



Imperum User Documentation

Agents

Version

0.3.0

Date of Publication

November 2025

✦ Agents Section Main Menu

This interface is part of a comprehensive system designed to monitor, manage, and interact with agents and associated tasks or hunts. It enables users to maintain a structured view of all active and available agents while facilitating efficient management of operations.

Overview of the Interface

The interface is divided into two primary sections: Agents and Hunts, which can be toggled through tabs located at the top. Each section plays a distinct role in enabling system operations and offers dedicated functionalities to streamline management processes.

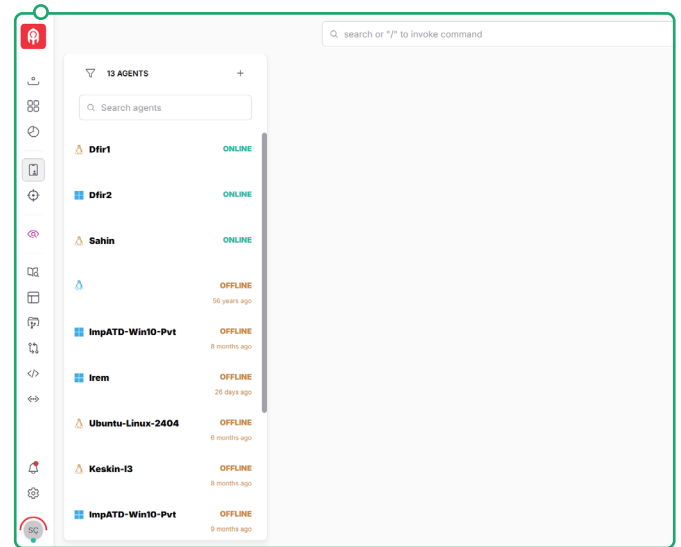
Agent List

The left panel displays a scrollable list of all registered agents. Each agent is presented with essential details to help users monitor their status and manage associated tasks effectively.

Agent Name

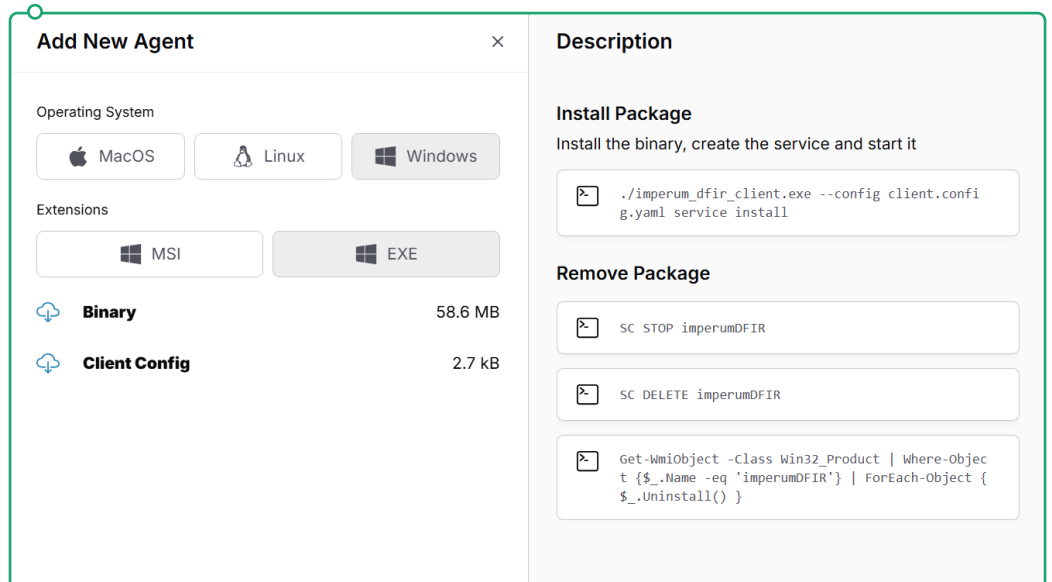
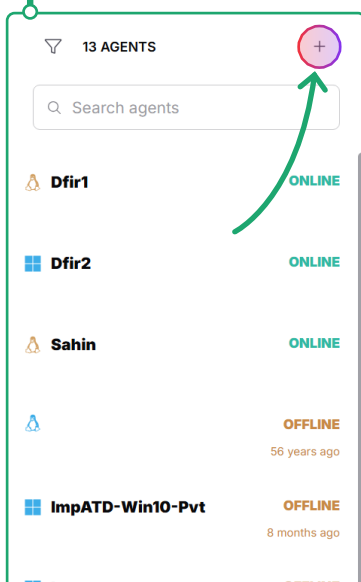
The displayed name or identifier for each agent (e.g., "Dfir1" or "ImpATD-Win10-Pvt") allows users to quickly identify specific devices or endpoints within the system. These names often align with the hostnames or labels defined during the agent setup process.

- The term DFIR stands for Digital Forensics and Incident Response. It refers to a specialized field within cybersecurity focused on investigating and responding to security incidents, such as data breaches, malware infections, or unauthorized access to systems.



✦ Adding New Agents

- Navigate to the Agents page.
- Click the "+" button.
- Follow the step-by-step instructions for your operating system (Linux, macOS, or Windows).



✦ Control Panel

○ Agent Status^[1]

A status label indicates whether the agent is actively communicating with the system. A green "ONLINE" tag signifies active connectivity and readiness for interaction, whereas an offline status would be marked differently (not shown in this example).

○ Search Functionality^[2]

A search bar is positioned above the agent list. This tool allows users to quickly locate specific agents by entering their name, hostname, or related attributes. This feature is especially valuable in environments with large numbers of agents, enhancing operational efficiency.

○ Filtering Agents^[3]

Narrow results by agent label, operating system or status to quickly find the exact agents you need.

Within minutes, the new device will appear in the Agent List, ready for monitoring and management. The setup process is straightforward no additional configurations or hidden steps required.

The screenshot shows the '13 AGENTS' header with a filter icon (3) and a plus icon (+). Below is a search bar labeled 'Search agents' (1). The agent list contains the following entries:

Agent Name	Status	Last Seen
Dfir1	ONLINE	
Dfir2	ONLINE	
Sahin	ONLINE	
	OFFLINE	56 years ago
ImpATD-Win10-Pvt	OFFLINE	8 months ago
Isom	OFFLINE	

Callout 2 points to the 'ONLINE' status tag of the first agent.

The 'Filter Agents' dialog box contains the following fields and buttons:

- Label:** Text input field with placeholder 'Enter agent label'.
- Operating System:** Dropdown menu with 'All Operating Systems' selected.
- Status:** Dropdown menu with 'All Statuses' selected.
- Buttons:** 'Reset Filters', 'Cancel', and 'Apply Filters'.

✦ Agent Details

Each agent detail page provides a comprehensive overview, including:

debian12.12

77f5abd4491f5a8c

6 Oct 2025, 13:40

Delete

Isolate Host

Last IP

172.29.0.11:44584

Labels

test

another

FQDN

Hostname

Arch

sahin

sahin

amd64

Bash

Execute a terminal command

Login to Activate

DetectRaptor.Linux.Detection.YaraProcessLinux

Exchange.Linux.Applications.Docker.Ps

Exchange.Linux.Applications.WgetHSTS

Not Logged in

CPU Usage

100%

75%

50%

25%

0%

RAM Usage

100%

75%

50%

25%

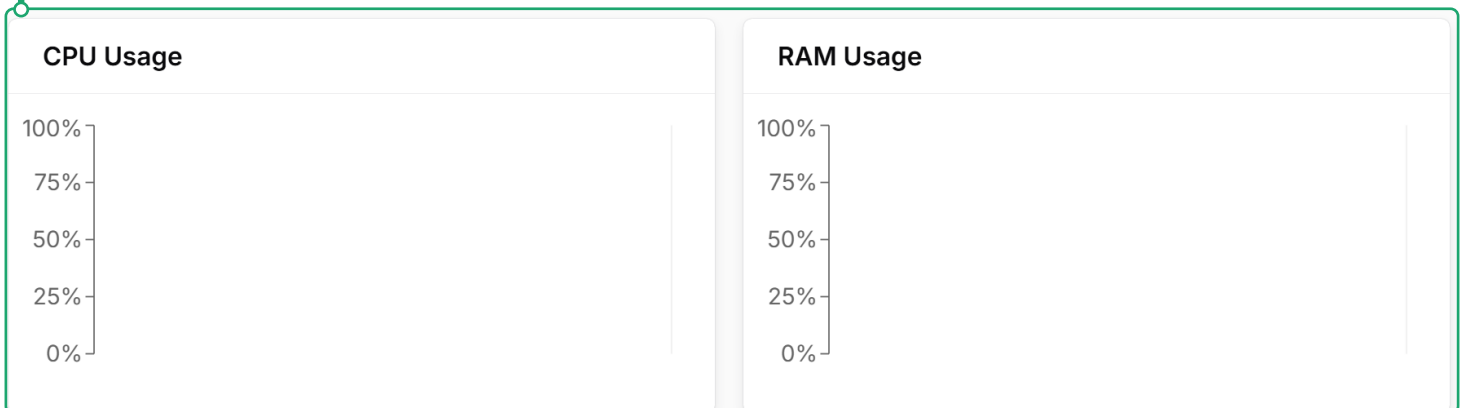
0%

TASK LIST	COMMANDS	DATE	STATUS	
F.D3DMVP5A39NNA	Linux.Sys.BashShell	30 Sept 2025, 08:51:32	FINISHED	...
F.D3D6MEBOHTTMG	Linux.Network.Netstat	29 Sept 2025, 14:19:21	FINISHED	...

Show rows per page 10

1 - 2 of 2

- System resource usage at a glance.



- Recent command executions and their results.

TASK LIST	COMMANDS	DATE	STATUS	
F.D3DMVPSA39NNA	Linux Sys.BashShell	30 Sept 2025, 08:51:32	FINISHED	...
F.D3D6MEBOHTTMG	Linux Network.Netstat	29 Sept 2025, 14:19:21	FINISHED	...

Show rows per page

10

1 - 2 of 2

- Direct access for executing terminal commands or running pre-built artifact scripts.

To execute terminal commands:

- Click Login to Activate to enable the interactive session

Bash Execute a terminal command [Login to Activate](#)

- Create and run your own custom command or open the predefined command list using the three-dot (...) menu.

Create and run your own custom command^[1]

Select the desired command type (Bash, PowerShell, or VQL). Then you can create and execute your custom terminal command.

Bash

Bash

Powershell

Vql

Execute a terminal command

Exchange.Linux.Detection.YaraProcessLinux Exchange.Linux.Applications.Docker.Ps Exchange.Linux.Applications.WgetHSTS

1

2

Using Predefined Command List^[2]

Open the predefined command list using the three-dot (...) menu. Select the desired command, provide the required parameters, and then execute command.

Select the desired command, provide the required parameters, and then execute command.

Commands

Search commands

DetectRaptor.Linux.Detection.YaraProcessLinux

Exchange.Linux.Applications.Docker.Ps

Exchange.Linux.Applications.WgetHSTS

Exchange.Linux.Carving.SSHLogs

Exchange.Linux.Collection.Autoruns

Exchange.Linux.Collection.BrowserExtensions

Exchange.Linux.Collection.BrowserHistory

Exchange.Linux.Collection.CatScale

Exchange.Linux.Collection.DBConfig

Exchange.Linux.Collection.History

Exchange.Linux.Collection.NetworkConfig

Exchange.Linux.Collection.SysConfig

Exchange.Linux.Collection.SysLogs

Exchange.Linux.Collection.UserConfig

Exchange.Linux.Debian.GPGKeys

Exchange.Linux.Detection.BruteForce

Parameters

Outfile

collection

OutfilePrefix

catscale_

OutDir

catscale_out

- When needed, you can isolate a device with a single action containing potential threats and protecting the rest of your environment. To perform isolation, you must first click the Login to Activate button.

sahin

debian12.12 77f5abd4491f5a8c 6 Oct 2025, 13:53

Delete Isolate Host

Last IP

172.29.0.11:44944

Labels

test x anoth... x +

FQDN

sahin

Hostname

sahin

Arch

amd64

✦ Hunts

The Hunts page enables you to run pre-defined artifacts across multiple agents simultaneously. Artifacts streamline repetitive tasks, ensuring accuracy and standardization while saving time. Typical use cases include:

- Performing system audits
- Running security checks
- Collecting log files
- Cleaning temporary data
- Validating compliance configurations

With just a few clicks, you can execute these actions at scale whether on a single group of agents or your entire environment.

One Time Hunt

- Enter a description and set an expiry time
- Define inclusion and exclusion rules (e.g., all Windows agents except those with label abc).
- Select the artifacts to be executed

Each execution is visible in the dashboard, allowing you to track, monitor, and review results easily.

Add New Hunt

To create a hunt:

- Enter a description and set an expiry time.
- Define inclusion and exclusion rules (e.g., all Windows agents except those with label abc).

Hunts automatically apply not only to online agents but also to any offline or newly added agents until the hunt expires. This ensures complete coverage without manual reconfiguration.

The image displays three screenshots of the Hunt interface, illustrating the process of creating and managing hunts.

Left Screenshot: Hunt List
This screenshot shows the 'Hunts' page with a list of hunts. The 'One-Time' tab is selected. The list includes hunts like 'ImpATD Monitoring' (RUNNING), 'Automation Test' (STOPPED), 'Simulate' (STOPPED), 'Dfir2 Netstat' (STOPPED), 'Dfir1 Local' (STOPPED), 'Dfir2 Local User' (STOPPED), 'Staging One-Time ...' (STOPPED), and 'Escape Char' (STOPPED). A red arrow points from the 'Simulate' hunt to the 'Add New Hunt' dialog.

Middle Screenshot: Add New Hunt - Configure Hunt
This screenshot shows the 'Add New Hunt' dialog, Step 1/2. It includes fields for 'Description' (Enter Description), 'Expiry' (gg.aa.yyyy --:--), and 'Include Condition' (Run Everywhere, Match by Label, Operating System). There is also an 'Exclude Condition' section with 'Run Everywhere' and 'Match by Label' options. At the bottom are 'Cancel' and 'Next Step' buttons.

Right Screenshot: Add New Hunt - Select Artifacts
This screenshot shows the 'Add New Hunt' dialog, Step 2/2. It includes a search bar for artifacts and a list of artifacts to select. The artifacts listed are: Admin.Client.Uninstall, Admin.Client.UpdateClientConfig, Admin.Client.Upgrade.Debian, Admin.Client.Upgrade.RedHat, Admin.Client.Upgrade.Windows, Demo.Plugins.GUI, DetectRaptor.Generic.Detection.WebshellYara, DetectRaptor.Generic.Detection.YaraFile, DetectRaptor.Generic.Detection.YaraWebshell, DetectRaptor.Linux.Detection.YaraProcessLinux, DetectRaptor.Macos.Detection.YaraProcessMacos, DetectRaptor.Windows.Detection.Amcache, DetectRaptor.Windows.Detection.Applications, and DetectRaptor.Windows.Detection.BinaryRename. At the bottom are 'Back' and 'Configure' buttons.

Continuous Hunts

Continuous Hunts extend regular hunts with scheduling capabilities. They run automatically at defined intervals (daily, weekly, monthly, etc.), making them ideal for:

- Routine system health checks
- Recurring security audits
- Ongoing compliance verification

Each execution is visible in the dashboard, allowing you to track, monitor, and review results easily.

Add New Continuous Hunt

- Enter a description and set an expiry time
- Enter repeat time. (e.g., if "Every 10 minutes" is selected, this command will be executed every 10 minutes for the selected agents.)
- Define inclusion and exclusion rules (e.g., all Windows agents except those with label abc)
- Select the artifacts to be executed

One-Time

Continuous

0 HUNTS

Add New Continuous Hunt

Configure Hunt

STEP 1 / 2

Description

Enter Description

Expiry

gg.aa.yyyy --:--

Repeat

Every 10 minutes

* / 10

*

*

*

*

Minute

Hour

Day of Month

Month

Day of Week

Examples

Run Everywhere

Match by Label

Operating System

Exclude Condition

Run Everywhere

Match by Label

Cancel

Next Step

Add New Continuous Hunt

Select Artifacts

STEP 2 / 2

Q Search artifacts

☐ Admin.Client.Uninstall
 ☐ Admin.Client.UpdateClientConfig
 ☐ Admin.Client.Upgrade.Debian
 ☐ Admin.Client.Upgrade.RedHat
 ☐ Admin.Client.Upgrade.Windows
 ☐ Demo.Plugins.GUI
 ☐ DetectRaptor.Generic.Detection.WebshellYara
 ☐ DetectRaptor.Generic.Detection.YaraFile
 ☐ DetectRaptor.Generic.Detection.YaraWebshell
 ☐ DetectRaptor.Linux.Detection.YaraProcessLinux
 ☐ DetectRaptor.Macos.Detection.YaraProcessMacos
 ☐ DetectRaptor.Windows.Detection.Amcache
 ☐ DetectRaptor.Windows.Detection.Applications
 ☐ DetectRaptor.Windows.Detection.BinaryRename

Back

Configure

Continuous Hunts Details

Selecting a hunt from the list opens the Hunt Details view, where you can access detailed information:

General Information

- Hunt name
- Current status (Running or Stopped)
- Start and end date/time
- Execution interval (e.g., Every 10 minutes)

🔍 search or "/" to invoke command

One-TimeContinuous

9 HUNTS

🔍 Search hunts

Irem_994 HuntsSTOPPED

28.08.2025_i2_99...9 HuntsSTOPPED

V0.3.0-Rc.342 HuntsSTOPPED

22.08.2025_i42 HuntsSTOPPED

Irem_test_22 HuntsSTOPPED

Irem_test_21.08STOPPED

28.08.2025_i2_99_5_1

STOPPED

DeleteEditStart

🕒 28 Aug 2025, 17:18🕒 8 Sept 2025, 13:00🕒 Started Every 10 minutes

28.08.2025_i2_99_5_1

HUNT	COMMANDS	STARTED TIME	
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:50:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:40:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:30:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:20:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:10:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:50:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:40:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:30:00	STOPPED

Commands Table

Displays a log of all executions, including:

- Hunt name
- Artifact/command executed (e.g., Windows.Network.Netstat)
- Execution time
- Execution status (e.g., Stopped, Completed, Running)

🔍 search or "/" to invoke command

One-TimeContinuous

9 HUNTS

🔍 Search hunts

Irem_994 HuntsSTOPPED

28.08.2025_i2_99...9 HuntsSTOPPED

V0.3.0-Rc.342 HuntsSTOPPED

22.08.2025_i42 HuntsSTOPPED

Irem_test_22 HuntsSTOPPED

Irem_test_21.08STOPPED

28.08.2025_i2_99_5_1

STOPPED

DeleteEditStart

🕒 28 Aug 2025, 17:18🕒 8 Sept 2025, 13:00🕒 Started Every 10 minutes

28.08.2025_i2_99_5_1

HUNT	COMMANDS	STARTED TIME	
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:50:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:40:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:30:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:20:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:10:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:50:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:40:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:30:00	STOPPED

Action Buttons (top-right corner)

- **Start** begin the execution of the hunt.
- **Stop** terminate an active hunt.
- **Edit** update hunt parameters such as artifacts or schedule.
- **Delete** remove the hunt from the system.

The screenshot displays the Hunt Management interface. On the left, a sidebar lists several hunts, all marked as **STOPPED**. The main panel shows a detailed view of the hunt **28.08.2025_i2_99_5_1**, which is also **STOPPED**. The hunt's schedule is set to **Every 10 minutes**, with the last execution on **8 Sept 2025, 13:00**. The top-right corner of the hunt detail panel features three action buttons: **Delete**, **Edit**, and **Start**. Below the hunt details, a table lists the individual commands executed by the hunt.

HUNT	COMMANDS	STARTED TIME	STATUS
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:50:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:40:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:30:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:20:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	8 Sept 2025, 12:10:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:50:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:40:00	STOPPED
28.08.2025_i2_99...	Windows.Network.Netstat	28 Aug 2025, 17:30:00	STOPPED