

FlowDoc Installation & Configuration Guide

Initial Installation Steps

Please follow the steps below to start using the FlowDoc App:

1. Select the user type for whom you want to install the app.
2. Acknowledge the agreement by clicking the checkbox.
3. Click on the Install button.

**Install FlowDoc**
By ChazeCloud Services Pvt. Ltd.


☒ **Install for Admins Only**


☐ **Install for All Users**


☐ **Install for Specific Profiles...**

☒ I acknowledge that I'm installing a Non-Salesforce Application that is not authorized for distribution as part of Salesforce's AppExchange Partner Program.

Install

Cancel

App Name	Publisher	Version Name	Version Number
FlowDoc	ChazeCloud Services Pvt. Ltd.	ver 0.1	1.0

Additional Details

[View Components](#)

Once the installation is completed, click on Done.

**Install FlowDoc**
By ChazeCloud Services Pvt. Ltd.

 **Installation Complete!**

Done

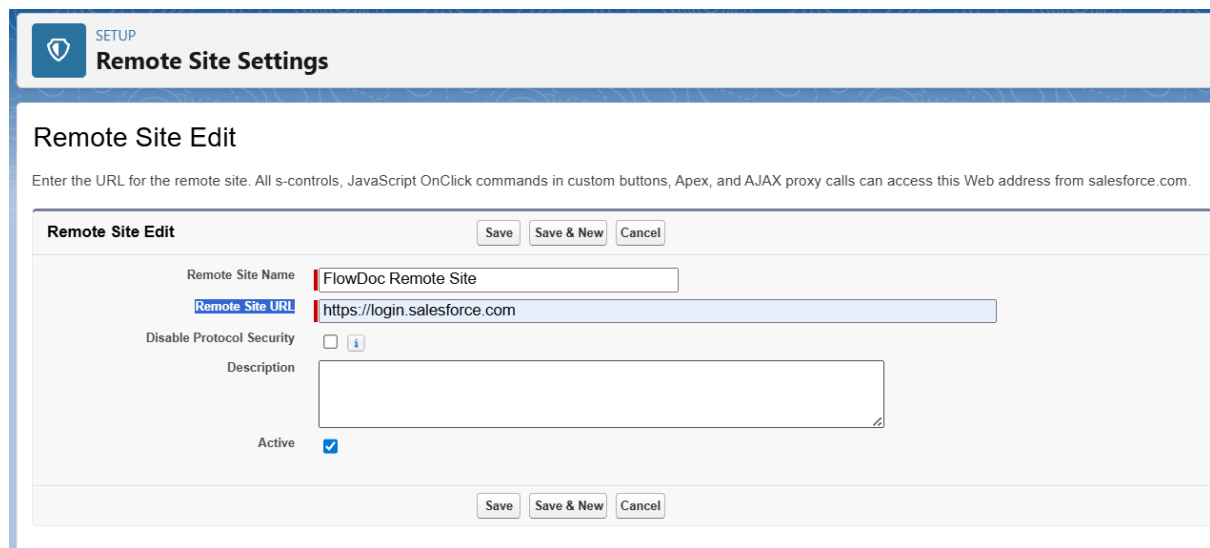
App Name	Publisher	Version Name	Version Number
FlowDoc	ChazeCloud Services Pvt. Ltd.	ver 0.1	1.0

Post-Installation Configuration

Once FlowDoc is installed in your org, configure the following settings:

1. Set the Remote Site Setting

- Go to Setup (click on the gear icon).
- In the Quick Find box, type Remote Site Settings.
- Click on New Remote Site.
- Enter the following:
 - Remote Site Name: Your preferred name
 - Remote Site URL: `https://login.salesforce.com`
- Click Save.



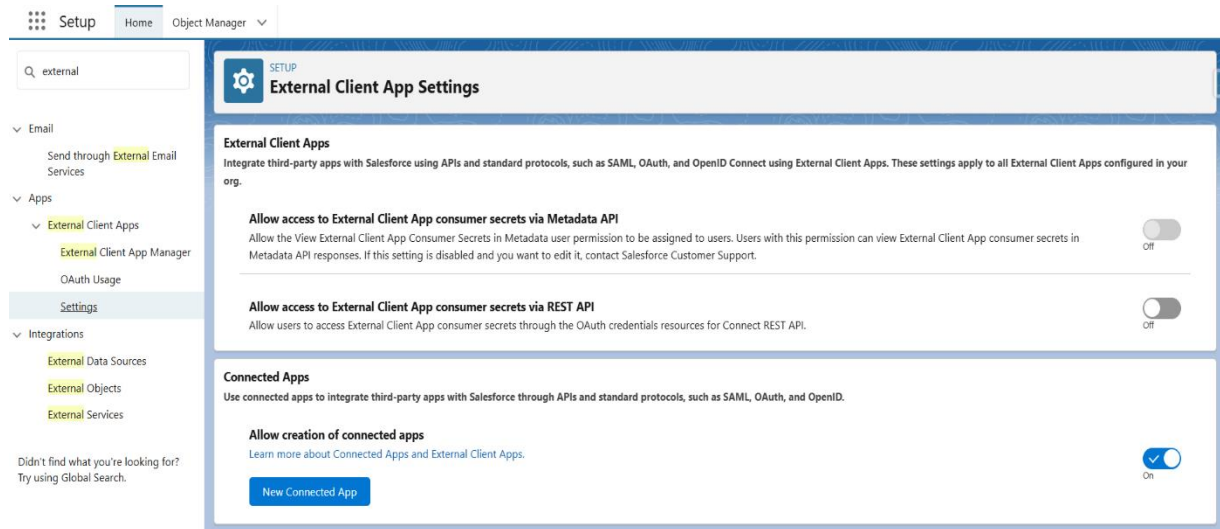
The screenshot shows the 'Remote Site Edit' page in Salesforce Setup. The page header includes the 'SETUP' icon and the title 'Remote Site Settings'. Below the header, the page title 'Remote Site Edit' is displayed, followed by a note: 'Enter the URL for the remote site. All s-controls, JavaScript OnClick commands in custom buttons, Apex, and AJAX proxy calls can access this Web address from salesforce.com.' The main form area is titled 'Remote Site Edit' and contains the following fields and controls:

- Remote Site Name:** A text input field containing 'FlowDoc Remote Site'.
- Remote Site URL:** A text input field containing 'https://login.salesforce.com'.
- Disable Protocol Security:** A checkbox that is currently unchecked, with an information icon to its right.
- Description:** A large text area for providing a description of the remote site.
- Active:** A checkbox that is currently checked.

At the bottom of the form, there are three buttons: 'Save', 'Save & New', and 'Cancel'.

2. Create a Connected App

Before creating the Connected App, make sure your org has the required permissions (as shown in the image in the original doc)



Use the Salesforce guide to create the app:

https://help.salesforce.com/s/articleView?id=platform.ev_relay_create_connected_app.htm&type=5

Important values to fill in:

- Selected OAuth Scopes: Full access (full)
- Callback URL: <https://login.salesforce.com>

After creating the Connected App, make sure to note down the:

- Consumer Key
- Consumer Secret

3. Reset Security Token

- Reset your Security Token.
- Note it down once received.

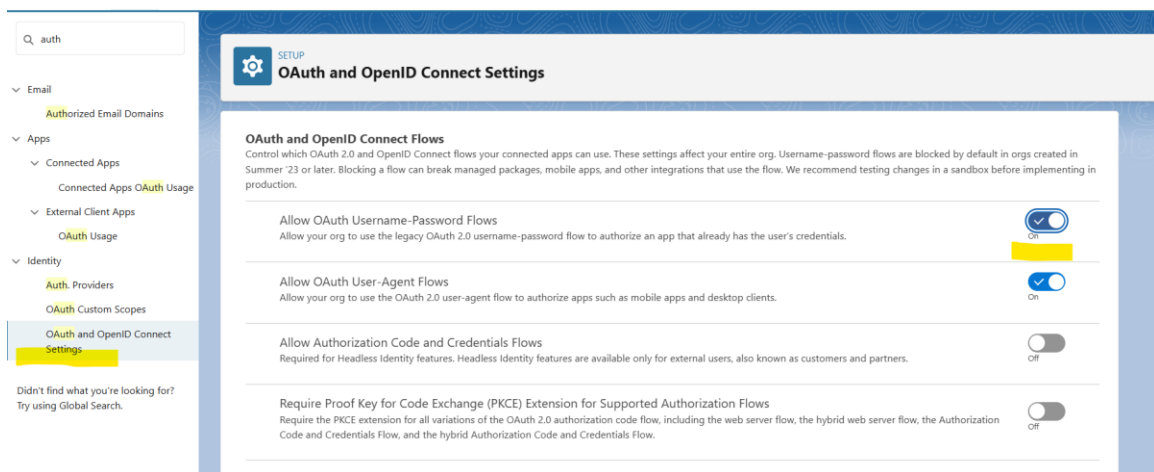
4. Configure the Custom Setting

- Open Custom Settings from the Quick Find box.
- Click on Integration Configuration.
- Click Manage, then click New.
- Fill in the fields as follows:

Field	Value
Name	Flow Metadata
Access Token	(Will be generated automatically)
Client Key	Your Connected App Consumer Key
Client Secret Key	Your Connected App Consumer Secret
Endpoint URL	https://<your-instance>.my.salesforce.com/services/data/v60.0/tooling/subjects/Flow
Password	Your org password
Security Token	Your org security token
Token URL	https://login.salesforce.com/services/oauth2/token
User Name	Your org username

5. Enable OAuth Username-Password

Make sure the OAuth Username-Password flow is enabled (refer to the image in the document).



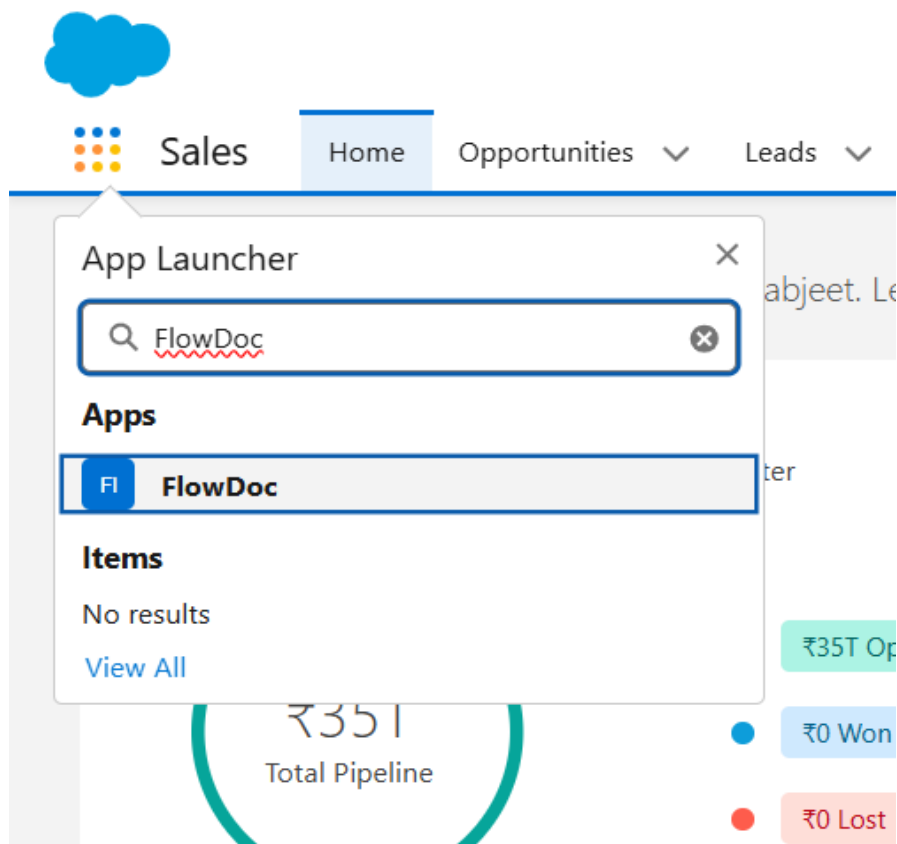
OAuth and OpenID Connect Settings

OAuth and OpenID Connect Flows
Control which OAuth 2.0 and OpenID Connect flows your connected apps can use. These settings affect your entire org. Username-password flows are blocked by default in orgs created in Summer '23 or later. Blocking a flow can break managed packages, mobile apps, and other integrations that use the flow. We recommend testing changes in a sandbox before implementing in production.

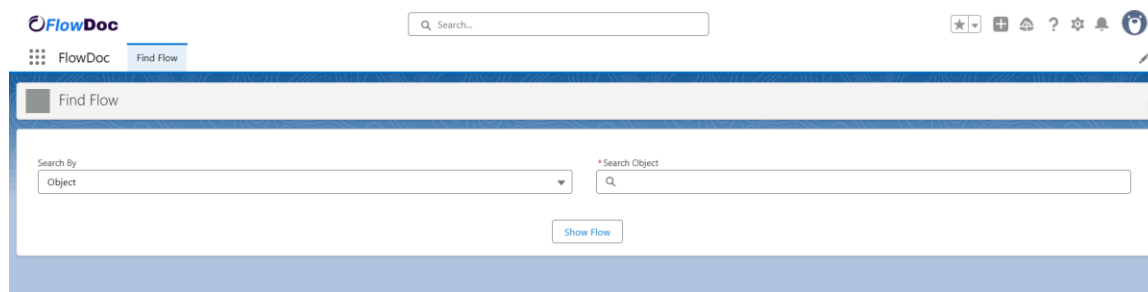
- Allow OAuth Username-Password Flows**
Allow your org to use the legacy OAuth 2.0 username-password flow to authorize an app that already has the user's credentials. **On**
- Allow OAuth User-Agent Flows**
Allow your org to use the OAuth 2.0 user-agent flow to authorize apps such as mobile apps and desktop clients. **On**
- Allow Authorization Code and Credentials Flows**
Required for Headless Identity features. Headless Identity features are available only for external users, also known as customers and partners. **Off**
- Require Proof Key for Code Exchange (PKCE) Extension for Supported Authorization Flows**
Require the PKCE extension for all variations of the OAuth 2.0 authorization code flow, including the web server flow, the hybrid web server flow, the Authorization Code and Credentials Flow, and the hybrid Authorization Code and Credentials Flow. **Off**

6. Launch FlowDoc

- Search for FlowDoc in the App Launcher.
- Click on FlowDoc from the results.



Now you're ready to use FlowDoc!



Note: [Only flows with Package Status = Unmanaged will be listed in the app]