JFrog Enables AI-Driven Developer Workflows with Robust MCP Server

JFrog's Model Context Protocol (MCP) server allows developers to seamlessly employ AI-agents across the JFrog Platform, enabling faster, more reliable, secure software development & delivery at scale

Sunnyvale, Calif. – July 17, 2025 — JFrog Ltd (Nasdaq: FROG), the Liquid Software company and creators of the award-winning JFrog Software Supply Chain Platform, today unveiled a new Model Context Protocol (MCP) Server. This architecture enables Large Language Models (LLMs) and AI agents to securely interact with tools and data sources within the JFrog Platform directly from MCP clients, including popular agentic coding development environments and IDEs, boosting developer productivity and streamlining workflows.

"The developer tool stack and product architecture has fundamentally changed in the AI era. With the launch of the JFrog MCP Server, we're expanding the open integration capabilities of the JFrog Platform to seamlessly connect with LLMs and agentic tools," said Yoav Landman, Co-Founder and CTO, JFrog. "This allows developers to natively integrate their MCP-enabled AI tools and coding agents with our Platform, enabling self-service AI across the entire development lifecycle, which helps increase productivity and build smarter, more secure applications faster."

Securely Powering the JFrog Software Supply Chain Platform with Agentic AI

The Model Context Protocol (MCP) is an open, industry-standard integration framework designed to connect AI systems with external tools, data, and services. With JFrog's MCP Server, developers can now use natural language commands like *"Create a new local repository"* or *"Do we have this package in our organization?"* to interact with the JFrog Platform directly from their IDE or AI assistant. Teams gain immediate awareness of open-source vulnerabilities and software package usage without context switching, saving developers time. AI automation also helps simplify complex queries that previously required advanced developer knowledge, helping all teams work smarter and faster.

While remote MCP servers can help facilitate rapid code iteration and improve software reliability, they are not without risk. The JFrog Security Research Team recently discovered vulnerabilities, such as CVE-2025-6514 that could hijack MCP clients and execute remote code, potentially leading to severe consequences. This is another reason why JFrog's MCP

Server is designed with security in mind and relies exclusively on trusted connection methods, such as HTTPS.

JFrog's MCP Server securely provides:

- **Essential Tools for Gaining Software Package Insights:** Users can leverage a base toolset to create and manage projects, repositories, view build status, and query detailed package and vulnerability information.
- **Centralized, Cloud-Native MCP Server with Automatic Updates:** Available to JFrog SaaS customers and multi-tenant environments, JFrog's MCP server is implemented as a remote, secure server available in all JFrog cloud environments, providing automatic version updates and improvements with less maintenance.
- **Secure OAuth 2.1 Authentication:** Enforcing modern token-based authorization with scoped access per tenant and tool, making sure all operations are authenticated and performed under the identity of the end user.
- **Production-Grade Monitoring:** Comprehensive logging and event tracking for actionable insights into tool usage.

JFrog's new MCP Server for the JFrog Platform is now available for developers to test and provide feedback during a preview period. For more information and to get started, check out this blog or visit the AWS marketplace. Interested parties can also check out this step-by-step guide on how to get your JFrog MCP client up and running quickly.

###

Like this Story? Share this on X: .@jfrog introduced its new MCP Server for the JFrog Platform so developers can utilize their favorite LLMs and agents quickly and securely directly from their IDE to speed their workflows. Learn more: https://jfrog.co/46dUcMf
#agenticAI #SoftwareSupplyChain #DevOps #DevSecOps #cybersecurity #AI #DeveloperTools

About JFrog
JFrog Ltd. (Nasdaq: FROG) is on a mission to power the world with liquid software. We are replacing endless software updates with a single system of record that seamlessly delivers secure applications from developer to device. The JFrog Software Supply Chain Platform helps organizations build, manage, and distribute software quickly and securely, making applications available, traceable, and tamper-proof. Its integrated security features also help identify, protect, and remediate against threats and vulnerabilities. The Platform also brings ML models in line with all other software development processes, providing a single source of truth for all software components across Engineering, MLOps, DevOps, and DevSecOps teams so they can build and release AI applications

faster, with minimal risk and less cost. JFrog's hybrid, universal, multi-cloud platform is available as both self-hosted and SaaS services across major cloud service providers. Millions of users and 7K+ customers worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation. Once you leap forward, you won't go back! Learn more at jfrog.com and follow us on X: @jfrog.

Cautionary Note About Forward-Looking Statements

This press release contains "forward-looking" statements, as that term is defined under the U.S. federal securities laws, including, but not limited to, statements regarding our expectations with respect to the anticipated performance of the MCP Server, including the ability to securely interact with tools and data sources within the JFrog Platform directly; and anticipated increases in efficiency and security.

These forward-looking statements are based on our current assumptions, expectations and beliefs and are subject to substantial risks, uncertainties, assumptions and changes in circumstances that may cause JFrog's actual results, performance or achievements to differ materially from those expressed or implied in any forward-looking statement. There are a significant number of factors that could cause actual results, performance or achievements to differ materially from statements made in this press release, including but not limited to risks detailed in our filings with the Securities and Exchange Commission, including in our annual report on Form 10-K for the year ended December 31, 2024, our quarterly reports on Form 10-Q, and other filings and reports that we may file from time to time with the Securities and Exchange Commission. Forward-looking statements represent our beliefs and assumptions only as of the date of this press release. We disclaim any obligation to update forward-looking statements except as required by law.

Media Contact:

Siobhan Lyons, Director, Global Communications, siobhanL@jfrog.com

Investor Contact:

Jeff Schreiner, VP of Investor Relations, jeffS@jfrog.com