**LAB-**03 **Give your public website chatbot a brain and make it an agent**

**Create an intelligent agent that delivers contextual, multi-part answers using your content and real-time data.**

# Lab Details

|  |  |  |  |
| --- | --- | --- | --- |
| Level | Persona | Purpose | Estimated time to complete |
| 100 | Basic Maker | After completing this lab, attendees will be able to create and deploy an intelligent agent capable of answering complex, multi-part questions by combining information from their public website and uploaded files, using a tone and behavior that reflect their organization’s brand. | 15 minutes |

## Prerequisites

You need to be able to create a custom agent in Copilot Studio<https://copilotstudio.microsoft.com/>.

To publish your agent to your website or to a demo website, the following [data loss prevention policies](https://learn.microsoft.com/en-us/microsoft-copilot-studio/admin-data-loss-prevention) should NOT be blocked on your environment:

* Chat without Microsoft Entra ID authentication in Copilot Studio,
* Direct Line channels in Copilot Studio,
* Knowledge source with public websites and data in Copilot Studio.

## Summary of targets

Use the conversational agent creation experience to build an intelligent assistant capable of answering complex, multi-part questions. You’ll add a public knowledge source like Wikipedia, connect a tool (e.g., weather), and see how generative orchestration enables the agent to combine knowledge and actions in a single, contextual response.

| Use case/topic | Tagline | Page |
| --- | --- | --- |
| Create a new agent and add knowledge [Conversational creation experience with knowledge sources] | From idea to insight – Use the conversational experience to create an intelligent agent and enrich it with knowledge from websites like Wikipedia and your own files. | 5 |
| Disable AI knowledge [reduce risks of hallucinations] | Your agent isn’t ChatGPT – Scope and ground AI-generated answers on your data. | 8 |
| Add connectors [Add actions like weather lookup] | Make your agent act, not just answer – Add actions like weather to give your agent real-time capabilities. | 11 |
| Turn on the generative mode [Enable the full power of generative AI to orchestration your agent] | Make your agent act, not just answer – Add actions like weather to give your agent real-time capabilities. | 13 |
| Summary of learnings | Mastery is not a destination but a journey—a joyful path where every step brings growth, discovery, and endless possibilities. | 17 |
| Glossary | Speak the language, bridge the world—unlock hearts, opportunities, and the true essence of every land. | 18 |

## Documentation and additional training links

* [QuickStart: Create and deploy an agent](https://learn.microsoft.com/en-us/microsoft-copilot-studio/fundamentals-get-started?tabs=web)
* [Add a public website as a knowledge source](https://learn.microsoft.com/en-us/microsoft-copilot-studio/knowledge-add-public-website)
* [Orchestrate agent behavior with generative AI](https://learn.microsoft.com/en-us/microsoft-copilot-studio/advanced-generative-actions)

# Use Case #1: Create a new agent and add knowledge

*From idea to insight – Use the conversational creation experience to build Nova AI, an intelligent agent capable of answering complex, multi-part questions grounded in your content and public sources like Wikipedia.*

|  |  |  |
| --- | --- | --- |
| Use case | Value added | Estimated effort |
| Create a new agent and add knowledge | Quickly build a reasoning-capable agent and ground it in relevant data using a natural, no-code setup process. | 5 minutes |

## Summary of tasks

In this section, you’ll use the conversational creation flow to define Nova AI, configure its tone and instructions, and connect it to websites and files to ground its answers in trusted data.

**Scenario**: Build the foundation of Nova AI, your intelligent agent designed to handle complex, contextual queries by drawing from reliable, grounded content.

## Step-by-step instructions

1. Start from your **solution**
2. Select **New** and choose **Agent**
3. In the **Describe your agent** **to create it** input box, set:

|  |
| --- |
| An intelligent assistant that can answer multi-part questions by combining historical facts, biographical data, and real-time information like weather. Ideal for deep research, exploration, and knowledge synthesis. |

This will trigger the **conversational experience** to create a new agent.  
When asked about a **name** for your agent, set:

|  |
| --- |
| Let’s call it Nova AI |

**The conversational experience will try to help you create the best agent descriptions and instructions. It is OK if the questions are not asked in the below order.**

When asked about what the agent should **do**, set:

|  |
| --- |
| Nova AI should answer complex, multi-step questions by combining data from public sources, performing real-time lookups like weather or conversions, and presenting clear, concise responses. |

When asked about what the agent should **avoid**, set:

|  |
| --- |
| Nova AI should not speculate, provide information from unreliable sources, compare competitors, or answer personal, sensitive, or confidential questions. |

When asked about how the agent should **interact with users**, set:

|  |
| --- |
| Nova AI should interact in a friendly and professional manner, using clear language, helpful tone, and light emojis 😊 when appropriate. It should feel approachable, smart, and a bit curious—like a knowledgeable companion. |

When asked about **public website knowledge sources**, set:

|  |
| --- |
| Add https://en.wikipedia.org/ as a public data source for general knowledge and factual information. |

💡 **PRO TIPS:**

* Confirm website ownership for better search results. Doing so allows Copilot Studio to access additional information from your webpages, enhancing the quality of responses.
* URLs can have up to two levels of depth—subpaths indicated by a forward slash /.
* Copilot Studio doesn’t index your website content, instead, it’s using the Bing index, so results will only be as good as the quality of your indexing by Bing.   
  You can learn more about this with [Microsoft Bing Webmaster Tools](https://www.bing.com/webmasters/about).
* When using a public website as a knowledge source, [query data for the Bing Search is stored and processed in the United States](https://learn.microsoft.com/en-us/power-platform/admin/geographical-availability-copilot?tabs=new#regions-where-data-is-processed-for-copilots-and-generative-ai-features).
* Copilot Studio allows you to add up to four public website URLs for knowledge search at a time. If your use case requires more sources, consider setting up a [Bing Custom Search](https://learn.microsoft.com/en-us/microsoft-copilot-studio/nlu-generative-answers-bing) configuration, which enables broader access to relevant information while maintaining control over the content your agent references. This approach ensures your AI assistant remains well-informed without exceeding platform limitations.

1. **If you didn’t start from your solution, you have a second chance:   
   Before creating the agent:** Select the ***…*** menu, go to **Advanced Settings**, and choose the **Solution** you have created. This allows for easy export and deployment to other environments. Ensure your **Schema Name** is unique to avoid creation errors.
2. Select **Create**

## Test your understanding

Now that you’ve created Nova AI and connected it to trusted data sources, take a moment to reflect on what you’ve learned.

**Key takeaways:**

* Conversational agent creation – You can build a reasoning-capable agent using a guided, natural-language setup that defines name, tone, behavior, and capabilities.
* Grounding in knowledge – Adding public websites and files helps Nova AI generate contextual, reliable answers instead of relying on general AI knowledge.
* Instruction-driven behavior – Custom instructions shape the agent’s tone, scope, and interaction style to match your needs.

**Lessons learned & troubleshooting tips:**

* Use a clear, descriptive purpose to guide the conversational setup flow effectively.
* Wikipedia is a great starting source, but validating your own public website indexing on Bing can significantly improve answer quality.
* Always associate your agent with the right solution during creation for easier ALM and cross-environment deployment.
* If the creation fails, check for duplicate schema names or missing required fields in the advanced settings.

**Challenge: apply this to your own use case**

* What knowledge sources would your agent need to best support your users?
* How would you adjust the tone or behavior to reflect your brand or scenario (e.g., internal support vs public info)?
* Could you replace static FAQ pages with a dynamic, grounded agent experience?

Take it further: Try creating a second version of Nova AI with a different tone or alternative knowledge sources. Compare how the answers differ, and evaluate which approach fits your audience best.

|  |
| --- |
|  |
|  |
|  |
|  |

# Use Case #3: Disable AI knowledge

*Your agent isn’t ChatGPT – Scope and ground AI-generated answers on your data.*

|  |  |  |
| --- | --- | --- |
| Use case | Value added | Estimated effort |
| Disable AI knowledge | Learn when to leverage or disable the built-in knowledge of Large Language Models (LLMs), reducing risks of hallucinations and ensuring your agent provides reliable, accurate responses. | 5 minutes |

## Summary of tasks

In this section, you’ll learn how to improve the accuracy and reliability of your agent by disabling its ability to rely on general AI knowledge. While allowing the AI to use its own training data can sometimes be helpful, it also increases the risk of hallucinations, outdated information, responses that may not align with your business objectives (such as suggesting a car model from another car dealer) and can contribute to customers getting inconsistent responses.

**Scenario**: To ensure your Copilot Studio AI Assistant provides fact-based, up-to-date, and controlled responses, you will disable the "Allow the AI to use its own general knowledge" setting. This prevents the AI from generating answers based on outdated or non-curated information, ensuring it only pulls responses from approved sources such as your uploaded documents and specified websites.

By taking this step, you reduce the risk of misinformation, prevent responses based on obsolete AI training data, and maintain trust in the assistant’s answers.

## Step-by-step instructions

1. Navigate to the Copilot Studio **agent** you created in the first use case.

[aka.ms/MCSStart](https://aka.ms/MCSStart)

1. **Ask** your agent a question that is not grounded in its existing knowledge sources (e.g., something outside the scope of its uploaded documents or added websites).

**Observe the response**: Notice how the assistant still attempts to generate an answer. This indicates that the agent is pulling from general AI knowledge, which may lead to hallucinations, outdated information, or unreliable answers.

|  |
| --- |
| Create a Haiku describing Copilot Studio |

A screenshot of a phone

AI-generated content may be incorrect.

1. From the **overview** tab, **disable** the **Allow the AI to use its own general knowledge** setting.
2. **Wait** a minute, **refresh** the test pane, and **test** your agent again

A screenshot of a chat

AI-generated content may be incorrect.

💡 **PRO TIPS:**

* Understanding General AI Knowledge: The "Allow the AI to use its own general knowledge" setting on the Overview page enables your agent to use generative AI for responses. This includes the foundational knowledge the AI was trained on, which may be outdated or inaccurate for certain topics.
* Debugging Responses: When your agent doesn’t find an answer from its configured knowledge sources, you can check Debug Insights to see why (e.g., "No information was found that could help answer this"). These insights are only visible to makers and do not appear to end users.

## Test your understanding

Now that you’ve disabled general AI knowledge for your Copilot Studio AI Assistant, take a moment to reflect on how this impacts your agent’s accuracy and reliability.

**Key takeaways:**

* Scoped Responses – Your agent now relies only on approved knowledge sources, preventing hallucinations and outdated information.
* Trust & Consistency – Disabling general AI knowledge ensures control over the assistant’s responses, making them more predictable and aligned with your business needs.
* Debugging Tools – Debug Insights help troubleshoot why an agent isn’t returning answers, giving makers more visibility into knowledge gaps.

**Lessons Learned & troubleshooting tips:**

* If disabling AI knowledge results in too many unanswered queries, consider enriching your knowledge sources with relevant documents and websites.
* When testing responses, always refresh the test pane after making changes to ensure the latest settings are applied.
* If responses are still appearing overly generic, double-check that the AI knowledge setting is properly disabled in the Overview tab.

**Challenge: apply this to your own use case**

* What types of information should always be grounded in approved sources rather than general AI knowledge?
* How would enabling or disabling AI knowledge impact your organization’s chatbot strategy?
* When might it be beneficial to partially enable AI knowledge for broader responses?

Take it further: Test your assistant on a series of domain-specific questions before and after disabling AI knowledge. How does its accuracy and consistency improve?

|  |
| --- |
|  |
|  |
|  |
|  |

# Use Case #4: Add connectors

*Make your agent act, not just answer – Extend Nova AI’s capabilities by adding connectors that let it perform real-time actions like checking the weather or creating or update records.*

|  |  |  |
| --- | --- | --- |
| Use case | Value added | Estimated effort |
| Add connectors | Enable your agent to go beyond answering questions by connecting it to actions that enhance replies. | 5 minutes |

## Summary of tasks

In this section, you’ll add a connector to your agent—for example, a weather action—so it can retrieve real-time data and deliver richer, more contextual answers.

**Scenario**: Enhance Nova AI by giving it the ability to act on queries that require up-to-date information or calculations, improving the depth and utility of its responses.

## Step-by-step instructions

1. Navigate to the Copilot Studio **agent** you created in the first use case.

[aka.ms/MCSStart](https://aka.ms/MCSStart)

1. Go to the **Tools** tab and choose **Add a tool.**
2. Search for **MSN Weather**, and select **Get current weather** action.
3. Select **Add to agent**
4. Open the **Get current weather** tool.
5. Under **Additional details**, set the **Authentication** to **agent author authentication**.

💡 **PRO TIPS:**

* For connectors that need to run in the context of the end-users (e.g., for actions that apply role-based access, or filters, like “show my Salesforce opportunities), you should leave user authentication.
* Choosing agent author authentication eases the end-user experience as they do not need to create a connection but may create data exfiltration risks. Be sure to review agents with such end user authentication settings for connectors and flows.

1. Under **Inputs**, for Units, choose **Custom value** for **Fill using**, and select Imperial or Metric.
2. **Save**

## Test your understanding

Now that you’ve added a connector to Nova AI, reflect on how this unlocks dynamic, real-time responses beyond static knowledge.

**Key takeaways:**

* Real-time tools – Connectors enable Nova AI to not only retrieve facts but also trigger real-world actions like checking the weather, calling standard or custom APIs, or creating or updating records.
* Authentication models – You can choose between agent author and end-user authentication depending on the scenario and data sensitivity.

**Lessons learned & troubleshooting tips:**

* Use agent author authentication when responses don’t need to be personalized to the user—it simplifies access but must be reviewed for security risks.
* For user-specific data, retain end-user authentication to respect role-based access.
* Ensure the connector is added and configured correctly, especially around required inputs like temperature units or locations.

**Challenge: apply this to your own use case**

* What kinds of real-time data could your agent retrieve to be more useful (e.g., weather, currency, live KPIs, or integration with systems like Dynamics 365, SharePoint Lists, Salesforce, SAP, ServiceNow..)?
* Are there internal systems you’d want your agent to connect to?
* How might dynamic actions improve decision-making for your users??

Take it further: Add another action—such as an agent flow—to let Nova AI perform tasks like creating records or sending approval requests. Test how chaining multiple actions affects the richness of your agent’s responses.?

|  |
| --- |
|  |
|  |
|  |
|  |

# Use Case #5: Test the generative mode

*Intelligence unlocked – Enable generative mode to let your agent reason, synthesize, and act across multiple steps using orchestration.*

|  |  |  |
| --- | --- | --- |
| Use case | Value added | Estimated effort |
| Test the generative mode | Assess the full potential of generative AI to allow your agent to reason across knowledge and actions. | 5 minutes |

## Summary of tasks

In this section, you’ll test generative orchestration for your agent. This allows Nova AI to combine information from different knowledge sources, reason across actions, topics and knowledge, and trigger real-time actions—like retrieving the weather—within a single conversation.

**Scenario**: You want Nova AI to go beyond static answers and dynamically respond to multi-step queries that require both factual lookup and external data (e.g., combining historical facts with a real-time weather report). Enabling generative mode ensures your agent can handle these complex, contextual scenarios by chaining knowledge and actions together.

By using generative orchestration, you unlock the agent's ability to understand intent, process intermediate steps, and deliver rich, synthesized answers—making it smarter, more responsive, and more useful..

## Step-by-step instructions

1. Navigate to the Copilot Studio **agent** you created in the first use case.

[aka.ms/MCSStart](https://aka.ms/MCSStart)

1. **Test** your agent with this question

|  |
| --- |
| Which Apollo mission returned the first lunar samples? Who was the command module pilot for that mission? What's the weather in the city where that NASA pilot was born? |

1. **Notice** how the generative orchestration does **one or multiple searches** to get an answer, and then triggers the **weather connector**.

## Test your understanding

Now that you’ve enabled generative mode in your Nova AI agent, reflect on how orchestration enhances your agent’s reasoning and responsiveness.

**Key takeaways:**

* Multi-step reasoning – Generative orchestration allows your agent to break down complex queries and resolve them step by step across knowledge and actions.
* Knowledge + action chaining – Your agent can now blend facts from sources like Wikipedia with live data (e.g., weather) to deliver complete, contextual answers.
* AI that adapts – With generative mode, Nova AI better understands intent, even when user prompts are ambiguous or layered.

**Challenge: apply this to your own use case**

* What types of questions or tasks in your domain could benefit from chained reasoning and real-time action?
* How could orchestration improve user experience compared to rigid, pre-scripted dialogs?
* Are there limits or safeguards you would consider adding when your agent starts acting on external systems?

Take it further: Try rephrasing the test question in a more natural or vague way. Does the agent still respond correctly? Experiment with other multi-hop queries to see how well your agent chains reasoning steps together.

|  |
| --- |
|  |
|  |
|  |
|  |

# Summary of learnings

Une image contenant jaune, conception

Le contenu généré par l’IA peut être incorrect. *Mastery is not a destination but a journey—a joyful path where every step brings growth, discovery, and endless possibilities.*

Congratulations on completing this lab! You’ve learned how to create and configure a generative AI assistant capable of answering complex, multi-step questions by orchestrating knowledge and real-time actions.

* **Create structured foundations** – Organize your work using solutions for better lifecycle management and deployment readiness.
* **Design intelligent agents** – Build Nova AI using the conversational creation experience, defining tone, behavior, and purpose.
* **Ground responses in data** – Add public websites and files as knowledge sources to ensure factual, relevant, and contextual answers.
* **Ensure reliability** – Disable general AI knowledge to reduce hallucinations and keep answers aligned with your trusted sources.
* **Enable action and orchestration** – Add connectors and turn on generative mode to support multi-hop queries that combine data retrieval with real-time plugin execution.
* **Optimize accessibility** – Configure authentication settings to match your audience and ensure a seamless user experience across public and internal channels.

**Conclusions and recommendations**

To maximize the effectiveness of your AI agent:

* **Keep knowledge fresh** – Regularly review and update knowledge sources for accuracy and completeness.
* **Monitor interactions** – Analyze user queries to uncover gaps, refine instructions, and improve response quality.
* **Align security with experience** – Match authentication settings to your intended audience while adhering to your organization’s security and compliance requirements.
* **Test early and often** – Use the demo website to validate behavior, tone, and accuracy before deploying publicly.
* **Be intentional with orchestration** – Use clear instructions and connectors to shape how your agent processes multi-part queries, ensuring it delivers value and relevance.

By following these practices, you’ll be well on your way to building intelligent agents that are not only useful but also delightful, trusted, and aligned with your organization’s goals.

**We want your feedback!**

[**Start now**](https://aka.ms/MCSLabsFeedback)

# Glossary

*Speak the language, bridge the world—unlock hearts, opportunities, and the true essence of every land.*

**Agent:**  
A digital assistant powered by AI, capable of understanding and responding to user inputs. In Copilot Studio, agents can be customized to for conversational experiences and/or can act autonomously based on pre-configured triggers and instructions.

**Channel:**  
A communication medium or platform through which users interact with an agent, such as a website, telephony, WhatsApp, Facebook messenger, Microsoft Teams, Slack, etc. While Copilot Studio can be seen as the engine or back-end, the channels effectively relay the activities between the agent and the end-user interacting through a client – or front-end. Each channel and client may each have their own specificities and limitations.

**Generative Answers / AI:**  
Responses created dynamically by AI based on user inputs and available knowledge sources. These answers are not pre-programmed but are generated in real-time using large language models and generative AI.

**Instructions:**  
Custom settings or guidelines configured in Copilot Studio to shape the behavior of Copilot agents. Instructions define how the agent should respond to specific queries or scenarios.