



**TitanHQ™**

**WebTitan**

## **WebTitan Azure AD Enterprise App**

The WebTitan Azure AD Enterprise App is a built-in component of DNS Proxy. It is responsible for synchronizing Azure AD User & Groups to DNS Proxy. It regularly performs scans of the Azure sign-ins to find new sign-ins for Users. It pairs the user with the IP of the Virtual Machine that was signed into so that WebTitan Cloud can apply policies to those users.

### **Table of Contents**

1. [Prerequisites for the WebTitan AzureAD Enterprise App](#)
2. [Configure WebTitan AzureAD Enterprise App on DNS Proxy](#)
3. [Configure Multiple DNS Proxies with WebTitan AzureAD Enterprise App](#)
4. [Troubleshooting DNSProxy Deployment](#)
5. [Troubleshooting WebTitan AzureAD Enterprise App](#)

## Prerequisites for the WebTitan AzureAD Enterprise App

The WebTitan AzureAD Enterprise App requires access to the (Azure AD) reporting APIs to provide you with User sign-in data.

The WebTitan AzureAD Enterprise App uses OAuth to authorize access to the MS Azure APIs.

To Deploy DNSProxy and access the functionality of the WebTitan AzureAD Enterprise App the following has to be done:

1. [License Requirements](#)
2. [Deploying DNSProxy](#)
3. [Assign roles](#)
4. [Register DNSProxy/WebTitan AzureAD Enterprise App as an application](#)
5. [Grant API permissions](#)
6. [Add Custom Role Assignment](#)
7. [Gather configuration settings](#)

### License Requirements

To access the sign-in reports for a tenant it must have an associated Azure AD Premium license. Azure AD Premium P1 (or above) license is required to access sign-in reports for any Azure AD tenant. Alternatively, if the directory type is Azure AD B2C, the sign-in reports are accessible through the API without any additional license requirement.

### Deploying DNSProxy

DNSProxy is made available via an Azure App hosted by TitanHQ on its Azure Directory. This app needs to be made available on the target tenant to deploy DNSProxy.

#### Make DNSProxy-Distribution-Prod App available to External Organisation:

1. In the [Azure portal](#), select **Azure Active Directory** from the left navigation pane.



2. Take note of your **Tenant ID** <Tenant 2 ID>

Home > **Default Directory | Overview**  
Azure Active Directory

Switch tenant | Delete tenant | Create a tenant | What's new | Preview features | Got feedback?

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

### Default Directory

Search your tenant

**Tenant information**

- Your role: Global administrator [More info](#)
- License: Azure AD Free
- Tenant ID: [REDACTED]
- Primary domain: molloytphotmail.onmicrosoft.com

**Azure AD Connect**

- Status: Not enabled
- Last sync: Sync has never run

Navigation menu: Overview, Getting started, Preview hub, Diagnose and solve problems, Manage (Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy)

3. Open a **new tab** in your browser and enter the following **URL**:

[https://login.microsoftonline.com/<Tenant Id>/oauth2/authorize?client\\_id=a248315f-7d19-41c2-8acb-2619857956c9&response\\_type=code&redirect\\_uri=https%3A%2F%2Fwww.microsoft.com%2F](https://login.microsoftonline.com/<Tenant Id>/oauth2/authorize?client_id=a248315f-7d19-41c2-8acb-2619857956c9&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F)

Microsoft

[REDACTED]

### Permissions requested

DNSProxy-Distribution-Prod  
**unverified**

**This application is not published by Microsoft or your organization.**

This app would like to:

- Sign in and read user profile
- Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

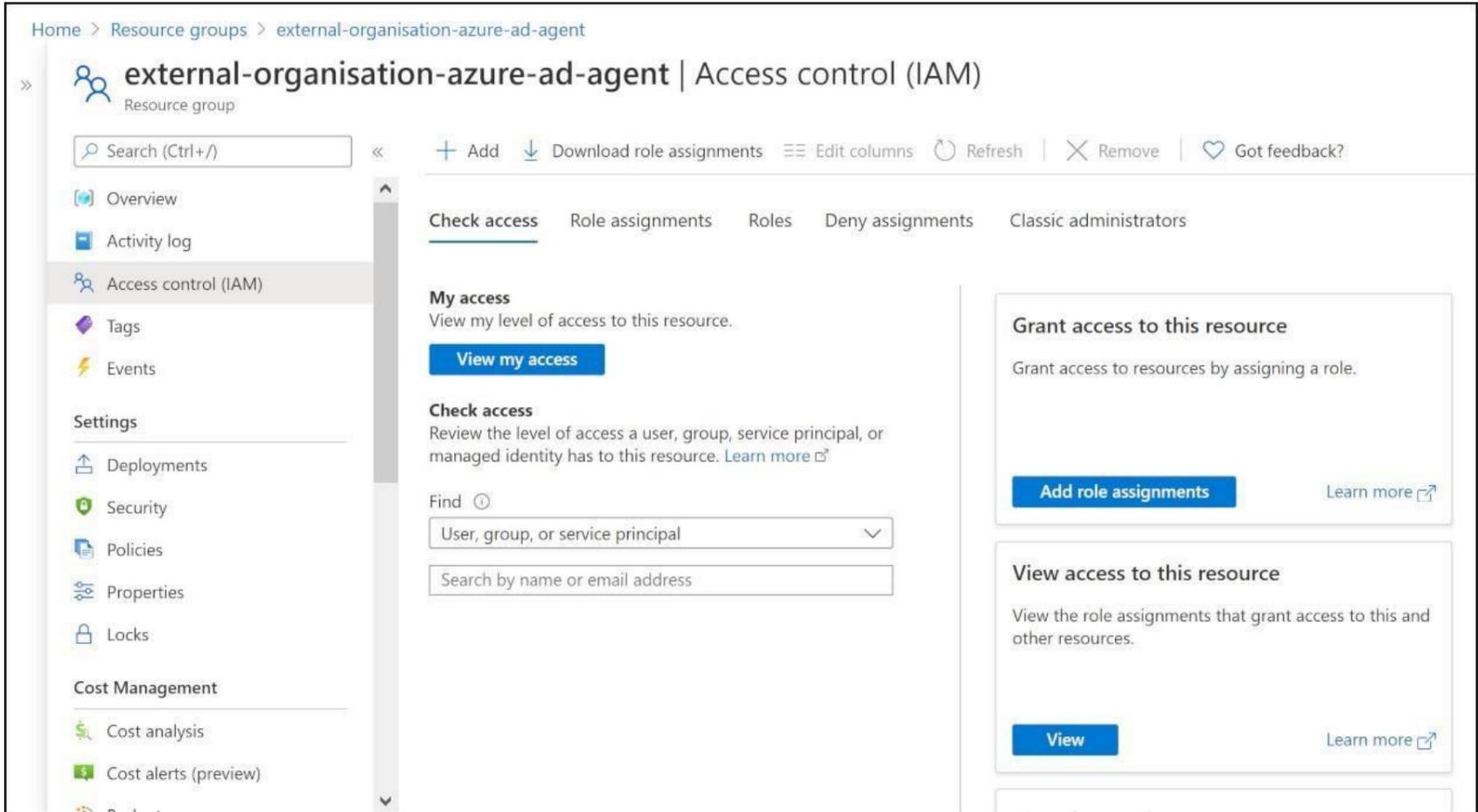
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

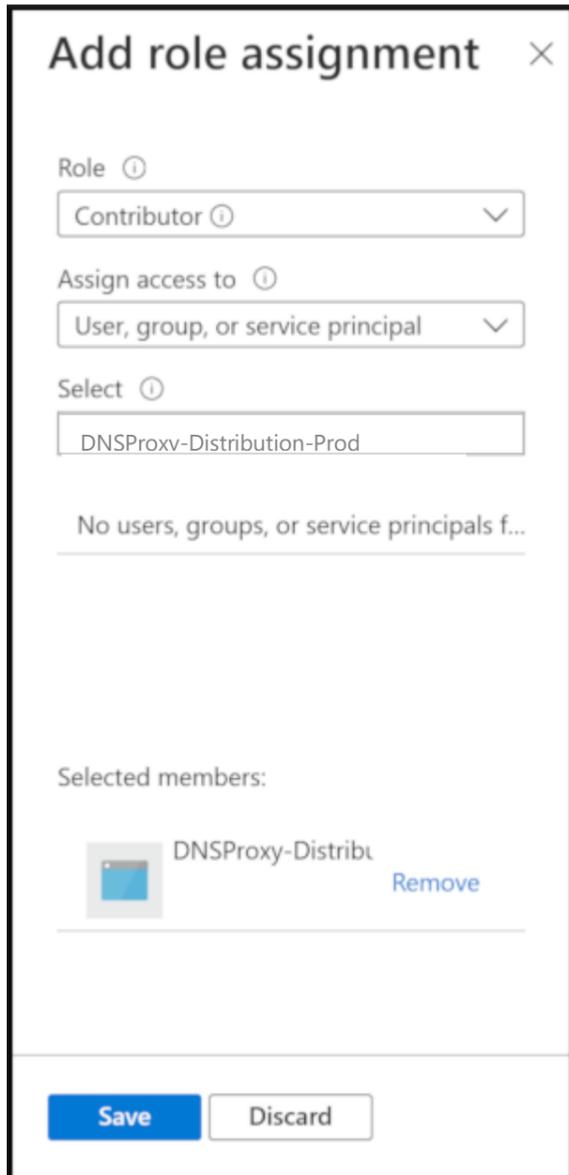
Cancel Accept

**IMPORTANT:** This will make the DNSProxy-Distribution-Prod App available to your tenant.

4. Navigate to the **resource group** you are going to **launch DNSProxy into**.



5. On the **Add role assignment** pane, add:



- a. In the **Role** dropdown, select Contributor.
- b. In the **Assign access to** dropdown, select User, group, or service principal.
- c. Select **DNSProxy-Distribution-Prod**.
- d. Click **Save**.

## Deploy DNSProxy into Resource Group of an External Organisations Tenant

IMPORTANT: You must launch DNSProxy into an existing ResourceGroup with an existing VNet & NetworkSecurityGroup. The Subnet you launch DNSProxy into must have an NSG associated with it. To access the UI HTTPS or HTTP ports must be open on the VNet. As a part Port 7780 will be open on the NSG, this port is required for DNSProxy to communicate with other DNSProxies in your Azure estate.

**NB: You must have the Azure CLI installed on the computer you run the DNSProxy Installer on. If you need to add the azure cli module to your powershell or bash shell please see Microsofts instructions which are available at [Azure CLI](#)**

**NB: You must have a default ssh key in your ~/.ssh folder (C:\Users<username>.ssh). If you do not have one you can generate one in powershell with the following command: "ssh-keygen -m PEM -t rsa -b 4096".**

The Azure DNSProxy Installer is available for download at [DNSProxy Azure Installer](#)

**When you run the Installer, it will launch a CLI where you will be asked for the following information:**

- a. Your Tenant Id.
- b. The suffix for TitanHQ-DnsProxy- VM e.g. if 1 the VM name will be TitanHQ-DnsProxy-1.
- c. Name of the existing Resource Group DNSProxy will be launched into.
- d. Name of the existing VNet DNSProxy will be launched into.
- e. Name of the existing Subnet DNSProxy will be launched into.

IMPORTANT: This will launch DNSProxy into your resource group.

## Assign roles

To get access to the reporting data through the API, you need to have one of the following roles assigned:

- Security Reader
- Security Administrator
- Global Administrator

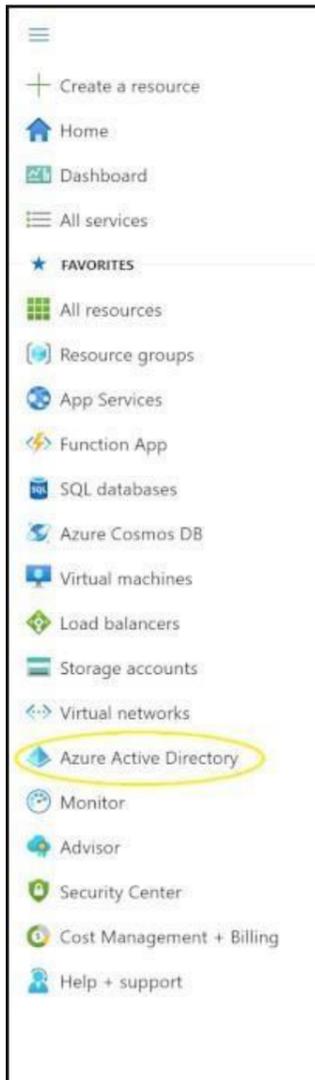
## Register DNSProxy/WebTitan AzureAD Enterprise App as an application

Registration is to access the reporting & management APIs. The registration gives you an **Application ID**, which is required for the authorization calls and enables the WebTitan AzureAD Enterprise App to receive tokens.

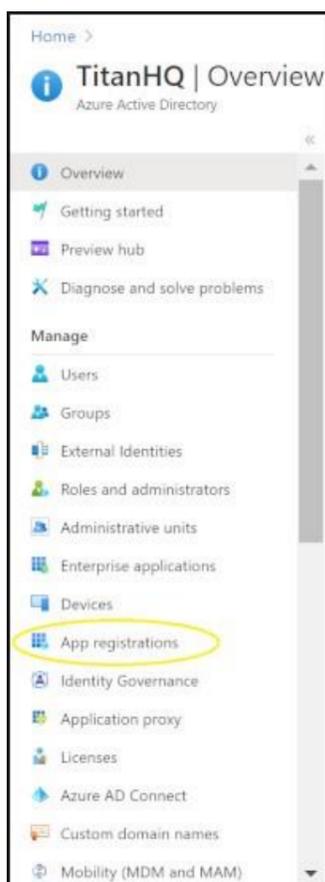
To configure your directory to access the Azure AD reporting API, you must sign in to the [Azure portal](#) with an Azure administrator account that is also a member of the **Global Administrator** directory role in your Azure AD tenant.

### To register an Azure AD application:

1. In the [Azure portal](#), select **Azure Active Directory** from the left navigation pane.



2. In the **Azure Active Directory** page, select **App registrations**.



3. From the **App registrations** page, select **New registration**.



4. The **Register an Application** page:

Home > TitanHQ >

## Register an application

**\* Name**  
The user-facing display name for this application (this can be changed later).

DNSProxy ✓

**Supported account types**  
Who can use this application or access this API?

Accounts in this organizational directory only (TitanHQ only - Single tenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)  
 Personal Microsoft accounts only

[Help me choose...](#)

**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

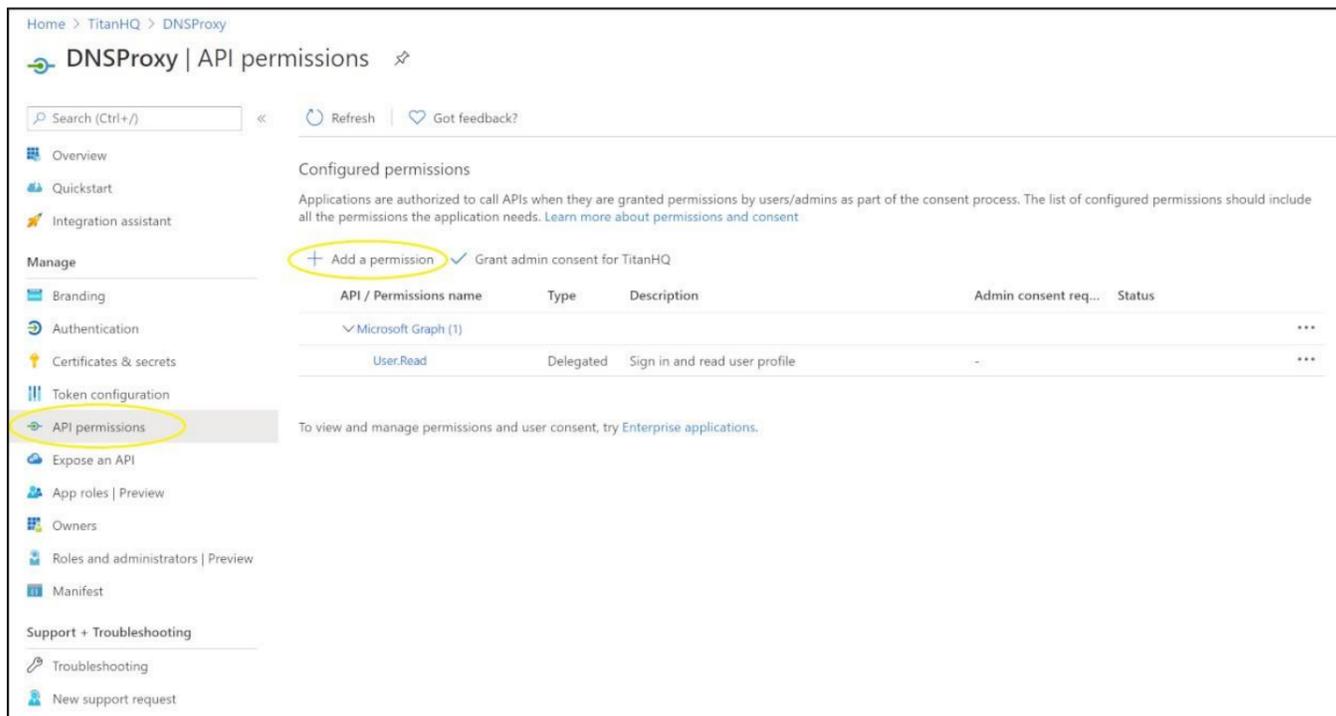
- In the **Name** textbox, type DNSProxy.
- For **Supported accounts type**, select **Accounts in this organizational directory only**.
- In the **Redirect URL** leave it blank.
- Select **Register**.

### Grant API permissions

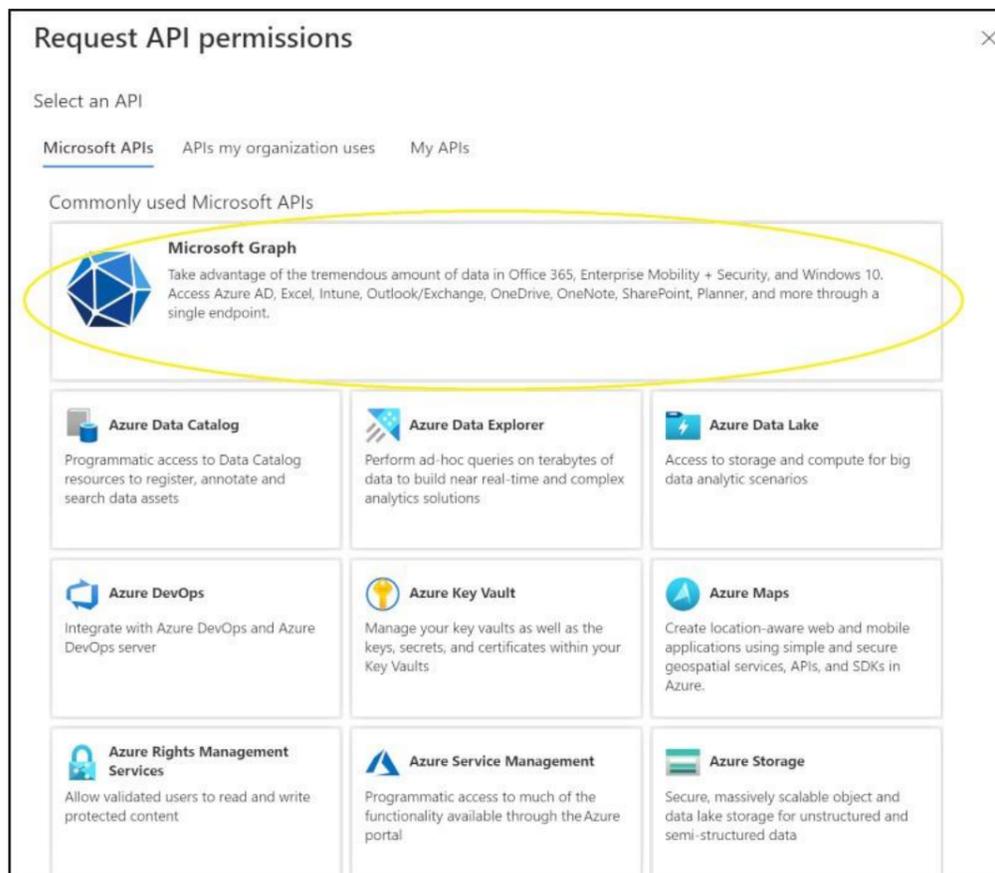
You need to grant your app the following permissions:

API	Permission
Microsoft Graph	User.Read.All
Microsoft Graph	Group.Read.All
Microsoft Graph	AuditLog.Read.All
Azure Service Management	user_impersonate

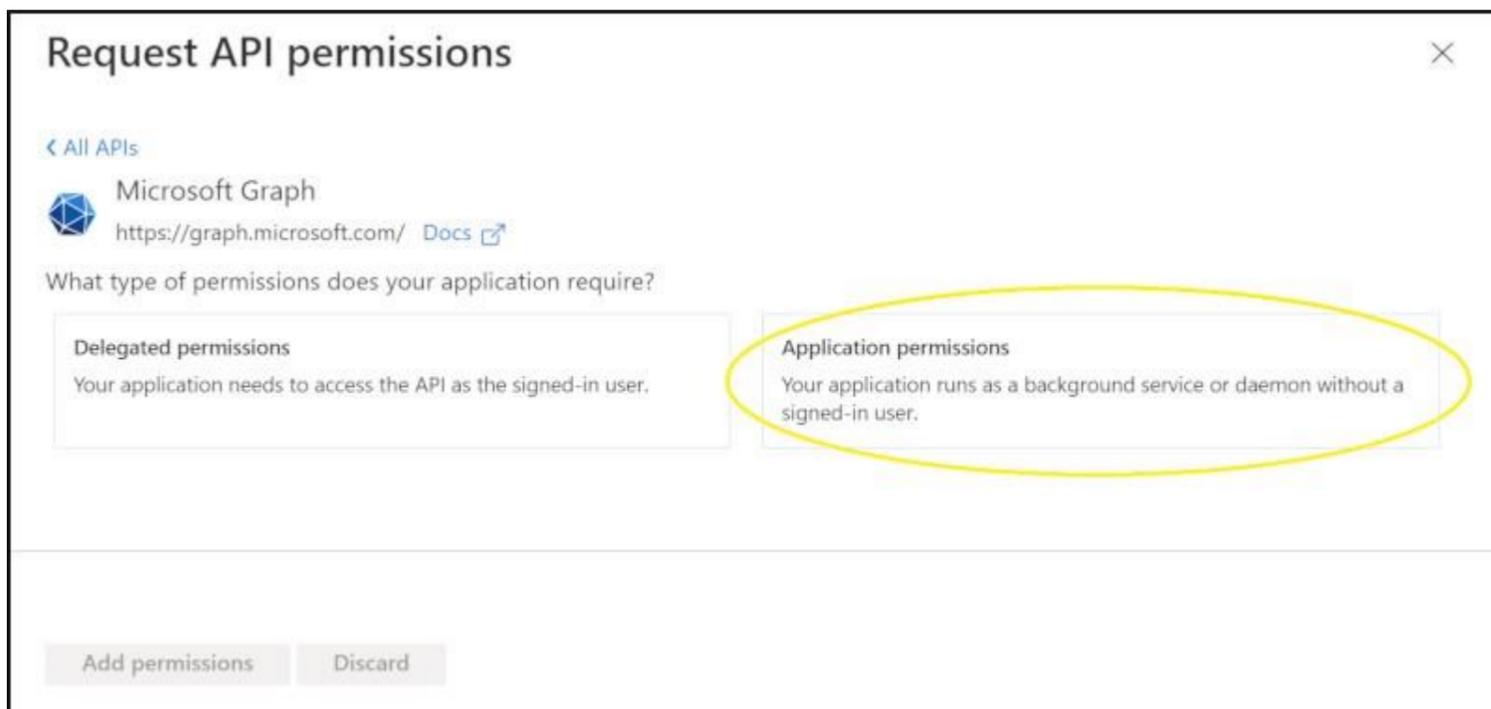
1. Select **API permissions** then **Add a permission**.



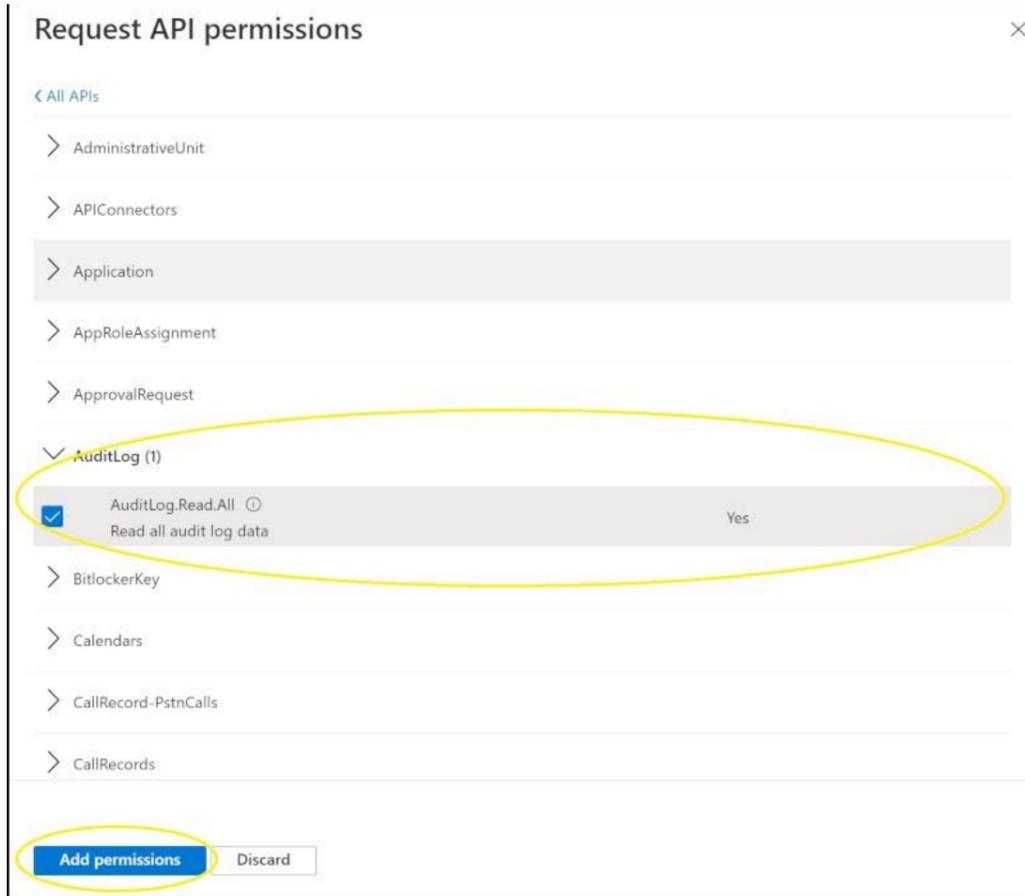
2. On the **Request API permissions page**, locate **Microsoft Graph**.



3. On the **Required permissions** page, select **Application Permissions**.



4. Expand **AuditLog** checkbox **AuditLog.ReadAll**.

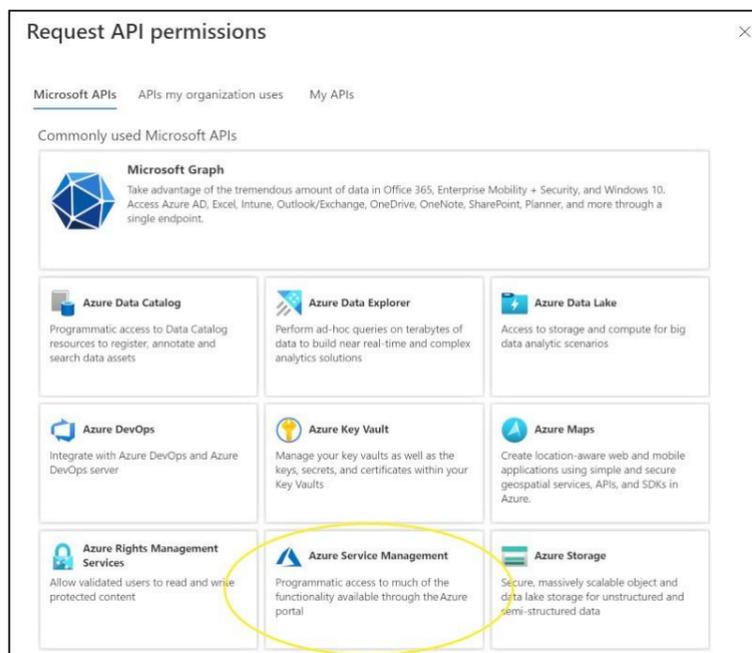


a. Expand **User** checkbox **User.Read.All**

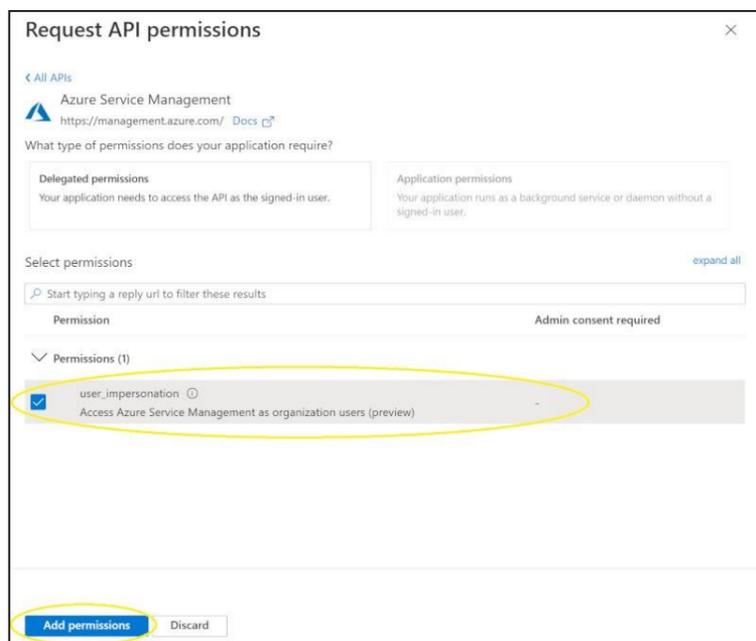
b. Expand **Group** checkbox **Group.Read.All**

c. Select **Add permissions**.

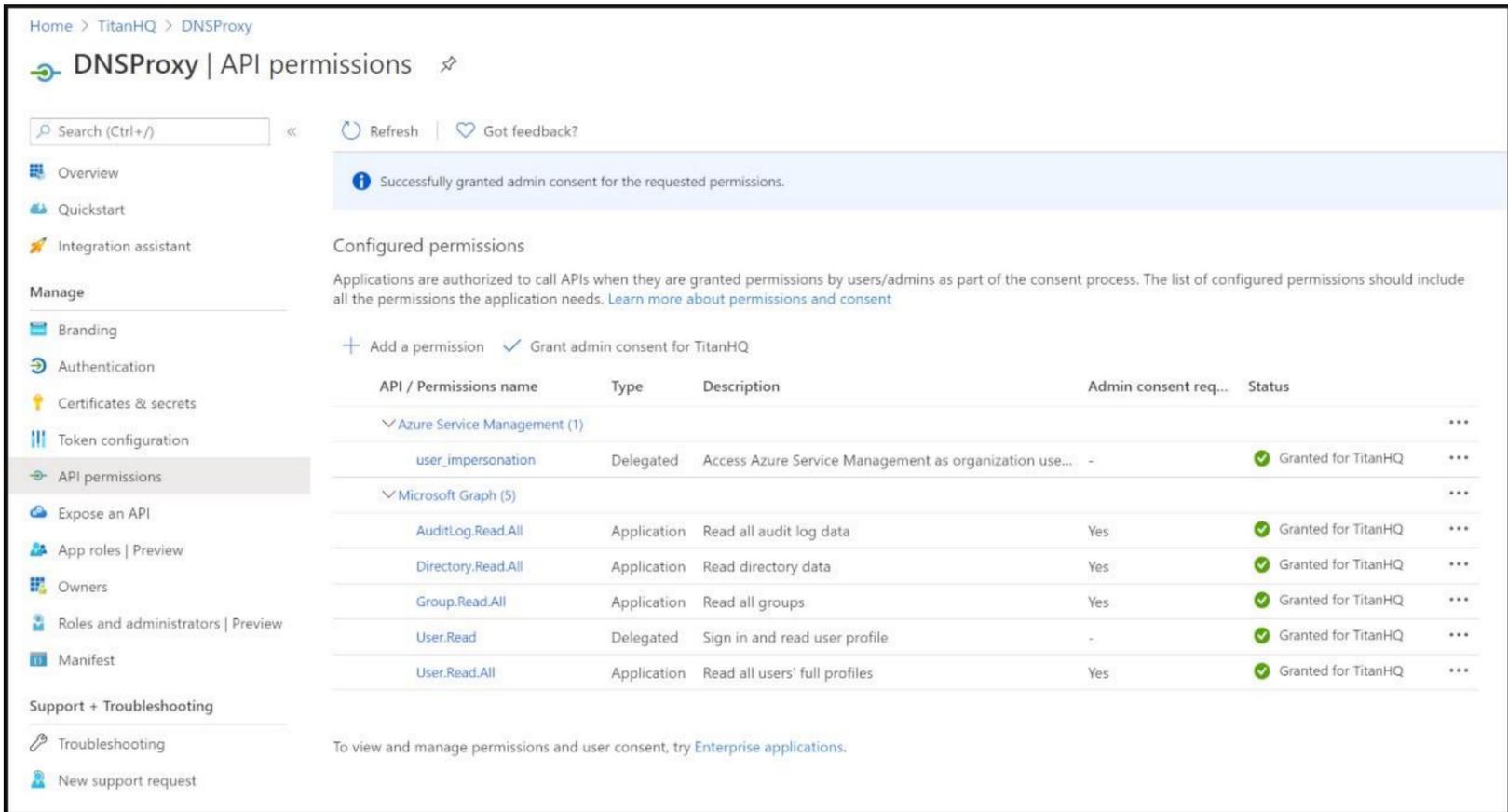
5. On the **Request API permissions** page, locate **Azure Service Management**.



6. Expand **Permissions** checkbox **user\_impersonate** and Select **Add permissions**.



7. On the **DNSProxy Application - API Permissions** page, select **Grant admin consent**.



Home > TitanHQ > DNSProxy

## DNSProxy | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Successfully granted admin consent for the requested permissions.

### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for TitanHQ

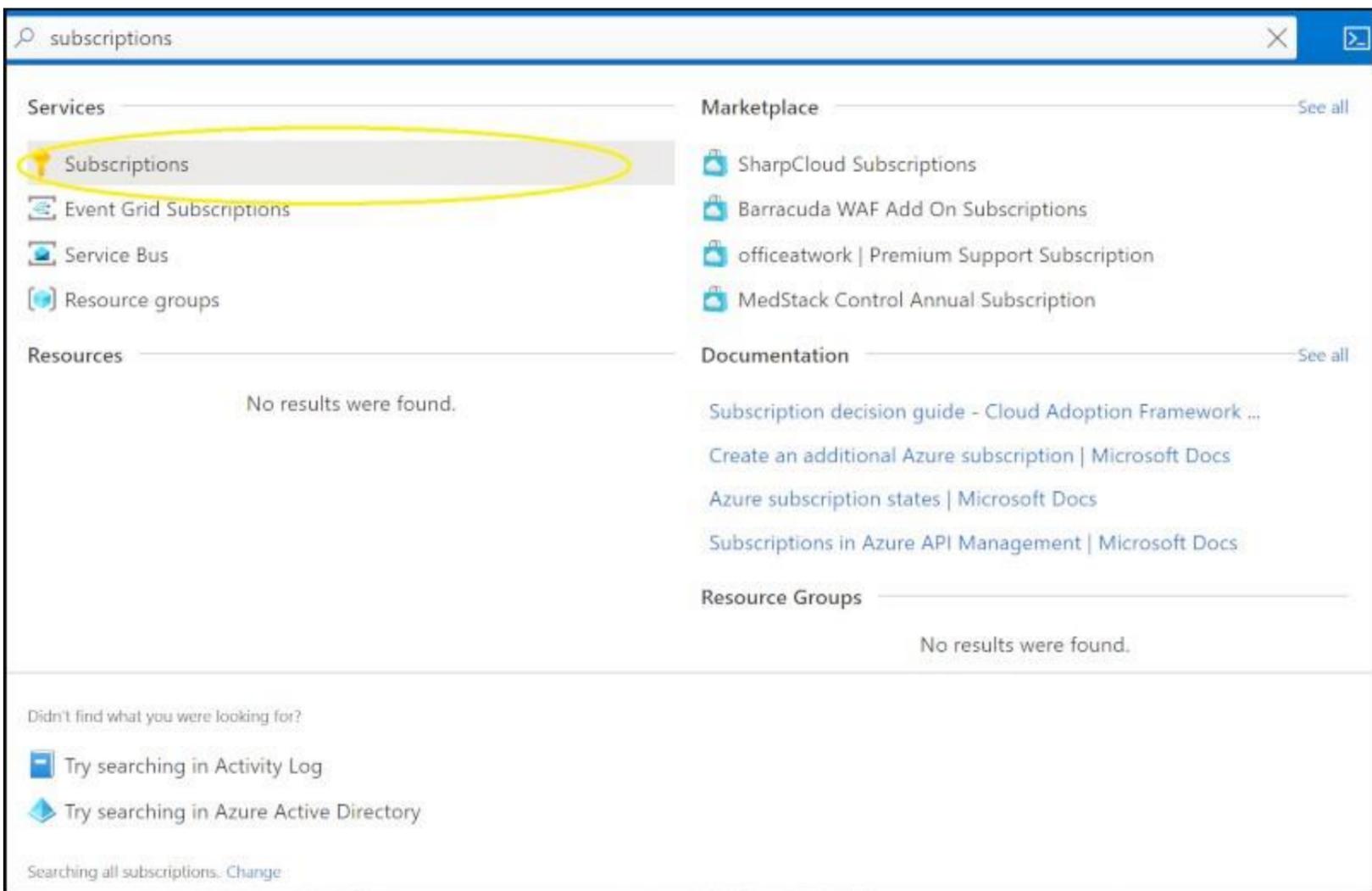
API / Permissions name	Type	Description	Admin consent req...	Status
▼ Azure Service Management (1)				
user_impersonation	Delegated	Access Azure Service Management as organization use...	-	✓ Granted for TitanHQ
▼ Microsoft Graph (5)				
AuditLog.Read.All	Application	Read all audit log data	Yes	✓ Granted for TitanHQ
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for TitanHQ
Group.Read.All	Application	Read all groups	Yes	✓ Granted for TitanHQ
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for TitanHQ
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for TitanHQ

To view and manage permissions and user consent, try [Enterprise applications](#).

## Add Custom Role Assignment

Custom roles are used to harden access of the DNSProxy application rather than using the Azure built-in permission which are currently more liberal with access rights.

1. In the **Search Bar** type **subscriptions**, Select **subscriptions** from the results.



subscriptions

Services

- Subscriptions**
- Event Grid Subscriptions
- Service Bus
- Resource groups

Resources

No results were found.

Marketplace

- SharpCloud Subscriptions
- Barracuda WAF Add On Subscriptions
- officeatwork | Premium Support Subscription
- MedStack Control Annual Subscription

Documentation

- Subscription decision guide - Cloud Adoption Framework ...
- Create an additional Azure subscription | Microsoft Docs
- Azure subscription states | Microsoft Docs
- Subscriptions in Azure API Management | Microsoft Docs

Resource Groups

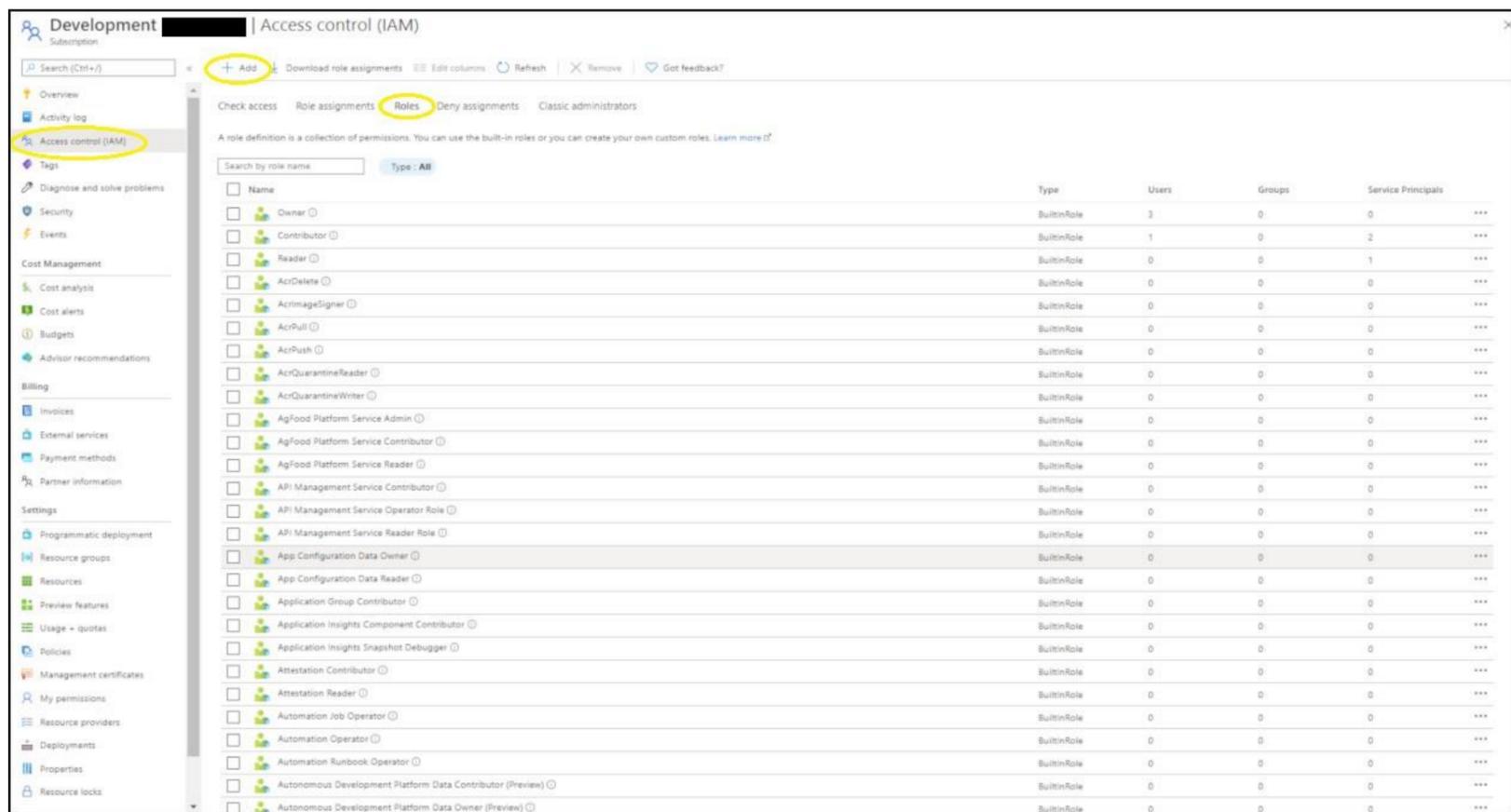
No results were found.

Didn't find what you were looking for?

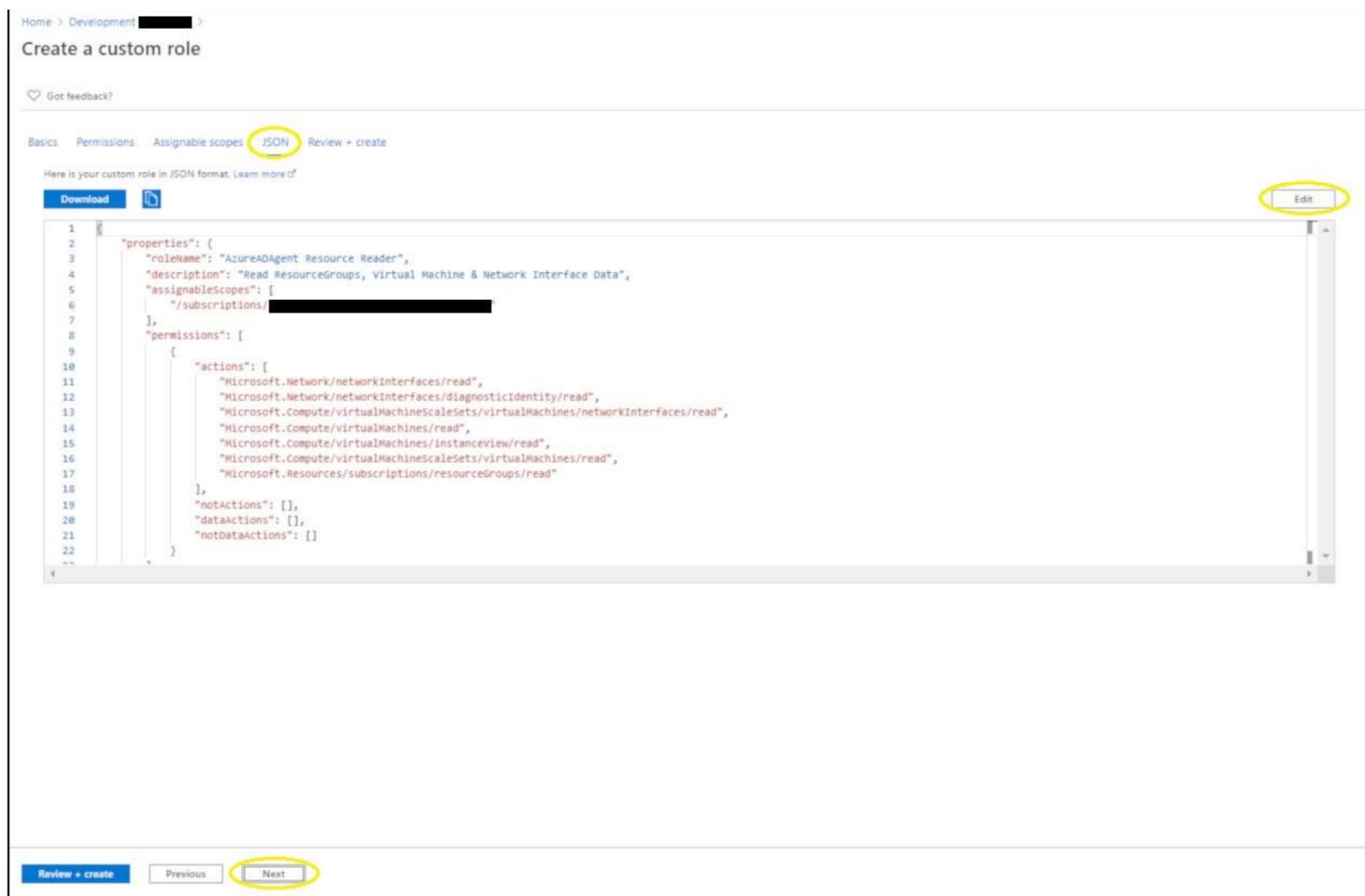
- Try searching in Activity Log
- Try searching in Azure Active Directory

Searching all subscriptions. [Change](#)

2. On the **Subscriptions** page, locate **Access control (IAM)**, Select **Roles**, Click on **+ Add**, and Select **Add custom role**.



3. On the **Custom Role page**, Select **JSON**, and Click on **Edit**.



a. Copy & paste the following JSON into the text box. b. Click on **Next**

```

{
  "properties": {
    "roleName": "AzureADAgent Resource Reader",
    "description": "Read ResourceGroups, Virtual Machine & Network Interface Data",
    "assignableScopes": [
      "/subscriptions/3f51630f-4c88-4fba-b57a-5c39b5662a2f"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/networkInterfaces/read",
          "Microsoft.Network/networkInterfaces/diagnosticIdentity/read",
          "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/read",

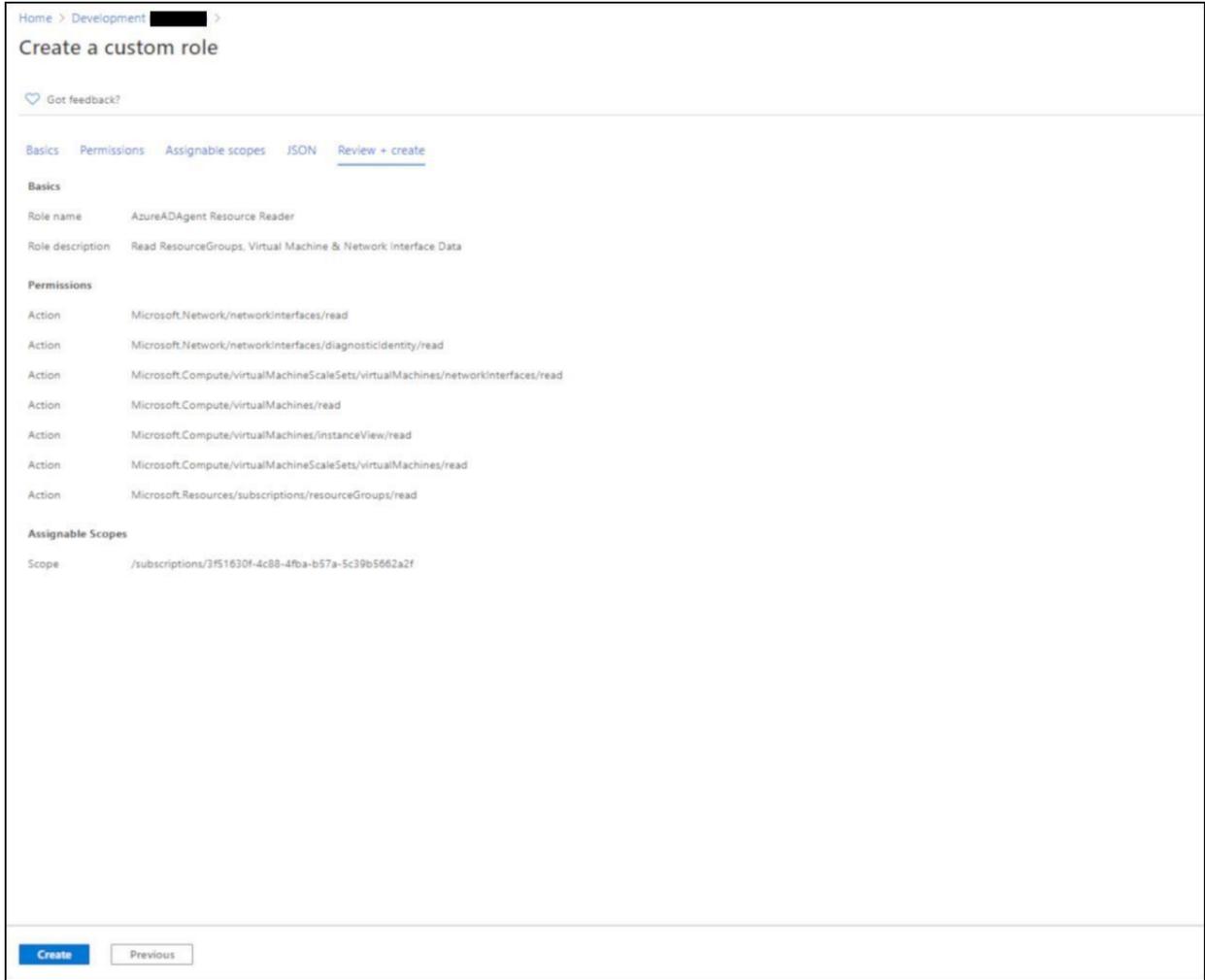
```

```

    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read"
  ],
  "notActions": [],
  "dataActions": [],
  "notDataActions": []
}
]
}
}

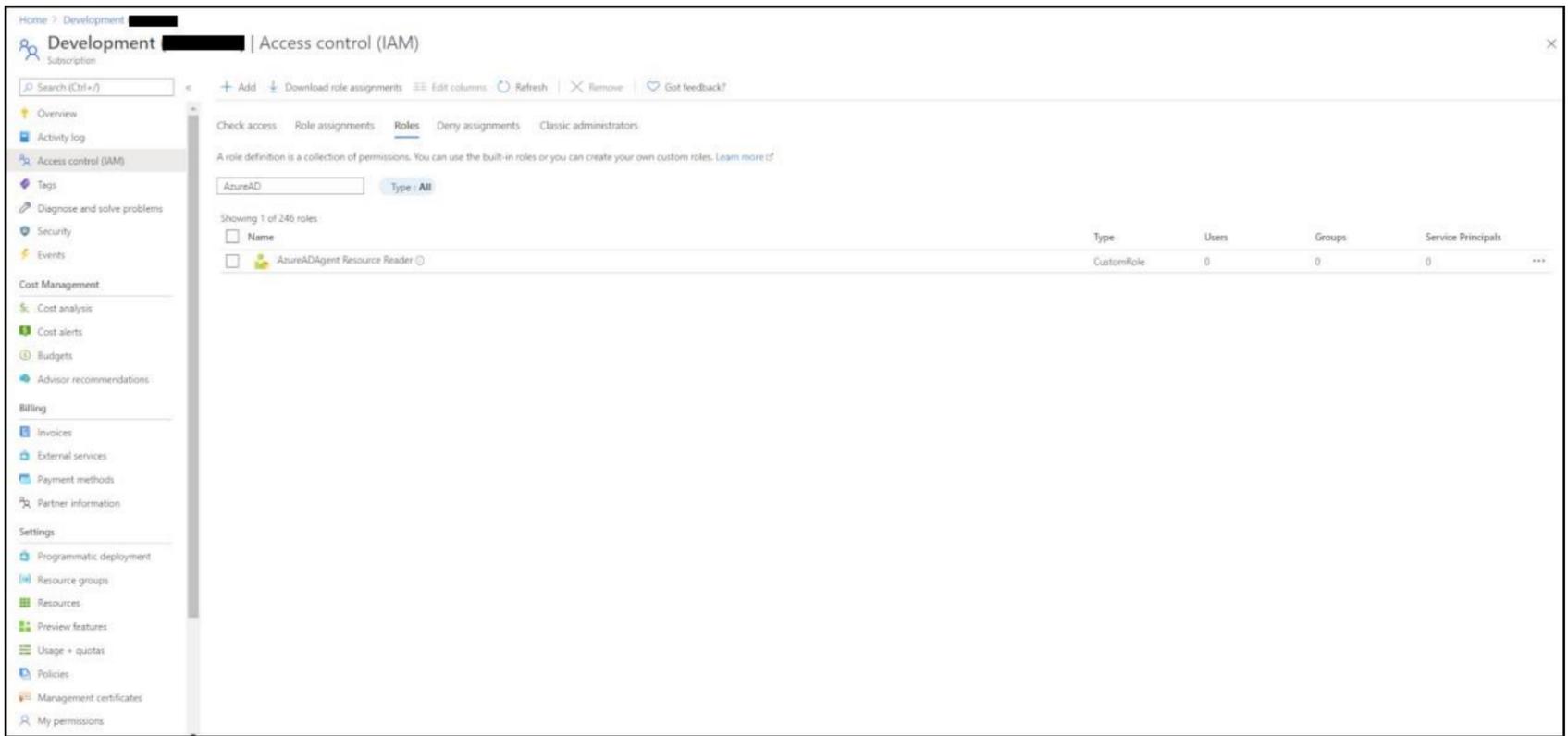
```

4. Select **Create**.

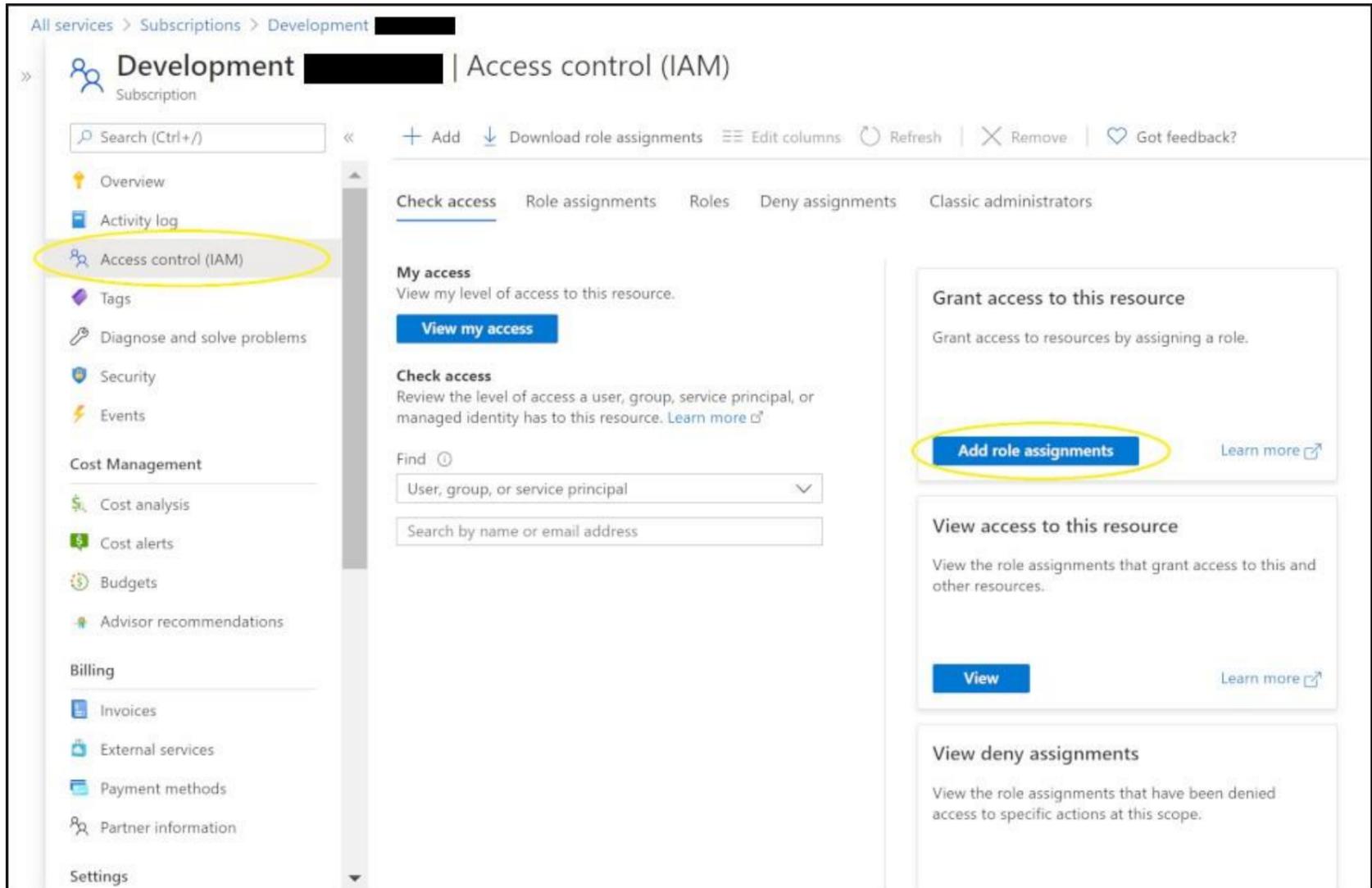


On the **Subscriptions** page, locate **Access control (IAM)**, Select **Roles**, In the roles search bar type **AzureADAgent Resource Reader**.

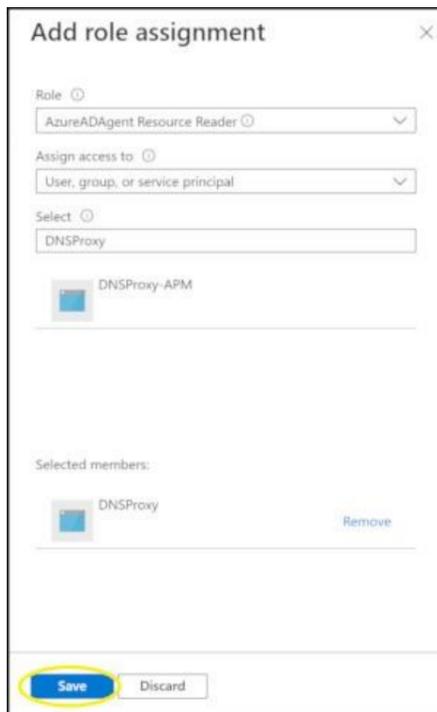
IMPORTANT: It may take a few minutes for the custom role to propagate everywhere in the tenant.



5. On the **Subscriptions** page, locate **Access control (IAM)** and Select **Add Role Assignment**.



6. On the **Add role assignment** pane, add:



- a. In the **Role** dropdown, select AzureADAgent Resource Reader.
- b. In the **Assign access to** dropdown, select User, group, or service principal.
- c. Select **DNSProxy**.
- d. Click **Save**.

## Gather configuration settings

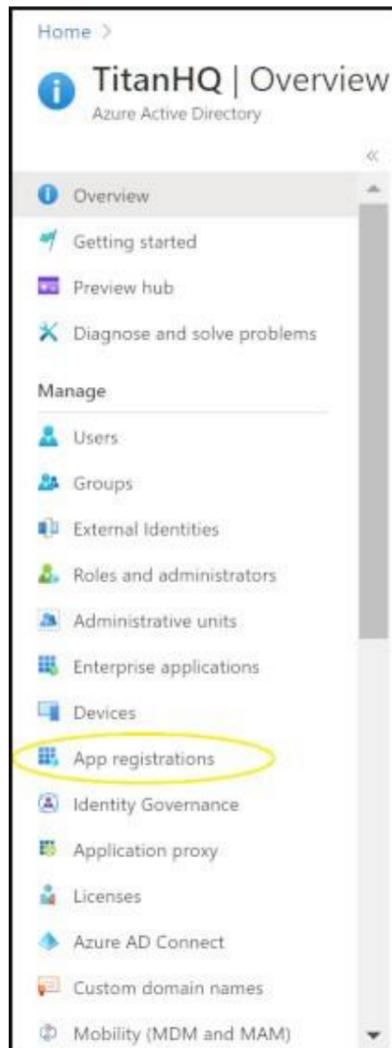
This section shows you how to get the following settings for your tenant:

- Client ID
- Client secret

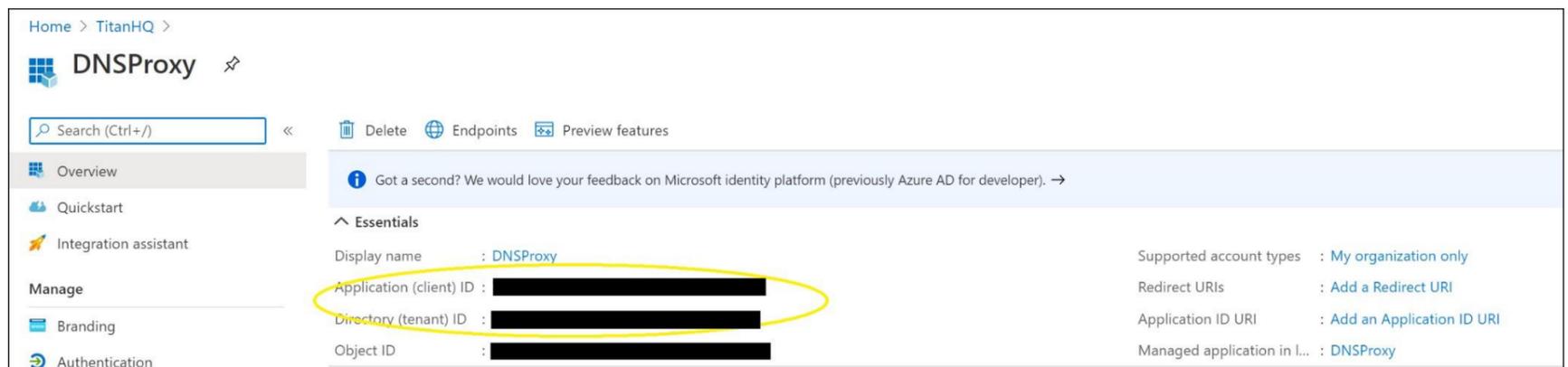
## Get your application's client ID

### To get your application's client ID:

1. In the [Azure portal](#), on the left navigation pane, click **Azure Active Directory**.
2. Select your application from the **App Registrations** page.



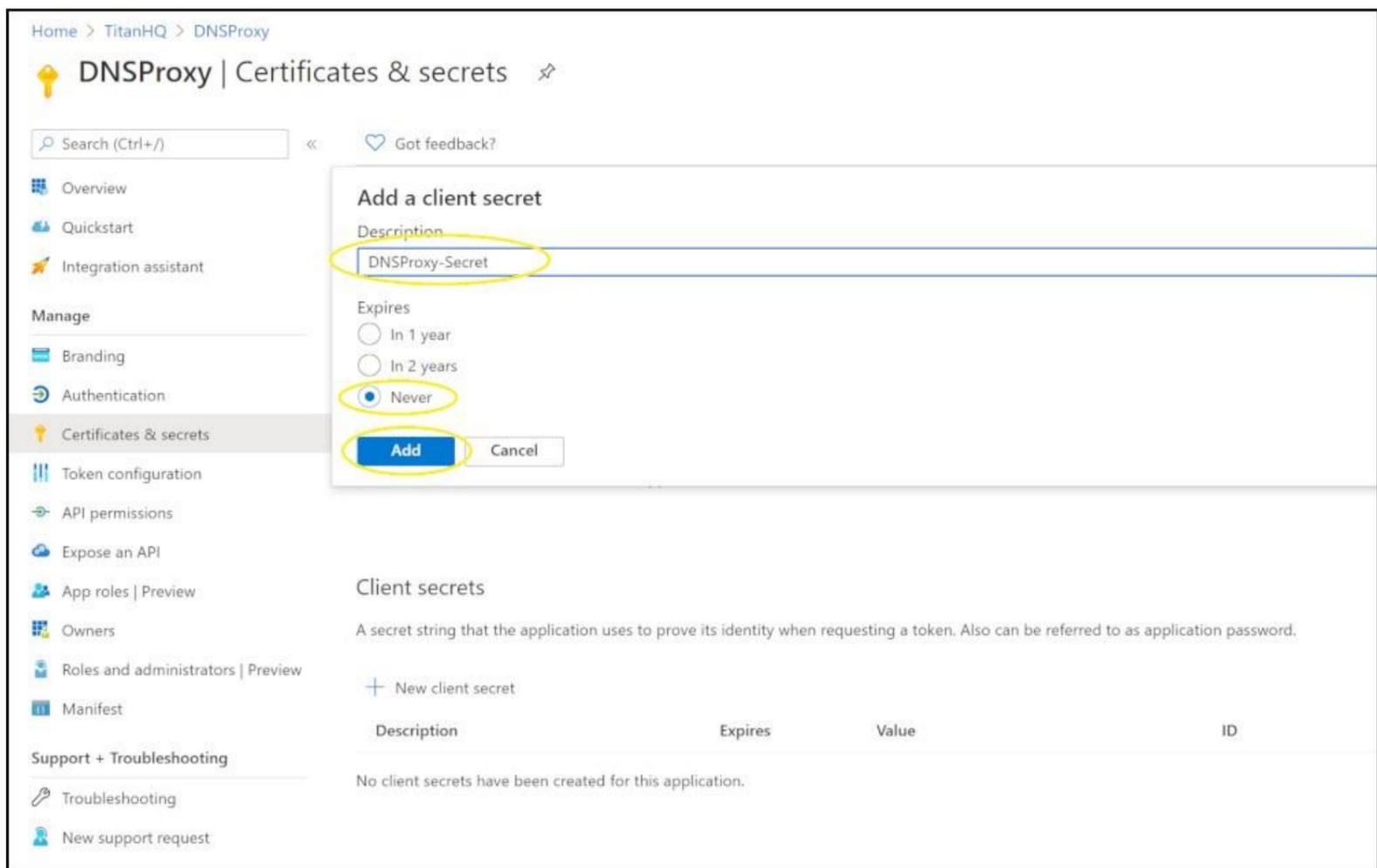
3. Take note of your **Client ID**.



## Get your application's client secret

### To get your application's client secret:

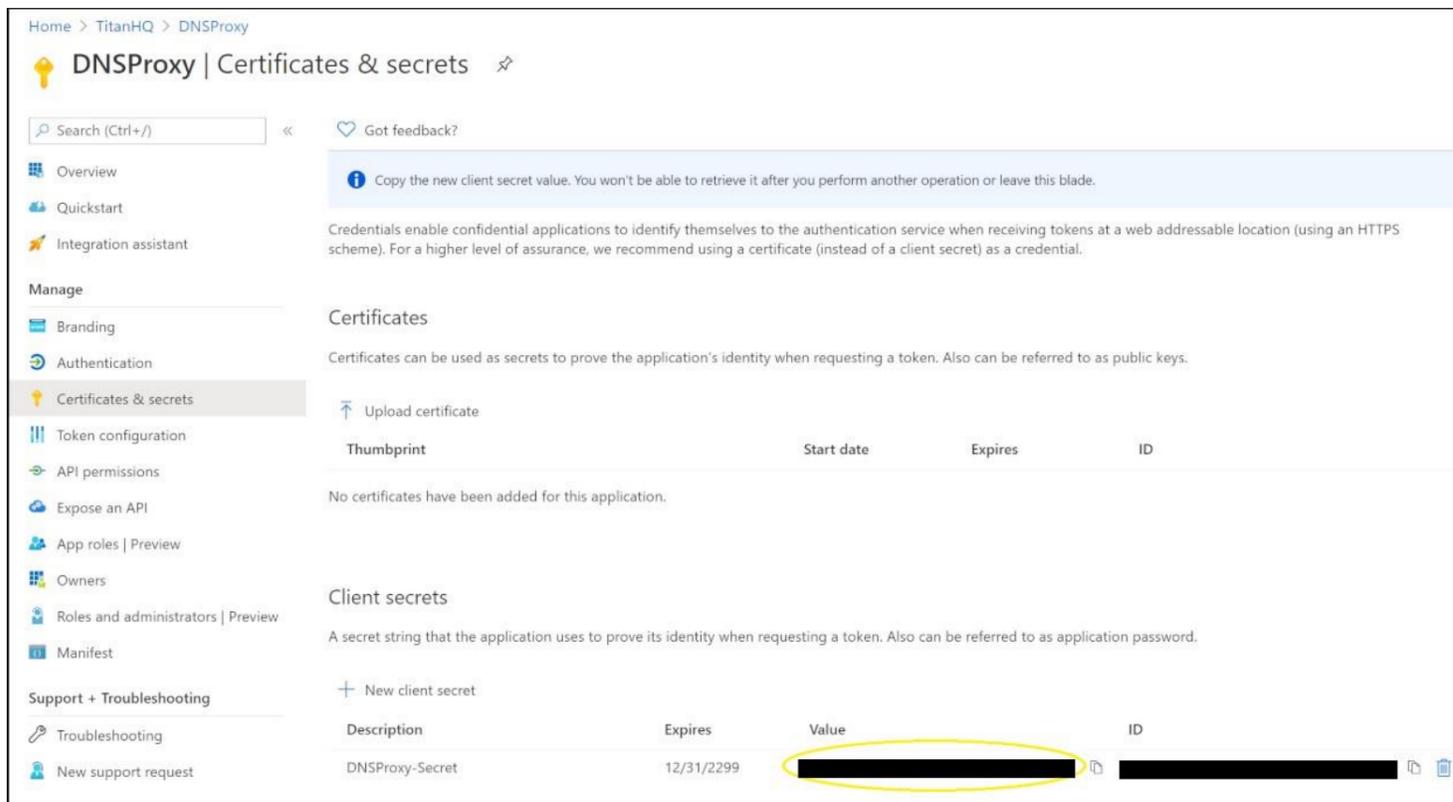
1. Select **Certificates and Secrets** on the **API Application** page, in the **Client Secrets** section, click **+ New Client Secret**.



2. On the **Add a client secret** page, add:

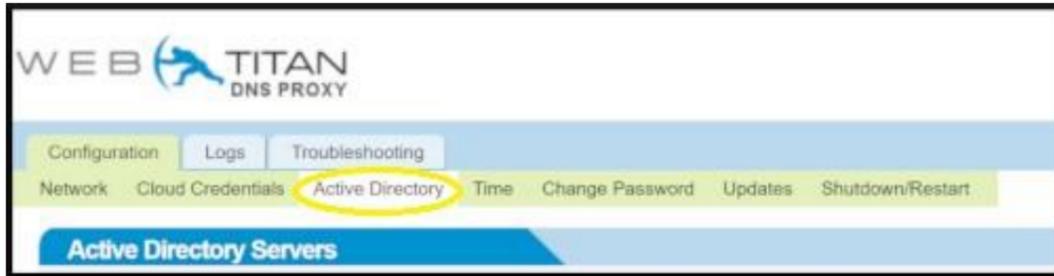
- In the **Description** textbox, type DNSProxy Secret.
- As **Expires**, select **Never**.
- Click **Save**.
- Copy the key value.

3. Take note of your **client secret**.

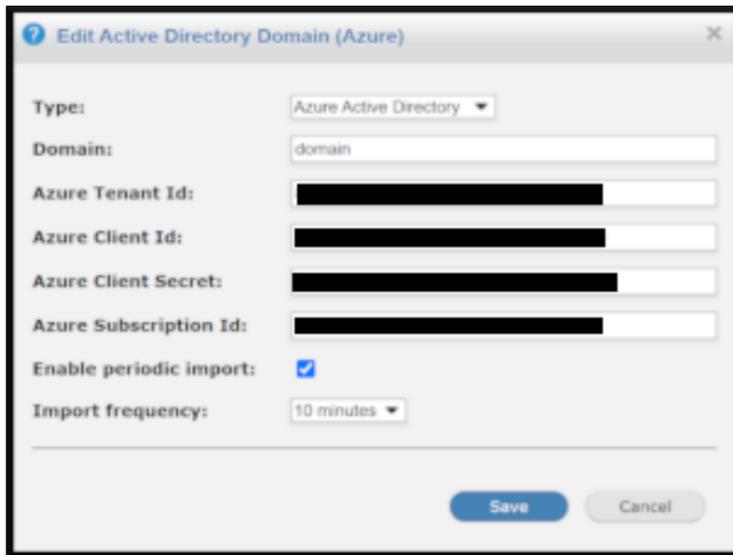


# Configure WebTitan Azure AD Enterprise App on DNS Proxy

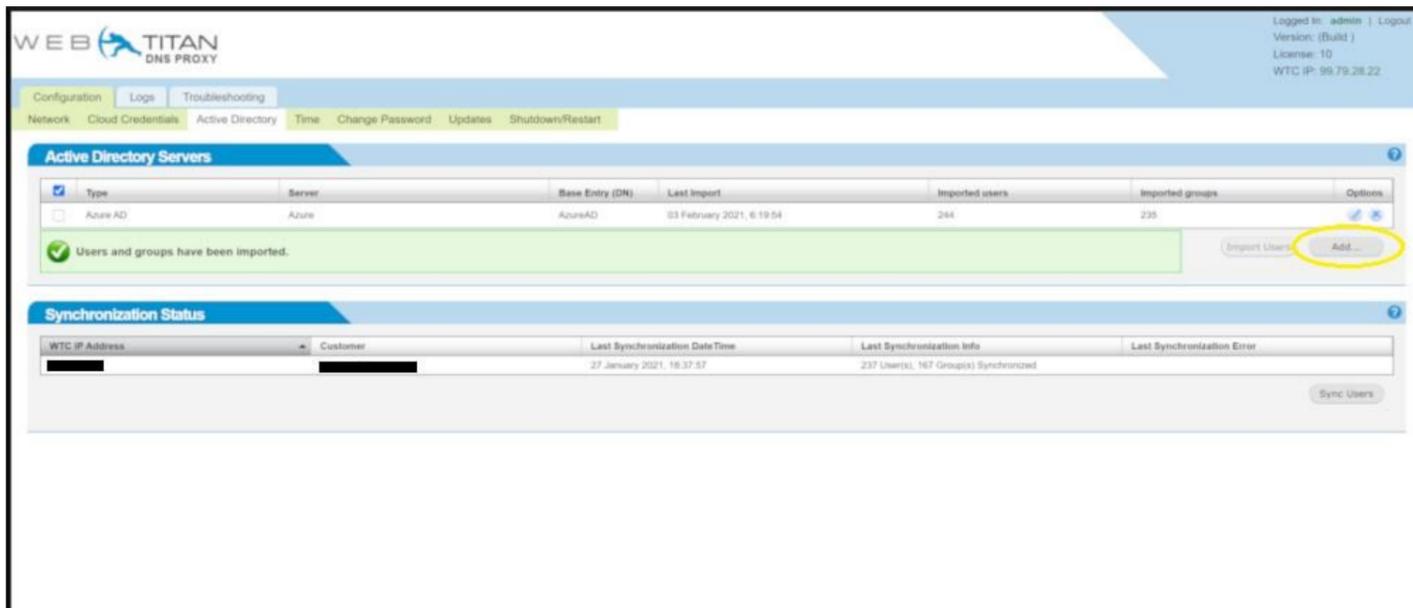
1. On your DNSProxy locate **Active Directory** and Click on **Add**.



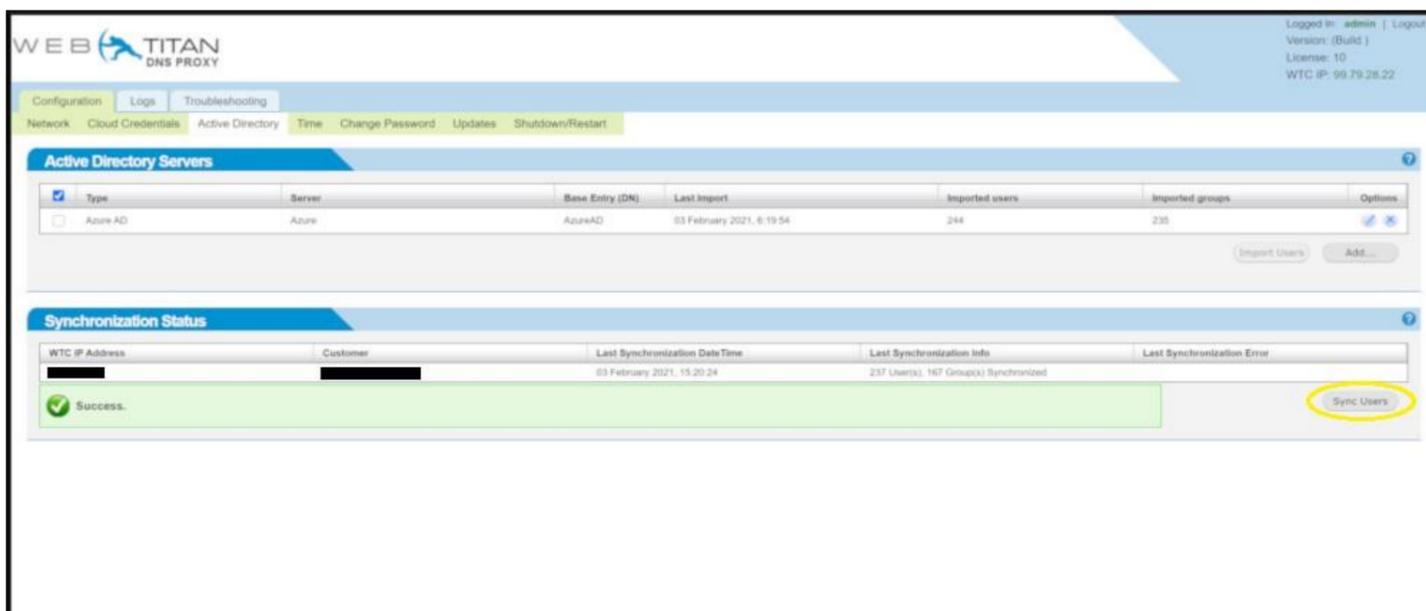
2. On the **Add Active Directory** modal Select **Azure Active Directory** from the dropdown menu.



3. On the **Active Directory Servers** table Select Azure AD tickbox and Click on **Import Users**.



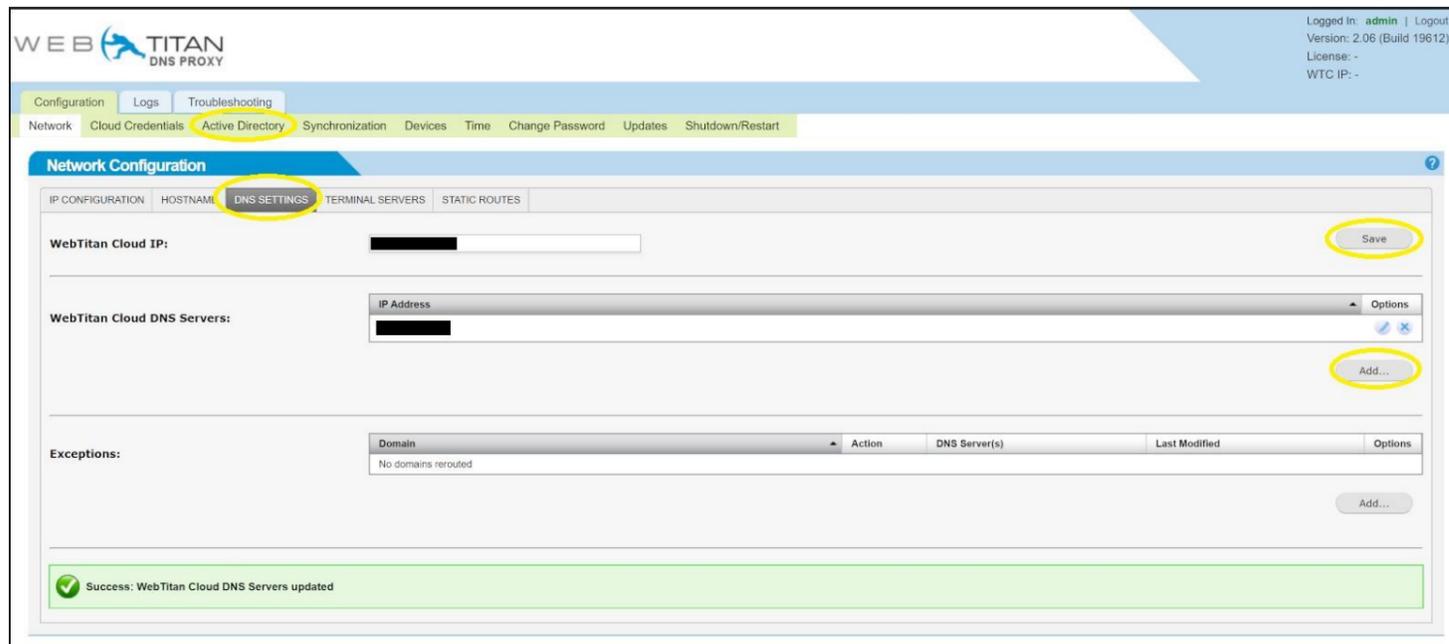
4. On the **Synchronization Status** table Click on **Import Users**.



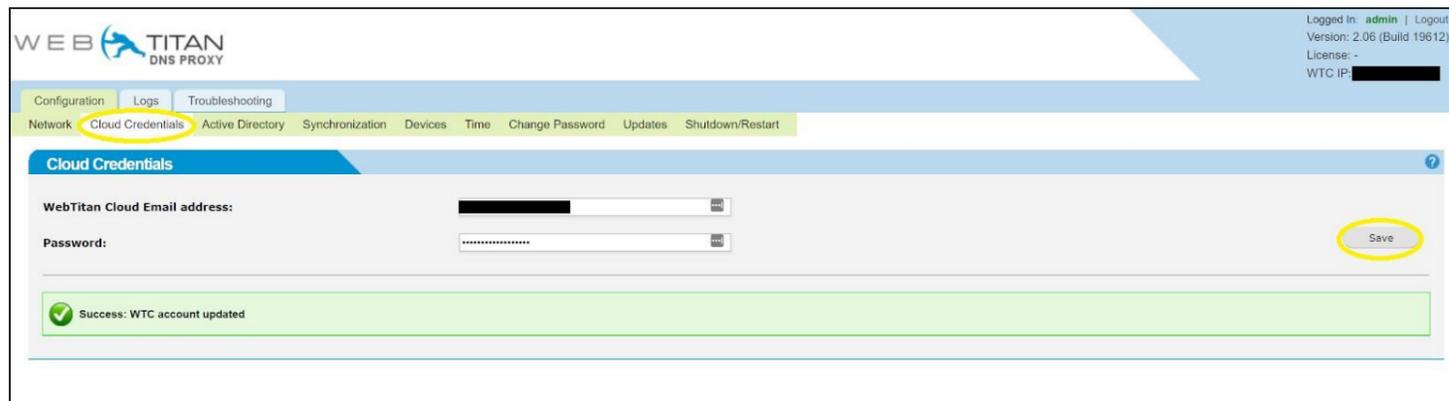
# Configure Multiple DNSProxies with WebTitan AzureAD Enterprise App

## Primary DNSProxy Basic Setup

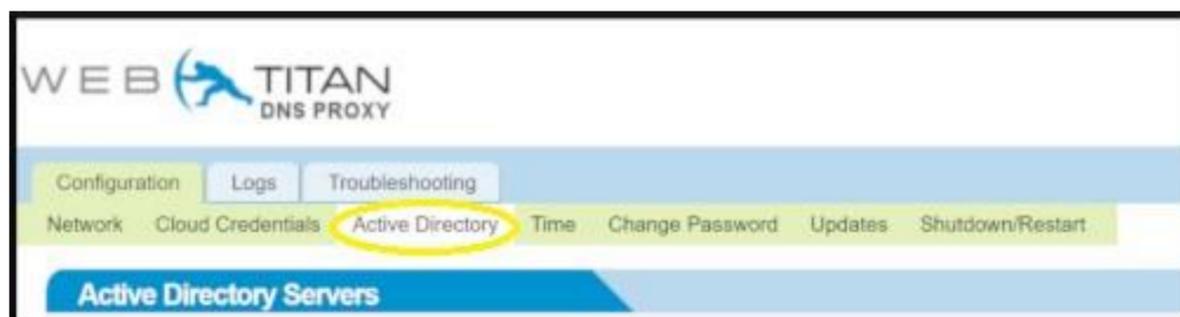
1. On your DNSProxy locate **Network->DNS Settings** a. Enter your **WebTitan Cloud IP** in the text area and Click **Add** b. Click **Add** in the **WebTitan Cloud DNS Servers** section and Enter your WTC IP into the modal box.



2. Locate the **Cloud Credentials** tab, enter the credentials of **Customer Account from your WTC** & Click **Save**



3. On your DNSProxy locate **Active Directory** and Click on **Add**.



4. On the **Add Active Directory** modal Select **Active Directory** from the dropdown menu.



5. On the **Add Active Directory** modal Select **Azure Active Directory** from the dropdown menu.

**Edit Active Directory Domain (Azure)**

Type: Azure Active Directory

Domain: [Redacted]

Azure Tenant Id: [Redacted]

Azure Client Id: [Redacted]

Azure Client Secret: [Redacted]

Azure Subscription Id: [Redacted]

Enable periodic import:

Import frequency: 24 hours

Save Cancel

## Secondary DNSProxy Basic Setup

1. On your DNSProxy locate **Network->DNS Settings** a. Enter your **WebTitan Cloud IP** in the text area and Click **Add** b. Click **Add** in the **WebTitan Cloud DNS Servers** section and Enter your WTC IP into the modal box.

WEB TITAN DNS PROXY

Logged In: admin | Logout  
Version: 2.06 (Build 19612)  
License: -  
WTC IP: -

Configuration | Logs | Troubleshooting

Network | Cloud Credentials | Active Directory | Synchronization | Devices | Time | Change Password | Updates | Shutdown/Restart

**Network Configuration**

IP CONFIGURATION | HOSTNAME | **DNS SETTINGS** | TERMINAL SERVERS | STATIC ROUTES

WebTitan Cloud IP: [Redacted] Save

WebTitan Cloud DNS Servers:

IP Address [Redacted] Options

Add...

Exceptions:

Domain	Action	DNS Server(s)	Last Modified	Options
No domains rerouted				

Add...

Success: WebTitan Cloud DNS Servers updated

2. Locate the **Cloud Credentials** tab, enter the credentials of **Customer Account from your WTC** & Click **Save**

WEB TITAN DNS PROXY

Logged In: admin | Logout  
Version: 2.06 (Build 19612)  
License: -  
WTC IP: [Redacted]

Configuration | Logs | Troubleshooting

Network | **Cloud Credentials** | Active Directory | Synchronization | Devices | Time | Change Password | Updates | Shutdown/Restart

**Cloud Credentials**

WebTitan Cloud Email address: [Redacted]

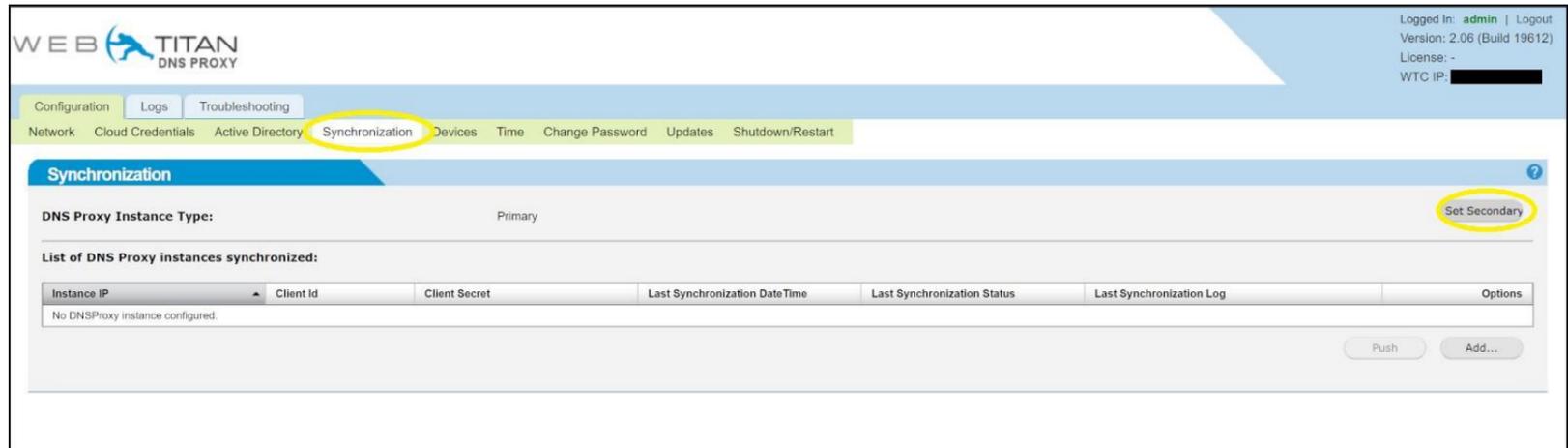
Password: [Redacted]

Save

Success: WTC account updated

## Secondary DNSProxy Synchronization Setup

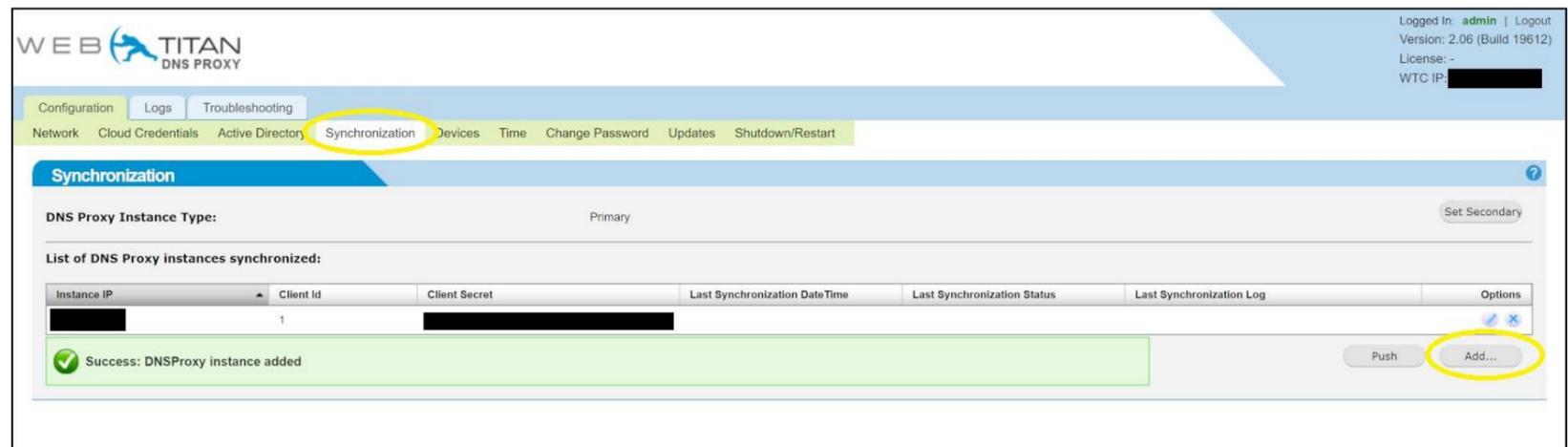
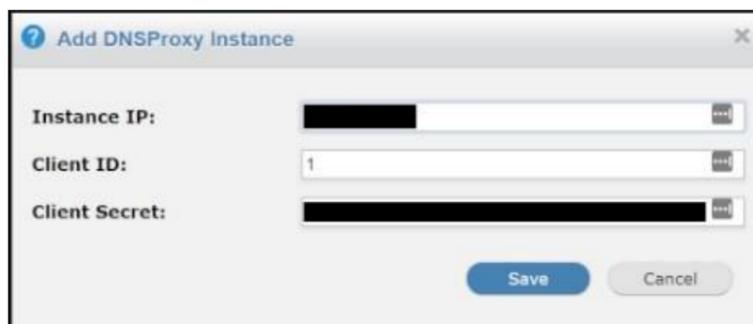
1. On your DNSProxy locate **Synchronization** and Click on **Set Secondary**.



2. Take Note of the Credentials Displayed for entry onto the Primary DNSProxy

## Primary DNSProxy Synchronization Setup

1. Locate the **Synchronization** tab, enter the credentials for **Secondary DNSProxy** & Click **Save**.



2. On the **Active Directory Servers** table Select Azure AD tick box and Click on **Import Users**.

WEB TITAN DNS PROXY

Configuration | Logs | Troubleshooting

Network | Cloud Credentials | Active Directory | Synchronization | Devices | Time | Change Password | Updates | Shutdown/Restart

Active Directory Servers

Type	Server	Base Entry (DN)	Last Import	Imported users	Imported groups	Options
<input checked="" type="checkbox"/>	Active Directory	10.1.0.100	DC=copperf,DC=local	0	0	<a href="#">↕</a> <a href="#">✕</a>
<input checked="" type="checkbox"/>	Azure AD	Azure	AzureAD	0	0	<a href="#">↕</a> <a href="#">✕</a>

Import Users Add...

Synchronization Status

WTC IP Address	Customer	Last Synchronization DateTime	Last Synchronization Info	Last Synchronization Error
[Redacted]	[Redacted]			

Sync Users

3. On the **Synchronization Status** table Click on **Import Users**.

WEB TITAN DNS PROXY

Configuration | Logs | Troubleshooting

Network | Cloud Credentials | Active Directory | Synchronization | Devices | Time | Change Password | Updates | Shutdown/Restart

Active Directory Servers

Type	Server	Base Entry (DN)	Last Import	Imported users	Imported groups	Options
<input type="checkbox"/>	Active Directory	10.1.0.100	30 March 2021, 10:21:49	124	17	<a href="#">↕</a> <a href="#">✕</a>
<input type="checkbox"/>	Azure AD	Azure	30 March 2021, 10:22:13	297	243	<a href="#">↕</a> <a href="#">✕</a>

Import Users Add...

Synchronization Status

WTC IP Address	Customer	Last Synchronization DateTime	Last Synchronization Info	Last Synchronization Error
[Redacted]	[Redacted]	30 March 2021, 10:23:53	416 User(s), 192 Group(s) Synchronized	

Success.

Sync Users

4. Locate the **Synchronization** tab and Click on **Push**.

WEB TITAN DNS PROXY

Configuration | Logs | Troubleshooting

Network | Cloud Credentials | Active Directory | Synchronization | Devices | Time | Change Password | Updates | Shutdown/Restart

Synchronization

DNS Proxy Instance Type: Primary [Set Secondary](#)

List of DNS Proxy instances synchronized:

Instance IP	Client Id	Client Secret	Last Synchronization DateTime	Last Synchronization Status	Last Synchronization Log	Options
[Redacted]	1	[Redacted]	2021-03-30 09:24:33	200	Synchronization was made successfully.	<a href="#">↕</a> <a href="#">✕</a>

The request to push data to DNSProxy instance(s) was made successfully.

Push Add...

## Configure Azure VNet to use DNSProxy

1. Navigate to the **DNSProxy VM** and take note of its **Private IP Address**.

Home > Resource groups > apm-azure-ad-agent >

**DNSProxy-206.01** Virtual machine

Search (Ctrl+/)

Connect Start Restart Stop Capture Delete Refresh Open in mobile

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Security

Advisor recommendations

Extensions

Continuous delivery

Availability + scaling

Configuration

Identity

Properties

Essentials

Resource group (change): apm-azure-ad-agent

Status: Running

Location: West Europe

Subscription (change): Development (sean's CC)

Subscription ID: 3f51630f-4c88-4fba-b57a-5c39b5662a2f

Tags (change): Click here to add tags

Operating system: Linux (freebsd 11.2)

Size: Standard DS1 v2 (1 vcpu, 3.5 GiB memory)

Public IP address: 20.71.182.217

Virtual network/subnet: aadds-vnet/aadds-subnet-01

DNS name: Configure

Properties

Monitoring

Capabilities (7)

Recommendations

Tutorials

Virtual machine

Computer name: dnsproxy-az.example.com

Operating system: Linux (freebsd 11.2)

Publisher: -

Offer: -

Plan: -

VM generation: V1

Agent status: Ready

Agent version: 9.9.9.9

Host group: None

Host: -

Proximity placement group: -

Networking

Public IP address: 20.71.182.217

Public IP address (IPv6): -

Private IP address: 10.101.1.6

Private IP address (IPv6): -

Virtual network/subnet: aadds-vnet/aadds-subnet-01

DNS name: Configure

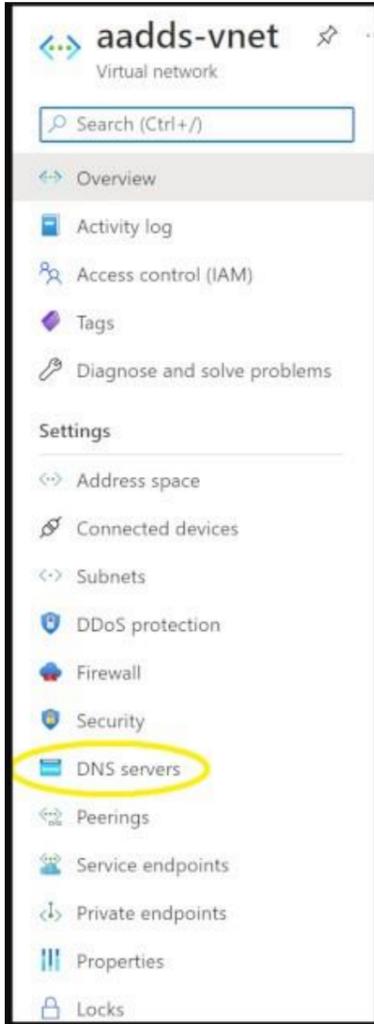
Size

Size: Standard DS1 v2

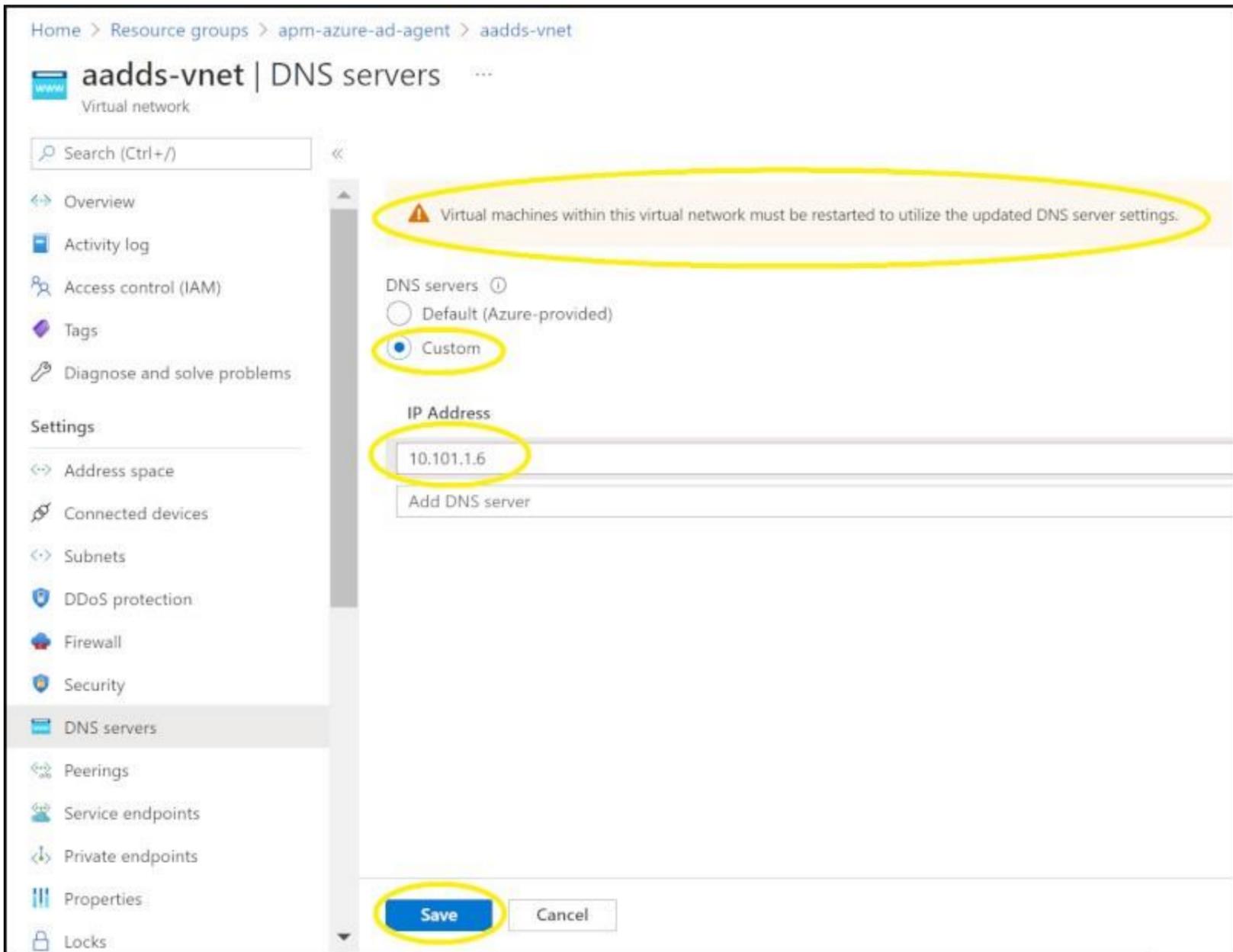
vCPUs: 1

RAM: 3.5 GiB

2. Navigate to the **VNet page**, in the left-hand navigation pane locate **DNS Servers** & Click on it.



3. On the DNS Server page, Select custom and Add the Private IP of the DNSProxy.

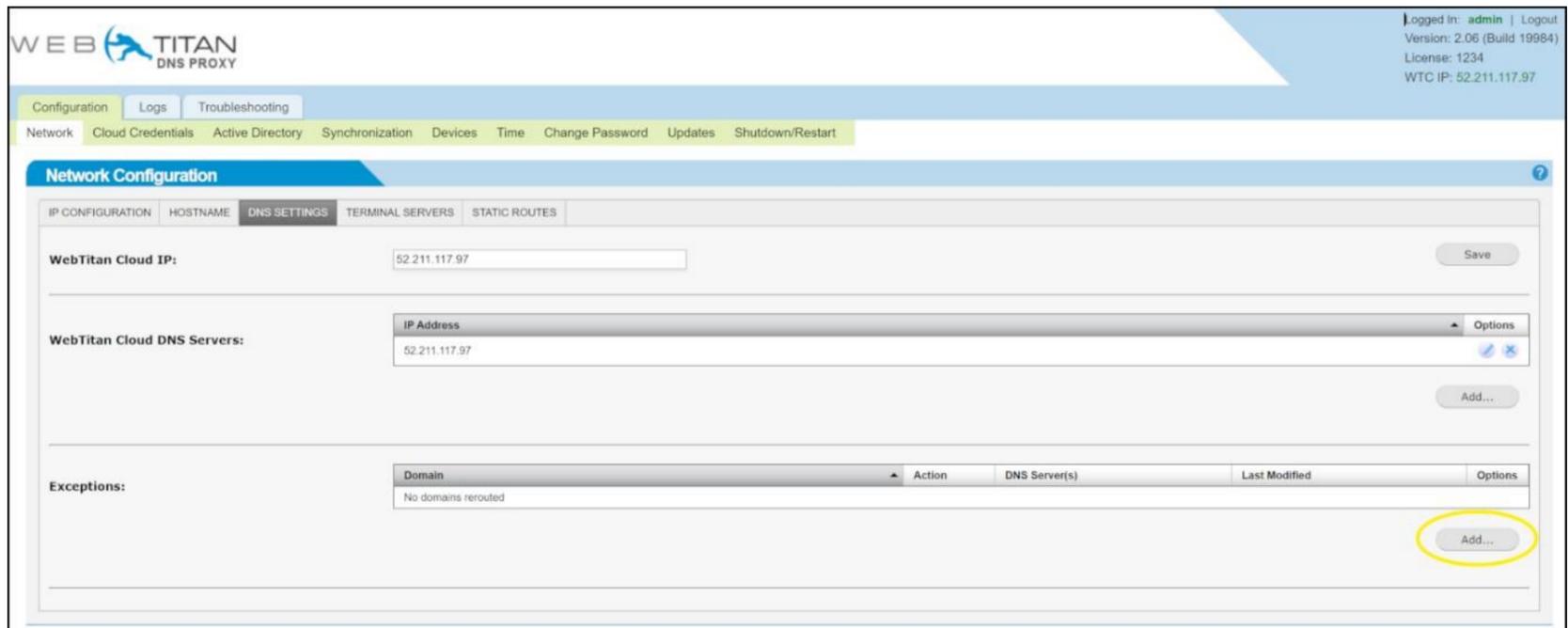


IMPORTANT: You must restart the DNSProxy immediately after this step.

IMPORTANT: All VM must be restarted for them to use the DNSProxy for processing DNS request, they will keep using the oldDNS settings till restarted.

# Configure DNSProxy with Azure Specific Redirects

1. On DNSProxy Navigate to **Configuration->Network->DNS Settings**



2. On the **Redirect Pane** click on **Add**



The following list is by no means exhaustive:

```
core.windows.net
internal.cloudapp.net
prd.aadg.trafficmanager.net
prd.ags.akadns.net
prd.ags.msidentity.com
prd.ags.trafficmanager.net
privatelink.msidentity.com
```

These domains have been observed as windows azure related lookups that generate a lot of noise in the history on WTC.

# Troubleshooting DNSProxy Deployment

## Error: The access token is from the wrong issuer

az account get-access-token needs to be applied in Azure Cloud Shell

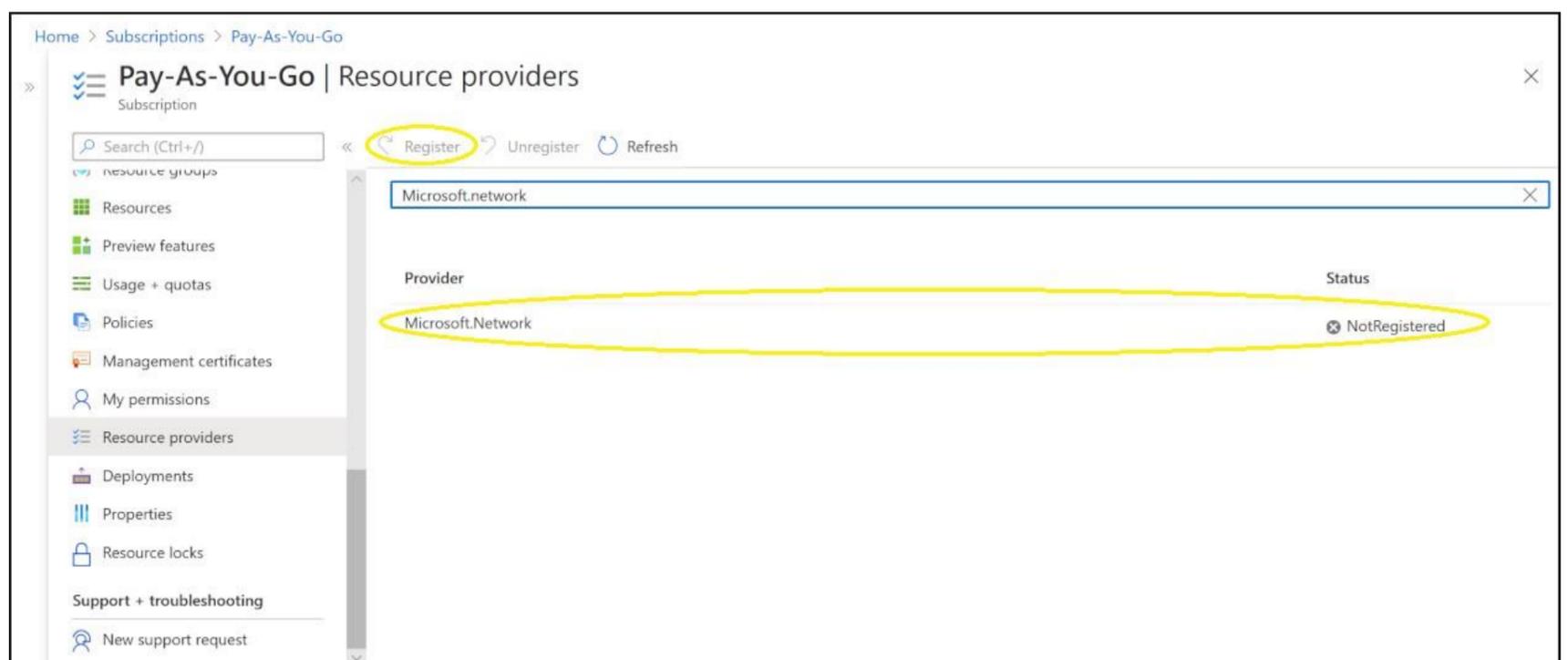
```
The access token is from the wrong issuer 'https://sts.windows.net/642f1773-84ee-4a58-81b8-1b2c13bdaa93/'. It must match the tenant 'https://sts.windows.net/896d169b-ffab-4391-8348-fc1b4644dfdd/' associated with this subscription. Please use the authority (URL) 'https://login.windows.net/896d169b-ffab-4391-8348-fc1b4644dfdd' to get the token. Note, if the subscription is transferred to another tenant there is no impact to the services, but information about new tenant could take time to propagate
```

## Error: The subscription is not registered to use namespace

The Resource provider for the mentioned namespace needs to be made available to your tenant.

```
StatusCode: 409
ReasonPhrase: Conflict
ErrorCode: MissingSubscriptionRegistration
ErrorMessage: The subscription is not registered to use namespace 'Microsoft.Network'. See https://aka.ms/rps-not-found for how to register subscriptions.
Additional details:
  Code: MissingSubscriptionRegistration
  Message: The subscription is not registered to use namespace 'Microsoft.Network'. See https://aka.ms/rps-not-found for how to register subscriptions.
```

Navigate to **Resource providers**, search for the missing namespace, **highlight** it and click on **register**



## Troubleshooting WebTitan AzureAD Enterprise App

This section lists the common error messages you may run into while accessing activity reports using the Microsoft Graph API and steps for their resolution.

### **Error: Tenant is not B2C or tenant doesn't have premium license**

Accessing sign-in reports requires an Azure Active Directory premium 1 (P1) license. If you see this error message while accessing sign-ins, make sure that your tenant is licensed with an Azure AD P1 license.

### **Error: Application missing AAD 'Read directory data' permission**

Follow the steps in the [Prerequisites to access the WebTitan AzureAD Enterprise App] to ensure your application is running with the right set of permissions.

### **Error: Application missing Microsoft Graph API 'Read all audit log data' permission**

Follow the steps in the [Prerequisites to access the WebTitan AzureAD Enterprise App] to ensure your application is running with the right set of permissions.

### **Error: Access token validation failure. Invalid audience.**

Follow the steps in the Prerequisites to access the WebTitan AzureAD Enterprise App to ensure your application is running with the right set of permissions.