

LoginRadius MCP Auth Moves to GA to Secure AI Agent Access

VANCOUVER, BRITISH COLUMBIA, CANADA, June 2, 2026 /EINPresswire.com/ -- [LoginRadius](#), a global leader in customer identity and access management (CIAM), today announced the general availability of its Model Context Protocol (MCP) Authorization capability. This enterprise-grade identity framework for securing how AI agents access and act on user data is now available for all, across production environments.

“

With MCP Auth, we have introduced standards-based, user-rooted token flows. It gives organizations the exact granular controls, human-in-the-loop, and audit visibility they need to scale AI agents.”

*Kundan Singh, VP Engineering
at LoginRadius*

The AI industry is rapidly shifting from passive chatbots to autonomous "AI Agents" that can execute real-world tasks - like booking flights, writing code, or fetching corporate data. To do this, AI applications rely on a new universal connector called the Model Context Protocol (MCP).

However, currently, giving an AI agent unlimited access to a system means opening up a playground for hackers. To combat this, one would need a trusted authorization server that can manage agentic identity end-to-end, starting from identity, authorization, user consent, to audit

and governance controls. This is where LoginRadius steps in.

LoginRadius [MCP Auth](#) acts as an enterprise-grade identity and auth layer, delivering delegated access to AI agents and assigning unique verifiable identities to each agent. To do so, the platform utilises the gold standard of modern cybersecurity: OAuth 2.1 with PKCE.

"AI agents are fundamentally changing workflows, but giving an agent access to a system shouldn't mean handing it unconstrained power," said Kundan Singh, Vice President of Engineering and Information Security at LoginRadius. "With MCP Auth, we have introduced standards-based, user-rooted token flows to the AI ecosystem. It gives organizations the exact granular controls, human-in-the-loop guardrails, and audit visibility they need to scale autonomous agents without any threat."

Key Capabilities of LoginRadius MCP Auth Include the following:

1. Secure Delegated Access - By utilizing OAuth 2.1 with PKCE, LoginRadius securely issues tokens to desktop-based AI hosts (like Claude Desktop or Cursor) without embedding vulnerable "Client

Secrets" in the application code.

2. Granular Scoping (Least Privilege) - The platform issues short-lived, explicitly scoped access tokens (e.g., mcp:tool:invoke:book_flight). This ensures an AI agent might be authorized to read logs but is strictly blocked from executing destructive actions, such as dropping a database table.

3. Human-in-the-Loop (HITL) Enforcement - Acting as the ultimate firewall, LoginRadius allows systems to pause execution on high-risk actions. It requires explicit user approval or Adaptive MFA before an agent can proceed, ensuring the user remains in the driver's seat against AI hallucinations.

4. Advanced Threat Mitigation - The architecture stops "Exposed Server" attacks by validating Bearer tokens before requests reach the data layer, and prevents token forwarding ("Confused Deputy") attacks by cryptographically binding tokens to a specific target server.

5. Audit & Governance - To meet strict enterprise compliance (such as SOC and GDPR), the feature maintains full visibility with comprehensive audit trails that track the specific User, Agent, Tool, and Action.

The LoginRadius MCP Auth solution is built for real-world applications across various sectors and agents, including customer support agents, travel assistants, knowledge assistants, internal productivity agents, developer agents, B2B SaaS (CRM/ERP), API-first environments, and for large enterprises such as banks and healthcare organizations.

By adopting this strong identity standard, organizations can deploy autonomous AI agents with the trust and security required for live infrastructure, effectively solving the dichotomy of utility versus security.

Availability and Activation

Initially introduced in January 2026 under an exclusive early-access period, the feature has been highly praised by early adopters and testers for its seamless integration and robust security control.

LoginRadius MCP Auth is now available for all existing customers and new tenants. Because securing AI agent infrastructure requires precise configuration, this feature is activated via a guided onboarding process. Customers can initiate activation by contacting their dedicated LoginRadius Success Team member to evaluate their specific deployment architecture.

To activate the feature or to schedule a technical deep-dive with an identity architect, current customers can submit a request to their Customer Success Managers, while new customers may visit the official LoginRadius [Contact Us](#) page to connect with the LoginRadius sales team.

About LoginRadius

LoginRadius is a leading cloud-based consumer identity and access management (CIAM) solution that empowers businesses to deliver a delightful consumer experience.

The developer-friendly Identity Platform provides a comprehensive set of APIs to enable authentication, identity verification, single sign-on, user management, and account protection capabilities such as multi-factor authentication on any web or mobile application.

The company offers open- source SDKs, integrations with over 150 third-party applications, pre-designed and customizable login interfaces, and best-in-class data security products. The platform is already loved by over 500 brands, with a monthly reach of 1.17 billion consumers worldwide.

The company has been named a leading industry player in consumer identity and access management (CIAM) by Gartner, KuppingerCole Analysts, and Computer Weekly. Microsoft is a major technology partner and investor.

Media Team

LoginRadius Inc

+1 844-625-8889

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/916763124>

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.