400** - Permission cannot be added, see response body for details
- **401** - Unauthorized
- **403** - Access denied
- **404** - Datasource not found

**Remove permission for a data source**

`DELETE /api/datasources/:id/permissions/:permissionId`

Removes the permission with the given `permissionId` for the data source with the given `id` .

**Required permissions**

See note in the [introduction]({{< ref "#data-source-permissions-api" >}}) for an explanation.

Action	Scope
datasources.permissions:write	datasources:* datasources:id:*

	datasources:id:1 (single data source)
--	---------------------------------------

## Examples

### Example request:

```
DELETE /api/datasources/1/permissions/2
Accept: application/json
Content-Type: application/json
Authorization: Bearer eyJrIjoiT0tTcG1pU1Y2RnVKZTFVaDFsNFZXXde9ZWmNrMkZYbk
```

### Example response:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 35

{"message":"Datasource permission removed"}
```

### Status codes:

- **200** - Ok
- **401** - Unauthorized
- **403** - Access denied
- **404** - Datasource not found or permission not found