

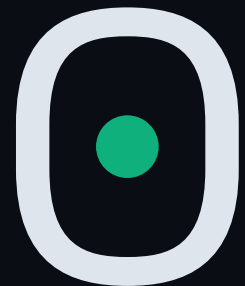
POISON/ZERO

Onboarding

Sechs Schritte für Admins und Entwickler, vom Installationsschlüssel bis zum Feedback.

- 01 Konsole vorbereiten
- 02 Installieren
- 03 Einrichten
- 04 Verwenden
- 05 Telemetrie einsehen
- 06 Feedback geben

Für **poison0** **exec0**



1 Konsole vorbereiten

TARIF

KONSOLE

Enterprise

`https://<tenant>.poison0.com` oder die eigene Domain

Solo Dev, Pro

`https://console.poisonzero.com`

- 1 Weitere Admins einladen: **Settings** → **Zugang & Sicherheit** → **Personen** → E-Mail eintragen → **Einladen**. Der Link gilt 7 Tage.
- 2 Installationsschlüssel anlegen: **Geräte** → **Mehrere Geräte per Schlüssel** → **Variante wählen: Cloud** → **Schlüssel erzeugen**. Der Schlüssel wird nur einmal angezeigt.
- 3 Schlüssel an Entwickler oder IT weitergeben. Er gilt 30 Tage, für so viele Geräte, wie der Tarif erlaubt (Enterprise: unbegrenzt).

2 Installieren

Variante A oder B. Beide richten `/pz` und die Statuszeile in Claude Code ein.

Prüfen nach der Installation: Claude Code neu starten. Die Statuszeile zeigt  **PoisonZero** .

2A. Entwickler installiert selbst

MACOS / LINUX · TERMINAL

```
curl -fsSL https://poisonzero.com/install.sh | sudo PZ_ENROLL_CODE=<schlüssel> PZ_SETUP_AGENTS=claude PZ_SETUP_STATUSLINE=1 sh
```

WINDOWS · POWERSHELL ALS ADMINISTRATOR

```
$env:PZ_ENROLL_CODE='<schlüssel>'; $env:PZ_SETUP_AGENTS='claude'; $env:PZ_SETUP_STATUSLINE='1'; irm https://poisonzero.com/install.ps1 | iex
```

Headless-Geräte (z. B. per SSH): zusätzlich `PZ_HEADLESS=strict` setzen. Unklare Änderungen werden dann sofort zurückgerollt statt per Dialog nachgefragt. Ohne Angabe erkennt der poison0-Agent das selbst.

2B. IT verteilt per Jamf, Intune oder Ansible

Schritt 1: installieren (als root bzw. SYSTEM)

MACOS / LINUX · ROOT

```
PZ_ENROLL_CODE=<schlüssel> sh -c "$(curl -fsSL https://poisonzero.com/install.sh)"
```

WINDOWS · SYSTEM

```
$env:PZ_ENROLL_CODE='<schlüssel>'; irm https://poisonzero.com/install.ps1 | iex
```

Schritt 2: Claude Code einrichten (als angemeldeter Benutzer)

MACOS / LINUX · BENUTZER

```
poisonzero setup-claude
poisonzero setup-claude --statusline-only
```

WINDOWS · BENUTZER

```
& "$env:ProgramFiles\PoisonZero\poisonzero.exe" setup-claude
& "$env:ProgramFiles\PoisonZero\poisonzero.exe" setup-claude --statusline-only
```

JAMF · ROOT, IM KONTO DES ANGEMELDETEN BENUTZERS

```
u=$(stat -f%Su /dev/console)
sudo -u "$u" -H env -u SUDO_USER /usr/local/bin/poisonzero setup-claude
sudo -u "$u" -H env -u SUDO_USER /usr/local/bin/poisonzero setup-claude --statusline-only
```

WERKZEUG EINSTELLUNG

Intune	„Mit den Anmeldeinformationen des angemeldeten Benutzers ausführen: Ja“ („Run this script using the logged on credentials“). Der volle Pfad ist nötig, weil <code>PATH</code> den Programmordner nicht enthält.
Jamf	Läuft als root; der Jamf-Tab führt Schritt 2 im Konto des angemeldeten Benutzers aus.

2C. Geräteame bei der Installation (optional)

Eine der Variablen zusätzlich zu `PZ_ENROLL_CODE` setzen. Es gilt die erste gesetzte in dieser Reihenfolge:

VARIABLE	WIRKUNG
<code>PZ_DEVICE_NAME="Platform / Laptop 07"</code>	Name wird so übernommen
<code>PZ_DEVICE_NAMES_CSV=<Datei oder https-URL></code>	CSV mit Kopfzeile <code>hostname,name</code> . Der Installer sucht den eigenen Hostnamen und übernimmt den Namen. Gesendet wird nur der Name, nie der Hostname
<code>PZ_DEVICE_NAME_FROM_HOSTNAME=1</code>	Hostname wird Geräteame. Nicht empfohlen

PZ-NAMES.CSV

```
hostname,name
mbp-0231,Platform / Laptop 07
```

Hinweis: Den Gerätenamen legt der Administrator fest. Der Name soll keine personenbezogenen Daten enthalten, also zum Beispiel keinen Personennamen.

Länge	1 bis 60 Zeichen, keine Steuerzeichen
Ungültiger Name	wird ignoriert, das Gerät wird trotzdem eingerichtet
Wann der Name übernommen wird	nur bei der ersten Einrichtung eines Geräts. Bei einem bereits eingerichteten Gerät ändern Sie den Namen in der Konsole: Geräte → Gerät umbenennen .
Verfügbar ab	Version 1.16.45

3 Einrichten

1 Geräte ohne Namen benennen: **Geräte** → beim Gerät **Gerät umbenennen** → **Anzeigename des Geräts** eintragen, zum Beispiel „Plattform / Laptop 07“.

2 Teams trennen (optional): je Team einen eigenen Installationsschlüssel anlegen, jeweils mit eigenem **Profil (optional)**. Profile verwalten: **Settings** → **Schutz & Geräte** → **Profile**.

3 Tool-Aufrufe mit **exec0** prüfen (optional)

exec0 prüft jeden Tool-Aufruf Ihrer KI-Agenten, bevor er ausgeführt wird. Dafür braucht das Gerät eine für Melira Ultra geeignete GPU. Ob ein Gerät **exec0** ausführen kann, zeigt seine Geräteseite.

Einstellen: **Settings** → **Schutz & Geräte** → **Profile** → beim Profil **Bearbeiten** → **exec0 mit Melira AI** → **Modus**

MODUS	WIRKUNG
-------	---------

Aus (Standard)	Keine Prüfung
--------------------------	---------------

Beobachten	Prüft jeden Aufruf. Harte Regeln blocken weiterhin, gefährliche Aufrufe werden nur gezählt. Standarddauer 14 Tage, danach beobachtet exec0 weiter und schaltet nicht selbst auf Schutz um.
-------------------	---

Schutz	Blockiert gefährliche Aufrufe vor der Ausführung
---------------	--

Unklare Fälle: In beiden Modi entscheidet die Person am Gerät.

Prüfung nicht möglich: Im Modus Schutz wird der Aufruf blockiert (Standard).

Private Geräte: am Gerät einstellen, unter Windows ohne `sudo` in einem Terminal als Administrator.

BEFEHL	WIRKUNG
--------	---------

<code>sudo poison0 exec0 observe</code>	Beobachten
---	------------

<code>sudo poison0 exec0 enforce</code>	Schutz
---	--------

<code>sudo poison0 exec0 off</code>	Aus
-------------------------------------	-----

<code>poison0 exec0 fail open</code>	Aufruf durchlassen, wenn exec0 ihn nicht prüfen kann
--------------------------------------	---

Mehr dazu: [So prüft exec0 Tool-Aufrufe](#)

4

Verwenden

WO	EINGABE	ERGEBNIS
Claude Code	<code>/pz</code>	Schutzstatistik dieses Monats
Claude Code	Statuszeile	● Schutz läuft; ● Dienst läuft, meldet aber ein Problem; ● Dienst läuft nicht
Kommandozeile	<code>poisonzero stats</code>	Schutzstatistik
Kommandozeile	<code>sudo poisonzero status</code>	Alle Entscheidungen, offene Quarantäne
Kommandozeile	<code>sudo poisonzero quarantine list</code>	Zurückgehaltene Änderungen; <code>show</code> , <code>restore</code> , <code>discard</code> <code><id></code>
Kommandozeile	<code>poisonzero doctor</code>	Selbsttest
Kommandozeile	<code>sudo poisonzero egress</code>	Was den Rechner verlassen hat (Linux auch ohne <code>sudo</code>)
Kommandozeile	<code>poisonzero exec0 status</code>	exec0-Modus auf diesem Gerät, Hook in Claude Code, letzte 24 Stunden

Windows: ohne `sudo`, in PowerShell als Administrator und mit vollem Pfad `& "$env:ProgramFiles\PoisonZero\poisonzero.exe"`.

UPDATE ÜBER

`/PZ` IN CLAUDE CODE

<code>install.sh</code> , <code>install.ps1</code>	Vorhandene <code>/pz</code> -Dateien des installierenden Benutzers werden automatisch erneuert
Homebrew, Scoop, <code>.deb</code> / <code>.rpm</code> , automatisches Update	Jeder Benutzer führt einmal <code>poisonzero setup-claude</code> aus

5

Telemetrie einsehen

KONSOLE	INHALT
Geräte	Zustand und Vorfälle je Gerät
Analytics	Geblockte Änderungen nach Art und Tag; Filter Gerät, Agent, Betriebssystem, 7/30/90 Tage
Audit	Jeder Vorfall mit redigiertem Angriffstext

Nie übertragen: Volltexte der Dateien (nur redigierte Änderungen), Dateien außerhalb der geschützten Pfade, Prozess- und Systeminformationen.

6 Feedback geben

WO	EINGABE
Claude Code	<code>/pz feedback <Text></code>
Kommandozeile	<code>poisonzero feedback "<Text>"</code> (ohne <code>sudo</code>)
PUNKT	REGEL
Länge	Höchstens 2000 Zeichen
Redaktion	Lokal vor dem Versand: Geheimnisse, E-Mail-Adressen, IBAN, Kartennummern, IP-Adressen, Telefonnummern, Zuweisungen von Schlüsseln und Tokens sowie der Benutzername in Home-Pfaden (<code>/Users/<Name></code> , <code>/home/<Name></code> , <code>C:\Users\<Name></code>). Der Befehl zeigt den Text nach der Redaktion
Versand	Mit dem nächsten Check-in. Das Gerät sendet nur Text, Version und Plattform; PoisonZero speichert dazu beim Eingang den aktuellen Namen des Geräts
Empfänger	Den Text sieht nur das PoisonZero-Team, nicht die eigenen Admins
Antwort	Antwortet das Team, erfährt der Kontoinhaber Datum und Gerät des Feedbacks, nicht den Text
Private-Modus	Gesperrt; stattdessen das Kontaktformular auf poisonzero.com

Weiterlesen

Alle Variablen und Pfade des Installers: [den poison0-Agenten installieren](#). Was die Konsole je Vorfall zeigt: [Vorfälle und Audit](#). Wie Updates ankommen: [Updates und Lebenszyklus](#).