MCP SERVER | NO CODE | CLOUD HOSTED

Password Generator API MCP

Automate High-Entropy Credential Creation and Auditing

Password Generator API MCP generates high-entropy, cryptographically secure passwords on demand. It lets your AI agent audit credential strength against custom rules, checking for specific character sets and calculating entropy levels automatically. Stop relying on weak manual generators; start enforcing real security standards instantly.

A+ Quality Score 100/100

password-generation | cryptography | security-best-practices | entropy | credential-management

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/password-generator-api

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.

Password Generator API MCP

2 tools available
Cloud-hosted on Vinkius

Generating strong credentials used to be a multi-step nightmare. You needed a password that met length requirements, contained symbols, and had high entropy—all while making sure it wasn't easily guessable. With this MCP, your AI agent handles the whole process. Instead of manually juggling multiple generators or asking a team member for a temporary key, you simply ask your agent to create credentials based on specific security policies.

It checks far more than just length; it audits the complexity and entropy of the password against established organizational standards. Whether you're setting up new infrastructure access or running compliance audits, your agent acts like an embedded security consultant. You connect this service through Vinkius, giving any compatible AI client the ability to perform complex credential generation and auditing right in the middle of a conversation. You get robust, verifiable passwords instantly.

Core Capabilities

01 — Generate credentials with custom constraints

The MCP creates highly secure passwords that match specific requirements for length, characters, or complexity.

02 — Verify service operational status

You check the API to confirm that credential generation is currently active and ready for use.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/password-generator-api** — connect your AI agent in three steps.

01 Subscribe to this MCP and enter your Apify API Key into your AI client.

02 Your agent initiates a request, specifying the required password length and character constraints (e.g., 'must include symbols and uppercase letters').

03 The system returns a unique, high-entropy password along with metadata confirming its security strength.

The bottom line is that you get cryptographically strong credentials automatically generated and audited without leaving your chat interface.

Built For

This MCP is essential for Security Analysts, DevOps Engineers, and Compliance Officers who are tired of manual credential testing. If your job requires enforcing strict security policies or auditing infrastructure access, this tool saves hours of repetitive work.

Security Analyst

Runs mandatory password audits by asking the agent to generate test credentials that meet specific internal entropy and character set rules.

DevOps Engineer

Automates the creation of temporary, complex service accounts for testing new infrastructure access points without manual key generation.

Compliance Officer

Performs rapid security audits by verifying that newly created credentials adhere to industry best practices regarding character type and minimum length.

What Changes When You Connect

01 Stop guessing password requirements. You can enforce strict policies, requiring combinations of numbers, symbols, and case sensitivity when you use generate_secure_password.

02 Boost your audit confidence by getting real entropy metadata with every generated credential. This goes beyond just checking the length.

03 The API status check tool lets your agent verify that the service is active before running a critical security task, preventing workflow interruptions.

04 You eliminate manual key generation entirely. Your agent handles the entire process from defining constraints to delivering the final secure password.

05 This MCP allows you to use complex security data—like cryptographic strength measurements—within natural language conversations.

Real-World Applications

Auditing a new application's access keys

A Security Analyst needs to test if the default passwords for three newly provisioned services meet corporate policy (18 chars, symbols required). Instead of logging into each system manually, they prompt their agent: 'Generate secure passwords for three accounts using generate_secure_password with 18 characters and symbols.' The agent provides all three, complete with entropy scores.

Validating DevOps testing credentials

A DevOps Engineer is setting up a staging environment and needs to create temporary, unique access keys for integration tests. They use the agent's ability to generate secure passwords repeatedly, ensuring every test account has a high-entropy key without ever touching a manual generator.

Quickly checking security tool availability

Before starting an audit session, a Compliance Officer wants to confirm that the password generation service is working. They simply ask their agent to check_api_status and get instant confirmation it's fully operational.

Defining complex password policies in plain language

A manager needs to document a new policy: 'Passwords must be 16 characters long, include numbers and symbols.' Instead of writing a technical spec, they ask their agent to generate_secure_password with those exact constraints, demonstrating the required complexity.

Patterns to Avoid

Relying on simple online generators

✗ AVOID

Using a basic password tool that only allows random character sets and doesn't calculate or report entropy.

✓ INSTEAD

Use the generate_secure_password tool. It calculates real cryptographic entropy, giving you proof of strength needed for compliance reporting.

Ignoring service health checks

✗ AVOID

Starting a major audit workflow only to find out halfway through that the generation API is temporarily down or misconfigured.

✓ INSTEAD

Always start by running check_api_status. This verifies the entire security research workflow is operational before you write a single prompt.

Mixing up password policies

✗ AVOID

Trying to remember if the policy requires 14 characters or 16, and accidentally generating credentials that don't match the current rule.

✓ INSTEAD

Be explicit. Tell your agent exactly what you need: 'Generate a secure password using generate_secure_password with length 16 and symbols.' The tool enforces the constraint.

The Right Fit

Use this MCP if your core job involves generating, auditing, or verifying high-entropy credentials. If compliance requires proof of cryptographic strength (entropy), you need this. It's perfect for roles that build secure access systems, like DevOps and Security Analysis. Don't use it if you just need general information retrieval; don't ask the agent about network topology—that's outside its scope. Also, don't use it if you only need to list existing passwords

(it can only generate them). If your goal is simply writing documentation on security best practices, this MCP won't help. It deals with the *data* itself, not the surrounding text.

Security audits and credential management used to be a manual headache.

Today, if you need credentials for an audit or a new system, you're usually copying and pasting into three different dashboards. You check the length in one place, verify character sets in another, and then you manually run a separate entropy checker. It’s tedious, prone to copy-paste errors, and it takes way too long.

With this MCP, your agent handles all that complexity inside a single conversation. You simply tell your agent what the security policy is —'I need 18 characters, including symbols.' The agent generates the password *and* provides the full entropy report in one go. It just works.

Generate high-entropy passwords with generate_secure_password.

Before this, defining a secure credential meant juggling multiple tools and keeping track of specific character type rules across various spreadsheets. You were always playing catch-up just to ensure the password was compliant enough for audit purposes.

Now you can automate that entire process. The generate_secure_password tool makes your agent a real-time security consultant, ensuring every credential is robust and precise without any manual intervention.

Password Generator API with 2 Tools

These tools let you check the operational status of the service or generate brand new, cryptographically strong credentials based on specific security parameters.

#	TOOL	DESCRIPTION
01	`check_api_status`	Checks if the password generation service is currently online and running properly.
02	`generate_secure_password`	Creates a high-entropy, unique password based on parameters you define (length, characters).

See It in Action

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

U Generate a 20-character secure password using Password Generator API.

I've generated a 20-character secure password for you! It is currently identified as: `[Password]`. It features a high level of entropy for maximum security. Would you like me to generate another one with different constraints?

U Generate a password with numbers and symbols, length 16.

I've retrieved a secure password matching your requirements! It is identified as `[Password]`. I can provide the entropy metadata to assist you with a deep-dive security audit of this credential.

U Check the status of the Password Generator service.

I've checked the status of the Password Generator service! It is currently identified as 'active' and fully operational. I can assist you with high-entropy credential generation for your security projects.

Frequently Asked Questions

01 **How does the Password Generator API use entropy?**

The API calculates the cryptographic strength of a password (entropy) and reports it to you. This gives you a measurable score, proving how difficult or impossible the password is to guess.

02 **Can I check_api_status multiple times with Password Generator API?**

Yes. You can run check_api_status repeatedly through your agent. This allows you to build automated checks into a larger security research workflow.

03 **What if my password requirements change mid-audit using Password Generator API?**

You just tell the agent the new rules in natural language. The agent will then use generate_secure_password to create a brand new credential matching the updated constraints.

04 **Does this MCP handle passwords for different types of accounts?**

Yes, it generates credentials based on your specified requirements, making it suitable for service accounts, user logins, or temporary access keys.

05 **Is the password generated secure enough for production use with Password Generator API?**

The tool is designed to generate high-entropy passwords that meet modern cryptographic security standards. You always get metadata confirming its strength level.

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 `"password-generator-api": { "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

Password Generator API 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 Password Generator API. 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	Password Generator API MCP
Server ID	`019d846a-0d8c-709f-a94c-c14727143c34`
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/password-generator-api.