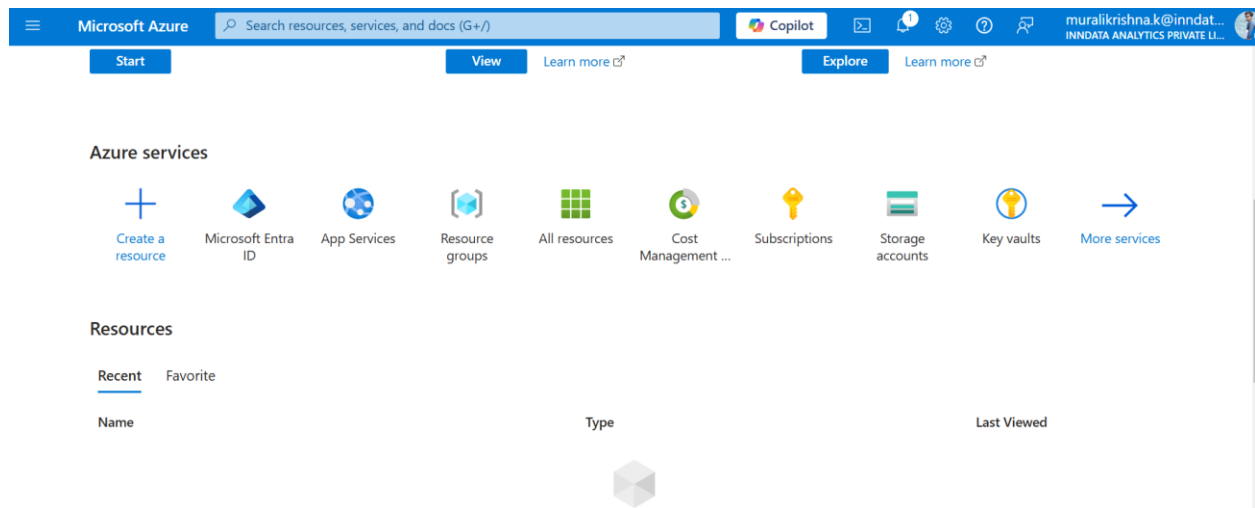


1. Click on Microsoft Entra ID



2. Click on +Add then click on App registration

Home >

innData Analytics Private Limited | Overview

+ Add Manage tenants What's new 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

User

Group

Enterprise application

App registration

Properties Recommendations Setup guides

Basic information

Name	innData Analytics Private Limited	Users	77
Tenant ID	b309ea5a-b8e2-49d5-bbb7-232c6d9008d7	Groups	46
Primary domain	inndata.in	Applications	44
License	Microsoft Entra ID Free	Devices	51

3. Set a meaningful name.

Microsoft Azure

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

Copilot

muralikrishna.k@inndat...
INNDATA ANALYTICS PRIVATE LI...

Home > innData Analytics Private Limited | Overview >

Register an application

* Name

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

Nifi-Authen

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (innData Analytics Private Limited only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

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

Register

^ Essentials

Display name
[Nifi-Authen](#)

Application (client) ID
3a9395d3-5b29-42f8-953f-16ac9f05015a

Object ID
3222d9f-ce75-4189-91ac-3825a120f526

Directory (tenant) ID
b309ea5a-b8e2-49d5-bbb7-232c6d9008d7

Supported account types
[My organization only](#)

Client credentials
[Add a certificate or secret](#)

Redirect URIs
[Add a Redirect URI](#)

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

Managed application in local directory
[Nifi-Authen](#)

4. Copy the **Application (Client) ID**, **Object ID**, and **Tenant ID**.

5. Click on **Certificates & Secrets**, Then New client secret

The screenshot shows the 'Nifi-Authen | Certificates & secrets' page in a web application. The left sidebar contains a navigation menu with items like Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, Branding & properties, Authentication, Certificates & secrets (highlighted), Token configuration, API permissions, Expose an API, App roles, and Owners. The main content area shows tabs for Certificates (0), Client secrets (0), and Federated credentials. A blue information banner at the top states: 'Application registration certificates, secrets and federated credentials are used to prove the identity of the application to the service it is connecting to.' Below the tabs, there is a '+ New client secret' button and a table with headers 'Description' and 'Expires'. The table is currently empty, with the message 'No client secrets have been created for this application.' at the bottom. An 'Add a client secret' modal is open on the right, featuring a close button (X) in the top right corner. The modal has two input fields: 'Description' with the placeholder 'Enter a description for this client secret' and 'Expires' with a dropdown menu showing 'Recommended: 180 days (6 months)'. At the bottom of the modal are 'Add' and 'Cancel' buttons.

Home > innData Analytics Private Limited | Overview > Nifi-Authen

Nifi-Authen | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Application registration certificates, secrets and federated credentials are used to prove the identity of the application to the service it is connecting to.

Certificates (0) **Client secrets (0)** Federated credentials

A secret string that the application uses to prove its identity when it accesses resources in the service.

+ New client secret

Description	Expires
No client secrets have been created for this application.	

Add a client secret

Description: Enter a description for this client secret

Expires: Recommended: 180 days (6 months)

Add Cancel

6. Click on **Delegated Permissions** under **Required Permissions**.

Select the following permissions :

openid

Profile

Directory.Read.All

Group.Read.All

email

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.

Add permissions

Discard

Request API permissions



Select permissions

[collapse all](#)

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, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
▼ Directory (1)	
<input type="checkbox"/> Directory.AccessAsUser.All ⓘ Access directory as the signed in user	Yes
<input checked="" type="checkbox"/> Directory.Read.All ⓘ Read directory data	Yes

Add permissions

Discard

7. Click on **Application Permissions** under **Required Permissions**.
Select **Directory.Read.All** and **Group.Read.All**.

Request API permissions



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.

Select permissions

[expand all](#)

Permission	Admin consent required
▼ Directory (1)	
<input checked="" type="checkbox"/> Directory.Read.All ⓘ Read directory data	Yes
<input type="checkbox"/> Directory.ReadWrite.All ⓘ Read and write directory data	Yes

Add permissions

Discard

Click Add permission Then Grant admin Consent

Microsoft Azure

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

Copilot

prasanra.ravva@inn-dat...

Home > App registrations > Nifi-Authen

Nifi-Authen | API permissions

Search x Refresh Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

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, or in organizations where this app will be used. [Learn more](#)

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 innData Analytics Private Limited

API / Permissions name			Admin consent requ...	Status
Microsoft Graph (5)				
Directory.Read.All	Delegated	Read directory data	Yes	Not granted for innData_...
Directory.Read.All	Application	Read directory data	Yes	Not granted for innData_...
email	Delegated	View users' email address	No	
profile	Delegated	View users' basic profile	No	
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Microsoft Azure

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

Copilot

prasanna.ravva@inn-dat...

Home > App registrations > Nifi-Authen

Nifi-Authen | API permissions

Search

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in innData Analytics Private Limited? This will update any existing admin consent records this application already has to match what is listed below.

Yes

No

where this app will be used.

mission, user, or app. This column may not reflect the value in your organization, or in organizations

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 innData Analytics Private Limited

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
Directory.Read.All	Delegated	Read directory data	Yes	Not granted for innData...
Directory.Read.All	Application	Read directory data	Yes	Not granted for innData...
email	Delegated	View users' email address	No	
profile	Delegated	View users' basic profile	No	
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Microsoft Azure

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

Copilot

prasanna.ravva@inn-dat...

Home > App registrations > Nifi-Authen

Nifi-Authen | API permissions

Search

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

New support request

Successfully granted admin consent for the requested permissions.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

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, or in organizations where this app will be used. [Learn more](#)

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 innData Analytics Private Limited

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
Directory.Read.All	Delegated	Read directory data	Yes	Granted for innData An...
Directory.Read.All	Application	Read directory data	Yes	Granted for innData An...
email	Delegated	View users' email address	No	Granted for innData An...
profile	Delegated	View users' basic profile	No	Granted for innData An...
User.Read	Delegated	Sign in and read user profile	No	Granted for innData An...

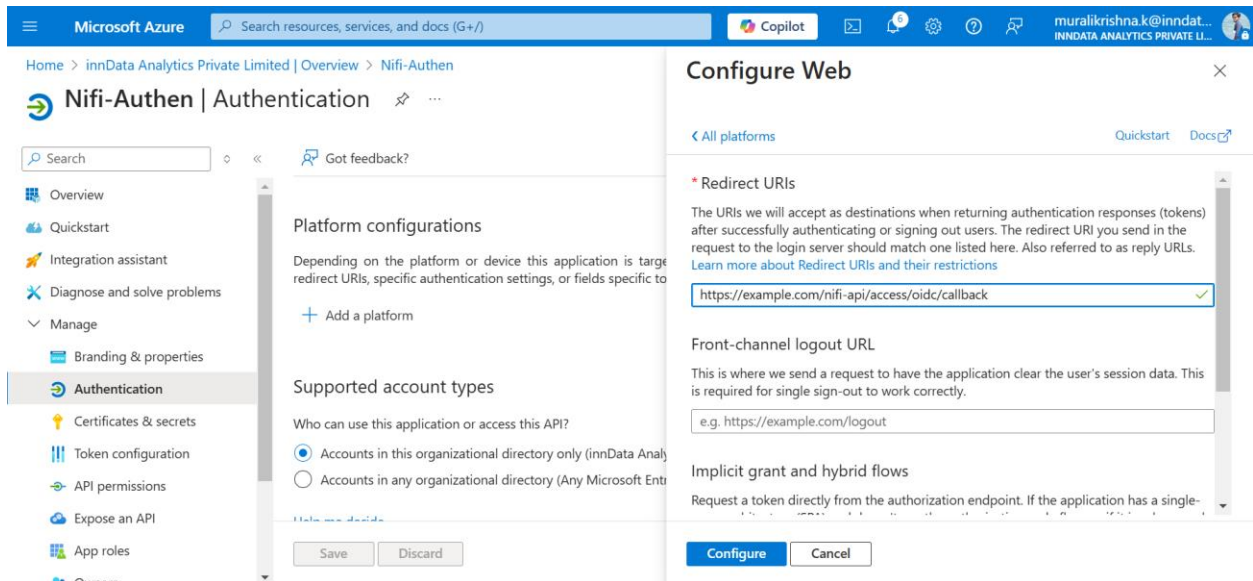
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

8. Click on **Authentication**, then click on **Add a Platform**.

Choose **Web** and set the Redirect URIs, such as:

<https://nifi-domain.com/nifi-api/access/oidc/callback>

Finally, click **Configure**.



9. Click on **Token Configuration**, then click on **Add Optional Claim**.

Under **Token Type**, select **ID**.

Check the boxes for **email** and **upn**, then click **Add**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'muralikrishna.k@inndata...'. The main content area is titled 'Nifi-Authen | Token configuration'. The left sidebar shows the navigation menu with 'Token configuration' selected. The main area displays 'Optional claims' with a table showing 'No results.' A modal window titled 'Add optional claim' is open on the right, showing 'Token type' as 'ID' and a list of claims including 'email', 'family_name', 'fwd', and 'given_name'.

Note: Create 2 Groups i.e admin & dev. And add one user to Admin group.
Make sure you create one admin user for initial login for Nifi.

Once Completed please share me the below details :

Client Secret

Application ID

Directory ID

Group names

Initial admin user details.