

## Microsoft Entra ID App Registration for IMAP Authentication

1. Log into <https://entra.microsoft.com/#home> using an admin account.
2. Select App Registrations under the Entra ID on the left hand side column.

The screenshot displays the Microsoft Entra admin center interface. The left-hand navigation pane is visible, with the 'App registrations' option highlighted by a red rectangular box. The main content area shows the 'App registrations' page, which includes a breadcrumb trail 'Home > IMAP Authentication | API permissions >', a title 'App registrations', and a set of action links: '+ New registration', 'Endpoints', 'Troubleshoot', 'Refresh', 'Download', 'Preview features', and 'Got feedback?'. Below these links is a blue informational banner regarding the transition from ADAL to MSAL. Further down, there are tabs for 'All applications', 'Owned applications' (which is selected), and 'Deleted applications'. A search bar prompts the user to 'Start typing a display name or application (client) ID to filter these r...'. At the bottom of the main area, a message states 'This account isn't listed as an owner of any applications in this directory.' with a blue button labeled 'View all applications in the directory'.

3. Select + New registration in app registrations window.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links: Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Enterprise apps, App registrations (highlighted), Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, and Identity Secure Score. The main content area is titled 'App registrations' and includes a breadcrumb 'Home > IMAP Authentication | API permissions >'. A red box highlights the '+ New registration' button. Below this are links for Endpoints, Troubleshoot, Refresh, Download, Preview features, and Got feedback. A blue information banner states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory 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](#)'. Below the banner are tabs for 'All applications', 'Owned applications' (selected), and 'Deleted applications'. A search bar prompts 'Start typing a display name or application (client) ID to filter these r...' with an 'Add filters' button. At the bottom, a message reads 'This account isn't listed as an owner of any applications in this directory.' with a button 'View all applications in the directory'.

Microsoft Entra admin center

Search resources, services, and docs (G+)

Home > IMAP Authentication | API permissions >

## App registrations

+ New registration | Endpoints | Troubleshoot | 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 Active Directory 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

This account isn't listed as an owner of any applications in this directory.

[View all applications in the directory](#)

4. Give your application a unique name, and select Accounts in this organisations directory only as the supported accounts type. The redirect URI is not required for this application type.

Microsoft Entra admin center

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

Copilot

Home > IMAP Authentication | API permissions > App registrations >

## Register an application

\* Name

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

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only  only - Single tenant

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - 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

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

[Register](#)


5. Copy the Client ID and Tenant ID fields under the application overview page.

Home > IMAP Authentication | API permissions > App registrations > Register an application > App registrations >

## IMAP Authentication

 Search <<

 Delete  Endpoints  Preview features

 Overview

 Quickstart

 Integration assistant

 Diagnose and solve problems

### Manage

 Branding & properties

 Authentication (Preview)

 Certificates & secrets


 Token configuration

 API permissions

 Expose an API

 App roles

 Owners

 Roles and administrators

 Manifest

### Support + Troubleshooting

 New support request

#### ^ Essentials

Display name

[IMAP Authentication](#)

Application (client) ID

[REDACTED]



Object ID

[REDACTED]

Directory (tenant) ID

[REDACTED]



Supported account types

[My organization only](#)

Client credentials

[0 certificate, 1 secret](#)

Redirect URIs

[Add a Redirect URI](#)

Application ID URI


[Add an Application ID URI](#)

Managed application in local directory

[IMAP Authentication](#)

State

 Activated

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory 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](#)

[Get Started](#)

[Documentation](#)

## Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

6. Once you've copied the required fields, click on the certificates and secrets option from the navigation menu on the left hand side.

Home > IMAP Authentication | API permissions > App registrations > Register an application > App registrations >



## IMAP Authentication



Delete



Endpoints



Preview features



Overview



Quickstart



Integration assistant



Diagnose and solve problems

### Manage



Branding & properties



Authentication (Preview)



Certificates & secrets



Token configuration



API permissions



Expose an API



App roles



Owners



Roles and administrators



Manifest

### Support + Troubleshooting



New support request

#### Essentials

Display name

[IMAP Authentication](#)

Application (client) ID

[Redacted]

Object ID

[Redacted]

Directory (tenant) ID

[Redacted]

Supported account types

[My organization only](#)

Client credentials

[0 certificate, 1 secret](#)

Redirect URIs

[Add a Redirect URI](#)

Application ID URI

[Add an Application ID URI](#)

Managed application in local directory

[IMAP Authentication](#)

State

Activated



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory 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](#)



[Get Started](#)


[Documentation](#)

## Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

7. Select client secrets and add a 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.

Certificates (0) **1** Client secrets (0) Federated credentials (2)

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

**2**  New client secret


Description	Expires	Value ⓘ	Secret ID
-------------	---------	---------	-----------

No client secrets have been created for this application.


8. Provide a description for your client secret then select add. Leave the secret expiry to the recommended period.


### Add a client secret

Description

1 

Expires

Recommended: 180 days (6 months) 

2 

9. Copy the value field of the client secret, this will be used under the Secret ID field of the script.

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
IMAP Authentication	1/27/2026	PxO*****	<div></div> 

10. Once the client secret is configured, select API permissions from the navigation menu, then select Add a permission option.

✖ Diagnose and solve problems

Manage

🏠 Branding & properties

🔄 Authentication (Preview)

🔑 Certificates & secrets

📋 Token configuration

**🔗 API permissions**

☁️ Expose an API

👥 App roles

👤 Owners

👤 Roles and administrators

📄 Manifest

Support + Troubleshooting

👤 New support request

📘

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

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 shows all the permissions the application needs. [Learn more about permissions and consent](#)

+

Add a permission

2 Grant admin consent for dte-tech.com

1 API / Permissions name	Type	Description	Admin consent required	Status
No permissions added				

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

11. From the request API permissions page, select Microsoft Graph.

## Request API permissions

×


Select an API

Microsoft APIs


APIs my organization uses

My APIs


Commonly used Microsoft APIs

**Microsoft Graph**


Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Communication Services**


Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

**Azure DevOps**


Integrate with Azure DevOps and Azure DevOps server

**Azure Rights Management Services**


Allow validated users to read and write protected content

**Azure Service Management**


Programmatic access to much of the functionality available through the Azure portal

**Data Export Service for Microsoft Dynamics 365**


Export data from Microsoft Dynamics CRM organization to an external destination

**Dynamics 365 Business Central**


Programmatic access to data and functionality in Dynamics 365 Business Central

**Dynamics CRM**

Access the capabilities of CRM business software and ERP systems

**Intune**

Programmatic access to Intune data

**Microsoft Purview**

Unified data governance service that helps you manage and govern your on-

12. For the permissions type, select Application Permissions then Add permissions.

## Request API permissions



[← All APIs](#)



Microsoft Graph

<https://graph.microsoft.com/> [Docs](#)

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.

1

2

Add permissions

Discard

13. Scroll down the permissions lists provided/search from the search bar for Mail permissions. Select **Mail.Read** and **Mail.Send** permissions then add the selected permissions.

### Request API permissions

> MailboxSettings

✓ Mail (2)

<input checked="" type="checkbox"/>	Mail.Read ⓘ Read mail in all mailboxes	1	Yes
<input type="checkbox"/>	Mail.ReadBasic ⓘ Read basic mail in all mailboxes		Yes
<input type="checkbox"/>	Mail.ReadBasic.All ⓘ Read basic mail in all mailboxes		Yes
<input type="checkbox"/>	Mail.ReadWrite ⓘ Read and write mail in all mailboxes		Yes
<input checked="" type="checkbox"/>	Mail.Send ⓘ Send mail as any user	2	Yes

> Member

> MultiTenantOrganization

> MutualTlsOauthConfiguration

> NetworkAccess-Reports


3






Add permissions

Discard

14. Once the permissions are added, navigate back to the API Permissions page and click on the Grant Admin Consent for your organisation.

The **mail.read** and **mail.send** permissions should be listed, with an indicator showing the Granted status as shown below.

Permission  Grant admin consent for [redacted] 1

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (5) ...				
Mail.Read	Application	Read mail in all mailboxes	Yes	 Granted for [redacted] ...
Mail.Read	Delegated	Read user mail	No	 Granted for [redacted] ...
Mail.Send	Application	Send mail as any user	Yes	 Granted for [redacted] ...
Mail.Send	Delegated	Send mail as a user	No	 Granted for [redacted] ...
User.Read	Delegated	Sign in and read user profile	No	 Granted for [redacted] ...

## Creating App Passwords on Gmail

### 1) Prerequisites

- a) Use a Google account with 2-Step Verification (2FA) enabled.
- b) App Passwords do not work on accounts:
  - Without 2FA enabled.
  - Managed by some organizations (Google Workspace admins may disable it).
  - Using Advanced Protection Program.

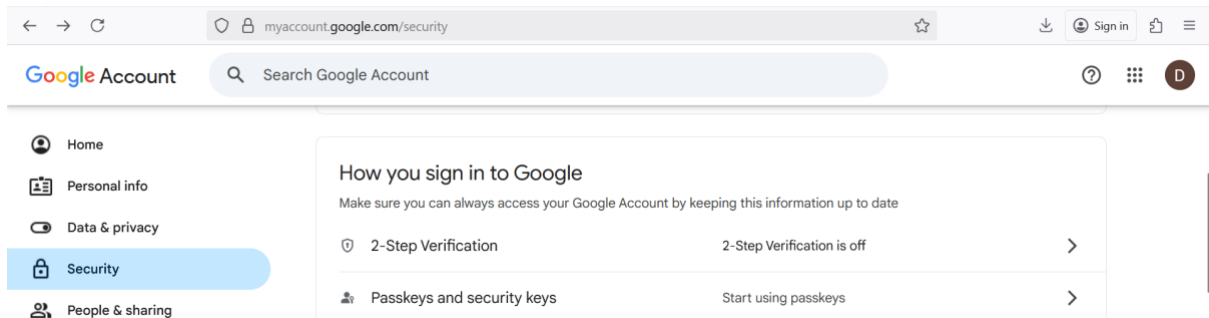
### 2) Step-by-Step: Enable App Passwords on Gmail

#### a) Step 1: Enable 2-Step Verification

- i) Go to: <https://myaccount.google.com/security>



- ii) Under Security, click 2-Step Verification.



- iii) Click Turn on 2-Step Verification, and follow the on-screen prompts to complete the setup using your phone number or Google Prompt.

### ← 2-Step Verification

#### Turn on 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

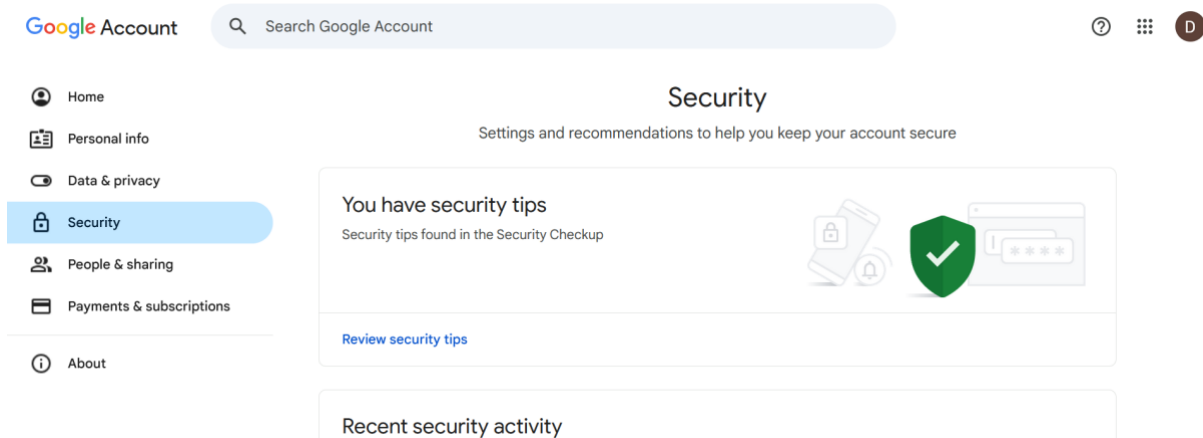
Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#)



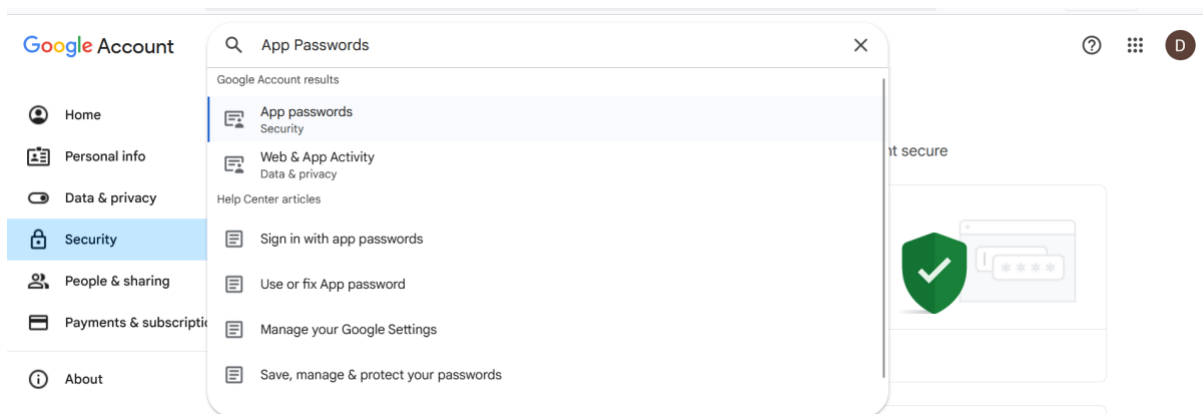
[Turn on 2-Step Verification](#)

#### b) Step 2: Generate an App Password

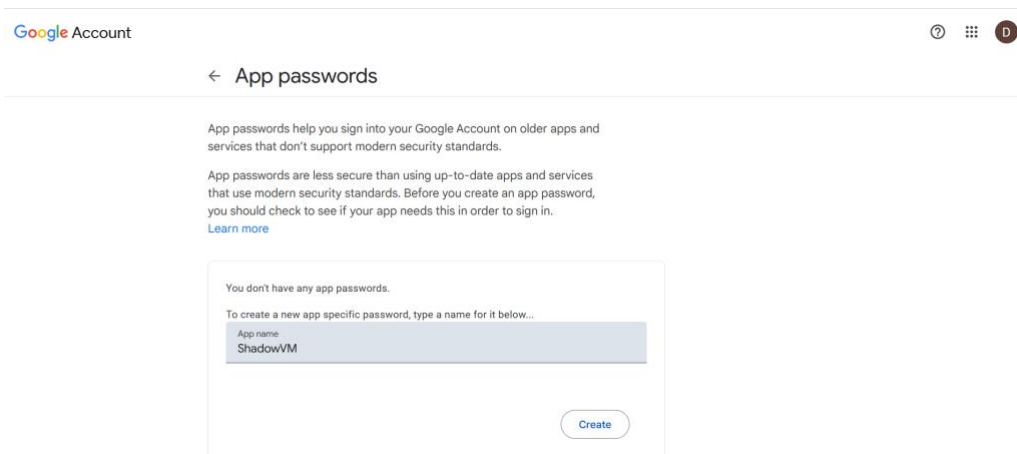
- i) After 2-Step Verification is enabled, return to the Security section.



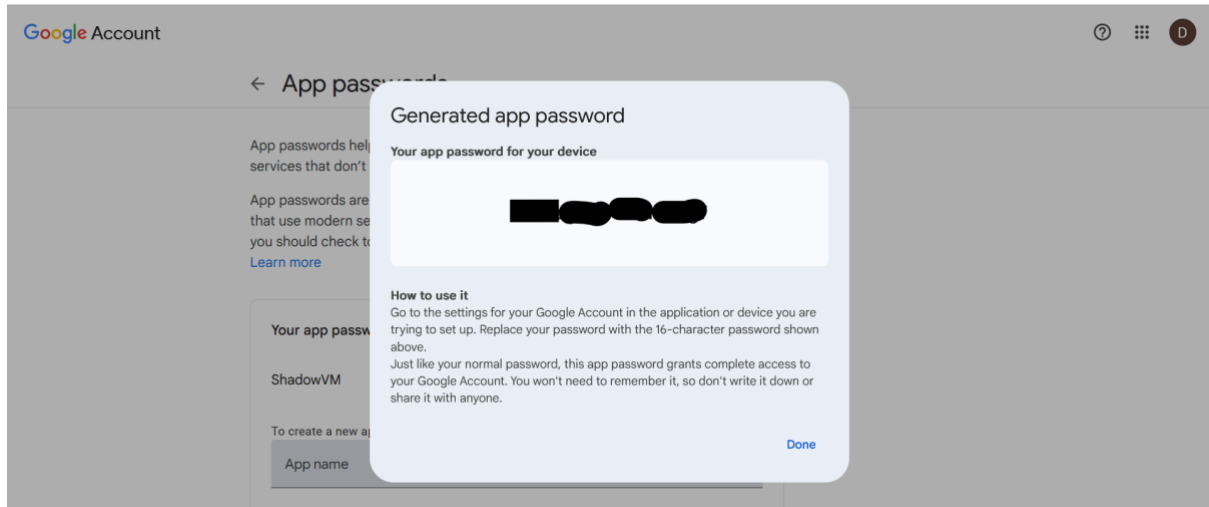
- ii) Look for **App Passwords**. If you don't see it directly, use the search bar within your Google Account settings and type "App Passwords" to find it. If you don't see it, make sure 2FA is enabled and you're not using a Workspace/child account.



- iii) You may be prompted to re-enter your Google password.
- iv) Type the App name and click on Create to Generate the 16 digit password.  
(e.g., **ShadowVM**).



- v) After clicking on Create, immediately copy the **Generated app password** on display screen before clicking on **Done** as it will not be display again.



c) Step 3: Use the App Password

- i) Copy this password (no spaces) and use it instead of your regular Gmail password in the application or script.

d) Step 4: Deleting It.

- i) When you no longer need the application that is using the app passwords, its best practice to delete the App Password “ShadowVM”

