



Nutanix Puts Agentic AI into Action for Enterprises

August 10, 2026

MCP server for Nutanix Cloud Platform brings secure, natural-language, agentic AI automation to hybrid cloud environments without sacrificing control

SAN JOSE, Calif. , Aug. 10, 2026 (GLOBE NEWSWIRE) -- [Nutanix](#) (NASDAQ: [NTNX](#)), a leader in hybrid cloud computing, today announced the Model Context Protocol (MCP) server for Nutanix Cloud Platform (NCP), enabling customers to safely use AI tools to automate their daily cloud operations. The MCP server for NCP is open-source software that implements the Model Context Protocol specification and enables AI agents and developer tools to interact with NCP through the Nutanix Prism v4 API.

With the launch of its MCP server, Nutanix customers can build agentic AI applications that have access to a robust tools layer to power secure actions on NCP, empowering IT teams to speed up daily operations across large hybrid cloud environments without losing visibility or control.

Operating modern hybrid cloud environments traditionally depends on deep technical expertise and strict access controls. Although AI assistants can drastically speed up how these systems are managed, enterprises need the certainty that AI actions are safe and authorized. This level of security is necessary for everyday operations, from executing major system upgrades to tracking network performance across the entire business.

The new MCP Server for NCP solves these challenges by acting as a secure passthrough between AI assistants, such as GitHub Copilot, Claude Code, and Cursor to safely translate plain-English requests into precise infrastructure API actions for an organization's hybrid cloud environment. The solution translates everyday language requests into precise, safe system actions while automatically enforcing existing corporate security and access policies. By creating a dedicated safety passthrough around AI tools, the solution allows IT teams to confidently automate routine operations and build custom AI-driven workflows.

"Nutanix has a long history of using automation to simplify complex cloud operations. The MCP server is an exciting next step on our journey, allowing us to bring the power of autonomous AI agents to cloud management," said Thomas Cornely, executive vice president, Product Management, Nutanix. "By creating a secure gateway between AI tools and our platform, we are giving customers the confidence to safely use AI to operate and govern their hybrid cloud environments."

Enterprise AI tools are only as secure as the platform APIs powering them. The MCP server addresses this reality by building directly on the Nutanix Prism V4 API Gateway, allowing connected AI tools to inherit the native governance and fine-grained access controls of NCP. Rather than risking unassisted changes to production environments, IT operators can safely use AI assistants to analyze system health, surface diagnostics, and accurately stage automation workflows while maintaining operator oversight through 'human-in-the-loop' capabilities.

Architectural Governance and Developer Capabilities

The Nutanix Prism V4 API Gateway strictly handles all execution, governance, and security controls, enabling the MCP Server to provide a highly secure and predictable environment for enterprise AI operations. It is designed to support:

- **Fine-Grained Role-Based Access Control (RBAC):** Confines autonomous agents to executing calls only on specific APIs for which they have been granted explicit, granular authorization.
- **Throttling and Metering:** Implements built-in traffic regulation to help prevent agent swarm attacks while natively tracking API usage across automated workflows.
- **Comprehensive Auditing:** Generates detailed system logs to maintain visibility into which AI agent initiated which specific command.
- **Asynchronous Task Management:** Offloads long-running operations as asynchronous tasks, allowing autonomous agents to efficiently track progress and execution status until completion.

For developers, the MCP server makes building automation tools faster and more intuitive. By giving AI coding assistants exact system blueprints up front, developers can instantly generate platform-ready scripts in their preferred languages – including Python, Go, Java, JavaScript, PowerShell, curl, or any REST and JSON-compatible format. This allows teams to easily configure precise security permissions through a single interface or build their own custom AI agents to automate and govern their Nutanix infrastructure from end to end.

Customers can download the MCP server for NCP from developers.nutanix.com and use it with any of their own AI agents.

About Nutanix

Nutanix is a hybrid cloud leader, offering organizations a unified infrastructure software platform to safely run AI, applications and data anywhere. Trusted by customers worldwide, Nutanix empowers over 50% of the Global 2000 to innovate faster with AI, while modernizing infrastructure, simplifying operations, and controlling costs. Learn more at www.nutanix.com or follow us on social media.

© 2026 Nutanix, Inc. All rights reserved. Nutanix, the Nutanix logo, and all Nutanix product and service names mentioned herein are registered trademarks or unregistered trademarks of Nutanix, Inc. ("Nutanix") in the United States and other countries. Other brand names or marks mentioned herein are for identification purposes only and may be the trademarks of their respective holder(s). This press release is for informational purposes only and nothing herein constitutes a warranty or other binding commitment by Nutanix. This content contains express and implied forward-looking statements, including but not limited to statements regarding the availability and capabilities of the MCP server for Nutanix Cloud Platform, its integration with AI agents and developer tools, its features and performance, and our plans regarding the Nutanix Agentic AI solution. Such statements are not historical facts and are instead based on our current expectations, estimates, and beliefs. The accuracy of such statements involves risks and

uncertainties and depends upon future events, including those that may be beyond our control, and actual results may differ materially and adversely from those anticipated or implied by such statements, including, among others: potential development or distribution delays; risks inherent in the adoption of agentic AI and the MCP server for Nutanix Cloud Platform; the effectiveness of security and governance frameworks; and evolving industry standards for AI-driven automation. Any forward-looking statements included speak only as of the date hereof and, except as required by law, we assume no obligation to update or otherwise revise any such forward-looking statements to reflect subsequent events or circumstances.

Media Contact: Ken Lotich pr@nutanix.com