

# Configure Microsoft Portal (portal.azure.com)

In order for one to be able to display groups and units in Moreservice, some setup must be done on Microsoft's cloud service (portal.azure.com).

Log in to portal.azure.com with a user who has elevated privileges

## 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](#)

[Learn more](#)



### Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

[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](#)

[Azure Active Directory](#)

[Intune](#)

[Cost Management ...](#)

[Subscriptions](#)

[Virtual machines](#)

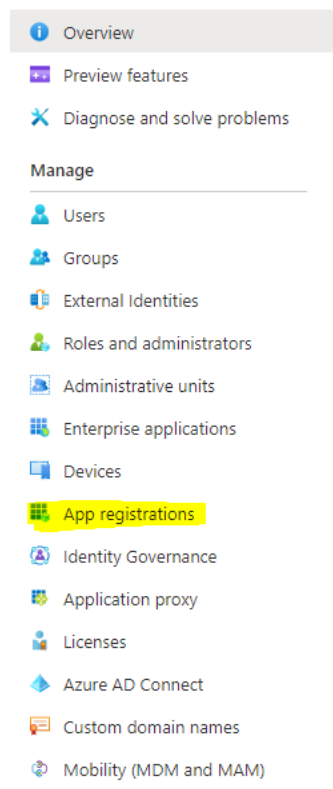
[Cost Management](#)

[Network security groups](#)

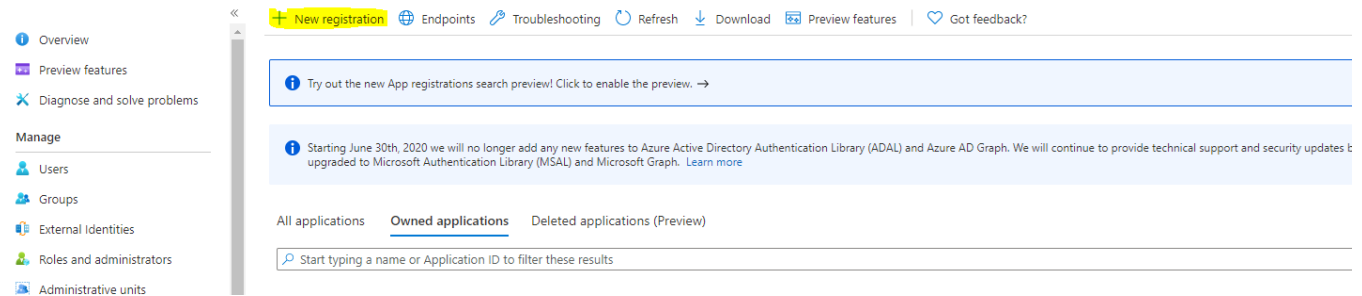
[All resources](#)

[More services](#)

In left menu tapp on App registration



## Tapp New registration



Enter a name for the app

\* Name

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

More Service Sync

Under **Supported account types** choose *Accounts in this organizational directory only (amesistech.net only - Single tenant)*

### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (amesistech.net only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

Under **Redirect URI (optional)**, choose *Single-page application (SPA)*. In the textbox field, enter the url of your agent portal

### 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.

Single-page application (SPA)

https://amer.dev.lan

Then tap Register at the bottom of the page

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

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

Register

Open Authentication in the menu on the left

[Home](#) > [amesistech.net](#) >



## More Service Sync



Search (Ctrl+/) <<

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

### Essentials

Display name : More Service Sync

Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : My organization only

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

[Get Started](#)

[Documentation](#)

Under *Implicit grant and hybrid flows* activate

- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)

[Home](#) > [amesistech.net](#) > [More Service Sync](#)



## More Service Sync | Authentication



Search (Ctrl+/) <<

Save Discard Got feedback?

https://amer.dev.lan

Add URI

Grant types

MSAL.js 2.0 does not support implicit grant. Enable implicit grant settings only if your app is using MSAL.js 1.0. [Learn more about auth code flow](#)

✓ Your Redirect URI is eligible for the Authorization Code Flow with PKCE.

### Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. <https://example.com/logout>

### Implicit grant and hybrid flows

Request 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. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

☒ Access tokens (used for implicit flows)

☒ ID tokens (used for implicit and hybrid flows)

Then press **Save**, at the top of the page

## More Service Sync | Authentication



Save



Discard



Got feedback?

Overview

Quickstart

Integration assistant

**Manage**

Branding

**Authentication**

### Platform configurations

Depending on the platform or device this application is targeting, additional configuration redirect URIs, specific authentication settings, or fields specific to the platform.

[+ Add a platform](#)[^ Single-page application](#)

Open **Add a certificate or secret** in the menu on the left, then click **New client secret**

## More Service Sync | Certificates & secrets



Got feedback?

Overview

Quickstart

Integration assistant

**Manage**

Branding

Authentication

**Certificates & secrets**

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

**Support + Troubleshooting**

Troubleshooting

New support request

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.

### Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[↑ Upload certificate](#)

Thumbprint	Start date	Expires	Certificate ID
------------	------------	---------	----------------

No certificates have been added for this application.

### Client secrets

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
-------------	---------	-------	-----------

No client secrets have been created for this application.

Give the **secret a name and choose an expiration date**. Then press **Add** at the bottom of the page

# Add a client secret



Description

MoreserviceSyncSecret

Expires

Recommended: 6 months



You will see the newly created value appear in the list

Copy the value located under **Value** and save it somewhere. It disappears when the page is refreshed

Microsoft Azure

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

Home > amesistechnet > More Service Sync

More Service Sync | Certificates & secrets

✦ ...

Search (Ctrl+/)

«

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

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.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	Certificate ID
No certificates have been added for this application.			

Client secrets

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
MoreserviceSyncSecret	1/2/2022	0~Zk4QaTM1NulnY~j1E0h~1i0_pK2LMZ	6b4d9aeb-8ed7-48f1-9d4b-5412e0a55ce3

Open **API permissions** in the menu on the left, and press **Add a permission**

Search (Ctrl+/)

«

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

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 v

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 amesistechnet

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

Then tap on **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 Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



### 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

The following permissions for Microsoft Graph must be entered

- Delegated
  - Device.Read.All
  - DeviceManagementManagedDevices.Read.All (Dersom dere har intune lisens)
  - Group.Read.All
- Application (Disse trenger admin rettigheter)
  - Device.Read.All
  - DeviceManagementManagedDevices.Read.All (Dersom dere har intune lisens)
  - Directory.Read.All
  - Group.Read.All
  - GroupMember.Read.All
  - User.Read.All

When you have added all the necessary permissions, press **Add permissions** at the bottom of the page

Permissions should then look like this

## 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 amesistechnet

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (9) ...				
<a href="#">Device.Read.All</a>	Delegated	Read all devices	Yes	⚠ Not granted for amesistech... ...
<a href="#">Device.Read.All</a>	Application	Read all devices	Yes	✅ Granted for amesistech... ...
<a href="#">DeviceManagementManagedDe</a>	Delegated	Read Microsoft Intune devices	Yes	⚠ Not granted for amesistech... ...
<a href="#">DeviceManagementManagedDe</a>	Application	Read Microsoft Intune devices	Yes	✅ Granted for amesistech... ...
<a href="#">Directory.Read.All</a>	Application	Read directory data	Yes	✅ Granted for amesistech... ...
<a href="#">Group.Read.All</a>	Delegated	Read all groups	Yes	⚠ Not granted for amesistech... ...
<a href="#">Group.Read.All</a>	Application	Read all groups	Yes	✅ Granted for amesistech... ...
<a href="#">GroupMember.Read.All</a>	Application	Read all group memberships	Yes	✅ Granted for amesistech... ...
<a href="#">User.Read.All</a>	Application	Read all users' full profiles	Yes	✅ Granted for amesistech... ...

Click on **Overview** in the menu on the left. Then copy the values from ( Application (client) ID and Directory (tenant) ID ) and save them along with the Client secret created earlier

[Home](#) > [amesistechnet](#) >



## More Service Sync



Delete



Endpoints



Preview features

Overview

Quickstart

Integration assistant

### Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

### Essentials

Display name : More Service Sync

Application (client) ID :

Object ID :

Directory (tenant) ID :

Supported account types : My organization only



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

[Get Started](#)

[Documentation](#)

Then the setup on Microsoft's cloud service is done, and you can return to More Service agent web and create a connection to Azure in the Microsoft Azure - AD app.