

MoxiEngage Integration Process using Microsoft 365

Introduction

Don't panic! This setup has been completed by hundreds of individuals with no previous experience in setting up email accounts and/or credentials. This document includes screenshots of each step as well as links to the [training video](#) that goes through the entire process. You got this!

Use the links below to jump to a particular MoxiEngage integration set-up step:

- [Create a Service Account User](#)
- [Grant Application Impersonation to the Service Account User](#)
- [Ensure Service Account User has a Password that Never Expires](#)
- [Register the MoxiEngage Applications as an API Client](#)
- [Submit Credentials to MoxiEngage](#)

If you have questions or concerns, please check out our [Tips and Further Info!](#)

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.

This process is documented step by step in the following training video:

https://www.youtube.com/watch?v=QvU5mnxVjE4&feature=emb_imp_woyt

Additionally, each section of this document includes time stamps and links referring back to this video to assist you.

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.

Service Account Setup

MoxiEngage is designed to utilize service account credentials for organizations that use Microsoft 365 (formerly Office 365) in combination with the EWS Managed API for administration of the company's email functions.

An administrator in your company organization will need to perform steps to create a service account and obtain the necessary credentials for MoxiEngage to use and register an API client for MoxiEngage with appropriate permissions.

Refer to [Microsoft 365 Setup Instructions for Administrators](#) in this document and follow the step-by-step instructions to set up a service account with application impersonation with a password that will not expire and register a client application with delegation access to the EWS Managed API.

You will need to provide the service account email address and non-expiring password, the Client ID for the registered application, and your Microsoft Tenant ID, along with a regular (non-administrator) user email address that we can use for testing.

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, you will be notified. Your email administrator will need to resolve the issue and then provide us with the updated information via a new [Cognito](#) submission. We recommend redoing the entire process in its entirety and creating all new credentials along the way. If you continue to have issues, we recommend you reach out to your email provider for further assistance.

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

The following steps describe the recommended process for creating a service account in Microsoft 365 with the Application Impersonation role for use with your brokerage's MoxiWorks integration. Special consideration must be given to ensure the service account user has a password that never expires. A client application must also be registered and configured with delegation access to the Exchange Web Services (EWS) Managed API to support Modern Authentication.

Note

If your Microsoft 365 instance is hosted by a third-party vendor (i.e., GoDaddy, etc.), your Admin user interface may not match the instructions provided here. Please contact your email vendor for assistance. Feel free to provide a copy of this document to your vendor as a guide and explanation of what is required.

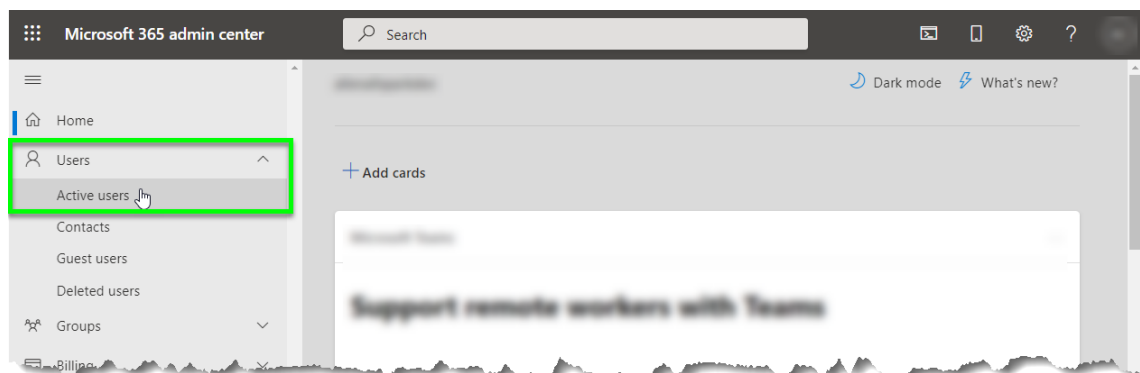
Microsoft 365 menu structure and user interface is subject to change. Steps provided in this document were performed from a computer running Windows 10 Pro against a Microsoft 365 instance created in July 2021. If you are running an on-premises installation of Exchange Server, the actual steps required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

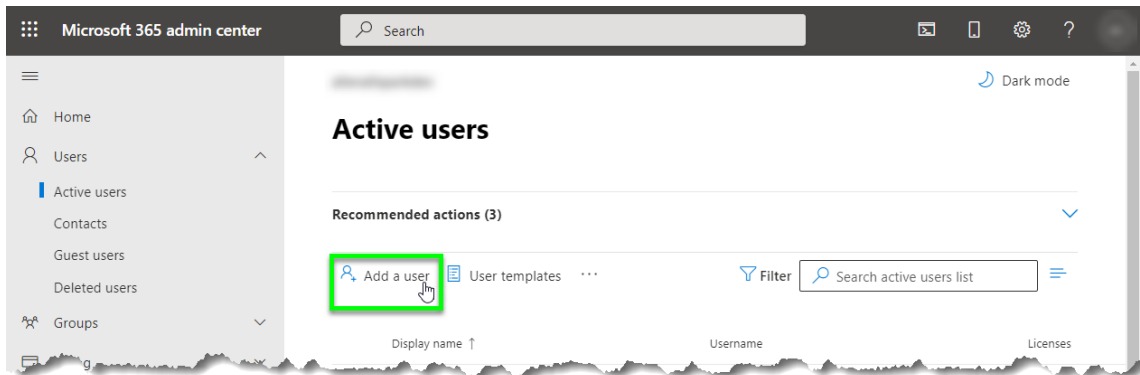
Create a Service Account User

Jump to this step in the [training video](#).

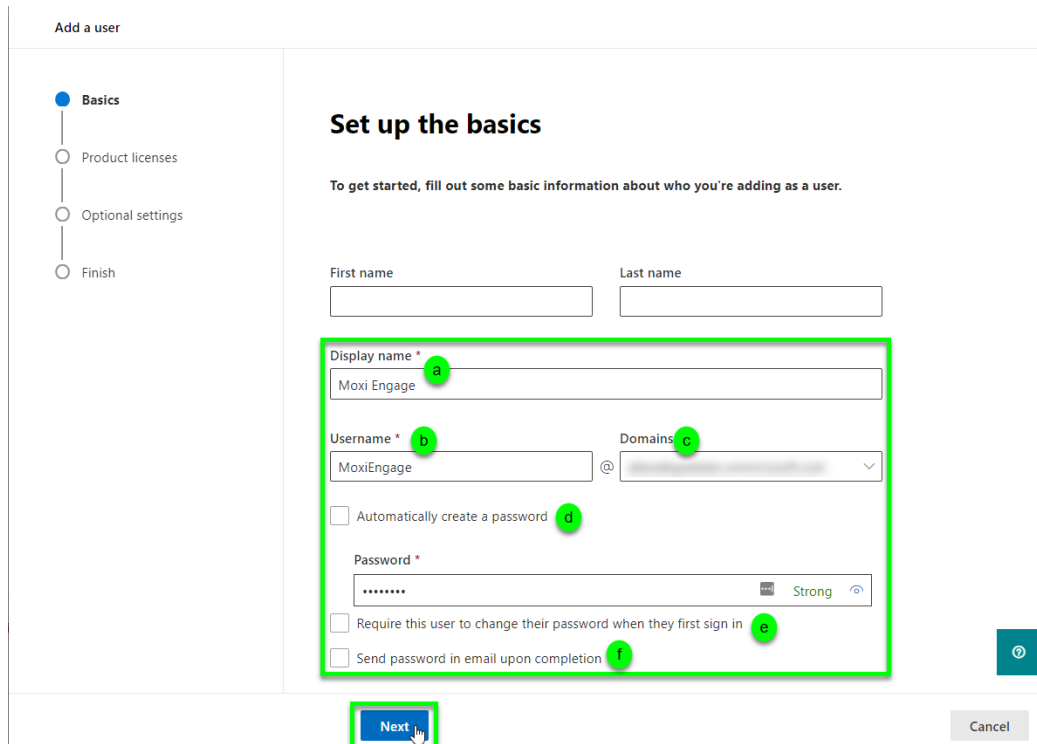
1. Login to your [Microsoft 365 Admin Center](#).
2. Click to expand the "Users" section of the menu, then click on the "Active users" option.



- Click on the “Add a user” action link.



- Enter the following basic information, then click on the “Next” button:
 - Display Name (e.g., Moxi Engage)
 - Username (e.g., MoxiEngage)
 - Domains (select the domain or use the default)
 - Ensure the “Automatically create a password” checkbox is cleared (not marked), then enter a Password. (Be sure to make note of the password so you can provide it to us.)
 - Ensure the “Require this user to change their password when they first sign in” checkbox is cleared (not marked).
 - Ensure the “Send password in email upon completion” checkbox is cleared (not marked).

The screenshot shows the 'Add a user' form. On the left is a progress indicator with steps: Basics (selected), Product licenses, Optional settings, and Finish. The main section is titled 'Set up the basics' and contains the following fields and checkboxes:

- First name and Last name text boxes.
- Display name * text box with 'Moxi Engage' entered (labeled 'a').
- Username * text box with 'MoxiEngage' entered (labeled 'b').
- Domains dropdown menu (labeled 'c').
- Automatically create a password checkbox (labeled 'd'), which is unchecked.
- Password * text box with a masked password and a 'Strong' indicator (labeled 'e').
- Require this user to change their password when they first sign in checkbox (labeled 'e'), which is unchecked.
- Send password in email upon completion checkbox (labeled 'f'), which is unchecked.

At the bottom, the 'Next' button is highlighted with a green box, and a 'Cancel' button is visible on the right.

5. Ensure the correct location is selected, then mark the radio button next to the “Create user without product license” option. A service account user does not require a product license. Click on the “Next” button.

Add a user

✓ Basics

● Product licenses

○ Optional settings

○ Finish

Assign product licenses

Assign the licenses you'd like this user to have.

Select location *
United States

Licenses (0)*

☐ Assign user a product license

☐ **Microsoft 365 E5 Developer (without Windows and Audio Conferencing)**
9 of 25 licenses available

☒ **Create user without product license (not recommended)**
They may have limited or no access to Office 365 until you assign a product license.

Apps (0)

Back

Next

Cancel

6. No optional settings are required at this time. Click on the “Next” button.

Add a user

☒ Basics

☒ Product licenses

☒ **Optional settings**

☐ Finish

Optional settings

You can choose what role you'd like to assign for this user, and fill in additional profile information.

Roles (User: no administration access)

▼


Profile info

▼

Back

Next

Cancel



7. Review your changes, then click on the “Finish adding” button.

Add a user

✓ Basics

✓ Product licenses


✓ Optional settings

● Finish

Review and finish

Assigned Settings

Review all the info and settings for this user before you finish adding them.

Display and username
Moxi Engage
MoxiEngage@ 
[Edit](#)

Password
Type: Custom password
[Edit](#)

Product licenses
Create user without product license.
[Edit](#)


Roles (default)
User (no admin center access)
[Edit](#)

Profile info

[Back](#)

[Finish adding](#)

[Cancel](#)



8. View the confirmation that the new user has been added. Click on the “Close” button.

Add a user

✓ Basics

✓ Product licenses

✓ Optional settings

✓ Finish

✓ **Moxi Engage added to active users**

Moxi Engage will now appear in your list of active users.

User details
Display name: Moxi Engage
Username: MoxiEngage@
Password: ***** [Show](#)

Licenses bought
None

Licenses assigned
None

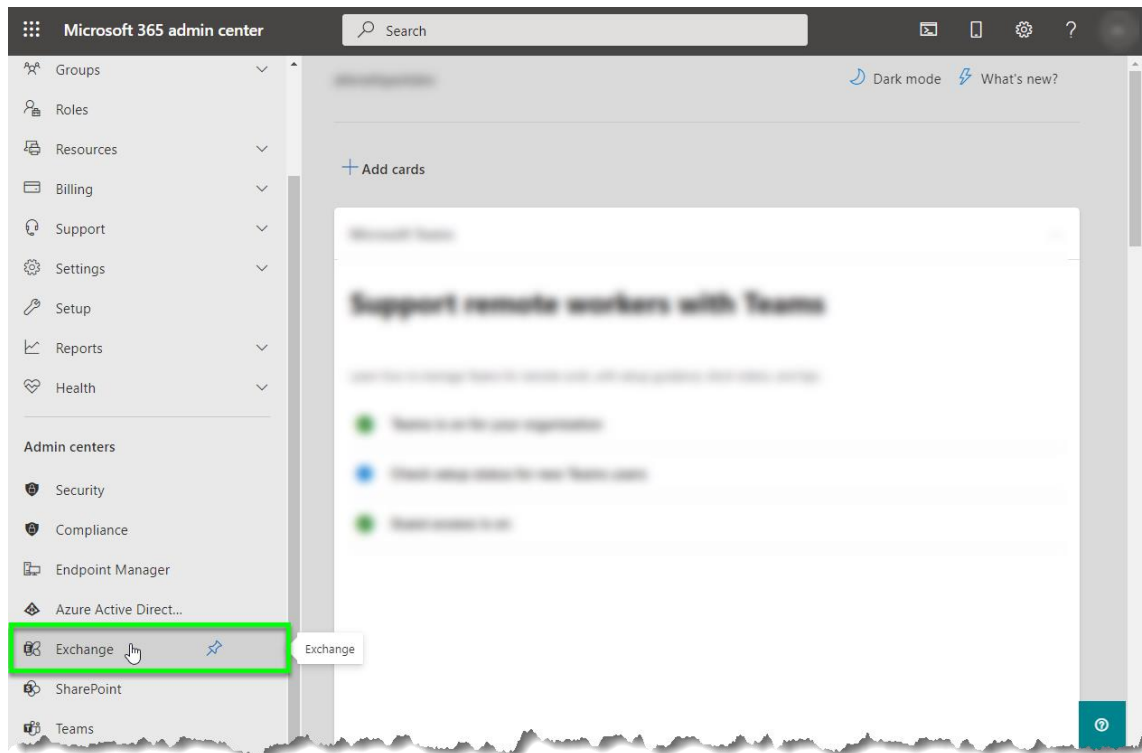
Save these user settings as a template?
User templates allow you to quickly add similar users in the future by saving a set of shared settings such as domain, password, product licenses, and roles.
[Review settings for this user template](#)

Close

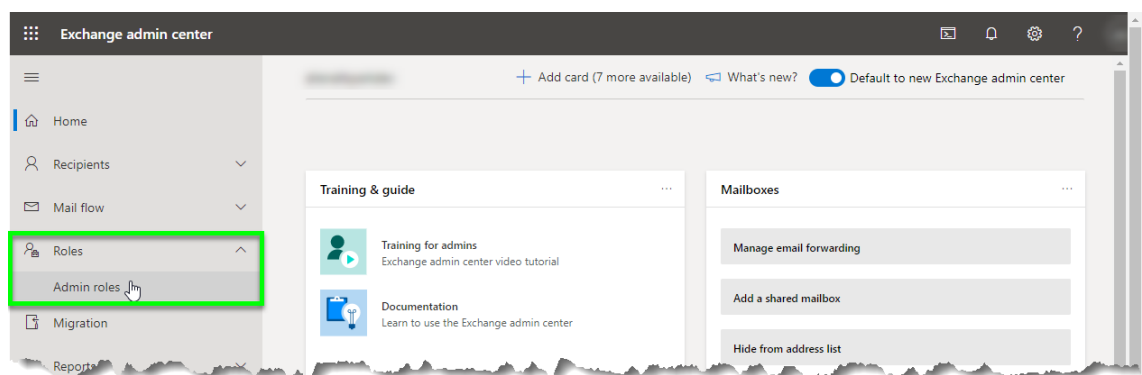
Grant Application Impersonation to the Service Account User

Jump to this step in the [training video](#).

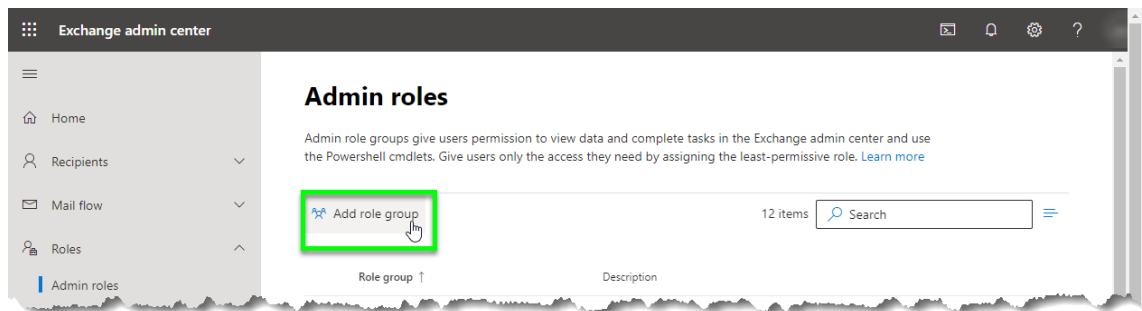
1. Login to your [Microsoft 365 Admin Center](#).
2. Click on the “Exchange” menu option under the “Admin centers” area of the menu. (If this option is not visible, you can click on “Show all” to expand the menu.)



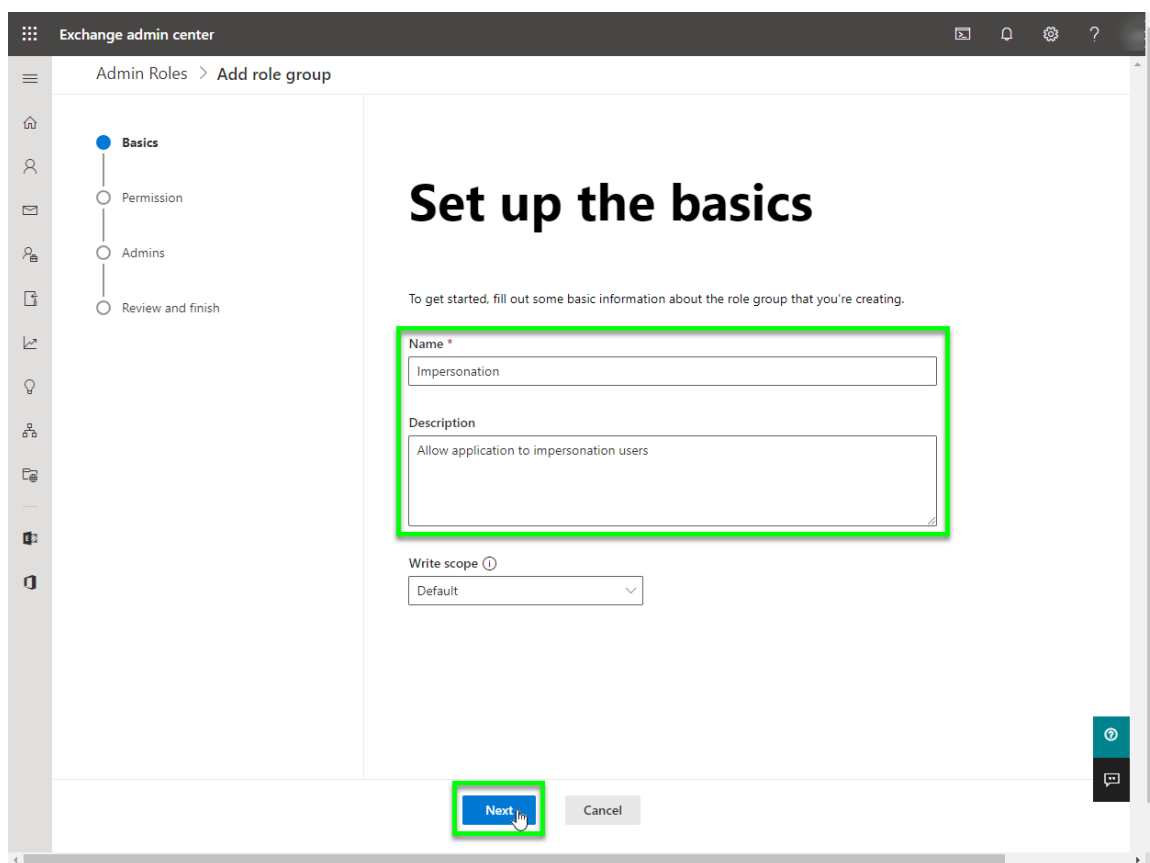
3. In the Exchange Admin Center, expand the “Roles” area of the menu and click on the “Admin roles” option.



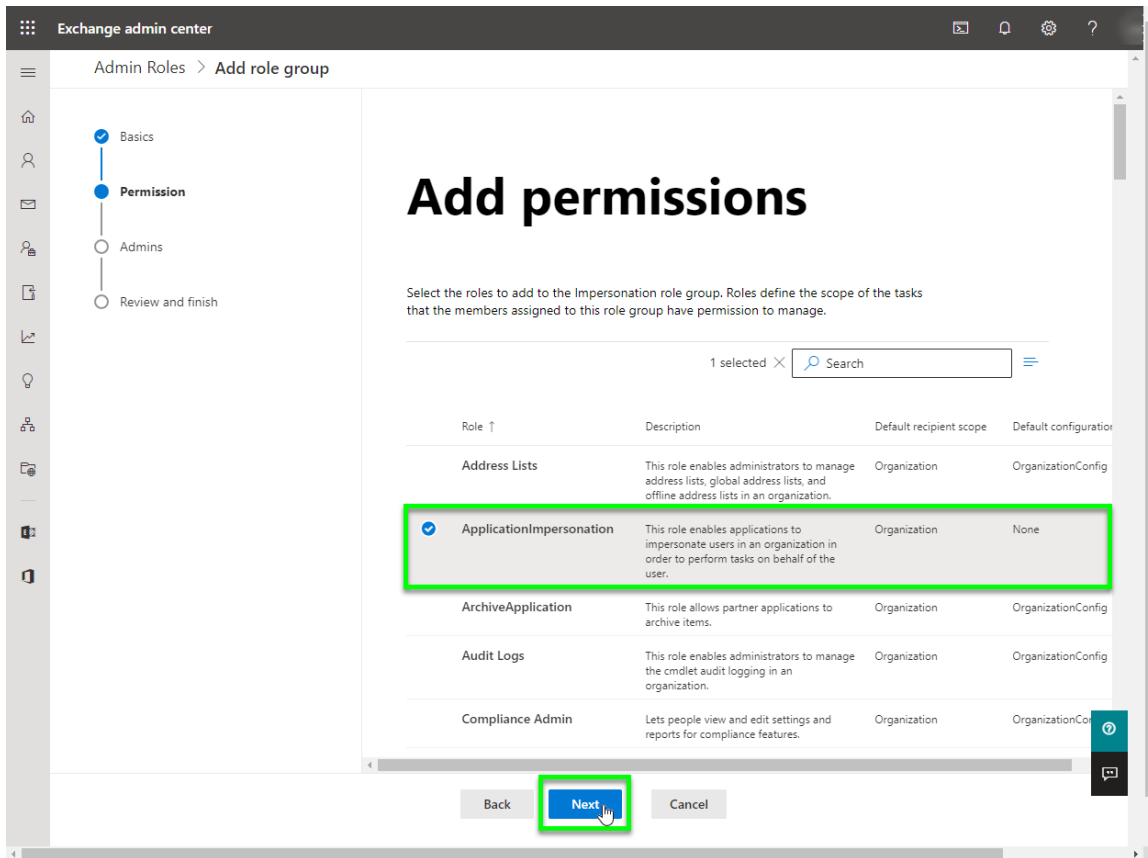
- Click on the “Add role group” option button.



- Enter a Name and Description for the new role group, then click on the “Next” button.



6. Select the “ApplicationImpersonation” role, then click on the “Next” button.



Exchange admin center

Admin Roles > Add role group

Basics
Permission
Admins
Review and finish

Add permissions

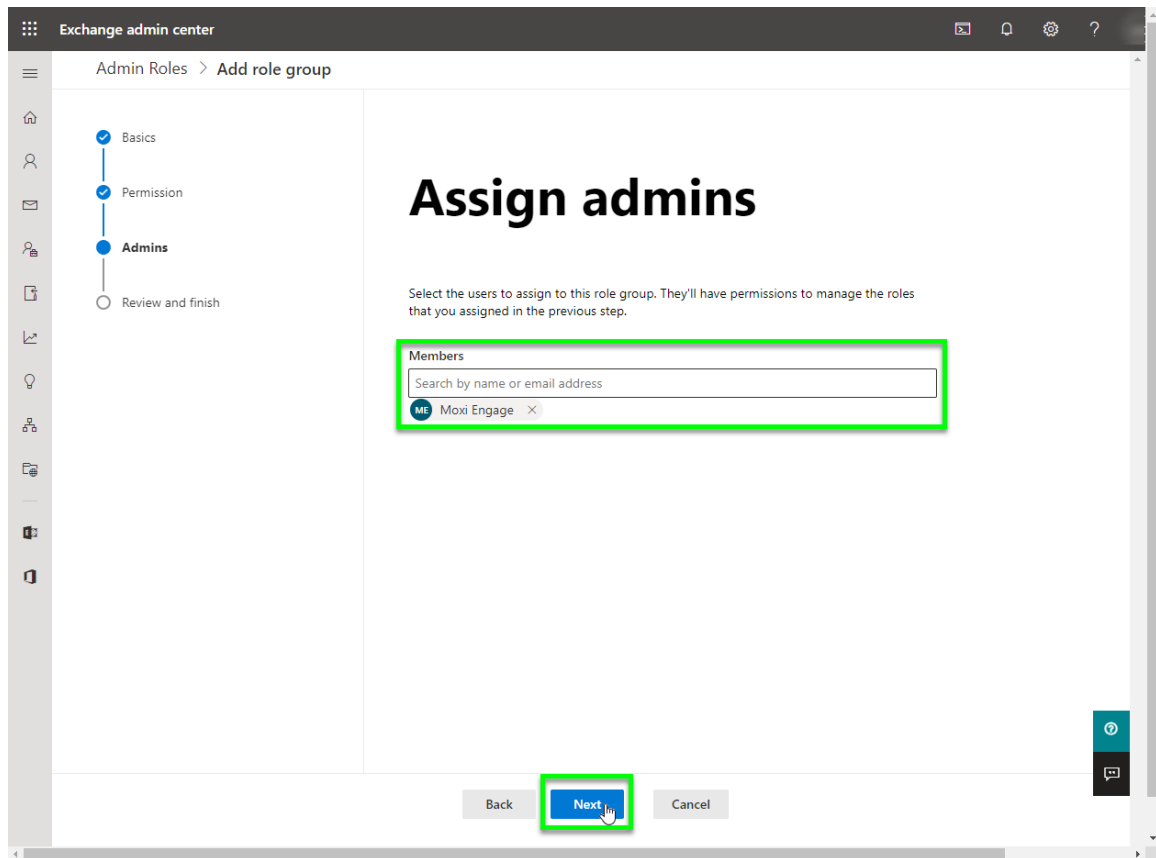
Select the roles to add to the Impersonation role group. Roles define the scope of the tasks that the members assigned to this role group have permission to manage.

1 selected X Search

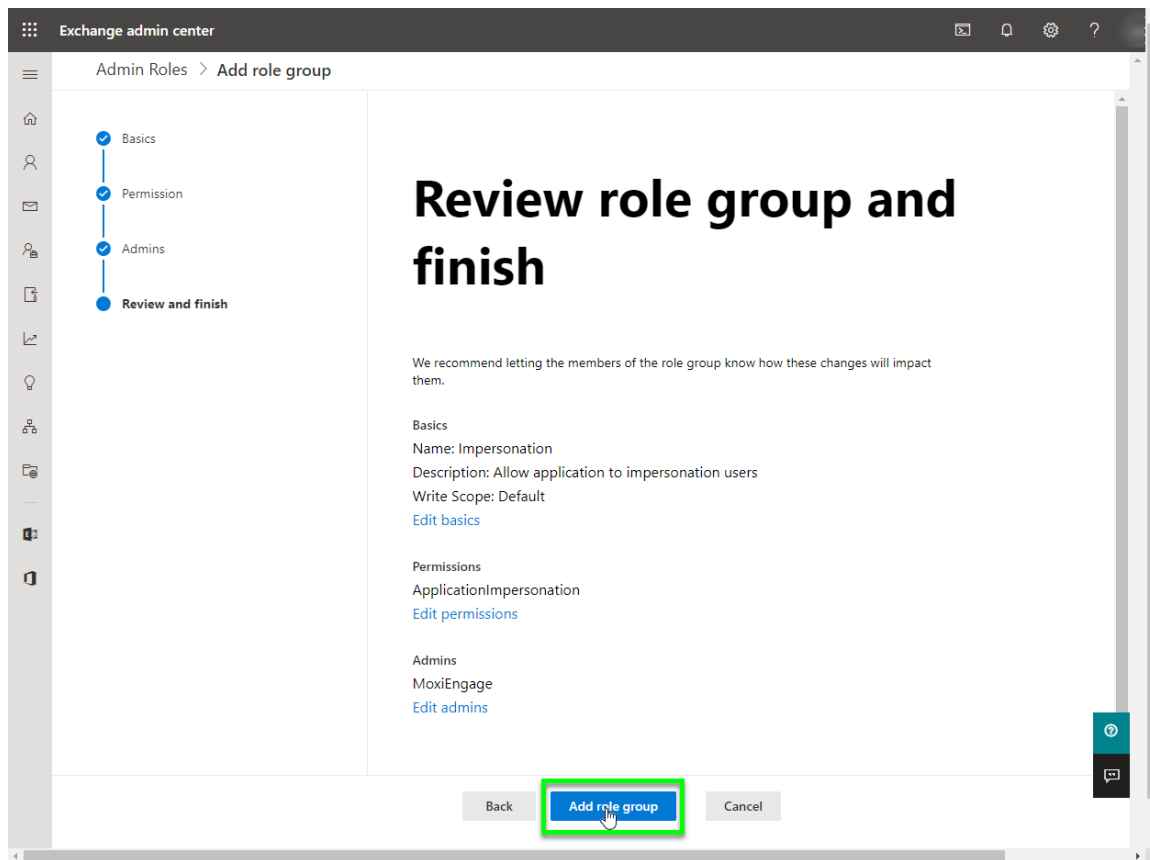
Role ↑	Description	Default recipient scope	Default configuration
Address Lists	This role enables administrators to manage address lists, global address lists, and offline address lists in an organization.	Organization	OrganizationConfig
<input checked="" type="checkbox"/> ApplicationImpersonation	This role enables applications to impersonate users in an organization in order to perform tasks on behalf of the user.	Organization	None
ArchiveApplication	This role allows partner applications to archive items.	Organization	OrganizationConfig
Audit Logs	This role enables administrators to manage the cmdlet audit logging in an organization.	Organization	OrganizationConfig
Compliance Admin	Lets people view and edit settings and reports for compliance features.	Organization	OrganizationConfig

Back Next Cancel

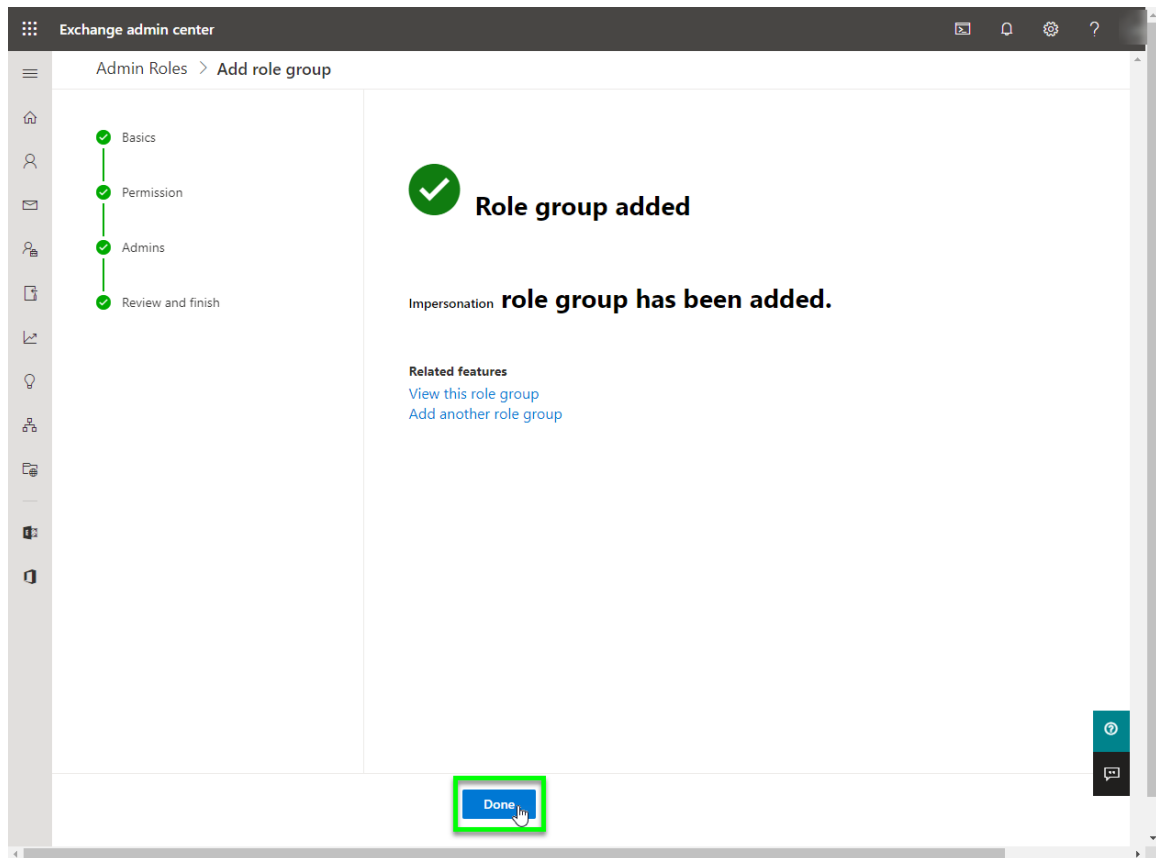
7. Search for and add the MoxiEngage service account, then click on the “Next” button.



8. Review your changes, then click on the “Add role group” button.



9. View the confirmation that the role group has been added, then click on the “Done” button.



Ensure Service Account User has a Password that Never Expires

Jump to this step in the [training video](#).

Connectivity to your Microsoft 365 instance depends on having the correct credentials stored and available for use when synchronizing your agents' contact data. When the service account password expires, synchronization will be interrupted until the password has been reset, provided to MoxiWorks, and stored securely for MoxiEngage to authenticate against your account.

Unlike the classic Active Directory interface, Azure Active Directory does not provide a simple method to set a password to never expire for a single user. Instead, setting a user's password to never expire must be done using the AzureAD module in PowerShell.

1. Run Windows PowerShell as an administrator. (From your Windows Start menu, right click over the Windows PowerShell shortcut, select More => Run as administrator.)
2. At the PowerShell prompt, type

```
Install-Module -Name AzureAD
```

and press Enter on your keyboard to begin installation of the Azure AD module.



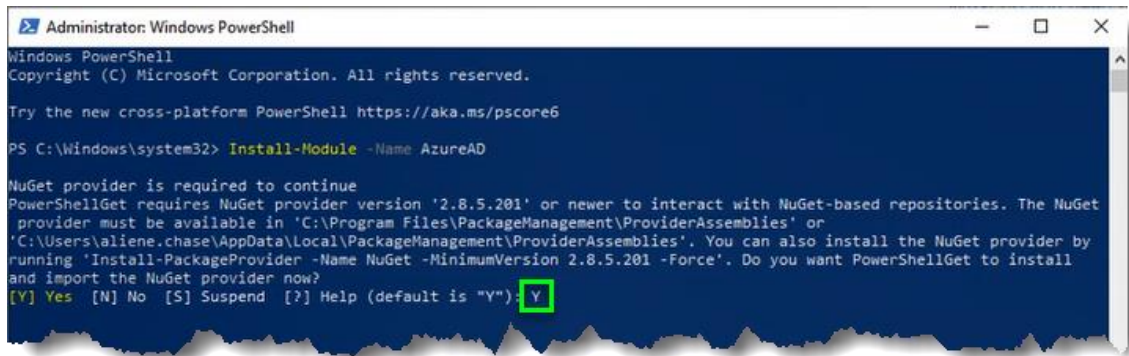
Note

If the AzureAD module is already installed, the message prompts shown in steps 3-5 will not be displayed.

3. Type

```
Y
```

and press Enter on your keyboard to accept installation of the NuGet provider.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

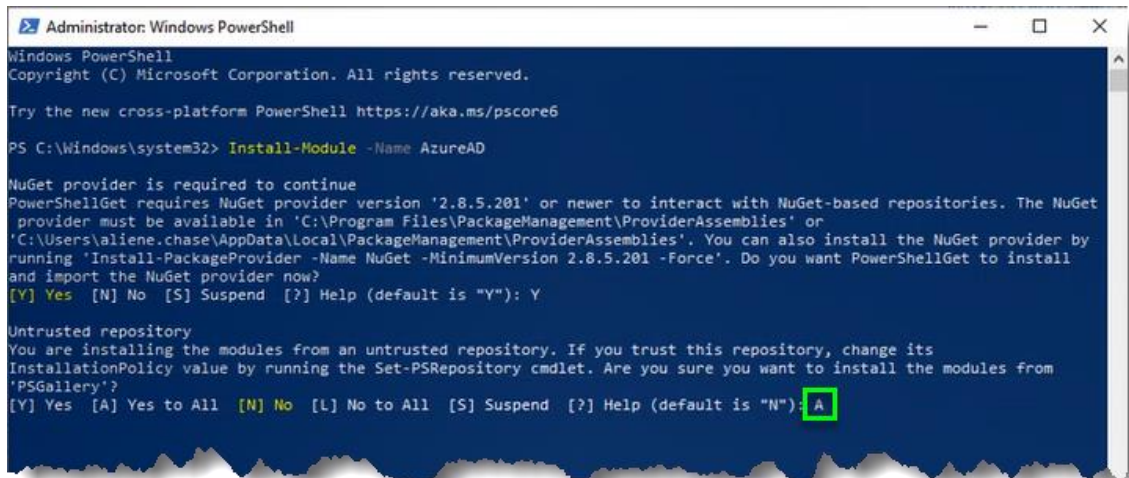
PS C:\Windows\system32> Install-Module -Name AzureAD

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\aliene.chase\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
```

4. Wait for the next prompt.
5. The AzureAD module is part of the PowerShell Gallery (PSGallery), which is not by default configured as a trusted repository for PowerShell. If a message is displayed about an untrusted repository, review the warning. If you wish to continue the installation, type

A

and press Enter on your keyboard.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Install-Module -Name AzureAD

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\aliene.chase\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
```

6. Wait for the next prompt. It may take a few minutes to complete the installation.
7. At the prompt, type

Connect-AzureAD

and press Enter on your keyboard.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

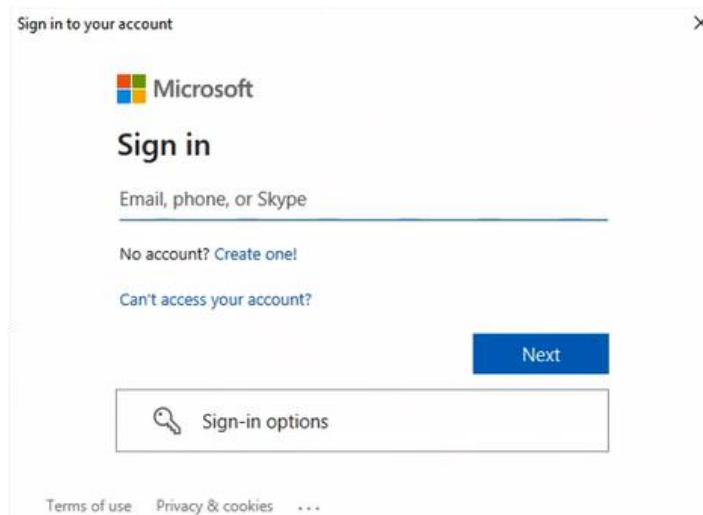
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Install-Module -Name AzureAD

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\aliene.chase\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Windows\system32> Connect-AzureAD
```

8. Follow the on-screen instructions to log into your Microsoft 365 account using a login with administrative rights. The login screen that may appear as a pop-up over your PowerShell window supports multi-factor authentication (MFA).



Sign in to your account

Microsoft


Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

[Next](#)

 Sign-in options

[Terms of use](#) [Privacy & cookies](#) ...

9. When you have logged in successfully, connection information including your login account, environment, and domain will be displayed.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Connect-AzureAD

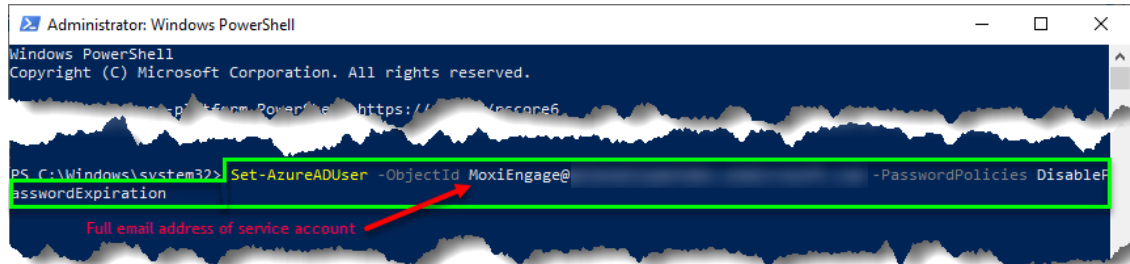
Account Environment TenantId TenantDomain
-----
PS C:\Windows\system32>
```

Connection details confirm you are logged in

10. At the prompt, type

```
Set-AzureADUser -ObjectId {email address} -PasswordPolicies DisablePasswordExpiration
```

replacing "{email address}" with the email address of the service account you created for MoxiEngage, and press Enter on your keyboard.

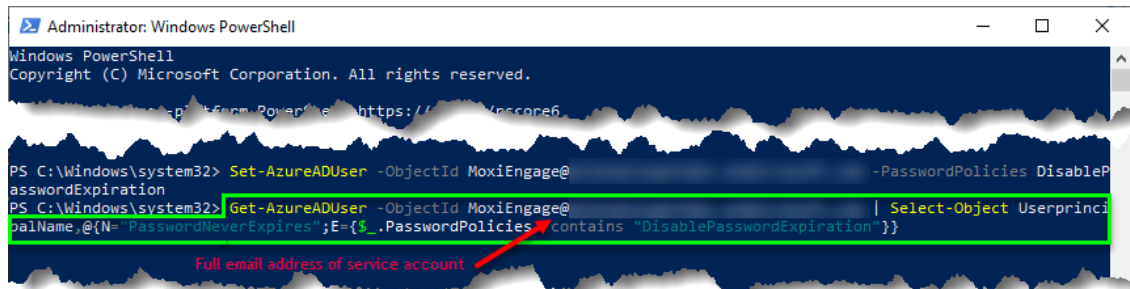


The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt is at C:\Windows\system32. The command entered is `Set-AzureADUser -ObjectId MoxiEngage@ -PasswordPolicies DisablePasswordExpiration`. A red arrow points to the email address `MoxiEngage@` in the command, with a label "Full email address of service account" below it.

11. To verify the service account's password is set to never expire, type

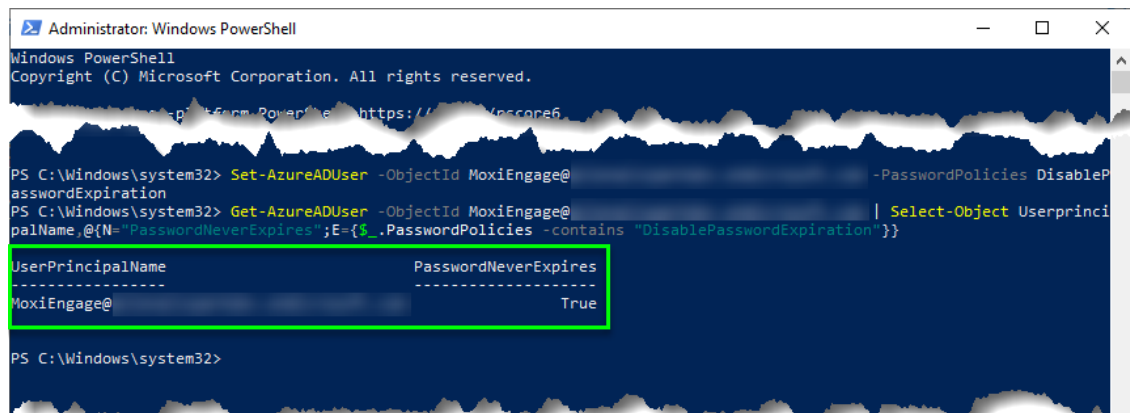
```
Get-AzureADUser -ObjectId {email address} | Select-Object UserprincipalName,@{N="PasswordNeverExpires";E={$_.PasswordPolicies -contains "DisablePasswordExpiration"}}
```

replacing "{email address}" with the email address of the service account you created for MoxiEngage, and press Enter on your keyboard.



The screenshot shows the same Windows PowerShell window. The command entered is `Get-AzureADUser -ObjectId MoxiEngage@ | Select-Object UserprincipalName,@{N="PasswordNeverExpires";E={$_.PasswordPolicies -contains "DisablePasswordExpiration"}}`. A red arrow points to the email address `MoxiEngage@` in the command, with a label "Full email address of service account" below it.

12. Observe the displayed confirmation that the password never expires.



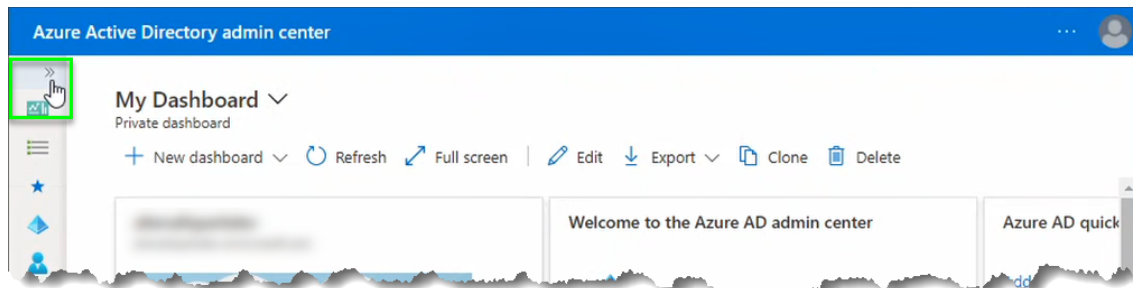
The screenshot shows the output of the command from the previous step. The output is a table with two columns: `UserPrincipalName` and `PasswordNeverExpires`. The first row shows `MoxiEngage@` and `True`. A green box highlights the output table.

UserPrincipalName	PasswordNeverExpires
MoxiEngage@	True

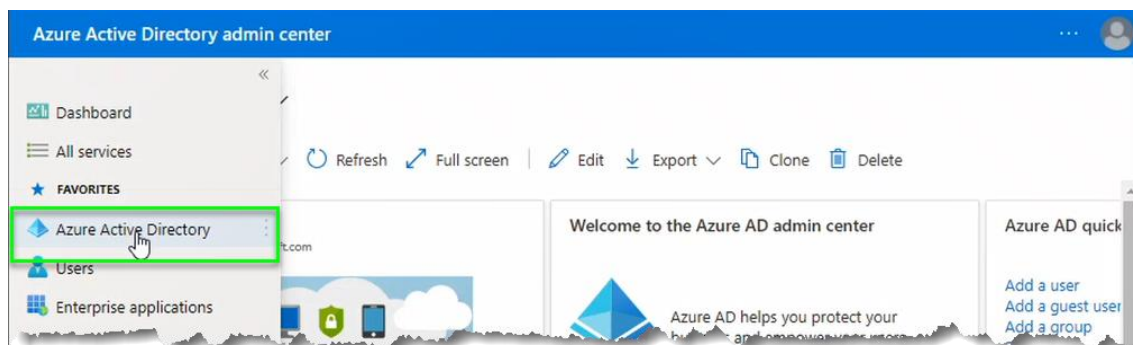
Register the MoxiEngage Application as an API Client

Jump to this step in the [training video](#).

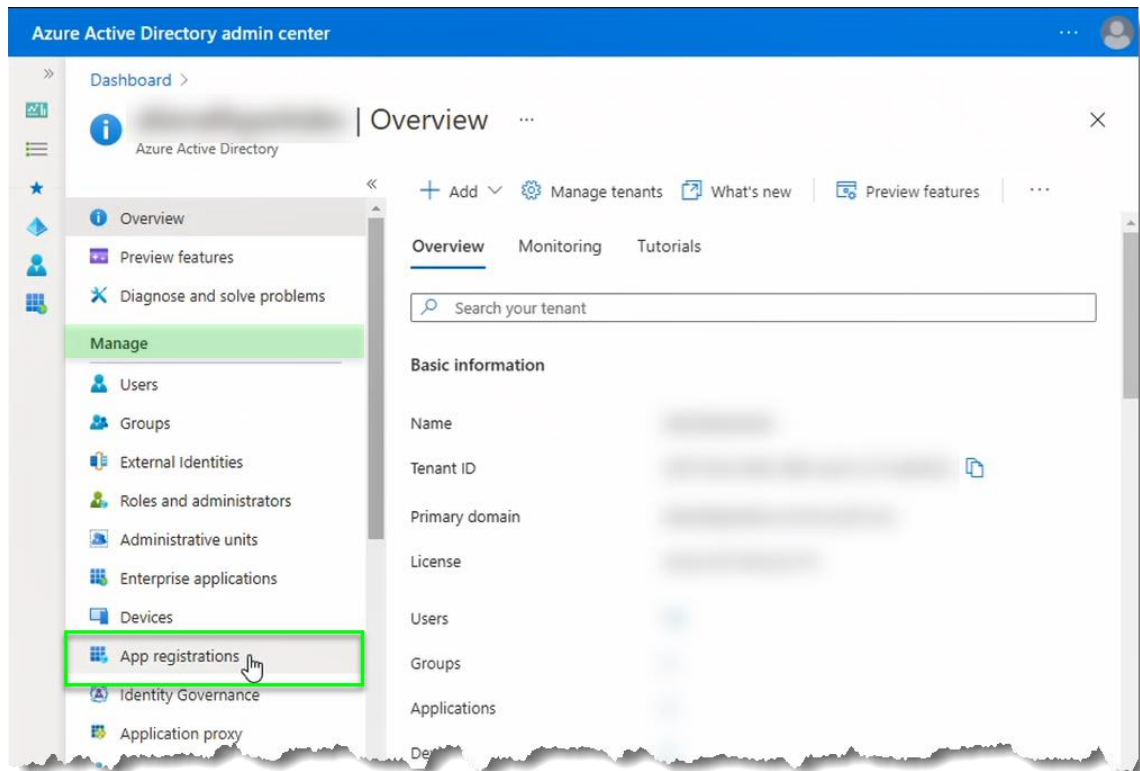
1. Login to your [Azure Active Directory Admin Center](#).
2. Click on the double chevron in the top left corner of the screen to expand the written menu.



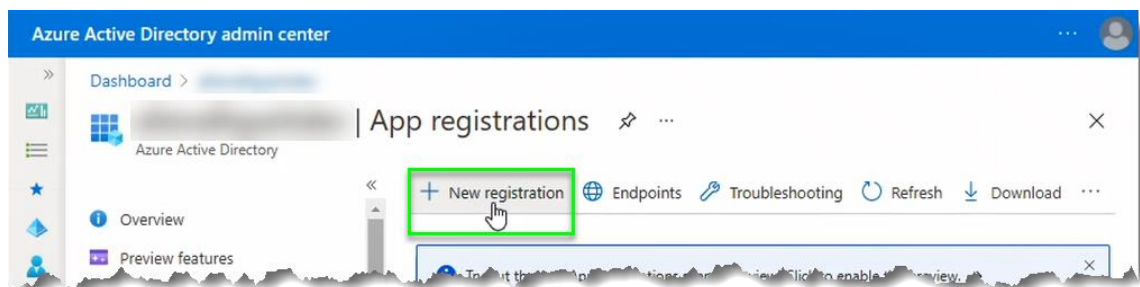
3. Click on the "Azure Active Directory" option in the menu.



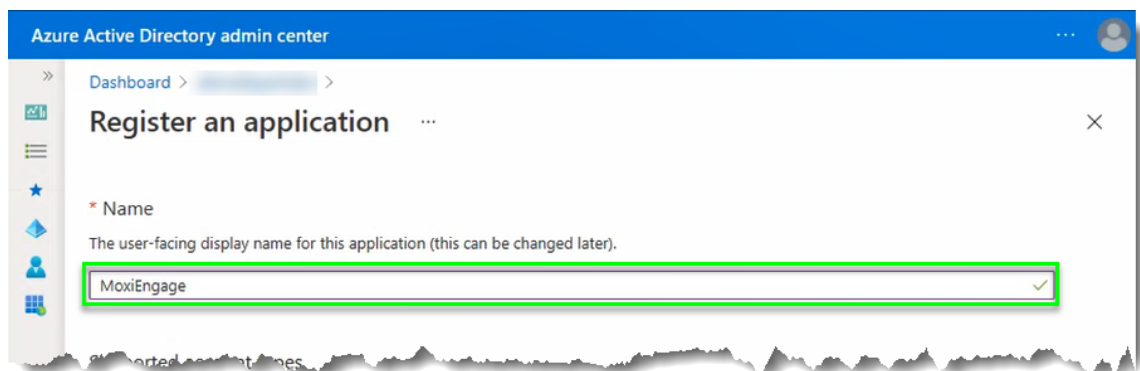
- From the Azure Active Directory Dashboard for your Microsoft 365 instance, click on the “App Registrations” menu option under the “Manage” grouping.



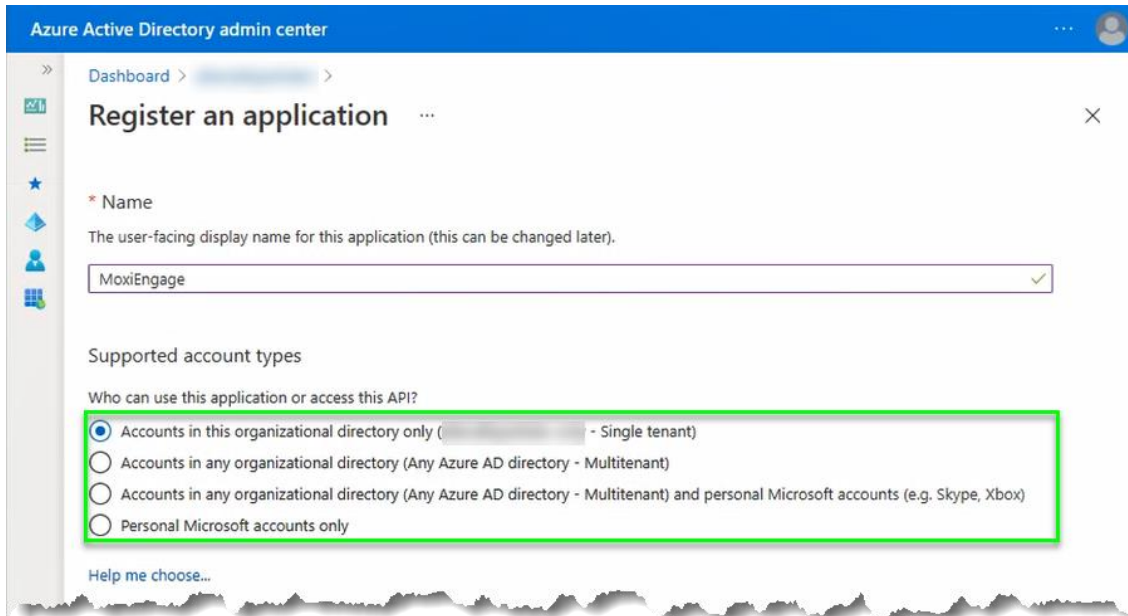
- Click on the “New registration” link.



- 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 ✓

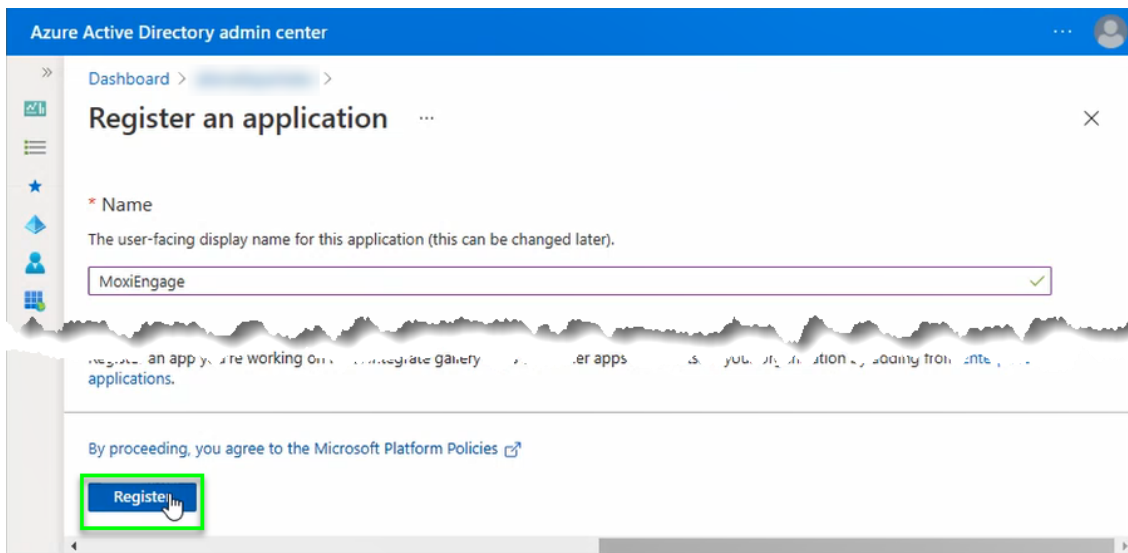
Supported account types

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

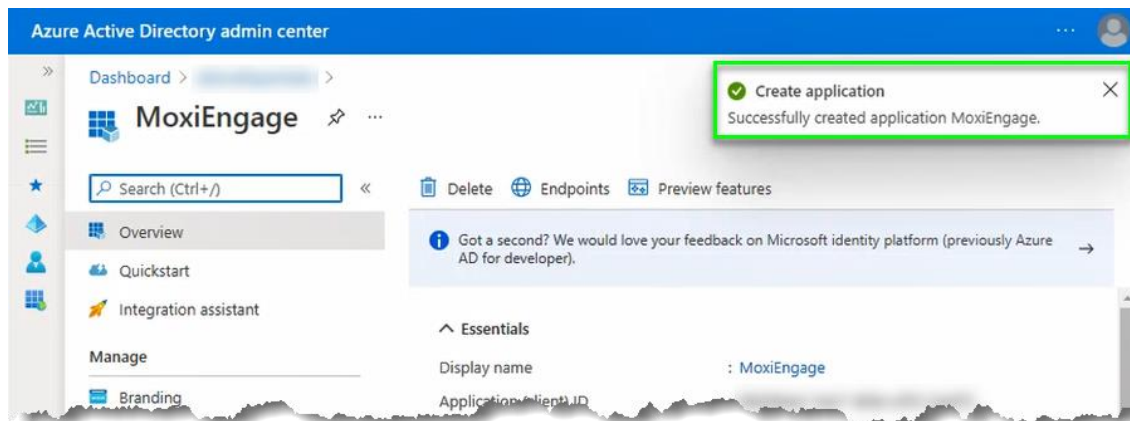
The user-facing display name for this application (this can be changed later).

MoxiEngage ✓

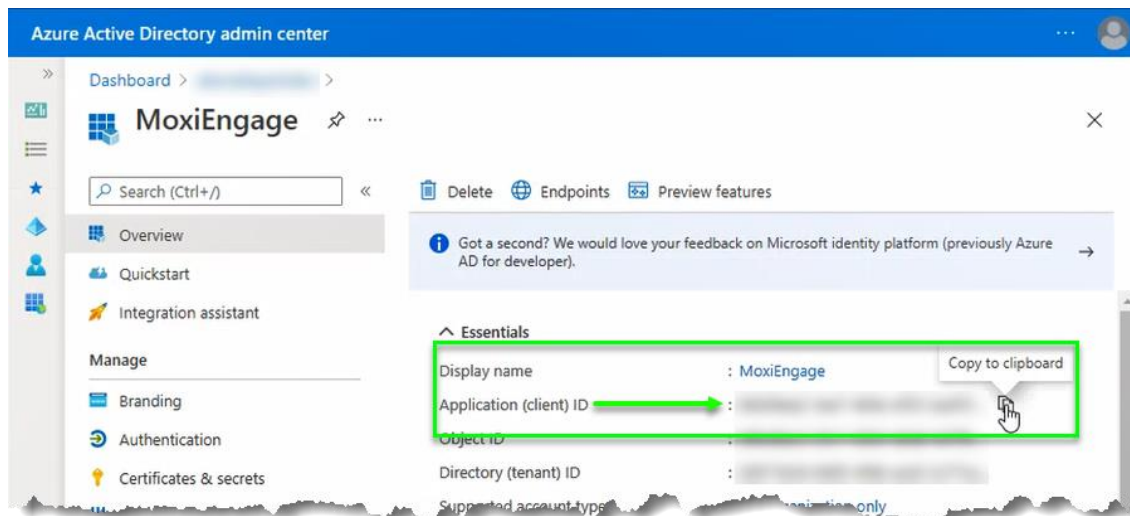
By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

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

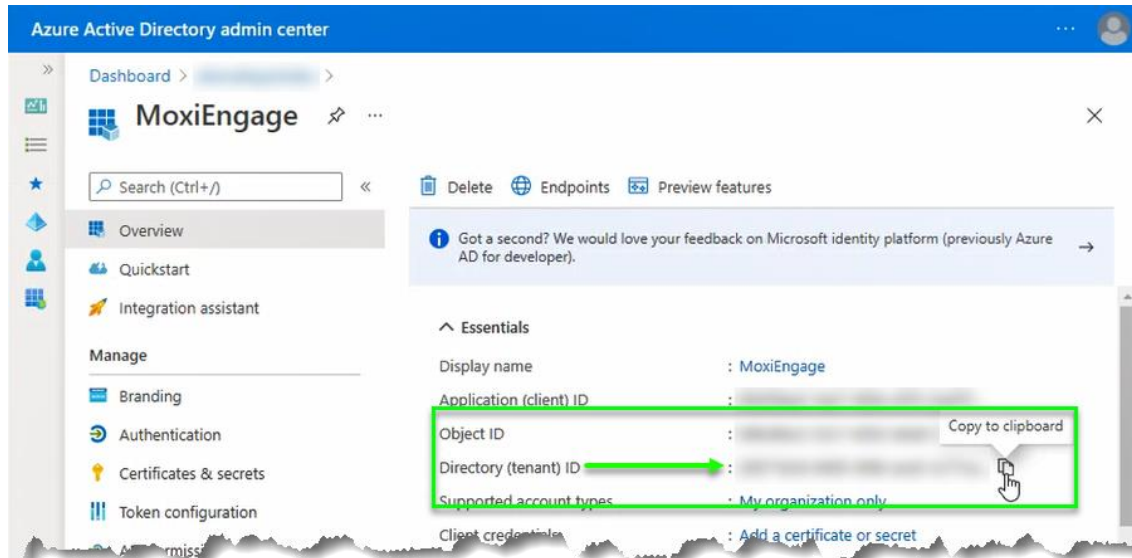


11. Locate the value next to the "Application (client) ID" label, then click on the "Copy to clipboard" button (only visible when you hover over the value).

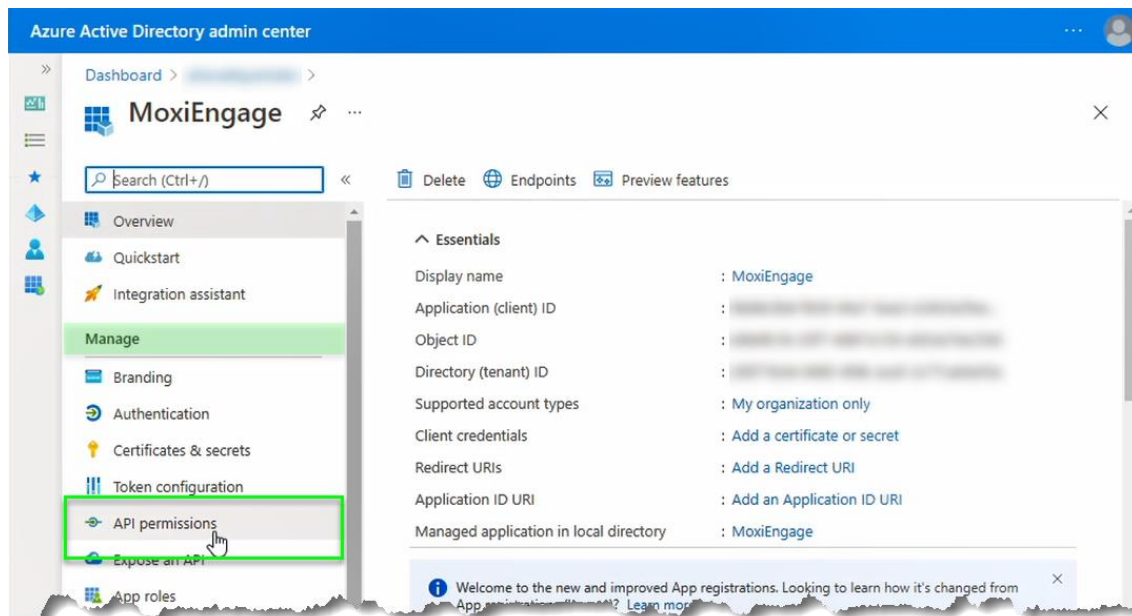


12. Paste the value to a text file for reference. You will need to provide this value to MoxiWorks as your Client ID.

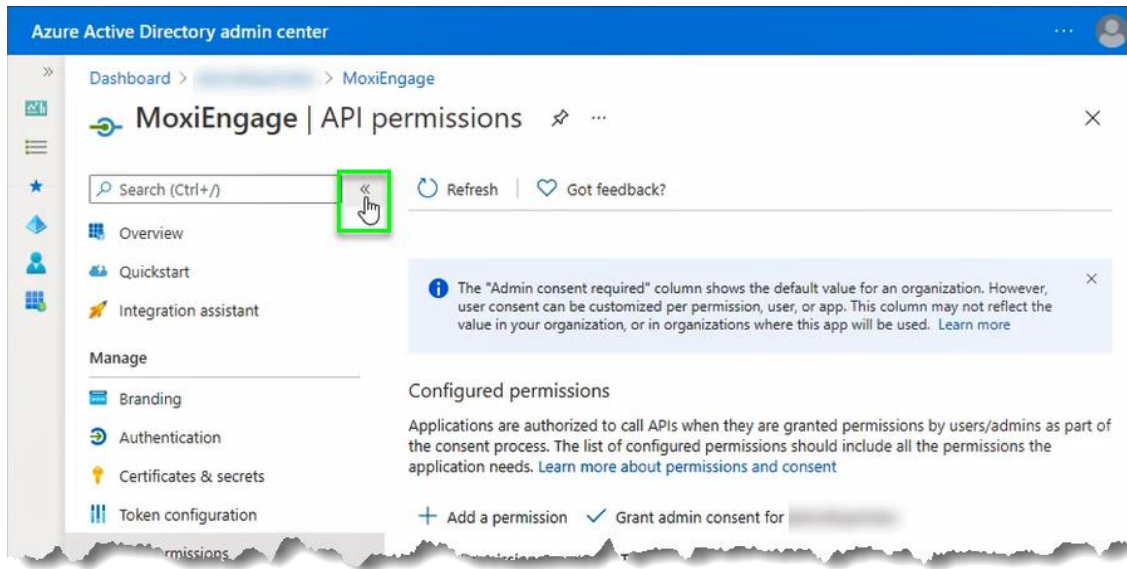
13. Locate the value next to the “Directory (tenant) ID” label, then click on the “Copy to clipboard” button (only visible when you hover over the value).



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.



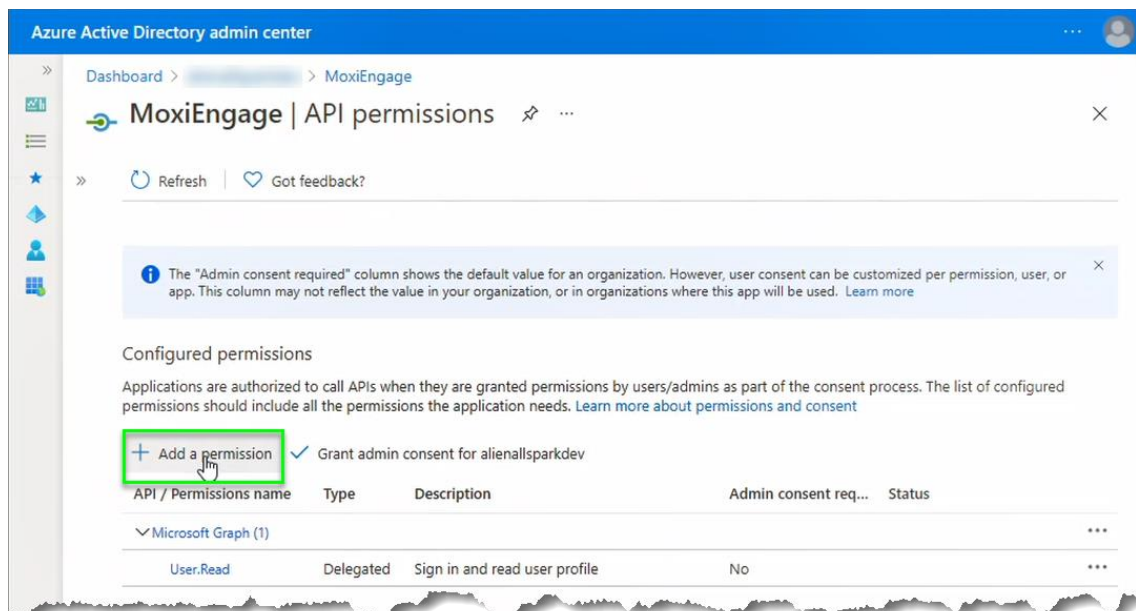
16. Click on the double chevron to collapse the side menu.



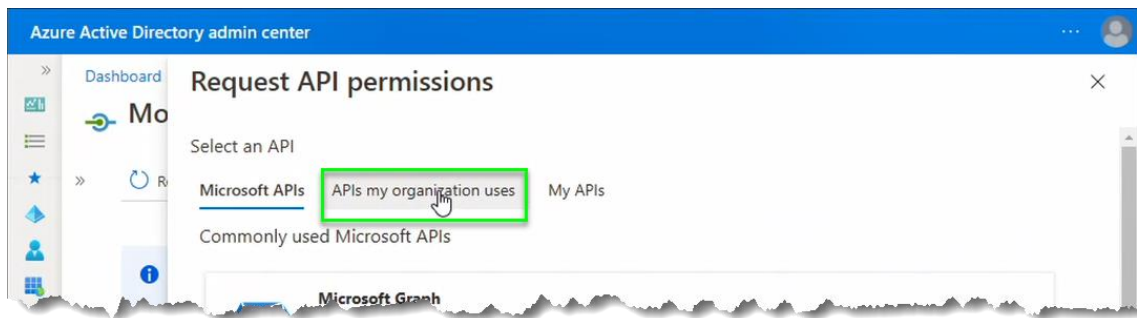
Note

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.

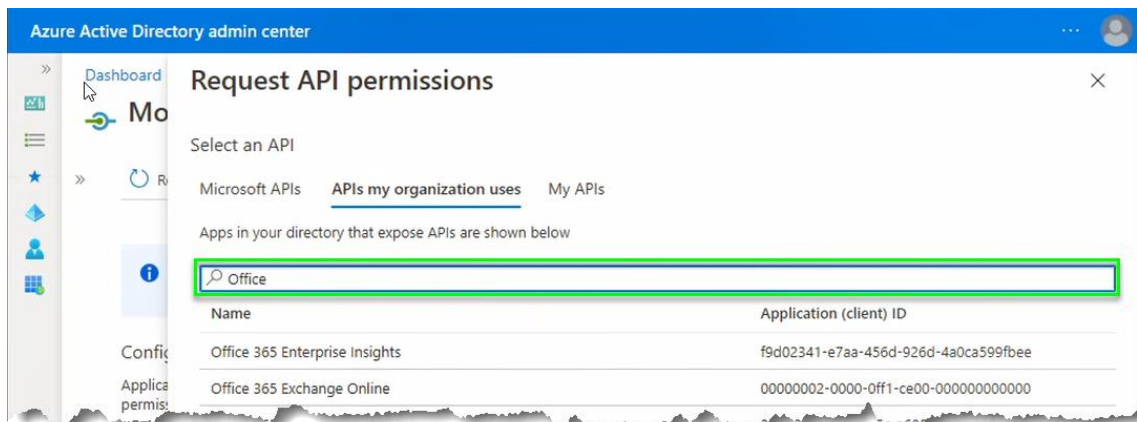
17. Click on the “Add a permission” link.



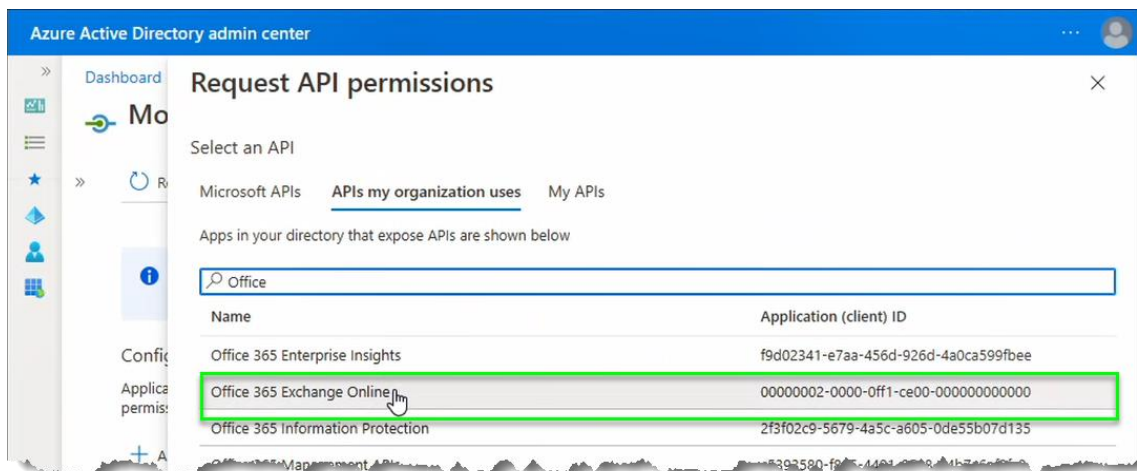
18. Click on “APIs my organization uses” tab to change the view of available APIs.



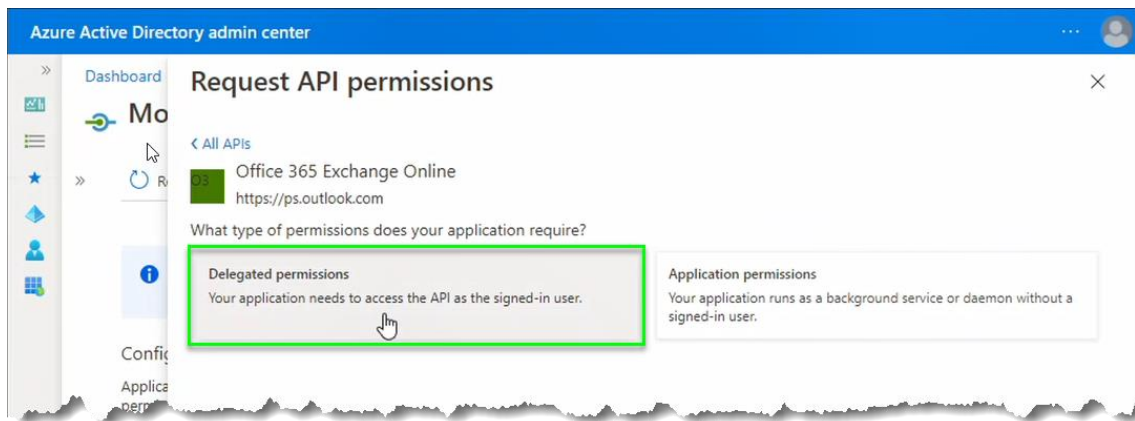
19. Type “Office” in the Search box to filter the API list.



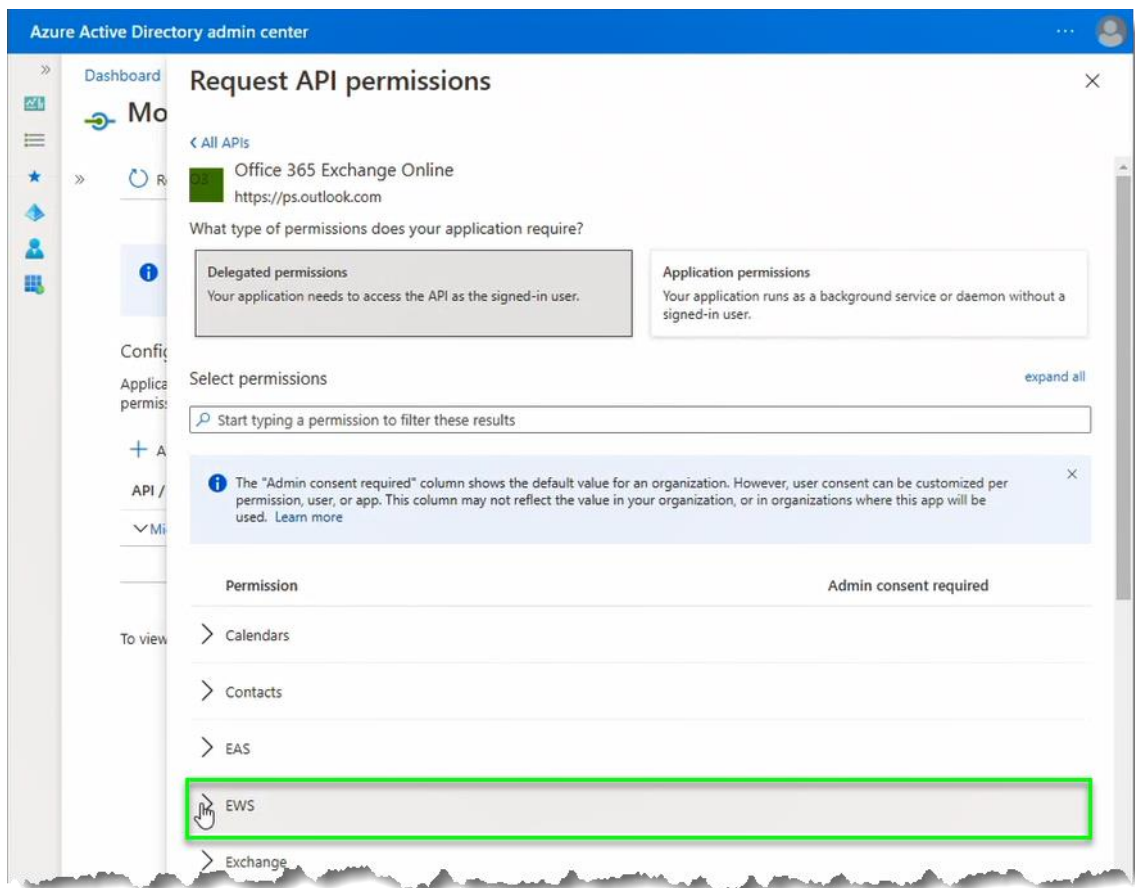
20. Click on the “Office 365 Exchange Online” API name.



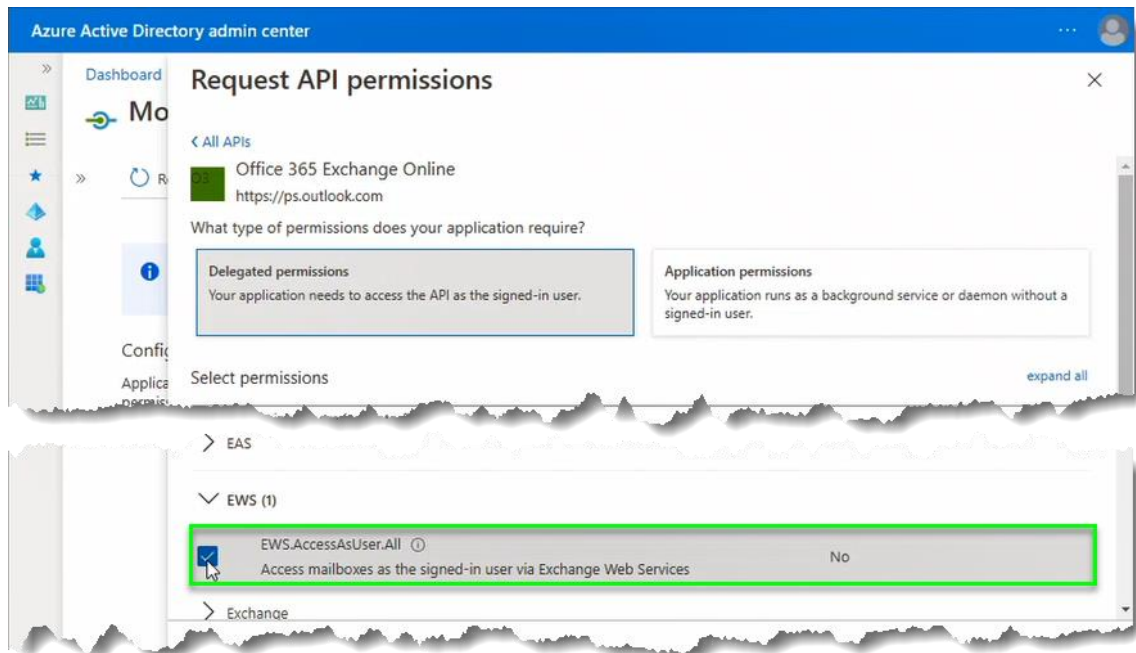
21. Click on the button with “Delegated permissions” as the title.



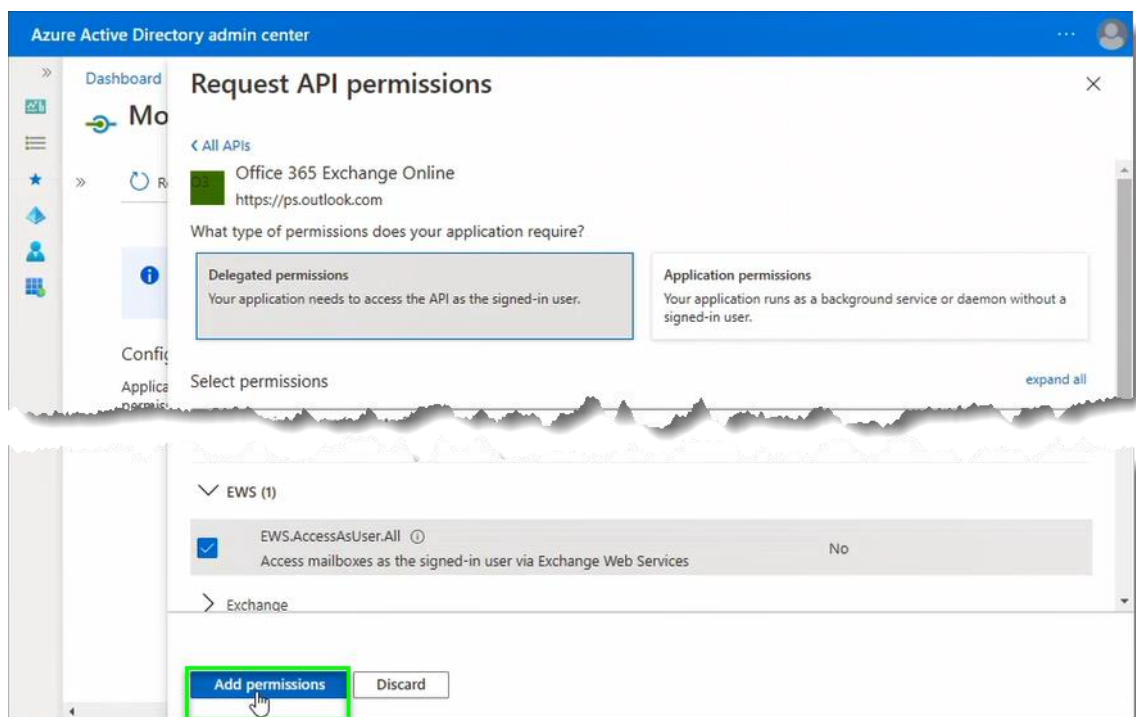
22. Locate the “EWS” item under the “Select permissions” area of the screen, then click to expand the permission group.



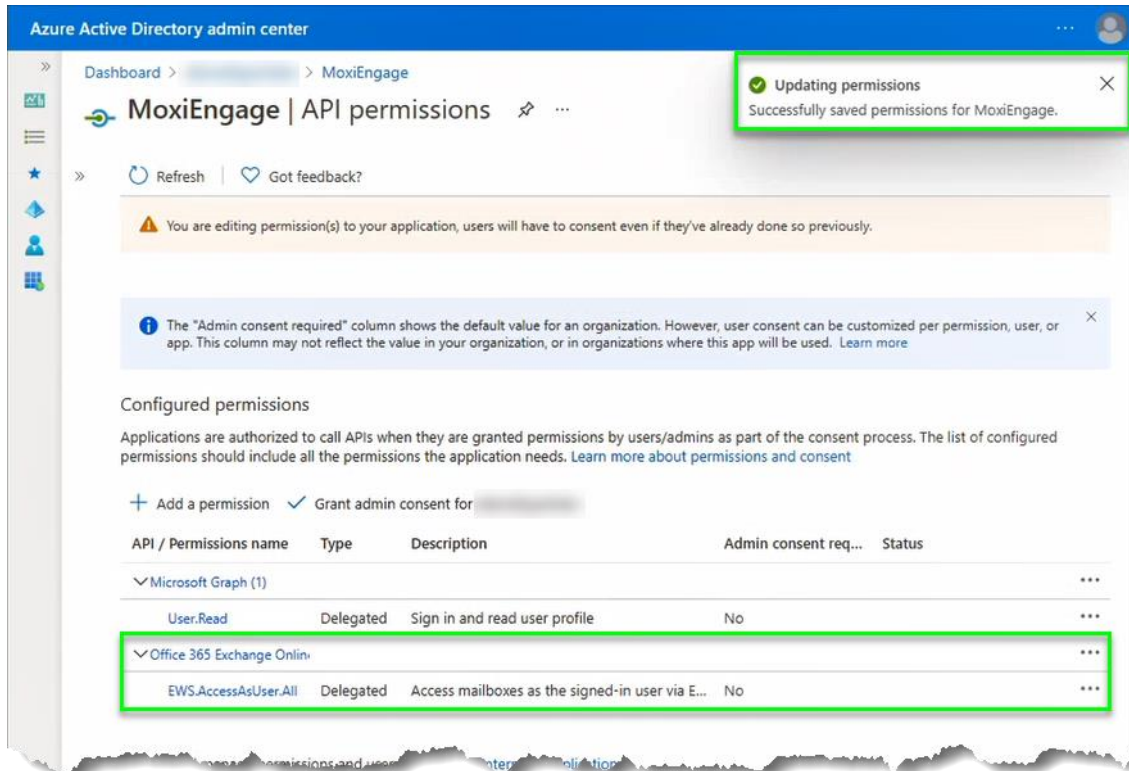
23. Check the box next to the “EWS.AccessAsUser.All” permission under the “EWS” permission group.



24. Click on the “Add permissions” button.



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



Azure Active Directory admin center

Dashboard > MoxiEngage

MoxiEngage | API permissions

Updating permissions
Successfully saved permissions for MoxiEngage.

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

The “Admin consent required” column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

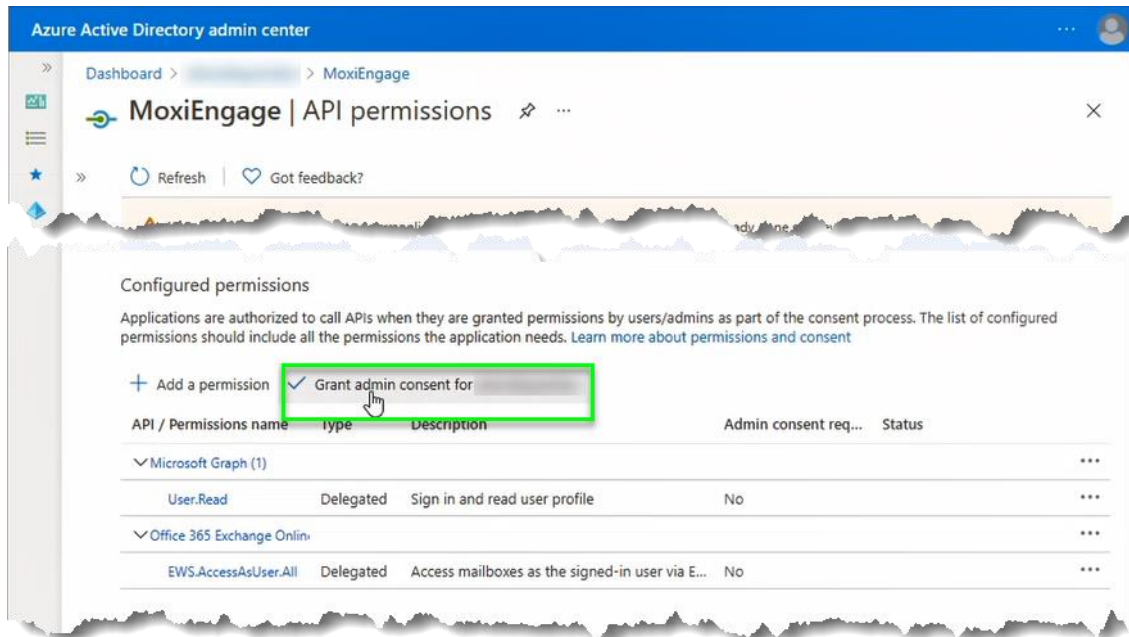
Configured permissions

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

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	...

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



Azure Active Directory admin center

Dashboard > MoxiEngage

MoxiEngage | API 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

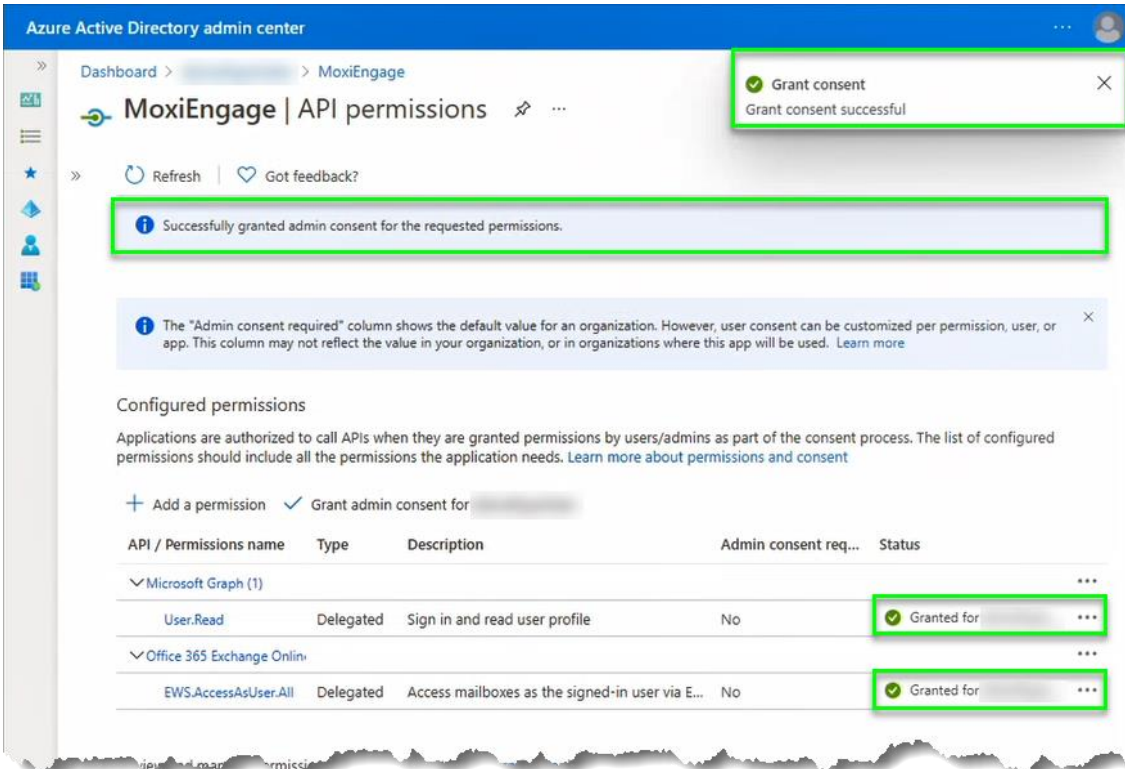
API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...
Office 365 Exchange Online				...
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via E...	No	...

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

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in alienallsparkdev? This will update any existing admin consent records this application already has to match what is listed below.

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



Azure Active Directory admin center

Dashboard > MoxiEngage

MoxiEngage | API permissions

Refresh | Got feedback?

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

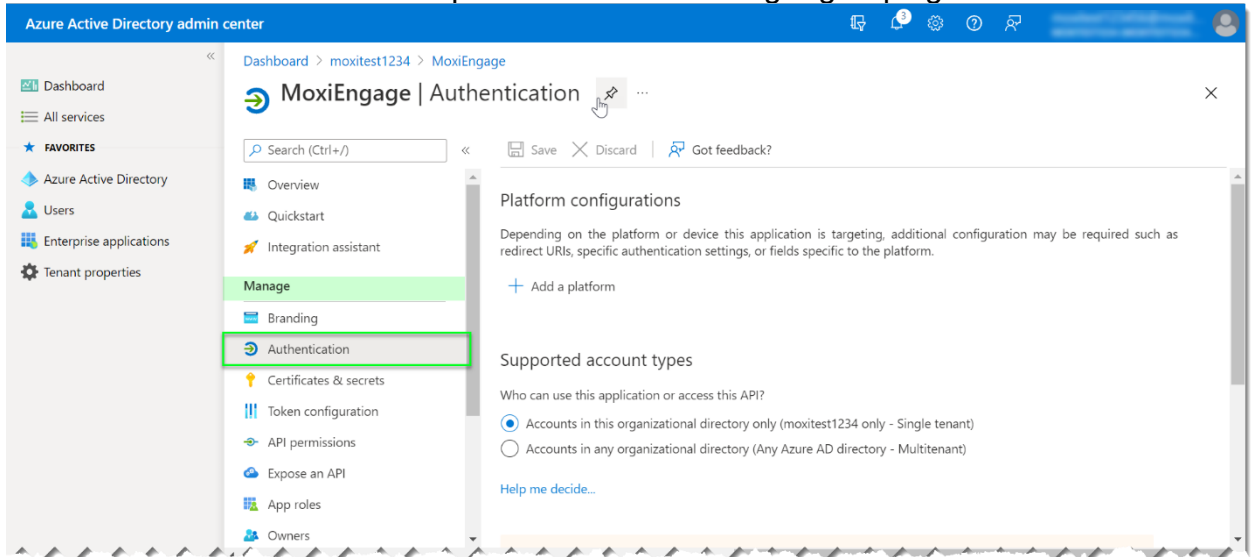
Configured permissions

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](#)

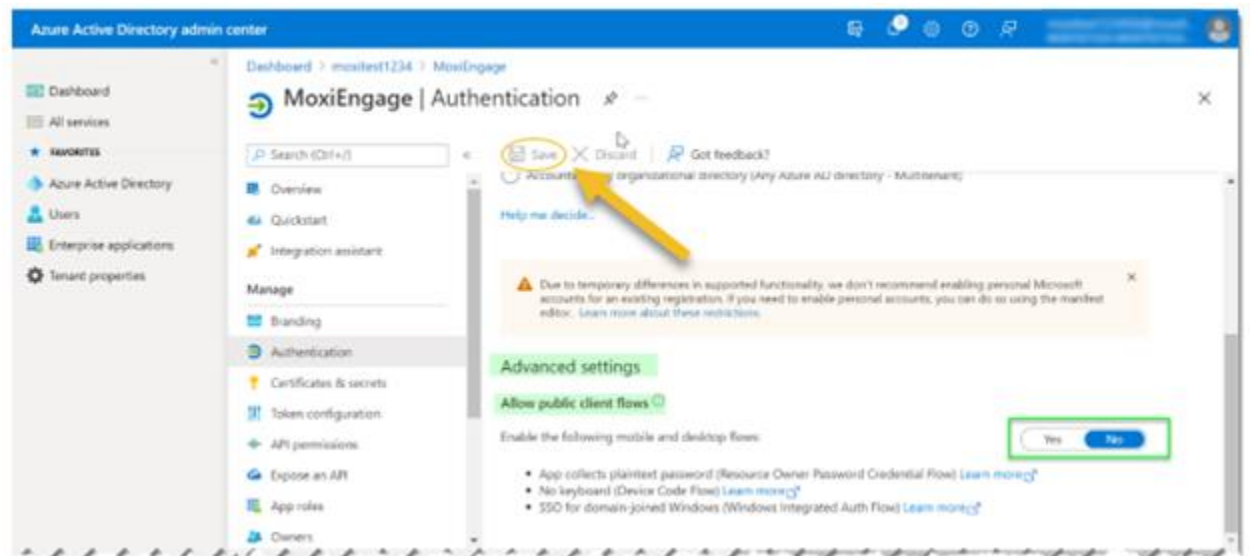
+ Add a permission ✓ Grant admin consent for [redacted]

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

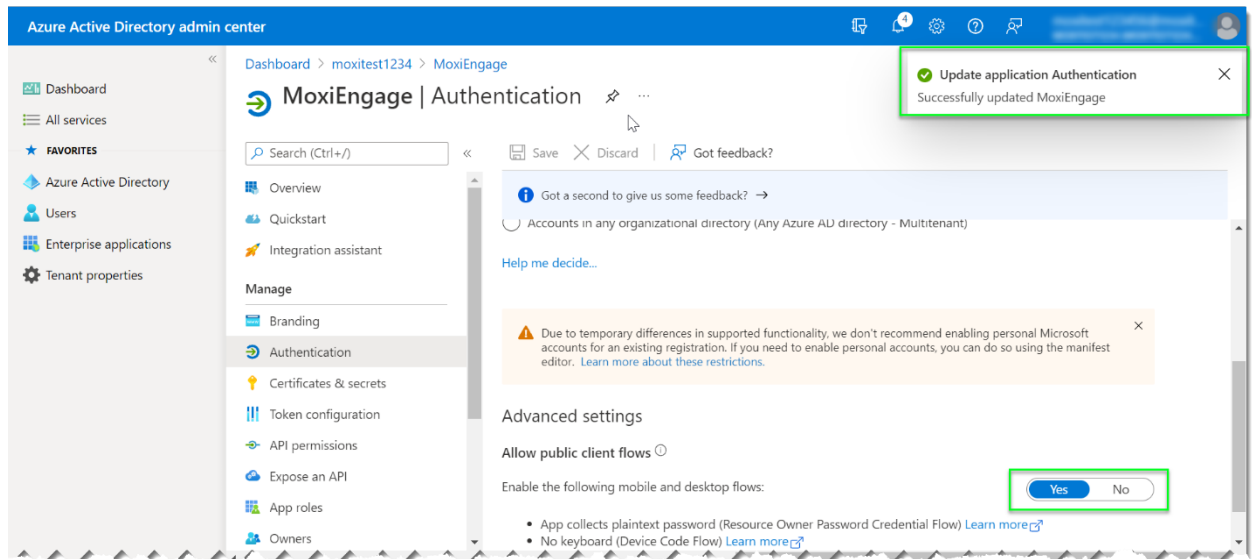
29. Click on the “Authentication” option under the “Manage” grouping of the menu.



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



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



32. Provide to MoxiWorks the values you have saved for the registered application Client ID, your Microsoft 365 Tenant ID, the username and password for the service account you created for MoxiEngage, and a standard (non-administrator) user account that may be used for testing the impersonation setup.



Submit Credentials to MoxiEngage

Jump to this step in the [training video](#).

1. Once the above process is completed please submit your credentials to us through this [Cognito](#) form

Tips and Further Information

- Why is this process necessary for Engage to function for our agents?
 - Engage functions through a sync between itself and an agent's email. Without an email to sync to Engage cannot work.
 - Engage can sync to an office-provided MS365 or Google Workspace account, provided that your office completes the Integration Process.
 - Integration process can only be completed by someone with admin credentials to the office email tenant.
 - Once you've completed the process you must submit those credentials to us here:
<https://www.cognitoforms.com/MoxiWorks2/moxiworksrealogyengagecredentialsform>
 - If you do not have an office provided email or prefer not to do this process for any reason, **your agents will always have the option to sync using a Free Gmail account**. No further action is required by your office in this case.
- Notes about known issues and what to do
 - **3rd Party Provided Email** - Offices with email accounts purchased through third party companies such as Go-Daddy may not be able to complete process due to limitations they place on admin access. Your agents will still be able to sync with Free Gmail.
 - **Access / Permissions** - If you do not have admin privileges to your email tenant you must escalate to someone who does or reach out to your email provider. Moxi cannot assist you with your permissions in your email tenant.
 - **Stuck?** - If you are stuck on a step of the process, compare your screen to the screenshot shown for that step and ensure they look the same. Additionally, each section of the process includes a time stamp and link to a video going through the process step by step.
 - **Failed Submission** – If you have submitted credentials and have subsequently been notified that your submission failed, we recommend redoing the setup process entirely. During this new setup, do not use anything created in the previous attempt, instead create a new service account with a new name, etc. If you use any previously created accounts, permissions, etc you will likely experience the same issue.
 - Most offices that have resubmitted credentials after failing their first submission passed on their 2nd attempt.
 - When redoing the process, it is critical that any field where you name something is filled in differently than your previous attempt. If you reuse names from a previous attempt this will likely cause an issue, even if you have deleted the previously created account / permission. We recommend putting a number at the end of the

name that reflects the attempt # (i.e. MoxiEngage2 & Impersonation2)

- If you continue to have issues we recommend reaching out to your email provider and requesting assistance.

Related Resources

[Google Workspace Support](#)

[Microsoft Office Support](#)

The following resources may provide additional information you need to perform the requisite tasks:

- [Compare Active Directory to Azure Active Directory](#)
- [Azure AD PowerShell Module](#)
- [Connect to Microsoft 365 with PowerShell](#)
- [Set an individual user's password to never expire](#)