

Azure Active Directory Registration and Configuration

Overview

Read this guide to learn how to configure authentication for Azure App Service or Azure Functions so that your app signs in users with the [Microsoft identity platform](#) (Azure AD) as the authentication provider.


During creation of the app registration, collect the following information which you will need later when you configure Identity Service authentication in the WebUI.

- Client ID
- Tenant ID
- Client secret


Step 1: Create an app registration in Azure AD for your App Service app

1. Sign in to the [Azure portal](#), search for and select **App Services**, and then select your app. Note your app's **URL**. You'll use it to configure your Azure Active Directory app registration.


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](#)


[Email Communications](#)


[Azure Active Directory](#)


[SQL databases](#)


[Help + support](#)

[Virtual machines](#)

[App Services](#)

[App registrations](#)

[App Configuration](#)

[More services](#)

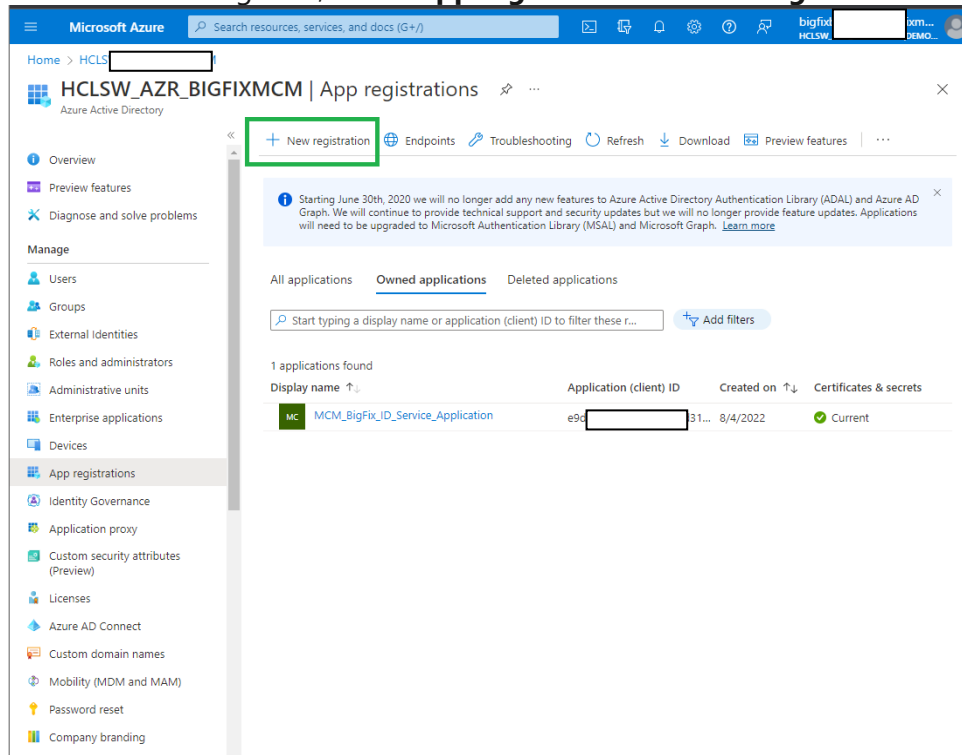
Resources

[Recent](#) [Favorite](#)

Name	Type	Last Viewed
------	------	-------------

2. From the portal menu, select **Azure Active Directory**.

- From the left navigation, select **App registrations** > **New registration**.



- In the **Register an application** page, enter a **Name** for your app registration.
- In **Supported account types**, select the account type that can access this application.
- Select **New registration** under App registration.

- Set **Supported account types** as desired. The options are:

Option	Who can sign in?
Accounts in this organizational directory only	Only users in your Microsoft 365 organization
Accounts in any organizational directory	Users in any Microsoft 365 organization (work or school accounts)
Accounts in any organizational directory ... and personal Microsoft accounts	Users in any Microsoft 365 organization (work or school accounts) and personal Microsoft accounts

- Redirect URI must have the information of the enrollment URL.

Microsoft Azure Search resources, services, and docs (G+)

Home > HC [redacted] XMCM | App registrations >

Register an application

* Name

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

Azure_AD_ID_SERVICE_DEMO_APP ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (HCLSW_AZR_BIGFIXMCM 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

[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.

Select a platform

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](#)

9. Select **Register**. On the application's **Overview** page, copy the value of the **Application (client) ID** and save it, you will need it in the next step. If you chose **Accounts in this organizational directory only** for **Supported account types**, also copy the **Directory (tenant) ID**.

Microsoft Azure Search resources, services, and docs (G+)

Home > HCL | App registrations >

Azure_AD_ID_SERVICE_DEMO_APP

Search (Ctrl+) Delete Endpoints Preview features

- 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
 - Troubleshooting
 - New support request

Essentials

Display name Azure_AD_ID_SERVICE_DEMO_APP	Client credentials Add a certificate or secret
Application (client) ID 91f91-██████████5b1	Redirect URIs Add a Redirect URI
Object ID 34120-██████████f448	Application ID URI Add an Application ID URI
Directory (tenant) ID 96fa-██████████5	Managed application in local directory Azure_AD_ID_SERVICE_DEMO_APP
Supported account types My organization only	

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

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to 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](#)

10. Click on Client Credentials.

Microsoft Azure Search resources, services, and docs (G+)

Home > HCL | App registrations >

Azure_AD_ID_SERVICE_DEMO_APP

Search (Ctrl+) Delete Endpoints Preview features

- 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
 - Troubleshooting
 - New support request

Essentials

Display name Azure_AD_ID_SERVICE_DEMO_APP	Client credentials Add a certificate or secret
Application (client) ID 91f91-██████████5b1	Redirect URIs Add a Redirect URI
Object ID 34120-██████████f448	Application ID URI Add an Application ID URI
Directory (tenant) ID 96fa-██████████5	Managed application in local directory Azure_AD_ID_SERVICE_DEMO_APP
Supported account types My organization only	

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

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

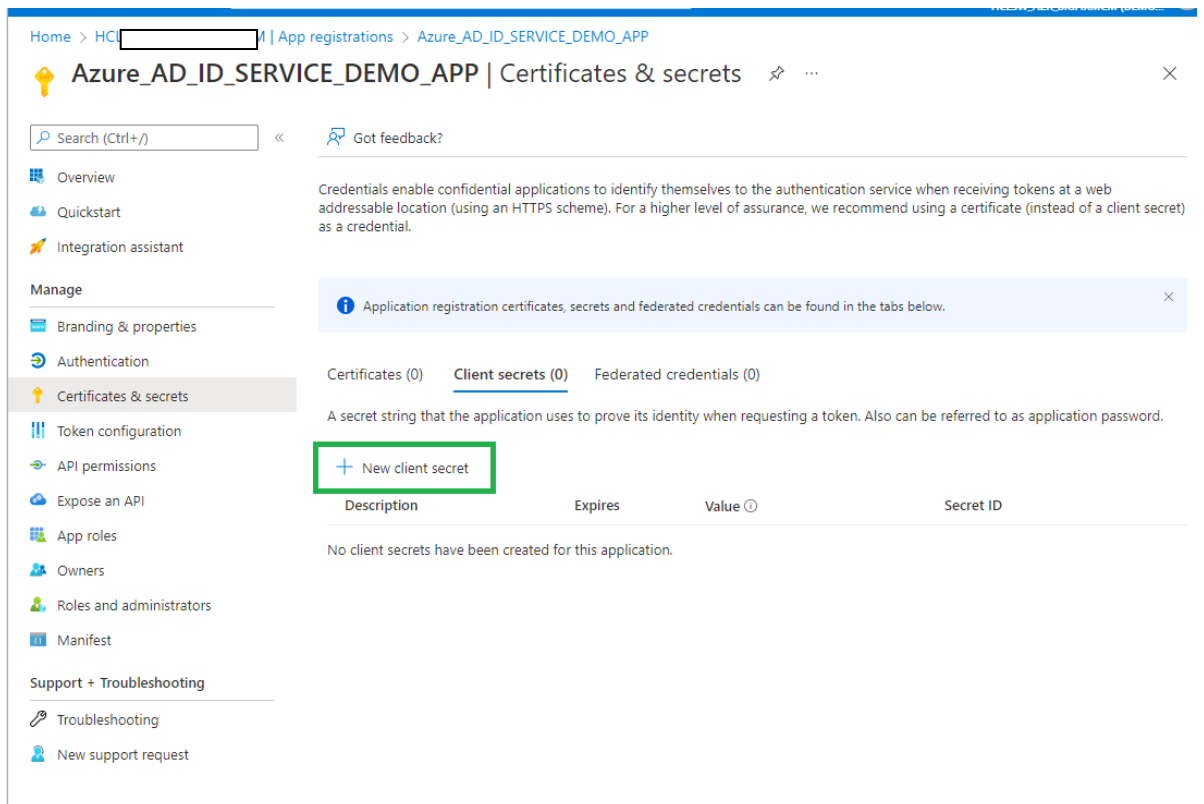
Get Started Documentation

Build your application with the Microsoft identity platform

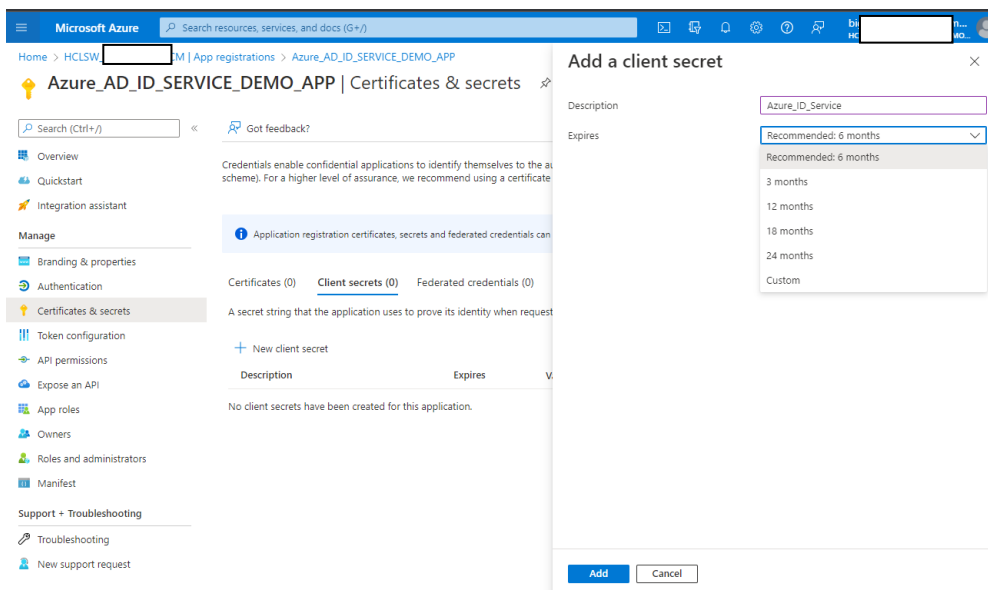
The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

11. Generate a new client secret: To create a client secret complete the following steps:

- a. From the left navigation, select **Certificates & secrets** and from the **Client secrets** tab, click **New client secret**.



- b. Enter a description and expiration and select **Add**.



c. Copy and keep the client secret value for future use.

Home > HCLSW_AZR_BIGFIXMCM | App registrations > Azure_AD_ID_SERVICE_DEMO_APP

Azure_AD_ID_SERVICE_DEMO_APP | Certificates & secrets

Search (Ctrl+/) Got feedback?

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

- 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.

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
Azure_ID_Service	9/5/2023	kl2[REDACTED]3ZP6...	ccdc[REDACTED]b8

You can see there will be a client secret value under client credentials in overview page of application

Home > HCLSW_AZR_BIGFIXMCM | App registrations >

Azure_AD_ID_SERVICE_DEMO_APP

Search (Ctrl+/) Delete Endpoints Preview features

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

- Troubleshooting
- New support request

Essentials

Display name
[Azure_AD_ID_SERVICE_DEMO_APP](#)

Application (client) ID
91f[REDACTED]

Object ID
3412[REDACTED]

Directory (tenant) ID
96f[REDACTED]

Supported account types
[My organization only](#)

Client credentials
[0 certificate, 1 secret](#)

Redirect URIs
[Add a Redirect URI](#)

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

Managed application in local directory
[Azure_AD_ID_SERVICE_DEMO_APP](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to 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](#)

With the collected Azure AD credentials information, create a .json file in the following format to upload it to WebUI on the Manage MDM server capability page.

```
{ "client_id": "06b6d920-xxxx-xxxx-xxxx-73792306xxxx",  
  "tenant_id": "31ac2431-xxxx-xxxx-xxxx-6215b1c2xxxx",  
  "client_secret": "d7bc6b2e-xxxx-xxxx-xxxx-b5c681e5xxxx"  
}
```

Step 2: Add permissions for Microsoft graph API to fetch user and group details

1. Under the application, click on the **API permissions** section.

The screenshot shows the 'Request API permissions' dialog in the Azure portal. The left sidebar shows the navigation menu with 'API permissions' selected. The main content area shows the 'Request API permissions' dialog with the 'Microsoft APIs' tab active. A table of 'Commonly used Microsoft APIs' is displayed, with 'Microsoft Graph' selected. The table lists various APIs with their descriptions and icons.

API Name	Description
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 DevOps	Integrate with Azure DevOps and Azure DevOps server
Azure Service Management	Programmatic access to much of the functionality available through the Azure portal
Azure Storage	Secure, massively scalable object and data lake storage for unstructured and semi-structured data
Data Export Service for Microsoft Dynamics 365	Export data from Microsoft Dynamics CRM organization to an external destination
Dynamics 365 Business Central	Programmatic access to data and functionality in Dynamics 365 Business Central
Dynamics CRM	Access the capabilities of CRM business software and ERP systems
Flow Service	Embed flow templates and manage
Intune	Programmatic access to Intune data
Office 365 Management APIs	Retrieve information about user, admin,

2. Request user and group permissions

The screenshot shows the 'Request API permissions' dialog in the Azure portal, specifically the 'User (2)' section. The dialog is open to the 'User (2)' section, showing a list of permissions. The 'User.Read' and 'User.Read.All' permissions are selected, indicating that the application is requesting permissions to read user profiles.

Permission Name	Description	Consent Status
User.Export.All	Export user's data	Yes
User.Invite.All	Invite guest users to the organization	Yes
User.ManageIdentities.All	Manage user identities	Yes
User.Read	Sign in and read user profile	No
User.Read.All	Read all users' full profiles	Yes
User.ReadBasic.All	Read all users' basic profiles	No
User.ReadWrite	Read and write access to user profile	No
User.ReadWrite.All	Read and write all users' full profiles	Yes

3. Once you add permission and the same is approved by the Admin, you can view list of available permission as below.

Search (Ctrl+/)

Refresh | Got feedback?

- 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
 - Troubleshooting
 - New support request

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.

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 HCLSW_AZR_BIGFIXMCM

API / Permissions name	Type	Description	Admin consent required	Status
▼ Microsoft Graph (4)				
Group.Read.All	Application	Read all groups	Yes	✓ Granted for HCLSW_AZR_BIGFIXMCM
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for HCLSW_AZR_BIGFIXMCM
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for HCLSW_AZR_BIGFIXMCM
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for HCLSW_AZR_BIGFIXMCM

To view and manage permissions and user consent, try [Enterprise applications](#).