

PDQ Launches MCP Server to Bring Secure AI Workflows to Endpoint Management

New integration lets IT teams investigate issues, answer operational questions, trigger deployments, and build custom automations from supported AI tools



SALT LAKE CITY, UT, UNITED STATES,

August 12, 2026 /EINPresswire.com/ -- PDQ, a leading provider of endpoint management solutions, today announced early access to its Model Context Protocol (MCP) server, giving IT teams a new way to investigate their environments, answer questions, trigger deployments, generate reports, and build custom automations directly from supported AI tools including Claude, Microsoft Copilot, VS Code, and other MCP-compatible tools. PDQ's MCP server is being published through native AI connector directories, making it easier for customers to discover and securely connect to PDQ from the AI tools they already use to [automate routine tasks](#).

For example, an IT administrator could ask an AI assistant to:

- Show every device missing Google Chrome.
- Identify devices that have not checked in during the last 30 days.
- Deploy the latest Chrome update to the marketing device group.
- Create a Patch Tuesday interactive HTML report.
- Report how many devices are still running Windows 10.
- Identify devices missing Zoom and deploy it.

"IT teams shouldn't have to spend their time translating a straightforward goal into the right combination of clicks, filters, and reports," said Mark Littlefield, VP of Product at PDQ. "PDQ's MCP server gives admins a more flexible way to investigate their environments and take action while keeping permissions, authentication, and auditing firmly under their control."

Another Way to Work With PDQ

PDQ's MCP server gives IT teams another way to interact with their endpoint environment. Because MCP exposes approved PDQ capabilities through customers' preferred AI tools, teams can investigate their environment, trigger deployments, generate reports, and build automations without changing the way they work.

AI Access With Administrator-Defined Controls

PDQ designed its MCP implementation to pair expanded automation capabilities with clear security boundaries.

Connections use existing administrator-defined user permissions carry through to MCP interactions. Administrators determine what each user and AI integration can access and do, including whether they have read-only, reporting, deployment, or administrative permissions.

Supported actions are authenticated and recorded in PDQ's audit log, including the user and AI client that initiated the request. Administrators can also view active MCP connections and revoke access from the app connections page in PDQ settings.

The PDQ MCP server is available for free in early access to customers across all PDQ subscription tiers. Additional availability and packaging information will be announced at a later date. Claude users can access PDQ's MCP through [Anthropic's Connectors Directory](#), with support for additional AI marketplaces planned.

To learn more about how to customize and automate IT with PDQ AI, visit www.pdq.com/pdq-connect/features/ai-package-assistant/

Frequently Asked Questions

What is Model Context Protocol?

Model Context Protocol, or MCP, is an open standard that allows AI assistants to securely interact with software. Instead of requiring a separate custom integration between every AI assistant and every software product, MCP provides a consistent way for software to make approved information and actions available to AI tools.

What can IT teams do with PDQ's MCP server?

IT teams can use supported AI assistants to investigate endpoint health, identify devices missing software, review deployment results, generate reports, answer operational questions, initiate deployments, and build custom automations.

The actions available to each user depend on the permissions assigned by their PDQ administrator.

Does MCP replace the PDQ interface?

No. The PDQ interface remains available for managing devices, deployments, vulnerabilities, software, and other endpoint operations. MCP provides another way to interact with PDQ, particularly when an administrator wants to ask a question, investigate an issue, or incorporate endpoint management into a broader AI-assisted workflow.

How does PDQ secure AI integrations?

PDQ uses OAuth authentication, administrator-defined permissions, and audit logging to control MCP access. Existing PDQ permissions determine what a user can view or do through an AI assistant.

Supported actions are attributed to the specific user and AI client that initiated them.

Administrators can review active connections and revoke access from PDQ settings.

How is MCP different from an API?

APIs are primarily designed for developers who know which endpoint to call, what information to request, and how to structure the interaction. MCP makes product capabilities easier for AI assistants to discover and use based on the user's stated goal.

In simple terms, APIs allow software to communicate with software. MCP gives AI assistants a standardized way to understand and interact with approved software capabilities. Many MCP servers are built using existing APIs.

Is PDQ's MCP server officially supported?

Yes. PDQ's MCP server is developed and supported by PDQ. It is not a community-maintained or unofficial integration.

Who can access the MCP server?

The MCP server is available to customers on all PDQ subscription tiers during early access.

Access remains subject to administrator-defined permissions and supported AI clients.

Availability and packaging after the early-access period will be announced separately.

About PDQ

PDQ builds IT management tools that are simple, secure, and pretty damn quick. Trusted by system administrators, MSPs, and IT professionals worldwide, PDQ is an autonomous endpoint management solution for Windows and macOS devices, supporting patching, software deployment, and vulnerability management. Founded in 2001 and based in Salt Lake City, Utah, PDQ serves over 33,000 customers and has received G2 Leader and High Performer awards across Endpoint Management, Patch Management, and Remote Support. Learn more at pdq.com.

Meredith Kreisa

PDQ

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)

[X](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/933607104>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.