Аутенификация OpenID (Azure AD)

# Общая информация

Аутенификация **OpenID** включается в файле **Web.config**  в разделе **<appSettings>**. Добавьте туда ключ **openIdAuthentication**. Значением этого ключа должна быть json-строка с необходимыми параметрами. Например:

<appSettings>

<add key="openIdAuthentication" value="{clientId:'clientId',   
 aadInstance:'https://login.microsoftonline.com/', domain:'domain',   
 tenantId:'tenantId', redirectUri:'http://localhost/'}"/>

…

</appSettings>

Нам понадобятся следующие параметры:

* **tenantId**  - идентификатор тенанта в подписке Azure или MS 365;
* **clientId** – идентификатор приложения;
* **aadInstance** – URL экземпляра для входа. Обычно: <https://login.microsoftonline.com/>’;
* **domain**  - первичный домен, к которому подключен экземпляр;
* **redirectUri** – URL, куда будет переадресован залогиненый пользователь. Может быть и localhost;

Параметры **tenantId**, **domain** и **aadInstance** – будут всегда одинаковыми для конкретной подписки.

clientId – идентификатор конкретного приложения. Разумеется его надо зарегистрировать в AAD.

Обратите внимание, все URL задаются со слешем в конце строки.

# Где взять параметры

Открываем **Microsoft 365 admin center**, нажимаем **Show All** и переходим на **Azure Active Directory**.

Выбираем **Azure Active Directory | Overview**. На странице будут показаны нужные значения:

* **Tenant ID** – это наш **tenantId**
* **Primary domain** – это наш **domain**.

Теперь надо зарегистрировать приложение.

Переходим в раздел **App registrations** и нажимаем **New registration**.

* Вводим имя приложения (Имя произвольное. Показывается только внутри админки Azure)
* Выбираем типы поддерживаемых учеток. В подавляющем большинстве случаев это будет **Accounts in this organizational directory only**.
* Нужно будет зарегистрировать все **Redirect URI** для перехода после аутенификации. Другими словами, все значения, которые указываются в файле **web.config** приложения должны быть перечислены в **Redirect URI** (в дальнейшем это можно настраивать без пересоздания приложения). Обратите внимание, все URL задаются со слешем в конце строки

После того, как приложение будет создано, откроется страница его свойств. Нас интересует только одно значение: **Application (client) ID**. Это и будет наш **clientId**.

Теперь нужно зайти на закладку **Authentication** и разрешить **ID tokens** в разделе **Implicit grant and hybrid flows.**

На этой же вкладке можно добавлять/удалять **Redirect URI**. Обратите внимание, все URL задаются со слешем в конце строки.