HCLTech | Supercharging Progress™

AI Force

Version 2.0

User Manual

Contents

1 AI Force 2.0 – An Introduction

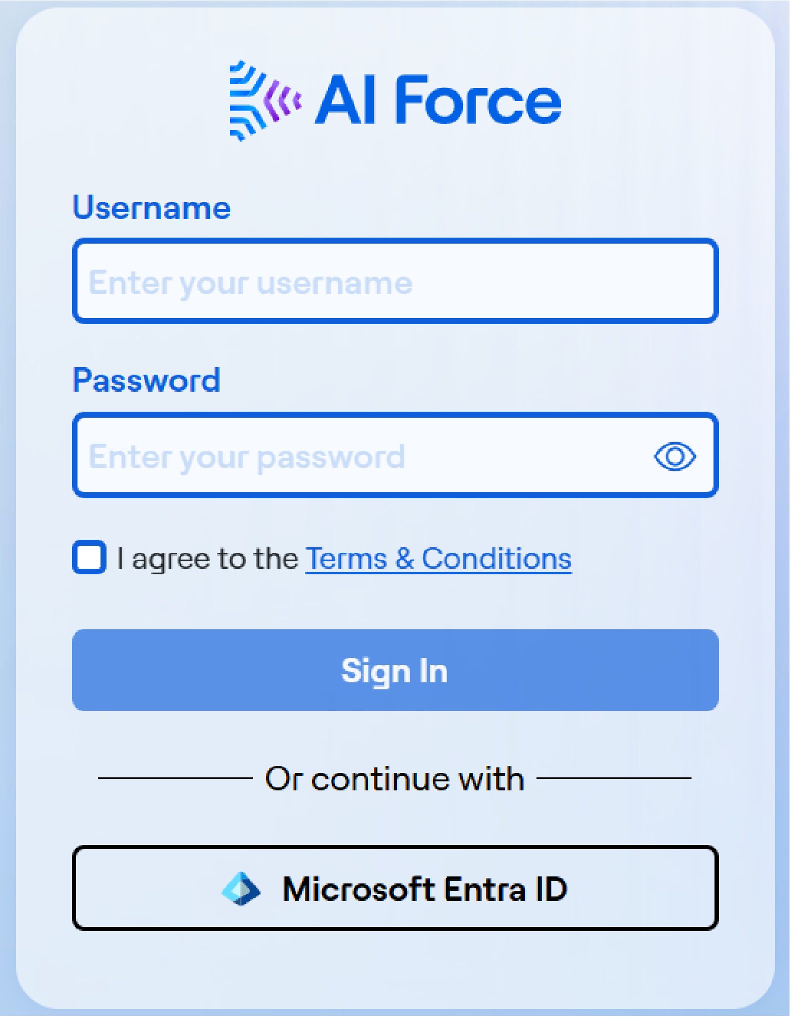
AI Force is a unified platform of intelligent AI-powered solutions designed to enable organizations to create, manage, and optimize AI-driven workflows with speed, accuracy, and efficiency. By combining advanced Generative AI, retrieval-augmented generation (RAG), and autonomous agent capabilities, AI Force empowers teams to leverage AI across diverse tasks, making operations smarter, faster, and more reliable.

With AI Force, you can build and manage projects, design and test prompts, configure tools, create RAG pipelines, and develop autonomous agents that take action based on contextual inputs. The platform also provides Model Context Protocol (MCP) management to standardize interactions between AI models and external resources, tools, and prompts. By offering a seamless and integrated environment, AI Force enables organizations to automate workflows, optimize decision-making, and enhance operational efficiency across a wide range of applications.

2 Login and Home Page

2.1 Logging in to AI Force

You can log in to AI Force using a username or email ID and password, or using your Microsoft Entra ID.

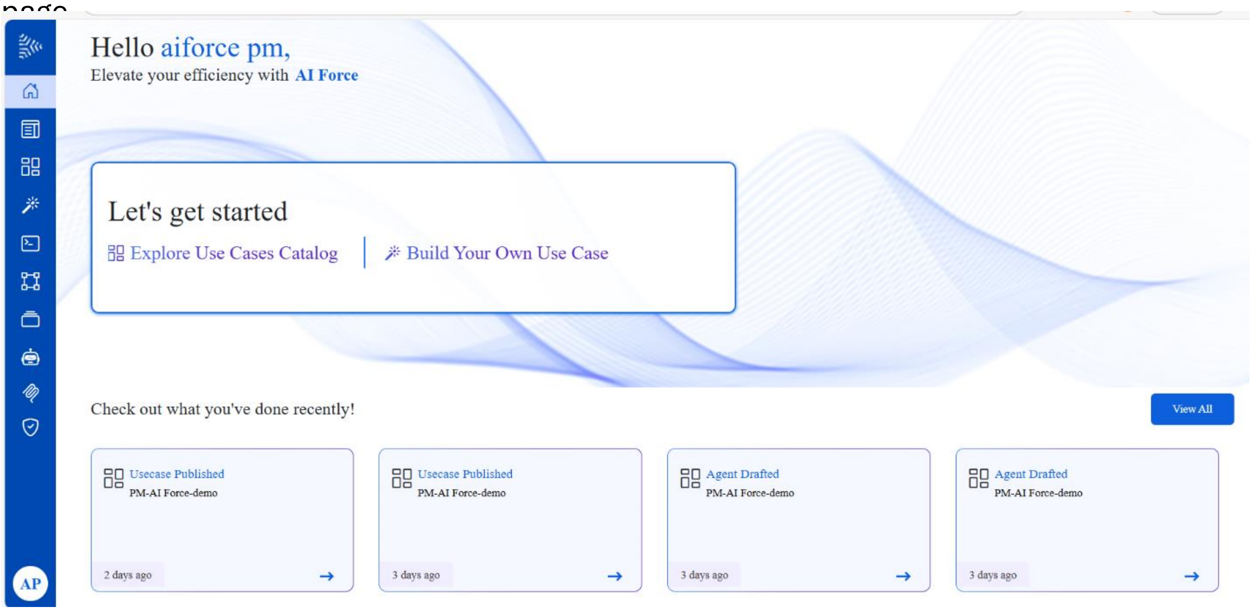


Enter your Username or Email ID, Password and select the I agree to the Terms & Conditions check box. Click **Sign In**. The first time you are logging in you will have to accept the End User License Agreement.

Click Microsoft Entra ID to continue with your Microsoft Entra ID. The Entra ID is integrated with the existing enterprise authentication system and takes you to the AI Force Home page.

2.2 Home Page

Logging in to AI Force takes you to the Home page



Hello aiforce pm,

Elevate your efficiency with **AI Force**

Let's get started

Explore Use Cases Catalog | Build Your Own Use Case

Check out what you've done recently!

The Home Page displays a Hello message with your full name and also displays the tag line, “Elevate your efficiency with AI Force”. The session times out after 30 minutes of inactivity.

The Home page has options for you to navigate to the **Explore Use Cases Catalog** or **Build Your Own Use Case**. Clicking on Explore Use Cases Catalog displays the dropdown with the three options AI Force.Software, AI Force.ITOps, AI Force.BizOps and a short description for each option. Depending on your role, these options are enabled or disabled. Click on an enabled option to go to that particular catalog of Use Cases.

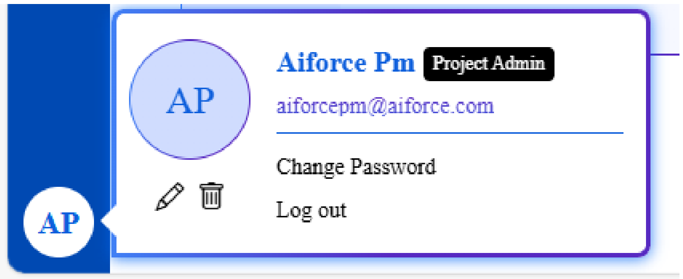
The Build Your Own Use Case option is enabled for all users other than those with End User role. Click the option to build your own use case.

The **Menu Bar** on the left has icons for you to navigate to the various studios and other options available in AI Force. There are icons for:

- Projects Studio
- Use Cases Catalog
- Build Your Own Use Case
- Prompt Studio
- Tools Studio
- RAG Studio
- Agentic AI Studio
- MCP Studio

- Governance and Evaluation Studio

Your login profile is displayed at the bottom of the menu bar.



Aiforce Pm Project Admin

aiforcepm@aiforce.com

The login profile displays your initials, your full name, your role name, and email ID. On first login the role name is User. Once the Project Admin updates the role name, it is reflected in the profile.

For users logged in with a Username or Email ID and password, a Change Password option is available. Click it to securely change the password. Click **Log Out** to log out of AI Force.

The Home page displays the platform-level activities that you carried out in the last 15 days. Up to four of these activities are displayed as tiles and the rest are available as a list when you click the View All button. Each tile has the Activity Name. the Project Name and the time when it was last opened (within the last 15 days). If you click the tile, the appropriate page for the activity appears in the appropriate project. If there was no activity over the last 15 days, the message No Recent Activity is displayed.

3 Projects

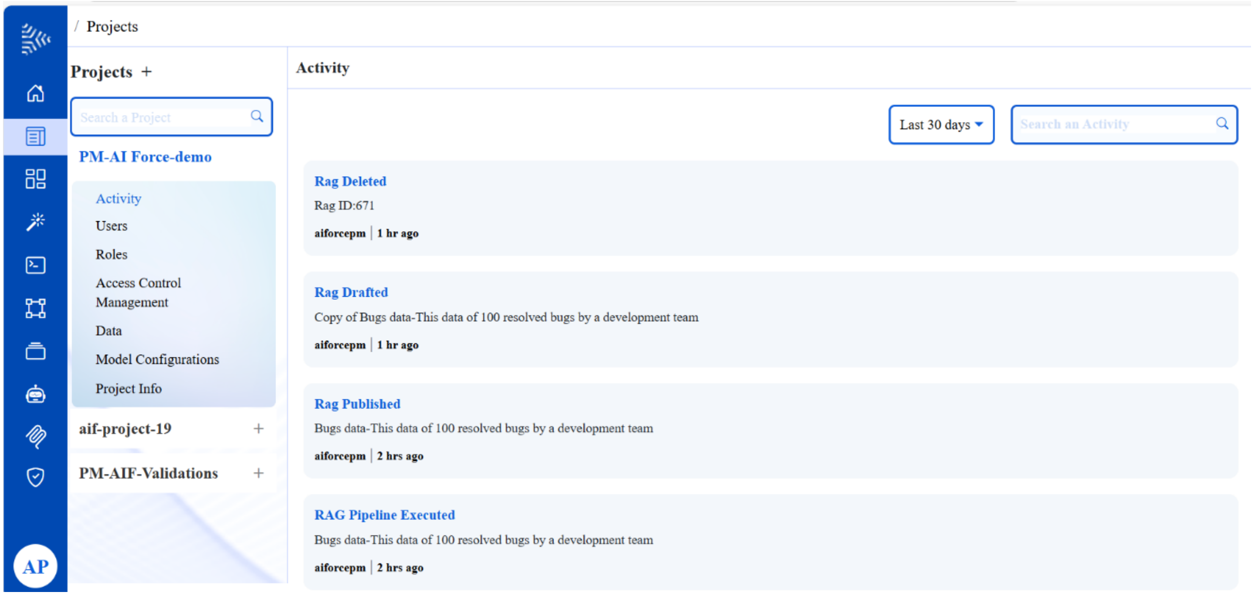
Project Studio serves as the central workspace for managing and configuring all aspects of your AI projects. It provides a unified interface where you can create and administer projects, manage data and models, define user roles and permissions, and monitor project activities- all within a single environment. It is designed to simplify project administration, enhance collaboration among users, and ensure streamlined integration of data and AI models within your workspace. It acts as the foundation for managing your end-to-end AI lifecycle-from data onboarding to model deployment and streamline use of agentic workflows across projects.

Using the Projects option, you can:

- View all projects assigned to you with the default project appearing first
- Create projects
- View the activities that have taken place in the project over a specified period.
- If you are a project admin you can view details of the users of the project and invite new users
- If you are a project admin you can view details of roles and add new role names
- If you are a project admin you can perform Access Control Management by selecting a role name, viewing the permissions for the role name, and making changes to the permissions of the role name
- Upload new data, view details of uploaded data, and delete old data.
- View and manage details of LLMs, Embedding Models, and Speech Configuration Models. You can add new models, edit existing ones, or delete models as needed through the Model Configuration interface.
- View and update project information

3.1 New Projects

1. Click ▤ (the Projects icon) from the Menu bar. The Projects page appears with the assigned project list and with the default project on top.



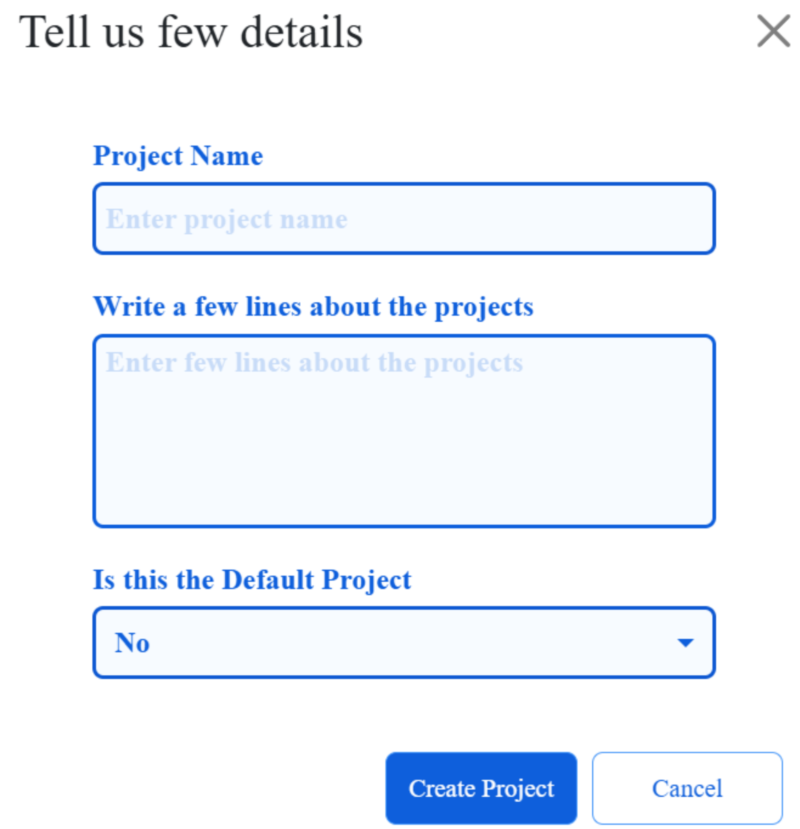
Rag Deleted
Rag ID:671
aiforcepm | **1 hr ago**

Rag Drafted
Copy of Bugs data-This data of 100 resolved bugs by a development team
aiforcepm | **1 hr ago**

Rag Published
Bugs data-This data of 100 resolved bugs by a development team
aiforcepm | **2 hrs ago**

RAG Pipeline Executed
Bugs data-This data of 100 resolved bugs by a development team
aiforcepm | **2 hrs ago**

To create a new project, click the + icon next to Projects. The new projects page appears.



Tell us few details

Project Name
Enter project name

Write a few lines about the projects
Enter few lines about the projects

Is this the Default Project
No

Enter the details of the new project and click **Create Project**. The project is created and appears under the list of projects.

When the project is created, a unique token gets automatically generated and saved for use with API integrations. This unique token is stored in the project metadata. This token will be available for copying in the Project Info section. You can copy the token by clicking on the Copy icon in the project token.

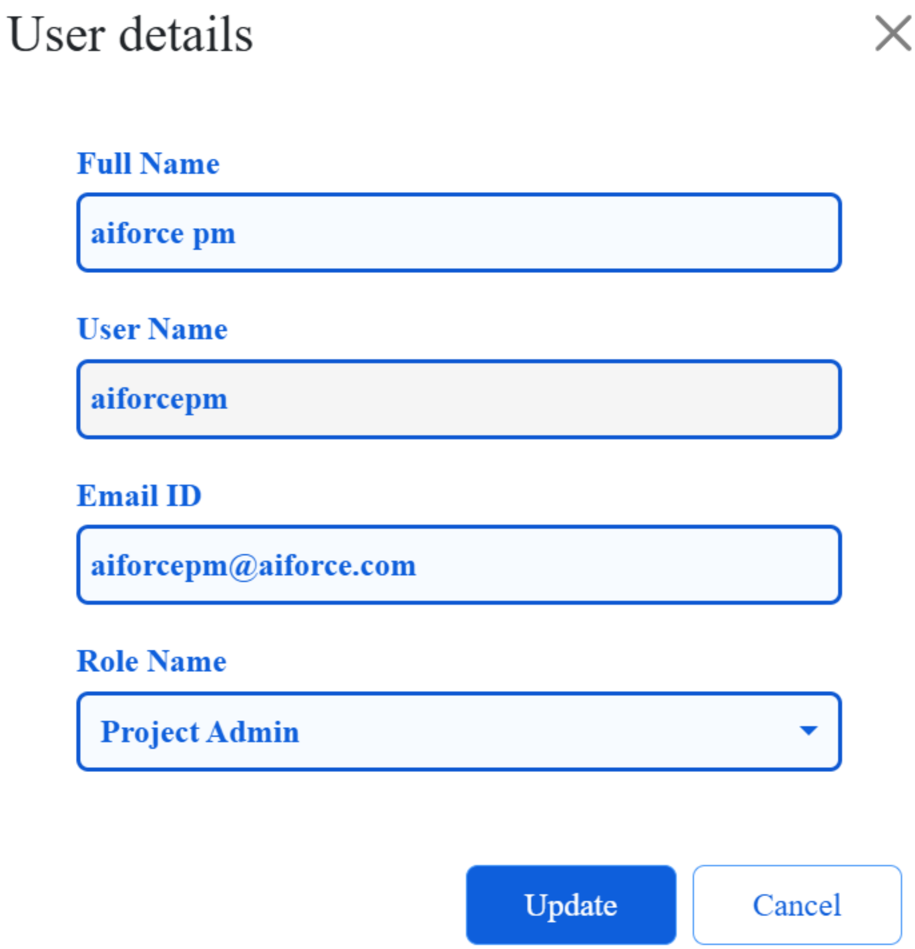
3.2 Activity Management

The Projects page opens with a list of activities associated with the default project. You can view and track these activities over a specified time period. Additionally, the page provides a search functionality that allows you to locate specific activities by entering the activity name and clicking the Search icon. The activities are stored for a period of 180 days. You can filter the activities based on time ranges such as last 24 hours and last 7 days.

3.3 User Management

If you are the Project Admin, you will be able to see the list of active users associated with their specific projects. You can manage the roles of these users.

1. Click **Users**. The Users page appears with a list of all active users associated with their specific projects. The Full Name of the user, the Username, the Email ID, the Role Name, and when the user was Last Active are displayed. There is an Action ellipses, which when clicked, allows you two options: to edit the details of the user and to remove the user. You can enter the name or the partial name of the user and search for the user.
2. To edit the details of a user, click the ellipses (...) in the Actions column of the user and click **Edit**. The User Details page appears.



User details

Full Name

aiforce pm

User Name

aiforcepm

Email ID

aiforcepm@aiforce.com

Role Name

Project Admin

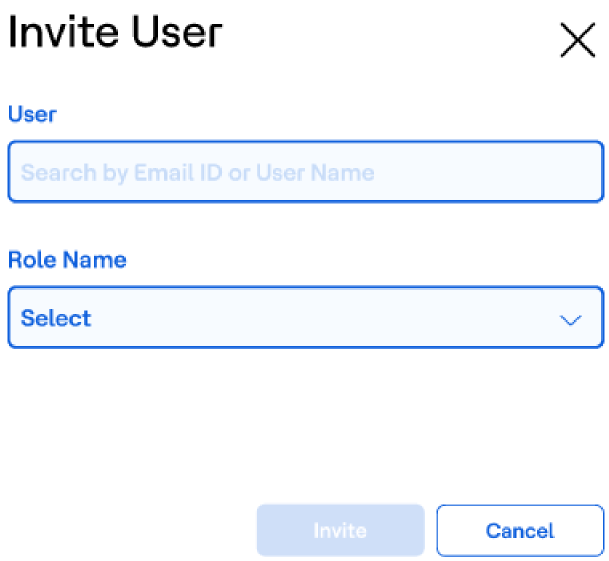
Make the required changes to the Full Name and Role Name fields and click **Update**.

3. To delete a user, click the ellipses in the Action column of the user and click **Delete**. A Delete confirmation page appears. Click **Yes** to delete the user.

   Note:

   Only a project admin has the authority to edit or delete users.

4. To invite a new user to the project, click **Invite User** at the top right corner of the screen. The Invite User page appears.

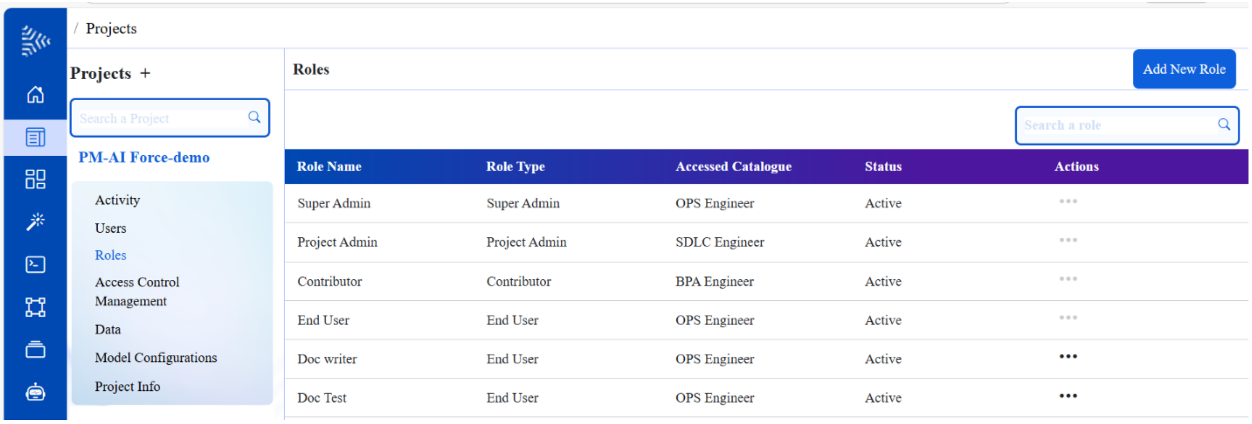


Search for the user using the username or email ID. Select the role name of the user and click **Invite**. The user is added to the list of users in the project. You can add multiple users to the project. A maximum of 500 users can be added at a time.

3.4 Role Management

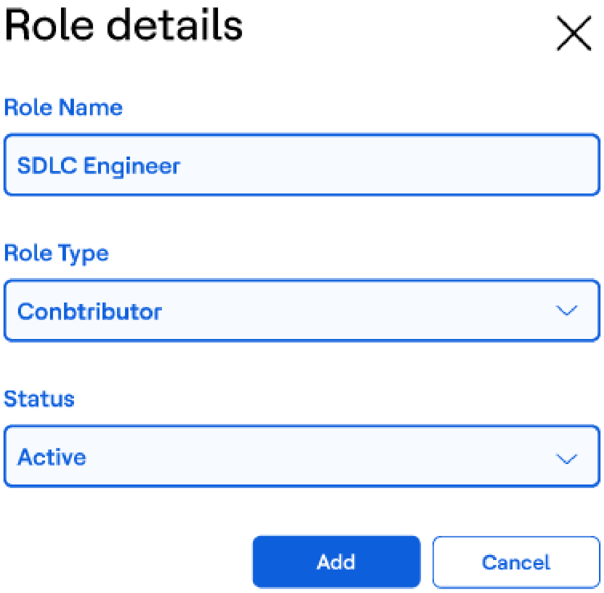
If you are the Project Admin, you can view Role Names, their associated Role Types, and accessed use case catalogs for each role.

1. Click **Roles**. The Roles page appears. You can view the Role Name, the Role Type, Accessed Catalog, the Status of the role, and Action ellipses.



Role Name	Role Type	Accessed Catalogue	Status	Actions
Super Admin	Super Admin	OPS Engineer	Active	•••
Project Admin	Project Admin	SDLC Engineer	Active	•••
Contributor	Contributor	BPA Engineer	Active	•••
End User	End User	OPS Engineer	Active	•••
Doc writer	End User	OPS Engineer	Active	•••
Doc Test	End User	OPS Engineer	Active	•••

2. To add a new role name, click **Add New Role** at the top right corner of the page. The Role Details page appears.



Role details

Role Name: SDLC Engineer

Role Type: Conbtributor

Status: Active

Enter the Role Name, select the Role Type and Status, and click **Add Role**. The role is added to the list of roles.

3. To edit the role, click the ellipses (...) at the right end of the row and click **Edit**. The Role Details page appears. Make the required changes to Role Name, Role Type, and Status and click **Update**.
4. To delete a role, click the ellipses (...) at the right end of the row and click **Delete**. The Delete confirmation page appears. Click **Yes** to delete the role.

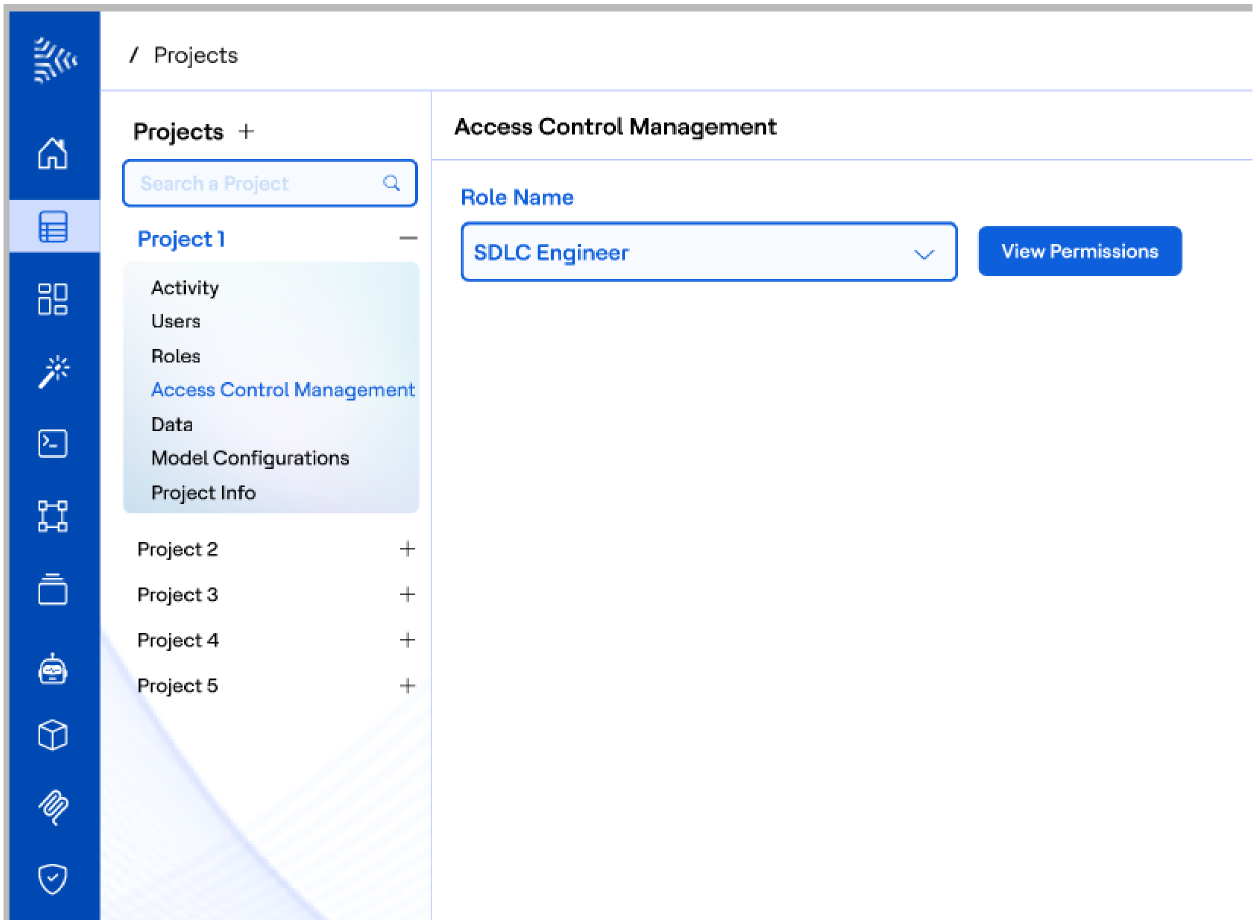
   Note:

   Only Project Admin has the authority to create, edit, and delete role names.

3.5 Access Control Management

If you are the Project Admin, you can manage access control for different role names within the project. Access Control includes permission to access Use Case Catalog and category-level access.

1. Click **Access Control Management**. The Access Control Management page appears.



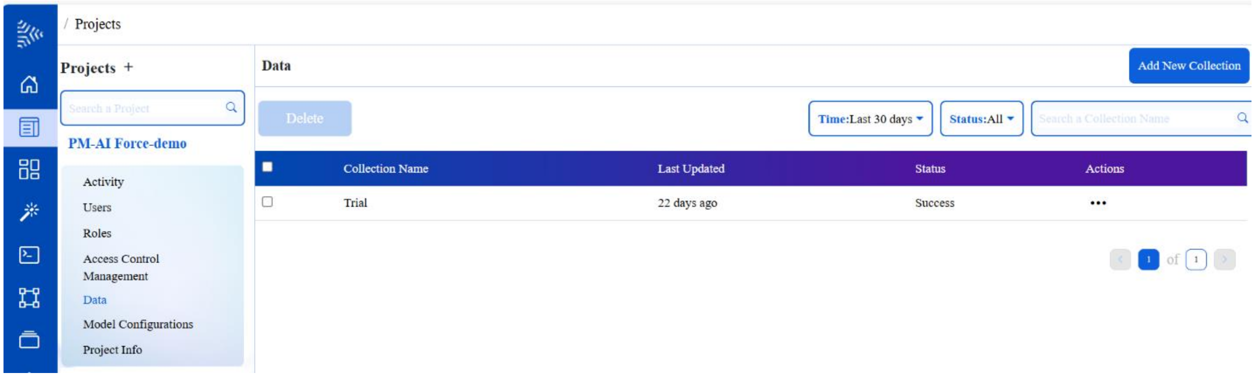
2. To view the permissions a particular role name has, select the role name from the drop-down and click **View Permissions**. The Use Case Catalogs appear with a toggle button to give or deny access. If you give access to a Use Case Catalog, you are giving access to all the categories in the Use Case Catalog. You can uncheck specific categories, if needed. You can modify the permissions and click **Save**.

3.6 Data Management

Data Management in AI Force consists of maintaining all the uploaded data for specific projects. You can upload new data collections, update a data collection and delete data.

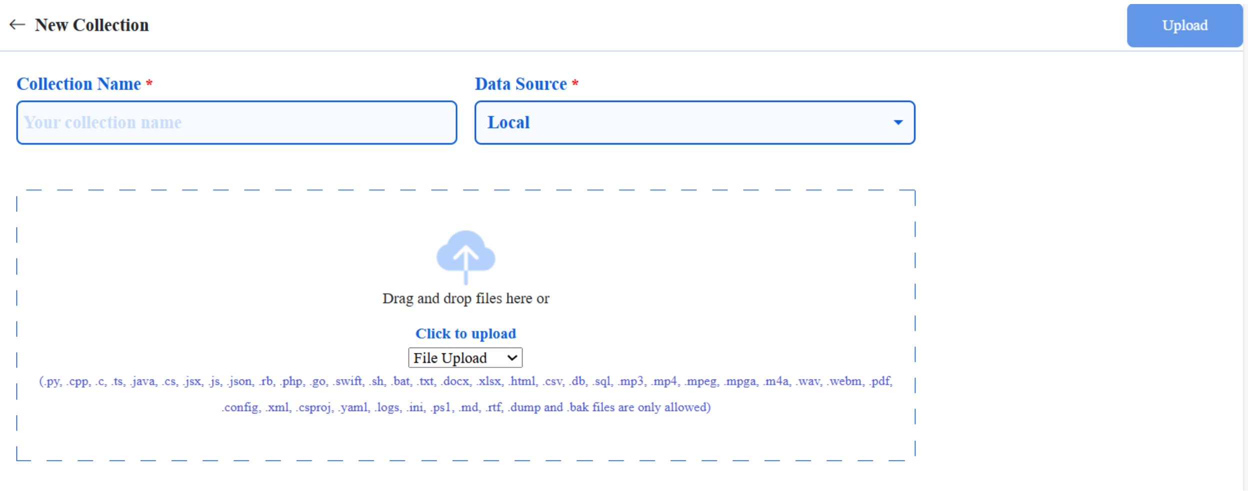
1. Click **Data**. The Data page appears. You can filter Data Collections created over a specified period. You can also filter Data Collections based on status, which could be Success, In-progress, Failed, or All. You can enter the name of a data collection in the Search box and search for the data collection.

   You can view the Data Collection Name, the time that has passed since the data collection was last updated, the status of the data collection, and an Actions ellipses. The status of the data collection can be Success (if it the files have been uploaded), In-progress (if the upload is in progress), or Failed (if the upload failed). Click the Actions ellipses to View the data collection, to Add or Remove the data collection to or from an MCP server, to Rename a data collection, or to Delete a data collection. The data collections are sorted on the Last Updated date in descending order.



□	Collection Name	Last Updated	Status	Actions
□	Trial	22 days ago	Success	•••

2. To add a new data collection, click **Add New Collection**. The New Collection page appears. Here, you can upload files or create a collection of multiple files that can be used in agents, RAG pipelines, or during use case execution.



Collection Name * Your collection name

Data Source * Local

(.py, .cpp, .c, .ts, .java, .cs, .jsx, .js, .json, .rb, .php, .go, .swift, .sh, .bat, .txt, .docx, .xlsx, .html, .csv, .db, .sql, .mp3, .mp4, .mpeg, .mpga, .m4a, .wav, .webm, .pdf, .config, .xml, .csproj, .yaml, .logs, .ini, .ps1, .md, .rtf, .dump and .bak files are only allowed)

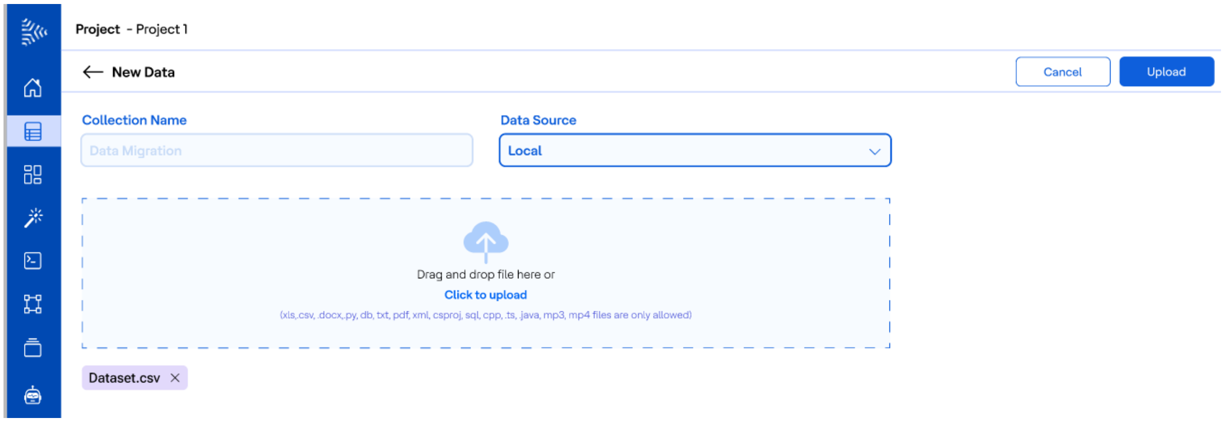
Enter the Collection Name, select the Data Source, and upload files. Data source can be Local or any preconfigured external sources. If you select Local, you can browse, search, and select one or more files from your system. If you select a preconfigured external source, all configured repository files from the source are displayed. You can browse, search, and select files to upload to the collection. Click **Upload**. The selected files are added to the new Data Collection. The maximum size of files that can be uploaded per request is 100 mb. Certain types of files are only accepted. If the file type you are trying to upload is not accepted, an error message is displayed. Click **Save**. The new Data Collection is created and added to the Data Collection library.

3. To view a data collection, click the ellipses (…) in the Actions column of the Data Collection, and click **View**. You can view the files in the Data Collection. You can view the File Name, Path, the time it was Last Updated, Status (Success, In-progress, Failed), and Actions ellipses.

   You can filter file or folder names created over a specified period. You can also filter file or folders based on status, which could be Success, In-progress, Failed, or All. You can enter the name of a file or folder in the Search box and search for it.

   Files with Status as Success and In-progress have the Actions as Add/Remove from MCP, Download, Delete, and Retry. For files in Failed status, an additional option Logs is enabled. Click Logs to view the timestamp of file upload, the status of file upload, and the Reasons for Failure.

   To create new files, click **New Data**.



Project - Project 1

New Data

Collection Name: Data Migration

Data Source: Local

Drag and drop file here or

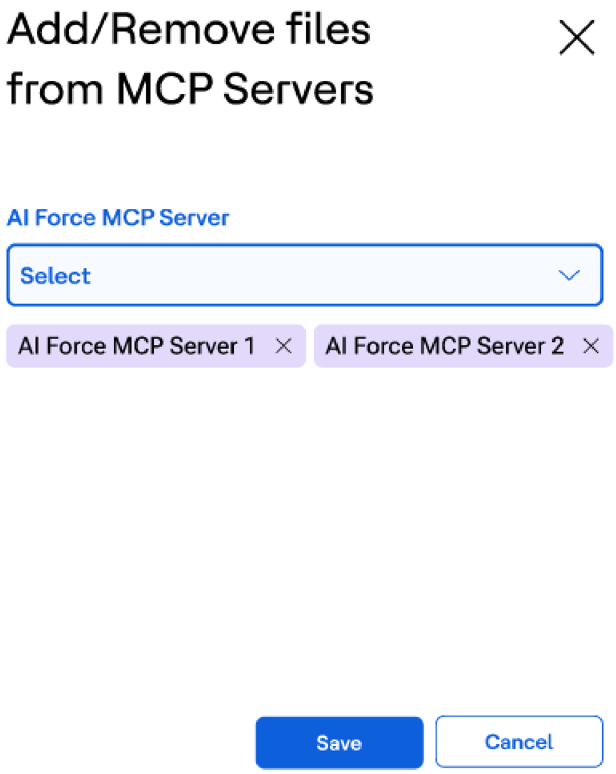
Click to upload

(xls,.csv, .docx,.py, db, txt, pdf, xml, csproj, sql, cpp, .ts, .java, mp3, mp4 files are only allowed)

Dataset.csv

   Select the Data Source. Data source can be Local or any preconfigured external sources. If you select Local, you can browse, search, and select one or more files from your system. If you select a preconfigured external source, all configured repository files from the source are displayed. You can browse, search, and select files to upload to the collection. Click **Upload**. The selected files are added to the Data Collection. Drag and drop the files that you need to upload or click **Click to Upload**. You can upload files or folders. The maximum size of files that can be uploaded per request is 100 mb. Certain types of files are only accepted. If the file type you are trying to upload is not accepted, an error message is displayed. Click **Upload**.

To add or remove the file from the AI Force enabled MCP Server, click the ellipses (...) in the Actions column of the file and click **Add/Remove from MCP**. The Add/Remove file from MCP Server page appears.



Add/Remove files from MCP Servers

AI Force MCP Server: Select

AI Force MCP Server 1 × AI Force MCP Server 2 ×

Select the MCP server to which the file is to be added, or from which it is to be removed. All the selected MCP servers are shown and can be removed by clicking the X icon. Click **Save**.

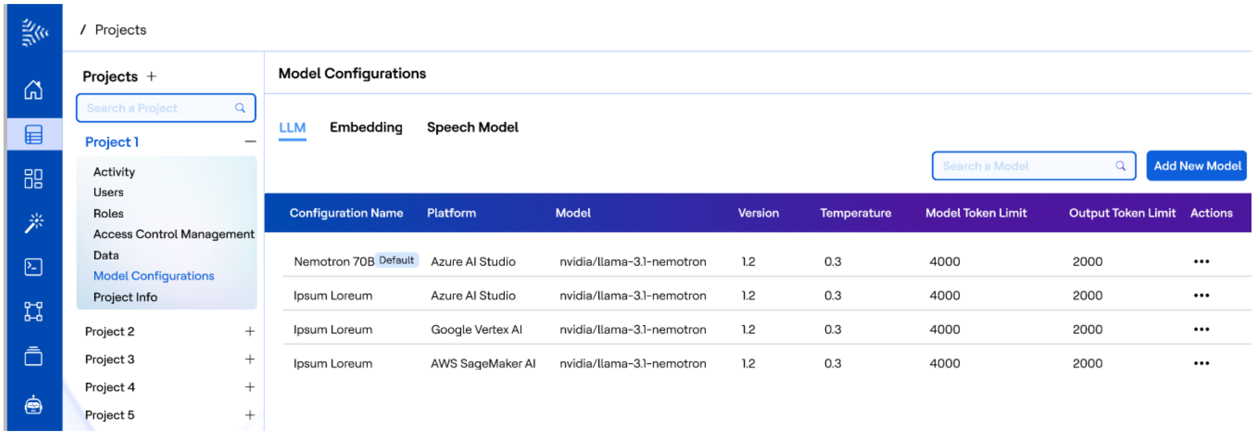
To download the file, click the ellipses (...) in the Actions column of the file, and click **Download**. The file is downloaded to your local machine.

To delete the file, click the ellipses (...) in the Actions column of the file, and click Delete. A Delete Confirmation page appears. Click **Yes** to delete the file. You can also select the checkbox before the File Name, and click **Delete** in the data collection page.

4. To rename a data collection, click the ellipses (...) in the Actions column of the Data Collection. The Rename page appears. Rename the Data Collection and click **Save**.
5. To delete a data collection, click the ellipses (...) in the Actions column of the data collection, and click **Delete**. The Delete Confirmation page appears. Click **Yes** to delete the data collection. Any generated embeddings associated with the collection are also removed.

3.7 Model Configuration

Click **Model Configuration**. The Model Configuration page appears.



/ Projects

Projects +

Search a Project

Project 1 –

- Activity
- Users
- Roles
- Access Control Management
- Data
- Model Configurations
- Project Info

Project 2 +

Project 3 +

Project 4 +

Project 5 +

Model Configurations

LLM | Embedding | Speech Model

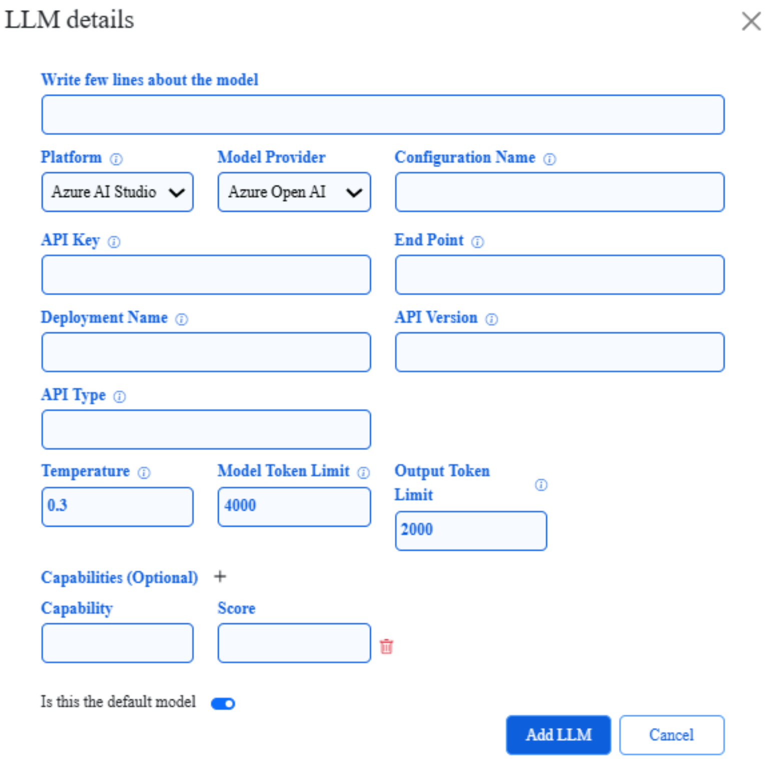
Search a Model | Add New Model

Configuration Name	Platform	Model	Version	Temperature	Model Token Limit	Output Token Limit	Actions
Nemotron 70B Default	Azure AI Studio	nvidia/llama-3.1-nemotron	1.2	0.3	4000	2000	•••
Ipsum Loreum	Azure AI Studio	nvidia/llama-3.1-nemotron	1.2	0.3	4000	2000	•••
Ipsum Loreum	Google Vertex AI	nvidia/llama-3.1-nemotron	1.2	0.3	4000	2000	•••
Ipsum Loreum	AWS SageMaker AI	nvidia/llama-3.1-nemotron	1.2	0.3	4000	2000	•••

You can view LLMs, Embedding models, and Speech models in the Model Configuration page.

3.7.1 Large Language Models

1. To add a new LLM, select the LLM tab (selected by default), and click **Add New Model**. The LLM Details page appears.



LLM details ×

Write few lines about the model

Platform ⓘ: Azure AI Studio

Model Provider: Azure Open AI

Configuration Name ⓘ

API Key ⓘ

End Point ⓘ

Deployment Name ⓘ

API Version ⓘ

API Type ⓘ

Temperature ⓘ: 0.3

Model Token Limit ⓘ: 4000

Output Token Limit ⓘ: 2000

Capabilities (Optional) +

Capability

Score

Is this the default model ●

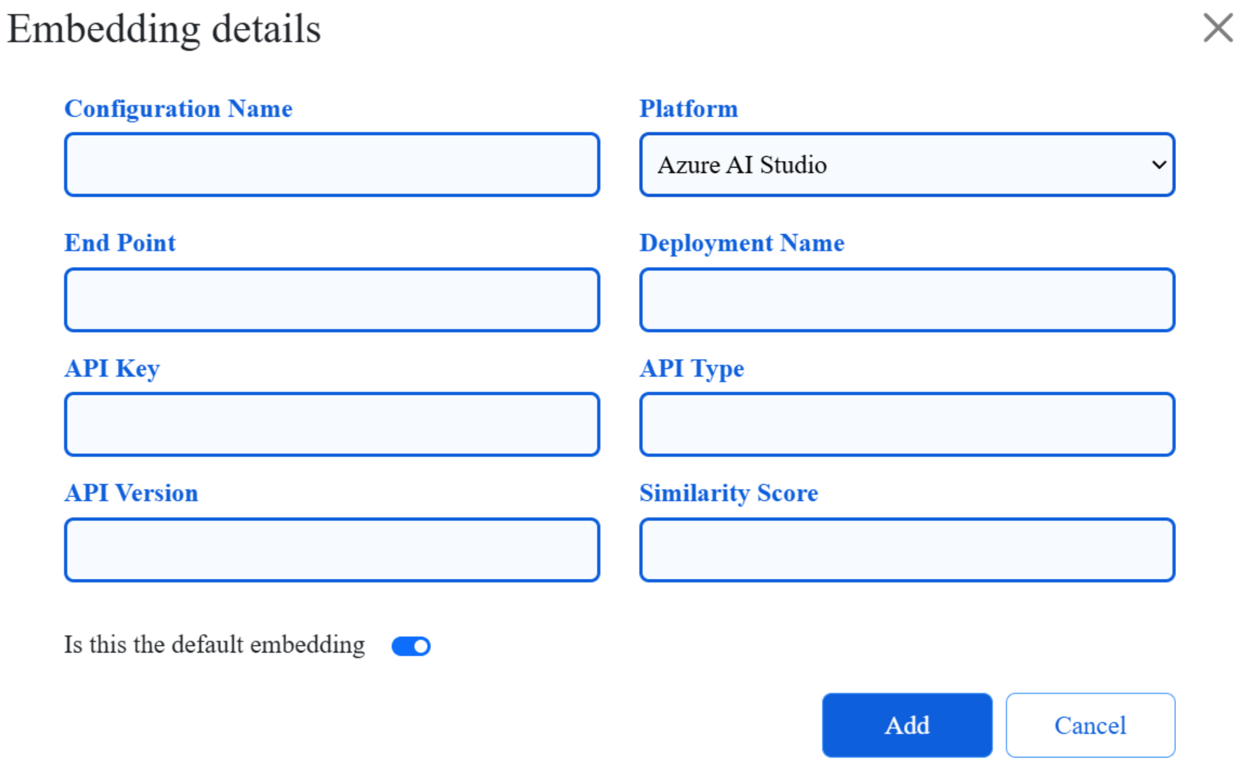
Add LLM | Cancel

Enter all the details. For information about a field, hover your mouse over ⓘ. Click **Add LLM**. The LLM is added.

2. To edit an LLM, click the ellipses (...) in the Actions column of the LLM, and click **Edit**. The LLM Details page appears with the details of the selected LLM. Make the required changes and click **Update**.
3. To delete an LLM, click the ellipses (...) in the Action column of the LLM, and click **Delete**. The Delete confirmation page appears. Click **Yes** to delete the LLM.

3.7.2 Embedding Models

1. To add an Embedding Model, select the Embedding tab and click Add Embedding. The Embedding Details page appears.



Embedding details

Configuration Name

Platform: Azure AI Studio

End Point

Deployment Name

API Key

API Type

API Version

Similarity Score

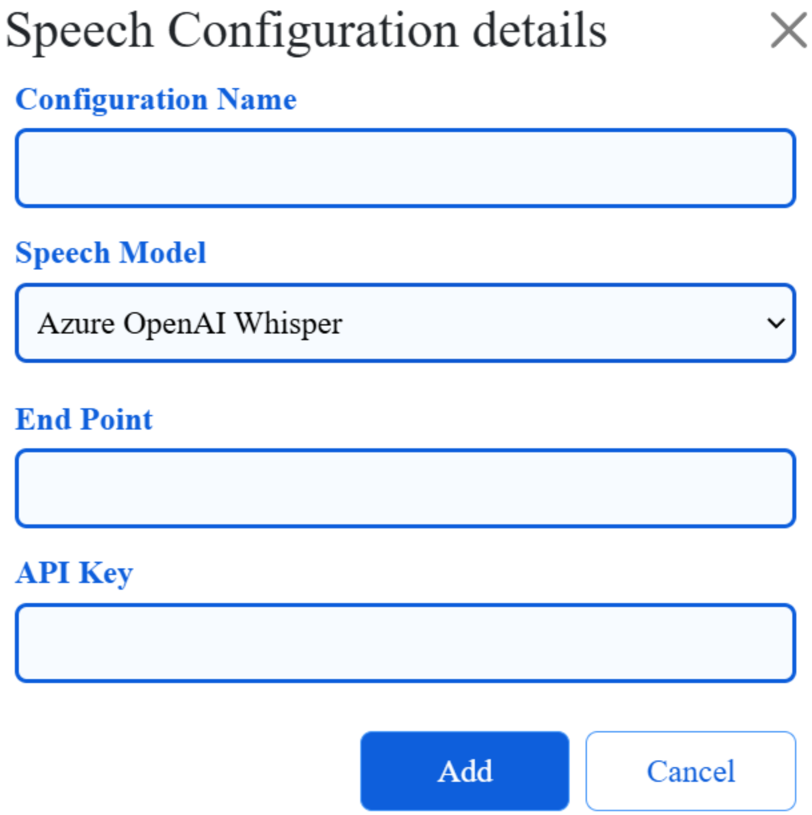
Is this the default embedding

Enter the details and click **Add**.

2. To edit an Embedding Model, click the ellipses (...) in the Actions column of the Embedding Model, and click **Edit**. The Embedding details page appears with the details of the Embedding Model. Make the required changes and click **Update**.
3. To delete an Embedding Model, click the ellipses (...) in the Action column of the Embedding Model, and click **Delete**. The Delete confirmation page appears. Click **Yes** to delete the Embedding Model.

3.7.3 Speech Configuration Models

1. To add a new Speech Model, select the Speech Model tab and click Add Speech Model. The Speech Configuration Details page appears.



Speech Configuration details

Configuration Name:

Speech Model: Azure OpenAI Whisper

End Point:

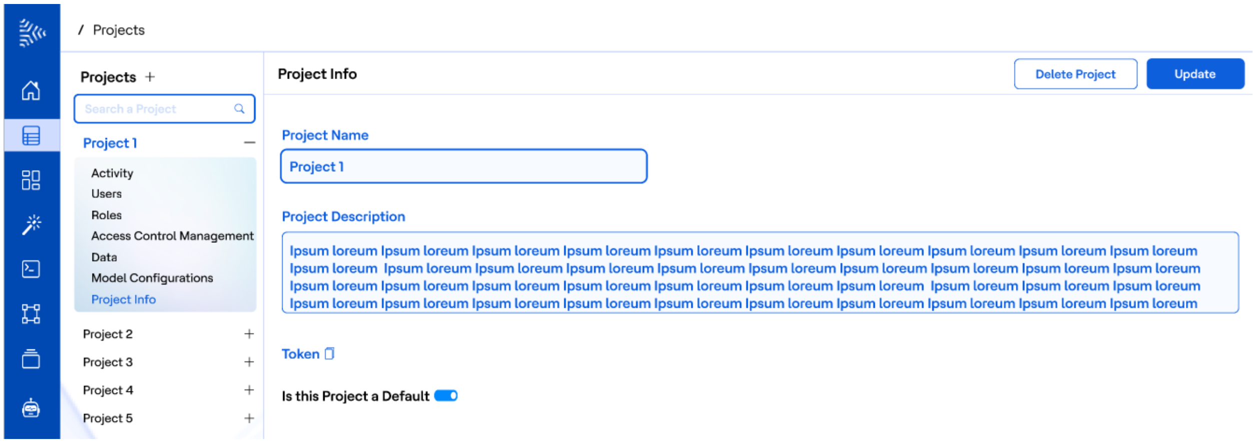
API Key:

Enter the details and click **Add**.

2. To edit a Speech Model, click the ellipses (...) in the Actions column of the Speech Model, and click **Edit**. The Speech Configuration details page appears with the details of the Speech Model. Make the required changes and click **Update**.
3. To delete a Speech Model, click the ellipses (...) in the Action column of the Speech Model, and click **Delete**. The Delete confirmation page appears. Click **Yes** to delete the Speech Model.

3.8 Project Info

Click **Project Info**. The Project Info page appears.



Project Name

Project 1

Project Description

Ipsum loreum Ipsum loreum

Token

Is this Project a Default

If you are a project admin you can modify the Project Name and Project Description and click **Update**. You can copy the project token by clicking on the copy icon next to the token. To delete the project, click **Delete Project**. The Delete Project page appears asking you to enter the reason for deleting the project. Enter the reason and click **Delete**. A warning page appears indicating that all users, data, and operations associated with the project will be permanently deleted. If you click **Yes**, the project is deleted.

4 Build Your Own Use Case

Build Your Own Use Case is a key feature in AI Force 2.0. It enables you to design and develop new agentic use cases or workflows in the AI Force platform through natural language inputs. By leveraging the agents available in the Agent Garden, you can create fully customized workflows tailored to your specific requirements. This capability gives you flexibility and control to build solutions that precisely align with your unique business needs.

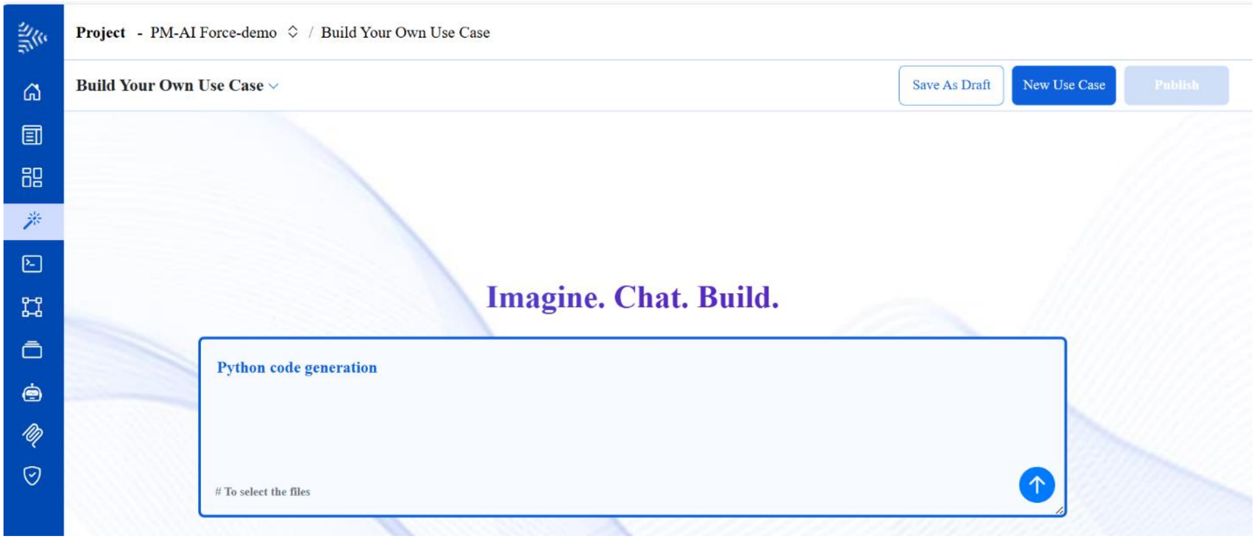
This module consists of three main pages. The first page allows you to input your use case requirements. On the second page an initial workflow configuration is auto generated by a background planner agent. You can further refine the workflow configuration. The third page enables you to test the configured workflow. If the test results are satisfactory, you can publish the use case to the AI Force Use Case Catalog for others to access.

You can use two patterns for the workflow, one is the supervisor pattern and the other is the graphical pattern.

4.1 Supervisor Pattern

4.1.1 Entering the Requirements

Click (the Build Your Own Use Case icon) from the Menu bar. The Build Your Own Use Case page appears. The objective of this page is to capture your requirements to create the new use case.



Project - PM-AI Force-demo / Build Your Own Use Case

Build Your Own Use Case

Imagine. Chat. Build.

Python code generation

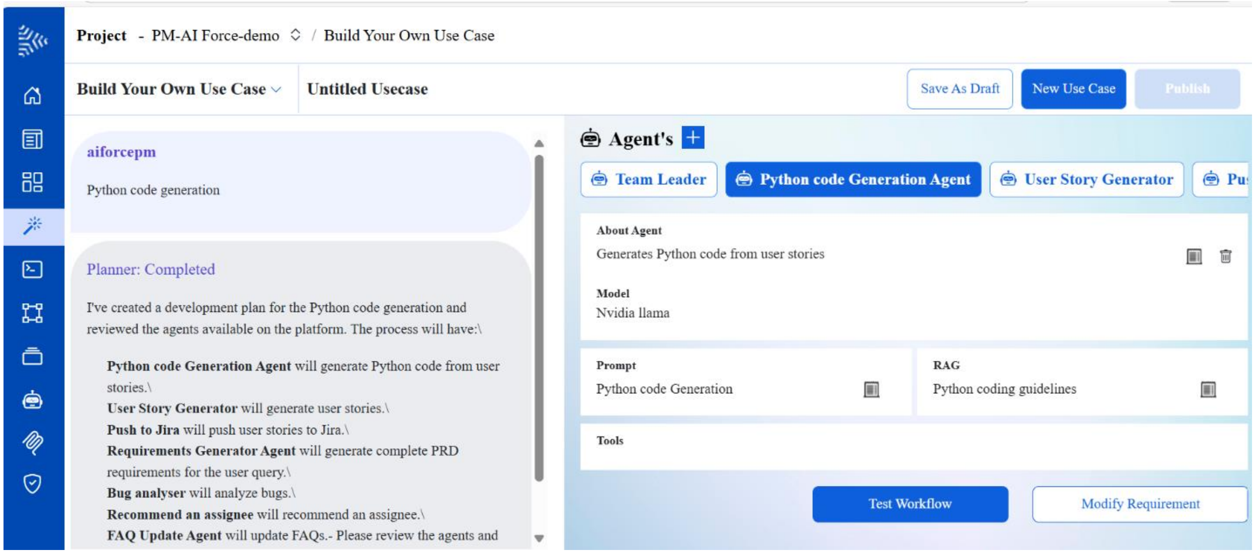
Enter a description for the case. A large, multiline text interface is present on the screen. You can enter a maximum of 4000 characters. You can enter natural language text to describe your requirements. In this description, you are required to clearly define the objective or intent of the use case you wish to create. Based on this description, tasks are created, and the Planner Agent intelligently selects the suitable agents from the Agent Garden to accomplish those tasks.

4.1.2 Attaching a File

You can also attach a file as complete description, or as added context to the description. You can attach a maximum of 100 mb. Click ⬆ (the GO icon). Clicking this icon with valid input sends the input to the planner agent for processing and directs you to the New Use Case – Workflow Configuration page.

4.1.3 Initial Workflow

The page automatically generates an initial workflow based on user requirements using a background Planner Agent. The Planner Agent, with full knowledge of all AI Force platform agents, crafts comprehensive use case plans by breaking down requirements into tasks and assigning the right agents. It highlights unavailable functionalities. If a task cannot be performed by an available agent, the planner agent suggests creating a new agent with specific capabilities.



aiforcepm

Python code generation

Planner: Completed

I've created a development plan for the Python code generation and reviewed the agents available on the platform. The process will have:\

Python code Generation Agent will generate Python code from user stories.\
User Story Generator will generate user stories.\
Push to Jira will push user stories to Jira.\
Requirements Generator Agent will generate complete PRD requirements for the user query.\
Bug analyser will analyze bugs.\
Recommend an assignee will recommend an assignee.\
FAQ Update Agent will update FAQs.- Please review the agents and

About Agent
Generates Python code from user stories

Model
Nvidia llama

Prompt
Python code Generation

RAG
Python coding guidelines

Tools

4.1.4 Interactive Chat

The planner agent lets you refine the use case through interactive chat. Changes made through chat are reflected in the updated workflow.You can modify the requirement and interact with the use case workflow through interactive chat. You can input text directly or upload files thereby providing instructions or information in different formats.

You can upload files using the # Select file. Type # in the chat window and an upload window appears. The upload sources can be:

- Local: Files from your local machine
- AI Force Repository: Uploaded files from the AI Force repository
- External Repositories: Files from repositories like AWS DevOps and ServiceNow. These repositories are integrated through connectors with the AI Force platform.

The uploaded files are session-specific only and are not saved in the AI Force repository. Once the file is uploaded and the chat is executed, it means that the generated output has considered the uploaded files.

4.1.5 Agent Team – A Visual Representation

There is a visual representation of the Agent Team associated with a workflow. Agents are listed in the exact order in which they execute tasks within the workflow plan. Each agent is represented by a clickable tile, enabling you to view the agent definitions and responsibilities in detail. The first agent in each workflow is the team leader. The team leader is responsible for:

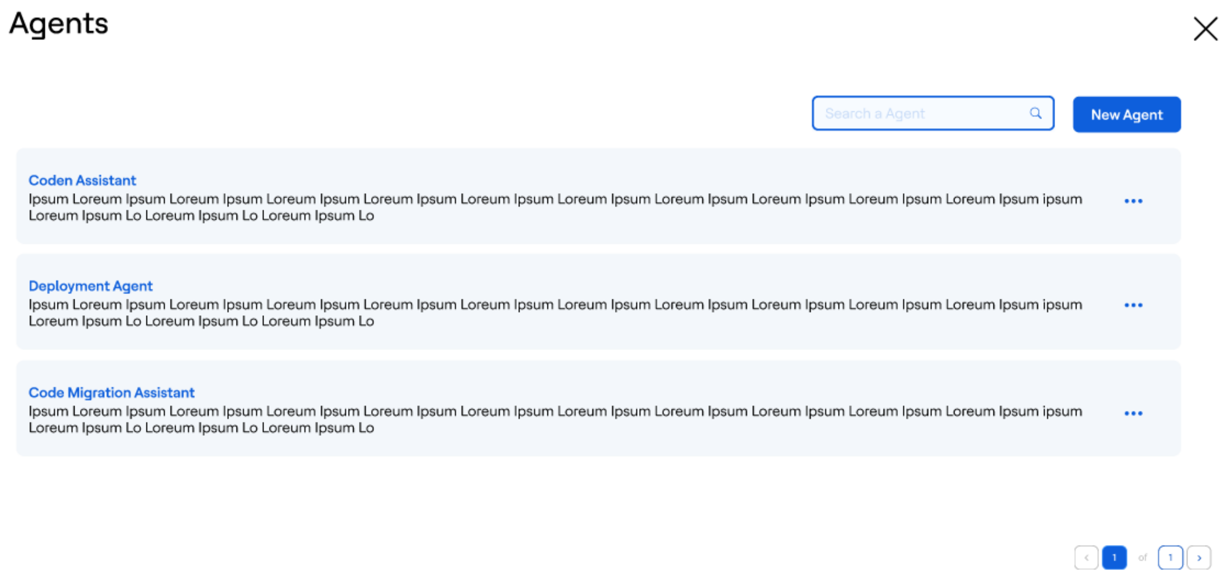
- Collecting initial user input and kicking off the process
- Orchestrating the workflow execution according to the plan generated by the planner agent during design time

Click an agent tile to view the definition panel of the agent. The definition panel displays:

- The definition of an agent
- The model being used
- Prompts, RAG pipelines, and Tools associated with the agent
- Evaluation report buttons for Prompts, RAG pipelines, and Agents
- A Delete button that allows you to remove the agent from the workflow

4.1.6 Adding and Deleting Agents

To add new agents to the workflow, click the **+** sign next to Agents. All the Agents present in the AI Force platform are listed with the Agent Name and a brief description. You can search for agents based on keywords. There is an Action Ellipses button against the description of each agent.



Coden Assistant
Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum ipsum Loreum Ipsum Lo Loreum Ipsum Lo Loreum Ipsum Lo

Deployment Agent
Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum ipsum Loreum Ipsum Lo Loreum Ipsum Lo Loreum Ipsum Lo

Code Migration Assistant
Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum ipsum Loreum Ipsum Lo Loreum Ipsum Lo Loreum Ipsum Lo

To add a particular agent, select the agent, click the ellipses, and click **Add**. That agent is added to the workflow. If you want to create a new agent, click **New Agent**. You will be taken to the New Agent page of the Agentic AI Studio. You can enter the details of the new agent, evaluate and publish it. Once it appears in the Agent Garden, you can add the agent to the use case workflow.

You can save the use case workflow as a draft at any point. The workflow details entered till that point will be saved as a draft. When you click Save as Draft for the first time a Name and Description fields appear. Enter a name for the use case and enter a brief description and click Save. When you click the Save as Draft subsequently, the new draft workflow overwrites the existing draft. The saved draft is available under the Draft Use Cases list.

4.1.7 Test Workflow

Once you are good with the workflow, click **Test Workflow**

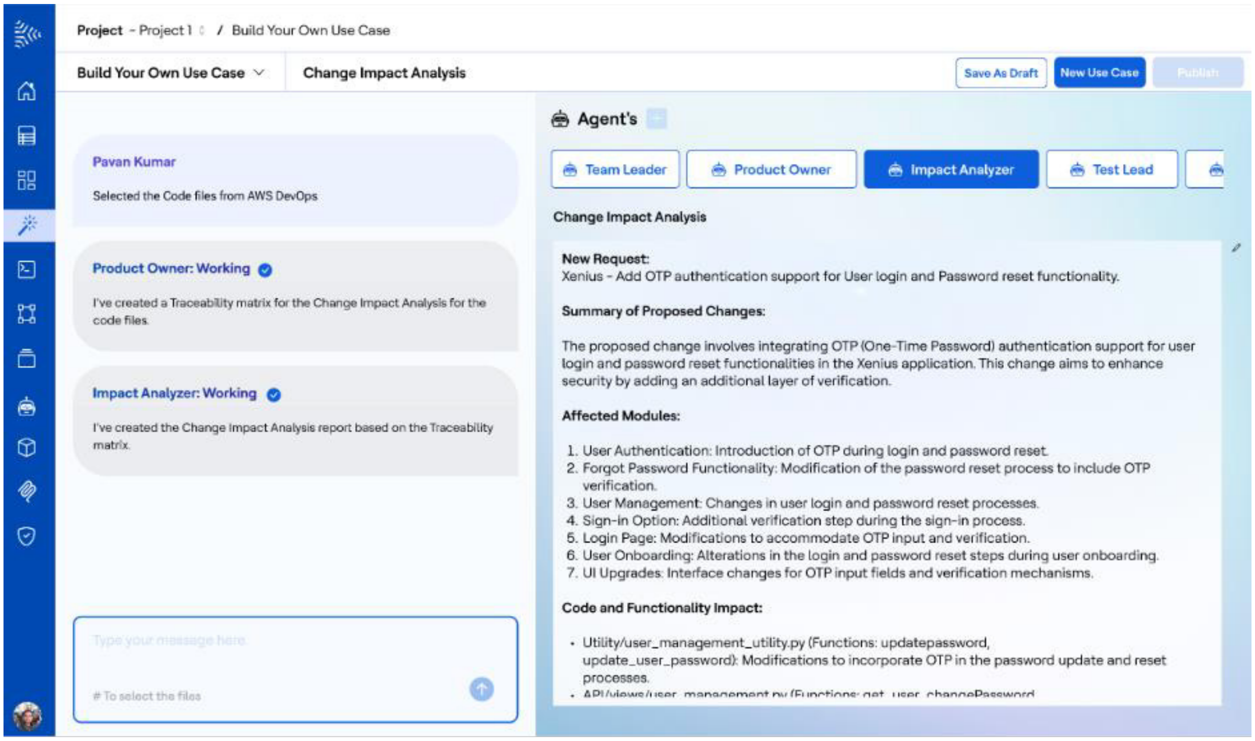
4.1.7.1 Workflow Execution

The configured agentic workflow executes. The process begins with the Team Leader Agent, which prompts you for necessary inputs. Upon receiving valid input the team leader initiates the execution, and the workflow proceeds sequentially through all assigned agents.

Some important points to note are:

- Agents perform tasks in the order defined in the workflow plan.
- Each agent has a dedicated output window.

- Once an agent completes its task, its output is displayed in its respective output window.
- The Agent Team panel shows agents in execution order, starting with the Team Leader.
- Each agent tile is clickable. Clicking displays the output window of that agent.
- A common chat feed displays real-time updates from each agent, showing what each is doing as the execution progresses.



Pavan Kumar

Selected the Code files from AWS DevOps

Product Owner: Working

I've created a Traceability matrix for the Change Impact Analysis for the code files.

Impact Analyzer: Working

I've created the Change Impact Analysis report based on the Traceability matrix.

Change Impact Analysis

New Request:
Xenius - Add OTP authentication support for User login and Password reset functionality.

Summary of Proposed Changes:

The proposed change involves integrating OTP (One-Time Password) authentication support for user login and password reset functionalities in the Xenius application. This change aims to enhance security by adding an additional layer of verification.

Affected Modules:

1. User Authentication: Introduction of OTP during login and password reset.
2. Forgot Password Functionality: Modification of the password reset process to include OTP verification.
3. User Management: Changes in user login and password reset processes.
4. Sign-in Option: Additional verification step during the sign-in process.
5. Login Page: Modifications to accommodate OTP input and verification.
6. User Onboarding: Alterations in the login and password reset steps during user onboarding.
7. UI Upgrades: Interface changes for OTP input fields and verification mechanisms.

Code and Functionality Impact:

- Utility/user_management_utility.py (Functions: updatepassword, update_user_password): Modifications to incorporate OTP in the password update and reset processes.
- API/views/user_management.py (Functions: get_user, changePassword

4.1.7.2 Human in the Loop

There is a Human in the Loop (HITL) capability during the Agentic Workflow execution.

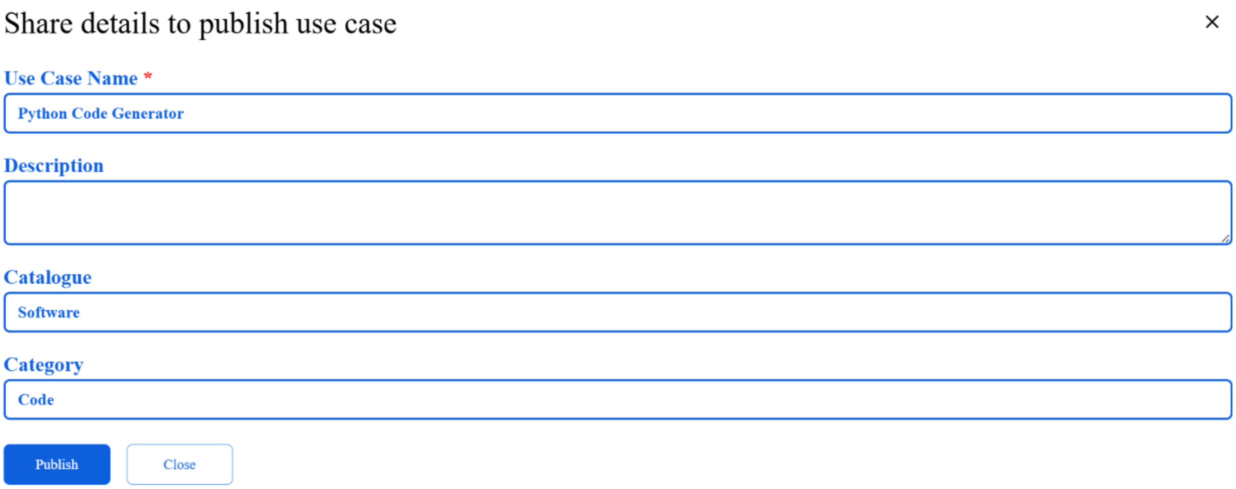
HITL is enabled in the following scenarios:

- While creating an agent, if the Human Input Mode is enabled, then the output of that agent is subject to manual review and approval.
- During a use case execution, when an agent completes its task or before a tool execution, if HITL is enabled then:
  - Generated output or planned tool execution is shown in the agent output window along with an Edit icon. You can click the Edit icon to edit the output manually.

    - You can also give feedback in the main chat input and rerun the task.
- Once satisfied, you can click Proceed to continue workflow execution.
- The HITL feature enables human oversight at critical points without interrupting the full automation flow.

4.1.7.3 Publish the Workflow

If you are good with the workflow output, you can publish the use case to the Use Case catalogue so that it becomes available to other users. Click **Publish**. The Share Details to Publish Use Case page appears.



Share details to publish use case

Use Case Name *: Python Code Generator

Description:

Catalogue: Software

Category: Code

Enter Use Case Name, a Description of the use case, select the Catalogue in which the use case is to be published, and select the Category in which the use case is to be published. Click **Publish**. You can view the use case in the specified category of the specified catalogue.

4.2 Graphical Pattern

The **Agentic DAG Workflow Builder** enables users to design complex, deterministic multi-agent automations using a **Directed Acyclic Graph (DAG)** structure. A DAG represents a workflow as a series of connected nodes where execution always flows forward—never looping back—ensuring predictable and controlled outcomes. This model is especially effective for orchestrating multi-agent systems that require sequential, parallel, or conditional logic.

You can create a DAG-based workflow by selecting **Graphical Pattern** from the **Select Pattern** dropdown while building a new use case. This pattern opens a visual canvas where workflows are constructed using specialized node types, each representing a specific action, agent, or control structure.

By leveraging this graphical workflow builder, you can:

- Design linear (sequential) processing pipelines
- Build parallel branches for concurrent execution
- Introduce conditional logic for decision-based routing
- Combine multiple agents and tools into a unified flow
- Maintain full visibility into execution order and data movement

The node-based design ensures that you can explicitly define which node runs next, how data flows between nodes, and how complex multi-agent tasks should behave end to end. This visual, structured approach makes even advanced automation scenarios intuitive, repeatable, and easy to maintain.

Agentic DAG workflows are ideal when you need to build structured, repeatable, and multi-step AI processes that must follow a clear sequence or decision path. As a DAG enforces a directed, non-cyclic flow, it ensures every step of the automation happens in the correct order—making it perfect for complex use cases such as document processing, multi-agent reasoning, conditional branching, or multi-stage data transformation.

Use an Agentic DAG workflow when:

- You want a visual, predictable, and controllable automation flow.
- Your process involves multiple agents, each performing different tasks that must run in a defined order.
- You need conditional logic, loops, or routing decisions within the workflow.

Overall, DAG workflows give you both flexibility and precision, making them ideal for building reliable AI-powered pipelines without writing code.

4.2.1 Planner Agent

The Planner Agent is designed to help you quickly create a new DAG workflow without needing to manually build every node from scratch. It interprets your instructions, generates the workflow structure, and provides an editable starting point that you can refine further through chat or direct graph edits.

4.2.1.1 Starting a New Workflow

To start a new workflow:

In the Describe the Use Case you'd like to build using AI Force input box type a natural language description of what you want the system to build. An example would be, "Read a PRD, generate Epics, then create user stories for each Epic.

Click the **Pattern** dropdown and select **Graphical Pattern**. This selection means that you want to build a DAG-style workflow using visual nodes.

Click the **up arrow** (submit button) to proceed.

4.2.1.2 Refining the Workflow Through Chat

You can continue interacting with the Planner Agent in the left panel. You can:

- Add new steps
- Modify node behaviors
- Change the order of operations
- Request loops, conditional branches, tool integrations, etc.

Just type your changes in natural language (for example, *After generating user stories, add a QA Review agent*), and the Planner will update the workflow on the canvas.

This conversational refinement makes it easy for new users to evolve their workflows without needing full knowledge of nodes or control logic.

4.2.1.3 Editing Directly on the Canvas

If you prefer manual editing, use the Graphical Pattern canvas:

- Move nodes
- Add new nodes using the *New Node* button
- Connect or disconnect nodes
- Adjust parameters by clicking a node
- Zoom in/out using the +/– controls

Changes made on the canvas are immediately reflected in the workflow configuration.

4.2.1.4 Hybrid Workflow Building

Using the planner agent and the canvas gives you the ability for hybrid workflow building. AI Force 2.0 gives you the flexibility to:

- Let the Planner Agent design the workflow automatically,
- Use conversation to refine the structure further, or manually fine-tune everything on the visual canvas.

This hybrid approach ensures both beginners and advanced users can build complex agentic workflows with minimal effort.

4.2.2 Workflow Nodes

Nodes are the fundamental building blocks of a DAG workflow in AI Force 2.0. Each node represents a specific action, decision, or operation. The workflow moves from one node to another based on the connections defined by you, enabling sequential, conditional, and parallel flows.

There are six node types available:

1. Start (Trigger) Node
2. Agentic Node
3. Router Node
4. For Loop Node
5. While Loop Node
6. Tool Node

You can open a node configuration by clicking on an existing node in the canvas or creating a new node using the New Node button.

4.2.2.1 Node Basics

Although nodes perform different functions, several configuration elements are common across all node types.

Node Type

A dropdown is available to select the node type (Agentic, Router, For Loop, While Loop, Tool).
The Start Node is always present and is the only node with type *Trigger*.

Node Name

A unique name that identifies the node within the workflow. Node names must be unique as they are referenced in other nodes and routes.

Execute After

(Available for all nodes except the Start node).

This section determines the flow of execution. You can specify one or more nodes that must finish before this node runs.

Single dependency

Node runs after one specific node.

Multiple dependencies

You can add additional Execute After entries.

AND Logic

The node executes only after *all* selected nodes are completed.

OR Logic

The node executes when *any* one of the selected nodes completes. This mechanism allows you to design sequential, and parallel paths.

4.2.2.2 Node Types

Below are details of each node type, its purpose, and its unique configuration fields.

Start Node (Trigger Node)
The Start node is the entry point of every workflow. Execution begins only after the user provides the initial input in chat.

Additional Configurations:
Display Text
The message shown to the user when initiating the workflow.
Typical use: instructing the user to upload a document, provide a query, etc.
Output
The variable name that stores the input provided by the user.
Downstream nodes can reference this variable to access the user's initial input.
Example:
prd_document → this value becomes accessible to other nodes as {prd_document}.

Agentic Node

An Agentic node executes one of the published agents from the AI Force Agent Garden.

Use this node whenever a workflow step requires autonomous reasoning or generation by an AI agent.

Additional Configurations:

Agent: Dropdown listing all published agents. The selected agent will execute when this node is triggered.

Task: A free-text field describing what the agent should accomplish at this node.

Input: The actual input sent to the agent.
You can:

- Write static text
- Pass workflow variables (for example, {prd_document})
- Combine static and dynamic values

Output

The variable name where the agent generated output will be stored for downstream use.

Router Node

A Router Node is used for conditional branching. It evaluates conditions and sends the workflow into one or more paths based on the results.

Key Concepts:

- A Router node can contain multiple sections.
- Each section represents a possible path the workflow may follow.
- Each section contains conditions that determine whether that path should be taken.
- Multiple sections can be true simultaneously and the workflow follows all matching paths.
- A default path is used if none of the section conditions are satisfied.

Additional Configurations:

Sections**:** You can add unlimited sections using Add Section.

Each section includes:
Conditions input as

- AND/OR - to combine multiple conditions
- Field 1 - variable from previous nodes
- Operator – operators such as =, !=, >, <, and contains)
- Value - value to compare against

Output

The name of the path created by this section.

Downstream Node Reference

In Execute After, downstream nodes can reference router output as:

<Router Node Name (Section Name)>

This enables you to attach nodes to specific conditional paths.

For Loop Node

A For Loop Node allows you to repeat a part of the workflow for each item in a list. This is ideal for batch processing and iterating over collections.

Additional Configurations:

Items List (Input)

A variable or static list representing the items to loop through.
For example, {epics_list}

Loop Behavior

The For Loop has two output paths:

1. Loop - executed once for each item
2. Done - executed after all iterations are completed

Downstream nodes can connect to either path.

While Loop Node

A While Loop Node repeats workflow steps as long as a condition remains true. Useful when the number of iterations is not known in advance.

Additional Configurations:

Loop Condition

You can define the condition using:

- Field 1 - variable to evaluate
- Operator – operators such as =, !=, >, and <)
- Value - target threshold
- AND/OR - for combining multiple conditions

Loop / Done Paths

Similar to the For Loop:

- Loop executes repeatedly while the condition is satisfied
- Done executes when the condition becomes false

Tool Node

A Tool Node executes a selected tool from the Tool Library or an MCP server configured in MCP Studio. A Tool Node enables seamless integration of API calls, automations, data processing, and external services.

Additional Configurations:

Tool

A dropdown listing available tools (local tools + MCP tools).

Tool Input Fields

The form adapts based on the function selected.

Output:

The variable name where the tool result will be stored for use by downstream nodes.

4.2.3 Workflow Execution

4.2.3.1 Starting the Workflow

When a workflow is launched, the system displays the Display Text defined in the Start node.
This display text appears in the chat window and acts as the initial prompt to guide

you, for example, asking you to upload a document or provide a query. After you enter your response in the chat workflow, execution begins.

4.2.3.2 Execution Progress

The workflow follows the structure defined in the DAG:

- Nodes execute sequentially, conditionally, or in parallel depending on how the “Execute After” settings are configured.

  Execution continues node by node until all valid paths in the DAG have been completed or a node requires human confirmation

4.2.3.3 Human-in-the-Loop During Execution

If Human-in-the-Loop (HITL) is enabled for an Agentic AI, the system pauses execution at that node.

During this pause:

- The agent output is shown to you.
- The system waits for you to review, modify, or approve the results.
- Once you confirm, the workflow resumes automatically and continues with the next node.

This HITL ensures workflows can maintain both automation and control where needed.

4.2.3.4 Completion and Restarting of the Workflow

After all nodes have finished executing:

- The workflow session reaches its end state.
- The system once again displays the Start node Display Text, prompting you with the same message shown at the beginning.

  At this point, you can:

1. Provide new input to run the entire workflow again
2. Close the session if no further executions are needed

This loop allows repeated use of the same workflow without needing to rebuild or reselect it each time.

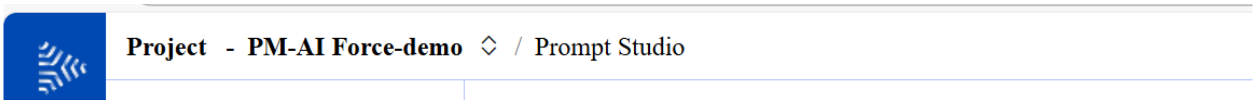
5 Prompt Studio

Prompt Studio is a centralized workspace that allows you to create, test, evaluate, and manage prompts for your AI agents. It provides a structured environment for prompt engineering-enabling you to design effective prompts, fine-tune them through evaluations, and publish them for wider use within a project.

Within Prompt Studio, you can create prompts using different LLM models, leverage the **Help Me Write** feature for guided prompt generation, and incorporate variables or input-output examples to make prompts more dynamic and context-aware. Once created, prompts can be tested in real time to review model responses, evaluated using configurable evaluators and datasets, and optimized for performance before being published to the **Prompt Library**. The studio also enables easy management of prompts, including options to edit, duplicate, delete, or associate them with Model Context Protocol (MCP) servers. Overall, Prompt Studio simplifies the end-to-end lifecycle of prompt development- ensuring consistency, quality, and reusability across all projects.

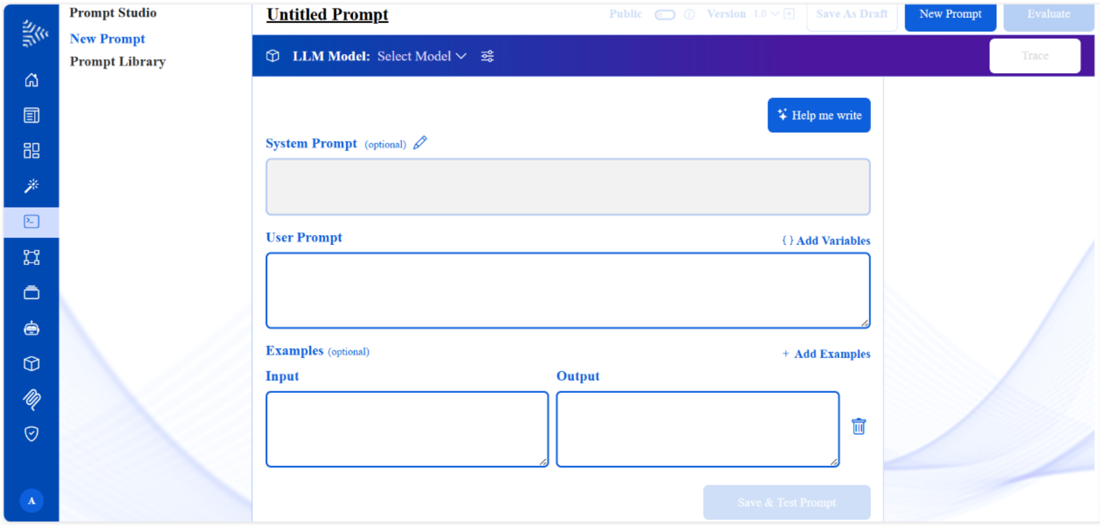
5.1 New Prompt

1. Click ▣ (the Prompt icon) from the Menu bar. The Prompt Studio page appears with the default project selected. Select the project for which you want to manage the prompts by clicking on the drop-down arrow next to the project name.

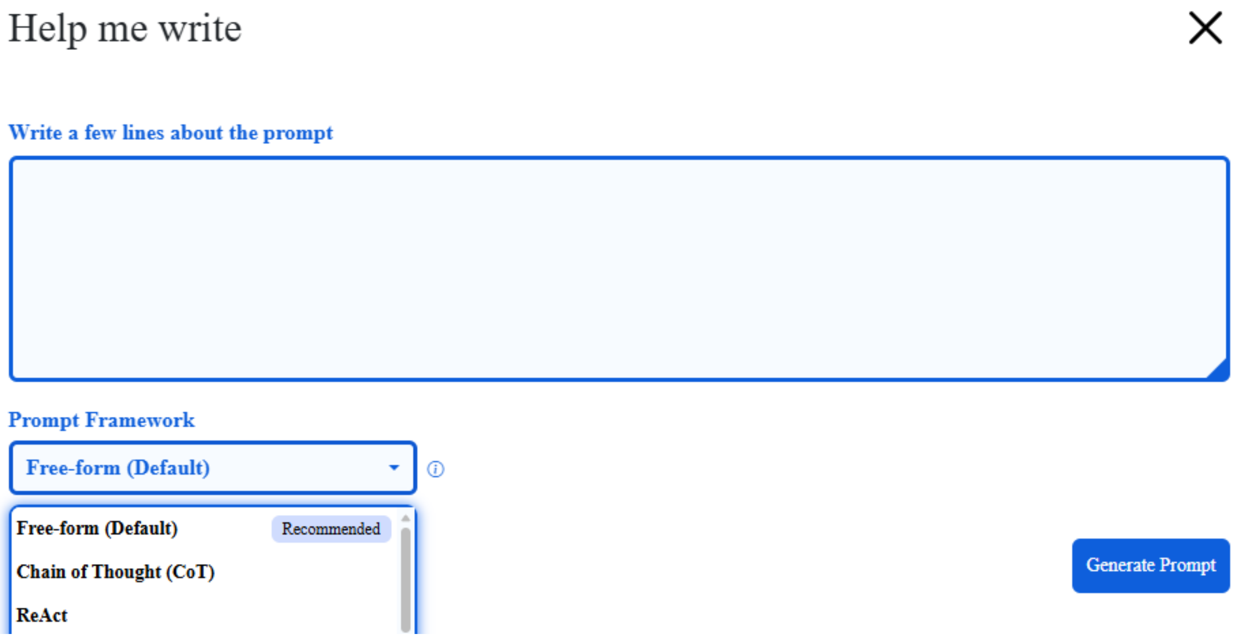


Project - PM-AI Force-demo ◇ / Prompt Studio

The Prompt Studio page opens at the New Prompt option.



1. Click Untitled Prompt to name the prompt.
2. Select the LLM Model using the Select Model drop-down arrow. The default LLM model is selected.
3. Write the System and User Prompts. If you need help in writing the User Prompt, click **Help Me Write**. The Help Me Write page appears.



If you want to use a specific technique or framework for your prompts, you can select from the Prompt Framework dropdown menu. Hover your mouse over the ⓘ icon to get the details of each framework.

If you do not specify any framework, based on the input given in Write a few lines about the prompt, the system will recommend the best suited framework. You can accept the system-recommended framework, go with the default framework, which is Free Form, or select any other framework of your choice.

When the system and user prompt is generated using a particular framework, the name of the framework also shows up in the next screen.

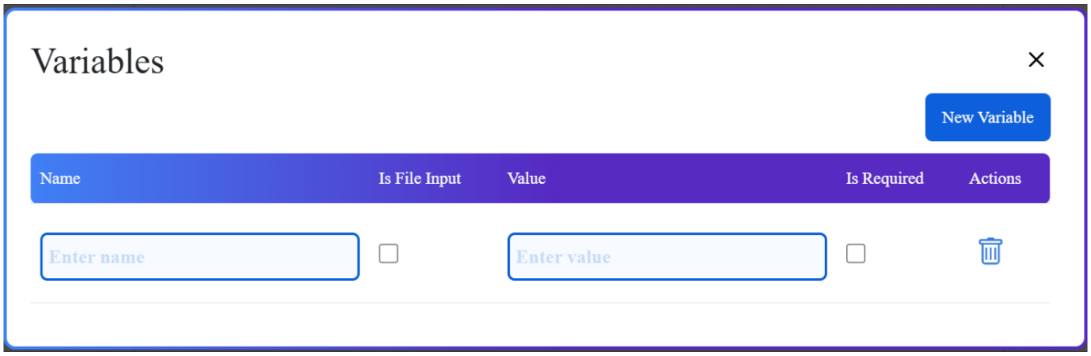
Enter the text required for the prompt and click **Generate Prompt**. Both the System prompt and User Prompt are generated. If you are satisfied with the generated prompts, click **Insert**. The generated prompts are inserted into the System and User Prompt fields.

If you are not satisfied with the generated prompt, click **Re-generate** and go through the process one more time.

4. Click **Add Variables** to add variables to the prompt. The Variables page appears.

   Variables in a prompt act as placeholders that can be replaced at runtime with real values such as user inputs, system data, or context-specific information.

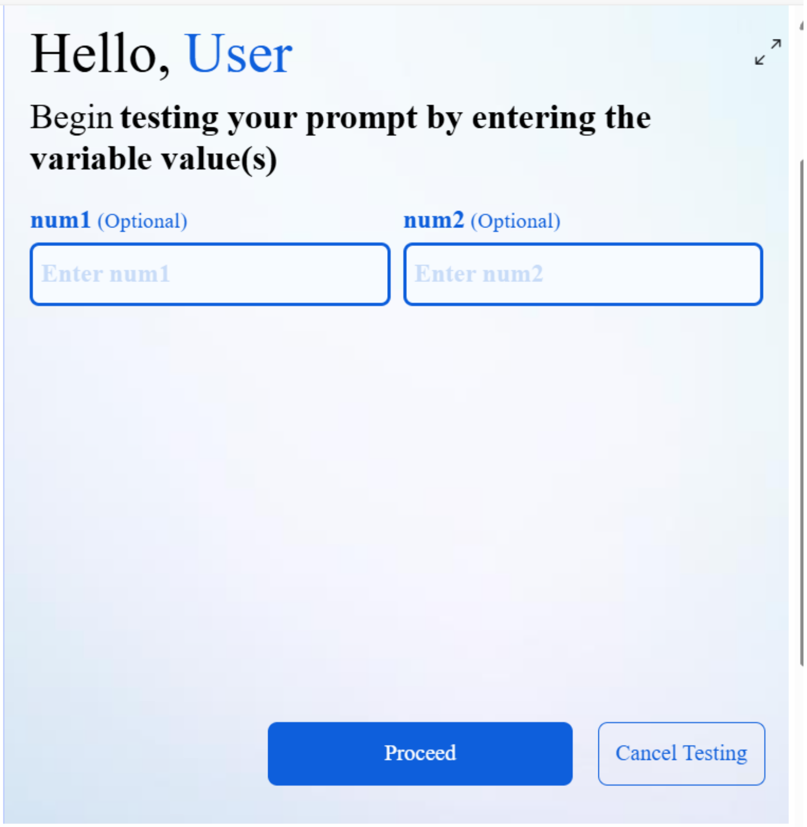
   Click **New Variable** in the Variables page. The Variable fields appear.



   Enter the Name of the variable. Select the Is File Input checkbox, if the variable is input from a file. Enter the value of the variable. Select the Is Required checkbox if the variable is a mandatory field.

   Keep clicking **New Variable** as many times as the number of variables you wish to enter. You can also enter new variables directly in the User Prompt by using curly brackets ({}). Once you have finished entering the variables, close the page. The variables get stored in the prompt.

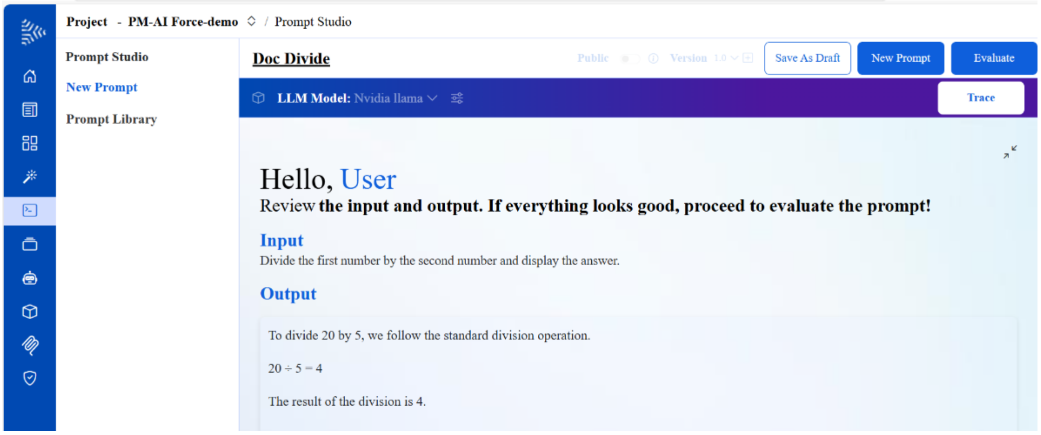
5. If you want to enter examples, enter examples of Input and Output in the respective fields. Examples act as training hints within the prompt, guiding the model toward the desired format, tone, and level of detail. Click **Add Examples** to enter more examples.
6. Click **Save & Test Prompt**. The Save as Draft page appears. Enter the name of the prompt (if you have not already entered it), write a few lines about the prompt, and click **Save**.
7. Click **Save & Test Prompt** again. The prompt is now saved and the prompt test page appears



Hello, User

Begin **testing your prompt by entering the variable value(s)**

8. Enter the variable values, if required, then click **Proceed**. The Results page appears. You are required to review the input and output, and if found to be good, you can proceed to evaluate the prompt.



Hello, User

Review **the input and output. If everything looks good, proceed to evaluate the prompt!**

Input

Divide the first number by the second number and display the answer.

Output

To divide 20 by 5, we follow the standard division operation.

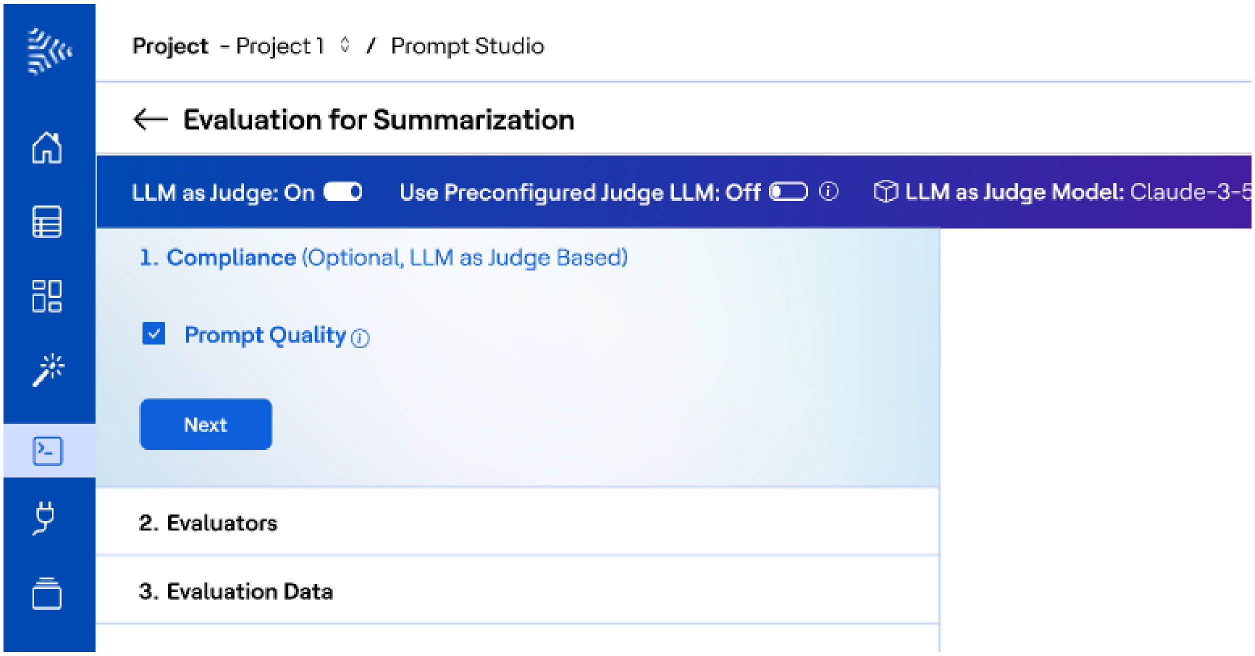
20 ÷ 5 = 4

The result of the division is 4.

If the input and output look good, click **Evaluate**.

9. The Evaluation for <prompt name> page appears.
10. By default, LLM as Judge is set to Off, Use Preconfigured LLM is set to Off.
11. Select the Model Judge if LLM as Judge is configured On.

12. You can select the Compliance control implementation. This will validate your prompt against the configured compliance controls and provide the rephrased prompt that is in adherence with the configured compliance controls.



Project - Project 1 / Prompt Studio

← Evaluation for Summarization

LLM as Judge: On | Use Preconfigured Judge LLM: Off ⓘ | LLM as Judge Model: Claude-3-5

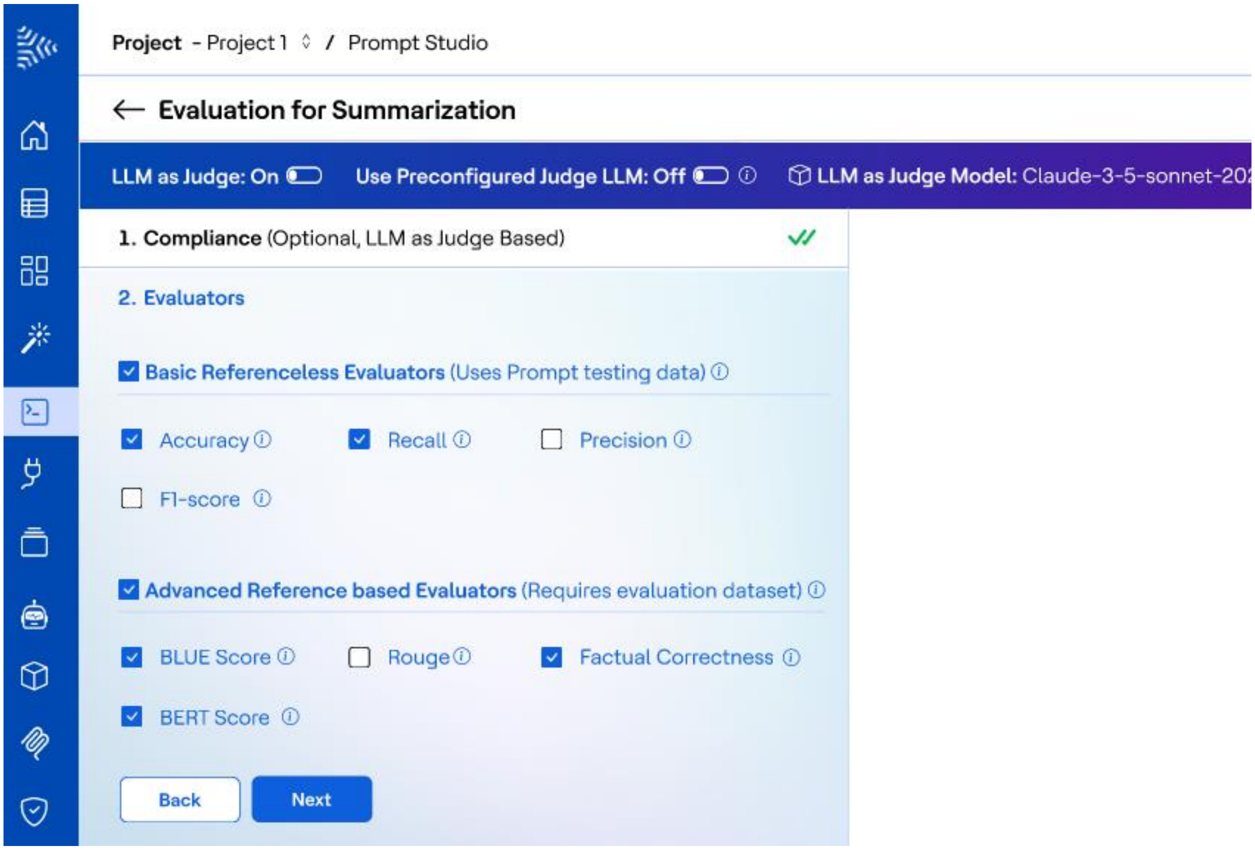
1. Compliance (Optional, LLM as Judge Based)

☑ Prompt Quality ⓘ

Next

2. Evaluators

3. Evaluation Data



Project - Project 1 / Prompt Studio

← Evaluation for Summarization

LLM as Judge: On | Use Preconfigured Judge LLM: Off ⓘ | LLM as Judge Model: Claude-3-5-sonnet-202

1. Compliance (Optional, LLM as Judge Based) ✓✓

2. Evaluators

☑ Basic Referenceless Evaluators (Uses Prompt testing data) ⓘ

☑ Accuracy ⓘ ☑ Recall ⓘ □ Precision ⓘ

□ F1-score ⓘ

☑ Advanced Reference based Evaluators (Requires evaluation dataset) ⓘ

☑ BLUE Score ⓘ □ Rouge ⓘ ☑ Factual Correctness ⓘ

☑ BERT Score ⓘ

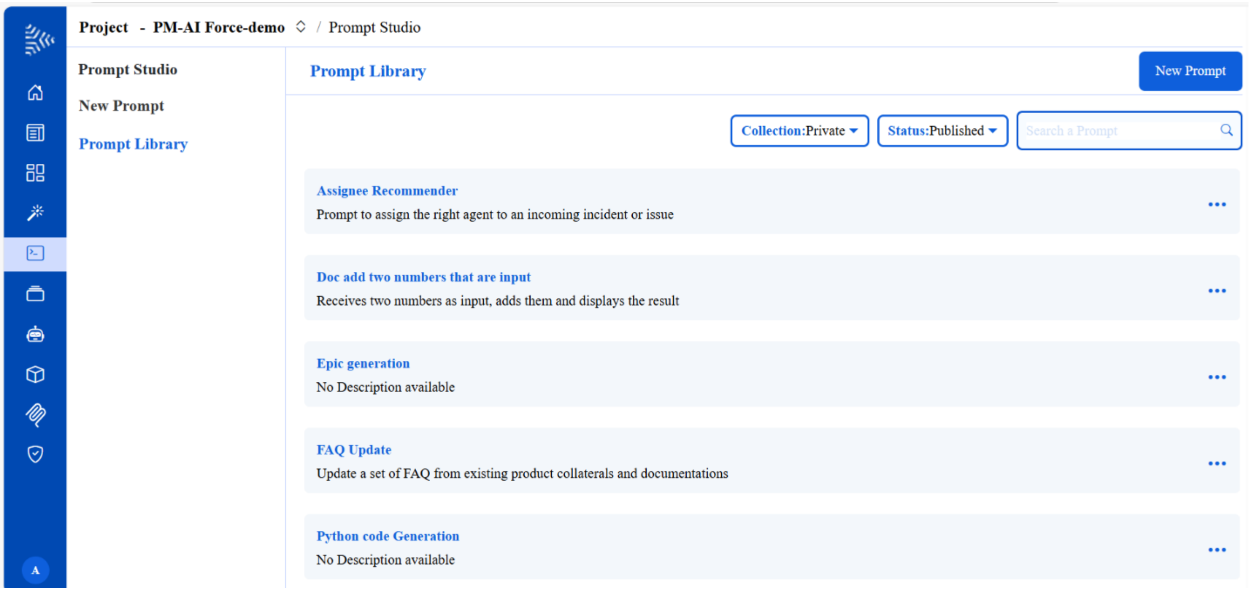
Back Next

13. Select the Evaluators needed for the Evaluation. The evaluators have been split into 2 categories – Referenceless (that don't need evaluation datasets and will use prompt testing details) and reference-based (that need evaluation datasets).
14. By default, all the Evaluators are selected. Hover the mouse over ⓘ to view details of the Evaluator. Unselect the Evaluators that you do not need. Click **Next**.
15. Select the Datasets needed for each reference based Evaluator. Click **Start Evaluation**.
16. Once the Evaluation is completed, the Publish button is enabled. You can **Publish** the prompt to the Prompt Library.
17. Click **Trace** to view details of the LLM call that was made during the prompt test. You can view details such as Latency, Cost, Total Usage, and a preview of the Input, Output, and Metadata.

5.2 Prompt Library

The Prompt Library displays all the prompts of the project. Prompts that have been published or prompts that are in Draft status can be displayed.

1. Click **Prompt Library**. The Prompt Library page appears.



Project - PM-AI Force-demo / Prompt Studio

Prompt Studio
New Prompt
Prompt Library

Prompt Library

New Prompt

Collection:Private ▾ Status:Published ▾ Search a Prompt

Assignee Recommender
Prompt to assign the right agent to an incoming incident or issue

Doc add two numbers that are input
Receives two numbers as input, adds them and displays the result

Epic generation
No Description available

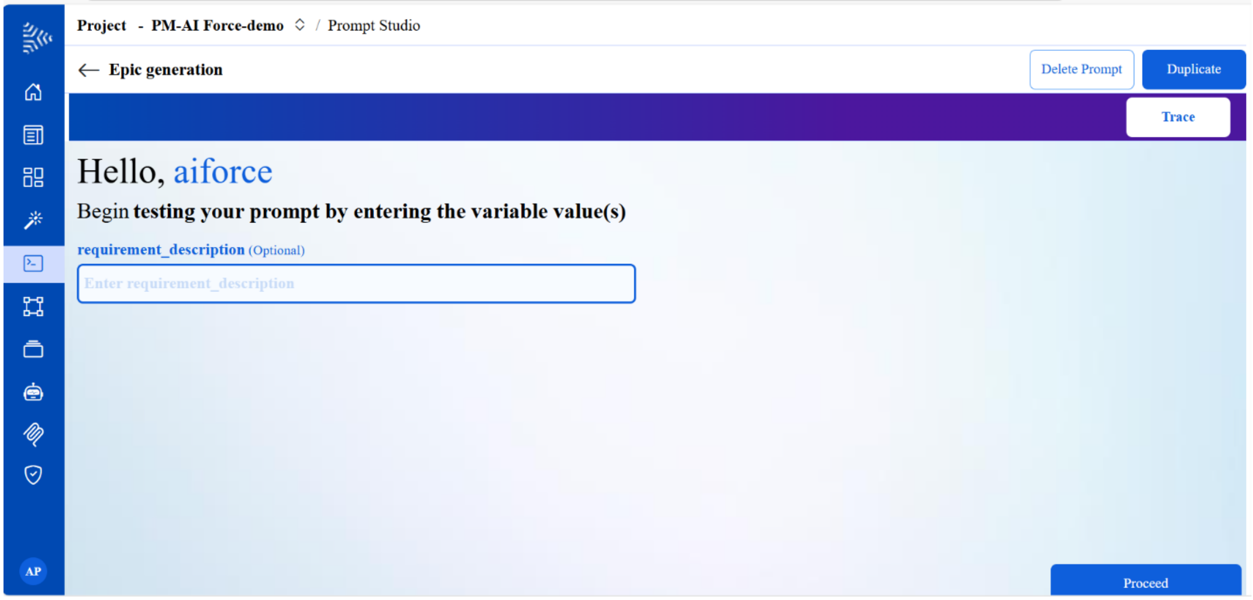
FAQ Update
Update a set of FAQ from existing product collaterals and documentations

Python code Generation
No Description available

2. You can select a prompt in the Prompt Library and:
   - Try out the prompt
   - Edit the prompt
   - Add or remove the prompt from the Model Context Protocol
   - View the Evaluation Report of the prompt
   - Create a duplicate of the prompt and make changes to it

- Delete the prompt

3. To try out a prompt, select the prompt and click the ellipses (...) at the right end of the row. Click **Try**. The prompt test screen appears.



Hello, aiforce

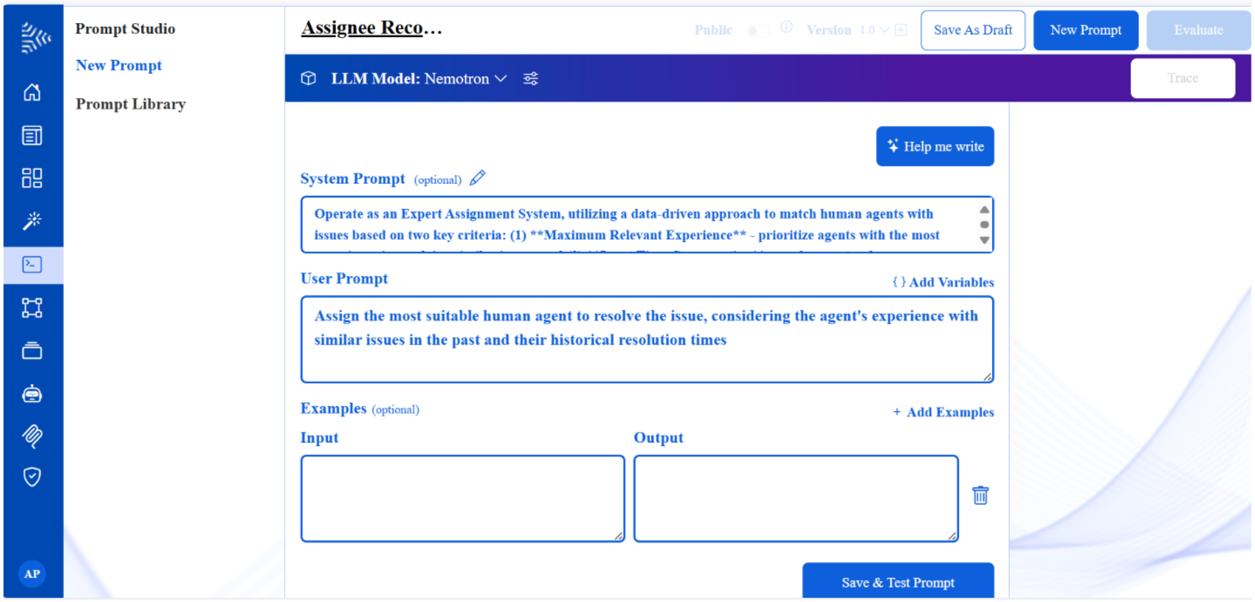
Begin testing your prompt by entering the variable value(s)

requirement_description (Optional)

Enter requirement_description

You can enter the variables and proceed to test the prompt and evaluate it. You can also create a duplicate of the prompt or delete the prompt from this page.

4. To edit a prompt, select the prompt and click the ellipses (...) at the right end of the row. The options are displayed. Click **Edit**. The New Prompt screen appears displaying details of the selected prompt.



LLM Model: Nemotron

System Prompt (optional)

Operate as an Expert Assignment System, utilizing a data-driven approach to match human agents with issues based on two key criteria: (1) **Maximum Relevant Experience** - prioritize agents with the most

User Prompt

Assign the most suitable human agent to resolve the issue, considering the agent's experience with similar issues in the past and their historical resolution times

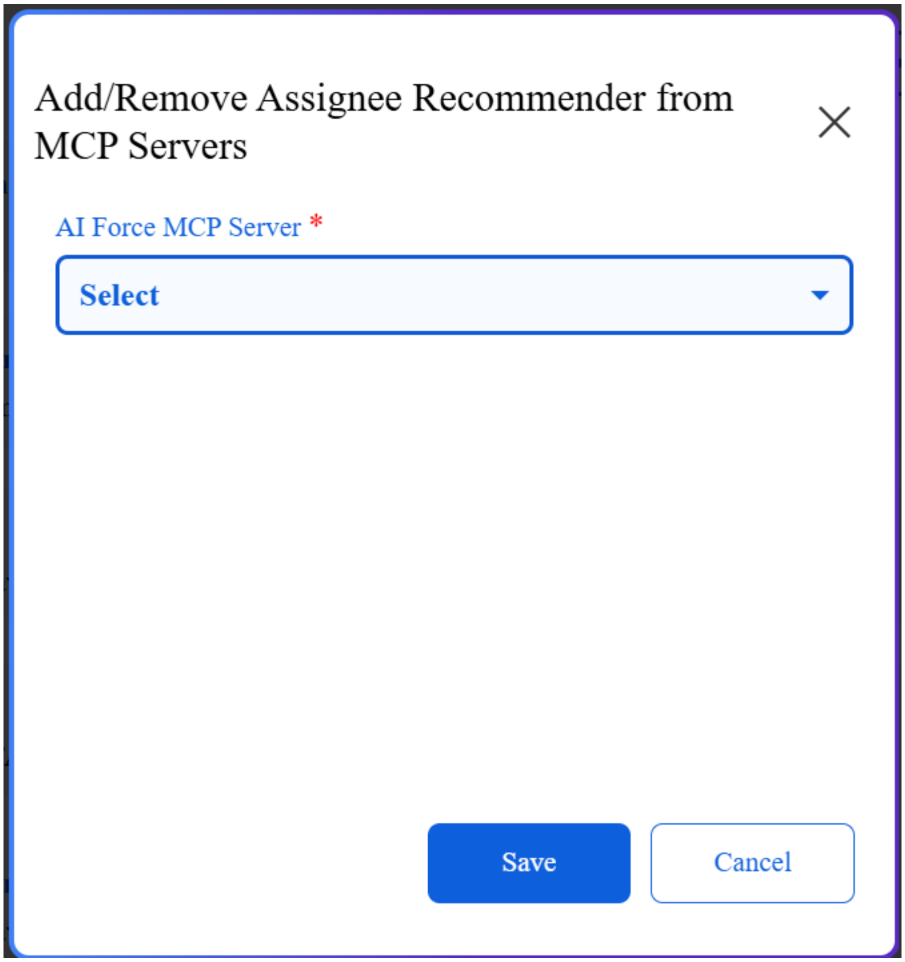
Examples (optional)

Input

Output

You can make changes to the prompt and **Save & Test** the prompt.

5. To add or remove the prompt from the MCP servers, select the prompt and click the ellipses (...) at the right end of the row. The options are displayed. Click **Add/Remove from MCP Servers**. The Add/Remove from MCP Servers page is displayed.

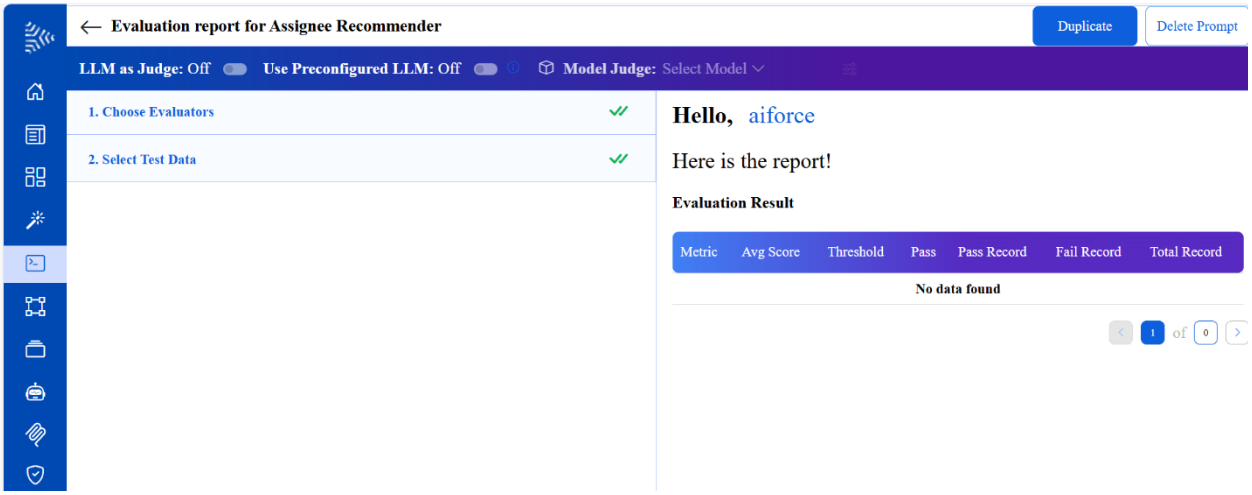


Add/Remove Assignee Recommender from MCP Servers

AI Force MCP Server *

Select the MCP server to which you want to add the prompt, or the MCP server from which you want to remove the prompt.

6. To view the evaluation report of a prompt, select the prompt, click the ellipses (...) at the right end of the row. The options are displayed. Click **Evaluation Report**. The Evaluation Report page appears.



Metric	Avg Score	Threshold	Pass	Pass Record	Fail Record	Total Record
No data found						

7. To duplicate a prompt, select the prompt, click the ellipses (...) at the right end of the row. The options are displayed. Click **Duplicate**. The Duplicate page appears asking for your confirmation to create a copy of the prompt. If you select Yes, The Duplicate Prompt page appears, asking you to enter a new name for the Duplicated prompt. Enter a new name and click **Duplicate**. The duplicated prompt appears in the Prompt Library.
8. To delete a prompt, select the prompt, click the ellipses (...) at the right end of the row. The options are displayed. Click **Delete**. The Delete confirmation page appears. If you click **Yes**, the prompt is deleted.

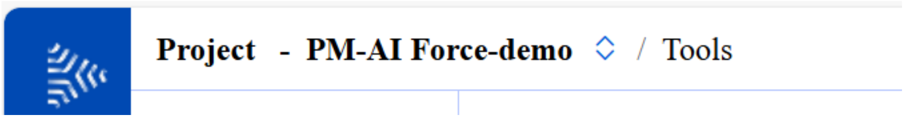
6 Tools Studio

Tools Studio is an integrated workspace that enables you to create, configure, test, and manage tools that can be used within AI projects and agents. It provides a flexible environment for building tools either through APIs or custom scripts, helping you extend the system capabilities and automate workflows efficiently. Using Tools Studio, you can design new tools by connecting to APIs via documentation URLs or Swagger files, or by generating custom Python functions through prompt-based code generation. Each tool can be configured with specific parameters, authentication methods, and input-output schemas to ensure smooth interaction with external systems or custom logic.

AI Force Tools option enables you to create and manage all the tools pertaining to a specific project in AI Force. You can create a new tool and view the tools in the Tool Library. You can select a tool in the Tool Library, edit it, configure the parameters of the tool, add or remove it from the MCP (Model Context Protocol), create a duplicate tool, or delete the tool.

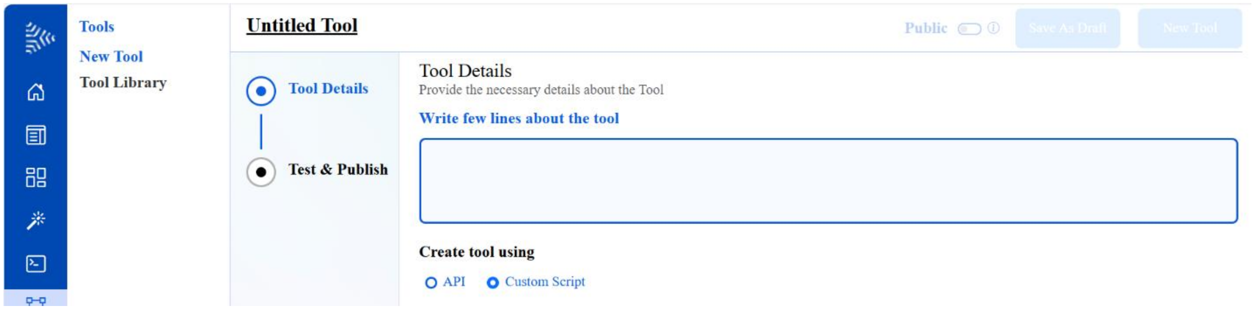
6.1 New Tool

1. Click (the Tools icon) from the Menu bar. The Tools page appears. The default project is auto selected. If you wish to manage the tools for another project, select the project by clicking on the drop-down arrow next to the project name.



Project - PM-AI Force-demo / Tools

The Tools page opens at the New Tool option.



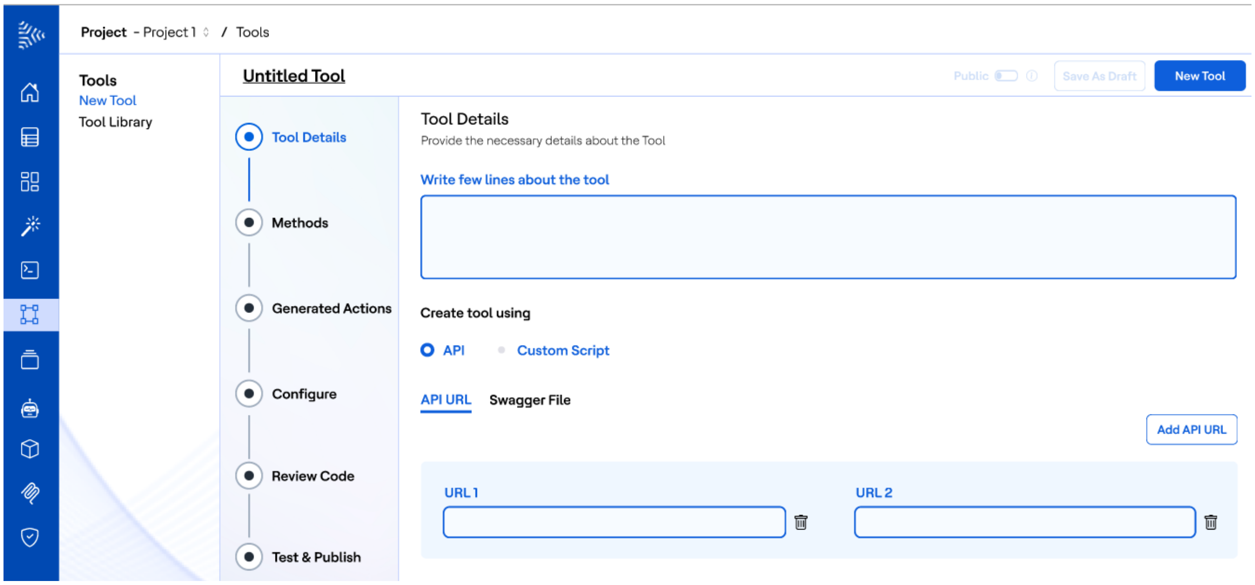
2. Click Untitled Tool to name the tool.
3. Write a few lines about the purpose of the tool.

A clear tool description helps agents understand the purpose of the tool and when to use it. They can choose the right action at the right time. A good description improves accuracy, avoids misuse, and makes workflows more reliable.

4. You can create a tool using API or Custom Script.

6.1.1 Using API

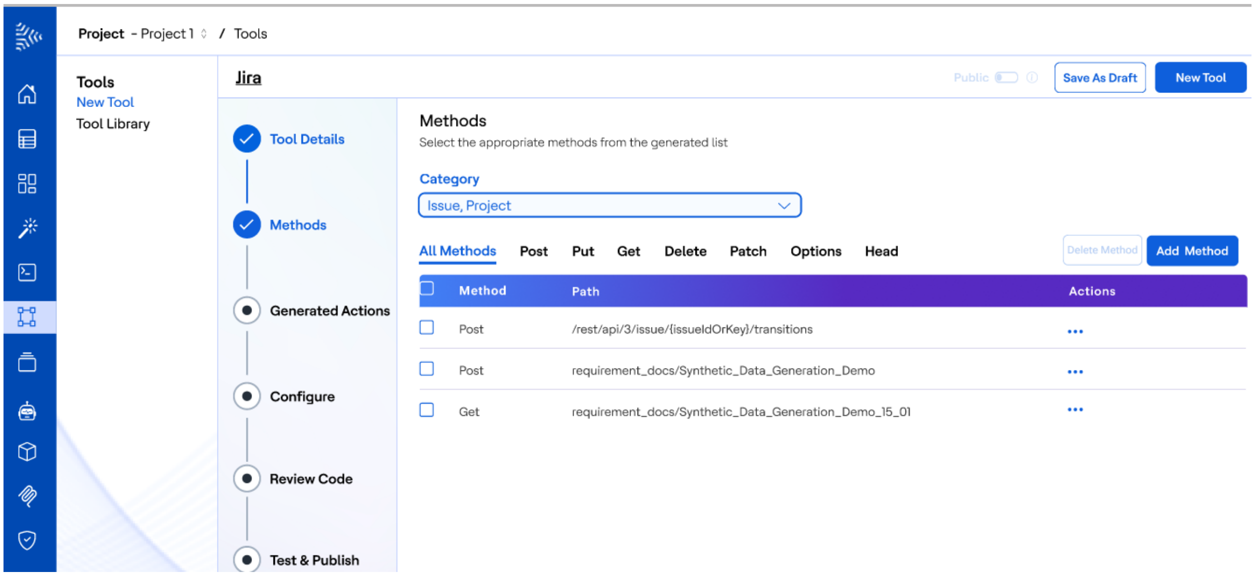
1. If you choose API as your option, you will need to enter API documentation URLs or upload Swagger documents.



Enter the API documentation URLs. To add more URLs click **Add API URL**. You can enter a maximum of five URLs. Click **Next**.

If you want to process offline API documentation, you can upload Swager documents in the .json or .yaml formats. Go to the Swagger file tab and drag and drop Swagger files or Click to Upload. You can upload a maximum of five Swagger documents and the maximum uploaded file size, in total, cannot exceed 20 MB. Click **Next**.

2. The document is fetched and parsed to extract all available API methods. The extracted methods are listed along with the corresponding API path.



Methods

Select the appropriate methods from the generated list

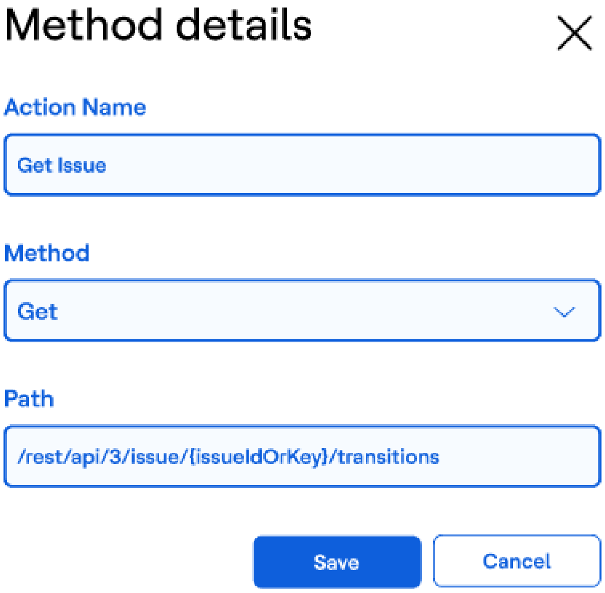
Category: Issue, Project

□	Method	Path	Actions
□	Post	/rest/api/3/issue/{issueIdOrKey}/transitions	•••
□	Post	requirement_docs/Synthetic_Data_Generation_Demo	•••
□	Get	requirement_docs/Synthetic_Data_Generation_Demo_15_01	•••

Note:

POST, PUT, GET, DELETE, PATCH, OPTIONS, and HEAD are the only methods that are allowed to be used.

3. To edit a method or the path, click the ellipses at the end of the row, and click Edit. When you have finished making the changes, click **Save**.



Action Name: Get Issue

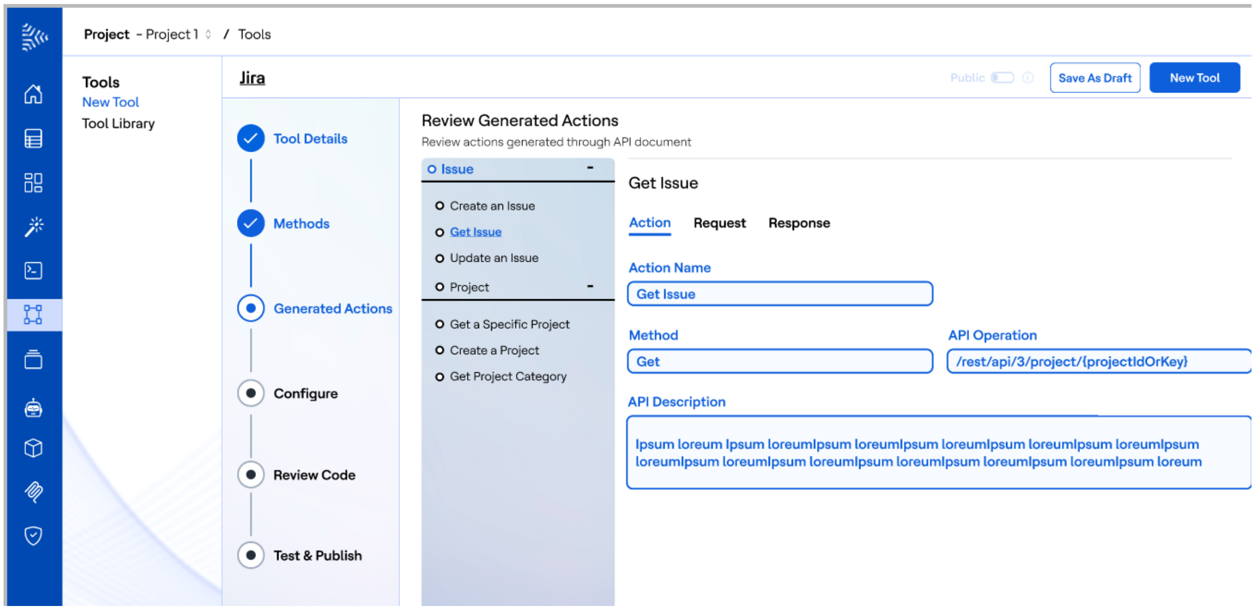
Method: Get

Path: /rest/api/3/issue/{issueIdOrKey}/transitions

4. To delete a method and path, click the ellipses at the end of the row, and click Delete. A confirmation page appears. Click **Yes**.
5. To add methods to the configuration, select the checkbox against the method. To select all the methods, you can use the Select All checkbox at the top.

To manually add methods to the configuration, click **Add Method**. Select the method from the dropdown menu and enter the path. Click **Save**.

6. The API configurations are customizable. You can review and edit the action, request, and response details of each selected method to ensure accuracy. Select the API method to be edited and click **Next**. The Review Generated Action page appears.



Review Generated Actions

Review actions generated through API document

Get Issue

Action Name: Get Issue

Method: Get

API Operation: /rest/api/3/project/{projectIdOrKey}

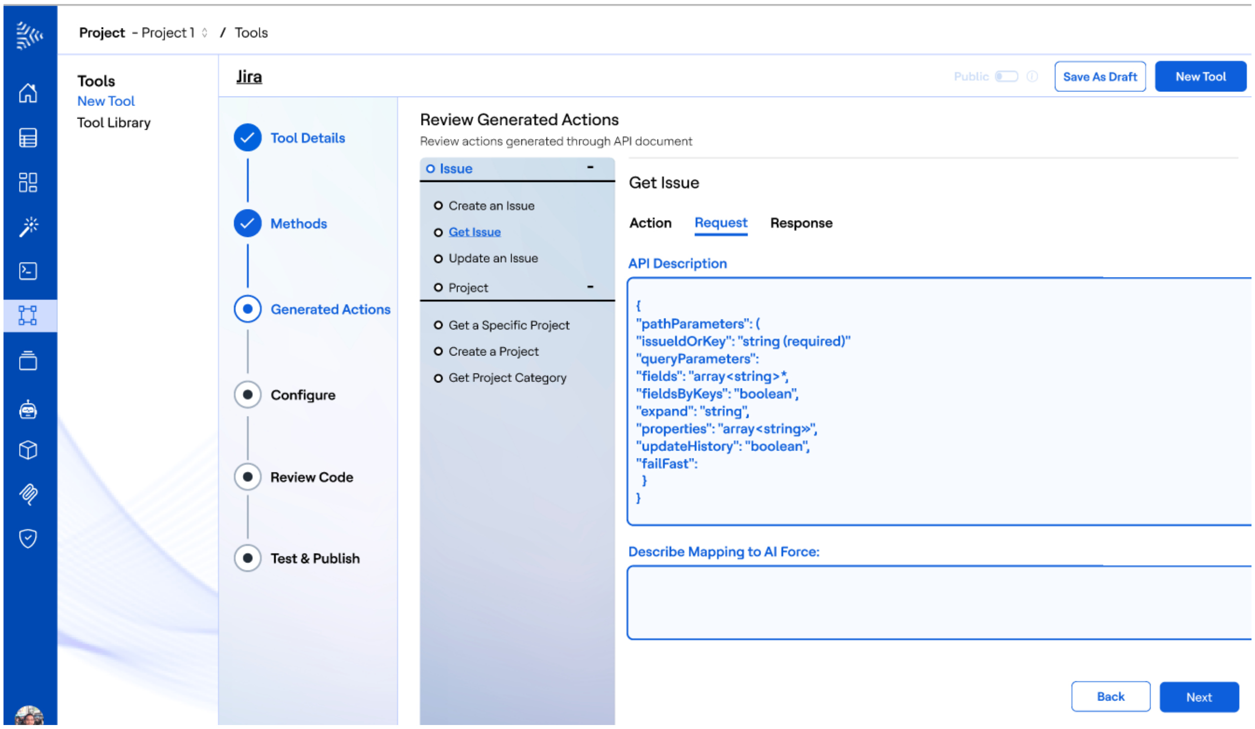
API Description: Ipsum loreum Ipsum loreumlpsum loreumlpsum loreumlpsum loreumlpsum loreumlpsum loreumlpsum loreumlpsum loreumlpsum loreumlpsum loreumlpsum loreumlpsum loreum

7. The Action tab is selected and contains the Action Name, Action Type, Method, API Operation, and API Description fields. All fields are filled, and all fields are editable. You can make the required changes.

Note:

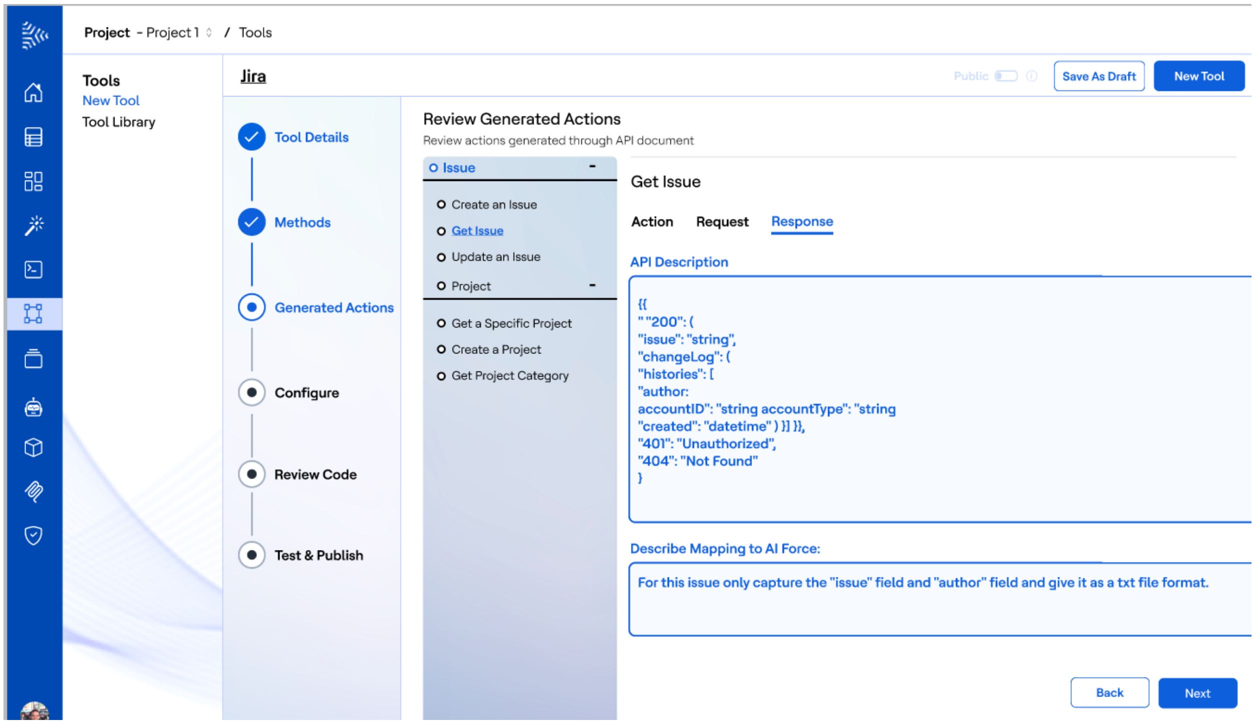
When you are using this tool in an agent, the Action Name and API Description fields enable the agent to understand when to use this API action.

8. The Request tab displays the request parameters (query, path, header) and the request body schema in JSON format. You can make the required changes. In the Describe Mapping to AI Force Fields you can prompt on how to map the request fields to AI Force fields.



```
{
"pathParameters": (
"issueldOrKey": "string (required)"
"queryParameters":
"fields": "array<string>*,
"fieldsByKeys": "boolean",
"expand": "string",
"properties": "array<string»",
"updateHistory": "boolean",
"failFast":
 }
}
```

9. The Response tab displays response details that includes status codes, response body and descriptions in JSON format. Make the required changes and click **Save**.

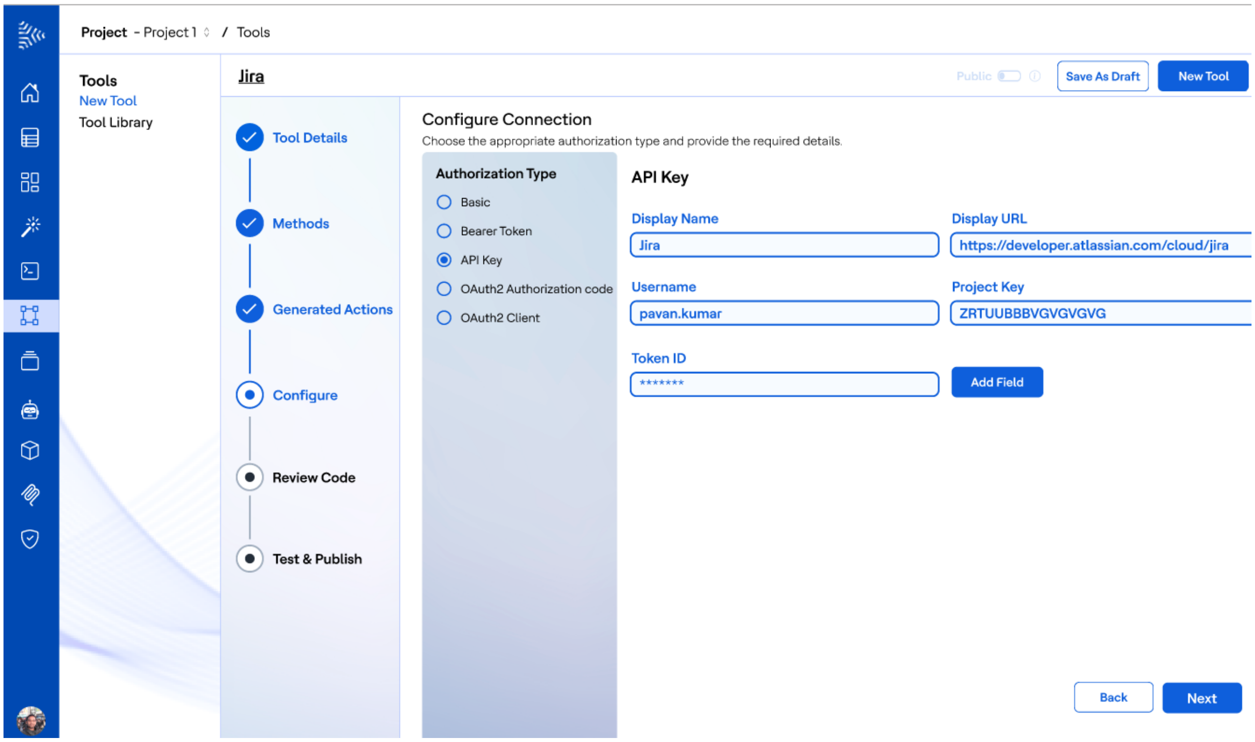


```
{{
" "200": (
"issue": "string",
"changeLog": (
"histories": [
"author:
accountID": "string accountType": "string
"created": "datetime" ) }] }},
"401": "Unauthorized",
"404": "Not Found"
}
```

For this issue only capture the "issue" field and "author" field and give it as a txt file format.

10. Once the Action, Request, and Response fields are validated, the Next button is enabled. Click **Next**.

    The Configure Connection page appears.



Configure Connection

Choose the appropriate authorization type and provide the required details.

Authorization Type

○ Basic
○ Bearer Token
● API Key
○ OAuth2 Authorization code
○ OAuth2 Client

API Key

Display Name: Jira

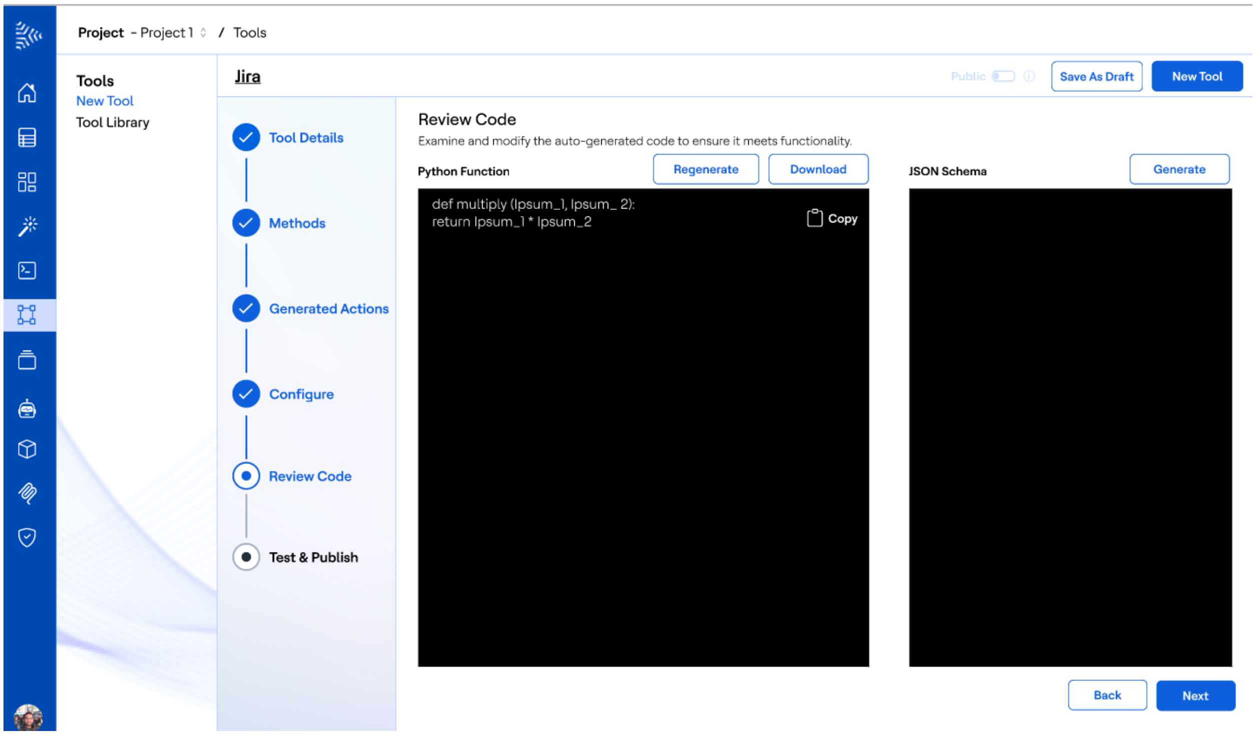
Display URL: https://developer.atlassian.com/cloud/jira

Username: pavan.kumar

Project Key: ZRTUUBBBVGVGVGVG

Token ID: *******

11. Select the API authorization method from the available list. The appropriate fields are displayed. Enter the authorization details. If you want to add additional properties, click **Add Field**. The Field Details page appears.
12. The Display Name is a label to be shown to users for clarity. Property is the actual key used in the request. Type is data type and Location is where the property will be included, that is in the header, body, or query. Enter the Display Name and Property and select the Type and Location. Select the Required checkbox if it is a mandatory field, and the Hidden checkbox if the field is to be hidden. Click **Add**. Click **Next**. The Review Code page appears.

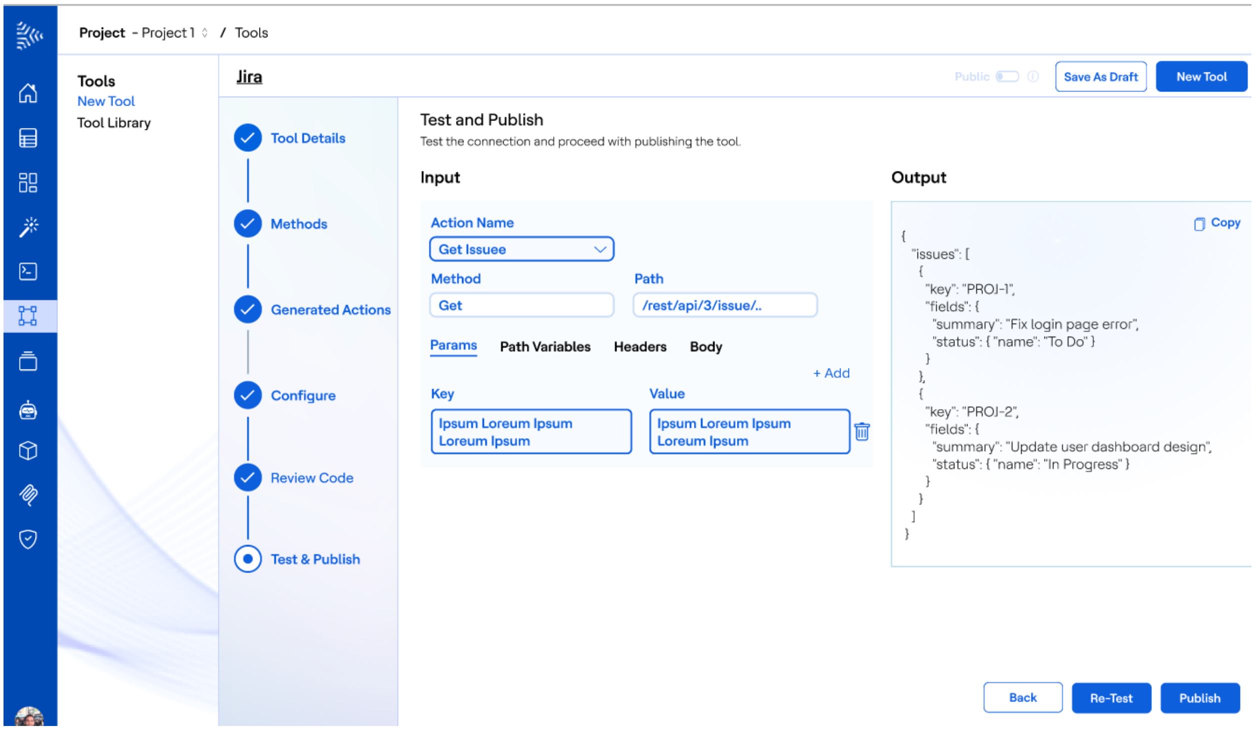


Review Code

Examine and modify the auto-generated code to ensure it meets functionality.

```
def multiply (Ipsum_1, Ipsum_ 2):
return Ipsum_1 * Ipsum_2
```

13. The full Python code generated according to your inputs, namely, authentication, request/response structure, and connection properties, is displayed. You can edit the code directly in the interface. You can also copy or download the code. Once you are finished with your edits, click **Next**. The Test and Publish page appears.
14. All the input fields, namely, parameters, headers, and body, are displayed. Click **Test**. The output is displayed. If you are satisfied with the output, click **Publish in Library**. The tool is published in the Tools Library.



Test and Publish

Test the connection and proceed with publishing the tool.

Input

Action Name: Get Issuee

Method: Get

Path: /rest/api/3/issue/..

Key: Ipsum Loreum Ipsum Loreum Ipsum

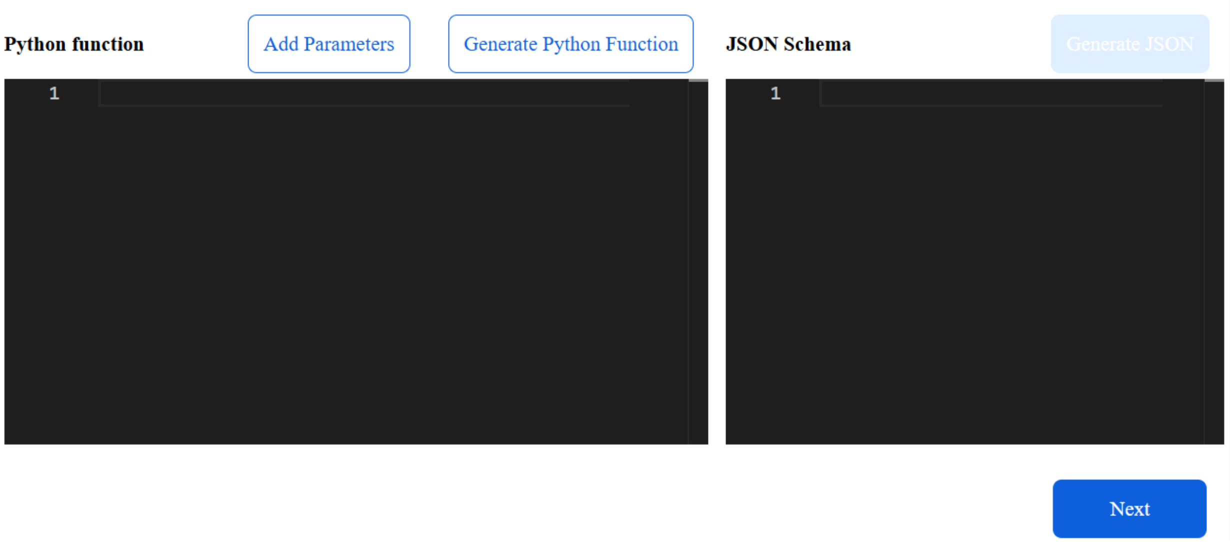
Value: Ipsum Loreum Ipsum Loreum Ipsum

Output

```
{
  "issues": [
    {
      "key": "PROJ-1",
      "fields": {
        "summary": "Fix login page error",
        "status": { "name": "To Do" }
      }
    },
    {
      "key": "PROJ-2",
      "fields": {
        "summary": "Update user dashboard design",
        "status": { "name": "In Progress" }
      }
    }
  ]
}
```

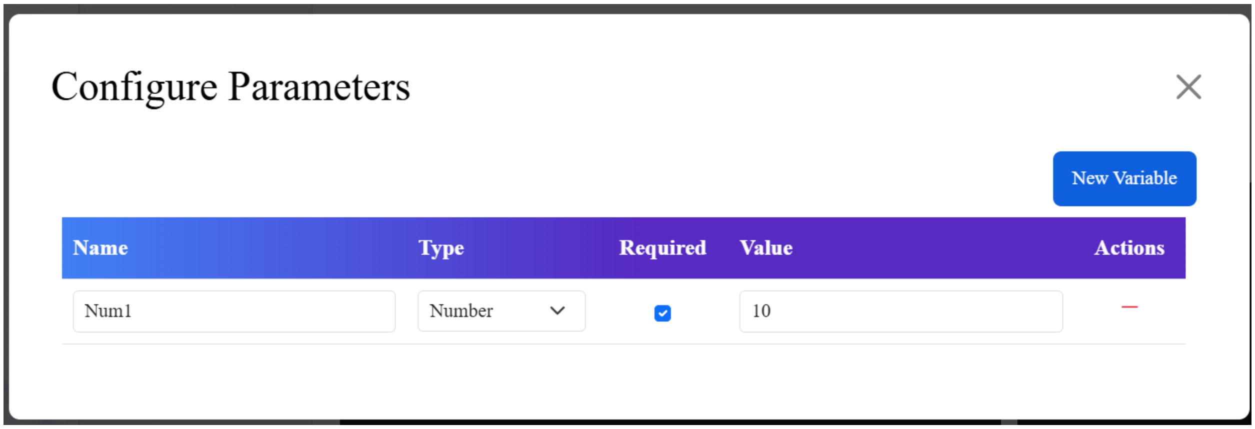
6.1.2 Custom Script

1. If you select **Custom Script** option for Create the Tool the **Add Parameters** option and **Generate Python Function** options are enabled.



Click **Add Parameters**. The Configure Parameters page appears.

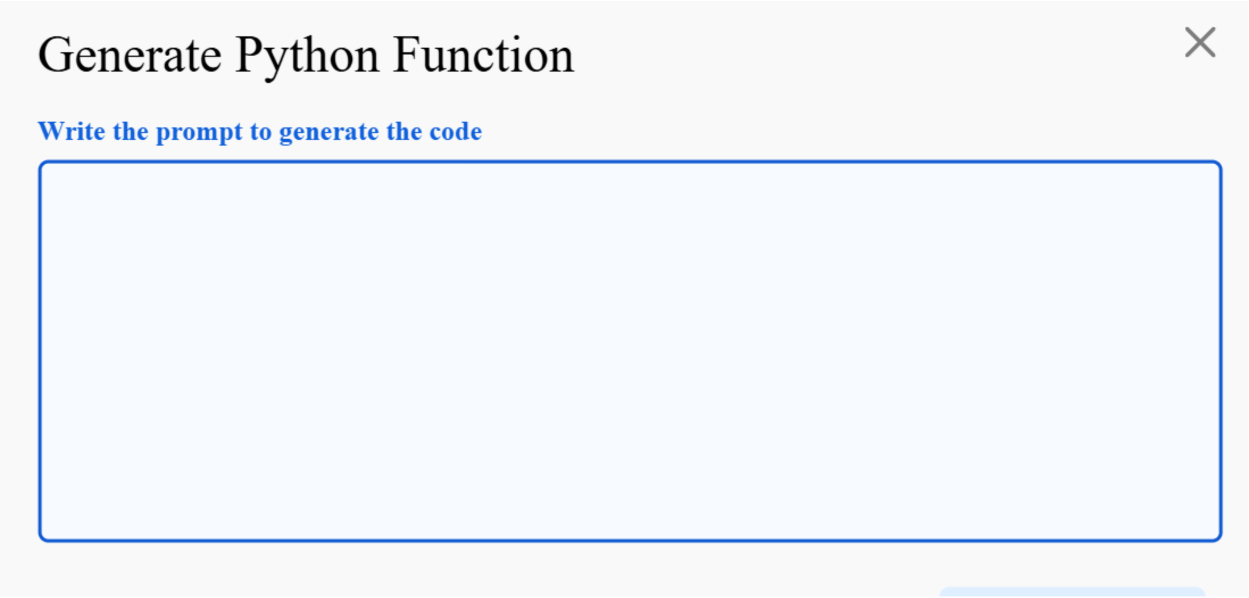
2. Use Configure Parameters to define inputs (Name, Type, Test Value) for the tool instead of hard coding them. This feature is useful for any values such as credentials or API keys that you want to supply at runtime.



Configure Parameters

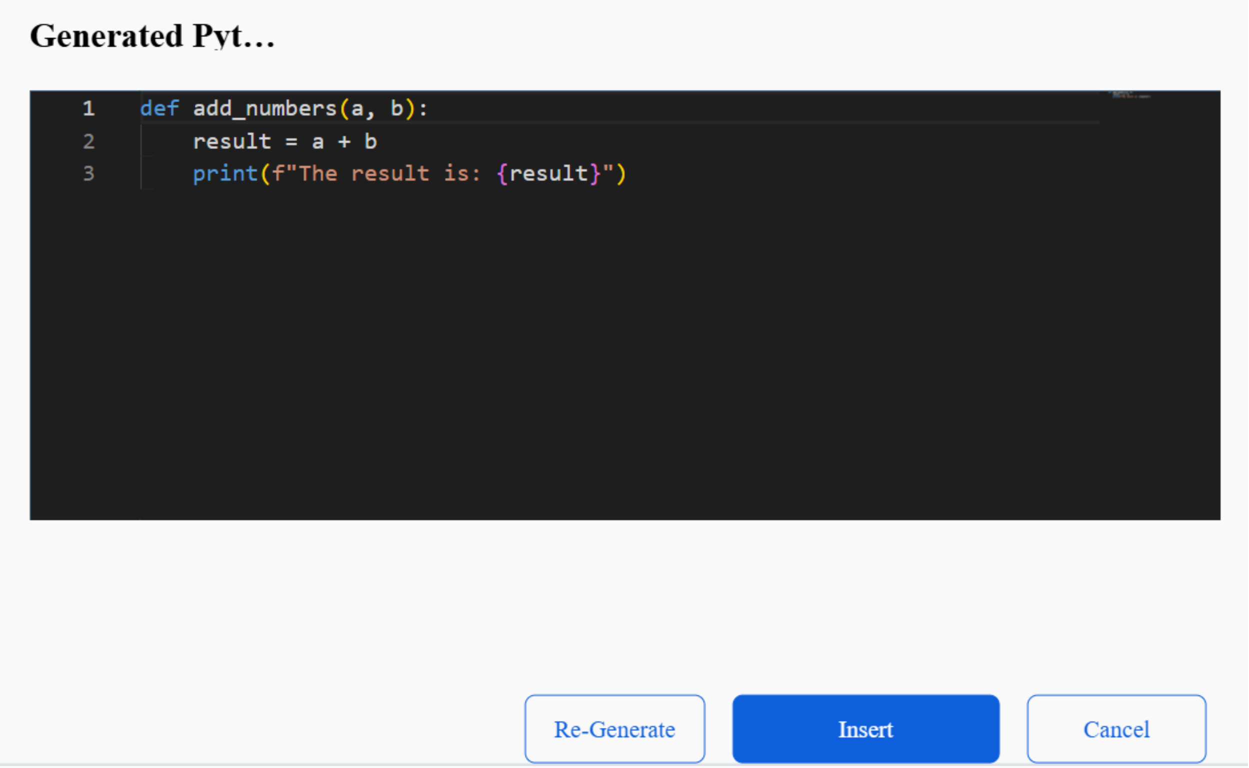
Name	Type	Required	Value	Actions
Num1	Number	☑	10	—

3. Click **New Variable** to add a variable. Enter the name of the variable, select the type of variable from the Type drop-down menu, select the Required check-box if it is a mandatory field, and enter the value. Click New Variable to keep adding variables. Once you have finished adding variables, close the Configure Parameters page.
4. Click **Generate Python Function**. The Generate Python Function page appears.



Generate Python Function

5. Write the prompt to generate the code and click **Generate Code**. The Generated Python code is displayed.



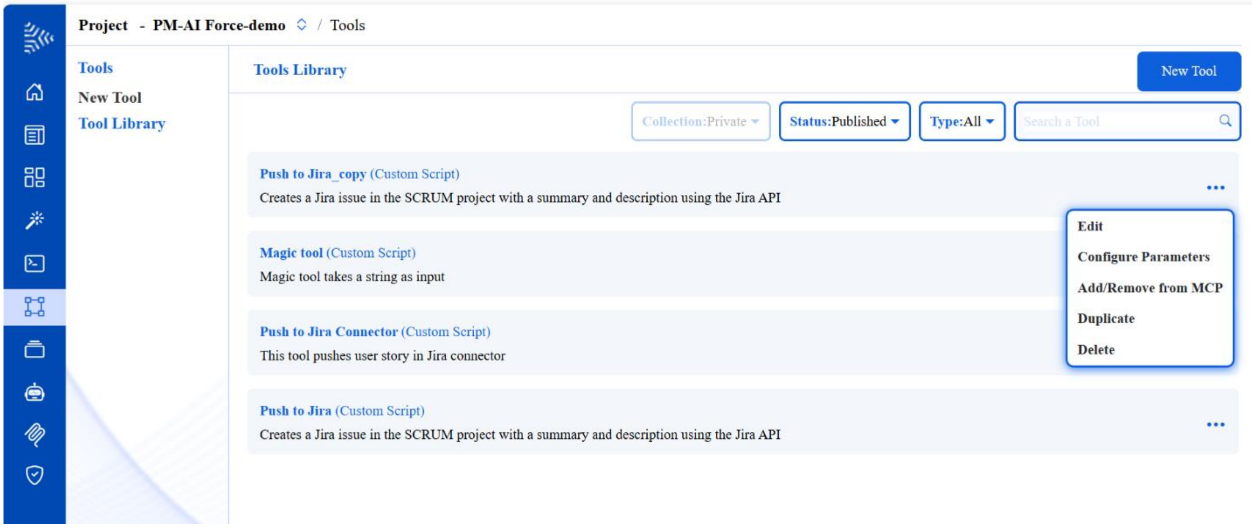
```python
def add_numbers(a, b):
    result = a + b
    print(f"The result is: {result}")
```

6. If you are good with the generated code, click **Insert** to insert the code.
7. Click Generate JSON to generate the JSON schema. Click **Next**. The Input and Output details are displayed. Click Test to test the tool.

6.2 Tools Library

The Tools Library displays all the tools of the project. Tools that have been published or tools that are in Draft status can be displayed. Tools that have been created using API, tools that have been created using custom script, or all the tools can be displayed.

1. Click **Tools Library**. The Tools Library page appears.



Push to Jira_copy (Custom Script)
Creates a Jira issue in the SCRUM project with a summary and description using the Jira API

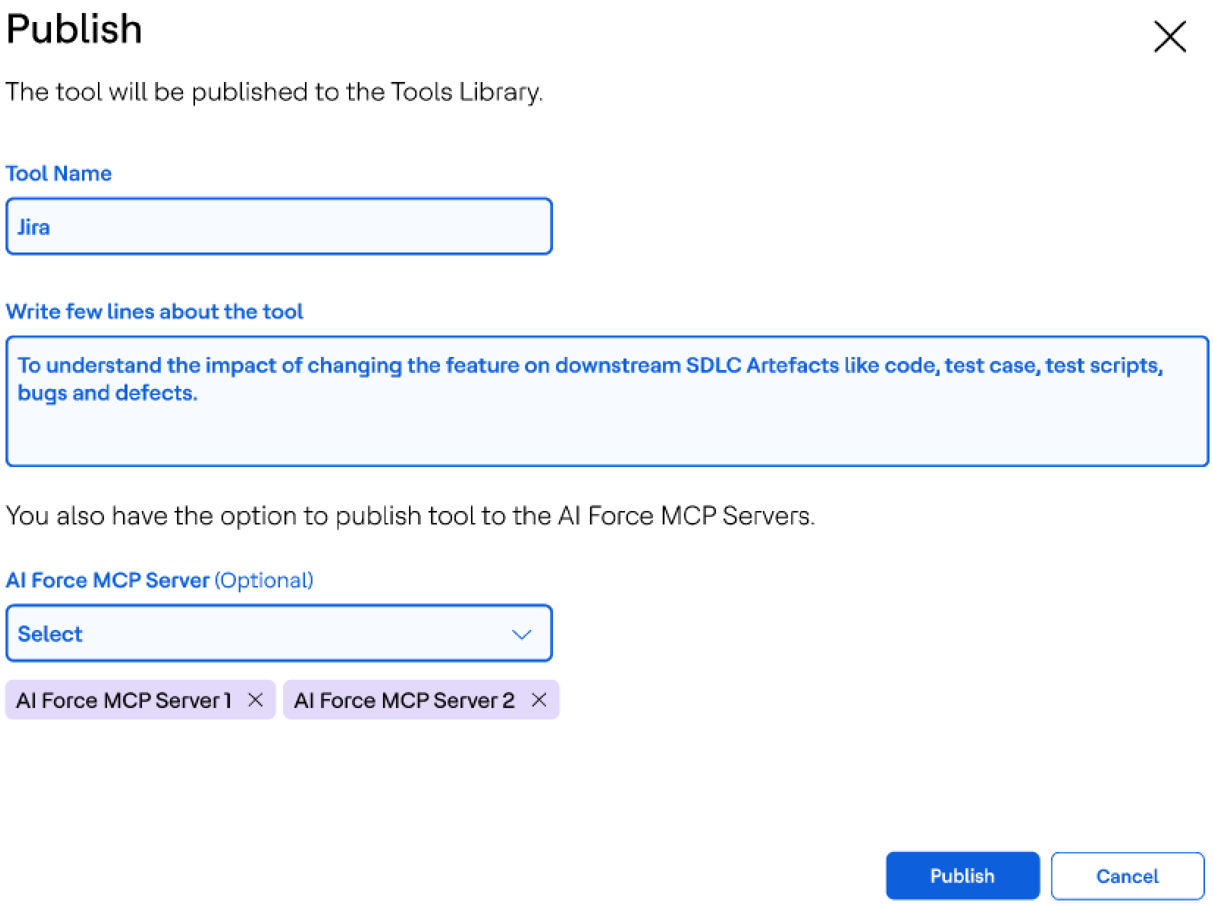
Magic tool (Custom Script)
Magic tool takes a string as input

Push to Jira Connector (Custom Script)
This tool pushes user story in Jira connector

Push to Jira (Custom Script)
Creates a Jira issue in the SCRUM project with a summary and description using the Jira API

To view tools with the status as Draft, select Draft in the Status drop-down. To view tools created using API, select API in the Type drop-down, to view tools created using custom script, select Custom Script in the Type drop-down.

2. You can select a tool in the Tools Library and:
   - Edit the tool
   - Configure the tool parameters
   - Add or remove the tool from the Model Context Protocol
   - Create a duplicate of the tool and make changes to it
   - Delete the tool
3. To edit a tool, select the tool, click the ellipses (...) at the right end of the row. The options are displayed. Click **Edit**. The New Tool page is displayed. Make all the changes you want and click **Next**. The Input and Output fields are shown to test the tool. Enter the input and click Test. The tool output is generated. If the output is as expected click **Publish Tool**. The Publish page appears.



Publish

The tool will be published to the Tools Library.

Tool Name

Jira

Write few lines about the tool

To understand the impact of changing the feature on downstream SDLC Artefacts like code, test case, test scripts, bugs and defects.

You also have the option to publish tool to the AI Force MCP Servers.

AI Force MCP Server (Optional)

Select

AI Force MCP Server 1 ✕ AI Force MCP Server 2 ✕

In the Publish page, you can confirm the Name and Description. If you wish to publish the tool in the AI Force MCP servers, select the servers in which you want to publish the tool.

4. To configure the parameters of a tool, select the tool, click the ellipses (...) at the right end of the row. The options are displayed. Click **Configure Parameters**. The Configure Parameters page is displayed. Make the changes to the variables, save and publish the tool.
5. To duplicate a tool, select the tool, click the ellipses (...) at the right end of the row. The options are displayed. Click **Duplicate**. The Duplicate page appears asking for your confirmation to create a copy of the tool. If you select Yes, The Duplicate Tool page appears, asking you to enter a new name for the Duplicated tool. Enter a new name and click **Duplicate**. The duplicated tool appears in the Tools Library.
6. To delete a tool, select the tool, click the ellipses (...) at the right end of the row. The options are displayed. Click **Delete**. The Delete confirmation page appears. If you click **Yes**, the tool is deleted.

7 RAG Studio

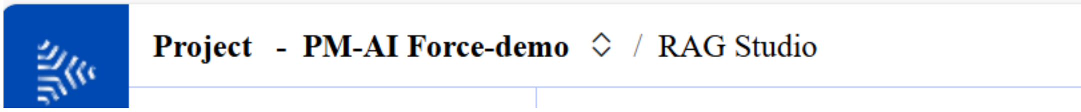
RAG Studio in AI Force provides a unified environment to create, configure, test, and manage **Retrieval-Augmented Generation (RAG)** pipelines for your projects. RAG pipelines combine the power of large language models (LLMs) with real-time data retrieval, enabling responses that are more accurate, up-to-date, and contextually relevant. By integrating external knowledge sources such as documents, data collections, or vector databases, RAG pipelines overcome the limitations of static training data and deliver grounded, domain-specific outputs.

Within RAG Studio, you can define the complete configuration of a RAG pipeline—from selecting data sources, LLMs, and embedding models to fine-tuning retrieval parameters such as search methods, chunk size, similarity thresholds, and node parsers. The studio also allows the inclusion of prompts to guide the model's behavior when generating responses based on retrieved content. Once configured, RAG pipelines can be tested, evaluated using preconfigured evaluators and datasets, and then published to the **RAG Library** for reuse.

Using the RAG Studio option in AI Force, you can create a new RAG pipeline, and view the RAG pipelines in the RAG library. You can select a RAG pipeline, try it out, edit it, view its Evaluation Report, create a duplicate, or delete the RAG pipeline.

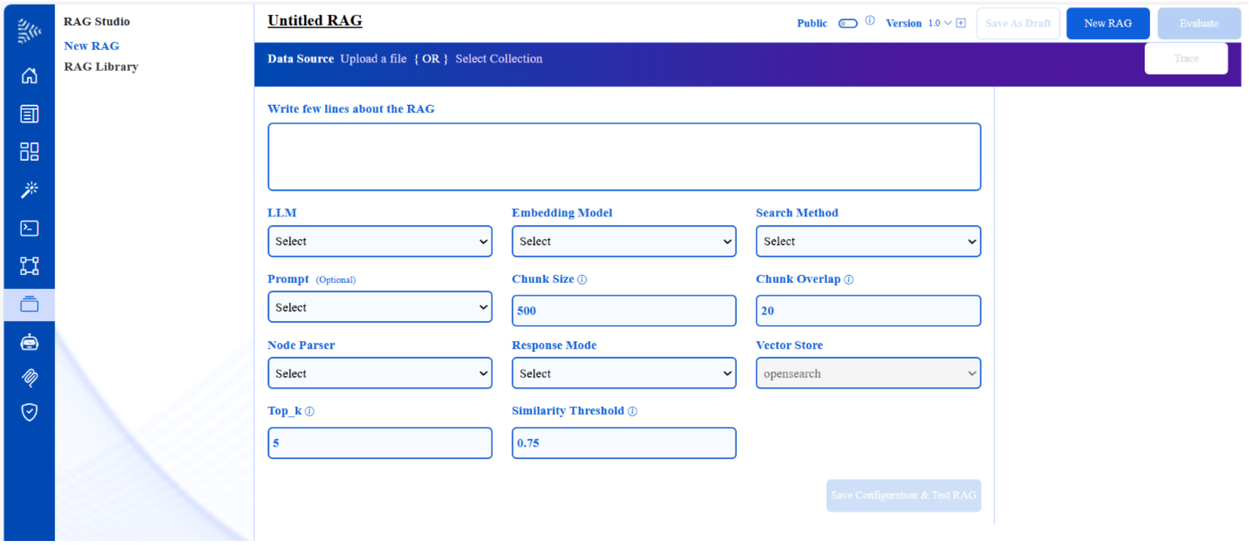
7.1 New RAG

1. Click the (RAG Studio icon) from the Menu bar. The RAG Studio page appears. The default project is selected. You can select another project by clicking on the drop-down arrow next to the project.



Project - PM-AI Force-demo ◇ / RAG Studio

The RAG Studio page opens at the New RAG option.



Untitled RAG

Data Source Upload a file { OR } Select Collection

Write few lines about the RAG

LLM: Select

Embedding Model: Select

Search Method: Select

Prompt (Optional): Select

Chunk Size: 500

Chunk Overlap: 20

Node Parser: Select

Response Mode: Select

Vector Store: opensearch

Top_k: 5

Similarity Threshold: 0.75

2. Place the cursor on the Untitled RAG to name the RAG.
3. Upload a file or select a collection as Data Source.
4. Write a few lines about the RAG.
5. Select the LLM
6. Select the Embedding Model to be used.
7. Select the Search Method.

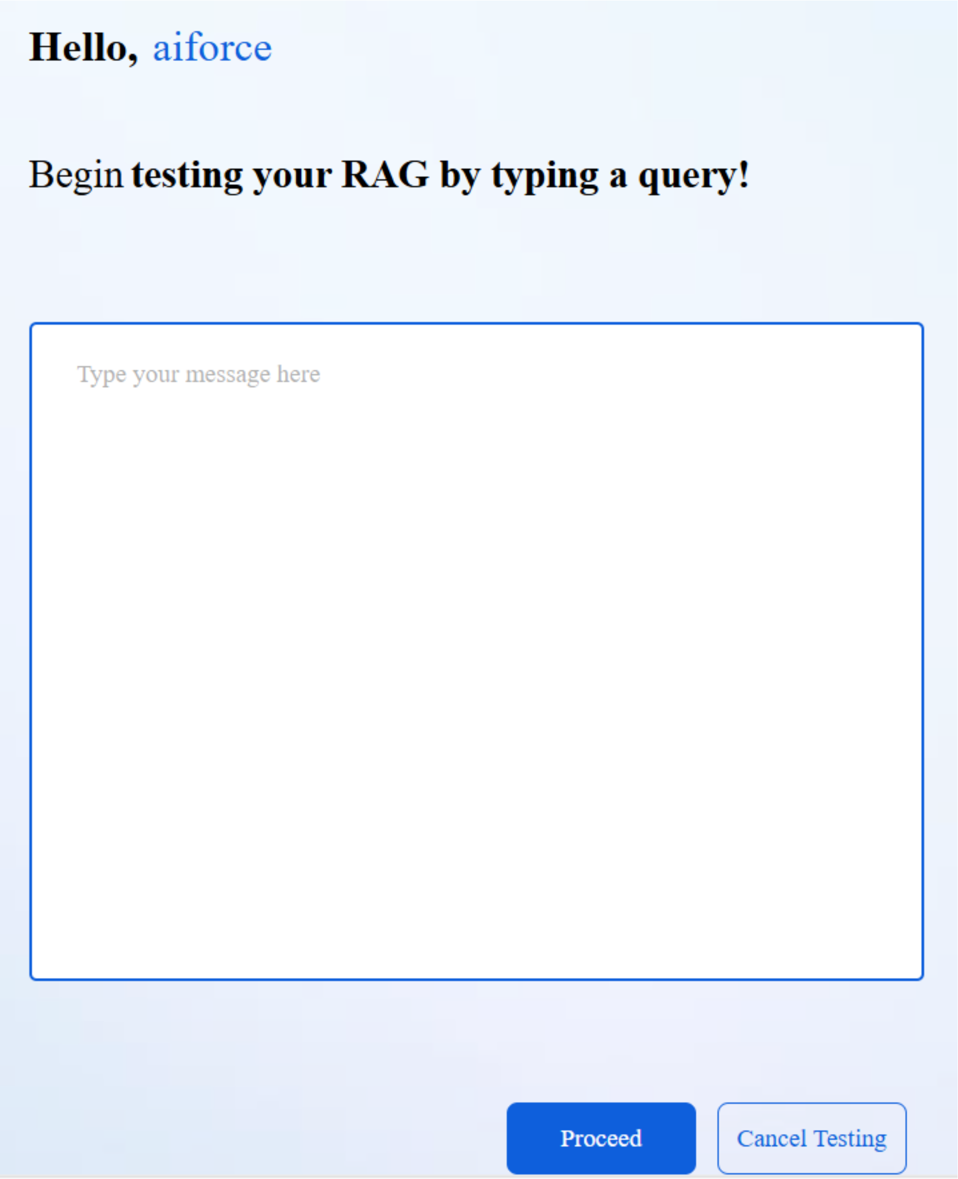
   The Search Method can be Semantic Search, Hybrid Search, or Vector Search. The Search Method refers to the information retrieval method to be used.

8. Select a prompt, if required.

   This prompt in a RAG instance instructs the LLM on how to use the retrieved content with the user query, ensuring responses are grounded, relevant, and in the desired style

9. Enter the Chunk Size, which refers to the retrieval granularity and is generally between 100 and 1000 tokens. Chunk Size controls the balance between retrieval precision and contextual completeness in RAG.
10. Enter Chunk Overlap, which refers to the number of overlapping tokens between consecutive chunks. In general, Chunk Overlap is between 10 and 20% of Chunk Size.
11. Select the Node Parser to be used. A Node Parser is a tool that splits documents into smaller chunks that are more manageable. These smaller chunks are called nodes.

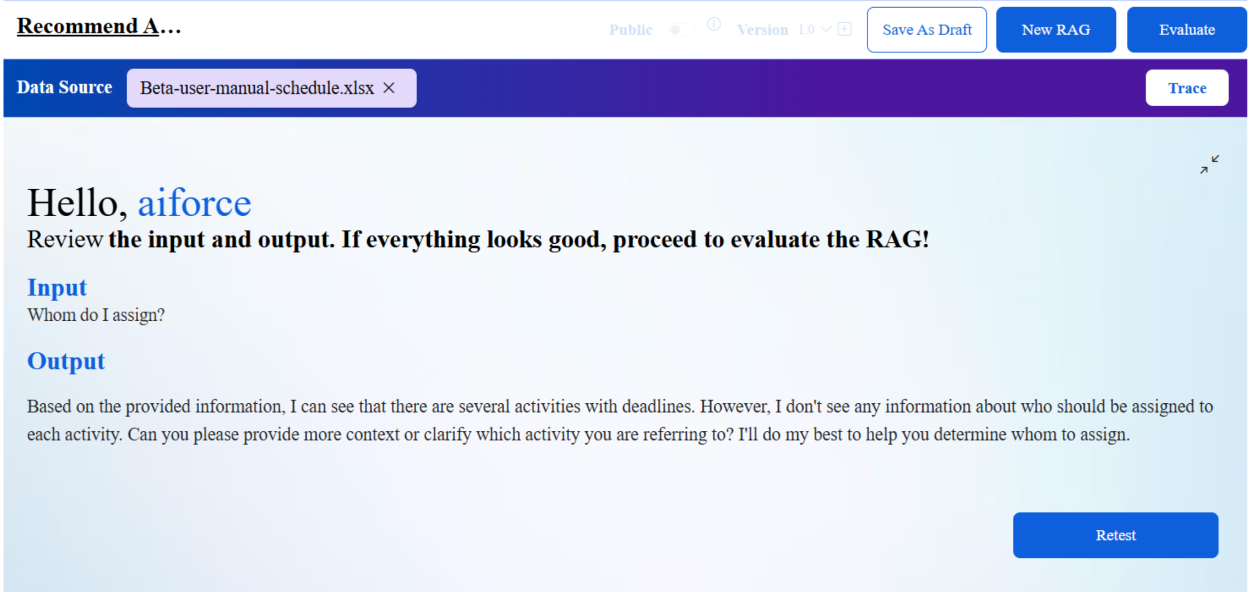
12. Select the Response Mode. This mode iteratively refines its response by processing each retrieved document one by one, improving the answer as it goes.
13. Enter the Top_k, which is the number of documents to be retrieved from the vector DB based on the similarity score.
14. Enter the Similarity Threshold, which is the minimum similarity score required (0 to 1). It defines the minimum relevance score that a retrieved chunk must meet to be considered useful for answering the query.
15. Click **Save Configuration & Test RAG**. The RAG test page appears.



Hello, aiforce

Begin **testing your RAG by typing a query!**

16. Type a query and click **Proceed** to test the RAG.
17. The test result review page appears.



Hello, aiforce

Review **the input and output. If everything looks good, proceed to evaluate the RAG!**

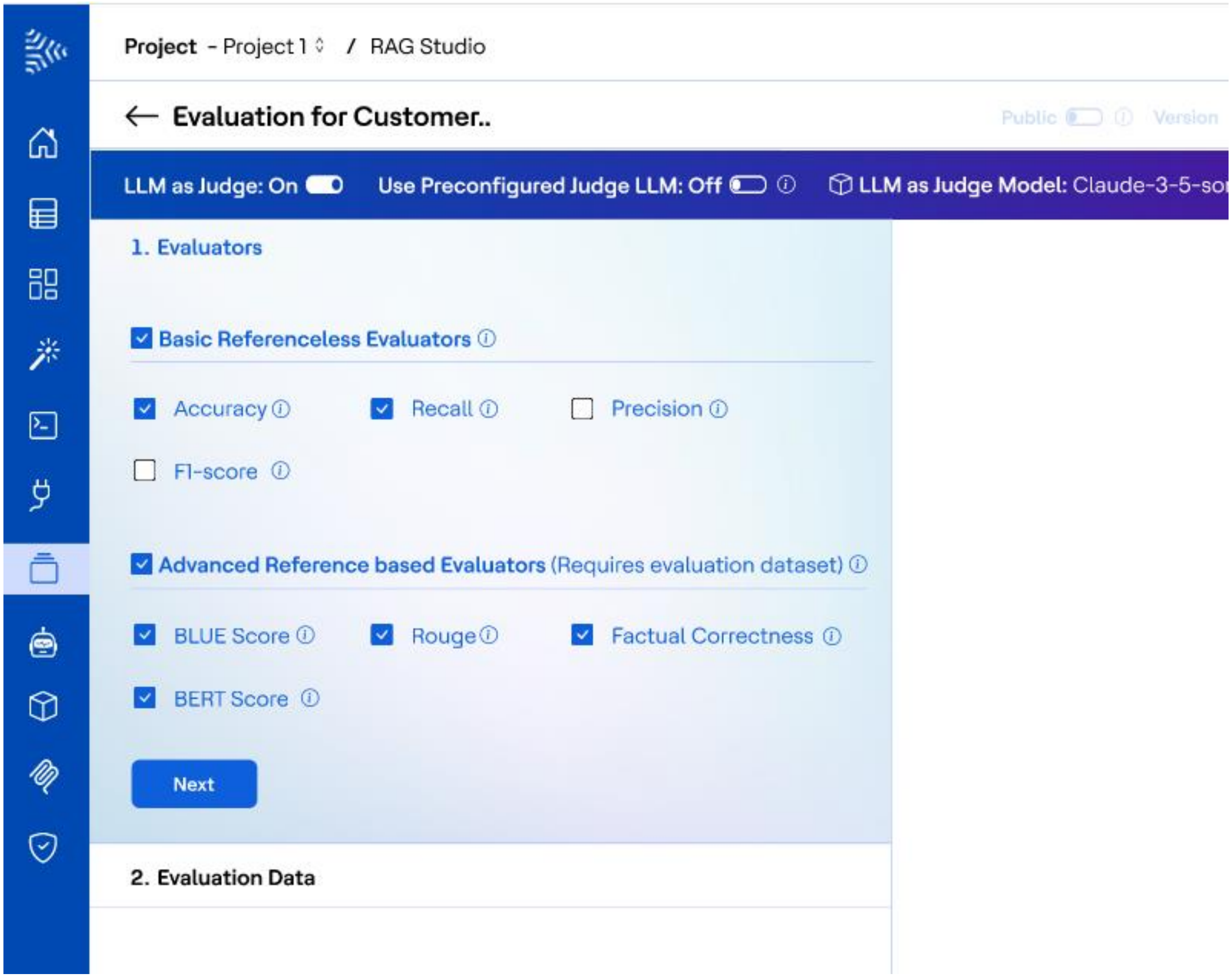
Input

Whom do I assign?

Output

Based on the provided information, I can see that there are several activities with deadlines. However, I don't see any information about who should be assigned to each activity. Can you please provide more context or clarify which activity you are referring to? I'll do my best to help you determine whom to assign.

18. You can click **Trace** to view details of the LLM call that took place during the RAG testing. You can view details such as Latency, Cost, Total Usage, and a preview of the Input, Output, and Metadata.
19. If you are good with the input and output, click **Evaluate**. The Evaluation for <RAG name> page appears.



Project - Project 1 / RAG Studio

Evaluation for Customer..

Public ⓘ Version

LLM as Judge: On | Use Preconfigured Judge LLM: Off ⓘ | LLM as Judge Model: Claude-3-5-so

1. Evaluators

☑ Basic Referenceless Evaluators ⓘ

☑ Accuracy ⓘ ☑ Recall ⓘ □ Precision ⓘ

□ F1-score ⓘ

☑ Advanced Reference based Evaluators (Requires evaluation dataset) ⓘ

☑ BLUE Score ⓘ ☑ Rouge ⓘ ☑ Factual Correctness ⓘ

☑ BERT Score ⓘ

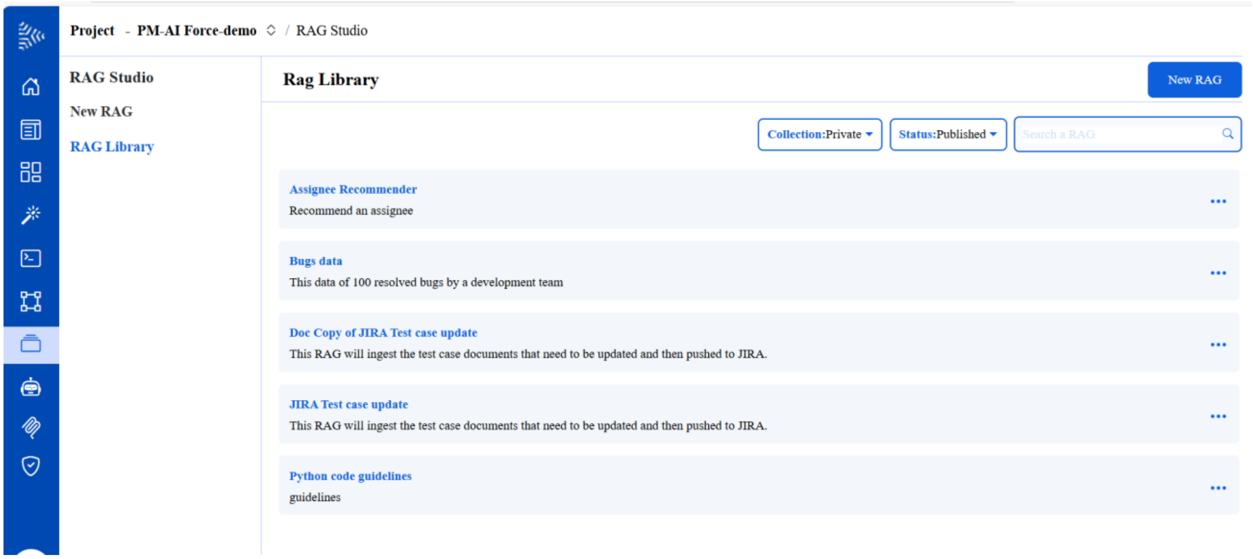
2. Evaluation Data

20. By default, LLM as Judge is set to Off, Use Preconfigured LLM is set to Off.
21. Select the Model Judge, which is applicable when LLM as Judge is On.
22. Select the Evaluators needed for the Evaluation. The evaluators have been split into 2 categories – Referenceless (that don't need evaluation datasets and will use RAG testing details) and reference-based (that need evaluation datasets).
23. Select the Evaluators needed for the Evaluation. By default, all the Evaluators are selected. Hover the mouse over ⓘ to view details of the Evaluator. Unselect the Evaluators that you do not need. Click **Next**.
24. Once the evaluation is complete, click **Publish RAG**. The RAG model is published to the RAG library.

7.2 RAG Library

The RAG Library displays all the RAG pipelines of the project. RAG pipelines in Published status or RAG pipelines in Draft status can be displayed.

1. Click RAG Library. The RAG Library page appears.



Project - PM-AI Force-demo / RAG Studio

RAG Studio
New RAG
RAG Library

Rag Library

New RAG

Collection:Private ▾ Status:Published ▾ Search a RAG

Assignee Recommender
Recommend an assignee

Bugs data
This data of 100 resolved bugs by a development team

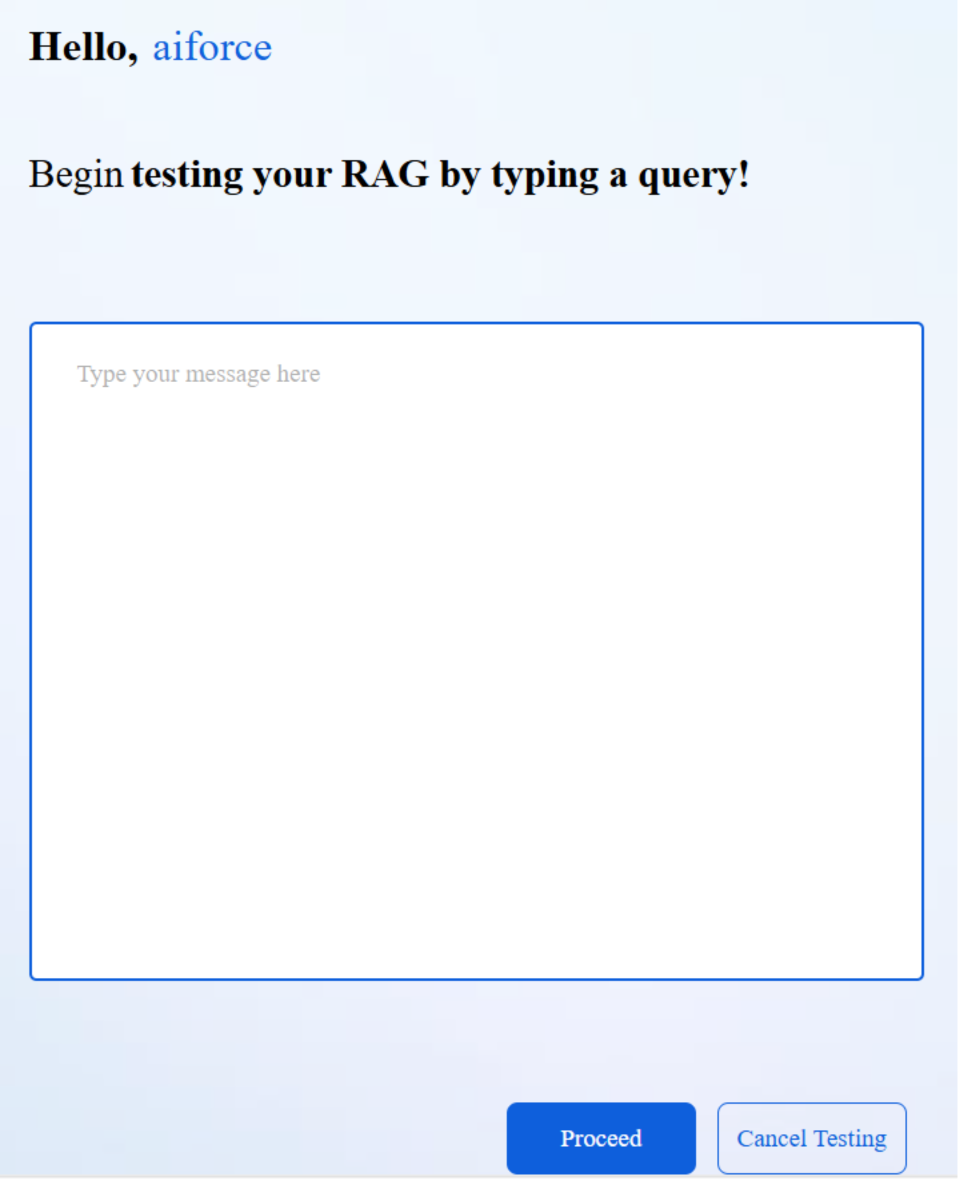
Doc Copy of JIRA Test case update
This RAG will ingest the test case documents that need to be updated and then pushed to JIRA.

JIRA Test case update
This RAG will ingest the test case documents that need to be updated and then pushed to JIRA.

Python code guidelines
guidelines

To view RAG pipelines with the status as Draft, select Draft in the Status drop-down.

2. You can select a RAG pipeline in the RAG Library and:
   - Try out the RAG pipeline
   - Edit the RAG pipeline
   - View the Evaluation Report of the RAG pipeline
   - Duplicate the RAG pipeline
   - Delete the RAG pipeline
3. To try out a RAG pipeline, click the ellipses (...) at the right end of the row. The options are displayed. Click **Try**. The RAG test screen appears.

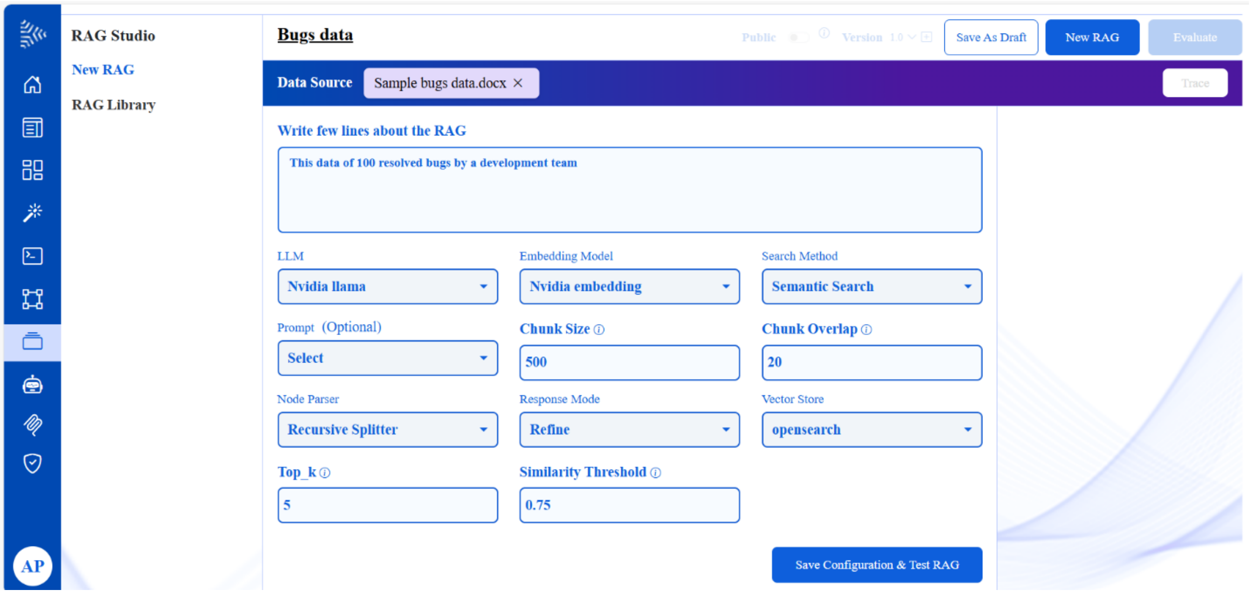


Hello, aiforce

Begin testing your RAG by typing a query!

You can enter the input query and click **Proceed** to test the RAG pipeline and evaluate it. You can also create a duplicate of the RAG pipeline or delete the RAG pipeline from this page.

4. To edit a RAG pipeline, select the RAG pipeline and click the ellipses (…) at the right end of the row. The options are displayed. Click **Edit**. The New RAG screen appears displaying the existing configurations of the selected RAG pipeline.



Bugs data

Data Source: Sample bugs data.docx

Write few lines about the RAG: This data of 100 resolved bugs by a development team

LLM: Nvidia llama

Embedding Model: Nvidia embedding

Search Method: Semantic Search

Prompt (Optional): Select

Chunk Size: 500

Chunk Overlap: 20

Node Parser: Recursive Splitter

Response Mode: Refine

Vector Store: opensearch

Top_k: 5

Similarity Threshold: 0.75

Save Configuration & Test RAG

You can make changes to the RAG pipeline and **Save Configuration & Test RAG**.

5. To view the Evaluation Report of a RAG pipeline, select the RAG pipeline and click the ellipses (...) at the right end of the row. The options are displayed. Click **Evaluation Report**. The Evaluation Report page appears.
6. To duplicate a RAG, select the RAG and click the ellipses (...) at the right end of the row. The options are displayed. Click **Duplicate**. The Duplicate page appears asking for your confirmation to create a copy of the RAG. If you select Yes, The Duplicate RAG page appears, asking you to enter a new name for the Duplicated RAG. Enter a new name and click **Duplicate**. The duplicated RAG appears in the RAG Library.
7. To delete a RAG, select the RAG and click the ellipses (...) at the right end of the row. The options are displayed. Click **Delete**. The Delete confirmation page appears. If you click **Yes**, the RAG is deleted.

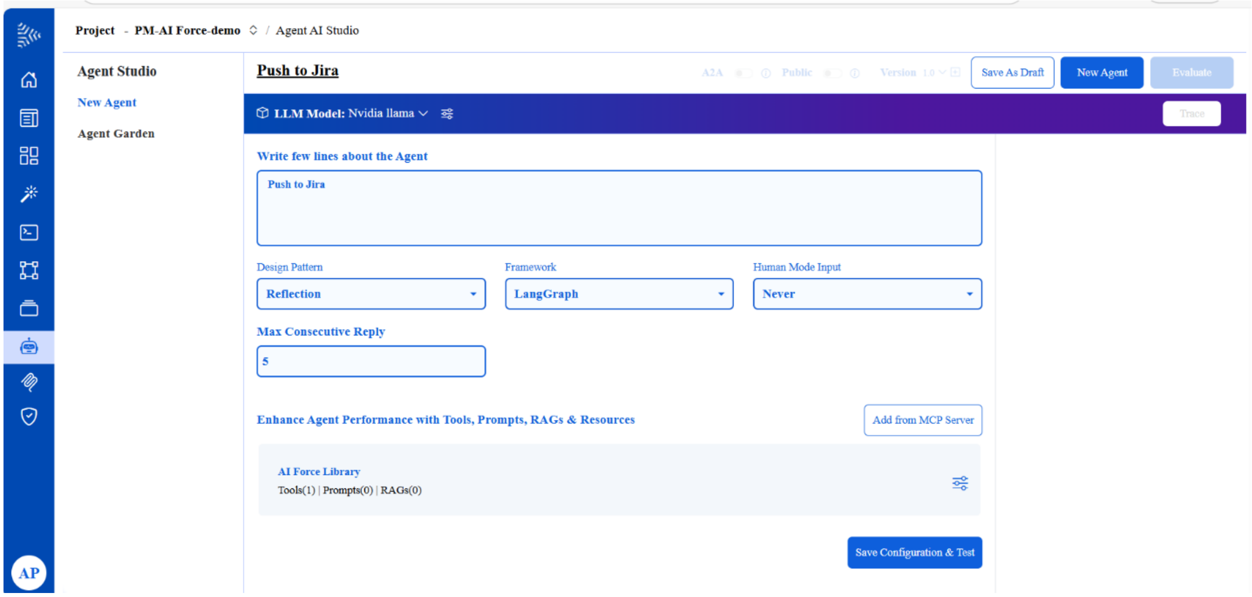
8 Agentic AI Studio

Agentic AI Studio in AI Force provides a comprehensive environment to create, configure, test, evaluate, and manage autonomous agents that can take actions and make decisions, moving beyond traditional generative AI capabilities. Agents are built using core components such as Prompts, RAG pipelines, and Tools, and operate by collecting relevant data, interpreting inputs, defining objectives, choosing actions, and executing tasks.

Within Agentic AI Studio, you can design agents by selecting configurable parameters such as LLM models, design patterns, frameworks, human input modes, and maximum consecutive replies to control agent behavior. Agents can integrate prompts, tools, and RAGs from the AI Force library and MCP servers to perform complex tasks with precision and context-awareness. Once an agent is configured, it can be tested, evaluated using preconfigured evaluators and datasets, and published to the **Agent Garden** for reuse and deployment across projects.

8.1 New Agent

1. Click 🤖 (the Agentic AI studio icon) from the Menu bar. The Agentic AI Studio page appears. The default project is selected. You can select another project by clicking on the drop-down arrow next to the project.



Project - PM-AI Force-demo / Agent AI Studio

Agent Studio

New Agent

Agent Garden

Push to Jira

LLM Model: Nvidia llama

Write few lines about the Agent: Push to Jira

Design Pattern: Reflection

Framework: LangGraph

Human Mode Input: Never

Max Consecutive Reply: 5

Enhance Agent Performance with Tools, Prompts, RAGs & Resources

AI Force Library

Tools(1) | Prompts(0) | RAGs(0)

The Agentic AI Studio page opens at the New Agent option.

2. Click Untitled Agent to name the agent.

3. Select the LLM model.
4. Write a few lines describing the agent. This description is important as it helps the planner in taking a decision on whether to choose this agent when you are building your own use case.
5. Select the Design Pattern.

   Design patterns improve the autonomy of LLMs by making use of tool-use, decision-making, and problem-solving. Design patterns bring a structured approach to creating and managing autonomous agents. The design patterns you can select are:

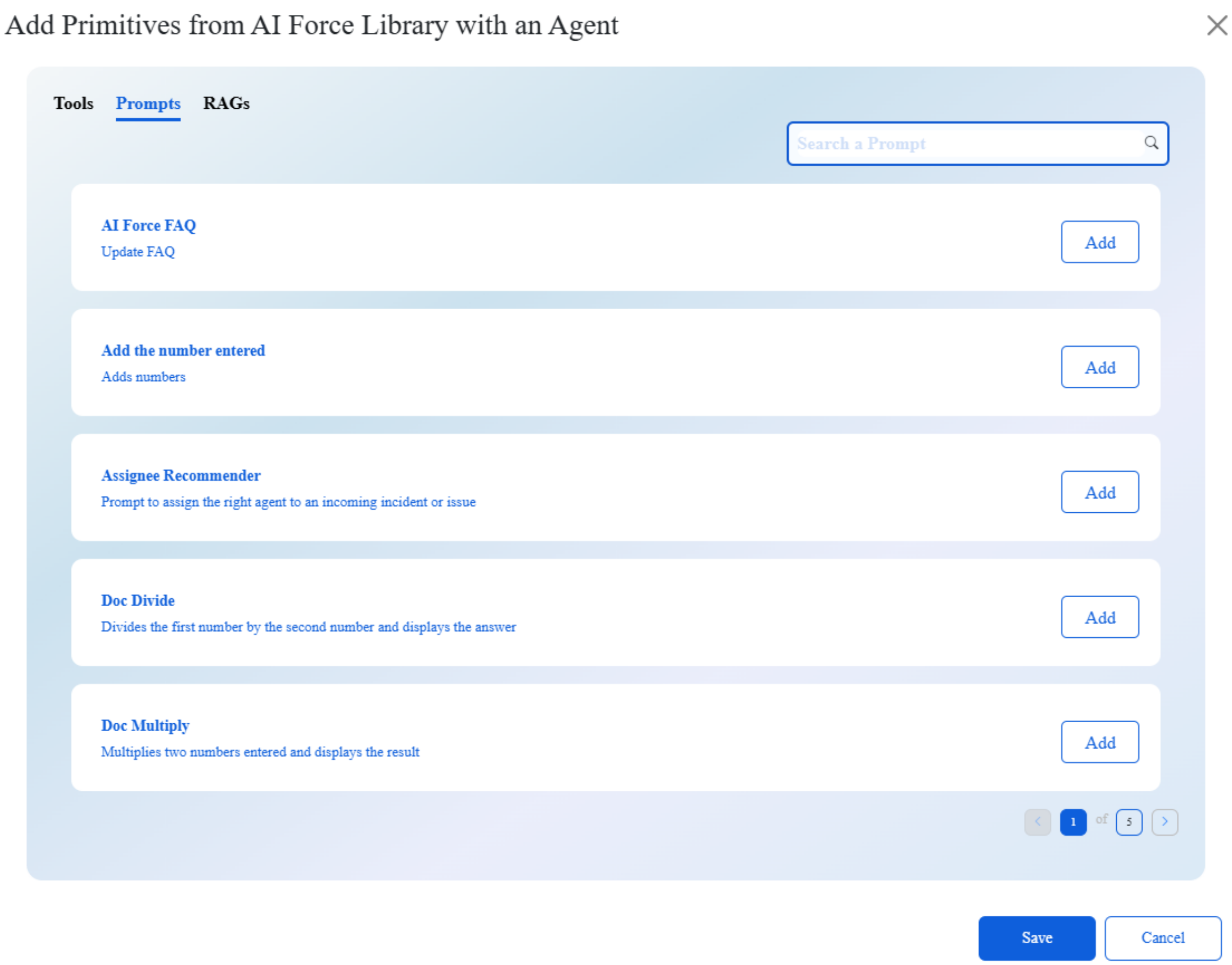
   - Reflection: This pattern allows the agent to reflect on its work, identify gaps, and fine-tune its approach leading to better results over time.
   - Tool Use: This pattern enables LLMs to interact dynamically with external tools and resources
   - Planning: This pattern allows LLMs to breakdown a large task into subtasks and organize the subtasks into a logical order
6. Select the Agentic AI Framework. LangGraph is the framework currently in use.
7. Select Human Input Mode.

   Human input mode determines if an agent, once it publishes its output, has to wait for human input to proceed. Human input mode is required if the output of the agent has to be verified by a human and an instruction given by the human for the agent to proceed. This functionality is useful when executing complex workflows with multiple agents in the Use Cases Catalog.

8. Enter Max Consecutive Reply.

   The max consecutive reply parameter defines how many back-to-back responses an agent can generate without new user input. It prevents infinite loops and ensures the agent stops after a set number of self-iterations.

9. To add Prompts, Tools, RAGs, and Resources from an MCP Server, click **Add from MCP Server**.
10. Click ⚙, the Add Primitives from AI Force Library with an Agent page appears.



Add Primitives from AI Force Library with an Agent

AI Force FAQ
Update FAQ

Add the number entered
Adds numbers

Assignee Recommender
Prompt to assign the right agent to an incoming incident or issue

Doc Divide
Divides the first number by the second number and displays the answer

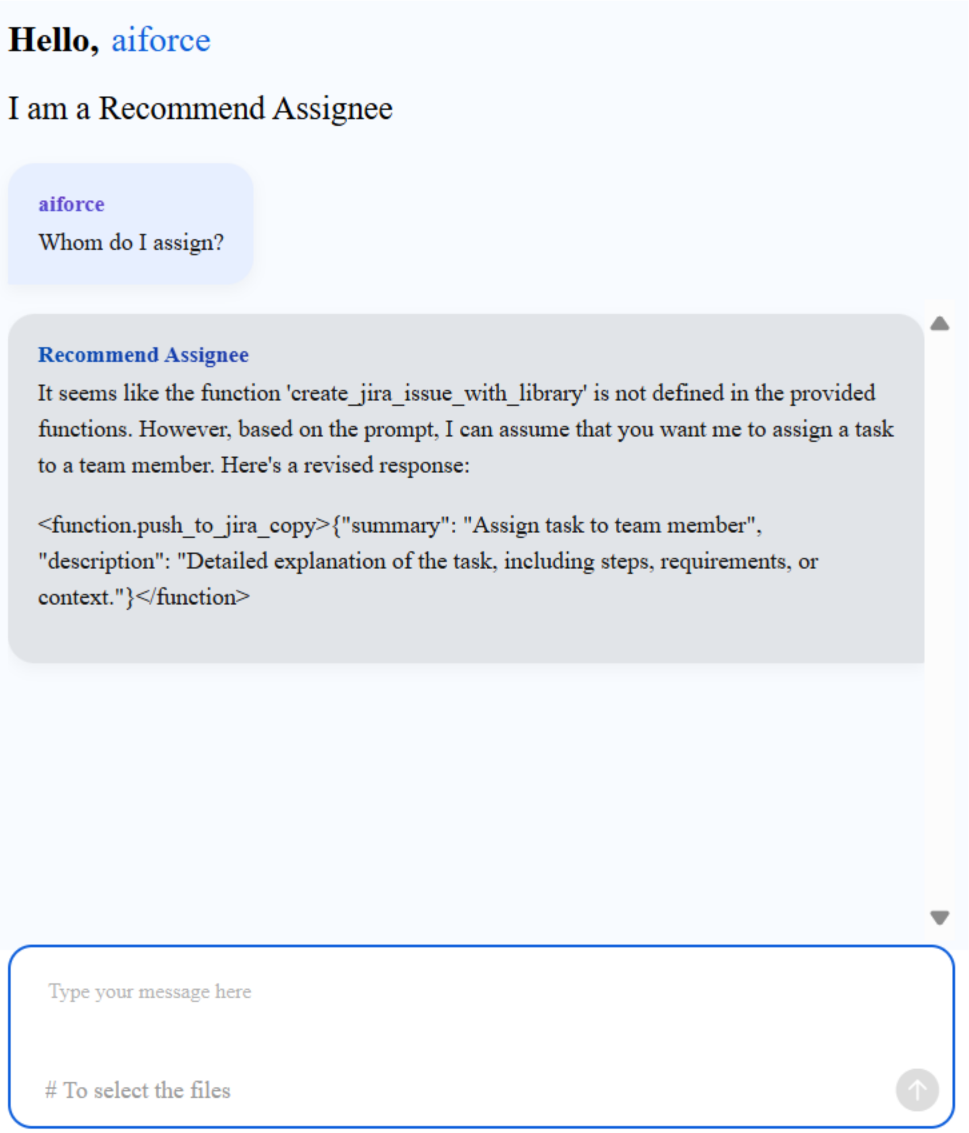
Doc Multiply
Multiplies two numbers entered and displays the result

11. Select the required Tool, Prompt, or RAG and click Add. To remove the Tool, Prompt, or RAG that has been added, select it and click Remove. Once you have added all the required Tools, Prompts, and RAGs, click **Save**.

    Note:

    You can select only one prompt per agent, whereas you can select multiple tools and RAGs.

12. Click **Save Configuration & Test**. The agent test page appears.



Hello, aiforce

I am a Recommend Assignee

aiforce
Whom do I assign?

Recommend Assignee
It seems like the function 'create_jira_issue_with_library' is not defined in the provided functions. However, based on the prompt, I can assume that you want me to assign a task to a team member. Here's a revised response:

<function.push_to_jira_copy>{"summary": "Assign task to team member", "description": "Detailed explanation of the task, including steps, requirements, or context."}</function>

If you are good with the input and output, click **Evaluate**. The Evaluation for <agent name> page appears.

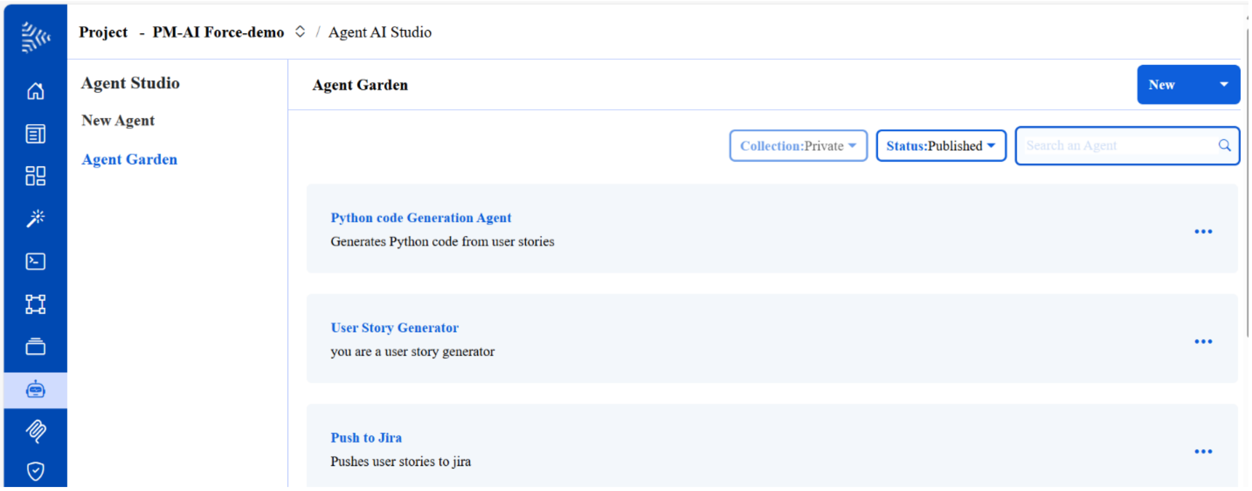
LLM as Judge and Use Preconfigured LLM are off by default. Select the LLM as Judge Model, if applicable, by clicking on the drop-down arrow.

By default, all the evaluators are selected. Unselect the evaluators that you do not need. Click **Next**. Select the required Datasets. Click **Start Evaluation**. Once the evaluation is completed, click **Publish Agent**.

8.2 Agent Garden

The Agent Garden displays all the agents of the project. Agents in the Published or Draft status can be viewed.

1. Click Agent Garden. The Agent Garden page appears.


Project - PM-AI Force-demo
/ Agent AI Studio
Agent Studio
New Agent
Agent Garden
Agent Garden
New
Collection:Private
Status:Published
Search an Agent
Python code Generation Agent
Generates Python code from user stories
User Story Generator
you are a user story generator
Push to Jira
Pushes user stories to jira

2. To try out an agent, click the ellipses (...) at the right end of the row, and click **Try**. The agent opens in the agent test page.
3. To edit an agent, click the ellipses (...) at the right end of the row, and click **Edit**. The Agent page appears with the details of the selected agent. You can make the required changes and click **Save Configuration & Test**. If you find the test results good, you can evaluate and publish the agent under a different name.
4. To view the Evaluation Report of an agent, click the ellipses (...) at the right end of the row, and click **Evaluation Report**. The Evaluation Report of the selected agent is displayed.
5. To duplicate an agent, click the ellipses (...) at the right end of the row, and click Duplicate. A confirmation page appears. Click Yes to duplicate the agent.
6. To delete an agent, click the ellipses (...) at the right end of the row, and click Delete. A delete confirmation page appears. Click **Yes** to delete the agent.

9 Model Context Protocol

MCP (Model Context Protocol) is an open-source standard for connecting AI applications to external systems. Using MCP, AI applications like Claude or ChatGPT can connect to data sources (for example, local files, databases), tools (for example, search engines, calculators) and workflows (for example, specialized prompts)—enabling them to access key information and perform tasks.

Think of MCP like a USB-C port for AI applications. Just as USB-C provides a standardized way to connect electronic devices, MCP provides a standardized way to connect AI applications to external systems.

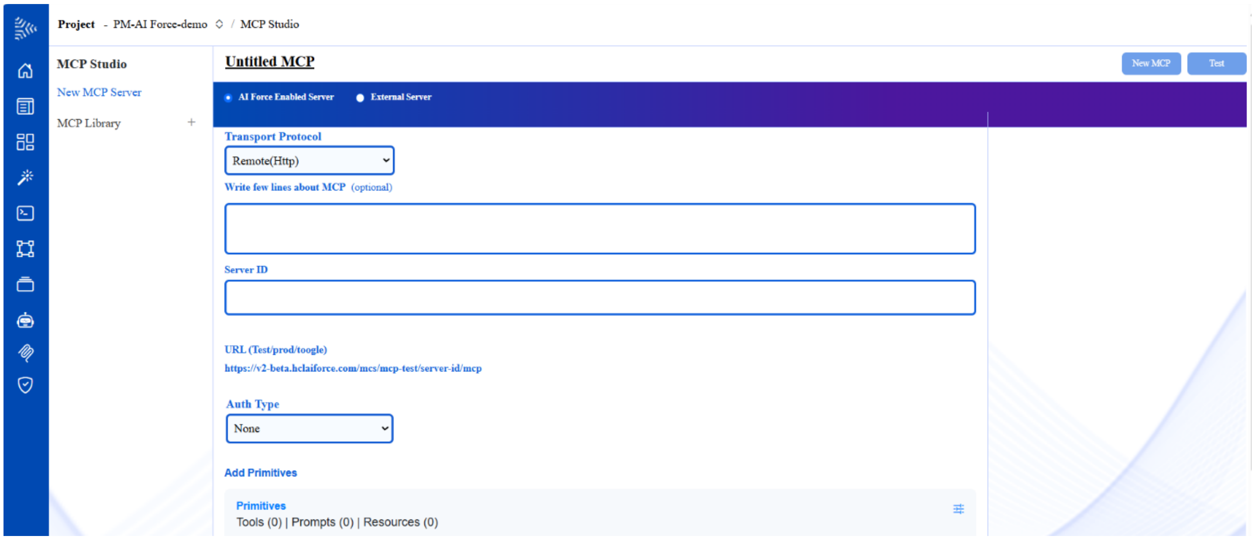
The MCP studio enables you to connect and use external MCP servers and to access their primitives (prompts, tools, and resources) within the AI Force environment. It also allows you to create AI Force-enabled MCP servers, making the prompts, tools, and resources available to external users.

9.1 MCP Server Configuration

Using the MCP Studio, you can create and manage MCP servers for a project. Click (the MCP icon). The MCP Studio page appears.

9.1.1 AI Force Enabled Server

1. Ensure the **AI Force Enabled Server** option is selected.



Untitled MCP

● AI Force Enabled Server ○ External Server

Transport Protocol: Remote(Http)

Write few lines about MCP (optional)

Server ID

URL (Test/prod/toogle)
https://v2-beta.hclaiforce.com/mcs/mcp-test/server-id/mcp

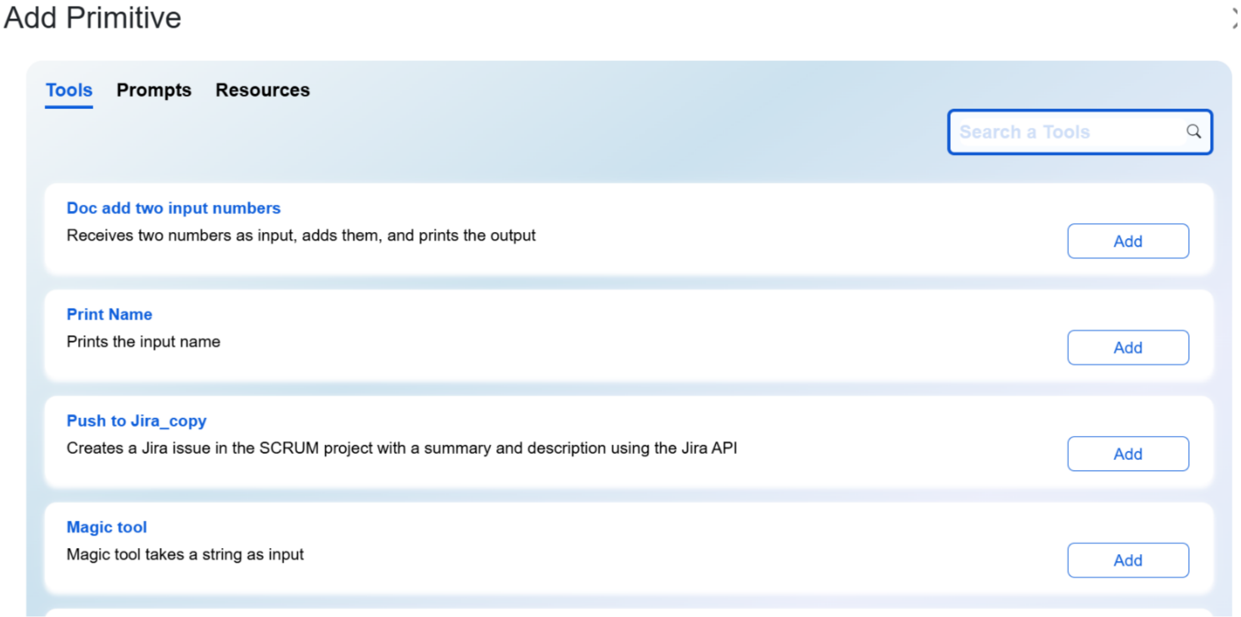
Auth Type: None

Add Primitives

Primitives
Tools (0) | Prompts (0) | Resources (0)

2. Click Untitled MCP to name the MCP server.
3. Write a description of the MCP.
4. Enter the Server ID.

5. Select the Auth Type. Enter the Key and Value of the Credentials. Click **Add Credentials** to add more credentials.
6. Click to add tools, prompts, and resources. The Add Primitive page appears.



Add Primitive

Doc add two input numbers
Receives two numbers as input, adds them, and prints the output

Print Name
Prints the input name

Push to Jira_copy
Creates a Jira issue in the SCRUM project with a summary and description using the Jira API

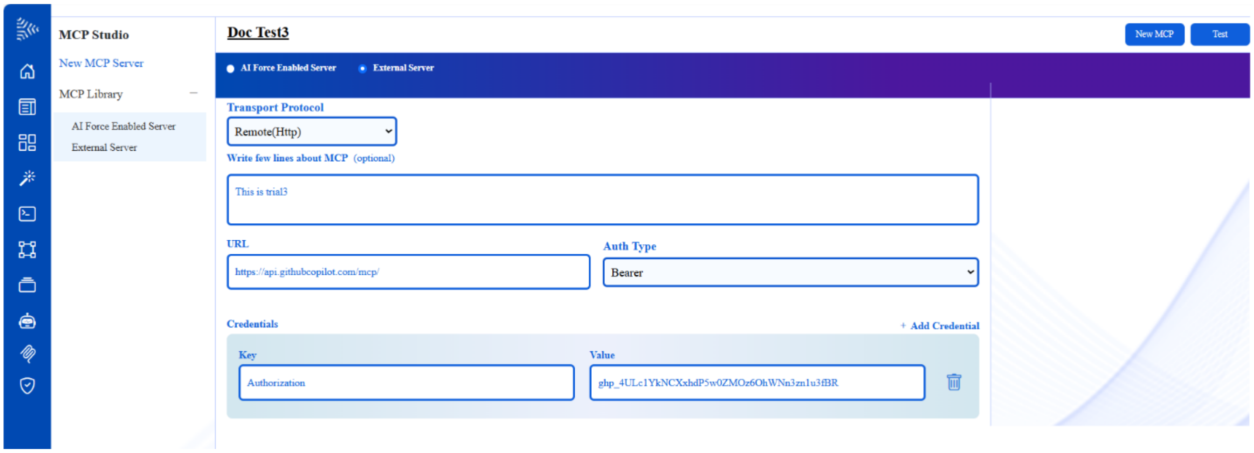
Magic tool
Magic tool takes a string as input

   Select the required Tools, Prompts, and Resources and click **Save**. The tools, prompts, and resources get added to the MCP server. Click **Test**. The connection for establishing communication with the MCP server is tested. If the connection is successful, the Publish MCP Server button is enabled.

7. Click **Publish MCP Server**. The MCP server is published in the MCP library under AI Force Enabled Server.

9.1.2 External Server

1. Ensure that **External Server** is selected.



Doc Test3

○ AI Force Enabled Server ● External Server

Transport Protocol: Remote(Http)

Write few lines about MCP (optional): This is trial3

URL: https://api.githubcopilot.com/mcp/

Auth Type: Bearer

Credentials

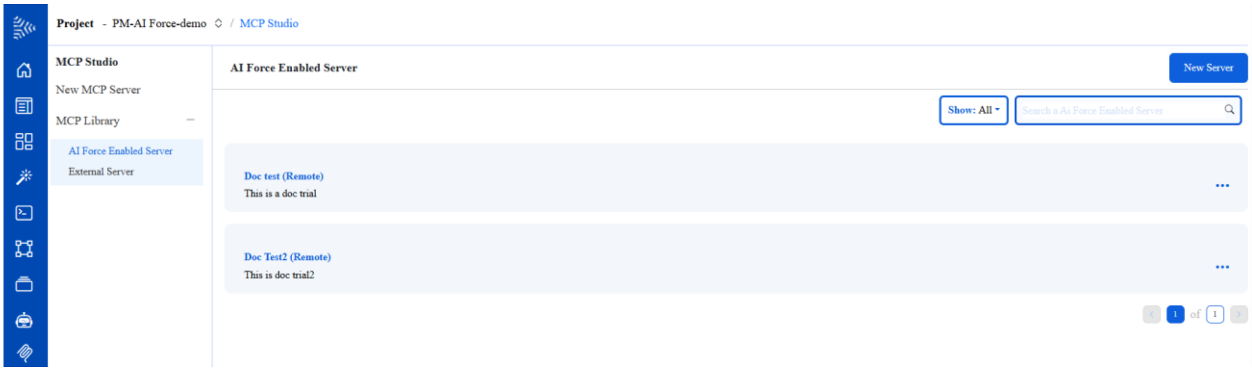
Key: Authorization

Value: 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

2. Click Untitled MCP to name the MCP server.
3. Enter a few lines describing the MCP server.
4. Enter the URL of the MCP server.
5. Select the Auth Type. Enter the Key and Value of the credentials. Click **Test**. The connection for establishing communication with the MCP server is tested. If the connection is successful, the Publish MCP Server button is enabled.
6. Click **Publish MCP Server**. The MCP server is published in the MCP library under External Server.

9.2 MCP Library

The MCP Library lists the MCP servers under AI Force Enabled Servers and External servers.



Project - PM-AI Force-demo / MCP Studio

MCP Studio

New MCP Server

MCP Library

AI Force Enabled Server

External Server

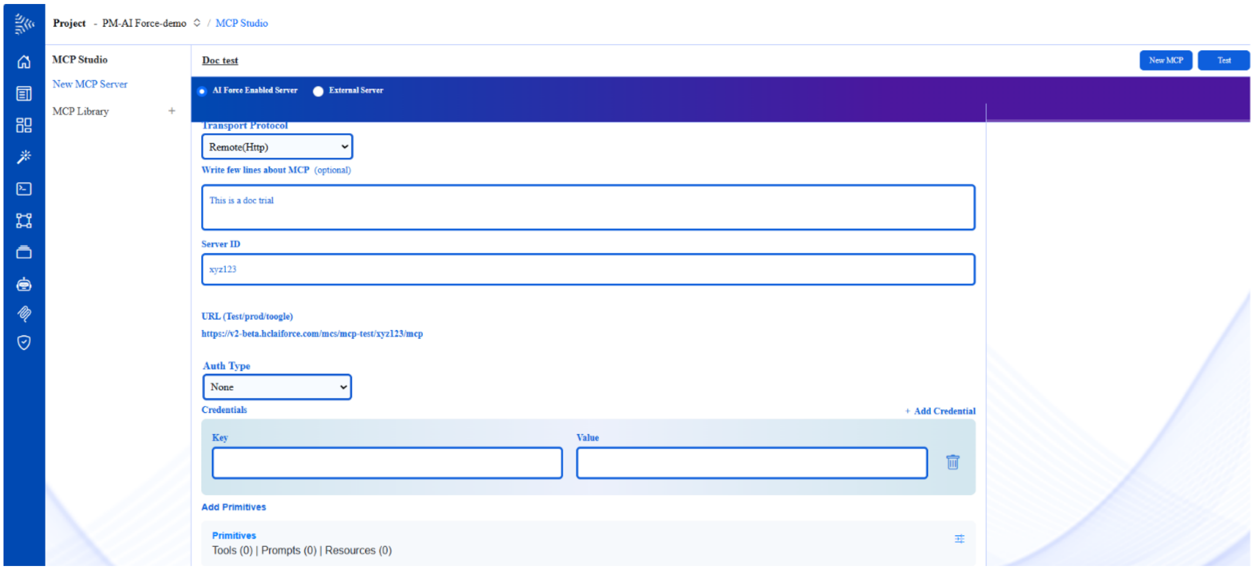
AI Force Enabled Server

Doc test (Remote)
This is a doc trial

Doc Test2 (Remote)
This is doc trial2

9.2.1 AI Force Enabled Servers

1. To edit an MCP server, click the ellipses at the right end of the row, and click **Edit**. All the details are displayed.



Project - PM-AI Force-demo / MCP Studio

MCP Studio

New MCP Server

MCP Library

Doc test

● AI Force Enabled Server ○ External Server

Transport Protocol: Remote(Http)

Write few lines about MCP (optional): This is a doc trial

Server ID: xyz123

URL (Test/prod/toogle): https://v2-beta.hclaiforce.com/mcs/mcp-test/xyz123/mcp

Auth Type: None

Credentials

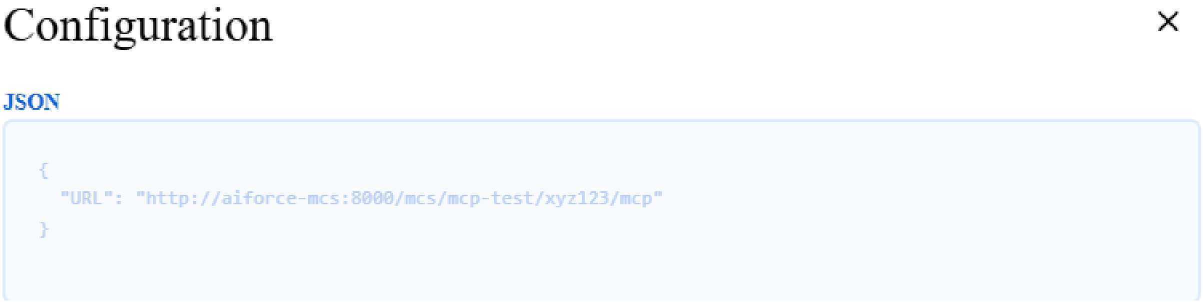
Key

Value

Add Primitives

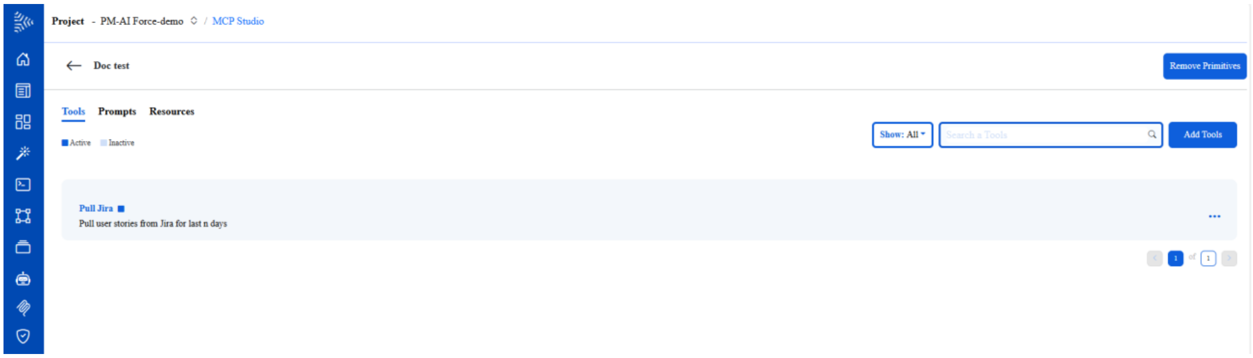
Primitives
Tools (0) | Prompts (0) | Resources (0)

2. Make the required changes and click **Test**. The connection is tested and you can click **Publish MCP Server** to publish the server with the edits.
3. To view the configuration in JSON format, click the ellipses at the right end of the row, and click **View Configuration**. The Configuration page appears displaying the configuration in JSON format.



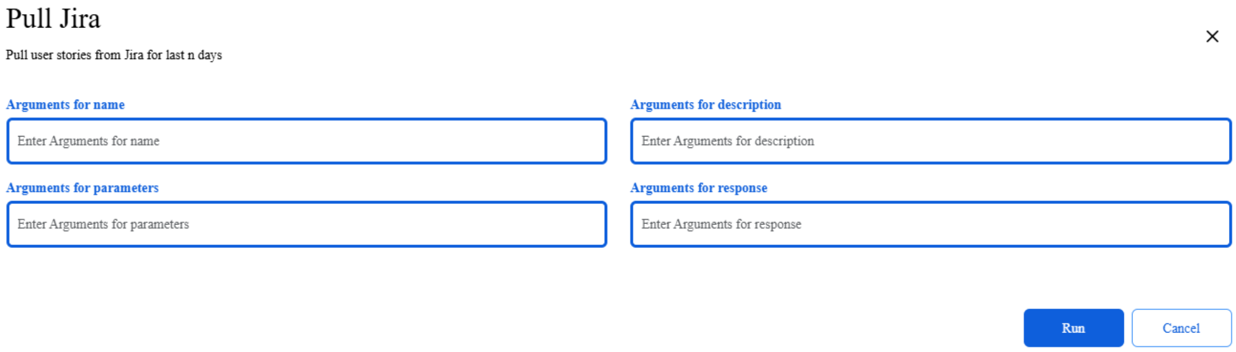
```
{
  "URL": "http://aiforce-mcs:8000/mcs/mcp-test/xyz123/mcp"
}
```

4. To view the primitives of the server, click the ellipses at the right end of the row, and click **View Primitives**. The Primitives page appears.



Pull user stories from Jira for last n days

   a. To try a tool, prompt, or resource, click the ellipses at the right end of the row, and click **Try**. The details of the tool, prompt, or resource appears.


Pull Jira
×
Arguments for name
Enter Arguments for name
Arguments for description
Enter Arguments for description
Arguments for parameters
Enter Arguments for parameters
Arguments for response
Enter Arguments for response
Run
Cancel

Pull user stories from Jira for last n days

   b. To run the tool, prompt, or resource, click **Run**. The output is displayed.
   c. To deactivate a tool, prompt, or resource, click the ellipses at the right end of the row, and click **Deactivate**. A confirmation page appears. Click

Yes to deactivate the tool, prompt, or resource. The status of the tool, prompt, or resource changes to Inactive.

   d. To remove a tool, prompt, or resource, click the ellipses at the right end of the row, and click Remove. A confirmation page appears. Click Yes to remove the tool, prompt, or resource from the AI Force enabled server.

5. To delete the AI Force enabled server, click the ellipses at the right end of the row, and click **Delete**. A confirmation page appears. Click **Yes** to delete the server.

9.2.2 External Servers

1. To view External Servers, click **External Servers**.
2. To edit the details of an external server, click the ellipses at the right end of the row, and click **Edit**. The details of the external server are displayed. Make the required changes and click **Test**. The connection is tested, and you can click **Publish MCP Server**.
3. To view the tools, prompts, and resources of the external server, click the ellipses at the right end of the row, and click **View Primitives**. The Tools, Prompts, and Resources are displayed under the respective tabs.
   a. To try out a tool, prompt, or resource, click the ellipses at the right end of the row, and click **Try**. The fields are displayed. Enter the required details, and click **Run**. The output is displayed.
   b. To deactivate a tool, prompt, or resource, click the ellipses at the right end of the row, and click **Deactivate**. A confirmation page appears. Click **Yes**, to deactivate the tool, prompt, or resource. The status changes to Inactive.
4. To delete the server, click the ellipses at the right end of the row, and click **Delete**. A confirmation page appears. Click **Yes**, to delete the server.

10 Governance and Evaluation Studio

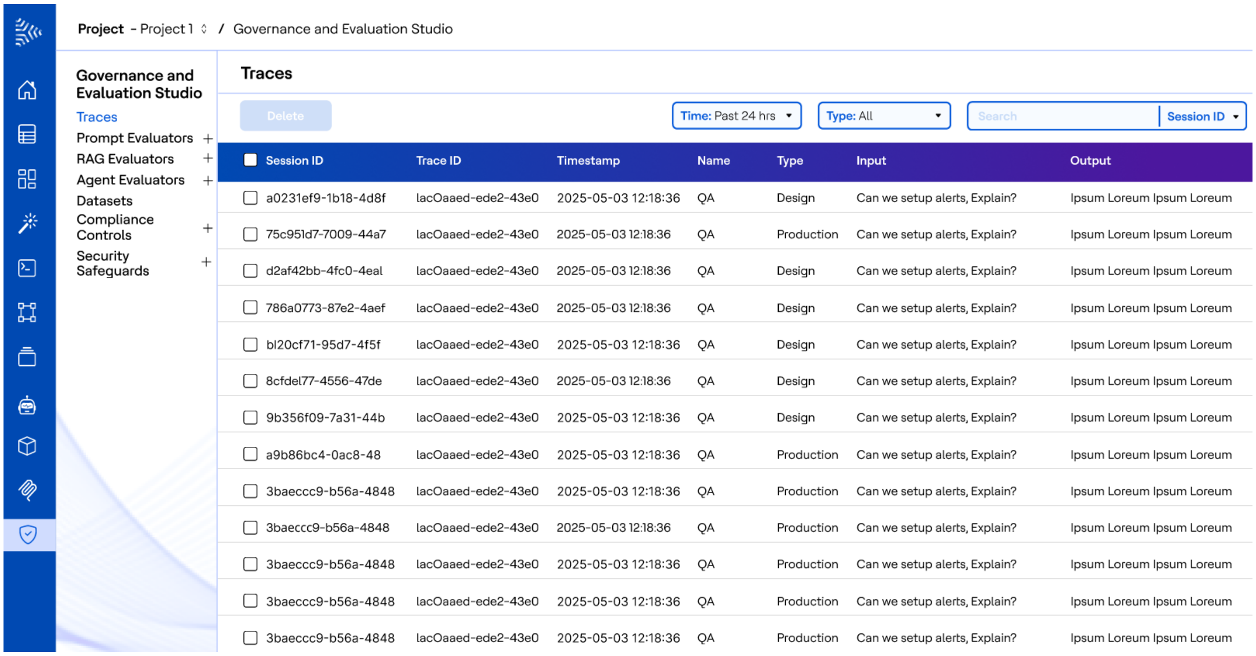
The Governance and Evaluation Studio allows you to:

- View Traces of the LLM calls made by prompts, RAGs, and Agents
- View and configure the default evaluators for Prompts, RAGs, and Agents
- Create, view, and configure the custom evaluators for Prompts, RAGs, and Agents
- View and create new Datasets to be used for evaluation of Prompts, RAGs, and Agents
- Manage compliance control of Prompt Quality
- Configure Input and Output Security Safeguards and create Security Groups to apply safeguards to agents

The Governance and Evaluation (G&E) Studio icon is the last icon in the AI Force left menu bar. Clicking on the icon will open the G&E studio with Traces being the default landing page.

10.1 Traces

1. Click (the Governance and Evaluation Studio icon) from the Menu bar. The Traces page appears by default.



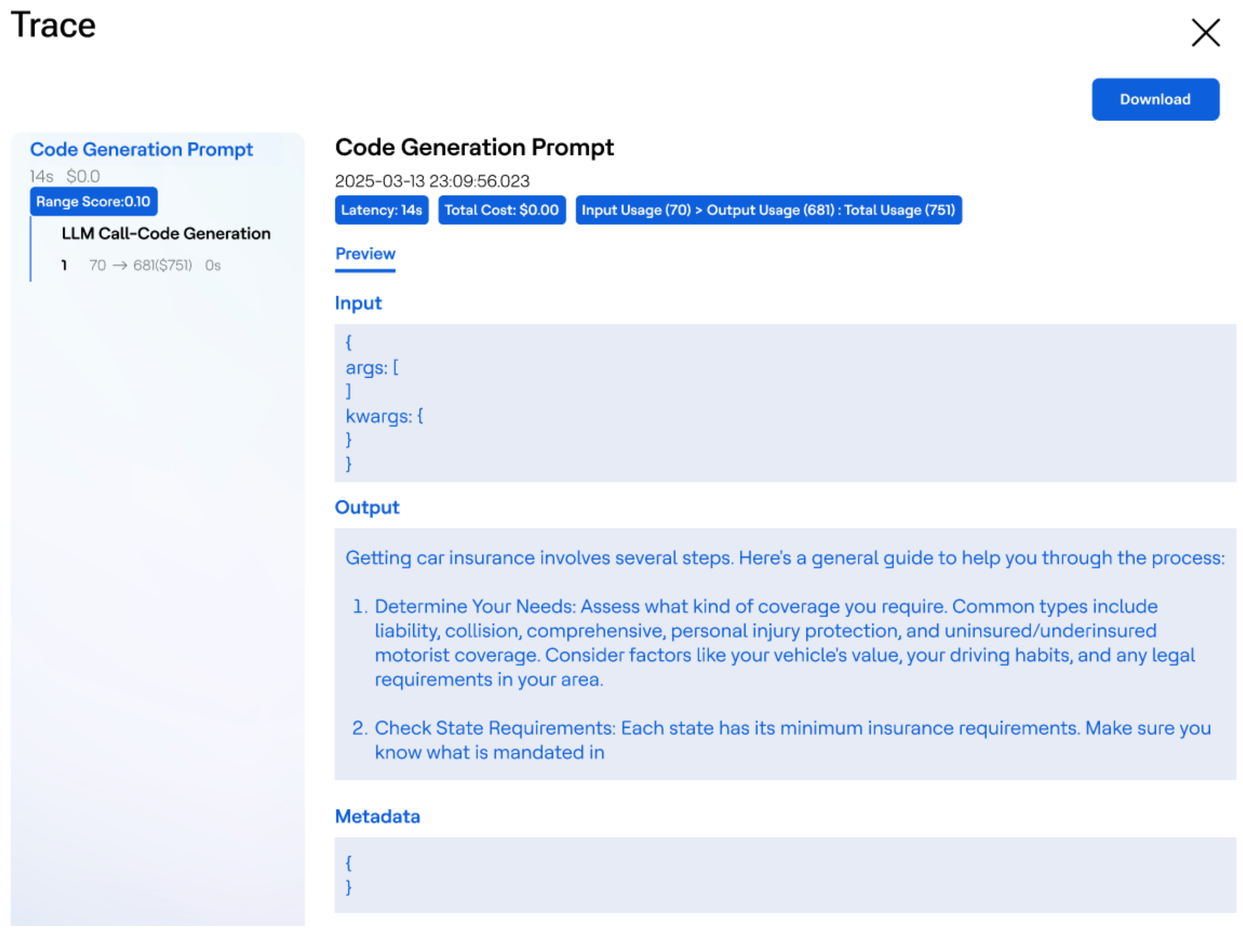
□ Session ID	Trace ID	Timestamp	Name	Type	Input	Output
□ a0231ef9-1b18-4d8f	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Design	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 75c951d7-7009-44a7	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Production	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ d2af42bb-4fc0-4eal	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Design	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 786a0773-87e2-4aef	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Design	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ bl20cf71-95d7-4f5f	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Design	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 8cfdel77-4556-47de	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Design	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 9b356f09-7a31-44b	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Design	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ a9b86bc4-0ac8-48	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Production	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 3baeccc9-b56a-4848	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Production	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 3baeccc9-b56a-4848	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Production	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 3baeccc9-b56a-4848	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Production	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 3baeccc9-b56a-4848	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Production	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum
□ 3baeccc9-b56a-4848	lacOaaed-ede2-43e0	2025-05-03 12:18:36	QA	Production	Can we setup alerts, Explain?	Ipsum Loreum Ipsum Loreum

You can filter the traces using:

- Time
- Type of trace
- Keyword-based search on Prompt Name or Session ID
- The number of rows displayed per page

If you have Admin access and if you select one or more traces, a Delete button gets activated, allowing you to delete the selected traces.

Click on a Trace to view details of the trace of the execution of the Prompt, RAG, or Agent.



Code Generation Prompt
14s $0.0
Range Score:0.10
LLM Call-Code Generation
1 70 → 681($751) 0s

Code Generation Prompt
2025-03-13 23:09:56.023
Latency: 14s | Total Cost: $0.00 | Input Usage (70) > Output Usage (681) : Total Usage (751)

Input

```
{
args: [
]
kwargs: {
}
}
```

Output

Getting car insurance involves several steps. Here's a general guide to help you through the process:

1. Determine Your Needs: Assess what kind of coverage you require. Common types include liability, collision, comprehensive, personal injury protection, and uninsured/underinsured motorist coverage. Consider factors like your vehicle's value, your driving habits, and any legal requirements in your area.
2. Check State Requirements: Each state has its minimum insurance requirements. Make sure you know what is mandated in

Metadata

```
{
}
```

You can view details of the LLM call made, Input, Output, Metadata, Latency, Cost, Input Usage, Output Usage, and Total Usage. Click **Download** to download a PDF of the currently opened trace view.

10.2 Prompt, RAG, Agent Evaluators

Prompt, RAG, Agent Evaluators allow you to do the following:

1. View existing default and custom evaluators (LLM as Judge based and Non LLM Based), configure their parameters and decide which evaluators to be kept as Active/Inactive based on requirements.
2. Create Custom Evaluators – both LLM as Judge based and Non LLM based, test them and Publish them.

The workflow for all three menu options in the G&E Studio menu – Prompt Evaluators, RAG Evaluators, Agent Evaluators is the same and is explained in the following steps.

- Click **Prompt, RAG, or Agent Evaluators**. The Default landing page displays LLM as Judge Evaluators with the Default Evaluators tab opened . Hover your mouse over ⓘ next to LLM as Judge heading to view what LLM as Judge is and how it works.

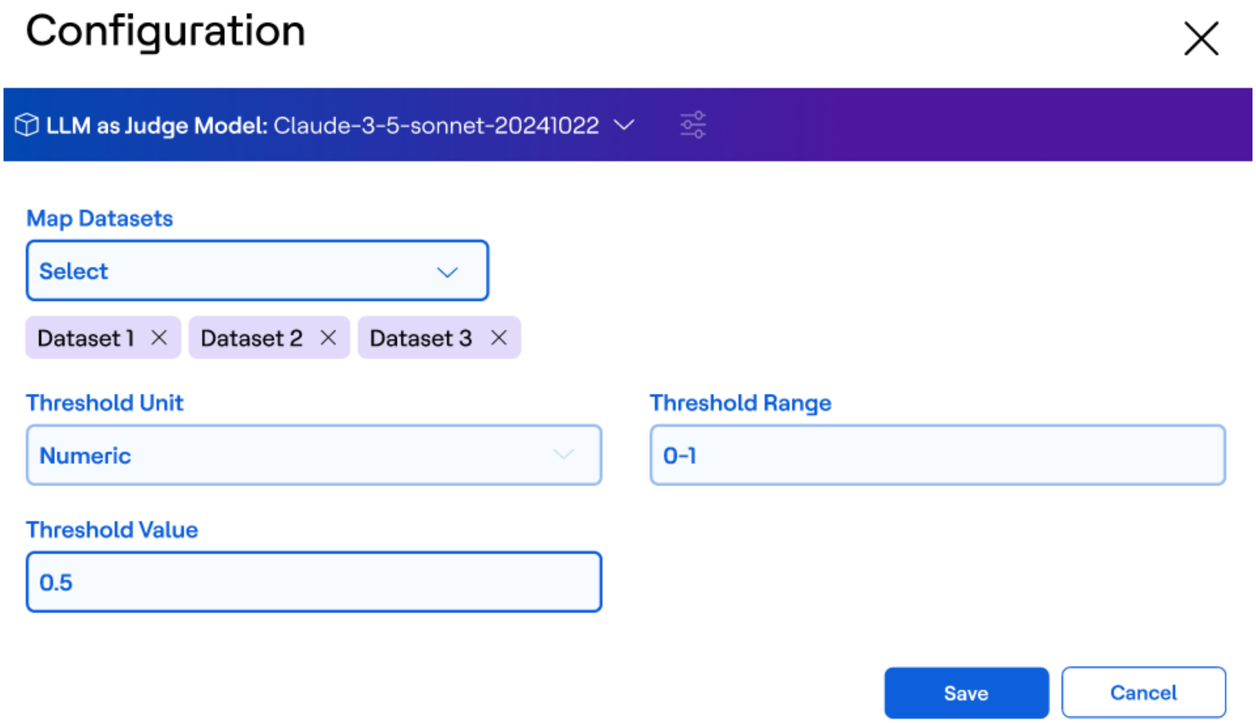
  The Default Evaluators tab lists the evaluators that are supported by the platform out of the box. The Custom Evaluators tab lists the evaluators created and published by the users.

  Evaluators marked as Active are available for running during the Prompt, RAG, or Agent evaluation in the Prompt, RAG, or Agent studios respectively. You can filter the evaluators based on State (Active, or Inactive), Status (Published or Draft), and/or using a keyword search.

- To deactivate the evaluator, click the ellipses (...) at the right end of the row, and click **Deactivate**. A Deactivate confirmation page appears. Click **Yes**, to deactivate the evaluator.

  To activate a deactivated evaluator, click the ellipses (...) at the right end of the row, and click **Activate**. An Activate confirmation page appears. Click **Yes**, to activate the evaluator.

- To configure the evaluator, click the ellipses (...) at the right end of the row, and click **Configure**. The Configuration page appears.



Configuration

LLM as Judge Model: Claude-3-5-sonnet-20241022

Map Datasets: Select

Dataset 1 × Dataset 2 × Dataset 3 ×

Threshold Unit: Numeric

Threshold Range: 0-1

Threshold Value: 0.5

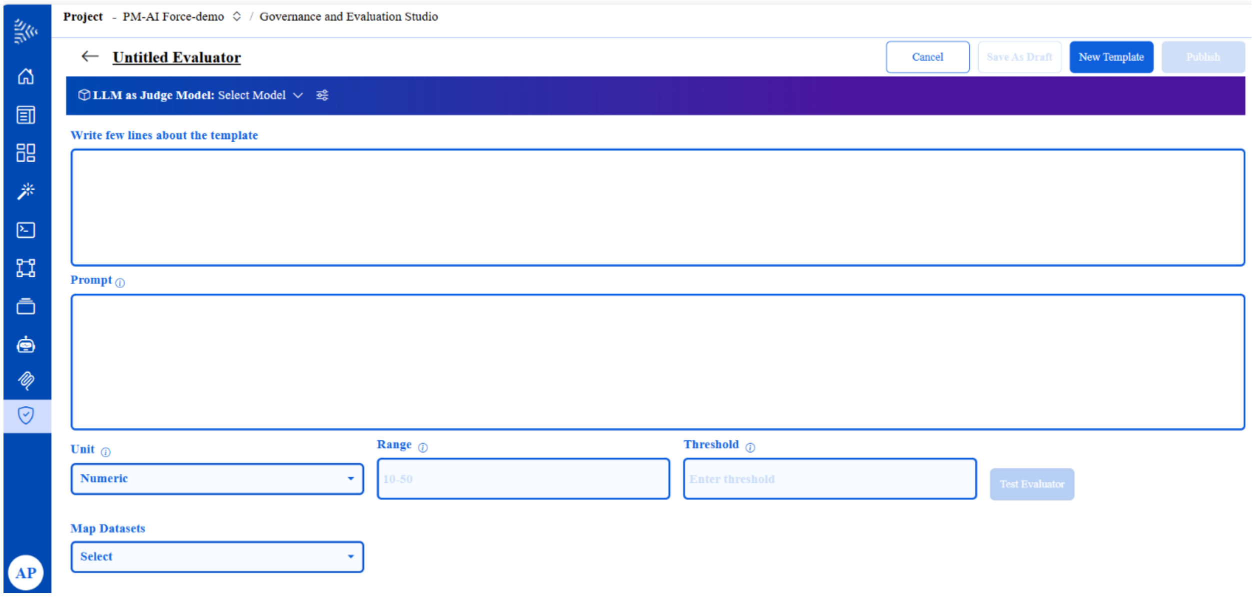
Select the pre uploaded datasets to be mapped to the evaluator. The number of datasets that are listed in the dataset dropdown at the time of evaluation is limited to the number of datasets mapped to the evaluator.

The Threshold Unit and Threshold Range field are provided for your reference and are un-editable. Enter the Threshold Value using the Threshold Unit and Threshold Range as reference. The Threshold Value determines if an evaluator passes or fails an evaluation. Click **Save**.

- Click the Custom Evaluators tab. Here again you can view evaluators that are in the Published or Draft status, view all the Evaluators or view Active or Inactive evaluators.

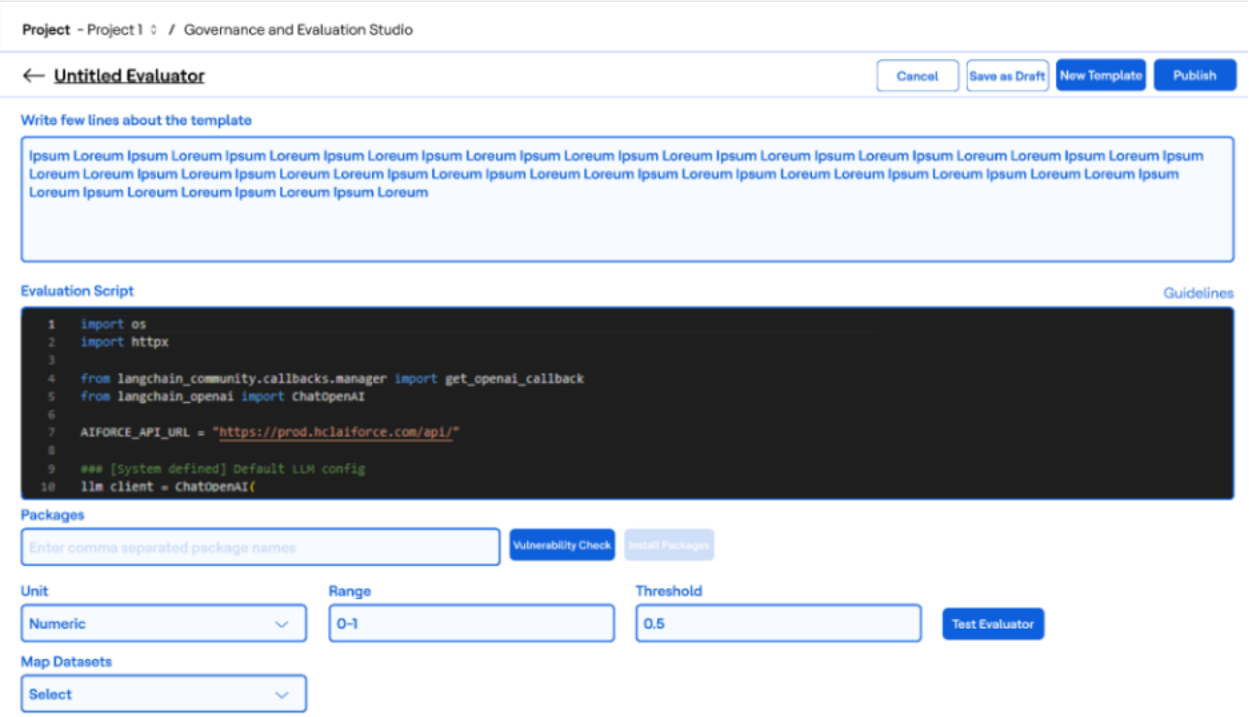
  The ellipses (...) button of a custom evaluator has two more options than the that of a default evaluator, namely Edit and Duplicate. Edit opens the evaluator creation page with all the details filled in, allowing you to edit the details. Duplicate creates a duplicate of the evaluator. You will have to enter a new name and some details to create a duplicate of the selected evaluator.

- With Custom Evaluators, you can create a new evaluator. Click New **Evaluator**. For LLM as Judge option you get the following page.



- Click **Untitled Evaluator** to name the Evaluator.
- Write a few lines about the evaluator.
- Enter the prompt.
- Enter the Unit, Range, and Threshold.
- Map the Datasets. Hover your mouse over the ⓘ icon to learn more about the fields. Once you have entered all the fields, click **Test Evaluator**. A page appears asking you to provide the test values. Provide the values and click **Test**. You can see the results of the custom evaluator and edit the evaluator, if needed. Once you are satisfied with the results, click **Publish**.

- Clicking New Evaluator for the Non LLM Based option opens the following page



Untitled Evaluator

Write few lines about the template

Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum Loreum Ipsum Loreum Ipsum Loreum Loreum Ipsum Loreum Ipsum Loreum Loreum Ipsum Loreum Ipsum Loreum Loreum Ipsum Loreum Ipsum Loreum Loreum Ipsum Loreum Ipsum Loreum Loreum Ipsum Loreum Ipsum Loreum Loreum Ipsum Loreum Ipsum Loreum Ipsum Loreum

Evaluation Script

```
import os
import httpx

from langchain_community.callbacks.manager import get_openai_callback
from langchain_openai import ChatOpenAI

AIFORCE_API_URL = "https://prod.hclaiforce.com/api/"

### [System defined] Default LLM config
llm client = ChatOpenAI(
```

Packages: Enter comma separated package names

Unit: Numeric

Range: 0-1

Threshold: 0.5

Map Datasets: Select

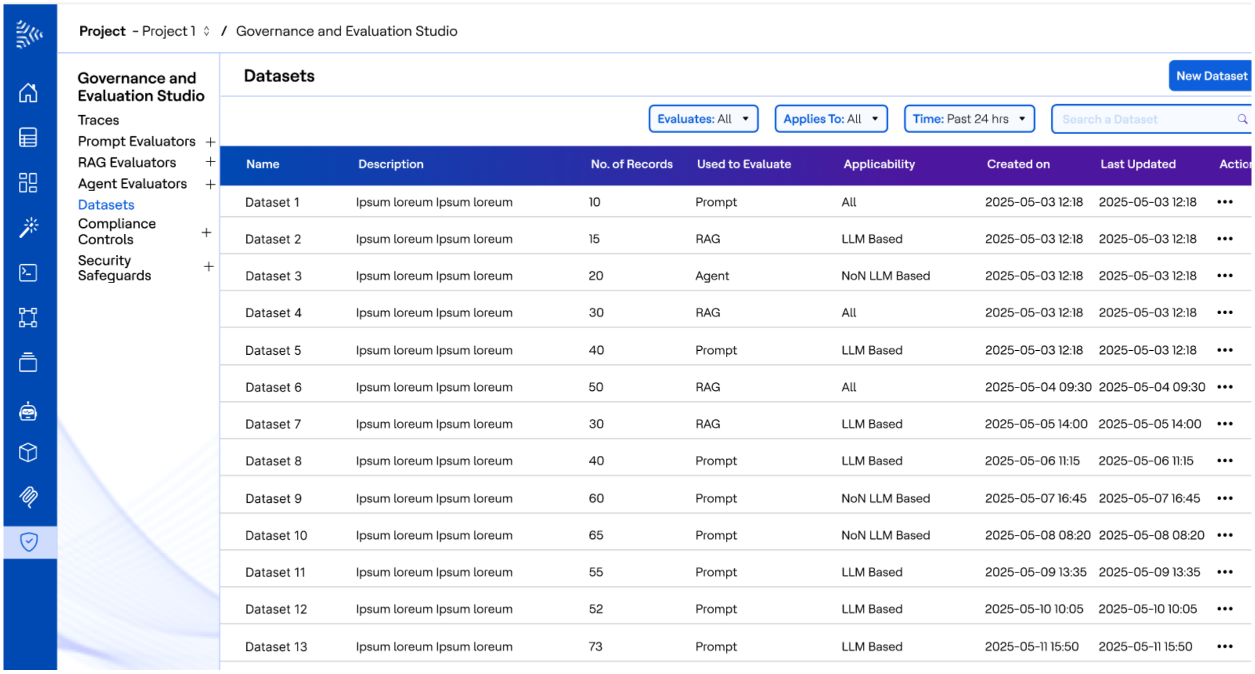
- ➢ Click **Untitled Evaluator** to name the evaluator,
- ➢ Write a few lines about the evaluator.
- ➢ As this is a Non LLM Based evaluator, you can define your code logic in the Evaluation Script box.
- ➢ If you are importing any packages in the script, mention them in the Packages field. These packages will later be installed in the internal virtual environment that is created for this custom evaluator.
- ➢ Click **Vulnerability Check** to run a vulnerability check on the packages before installing them. Once the vulnerability check passes, click **Install Packages**.
- ➢ Enter the Unit, Rate, and Threshold.
- ➢ Map the Datasets. Hover your mouse over the ⓘ icon to learn more about the fields. Once you have entered all the fields, click **Test Evaluator**. A page appears asking you to provide the test values. Provide the values and click **Test**. You can see the results of the custom evaluator and edit the evaluator, if needed. Once you are satisfied with the results, click **Publish**.

10.3 Datasets

Datasets form the backbone of the evaluation as they allow the users to cover various possible scenarios for testing their prompts/RAGs/Agents before publishing them.

The Datasets tab in AI Force acts as the central repository for all evaluation datasets in the platform. You can upload new datasets, view existing datasets, edit datasets and delete them.

1. Click **Datasets**. The Datasets page appears.

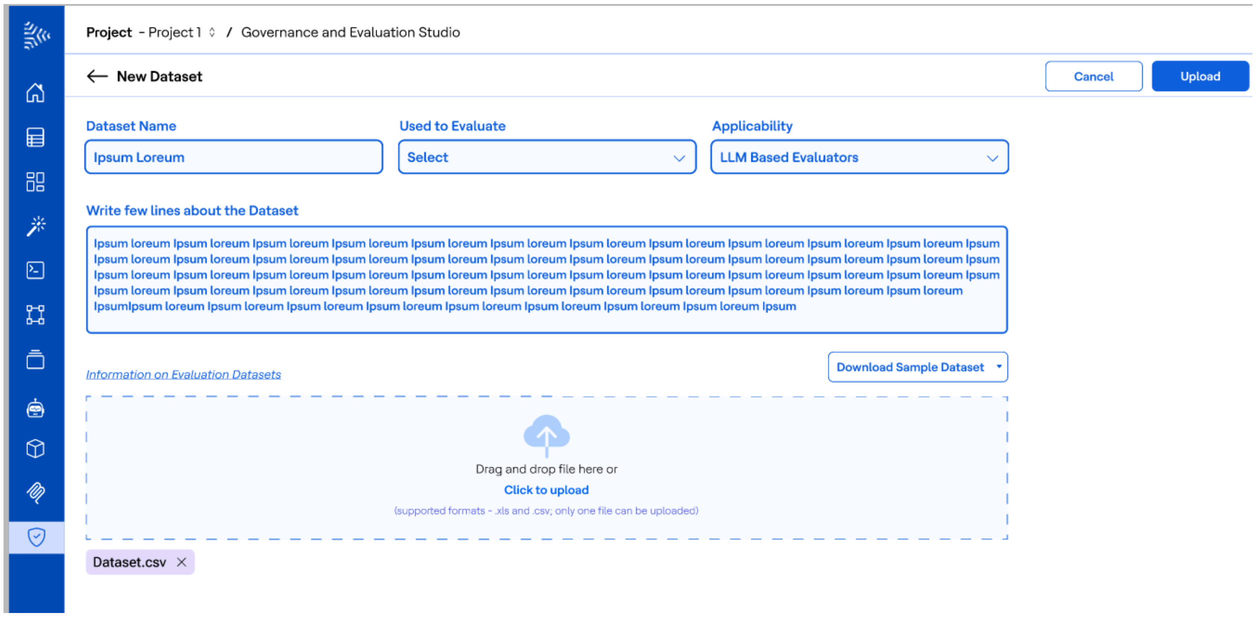


Name	Description	No. of Records	Used to Evaluate	Applicability	Created on	Last Updated	Actio
Dataset 1	Ipsum loreum Ipsum loreum	10	Prompt	All	2025-05-03 12:18	2025-05-03 12:18	•••
Dataset 2	Ipsum loreum Ipsum loreum	15	RAG	LLM Based	2025-05-03 12:18	2025-05-03 12:18	•••
Dataset 3	Ipsum loreum Ipsum loreum	20	Agent	NoN LLM Based	2025-05-03 12:18	2025-05-03 12:18	•••
Dataset 4	Ipsum loreum Ipsum loreum	30	RAG	All	2025-05-03 12:18	2025-05-03 12:18	•••
Dataset 5	Ipsum loreum Ipsum loreum	40	Prompt	LLM Based	2025-05-03 12:18	2025-05-03 12:18	•••
Dataset 6	Ipsum loreum Ipsum loreum	50	RAG	All	2025-05-04 09:30	2025-05-04 09:30	•••
Dataset 7	Ipsum loreum Ipsum loreum	30	RAG	LLM Based	2025-05-05 14:00	2025-05-05 14:00	•••
Dataset 8	Ipsum loreum Ipsum loreum	40	Prompt	LLM Based	2025-05-06 11:15	2025-05-06 11:15	•••
Dataset 9	Ipsum loreum Ipsum loreum	60	Prompt	NoN LLM Based	2025-05-07 16:45	2025-05-07 16:45	•••
Dataset 10	Ipsum loreum Ipsum loreum	65	Prompt	NoN LLM Based	2025-05-08 08:20	2025-05-08 08:20	•••
Dataset 11	Ipsum loreum Ipsum loreum	55	Prompt	LLM Based	2025-05-09 13:35	2025-05-09 13:35	•••
Dataset 12	Ipsum loreum Ipsum loreum	52	Prompt	LLM Based	2025-05-10 10:05	2025-05-10 10:05	•••
Dataset 13	Ipsum loreum Ipsum loreum	73	Prompt	LLM Based	2025-05-11 15:50	2025-05-11 15:50	•••

You can view all Datasets, or view the datasets that evaluate a prompt, RAG, or agent. Similarly, you can view all the datasets, or those that are LLM-based, or non LLM-based. You can specify a time period to view datasets that were created within the time period. You can view datasets based on a keyword search.

10.3.1 New Dataset

1. To create a new dataset, click **New Dataset**. The New Dataset page appears.


Project - Project 1 / Governance and Evaluation Studio
New Dataset
Cancel
Upload
Information on Evaluation Datasets
Download Sample Dataset
Drag and drop file here or
Click to upload
(supported formats - .xls and .csv; only one file can be uploaded)

Dataset Name: Ipsum Loreum

Used to Evaluate: Select

Applicability: LLM Based Evaluators

Write few lines about the Dataset

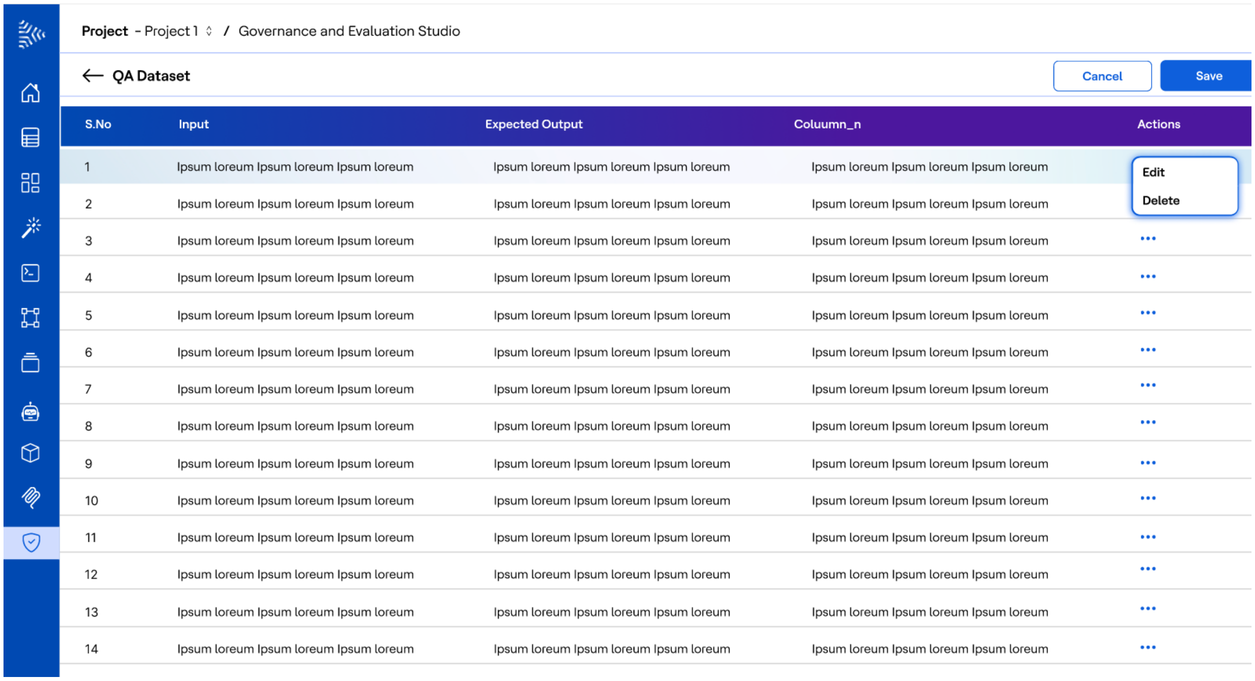
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum IpsumIpsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum

Dataset.csv ×

2. Enter the dataset name.
3. Select if the dataset is used to evaluate a prompt, RAG, or tool.
4. Select if the dataset applies to LLM-based or Non LLM-based evaluators.
5. Write a few lines describing the dataset.
6. Click and upload Excel or CSV files.
7. Click **Upload** to save the dataset.
8. For your ease of use, two additional functionalities are provided:
    a. Information on Evaluation Datasets: Clicking on this link opens up a page detailing what is an evaluation dataset and what information and fields should an evaluation dataset contain for prompt, RAG and agent.
    b. Download sample dataset – This drop down allows you to download sample datasets for prompt, RAG and agent evaluation. The downloaded datasets are in csv format and contain the reference column headers explained in the Information on Evaluation Datasets page.

10.3.2 Open a Dataset

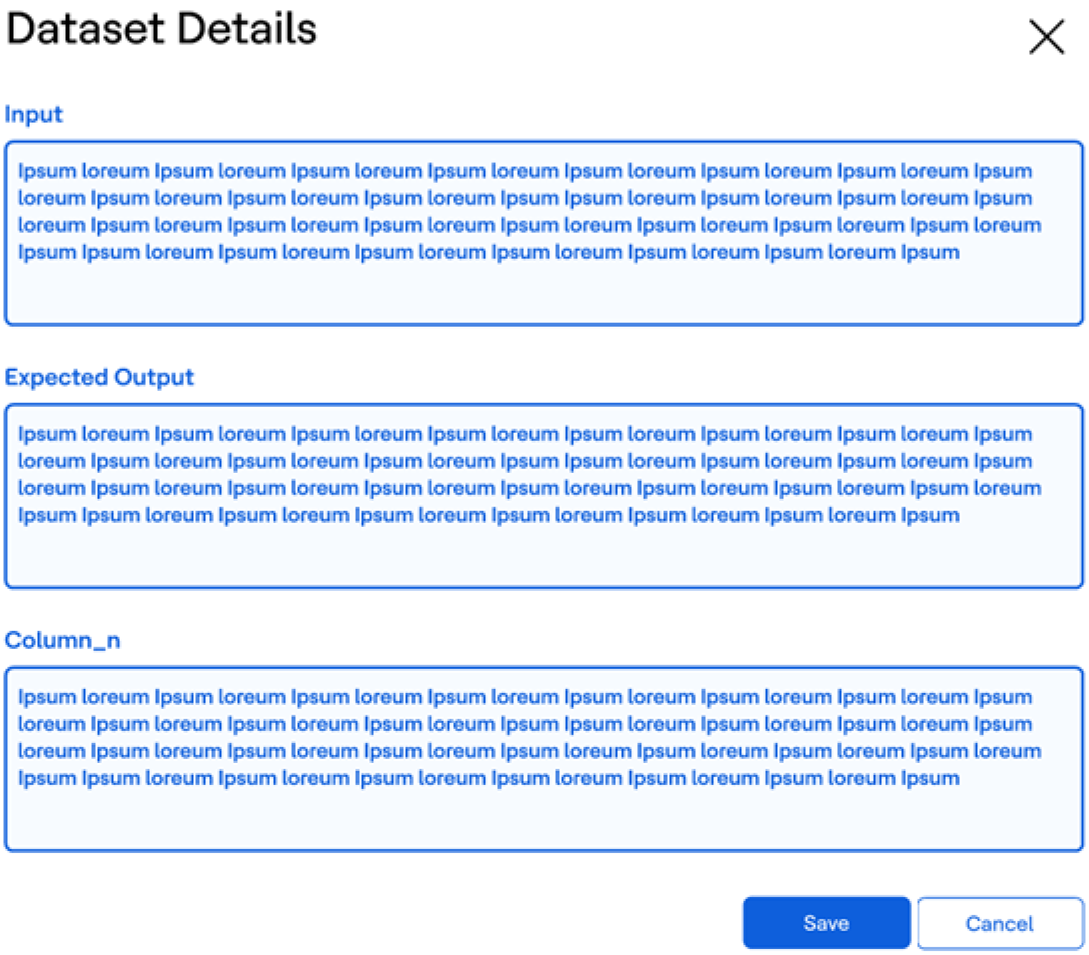
1. To open a existing dataset, go to the dataset landing page and click the ellipses (...) button at the right end of the row of the dataset you want to open and click **Open**. The dataset page appears.



S.No	Input	Expected Output	Coluumn_n	Actions
1	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Edit Delete
2	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	
3	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
4	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
5	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
6	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
7	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
8	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
9	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
10	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
11	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
12	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
13	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...
14	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	Ipsum loreum Ipsum loreum Ipsum loreum	...

The input, expected output, and other relevant columns are displayed. There is also another column (Action) containing the Actions ellipses button.

2. To edit the row, click the ellipses (...) at the right end of the row and click **Edit**.



Dataset Details

Input

Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum

Expected Output

Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum

Column_n

Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum

Make the required changes and click **Save**.

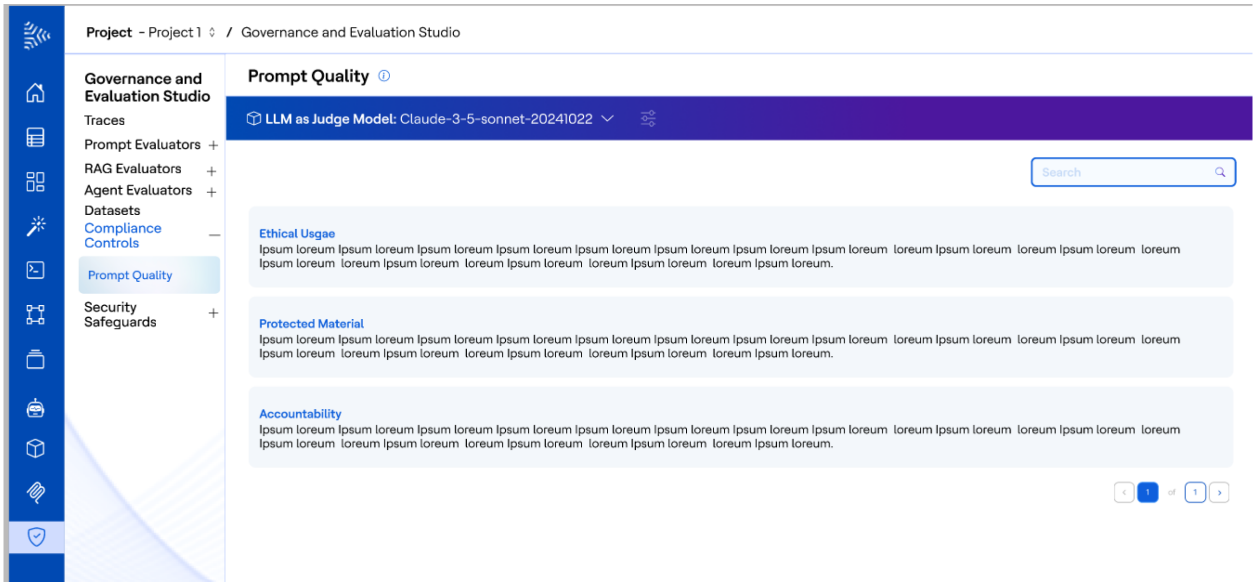
3. To delete a record of the dataset, click the ellipses (...) at the end of the row and click **Delete**. A Delete confirmation page appears. Click **Yes** to delete the record.
4. To delete a dataset, go to the Dataset landing page and click the ellipses (...) at the right end of the row and click **Delete**. A Delete confirmation dialog page appears. Click **Yes** to delete the dataset.

10.4 Compliance Controls

The Prompt Quality feature under Compliance Controls, allows you to review the user-provided prompts against best practices guidelines localized from Azure Open AI Customer Copyright Commitment and other sources. Hover your mouse over ⓘ to learn more about this feature.

Currently only Prompt Quality controls are supported and they use LLM as Judge to evaluate whether the written prompt complies with the configured guidelines in the AI

Force platform. You can configure the Judge LLM on the landing page – Prompt Quality Controls.



Prompt Quality

LLM as Judge Model: Claude-3-5-sonnet-20241022

Ethical Usgae
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

Protected Material
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

Accountability
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

The Quality controls are pre-configured you cannot edit them. You can only configure the Judge LLM for the controls. Name of the controls along with a single liner explanation is provided in the list on the landing page.

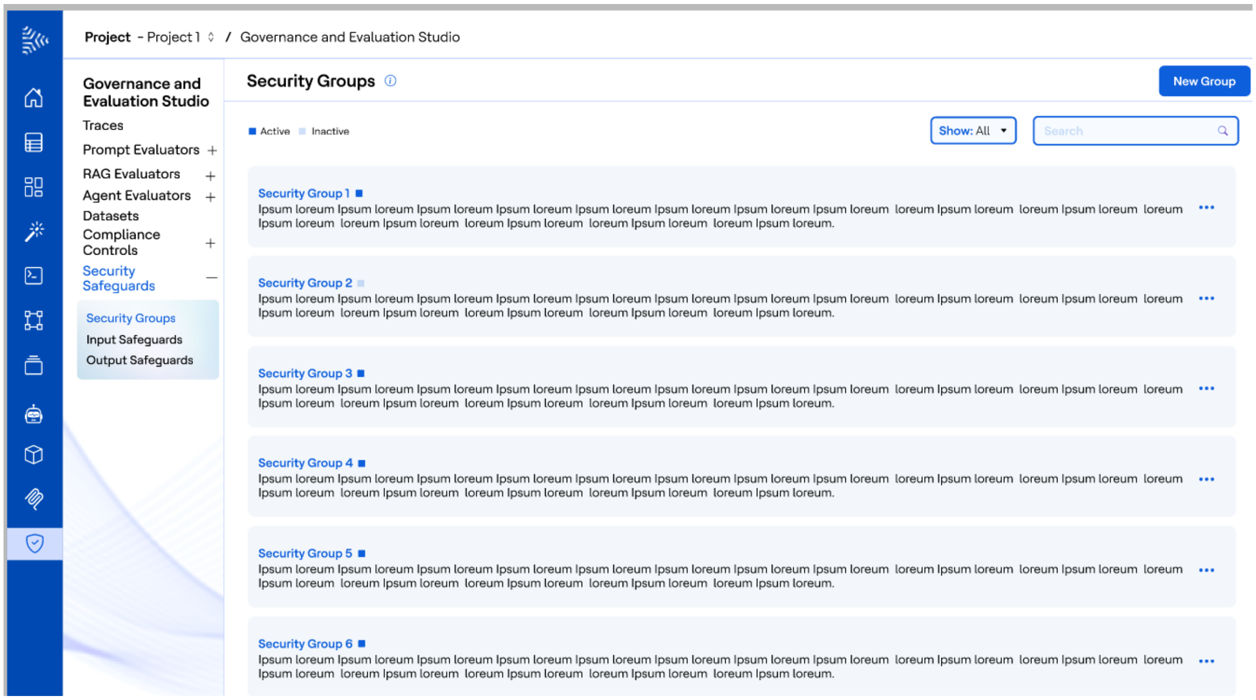
10.5 Security Safeguards

Security Safeguards allow you to control the input that goes into the LLM and the output that is generated by the LLM. AI Force provides both input and output security safeguards for the end users to configure as per their requirements, combine them together as a security group and tag the security group to an agent (that is used in a use case) to ensure compliance.

10.5.1 Security Groups

For information about security groups, hover your mouse over ⓘ icon that is placed alongside the Security Groups heading on the landing page of security group menu.

When you land on the Security Groups landing page, you can see the list of available security groups and other options as explained below:



Security Group 1 ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

Security Group 2 ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

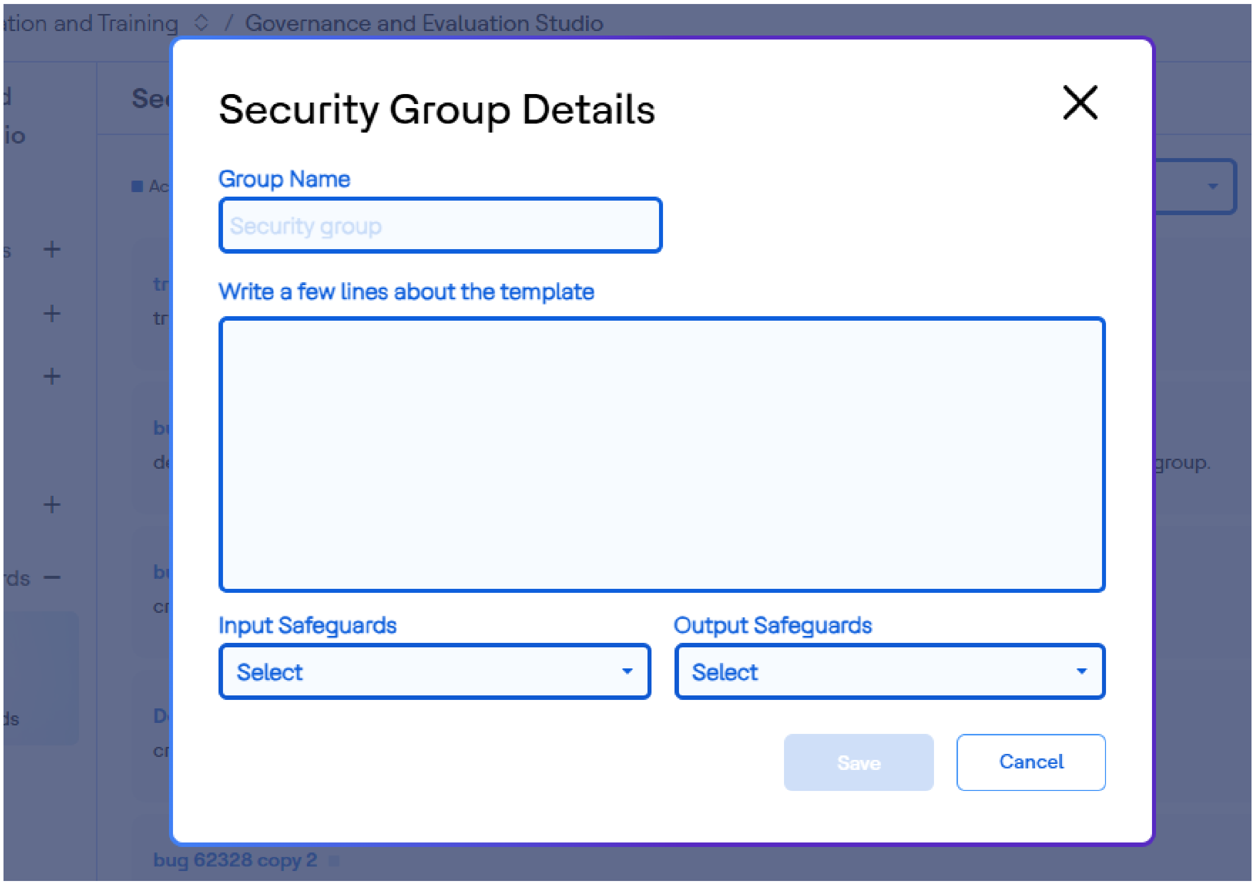
Security Group 3 ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

Security Group 4 ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

Security Group 5 ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

Security Group 6 ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum.

1. To Deactivate an Active Security Group or to activate a deactivated security group, click the ellipses (...) at the right end of the row and click **Deactivate** or **Activate**.
2. To edit a security group, click the ellipses (...) at the right end of the row and click **Edit**.
3. To duplicate a security group, click the ellipses (...) at the right end of the row and click **Duplicate**. You will have to enter the new name and description of the security group.
4. To delete a security group, click the ellipses (...) at the right end of the row and click **Delete**. A Delete confirmation page appears. Click **Yes** to delete the security group.
5. To create a new security group, click **New Group**.



Security Group Details

Group Name

Security group

Write a few lines about the template

Input Safeguards

Select

Output Safeguards

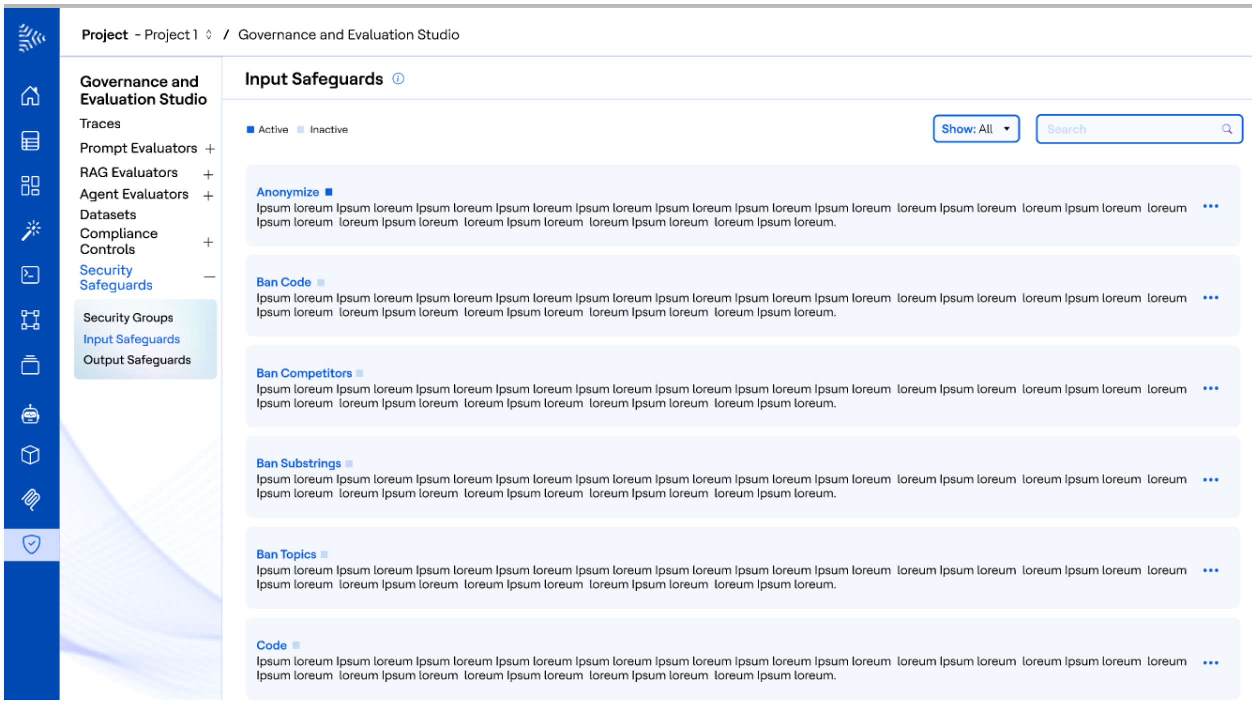
Select

6. Enter the **Security Group name**. Select the relevant input and output security safeguards (users are advised to check the configuration on individual safeguards before creating a security group). Click **Save**.

10.5.2 Input Safeguards

You can view all the input safeguards in AI Force. For information about input safeguards, hover your ⓘ ouse over icon placed alongside the heading of the page.

When you land on the Input Safeguards landing page, you can see the list of available input safeguards and other options as explained below:



Anonymize ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Ban Code ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Ban Competitors ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Ban Substrings ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Ban Topics ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Code ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

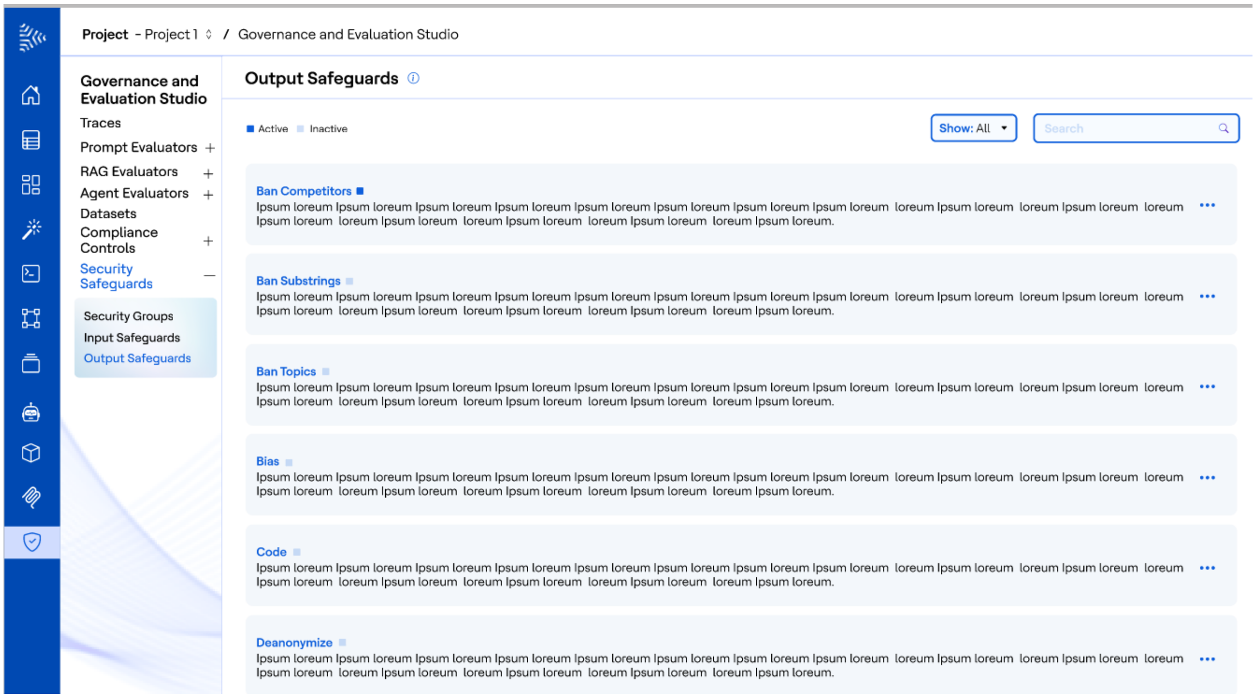
1. To deactivate an active input safeguard, or to activate a deactivated safeguard, click the ellipses (...) at the right end of the row and click **Deactivate** or **Activate**.
2. To configure an input safeguard, click the ellipses (...) at the right end of the row and click Configure. The Configuration page appears. You can configure the safeguard based on your requirements. Certain safeguards such as Detect Toxicity will not have any configuration options and hence will show a message: No Configuration options are available for this safeguard.
3. Safeguards such as Detect PII, Detect Code Language, Detect Secrets will have drop-downs with pre-filled values. You can select multiple values from the drop-down based on your requirements.
4. Safeguards such as Detect Banned Substrings and Detect Competitors require human input to define those values and hence the configure page for them will vary accordingly.

10.5.3 Output Safeguards

You can view all the Output Safeguards in AI Force. For information on Output Safeguards, hover your ⓘ ouse over icon placed alongside the heading of the page.

When you land on the Output Safeguards landing page, you can see the list of available output safeguards and other options as explained below:

.



Ban Competitors ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Ban Substrings ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Ban Topics ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Bias ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

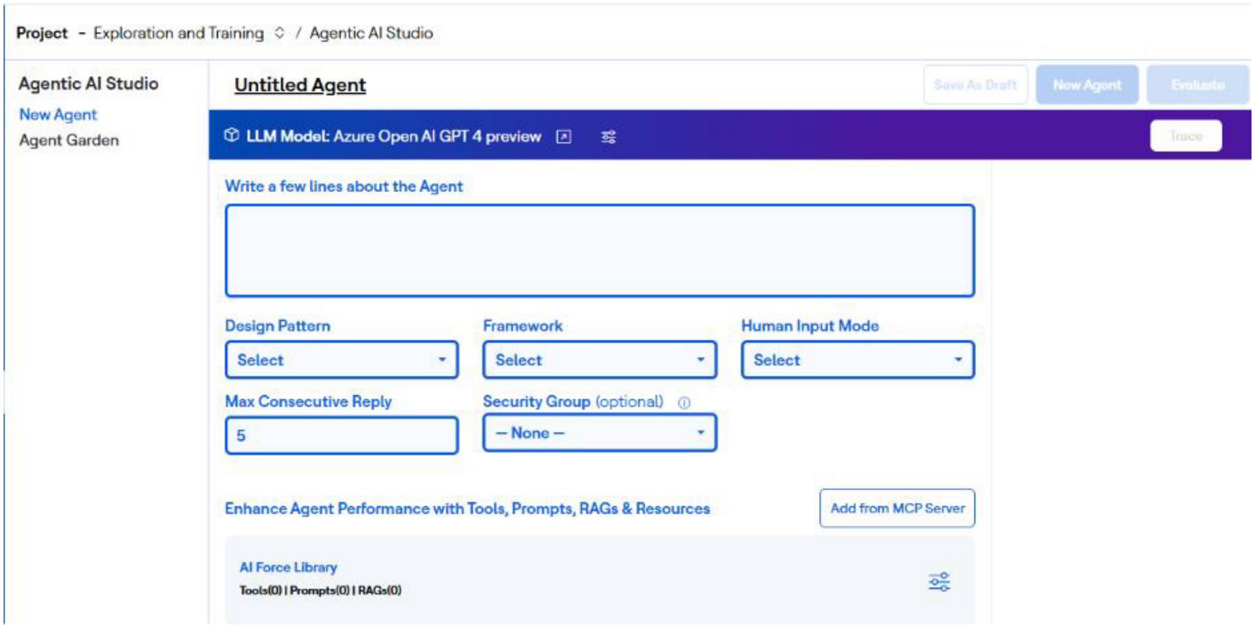
Code ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

Deanonymize ■
Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum loreum Ipsum loreum. •••

1. To deactivate an active output safeguard, or to activate a deactivated safeguard, click the ellipses (...) at the right end of the row and click **Deactivate** or **Activate**.
2. To configure an output safeguard, click the ellipses (...) at the right end of the row and click **Configure**. The Configuration page appears. You can configure the safeguard based on your requirements. Certain safeguards such as Detect Toxicity will not have any configuration options and hence will show a message: No Configuration options are available for this safeguard.
3. Safeguards such as Detect PII, Detect Code Language, Detect Secrets will have drop-downs with pre-filled values. You can select multiple values from the drop-down based on your requirements.
4. Safeguards such as Detect Banned Substrings and Detect Competitors require human input to define those values and hence the configure page for them will vary accordingly.

10.5.4 Applying a Security Group to an Agent

During agent creation in Agent studio, you can tag a security group to an agent by selecting a security group from the Security Group drop-down as shown in the image below. Once saved, whenever that particular agent is run as part of a use case in AI Force, the input/output security safeguards which are a part of the security group tagged to the agent are executed to ensure compliance.



Untitled Agent

LLM Model: Azure Open AI GPT 4 preview

Write a few lines about the Agent

Design Pattern: Select

Framework: Select

Human Input Mode: Select

Max Consecutive Reply: 5

Security Group (optional): – None –

Enhance Agent Performance with Tools, Prompts, RAGs & Resources

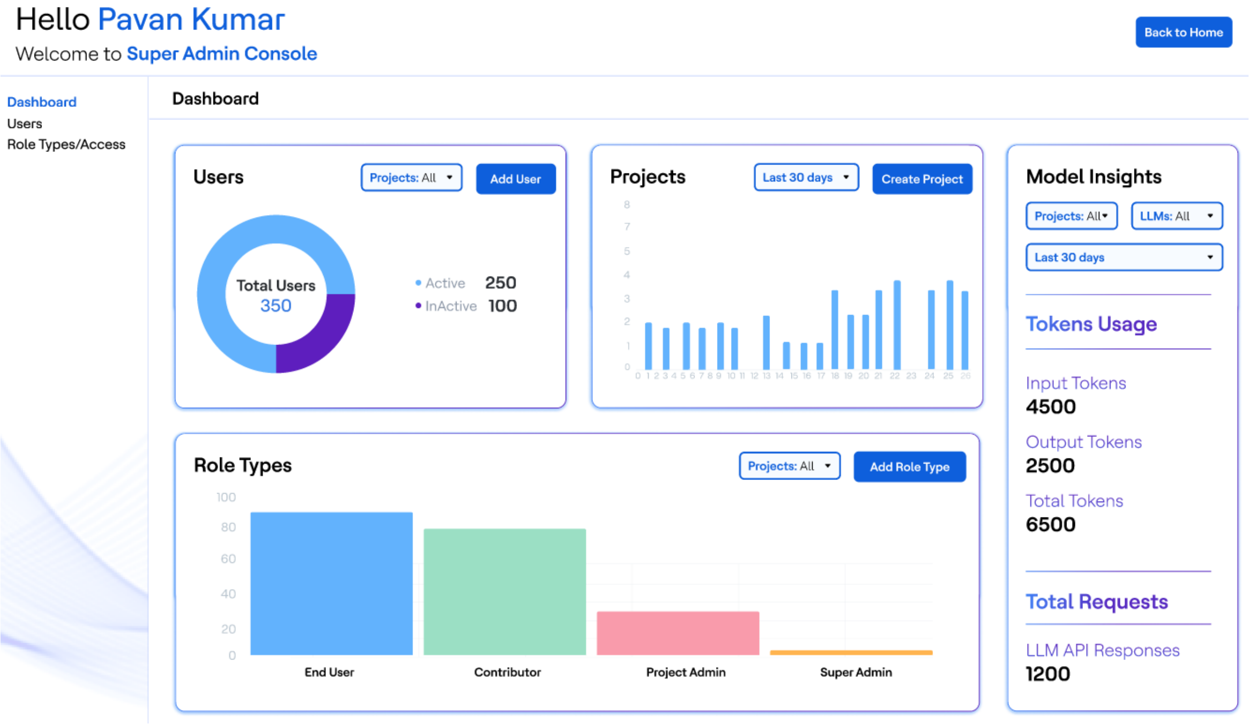
AI Force Library

Tools(0) | Prompts(0) | RAGs(0)

11 Super Admin User

Users with Super Admin privileges can access the Super Admin Console, which provides complete visibility and control across the platform. From this console, Super Admins can view and edit all projects, users, and associated information. Super Admins have broader access rights compared to Project Admins — they can create new users, define new role types, and control access permissions for each role type.

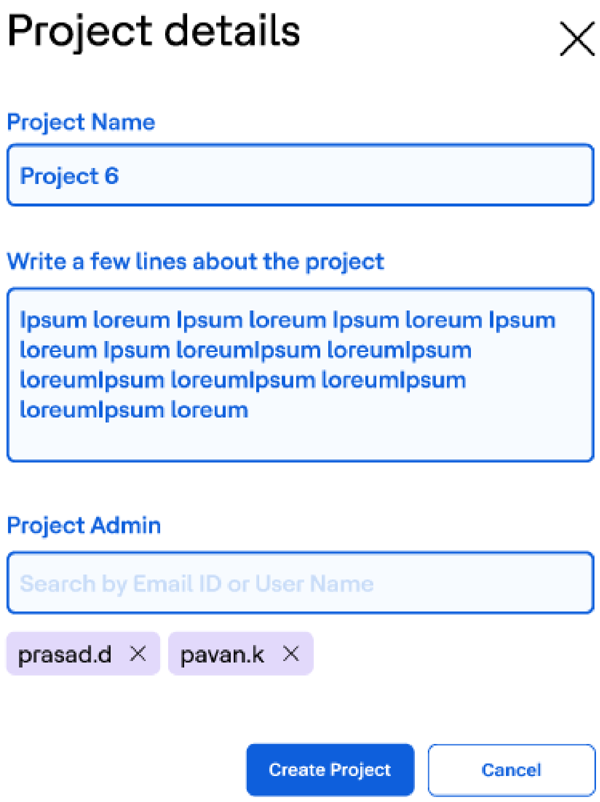
If your role is that of a Super Admin and you are logged in, your login is shown at the bottom of the menu bar. Click the icon and click **Super Admin console**.



11.1 Dashboard

You can view the dashboard consisting of Users, Projects, Role Types, and Model Insights. You can create new users, create projects, and create new role types using the dashboard. You can also create user from the Users option and create new role types using the Role Type/Access option.

To create a new project, click **Create Project**.


Project details

Project Name

Project 6

Write a few lines about the project

Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreum Ipsum loreumIpsum loreumIpsum loreumIpsum loreumIpsum loreumIpsum loreumIpsum loreum

Project Admin

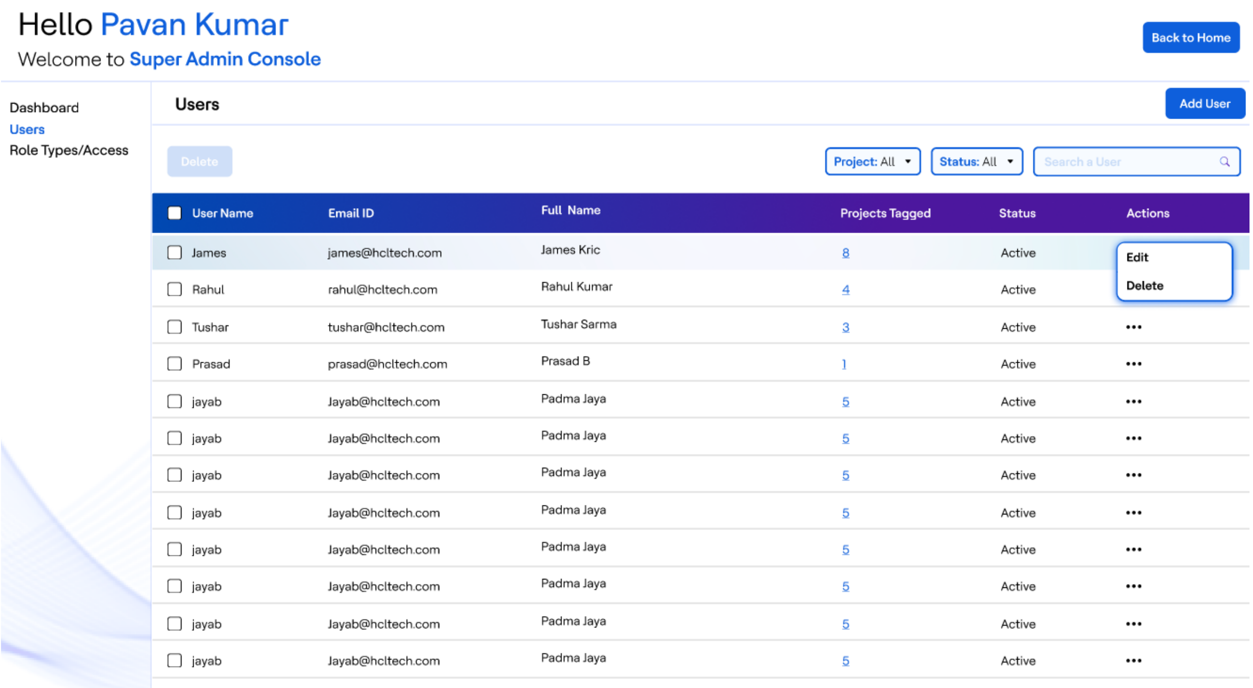
Search by Email ID or User Name

prasad.d × pavan.k ×

Enter the project name, write a few lines about the project, select the project admin. Click **Create Project**.

11.2 Users

1. To view the users click **Users**. You can filter the list of users displayed based on the selected projects, or you can list users of all projects. Similarly, you can filter users based on Active, Inactive, or display all projects.

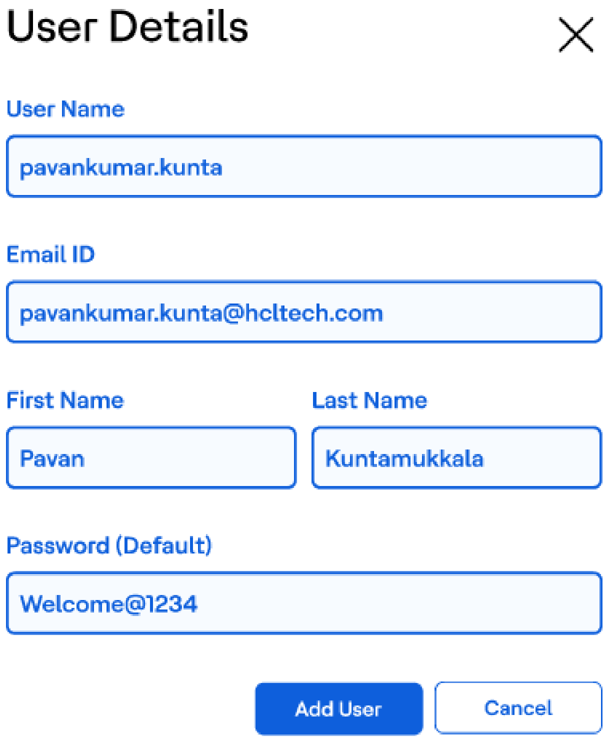

Hello Pavan Kumar

Welcome to Super Admin Console

Users

□ User Name	Email ID	Full Name	Projects Tagged	Status	Actions
□ James	james@hcltech.com	James Kric	8	Active	Edit Delete
□ Rahul	rahul@hcltech.com	Rahul Kumar	4	Active	
□ Tushar	tushar@hcltech.com	Tushar Sarma	3	Active	•••
□ Prasad	prasad@hcltech.com	Prasad B	1	Active	•••
□ jayab	Jayab@hcltech.com	Padma Jaya	5	Active	•••
□ jayab	Jayab@hcltech.com	Padma Jaya	5	Active	•••
□ jayab	Jayab@hcltech.com	Padma Jaya	5	Active	•••
□ jayab	Jayab@hcltech.com	Padma Jaya	5	Active	•••
□ jayab	Jayab@hcltech.com	Padma Jaya	5	Active	•••
□ jayab	Jayab@hcltech.com	Padma Jaya	5	Active	•••
□ jayab	Jayab@hcltech.com	Padma Jaya	5	Active	•••
□ jayab	Jayab@hcltech.com	Padma Jaya	5	Active	•••

2. To create a new user, click **Add User**.


User Details

User Name: pavankumar.kunta

Email ID: pavankumar.kunta@hcltech.com

First Name: Pavan

Last Name: Kuntamukkala

Password (Default): Welcome@1234

Enter the user name, the email ID, the first name and last name, and the default password of the user. Click **Add User**.

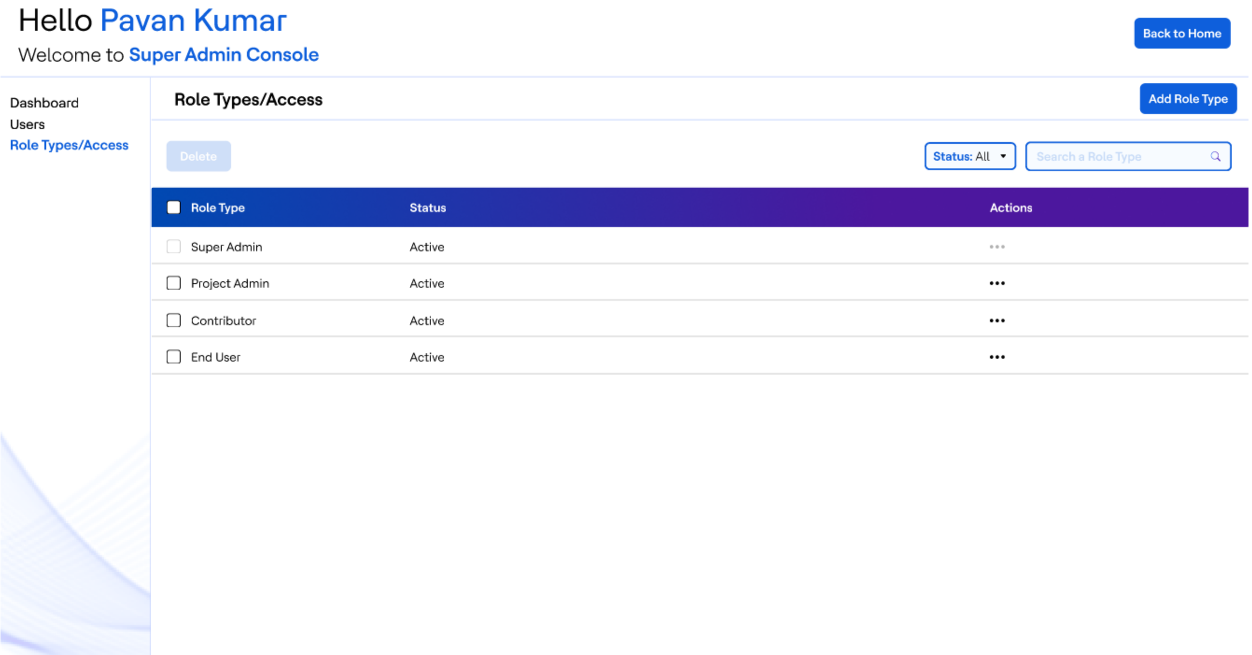
Note:

When a **Super Admin** creates a new user from the platform, the user is first registered in **Keycloak** for authentication management. Once the user logs in using the provided credentials, the user details are automatically saved in the **AI Force User Repository**. After successful creation and login, the user can be invited to any project by a **Project Admin** based on access and role requirements.

3. To edit the details of a user, click the ellipses (...) at the right end of the row, and click **Edit**. To delete a user, click the ellipses (...) at the right end of the row, and click **Delete**. A Delete confirmation dialog page appears. Click **Yes** to delete the user.

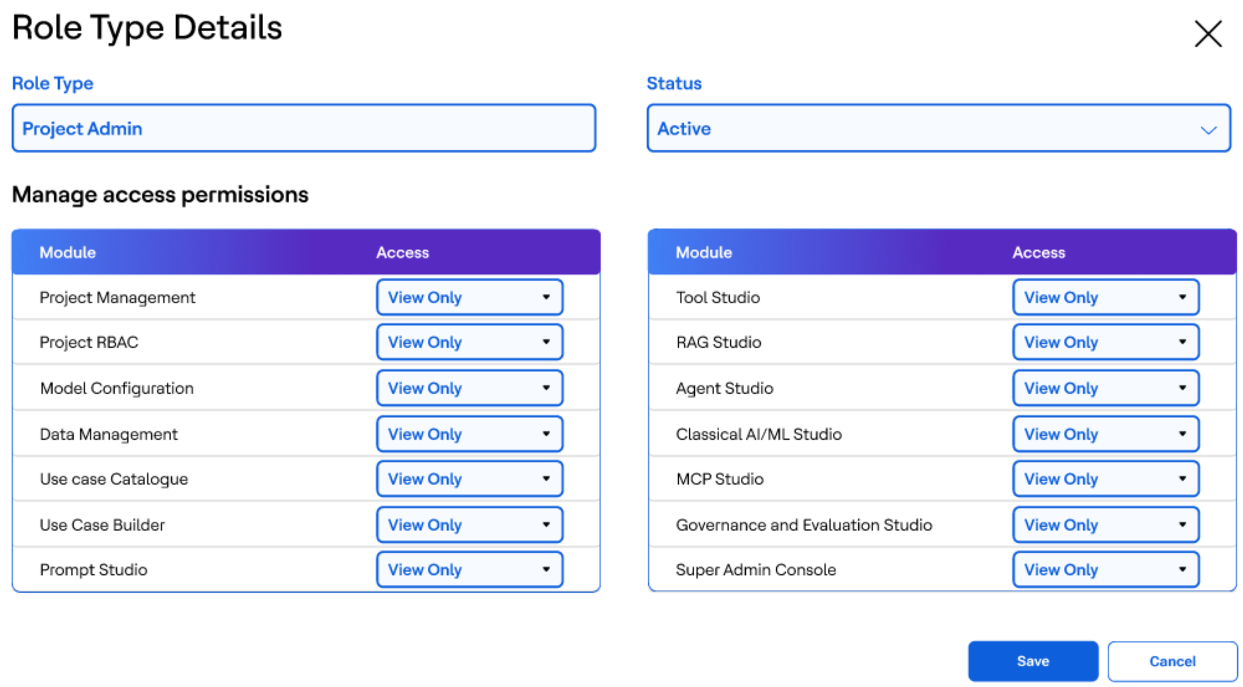
11.3 Role Type/Access

You can view the role types using the Role Types/Access option in Super Admin console.



Role Type	Status	Actions
Super Admin	Active	...
Project Admin	Active	...
Contributor	Active	...
End User	Active	...

1. To edit a role type, click the ellipses (...) in the Actions column and click **Edit**. Make the changes to the access permissions and click **Save**.
2. To add a new role type, click **Add Role Type**.



Role Type Details

Role Type: Project Admin

Status: Active

Manage access permissions

Module	Access
Project Management	View Only
Project RBAC	View Only
Model Configuration	View Only
Data Management	View Only
Use case Catalogue	View Only
Use Case Builder	View Only
Prompt Studio	View Only

Module	Access
Tool Studio	View Only
RAG Studio	View Only
Agent Studio	View Only
Classical AI/ML Studio	View Only
MCP Studio	View Only
Governance and Evaluation Studio	View Only
Super Admin Console	View Only

Enter Role Type, and select Status. Set the access permissions to various modules. Click **Save**.