



IMTLazarus Integration with Microsoft Azure



www.imtlazarus.com

Introduction

The purpose of this document is to provide the necessary steps to integrate IMTLazarus with Microsoft Azure.

Steps to Follow

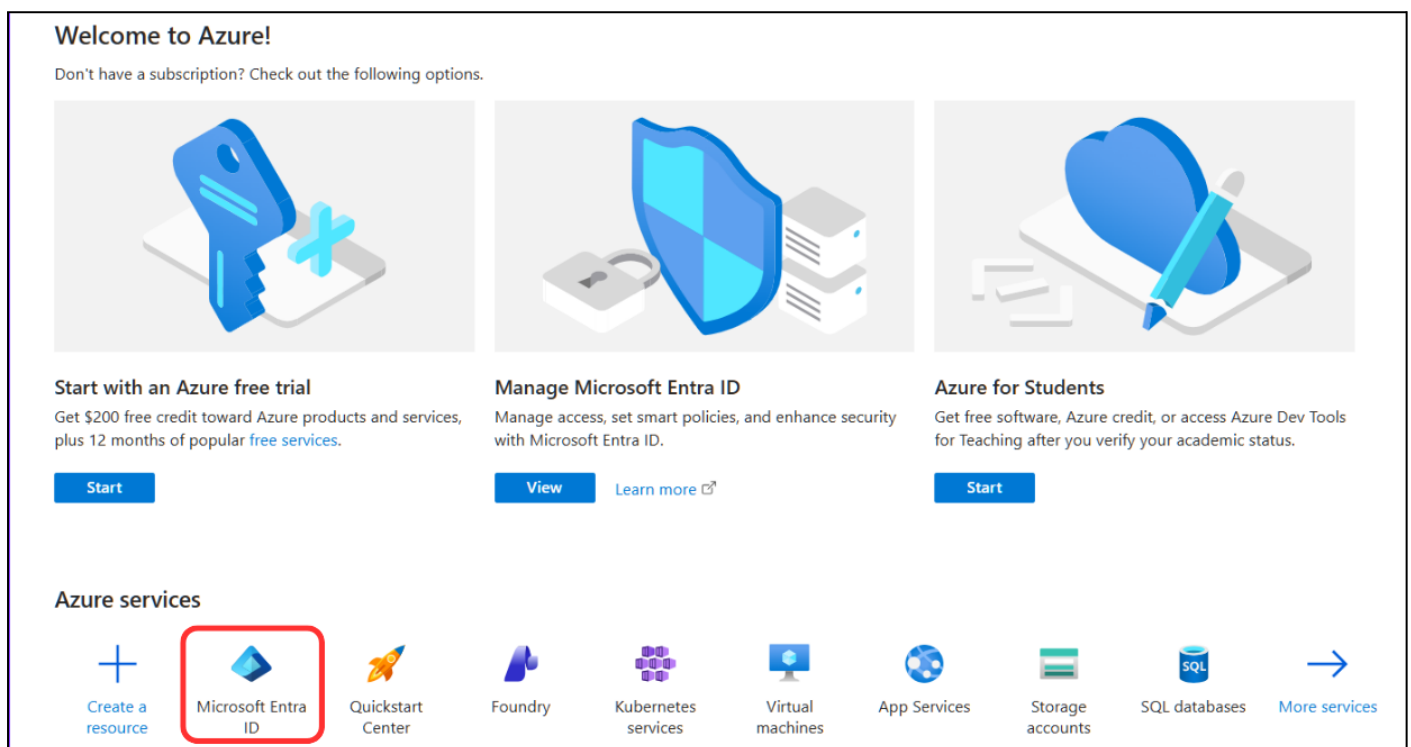
To enable the integration with Microsoft, the following requirements are needed:

- An IMTLazarus account with Administrator permissions.
- An account with access to the Microsoft Tenant.

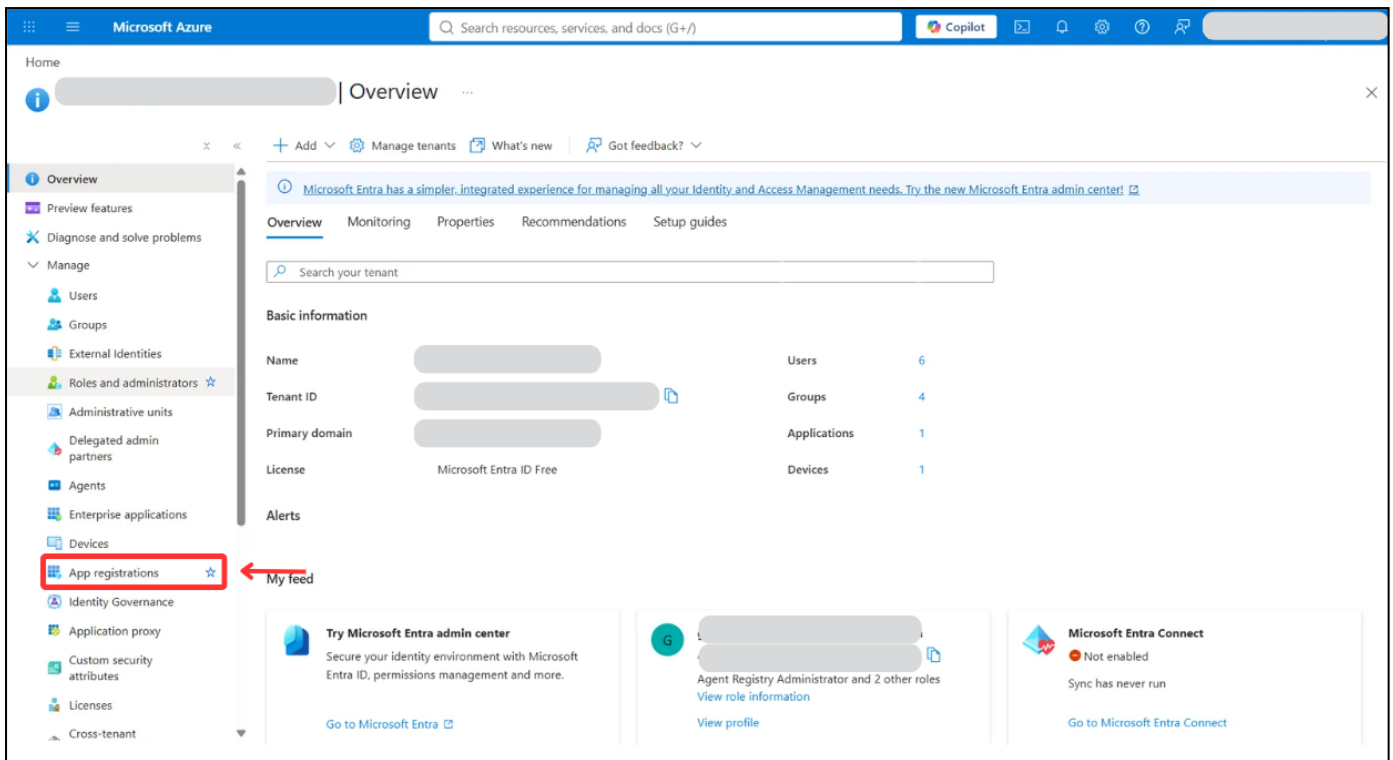
Step 1

Access the Azure portal using an Administrator account through the following link: <https://portal.azure.com/>

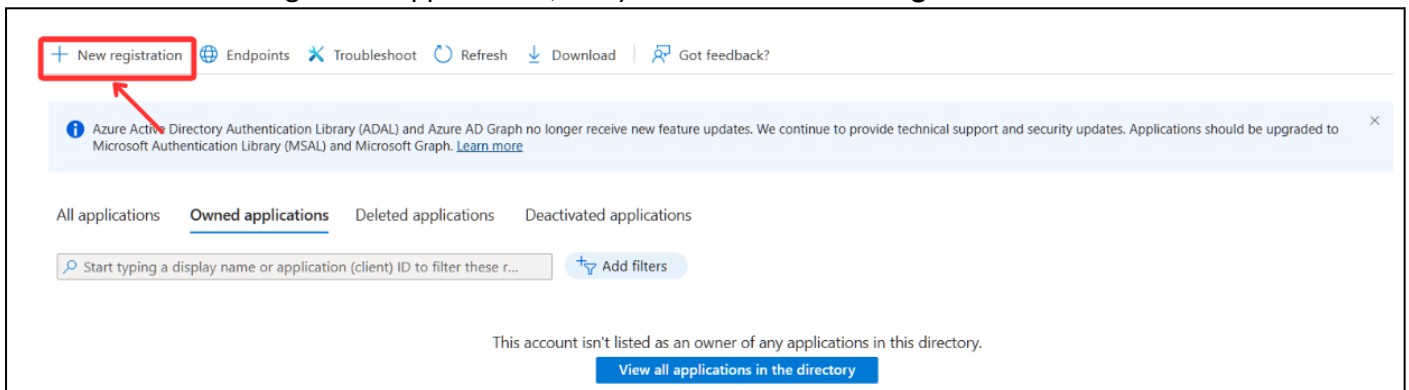
Once logged in, you will see a screen similar to the one below. Click on: **Azure Services** → **Microsoft Entra ID**



On the next screen, click on **Manage** → **App registrations**.



You will see a list of registered applications, if any exist. Click on **New registration**.



It is very important to complete the following fields correctly:

- **Name:** *IMTLazarus* (this is optional, but it is recommended to use this name).
- **Supported account types:** **MANDATORY** – Select the first option, "Single tenant only: [ORGANIZATION]".
- **Redirect URI:** <https://XXXXX.imtlazarus.com/lazarus/mlogin.php>
(Replace XXXXX with your IMTLazarus tenant name.)
- **Redirect URI 2:**
<https://internal.imtlazarus.com/lazarus/api/ios-multiuser-login/mlogin.php>
(This URI enables multiple students to use the same iPad device while applying each student's corresponding settings and configurations.)

*** Name**

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

IMTLazarus ✓

Supported account types

Choose the account types that can use this application or access this API

Single tenant only - LAZARUS INTEGRACIÓN SL ▼ [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.

Web ▼ <https://latamtest1.imtlazarus.com/lazarus/mlogin.php> ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

Once all the information has been entered, click on **Register**.

After the application registration is complete, an information screen will be displayed. We will need the **Application (client) ID** and the **Directory (tenant) ID** later in the process, so please copy and save these values in a temporary document.

Search

Deactivate Delete Endpoints

Overview 1

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview) 2

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support Troubleshooting

Essentials

Display name : [IMTLazarus](#)

Application (client) ID : a04de0c0-2350-4abd-b179-18906df95523

Object ID : 121d5332-ba49-4f56-a05c-a9a0eead1cb1

Directory (tenant) ID : a12bdbbe-9fc0-4c04-a1e1-a855607019f7

Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [1 web, 0 spa, 0 public client](#)

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

Managed application in L... : [IMTLazarus](#)

State : [Activated](#)

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

Azure Active Directory Authentication Library (ADAL) and Azure AD Graph no longer receive new feature updates. We continue to provide technical support and security updates. Applications should be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

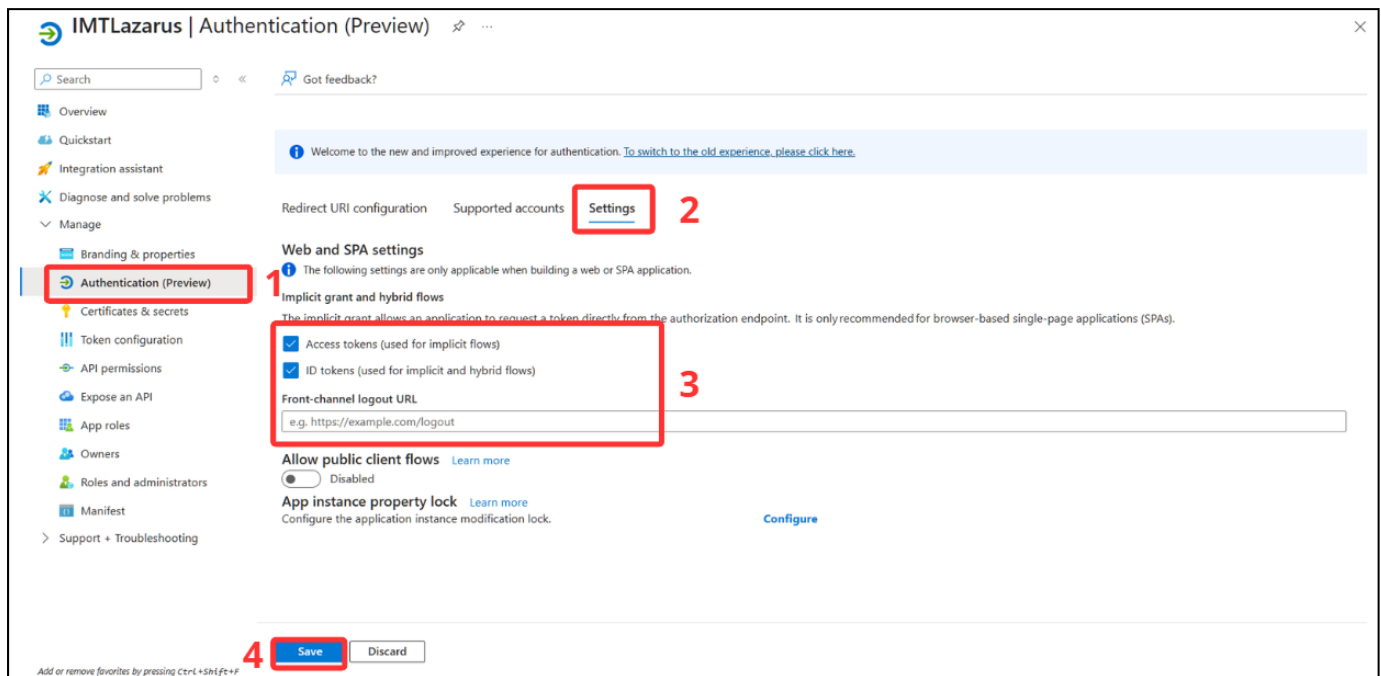
[Get Started](#) [Documentation](#)

Build your application with the Microsoft identity platform

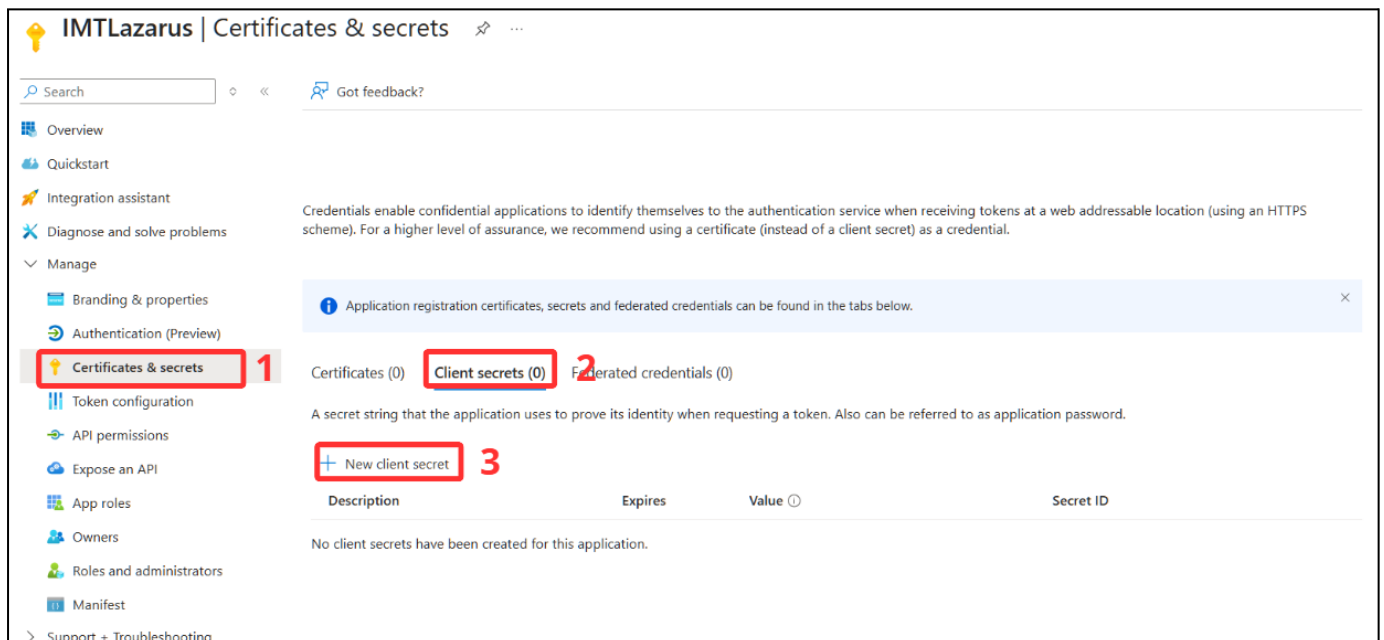
The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Next, click on **Authentication**.

In the **Authentication** section, click on **Settings** and enable the following two options: **Access tokens** and **ID tokens**. Check both boxes and then click **Save**.



Finally, navigate to **Certificates & secrets** and click on **New client secret**.



For the Description, enter **IMTLazarus**, and set the **expiration period** to the **maximum duration** available. Then, click **Add**.

Add a client secret

Description → IMTLazarus

Expires → Recommended: 180 days (6 months) ✓

90 days (3 months)

365 days (12 months)

545 days (18 months)

730 days (24 months)

Custom

The new client secret will now appear in the list of configured secrets.

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	
IMTLazarus	8/6/2028	4fK8Q~rTsw-xqvJ_AA7Uvty6IybuRi1QD9...	e68b8885-9efe-47e5-a729-22f58e9b971f	

Important: Be sure to copy the Secret Value and save it in your temporary document immediately. Once you leave this page, the secret value will no longer be displayed and cannot be retrieved again.

Return to the main menu and click on **API permissions** → **Add a permission**.

IMTLazarus | API permissions

Search

Refresh

Got feedback?

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

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

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 LAZARUS INTEGRACIÓN SL

API / Permissions name	Type	Description	Admin consent requ...	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](#).

Then, select **Microsoft Graph**.

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.

Add the following permissions:

Delegated Permissions

- **Device**
 - `Device.Read`
- **Family**
 - `Family.Read`
- **User**
 - `User.Read`
 - `User.ReadBasic.All`

Application Permissions

- **AppCatalog**
 - `AppCatalog.Read.All`
 - `AppCatalog.ReadWrite.All`
- **Channel**
 - `Channel.Create`
- **Device**
 - `Device.Read.All`
- **Directory**
 - `Directory.Read.All`
- **Domain**
 - `Domain.Read.All`
- **Group**
 - `Group.Read.All`

- Member
 - Member.Read.Hidden
- TeamsTab
 - TeamsTab.Create
 - TeamsTab.Read.All
 - TeamsTab.ReadWrite.All
 - TeamsTab.ReadWriteForTeam.All
- User
 - User.Read.All

Finally, grant the Administrator Consent for the configured 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 LAZARUS INTEGRACIÓN SL

We have now finished configuring the Azure portal.

Next, log in to your **IMTLazarus Admin Panel** and navigate to:

Administrator Menu → Settings → Integration → Microsoft

Then, complete the following sections using the information obtained from the Azure portal:

- Azure Connection Data
- Sign in with Microsoft

Fill in these tabs with the corresponding values from Azure, including the **Application (Client) ID**, **Directory (Tenant) ID**, and **Client Secret Value**. Once these details have been entered and saved, the integration between IMTLazarus and Microsoft Azure will be successfully configured.

Azure Link Data
Import Groups - (0)
Import Devices - (0)
Import Supervisors (Centro) - (0)
Observation
Sign in with Microsoft - (Enabled)

Directory ID (Tenant):
11111111-1111-1111-1111-111111111111

Client ID:
22222222-2222-2222-2222-222222222222

Client Secret:
-pUgu@0]?Ecepqj179z@wgT@]LWcXMeN

Active Link
☒

Microsoft Azure

Azure Link Data Import Groups - (0) Import Devices - (0) Import Supervisors (Centro) - (0) Observation Sign in with Microsoft - (Enabled)

Directory ID (Tenant): 11111111-1111-1111-1111-111111111111

Client ID: 22222222-2222-2222-2222-222222222222

Client Secret: -pUgu@0]?Ecepqj179z@wgT@]LWcXMeN

Sign in with Microsoft: ☒

Configure the settings as follows:

IMTLazarus	Microsoft Azure	(valor mostrado en las capturas)
Application ID (Client)	Id. de aplicación (cliente)	11111111-1111-1111-1111-111111111111
Directory ID (Tenant)	Id. de directorio (inquilino)	22222222-2222-2222-2222-222222222222
Client Secret	El valor del secreto generado	-pUgu@0]?Ecepqj179z@wgT@]LWcXMeN

Once the three information fields have been completed, the only remaining step is to enable the following options:

- **Active Integration**
- **Sign in with Microsoft**

Then, click **Save Configuration** to apply the settings.

The integration is now complete, and users will be able to authenticate using their Microsoft accounts through IMTLazarus.