

## 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 shows the Microsoft Entra admin center interface. The left sidebar is titled "Microsoft Entra admin center" and contains several navigation items: Home, Agents, Favorites, Overview, Users, Groups, Devices, Enterprise apps, App registrations (which is highlighted with a red box), Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, and Identity Secure Score. The main content area is titled "App registrations" and shows the "Owned applications" tab selected. A message at the top 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 this, there are three tabs: All applications, Owned applications (which is underlined), and Deleted applications. A search bar says "Start typing a display name or application (client) ID to filter these r...". A blue button labeled "Add filters" is next to it. A message below the tabs says "This account isn't listed as an owner of any applications in this directory." and a blue button says "View all applications in the directory". The URL in the browser is "entra.microsoft.com/#view/Microsoft\_AAD\_RegisteredApps/ApplicationsListBlade/quickStartType~/null/sourceType/Microsoft\_AAD\_IAM".

3. Select + New registration in app registrations window.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is visible with various navigation options like Home, Agents, Favorites, and App registrations (which is currently selected). The main content area is titled "App registrations". At the top of this section, there is a toolbar with several buttons: "+ New registration" (which is highlighted with a red box), Endpoints, Troubleshoot, Refresh, Download, Preview features, and Got feedback?. Below the toolbar, a message box contains a note about the end of support for ADAL and AAD Graph. The main content area shows tabs for All applications, Owned applications (which is underlined in blue), and Deleted applications. There is a search bar with placeholder text "Start typing a display name or application (client) ID to filter these r..." and a "Add filters" button. A message at the bottom states "This account isn't listed as an owner of any applications in this directory." with a "View all applications in the directory" button.

Microsoft Entra admin center

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](#)

Home Agents Favorites Entra ID Overview Users Groups Devices Enterprise apps App registrations Roles & admins Delegated admin partners Domain services Conditional Access Multifactor authentication Identity Secure Score

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.

Screenshot of the Microsoft Entra admin center showing the "Register an application" page. The left sidebar shows navigation options like Home, Agents, Favorites, Overview, Users, Groups, Devices, Enterprise apps, App registrations (selected), Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, and Authentication methods. The main content area shows the "Register an application" form. A red arrow labeled "1" points to the "Name" input field, which is empty. Another red arrow labeled "2" points to the "Accounts in this organizational directory only" radio button, which is selected. The "Supported account types" section also includes options for Multitenant and Personal Microsoft accounts.

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 [REDACTED] only - Single 2

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

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** X

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

**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](#)

**Essentials**

Display name <a href="#">IMAP Authentication</a>	Client credentials <a href="#">0 certificate, 1 secret</a>
Application (client) ID [REDACTED] <span style="color: red;">1</span>	Redirect URIs <a href="#">Add a Redirect URI</a>
Object ID [REDACTED]	Application ID URI <a href="#">Add an Application ID URI</a>
Directory (tenant) ID [REDACTED] <span style="color: red;">2</span>	Managed application in local directory <a href="#">IMAP Authentication</a>
Supported account types <a href="#">My organization only</a>	State <span style="color: green;">Activated</span>

**Information**

**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](#)**

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** X

Search ...

Delete Endpoints Preview features

Overview Quickstart Integration assistant Diagnose and solve problems

Certificates & secrets Activated

Manage

Branding & properties Authentication (Preview) Certificates & secrets Activated

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

**Get Started Documentation**

**Build your application with the Microsoft identity platform**

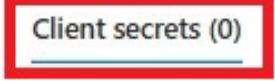
The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#) X

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.

1

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

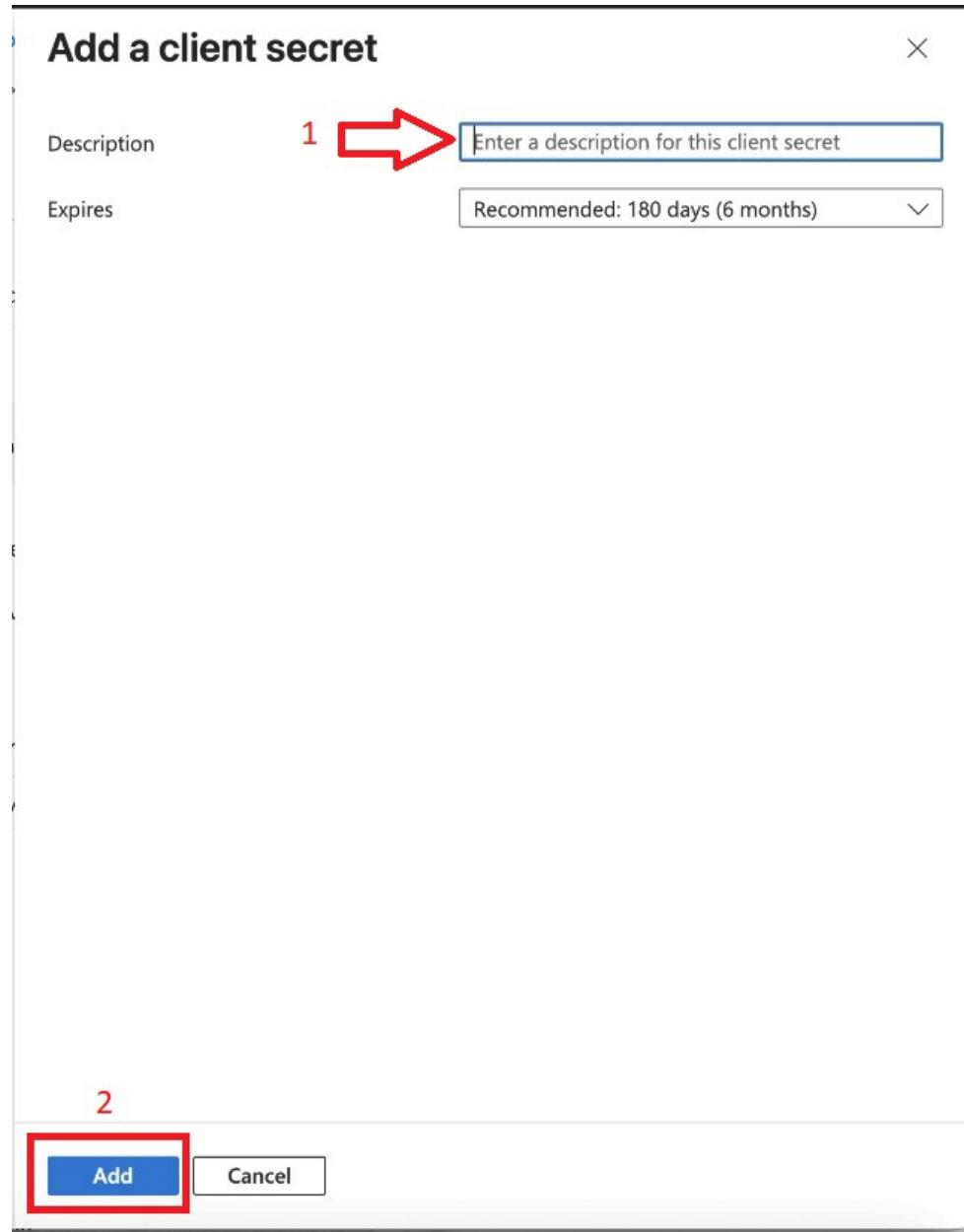
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

 2

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.



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*****	[REDACTED]	

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

Screenshot of the Azure portal showing the configuration of API permissions for an application.

The left sidebar shows the following navigation items:

- Diagnose and solve problems
- Manage
- Branding & properties
- Authentication (Preview)
- Certificates & secrets
- Token configuration
- API permissions** (highlighted with a red box)
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

The main content area displays the following information:

**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** (button highlighted with a red box)

1 API / Permissions name	Type	Description	Admin consent requ...	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.

 <b>Azure Communication Services</b> <p>Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams</p>	 <b>Azure DevOps</b> <p>Integrate with Azure DevOps and Azure DevOps server</p>	 <b>Azure Rights Management Services</b> <p>Allow validated users to read and write protected content</p>
 <b>Azure Service Management</b> <p>Programmatic access to much of the functionality available through the Azure portal</p>	 <b>Data Export Service for Microsoft Dynamics 365</b> <p>Export data from Microsoft Dynamics CRM organization to an external destination</p>	 <b>Dynamics 365 Business Central</b> <p>Programmatic access to data and functionality in Dynamics 365 Business Central</p>
 <b>Dynamics CRM</b> <p>Access the capabilities of CRM business software and ERP systems</p>	 <b>Intune</b> <p>Programmatic access to Intune data</p>	 <b>Microsoft Purview</b> <p>Unified data governance service that helps you manage and govern your on-</p>

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

## Request API permissions

[X](#)

[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

> MutualITIsOauthConfiguration

> NetworkAccess-Reports

3

Add permissions Discard

The screenshot shows the 'Request API permissions' dialog. Under the 'Mail' category, two permissions are selected: 'Mail.Read' (marked with a red box and number 1) and 'Mail.Send' (marked with a red box and number 2). Both permissions are set to 'Yes'. At the bottom, there are 'Add permissions' and 'Discard' buttons, with 'Add permissions' also highlighted with a red box and number 3.

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.

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>

A screenshot of a web browser showing the Google Account security settings. The URL in the address bar is myaccount.google.com/intro/security. The page title is "Google Account". On the left, there's a sidebar with links: Home, Personal info, Data & privacy, Security (which is highlighted with a blue background), and People & sharing. The main content area is titled "How you sign in to Google" and says "Make sure you can always access your Google Account by keeping this information up to date". It shows two sections: "2-Step Verification" (status: "2-Step Verification is off") and "Passkeys and security keys" (status: "Start using passkeys"). At the bottom right of the content area, there are two arrows pointing right: one for each section.

ii) Under Security, click 2-Step Verification.

A screenshot of the same Google Account security settings page as above, but with a larger view of the "2-Step Verification" section. The sidebar is visible on the left. The main content area now has a large callout box over the "2-Step Verification" section. The box title is "How you sign in to Google" and it says "Make sure you can always access your Google Account by keeping this information up to date". Below the title, there are two rows of options: "2-Step Verification" (status: "2-Step Verification is off") and "Passkeys and security keys" (status: "Start using passkeys"). Each row has a right-pointing arrow at the end. The "Security" link in the sidebar is also highlighted with a blue background.

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.

Google Account

Search Google Account

Home Personal info Data & privacy Security People & sharing Payments & subscriptions About

## Security

Settings and recommendations to help you keep your account secure

You have security tips

Security tips found in the Security Checkup

Review security tips

Recent security activity

- 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.

Google Account

Search App Passwords

Home Personal info Data & privacy Security People & sharing Payments & subscriptions About

App Passwords

Google Account results

- App passwords
- Web & App Activity
- Help Center articles
- Sign in with app passwords
- Use or fix App password
- Manage your Google Settings
- Save, manage & protect your passwords

- 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**).

Google Account

App passwords

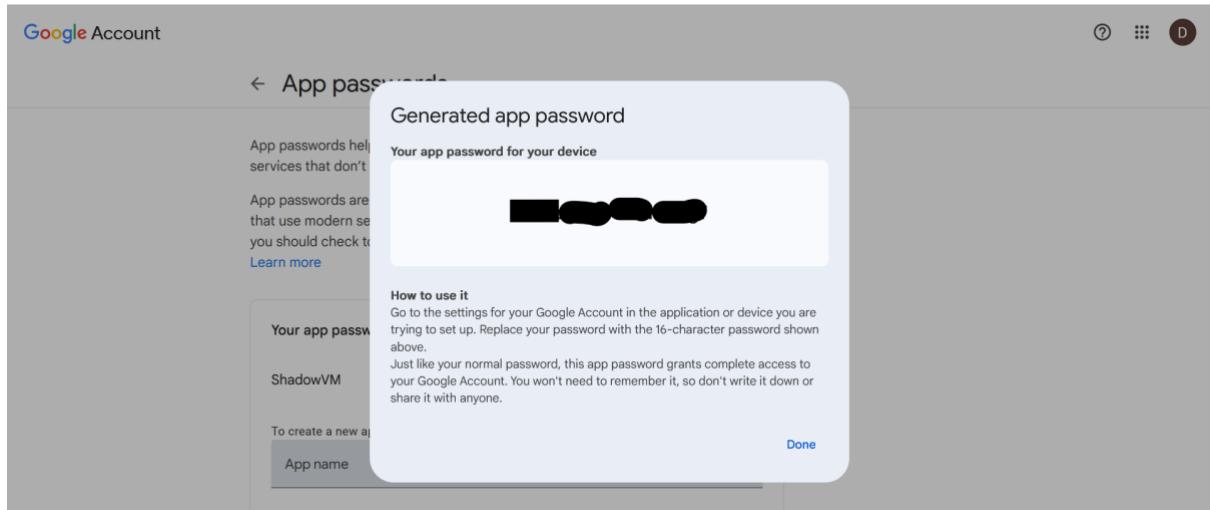
You don't have any app passwords.

To create a new app specific password, type a name for it below...

App name  
ShadowVM

Create

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

