

# **SSO providers' configuration guide**



# Table of Contents

Table of Contents.....	2
OKTA.....	3
Create OIDC app integrations using OKTA.....	4
Task 1: Launch the Wizard.....	4
Task 2: Configure initial settings.....	6
Task 3: Set up SSO settings inFlow.....	8
GOOGLE.....	9
Create OIDC app integrations using Google.....	10
ONELOGIN.....	17
Create OIDC app integrations using One Login.....	17
ENTRA.....	20
Create OIDC app integrations using Entra.....	21
ADFS Configuration.....	25
Configure inFlow SSO settings:.....	27

## Note:

These steps should help you get connected to your SSO provider; if you encounter any issues when setting up, contact your SSO provider to troubleshoot.



# OKTA

[Okta is an identity and access management \(IAM\)](#) service that provides a secure, single sign-on (SSO) solution for businesses.

It is a cloud-based platform that helps organizations securely manage user identities, access rights, and credentials across multiple applications, websites, and databases.

It also provides a central hub for user authentication and authorization, allowing users to easily log in to multiple applications and websites with one set of credentials.

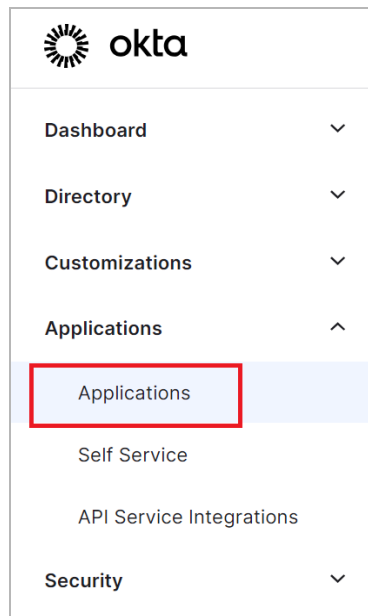
It is used by thousands of organizations worldwide, including major corporations and governmental agencies.



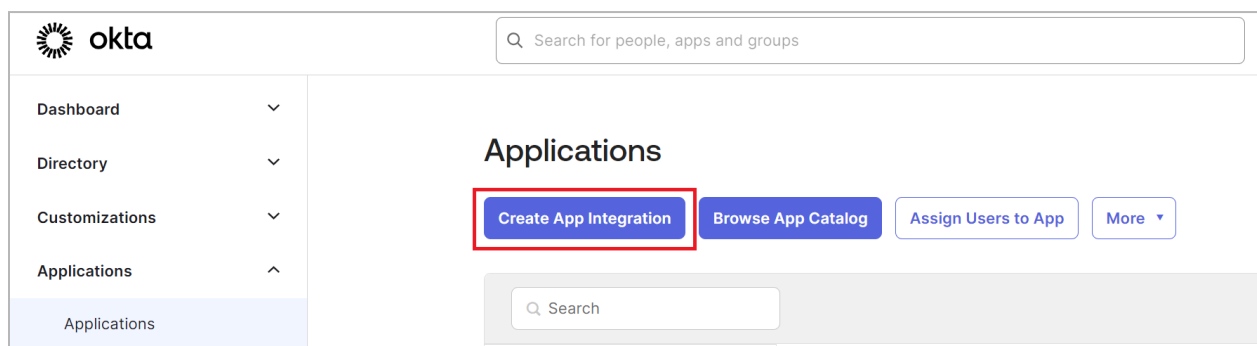
# Create OIDC app integrations using OKTA

## Task 1: Launch the Wizard

1. Log into your Admin Console, then go to *Applications* > *Applications*.



2. Click *Create App Integration*.



3. For the Sign-in method, select *OIDC - OpenID Connect*.

Create a new app integration ✕

Sign-in method

[Learn More](#)

- OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

[Cancel](#) [Next](#)

4. Choose *Web Application* as the type of app to integrate with Okta.

5. Click *Next*.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**  
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**  
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**  
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#) [Next](#)



## Task 2: Configure initial settings




The App Integration Wizard for OIDC has three sections:

1. In General Settings:
  - **App integration name:** Specify a name for your app integration (e.g., inFlow)
  - **Logo:** Add a logo to accompany your app integration in the Okta org. The logo file must be in .png, .jpg, or .gif format and be smaller than 1 MB.
  - **Grant type:** Select *Authorization Code* (it'll be selected by default)

**New Web App Integration**

**General Settings**

**App integration name**

**Logo (Optional)**   

**Proof of possession**  Require Demonstrating Proof of Possession (DPoP) header in token requests

**Grant type**


Client acting on behalf of itself

Client Credentials

Core grants

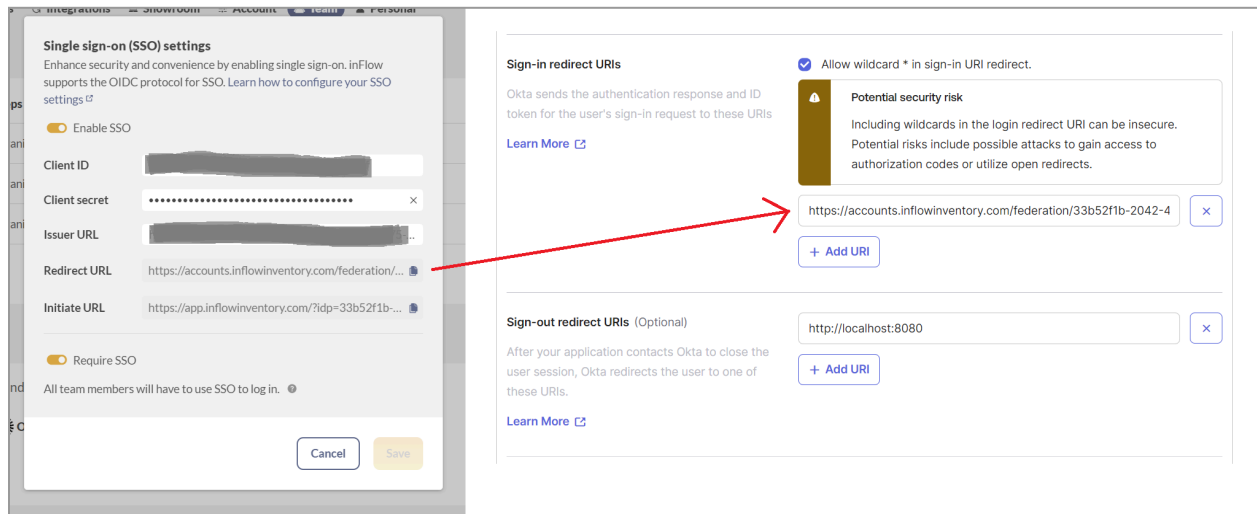
Authorization Code

Refresh Token

[Advanced](#) 



- **Sign-in redirect URIs:** Copy the Redirect URL from inFlow SSO settings and paste it into the input field. For complete steps on setting up [inFlow's single sign-on settings, take a look at this guide](#).



- **Assignments:** Choose the options appropriate to your organization.
- Save the settings.

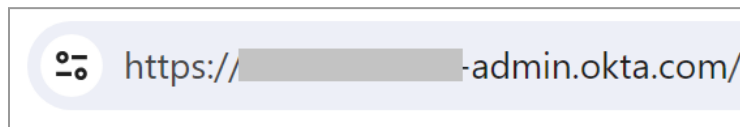


## Task 3: Set up SSO settings inFlow

1. Copy the *Client ID* and *Client Secret* from the Okta configuration settings and paste them into inFlow's SSO settings.

The screenshot shows two panels from the Okta management console. The left panel, titled 'Client Credentials', shows the 'Client ID' field with a copy icon and a 'Generate new secret' button. Below it is a table of 'CLIENT SECRETS' with columns for 'Creation date', 'Secret', and 'Status'. The right panel, titled 'Single sign-on (SSO) settings', shows the 'Enable SSO' toggle checked, and fields for 'Client ID', 'Client secret', 'Issuer URL', 'Redirect URL', and 'Initiate URL'. Red arrows point from the 'Client ID' and 'Client secret' fields in the left panel to the corresponding fields in the right panel.

2. Copy the Okta URL in the Issuer URL in the inFlow SSO settings.



3. Save the inFlow SSO settings.





# GOOGLE

[Google provides a single sign-on \(SSO\)](#) feature that lets you authenticate users via external identity providers (IdP).

For example, you can allow users in an organization to sign into their Google-based email with the same username and password they use to access the corporate network.

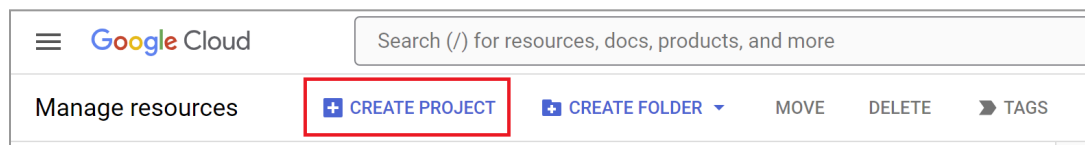
Google offers SSO for Cloud Identity and Google Workspace accounts. After enabling SSO, users no longer need to enter a password when attempting to access Google services and apps. Instead, the SSO functionality redirects users to an external identity provider (IdP) for authentication.

It facilitates a better user experience, enabling using existing credentials to authenticate.



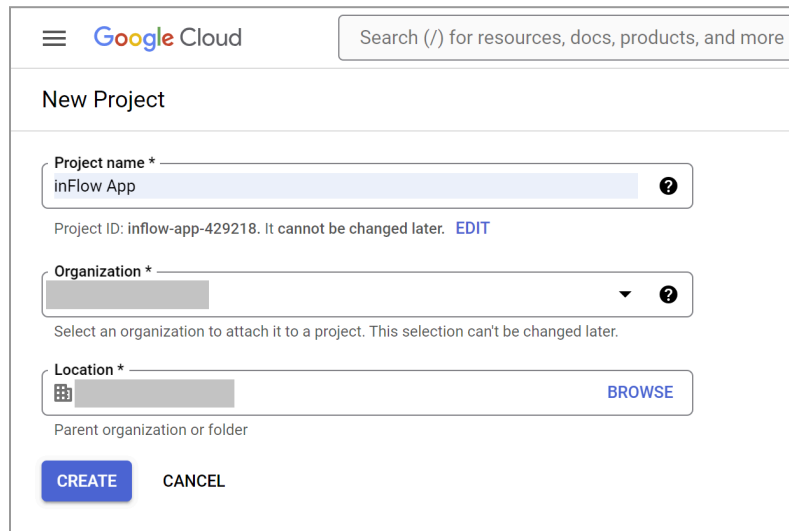
# Create OIDC app integrations using Google

1. Login into Google's cloud resource manager from:  
<https://console.cloud.google.com/cloud-resource-manager>
  - a. If you are new to Google Cloud and have not created a project yet, the organization resource will be created for you when you log in to the Google Cloud console and accept the terms and conditions.
  - b. If you are an existing Google Cloud user, the organization resource will be created for you when you create a new project or billing account. Any projects you created previously will be listed under "No organization," and this is normal. The organization resource will appear, and the new project you created will be linked to it automatically.
2. Click on *Create project* from the menu or create one under the existing folder/project if it already exists.



3. Fill in the project details and click *Save*.

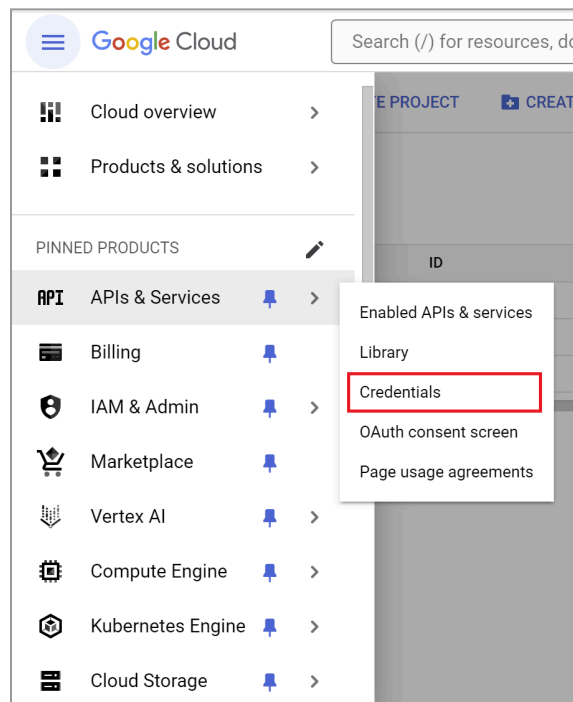
- a. Fill out the *Project name* field (e.g., "inFlow App.")
- b. Below, enter your organization resource as the organization.
- c. Select your organization resource as the parent folder.
  - i. If not created automatically, create a parent folder based on your organization's resource.



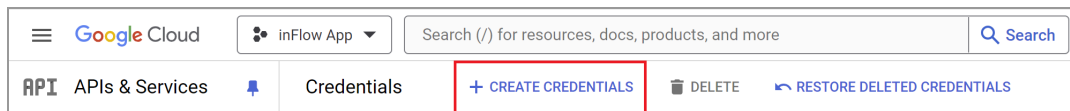
The screenshot shows the 'New Project' form in the Google Cloud console. At the top, there is a search bar with the text 'Search (/) for resources, docs, products, and more'. Below the search bar, the title 'New Project' is displayed. The form contains three main sections: 1. 'Project name \*' with a text input field containing 'inFlow App' and a help icon. Below this field, the text 'Project ID: inflow-app-429218. It cannot be changed later. EDIT' is shown. 2. 'Organization \*' with a dropdown menu and a help icon. Below this field, the text 'Select an organization to attach it to a project. This selection can't be changed later.' is shown. 3. 'Location \*' with a dropdown menu and a 'BROWSE' button. Below this field, the text 'Parent organization or folder' is shown. At the bottom of the form, there are two buttons: 'CREATE' and 'CANCEL'.



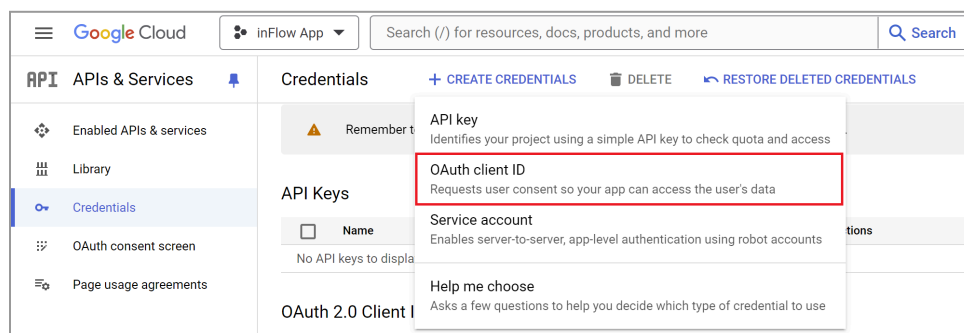
- Go to Google Cloud menu > *API & services* > *Credentials*.
- Select the project created in Step #3.



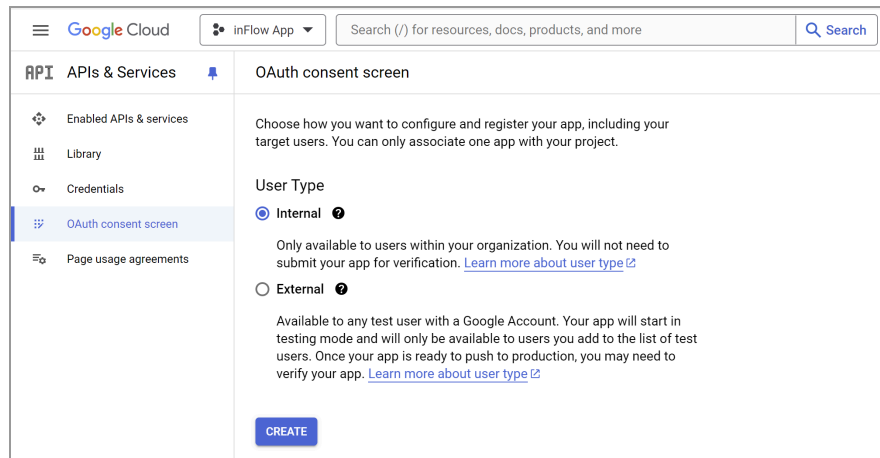
- Click on *Create Credentials* from the menu.



- Select *OAuth Client ID* from the Credentials options.



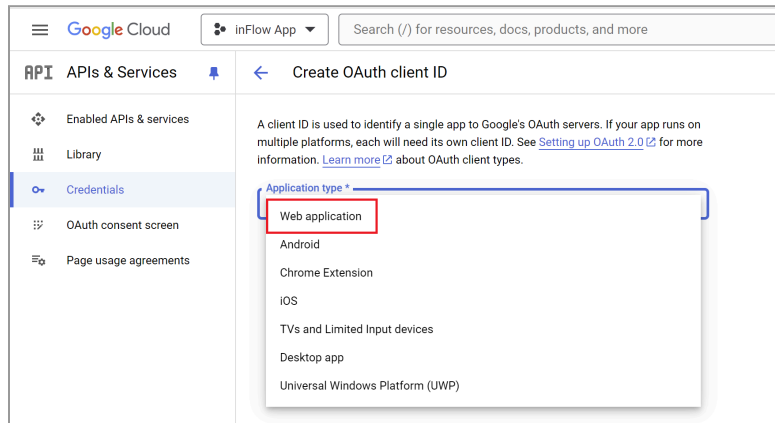
- a. You might need to set up the OAuth Consent if one has not been created previously.



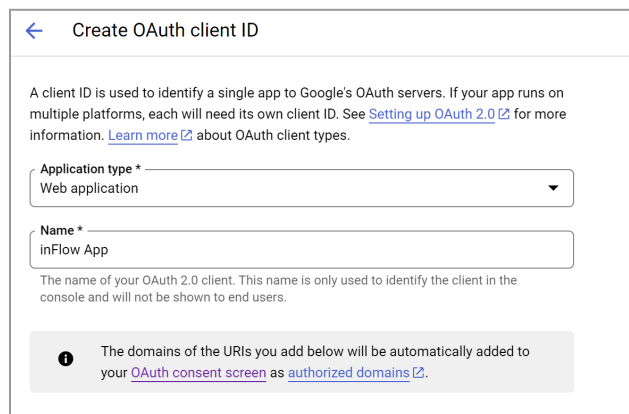
- b. Add the API scopes if needed.
- c. Add the App name and enter the required email credentials for contact purposes.



8. For application type, select *Web application*.



9. In the *Application type* field, enter the application name.



10. Under *Authorized redirect URIs*, click *Add URI*. Copy the Redirect URL from [inFlow SSO settings](#) and paste it into the input field.

**Single sign-on (SSO) settings**  
Enhance security and convenience by enabling single sign-on. inFlow supports the OIDC protocol for SSO. Learn how to configure your SSO settings

Enable SSO

Client ID

Client secret

Issuer URL

Redirect URL

Initiate URL

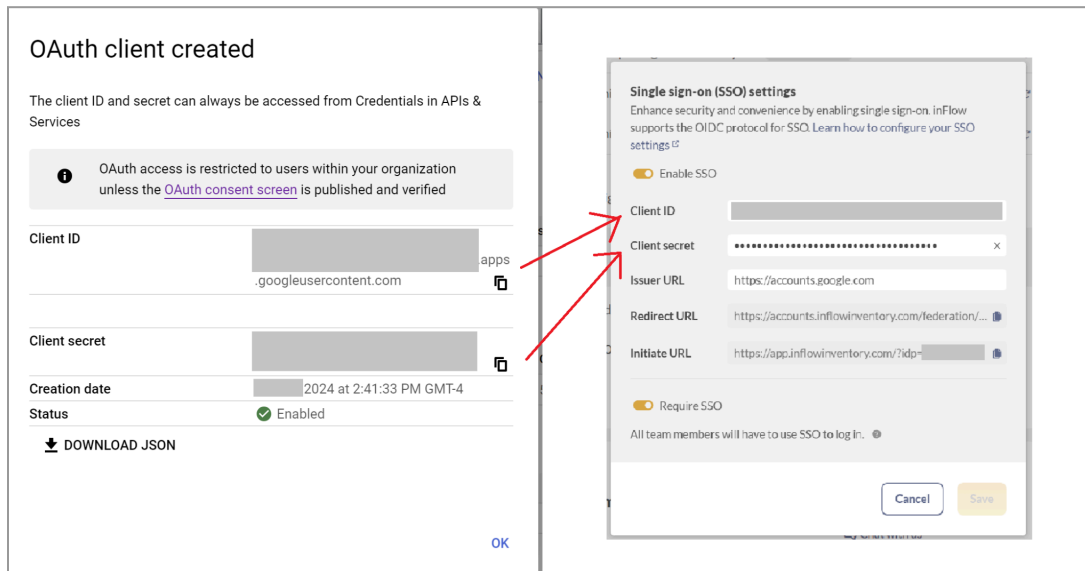
Require SSO  
All team members will have to use SSO to log in.

**Authorized redirect URIs** ⓘ  
For use with requests from a web server

URIs 1 \*



11. Copy and paste the Client ID and Client secret in inFlow SSO settings and set up SSO in inFlow.
12. Add the Issuer URL in inFlow SSO settings as <https://accounts.google.com>
13. Save the Settings





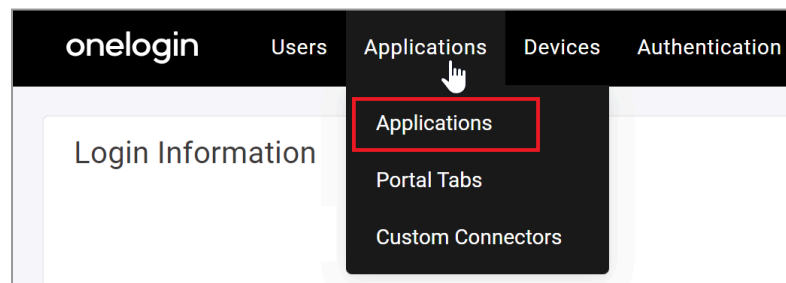
# ONELOGIN

[OneLogin gives users the ability to access the applications](#) and other resources they need to do their job by logging in once to a single interface.

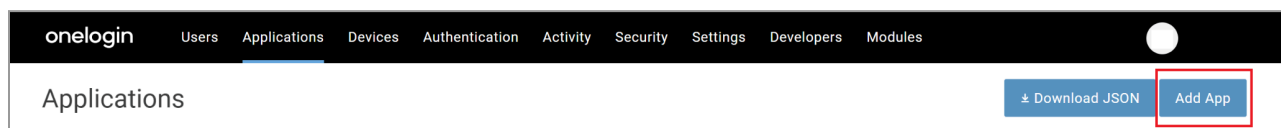
Platforms like OneLogin are known as Identity and Access Management (IAM) solutions that are primarily used to provide their users with a Single Sign-on (SSO) experience.

## Create OIDC app integrations using One Login

1. Log in to your OneLogin account.
2. Navigate to the Administration panel, then click on *Applications*.



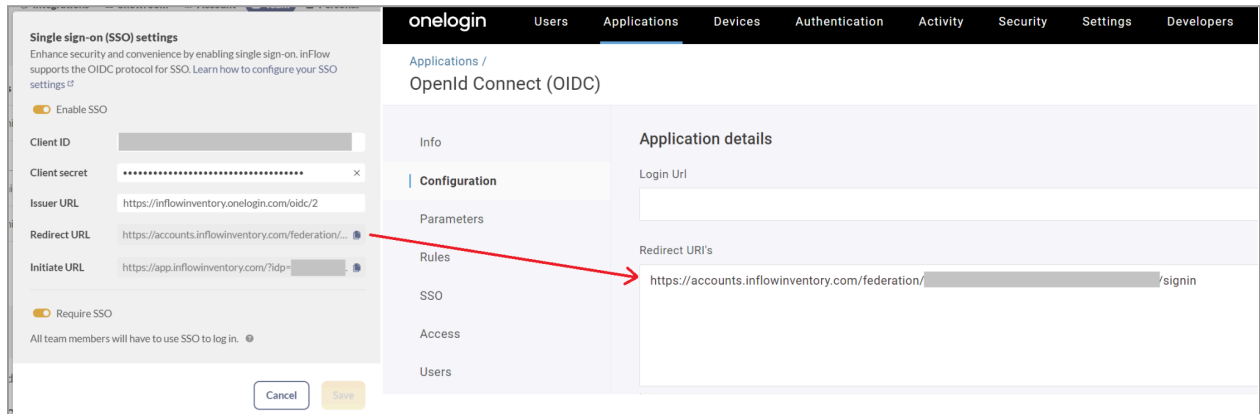
3. Click *Add App*.



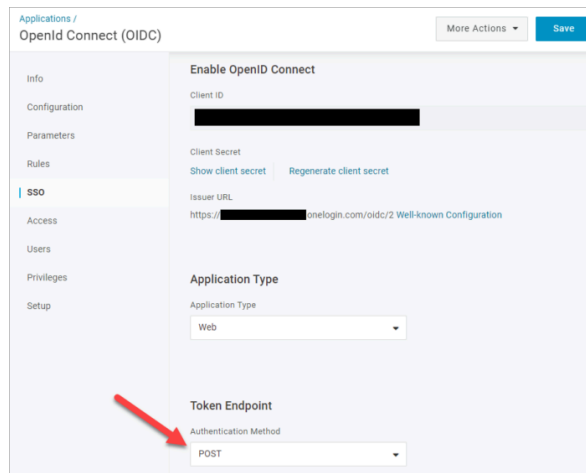
4. Search for *OIDC*.
5. Click on *OpenId Connect (OIDC) by OneLogin, Inc.*



6. For Display Name, enter *inFlow Inventory* and click *Save*.
7. To the left, select *Configuration*.
8. Under *Redirect URIs*, click *Add URI*.
9. Copy the Redirect URL from [inFlow SSO settings](#) and paste it into the input field.

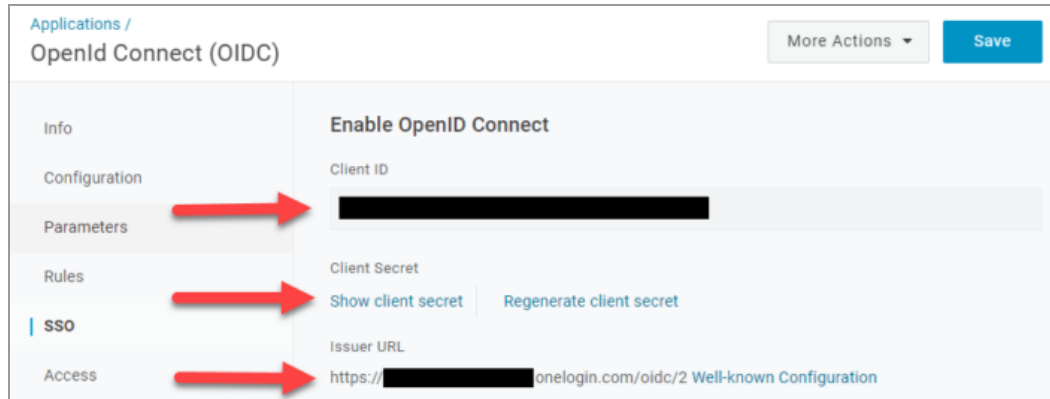


10. In inFlow, click *Save*.
11. In OneLogin, go to the menu and change the *Token Endpoint Authentication Method* to *POST*.
12. Click *Save*.



13. On the same page, copy and save the following information to add to inFlow's SSO settings.

- Client ID
- Client Secret
- Issuer URL



14. Go to *Users* from the navigation bar, and edit your users to give them access to the app.



# ENTRA

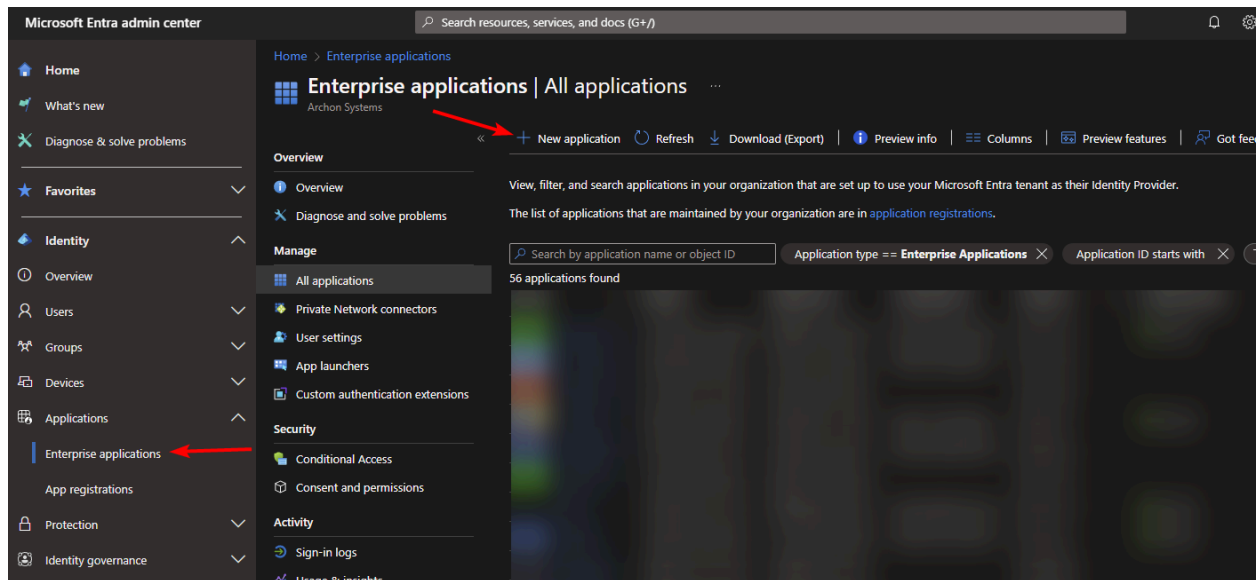
[Microsoft Entra, formally known as Azure AD](#), is Microsoft's cloud-based identity and access management service. Microsoft Entra Single Sign-On (SSO), a feature within the Microsoft Entra ID platform, is the primary SSO solution offered by Microsoft.

It is a user authentication service that permits a user to use one set of login credentials and access multiple applications.

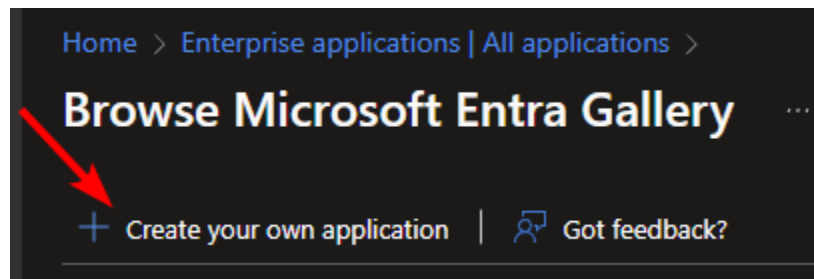


# Create OIDC app integrations using Entra

1. Navigate to [Enterprise applications](#) in the Entra admin center.
2. Click *New Application*.



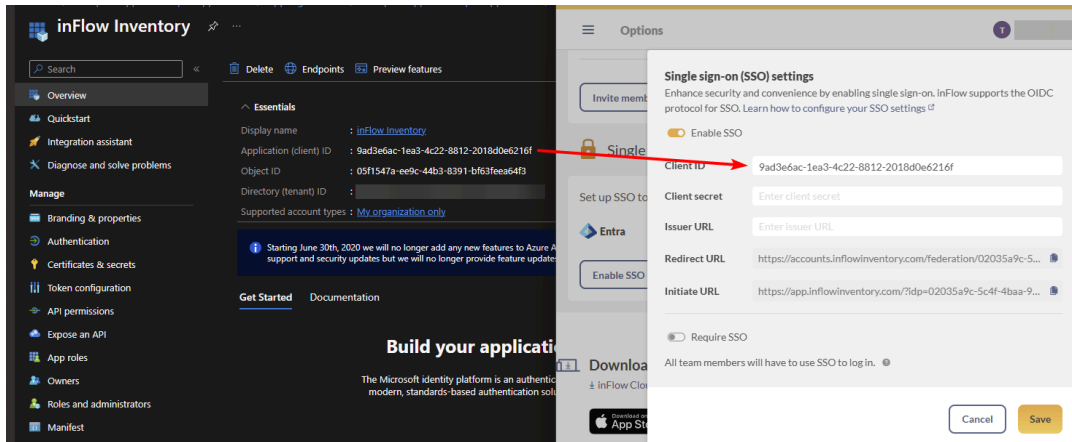
3. Select *Create your own application*.



4. Navigate to [App registrations](#) in the Entra admin center, search for the application you just created by name, and select it.

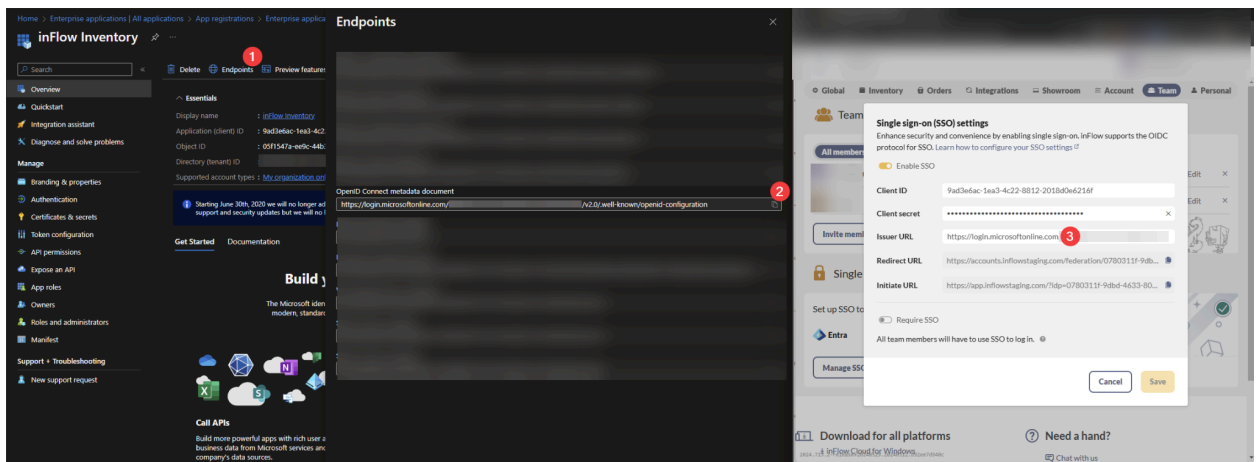


5. Copy the *Application (client) ID* into [inFlow's Client ID](#) field.

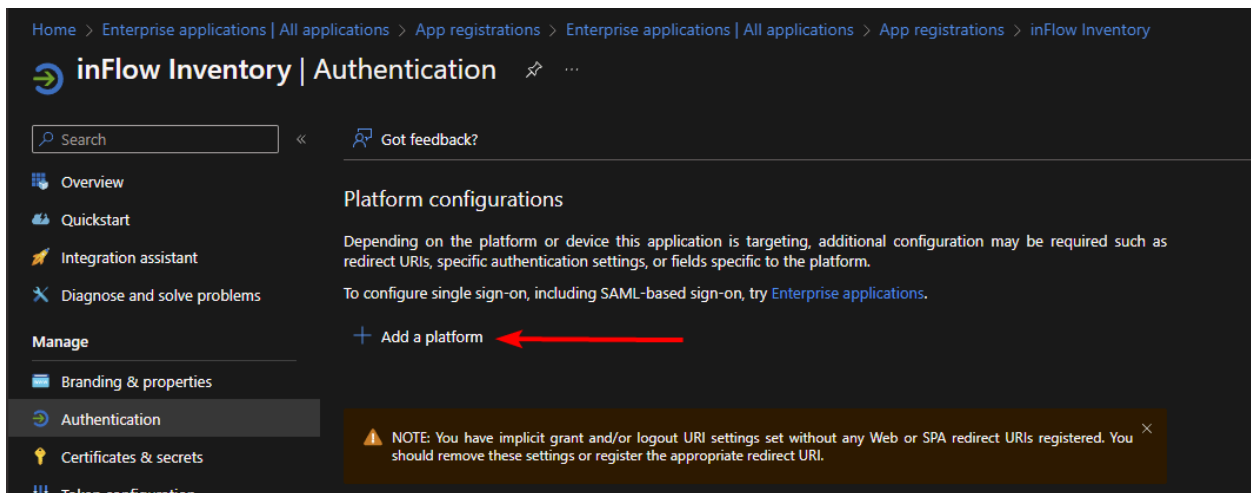


6. Click the "Endpoints" button.

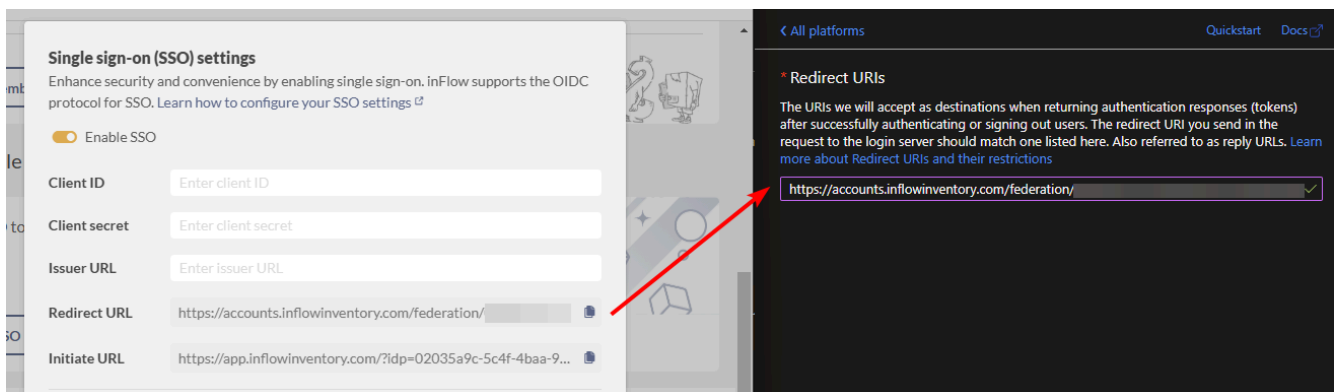
7. Copy the *OpenID Connect metadata document URL* into inFlow's *Issuer URL* field.



8. From the menu on the left, select Authentication. Under *Platform configurations* select *+Add a platform*.



9. Click *Web* and input the *Redirect URI* from inFlow's SSO settings, then click the *Configure* button below.



10. Go to *Certificates & secrets* and click *New client secret*.
  - a. Enter a helpful name.
  - b. Set the expiry date according to your organization's policies.
  - c. Click "Add."
11. Copy the generated secret value into inFlow's *client secret* field.
12. The setup in inFlow is complete. To complete the setup in Entra, [adjust the assignment](#) to meet your business requirements.
  - a. We suggest disabling the required assignment, as only users you invite to inFlow will be able to log in with SSO.





# ADFS Configuration

Note: We cannot guarantee the accuracy of this configuration as it involves a third-party product.

1. In AD FS, open the Server Manager.
2. In the menu to the right, select *Tools > AD FS Management*.
3. In the AD FS management pane, select *Application Groups > Actions > Add an Application Group*.
4. Select *Server Application*. Enter a name and description. Click *Next*.
5. Under *Server Application*, there is a client ID. Note it down.
6. Enter the Redirect URI: Copy the Redirect URL from inFlow SSO settings and paste it here. [See how to set up SSO in inFlow here](#).
7. Click *Next*.
8. Select *Generate a shared secret*. A secret key is generated. Note it down.  
A summary of your settings is displayed. Click *Next* and complete the steps for adding the application group.
9. Open the created application group.  
The *Properties* window appears.
10. Click *Add application*.  
A new window appears: *Add a new application to 'inFlow App'*.
11. Select *Web API* template. Click *Next*.
12. Optionally, edit the *Web API* name.
13. Under *Identifier*, add the client ID that you noted down when creating the server application in this application group. Click **Next**.
14. Under *Apply Access Control Policy*, select the appropriate option and click *Next*.



15. Under *Configure Application Permissions* > *Client application*, the server application is selected. Keep this unchanged. Under *Permitted scopes*, select *allatclaims*, *email*, *openid*, and *profile*. Click *Next*.
16. A summary of your settings is shown. Click *Next* to complete the steps for adding the Web API.
17. Open *Web API* > *Issuance Transform Rules*.
18. Click *Add Rule*. Enter a name for the rule, select *Active Directory for Attribute store*, and then add "*E-Mail Addresses*" – "*E-Mail Address*". Save your changes.
19. Navigate to *Relying Party Trusts* in the *ADFS Management* tool.
20. Make sure you have the following relying party trust. *Identifier* should be *https://<ADFShostname>/adfs/services/trust*.
21. If the relying party trust is not available, you need to add a new one. Follow the steps described in <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-relying-party-trust#to-create-a-claims-aware-relying-party-trust-manually>, but skip the steps *Configure certificate* and *Configure URL*.
22. Make sure you add the email address for users who will be using the inFlow app through ADFS authentication.
  - a. Open *Active Directory Users and Computers* on the AD server.
  - b. Navigate to the *Users* folder, right-click the user, and select *Properties*.
  - c. Under *General*, enter the user's email address in the *E-mail* field.
  - d. Click *OK* to save the changes.



# Configure inFlow SSO settings

Follow the instructions [in this article to set up SSO in inFlow.](#)

1. Copy and paste the Client ID from Step #5.
2. Copy and paste the Client secret from Step #8.
3. Copy and paste the Issuer URL from Step #20.
4. Save the SSO settings.

