+++ title = "Okta OAuth2 authentication" description = "Grafana Okta OAuth Guide " keywords = ["grafana", "configuration", "documentation", "oauth"] weight = 1000 +++

Okta OAuth2 authentication

> *Only available in Grafana v7.0+*

The Okta authentication allows your Grafana users to log in by using an external Okta authorization server.

Create an Okta application

Before you can sign a user in, you need to create an Okta application from the Okta Developer Console.

1. Log in to the Okta portal.
2. Go to Admin and then select **Developer Console**.
3. Select **Applications**, then **Add Application**.
4. Pick **Web** as the platform.
5. Enter a name for your application (or leave the default value).
6. Add the **Base URI** of your application, such as https://grafana.example.com.
7. Enter values for the **Login redirect URI**. Use **Base URI** and append it with `/login/okta`, for example: https://grafana.example.com/login/okta.
8. Click **Done** to finish creating the Okta application.

Enable Okta OAuth in Grafana

1. Add the following to the [Grafana configuration file]({{< relref "../administration/configuration.md#config-file-locations" >}}):

```
[auth.okta]
name = Okta
icon = okta
enabled = true
allow_sign_up = true
client_id = some_id
client_secret = some_secret
scopes = openid profile email groups
auth_url = https://<tenant-id>.okta.com/oauth2/v1/authorize
token_url = https://<tenant-id>.okta.com/oauth2/v1/token
api_url = https://<tenant-id>.okta.com/oauth2/v1/userinfo
allowed_domains =
allowed_groups =
role_attribute_path =
```

Configure allowed groups and domains

To limit access to authenticated users that are members of one or more groups, set `allowed_groups` to a comma- or space-separated list of Okta groups.

```
allowed_groups = Developers, Admins
```

The `allowed_domains` option limits access to the users belonging to the specific domains. Domains should be separated by space or comma.

```
allowed_domains = mycompany.com mycompany.org
```

Map roles

Grafana can attempt to do role mapping through Okta OAuth. In order to achieve this, Grafana checks for the presence of a role using the JMESPath specified via the `role_attribute_path` configuration option.

Grafana uses JSON obtained from querying the `/userinfo` endpoint for the path lookup. The result after evaluating the `role_attribute_path` JMESPath expression needs to be a valid Grafana role, i.e. `Viewer`, `Editor` or `Admin`. Refer to [About users and permissions]({{< relref "../administration/manage-users-and-permissions/about-users-and-permissions.md" >}}) for more information about roles and permissions in Grafana.

Read about how to add custom claims to the user info in Okta. Also, check Generic OAuth page for [JMESPath examples]({{< relref "generic-oauth.md/#jmespath-examples" >}}).

Team Sync (Enterprise only)

Map your Okta groups to teams in Grafana so that your users will automatically be added to the correct teams.

Okta groups can be referenced by group name, like `Admins`.

[Learn more about Team Sync]({{< relref "../enterprise/team-sync.md" >}})