

## **MoxiEngage Integration Process using Microsoft 365 (Client secret)**

### ***Overview***

MoxiEngage integrates directly with your brokerage's Microsoft 365 (formerly Office 365) account to provide your agents and support staff with consistent and convenient access to their information, while eliminating any need to enter the same information multiple times.

MoxiEngage uses Modern Authentication with an impersonation service account through the Exchange Web Services (EWS) Managed API to synchronize data and perform actions on behalf of individual users. Each MoxiEngage user account has an email address that corresponds to a mailbox on your Microsoft 365 account. All integration actions are performed within the context of a single given mailbox. MoxiEngage never requires administrative access to your Microsoft 365 account.

### **Contacts**

MoxiEngage continually synchronizes a user's contacts and contact details with the Microsoft 365 Exchange mailbox. Contacts created in Microsoft 365 will appear in MoxiEngage. Contacts created in MoxiEngage are synchronized back to the Microsoft 365 mailbox.

### **Calendar**

MoxiEngage displays the user's calendar events and appointments. Calendar events and appointments can also be added through MoxiEngage and are synchronized to the Microsoft 365 mailbox.

### **Email**

MoxiEngage sends certain email messages through user's mailbox. These email messages will appear in the Sent mail folder and will be delivered to the recipient from the mailbox just as if the user had sent the email from Microsoft 365 directly. MoxiEngage does not synchronize or inspect incoming email messages.

### ***Information Gathering***

To enable configuration of the MoxiEngage integration, we will need to gather some key information and credentials from you, including the service account credentials, Client ID, and Tenant ID obtained by following the steps in the [Microsoft 365 Setup Instructions for Administrators](#) section of this document.

### ***Next Steps***

#### **Verification of Credentials**

MoxiWorks staff will begin the next step of the integration process. We will test the credentials you provided to verify that the service account is able to connect to your email service using Modern Authentication and perform a synchronization for the test email address you supplied.



### **Outcome: Credentials Cannot be Verified**

If your entered credentials cannot be verified, we will contact you. Your email administrator will need to resolve the issue and then you will provide us with the updated information.

### **Outcome: Credentials are Verified Successfully**

If your credentials are verified successfully, we will store the credentials securely. Congratulations! This is a key milestone that enables us to continue the process of getting MoxiEngage enabled for your brokerage.

## ***Security***

MoxiWorks requires the use of a single username/mailbox on your Microsoft 365 instance, configured as a service account with the Application Impersonation role. All interactions between the MoxiWorks system and your user's mailboxes happens through this designated impersonation account and delegation access to the EWS Managed API. MoxiEngage never requires administrative access to your Microsoft 365 instance.

### **Network Access**

MoxiWorks systems communicate directly with Microsoft 365 servers over secure HTTPS/SSL connections.

### **Managing Shared Secrets and Credentials**

For automated access, MoxiWorks makes use of methods native to our configuration management software. Credentials are stored in encrypted objects accessible only to servers with the relevant service role and environment. These credentials are pulled and decrypted during software deployment. Server identity is validated via pre-shared public/private key. Credentials are managed through a commercial password manager and any non-automated access is limited to the MoxiWorks Technical Operations team and, with customer approval, limited support personnel on an as-needed basis. See also:

<https://docs.chef.io/secrets.html#encrypt-a-data-bag-item>

<https://www.lastpass.com/en/enterprise>

### **Communications Policy for Security Breaches**

In the unlikely event of a security breach where client data such as account credentials for registrar management, impersonation credentials, and the like may have been compromised, MoxiWorks Technical Operations and/or Account Management staff will notify affected clients. If the client is aware of a potential security breach, they should notify MoxiWorks immediately so that we may contain and mitigate potential risk in a timely manner. In either case, a change to Impersonation account credentials will be coordinated between both parties.

## **Microsoft 365 Setup Instructions for Administrators**

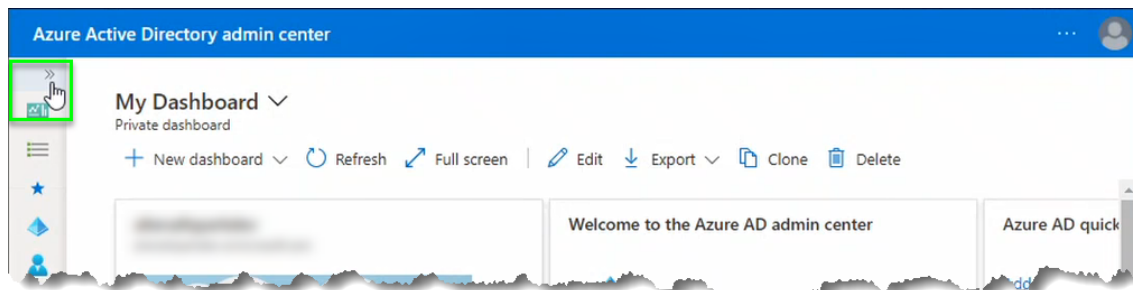
A client application must also be registered and configured with delegation access to the Exchange Web Services (EWS) Managed API to support Modern Authentication.

Microsoft 365 menu structure and user interface is subject to change. Steps provided in this document were performed from a computer running Windows 10 Pro against a Microsoft 365 instance created in July 2021. If you are running an on-premises installation of Exchange Server, the actual steps required to accomplish these tasks may be different than those described in this document.

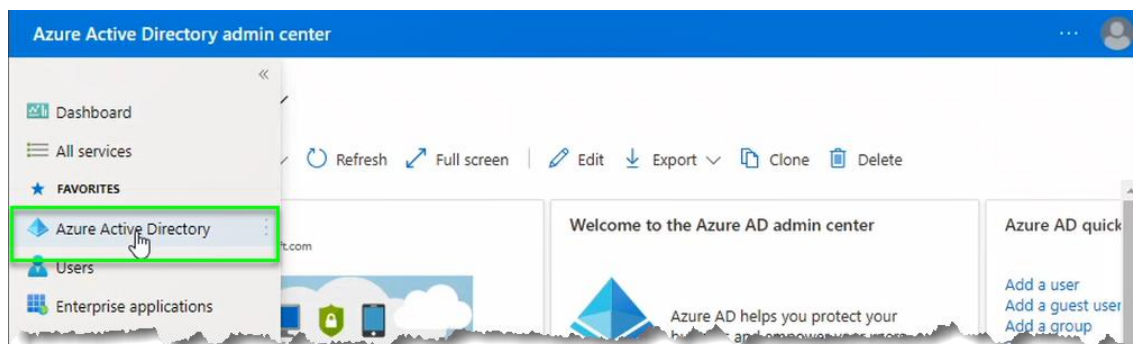
The instructions provided in this guide are not intended to provide security advice for configuring your Microsoft 365 instance. The documented steps represent the most direct approach available at the time of this writing to achieve the necessary access required by MoxiWorks products. Other methods of configuration may be available.

## Register the MoxiEngage Application as an API Client

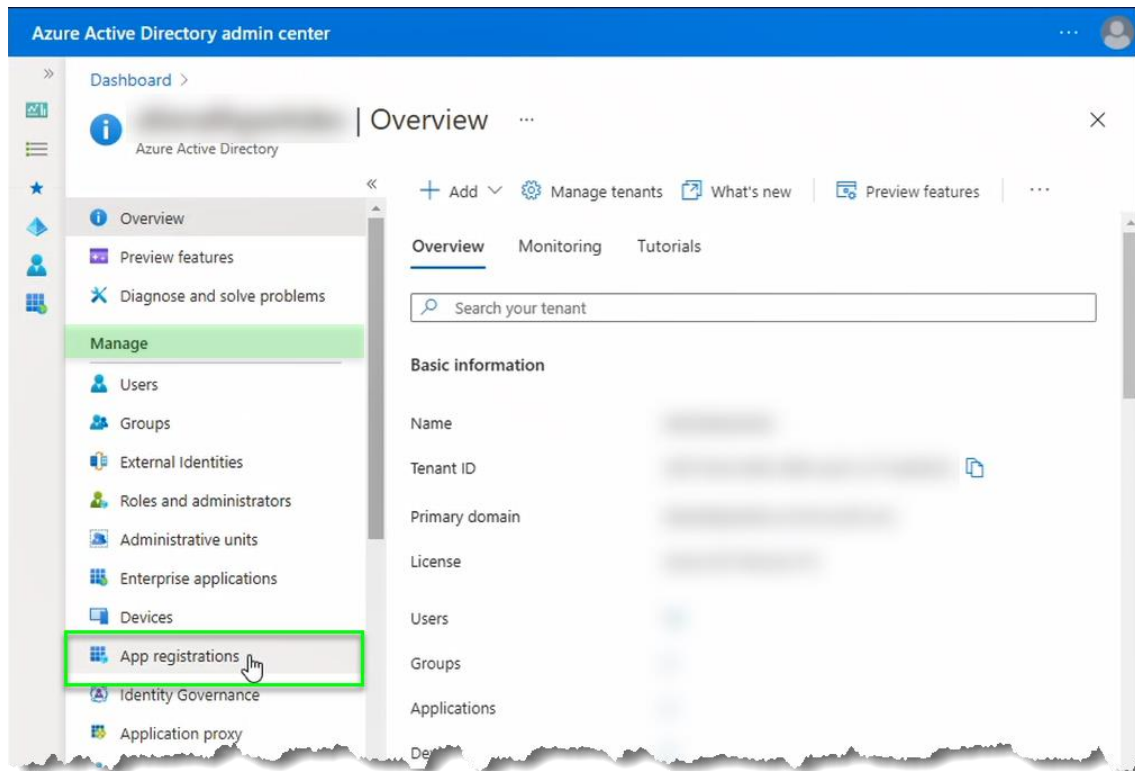
1. Login to your [Azure Active Directory Admin Center](#).
2. Click on the double chevron in the top left corner of the screen to expand the written menu.



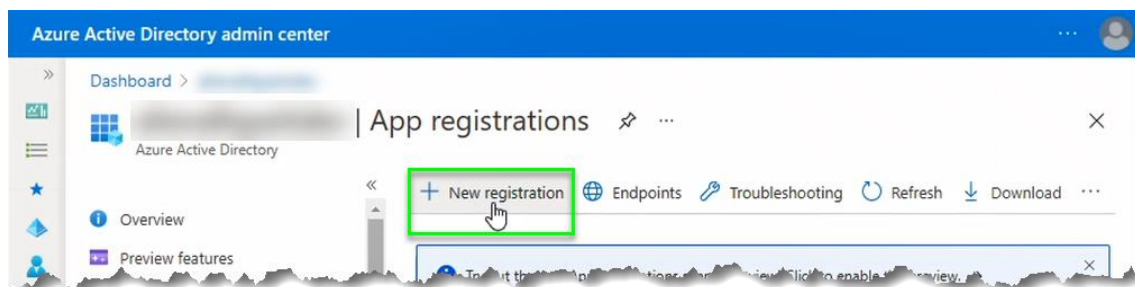
3. Click on the "Azure Active Directory" option in the menu.



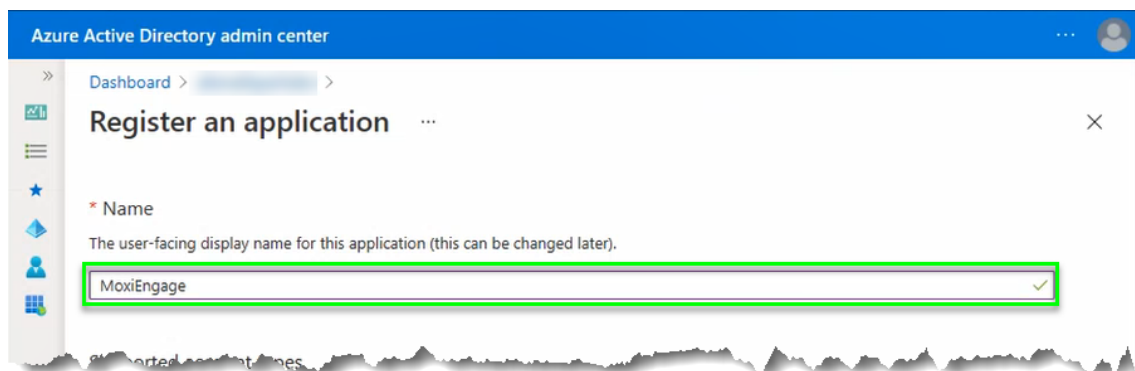
- From the Azure Active Directory Dashboard for your Microsoft 365 instance, click on the “App Registrations” menu option under the “Manage” grouping.



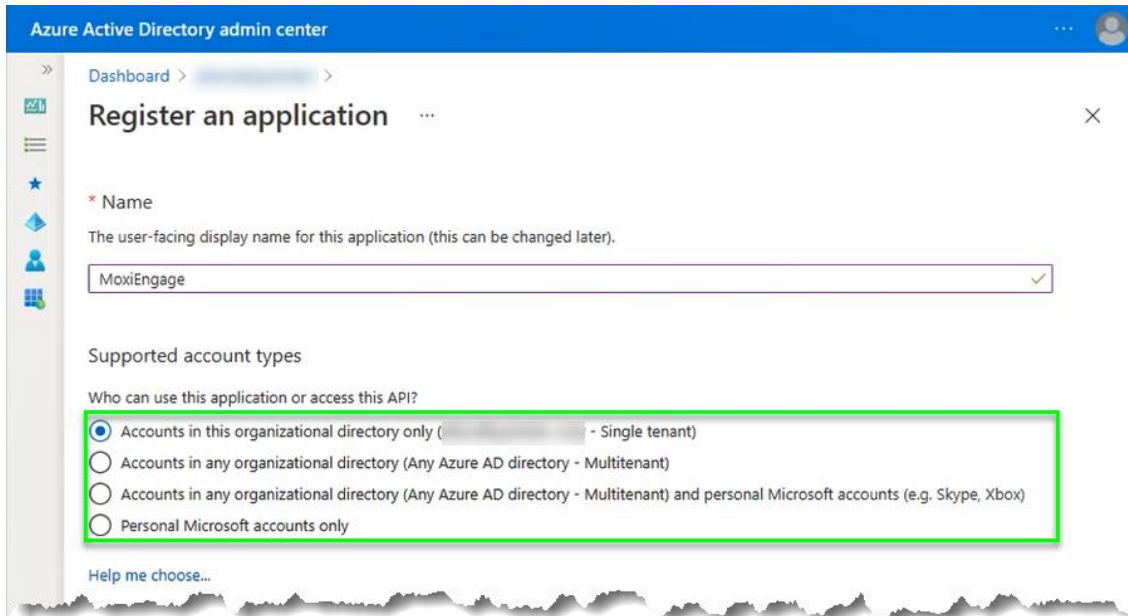
- Click on the “New registration” link.



- Enter a name for the MoxiWorks client application (e.g., MoxiEngage).



7. Indicate the type of Microsoft 365 account that will be using MoxiEngage. In most instances, the Single Tenant default selection will be correct.



Azure Active Directory admin center

Dashboard > >

## Register an application

\* Name

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

MoxiEngage ✓

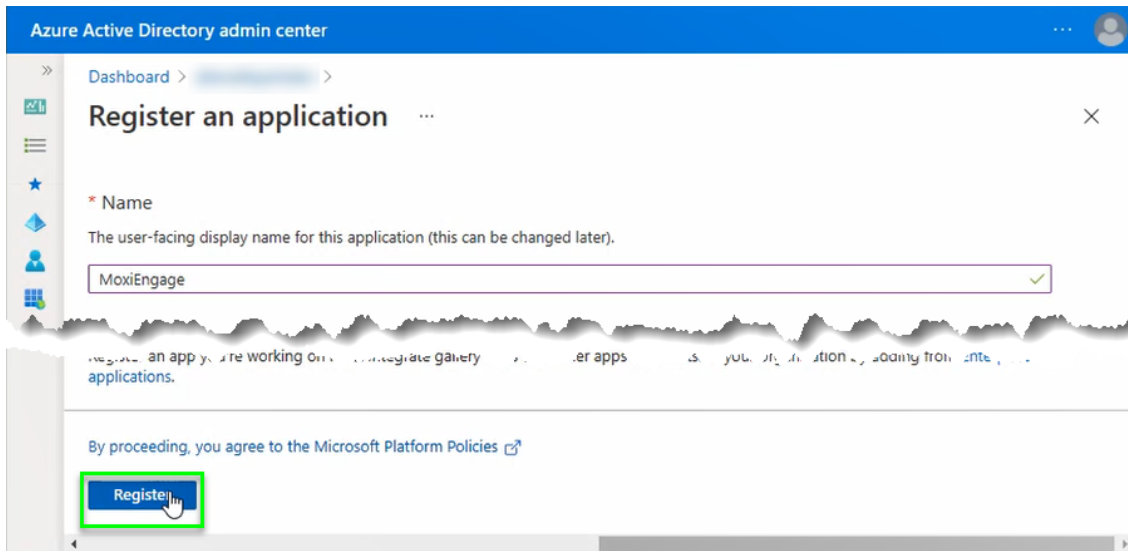
Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory 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...](#)

8. The Redirect URI settings are optional. No changes are needed.
9. Click on the “Register” button.



Azure Active Directory admin center

Dashboard > >

## Register an application

\* Name

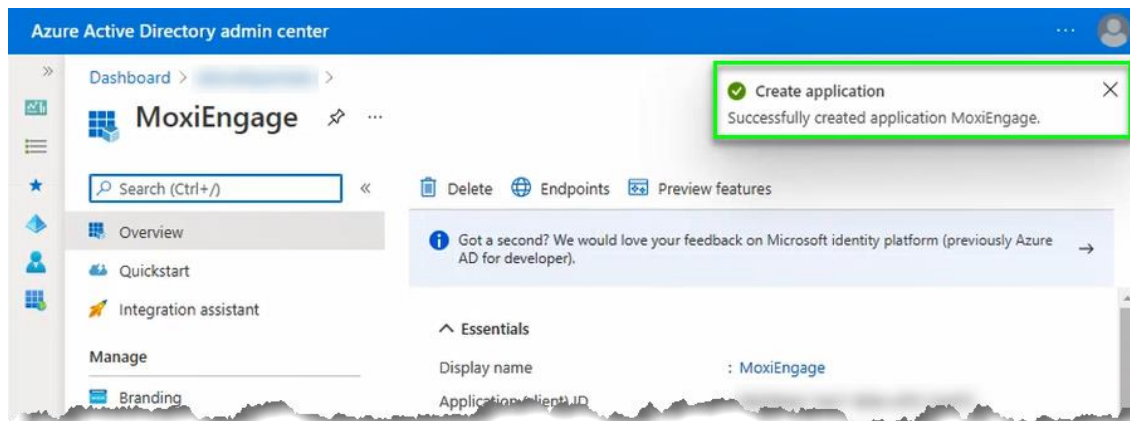
The user-facing display name for this application (this can be changed later).

MoxiEngage ✓

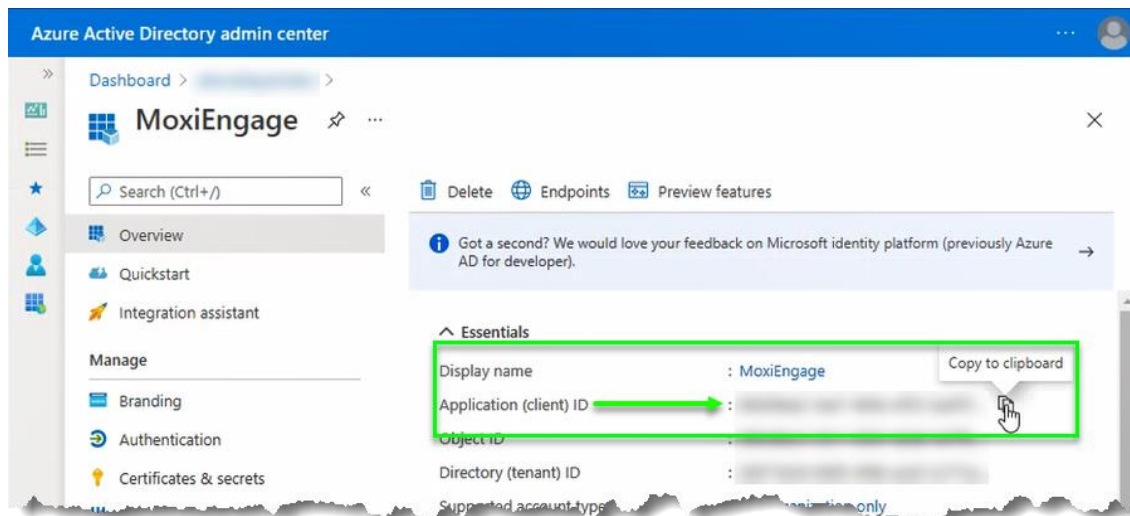
By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

10. Observe the notification that your application was created successfully.



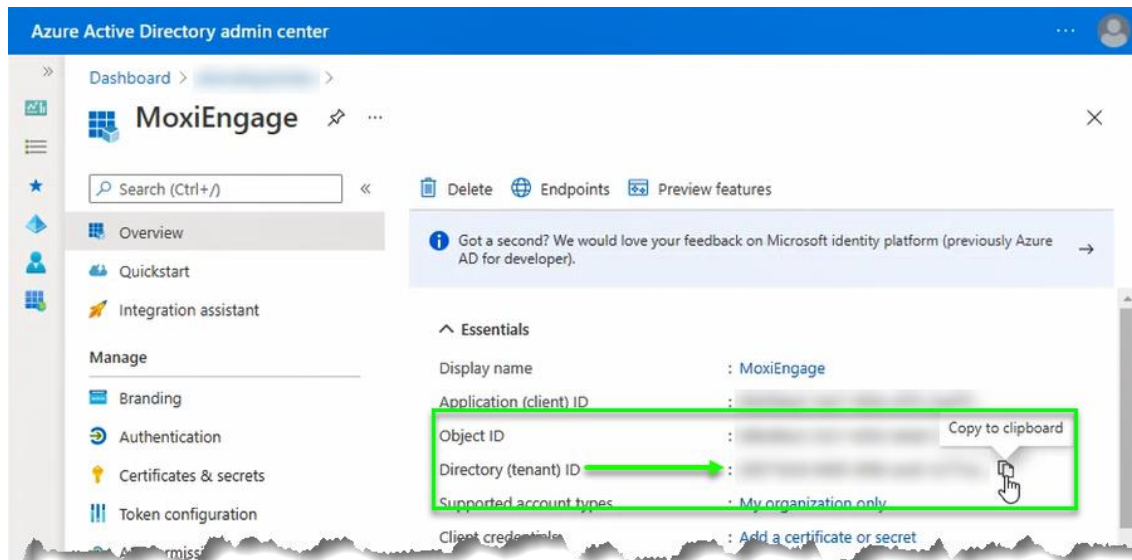
11. Locate the value next to the "Application (client) ID" label, then click on the "Copy to clipboard" button (only visible when you hover over the value).



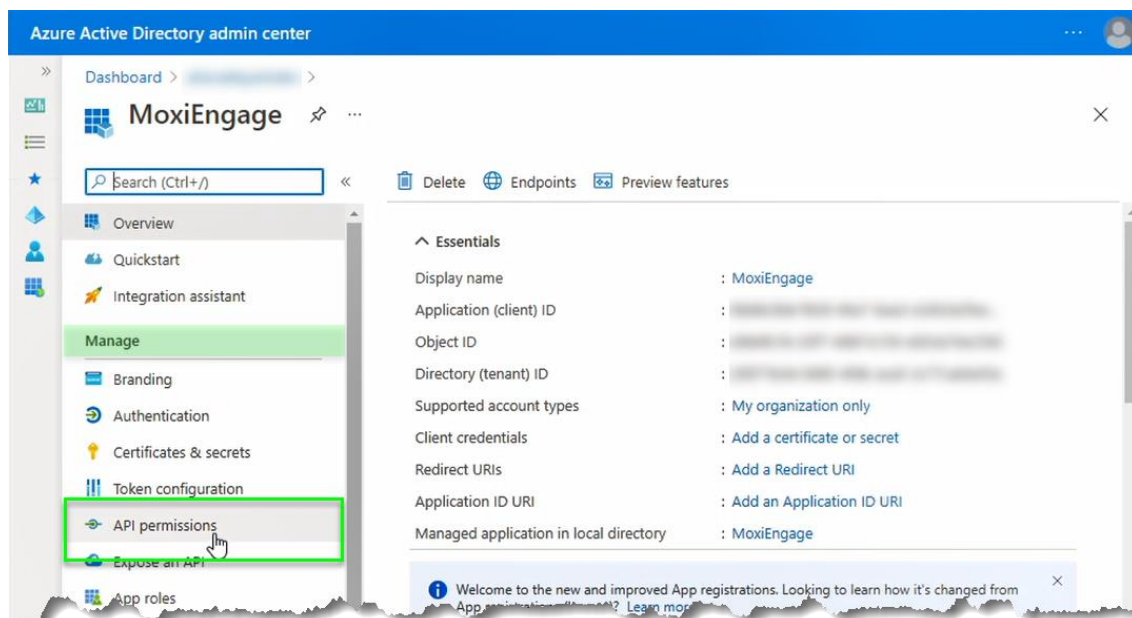
12. Paste the value to a text file for reference. You will need to provide this value to MoxiWorks as your Client ID.



13. Locate the value next to the “Directory (tenant) ID” label, then click on the “Copy to clipboard” button (only visible when you hover over the value).

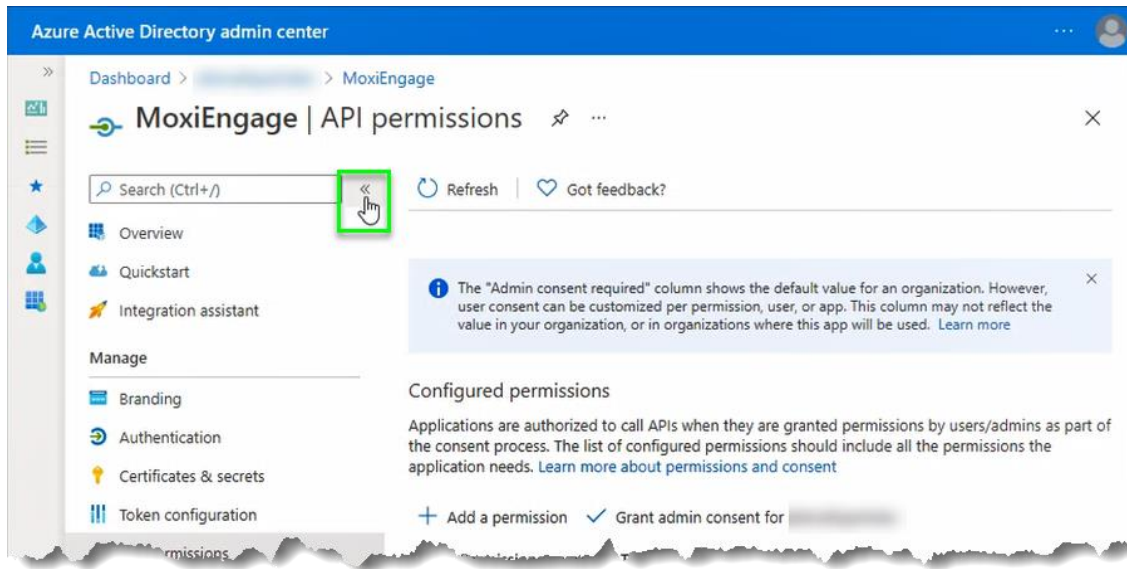


14. Paste the value to a text file for reference. You will need to provide this value to MoxiWorks as your Tenant ID.
15. Click on the “API permissions” option under the “Manage” grouping of the menu.





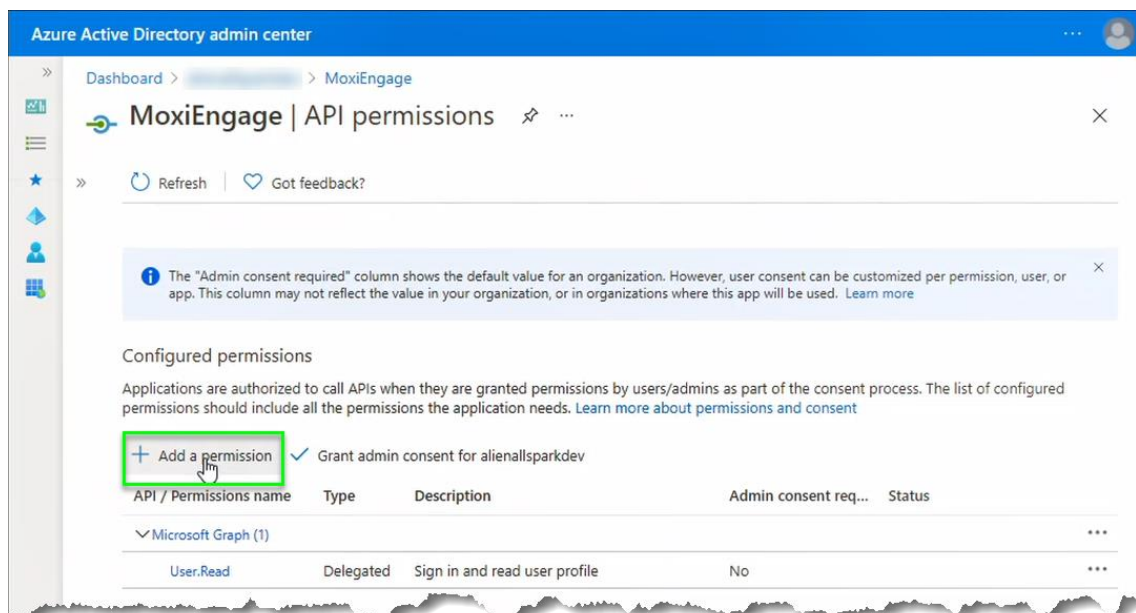
16. Click on the double chevron to collapse the side menu.



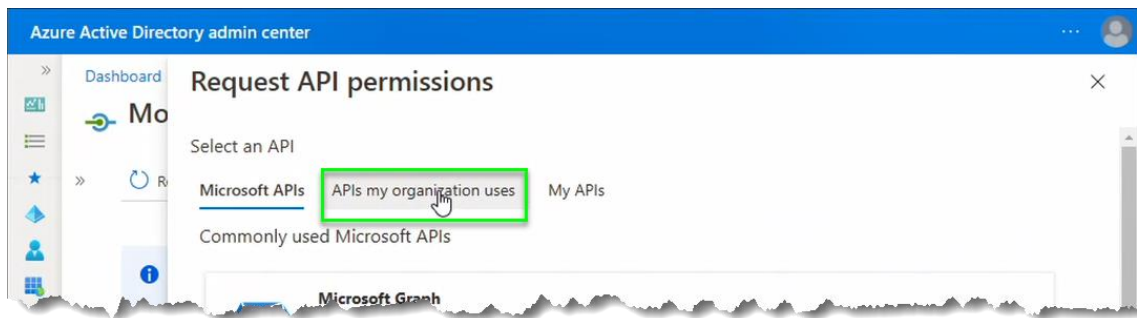
### Note

The “User.Read” permission for the “Microsoft Graph” API may be listed in the “Configured permissions” list. This permission does not provide sufficient permissions for MoxiEngage to perform core functionality.

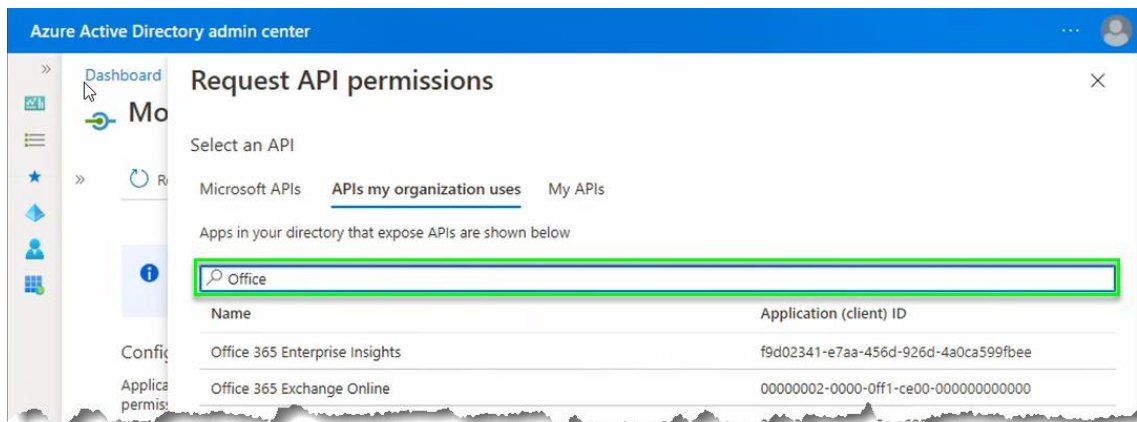
17. Click on the “Add a permission” link.



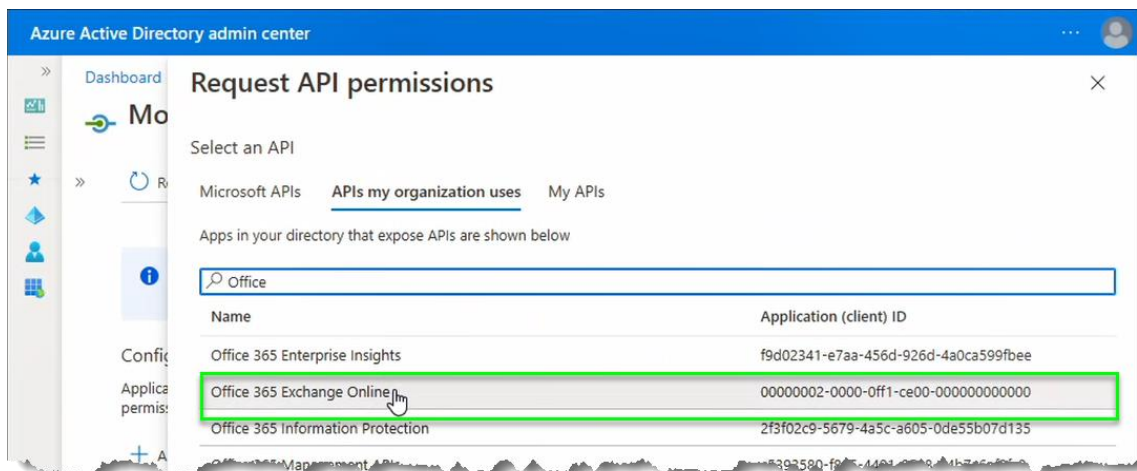
18. Click on “APIs my organization uses” tab to change the view of available APIs.



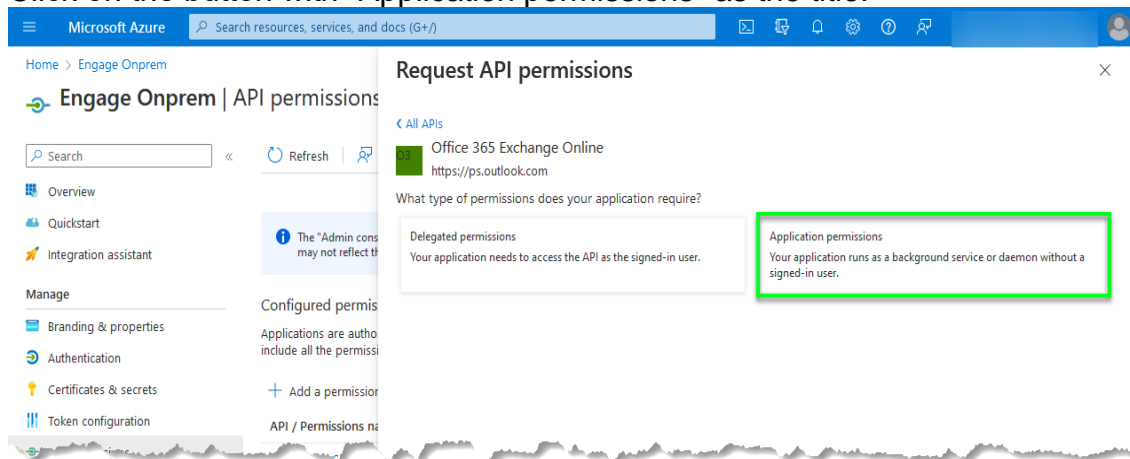
19. Type “Office” in the Search box to filter the API list.



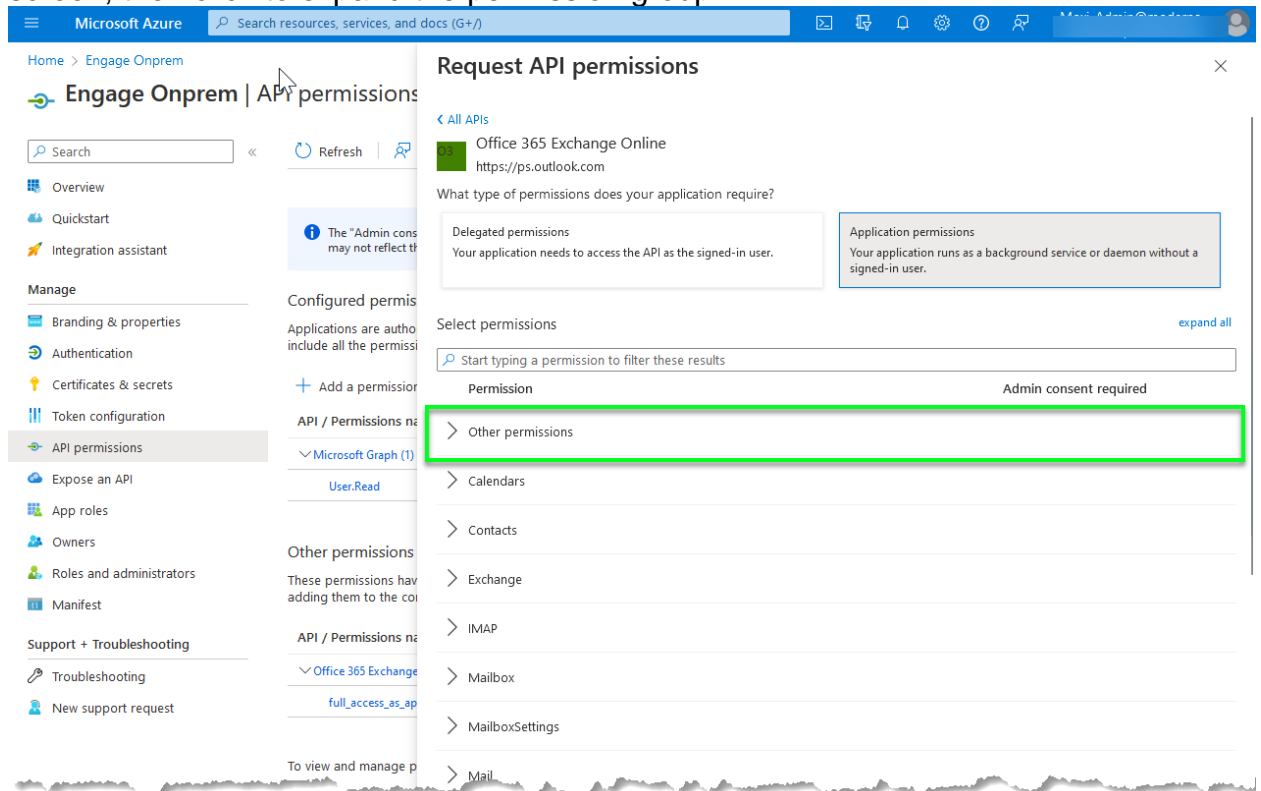
20. Click on the “Office 365 Exchange Online” API name.



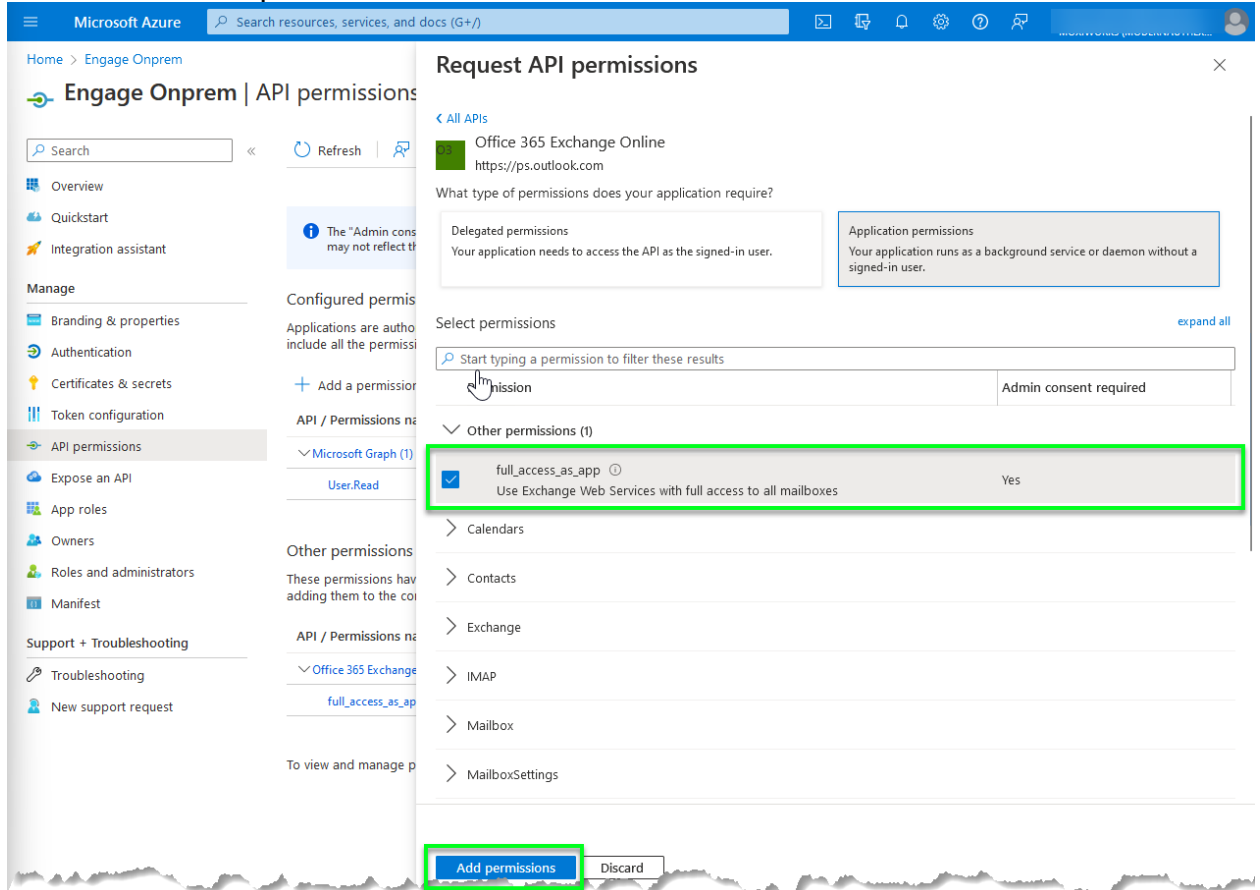
21. Click on the button with “Application permissions” as the title.



22. Locate the “Other permissions” item under the “Select permissions” area of the screen, then click to expand the permission group.



23. Check the box next to the “full\_access\_as\_app” permission under the “Others” permission group.
24. Click on the “Add permissions” button.



The screenshot shows the Microsoft Azure portal interface. On the left, the 'Engage Onprem | API permissions' page is visible, with a sidebar containing navigation links like Overview, Quickstart, Integration assistant, and various management options. The main content area displays the 'Request API permissions' dialog for the 'Office 365 Exchange Online' API. The dialog is titled 'Request API permissions' and includes a search bar and a list of permissions. The 'full\_access\_as\_app' permission is selected, and the 'Add permissions' button at the bottom is highlighted with a green box. The 'Discard' button is also visible next to it.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Engage Onprem

Engage Onprem | API permissions

Search Refresh

Overview Quickstart Integration assistant

Manage

Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest Support + Troubleshooting Troubleshooting New support request

The "Admin console" may not reflect the current state of the application.

Configured permissions

Applications are authorized to include all the permissions.

+ Add a permission

API / Permissions namespace

Microsoft Graph (1)

User.Read

Other permissions

These permissions have been added to the configuration.

API / Permissions namespace

Office 365 Exchange Online

full\_access\_as\_app

To view and manage permissions, click on the permission name.

Request API permissions

< All APIs

Office 365 Exchange Online  
https://ps.outlook.com

What type of permissions does your application require?

Delegated permissions  
Your application needs to access the API as the signed-in user.

Application permissions  
Your application runs as a background service or daemon without a signed-in user.

Select permissions

Start typing a permission to filter these results

permission Admin consent required

Other permissions (1)

☒ full\_access\_as\_app ⓘ  
Use Exchange Web Services with full access to all mailboxes Yes

> Calendars

> Contacts

> Exchange

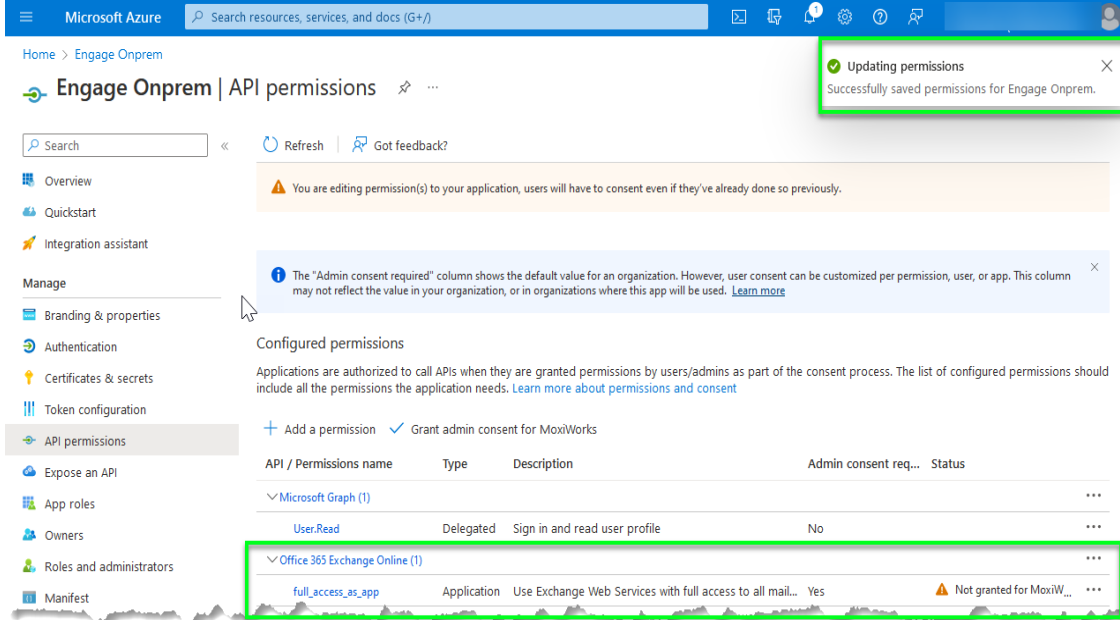
> IMAP

> Mailbox

> MailboxSettings

Add permissions Discard

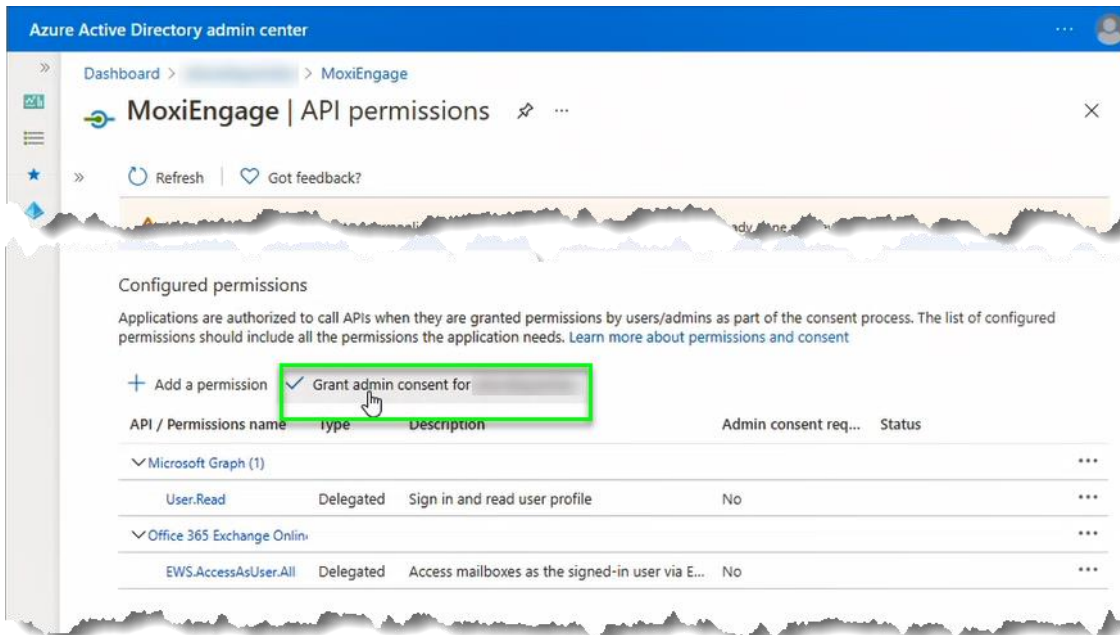
25. Observe the confirmation message and note that the selected permission has been added to the “Configured permissions” list.



The screenshot shows the Microsoft Azure portal interface. A notification at the top right states: "Updating permissions" and "Successfully saved permissions for Engage Onprem." Below this, a warning message indicates that users will have to consent even if they've already done so previously. The main section is titled "Configured permissions" and includes a table with columns: "API / Permissions name", "Type", "Description", "Admin consent req...", and "Status". The table lists permissions for "Microsoft Graph (1)" and "Office 365 Exchange Online (1)". The "full\_access\_as\_app" permission under "Office 365 Exchange Online (1)" is highlighted with a green box, showing a status of "Not granted for MoxiW...".

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...
Office 365 Exchange Online (1)				
full_access_as_app	Application	Use Exchange Web Services with full access to all mail...	Yes	Not granted for MoxiW... ..

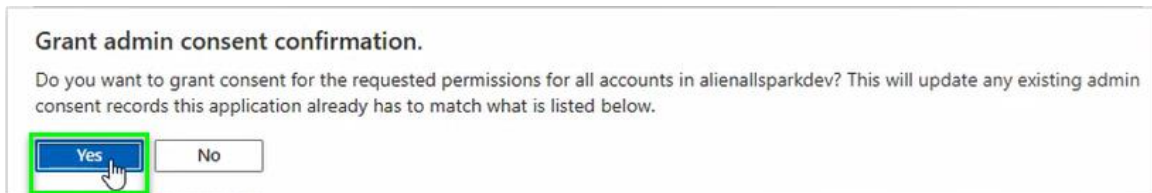
26. Click on the link to “Grant admin consent for” your domain.



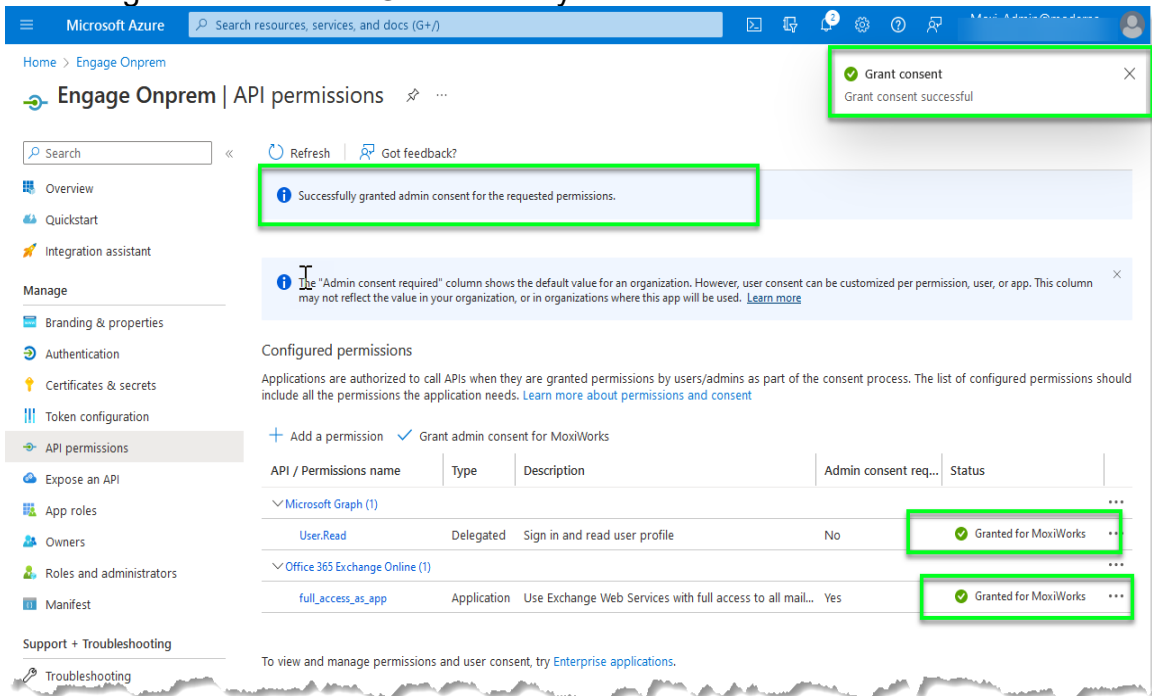
The screenshot shows the Azure Active Directory admin center interface. The page is titled "MoxiEngage | API permissions". Below the title, there is a section for "Configured permissions" with a table of permissions. A green box highlights the link "Grant admin consent for" in the "Add a permission" section.

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	...
Office 365 Exchange Online				
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via E...	No	...

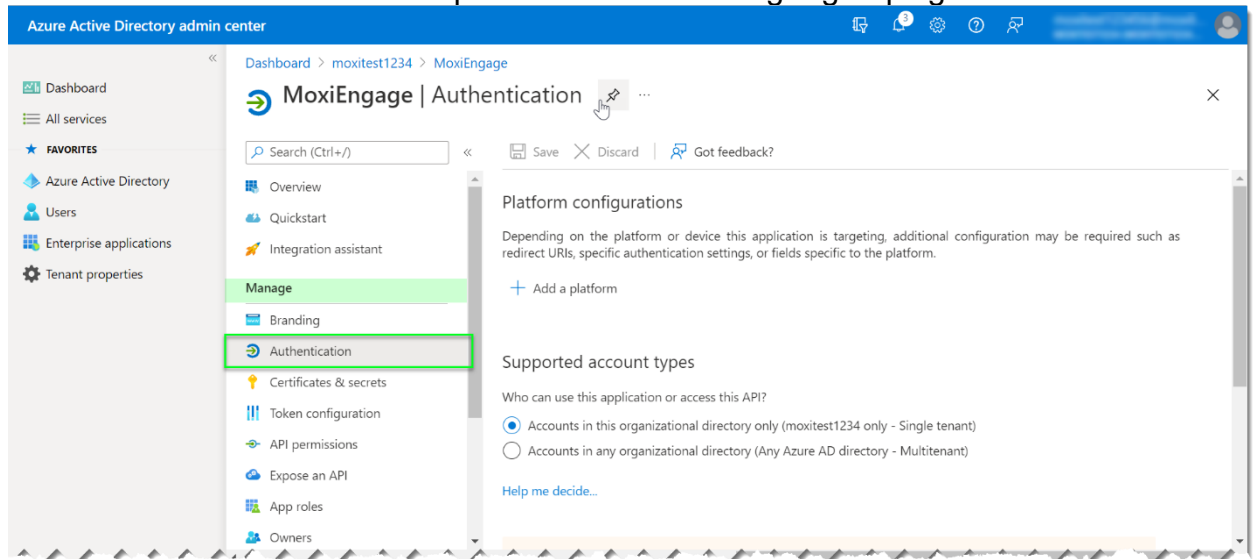
27. Click on the “Yes” button to confirm.



28. Observe the confirmation message(s) and the change in permission status indicating that consent is “Granted for” your domain.

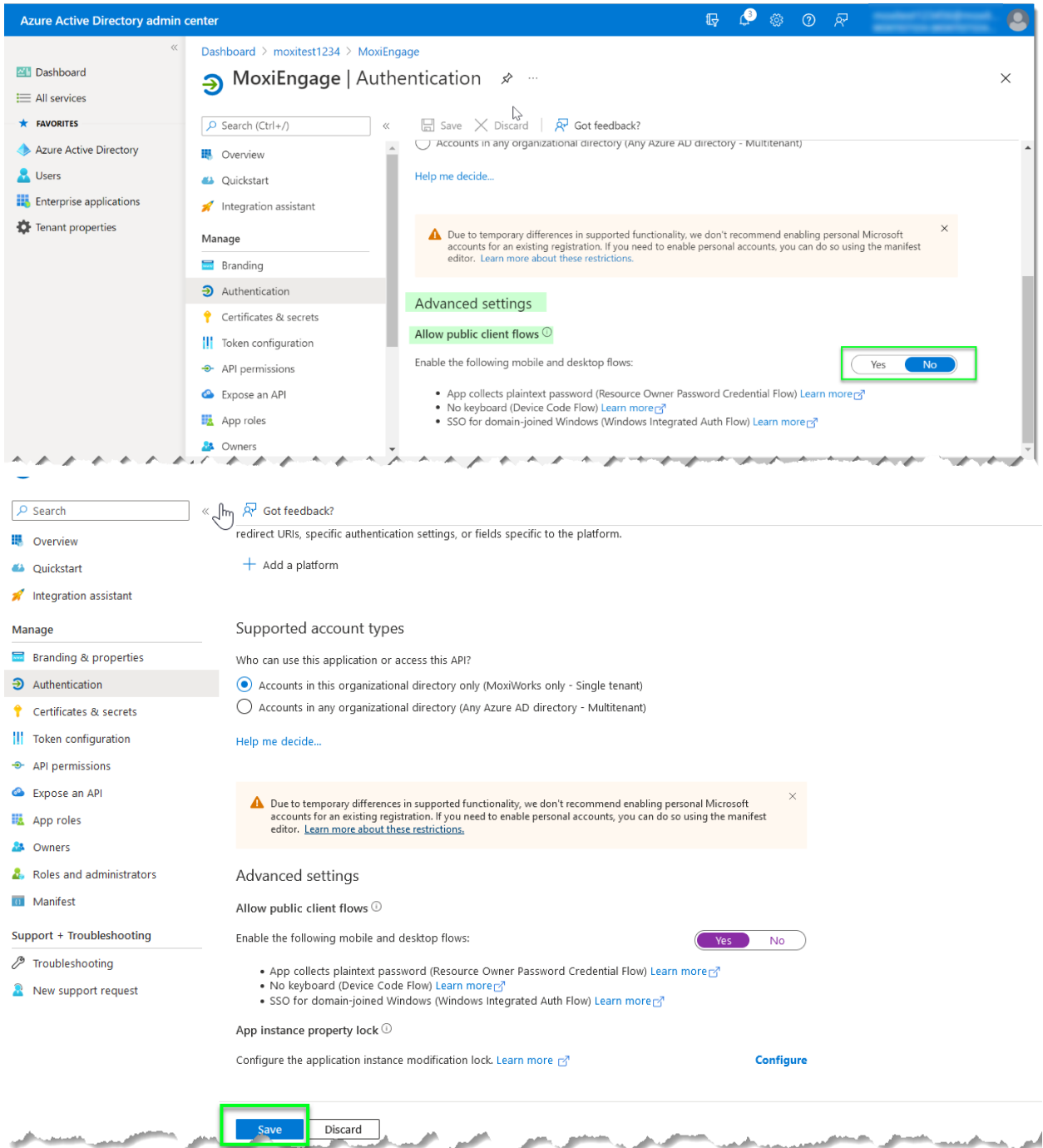


29. Click on the “Authentication” option under the “Manage” grouping of the menu.



30. Scroll down to “Advance settings”, locate the “Allow public client flows” setting and change the setting to “Yes”. Click “Save” button.





Azure Active Directory admin center

Dashboard > moxitest1234 > MoxiEngage

MoxiEngage | Authentication

Search (Ctrl+/)

Save Discard Got feedback?

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

Search

Got feedback?

redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (MoxiWorks only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows:

Yes No

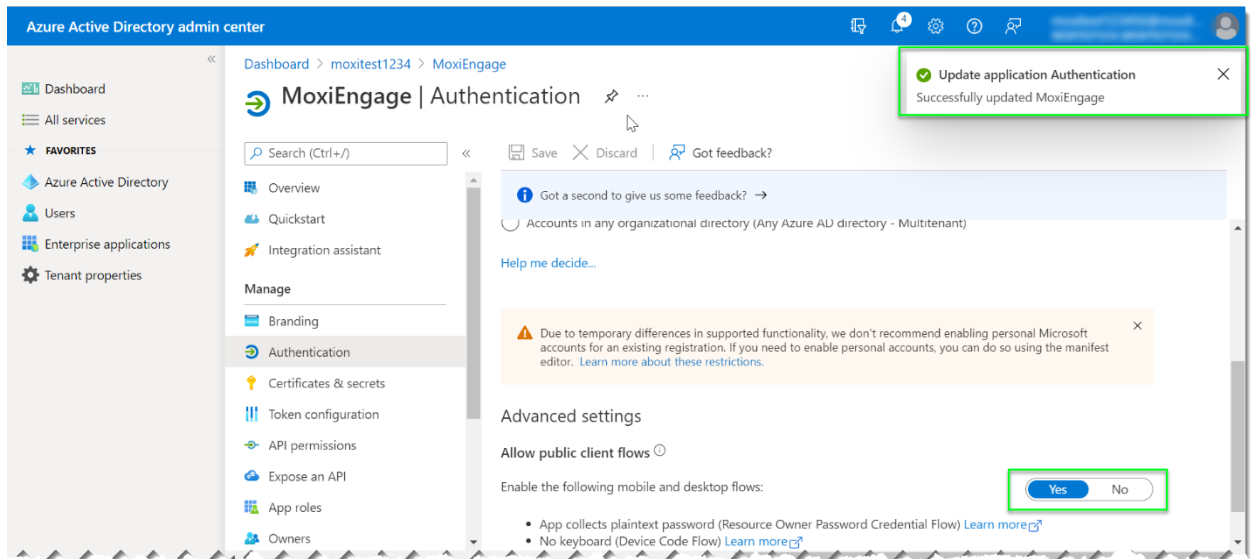
- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

App instance property lock

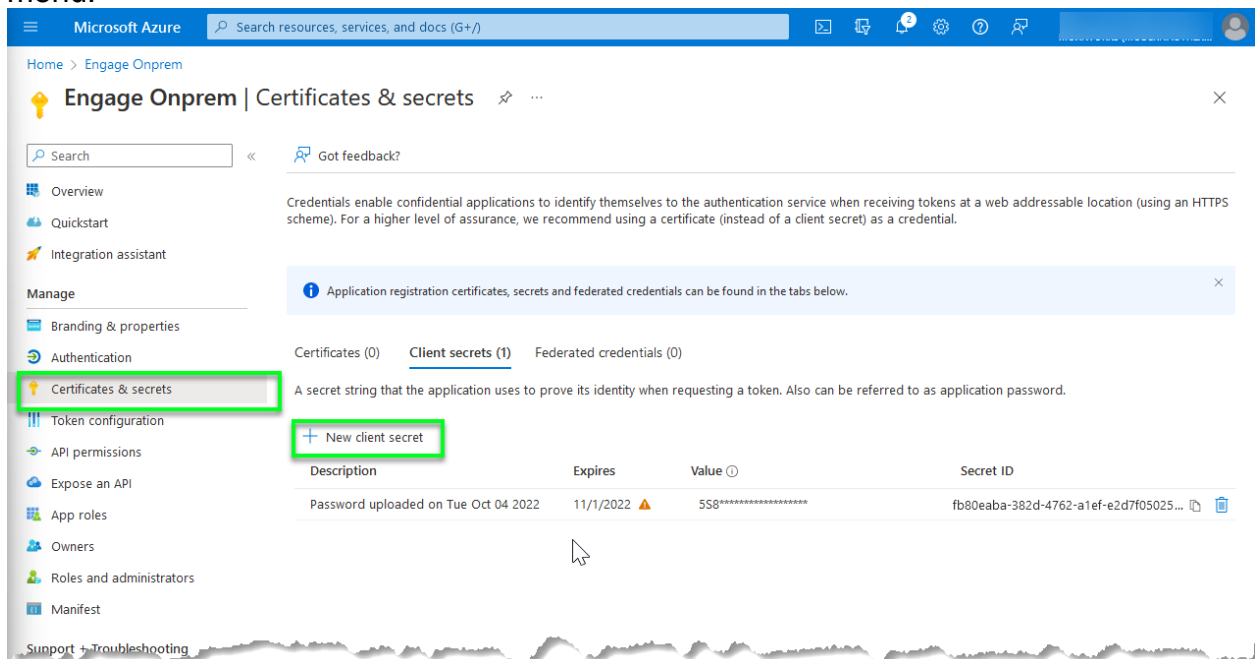
Configure the application instance modification lock. [Learn more](#) [Configure](#)

Save Discard

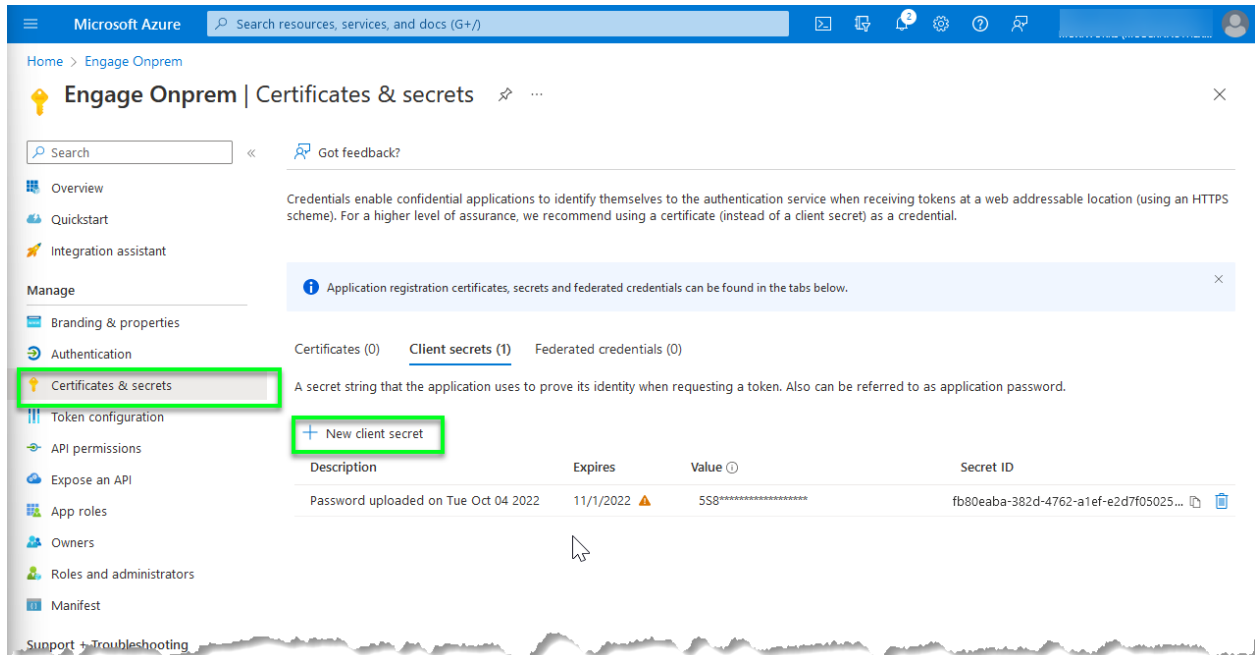
31. Observe the confirmation message and the change in setting is "Yes".



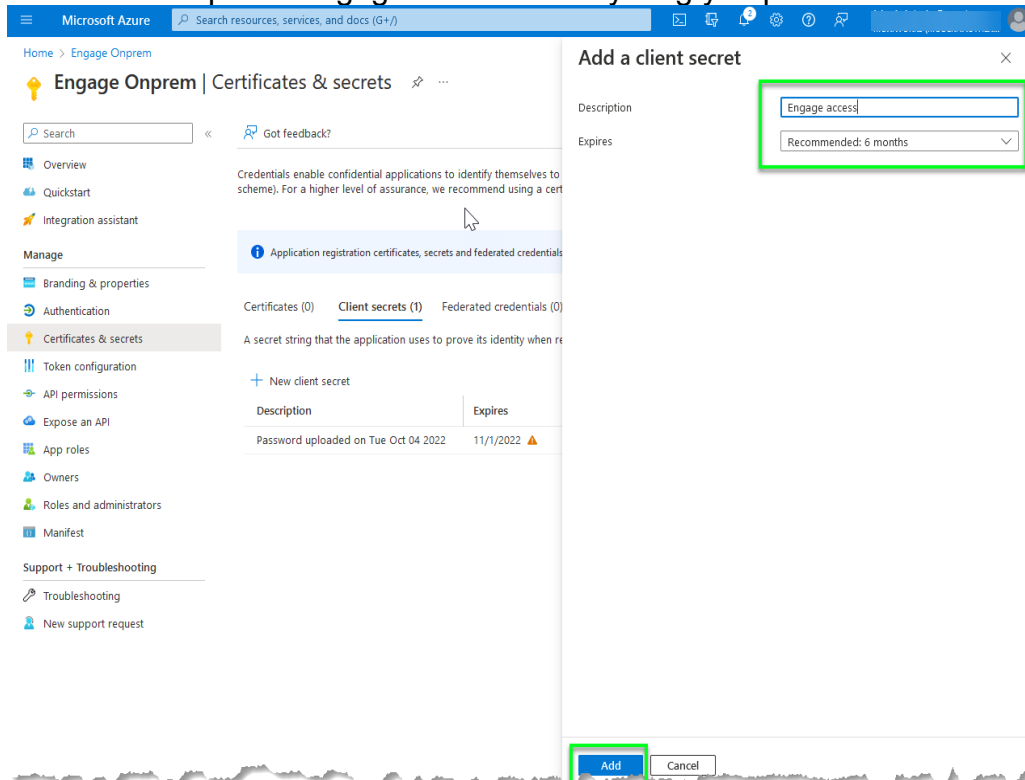
32. Click on the “Certificates & Secrets” option under the “Manage” grouping of the menu.



33. Click “New client secret”.

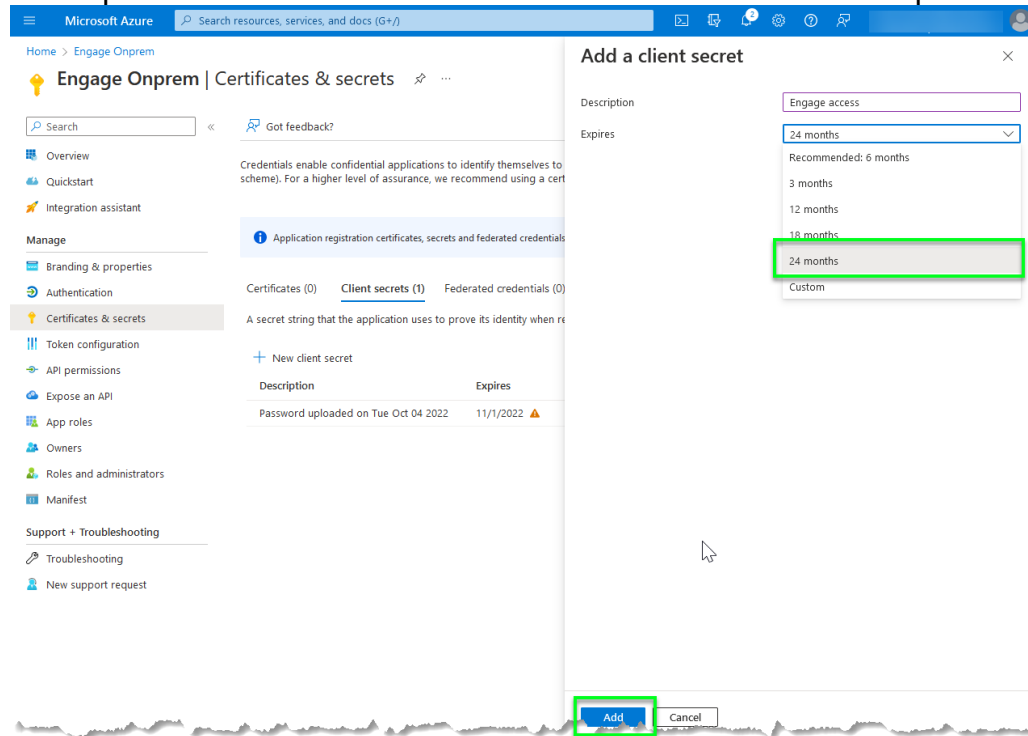


34. Insert a description “Engage access” or anything you prefer.

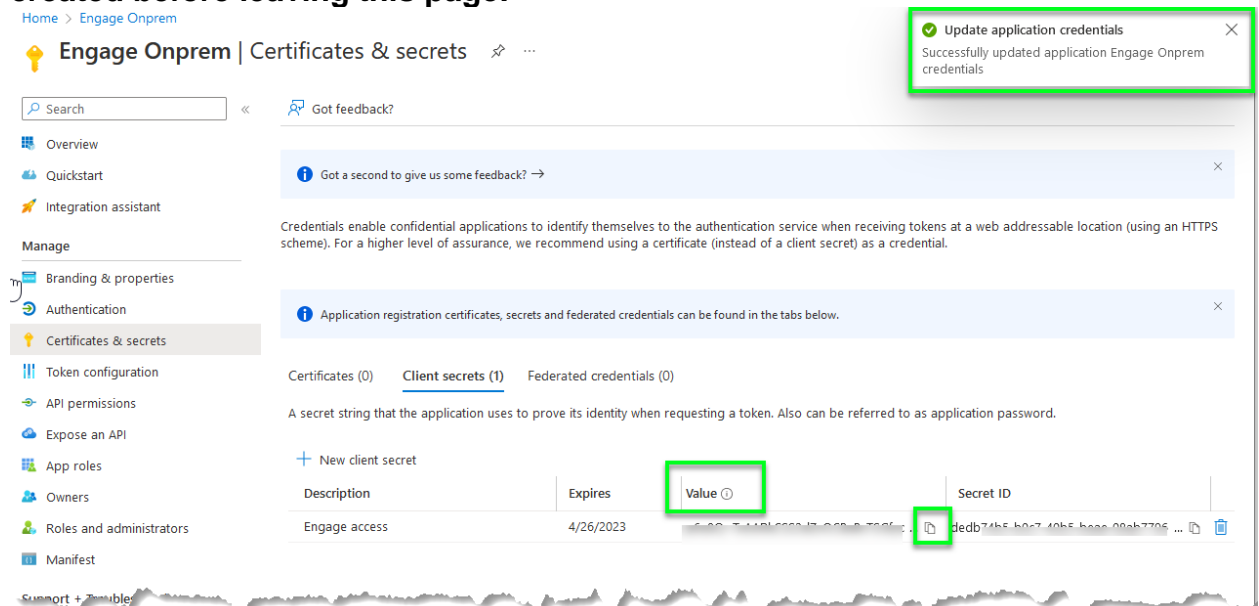


35. In the Expires dropdown menu select a date you would like to grant access to Engage. Please record this date as you will need this information when submitting your credentials. **We recommend a minimum of 2 years.** Note we

will require a new client secret to be created when this secret expires.



36. Find the secret you just created in the list. Click icon to copy the secret into a location to be submitted later. **Note, Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving this page.**



37. Provide to MoxiWorks the values you have saved for the registered application Client ID (step 11), Tenant ID (step 13), the client secret (step 36), and a **standard (non-administrator) user account that may be used for testing the impersonation setup.**

