



Microsoft Azure – Azure AD

Milan Pekardy

pekardy@dcs.uni-pannon.hu



Azure Active Directory

- You automatically have one Azure AD tenant for your Azure account
- You can add additional directories if necessary (eg. development, testing, etc.)
- The portal has full support for creating, deleting, and managing users within this environment

The screenshot displays the Azure Active Directory (Azure AD) management portal. At the top, there are links for 'Switch directory' and 'Delete directory'. Below this, the tenant information is shown: 'pekmlfreemail.onmicrosoft.com' and 'alapértelmezett címtár' (Azure AD Free). The 'Sign-ins' section indicates that to view sign-in data, the organization needs Azure AD Premium P1 or P2, with a link to 'Start a free trial'. The 'What's new in Azure AD' section provides updates on release notes and blog posts, mentioning 17 entries since January 15, 2018, and a link to 'View archive'. A list of services is shown with checkboxes: 'All services' (checked, 17), 'Directory' (3), 'Monitoring & Reporting' (2), 'SSO' (3), 'User Authentication' (1), 'Platform' (3), 'Identity Security & Prote...' (2), 'Governance' (1), '3rd Party Integration' (1), and 'Identity Lifecycle Manage...' (1). A 'Plan for change' button is visible. The 'Your role' section shows the user as 'Global administrator' with a 'More info >' link. The 'Find' section has a dropdown menu set to 'Users' and a search box. The 'Azure AD Connect sync' section shows the status as 'Not enabled' and 'Last sync' as 'Sync has never run'. The 'Create' section lists options: 'User', 'Guest user', 'Group', 'Enterprise application', and 'App registration'. The 'Other capabilities' section lists 'Identity Protection', 'Privileged Identity Management', 'Azure AD Domain Services', 'Access reviews', and 'Tenant restrictions'. At the bottom, there are links for 'Getting started with Azure AD >' and 'Create a directory >'. A 'New feature' section highlights 'Sovereign Clouds - Monitoring & Reporting' and 'Availability of sign-ins and audit reports in Microsoft Azure operated by 21Vianet (Azure China 21Vianet)'.



Azure Active Directory – Create New Group

Group

*

Group type

Security

*

Group name ⓘ

TestGroup

Group description ⓘ

Group for testing purposes

*

Membership type ⓘ

Assigned

Members ⓘ

0 members selected



User

alapértelmezett címár

* Name ⓘ

Jane Doe ✓

* User name ⓘ

jane.doe@pekmilfreemail.onmicrosoft.com ✓

Profile ⓘ

Not configured >

Properties ⓘ

Default >

Groups ⓘ

0 groups selected >

Directory role

User >

Password

.....

☐ Show Password

Profile

User

General

First name

Jane

Last name

Doe

Work info

Job title

manager

Department

sales

Groups

select groups to join

+ Invite

Select ⓘ

Search by name or email address ✓

☒

TE

TestGroup

Directory role ⓘ

☒ User

☐ Global administrator

☐ Limited administrator

Users can access assigned resources but cannot manage most directory resources.

[Learn more about directory roles](#)



Azure Active Directory – Users

Users - All users

alapértelmezett címár - Azure Active Directory

Search (Ctrl+I)

All users

Deleted users

Password reset

User settings

ACTIVITY

Sign-ins

Audit logs

TROUBLESHOOTING + SUPPORT

Troubleshoot

New support request

+ New user

+ New guest user

Reset password

Delete user

Multi-Factor Authentication

Refresh

Columns

Name

Search by name or email

Show

All users

NAME	USER NAME	USER TYPE	SOURCE
<div>JD</div> <div>Jane Doe</div>	jane.doe@pekmlfreemail.onmicrosoft.com	Member	Azure Active Directory
<div>MP</div> <div>Milan Pekardy</div>	pekml@freemail.hu	Member	Azure Active Directory



Azure Active Directory – Sample Application

- Visual Studio > Create New ASP.NET Core Web Application
- Change Authentication to Work or School Accounts

Change Authentication

☐ No Authentication

☐ Individual User Accounts

☒ Work or School Accounts

☐ Windows Authentication

For applications that authenticate users with Active Directory, Microsoft Azure Active Directory, or Office 365.

[Learn more](#)

Cloud - Single Organization ⓘ

Domain:

pekmlfreemail.onmicrosoft.com ⓘ

Directory Access Permissions:

☐ Read directory data ⓘ

▼ More Options

[Learn more about third-party open source authentication options](#)

OK Cancel



Azure Active Directory – Sample Application

- Register the correct reply URL: Azure Active Directory > App registrations > All apps > AzureADWebApplication > Settings > Reply URLs

The screenshot displays the Azure portal interface for managing an application. It is divided into three main panes:

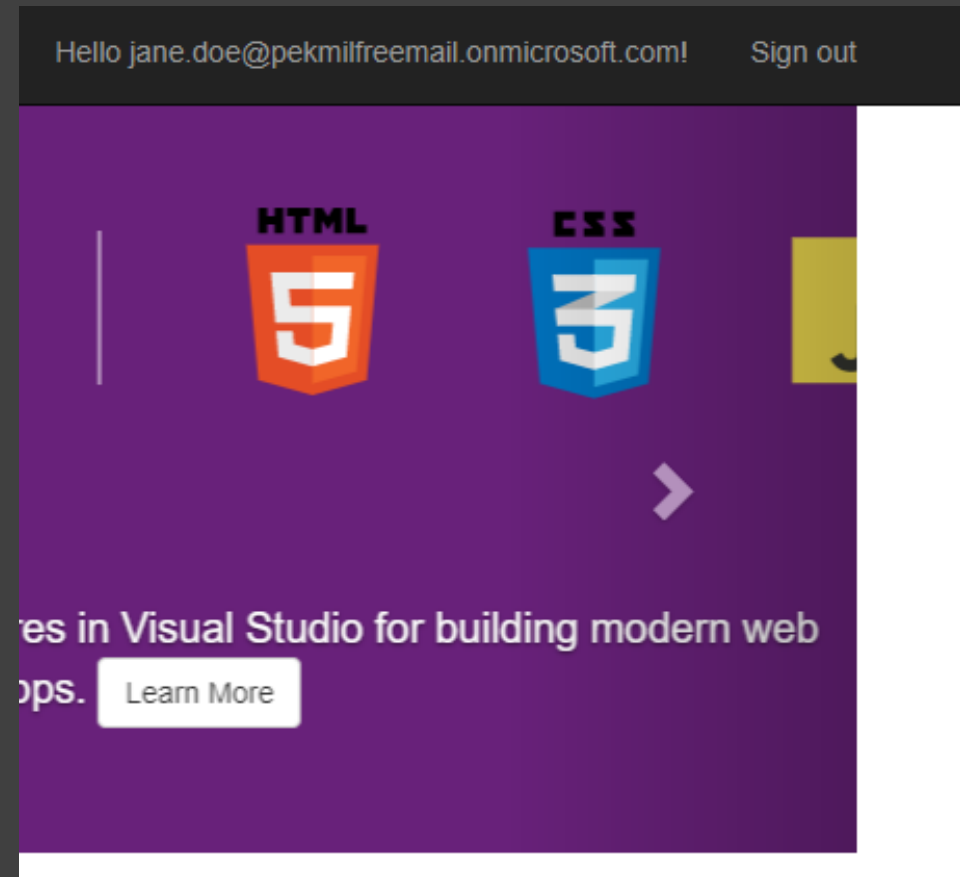
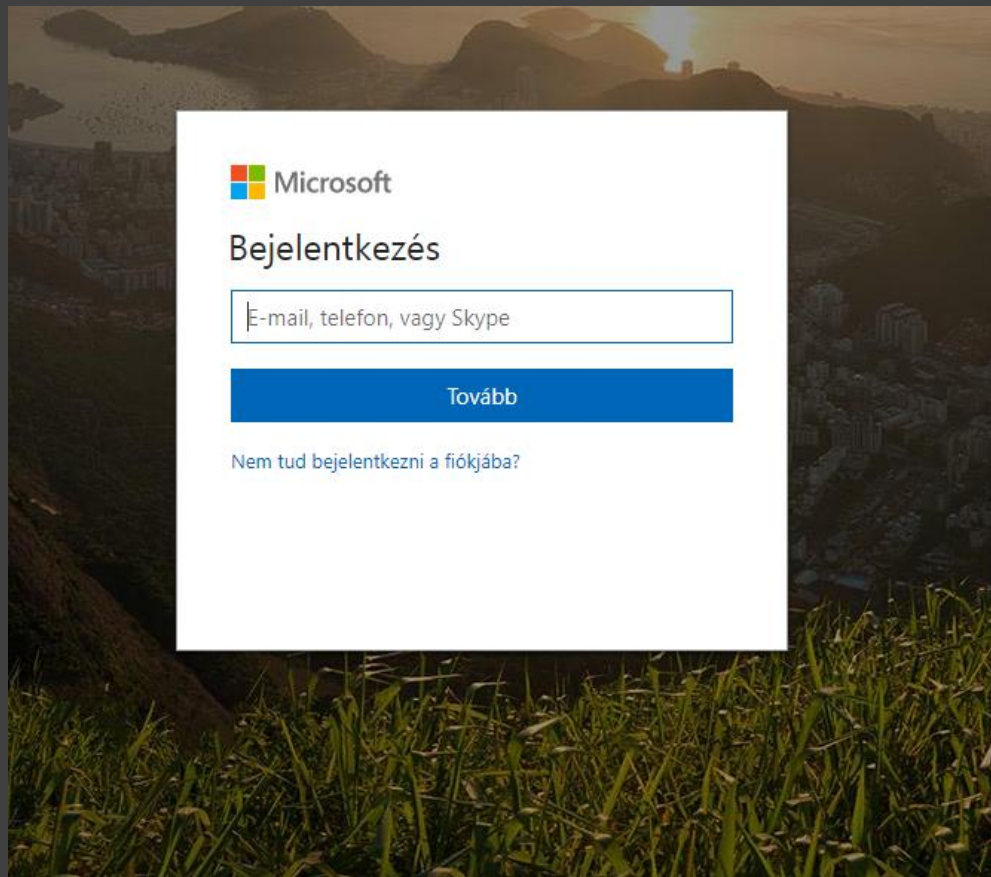
- Left Pane (AzureADWebApplication):** Shows the application's metadata.

Property	Value
Display name	AzureADWebApplication
Application type	Web app / API
Home page	https://localhost:44385/
Application ID	003af13c-8f65-474c-a626-9e9725202f64
Object ID	808a8cab-cf17-4ebc-a41e-6d3598a44cf0
Managed application in local directory	AzureADWebApplication
- Middle Pane (Settings):** A sidebar menu for configuring the application.
 - Filter settings
 - GENERAL
 - Properties
 - Reply URLs** (selected)
 - Owners
 - API ACCESS
 - Required permissions
 - Keys
 - TROUBLESHOOTING + SUPPORT
 - Troubleshoot
 - New support request
- Right Pane (Reply URLs):** A list of reply URLs for the application.
 - Buttons: Save, Discard
 - Current list:
 - <https://localhost:44385/signin-oidc>
 - <http://azureadwebapplication.azurewebsites.net/signin-oidc> (highlighted with a red box)
 - Input field for a new URL.



Azure Active Directory – Sample Application

- You can now log into the app with your account





Azure Active Directory – Role based authorization

- Configure Azure AD to send back claims representing a user's group membership
- App registrations > All apps > AzureADWebApplication > Manifest

```
{  
  "appId": "003af13c-8f65-474c-a626-9e9725202f64",  
  "appRoles": [],  
  "availableToOtherTenants": false,  
  "displayName": "AzureADWebApplication",  
  "errorUrl": null,  
  "groupMembershipClaims": "SecurityGroup",  
  "optionalClaims": null,  
  "acceptMappedClaims": null,  
  "homepage": "https://localhost:44385/",  
  "informationalUrls": {  
    "privacy": null,  
    "termsOfService": null  
  },  
}
```



Azure Active Directory – Role based authorization

- Defining authorization policy:
 - The authorization primitives in ASP.NET Core are **claims** and **policies**.
 - Claims hold information about a user,
 - Policies encapsulate simple logic to evaluate the current user against the current context and return true to authorize a user.

```
services.AddAuthorization(options =>
{
    options.AddPolicy("TestGroupPolicy", builder => builder.RequireClaim("groups", "4097c541-9b33-4a84-b409-7030bc525438"));
});
```

```
[Authorize("TestGroupPolicy")]
0 references | 1 request | 0 exceptions
public IActionResult About()
{
    ViewData["Message"] = "Your application description page.";

    return View();
}
```



Azure Active Directory – Role based authorization

AzureADWebApplication

[Home](#)

[About](#)

[Contact](#)

Hello live.com#peknil@freemail.hu!

[Sign out](#)

ViewData["Title"]

You do not have access to this resource.

© 2018 - AzureADWebApplication



Azure Active Directory – Role based authorization

AzureADWebApplication

[Home](#)

[About](#)

[Contact](#)

Hello jane.doe@peknilfreemail.onmicrosoft.com!

[Sign out](#)

About

Your application description page.

Use this area to provide additional information.

aio	ASQA2/8GAAAABeCNZP2Bycw3KBSGq0gHswi2XB1fvWndQHGDx+uQA=
http://schemas.microsoft.com/claims/authnmethodsreferences	pwd
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Doe
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Jane
groups	4097c541-9b33-4a84-b409-7030bc525438
name	Jane Doe
http://schemas.microsoft.com/identity/claims/objectidentifier	6be31369-161a-4d5c-b44e-0f2ff27574a1
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	THWz1wrfm5IJOsf0F09r-xIHtpEn4t8GE6zCfLlv26c
http://schemas.microsoft.com/identity/claims/tenantid	02676314-818b-4a6e-b65b-a9c60f25a1b6
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	jane.doe@peknilfreemail.onmicrosoft.com
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	jane.doe@peknilfreemail.onmicrosoft.com
uti	qO8pVu52tUy0-hP61UUAAA