

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

Repair Access Arrangement MCP

Coordinate onsite repairs and technician visits through your AI agent.

Repair Access Arrangement MCP handles the logistics of onsite maintenance. It links your AI client to property access rules, technician availability, and site prep requirements. Your agent can check if a contact is authorized to grant entry, find open time slots, and generate full visit schedules and preparation checklists.

A+ Quality Score 100/100

repair

scheduling

access-control

technician

coordination



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.

Repair Access Arrangement MCP

4 tools available

Cloud-hosted on Vinkius

Managing onsite repairs usually involves a mess of scheduling conflicts and access issues. This MCP solves that by giving your AI agent direct access to the constraints that govern property visits. Instead of manually checking if a technician is free or if a specific person can let them in, you just ask your AI client. It checks technician availability against permitted access hours and verifies that the person requesting entry actually has the authority to do so. Once the details are cleared, your agent can build a complete visit plan. It also identifies exactly what needs to be done on-site before the technician arrives, like clearing a path to a meter or unlocking a gate. This moves the coordination work from manual back-and-forth messages into a single, automated flow within your existing AI workflow.

Core Capabilities

01 — Access Validation

Your agent checks if a contact has the right to grant entry to a specific location.

02 — Schedule Generation

The AI builds a complete visit plan including times and contact details.

03 — Availability Checks

Your client verifies technician openings against allowed property hours.

04 — Site Preparation

The agent retrieves specific tasks required to ready a site for a technician.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/repair-access-arrangement — connect your AI agent in three steps.

- 01
- Connect your preferred AI client to the Vinkius catalog.
- 02
- Ask your agent to check technician availability or access rules.
- 03
- The agent uses the MCP tools to pull real-time data.
- 04
- Your agent provides a confirmed schedule or a preparation list.

Connect your AI client to the Vinkius-hosted MCP to start managing repairs.

Built For

This MCP is built for professionals managing physical assets and maintenance workflows.

Property Managers

They hand off the coordination of tenant access and technician scheduling to the AI.

Maintenance Coordinators

They use the agent to verify site readiness and technician availability.

Facility Operators

They rely on the AI to ensure all access requests meet site-specific rules.

What Changes When You Connect

- 01
- Reduces scheduling errors by checking technician availability against property hours.
- 02
- Prevents unauthorized access by validating contact roles.
- 03
- Ensures technicians can work immediately by providing site prep checklists.

04 Automates the creation of visit schedules and contact plans.

Real-World Applications

Tenant Access Management

Your agent verifies if a tenant or manager can legally authorize a repair visit.

Technician Dispatching

The AI finds available time slots that align with property access windows.

Pre-Visit Readiness

The agent tells users exactly what to clear or unlock before a technician arrives.

Repair Scheduling

The AI generates a full contact and timing plan for a specific repair ID.

Patterns to Avoid

Assuming access is always open

❌ AVOID

You tell your agent to send a technician to a property at 2 PM without checking if the tenant is actually allowed to let people in.

✓ INSTEAD

Always use ``validate_access_eligibility`` first to confirm the contact has the authority to grant entry.

Ignoring site preparation needs

❌ AVOID

A technician arrives at a site only to find a locked gate or a blocked meter, wasting the entire appointment.

✓ INSTEAD

Run ``get_preparation_checklist`` before dispatching anyone to ensure the site is ready for work.

Scheduling without checking windows

❌ AVOID

You book a repair for a time when the property is closed or the technician is already busy.

✓ INSTEAD

Use ``check_slot_availability`` to match technician openings with the specific permitted access hours of the property.

The Right Fit

Property managers and maintenance coordinators should connect this MCP if they handle physical asset repairs. If your workflow doesn't involve coordinating onsite visits or managing tenant access, you don't need this. The deciding factor is whether you currently spend time manually verifying if a technician can actually get into a building.



4 Tools for Managing Repair Access and Scheduling

These tools handle the logic of technician availability, site readiness, and access permissions.

#	TOOL	DESCRIPTION
01	check_slot_availability	This tool confirms if a technician is available during the property's permitted access hours.
02	get_access_plan	This tool generates a finalized schedule and contact plan for a specific repair request.
03	get_preparation_checklist	This tool provides a list of tasks that must be completed before the technician arrives on-site.
04	validate_access_eligibility	This tool verifies if a specific contact role is permitted to grant access for a specific item location.

See It in Action

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

U Can you schedule a repair for repair-123 on 2025-05-10?



Your repair visit is confirmed for 2025-05-10 between 10:00 AM and 12:00 PM. The authorized contact is the Building Manager.

U What do I need to prepare for repair-456?



Please clear the path to the water meter and ensure the rear gate is unlocked before the technician arrives.

U Is there any technician availability at location-789 on 2025-06-01?



Yes, there are two available slots between 09:00 AM and 11:00 AM for that location.

Frequently Asked Questions

01 What can this MCP do for my property management business?

It automates the coordination of onsite repairs by managing technician schedules, access permissions, and site preparation tasks.

02 How does the MCP ensure a technician can actually get into a building?

It uses the `validate_access_eligibility` tool to check if a contact is authorized to grant entry and `check_slot_availability` to ensure the visit happens during permitted hours.

03 Can I use this with Claude or Cursor?

Yes, you can connect this MCP to any MCP-compatible client like Claude, Cursor, or Windsurf through the Vinkius platform.

04 Does it help with preparing the site for a technician?

Yes, the `get_preparation_checklist` tool provides specific tasks that must be completed before a technician arrives onsite.

05 Do I need to host the MCP myself?

No, Vinkius hosts and manages the MCP for you, so it is ready to use as soon as you connect your client.

06 How do I schedule a repair visit?

You can use the `get_access_plan` tool by providing the unique repair ID and your requested date to receive a confirmed schedule.

07 What should I do before the technician arrives?

Use the `get_preparation_checklist` tool with your repair ID to see the specific tasks required for your location.

08 Can I check if a specific person is allowed to grant access?

Yes, the `validate_access_eligibility` tool allows you to verify if a contact role is permitted to authorize access for a specific location.

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>"repair-access-arrangement": { "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

Repair Access Arrangement 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 Repair Access Arrangement. 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	Repair Access Arrangement MCP
Server ID	01a0eb97-f86c-7210-8d48-b38d57413541
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/repair-access-arrangement.