User Authentication Overview

 › [Administration](https://grafana.com/docs/grafana/latest/administration/) › [Authentication](https://grafana.com/docs/grafana/latest/auth/) › Overview

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

Grafana提供了多种方法去认证用户。一些集成的认证也可以同步用户权限和组织关系。

Here is a table showing all supported authentication providers and the features available for them. [Team sync](https://grafana.com/docs/grafana/latest/enterprise/team-sync/) and [active sync](https://grafana.com/docs/grafana/latest/enterprise/enhanced_ldap/#active-ldap-synchronization) are only available in Grafana Enterprise.

这里有一个表格，显示了所有受支持的认证供应者和他们可用的功能。团队同步和活跃同步只在Grafana企业版中可用。

| Provider | Support | Role mapping | Team sync *(Enterprise only)* | Active sync *(Enterprise only)* |
| --- | --- | --- | --- | --- |
| [Auth Proxy](https://grafana.com/docs/grafana/latest/auth/auth-proxy/) | v2.1+ | - | v6.3+ | - |
| [Azure AD OAuth](https://grafana.com/docs/grafana/latest/auth/azuread/) | v6.7+ | v6.7+ | v6.7+ | - |
| [Generic OAuth](https://grafana.com/docs/grafana/latest/auth/generic-oauth/) | v4.0+ | v6.5+ | - | - |
| [GitHub OAuth](https://grafana.com/docs/grafana/latest/auth/github/) | v2.0+ | - | v6.3+ | - |
| [GitLab OAuth](https://grafana.com/docs/grafana/latest/auth/gitlab/) | v5.3+ | - | v6.4+ | - |
| [Google OAuth](https://grafana.com/docs/grafana/latest/auth/google/) | v2.0+ | - | - | - |
| [LDAP](https://grafana.com/docs/grafana/latest/auth/ldap/) | v2.1+ | v2.1+ | v5.3+ | v6.3+ |
| [Okta OAuth](https://grafana.com/docs/grafana/latest/auth/okta/) | v7.0+ | v7.0+ | v7.0+ | - |
| [SAML](https://grafana.com/docs/grafana/latest/enterprise/saml/) (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 is also options for allowing self sign up.

Grafana内置的带密码的用户认证系统默认是启用的。你可以通过启用匿名访问来禁用认证。你也可以隐藏登录表单，只允许通过认证供应者（上面表格列出来的）登录。也可以选择允许自身登录。

Login and short-lived tokens

登录和短期令牌

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

当使用Grafana内置的用户认证，LDAP（没有认证代理）或OAuth集成时，以下方法可用。

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.

Grafana使用短期令牌作为机制来验证已认证的用户。对于活动的已认证的用户，这些短期的令牌会在token\_rotation\_interval\_minutes中轮调。

An active authenticated user that gets it token rotated will extend the login\_maximum\_inactive\_lifetime\_days 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\_days and still being authenticated. This is true as long as the time since user login is less than login\_maximum\_lifetime\_days.

一个活跃的得到它令牌轮调的已认证用户，会延长从login\_maximum\_inactive\_lifetime\_days到现在的时间，使得Grafana会记住用户。这样就意味着用户可以关掉浏览器，然后在now + login\_maximum\_inactive\_lifetime\_days时间前回来，用户还是被认证的。这代表着用户的登录最长时间小于login\_maximum\_lifetime\_days。

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.

你可以从其他设备通过移除配置页面底部的登录session进行登出。如果你是Grafana的管理员用户，你可以对服务器的管理员/编辑者做同样的事情。

Settings

Example:

[auth]

# Login cookie name

# 登录cookie名字

login\_cookie\_name = grafana\_session

# The lifetime (days) an authenticated user can be inactive before being required to login at next visit. Default is 7 days.

# 用户在下一次要求再次登录之前可以不活跃的生存期。默认为7天。

login\_maximum\_inactive\_lifetime\_days = 7

# The maximum lifetime (days) an authenticated user can be logged in since login time before being required to login. Default is 30 days.

# **用户在被要求再次登录前可保留登录的最大生存期。默认为30天。**

login\_maximum\_lifetime\_days = 30

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

# 当处于活跃状态时，已认证的用户多长时间被要求进行一次认证令牌的轮调。默认为每10分钟一次。

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密钥可以使用的最大时间长度。如果设置了这个值，那么所有API密钥的生存期都要小于这个值。-1表示不限制。

api\_key\_max\_seconds\_to\_live = -1

Bash

Anonymous authentication

You can make Grafana accessible without any login required by enabling anonymous access in the configuration file.

你也可以在配置文件中启用匿名访问，不进行任何登录来访问Grafana。

Example:

[auth.anonymous]

enabled = true

# Organization name that should be used for unauthenticated users

# 未认证用户应该使用的组织名

org\_name = Main Org.

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

# 对于未认证用户设置的角色，其他有效值为Editor和Admin。

org\_role = Viewer

Bash

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

如果在Grafana界面中你更改了你的组织名，那么这个设置就需要去更新为新修改的组织名。

Basic authentication

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

默认启用基础的认证，使用Grafana内置的用户密码认证系统，和LDAP认证的集成。

To disable basic auth:

[auth.basic]

enabled = false

Bash

Disable login form

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

你也可以使用下面的配置设置来隐藏Grafana登录表单

[auth]

disable\_login\_form = true

Bash

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.

设置为true可以自动跳过登录界面，并使用OAuth来尝试登录。如果多个OAuth供应者被配置，那么这个设置会被忽略。默认值为false。

[auth]

oauth\_auto\_login = true

Bash

Hide sign-out menu

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

设置这个选项为true可以隐藏登出菜单的链接。如果你使用认证代理的话是很有用的。

[auth]

disable\_signout\_menu = true

Bash

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.

从Grafana登出后用户被重定向到的URL。这个可以被作为例子，用来启用OAuth供应者的登出。

[auth]

signout\_redirect\_url =