

```
+++ title = "Grafana Authentication" description = "Grafana OAuthentication
Guide" keywords = ["grafana", "configuration", "documentation", "oauth"]
weight = 100 +++
```

## Grafana Auth

Grafana of course has a built in user authentication system with password authentication enabled by default. You can disable authentication by enabling anonymous access. You can also hide login form and only allow login through an auth provider (listed above). There is also options for allowing self sign up.

### Login and short-lived tokens

The following applies when using Grafana's built in user authentication, LDAP (without Auth proxy) or OAuth integration.

Grafana are using short-lived tokens as a mechanism for verifying authenticated users. These short-lived tokens are rotated each `token_rotation_interval_minutes` for an active authenticated user.

An active authenticated user that gets its token rotated will extend the `login_maximum_inactive_lifetime_duration` time from "now" that Grafana will remember the user. This means that a user can close its browser and come back before `now + login_maximum_inactive_lifetime_duration` and still be authenticated. This is true as long as the time since user login is less than `login_maximum_lifetime_duration`.

**Remote logout** You can logout from other devices by removing login sessions from the bottom of your profile page. If you are a Grafana admin user you can also do the same for any user from the Server Admin / Edit User view.

## Settings

Example:

```
[auth]
```

```
# Login cookie name
```

```
login_cookie_name = grafana_session
```

```
# The lifetime (days) an authenticated user can be inactive before being required to login
```

```
login_maximum_inactive_lifetime_duration = 7d
```

```
# The maximum lifetime (days) an authenticated user can be logged in since login time before
```

```
login_maximum_lifetime_duration = 30d
```

```
# How often should auth tokens be rotated for authenticated users when being active. The de
```

```
token_rotation_interval_minutes = 10
```

```
# The maximum lifetime (seconds) an api key can be used. If it is set all the api keys shou  
api_key_max_seconds_to_live = -1
```

### Anonymous authentication

You can make Grafana accessible without any login required by enabling anonymous access in the configuration file. For more information, refer to [Implications of allowing anonymous access to dashboards]({{< relref “../administration/security.md” >}}).

Example:

```
[auth.anonymous]  
enabled = true
```

```
# Organization name that should be used for unauthenticated users  
org_name = Main Org.
```

```
# Role for unauthenticated users, other valid values are `Editor` and `Admin`  
org_role = Viewer
```

```
# Hide the Grafana version text from the footer and help tooltip for unauthenticated users  
hide_version = true
```

If you change your organization name in the Grafana UI this setting needs to be updated to match the new name.

### Basic authentication

Basic auth is enabled by default and works with the built in Grafana user password authentication system and LDAP authentication integration.

To disable basic auth:

```
[auth.basic]  
enabled = false
```

### Disable login form

You can hide the Grafana login form using the below configuration settings.

```
[auth]  
disable_login_form = true
```

### Automatic OAuth login

Set to true to attempt login with OAuth automatically, skipping the login screen. This setting is ignored if multiple OAuth providers are configured. Defaults to false.

```
[auth]
oauth_auto_login = true
```

### **Hide sign-out menu**

Set the option detailed below to true to hide sign-out menu link. Useful if you use an auth proxy or JWT authentication.

```
[auth]
disable_signout_menu = true
```

### **URL redirect after signing out**

URL to redirect the user to after signing out from Grafana. This can for example be used to enable signout from oauth provider.

```
[auth]
signout_redirect_url =
```