MCP SERVER | NO CODE | CLOUD HOSTED

# KnowBe4 (KMSAT) MCP

## Audit risk scores and training compliance data.

KnowBe4 (KMSAT Reporting) provides instant visibility into corporate security risk and training compliance. Connect this MCP to audit user enrollment, track phishing test results, and monitor individual and organizational risk scores across your entire employee base.

**A+** Quality Score 100/100

phishing-simulation | security-awareness | risk-assessment | compliance-training | user-auditing

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/knowbe4-kmsat-reporting

SCAN TO VIEW

# The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

# Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

# KnowBe4 (KMSAT Reporting) MCP

10 tools available
Cloud-hosted on Vinkius

Need a real-time picture of how secure your organization actually is? This MCP connects your AI agent directly to KnowBe4 KMSAT data. Instead of wading through dozens of dashboards, you can ask natural language questions about your security posture—and get specific answers back.

It lets you audit user enrollment status and check group assignments across different departments. You can track phishing tests, pulling out metrics like click rates or report rates to see if training is actually sticking. Furthermore, it gives you access to individual and organization-wide risk scores, helping you flag high-risk users immediately. If you're using Vinkius, this MCP lets your agent pull all that compliance data together, so you can audit training campaign progress against specific user groups and departments without ever leaving your AI client.

## Core Capabilities

**01 — Audit User Enrollment Status**

Get a list of every employee in the system along with their current enrollment status for mandatory training.

**02 — Track Phishing Test Performance**

Pull detailed results from past phishing simulations, including specific click rates and reporting statistics.

**03 — Assess Organizational Risk Scores**

Retrieve the overall account risk score and drill down to identify which individuals carry the highest security risks.

**04 — Review Training Compliance History**

Audit specific training campaigns to determine department-wide completion rates and compliance status.

**05 — Understand Group Policies**

List all defined user groups and see which assignments are currently active within the system.

## One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/knowbe4-kmsat-reporting** — connect your AI agent in three steps.

01 Subscribe to this MCP, then log into KnowBe4 and generate an API Key from the Account Settings > Reporting API section.

02 Input your unique key into the Vinkius configuration panel for this MCP.

03 Use natural language prompts in your AI client to query specific security metrics or user lists.

The bottom line is you can talk to KnowBe4's compliance data directly through your agent, instead of logging into multiple dashboards.

## Built For

Compliance Officers and Security Analysts need this. They spend too much time manually compiling reports on who failed which test or who hasn't completed required training. This MCP lets them automate the entire audit process.

**Security Analyst**

Runs weekly audits to correlate user risk scores with recent phishing failures, identifying immediate policy gaps.

**Compliance Officer**

Generates quarterly reports showing training completion rates across departments to prove regulatory adherence.

**HR Manager (Training Lead)**

Checks overall user enrollment status after a policy change, ensuring every employee is covered by the new mandatory module.

## What Changes When You Connect

01 Consolidate security metrics into a single chat session. Instead of jumping between user lists, test results, and compliance dashboards, your agent pulls all the required KnowBe4 KMSAT data instantly.

02 Pinpoint high-risk employees immediately. Use get_account_risk_score to find out which users are flagged with critical scores, allowing you to focus remediation efforts where they matter most.

03 Verify training coverage across departments. You can list_users and then use list_user_groups to confirm that specific user populations have the correct security policies applied.

04 Measure the effectiveness of simulations. By checking detailed results via get_phishing_test_details, you can quickly calculate true click-through rates and track improvements month over month.

05 Automate compliance reporting. You don't have to manually run list_training_campaigns every quarter; your agent gathers all necessary completion details for audit readiness.

## Real-World Applications

#### Identifying High-Risk Users After a Policy Change

A Security Analyst needs to know who in Finance failed the last phishing test and who also hasn't completed the new GDPR training. They prompt their agent: 'Show me all users with high risk scores who are in the Finance group and whose status is not complete for the GDPR module.' The agent uses get_account_risk_score, list_user_groups, and get_training_campaign_details to provide an immediate, actionable list.

#### Preparing for a Board Audit

A Compliance Officer needs to prove that 95% of employees completed the mandatory annual security training. They prompt: 'What is the completion rate for all users across Department X?' The agent calls list_users and then checks get_training_campaign_details, delivering a precise percentage ready for presentation.

#### Investigating Phishing Trends

The team noticed an uptick in credential harvesting attempts. A Security Analyst asks: 'What were the results of our last two phishing tests?' The agent uses list_phishing_tests and get_phishing_test_details to compare click rates, helping them prove if the recent training was effective.

#### Onboarding a New Department

An HR Manager needs to ensure an entire newly formed department is correctly assigned and trained. They prompt: 'List all users in the new Sales group and confirm their enrollment status for mandatory modules.' The agent uses list_users and list_user_groups to validate coverage instantly.

## Patterns to Avoid

### Using separate dashboards

✗ AVOID

Manually logging into the KnowBe4 UI, clicking 'Users,' downloading a CSV. Then logging into 'Reporting' and running a second report on 'Test Results.' Finally, opening an Excel sheet to combine them.

✓ INSTEAD

Connect this MCP. Ask your agent: 'Combine the user list with the results of the last two phishing tests.' The tool handles all the data fetching (list_users, get_phishing_test_details) and combines it for you in one conversation.

### Forgetting specific metrics

✗ AVOID

Running a general 'Compliance Report' but forgetting to filter out non-compliant users who are currently on leave.

✓ INSTEAD

Use the targeted tools. Start with list_users, then pair it with get_user_details or list_user_groups to filter down exactly to the population you need before auditing their training records.

### Asking for raw data without context

✗ AVOID

Getting a massive spreadsheet of every single test result and having no idea which metrics matter.

✓ INSTEAD

Ask your agent pointed questions: 'What was our click rate compared to last month's benchmark?' The agent calls list_phishing_tests and get_phishing_test_details, giving you the answer, not just a dump of numbers.

## The Right Fit

Use this MCP if your primary pain point is correlating distinct security datasets. For example, if you need to know: 'Are users with high account risk scores also failing compliance training?' This connector excels at linking user identity data (list_users) with behavioral metrics (get_phishing_test_details) and organizational policies (get_training_campaign_details). Don't use this if you only need a simple list of emails or a single, static report. If all you need is the current roster of users, a basic directory service connector will do. But when your job involves auditing *why* someone is at risk—connecting policy failure to user behavior—this MCP is essential.

## Auditing Security Compliance Used To Mean Hours in Spreadsheets

Today, checking organizational compliance feels like a scavenger hunt. You log into the main dashboard for roster status, download that data. Then you switch tabs to find phishing test results and download those metrics separately. Next, you open your HR platform to check group assignments and finally, you dump all three CSV files into Excel just to start manually cross-referencing which users failed what, and why.

With this MCP, the whole process is one conversation. You talk to your agent about compliance gaps—for example, 'Show me everyone in Group X who missed training Y.' The agent executes all the necessary data fetches (list_users, list_user_groups) behind the scenes. You get an instant, filtered answer without ever opening a spreadsheet.

# KnowBe4 (KMSAT Reporting) MCP Provides Actionable Risk Insights

Manual auditing requires you to run multiple reports and then manually correlate the scores. You have to compare the results from list_phishing_tests against the current risk score provided by get_account_risk_score, which is slow, error-prone, and never keeps up with real time.

Now, you ask the question once: 'Which users need immediate retraining?' The agent combines the data from all those sources into one clear report. You stop guessing where the risk is; you know exactly who needs help.

# KnowBe4 (KMSAT Reporting) with 10 Tools

Use these tools to retrieve specific data points, allowing your agent to build complex reports on security posture and compliance history.

| # | TOOL | DESCRIPTION |
|---|---|---|
| 01 | `list_users` | Retrieves a complete list of all users in KnowBe4 KMSAT for enrollment checks. |
| 02 | `get_user_details` | Pulls specific, detailed information about an individual user's account status. |
| 03 | `list_groups` | Provides a list of all organizational groups defined within KnowBe4 for policy review. |
| 04 | `list_phishing_tests` | Returns high-level details and names from recently conducted phishing security tests. |
| 05 | `get_phishing_test_details` | Gets the full, detailed results for a specific phishing test instance. |
| 06 | `list_training_campaigns` | Lists all available security awareness training campaigns to audit compliance scope. |
| 07 | `get_training_campaign_details` | Retrieves the specific completion and progress details for a chosen training campaign. |
| 08 | `list_phishing_store_results` | Lists results related to items found within the phishing store catalog. |
| 09 | `get_account_risk_score` | Retrieves the overall, aggregated risk score for the entire KnowBe4 account. |
| 10 | `list_user_groups` | Lists all user groups assigned to a particular individual. |

# See It in Action

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

**U** Show me the overall risk score for my KnowBe4 account

The aggregated risk score for your account is currently 42.5 (Medium). This is based on phishing performance, training completion, and overall user behavior.

**U** List the results of our last phishing simulation

Retrieving results for the latest simulation: 'Q1 Compliance Check'. Results: 5% Click Rate, 85% Report Rate, and 0 Data Entry incidents. This is a significant improvement from last month.

**U** Which users have the highest risk scores?

I've identified 5 users with a High Risk Score (>80). These users have failed multiple phishing tests recently. Would you like to see the list and their departments?

# Frequently Asked Questions

01 **How do I check if a user completed mandatory training using KnowBe4 (KMSAT) MCP?**

You can use list_training_campaigns to find the right module, and then get_training_campaign_details to see individual progress. This verifies compliance status quickly.

02 **Can I get the current organizational risk score with KnowBe4 (KMSAT) MCP?**

Yes, you use get_account_risk_score. It gives you a single number that aggregates all security performance data for your entire account.

03 **What does list_users do in the KnowBe4 (KMSAT) MCP?**

list_users pulls a comprehensive roster of everyone in your system, including their ID, name, and current enrollment status, which is vital for initial audits.

04 **Does this MCP help me compare phishing results across groups?**

Yes. You can use list_groups to identify the group boundaries, and then correlate that with get_phishing_test_details to see if specific departments performed differently during a test.

05 **Is KnowBe4 (KMSAT) MCP better than manual reporting?**

It's vastly superior. Manual reports are static and require stitching together data from multiple sources; this MCP provides real-time, conversational analysis of the same metrics.

# 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 `"knowbe4-kmsat-reporting": { "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

# KnowBe4 (KMSAT Reporting) 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 KnowBe4 (KMSAT Reporting). 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 | KnowBe4 (KMSAT Reporting) MCP |
| Server ID | `019d75c2-3369-732e-9484-9d3ef750c57e` |
| 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/knowbe4-kmsat-reporting.