MISP CLI

AUTOMATE ALL THE THINGS

CIRCL / TEAM MISP PROJECT



NSPA

MISP CLI 09-08-08 2025



မ်းကို MISP CLI

- The MISP API is great for remotely executing administrative tasks
- But sometimes we want to simplify the process / avoid
- MISP also has an extensive CLI sub-system for this reason

- The MISP API is great for remotely executing administrative tasks
- But sometimes we want to simplify the process / avoid having to deal with authentication
- MISP also has an extensive CLI sub-system for this reason

MISP CLI 5052-08-02

└─Types of objectives for the scripts

Automating recurring tasks
 Recovery from loss of access
 Updates / initialisation
 Background worker management

- Automating recurring tasks
- Recovery from loss of access
- Updates / initialisation
- Background worker management

CLI DOCUMENTATION

မ်ကို ရီ နိုင်ငံ CLI documentation

CLI DOCUMENTATION

https://path.to.your.misp/events/automation

inidating the background workers via the APL control accounts beginned workers on texts

An analysis of the second seco

https://path.to.your.misp/events/automation

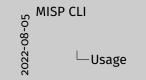
Administering the background workers via the API.

You can start/stop and view the bacground workers via the API. Add worker: http://localhost:5001/servers/startWorker/[queue_name] Stop worker: http://localhost:5001/servers/stopWorker/[worker_pid] Get worker into: http://localhost:5001/servers/getWorkers

Administering MISP via the CLI

Certain administrative tasks are exposed to the API, these help with maintaining and configuring MISP in an automated way / via external tools. Get Setting: MISP/app/Console/cake Admin getSetting [setting] Set Setting: MISP/app/Console/cake Admin getAuthkey [email] Set Authkey: MISP/app/Console/cake Baseur1 [baseur1] Change Password: MISP/app/Console/cake Baseur1 [mex_password] [--override_password_change] Clear Bruteforce Entries: MISP/app/Console/cake Admin update0atbase Update All SON Structures: MISP/app/Console/cake Admin update0atbase Update All SON Structures: MISP/app/Console/cake Admin update0atbase Update Galaxy Definitions: MISP/app/Console/cake Admin update0atbase Update Object Templates: MISP/app/Console/cake Admin update0atbase Update Object Templates: MISP/app/Console/cake Admin update0atbase Update Misp/app/Console/cake Admin update0atbases Update Dipedremplates MISP/app/Console/cake Admin update0atbases Update Dipedremplates: MISP/app/Console/cake Admin update0atbases Update Misp/app/Console/cake Admin update0atbases MISP/app/Console/cake Admin update0atbases Update Misp/app/Console/cake Admin update0atbases MISP/app/Console

3



/var/www/MISP/app/Console/cake [Shell] [Command [parameters] m Example:

- /var/www/MISP/app/Console/cake Password "andras.iklody@gmail.com" "Nutella"
- Change password to "Nutella" for my user
 Some shells are single use and don't need a comma
- parameter Also used by the background processing
- Automation is meant to be used via cron jobs

/var/www/MISP/app/Console/cake [Shell] [Command]
[parameters]

Example:

- /var/www/MISP/app/Console/cake Password "andras.iklody@gmail.com" "Nutella"
- Change password to "Nutella" for my user
- Some shells are single use and don't need a command parameter
- Also used by the background processing
- Automation is meant to be used via cron jobs

MISP CLI

05

8 8 0

2022-

AUTOMATION VIA CRONTAB

Editcrontab of www-data user
 crontab - u www-data - e
 0 - 3,0;3;3;4 + *.
 rootab / a www.data - e
 your / www.data - e
 Fall server 10 tipo as user it every 6 hours
 Binury / your, www.data / a www.data /

- Edit crontab of www-data user
- ∎ crontab -u www-data -e
- 0 3,9,15,21 * * *
 /var/www/MISP/app/Console/cake Server pull 1
 30 full
- Pull server ID #30 as user #1 every 6 hours
- @hourly /var/www/MISP/app/Console/cake Server cacheFeed 1 csv full
- Cache all csv feeds as user #1 every hour