

Enabling Single Sign On with Microsoft Azure Active Directory

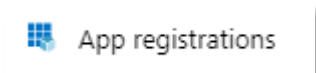
1 – Introduction

InEight Document offers Single Sign-On functionality using Microsoft Azure Active Directory and Active Directory Federation Service. Single Sign-On allows users to log into and access InEight Document with the same credentials as those used when logging into their computer or organization network.

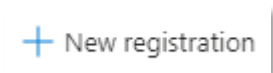
2 – Setup Instruction

2.1 App Registration

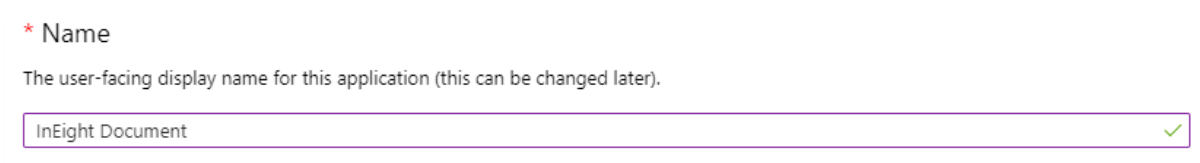
1. In Azure Portal, Go to **Azure Active Directory**.
2. Click **App Registrations** in the left menu.



3. Select **New Registration** from the top menu.



4. For the Name, enter **"InEight Document"**.



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

5. Select the suitable Supported Account Types. This is usually:
Accounts in this organizational directory only
6. Enter the **Redirect URI** (This will be shown in the Redirect URI field in the company screen).
7. Click **Register**.

Enabling Single Sign On with Microsoft Azure Active Directory

2.2 Authentication

1. Once the Registration is complete, go to **Authentication**.



2. In the Advanced Settings, ensure that **ID Tokens** is selected.

Advanced settings

Logout URL ⓘ

Implicit grant

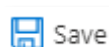
Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

Access tokens

ID tokens

3. Click **Save**.



2.3 API Permissions

1. Go to **API Permissions**.
2. Verify that, under **Microsoft Graph**, the **User.Read** permissions are set to **Delegated**.

API 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.

[+ Add a permission](#)

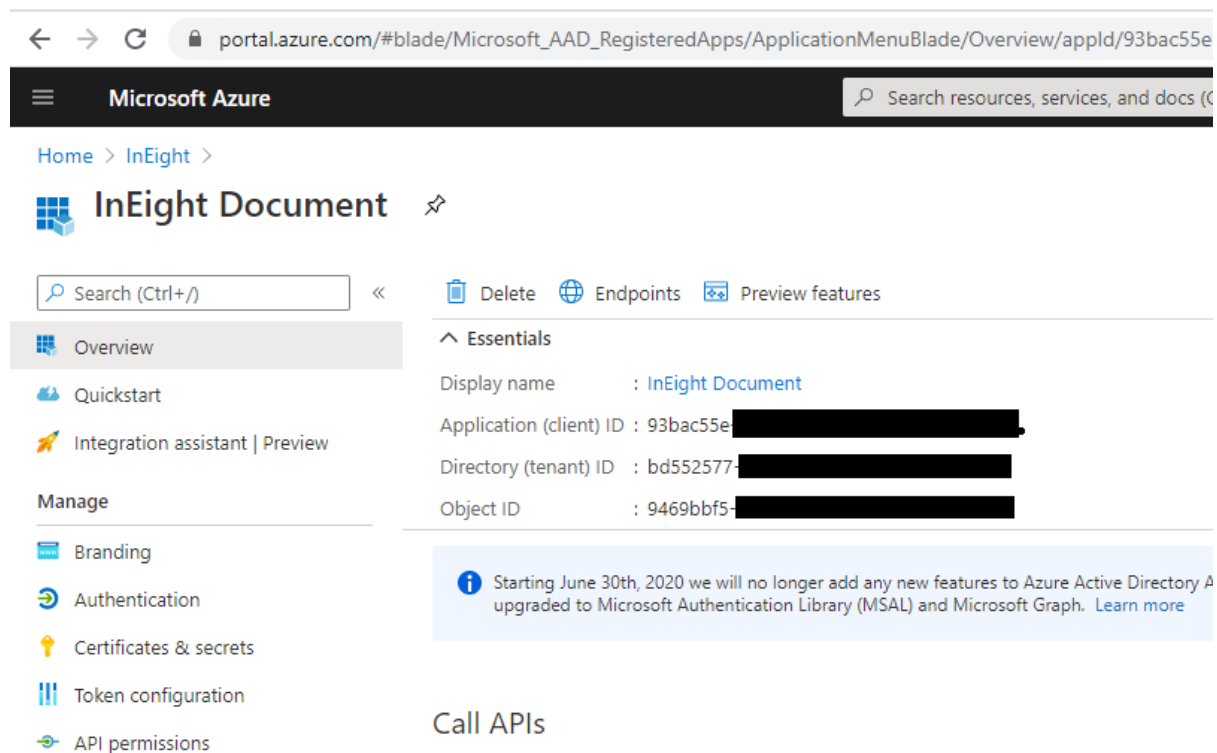
API / Permissions name	Type	Description	Admin Consent Required	Status
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	

2.4 Information Required

Please enter the following information on the company screen and click Save.

1. Application (client) ID – This will be shown in the Overview section of your Azure AD Setup

Enabling Single Sign On with Microsoft Azure Active Directory



The screenshot shows the Microsoft Azure portal interface. The browser address bar displays the URL: `portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/Overview/appld/93bac55e...`. The page title is "Microsoft Azure" with a search bar for resources, services, and docs. The breadcrumb navigation shows "Home > InEight >". The main heading is "InEight Document" with a share icon. Below this is a search bar and action buttons: "Delete", "Endpoints", and "Preview features". The left sidebar contains a navigation menu with categories: "Overview" (selected), "Quickstart", "Integration assistant | Preview", "Manage", "Branding", "Authentication", "Certificates & secrets", "Token configuration", and "API permissions". The main content area shows the "Essentials" section with the following details:

- Display name : InEight Document
- Application (client) ID : 93bac55e-██████████
- Directory (tenant) ID : bd552577-██████████
- Object ID : 9469bbf5-██████████

A blue information banner states: "Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory A upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)". Below this is a "Call APIs" section.

3 – More information?

For further information, please contact InEight.

<https://support.ineight.com>

Email: support@ineight.com