

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Account Recovery Readiness Audit MCP

Find and fix vulnerabilities in your account recovery setup.

Account Recovery Readiness Audit MCP lets your AI client inspect how prepared a user is for account lockout scenarios. It analyzes recovery vectors like email, phone, and hardware keys to find critical security gaps. You can use it to score readiness or compare current settings against a target security profile to ensure you have enough redundancy.

A+ Quality Score 100/100

security

audit

recovery

account-safety

risk-assessment



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.

Account Recovery Readiness Audit MCP

4 tools available

Cloud-hosted on Vinkius

You can't fix what you haven't measured. This MCP gives your AI agent the ability to look under the hood of user security profiles to see if they'll actually be able to get back into their accounts if things go wrong. Instead of guessing if a user has enough backup methods, you can run a precise audit. It looks at the specific recovery vectors currently in place, such as hardware keys or backup codes, and flags where the setup is too thin. You can use it to calculate the exact gap between a user's current state and a hardened security standard. It's a direct way to move from vague security assumptions to a quantified readiness score. Whether you are checking a single account or comparing profiles against a strict target, this tool provides the data needed to prioritize which recovery factors to add next.

Core Capabilities

01 — Readiness Scoring

Your agent uses this to assign a numerical value to an account's ability to recover from lockout.

02 — Gap Analysis

Your agent compares current user settings against a desired security standard to find missing pieces.

03 — Factor Inventory

Your agent pulls a list of all recovery methods currently tied to a user profile.

04 — Requirement Lookup

Your agent checks the specific standards and characteristics required for different recovery types.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/account-recovery-readiness-audit — connect your AI agent in three steps.

- 01 Connect your MCP-compatible client to Vinkius.
- 02 Ask your agent to audit a specific user account.
- 03 The agent uses the MCP to pull recovery factors and calculate scores.
- 04 Review the identified gaps and missing requirements provided by the agent.

Connect your client to Vinkius to start running security audits through your agent.

Built For

Security professionals and system administrators use this to automate the assessment of user account safety.

Security Analysts

They hand off user profile data to the agent to identify high-risk accounts.

System Administrators

They use the tool to verify that account recovery policies are actually being met by users.

DevSecOps Engineers

They integrate these checks into automated workflows to monitor account security health.

What Changes When You Connect

- 01 Quantifies security gaps with numerical scores.
- 02 Identifies specific missing recovery factors like hardware keys.
- 03 Compares current user settings against strict security targets.

04 Provides a raw inventory of all active recovery methods.

Real-World Applications

Risk Assessment

Identify which users are most vulnerable to permanent account lockout.

Remediation Planning

Determine which recovery factors to suggest to a user based on their specific gaps.

Policy Enforcement

Check if a user's recovery setup meets the company's required security profile.

Security Auditing

Run regular checks to ensure recovery redundancy across a user base.

Patterns to Avoid

Guessing security strength

❌ AVOID

You ask your agent if a user's account is 'secure enough' without looking at their actual recovery methods.

✓ INSTEAD

Use `audit_account_readiness` to get a concrete evaluation of the account's current state.

Ignoring specific gaps

❌ AVOID

You assume a user is safe because they have MFA, but you don't know if they lack hardware keys.

✓ INSTEAD

Run `calculate_readiness_gap` to find the exact difference between their setup and your target profile.

Manual inventory checks

❌ AVOID

You try to manually cross-reference user settings against a list of required recovery types.

✓ INSTEAD

Let your agent pull the full list of active methods using `list_user_recovery_factors`.

The Right Fit

Security teams and system admins should connect this MCP if they need to quantify account lockout risks. If you only care about general security posture and don't need to measure specific recovery readiness, you don't need this. The decision comes down to whether you need a numerical gap analysis for recovery protocols.

Account Recovery Readiness Audit 4 Tools

These tools let your agent inspect user security profiles, inventory recovery methods, and measure the distance between current setups and your security standards.

#	TOOL	DESCRIPTION
01	audit_account_readiness	This tool evaluates a specific user account to determine its current readiness and identify security gaps.
02	calculate_readiness_gap	This tool compares existing recovery factors against a target security profile to quantify the remaining gap.
03	get_factor_requirements	This tool retrieves the standard definitions and required characteristics for every type of recovery factor.
04	list_user_recovery_factors	This tool provides a raw inventory of all recovery methods currently linked to a specific user.

See It in Action

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

Can you audit the readiness for account ID user_123?



The audit for user_123 shows a status of 'At Risk' with a score of 45. Missing factors include 'security_key' and 'backup_codes'. It is highly recommended to set up a hardware security key immediately.

What are the requirements for a security key factor?



A security key is a high-importance, high-risk factor that provides phishing-resistant, hardware-based authentication for account recovery.

Calculate the gap between these factors: ['recovery_email'] and ['recovery_email', 'backup_codes', 'security_key'].



The gap score is 2. The missing factors are 'backup_codes' and 'security_key'. You should prioritize adding a security key first.

Frequently Asked Questions

01 What can this MCP do?

This MCP audits user account security to see if they have enough recovery methods to prevent permanent logout.

02 How does it identify security gaps?

It compares the recovery factors a user actually has against a target security profile to find what is missing.

03 Which clients can I use with this MCP?

You can use this with any MCP-compatible client like Claude, Cursor, Windsurf, or VS Code.

04 Can I see a list of a user's current recovery methods?

Yes, you can use the tool to get a raw inventory of all recovery methods linked to a specific user.

05 Does this MCP host the data?

Vinkius hosts the MCP and manages the connection, so you can use it immediately after connecting your client.

06 What does the readiness score represent?

The score is a numerical value representing the strength of the recovery profile based on the diversity and security of configured factors.

07 How can I see which recovery methods a user has configured?

You can use the `list\_user\_recovery\_factors` tool to retrieve a raw inventory of all recovery methods currently linked to a specific account.

08 What is the difference between hard and soft recovery factors?

Hard factors, like Security Keys, provide autonomous, high-security recovery. Soft factors, like Recovery Email, rely on external infrastructure or human interaction.

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>"account-recovery-readiness-audit": { "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

Account Recovery Readiness Audit 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 Account Recovery Readiness Audit. 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	October 2026
MCP Server	Account Recovery Readiness Audit MCP
Server ID	01a0ee75-49df-7148-b703-799838643ba6
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/en/ai-agent-connect/account-recovery-readiness-audit.