Use And POC on AI Agents

In the Pega Infinity 25' version there are many changes that are being introduced when compared to last previous releases. There are new rules that are being introduced are AI Agents and Tool.

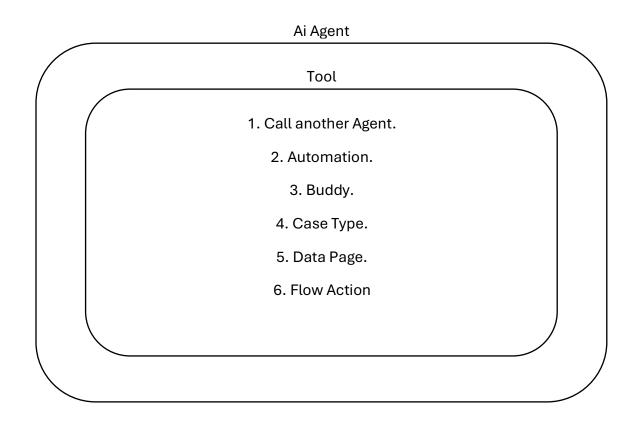
Ai Agents:

This new rule is not just like an Ordinary Agent it has its own agenda and brain. And It does not come under AI Chatbot as well. Or this is not something like Gen Ai connect rule in pega.

Different Between traditional Agents and Al Agent Rule:

Traditional Agents	Gen Al Agent
 Manual and reactive, executing a predefined activity based on the set schedule. Follows, static and pre-configured task. Performs simple and repetitive tasks. Security and access are defined through the group. Risk is minimal since the actions are preconfigured. 	 Autonomous and proactive, able to plan and execute complex workflows, without human Interventions. Use Large Action models(LAMs) and generative AI to reason, learn and adapt to the situations. Performs End-to-end process with complex task and dynamically resolve the cases. Introduced for Workflows and auditability for transparency. Requires care management to mitigate risk like inaccuracy and Unpredictability.

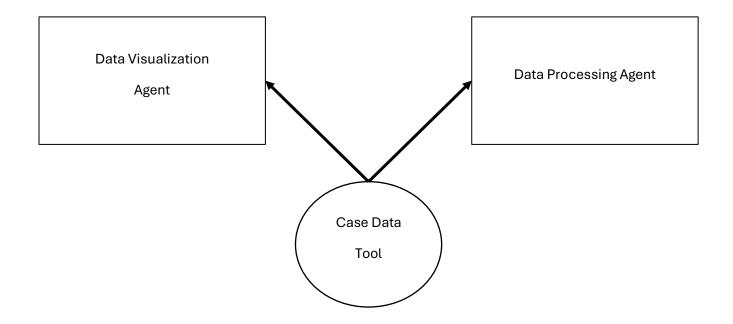
Tasks that can be Performed by the Al Agent:



Tool:

Agent rule and Tool rule are Interrelated. If we consider agent rule as frontend then tool rule is the Back end that does the work. We define what action should be done in the Tool rule and then How and When these rules should be executed is defined in the agent rule and how that task is also done is being defined in the Agent rule.

Why Pege introduced 2 different rules instead of introducing only one rule? The answer is simple for reusability since we can use the Tool rule only in the Agent rule. Where we can use One tool rule in different Agent and according to the System rules that are defined in the Agents, we can see different behaviors when different agents execute. Since We can use different Al for Different Agents.



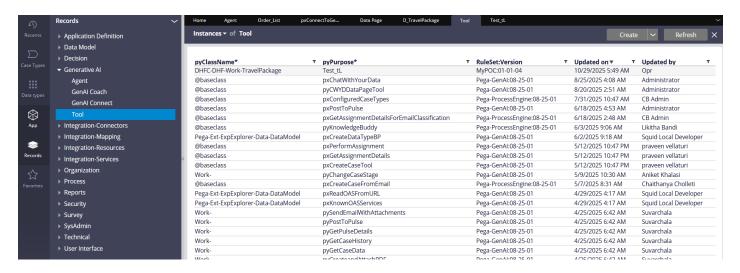
POC On Ai Agents

Use Case:

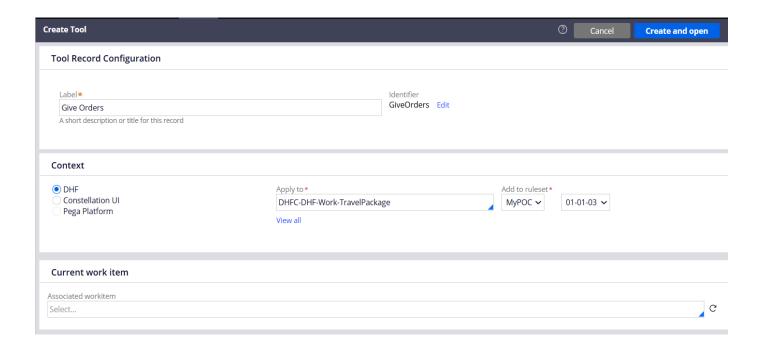
The business wants to fetch the highest ordered Product category from the data type using Al Agent. Where the task is, we are going tell Al agent that gives me the Highest ordered product Category in the Db and give an output.

Steps:

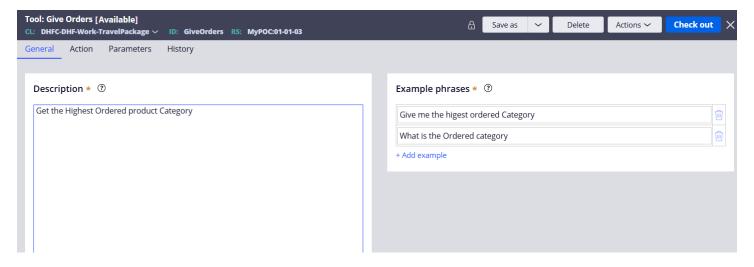
1. First We are going to Create a Tool for giving the data to Al for Processing. Go to Records>Generative Al>Tool.



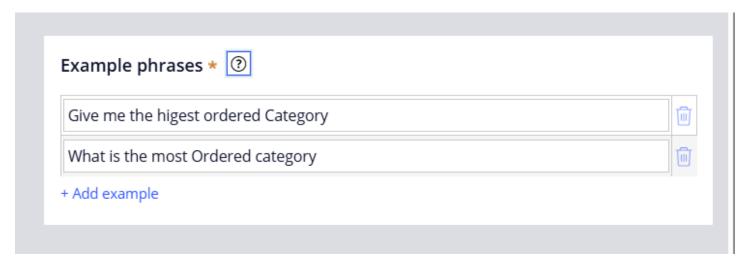
2. Creating a rule named "Give Orders" in the version 01-01-03.



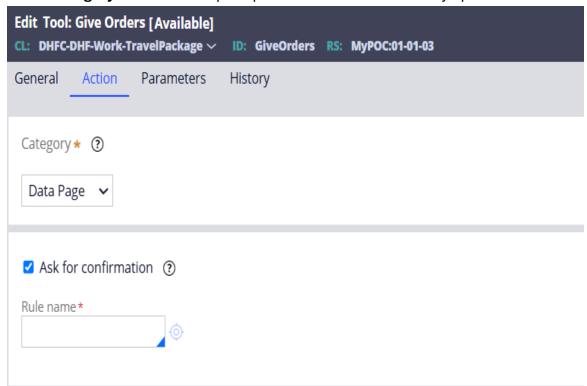
3. In the General Tab where we are going to give instructions and Description of the task that tool is going to perform and give the output for User information.

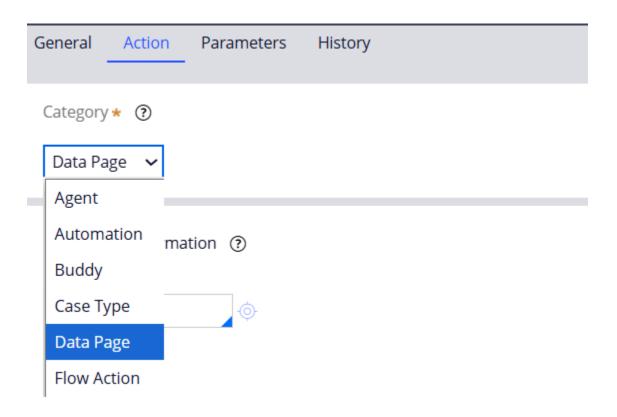


4. There is Example Phrases that we going to give to the user most options to express this tool by user. We have given it 2 different pharases.



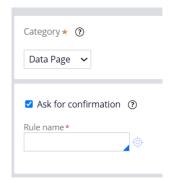
5. Next, in the Action tab where we are going to configure the task that this Tool. In the **Category** We have multiple Options where there are many options:



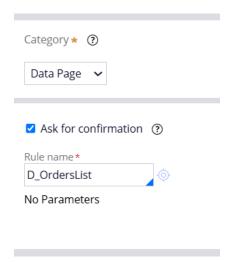


Agent	Calling another Agent.
Automation	Perform an Automated action.
Buddy	Integrating the Knowledge Buddy with the
	Agent using the Tool.
Case type	Select the Case type that an Agent can pick
	and create a case automatically.
Data Page	You can use Data Pages to retrieve lists of
	items, such as a list of transactions, a list
	of followers of a given Case, and so on.
Flow Action	To run a User Action.

There is a check box named "Ask for confirmation" this is used whether we need a confirmation before performing the task or not. We are checking this checkbox.



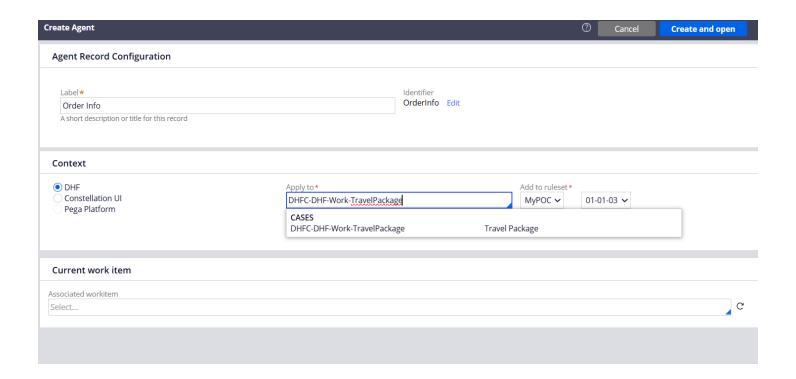
6. Now in the Rule Name We are going to provide Data page of D_orderlist and Saving the rule.



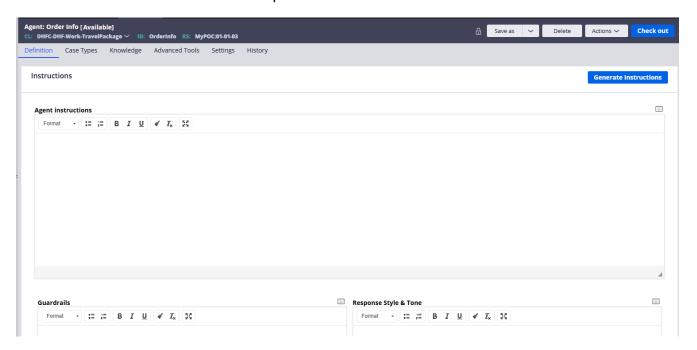
 After the creation of tool rule and we are going to create an agent rule. Go to the Records>Generative Al>Agents.

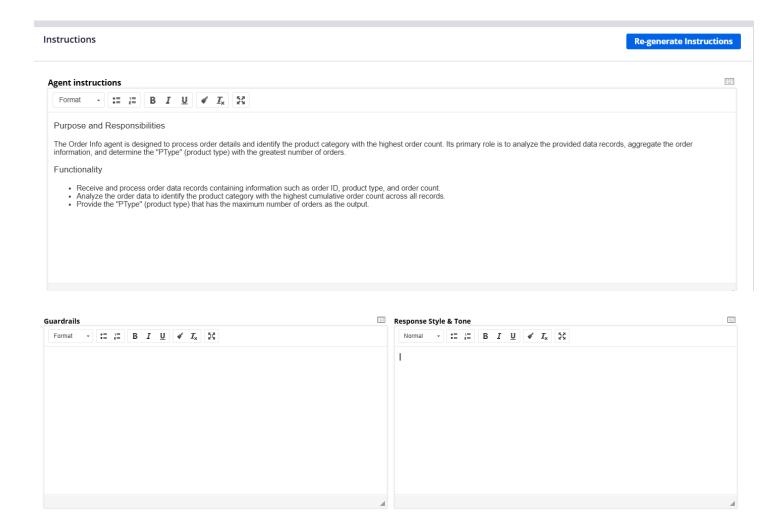


8. Created an Agent rule named as "Order Info" in the same class as Case type that we are going to refer.



9. There are Three different Prompt areas in the first tab.





The three text areas are having different purposes where:

Agent Instructions:

We are going to provide a detailed description of what this agent is supposed to work on and what needs to be given output.

In the top we have button "Generate Instructions" when clicked the instructions are generated automatically according to the Tool that is being provided as input in Agent.

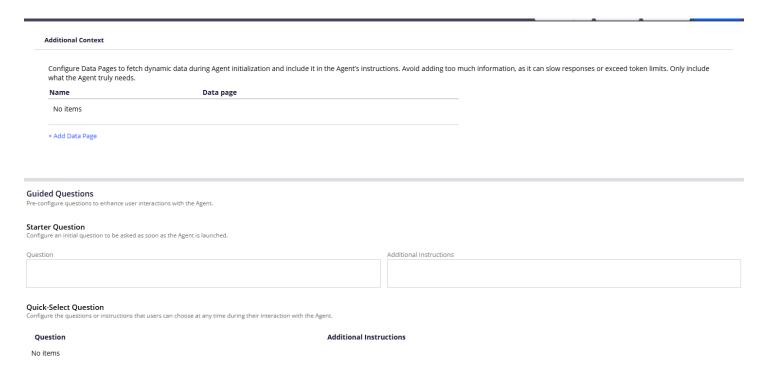
Guardrails:

Providing the Strict info to Ai for the Security purpose where it should not provide inappropriate answers and an output that is not expected.

Response Style & Tone:

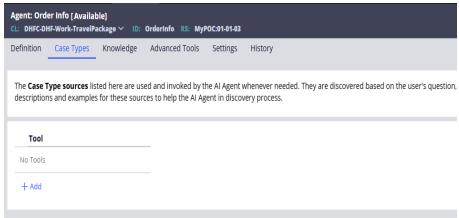
This area is where the output should be presented and the tone and format of the response of AI.

10. If we go further down, we will be able to see some more options where we have quickly selected a question we can define and its instructions.

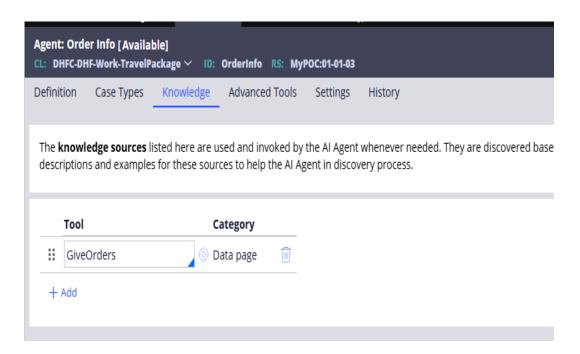


We even have an option where we have an additional context exactly; we can provide data pages as an input for providing Agent Instructions dynamically.

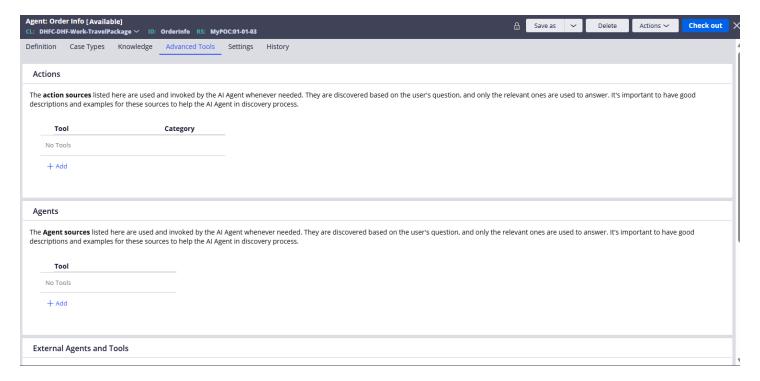
11. We have Different tabs for different purposes in this rule if we go to Case type tab. Where we are going to provide a Tool which is going create a case for us.



12. Next Knowledge tab where we are going provide the data as an input for the Agent to process and give an output. In this one we are going to provide our created Tool.



13. In Advanced Tools, we have options that are being used for specific purposes.



Actions:

All the tools for the automation are being referred to under this tab and being used.

Agents:

Call for another agent.

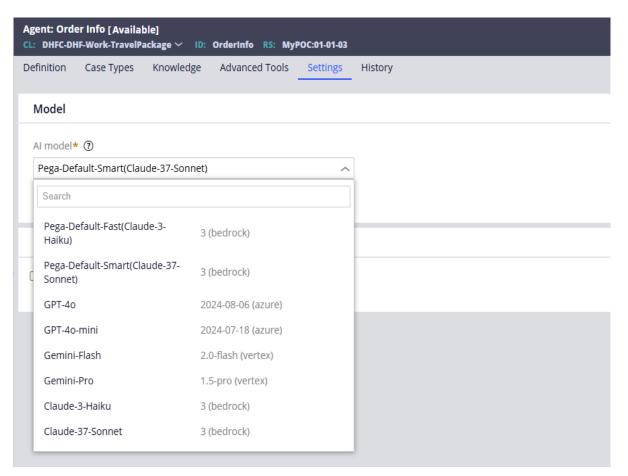
External Agents and Tools:

Call an external agent

Model Context protocol(MCP):

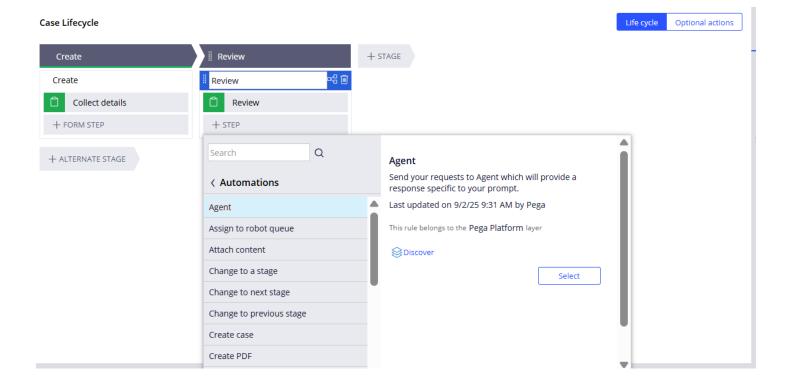
Calling an MCP Connect rule through tool rule.

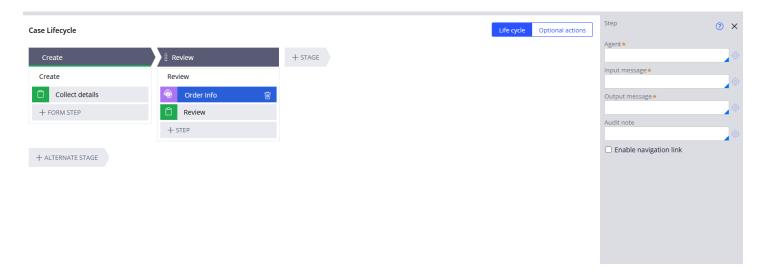
14. In the Settings tab, we can get an option to specific Al Model. Now we are selecting pega default Al.



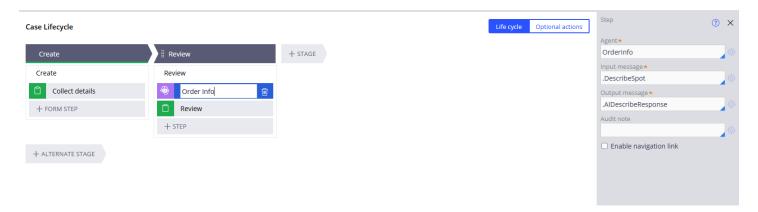
15. Now we go the Case type and then in the Review stage and then Add our Gen Al Agent Step which is under automation.



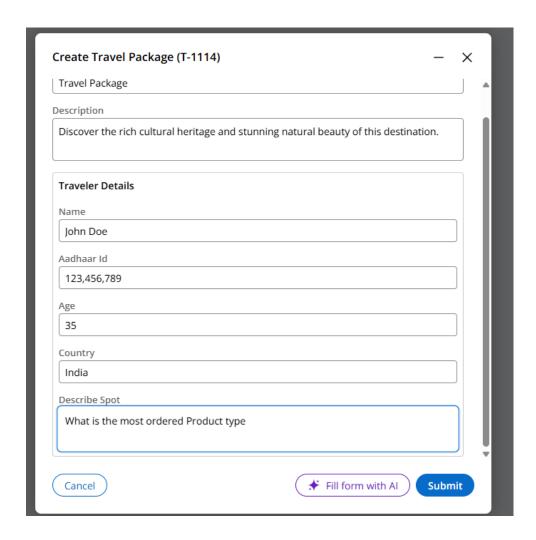




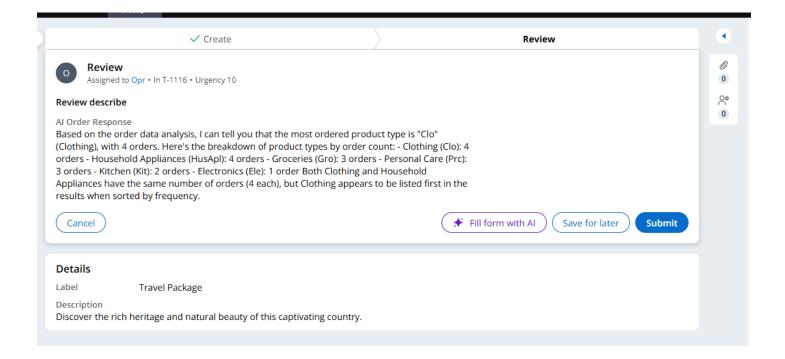
16. Provide the Agent name and input and Output of the property where the prompt is going the map.



17. Now saving the case type and running the case and provided the required details and giving the prompt in the DescribeSpot field.



18. The Output is going to be mapped to the **Al Order Response** and we can see the output of the Ai Agent and it performed the action for us.



Note:

If you want to trace the rules, we can enable the Gen AI in tracer settings.

