MoxiWorks

MoxiEngage Integration Process using Microsoft 365 (Client secret)

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 of the entire process, step-by-step. 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

Test Service Account Impersonation for MoxiEngage

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.

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

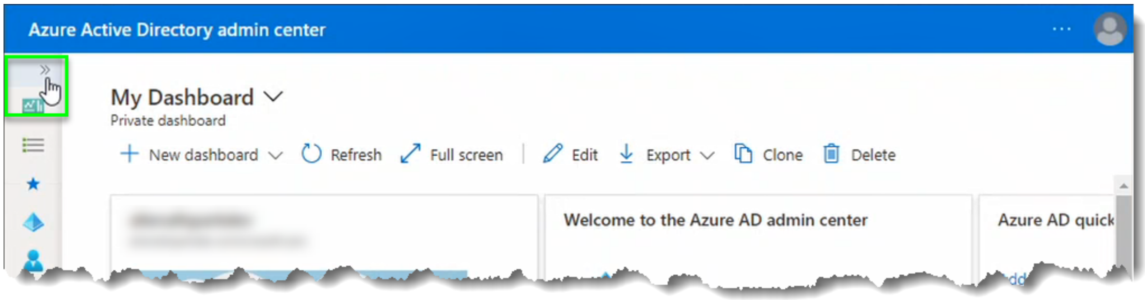
A client application must also be registered and configured with delegation access to the Exchange Web Services (EWS) Managed API to support Modern Authentication.

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.

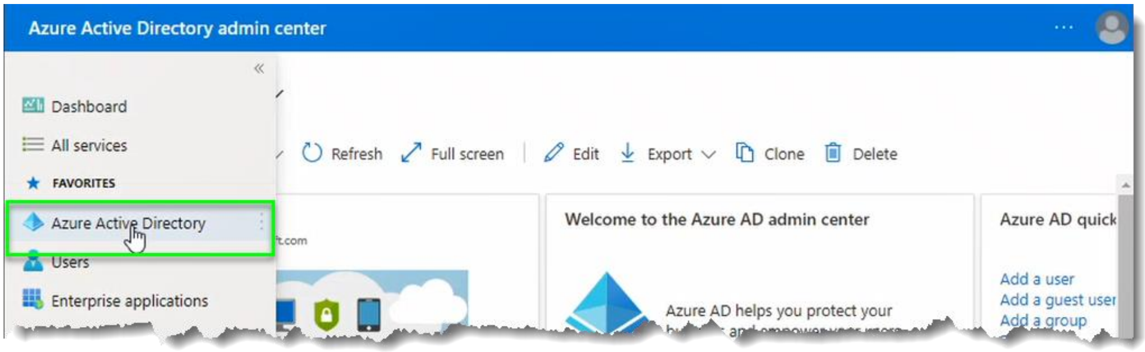
The instructions provided in this guide are not intended to provide security advice for configuring your Microsoft 365 instance. The documented steps represent the most direct approach available at the time of this writing to achieve the necessary access required by MoxiWorks products. Other methods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

Register the MoxiEngage Application as an API Client

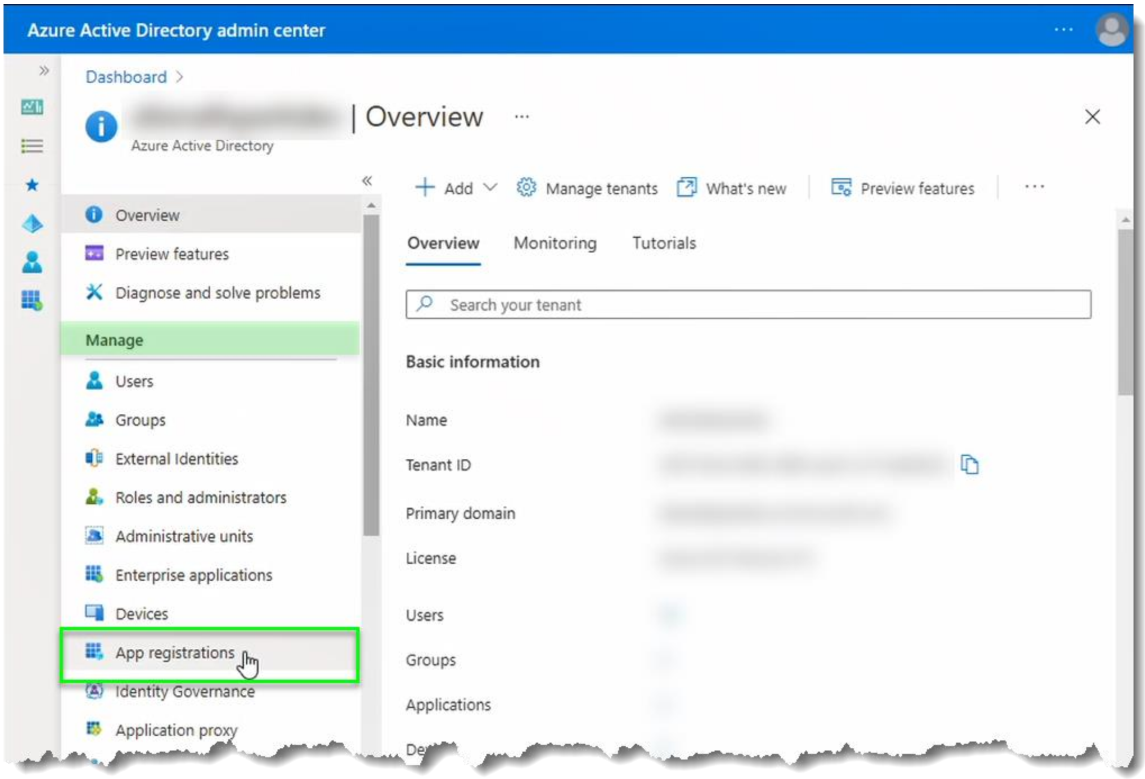
1. Login to your Azure Active Directory Admin Center.
2. Click on the double chevron in the top left corner of the screen to expand the written menu.



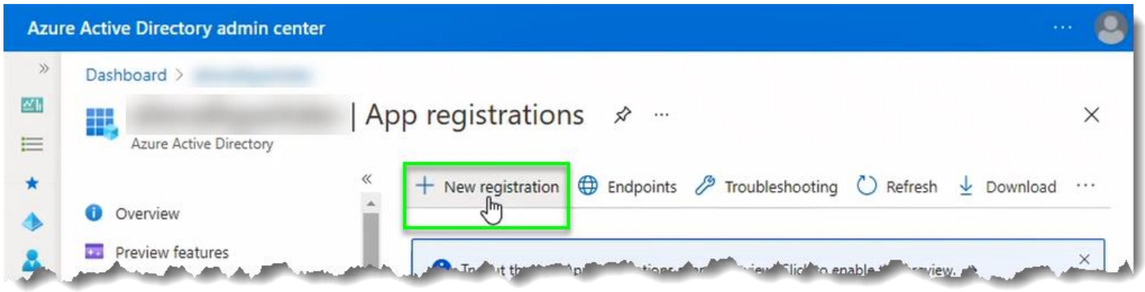
3. Click on the "Azure Active Directory" option in the menu.



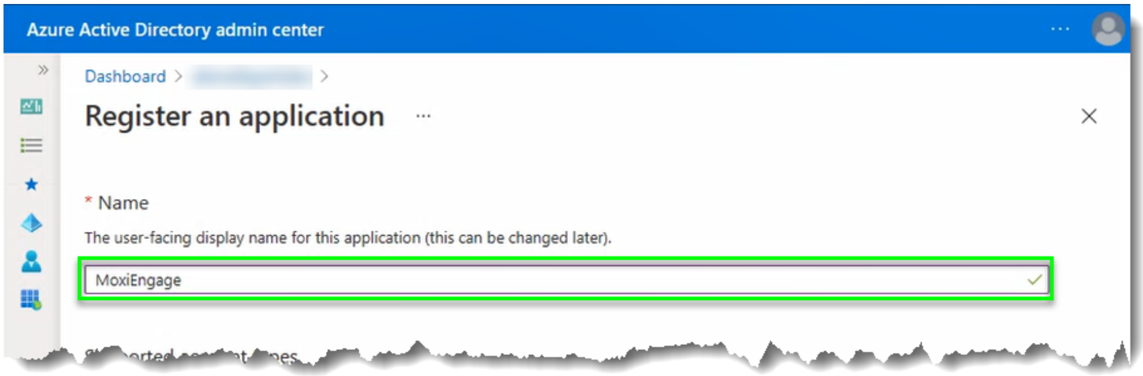
4. From the Azure Active Directory Dashboard for your Microsoft 365 instance, click on the “App Registrations” menu option under the “Manage” grouping.



5. Click on the “New registration” link.



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

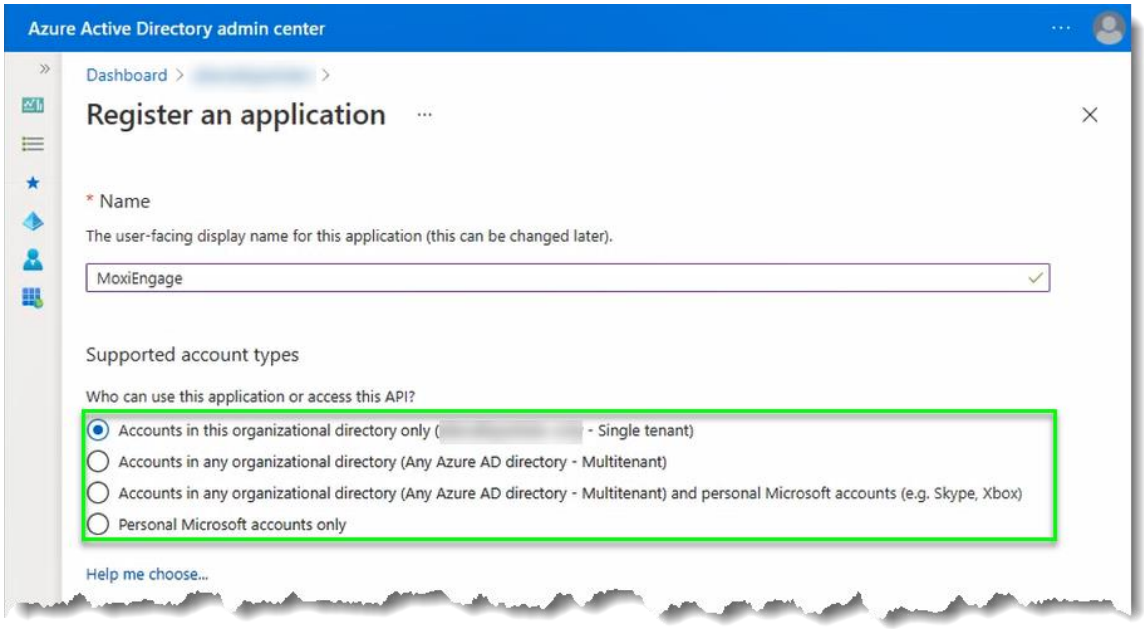


* Name

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

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.



Register an application

* Name

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

MoxiEngage ✓

Supported account types

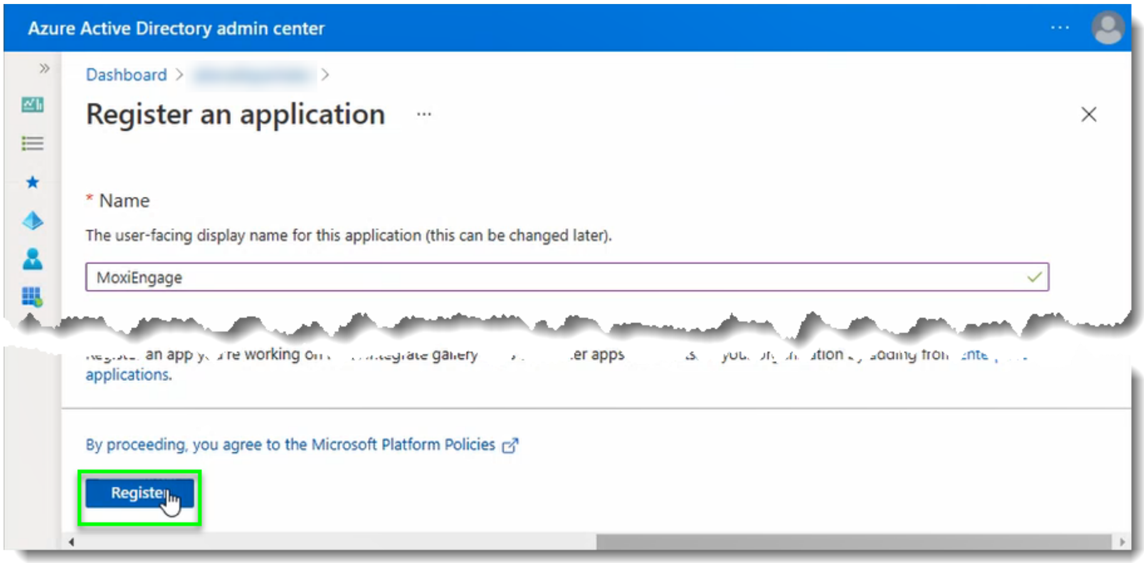
Who can use this application or access this API?

● Accounts in this organizational directory only ([redacted] - 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.



Register an application

* Name

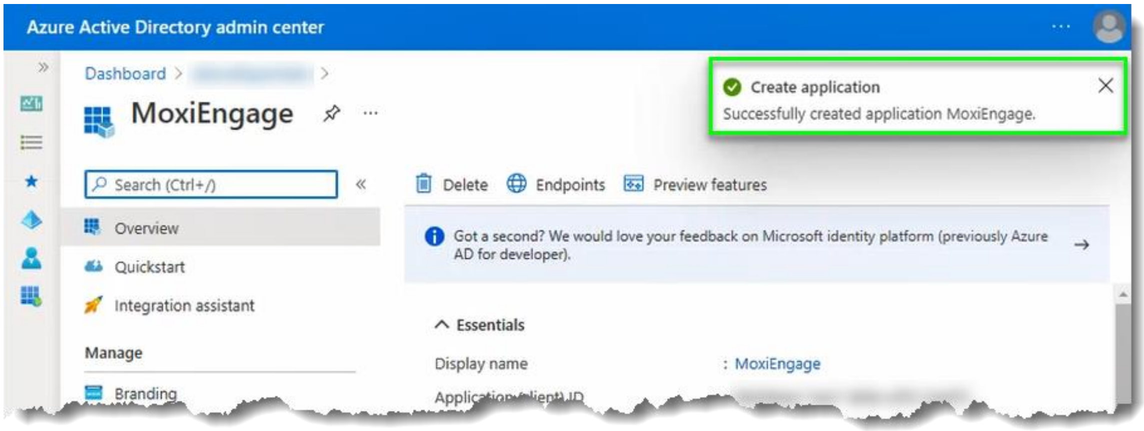
The user-facing display name for this application (this can be changed later).

MoxiEngage ✓

[illegible] an app [illegible] re working on [illegible] gallery [illegible] er apps [illegible] ation [illegible] applications.

By proceeding, you agree to the Microsoft Platform Policies

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

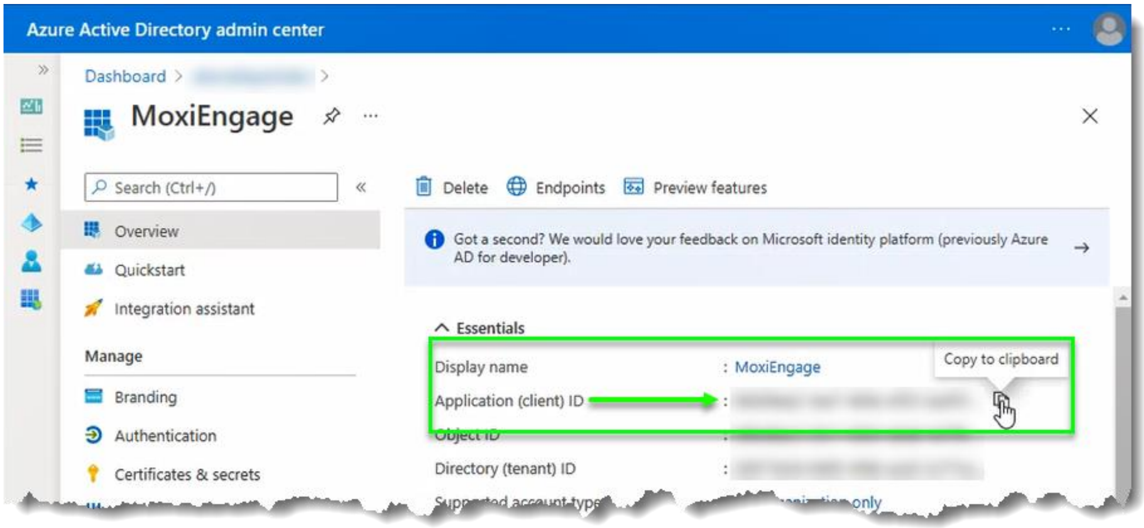


Create application
Successfully created application MoxiEngage.

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

Display name : MoxiEngage

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).

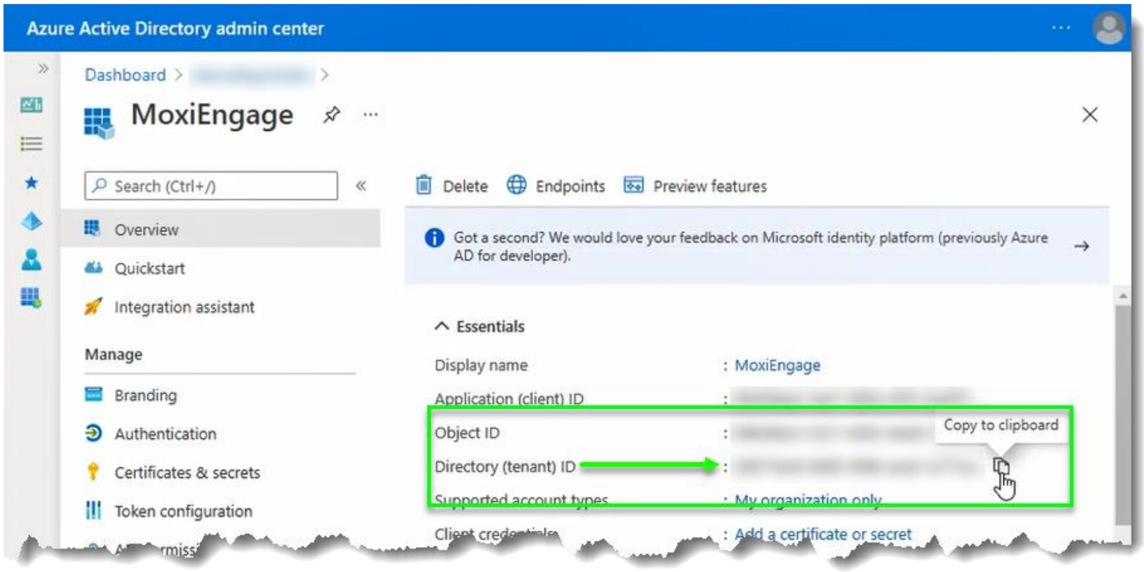


Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

Display name : MoxiEngage
Application (client) ID : [redacted]
Object ID : [redacted]
Directory (tenant) ID : [redacted]

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).



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).

Display name : MoxiEngage

Application (client) ID : [redacted]

Object ID : [redacted]

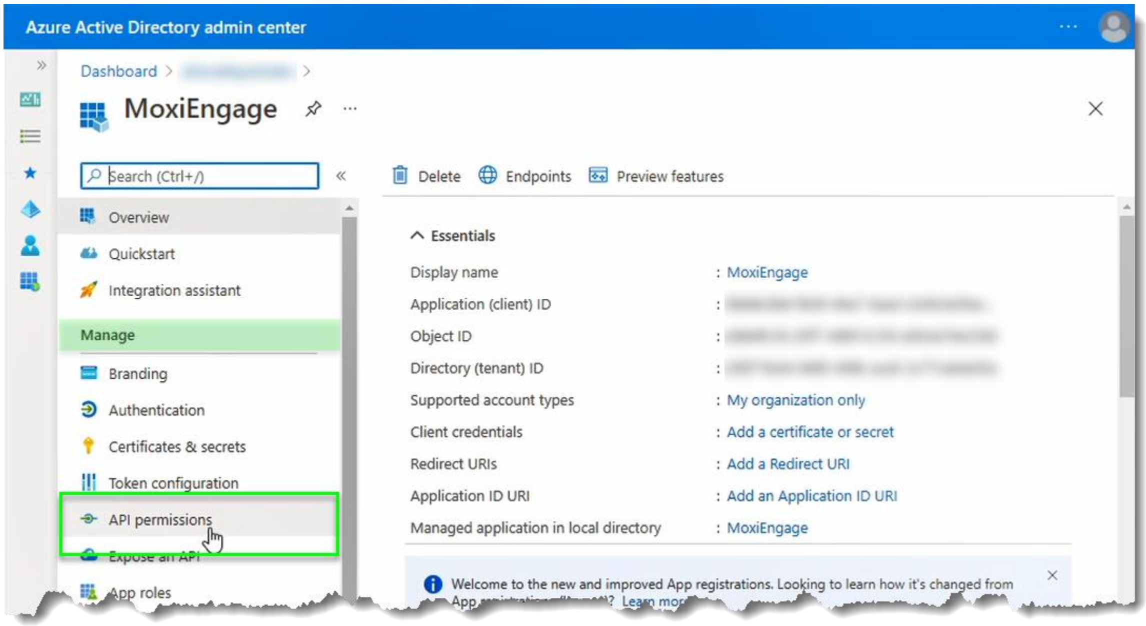
Directory (tenant) ID : [redacted]

Supported account types : My organization only

Client credentials : Add a certificate or secret

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.



Display name : MoxiEngage

Application (client) ID : [redacted]

Object ID : [redacted]

Directory (tenant) ID : [redacted]

Supported account types : My organization only

Client credentials : Add a certificate or secret

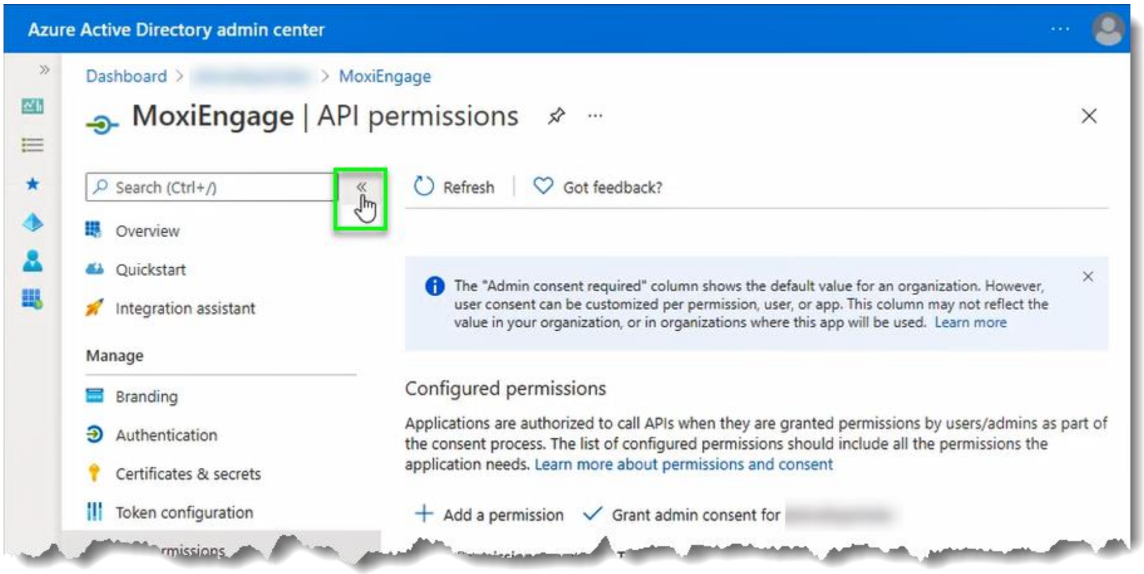
Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

Managed application in local directory : MoxiEngage

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

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



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

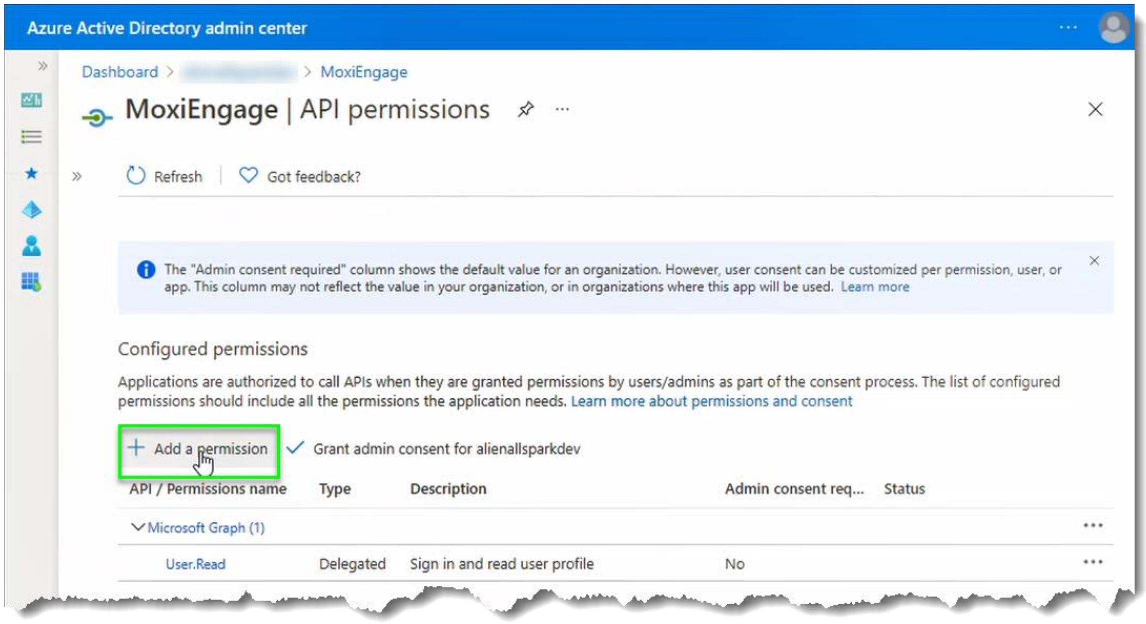
Configured permissions

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

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.


Azure Active Directory admin center
Dashboard > [redacted] > MoxiEngage
MoxiEngage | API permissions
»
Refresh
Got feedback?
Add a permission
Grant admin consent for alienallsparkdev

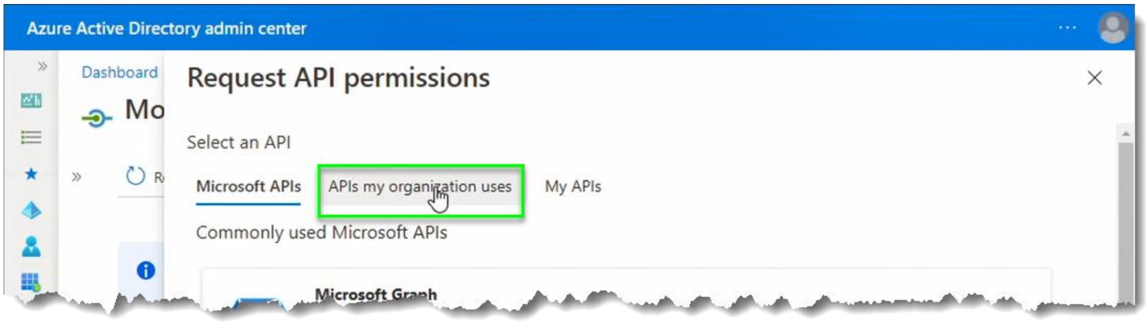
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

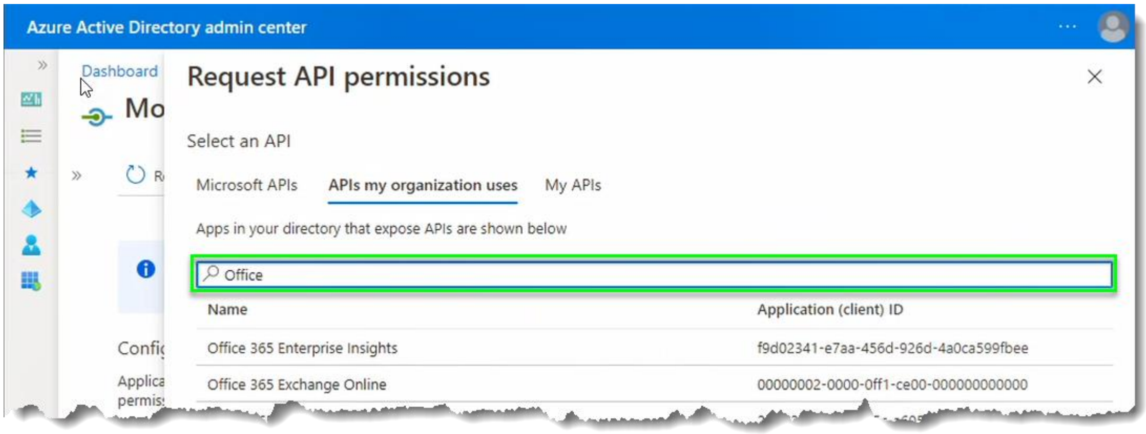
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

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


Azure Active Directory admin center
Dashboard
Mo
Request API permissions
Select an API
Microsoft APIs
APIs my organization uses
My APIs
Commonly used Microsoft APIs
Microsoft Graph

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

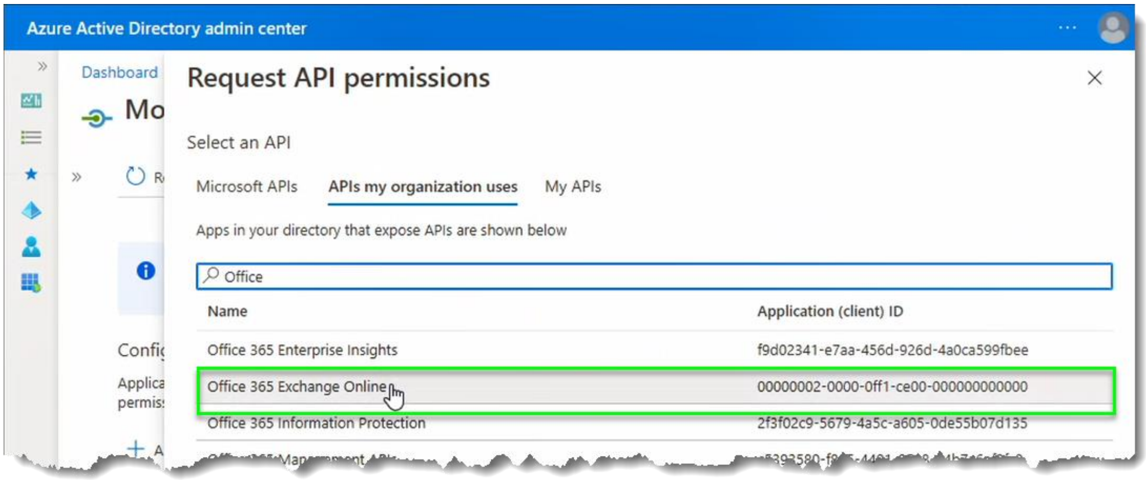


Apps in your directory that expose APIs are shown below

Office

Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000

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

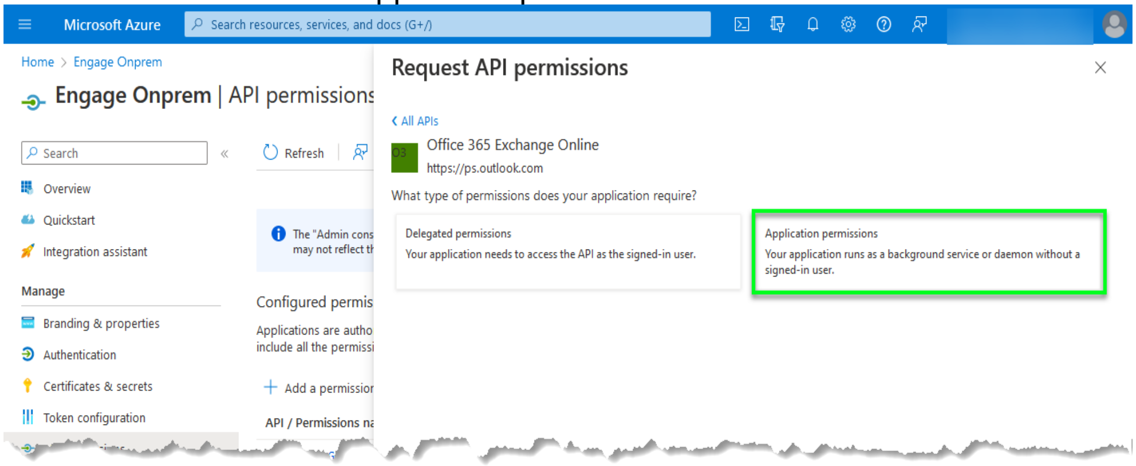


Apps in your directory that expose APIs are shown below

Office

Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135

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



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

The "Admin cons
may not reflect th

Configured permis

Applications are autho
include all the permissi

Add a permission

API / Permissions na

Request API permissions

All APIs

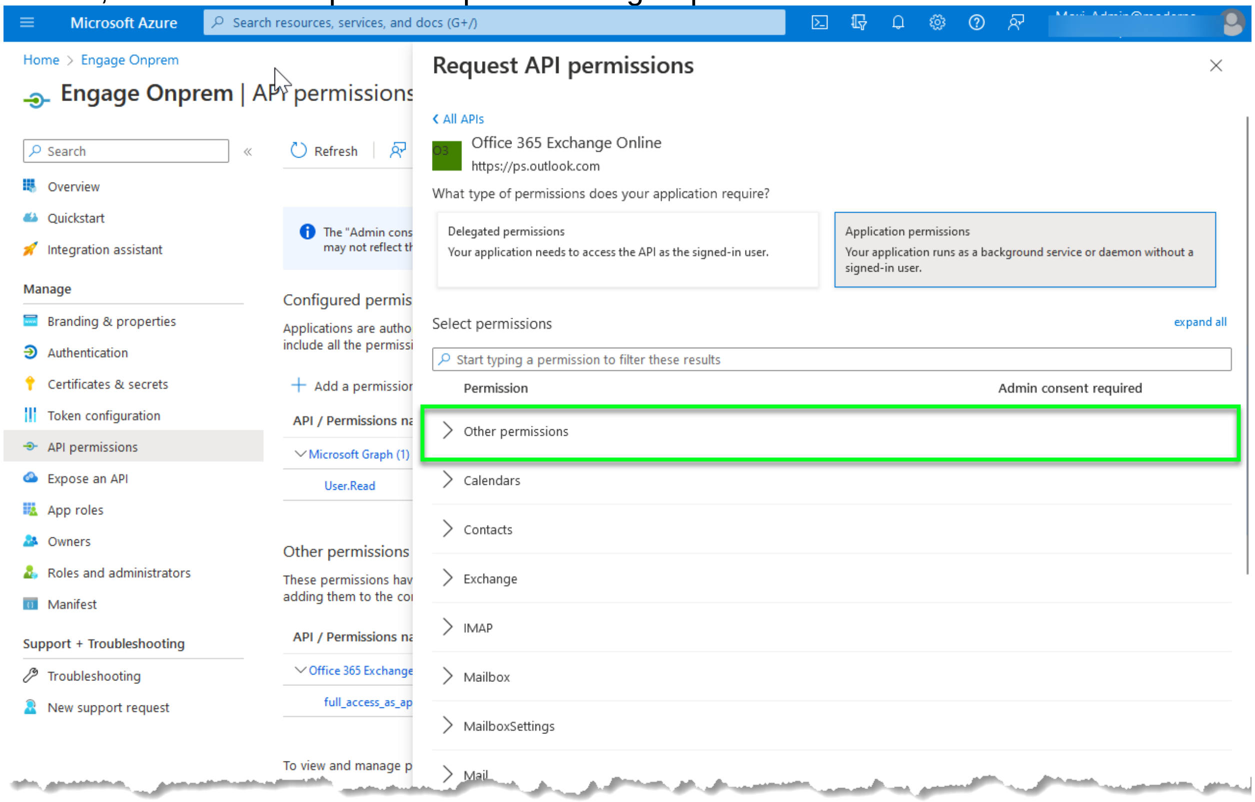
Office 365 Exchange Online
https://ps.outlook.com

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.

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



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 cons
may not reflect th

Configured permis

Applications are autho
include all the permissi

Add a permission

API / Permissions na

Microsoft Graph (1)
User.Read

Other permissions

These permissions hav
adding them to the co

API / Permissions na

Office 365 Exchange
full_access_as_ap

To view and manage p

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.

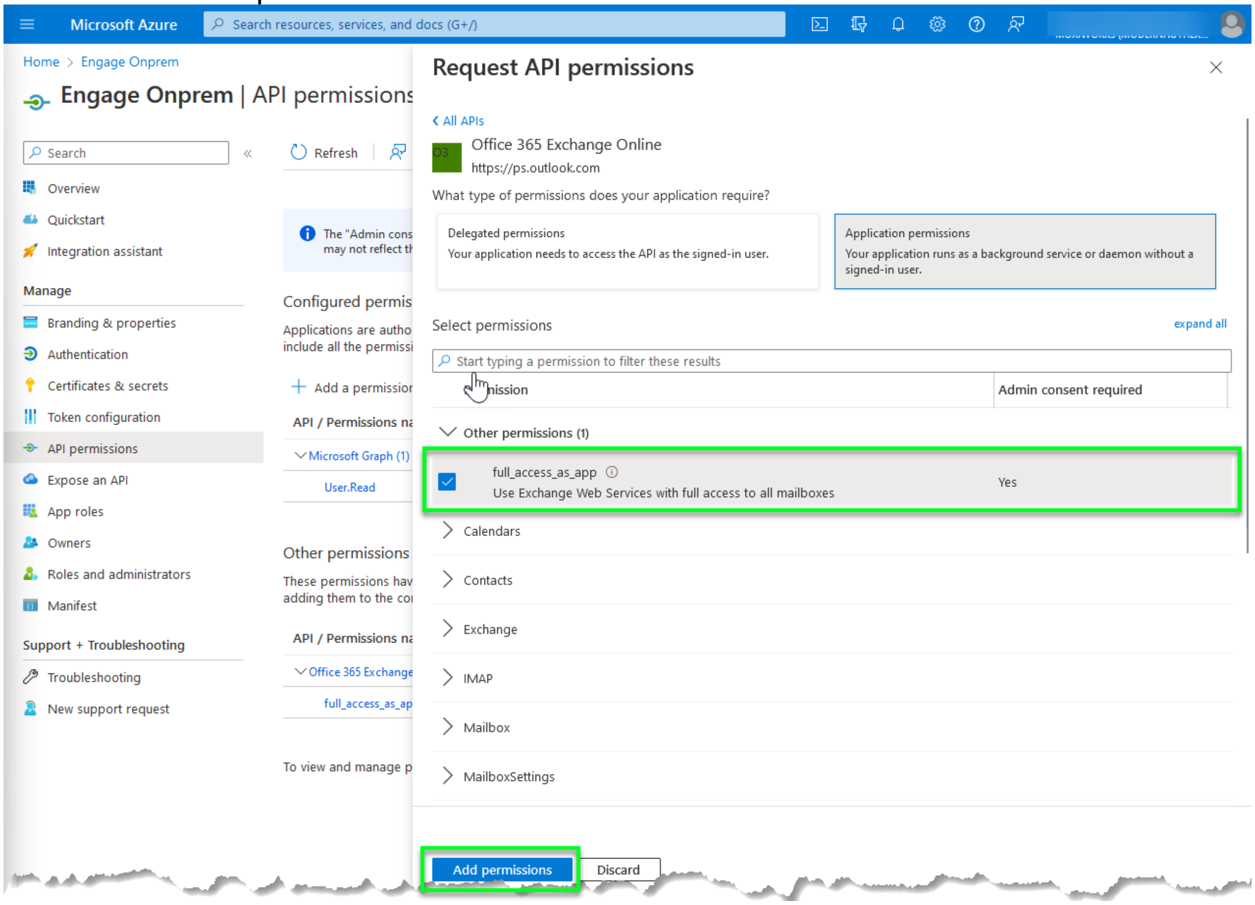
Select permissions | expand all

Start typing a permission to filter these results

Permission	Admin consent required
> Other permissions	
> Calendars	
> Contacts	
> Exchange	
> IMAP	
> Mailbox	
> MailboxSettings	
> Mail	

23. Check the box next to the “full_access_as_app” permission under the “Others” permission group.

24. Click on the “Add permissions” button.



Request API permissions

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.

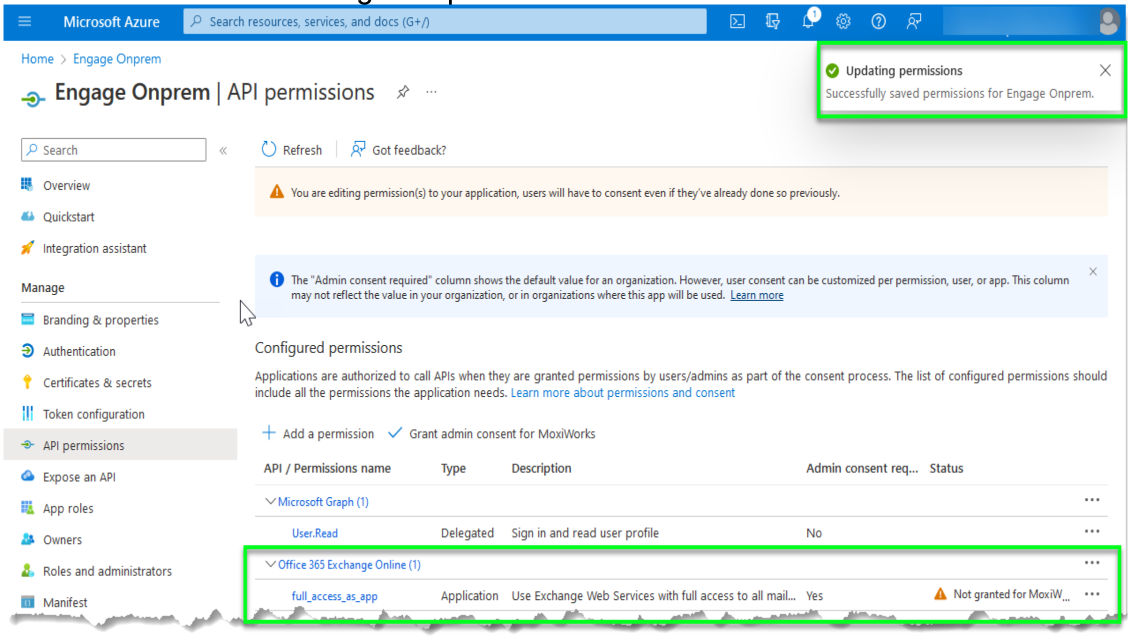
Application permissions
Your application runs as a background service or daemon without a signed-in user.

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	

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



Engage Onprem | API permissions

Updating permissions
Successfully saved permissions for Engage Onprem.

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

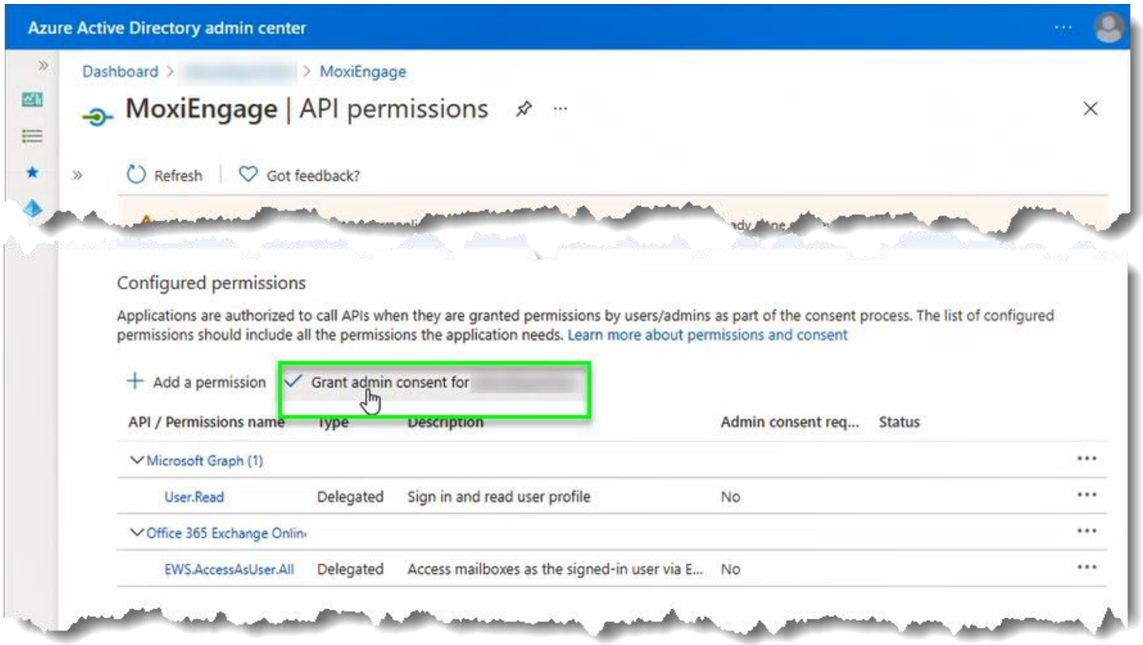
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

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

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.



Azure Active Directory admin center
Dashboard > [redacted] > MoxiEngage

MoxiEngage | API permissions

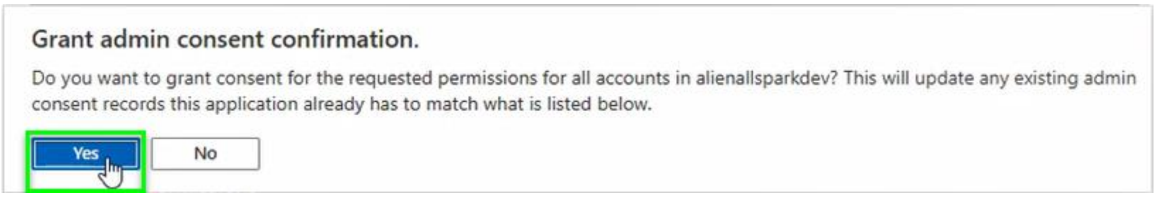
Configured permissions

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 [redacted]

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 Onlin				
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via E...	No	

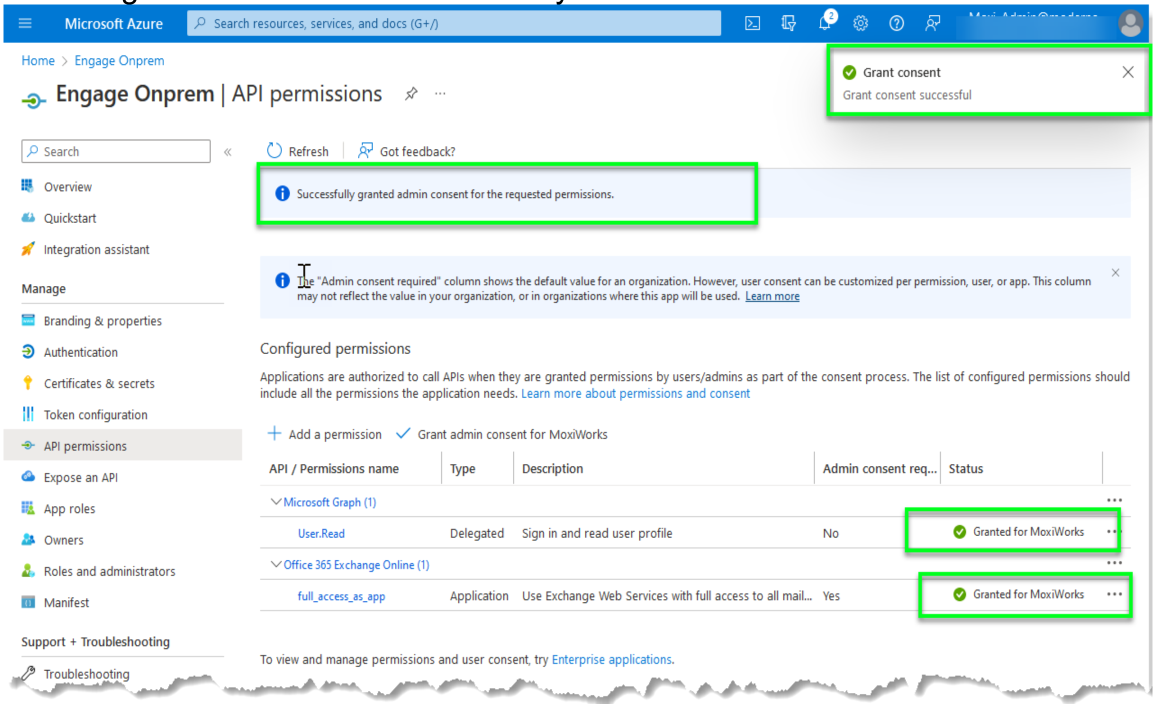
27. Click on the “Yes” button to confirm.



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.



Grant consent

Grant consent successful

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

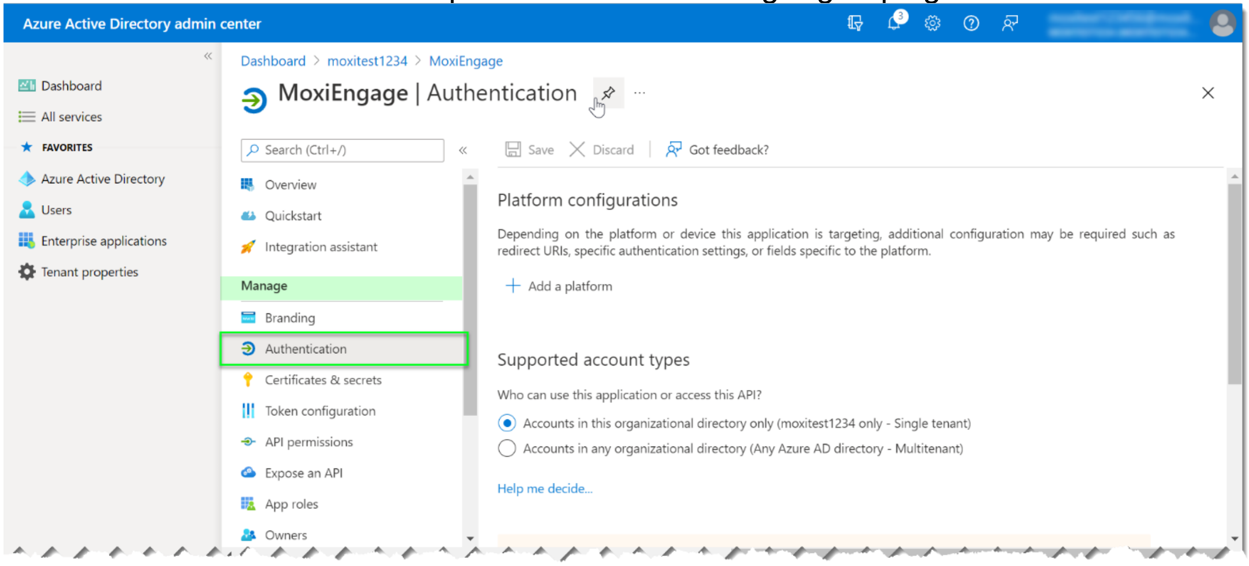
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for MoxiWorks

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for MoxiWorks
Office 365 Exchange Online (1)				
full_access_as_app	Application	Use Exchange Web Services with full access to all mail...	Yes	✓ Granted for MoxiWorks

To view and manage permissions and user consent, try Enterprise applications.

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



Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

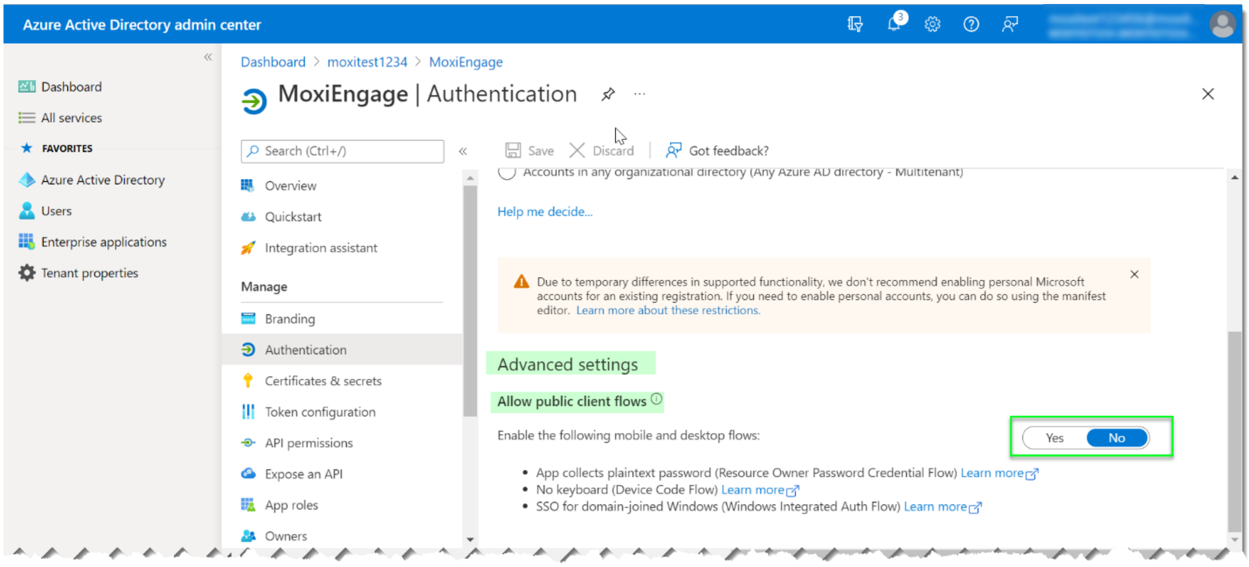
Who can use this application or access this API?

● Accounts in this organizational directory only (moxitest1234 only - Single tenant)

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

Help me decide...

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



MoxiEngage | Authentication

○ 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.

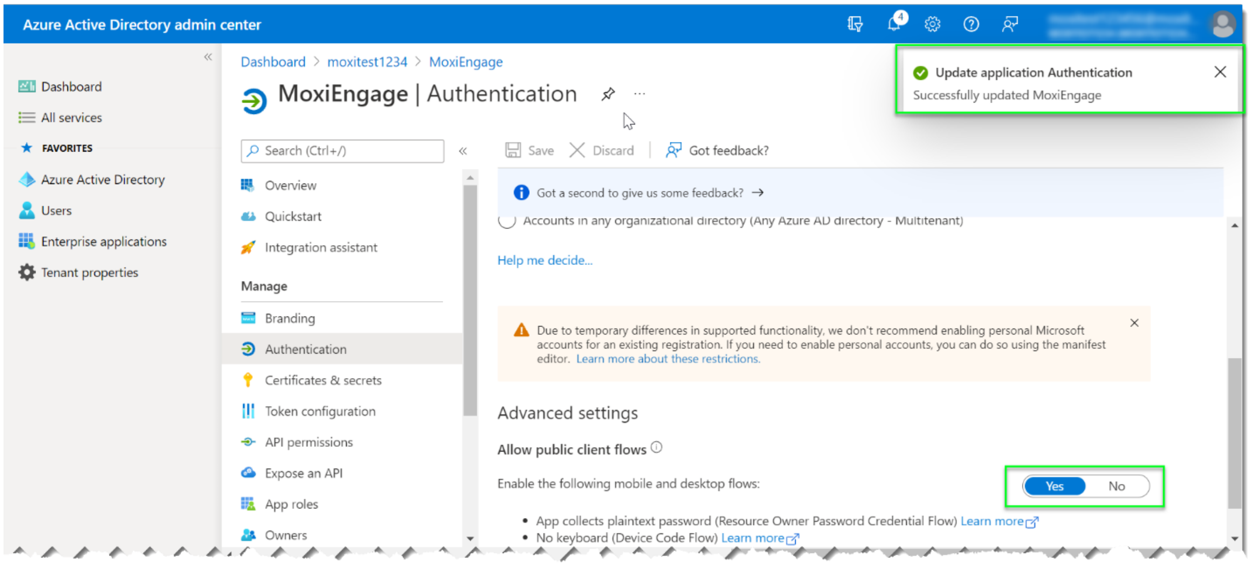
Advanced settings

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

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



MoxiEngage | Authentication

Update application Authentication
Successfully updated MoxiEngage

Got a second to give us some 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.

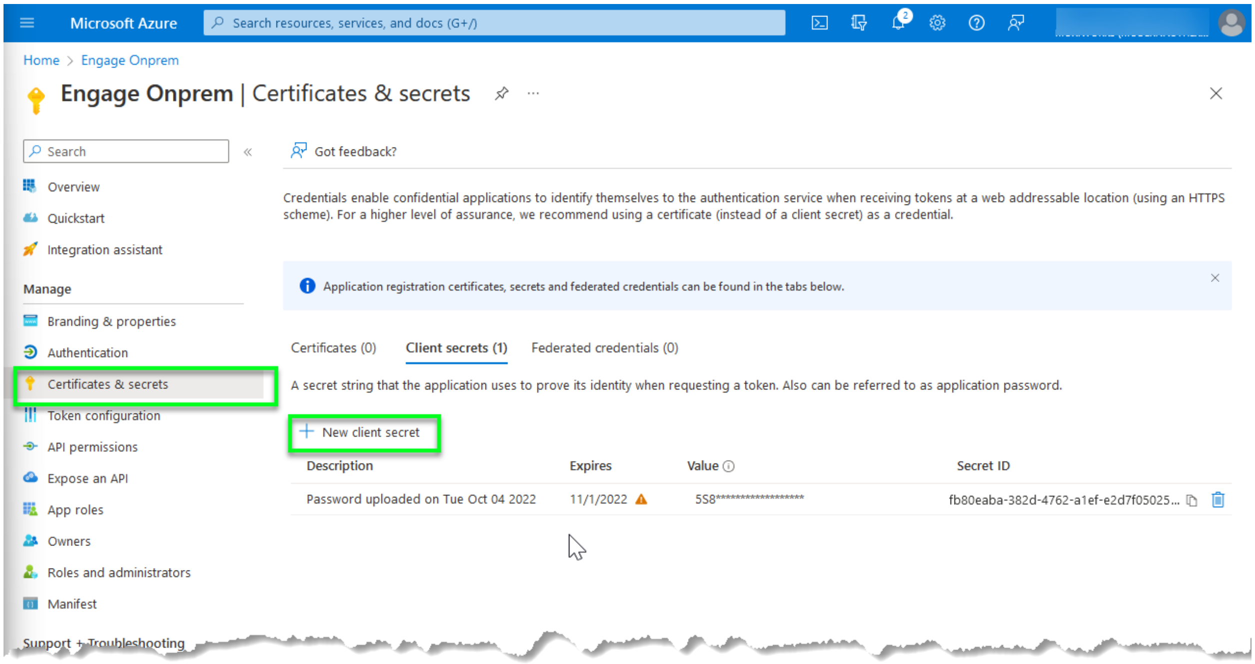
Advanced settings

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

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



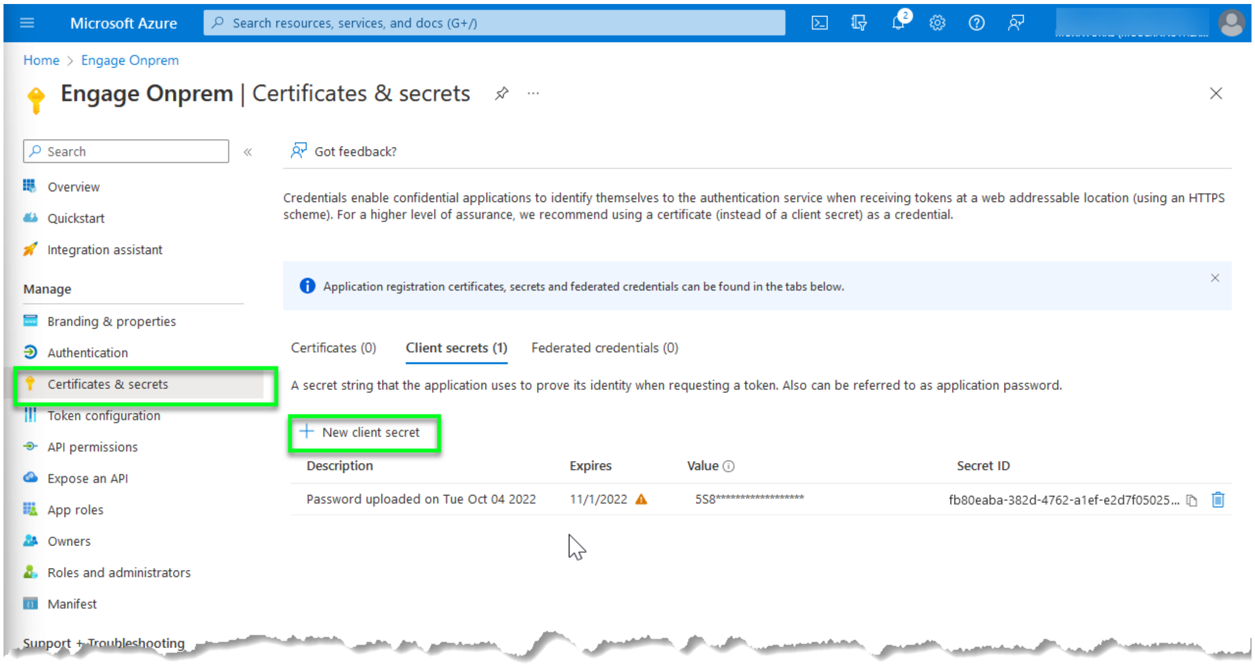
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Password uploaded on Tue Oct 04 2022	11/1/2022 ⚠	5S8******************	fb80eaba-382d-4762-a1ef-e2d7f05025...

33. Click “New client secret”.



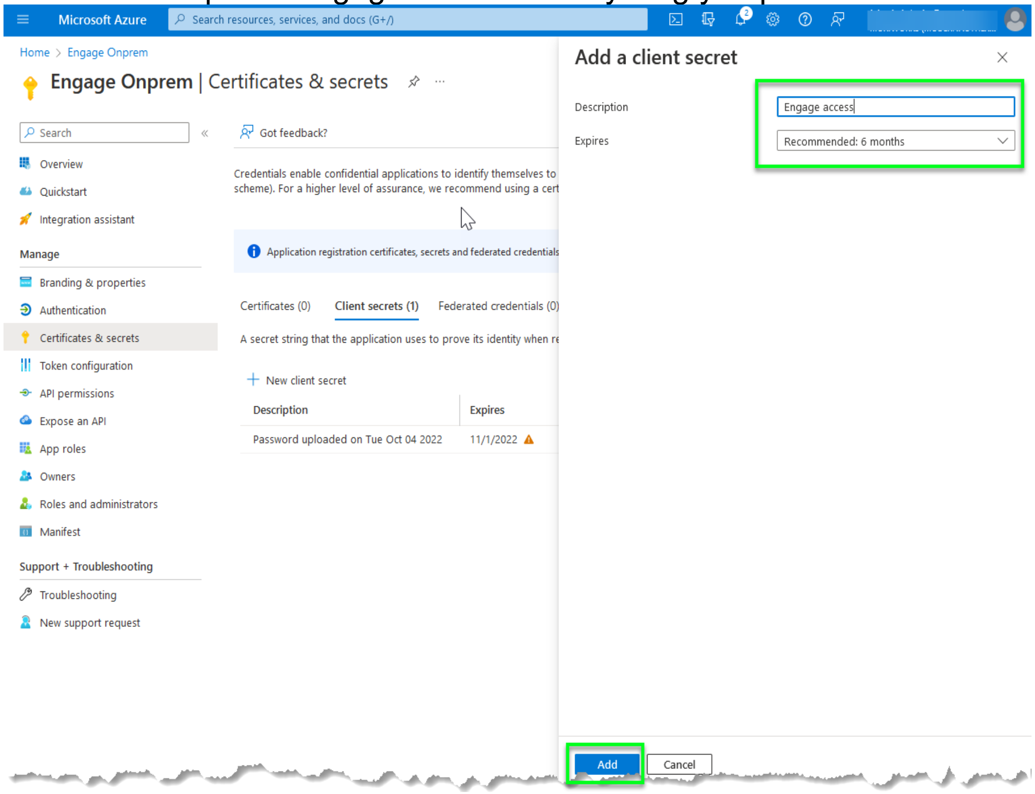
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Password uploaded on Tue Oct 04 2022	11/1/2022 ⚠	5S8******************	fb80eaba-382d-4762-a1ef-e2d7f05025...

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



Credentials enable confidential applications to identify themselves to
scheme). For a higher level of assurance, we recommend using a cert

Application registration certificates, secrets and federated credentials

A secret string that the application uses to prove its identity when re

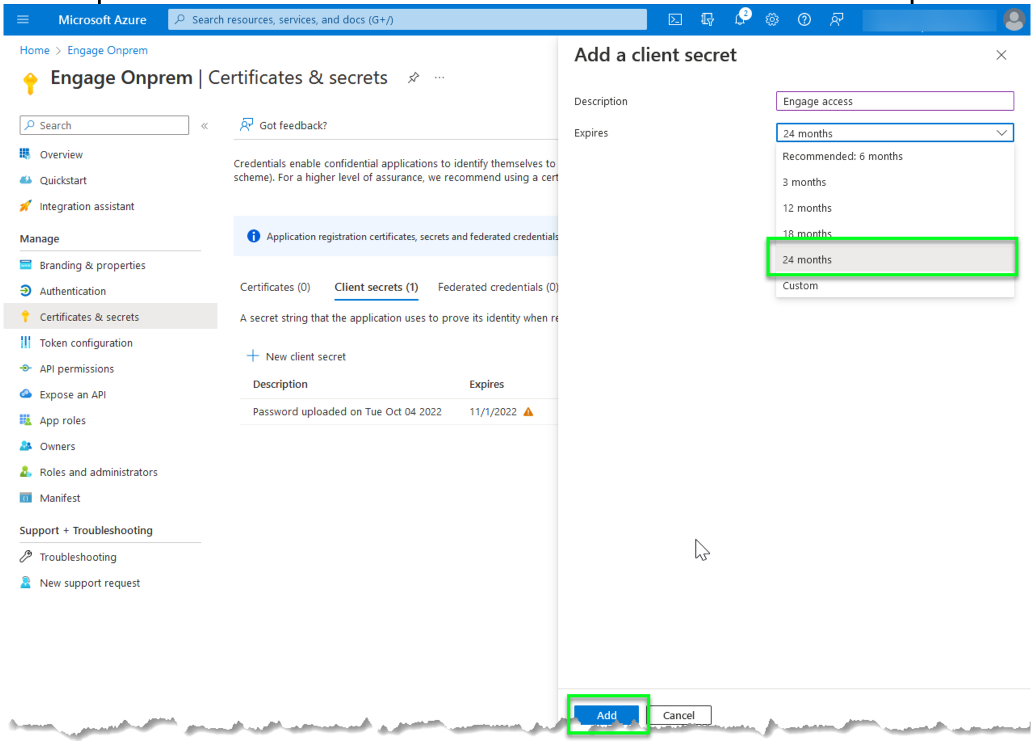
Description	Expires
Password uploaded on Tue Oct 04 2022	11/1/2022 ⚠

Add a client secret

Description: Engage access

Expires: Recommended: 6 months

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.



Credentials enable confidential applications to identify themselves to
scheme). For a higher level of assurance, we recommend using a cert

Application registration certificates, secrets and federated credentials

A secret string that the application uses to prove its identity when re

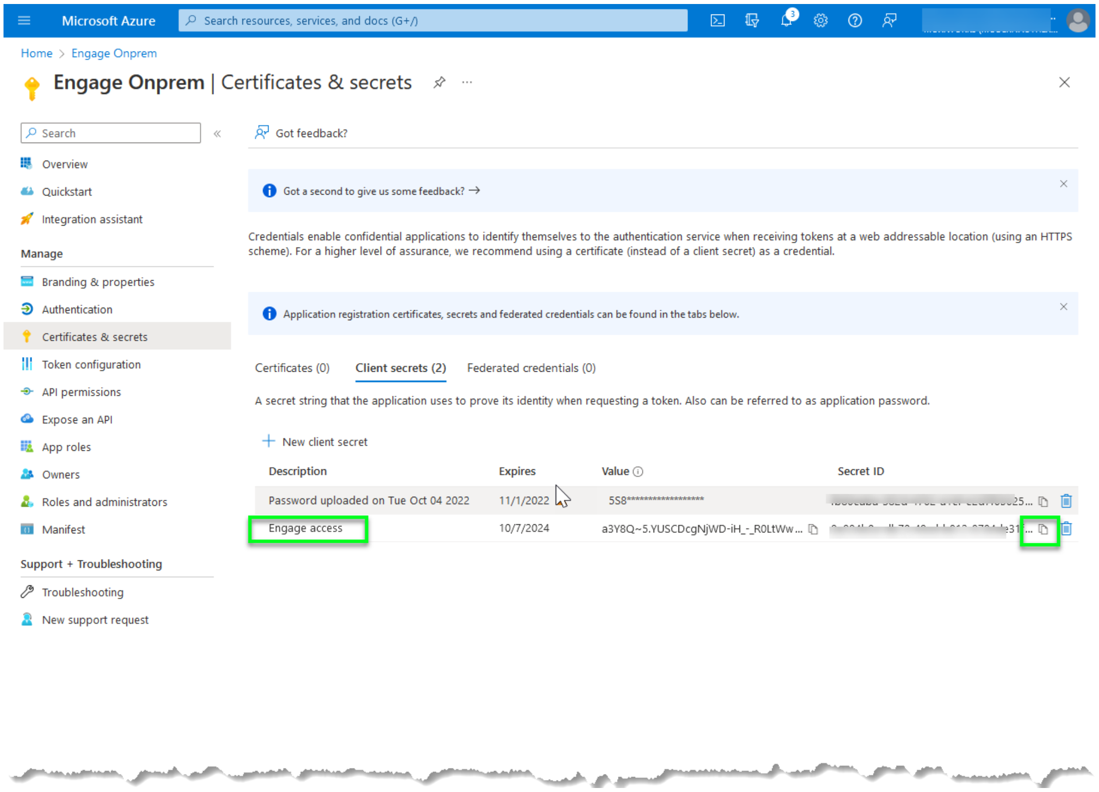
Description	Expires
Password uploaded on Tue Oct 04 2022	11/1/2022 ⚠

Add a client secret

Description: Engage access

Expires: 24 months

36. Find the secret you just created in the list. Click icon to copy the secret into a location to be submitted later.



Engage Onprem | Certificates & secrets

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Password uploaded on Tue Oct 04 2022	11/1/2022	5S8******************	[redacted]
Engage access	10/7/2024	a3Y8Q~5.YUSCDcgNjWD-iH_-_R0LtWw...	[redacted]

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.**

Submit Credentials to MoxiEngage

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 that 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