如何创建一个使用Azure AD调用web API的多租户SaaS web应用程序

这篇文章主要讲述如何创建一个可以通过Azure AD做用户sign up/sign in的多租户web本地应用程序。

关于使用多租户应用程序模式将 Azure Active Directory (AD) 用户登录的更多信息，可以参考链接：

<https://www.azure.cn/documentation/articles/active-directory-devhowto-multi-tenant-overview/>

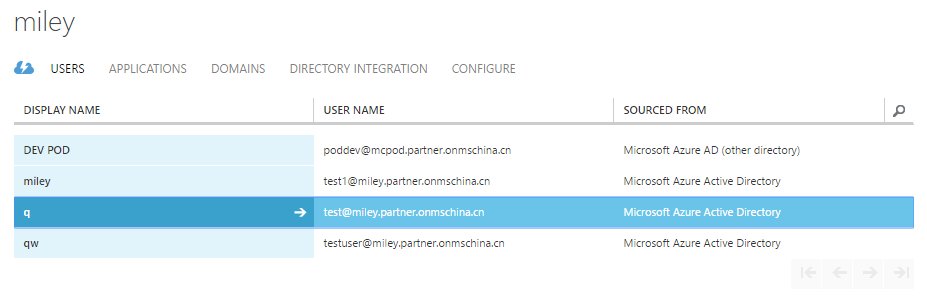
**准备工作：**

* Visual Studio 2013/2015/2017
* Azure Active Directory Tenants
* AD租户中的user账户

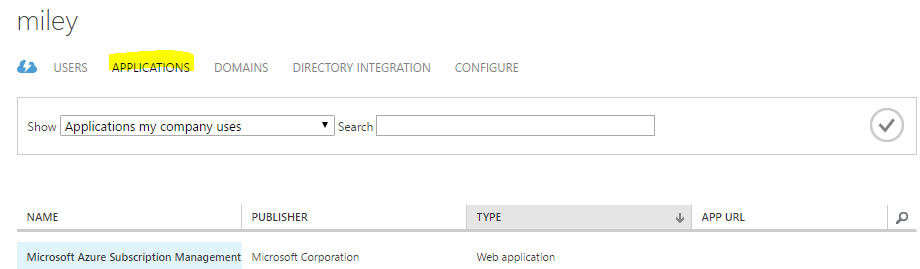
**创建应用的方法：**

* 管理门户部分

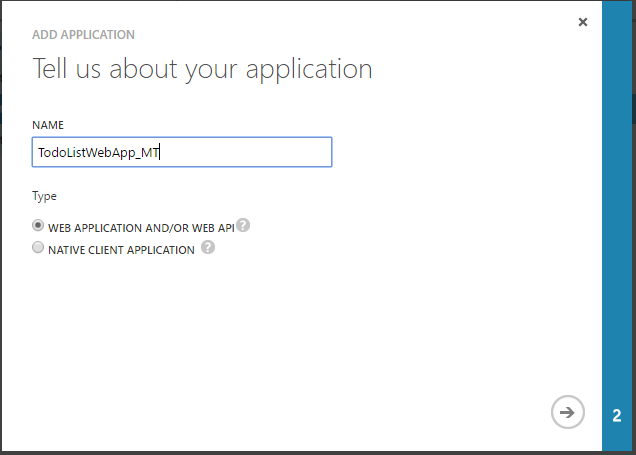
1. 登录azure 管理门户，在Azure Active Directory下创建一个Azure AD tenant及User。



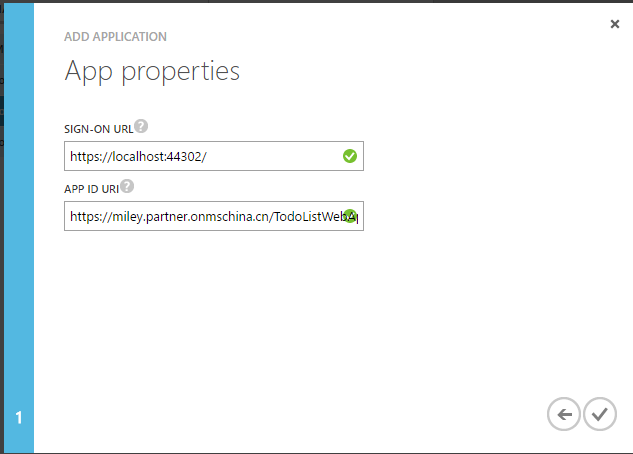
1. 使用Azure AD tenant注册应用。
2. 登录[管理门户](https://portal.azure.cn/)。
3. 找到刚才注册的Azure AD tenant，选择applications.



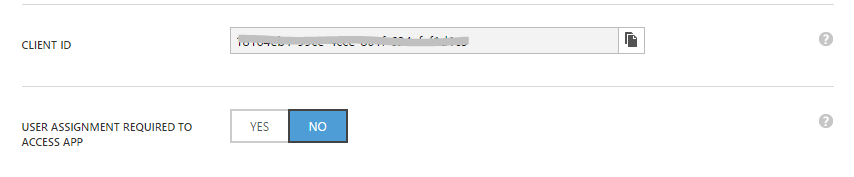
1. 同一页面上，点击下方的add注册一个应用，并为该应用起一个有效的名称如'TodoListWebApp\_MT'，同时在type里选择'Web Application and/or Web API'作为应用的类型，点击下一步。



1. 输入sign-on URL，可以输入默认值<https://localhost:44302/>；输入App ID URL，例如https://<your\_tenant\_domain>/TodoListWebApp\_MT,将对应的<your\_tenant\_domain>部分用自己的AD tenant的domain名称代替。最后点击complete创建application。



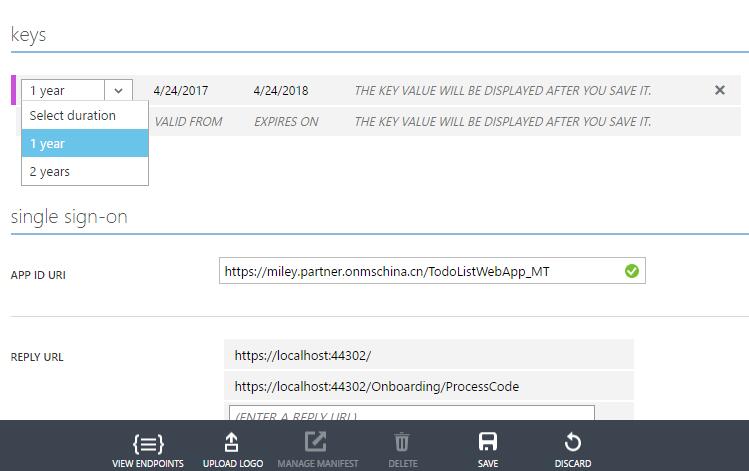
1. 创建完成后找到你刚才创建的应用，选择configure找到CLIENT ID，将其复制并保存在安全的位置，稍后将会在Visual Studio中配置该值。



1. 为你的Azure AD tenant 创建你的应用程序密钥。

点击刚才第二步中创建好的APP，选择configure，找到keys选项，为该App创建有效期为1年或者两年的密钥，点击下方的save来创建密钥。

注意：当你保存此页面时，将显示密钥值，将其复制并保存在安全的位置，稍后将会在Visual Studio中配置该值，另外此键值不会再次显示，所以创建完成后尽快保存。

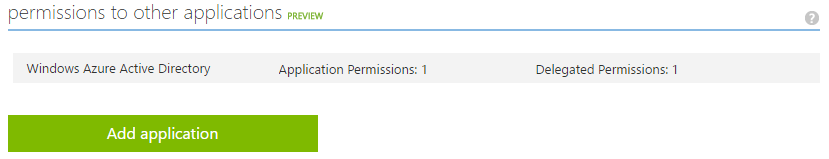


1. 同样在configure tab下，将你的应用配置为多租户应用程序并点击save保存。

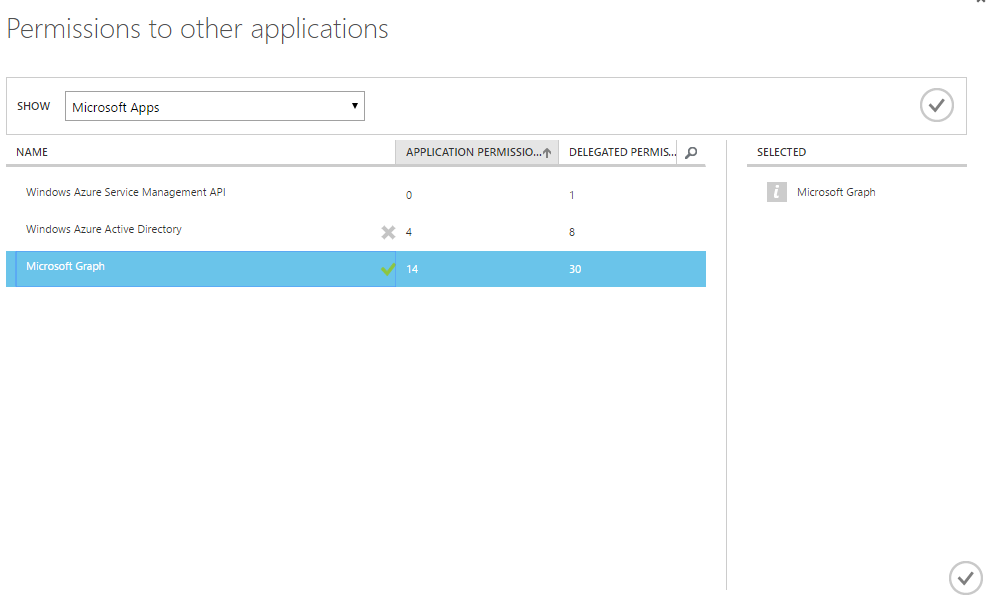
需要注意的是，在将某个应用程序设为多租户之前，Azure AD 要求该应用程序的应用 ID URI 全局唯一。应用 ID URI 是在协议消息中标识应用程序的方式之一，就单租户应用而言，应用 ID URI 在该租户中保持唯一便已足够。但是就多租户应用程序而言，该 URI 必须全局唯一，以便 Azure AD 能够在所有租户中找到该应用程序。



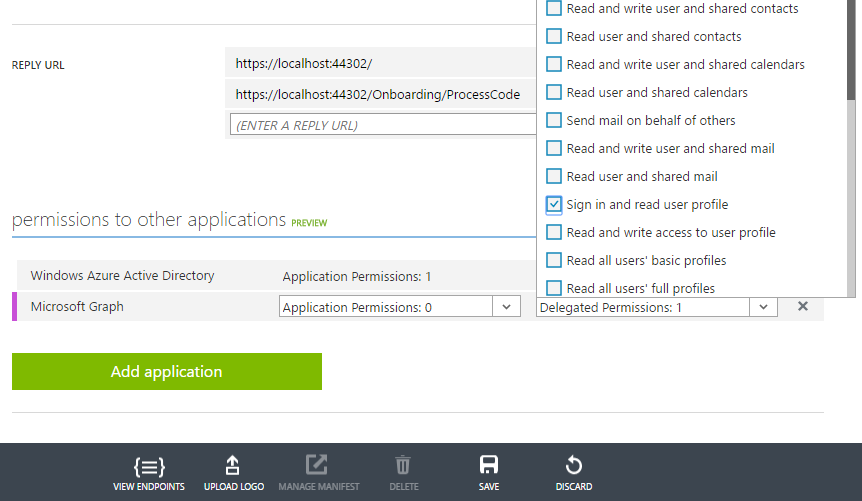
1. 为你的应用配置权限。
2. 在configure最下方找到permissions to other applications，点击Add application.



1. 选择添加Microsoft graph权限，点击complete.



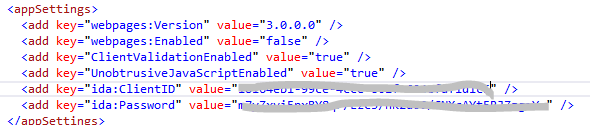
1. 找到刚才添加的Microsoft Graph权限，勾选'Sign in and read user profile'权限并保存。

这将允许你的应用程序接收委托的权限，以便为给定的用户帐户验证和读取用户配置文件数据。

到目前为止，在azure管理门户上做的配置工作已经全部完成，接下来，你需要通过在Visual studio中运行示例应用代码来体验多租户sign up和sign in.

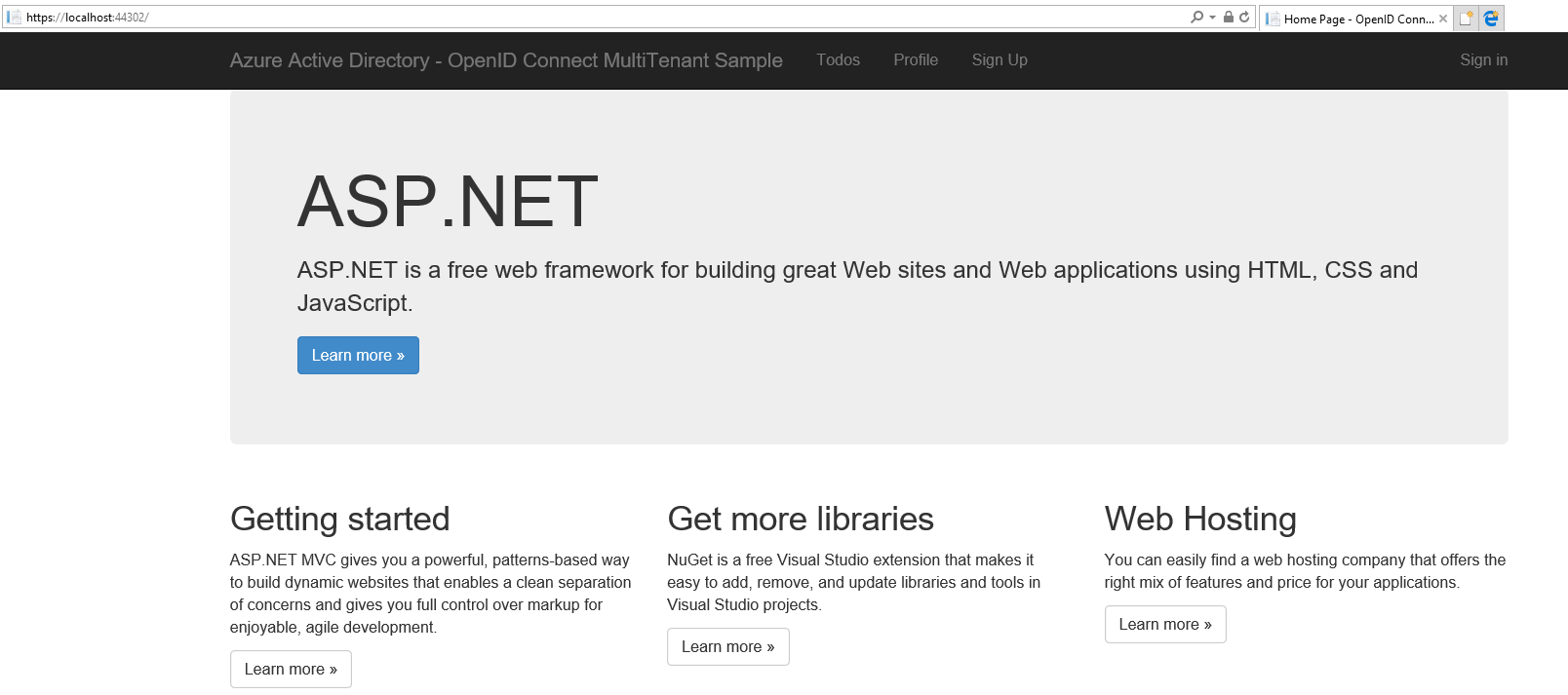
* 运行示例代码：

1. 从[这里](https://mileytest.blob.core.chinacloudapi.cn/videofile/active-directory.rar)下载示例代码。
2. 在Visual Studio中打开示例应用项目。
3. 打开web.config文件。
4. 将ida:Password的值用刚才创建应用密钥时保存的值代替。
5. 将ida:Password的值用刚才创建应用时生成的CLIENT ID代替。



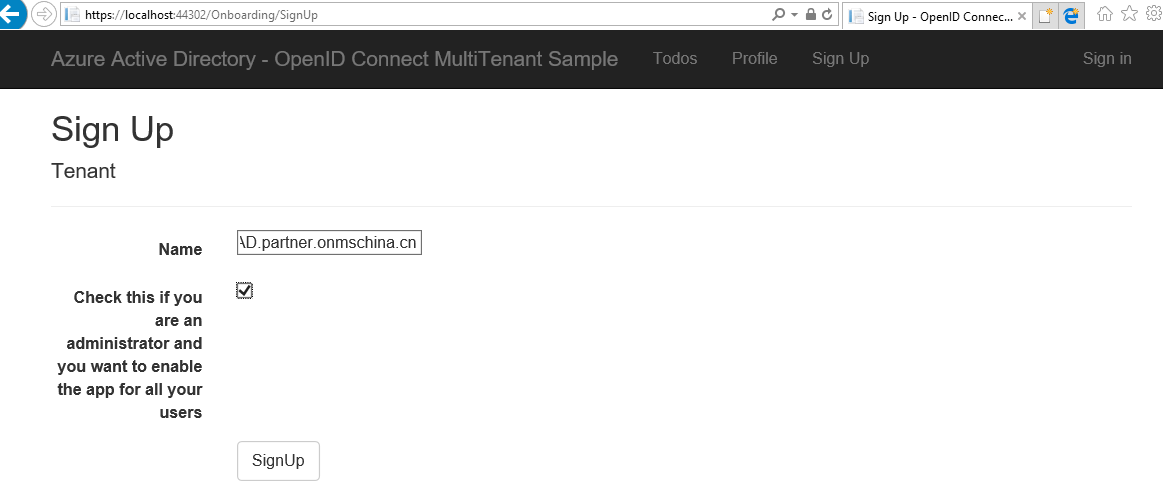
* 测试结果

1. 运行该应用程序，会得到如下的界面：

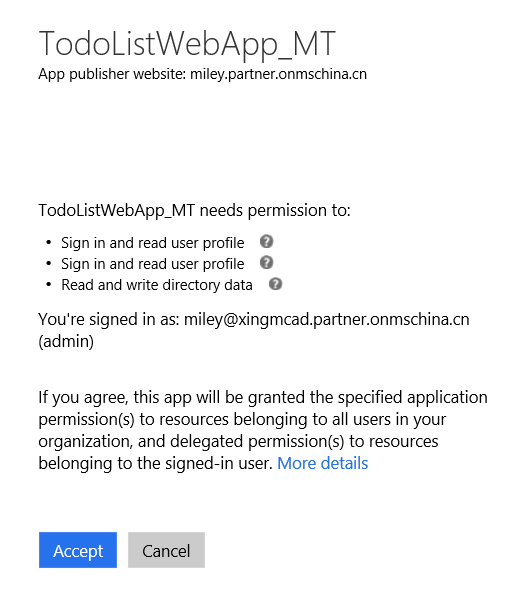


1. Sign up:

点击sign up，你可以选择是否要遵循“管理员同意”模式或“普通用户同意”模式。



然后您将被跳转到Azure AD登录界面，用你想要登录的用户名和密码登录，如果你用其他tenant（同一订阅非该应用注册的tenant）下的用户登录，将会有同意页面出现，点击accept会有提示信息提示登录成功。



1. Sign in

一旦sign up成功，就可以用刚才的用户名信息点击sign in登录到应用中。

