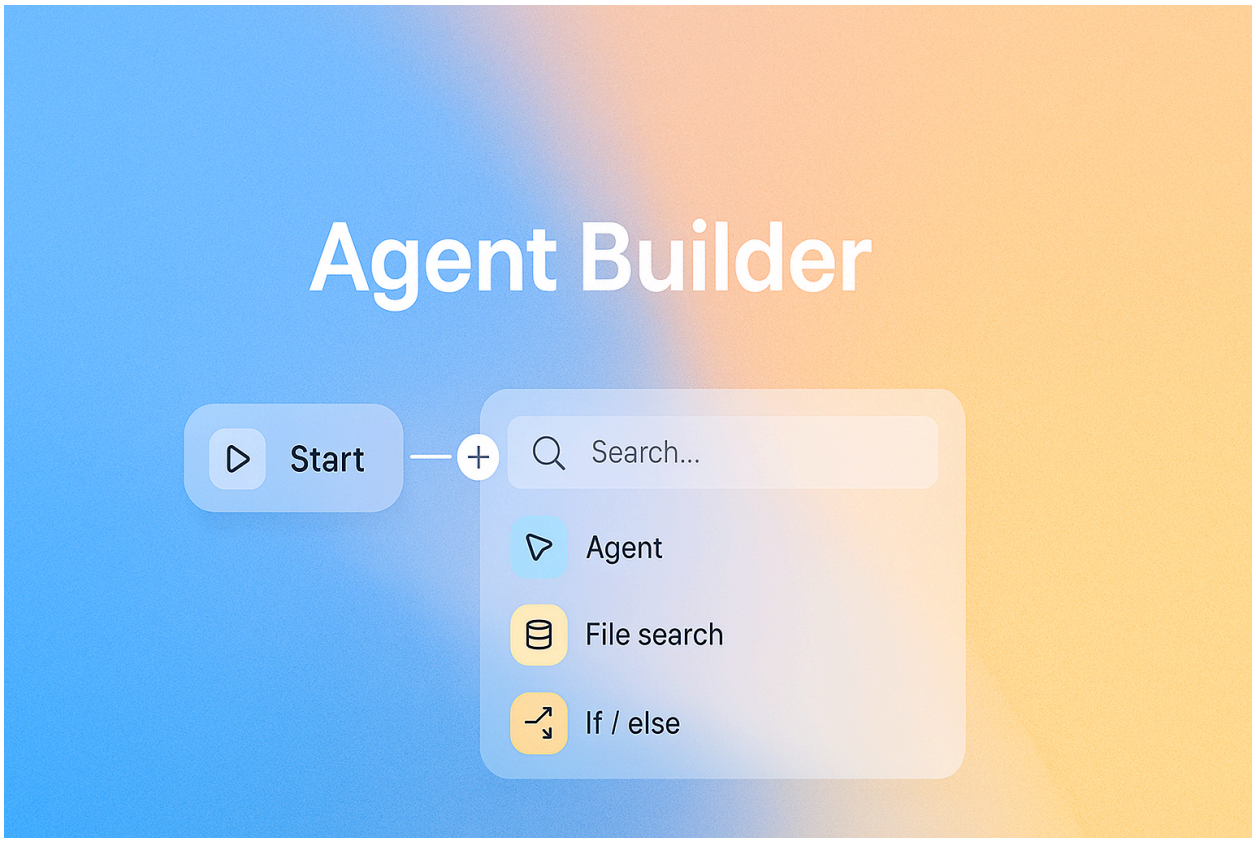


A Beginners Guide to Chat-GPT Agent Builder

By Kazi Islam

Version 1.0

Prepared for Prof David Smith

Date [11-16-2025]

Table of Contents

Introduction

Building with AI can be a fast way to turn ideas into working helpers. No waiting on long dev cycles or complex setup. You can go straight from a problem to a prototype that answers questions, automates steps, and plugs into your docs or tools. And the easiest way to do it is by hopping into ChatGPT Agent Builder.

ChatGPT Agent Builder lets you create and launch custom AI agents without code. You can name your agent, set its tone, add instructions and knowledge (like FAQs or manuals), connect actions/tools, and share it with a simple link or embed. Start in one place and improve as you go—agents can be updated, versioned, and reused across projects.

This guide is meant for absolute beginners or first-time builders who want a clear path from idea to working agent. Take a look below to get started, set up your agent, and learn a few testing and safety tips.

The content is organized as follows:

- What is Agent Builder and how it works
- How to plan and create your first agent
- How to test, fix, and publish your agent

What is Agent Builder and how it works

ChatGPT Agent Builder is a no-code/little-code system for creating AI “helpers” that answer questions, follow your rules, and (optionally) call tools like search or APIs. You can use it for personal projects, classes, or team workflows across websites, forms, and internal docs.
You can start with a single agent and grow to multiple versions as your needs evolve.

It’s so easy. Here’s how it works

1. Create it. Give your agent a name, description, and tone.
2. Teach it. Add Instructions (what to do/how to speak) and Knowledge (your FAQs, PDFs, docs).
3. Power it. Turn on Actions/Tools only if needed (e.g., web, spreadsheets, APIs).
4. Test it. Run sample prompts, check answers, and tighten rules.
5. Ship it. Save a Version, then share a link or embed it on a site/app.

Types of Agents

There are a variety of tasks that can be accomplished by an AI agent. Research, summarization, analyzing data, setting meetings and much more can be done with the agents. Based on the type of tasks these agents can be divided mainly into 4 types. They are-

- **FAQ / Knowledge Agent:** Answers from your docs and policies.
- **Workflow Assistant:** Walks users through steps, forms, or checklists.
- **Data/Reporting Agent:** Summarizes files, generates briefs, or drafts emails.
- **Tool-Powered Automator:** Uses enabled actions (least-privilege) to look up info or trigger tasks.

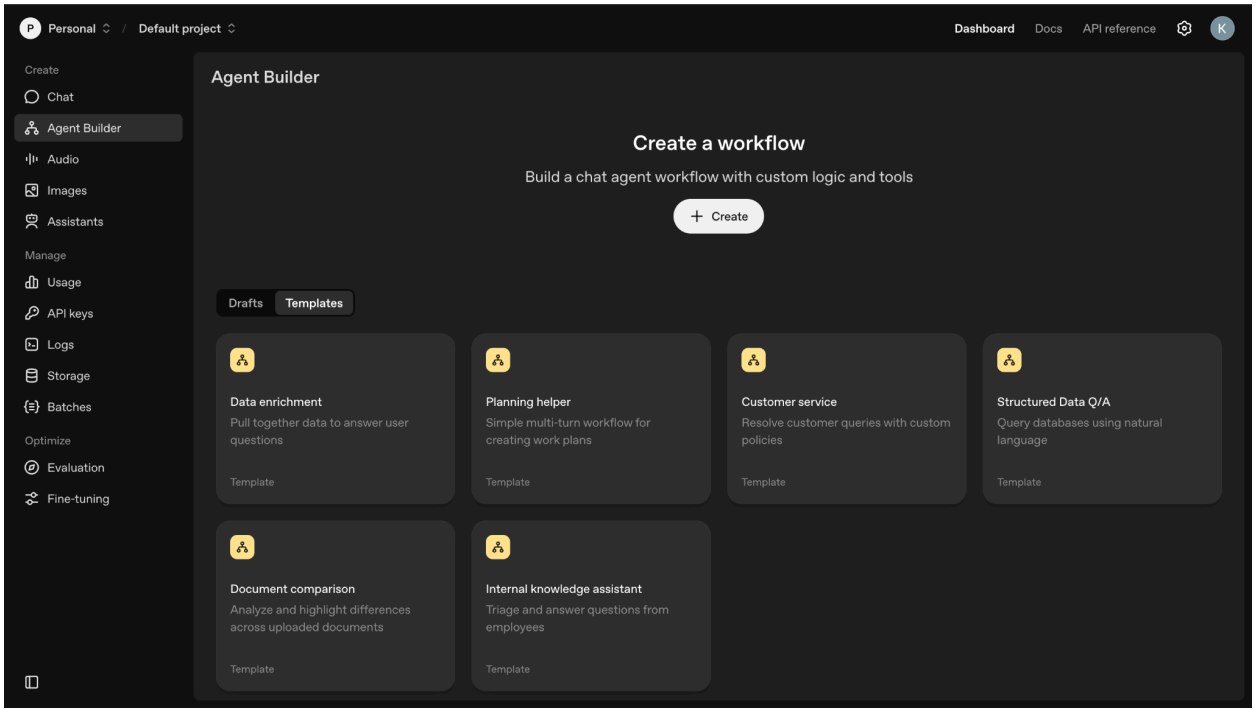
Types of Access (How people use your agent)

People can use your agent in ways described below:

- **Embed in your app/site with ChatKit:** After you Publish your workflow, you will get a workflow ID. You will use ChatKit to wire a chat UI to that workflow in your frontend. This is the primary way to put an agent in front of end users. OpenAI Platform+1

- **Share inside a team/project:** Teammates can collaborate on agents and workflows via ChatGPT Projects and workspace permissions (RBAC). You can use this for internal testing and review but not as a public end-user link. OpenAI Help Center+1

Note: Agent Builder doesn't provide a universal "public share link" widget for end users. You would have to publish your agent before people can use it.



How to plan and create your first agent

Planning the Agent

There are different steps when we plan about the AI agent. These tasks are described below:

Fix the Audience

We would have to fix the audience who will be the primary users of the agent because there are different types of audience such as academic, non-academic, technical, non-technical and more.
We would also have to fix the tone of response for the agent's responses.

Define the Task

We would have to define what the AI agent will be responsible for doing. It can be text summarization, checking the news or something else.

Gather Resources

We would have to gather any files, docs, pictures or any type of data that we want the agent to use as a source of info or instruction base while it will perform its task.

Fix the Guadrails

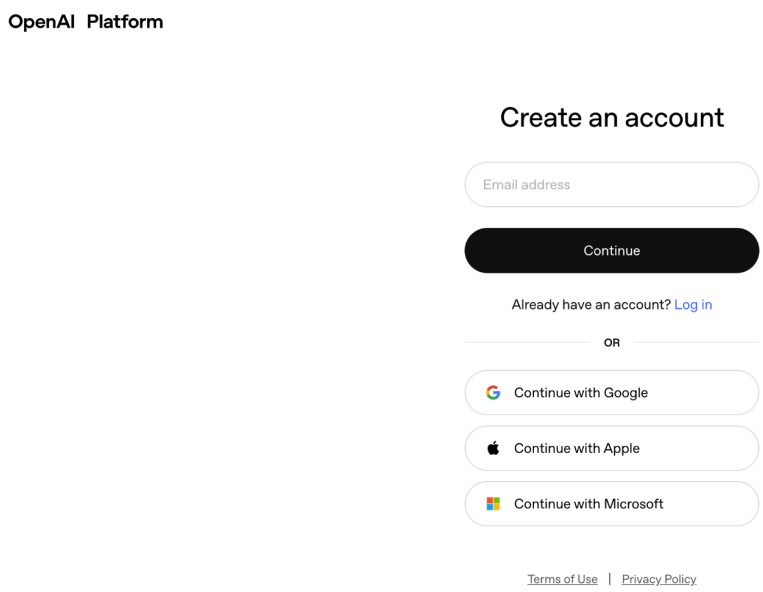
We would have to take note of what type of information we want the agent to accept while someone uses it.
We must make sure the agent rejects out of context sensitive information like Social security number, Bank account Number, Address etc.

Creating the Agent

When we create the agent we would have to follow the steps mentioned below:

Creating an Agent Builder Account

We must create an Open AI agent builder account before we can do anything. We have to go to this [Agent Builder Link] and sign up.

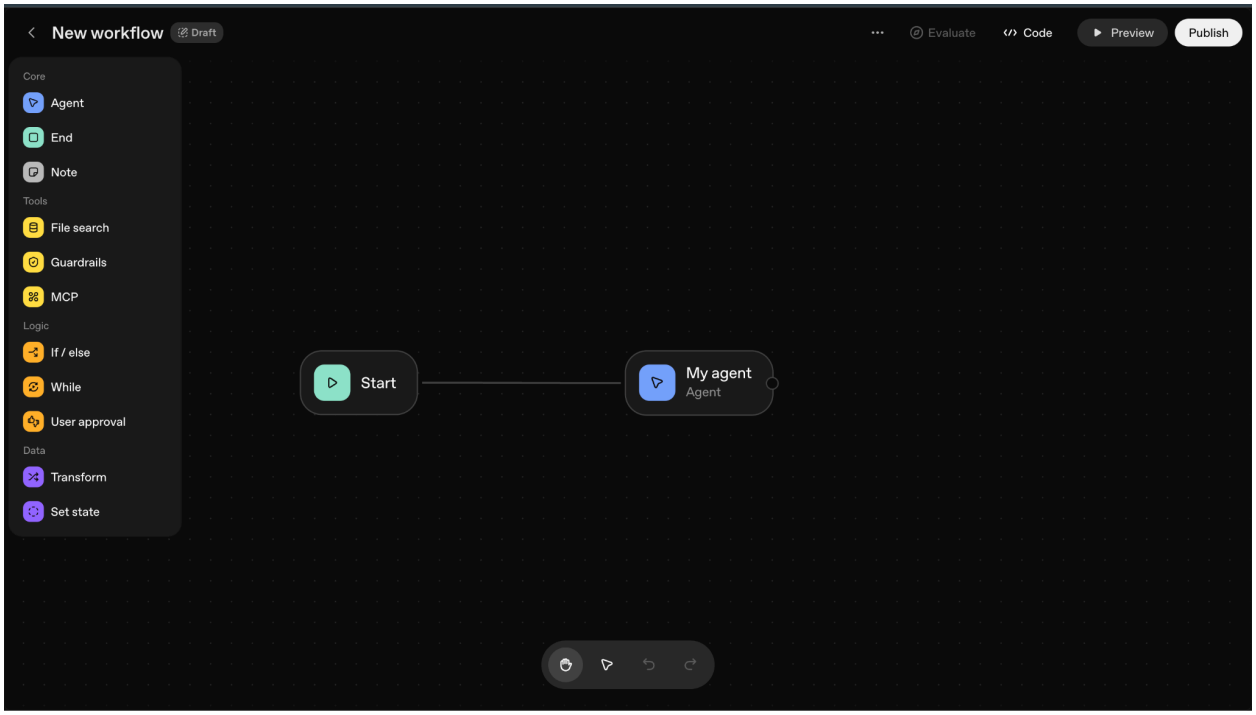


We will see something like this. We can either sign in with one of these three methods or our email address.
After we sign in, it will ask us to provide a picture of our photo ID such as state id (both front and back of the ID). After we provide the picture, it will prompt us to take a face scan where we will scan our face through our camera.

After scanning, our face will be matched with the photo ID's picture. If both pictures match, we will be given authorization as an organization to create agents.

Building the Agent

When we start building the agent, we will see something like this.

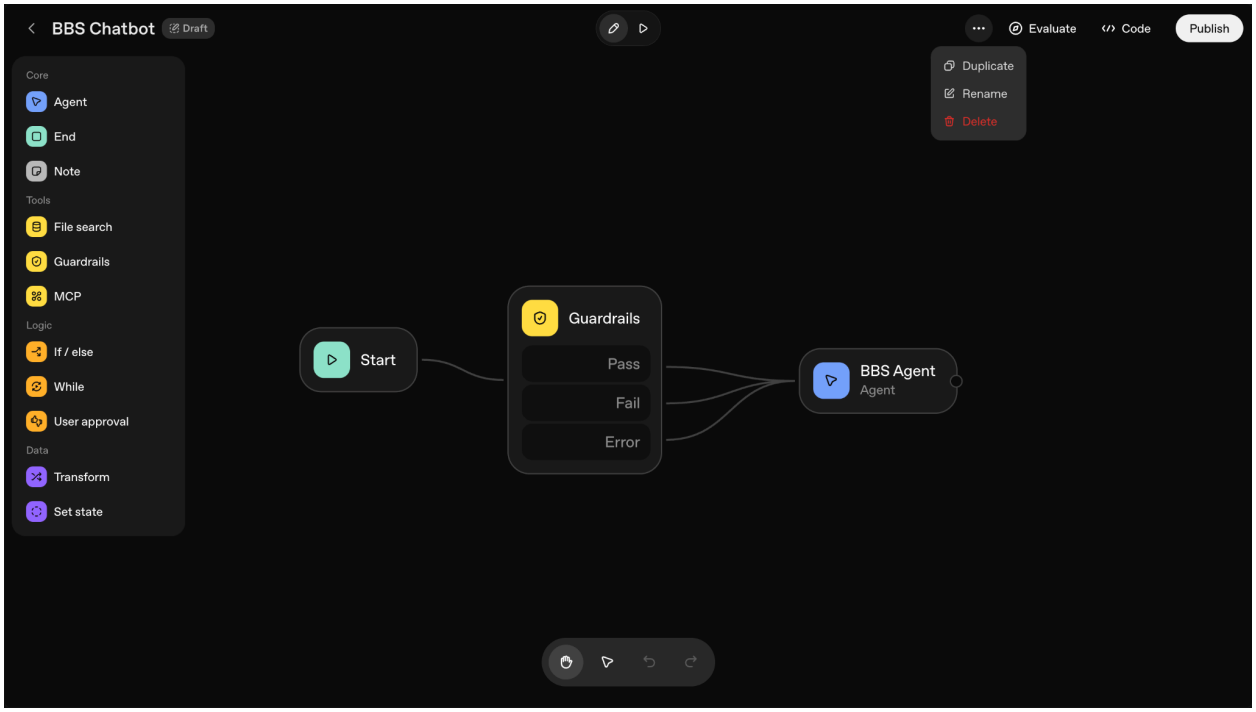


There are different nodes such as Agent, End, Note at the top right Core section.

There are tools such as File Search, Guardrails (Limitations), MCP (different apps that we can connect).

We have a logic bar which can be used to establish logic (Example: In case a user asks about contact info, give the user contact info. Otherwise don't give the user contact info).

There are other functions as well which are not used on a regular basis.

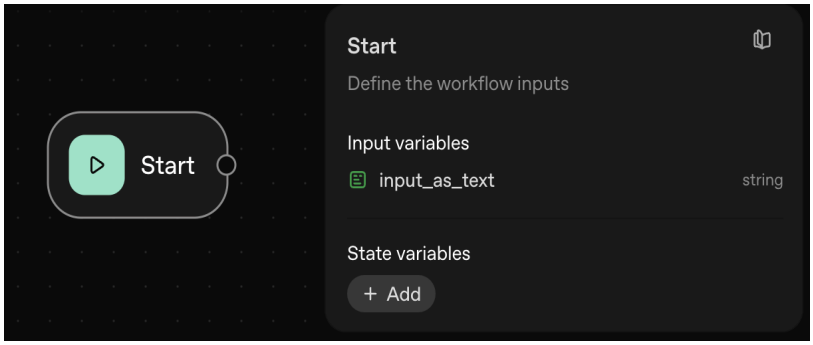


We can rename the agent based on our choice by clicking the three dots at the top. We can copy or delete the agent as well.

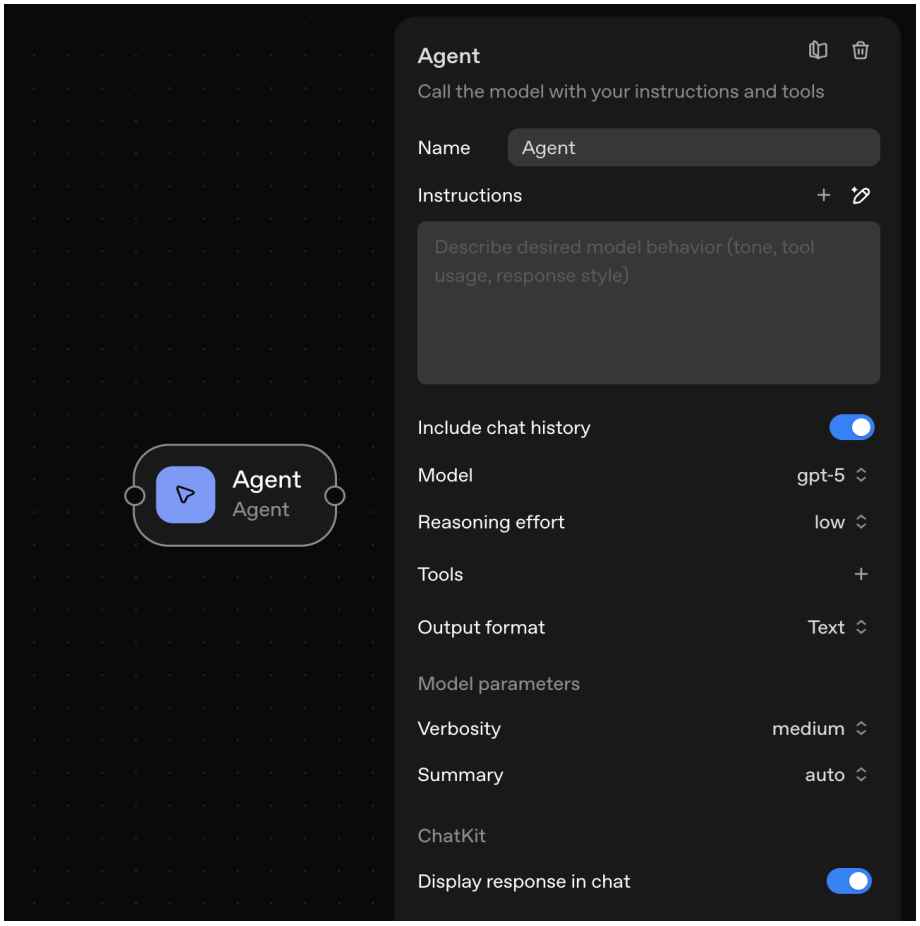
Main Nodes to Consider

We can use nodes as necessary to create an AI agent of our choice. But in order to do so, we need basic knowledge about the main nodes used in all the agents such as-

1. Start Node: This is the beginning of the AI agent. In this agent we can add variables (mathematical operators such as x,y,z that can be assigned a value of our choice). We can also set the data type of the input (letters, numbers etc).

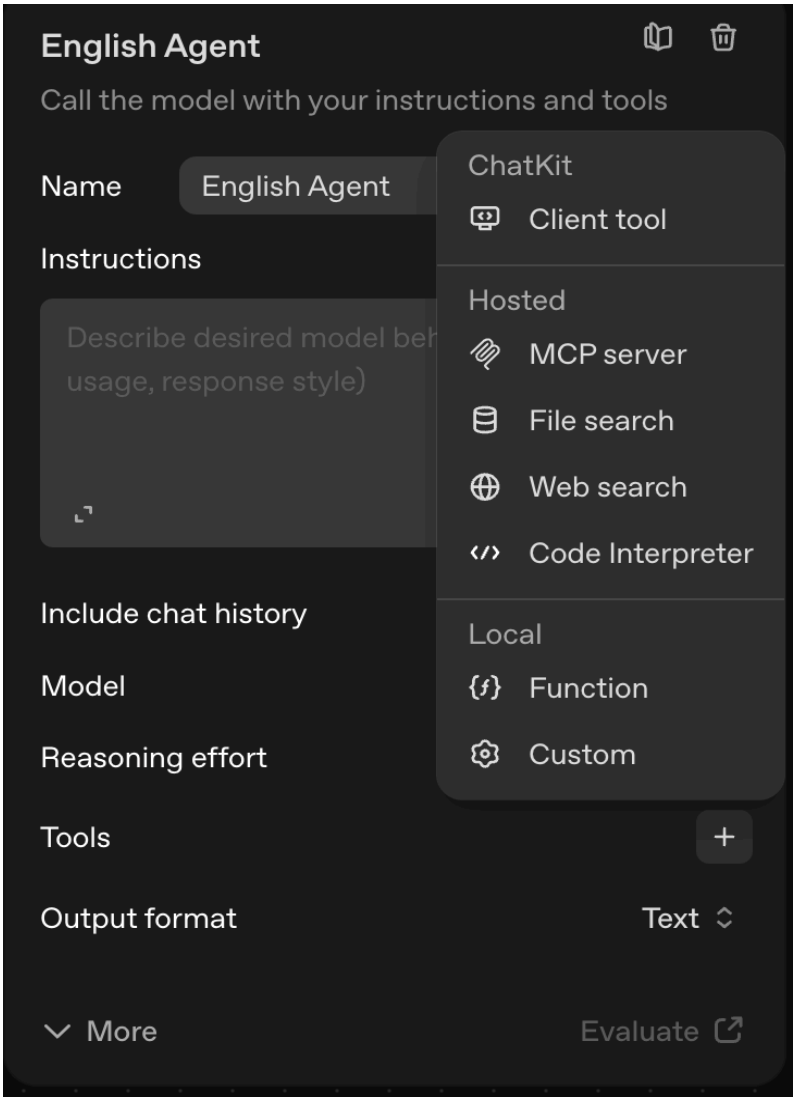


2. Agent Node: The agent node is the heart of any workflow.



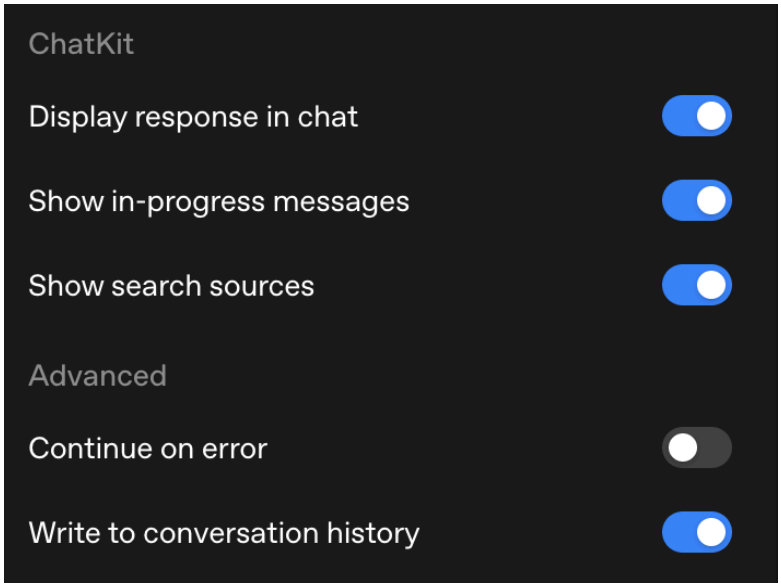
In this node we can give names to the node. Here we have to write instructions for the agent to follow in the instructions section. We can select the AI model that we want to use for the responses.

We can select the reasoning effort (how much the model will think before responding), and the output format. We can add tools as well.

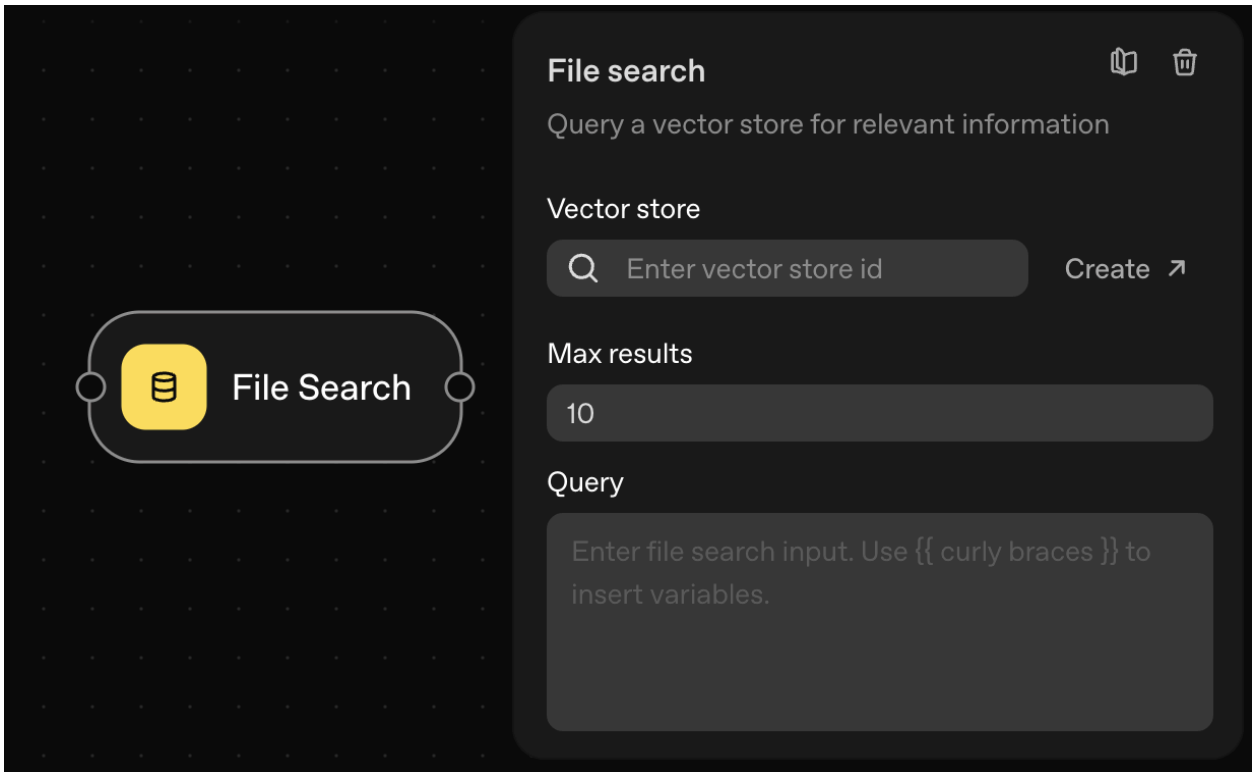


We can use features like search the internet (Web Search), Interpreting Code, searching files that we upload (File Search) and many more.

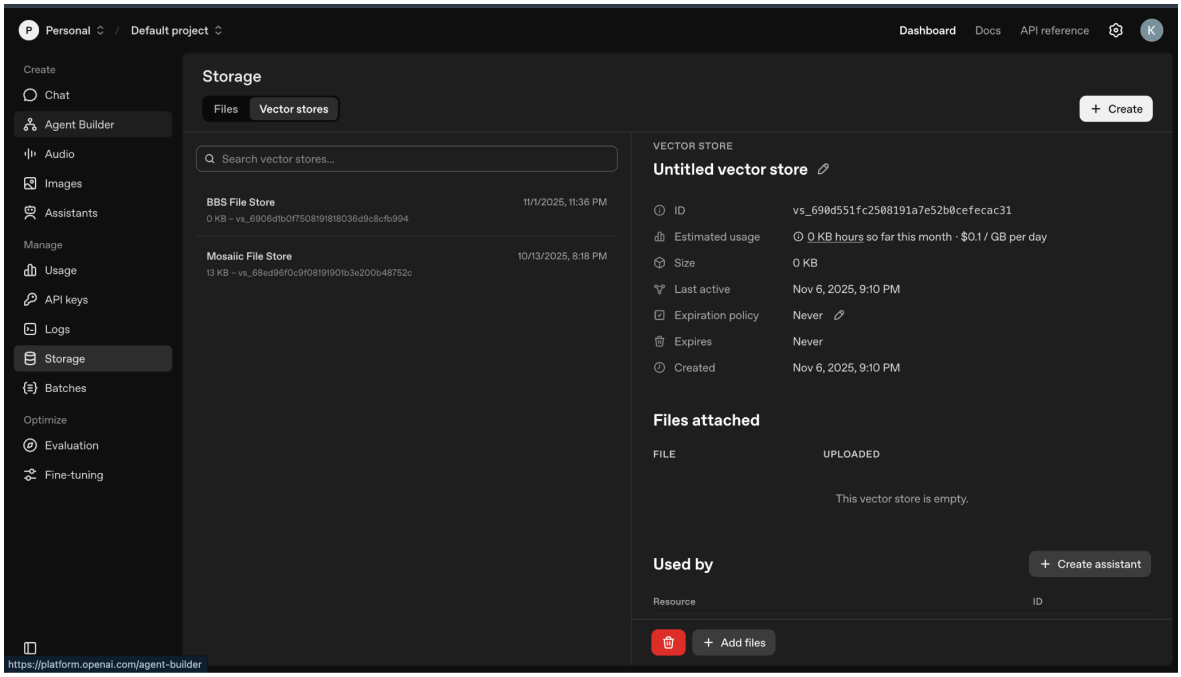
We can also control other chat features displayed below as well.



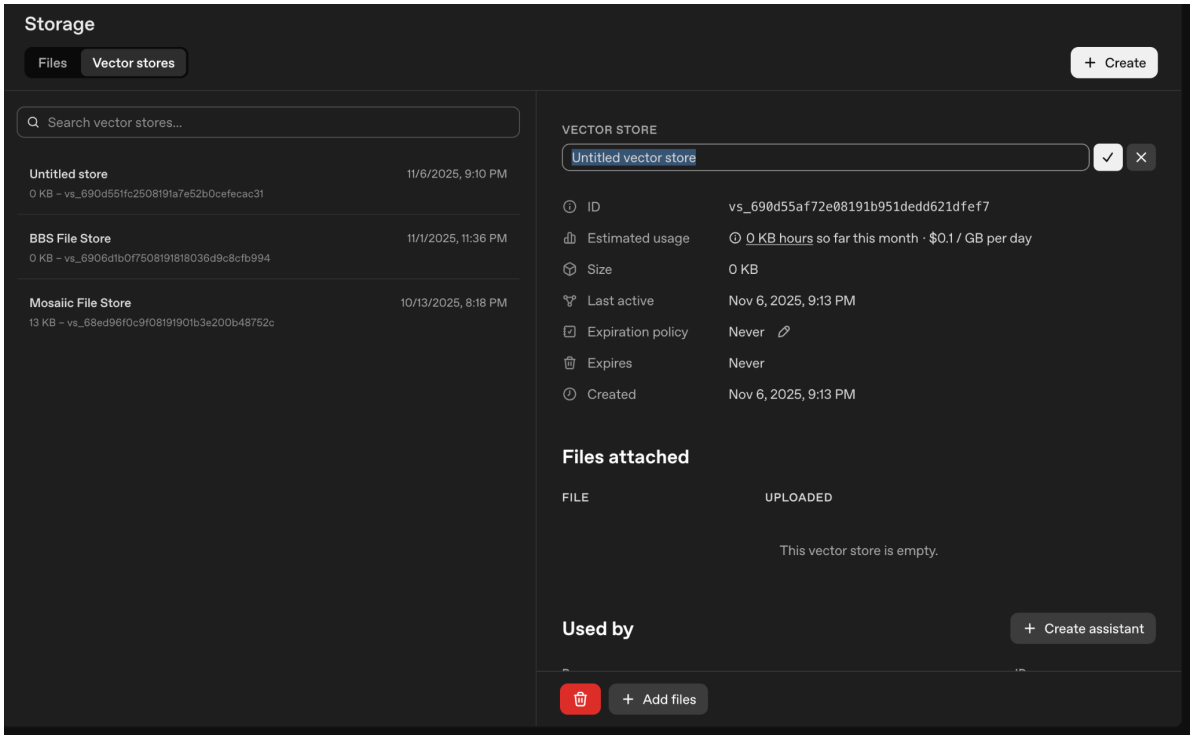
3. File Search: The file search node is the node that will use the resources that we upload in our chat [GPT vector store](#).



If we go to the vector store, we will see something similar.

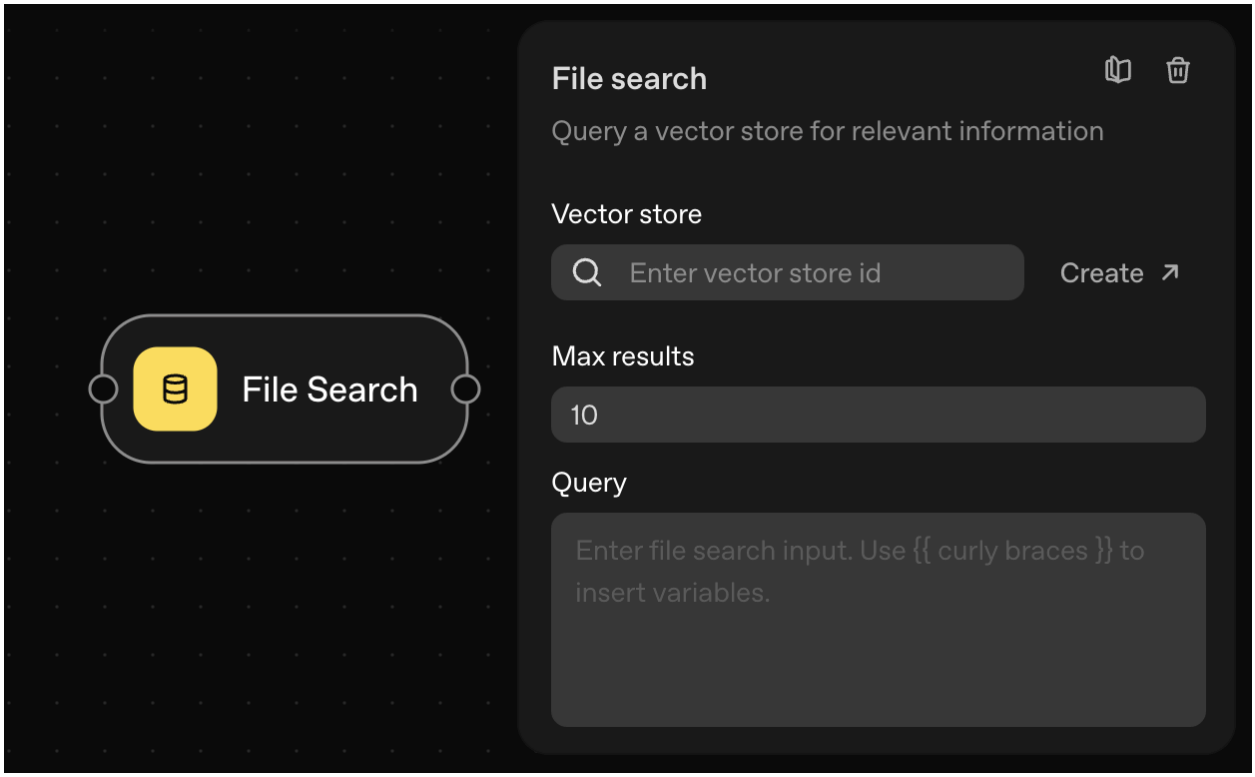


We have to click the create icon to create a vector store.



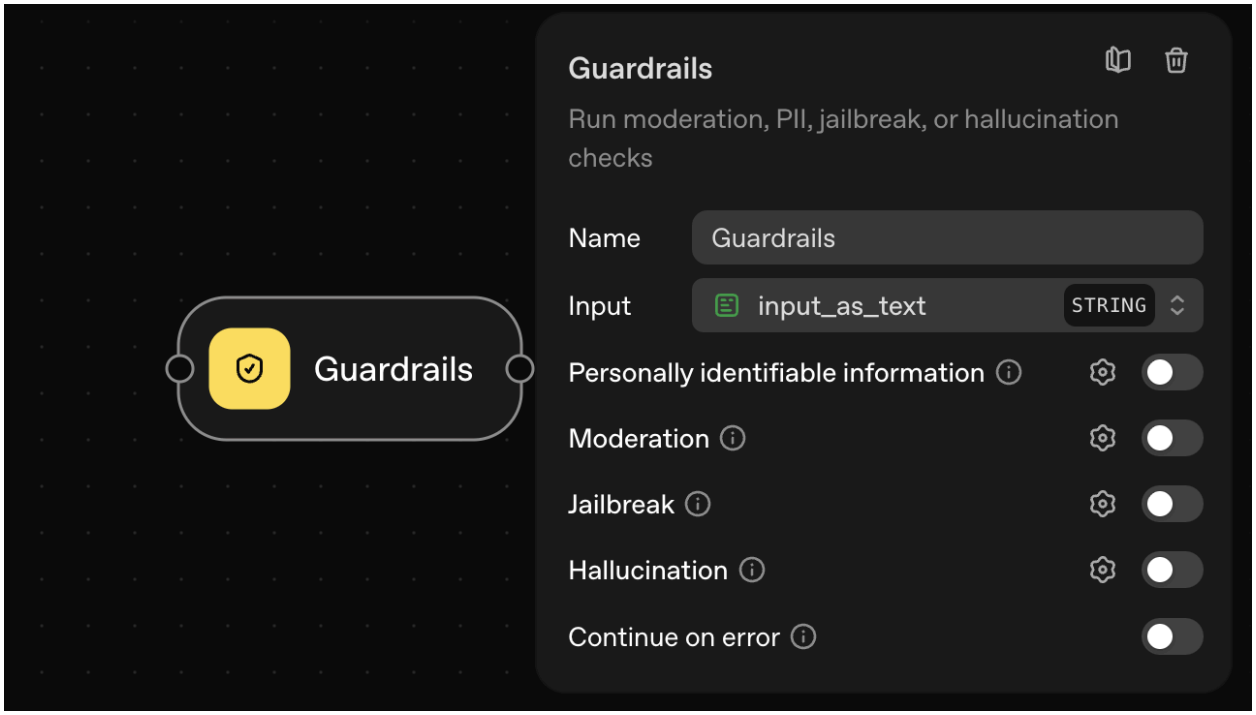
After clicking the create icon, we would have to give the store a name and click the Add files button to add the files we want as a resource for the agent.

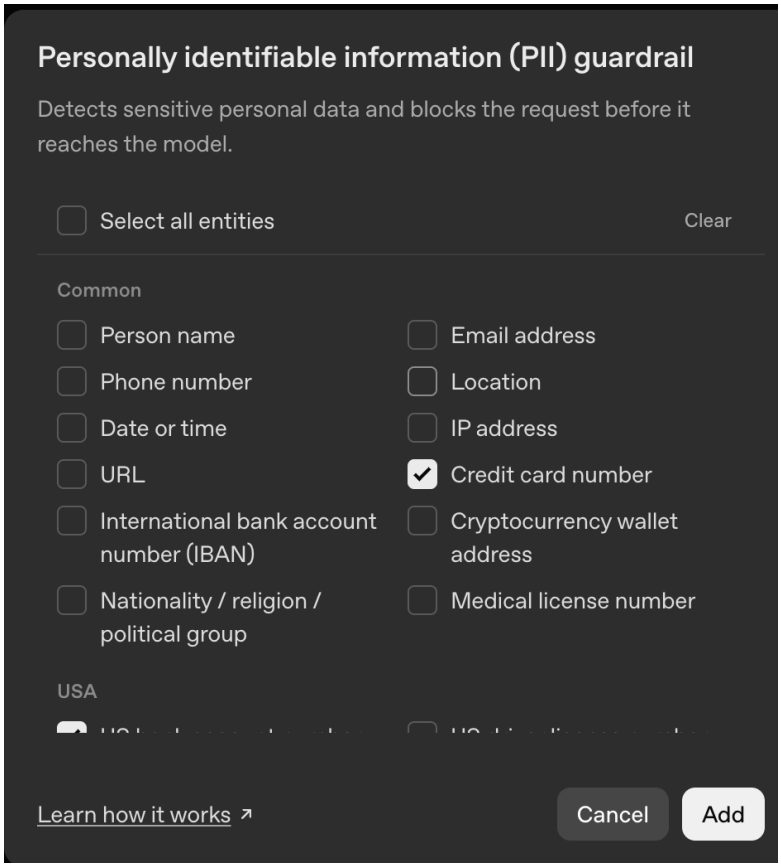
Then we will click the tick icon to finish preparing our vector store.
We will need the vector store id for our file search node to get access to the store.



After we enter the vector store id and connect the file search node with the agent node, our agent node will be able to function with our resources.

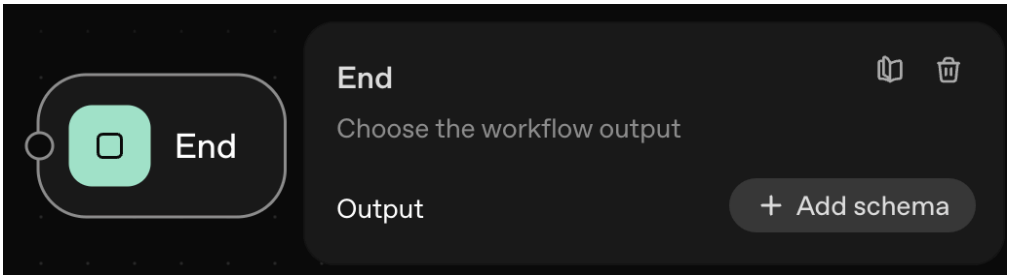
4. Guardrails Node: One of the most important nodes is the guardrails node. This is the node that allows us to restrict the sensitive information that the user types.


Guardrails
Guardrails
Run moderation, PII, jailbreak, or hallucination checks
Name
Guardrails
Input
input_as_text
STRING
Personally identifiable information
Moderation
Jailbreak
Hallucination
Continue on error


Personally identifiable information (PII) guardrail
Detects sensitive personal data and blocks the request before it reaches the model.
Select all entities
Clear
Common
Person name
Email address
Phone number
Location
Date or time
IP address
URL
Credit card number
International bank account number (IBAN)
Cryptocurrency wallet address
Nationality / religion / political group
Medical license number
USA
Learn how it works
Cancel
Add

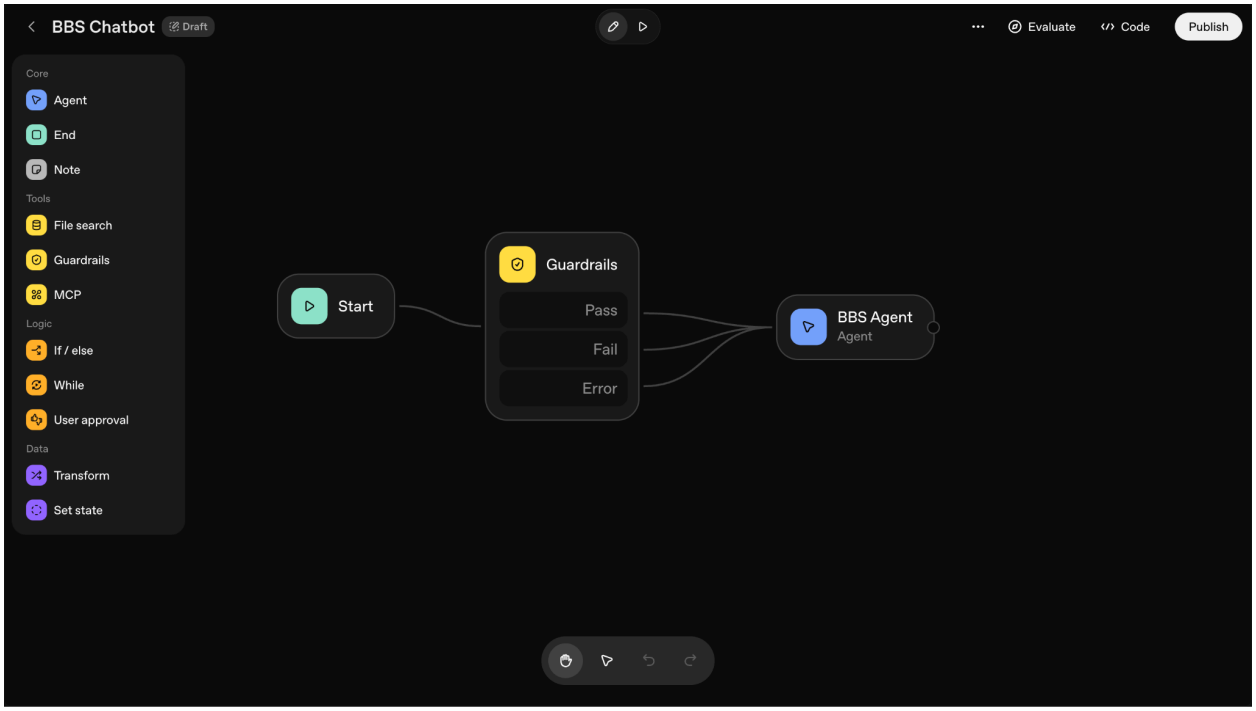
There are subsections like this inside the guardrails node which will allow us to restrict or moderate the info we want from the user's end.

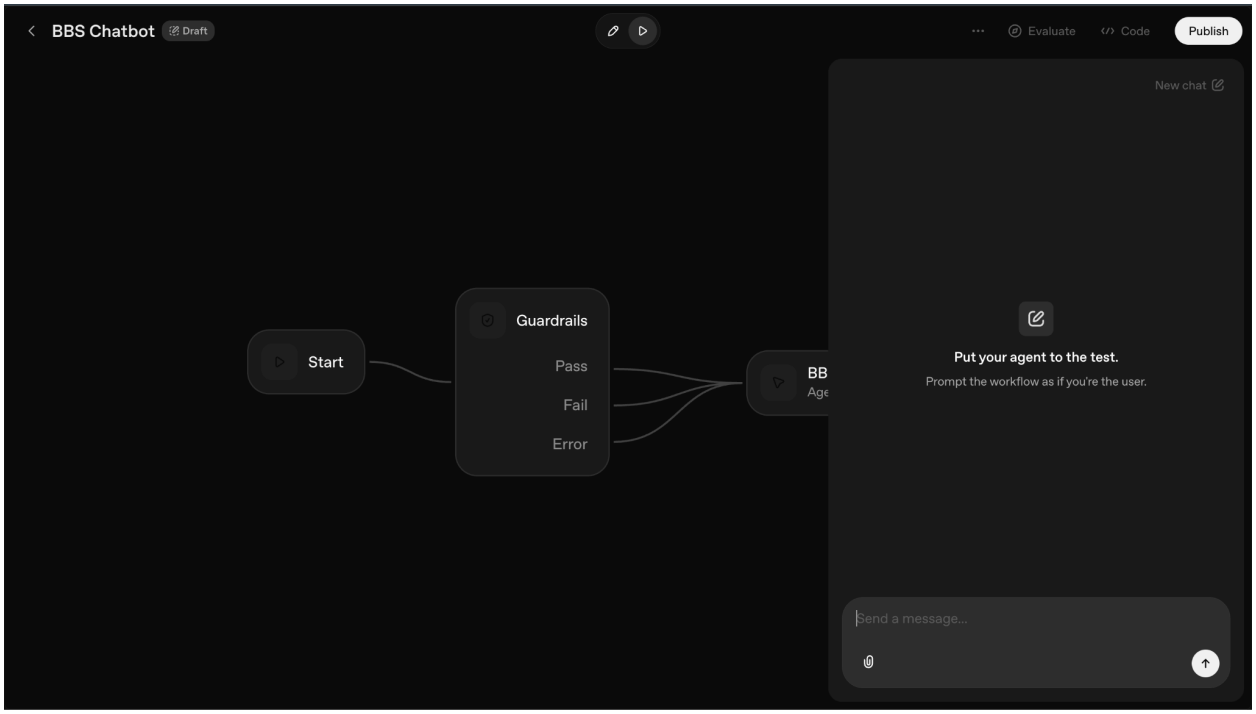
5. End Node: The End node is similar to the Start node, but the difference is in this node, we will be able to change the format of the output given by the agent.



How to Test, Fix and Publish your agent

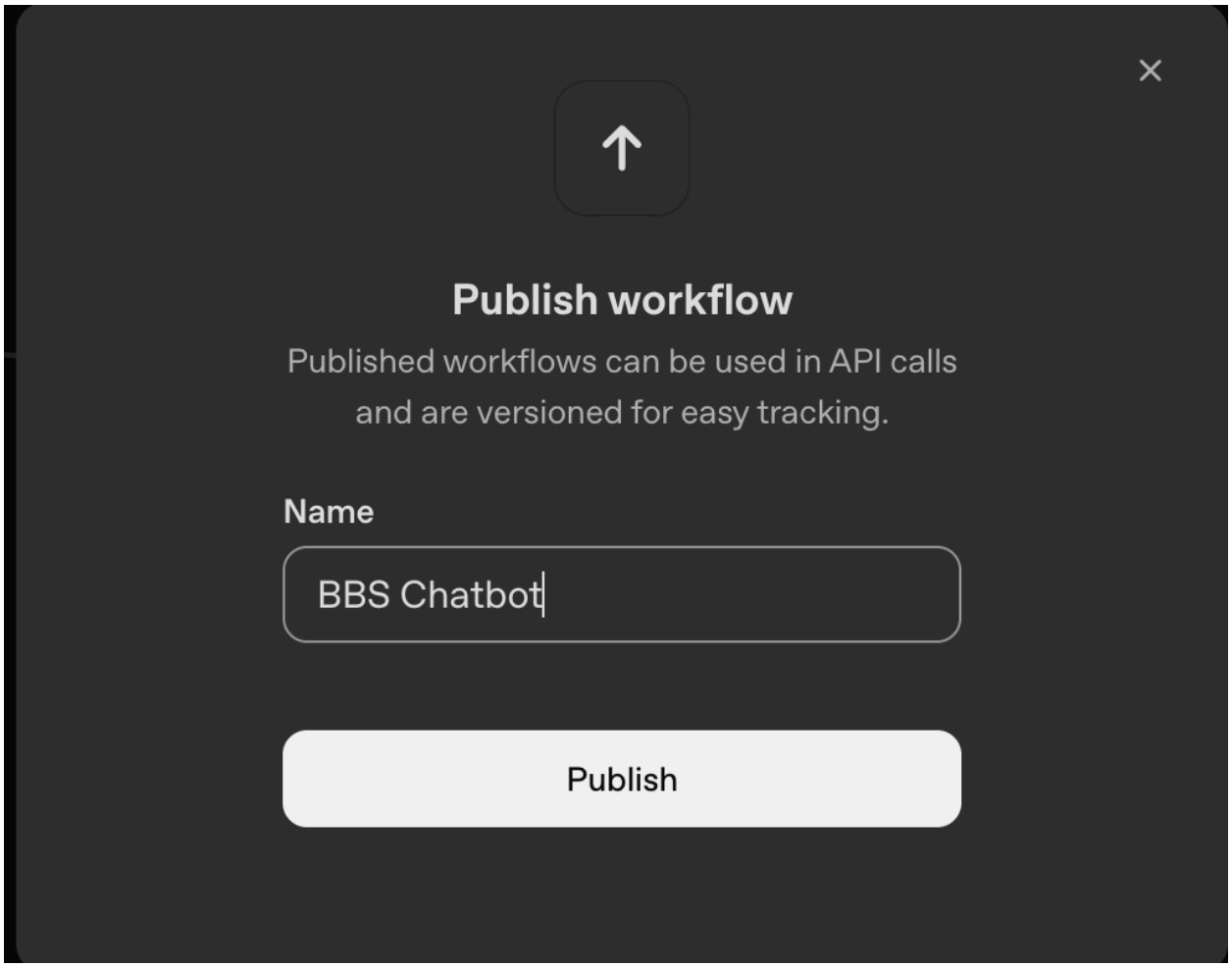
While we are developing the agent or have finished developing the agent we can keep using the preview option (The play button at the top) to test our agent.





We can type messages here and test the agent based on our specific requirements and keep changing the agent based on responses until we get the perfect agent for our tasks.

Then we have to click the publish button at the top to publish the agent. Without this step, we can’t use or deploy the agent.



After we publish the agent we can share the agent with people and use it as well by embedding it in our website.