

IMTLazarus integration manual with Microsoft Azure

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

an IMTLazarus account with Administrator permissions.

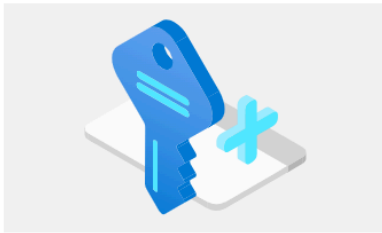
An account with access to the Microsoft Tenant.

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:**

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 Microsoft Entra ID

Manage access, set smart policies, and enhance security with Microsoft Entra ID.

[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](#)


[Microsoft Entra ID](#)


[Static Web Apps](#)


[Managed applications](#)


[App Services](#)


[App Configuration](#)


[Subscriptions](#)

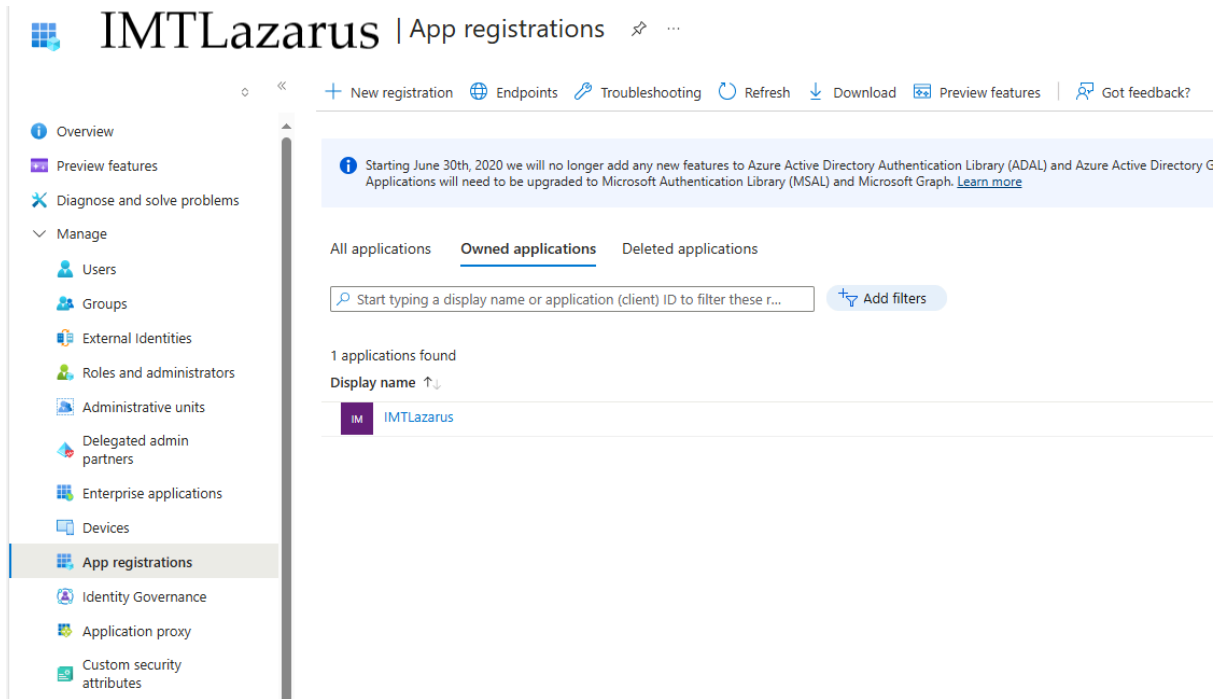

[Resource groups](#)


[Virtual machines](#)


[More services](#)

IMTLazarus integration manual with Microsoft Azure

On the next screen, click on Manage > App registrations



IMTLazarus | App registrations

[+ New registration](#)
[Endpoints](#)
[Troubleshooting](#)
[Refresh](#)
[Download](#)
[Preview features](#)
[Got feedback?](#)

[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](#)
 - [Application proxy](#)
 - [Custom security attributes](#)

[Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library \(ADAL\) and Azure Active Directory Graph. Applications will need to be upgraded to Microsoft Authentication Library \(MSAL\) and Microsoft Graph. \[Learn more\]\(#\)](#)

[All applications](#)
[Owned applications](#)
[Deleted applications](#)

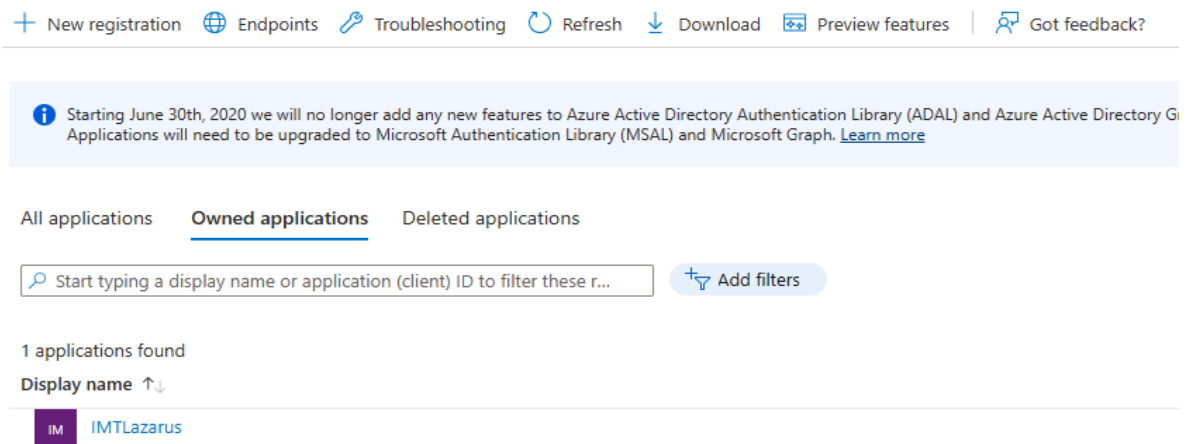
[Add filters](#)

1 applications found

Display name ↑↓

IM	IMTLazarus
----	------------

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



[+ 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 Active Directory Graph. Applications will need to be upgraded to Microsoft Authentication Library \(MSAL\) and Microsoft Graph. \[Learn more\]\(#\)](#)

[All applications](#)
[Owned applications](#)
[Deleted applications](#)

[Add filters](#)

1 applications found

Display name ↑↓

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

IMTLazarus integration manual with Microsoft Azure

Only iOS

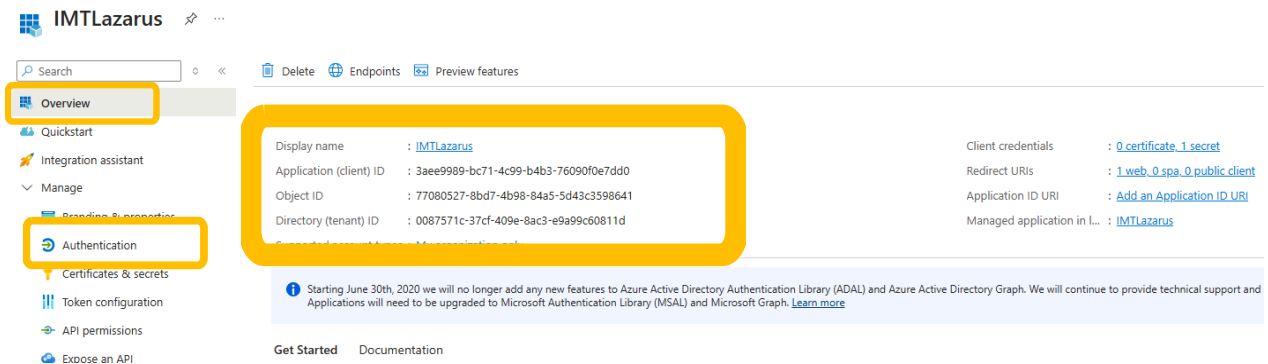
Redirect

URI

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

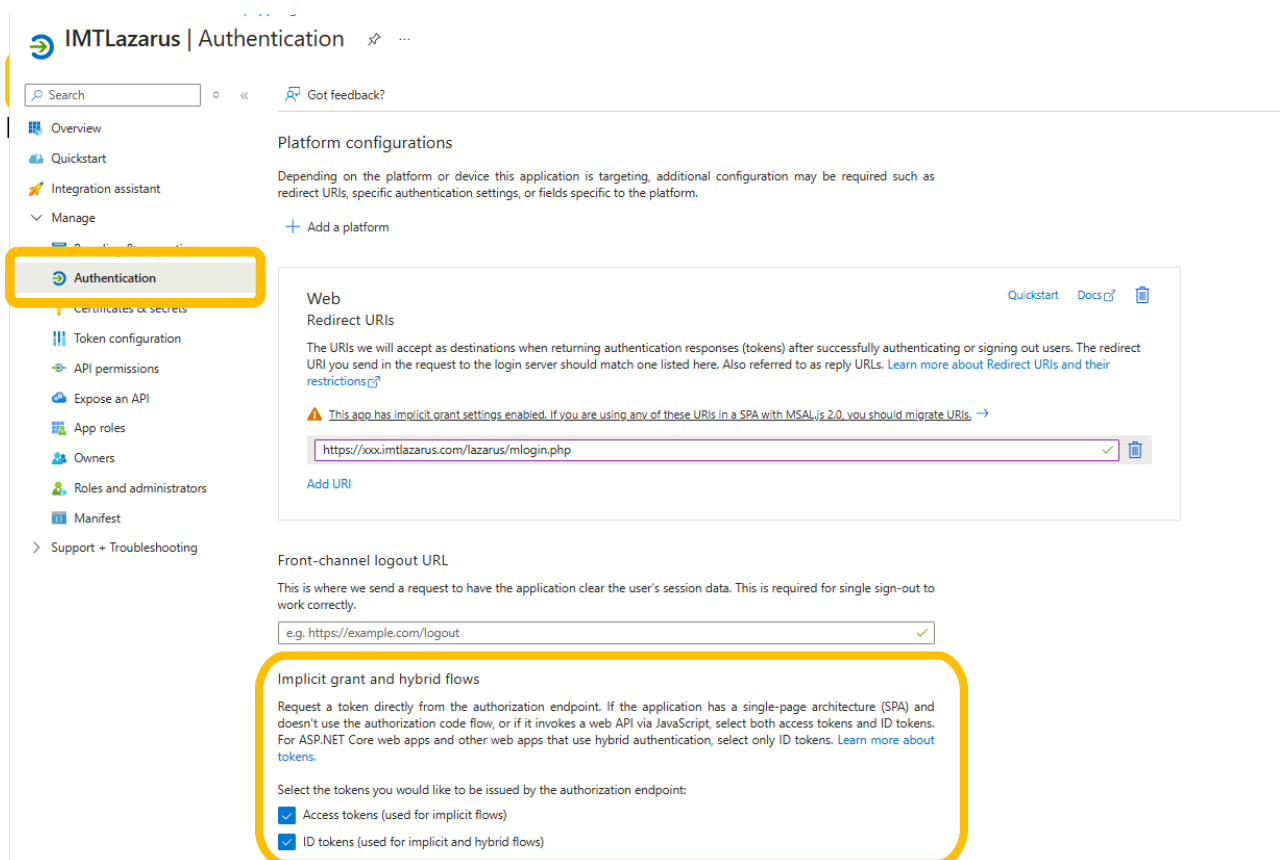
Once we have the data filled in, click on **Register**

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.



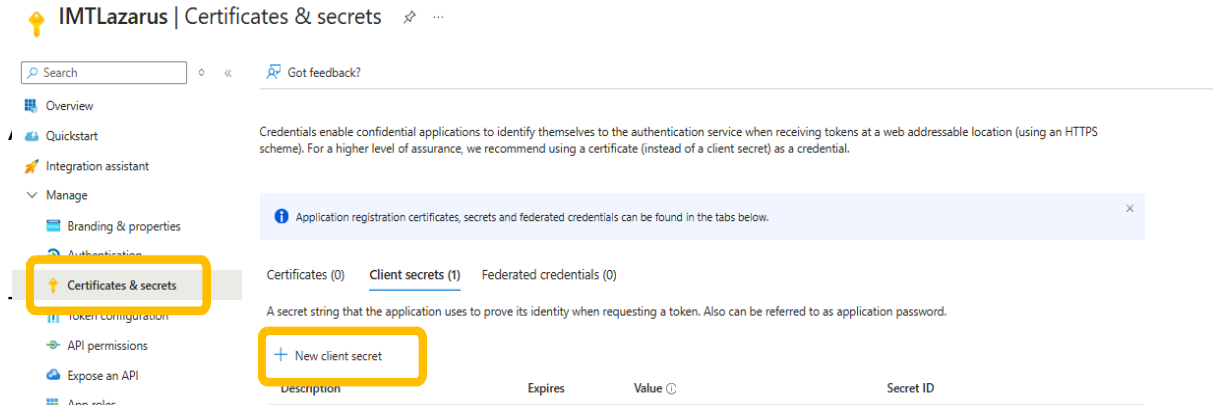
Now we click **Authentication**, by default the **Implicit grant** It is unchecked, we activate both options **Access tokens** and **Tokens are id**.

And we don't forget to give **Keep** on footer



IMTLazarus integration manual with Microsoft Azure

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



IMTLazarus | Certificates & secrets

Search Got feedback?

Overview

Quickstart

Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles

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)

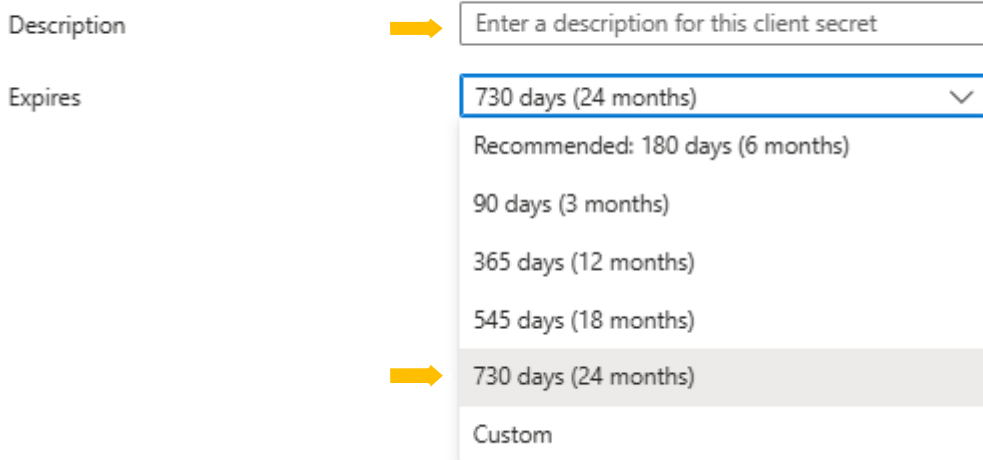
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

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

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

Add a client secret



Description

Expires

Recommended: 180 days (6 months)

90 days (3 months)

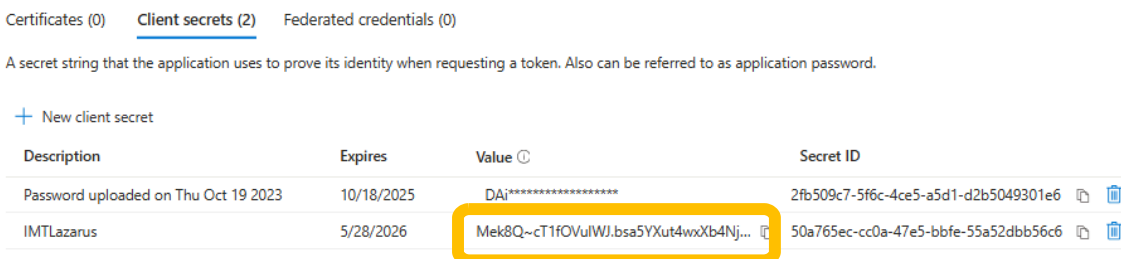
365 days (12 months)

545 days (18 months)

730 days (24 months)

Custom

The new secret appears already configured



Certificates (0) **Client secrets (2)** 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.

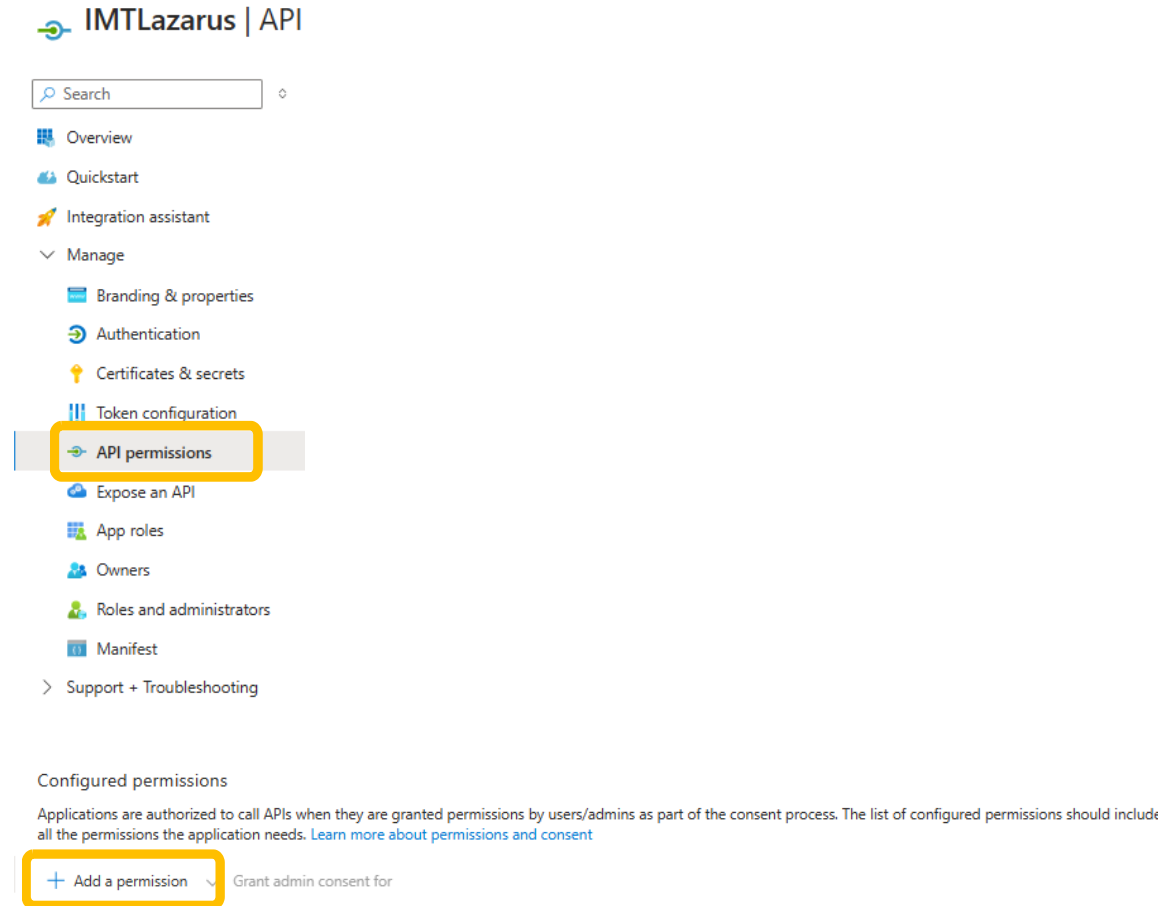
+ New client secret

Description	Expires	Value	Secret ID
Password uploaded on Thu Oct 19 2023	10/18/2025	DAj*****	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**



IMTLazarus | API

Search

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

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

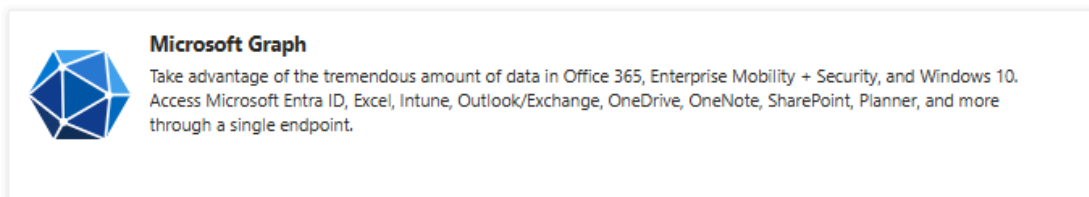
Request API permissions



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.

IMTLazarus integration manual with Microsoft Azure

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
 - 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

IMTLazarus integration manual with Microsoft Azure

Finally, we grant administrator consent

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

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	Import Groups - (0)	Import Devices - (0)	Import Supervisors (Centro) - (0)	Observation	Sign in with Microsoft - (Disabled)
Directory ID (Tenant):	<input type="text" value="11111111-1111-1111-1111-111111111111"/>				
Client ID:	<input type="text" value="22222222-2222-2222-2222-222222222222"/>				
Client Secret:	<input type="text" value="-pUgu@0]?Ecepqj179z@wgT@]LWcXMeN"/>				
Active Link	<input checked="" type="checkbox"/>				

Azure Link Data	Import Groups - (0)	Import Devices - (0)	Import Supervisors (Centro) - (0)	Observation	Sign in with Microsoft - (Disabled)
Directory ID (Tenant):	<input type="text" value="11111111-1111-1111-1111-111111111111"/>				
Client ID:	<input type="text" value="22222222-2222-2222-2222-222222222222"/>				
Client Secret:	<input type="text" value="-pUgu@0]?Ecepqj179z@wgT@]LWcXMeN"/>				
Sign in with Microsoft:	<input checked="" type="checkbox"/>				

IMTLazarus integration manual with Microsoft Azure

We carry out the configuration in the following way:

IMTLazarus	Microsoft Azure	<i>(value shown in the screenshots)</i>
Directory ID (Tenant)	Directory ID (tenant)	11111111-1111-1111-1111-111111111111
Application ID (client)	Application ID (client)	22222222-2222-2222-2222-222222222222
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.