

IMTLazarus integration manual with Microsoft Azure

To activate the integration with Microsoft we will need the following requirements:

an IMTLazarus account with Administrator permissions.

An account with access to the Microsoft Tenant.

Step 1: We access the Azure portal with the Administrator user through the following link: https://portal.azure.com/

Once inside, we will see a screen similar to this one. We will click on **Azure services** » **Azure Enter ID**:





On the next screen, click on Manage > App registrations

\rm IMTLaza	rus App registrations 🖉 🐇
° «	🕂 New registration 🌐 Endpoints 🧷 Troubleshooting 💍 Refresh 🞍 Download 💀 Preview features 🕴 🞘 Got feedback?
() Overview	
Preview features	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory G Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph Learn more
🗙 Diagnose and solve problems	Аррінаціоні мін песа то зе ардіацец то інклозон Ацпенисаціон цілану (тізяк) апо тіслозон огарні, <u>цеант поле</u>
\vee Manage	All applications Owned applications Deleted applications
🚨 Users	
🎎 Groups	Start typing a display name or application (client) ID to filter these r
External Identities	1 applications found
🤱 Roles and administrators	Display name ↑↓
Administrative units	M IMTLazarus
Delegated admin partners	-
Enterprise applications	
Devices	
App registrations	
Identity Governance	
Application proxy	
Custom security attributes	

It will show us the list of applications, if any. We click on New registration

+ New registration	Endpoints	🤌 Troubleshooting	🕐 Refresh		Preview features	Got feedback?
Starting June 30t Applications will	h, 2020 we will no need to be upgrad	longer add any new feat led to Microsoft Authen	tures to Azure Ac tication Library (N	tive Directory Aut MSAL) and Microso	nentication Library (ADAL oft Graph. <u>Learn more</u>) and Azure Active Directory G
All applications	Owned applicat	ions Deleted app	lications			
Start typing a dis	play name or app	lication (client) ID to f	ilter these r	+ _{\\\} Add fi	lters	
1 applications found						
Display name \uparrow_{\downarrow}						
IM IMTLazarus						

Now it is very important that we fill in the 3 fields:

Name: IMTLazarus (it is optional, but it should be called that way)

Account types: MANDATORY TO CHOOSE THE FIRST **OPTION**, ACCOUNTS OF THIS ORGANIZATIONAL BOARD

Redirect URI: <u>https://XXXXX.imtlazarus.com/lazarus/mlogin.php</u> (XXXXX is our IMTLazarus tenant)



<u>Only iOS</u>

Redirect

URI

2:<u>https://internal.imtlazarus.com/lazarus/api/ios-multiuser-login/mlogin.php</u> (with this direction, we would allow different students to use the same iPad device and apply their corresponding settings)

Once we have the data filled in, click on Register

After completing the application registration, it shows us an information screen (**Overview**). Later we will use the **Application ID (client)** and the **Directory ID (tenant)** so we copy them into a temporary document.

🔣 IMTLazarus 🖈 …			
	🗎 Delete 🌐 Endpoints 🖪 Preview features		
👯 Overview			
Quickstart Integration assistant Manage Demotion & presenties Authentication	Display name : IMTLazarus Application (dient) ID : 3aee9989-bc71-4c99-b4b3-76090f0e7dd0 Object ID : 77080527-8bd7-4b98-84a5-5d43c3598641 Directory (tenant) ID : 0087571c-37cf-409e-8ac3-e9a99c60811d	Client credentials Redirect URIs Application ID URI Managed application in	: <u>0 certificate_1 secret</u> : <u>1 web.0 spa.0 public client</u> : <u>Add an Application ID UR</u> I : I <u>MTLazarus</u>
Certificates & secrets	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Ar Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Micro	uthentication Library (ADAL) and Azure Active Directory Graph. We will cont soft Graph. <u>Learn more</u>	tinue to provide technical support and
 Expose an API 	Get Started Documentation		

Now we click **Authentication**, by default the **Implicid grant** It is unchecked, we activate both options **Access tokens** and **Tokens are id**.

earch	₽ Got feedback?
Dverview Quickstart Integration assistant Manage	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
 Authentication Certificates or secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest upport + Troubleshooting 	Web Quicksant Docsg" Image: Construct Construction Redirect URIs The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URIs use will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URIs and their restrictions? Image: The use of the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions? Image: The use has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSAL/s 2.0, you should migrate URIs. Image: The use has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSAL/s 2.0, you should migrate URIs. Image: The user was and a request to have the application clear the user's session data. This is required for single sign-out to work orrectly. Image: 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. The authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. Select the tokens you would like to be issued by the authorization endpoint.

And we don't forget to give Keep on footer



Finally, we go to Certificates and secrets and click on New client secret

💡 IMTLazarus Cert	ificates & secrets 👒 🚥	
	« 🔊 🔊 Got feedback?	
🐺 Overview		
🝊 Quickstart	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 bindner level of assurance, we recommend using a certificate (instead of a client secret) as a credential.	
🚀 Integration assistant		
∨ Manage	• • • • • • • • • • • • • • • • • • •	<
🧮 Branding & properties	Application registration certificates, secrets and federated credentials can be found in the tabs below.	
 Authentication Certificates & secrets 	Certificates (0) Client secrets (1) Federated credentials (0)	
III Token configuration	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.	
API permissions	+ New client secret	
Expose an API	Description Expires Value () Secret ID	
🗰 Ann roles		

As a description we put IMTLazarus and we tell you that expires maximum time, we click Add

Add a client secret			\times
Description		Enter a description for this client secret	
Expires		730 days (24 months)	\sim
		Recommended: 180 days (6 months)	
		90 days (3 months)	
		365 days (12 months)	
		545 days (18 months)	
	-	730 days (24 months)	
		Custom	

The new secret appears already configured

Certificates (0)	Client secrets (2)	Federated credentials (0)	
A secret string that	the application uses t	to prove its identity when red	questing a token. Also can be referred to as applic	ation password.
+ New client sec	rret			
Description		Expires	Value ①	Secret ID
Password upload	ed on Thu Oct 19 20	23 10/18/2025	DAi*********	2fb509c7-5f6c-4ce5-a5d1-d2b5049301e6 🗈 📋
IMTLazarus		5/28/2026	Mek8Q~cT1fOVulWJ.bsa5YXut4wxXb4Nj 🕅	50a765ec-cc0a-47e5-bbfe-55a52dbb56c6 🗈 📋
				•

Note: It is very important to copy the Secret VALUE NOW to the temporary document



IMTLazarus integration manual with Microsoft Azure

We return to the menu and click API permissions » Add a permission » Microsoft Graph



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. \times



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.

We added the following permissions:

» Delegated permissions

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

» Application Permissions

- AppCatalog
 - $\circ \quad \mathsf{AppCatalog.Read.All}$
 - 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

 \times



Finally, we grant administrator consent

Configured permiss	ions	
Applications are authori all the permissions the a	zed to call APIs when they are granted permissions by users/adm application needs. Learn more about permissions and consent	ns as part of the consent process. The list of configured permissions should include
+ Add a permission	\checkmark Grant admin consent for	

We are done with the Azure portal. We now go to our IMTLazarus panel and enter **Administrator Menu** » **Setup** » **Integration** » **Microsoft** and fill out the tab **Azure link data** and the tab **Sign in with Microsoft** with the information from the Azure portal

Azure Link Data Ir	nport Groups	: - (0) Import Devices - (0)	Import Supervisors (Centro) - (0)	Observation	Sign in with Mi	crosoft - (Disabled)
Directory ID (Te	enant):	11111111-1111-1111-1111	11111111		۲	
Cli	ent ID:	22222222-2222-2222-2222-22222	22222222		۲	
Client	Secret:	-pUgu@0]?Ecepqj179z@wgT@]L	WcXMeN		۲	
	Active	e Link 🔽				

Azure Link Data Import Grou	ps - (0) Import Devices - (0)	Import Supervisors (Centro) - (0)	Observation	Sign in with Microsoft - (Disabled)
Directory ID (Tenant):	1111111-1111-1111-1111	1111111		۲
Client ID:	2222222-2222-2222-2222-2222-2222-2222-2222	22222222		۲
Client Secret:	-pUgu@0]?Ecepqj179z@wgT@]l	LWcXMeN		۲
Sign in with Mi	crosoft: 🗸			



IMTLazarus integration manual with Microsoft Azure

We carry out the configuration in the following way:

IMTLazarus	Microsoft Azure	(value shown in the screenshots)
Directory ID (Tenant)	Directory ID (tenant)	11111111-1111-1111-1111-111111111111111
Application ID (client)	Application ID (client)	22222222-2222-2222-2222-22222222222222
Client Secret	The value of the generated secret	-pUgu@0]?Ecepqj179z@wgT@]LWcXMeN

Once the 3 information fields are filled in, all we have to do is check the box **Active Link and Sign in with Microsoft** and press the save settings button.