

LOGICMONITOR MCP FOR EDWIN AI:

Unified, Governed Context for AI Agents



CORE CAPABILITIES

Unified Access

Use one customer-specific endpoint to access available hybrid observability, digital experience, and AI investigation context across LogicMonitor.

AI Client and Workflow Connectivity

Retrieve Edwin AI investigations, understand alert or insight context, and find related incidents and operational evidence grounded in the customer environment

Operational Health From the AI Workspace

Connect supported MCP-compatible clients, custom agents, and approved operational tools to bring LogicMonitor context into AI workflows and extend Edwin AI across the operational environment.

Governed Access

Limit access based on the organization, entitlements, permissions, and resource groups. LogicMonitor Envision tools honor existing authorization controls.

Bring Trusted ITOps Context to the AI Tools Your Teams Already Use

AI assistants and custom agents are only as useful as the operational context they can access. In hybrid environments, alerts, device health, telemetry, topology, incidents, and AI investigation data are often distributed across multiple systems and interfaces. Engineers must gather that context manually or maintain custom integrations before an agent can provide a useful, evidence-based answer.

LogicMonitor MCP for Edwin AI provides a standards-based, LogicMonitor-hosted connection that gives approved MCP-compatible clients access to the hybrid observability and AI investigation context across LogicMonitor through a single endpoint. This brings trusted ITOps context into the AI interfaces and workflows teams already use, while also giving Edwin AI a standardized way to connect with approved tools and systems across the broader operational environment. LogicMonitor MCP provides the interoperability layer; Edwin AI remains the intelligence layer for investigation, root cause analysis, recommendations, and automation.

How It Works

LogicMonitor MCP follows a simple connect, discover, route, and respond flow.



Connect

Configure an MCP-compatible client with the customer-specific LogicMonitor MCP for Edwin AI endpoint and the required credentials.



Discover

The client lists the tools available to the organization based on product entitlements, available capabilities, and permissions.



Route and Retrieve

When a user asks a question, the LogicMonitor MCP server routes the request to the appropriate LM Envision, Edwin AI, or Digital Experience capability and retrieves the permitted context.

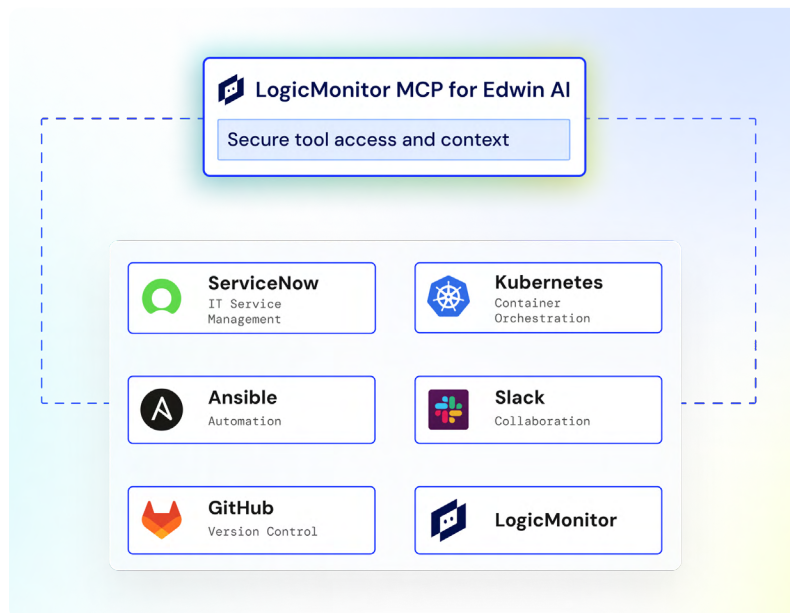


Reply

LogicMonitor MCP returns structured data to the AI client. The client can then present a natural-language answer or pass the context into an approved internal workflow.

Where LogicMonitor MCP Delivers the Most Value

- 
Investigating Alerts Without Switching Tools
 Ask an AI client for the context behind an alert or insight, retrieve the associated Edwin AI investigation, and review related incidents or operational history from the same interface. This reduces time spent opening dashboards and manually assembling the initial incident picture.
- 
Checking Environment Health on Demand
 Query device or collector health during triage, troubleshooting, or change validation. Engineers can get an initial operational answer directly from an IDE, AI assistant, or other approved MCP client.
- 
Grounding Custom Agents in LogicMonitor Data
 Give internally developed agents a standardized way to retrieve approved LogicMonitor context instead of creating and maintaining a separate API wrapper for every data set and workflow.
- 
Evaluating Agentic Operations with Lower Risk
 Begin with read-only context retrieval to validate answer quality, data access, permissions, and workflow usefulness before introducing higher-autonomy actions. Teams can build confidence in agent-assisted operations while preserving human control.



What Sets LogicMonitor MCP Apart

Operational and AI context through one connection.

LogicMonitor MCP brings LM Envision monitoring tools, Edwin AI investigation tools, and Digital Experience capabilities together behind a single endpoint. Teams can access available operational data and AI-generated investigation context without managing separate MCP servers for each LogicMonitor product.

Purpose-built context for IT operations.

The server exposes more than generic enterprise records. It provides access to alerts, operational health, Edwin investigations, alert and insight context, similar incidents, and related operational evidence that agents can use to investigate IT issues.

An open protocol that meets teams where they work.

MCP-compatible clients can access LogicMonitor context from IDEs, AI assistants, and custom workflows. Different teams can use the interface that fits their operating model rather than being forced into another standalone destination.

A governance-first path toward autonomy.

The current release begins with controlled, read-only access and existing LogicMonitor authorization controls for Envision data. This provides a practical starting point for evaluating agentic workflows before progressing toward broader context, policy-controlled actions, and agent-to-agent collaboration.



Bring LogicMonitor Context to Your AI Workflows

Connect approved AI clients and custom workflows to LogicMonitor Envision monitoring data and Edwin AI investigation context through one standards-based endpoint.

LET'S TALK