

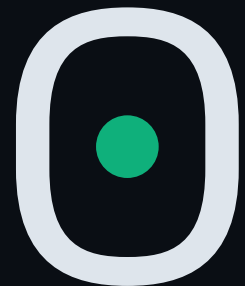
POISON/ZERO

Onboarding

Six étapes pour les administrateurs et les développeurs, de la clé d'installation au retour.

- 01 Préparer la console
- 02 Installer
- 03 Configurer
- 04 Utiliser
- 05 Consulter la télémétrie
- 06 Donner un retour

Pour **poison0** **exec0**



1 Préparer la console

FORFAIT

CONSOLE

Enterprise `https://<tenant>.poison0.com` ou votre propre domaine

Solo Dev, Pro `https://console.poisonzero.com`

- 1 Inviter d'autres administrateurs : **Settings** → **Accès et sécurité** → **Personnes** → saisir l'e-mail → **Inviter**. Le lien est valable 7 jours.
- 2 Créer une clé d'installation : **Appareils** → **Déployer plusieurs appareils avec une clé** → **Choisir la variante : Cloud** → **Générer une clé**. La clé n'est affichée qu'une fois.
- 3 Transmettre la clé aux développeurs ou à l'IT. Elle est valable 30 jours, pour autant d'appareils que votre forfait le permet (Enterprise : illimité).

2 Installer

Variante A ou B. Les deux configurent `/pz` et la ligne d'état dans Claude Code.

Vérifier après l'installation : redémarrez Claude Code. La ligne d'état affiche  PoisonZero .

2A. Le développeur installe lui-même

MACOS / LINUX · TERMINAL

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

WINDOWS · POWERSHELL EN ADMINISTRATEUR

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

Appareils headless (p. ex. via SSH) : ajoutez `PZ_HEADLESS=strict`. Les modifications douteuses sont alors annulées immédiatement au lieu de demander dans une boîte de dialogue. Sans cette variable, l'agent poison0 le détecte lui-même.

2B. L'IT déploie via Jamf, Intune ou Ansible

Étape 1 : installer (en root ou SYSTEM)

MACOS / LINUX · ROOT

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

WINDOWS · SYSTEM

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

Étape 2 : configurer Claude Code (en tant qu'utilisateur connecté)

MACOS / LINUX · UTILISATEUR

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

WINDOWS · UTILISATEUR

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

JAMF · ROOT, DANS LE COMPTE DE L'UTILISATEUR CONNECTÉ

```
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
```

OUTIL RÉGLAGE

Intune Exécuter le script avec les informations d'identification de l'utilisateur connecté : Oui (« Run this script using the logged on credentials »). Le chemin complet est nécessaire car `PATH` n'inclut pas le dossier du programme.

Jamf S'exécute en root ; l'onglet Jamf exécute l'étape 2 dans le compte de l'utilisateur connecté.

2C. Nom de l'appareil à l'installation (optionnel)

Définissez l'une de ces variables en plus de `PZ_ENROLL_CODE`. La première définie, dans cet ordre, s'applique :

VARIABLE	EFFET
<code>PZ_DEVICE_NAME="Platform / Laptop 07"</code>	Le nom est repris tel quel
<code>PZ_DEVICE_NAMES_CSV=<fichier ou URL https></code>	CSV avec l'en-tête <code>hostname,name</code> . L'installateur cherche son propre nom d'hôte et reprend le nom. Seul le nom est envoyé, jamais le nom d'hôte
<code>PZ_DEVICE_NAME_FROM_HOSTNAME=1</code>	Le nom d'hôte devient le nom de l'appareil. Déconseillé

PZ-NAMES.CSV

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

Remarque : Le nom de l'appareil est choisi par l'administrateur. Le nom ne doit pas contenir de données personnelles, par exemple aucun nom de personne.

Longueur 1 à 60 caractères, sans caractères de contrôle

Nom non valide est ignoré, l'appareil est tout de même enrôlé

Quand le nom est repris uniquement lors du premier enrôlement d'un appareil. Pour un appareil déjà enrôlé, modifiez le nom dans la console : **Appareils** → **Renommer l'appareil**.

Disponible à partir de la version 1.16.45

3 Configurer

- 1 Nommer les appareils sans nom : **Appareils** → sur l'appareil **Renommer l'appareil** → saisir le **Nom affiché de l'appareil**, par exemple « Platform / Laptop 07 ».
- 2 Séparer les équipes (optionnel) : créer une clé d'installation par équipe, chacune avec son propre **Profil (optionnel)**. Gérer les profils : **Settings** → **Protection et appareils** → **Profils**.

3 Vérifier les appels d'outils avec **exec0** (optionnel)

exec0 vérifie chaque appel d'outil de vos agents IA avant son exécution. L'appareil a besoin d'un GPU adapté à Melira Ultra. La page de l'appareil indique s'il peut exécuter **exec0**.

Réglage : **Settings** → **Protection et appareils** → **Profils** → **Modifier** sur le profil → **exec0 avec Melira AI** → **Mode**

MODE	EFFET
Désactivé (par défaut)	Aucune vérification
Observer	Vérifie chaque appel. Les règles fixes bloquent toujours, les appels dangereux sont seulement comptés. 14 jours par défaut, ensuite exec0 continue d'observer et ne passe pas de lui-même en Protection.
Protection	Bloque les appels dangereux avant leur exécution

Cas incertains : dans les deux modes, la personne sur l'appareil décide.

Vérification impossible : en Protection, l'appel est bloqué (par défaut).

Appareils privés : réglage sur l'appareil ; sous Windows sans `sudo` dans un terminal ouvert en tant qu'administrateur.

COMMANDE	EFFET
<code>sudo poison0 exec0 observe</code>	Observer
<code>sudo poison0 exec0 enforce</code>	Protection
<code>sudo poison0 exec0 off</code>	Désactivé
<code>poison0 exec0 fail open</code>	Laisser passer un appel quand exec0 ne peut pas le vérifier

En savoir plus : [Comment **exec0** vérifie les appels d'outils](#)

4 Utiliser

OÙ	SAISIE	RÉSULTAT
Claude Code	<code>/pz</code>	Statistiques de protection du mois
Claude Code	Ligne d'état	● protection active ; ● le service tourne mais signale un problème ; ● le service ne tourne pas
Ligne de commande	<code>poisonzero stats</code>	Statistiques de protection
Ligne de commande	<code>sudo poisonzero status</code>	Toutes les décisions, quarantaine ouverte
Ligne de commande	<code>sudo poisonzero quarantine list</code>	Modifications retenues ; <code>show</code> , <code>restore</code> , <code>discard <id></code>
Ligne de commande	<code>poisonzero doctor</code>	Autotest
Ligne de commande	<code>sudo poisonzero egress</code>	Ce qui a quitté la machine (sous Linux aussi sans <code>sudo</code>)
Ligne de commande	<code>poisonzero exec0 status</code>	Mode d'exec0 sur cet appareil, hook dans Claude Code, dernières 24 heures

Windows : sans `sudo` , dans PowerShell en administrateur et avec le chemin complet `& "$env:ProgramFiles\PoisonZero\poisonzero.exe"` .

MISE À JOUR VIA	<code>/PZ</code> DANS CLAUDE CODE
<code>install.sh</code> , <code>install.ps1</code>	Les fichiers <code>/pz</code> existants de l'utilisateur qui installe sont renouvelés automatiquement
Homebrew, Scoop, <code>.deb</code> / <code>.rpm</code> , mise à jour automatique	Chaque utilisateur exécute une fois <code>poisonzero setup-claude</code>

5 Consulter la télémétrie

CONSOLE	CONTENU
Appareils	État et incidents par appareil
Analytique	Modifications bloquées par type et par jour ; filtre par appareil, agent, système d'exploitation, 7/30/90 jours
Audit	Chaque incident avec le texte d'attaque expurgé

Jamais transmis : contenu intégral des fichiers (seulement les modifications expurgées), fichiers hors des chemins protégés, informations sur les processus et le système.

6 Donner un retour

OÙ

SAISIE

Claude Code

`/pz feedback <texte>`

Ligne de commande

`poisonzero feedback "<texte>"` (sans `sudo`)

POINT

RÈGLE

Longueur 2000 caractères au maximum

Expurgation En local avant l'envoi : secrets, adresses e-mail, IBAN, numéros de carte, adresses IP, numéros de téléphone, affectations de clés et de jetons, et le nom d'utilisateur dans les chemins personnels (`/Users/<nom>` , `/home/<nom>` , `C:\Users\<nom>`). La commande affiche le texte après expurgation

Envoi Au prochain check-in. L'appareil n'envoie que le texte, la version et la plateforme ; à la réception, PoisonZero enregistre avec lui le nom actuel de l'appareil

Destinataire Seule l'équipe PoisonZero voit le texte, pas vos propres administrateurs

Réponse Si l'équipe répond, le titulaire du compte apprend la date et l'appareil du retour, pas son texte

Mode privé Bloqué ; utilisez plutôt le formulaire de contact sur poisonzero.com

À lire ensuite

Toutes les variables et chemins de l'installateur : [installer l'agent poison0](#). Ce que la console affiche par incident : [incidents et audit](#). Comment arrivent les mises à jour : [mises à jour et cycle de vie](#).