+++ title = "Overview" description = "Overview for auth" weight = 1 +++

User Authentication Overview

Grafana provides many ways to authenticate users. Some authentication integrations also enable syncing user permissions and org memberships.

Here is a table showing all supported authentication providers and the features available for them. [Team sync]({{< relref "../enterprise/team-sync.md" >}}) and [active sync]({{< relref "../enterprise/enhanced_ldap.md#active-ldap-synchronization" >}}) are only available in Grafana Enterprise.

Provider	Support	Role mapping	Team sync *(Enterprise only)*	Active sync *(Enterprise only)*
[Auth Proxy]({{< relref "auth-proxy.md" >}})	v2.1+	-	v6.3+	-
[Azure AD OAuth]({{< relref "azuread.md" >}})	v6.7+	v6.7+	v6.7+	-
[Generic OAuth]({{< relref "generic-oauth.md" >}})	v4.0+	v6.5+	-	-
[GitHub OAuth]({{< relref "github.md" >}})	v2.0+	-	v6.3+	-
[GitLab OAuth]({{< relref "gitlab.md" >}})	v5.3+	-	v6.4+	-
[Google OAuth]({{< relref "google.md" >}})	v2.0+	-	-	-
[JWT]({{< relref "jwt.md" >}})	v8.0+	-	-	-
[LDAP]({{< relref "ldap.md" >}})	v2.1+	v2.1+	v5.3+	v6.3+
[Okta OAuth]({{< relref "okta.md" >}})	v7.0+	v7.0+	v7.0+	-
[SAML]({{< relref "../enterprise/saml.md" >}}) (Enterprise only)	v6.3+	v7.0+	v7.0+	-

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 are 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 it 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 being 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 maximum lifetime (duration) an authenticated user can be inactive before being
required to login at next visit. Default is 7 days (7d). This setting should be
expressed as a duration, e.g. 5m (minutes), 6h (hours), 10d (days), 2w (weeks), 1M
(month). The lifetime resets at each successful token rotation
(token_rotation_interval_minutes).
login_maximum_inactive_lifetime_duration =


# The maximum lifetime (duration) an authenticated user can be logged in since login
time before being required to login. Default is 30 days (30d). This setting should
be expressed as a duration, e.g. 5m (minutes), 6h (hours), 10d (days), 2w (weeks),
1M (month).
login_maximum_lifetime_duration =

# How often should auth tokens be rotated for authenticated users when being active.
The default is each 10 minutes.
token_rotation_interval_minutes = 10

# The maximum lifetime (seconds) an API key can be used. If it is set all the API
keys should have limited lifetime that is lower than this value.
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.

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
```

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
```

Avoid automatic OAuth login

To sign in with a username and password and avoid automatic OAuth login, add the `disableAutoLogin` parameter to your login URL. For example: `grafana.example.com/login?disableAutoLogin` or `grafana.example.com/login?disableAutoLogin=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 =
```