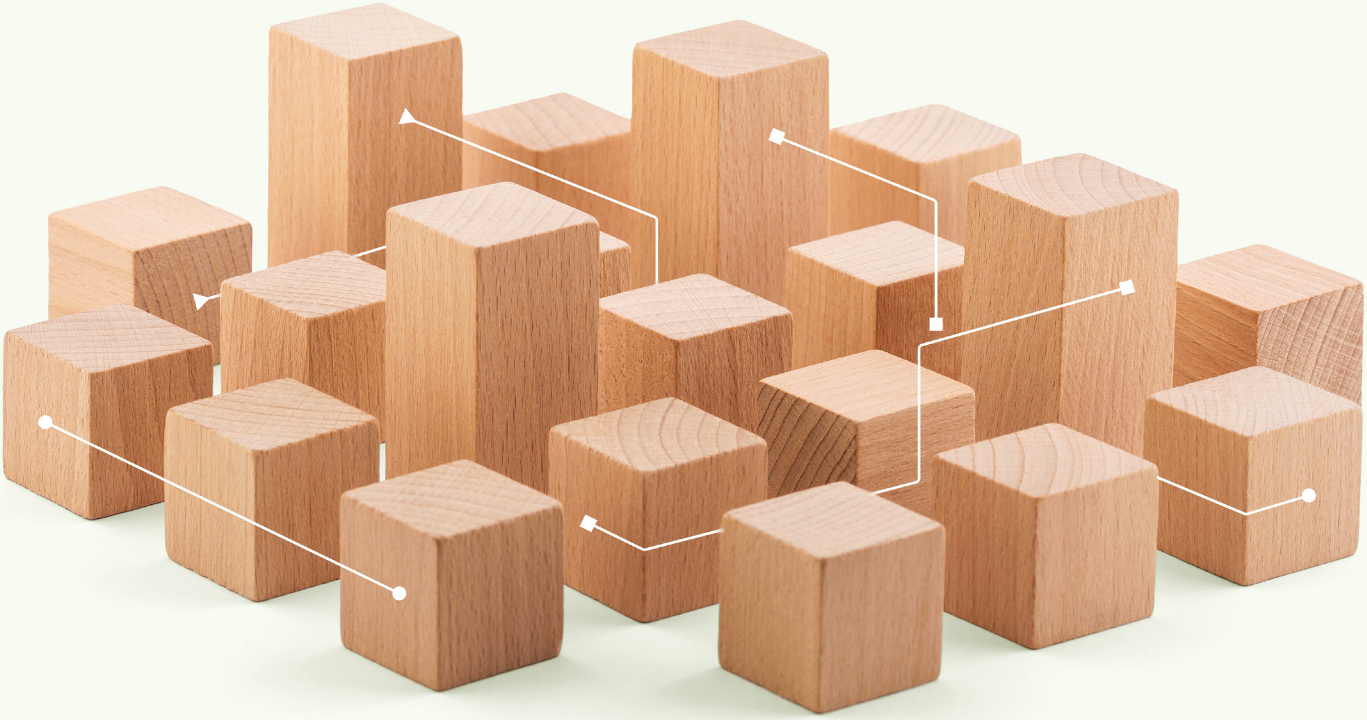
Transitioning Your Data Team to AI Agent Readiness: A Practical Guide with KNIME

Your data team already has what it takes to build AI agents with KNIME



Generative AI has captured plenty of attention but much of it has been focused on surface-level capabilities: chatbot demos, content generation tools, and productivity hacks. While these examples are interesting, they often fall short when it comes to delivering lasting value inside an organization.

A more practical and impactful approach lies in agentic AI — AI systems that don't just respond, but act. AI agents can make decisions, call tools, work across systems, and automate tasks that would otherwise require manual effort. They go beyond conversation and into execution.

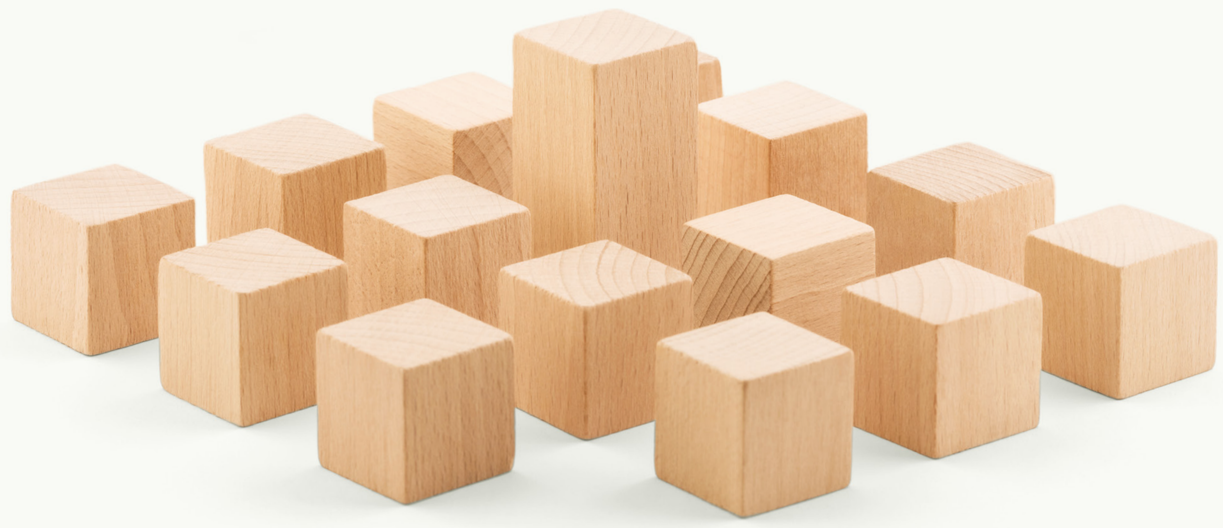
Moreover, organizations have put significant effort into determining how best to use the large amounts of structured and unstructured data they've accumulated. Companies have established data practices and trained employees in data science, but these measures have barely uncovered the potential of the troves of proprietary data stored within each organization.

This guide shows you how agents created with KNIME can combine the expertise of data specialists with the domain knowledge of subject matter experts, allowing organizations to build agentic data workers that provide information or execute tasks according to organizational needs.

The best part is organizations already possess much of what's needed to develop AI agents. Centralized data teams — analytics, data science, or business intelligence — have long been building the infrastructure, expertise, and data assets necessary to enable agentic solutions. Rather than creating entirely new departments or starting from scratch, businesses can use existing analytics tools, pipelines, and the extensive expertise their data specialists already hold.

For instance, with KNIME, your organization can integrate your existing analytics workflows, turning them into a repository of tools accessible to AI agents. Starting with the resources and talent you already have, this guide will show you how to incrementally build and maintain these agentic data workers transparently, efficiently, and practically using KNIME.

Contents



Introduction to Agentic AI

What Are AI Agents?

An AI agent is a system that can reason, decide, and act. Unlike large language models (LLMs), which simply return a response to a prompt, agents can take that response and do something with it — like fetch data, make a decision, call an API, or generate a report.

Agents are typically made up of a few key components:

TOOLS

Tools handle specific tasks like data aggregation and event prediction. While these functions have been automated for years, agentic systems require different design approaches.

INTELLIGENT TOOLS

An intelligent tool extends the functionality of a tool by incorporating a large language model (LLM). This allows it to understand context and perform tasks that involve language comprehension or generation. For example, an intelligent tool might summarize a document, or it could summarize the document and then use the summary to compose and send an email.

AI WORKFLOWS

AI workflows connect multiple tools to accomplish more complex tasks.

AI workflows orchestrate multiple components — including LLM models, APIs, and logic — to solve complex, multi-step tasks that go beyond what a single model or tool can handle alone. These AI workflows can be dynamically assembled by an agent.

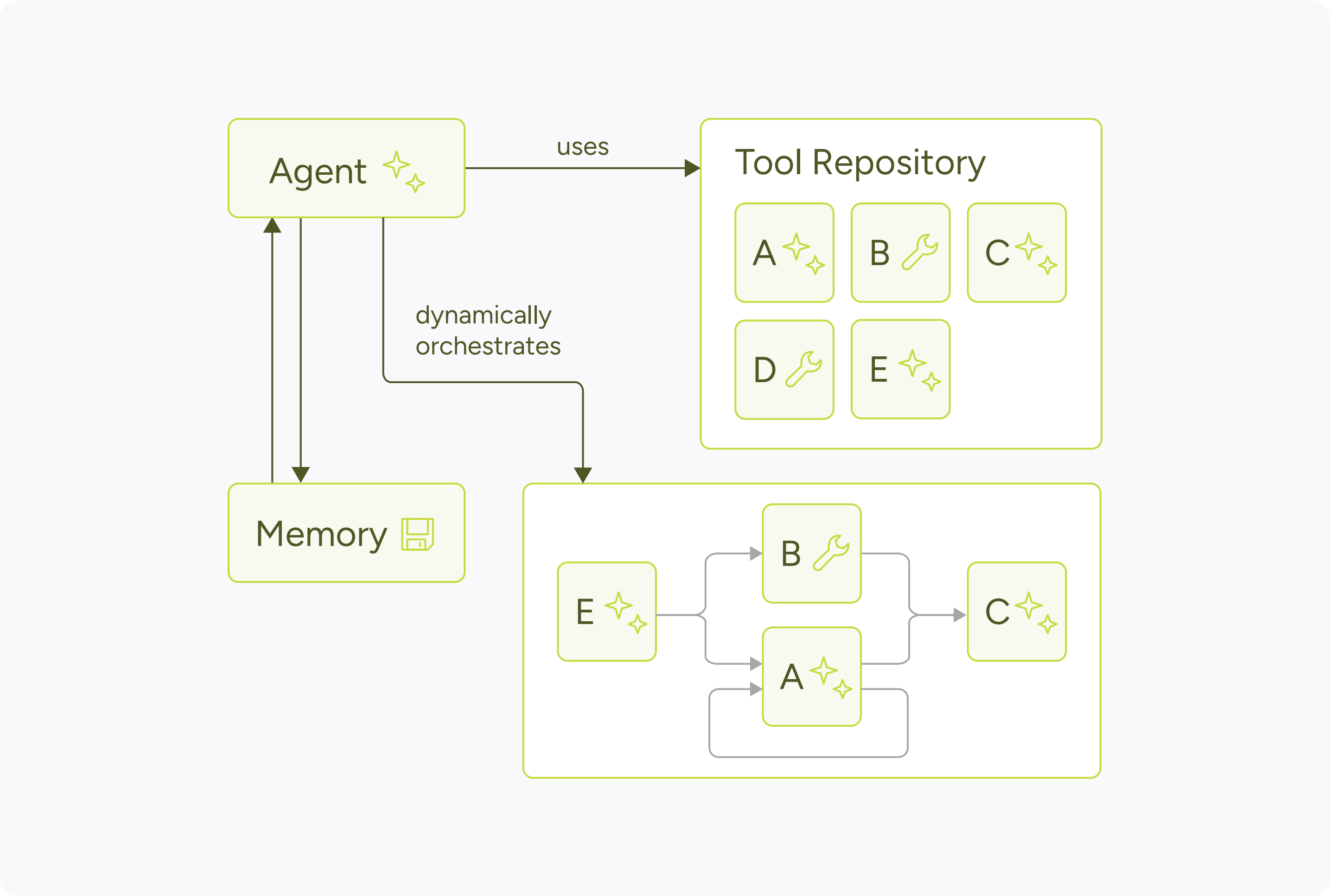
AI workflows can themselves often become tools used by other AI workflows within larger systems.

AGENTS

An agent has access to a diverse set of tools and orchestrates their use for each specific request.

MEMORY

An agent has access to all prior actions it has completed and feedback on those actions so it can adapt behavior or follow patterns based on prior experience. This helps refine the quality of agent decision-making and actions.



How this works behind the scenes varies widely. Some agents use AI to map out the entire approach first, planning exactly which tools to use and in what order. Others take a more step-by-step approach, using one tool at a time until they've gathered enough information to provide a good response.

Agents come in two main varieties:

- Agentic applications that interact directly with people
- Agentic services that run in the background, available as tools for other workflows or agents

What makes this approach powerful is how it can grow and evolve. New tools, which might themselves be AI workflows or other agents, can be continuously added to the collection. Sometimes human designers add these new tools, but agents can also develop and add tools themselves, expanding their own capabilities or those of other agents.

As the tool collection becomes more sophisticated, agents can handle increasingly complex tasks. This creates a natural progression toward more advanced behavior. The whole is greater than the sum of its parts. Individual parts that aren't too complicated on their own combine to create something remarkably powerful.

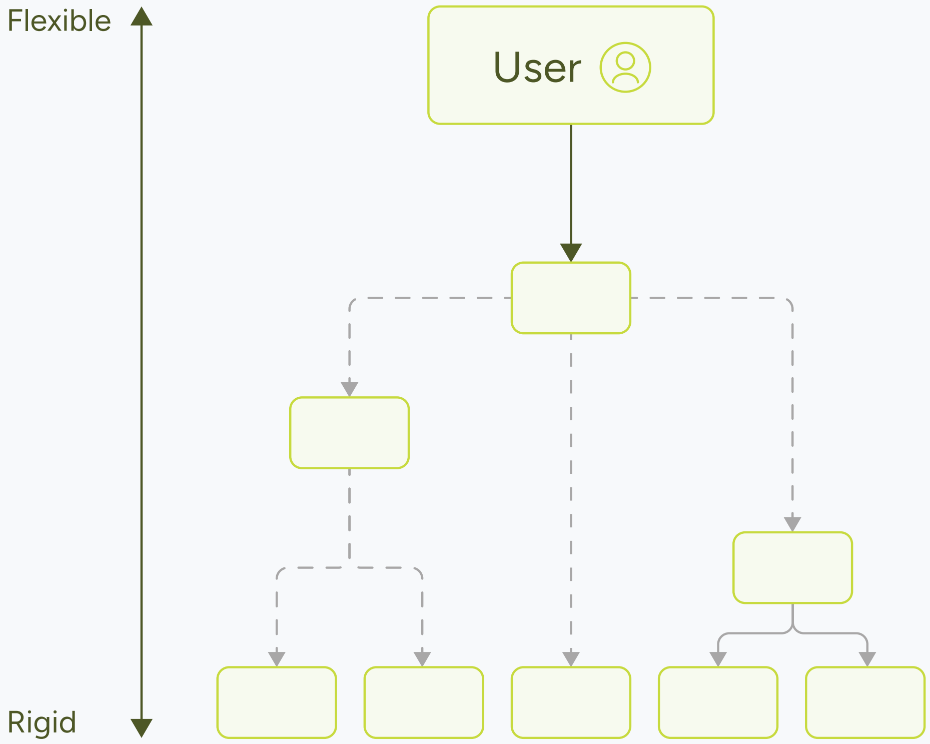
Levels of Agent Autonomy

Agent autonomy can range from general to specific. Higher-level general agents can perform tasks by delegating to more specialized subagents and integrating their results to accomplish increasingly complex goals.

For example:

> **Activity Recommendation Agent (general):** Provides activity suggestions based on user preferences and contextual conditions.
>
> - **Weather Subagent (specific):** Provides weather forecasts.
> - **Hiking Trail Subagent (specific):** Identifies hiking trails in a specified location.
> - **Cinema Subagent (specific):** Lists movies currently playing at cinemas.

If a user asks, "What can I do tomorrow?", the Activity Recommendation Agent would first check the Weather Subagent. If the weather forecast is favorable, it would delegate to the Hiking Trail Subagent to suggest outdoor activities. If the weather is unfavorable, it would instead delegate to the Cinema Subagent to recommend movies.



Why Agentic Systems Are Now Becoming Essential for Businesses

Language models have demonstrated their ability to generate text, but businesses need solutions that drive decisions and actions. Agentic systems with their ability to reason independently and take action bridge this gap.

Several business challenges make these systems particularly valuable now:

- **Underutilized data:** Despite investments in data infrastructure, organizations struggle to extract value from their vast structured and unstructured data. Agentic systems can act as data workers that continuously analyze this data and surface relevant insights.
- **Decision latency:** In fast-paced markets, manual approval processes and delays in data analysis can create bottlenecks that hinder timely decision-making and reduce business agility.
- **Operational and data fragmentation:** Large enterprises often face challenges due to disconnected systems and teams working with siloed data, leading to inefficiencies and limited collaboration.
- **Resource constraints:** Companies face pressure to increase productivity without expanding headcount. Agentic systems can handle routine analytical and decision-making tasks that would otherwise require additional staff.
- **Regulatory complexity:** Compliance requirements continue to grow more demanding. Agentic systems can consistently apply rules across operations, reducing human error and compliance risk.
- **Rising customer expectations:** Customers demand faster, more personalized service. Agentic systems can provide immediate responses based on comprehensive customer data analysis.

The practical benefit of these systems is their ability to work autonomously and enhance human productivity by analyzing situations, evaluating options, and taking appropriate actions while adhering to established parameters.

Organizations that implement agentic systems can deploy them as data workers that actively extract, analyze, and apply insights from organizational data.

These AI agents combine the technical expertise of data scientists with the contextual knowledge of domain experts, allowing organizations to finally make productive use of their accumulated data assets.

Instead of data sitting underutilized in various systems, these agents transform it into actionable intelligence that supports informed decision-making throughout the business.

Why Use KNIME to Build Your AI Agents

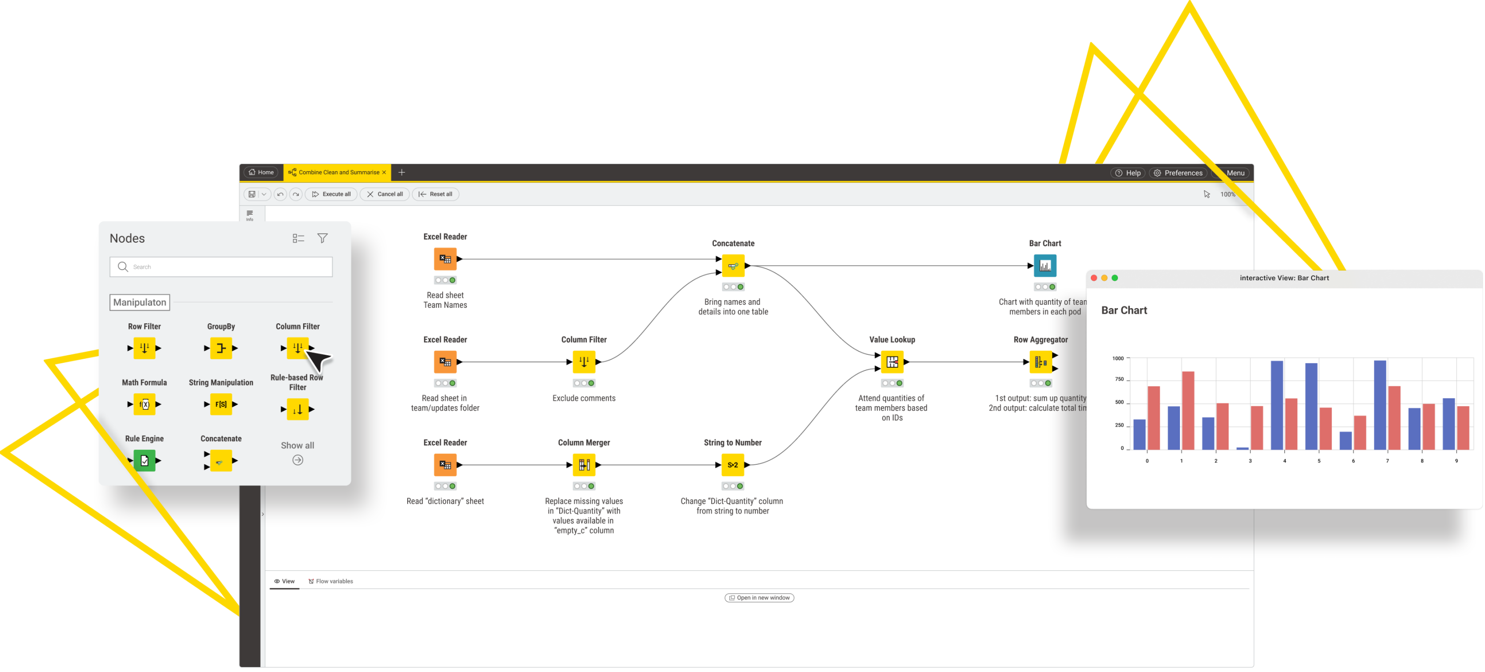
KNIME provides modular building blocks for constructing AI agents in a manageable way. Here's a detailed look at this:

Visual Workflows

KNIME's visual workflows make it accessible to both technical and non-technical users.

KNIME's visual workflows empower both technical and non-technical users by replacing traditional code with a drag-and-drop interface. Each step in the process is represented by a connected node, making it easier to track data flow, identify issues, and explain logic clearly.

Workflows are fully traceable and reproducible, ensuring transparency, reliability, and easy auditing.



Visual workflows function as tools that enable agents to access information and execute tasks. These workflows can be enhanced with generative AI (GenAI) capabilities, resulting in intelligent tools. Agents themselves can also be developed using KNIME workflows, allowing them to orchestrate these enhanced tools effectively. For example, a customer churn model or a report generator, can now act as callable tools inside an AI agent's decision flow.

For existing KNIME users, converting their library of workflows into agent-ready tools is straightforward. This enables immediate reuse of existing workflows within agentic workflows.

Broad Data Access

With over 300+ connectors, KNIME connects easily with internal systems, APIs, databases, and modern LLMs. Additionally, KNIME offers native support for REST APIs via nodes like GET Request, POST Request, and JSON Path.

This connectivity enables workflows to access, retrieve, and manipulate data from diverse sources, making KNIME a powerful bridge between AI processing and enterprise data ecosystems.

READER NODES

- Table Reader
- File Reader
- Tika Parser
- Tess4J
- JSON Reader
- Web Log Reader
- List Audio Files
- Image Reader
- Model Reader
- TensorFlow Network Reader
- Triple File Reader
- Webpage Retriever
- RSS Feed Reader
- Keras Network Reader
- TensorFlow 2 Network Reader
- OpenNLP NER Model Reader
- Network Reader
- Viz Input Connector
- SDF Reader
- MDF Reader
- Python Source
- Python Object Reader
- R Source (Table)
- Index Reader
- H2O MOJO Reader
- SAS7BDAT Reader

CONNECTOR NODES

- KNIME REST Client Extension
- SPARQL Endpoint
- Memory Endpoint
- KNIME Twitter Connectors
- SAP Reader (Theobald Software)
- Kafka Connector
- Kafka Consumer
- SMB Connector
- Google Analytics Connector
- Google Sheets Connector
- KNIME Amazon Machine Learning Integration
- KNIME Salesforce Integration
- FTP Connector
- SSH Connector
- HTTP(S) Connector
- Box Connector
- Google Drive Connector
- Amazon S3 Connector
- Google Cloud Storage Connector
- SharePoint Online Connector
- Azure Blob Storage Connector
- HDFS Connector
- HDFS Connector (KNOX)
- Databricks File System Connector
- Neo4j Connection
- OrientDB Connection

LLM CONNECTORS

- OpenAI LLM Connector
- OpenAI Embeddings Connector
- OpenAI Chat Model Connector
- Azure OpenAI LLM Connector
- Azure OpenAI Embeddings Connector
- Azure OpenAI Chat Model Connector
- Databricks Chat Model Connector
- Databricks Embedding Connector
- DeepSeek Chat Model Connector
- GPT4All Embeddings Connector
- HF Hub LLM Connector
- HF Hub Chat Model Connector
- HF Hub Embeddings Connector
- HF TEI Embeddings Connector
- HF TGI Chat Model Connector
- HF TGI LLM Connector
- Local GPT4All Chat Model Connector
- Local GPT4All LLM Connector
- KNIME Hub Chat Model Connector
- KNIME Hub Embeddings Connector

AUTHENTICATION NODES

Google Authenticator
Microsoft Authenticator
Amazon Authenticator
OpenAI Authenticator
Azure OpenAI Authenticator
DeepSeek Authenticator
HF Hub Authenticator

DATABASE CONNECTORS

Connector (generic JDBC)
DB Connector
Oracle Connector
Snowflake Connector
PostgreSQL Connector
H2 Connector
SQLite Connector
Microsoft Access Connector
Microsoft SQL Server Connector
Vertica Connector
Impala Connector
Hive Connector
Google BigQuery Connector
KNIME Amazon DynamoDB Nodes
Amazon Redshift Connector
Amazon Athena Connector
MySQL Connector

KNIME's open source nature makes it highly integrative of the latest and greatest technologies and doesn't lock users into one way of doing things.

If the underlying tech stack changes, you can simply swap out the connector in your visual workflow — no need to rebuild everything. That kind of flexibility makes it a future-proof choice for building agents, particularly in the fast-moving and unpredictable AI landscape.

Well Integrated Data to Give Agents Context

Agents rely on specialized tools to do their jobs. These tools supply information or handle tasks that the primary agent cannot perform on its own.

KNIME Hub acts as a central repository of reusable tools for agents. KNIME workflows can flexibly call and orchestrate these tools as needed, creating autonomous solutions that easily adjust to changing requirements. You can also set up KNIME Business Hub to act as a model context protocol (MCP) server, giving you an easier and scalable way to browse and call tools from your repository.

Bringing Together Tools, AI Workflows, and Agents in a Modular and Transparent Way

Using KNIME's visual workflows, all the components of an agentic system can be built very naturally:

- **Tools:** Creating useful tools, especially ones involving data, is what you can do with KNIME Analytics Platform. KNIME Hub is a great repository for various tools, including intelligent ones powered by new AI features.
- **AI workflows:** You can also use KNIME to orchestrate and make use of a series of tools to solve complex tasks.
- **Agents:** By using AI capabilities, KNIME workflows can also include prompts that help figure out plans or instruct AI to use specific tools.

More Than a Chat Interface

You can also use KNIME workflows to create applications or services that act like agents. Just like regular workflows, agent-based workflows can also be deployed easily through KNIME Hub as data apps, background services, or REST APIs — whatever makes sense for your environment.

Finally a Way to Get The Most out of Your Data

While many organizations have significant stores of data, truly capitalizing on this asset often remains challenging. Agents built using KNIME help you overcome this challenge by combining analytical methods from your data experts with the practical insights of your domain specialists.

KNIME's modular, visual workflows allow both technical and non-technical users to clearly and collaboratively define actionable processes. Your domain experts can visually map out business logic and operational contexts directly into workflows, while your data scientists integrate advanced analytical models seamlessly into these visual structures.

As you build more and more agents using KNIME, you are essentially building agentic data workers that function much like expert data colleagues. These agents can intelligently understand context, access relevant information, and use your organization's data effectively according to your organization's specific needs. They proactively surface insights, make informed recommendations, and finally let you make the most out of your data.

Understanding the Business Value of Custom AI Agents with Practical Use Cases

The value of agents comes from what they enable teams to do, not just what they generate. Used well, they can drive efficiency, consistency, and adaptability across a range of workflows.

- **Efficiency Gains**

  Agents are especially good at taking over routine, time-consuming tasks that don't require deep judgment but still need to get done accurately and quickly. This frees people up to focus on work that actually benefits from human attention.

  According to a LangChain report, the most common uses for agents are research and summarization (58%), followed by support with personal tasks and productivity (53.5%). These figures suggest that many people are looking for ways to offload time-consuming work.

  Efficiency gains extend beyond individual use. About 45.8% of use cases relate to customer service, where agents are used to manage inquiries, assist with troubleshooting, and help teams respond to customers more quickly.

  - Handling incoming customer support requests by auto-tagging, routing to the right team, and suggesting responses based on past tickets and support documentation.
  - Summarizing lengthy documents, such as meeting transcripts or case notes.
  - Pulling data from multiple systems to build routine weekly or monthly reports.
  - Reviewing and flagging documents for missing metadata or inconsistent formatting.
  - Answering frequently asked internal questions (HR policies, tool access, etc.) using a central knowledge base.

- **Scalability & Consistency**

  When the goal is to ensure that work is done the same way, every time and everywhere, agents can help apply rules evenly, reducing discrepancies across teams and locations.

  - Drafting first-pass responses to RFPs using approved language and formatting.
  - Generating onboarding checklists based on role, department, and region.
  - Checking submitted forms or documents for compliance with internal standards.
  - Filling in recurring templates (e.g., performance reviews, customer success plans).
  - Translating standard operating procedures (SOPs) into regional formats or languages, while keeping the structure consistent.

- **Strategic Differentiation**

  Tailored agents can do more than automate. They can reflect how your organization thinks and operates. That alignment can help speed up complex decisions or give teams new tools to compete more effectively.

  - Analyzing competitor announcements and summarizing implications for your business.
  - Generating targeted outreach suggestions based on industry, persona, and deal stage.

- Assisting field teams with localized product data or regulatory requirements during client visits.
- Building internal “briefing books” ahead of key meetings using CRM, news, and project data.
- Synthesizing feedback from multiple channels (support, sales, surveys) into actionable themes.

- **Compliance & Risk Management**

  In settings where accuracy and traceability matter as much as speed, agents can help enforce rules and document decisions. This is especially relevant in finance, healthcare, and other regulated environments.

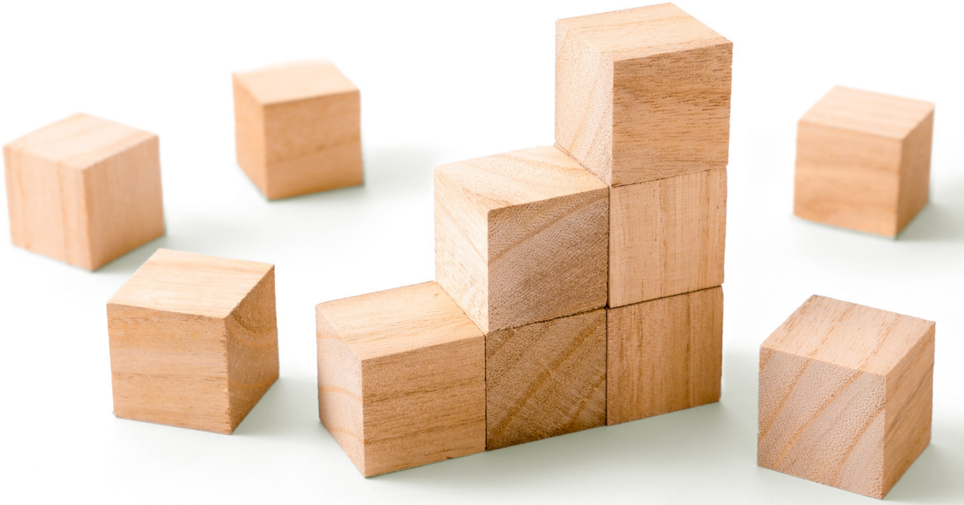
  - Reviewing and annotating contracts to highlight deviations from standard terms.
  - Comparing versions of regulatory filings for discrepancies or missing language.
  - Scrubbing sensitive data (PII, PHI, etc.) from documents before external sharing.
  - Tracking which steps were taken in a compliance-related process and when.
  - Pre-validating report drafts against industry or internal compliance checklists.

- **Augmentation, Not Replacement**

  Agents are often most effective when they act as copilots — boosting the work people already do rather than trying to replace it. They can handle prep work, offer suggestions, or surface relevant context right when it’s needed, helping humans make faster, more informed decisions.

  - Assisting analysts by gathering context and drafting summaries for research or competitive intelligence.
  - Reviewing drafted reports or slide decks for clarity, tone, and internal consistency.
  - Providing live suggestions or references during customer support chats, based on prior cases.
  - Offering context-specific answers to internal questions (e.g., “What’s our procurement process for vendors in Europe?”).
  - Prepping team members for meetings by compiling agendas, prior notes, and recent activity from relevant tools.

Across industries, these gains of using agents are quantifiable: businesses report a 61% increase in employee efficiency, and some (like JPMorgan) have seen productivity boosts of up to 20% using AI copilots for engineering tasks.



How to Build 3 Different Agents of Increasing Complexity in KNIME

You don't need weeks of planning or a specialized engineering team to get started building your first AI agent. In this section, we'll walk through how to build three agents in KNIME, each more capable than the last. You'll start small, learn the mechanics, and scale up from there.

We will **begin** with the tech setup and understanding how KNIME's features map to agentic AI concepts

Next, we'll build some tools and move to a basic agent that analyzes user feedback sentiment and routes the feedback appropriately.

Then we'll expand that agent's capabilities by integrating internal tools with external data-aware tools.

Finally, we will build a full-fledged "ask-me-anything" agent that responds dynamically to diverse user queries directly via a chat interface.

Step 0: Tech stack + KNIME

To begin, you'll need KNIME Analytics Platform installed and access to an LLM API. OpenAI is used in our example, but you can use others. If you have internal tools, APIs, or data repositories, it helps to have connections to those as well.

KNIME's strength here is flexibility, it connects with almost anything, and you're not tied to a specific vendor for your data, model, or storage.

BASIC AGENT SETUP IN KNIME

Before diving into the details, it's helpful to understand how KNIME's core features align with the foundational concepts of agent design.

- **Tools in KNIME**

  In KNIME, tools refer to visual workflows built with predefined logic that solve structured problems without machine learning or generative models. These workflows are useful for tasks that follow clear rules and can be built with ETL nodes, for instance retrieving information on customer data, employees, top customers, or sending emails.

- **Intelligent Tools in KNIME**

  In KNIME, intelligent tools are task-specific workflows powered by AI components, such as LLMs. An example is a workflow for sentiment analysis.

  The KNIME AI extension enables seamless integration with a variety of models, including those from OpenAI, Hugging Face Hub, DeepSeek, as well as locally hosted models like GPT4All. It provides dedicated nodes for prompting chat and embedding models, along with tools for working with vector stores such as Chroma and FAISS.

- **AI Workflows in KNIME**

  AI workflows line up tools and intelligent tools to solve a complex, but standardized task. For example, call one tool to read customer data, another to retrieve recent transactions, and a third to predict churn. AI workflows are not just about isolated tasks — they can be orchestrated as part of more complex, agentic systems.

  These workflows are designed for flexibility and can be triggered independently or embedded into larger automation pipelines. They also support interaction with external services through APIs, database connections, and other integrations.

  An example is a workflow to summarize JIRA tickets, combining text parsing, API access, and LLM-based summarization in one process.

- **AI Agents in KNIME**

  Instead of predefining every step manually, AI agents dynamically assemble and execute the necessary tools based on input data and flow control mechanisms. This can be achieved using KNIME workflows for flow control, such as:

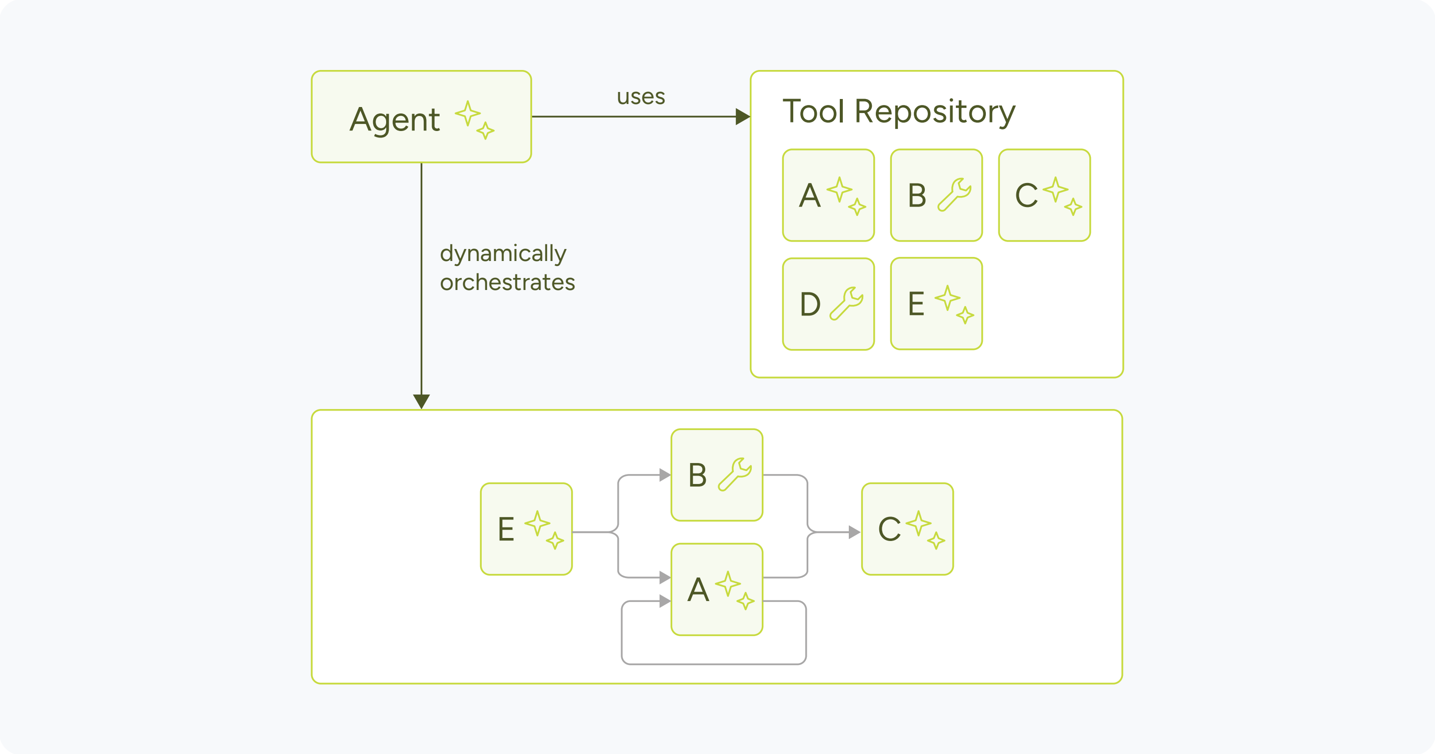
  - Conditional Logic: Directing the workflow based on input conditions, ensuring tasks are executed only when relevant.
  - Loops and Recursion: Repeating steps until a condition is met, allowing workflows to refine results over multiple iterations.
  - Parallel Processing: Running multiple tasks simultaneously, improving efficiency by handling different aspects of a problem at the same time.

  AI agents make use of both rule-based and LLM techniques to select and use the right tools. These principles allow AI agents to autonomously manage tools, making them adaptive and scalable rather than rigid sequences of predefined steps.

- **Tool Repository for Agents**

  Each KNIME workflow can serve as a reusable tool in a repository, allowing AI agents to dynamically access it for specialized tasks. KNIME Hub acts as a central repository of tools. It lets agents select and run the most suitable tool based on real-time conditions, rather than relying on a single, monolithic workflow.

  KNIME Hub houses both traditional tools — such as those for data filtering or formatting — and intelligent tools powered by AI models for tasks like classification or summarization. Agents can dynamically integrate these tools to generate responses tailored to user input or specific business contexts.



- **Making Agents Available to Users**

  Agent-based workflows, like regular ones, can be deployed through KNIME Hub in a variety of ways — whether as data apps, background services, or REST APIs — depending on what fits best in your setup.

- **Giving Agents Structured Access to Tools with Model Context Protocol (MCP)**

  The more context an agent has about available tools and how to use them, the more effectively it can solve problems and take action.

  MCP provides a structured way to give AI agents the context they need to operate in real business environments where actions must be informed by both data and context.

  With MCP:

  - AI agents can automatically discover available tools.
  - They interact with tools using a standardized format.
  - Tool descriptions are clear and accessible to both humans and AI.

  In KNIME, an MCP-compatible tool is a KNIME workflow that accepts defined inputs, returns JSON outputs, and is exposed as a REST service via KNIME Business Hub. It includes a description file that follows the MCP schema, allowing AI agents to understand and use the tool in a consistent way.

Step 1: Build Your Tools

Let's start with building some tools that can be used by our agents:

TOOL 1: DISCOUNT CODE GENERATOR

This tool is a KNIME workflow that generates a discount code based on user feedback. It takes input such as product details and user comments, automatically producing a personalized discount code.

Download the workflow and open it in your KNIME Analytics Platform to start using it as a tool.

Note that this is a demonstration tool only. No actual discount codes are generated.

TOOL 2: SUPPORT ESCALATOR

The Support Escalator tool is a KNIME workflow that handles negative feedback. It creates support tickets automatically and escalates user complaints for further attention. It requires input such as product name and detailed feedback.

Download the workflow here.

Note that this is a demonstration tool only. No actual support ticket is generated.

TOOL 3: COMPANY INSIGHTS RETRIEVER

The Company Insights Retriever Tool is a KNIME workflow that pulls key information about a company from the database — such as domain, industry, market presence, revenue, employee count, and customer status. It also identifies people linked to the company, helping answer questions like whether someone works for a customer. Download the workflow here.

TOOL 4: EMPLOYEE LOOKUP

This tool performs similarity searches in KNIME's employee database, retrieving details of current or former employees. It doesn't require AI but leverages database queries to gather relevant data. Get the workflow here.

Defining each tool involves:

- Naming the tool clearly.
- Providing a precise, descriptive summary (the tool description).
- Specifying input and output parameters and data formats clearly, usually as JSON.

The clarity of your tool descriptions significantly impacts how effectively your agent interacts with these tools.

Optional Step 1.2: Make Your Tools MCP Compatible

If this step feels a bit advanced right now, feel free to come back to it later once you're more comfortable with the basics of agent development.

To make your tools MCP-compatible, you'll need to:

1. **Structure Your Tool Workflow**

   Create a KNIME workflow using three parts:

   - **Input processing:** Use Container Input (JSON) nodes to define the tool's input format and validation.
   - **Core logic:** Use KNIME nodes to fetch or process data. Validate the input and handle errors using a Try-Catch pattern.
   - **Output preparation:** Format results as a JSON content array (text, image, etc.). Send it via a Container Output (JSON) node.

2. **Deploy The Tool**

   Deploy the workflow as a service on KNIME Business Hub. Use clear, consistent naming (e.g., prefix with "Tool:") so it can be listed and discovered easily.

3. **Set up an MCP Server**

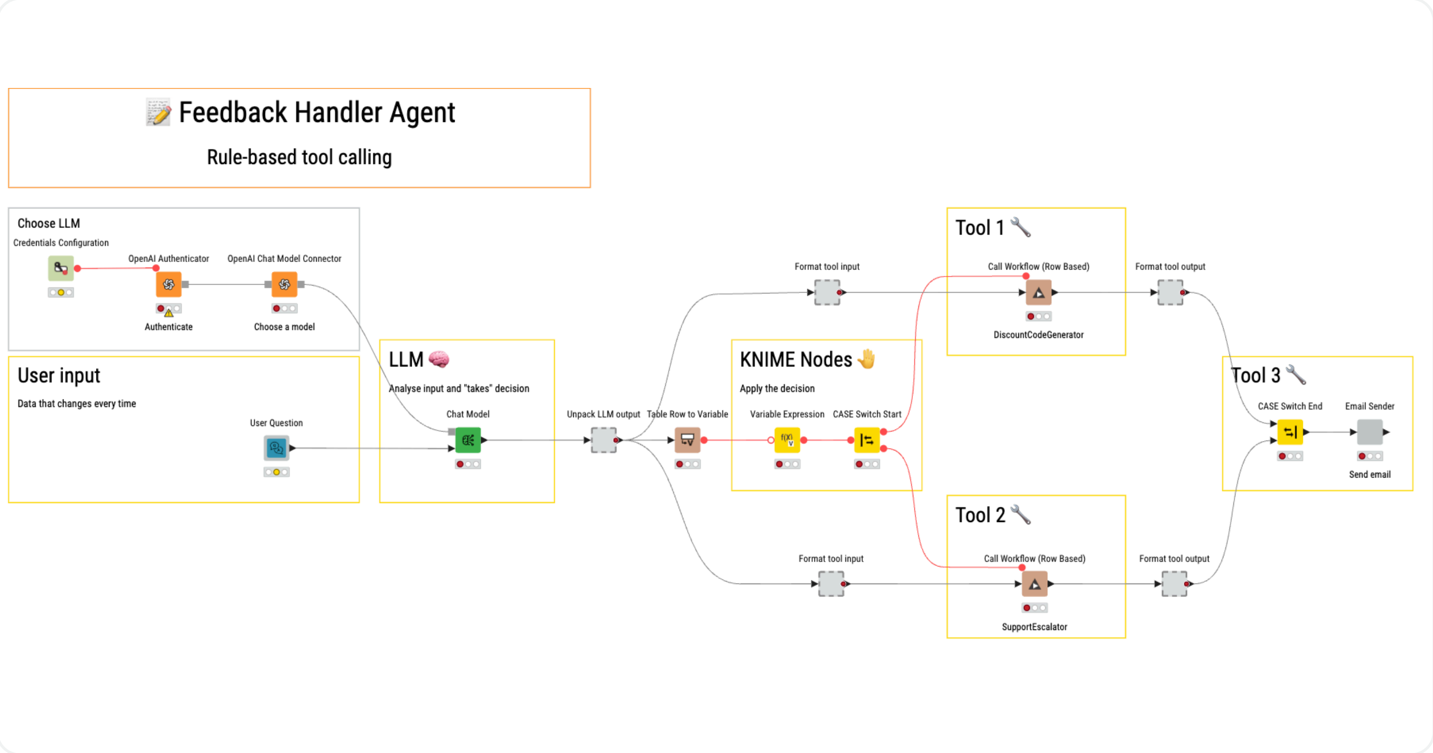
   Build a KNIME workflow that acts as the MCP Server. It should:

   - Respond to *initialize*, *initialized*, *tools/list*, and *tools/call* methods.
   - Return schema and metadata based on tool deployments.
   - Route requests to the appropriate tool services and return the output or error.

If you still need more examples and details, take a look at this article.

Step 2: Build a Simple Agent That References Tools

Now, let's build a basic agent using the tools we've created. This agent analyzes user feedback sentiment (positive or negative) and routes the feedback appropriately.



The agent is a KNIME workflow that consists of three key phases:

1. **Decision-Making Layer:** The workflow starts with an LLM node that analyzes user feedback and returns a structured JSON output. This output contains the sentiment polarity (positive or negative) and the identified product, if available. A Case Switch Start node then uses the sentiment value to direct the flow of data to the correct processing branch.

2. **Workflow Execution:** Based on the sentiment of the input, the agent routes it to the right workflow using the Call Workflow (Row Based) node:
   - If the feedback is **positive**, the agent triggers the Discount Code Generator workflow, optionally using the referenced product to create a personalized reward.
   - If the feedback is **negative**, it kicks off the Support Escalator workflow to open a support ticket and log the issue.

3. **Final Processing and Response Generation:** Once the chosen workflow finishes running — whether it returns a discount code or a support ticket number — that result is sent to the Email Sender tool. This tool sends a confirmation email to the user, wrapping things up with either a thank-you message or a support response. Finally, the Case Switch End node brings everything together into one unified response stream.

Download the feedback handler agent workflow here.

Note that this is a manually constructed agent — you explicitly define the logic for each case, and manually configure which tools are triggered for which type of input. The downside with this approach is that you know the tools you want to call, but each tool call must be created manually.

For every new tool, or if the logic needs to expand (e.g., adding a third tool for neutral sentiment), you have to change the system prompt, update the routing logic, and edit the workflow structure accordingly. This setup doesn't scale well and introduces friction if your logic becomes more complex. So, let's make it a little more "agentic" in the next step.

Step 3: Build a More Complex Agent That References Internal And External Tools

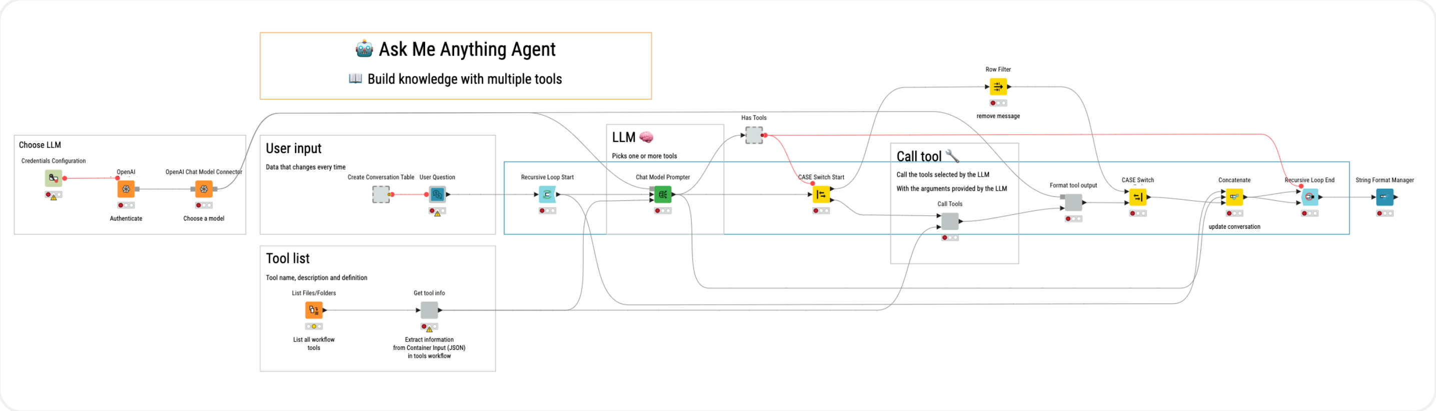
Our second agent improves on the first by allowing the LLM itself to select which tool to call, eliminating the need for manual routing.

This allows the agent to perform multiple steps, combining information from different tools.

The agent's goal is to deliver accurate, relevant answers even when the response depends on structured company data, employee records, or past support interactions.

To do this:

- The LLM analyses the user input
- The LLM selects one or more tools
- The tool is called and produces an output
- The LLM decides if there's enough information or if it needs more information, perhaps from another tool



This agent operates in three main phases:

1. **Response Generation:** When a user submits a question, the agent creates an initial draft using an LLM. At this stage, the response might be missing important business context or verified information.

A key factor in the success of this phase is prompt design. The system prompt needs to clearly explain the agent's role, what tools are available, and when each one should be used. Effective prompts avoid naming specific software systems (e.g., Salesforce or Zendesk) and instead focus on the type of information a tool provides. This makes prompts more stable over time and easier to maintain as systems change.

2. **Evaluation & Refinement**: Next, the agent reviews the draft to see if it needs more detail or context. Depending on what the user asked, it can call one or more tools using the Call Workflow (Row Based) node, including:
   - Company Insights Retriever: Finds key company details like domain, size, and customer status.
   - KNIME Employees Lookup: Checks whether someone currently works — or previously worked — at KNIME.
   - KNIME User Info: Looks up a user's presence on KNIME's forum and Hub.
   - Ticket Retrieval Tool: Pulls support history from Zendesk for a given company.

   These tools are used in order when needed — for example, it might fetch the domain first, then use that to get support tickets. This loop continues until all the necessary information is gathered and the response is complete. The Loop Start and Loop End nodes manage this back-and-forth process.

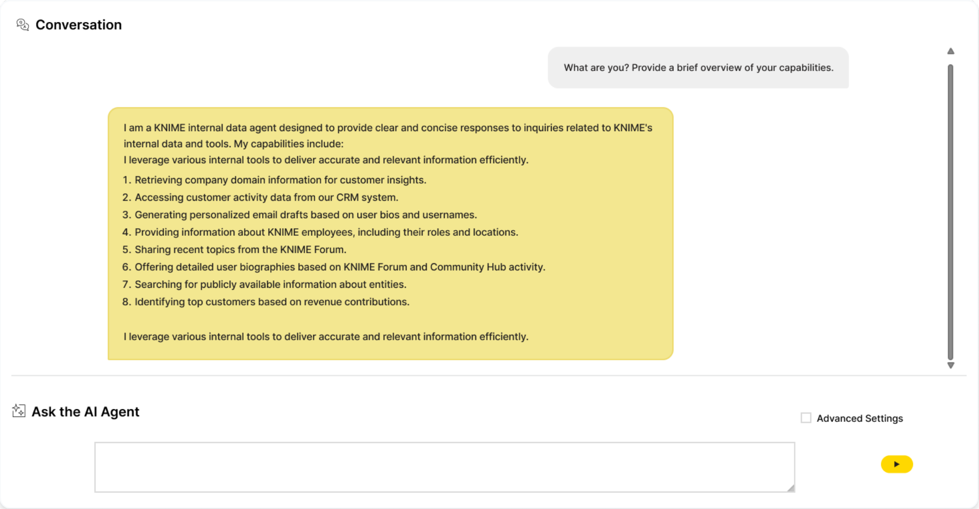
3. **Final Approval & Delivery:** Once the response meets quality standards, the workflow exits the loop. The final answer is well-structured, supported by data, and ready to send back to the requester.

Step 4: Build an Ask-Me-Anything Agent

Finally, we will build an ask-me-anything agent that users can access through a KNIME data app. Users type questions into the chat, and the agent selects and runs the appropriate tools. It then integrates their outputs to provide an informed response.

The chat interface is effective because users don't need to know data locations or which tools to use. They simply ask their question, and the agent handles the technical work.

Here's what it will look like:



What are you? Provide a brief overview of your capabilities.

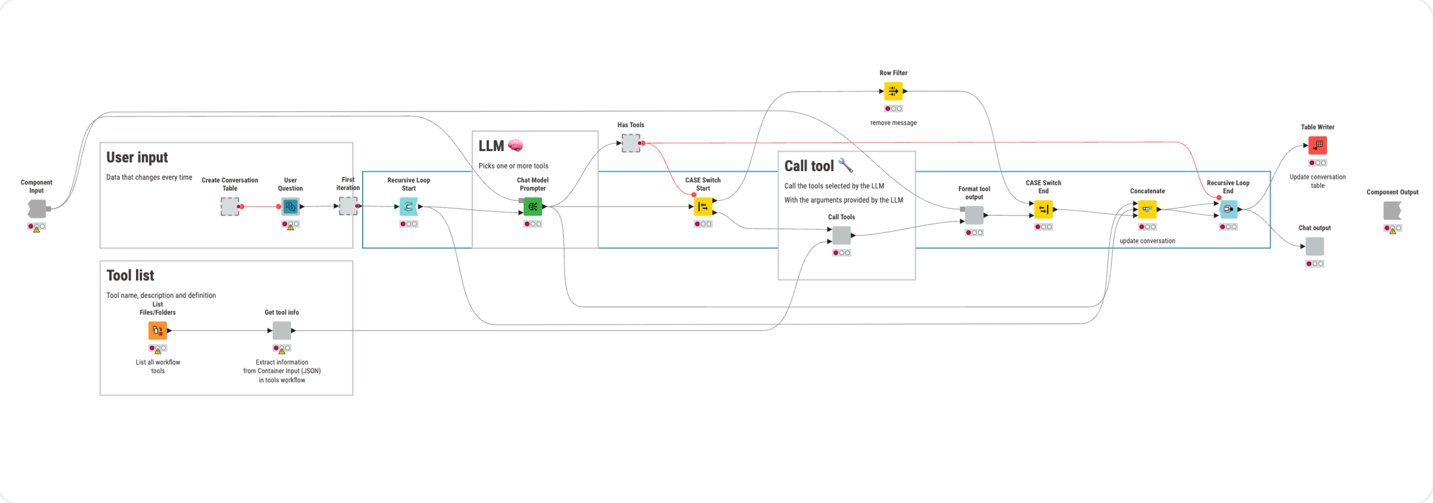
I am a KNIME internal data agent designed to provide clear and concise responses to inquiries related to KNIME's internal data and tools. My capabilities include:
I leverage various internal tools to deliver accurate and relevant information efficiently.

1. Retrieving company domain information for customer insights.
2. Accessing customer activity data from our CRM system.
3. Generating personalized email drafts based on user bios and usernames.
4. Providing information about KNIME employees, including their roles and locations.
5. Sharing recent topics from the KNIME Forum.
6. Offering detailed user biographies based on KNIME Forum and Community Hub activity.
7. Searching for publicly available information about entities.
8. Identifying top customers based on revenue contributions.

I leverage various internal tools to deliver accurate and relevant information efficiently.

Here's what you need to do:

1. Build your agent as outlined in stage 4, connecting to an LLM model and KNIME Hub to access the tools from the previous example and others.
2. Create a KNIME data app to enable user interaction with your agent.
3. Deploy to KNIME Business Hub or KNIME Community Hub to make it available to users.



Download the agent here

And that's it! You've now constructed three progressively advanced AI agents, from basic sentiment routing to an agentic application capable of multi-step reasoning.

Governing And Managing Risk with AI Agents

You've taken a major step forward with building and deploying three agents. But it also means that you now need to manage the associated risks. AI agents operating in real-world environments can make decisions that affect users, data, and systems, so it's important to put proper safeguards in place.

With KNIME Business Hub, you can start by enforcing data and model governance across your workflows. For example, you can intercept and block any attempts to send sensitive information such as personal identifiers or confidential records to external LLM providers. Alternatively, you can configure your workflows to anonymize such data before it's ever exposed.

Govern Centrally

Controlling Models we don't understand isn't new — it's just now top of mind. KNIME's governance framework has been developed over 5+ years.

Govern access to technology

Manage user access to only approved vendors

Govern output & quality of models

Monitor and validate model output, ensuring safeguards for consistency, accuracy, and reliability

Govern data sent to models

Control data inputs sent to models, sharing standards on which data is sent and how (e.g. anonymized)

Govern regulatory compliance

Implement automated auditing and monitoring of model usage and data handling, ensuring adherence to industry regulation and data privacy laws

KNIME's workflow-based environment gives you the flexibility to define and adapt these controls to meet your internal policies or compliance needs.

On top of that, you can use KNIME Giskard nodes to introduce LLM-as-a-judge structures, where one model checks another's outputs for reliability or appropriateness. If needed, you can manually coordinate multiple LLMs to audit or confirm decisions before they're acted upon.

These practices help reduce the likelihood of errors, misuse, or unintended consequences as your agents continue to run in production.

Applying This Knowledge And Finding Use Cases Within Your Enterprise

You don't need to overhaul your infrastructure or rewrite your processes to benefit from agents. The key is to start small. Identify tasks that are repetitive, structured, and already require data or decision-making. These are perfect candidates.

Think of places where people routinely have to look things up, format something, compare values, or wait for approvals. Those friction points are where agents can immediately help.

As you build more agents, patterns will emerge. You'll start to recognize reusable components, scalable workflows, and team-specific needs. And because KNIME keeps everything visual and modular, it's easy to adapt and iterate as you go.

Organizational Structure: Evolving Instead of Expanding

When integrating AI agent capabilities into your organization, reconsider building entirely new departments dedicated to AI. Your current data science or analytics teams likely already possess most of the required expertise and infrastructure. Rather than starting from scratch, focus on adding agentic tooling, upskilling existing staff, and subtly adjusting team responsibilities to include agent development and management.

This evolutionary approach aligns with the growing emphasis on integrated data and AI literacy, recognizing that data professionals already have a deep understanding of the data landscape and analytical methodologies. By enhancing your existing team's skills and scope, your organization can efficiently and sustainably integrate AI agents without unnecessary structural overhead.

Looking Ahead: The Future of Agentic Workflows

Agentic AI is still early, but it's evolving quickly. One trend to watch is the rise of multi-agent systems — agents that work together, handing off tasks or collaborating on complex workflows.

Another is the integration of agents across systems, where they can orchestrate processes that span CRMs, ERPs, and communication tools.

Over time, we're likely to see marketplaces or libraries of prebuilt agents tailored to common business functions. But custom agents will still matter — because no two organizations work exactly the same way.

If you're just getting started, the opportunity is clear: you can build useful, tailored automation without waiting for a vendor to catch up.

KNIME's approach to agentic AI is built around flexibility. Agents aren't locked into narrow tasks, rather they can take on broader responsibilities and evolve as needs change. Tools don't have to live in one place; they can be brought in from wherever they're already working. Prompts are editable and specific, shaped by the people using them. And importantly, collaboration isn't limited to one part of the organization. Whether you're a data engineer or a business analyst, you can contribute to systems that grow more capable over time, without having to start from scratch each time.

As these systems become more complex and widely adopted, structure and oversight become just as important as flexibility. That's where KNIME Business Hub comes in. It provides a foundation not just for building and running agentic workflows, but for doing so in a way that's accountable, maintainable, and grounded in reliable data.

As a final note, start simple, focus on real problems, and keep humans in the loop. That's how you go from zero to something that actually works. ■

Get in Touch

If your organization is starting to think seriously about deploying intelligent systems across teams, KNIME Business Hub is worth exploring. It's designed for exactly this kind of scaling up, with the guardrails that help keep things on track.

Learn more about productionizing agents with KNIME Business Hub

Additional Resources

- Download more agent examples from KNIME Community Hub
- Take the "AI for Data Analytics" online course