imperum

Imperum User Documentation

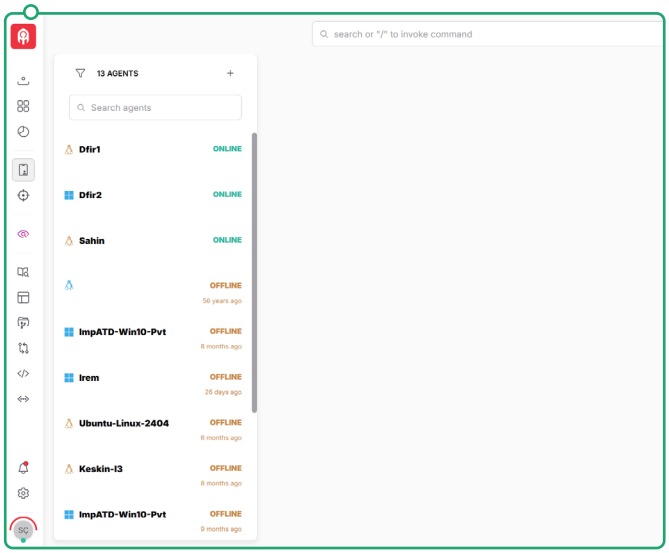
Agents

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.

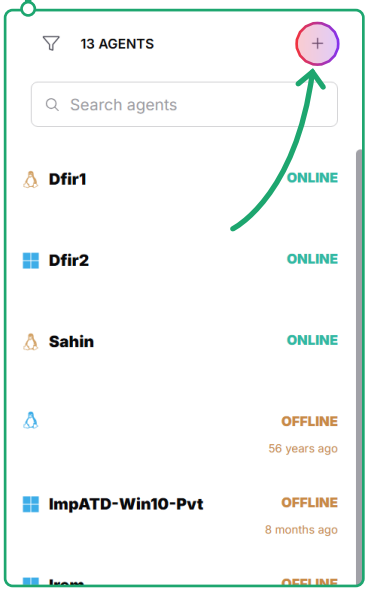
Agent Name

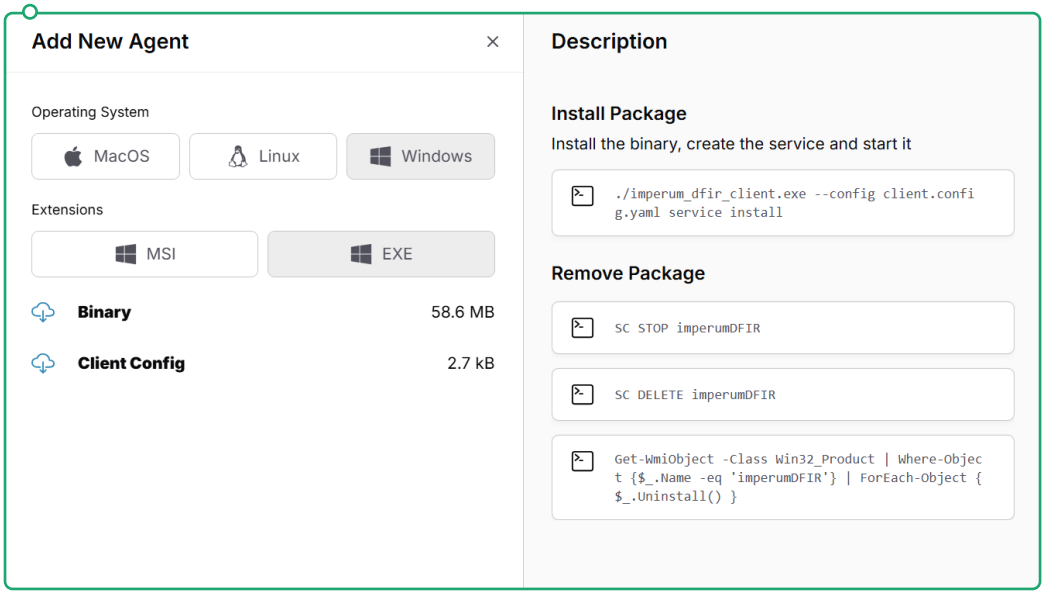
The displayed name or identifier for each agent (e.g., “Dfir1” or “ImpATD-Win10-Pvt”) allows users to quickly identify specific devices or endpoints within the system. These names often align with the hostnames or labels defined during the agent setup process.

- 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).

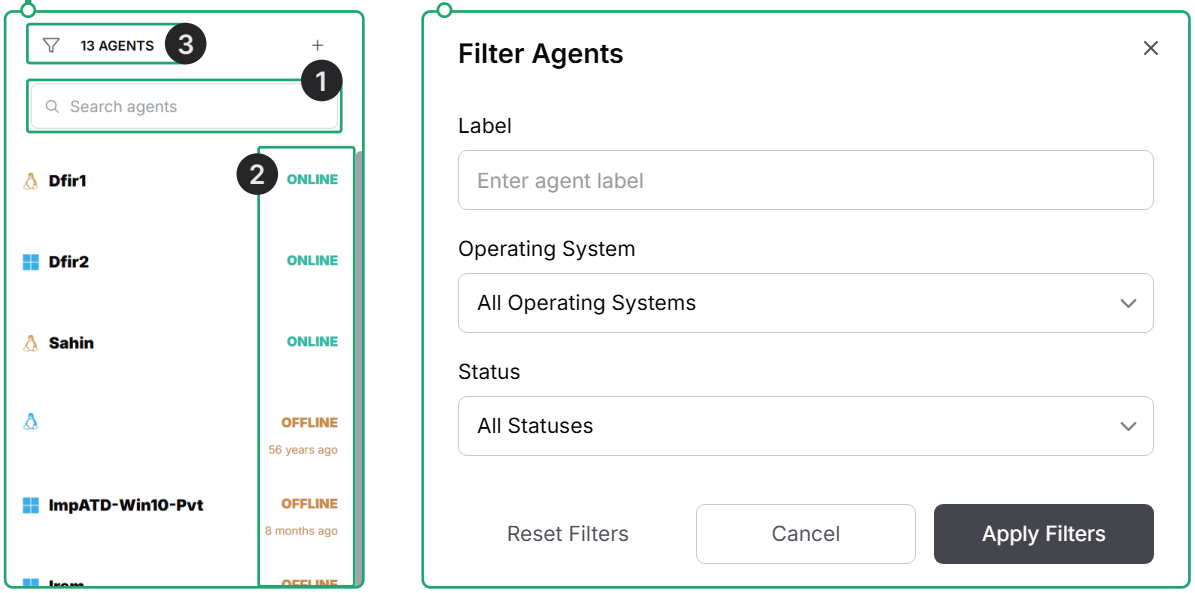
Search Functionality[2]

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]

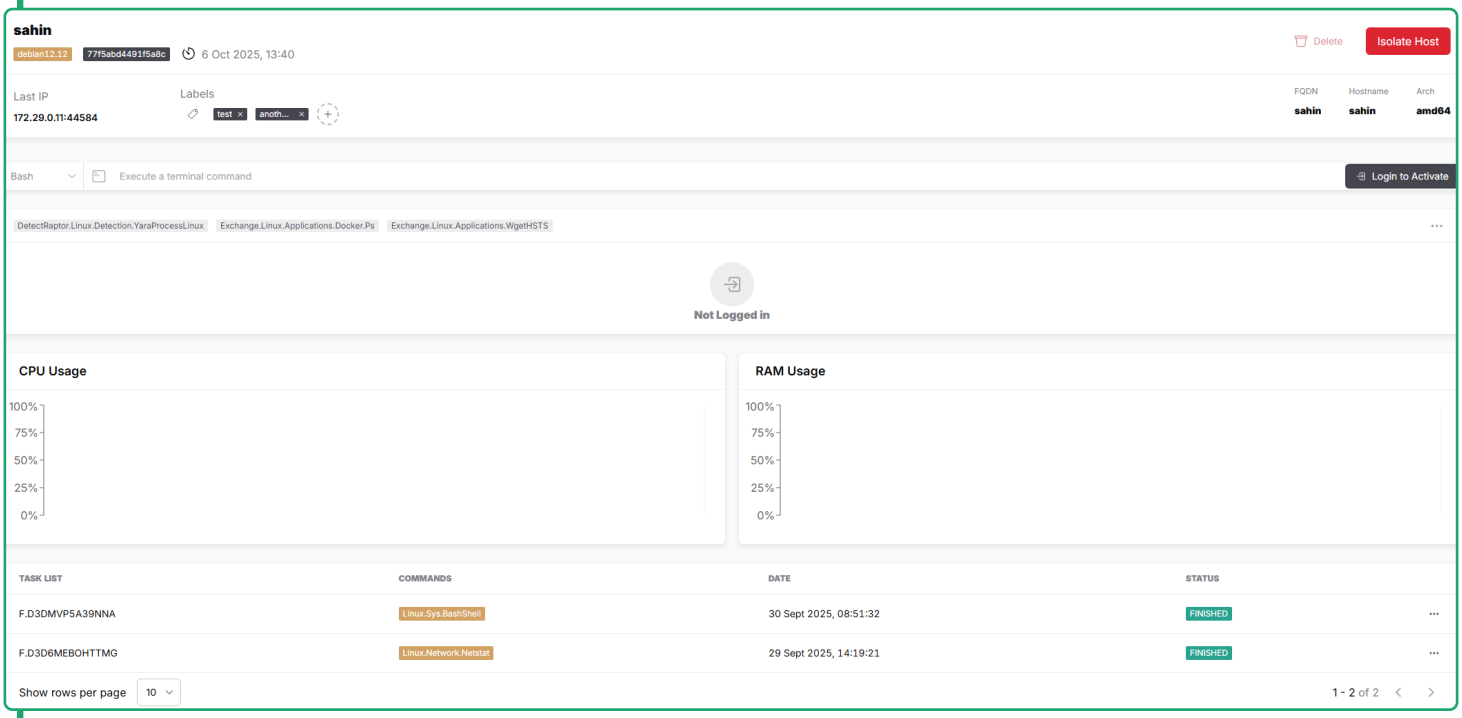
Narrow results by agent abel, operating system or status to quickly find the exact agents you need.

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.

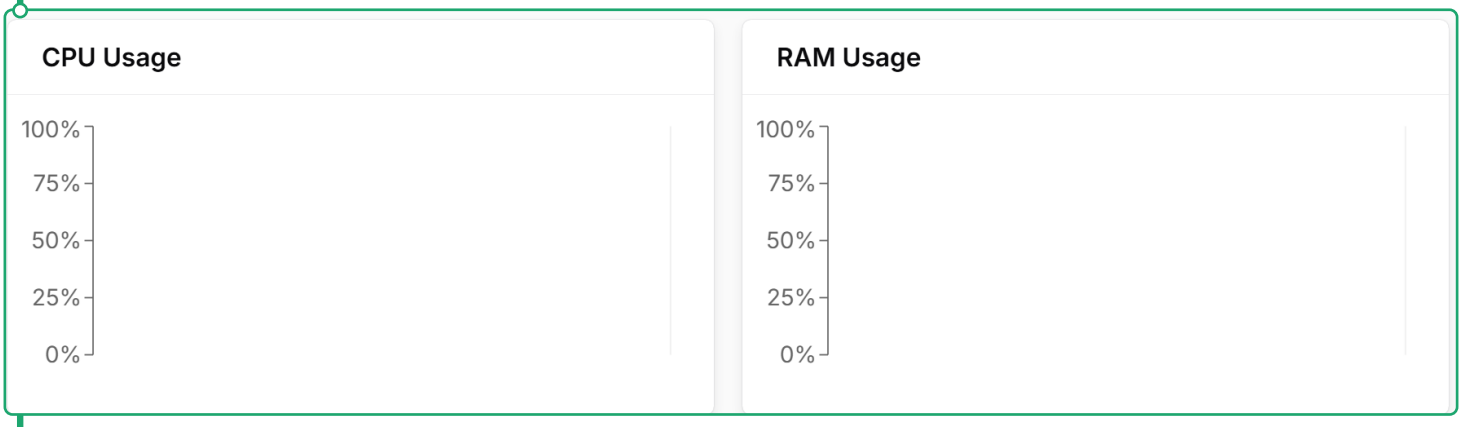


Agent Details

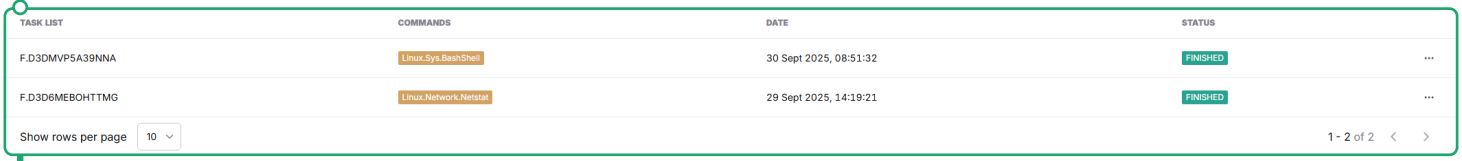
Each agent detail page provides a comprehensive overview, including:



System resource usage at a glance.



Recent command executions and their results.



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

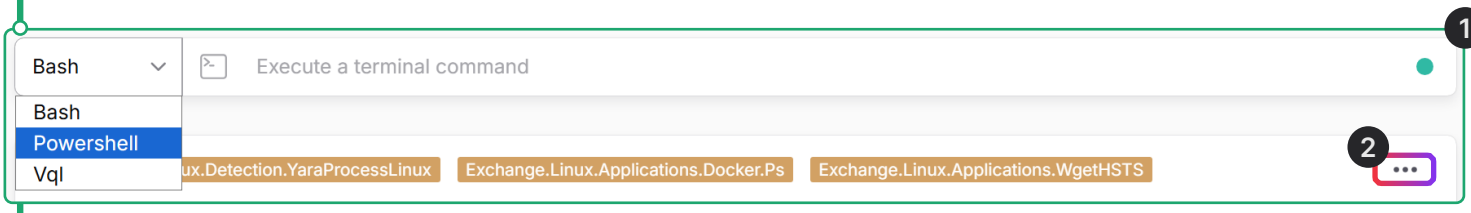
To execute terminal commands:

- Click Login to Activate to enable the interactive session

- 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]

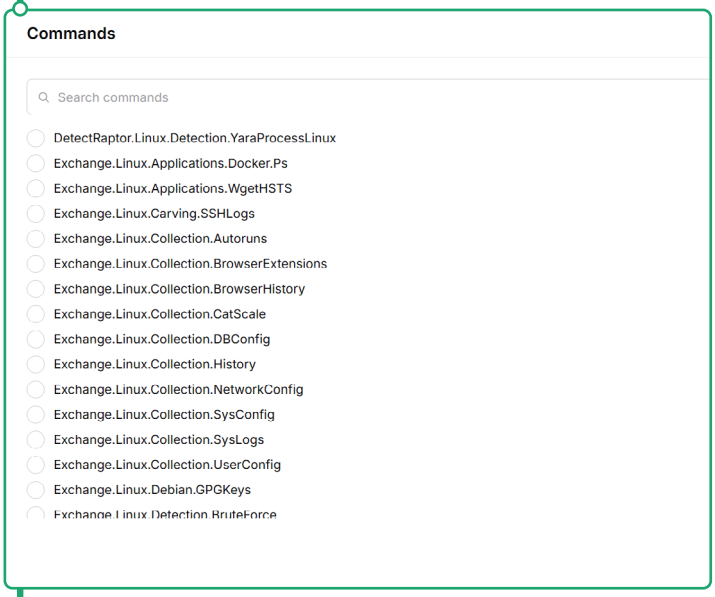
Select the desired command type (Bash, PowerShell, or VQL). Then you can create and execute your custom terminal command.

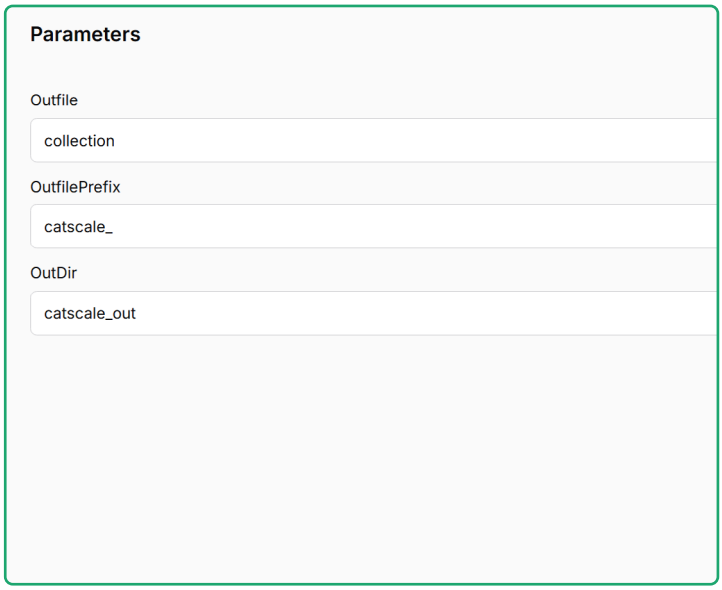


Using Predefined Command List[2]

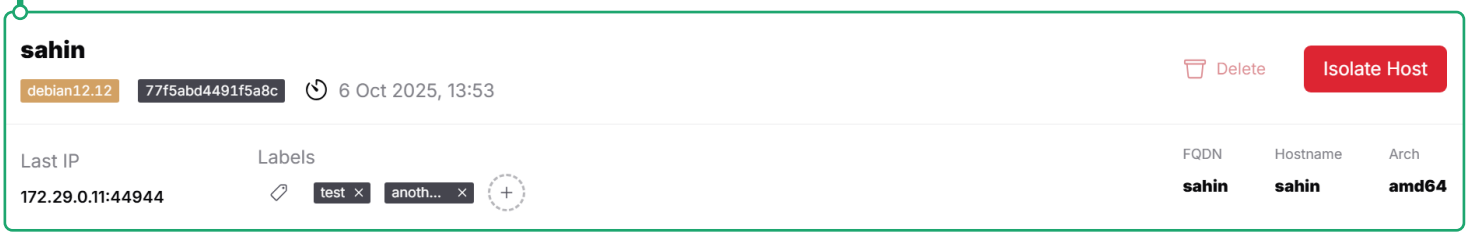
Open the predefined command list using the three-dot (...) menu. Select the desired command, provide the required parameters, and then execute command.

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





- 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.



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

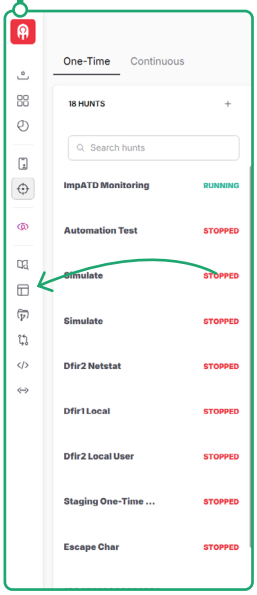
Each execution is visible in the dashboard, allowing you to track, monitor, and review results easily.

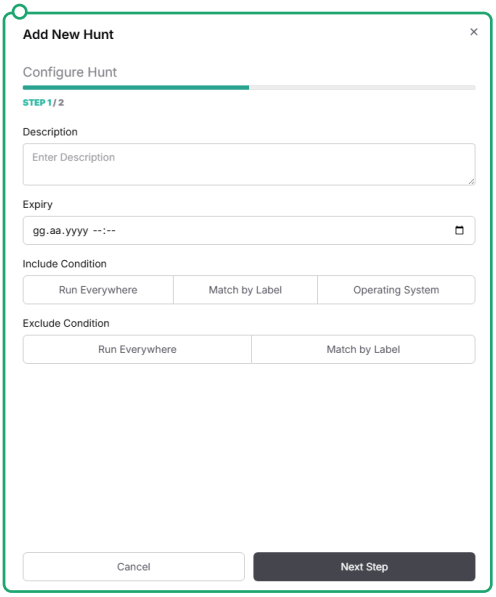
Add New Hunt

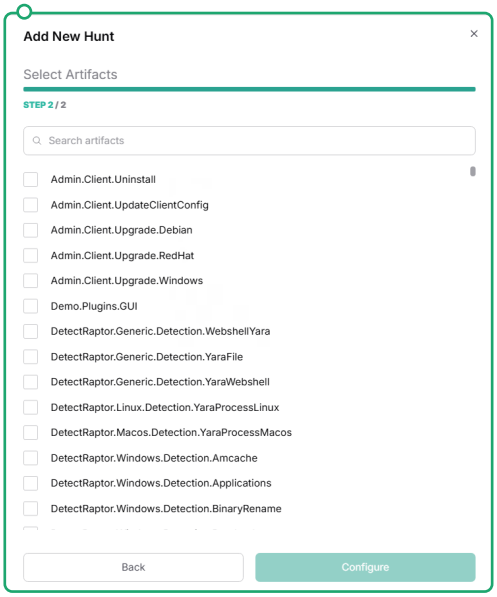
To create a hunt:

- 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.







Continuous Hunts

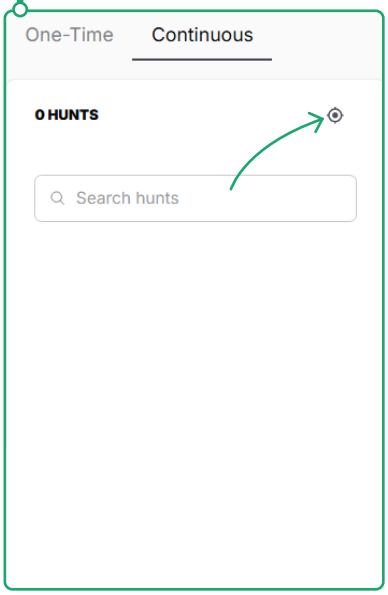
Continuous Hunts extend regular hunts with scheduling capabilities. They run automatically at defined intervals (daily, weekly, monthly, etc.), making them ideal for:

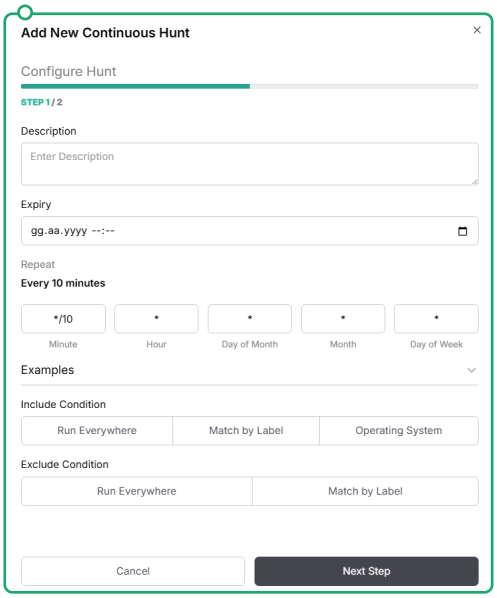
- Routine system health checks
- Recurring security audits
- Ongoing compliance verification

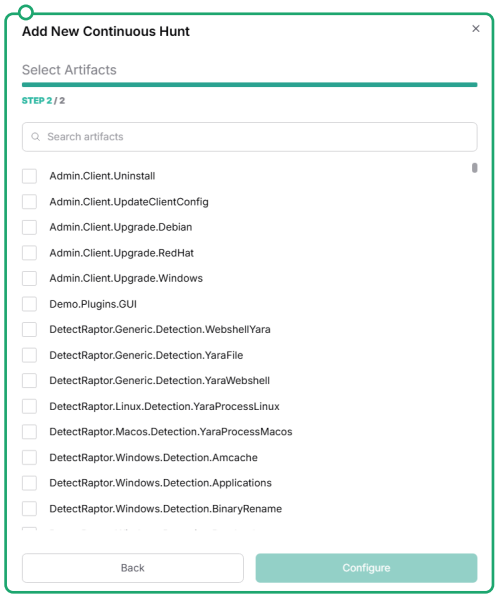
Each execution is visible in the dashboard, allowing you to track, monitor, and review results easily.

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





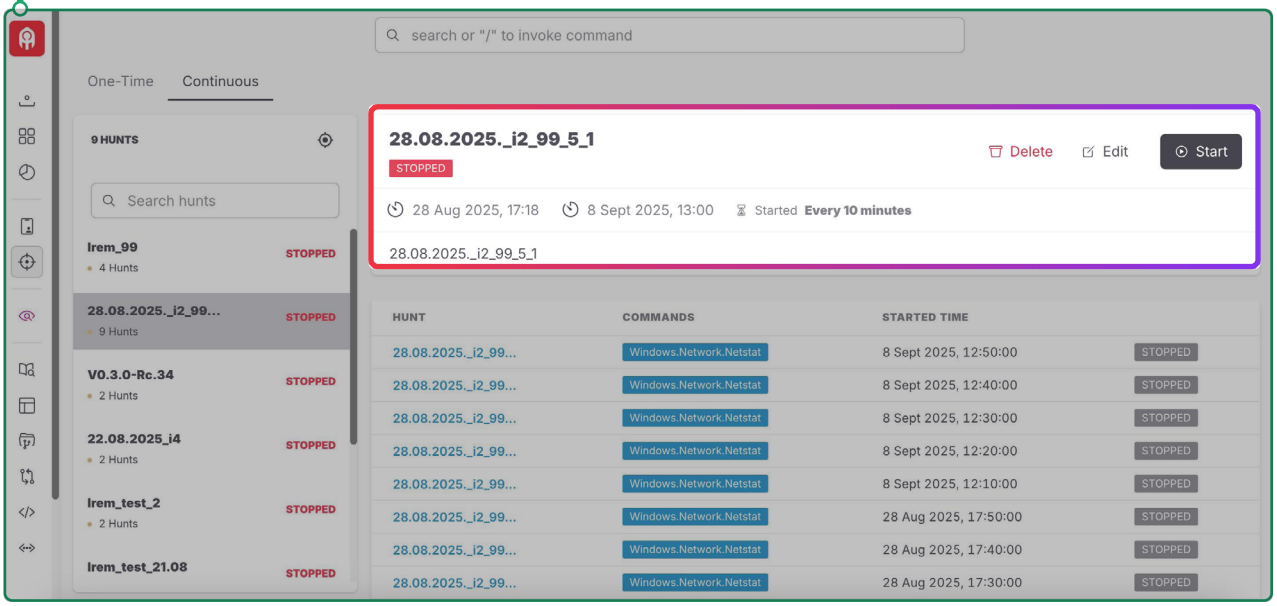


Continuous Hunts Details

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

General Information

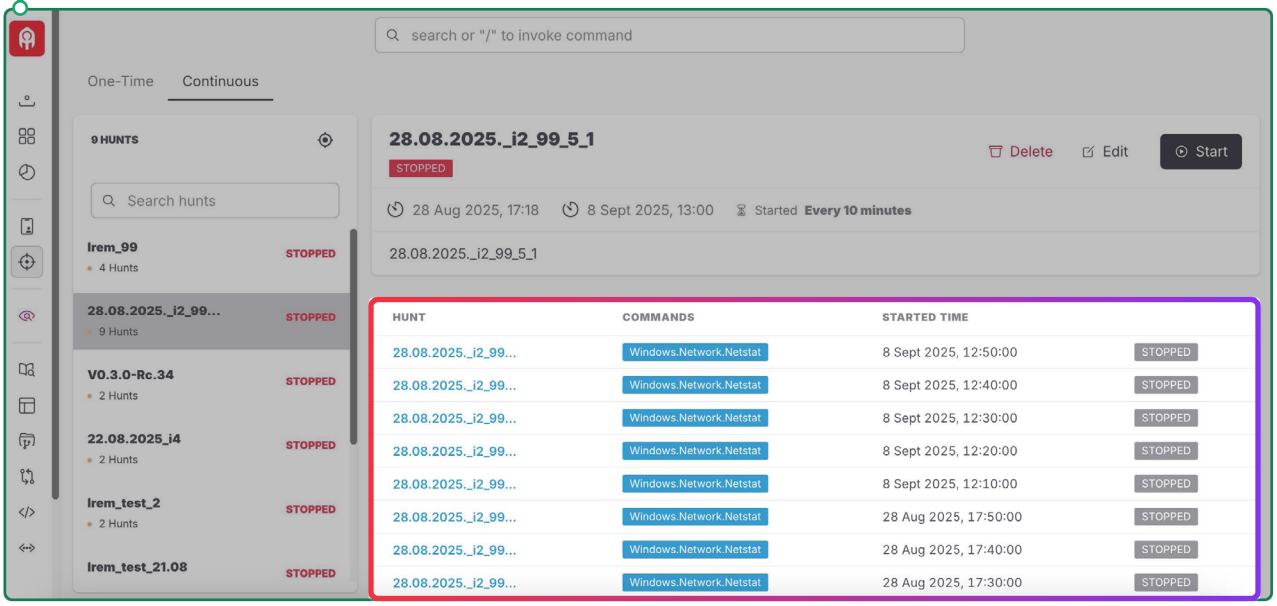
- Hunt name
- Current status (Running or Stopped)
- Start and end date/time
- Execution interval (e.g., Every 10 minutes)



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)



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.