

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

Collaborative Workspace Handoff MCP

Move digital workspaces between owners without losing control or security.

Collaborative Workspace Handoff MCP manages the messy process of moving digital workspaces from one owner to another. It helps your agent audit permissions, identify successors, and run through staged checklists to ensure no files or access rights are left in limbo during a transition.

A+ Quality Score 100/100

migration

workspace

ownership

permissions

checklist



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.

Collaborative Workspace Handoff MCP

4 tools available

Cloud-hosted on Vinkius

Moving a workspace to a new owner is usually a manual, error-prone headache. You have to track who has access, who is supposed to take over, and whether every file actually moved. This MCP turns that chaos into a structured process your AI client can manage for you. Instead of guessing if a migration is complete, you use your agent to run a full audit of current permissions and identify the right people to step into key roles. It breaks the transition down into logical stages like Role Succession, Permission Audit, and File/Asset Transfer. You can use it to verify that security gaps aren't created during the handoff and to generate a step-by-step checklist that keeps the migration on track. It's built to ensure that when an owner leaves, the workspace stays secure and functional for the next person in charge.

Core Capabilities

01 — Workspace Auditing

Your agent checks the current state and membership of a workspace.

02 — Security Gap Detection

The MCP identifies permission issues during a handoff.

03 — Succession Planning

Your agent identifies which users are ready to take over key roles.

04 — Staged Migration

The tool creates a step-by-step checklist for the transfer process.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/collaborative-workspace-handoff — connect your AI agent in three steps.

- 01 Connect your AI client to the Vinkius hosted MCP.
- 02 Ask your agent to get a summary of the target workspace.
- 03 Run a permission audit to find security gaps.
- 04 Identify successors for the necessary roles.
- 05 Generate a staged checklist to guide the final transfer.

Connect your client to Vinkius and start managing migrations through your agent.

Built For

This MCP is for teams managing digital assets and workspace ownership transitions.

IT Administrators

They use the MCP to audit permissions and ensure secure handoffs.

Project Managers

They use it to track the progress of workspace migrations via checklists.

Operations Leads

They use it to manage role succession when team members change.

What Changes When You Connect

- 01 Reduces manual errors in permission audits.
- 02 Provides a clear roadmap for ownership transfers.

03 Identifies potential security risks during transitions.

04 Automates the creation of migration checklists.

Real-World Applications

Employee Offboarding

Transfer workspace ownership from a departing employee to a successor.

Security Audits

Check for permission gaps before a major organizational change.

Departmental Restructuring

Move assets and permissions between different team groups.

Role Succession

Identify and prepare the next set of leaders for specific workspace roles.

Patterns to Avoid

Manual permission tracking

❌ AVOID

You try to keep a spreadsheet of every user and their access levels while an admin is leaving the company.

✓ INSTEAD

Let your agent run a full audit using ``audit_access_permissions`` to catch security gaps automatically.

Guessing successor readiness

❌ AVOID

You assume the next person in line has the right permissions to take over a workspace.

✓ INSTEAD

Use ``list_successor_roles`` to see exactly who is currently designated to step into key roles.

Unstructured migration attempts

❌ AVOID

You start moving files and changing owners without a clear plan, hoping you don't miss anything.

✓ INSTEAD

Run ``generate_handoff_checklist`` first to get a staged, sequenced list of every task required for the transfer.

The Right Fit

IT admins and operations leads should connect this MCP if they manage frequent team changes or departmental restructuring. If your workspace ownership is static and rarely changes, you don't need this. The deciding factor is whether your handoff process currently relies on manual checklists and human memory.

Collaborative Workspace Handoff Toolset

These tools handle the heavy lifting of auditing permissions, identifying successors, and building migration checklists.

#	TOOL	DESCRIPTION
01	generate_handoff_checklist	This tool creates a sequenced, staged checklist of every task needed to finish an ownership transfer.
02	list_successor_roles	Use this to find every person currently designated as a successor for key roles in the workspace.
03	audit_access_permissions	This tool evaluates current access restrictions to find security gaps during a transition.
04	get_workspace_summary	This tool provides a high-level overview of the current state of a specific workspace.

See It in Action

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

U Give me a summary of the workspace with ID 'ws-123'.



The workspace 'ws-123' is currently owned by Alice, has 5 members, 12 files, and the transfer status is pending.

U Who are the successors for the current roles in workspace 'ws-456'?



The designated successors for workspace 'ws-456' are Bob (Manager, readiness 0.9) and Charlie (Contributor, 0.7).

U Generate a handoff checklist for workspace 'ws-789' for the date 2025-12-01.



The handoff checklist for 'ws-789' has been generated. The current completion is 0%. Stages include Role Succession, Permission Audit, File/Asset Transfer, and Final Ownership Shift.

Frequently Asked Questions

01 What clients can I use with this MCP?

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

02 How does the checklist work?

The tool generates a sequenced list of tasks covering Role Succession, Permission Audit, File/Asset Transfer, and Final Ownership Shift.

03 Can I use this to find security risks?

Yes, the audit tool evaluates current access restrictions to find potential security gaps during a transition.

04 Do I need to host the MCP myself?

No, Vinkius hosts and manages the MCP for you. You just connect your client and start working.

05 What information can I get about a workspace?

You can get a high-level summary including ownership, member count, file counts, and current transfer status.

06 How do I start a workspace migration?

You can begin by using ``get_workspace_summary`` to understand the current state of the workspace and then call ``generate_handoff_checklist`` to receive the required sequence of tasks.

07 Can I audit security during the handoff?

Yes, the ``audit_access_permissions`` tool allows you to evaluate access restrictions and identify potential security conflicts during the transition.

08 What are the stages of the handoff checklist?

The checklist follows a strict sequence: 1. Role Succession, 2. Permission Audit, 3. File/Asset Transfer, and 4. Final Ownership Shift.

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>"collaborative-workspace-handoff": { "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

Collaborative Workspace Handoff 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 Collaborative Workspace Handoff. 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	September 2026
MCP Server	Collaborative Workspace Handoff MCP
Server ID	01a0dabe-7508-71b3-9580-43f888e66142
Platform	Vinkius Cloud for AI Agents
Endpoint	<code>https://edge.vinkius.com/{token}/mcp</code>

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/collaborative-workspace-handoff.