

MCP SERVER

NO CODE

CLOUD HOSTED

BOSSDesk MCP for AI Agents

Track service requests and manage IT assets from any conversation

BOSSDesk connects your IT Service Management (ITSM) account directly to your AI agent. It lets you manage everything from tracking service tickets and finding specific assets, to querying user directories—all without opening the BOSSDesk portal.

A+ Quality Score 100/100

itsm

asset-management

incident-reporting

service-desk

it-operations

ticket-tracking



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

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

Firewall & DLP

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

Agent Activity

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

Tool Health

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

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.

BOSSDesk MCP

10 tools available

Cloud-hosted on Vinkius

Need to handle complex IT requests but hate switching between dashboards? This MCP plugs your entire BOSSDesk ITSM environment into your natural conversation flow. Your AI agent handles the heavy lifting: you can ask it to list all open tickets, find out who owns a specific laptop by serial number, or check an employee's profile—and it just does it.

If you're already using Vinkius for other APIs, adding BOSSDesk keeps your IT operations management in one place. You tell your agent what needs fixing, and it interacts with the system to create new tickets, update notes, or even verify if an asset is still assigned to a user. It turns complex, multi-step service workflows into simple chat commands.

Core Capabilities

01 — Create New Support Tickets

Instantly generate a new support ticket and file it under the correct department.

03 — List All Tickets and History

Fetch a list of all support tickets, including detailed history and who originally filed the request.

05 — Check User Directory Info

Pull specific profile data for any employee, like department or manager name.

02 — Query Asset Details

Look up specific hardware or software assets using serial numbers or asset IDs.

04 — Update Ticket Statuses

Change an existing ticket's details or add public notes directly from your agent conversation.

06 — Inventory Physical Locations

Get a list of all registered office sites and their details.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/mcp/bosssdesk — connect your AI agent in three steps.

- 01 Subscribe to the BOSSDesk MCP on Vinkius.
- 02 Enter your required API Token and Subdomain credentials into your AI client settings.
- 03 Start talking to your agent. You can then ask it to list tickets, check assets, or update user records.

The bottom line is you never have to open the BOSSDesk web portal again just to get basic IT service information.

Built For

This MCP serves anyone who lives in the intersection of tech support and operations. It's for Help Desk Technicians drowning in ticket dashboards, System Admins tracking hardware inventory across multiple sites, or IT Managers needing a quick overview without logging into the main portal.

Help Desk Technician

Needs to quickly check user details and list open tickets straight from their workflow tools while talking to an end-user.

System Administrator

Must verify asset metadata, like warranty expiration or serial numbers, without navigating the complex asset management screens.

IT Manager

Wants to run high-level reports by listing all physical office locations and checking ticket queues in natural language conversation.

What Changes When You Connect

- 01 No more clicking through tabs. You can list all tickets or find specific asset details just by asking your agent a question.
- 02 When you need to update information, using the `update_ticket` tool means changing status or adding notes without logging into a dashboard.

-
- 03 Quickly get user context. The `get_user` capability lets your agent check an employee's profile instantly when resolving a case.

 - 04 `list_assets` gives you an immediate inventory overview, letting you verify if equipment exists and who it belongs to—all in plain text responses.

 - 05 Write notes directly into the record using `add_ticket_note`, keeping high team visibility on every case without manual updates.
-

Real-World Applications

A new employee needs a laptop and desk setup

Instead of opening multiple forms, you ask your agent to check asset availability (`list_assets`) and then use `create_ticket` to file the request. The agent handles the entire ticket lifecycle from discovery to submission.

A user reports a broken monitor at their remote site

You tell your agent the issue, and it uses `get_user` to find out who is assigned that asset, then uses `add_ticket_note` on the existing ticket with next steps.

IT Manager needs a headcount of all managed sites

You prompt your agent to list all physical office locations (`list_locations`). The tool pulls the data and presents it immediately, saving you from navigating complex geographical reports.

Patterns to Avoid

Treating the MCP like a simple database query

✗ AVOID

Asking the agent only to 'list all users' without specifying parameters. The response might be overwhelming and unusable.

✓ INSTEAD

Always refine your request. Instead of just listing, ask the agent to use `get_user` for a specific person, or combine `list_users` with a filter like department.

Trying to edit assets outside of tickets

X AVOID

Assuming you can change an asset's status just by mentioning it. The system needs proper context.

✓ INSTEAD

If you need to update an existing ticket, always use ``update_ticket`` or ``add_ticket_note``. Never assume a direct modification capability without using the appropriate tool.

Ignoring asset assignment details

X AVOID

Just getting a list of assets and assuming who they belong to. The data needs context.

✓ INSTEAD

Use ``get_asset`` with an ID, which will include detailed information on current assignment status and assigned user.

The Right Fit

Use this MCP if your primary need is integrating complex ITSM actions—like creating records or updating ticket statuses—directly into a conversational workflow. You want your agent to act as an immediate, hands-on help desk technician. Don't use it if you only need simple read access; for instance, if all you need is the list of users, a basic directory API might suffice. However, if you need to combine listing tickets (`list_tickets`) with updating notes (`add_ticket_note`), this MCP is necessary.

BOSSDesk MCP: Automating IT Incident Reporting via AI Agents

Currently, reporting an incident requires multiple clicks. You have to log into BOSSDesk, find the 'Create Ticket' button, fill out required fields like asset ID and user name, select a category from dropdowns, and then hit submit. This manual process is slow and prone to skipping necessary context.

With this MCP, you simply tell your agent what happened—for example, 'My desk projector isn't turning on.' The agent handles the rest: it uses `create_ticket` in the background, correctly populating all required fields and ensuring no critical step is missed. You just get confirmation that the ticket was filed.

BOSSDesk MCP: Managing IT Asset Inventory with AI Agents

Tracking assets today involves opening the asset portal, filtering by location or user name, and manually cross-referencing serial numbers against purchase orders. If you need to know if an old laptop is still in use, it's a multi-step investigation.

Now, you can ask your agent directly: 'What's the status of the Dell XPS 15 with serial number XYZ123?' The agent uses `get_asset` and provides a single, definitive answer about its assignment, location, and warranty date. It cuts out all the filtering and searching.

BOSSDesk: 10 Tools for IT Support and Asset Management

Use these tools to create tickets, list all users, check asset details, and update records without ever opening the BOSSDesk web portal.

#	TOOL	DESCRIPTION
01	<code>add_ticket_note</code>	Appends a public or private comment directly to an existing support ticket.
02	<code>create_ticket</code>	Generates and submits a brand new IT support ticket into the system.
03	<code>get_asset</code>	Retrieves detailed specifications for one specific piece of equipment using an ID or serial number.
04	<code>get_ticket</code>	Fetches the full history and details for a single, specified support ticket.
05	<code>get_user</code>	Pulls specific profile information about an employee from the directory.
06	<code>list_assets</code>	Provides a comprehensive list of every hardware and software asset managed by the company.
07	<code>list_locations</code>	Lists all physical office or site locations registered in the system.
08	<code>list_tickets</code>	Returns a summary list of all open and closed IT support tickets.
09	<code>list_users</code>	Generates a directory listing containing basic information for every system user.
10	<code>update_ticket</code>	Modifies the status or core details of an already existing ticket.

See It in Action

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

U Can you list my open tickets and find details on ticket 102?



Open Tickets Summary

- Broken Printer (ID: 102) - Status: Waiting for Parts
- New Laptop Request (ID: 105) - Status: Pending Approval

Details for Ticket 102:

The printer issue is confirmed. The initial report mentioned the network connection failing, but a note added today confirms it's likely due to driver incompatibility. Parts ETA: next Tuesday.

U I need the user profile and all assets assigned to John Doe.



User Profile: John Doe

- Department: Marketing
- Manager: Jane Smith
- Email: john.doe@company.com

Assigned Assets:

- Laptop (ID 502): Dell XPS 15, Assigned Status: In Use. Warranty ends in 6 months.
- Monitor (ID 311): Samsung Curve, Assigned Status: In Use. Last serviced: Yesterday.

U Add a note to ticket 102 saying we ordered the replacement hardware.



Success: Note added to Ticket ID 102.

The new private note reads: 'Hardware ordered, tracking number ABC789. Expected delivery date: Oct 3rd.' The ticket status has been updated to 'Waiting for Parts,' keeping all team members informed.

Frequently Asked Questions

01 How does the BOSSDesk MCP help me manage tickets without logging into my portal?

It lets your agent handle ticket creation, status updates, and notes using natural conversation. You get full workflow control over your service requests directly from your chat window.

02 Can I use the BOSSDesk MCP to track physical office locations?

Yes, you can list all registered sites across the organization. This is useful for knowing where specific assets might be located or planning regional rollouts.

03 What if I need details on a user's profile using BOSSDesk MCP?

You just ask your agent to fetch the user record. It pulls accurate data like department, manager, and contact info right into your conversation thread.

04 Is the BOSSDesk MCP only for listing things?

No, it's much more than that. You can create new tickets, update existing ones, and add notes to maintain a complete record of every interaction.

05 Does this MCP handle inventory tracking for hardware assets?







Absolutely. It lets you list all managed IT assets and pull specific details—like serial numbers or warranty status—for any single item you need to check.

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 <code>"bosssdesk": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

BOSSDesk 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](https://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 BOSSDesk. 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	BOSSDesk MCP
Server ID	019d7561-7525-7197-8660-078c9088670b
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/bosssdesk.