

# HOWTO: Setup Azure AD to work with World of Workflows

---

## Introduction

This document describes how to setup Azure AD to work with World of Workflows. World of Workflows includes a **Credential Manager** which allows you to store and process credentials for external applications. However to connect to Azure AD you need to setup a **Registered Application** and connect the credential. This simple guide shows you how to perform that.

## Prerequisites

- Application Read/Write/Create Permissions in your Azure AD

## Output Table

Complete this table as you move through the steps

Item	Value	Description
Client Secret		This is a secret value that identifies this application
Authorization URL		This is the URL Workflows will use to access Azure AD
Access Token URL		This is the Access Token URL Workflows will use to access Azure AD
Client ID		This is the Client ID Workflows will use to access Azure AD
Scope	offline_access Mail.ReadWrite Mail.Send	This is the Scope Workflows will use to access Azure AD

## Steps to configure Azure AD

1. Connect to [Microsoft Azure Portal](#) and navigate to Azure AD. Alternatively click [here](#)

Welcome to Azure!

Don't have a subscription? Check out the following options.



Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular [free services](#).

[Start](#)



Manage Azure Active Directory

Azure Active Directory is becoming Microsoft Entra ID. Secure access for everyone.

[View](#) [Learn more](#)



Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

[Explore](#) [Learn more](#)

Azure services

[Create a resource](#)

[Azure Active Directory](#)

[Quickstart Center](#)

[Virtual machines](#)

[App Services](#)

[Storage accounts](#)

[SQL databases](#)

[Azure Cosmos DB](#)

[Kubernetes services](#)

[More services](#)

[Home](#) >

[Contoso | Overview](#) ...

Azure Active Directory

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Delegated admin partners

Enterprise applications

Devices

App registrations

Identity Governance

+ Add

Manage tenants

What's new

Preview features

Got feedback?

Azure Active Directory is becoming Microsoft Entra ID. [Learn more](#)

Overview

Monitoring

Properties

Recommendations

Tutorials

Search your tenant

Basic information

Name	Contoso	Users	35
Tenant ID	c341abae-73dc-4a02-b018-3b9d18d51714	Groups	43
Primary domain	M365x55194390.onmicrosoft.com	Applications	9
License	Azure AD Premium P2	Devices	0
Workload License	Azure AD Workload Free		

Alerts

## 2. Click **App registrations** on the left menu or click [here](#).

+ New registration   Endpoints   Troubleshooting   Refresh   Download   Preview features   Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications   **Owned applications**   Deleted applications

Start typing a display name or application (client) ID to filter these r...   Add filters

4 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
World of Workflows Client	694bbd7b-9293-4873-90ef-64c88bf05d76	6/20/2023	-
World of Workflows Server	ead83cdf-8348-4a7a-8587-3cabcaa1da29	6/20/2023	Current
WOWF Client	8042c499-b1db-4bc3-a510-3cafabcc71dc	7/6/2023	-
WOWF Server	72db5bf5-5654-44a7-9bf7-1e9aa5a0561a	7/6/2023	Current

## 3. Click **New registration**

4. Type the name of this application. It's important to make this something you can understand later. In this example, we're going to call it **World of Workflows HOWTO**. Ensure **Accounts in this organizational directory only** is checked and click **Register**.

[Home](#) > [Contoso | App registrations](#) >

## Register an application

### \* Name

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

World of Workflows HOWTO

### Supported account types

Who can use this application or access this API?

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

[Help me choose...](#)

### Redirect URI (optional)

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

Select a platform

e.g. <https://example.com/auth>

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

Register

5. Click on **Endpoints**

## Endpoints



OAuth 2.0 authorization endpoint (v2)

<https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/oauth2/v2.0/authorize>

OAuth 2.0 token endpoint (v2)

<https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/oauth2/v2.0/token>

OAuth 2.0 authorization endpoint (v1)

<https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/oauth2/authorize>

OAuth 2.0 token endpoint (v1)

<https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/oauth2/token>

OpenID Connect metadata document

<https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/v2.0/.well-known/openid-configuration>

Microsoft Graph API endpoint

<https://graph.microsoft.com>

Federation metadata document

<https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/federationmetadata/2007-06/federationmetadata.xml>

WS-Federation sign-on endpoint

<https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/wsfed>

SAML-P sign-on endpoint

<https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/saml2>

SAML-P sign-out endpoint

6. Copy the OAuth 2.0 authorization endpoint (v2) into the **Authorization URL** field in the table above7. Copy the OAuth 2.0 token endpoint (v2) into the **Access Token URL** field in the table above

8. Close Endpoints

Delete Endpoints Preview features

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

### ^ Essentials

Display name : [World of Workflows HOWTO](#)Client credentials : [Add a certificate or secret](#)

Application (client) ID : b7dbbd17-2af9-4f4b-94bc-76d8408ed993

Redirect URIs : [Add a Redirect URI](#)

Object ID : d020bb94-379c-4326-88e8-c3673c780f47

Application ID URI : [Add an Application ID URI](#)

Directory (tenant) ID : c341abae-73dc-4a02-b018-3b9d18d51714

Managed application in I... : [World of Workflows HOWTO](#)Supported account types : [My organization only](#) Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#) Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

9. Copy the Application (client) ID into the table above under Client ID

10. Choose **Certificates and secrets** from the menu on the left

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

Certificates (0)

**Client secrets (0)**

Federated credentials (0)

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

+ New client secret

Description	Expires	Value ⓘ	Secret ID
No client secrets have been created for this application.			

11. Click **+ New client secret**

Add a client secret

Description

World of Workflows HOWTO

Expires

Recommended: 180 days (6 months) ▾

12. Now give the secret a description and an expiry date. In this example, we're going to call it **World of Workflows HOWTO** and set the expiry to **180 days**. Click **Add**

Got feedback?

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.

Certificates (0)

**Client secrets (1)**

Federated credentials (0)

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


+ New client secret

Description	Expires	Value ⓘ	Secret ID
World of Workflows HOWTO	1/9/2024	5Ty8Q~drFpTBVh4kWQGItTn5PMb6yKxS5...	d37d00a7-25dd-468c-8c8a-cfa1c1f92380

13. **IMPORTANT** Copy the value of the secret in the table above. You will need this later and this is the last time it will appear in the portal. If you lose this value, you will need to create a new secret.


5 / 12


14. Click **API Permissions** on the left pane




 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 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 Contoso


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


To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).





15. Click **Grant Admin Consent** and click **Yes**

### 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 Contoso

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

16. Click **Authentication** on the left pane

### 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 (Contoso only - Single tenant)

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

[Help me decide...](#)

17. Click **Add a Platform**

## Configure platforms



### Web applications



#### Web

Build, host, and deploy a web server application. .NET, Java, Python



#### Single-page application

Configure browser client applications and progressive web applications. Javascript.

### Mobile and desktop applications



#### iOS / macOS

Objective-C, Swift, Xamarin



#### Android

Java, Kotlin, Xamarin



#### Mobile and desktop applications

Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

18. Click **Web**

19. Enter the redirect URI <https://localhost:7063/v1/oauth2/callback> for Personal Edition, for Business Edition, the address will be <https://<WOWServer>/v1/oauth2/callback>

# Configure Web

[← All platforms](#)[Quickstart](#)[Docs](#)

## \* Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs.

[Learn more about Redirect URIs and their restrictions](#)

`https://localhost:7063/v1/oauth2/callback` ✓

## Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. `https://example.com/logout`

## Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

- ☒ Access tokens (used for implicit flows)
- ☒ ID tokens (used for implicit and hybrid flows)

**Configure**

Cancel

20. Check Access Tokens and ID Tokens and click **Configure**

Finally you need to choose scopes. These will determine what actions World of Workflows will perform with Office 365 and Azure AD.

There are hundreds of scopes available [here](#) however here are some common ones:

- **offline\_access** - always add this scope to ensure that the system keeps a persistent connection with Azure AD and you don't need to continually reauthenticate.
- **Mail.ReadWrite** - Allows the app to create, read, update, and delete email in user mailboxes. Does not include permission to send mail.

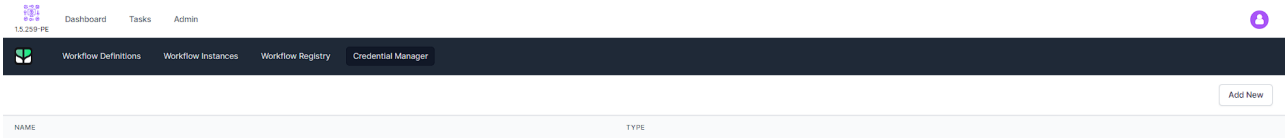


- **Mail.ReadWrite.Shared** - Allows the app to create, read, update, and delete mail that the user has permission to access, including the user's own and shared mail. Does not include permission to send mail.
- **Mail.Send** - Allows the app to send mail as users in the organization.

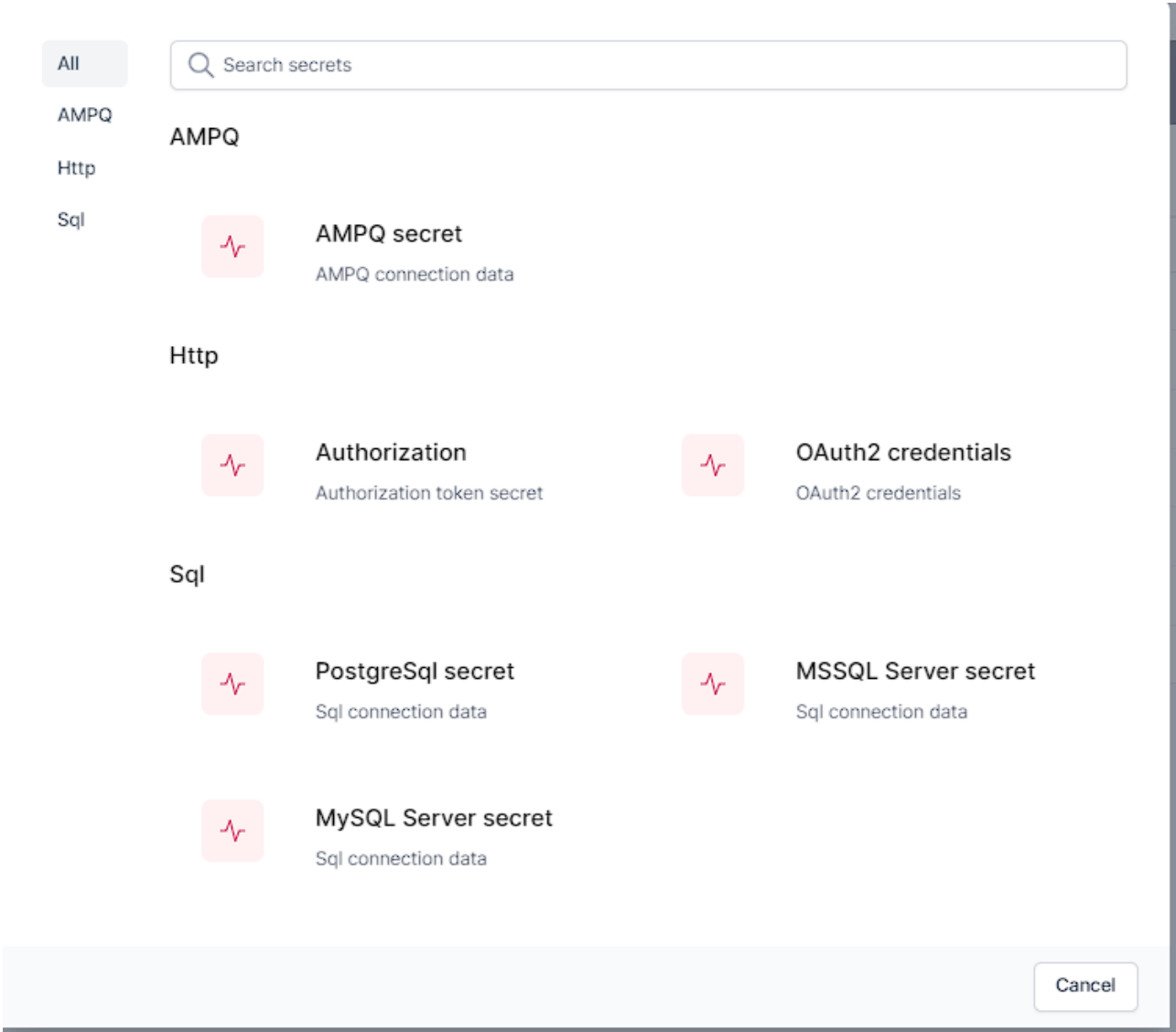
Record the ones you need in the table above.

## Configure a credential in World of Workflows

1. Navigate to World of Workflows
2. Click **Admin -> Workflows**
3. Click **Credential Manager**



4. Click **Add New**



5. Choose **oAuth2 credentials**
6. Give your new credential a name, and change the Grant Type to **Authorization Code**
7. Now enter the **Authorization URL**, **Access Token URL**, **Client ID**, **Client Secret** and **Scope** from the table above.

OAuth2

OAuth2 credentials

Name

WOW HOWTO

Secret's name

Type

OAuth2 credentials

Secret's type

Grant Type

Authorization Code

Authorization URL

https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/oauth2/v2.0/authorize

Access Token URL

https://login.microsoftonline.com/c341abae-73dc-4a02-b018-3b9d18d51714/oauth2/v2.0/token

Client ID

b7dbbd17-2af9-4f4b-94bc-76d8408ed993

Client Secret

5Ty8Q~drFpTBVh4kWQGITn5PMb6ykxS54LQc3dzj

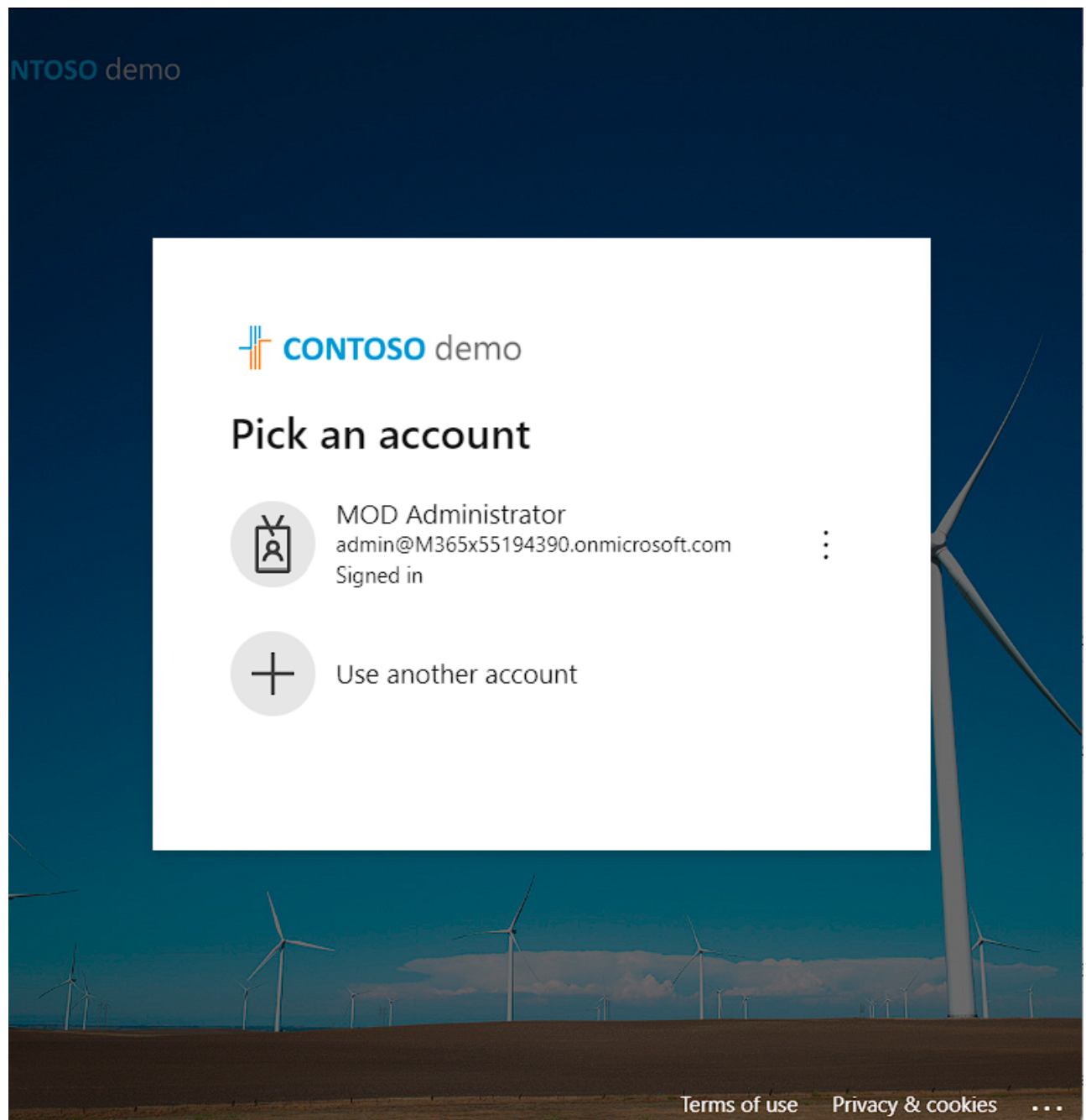
Scope

offline\_access Mail.ReadWrite Mail.Sen

Authorize

Cancel

Save

8. Click **Authorize**

## 9. Login to Azure AD.'



admin@m365x55194390.onmicrosoft.com

## Permissions requested

World of Workflows HOWTO

[App info](#)

**This application is not published by Microsoft.**

This app would like to:

- ✓ Maintain access to data you have given it access to
- ✓ Read and write access to your mail
- ✓ Send mail as you
- ✓ View your basic profile

☐ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

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

Cancel

Accept

10. Check the permissions are correct and click **Accept**

11. Finally, click **Save** when returned to Credential Manager

This credential is now available for use when calling Microsoft Graph using HTTP or through any Office 365 or Microsoft Graph plugin.