Azure AD OAuth2 authentication

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

Only available in Grafana v6.7+

The Azure AD authentication provides the possibility to use an Azure Active Directory tenant as an identity provider for Grafana. By using Azure AD Application Roles it is also possible to assign Users and Groups to Grafana roles from the Azure Portal.

Azure AD认证提供了使用Azure动态目录租户作为Grafana身份提供者的可能性。通过使用Azure AD应用规则，它也有可能从Azure Portal分配用户和组到Grafana规则。

Create the Azure AD application

创建Azure Ad应用

To enable the Azure AD OAuth2 you must register your application with Azure AD.

为了启用Azure AD OAuth2，你必须使用Azure AD去注册你的应用。

1. Log in to [Azure Portal](https://portal.azure.com/) and click **Azure Active Directory** in the side menu. If you have access to more than one tenant, select your account in the upper right. Set your session to the Azure AD tenant you wish to use.

登录到Azure Portal，在侧边菜单中点击Azure Active Directory。如果你有权限使用超过一个租户的时候，在右上方选择你的账号。设置你的seesion到你希望使用的Azure AD租户。

1. Under **Manage** in the side menu, click **App Registrations** and then **New Registration**. Provide a fitting name.

在侧边菜单Manage的下面，点击App Registration，接着点New Registration。提供一个合适的名字。

1. Under **Redirect URI**, select **Web** as the app type.

在Redirect URI下面，选择Web作为应用类型。

1. Add the redirect URL https://<grafana domain>/login/azuread, then click **Register**.

添加重定向URL https://<grafana domain>/login/azuread，然后点击Register。

1. The app’s **Overview** page is displayed. Note the **Application ID**, this is the OAuth client id.

应用的Overview页面显示了。注意Application ID，这是OAuth的客户端ID。

1. Click **Endpoints** from the top menu.

从顶部菜单点击Endpoints。

* + Note the **OAuth 2.0 authorization endpoint (v2)**, this is the auth URL.

注意OAuth 2.0 authorization endpoint(v2)，这是认证的URL。

* + Note the **OAuth 2.0 token endpoint (v2)**, this is the token URL.

注意OAuth 2.0 token endpoint(v)2,这是令牌的URL。

1. Click **Certificates & secrets** and add a new entry under Client secrets.

点击Certificates & secrets，然后在客户端机密下添加新的条目。

* + Description: Grafana OAuth

描述：Grafana OAuth

* + Expires: Never

过期时间：从不

1. Click **Add**, then copy the key value. This is the OAuth client secret.

点击Add，然后复制密钥的值。这是OAuth客户端的机密。

1. Click **Manifest**.

点击Manifest

* + Add definitions for the required Application Roles for Grafana (Viewer, Editor, Admin). Without this configuration, all users will be assigned the Viewer role.

为Grafana所需的应用角色添加定义（Viewer，Editor，Admin）。没有这个配置，所有的用户都会分配为Viewer角色。

* + Every role requires a unique id. On Linux, this can be created with uuidgen. For example:

每个角色都要求一个唯一的ID。在Linux平台，可能通过uuidgen来实现。例子：

"appRoles": [

{

"allowedMemberTypes": [

"User"

],

"description": "Grafana admin Users",

"displayName": "Grafana Admin",

"id": "SOME\_UNIQUE\_ID",

"isEnabled": true,

"lang": null,

"origin": "Application",

"value": "Admin"

},

{

"allowedMemberTypes": [

"User"

],

"description": "Grafana read only Users",

"displayName": "Grafana Viewer",

"id": "SOME\_UNIQUE\_ID",

"isEnabled": true,

"lang": null,

"origin": "Application",

"value": "Viewer"

},

{

"allowedMemberTypes": [

"User"

],

"description": "Grafana Editor Users",

"displayName": "Grafana Editor",

"id": "SOME\_UNIQUE\_ID",

"isEnabled": true,

"lang": null,

"origin": "Application",

"value": "Editor"

}

],

JSON

1. Go to **Azure Active Directory** and then to **Enterprise Applications**. Search for your application and click on it.

到Azure Active Directory然后到Enterprise Applications。查询你的应用然后点击它。

1. Click on **Users and Groups** and add Users/Groups to the Grafana roles by using **Add User**.

点击Users and Groups，然后通过Add User添加用户/组到Grafana角色。

Enable Azure AD OAuth in Grafana

1. Add the following to the [Grafana configuration file](https://grafana.com/docs/grafana/latest/administration/configuration/#config-file-locations):

添加以下的内容到Grafana配置文件：

[auth.azuread]

name = Azure AD

enabled = true

allow\_sign\_up = true

client\_id = APPLICATION\_ID

client\_secret = CLIENT\_SECRET

scopes = openid email profile

auth\_url = https://login.microsoftonline.com/TENANT\_ID/oauth2/v2.0/authorize

token\_url = https://login.microsoftonline.com/TENANT\_ID/oauth2/v2.0/token

allowed\_domains =

allowed\_groups =

Ini

Note: Ensure that the [root\_url](https://grafana.com/docs/grafana/latest/administration/configuration/" \l "root-url) in Grafana is set in your Azure Application Reply URLs (App -> Settings -> Reply URLs)

注意：确保在你的Azure应用的Reply URL中设置的是Grafana的root\_url（App -> Settings -> Reply URLs）

Configure allowed groups and domains

配置受允许的组和域名

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 group Object Ids. Object Id for a specific group can be found on the Azure portal: go to Azure Active Directory -> Groups. For instance, if you want to only give access to members of the group example which has Id 8bab1c86-8fba-33e5-2089-1d1c80ec267d, set

allowed\_groups = 8bab1c86-8fba-33e5-2089-1d1c80ec267d

Ini

为了限制已授权的，有一个或多个组的用户，设置allowed\_groups为以逗号或空格为分隔的组Object ID的列表。可以在Azure protal中找到指定组的Object ID：到Azure Active Directory -> Groups。例如，如果你想要只给id为8bab1c86-8fba-33e5-2089-1d1c80ec267d的组example成员权限，那么你要这样设置allowed\_groups = 8bab1c86-8fba-33e5-2089-1d1c80ec267d

You’ll need to ensure that you’ve [enabled group attributes](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-group-claims#configure-the-azure-ad-application-registration-for-group-attributes) in your Azure AD Application Registration manifest file (Azure Portal -> Azure Active Directory -> Application Registrations -> Select Application -> Manifest)

你需要去确保你已经在Azure AD应用注意manifest文件中启用了group属性(Azure Portal -> Azure Active Directory -> Application Registrations -> Select Application -> Manifest)

"groupMembershipClaims": "ApplicationGroup"

JSON

The allowed\_domains option limits access to the users belonging to the specific domains. Domains should be separated by space or comma.

allowed\_domains选项限制了属于指定域名的用户的权限。域名应该使用逗号或空格分隔。

allowed\_domains = mycompany.com mycompany.org

Ini

Team Sync (Enterprise only)

团队同步（仅限企业版）

Only available in Grafana Enterprise v6.7+

只在Grafana企业版6.7版本后可用

With Team Sync you can map your Azure AD groups to teams in Grafana so that your users will automatically be added to the correct teams.

通过团队同步，你可以映射你的Azure AD组到Grafana的团队中，这样你的用户就可以自动被添加到正确的团队中。

Azure AD groups can be referenced by group Object Id, like 8bab1c86-8fba-33e5-2089-1d1c80ec267d.

Azure AD组可以被group Object ID引用，像8bab1c86-8fba-33e5-2089-1d1c80ec267d.

[Learn more about Team Sync](https://grafana.com/docs/grafana/latest/auth/team-sync/)