Azure AD admin automation using service principal

Last updated by | Vitor Tomaz | Feb 18, 2021 at 2:30 AM PST

Azure AD admin automation using service principal

Contents

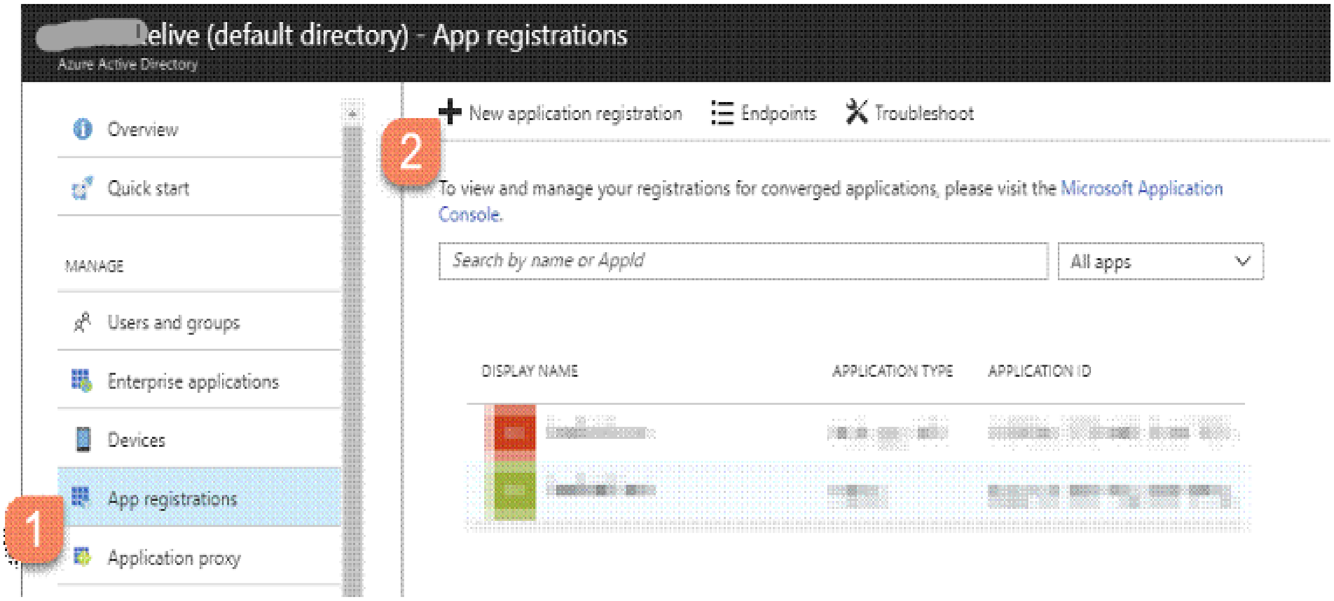
Issue

This guide will assist with auto assigning Ad admin role. Assuming you want to set the Azure AD admin via some form of automation, the following are detailed steps to provision a new service principal, granting it with permissions to run the cmdlet and running a sample script to perform the operation.

Mitigation

Steps to Handle

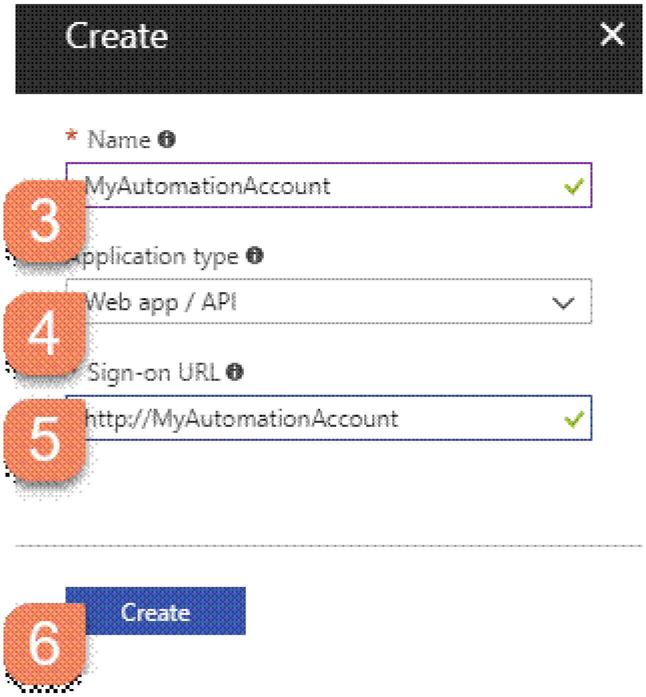
Provision a new service principal in your Azure AD tenant.



[redacted]elive (default directory) - App registrations

Azure Active Directory

To view and manage your registrations for converged applications, please visit the Microsoft Application Console.



Create

* Name

MyAutomationAccount

Application type

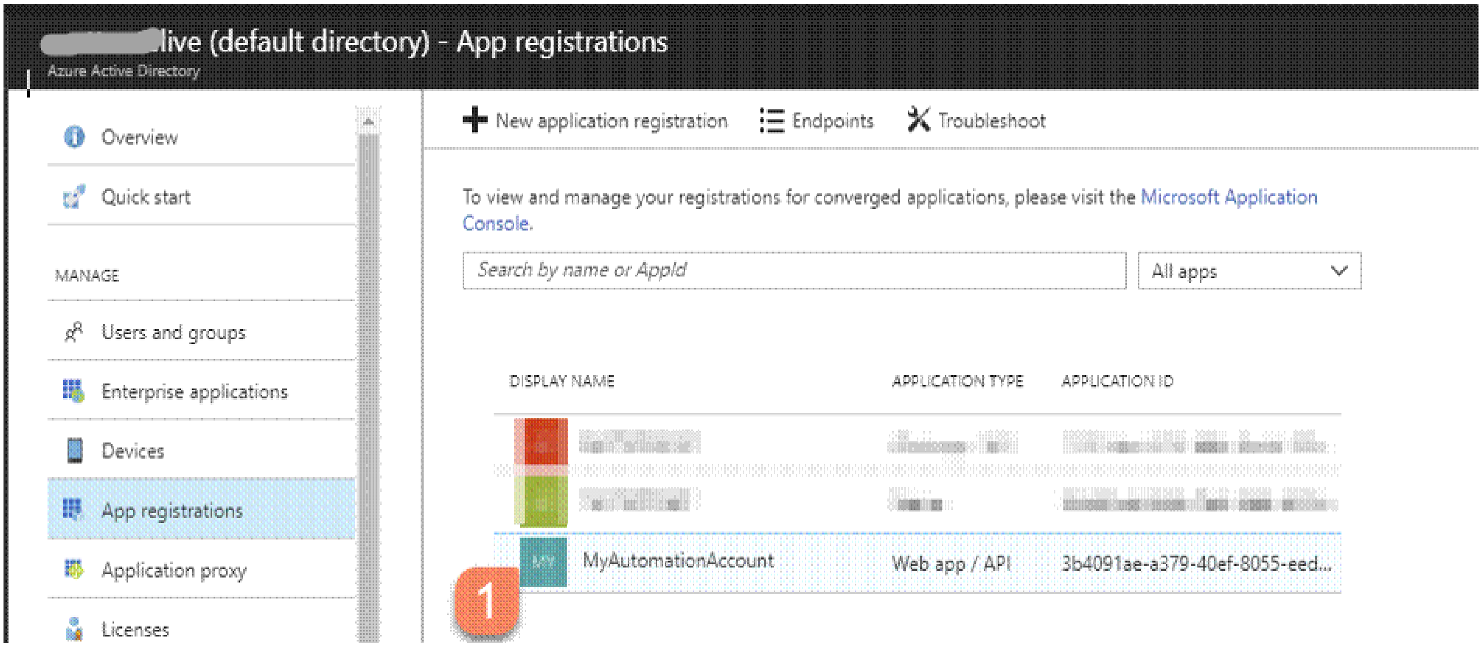
Web app / API

Sign-on URL

http://MyAutomationAccount

Create a new Key for the service principal

Create a new key in the app registration

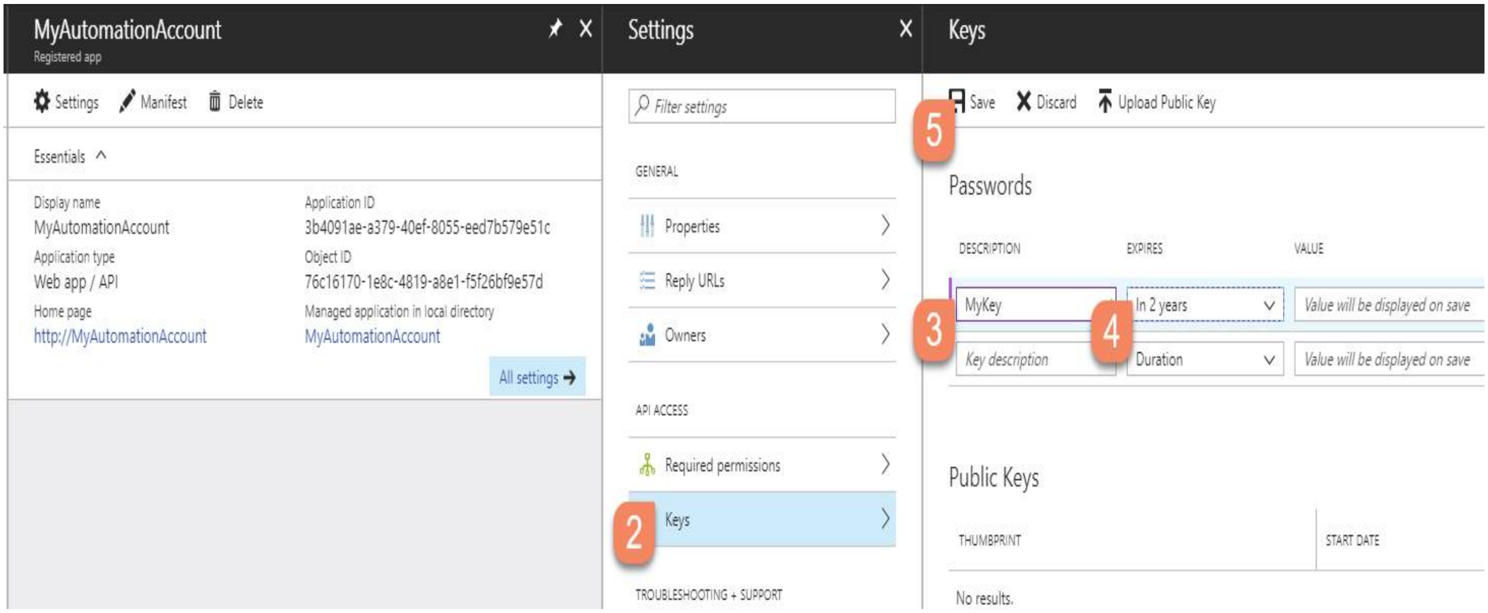


[redacted]live (default directory) - App registrations

Azure Active Directory

To view and manage your registrations for converged applications, please visit the Microsoft Application Console.

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
MyAutomationAccount	Web app / API	3b4091ae-a379-40ef-8055-eed...



Display name
MyAutomationAccount
Application type
Web app / API
Home page
http://MyAutomationAccount

Application ID
3b4091ae-a379-40ef-8055-eed7b579e51c
Object ID
76c16170-1e8c-4819-a8e1-f5f26bf9e57d
Managed application in local directory
MyAutomationAccount

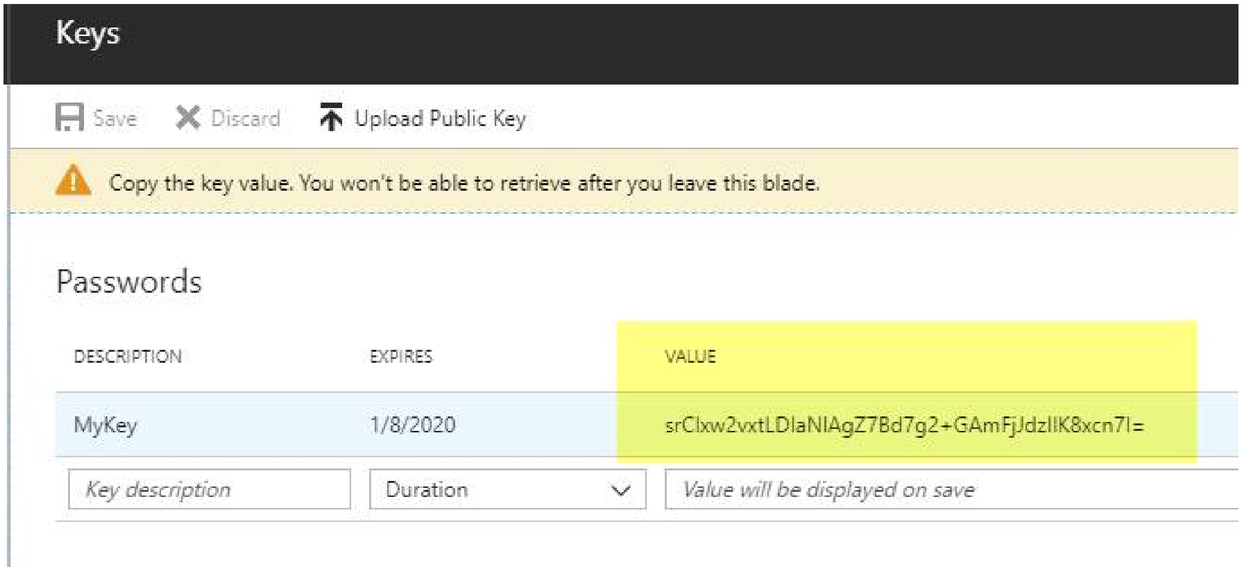
Passwords

DESCRIPTION	EXPIRES	VALUE
MyKey	In 2 years	Value will be displayed on save
Key description	Duration	Value will be displayed on save

Public Keys

THUMBPRINT	START DATE
No results.	

After clicking Save, take note of the generated Key value:



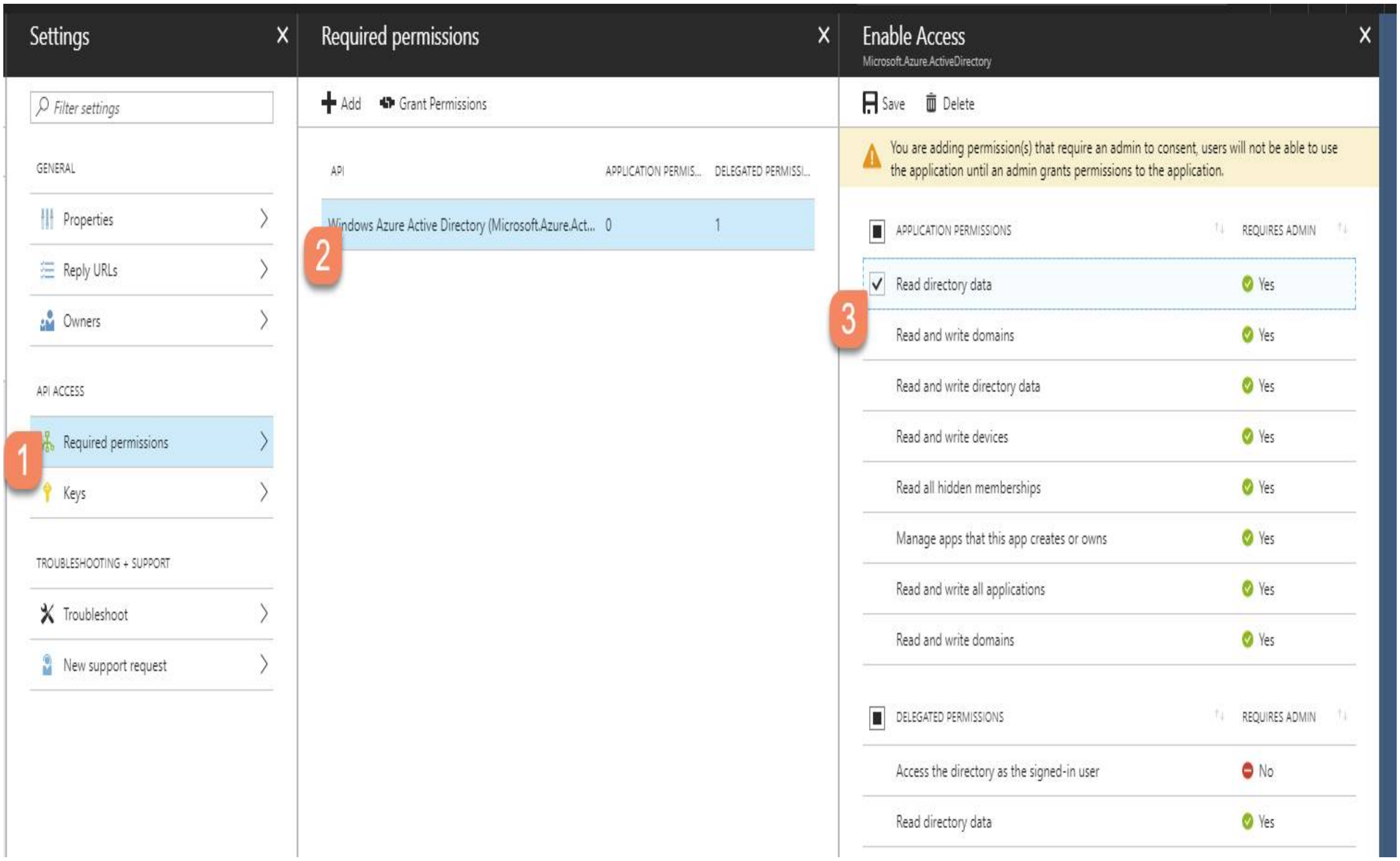
Copy the key value. You won't be able to retrieve after you leave this blade.

Passwords

DESCRIPTION	EXPIRES	VALUE
MyKey	1/8/2020	srClxw2vxtLDlaNIAgZ7Bd7g2+GAmFjJdzlIK8xcn7I=
Key description	Duration	Value will be displayed on save

Assign permissions in Azure AD

In the app registration, assign permissions to read directory data:



API	APPLICATION PERMIS...	DELEGATED PERMISSI...
Windows Azure Active Directory (Microsoft.Azure.Act...	0	1

You are adding permission(s) that require an admin to consent, users will not be able to use the application until an admin grants permissions to the application.

	APPLICATION PERMISSIONS	REQUIRES ADMIN
☑	Read directory data	✓ Yes
	Read and write domains	✓ Yes
	Read and write directory data	✓ Yes
	Read and write devices	✓ Yes
	Read all hidden memberships	✓ Yes
	Manage apps that this app creates or owns	✓ Yes
	Read and write all applications	✓ Yes
	Read and write domains	✓ Yes

	DELEGATED PERMISSIONS	REQUIRES ADMIN
	Access the directory as the signed-in user	⊖ No
	Read directory data	✓ Yes

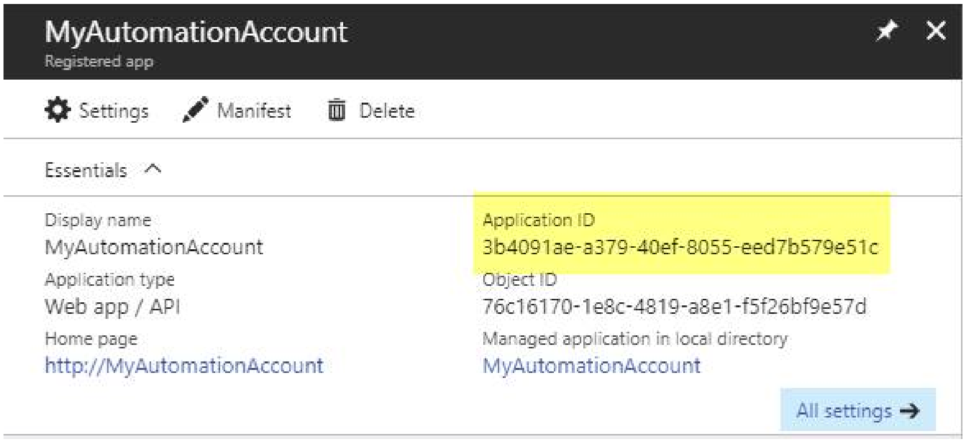
Give Consent

After providing the application with the "Read directory data" permission, you have to provide consent, only once, by navigating the following URL.

https://login.microsoftonline.com/**xxxxtelive.onmicrosoft.com**/oauth2/authorize?client_id=**3b4091ae-a379-40ef-8055-eed7b579e51c**&;response_type=code&resource=https://graph.windows.net&prompt=admin_consent

The operation must be performed by an Azure AD admin.

Make sure to replace the tenant with your domain, and the client_id with the Application ID from the app registration:



Display name
MyAutomationAccount

Application ID
3b4091ae-a379-40ef-8055-eed7b579e51c

Application type
Web app / API

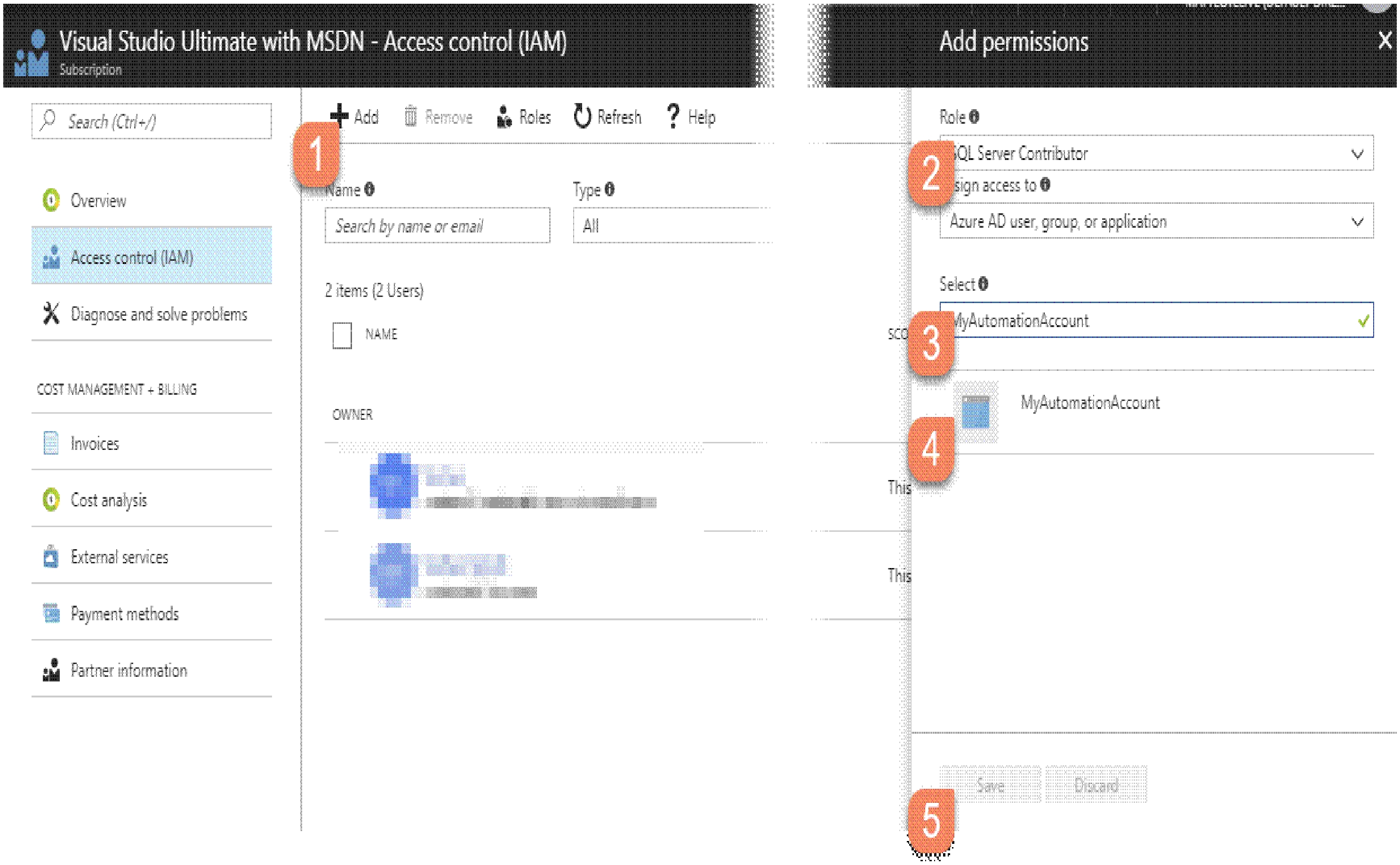
Object ID
76c16170-1e8c-4819-a8e1-f5f26bf9e57d

Home page
http://MyAutomationAccount

Managed application in local directory
MyAutomationAccount

Assign the service principal to the SQL Server Contributor role

The service principal needs the SQL Server Contributor role to set the Azure AD Admin.



Role: SQL Server Contributor

Assign access to: Azure AD user, group, or application

Select: MyAutomationAccount

MyAutomationAccount

Assign the Azure AD admin in PowerShell using the service account

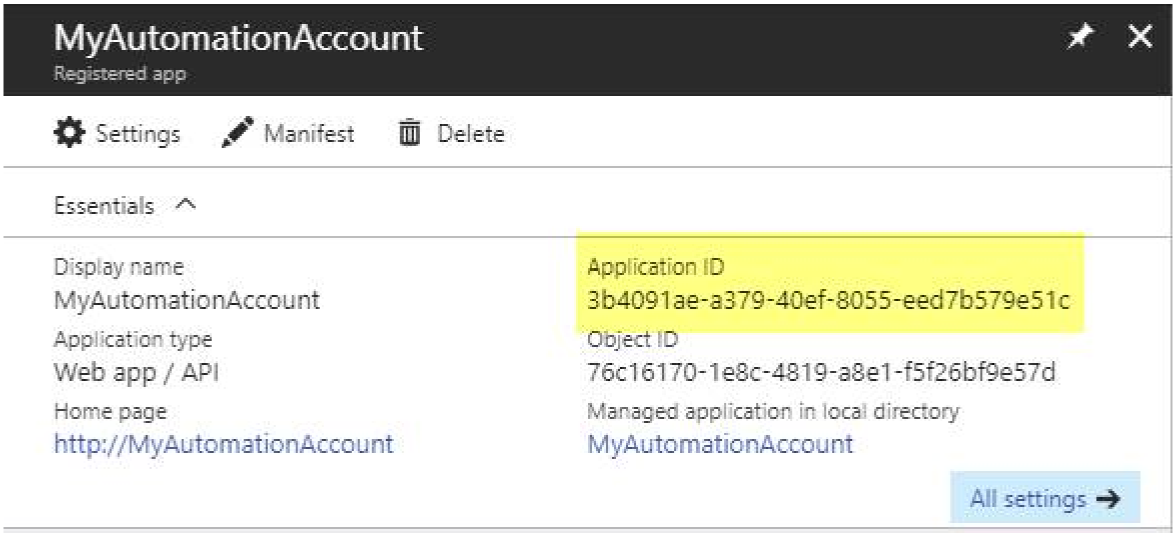
This script is the minimum required to assign an Azure AD in PowerShell using a service account.

```
ApplicationId = "3b4091ae-a379-40ef-8055-eed7b579e51c"
$ApplicationKey = "srClxw2vxtLDIaNlAgZ7Bd7g2+GAmFjJdzIlK8xcn7I="
$TenantId = "Input TenantId here"
$ResourceGroup = "test"
$ServerName = "mtlvwesql1"
$Admin = "dbadmin@xxxxlive.onmicrosoft.com"

$pwd = ConvertTo-SecureString $ApplicationKey -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential($ApplicationId, $pwd)
Login-AzurermAccount -Credential $cred -ServicePrincipal -TenantId $TenantId
Set-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName $ResourceGroup -ServerName $ServerName -Di
```

I specified the service principals credentials in clear-text. If you plan to use Azure Automation or similar tools to automate the script, please rely on their features to safely store secrets.

The application ID is available in the app registration blade on the Azure Portal.



Display name
MyAutomationAccount

Application type
Web app / API

Home page
http://MyAutomationAccount

Application ID
3b4091ae-a379-40ef-8055-eed7b579e51c

Object ID
76c16170-1e8c-4819-a8e1-f5f26bf9e57d

Managed application in local directory
MyAutomationAccount

The application key was generated earlier and you should have taken note of it as instructed.

The tenant ID is the GUID of your tenant. In case you are not sure what the tenant ID is, you can easily get it in PowerShell by running either Login-AzureRmAccount or Get-AzureRmSubscription:

```
PS C:\Users> Login-AzureRmAccount
Account : xxxxxte@live.com
SubscriptionName : Visual Studio Ultimate with MSDN
SubscriptionId : <input SubscriptionId>
TenantId : Input TenantId here
Environment : AzureCloud

PS C:\Users> Get-AzureRmSubscription

Name : Visual Studio Ultimate with MSDN

Id : e9bedced-f9ee-4f95-9631-b75ee06aa142
TenantId : Input TenantId here
State : Enabled
```

The remaining parameters identify the server, its resource group and the Azure AD user to become the Azure AD admin.

Classification

Root cause Tree - Connectivity/AAD Issue/Other AAD User / Service Principal errors

How good have you found this content?