viettel security

Viettel Endpoint Detection & Protection

(VCS-aJiant version EDP)

Documment version: 4.138 – Update: 22-Jan-2026

User Guide

Update history

No.	Update date	Version	Reason for change	Note
1	…	3.3.0		
2	June 30, 2022	3.3.20	Supplement/update instructions: 3.4.8 IRFlow Response - 73 3.6 Response - 119 3.7.5 Update management - 174	
3	October 10, 2022	3.3.31	Supplement/Update Instructions: 3.11 Anti-Malware – 247	
4	December 16, 2022	3.3.38	Supplement/update instructions: 3.5.4 Investigation_Deploy tool - 116	
5	December 28, 2022	3.3.43	Supplement/update instructions 3.6.1 Response_Live response - 154	
6	March 21, 2023	4.5.1	Add instructions for enabling 2FA.	
7	April 20, 2023	4.14.0	Update the new Agent GUI	
8	May 15, 2023	4.18.0	Add instructions for Device Control	

No.	Update date	Version	Reason for change	Note
9	December 9, 2023	4.48	- Added instructions for the Ransomware Protection feature - Updated the interface	
10	September 27, 2023	4.52	Update for feature 3.10.2 Endpoint Firewall	
11	July 15, 2024	4.52	Supplement and clarify the BLS rules.	
13	November 13, 2024	4,100	Instructions for Using Auto Scan Config in Policy	
14	December 17, 2024	4.106	User Guide for Using the Threat Hunting Feature	
15	October 6, 2025	4.110	Add the calculation method for the VCS-aJiant product license in section 3.7.1.	
16	October 7, 2025	4.115.0	User guide for the command line interface for the malware scanning feature. Section 3.17	
17	September 18, 2025	4.128.0	Add a description of the violation inspection rule for BLS Section 3.5.2.3.1.	
18	November 4, 2025	4,130.0	Add section 3.5.2 – Instructions for Using Isolate Devices Update section 3.3.4 – Do Not Display IR Flow Feature Update section 3.4.2 – Do Not Display Mark Artifacts Feature	

No.	Update date	Version	Reason for change	Note
19	November 4, 2025	4.131.0	Add a description of the malware isolation function. Section 3.14	
20	November 24, 2025	4.132.0	Update the interface of the Agent Management screen, section 3.6.1	
21	Nov 28, 2025	4.133.0	*Update 3.6.2 Policy Setting, add Performance control linux*	
22	Dec 24, 2025	4.135.0	*Add 3.4.5 Event Search V2*	
23	Dec 24, 2025	4.136.0	*Update 3.6.2 Policy Setting, add Prevention Known Threat*	
22	Dec 24, 2025	4.137.0	*Add 3.10.1 IOC Management*	
23	Jan 22, 2026	4.138.0	*Update 3.6.2 Policy Setting, add phần Fileless*	

MENU

Terminology

Terminology	Explanation	Note
VCS-aJiant	Product trade name	

Terminology	Explanation	Note
IR Flow	Incident Response Flow: the operational process for handling Alerts, investigation, and response.	
Artifact	Investigation subjects related to Alerts such as: file path/registry/process	
Detection	Detect objects related to the Alert	
Containment	Computer isolation process: network isolation, process suspension	
Investigation	Investigation process: based on event logs or proactive investigation using tools on the user's machine. The supported investigation methods include: Process Analysis, Searching event logs	
Response	Reaction process: Based on the investigation results, the operator handles the investigation outcomes using the following methods: Response Scenario, LiveResponse	
Timeline	The timeline displays activities in: Creating/closing Process Analysis sessions Creating/closing Live Response sessions	

1. INTRODUCTION

1.1 Current situation

Today, organizations and enterprises continue to face significant challenges in detecting, identifying, investigating, and mitigating advanced forms of malware within their systems. Traditional anti-malware technologies, such as signature-based antivirus, are being deliberately bypassed by highly skilled professional attackers

using advanced attack toolkits, customized malware, and targeted approaches. Many organizations have acknowledged that their traditional malware defense methods have failed, and a new strategy must be developed to identify these breaches at the endpoint. A substantial number of recent data breaches involving advanced malware have increased customer interest in Endpoint Detection and Response (EDR) solutions, among which VCS-aJiant is one.

1.2 The development of technology

The technology of the VCS-aJiant Solution addresses the shortcomings of signature-based technologies currently used by organizations, such as antivirus or IPS/IDS, by providing behavior-based anomaly detection and deeper insights into relevant specific information on endpoints to detect and mitigate advanced threats.

1.3 VCS-aJiant

VCS-aJiant is capable of providing detailed information about malware infections and the lateral movement behaviors of attackers as they conduct scanning or use stolen information within the internal network targeting systems and applications.

In addition, VCS-aJiant also complements existing security technologies such as Security Information and Event Management (SIEM) solutions, Network Forensics tools, and Advanced Threat Detection devices, thereby enhancing the organization's portfolio of information security incident response solutions.

2. OVERVIEW

2.1 Technology

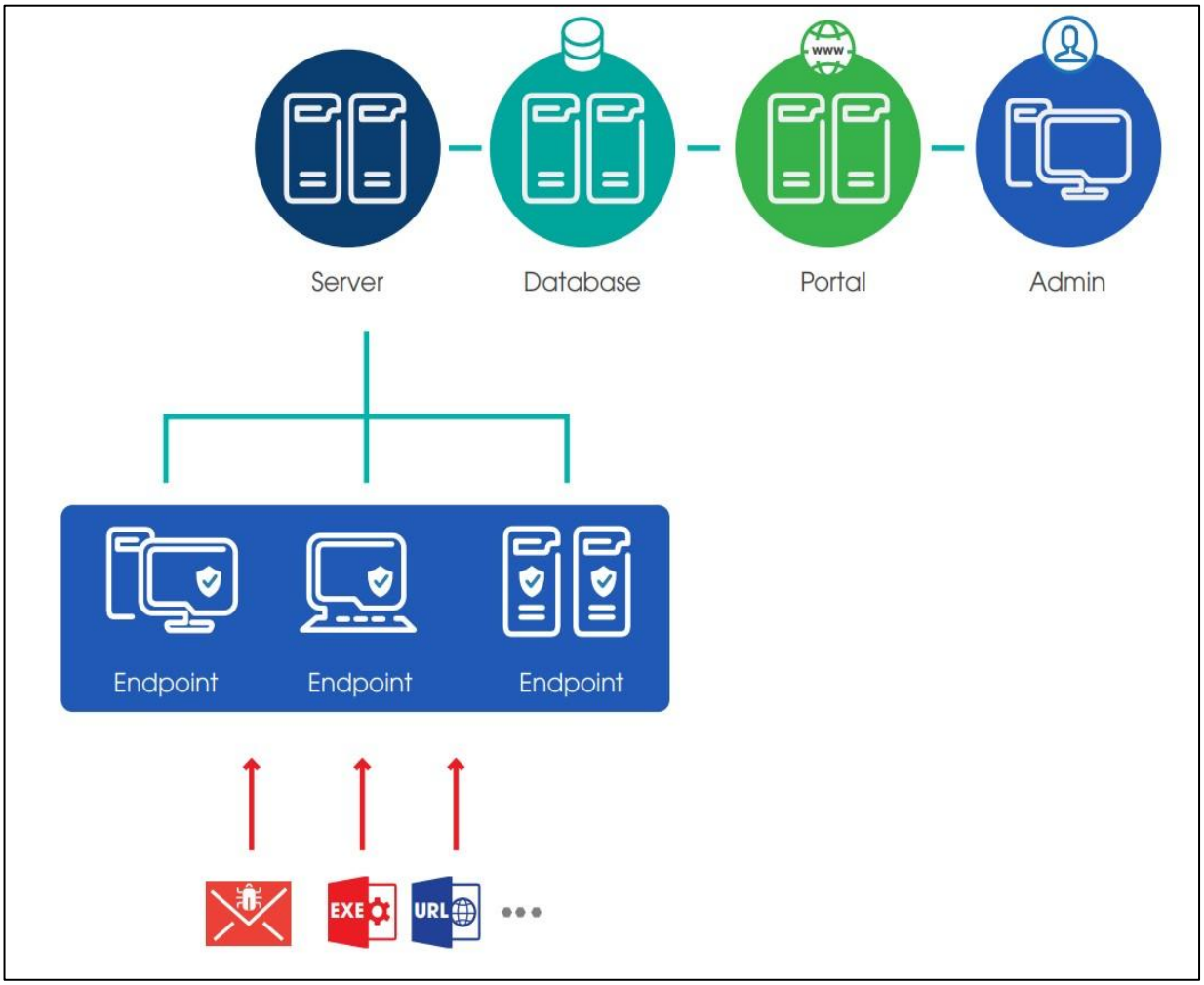
VCS-aJiant uses Filter Driver technology (allowing operation and monitoring at the Kernel-based level) to collect information including Files, Processes, Registry, and Network activities on user computers and servers. File indicators include modifications, deletions, and attribute changes; registry indicators include deletion of keys/values, setting values, renaming keys/values, and creating keys with suspicious access. Suspicious memory indicators are continuously and periodically scanned.

Behaviors identified as suspicious are sent to a centralized Back-end system for analysis.

The attack investigation workflow is designed as a closed loop following the incident response scenario, supporting the detection and analysis of anomalies within a single interface. It provides deep forensic investigation functions on the Endpoint. It supports suspicious file retrieval (Get Artifact), tool deployment for scanning (Tool Deployment), enables investigation and real-time evidence collection (Process Analysis, Live Response), and allows for response actions upon threat detection.

As soon as an anomaly is detected, the Endpoint provides tools for large-scale malware removal (Response Scenario), including network containment of the infected machine, process termination, and deletion of files/registry entries.

2.2 Infrastructure architecture



There are three main components:

Agent: A component installed on each workstation and server, responsible for monitoring abnormal signs on workstations and servers, and sending logs to the centralized management server;

The server cluster for management, centralized processing, and storage: This component processes data sent from agents and plays a key role in real-time data analysis and processing;

Web-Portal Interface: This is the component that administrators use to monitor, supervise, and analyze the system's information.

2.3 Working with the administrative interface

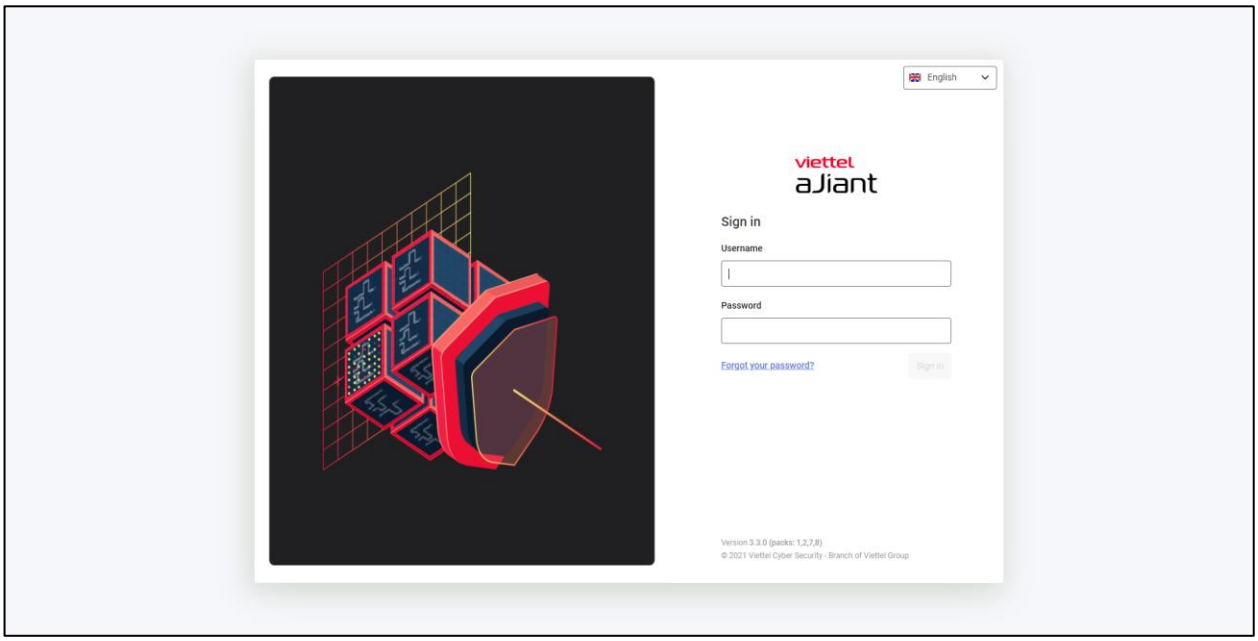
The Web-portal interface includes functional interfaces and processing flows as follows:

Dashboard: statistics and visual charts on the organization's information security status;
Alert management: a list of alerts regarding signs of malware presence on user devices;
Investigation: list of tools for investigation (Process Analysis, Event Search, and Deploy Tools);
Response: list of tools for live response and incident handling;
Protect & Prevention: list of workstation protection and prevention features (Application control and Endpoint firewall);
Setting: list of system configuration functions (Policy management, Agent management, Group management, Rule correlation, and Account management: User, Role, Permission management);

3. USER MANUAL

3.1 Log in

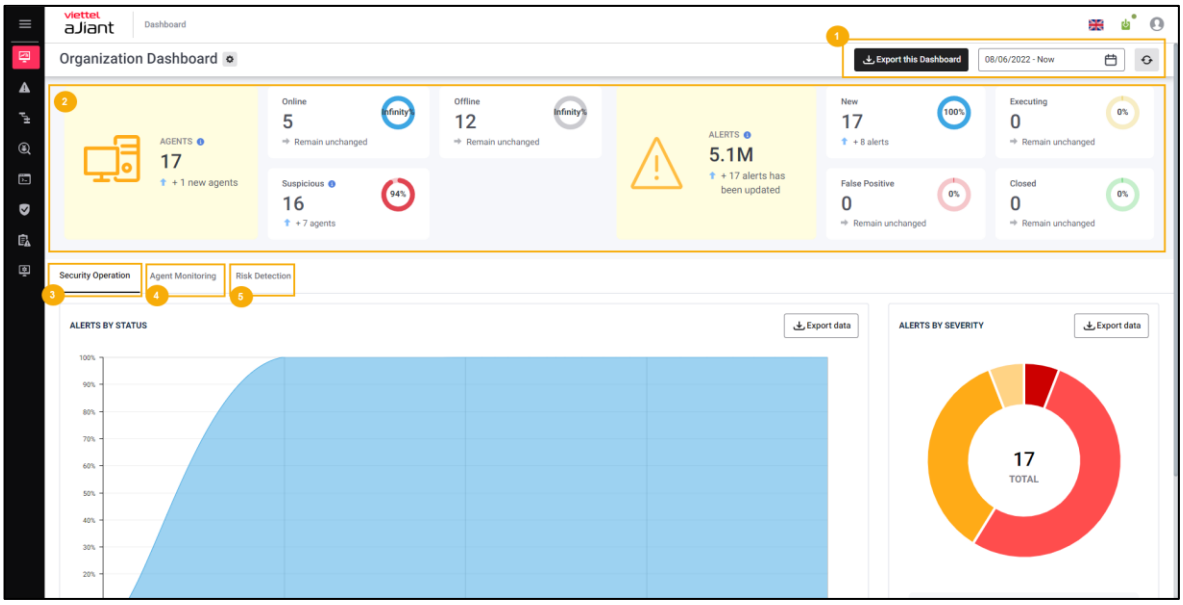
- Access the system at the provided address;



- Log in with the provided username/password;

3.2 VCS-aJiant Dashboard

The main features include:



1 – Data operations on the Dashboard:

Data extraction on the dashboard;

Search data for up to the past 90 days;

Refresh the data.

2 – Overview: Summary statistics of the organization's information security status (based on agent status and alerts);

3 – Security Operation: Monitoring the status of information security operations (through alert operation monitoring);

4 – Agent Monitoring: Monitoring the installation status and condition of agents;

5 – Risk Detection: Monitoring threats to the organization (by tracking entities generating the highest number of unresolved alerts in the system);

Data permissions in the feature are as follows:

User logged in as root group: Display data for the entire system;

User login belongs to level 1 group: Display data for the entire level 1 group and all its subordinate subgroups;

Users logging in belonging to group level 2 or higher: Display data for all level 1 groups containing the user's group and the subgroups directly under the corresponding level 1 group.

3.2.1 Data manipulation

Export data

Purpose: To enable the extraction of existing data on the dashboard interface by selection, as well as to add detailed data sheets to support reporting;

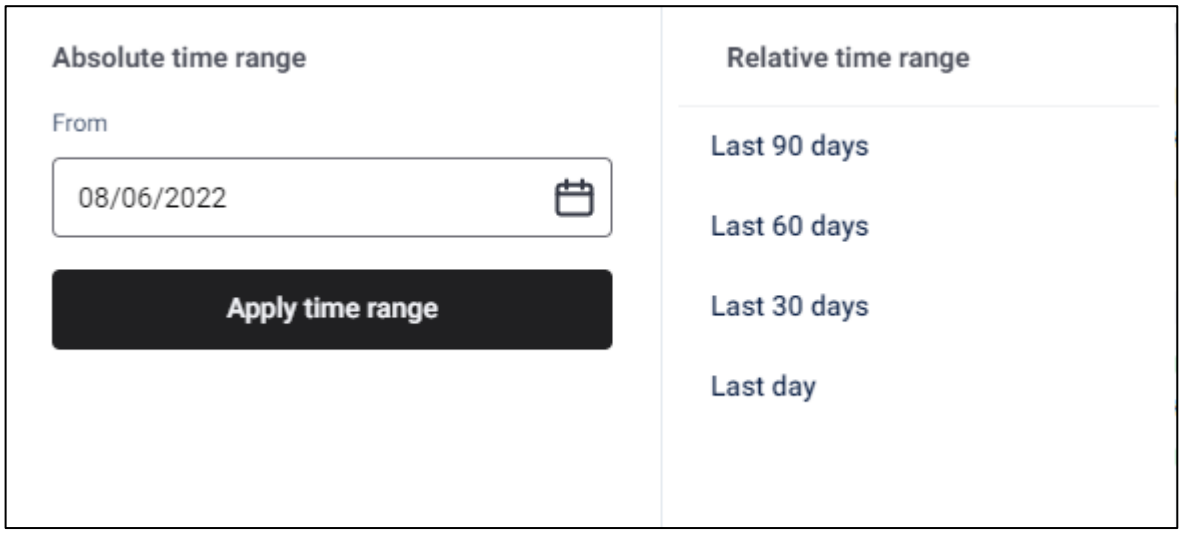
In cases of connection errors or no data across all components of the Dashboard, extraction and operations will be disabled and hidden;

In cases where data is available, support exporting files in .xlsx format;

Search by date

Allows adjustment of the time period for monitoring information security status up to the current time, with the default set from the previous day (Last day);

To select the start time of the monitoring period, you can choose either an absolute or a relative time:



- Absolute time: A specific start date value, supporting up to 90 days from the current date;

Example: It is currently 3:00 AM on June 7, 2021, with the start date selected as "06/06/2021."

Monitoring period: 00:00 on 06/06/2021 to 03:00 on 06/07/2021.

- Relative time: The relative time interval between the start date and the present.

Example: It is currently 3:00 AM on June 7, 2021. Selecting the start date as "Last 30 days" will prompt the system to automatically look back 30 days and begin counting from 00:00 of that day.

Monitoring period: 00:00 on 08/05/2021 to 03:00 on 07/06/2021.

After selecting the desired time period to monitor, choose to reload the corresponding data.

Refresh data

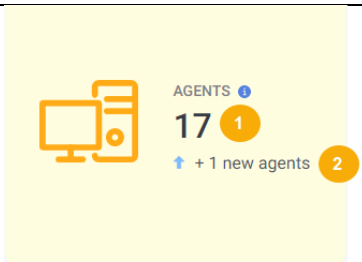
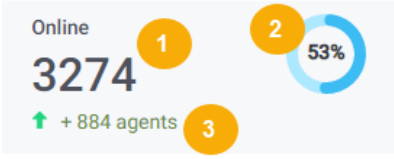
Purpose: Allows manual data refresh; select to update the data to the most current available at the present time.

3.2.2 Statistics Overview

Purpose: To enable quick statistics on the organization's information security status within the selected time period in the search section;

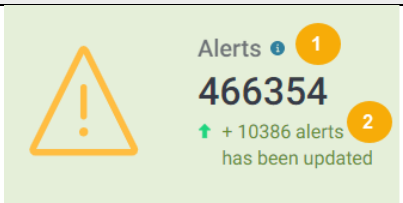
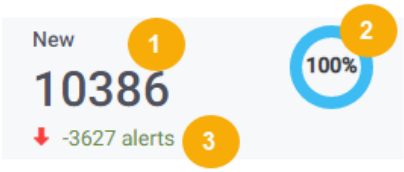
Statistics related to agents:

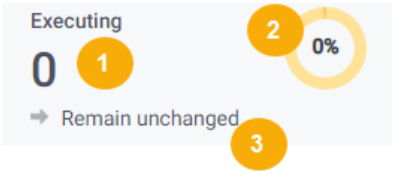
Statistics	Meaning

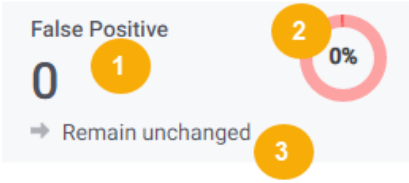
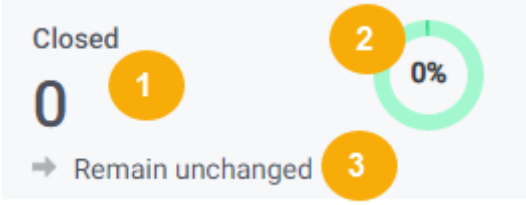
	Includes 2 indicators: - Total number of machines with the agent installed on the system (regardless of the search time period); - Total number of machines newly installed with the agent during the search time period; (+: Newly installed machines, Remain unchanged: No new machines installed during the search time period)
	Includes 03 indicators: - Average number of online machines during the search period (counting only working hours from 08:00 to 18:00); - Average online machine rate compared to the entire system; - Average difference in the number of online machines compared to the previous cycle. (+ indicates an increase in the average number of online machines compared to the previous period, Remain unchanged: No difference)
	Includes 03 indicators: - Average number of offline machines during the search period (counting only working hours from 08:00 to 18:00); - Average offline machine rate compared to the entire system; - Average difference in the number of offline machines compared to the previous cycle. (+ indicates an increase in the average number of offline machines compared to the previous period; Remain unchanged: No difference)

	Includes 03 indicators: - Total number of machines with agents installed on the system (regardless of the search time period) that have generated unprocessed Alerts; - The ratio of machines with Alerts to the total number of machines in the entire system (regardless of the search time period); - Total number of machines that generated Alerts within the search time period. (+: Newly generated Alert machines, Remain unchanged: No new Alert machines generated within the search time period)

Statistics related to Alerts:

Statistics	Meaning
	Includes 2 indicators: - Total number of Alerts across the entire system (regardless of the search time range); - Total number of new Alerts generated or updated within the search time range; (+: New Alerts generated, Remain unchanged: No new Alerts generated within the search time range)
	Includes 03 indicators: - Total number of new Alerts generated or updated within the search period and currently in the NEW status; - Ratio of new Alerts generated or updated within the search period and currently in the NEW status compared to the total number of Alerts generated or updated within the search

	period; - Difference in the total number of new Alerts generated or updated within the search period and currently in the NEW status compared to the previous cycle. (+ indicates an increase in the total number of new Alerts compared to the previous period; Remain unchanged indicates no change in the total number of new Alerts compared to the previous period)
	Includes 03 indicators: - Total number of new Alerts generated or updated within the search period and currently in the status <> (NEW, FALSE POSITIVE, CLOSED); - Ratio of new Alerts generated or updated within the search period and currently in the status <> (NEW, FALSE POSITIVE, CLOSED) compared to the total number of new Alerts generated or updated within the search period; - Difference in the total number of new Alerts generated or updated within the search period and currently in the status <> (NEW, FALSE POSITIVE, CLOSED) compared to the previous cycle. (+ : Total number of Alerts increased compared to the previous period, Remain unchanged: Total number of Alerts remained the same compared to the previous period)

	Includes 03 indicators: - Total number of new Alerts generated or updated within the search period and currently in the CLOSED status; - Ratio of new Alerts generated or updated within the search period and currently in the CLOSED status compared to all new Alerts generated or updated within the search period; - Difference in the total number of new Alerts generated or updated within the search period and currently in the CLOSED status compared to the previous cycle. (+ : Total number of Alerts increased compared to the previous period; Remain unchanged: Total number of Alerts remained the same compared to the previous period)
	Includes 03 indicators: - Total number of new Alerts generated or updated during the search period that are in the status = FALSE POSITIVE; - The ratio of new Alerts generated or updated during the search period with status = FALSE POSITIVE compared to the total number of new Alerts generated or updated during the search period; - The difference in the total number of new Alerts generated or updated during the search period with status = FALSE POSITIVE compared to the previous cycle. (+ : Total Alerts increased compared to the previous period; Remain unchanged: Total

	Alerts remained the same compared to the previous period)

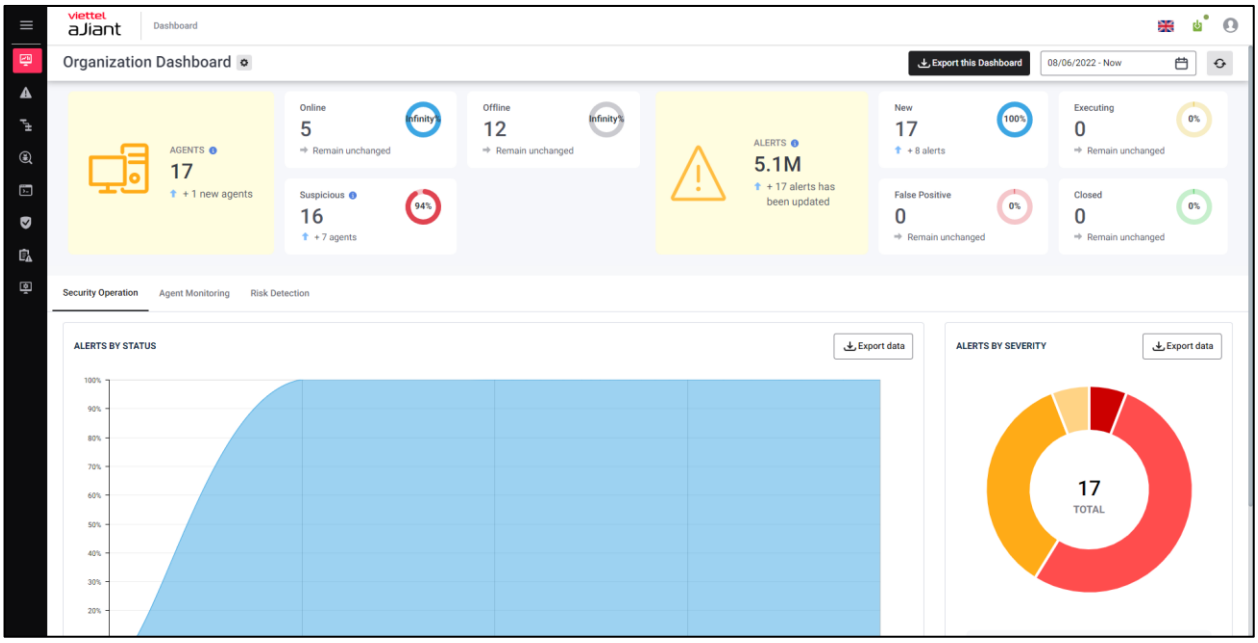
3.2.3 Security Operation Monitoring

Purpose: To enable monitoring of information security operations (through Alert operation tracking) within the selected time period in the search section.

Statistics on Alert handling status by state;

Alert statistics by severity level;

Extract the corresponding data in the charts;



Chart/Statistics	Meaning
Alert by status	Area Chart - Tracks the status of newly recorded or updated Alerts within the search period, including: X-axis: time; Y-axis: Alert rate divided into 4 status groups = (New, Executing, Closed, False Positive); Allows selection to download the Alert list sorted by status.
Alert by severity	Pie Chart - Monitoring the status of newly recorded or updated Alerts by severity level within the search period, including: Ratio: the proportion of Alerts at each severity level; The center of the chart displays the total number of new or updated Alerts during the period; Allows selection to download the list of Alerts sorted by severity level.

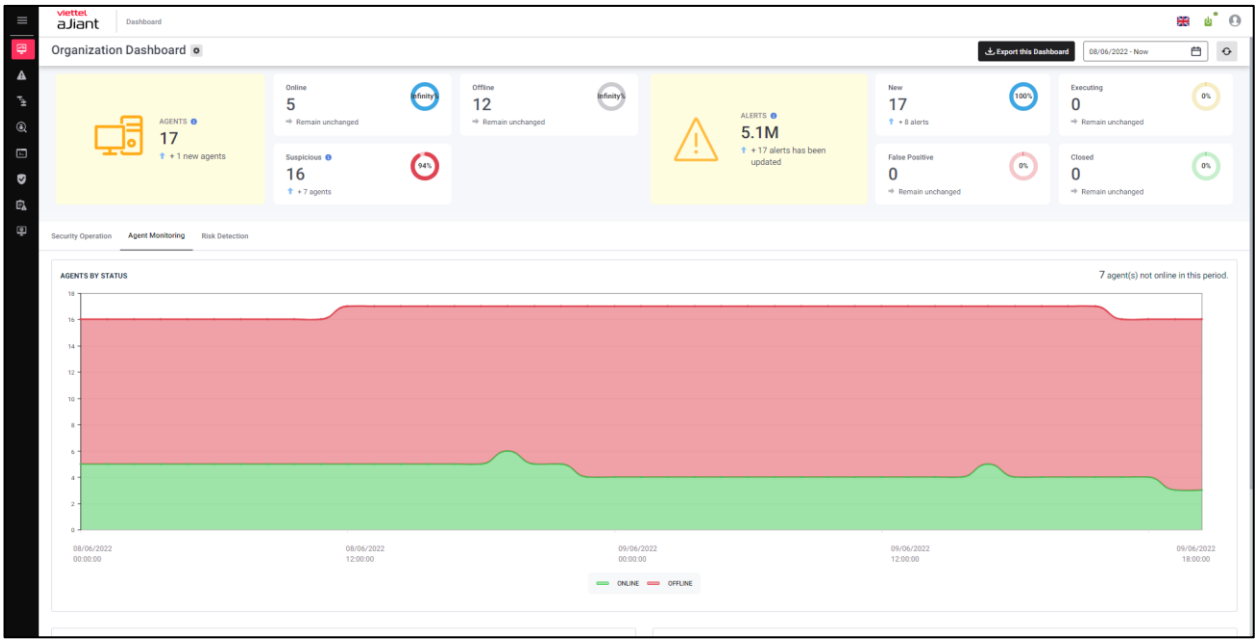
3.2.4 Agent Monitoring Tracking

Purpose: To allow the statistics of agents by status and operating system information within the selected time range in the search section.

Agent status statistics (Online, Offline);

Statistics of agents by operating system and operating system version;

Extract agent information data;



Chart/Statistics	Meaning
Agent by status	Area Chart - Monitoring the status of machine recordings (Online/Offline) during the reporting period up to the current time, including: Y-axis: Percentage of machines divided into 2 status groups (Online, Offline); X-axis: Statistical time; Displays the number of machines that have never been online (in cases where a machine has not been online for more than 30 days, it is automatically excluded from the records).
Agent by operating system	Pie Chart - Monitoring the recording status of devices by OS, including: Ratio: the proportion of devices for each OS; The notes section lists the operating systems: Windows, MacOS, Linux, and other operating

	systems; Allows selection to download the device list sorted by operating system information.
Agent theo phiên bản hệ điều hành	Statistics of the most installed operating system versions on devices; Allows changing the statistical range: Top 5, Top 10, Top 20, Top 50. Default selection is Top 5.

3.2.5 Monitor Risk Detection

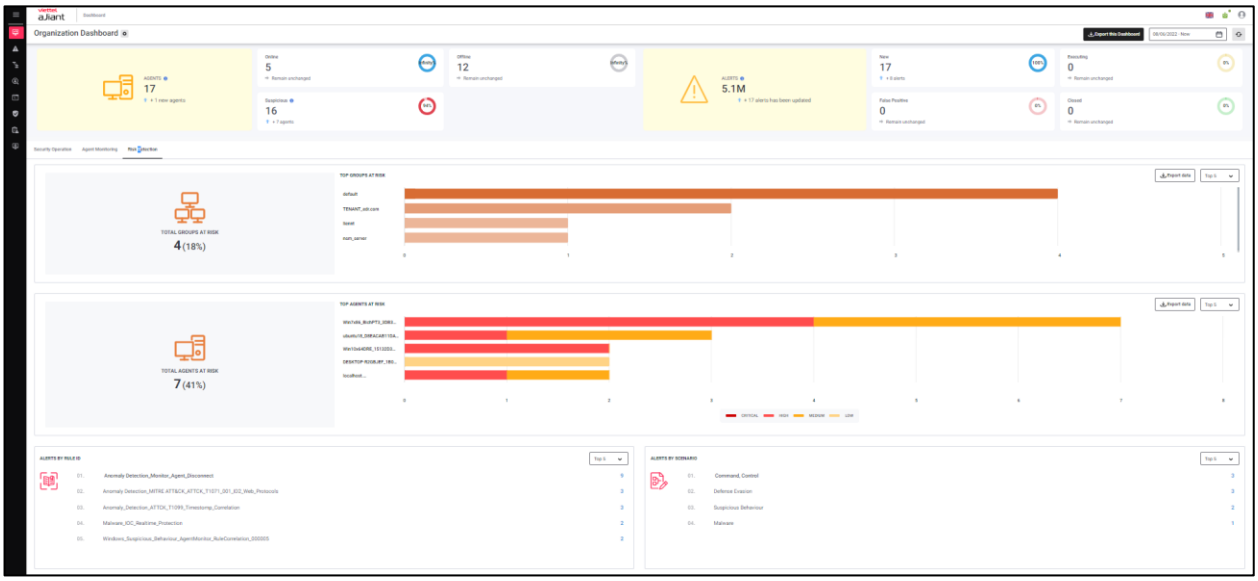
Allows monitoring of hazards to the organization (by tracking the entities generating the highest number of unresolved alerts in the system):

Statistics of the top groups generating the most Alerts;

Statistics of top agents generating the most Alerts;

Statistics of the top rule IDs and scenarios generating the most bsao alerts;

Extract data information according to hazardous objects;

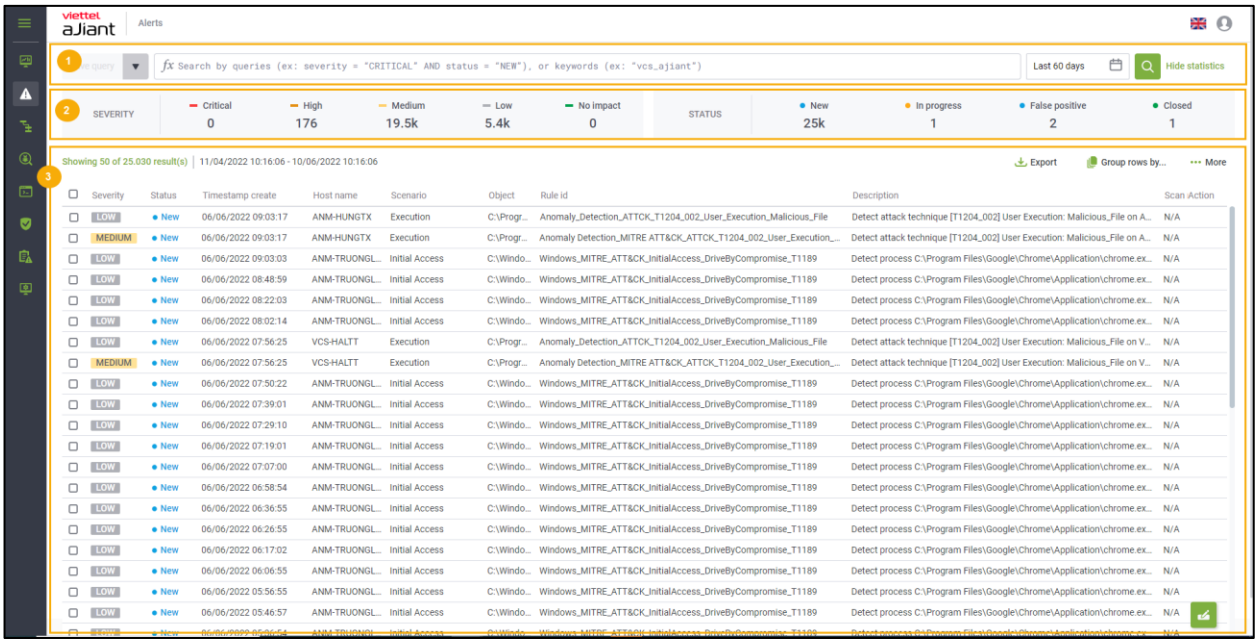


Chart/Statistics	Meaning
Total groups at risk	The total number of groups containing computers with newly recorded or updated Alerts (excluding false positive and closed Alerts, and excluding deleted groups) during the search period; The proportion of suspicious groups compared to the total number of groups in the system (excluding deleted groups).
Top groups at risk	Column chart – statistics of top groups containing the highest number of computers generating new or updated Alerts (excluding false positives and closed Alerts, and excluding deleted groups) within the search period; X-axis: number of computers generating Alerts in each group; Y-axis: corresponding group names; Allows changing the statistical range: Top 5, Top 10, Top 20, Top 50. Default selection is Top 5; Allows downloading the list of computer groups generating Alerts.
Total agents at risk	Total number of computers with newly recorded or updated Alerts (excluding false positives and closed Alerts, and excluding computers inactive for more than the past 30 days) during the search period; Ratio of suspicious computers to the total number of computers in the system (excluding computers inactive for more than the past 30 days).
Top agents at risk	Bar chart – statistics of the top computers generating the most newly recorded or updated Alerts

	(excluding false positives and closed Alerts) during the search period; X-axis: number of Alerts per host, clearly divided by severity levels = (Critical, High, Medium, Low) Y-axis: corresponding computer names; Allows changing the statistical range: Top 5, Top 10, Top 20, Top 50. Default selection is Top 5; Allows selecting and downloading the list of computers generating Alerts.
Alerts by RuleID	Statistics of the top rule IDs generating the most newly recorded or updated Alerts during the search period; Allows changing the statistical range: Top 5, Top 10, Top 15, Top 20. Default selection is Top 5.
Alerts by scenarios	Statistics of top Scenarios generating the most new or updated Alerts during the reporting period up to the present: Allows changing the statistical range to Top 5, Top 10, Top 15, or Top 20. Default selection is Top 5.

3.3 Alert Management

The main features include:



1 – Search data by query and time:

Search for data using query commands and utilize saved query commands;

Search data by time.

1 – Quick search;

2 – List of Alerts and actions with Alerts:

View the Alert list;

Group Alerts;

View Alert Summary;

View details of 01 Alert;

View the investigation graph;

Mark as False Positive for one/multiple Alerts;

Data permissions in the feature are as follows:

User logged in as root group: Display all Alerts in the system;

User logged in to the default group: Display all Alerts belonging to the default group;

User login belongs to parent group: Display all Alerts belonging to the user's current group and the corresponding child groups;

User logged in belongs to one or more subgroups: Display all Alerts belonging to the user's groups currently logged in;

3.3.1 Search Alert

Purpose: To allow the creation of query statements, use saved query statements, or perform quick searches to find Alerts based on the time the Alert occurred.

Search by time

By default, when accessing the system, search for Alerts from the past 7 days;
Purpose: To allow changing the time value by selecting either an absolute time or a relative time.

Absolute time: The specific start time – end time value, allowing input or selection from a calendar, supporting the date/month/year hour:minute:second format;

Relative time: The approximate duration between the start time and the current time;

Example: It is currently 3:00 AM on June 7, 2021. Selecting the start date as "Last 30 days" will prompt the system to automatically look back 30 days and begin counting from 3:00 AM on that day.

Monitoring period: 03:00 on May 8, 2021, to 03:00 on June 7, 2021.

Quick search

Purpose: To support quick Alert searches based on the following fields:

Time: Alert occurrence time;

Status: the state of the Alert;

Severity: the level of hazard of the Alert;

Scenario: Alert generation script;

Assigned to: the person assigned to handle the Alert;

Search by query sentence

1 – Use the previously saved query to perform the search;

2 – Enter the query to search;

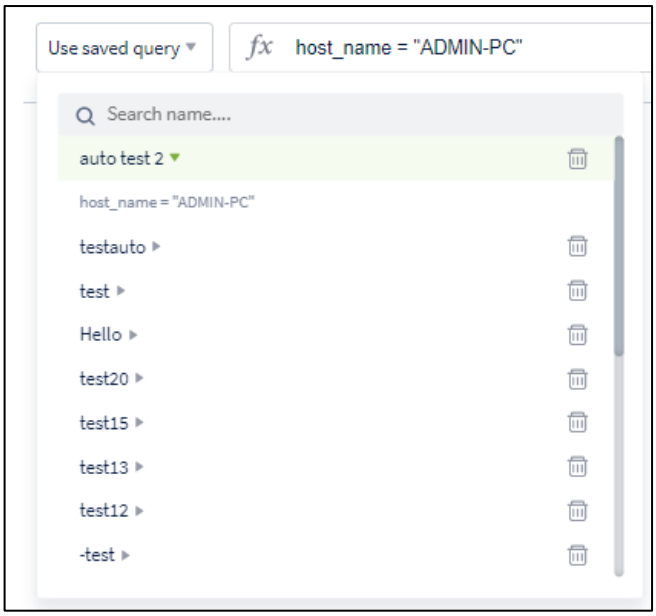
(*) Use the previously saved query to perform the search.

- Select the previously saved query from the combobox;

- Review the query content before selecting by choosing ;

-In you want to delete an old query, hover over the record you want to delete and select it;

- Click on the record you want to use for the query; the old query content will be displayed in the query input box.



➔ In case you want to add or edit the query content, you can update it directly in the query input box and select to save it.

Note: The button only appears when the query command is correctly structured.

(*) Enter the query to search:

1. Enter the query into the Search textbox using the following format:

<field_name> <operator> "<value>" AND/OR <field_name> <operator> "<value>"…..

Including:

<school_name> are the following values:

- severity: severity level of the Alert
- Alert_id: Alert code
- status: the state of the Alert
- group: event alert group
- hostname: Name of the workstation
- scenario: script generating Alerts based on MITRE ATT&CK
- assignee: the person assigned to handle the Alert
- signature_id: event code triggering Alert
- rule_id: code of law generated Alert
- description: description of the context information triggering the Alert

<operator> are the values:

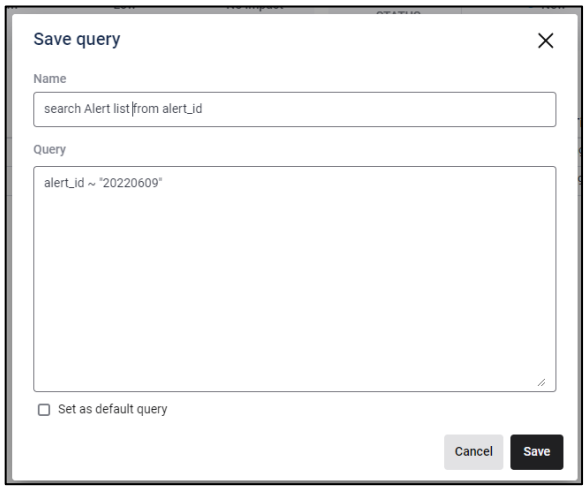
- = : find the exact value which is value
- != : find values different from value
- ~: find the value corresponding to the key 'like'
- AND/OR: operators used to combine two query statements.

2: Click the “Search” button.

In case there are no matching results, the system will display the message: No data;

In cases where matching results are found, the system displays 50 records by default in descending order by time. To view more records, scroll to the bottom of the page, and the system will load the next 50 records.

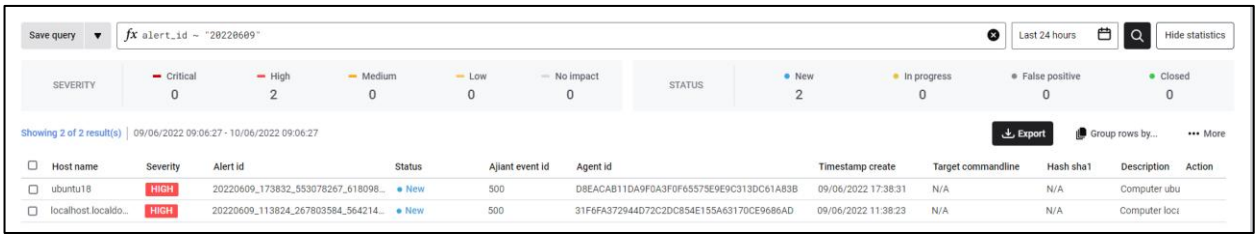
In cases where the query is correctly structured and you want to save it for future use, select and enter a memorable name for the query:



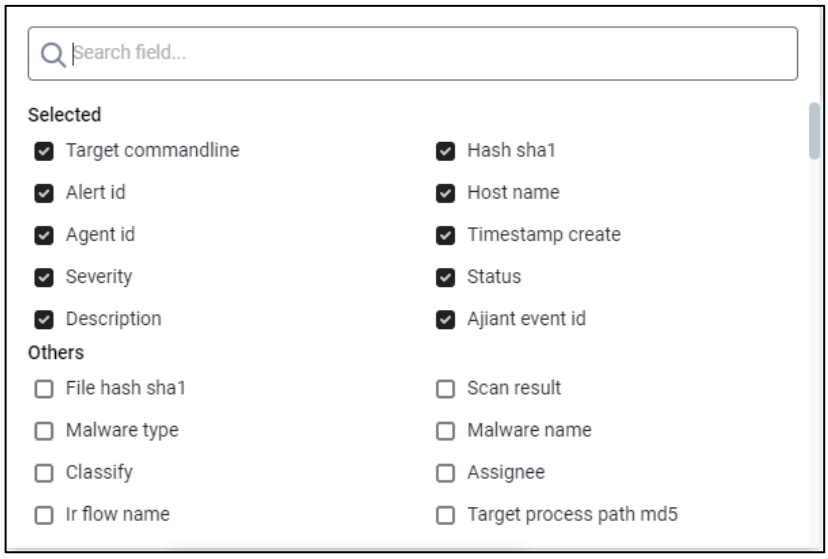
Note: The button only appears when the query command has the correct structure.

3.3.2 Alert List

Purpose: To display the list of Alerts in the system;
Allow viewing the list of Alerts that meet the search criteria.



1. Select View column to choose the fields you want to display on the Alert list:



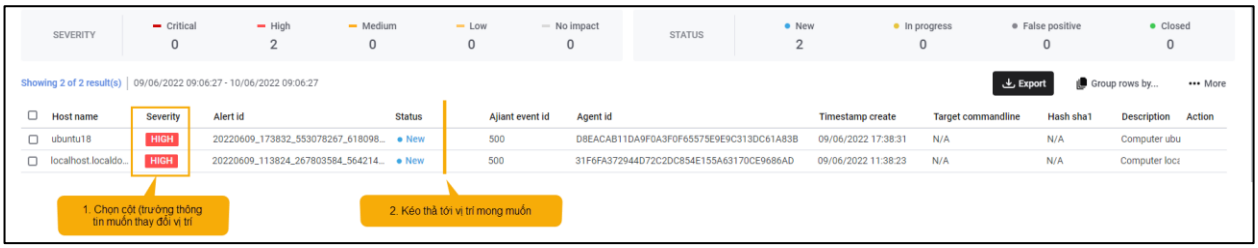
Here you can search for information fields by field name and support selecting/deselecting all fields;

2.The list supports the following operations:

Sort according to the data in each column:

Example: To sort data by the creation time field, click the field name once to sort by creation time in ascending order, click a second time to sort by creation time in descending order, and click a third time to remove sorting and return to the original state.

Drag and drop the information field to the desired position:

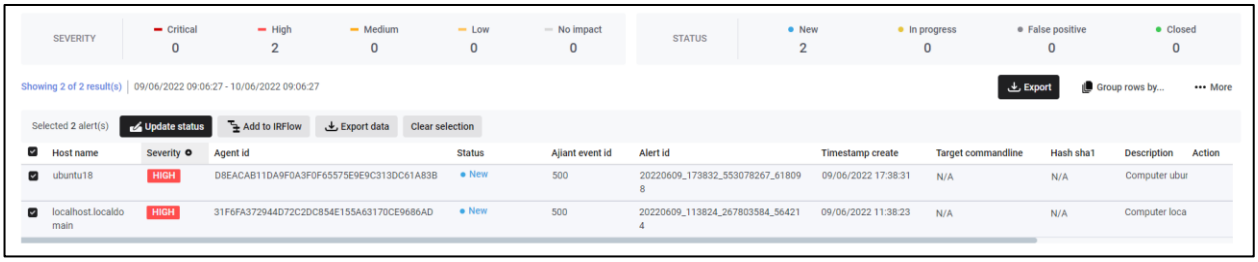


Click once to view detailed information or select and choose “View detail.” Details can be found in section 3.3.4 View Alert Details.

Select and choose “Update status” to update the status of the Alert (Update status to “False Positive” or Update status to “Close”, see the case of marking one Alert in

Select to view the reasons for marking alerts in the "FALSE POSITIVE" status as not dangerous.

1. After completing the operations on the records, you can select one or multiple records by clicking at the beginning of each Alert to continue the operations, supporting the following actions:



2. Select to update the status of the Alert:

- Select Update Status to “False Positive” to mark the Alert as non-threatening;
- Select Update Status to “Close” to close the Alert;

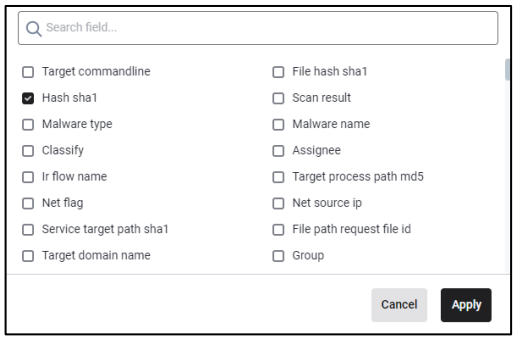
Note: This action only applies when all selected Alerts are in the "NEW" status. If at least one Alert is in a status other than "NEW," the action will be hidden. For details, see the case of marking one Alert as non-hazardous in section 3.3.5 Marking one or multiple Alerts or Alert groups as non-hazardous.

Select to extract the currently selected Alerts.

3.3.3 Group Alerts

Purpose: To allow grouping of Alerts based on one or multiple criteria: hostname, scenario, group, ruleid;

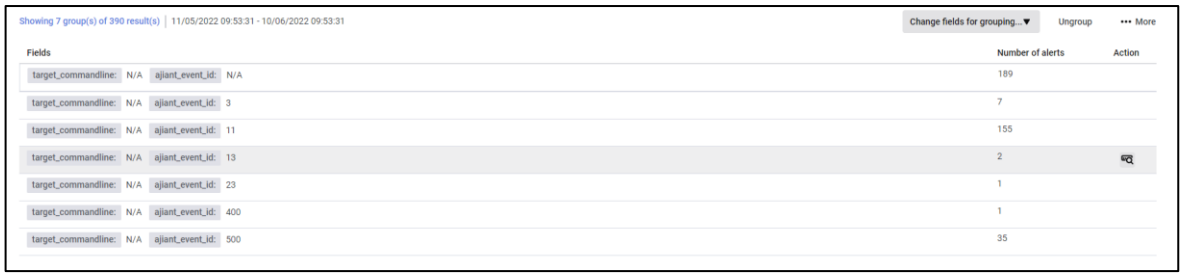
1. After searching, you can group Alerts together by selecting the criteria you want to use for grouping the Alerts;



Support searching by criterion name and selecting one or multiple criteria for grouping.

2. Select to apply.

Alerts with the same selected criteria and status will be grouped into a single line in the result list.

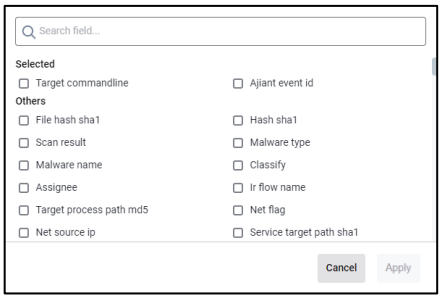


Including:

The fields used as grouping criteria will be highlighted in bold;

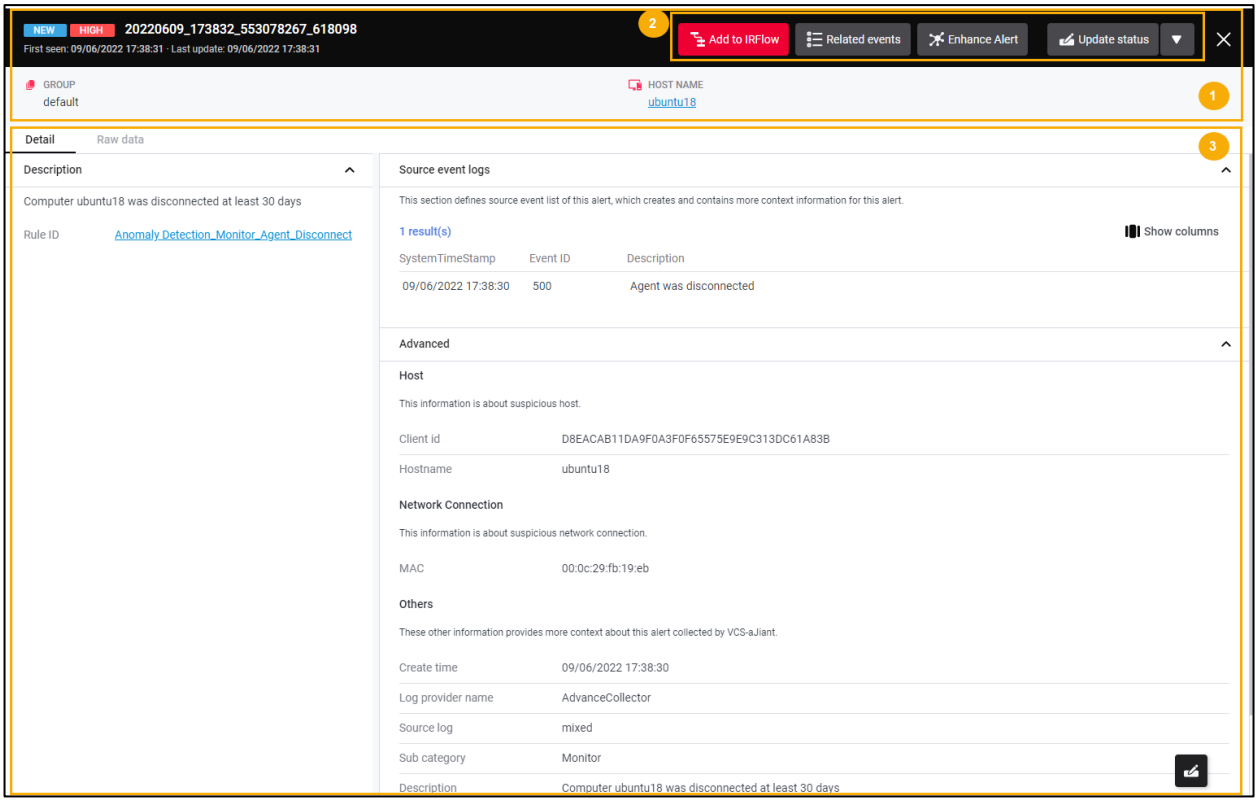
Display the number of Alerts grouped by the selected criteria.

3. To remove grouping, perform the same steps but do not select any criteria and click “Apply.”



3.3.4 View Alert Details

Purpose: To allow viewing detailed Alert information, support automatic enrichment of information by automatically collecting data on events related to the newly generated Alert, and provide visual charts for quickly viewing the relationships between objects involved in the Alert.



1 – General information group of the Alert, including:

2 –

Status: Display the status of the Alert (New, In Progress, False Positive, Closed);

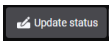
Severity: Classify Alerts according to the level of risk (Critical, High, Medium, Low);

Alert_id: Displays the Alert ID information;

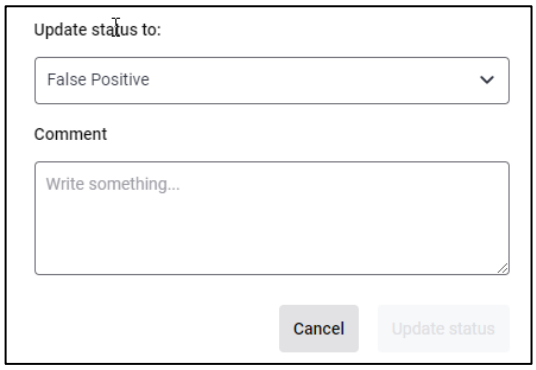
First seen: Time the alert was created;

Last seen: The most recent time the Alert was updated;

3 – Group of actions with Alert

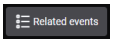
Select 

to update the status of the Alert:



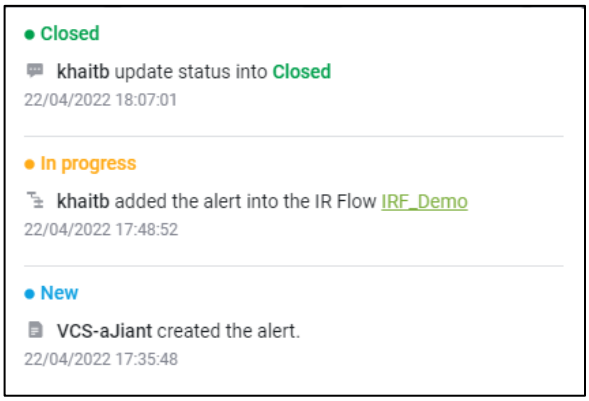
- Select Update Status to “False Positive” to mark the Alert as not dangerous;
- Select Update Status to “Close” to close the Alert;

Note: This action only applies when the Alert is selected with the status = "NEW"; the action will be hidden otherwise. For details, see the case of marking one Alert as non-hazardous in section 3.3.5 Marking one/multiple Alerts or Alert groups as non-hazardous.

Select 

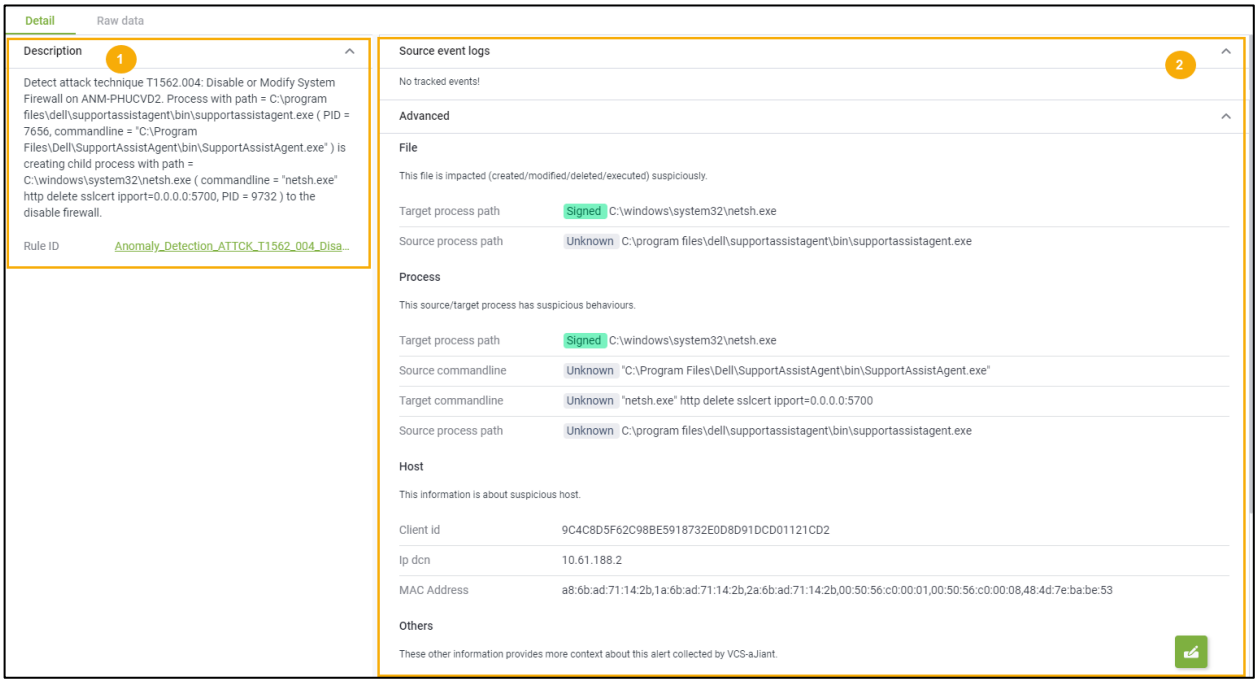
to navigate to the Event Search feature with the default time set to 4 hours before and after the Alert occurrence time;

Select  to view activity logs related to Alerts;



4 – Tabs containing information related to Alerts:

Tab Detail: Allows displaying all detailed information related to the Alert;

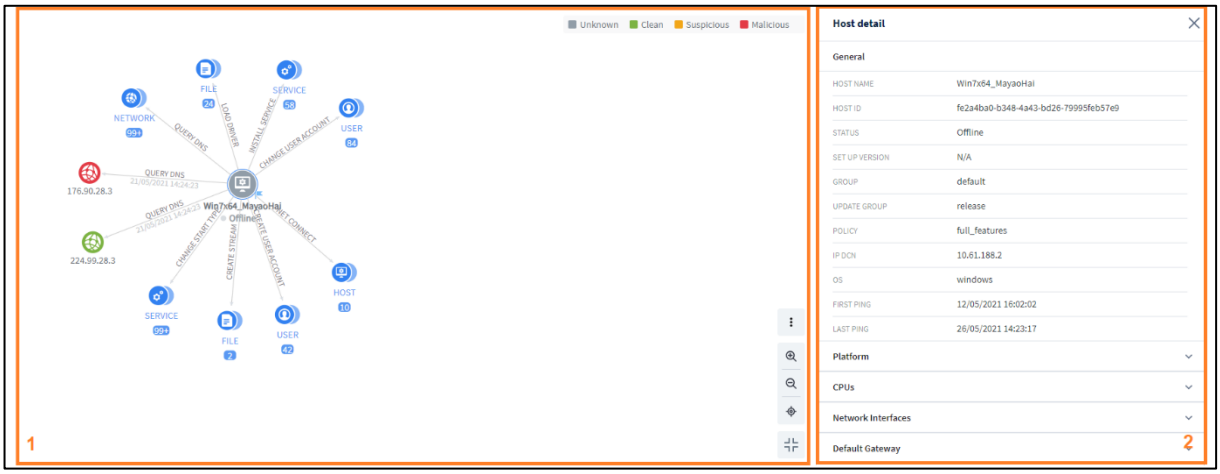


- Information frame (1) Description: Allows displaying detailed information about the Alert and RuleID;
- Information frame (2):
  - Source event logs: Record source event logs related to the alert (if any);

- Advance: Advanced information related to Alerts including: File, Process, Host, Others, ...

3.3.5 *Survey Chart (Enhance Alert)*

Purpose: To allow the display of relationships between objects in Alerts, view detailed information of the objects, and support investigation of spreading based on the set of events collected within the system.



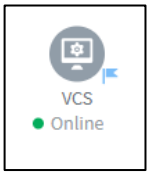
1 – Chart display area and chart operations

2 – The area displaying detailed information about the objects on the chart.

Chart display area and chart operations

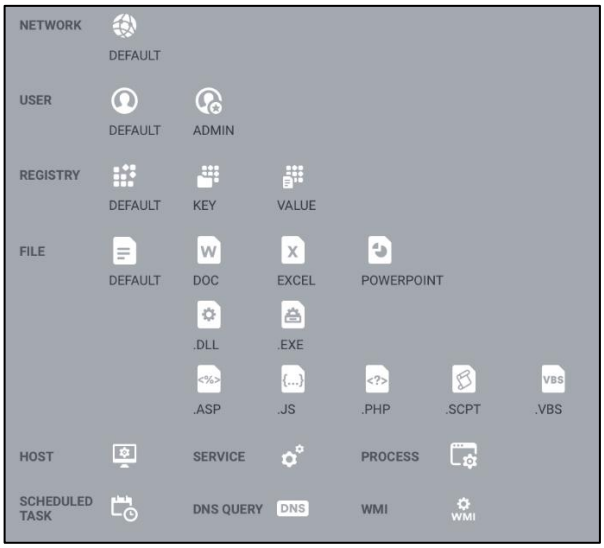
Allows visual display of objects in Alerts to facilitate information viewing and investigation;

By default, upon access, the chart displays information related to the source machine that triggered the Alert, specifically as follows:



In the chart, there is always one machine flagged to mark the original machine that triggered the Alert. By default, each machine is accompanied by objects that have a

direct relationship with the original machine within one day from the time the Alert occurred. The list of objects includes:

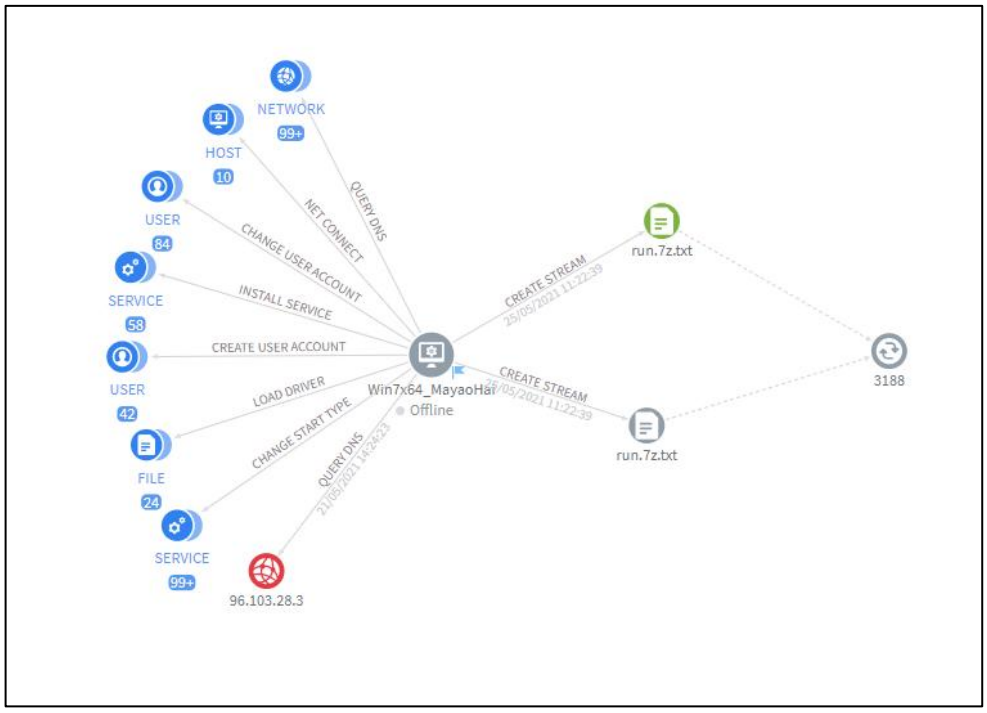


Each object includes the following states:
Between the objects, display the relationships including:

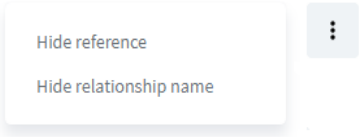
Relationship: The relationship is defined based on events occurring within one day from the time the Alert is triggered (where the name of the relationship is placed above the arrow connecting the two objects).

Reference relationship: these are other objects recorded in the main event that generates the object (represented by a dashed line without a specific relationship name).

Example:

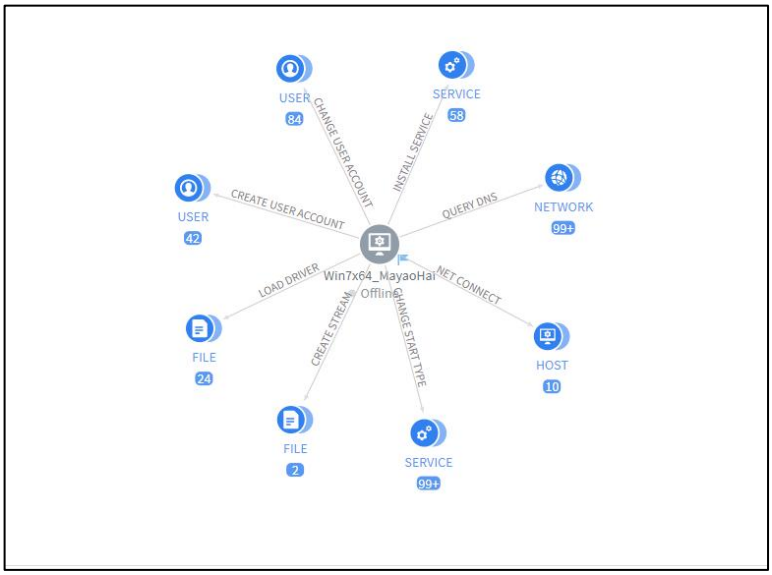


The operations supporting chart display include:

Display support operation	Meaning
	Allow toggling the visibility of information on the chart: Reference: When selected, allows hiding/showing reference information, including dashed arrows and reference objects for all existing objects on the chart; Relationship name: When selected, allows hiding/showing the relationship name information above all solid arrows currently present on the chart.

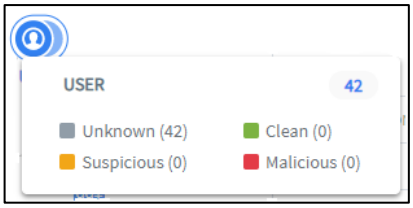
	Allow zooming in/out of the chart at the cursor position. Additionally, enable scrolling the mouse wheel at the desired position to quickly zoom in/out.
	Allow returning to the center position of the chart (origin).
	Allow maximizing the screen to view and interact with the chart.

For example, a default chart is as follows:



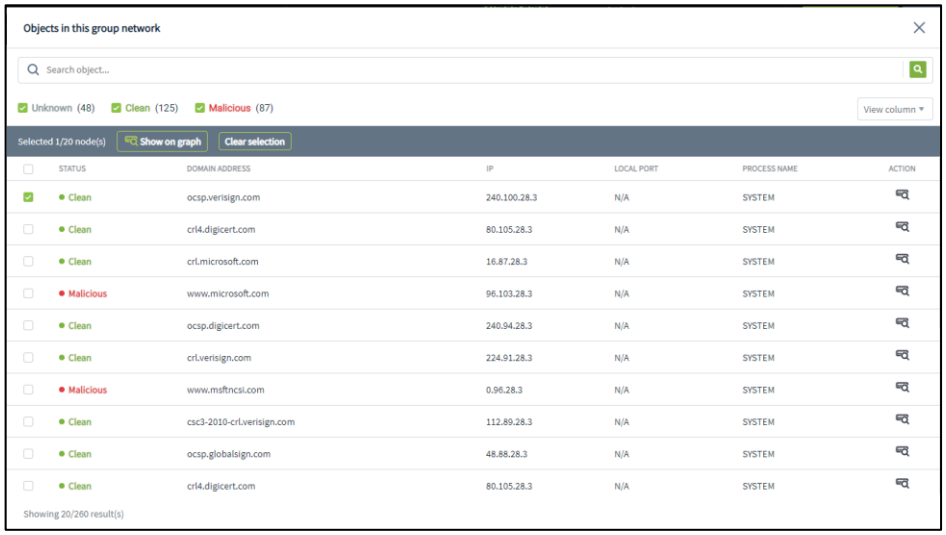
In cases where each type of entity has more than one subordinate entity, the entities will be automatically grouped together.

Hover to quickly view statistics for each target group as follows:



➔ From here, to further investigate the subjects, proceed with the following steps:

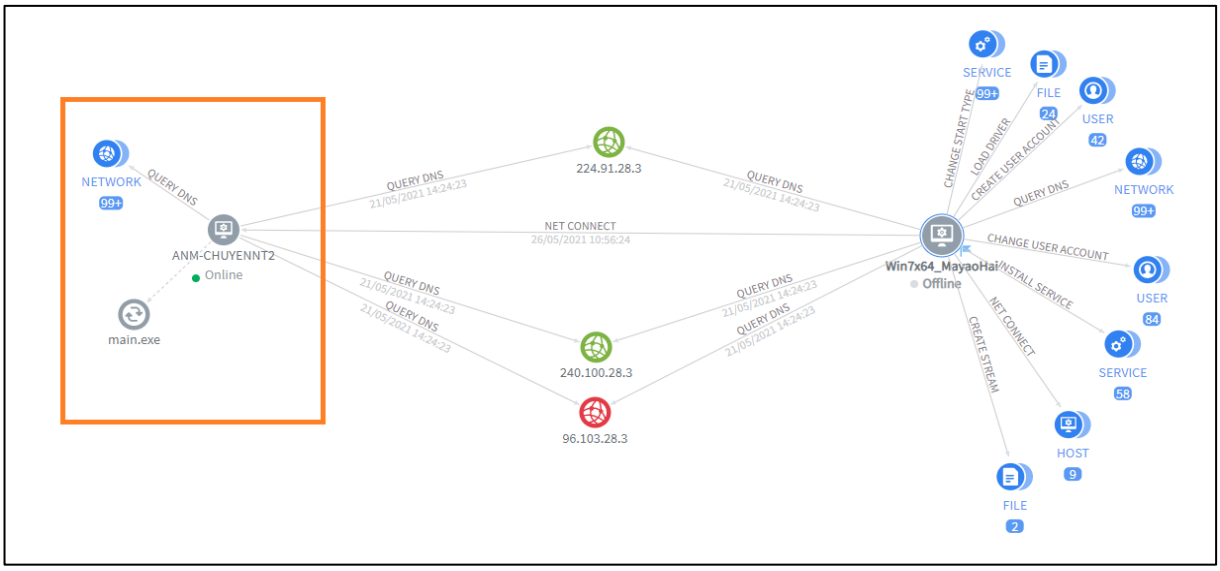
Step 1: Click to select the target group you want to view; the interface will display as follows:



Allows filtering objects within the group by status or quick searching by entering the desired data to search across all fields;

Once the appropriate object has been selected, choose to display one object on the chart or select up to 20 objects to display on the chart;

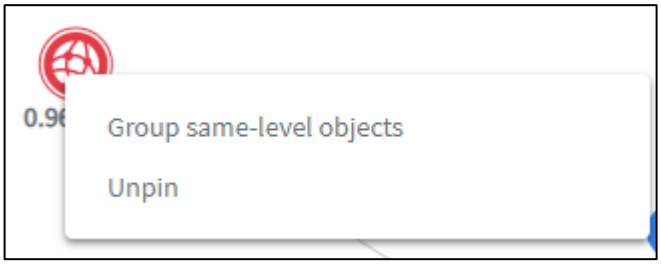
Note: If the expanded object is a computer, by default when displaying the object, it also automatically displays objects that have direct relationships with the computer within 01 day from the time the Alert occurred.



Step 2: After displaying the objects to be investigated on the chart, the supporting operations for expanding/collapsing include:

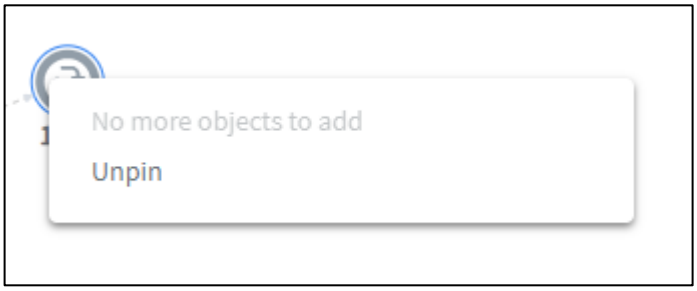
On the main machine/regular computer: Supports collapsing objects to their default state when displaying the machine (including only objects directly related to the machine; if there are multiple objects of the same type, they are displayed as a group) by right-clicking on the object, then selecting “Group child-level objects.”

For other objects: Support collapsing by grouping according to object type and relationship type with peer objects by right-clicking on the object, then selecting "Group same-level objects";

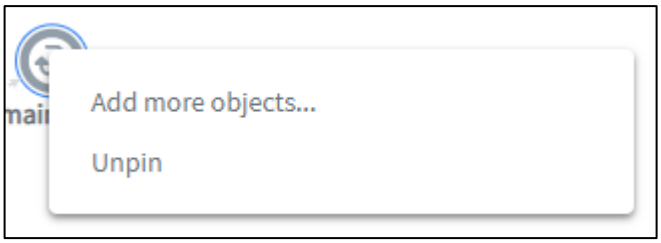


For the object that is a process, it allows expansion to investigate the spread by right-clicking on the object.

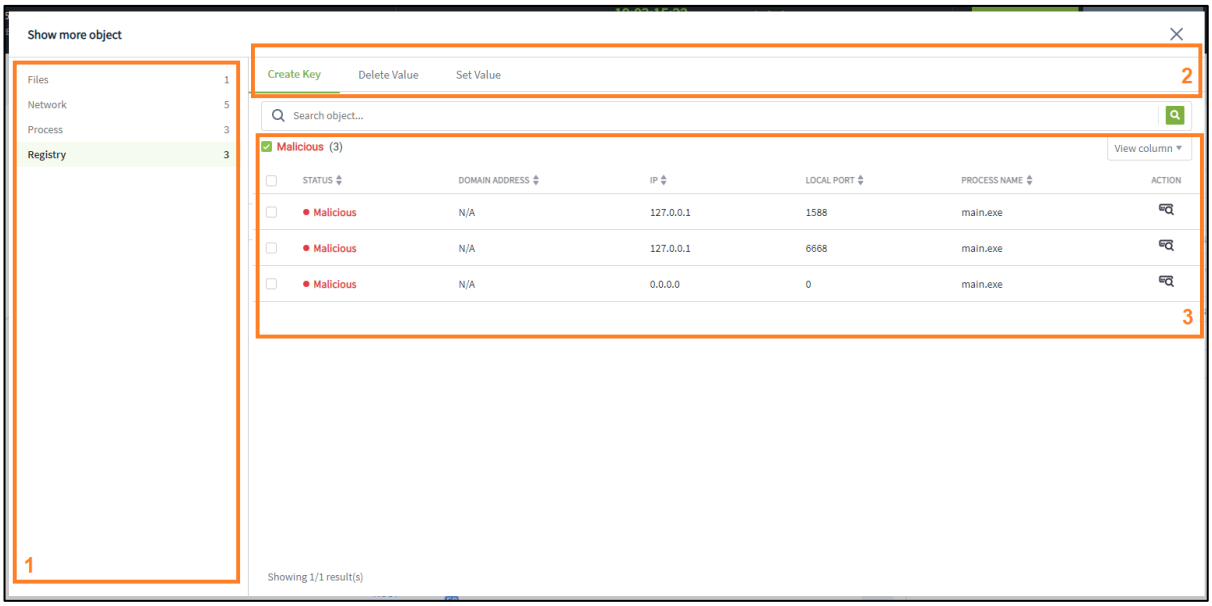
In cases where spreading cannot continue, display:



In case of possible bleeding, select “Add more objects…”



Display an interface that allows selecting the target object for spreading.



1 – Select object type;

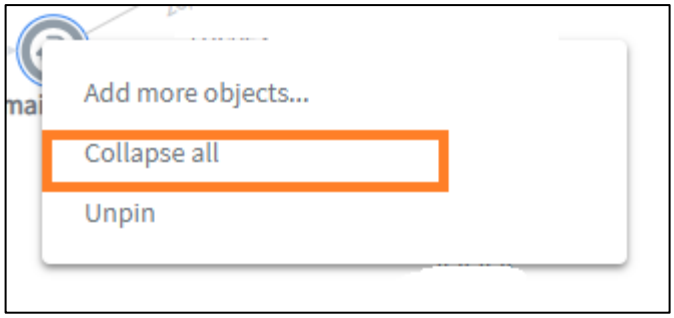
2 – Select the type of relationship from the process to the object;

3 – Directly select the object you want to display. Supports searching by the object's infected/clean status or searching by content within the object's information fields.

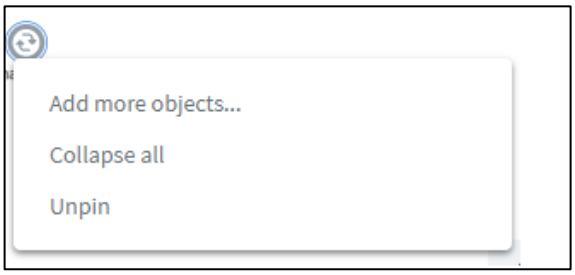
Select to choose the information fields to display or use the feature to sort the information in the list.

Once the appropriate object has been selected, choose to display one object on the chart or select up to 20 objects to display on the chart;

For the object being a process, when there are objects currently expanded, you can collapse them by right-clicking on the object;

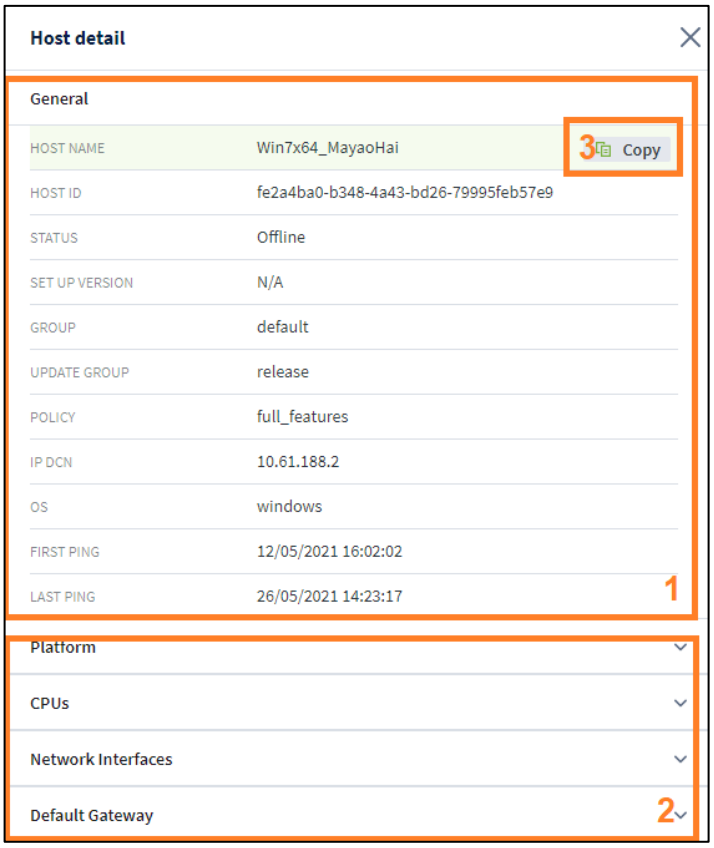


By default, on the chart, objects automatically move and maintain distance from each other when being moved. When selecting and dragging objects with the mouse, after releasing the mouse button, the objects are automatically pinned to the new position. To cancel the Pin action, select



Detailed information display area

As an additional feature of the chart, it allows displaying detailed information of the components within the chart (including objects and relationships in the chart);

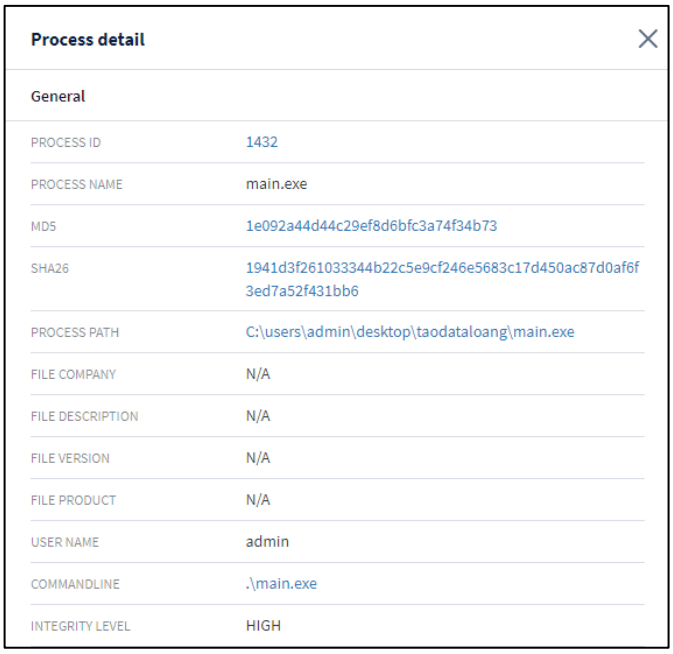


1 – General information group: Includes general information/identification information of the object, always displayed by default upon access;

2 – Detailed information groups: Include detailed information about the object, divided into different information groups. By default, these information groups are collapsed; select to expand and display the information group.

Operation to support copying field content

Note: Some object identification fields allow quick linking for lookup in Event Search or Agent Management.

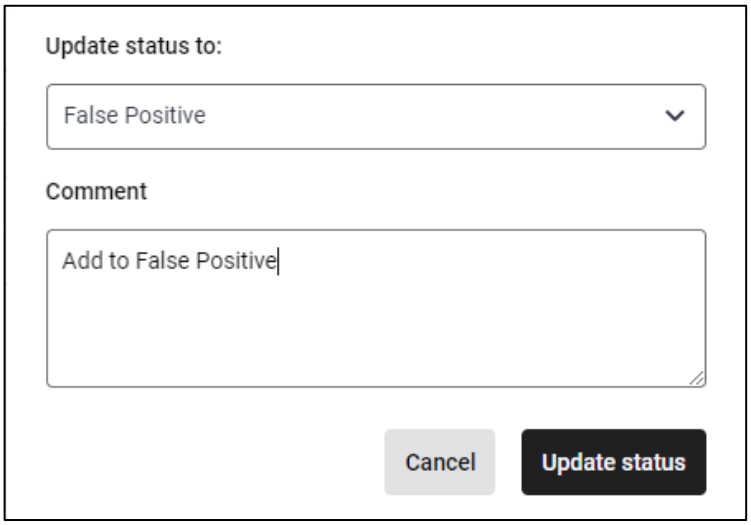


3.3.6 Update the status to non-hazardous or close the alert for one/multiple alerts or alert groups.

Purpose: To allow marking an Alert as non-dangerous;

Bước 1: Select one or multiple Alerts to mark as non-critical;

Bước 2: Select to update the status of the Alert:



Bước 3: Select Update Status to “False Positive”;

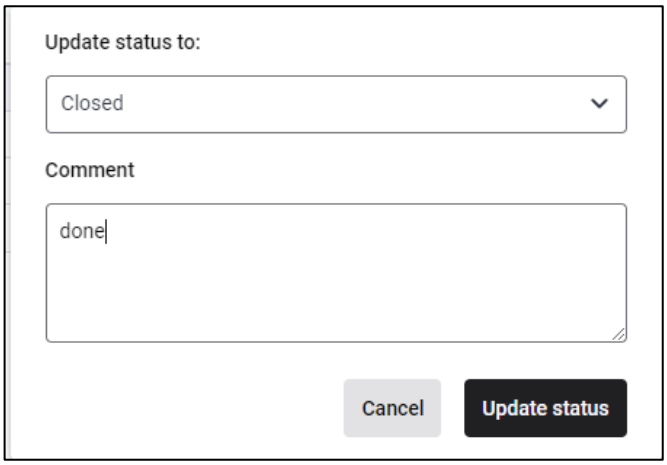
Bước 4: Enter the reason for marking as non-hazardous and:

- Select "Update status" to confirm marking the Alert as not dangerous;
- Select "Cancel" to confirm the cancellation of marking the Alert as non-hazardous;

Select Update Status to “Close” to close the Alert;

Bước 1: Select one or multiple Alerts to close;

Bước 2: Select to update the status of the Alert:



Bước 3: Select Update Status to “Closed”;

Bước 4: Enter the reason for closing the Alert and:

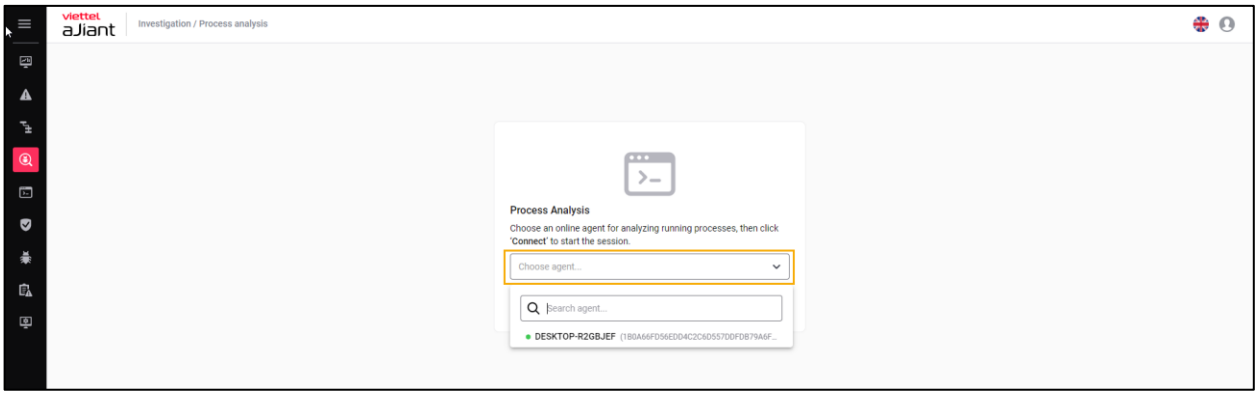
- Select "Update status" to confirm closing the Alert;
- Select “Cancel” to confirm the cancellation of the Alert closure action;

3.4 Investigation Screen

The Investigation screen consists of several small tabs: Process Analysis, Event Search, and Deploy Tools.

3.4.1 Investigation Process Analysis

- Purpose: This function allows users to establish connections and monitor the status of processes on their machines. Specifically:



User device list:

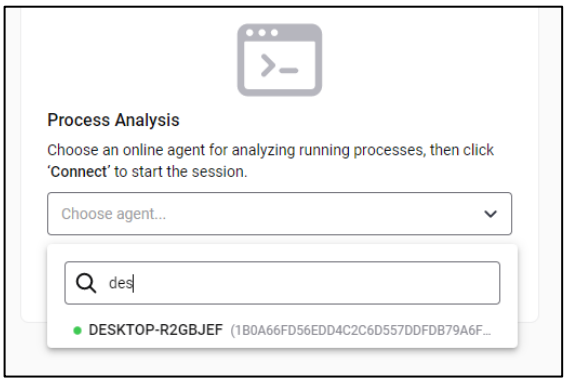
User logged in as root group: Display all Agents in the system active for less than 30 days;

User logged in belongs to the default group: Display all Agents belonging to the default group;

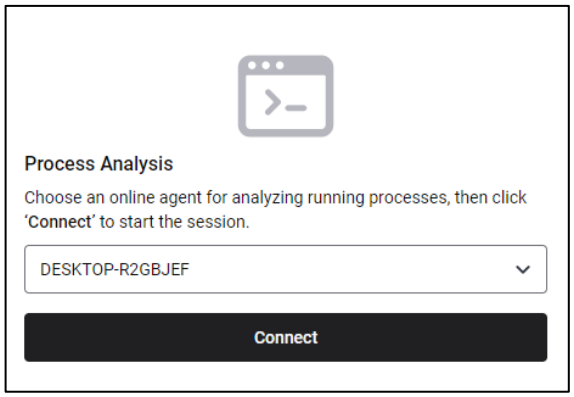
User login belongs to parent group: Display all Agents belonging to the user's current group and the corresponding subgroups;

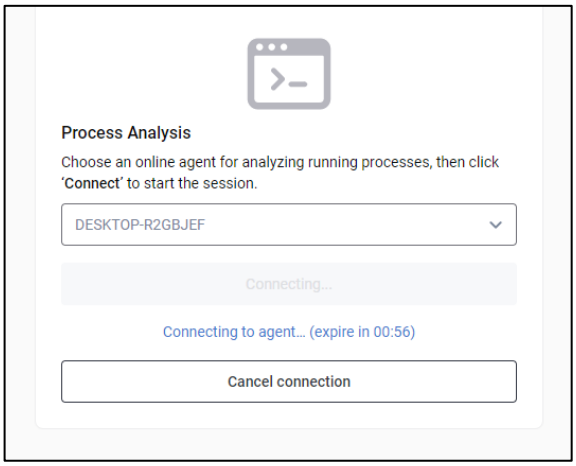
User logged in belongs to one or multiple sub-groups: Display all Agents belonging to the user's group currently logged in;

Step 1: Search for and select a connection Agent (Note: to ensure connectivity, the list only displays machines that are Online);

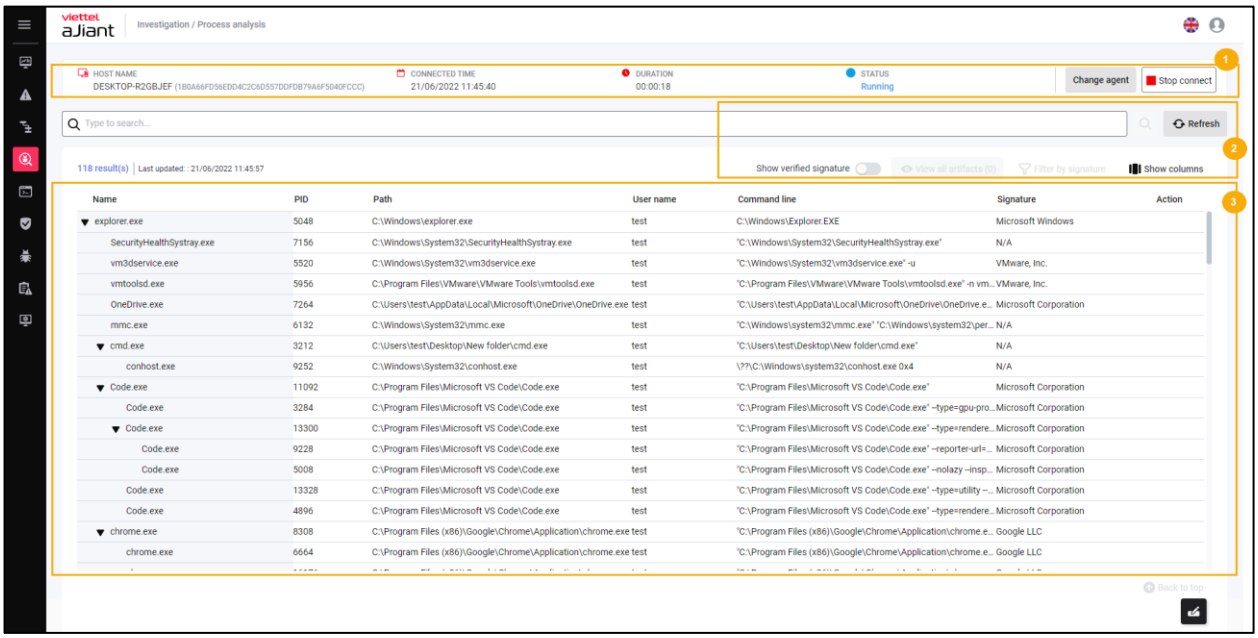


Select one device and click the "Connect" button to initiate the connection (the connection may take up to 60 seconds).





Step 2: View the list of processes currently running on the user's machine.



The interface is divided into information groups:

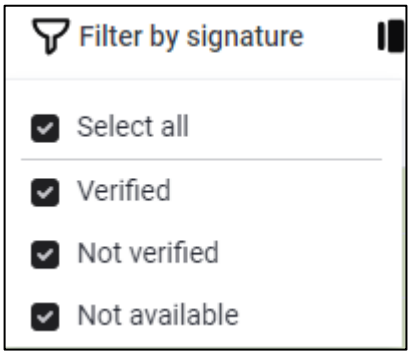
1 – Information related to the connection group includes: the device currently connected, connection creation time, connection duration up to the present, and connection status.

2 – The group of information supports searching/refreshing and filtering data in the list, including the following operations:

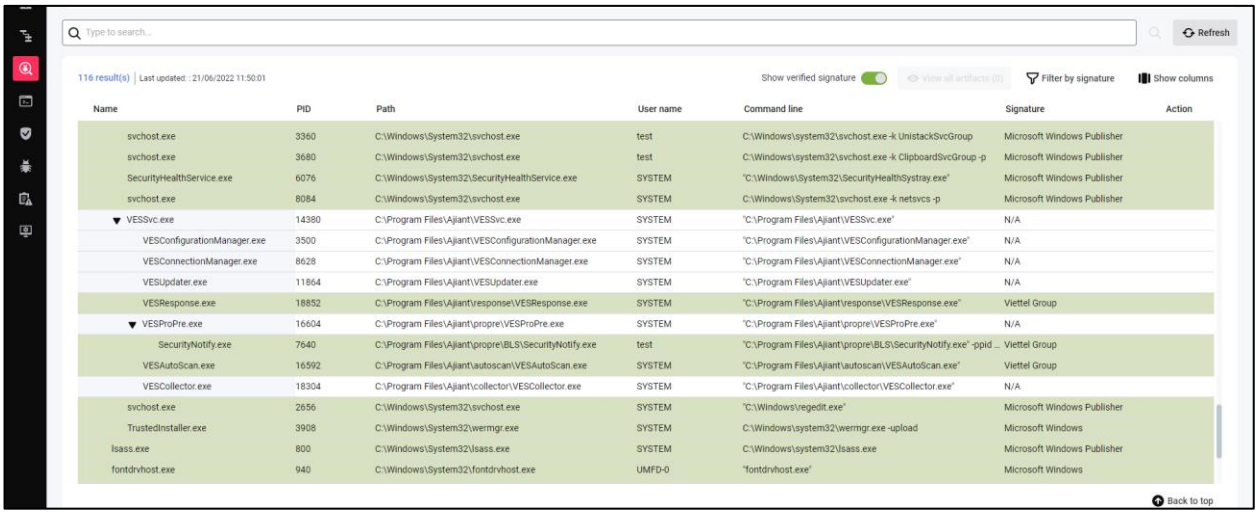
Allow keyword search within the displayed data across all fields in the list;

Allow data refresh (while retaining the current search and filter conditions, only retrieving the latest data from the user's device for display);

Allows enabling/disabling the retrieval of digital signature information for processes. When this configuration is enabled, it allows filtering process data based on the digital signature:



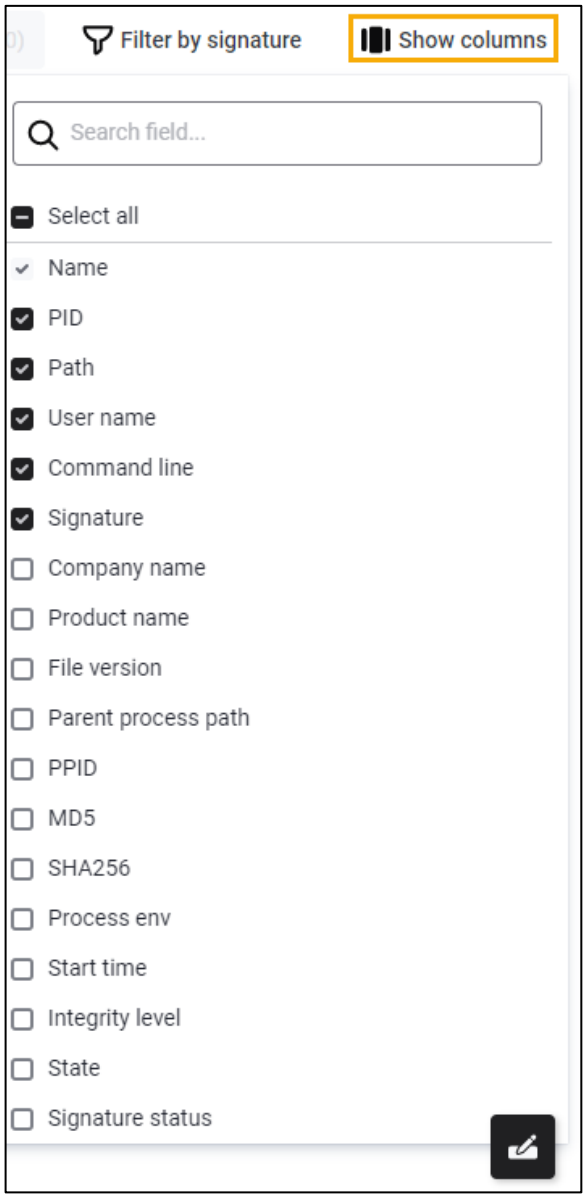
The digital signature statuses will determine the color of the corresponding record.



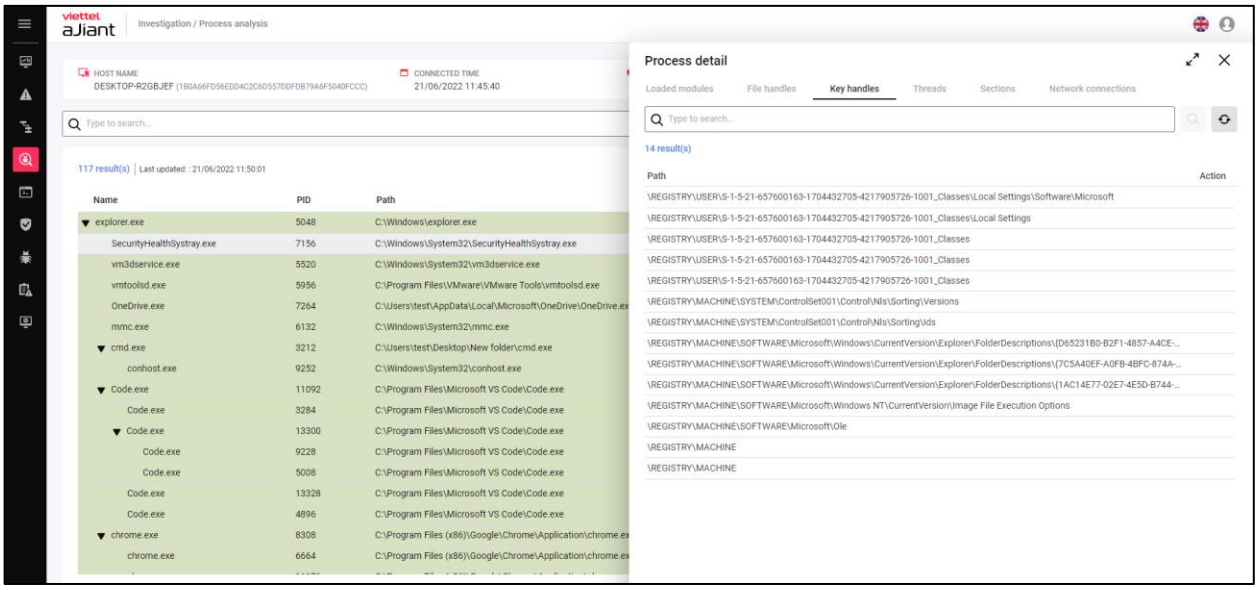
- Verified: Green – has a digital signature and is still valid;
- Not verified: Red - no digital signature or expired signature;
- N/A: White – digital signature information not found;

Allows adjustment of the display fields in the process list.

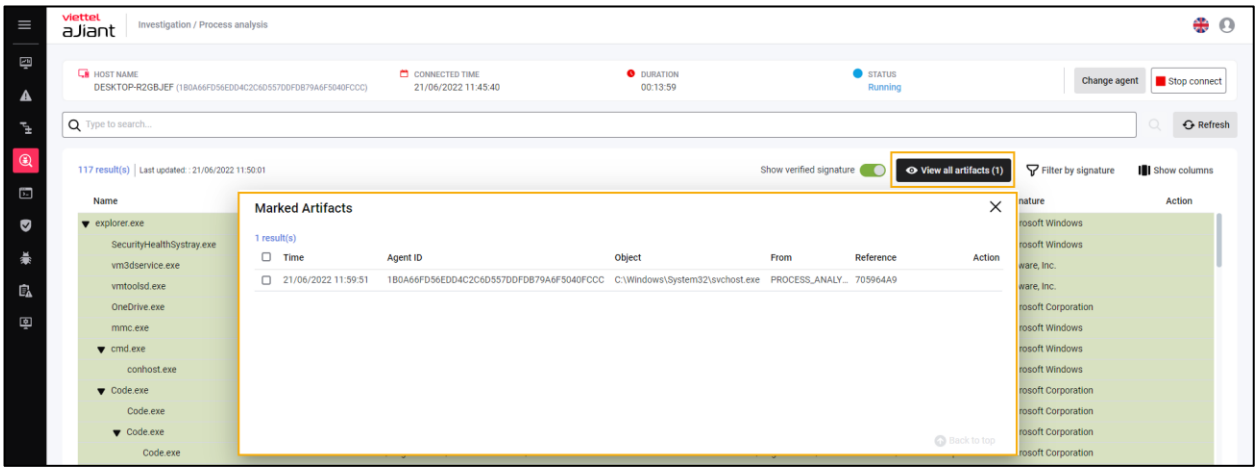
In the list, the "Name" field is always displayed by default, while the other fields can be optionally shown or hidden.



3 – Process list, displaying current process data on the user's machine with selected information fields in the Show column. Double-click each record to view process details;



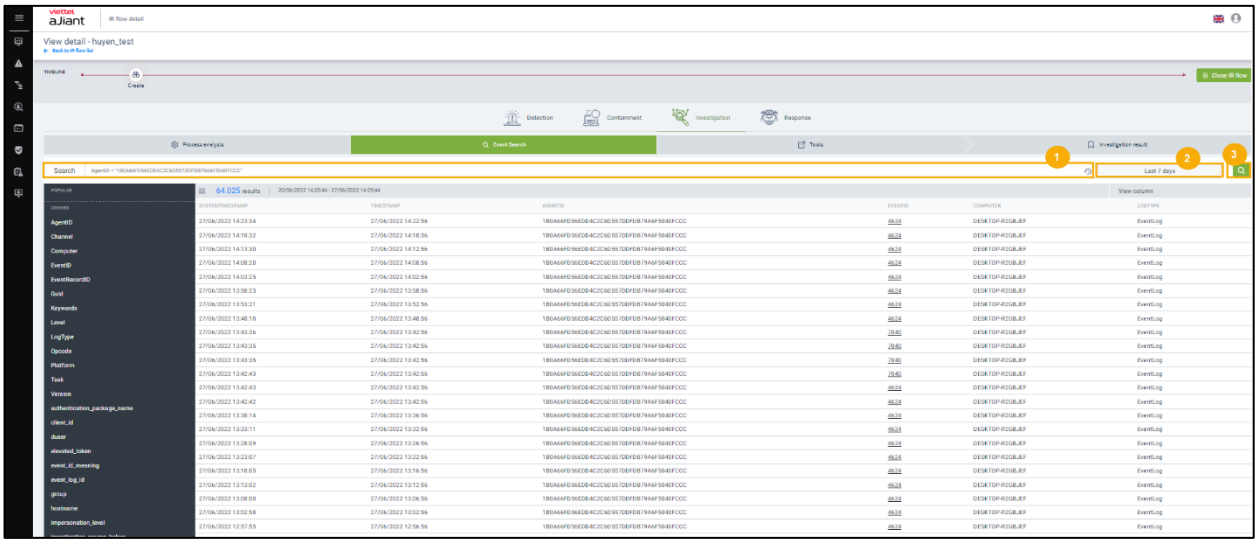
The process details are divided into tabs, with each tab displaying the corresponding list of information.



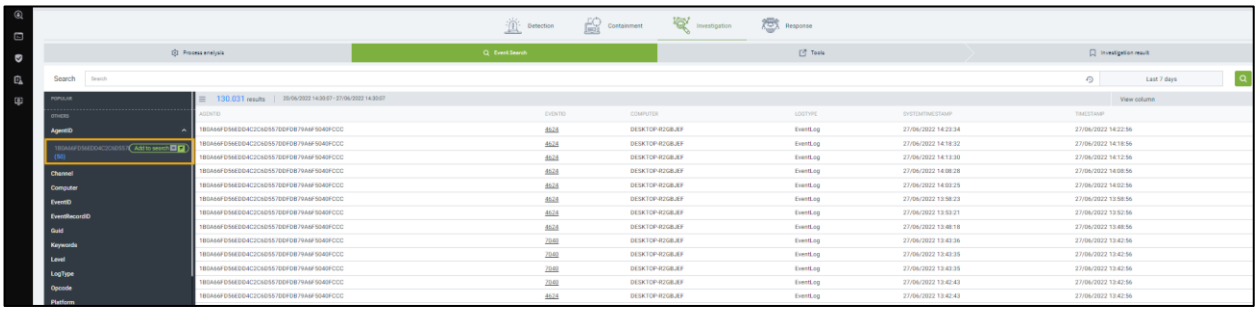
3.4.2 Investigation_Event Search

Search Event

Step 1: Enter the query > Select the time range > Click the “Search” button:



Step 2: Add search fields to the query with the Popular and Others fields by selecting the queries "=" or "#" in Add to search:



Highlight

Purpose: To allow adding one or multiple highlights for simultaneous review at any given time (with no maximum limit). When performing a search or sort, all existing highlights will be cleared.

Steps to perform:

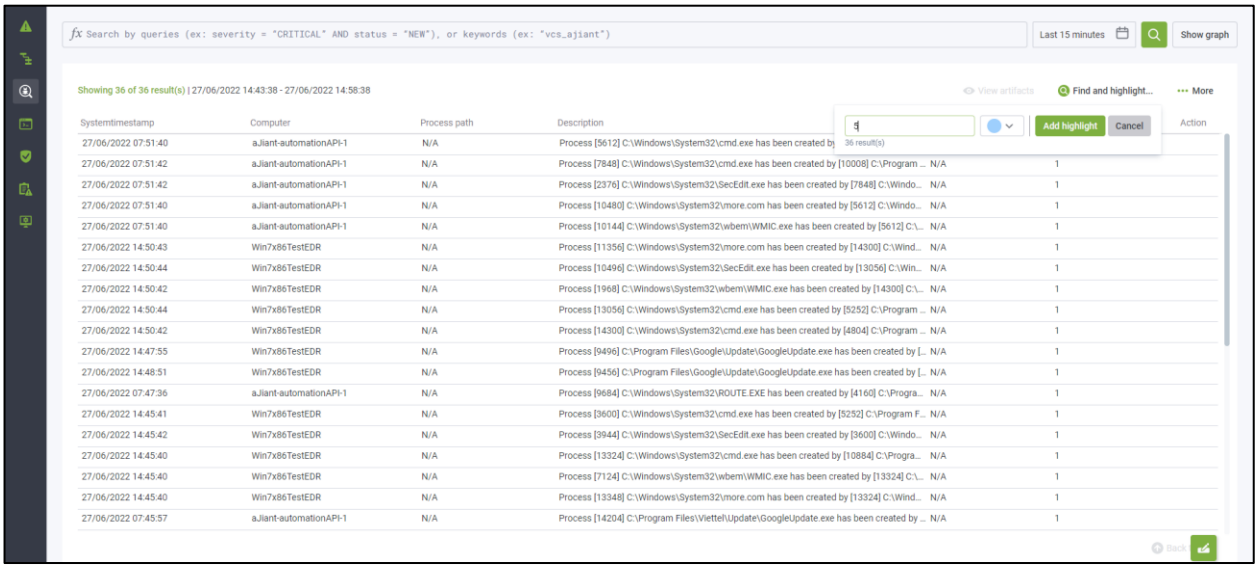
Step 1: Select Investigation >> Choose the Event Search tab;

Step 2: The screen displays the list of events. Select the "Find and highlight" button, and the system will display the "Find in table" popup.

Step 3: Enter the highlight keyword, select the highlight color, and confirm the action:

Select the "Add highlight" button to confirm the highlighted keyword;

Select the "Cancel" button to cancel the keyword search marking operation;



I need help.

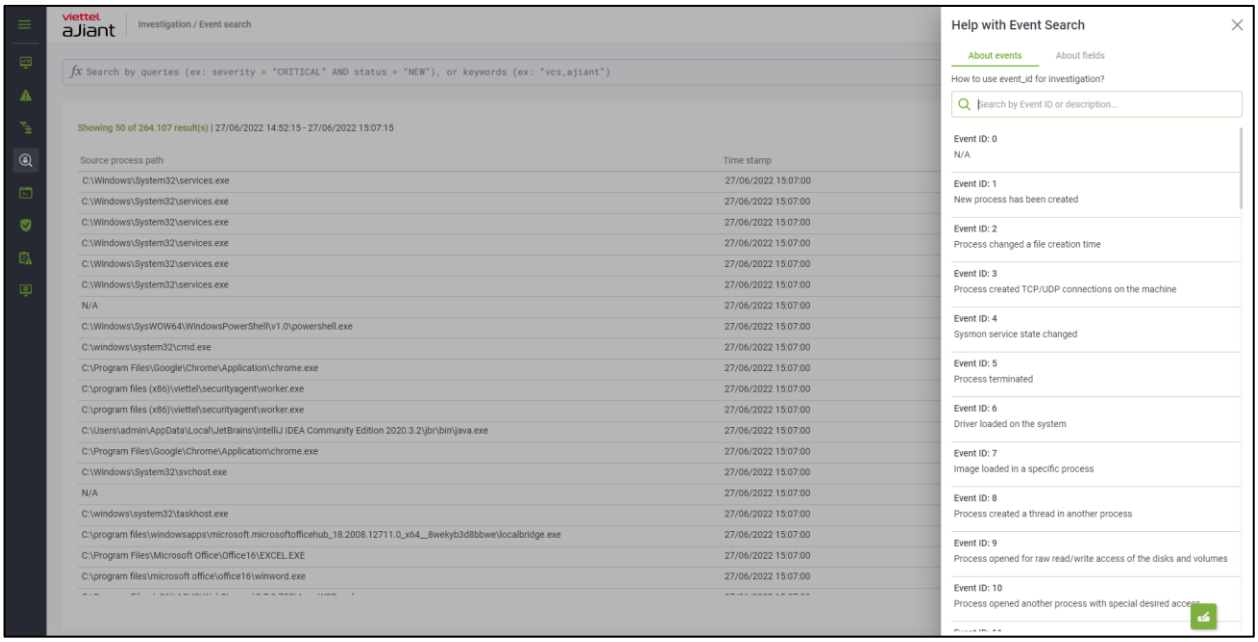
- Purpose: to look up event information and the meaning of the field;
- Steps to follow:

Step 1: Select Investigation >> Choose the Event Search tab;

Step 2: On the Event Search screen, select “More”;

Step 3: The interface displays a list of actions: Show columns, Wrap text, Export, Need help. Select "Need help?"

Step 4: The system displays a Help with Event Search popup, allowing users to look up information and the meanings of fields in Event Search.



Wrapped text

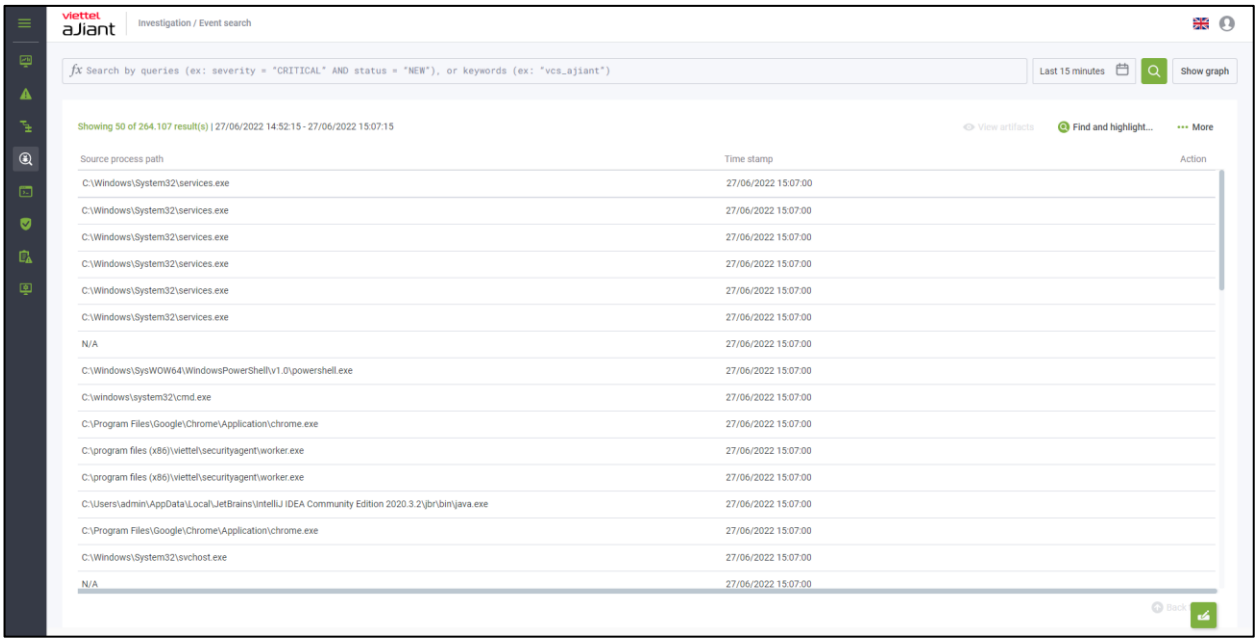
Purpose: To be able to display the entire data or collapse the data when clicking the "wrap text" button;

Steps to follow:

Step 1: On the Event Search screen, select “More”;

Step 2: The interface displays a list of actions: Show columns, Wrap text, Export, Need help. Select "Wrap text."

Step 3: The system changes the display information to show all data or condense the data when clicking the "Wrap text" button.



Export Data

Purpose: To allow downloading of data related to Events within the system.

Steps to follow:

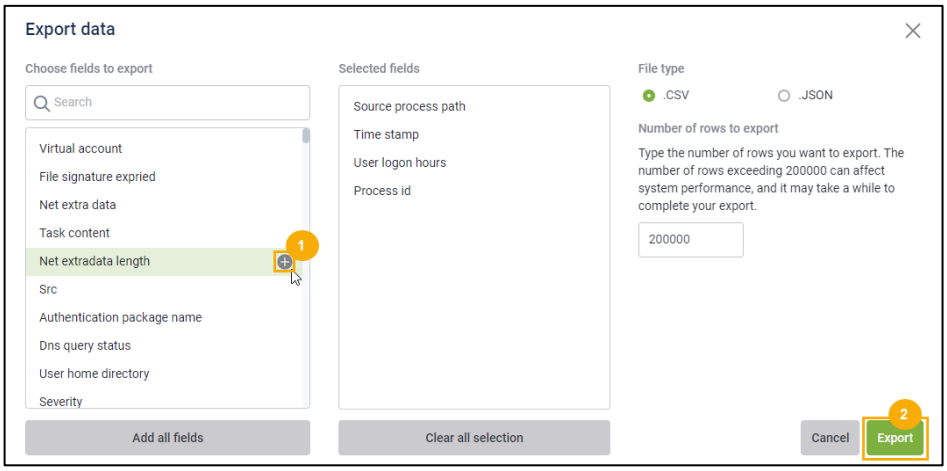
Step 1: On the Event Search screen, select “More”;

Step 2: The interface displays a list of actions: Show columns, Wrap text, Export, Need help. Select "Export".

Step 3: The system displays a popup for filtering Data Event information, allowing selection of filter parameters based on available system conditions: choose information fields, export file format, number of rows, and confirm the action.

Select the "Export" button to confirm the action of downloading the Data Event;

Select the "Cancel" button to abort the operation;

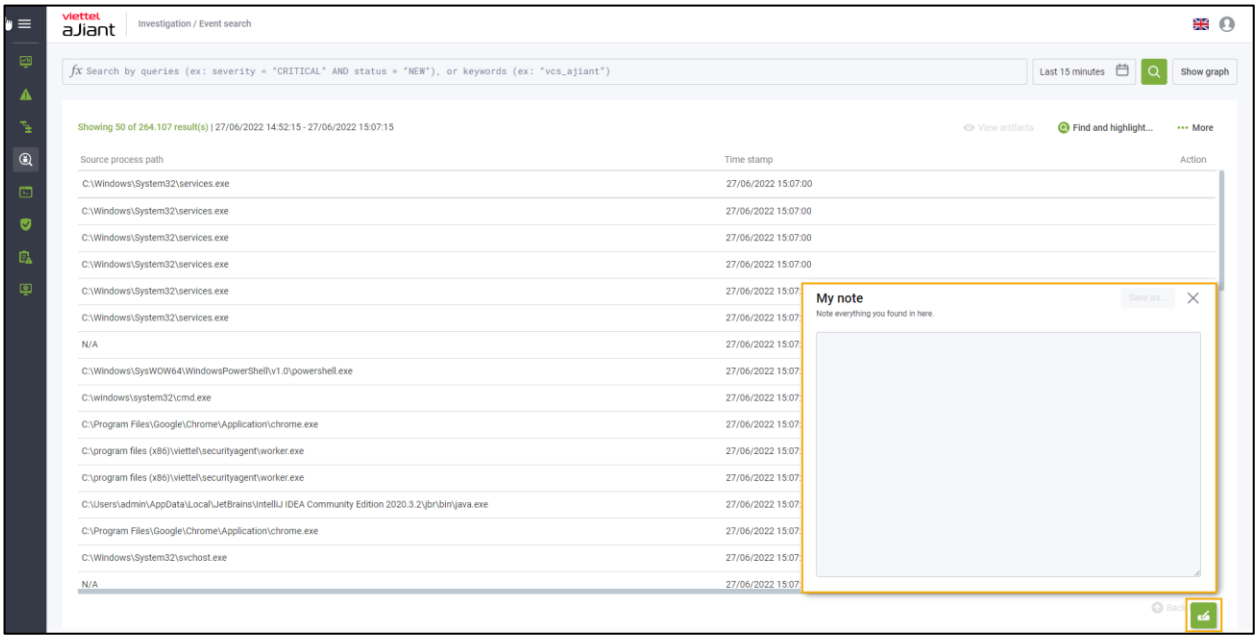


3.4.3 Note

Purpose: Display on all screens; when navigating between screens, the content remains unchanged, and the "Note" button can be moved.

Steps to follow:

- On the Event Search screen, select the icon;
- The note is displayed on all screens, and its content remains unchanged when navigating between screens. The "Note" button can be moved.



3.4.4 *Investigation_Deploy Tools*

Purpose: the function allows deploying tools to support investigation and handling of information security incidents from the Portal to the Agents.

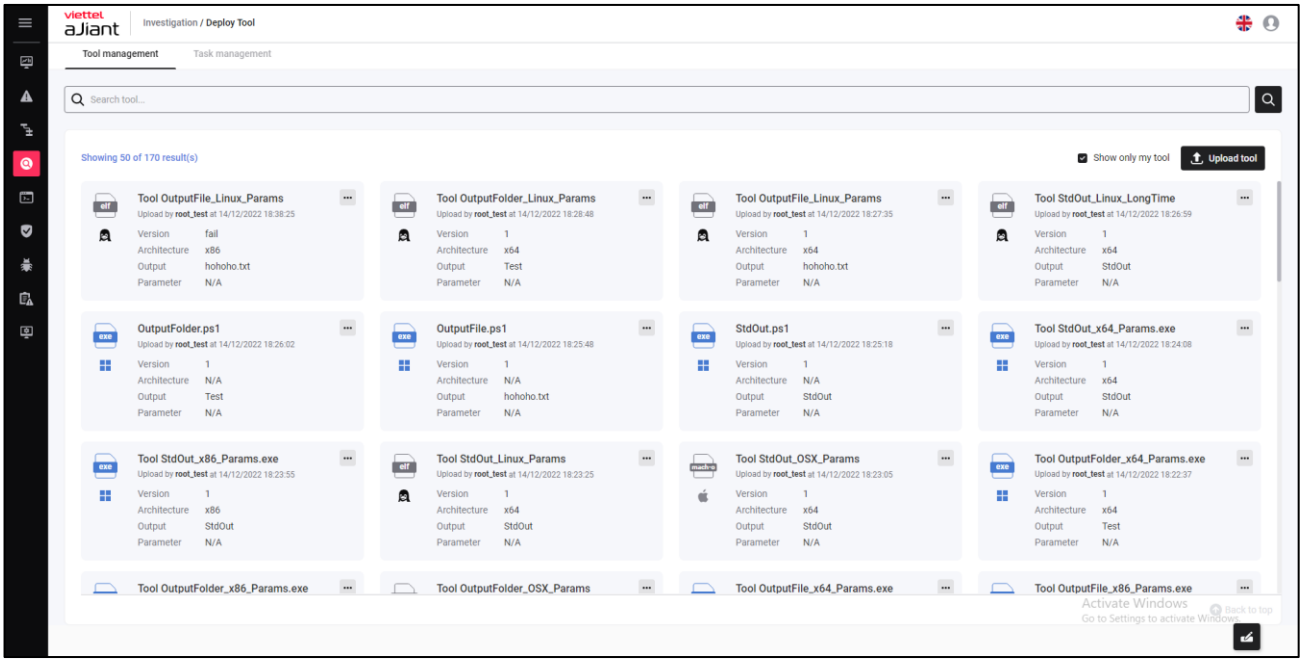
Tool Management

Purpose: to manage all the tools of the system, users can add or delete tools on this screen. The features on this screen include:

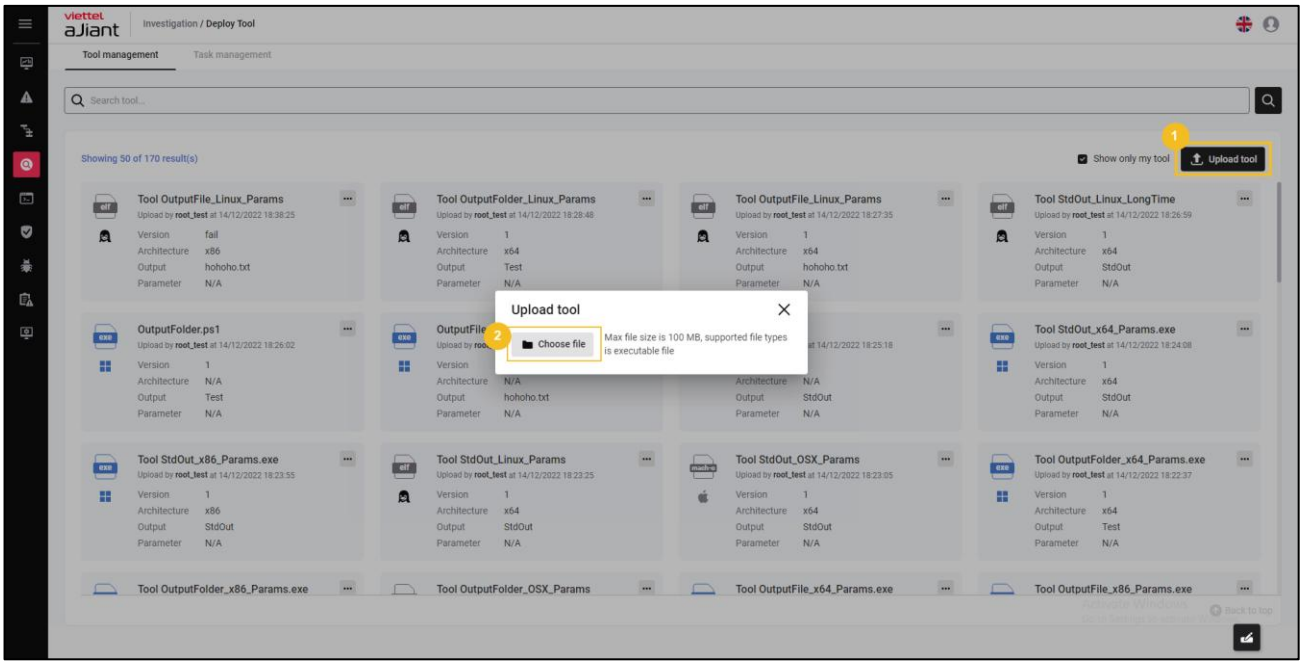
Display the list of tools along with detailed information for each tool: Name, Parameter, Version, Architecture, Upload User, Platform, Output, Upload Time;

Search tool: Search by tool name

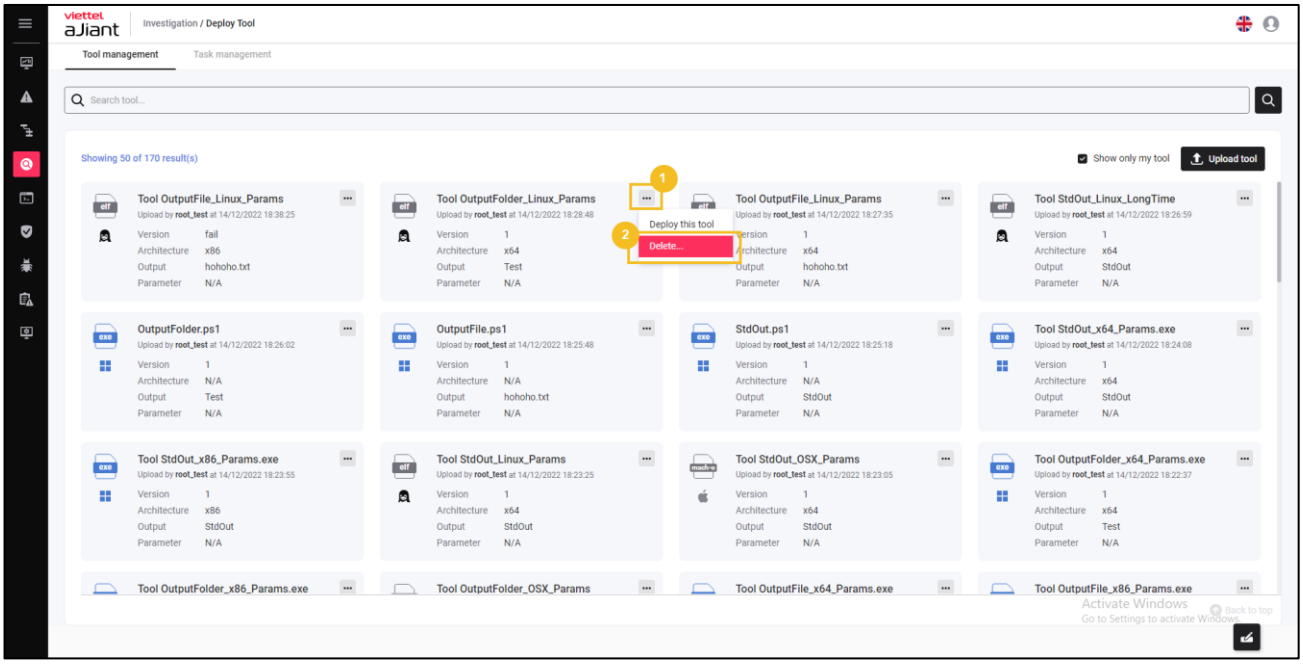
Upload tool: The upload tool runs on Windows, MacOS, and Linux agents with a maximum file size of 100MB;



With the Upload tool feature, follow these steps:
Click on “Upload tool” > Select the path to the tool you want to upload or drag and drop the tool into the interface > Enter the information in the Tool info popup > click Upload tool:



With the delete tool feature, select the icon ••• on the tool you want to delete > choose Delete.



Deploy tool

Purpose: Configure deploy tool information under the agent

Conditions:

User logged in as root group: Display all Agents in the system active for less than 30 days;

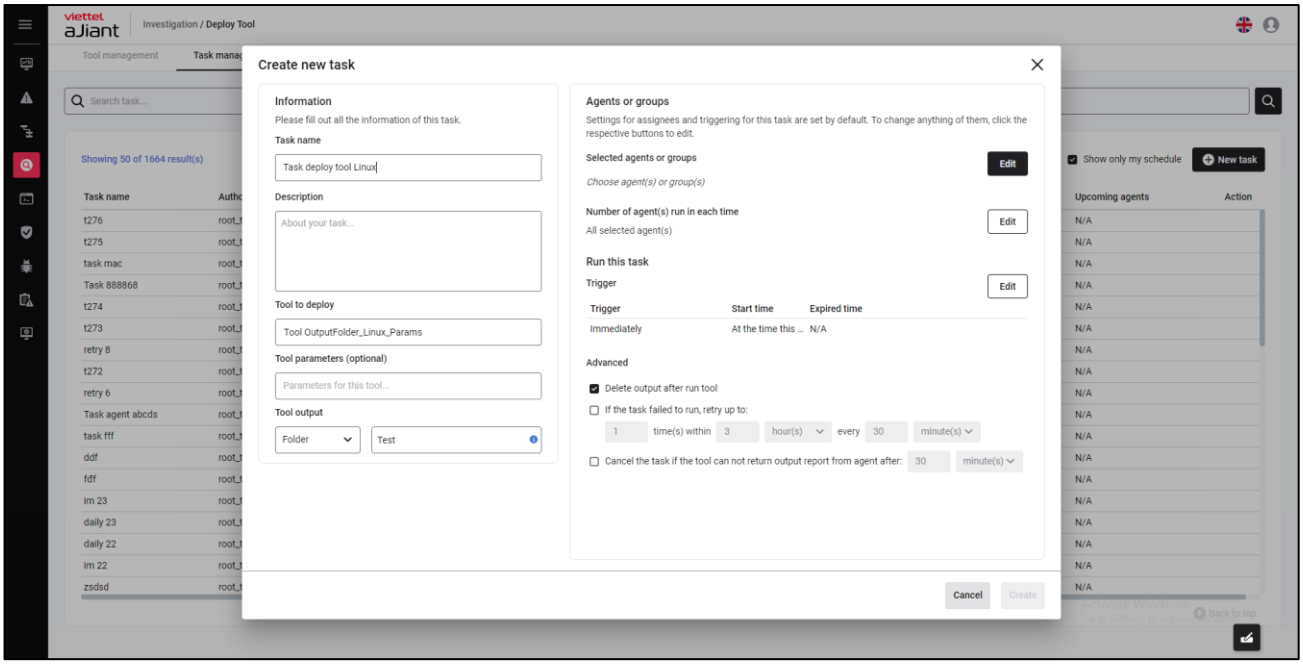
User logged in belongs to the default group: Display all Agents belonging to the default group;

User login belongs to parent group: Display all Agents belonging to the user's current group and the corresponding child groups;

User logged in belongs to one or more subgroups: Display all Agents belonging to the user's groups currently logged in;

Steps to deploy the tool on the Tool Management tab screen:

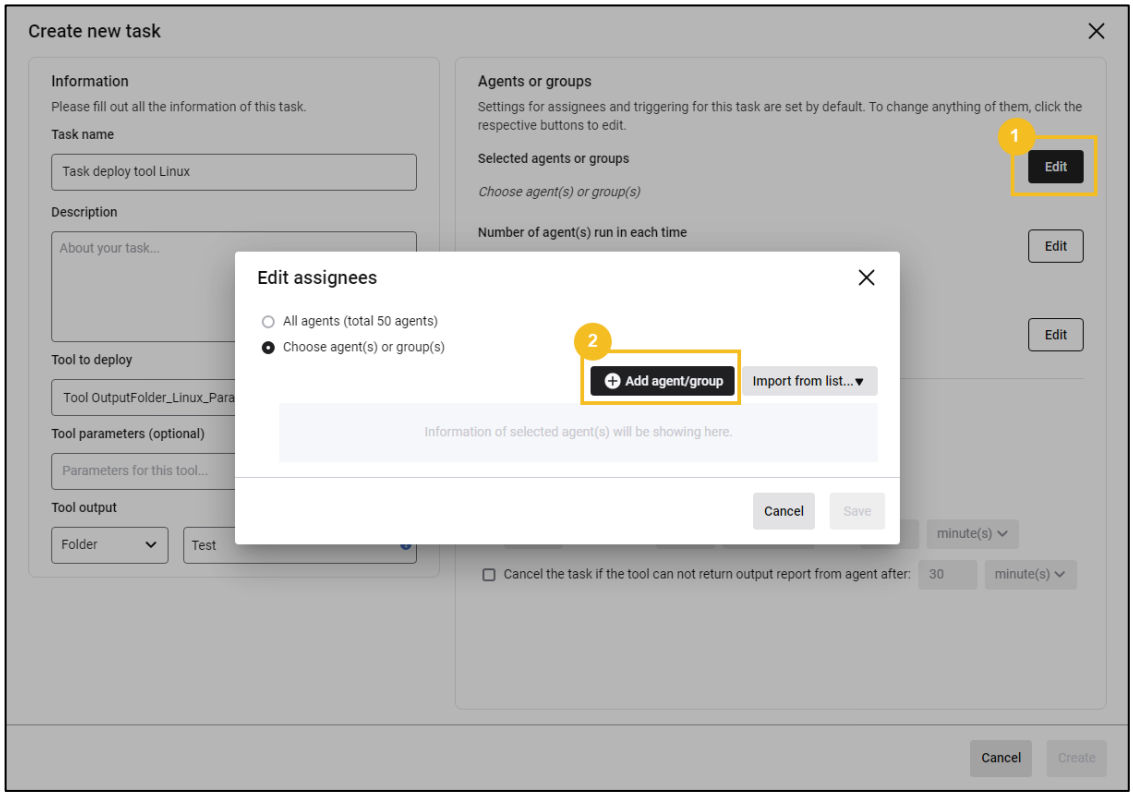
- After selecting the tool, click the icon on the tool record you want to deploy > select Deploy this tool, the Create new task screen will appear:



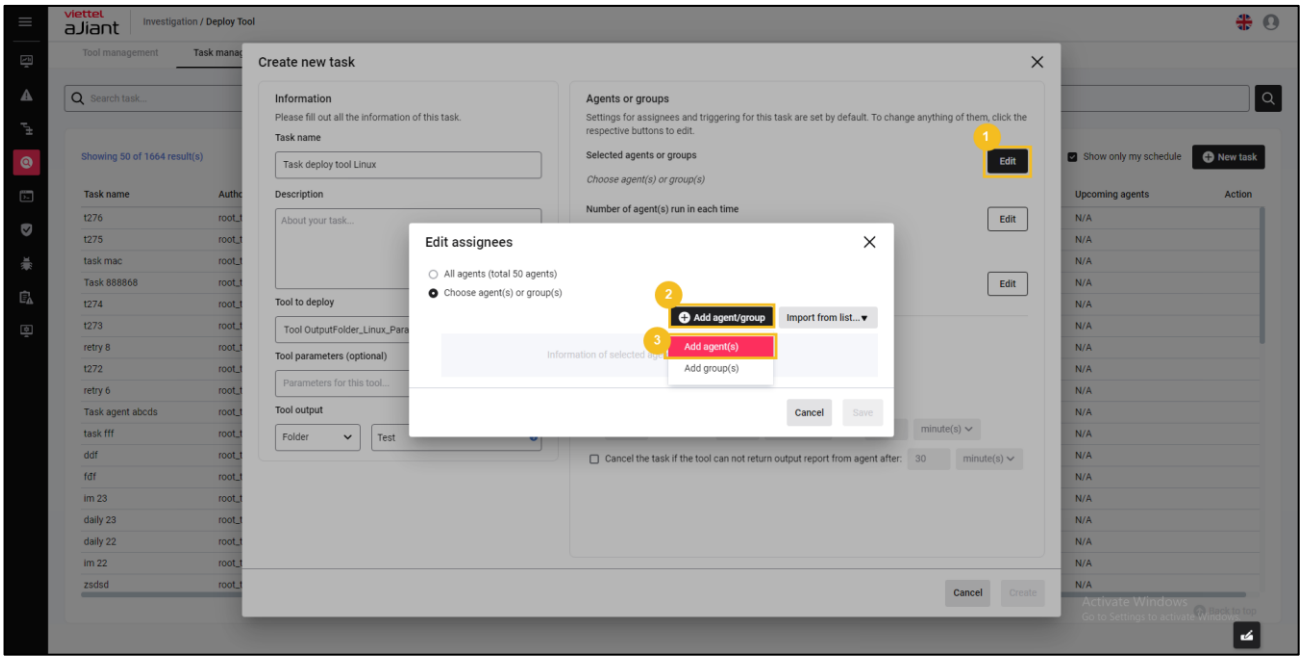
- Enter the task information for tool deployment: Task name, Description, Tool parameters, Tool output;

- Select the group and workstation (agent) information to perform the deployment:

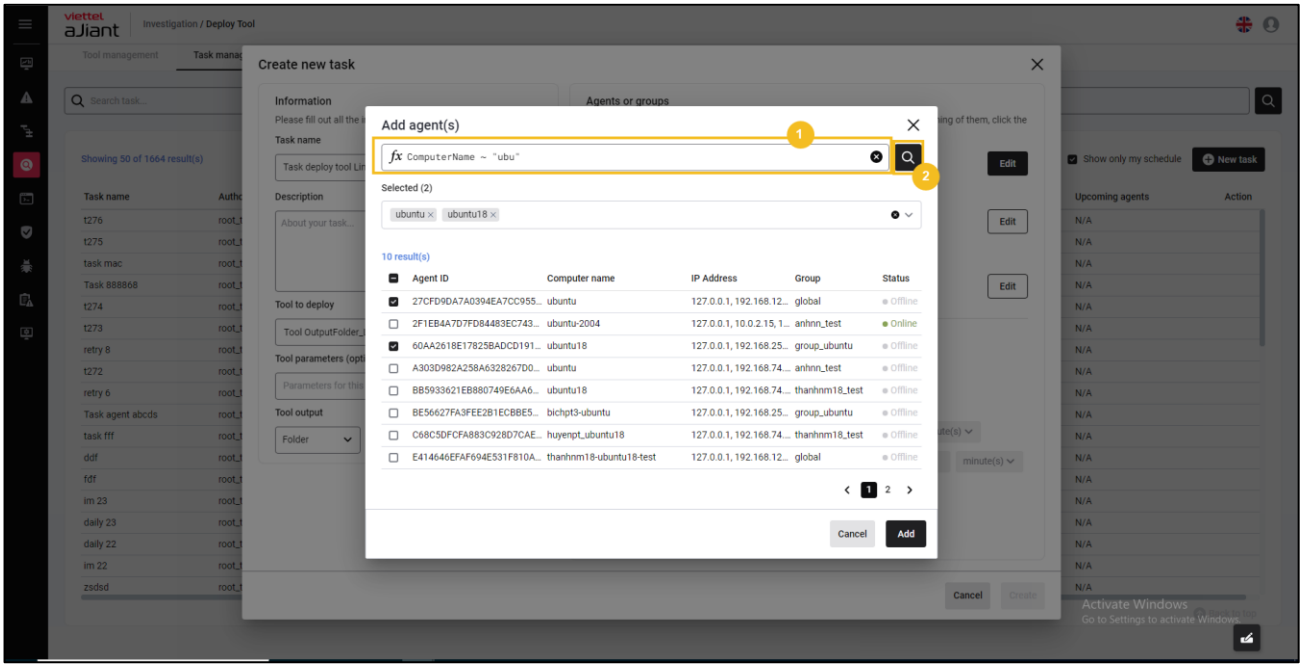
Select All agent(s): choose all agents within the management scope of the currently logged-in user to perform the deployment;
Select agents or groups to perform deployment – Choose agent(s) or group(s):



Select Add agent(s):

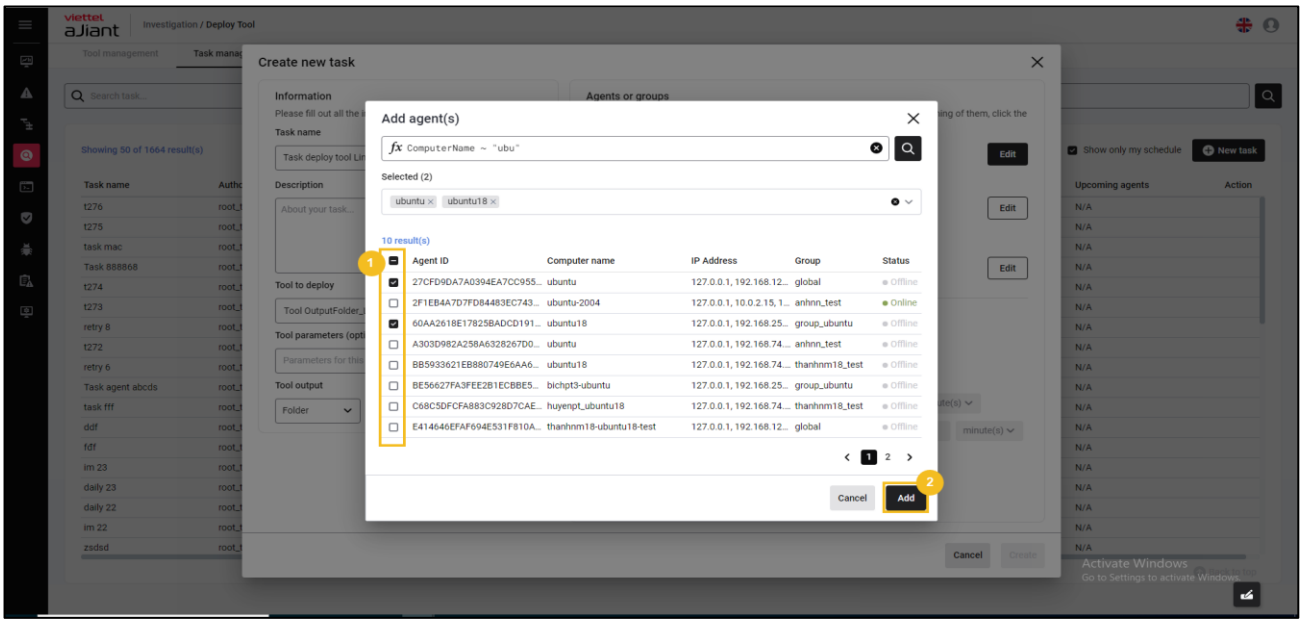


- Search Agent: Allows creating query statements and using query statements to search for Agents.

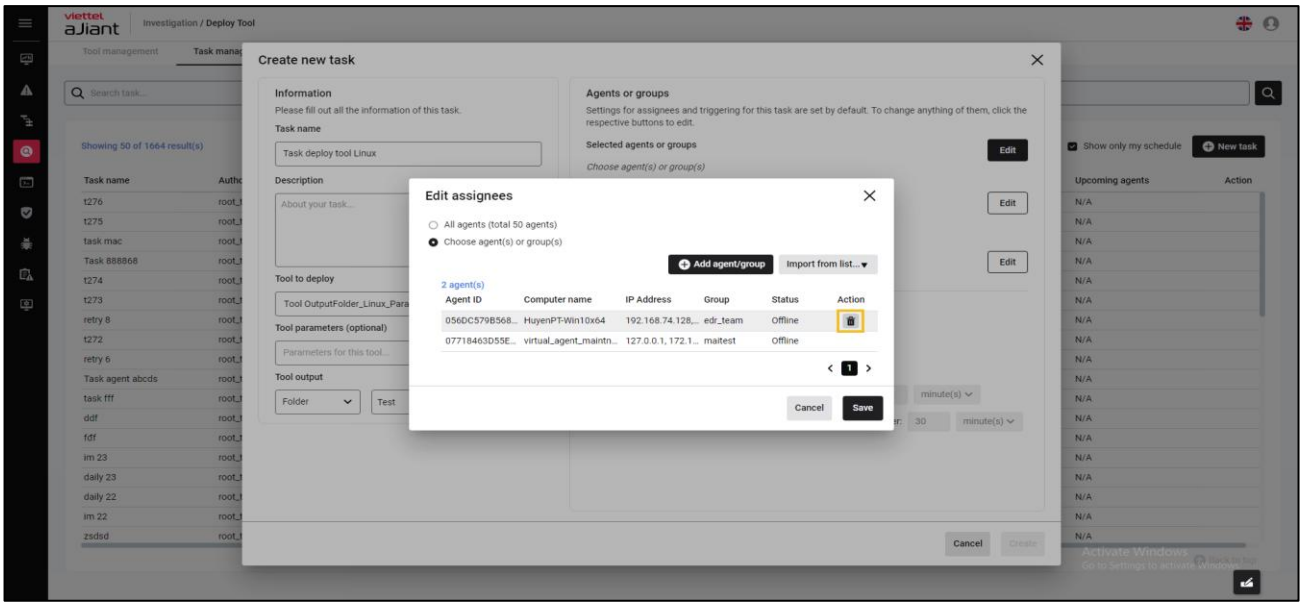


- Select the Agent(s) to deploy by checking one or more Agents > Information of the selected Agent(s) will be displayed in the Selected box > choose

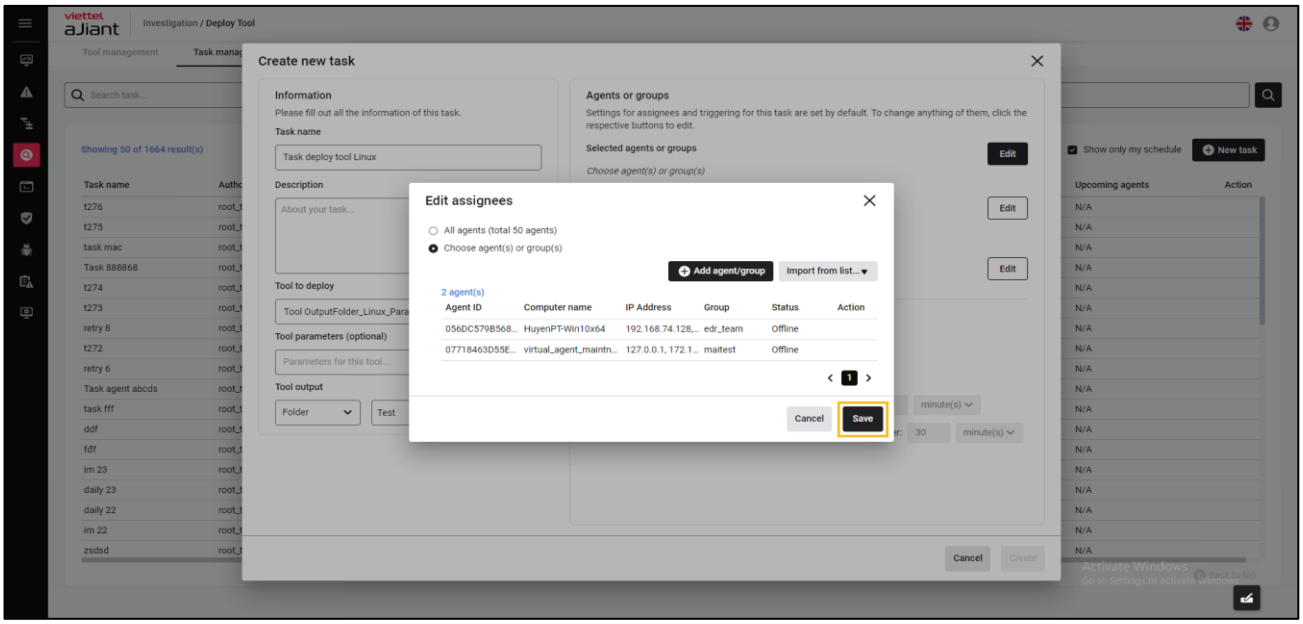
Cancel to cancel adding Agents for deployment or click the Add button to confirm the list of Agent(s):



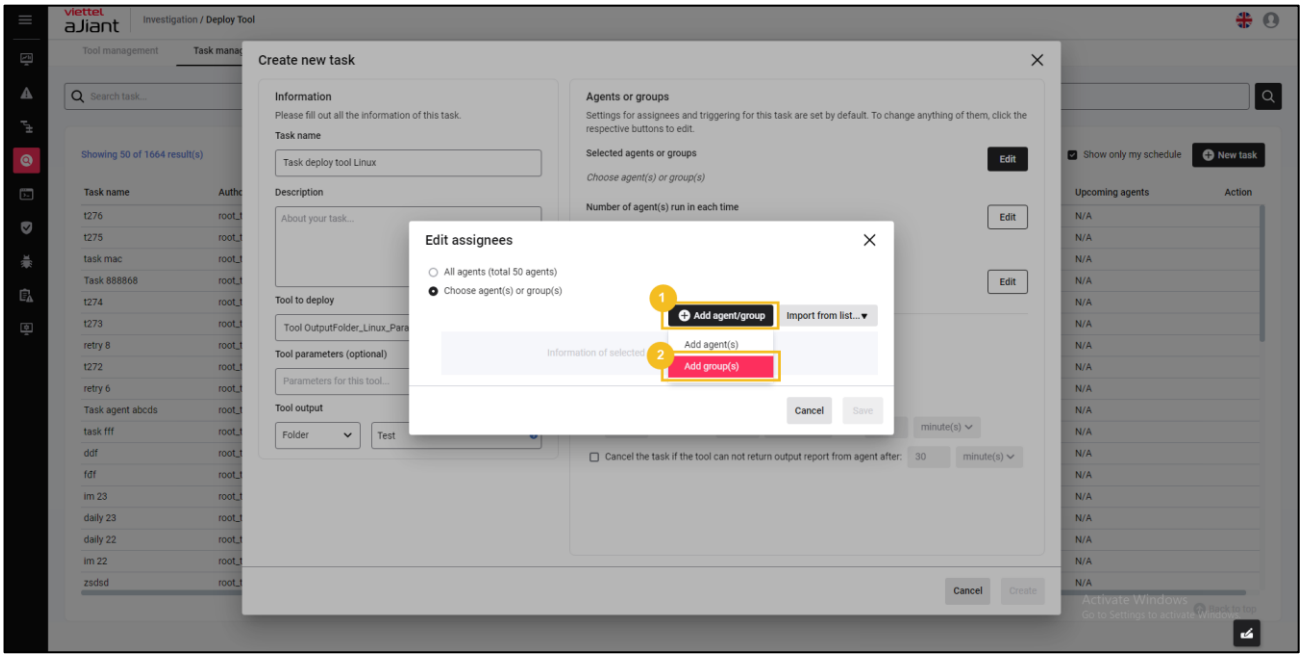
- Hover over the selected Agent(s) > Click the icon to remove the Agent(s) from the selected list.



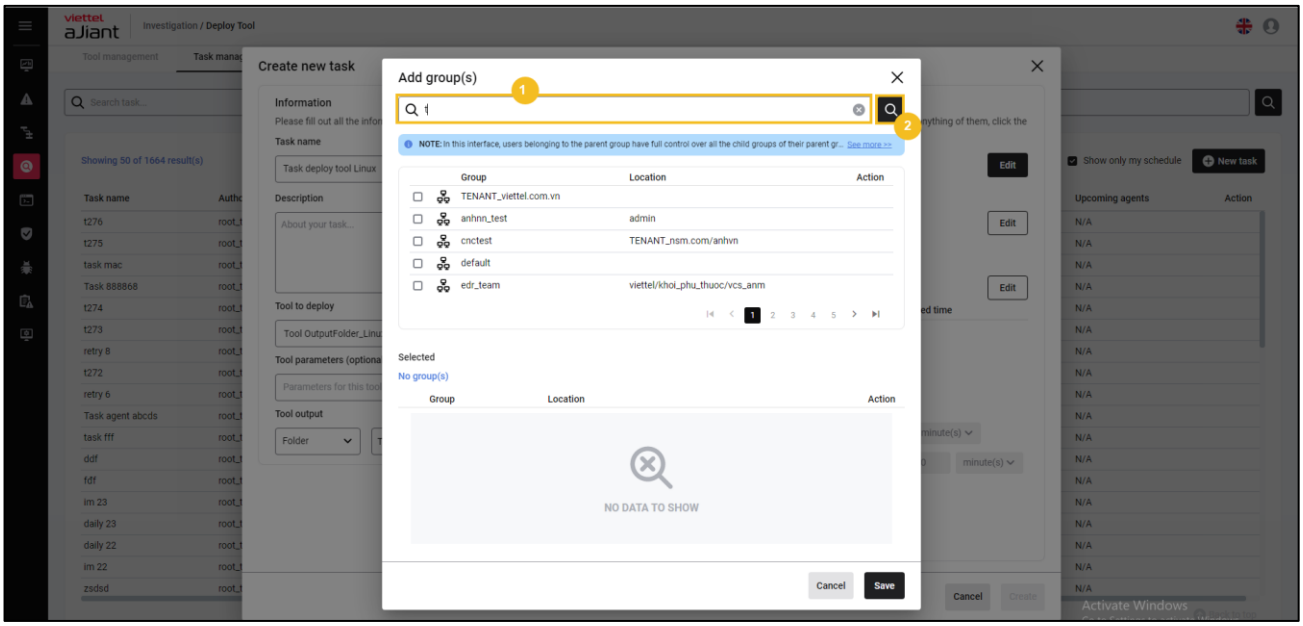
- Select Cancel to cancel or select Save to save the information of the selected Agent(s) for deployment:



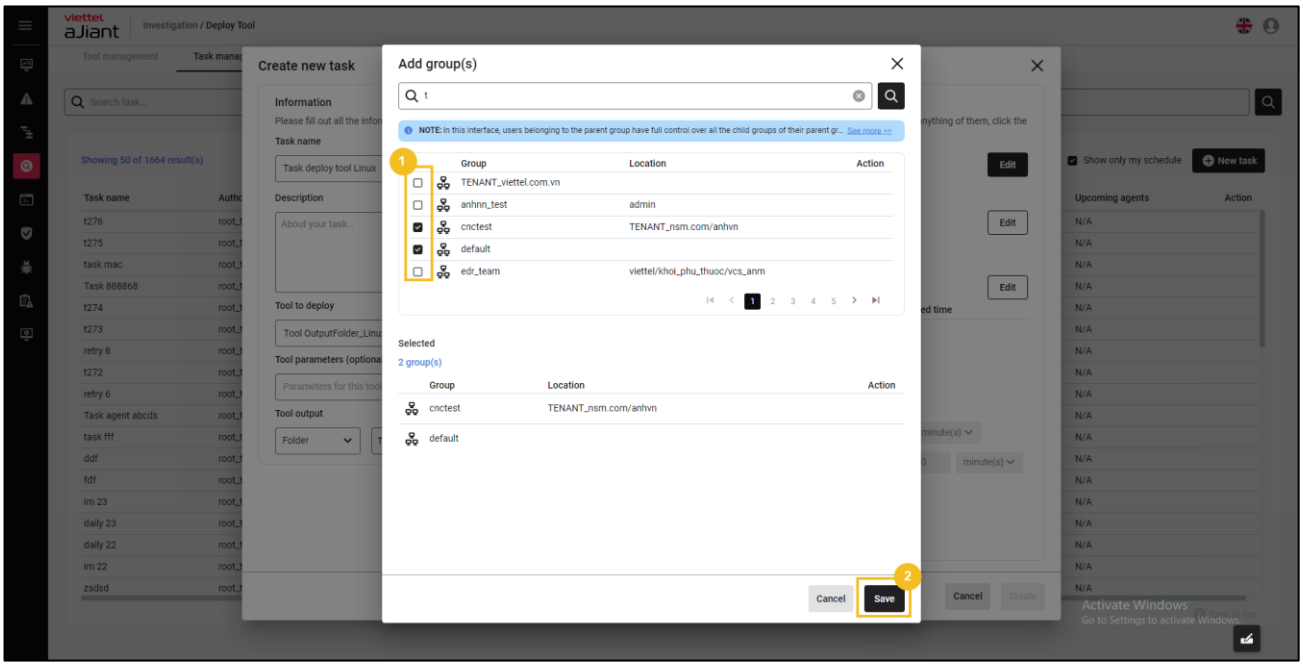
Select Add group(s):



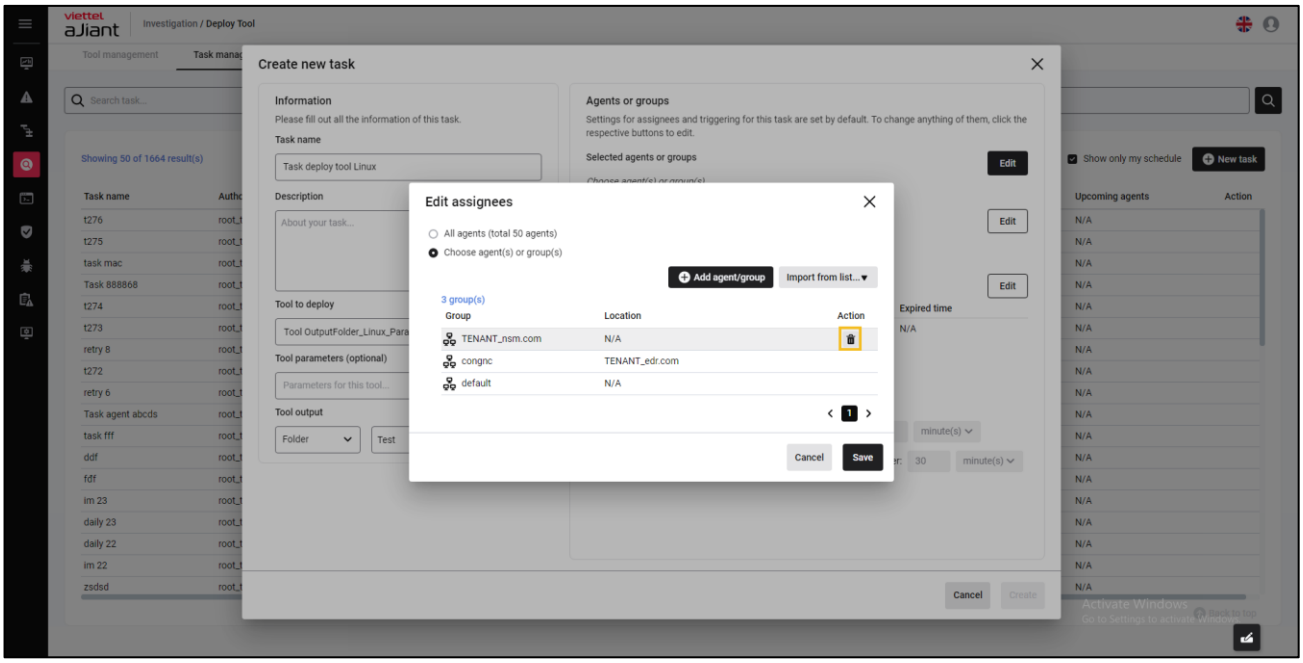
- Search for group(s) by name, allowing input of keywords to search for groups by group name:



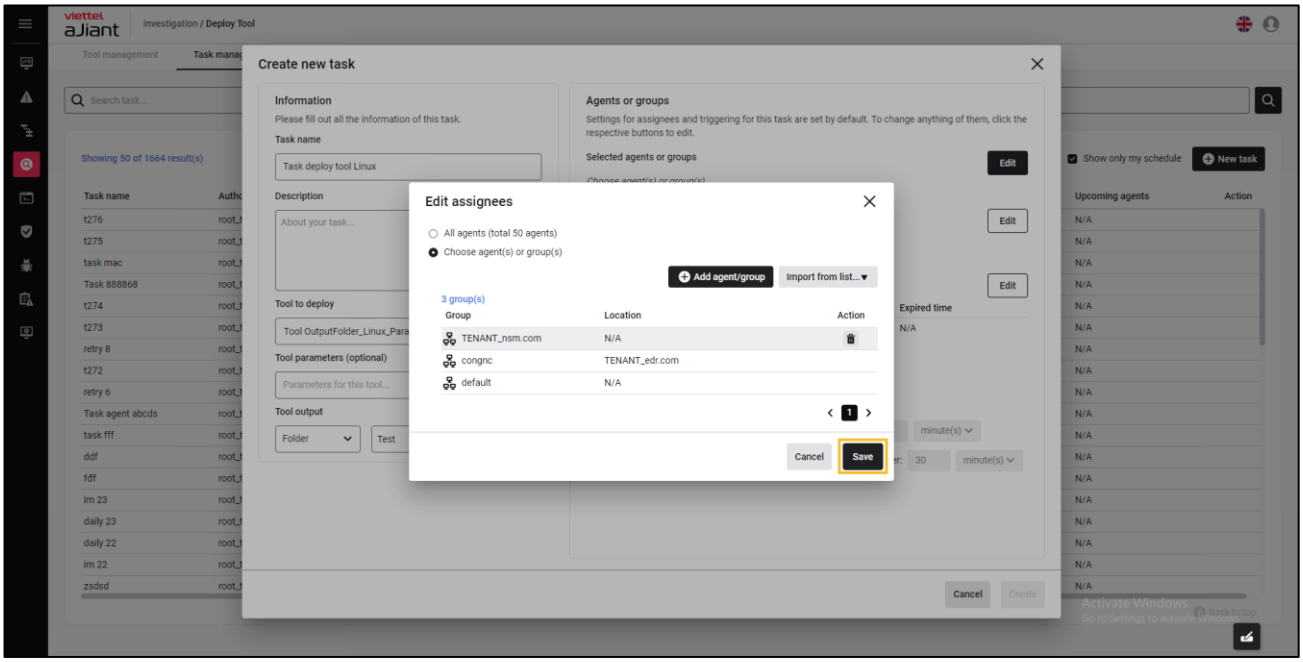
- Select group(s) to deploy by checking one or more groups > Information of the selected group(s) will be displayed in the Selected box > choose Cancel to cancel adding group(s) for deployment or select the Save button to confirm the list of group(s):



  - Hover over the selected group(s) > Click the icon to remove the group(s) from the selected list.



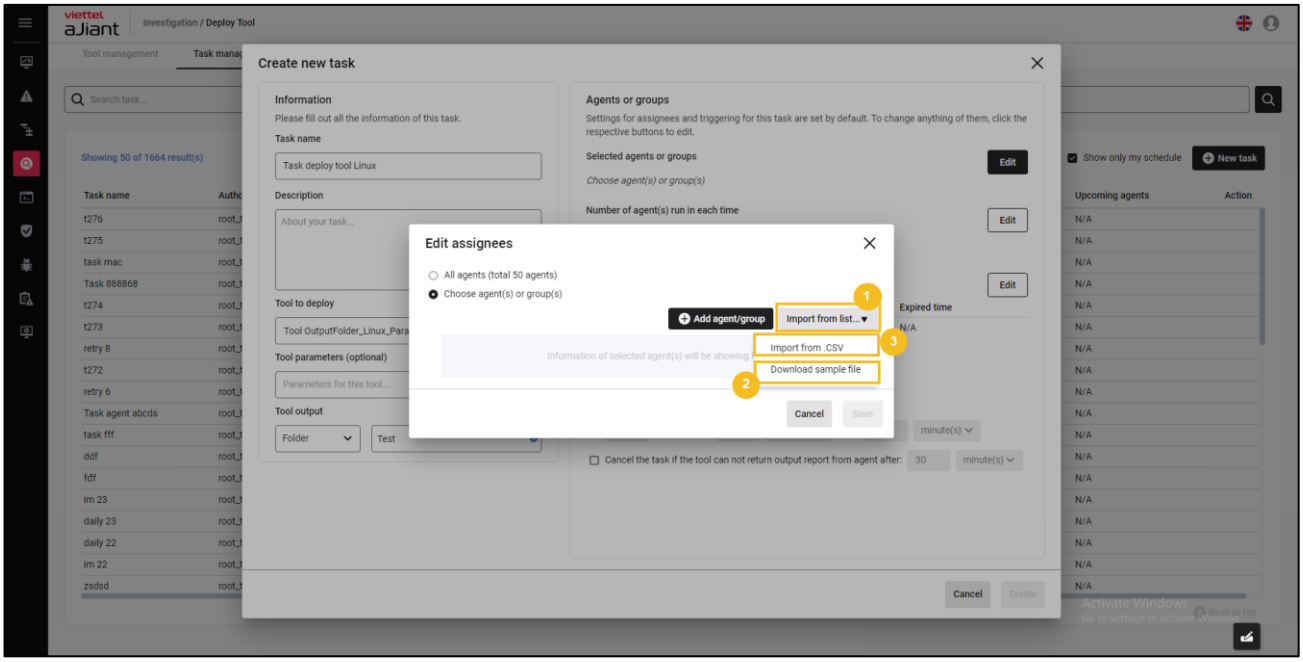
- Select Cancel to abort or select Save for the chosen group(s) to deploy:



Import from list: Allows uploading a list of agents from a .csv file > Select Import from list

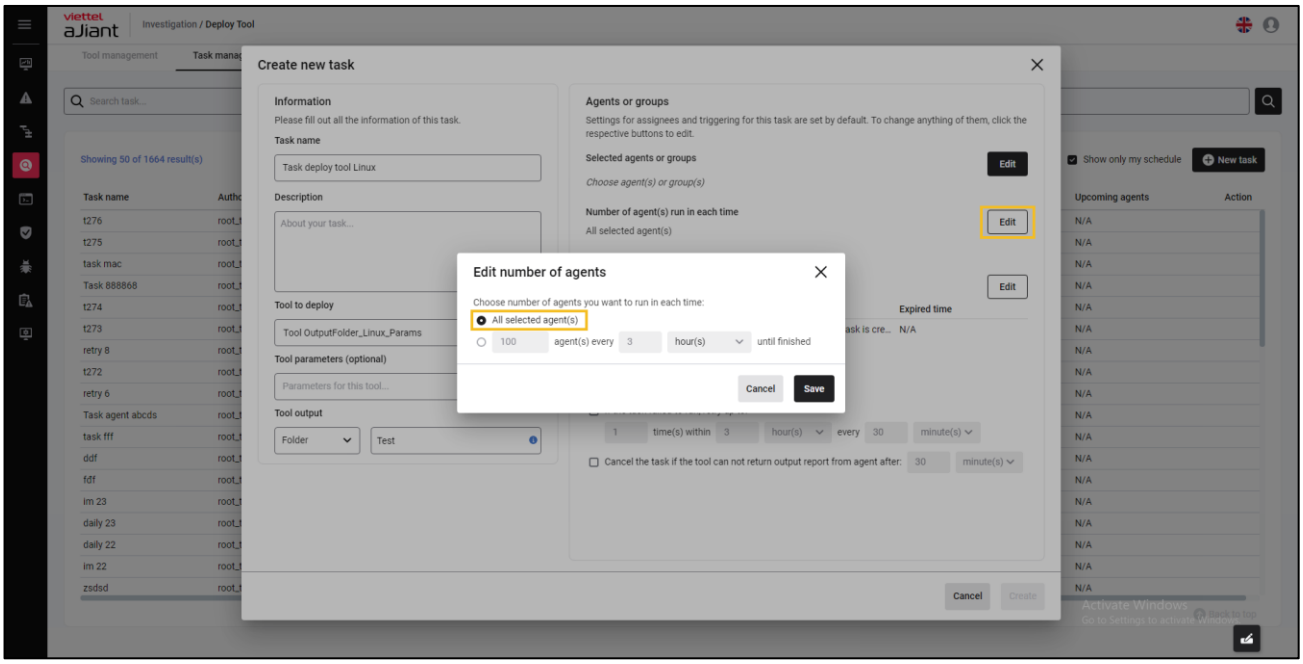
- Select Download sample file to obtain the sample agent(s) file list form;

- Enter agent(s) information > select Import from .CSV to upload the list of agent(s).

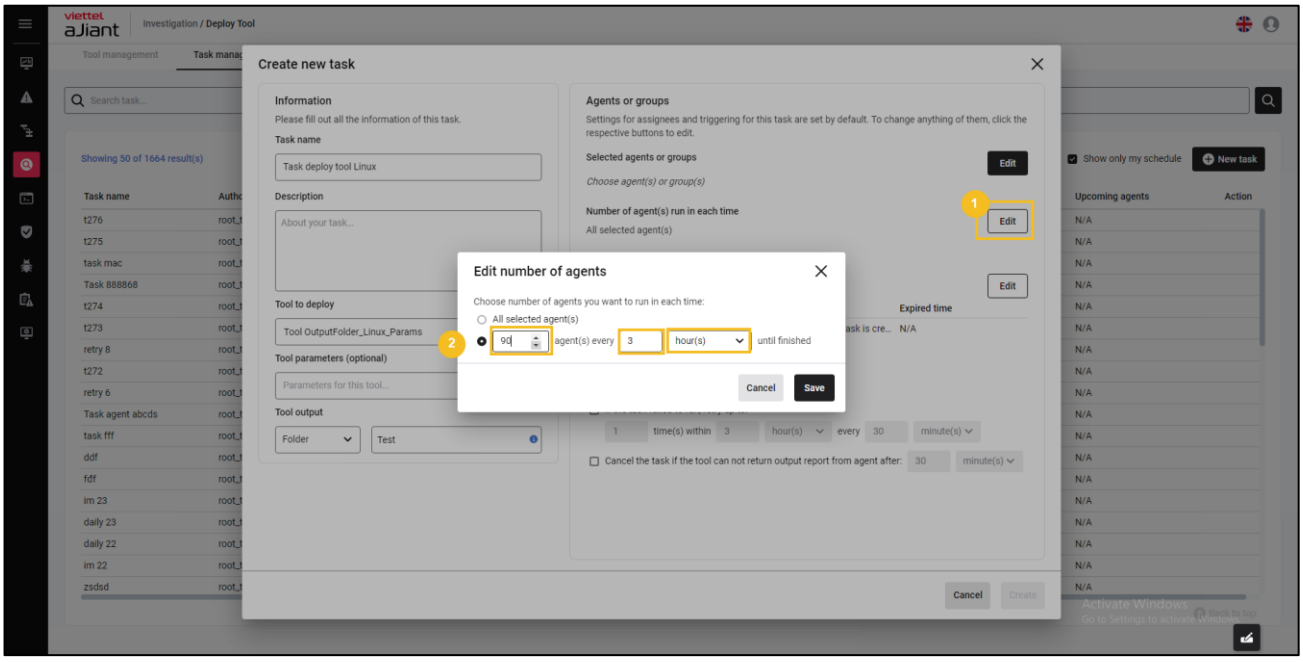


- Configuration of the number of agents deployed per tool each time:

All Agent: Allows deployment of all selected user agent(s)

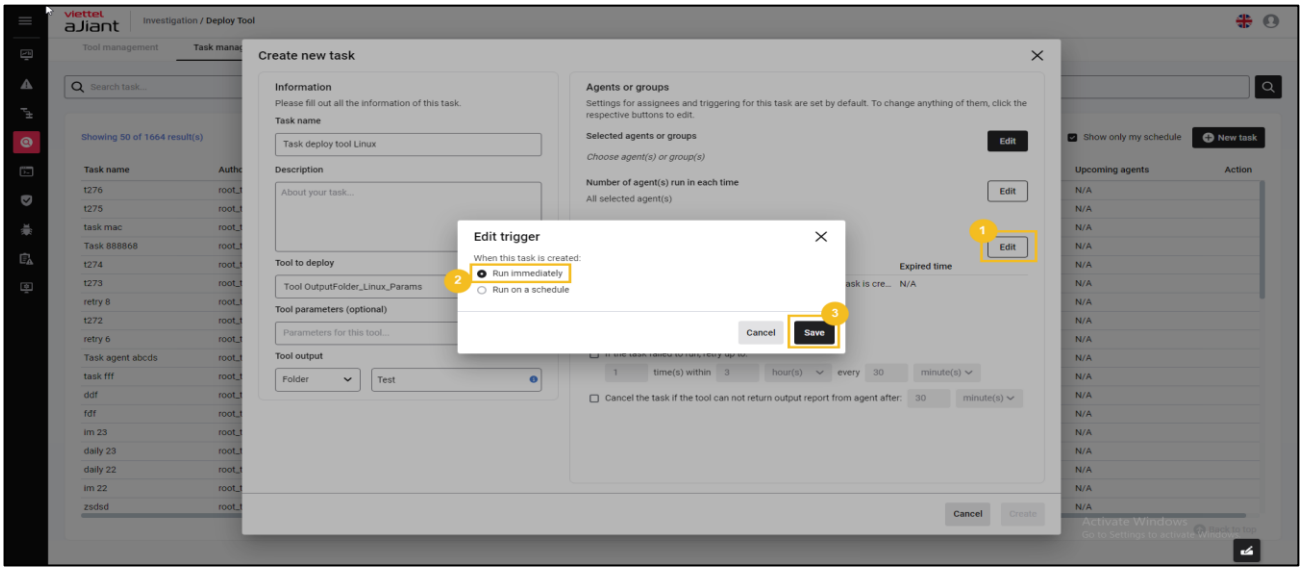


Configure the number of agents per deployment:



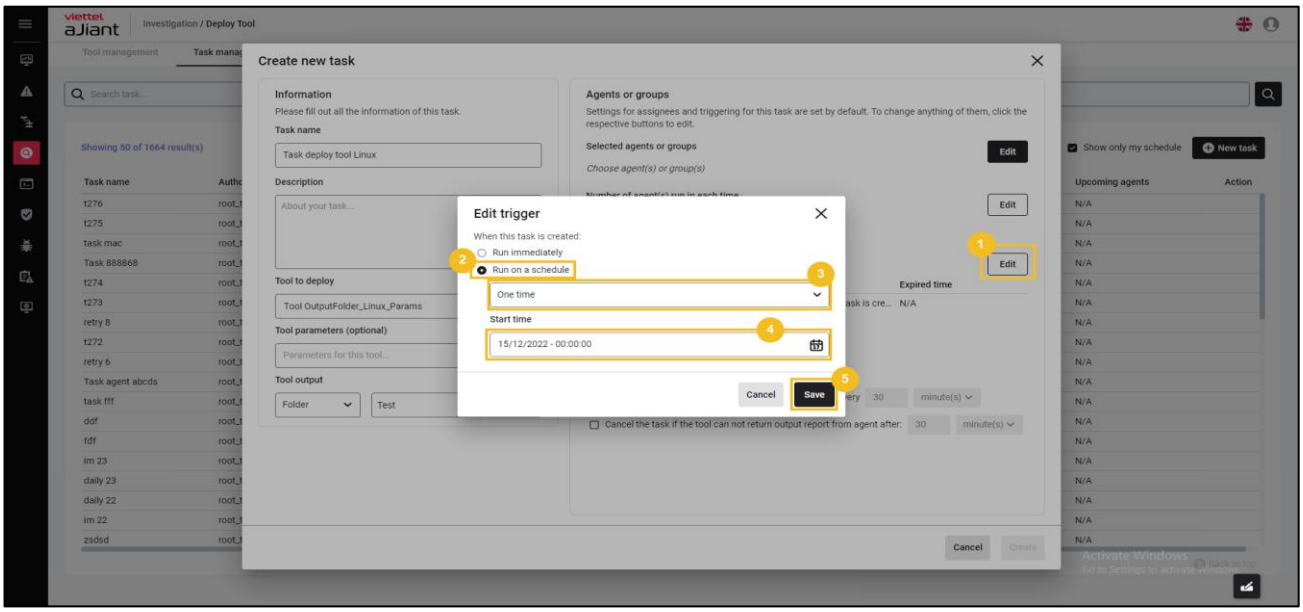
- Configuration of time information (scheduling) for executing the deploy tool:

Select Run immediately to execute the deploy tool configuration right away (after successfully creating the task).

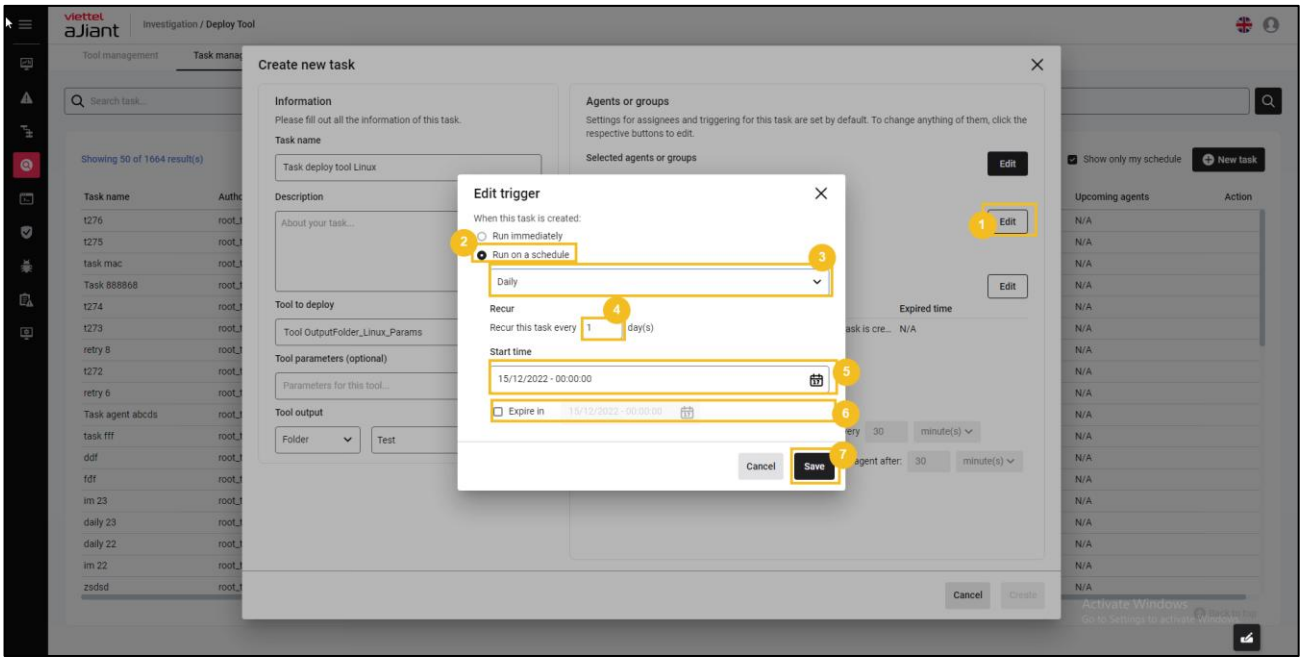


Select Run on schedule to configure the tool deployment timing according to the schedule:

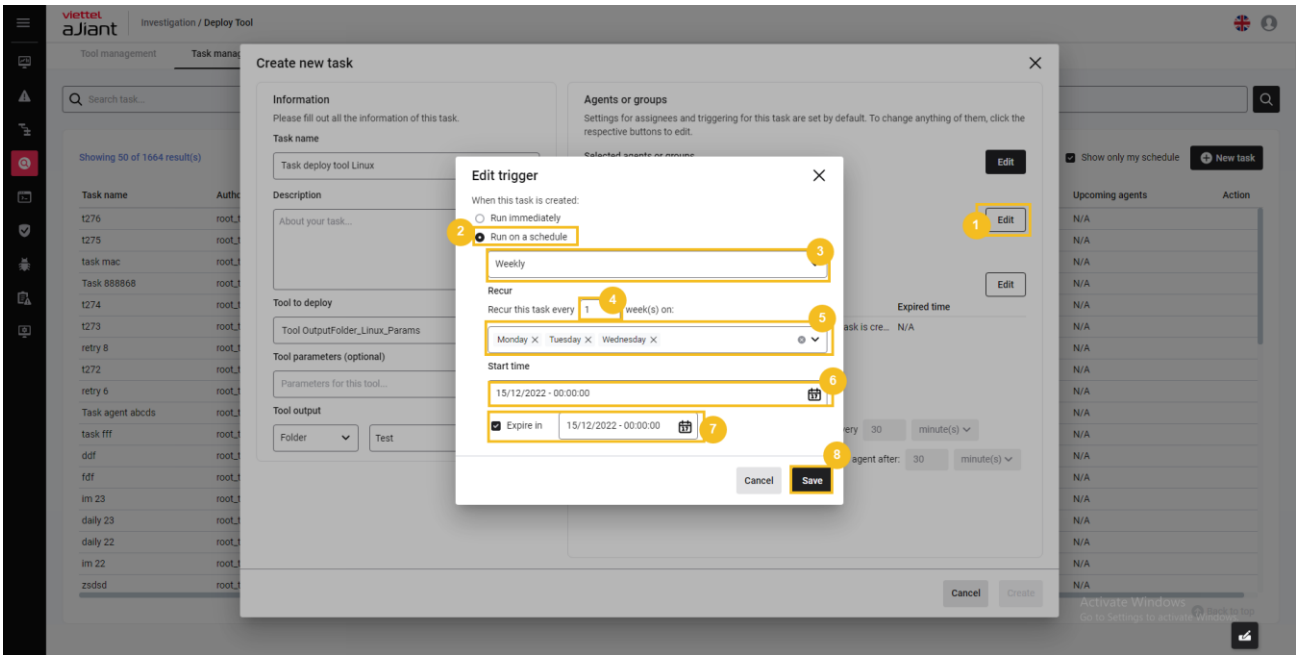
- Select schedule: One time
  - Allow scheduling the deployment tool once;
  - Start time configuration:



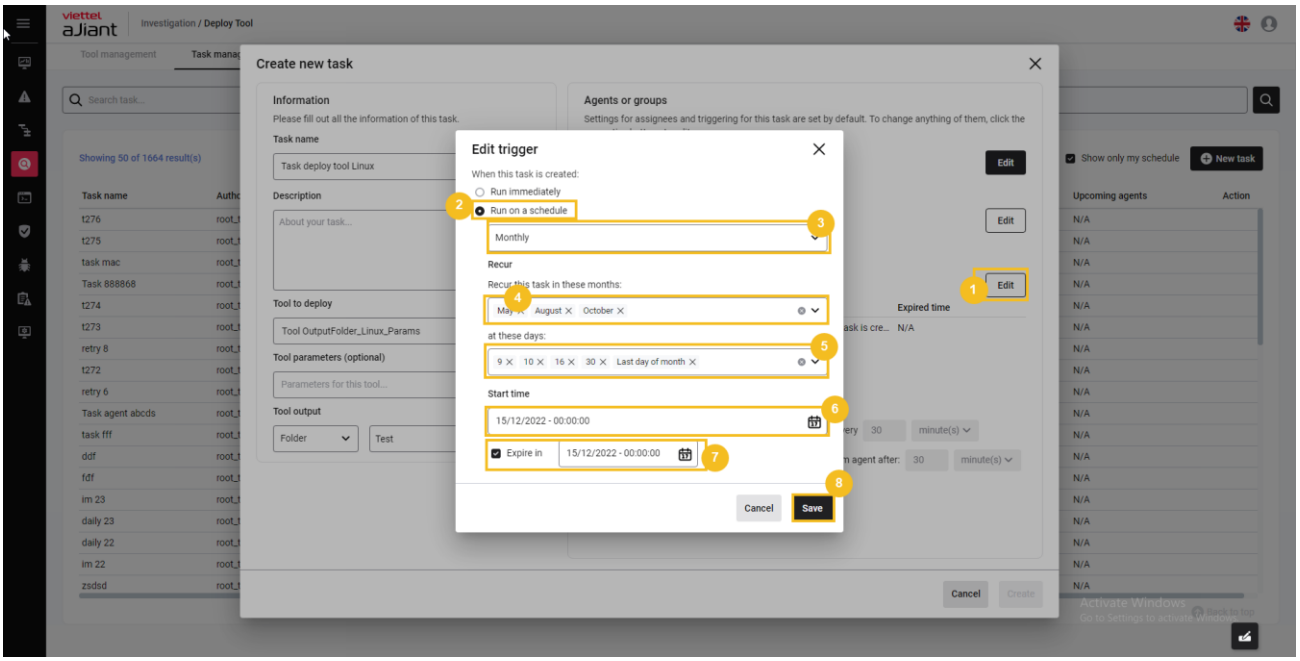
- Select Daily schedule:
  - Allow scheduling of daily tool deployment;
  - Repetition time;
  - Start and end time configuration:



- Select Weekly schedule:
  - Allow scheduling of weekly tool deployment;
  - Repetition time;
  - Start and end time configuration:



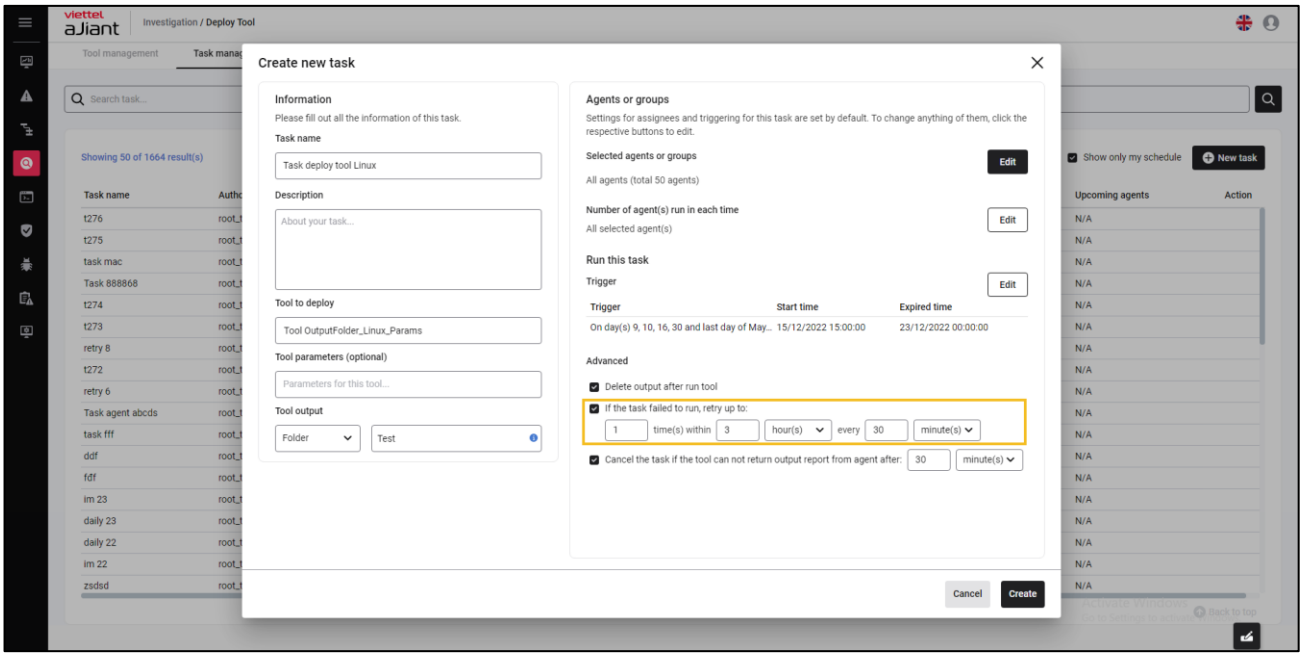
- Select Monthly schedule:
  - Allow scheduling of monthly tool deployments;
  - Repetition time;
  - Start and end time configuration:



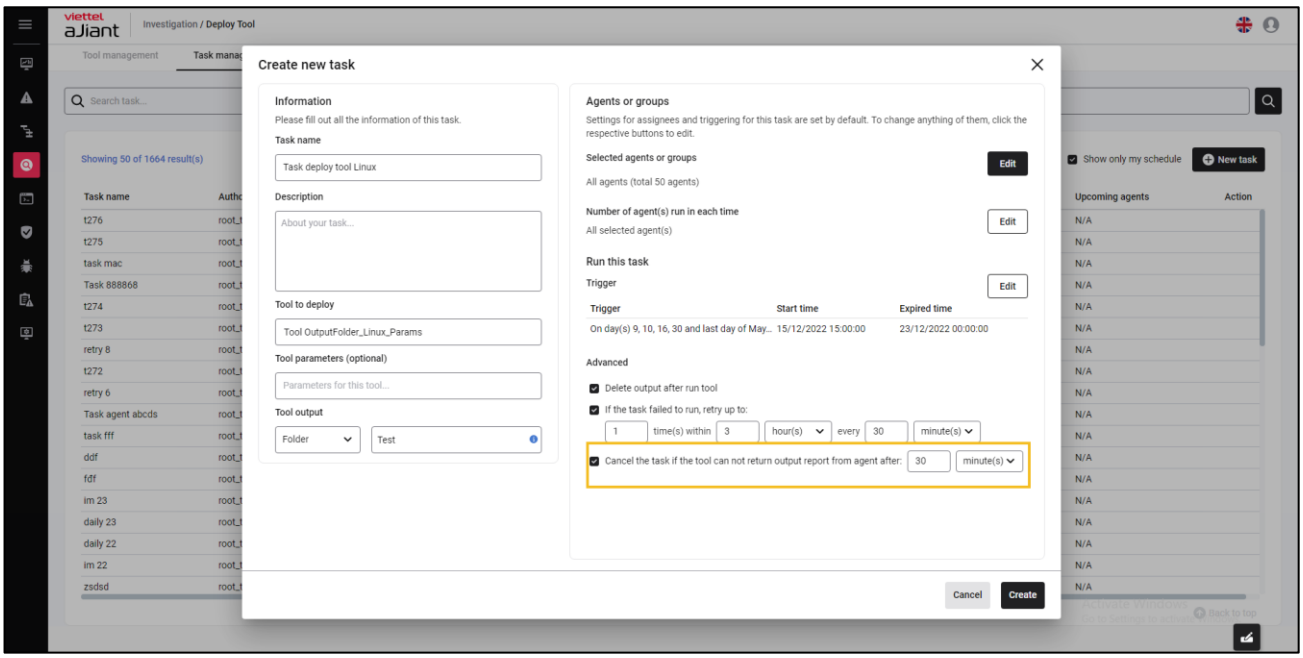
- Advanced information configuration for the task

Delete tool after run tool allows the tool output to be deleted after running the tool and successfully returning the result to the backend.

If the task fails to run, retry up to a specified limit when the task deployment fails, allowing configuration of the retry task information (redeploy the task).



Allow canceling the task if the tool cannot return an output report from the agent after permitting task cancellation when the task cannot run within the user-configured time.

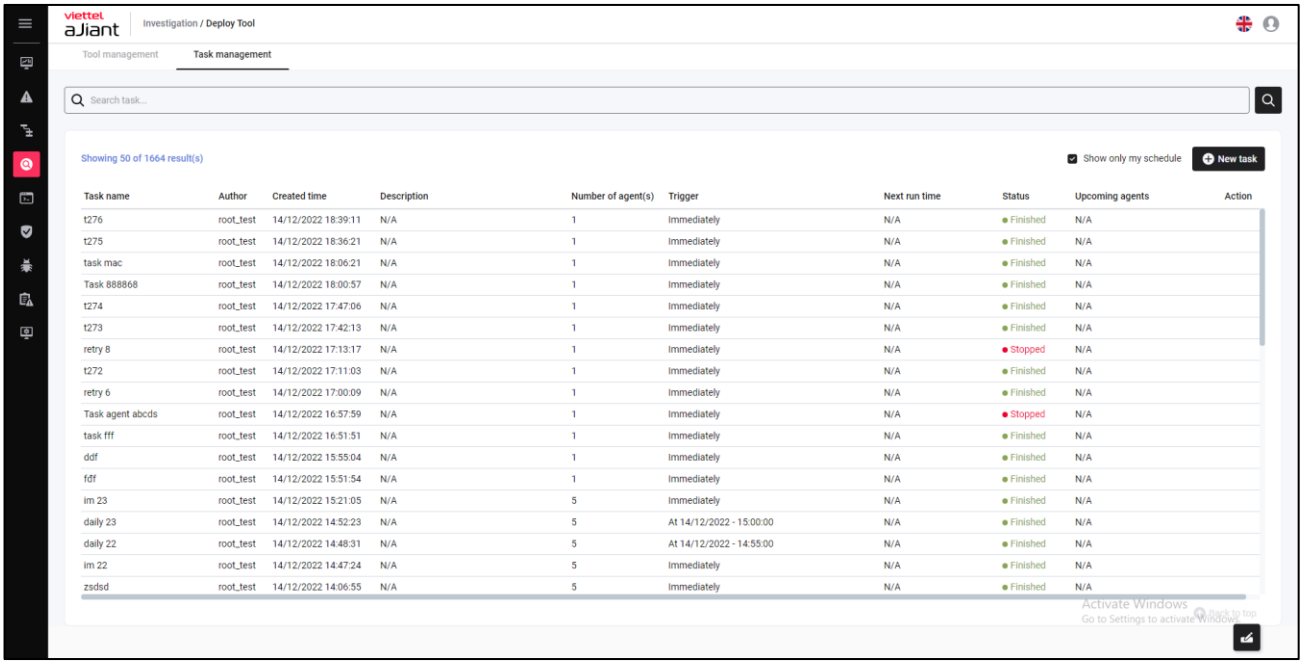


- Select Create to create a new task/configure deploy tool information under the agent, or select Cancel to cancel the task/configuration of deploy tool information under the agent.

Manage task

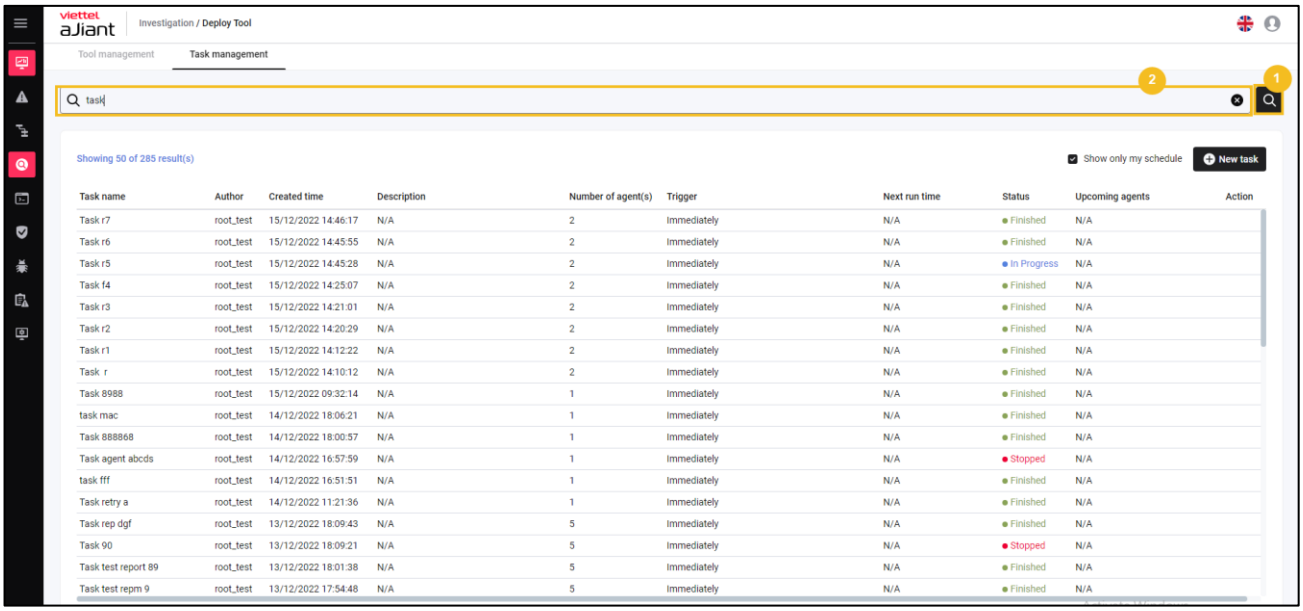
a. Task list

Purpose: Display the list of scheduled deployment tool tasks;
Displayed information fields: Task name, Author, Created time, Description, Number of agent(s), Trigger, Next run time, Status, Upcoming agents



b. Search for task

Purpose: To allow searching for tasks by task name;
Steps to follow: Enter the search keyword > select the Search button or finish entering the keyword > press enter. The system will perform a search for Agent information related to the search keyword available in the system.



c. Create a task

(Function similar to section 3.5.4.2. Deploy tool)

Purpose: Configure deploy tool information under the agent
Conditions:

User logged in as root group: Display all Agents in the system active for less than 30 days;

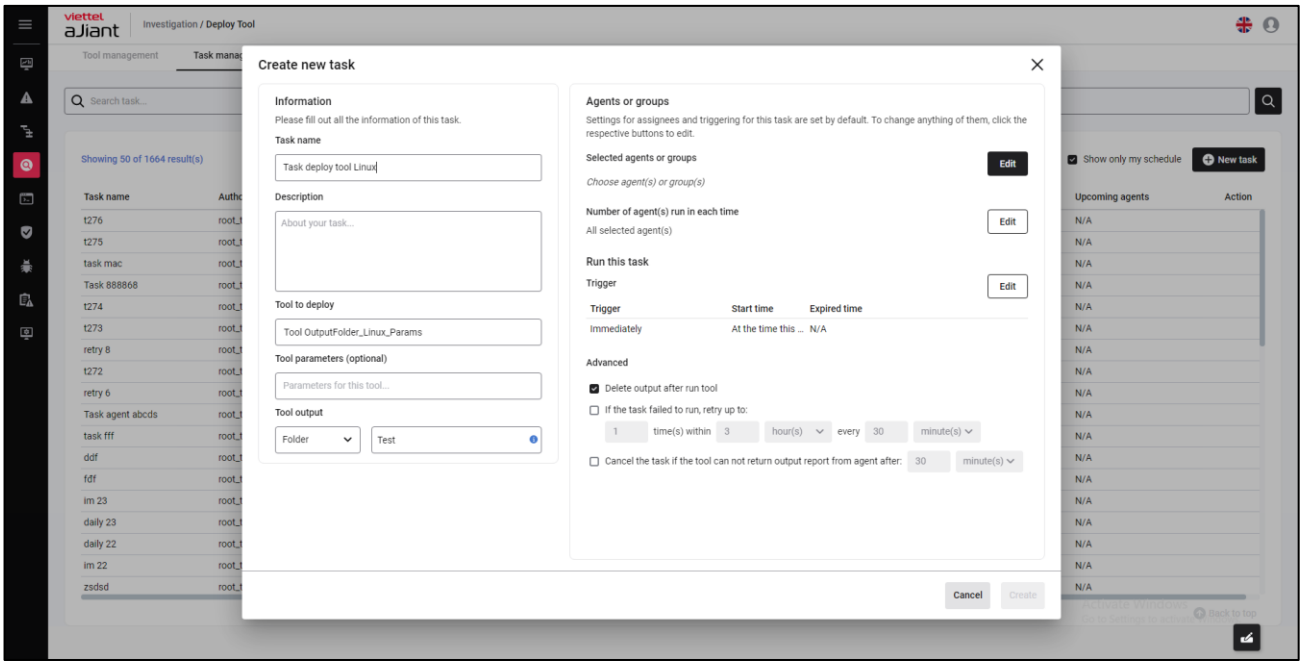
User logged in belongs to the default group: Display all Agents belonging to the default group;

User login belongs to parent group: Display all Agents belonging to the user's current group and the corresponding child groups;

User logged in belongs to one or more sub-groups: Display all Agents belonging to the user's group currently logged in;

Steps to deploy the tool in the Task Management tab:

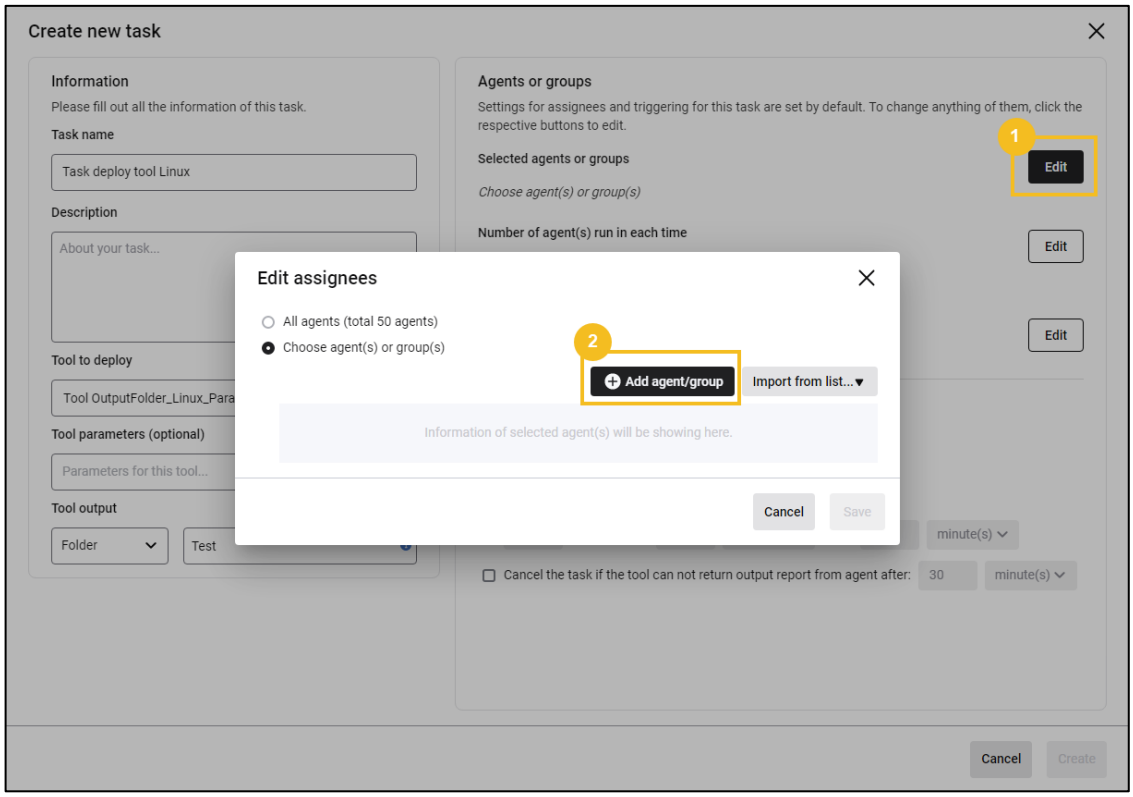
- After selecting the tool, click the icon on the tool record you want to deploy > select Deploy this tool, the Create new task screen will appear:



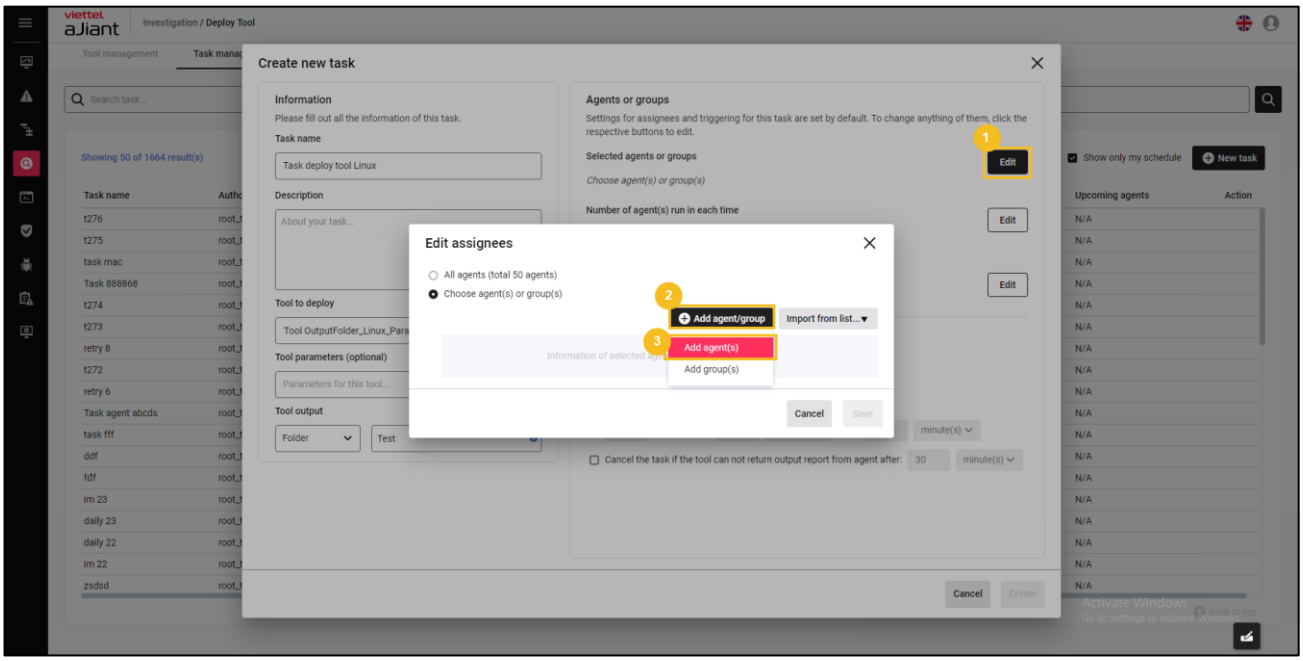
- Enter the task information for deploying the tool: Task name, Tool to deploy, Description, Tool parameters, Tool output;
- Select the group and workstation (agent) information for deployment:

Select All agent(s): choose all agents within the management scope of the currently logged-in user to perform deployment;

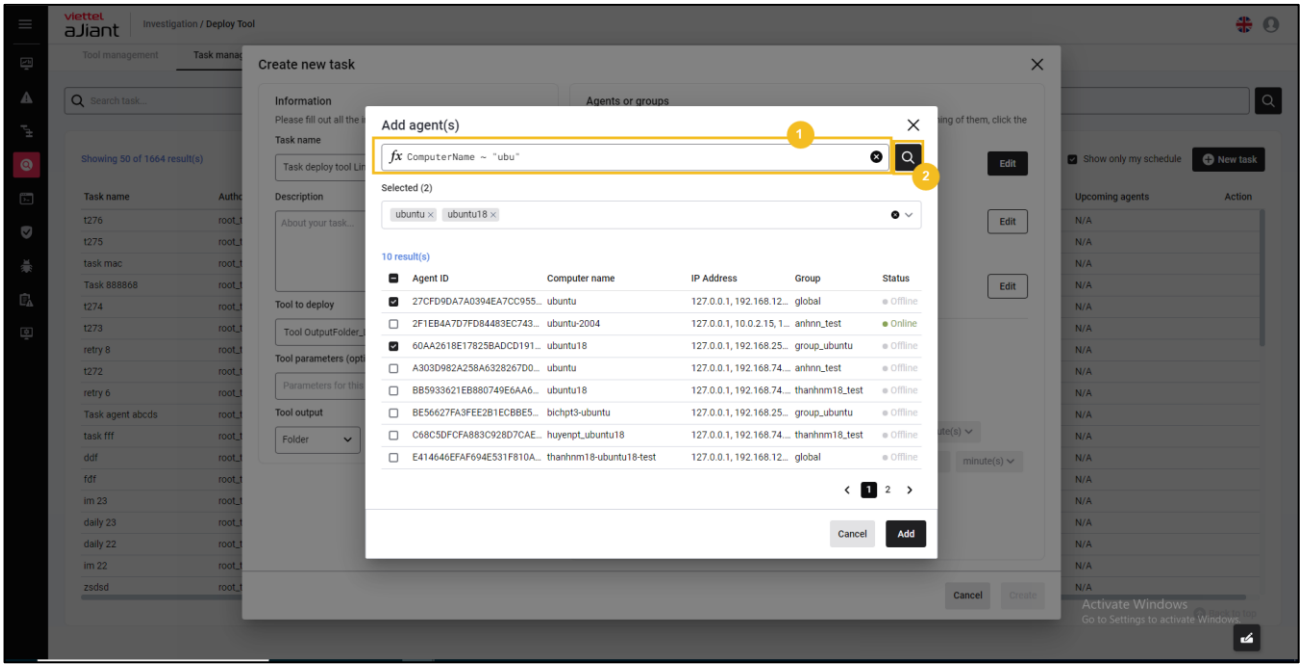
Select agents or groups to perform deployment – Choose agent(s) or group(s):



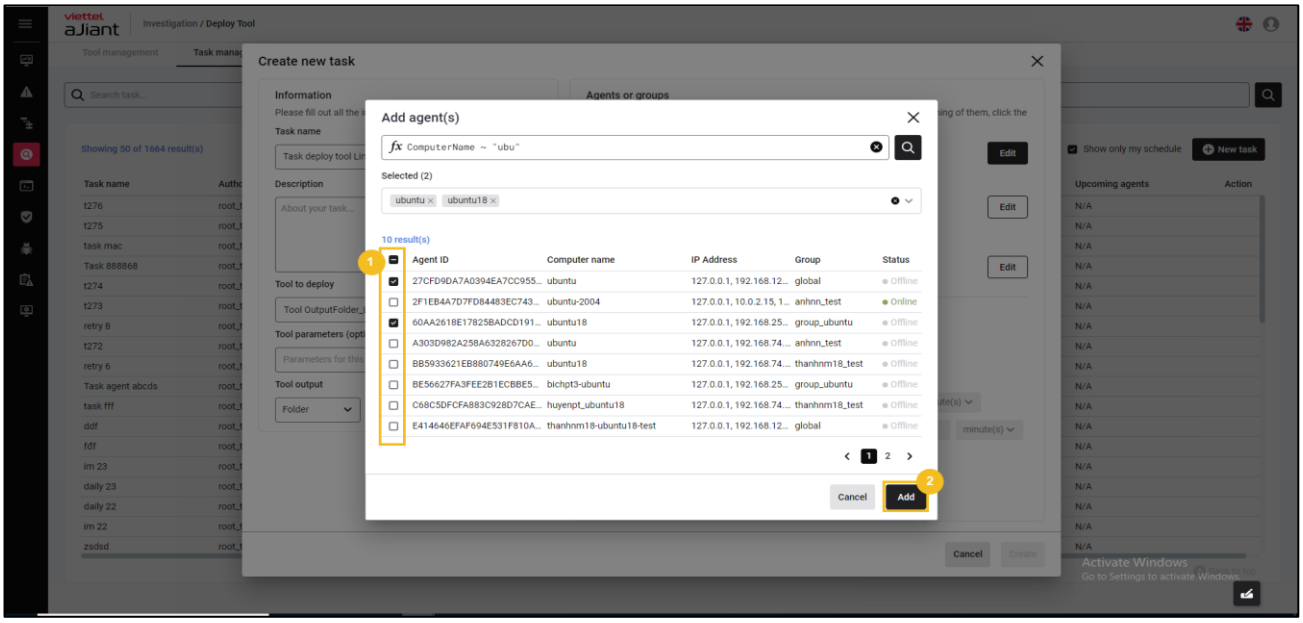
Select Add agent(s):



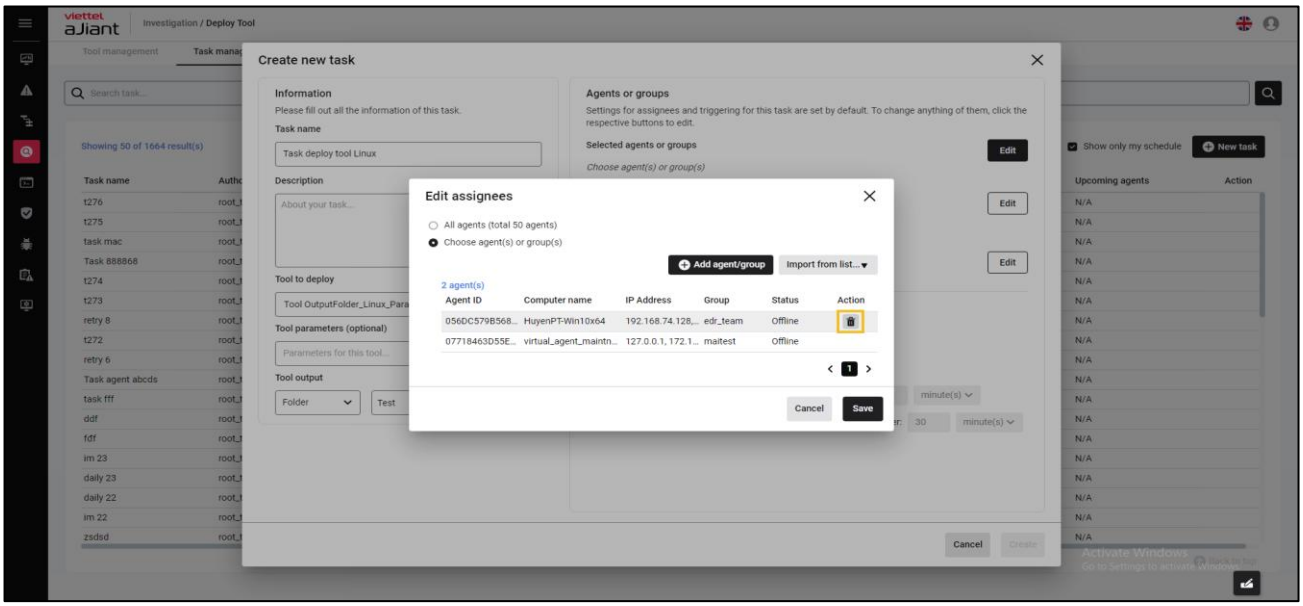
- Search Agent: Allows creating query statements and using query statements to search for Agents.



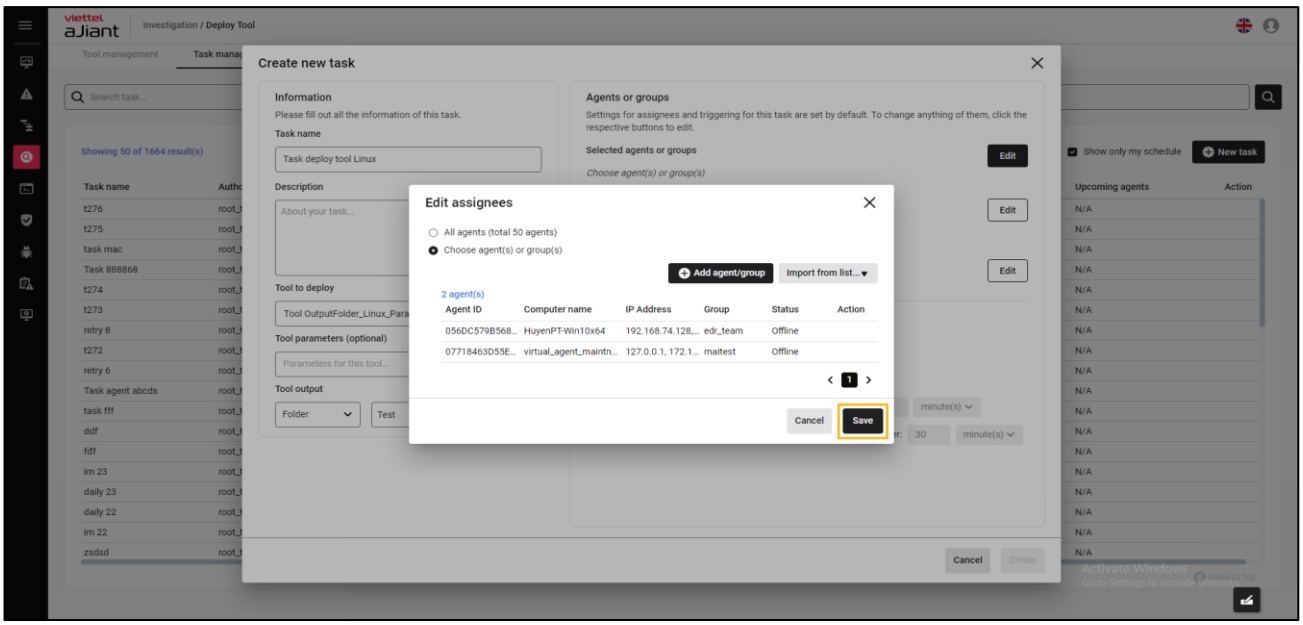
- Select the Agent(s) to deploy by checking one or more Agents > Information of the selected Agent(s) will be displayed in the Selected box > choose Cancel to cancel adding Agents for deployment or click the Add button to confirm the list of Agent(s):



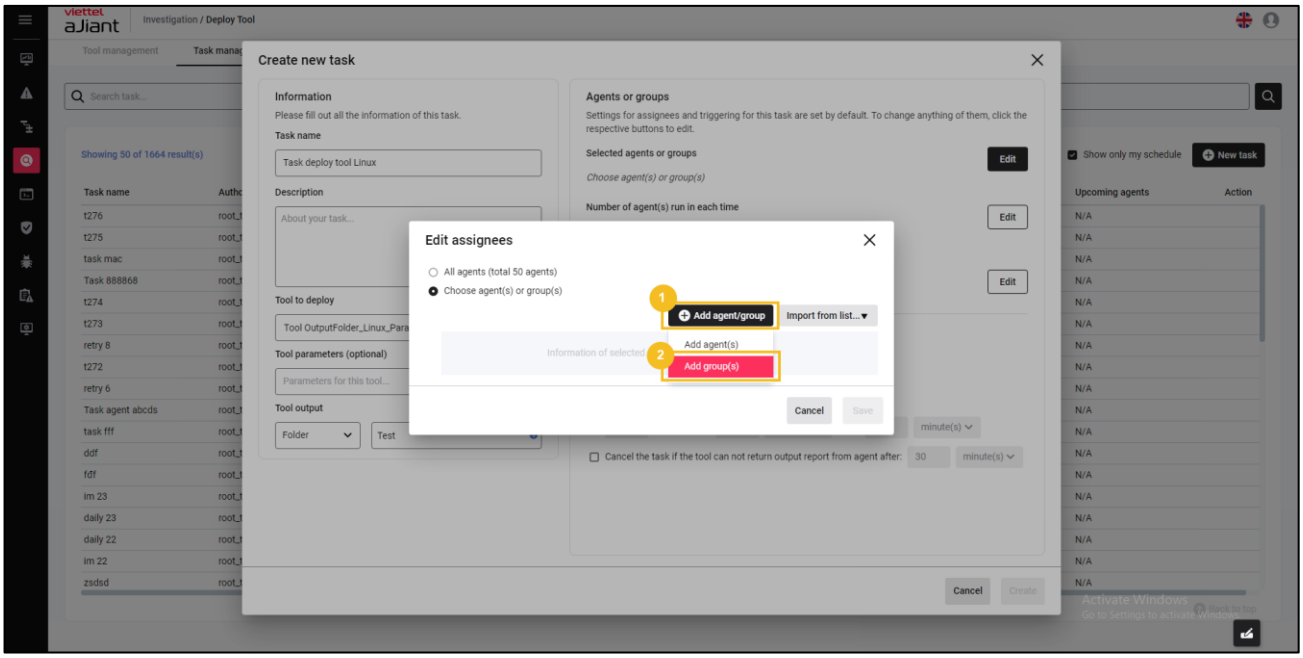
- Hover over the selected Agent(s) > Click the icon to remove the Agent(s) from the selected list:



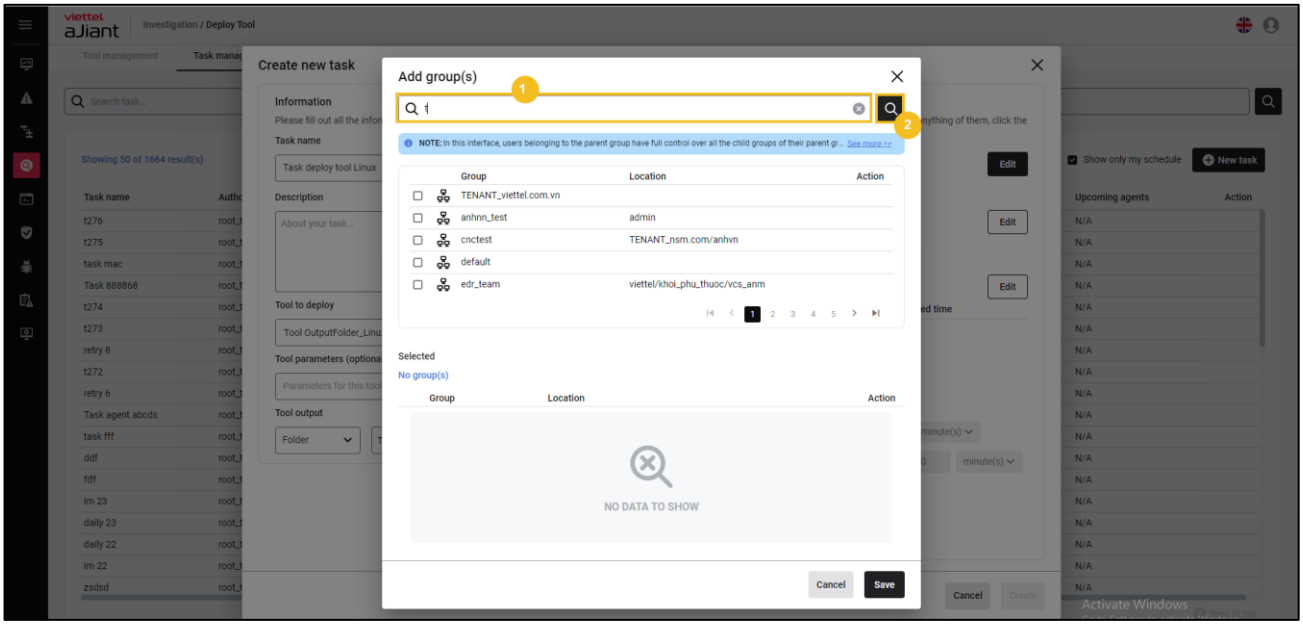
- Select Cancel to cancel or select Save to save the information of the selected Agent(s) for deployment:



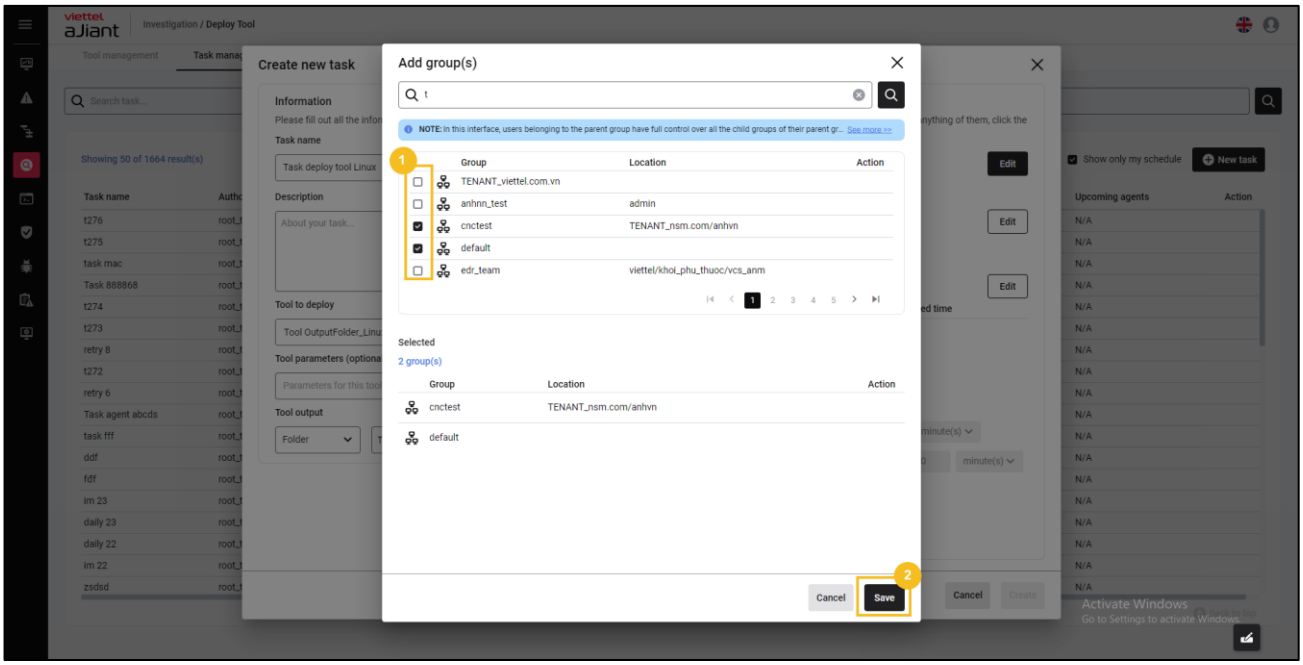
Select Add group(s):



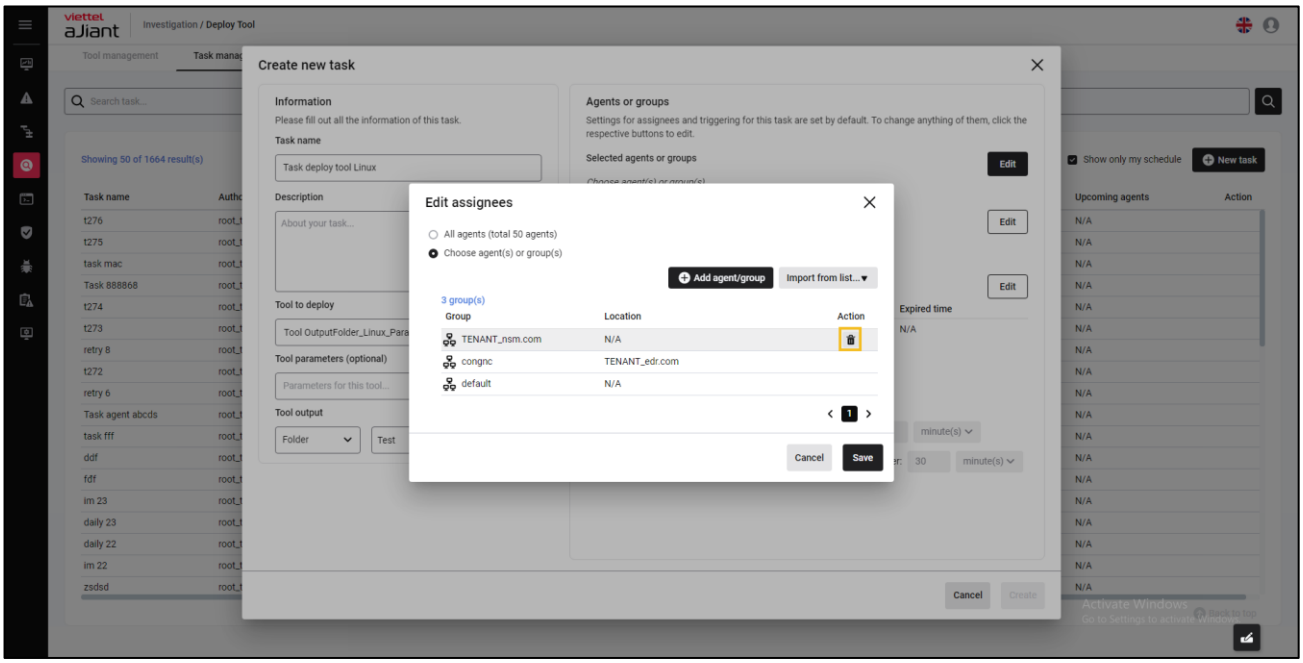
- Search for group(s) by name, allowing input of keywords to search for groups by group name:



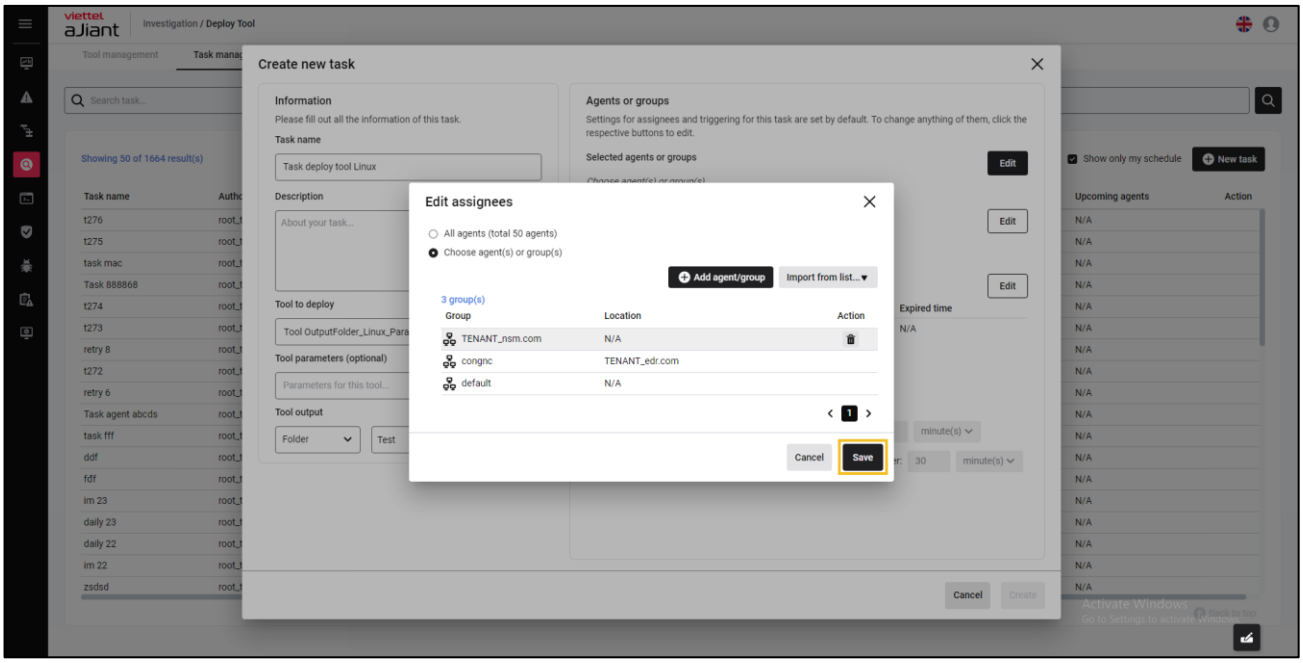
- Select the group(s) to deploy by checking one or more groups > Information of the selected group(s) will be displayed in the Selected box > choose Cancel to cancel adding group(s) for deployment or click the Save button to confirm the list of group(s):



- Hover over the selected group(s) > Click the icon to remove the group(s) from the selected list.

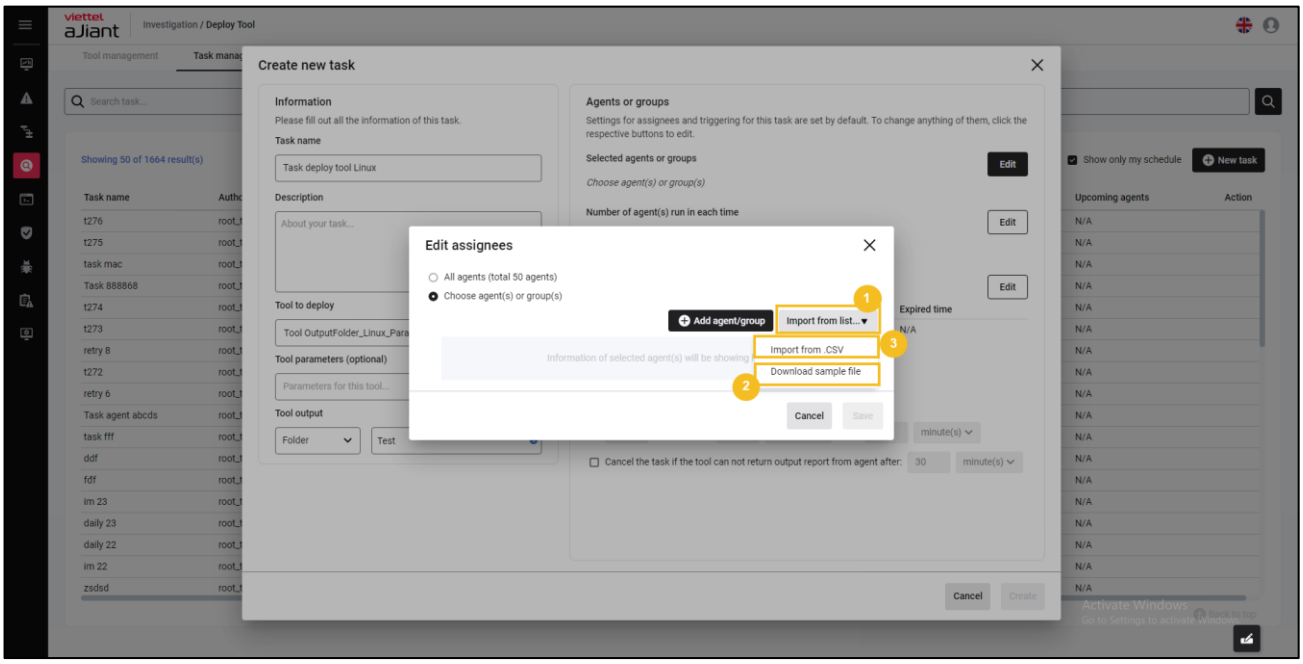


- Select Cancel to cancel or select Save to deploy the selected group(s):



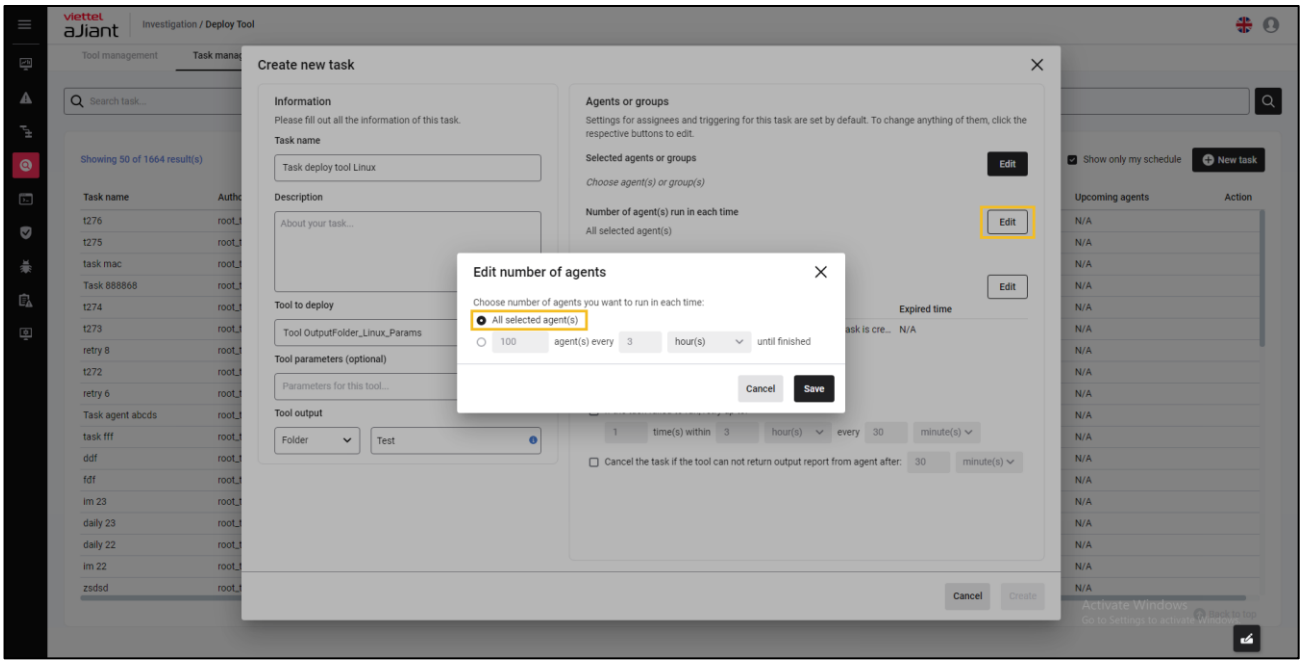
Import from list: Allows uploading a list of agents from a .csv file > Select Import from list

- Select Download sample file to obtain the sample agent(s) file list form;
- Enter agent(s) information > select Import from .CSV to upload the list of agent(s).

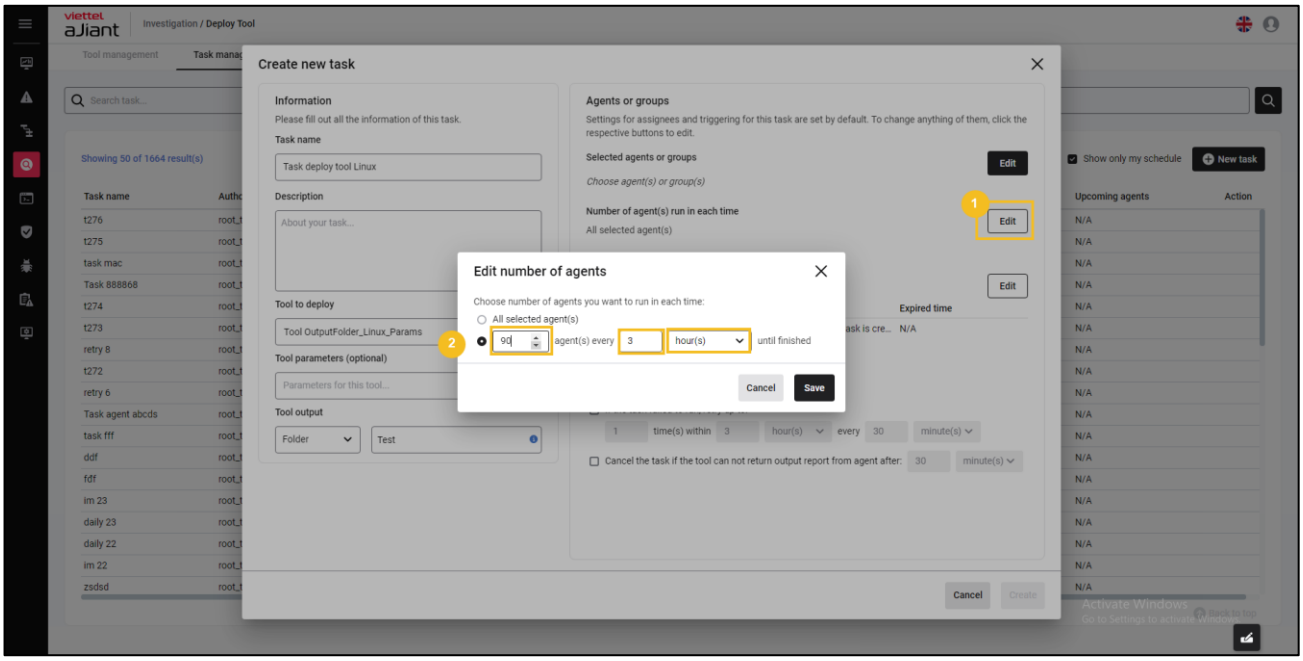


- Configuration of the number of agents deployed per tool each time:

All Agent: Allows deployment of all selected user agent(s)

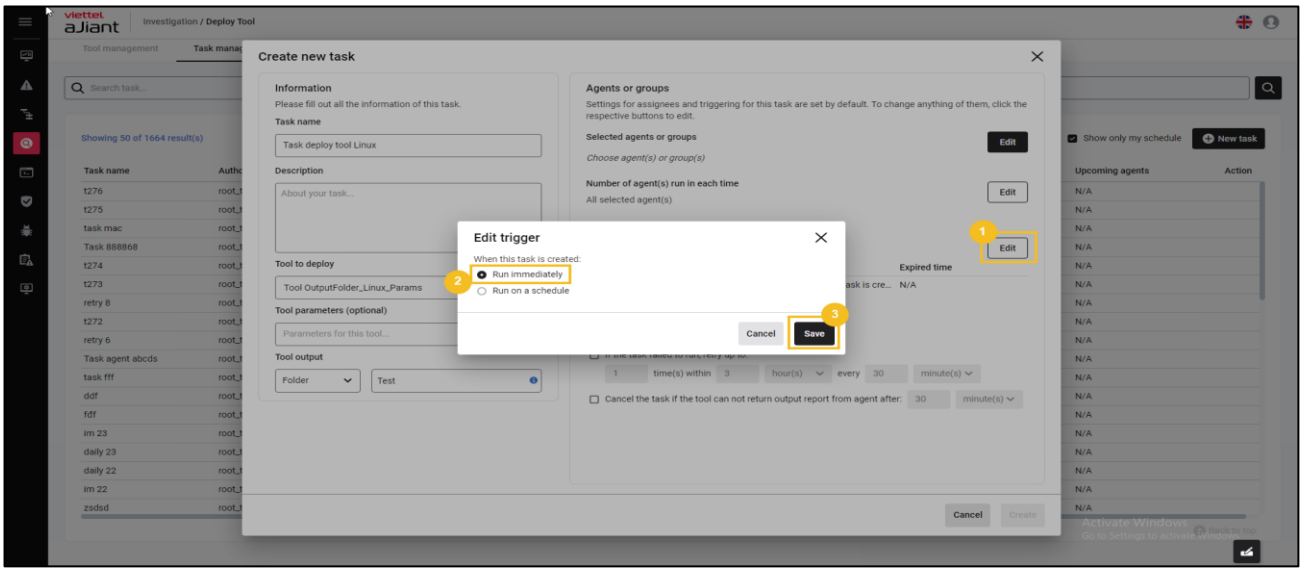


Configuration of the number of agents per deployment:



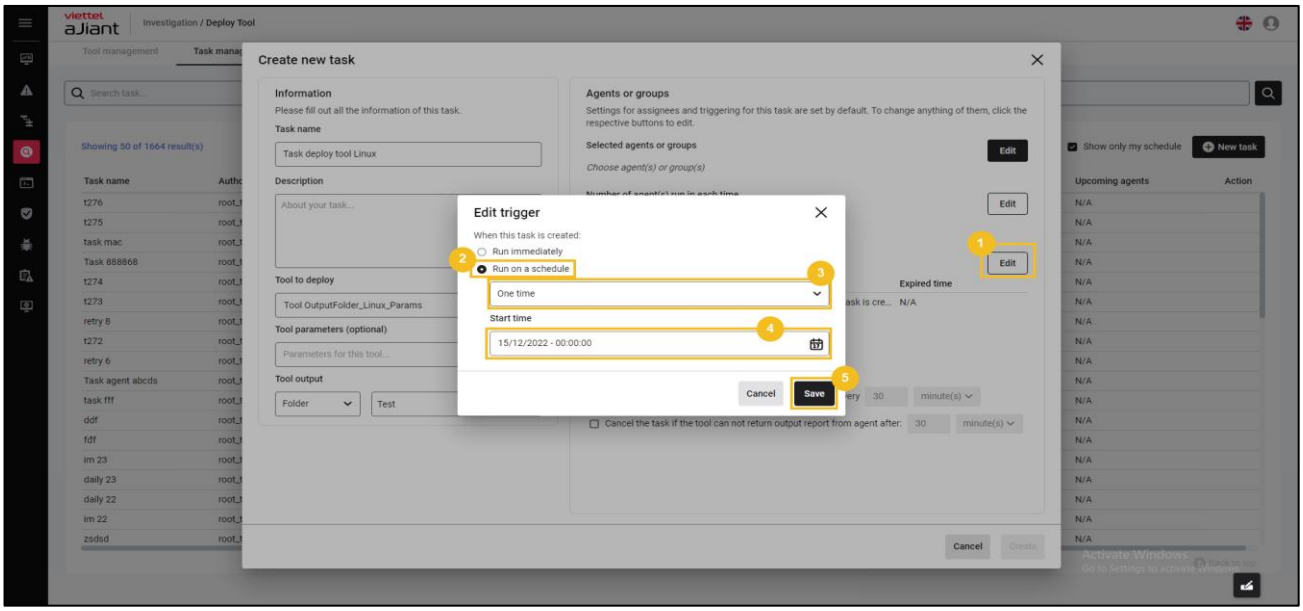
- Configuration of time information (scheduling) for executing the deploy tool:

Select Run immediately to execute the deploy tool configuration right away (after successfully creating the task).

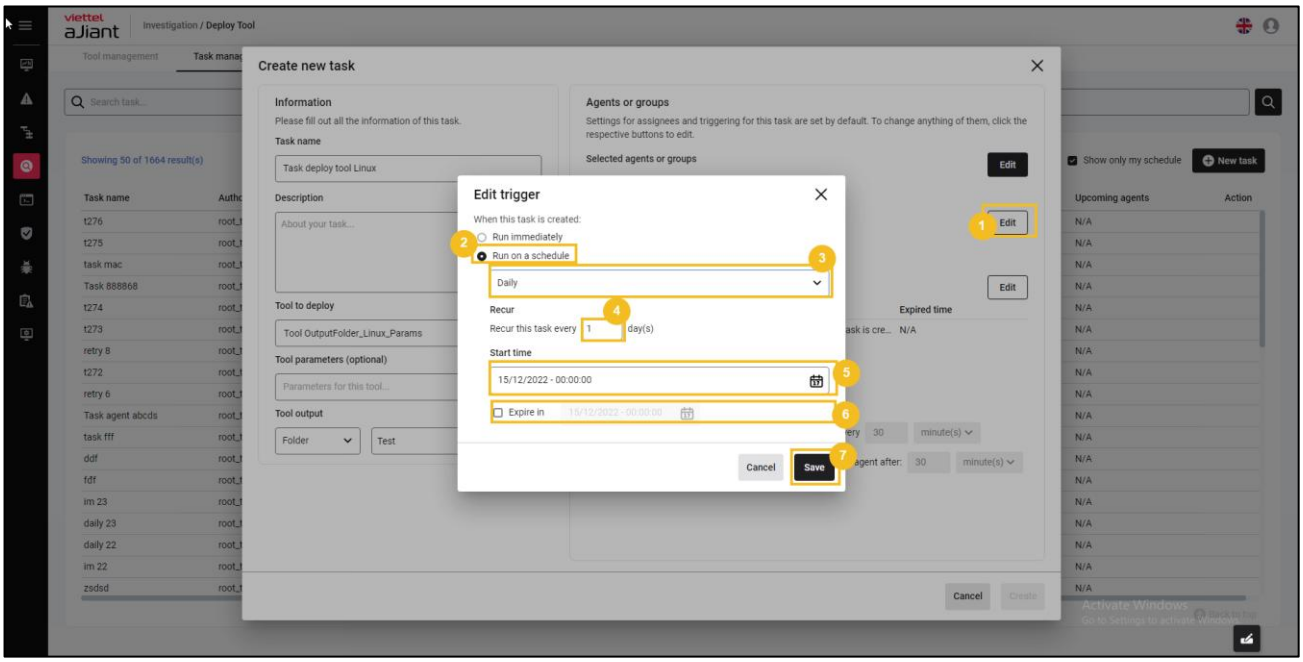


Select Run on schedule to configure the tool deployment timing according to the schedule:

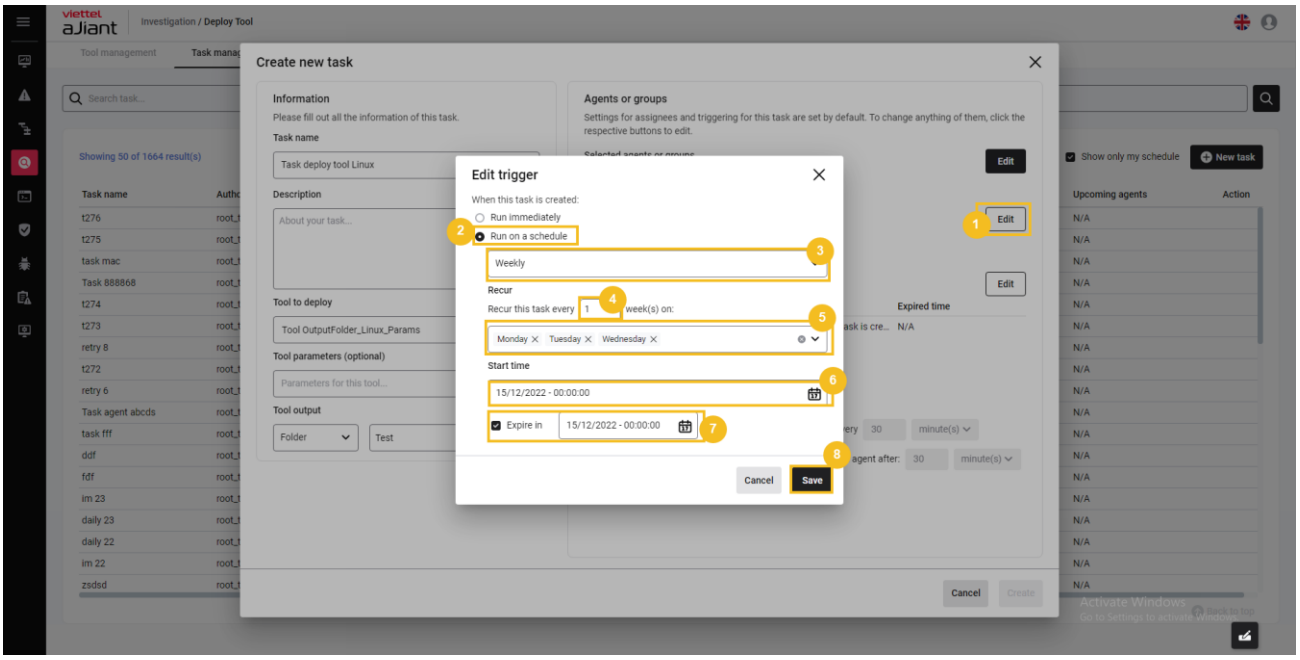
- Select schedule One time:
  - Allow scheduling the deployment tool once;
  - Start time configuration:



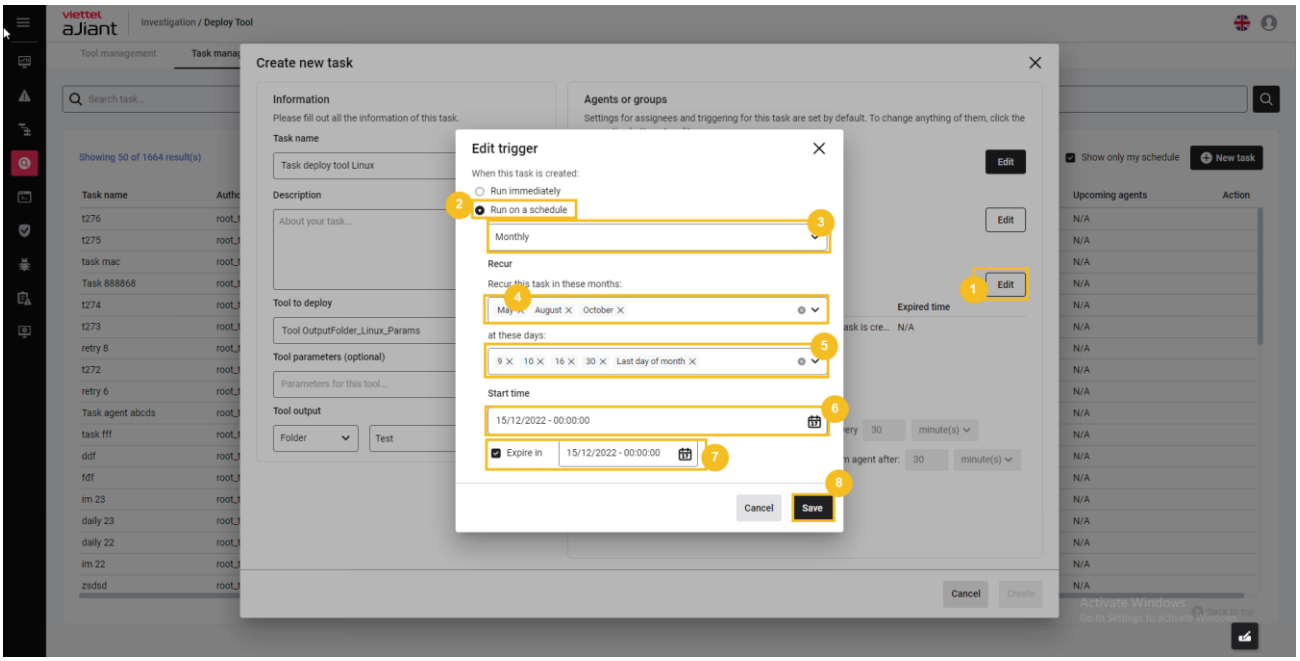
- Select Daily schedule:
  - Allow scheduling of daily tool deployment;
  - Repetition time;
  - Start and end time configuration:



- Select Weekly schedule:
  - Allow scheduling of weekly tool deployments;
  - Repetition time;
  - Start and end time configuration:



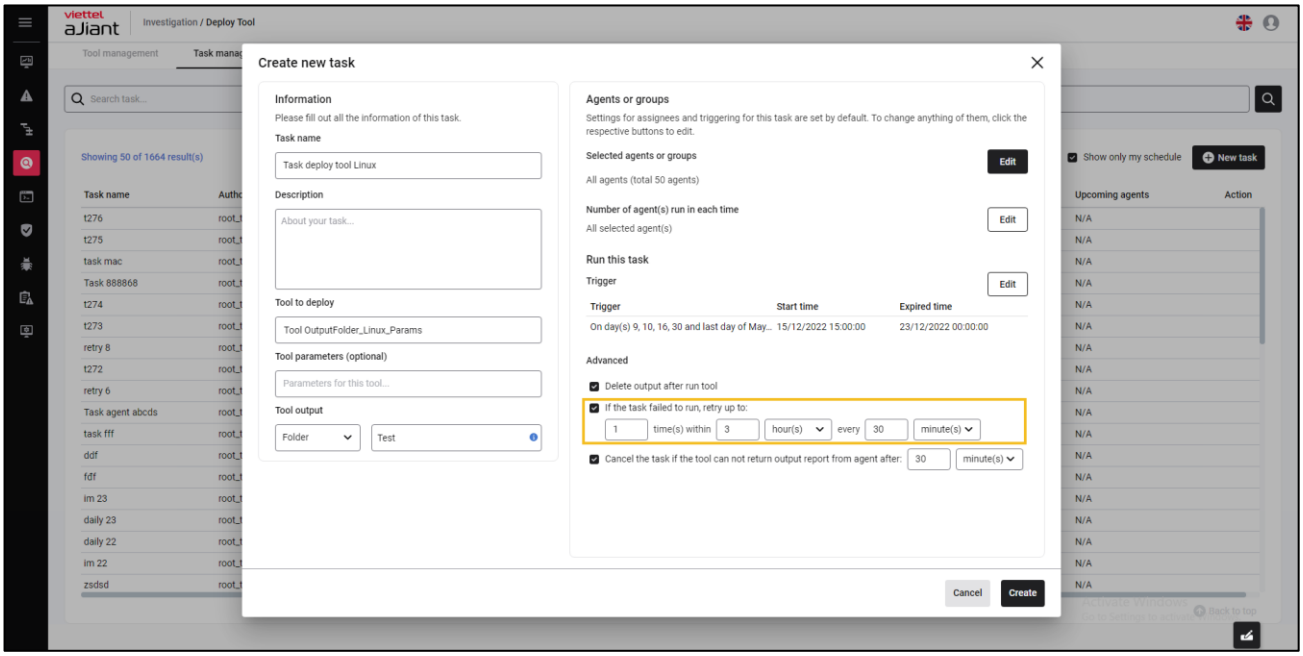
- Select Monthly schedule:
  - Allow scheduling of monthly tool deployments;
  - Repetition time;
  - Start and end time configuration:



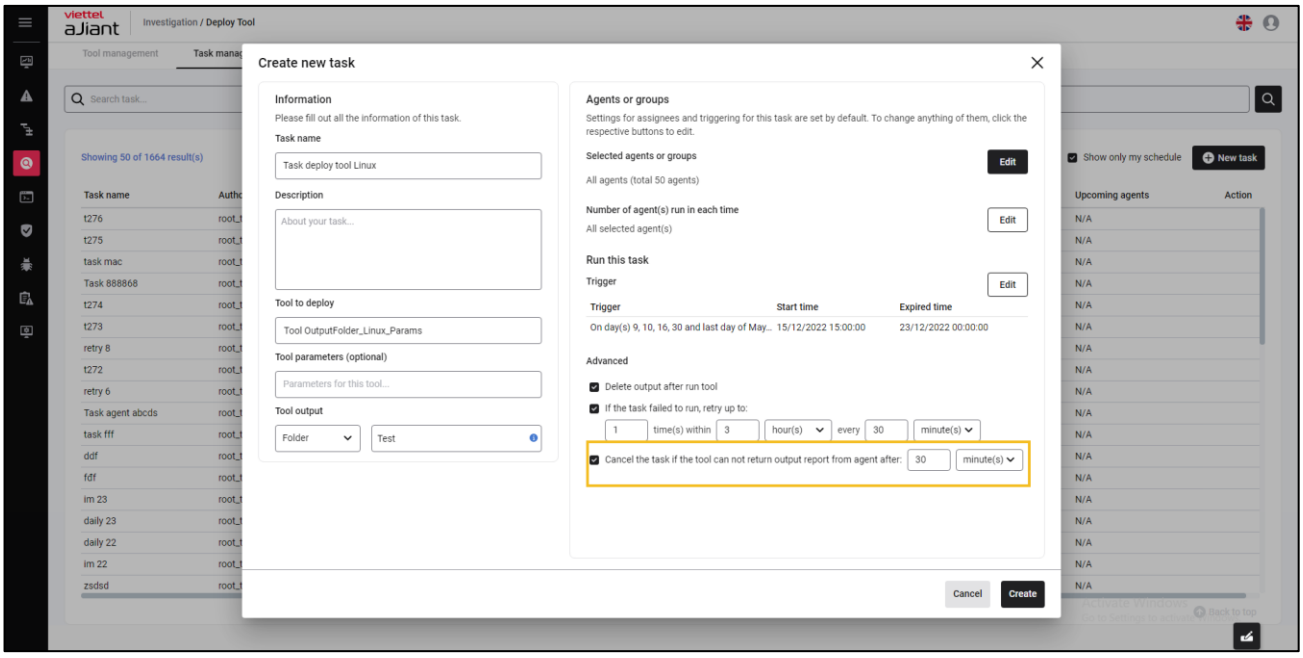
- Advanced information configuration for the task

Delete tool after run tool allows the tool output to be deleted after running the tool and successfully returning the result to the backend.

If the task fails to run, retry up to a specified limit when the task deployment fails, allowing configuration of the retry task information (redeploy the task).



Cancel the task if the tool cannot return an output report from the agent after allowing task cancellation when the task cannot run within the user-configured time.



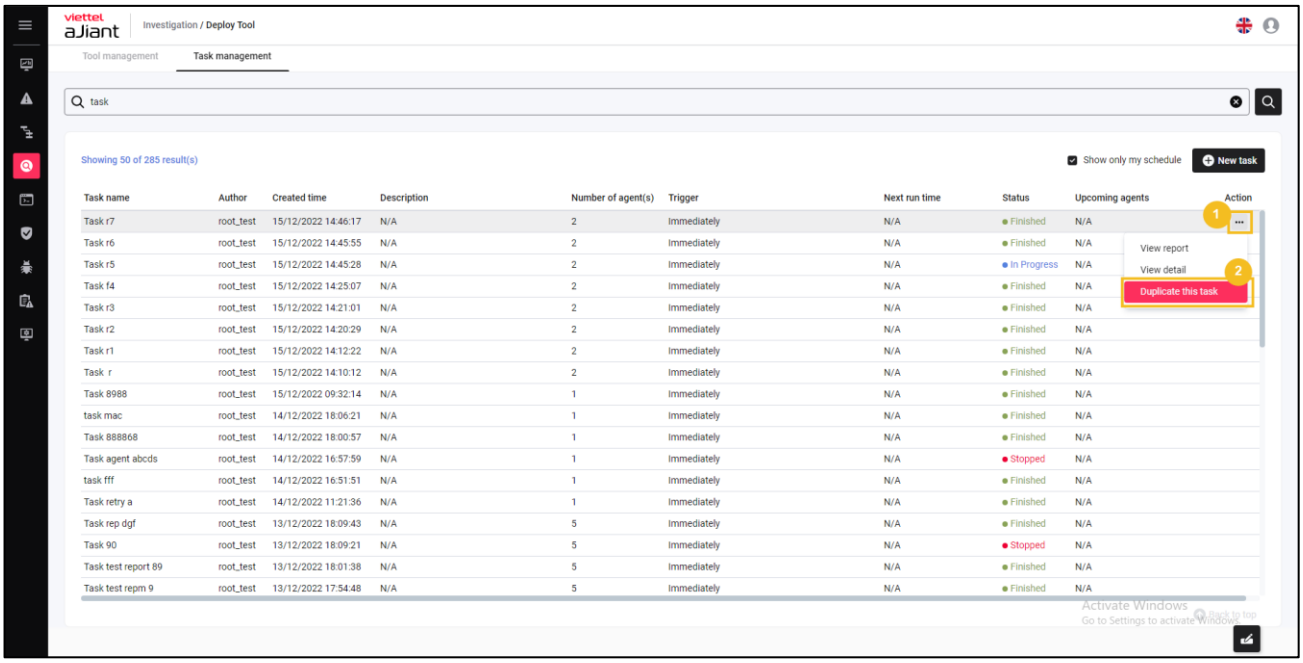
Select Create to create a new task/configure deploy tool information under the agent, or select Cancel to cancel the task/configuration of deploy tool information under the agent.

d. Duplicate task

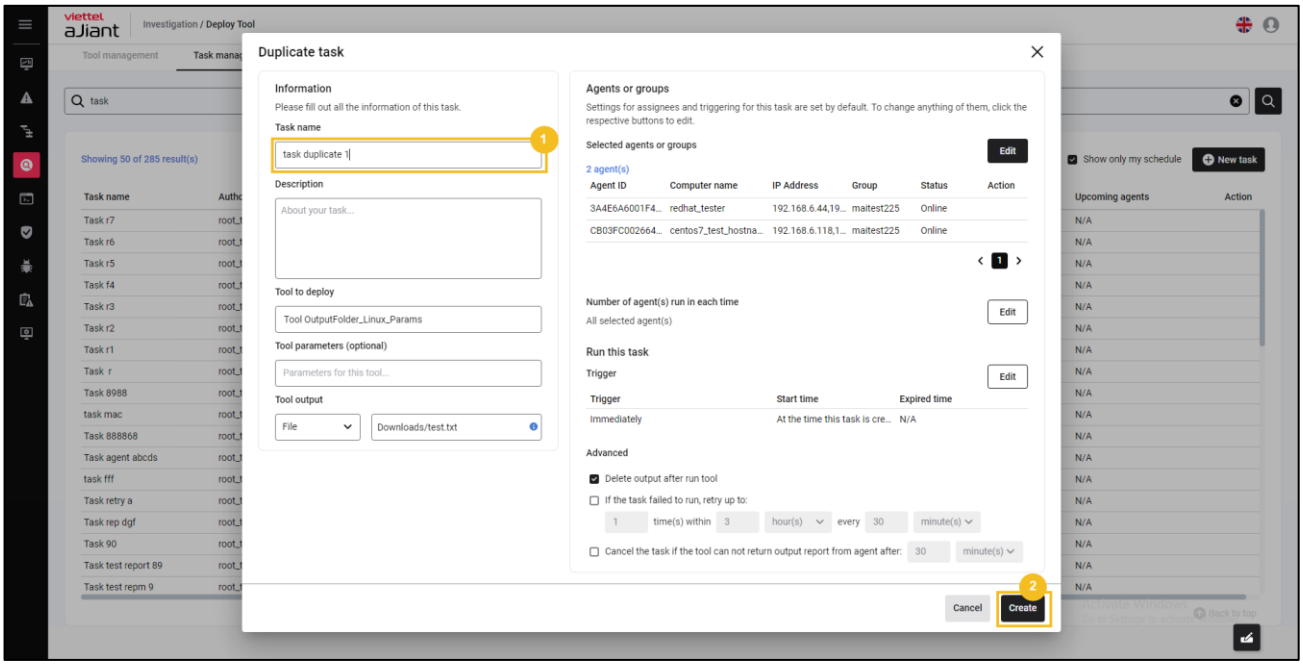
Purpose: To allow task duplication (copying tasks), automatically filling in values from the original task except for the Task Name field (requiring the user to enter/edit the task name).

Steps to follow:

- On the tool list screen, hover over the tool you want to duplicate > select > choose duplicate this task.



- Enter the Task name information and review/update the task details > Select Create to complete the configuration or select Cancel to cancel the task duplication operation.

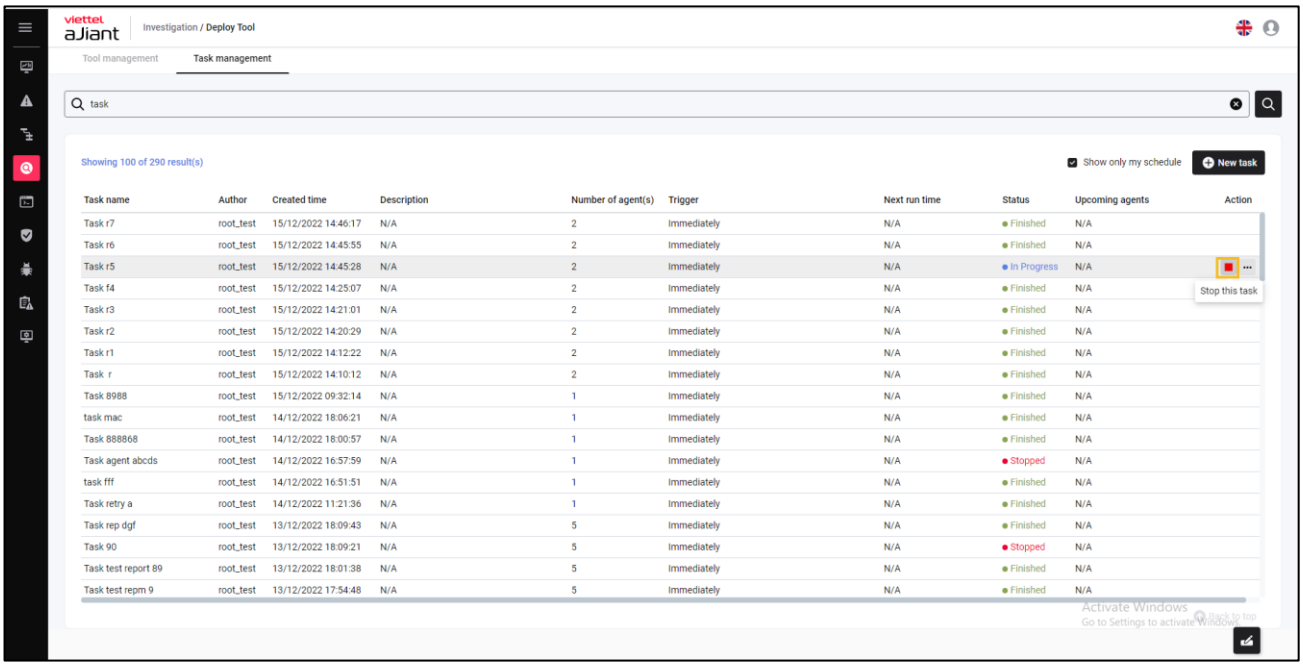


e. List of Upcoming Agents

Purpose: To allow the display of the list of Agents scheduled for tool deployment;
Steps to follow: On the task list screen > Select the Upcoming Agents List.

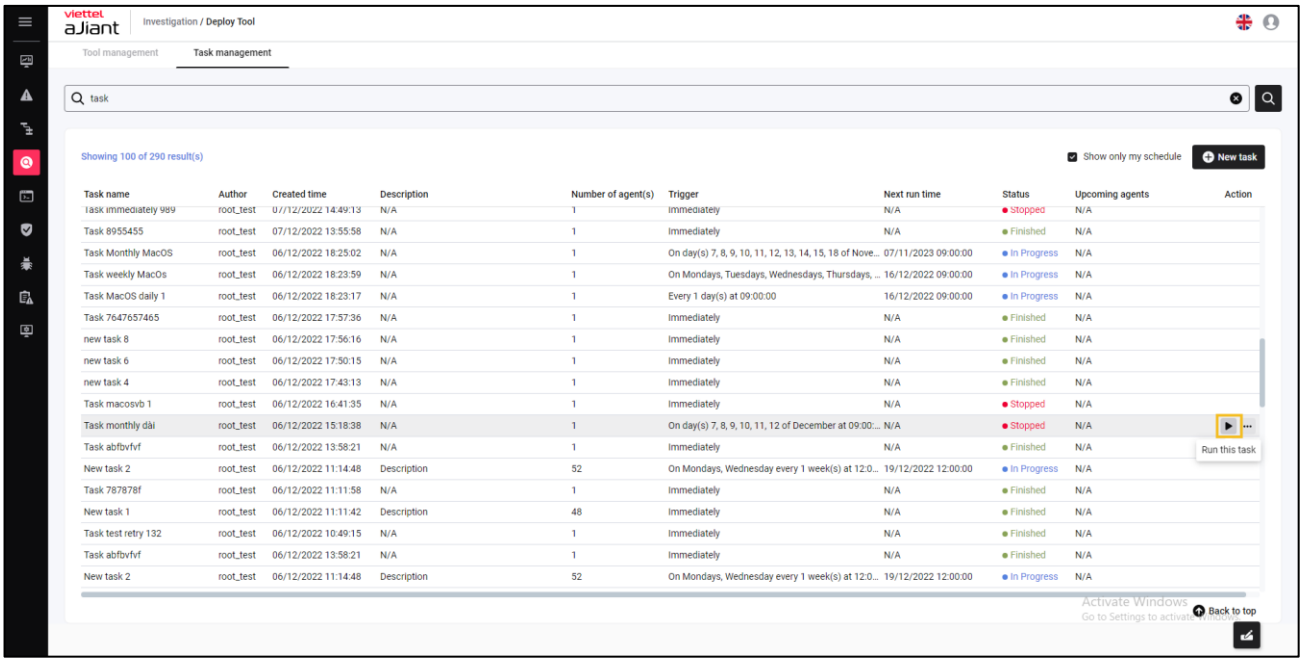
f. Stop/Start task

Purpose: To allow stopping or restarting a task (stop deploying a task or redeploy a previously paused task).
Steps to pause a task: On the task list screen, hover over the task you want to pause > Select the icon to pause the task:



Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
Task r7	root_test	15/12/2022 14:46:17	N/A	2	Immediately	N/A	Finished	N/A	
Task r6	root_test	15/12/2022 14:45:55	N/A	2	Immediately	N/A	Finished	N/A	
Task r5	root_test	15/12/2022 14:45:28	N/A	2	Immediately	N/A	In Progress	N/A	
Task f4	root_test	15/12/2022 14:25:07	N/A	2	Immediately	N/A	Finished	N/A	
Task r3	root_test	15/12/2022 14:21:01	N/A	2	Immediately	N/A	Finished	N/A	
Task r2	root_test	15/12/2022 14:20:29	N/A	2	Immediately	N/A	Finished	N/A	
Task r1	root_test	15/12/2022 14:12:22	N/A	2	Immediately	N/A	Finished	N/A	
Task r	root_test	15/12/2022 14:10:12	N/A	2	Immediately	N/A	Finished	N/A	
Task 8988	root_test	15/12/2022 09:32:14	N/A	1	Immediately	N/A	Finished	N/A	
task mac	root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	Finished	N/A	
Task 888868	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	Finished	N/A	
Task agent abcds	root_test	14/12/2022 16:57:59	N/A	1	Immediately	N/A	Stopped	N/A	
task fff	root_test	14/12/2022 16:51:51	N/A	1	Immediately	N/A	Finished	N/A	
Task retry a	root_test	14/12/2022 11:21:36	N/A	1	Immediately	N/A	Finished	N/A	
Task rep dgf	root_test	13/12/2022 18:09:43	N/A	5	Immediately	N/A	Finished	N/A	
Task 90	root_test	13/12/2022 18:09:21	N/A	5	Immediately	N/A	Stopped	N/A	
Task test report 89	root_test	13/12/2022 18:01:38	N/A	5	Immediately	N/A	Finished	N/A	
Task test repm 9	root_test	13/12/2022 17:54:48	N/A	5	Immediately	N/A	Finished	N/A	

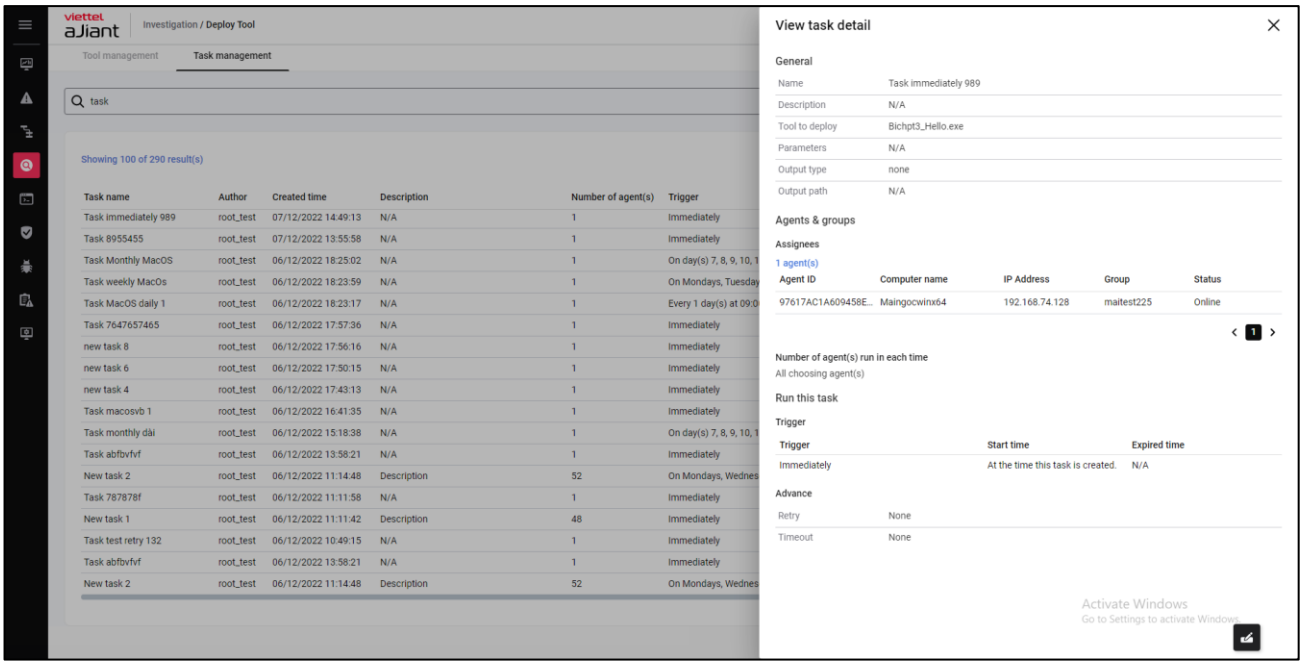
Steps to redeploy a task (that has been stopped): On the task list screen, hover over the task you want to redeploy > Select the icon to redeploy the task:



g. Task details

Purpose: To allow viewing detailed task information;

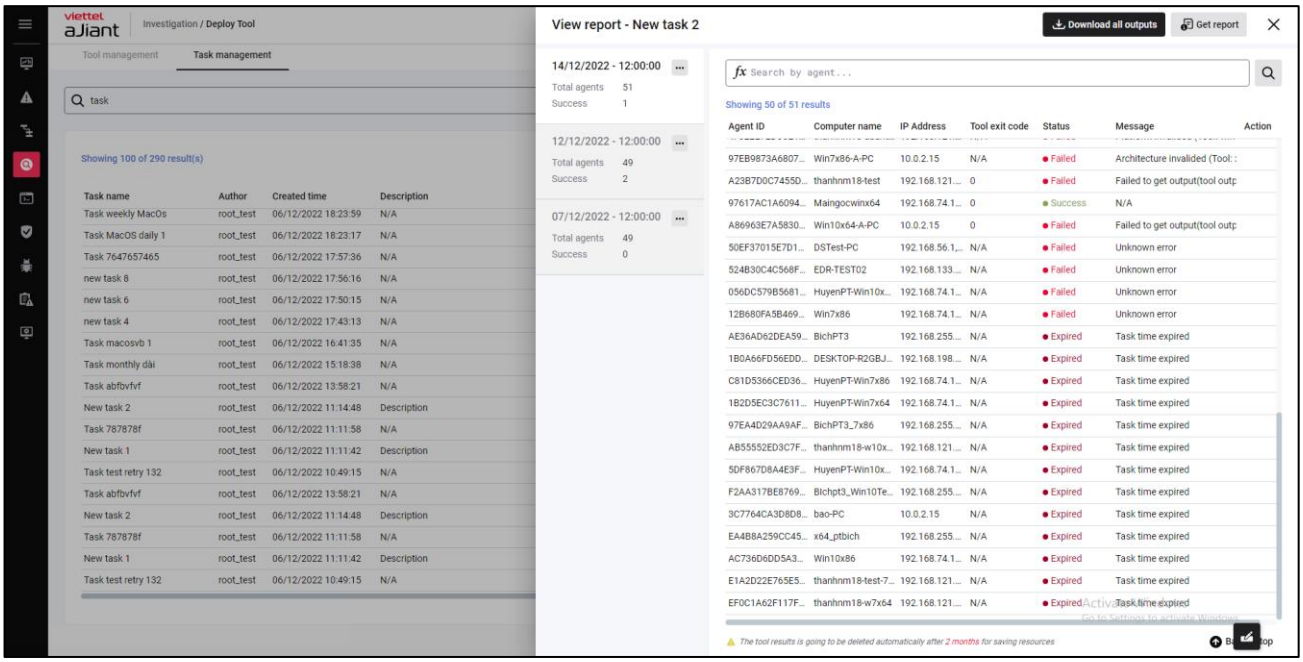
Steps to follow: On the task list screen, hover over the task you want to view details for > Select View detail:



h. View report (View tool result)

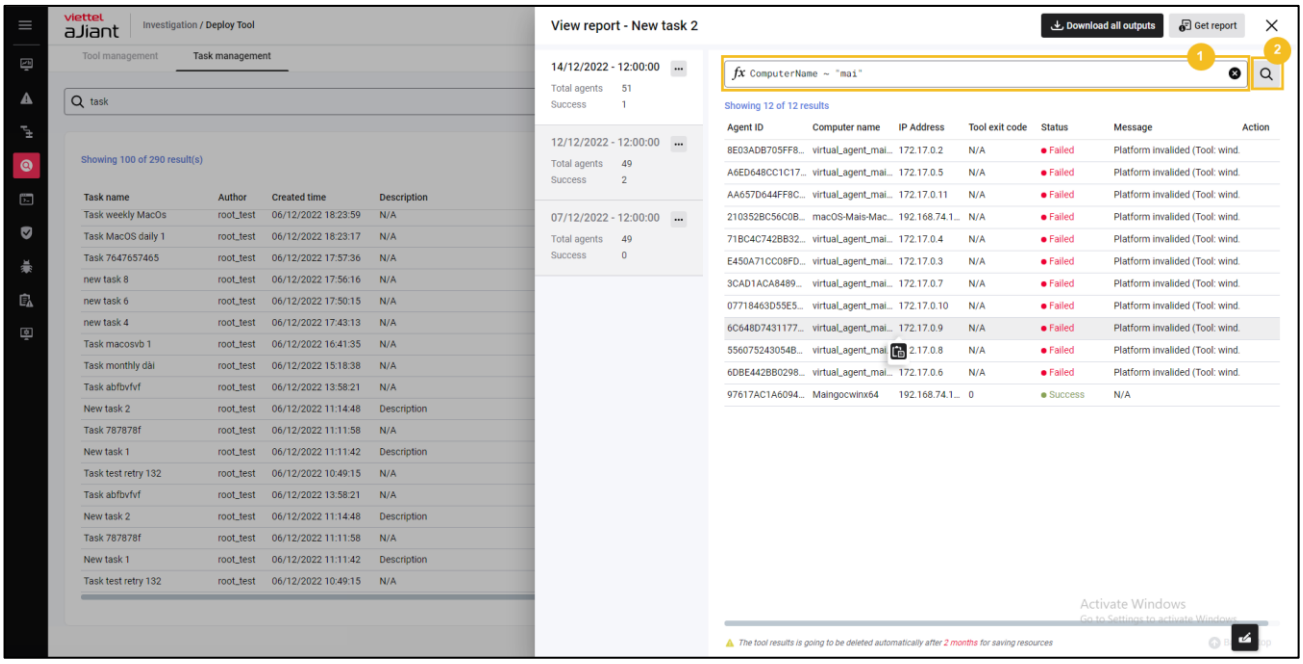
Purpose: To review the deployment tool report results;

Steps to follow: On the task list screen, hover over the task you want to view details for > Select View report:



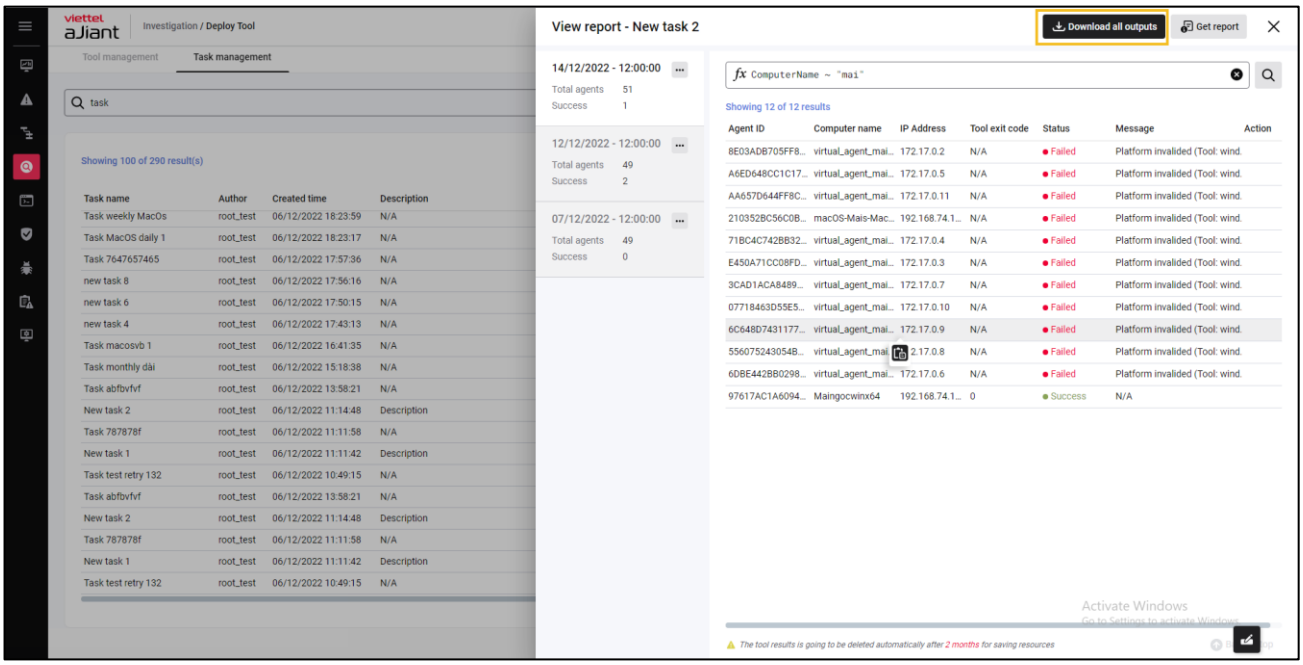
Search for deploy tool results using the following query commands:

- Purpose: To enable searching for deploy tool results based on query commands;
- Steps to follow: Enter the search query > select the Search button or finish entering the keyword > press enter. The system will perform a search for information related to the search keyword within the system.



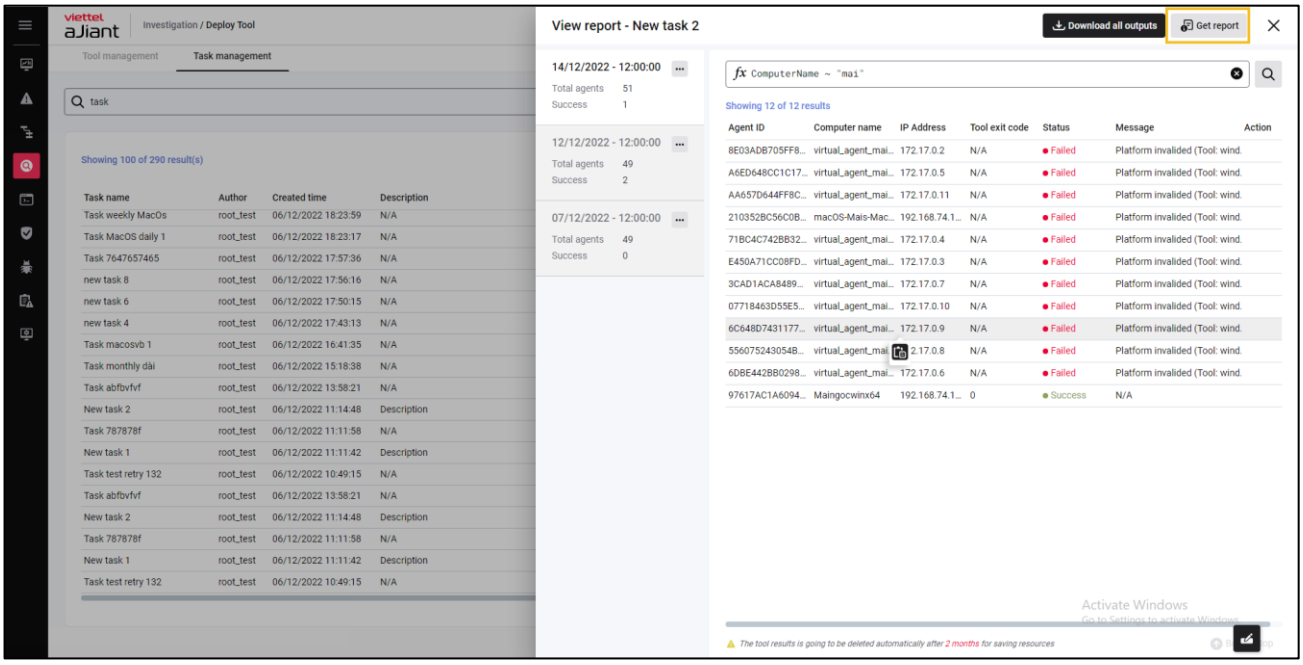
Download the entire deploy tool results (according to the scheduled task):

- Purpose: To allow downloading the entire deploy tool results (according to the scheduled task);
- Steps to follow: On the View report screen, select the Download all output button.



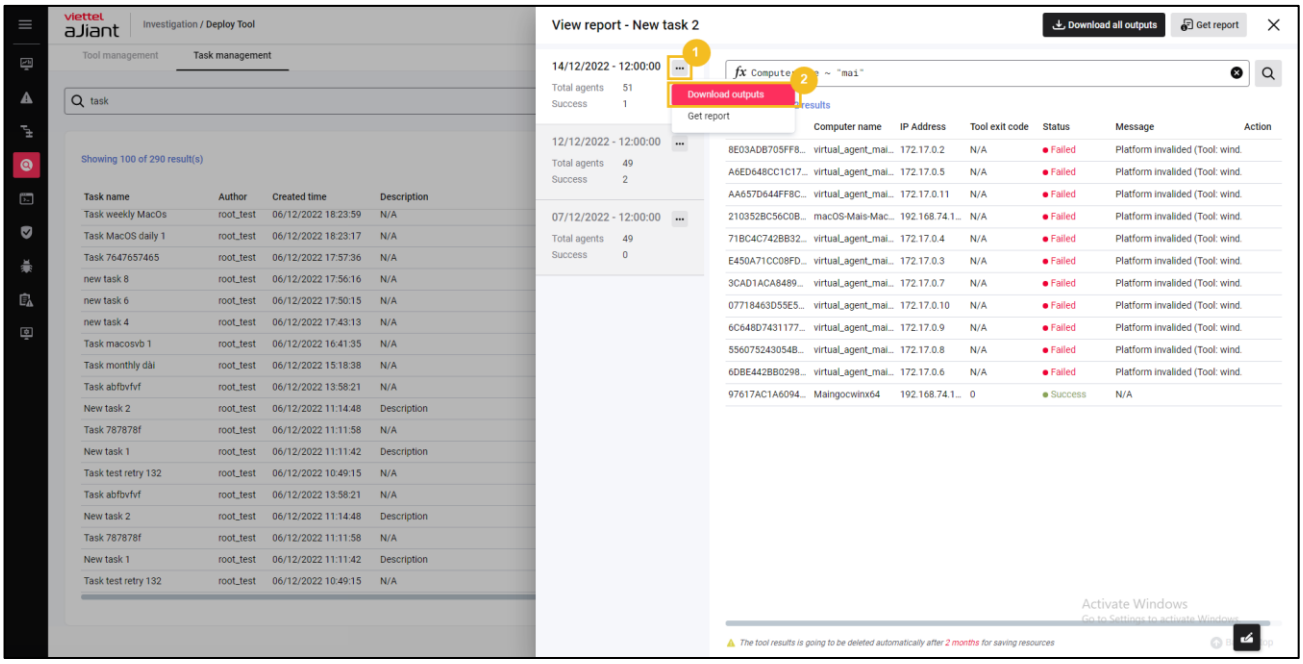
Get all reports:

- Purpose: To allow downloading the entire list of deployment tool result reports.
- Steps to perform: On the View report screen, select the Get report button:



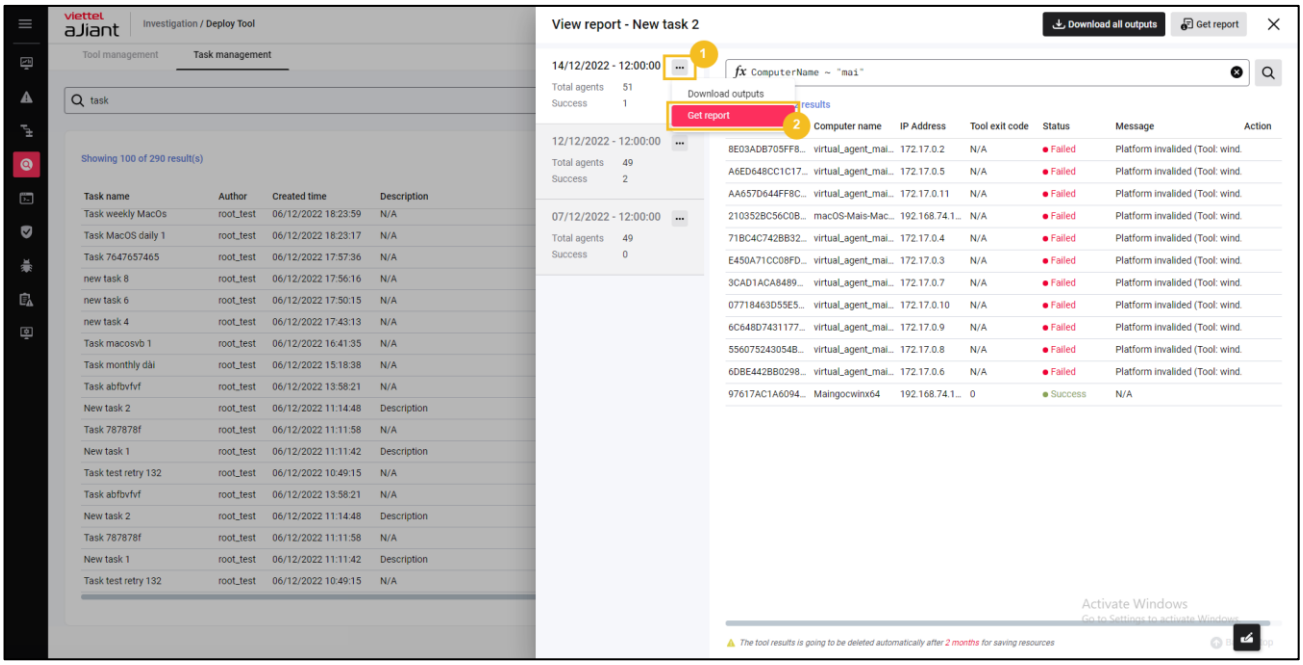
Download the output of each scheduling iteration:

- Purpose: To allow downloading the complete list of deployment tool result reports for each scheduled run;
- Steps to follow: On the View report screen, select the scheduled record icon for which the user wants to download outputs > Select Download outputs.



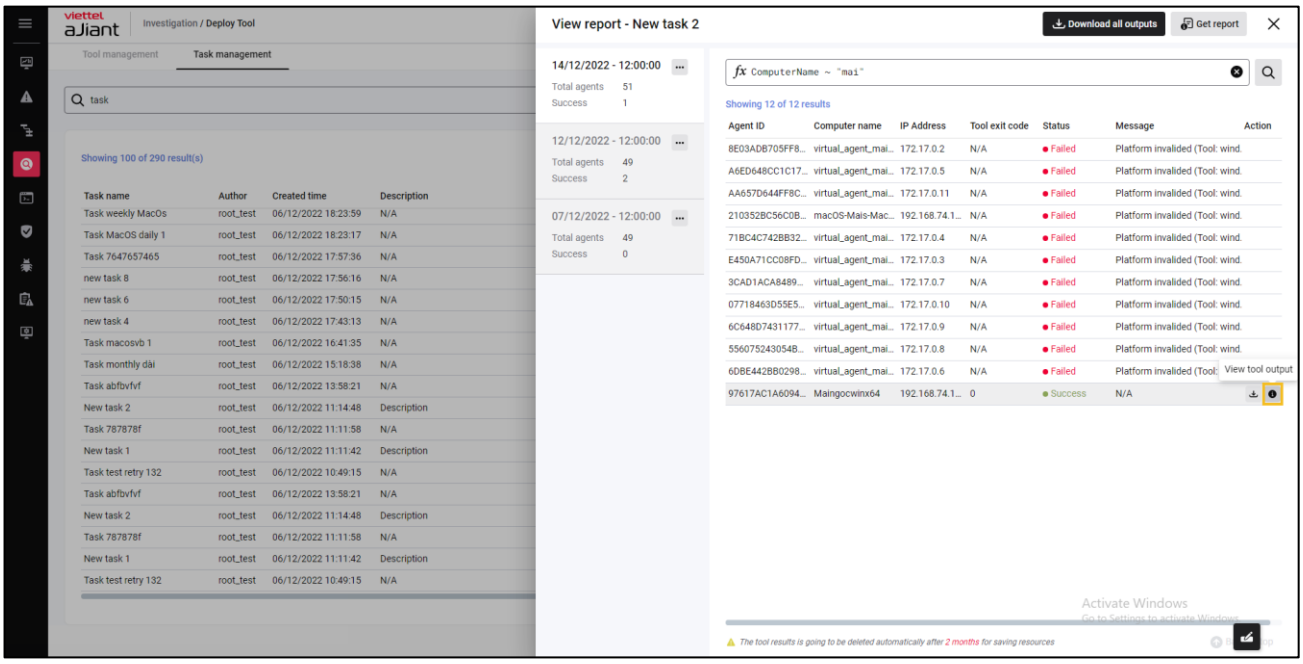
Download the report for each scheduling instance:

- Purpose: To allow downloading the complete list of deployment tool report statistics for each scheduled run (in .csv format).
- Steps to follow: On the View report screen, select the schedule record icon for the report you want to download > Select Get report.



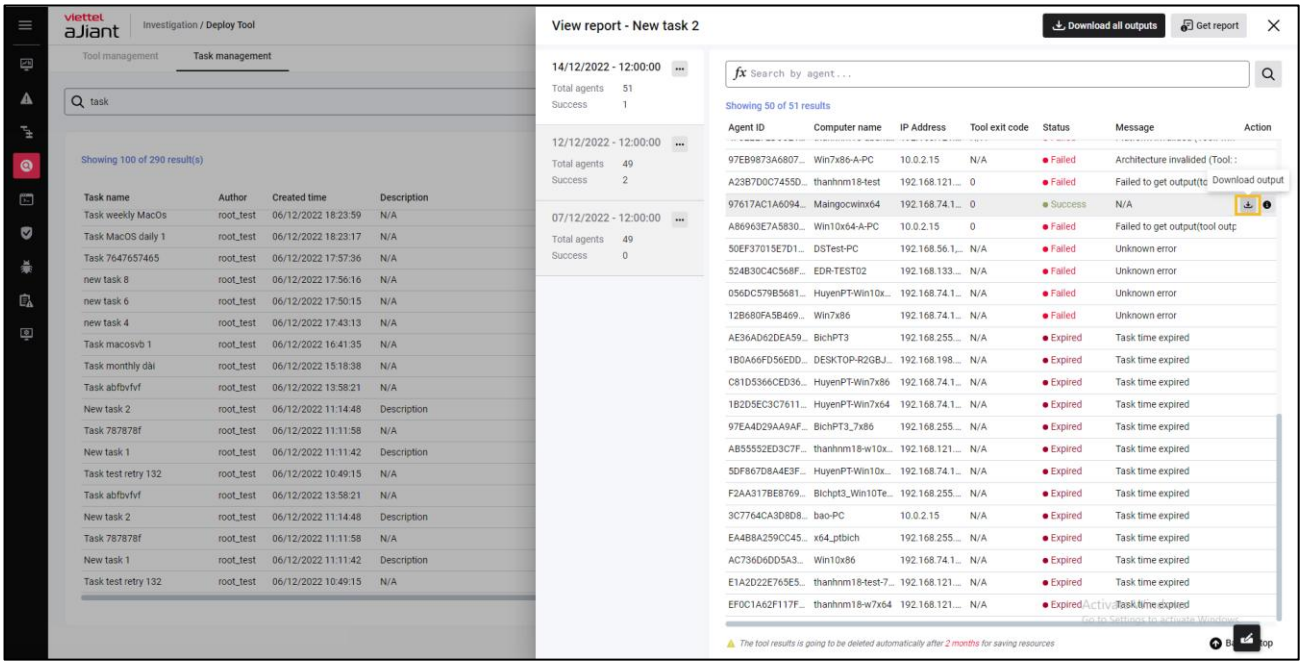
View the tool outputs of each agent:

- Purpose: To allow users to view the tool outputs of each agent.
- Steps to follow: On the View report screen, hover over the record you want to view the report for (with a Success status) > select the icon > choose View tool output.



Download the deployment result report for each agent tool:

- Purpose: To allow downloading the deployment result report for each agent;
- Steps to follow: On the view report screen, hover over the agent record you want to view the report for (with Success status) > select the icon > Choose Download output.



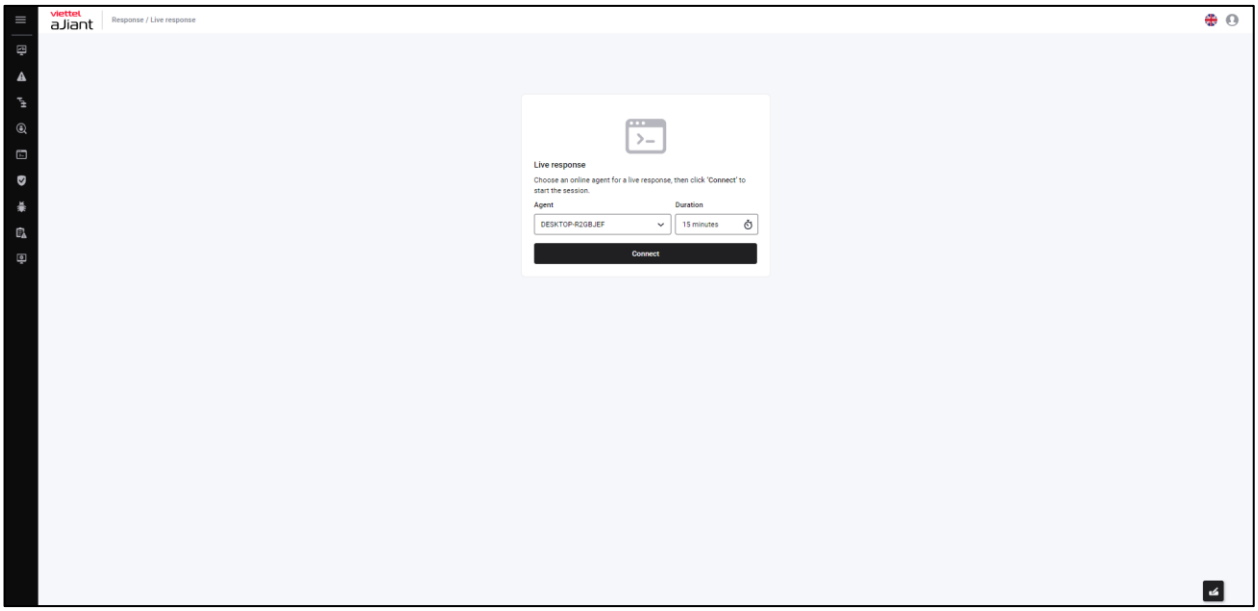
3.5 Response Screen

3.5.1 Live Response

Purpose: The Live Response function provides the capability to execute a set of remote commands within a session to retrieve information or handle requests on the host.

Steps to perform the Live Response function:

- Click the “Response” tab and select “Live Response.”



- Create a new live response session.

Select Agent: Display the list of agents:

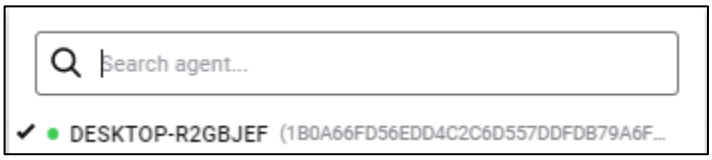
User logged in as root group: Display all Agents in the system active for less than 30 days;

User logged in belongs to the default group: Display all Agents belonging to the default group;

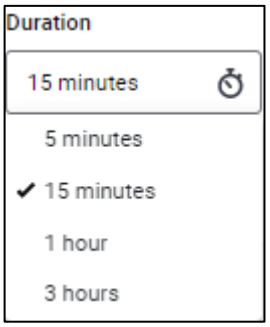
User login belongs to parent group: Display all Agents belonging to the user's current group and the corresponding child groups;

User logged in belongs to one or multiple subgroups: Display all Agents belonging to the user's groups currently logged in;

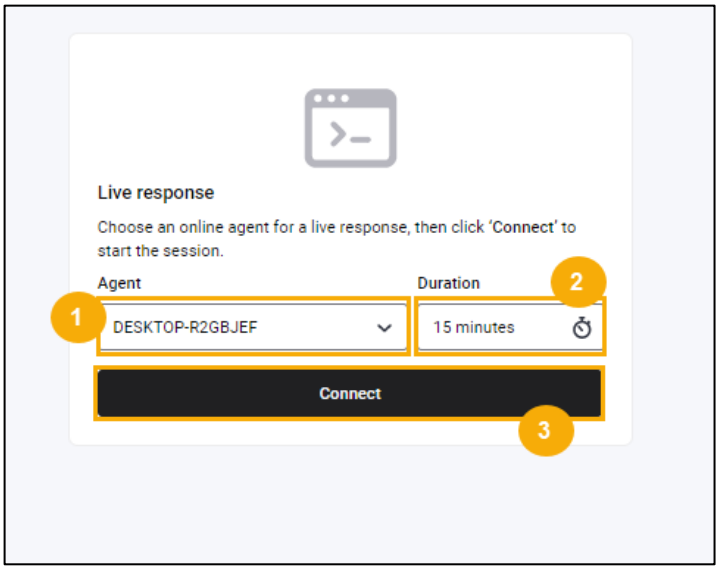
Users can only perform Live Response with agents who are currently online:



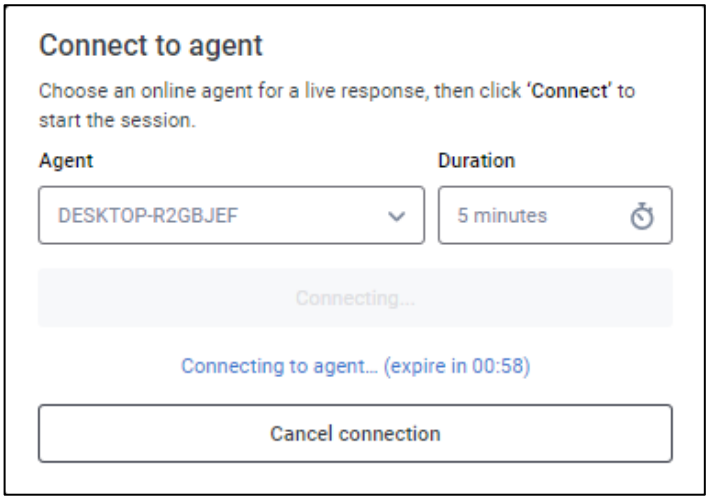
Select Duration: options include 5 minutes, 15 minutes, 1 hour, 3 hours;



Click the “Connect” button:

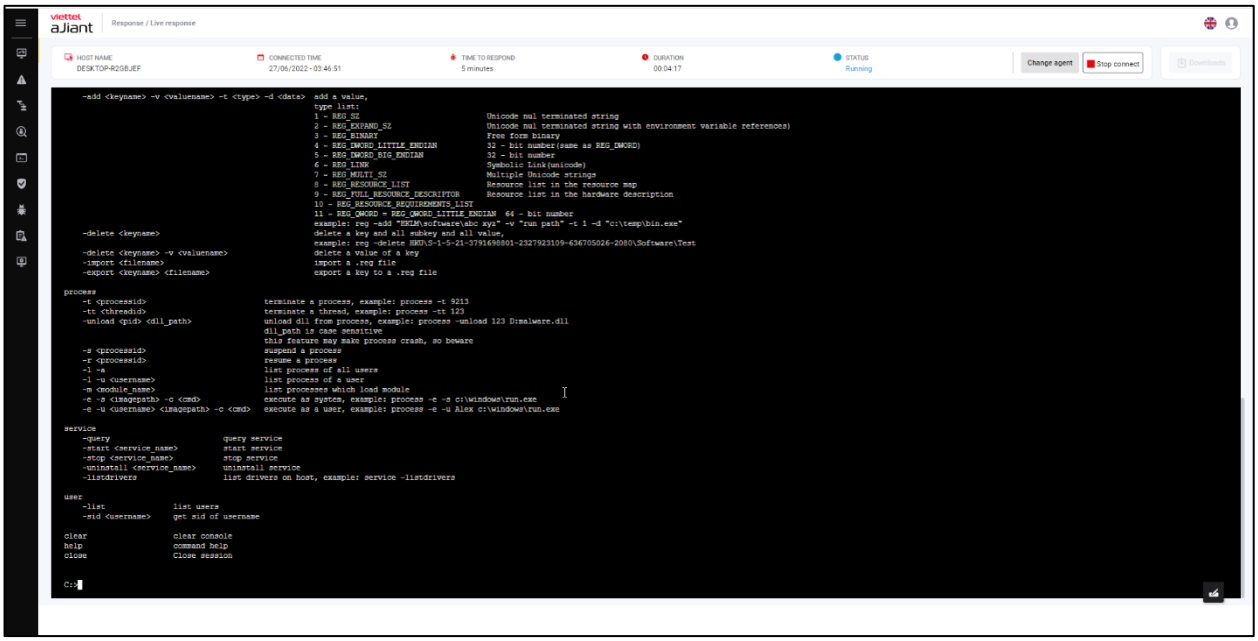


Bước 5: Wait 1 minute for the system to connect to the agent; the system status is "connecting":

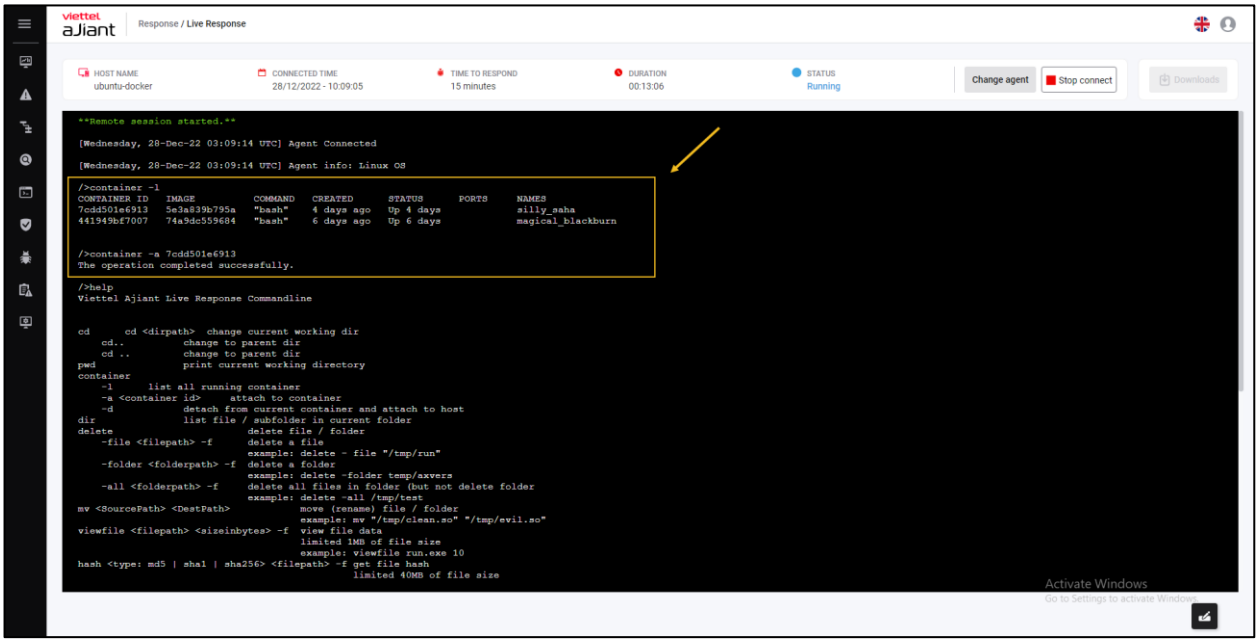


- Upon successful connection, the user is allowed to execute commands on the console screen, and the Live Response session status is "running."

Note: Each agent can only have one active Live Response session at a time.



Note: Users can connect to the container by executing commands through the container's console screen.



Users can execute commands on the console screen as follows:

Window: execute the following commands:

No.	Commands	Parameter	Description
1	cd	cd <dirpath>	Change the current working directory
		cd.. or cd ..	Move to the parent directory
2	pwd		Print the current working directory
3	directory	dir [drive:][path][filename] [/A[[:]attributes]] [/O[[:]sortorder]] [/T[[:]timefield]] [/L] [/Q] [/R] [/S] [/X]	List the files/subdirectories in the current directory.
		/ A: [-] attributes Displays files with specified attributes. Attributes: D Directories R Read-only files H Hidden files A Files ready for archiving S System files L Reparse Points	

No.	Commands	Parameter	Description
		/ L Lower-case filename	
		/ O:[-]sortorder List files in sorted order. sortorder N By name (alphabetical) S By size (smallest first) E By extension (alphabetical) D By date/time (oldest first) G Group directories first - Prefix to reverse order Example: dir /O:N;	

No.	Commands	Parameter	Description
		/ T:timefield Choose which time field to display timefield C Creation M MFT Creation A Last Access W Last Written Example: dir /T:A - Prefix to exclude attribute Example: dir /A:D-AH	
		/ Q Display the owner of the file. Example: dir /Q	

No.	Commands	Parameter	Description
		/ R Display alternate data streams of the file. Example: dir /R	
		/S Displays files in the specified directory and all subdirectories. Example: dir /S	
		/ X This displays the short names generated for non-8dot3 file names. Example: dir /X	
4	delete	delete –file <path> example: delete -file "c:\temp\run path.exe"	Delete a file
		delete -folder <folderpath> example: delete -folder temp\axvers	Delete a folder

No.	Commands	Parameter	Description
		delete –all <folderpath> example: delete –all c:\temp	Delete all files/subfolders within the folder (but do not delete the folder itself)
5	mv	<SourcePath> <DestPath> move (rename) file / folder Example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"	Allow moving files/folders
6	view file	<filepath><sizeinbytes>	Display data in the file (file size limit)
7	Hash	hash <type: md5 | sha1 | sha256> <filepath> -f get file hash example: hash md5 c:\test\run.exe	Allows encryption of files up to 1MB Option -f to force open the file when it is being used by another process
8	dump		Allow process dump. If you omit the dump file path, it will default to <processname>_<datetime>.dmp.

No.	Commands	Parameter	Description
		-process -pid <ProcessID> [-f <DestPath>] dump process by process ID Example: dump -process -pid 452 -f "C:\Users\Evil_dumped.dmp"	Dump process by Process ID
		-process -name <ProcessName> [-f <DestPath>] dump process by process name Example: dump -process -name Evil.exe -f "C:\Users\Evil_dumped.dmp"	Dump process by Process name
		-process -path <ProcessPath> [-f <DestPath>] dump process by process path Example: dump -process -path "C:\Users\Evil.exe" -f "C:\Users\Evil_dumped.dmp"	Dump process by Process Path

No.	Commands	Parameter	Description
9	lấy	<filepath>	Upload 1 file from host to server
10	put	<url><folderpath>	Download 1 file to the host machine
11	mkdir	<dir name>	Create a folder.
12	reg		Commands related to the Registry
		query <keyname> -v <valuename> Example: reg-query "HKLM\Software\abc xyz" -v "run path"	Query the value data of a key
		query <keyname> -s example: reg-query "HKLM\Software\abc xyz" -s	Query all subkeys, values, and data.
		add <keyname> example:	Add one more key

No.	Commands	Parameter	Description
		reg-add "HKLM\software\abc xyz"	
		add <keyname> -v <valuename> -t <type> -d <data> example: reg-add "HKLM\software\abc xyz" -v "run path" -t REG_SZ -d "c:\temp\bin.exe"	Add 1 value
		delete <keyname> example: reg delete HKU\S-1-5-21-3791698801-2327923109-636705026-2080\Software\Test	Delete one key along with all its subkeys and values.
		delete <keyname> -v <valuename>	Delete a value of a key

No.	Commands	Parameter	Description
		import <filename>	Import one .reg file
		export <keyname> <filename>	Export 1 .reg file
13	process		Commands related to processes
		-t <processid>	Terminate a running process by process ID.
		-s <processid>	Pause a process
		-r <processid>	Resume a previously paused process.
		-l -a	List all processes of all users.
		-l -u <username>	List the processes of a user.
14	service		Commands related to services
		-query	List the services currently running on the host machine.
		-start <servicename>	Start one service
		-stop <servicename>	Stop one service
		-uninstall <service_name> uninstall service	Uninstall the service

No.	Commands	Parameter	Description
		-listdrivers list drivers on the host, example: service -listdrivers	List the drivers on the host.
15	user	-list	List the users on the machine.
		-sid<username>	Get the SID of the username
16	grep	grep -t <text> <param> <command>	Support search by word or phrase with output results according to the input command.
17	cls		Clear the console screen
18	Help		Help command
19	Clear		Clear the console
20	Close		Close the session
21	container	- l	List the containers.
		-a <container id>	Connect to each container individually
		-d	Disconnect container

Ubuntu: Execute the following commands:

No.	Commands	Parameter	Description
1	cd	cd <dirpath>	Change the current working directory

No.	Commands	Parameter	Description
		cd.. or cd ..	Move to the parent directory
2	pwd		In the current working directory
3	directory	List files and subfolders in the current folder	List files/subdirectories in the current directory.
4	delete	delete –file <path> example: delete -file "c:\temp\run path.exe"	Delete a file
		delete -folder <folderpath> example: delete -folder temp\axvers	Delete a folder
		delete –all <folderpath> example: delete –all c:\temp	Delete all files/subfolders within the folder (but do not delete the folder itself)
5	mv	<SourcePath> <DestPath> move (rename) file / folder Example: mv	Allow moving files/folders

No.	Commands	Parameter	Description
		"c:\temp\clean.exe" "c:\temp\evil.exe"	
6	view file	<filepath><sizeinbytes>	Display data in the file (file size limit)
7	Hash	hash <type: md5 | sha1 | sha256> <filepath> -f get file hash example: hash md5 c:\test\run.exe	Allows encryption of files up to 1MB Option -f to force open the file when it is being used by another process
8	lấy	Please provide the Vietnamese text you would like me to translate.	Upload 1 file from host to server
9	đặt	<url><folderpath>	Download 1 file to the host machine
10	mkdir	<dir name>	Create a folder.
11	process		Commands related to processes
		-t <processid>	Terminate a running process by its process ID.
		-s <processid>	Pause a process

No.	Commands	Parameter	Description
		-r <processid>	Resume a previously paused process.
		-l -a	List all processes of all users.
		-l -u <username>	List the processes of a user.
		-e -s <imagepath> -c <cmd> execute a non-GUI process as system Example: process -e -s /tmp/run	
		-e-u<username> <imagepath> -c <cmd> execute a non-GUI process as a user Example: process -e -u Alex /tmp/run	
		-d <processid> -o <imagepath> generate a core file of a running program, for example: process -d 231 -o /tmp/core_file	
12	service		Commands related to service

No.	Commands	Parameter	Description
		-query	List the services currently running on the host machine.
		-start <servicename>	Start one service
		-stop <servicename>	Stop one service
		-uninstall <service_name> uninstall the service	Uninstall the service
		-listdrivers list drivers on the host, example: service -listdrivers	List the drivers on the host.
13	user	-list	List the users on the machine.
		-sid<username>	Get the SID of the username
14	Help		Help command
15	Clear		Clear the console
21	container	- l	List the containers.
		-a <container id>	Connect to each container individually
		-d	Disconnect container

MACOS:

No.	Commands	Parameter	Description
1	cd	cd <dirpath>	Change the current working directory
		cd.. or cd ..	Move to the parent directory
2	pwd		Print the current working directory
3	directory	List files and subfolders in the current folder	List files and subdirectories in the current directory.
4	delete	delete –file <path> Example: delete -file "c:\temp\run path.exe"	Delete a file
		delete -folder <folderpath> example: delete -folder temp\axvers	Delete a folder
		delete –all <folderpath> example: delete –all c:\temp	Delete all files/subfolders within the folder (but do not delete the folder itself)

No.	Commands	Parameter	Description
5	mv	<SourcePath> <DestPath> move (rename) file / folder Example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"	Allow moving files/folders
6	view file	<filepath><sizeinbytes>	Display data in the file (file size limit)
7	Hash	hash <type: md5 | sha1 | sha256> <filepath> -f get file hash example: hash md5 c:\test\run.exe	Allows encryption of files up to 1MB Option -f to force open the file when it is being used by another process
8	lấy	Please provide the Vietnamese text you would like translated.	Upload 1 file from host to server
9	đặt	<url><folderpath>	Download 1 file to the host machine
10	mkdir	<dir name>	Create a folder
11	process		Commands related to processes

No.	Commands	Parameter	Description
		-t <processid>	Terminate a running process by its process ID.
		-s <processid>	Pause a process
		-r <processid>	Resume a previously paused process.
		-l -a	List all processes of all users.
		-l -u <username>	List the processes of a user.
		-e -s <imagepath> -c <cmd> execute a non-GUI process as system Example: process -e -s /tmp/run	
		-e-u<username> <imagepath> -c <cmd> execute a non-GUI process as a user Example: process -e -u Alex /tmp/run	
12	service		Commands related to service
		-query	List the services currently running on the host machine.

No.	Commands	Parameter	Description
		-start <servicename>	Start one service
		-stop <servicename>	Stop one service
		-uninstall <service_name> uninstall the service	Uninstall the service
		-listdrivers list drivers on the host, example: service -listdrivers	List the drivers on the host.
13	user	-list	List the users on the machine.
		-sid<username>	Get the SID of the username
14	help		Help command
15	Clear		Clear the console

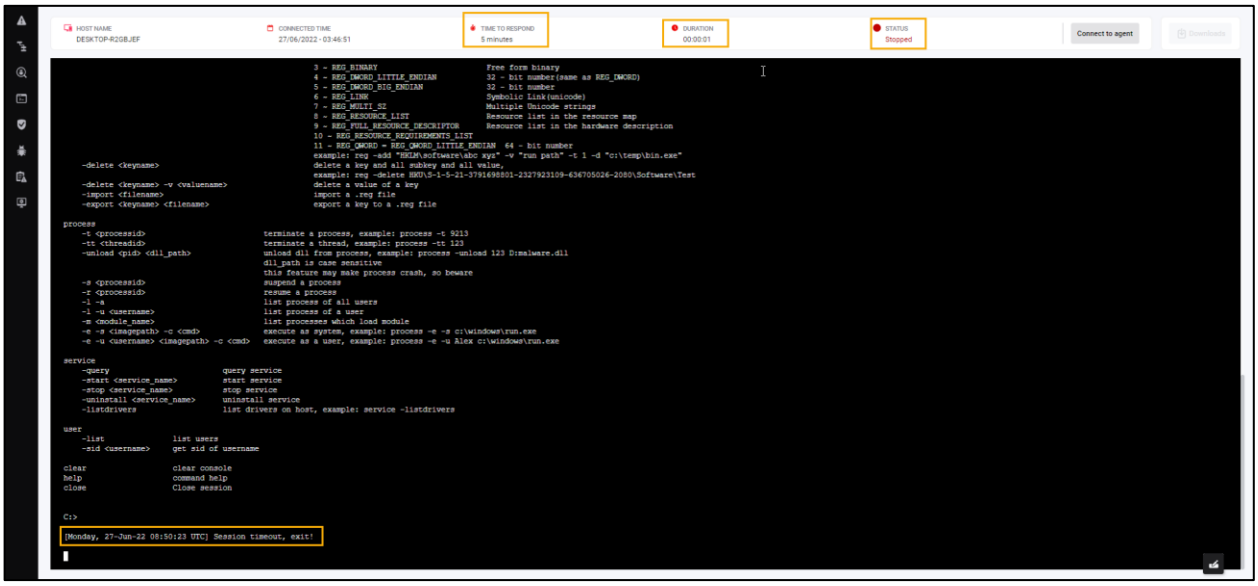
Some notes when working with commands on the console screen:

Clear Command: After executing the clear command, the system will allow the user to download the entire log previously displayed on the console screen by clicking on the “here” link;

The command get <filepath>: for example, get procexp.exe in the console screen will result in the file being retrieved and displayed in the Attachment Log at the bottom right corner of the screen. Users are allowed to download the file to their browser or delete the file retrieved from the server.

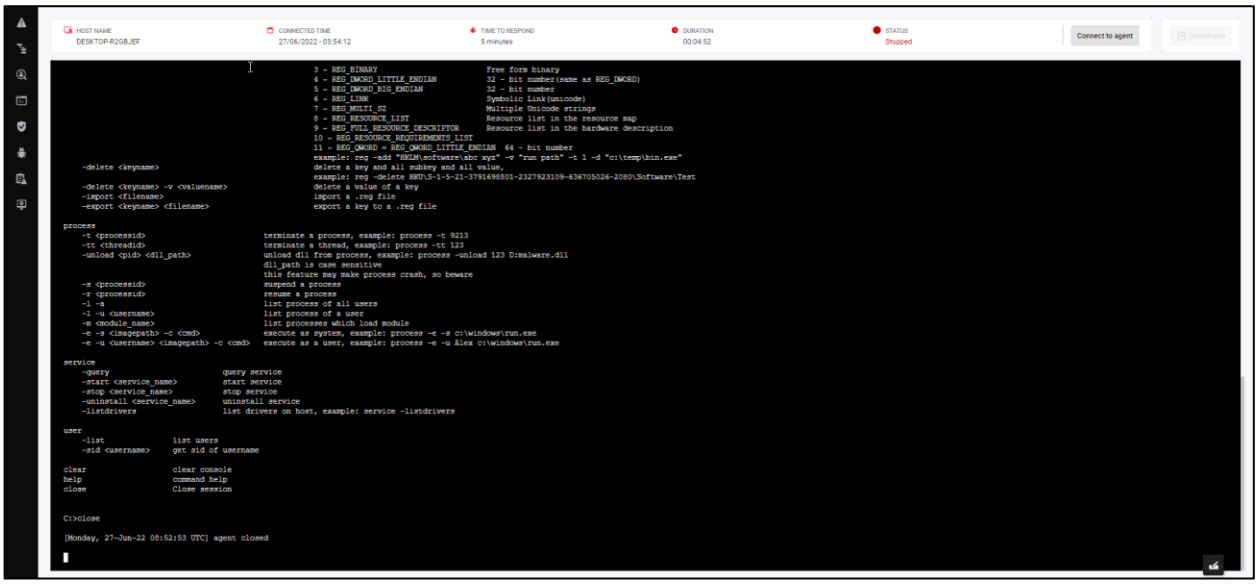
- The Live Response session ends when:

Session expiration time: When the "Duration" field equals the time in the "Time To Live" field;



The user actively requests to close the connection using the "close" command;

When the connection with the agent is lost, the server performs ping/pong failure checks more than 3 times.

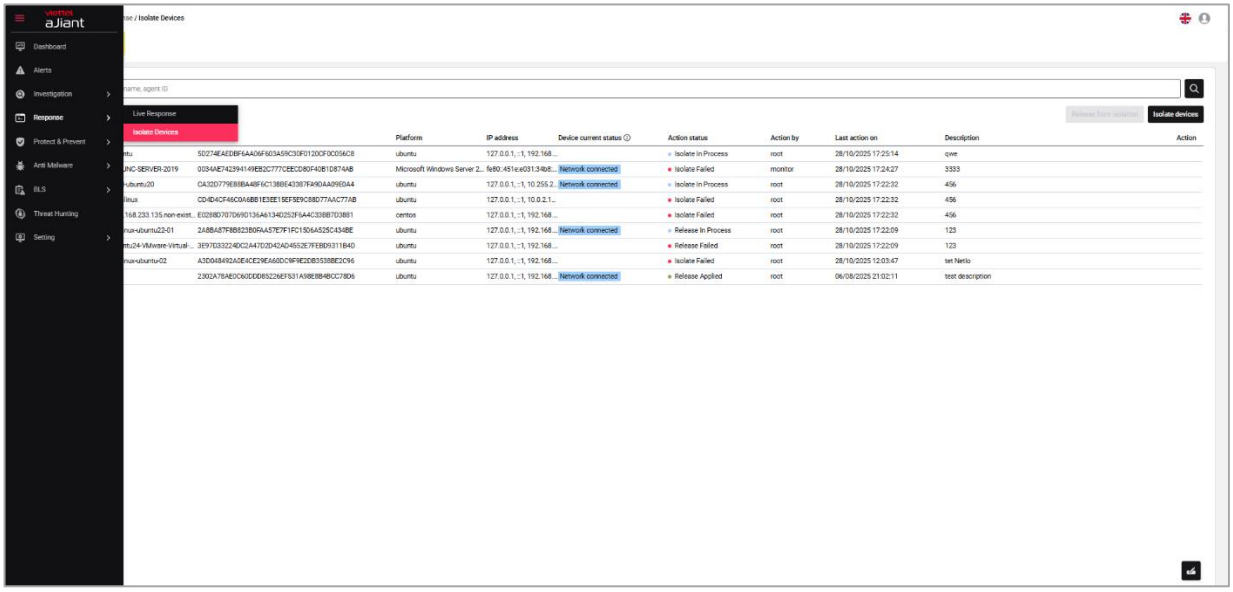


3.5.2 Isolate Devices

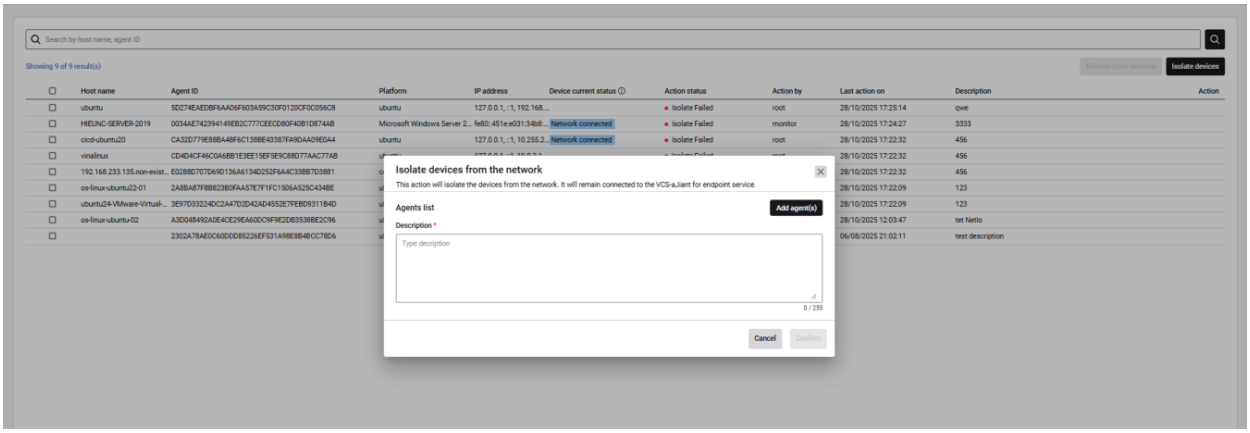
Purpose: To enable the SOC to isolate a device suspected of being compromised from the network. The primary objective is to prevent the spread of malware, limit dangerous communications, while maintaining the connection between the device and the VCS-aJiant system to continue investigation, evidence collection, and device recovery.

Create Isolate Devices command

Step 1: Go to the Response menu -> select the Isolate Devices menu.



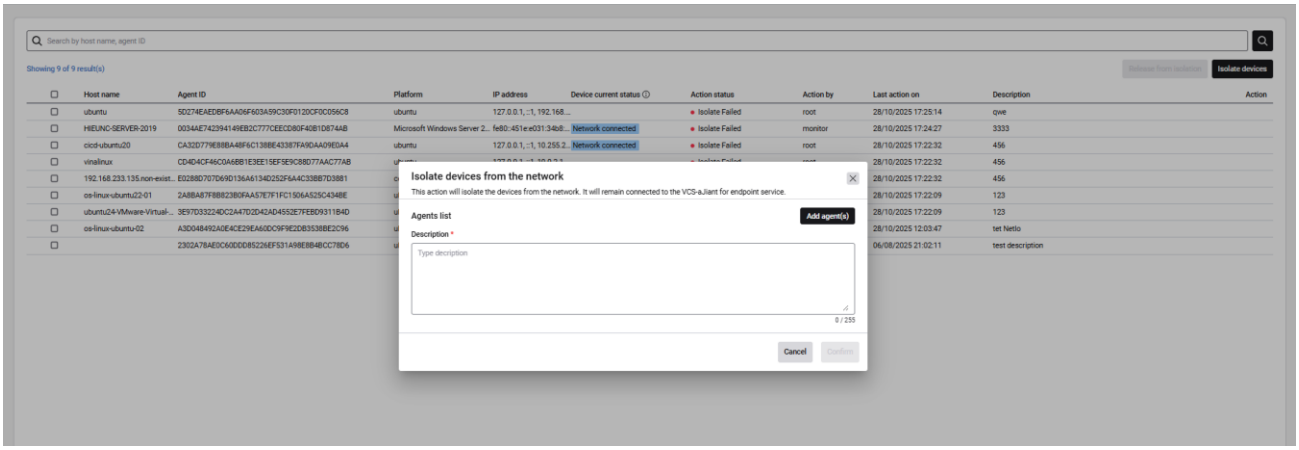
Step 2: Select the Isolate devices button.

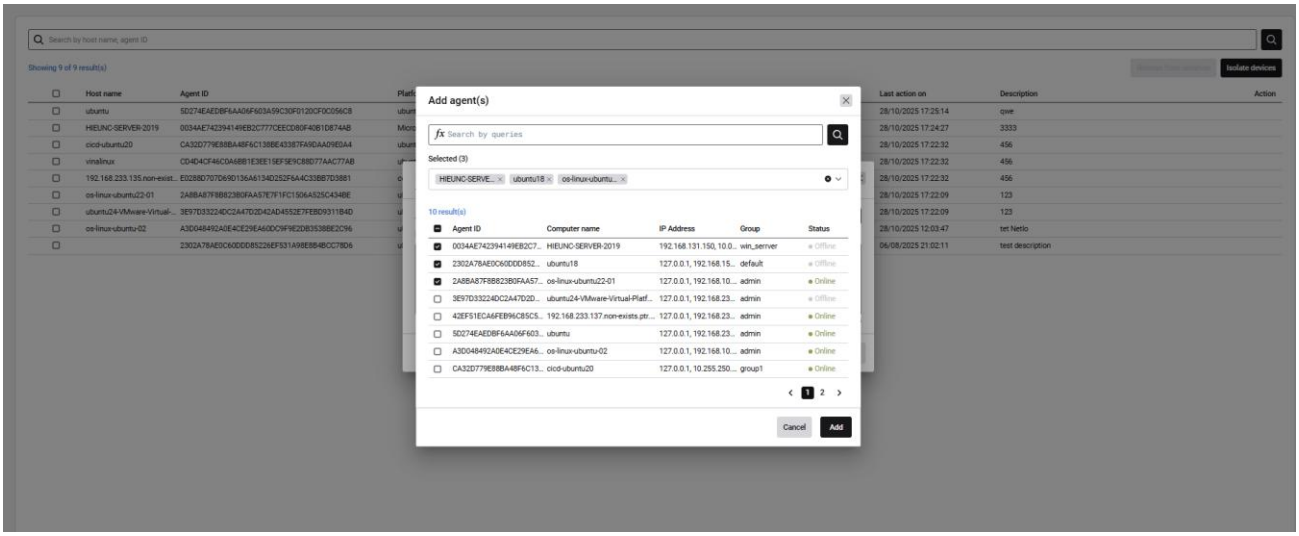


Step 3: Enter the required information, including

- Description (required)
- Select Agent(s)

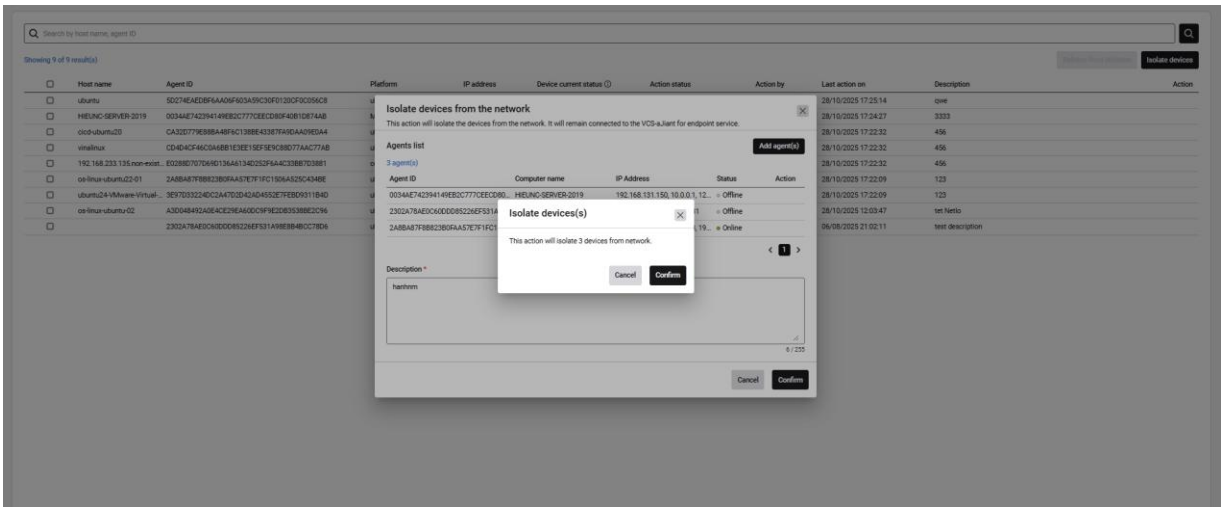
Note: Users are only allowed to operate with agents they have been authorized for.





Step 4: Confirm device isolation

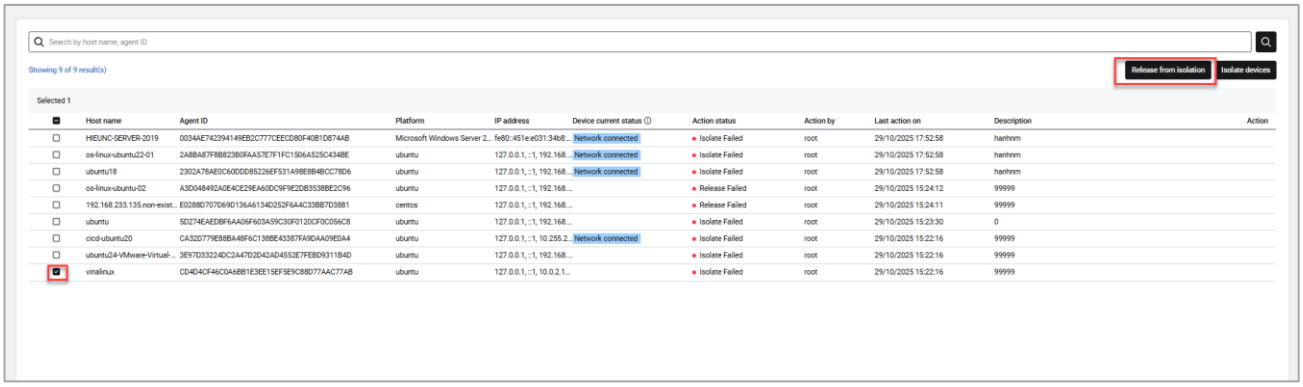
The user presses Confirm to confirm the device isolation.



Create a Release Isolation command (remove isolation)

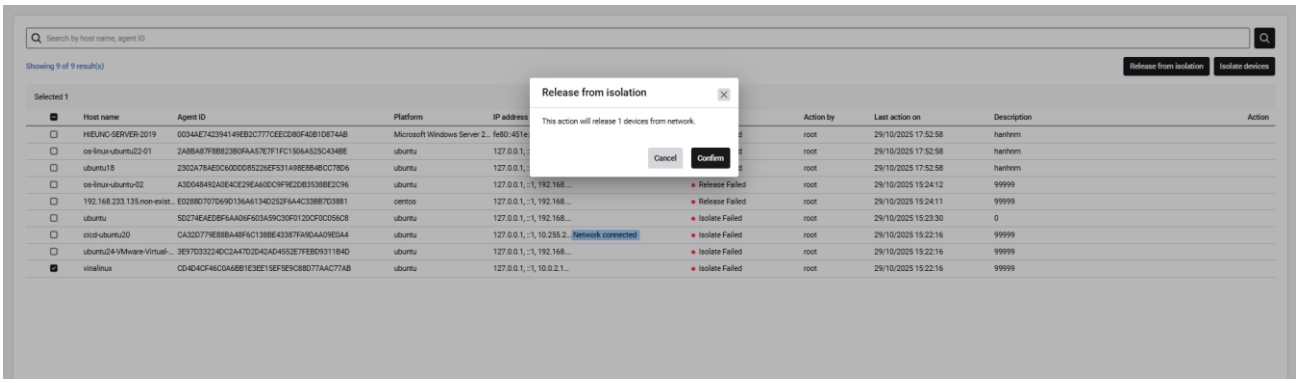
Users can remove device isolation as follows:

Step 1: From the list, the user selects one or more devices they want to remove from isolation.

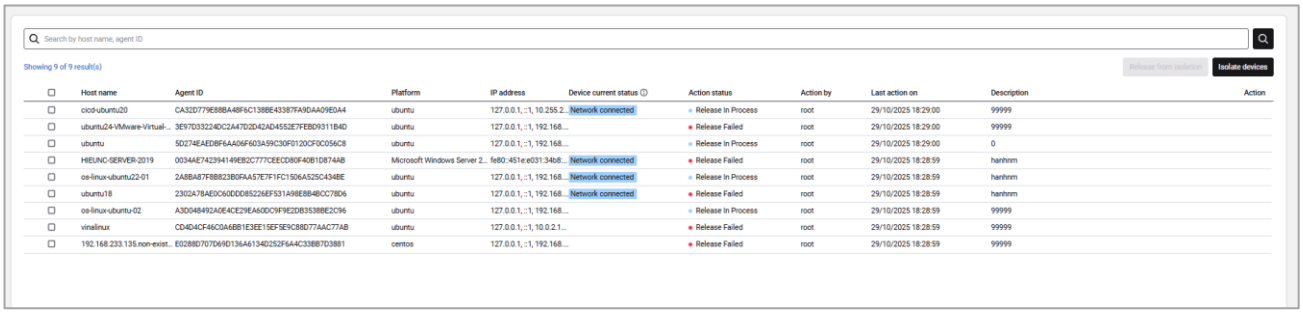


Step 2: Select the Release from isolation button -> proceed with Confirmation.

After confirming the removal of isolation, the system proceeds to unisolate the device.



Users can monitor the unquarantine status on the list screen (as shown in the example image below, the system is executing the unquarantine command).

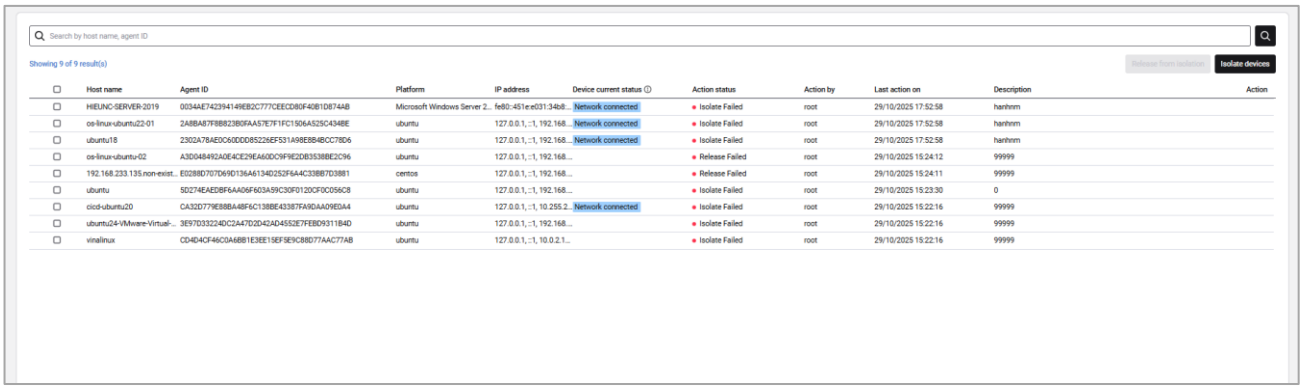


Check device isolation information / remove device isolation

After the user executes Isolate devices, the device information will be displayed on the list, allowing the user to check the following details:

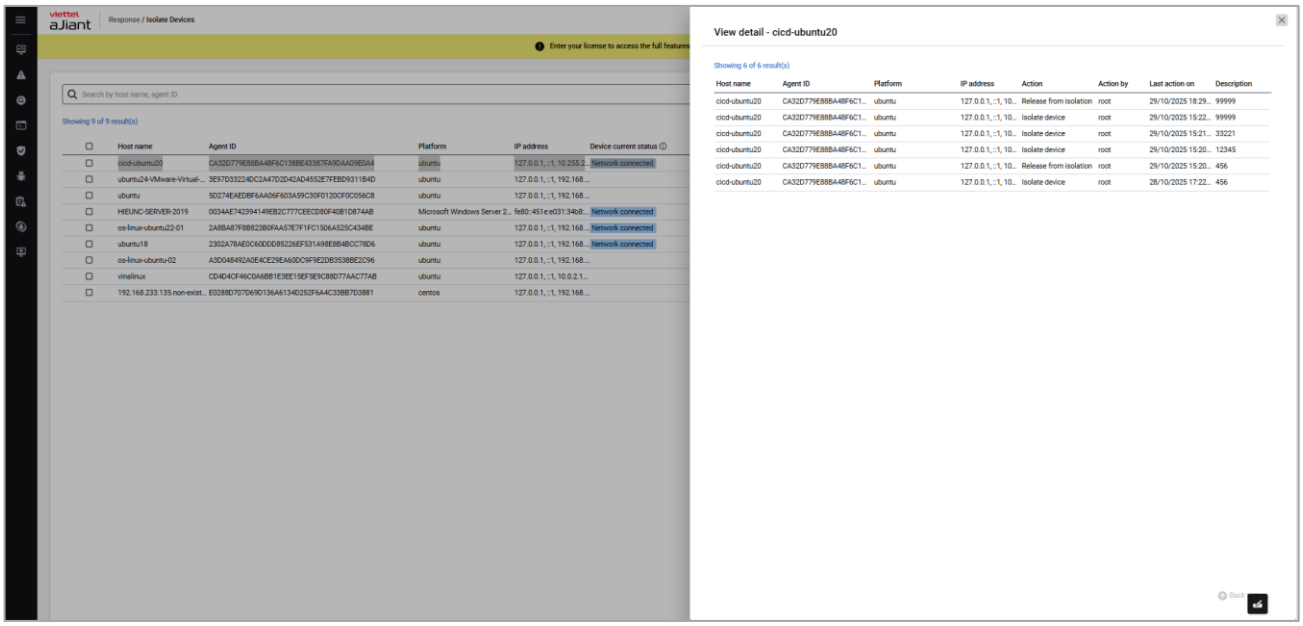
- Host name: information about the affected machine name (isolated/unisolated)
- Agent ID: is the ID of the affected machine.
- Platform: OS platform information of the affected device
- IP address: information of the affected device's IP
- Device current status: refers to the actual network status of the device, which has two states.
    - Network connected: normal network connection status
    - Network isolated: the device has been isolated, disconnected from the network, and can only connect to the VCS-aJiant system.

- Action status: represents the actual status based on user actions, including the following states.
    - In process: indicates that the system is currently executing the user's request (Isolate devices/ Release from isolation).
    - Applied: refers to the status indicating that the system has successfully executed the user's action (Isolate devices/ Release from isolation).
    - Fail: the system failed to successfully execute the user's request to Isolate devices/ Release from isolation.
- Action by: user information executing
- Last action on: the last update time of a record
- Description: description



View the impact history list by device

Users select the Action View on each record to see the list of impact history over time (Isolate devices / Release from isolation).



3.6 Settings Screen

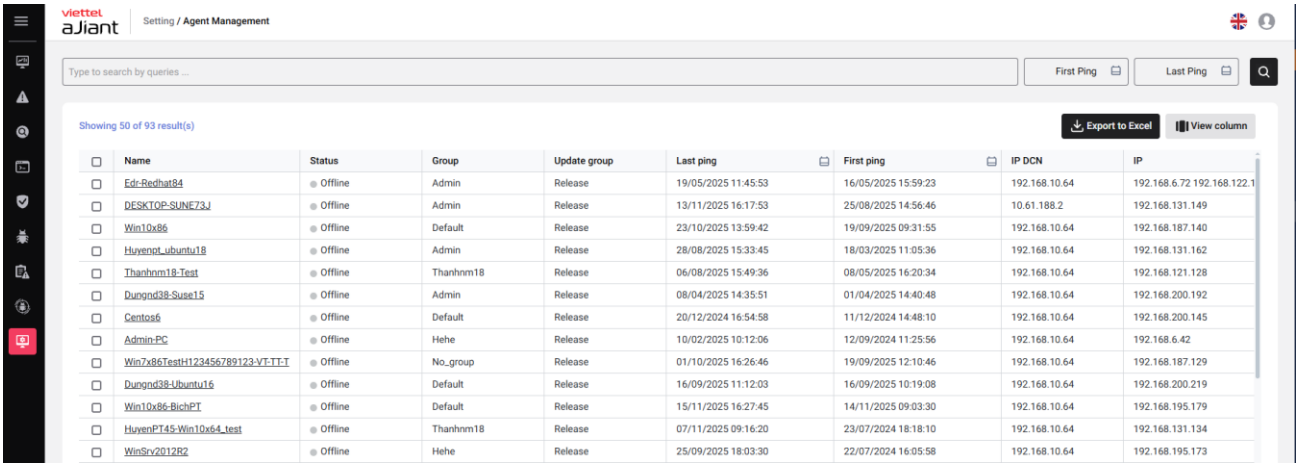
3.6.1 Agent Management

Purpose: The Agent Management function supports administrators in managing the installed agents, including:

View the list of agents and general information;

View Agent details;

Quickly select the agents and configure some settings (policy, update group);



The system supports the implementation of the following features:

1 – View the list of agents installed on the system:

User logged in as root group: Display all Agents in the system active for less than 30 days;

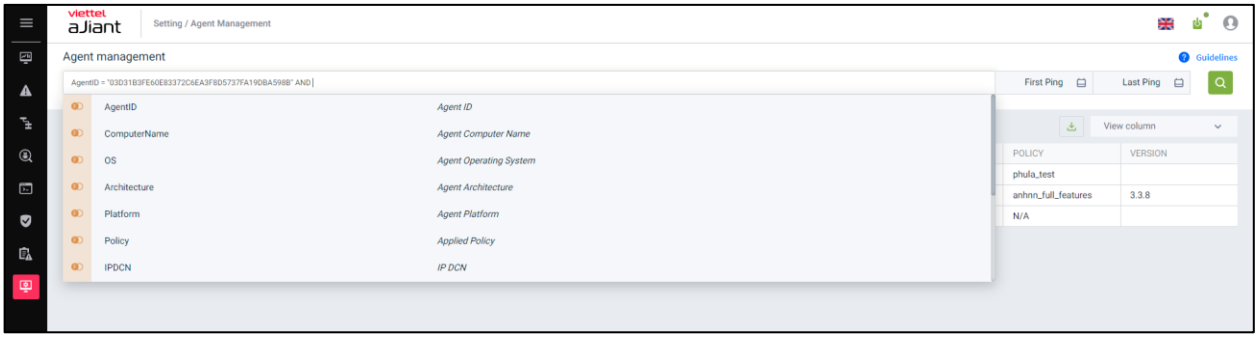
User logged in belongs to the default group: Display all Agents belonging to the default group;

User login belongs to parent group: Display all Agents belonging to the user's current group and the corresponding subgroups;

User logged in belongs to one or more subgroups: Display all Agents belonging to the user's groups currently logged in;

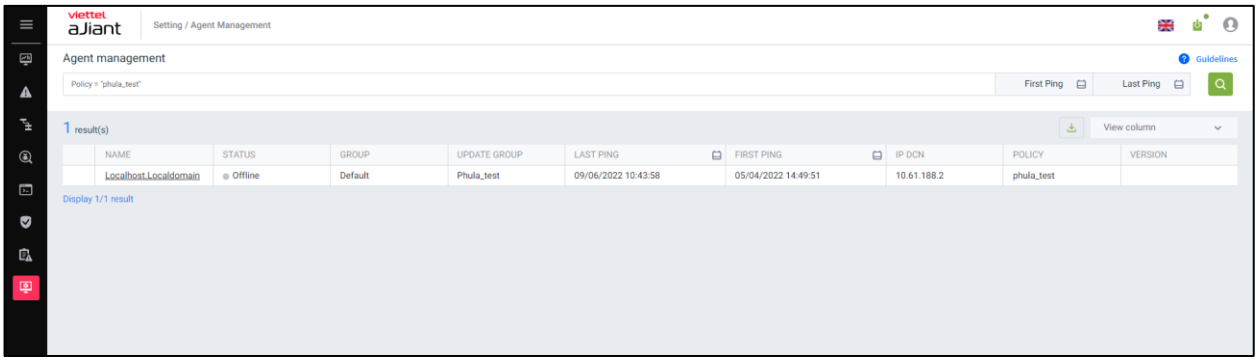
Each agent displays general information including: Name, Status, Group, Update Group, Last Ping, First Ping, DNS, Policy, AgentID, Platform, Platform Version, Architecture, DNS, Version, IP, License.

2 – Support the search function for Agents by AgentID, ComputerName, OS, Architecture, Platform, Policy, IPDCN, Online status, Update Group, Group ID, IP, Mac, and Version. For each search criterion, support the search operators "=", "!=", and "~".

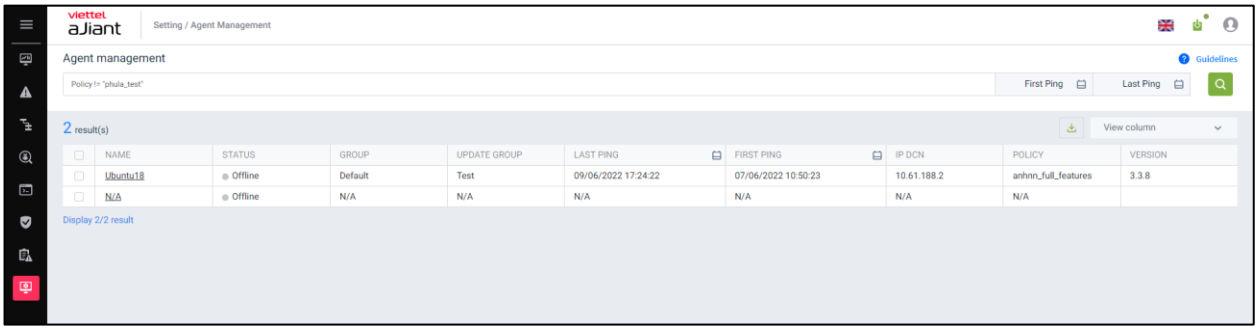


Examples of search queries:

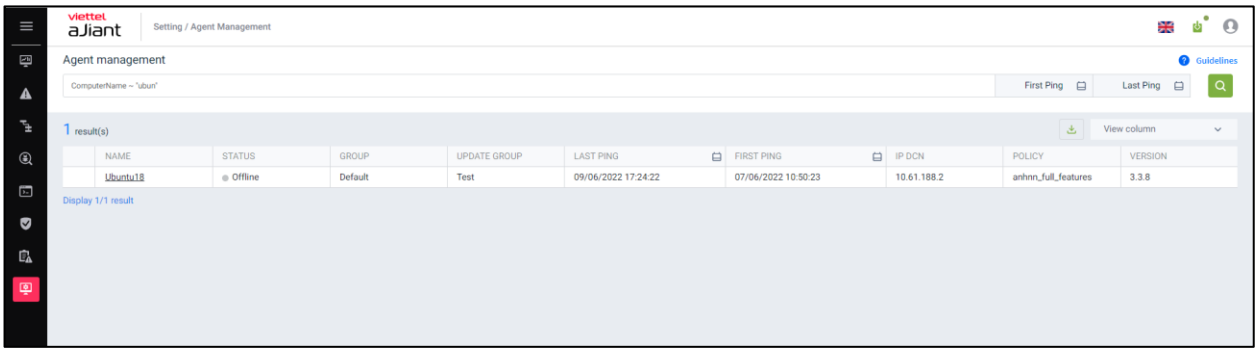
Search with the condition "=":



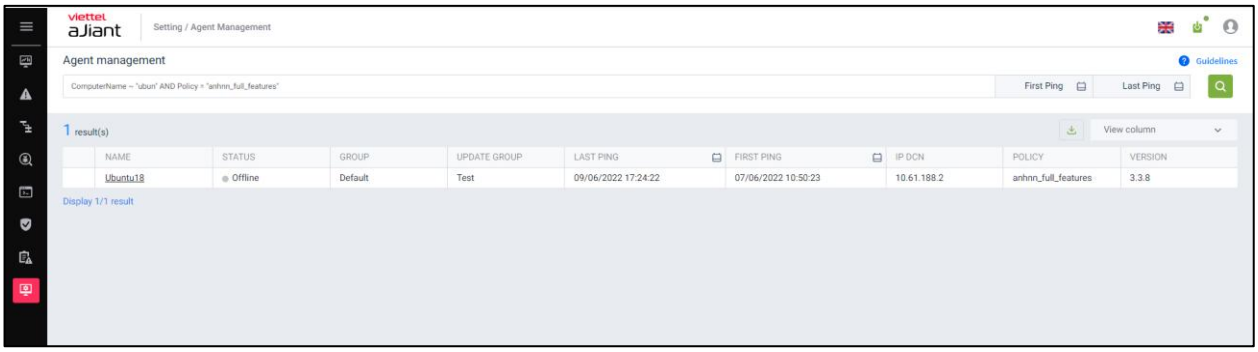
Search with the condition "!=":



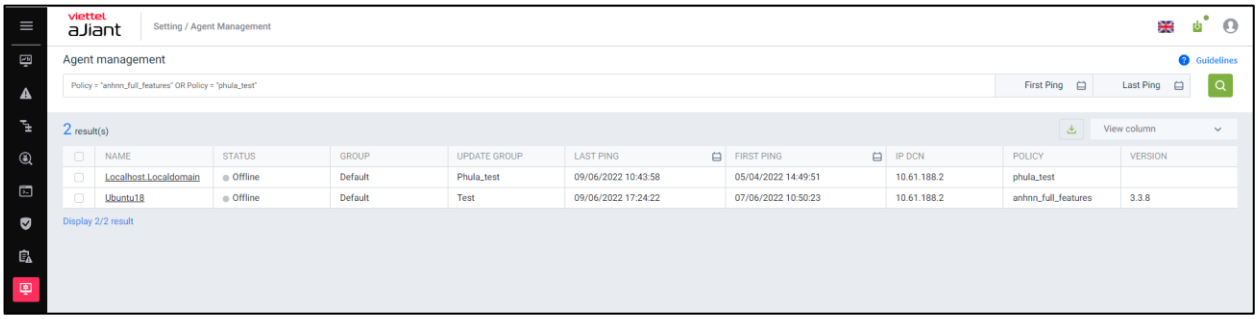
Search with the condition "~":



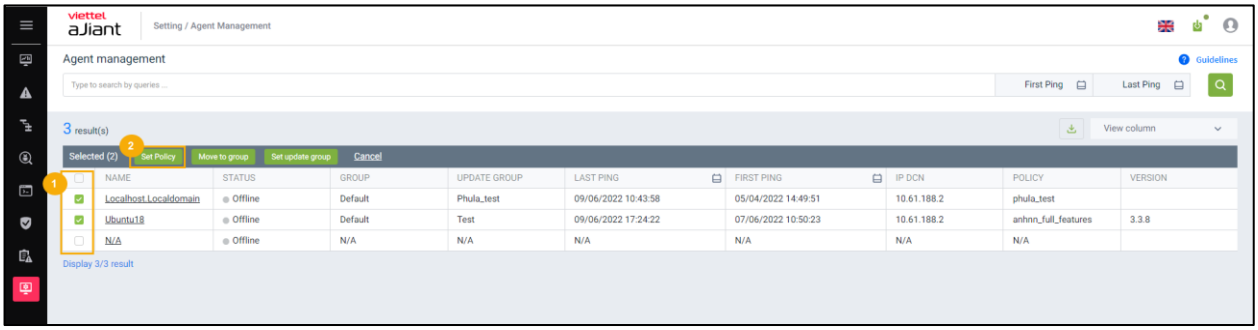
Search using combined AND criteria:



Search using combined OR criteria:



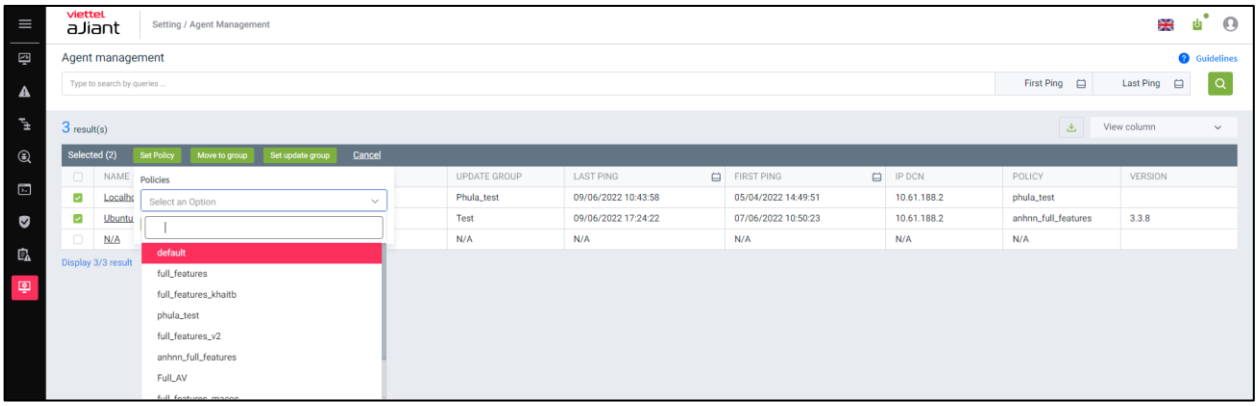
3 – Quickly select one agent or one group of agents to set up the Policy.



Select one agent/multiple agents to enter the Multiselected session;

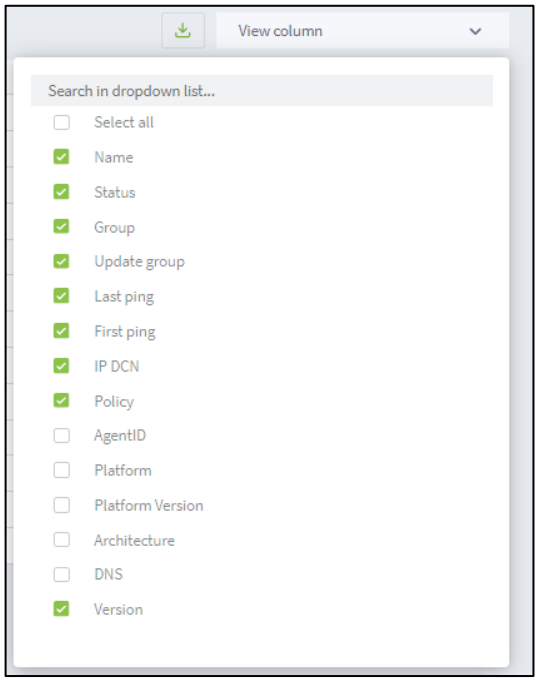
Implement Set Policy:

- Select Policy:



- Confirm the action by selecting the “Set policy” button;
- Confirm the cancellation by selecting the “Cancel” button.

4 – View Column: Configure the display of columns according to your preferences.



5 – View the details of an agent by double-clicking on any row.

The system supports users in quickly setting up Policies, Update Groups, and Move to Group actions for Agents.

User logged in as root group: Display all Groups in the system;

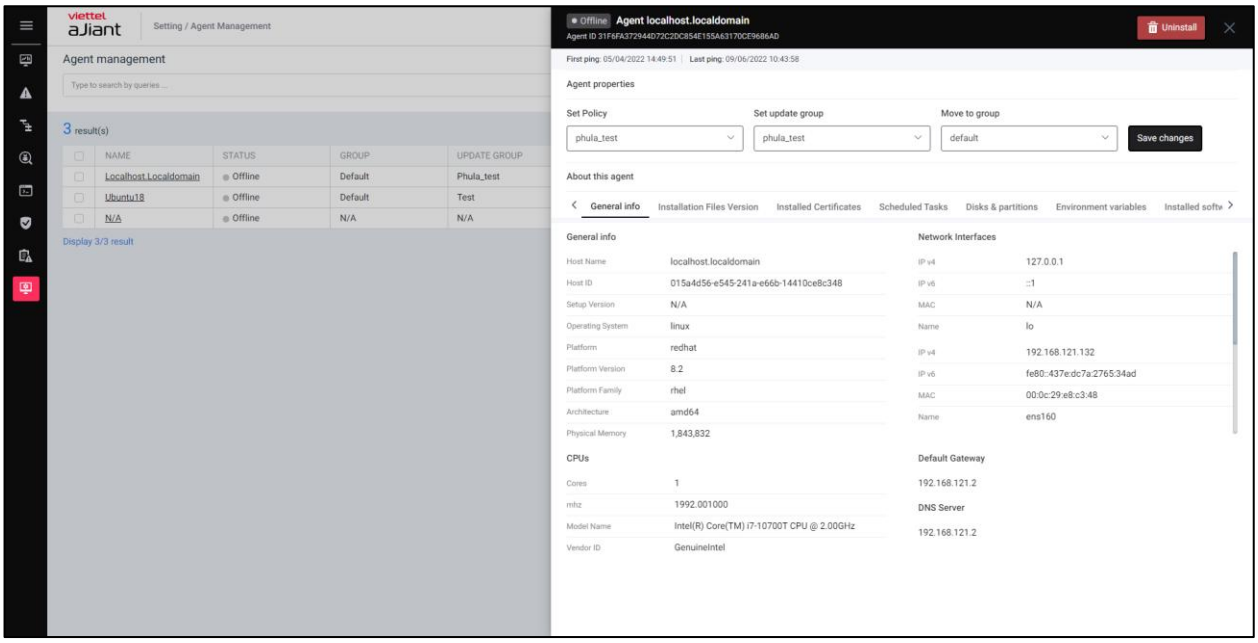
User login belongs to default group: Display Default Group;

User login belongs to parent group: Display all groups that the logged-in user belongs to and the users belonging to the corresponding child groups;

User logged in belongs to one or more subgroups: Display all groups associated with the logged-in user;

General Info Tab

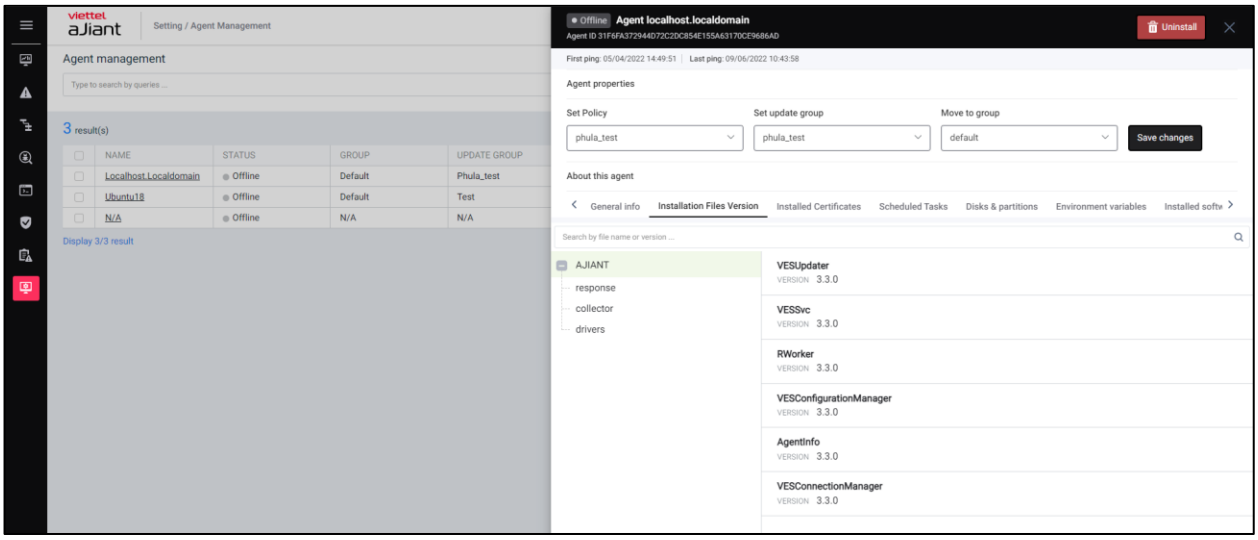
The system displays general information about the agent, including: General Information, CPUs, Network Interfaces, Default Gateway, and DNS Server.



Phiên bản Tệp Cài đặt

Compile statistics for all agent installation files, including the following information: Folder name containing the installation file, File name, Version;

Support quick search by File name and Version in the search text box.



Installed Certificates

Statistics of all certificates on the machine with the agent installed, including the following information: List of certificates on the machine, Issued by, Issued to, Expiration date, Status;

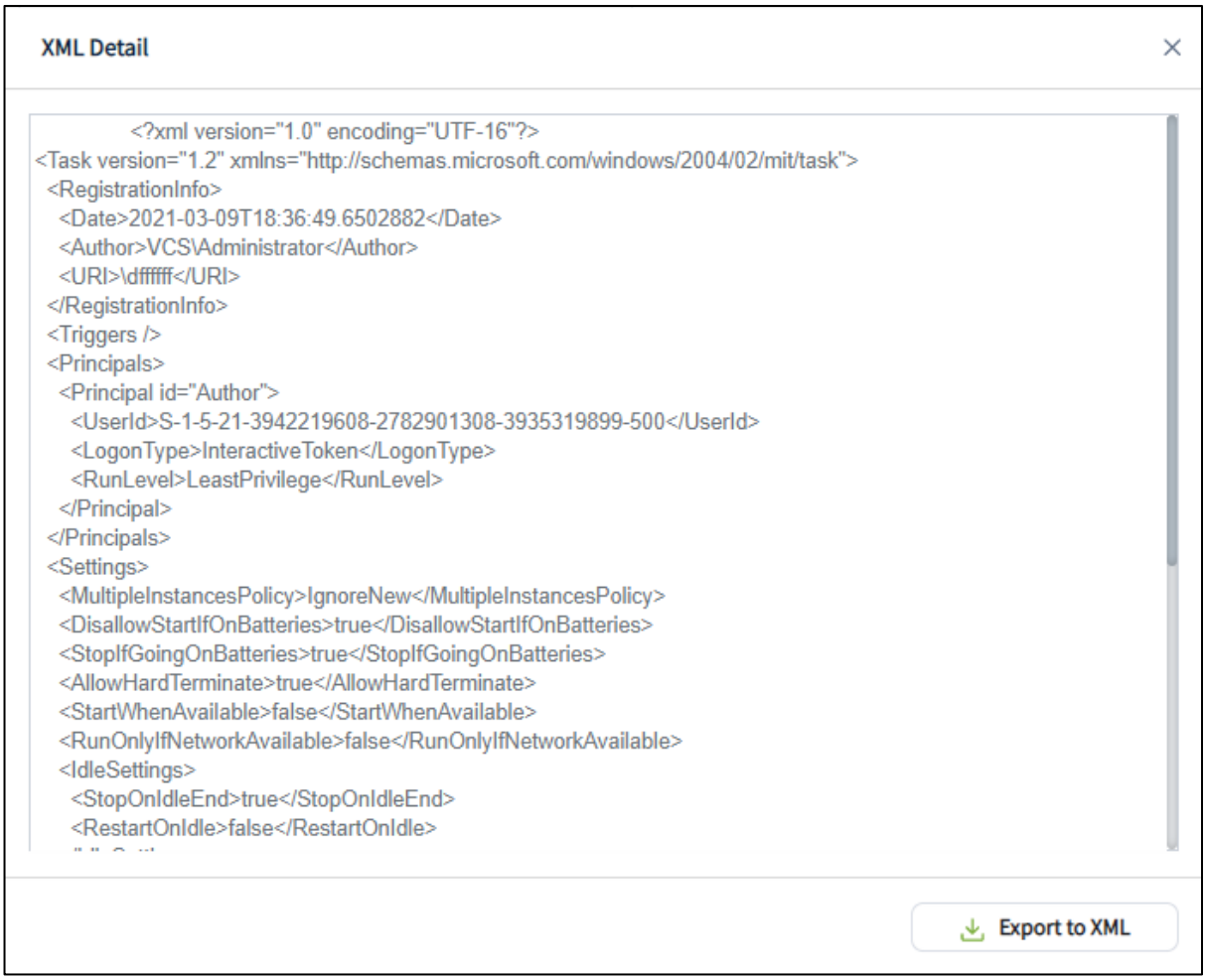
In case you want to view more detailed information, select , and the screen will display as follows:

Scheduled Tasks

List all scheduled tasks on the machine with the agent installed, including the following information: Scheduled tasks list, Name, Status, Trigger, Next run time, Last run time, Author, Created date;

Select or customize the display of additional information for each task;

Hover over the task and select to view the full task information in XML format.

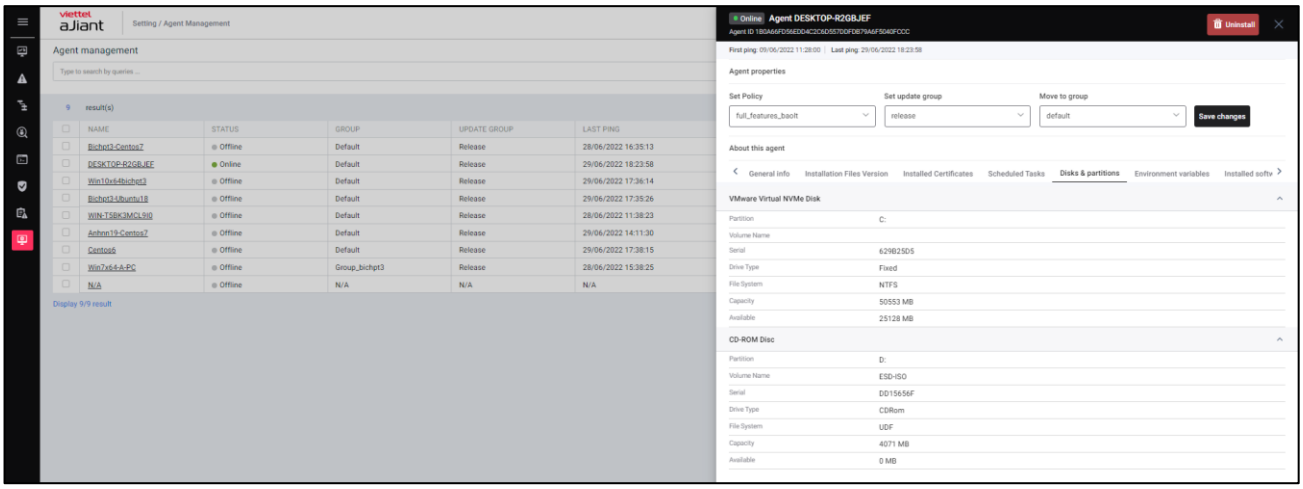


Select to download scheduled task information, supporting .xml format.

Disks & partitions

Statistics of all disks and partitions on the machine with the agent installed, including the following information: List of Disks, Partitions, Volume Name, Serial Number, Drive Type, File System, Capacity, Available Space.

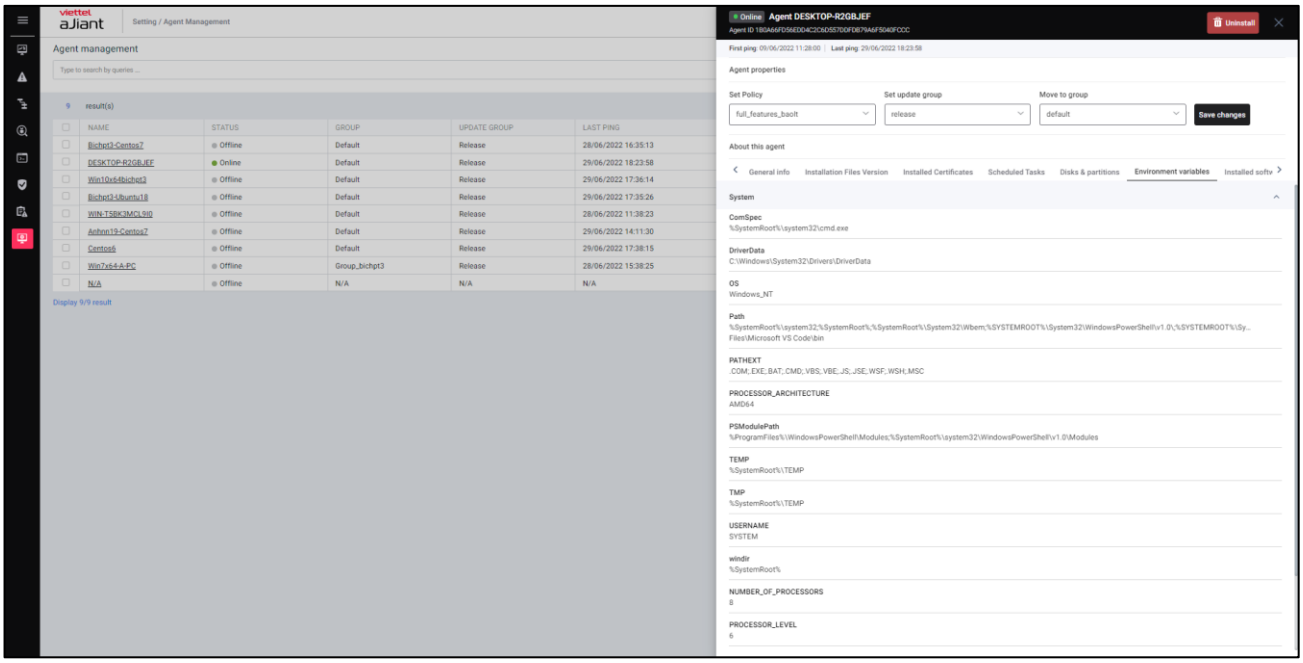
Select or leave blank to customize the display of additional information for each disk.



Enviroment variables

Statistics of all environment variables on the machine with the agent installed, including the following information: list of systems and users, variable names, and values belonging to the system or user;

Select or leave blank to customize the display of additional information for each disk.



Installed Software Tab

List all software installed on the agent, including the following information: software name, installed version, installation date;

Supports quick search of installed Antivirus software or enter the software name into the search text box;

Tab Required Software

Compile statistics of all mandatory software installed or not installed on the agent, including the following information: software name, installed version, installation status.

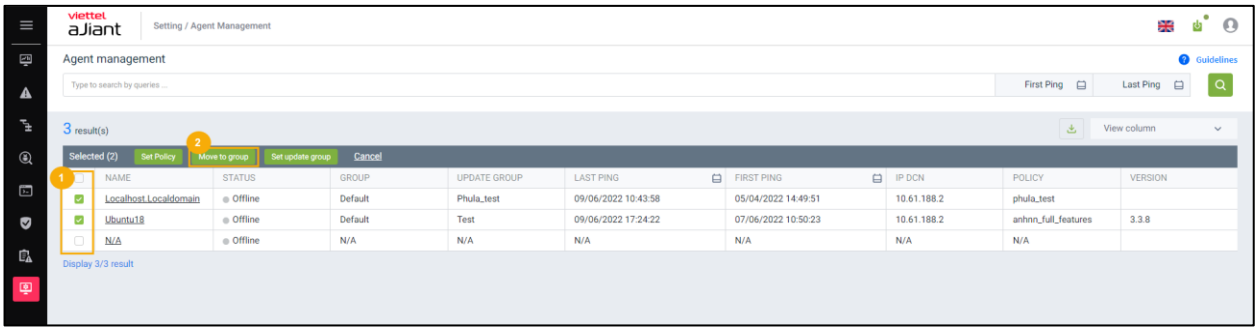
Support quick search for mandatory software not yet installed on the machine or enter the software name into the search text box.

User List Tab

Statistics of all users logged into the agent, including the following information: Username, active status, administrator status.

6 – Quickly select 1 agent or 1 group of agents to set up Move to group.

Select one agent/multiple agents to enter the Multiselected session;



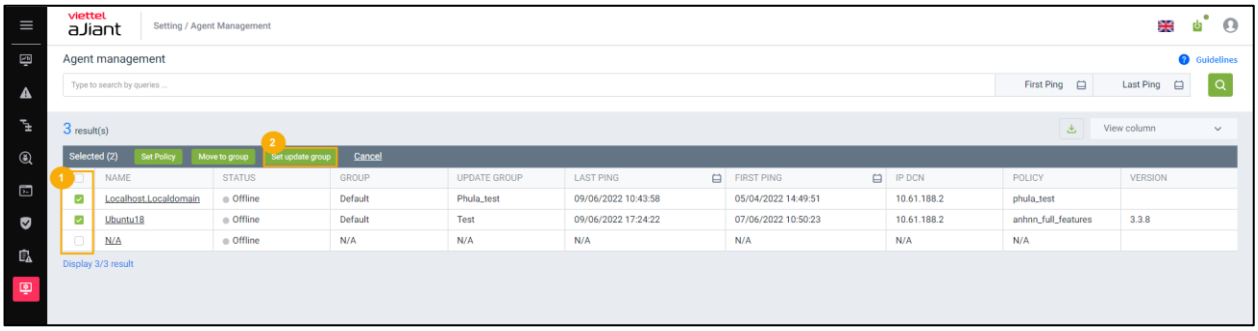
Perform Move to group:

List of Groups in the "Move to group" combobox:

- User logged in as root group: Display all Groups in the system;
- User login belongs to default group: Display default Group;
- User login belongs to parent group: Display all groups the logged-in user belongs to and the users belonging to the corresponding child groups;
- User logged in belongs to one or multiple subgroups: Display all groups associated with the logged-in user;

Quickly select 1 agent / 1 group of agents to set up the update group:

- Select one agent/multiple agents to enter the Multiselected session;



- Perform Set update group;

Note:

Move to group: Transfer agents into the groups displayed on the Group Management screen;

Update group: move agents into groups that store files running under the Agent; each group contains different executable files as defined on the server.

How to calculate the VCS-ajiant license:

The license will be calculated based on the number of endpoints (for example, if the customer purchases a 10-endpoint license, they will be allowed to install the agent on 10 devices).

The system will calculate the license for the agent based on the time the agent connects to the VCS-aJiant system (the first ping time; agents that connect earlier will be assigned licenses first).

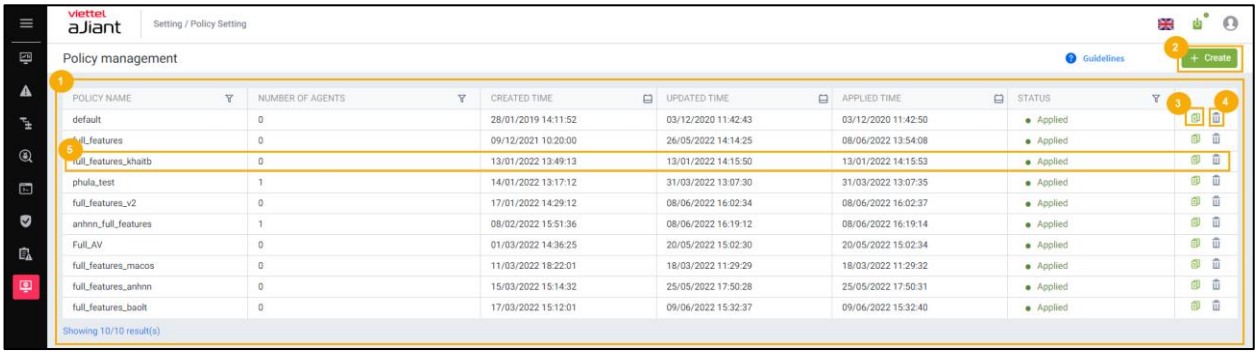
In the case of:

1. If the customer installs more licenses than allowed: the detection, prevention, response, and other features will not function on these devices.

2. If the license expires: the system will automatically disable all features on all devices until the license is renewed, while customers will still see the agent online on the portal.

3.6.2 Policy Setting

Purpose: To assist users in managing the list of configuration policies for Agents;
Interface screen when the user accesses Setting >> Policy Setting:

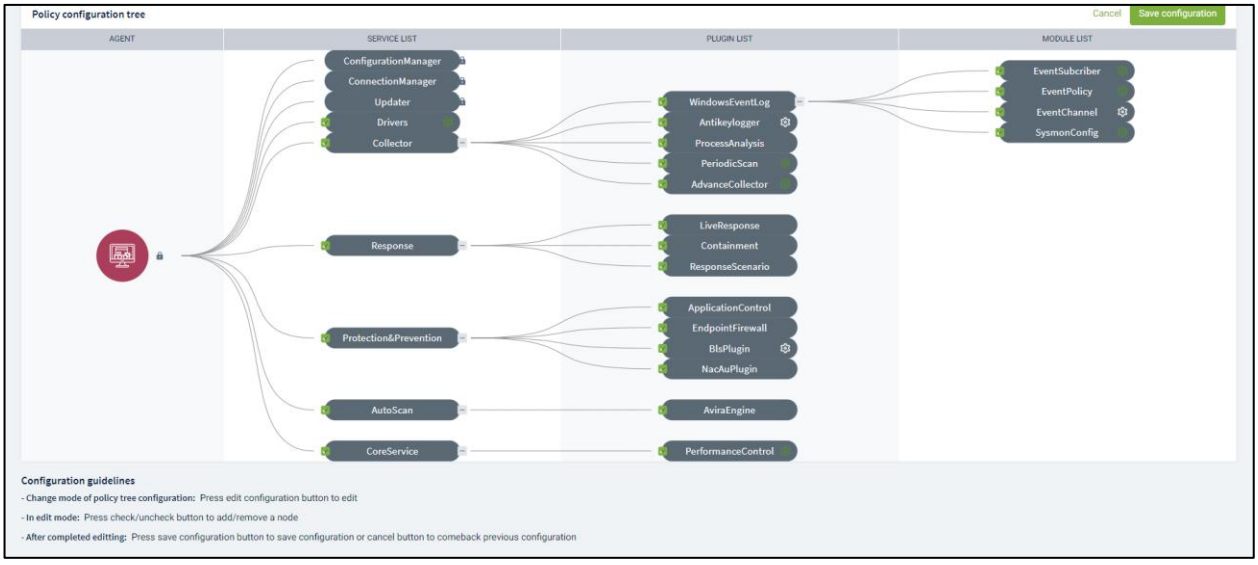


1 – Display the list of Policies created in the system. Each policy includes the following information: Name, number of Agents the policy is applied to, creation time, update time, policy application time, and status (with 2 statuses: Applied and Not Applied).

2 – Create a new policy: Click the "Create" button, and the system will display a popup for creating a new policy as follows:

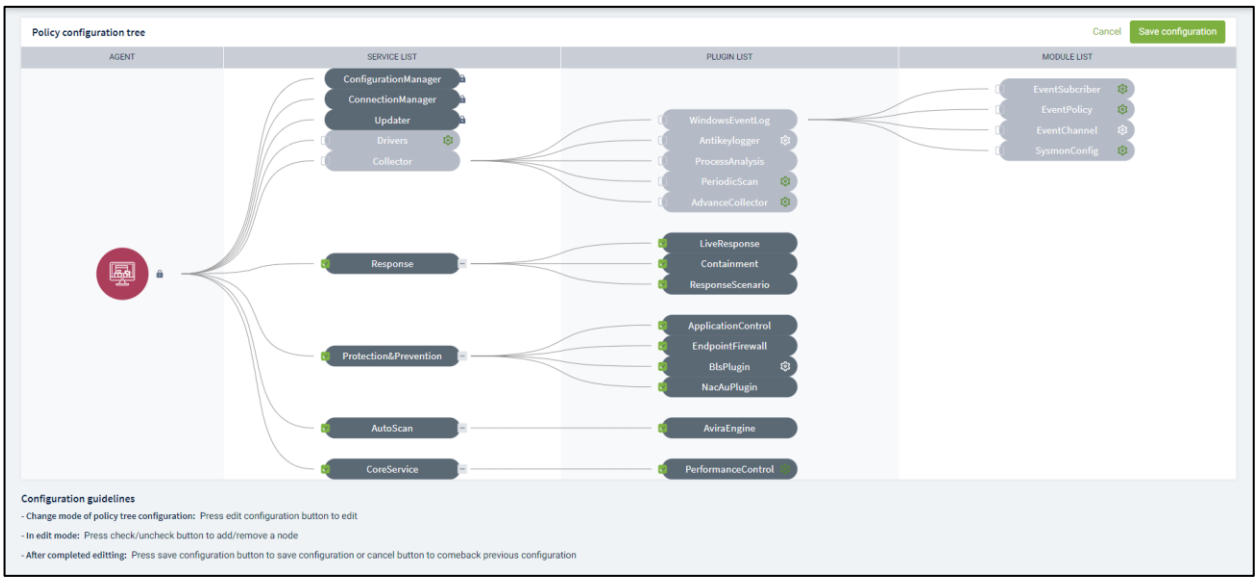
Note: When creating a new policy, the policy name must not duplicate any previously created policies.

After successfully creating a new policy, the system will display the detailed screen of the policy:



Each policy created typically has 3 default core services: ConfigurationManager, ConnectionManager, Updater. Note that these 3 services must not be deleted from the system. The steps to configure a policy are:

- Click the button to change the Policy tree.
- In Edit mode, users are allowed to Check/Uncheck to Add/Remove other services:



- After completing the edit mode:
    - The user clicks the "Save config" button to save the changes;
    - The user presses the "Cancel" button to abort the Policy update operation, and the system reverts to the previous configuration.
- Click the icon to configure detailed settings for each module/plugin of the Services.

Module/plugin	Description
Windows Event Log	- WindowsEventLog Configuration: Configure log sources to be collected by the Agent + EventSubscriber: specify the log channels to collect Data requirements:

	Event_filter field (filter by Event ID): substrings separated by commas (,); Example: “4”: filter events with eventID = 4 “-689”: filter events with eventID ≠ 689 Providers field: substrings separated by semicolons (;); Mandatory fields: subs_type, channel; Channel: log source; sub_type: PUSH: when a new event occurs, call the VCS-aJiant function to process it; POLLING: VCS-aJiant actively collects logs after a certain interval; PULL: VCS-aJiant actively retrieves logs after a certain interval; After configuration, remember to Save: EventPolicy: Set policies to enable/disable certain log types that are not enabled by default in the system; Requirement: at least one field must be selected EventChannel: detailed configuration for certain log sources: Retention: whether to enable log rotation (if Retention is selected, when the log file is full, new logs will overwrite the oldest logs); Log file path: path to the log file; Log file size: size of the log file; Requirement: all fields must be filled in; SysmonConfig: enable/disable the Sysmon tool on the

	Agent to collect sysmon logs: Microsoft-Windows-Sysmon/Operational;
Antikeylogger	Antikeylogger Configuration: This is a SelfRun Plugin of VCS-aJiant, responsible for periodically scanning the entire system to detect any running KeyLoggers if present. Scan Setting: Configure the types of KeyLoggers to be scanned. Requirements: - Scan cycle: minimum 1 minute, maximum 180 minutes; - Select at least one type of KeyLogger; Whitelist Setting: Configure a whitelist for certain software based on the file path on the disk or the digital signature (certificate) of the KeyLogger executable file. Requirements: Fill in all fields completely; After completing the entries, remember to “Save” the configuration.
Self-defense	Self Defense Configuration: Add an uninstall protection mechanism for Self Defense; Instructions: Select Choose Drivers > Check Self Defense to enable the Self Defense feature or uncheck to disable it > select Save > select Apply Policy;
Autoscan	Autoscan Configuration: allows users to add additional configurations when scanning for malware. - Requirement: Select Autoscan -> Add new configuration. The new information to be added includes: + Version + Description + Data config for Windows will have a format as follows: Note: For configurations of the automatic or manual malware

	scanning streams, they must be placed under the corresponding key “auto_scan” / “manual_scan”.
AntiRansomware	AntiRansomware: allows configuration changes when removing ransomware malware Requirement: Select Auto Scan -> choose Anti Ransomware
HIPS (High Impact Polystyrene)	HIPS: allows configuration changes when eliminating malware based on behavior Requirement: Select Auto Scan -> choose HIPS
Performance control linux	Performance control is a module that monitors and limits the resources used by each EDR service on the user's machine. The resource limit parameters configured on the portal include: - CPU threshold: Allows users to configure a CPU limit for each agent. Agents will operate within the configured range and will not exceed the set CPU threshold. - MEM threshold: Allows users to configure a memory limit for a process. When memory usage exceeds the configured threshold, the process will automatically restart to free up resources. - FD value: Allows users to configure a limit on the number of files opened by a process. When memory usage exceeds the configured threshold, the process will automatically restart to free up resources. - DiskIO value: Allows users to limit the disk access speed (read/write) of a process. The process will throttle below the configured value. - Configure Network value: Limits the network speed the process can handle per second. The process will throttle below the configured value.

<table>
<tr>
<td></td>
<td>
- Requirements: Select CoreService -> select PerformanceControl

Supported configuration fields are as follows:

<table>
<tr><th>#</th><th>Config</th><th>Value type</th><th>Description</th></tr>
<tr><td>1</td><td>Process name</td><td>String</td><td>Name of process</td></tr>
<tr><td>2</td><td>Cpu peak</td><td>Int</td><td>Peak Cpu threshold</td></tr>
<tr><td>3</td><td>Cpu Avr</td><td>Int</td><td>Avr cpu threshold</td></tr>
<tr><td>4</td><td>Memory peak</td><td>int</td><td>Peak memory threshold</td></tr>
<tr><td>5</td><td>Memory Avr</td><td>Int</td><td>Avr memory threshold</td></tr>
<tr><td>6</td><td>Disk IO peak</td><td>Int</td><td>Peak io threshold</td></tr>
<tr><td>7</td><td>Disk IO Avr</td><td>int</td><td>Avr io threshold</td></tr>
<tr><td>8</td><td>Network Peak</td><td>Int</td><td>Peak network threshold</td></tr>
<tr><td>9</td><td>Network Avr</td><td>Int</td><td>Avr network threshold</td></tr>
<tr><td>10</td><td>deltatime_cpu</td><td>Int</td><td>Time counting cpu</td></tr>
<tr><td>11</td><td>deltatime_memory</td><td>Int</td><td>Time counting mem</td></tr>
<tr><td>12</td><td>deltatime_disk_io</td><td>Int</td><td>Time counting io</td></tr>
<tr><td>13</td><td>deltatime_network</td><td>Int</td><td>Time counting net</td></tr>
</table>
</td>
</tr>
<tr>
<td>Prevention Known Threat</td>
<td>
Prevention Known Threat is a feature that helps detect attacks or malware that have been published/recorded worldwide, displayed via IOC hash.

- Requirements: Select Autoscan -> select IocEngine.

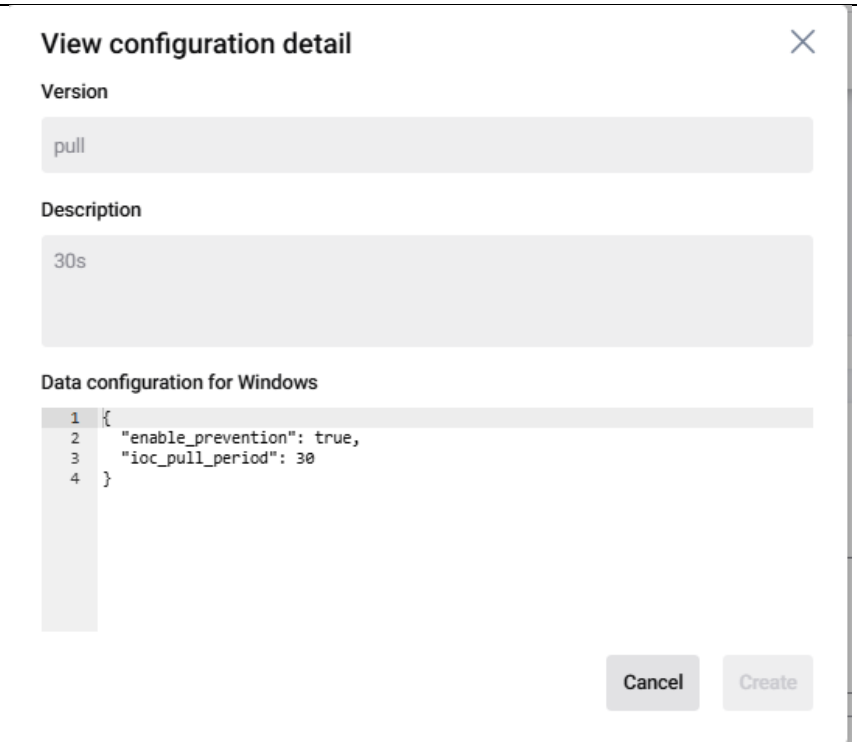
- If there is no configuration, IocEngine will use the default configuration.

- If you want to add a configuration, select IocEngine -> Add new configuration. The information to add includes:

+ Version

+ Description

+ Data config for Windows will have a format like this (e.g., as shown below).
</td>
</tr>
</table>



The configuration support fields in the IocEngine flow are as follows:

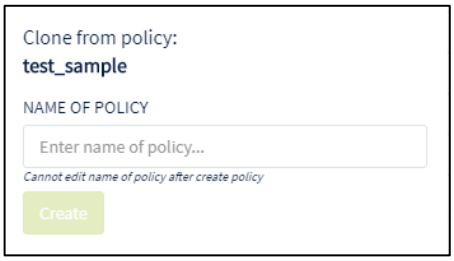
Config	Type	Description	Default value
enable_prevention	bool	Enable/disable malicious IOC blocking mode	false
revoke_ttl	integer	Maximum time the revoke list is in effect	7*24 (7 days)
max_file_size	integer	Maximum file size to scan; files larger than this size will be skipped from IOC scanning	10MB

	whitelist_ioc	string array	List of whitelisted hashes	Empty list
	max_hash_speed	integer	Maximum hash file reading speed	512 KB/s
	max_queue_length	integer	Maximum number of elements in the IOC scan queue	10.000
	delay_scan_time	integer	Delay time before retrying IOC scan with a failed file scan	10 second
	max_cache_size	integer	Maximum number of elements in the IOC scan cache	100000
	ioc_pull_period	integer	IOC DB pull cycle from backend	600(10 minutes)
	disinfect_timeout_ms	integer	Time to attempt to delete an IOC	3000 miliseco nd
	rescan_timeout_min	integer	Time to not rescan a file after scanning is complete	5 minute
	disinfect_retry_interval_ hour	integer	Time to not retry after a failed deletion of a malicious IOC	24 hour
	scan_sleep_time_ms	integer	Delay time between each scan	50 miliseco nd

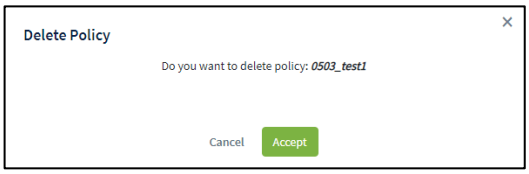
Fileless	Fileless detection is a feature that helps detect hidden malware behaviors that bypass antivirus and gain execution privileges. - Requirements: Select VESCollector -> select MemoryScanner.

- Click the button to apply the newly configured Policy to the Agent:

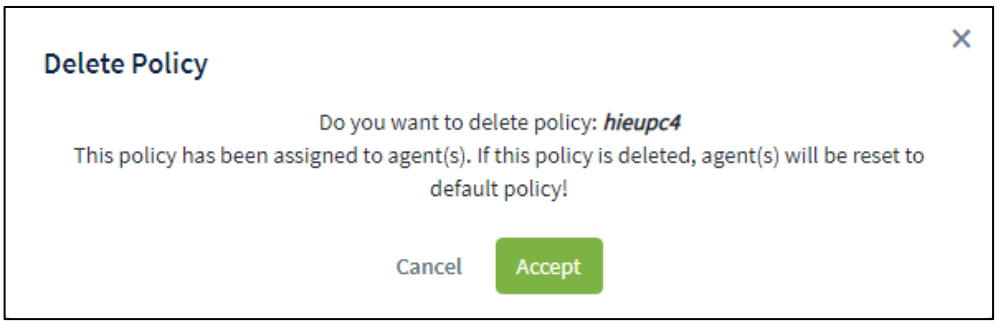
Clone new policy: Click the button and the system will copy all details of the policy being cloned except for the policy name.



Delete policy: Click the button to display a pop-up for the user to decide whether to delete or not.



In cases where the Policy already has an assigned agent, after deletion, the system automatically assigns the "default policy" to those agents;



When double-clicking on each record, the system will redirect to the detailed page of a policy for the user to view or modify the policy configuration.

3.6.3 Group Management

Configure rules to automatically change policies and reassign groups for agents if they meet the criteria on the Portal, reducing the time spent on policy changes and group reassignment for each agent, and synchronizing policies for agents who meet the configured rules.
The main features on this screen include:

Tree-structured group management;

Search group;

Add new group:

- Create an automatic group transfer rule for agents;
- Options for transfer method (All existing agents, New agents only, All existing and new agents) and assign policy (assign immediately, do not assign);

Monitor the agents belonging to the group, total number of agents in the group;

Edit group;

Delete group, delete agents belonging to the group;

1 – Tree-based group management:

User logged in as root group: Display all Groups in the system;

User login belongs to default group: Display default group;

User login belongs to parent group: Display groups belonging to the logged-in user's group and the corresponding subgroups;

User login belongs to one or more subgroups: Display all groups belonging to the user's group currently logged in;

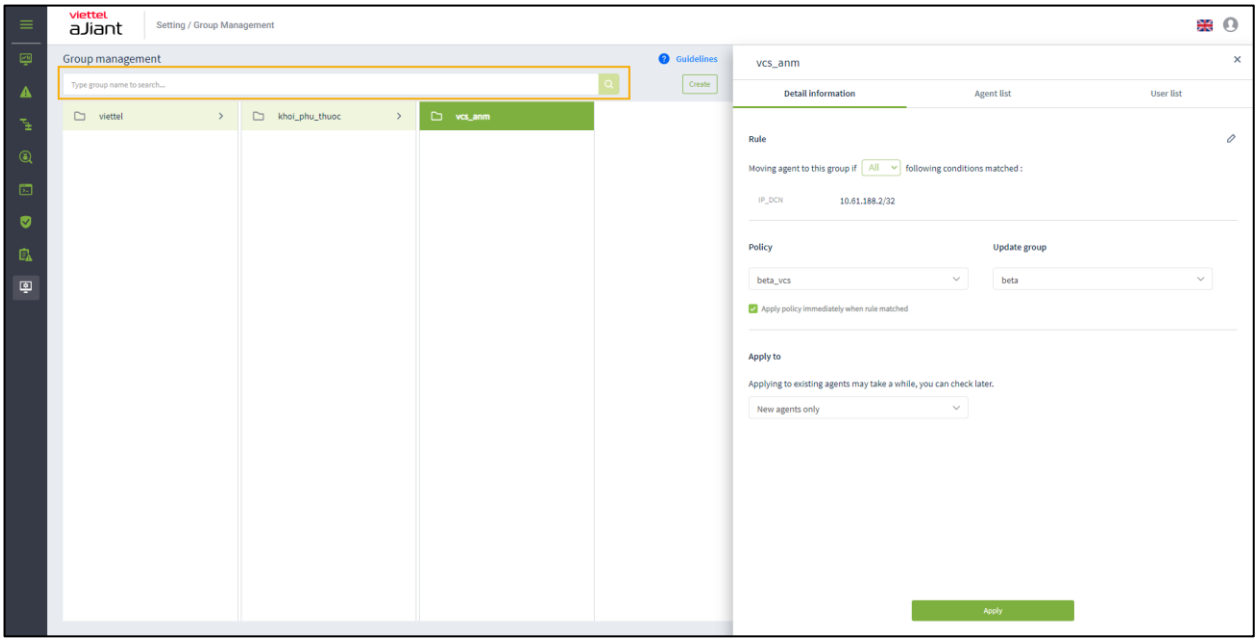
The group list is displayed in a tree structure, including root groups, each containing first-level subgroups, second-level subgroups, and so on.
Each group includes the group name, configuration information of the group (rule, policy, apply to), and the list of agents belonging to the group.

The rules of each group are independent from one another (no parent-child inheritance). Group management is organized in a tree structure to facilitate easier management when the number of agents is large and there is a hierarchical management of agents by company, department, division, etc.
When a user belongs to a child group, selecting the parent group will not display the group detail popup.

2 – Search group

Method 1: Click on the Search textbox > a list of groups corresponding to the logged-in user will appear and can be scrolled > Select a group from the displayed list;

Method 2: Click on the Search textbox > enter the search characters into the textbox > the system will automatically search for records containing the entered characters > select a suitable record from the suggested list or click Search or press Enter to display a list of matching records;



Double-clicking on a record will display the detailed information of that record.

The detailed information tab displayed is Detail, and the data for that group includes Rule, Policy, and Apply to;

When selecting the Agent list tab, the data of agents matching that group is displayed.

When right-clicking on a record, two options will be displayed: Go to group and Delete group.

If "Go to group" is selected, the user will be taken to the location of that group on the tree.

If Delete group is selected, a confirmation popup to delete the group will be displayed.

When clicking on the menu in the top right corner of each record, two options are also displayed: Go to group and Delete group.

3 – Add new group:

User logged in as root group: Can add all Groups;

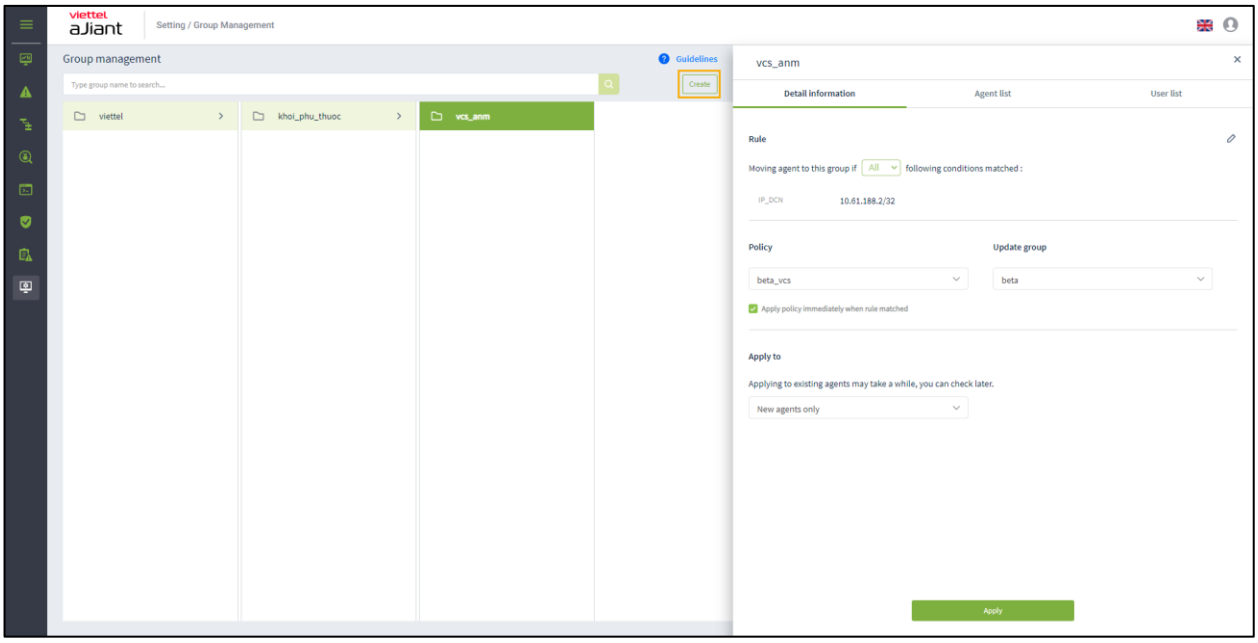
User login belongs to default group: Cannot add new;

The user logged in under the parent group: can add new subgroups corresponding to the group the user belongs to.

The user logged in belongs to one or more subgroups: it is possible to add new subgroups corresponding to the groups the logged-in user belongs to.

- Select the position where the group will be created.

To create a new group in the original group list, click the “Add new” button at the top right corner of the screen or hover at the end of the original group list on the screen and click Add new;



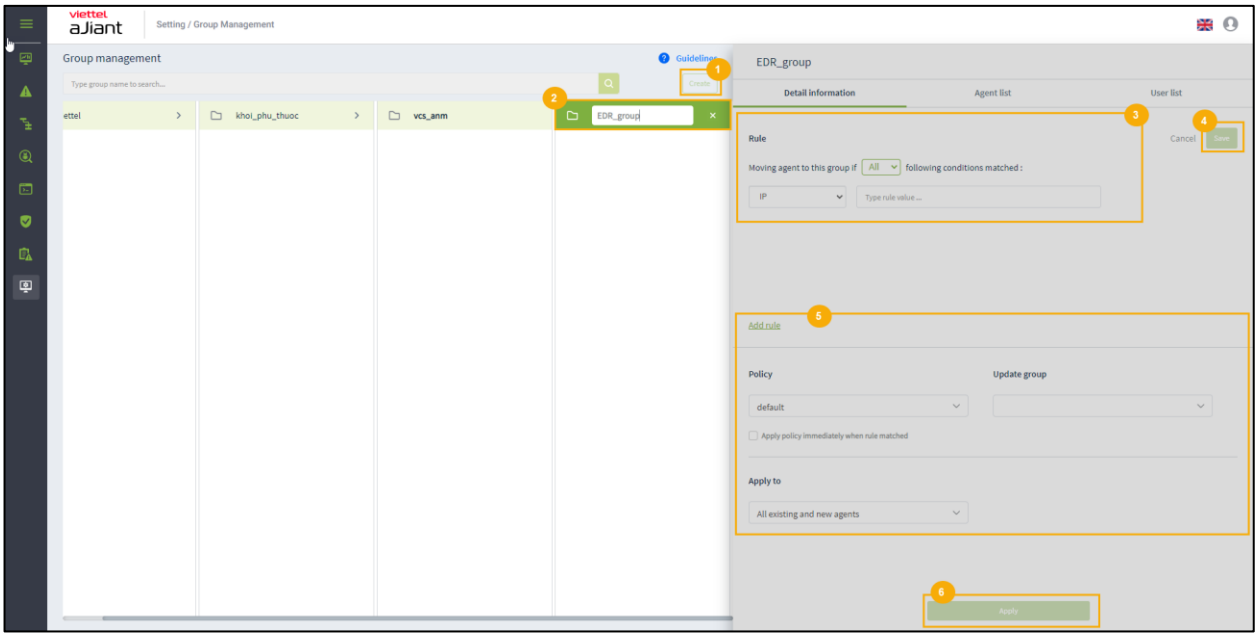
If creating a new subgroup within a parent group or a level 1, level 2 group, etc., click on the parent group, then click “Create” on the screen, or hover at the end of the list of groups at the same level and click “Create.”

- Enter the group name and configure the rules;

Note: Names and configuration rules must not duplicate existing names and rules.

If the "All" operator is selected: the rule is satisfied when both fields are met;

If the operator "Any" is selected: the rule is satisfied when either one of the two fields or both fields are satisfied;



- Select the policy and the type of agent that will apply the policy if the rule is satisfied:

After clicking Apply, check that the agents have been moved to the group in the Agent list tab: the list of agents that meet the criteria and have been transferred to the newly added group. The group transfer for agents in the system depends on the selection made in the "Apply to" section:

All existing agents: transfer groups for all agents currently in the system; newly installed agents, even if they match the rules after applying, will NOT have their groups transferred.

New agents only: only transfer groups for agents newly installed after applying; existing agents in the system, even if they match the rules, will NOT be transferred.

All existing and new agents: transfer groups for all agents currently in the system and newly installed agents after applying if they match the rules;

Note:

If the checkbox "Apply policy now when rule matched" is selected, then clicking "Apply" will cause the selected agents to check the values. If they match the

configured rule, the policy for the agent will be changed to the policy selected in the "Policy" section, and the group will be changed accordingly.

In the case where the checkbox above is not selected, after clicking Apply, the selected agents will be moved to a different group but their policy will not change; that is, the agents retain their current policy while moving to a group with a different policy. For newly installed agents, if they match the rule, they will be moved to the group and the "default" policy will be applied because the checkbox > apply default policy is not selected.

If a new agent matches the rules of multiple groups, priority will be given to transferring them to the most recently created group, regardless of the group modification time.

4 – Edit group: you can choose to edit 1, 2, or all 3 components within a group: Rule, Policy, Apply to

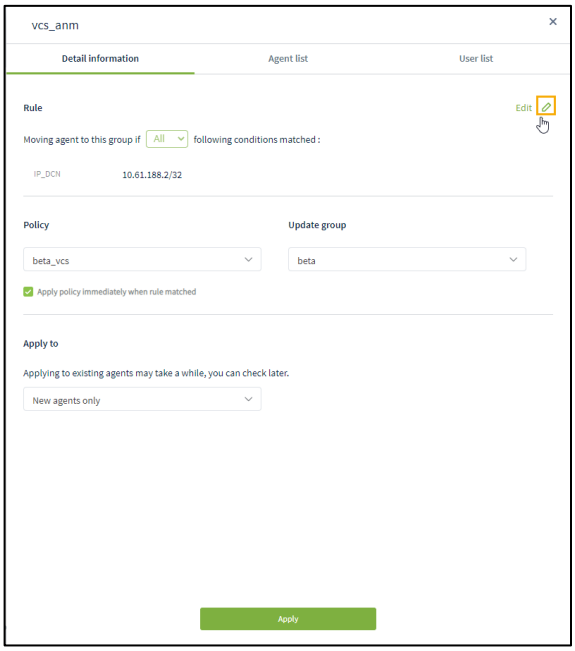
User logged in as root group: Can modify all groups in the system;

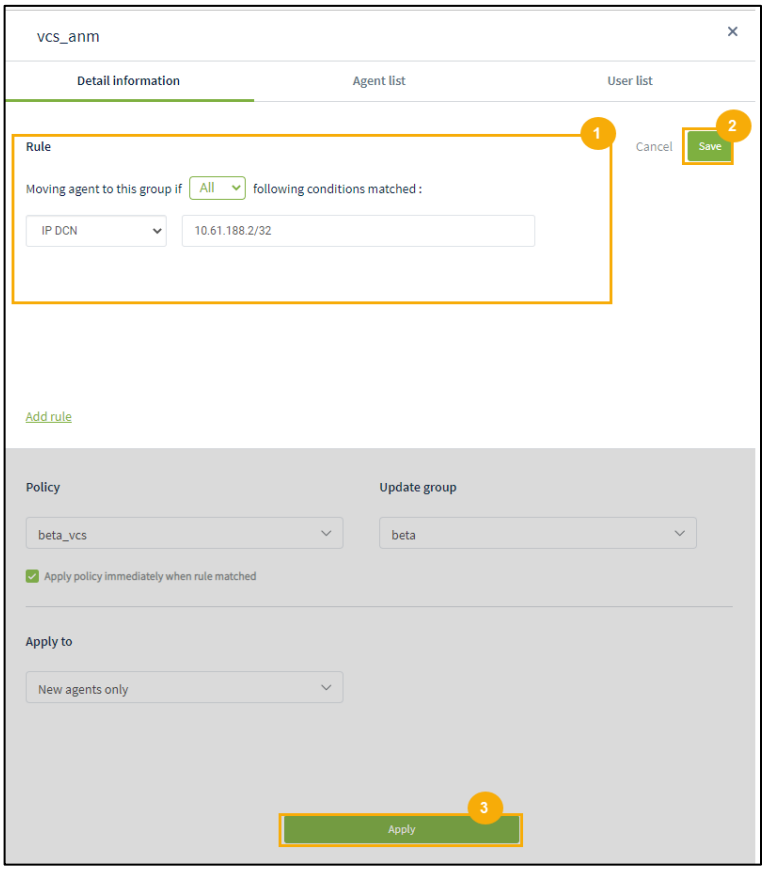
User login belongs to the default group: Modifying the default group is not allowed;

User login belongs to parent group: Can modify all groups currently logged in and child groups whose roles also belong to the child group roles of the logged-in user's role;

User logged in belongs to one or more subgroups: Can edit all groups that the logged-in user belongs to;

To edit the group's Rule, click on the Edit icon > Modify the group's rule, then click Save > After that, you can adjust the "Policy" and "Apply to" sections, then click Apply;


vcs_anm
Detail information
Agent list
User list
Rule
Edit
Moving agent to this group if All following conditions matched :
IP_DCN
10.61.188.2/32
Policy
Update group
beta_vcs
beta
Apply policy immediately when rule matched
Apply to
Applying to existing agents may take a while, you can check later.
New agents only
Apply


vcs_anm
Detail information
Agent list
User list
1
Rule
Moving agent to this group if All following conditions matched :
IP DCN
10.61.188.2/32
Cancel
2
Save
Add rule
Policy
Update group
beta_vcs
beta
Apply policy immediately when rule matched
Apply to
New agents only
3
Apply

Note:

In cases where components of the group (Rule, Policy, or Apply to) are modified but Apply is not clicked, the edits are saved but the Agent list is not updated. For newly installed Agents, the process is as follows:

- Group transfer: depends on whether the new Agent is selected in the "Apply to" field; if selected, the Agent side will be checked, and if the group's rules match, it will be transferred to the group.

- Apply policy: The agent's policy depends on whether the "Apply policy now when rule matched" checkbox is selected. If the checkbox is selected, the group's policy will be applied; if not selected, the default policy will be applied since not selecting the checkbox triggers the default policy.

In the case where the components of the group have been edited and the Apply button is clicked, the changes will be saved. Additionally, if the "All existing agents" option is selected in the "Apply to" section, the system will scan information for all agents and reassign the group to each agent, then update the Agent list.

For new agents, handle it in the same manner as above.

5 – Delete group or remove agent from group:

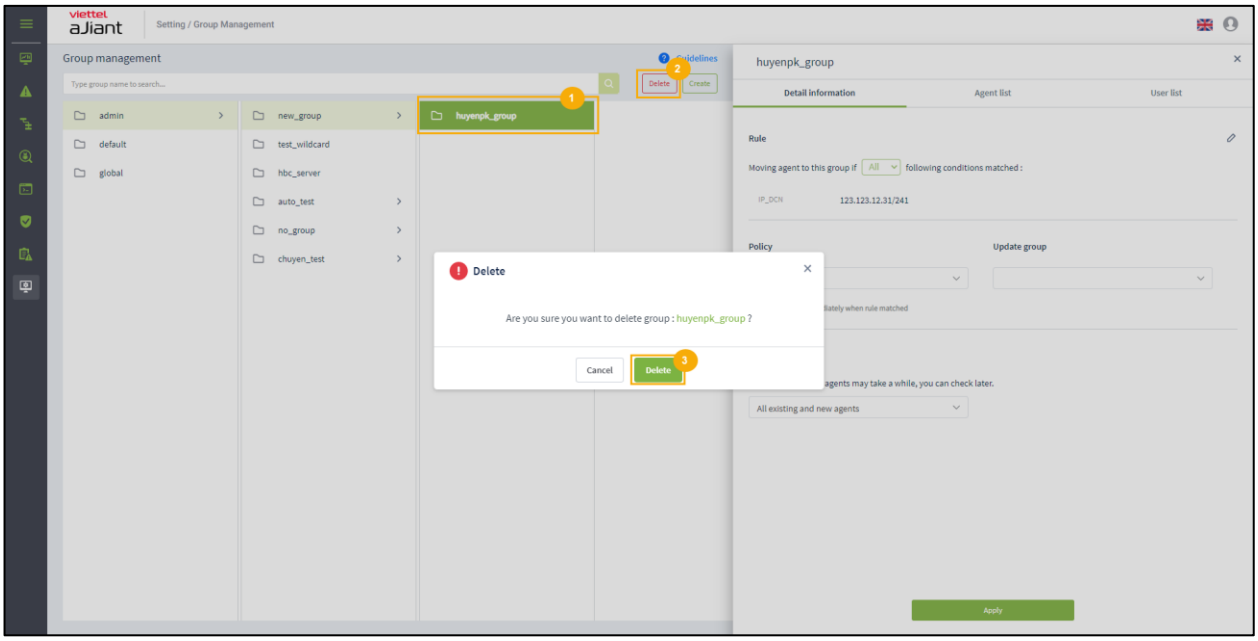
User logged in as root group: Can delete all groups in the system;

User login belongs to the default group: The default group cannot be deleted;

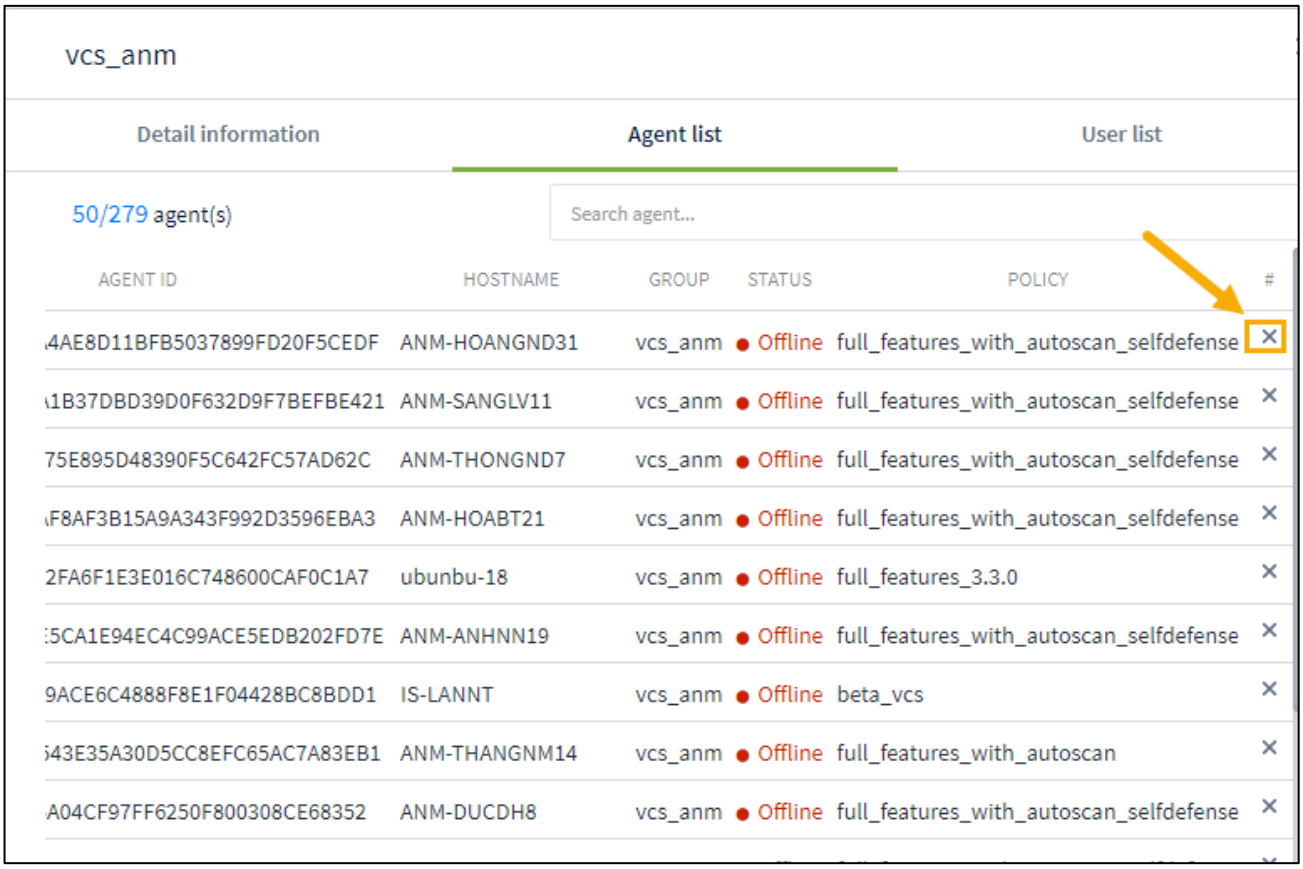
User logged in belongs to parent group: Can delete all groups currently logged in and child groups whose roles also belong to the child role group of the logged-in user's role;

User logged in belongs to one or multiple subgroups: It is possible to delete all groups associated with the logged-in user;

To delete a group, click on the group you want to delete, then click "Delete" and confirm by clicking "OK" on the confirmation screen. After deleting a group, the agents belonging to that group will be moved to the default group, "default," while the policy remains unchanged.



To remove an Agent from the group, click on the Agent list tab, then click the "x" icon to delete the agent from the group. After removal, the agent will be moved to the default group: "default," with the policy remaining unchanged.



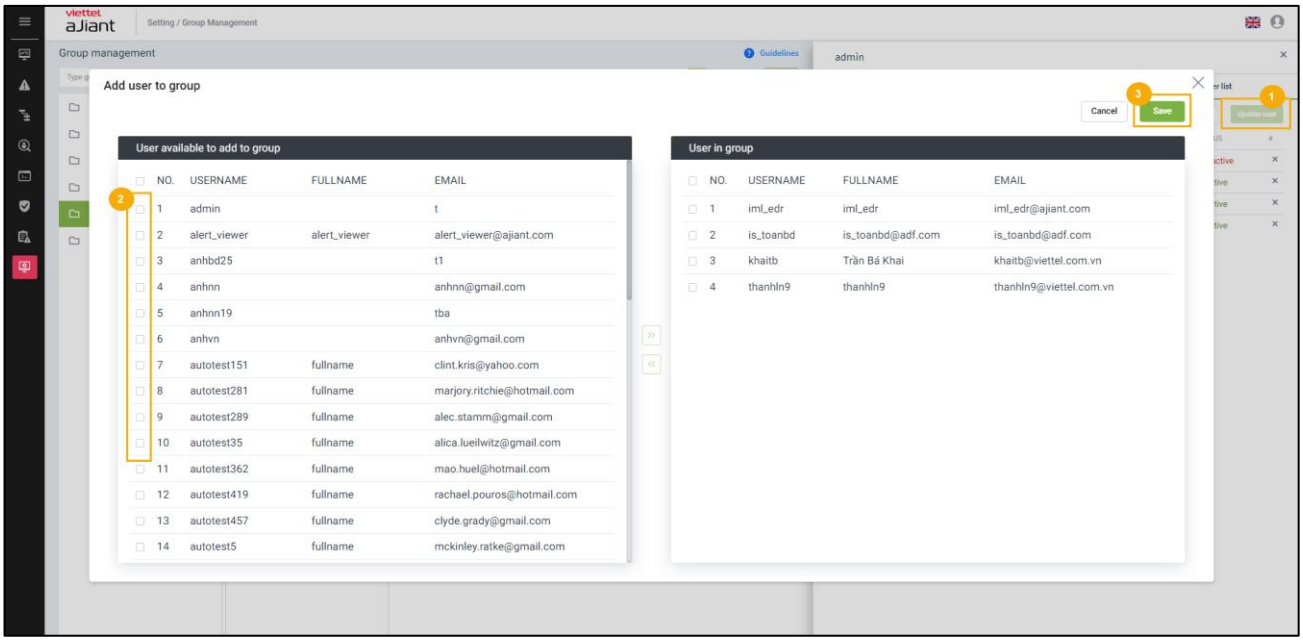
Note: in the case of deleting a parent group:

Delete all subgroups;

Move all agents from the parent group and subgroups to the default group: "default";

Keep the policies of the agents in both the parent and child groups unchanged;

6 – Add a new user to the group



User list:

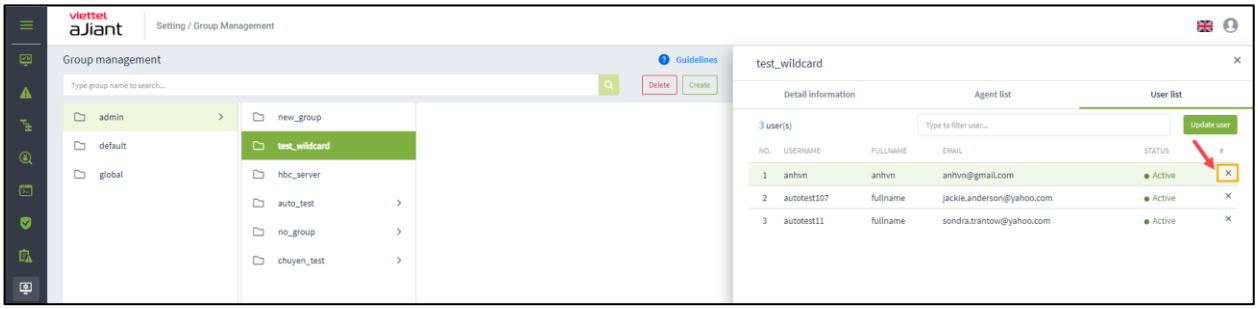
User logged in as root group: Display all users in the system;

User login belongs to default group: Display users belonging only to default;

User login belongs to parent group: Display the currently logged-in user and users belonging to child groups who have roles also within the child group roles of the logged-in user's role;

User login belongs to one or more subgroups: Display the currently logged-in user:

7 – Delete user



3.6.4 Account Management

Manage accounts, permissions, and permission groups of the Portal system.

Permission management

Manage access rights to the system's resources (APIs). One permission corresponds to access to a specific resource (API) of the system;
The main functions on this screen are:

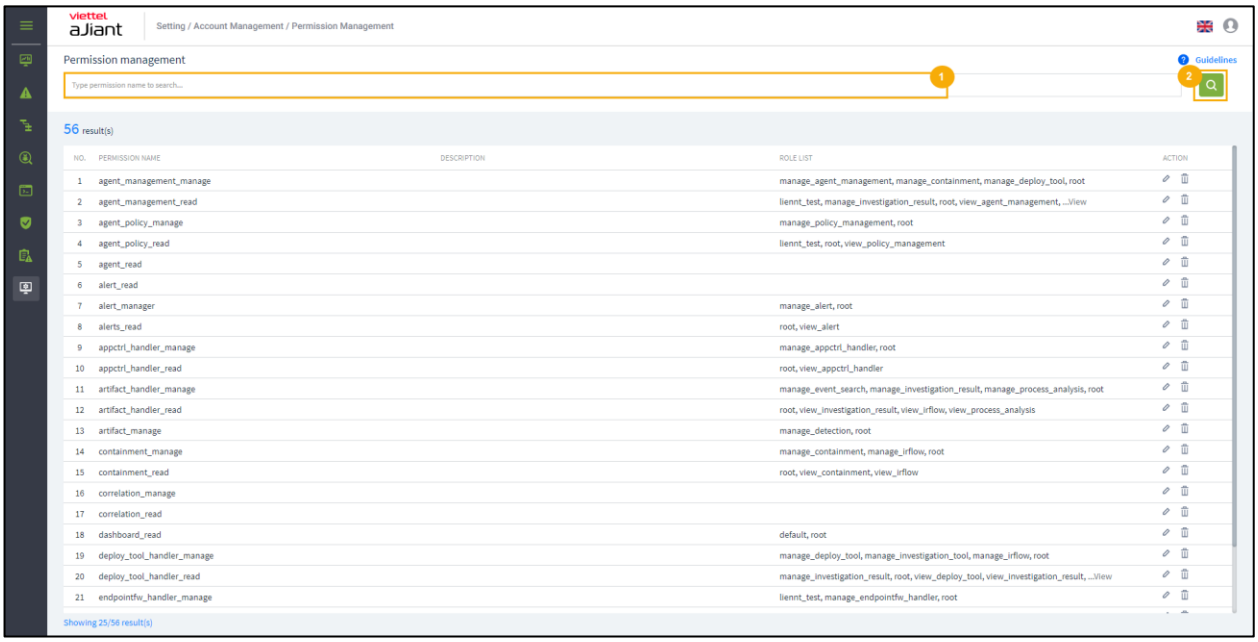
Manage permissions;

Search for permission;

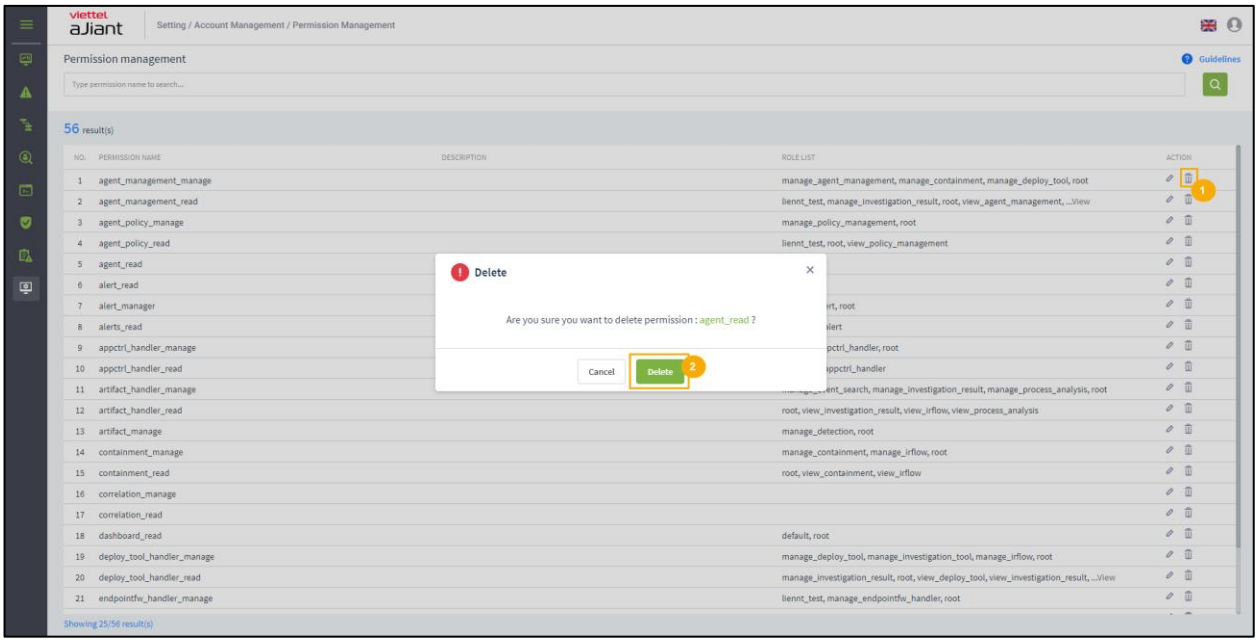
Delete permission;

1 – Manage permissions: display all system permissions. If a permission is deleted on this screen, and a function on the portal requires that missing permission, the deleted permission will be automatically restored in the Permission management screen.

2 – Search for permission: enter search characters into the Search textbox > press Enter or click the “Search” button => display the list of matching permissions.



3 – To delete permission: click the “Delete” icon > click “OK” on the confirmation screen to successfully delete.



Role management

Manage the system roles (permission groups or permission sets);
The functions on this screen include:

Role list management:

- User logged in with root Role: Display all Roles in the system;
- User login belongs to default Role: Display default Role;
- User login under parent Role: Display all Roles belonging to the logged-in user and the corresponding child groups;
- User login belongs to a Role that has one or more child roles: Display all Roles that belong to the user's current Role.

Search for role;

Add new role;

Delete role.

1 – Role list management: manage the role list in a tree structure. There are 2 default root roles pre-created: the "default" role and the "root" role.

Role “default”: Users with the “default” role only have access to the Portal and do not have permission to view data or perform any functions;

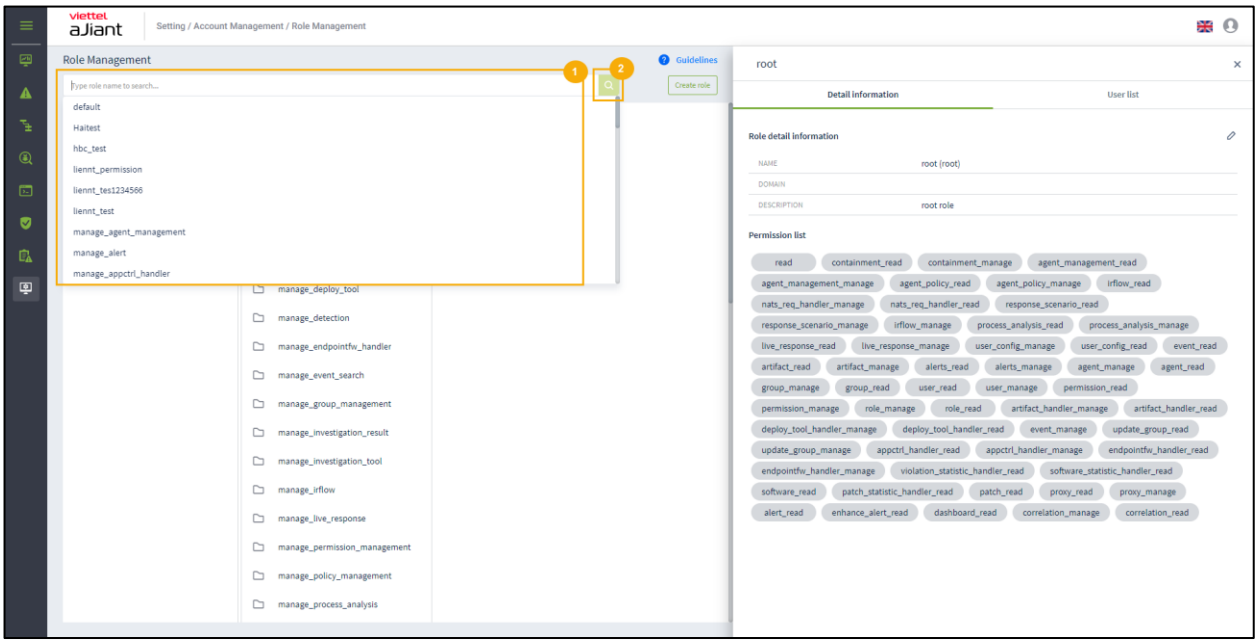
Role “root”: includes all system roles. A user with the “root” role has full access to all functions on the Portal;

Clicking on a role will display detailed information about the role. A role includes the following information: role name, list of permissions, list of users (accounts) assigned to the role, parent role, or list of child roles (if any).

2 – Search for role

Method 1: Click on the Search textbox > a list of roles in the system will be displayed and can be scrolled > Select a role from the displayed list.

Method 2: Click on the Search textbox > Enter the search characters into the textbox > The system filters roles containing the search characters > select a role from the filtered list or press Enter or click the “Search” button.



- Double-clicking on a record will display the detailed information of that record.

- The detailed information tab displayed is Detail, with the role data including the role information and the permissions associated with that role.
- When selecting the User list tab, it displays the list of Users along with their roles;

When right-clicking on a record, "Go to role" will be displayed. Clicking on "Go to role" will return to the original tree-form role list.

When clicking on the menu in the top right corner of each record, the option "Go to role" is also displayed;

3 – Add new role:

User logged in as root group: Can add all roles in the data trees;

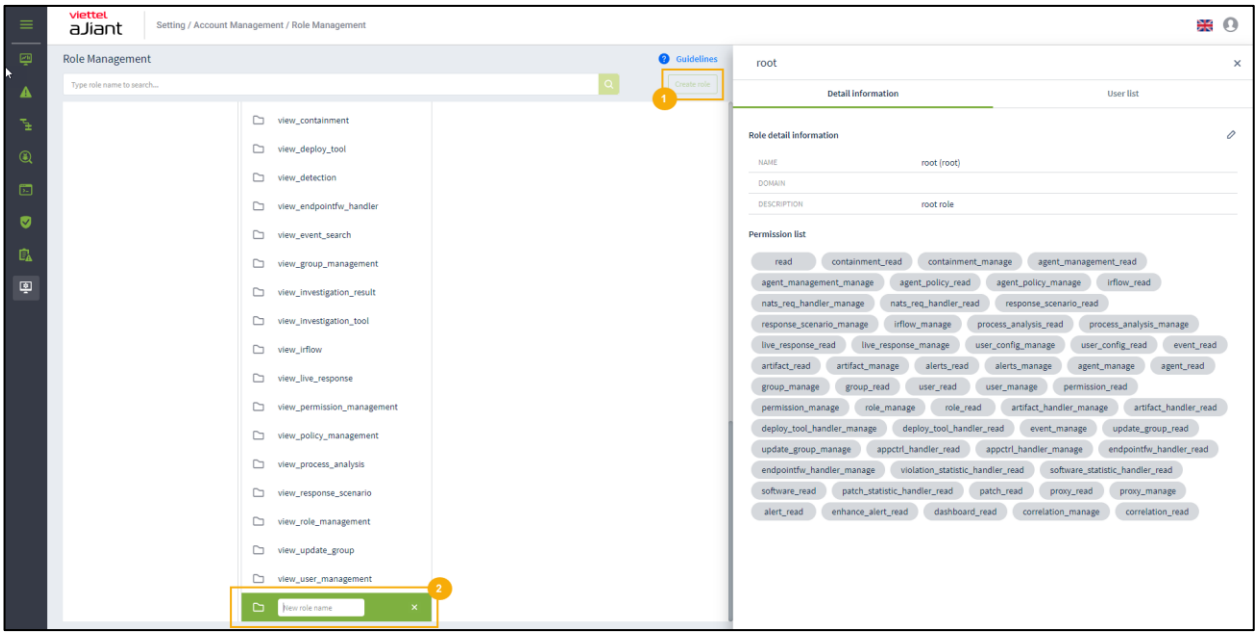
User login belongs to default group: Cannot add new;

User logged in belongs to parent group: Can add new child roles corresponding to the user's group, but cannot add new roles at the same level;

A user logged into one or more sub-groups: can add new sub-groups corresponding to the groups the user belongs to.

- There are the following methods to create a new role:

Click on a role, then hover at the end of the role list and select "Add new" to create a role at the same level as the selected role.
Click “Add new” on the screen to create a sub-role of the selected role.
Right-click on a column in the tree and select "Add new role".
Then enter a role name that does not duplicate any existing role name in the system.



- Click the Edit icon to add permission information for the role > Select the permissions to add to the role > click Save:

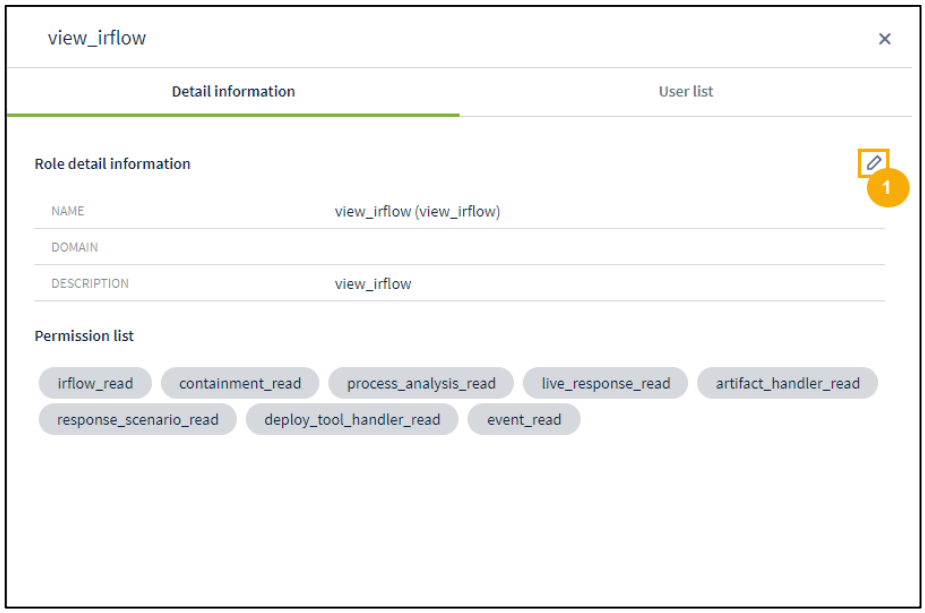
User logged in as root group: Can modify all roles in the system;

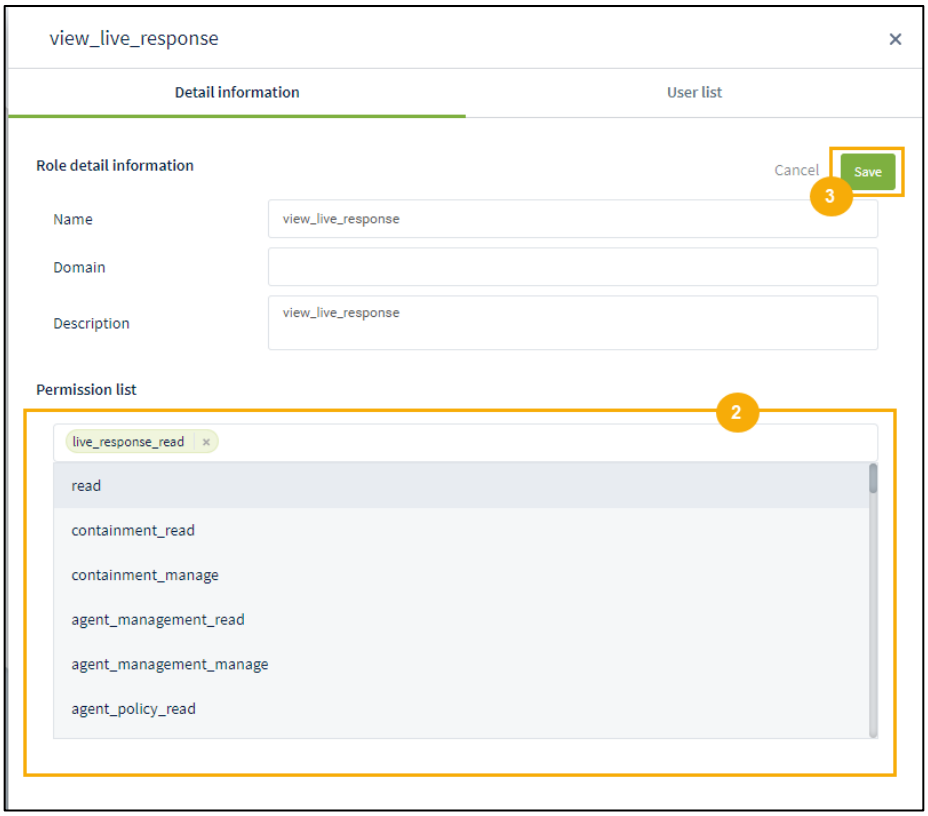
User login belongs to the default group: Default role cannot be modified;

User logged in under parent group: Can modify all roles belonging to the logged-in role and its child roles;

User logged in belongs to one or multiple sub-groups: Can modify all roles associated with the logged-in user;

Note: The permission list of the child role is a subset of the parent role's permissions. This means that when selecting permissions to assign to the child role, those permissions must be included in the parent role's permission list.





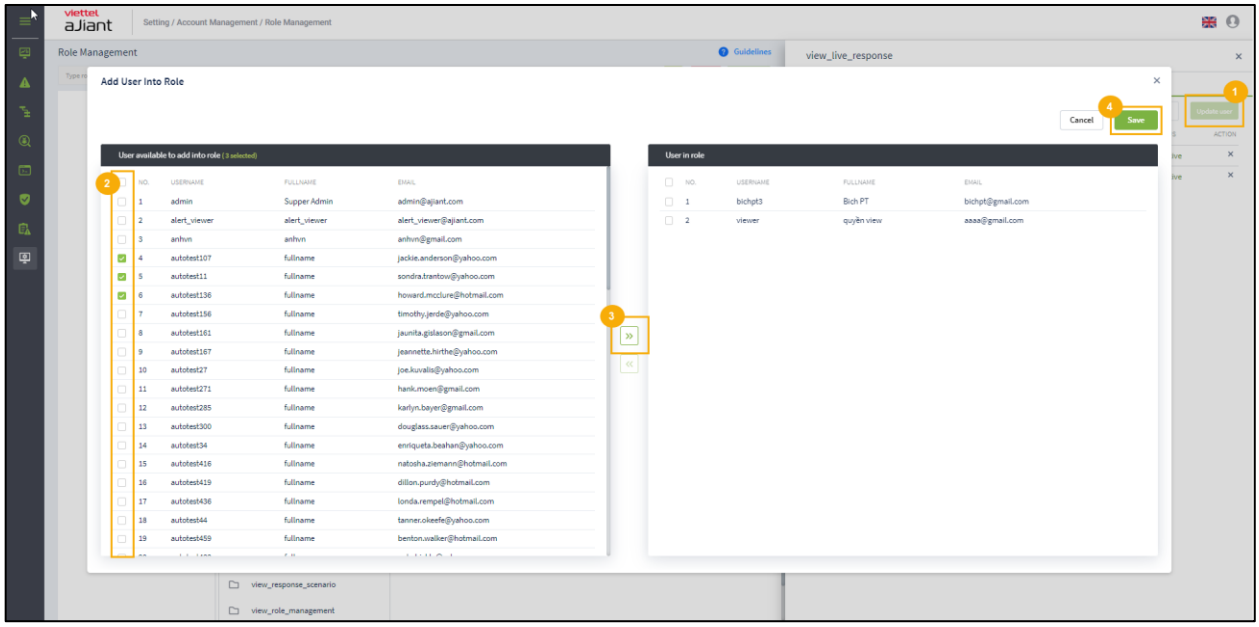
- Switch to the User list tab to add a role to the User's role list.

User logged in as root group: Display all Users in the system;

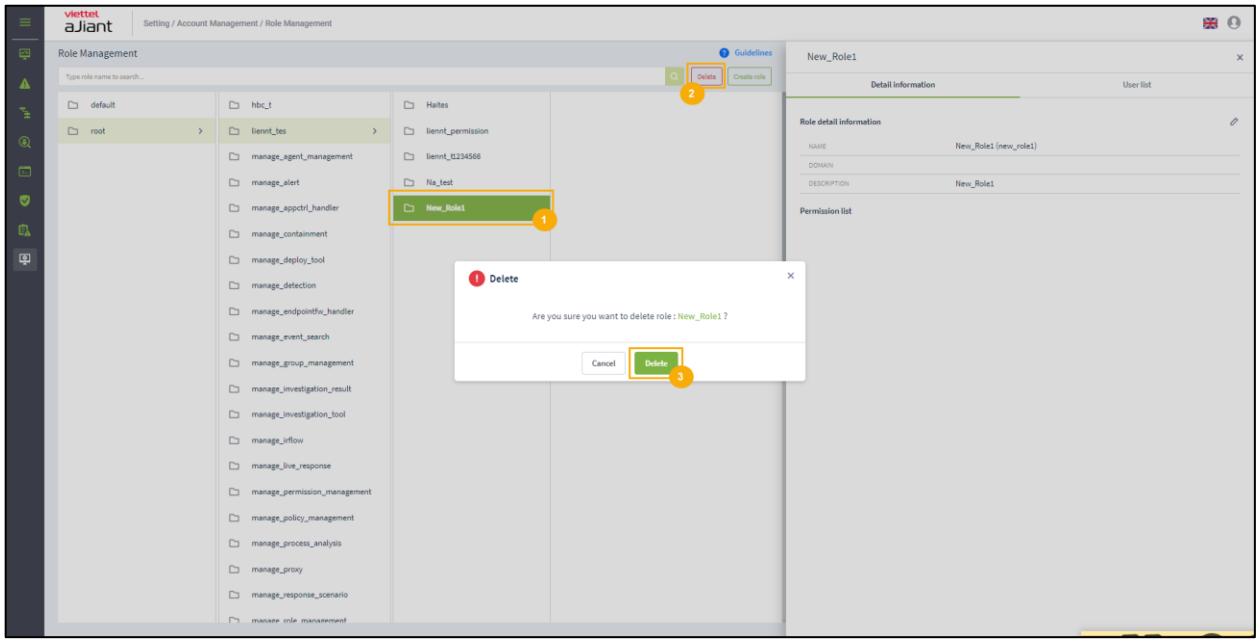
User login belongs to default group: Display users belonging only to default;

User login belongs to parent group: Display the currently logged-in user and users belonging to child groups who have roles that are also part of the child group roles of the logged-in user's role.

User logged in belonging to one or more subgroups: Display the currently logged-in user;



4 – Delete role: click on the role you want to delete, select “Delete” > click OK on the confirmation screen.



Note: After deleting a role, all users assigned to that role will be updated as follows: If user X belongs to the deleted role and has only that one role, user X will be assigned to the default role. Conversely, if user X has multiple roles, only the deleted role will be removed from user X's list of roles.

User management

Manage the accounts logging into the VCS-aJiant Portal system.
The main functions on this screen include:

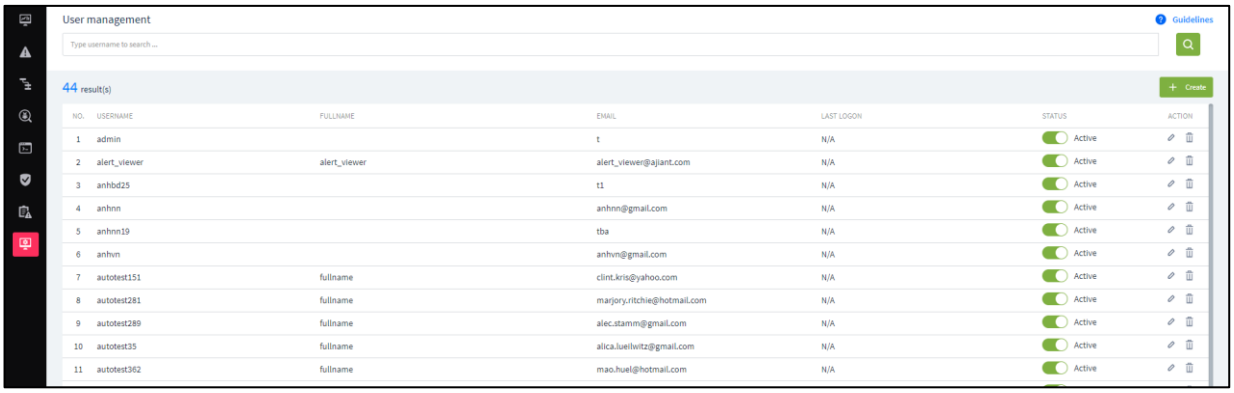
Search account;

Add new account;

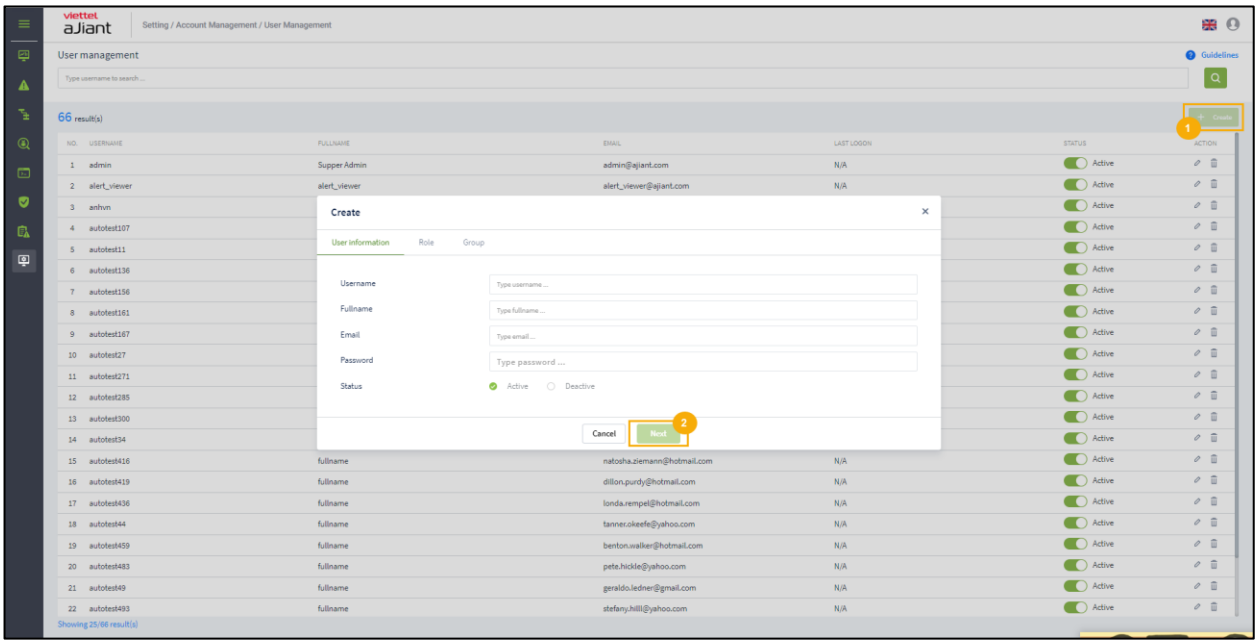
Edit account;

Delete account;

1 – Search for an account: click on the Search textbox > a list of accounts in the system will appear > select the desired account from the list or enter the characters <text> into the textbox to filter the accounts > click “Search” or select the desired account from the filtered list.



Add a new account: click “Create” > Enter information in the displayed form > click “Next”

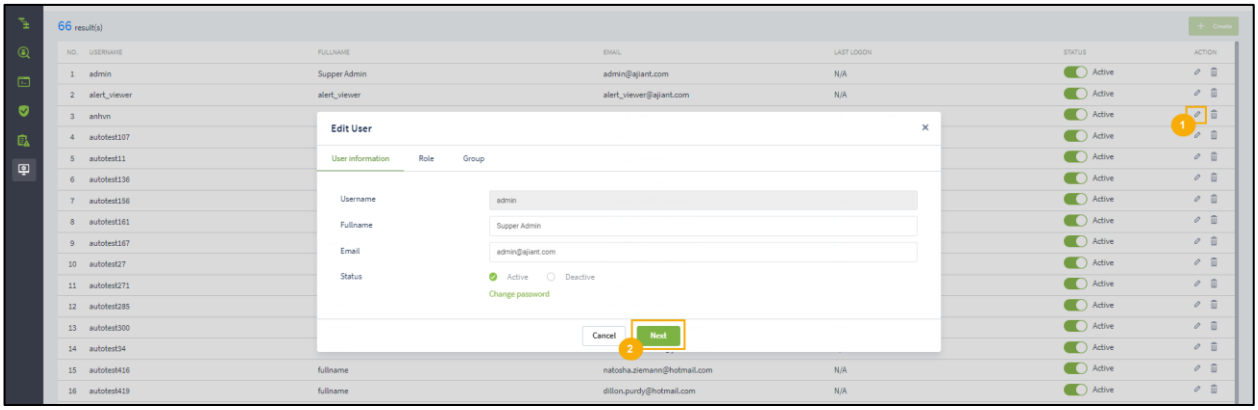


Select the role (permission group) to assign to the account, then click “next”;

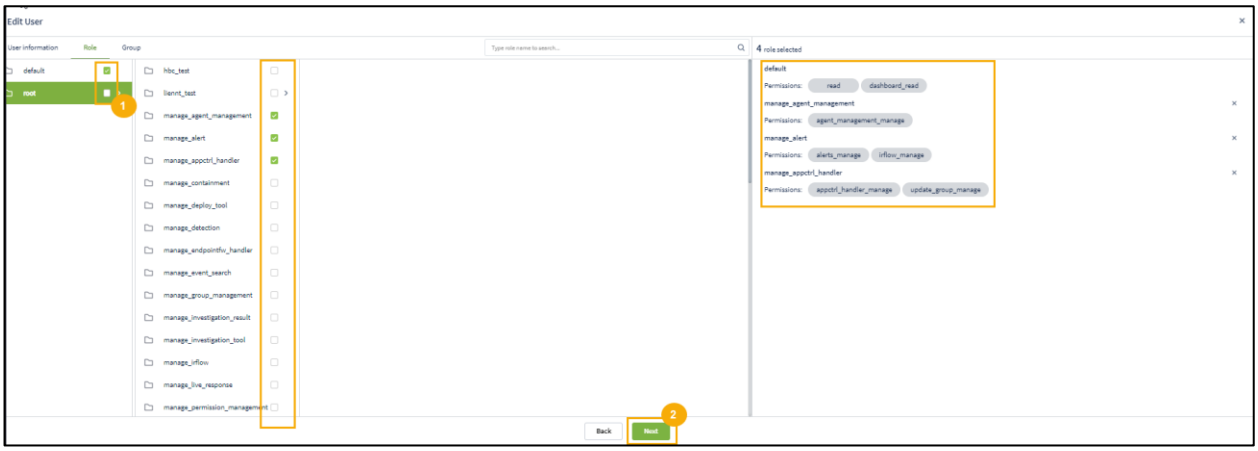
When clicking on the checkbox for each role, the corresponding permissions for that role will be displayed:

- User logged in with root Role: Display all Roles in the system;
- User login belongs to default Role: Display default Role;
- User login under parent Role: Display all Roles belonging to the currently logged-in user and the corresponding child groups;

- User login belongs to a Role that has one or more child roles: Display all Roles belonging to the user's current Role.



On the Add Role to User screen, you can search for roles similarly to how you search for accounts. After entering search characters into the "Search" textbox, click the Search icon or press Enter to display a list of roles that meet the search criteria.



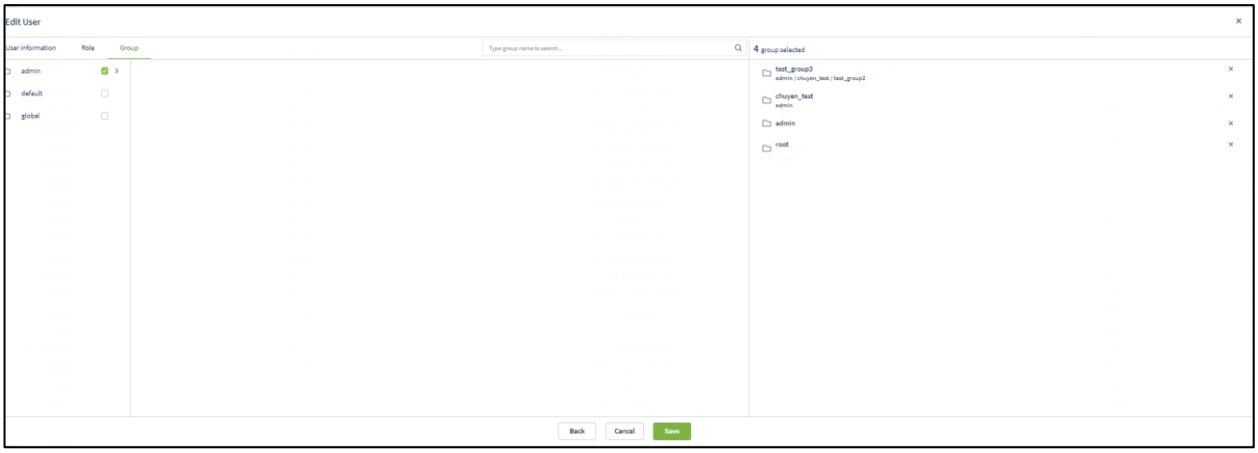
Click the checkbox corresponding to the role to be added, then click "Go to role" to return to the initial role list screen, and then click "Create" to create the account;

Note: The currently logged-in account can only create new accounts with roles that are sub-roles within the list of roles assigned to the logged-in account.

Select the group to assign to the account, then click "Create";

When clicking on the checkbox for each role, the corresponding permissions for that role will be displayed.

- User logged in as root group: Display all Groups in the system;
- User login belongs to default group: Display default group;
- User login belongs to parent group: Display groups belonging to the logged-in user's group and the corresponding child groups;
- User login belongs to one or more subgroups: Display all groups that belong to the user's group currently logged in;



Click the checkbox corresponding to the group you want to add, then click "Go to role" to return to the initial group list screen, and finally click "Create" to create the account.

Delete account: click on the Delete icon, then click OK on the confirmation screen.

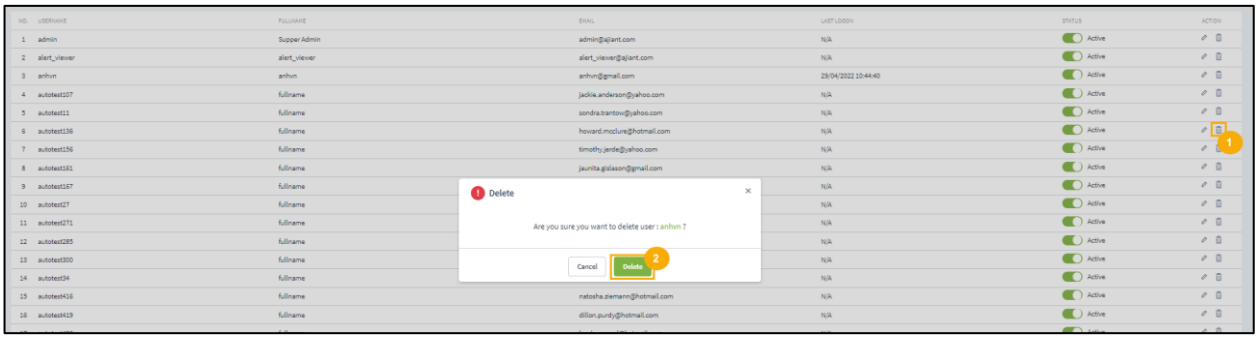
Check the display of the delete icon:

User logged in as root group: Display all Users in the system;

User login belongs to default group: Display users belonging only to default;

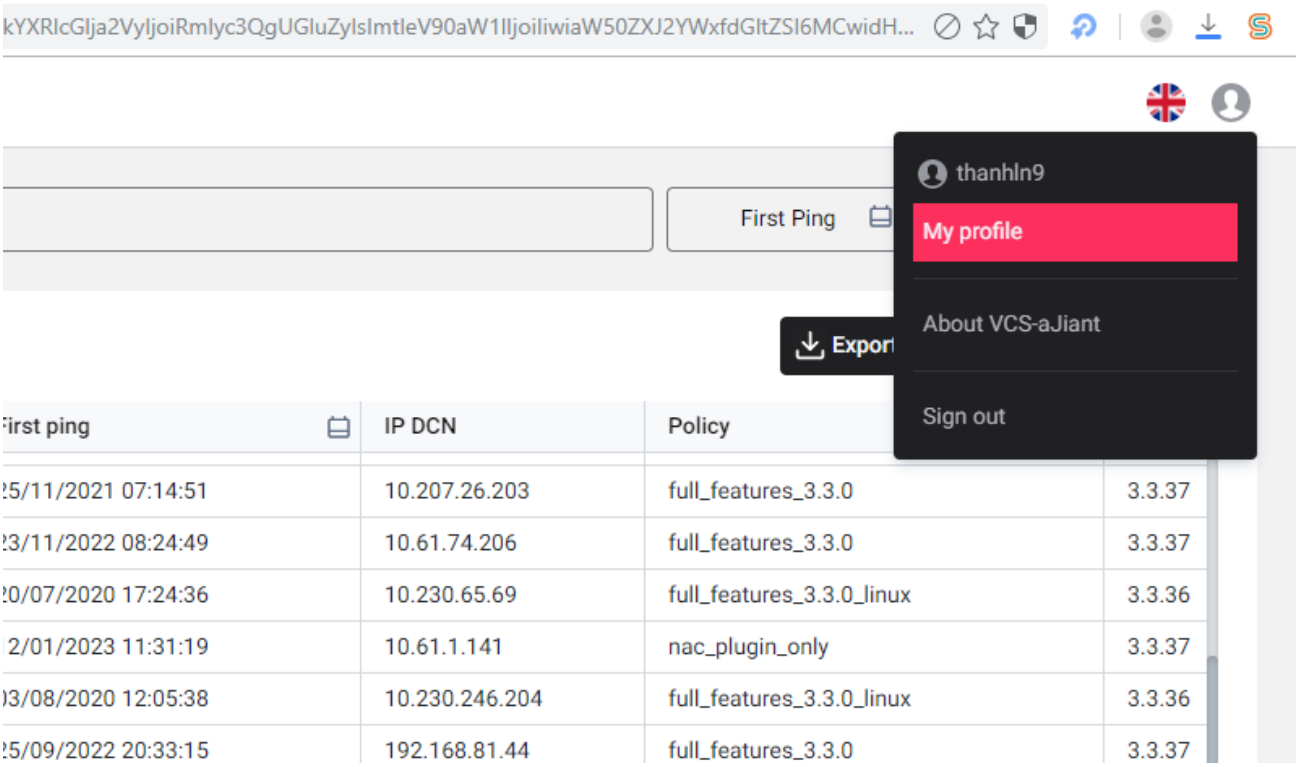
User login belongs to parent group: Display the currently logged-in user and users belonging to child groups who have roles that also belong to the child role group of the logged-in user's role;

User logged in belongs to one or more subgroups: Display the currently logged-in user;

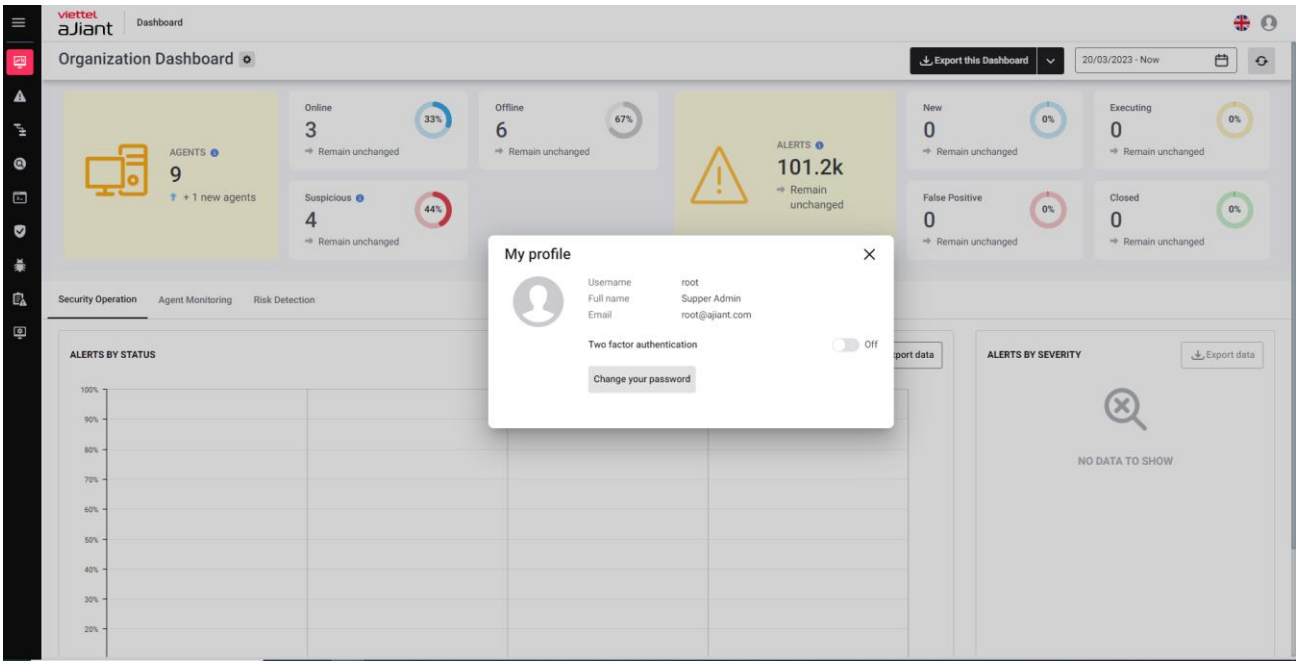


Enable two-factor authentication for the account:

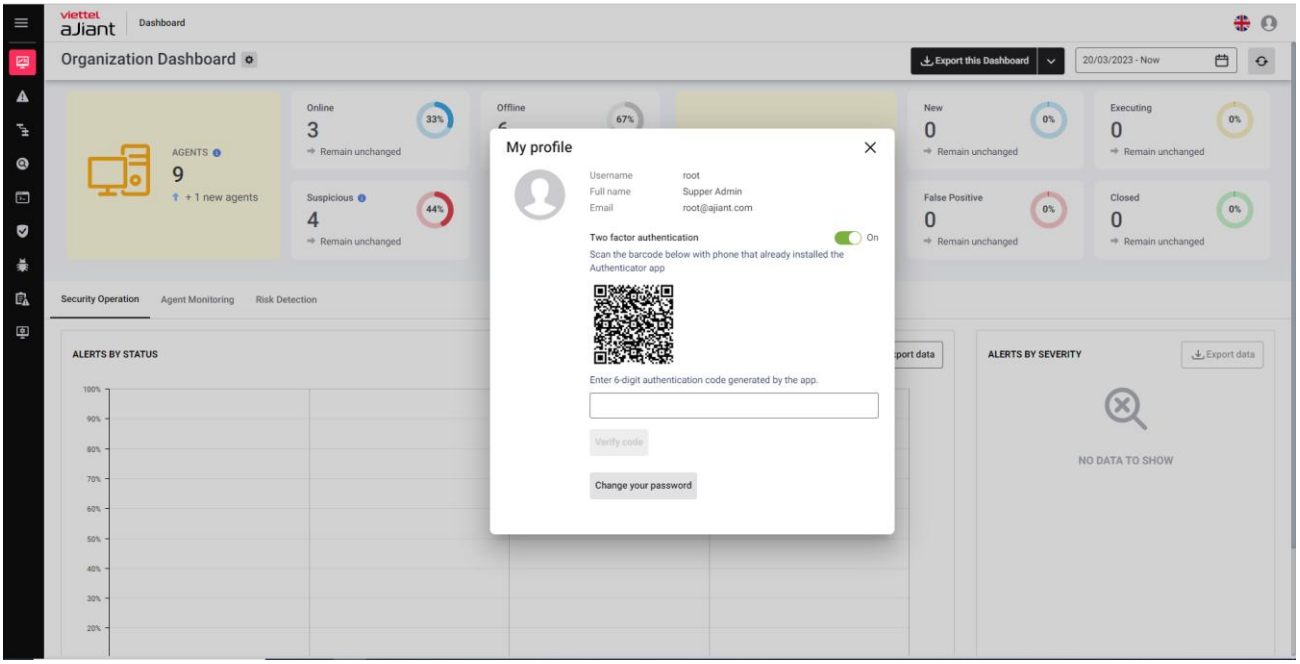
Step 1: Go to the My Profile interface as shown in the image below.



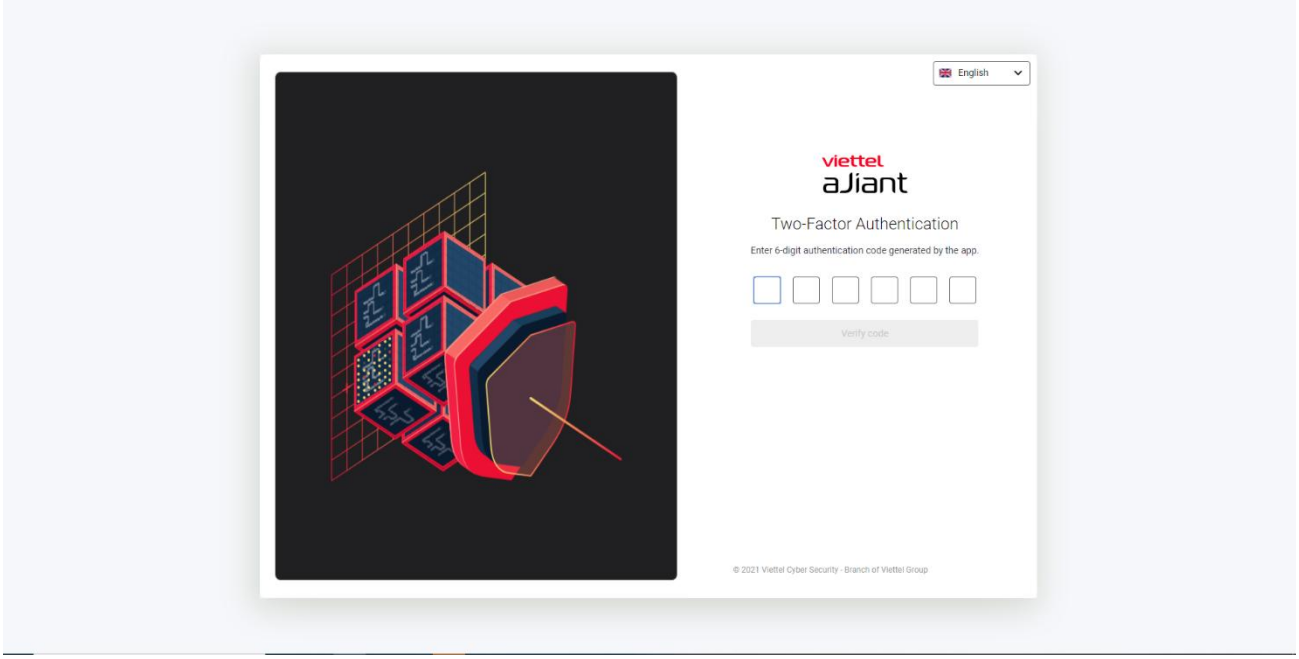
Step 2: Click to enable Two-Factor Authentication.



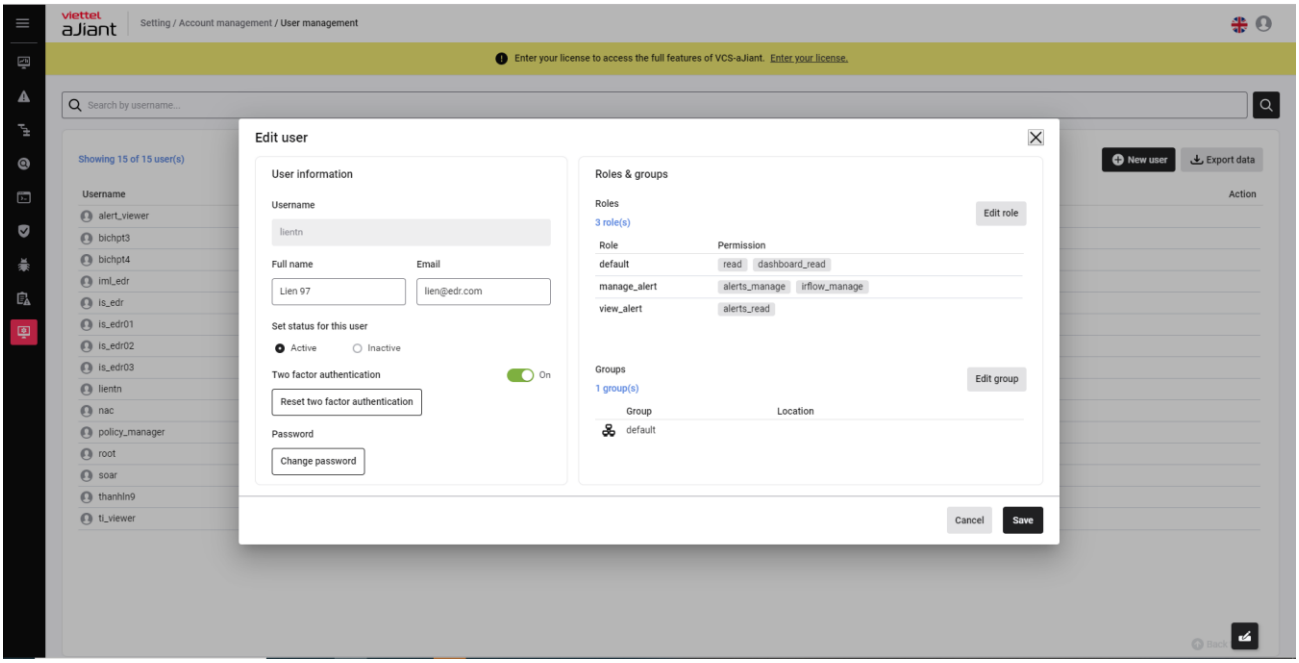
Step 3: Use a 2FA app to scan the QR code, then enter the OTP to complete the 2FA activation process.



After enabling 2FA, users will be required to enter an OTP when logging in, as shown in the image below.



You can enable 2FA for other users as shown in the image below.



The solution also supports force enabling 2FA for all accounts.

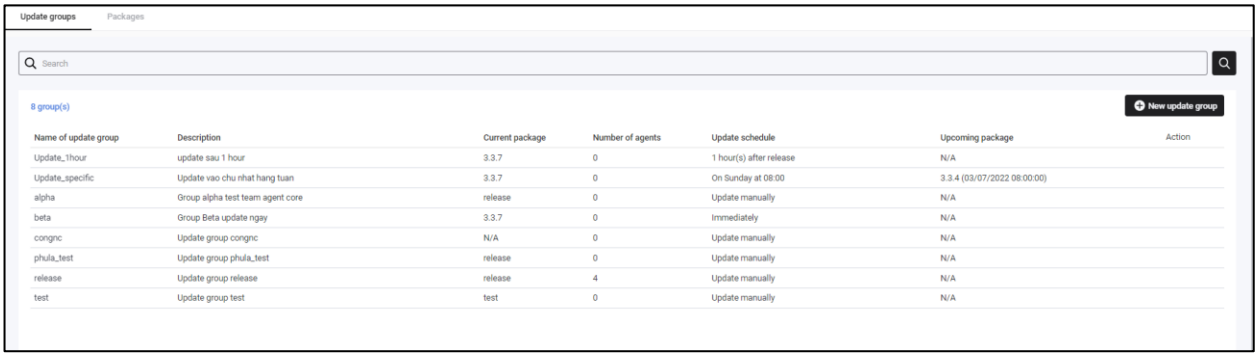
3.6.5 *Update management*

Update group

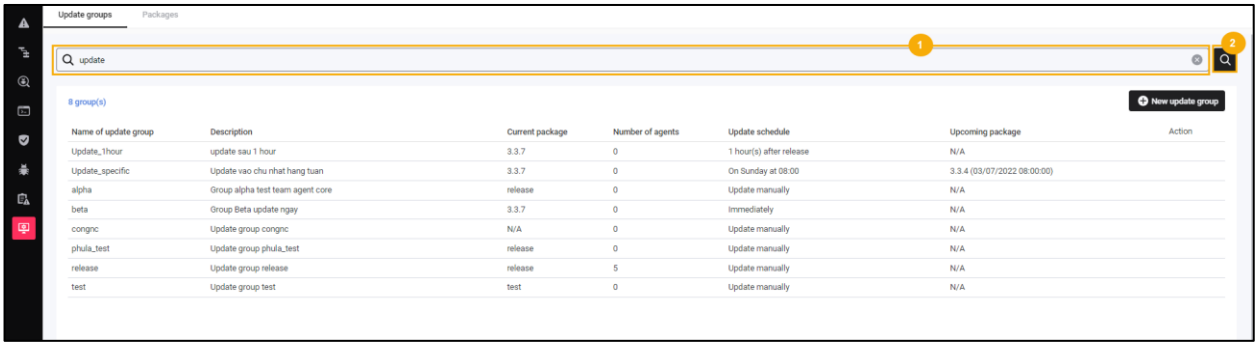
Purpose: This feature allows for the management, creation, and updating of Update Groups (dividing Agents into update groups to facilitate easier allocation and management).

1 – Search:

- Log in to the Portal using the provided account credentials;
- Select Settings, the system will display the sub-menus: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- Select Update Management, the system displays the list of Update Groups;



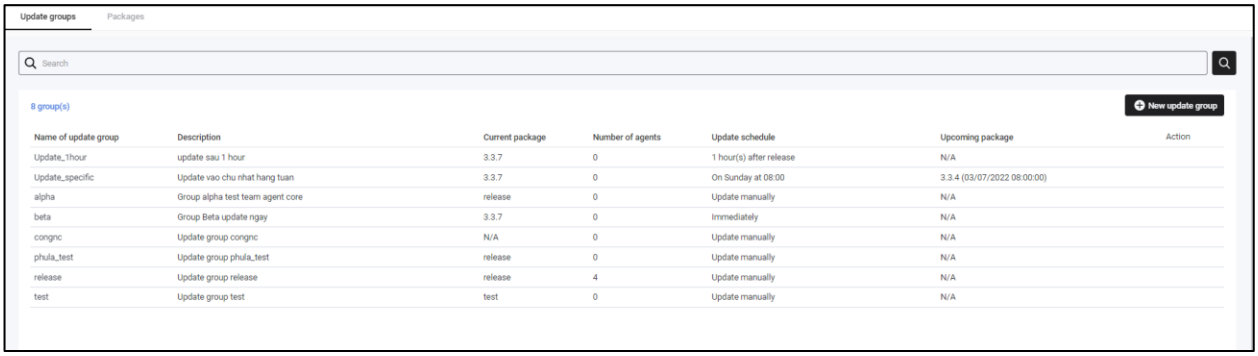
- Select Update Management, the system displays the list of Update Groups;
- Enter the search keyword into the textbox and click the "Search" button.



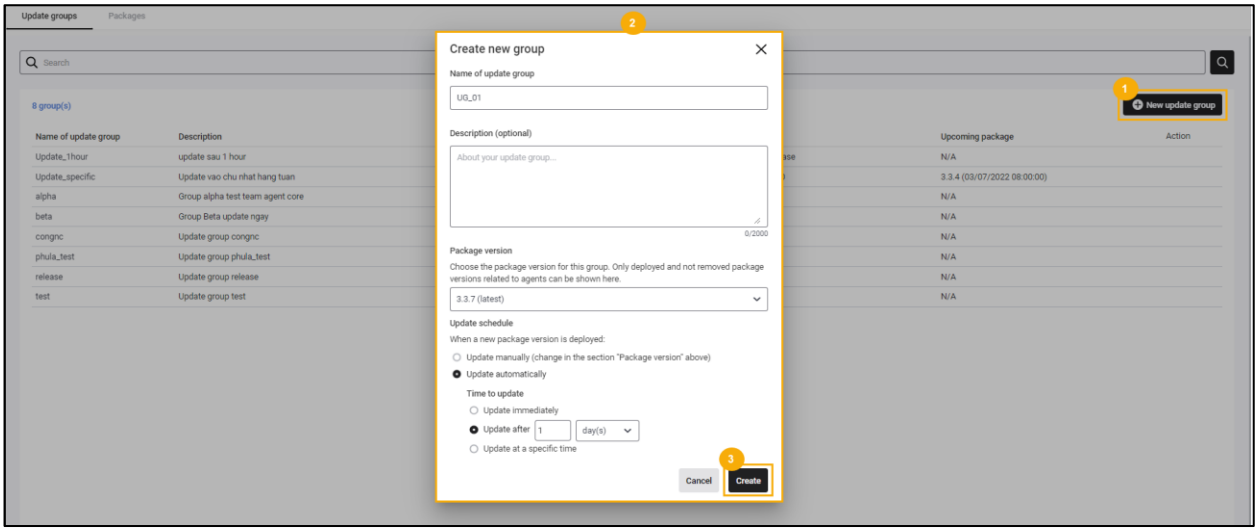
2 – Add new Update groups:

- Log in to the Portal using the provided account credentials;

- Select Settings, the system will display the sub-menus: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- Select Update Management, the system displays the list of Update Groups;



- Select the "New update group" button, the system will display the Add New Update Group screen;

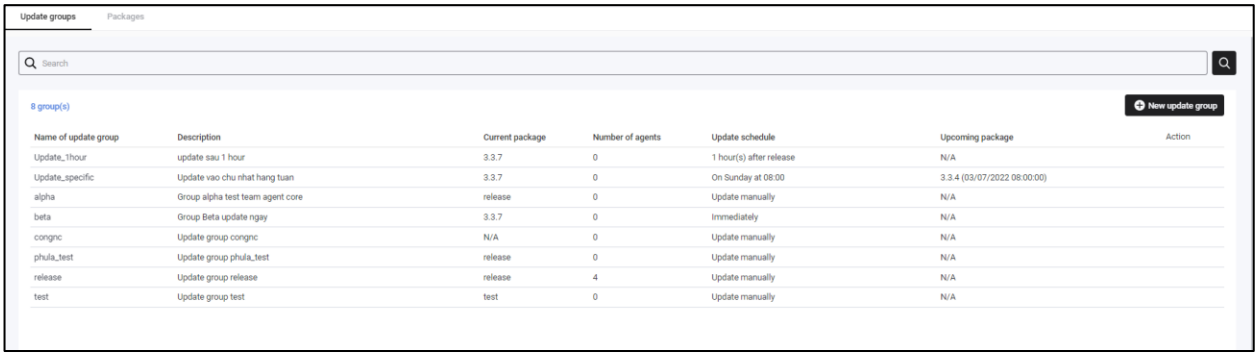


- Enter the new Update Group information and select the "Create" button. The system will save the data and return to the Update Group list screen.

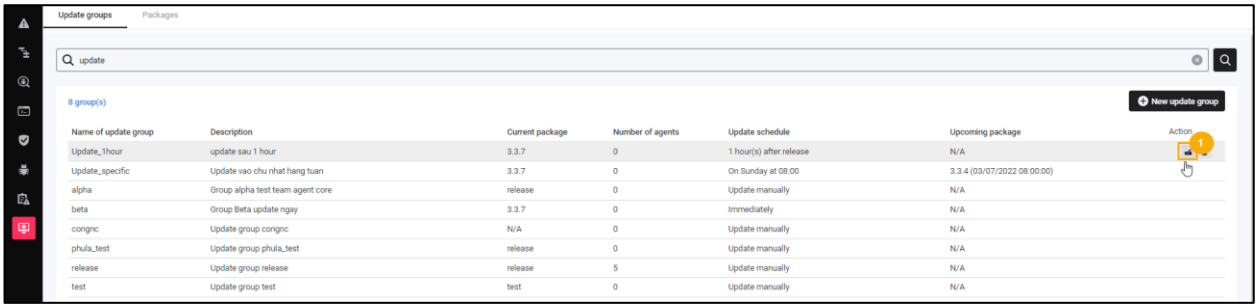
3 – Update groups:

- Log in to the Portal using the provided account credentials;

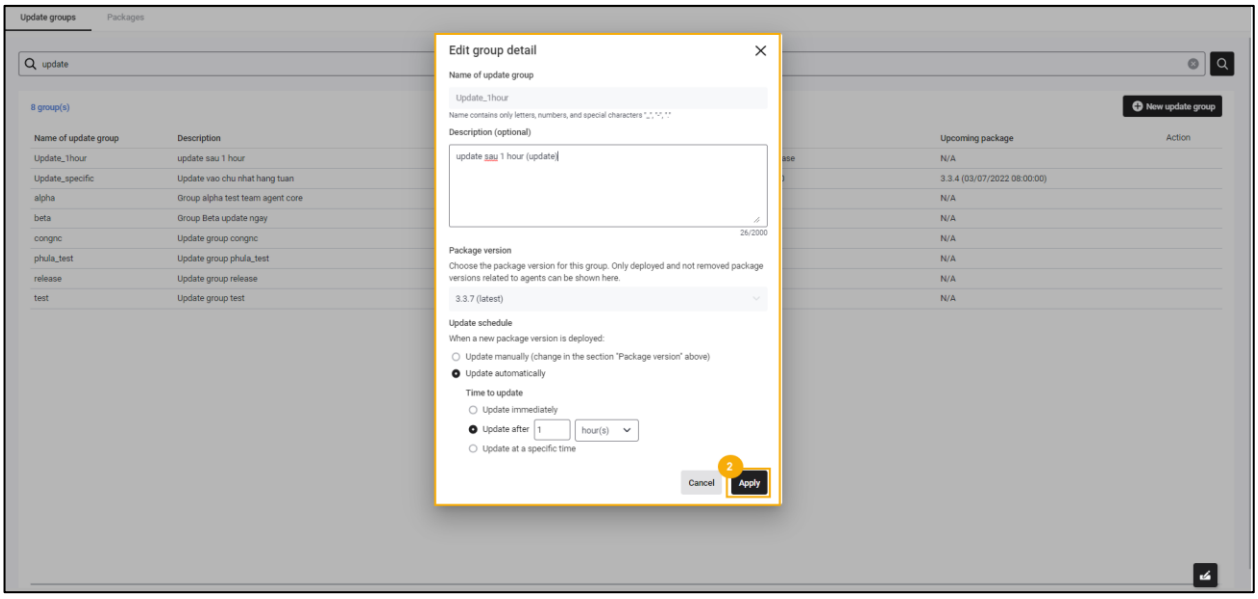
- Select Settings, the system will display the sub-menus: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- Select Update Management, the system displays the list of Update Groups;



- At the record where information needs to be updated/edited, select the "Update" icon to update the Group information:

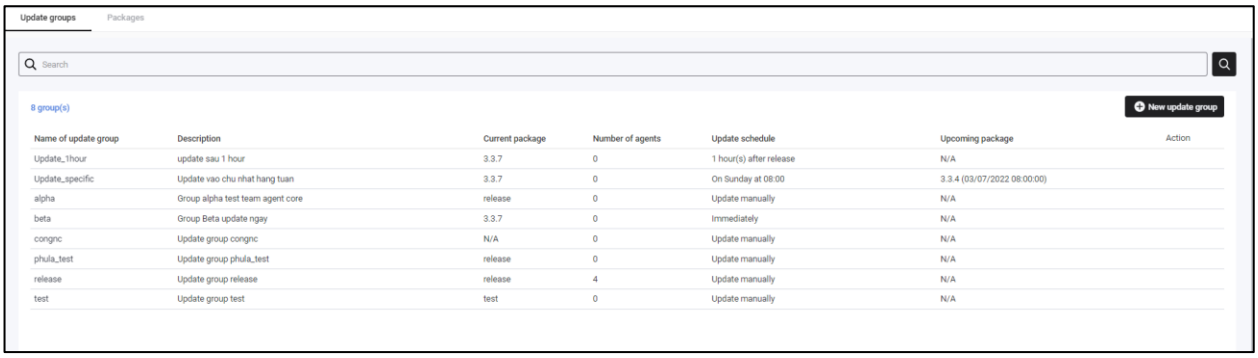


- The system displays the detailed information screen for Update Group, allowing updates/edits to the information and saving by selecting the "Apply" button:

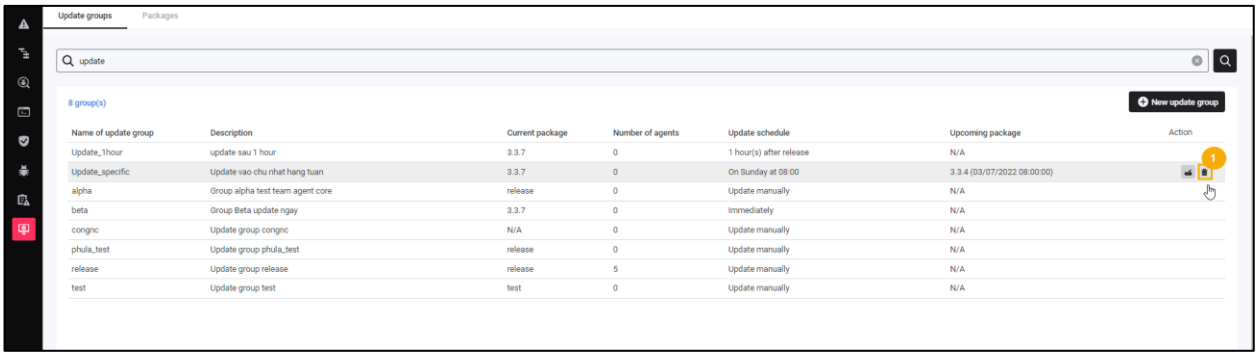


4 – Delete Update groups:

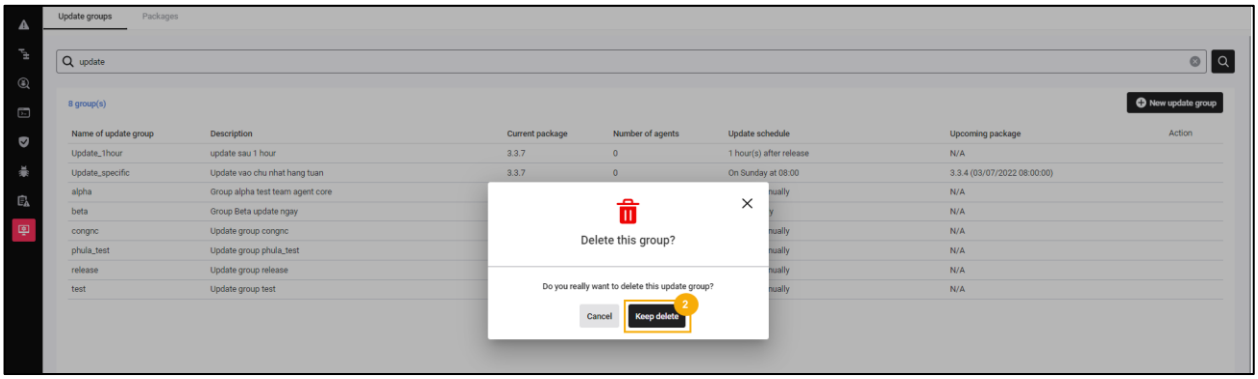
- Log in to the Portal using the provided account credentials;
- Select Settings, the system will display the sub-menus: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- Select Update Management, the system displays the list of Update Groups;



- At the record to be deleted, select the "Delete" icon Update Group:



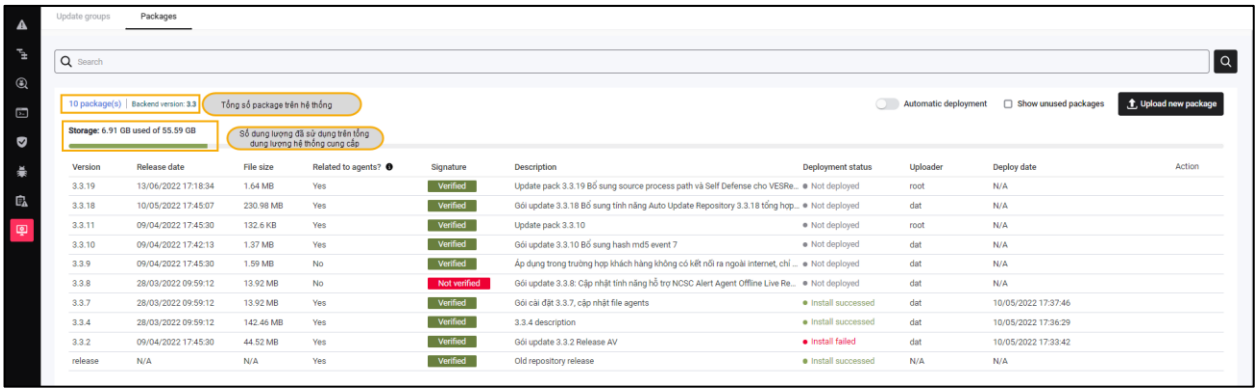
- The system displays a Delete Update Group confirmation popup. The user selects the "Delete" button to confirm the Delete Update Group request or selects the "Cancel" button to cancel the Delete Update Group request.



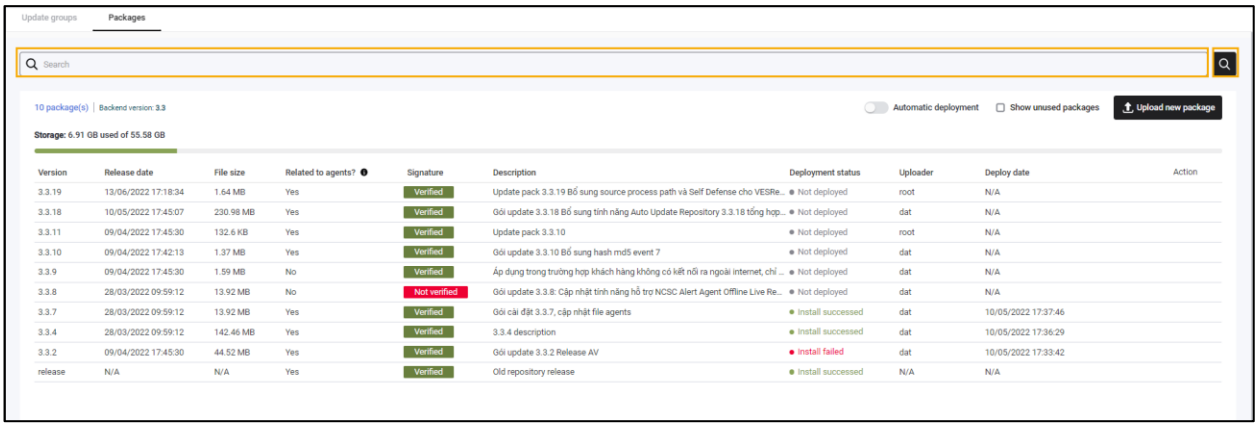
Packages update

1 – Searching for packages:

- Log in to the Portal using the provided account credentials;
- Select Settings, the system displays the sub-menus: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- Select Update Management, the system displays the list of Update Groups;
- Select the "Package" tab, the system will display the list of Packages in the system;



- Enter the search keyword into the textbox and click the "Search" button.



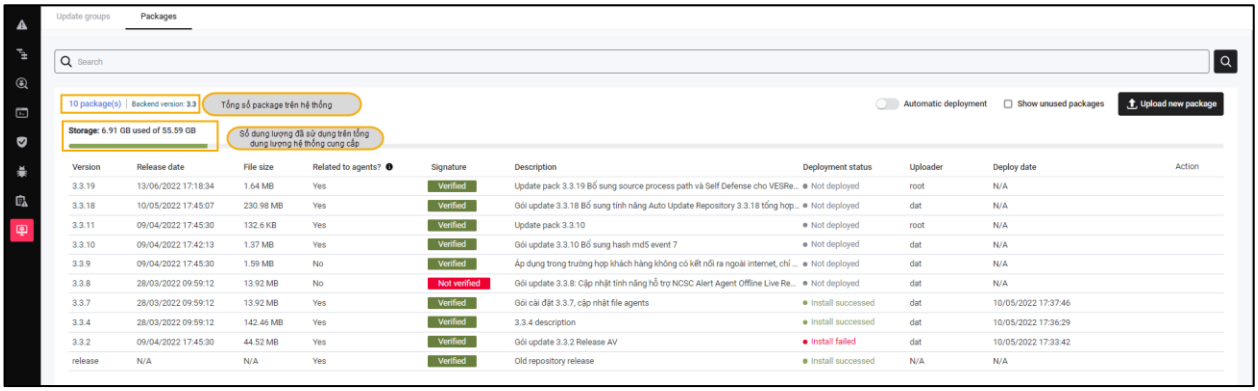
2 – Automation update

Purpose: This feature allows for the automatic deployment of updates to customers quickly and efficiently. Auto Update enables uploading packages through the portal interface or automatically retrieving updates from the hub.viettelcybersecurity.com website.

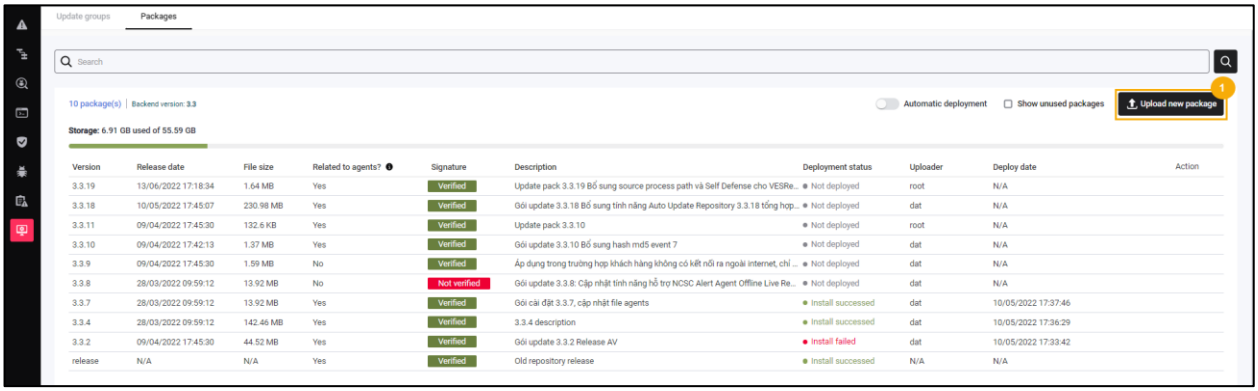
Note: The deployment team should resend the above information to the Ajiant project team for updating in the system to enable automatic package deployment at the customer site. In the future, when a new update package needs to be deployed, the deployment team or the customer only needs to obtain the provided update package, upload it to the Ajiant portal, and select to deploy the package.

- Log in to the Portal using the provided account credentials;

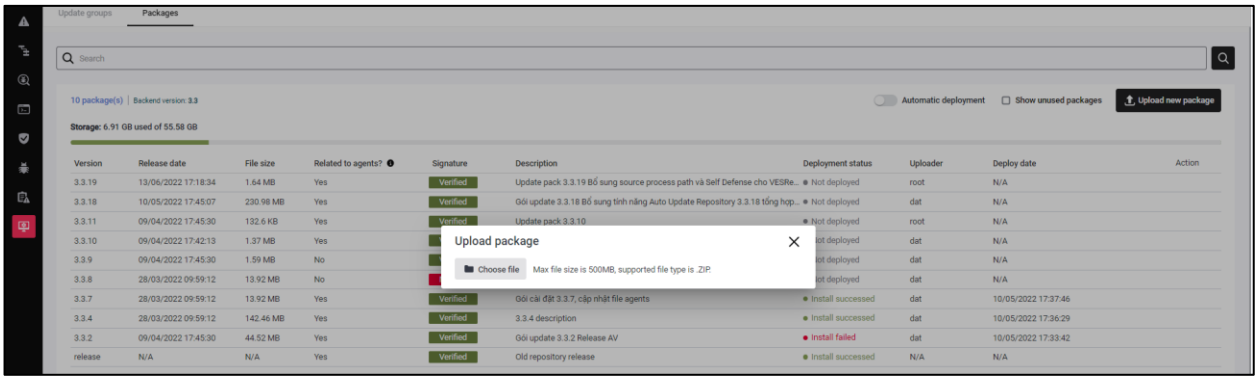
- Select Settings, the system will display the sub-menus: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- Select Update Management, the system displays the list of Update Groups;
- Select the "Package" tab, the system will display the list of Packages in the system;



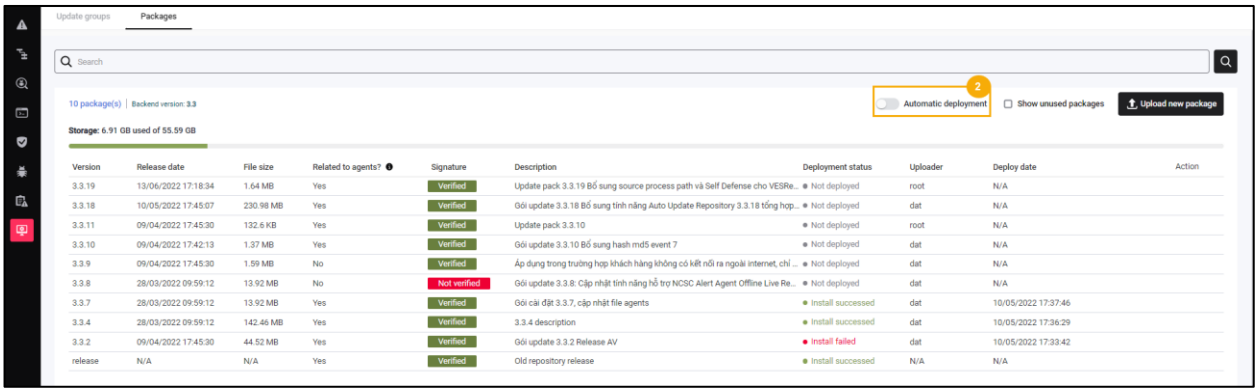
- Select the "Update new package" button, the system will display the "Upload package" popup;



- Select upload package;

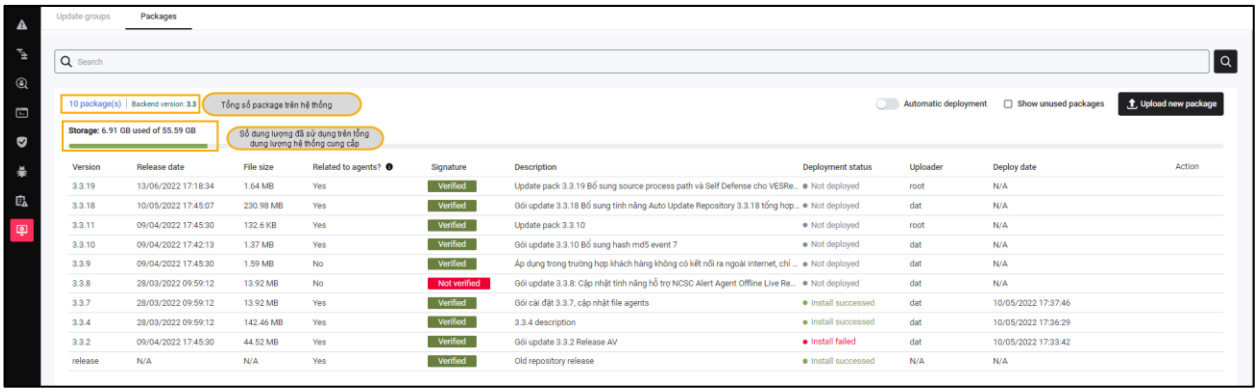


- Enable/Disable the "Automatic Development" action to automatically deploy package updates to customers.

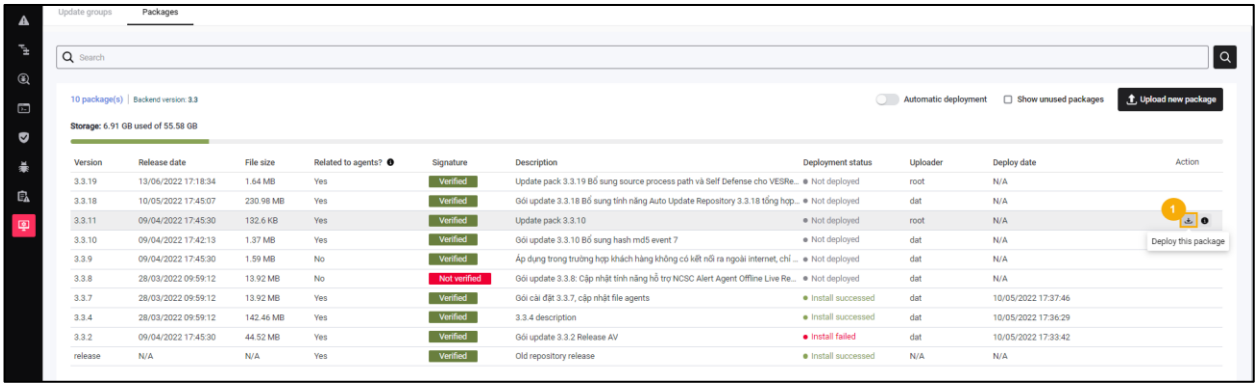


3 – Deploy a package

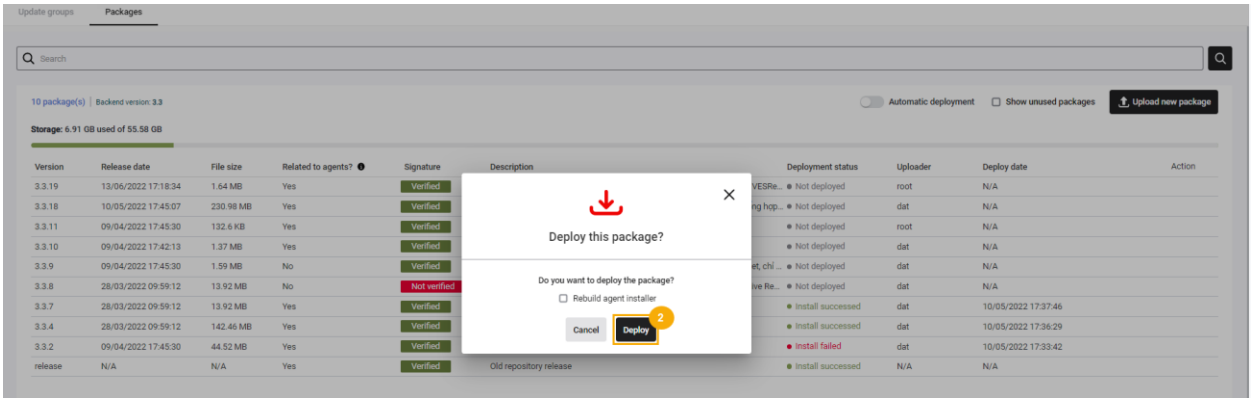
- Log in to the Portal using the provided account credentials;
- Select Settings, the system will display the sub-menus: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- Select Update Management, the system displays the list of Update Groups;
- Select the "Package" tab, the system displays the list of Packages in the system;



- Select the "Deploy this package" icon on the package record, and the system will display a Deploy Package Confirmation popup.



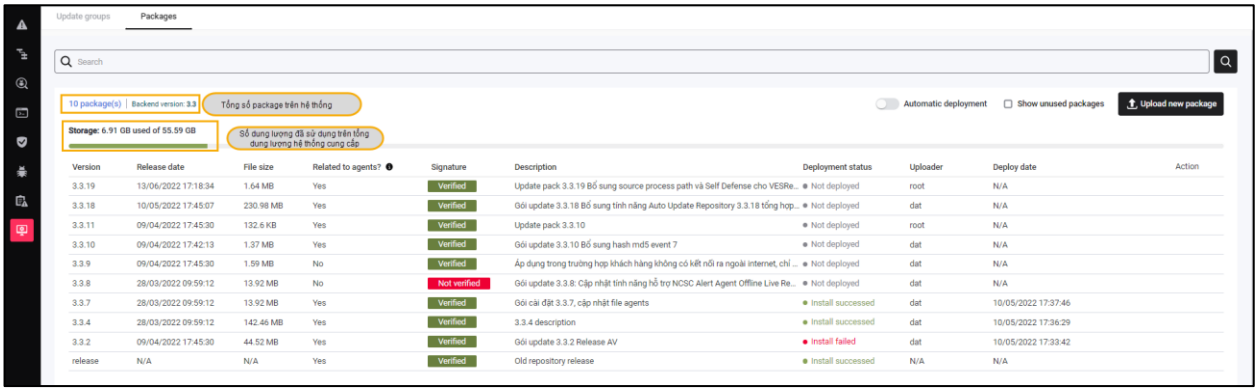
- Select the "Deploy" button to confirm the package deployment on the device, or select the "Cancel" button to cancel the package deployment operation.



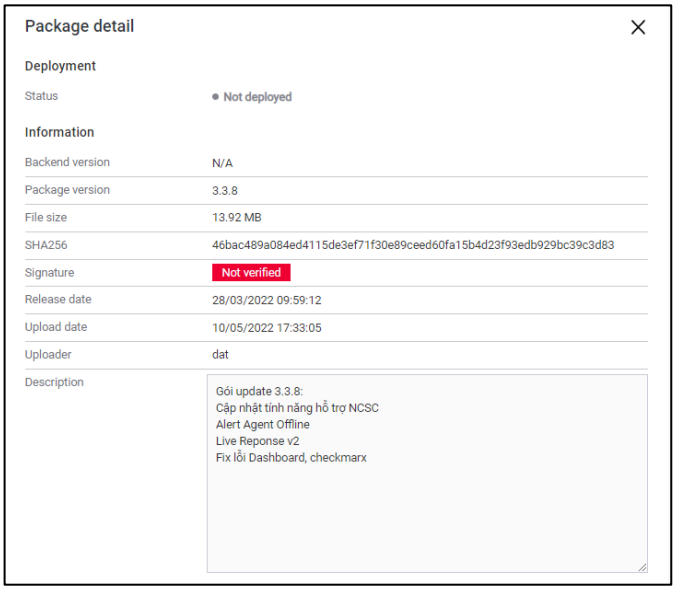
4 – Package Details

- Log in to the Portal using the provided account credentials;

- Select Settings, the system will display the sub-menus: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;
- Select Update Management, the system displays the list of Update Groups;
- Select the "Package" tab, the system will display the list of Packages in the system;



- Select the "View Detail" icon on that package record, and the system will display a popup with detailed information of the selected package.



3.7 BLS Screen

3.7.1 Violation Statistics

Purpose: The Violation Statistics function supports administrators in compiling statistics of violations committed by installed agents, including:

Top baseline violations, top units violating the baseline;

View the list of violations and the list of agents violating in each unit;

View the list of violating units and the list of violations within each unit;

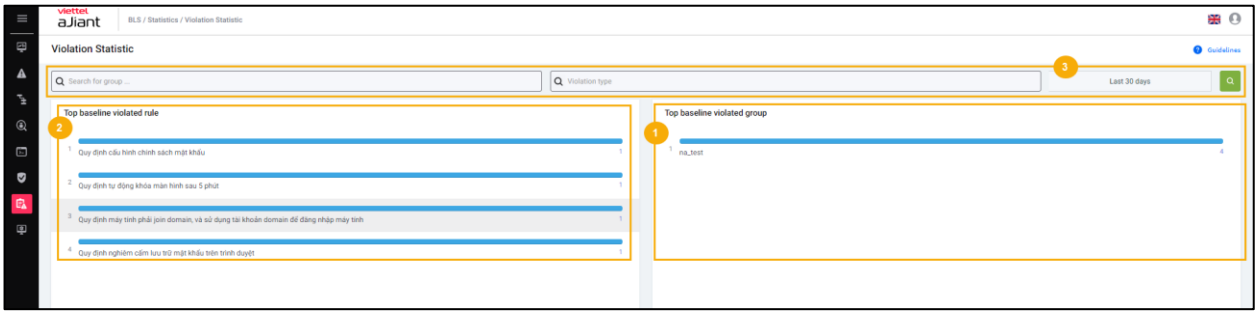
View Agent details;

Export violation;

Violation report;

Click on the "BLS" tab >> Violation statistics;

Violation Statistics Screen



The system supports the implementation of the following features:

Statistics of the Top 10 baseline violations ranked in descending order

- Each record displays the following information: violation details and the number of violating devices.
- Selecting any record in the Baseline Violation Top will navigate the system to the detailed screen corresponding to the selected violation;

Statistics of the Top 10 units with the highest number of baseline violations, arranged in descending order:

- Each record displays the following information: Name of the violating unit, number of violating machines;
- Selecting any record in the Top baseline violation units will navigate the system to the detailed screen corresponding to the selected unit.

Search

- Individual search:
- Search by Unit
  - Top violating units display the entered unit and the corresponding list of subordinate units (if any);
  - Top violations: Display violations of the unit and its subordinate units (if any) accordingly;
- Type of violation
  - Top violating units: display the list of units violating the selected type of violation;
  - Top violations: Display selected violations;
  - Duration of violation;
- Combined search: When entering two or more search criteria, the search will be performed using the AND condition;

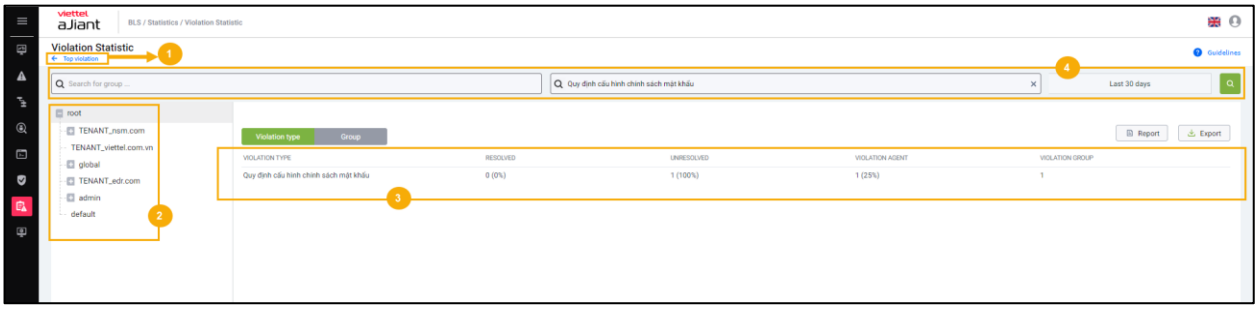
Description of the rules in BLS

Rule	Detailed description
Regulations on displaying file extension suffixes	On the endpoint machine, it is required to display the file extension.
Regulations for Disabling Remote Desktop Configuration	Disable Remote Desktop access

Set automatic screen lock after 5 minutes	Violation of not locking the screen after 5 minutes
Regulations on Disabling the Autorun Function of USB Drives and CD Drives	Allows enabling/disabling the Autorun feature for USB and CD.
Regulation on working hours not exceeding 7 PM	The machine should not operate for more than 19 hours.
Computer violating USB 3G usage regulations	Workstations are not allowed to use MTP devices (smartphones, etc.) or USB devices (storage, 3G, etc.).
Regulations strictly prohibit direct connection to the Internet.	Users can access the network either through a browser or via the system proxy.
Operating System Update Configuration Regulations	Require workstations to enable automatic operating system patch updates.
Regulations on Software Installation and Usage	The workstation violates this rule when installing or not installing the configured software.
Mandatory regulations for installing and using antivirus software	Workstations are required to have antivirus software installed: real-time protection must always be enabled, and update configurations must be set.
Regulations Mandating the Use of Firewall Bypass Software	Workstations are required to have the firewall enabled either on the operating system or within the antivirus software.

Regulations for Installing and Using Kaspersky Antivirus Software	Workstations are required to have Kaspersky AV software installed.
Regulations require computers to join the domain and use domain accounts to log in.	Regulations require computers to join the domain and use domain accounts to log in.
Regulations on local account revocation	Automatically revoke local account upon violation
Regulations strictly prohibit storing passwords in the browser.	Storing passwords in the browser is strictly prohibited.
Password Policy Configuration Regulations	The regulations include the following rules: + Meet the required number of characters + Change the password after a configured period of time + Account is locked after multiple failed login attempts

Violation Type Tab



The system supports the implementation of the following features:

Select the Top Violations link: Navigate to the Dashboard screen, the list of top violations, and the top violating units.

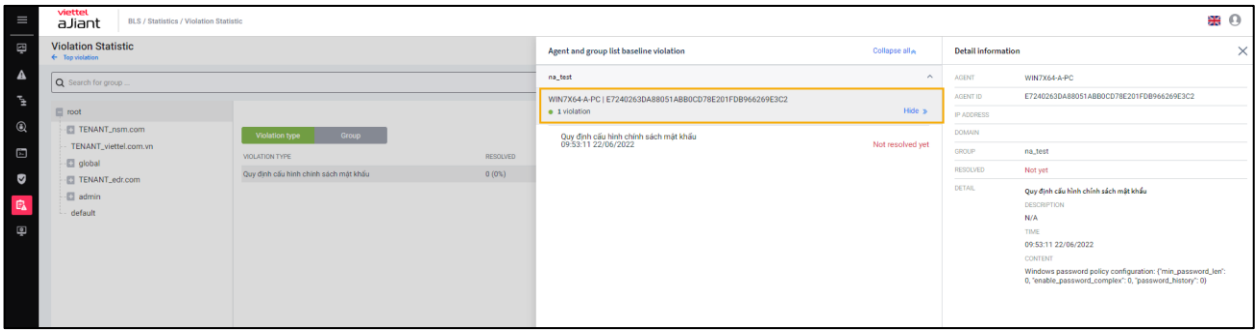
Unit data tree of the system

- Display all system units organized in a parent-child hierarchy;
- You can select units on the unit data tree to perform violation filtering.

Violation Type Tab:

- Each type of violation displays general information including: Violation type, Resolved, Unresolved, Violation Computer, Violation unit;
- Select the Violation Type record from the list: Display the list of computers in each violating unit;
- Select computer: Display detailed computer information and the corresponding list of violations for the computer;

Select a computer from the computer list popup: display a popup with detailed computer information including Computer, AgentID, IP Address, Domain, Group, Resolved, and Detail (all types of violations for the computer).



Search

Individual search:

- Search by Unit: Display the entered unit and the corresponding list of subordinate units.
- Violation type: Display the selected violation
- Violation time

Combined Search: When entering two or more search criteria, the search will be performed using the AND condition.

Unit Tab

The system supports the implementation of the following features:

Select the Top Units link: Navigate to the Dashboard screen, displaying the list of top violations and top violating units;

Unit data tree of the system;

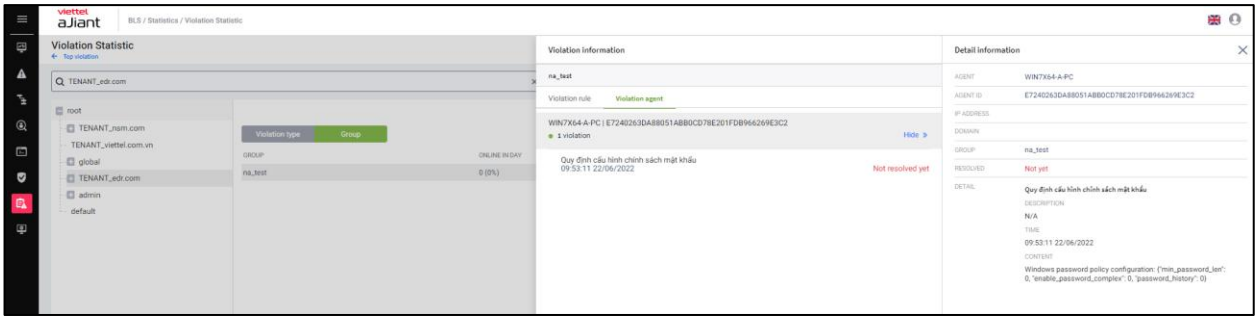
- Display all system units organized in a parent-child hierarchy;

- It is possible to select units on the unit data tree to perform parent-child unit filtering;

Unit Tab;

- Each type of violation displays the following general information: Unit, Online in day, Online in the most recent 30 days, Resolved, Unresolved, Violation computer, Violation rule.

- Select the detail icon of the violation computer column in the list: Display the list of computers in each violating unit, including Unit Name, Computer Name | Agent ID, the list of violations for each computer, violation time, and violation status (fixed or not fixed).



Select a computer from the computer list popup: display a popup with detailed computer information including Computer, AgentID, IP Address, Domain, Group, Resolved, and Detail (all types of violations for the machine);

Select the detail icon of the violation rule column in the list: Display the unit's violation list;

Search

Individual search:

- Search by Unit: Display the entered unit and the corresponding list of subordinate units;
- Violation type: Display the selected violation;
- Duration of violation;

Combined search: When entering two or more search conditions, the search will be performed using the AND condition;

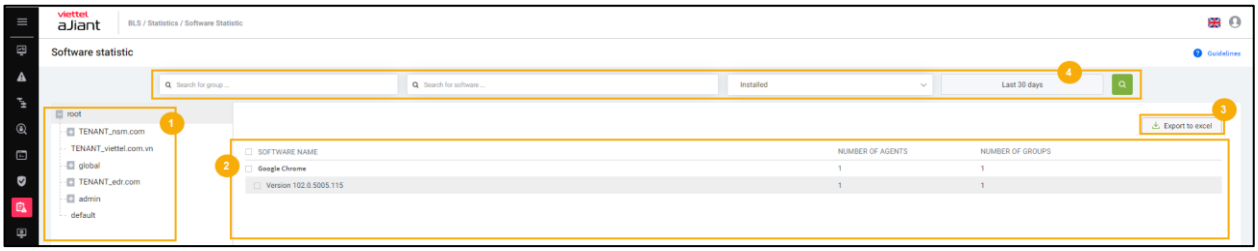
3.7.2 Software Statistics

Purpose: The Software Statistics function assists administrators in compiling statistics on the software installed within an organization, including:

View the list of software installed in a selected unit;

View Agent details;

Software export;



The system supports the implementation of the following features:

Unit data tree of the system

Display all units of the system organized in a parent-child hierarchy.

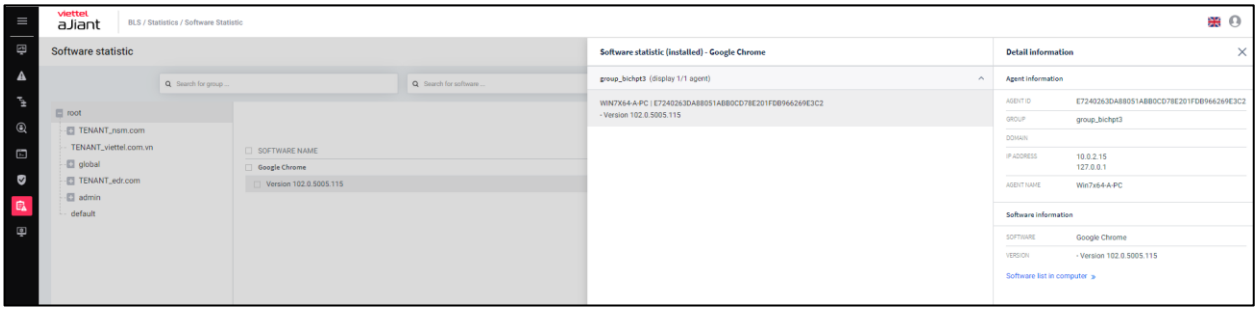
You can select units on the unit data tree to perform software filtering.

Software list

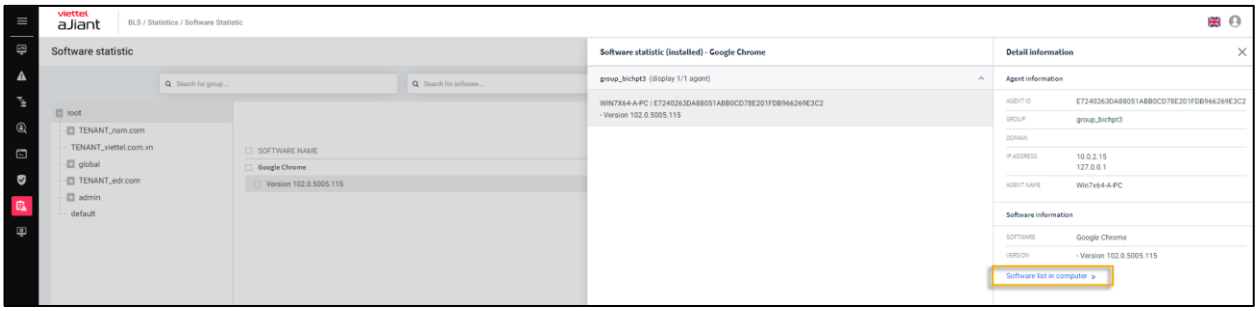
- Each software displays general information including: Software name, number of computers, number of units;

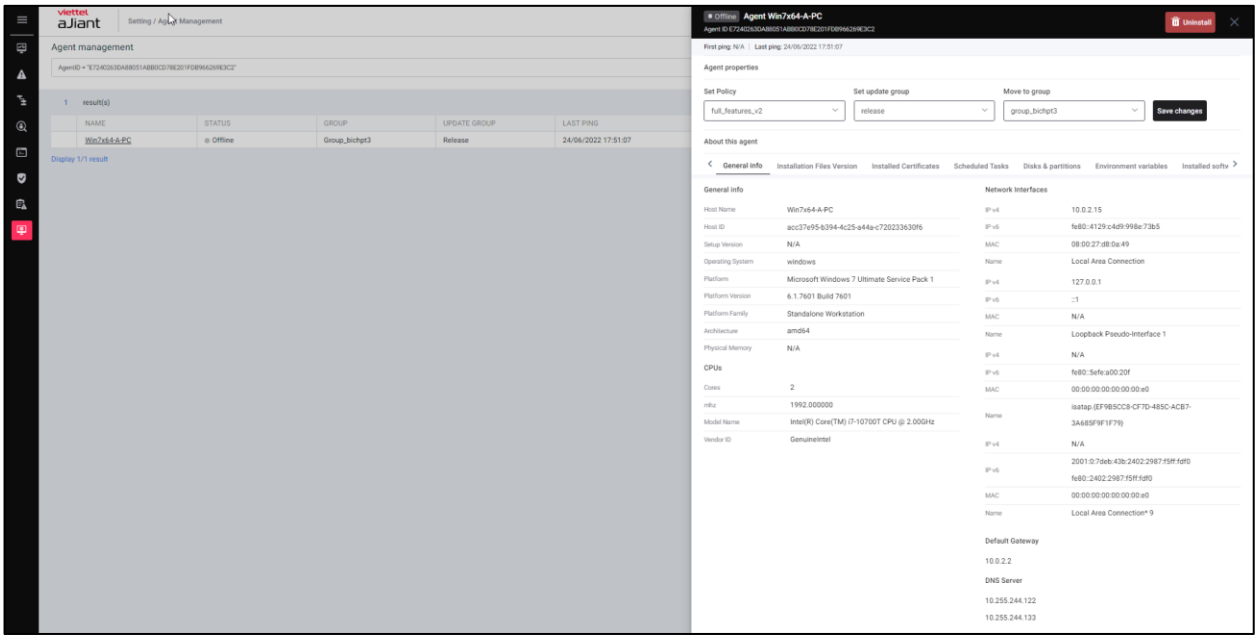
- Select the detail icon of the violation computer column in the list: Display the list of computers in each unit, including Unit Name, Computer Name | Agent ID, Version;

- Select a computer from the computer list popup: display a popup with detailed computer information including Computer, AgentID, IP Address, Domain, Group, and Software information (software name, version);



- Select the link [List softwares in computer]: The system navigates to the Agent Management screen and displays a popup with details of the selected computer.





Search

Individual search:

- Search by Unit: Display the software installed in the unit
- Software name: display the list of entered software
- Search by status: Installed, uninstalled
- Installation time

Combined search: When entering two or more search conditions, the search will be performed using the AND condition.

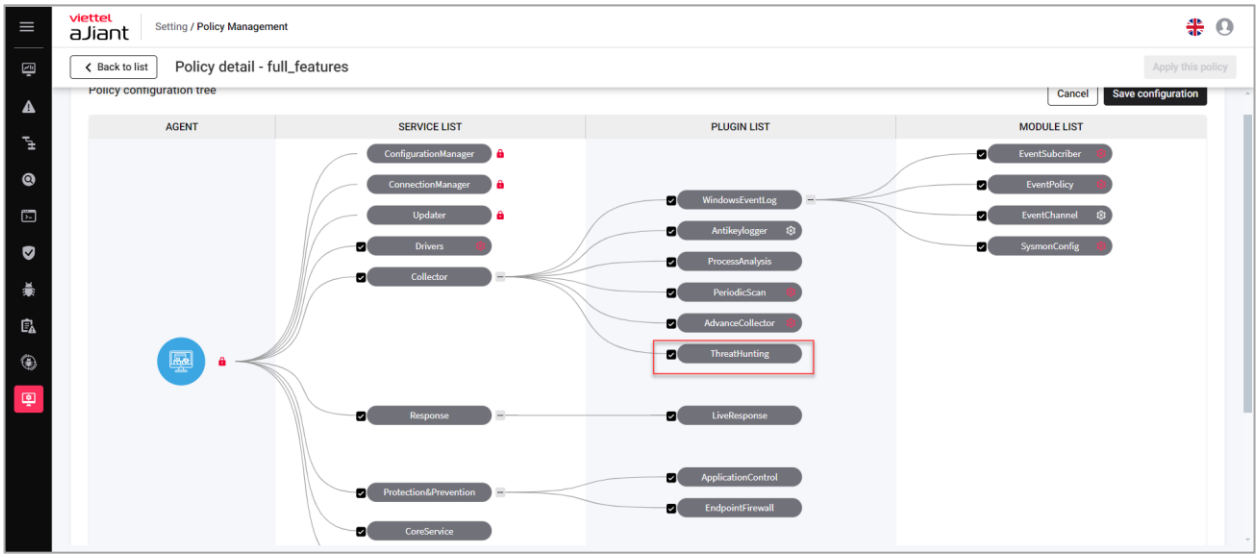
Export: Select Export: The system will download an Export file containing data identical to what is currently displayed on the screen.

3.8 Threat Hunting

The Threat Hunting feature allows users to search for signs of suspected attacks and IOCs on workstations within the organization, enabling early response and mitigation measures. This feature supports the process of...

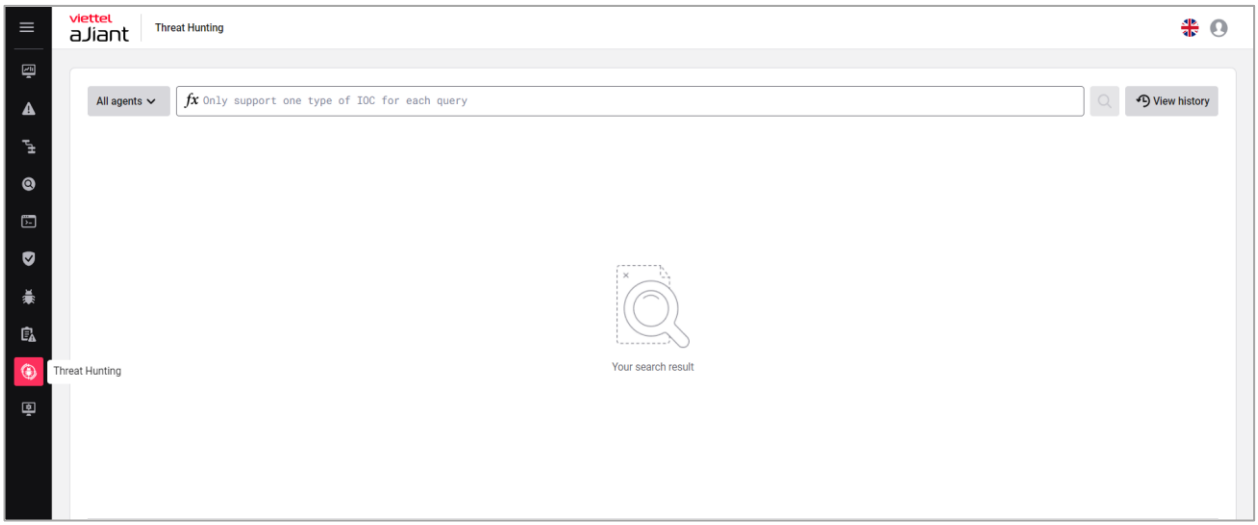
3.8.1 Enable/disable policy

- To use the Threat Hunting feature, you need to enable the policy in Policy Management -> Select the Collector service -> Choose the ThreatHunting plugin.
- Note: The agent must have the ThreatHunting policy applied in order to perform IOC searches.

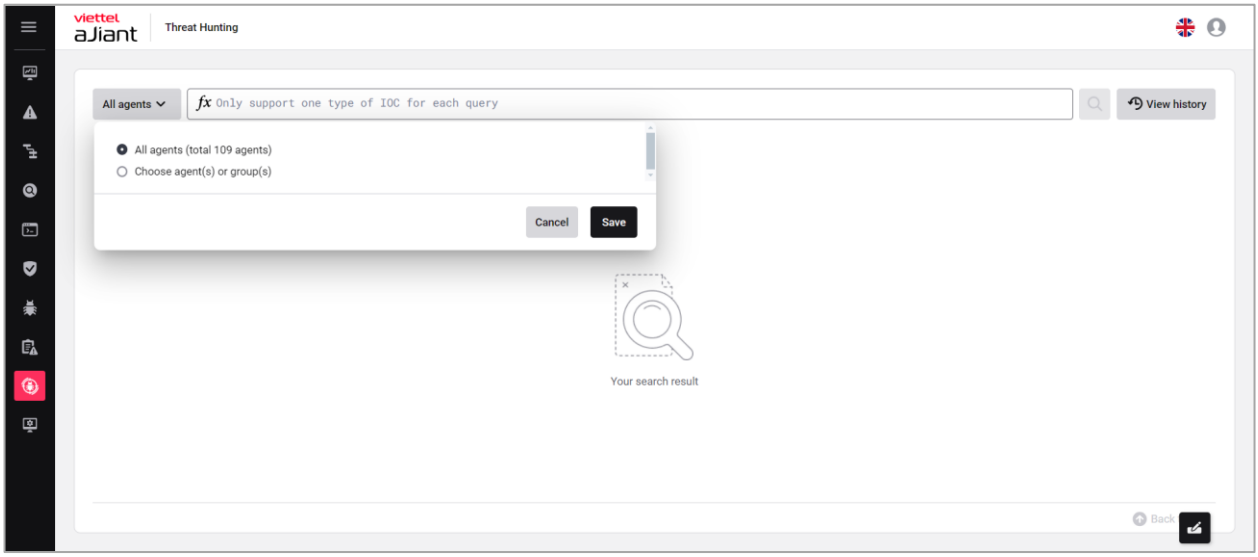


3.8.2 Search by agents/groups

- On the menu, select Threat Hunting.



- Allow admin to search for IOCs by agents/groups.
    - Allow searching across all agents (All agents)
    - Allow searching by specific agent or by group selection.



3.8.3 Search for IOCs

Supported types of IOCs

- Users can search by IOC types in the table below:

IOCs	Tab	Query field	Support operator	Note

File path	File	file_path	=, ~	Search by file path
File name	File	file_name	=,~	Search by file name
File hash SHA256	File	file_sha256	=	Search for SHA256 hash file
Đường dẫn đăng ký	Registry	registry_path	=,~	Search by Registry path
Registry key	Registry	registry key	=,~	Search by Registry key
Dữ liệu đăng ký	Registry	registry_data_string	~	Search by Registry data type: string, DWORD, binary
		registry_data_dword	=	
		registry_data_binary	=,~	
Strings Memory	Memory	strings_memory	~	Allow searching by memory string
Hex Memory	Memory	Hex_memory	~	Allow search by hex format
User Name	User	User_name	=,~	Allow searching by user on the endpoint machine
Domain	Mạng	Domain	=,~	Allow searching by domain that endpoint devices

				have previously accessed.
IP	Mạng lưới	Domain	=,~	Allow searching by IP addresses that endpoint devices have previously accessed.
Quy trình xử lý	Quy trình	Process_path	=,~	Allow searching by process path
Process Command Line	Quy trình	Process_commandline	=, ~	Allow searching by process command line
DLL	DLL	Dll_path	=, ~	Allow searching by DLL path

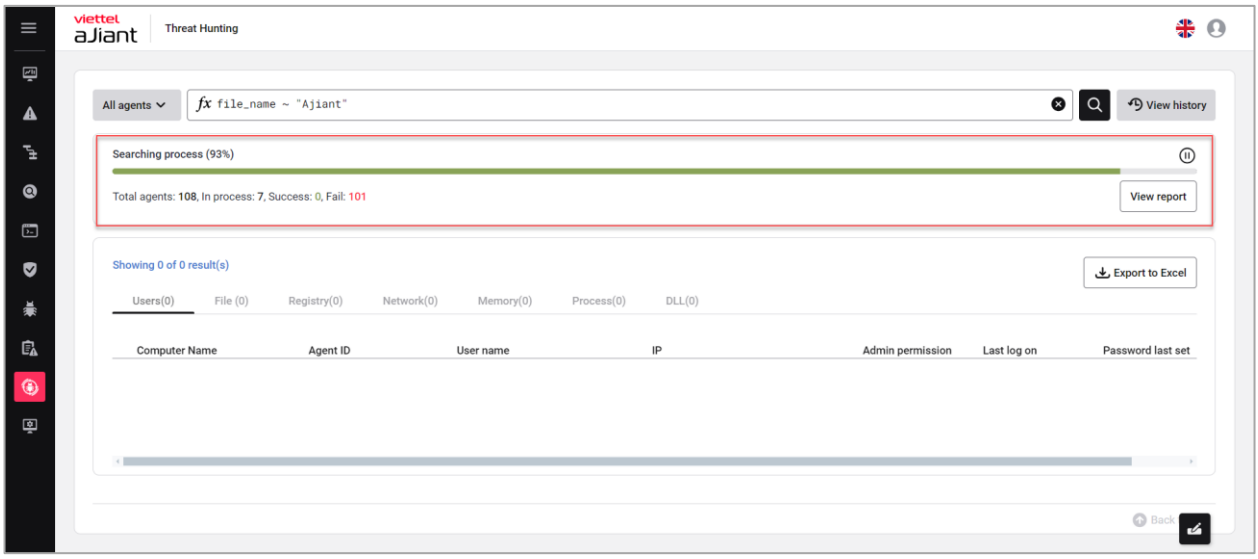
Note:

- Users are only allowed to search for one type of IOC per query.
- Allow searching using AND, OR conditions.
- Search values are case-insensitive.
- After the user performs a search, the system scans the endpoint device according to the query requirements and sends the results to the portal.
- The search time depends on the complexity of the query and the number of agent machines performing the search.

Search result details

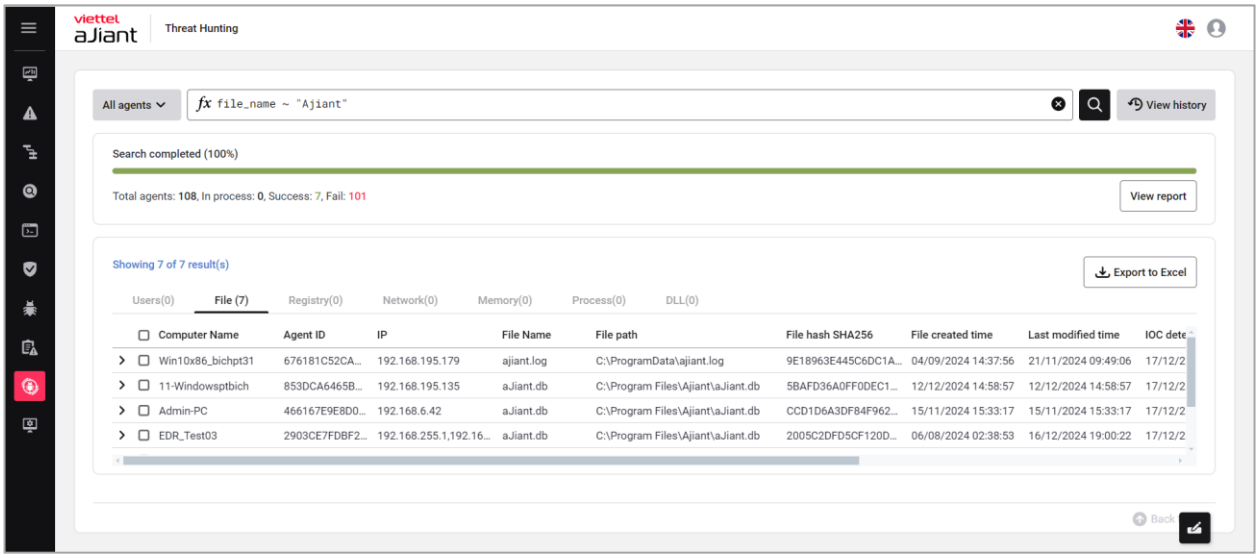
3.9.3.1.1. Track search status

- Allow users to track the search progress.
    - Total agent: Total number of agents performing the search
    - In-process: Search in progress
    - Success: Search successful
    - Fail: Search failed



3.9.3.1.2. Search result details

- Allow users to view detailed search results by each tab.
  - Users
  - File
  - Registry
  - Mạng
  - Memory
  - Quy trình
  - DLL
- The results are displayed correctly in each tab according to the user's query.

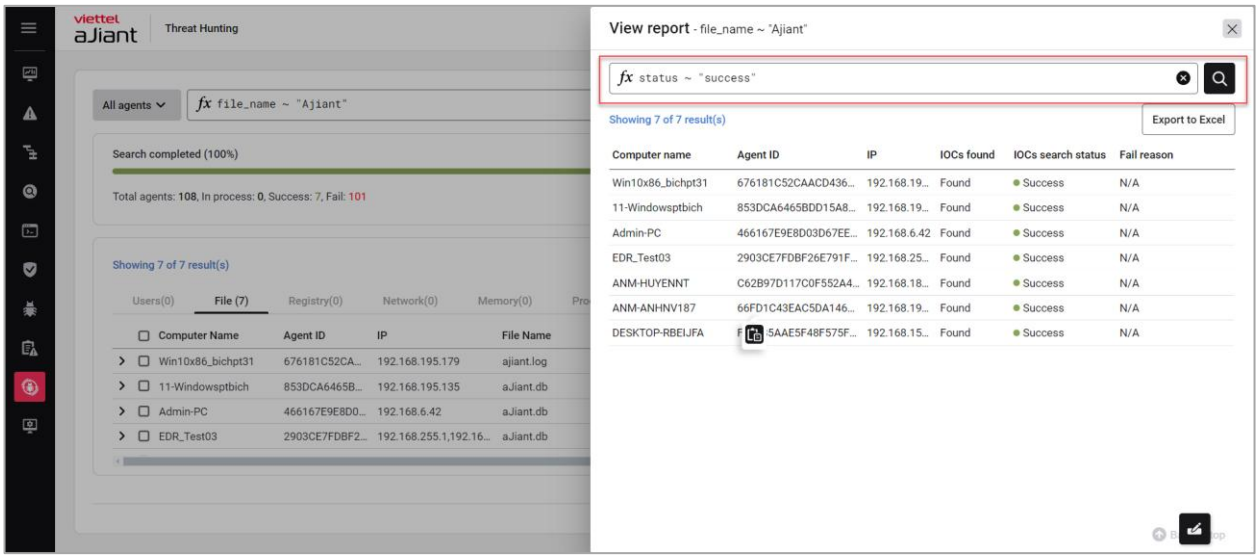


3.9.3.1.3. Stop searching

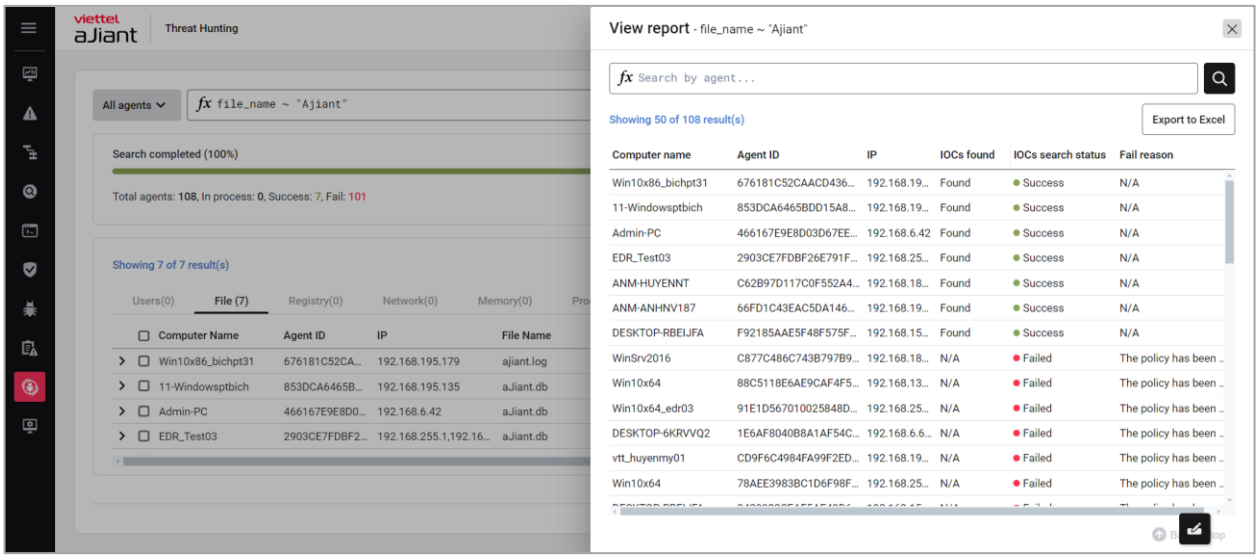
- Allow users to pause the search: On the Searching Process bar -> select the Pause button.
- After stopping the search:
    - The system will stop searching.
    - Continuation of query search is not supported.

3.9.3.1.4. View detailed report on IOC search under agents (View report)

- Allow users to search by Computer Name, AgentID, IP, and IOCs Search Status.

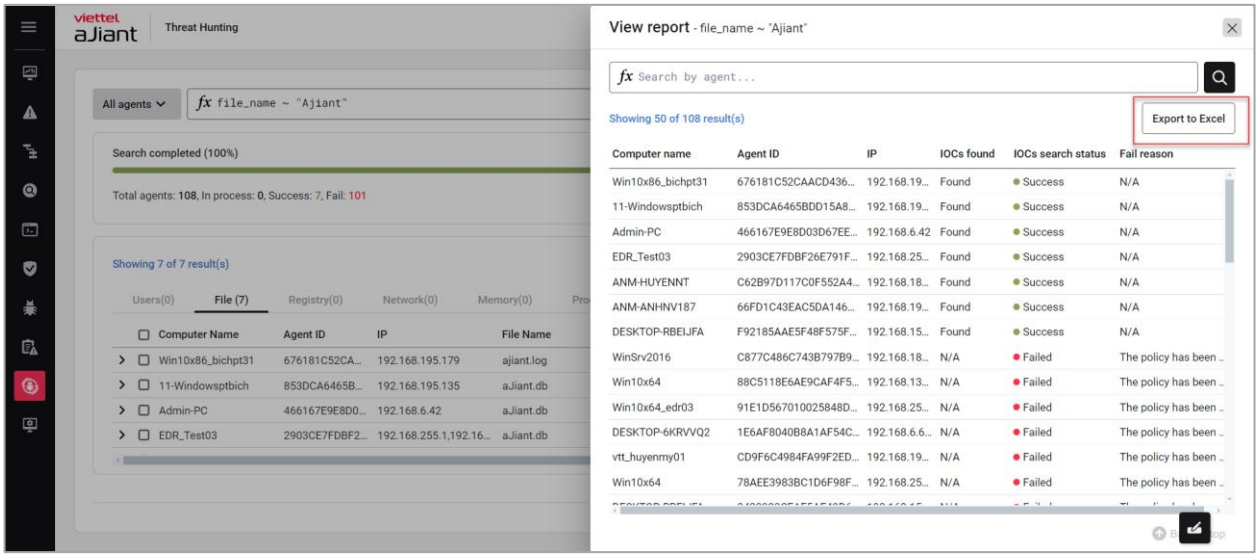


- This report will provide users with detailed information about the status of IOC searches on each agent. The information included in the report consists of:
    - Computer name
    - Agent ID
    - IP
    - IOCs found: Whether any IOCs were found based on the user's query
    - IOCs search status: Status of IOC search on the agent
    - Fail reason: Detailed reason for search failure



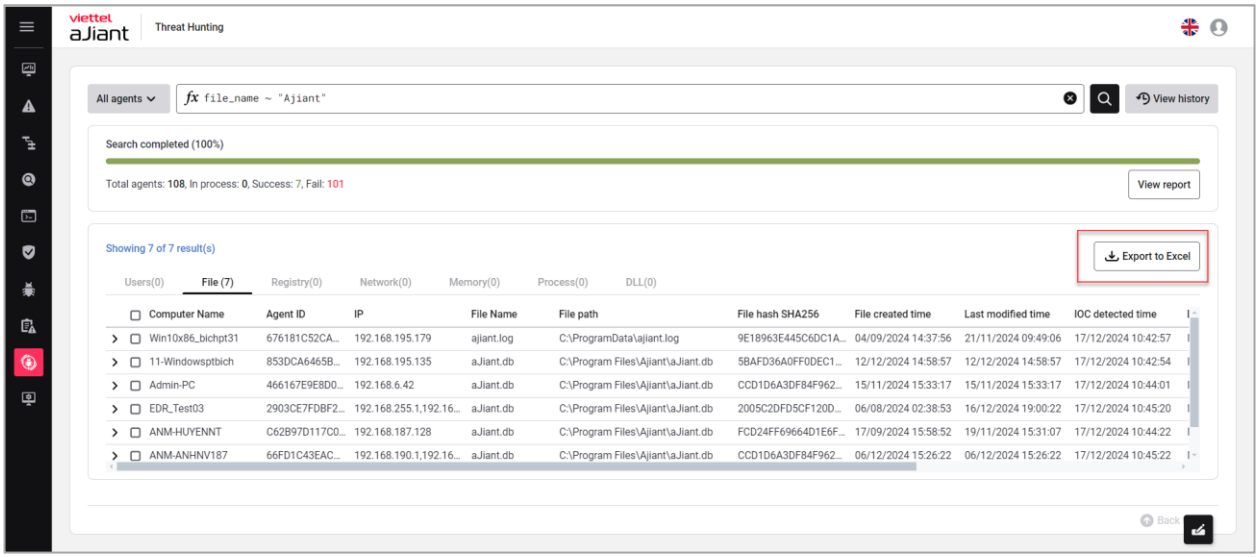
3.9.3.1.5. Export to Excel

- Allow users to download an Excel file summarizing search results under the agent.
- The information in the file includes
  - Tên máy tính
  - Agent ID
  - IP
  - IOCs found: Whether any IOCs were found based on the user's query
  - IOCs search status: Status of IOC search on the agent
  - Fail reason: Detailed reason for search failure



3.9.3.1.6. Download search results

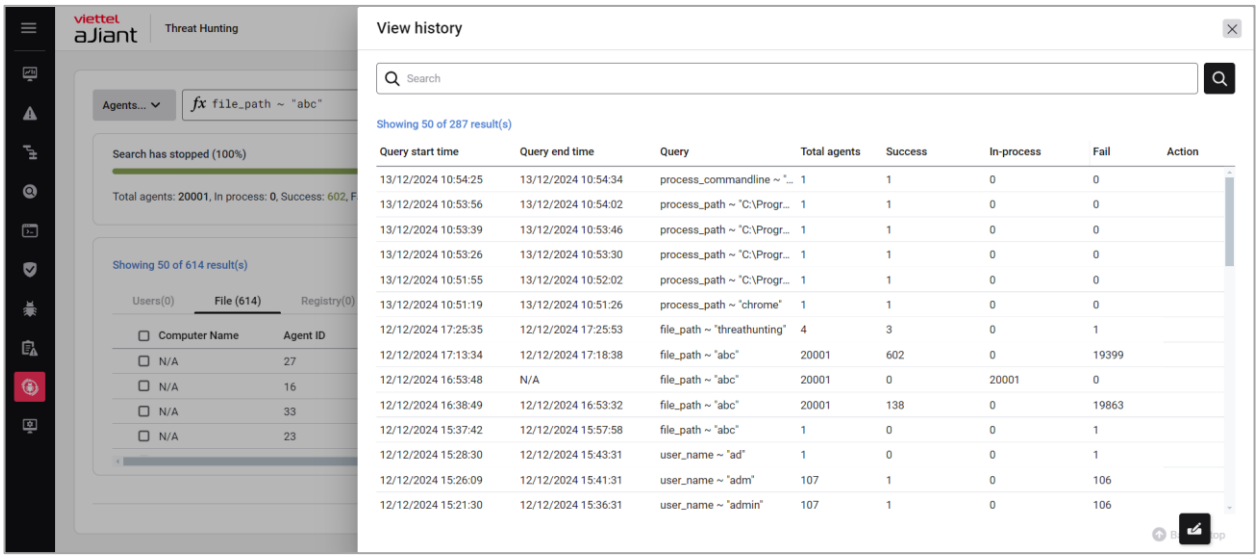
- Allow users to download IOC search results on the agent machine.
- Support for downloading Excel files



3.8.4 View Query History

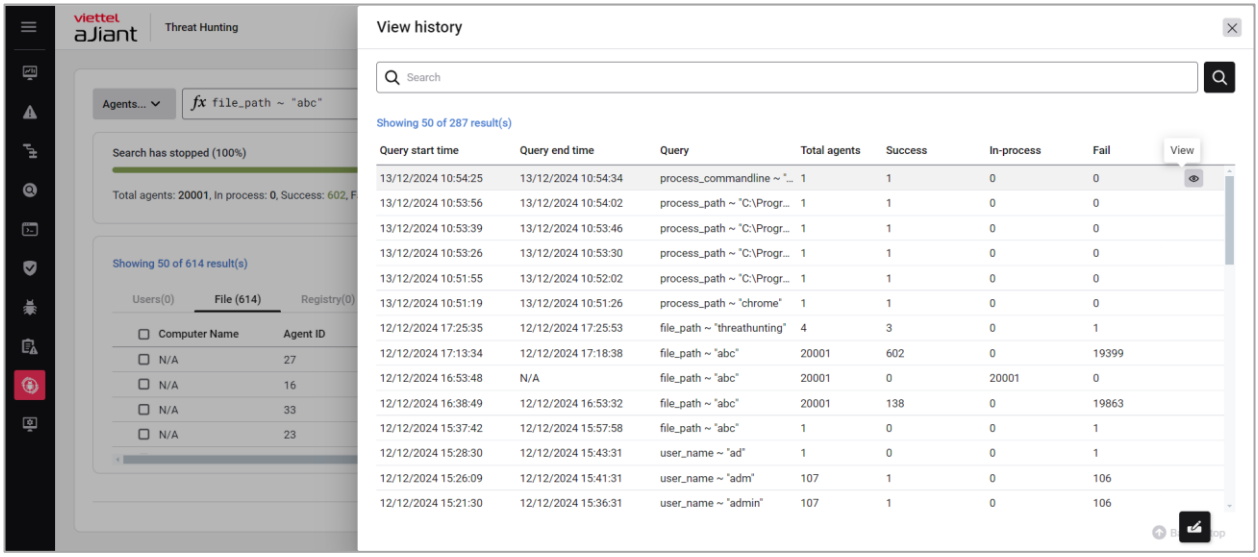
View query list

- Allow users to review their query history. The query history information includes the following details:
  - Query start time: The time when the query execution begins
  - Query end time: Search completion time
  - Query: user's query
  - Total agents: Total number of agents searched
  - Success: Search completed successfully on the endpoint device
  - In-process: Currently searching on the endpoint device.
  - Fail: Search failed

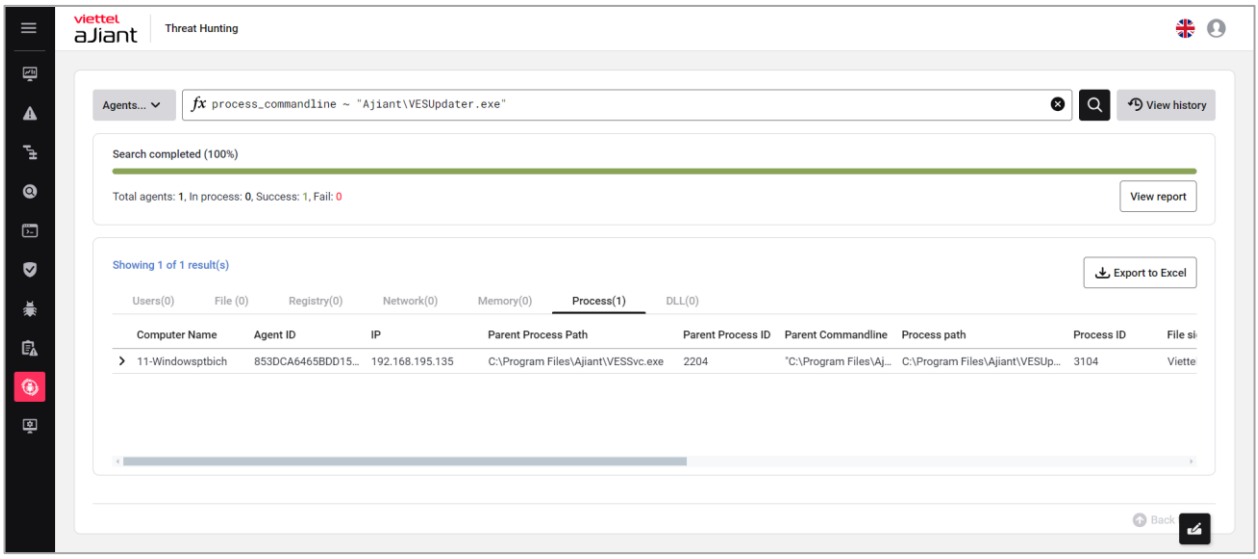


View detailed query history

- Allow users to review the detailed results of each query: Action -> select View



- Allow viewing detailed results of the query in the history:



3.9 Rules Correlation

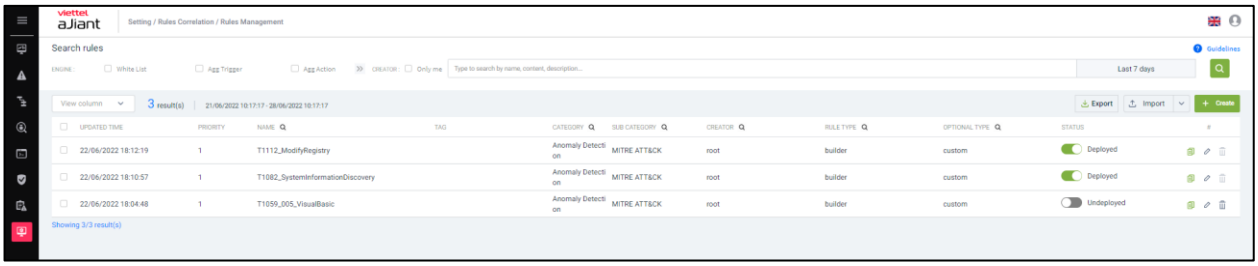
3.9.1 Display list

Purpose: This function allows users to view the list of correlation rules in the system. Users can enter or select search criteria to find existing rules in the system and quickly perform deploy/undeploy/delete actions on the rules.

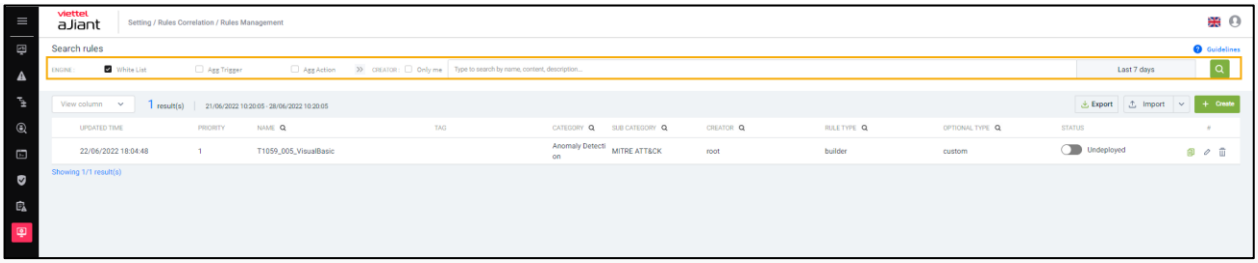
;FITTER filter;

The FITTER filter includes:

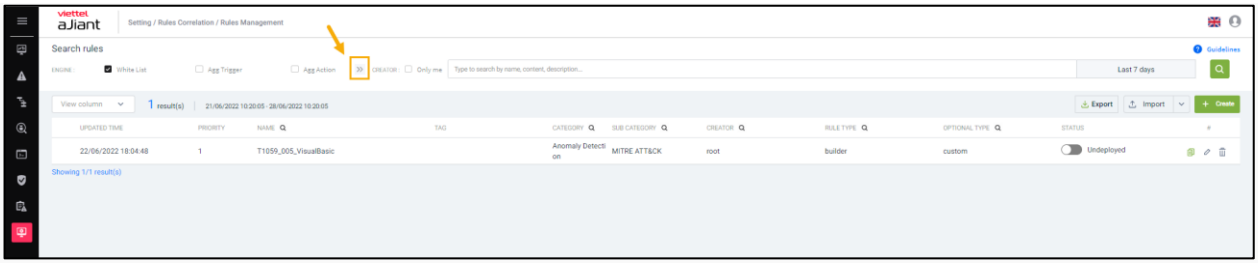
- 6 Engine: Whitelist, Agg Trigger, Agg Action, Filter, Indicator, False Positive;
- Search text box by fields: Name, content, description;
- Update time;
- Created by me;
- ;Filter by Engine;



- Select one or more default Engines;

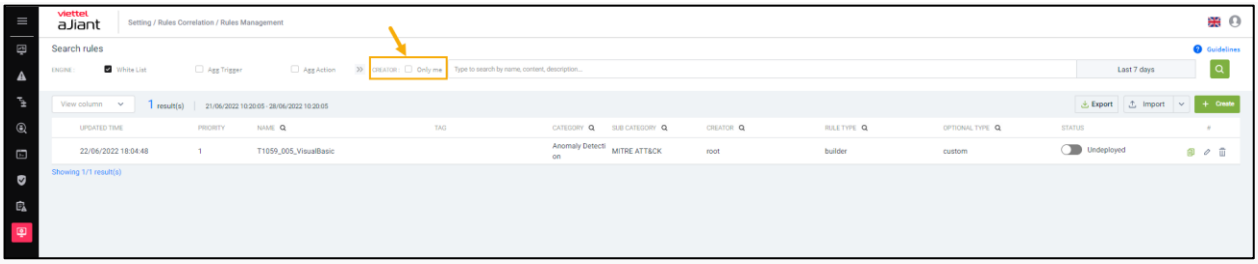


- Select Extensions to add the Engines to be filtered;

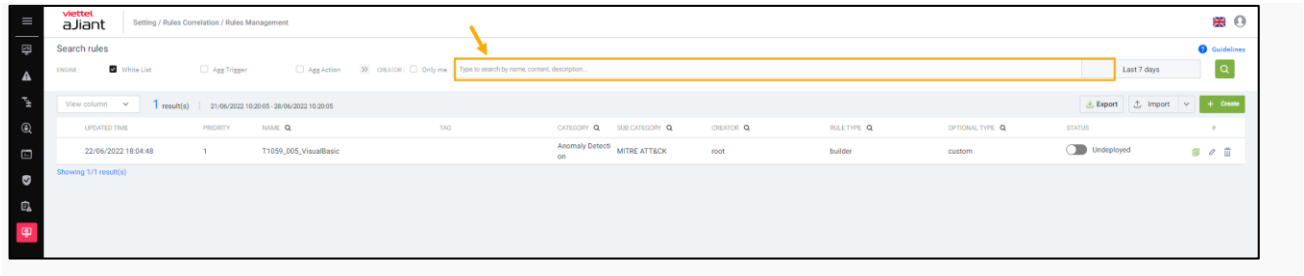


When selecting 2 or more Engines, the screen returns results filtered using the AND operation;

- Select the rule creator as the user currently logged into the system;



- Enter the Name, content, and description you want to search for into the text box;



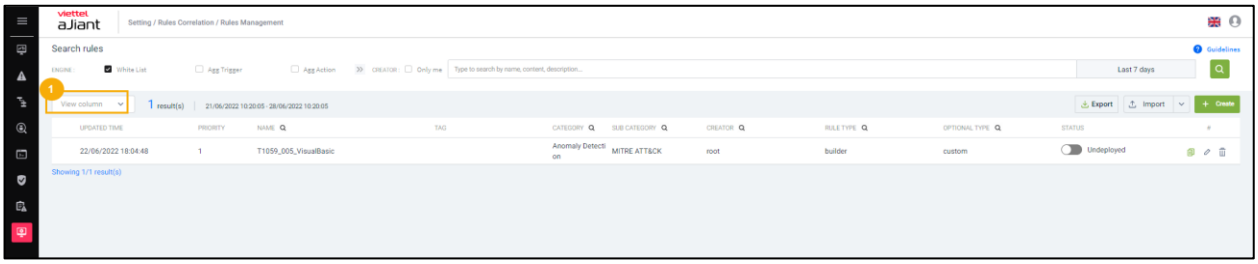
- Enter the information to search for;
- Click Search to display the search results.

Select column

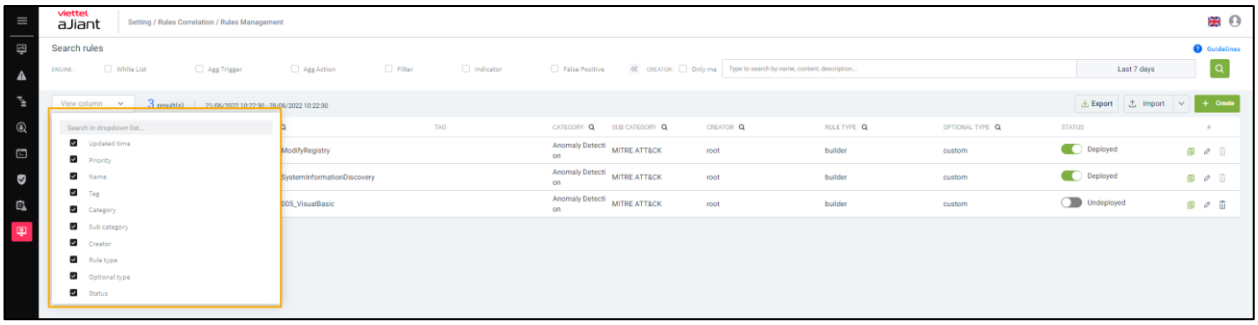
Allow users to select the columns displayed on the correlation screen.

Steps to follow:

- Click on the View column combo box. The screen displays a list of column options in the form of check boxes;

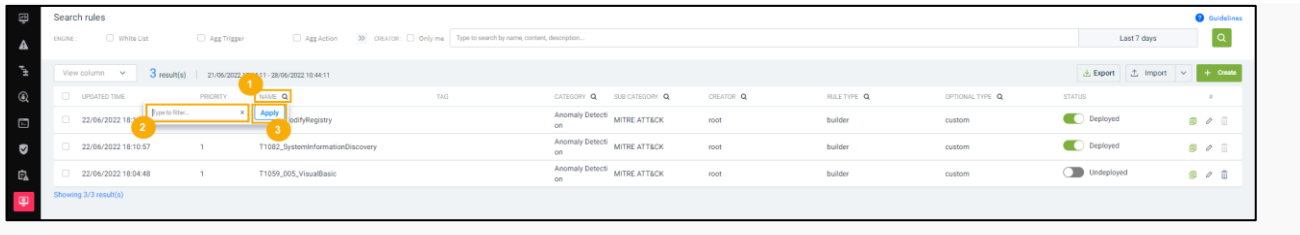


- Select the column names you want to display;

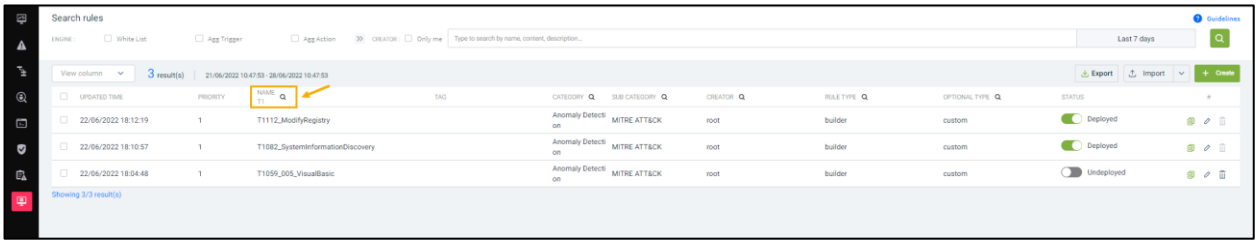


1 – Support for quick search

- Search by rule name
- Click the icon to display the search bar;

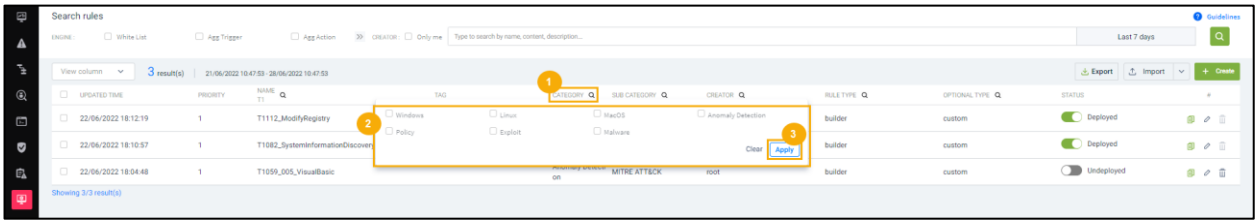


- Enter the name of the rules you want to search for;
- Press Enter to display the search results.



Search by Category: Quick search support includes 3 default types: Windows, Linux, MacOS.

- Click the icon to display the list of Category types.



- Select the category you want to search for;
- Click “Apply.”

Search Sub Category: Support quick search by deployment type, including 3 default types: Metre ATT&CK, Malware, Suspicious Behaviour.

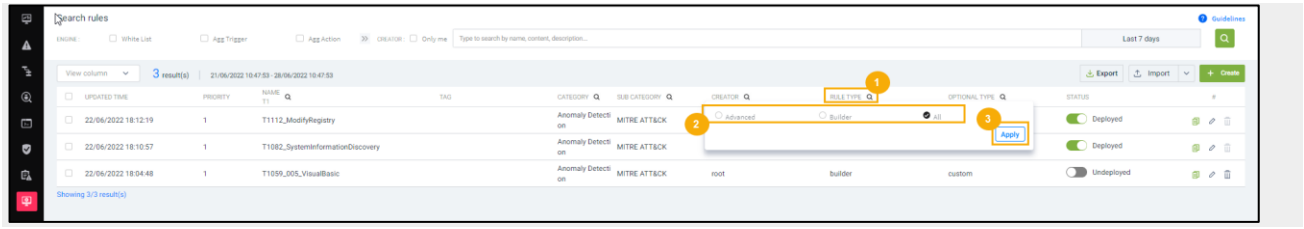
- Click the icon to display the search bar;
- Select the subcategory you want to search for;
- Click “Apply.”

Search for Creator

- Click the icon to display the search bar;

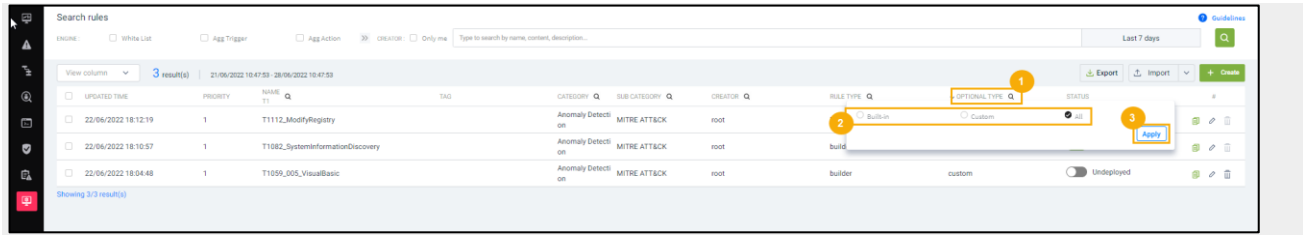
- Enter the name of the creator you want to search for;
- Click “Apply.”

Search Rule type: Quick search support includes 3 default types: Advanced, Builder, All.



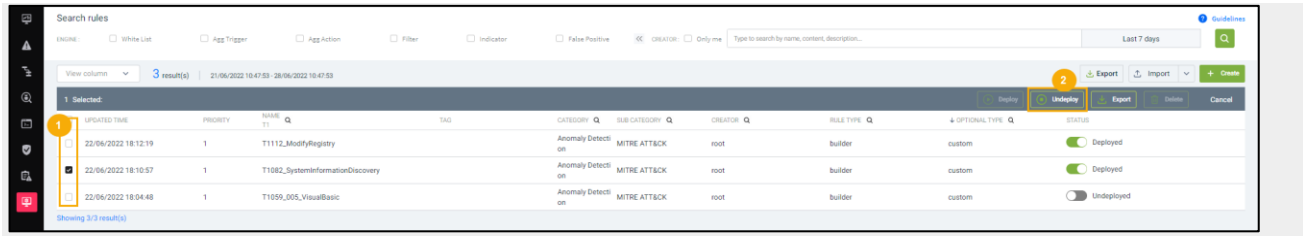
- Click the icon to display the list of Rule types.
- Click on the “Rule type” you want to search for;
- Click “Apply.”

Search Optional type: Supports quick search with 3 default types: Built-in, Custom, All.

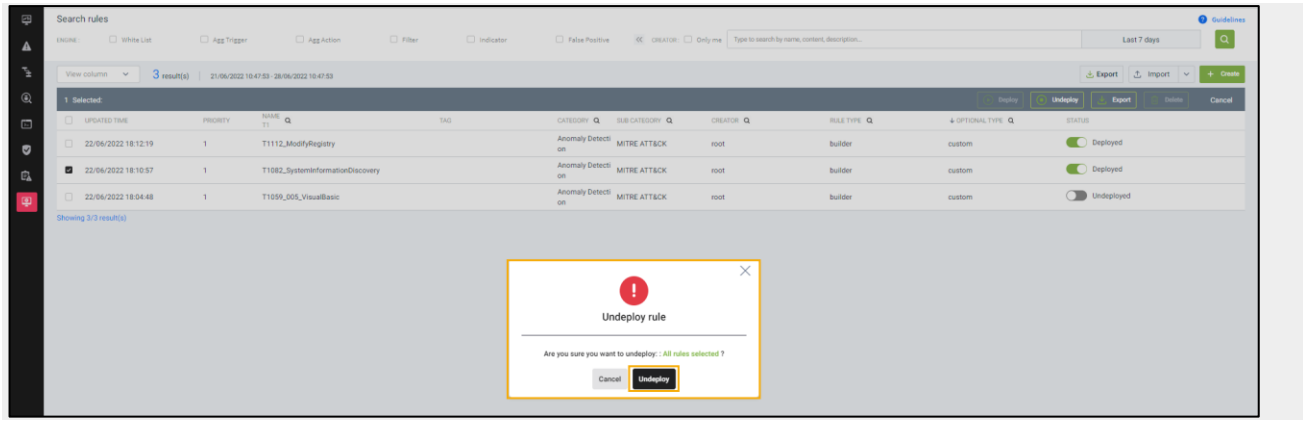


- Click the icon to display the list of Optional types;
- Click the “Optional” type you want to search for;
- Click “Apply.”

Support Deploy/Undeploy for multiple Rules



- Click on multiple checkboxes that have the same status, either Deploy or Undeploy;
- Click the “Deploy/Undeploy” button;
- Select “Deploy/Undeploy” on the displayed popup to perform Deploy/Undeploy;



3.9.2 Add New Rules Correlation

Purpose: This function allows users to configure a complete new correlation rule.

Overview

Engine: Includes a total of 6 engines with detailed information as follows:

- Whitelist is a Stateless Engine that quickly filters out events that the system does not need to process. Events matching the whitelist rules will be dropped from the processing flow.
- Agg_trigger and Agg_action are Stateful Engines that perform grouping of similar events. Each aggregate rule contains information about the grouping conditions (defining similar events) and the grouping time interval (e.g., 30 seconds, 1 minute, 2 minutes, etc.). Events that match the grouping conditions are stored and

only one event is returned after the specified time interval, accompanied by the count. Events that do not match the grouping conditions are returned immediately with a count of 1.

- A filter is a Stateless Engine that performs condition filtering to feed into the indicator.

- An Indicator is a Stateful Engine that performs checks and statistics on events that satisfy a Filter. The input to the Indicator consists of events meeting the Filter criteria, and the output is Indicator Events or Alert Events. The Indicator supports counting statistics within a specified time window for the same object and prevents repeated Alerts for the same object within a predefined time period. Each indicator rule only evaluates conditions of the same type within the same system.

- The FalsePositive engine is a Stateless Engine that eliminates cases of false alerts. Each alert that matches a FalsePositive rule will be dropped.

Debug/Not Debug are two states of the engine. When performing a debug operation, logs that meet the engine's conditions will be displayed on the Correlation Debug screen.

Conditions: Each engine will support different conditions regarding Event, not Event, Alert Event, not Alert Event, Accumulate, Function, and not Function. Details about the conditions and how to use them:

- Event: Used for event fields;
- Not Event: Can only be created when there is an event;
- Alert: Used for Alert fields;
- Not Alert: Check how long there has been no Alert event;
- Accumulate: Group event conditions that meet the quantity threshold to generate an Alert;
- Function: These are functions. Note: For boolean functions, the return value is true or false;

- Not Function: With the not function, the functions used are the same as those in the function. However, the return value will be the opposite true/false result.

Operator:

- The basic operators include: =, !=, >, <, >=, <=.
- Check whether the value of a field is included in the list.
  - Left side of the operator: The field name to be checked.
  - Right side of the operator: The list of values to be checked is separated by commas.
- Contains: checks the value of a field that contains the value to be verified.
  - Left side of the operator: The field name to be checked (this field must have a value that is an array or a string);
  - Right side of the operator: The value to be checked.
- Assign: to assign the value of a field to a variable.
  - Left side of the operator: Name of the field to be assigned;
  - Right side of the operator: The name of the variable to be assigned.
- Matches: checks whether the value of a field satisfies a regex pattern.
  - Left side of the operator: Name of the field to be checked;
  - Right side of the operator: Regex string.
- Time configuration: Check conditions within a time interval, available only in Agg_trigger, Agg_action, and Indicator engines.
- Count: Check whether the number of events counted within a given time period meets the specified condition.

Group/Ungroup: Allows users to quickly combine or separate conditions within an AND or OR operator. Steps to group/ungroup:

- Group merging

- Click on the field that needs to be grouped;
- Select GROUP Detailed screen of the steps to merge groups;
    - Split group:
- Click on the items to be grouped separately;
- Select REMOVE FROM GROUP Detailed screen of the steps to separate the group

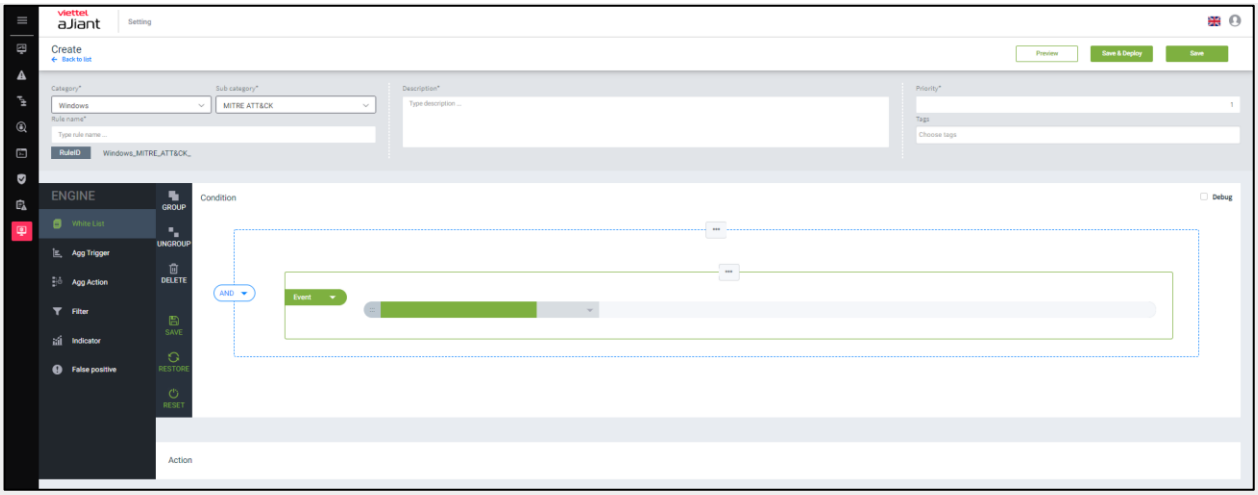
Restore: Automatically reset immediately after the most recent "Save" action;

Reset: Perform reset condition (to the initial state);

Delete: Delete the condition currently in focus;

Steps to add a new correlation rule:

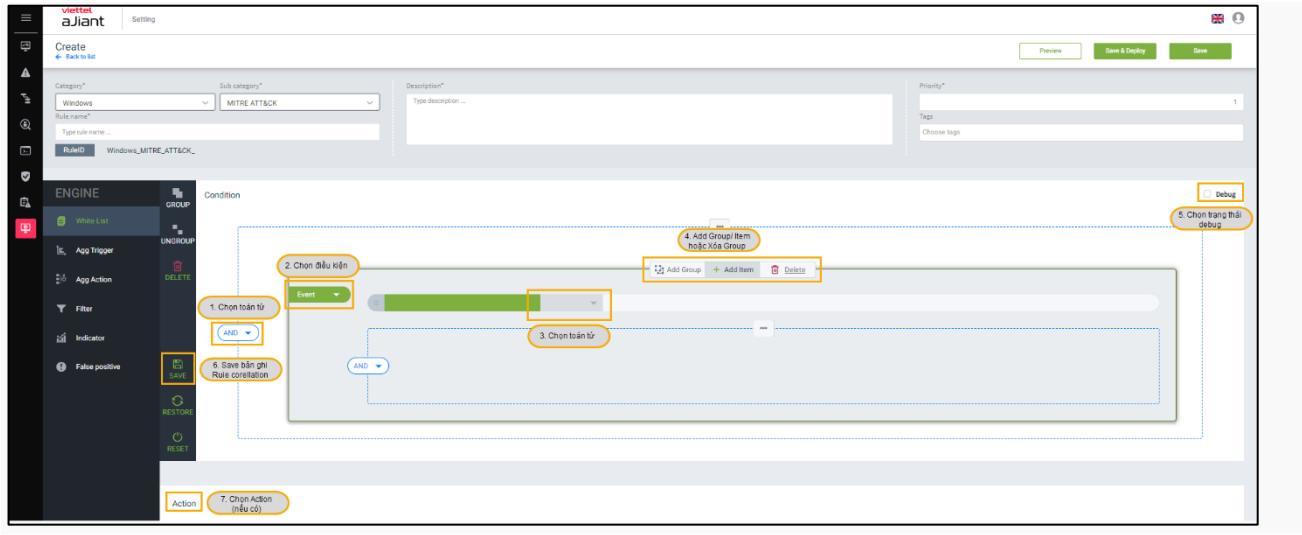
- On the Correlation screen, select the "Create" button > The system displays the new rule creation screen;



- Enter the rule information;

Note: Fields marked with an asterisk (*) are mandatory.

- Select the Engine, enter conditions for the corresponding Event, not Event, Alert, not Alert, Accumulate, and Function;



- Click "Save" to save the condition or click "Restore" to immediately revert to the last saved step;
- In the Action section, select the action to be performed on that engine.

Steps to add actions corresponding to each engine: When the user completes the condition creation steps and clicks save, the screen will display actions for each engine. Each engine will include its respective actions. The Agg_trigger engine will have no actions.

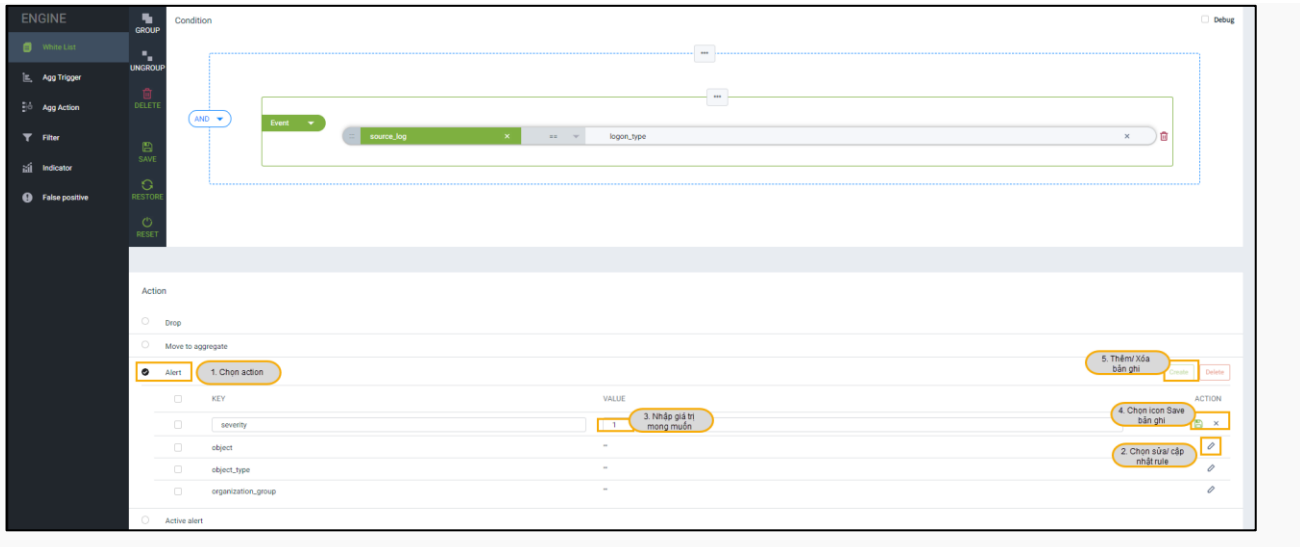
Whitelist: Includes 4 actions in the form of checkboxes: Drop, Convert to Aggregate, Alert, and Active List. Users are required to select one of these four actions. When logs that meet the conditions are pushed in, one of the four selected actions will be executed. Detailed functions of the 4 actions:

- Drop: Logs that meet the specified condition will be removed from the processing stream;
- Switching to aggregate: Logs that meet the conditions will be transferred to the aggregate engine for further processing;
- Alert: When adding key and value fields for the Alert, logs that meet the conditions will trigger the Alert to be displayed on the Alert management screen.

- Active List: The values of the active list will be added to the display list on the Active List screen;

Steps to add a field for the Alert action / Active list:

- Step 5.1: Click to select the action you want to add;
- Step 5.2: Click the "edit" button to enter a value for the field;
- Step 5.3: Enter the value for the field;
- Step 5.4: Click the “Save” button;
- Step 5.5: Click the "Add" button to add a new field to the Alert.



To delete the action just created, click the "Delete" icon;

To edit the action, click the "edit" icon;

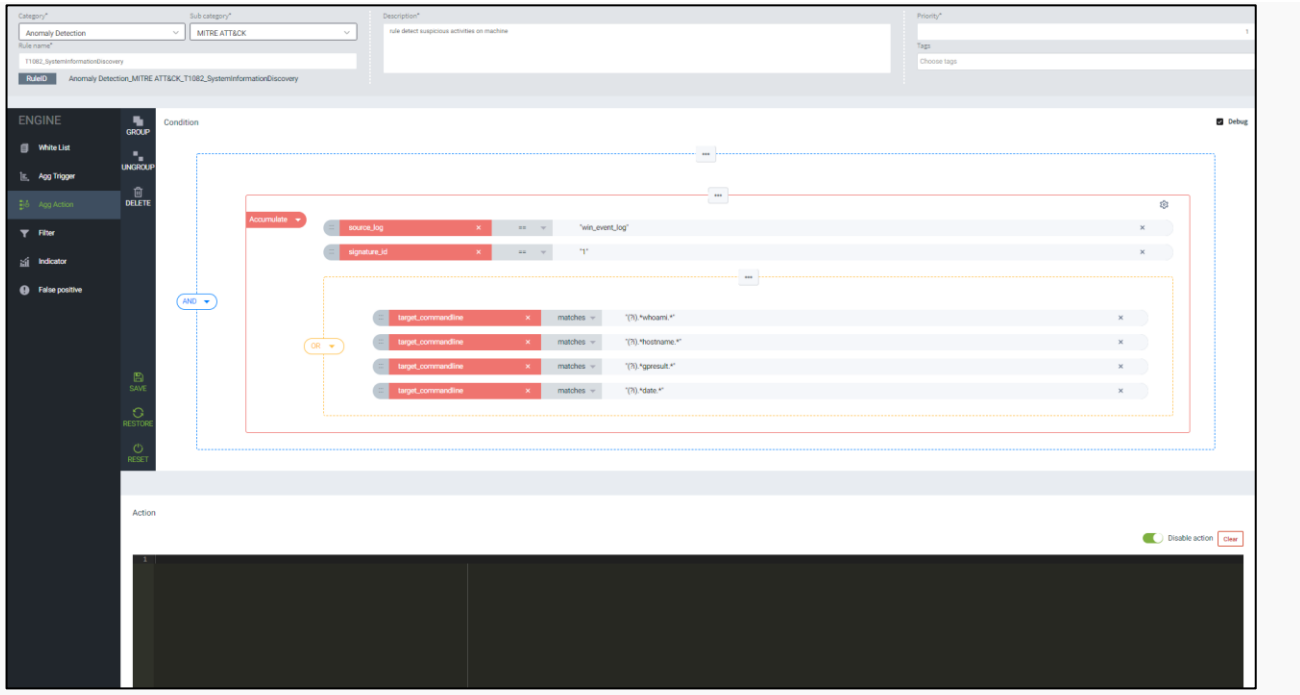
Note: Multiple actions can be created with different fields depending on the user's purpose.

Agg_action: In this engine, users can perform the action of adding code.

Steps to add a field for the add code action

- Step 5.1: Enter all conditions and operators. Click "Save";
- Step 5.2: In the Action section, click on the "Enable action" icon;

- Step 5.3: Enter the content of the code;
- Step 5.4: Select the "clear" button => The entered code content will be completely erased;



Filter: Includes 3 actions: Alert, Enrichment, and Active List. Users can apply one or multiple actions within the same engine. Detailed functions of the 3 actions:

- Enrichment: Add field to Alert;
- Alerts and Active List (such as engine Whitelist).

The operations for adding, editing, and deleting actions of the engine filter are similar to those for adding fields to the engine whitelist.

Indicator: Alert actions. The operations of adding, editing, and deleting for the engine Indicator actions are similar to those for adding new fields to the whitelist engine.

FalsePositive: Enrichment actions. The operations of adding, editing, and deleting for FalsePositive engine actions are similar to those when adding new fields for the whitelist engine.

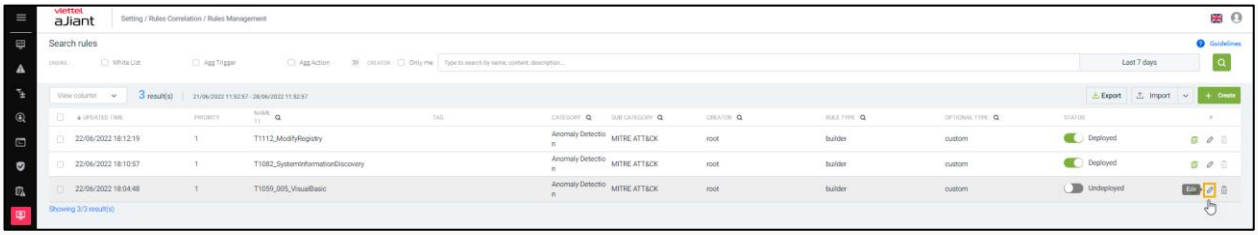
- Click "Save" to save the rule into the system. When the user wants to save it into the system and simultaneously deploy it to the correlation engine, click "Save & Deploy."

Note: When an error occurs, users can click the "Preview" button to view the error.

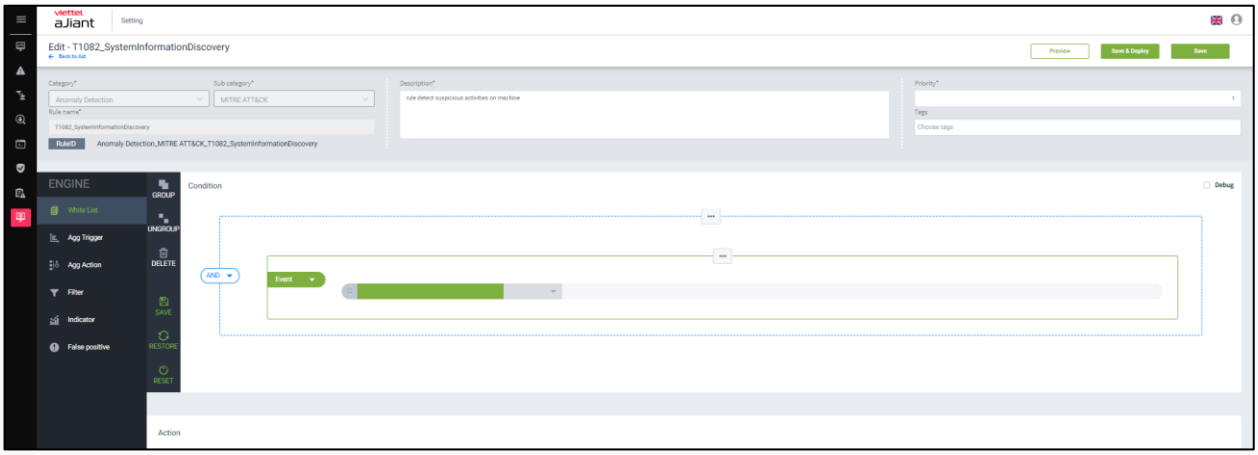
Fix Rules Correlation

Allow users to edit the rules they have created.
Steps to follow:

- On the rule management screen, click the Edit icon of the rule you want to modify;



- On the editing screen, enter the information to be edited;



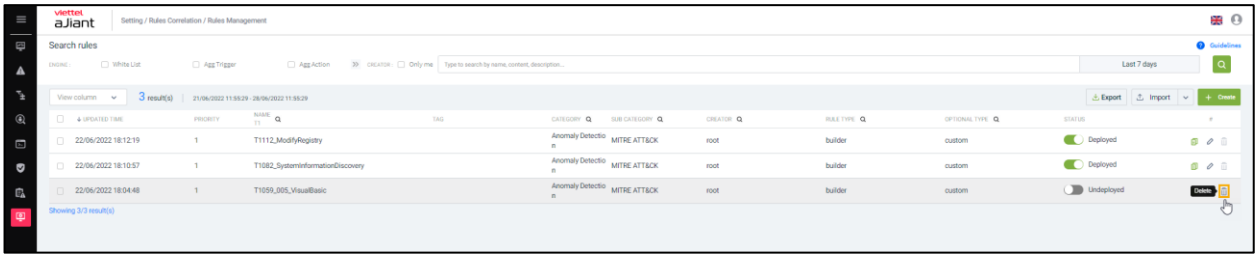
Note: The fields for rule name, category, and subcategory are not editable.

- Press the "Save" button to save the rule into the system. When the user wants to save it into the system and simultaneously deploy it to the correlation engine, press "Save & Deploy."

For rules that are only saved, users must click Redeploy on the rule management screen for the rules to take effect on the system.

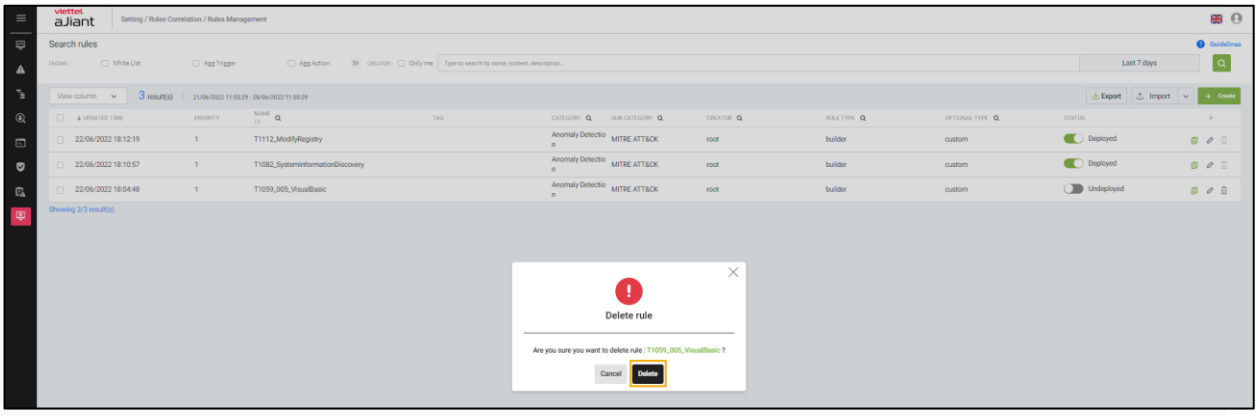
Note: When there is an error, users can click Preview to view the error.

3.9.3 Delete Rules Correlation

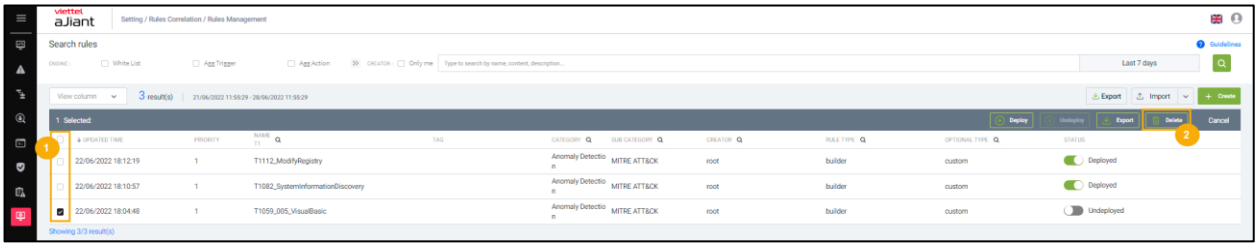


Steps to delete one rule:

- Click the "Delete" icon on the rule you want to delete;
- The screen displays a delete confirmation message, select "Cancel" or "Delete";

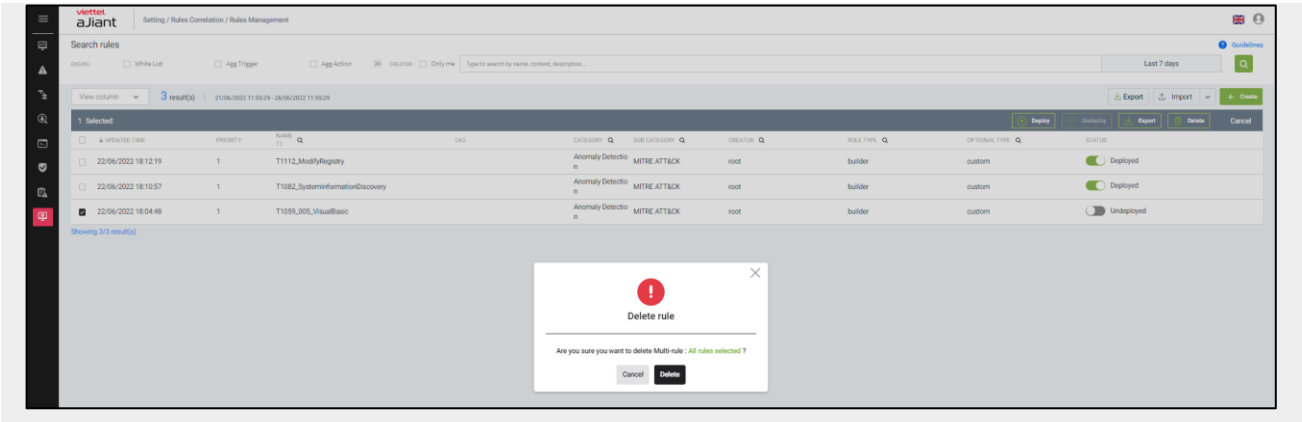


If "Delete" is selected, the chosen rule will be removed from the display screen;



Steps to delete multiple rules:

- Click to select the rules you want to delete (You can delete all by clicking Select all rules);
- The screen displays a delete confirmation message; select "Cancel" or "Delete."



- Select "Delete" to remove all rules from the display screen. Select "Cancel" to abort the current operation.

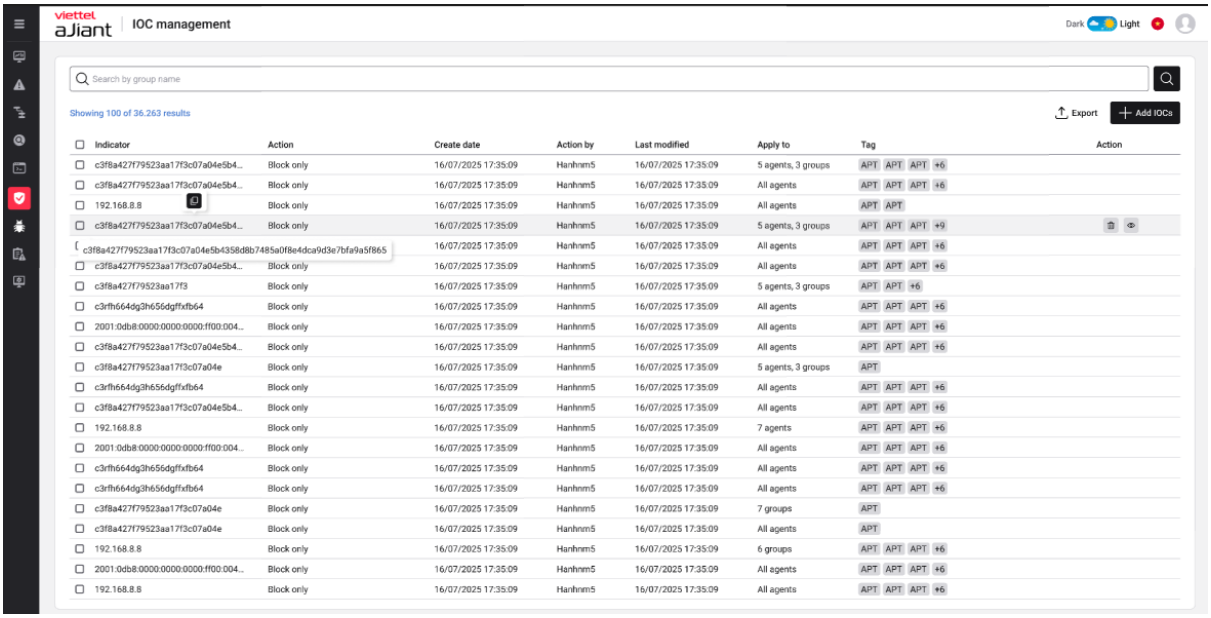
3.10 Protection & Prevention

3.10.1 IOC Management

Purpose: The IOC Management function acts as an "active shield" to help administrators control and protect the system through three main objectives:

- Application Execution Control: Thoroughly prevent the launch of unfamiliar software, unsafe applications, or blacklisted applications directly on users' workstations.
- Monitoring and Blocking Malicious Connections: Monitor internet traffic, automatically detect and disconnect from suspicious addresses (IPs/Domains) to prevent unauthorized access or data theft.
- Proactive Malware Prevention: Protect critical data and applications by early detection of attack signs (IOC), thereby isolating threats before malware can harm the system.

View list of rule



Step 1: The customer logs into the system using an account with iocmanagement_manage and iocmanagement_read permissions.

Step 2: In the menu -> Click on the Protect & Prevent tab -> Click on the IOC Management tab.

The data table screen displays the following information:

o Indicator: Name of the hash/IP

o Action: Displays the action taken on the hash/IP, including: Block only

o Create date: Time the rule was created

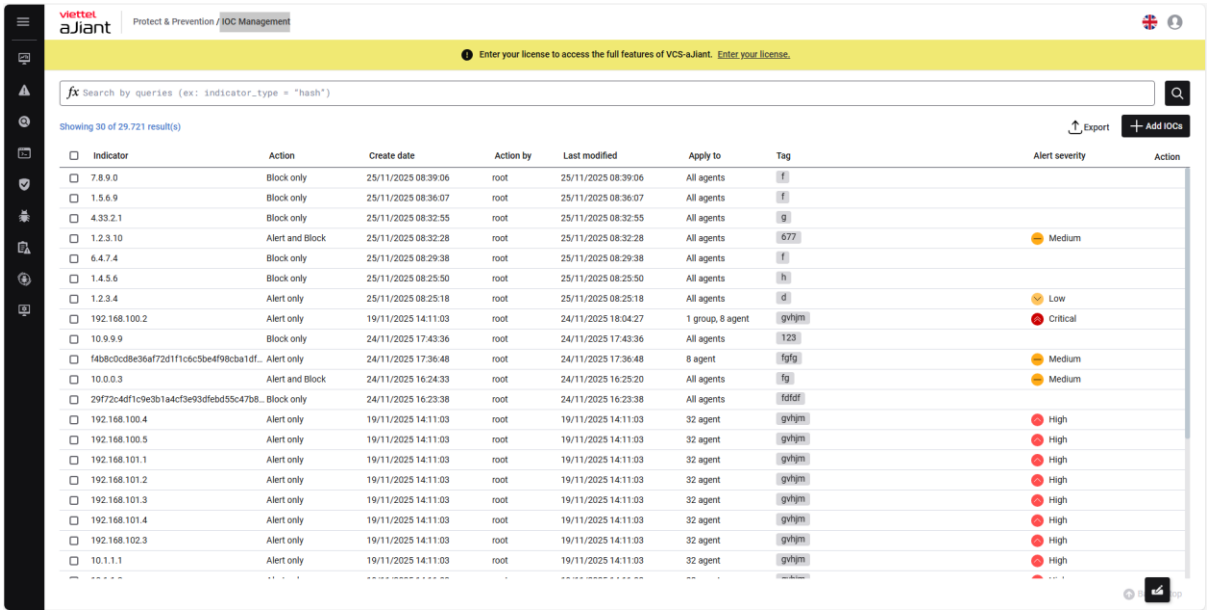
o Action by: User who performed the last action on the hash/IP

o Last modified: Time the rule was last modified

o Apply to: Displays the agent assigned to the rule

o Tag: Displays the tag assigned to that hash/IP

o Action: Displays the Delete and View icons

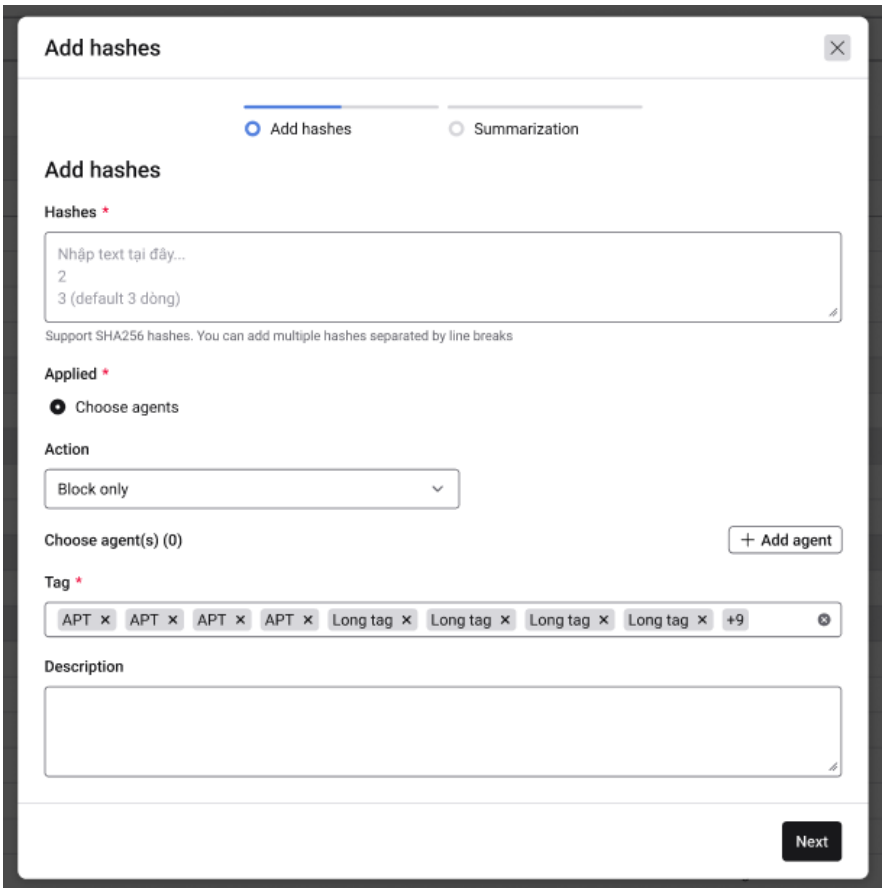


Add new hashes/IP

Add new hashes

Step 1: The customer logs into the system using an account with iocmanagement_manage and iocmanagement_read permissions.

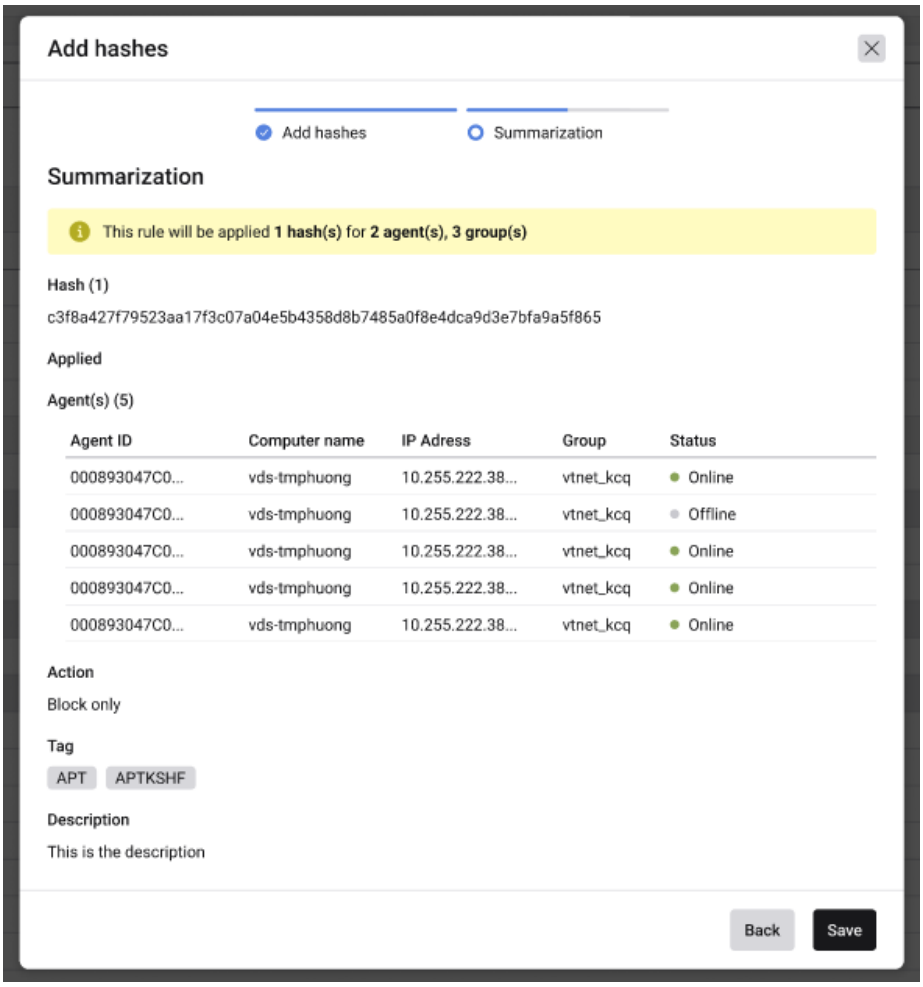
Step 2: On the IOC Management screen -> Click the [Add IOCs] button -> Click [Add hashes] to open the Add hashes popup.



Step 3: Fill in all required fields

- "Hashes" field (required): Enter one or more SHA256 codes, separated by line breaks (maximum 50 codes)
- "Applied" field (required): Default selection is Choose agents
- "Action" field (required): Default selection is Block only
- "Tags" field (required): Enter characters -> Press Enter to complete tag entry
- "Description" field (required): Enter a maximum of 255 characters

Step 4: Click the [Next] button to move to the "Summarization" tab

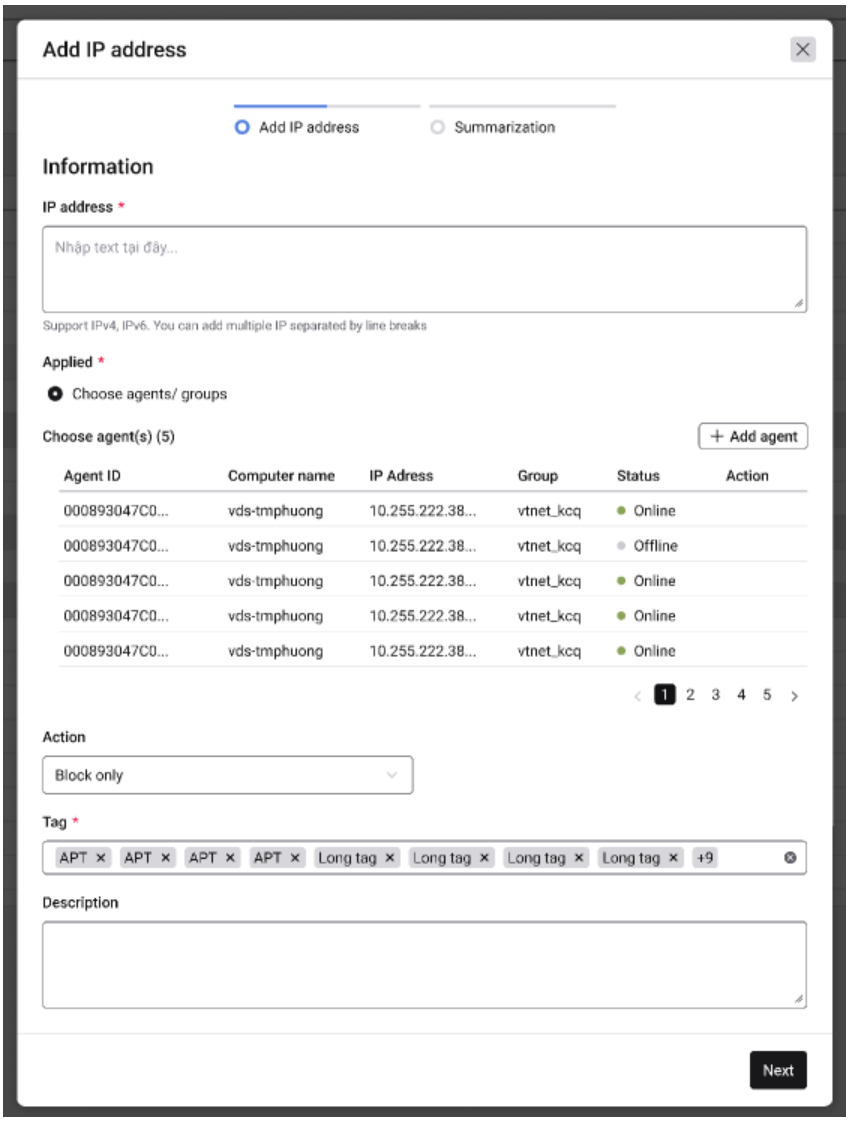


Step 5: Click the [Apply] button in the "Summarization" tab.
Step 6:
- A message "Add IOC successfully" will be displayed.
- The hash has been successfully created.
- The screen will return to the IOC list screen.
- The newly created hash will be displayed at the top of the list screen.

Add new IP

Step 1: The customer logs into the system using an account with iocmanagement_manage and iocmanagement_read permissions.

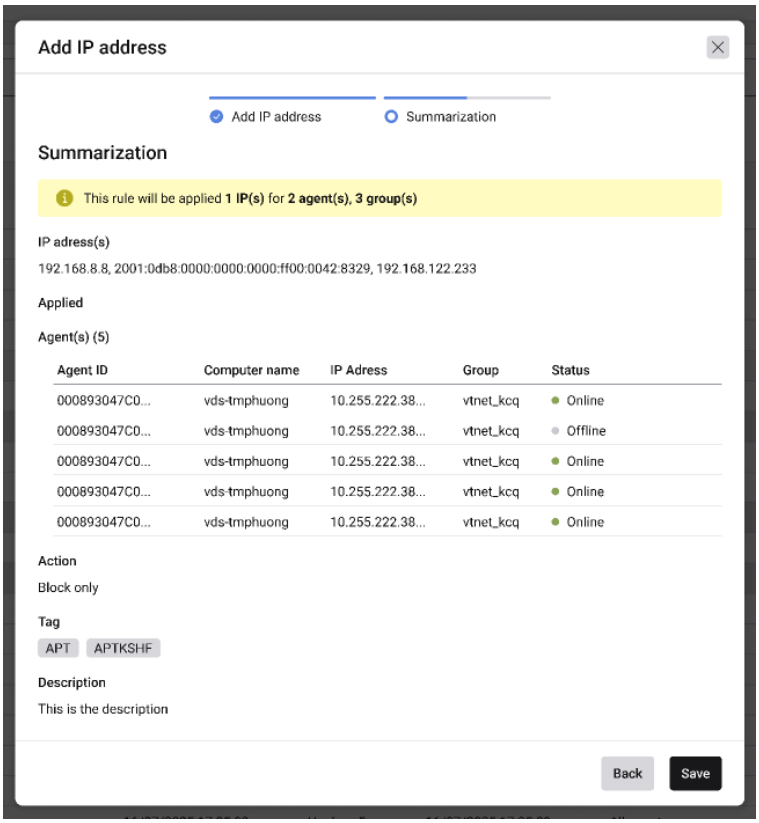
Step 2: On the IOC Management screen -> Click the [Add IOCs] button -> Click [Add IP] to open the Add IP popup.



Step 3: Fill in all required fields

- "IP" field (required): Enter one or more IPV4/IPV6 codes, separated by line breaks (maximum 50 codes)
- "Applied" field (required): Default selection is Choose agents
- "Action" field (required): Default selection is Block only
- "Tags" field (required): Enter characters -> Press Enter to complete tag entry
- "Description" field (required): Enter a maximum of 255 characters

Step 4: Click the [Next] button to move to the "Summarization" tab



Step 5: Click the [Apply] button in the "Summarization" tab.

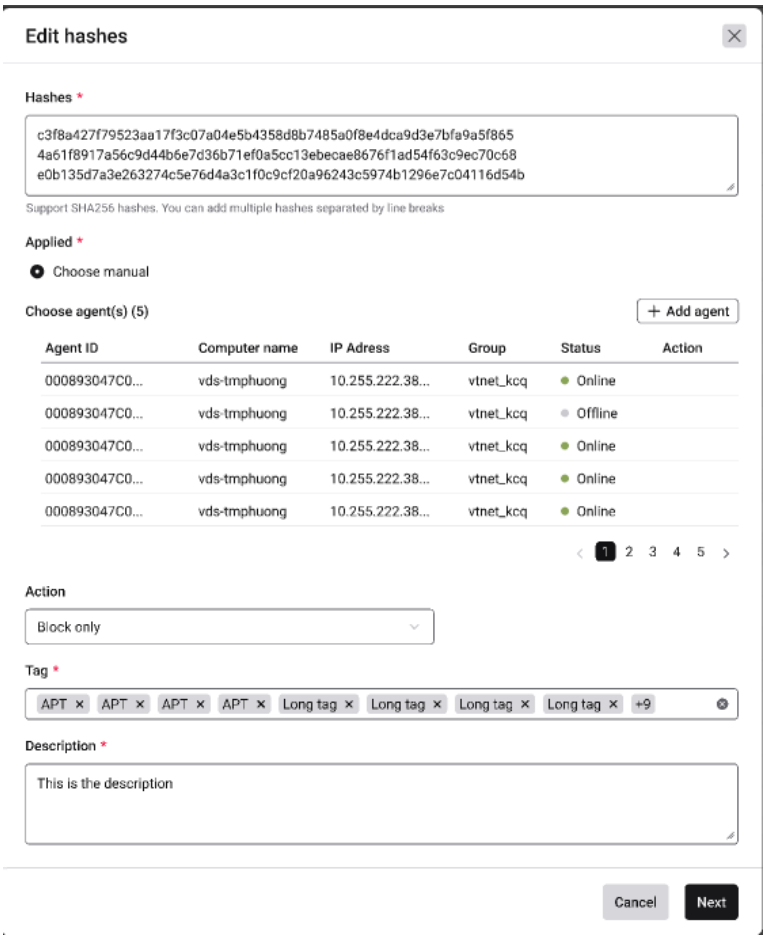
Step 6:

- Display the message "Add IOC successfully".
- New IP successfully created.
- The screen returns to the IOC list screen.
- The newly created hash is displayed at the top of the list screen.

Update a rule block

Step 1: The customer logs into the system using an account with iocmanagement_manage and iocmanagement_read permissions.

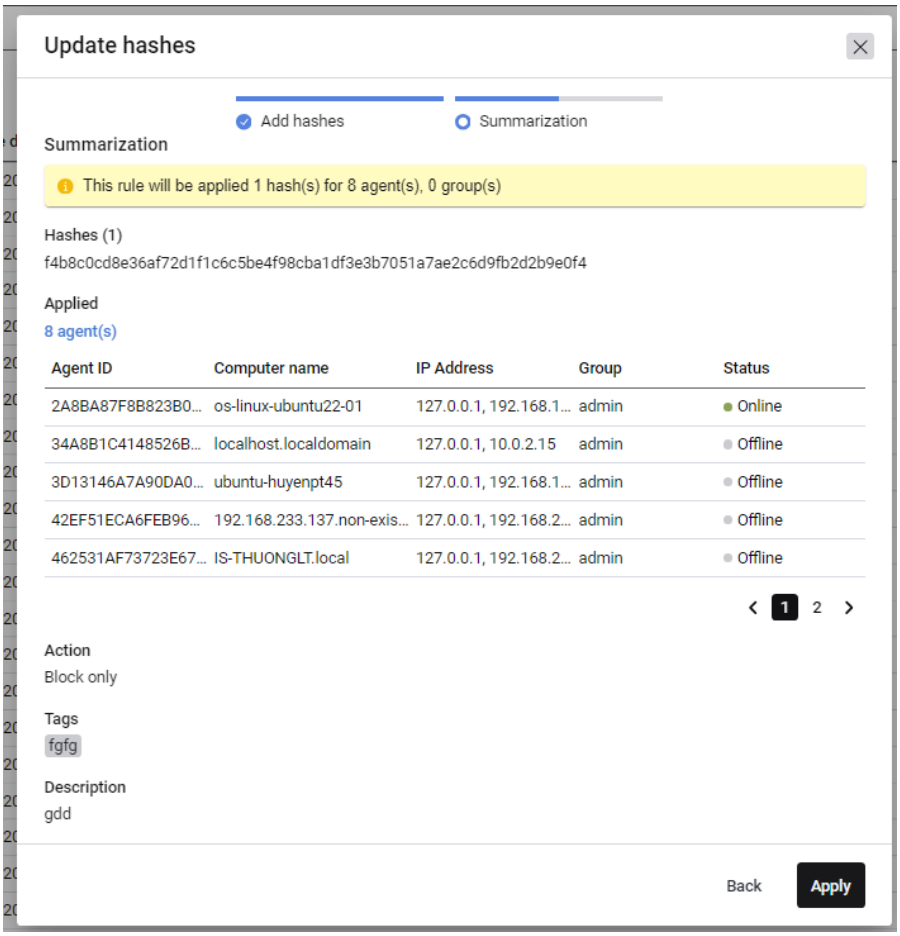
Step 2: On the IOC Management screen -> Click on the view icon of any record to open the Edit popup.



Step 3: Make changes to the fields as desired:

- "Applied" field (required): Default selection is Choose agents
- "Action" field (required): Default selection is Block only
- "Tags" field (required): Enter characters -> Press Enter to complete tag entry
- "Description" field (required): Enter a maximum of 255 characters

Step 4: Click the [Next] button to move to the "Summarization" tab



Step 5: Click the [Apply] button in the "Summarization" tab to update the hash/IP.
Step 6:
- A message "Update IOC successfully" will be displayed.
- The rule update was successful.
- The screen will return to the IOC list screen.
- The newly updated rule will be displayed at the top of the list screen.

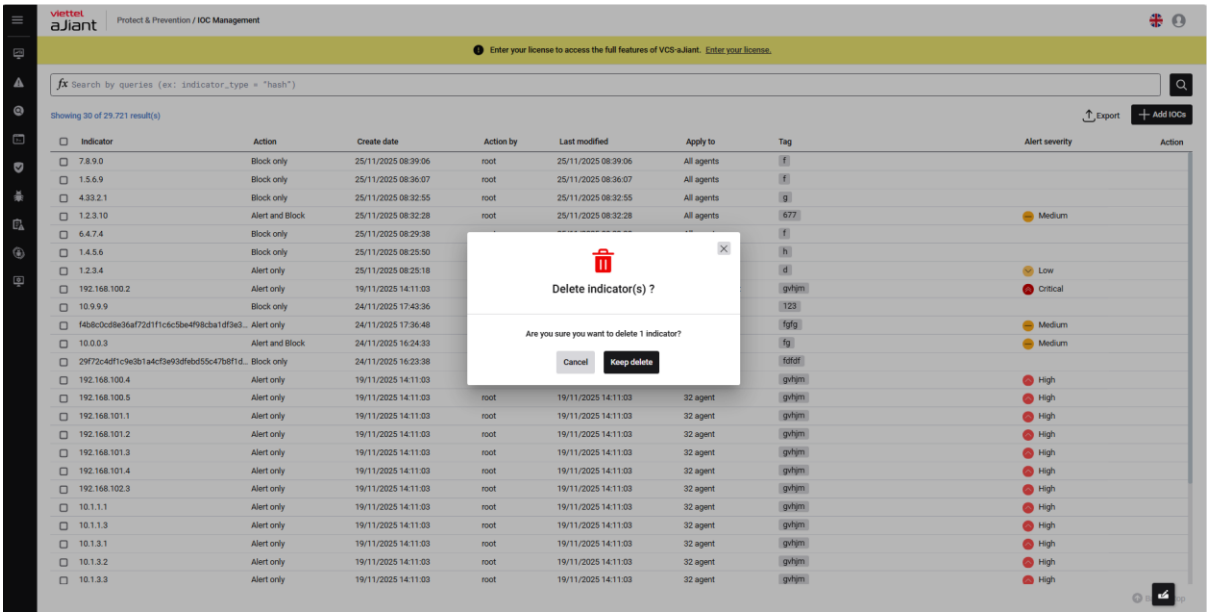
Delete a rule block

Step 1: The customer logs into the system using an account with iocmanagement_manage and iocmanagement_read permissions.

Step 2: On the IOC Management screen:

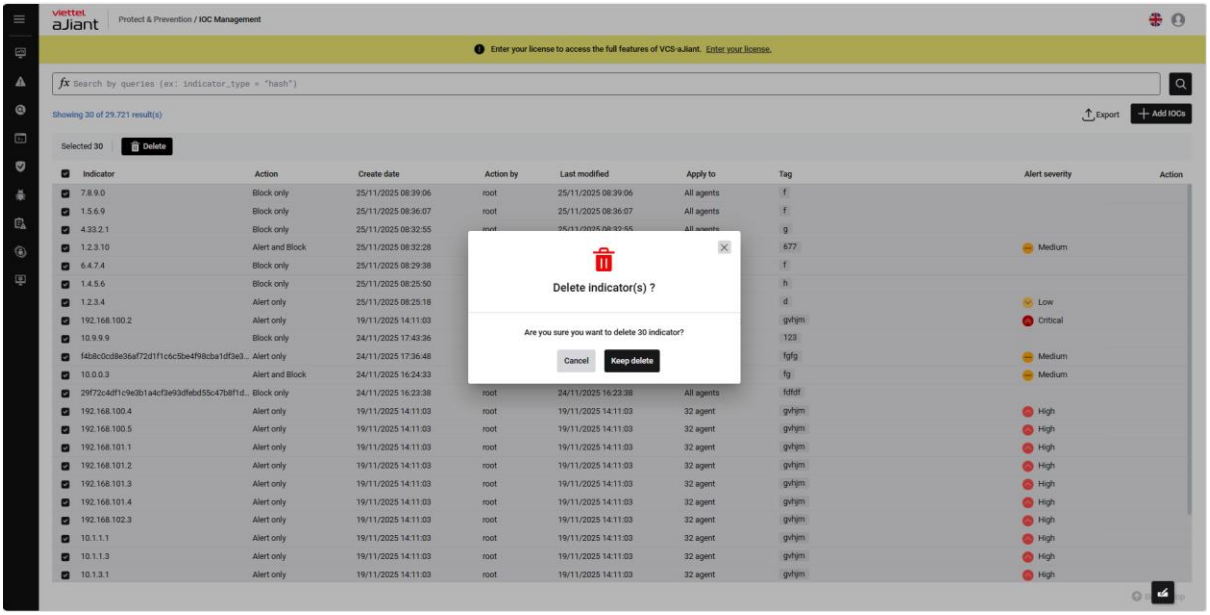
o In case of deleting a rule:

Hover your mouse over the Action column -> Click the [Delete] icon next to any rule you want to delete.



o In case of deleting multiple rules:

Check the rules you want to delete -> Click the [Keep delete] button



Step 3: Click the [Keep delete] button to confirm deleting the rule.

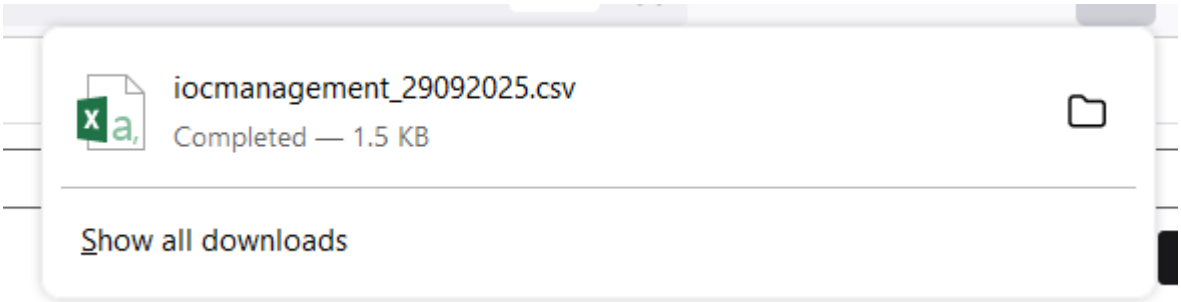
Step 4:

- A message "Deleted successfully" will be displayed.

- The screen will return to the IOC list screen.
- The deleted record will be removed from the list and database.

Export rule block

Step 1: The customer logs into the system using an account with iocmanagement_manage and iocmanagement_read permissions.
Step 2: On the IOC Management screen, click the [Export] button.
Step 3: The export file is successfully downloaded to the computer.
- The export file contains all the fields and corresponding data on the portal:
o Indicator: Name of the hash/IP
o Action: Displays the action taken on the Hash/IP
o Create date: Time the rule was created
o Action by: User who performed the last action on the hash/IP
o Last modified: Time the rule was last modified
o Apply to: Displays the agent assigned to the rule
o Tag: Displays the tag assigned to that Hash/IP
- The downloaded file is in CSV format with the filename: iocmanagement_ddmmyy (ddmmyy is the download time)



Search rule block

Step 1: The customer logs into the system using an account with iocmanagement_manage and iocmanagement_read permissions.

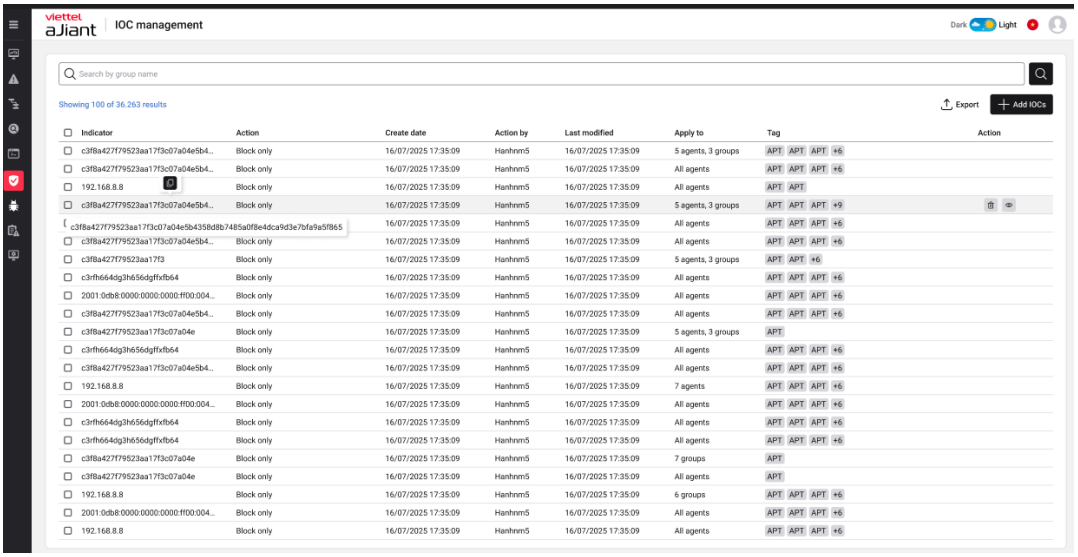
Step 2: On the IOC Management screen, click the search bar.

Step 3: Perform a search using a query.

Example: Search by indicator: indicator = "2.2.2.2"

Step 4: Click the [Search] button to perform the search.

Step 5: Display the search results that meet the search criteria.



3.11 Anti-Malware

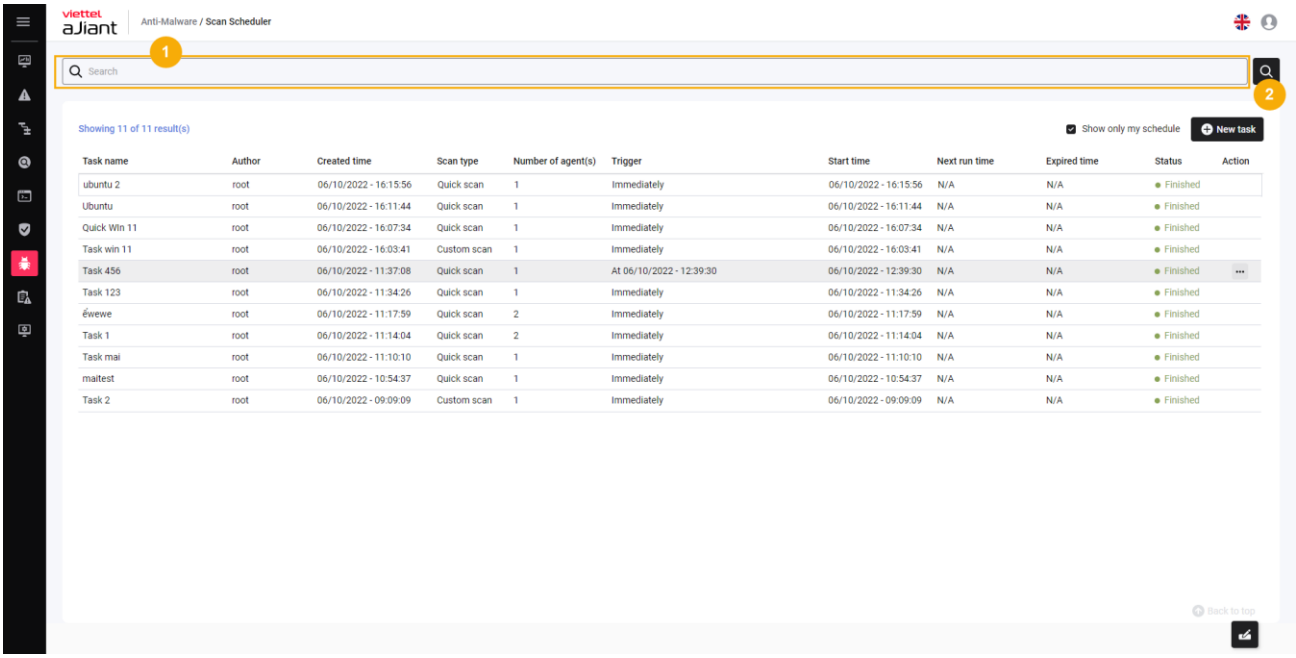
3.11.1 Scan Scheduler

Purpose: The Scan Schedule function allows users to remotely schedule virus scans on workstations.

Search for Scan Schedule task

Purpose: The Scan Schedule task search function allows users to search for scan schedules on workstations by Task name.

Steps to follow:



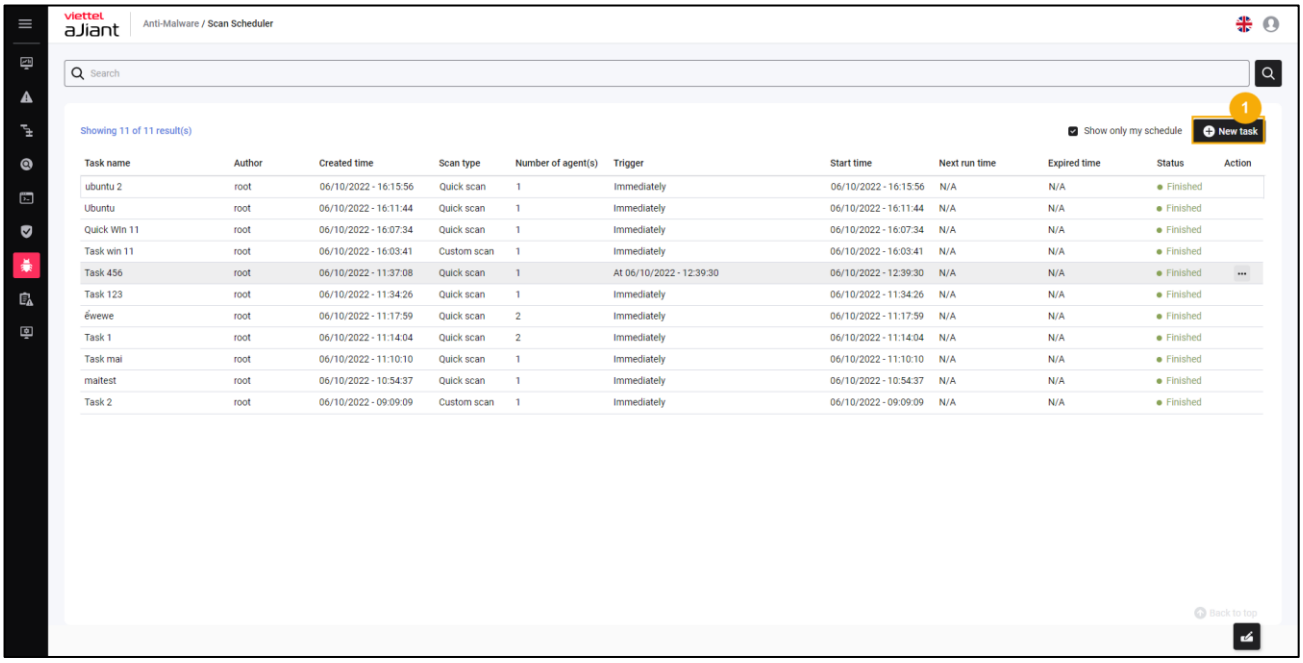
- The user enters the search keyword;
- Select the button or press Enter to confirm the search action with the entered keyword.
- The system will display a list of scheduled scans based on the search keywords.

Add new Scan Schedule task

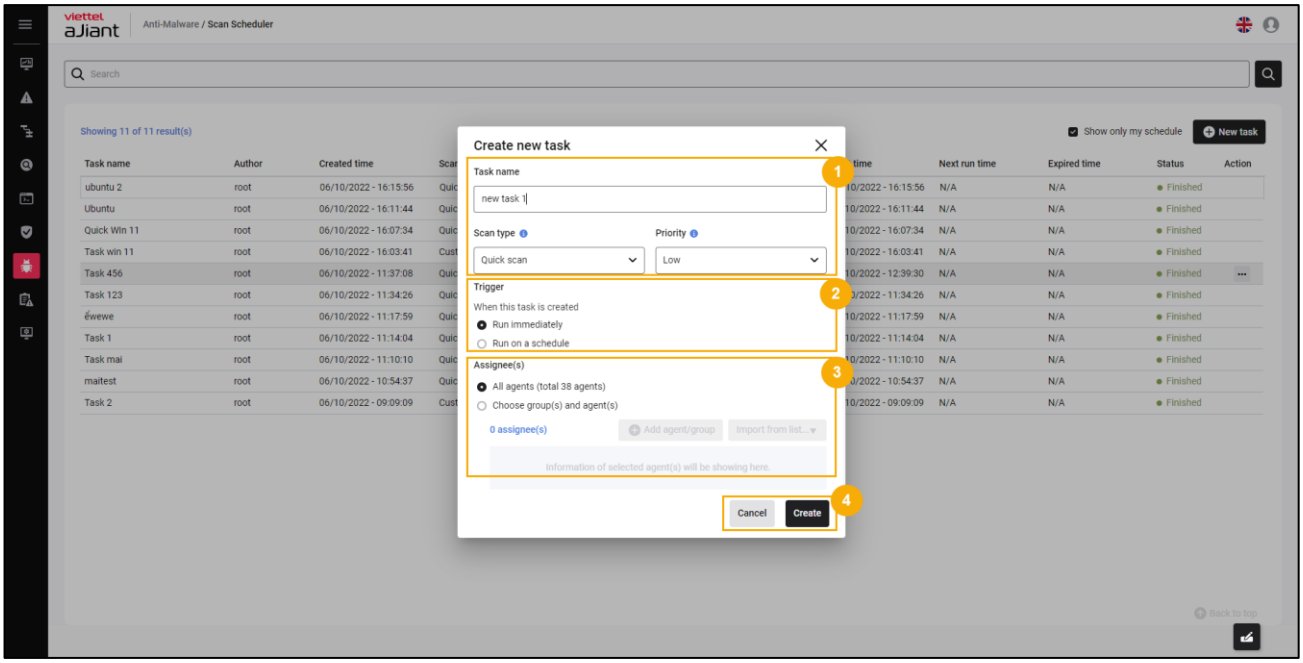
Purpose: To allow users to add a new scan schedule, configure the timing, and input workstation information.

Steps to follow:

- On the scan schedule list screen, the user selects the New task button.



- The system displays a screen for adding a new scan schedule, where the user enters the following information:



1 – The scan scheduling information includes: Task name, Scan type, Priority.

Task name: User enters the name of the scan scheduler;
Scan type: The user selects one of the three scan types. Allowed:

Quick Scan: Rapidly check files and folders for potential suspicious items;

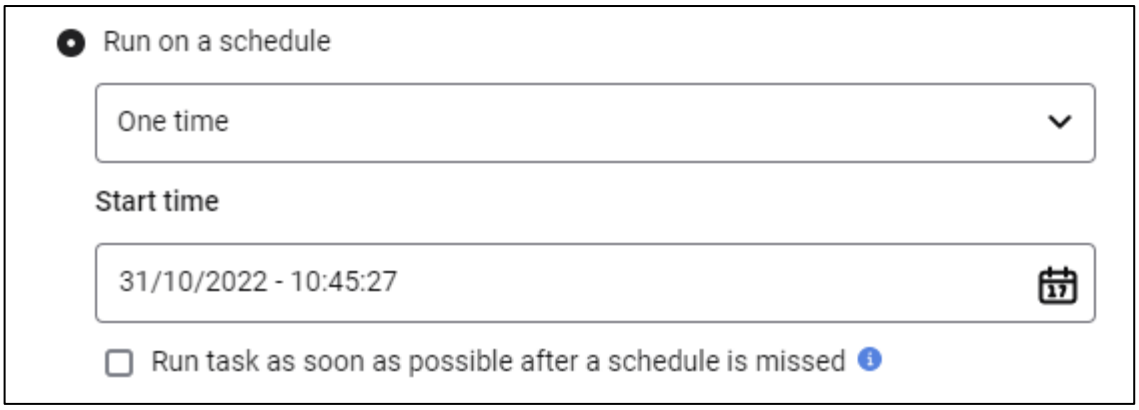
Full scan: Checks all files and folders on the computer. This process may take several hours to complete;

Custom Scan: Allows users to select a specific file or folder on their computer to scan.

Priority: Allows users to select the scan speed and adjust the level of resource usage on the machine. When set to high priority, the system will scan quickly but will consume more CPU resources. Conversely, if a low priority level is chosen, the system will scan more slowly and conserve CPU resources.

2 – Trigger information allows users to select the type of scan scheduling:

Run immediately: Allows users to schedule an immediate scan on workstations as soon as the task is successfully created;
Run on Schedule: Allows users to schedule scans according to their configuration.



Schedule:

- One time: Schedule a one-time scan;
- Daily: Schedule daily scans;
- Weekly: Schedule weekly scans;

- Monthly: Schedule monthly scans;

Start time: Allows users to enter the scan scheduling start time.

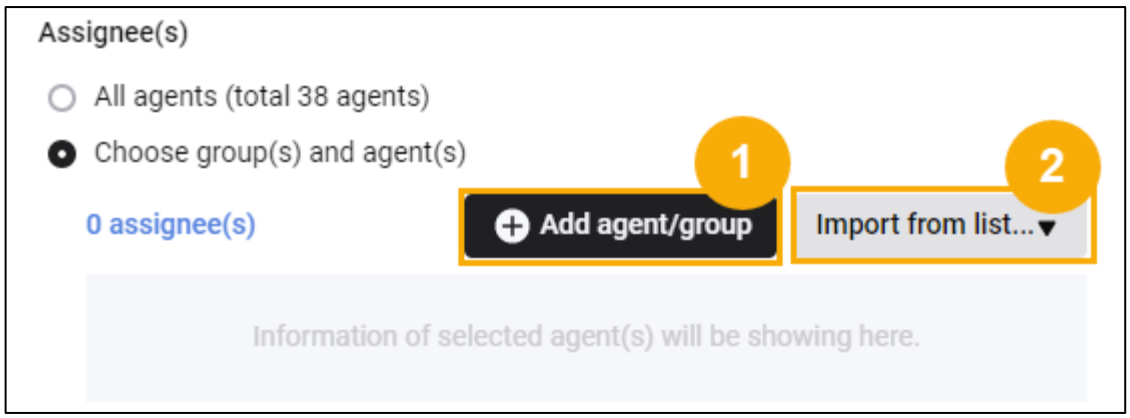
Example: Schedule: Daily, Start time: 15/08/2022 – 03:00:00. This is understood as configuring a daily scan schedule at 03:00:00.

Run task as soon as possible after schedule is missed: Allows users to configure the scan schedule to run immediately if the previous schedule was missed.

3 – Assignee Information: Allows users to configure information for workstations receiving scheduling tasks.

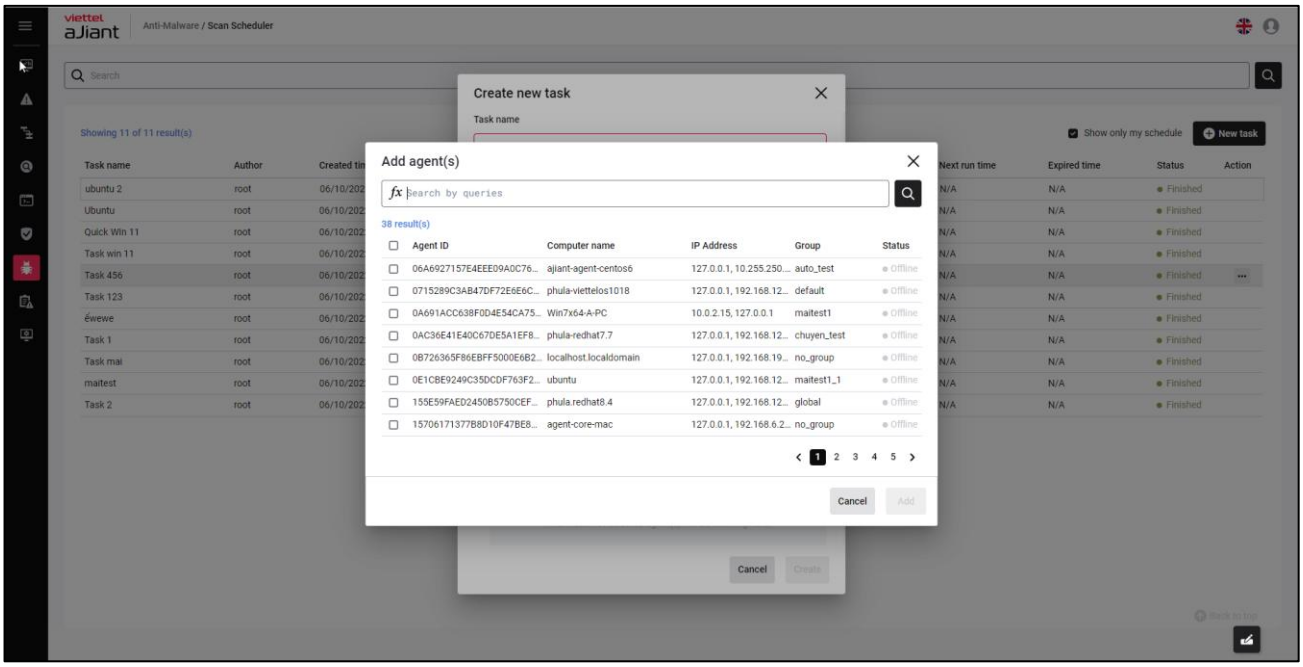
All Agent(s): Schedule with all workstations managed by the currently logged-in user;
Select Agent(s) or Group(s):

Purpose: To allow configuration and selection of workstations or groups of workstations:

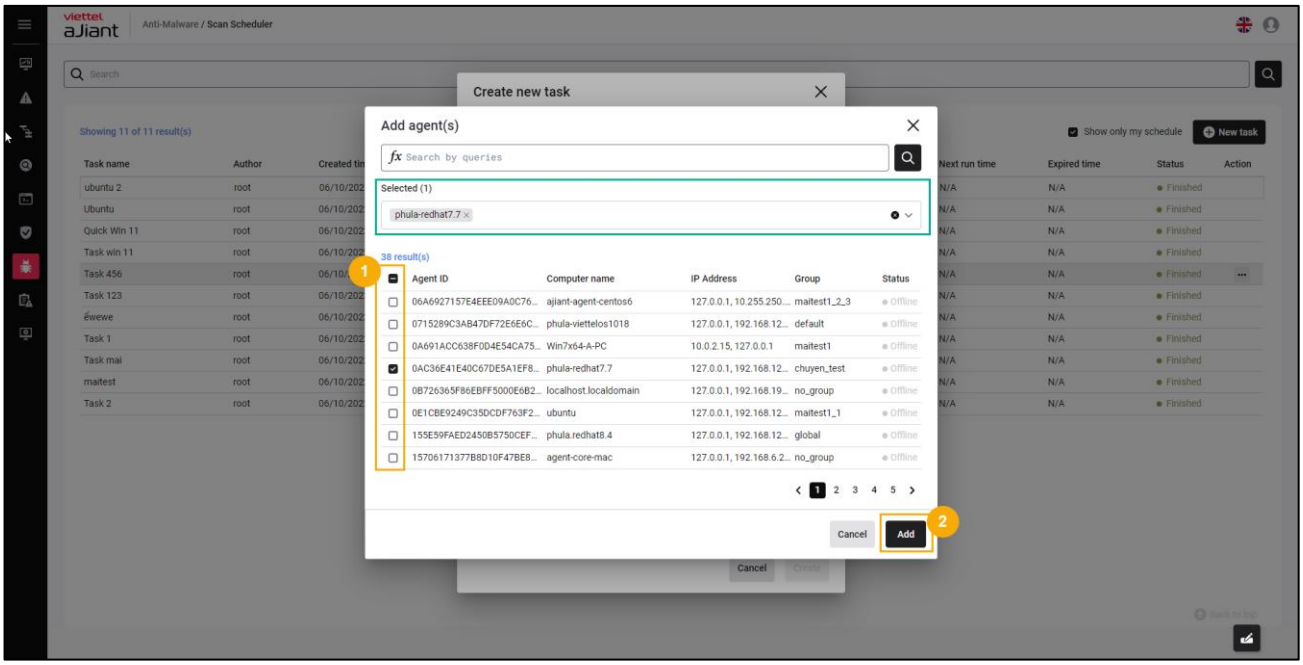


Steps to follow: Add Agents or Group

- Add Agents or Group - The user selects Add Agent. The system displays a popup for selecting a workstation:



- Search for workstations:
  - In the Add agent(s) popup, users can search for workstations using query fields such as AgentID, Computer name, IP Address, Group, Status, and more.
  - The user selects the icon or presses the Enter key to confirm the search;
  - The system will display the list of workstations according to the query.
- Select one or more workstations to execute the scan scheduling:



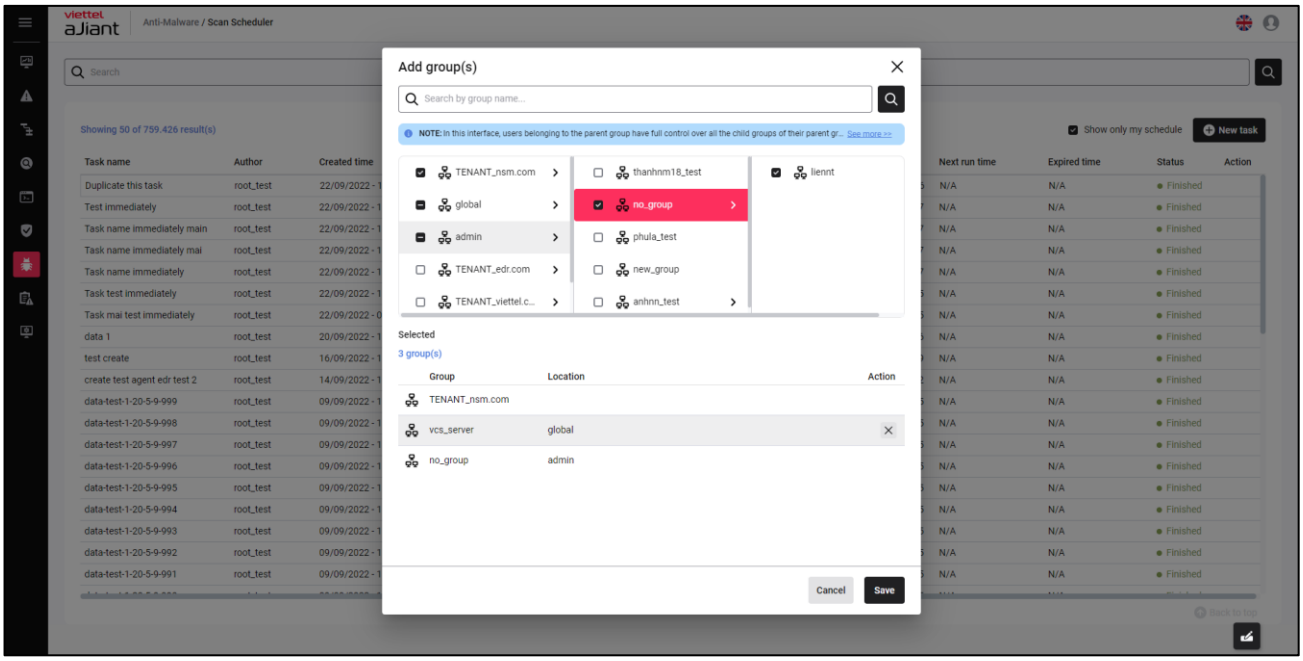
- Select the Add button to add Agent/Group information → HT returns to the Agent/Group list;
- Or select the Cancel button to cancel the action of adding Agent/Group information;

➔ The list of selected workstations will be automatically added to the selected workstation information frame.

- Add Agents or Group - The user selects Add Group. The system displays a popup to choose a group:
  - Search for group:
    - In the Add group(s) popup, users can search for workstations by querying the following information fields: Group name.
    - The user selects the icon or presses the Enter key to confirm the search;

➔ The system will display the list of groups.

- Select one or more groups to execute the scan scheduling:



- Select the Add button to add Agent/Group information → HT returns to the Agent/Group list;
- Or select the Cancel button to cancel the action of adding Agent/Group information;

➔ The list of selected workstations will be automatically added to the information frame of the chosen group.

Import from .CSV: Allows users to upload a list of workstations by:

- Select the Import from list button;
- Selecting Download sample file allows you to download a sample workstation list file;
- The user enters workstation information and uploads the workstation list file by selecting the Import from .CSV button.

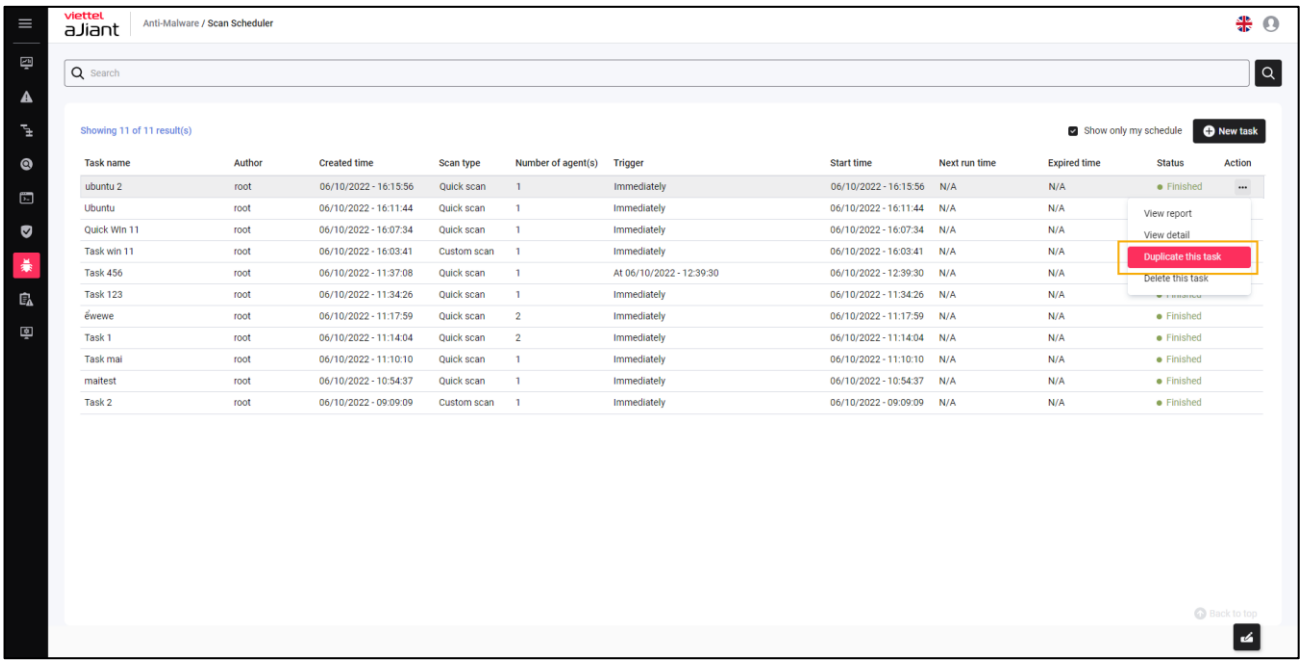
- The user selects the Create button to complete the process of adding a new scan schedule. Alternatively, select the Cancel button to cancel the addition of a new scan schedule.

Clone Schedule Task

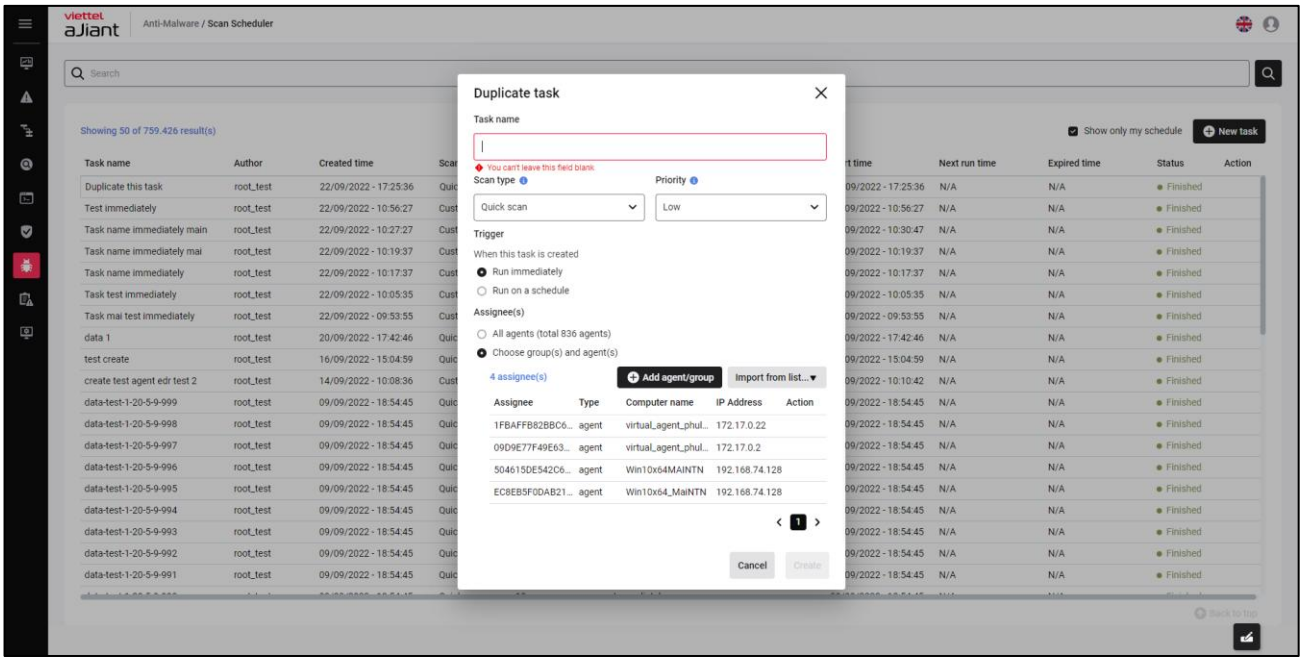
Purpose: To allow users to duplicate scan schedules.

Steps to follow:

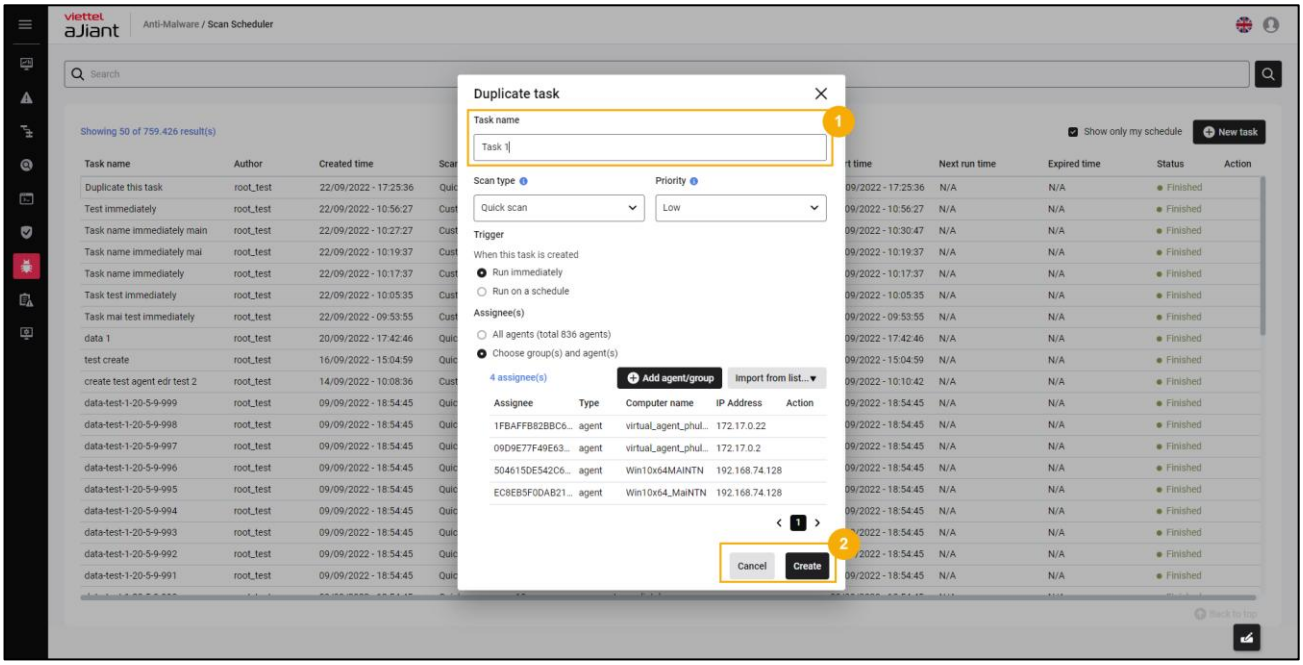
- On the task list screen, the user selects Duplicate for the task record that needs to be copied:



- The system displays the Duplicate Task screen, where the user re-enters the task name and reviews all information before duplicating.



- The user selects the Create button to complete the scan schedule duplication process. Alternatively, select the Cancel button to cancel the scan schedule duplication process.



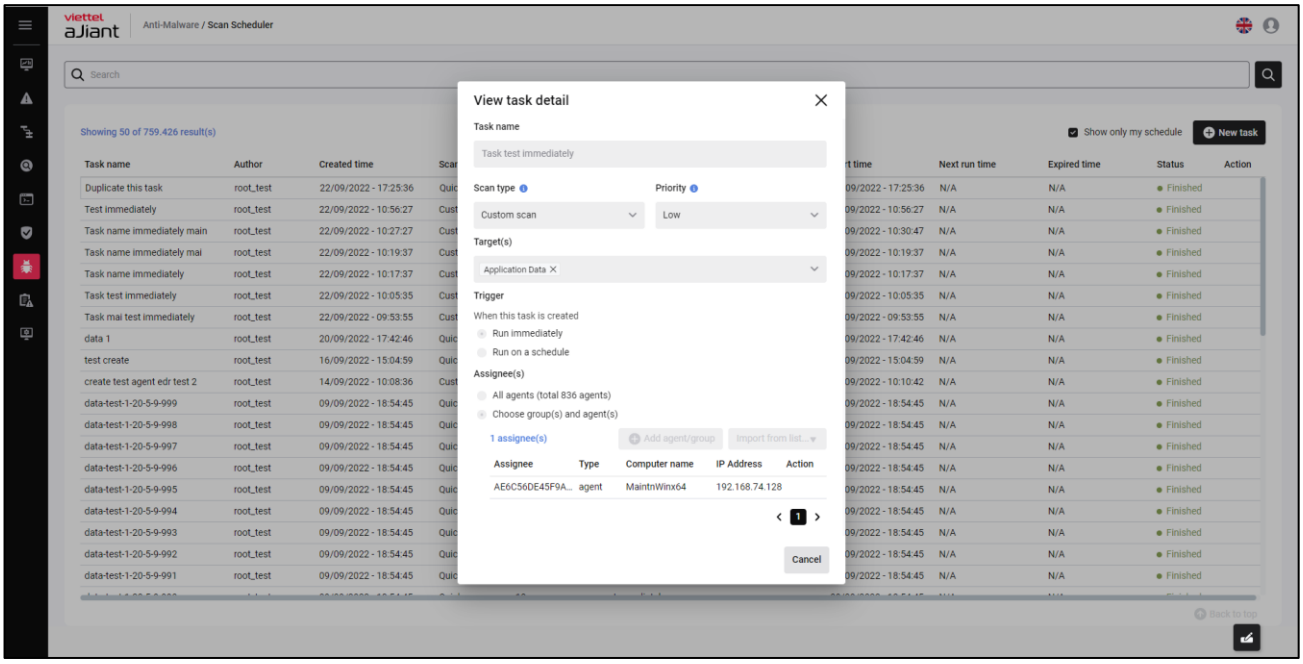
View details

Purpose: To allow users to view detailed information about the scan schedule.

Steps to follow:

- On the task list screen, the user selects View Detail for the task record they want to view in detail;

➔ System display for detailed scan scheduling screen



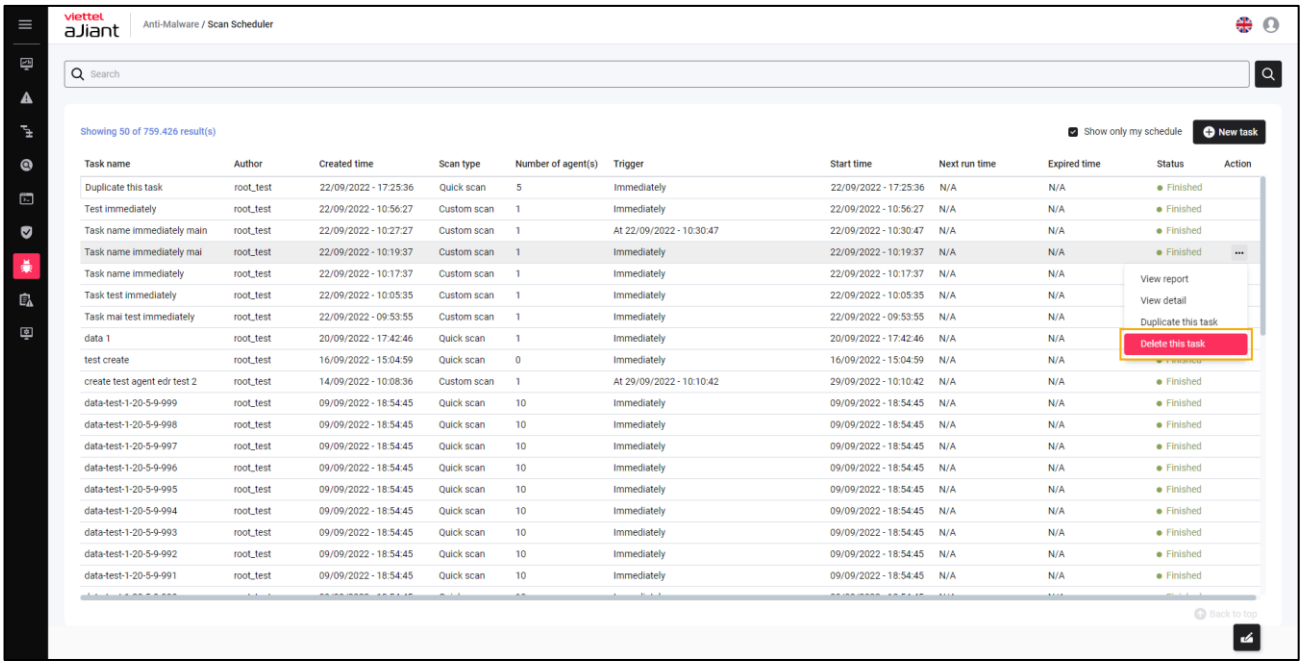
- The user selects the Cancel button or the Close icon to cancel the action of viewing the scan schedule details.

Delete Scheduled Task

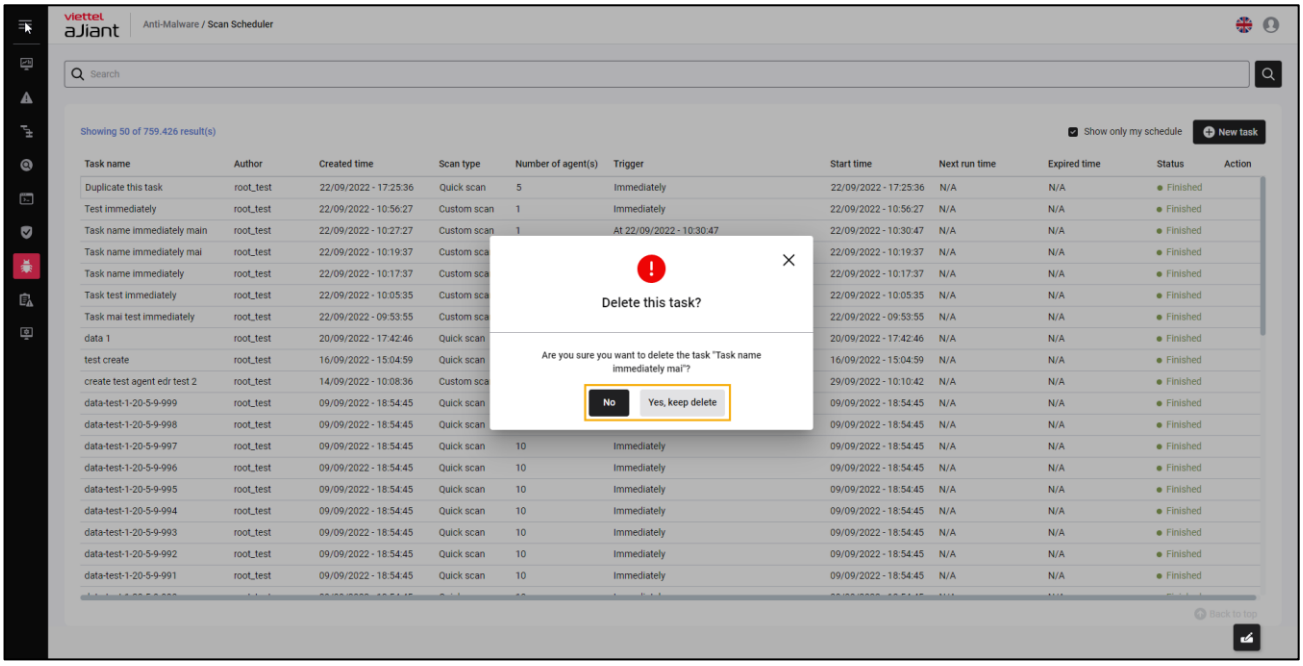
Purpose: Allow deletion of scan schedules in the task list;

Steps to follow:

- On the task list screen, the user selects Delete this task for the task record to be deleted;



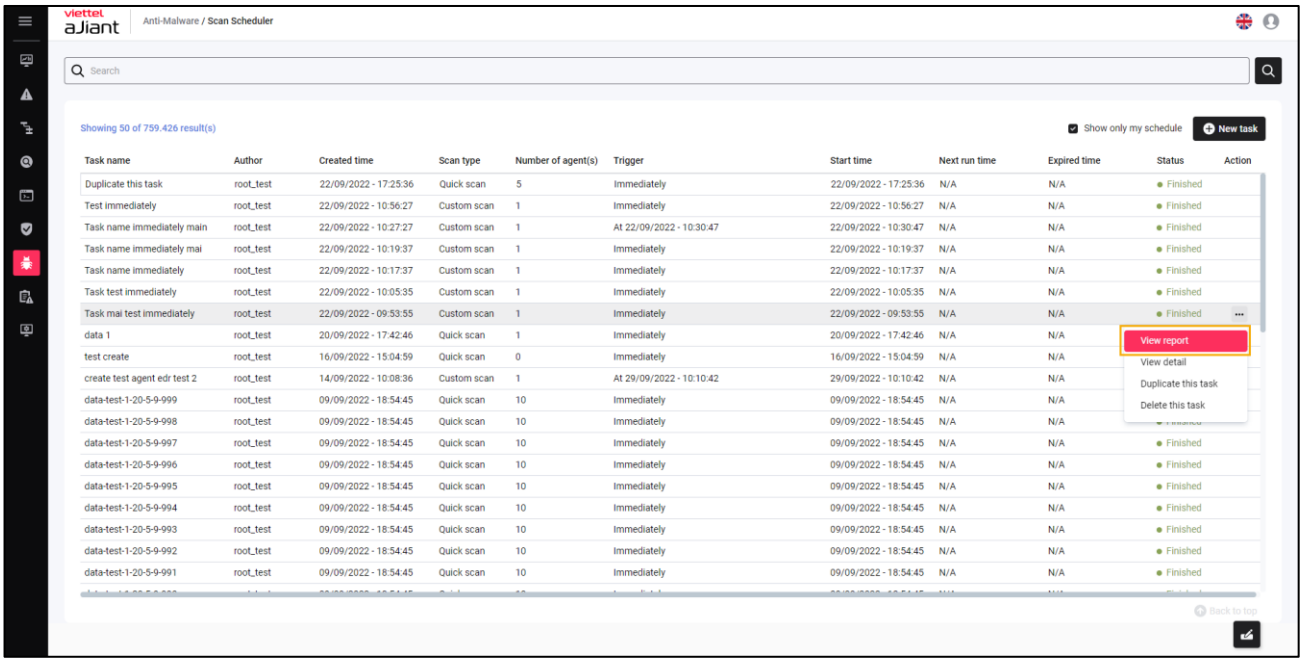
- The system displays a popup screen for Delete Confirmation. The user selects No to cancel the scheduled scan deletion or selects Yes, keep delete to proceed with the deletion.



View report

Purpose: To allow users to view the scheduled scan reports;
Steps to follow:

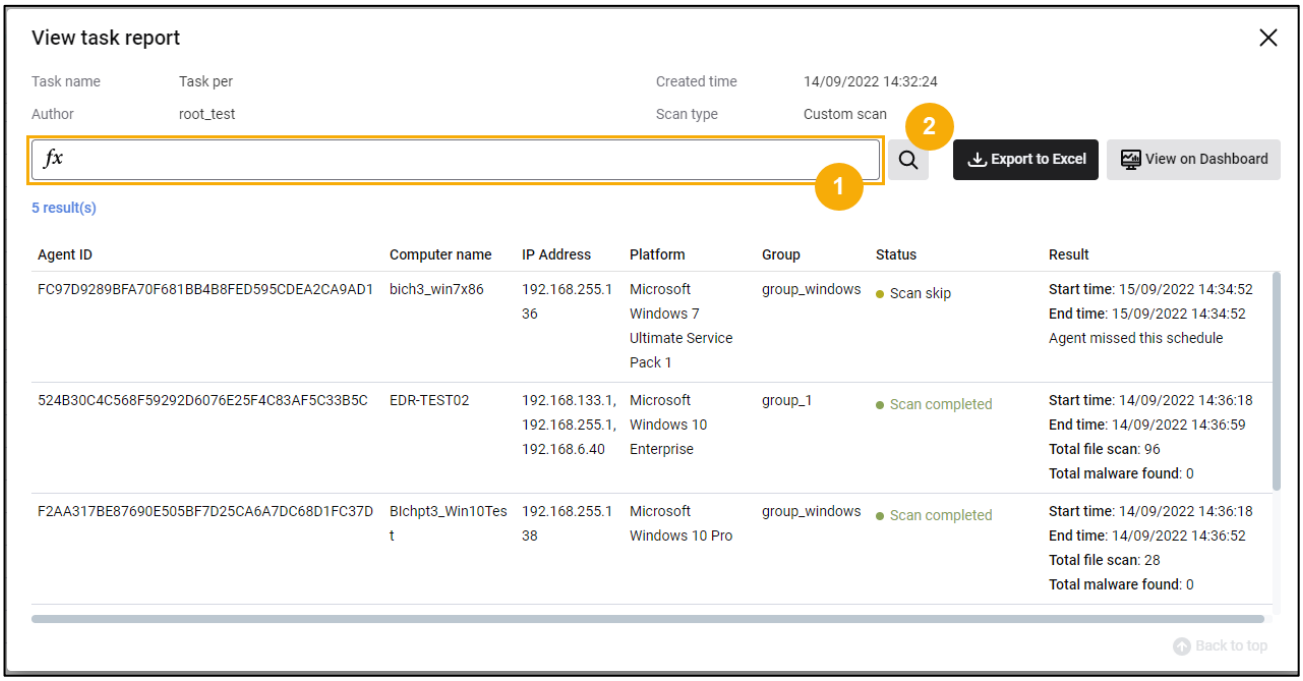
- On the task list screen, the user selects View report for the task record they want to view the report for;



- View report display system:

1 – Search:

Purpose: To enable query searches for information in the report such as AgentID, Computer Name, IP Address, Platform, Group, Status, and Result.
Steps to follow:

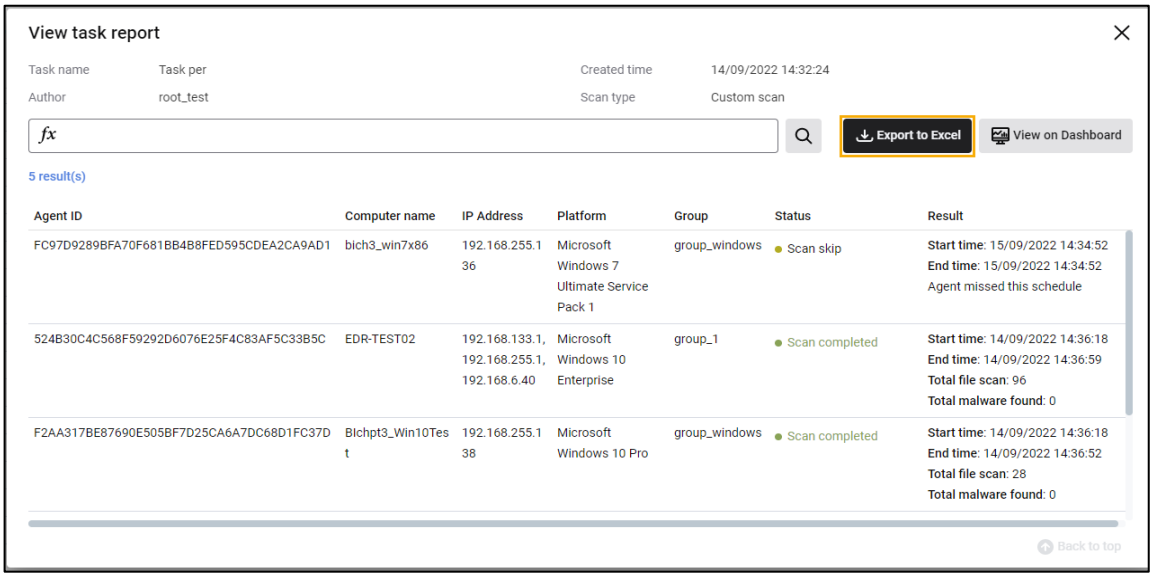


The user enters the query information and selects the icon or presses the Enter key to confirm the query;

➔ The system displays the list of scheduled scan report results after the query.

2 – Export to Excel

Purpose: To allow users to download the scan scheduling result report in Excel file format;

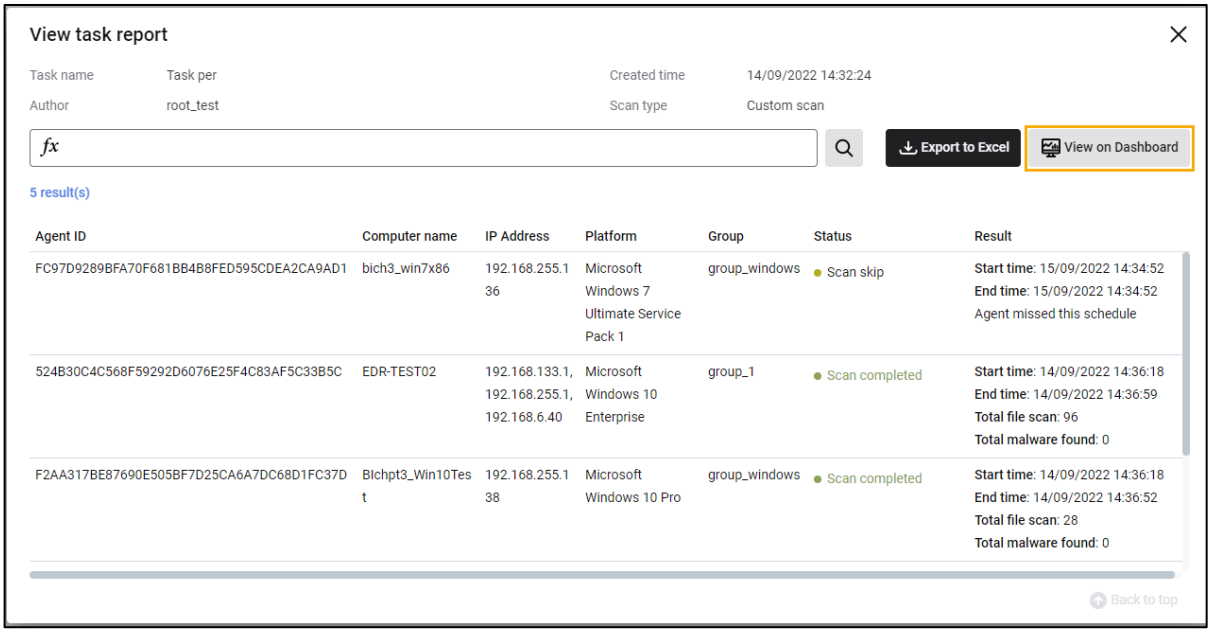


Steps to perform: On the View task report screen, the user selects the Export to Excel button.

➔ The system allows downloading the scheduled scan report result file.

3 – View on dashboard

Purpose: To allow viewing of the system's Anti-malware statistical report.



Steps to perform: On the View task report screen, the user selects the View on dashboard button.

➔ Navigation system to the system's Anti-malware statistical report page;

3.11.2 Device control

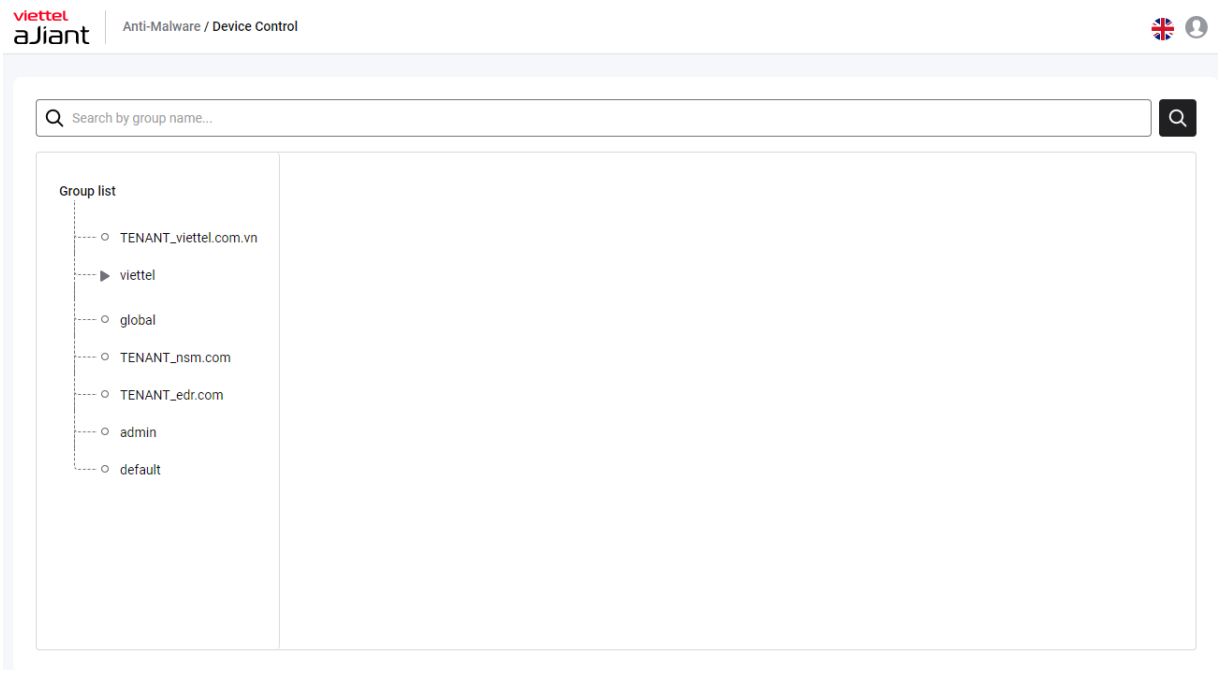
Function: Allows control and protection of important data through peripheral devices such as USB drives, Bluetooth devices, and writable CDs and DVDs.

Purpose: USB devices, CDs, DVDs, and other peripheral devices, while very useful, also pose real threats to the organization. Therefore, it is necessary to manage information and control peripheral devices that access end users' computers.

Search Group

Purpose: The Group search function allows users to display the group list in a tree structure.

Interface screen when accessing the Device Control feature: Anti-malware/Device Control

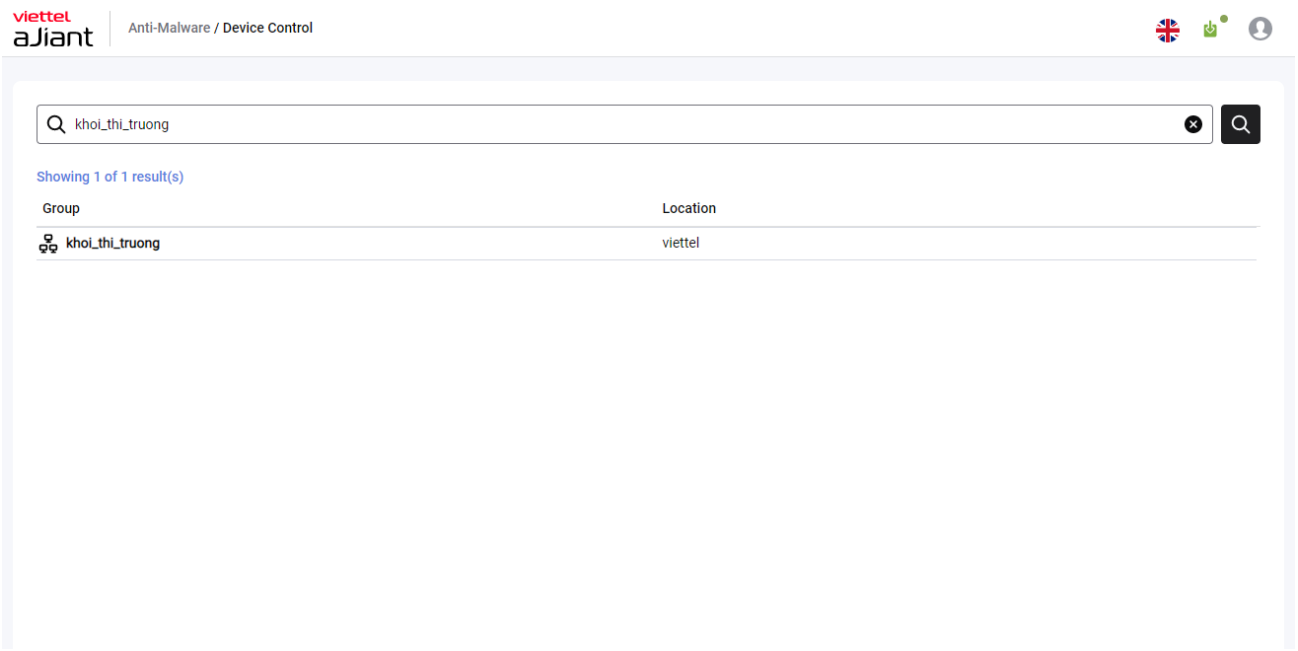


Step 1: The user enters the search keyword in the Search by group name field (with keyword suggestions based on the text).

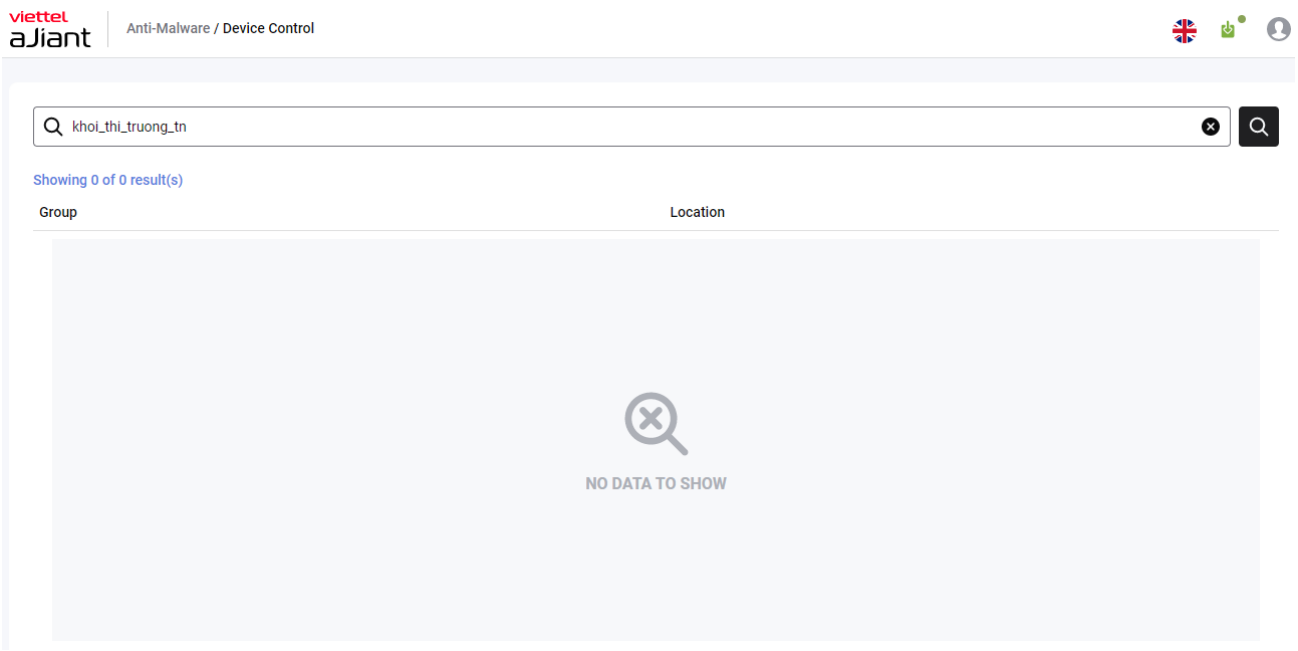
Step 2: Click the button or press Enter to confirm the search action with the entered keyword.

Step 3: The system will display a list based on the search keywords.

If there are results, they will be returned.



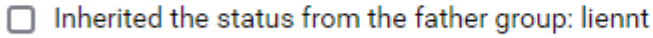
No results found for the search.



Device list of each group

After selecting the desired group to display, the screen will show the Device Type table.

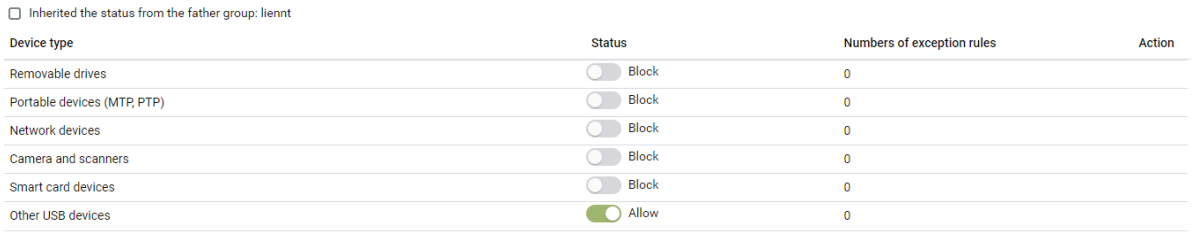
There is a checkbox.



For subordinate groups, when the "inherit" option is checked, they will inherit the status and exceptions from the nearest parent group >> No edit permissions, view-only access.

If unchecked, the opposite applies, allowing add, edit, and delete permissions.

Regarding the Device List Table, it includes the following information fields:



+ Device type: display fixed device name
+ Status: Allow/Block displays the access permission status for each device type for each group.

+ Numbers of exception rules: displays the number of exception rules for each device type in each group.

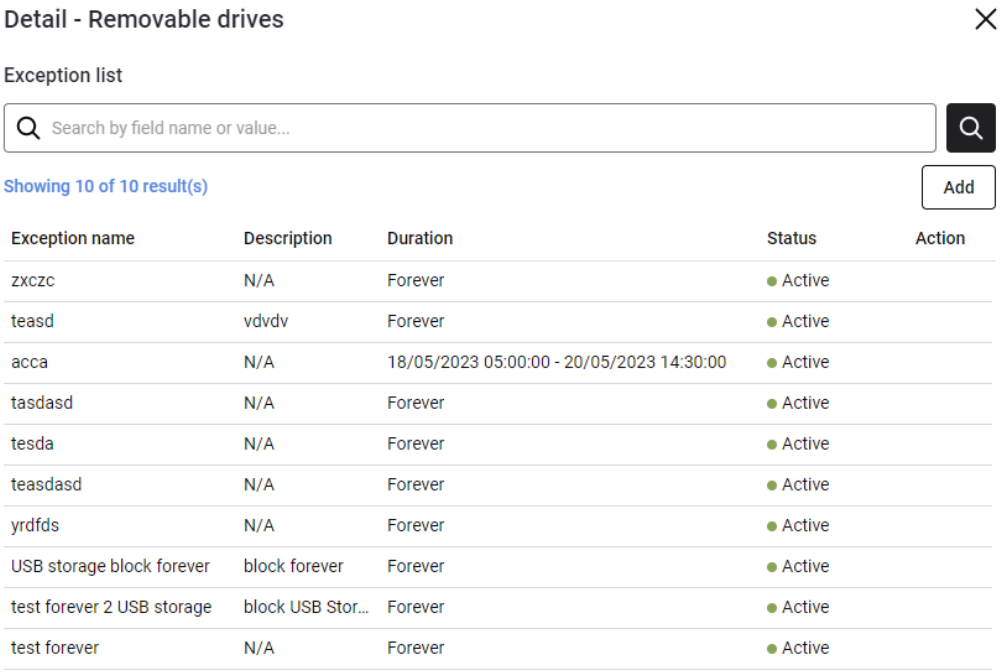
+ Action: Display the Edit Exception icon in the Action column for each record when hovering over the record (Clicking the edit icon => Display the Exception list tab).

Exception Screen

Purpose:

Allow users to view the list of exceptions for device types by group.

Exception list



- Number of exception rules = 0

>> Display message "NO DATA TO SHOW"

- TH Numbers of exception rules != 0

>> Display the list of exceptions corresponding to the device

No results found

>>Display message "NO DATA TO SHOW"

Search results found

>>Check if the entered string partially or fully matches the name field, case-insensitive. When starting to type, a clear icon will appear at the corner of the input. Click the search button or press enter.

Always display the exception list table including the following information fields:

1. Exception name - display the exception name
2. Description - Information to which the exception applies

3. Device(s) - display the device name

4. Duration - displays the duration of the exception

5. Status - displays the status of the exception, including Expired and Active.

If the exception has exceeded the allowed duration compared to the current time, display Status = "Expired".

+ If the exception ensures the duration is allowed compared to the current time, then display Status = "Active"

6. Action:

Add Button: allows creating new Exceptions

Display the number of results as "Showing x of n results"

- x: count the number of records currently displayed on the list table
- y: count the total number of all recorded entries

Maximum of 20 records on the exception list table.

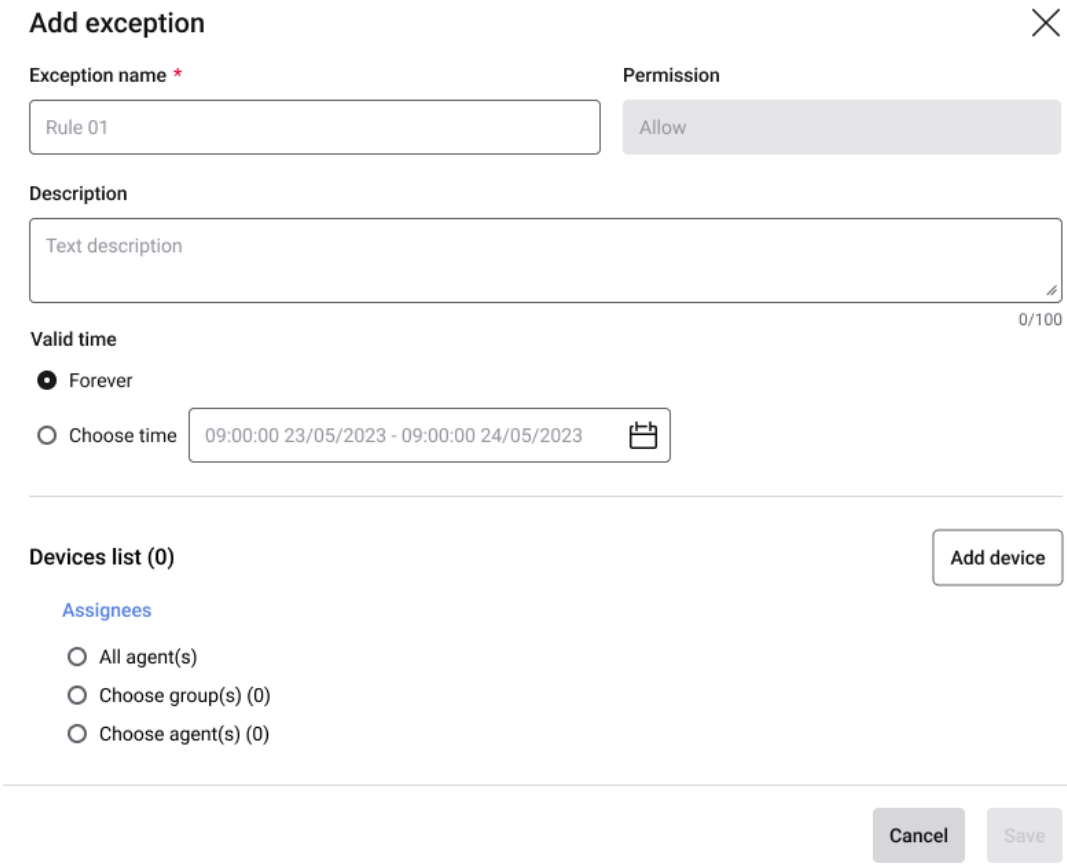
→ Paginate the data table if there are more than 20 records; users can select a page to display the data table corresponding to that page.

→ Default display is the first page

→ The records are displayed in order of creation or modification time (most recent at the top, with older records gradually pushed down).

Add Exception Screen

Purpose: to create new exceptions so that each unit can exempt certain end users allowed to access the device (serving individual business purposes).



- Exception name: Allows entering the name of the exception (Required, must be unique). Characters include alphabet letters, numbers 1, 2, 3...0, case-insensitive, under 500 characters.
- Permission - Display access permissions of exceptions (in Disabled mode),

  If the type of device is granted access as Allow, the corresponding access permission for the exception is Block.
  + If the type of device access permission is Block, the corresponding exception access permission is Allow.

- Description: description of information regarding exception creation
- Valid time - Allows selection of the valid duration of the exception

Use radio buttons with two options for the user:

- Forever: Allow/Block permanently

- Absolute time range → Display format dd/mm/yyyy hh:mm:ss - dd/mm/yyyy hh:mm:ss (default is from the current time to the future, with a 5-minute time difference to prevent users from encountering errors when adding exceptions due to longer processing times)

If there is at least one exception record, display the Exception List Table including the following information fields:

1. Exception name - display the exception name
2. Description - Information to which the exception applies
3. Device(s) - display the device name
4. Duration - displays the duration of the exception
5. Status - displays the status of the exception, including Expired and Active.

If the exception has exceeded the allowed duration compared to the current time, display Status = "Expired".

+ If the exception ensures the duration allowed compared to the current time, then display Status = "Active"

6. Action:

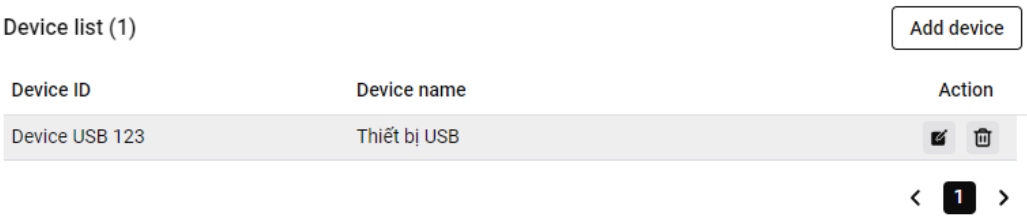
- Add Button: allows creating new Exceptions

Device list (at least one device record by default)

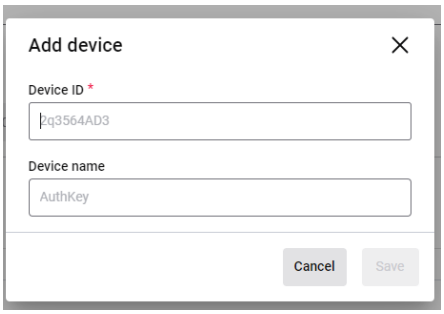
When there is no device: Only display the Add device button.

When a device is present: Display the "Add Device" button and show a table with the following columns: Device Control ID, Action (display edit and delete icons when hovering the mouse).

- If the user only has view permissions, they can only view and are not allowed to add, edit, or delete.



Click the Add device button to open a popup for the user to enter information to create an exception device.



Information includes:

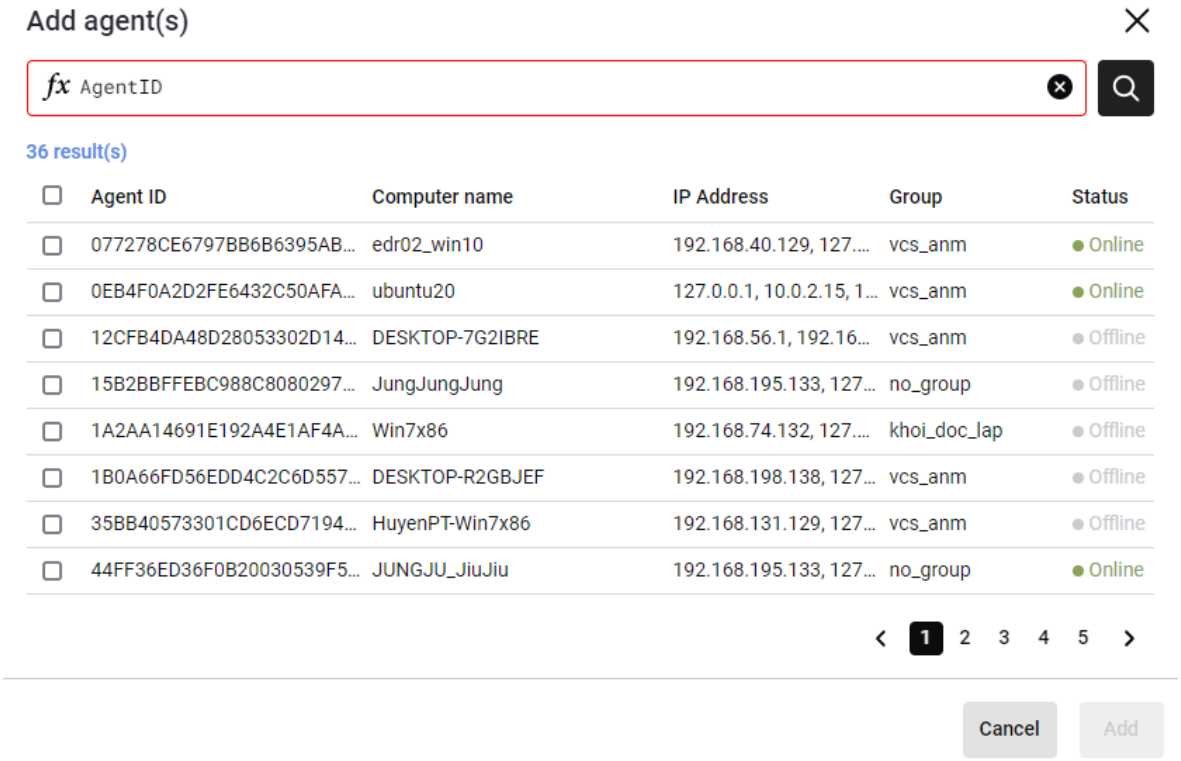
- Device ID: contains alphabetic characters, numbers, special characters, peripheral device ID, mandatory field
- Device name: displays the name of the device, can be left blank

The Save button will be disabled until the Device ID is entered.
Once all the information has been entered, the Save button will be available.
Press Cancel or click the close icon to exit the popup screen.

Return to the Add Exception screen.
Assignees have 3 options for users to choose from (only 1 option can be selected).

- If All agent(s) is selected, all agents are chosen to allow/block this Exception device.
- If "Choose agent(s) (0)" is selected, the user can choose one or multiple agents to allow/block this Exception device.

At this time, the Add Agent button will also be displayed.
Clicking the button will display a corresponding popup (Only agents belonging to that group will be shown in the Add agent(s) section.)



Search:

Allow users to enter a search key to query suggested information available in the system by AgentID, Computer name, or IP address.

Default is empty, not mandatory to fill, special characters allowed;

>> When clicking to check, verify whether the query content is in the correct query format:

Perform data search and check for data that meets the condition: input string matches partially or fully with the "name" field, case-insensitive. When text input begins, a clear icon will appear at the corner of the input field.

=> Click the search button or press enter

- Always display information fields such as columns: Agent ID, Computer Name, IP Address, Group, Status.

  + If no data is found, display the message: No data;

+ If there is matching data: Display the corresponding list;

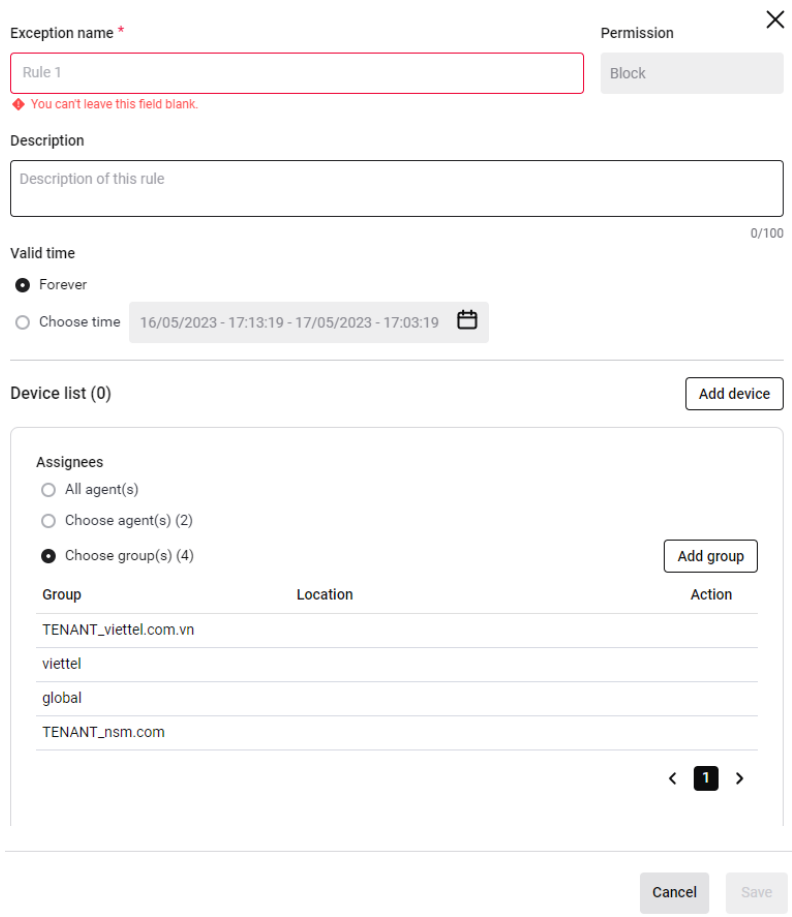
- Checkbox: Allows selecting one or multiple Agents, unchecked by default;
- Agent ID: Display Agent ID information
- Computer name: Display device (computer) information
- IP address: Displays the IP address information of the device (workstation)
- Group: Display Agent's Group information
- Status: Displays the operational status information of the Agent: Online/Offline
- Pagination is available, with a minimum of 8 records.

After selecting the appropriate agent, the Add button will become available. Click the Add button to successfully select one or more agents into the Add Exception section.

After adding the Agent, return to the Add Exception screen:

The following fields will be displayed: Agent ID, Computer Name, IP Address, Group, Status.

This screen displays an additional Action column (Delete Icon). If there are more than 5 records, pagination will be applied.

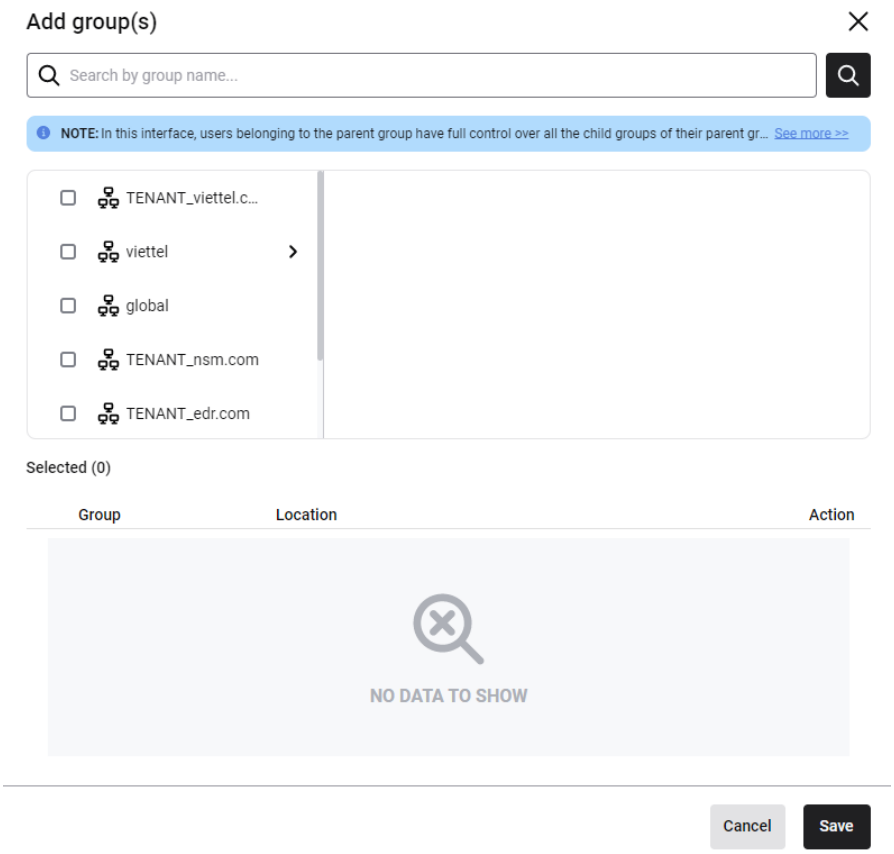


- If "Choose group(s) (0)" is selected, the user can choose one or multiple groups allowed to block this device. By default, the list of Groups (based on the logged-in managing user) is displayed.

The Group list is required to be displayed in a tree structure, with duplicate checks within the Group list itself.

Search box: Allows users to enter a search key to find Group information in the system by Group name.
Default is empty, input is not required, trim leading and trailing whitespace, special characters are allowed;
Click the Search button to perform a search for Group information related to the search key within the system.

Checkbox Item: Allows selecting one or multiple Groups, unchecked by default;



Check duplicate Group(s);

By default, do not display results if the user has not selected any records.

If at least one record exists, display pagination and the number of selected Agent(s).

Checkbox: Select one or more groups that the Agent belongs to among the related groups. Default is unchecked.

The column attributes include: Group, Location, Action. Selecting any of these will correspond to Selected(0).

Group: Display Agent's Group information

Location: Display the hierarchical position of the Group;

Example: root/ TT GPSP/EDR

Action: (delete) if you do not want to select that group

If no group is selected >> Return No data

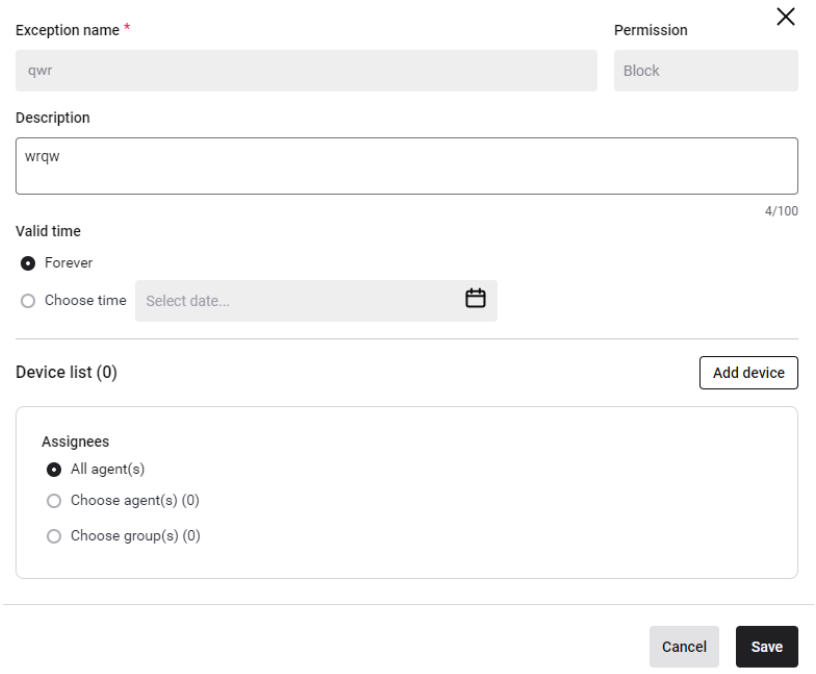
After selecting the appropriate group, the user clicks the Save button successfully and returns to the Add Exception screen. At this point, the Portal will display a notification stating, "You have successfully added the exception."

If you do not want to select a group, click Cancel to return to the Add Exception screen.

Once all necessary information for Add Exception has been provided, the user selects Save to store all details of this Exception. >> return to the Exception list screen of that group.

In the Exception list screen, under the Action section, there are Edit and Delete icons.

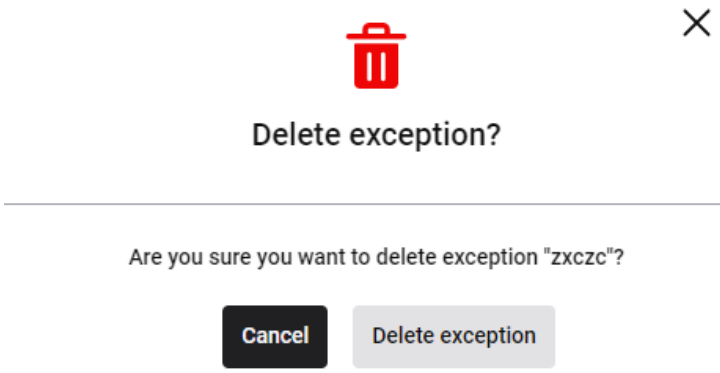
If you select the Edit icon, a similar screen will appear.



Only the Exception name and Permission are locked and cannot be changed. All other fields can be modified by the user at will.

After making edits, click Save to save the information. At this point, the Portal will display a notification stating, "You have successfully edited the exception."

In the case of the delete icon, display a popup.



If the user selects the Delete Exception button, they agree to delete this exception. At this point, the portal will display a notification stating, "You have successfully deleted the exception."

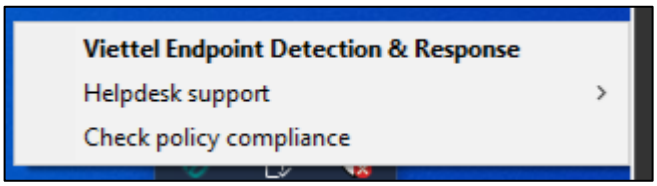
Select Cancel to return to the Device list screen.

Below are instructions for end-user features, to be used directly on the endpoint machine:

3.12 Agent GUI – Main interface

The function allows users to quickly view the information security status on the machine where the agent is installed;

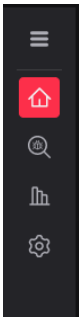
On the taskbar, find the icon, right-click on it, and select “Viettel Endpoint Detection & Response”:



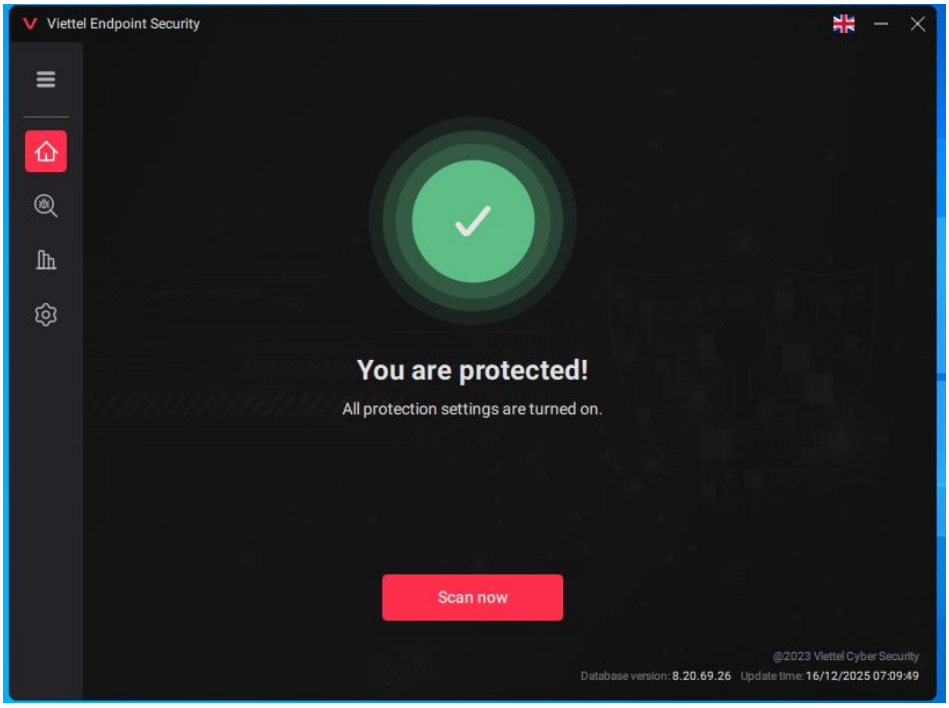
The system displays the following information:

Displayed in two languages: English-Vietnamese.

On the Sidebar, icons are displayed for major features: Home, Malware Scan, Reports, Settings. The sidebar can be collapsed or expanded.



In cases where the machine has no malware, Real-time Protection is enabled, or all malware has been handled:



In cases where the machine has at least one malware due to Real-time protection being disabled.

Version information: details about the Agent version installed on the user's device, update time, and product support information are displayed in the corner of the screen.

3.13 Agent GUI – Protection feature

Purpose: to enable users to proactively use the system to scan and handle malware on their devices.
Only allow one type of scan to be performed: Quick scan, Full scan, Custom scan (quick scan, full scan, folder scan).

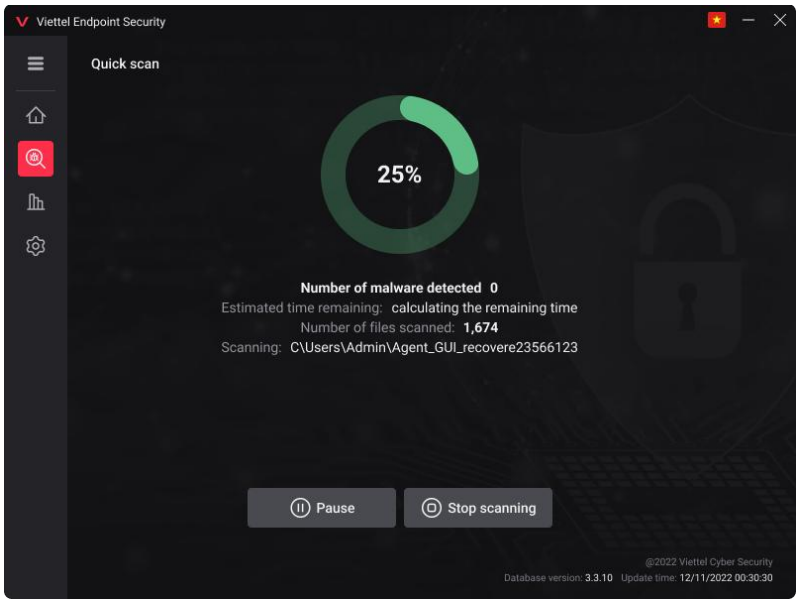
The supported scanning methods include

Select scanning methods from the agent interface;

- Quick scan: Scans a predefined set of directories, which are directories where malware frequently occurs, by selecting to scan all files and subdirectories within the chosen directories;
- Full scan: Scan all files and folders present on the user's device;
- Custom scan: Similar to context scan, when selecting this option, the agent displays a file explorer allowing the user to choose a file or folder to scan.

+ Direct selection from the file explorer, allowing multiple files and folders to be selected, right-click to choose scan (Context scan);

After selecting the appropriate method, the system performs scanning and malware processing:



+ Display the total scan progress percentage

+ Display information on the number of detected malware samples

+ Display the estimated remaining time to complete the scan

+ Display the number of files that have been scanned

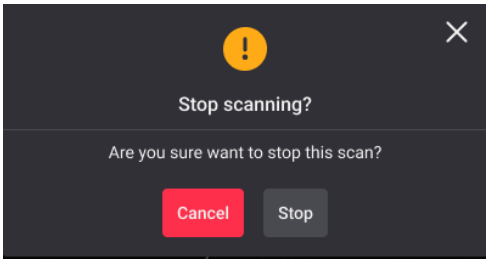
+ Display the file path being scanned

Support the following operations during scanning:

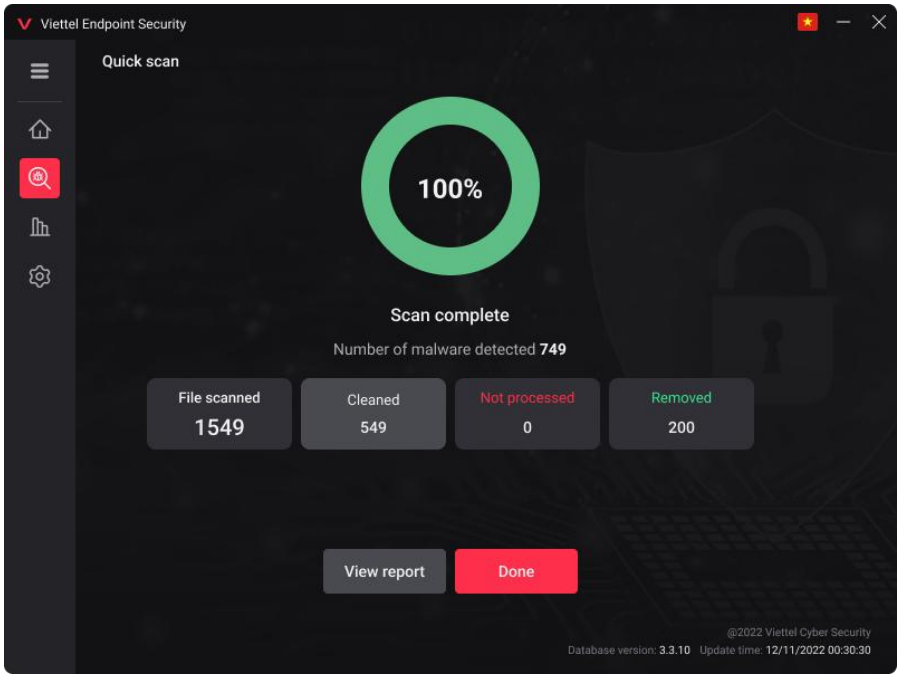
: Allow termination of the scanning process;

: Allows pausing the scanning process;

When clicking on Pause, the button simultaneously changes to Resume, allowing you to select it to continue scanning.



After completing the scanning process, display the scan results.



+ Scanned files: Display the number of files that have been scanned
+ Cleaned: Display the total number of files that have been eliminated
+ Not processed: Display the total number of unprocessed files
+ Removed: Display the total number of files deleted

These buttons can directly link to the related report section.

Alternatively, you can click the button to view the overall report of the scan results.

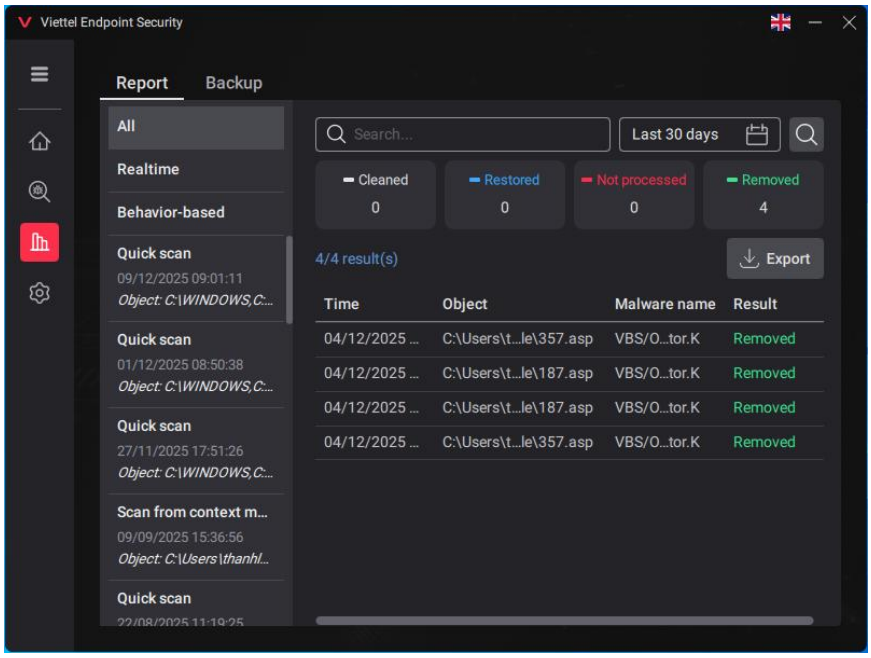
Click done to return to the main screen of Protection.

After the scanning process, if the agent detects a malicious DLL being loaded that cannot be deleted directly, the agent will display a popup requesting a system restart to complete the scanning process.

3.14 Agent GUI – Report feature

Purpose: To compile a report on malware detections by the device, displaying the total number of malware listed.

a. Tab report (Report)



- In case there are no results matching the search criteria, display the status "No data available."

- If the user selects All:

+ Malware list: Displays all detected malware;

- If the user selects Manual scan:

+ Scan count list: Displays the scan history for the past 30 days;

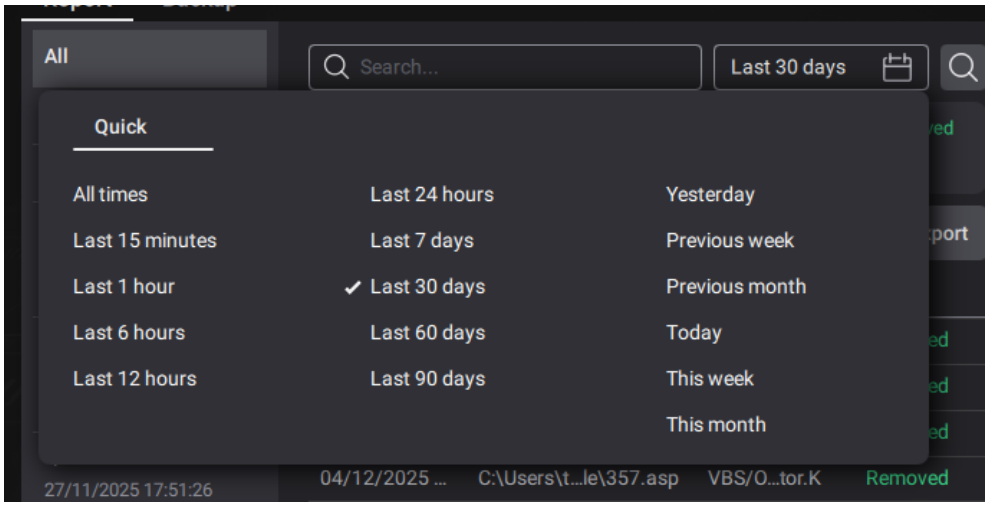
+ Default: Select the most recent scan to display the corresponding list of malware for the user;

+ Malware list: Displays all malware detected during the user-selected scan;

- If the user selects Real-time:

+ Malware list: Displays all malware detected in real-time

- Time-based search: Allows adjustment of the time period for monitoring information security status up to the present, with the default set from the previous day.



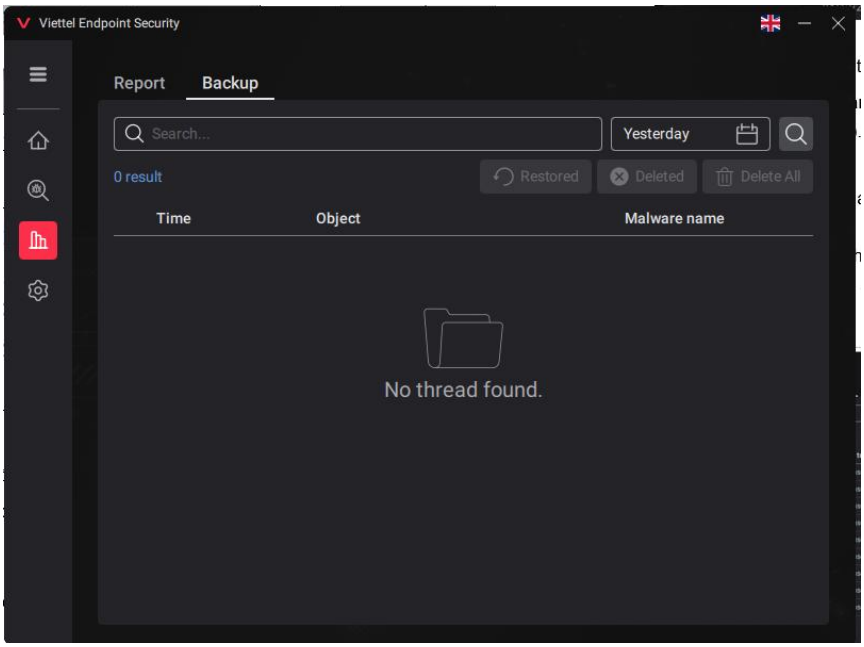
- Search by malware results

In the report section, users can download the entire report to their device (based on the selected items).

b. Backup Tab

Purpose: to provide information on the list of malware files currently being backed up.

Users can search, select the time, and then click search; the list will be displayed according to the search parameters.



Files containing malware are stored in their original form in the Backup folder before processing. To clean the Backup folder or restore files, the product offers the following features:

Allows selection of one or multiple files for recovery;

Allow selection of one or multiple files to delete from the Backup folder;

Allows quick deletion of all existing files in the Backup folder;

- In case no results match the search criteria, display the status "No matching results found."

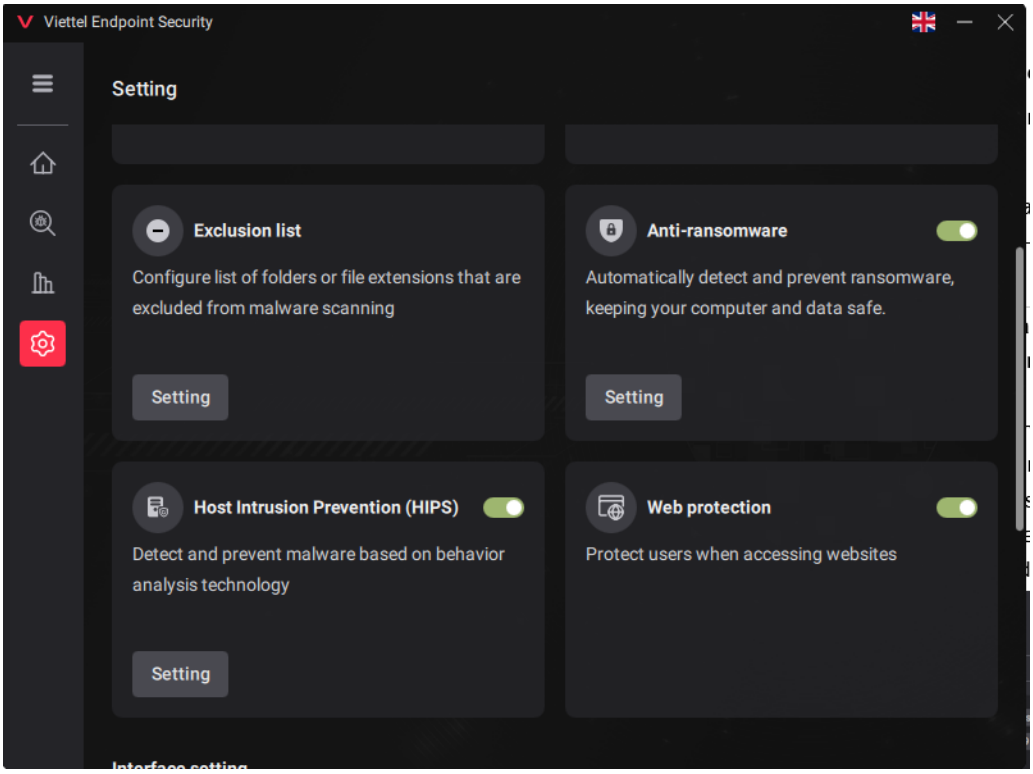
3.15 Agent GUI – Setting feature

Purpose: Configuration settings on each agent machine

Allow searching all content within the settings page by keyword.

a. Protection setting: Because there are two Policy configuration locations (Self defense and Real-time protection) on the Portal and under each Agent.

- Self Defense: Allows enabling or disabling Self Defense. → Protects the agent's resources from unauthorized interference by external agents - Not yet fully updated.
- Real-time protection: Comprehensive protection for the computer, automatically detecting and eliminating malware as soon as it appears on the device (Enable/Disable device)
- Exclusion list: Allows selection of folders to be excluded (not scanned by Real-time Protection); Add/Edit excluded folders



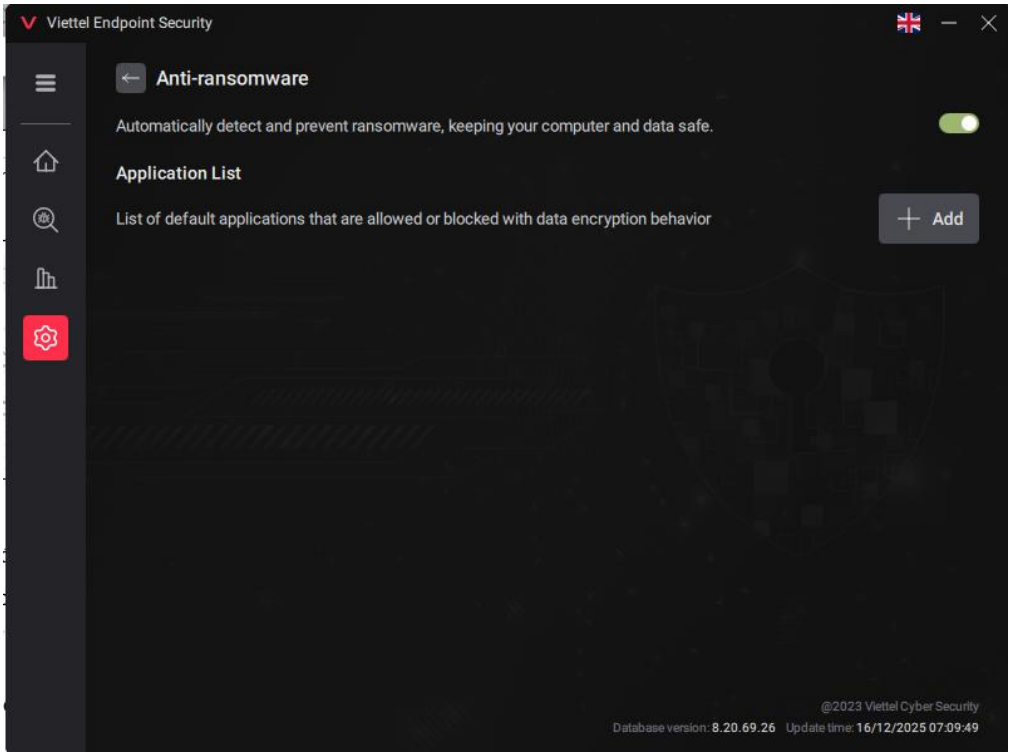
- Extension: Allows adding/editing Extensions (document file types) to be excluded (not scanned by Real-time Protection);

b. Interface setting

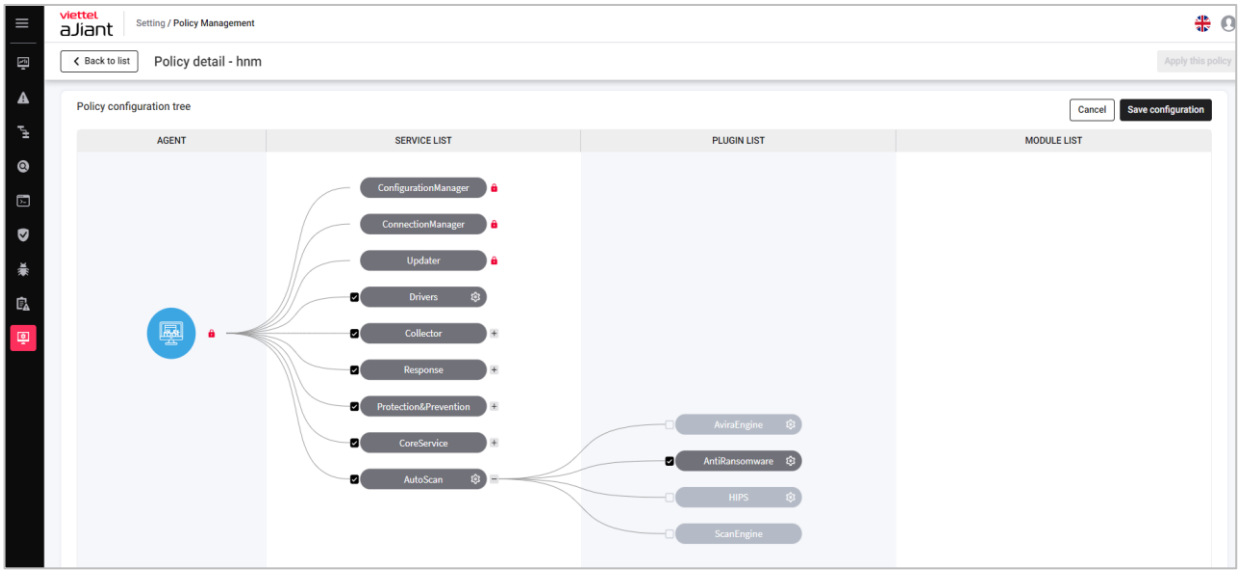
- Allow enabling/disabling Notifications → Display notifications on the device screen when a scan command is received from the system, upon detecting malware.
- Language: Allows selection of English/Vietnamese language

c. Anti-Ransomware

- Allow users to enable or disable ransomware protection mode. The system will automatically detect and block ransomware on the computer.



Note: To use this feature, you need to enable the AntiRansomware Policy on the Portal.



- Application list: Allows users to select applications that may perform suspicious behaviors indicative of data-encrypting malware.

d. Backup setting: Supports users in configuring backup file storage information.

- Check to display the backup size limit, and allow input of the backup file storage size limit.

  (Allow configuration up to 5120 MB → Notification when reaching the 5G threshold: The size of the backup file has reached the limit! The system will delete the oldest files from the backup.)

  To avoid exceeding the maximum storage size, the oldest files in the storage section will be automatically deleted when the maximum storage size is reached.

3.16 Agent GUI – Command line interface of the On-demand Scan feature

The command allows management of malware scanning, viewing reports, and backups of detected malware.

Run the command to list supported features.

Note: navigate to the agent installation directory */usr/local/bin/ajiant/autoscan* to use the VESAutoScan program commands.

```
$ VESAutoScan -h
Usage: VESAutoScan <command>

Manage scan & protection service

Commands:
  scan                  Manage scan sessions
  |- start              Start a scan session
  |  |- <files> ...     File paths to scan
  |- stop               Stop a scan session
  |  |- <id>            Scan session ID to stop
  |- show               Show scan session details
  |  |- <id>            Scan session ID to query
  |- list               List all running scan sessions

  report                Manage scan reports
  |- list               List all scan reports
  |  |- <type>          Report type; available types are realtime, manual,
                        all
  |- show               Show scan report details
  |  |- <id>            Report ID to show; ID can be 'realtime' or a report number
  |- search             Search for files in scan reports
  |  |- <str>           String to search for in file paths

  backup                Manage backup files
  |- restore            Restore a backup file
  |  |- <id>            ID of file to restore
  |  |- <output-path>   Output path for restored file
  |- list               List all backup files
  |- search             Search backup files
  |  |- <str>           String to search for in file names

  show                  Show scan service information
  |- version            Show version
  |- database-version   Show database version

Flags:
  -h, --help    Show context-sensitive help.

Run "VESAutoScan <command> --help" for more information on a command.
```

Sub-command scan

Manage scan sessions, allowing users to manually create scan sessions and manage the scan sessions created in this way.

a. Start a scan session

Users specify the locations to be scanned for malware and can designate more than one location.

```
$ VESAutoScan scan start /home/ /usr/
path: /home
path: /usr
Scan started successfully, ID: 1
Use the command `VESAutoScan scan show 1` to display scan details.
```

b. Stop a scan session

The user specifies the scan session that needs to stop scanning.

```
$ VESAutoScan scan stop 1
stop successful
```

c. Display the status of a scan session.

The user specifies the scan session for which information needs to be displayed.

```
$ VESAutoScan scan show 1
+----+---------+----------+--------------+------------------+-----------------+
| ID | STATUS  | PROGRESS | FILES SCANNED | MALWARE DETECTED | MALWARE CLEANED |
+----+---------+----------+--------------+------------------+-----------------+
|  1 | Stopped | 9.00%    |        30231 |                0 |               0 |
+----+---------+----------+--------------+------------------+-----------------+
```

d. List the running scan sessions created using the command line method.

Display the scan sessions currently in progress and their scanning locations.

```
$ VESAutoScan scan list
+---------+------------+
| SCAN ID | LOCATION   |
+---------+------------+
|       1 | /usr,/home |
+---------+------------+
```

Sub-command report

a. List scan history and information

Users specify the type of report, which can be "realtime" for reports on real-time malware scans, "manual" for reports on manual scans, or "all" to display all reports.

```
$ VESAutoScan report list realtime
+------------------------------+
| Realtime Scan Report         |
+-----------+------------------+
| REPORT ID | MALWARE DETECTED |
+-----------+------------------+
| realtime  |                2 |
+-----------+------------------+
```

```
$ VESAutoScan Report List Manual
+-------------------------------------------------------------------------------------------------------
-------+
| Manual Scan Report
|
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
| REPORT ID | TIMESTAMP                | LOCATION   |  FILE | FILE SCANNED | MALWARE DETECTED |
STATUS   |
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
|         1 | 2025-07-10T17:46:32+07:00 | /usr,/home | 30231 | 312,837      |                0 |
Stopped  |
|         2 | 2025-07-10T17:53:01+07:00 | /usr,/home | 31795 | 312,838      |                0 |
Scanning |
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
```

```
$ VESAutoScan report list all
+------------------------------+
| Realtime Scan Report         |
+-----------+------------------+
| REPORT ID | MALWARE DETECTED |
+-----------+------------------+
| realtime  |                2 |
+-----------+------------------+

+-------------------------------------------------------------------------------------------------------
-------+
| Manual Scan Report
|
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
| REPORT ID | TIMESTAMP                | LOCATION   | FILES | FILE SCANNED | MALWARE DETECTED |
STATUS   |
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
|         1 | 2025-07-10T17:46:32+07:00 | /usr,/home | 30231 | 312,837      |                0 |
Stopped  |
|         2 | 2025-07-10T17:53:01+07:00 | /usr,/home | 56013 | 312,838      |                0 |
Scanning |
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
```

b. Display detailed information about a report.

The user specifies the ID of the report to be displayed and can specify "realtime" to display a detailed report for the real-time malware scanning feature.

```
$ VESAutoScan report show realtime
+---------------+------------------------+-------------+
| FILE PATH     | MALWARE NAME           | STATUS      |
+---------------+------------------------+-------------+
| /adware+virus | ADWARE/Patched.Ren.Gen | Deleted     |
+---------------+------------------------+-------------+
|               | TOTAL                  | 1           |
+---------------+------------------------+-------------+
```

```
$ VESAutoScan report show 3
+-----------+--------------------------+----------+------+--------------+------------------+------
----+
| REPORT ID | TIMESTAMP                | LOCATION | FILE | FILE SCANNED | MALWARE DETECTED |
STATUS   |
+-----------+--------------------------+----------+------+--------------+------------------+------
----+
|         3 | 2025-07-10T18:13:19+07:00 | /home    |  496 | 153052       |                1 |
Scanning |
+-----------+--------------------------+----------+------+--------------+------------------+------
----+
+--------------------+------------------------+-------------+
| FILE PATH          | MALWARE NAME           | STATUS      |
+--------------------+------------------------+-------------+
| /home/adware+virus | ADWARE/Patched.Ren.Gen | Deleted     |
+--------------------+------------------------+-------------+
|                    | TOTAL                  | 1           |
+--------------------+------------------------+-------------+
```

c. Search for files or malware that have been previously detected

Users can specify a part of the path to the file they want to find.

```
$ VESAutoScan report search home
+-----------------------------------------------------------+
| REPORT ID: 3                                              |
+--------------------+------------------------+-------------+
| FILE PATH          | MALWARE NAME           | STATUS      |
+--------------------+------------------------+-------------+
| /home/adware+virus | ADWARE/Patched.Ren.Gen | Deleted     |
+--------------------+------------------------+-------------+
|                    | TOTAL                  | 1           |
+--------------------+------------------------+-------------+
```

Sub-command backup

a. List the detected files that can be recovered.

```
$ VESAutoScan backup list
+---------+--------------------+
| FILE ID | FILE PATH          |
+---------+--------------------+
|       1 | /adware+virus      |
|       2 | /home/adware+virus |
+---------+--------------------+
|   TOTAL | 2                  |
+---------+--------------------+
```

b. Search for detected and recoverable files

The user specifies a part of the path to the file to be found.

```
$ VESAutoScan backup search home
+---------+--------------------+
```

```
| FILE ID | FILE PATH          |
+---------+--------------------+
|       2 | /home/adware+virus |
+---------+--------------------+
|   TOTAL | 1                  |
+---------+--------------------+
```

c. Restore one file

The user specifies the ID of the file to be backed up and the filename after restoration; the filename can be specified as an absolute or relative path.

The recovered file is compressed in zip format and password-protected with "infected".

```
$ VESAutoScan backup restore 2 /home/linux/malware
Restoring adware and virus to /home/linux/malware.zip
Restore successful to /home/linux/malware.zip with password: infected
```

Sub-command show

a. Display the version of the malware scanning management service.

```
$ VESAutoScan show version
Version: 3.3.0.545.e8d14fe
Build: 2025-06-09T10:30:04+0000
```

b. Display database version

```
$ VESAutoScan show database-version
DatabaseVersion: 8.20.57.224
UpdateDate: 10/07/2025 17:55:30
```