Secure Multi-tenant Apps with Azure and Azure DevOps

Benny Michielsen
DevOps Pro Europe
21 March 2019

Benny Michielsen

@bennymichielsen
bennymichielsen.be
bennym@infosupport.com

Tech aficionado

Programming, Zbgureshpxre


4
18
6
9
5
1
2
11
8
3

Secure

Isolated

Automated


E
F

Secure

defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction

Azure AD

Integrate with Azure AD

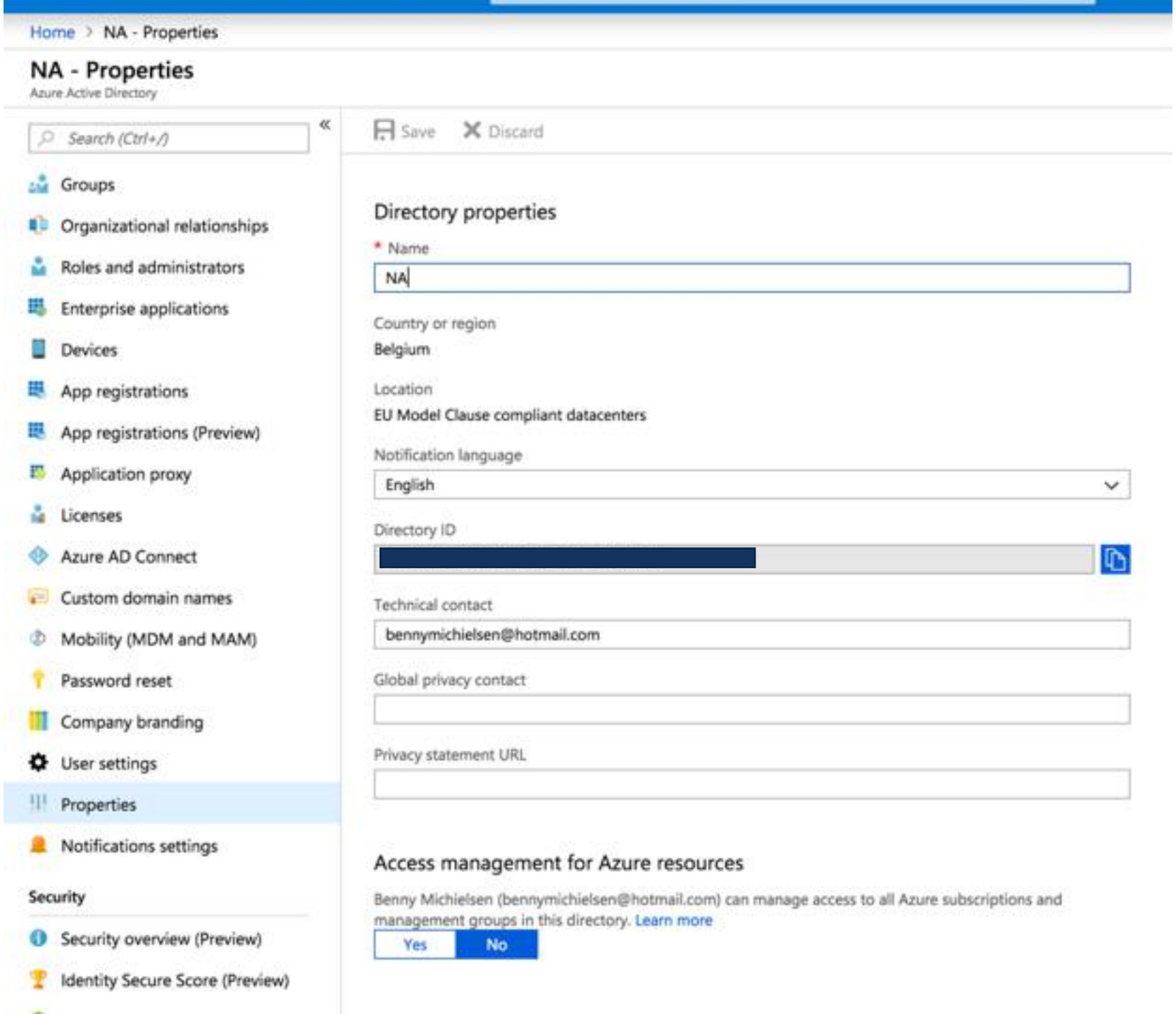
```
<ItemGroup>
        <PackageReference
                Include="Microsoft.AspNetCore.App" />
        <PackageReference
                Include="Microsoft.AspNetCore.Authentication.AzureAD.UI"
                Version="2.1.1" />
</ItemGroup>
```

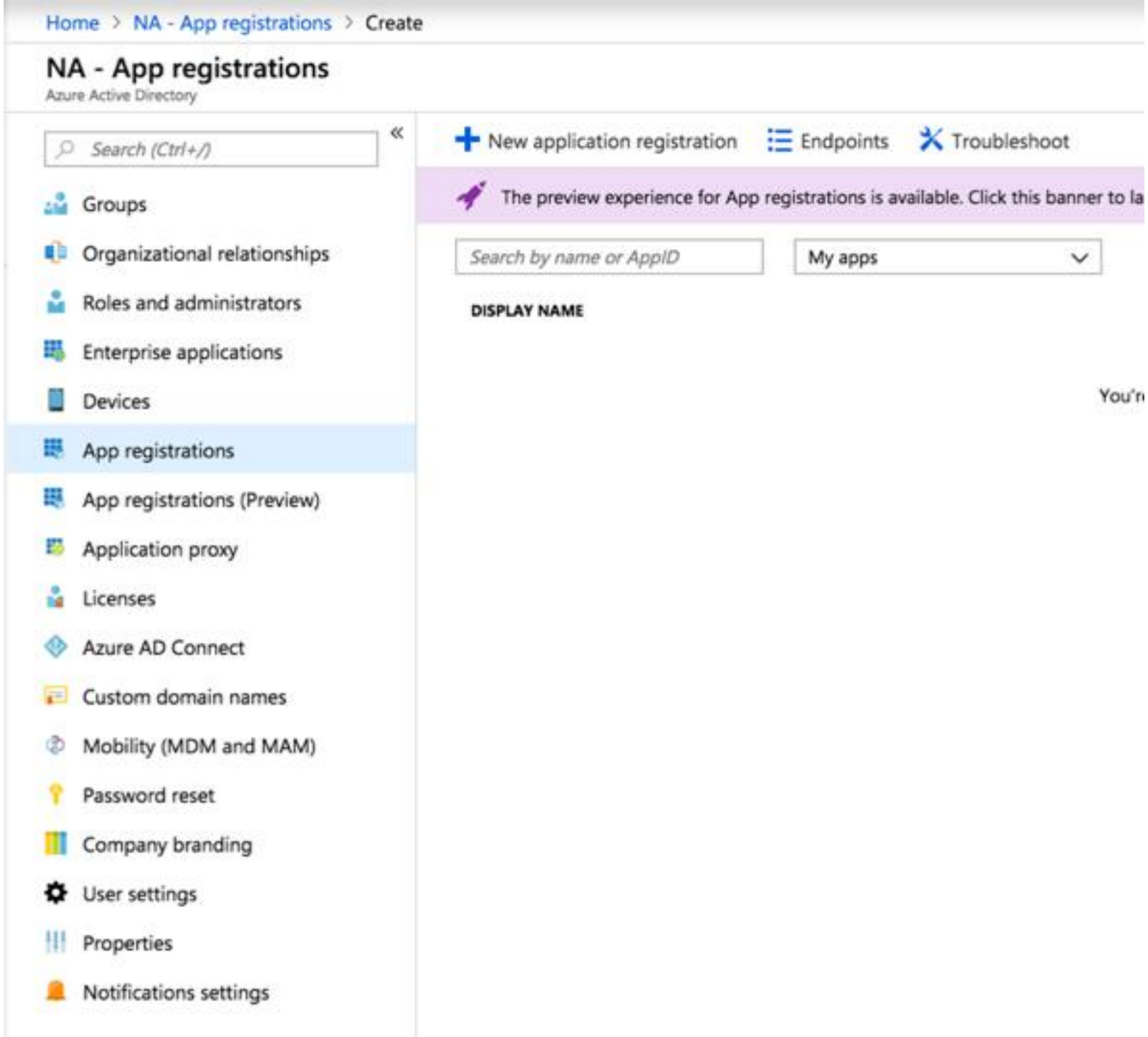
Integrate with Azure AD

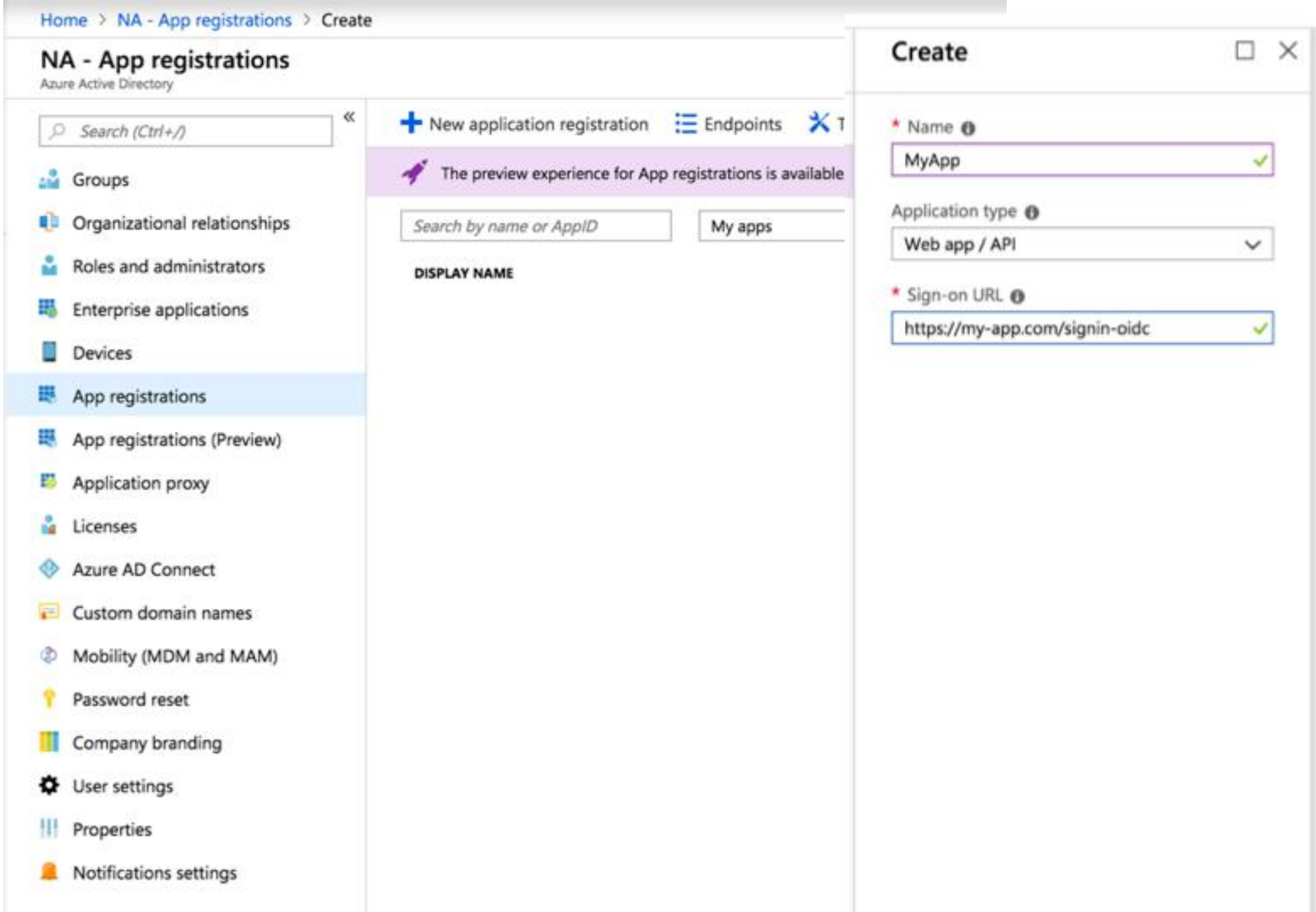
```
public void ConfigureServices(IServiceCollection services)
{
	services.AddAuthentication(AzureADDefaults.AuthenticationScheme)
		.AddAzureAD(options =>
			Configuration.Bind("AzureAd", options));

	services.Configure<OpenIdConnectOptions>(
		AzureADDefaults.OpenIdScheme,
		options => {
			options.Authority = options.Authority + "/v2.0/";
			options.TokenValidationParameters.ValidateIssuer = true;
		});
```

Integrate with Azure AD

```
{
        "AzureAd": {
                "Instance": "https://login.microsoftonline.com/",
                "TenantId": "",
                ”ClientId": "",
                "CallbackPath": "/signin-oidc"
                }
}
```


Home > NA - Properties
NA - Properties
Azure Active Directory
Search (Ctrl+/)
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings
Security
Security overview (Preview)
Identity Secure Score (Preview)
Save
Discard
Directory properties
* Name
NA
Country or region
Belgium
Location
EU Model Clause compliant datacenters
Notification language
English
Directory ID
Technical contact
bennymichielsen@hotmail.com
Global privacy contact
Privacy statement URL
Access management for Azure resources
Benny Michielsen (bennymichielsen@hotmail.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more
Yes
No


Home > NA - App registrations > Create
NA - App registrations
Azure Active Directory
Search (Ctrl+/)
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings
New application registration
Endpoints
Troubleshoot
The preview experience for App registrations is available. Click this banner to la
Search by name or AppID
My apps
DISPLAY NAME
You'r


Home > NA - App registrations > Create
NA - App registrations
Azure Active Directory
Search (Ctrl+/)
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings
New application registration
Endpoints
The preview experience for App registrations is available
Search by name or AppID
My apps
DISPLAY NAME
Create
* Name
MyApp
Application type
Web app / API
* Sign-on URL
https://my-app.com/signin-oidc

NA - App registrations

Azure Active Directory

Search (Ctrl+/)

Overview
Getting started

Manage

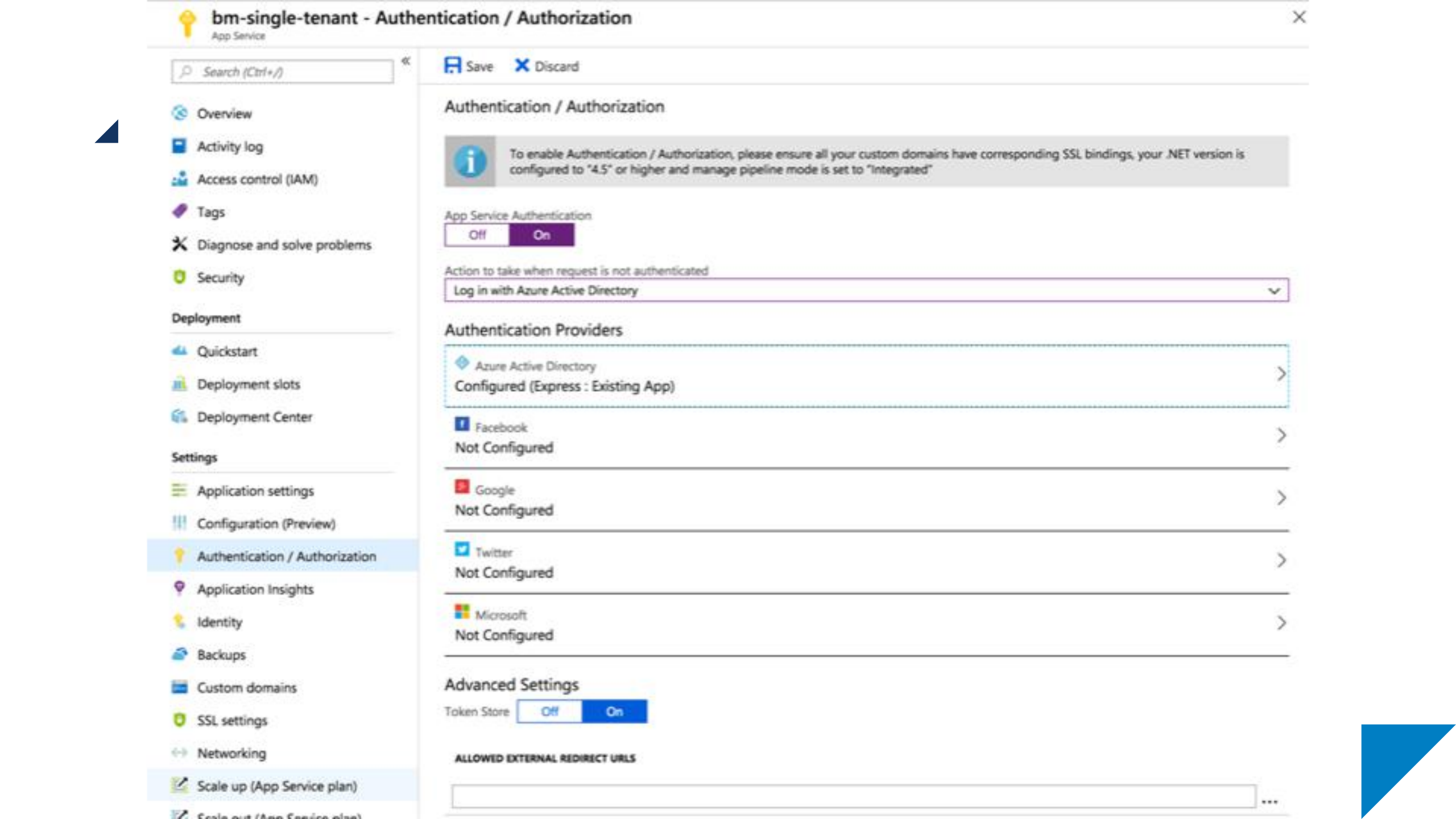
Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

New application registration | Endpoints | Troubleshoot

The preview experience for App registrations is available. Click this banner to launch the preview experience. →

Search by name or AppID | All apps

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
my-web-app-1234-qwerty	Web app / API	[redacted]
My App	Web app / API	[redacted]
bennym-HobbyStreak-234c9204-07ea-49d8-95b2-a1386d7f02e4	Web app / API	[redacted]
Multi Tenant App	Web app / API	[redacted]
https://localhost:44320/	Web app / API	[redacted]
bennym-MultitenantSample-9aea80f3-cc22-414f-9389-cb2d3918bd0c	Web app / API	[redacted]
bennym-HobbyStreak-234c9204-07ea-49d8-95b2-a1386d7f02e4	Web app / API	[redacted]
bm-automation_k3jVEy69vFwLzrwGajlSTCUZAobAFWCOsoxau9wjjyM=	Web app / API	[redacted]
bm-web	Web app / API	[redacted]


bm-single-tenant - Authentication / Authorization
App Service
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Deployment
Quickstart
Deployment slots
Deployment Center
Settings
Application settings
Configuration (Preview)
Authentication / Authorization
Application Insights
Identity
Backups
Custom domains
SSL settings
Networking
Scale up (App Service plan)
Save
Discard
Authentication / Authorization
To enable Authentication / Authorization, please ensure all your custom domains have corresponding SSL bindings, your .NET version is configured to "4.5" or higher and manage pipeline mode is set to "Integrated"
App Service Authentication
Off
On
Action to take when request is not authenticated
Log in with Azure Active Directory
Authentication Providers
Azure Active Directory
Configured (Express : Existing App)
Facebook
Not Configured
Google
Not Configured
Twitter
Not Configured
Microsoft
Not Configured
Advanced Settings
Token Store
Off
On
ALLOWED EXTERNAL REDIRECT URLS

Azure AD – Restricting access

- By default all registered apps are available to all users
- All apps show up on their profile

Enterprise applications - All applications

NA - Azure Active Directory

Overview

Manage

All applications

Application proxy

User settings

Security

Conditional Access

Activity

Sign-ins

Audit logs

Access reviews

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

New application Columns

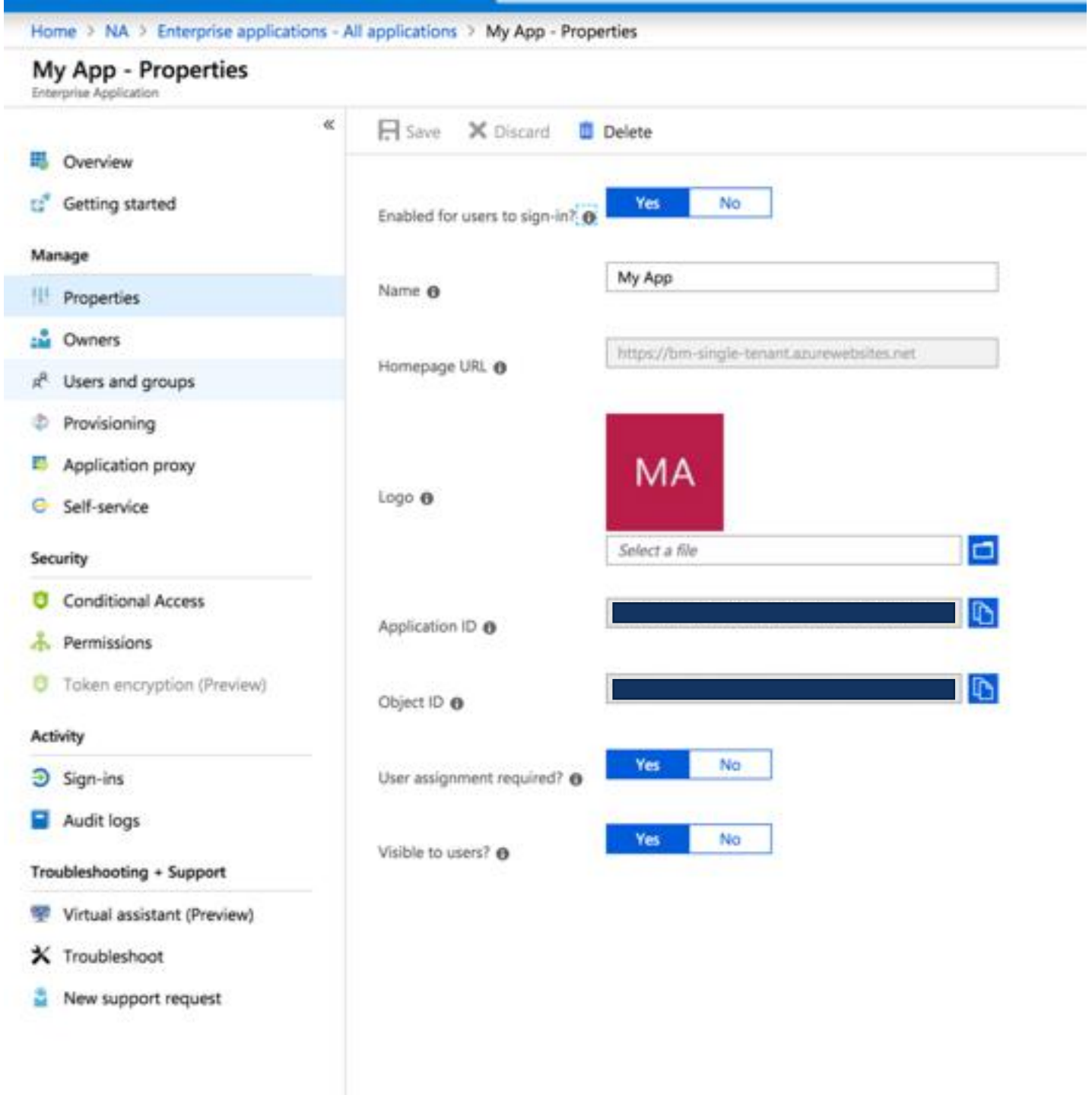
Application Type: Enterprise Applications

Applications status: Any

Application visibility: Any

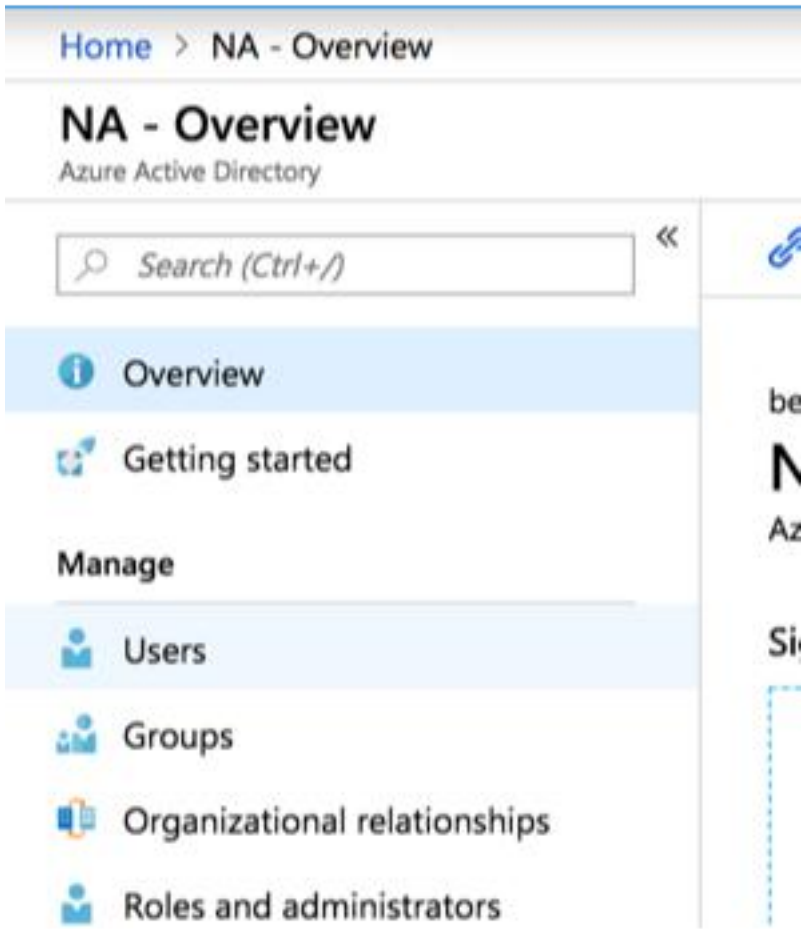
First 50 shown, to search all of your applications, enter a display name or the application ID.

NAME	HOMEPAGE URL
Azure DevOps	http://azure.com/devops
bm-web	https://bm-web.azurewebsites.net
https://localhost:44320/	https://localhost:44320/
Multi Tenant App	https://bm-multi.azurewebsites.net
My App	https://bm-single-tenant.azurewebsites.net
Office 365 Exchange Online	http://office.microsoft.com/outlook/
Office 365 Management APIs	
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/
Outlook Groups	
Skype for Business Online	


Home > NA > Enterprise applications - All applications > My App - Properties
My App - Properties
Enterprise Application
Save
Discard
Delete
Overview
Getting started
Manage
Properties
Owners
Users and groups
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption (Preview)
Activity
Sign-ins
Audit logs
Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request
Enabled for users to sign-in?
Yes
No
Name
My App
Homepage URL
https://bm-single-tenant.azurewebsites.net
Logo
MA
Select a file
Application ID
Object ID
User assignment required?
Yes
No
Visible to users?
Yes
No

Groups and roles

- Groups (Security Groups)
  - Can be assigned to users
  - Managed for the entire Azure AD
  - Group information can be made available to the application
- Application Roles
  - Application can define roles
  - Scoped per application
  - Role information can be read to check authorisation


Home > NA - Overview
NA - Overview
Azure Active Directory
Search (Ctrl+/)
Overview
Getting started
Manage
Users
Groups
Organizational relationships
Roles and administrators

Home > NA - App registrations > Multi Tenant App > Edit manifest

Multi Tenant App

Registered app

Settings | Manifest | Delete

Display name
Multi Tenant App

Application type
Web app / API

Home page
https://bm-multi.azurewebsites.net

Application ID
[redacted]

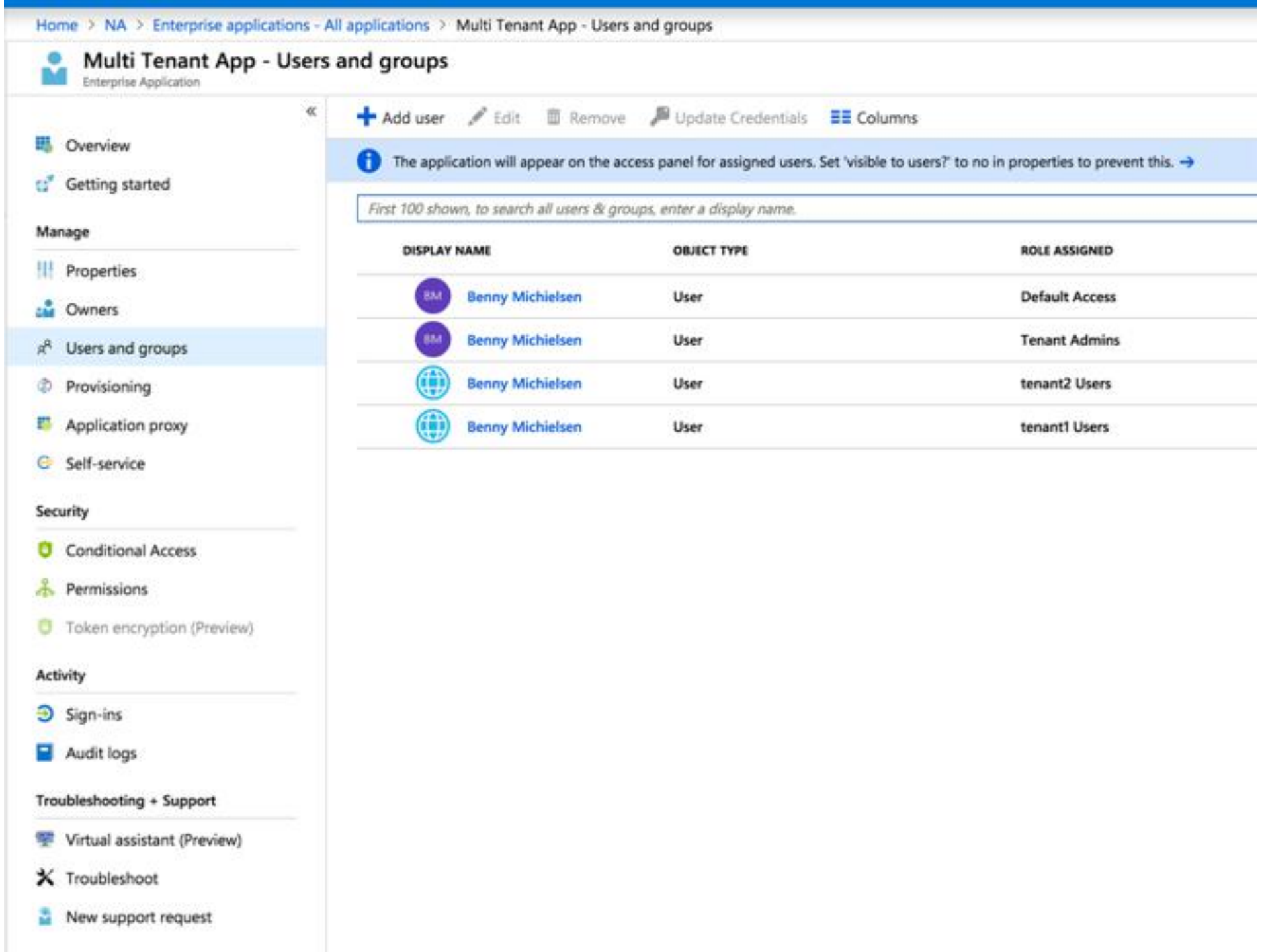
Object ID
afbe973d-20d9-42fd-ae85-7e2487e903e5

Managed application in local directory
Multi Tenant App

Edit manifest

Save | Discard | Edit | Upload | Download

```
{
  "appId": [redacted]
  "appRoles": [
    {
      "allowedMemberTypes": [
        "User"
      ],
      "displayName": "tenant2 Users",
      "id": "8208ea18-a468-45e6-81b5-3acb4f321e84",
      "isEnabled": true,
      "description": "Users of the tenant",
      "value": "tenant2"
    },
    {
      "allowedMemberTypes": [
        "User"
      ],
      "displayName": "tenant1 Users",
      "id": "2db78c2f-f8b4-48ad-9b13-ce9d0e658bf0",
      "isEnabled": true,
      "description": "Users of the tenant",
      "value": "tenant1"
    },
    {
      "allowedMemberTypes": [
```


Home > NA > Enterprise applications - All applications > Multi Tenant App - Users and groups
Multi Tenant App - Users and groups
Enterprise Application
Overview
Getting started
Manage
Properties
Owners
Users and groups
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption (Preview)
Activity
Sign-ins
Audit logs
Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request
Add user
Edit
Remove
Update Credentials
Columns
The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.
First 100 shown, to search all users & groups, enter a display name.
DISPLAY NAME
OBJECT TYPE
ROLE ASSIGNED
Benny Michielsen
User
Default Access
Benny Michielsen
User
Tenant Admins
Benny Michielsen
User
tenant2 Users
Benny Michielsen
User
tenant1 Users

Azure AD 

- Multi-tenant service that provides enterprise-level identity and access management

- Manage users and access to resources
- Provide single sign on
- Multi factor authentication
- Manage Groups
- Manage Applications
- Actively being integrated in azure services

KeyVault

Solid Innovator

```
{
        "Logging": {
                "LogLevel": {
                        "Default": "Warning"
                }
        },
        "AllowedHosts": "*",
        "Storage": {
                "Name": "",
                "ConnectionString": ""
        },
        "ConnectionStrings": {
                "CustomerAppDatabase": ""
        },
        "AzureAd": {
                "Instance": "https://login.microsoftonline.com/",
                "Domain": "",
                "TenantId": "",
                "ClientId": "",
                "ClientSecret": "",
                "CallbackPath": "/signin-oidc"
        },
        "KeyVault": {
                "Name": ""
        }
}
```

Azure KeyVault 

- Safeguard cryptographic keys and other secrets used by cloud apps and services

- Secret Management
- Key Management
- Certificate Management

bm-single-keyvault - Secrets

Key vault

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

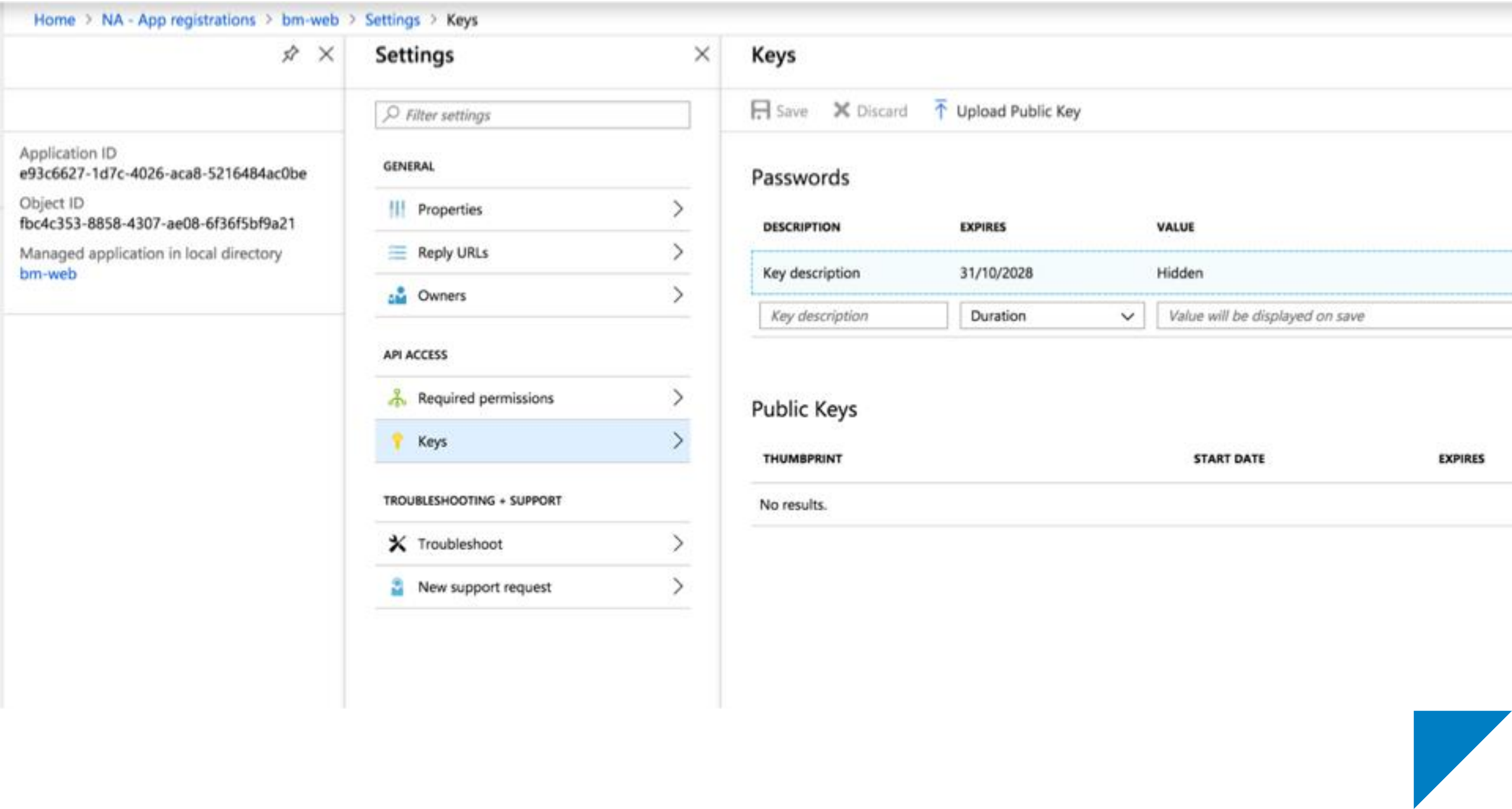
Settings

Keys
Secrets
Certificates
Access policies
Firewalls and virtual networks
Properties
Locks
Automation script

Generate/Import | Refresh | Restore Backup

NAME	TYPE	STATUS
ConnectionStrings--CustomerAppDatabase		✓ Enabled

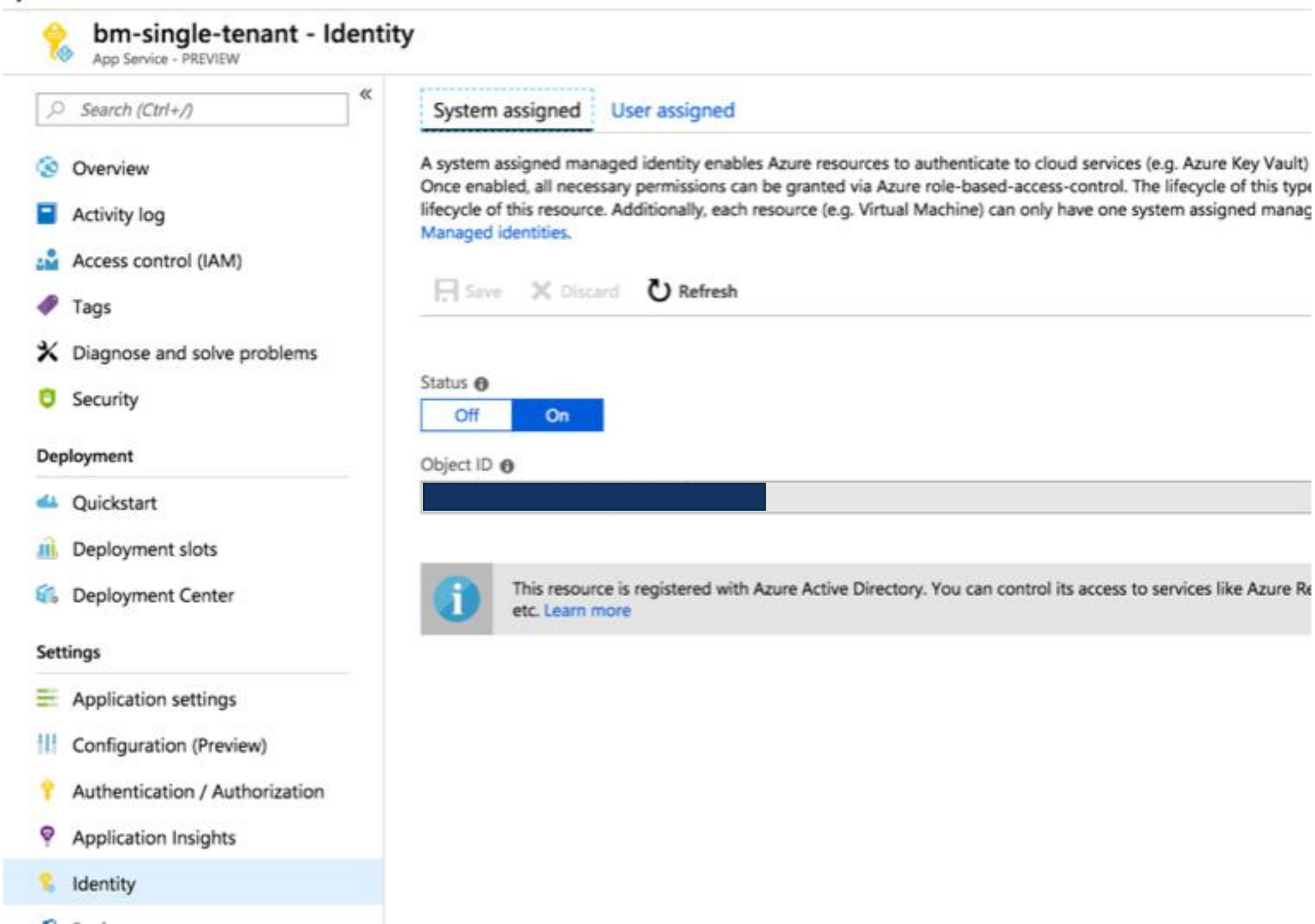
```
public static void Main(string[] args)
{
      CreateWebHostBuilder(args).Build().Run();
}

public static IWebHostBuilder CreateWebHostBuilder(string[]
args) =>
      WebHost.CreateDefaultBuilder(args)
            .ConfigureAppConfiguration((ctx, builder) =>
            {
                  var builtConfig = builder.Build();
                  builder.AddAzureKeyVault(
$"https://{builtConfig["KeyVault:Name"]}.vault.azure.net/",
      builtConfig["AzureAd:ClientId"],
      builtConfig["AzureAd:ClientSecret"]);
            })
      .UseStartup<Startup>();
```


Home > NA - App registrations > bm-web > Settings > Keys
Application ID
e93c6627-1d7c-4026-aca8-5216484ac0be
Object ID
fbc4c353-8858-4307-ae08-6f36f5bf9a21
Managed application in local directory
bm-web
Settings
Filter settings
GENERAL
Properties
Reply URLs
Owners
API ACCESS
Required permissions
Keys
TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request
Keys
Save
Discard
Upload Public Key
Passwords
DESCRIPTION
EXPIRES
VALUE
Key description
31/10/2028
Hidden
Key description
Duration
Value will be displayed on save
Public Keys
THUMBPRINT
START DATE
EXPIRES
No results.

```
{
        "Logging": {
                "LogLevel": {
                        "Default": "Warning"
                }
        },
        "AllowedHosts": "*",
        "Storage": {
                "Name": "",
                "ConnectionString": ""
        },
        "ConnectionStrings": {
                "CustomerAppDatabase": ""
        },
        "AzureAd": {
                "Instance": "https://login.microsoftonline.com/",
                "Domain": "",
                "TenantId": "",
                "ClientId": "",
                "ClientSecret": "",
                "CallbackPath": "/signin-oidc"
        },
        "KeyVault": {
                "Name": ""
        }
}
```

Managed Identity 

- Identity for Azure resources
  - System Assigned
  - User Assigned
- Remove the need to manage credentials
- Integrates with any resource that supports AD authentication


bm-single-tenant - Identity
App Service - PREVIEW
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Deployment
Quickstart
Deployment slots
Deployment Center
Settings
Application settings
Configuration (Preview)
Authentication / Authorization
Application Insights
Identity
System assigned
User assigned
A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault)
Once enabled, all necessary permissions can be granted via Azure role-based-access-control. The lifecycle of this type
lifecycle of this resource. Additionally, each resource (e.g. Virtual Machine) can only have one system assigned manag
Managed identities.
Save
Discard
Refresh
Status
Off
On
Object ID
This resource is registered with Azure Active Directory. You can control its access to services like Azure Re
etc. Learn more

ccess control (IAM)

bm-single-keyvault - Access control (IAM)

Key vault

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Keys
- Secrets
- Certificates
- Access policies
- Firewalls and virtual networks
- Properties
- Locks
- Automation script

Monitoring

- Alerts
- Metrics

Add | Edit columns | Refresh | Remove

Check access | Role assignments | Deny assignments | Classic a

Manage access to Azure resources for users, groups, service principals and mana
creating role assignments. Learn more

Name: Search by name or email

Type: All

Scope: All scopes

Group by: Role

4 items (4 Service Principals)

NAME	TYPE
CONTRIBUTOR	
bennym-MultitenantSam...	App
bm-automation_k3jVEy6...	App
OWNER	
bennym-MultitenantSam...	App

Add role assignment

Role: Select a role

Assign access to: Azure AD user, group, or service principal

Select: bm

- **bm-automation_k3jVEy69vFwLzrwGajlSTCUZAobAFWC...**
- **bm-multi**
  /subscriptions/9aea80f3-cc22-414f-9389-cb2d3918bd0...
- **bm-single-tenant**
  /subscriptions/9aea80f3-cc22-414f-9389-cb2d3918bd0...
- **bm-web**

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.

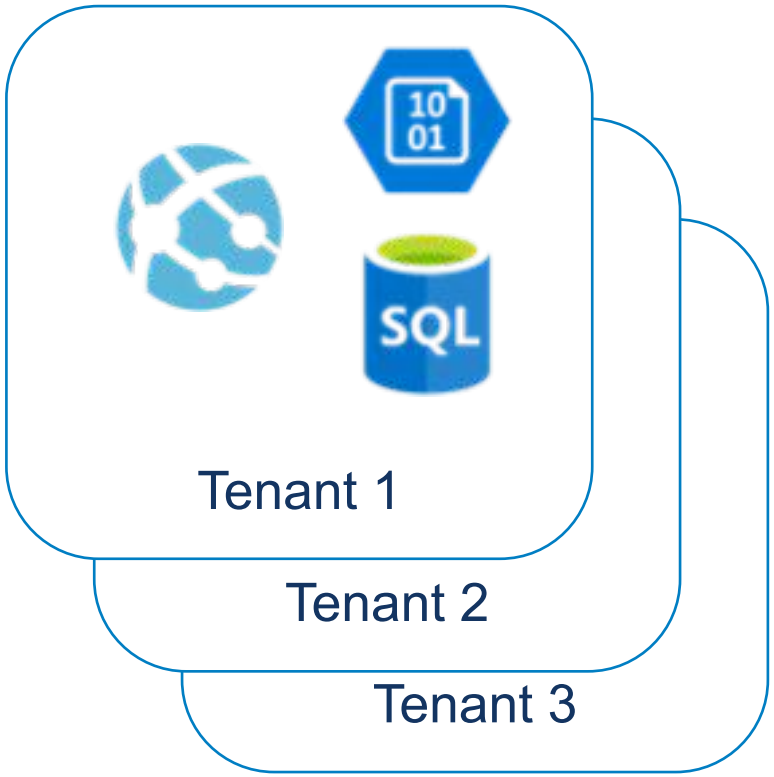
Learn more about RBAC

```
public static void Main(string[] args)
{
      CreateWebHostBuilder(args).Build().Run();
}

public static IWebHostBuilder
      CreateWebHostBuilder(string[] args) =>
          WebHost.CreateDefaultBuilder(args)
            .ConfigureAppConfiguration((ctx, builder) =>
            {
                  var builtConfig = builder.Build();
                  builder.AddAzureKeyVault(
$"https://{builtConfig["KeyVault:Name"]}.vault.azure.net/”
                  );
            })
            .UseStartup<Startup>();
```

Isolation

how and when the changes made by one operation become visible to other concurrent operations

Single tenant app



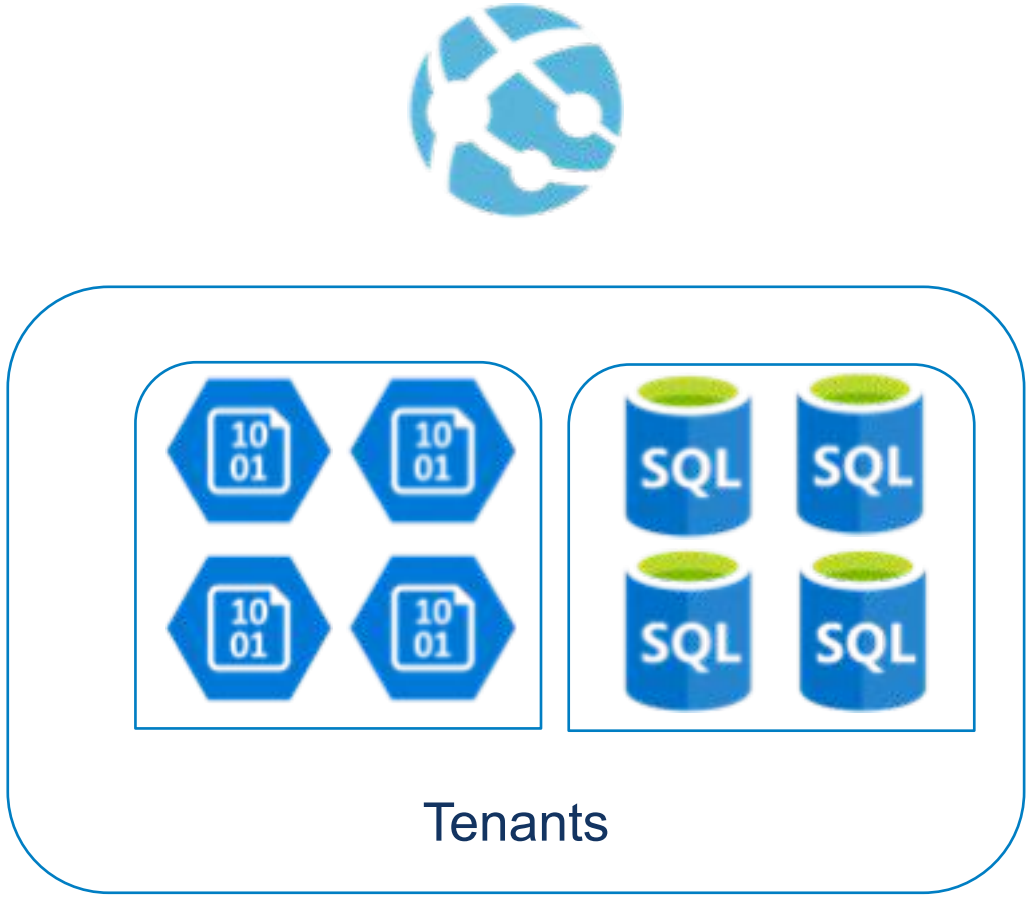
Multi tenant app

Tenant 1

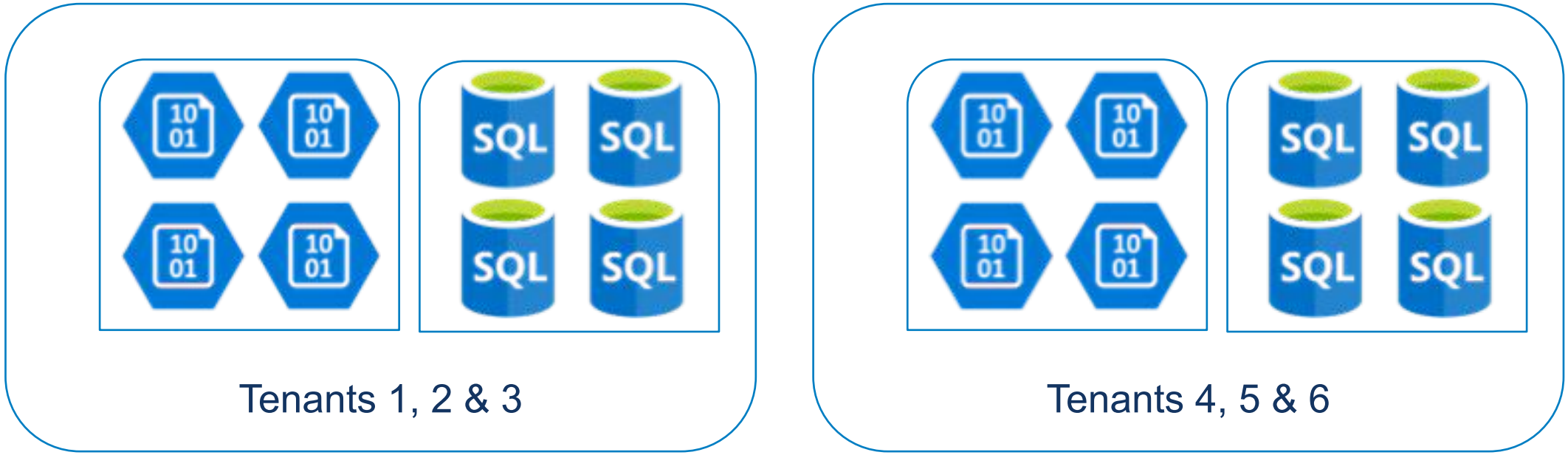
Tenant 2

Tenant 3

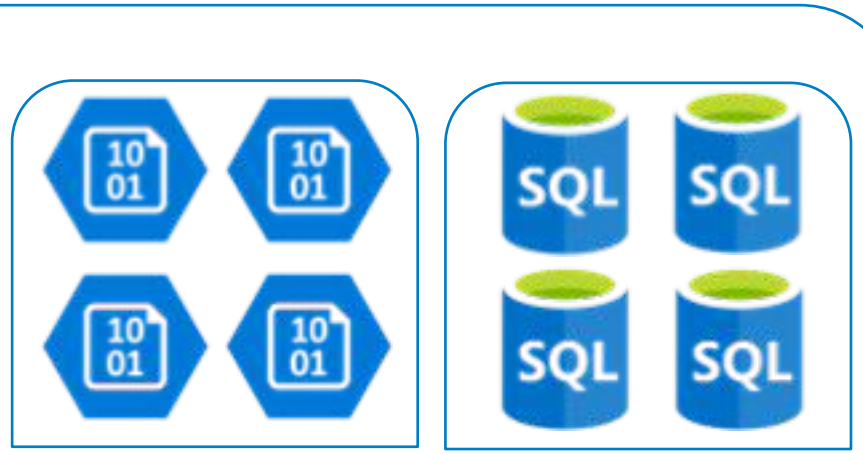
Multi tenant app



Multi tenant app



Multi tenant app



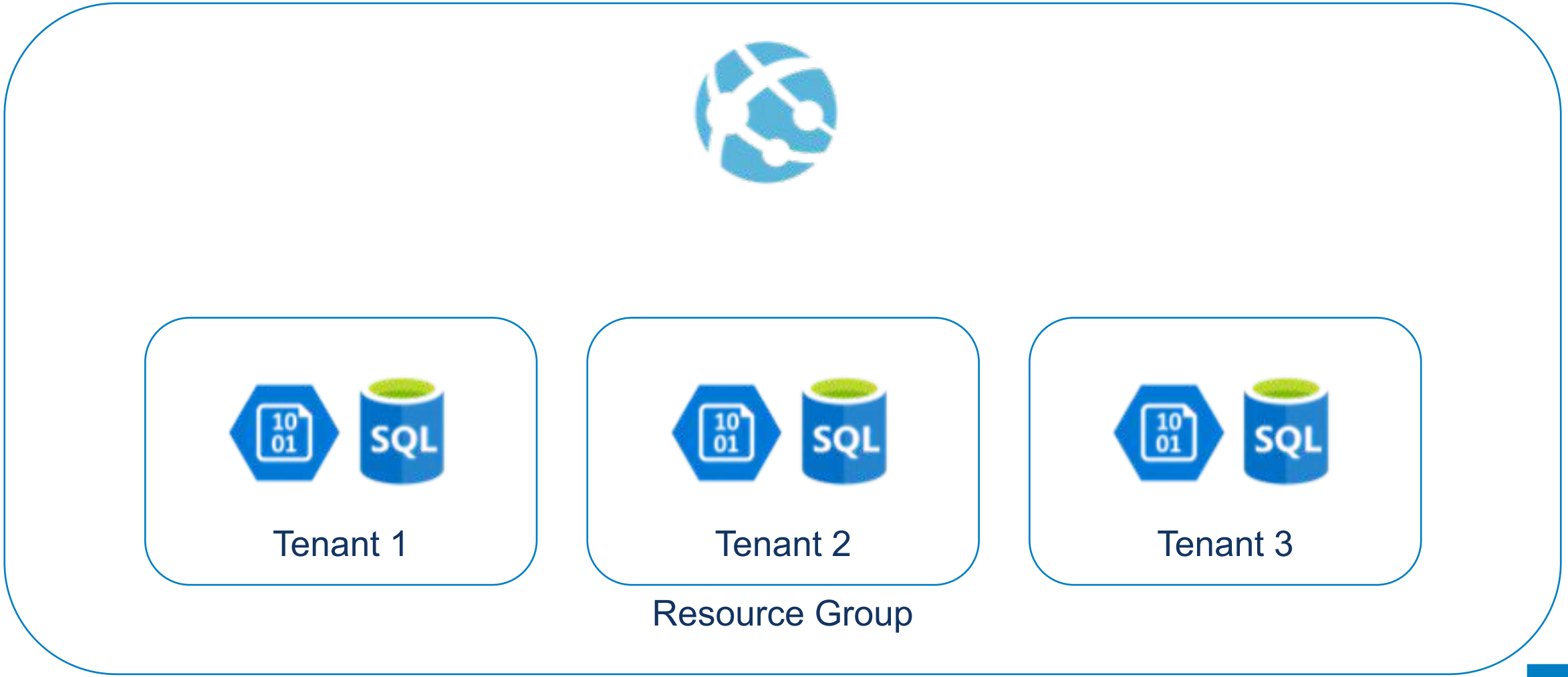
Stand alone single tenant

Stand alone single tenant

Automation

by which a process or procedure is performed with minimum human assistance.

Multi tenant app

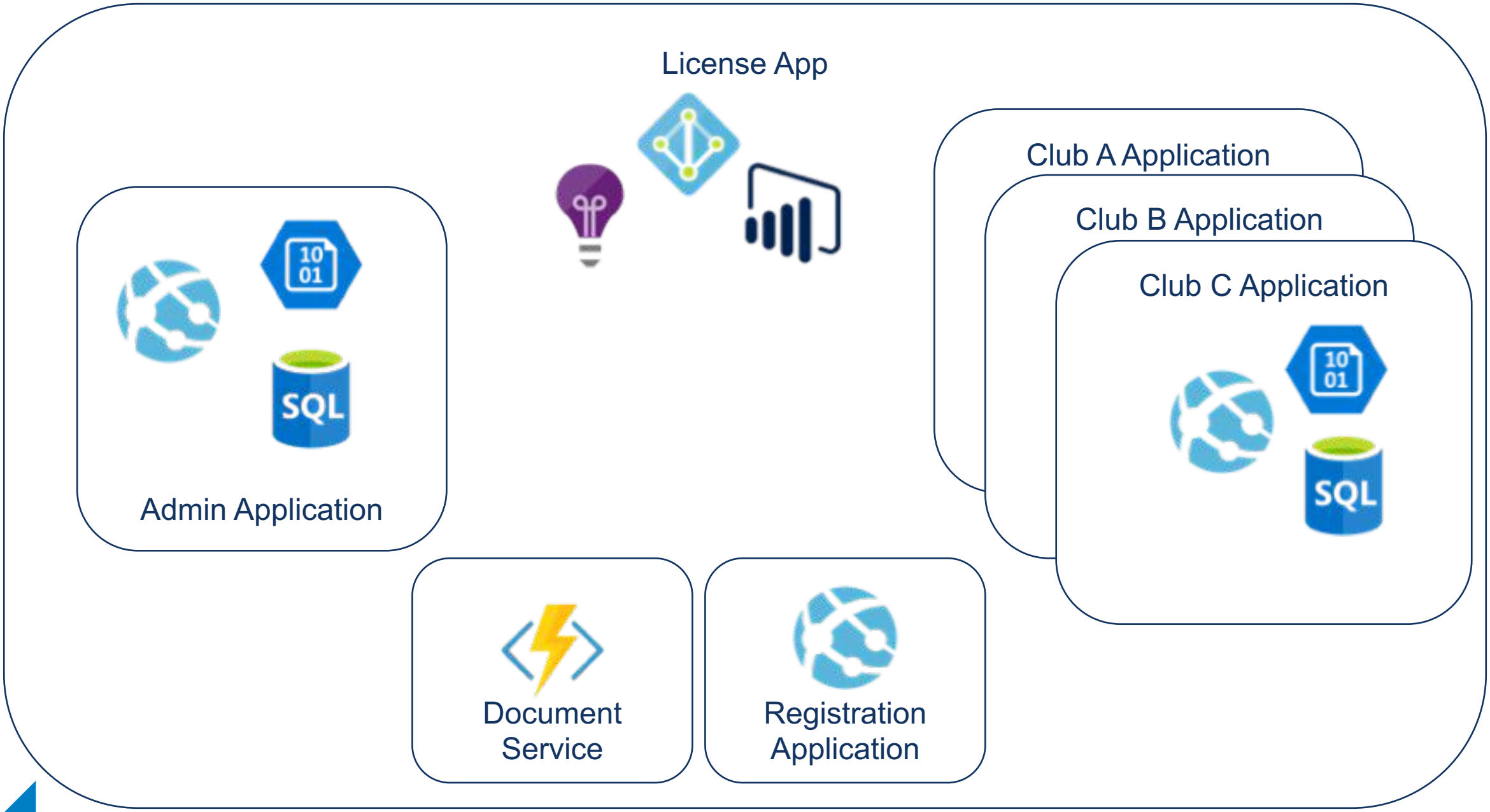


Automate provisioning

- ARM Templates
- Execute with
  - CLI
  - PowerShell
  - Azure DevOps
  - Azure Automation
  - Rest API

Stand alone single tenant

The entire picture


License App
Club A Application
Club B Application
Club C Application
10
01
SQL
Admin Application
Document
Service
Registration
Application

Thanks for listening!

@bennymichielsen
blog.bennymichielsen.be
bennym@infosupport.com