+++ title = “Azure AD OAuth2 authentication” description = “Grafana Azure AD OAuth Guide” keywords = [“grafana”, “configuration”, “documentation”, “oauth”] weight = 700 +++

Azure AD OAuth2 authentication

The Azure AD authentication allows you to use an Azure Active Directory tenant as an identity provider for Grafana. You can use Azure AD Application Roles to assign users and groups to Grafana roles from the Azure Portal. This topic has the following sections:

Create the Azure AD application

To enable the Azure AD OAuth2, register your application with Azure AD.

1. Log in to Azure Portal, then click **Azure Active Directory** in the side menu.
2. 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.
3. Under **Manage** in the side menu, click **App Registrations** > **New Registration**. Enter a descriptive name.
4. Under **Redirect URI**, select the app type **Web**.
5. Add the following redirect URLs `https://<grafana domain>/login/azuread` and `https://<grafana domain>` then click **Register**. The app's **Overview** page opens.
6. Note the **Application ID**. This is the OAuth client ID.
7. Click **Endpoints** from the top menu.
   - Note the **OAuth 2.0 authorization endpoint (v2)** URL. This is the authorization URL.
   - Note the **OAuth 2.0 token endpoint (v2)**. This is the token URL.
8. Click **Certificates & secrets**, then add a new entry under **Client secrets** with the following configuration.
   - Description: Grafana OAuth
   - Expires: Never

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

10. Click **Manifest**, then define the required Application Role values for Grafana: Viewer, Editor, or Admin. If not defined, all users will have the Viewer role. Every role requires a unique ID which you can generate on Linux with `uuidgen`, and on Windows through Microsoft PowerShell with `New-Guid`.

11. Include the unique ID in the configuration file:

```
"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"
        }
```

```
    ],
```

12. Go to **Azure Active Directory** and then to **Enterprise Applications**. Search for your application and click on it.
13. Click on **Users and Groups** and add Users/Groups to the Grafana roles by using **Add User**.

Enable Azure AD OAuth in Grafana

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

```
[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 =
role_attribute_strict = false
```

You can also use these environment variables to configure **client_id** and **client_secret**:

```
GF_AUTH_AZUREAD_CLIENT_ID
GF_AUTH_AZUREAD_CLIENT_SECRET
```

Note: Verify that the Grafana [root_url]({{< relref "../administration/configuration/#root-url" >}}) is set in your Azure Application Redirect URLs.

Configure allowed groups

To limit access to authenticated users who are members of one or more groups, set `allowed_groups` to a comma- or space-separated list of group object IDs. You can find object IDs for a specific group on the Azure portal:

1. Go to **Azure Active Directory -> Groups**. If you want to only give access to members of the group `example` with an ID of `8bab1c86-8fba-33e5-2089-1d1c80ec267d`, then set the following:

   ```
   allowed_groups = 8bab1c86-8fba-33e5-2089-1d1c80ec267d
   ```

2. Verify that group attributes is enabled in your Azure AD Application Registration manifest file by navigating to **Azure Portal** > **Azure Active Directory** > **Application Registrations** > **Select Application** -> **Manifest**, and set the following:

```
"groupMembershipClaims": "ApplicationGroup, SecurityGroup"
```

Configure allowed domains

The `allowed_domains` option limits access to users who belong to specific domains. Separate domains with space or comma. For example,

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

Team Sync (Enterprise only)

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.

You can reference Azure AD groups by group object ID, like `8bab1c86-8fba-33e5-2089-1d1c80ec267d`.

To learn more, refer to the [Team Sync]({{< relref “team-sync.md” >}}) documentation.