

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

Blue Light Mitigation Planner MCP

Fix your sleep schedule by managing light exposure.

Blue Light Mitigation Planner MCP gives your AI client the ability to build custom schedules that protect your circadian rhythm. It calculates your device risk, determines necessary screen-free windows, and suggests physical lighting changes to help you wind down effectively.

A+ Quality Score 100/100

blue-light

sleep

wellness

melatonin

circadian-rhythm



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.

Blue Light Mitigation Planner MCP

4 tools available

Cloud-hosted on Vinkius

If you spend your evenings staring at monitors or scrolling through phones, your sleep is likely taking a hit. This MCP helps you take control of your environment. Instead of guessing when to put the phone away, you can ask your AI client to build a specific plan based on your hardware and your intended bedtime. It looks at your specific device setup to see how much risk you're actually facing and then tells you exactly when to switch to blue light glasses or adjust your screen settings. You can even use it to audit your bedroom lighting to make sure your physical space isn't working against your sleep goals. It turns vague wellness advice into a concrete, actionable schedule you can follow every night.

Core Capabilities

01 — Risk Assessment

Your agent uses this to score the light exposure from your specific devices.

02 — Schedule Generation

Your agent builds a step-by-step timeline for wearing glasses and adjusting settings.

03 — Buffer Calculation

Your agent determines how long you need to stay off screens before sleep.

04 — Environment Auditing

Your agent suggests physical lighting changes for your room.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/blue-light-mitigation-planner — connect your AI agent in three steps.

- 01 Connect the MCP to your preferred client like Claude or Cursor via Vinkius.
- 02 Tell your agent about your intended bedtime and your device usage.
- 03 The agent uses the tools to calculate risk and buffer periods.
- 04 Receive a personalized schedule for glasses, settings, and lighting.

Connect the MCP to your client and start asking for sleep-related light management.

Built For

This is for anyone whose evening screen time is disrupting their sleep patterns.

Gamers

They hand off their hardware setup to the AI to get a nightly mitigation schedule.

Remote Workers

They use it to manage light exposure after a long day of monitor use.

Wellness Enthusiasts

They use the tools to optimize their circadian rhythm and sleep hygiene.

What Changes When You Connect

- 01 Calculates specific risk scores based on your actual hardware.
- 02 Provides exact timestamps for when to change device settings.
- 03 Identifies the necessary no-screen window for your specific needs.

04 Offers physical lighting adjustments to reduce light pollution.

Real-World Applications

Late Night Gaming

Get a plan that tells you exactly when to put on blue light glasses while playing.

Device Risk Check

See how much blue light your specific monitor and phone combo is emitting.

Bedroom Optimization

Find out how to change your LED lighting to better support sleep.

Bedtime Prep

Create a countdown to sleep that includes screen-free periods.

4 Tools Available

#	TOOL	DESCRIPTION
01	assess_device_risk	This tool calculates a cumulative blue light risk score for your specific hardware setup.
02	calculate_buffer_period	Use this to find the exact length of the no-screen window you need before bed.
03	generate_mitigation_plan	This tool creates a full schedule covering when to wear glasses and when to change device settings.
04	get_environment_optimization	This tool suggests specific changes to your physical room lighting to reduce light pollution.

See It in Action

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

U I want to go to sleep at 23:00. I'll be gaming on my laptop and scrolling on my phone. What should my plan be?



To prepare for your 23:00 bedtime, you should start wearing blue light blocking glasses at 20:00. Activate Night Shift on your laptop at 21:00. You must stop all screen usage by 22:15 to respect your buffer zone.

U How much blue light risk am I facing if I use a desktop monitor and a smartphone in the evening?



Your risk score is high due to the combination of a desktop monitor and smartphone usage.

U Suggest some lighting changes for my bedroom which currently uses LED lights.



Dim the overhead lights and consider using amber-tinted bulbs to reach an optimal color temperature.

Frequently Asked Questions

01 How does this MCP help with sleep?

It creates personalized schedules to reduce blue light exposure and optimize your sleep hygiene.

02 Can I use this with Claude?

Yes, you can connect this MCP to any compatible client including Claude, Cursor, and Windsurf.

03 What kind of devices can I assess?

You can use the tool to evaluate the blue light risk for specific hardware setups like laptops, desktops, and smartphones.

04 Does it suggest physical changes to my room?

Yes, the environment optimization tool suggests changes to your physical surroundings to minimize light pollution.

05 Do I need to set up my own hosting?

No, Vinkius hosts and manages the MCP for you, so it is ready to use immediately after you connect.

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>"blue-light-mitigation-planner": { "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

Blue Light Mitigation Planner 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 Blue Light Mitigation Planner. 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	Blue Light Mitigation Planner MCP
Server ID	01a0b67e-8e64-715c-af66-c677219a90cf
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/blue-light-mitigation-planner.