Cloudera AI

Cloudera AI Studios Release Notes

Date published: 2020-07-16
Date modified: 2026-01-06

https://docs.cloudera.com/

Legal Notice

Contents

What's New

This version of Cloudera AI Studios provides you with several new capabilities. Learn how the new features and improvements benefit you.

February 23, 2026

Release notes and fixed issues for AI Studios.

Agent Studio - 2.2.0

This version of Cloudera AI Studios provides you with several new capabilities. Learn how the new features and improvements benefit you.

New Features/Improvements

- Role-Based Access Control: Agent Studio now includes a comprehensive Role-Based Access Control (RBAC) system to ensure secure access to workflows, models, and tools. This system allows for fine-grained control over who can view, edit, deploy, and delete resources within the agent studio. For more information see, Managing user access with Role-Based Access Control (RBAC).
- Stopping Workflows: A running workflow can be stopped to safely terminate AI agents and halt active processes. For more information see, Stopping a workflow.
- Workflow Evaluations: A new Evaluations feature in Agent Studio, now provides a built-in suite of diagnostic and quality-assurance tools to measure the performance, accuracy, and safety of the Agentic Workflows. Users can now assess workflows during the development phase in Studio and audit historical runs in Deployed Workflows. For more information see, Managing Workflow Evaluations.

RAG Studio - 2.0.0

This version of Cloudera AI Studios provides you with several new capabilities. Learn how the new features and improvements benefit you.

New Features/Improvements

RAG Studio installation using ML Runtime image: RAG Studio is now exclusively shipped as a prebuilt, containerized ML Runtime Image for both on-premise and cloud deployments. This streamlined approach eliminates the need for compiling raw source code within the customer environment, providing a consistent, reliable, and production-ready installation. For more information see, Deploying RAG Studio using the ML Runtime Image

- Deprecation Notice: The existing methods of deployment (from source code) and AMP mode are now deprecated. The latest releases will be available only through an ML Runtime Image.

January 06, 2026

Release notes and fixed issues for AI Studios.

Agent Studios - Hotfix (version 2.1.1)

Release notes for the Agent Studio version 2.1.1. This hotfix release provides critical updates and fixes for the Agent Studio 2.1.0 release.

Fixed Issues

- Critical CVEs related to NextJS and React have been fixed. (CVE-2025-67779, CVE-2025-55184, and CVE-2025-55183)

- Resolved a bug in the Agent Studio's Smart Viz tool that caused incorrect visualization types, ensuring the correct visualization types are now generated across all environments. (DSE-50382)
- Resolved an issue where MCP registration would sometimes fail in environments where the MCP server enforced environment variable validation. (DSE-49389)

December 08, 2025

Release notes and fixed issues for AI Studios.

Agent Studios - TP (version 2.1.0)

Release notes and fixed issues for version Agent Studio 2.1.0.

New Features / Improvements

- Artifact Support: Agents can now reliably create, read, and share files such as CSV, JSON, images, and custom code within workflows. This allows agents to handle and exchange large datasets and rich outputs effectively.
- Smart Workflows: When enabled, the Smart Workflows feature uses an upgraded agentic framework that improves context management in complex multi-agent workflows, particularly those orchestrated by a Manager Agent. It ensures that agents receive the necessary historical context, reducing hallucination rates and improving overall workflow accuracy and stability.
- Planning and Thought Bubble: When enabled, the Manager Agent can now generate an explicit, multiple-step plan to dynamically decompose complex user queries into smaller, manageable subtasks. The Thought Bubble feature provides real-time visibility into the decision-making process, task delegation, and planning status of the agent.
- Tools Playground: Tools Playground is a dedicated UI now available for developers to test and validate custom tools and their parameters, including Artifact handling, in isolation before integrating them into a live workflow.

For more information on using Artifact Support, Smart Workflows, Planning and Thought Bubble, and Tools Playground, see Agentic Workflows.

- Secure Tool Execution and Development: The Secure Tool Execution and Development feature is a security enhancement ensuring that all tool runs are performed within a secure, sandbox environment. This isolation prevents malicious or unintended code execution from compromising the host system or other processes.

  For more information, see Secure Tool Execution and Development.
- Agent Studio installation using ML Runtime image: Agent Studio is now exclusively shipped as a prebuilt, containerized ML Runtime Image for both on-premise and cloud deployments. This streamlined approach eliminates the need to compile source code within the customer environment, providing a consistent, reliable, and production-ready installation.
  - Migration Support: Migration to ML Runtime Image mode is supported for the existing Agent Studio deployments.
  - Deprecation Notice: The existing methods of deployment (from source code) and AMP mode are now deprecated. The latest releases will be available only through an ML Runtime Image.

  For more information on how to install, see Deploying Agent Studio using the ML Runtime Image.
- Service Account support: Agent Studio supports deploying production and shared workflows using a Service Account (Machine User) identity and its corresponding namespace. This provides enhanced security and fine-grained permissions compared to deploying using a human account.

Fixed Issues

- A critical remote code execution vulnerability (NVD - CVE-2025-55182) in React Server Components has been fixed. For more information, see TSB 2025-921.
- Fixed an issue that caused API keys to be logged in plain text within Phoenix, addressing a significant security vulnerability. (DSE-48556)

- Resolved issues preventing the suspend and resume functionality of workflows from working correctly. This fix also resolves related UI inconsistencies. (DSE-48347)
- Fixed Model Context Protocol (MCP) server registration and configuration issues to ensure that third-party tools integrate reliably. (DSE-49771)
- Addressed MCP server functionality and stability issues impacting tool runs within workflows. (DSE-49772)
- Updated and refined several Workflow Templates to align with new features and improve the starting point quality. (DSE-49783)

Cloudera AI Studios Known Issues and Limitations

This topic describes known issues and workarounds in AI Studios.

Agent Studios

Tool Execution Failure in Azure Workbenches (DSE-50025)

Agent Studio workflow tools fail to execute in Cloudera AI Azure Workbenches, displaying the bwrap: Failed to make / slave: Permission denied error message. This occurs because Agent Studio requires Linux namespace isolation and elevated privileges for secure sandboxing, which are restricted in Azure Workbench environments.

Workaround: To enable tool execution in these environments, you can enable the Insecure Tool Execution mode. This allows tools to run without sandbox isolation.

Warning: Reduced Security: Enabling insecure mode allows tools to execute directly within the application runtime environment. Without sandbox isolation, malicious code or input could potentially access the host filesystem or exploit vulnerabilities.

To enable Insecure Tool Execution Mode:

1. Open your project in the Cloudera AI Workbench.
2. Navigate to Project Settings Advanced Environment Variables
3. Add a new environment variable:
   a. Name: ALLOW_AGENT_STUDIO_INSECURE_TOOL_EXECUTION
   b. Value: true
4. Click Submit and restart the Agent Studio application for the changes to take effect.

Caution: When using Insecure Mode, it is strongly recommended to implement validation guardrails in your tool code using Pydantic @field_validator. This creates a defense-in-depth layer to prevent path traversal, SQL injection, and unauthorized file access.

Remove or set ALLOW_AGENT_STUDIO_INSECURE_TOOL_EXECUTION to false, and restart Agent Studio application, to disable Insecure Tool Execution Mode.

TSB 2025-921 (Security): Remote code execution vulnerability in React Server Components

Learn more about the details communicated in TSB-2025-921.

Summary

Cloudera is issuing this TSB to provide updated information on the identified list of products containing the version of React affected by CVE-2025-55182.

Releases affected

- Cloudera AI running Agent Studio 2.0.0 and below

Addressed in release/refresh/patch

- Cloudera Agent Studio 2.1.0

Knowledge Base article

For the latest update on this issue see the corresponding Knowledge Base article: Technical Service Bulletin 2025-921 (Security): Remote code execution vulnerability in React Server Components