

MCP SERVER

NO CODE

CLOUD HOSTED

Authorize.net MCP for AI Agents

Manage E-Commerce Payments, Refunds, and Transaction Settlements

Authorize.net lets your AI agent manage every step of your e-commerce payment flow. You can process sales, initiate refunds on settled transactions, hold funds before shipping, and audit nightly batch settlements directly through conversation.

A+ Quality Score 100/100

payment-gateway

merchant-services

transaction-settlement

pci-compliance

cim-profiles

refund-management



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.

Authorize.net MCP

10 tools available

Cloud-hosted on Vinkius

This MCP connects your Authorize.net gateway to any compatible AI client, letting you run complex financial logic without logging into a clunky merchant dashboard. Think of it as having an expert payment processor sitting right inside your chat window.

You can manage the full payment lifecycle: instantly running 'Auth & Capture' for immediate sales, or using 'Auth Only' to hold funds temporarily while products ship. If a customer returns an item, you simply command a refund on previously settled transactions or void pending charges. It also lets you build and manage secure Customer Information Profiles (CIMs), linking card data without exposing raw account numbers.

When it comes time for reconciliation, the MCP queries detailed records for single transaction IDs or maps out everything that's still unsettled before batch processing runs. By connecting this Authorize.net connector through Vinkius, your AI agent handles daily financial anomalies and complex payment logic using nothing but pure dialogue.

Core Capabilities

01 — Run full sales cycles

Execute immediate charges or place temporary holds on customer funds for later capture.

03 — Process refunds and voids

Issue refunds for charges already settled, or void pending transactions that need cancellation before batching.

02 — Manage secure card records

Build and retrieve Customer Information Profiles (CIMs) by securely adding payment cards to existing customer accounts.

04 — Audit transaction data

Retrieve detailed information about any specific transaction ID or list all unsettled items waiting for nightly settlement.

One Click on Vinkius — From Prompt to Execution

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

- 01 Subscribe to this MCP and provide your Authorize.net Login ID, Transaction Key, and necessary environment mappings.
- 02 Connect the MCP within your preferred AI client (Claude, Cursor, etc.).
- 03 Directly ask your agent to perform a task, such as 'Refund transaction 719200' or 'List unsettled items for today'.

The bottom line is, you use conversational commands within your AI client to execute payment functions that normally require logging into the Authorize.net web portal.

Built For

This MCP is for e-commerce operations staff and financial analysts who spend time manually reconciling payments, managing returns, or auditing settled batches. If your job involves tracking down why a payment failed or processing post-sale adjustments, this tool saves you hours of dashboard clicking.

E-Commerce Manager

Manages customer accounts by using the MCP to process refunds on returned items or set up new secure Customer Information Profiles.

Financial Operations Analyst

Runs daily audits, querying for specific transaction details or listing all unsettled transactions before the nightly batch closes.

Sales Engineer

Verifies payment failure reasons—like AVS mismatch or CVV errors—by getting detailed reports on declined charges.

What Changes When You Connect

-
- 01 Execute complex payment logic conversationally: Use the `auth_capture_transaction` tool to process real funds instantly or use `auth_only_transaction` just to hold money before shipping.

 - 02 Secure customer data management: Create a new profile using `create_customer_profile`, then attach cards safely with `add_payment_profile` without handling raw, exposed PANs.

 - 03 Handle post-sale changes easily: Quickly refund settled sales via `refund_transaction` or cancel pending charges before they finalize with `void_transaction`.

 - 04 Deep auditing capabilities: Get full visibility by running `get_transaction_details` on any ID or using `get_unsettled_transactions` to prepare for batch closure.

 - 05 Streamline the payment process: The MCP lets your AI agent manage daily financial anomalies, eliminating the need to click through multiple web forms.
-

Real-World Applications

Customer returns an item months later

A customer initiates a return. Instead of manually finding and processing it in the dashboard, you ask your agent to 'Refund transaction 719200.' The MCP handles the necessary refund on the already settled charge.

Pre-shipping payment hold

You need to reserve money for a large order but don't want to charge it yet. You tell your agent to run ``auth_only_transaction``, placing the temporary hold, which you can later finalize with ``prior_auth_capture``.

Checking why a credit card payment failed

A sales engineer needs to know if a decline was due to an AVS mismatch or CVV error. You ask your agent to run ``get_transaction_details`` on the failure ID, getting precise compliance information instantly.

End-of-day reconciliation

Before closing the books, you ask the agent to 'List all unsettled transactions.' The MCP immediately retrieves a list of pending items that need to be voided or processed for batching.

Patterns to Avoid

Treating payments as simple data reads

X AVOID

Trying to just 'get' payment details when the money is actually involved. You might pull a transaction ID, but without action, you can't reverse or finalize anything.

✓ INSTEAD

If you need to change the state of money, use specific actions like ``refund_transaction`` for settled sales, or ``void_transaction`` for pending charges. Never just read; always act.

Ignoring CIM security protocols

X AVOID

Storing raw card numbers in plain text files instead of a secure gateway profile. This is an immediate PCI compliance risk.

✓ INSTEAD

Always use ``create_customer_profile`` and ``add_payment_profile``. The MCP handles linking sensitive data to isolated, compliant profiles.

Forgetting the settlement cycle

X AVOID

Attempting to void a transaction that has already gone through the full batch process. The money is out of reach.

✓ INSTEAD

Always check first by calling ``get_unsettled_transactions``. If it's settled, you must use ``refund_transaction``; if it's pending, you can use ``void_transaction``.

The Right Fit

Use this MCP if your core process involves managing the lifecycle of funds—meaning you handle sales, returns, holds, and daily batch reconciliation. If you only need to view basic historical reports without the ability to change status (like voiding or refunding), a read-only accounting tool will suffice. However, if you regularly encounter payment failure reasons, need to manage secure customer profiles, or must track unsettled items before close of business, this Authorize.net MCP is essential. Don't use it if your system only handles non-monetary data like shipping addresses; stick to a dedicated CRM connector for that.

Handling Refunds and Settlements with Authorize.net MCP

Right now, processing a return means logging into the gateway dashboard, searching for the original transaction ID, verifying the details, and then manually initiating a refund. This process involves copy-pasting multiple IDs and navigating several compliance screens.

With this MCP, you simply ask your agent: 'Refund \$50 on transaction 719200.' The agent handles all the necessary inputs—the original ID, the amount, and the card data—and executes the refund instantly. You get immediate confirmation that the funds are back on the customer's end.

Building Secure Customer Profiles with Authorize.net MCP

Without this tool, every time a new client makes a purchase, you have to manually input and store their card details into an internal system, which is complex, risky, and requires dedicated PCI compliance overhead.

This MCP solves that by letting your agent securely build the customer's record using `create_customer_profile` and link cards via `add_payment_profile`. Your data stays isolated and compliant; you just get a clean confirmation that the profile is ready for future use.

10 Authorize.net Tools for E-Commerce Payment Management

Use these tools to handle payments, build customer profiles, refund charges, and audit every transaction detail using your AI agent.

#	TOOL	DESCRIPTION
01	<code>add_payment_profile</code>	Attaches a new payment card to an existing customer record (CIM profile).
02	<code>auth_capture_transaction</code>	Performs the full process: authorizing funds and immediately capturing them in one go.
03	<code>auth_only_transaction</code>	Places a temporary hold on a credit card, reserving funds without completing the sale.
04	<code>prior_auth_capture</code>	Finalizes a previously authorized transaction by capturing the reserved funds.
05	<code>create_customer_profile</code>	Generates an isolated Customer Information Manager (CIM) profile for storing payment details securely.
06	<code>get_customer_profile</code>	Retrieves all stored details associated with a specific customer's CIM profile.
07	<code>get_transaction_details</code>	Fetches comprehensive details for any single transaction ID from the gateway.
08	<code>get_unsettled_transactions</code>	Lists all transactions that are currently pending and haven't been included in the nightly batch closure.
09	<code>refund_transaction</code>	Issues a refund for any transaction that has already successfully settled.
10	<code>void_transaction</code>	Cancels an unsettled payment charge before it can be included in batch processing.

See It in Action

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

U What were all the transactions that didn't settle last night?



Unsettled Batch Report

The system found 4 items waiting for closure. These need review before batch processing runs:

- 91230 : \$15.99 (Auth Only, pending void check)
- 6001293 : \$104.50 (Settled, but requires manual refund confirmation)
- 719200 : \$25.99 (Auth Capture, status: Settled Successfully)
- 800045 : \$5.00 (Pending Void Check)

U Can you process a full refund for the order from yesterday?



Refund Initiated

✓ Success: The request to refund \$129.99 for transaction ID 6001293 was processed successfully.

The funds will be returned to the original payment method within standard banking intervals. Please note that this action is irreversible and final.

U What happened with card ending in 4567?



Customer Profile Lookup

• **Profile Status:** Active

Last Card Used: Visa *4567 (Added on 2026-06-12)

• **Recent Activity:** The last transaction was an Auth Capture for \$89.00, which successfully settled yesterday.

Frequently Asked Questions

01 How can I manage refunds using the Authorize.net MCP?

You simply tell your agent to refund a specific transaction ID, providing the amount and original card details. The MCP handles communicating with Authorize.net to finalize the money transfer back to the customer's card.

02 Does this MCP help me track unsettled payments?

Yes, you can ask your agent for a list of all transactions that are currently pending batching. This gives you a systematic view of everything that needs reconciliation before the day closes.

03 Can I save payment details securely with this MCP?

Absolutely. You use the tools to create dedicated Customer Information Profiles (CIMs). The MCP handles linking sensitive card data to isolated, compliant profiles without you handling raw numbers.

04 How do I authorize funds without charging them yet?







You direct your agent to perform an 'Auth Only' transaction. This places a temporary hold on the money, allowing you time to ship goods before running the final capture command.

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>"authorizenet": { "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

Authorize.net 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 Authorize.net. 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	Authorize.net MCP
Server ID	019d7555-aa9e-7159-bf63-f8d985704827
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/authorizenet.