



**DIATEAM**

MILITARY & CIVIL CYBERSECURITY  
SOLUTIONS

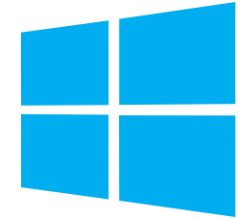
# ACTION MANAGER

2.6

# INTRODUCTION

---

- CROSS PLATFORM PRODUCT



- PRODUCT USED IN THE HYNESIM ENVIRONNEMENT



# Why

---

- ActionManager's main objective is to remotely execute "actions" in hynesim VMs (Virtual Machines)
- Execute multiple script in several entities easily
- Retrieve VM Files to host without network connection
- Actions will generate logs
  - The exit status of the script will be saved
  - History of executed Actions in HMI / API
- Create a script that can be execute on all registered entities
  - One script for everybody
  - Good Maintainability
- Execute an Action at a specific date (Scheduler)
- Run an action as root or as a specific user

# How it works

Client HMI



REST



Host  
Core service

VM Debian



Agent

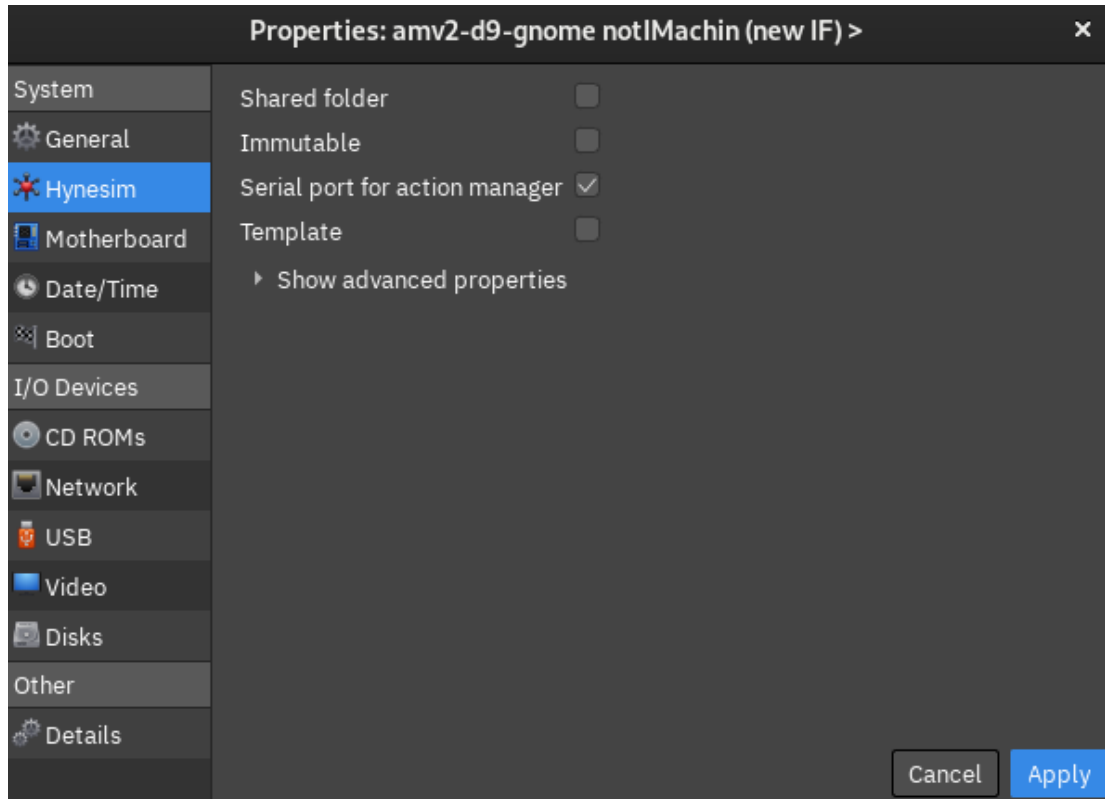


VM Win



Agent

# Works without network connection



# Execute "Actions" from client to VM

Client

VM

```
get /etc/hosts ✓ Succeeded Re-Run
Started: a minute ago Entity: Ubuntu client
Duration: 0.027 seconds Action: get /etc/hosts - 1.0.1
Exit status: 0 Run as user: root

Logs
Search... Run System Info Warning Error Follow logs

1 SYSTEM
2 level="info" msg="Received start action request" actionID="60f04a81225fd252532f61d9" actionName="get /etc/hosts"
3 level="info" msg="Sending run update"
4 level="info" msg="Updating run status to running"
5 level="info" msg="Start running action"
6 RUN
7 127.0.0.1 localhost
8 127.0.1.1 ubuntu-client
9 8.8.8.8 google.com
10 # The following lines are desirable for IPV6 capable hosts
11 ::1 ip6-localhost ip6-loopback
12 fe00::0 ip6-localnet
13 ff00::0 ip6-mcastprefix
14 ff02::1 ip6-allnodes
15 ff02::2 ip6-allrouters
16 SYSTEM
17 level="info" msg="runStdout read EOF"
18 level="info" msg="runStderr read EOF"
19 level="info" msg="Run succeeded without errors"
20 level="info" msg="Sending run update"
21 level="info" msg="Updating run status to success"
22 level="info" msg="No output file to retrieve"
23 level="info" msg="Finished Run"
```

```
Remote Control Manager
Ubuntu client (TP-HYNESIM)
avril 26 15:03

hns@ubuntu-client: ~
hns@ubuntu-client:~$ cat /etc/host
*cat: /etc/host: No such file or directory
hns@ubuntu-client:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu-client
8.8.8.8 google.com
# The following lines are desirable for IPV6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
hns@ubuntu-client:~$
```

# ACTION

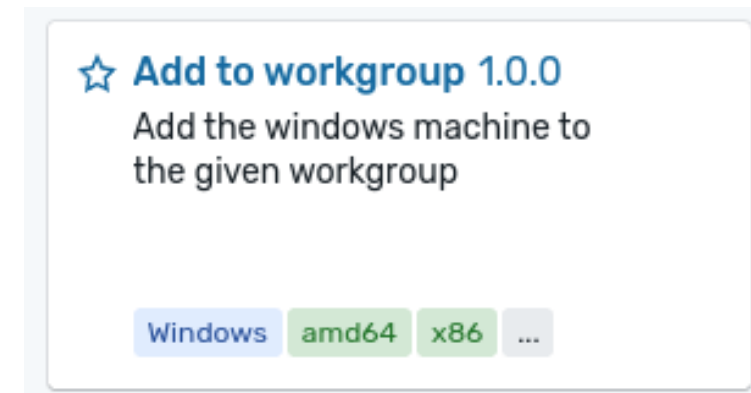
---

- Executable
  - Bash
  - Python
  - Powershell



- JSON
  - Describe the action and its inputs, resources...

- Executed in an Entity



# Run multiple Actions

### Launcher

ENTITIES Clear all

+ Add entity

**master 4.5.2**  
hynesim 4.5.2  
Linux amd64

ACTIONS Clear all

+ Add action

**uploadFile 2.0.0**  
Linux amd64 x86

**powerOff 1.0.0**  
Linux amd64 x86

#### Actions Library

Find action... 15

Hide incompatible actions

**Find and stop PLC 1.0.0** ⓘ  
Search for a PLC using the given target and launch a stop packet to it. target format...  
Linux amd64 x86  
Use

**uploadFile 2.0.0** ⓘ  
Linux amd64 x86  
Use

**nmapIPToPorts 1.0.0** ⓘ  
Linux amd64 x86  
Use

**pslist 1.0.0** ⓘ  
Linux amd64 x86  
Use

**powerOff 1.0.0** ⓘ

Last saved: May 5, 2023, 10:40:04

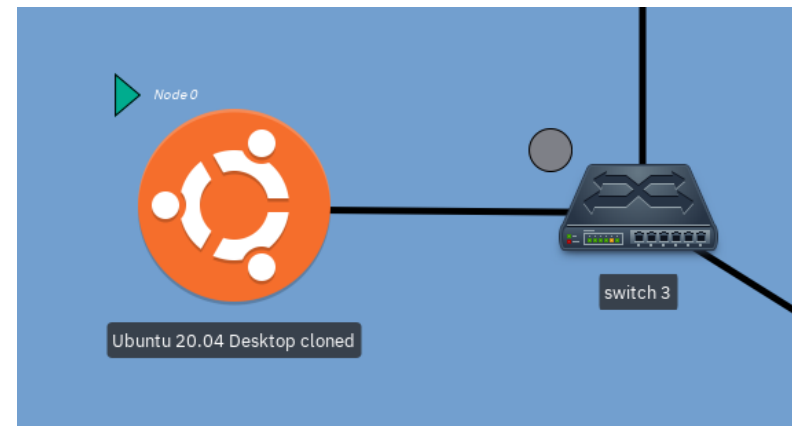
Cancel Run action(s) ▾



# AGENTS

---

- Run inside Entities
- Cross Platform (Windows / GNU Linux )
- Execute "Actions"
- Connected through serial port



```
hns@ubuntu:/tmp$ ls -la
total 7628
drwxrwxrwt 19 root root    4096 avril 26 12:03 .
drwxr-xr-x 20 root root    4096 févr.  5 2021 ..
-rwxr-xr-x  1 root root 7725056 avril 26 12:01 agent
```



# DIATEAM

MILITARY & CIVIL CYBERSECURITY  
SOLUTIONS

## MAIN USAGE

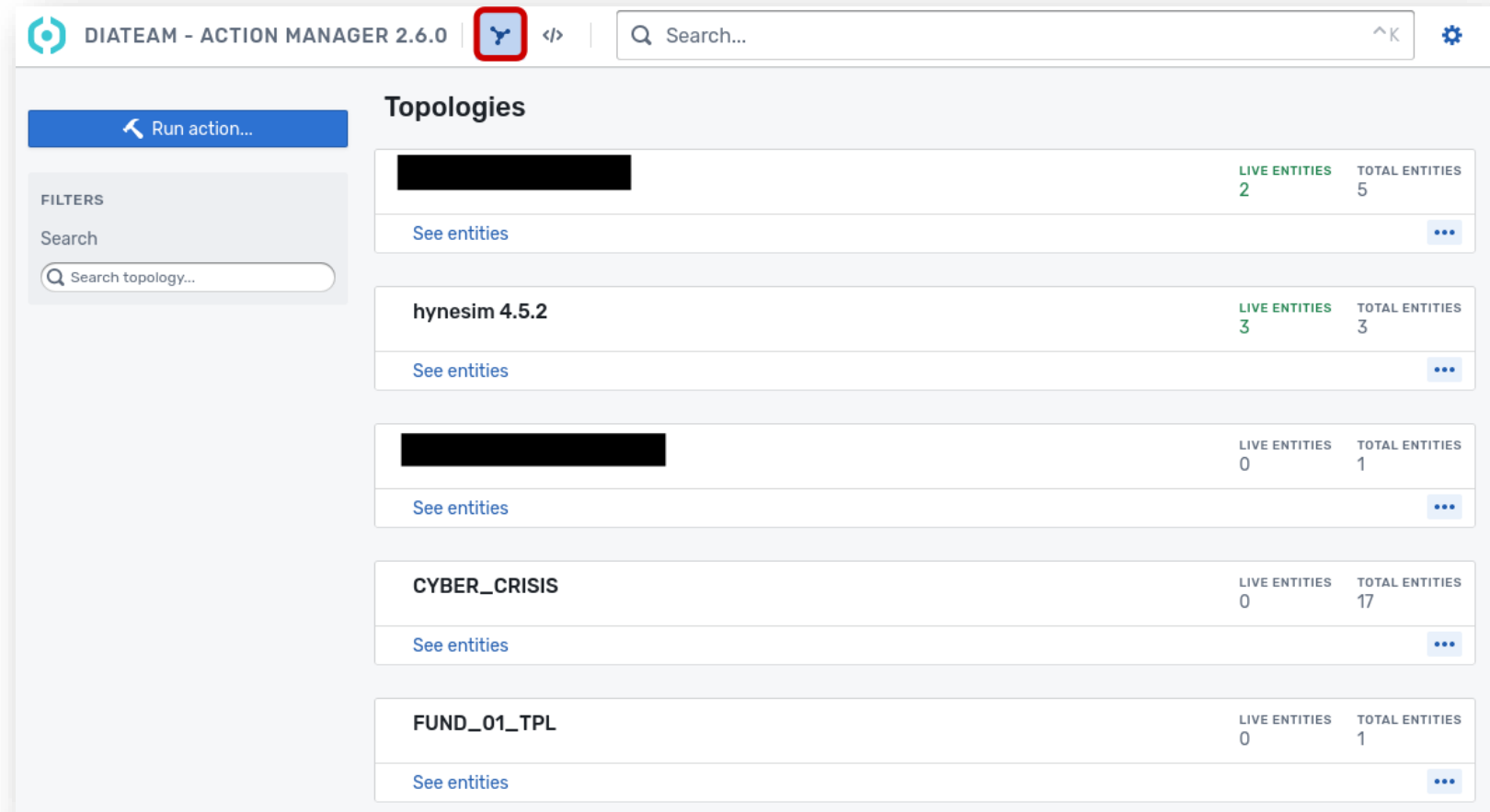
[www.diateam.net](http://www.diateam.net) – [contact@diateam.net](mailto:contact@diateam.net) - [@DIATEAM\\_Labs](https://twitter.com/DIATEAM_Labs)

© DIATEAM. All Rights Reserved.

# MAIN USAGE

- TOPOLOGIES PAGE
  - Run actions
  - Entities information & runs

- AM “AGENT” MUST BE RUNNING
- RUN ACTIONS FROM ANYWHERE



The screenshot displays the DIATEAM - ACTION MANAGER 2.6.0 interface. The top navigation bar includes the DIATEAM logo, the version number, a code editor icon, and a search bar. A red box highlights the code editor icon. Below the navigation bar, there is a 'Run action...' button and a 'FILTERS' section with a search input. The main content area is titled 'Topologies' and lists several topology entries. Each entry shows the topology name, the number of live entities, and the total number of entities. A 'See entities' link is provided for each topology.

Topology Name	LIVE ENTITIES	TOTAL ENTITIES
[REDACTED]	2	5
hynesim 4.5.2	3	3
[REDACTED]	0	1
CYBER_CRISIS	0	17
FUND_01_TPL	0	1

# MAIN USAGE

- ENTITIES PAGE

- Run actions
- Entities information & runs

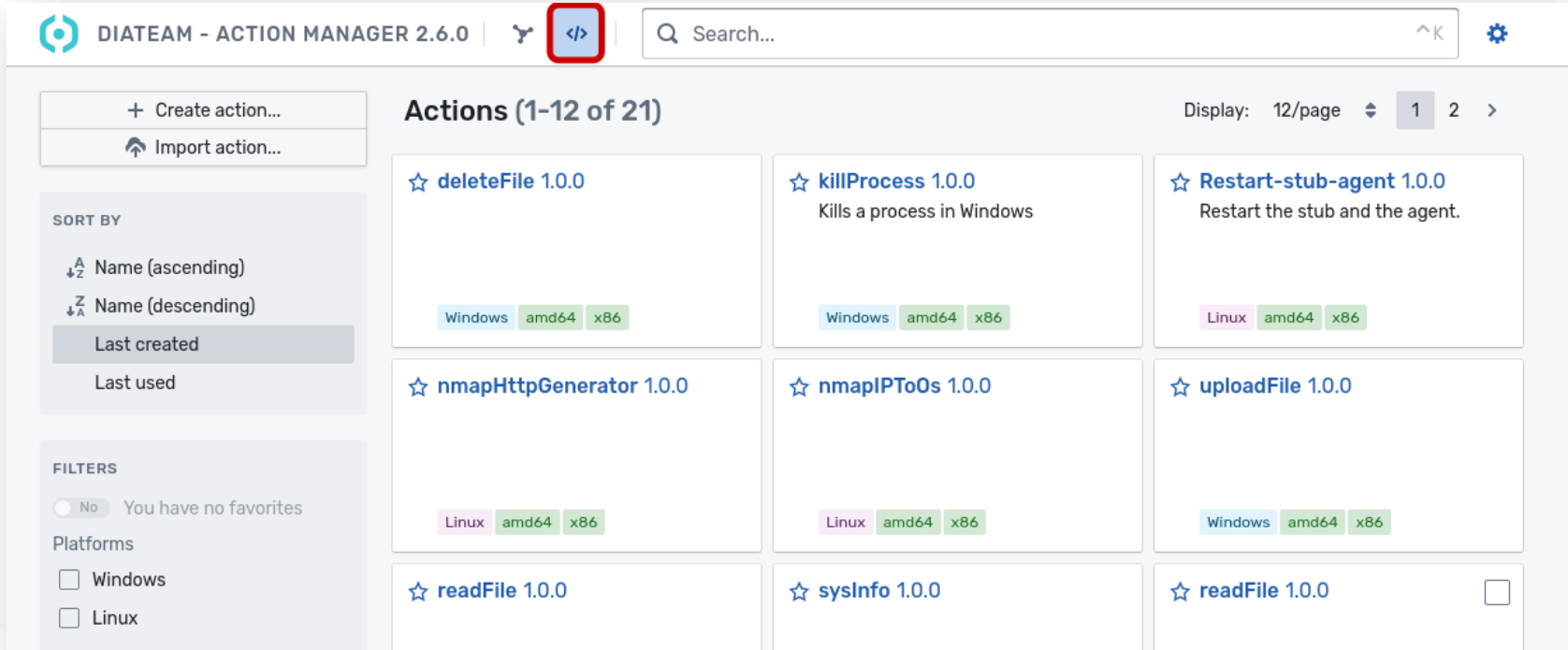
- AM “AGENT” MUST BE RUNNING

- RUN ACTIONS FROM ANYWHERE

The screenshot shows the Diateam Action Manager 2.6.0 interface. At the top, the breadcrumb navigation shows 'Topologies > hynesim 4.5.2', with 'hynesim 4.5.2' highlighted by a red box. The main content area is titled 'Entities' and lists three entities: 'debian 11', 'master 4.5.2', and 'node 4.5.2'. Each entity entry includes a status indicator (green dot), the topology name 'hynesim 4.5.2', the OS 'debian', and a table of run statistics: ACTIVE, FAILED, and TOTAL RUNS. For 'debian 11', the statistics are 0 active, 0 failed, and 6 total runs. For 'master 4.5.2', they are 0 active, 0 failed, and 1 total run. For 'node 4.5.2', they are 0 active, 0 failed, and 0 total runs. Each entry has a 'Run action on this entity...' button and a 'See runs' link. On the left side, there are 'SORT BY' options (Name ascending, Name descending, Last used) and 'FILTERS' (All, Only show live entities, Search entity...). A 'Run action...' button is also visible in the top right corner of the interface.

# MAIN USAGE

- ACTIONS PAGE
  - Create and import actions
  - Actions information
- WINDOWS
  - BAT or Powershell
- LINUX
  - Any executable file



# MAIN USAGE

- ACTION PAGE
  - inputs details
  - Version, exec file...

### writeFile

Edit action ▾

**DESCRIPTION**  
No description.

**INPUT LIST**

- Text to write**  
Example: Hello world! ^
- File** ▾
- Mode** ▾

**INFORMATION**

**ID**  
6454baf75c1b91c95133d8b8

**Version**  
1.0.0

**Executable**  
writeFile.sh

**Target OS**  
Linux 1.0.0

**Architecture**  
amd64, x86

**Added**  
May 5th 2023 10:14:47

**Last use**  
May 5th 2023 14:19:27

**Last update**  
May 5th 2023 10:14:47

**RESOURCE LIST**

**This action has no resources**  
Edit the action to add resources.

**TAGS**  
No tags.

# MAIN USAGE

- LAUNCHER
  - Select entities
  - Select actions
  - Configure actions
  
- LAUNCHER CAN BE ACCESSED FROM ANYWHERE

The screenshot shows the 'Launcher' application interface. It is divided into three main vertical sections:

- ENTITIES:** Contains a '+ Add entity' button and two entity cards. The first card is for 'master 4.5.2' (hynesim 4.5.2) with 'Linux' and 'amd64' tags. The second card is for 'node 4.5.2' (hynesim 4.5.2) with 'Linux' and 'amd64' tags. A blue box highlights this section with the text 'Selected entities'.
- ACTIONS:** Contains a '+ Add action' button and two action cards. The first card is for 'uploadFile 2.0.0' with 'Linux', 'amd64', and 'x86' tags. The second card is for 'pslist 1.0.0' with 'Linux', 'amd64', and 'x86' tags. An orange box highlights this section with the text 'Selected actions'.
- Actions Library:** A search bar with 'Find action...' and a '15' count. A toggle for 'Hide incompatible actions' is checked. Below are five action entries, each with a star icon, a title, a description, and tags: 'Find and stop PLC 1.0.0', 'uploadFile 2.0.0', 'nmapIPToPorts 1.0.0', 'pslist 1.0.0', and 'powerOff 1.0.0'. Each entry has a 'Use' button.

At the bottom, there is a status bar with 'Last saved: May 5, 2023, 14:47:13', a 'Cancel' button, and a 'Run action(s)' button with a dropdown arrow.

# MAIN USAGE

- RUN RESULT

- System logs & action logs
- Execution duration
- User

**listProcess** ✓ Succeeded ↶ Re-Run

📅 Started: a few seconds ago    🖥 Entity: master 4.5.2

🕒 Duration: 0.08 seconds    ⚡ Action: listProcess - 1.0.0

📄 Exit status: 0    👤 Run as user: root

[Logs](#)

Run System
Info Warning Error
Follow logs

	USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
1	root	1	0.0	0.1	163896	10168	?	Ss	14:00	0:02	/sbin/init
2	root	2	0.0	0.0	0	0	?	S	14:00	0:00	[kthreadd]
3	root	3	0.0	0.0	0	0	?	I<	14:00	0:00	[rcu_gp]
4	root	4	0.0	0.0	0	0	?	I<	14:00	0:00	[rcu_par_gp]
5	root	6	0.0	0.0	0	0	?	I<	14:00	0:00	[kworker/0:0H-kblockd]
6	root	8	0.0	0.0	0	0	?	I<	14:00	0:00	[mm_percpu_wq]
7	root	9	0.0	0.0	0	0	?	S	14:00	0:00	[rcu_tasks_rude_]
8	root										



# MAIN USAGE

- ENTITY RUNS PAGE
  - Sorted by date
  - Run an action again

**Runs (2)** Display: 10/page 1 Purge succeeded runs...

**listProcess 1.0.0**  
Started: 5 minutes ago Duration: 0.08 seconds  
✓ Succeeded Details Re-Run

**sysInfo 1.0.0**  
Started: 42 minutes ago Duration: 1.85 seconds  
✓ Succeeded Details Re-Run

Display: 10/page 1

**Entity Information**

**Name**  
master 4.5.2

**Hostname**  
debian

**Platform**  
Linux

**Architecture**  
amd64

**Last contact**  
05/05/2023

**Agent uptime**  
1 hour, 35 seconds

**Topology**  
hynesim 4.5.2

**Tags**  
Linux amd64



# DIATEAM

MILITARY & CIVIL CYBERSECURITY  
SOLUTIONS

## DEMONSTRATION

[www.diateam.net](http://www.diateam.net) – [contact@diateam.net](mailto:contact@diateam.net) - [@DIATEAM\\_Labs](https://twitter.com/DIATEAM_Labs)

© DIATEAM. All Rights Reserved.



# DIATEAM

MILITARY & CIVIL CYBERSECURITY  
SOLUTIONS

## ADVANCED FEATURES

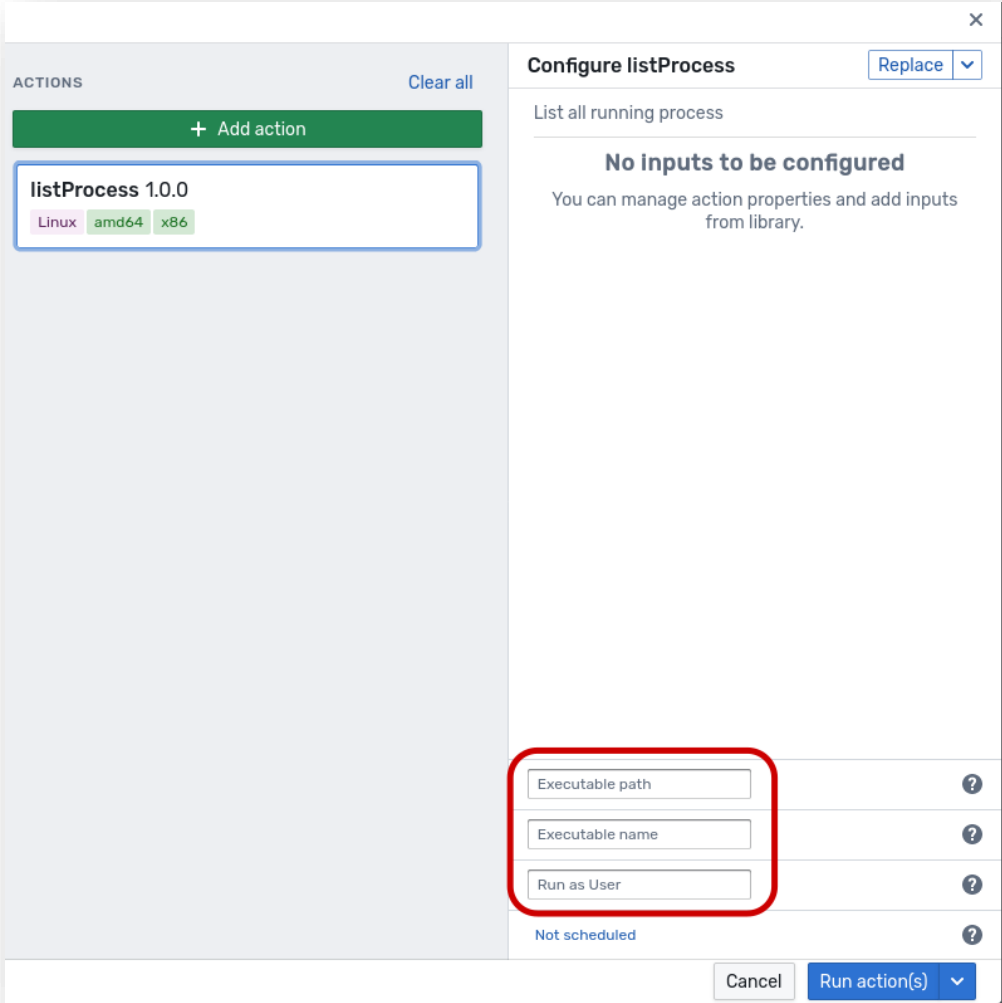
[www.diateam.net](http://www.diateam.net) – [contact@diateam.net](mailto:contact@diateam.net) - [@DIATEAM\\_Labs](https://twitter.com/DIATEAM_Labs)

© DIATEAM. All Rights Reserved.

# ADVANCED FEATURES

- USER ACTION

- Default: root/nt authority
- Allows to execute an action as a user
  - Launch graphical softwares
  - Create/Update content as a user
- Allow to change the location that the action will be runed
  - Default in the temporary directory
- Allow to change the executable name
  - Default name "exec"



# ADVANCED FEATURES

- SCHEDULER
  - Prepare your actions

The screenshot displays a scheduling interface. At the top, it shows the month 'March' and the year '2021'. Below this is a calendar grid for the month of March. The days of the week are labeled 'Su', 'Mo', 'Tu', 'We', 'Th', 'Fr', and 'Sa'. The date '25' is highlighted. Below the calendar is a time picker with a digital display showing '16 : 52 : 50'. There are up and down arrows for adjusting the time. At the bottom of the calendar view, there are 'Today' and 'Cancel' buttons. Below the calendar view, there is a blue button labeled 'Not scheduled' with a question mark icon. At the very bottom, there are 'Cancel' and 'Run action(s)' buttons, with a dropdown arrow next to 'Run action(s)'.

# ADVANCED FEATURES

- FILES

- Exchange files between the server and the VM
- Input files
- output files
- resources

### Create new action

**Name (Required)**  **Version (Required)**

**Description**   
Press enter to make a line break. max. 250 characters

**Tags**

**Executable (Required)**   **Platform**   **Architecture**

**Inputs (1)**

Name (Required)	Type	Description	Default/Savename	Example
<input type="text"/>	<input type="button" value="File"/> <input type="button" value="Text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Please give this input a name.

**Resources (1)**

Please provide a resource.

# ADVANCED FEATURES

- SWAGGER
  - Delivered with AM server
  - Browse & test the API

Swagger doc.json Explore

### ActionManager API 2.2.0-15-gb581f80-dirty

[ Base URL: /v2 ]  
doc.json

Core AM API

Array-type query parameters use the 'multi' collection format (eg.: `url?key=value1&key=value2` )  
Void value is also supported (eg.: `<url?>key == <url?>key=` )

#### Actions

An action is a script/software along with its metadata so it can easily be prepared and launch with the ActionManager

- GET /actions List actions
- POST /actions Upload action
- GET /actions/{id} Get action
- PUT /actions/{id} Update action
- DELETE /actions/{id} Delete action
- GET /actions/{id}/exec Get action executable file
- POST /actions/{id}:duplicate Duplicate action
- GET /actions/{id}:export Export the designated action as an action archive
- POST /actions:import Import an action archive into the actionmanager
- GET /agents/{agentId}/actions List agent actions
- POST /agents/{agentId}/actions/{actionId} Run action

#### Agents

An agent is a piece of software running on VMs and allowing to execute actions on them



**DIATEAM**

MILITARY & CIVIL CYBERSECURITY  
SOLUTIONS



**MANY THANKS !  
QUESTIONS ?**