MCP SERVER | NO CODE | CLOUD HOSTED

MindsDB (AI Database & Predictors) MCP

Run ML predictions with pure SQL queries.

MindsDB (AI Database & Predictors) connects your AI client directly to a database that runs machine learning predictions via SQL. You can execute complex queries, train models on demand, and audit data sources—all through natural language conversation.

A+ Quality Score 100/100

machine-learning | sql-ml | predictive-analytics | model-deployment | data-integration

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/mindsdb-ai-database-predictors

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

MindsDB (AI Database & Predictors) MCP

6 tools available
Cloud-hosted on Vinkius

This MCP lets you treat your entire database and its built-in AI models like one giant spreadsheet. Instead of jumping between an ML platform and a traditional SQL client, you just talk to your agent. You use standard SQL commands, but they suddenly gain the power to run predictions—for example, predicting housing prices or customer churn right inside a `SELECT` statement. Need to know what data sources are connected? Just ask, and it will list everything from Snowflake tables to PostgreSQL databases. This full control over both your raw data structure and the algorithms running on it makes complex analysis straightforward. If you're building out an advanced AI pipeline, Vinkius hosts this MCP so that any compatible client can access these powerful features immediately.

Core Capabilities

01 — Audit connected data sources

Lists all external databases linked to MindsDB, letting you verify your entire data pipeline boundary.

02 — Run predictive SQL queries

Executes custom SQL that incorporates machine learning functions, retrieving predicted values alongside historical data.

03 — Manage ML models and algorithms

Checks which trained AI tables are available for querying predictions or retrieves details on a specific prediction engine.

04 — Create new predictive models

Runs commands to train brand-new machine learning models directly from your agent's SQL prompt.

05 — Check system health and status

Retrieves diagnostic information about the MindsDB cluster, confirming its operational version and availability.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/mindsdb-ai-database-predictors** — connect your AI agent in three steps.

01 First, subscribe to this MCP and enter your MindsDB API URL and required credentials.

02 Next, tell your AI client what data you need. You can ask it to list connected databases or run a prediction query.

03 Finally, the agent executes the SQL against the MindsDB engine, returning both structured results and the machine-generated predictions.

The bottom line is: you use natural conversation to perform advanced data science tasks that used to require multiple dedicated tools.

Built For

This MCP is for engineers and analysts who struggle with context switching. If your job requires combining historical reporting with future forecasting, this tool saves you hours of jumping between dashboards and terminals.

Data Scientist

Runs complex queries to test predictor accuracy or monitor the status of a model's training progress without leaving their primary coding environment.

Software Developer

Integrates AI-powered predictions directly into application logic by running sophisticated SQL from within their development workspace.

BI Analyst

Generates rapid business insights by executing SQL that combines years of historical sales data with a single, predicted future quarter's revenue forecast.

What Changes When You Connect

01 Predict outcomes directly in your workflow. Instead of running a prediction on an external dashboard, you use `execute_sql_query` to wrap the model call right into your standard SELECT statement, fetching predicted data instantly.

02 Audit everything at once. Use `list_databases` to verify every single source feeding into your system—whether it's Snowflake or PostgreSQL—without manual console work.

03 Monitor ML status hands-free. Check which algorithms are ready for use by calling `list_models`, so you don't have to guess if a model is still training or fully deployed.

04 Stay connected to the core system. Run `get_status` anytime to confirm your MindsDB environment is healthy and running the correct version, eliminating guesswork about connectivity.

05 Build complex data pipelines easily. Use `list_views` to see all the virtual mappings that simplify messy source data into clean tables for analysis.

Real-World Applications

Forecasting next quarter's sales

A BI Analyst needs to know if their current inventory levels can support a 15% growth projection. They ask the agent to run SQL: `SELECT * FROM mindsdb.sales_forecaster WHERE region = 'West'`. The tool runs the prediction and returns not just historical sales, but the predicted revenue for next quarter.

Troubleshooting data flow

A Software Developer finds that a new feature is failing due to an unknown dependency. They use `list_databases` first to see every connected source and then run `get_status` to confirm the cluster's version, quickly isolating if the issue is internal or external.

Training on demand

A Data Scientist needs a new predictor for customer churn. Instead of running through a separate ML CLI tool, they use `execute_sql_query` to run a `CREATE MODEL ... PREDICT` command directly from the agent's chat prompt.

Auditing data integrity

An engineer needs to verify that their application is only reading from approved sources. They use `list_views` to see all proxy tables and then run `list_models` to ensure the correct, final version of the prediction engine is active.

Patterns to Avoid

Assuming model availability

✗ AVOID

The user tries to run a prediction query using an algorithm name they just heard about but haven't verified. The query fails with vague connection errors.

✓ INSTEAD

Before running any prediction, always use the `list_models` tool first. This confirms the exact names and status of all trained algorithms available for querying.

Ignoring data source scope

✗ AVOID

The user attempts to run a query that combines data from PostgreSQL and Snowflake without specifying both in the prompt, causing the agent to fail on schema resolution.

✓ INSTEAD

Use `list_databases` first. This confirms all available external sources are connected, letting you build complex queries that span multiple types of systems.

Overloading context memory

✗ AVOID

The user asks the agent to run a query with no limit clause on a large table (e.g., `SELECT * FROM big_sales`). The system hits a context overflow and fails.

✓ INSTEAD

When querying potentially massive tables, always wrap your logic using `execute_sql_query` and include an explicit `LIMIT N` statement to prevent context overloads.

The Right Fit

Use this MCP if your core workflow requires combining structured SQL data with predictive machine learning outcomes. If you're a developer or analyst who needs to ask 'What will happen?' while querying historical records, this is the tool for you. You must be comfortable writing SQL and understand the difference between raw data and trained models.

Don't use it if your only need is simple CRUD operations (Create, Read, Update, Delete) on a single database source. If you just want to pull a list of user IDs or names without running predictions, a basic standard database connector will suffice. This MCP adds the complexity and power of ML model execution directly into the query language.

The Pain Point: Jumping between dashboards to get a forecast.

Today, if you want to know what your sales might look like next quarter, you usually have to leave your main analytics tool. You copy the necessary data into an external ML platform, run the prediction there, then copy that result back into your dashboard—a process ripe for manual errors and wasted time.

With this MCP, that workflow collapses. You write a single SQL query using standard syntax but give it the power to predict outcomes live. Your agent executes the complex logic across multiple sources, returning only the finished insight.

MindsDB (AI Database & Predictors) MCP: Prediction in Plain View

The manual steps of exporting data, importing it into a separate ML environment, and then manually matching the results to your source records vanish. You no longer have to worry about which platform is talking to which.

You just ask for the insight. The agent handles the database connection, runs the model prediction via `execute_sql_query`, and presents you with the final answer.

MindsDB (AI Database & Predictors) with 6 Tools

These tools allow you to list connected databases, manage trained ML models, run complex predictive SQL, and check the health of your MindsDB environment.

#	TOOL	DESCRIPTION
01	`list_databases`	Lists all external databases connected through MindsDB to your instance.
02	`list_models`	Retrieves a list of trained AI tables (models) available within a specific project.
03	`get_model`	Fetches detailed information about an explicitly trained AI prediction engine.
04	`execute_sql_query`	Runs arbitrary SQL statements, allowing you to create models or run predictions within the MindsDB context.
05	`list_views`	Lists virtual data views and structural mappings used for complex data transformations.
06	`get_status`	Returns active cluster diagnostic information, confirming the current version and operational health of MindsDB.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U List all ML models in the 'mindsdb' project

I've retrieved your AI models from the 'mindsdb' project. Highlights include 'home_price_predictor' (Status: Complete), 'sales_forecaster' (Status: Training, 45%), and 'customer_churn_model'. Which one would you like to check the accuracy for?

U Execute SQL: SELECT price, price_explain FROM mindsdb.home_price_predictor WHERE sqft = 2500

Executing prediction query... The predicted price for a 2500 sqft home is $450,000. Explanation: The model heavily weighted the square footage and recent neighborhood sales trends. Would you like to run this prediction for a different set of features?

U Show me all connected databases in my MindsDB instance

I've identified 3 connected data sources: 'production_pg' (PostgreSQL), 'snowflake_warehouse' (Snowflake), and 'marketing_sheets' (Google Sheets). I can list the available tables for any of these sources if you'd like.

Frequently Asked Questions

01 **How do I check if my AI models are ready to use with MindsDB (AI Database & Predictors) MCP?**

You use the `list_models` tool. This shows you exactly which trained algorithms are available in your current project and whether they're still training or fully complete.

02 **Can I connect MindsDB (AI Database & Predictors) MCP to multiple types of databases?**

Yes, this MCP can list connections for various sources. You use the `list_databases` tool to see if your client supports everything from PostgreSQL to Snowflake.

03 **What is the difference between running an SQL query and using MindsDB (AI Database & Predictors) MCP?**

A standard SQL query reads existing data. Using this MCP lets you run predictions, meaning your query executes a calculation based on trained ML models, generating new, predicted data points.

04 **Is the MindsDB (AI Database & Predictors) MCP secure?**

The MCP manages connections to external sources like PostgreSQL and Snowflake. All actions are routed through your agent, allowing you to audit which data views are being accessed using `list_views`.

05 **Do I need to run a separate command line tool to use MindsDB (AI Database & Predictors) MCP?**

No. You interact with this entire system conversationally through your AI client, using the natural language interface that invokes the necessary tools.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"mindsdb-ai-database-predictors": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

MindsDB (AI Database & Predictors) is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by MindsDB (AI Database & Predictors). All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	MindsDB (AI Database & Predictors) MCP
Server ID	`019d75d4-f4d2-7351-8418-9ee045b83929`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/mindsdb-ai-database-predictors.