



Viettel Endpoint Detection & Protection (VCS-aJiant version EDP)

Document version: 4.133 – Update: 15-Dec-2025

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	

MENU

1. INTRODUCTION	11
1.1 Current situation	11
1.2 The development of technology	11
1.3 VCS-ajiant	11
2. OVERVIEW	12
2.1 Technology	12
2.2 Infrastructure architecture.....	13
2.3 Working with the administrative interface	14
3. USER MANUAL.....	15
3.1 Log in.....	15
3.2 VCS-ajiant Dashboard.....	15
3.2.1 Data manipulation	17
Export data.....	17
Search by date	17
Refresh data	18
3.2.2 Statistics Overview	18
3.2.3 Security Operation Monitoring.....	23
3.2.4 Agent Monitoring Tracking	24
3.2.5 Monitor Risk Detection	26
3.3 Alert Management	28
3.3.1 Search Alert.....	30
Search by time	30

Quick search	30
Search by query sentence	31
3.3.2 Alert List.....	33
3.3.3 Group Alerts	36
3.3.4 View Alert Details	37
3.3.5 Survey Chart (Enhance Alert)	40
Chart display area and chart operations	40
Detailed information display area	48
3.3.6 Update the status to non-hazardous or close the alert for one/multiple alerts or alert groups.....	50
3.4 Investigation Screen	51
3.4.1 Investigation Process Analysis.....	51
3.4.2 Investigation_Event Search.....	57
Search Event	57
Highlight	58
I need help.	59
Wrapped text.....	60
Export Data	61
3.4.3 Note	62
3.4.4 Investigation_Deploy Tools	63
Tool Management	63
Deploy tool	64
Manage task	78
3.5 Response Screen	101
3.5.1 Live Response.....	101

3.5.2 Isolate Devices	124
Create Isolate Devices command	124
Create a Release Isolation command (remove isolation)	126
Check device isolation information / remove device isolation.....	127
View the impact history list by device	128
3.6 Settings Screen	129
3.6.1 Agent Management	129
3.6.2 Policy Setting.....	140
3.6.3 Group Management	146
3.6.4 Account Management	157
Permission management	157
Role management.....	158
User management	164
3.6.5 Update management.....	171
Update group	171
Packages update	175
3.7 BLS Screen	181
3.7.1 Violation Statistics	181
Violation Statistics Screen	181
Violation Type Tab	184
Unit Tab	186
3.7.2 Software Statistics	188
3.8 Threat Hunting.....	191
3.8.1 Enable/disable policy.....	191

3.8.2 Search by agents/groups	191
3.8.3 Search for IOCs.....	192
Supported types of IOCs.....	192
Search result details	194
3.8.4 View Query History.....	198
View query list.....	198
View detailed query history.....	199
3.9 Rules Correlation.....	200
3.9.1 Display list	200
3.9.2 Add New Rules Correlation	205
3.9.3 Delete Rules Correlation	213
3.10 Protection & Prevention.....	214
3.10.1 Application Control	214
Display the list of blocked applications/processes.....	214
Search for blocked applications/processes	215
Add new blocked application/process.....	215
Add new application/process from an existing file	215
Delete blocked applications/processes from the list.....	216
The update stream of the number of agent machines that have successfully updated the new list.....	216
3.10.2 Endpoint Firewall	217
Display the list of blocked connections	217
Search for blocked connections.....	218
Add new blocked connections	218
Create a copy from the existing conditions.....	220

Add new blocked connections from an existing file	220
Remove blocked connections from the list	220
Export data of the conditions	221
3.11 Anti-Malware.....	221
3.11.1 Scan Scheduler	221
Search for Scan Schedule task	221
Add new Scan Schedule task	222
Clone Schedule Task.....	229
View details	230
Delete Scheduled Task.....	231
View report.....	233
3.11.2 Device control.....	235
Search Group.....	236
Device list of each group.....	238
Exception Screen.....	239
Add Exception Screen	240
3.12 Main.....	249
3.13 Protection	251
3.14 Report.....	253
3.15 Setting	256
3.16 VESAutoScan.....	259
Sub-command scan.....	260
Sub-command report.....	261
Sub-command backup.....	263

Terminology

Terminology	Explanation	Note
VCS-aJiant	Product trade name	
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	

Terminology	Explanation	Note
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

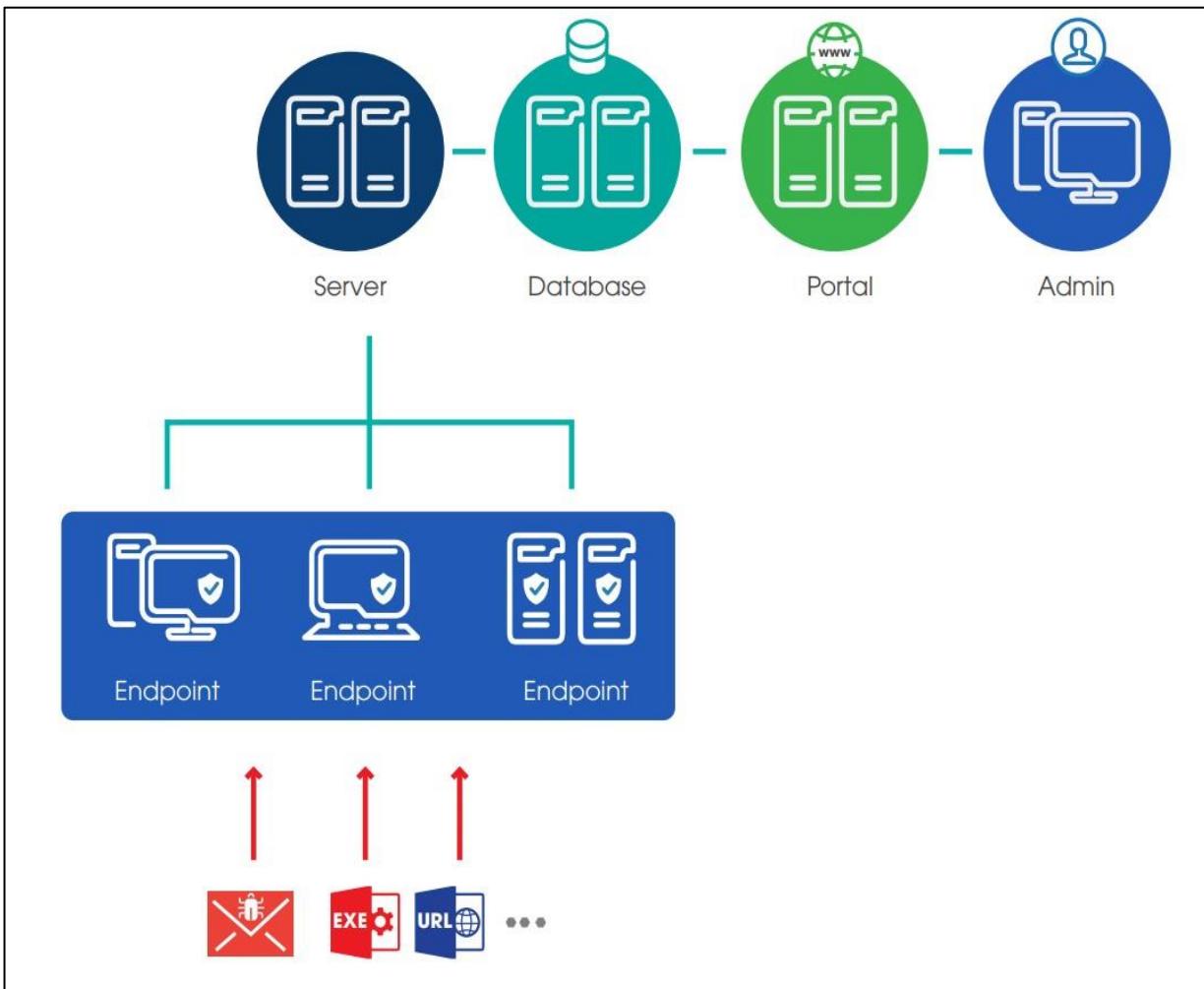
2.1 Technology

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

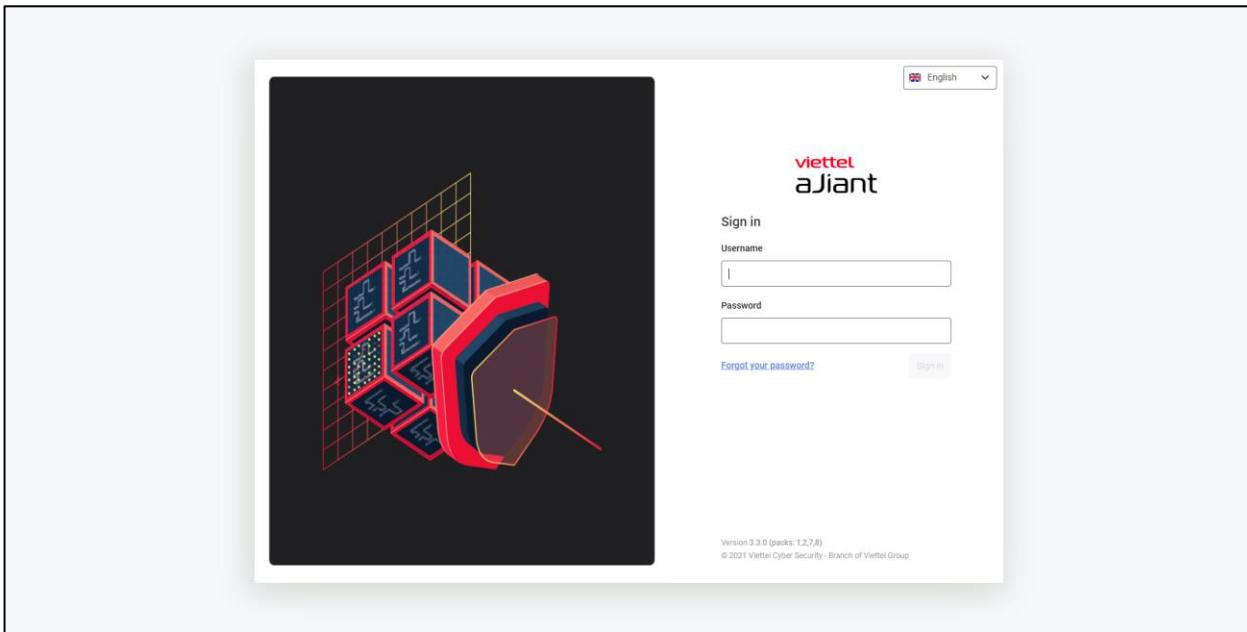
The Web-portal interface includes functional interfaces and processing flows as follows:

- 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

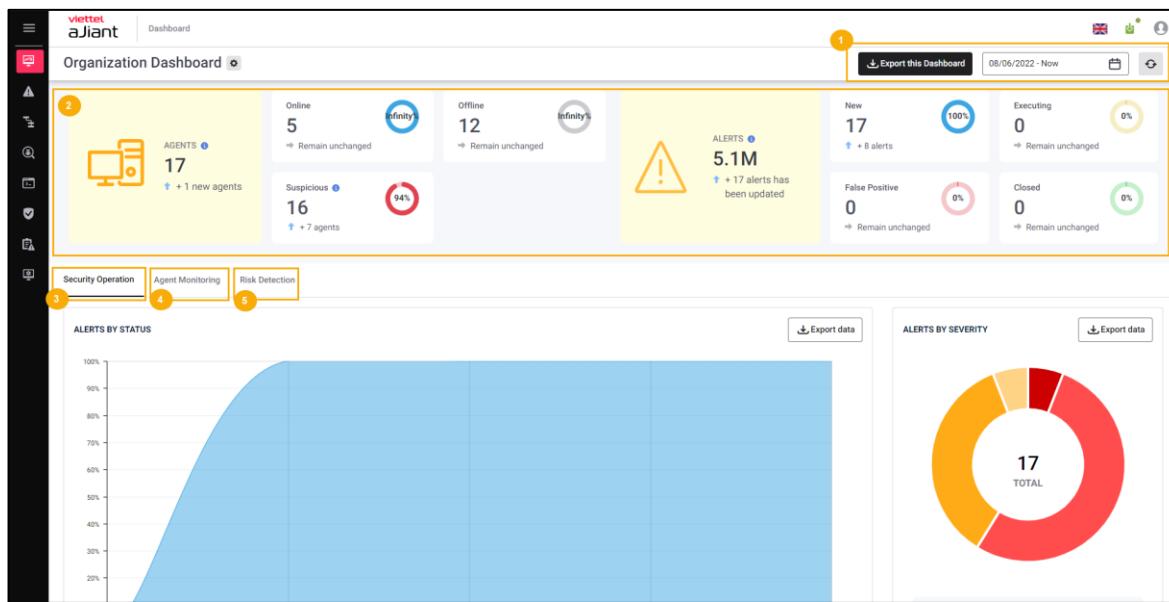
- Access the system at the provided address;



- 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 range	Relative time range
From <input type="text" value="08/06/2022"/> 	Last 90 days Last 60 days Last 30 days Last day
Apply time range	

- 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.

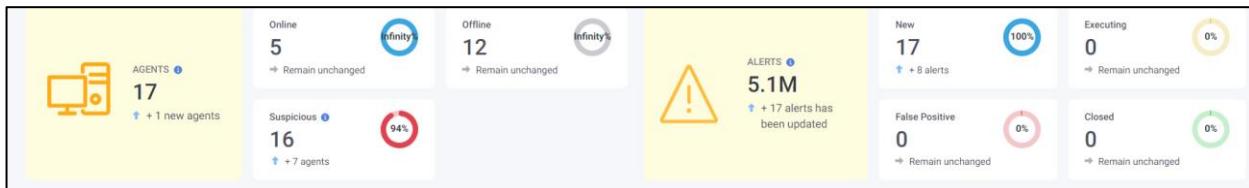
- + After selecting the desired time period to monitor, choose to reload the corresponding data.

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;



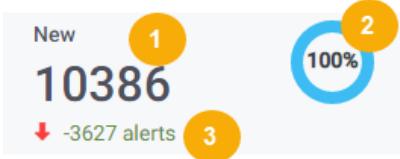
- + Statistics related to agents:

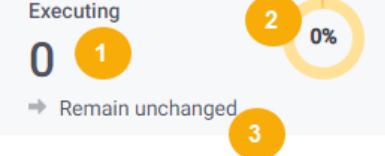
Statistics	Meaning
------------	---------

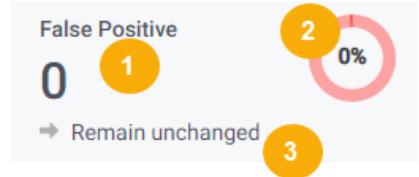
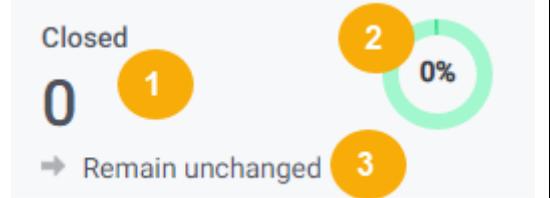
 <p>AGENTS 17 ↑ + 1 new agents 2</p>	<p>Includes 2 indicators:</p> <ul style="list-style-type: none"> - Total number of machines with the agent installed on the system (regardless of the search time period); - Total number of machines newly installed with the agent during the search time period; (+: Newly installed machines, Remain unchanged: No new machines installed during the search time period)
<p>Online 3274 ↑ + 884 agents 3</p> 	<p>Includes 03 indicators:</p> <ul style="list-style-type: none"> - 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)
<p>Offline 2897 ↓ - 898 agents 3</p> 	<p>Includes 03 indicators:</p> <ul style="list-style-type: none"> - 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)

 <p>Suspicious 3748 + 1529 agents</p>	<p>Includes 03 indicators:</p> <ul style="list-style-type: none"> - 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
 <p>Alerts 466354 + 10386 alerts has been updated</p>	<p>Includes 2 indicators:</p> <ul style="list-style-type: none"> - 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)
 <p>New 10386 - 3627 alerts</p>	<p>Includes 03 indicators:</p> <ul style="list-style-type: none"> - 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

	<p>period;</p> <ul style="list-style-type: none"> - 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)
 <p>Executing</p> <p>0 1 2 3</p> <p>➡ Remain unchanged</p>	<p>Includes 03 indicators:</p> <ul style="list-style-type: none"> - 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)

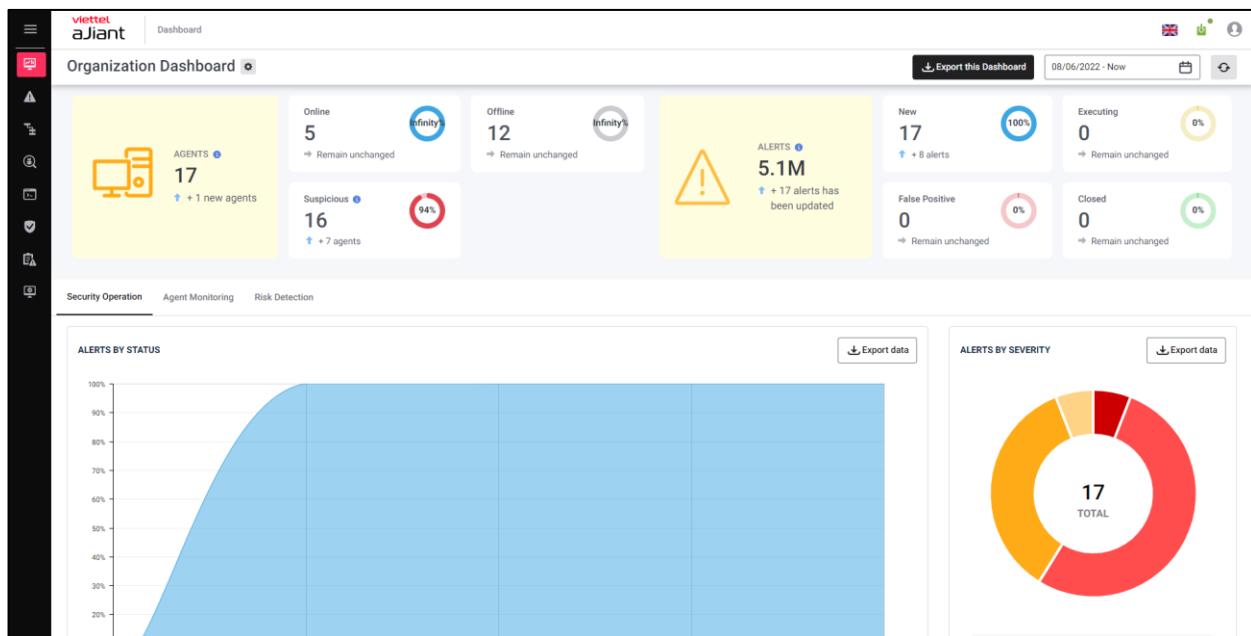
	<p>Includes 03 indicators:</p> <ul style="list-style-type: none"> - Total number of new Alerts generated or updated within the search period and currently in the CLOSED status; - Ratio of new Alerts generated or updated within the search period and currently in the CLOSED status compared to all new Alerts 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. <p>(+ : Total number of Alerts increased compared to the previous period; Remain unchanged: Total number of Alerts remained the same compared to the previous period)</p>
	<p>Includes 03 indicators:</p> <ul style="list-style-type: none"> - 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. <p>(+ : Total Alerts increased compared to the previous period; Remain unchanged: Total</p>

	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;

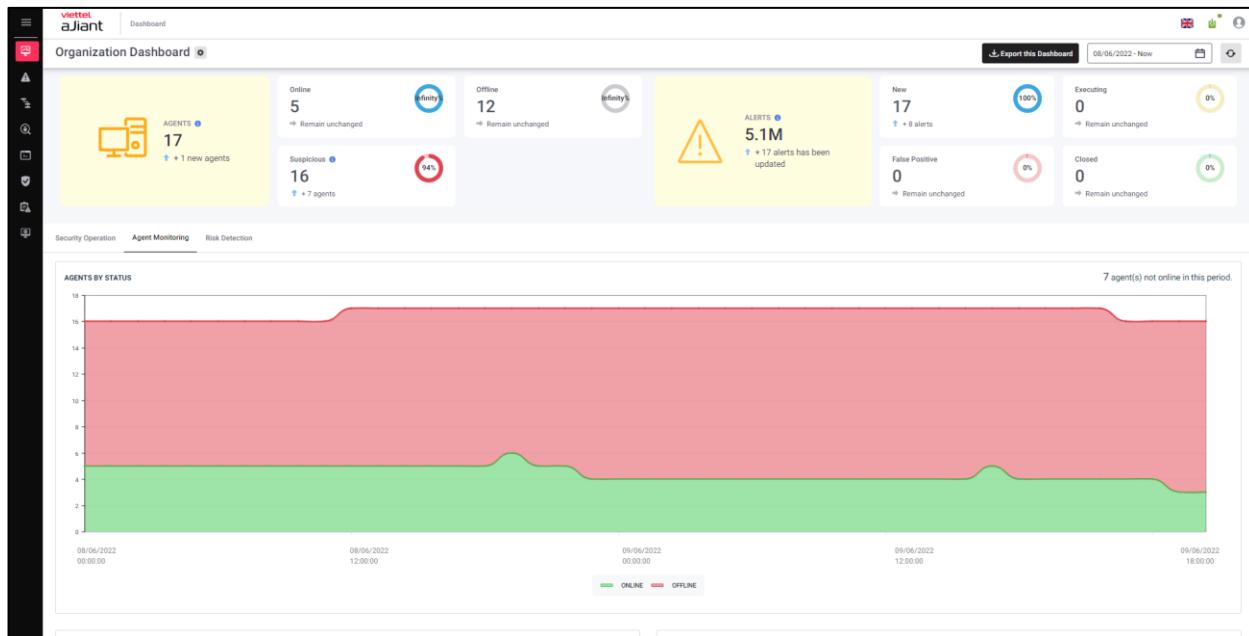


Chart/Statistics	Meaning
Alert by status	<p>Area Chart - Tracks the status of newly recorded or updated Alerts within the search period, including:</p> <p>X-axis: time;</p> <p>Y-axis: Alert rate divided into 4 status groups = (New, Executing, Closed, False Positive);</p> <p>Allows selection to download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

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;



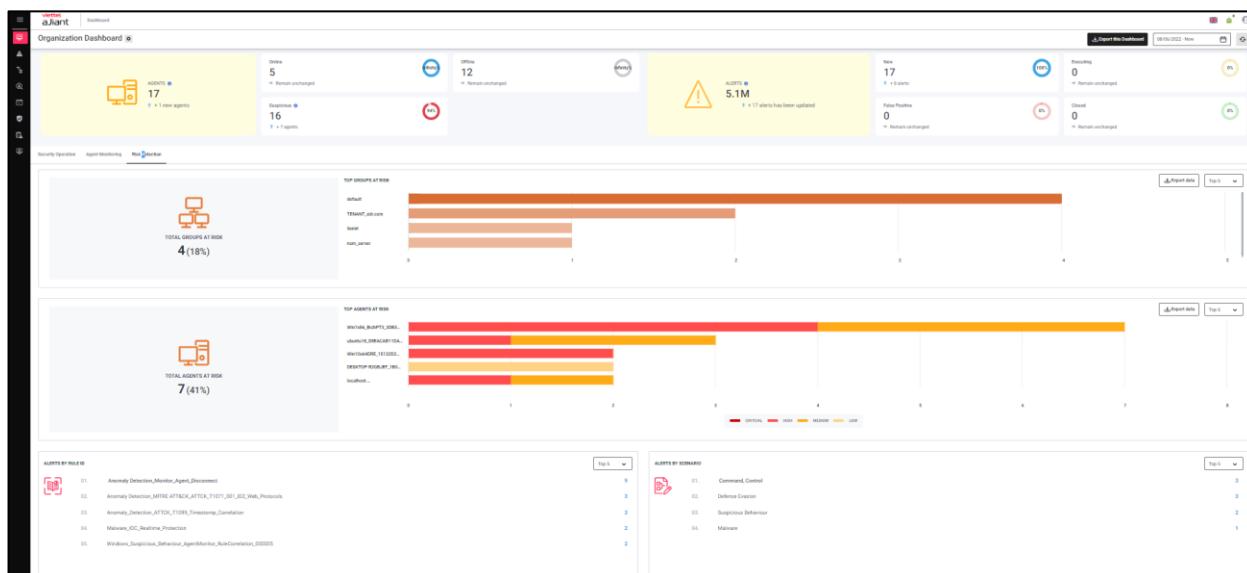
Chart/Statistics	Meaning
Agent by status	<p>Area Chart - Monitoring the status of machine recordings (Online/Offline) during the reporting period up to the current time, including:</p> <p>Y-axis: Percentage of machines divided into 2 status groups (Online, Offline); X-axis: Statistical time; Displays 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).</p>
Agent by operating system	<p>Pie Chart - Monitoring the recording status of devices by OS, including:</p> <p>Ratio: the proportion of devices for each OS; The notes section lists the operating systems: Windows, MacOS, Linux, and other operating</p>

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

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:

The screenshot shows the Viettel Ajiant security interface. At the top, there are navigation icons and a search bar with placeholder text: "fx Search by queries (ex: severity = "CRITICAL" AND status = "NEW"), or keywords (ex: "vcs_ajiant")". Below the search bar is a summary table with the following data:

SEVERITY	Critical	High	Medium	Low	No Impact	STATUS	New	In progress	False positive	Closed
0	176	19.5k	5.4k	0		25k	1	2		1

Below the summary table is a list of 25,030 results, showing details for each alert. The columns include: Severity, Status, Timestamp create, Host name, Scenario, Object, Rule Id, and Description. The list includes various entries such as "ANM-HUNGTX Execution", "ANM-HUNGTX Execution", and "Windows_MITRE_ATTACK_InitialAccess_DriveByCompromise_T1189". The "Description" column provides a brief summary of the detected attack technique or process.

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;

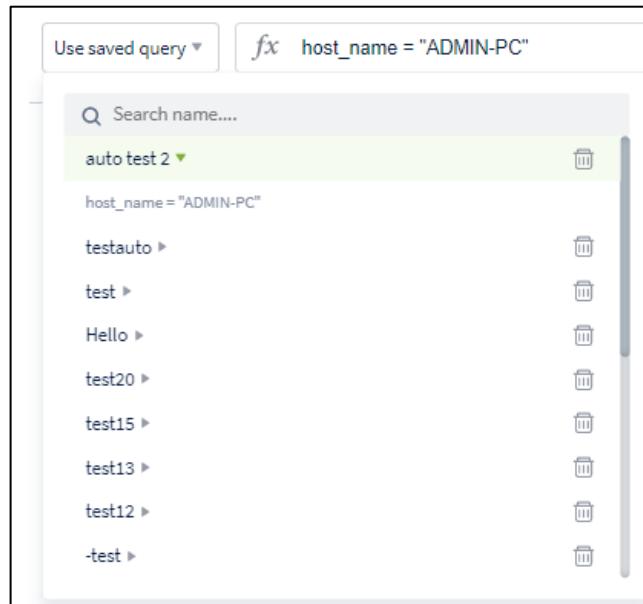
Search by query sentence



- 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:

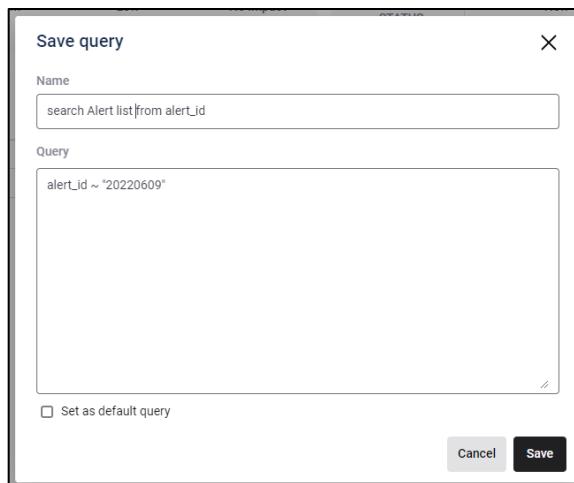
- + <school_name> are the following values:
 - severity: severity level of the Alert
 - Alert_id: Alert code
 - status: the state of the Alert
 - group: event alert group
 - hostname: Name of the workstation
 - scenario: script generating Alerts based on MITRE ATT&CK
 - assignee: the person assigned 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.

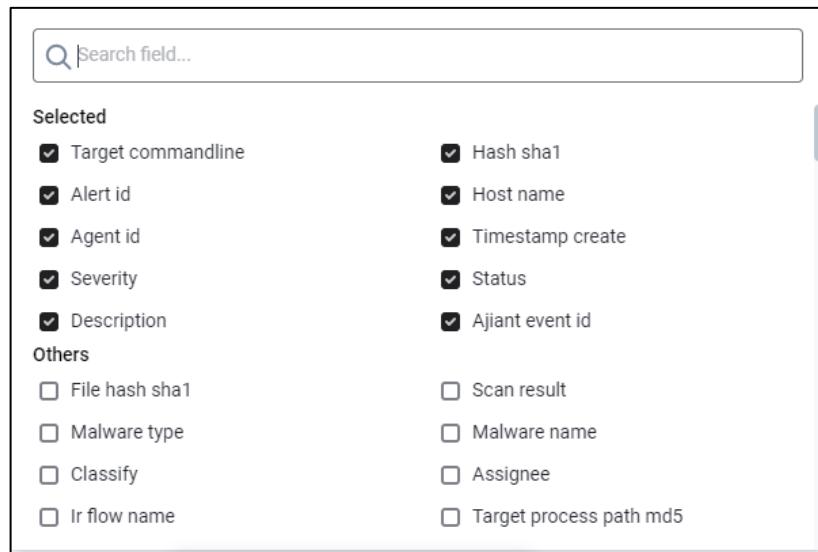
3.3.2 Alert List

Purpose: To display the list of Alerts in the system;

Allow viewing the list of Alerts that meet the search criteria.

Save query		fx alert_id ~ "20220609"					Last 24 hours		Group rows by...	Hide statistics		
SEVERITY		Critical	High	Medium	Low	No Impact	STATUS		New	In progress	False positive	Closed
Showing 2 of 2 result(s) 09/06/2022 09:06:27 - 10/06/2022 09:06:27												
<input type="checkbox"/>	Host name	Severity	Alert id	Status	Ajant event id	Agent id	Timestamp create	Target commandline	Hash sha1	Description	Action	
<input type="checkbox"/>	ubuntu18	HIGH	20220609_173832_553078267_618098...	● New	500	D8EACAB11DA9F0A3F0F65575E9E9C313DC61A83B	09/06/2022 17:38:31	N/A	N/A	Computer ubu		
<input type="checkbox"/>	localhost.localdo...	HIGH	20220609_113824_267803584_564214...	● New	500	31F6FA372944D72C2DC854E155A63170CE9686AD	09/06/2022 11:38:23	N/A	N/A	Computer loci		

1. Select 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:

SEVERITY	Critical	High	Medium	Low	No impact	STATUS	New	In progress	False positive	Closed
Showing 2 of 2 result(s) 09/06/2022 09:06:27 - 10/06/2022 09:06:27										
<input type="checkbox"/> Host name	0	2	0	0	0	<input type="radio"/> New	2	0	0	0
<input type="checkbox"/> ubuntu18						Ajiant event id	Agent id	Timestamp create	Target commandline	Hash sha1
<input type="checkbox"/> localhost.localdo...						20220609_173832_553078267_618098...	500	09/06/2022 17:38:31	N/A	N/A
						20220609_113824_267803584_564214...	500	09/06/2022 11:38:23	N/A	N/A

- + 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:

SEVERITY	Critical 0	High 2	Medium 0	Low 0	No impact 0	STATUS	New 2	In progress 0	False positive 0	Closed 0
Showing 2 of 2 result(s) 09/06/2022 09:06:27 - 10/06/2022 09:06:27										
Selected 2 alert(s) Update status Add to IRFlow Export data Clear selection										
Host name	Severity	Agent id	Status	Ajiant event id	Alert id	Timestamp create	Target commandline	Hash sha1	Description	Action
ubuntu18	HIGH	D8EACAB11DA9F0A3F0F65575E9E9C313DC61A83B	New	500	20220609_173832_553078267_610098	09/06/2022 17:38:31	N/A	N/A	Computer ubur	
localhost.localdomain	HIGH	31F6FA372944D72C2DC854E155A63170CE9686AD	New	500	20220609_113824_267803584_564214	09/06/2022 11:38:23	N/A	N/A	Computer loca	

2. Select to update the status of the Alert:

Update status to:

Comment

Write something...

Cancel
Update status

- 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.

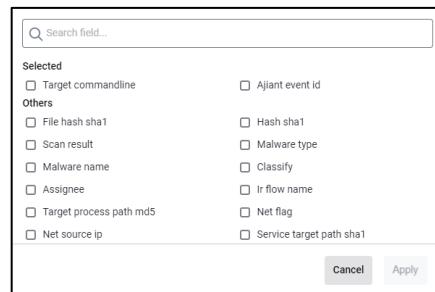
Alerts with the same selected criteria and status will be grouped into a single line in the result list.

Fields	Number of alerts	Action
target_commandline: N/A ajant_event_id: N/A	189	
target_commandline: N/A ajant_event_id: 3	7	
target_commandline: N/A ajant_event_id: 11	155	
target_commandline: N/A ajant_event_id: 13	2	
target_commandline: N/A ajant_event_id: 23	1	
target_commandline: N/A ajant_event_id: 400	1	
target_commandline: N/A ajant_event_id: 500	35	

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.

The screenshot shows the 'View Alert Details' interface for an alert with the ID 20220609_173832_553078267_618098. The alert is marked as NEW and HIGH priority. The summary includes the host name 'ubuntu18'. The interface is divided into several sections:

- General Information:** Shows the alert ID, priority, and creation date (09/06/2022 17:38:31). Buttons for 'Add to IRFlow', 'Related events', 'Enhance Alert', and 'Update status' are available.
- Source event logs:** Section 1 (highlighted with a yellow box). It shows 1 result(s) for the rule 'Anomaly_Detection_Monitor_Agent_Disconnect'. The log entry is: SystemTimeStamp 09/06/2022 17:38:30, Event ID 500, Description Agent was disconnected.
- Advanced:** Section 2 (highlighted with a yellow box). It includes sections for Host (Client ID: D8EACAB11DA9F0A3F0F65575E9E9C313DC61A83B, Hostname: ubuntu18), Network Connection (MAC: 00:0c:29:fb:19:eb), and Others (Create time: 09/06/2022 17:38:30, Log provider name: AdvanceCollector, Source log: mixed, Sub category: Monitor, Description: Computer ubuntu18 was disconnected at least 30 days).
- Raw data:** Section 3 (highlighted with a yellow box). This section contains raw log data and a 'Show columns' button.

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:



The dialog box has a title 'Update status to:' and a dropdown menu currently set to 'False Positive'. Below the dropdown is a 'Comment' section with a placeholder 'Write something...'. At the bottom are two buttons: 'Cancel' and 'Update status'.

- 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;

● **Closed**
khaitb update status into **Closed**
22/04/2022 18:07:01

● **In progress**
khaitb added the alert into the IR Flow **IRF_Demo**
22/04/2022 17:48:52

● **New**
VCS-aJiant created the alert.
22/04/2022 17:35:48

4 – Tabs containing information related to Alerts:

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

Description (1)

Detect attack technique T1562.004: Disable or Modify System Firewall on ANM-PHUCVD2. Process with path = C:\program files\dell\supportassistagent\bin\supportassistagent.exe (PID = 7656, commandline = "C:\Program Files\dell\SupportAssistAgent\bin\SupportAssistAgent.exe") is creating child process with path = C:\windows\system32\netsh.exe (commandline = "netsh.exe" http delete sslicert ipport=0.0.0.5700, PID = 9732) to the disable firewall.

Rule ID: [Anomaly_Detection_ATTCK_T1562_004_Dis...](#)

Source event logs (2)

No tracked events!

Advanced

File
This file is impacted (created/modified/deleted/executed) suspiciously.

Target process path **Signed** C:\windows\system32\netsh.exe

Source process path Unknown C:\program files\dell\supportassistagent\bin\supportassistagent.exe

Process
This source/target process has suspicious behaviours.

Target process path **Signed** C:\windows\system32\netsh.exe

Source commandline Unknown "C:\Program Files\dell\SupportAssistAgent\bin\SupportAssistAgent.exe"

Target commandline Unknown "netsh.exe" http delete sslicert ipport=0.0.0.5700

Source process path Unknown C:\program files\dell\supportassistagent\bin\supportassistagent.exe

Host
This information is about suspicious host.

Client Id 9C4C8D5F62C98BE5918732E0D8D91DCD01121CD2

Ip dcn 10.61.188.2

MAC Address a8:6b:ad:71:14:2b,1a:6b:ad:71:14:2b,2a:6b:ad:71:14:2b,00:50:56:c0:00:01,00:50:56:c0:00:08,48:4d:7e:ba:be:53

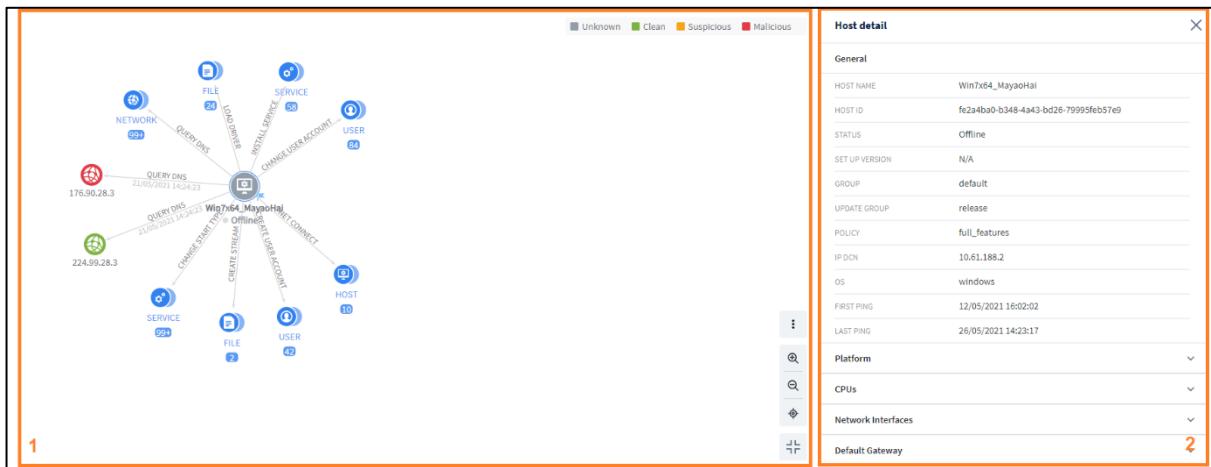
Others
These other information provides more context about this alert collected by VCS-aJiant.

- **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.



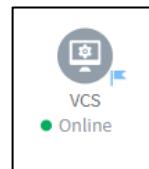
1 – Chart display area and chart operations

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:

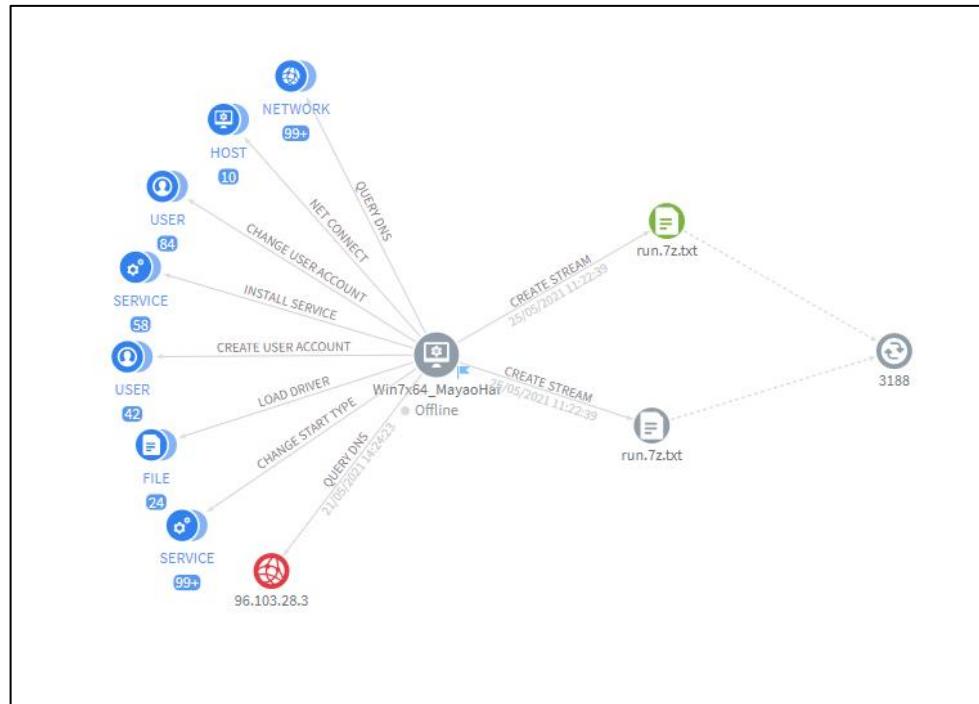


Each object includes the following states:

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:

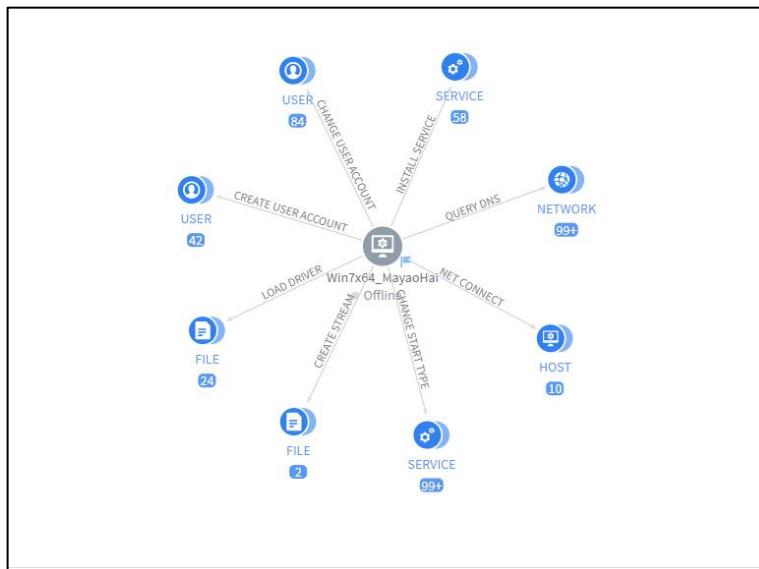


The operations supporting chart display include:

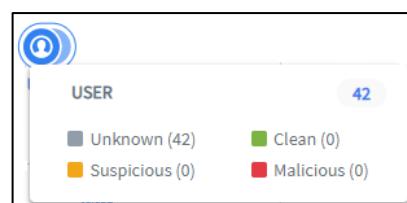
Display support operation	Meaning
<div style="display: flex; align-items: center;"> ⋮ Hide reference Hide relationship name </div>	<p>Allow toggling the visibility of information on the chart:</p> <p>Reference: When selected, allows hiding/showing reference information, including dashed arrows and reference objects for all existing objects on the chart;</p> <p>Relationship name: When selected, allows hiding/showing the relationship name information above all solid arrows currently present on the chart.</p> <p style="text-align: center;">+</p> <p style="text-align: center;">+</p>

	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:

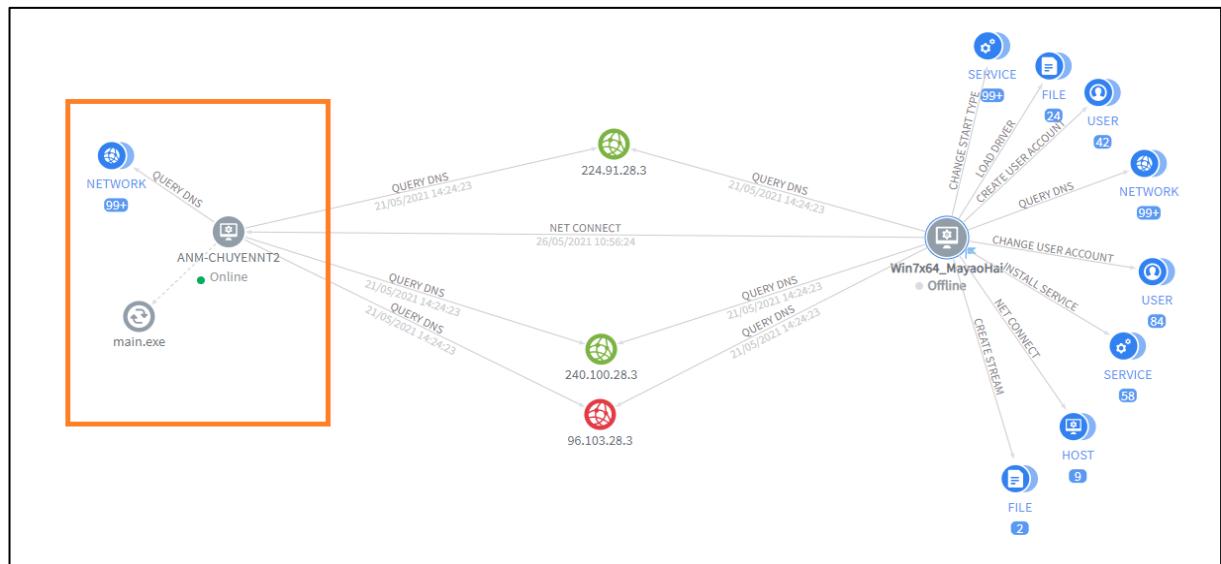
Objects in this group network						
<input type="text"/> Search object... <input type="button" value="Search"/> <input type="button" value="View column"/>						
<input checked="" type="checkbox"/> Unknown (48) <input checked="" type="checkbox"/> Clean (125) <input checked="" type="checkbox"/> Malicious (87)						
Selected 1/20 node(s) <input type="button" value="Show on graph"/> <input type="button" value="Clear selection"/>						
□ STATUS	DOMAIN ADDRESS	IP	LOCAL PORT	PROCESS NAME	ACTION	
<input checked="" type="checkbox"/> ● Clean	ocsp.verisign.com	240.100.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Clean	crl4.digicert.com	80.105.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Clean	crl.microsoft.com	16.87.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Malicious	www.microsoft.com	96.103.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Clean	ocsp.digicert.com	240.94.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Clean	crl.verisign.com	224.91.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Malicious	www.msftncsi.com	0.96.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Clean	csc3-2010-crl.verisign.com	112.89.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Clean	ocsp.globalsign.com	48.88.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> ● Clean	crl4.digicert.com	80.105.28.3	N/A	SYSTEM	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Showing 20/260 result(s)

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

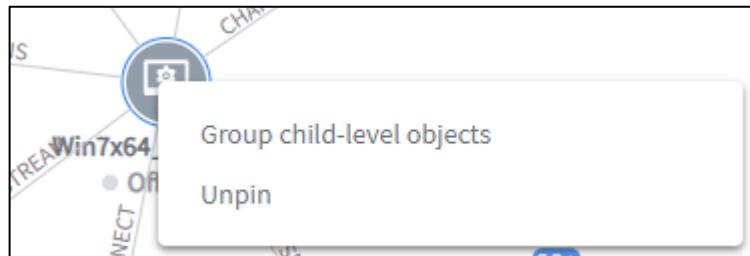
+ Once the appropriate object has been selected, choose to display one object on the chart or select up to 20 objects to display on the chart;

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:

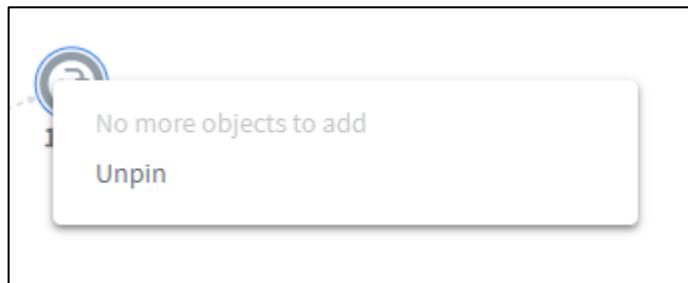
- + On the main machine/regular computer: Supports collapsing objects to their default state when displaying the machine (including only objects directly related to the machine; if there are multiple objects of the same type, they are displayed as a group) by right-clicking on the object, then selecting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



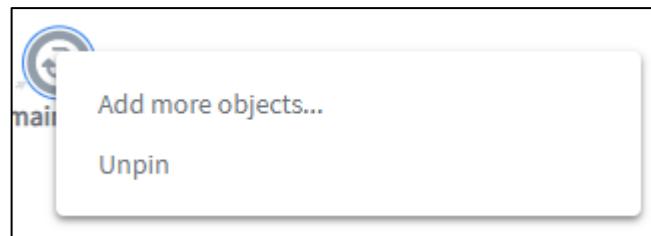
- + For other objects: Support collapsing by grouping according to object type and relationship type with peer objects by right-clicking on the object, then selecting "Group same-level objects";



- + 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.

The screenshot shows a software interface for managing objects. On the left, a sidebar lists 'Show more object' with categories: Files (1), Network (5), Process (3), and Registry (3). The 'Registry' category is highlighted with a green background and a red border, labeled '1'. The main area displays a table for the 'Malicious' category, which has 3 results. The table has columns: STATUS, DOMAIN ADDRESS, IP, LOCAL PORT, PROCESS NAME, and ACTION. Each row shows a red dot next to the word 'Malicious'. The table is labeled '2' at the top right. The bottom of the interface shows the text 'Showing 1/1 result(s)'.

Malicious (3)					
STATUS	DOMAIN ADDRESS	IP	LOCAL PORT	PROCESS NAME	ACTION
<input type="checkbox"/>	N/A	127.0.0.1	1588	main.exe	
<input type="checkbox"/>	N/A	127.0.0.1	6668	main.exe	
<input type="checkbox"/>	N/A	0.0.0.0	0	main.exe	

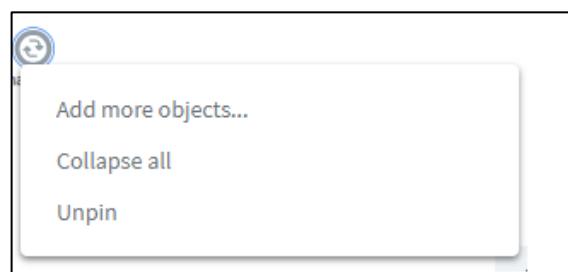
3

- 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);

General	
HOST NAME	Win7x64_MayaHai
HOST ID	fe2a4ba0-b348-4a43-bd26-79995feb57e9
STATUS	Offline
SET UP VERSION	N/A
GROUP	default
UPDATE GROUP	release
POLICY	full_features
IP DCN	10.61.188.2
OS	windows
FIRST PING	12/05/2021 16:02:02
LAST PING	26/05/2021 14:23:17

Platform	
CPU	▼
Network Interfaces	▼
Default Gateway	▼

- 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.

Process detail	
General	
PROCESS ID	1432
PROCESS NAME	main.exe
MD5	1e092a44d44c29ef8d6bfc3a74f34b73
SHA256	1941d3f261033344b22c5e9cf246e5683c17d450ac87d0af6f3ed7a52f431bb6
PROCESS PATH	C:\users\admin\desktop\taodataoang\main.exe
FILE COMPANY	N/A
FILE DESCRIPTION	N/A
FILE VERSION	N/A
FILE PRODUCT	N/A
USER NAME	admin
COMMANDLINE	.\main.exe
INTEGRITY LEVEL	HIGH

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:

Update status to:

False Positive

Comment

Add to False Positive

Cancel
Update status

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:

Update status to:
Closed
Comment
done
Cancel Update status

Bước 3: Select Update Status to "Closed";

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

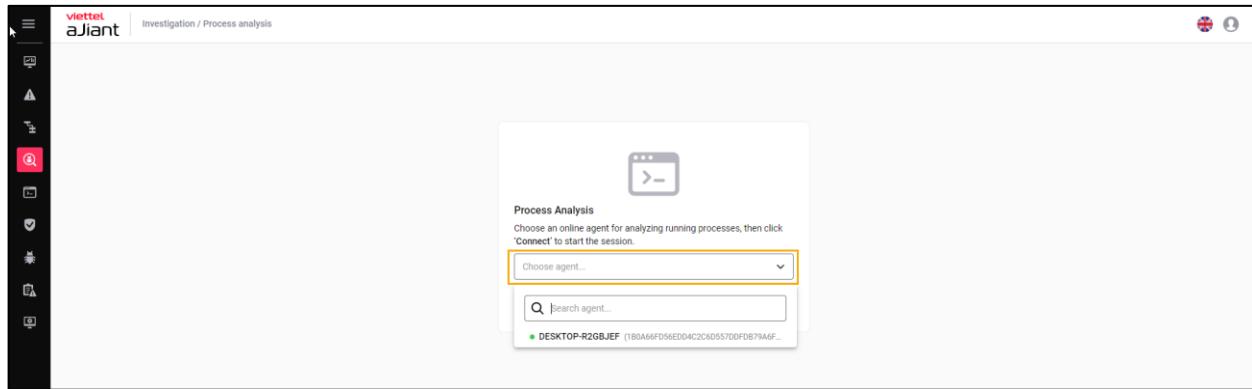
- Select "Update status" to confirm closing the Alert;
- Select "Cancel" to confirm the cancellation of the Alert closure action;

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*

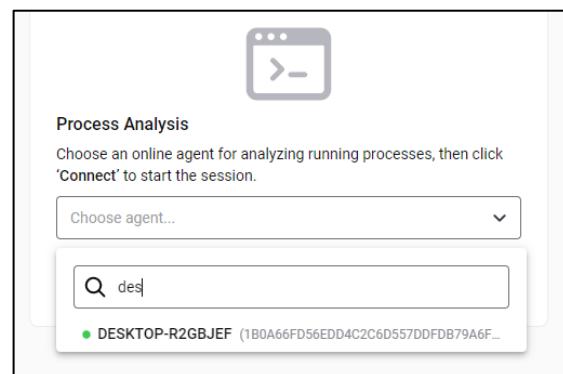
- Purpose: This function allows users to establish connections and monitor the status of processes on their machines. Specifically:



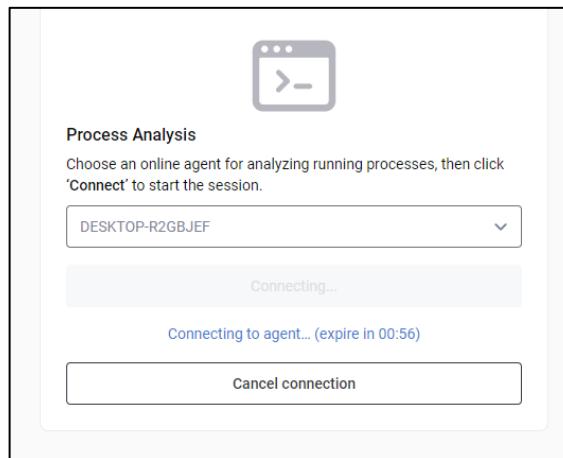
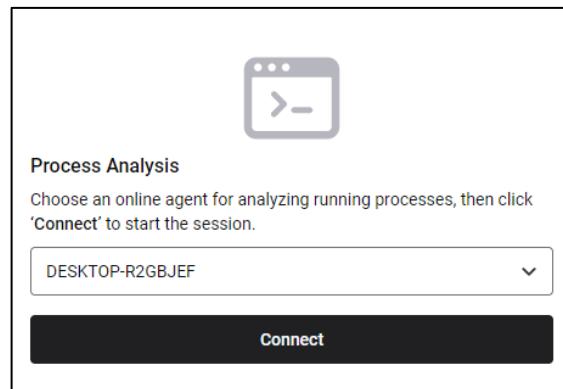
User device list:

- + 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.

Name	PID	Path	User name	Command line	Signature	Action
explorer.exe	5048	C:\Windows\explorer.exe	test	C:\Windows\Explorer.EXE	Microsoft Windows	
SecurityHealthSystray.exe	7156	C:\Windows\System32\SecurityHealthSystray.exe	test	"C:\Windows\System32\SecurityHealthSystray.exe"	N/A	
vm3dservice.exe	5520	C:\Windows\System32\vm3dservice.exe	test	"C:\Windows\System32\vm3dservice.exe" -u	VMware, Inc.	
vmtoolsd.exe	5956	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	test	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vm... VMware, Inc.		
OneDrive.exe	7264	C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.exe	test	"C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.exe"	Microsoft Corporation	
mmc.exe	6132	C:\Windows\System32\mmc.exe	test	"C:\Windows\System32\mmc.exe" "C:\Windows\system32\per... N/A		
cmd.exe	3212	C:\Users\test\Desktop\New folder\cmd.exe	test	"C:\Users\test\Desktop\New folder\cmd.exe"	N/A	
conhost.exe	9252	C:\Windows\System32\conhost.exe	test	"C:\Windows\System32\conhost.exe" 0x4	N/A	
Code.exe	11092	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"	Microsoft Corporation	
Code.exe	3284	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=gpu-pro...	Microsoft Corporation	
Code.exe	13300	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=rendere...	Microsoft Corporation	
Code.exe	9228	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=rendere...	Microsoft Corporation	
Code.exe	5008	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --nolazy --ins...	Microsoft Corporation	
Code.exe	13328	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=utility...	Microsoft Corporation	
Code.exe	4896	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=rendere...	Microsoft Corporation	
chrome.exe	8308	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	test	"C:\Program Files (x86)\Google\Chrome\Application\chrome.e...	Google LLC	
chrome.exe	6664	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	test	"C:\Program Files (x86)\Google\Chrome\Application\chrome.e...	Google LLC	

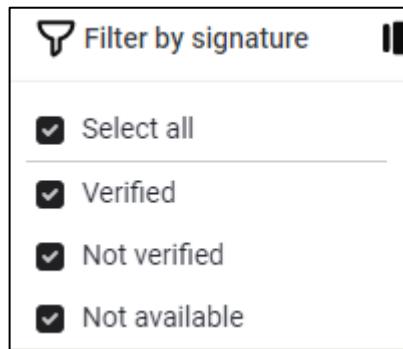
The interface is divided into information groups:

- 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.

116 result(s) Last updated: 21/06/2022 11:50:01							Show verified signature <input checked="" type="checkbox"/>	View as abstract <input type="checkbox"/>	Filter by signature <input type="checkbox"/>	Show columns <input type="checkbox"/>
Name	PID	Path	User name	Command line	Signature	Action				
svchost.exe	3360	C:\Windows\System32\svchost.exe	test	C:\Windows\system32\svchost.exe -k UnistackSvGroup	Microsoft Windows Publisher					
svchost.exe	3680	C:\Windows\System32\svchost.exe	test	C:\Windows\system32\svchost.exe -k ClipboardSvGroup -p	Microsoft Windows Publisher					
SecurityHealthService.exe	6076	C:\Windows\System32\SecurityHealthService.exe	SYSTEM	"C:\Windows\System32\SecurityHealthService.exe"	Microsoft Windows Publisher					
svchost.exe	8084	C:\Windows\System32\svchost.exe	SYSTEM	C:\Windows\System32\svchost.exe -k netsvcs -p	Microsoft Windows Publisher					
▼ VESSvc.exe	14380	C:\Program Files\Aijant\VESSvc.exe	SYSTEM	"C:\Program Files\Aijant\VESSvc.exe"	N/A					
VESServiceManager.exe	3500	C:\Program Files\Aijant\VESConfigurationManager.exe	SYSTEM	"C:\Program Files\Aijant\VESConfigurationManager.exe"	N/A					
VESConnectionManager.exe	8628	C:\Program Files\Aijant\VESConnectionManager.exe	SYSTEM	"C:\Program Files\Aijant\VESConnectionManager.exe"	N/A					
VESUpdater.exe	11864	C:\Program Files\Aijant\VESUpdater.exe	SYSTEM	"C:\Program Files\Aijant\VESUpdater.exe"	N/A					
VESResponse.exe	18852	C:\Program Files\Aijant\vesresponse\VESResponse.exe	SYSTEM	"C:\Program Files\Aijant\vesresponse\VESResponse.exe"	Viettel Group					
▼ VESProPre.exe	16604	C:\Program Files\Aijant\propre\VESProPre.exe	SYSTEM	"C:\Program Files\Aijant\propre\VESProPre.exe"	N/A					
SecurityNotify.exe	7640	C:\Program Files\Aijant\propre\BL5\SecurityNotify.exe	test	"C:\Program Files\Aijant\propre\BL5\SecurityNotify.exe" -ppid ...	Viettel Group					
VESAutoScan.exe	16592	C:\Program Files\Aijant\autoScan\VESAutoScan.exe	SYSTEM	"C:\Program Files\Aijant\autoScan\VESAutoScan.exe"	Viettel Group					
VESCollector.exe	18304	C:\Program Files\Aijant\collector\VESCollector.exe	SYSTEM	"C:\Program Files\Aijant\collector\VESCollector.exe"	N/A					
svchost.exe	2656	C:\Windows\System32\svchost.exe	SYSTEM	"C:\Windows\svchost.exe"	Microsoft Windows Publisher					
TrustedInstaller.exe	3908	C:\Windows\System32\wermgr.exe	SYSTEM	C:\Windows\system32\wermgr.exe -upload	Microsoft Windows					
lsass.exe	800	C:\Windows\System32\lsass.exe	SYSTEM	C:\Windows\system32\lsass.exe	Microsoft Windows Publisher					
fontdrvhost.exe	940	C:\Windows\System32\fontdrvhost.exe	UMFD-0	"fontdrvhost.exe"	Microsoft Windows					

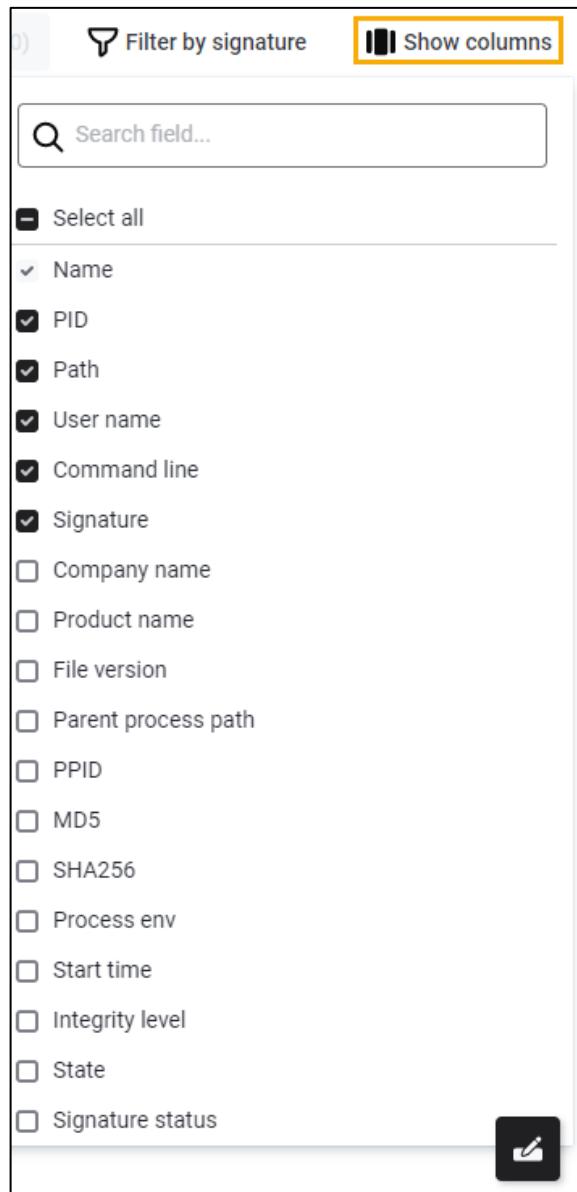
Back to top

- **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;

Show columns ▾

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;

Process detail

Loaded modules File handles **Key handles** Threads Sections Network connections

14 result(s)

Action
\REGISTRY\USER\{1-5-21-657600163-1704432705-4217905726-1001\Classes\Local Settings\Software\Microsoft
\REGISTRY\USER\{1-5-21-657600163-1704432705-4217905726-1001\Classes
\REGISTRY\USER\{1-5-21-657600163-1704432705-4217905726-1001\Classes
\REGISTRY\USER\{1-5-21-657600163-1704432705-4217905726-1001\Classes
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{D65231B0-B2F1-4B57-A4CE...
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{7C5A0EF-A0FB-4BFC-874A...
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744...
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Ole
\REGISTRY\MACHINE
\REGISTRY\MACHINE

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

117 result(s) | Last updated: 21/06/2022 11:50:01

Show verified signature View all artifacts (1) Filter by signature Show columns

Time	Agent ID	Object	From	Reference	Action
21/06/2022 11:59:51	1B0A66FD56ED04C2C6055700FD879A6F5040FCCC	C:\Windows\System32\svchost.exe	PROCESS_ANALYZE_705964A9		Microsoft Windows
					Microsoft Corporation
					Microsoft Windows
					Microsoft Corporation
					Microsoft Windows
					Microsoft Corporation
					Microsoft Corporation
					Microsoft Corporation
					Microsoft Corporation

3.4.2 *Investigation_Event Search*

Search Event

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

The screenshot shows a search results table with 64,025 results. The table has columns for ID, POPULAR, EVENTID, COMPUTER, LOGTYPE, and LASTTIME. The search term 'AgentID = '1804004042305570DF087944P504F0C0'' is highlighted in the search bar. The results show various AgentID values and their corresponding event details. The table is paginated with '1' at the top right.

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

The screenshot shows the 'Add to search' feature for the 'AgentID' field. The 'Popular' and 'Others' fields are highlighted with a yellow box. The 'AgentID' field is selected, and the 'Add to search' button is highlighted with a yellow box. The search results table shows 130,071 results for the query 'AgentID = '1804004042305570DF087944P504F0C0''. The results are identical to the previous screenshot.

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;

System timestamp	Computer	Process path	Description
27/06/2022 07:51:40	a.Jiant-automationAPI-1	N/A	Process [5612] C:\Windows\System32\cmd.exe has been created by [5612] C:\Windows\System32\cmd.exe
27/06/2022 07:51:42	a.Jiant-automationAPI-1	N/A	Process [7848] C:\Windows\System32\cmd.exe has been created by [10008] C:\Program...
27/06/2022 07:51:42	a.Jiant-automationAPI-1	N/A	Process [2376] C:\Windows\System32\SecEdit.exe has been created by [7848] C:\Wind...
27/06/2022 07:51:40	a.Jiant-automationAPI-1	N/A	Process [10480] C:\Windows\System32\more.com has been created by [5612] C:\Wind...
27/06/2022 07:51:40	a.Jiant-automationAPI-1	N/A	Process [10144] C:\Windows\System32\wbem\WMIC.exe has been created by [5612] C:\...
27/06/2022 14:50:43	Win7x86TestEDR	N/A	Process [11356] C:\Windows\System32\more.com has been created by [14300] C:\Wind...
27/06/2022 14:50:44	Win7x86TestEDR	N/A	Process [10496] C:\Windows\System32\SecEdit.exe has been created by [13056] C:\Wind...
27/06/2022 14:50:42	Win7x86TestEDR	N/A	Process [1968] C:\Windows\System32\wbem\WMIC.exe has been created by [14300] C:\...
27/06/2022 14:50:44	Win7x86TestEDR	N/A	Process [13056] C:\Windows\System32\cmd.exe has been created by [5252] C:\Program...
27/06/2022 14:50:42	Win7x86TestEDR	N/A	Process [14300] C:\Windows\System32\cmd.exe has been created by [4804] C:\Program...
27/06/2022 14:47:55	Win7x86TestEDR	N/A	Process [9496] C:\Program Files\Google\Update\GoogleUpdate.exe has been created by [...
27/06/2022 14:48:51	Win7x86TestEDR	N/A	Process [0456] C:\Program Files\Google\Update\GoogleUpdate.exe has been created by [...
27/06/2022 07:47:36	a.Jiant-automationAPI-1	N/A	Process [9684] C:\Windows\System32\ROUTE.EXE has been created by [4160] C:\Program...
27/06/2022 14:45:41	Win7x86TestEDR	N/A	Process [3600] C:\Windows\System32\cmd.exe has been created by [5252] C:\Program...
27/06/2022 14:45:42	Win7x86TestEDR	N/A	Process [3944] C:\Windows\System32\SecEdit.exe has been created by [3600] C:\Wind...
27/06/2022 14:45:40	Win7x86TestEDR	N/A	Process [13324] C:\Windows\System32\cmd.exe has been created by [10848] C:\Program...
27/06/2022 14:45:40	Win7x86TestEDR	N/A	Process [13348] C:\Windows\System32\more.com has been created by [13324] C:\Wind...
27/06/2022 07:45:57	a.Jiant-automationAPI-1	N/A	Process [14204] C:\Program Files\Viettel\Update\GoogleUpdate.exe has been created by [...

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.

Showing 50 of 264,107 result(s) | 27/06/2022 14:52:15 - 27/06/2022 15:07:15

Source process path	Time stamp
C:\Windows\System32\services.exe	27/06/2022 15:07:00
N/A	27/06/2022 15:07:00
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	27/06/2022 15:07:00
C:\Windows\system32\cmd.exe	27/06/2022 15:07:00
C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:00
C:\program files (x86)\viettel\securityagent\worker.exe	27/06/2022 15:07:00
C:\program files (x86)\viettel\securityagent\worker.exe	27/06/2022 15:07:00
C:\Users\admin\AppData\Local\JetBrains\IntelliJ IDEA Community Edition 2020.3.2\jb\bin\java.exe	27/06/2022 15:07:00
C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:00
C:\Windows\System32\svchost.exe	27/06/2022 15:07:00
N/A	27/06/2022 15:07:00
C:\Windows\system32\taskhost.exe	27/06/2022 15:07:00
C:\program files\windowsapps\microsoft.microsoftofficehub_18.2008.12711.0_x64_8wekyb3d8bbwe\localbridge.exe	27/06/2022 15:07:00
C:\Program Files\Microsoft Office\Office16\EXCEL.EXE	27/06/2022 15:07:00
C:\program files\microsoft office\office16\winword.exe	27/06/2022 15:07:00

Help with Event Search

About events **About fields**

How to use event_id for investigation?

Search by Event ID or description...

Event ID: 0
N/A

Event ID: 1
New process has been created

Event ID: 2
Process changed a file creation time

Event ID: 3
Process created TCP/UDP connections on the machine

Event ID: 4
Sysmon service state changed

Event ID: 5
Process terminated

Event ID: 6
Driver loaded on the system

Event ID: 7
Image loaded in a specific process

Event ID: 8
Process created a thread in another process

Event ID: 9
Process opened for raw read/write access of the disks and volumes

Event ID: 10
Process opened another process with special desired access

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.

Showing 50 of 264,107 result(s) | 27/06/2022 14:52:15 - 27/06/2022 15:07:15

Source process path	Time stamp	Action
C:\Windows\System32\services.exe	27/06/2022 15:07:00	
N/A	27/06/2022 15:07:00	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	27/06/2022 15:07:00	
C:\windows\system32\cmd.exe	27/06/2022 15:07:00	
C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:00	
C:\program files (x86)\viettel\security\agent\worker.exe	27/06/2022 15:07:00	
C:\program files (x86)\viettel\security\agent\worker.exe	27/06/2022 15:07:00	
C:\Users\admin\AppData\Local\JetBrains\IntelliJ IDEA Community Edition 2020.3.2\bin\bin\java.exe	27/06/2022 15:07:00	
C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:00	
C:\Windows\System32\svchost.exe	27/06/2022 15:07:00	
N/A	27/06/2022 15:07:00	

Export Data

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

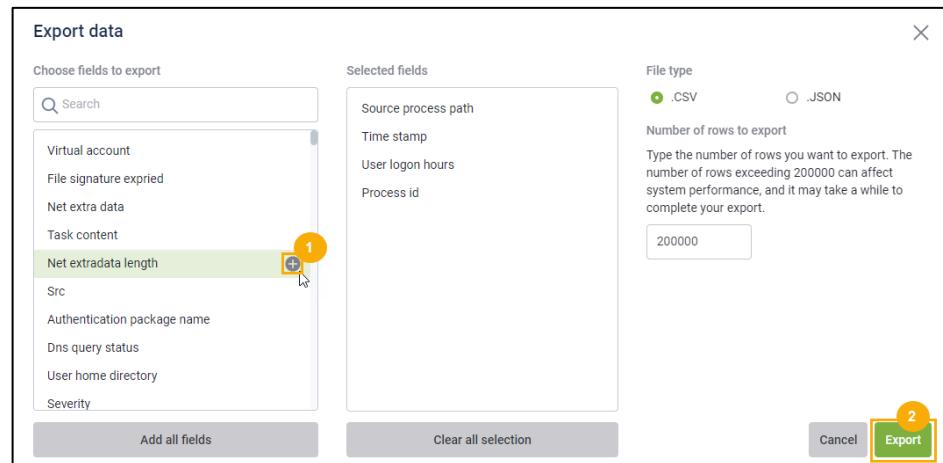
Steps to follow:

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;

Tool Name	Version	Architecture	Output	Parameter
Tool OutputFile_Linux_Params	1	x86	hohoho.txt	N/A
Tool OutputFolder_Linux_Params	1	x64	Test	N/A
Tool OutputFile_Linux_Params	1	x64	hohoho.txt	N/A
Tool StdOut_Linux_LongTime	1	x64	StdOut	N/A
OutputFolder.ps1	1	N/A	Test	N/A
OutputFile.ps1	1	N/A	hohoho.txt	N/A
StdOut.ps1	1	N/A	StdOut	N/A
Tool StdOut_x64_Params.exe	1	x64	StdOut	N/A
Tool StdOut_x86_Params.exe	1	x86	StdOut	N/A
Tool StdOut_Linux_Params	1	x64	StdOut	N/A
Tool StdOut OSX_Params	1	x64	StdOut	N/A
Tool OutputFolder_x64_Params.exe	1	x64	Test	N/A
Tool OutputFile_x64_Params.exe	1	x64	StdOut	N/A
Tool OutputFolder_x86_Params.exe	1	x86	StdOut	N/A
Tool OutputFolder OSX_Params	1	x64	StdOut	N/A
Tool OutputFile x86 Params.exe	1	x86	StdOut	N/A

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:

The screenshot shows the 'Tool management' section of the 'Investigation / Deploy Tool' interface. A search bar at the top is empty. Below it, a table lists 50 of 170 results. The first three rows are highlighted with a yellow background. The fourth row is highlighted with a yellow background and has a yellow circle with the number '1' in the top right corner. The fifth row is highlighted with a yellow background and has a yellow circle with the number '2' in the top right corner. The 'Upload tool' dialog box is open in the center, containing a 'Choose file' button and the text: 'Max file size is 100 MB, supported file types is executable file'. The dialog has a yellow border and a yellow 'X' button in the top right corner. The bottom right corner of the dialog has a yellow circle with the number '1'. The bottom right corner of the entire interface has a yellow circle with the number '1'. The bottom right corner of the 'Upload tool' dialog has a yellow circle with the number '2'.

Tool Name	Version	Architecture	Output	Parameter
Tool OutputFile_Linux_Params	fail	x86	hooho.txt	N/A
Tool OutputFolder_Linux_Params	1	x64	Test	Parameter
Tool OutputFile_Linux_Params	1	x64	hooho.txt	N/A
Tool StdOut_Linux_LongTime	1	x64	StdOut	Parameter
OutputFolder.ps1	1	N/A	Test	Parameter
OutputFile	N/A	N/A	hooho.txt	N/A
Tool StdOut_x64_Params.exe	1	x64	StdOut	Parameter
Tool StdOut_x86_Params.exe	1	x86	StdOut	Parameter
Tool StdOut_Linux_Params	1	x64	StdOut	Parameter
Tool StdOut OSX_Params	1	x64	StdOut	Parameter
Tool OutputFolder_x64_Params.exe	1	x64	Test	Parameter
Tool OutputFile_x64_Params.exe	1	x64	StdOut	Parameter
Tool OutputFolder_x86_Params.exe	1	x86	StdOut	Parameter
Tool OutputFolder OSX_Params	1	x64	StdOut	Parameter
Tool OutputFile_x86_Params.exe	1	x86	StdOut	Parameter

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

Showing 50 of 170 result(s)

Tool management Task management

Search tool...

1

2

Show only my tool

Upload tool

Tool Name	Upload by	Upload Date	Version	Architecture	Output	Parameter
Tool OutputFile_Linux_Params	root_test	14/12/2022 18:38:25	1	x86	hoho.txt	N/A
Tool OutputFolder_Linux_Params	root_test	14/12/2022 18:28:48	1	x86	Test	N/A
Tool OutputFile_Linux_Params	root_test	14/12/2022 18:27:35	1	x86	hoho.txt	N/A
Tool StdOut_Linux_LongTime	root_test	14/12/2022 18:26:59	1	x86	StdOut	N/A
OutputFolder.ps1	root_test	14/12/2022 18:26:02	1	N/A	Test	N/A
OutputFile.ps1	root_test	14/12/2022 18:25:48	1	N/A	hoho.txt	N/A
StdOut.ps1	root_test	14/12/2022 18:25:18	1	N/A	StdOut	N/A
Tool StdOut_x64_Params.exe	root_test	14/12/2022 18:24:08	1	x64	StdOut	N/A
Tool StdOut_x86_Params.exe	root_test	14/12/2022 18:23:55	1	x86	StdOut	N/A
Tool StdOut_Linux_Params	root_test	14/12/2022 18:23:25	1	x64	StdOut	N/A
Tool StdOut OSX_Params	root_test	14/12/2022 18:23:05	1	x64	StdOut	N/A
Tool OutputFolder_x86_Params.exe						
Tool OutputFolder OSX_Params						
Tool OutputFile x64_Params.exe						
Tool OutputFile x86_Params.exe						

Deploy tool

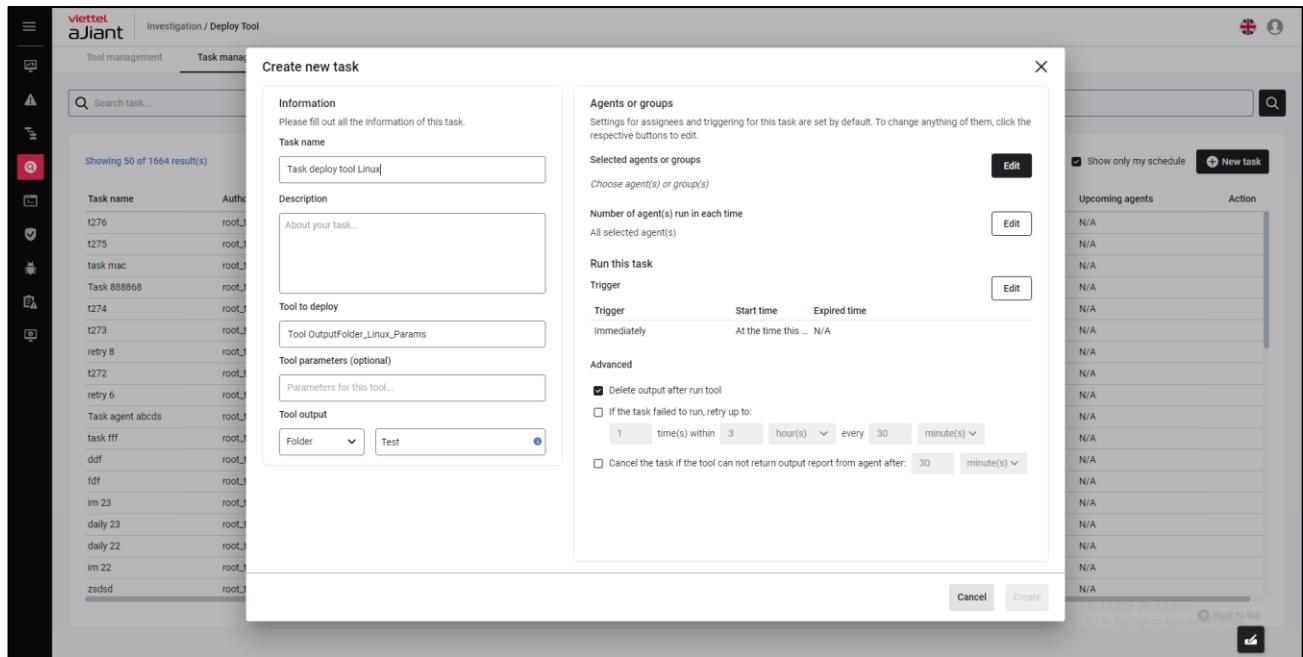
Purpose: Configure deploy tool information under the agent

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:

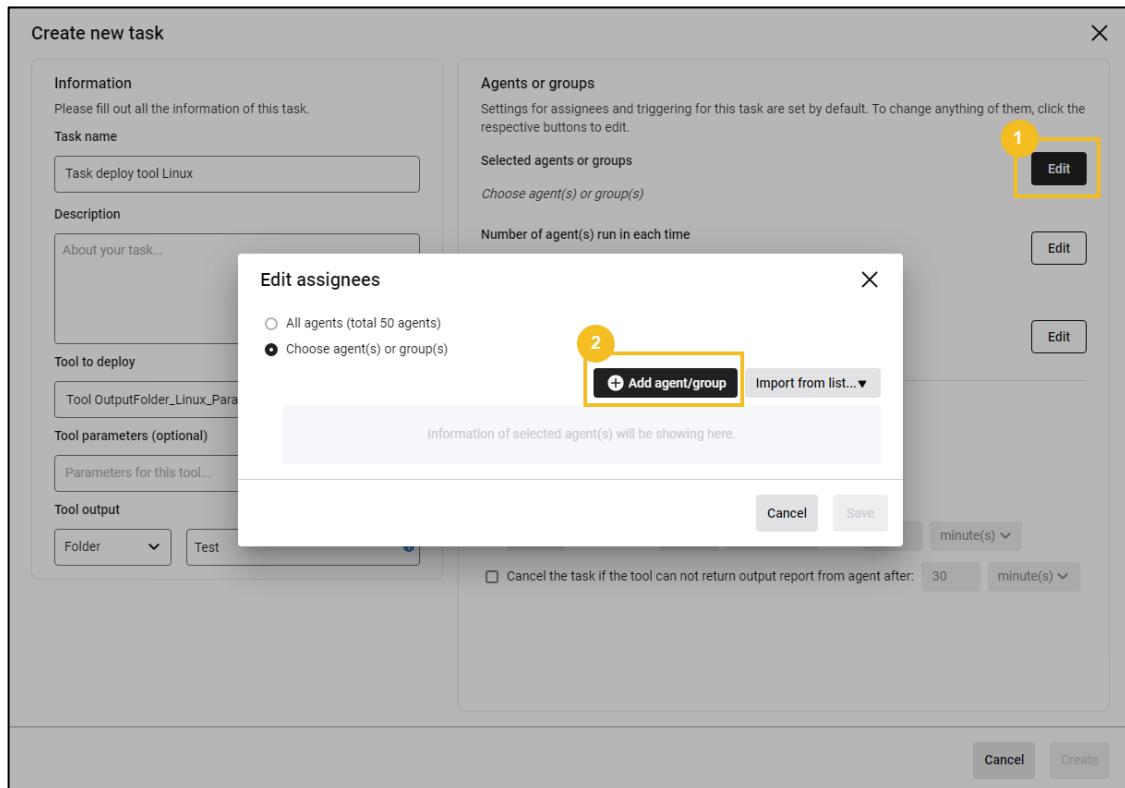


- Enter the task information for tool deployment: Task name, Description, Tool parameters, Tool output;

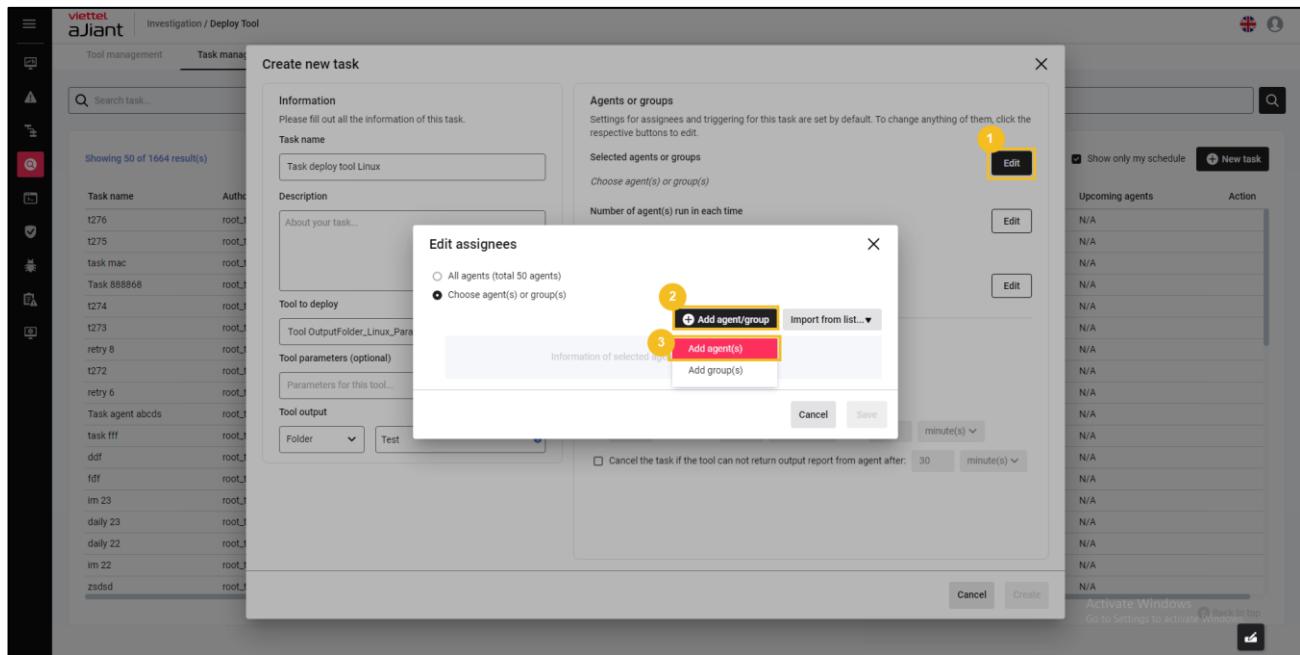
- Select the group and workstation (agent) information to perform the deployment:

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

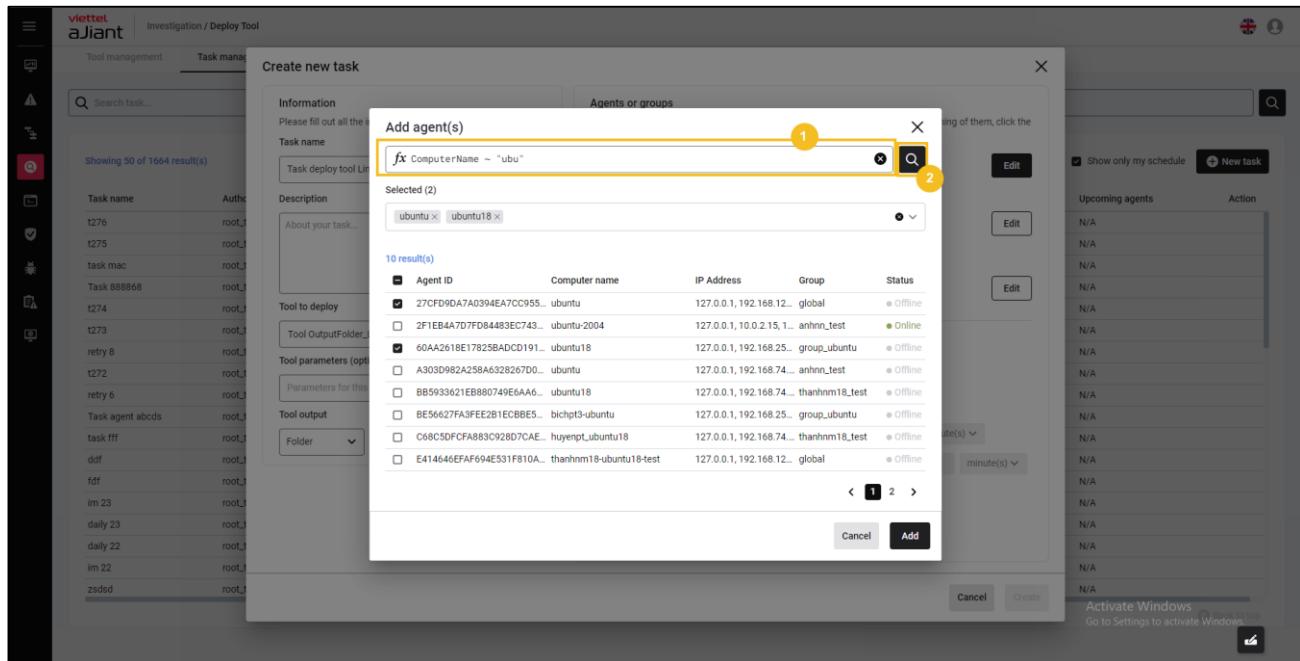
Select agents or groups to perform deployment – Choose agent(s) or group(s):



- + Select Add agent(s):

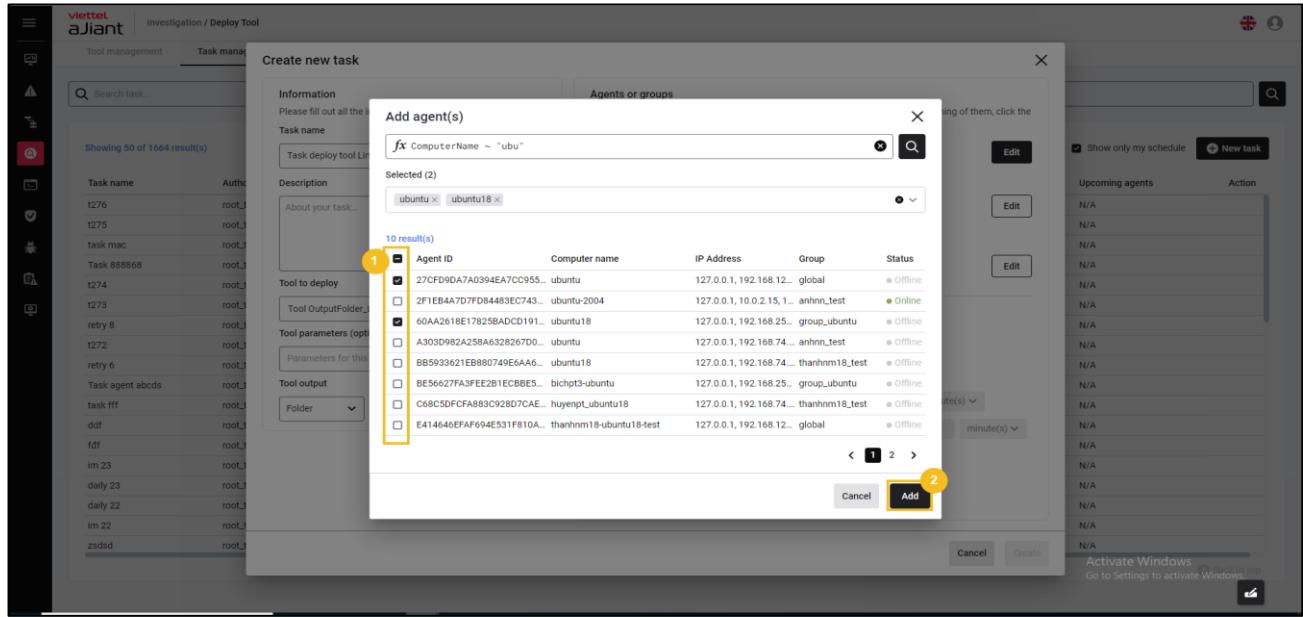


- **Search Agent:** Allows creating query statements and using query statements to search for Agents.

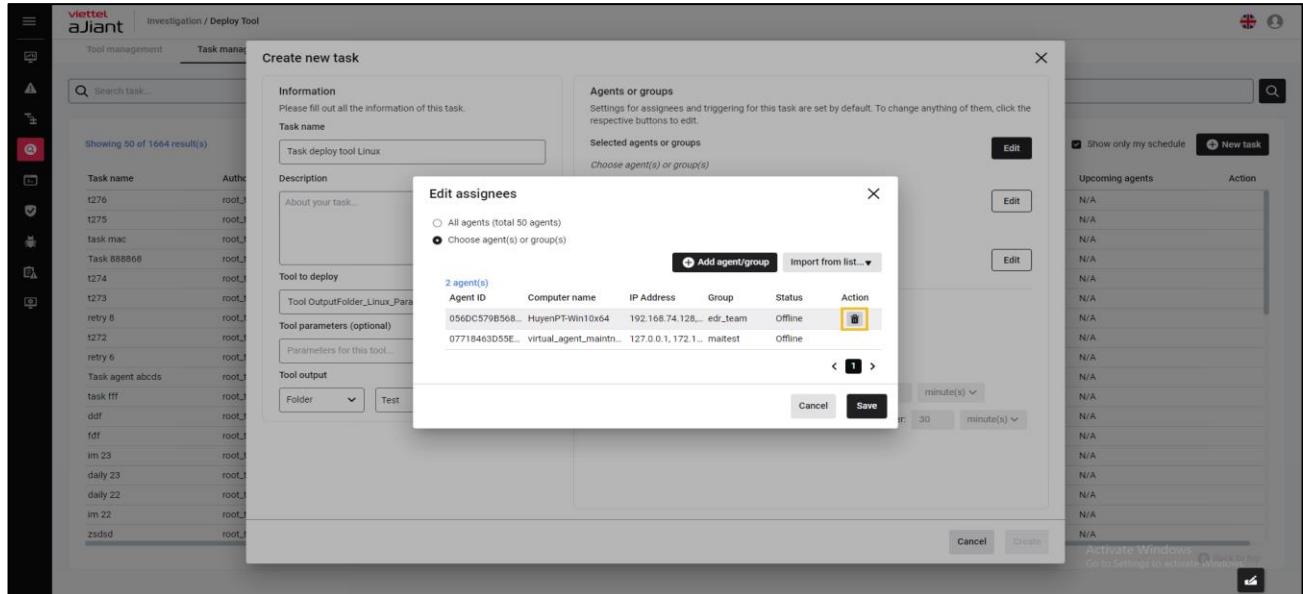


- **Select the Agent(s) to deploy by checking one or more Agents > Information of the selected Agent(s) will be displayed in the Selected box > choose**

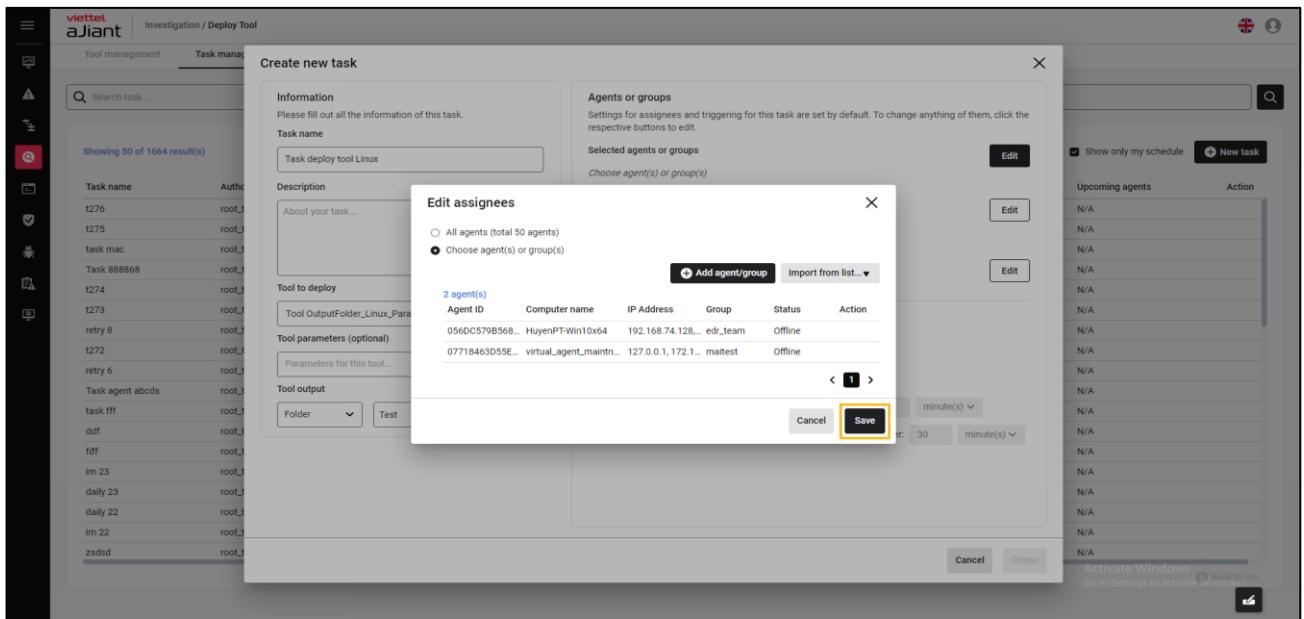
Cancel to cancel adding Agents for deployment or click the Add button to confirm the list of Agent(s):



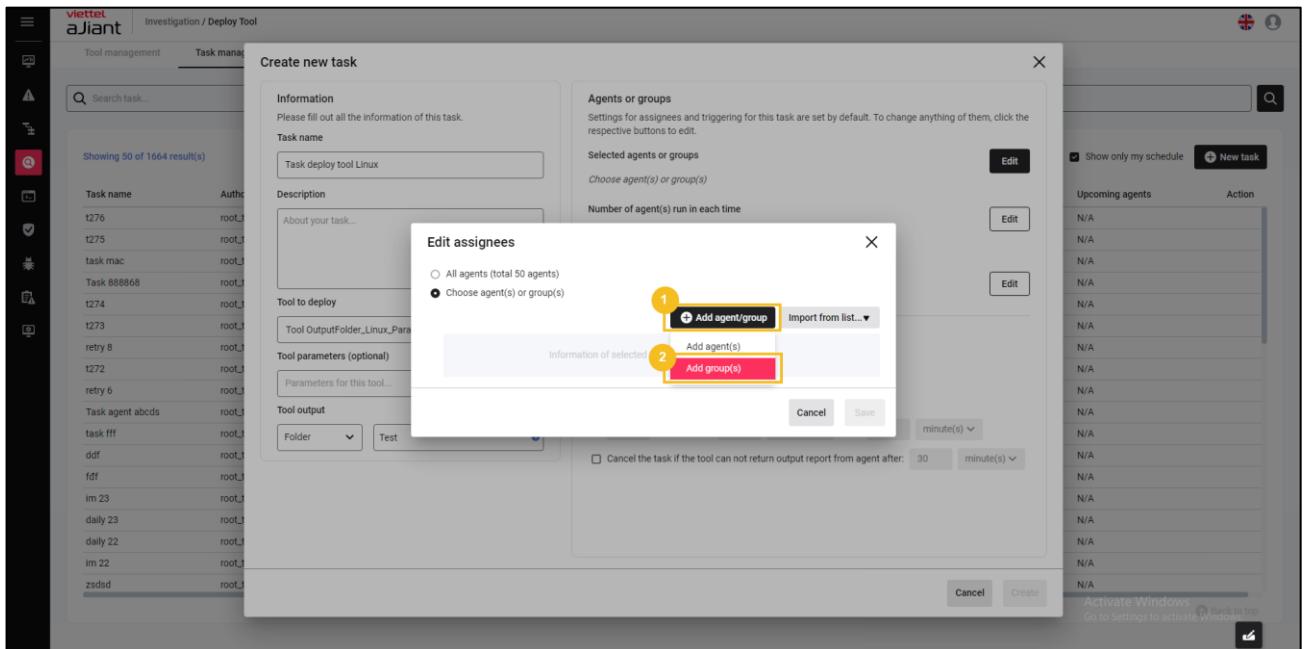
- Hover over the selected Agent(s) > Click the icon to remove the Agent(s) from the selected list.



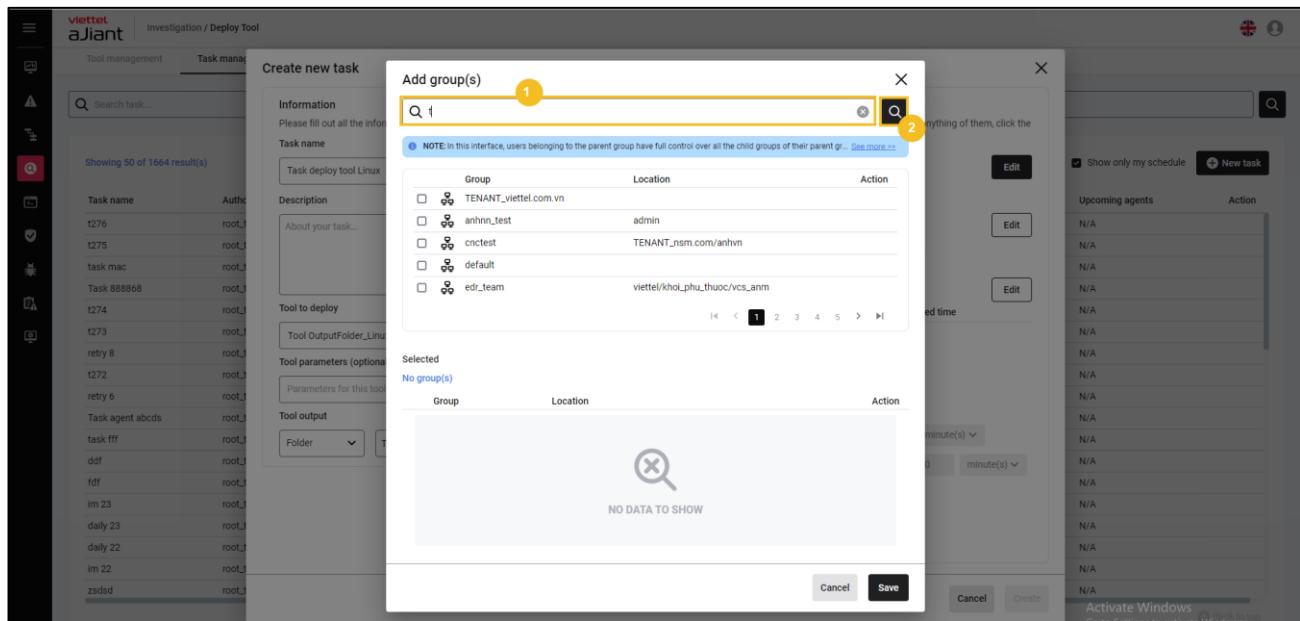
- Select Cancel to cancel or select Save to save the information of the selected Agent(s) for deployment:



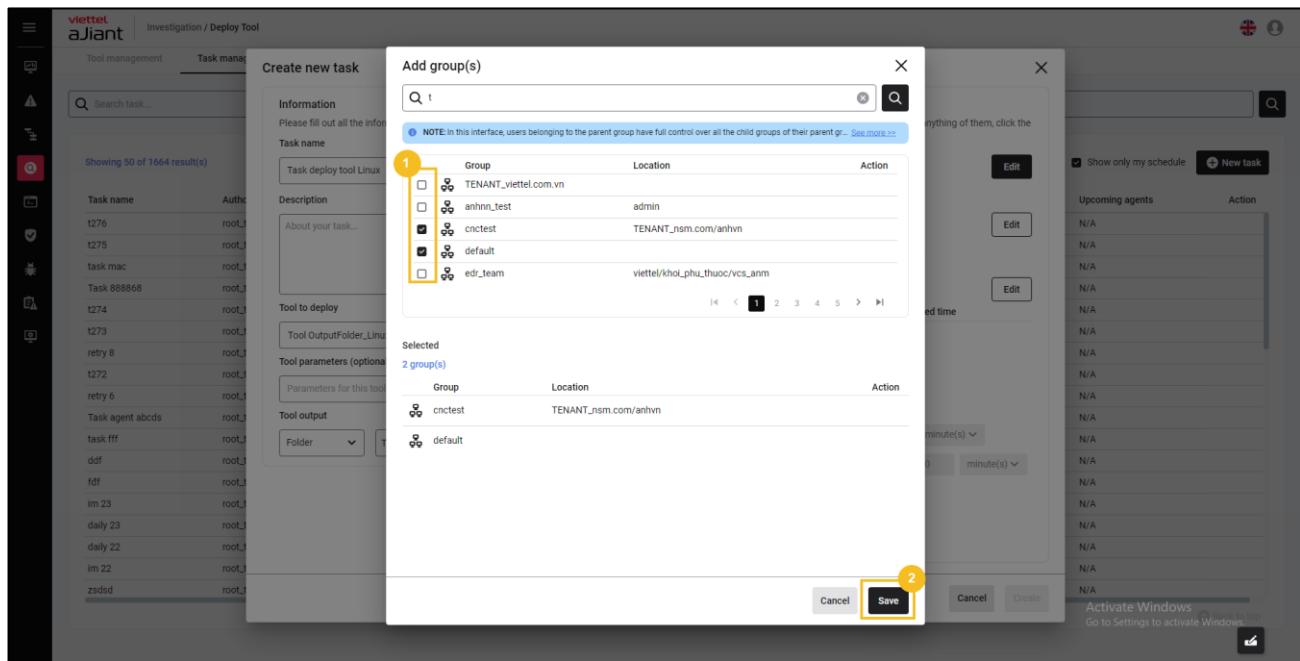
+ Select Add group(s):



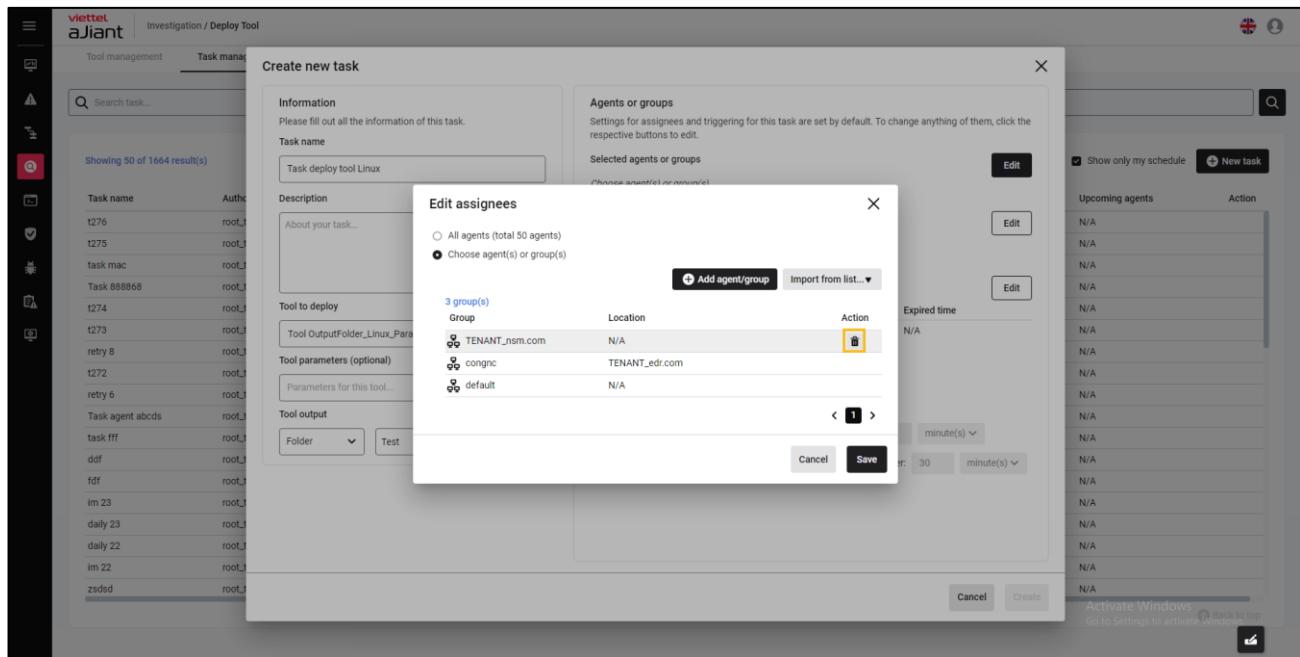
- Search for group(s) by name, allowing input of keywords to search for groups by group name:



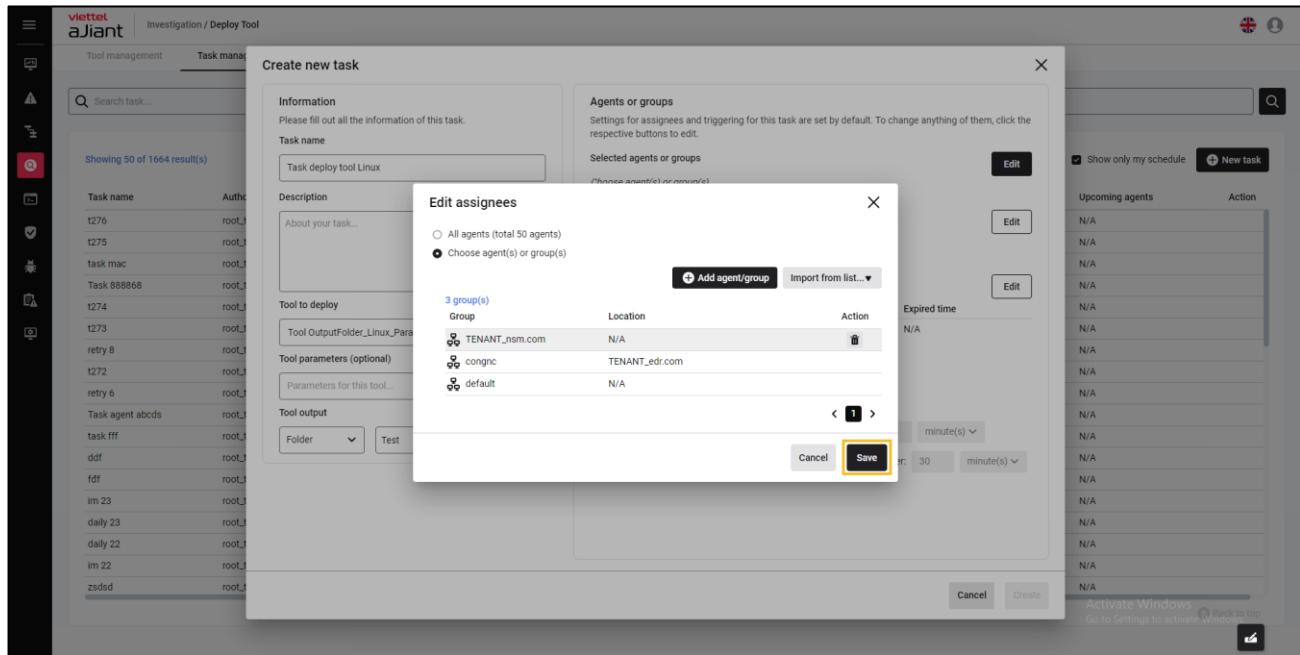
- Select group(s) to deploy by checking one or more groups > Information of the selected group(s) will be displayed in the Selected box > choose Cancel to cancel adding group(s) for deployment or select the Save button to confirm the list of group(s):



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



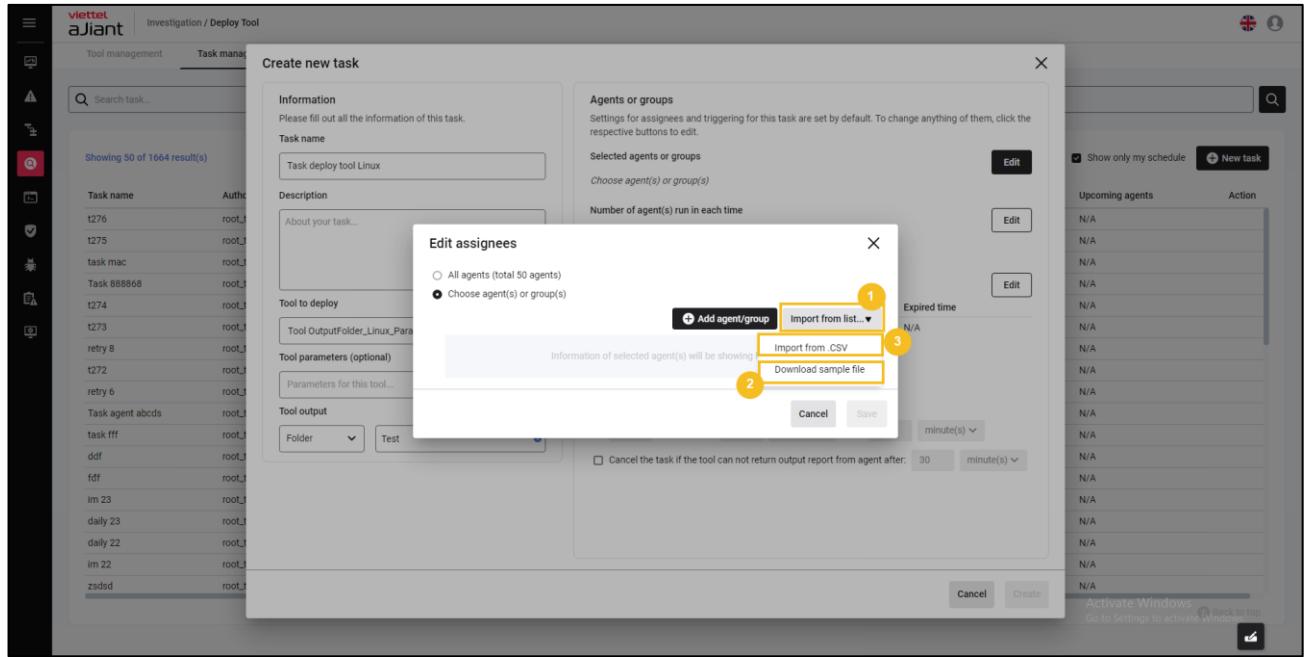
- Select Cancel to abort or select Save for the chosen group(s) to deploy:



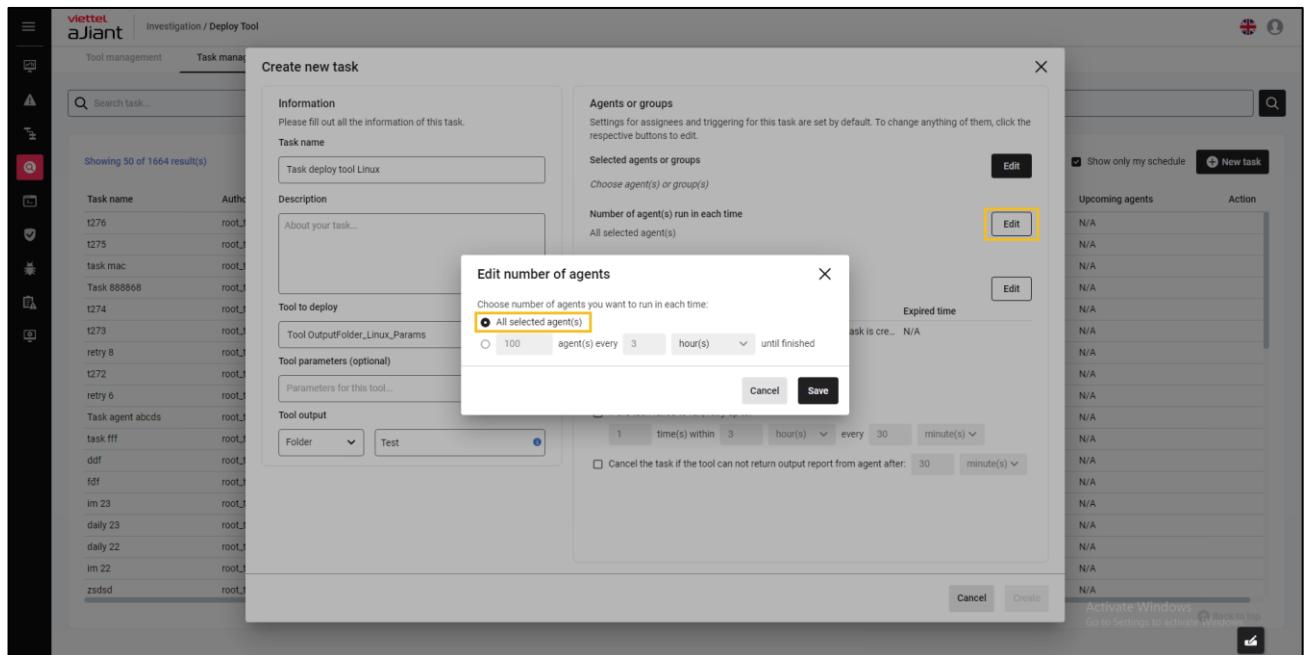
+ Import from list: Allows uploading a list of agents from a .csv file > Select Import from list

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

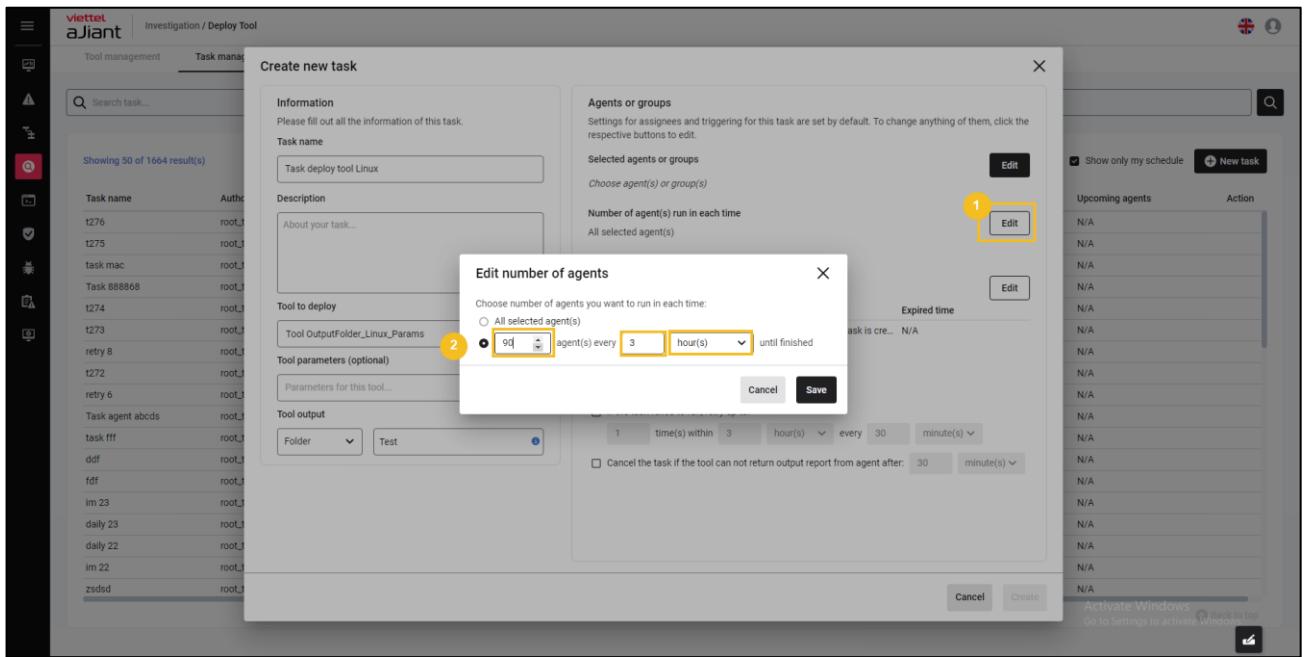
- Enter agent(s) information > select Import from .CSV to upload the list of agent(s).



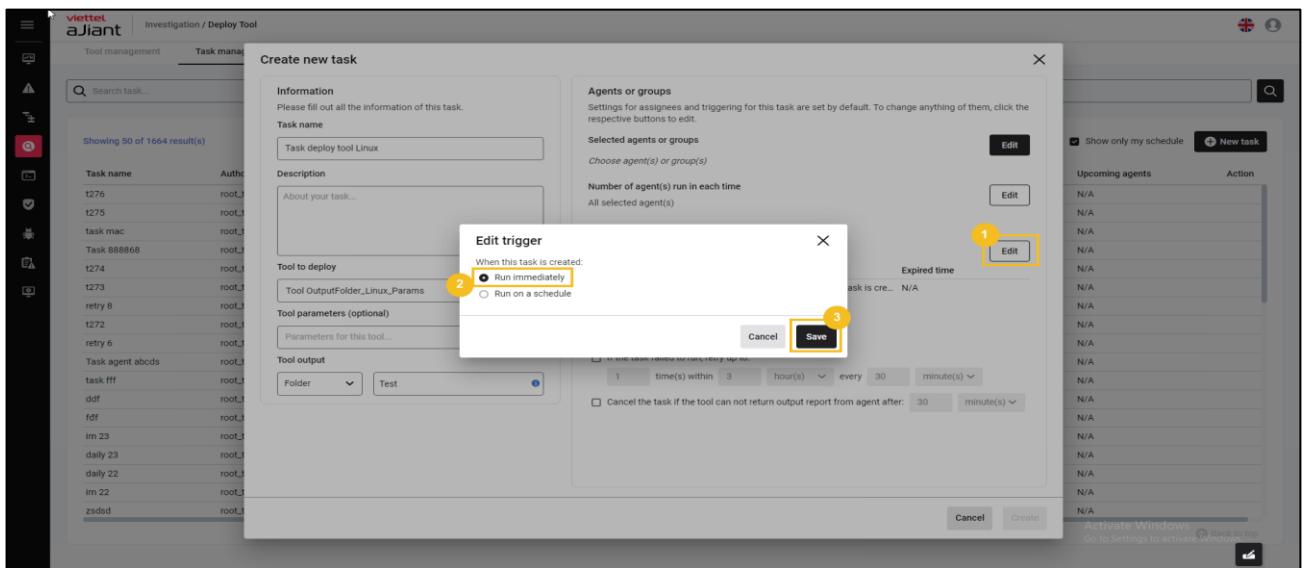
- Configuration of the number of agents deployed per tool each time:
 - + All Agent: Allows deployment of all selected user agent(s)



- + Configure the number of agents per deployment:

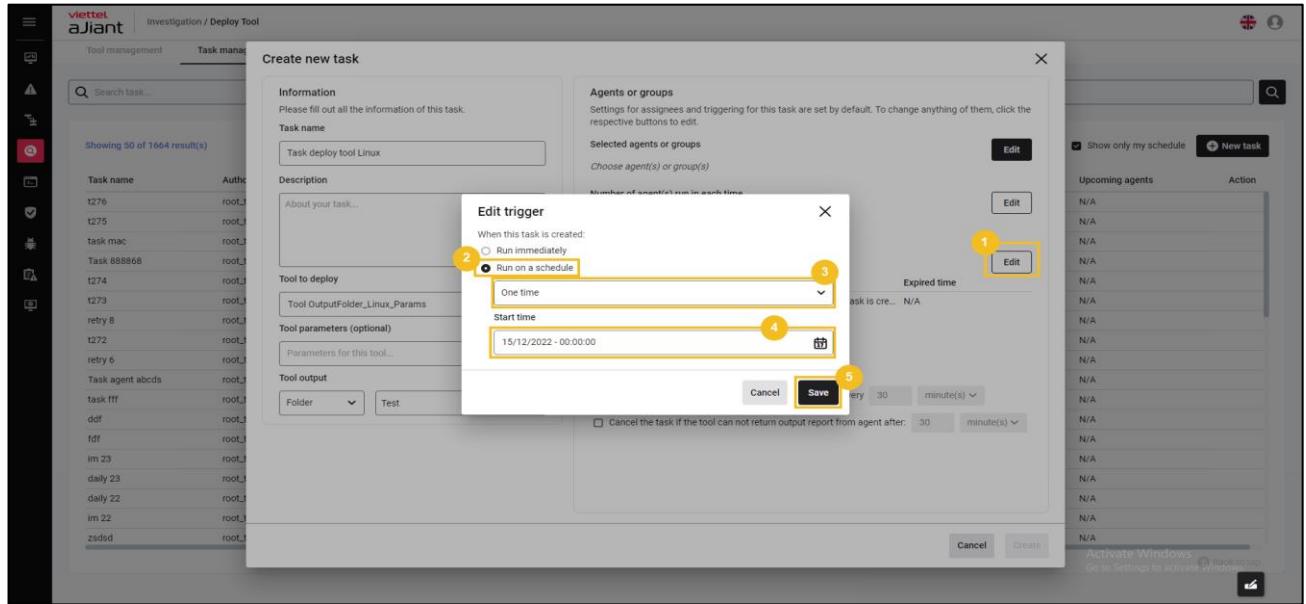


- Configuration of time information (scheduling) for executing the deploy tool:
 - + Select Run immediately to execute the deploy tool configuration right away (after successfully creating the task).

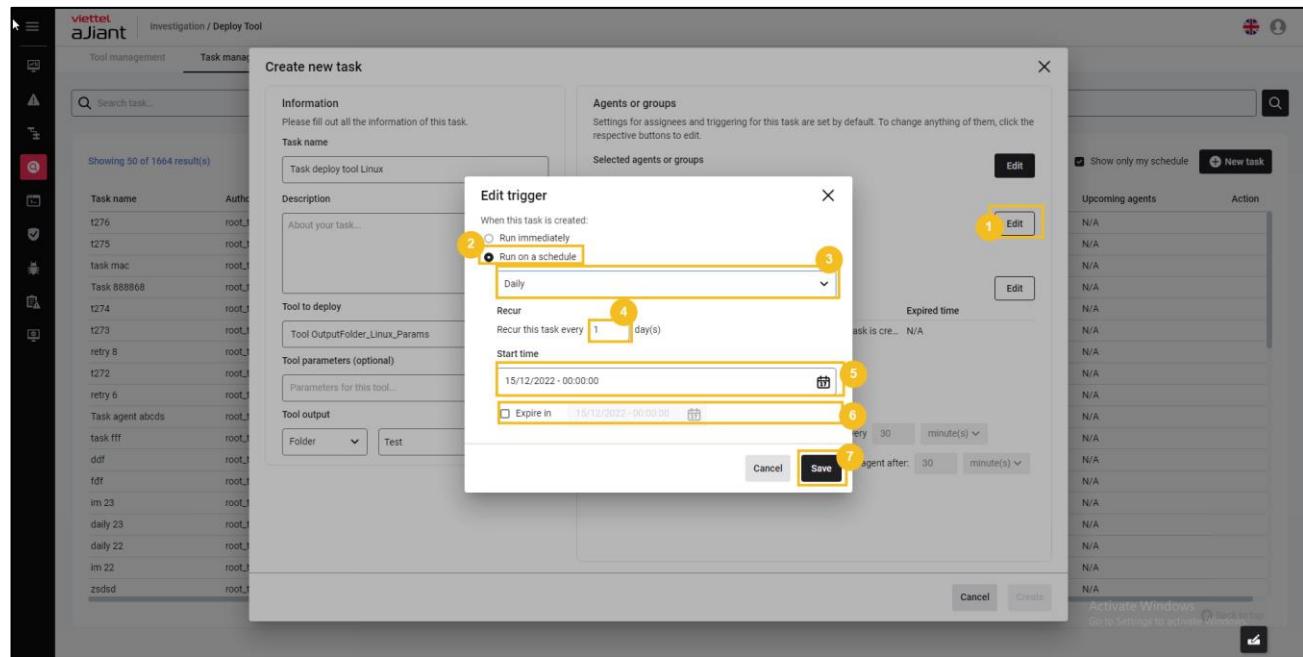


- + Select Run on schedule to configure the tool deployment timing according to the schedule:

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

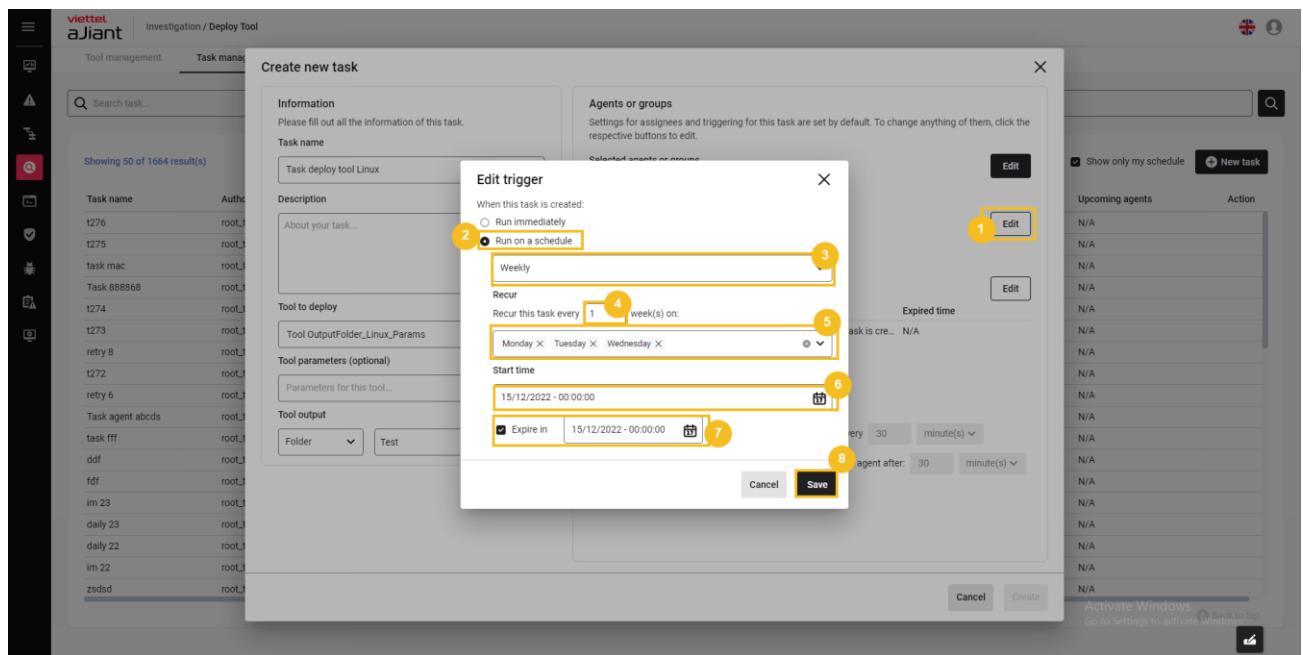


- Select Daily schedule:
 - Allow scheduling of daily tool deployment;
 - Repetition time;
 - Start and end time configuration:



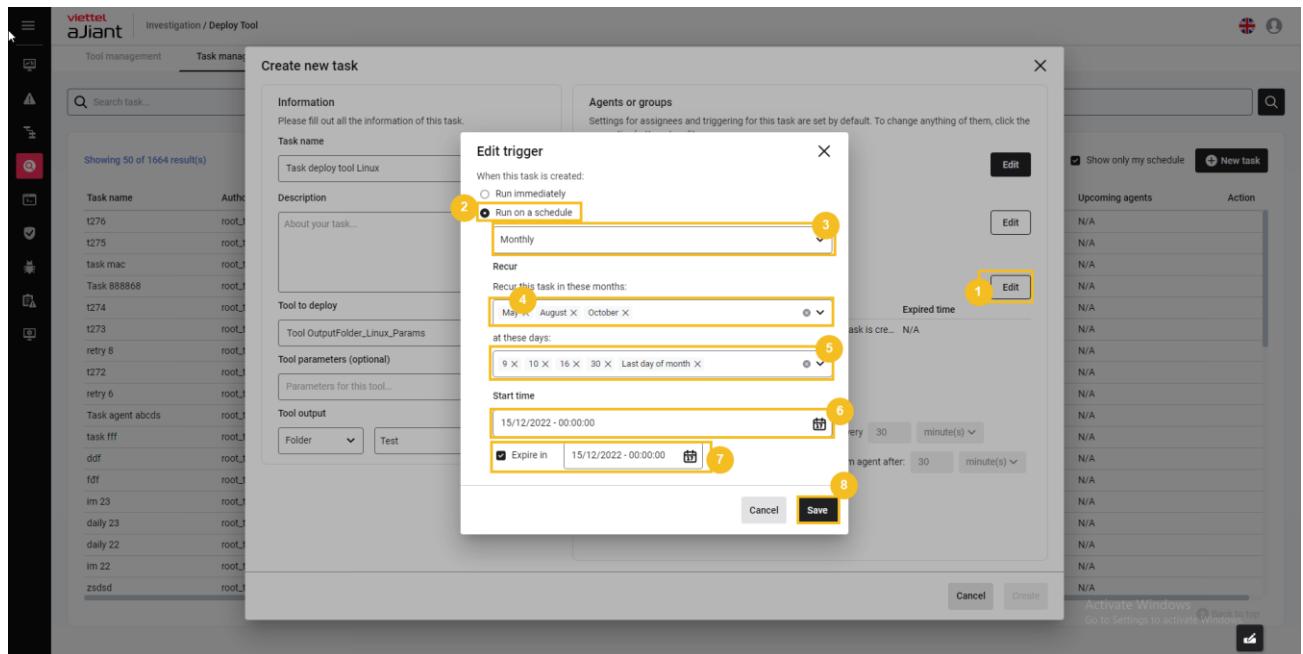
- Select Weekly schedule:

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



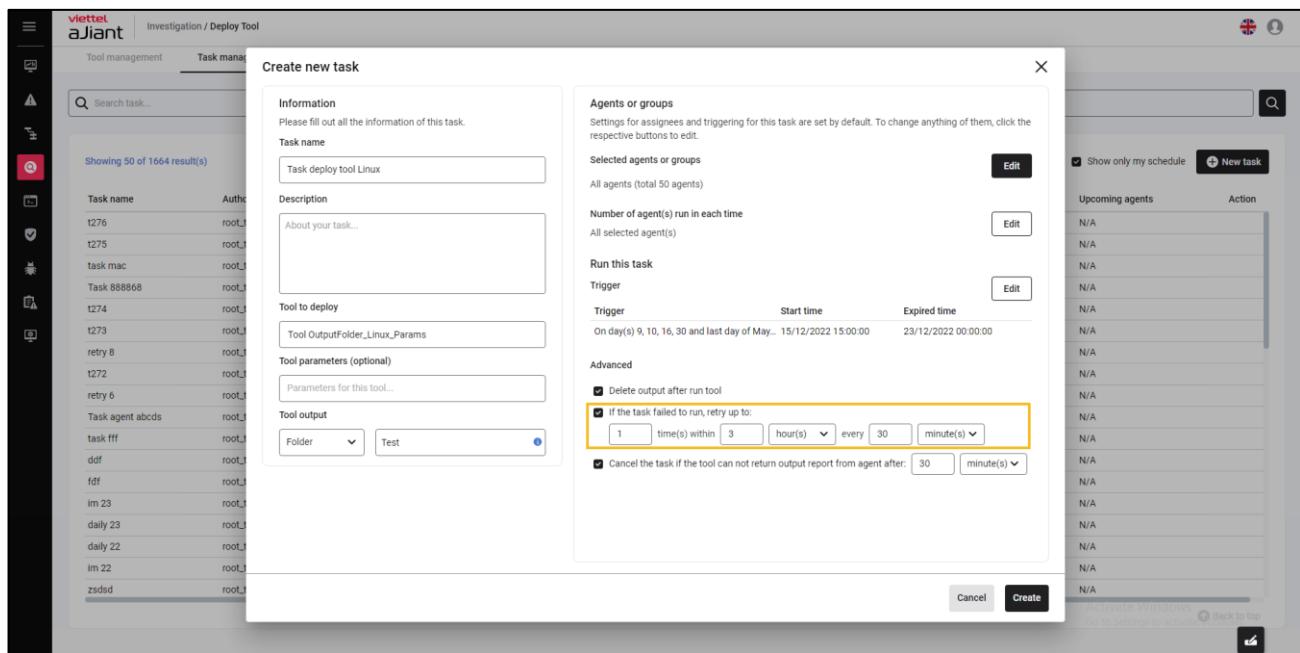
- Select Monthly schedule:

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

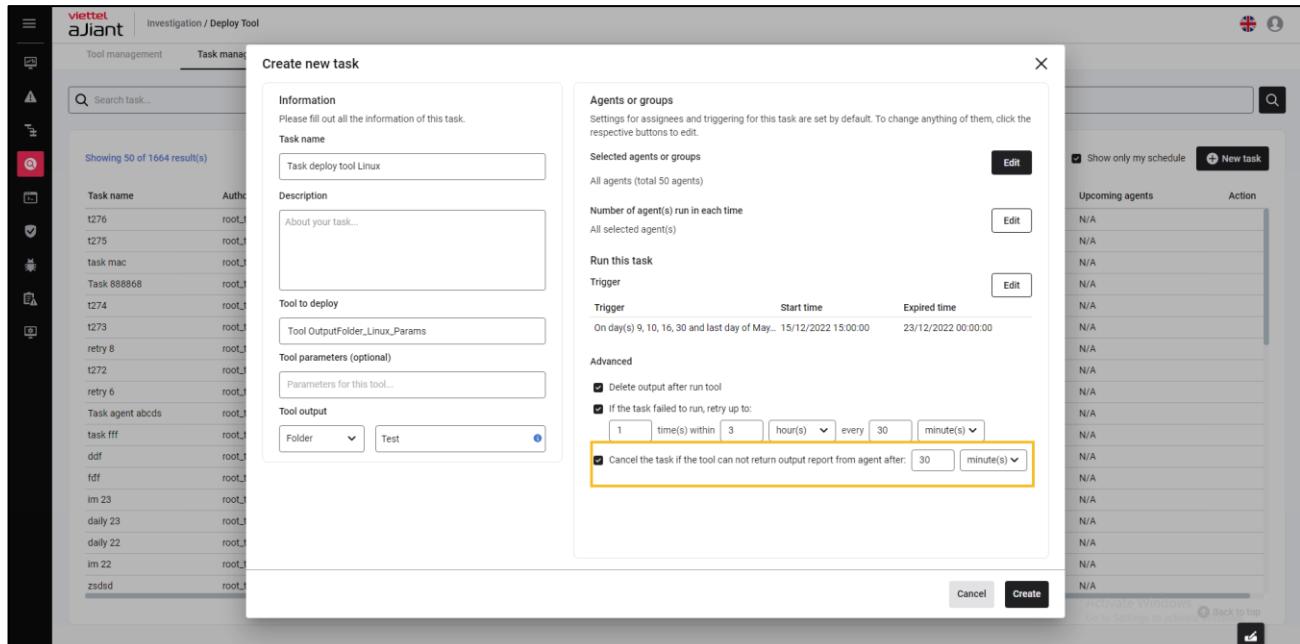


- Advanced information configuration for the task

- + 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

Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
t276	root_test	14/12/2022 18:39:11	N/A	1	Immediately	N/A	● Finished	N/A	
t275	root_test	14/12/2022 18:36:21	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	
t274	root_test	14/12/2022 17:47:06	N/A	1	Immediately	N/A	● Finished	N/A	
t273	root_test	14/12/2022 17:42:13	N/A	1	Immediately	N/A	● Finished	N/A	
retry 8	root_test	14/12/2022 17:13:17	N/A	1	Immediately	N/A	● Stopped	N/A	
t272	root_test	14/12/2022 17:11:03	N/A	1	Immediately	N/A	● Finished	N/A	
retry 6	root_test	14/12/2022 17:00:09	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	
ddf	root_test	14/12/2022 15:55:04	N/A	1	Immediately	N/A	● Finished	N/A	
fdf	root_test	14/12/2022 15:51:54	N/A	1	Immediately	N/A	● Finished	N/A	
im 23	root_test	14/12/2022 15:21:05	N/A	5	Immediately	N/A	● Finished	N/A	
daily 23	root_test	14/12/2022 14:52:23	N/A	5	At 14/12/2022 - 15:00:00	N/A	● Finished	N/A	
daily 22	root_test	14/12/2022 14:48:31	N/A	5	At 14/12/2022 - 14:55:00	N/A	● Finished	N/A	
im 22	root_test	14/12/2022 14:47:24	N/A	5	Immediately	N/A	● Finished	N/A	
zsdsd	root_test	14/12/2022 14:06:55	N/A	5	Immediately	N/A	● Finished	N/A	

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.

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 88886	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 retr 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	

c. Create a task

(Function similar to section 3.5.4.2. Deploy tool)

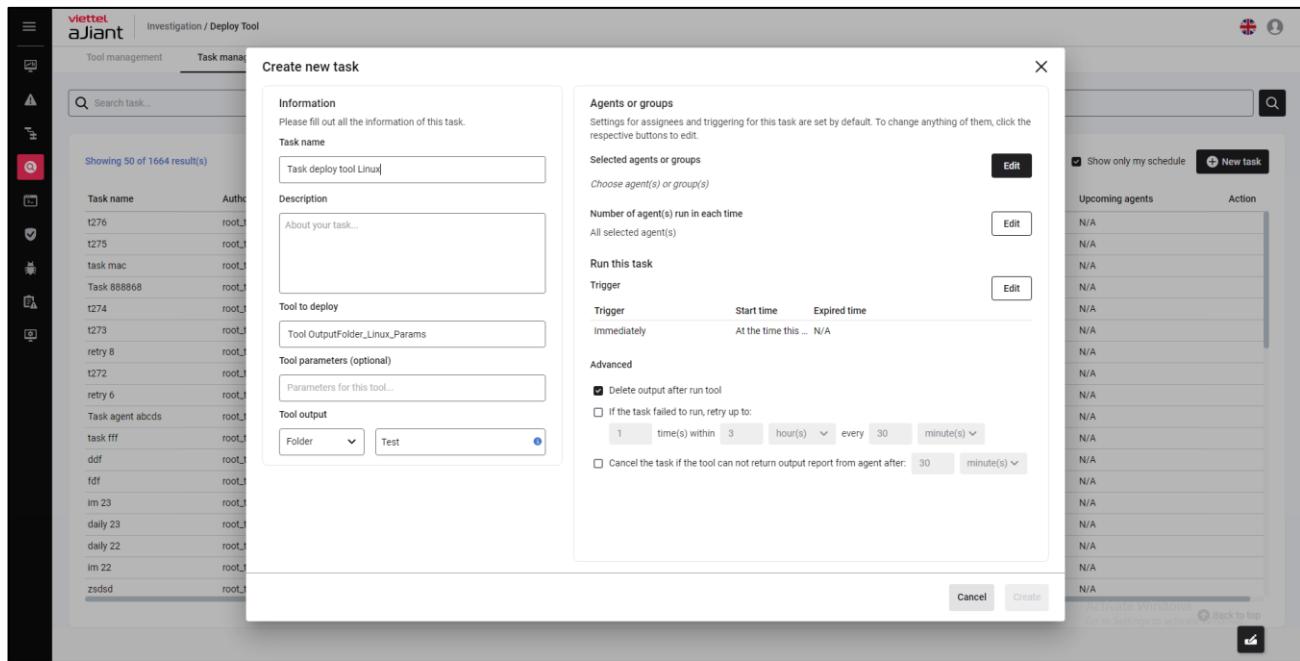
Purpose: Configure deploy tool information under the agent

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:

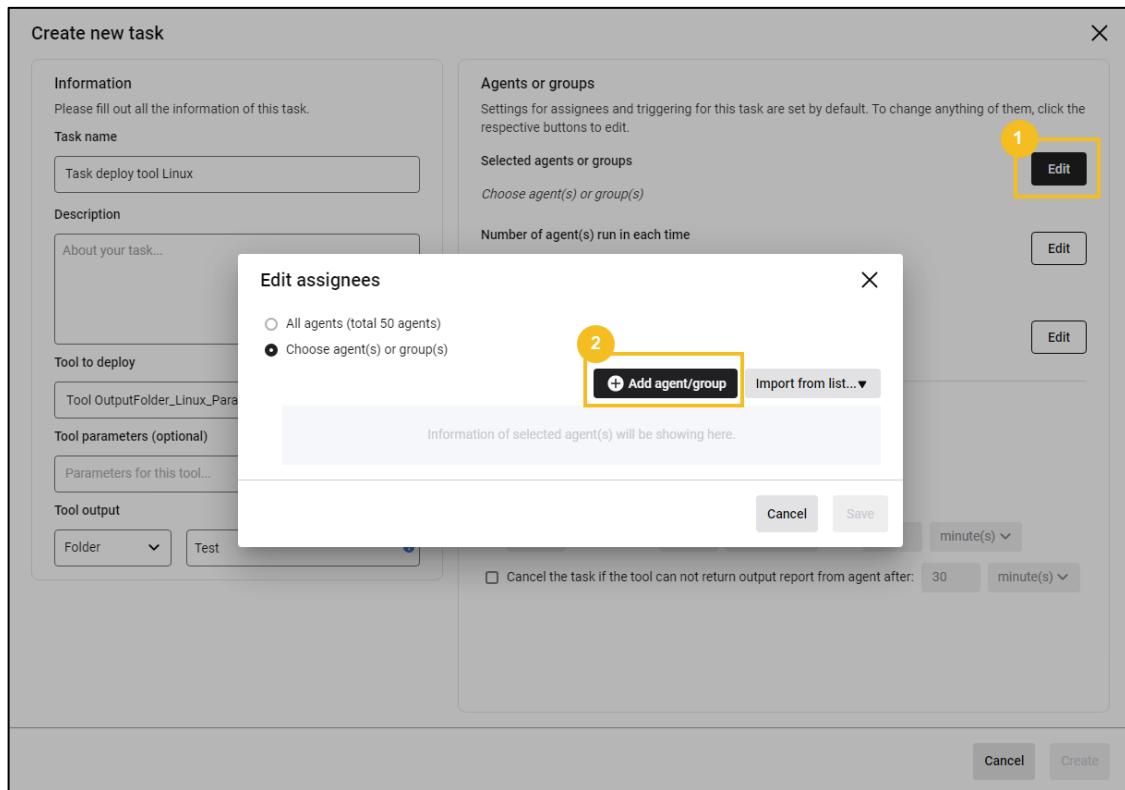
- After selecting the tool, click the icon on the tool record you want to deploy > select Deploy this tool, the Create new task screen will appear:



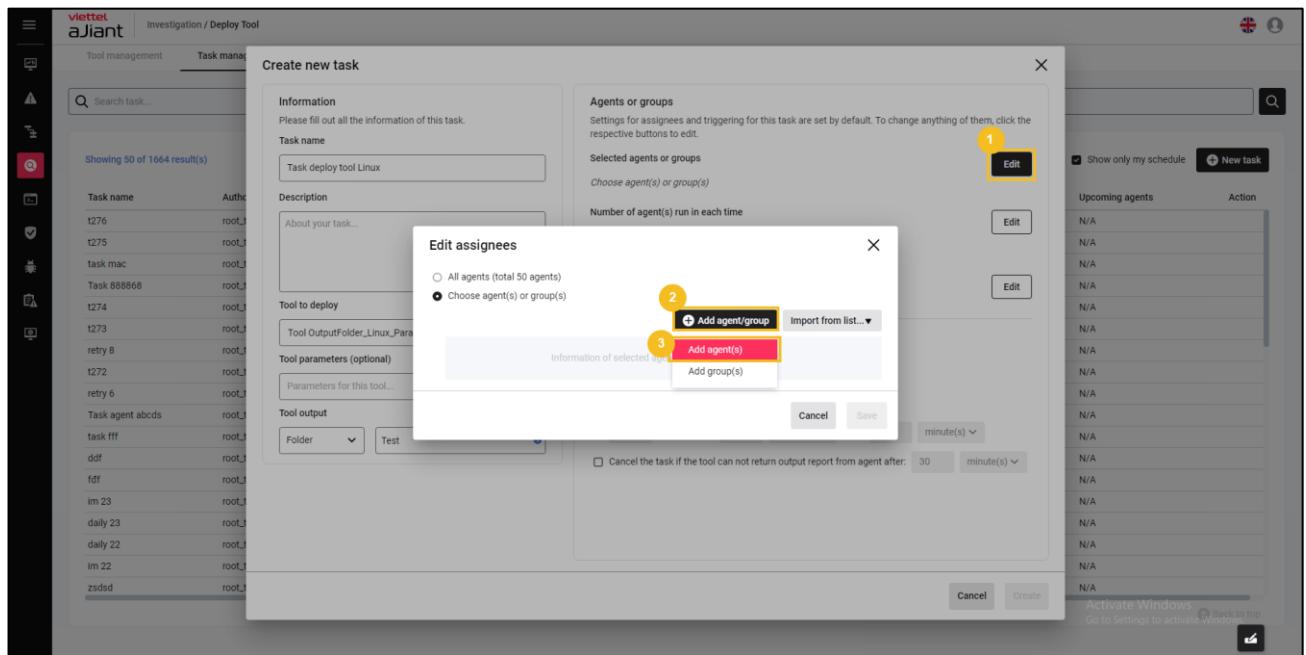
- Enter the task information for deploying the tool: Task name, Tool to deploy, Description, Tool parameters, Tool output;
- Select the group and workstation (agent) information for deployment:

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

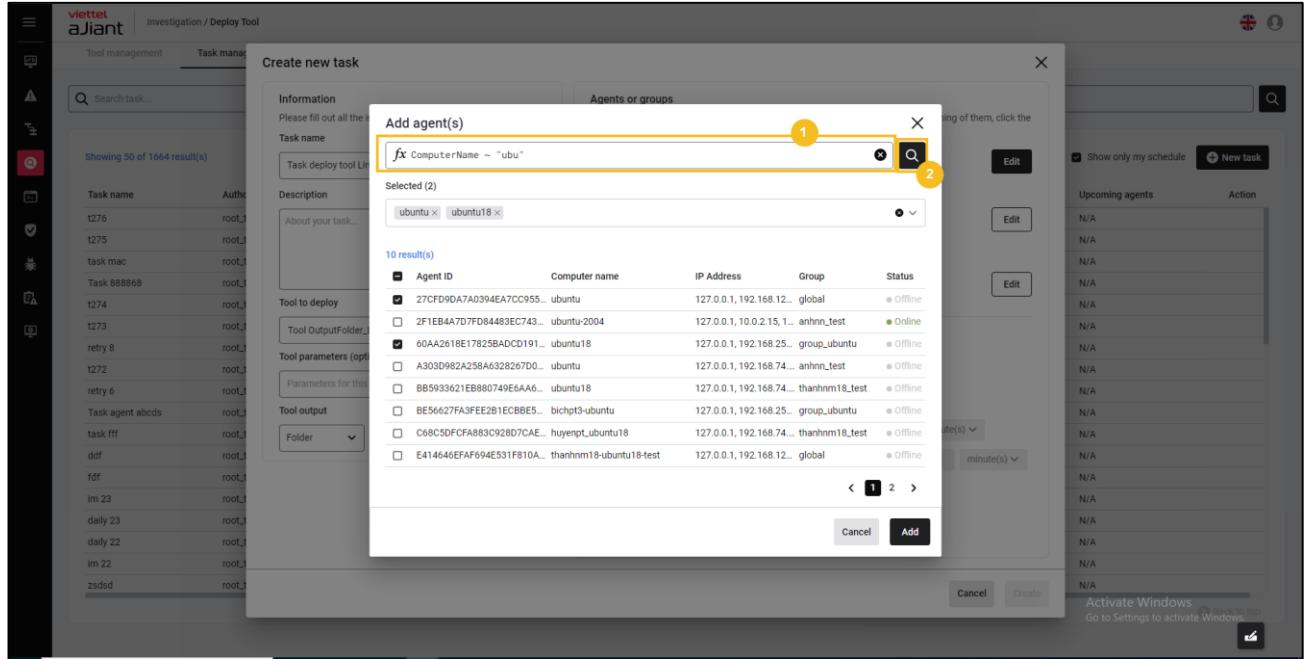
Select agents or groups to perform deployment – Choose agent(s) or group(s):



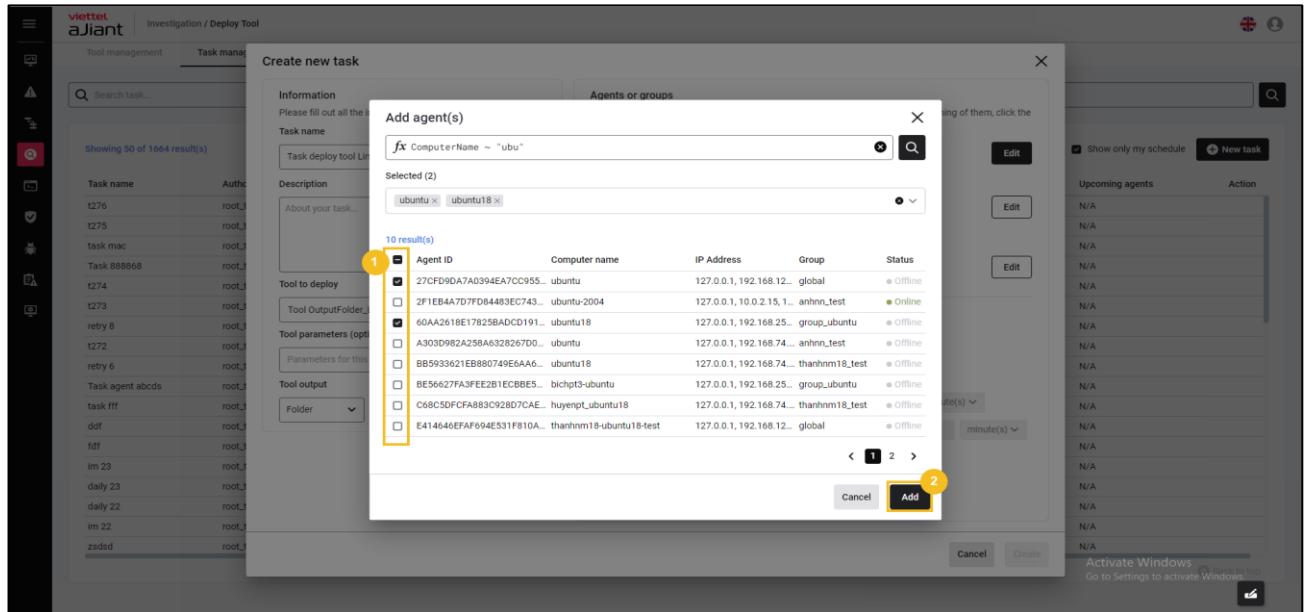
+ Select Add agent(s):



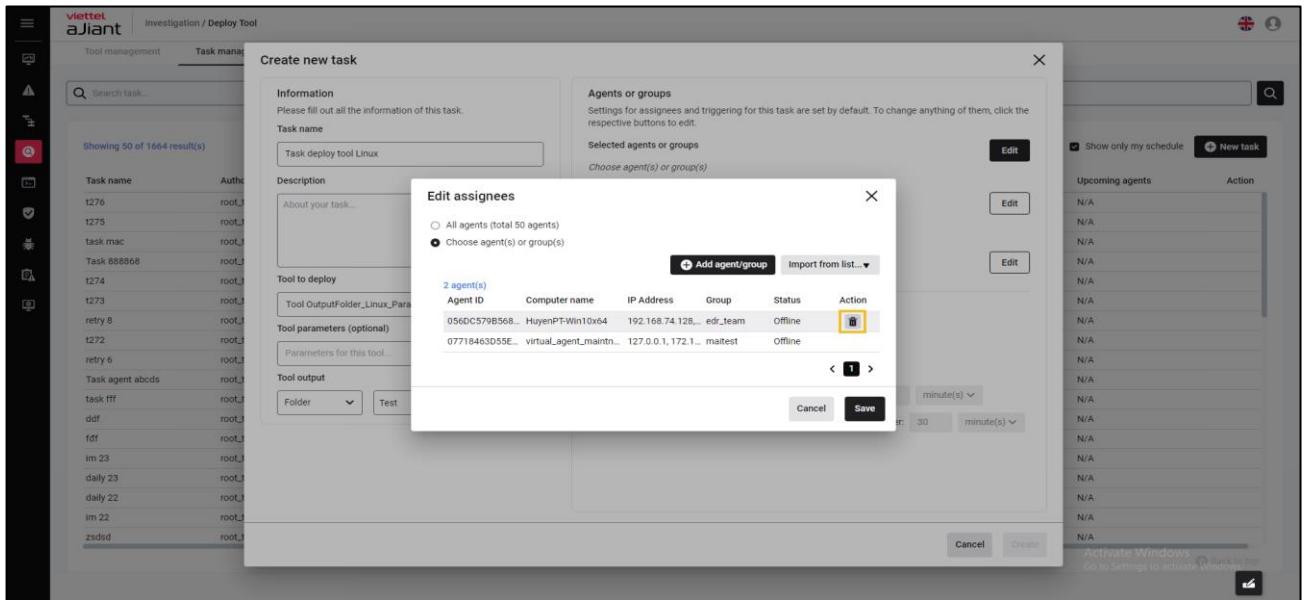
- **Search Agent:** Allows creating query statements and using query statements to search for Agents.



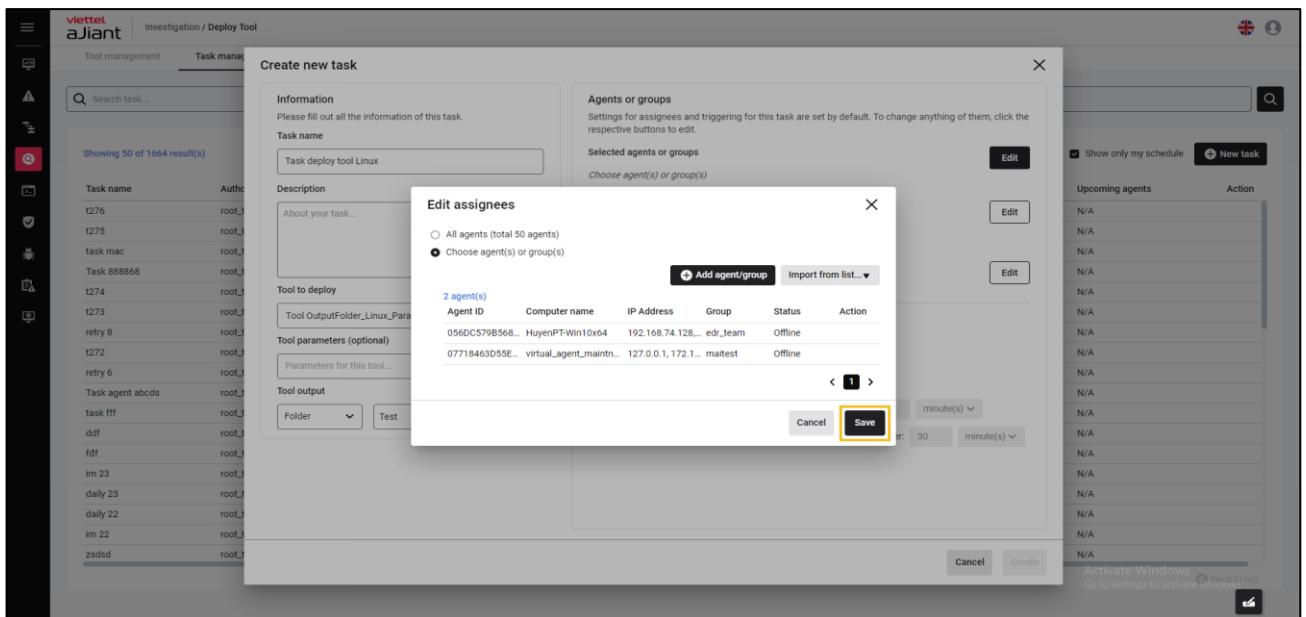
- Select the Agent(s) to deploy by checking one or more Agents > Information of the selected Agent(s) will be displayed in the Selected box > choose Cancel to cancel adding Agents for deployment or click the Add button to confirm the list of Agent(s):



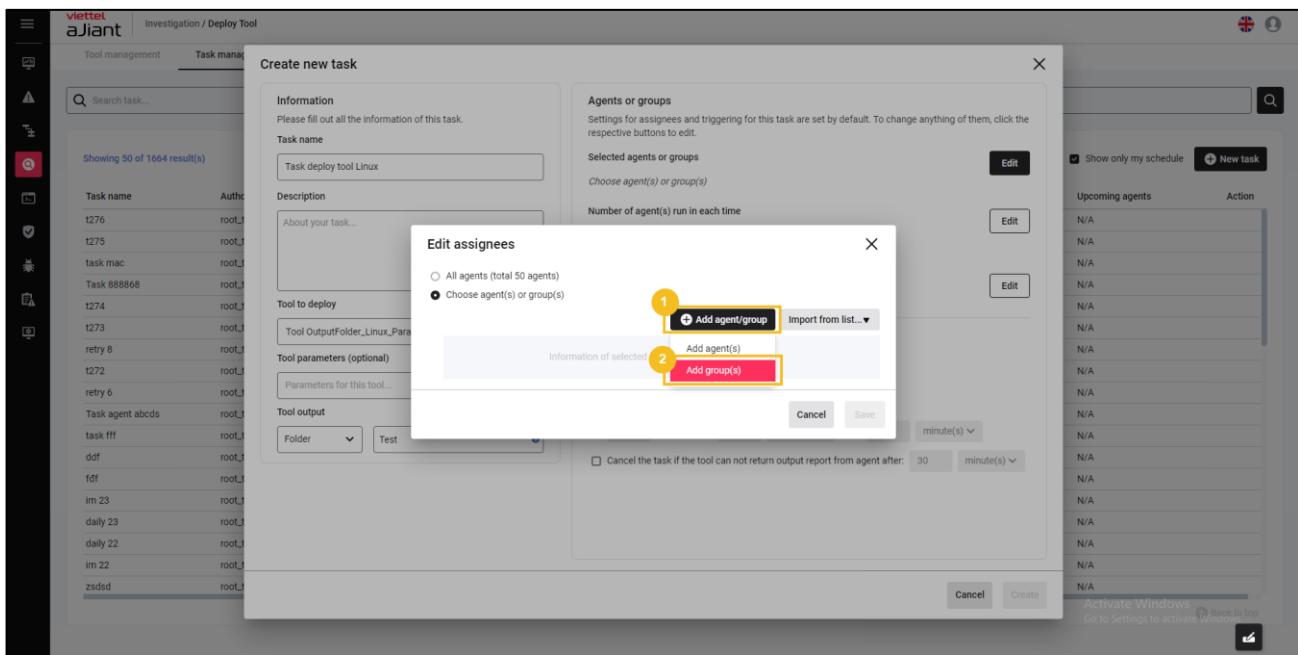
- Hover over the selected Agent(s) > Click the icon to remove the Agent(s) from the selected list:



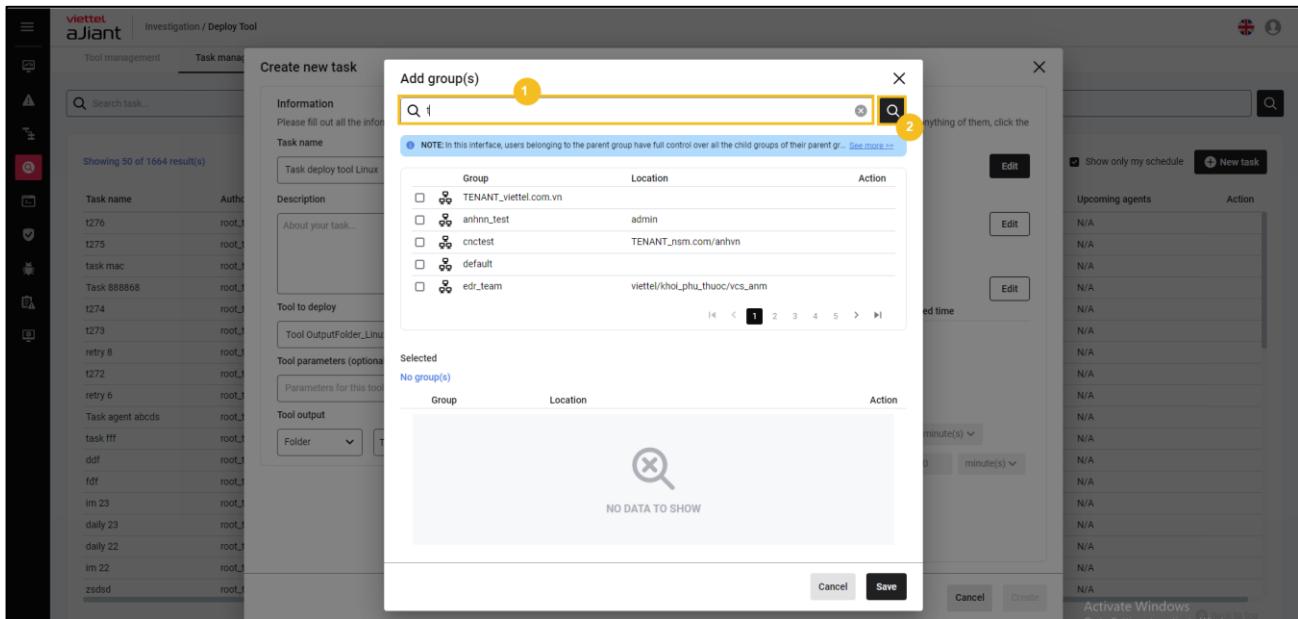
- Select Cancel to cancel or select Save to save the information of the selected Agent(s) for deployment:



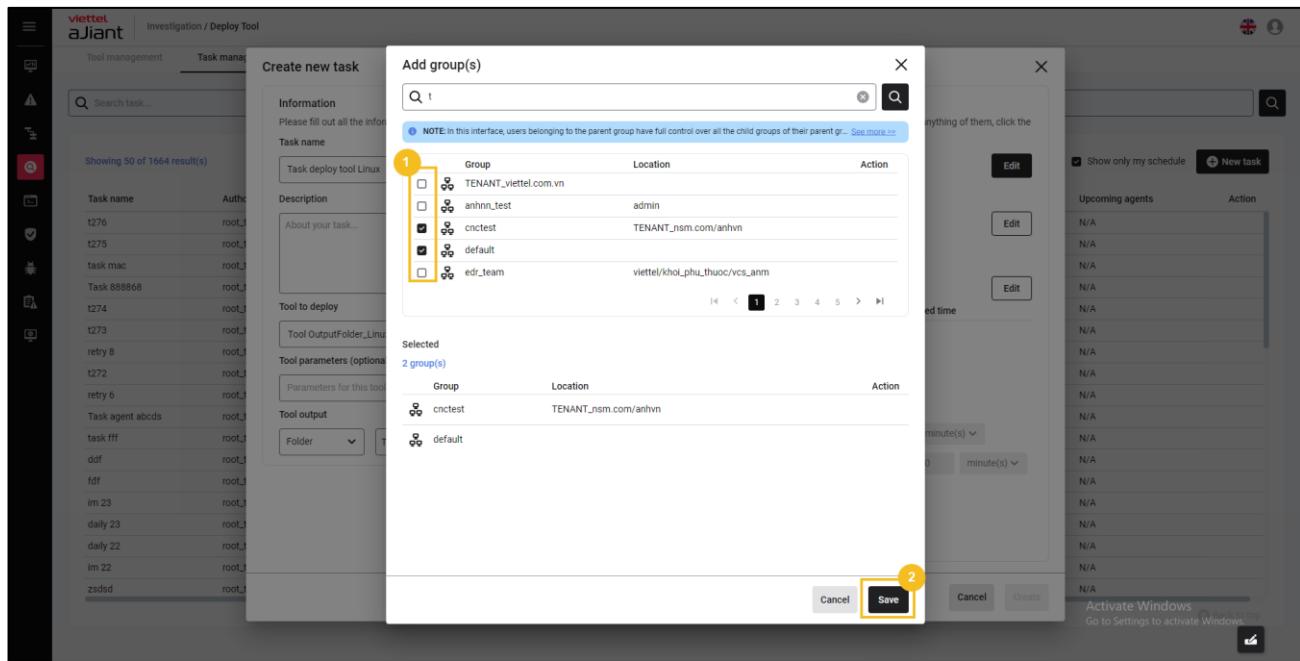
+ Select Add group(s):



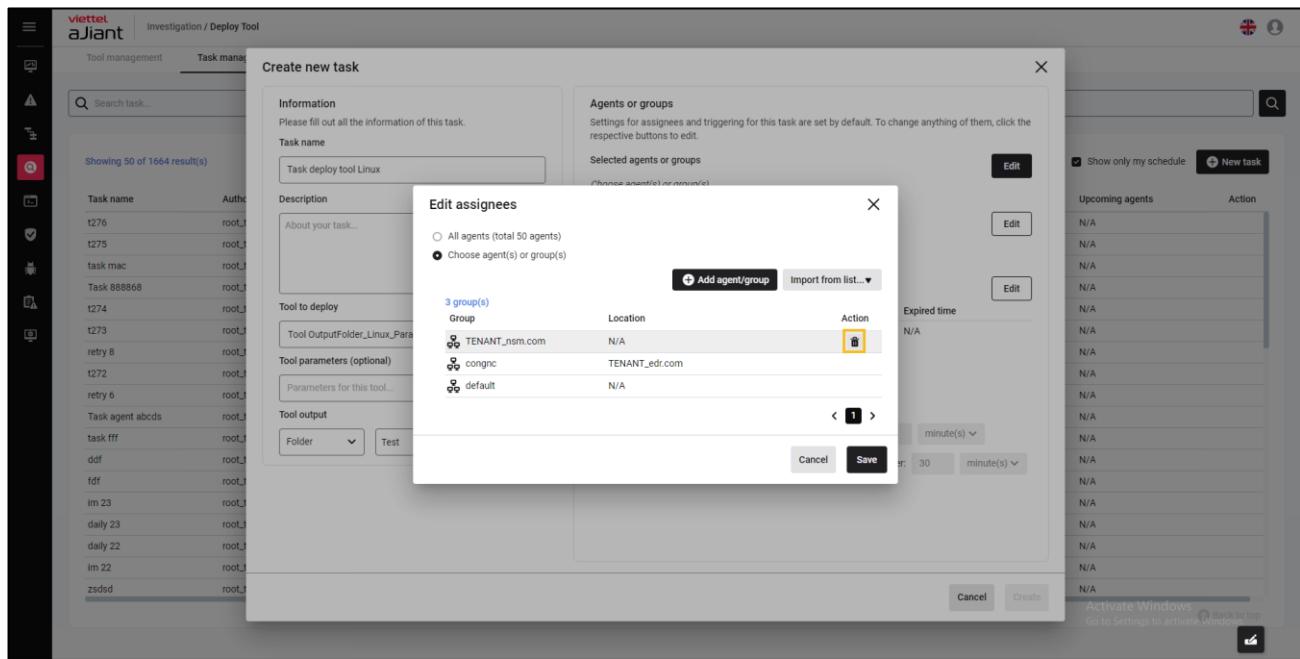
- Search for group(s) by name, allowing input of keywords to search for groups by group name:



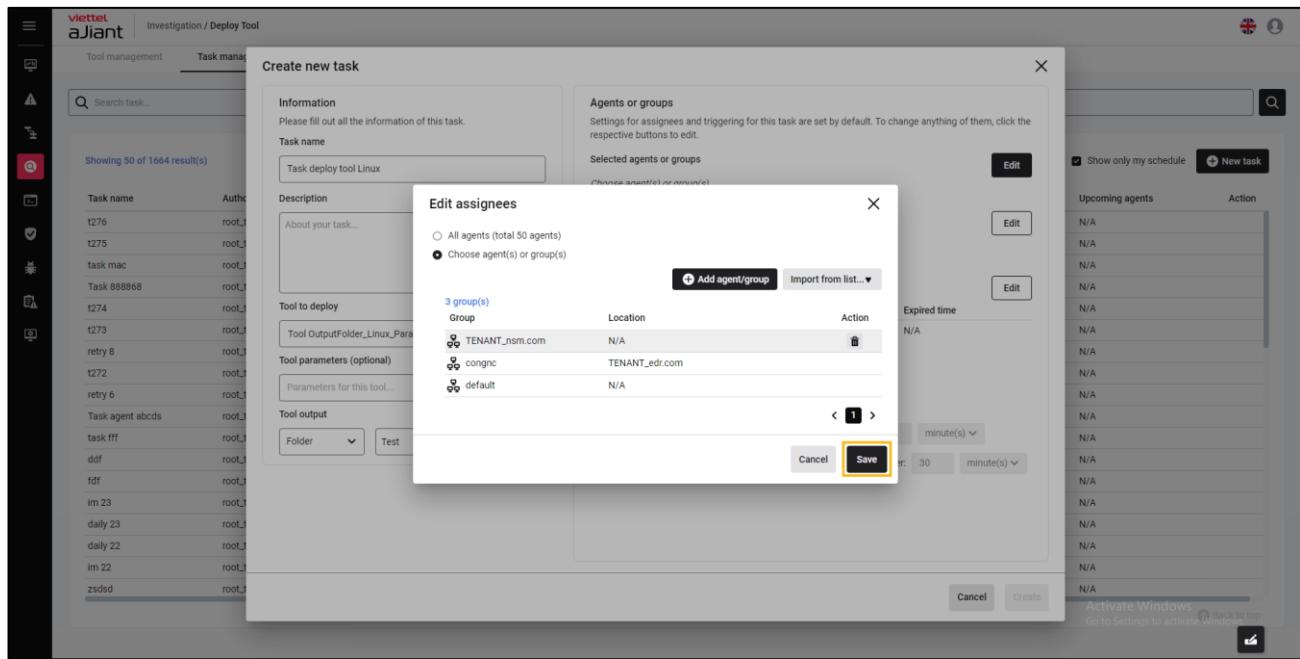
- Select the group(s) to deploy by checking one or more groups > Information of the selected group(s) will be displayed in the Selected box > choose Cancel to cancel adding group(s) for deployment or click the Save button to confirm the list of group(s):



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

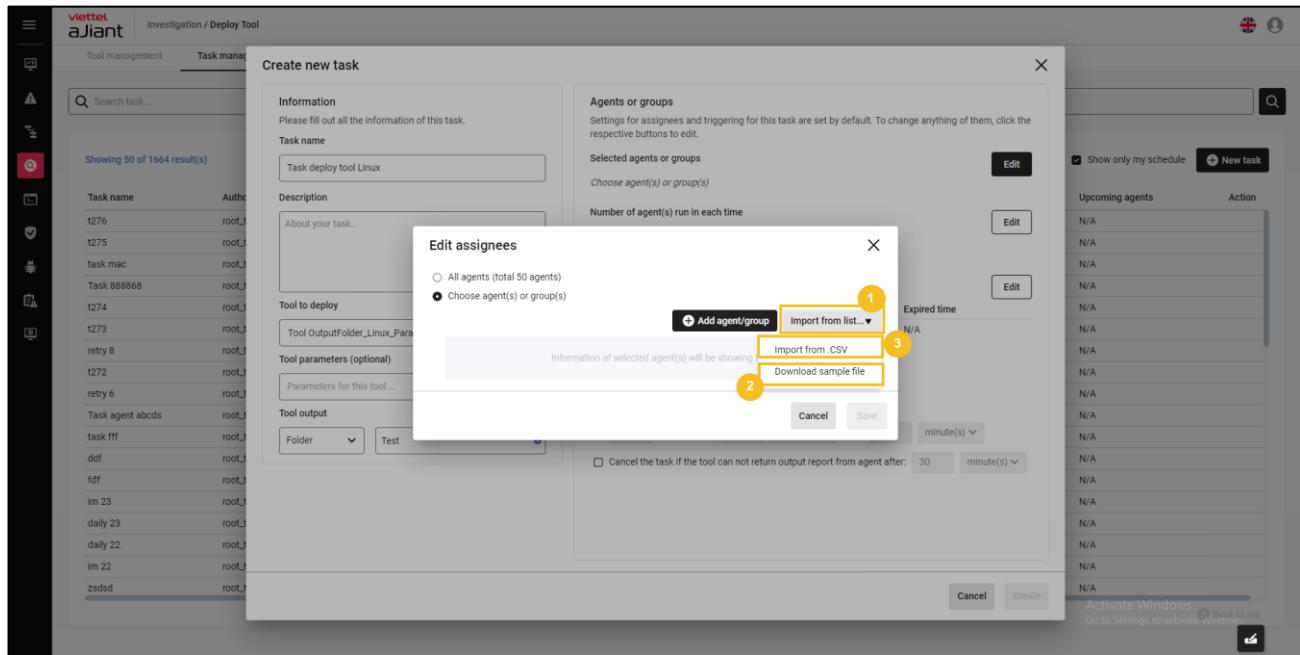


- Select Cancel to cancel or select Save to deploy the selected group(s):

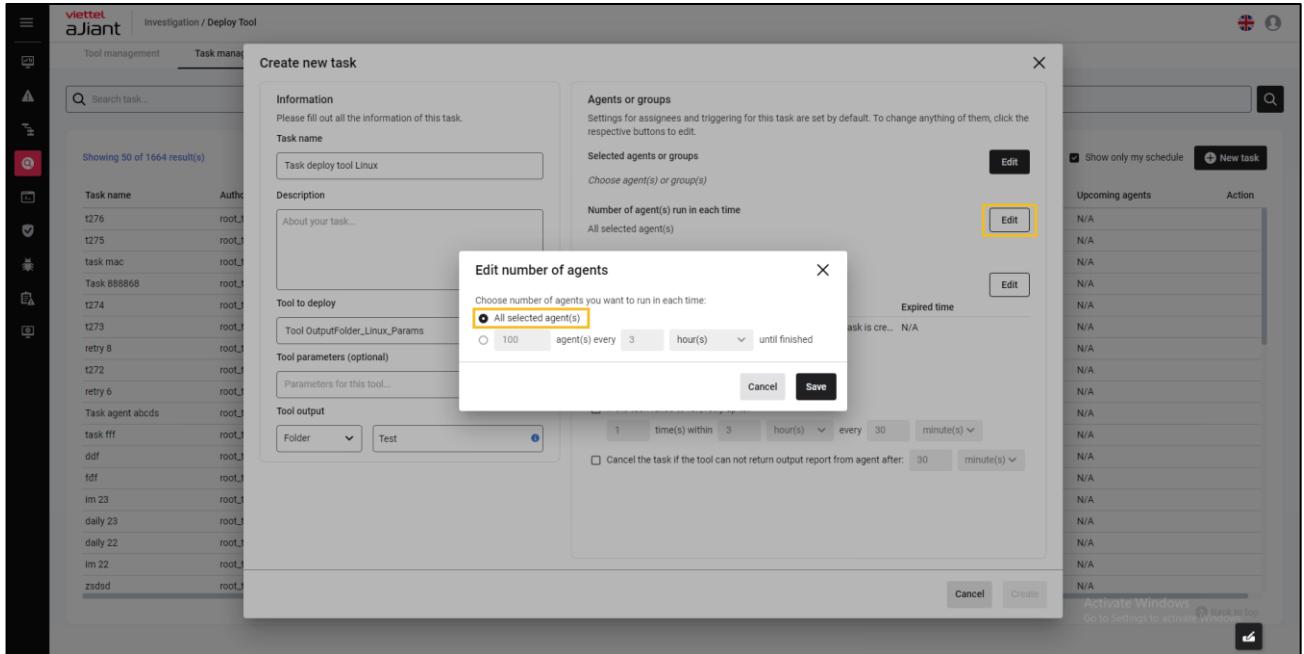


+ Import from list: Allows uploading a list of agents from a .csv file > Select Import from list

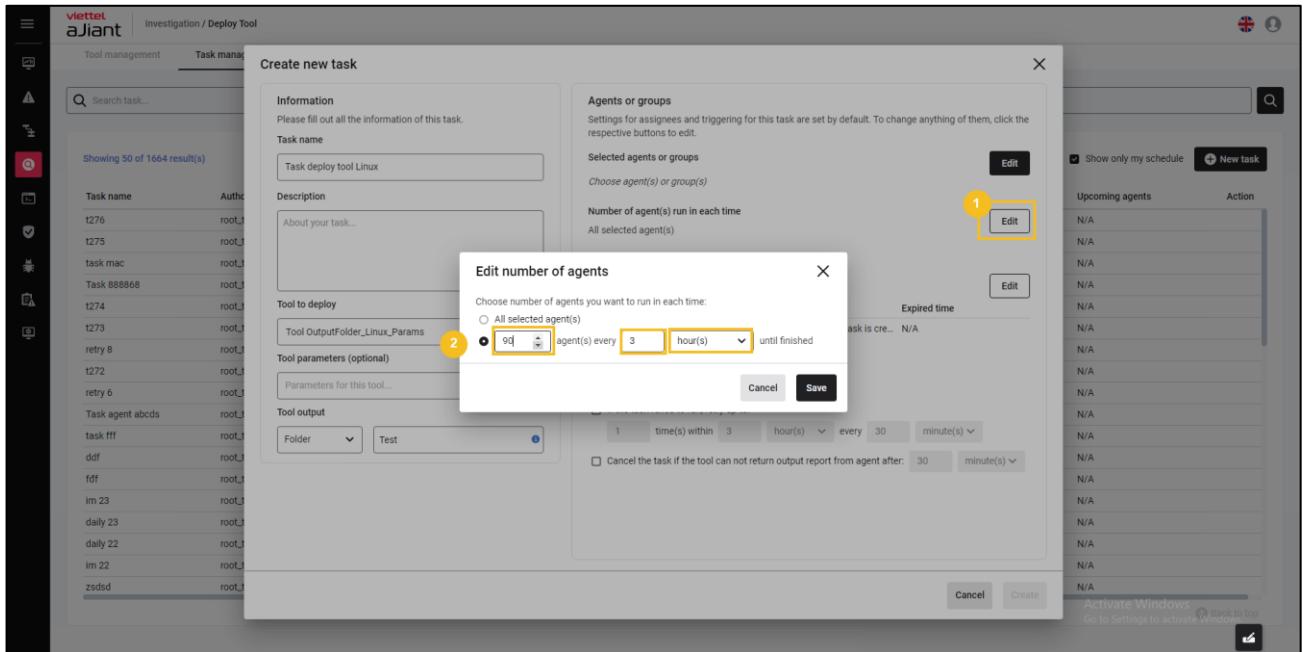
- Select Download sample file to obtain the sample agent(s) file list form;
- Enter agent(s) information > select Import from .CSV to upload the list of agent(s).



- Configuration of the number of agents deployed per tool each time:
 - + All Agent: Allows deployment of all selected user agent(s)

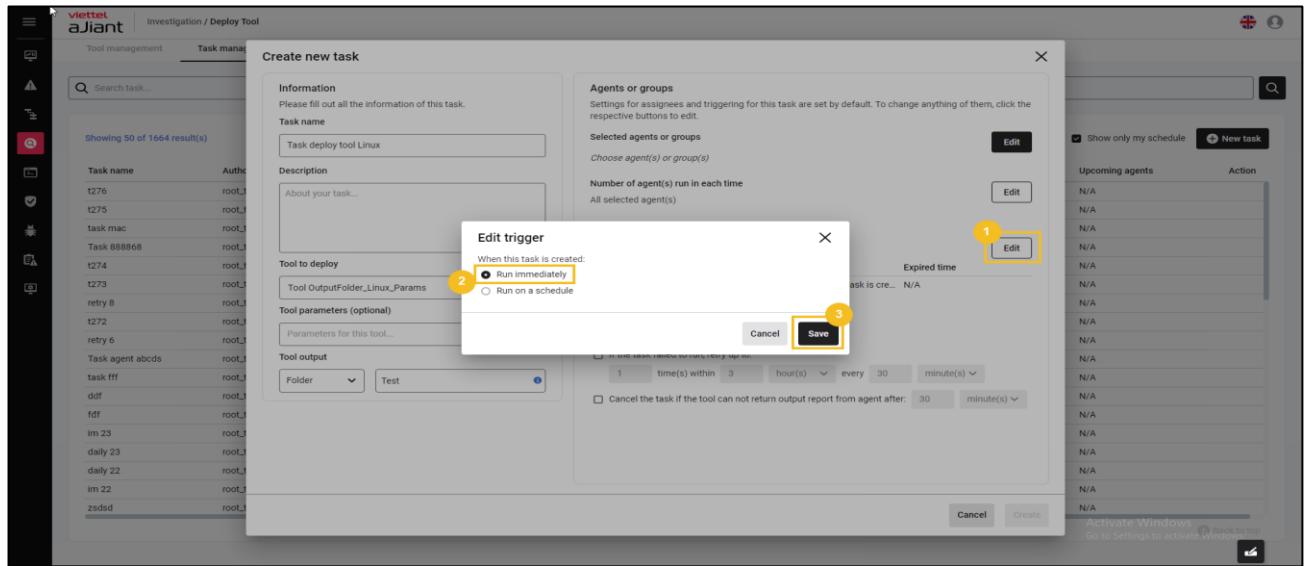


- + Configuration of the number of agents per deployment:



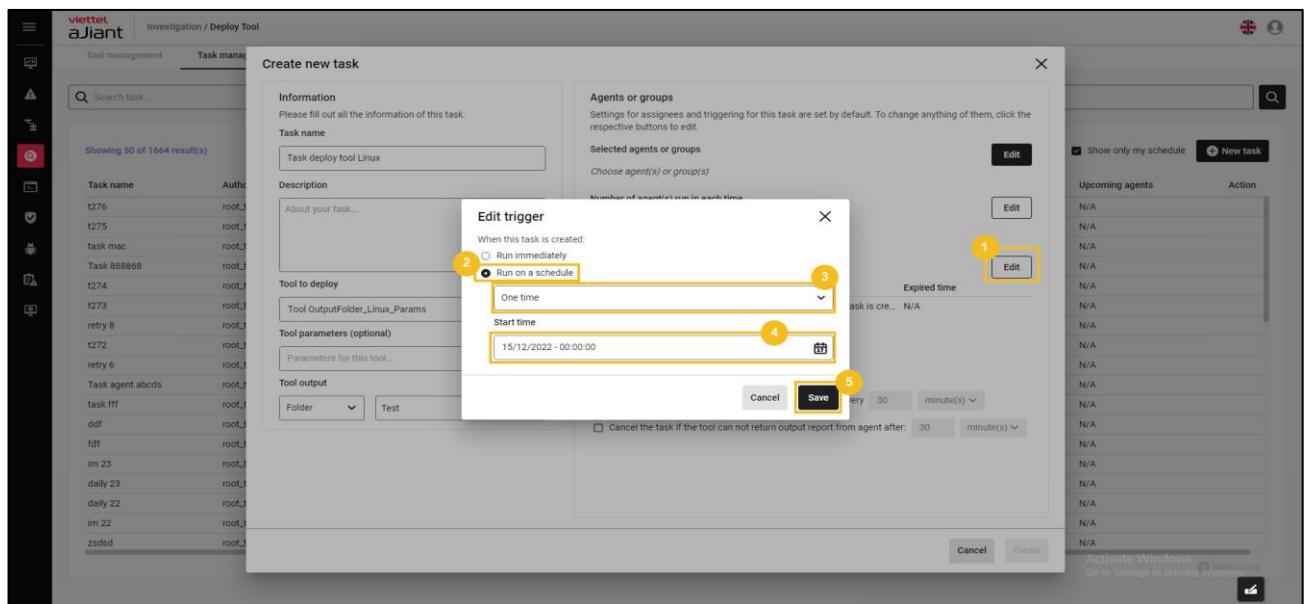
- Configuration of time information (scheduling) for executing the deploy tool:

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



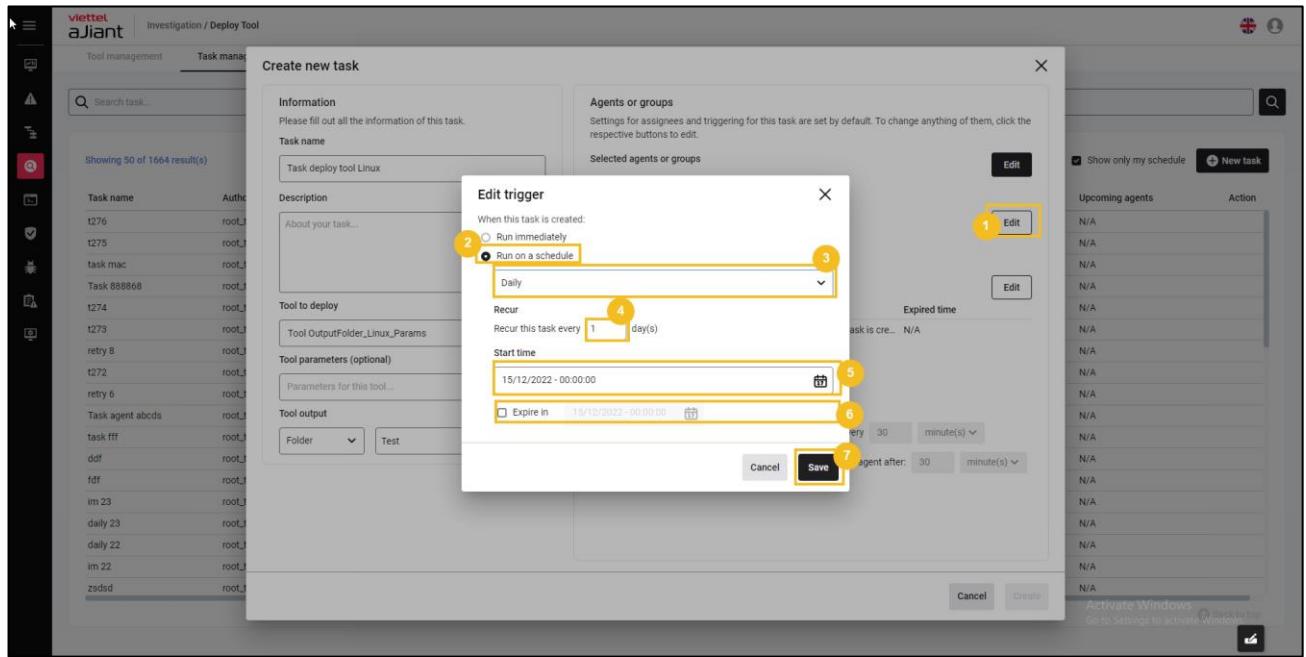
+ Select Run on schedule to configure the tool deployment timing according to the schedule:

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



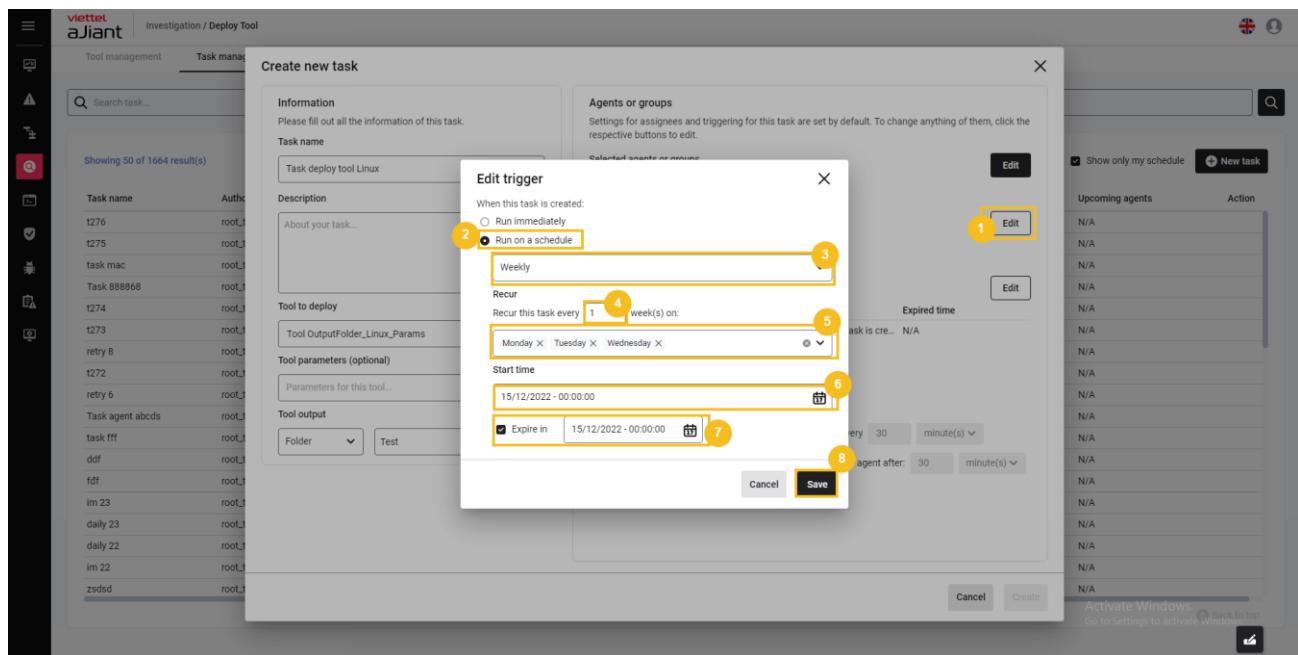
- Select Daily schedule:

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



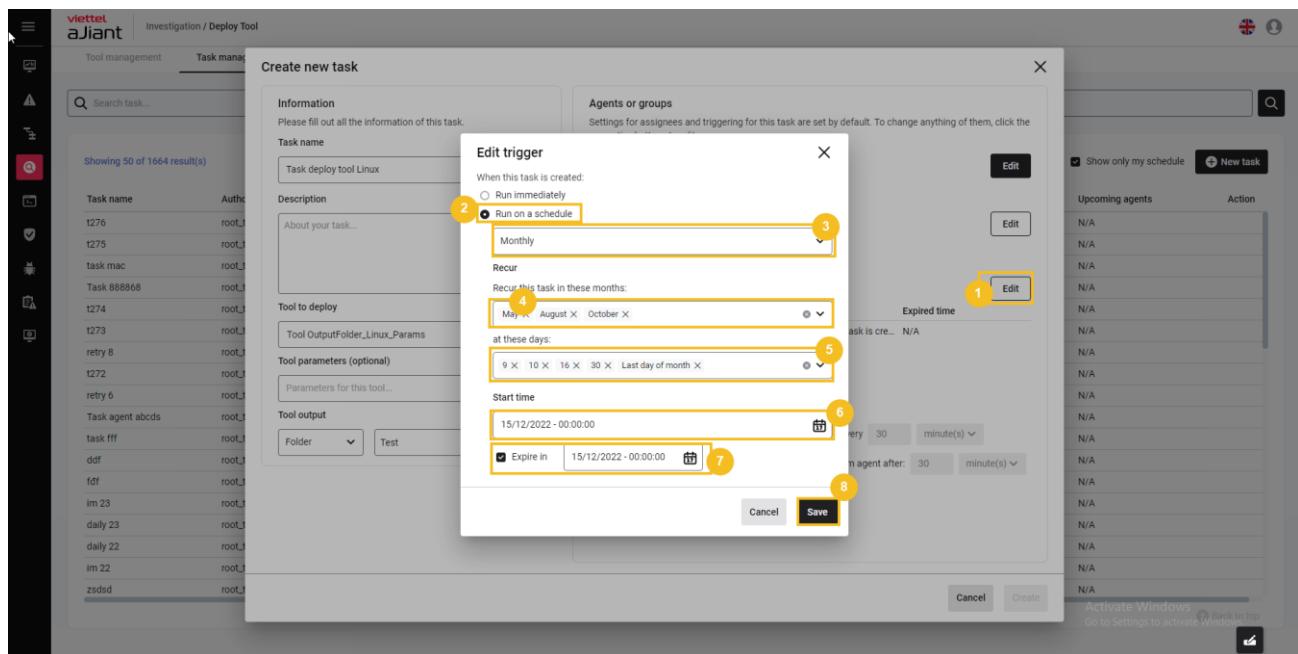
- Select Weekly schedule:

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

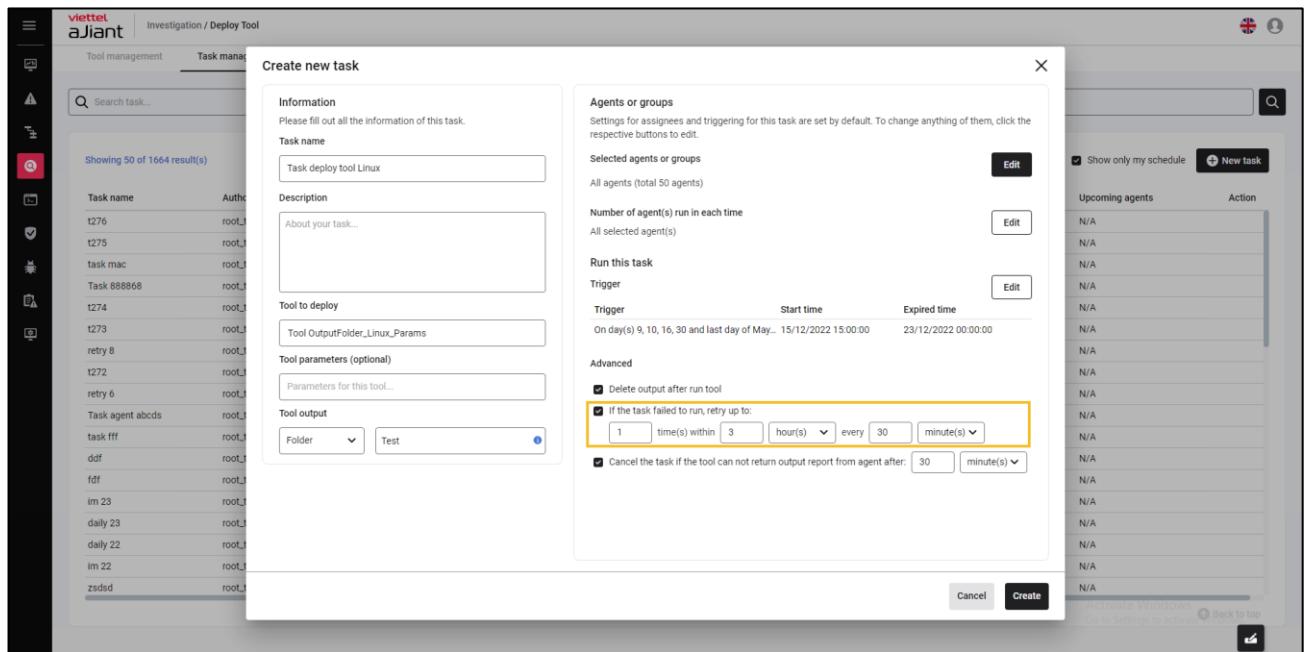


- Select Monthly schedule:

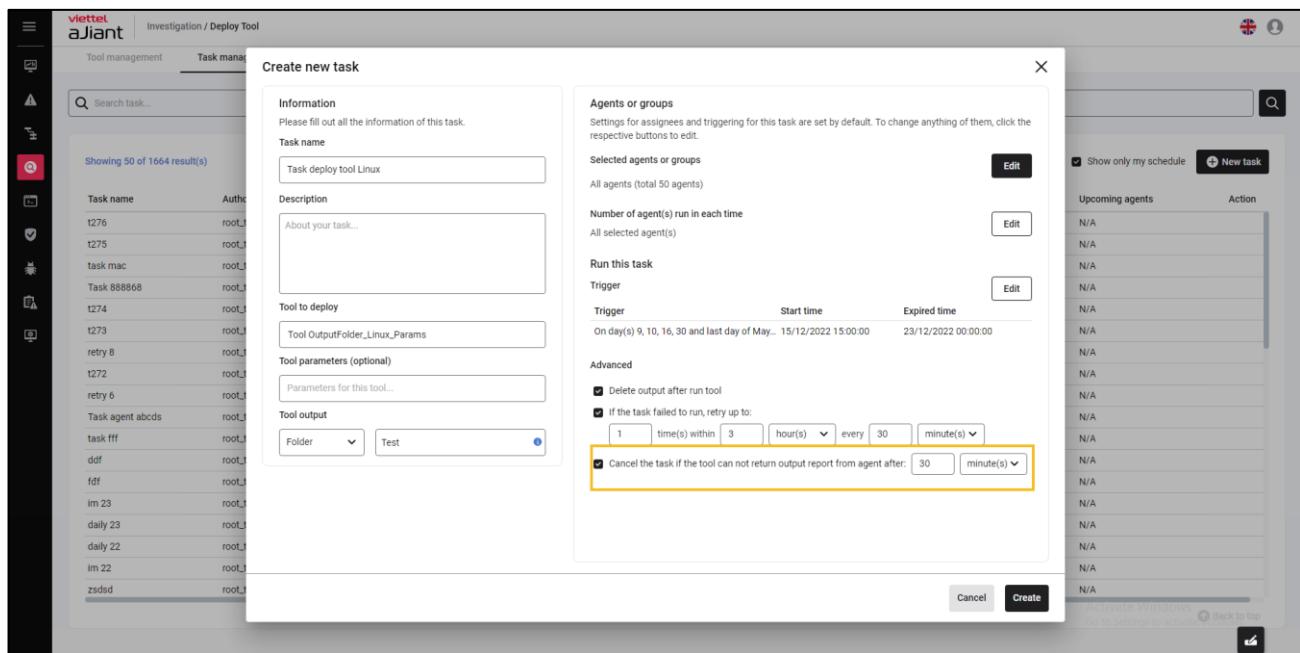
- Allow scheduling of monthly tool deployments;
- Repetition time;
- Start and end time configuration:



- 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.

viettel
aJiant | Investigation / Deploy Tool

Tool management Task management

task

Showing 50 of 285 result(s)

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	<input checked="" type="checkbox"/> Show only my schedule + New task
Task r6	root_test	15/12/2022 14:45:55	N/A	2	Immediately	N/A	● Finished	N/A	View report
Task r5	root_test	15/12/2022 14:45:28	N/A	2	Immediately	N/A	● In Progress	N/A	View detail
Task f4	root_test	15/12/2022 14:25:07	N/A	2	Immediately	N/A	● Finished	N/A	Duplicate this task
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	

Activate Windows Go to Settings to activate Windows

- 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.

viettel
aJiant | Investigation / Deploy Tool

Tool management Task management

task

Showing 50 of 285 result(s)

Duplicate task

Information
Please fill out all the information of this task.

Task name task duplicate 1 1

Description About your task...

Tool to deploy Tool OutputFolder_Linux_Params

Tool parameters (optional) Parameters for this tool...

Tool output File Downloads/test.txt 2

Agents or groups
Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit.

Selected agents or groups Edit

2 agent(s)

Agent ID	Computer name	IP Address	Group	Status	Action
3AAE6A6001F4...	redhat_tester	192.168.6.44,19...	maitest225	Online	
CB03FC002664...	centos7_test_hostname...	192.168.6.118,1...	maitest225	Online	

Number of agent(s) run in each time Edit

All selected agent(s)

Run this task

Trigger Edit

Trigger Immediately Start time At the time this task is cre... Expired time N/A

Advanced

Delete output after run tool

If the task failed to run, retry up to: 1 time(s) within 3 hour(s) every 30 minute(s)

Cancel the task if the tool can not return output report from agent after: 30 minute(s)

Cancel 2 Create

Activate Windows Go to Settings to activate Windows

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:

Showing 100 of 290 result(s)

Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
Task immediately 989	root_test	07/12/2022 14:49:13	N/A	1	Immediately	N/A	● stopped	N/A	
Task 8955455	root_test	07/12/2022 13:55:58	N/A	1	Immediately	N/A	● Finished	N/A	
Task Monthly MacOS	root_test	06/12/2022 18:25:02	N/A	1	On day(s) 7, 8, 9, 10, 11, 12, 13, 14, 15, 18 of November 2022	07/11/2023 09:00:00	● In Progress	N/A	
Task weekly MacOS	root_test	06/12/2022 18:23:59	N/A	1	On Mondays, Tuesdays, Wednesdays, Thursdays, ...	16/12/2022 09:00:00	● In Progress	N/A	
Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	1	Every 1 day(s) at 09:00:00	16/12/2022 09:00:00	● In Progress	N/A	
Task 7647657465	root_test	06/12/2022 17:57:36	N/A	1	Immediately	N/A	● Finished	N/A	
new task 8	root_test	06/12/2022 17:56:16	N/A	1	Immediately	N/A	● Finished	N/A	
new task 6	root_test	06/12/2022 17:50:15	N/A	1	Immediately	N/A	● Finished	N/A	
new task 4	root_test	06/12/2022 17:43:13	N/A	1	Immediately	N/A	● Finished	N/A	
Task macosvib 1	root_test	06/12/2022 16:41:35	N/A	1	Immediately	N/A	● stopped	N/A	
Task monthly dai	root_test	06/12/2022 15:18:38	N/A	1	On day(s) 7, 8, 9, 10, 11, 12 of December at 09:00:00	07/12/2022 09:00:00	● stopped	N/A	
Task abfbvrf	root_test	06/12/2022 13:58:21	N/A	1	Immediately	N/A	● Finished	N/A	
New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednesday every 1 week(s) at 12:00:00	19/12/2022 12:00:00	● In Progress	N/A	
Task 787878f	root_test	06/12/2022 11:11:58	N/A	1	Immediately	N/A	● Finished	N/A	
New task 1	root_test	06/12/2022 11:11:42	Description	48	Immediately	N/A	● Finished	N/A	
Task test retry 132	root_test	06/12/2022 10:49:15	N/A	1	Immediately	N/A	● Finished	N/A	
Task abfbvrf	root_test	06/12/2022 13:58:21	N/A	1	Immediately	N/A	● Finished	N/A	
New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednesday every 1 week(s) at 12:00:00	19/12/2022 12:00:00	● In Progress	N/A	

Activate Windows
Go to Settings to activate Windows 10

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:

Showing 100 of 290 result(s)

Task name	Author	Created time	Description	Number of agent(s)	Trigger
Task immediately 989	root_test	07/12/2022 14:49:13	N/A	1	Immediately
Task 8955455	root_test	07/12/2022 13:55:58	N/A	1	Immediately
Task Monthly MacOS	root_test	06/12/2022 18:25:02	N/A	1	On day(s) 7, 8, 9, 10, 11, 12, 13, 14, 15, 18 of November 2022
Task weekly MacOS	root_test	06/12/2022 18:23:59	N/A	1	On Mondays, Tuesdays, Wednesdays, Thursdays, ...
Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	1	Every 1 day(s) at 09:00:00
Task 7647657465	root_test	06/12/2022 17:57:36	N/A	1	Immediately
new task 8	root_test	06/12/2022 17:56:16	N/A	1	Immediately
new task 6	root_test	06/12/2022 17:50:15	N/A	1	Immediately
new task 4	root_test	06/12/2022 17:43:13	N/A	1	Immediately
Task macosvib 1	root_test	06/12/2022 16:41:35	N/A	1	Immediately
Task monthly dai	root_test	06/12/2022 15:18:38	N/A	1	On day(s) 7, 8, 9, 10, 11, 12 of December at 09:00:00
Task abfbvrf	root_test	06/12/2022 13:58:21	N/A	1	Immediately
New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednesday every 1 week(s) at 12:00:00
Task 787878f	root_test	06/12/2022 11:11:58	N/A	1	Immediately
New task 1	root_test	06/12/2022 11:11:42	Description	48	Immediately
Task test retry 132	root_test	06/12/2022 10:49:15	N/A	1	Immediately
Task abfbvrf	root_test	06/12/2022 13:58:21	N/A	1	Immediately
New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednesday every 1 week(s) at 12:00:00

View task detail

General

Name	Task immediately 989
Description	N/A
Tool to deploy	Bichpt3_Hello.exe
Parameters	N/A
Output type	none
Output path	N/A

Agents & groups

1 agent(s)

Agent ID	97617AC1A60945BE...	Computer name	Maingocwinx64	IP Address	192.168.74.128	Group	maitestd225	Status	Online
----------	---------------------	---------------	---------------	------------	----------------	-------	-------------	--------	--------

Number of agent(s) run in each time

All choosing agent(s)

Run this task

Trigger

Trigger	Immediately	Start time	At the time this task is created.	Expired time	N/A
---------	-------------	------------	-----------------------------------	--------------	-----

Advance

Retry	None
Timeout	None

Activate Windows
Go to Settings to activate Windows 10

h. View report (View tool result)

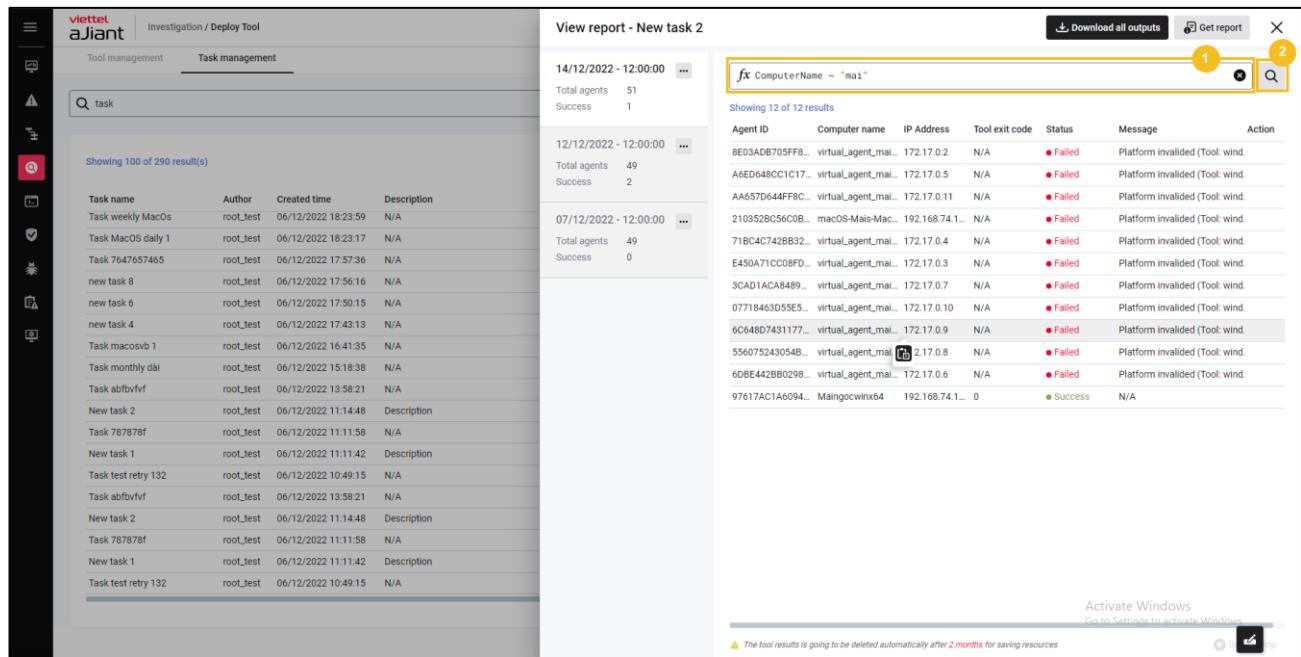
Purpose: To review the deployment tool report results;

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

The screenshot shows the aJiant investigation/deployment tool interface. On the left, there is a sidebar with various icons and a search bar. The main area has tabs for 'Tool management' and 'Task management', with 'Task management' selected. Below this, a search bar shows 'task'. The main content area displays a table of tasks with columns: Task name, Author, Created time, and Description. A search bar at the top right says 'Search by agent...'. Below the table, a detailed view report for a task is shown, with a header 'View report - New task 2' and a timestamp '14/12/2022 - 12:00:00'. The report table has columns: Agent ID, Computer name, IP Address, Tool exit code, Status, Message, and Action. The report shows 50 of 51 results. The status column includes icons for Failed (red), Success (green), and Expired (orange). The message column provides details for each entry, such as 'Architecture invalided (Tool:)' or 'Failed to get output(tool out...)'. A note at the bottom of the report says 'The tool results is going to be deleted automatically after 2 months for saving resources'.

+ 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.



View report - New task 2

14/12/2022 - 12:00:00

Total agents: 51 Success: 1

Showing 12 of 12 results

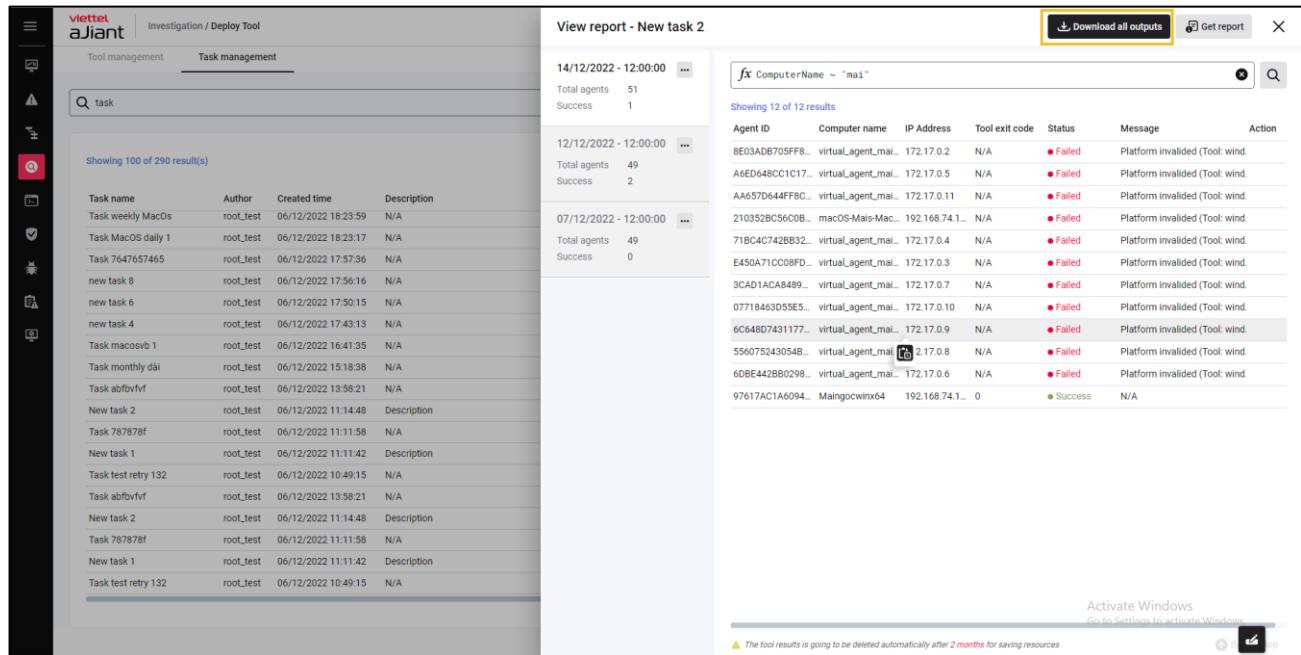
Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
8E03ADB705FF8...	virtual_agent_mai...	172.17.0.2	N/A	● Failed	Platform invalided (Tool: wind...	
A6ED648CC1C17...	virtual_agent_mai...	172.17.0.5	N/A	● Failed	Platform invalided (Tool: wind...	
AA6570644FF8C...	virtual_agent_mai...	172.17.0.11	N/A	● Failed	Platform invalided (Tool: wind...	
210352BC56C0B...	macOS-Mais-Mac...	192.168.74.1...	N/A	● Failed	Platform invalided (Tool: wind...	
71BC4C742B832...	virtual_agent_mai...	172.17.0.4	N/A	● Failed	Platform invalided (Tool: wind...	
E450A71CC08F0...	virtual_agent_mai...	172.17.0.3	N/A	● Failed	Platform invalided (Tool: wind...	
3CAD1ACA8489...	virtual_agent_mai...	172.17.0.7	N/A	● Failed	Platform invalided (Tool: wind...	
07718463D55E5...	virtual_agent_mai...	172.17.0.10	N/A	● Failed	Platform invalided (Tool: wind...	
6C648D7431177...	virtual_agent_mai...	172.17.0.9	N/A	● Failed	Platform invalided (Tool: wind...	
556075243054B...	virtual_agent_mai...	172.17.0.8	N/A	● Failed	Platform invalided (Tool: wind...	
60BE442B80298...	virtual_agent_mai...	172.17.0.6	N/A	● Failed	Platform invalided (Tool: wind...	
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	● Success	N/A	

Activate Windows
Go to Settings to activate Windows

The tool results is going to be deleted automatically after 2 months for saving resources

+ 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.



View report - New task 2

14/12/2022 - 12:00:00

Total agents: 51 Success: 1

Showing 12 of 12 results

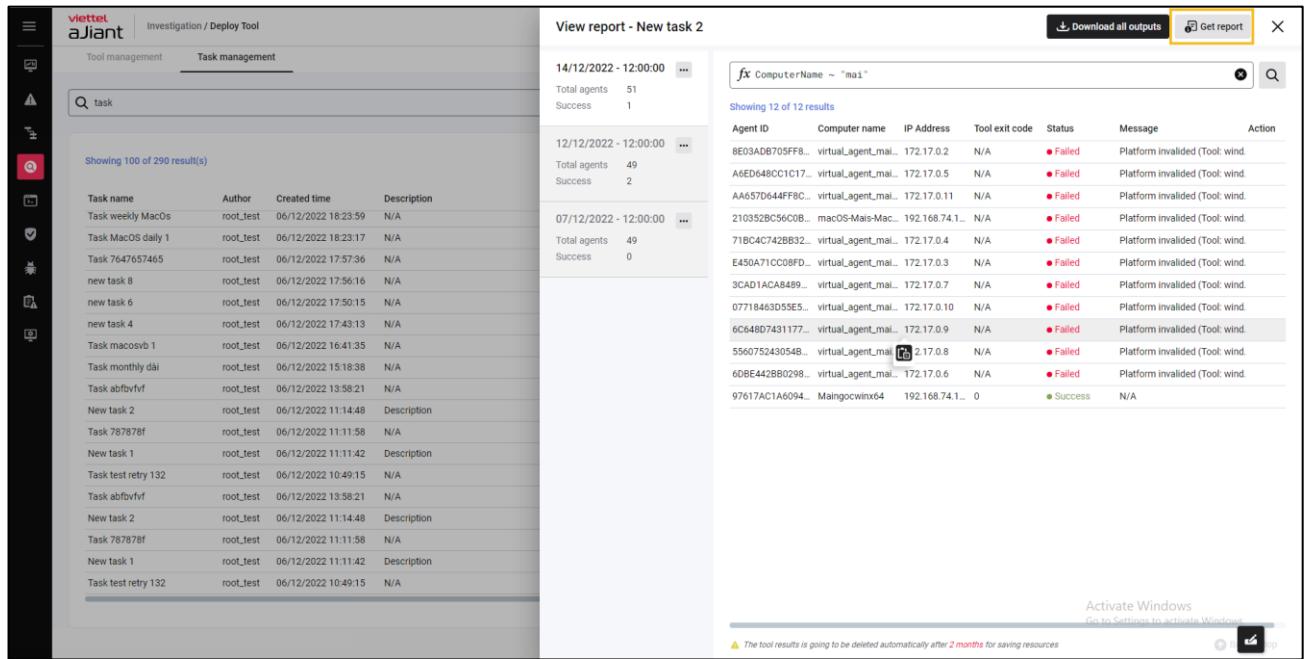
Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
8E03ADB705FF8...	virtual_agent_mai...	172.17.0.2	N/A	● Failed	Platform invalided (Tool: wind...	
A6ED648CC1C17...	virtual_agent_mai...	172.17.0.5	N/A	● Failed	Platform invalided (Tool: wind...	
AA6570644FF8C...	virtual_agent_mai...	172.17.0.11	N/A	● Failed	Platform invalided (Tool: wind...	
210352BC56C0B...	macOS-Mais-Mac...	192.168.74.1...	N/A	● Failed	Platform invalided (Tool: wind...	
71BC4C742B832...	virtual_agent_mai...	172.17.0.4	N/A	● Failed	Platform invalided (Tool: wind...	
E450A71CC08F0...	virtual_agent_mai...	172.17.0.3	N/A	● Failed	Platform invalided (Tool: wind...	
3CAD1ACA8489...	virtual_agent_mai...	172.17.0.7	N/A	● Failed	Platform invalided (Tool: wind...	
07718463D55E5...	virtual_agent_mai...	172.17.0.10	N/A	● Failed	Platform invalided (Tool: wind...	
6C648D7431177...	virtual_agent_mai...	172.17.0.9	N/A	● Failed	Platform invalided (Tool: wind...	
556075243054B...	virtual_agent_mai...	172.17.0.8	N/A	● Failed	Platform invalided (Tool: wind...	
60BE442B80298...	virtual_agent_mai...	172.17.0.6	N/A	● Failed	Platform invalided (Tool: wind...	
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	● Success	N/A	

Activate Windows
Go to Settings to activate Windows

The tool results is going to be deleted automatically after 2 months for saving resources

+ 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:



The screenshot shows the aJiant investigation / Deploy Tool interface. On the left, there's a sidebar with various icons. The main area has tabs for 'Tool management' and 'Task management', with 'Task management' selected. A search bar at the top right contains the query 'fx ComputerName ~ "mai"'. Below the search bar, it says 'Showing 12 of 12 results'. The results table has columns for 'Agent ID', 'Computer name', 'IP Address', 'Tool exit code', 'Status', 'Message', and 'Action'. Most entries show a red 'Failed' status with the message 'Platform invalidated (Tool: wind)'. One entry at the bottom shows a green 'Success' status with the message 'N/A'. The table header includes a '... More' button. At the bottom of the interface, there's a message about activating Windows and a note about tool results being deleted after 2 months.

+ 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.

The screenshot shows the aJiant Investigation / Deploy Tool interface. On the left, there is a sidebar with various icons and a search bar labeled 'task'. The main area is divided into two sections: 'Task management' and 'View report - New task 2'. The 'Task management' section shows a table of tasks with columns: Task name, Author, Created time, and Description. The 'View report - New task 2' section shows a table of results with columns: Computer name, IP Address, Tool exit code, Status, Message, and Action. The 'Status' column contains red dots indicating failed tasks. The 'Action' column shows a green dot for one successful task. A yellow callout box highlights the 'Download outputs' button in the report viewer.

Task name	Author	Created time	Description
Task weekly MacOs	root_test	06/12/2022 16:23:59	N/A
Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A
Task 7647657465	root_test	06/12/2022 17:57:36	N/A
new task 8	root_test	06/12/2022 17:56:16	N/A
new task 6	root_test	06/12/2022 17:50:15	N/A
new task 4	root_test	06/12/2022 17:43:13	N/A
Task macosvib 1	root_test	06/12/2022 16:41:35	N/A
Task monthly dài	root_test	06/12/2022 15:18:38	N/A
Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A
New task 2	root_test	06/12/2022 11:14:48	Description
Task 787878f	root_test	06/12/2022 11:11:58	N/A
New task 1	root_test	06/12/2022 11:11:42	Description
Task test retry 132	root_test	06/12/2022 10:49:15	N/A
Task abfbvfvf	root_test	06/12/2022 13:58:21	N/A
New task 2	root_test	06/12/2022 11:14:48	Description
Task 787878f	root_test	06/12/2022 11:11:58	N/A
New task 1	root_test	06/12/2022 11:11:42	Description
Task test retry 132	root_test	06/12/2022 10:49:15	N/A

14/12/2022 - 12:00:00	fx Computer: 2 ~ "mai"	Download outputs	Get report	Get results
12/12/2022 - 12:00:00	...	8E03AD8705FF8... virtual_agent_ma... 172.17.0.2 N/A ● Failed Platform invalided (Tool: wind.		
		A6ED648CC1C17... virtual_agent_ma... 172.17.0.5 N/A ● Failed Platform invalided (Tool: wind.		
		AA6570644FFBC... virtual_agent_ma... 172.17.0.11 N/A ● Failed Platform invalided (Tool: wind.		
07/12/2022 - 12:00:00	...	210352BC56C0B... macos-Mais-Mac... 192.168.74.1... N/A ● Failed Platform invalided (Tool: wind.		
		71BC4C742B832... virtual_agent_ma... 172.17.0.4 N/A ● Failed Platform invalided (Tool: wind.		
		E450A71CC086F0... virtual_agent_ma... 172.17.0.3 N/A ● Failed Platform invalided (Tool: wind.		
		3CA01ACA8489... virtual_agent_ma... 172.17.0.7 N/A ● Failed Platform invalided (Tool: wind.		
		07718463055E5... virtual_agent_ma... 172.17.0.10 N/A ● Failed Platform invalided (Tool: wind.		
		6C648D7431177... virtual_agent_ma... 172.17.0.9 N/A ● Failed Platform invalided (Tool: wind.		
		556075240504B... virtual_agent_ma... 172.17.0.8 N/A ● Failed Platform invalided (Tool: wind.		
		6D8E442BB0298... virtual_agent_ma... 172.17.0.6 N/A ● Failed Platform invalided (Tool: wind.		
		97617AC1A6094... Maingocwinx64 192.168.74.1... 0 ● Success N/A		

+ 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.

The screenshot shows the Ajiant Investigation / Deploy Tool interface. On the left, there's a sidebar with various icons and a search bar labeled 'task'. The main area has two tabs: 'Tool management' and 'Task management'. The 'Task management' tab is selected, showing a table of tasks with columns: Task name, Author, Created time, and Description. A search bar at the top of this table is also labeled 'task'. On the right, a detailed report for a task is displayed. The report title is 'View report - New task 2'. It shows a table of results with columns: Computer name, IP Address, Tool exit code, Status, Message, and Action. The status for most entries is 'Failed', except for one entry which is 'Success'. A yellow box highlights the 'Get report' button, and another yellow box highlights the 'Status' column for the successful entry. At the bottom of the report, there's a message: 'The tool results is going to be deleted automatically after 2 months for saving resources'.

+ 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.

This screenshot is similar to the one above, showing the Ajiant Investigation / Deploy Tool interface. The 'Task management' tab is selected, and the 'Status' column for the last entry in the report table is highlighted with a yellow box. This entry is for a task with 'Status' set to 'Success'. A yellow box also highlights the 'View tool output' icon in the bottom right corner of the report table.

- + 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.

The screenshot shows a 'View report - New task 2' interface. At the top, there are buttons for 'Download all outputs' and 'Get report'. The main area displays deployment results for 51 agents, with 1 success. The table includes columns for Agent ID, Computer name, IP Address, Tool exit code, Status, Message, and Action. A message at the bottom states: 'The tool results is going to be deleted automatically after 2 months for saving resources. Go to Settings to adjust. [Delete] [Stop]'.

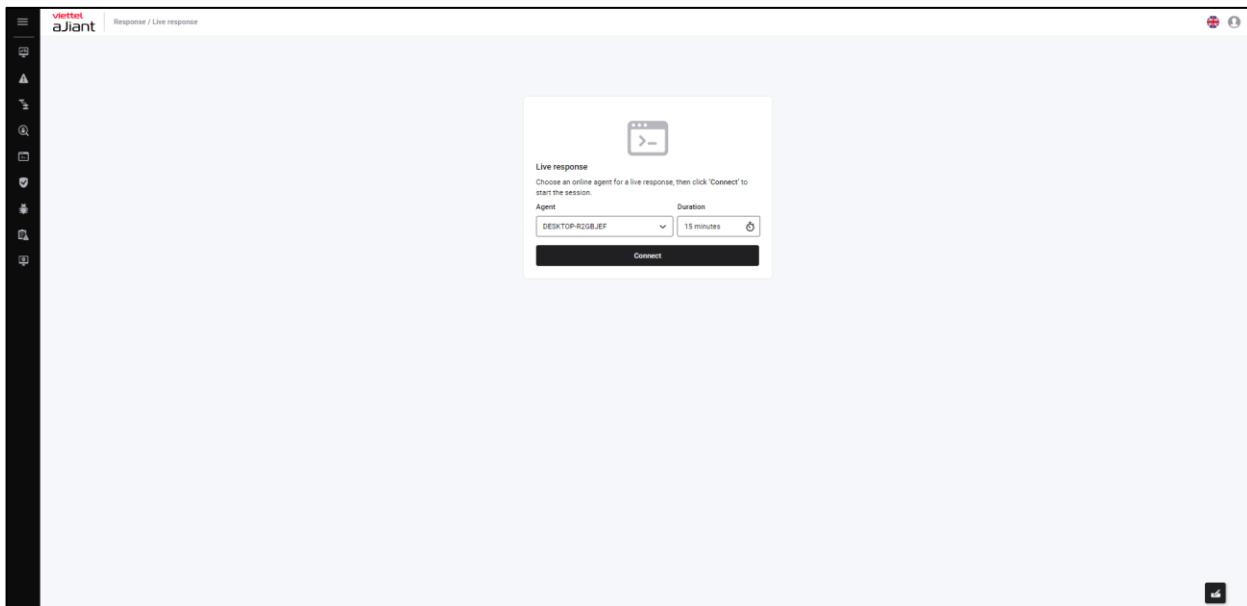
3.5 Response Screen

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.

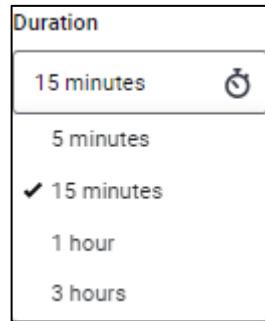
Select Agent: Display the list of agents:

- + 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:



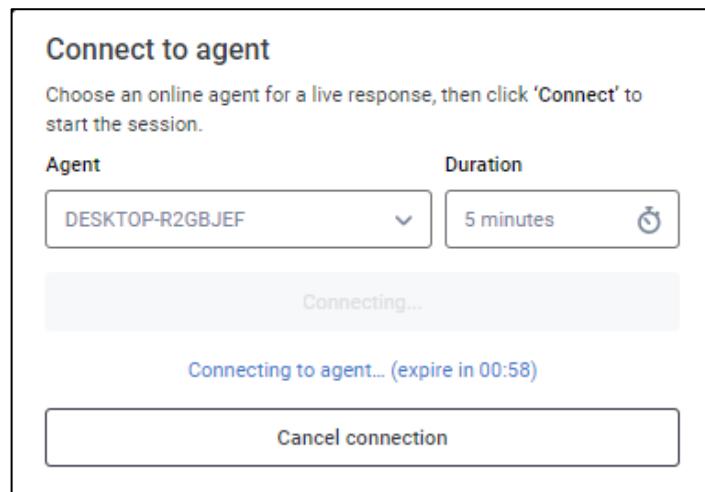
- + Select Duration: options include 5 minutes, 15 minutes, 1 hour, 3 hours;



- + Click the “Connect” button:

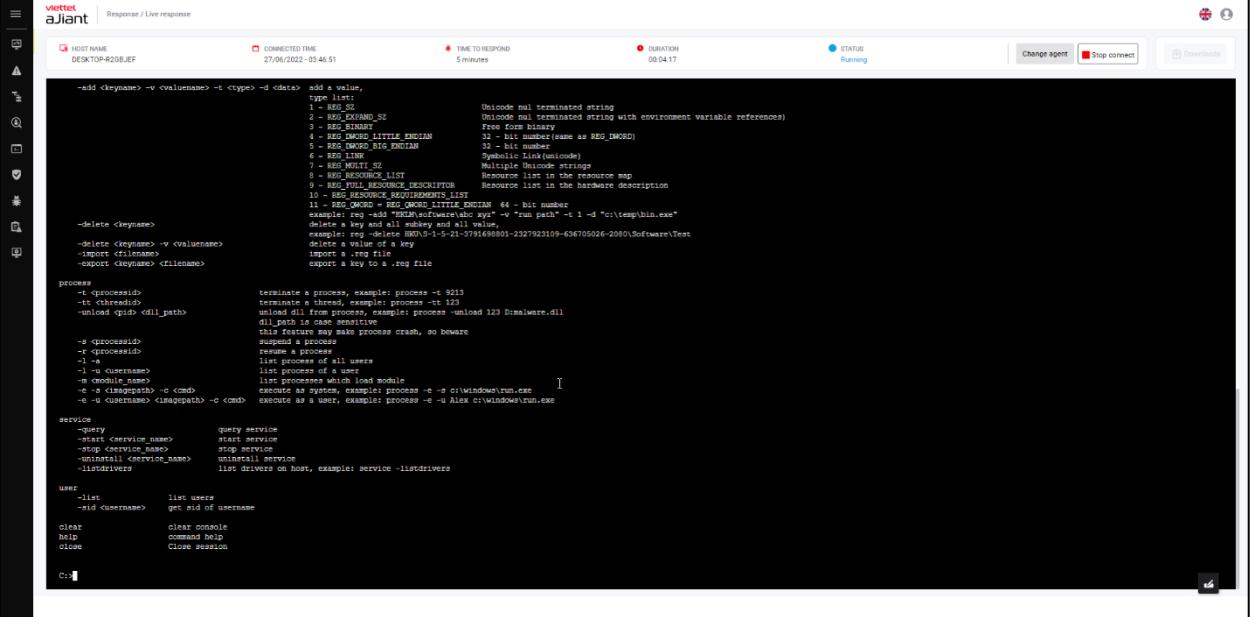


Bước 5: Wait 1 minute for the system to connect to the agent; the system status is "connecting":



- 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.



```

viettel
ajiant | Response / Live response

HOST NAME: DESKTOP-4208JEF CONNECTED TIME: 27/06/2022 - 03:46:51 TIME TO RESPOND: 5 minutes DURATION: 00:04:17 STATUS: Running
Change agent Stop connect Downloads

- add <keyname> -v <value> -t <type> -d <data> add a value, type list:
  1 - REG_EXPAND_SZ Unicode null terminated string
  2 - REG_EXPAND_SZ Unicode null terminated string with environment variable references
  3 - REG_BINARY Free form binary
  4 - REG_DWORD_LITTLE_ENDIAN 32 - bit number (name as REG_DWORD)
  5 - REG_DWORD_BIG_ENDIAN 32 - bit number (name as REG_DWORD)
  6 - REG_LINK Symbolic Link (unicode)
  7 - REG_MULTI_SZ Multiple Unicode strings
  8 - REG_RESOURCE_LIST Resource list in the registry
  9 - REG_FULL_RESOURCE_DESCRIPTOR Resource list in the hardware description
  10 - REG_RESOURCE_REQUIREMENTS_LIST

- delete <keyname>
- delete <keyname> -v <value>
- import <filename>
- export <keyname> <filename>

process
- t <processid> terminate a process, example: process -t 9215
- tt <processid> terminate a process, example: process -tt 123
- unload <pid> <dll_path> unload dll from process, example: process -unload 123 Dimware.dll
  dll_path is case sensitive
  -u <processid> send a process crash, so remove
  -r <processid> resume a process
  -l <username> list processes of all users
  -lu <username> list processes of a user
  -m <module_name> list processes which load module
  -e <s> <imagepath> <cmd> execute as system, example: process -e <s> c:\Windows\run.exe
  -e <u> <username> <imagepath> <cmd> execute as a user, example: process -e <u> ALEX c:\Windows\run.exe

service
- query
- start <service_name> start service
- stop <service_name> stop service
- uninstall <service_name> uninstall service
- listdrives list drives on host, example: service -listdrives

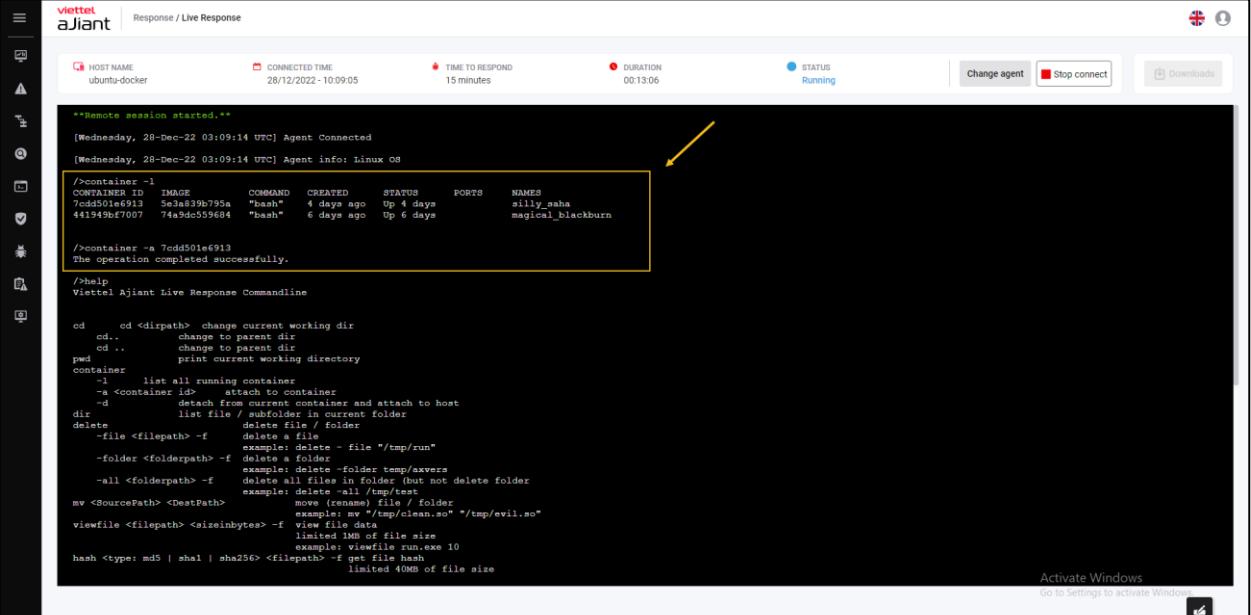
user
- list list users
- uid <username> get uid of username

clear
help command help
close Close session

C:\>

```

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



```

viettel
ajiant | Response / Live Response

HOST NAME: ubuntu-docker CONNECTED TIME: 28/12/2022 - 10:09:05 TIME TO RESPOND: 15 minutes DURATION: 00:13:06 STATUS: Running
Change agent Stop connect Downloads

**Remote session started.**
[Wednesday, 29-Dec-22 03:09:14 UTC] Agent Connected
[Wednesday, 28-Dec-22 03:09:14 UTC] Agent info: Linux OS

/>container -l
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
7cd501e6913 5ea839b795a "bash" 4 days ago Up 4 days silly_saha
44194bf7007 74a9d559684 "bash" 6 days ago Up 6 days magical_blackburn

/>container -a 7cd501e6913
The operation completed successfully.

/>help
Viettel Ajiant Live Response Commandline

cd cd <dirpath> change current working dir
  cd .. change to parent dir
  cd . change to parent dir
pwd print current working directory
container
  -l list all running containers
  -a <container id> attach to container
  -d detach from current container and attach to host
dir list file / subfolder in current folder
delete delete file / folder
  -f <filepath> -f
    example: delete -f "/tmp/run"
  -f <filepath> -f
    example: delete -f /tmp/xvers
  -all <filepath> -f
    delete all files in folder (but not delete folder)
    example: delete -all "/tmp/run"
mv <SourcePath> <DestPath>
  move (rename) file / folder
    example: mv "/tmp/clean.so" "/tmp/evil.so"
viewfile <filepath> <sizeinbytes> -f
  view file data
  -f <filepath> <sizeinbytes>
    example: viewfile run.exe 10
hash <type: md5 | sha1 | sha256> <filepath>
  get file hash
    limited 40MB of file size

Activate Windows
Go to Settings to activate Windows

```

Users can execute commands on the console screen as follows:

- + Window: execute the following commands:

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

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

No .	Command s	Parameter	Description
4		/ 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 .	Command s	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: "c:\temp\clean.exe" mv "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 .	Command s	Parameter	Description
		<pre>-process -pid <ProcessID> [-f <DestPath>] dump process by process ID Example: dump -process -pid 452 -f "C:\Users\Evil_dumped.dmp" "</pre>	Dump process by Process ID
		<pre>-process -name <ProcessName> [-f <DestPath>] dump process by process name Example: dump -process -name Evil.exe -f "C:\Users\Evil_dumped.dmp" "</pre>	Dump process by Process name
		<pre>-process -path <ProcessPath> [-f <DestPath>] dump process by process path Example: dump -process -path "C:\Users\Evil.exe" -f "C:\Users\Evil_dumped.dmp" "</pre>	Dump process by Process Path

No .	Command s	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.
			Commands related to the Registry
12	reg	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 .	Command s	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 .	Command s	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.	Command s	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\runpath.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.
		<p>-e -s <imagepath> -c <cmd> execute a non-GUI process as system Example: process -e -s /tmp/run</p>	
		<p>-e-u<username> <imagepath> -c <cmd> execute a non-GUI process as a user Example: process -e -u Alex /tmp/run</p>	
		<p>-d <processid> -o <imagepath> generate a core file of a running program, for example: process -d 231 -o /tmp/core_file</p>	
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
	13	-listdrivers list drivers on the host, example: service -listdrivers	List the drivers on the host.
13		-list -sid<username>	List the users on the machine. 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;

```

REG BINARY          Free form binary
4 - REG_DWORD LITTLE_ENDIAN 32 - bit number (same as REG_DWORD)
5 - REG_DWORD_BIG_ENDIAN 32 - bit number
6 - REG_LINK          Symbolic Link (unicode)
7 - REG_MULTI_SZ     Multiple Unicode strings
8 - REG_RESOURCE_LIST Resource list in the resource map
9 - REG_FULL_RESOURCE_DESCRIPTOR Resource list in the hardware description
10 - REG_RESOURCE_REQUIREMENTS_LIST

- delete <keyname>
- delete <keyname> -v <valueusername>
- import <filename>
- export <keyname> <filename>
- export

process
- t<processid>          terminate a process, example: process -t 9213
- tt<threadid>          terminate a thread, example: process -tt 123
- unload <pid> <dll_path> unload dll from process, example: process -unload 123 D:\malware.dll
  dll_path is case sensitive
  this feature may make process crash, so beware

-s <processid>          suspend a process
-r <processid>          resume a process
-l <u>                     list process of all users
-l <u> <username>          list process of a user
-m <module_name>          list processes which load module
-e <s> <imagepath> <-c <cmd> execute as system, example: process -e -s c:\windows\run.exe
-e <u> <username> <imagepath> <-c <cmd> execute as a user, example: process -e -u Alex c:\windows\run.exe

service
- query                query service
- start <service_name> start service
- stop <service_name>  stop service
- uninstall <service_name> uninstall service
- listdrivers           list drivers on host, example: service -listdrivers

user
- list                 list users
- sid <username>        get sid of username

clear
help
close
  
```

C:> [Monday, 27-Jun-22 08:50:23 UTC] Session timeout, exit!

- + 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.

```

REG BINARY          Free form binary
4 - REG_DWORD LITTLE_ENDIAN 32 - bit number (same as REG_DWORD)
5 - REG_DWORD_BIG_ENDIAN 32 - bit number
6 - REG_LINK          Symbolic Link (unicode)
7 - REG_MULTI_SZ     Multiple Unicode strings
8 - REG_RESOURCE_LIST Resource list in the resource map
9 - REG_FULL_RESOURCE_DESCRIPTOR Resource list in the hardware description
10 - REG_RESOURCE_REQUIREMENTS_LIST

- delete <keyname>
- delete <keyname> -v <valueusername>
- import <filename>
- export <keyname> <filename>

process
- t<processid>          terminate a process, example: process -t 9213
- tt<threadid>          terminate a thread, example: process -tt 123
- unload <pid> <dll_path> unload dll from process, example: process -unload 123 D:\malware.dll
  dll_path is case sensitive
  this feature may make process crash, so beware

-s <processid>          suspend a process
-r <processid>          resume a process
-l <u>                     list process of all users
-l <u> <username>          list process of a user
-m <module_name>          list processes which load module
-e <s> <imagepath> <-c <cmd> execute as system, example: process -e -s c:\windows\run.exe
-e <u> <username> <imagepath> <-c <cmd> execute as a user, example: process -e -u Alex c:\windows\run.exe

service
- query                query service
- start <service_name> start service
- stop <service_name>  stop service
- uninstall <service_name> uninstall service
- listdrivers           list drivers on host, example: service -listdrivers

user
- list                 list users
- sid <username>        get sid of username

clear
help
close
  
```

C:>close
[Monday, 27-Jun-22 08:52:53 UTC] agent closed

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.

Platform	IP address	Device current status	Action status	Action by	Last action on	Description	Action
ubuntu	127.0.0.1;1,192.168...	Network connected	Isolate In Process	root	28/10/2025 17:25:14	ovw	
Microsoft Windows Server 2...	fe80:451e:1031:340...	Network connected	Isolate Failed	monitor	28/10/2025 17:24:27	3333	
ubuntu20	127.0.0.1;1,10.25.2...	Network connected	Isolate In Process	root	28/10/2025 17:22:32	456	
ubuntu	127.0.0.1;1,10.2.2.1...	Network connected	Isolate Failed	root	28/10/2025 17:22:32	456	
centos	127.0.0.1;1,192.168...	Network connected	Isolate Failed	root	28/10/2025 17:22:32	456	
ubuntu	127.0.0.1;1,192.168...	Network connected	Release In Process	root	28/10/2025 17:22:32	123	
ubuntu	127.0.0.1;1,192.168...	Network connected	Release Failed	root	28/10/2025 17:22:32	123	
ubuntu	127.0.0.1;1,192.168...	Network connected	Isolate Failed	root	28/10/2025 17:22:32	456	
ubuntu	127.0.0.1;1,192.168...	Network connected	Release Applied	root	06/08/2025 21:02:11	test description	

Step 2: Select the Isolate devices button.

Isolate devices from the network

This action will isolate the devices from the network. It will remain connected to the VCS-aJiant for endpoint service.

Agents list

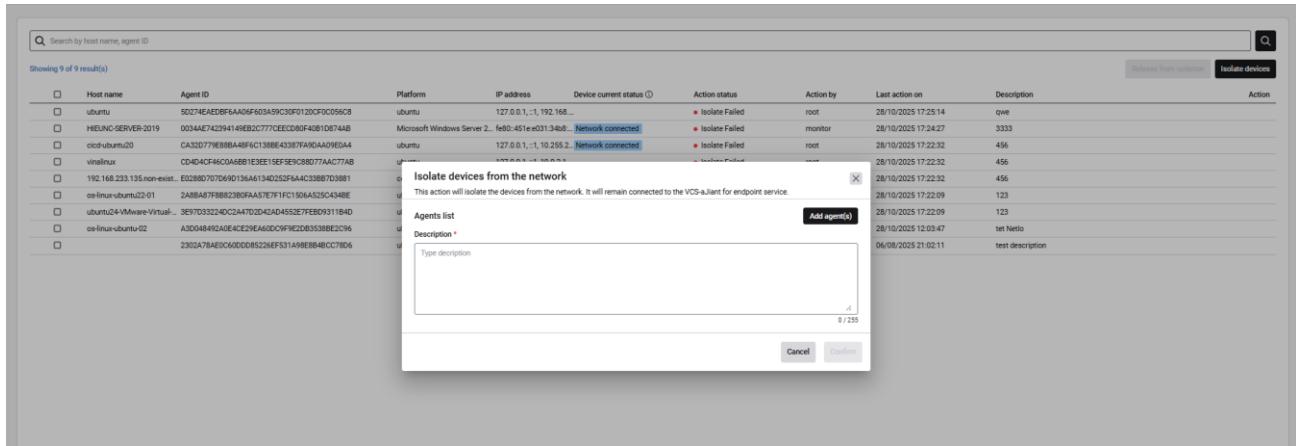
Add agents

Cancel Confirm

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.



Showing 9 of 9 result(s)

Host name	Agent ID	Platform	IP address	Device current status	Action status	Action by	Last action on	Description	Action
ubuntu	50274AE0D1B96A406F603A99C09F0120CF0C056C8	ubuntu	127.0.0.1...192.168...	Network connected	Isolate Failed	root	28/10/2025 17:25:14	qwe	
HEUNO- SERVER-2019	0034AE742394149EB2C777CEC0D940B10B744B	Microsoft Windows Server 2...	fe80:451:e031:34b:8...	Network connected	Isolate Failed	monitor	28/10/2025 17:24:27	3333	
ciod-ubuntu20	CA32D779E88BA4B94FC1398E4397FA90A409E6D44	ubuntu	127.0.0.1...10.255.2	Network connected	Isolate Failed	root	28/10/2025 17:22:32	456	
vinallinux	CD4D4CF46C0A68B1E5E16F9C98077A7ACT7AB	ubuntu	127.0.0.1...10.255.2	Network connected	Isolate Failed	root	28/10/2025 17:22:32	456	
192.168.233.135.non-exist...	E0288D707D601516A6134D252F6A4C3C887D3881	ubuntu	127.0.0.1...192.168...	Network connected	Isolate Failed	root	28/10/2025 17:22:32	456	
os-linux-ubuntu22-01	2A88A07F88B23B0FAA157EF1F1C1506A25C24348E	ubuntu	127.0.0.1...192.168...	Network connected	Isolate Failed	root	28/10/2025 17:22:09	123	
ubuntu24-VMware-Virtual...	3E97033224D2547D20424D4552E7F8909311B4D	ubuntu	127.0.0.1...192.168...	Network connected	Isolate Failed	root	28/10/2025 17:22:09	123	
os-linux-ubuntu22-02	A3D0484942A0E4C29E4600C9F9E2081938E8C7C9	ubuntu	127.0.0.1...192.168...	Network connected	Isolate Failed	root	28/10/2025 12:03:47	ter Netlo	
	2302A78A0C600D0B85226F531A98E884BCC7B6	ubuntu	127.0.0.1...192.168...	Network connected	Isolate Failed	root	06/08/2025 21:02:11	test description	

Isolate devices from the network
This action will isolate the devices from the network. It will remain connected to the VCS-assistant for endpoint service.

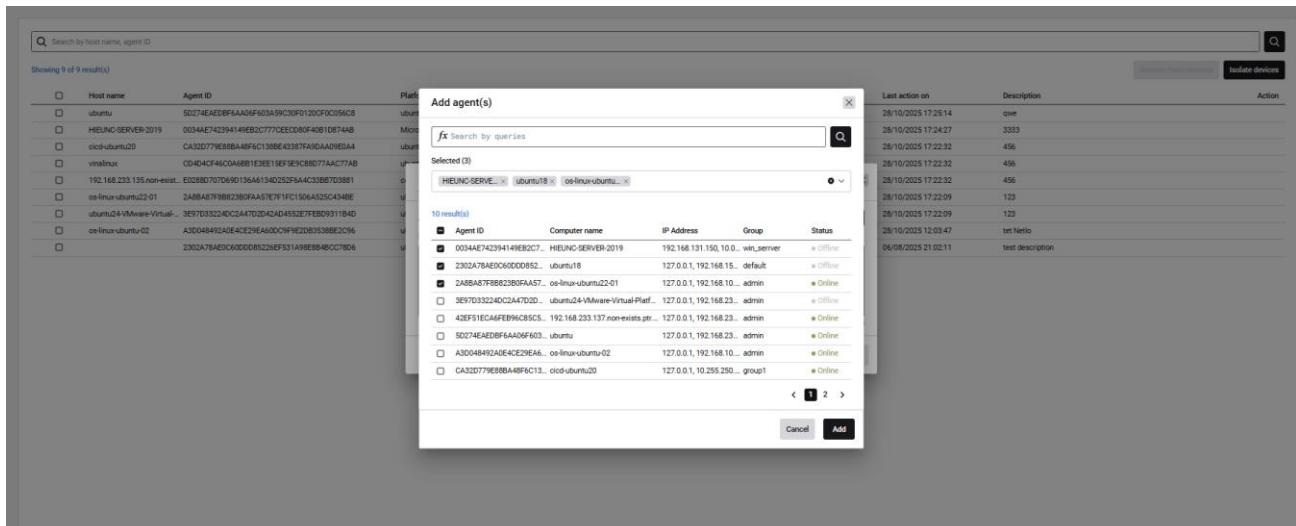
Agents list

Add agent(s)

Description :

Type description

Cancel Confirm



Showing 9 of 9 result(s)

Host name	Agent ID	Platform	IP address	Computer name	Group	Status	Last action on	Description	Action
ubuntu	50274AE0D1B96A406F603A99C09F0120CF0C056C8	ubuntu	192.168.150.10...	win_server	default	Online	28/10/2025 17:25:14	qwe	
HEUNO- SERVER-2019	0034AE742394149EB2C777CEC0D940B10B744B	Microsoft Windows Server 2...	fe80:451:e031:34b:8...	HEUNO-SERVER-2019	default	Online	28/10/2025 17:24:27	3333	
ciod-ubuntu20	CA32D779E88BA4B94FC1398E4397FA90A409E6D44	ubuntu	127.0.0.1...10.255.2	ubuntu18	default	Online	28/10/2025 17:22:32	456	
vinallinux	CD4D4CF46C0A68B1E5E16F9C98077A7ACT7AB	ubuntu	127.0.0.1...10.255.2	vinallinux	default	Online	28/10/2025 17:22:32	456	
192.168.233.135.non-exist...	E0288D707D601516A6134D252F6A4C3C887D3881	ubuntu	127.0.0.1...192.168...	192.168.233.135.non-exist...	default	Online	28/10/2025 17:22:32	456	
os-linux-ubuntu22-01	2A88A07F88B23B0FAA157EF1F1C1506A25C24348E	ubuntu	127.0.0.1...192.168...	os-linux-ubuntu22-01	default	Online	28/10/2025 17:22:09	123	
ubuntu24-VMware-Virtual...	3E97033224D2547D20424D4552E7F8909311B4D	ubuntu	127.0.0.1...192.168...	ubuntu24-VMware-Virtual...	default	Online	28/10/2025 17:22:09	123	
os-linux-ubuntu22-02	A3D0484942A0E4C29E4600C9F9E2081938E8C7C9	ubuntu	127.0.0.1...192.168...	os-linux-ubuntu22-02	default	Online	28/10/2025 12:03:47	ter Netlo	
	2302A78A0C600D0B85226F531A98E884BCC7B6	ubuntu	127.0.0.1...192.168...	ciod-ubuntu20	group1	Online	06/08/2025 21:02:11	test description	

Add agent(s)

Selected (3)

Selected (3) HUNO-SERVER-2019 ubuntu18 os-linux-ubuntu22-01

10 result(s)

Agent ID Computer name IP Address Group Status

0034AE742394149EB2C777CEC0D940B10B744B HUNO-SERVER-2019 192.168.150.10... win_server Online

2302A78A0C600D0B85226F531A98E884BCC7B6 ubuntu18 127.0.0.1...192.168.10... default Online

2A88A07F88B23B0FAA157EF1F1C1506A25C24348E 2A88A07F88B23B0FAA157EF1F1C1506A25C24348E 127.0.0.1...192.168.10... default Online

3E97033224D2547D20424D4552E7F8909311B4D 3E97033224D2547D20424D4552E7F8909311B4D 127.0.0.1...192.168.23... admin Online

42E8F151CA4FEB946C95C95 192.168.233.137.non-exist... 127.0.0.1...192.168.23... admin Online

50274AE0D1B96A406F603A99C09F0120CF0C056C8 50274AE0D1B96A406F603A99C09F0120CF0C056C8 127.0.0.1...192.168.23... admin Online

A3D0484942A0E4C29E4600C9F9E2081938E8C7C9 A3D0484942A0E4C29E4600C9F9E2081938E8C7C9 127.0.0.1...192.168.10... default Online

CA32D779E88BA4B94FC1398E4397FA90A409E6D44 CA32D779E88BA4B94FC1398E4397FA90A409E6D44 127.0.0.1...10.255.2 group1 Online

Cancel Add

Step 4: Confirm device isolation

The user presses Confirm to confirm the device isolation.

Showing 9 of 9 result(s)

Host name	Agent ID	Platform	IP address	Device current status	Action status	Action by	Last action on	Description	Action
Ubuntu	50274AE4DBF0AA0F65A9C95F012029C02056B			Network connected			28/10/2025 17:25:14	one	
HEINC- SERVER-2019	0034AE742394149E8C02777CEC080F40B10674AB			Network connected			28/10/2025 17:24:27	3333	
os- linux-ubuntu20	CA3207748898448F47388E433874904A09E044			Network connected			28/10/2025 17:22:32	496	
vinalinux	CD4D4C9F46C0448B1E2E15E5F3E90B8077AC77AB			Network connected			28/10/2025 17:22:32	496	
192.168.233.135.non-exist..	E038B0707061D136A8134D15F164C33B67038B1			Network connected			28/10/2025 17:22:32	496	
os- linux-ubuntu22-01	2A8B48788823B95A87E71F1190A530C4548E			Network connected			28/10/2025 17:22:32	123	
Ubuntu24-VMware-Virtual..	3E97033224D24A702D4A045527FEB0911B4D			Network connected			28/10/2025 17:22:32	123	
os- linux-ubuntu20	A30048492A0EACE29E460C9F9C2D035388E2C96			Network connected			28/10/2025 17:22:32	set Netio	
	2302A78AEB0909D0B085224F531A9E9848C0C7B06			Network connected			06/08/2025 21:02:11	test description	

Isolate devices from the network
This action will isolate the devices from the network. It will remain connected to the VCS-aJant for endpoint service.

Agents list

Agents

Agent ID Computer name IP Address Status Action

Isolate devices(s)

This action will isolate 3 devices from network.

Description hanhm

Cancel **Confirm**

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.

Showing 9 of 9 result(s)

Host name	Agent ID	Platform	IP address	Device current status	Action status	Action by	Last action on	Description	Action
HEINC-SERVER-2019	0034AE742394149E8C02777CEC080F40B10674AB	Microsoft Windows Server 2.._fe80:451:ef031:34b0..	Network connected				29/10/2025 17:52:52	hanhm	
os- linux-ubuntu22-01	2A8B48788823B95A87E71F1190A530C4548E	ubuntu	127.0.0.1..192.168..	Network connected	Isolate Failed	root	29/10/2025 17:52:58	hanhm	
ubuntu18	2302A78AEB0909D0B085224F531A9E9848C0C7B06	ubuntu	127.0.0.1..192.168..	Network connected	Isolate Failed	root	29/10/2025 17:52:58	hanhm	
os- linux-ubuntu-02	A30048492A0EACE29E460C9F9C2D035388E2C96	ubuntu	127.0.0.1..192.168..	Network connected	Release Failed	root	29/10/2025 15:24:12	99999	
192.168.233.135.non-exist..	E038B0707061D136A8134D15F164C33B67038B1	centos	127.0.0.1..192.168..	Network connected	Release Failed	root	29/10/2025 15:24:11	99999	
Ubuntu	50274AE4DBF0AA0F65A9C95F012029C02056B	ubuntu	127.0.0.1..192.168..	Network connected	Release Failed	root	29/10/2025 15:23:30	0	
os- linux-ubuntu20	CA3207748898448F47388E433874904A09E044	ubuntu	127.0.0.1..10.255.2..	Network connected	Isolate Failed	root	29/10/2025 15:22:16	99999	
Ubuntu24-VMware-Virtual..	3E97033224D24A702D4A045527FEB0911B4D	ubuntu	127.0.0.1..192.168..	Network connected	Isolate Failed	root	29/10/2025 15:22:16	99999	
vinalinux	CD4D4C9F46C0448B1E2E15E5F3E90B8077AC77AB	ubuntu	127.0.0.1..10.0.2..	Network connected	Isolate Failed	root	29/10/2025 15:22:16	99999	

Release from isolation

Isolate devices

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

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

Showing 9 of result(s)

Host name	Agent ID	Platform	IP address	Action
HEUNO-SERVER-2019	0034AE742394149EB2C777CECC00F428108744B	Microsoft Windows Server 2...	192.168.233.135	root 29/10/2025 17:52:58 hanhnm
ce-linus.ubuntu22.01	2A8BAE7F98823B0AA48F6C1388E43387FA90AA9ED44	ubuntu	127.0.0.1...	root 29/10/2025 17:52:58 hanhnm
ubuntu18	2302A878A9C000D0085229E5319A9E8B84BC7C7D6	ubuntu	127.0.0.1...	root 29/10/2025 17:52:58 hanhnm
ce-linus.ubuntu22.02	A30048492A0EACE29E460C09F92D0B3538BE2C296	ubuntu	127.0.0.1...,-1,192.168...	root 29/10/2025 15:24:12 99999
192.168.233.135.non-exist..	E0288D707D691396A6134D257F6A4C33887D3881	centos	127.0.0.1...,-1,192.168...	root 29/10/2025 15:24:11 99999
ubuntu	SD274EA2E9B5AA5F603A99C9D120CF0C056C8	ubuntu	127.0.0.1...	root 29/10/2025 15:23:30 0
ccid-ubuntu20	CA32D779E88A4B9613E91388E43387FA90AA9ED44	ubuntu	127.0.0.1...,-1,10.255.2	root 29/10/2025 15:22:16 99999
ubuntu24-VMware-Virtual...	3E97D03324D0C2A47024D424D52E7FEB911184D	ubuntu	127.0.0.1...,-1,192.168...	root 29/10/2025 15:22:16 99999
vinalinux	CD4D4CF46C0A68B1E3E19E5E9C98D77AAC77A8	ubuntu	127.0.0.1...,-10.0.2.1...	root 29/10/2025 15:22:16 99999

Release from isolation

This action will release 1 devices from network.

Cancel Confirm

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

Showing 9 of result(s)

Host name	Agent ID	Platform	IP address	Device current status	Action status	Action by	Last action on	Description	Action
ccid-ubuntu20	CA32D779E88A4B9613E91388E43387FA90AA9ED44	ubuntu	127.0.0.1...,-1,10.255.2	Network connected	Release In Process	root	29/10/2025 18:29:00	99999	
ubuntu24-VMware-Virtual...	3E97D03324D0C2A47024D424D52E7FEB911184D	ubuntu	127.0.0.1...,-1,192.168...	Release Failed	root	29/10/2025 18:29:00	99999		
ubuntu	SD274EA2E9B5AA5F603A99C9D120CF0C056C8	ubuntu	127.0.0.1...,-1,192.168...	Release In Process	root	29/10/2025 18:29:00	0		
HEUNO-SERVER-2019	0034AE742394149EB2C777CECC00F428108744B	Microsoft Windows Server 2...	192.168.233.135	Network connected	Release Failed	root	29/10/2025 18:28:59	hanhnm	
ce-linus.ubuntu22.01	2A8BAE7F98823B0AA48F6C1388E43387FA90AA9ED44	ubuntu	127.0.0.1...,-1,192.168...	Release In Process	root	29/10/2025 18:28:59	hanhnm		
ubuntu18	2302A878A9C000D0085229E5319A9E8B84BC7C7D6	ubuntu	127.0.0.1...,-1,192.168...	Release Failed	root	29/10/2025 18:28:59	hanhnm		
ce-linus.ubuntu22.02	A30048492A0EACE29E460C09F92D0B3538BE2C296	ubuntu	127.0.0.1...,-1,192.168...	Release In Process	root	29/10/2025 18:28:59	99999		
vinalinux	CD4D4CF46C0A68B1E3E19E5E9C98D77AAC77A8	ubuntu	127.0.0.1...,-10.0.2.1...	Release Failed	root	29/10/2025 18:28:59	99999		
192.168.233.135.non-exist..	E0288D707D691396A6134D252F6A4C33887D3881	centos	127.0.0.1...,-1,192.168...	Release Failed	root	29/10/2025 18:28:59	99999		

Release from isolation

This action will release 1 devices from network.

Cancel Confirm

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.
 - o Network connected: normal network connection status
 - o 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.
 - o In process: indicates that the system is currently executing the user's request (Isolate devices/ Release from isolation).
 - o Applied: refers to the status indicating that the system has successfully executed the user's action (Isolate devices/ Release from isolation).
 - o 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

Showing 9 of 9 results(s)

<input type="checkbox"/>	Host name	Agent ID	Platform	IP address	Device current status	Action status	Action by	Last action on	Description	Action
<input type="checkbox"/>	HEIINC-SERVER-2019	0034AE742394149EB2777CECDB0f40B1D6744B	Microsoft Windows Server 2...	fe80:451e:031-34b...	Network connected	● Isolate Failed	root	29/10/2025 17:52:58	hanhnm	Release from isolation Isolate devices
<input type="checkbox"/>	ce-linux-ubuntu02-01	2A88AB788B2389FA577F7FC1506A525C4348E	ubuntu	127.0.0.1,-,192.168...	Network connected	● Isolate Failed	root	29/10/2025 17:52:58	hanhnm	
<input type="checkbox"/>	ubuntu18	2302A78AEC0600D005226F531A98E8B4BCC7BD5	ubuntu	127.0.0.1,-,192.168...	Network connected	● Isolate Failed	root	29/10/2025 17:52:58	hanhnm	
<input type="checkbox"/>	ce-linux-ubuntu-02	A3D0484920204E4C29E6A600DC9F9E20B358E2C96	ubuntu	127.0.0.1,-,192.168...	...	● Release Failed	root	29/10/2025 15:24:12	99999	
<input type="checkbox"/>	192.168.233.135.non-exist.	E028B07070690136A41342525f64C4C38B7D3881	centos	127.0.0.1,-,192.168...	...	● Release Failed	root	29/10/2025 15:24:11	99999	
<input type="checkbox"/>	ubuntu	50274EAD8FAA406F603A49C30F0120FC0C95C8	ubuntu	127.0.0.1,-,192.168...	...	● Isolate Failed	root	29/10/2025 15:23:30	0	
<input type="checkbox"/>	clust-ubuntu	CA32D779E8B8A48FC1C198E43387FA0DA09E044	ubuntu	127.0.0.1,-,10.255.2...	Network connected	● Isolate Failed	root	29/10/2025 15:22:16	99999	
<input type="checkbox"/>	ubuntu224-Vmware-Virtual	3E97033242C2A47D204DAD5527FEB0931184D	ubuntu	127.0.0.1,-,192.168...	...	● Isolate Failed	root	29/10/2025 15:22:16	99999	
<input type="checkbox"/>	vininux	C04D40F460A4881E3EE15E9E9C88D77AAC77AB	ubuntu	127.0.0.1,-,10.0.2.1...	...	● Isolate Failed	root	29/10/2025 15:22:16	99999	

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).

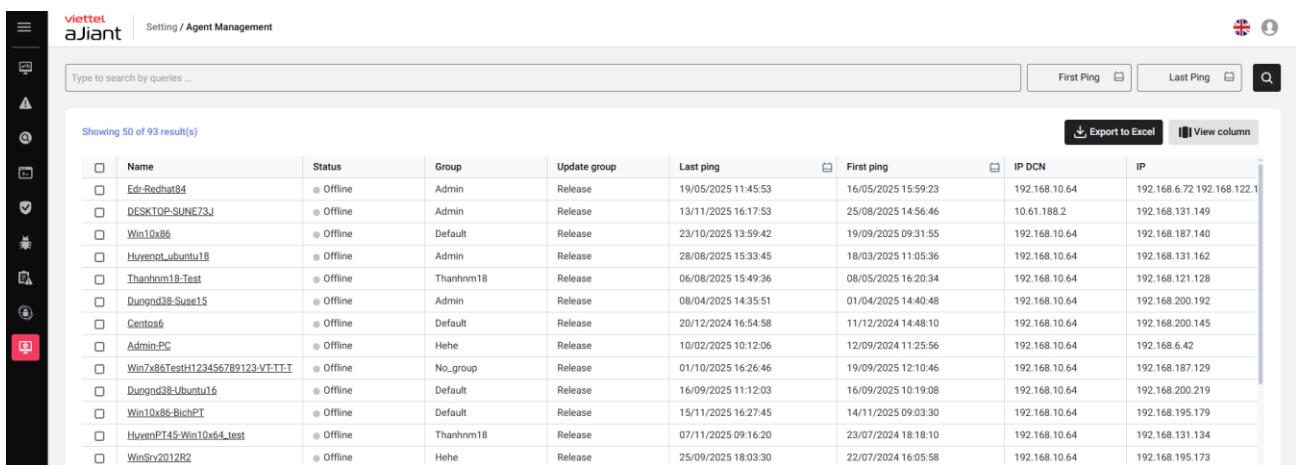
The screenshot shows the viettel ajiant interface for managing agents. On the left, a sidebar with icons for Home, Devices, Licenses, and Help. The main area has a search bar and a table titled 'Showing 9 of 9 result(s)'. The table columns are Host name, Agent ID, Platform, IP address, and Device current status. The table lists several agents, including 'cicc-ubuntu20' (Agent ID: CA32D77HE888BA48F6C1388E4397FA90A09EDAA, Platform: ubuntu, IP: 127.0.0.1, 192.168...), 'ubuntu24-VMware-Virtual...' (Agent ID: 3E570335240DC2A4702042AD4552E7EB059311B4D, Platform: ubuntu, IP: 127.0.0.1, 192.168...), and 'HIEUN- SERVER 2019' (Agent ID: 0334AE4742394149E8C77CEC0D80440B10744B, Platform: Microsoft Windows Server 2, IP: fe80:451e:037:348..., Status: Network connected). On the right, a detailed view for 'cicc-ubuntu20' is shown with a table titled 'View detail - cicc-ubuntu20' showing 6 results. The columns are Host name, Agent ID, Platform, IP address, Action, Action by, Last action on, and Description. The table lists 6 rows of actions taken on 10/20/2023, including 'Isolate device' and 'Release from isolation' for various IP addresses.

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);



Type to search by queries ...

Showing 50 of 93 result(s)

Export to Excel | View column

<input type="checkbox"/>	Name	Status	Group	Update group	Last ping	<input type="checkbox"/>	First ping	<input type="checkbox"/>	IP DCN	IP
<input type="checkbox"/>	Edr-Redhat84	<input type="checkbox"/> Offline	Admin	Release	19/05/2025 11:45:53	<input type="checkbox"/>	16/05/2025 15:59:23	<input type="checkbox"/>	192.168.10.64	192.168.6.72 192.168.122.1
<input type="checkbox"/>	DESKTOP-SUNE73J	<input type="checkbox"/> Offline	Admin	Release	13/11/2025 16:17:53	<input type="checkbox"/>	25/08/2025 14:56:46	<input type="checkbox"/>	10.61.188.2	192.168.131.149
<input type="checkbox"/>	Win10x86	<input type="checkbox"/> Offline	Default	Release	23/10/2025 13:59:42	<input type="checkbox"/>	19/09/2025 09:31:55	<input type="checkbox"/>	192.168.10.64	192.168.187.140
<input type="checkbox"/>	Huyenpt_ubuntu18	<input type="checkbox"/> Offline	Admin	Release	28/08/2025 15:33:45	<input type="checkbox"/>	18/03/2025 11:05:36	<input type="checkbox"/>	192.168.10.64	192.168.131.162
<input type="checkbox"/>	Thanhnm18-Test	<input type="checkbox"/> Offline	Thanhnm18	Release	06/08/2025 15:49:36	<input type="checkbox"/>	08/05/2025 16:20:34	<input type="checkbox"/>	192.168.10.64	192.168.121.128
<input type="checkbox"/>	Dungnd38-Suse15	<input type="checkbox"/> Offline	Admin	Release	08/04/2025 14:35:51	<input type="checkbox"/>	01/04/2025 14:40:48	<input type="checkbox"/>	192.168.10.64	192.168.200.192
<input type="checkbox"/>	Centos6	<input type="checkbox"/> Offline	Default	Release	20/12/2024 16:54:58	<input type="checkbox"/>	11/12/2024 14:48:10	<input type="checkbox"/>	192.168.10.64	192.168.200.145
<input type="checkbox"/>	Admin-PC	<input type="checkbox"/> Offline	Hehe	Release	10/02/2025 10:12:06	<input type="checkbox"/>	12/09/2024 11:25:56	<input type="checkbox"/>	192.168.10.64	192.168.6.42
<input type="checkbox"/>	Win7x86TestH123456789123-VT-TT-T	<input type="checkbox"/> Offline	No_group	Release	01/10/2025 16:26:46	<input type="checkbox"/>	19/09/2025 12:10:46	<input type="checkbox"/>	192.168.10.64	192.168.187.129
<input type="checkbox"/>	Dungnd38-Ubuntu16	<input type="checkbox"/> Offline	Default	Release	16/09/2025 11:12:03	<input type="checkbox"/>	16/09/2025 10:19:08	<input type="checkbox"/>	192.168.10.64	192.168.200.219
<input type="checkbox"/>	Win10x86-BichPT	<input type="checkbox"/> Offline	Default	Release	15/11/2025 16:27:45	<input type="checkbox"/>	14/11/2025 09:03:30	<input type="checkbox"/>	192.168.10.64	192.168.195.179
<input type="checkbox"/>	HuyenPT45-Win10x64_test	<input type="checkbox"/> Offline	Thanhnm18	Release	07/11/2025 09:16:20	<input type="checkbox"/>	23/07/2024 18:18:10	<input type="checkbox"/>	192.168.10.64	192.168.131.134
<input type="checkbox"/>	WinSrv2012R2	<input type="checkbox"/> Offline	Hehe	Release	25/09/2025 18:03:30	<input type="checkbox"/>	22/07/2024 16:05:58	<input type="checkbox"/>	192.168.10.64	192.168.195.173

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 "~".

Agent management

AgentID = '03031B3FE60E83372C4E45F8D5737FA190BA598B' AND

AgentID	Agent Computer Name	Agent Operating System	Agent Architecture	Agent Platform	Applied Policy	IP DCN
03031B3FE60E83372C4E45F8D5737FA190BA598B						

First Ping Last Ping

POLICY	VERSION
phula_test	
anhn_full_features	3.3.8
N/A	

Examples of search queries:

- + Search with the condition "=":

Agent management

Policy = 'phula_test'

1 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
localhost.Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	

Display 1/1 result

- + Search with the condition "!=":

Agent management

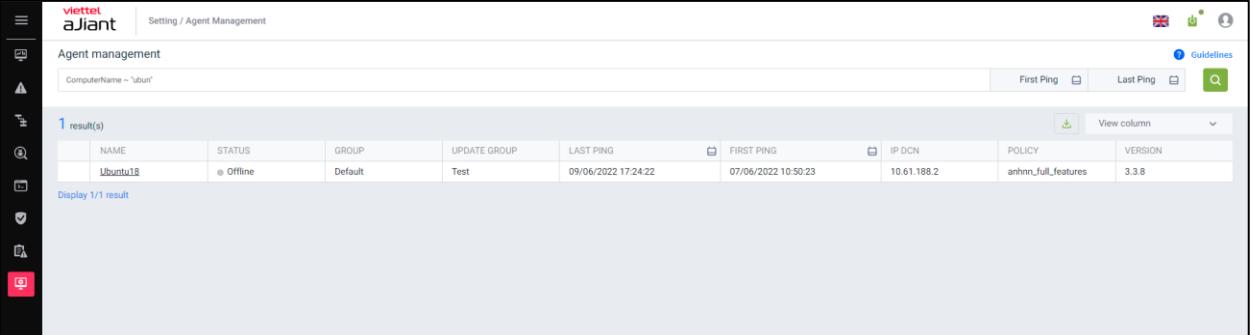
Policy != 'phula_test'

2 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhn_full_features	3.3.8
N/A	Offline	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Display 2/2 result

- + Search with the condition "~":



Agent management

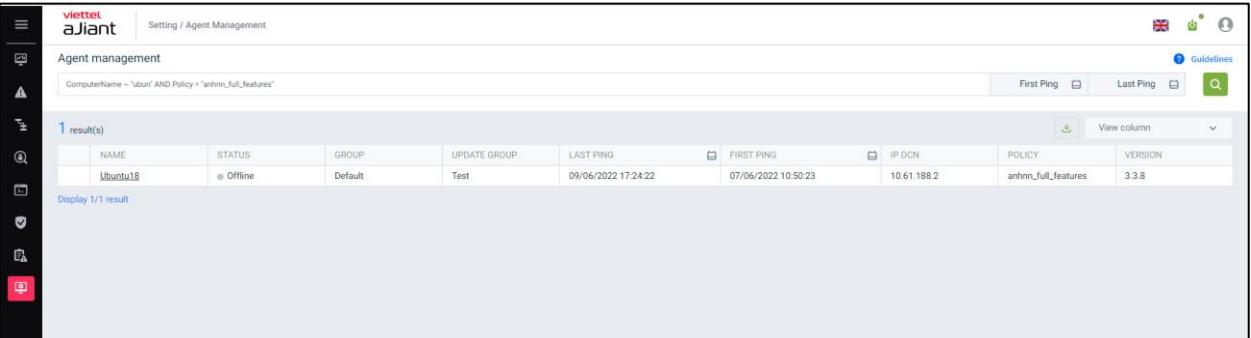
ComputerName ~ 'Ubuntu'

1 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8

Display 1/1 result

+ Search using combined AND criteria:



Agent management

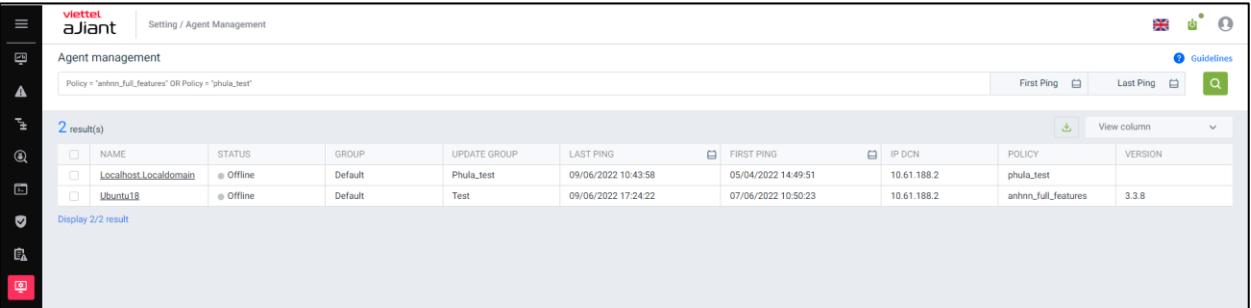
ComputerName ~ 'Ubuntu' AND Policy ~ 'anhnn_full_features'

1 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8

Display 1/1 result

+ Search using combined OR criteria:



Agent management

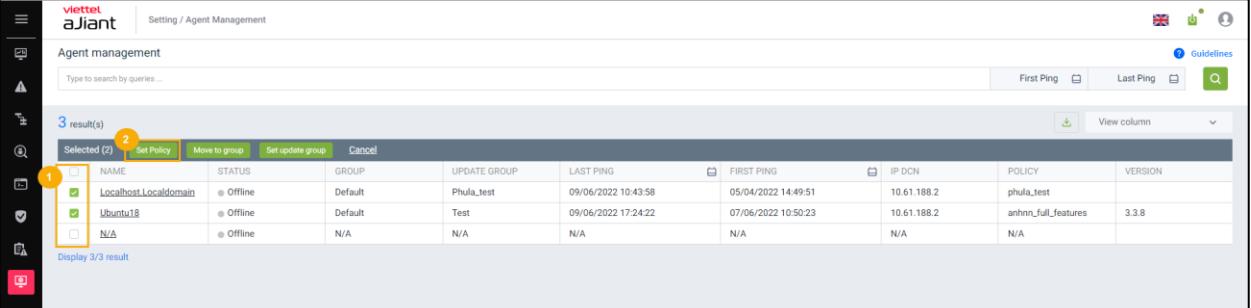
Policy ~ 'anhnn_full_features' OR Policy ~ 'phula_test'

2 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
localhost.localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8

Display 2/2 result

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



Agent management

Type to search by queries ...

3 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
localhost.localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnn_full_features	3.3.8

Display 3/3 result

Selected (2) 2 Set Policy Move to group Set update group Cancel

1

- + Select one agent/multiple agents to enter the Multiselected session;
- + Implement Set Policy:
 - Select Policy:

NAME	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test		
Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhn_n_full_features	3.3.8	
N/A	N/A	N/A	N/A	N/A	N/A	

- 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.

The screenshot shows the 'Agent management' section of the Viettel Agent Management interface. On the left, a sidebar with various icons and a search bar. The main area shows a table with 3 results, including 'localhost.localdomain' (Offline, Default group, Phula_test), 'Ubuntu18' (Offline, Default group, Test), and 'N/A' (Offline, N/A, N/A). On the right, the 'General info' tab is selected for the 'Agent localhost.localdomain'. It shows the following details:

General info	Network Interfaces
Host Name: localhost.localdomain	IP v4: 127.0.0.1
Host ID: 015a4d56-e545-241a-e66b-14410ce8c348	IP v6: ::1
Setup Version: N/A	MAC: N/A
Operating System: Linux	Name: lo
Platform: redhat	IP v4: 192.168.121.132
Platform Version: 8.2	IP v6: fe80::437edc7a:2765:34d
Platform Family: rhel	MAC: 00:0c:29:e8:c3:48
Architecture: amd64	Name: ens160
Physical Memory: 1,843,832	
CPUs	Default Gateway
Cores: 1	192.168.121.2
mhz: 1992.001000	DNS Server: 192.168.121.2
Model Name: Intel(R) Core(TM) i7-10700T CPU @ 2.00GHz	
Vendor ID: GenuineIntel	

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:

FRIENDLY_NAME	Microsoft Root Certificate Authority
ISSUER	DC=com, DC=microsoft, CN=Microsoft Root Certificate Authority
KEY_USAGE	Digital Signature, Non-Repudiation, Certificate Signing, Off-line CRL Signing, CRL Signing (c6)
SIGNATURE_ALGORITHM	sha1RSA
STATUS	R
SUBJECT	DC=com, DC=microsoft, CN=Microsoft Root Certificate Authority
VALID_FROM	10/05/2001 06:19:22

 A vertical scroll bar is visible on the right side of the window."/>

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.

XML Detail X

```

<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
<Date>2021-03-09T18:36:49.6502882</Date>
<Author>VCS\Administrator</Author>
<URI>dffffff</URI>
</RegistrationInfo>
<Triggers />
<Principals>
<Principal id="Author">
<UserId>S-1-5-21-3942219608-2782901308-3935319899-500</UserId>
<LogonType>InteractiveToken</LogonType>
<RunLevel>LeastPrivilege</RunLevel>
</Principal>
</Principals>
<Settings>
<MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
<DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
<StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
<AllowHardTerminate>true</AllowHardTerminate>
<StartWhenAvailable>false</StartWhenAvailable>
<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
<IdleSettings>
<StopOnIdleEnd>true</StopOnIdleEnd>
<RestartOnIdle>false</RestartOnIdle>
<...>

```

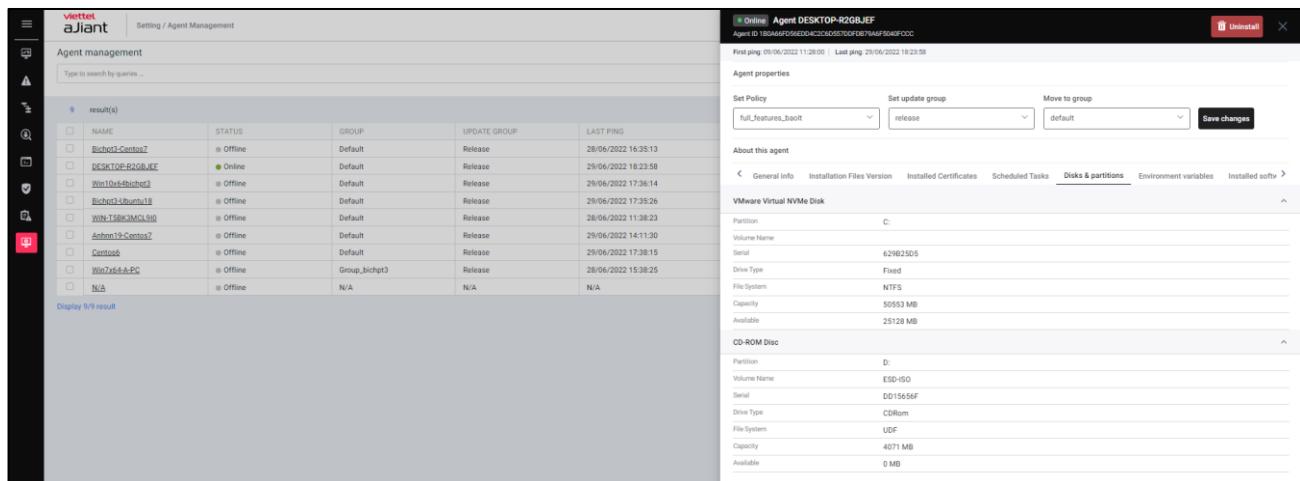
Export to XML

- + 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.



The screenshot shows the Viettel Agent management interface. On the left, a sidebar lists agents with their names and status (e.g., Online, Offline). The main panel displays detailed information for a selected agent, 'Agent DESKTOP-R2GBJEF'. The top right shows the agent's status as 'Online', its ID as '18EAGF016EDC2C505370DE7674A5504F0CC', and ping statistics. Below this are sections for 'Agent properties' (Set Policy, Set update group, Move to group), 'About this agent' (General info, Installation Files Version, Installed Certificates, Scheduled Tasks, Disks & partitions, Environment variables, Installed softw), and specific disk details for 'VMware Virtual NVMe Disk' and 'CD-ROM Disc'.

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.

The screenshot shows the 'Agent management' section of the Viettel ajiant interface. On the left, a sidebar with icons for search, refresh, and other management functions. The main area has a header 'Agent management' and a search bar 'Type to search by queries...'. Below is a table titled 'result(s)' with columns: NAME, STATUS, GROUP, UPDATE GROUP, and LAST PING. The table lists several agents, including 'DESKTOP-R20BIEF' (Online, Default, Release, 29/06/2022 18:23:58), 'Win10x48bcbp3' (Offline, Default, Release, 29/06/2022 17:36:14), and 'N/A' (Offline, N/A, N/A). To the right of the table is a detailed view of the selected agent 'DESKTOP-R20BIEF'. It shows 'Agent properties' with a 'Set Policy' dropdown set to 'full_features_basit', a 'Set update group' dropdown set to 'release', and a 'Move to group' dropdown set to 'default'. Below this are tabs for 'About this agent' (General info, Installation Files Version, Installed Certificates, Scheduled Tasks, Disks & partitions, Environment variables, Installed software), 'System' (ComSpec %SystemRoot%\system32\cmd.exe), 'DriverData' (C:\Windows\System32\Drivers\DriverData), and 'OS' (Windows_NT). Further down are sections for 'Path' (%SystemRoot%\system32\SystemRoot%\SystemRoot\System32\Wbem\%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\%SYSTEMROOT%\Files\Microsoft\VS Code\bin), 'PATHEXT' (.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC), 'PROCESSOR_ARCHITECTURE' (AMD64), 'PSModulePath' (%ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\System32\WindowsPowerShell\v1.0\Modules), 'TEMP' (%SystemRoot%\TEMP), 'TMP' (%SystemRoot%\TEMP), 'USERNAME' (SYSTEM), and 'windir' (%SystemRoot%).

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;

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Localhost_Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhn_n_full_features	3.3.8
N/A	Offline	N/A	N/A	N/A	N/A	N/A	N/A	N/A

- + 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 Multiselect session;

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Localhost_Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhn_n_full_features	3.3.8
N/A	Offline	N/A	N/A	N/A	N/A	N/A	N/A	N/A

- 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.

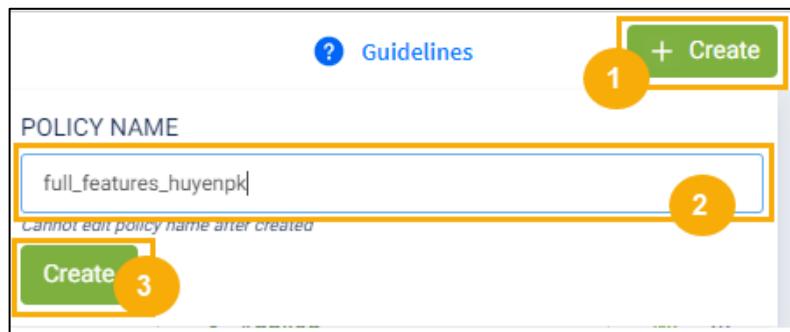
+ 2. If the license expires: the system will automatically disable all features on all devices until the license is renewed, while customers will still see the agent online on the portal.

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:

POLICY NAME	NUMBER OF AGENTS	CREATED TIME	UPDATED TIME	APPLIED TIME	STATUS
default	0	28/01/2019 14:11:52	03/12/2020 11:42:43	03/12/2020 11:42:50	● Applied
full_features	0	09/12/2021 10:20:00	26/05/2022 14:14:25	08/06/2022 13:54:08	● Applied
full_features_khaib	0	13/01/2022 13:49:13	13/01/2022 14:15:50	13/01/2022 14:15:53	● Applied
phula,test	1	14/01/2022 13:17:12	31/03/2022 13:07:30	31/03/2022 13:07:35	● Applied
full_features_v2	0	17/01/2022 14:29:12	08/06/2022 16:02:34	08/06/2022 16:02:37	● Applied
anhn,full_features	1	08/02/2022 15:51:36	08/06/2022 16:19:12	08/06/2022 16:19:14	● Applied
Full_AV	0	01/03/2022 14:36:25	20/05/2022 15:02:30	20/05/2022 15:02:34	● Applied
full_features_macos	0	11/03/2022 18:22:01	18/03/2022 11:29:29	18/03/2022 11:29:32	● Applied
full_features_anhn	0	15/03/2022 15:14:32	25/05/2022 17:50:28	25/05/2022 17:50:31	● Applied
full_features_baolt	0	17/03/2022 15:12:01	09/06/2022 15:32:37	09/06/2022 15:32:40	● Applied

- 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:



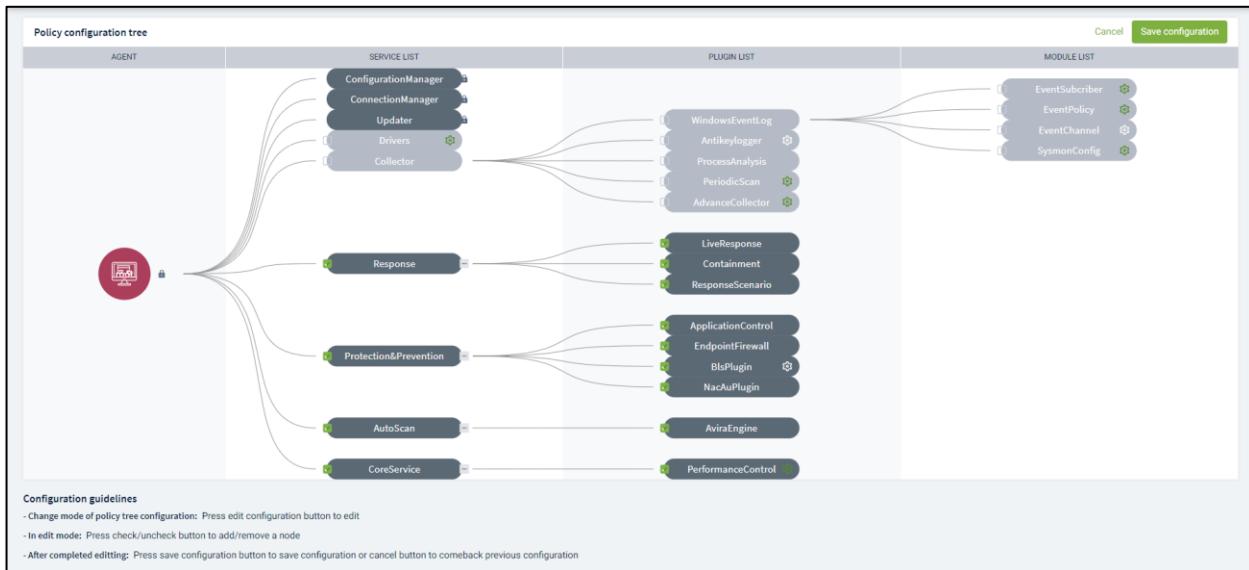
Note: When creating a new policy, the policy name must not duplicate any previously created policies.

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	<ul style="list-style-type: none"> - WindowsEventLog Configuration: Configure log sources to be collected by the Agent + EventSubscriber: specify the log channels to collect Data

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

	Agent to collect sysmon logs: Microsoft-Windows-Sysmon/Operational;
Antikeylogger	<p>Antikeylogger Configuration: This is a SelfRun Plugin of VCS-aJiant, responsible for periodically scanning the entire system to detect any running KeyLoggers if present.</p> <p>Scan Setting: Configure the types of KeyLoggers to be scanned.</p> <p>Requirements:</p> <ul style="list-style-type: none"> - Scan cycle: minimum 1 minute, maximum 180 minutes; - Select at least one type of KeyLogger; <p>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.</p> <p>Requirements: Fill in all fields completely; After completing the entries, remember to “Save” the configuration.</p>
Self-defense	<p>Self Defense Configuration: Add an uninstall protection mechanism for Self Defense;</p> <p>Instructions: Select Choose Drivers > Check Self Defense to enable the Self Defense feature or uncheck to disable it > select Save > select Apply Policy;</p>
Autoscan	<p>Autoscan Configuration: allows users to add additional configurations when scanning for malware.</p> <p>- Requirement: Select Autoscan -> Add new configuration.</p> <p>The new information to be added includes:</p> <ul style="list-style-type: none"> + Version + Description <p>+ Data config for Windows will have a format as follows:</p> <p>Note: For configurations of the automatic or manual malware</p>

	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

- 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.

Clone from policy:
test_sample

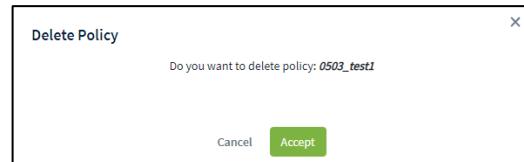
NAME OF POLICY

Enter name of policy...

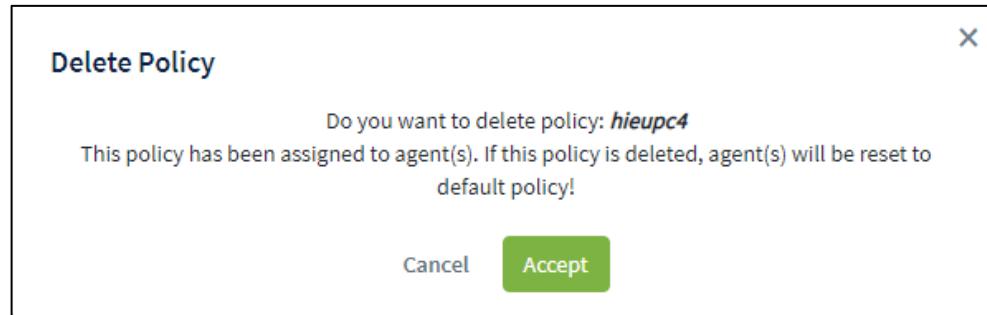
Cannot edit name of policy after create policy

Create

- + 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:

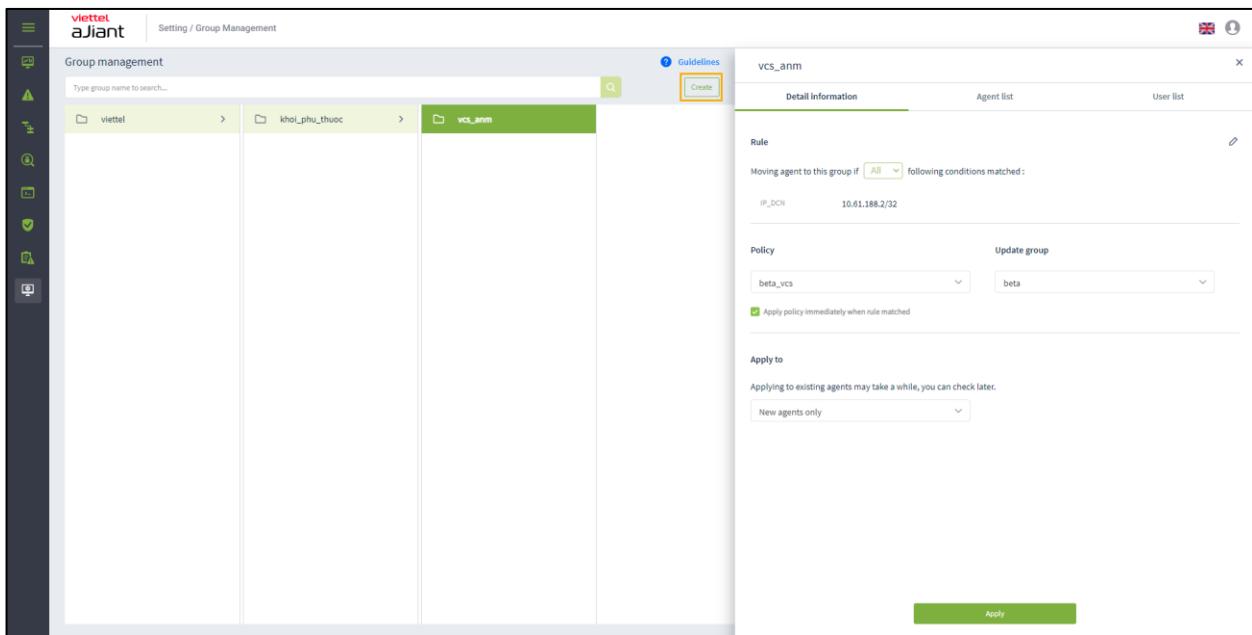
- + User logged in as root group: Can add all Groups;
- + User login belongs to default group: Cannot add new;

+ 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;



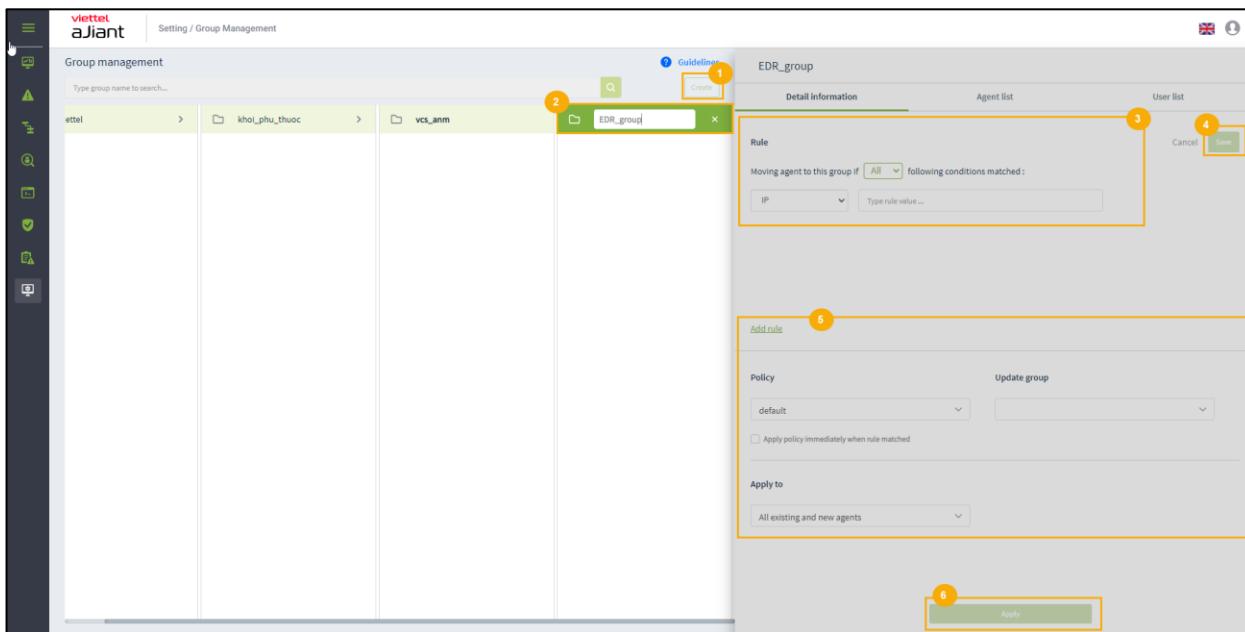
+ If creating a new subgroup within a parent group or a level 1, level 2 group, etc., click on the parent group, then click “Create” on the screen, or hover at the end of the list of groups at the same level and click “Create.”

- 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

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**

Rule

Moving agent to this group if **All** following conditions matched :

IP DCN **10.61.188.2/32**

Add rule

Policy **Update group**

beta_vcs **beta**

Apply policy immediately when rule matched

Apply to

New agents only

Save **Cancel**

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.

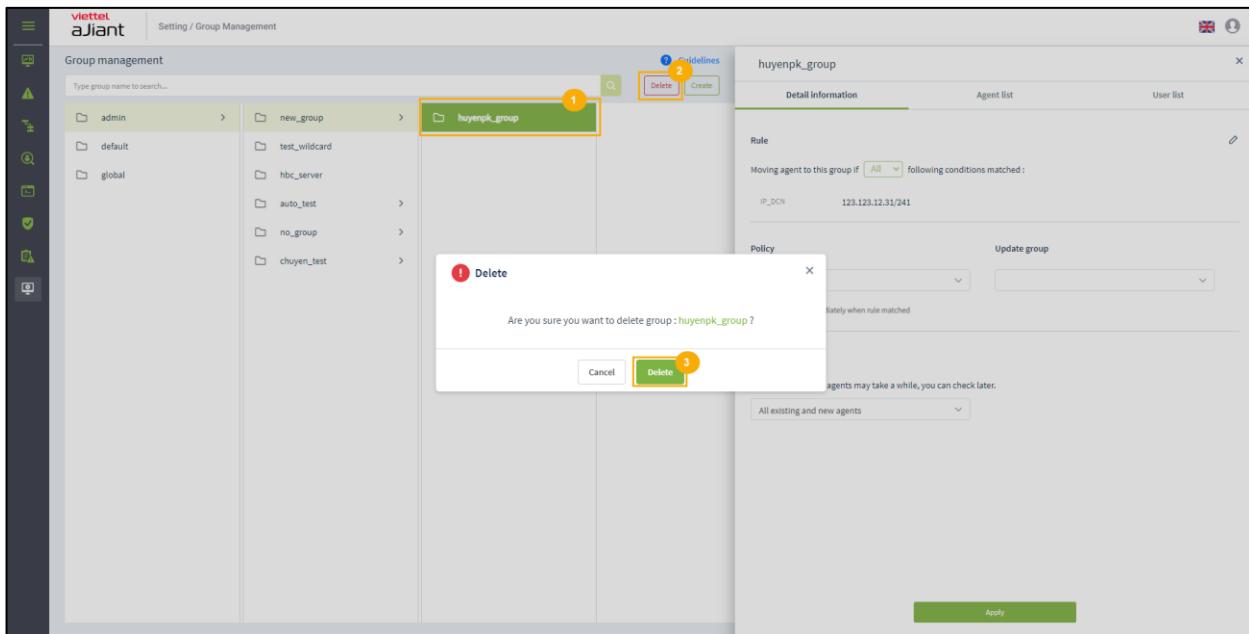
+ In the case where the components of the group have been edited and the Apply button is clicked, the changes will be saved. Additionally, if the "All existing agents" option is selected in the "Apply to" section, the system will scan information for all agents and reassign the group to each agent, then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

vcs_anm

Detail information		Agent list			User list	
50/279 agent(s)		Search agent...				
AGENT ID	HOSTNAME	GROUP	STATUS	POLICY	#	
4AE8D11BFB5037899FD20F5CEDF	ANM-HOANGND31	vcs_anm	● Offline	full_features_with_autoscan_selfdefense		
1B37DBD39D0F632D9F7BEFBE421	ANM-SANGLV11	vcs_anm	● Offline	full_features_with_autoscan_selfdefense		
75E895D48390F5C642FC57AD62C	ANM-THONGND7	vcs_anm	● Offline	full_features_with_autoscan_selfdefense		
1F8AF3B15A9A343F992D3596EBA3	ANM-HOABT21	vcs_anm	● Offline	full_features_with_autoscan_selfdefense		
2FA6F1E3E016C748600CAF0C1A7	ubunbu-18	vcs_anm	● Offline	full_features_3.3.0		
:5CA1E94EC4C99ACE5EDB202FD7E	ANM-ANHNN19	vcs_anm	● Offline	full_features_with_autoscan_selfdefense		
9ACE6C4888F8E1F04428BC8BDD1	IS-LANNT	vcs_anm	● Offline	beta_vcs		
i43E35A30D5CC8EFC65AC7A83EB1	ANM-THANGNM14	vcs_anm	● Offline	full_features_with_autoscan		
A04CF97FF6250F800308CE68352	ANM-DUCDH8	vcs_anm	● Offline	full_features_with_autoscan_selfdefense		

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

NO.	USERNAME	FULLNAME	EMAIL
1	admin	t	
2	alert_viewer	alert_viewer	alert_viewer@ajiant.com
3	anhbd25	t1	
4	anhnn	anhnn@gmail.com	
5	anhnn19	tba	
6	anhvn	anhvn@gmail.com	
7	autotest151	fullname	clint.kris@yahoo.com
8	autotest281	fullname	marjory.ritchie@hotmail.com
9	autotest289	fullname	alec.stamm@gmail.com
10	autotest35	fullname	alicia.lueiwitz@gmail.com
11	autotest362	fullname	mao.huel@hotmail.com
12	autotest419	fullname	rachael.pouros@hotmail.com
13	autotest457	fullname	clyde.grady@gmail.com
14	autotest5	fullname	mckinley.ratke@gmail.com

NO.	USERNAME	FULLNAME	EMAIL
1	iml_edr	iml_edr	iml_edr@ajiant.com
2	is_toanbd	is_toanbd@adf.com	is_toanbd@adf.com
3	khaibt	Trần Bá Khai	khaibt@viettel.com.vn
4	thanhln9	thanhln9	thanhln9@viettel.com.vn

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

NO.	USERNAME	FULLNAME	EMAIL	STATUS
1	anhvn	anhvn	anhvn@gmail.com	● Active
2	autotest107	fullname	jackie.anderson@yahoo.com	● Active
3	autotest11	fullname	sondra.trantow@yahoo.com	● Active

3.6.4 Account Management

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

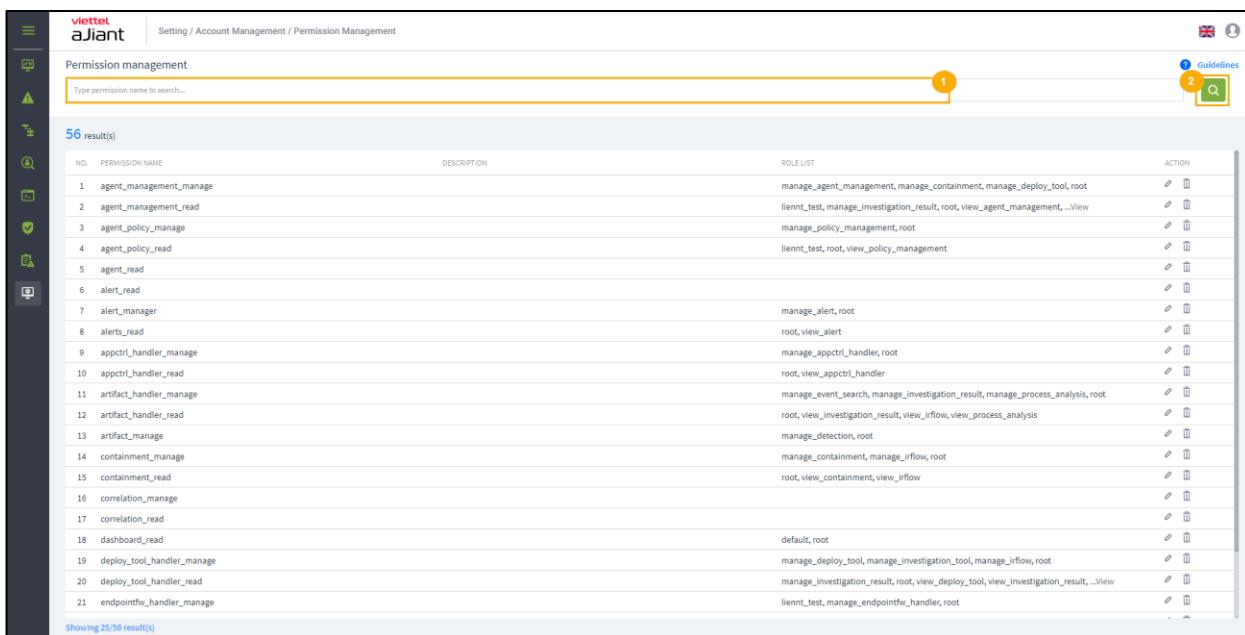
Permission management

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.



NO.	PERMISSION NAME	DESCRIPTION	ROLE LIST	ACTION
1	agent_management_manage		manage_agent_management, manage_containment, manage_deploy_tool, root	 
2	agent_management_read		lennet_test, manage_investigation_result, root, view_agent_management, ...View	 
3	agent_policy_manage		manage_policy_management, root	 
4	agent_policy_read		lennet_test, root, view_policy_management	 
5	agent_read			 
6	alert_read			 
7	alert_manager		manage_alert, root	 
8	alerts_read		root, view_alert	 
9	apctrl_handler_manage		manage_apctrl_handler, root	 
10	apctrl_handler_read		root, view_apctrl_handler	 
11	artifact_handler_manage		manage_event_search, manage_investigation_result, manage_process_analysis, root	 
12	artifact_handler_read		root, view_investigation_result, view_irflow, view_process_analysis	 
13	artifact_manage		manage_detection, root	 
14	containment_manage		manage_containment, manage_irflow, root	 
15	containment_read		root, view_containment, view_irflow	 
16	correlation_manage			 
17	correlation_read			 
18	dashboard_read		default, root	 
19	deploy_tool_handler_manage		manage_deploy_tool, manage_investigation_tool, manage_irflow, root	 
20	deploy_tool_handler_read		manage_investigation_result, root, view_deploy_tool, view_investigation_result, ...View	 
21	endpointfw_handler_manage		lennet_test, manage_endpointfw_handler, root	 

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.

The screenshot shows the 'Role Management' section of the aJiant portal. On the left, a search bar contains the text 'default'. Below it is a list of roles: 'default', 'Hatest', 'hbc_test', 'liennnt_permission', 'liennnt_te123456', 'liennnt_test', 'manage_agent_management', 'manage_alert', and 'manage_apptctr_handler'. The 'root' role is selected and detailed information is shown on the right. The 'Detail Information' tab is active, showing the role name 'root (root)', domain 'root role', and a large list of permissions. The permissions are represented as a grid of small blue buttons, each containing a permission name like 'read', 'containment_read', 'agent_management_manage', etc. A red arrow points from the text 'Double-clicking on a record will display the detailed information of that record.' to the 'root' role detail view on the right.

- 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.

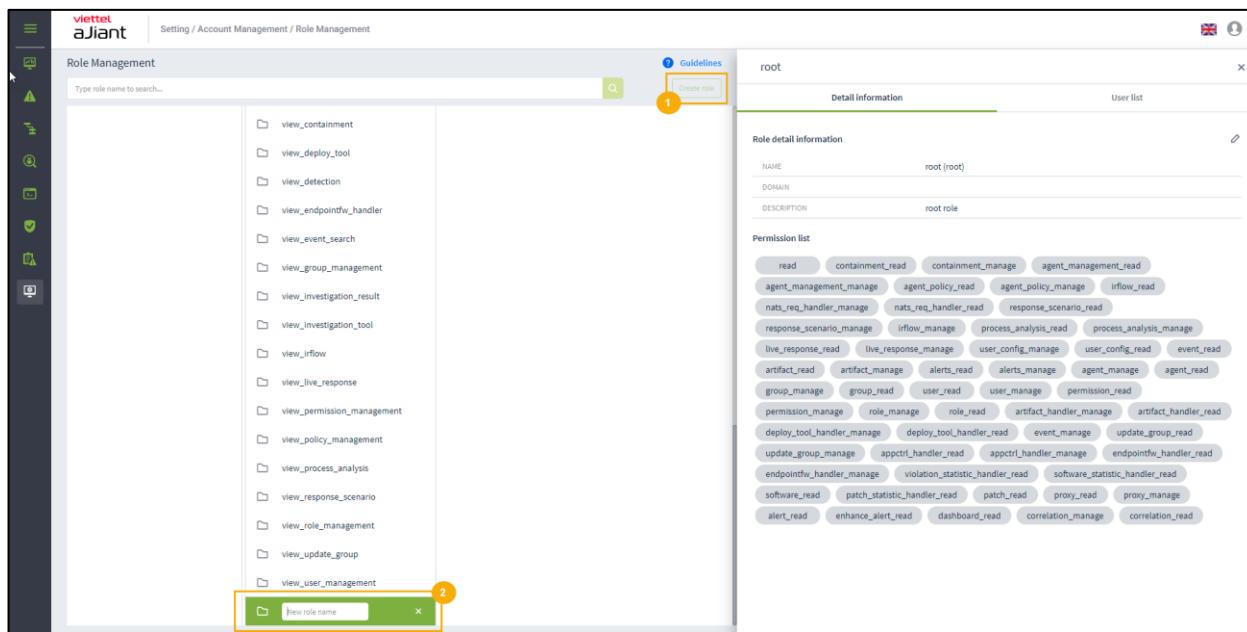
- There are the following methods to create a new role:

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.

view_irflow

Detail information **User list**

Role detail information

NAME: view_irflow (view_irflow)

DOMAIN:

DESCRIPTION: view_irflow

Permission list

irflow_read, containment_read, process_analysis_read, live_response_read, artifact_handler_read, response_scenario_read, deploy_tool_handler_read, event_read

view_live_response

Detail information **User list**

Role detail information

Name: view_live_response

Domain:

Description: view_live_response

Permission list

live_response_read

read

containment_read

containment_manage

agent_management_read

agent_management_manage

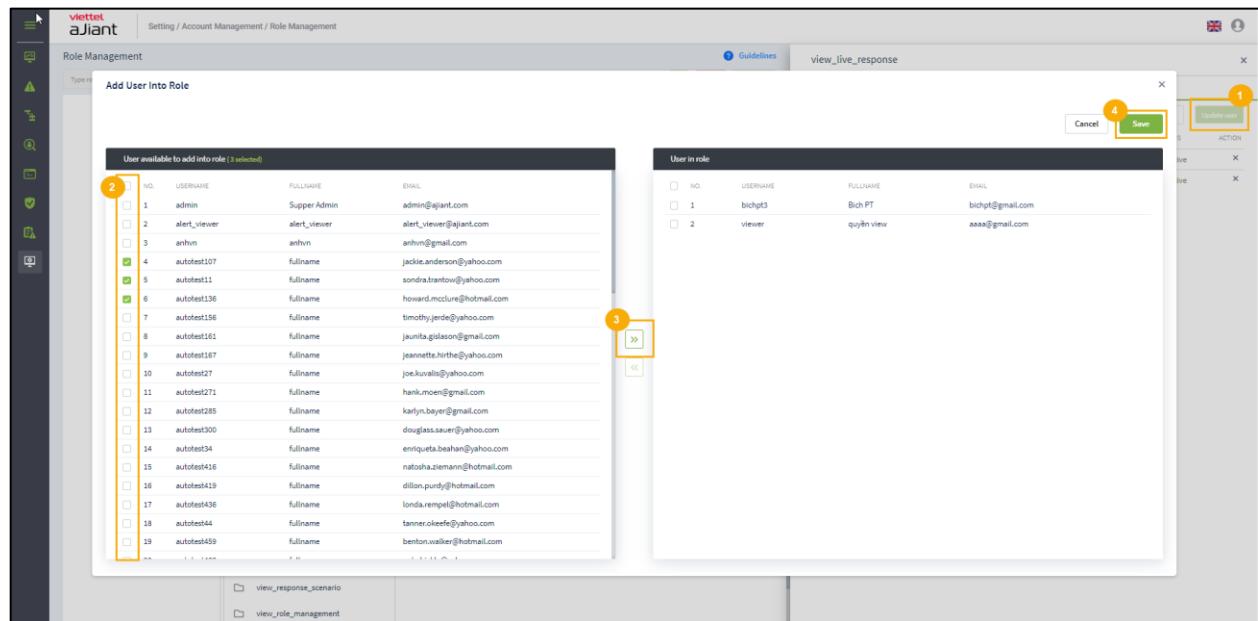
agent_policy_read

- 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;

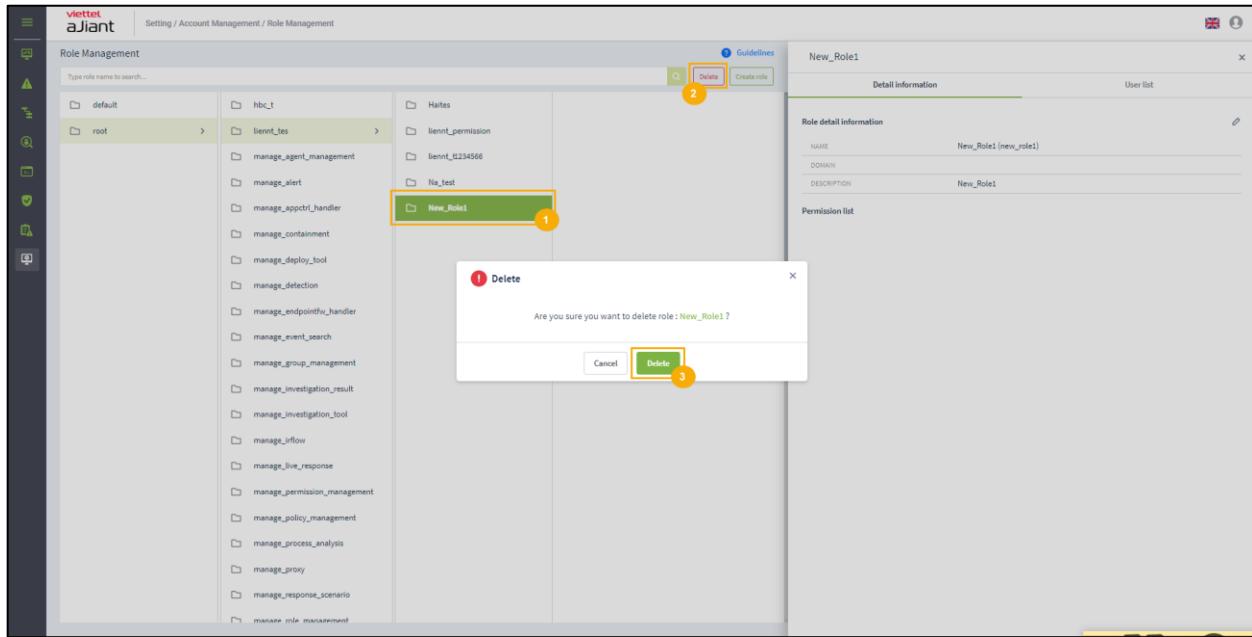
+ User login belongs to default group: Display users belonging only to default;

+ 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;

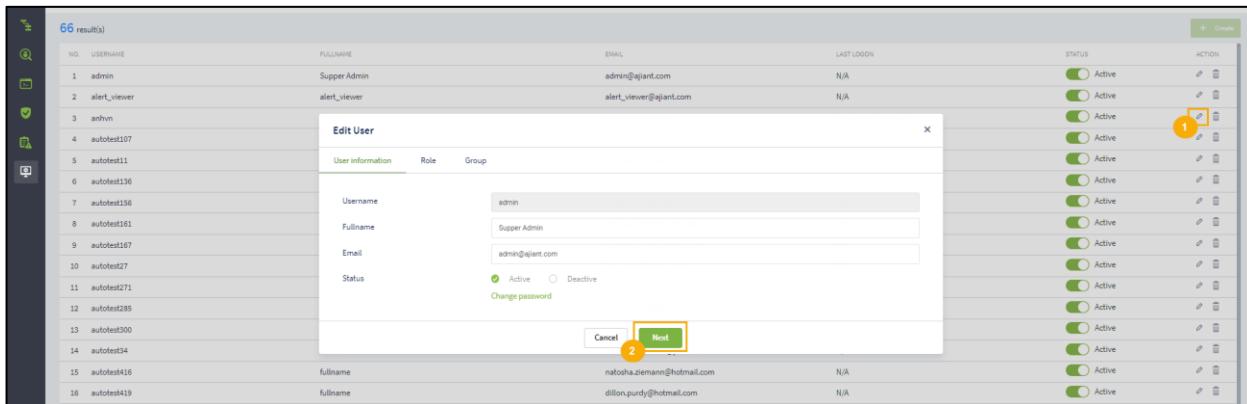
1 – Search for an account: click on the Search textbox > a list of accounts in the system will appear > select the desired account from the list or enter the characters <text> into the textbox to filter the accounts > click “Search” or select the desired account from the filtered list.

NO.	USERNAME	FULLNAME	EMAIL	LAST LOGON	STATUS	ACTION	
1	admin		t	N/A	Active		
2	alert_viewer	alert_viewer	alert_viewer@ajiant.com	N/A	Active		
3	anhbd25		t1	N/A	Active		
4	anhnn		anhnn@gmail.com	N/A	Active		
5	anhnn19		tba	N/A	Active		
6	anhm		anhvn@gmail.com	N/A	Active		
7	autotest151	fullname	clint.kris@yahoo.com	N/A	Active		
8	autotest281	fullname	margory.ritchie@hotmail.com	N/A	Active		
9	autotest289	fullname	alec.stamm@gmail.com	N/A	Active		
10	autotest35	fullname	alicia.luelwitz@gmail.com	N/A	Active		
11	autotest362	fullname	mao.huel@hotmail.com	N/A	Active		

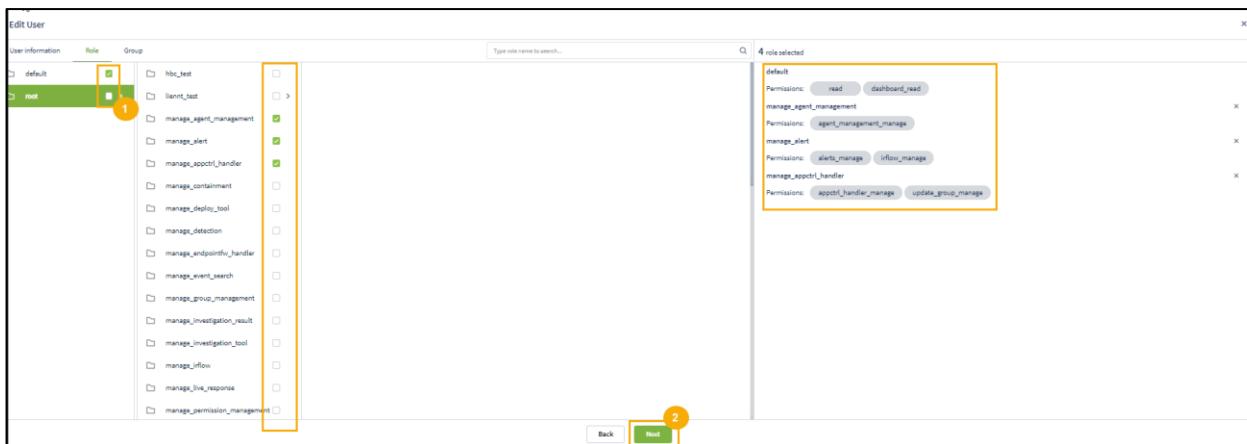
Add a new account: click “Create” > Enter information in the displayed form > click “Next”

- + 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.

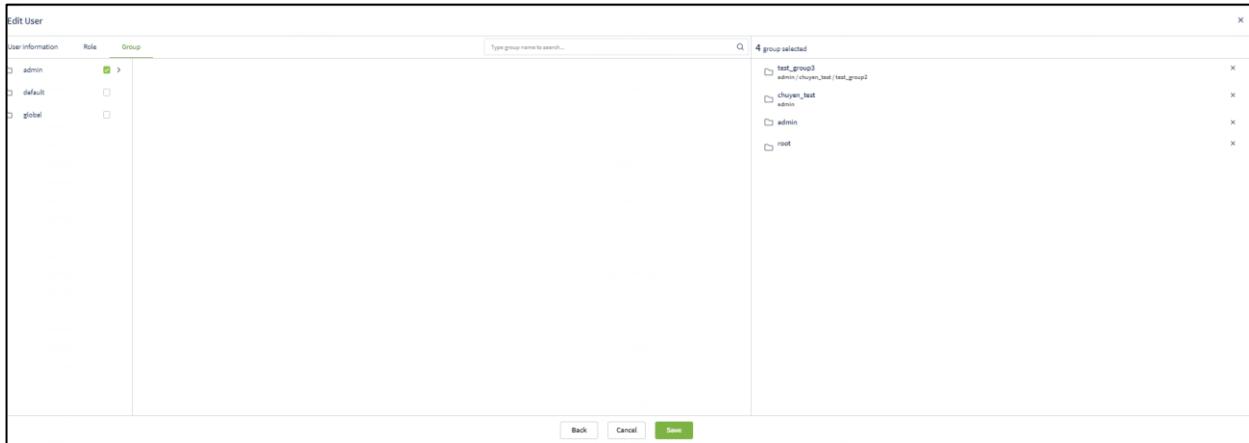


On the Add Role to User screen, you can search for roles similarly to how you search for accounts. After entering search characters into the "Search" textbox, click the Search icon or press Enter to display a list of roles that meet the search criteria.



- + 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;

ID	USERNAME	FULLNAME	EMAIL	LAST LOGIN	STATUS	ACTION
1	admin	Super Admin	admin@ajant.com	N/A	 Active	 
2	alert_viewer	alert_viewer	alert_viewer@ajant.com	N/A	 Active	 
3	anhrm	anhrm	anhrm@gmail.com	29/04/2022 10:44:40	 Active	 
4	autotest107	fullname	jackie.anderson@yahoo.com	N/A	 Active	 
5	autotest111	fullname	sondra.branton@yahoo.com	N/A	 Active	 
6	autotest136	fullname	howard.mcclure@hotmail.com	N/A	 Active	 
7	autotest156	fullname	timothy.jende@yahoo.com	N/A	 Active	 
8	autotest161	fullname	jacinta.gilesone@gmail.com	N/A	 Active	 
9	autotest167	fullname		N/A	 Active	 
10	autotest177	fullname		N/A	 Active	 
11	autotest271	fullname		N/A	 Active	 
12	autotest285	fullname		N/A	 Active	 
13	autotest300	fullname		N/A	 Active	 
14	autotest314	fullname		N/A	 Active	 
15	autotest416	fullname	natalie.ziemann@hotmail.com	N/A	 Active	 
16	autotest429	fullname	dillon.purdy@hotmail.com	N/A	 Active	 

Enable two-factor authentication for the account:

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

kYXRlcGlja2VyljoiRmlyc3QgUGluZylsImtleV90aW1lljoiliwiaW50ZXJ2YWxfdGltZSI6MCwidH... (1) ☆ 🛡 ⟳ 👤 ⬇️ 🔗

国人

thanhln9
My profile
About VCS-aJiant
Sign out

First ping	IP DCN	Policy	
25/11/2021 07:14:51	10.207.26.203	full_features_3.3.0	3.3.37
23/11/2022 08:24:49	10.61.74.206	full_features_3.3.0	3.3.37
20/07/2020 17:24:36	10.230.65.69	full_features_3.3.0_linux	3.3.36
2/01/2023 11:31:19	10.61.1.141	nac_plugin_only	3.3.37
13/08/2020 12:05:38	10.230.246.204	full_features_3.3.0_linux	3.3.36
25/09/2022 20:33:15	192.168.81.44	full_features_3.3.0	3.3.37

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 screenshot shows the 'Edit user' dialog for a user named 'lien'. The 'User information' section includes the username 'lien', full name 'Lien 97', and email 'lien@edr.com'. The 'Roles & groups' section shows three roles: 'default' with permissions 'read', 'dashboard_read'; 'manage_alert' with 'alerts_manage', 'inflow_manage'; and 'view_alert' with 'alerts_read'. The 'Groups' section shows one group 'default'. Two-factor authentication is enabled. The 'Edit user' dialog has 'Cancel' and 'Save' buttons.

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;

Update groups		Packages				
		<input type="text" value="Search"/> <input type="button" value="Search"/>				
8 group(s)						
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhut hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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

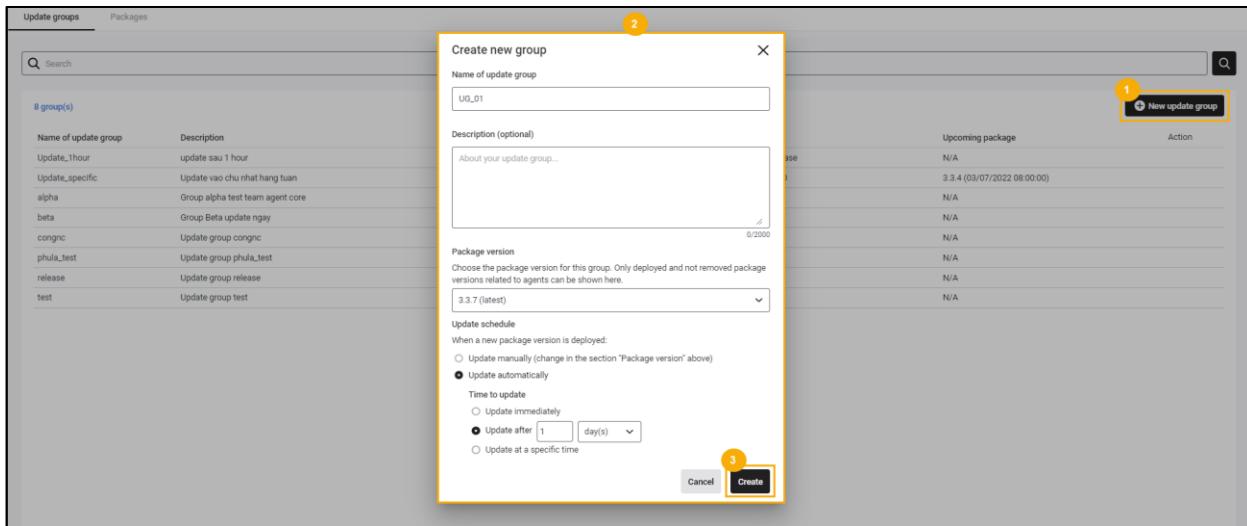
Update groups		Packages				
		<input type="text" value="Search"/> <input type="button" value="Search"/>				
8 group(s)						
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhut hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	5	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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;

Update groups		Packages				
		<input type="text" value="Search"/> <input type="button" value="Search"/>				
8 group(s)						
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhut hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

- 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;

Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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

Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhat hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	5	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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

Edit group detail

Name of update group
Update_1hour
Name contains only letters, numbers, and special characters "-", ".", "*", "

Description (optional)
update sau 1 hour (update)

Package version
Choose the package version for this group. Only deployed and not removed package versions related to agents can be shown here.
3.3.7 (latest)

Update schedule
When a new package version is deployed:
 Update manually (change in the section "Package version" above)
 Update automatically
 Time to update
 Update immediately
 Update after hour(s)
 Update at a specific time

Cancel **Apply**

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;

Update groups		Packages				
		<input type="text" value="Search"/> <input type="button" value="Search"/>				
8 group(s)						
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhut hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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

Update groups		Packages				
		<input type="text" value="Search"/> <input type="button" value="Search"/>				
8 group(s)						
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhut hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	5	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

- 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.

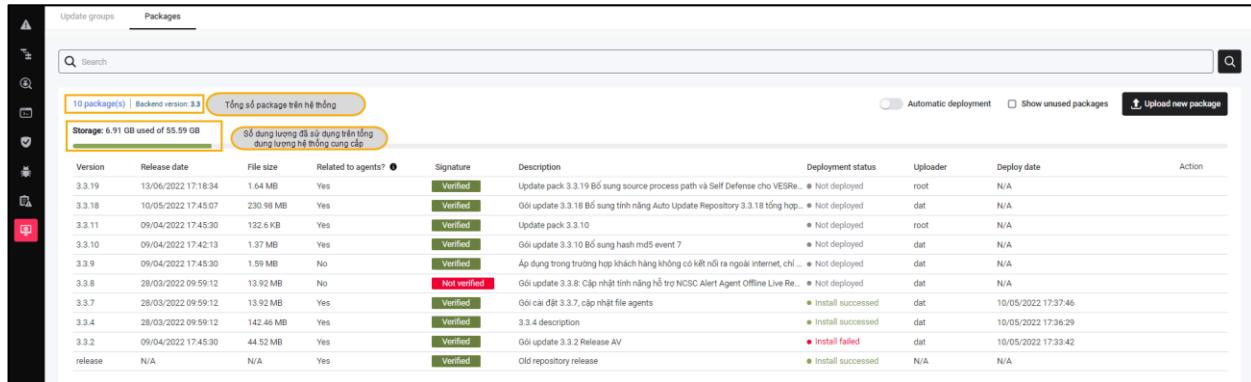
Update groups		Packages				
		<input type="text" value="Search"/> <input type="button" value="Search"/>				
8 group(s)						
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vao chu nhut hang tuan	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnc	Update group congnc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	5	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

Packages update

1 – Searching for packages:

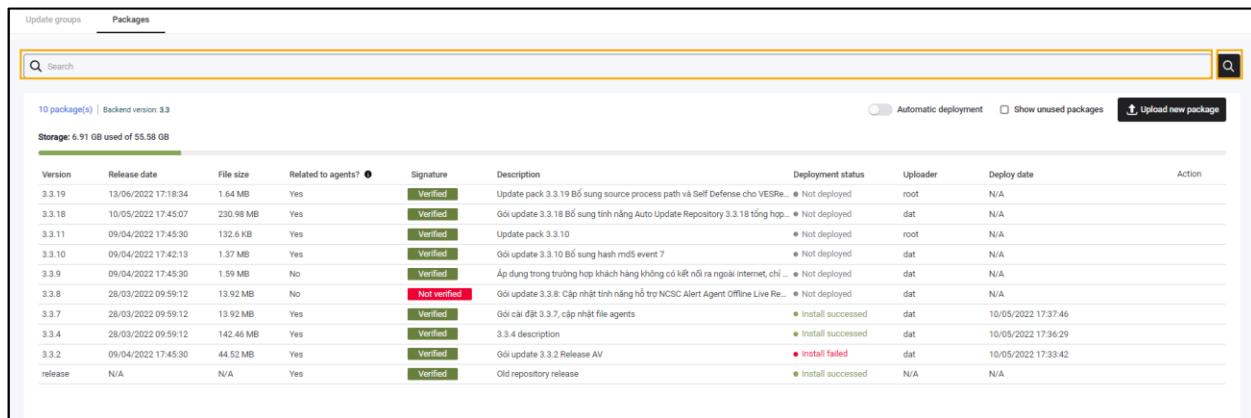
- Log in to the Portal using the provided account credentials;

- 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;



Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	● Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chí...	● Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

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



Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	● Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chí...	● Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

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;

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/05/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:36	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	● Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, ch...	● Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

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

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/05/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:36	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	● Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, ch...	● Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

- Select upload package;

10 package(s) | Backend version: 3.3

Storage: 6.91 GB used of 55.58 GB

Automatic deployment Show unused packages Upload new package

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified		● Not deployed	root	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified		● Not deployed	root	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified		● Not deployed	root	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7: cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

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

10 package(s) | Backend version: 3.3

Storage: 6.91 GB used of 55.59 GB

Automatic deployment Show unused packages Upload new package

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event ?	● Not deployed	root	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ ...	● Not deployed	root	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	root	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7: cập nhật file agents	● Install succeeded	root	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	root	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	root	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

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;

10 package(s) | Backend version: 3.3

Storage: 6.91 GB used of 55.59 GB

Số dung lượng đã sử dụng trên tổng dung lượng хранилище

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	● Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chí...	● Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

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

10 package(s) | Backend version: 3.3

Storage: 6.91 GB used of 55.58 GB

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	● Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chí...	● Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

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

10 package(s) | Backend version: 3.3

Storage: 6.91 GB used of 55.58 GB

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	● Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chí...	● Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

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;

Update groups Packages

Search

10 package(s) Backend version: 3.3

Tổng số package trên hệ thống

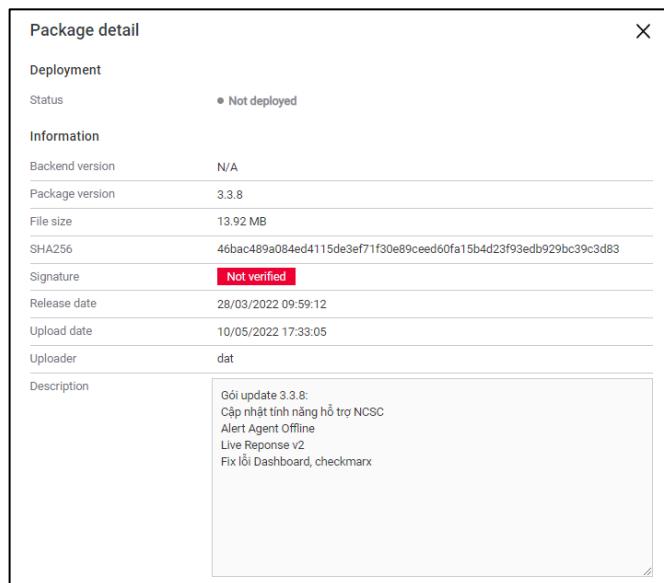
Storage: 6.91 GB used of 55.59 GB

Số dung lượng đã sử dụng trên tổng dung lượng hệ thống cung cấp

Automatic deployment Show unused packages Upload new package

Version	Release date	File size	Related to agents	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VSPRE...	● Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	● Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	● Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event ?	● Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ ...	● Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	● Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	● Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	● Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	● Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	● Install succeeded	N/A	N/A	

- 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

Rank	Rule/Group	Description
1	Top baseline violated rule	Quy định cấu hình chính sách mật khẩu
2	Top baseline violated rule	Quy định tự động khóa màn hình sau 1 phút
3	Top baseline violated rule	Quy định máy tính phải join domain, và sử dụng tài khoản domain để đăng nhập máy tính
4	Top baseline violated rule	Quy định nghiêm cấm lưu trữ mật khẩu trên trình duyệt
1	Top baseline violated group	1. ma_test
2	Top baseline violated group	2. ma_test
3	Top baseline violated group	3. ma_test
4	Top baseline violated group	4. ma_test
5	Top baseline violated group	5. ma_test
6	Top baseline violated group	6. ma_test
7	Top baseline violated group	7. ma_test
8	Top baseline violated group	8. ma_test
9	Top baseline violated group	9. ma_test
10	Top baseline violated group	10. ma_test

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	<p>The regulations include the following rules:</p> <ul style="list-style-type: none"> + 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



GROUP	ONLINE IN DAY	ONLINE IN 30 DAYS RECENTLY	RESOLVED	UNRESOLVED	VIOLATION AGENT	VIOLATION RULE
na_test	0 (0%)	0	0 (0%)	1 (100%)	1 (0%)	1

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;

VIOLATION TYPE	RESOLVED	UNRESOLVED
Quy định cấu hình chính sách mật khẩu	0 (0%)	1 (100%)

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).

The screenshot shows the 'Violation Statistic' page. On the left, there is a sidebar with a tree view of units: 'root' (TENANT_nsm.com, TENANT_viettel.com.vn), 'global' (TENANT_edr.com), 'admin', and 'default'. The main area shows a table with a single row for 'na_test'. The table columns are 'Violation type' (Group), 'GROUP' (na_test), 'ONLINE IN DAY' (0 (0%)), 'ONLINE IN 30 DAYS RECENTLY' (0), and 'RESOLVED' (Not resolved yet). To the right of the table is a 'Violation information' panel with a 'Violation rule' section showing 'WIN7X64-A-PC | E7240263DA88951A8B0CD78E201FDB966269E3C2' and a 'Violation agent' section showing '1 violation'. Below this is a 'Hide' button. To the right of the table is a 'Detail information' panel with sections for 'AGENT' (WIN7X64-A-PC), 'AGENT ID' (E7240263DA88951A8B0CD78E201FDB966269E3C2), 'IP ADDRESS' (N/A), 'DOMAIN' (na_test), 'GROUP' (na_test), 'RESOLVED' (Not yet), and 'DETAIL' (Quy định cấu hình chính sách mật khẩu). The 'DETAIL' section includes 'DESCRIPTION' (N/A), 'TIME' (09/5/22 22:09/2022), and 'CONTENT' (Windows password policy configuration: {"min_password_len": 0, "enable_password_complex": 0, "password_history": 0}).

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;

The screenshot shows the 'Violation Statistic' page with a simplified view. The main table now includes a 'Violation rule' column, which for 'na_test' shows the full rule text: 'Quy định cấu hình chính sách mật khẩu'.

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 screenshot shows the 'Software statistic' section of the BLS interface. On the left, there is a tree view of system units: 'root' (selected), 'TENANT_viettel.com.vn', 'global', 'TENANT_edr.com', 'admin', and 'default'. A yellow circle labeled '1' is on the 'root' node. In the center, there is a table showing software statistics. The table has columns: SOFTWARE NAME, NUMBER OF AGENTS, and NUMBER OF GROUPS. One row is visible: 'Google Chrome' with 1 agent and 1 group. A yellow circle labeled '2' is on the 'Google Chrome' row. At the top, there are search bars for 'Search for group...' and 'Search for software...', a dropdown for 'Installed', and a date range 'Last 30 days'. A yellow circle labeled '3' is on the 'Last 30 days' button. At the bottom right, there is a 'Export to excel' button.

SOFTWARE NAME	NUMBER OF AGENTS	NUMBER OF GROUPS
Google Chrome	1	1
Version 102.0.5005.115	1	1

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;

Software statistic

Search for group... Search for software... Installed Last 30 days Export to excel

SOFTWARE NAME	NUMBER OF AGENTS	NUMBER OF GROUPS
Google Chrome	1	1
Version 102.0.5005.115	1	1

- 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;

Software statistic (installed) - Google Chrome

group_bichpt3 (display 1/1 agent)

WIN7X64-A-PC | E72402630A8B051ABBD78E201FDB946269E3C2
- Version 102.0.5005.115

- 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);

Software statistic (installed) - Google Chrome

group_bichpt3 (display 1/1 agent)

WIN7X64-A-PC | E72402630A8B051ABBD78E201FDB946269E3C2
- Version 102.0.5005.115

Agent information	
AGENT ID	E72402630A8B051ABBD78E201FDB946269E3C2
GROUP	group_bichpt3
DOMAIN	
IP ADDRESS	10.0.2.15 127.0.0.1
AGENT NAME	Win7x64-A-PC

Software information

SOFTWARE	VERSION
Google Chrome	- Version 102.0.5005.115

[Software list in computer](#)

- 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.

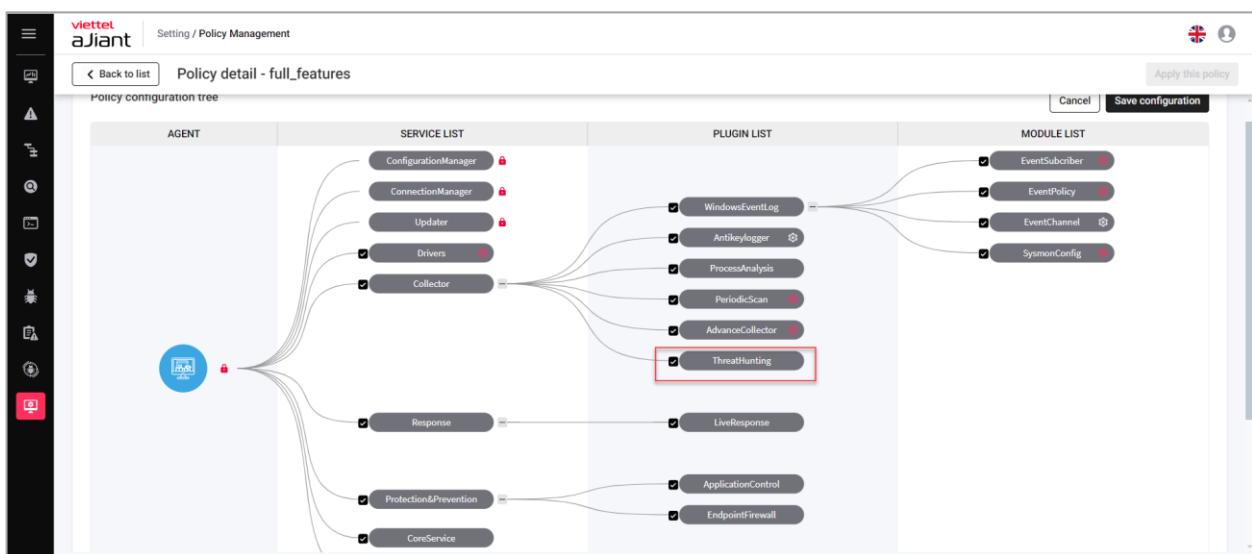
Export: Select Export: The system will download an Export file containing data identical to what is currently displayed on the screen.

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...

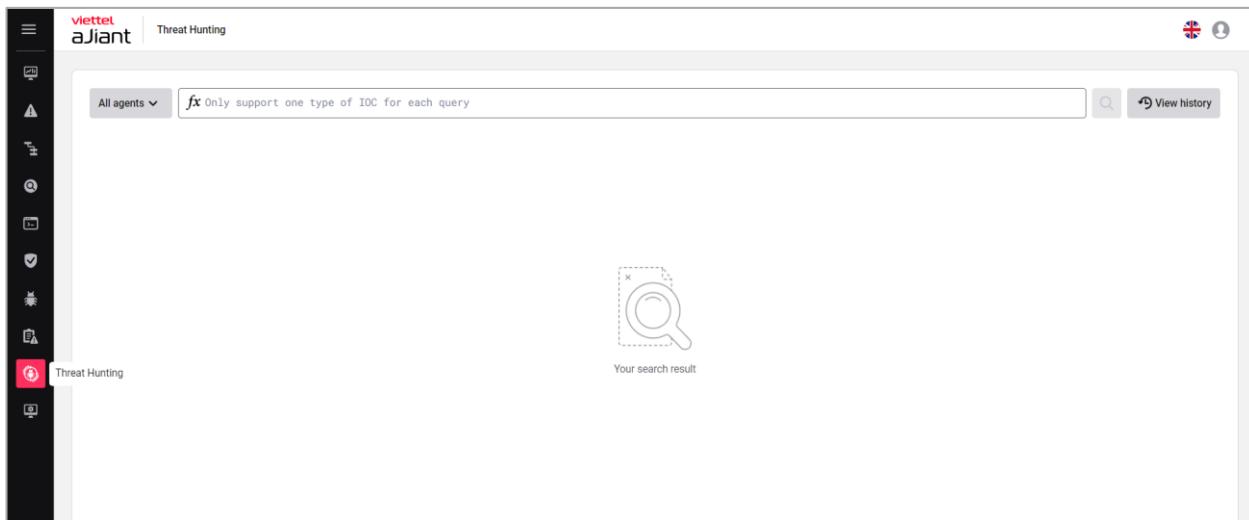
3.8.1 Enable/disable policy

- 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.

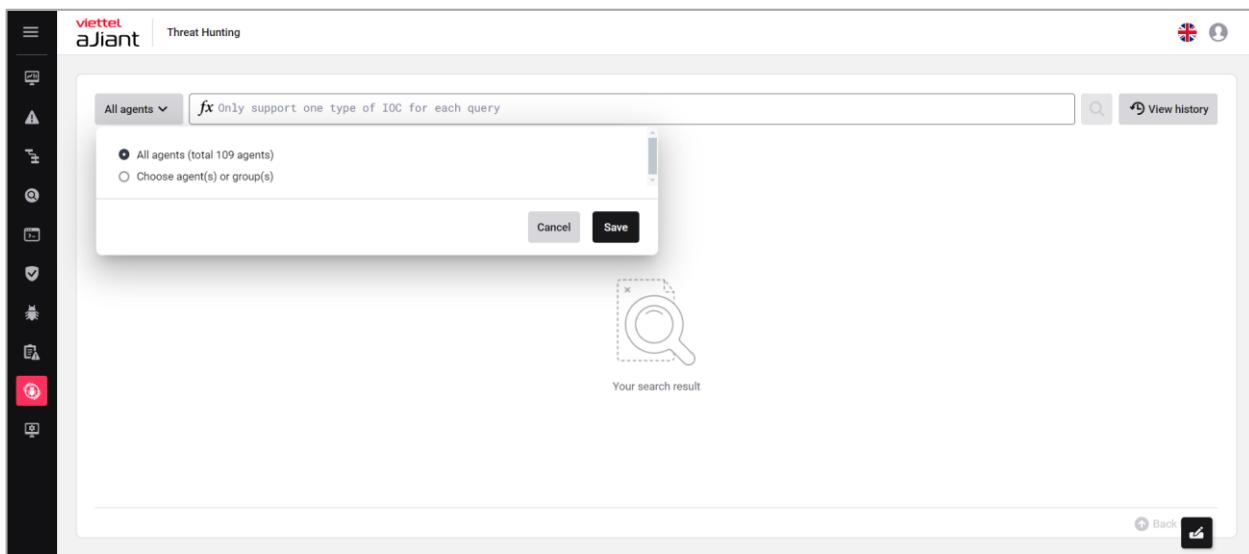


3.8.2 Search by agents/groups

- On the menu, select Threat Hunting.



- Allow admin to search for IOCs by agents/groups.
 - o Allow searching across all agents (All agents)
 - o 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.
 - o Total agent: Total number of agents performing the search
 - o In-process: Search in progress
 - o Success: Search successful
 - o Fail: Search failed

Threat Hunting

All agents

Searching process (93%)

Total agents: 108, In process: 7, Success: 0, Fail: 101

View report

Showing 0 of 0 result(s)

Users(0) File (0) Registry(0) Network(0) Memory(0) Process(0) DLL(0)

Computer Name Agent ID User name IP Admin permission Last log on Password last set

Export to Excel

Back

3.9.3.1.2. Search result details

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

Threat Hunting

All agents

Search completed (100%)

Total agents: 108, In process: 0, Success: 7, Fail: 101

View report

Showing 7 of 7 result(s)

File (7)

Users(0) File (7) Registry(0) Network(0) Memory(0) Process(0) DLL(0)

Computer Name	Agent ID	IP	File Name	File path	File hash SHA256	File created time	Last modified time	IOC det...
Win10x86_bichpt31	676181C52CA...	192.168.195.179	ajiant.log	C:\ProgramData\ajiant.log	9E18963E445C6DC1...	04/09/2024 14:37:56	21/11/2024 09:49:06	17/12/2...
11-Windowspbich	853DCA6465B...	192.168.195.135	ajiant.db	C:\Program Files\Ajiant\ajiant.db	5BAFD36A0FF0DEC1...	12/12/2024 14:58:57	12/12/2024 14:58:57	17/12/2...
Admin-PC	466167E9E8D0...	192.168.6.42	ajiant.db	C:\Program Files\Ajiant\ajiant.db	CCD1D6A3DF84F962...	15/11/2024 15:33:17	15/11/2024 15:33:17	17/12/2...
EDR_Test03	2903CE7FDBF2...	192.168.255.1,192.16...	ajiant.db	C:\Program Files\Ajiant\ajiant.db	2005C2DFD5CF120D...	06/08/2024 02:38:53	16/12/2024 19:00:22	17/12/2...

Export to Excel

Back

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:
 - o The system will stop searching.
 - o 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.

The screenshot shows the Threat Hunting interface. On the left, a sidebar has icons for Threat Hunting, Threat Intelligence, and Threat Response. The main area shows a search bar with 'fx file_name ~ "Ajiant"'. Below it, a progress bar indicates 'Search completed (100%)' with 'Total agents: 108, In process: 0, Success: 7, Fail: 101'. A table below shows 7 results for 'File (7)'. On the right, a modal window titled 'View report - file_name ~ "Ajiant"' displays a table of 7 results with columns: Computer name, Agent ID, IP, IOCs found, IOCs search status, and Fail reason. The table data is as follows:

Computer name	Agent ID	IP	IOCs found	IOCs search status	Fail reason
Win10x86_bichpt31	6761B1C52CAACD436...	192.168.19...	Found	Success	N/A
11-Windowspptbich	853DCA6465BDD15A8...	192.168.19...	Found	Success	N/A
Admin-PC	466167E9E8003D67EE...	192.168.6.42	Found	Success	N/A
EDR_Test03	2903CE7FDBF26E791F...	192.168.25...	Found	Success	N/A
ANM-HUYENNT	C62B97D117C0F552A4...	192.168.18...	Found	Success	N/A
ANM-ANHNV187	66FD1C43EAC5D0A146...	192.168.19...	Found	Success	N/A
DESKTOP-RBEIJFA	5AAE5F48F575F...	192.168.15...	Found	Success	N/A

- 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:
 - o Computer name
 - o Agent ID
 - o IP
 - o IOCs found: Whether any IOCs were found based on the user's query
 - o IOCs search status: Status of IOC search on the agent
 - o Fail reason: Detailed reason for search failure

View report - file_name ~ "Ajiant"

fx Search by agent...

Showing 50 of 108 result(s)

Export to Excel

Computer name	Agent ID	IP	IOCs found	IOCs search status	Fail reason
Win10x86_bichpt31	676181C52CAACD43...	192.168.19...	Found	● Success	N/A
11-Windowsptbich	853DCA6465BDD15A...	192.168.19...	Found	● Success	N/A
Admin-PC	466167E9E8D03D67EE...	192.168.6.42	Found	● Success	N/A
EDR_Test03	2903CE7FDBF26E791F...	192.168.25...	Found	● Success	N/A
ANM-HUENNT	C62B97D117C0F552A4...	192.168.18...	Found	● Success	N/A
ANM-ANHNV187	66FD1C43EAC5DA146...	192.168.19...	Found	● Success	N/A
DESKTOP-RBEIJFA	F92185AAE5F48F575F...	192.168.15...	Found	● Success	N/A
WinSrv2016	C877C486C743B797B9...	192.168.18...	N/A	● Failed	The policy has been ..
Win10x64	88C51186AE9CAF4F5...	192.168.13...	N/A	● Failed	The policy has been ..
Win10x64_edr03	91E1D567010025848D...	192.168.25...	N/A	● Failed	The policy has been ..
DESKTOP-6KRVVQ2	1E6AF8040B8A1AF54C...	192.168.6.6...	N/A	● Failed	The policy has been ..
vtt_huyenmy01	CD9F6C4984FA99F2ED...	192.168.19...	N/A	● Failed	The policy has been ..
Win10x64	78AE3983BC1D6F98F...	192.168.25...	N/A	● Failed	The policy has been ..

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

View report - file_name ~ "Ajiant"

fx Search by agent...

Showing 50 of 108 result(s)

Export to Excel

Computer name	Agent ID	IP	IOCs found	IOCs search status	Fail reason
Win10x86_bichpt31	676181C52CAACD43...	192.168.19...	Found	● Success	N/A
11-Windowsptbich	853DCA6465BDD15A...	192.168.19...	Found	● Success	N/A
Admin-PC	466167E9E8D03D67EE...	192.168.6.42	Found	● Success	N/A
EDR_Test03	2903CE7FDBF26E791F...	192.168.25...	Found	● Success	N/A
ANM-HUENNT	C62B97D117C0F552A4...	192.168.18...	Found	● Success	N/A
ANM-ANHNV187	66FD1C43EAC5DA146...	192.168.19...	Found	● Success	N/A
DESKTOP-RBEIJFA	F92185AAE5F48F575F...	192.168.15...	Found	● Success	N/A
WinSrv2016	C877C486C743B797B9...	192.168.18...	N/A	● Failed	The policy has been ..
Win10x64	88C51186AE9CAF4F5...	192.168.13...	N/A	● Failed	The policy has been ..
Win10x64_edr03	91E1D567010025848D...	192.168.25...	N/A	● Failed	The policy has been ..
DESKTOP-6KRVVQ2	1E6AF8040B8A1AF54C...	192.168.6.6...	N/A	● Failed	The policy has been ..
vtt_huyenmy01	CD9F6C4984FA99F2ED...	192.168.19...	N/A	● Failed	The policy has been ..
Win10x64	78AE3983BC1D6F98F...	192.168.25...	N/A	● Failed	The policy has been ..

3.9.3.1.6. Download search results

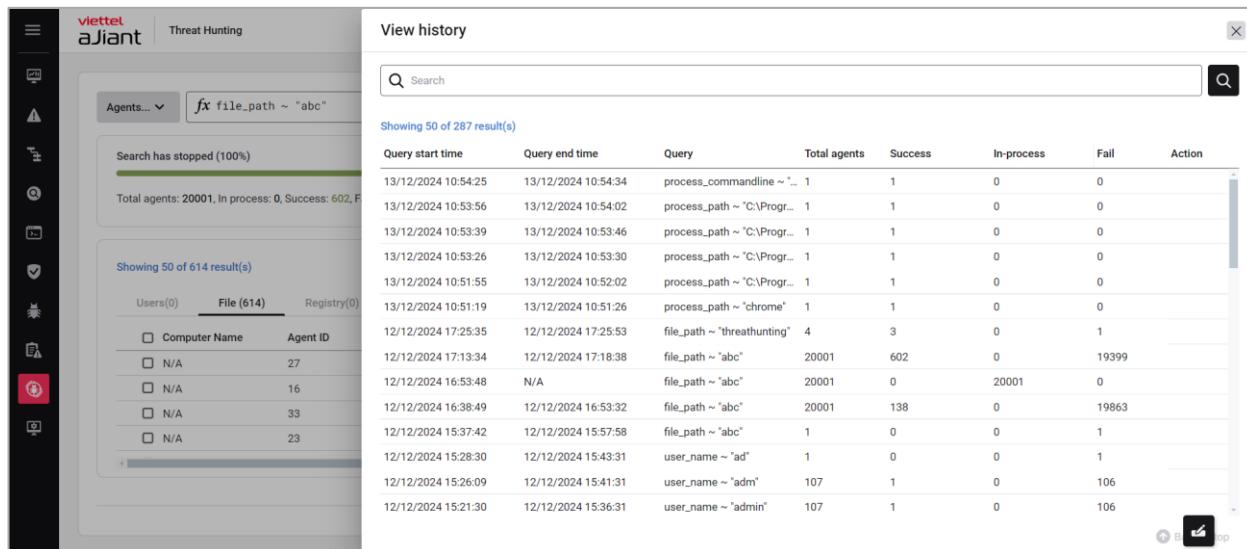
- Allow users to download IOC search results on the agent machine.
- Support for downloading Excel files

Computer Name	Agent ID	IP	File Name	File path	File hash SHA256	File created time	Last modified time	IOC detected time	
Win10x86_bichpt31	676181C52CA...	192.168.195.179	ajiant.log	C:\ProgramData\ajiant.log	9E18963E445C6DC1A...	04/09/2024 14:37:56	21/11/2024 09:49:06	17/12/2024 10:42:57	
11-Windowsptbich	853DCA6465B...	192.168.195.135	ajiant.db	C:\Program Files\Ajiant\ajiant.db	5BAFD36A0FF0DEC1...	12/12/2024 14:58:57	12/12/2024 14:58:57	17/12/2024 10:42:54	
Admin-PC	466167E9E8D0...	192.168.6.42	ajiant.db	C:\Program Files\Ajiant\ajiant.db	CCD1D6A3DF84F962...	15/11/2024 15:33:17	15/11/2024 15:33:17	17/12/2024 10:44:01	
EDR_Test03	2903CE7FDBF2...	192.168.255.1,192.16...	ajiant.db	C:\Program Files\Ajiant\ajiant.db	2005C2DF50F120D...	06/08/2024 02:38:53	16/12/2024 19:00:22	17/12/2024 10:45:20	
ANM-HUYENNNT	C62B97D117C0...	192.168.187.128	ajiant.db	C:\Program Files\Ajiant\ajiant.db	FCD24FF69664D1E6F...	17/09/2024 15:58:52	19/11/2024 15:31:07	17/12/2024 10:44:22	
ANM-ANHNV187	66FD1C43EAC...	192.168.190.1,192.16...	ajiant.db	C:\Program Files\Ajiant\ajiant.db	CCD1D6A3DF84F962...	06/12/2024 15:26:22	06/12/2024 15:26:22	17/12/2024 10:45:22	

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

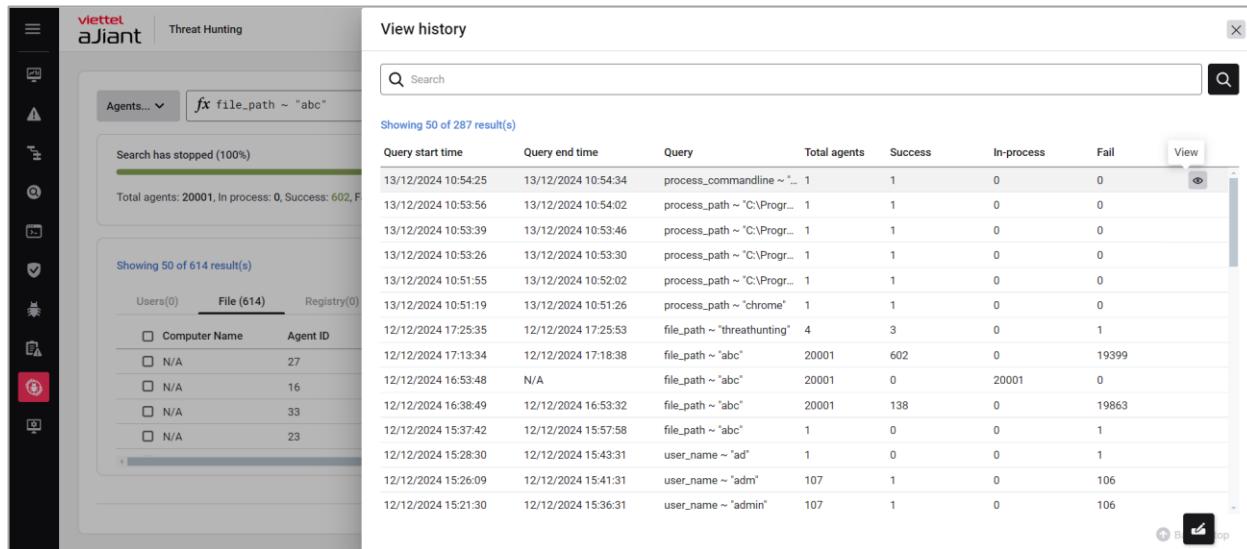


The screenshot shows the Threat Hunting interface with a search history table. The table has columns: Query start time, Query end time, Query, Total agents, Success, In-process, Fail, and Action. The table shows 50 of 287 results, with the first few rows including:

Query start time	Query end time	Query	Total agents	Success	In-process	Fail	Action
13/12/2024 10:54:25	13/12/2024 10:54:34	process_commandline ~ "... 1	1	1	0	0	
13/12/2024 10:53:56	13/12/2024 10:54:02	process_path ~ "C:\Progr..." 1	1	1	0	0	
13/12/2024 10:53:39	13/12/2024 10:53:46	process_path ~ "C:\Progr..." 1	1	1	0	0	
13/12/2024 10:53:26	13/12/2024 10:53:30	process_path ~ "C:\Progr..." 1	1	1	0	0	
13/12/2024 10:51:55	13/12/2024 10:52:02	process_path ~ "C:\Progr..." 1	1	1	0	0	

View detailed query history

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



The screenshot shows the Threat Hunting interface with a search history table. The table has columns: Query start time, Query end time, Query, Total agents, Success, In-process, Fail, and View. The table shows 50 of 287 results, with the first few rows including:

Query start time	Query end time	Query	Total agents	Success	In-process	Fail	View
13/12/2024 10:54:25	13/12/2024 10:54:34	process_commandline ~ "... 1	1	1	0	0	
13/12/2024 10:53:56	13/12/2024 10:54:02	process_path ~ "C:\Progr..." 1	1	1	0	0	
13/12/2024 10:53:39	13/12/2024 10:53:46	process_path ~ "C:\Progr..." 1	1	1	0	0	
13/12/2024 10:53:26	13/12/2024 10:53:30	process_path ~ "C:\Progr..." 1	1	1	0	0	
13/12/2024 10:51:55	13/12/2024 10:52:02	process_path ~ "C:\Progr..." 1	1	1	0	0	

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

The screenshot shows a search results page for a specific process commandline. The search bar at the top contains the query: `fx process_commandline ~ "Ajiant\VESUpdater.exe"`. The search results table has the following columns: Computer Name, Agent ID, IP, Parent Process Path, Parent Process ID, Parent Commandline, Process path, Process ID, and File size. One result is listed:

Computer Name	Agent ID	IP	Parent Process Path	Parent Process ID	Parent Commandline	Process path	Process ID	File size
11-Windowspbtich	853DCA6465BDD15...	192.168.195.135	C:\Program Files\Ajiant\VESSvc.exe	2204	"C:\Program Files\Aj...	C:\Program Files\Ajiant\VESUp...	3104	Viette

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;

The screenshot shows a search results table with the following columns: UPDATED TIME, PRIORITY, NAME, TAG, CATEGORY, SUB CATEGORY, CREATOR, RULE TYPE, OPTIONAL TYPE, and STATUS. The search bar at the top contains 'ModifyRegistry'. The results are as follows:

UPDATED TIME	PRIORITY	NAME	TAG	CATEGORY	SUB CATEGORY	CREATOR	RULE TYPE	OPTIONAL TYPE	STATUS
22/06/2022 18:12:19	1	T1112_ModifyRegistry		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Undeployed

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

The screenshot shows a search results table with the following columns: UPDATED TIME, PRIORITY, NAME, TAG, CATEGORY, SUB CATEGORY, CREATOR, RULE TYPE, OPTIONAL TYPE, and STATUS. The search bar at the top contains 'T1112_ModifyRegistry'. The results are as follows:

UPDATED TIME	PRIORITY	NAME	TAG	CATEGORY	SUB CATEGORY	CREATOR	RULE TYPE	OPTIONAL TYPE	STATUS
22/06/2022 18:12:19	1	T1112_ModifyRegistry		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Undeployed

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

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

The screenshot shows a search results table with the following columns: UPDATED TIME, PRIORITY, NAME, TAG, CATEGORY, SUB CATEGORY, CREATOR, RULE TYPE, OPTIONAL TYPE, and STATUS. The search bar at the top contains 'T1112_ModifyRegistry'. The results are as follows:

UPDATED TIME	PRIORITY	NAME	TAG	CATEGORY	SUB CATEGORY	CREATOR	RULE TYPE	OPTIONAL TYPE	STATUS
22/06/2022 18:12:19	1	T1112_ModifyRegistry		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:04:48	1	T1059_005_VisualBasic		Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Undeployed

Category filters are applied: Windows, Policy, Exploit, Malware, and Suspicious Behaviour. The 'Apply' button is highlighted.

- 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

1 Selected

UPDATED TIME	PRIORITY	NAME	CATEGORY	SUB CATEGORY	CREATOR	RULE TYPE	OPTIONAL TYPE	STATUS
22/06/2022 18:12:19	1	T1112_ModifyRegistry	Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:10:57	1	T11682_SystemInformationDiscovery	Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:04:48	1	T1059_005_VisualBasic	Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Undeployed

- 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;

1 Selected

UPDATED TIME	PRIORITY	NAME	CATEGORY	SUB CATEGORY	CREATOR	RULE TYPE	OPTIONAL TYPE	STATUS
22/06/2022 18:12:19	1	T1112_ModifyRegistry	Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:10:57	1	T11682_SystemInformationDiscovery	Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:04:48	1	T1059_005_VisualBasic	Anomaly Detect on	MITRE ATT&CK	root	builder	custom	Undeployed

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.

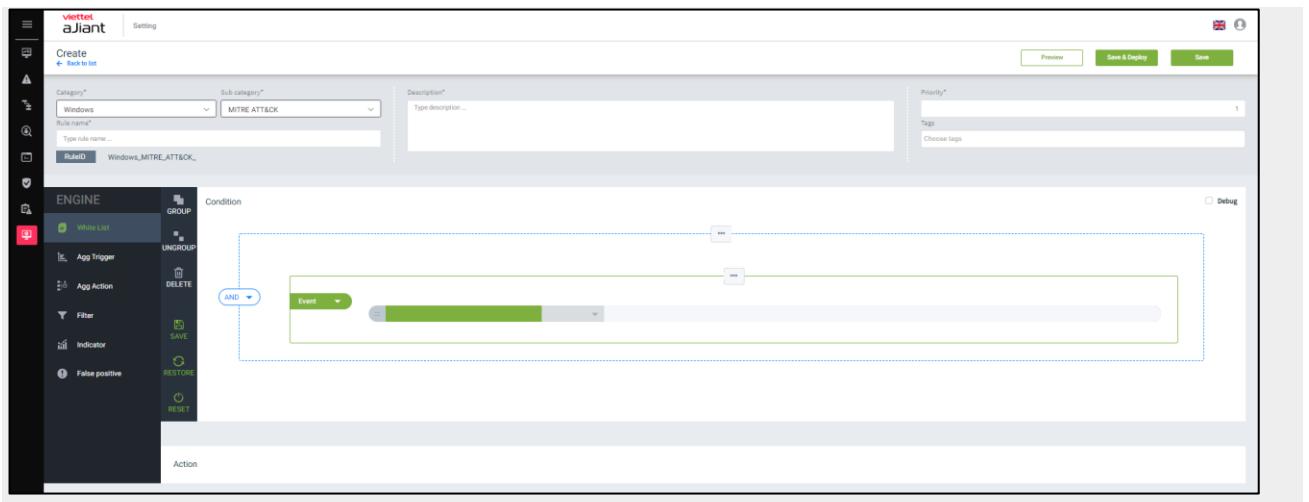
+ Group/Ungroup: Allows users to quickly combine or separate conditions within an AND or OR operator. Steps to group/ungroup:

- 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;

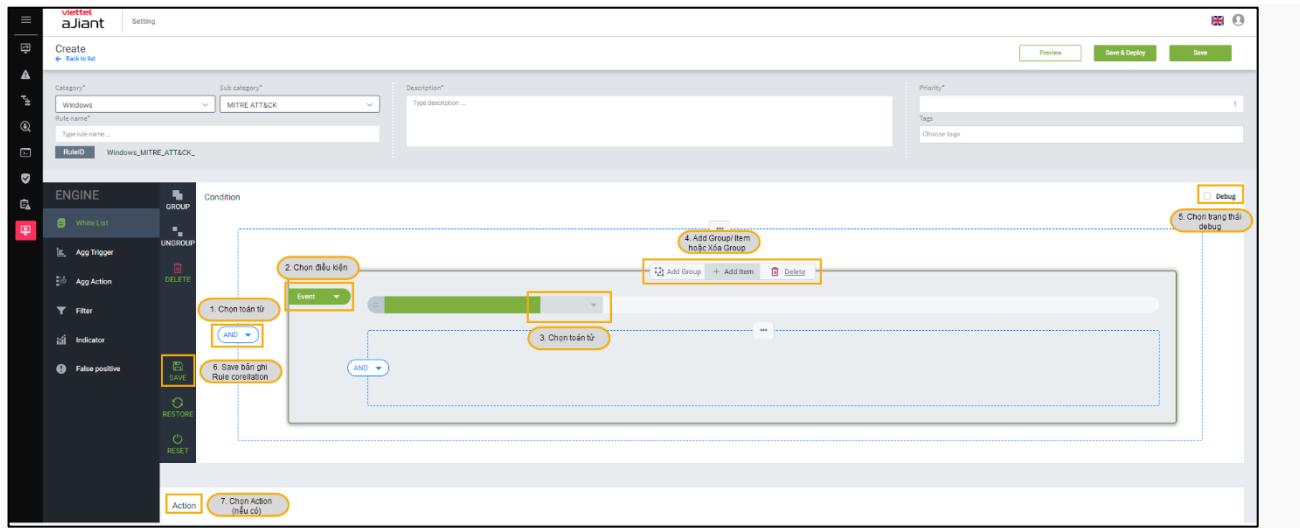


- Enter the rule information;



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.

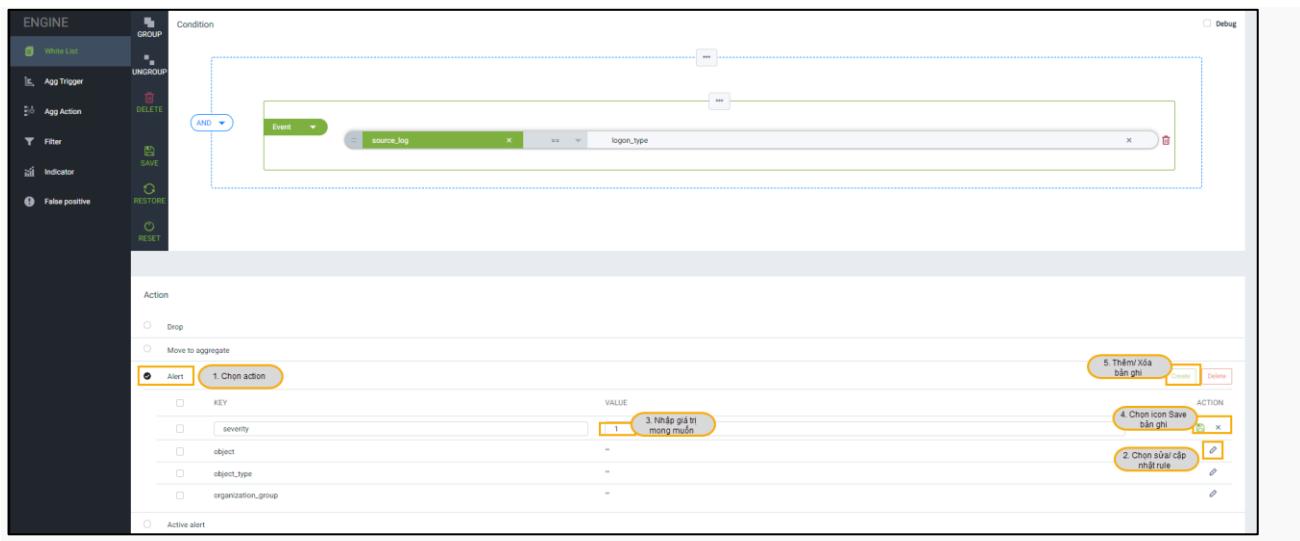
Whitelist: Includes 4 actions in the form of checkboxes: Drop, Convert to Aggregate, Alert, and Active List. Users are required to select one of these four actions. When logs that meet the conditions are pushed in, one of the four selected actions will be executed. Detailed functions of the 4 actions:

- 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;

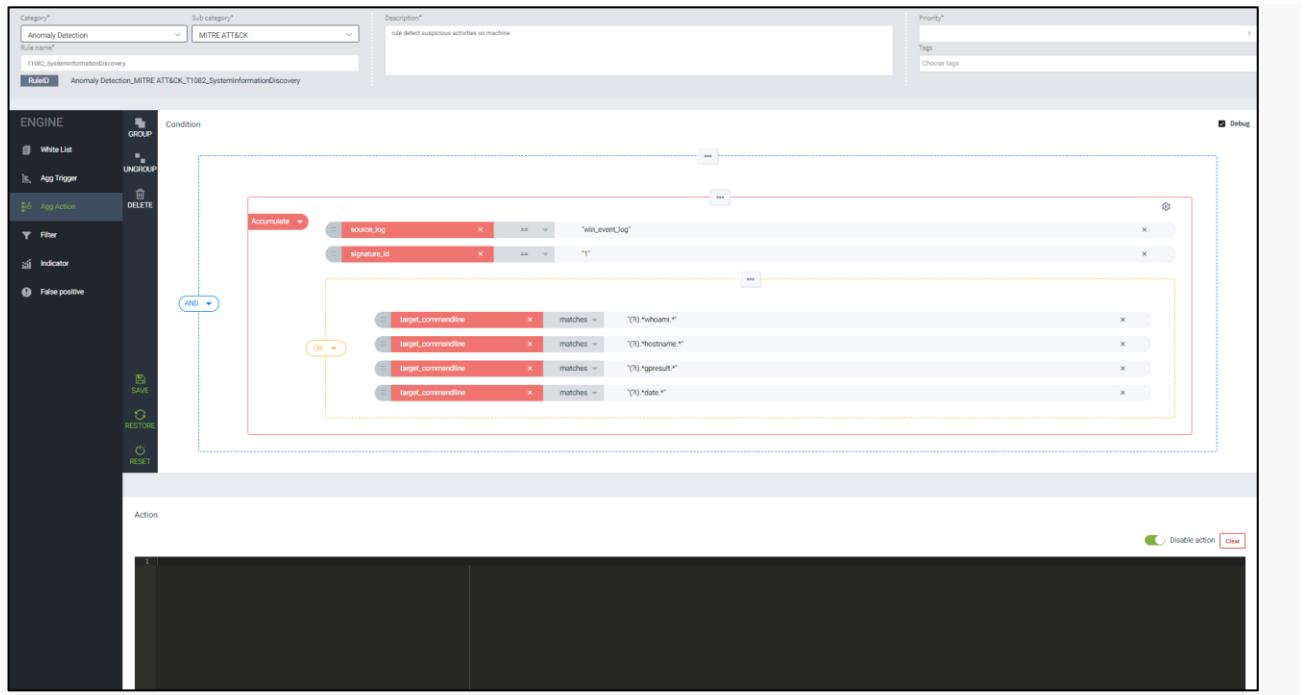
Note: Multiple actions can be created with different fields depending on the user's purpose.

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

UPDATED TIME	PRIORITY	NAME	CATEGORY	SUB CATEGORY	CREATOR	RULE TYPE	OPTIONAL TYPE	STATUS
22/06/2022 18:12:19	1	T1112_ModifyRegistry	Anomaly Detection	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:10:57	1	T1082_SystemInformationDiscovery	Anomaly Detection	MITRE ATT&CK	root	builder	custom	Deployed
22/06/2022 18:04:48	1	T1059_005_VisualBasic	Anomaly Detection	MITRE ATT&CK	root	builder	custom	Undeployed

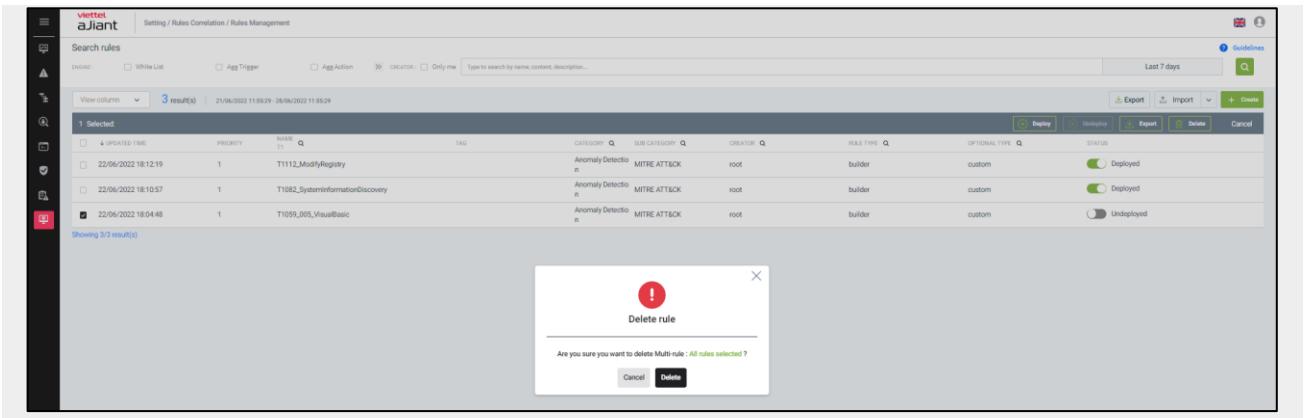
Steps to delete one rule:

- 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 Application Control

Purpose: The Application Control function allows configuring applications/processes to be blocked from running (executing) on the user's machine. Applications/processes are identified based on hash codes (MD5, SHA1, SHA256) or file paths.

Display the list of blocked applications/processes

Click on the Protect & Prevention tab > select Application Control to display all applications/processes on the user's machine that are blocked from use.

Type	Description	Created Time	Action
Path	import from file	2022/06/15 15:06:46	
Path	import from file	2022/06/15 15:06:46	
Hash	import from file	2022/06/15 15:06:46	
Path	import from file	2022/06/15 15:06:46	
Hash	import from file	2022/06/15 15:06:46	
Path	import from file	2022/06/15 15:06:46	
Hash	import from file	2022/06/15 15:06:46	
Path	ArINN Test	2022/02/08 14:38:11	

Search for blocked applications/processes

Users can search by the hash code or the path of the blocked application.

Type	Description	Created Time	Action
Path	import from file	2022/06/15 15:06:46	
Path	import from file	2022/06/15 15:06:46	
Hash	import from file	2022/06/15 15:06:46	
Path	import from file	2022/06/15 15:06:46	
Hash	import from file	2022/06/15 15:06:46	
Path	import from file	2022/06/15 15:06:46	
Hash	import from file	2022/06/15 15:06:46	
Path	ArINN Test	2022/02/08 14:38:11	

Add new blocked application/process

Click on “Add new” to add a new blocked application/process; users can choose to block by Path or by Hash code (MD5, SHA1, SHA256).

1. Click on the '+ Add New Application' button.

2. Enter the application name (e.g., Chrome) and select the type (Path or Hash).

3. Click the 'Apply' button to add the new application.

Add new application/process from an existing file

Users can add new blocked applications/processes from a .csv file following the provided template to the current application list;

Click “Import”, select the path to the file you want to upload, and click “Open”. The system will automatically add the list of applications to be blocked to the system.

0 agent(s) updated | Time updated: 2022/06/17 15:52:36

Object	Type	Description	Action
C:\tempransomware.exe	Path	import from file	2022/06/15 15:06:46
D:\Doc\temp.dll	Path	import from file	2022/06/15 15:06:46
B5454CF988E4E3F43D60F8FDCE52D26E14B4D93	Hash	import from file	2022/06/15 15:06:46
*tempvirus.dll	Path	import from file	2022/06/15 15:06:46
malware	Path	import from file	2022/06/15 15:06:46
D802C6E11B3D295C08FEF124870F9863CEDADF12	Hash	import from file	2022/06/15 15:06:46
C:\Windows\System32\asdawb.exe	Path	AnhNN Test	2022/02/08 14:38:11

Import Application List + Add New Application

Delete blocked applications/processes from the list

The system supports deleting one or multiple blocked applications; Click on each application you want to delete and click the “Delete” icon, or click the checkbox at the beginning of each application and then click the “Delete” button.

0 agent(s) updated | Time updated: 2022/06/17 15:52:36

Selected 2 application(s) Cancel

Object	Type	Description	Created Time	Action
C:\tempransomware.exe	Path	import from file	2022/06/15 15:06:46	
D:\Doc\temp.dll	Path	import from file	2022/06/15 15:06:46	
B5454CF988E4E3F43D60F8FDCE52D26E14B4D93	Hash	import from file	2022/06/15 15:06:46	
*tempvirus.dll	Path	import from file	2022/06/15 15:06:46	
malware	Path	import from file	2022/06/15 15:06:46	
D802C6E11B3D295C08FEF124870F9863CEDADF12	Hash	import from file	2022/06/15 15:06:46	
C:\Windows\System32\asdawb.exe	Path	AnhNN Test	2022/02/08 14:38:11	

Are you sure you want to delete application ?

The update stream of the number of agent machines that have successfully updated the new list.

After the user adds/edits/deletes the list of processes on the interface, the system will update this list to the agents through the agent file update flow (every 3 minutes). When an agent receives the new configuration, it generates a log with eventID = 101 and sends it to the server, which is displayed on the Event

Search screen. The system then automatically updates the number of agents that have updated the new configuration list on the Application Control screen.



3.10.2 *Endpoint Firewall*

Purpose: The Endpoint Firewall function allows configuration of connections to be blocked or allowed on the user's device, including blocking by application, IP, port, or both IP and port. It supports TCP, UDP, ICMP, ICMPv6, IGMP protocols, supports IPv4 and IPv6, and supports both inbound and outbound connections.

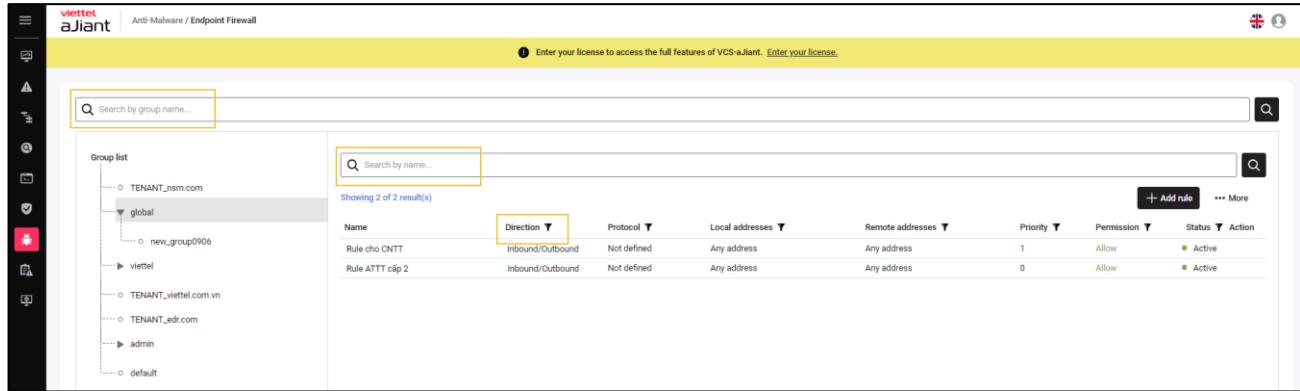
Display the list of blocked connections

Click on the Alti-Malware tab > select Endpoint Firewall to display the complete list of blocked connections categorized by user groups.

Name	Direction	Protocol	Local addresses	Remote addresses	Priority	Permission	Status	Action
Rule cho CNTT	Inbound/Outbound	Not defined	Any address	Any address	1	Allow	Active	
Rule ATTT clip 2	Inbound/Outbound	Not defined	Any address	Any address	0	Allow	Active	

Search for blocked connections

Users can search by user group, firewall rule name, or filter by the value of each condition (Name, connect type inbound/outbound, IP, etc.) on the firewall list screen.



The screenshot shows the Viettel Ajiant interface. On the left, there's a sidebar with icons for Home, Groups, Devices, and Logs. The main area has a search bar at the top. Below it, there are two search boxes: one for 'Search by group name...' and another for 'Search by name...'. The 'Group list' on the left shows several groups, including 'TENANT_nsrm.com', 'global' (which is selected), 'new_group0906', 'viettel', 'TENANT_viettel.com.vn', 'TENANT_edr.com', 'admin', and 'default'. The right side shows a table of 'Showing 2 of 2 result(s)' with columns: Name, Direction, Protocol, Local addresses, Remote addresses, Priority, Permission, Status, and Action. The table contains two rows: 'Rule cho CNTT' (Inbound/Outbound, Not defined, Any address, Any address, 1, Allow, Active) and 'Rule ATTT clip 2' (Inbound/Outbound, Not defined, Any address, Any address, 0, Allow, Active).

Add new blocked connections

Select the user group, then click the “Add new” button and enter the information in the popup to add a blocked connection.

- + Name: the name of the condition you want to create;
- + Program: programs that need to be blocked/allowed on the user's machine. For example, "%ProgramFiles% (x86)\Application_Name.exe"
- + Protocol: Not defined, ICMP, TCP, UDP, ICMPv6, IGMP
- + Port: the port to block; enter 0 to block all ports.
- + Direction: inbound, outbound, inbound/outbound
- + Permission: Allow / Block
- + Remote address/ Local address: supports IPv4, IPv6, and IP ranges.
- + Valid time: the time period during which the condition is effective

Note: inheritance rules from the parent group

- + If the option "Inherit the status from the parent group" is selected: the child group will inherit all conditions from the parent group and will not be allowed to add or modify the inherited conditions.
- + If the option "Inherit the status from the parent group" is not selected: the subgroup will not inherit from the parent group and can have conditions added or removed independently.

Name	Direction	Protocol	Local addresses	Remote addresses	Priority	Permission	Status
Rule cho CNTT	Inbound/Outbound	Not defined	Any address	Any address	1	Allow	Active
Rule ATTT clip 2	Inbound/Outbound	Not defined	Any address	Any address	0	Allow	Active

Create a copy from the existing conditions.

Select the condition for creating a copy, perform the Action, and choose Duplicate rule.

Name	Direction	Protocol	Local addresses	Remote addresses	Priority	Permission	Status	Action
Rule cho CNTT	Inbound/Outbound	Not defined	Any address	Any address	1	Allow	Active	
Rule ATTT clip 2	Inbound/Outbound	Not defined	Any address	Any address	0	Allow	Active	

Add new blocked connections from an existing file

Users can add new blocked applications/processes from a .csv file following the provided template to the current application list;

Click the “Import from .CSV” button, select the path to the file you want to upload, and click the “Open” button. The system will automatically add the list of applications to be blocked to the system.

Name	Direction	Protocol	Local addresses	Remote addresses	Priority	Permission
Rule cho CNTT	Inbound/Outbound	Not defined	Any address	Any address	1	Allow
Rule ATTT clip 2	Inbound/Outbound	Not defined	Any address	Any address	0	Allow

Remove blocked connections from the list

Click on each connection you want to delete and click the “Delete” icon.

Name	Direction	Protocol	Local addresses	Remote addresses	Priority	Permission	Status	Action
Rule cho CNTT	Inbound/Outbound	Not defined	Any address	Any address	1	Allow	Active	Edit rule
Rule ATTT cấp 2	Inbound/Outbound	Not defined	Any address	Any address	0	Allow	Active	Edit rule

Export data of the conditions

Select the user group, choose More, then select Export Rule to export a CSV file containing all the condition information of the selected group.

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:

Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
ubuntu 2	root	06/10/2022 - 16:15:56	Quick scan	1	Immediately	06/10/2022 - 16:15:56	N/A	N/A	● Finished	...
Ubuntu	root	06/10/2022 - 16:11:44	Quick scan	1	Immediately	06/10/2022 - 16:11:44	N/A	N/A	● Finished	...
Quick Win 11	root	06/10/2022 - 16:07:34	Quick scan	1	Immediately	06/10/2022 - 16:07:34	N/A	N/A	● Finished	...
Task win 11	root	06/10/2022 - 16:03:41	Custom scan	1	Immediately	06/10/2022 - 16:03:41	N/A	N/A	● Finished	...
Task 456	root	06/10/2022 - 11:37:08	Quick scan	1	At 06/10/2022 - 12:39:30	06/10/2022 - 12:39:30	N/A	N/A	● Finished	...
Task 123	root	06/10/2022 - 11:34:26	Quick scan	1	Immediately	06/10/2022 - 11:34:26	N/A	N/A	● Finished	...
éwewe	root	06/10/2022 - 11:17:59	Quick scan	2	Immediately	06/10/2022 - 11:17:59	N/A	N/A	● Finished	...
Task 1	root	06/10/2022 - 11:14:04	Quick scan	2	Immediately	06/10/2022 - 11:14:04	N/A	N/A	● Finished	...
Task mai	root	06/10/2022 - 11:10:10	Quick scan	1	Immediately	06/10/2022 - 11:10:10	N/A	N/A	● Finished	...
mailtest	root	06/10/2022 - 10:54:37	Quick scan	1	Immediately	06/10/2022 - 10:54:37	N/A	N/A	● Finished	...
Task 2	root	06/10/2022 - 09:09:09	Custom scan	1	Immediately	06/10/2022 - 09:09:09	N/A	N/A	● Finished	...

- 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.

Showing 11 of 11 result(s)

Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
ubuntu 2	root	06/10/2022 - 16:15:56	Quick scan	1	Immediately	06/10/2022 - 16:15:56	N/A	N/A	● Finished	...
Ubuntu	root	06/10/2022 - 16:11:44	Quick scan	1	Immediately	06/10/2022 - 16:11:44	N/A	N/A	● Finished	...
Quick Win 11	root	06/10/2022 - 16:07:34	Quick scan	1	Immediately	06/10/2022 - 16:07:34	N/A	N/A	● Finished	...
Task Win 11	root	06/10/2022 - 16:03:41	Custom scan	1	Immediately	06/10/2022 - 16:03:41	N/A	N/A	● Finished	...
Task 456	root	06/10/2022 - 11:37:08	Quick scan	1	At 06/10/2022 - 12:39:30	06/10/2022 - 12:39:30	N/A	N/A	● Finished	...
Task 123	root	06/10/2022 - 11:34:26	Quick scan	1	Immediately	06/10/2022 - 11:34:26	N/A	N/A	● Finished	...
éwewe	root	06/10/2022 - 11:17:59	Quick scan	2	Immediately	06/10/2022 - 11:17:59	N/A	N/A	● Finished	...
Task 1	root	06/10/2022 - 11:14:04	Quick scan	2	Immediately	06/10/2022 - 11:14:04	N/A	N/A	● Finished	...
Task mai	root	06/10/2022 - 11:10:10	Quick scan	1	Immediately	06/10/2022 - 11:10:10	N/A	N/A	● Finished	...
matetest	root	06/10/2022 - 10:54:37	Quick scan	1	Immediately	06/10/2022 - 10:54:37	N/A	N/A	● Finished	...
Task 2	root	06/10/2022 - 09:09:09	Custom scan	1	Immediately	06/10/2022 - 09:09:09	N/A	N/A	● Finished	...

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

Create new task

Task name: new task |

Scan type: Quick scan | Priority: Low

Trigger: Run immediately

Assignee(s): All agents (total 38 agents)

Create

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.

Run on a schedule

One time

Start time

31/10/2022 - 10:45:27

Run task as soon as possible after a schedule is missed i

+ 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:

Assignee(s)

All agents (total 38 agents)
 Choose group(s) and agent(s)

0 assignee(s)

 + Add agent/group

 Import from list...▼

Information of selected agent(s) will be showing here.

- + 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:

Agent ID	Computer name	IP Address	Group	Status
06A6927157E4EEE09A0C76...	ajiant-agent-centos6	127.0.0.1, 10.255.250...	auto_test	Offline
0715289C3AB47DF72E6E6C...	phula-viettelos1018	127.0.0.1, 192.168.12...	default	Offline
0A691AC0638F0D4E54CA75...	Win7x64-A-PC	10.0.2.15, 127.0.0.1	mailtest1	Offline
0AC36E41E40C670E5A1E8B...	phula-redhat7.7	127.0.0.1, 192.168.12...	chuyen_test	Offline
0B726365F86EBFF5000E6B2...	localhost.localdomain	127.0.0.1, 192.168.19...	no_group	Offline
0E1CE9E9249C35DC0F769F2...	ubuntu	127.0.0.1, 192.168.12...	mailtest1_1	Offline
155E59FAED0245085750CE...	phula.redhat8.4	127.0.0.1, 192.168.12...	global	Offline
1570617137788D10F47BE8...	agent-core-mac	127.0.0.1, 192.168.6.2...	no_group	Offline

- 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:

Agent ID	Computer name	IP Address	Group	Status
06A6927157E4EEE09A0C76...	ajiant-agent-centos6	127.0.0.1, 10.255.250...	maitest1_2_3	Offline
0715289C3A8470F726E65C...	phula-viettelos1018	127.0.0.1, 192.168.12...	default	Offline
0A691ACC638F004E54CA75...	Win7x64-A-PC	10.0.2.15, 127.0.0.1	maitest1	Offline
<input checked="" type="checkbox"/> 0AC36E41E40C67D65A1E8...	phula-redhat7.7	127.0.0.1, 192.168.12...	chuyen_test	Offline
0B726365F86E6FF5000E6B2...	localhost.localdomain	127.0.0.1, 192.168.19...	no_group	Offline
0E1C8E9249C350CDF763F2...	ubuntu	127.0.0.1, 192.168.12...	maitest1_1	Offline
155E59FAED2450B5750CE...	phula.redhat8.4	127.0.0.1, 192.168.12...	global	Offline
15706171377B8D10F47BE8...	agent-core-mac	127.0.0.1, 192.168.6.2...	no_group	Offline

- 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.

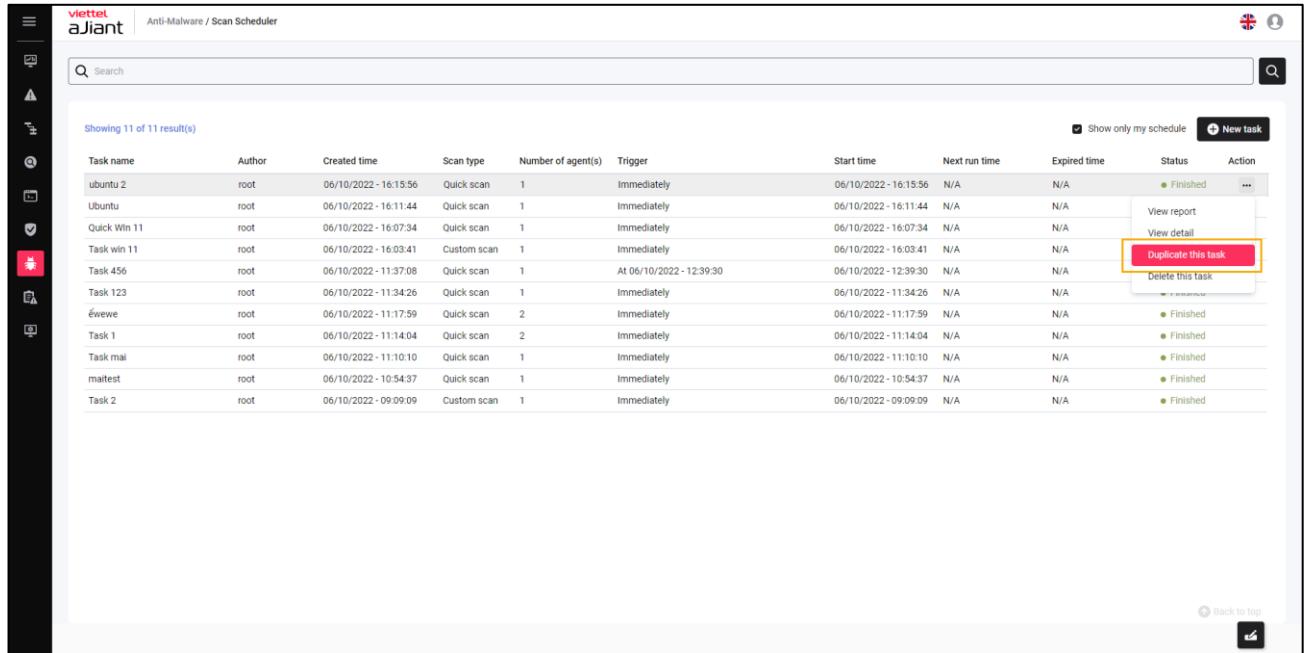
- + Import from .CSV: Allows users to upload a list of workstations by:
 - Select the Import from list button;
 - Selecting Download sample file allows you to download a sample workstation list file;
 - The user enters workstation information and uploads the workstation list file by selecting the Import 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 screenshot shows a table of scan tasks. The columns are: Task name, Author, Created time, Scan type, Number of agent(s), Trigger, Start time, Next run time, Expired time, Status, and Action. The 'Action' column contains buttons for 'View report', 'View detail', 'Duplicate this task' (which is highlighted with a red box), and 'Delete this task'. The 'Duplicate this task' button is located at the bottom right of the 'Action' column for the 'Task 1' row.

Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
ubuntu 2	root	06/10/2022 - 16:15:56	Quick scan	1	Immediately	06/10/2022 - 16:15:56	N/A	N/A	● Finished	View report
Ubuntu	root	06/10/2022 - 16:11:44	Quick scan	1	Immediately	06/10/2022 - 16:11:44	N/A	N/A	● Finished	View detail
Quick Win 11	root	06/10/2022 - 16:07:34	Quick scan	1	Immediately	06/10/2022 - 16:07:34	N/A	N/A	● Finished	View report
Task win 11	root	06/10/2022 - 16:03:41	Custom scan	1	Immediately	06/10/2022 - 16:03:41	N/A	N/A	● Finished	View detail
Task 456	root	06/10/2022 - 11:37:00	Quick scan	1	At 06/10/2022 - 12:39:30	06/10/2022 - 12:39:30	N/A	N/A	● Finished	Delete this task
Task 123	root	06/10/2022 - 11:34:26	Quick scan	1	Immediately	06/10/2022 - 11:34:26	N/A	N/A	● Finished	View report
éewe	root	06/10/2022 - 11:17:59	Quick scan	2	Immediately	06/10/2022 - 11:17:59	N/A	N/A	● Finished	View detail
Task 1	root	06/10/2022 - 11:14:04	Quick scan	2	Immediately	06/10/2022 - 11:14:04	N/A	N/A	● Finished	View report
Task mai	root	06/10/2022 - 11:10:10	Quick scan	1	Immediately	06/10/2022 - 11:10:10	N/A	N/A	● Finished	View detail
maiitest	root	06/10/2022 - 10:54:37	Quick scan	1	Immediately	06/10/2022 - 10:54:37	N/A	N/A	● Finished	Delete this task
Task 2	root	06/10/2022 - 09:09:09	Custom scan	1	Immediately	06/10/2022 - 09:09:09	N/A	N/A	● Finished	View report

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

Duplicate task

Task name: Task 1

Scan type: Quick scan Priority: Low

Trigger: Run immediately

Assignee(s): Choose group(s) and agent(s)

4 assignee(s):

Assignee	Type	Computer name	IP Address	Action
1FBAFB82BBC6...	agent	virtual_agent_phul...	172.17.0.22	
09D9E77F49E63...	agent	virtual_agent_phul...	172.17.0.2	
5046150E542C6...	agent	Win10x64MAINTN	192.168.74.128	
EC8EB5F0DAB21...	agent	Win10x64_MailNTN	192.168.74.128	

Cancel Create

- 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.

Duplicate task

Task name: Task 1

Scan type: Quick scan Priority: Low

Trigger: Run immediately

Assignee(s): Choose group(s) and agent(s)

4 assignee(s):

Assignee	Type	Computer name	IP Address	Action
1FBAFB82BBC6...	agent	virtual_agent_phul...	172.17.0.22	
09D9E77F49E63...	agent	virtual_agent_phul...	172.17.0.2	
5046150E542C6...	agent	Win10x64MAINTN	192.168.74.128	
EC8EB5F0DAB21...	agent	Win10x64_MailNTN	192.168.74.128	

Cancel Create

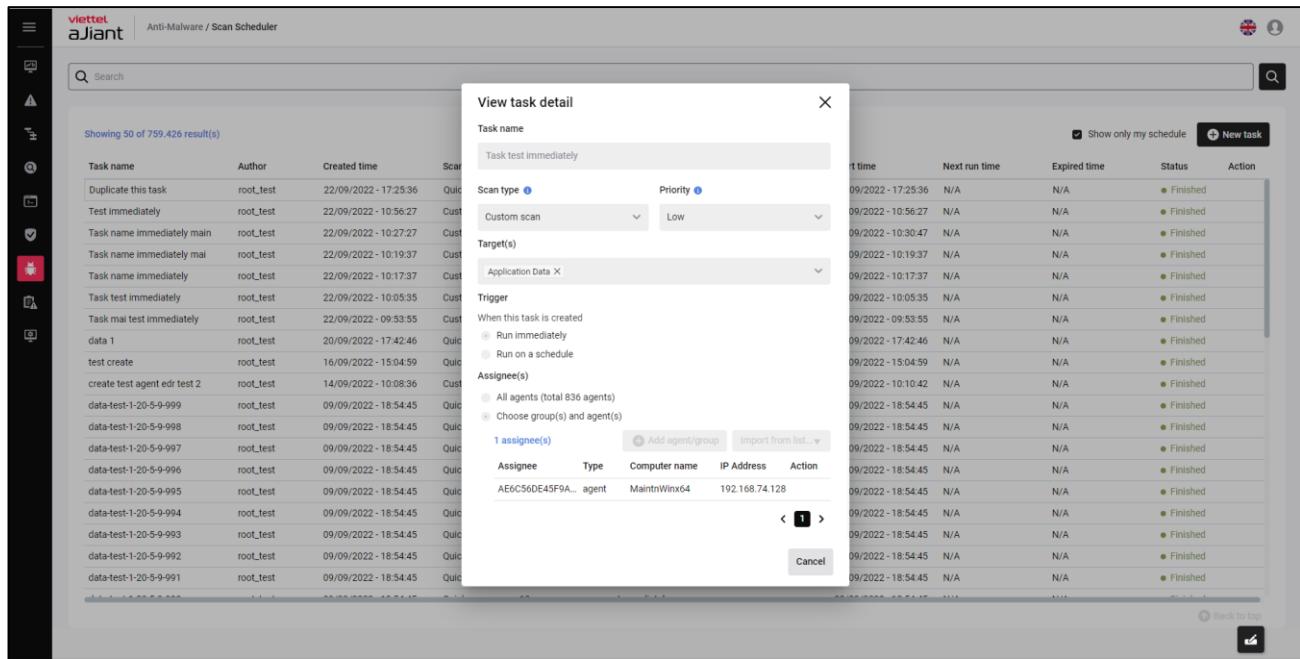
View details

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;

viettel
aJiant Anti-Malware / Scan Scheduler

Showing 50 of 759,426 result(s)

Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
Duplicate this task	root_test	22/09/2022 - 17:25:36	Quick scan	5	Immediately	22/09/2022 - 17:25:36	N/A	N/A	● Finished	View report
Test immediately	root_test	22/09/2022 - 10:56:27	Custom scan	1	Immediately	22/09/2022 - 10:56:27	N/A	N/A	● Finished	View detail
Task name immediately main	root_test	22/09/2022 - 10:27:27	Custom scan	1	At 22/09/2022 - 10:30:47	22/09/2022 - 10:30:47	N/A	N/A	● Finished	View report
Task name immediately mai	root_test	22/09/2022 - 10:19:37	Custom scan	1	Immediately	22/09/2022 - 10:19:37	N/A	N/A	● Finished	View detail
Task name immediately	root_test	22/09/2022 - 10:17:37	Custom scan	1	Immediately	22/09/2022 - 10:17:37	N/A	N/A	● Finished	View report
Task test immediately	root_test	22/09/2022 - 10:05:35	Custom scan	1	Immediately	22/09/2022 - 10:05:35	N/A	N/A	● Finished	View detail
Task mai test immediately	root_test	22/09/2022 - 09:53:55	Custom scan	1	Immediately	22/09/2022 - 09:53:55	N/A	N/A	● Finished	View report
data 1	root_test	20/09/2022 - 17:42:46	Quick scan	1	Immediately	20/09/2022 - 17:42:46	N/A	N/A	● Finished	View detail
test create	root_test	16/09/2022 - 15:04:59	Quick scan	0	Immediately	16/09/2022 - 15:04:59	N/A	N/A	● Finished	View report
create test agent edr test 2	root_test	14/09/2022 - 10:08:36	Custom scan	1	At 29/09/2022 - 10:10:42	29/09/2022 - 10:10:42	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-990	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail

Show only my schedule [New task](#)

[Delete this task](#)

- 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.

viettel
aJiant Anti-Malware / Scan Scheduler

Showing 50 of 759,426 result(s)

Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
Duplicate this task	root_test	22/09/2022 - 17:25:36	Quick scan	5	Immediately	22/09/2022 - 17:25:36	N/A	N/A	● Finished	View report
Test immediately	root_test	22/09/2022 - 10:56:27	Custom scan	1	Immediately	22/09/2022 - 10:56:27	N/A	N/A	● Finished	View detail
Task name immediately main	root_test	22/09/2022 - 10:27:27	Custom scan	1	At 22/09/2022 - 10:30:47	22/09/2022 - 10:30:47	N/A	N/A	● Finished	View report
Task name immediately mai	root_test	22/09/2022 - 10:19:37	Custom scan	1	Immediately	22/09/2022 - 10:19:37	N/A	N/A	● Finished	View detail
Task name immediately	root_test	22/09/2022 - 10:17:37	Custom scan	1	Immediately	22/09/2022 - 10:17:37	N/A	N/A	● Finished	View report
Task test immediately	root_test	22/09/2022 - 10:05:35	Custom scan	1	Immediately	22/09/2022 - 10:05:35	N/A	N/A	● Finished	View detail
Task mai test immediately	root_test	22/09/2022 - 09:53:55	Custom scan	1	Immediately	22/09/2022 - 09:53:55	N/A	N/A	● Finished	View report
data 1	root_test	20/09/2022 - 17:42:46	Quick scan	1	Immediately	20/09/2022 - 17:42:46	N/A	N/A	● Finished	View detail
test create	root_test	16/09/2022 - 15:04:59	Quick scan	0	Immediately	16/09/2022 - 15:04:59	N/A	N/A	● Finished	View report
create test agent edr test 2	root_test	14/09/2022 - 10:08:36	Custom scan	1	At 29/09/2022 - 10:10:42	29/09/2022 - 10:10:42	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View report
data-test-1-20-5-9-990	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail

Show only my schedule [New task](#)

[Delete this task](#)

Delete this task?

Are you sure you want to delete the task "Task name immediately mai"?

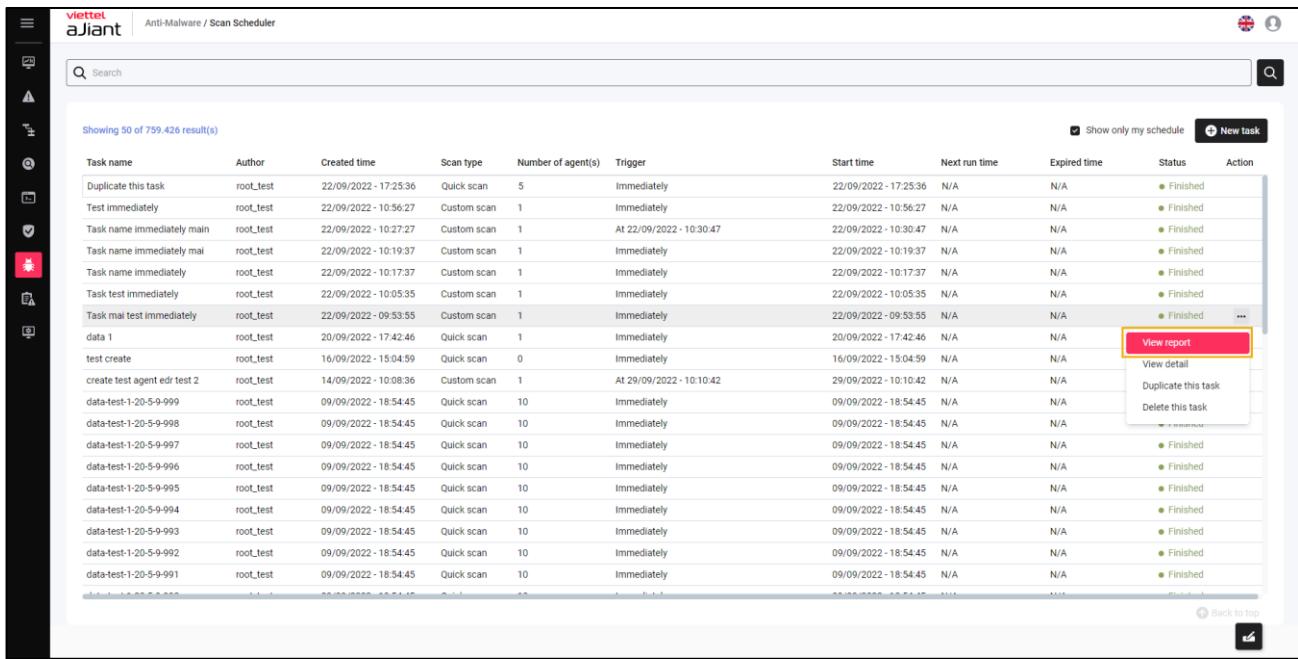
[No](#) [Yes, keep delete](#)

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;



The screenshot shows a list of 759 tasks. The columns include Task name, Author, Created time, Scan type, Number of agent(s), Trigger, Start time, Next run time, Expired time, Status, and Action. A context menu is open over the task 'data 1', with the 'View report' option highlighted.

Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
Duplicate this task	root_test	22/09/2022 - 17:25:36	Quick scan	5	Immediately	22/09/2022 - 17:25:36	N/A	N/A	● Finished	
Test immediately	root_test	22/09/2022 - 10:56:27	Custom scan	1	Immediately	22/09/2022 - 10:56:27	N/A	N/A	● Finished	
Task name immediately main	root_test	22/09/2022 - 10:27:27	Custom scan	1	At 22/09/2022 - 10:30:47	22/09/2022 - 10:30:47	N/A	N/A	● Finished	
Task name immediately mai	root_test	22/09/2022 - 10:19:37	Custom scan	1	Immediately	22/09/2022 - 10:19:37	N/A	N/A	● Finished	
Task name immediately	root_test	22/09/2022 - 10:17:37	Custom scan	1	Immediately	22/09/2022 - 10:17:37	N/A	N/A	● Finished	
Task test immediately	root_test	22/09/2022 - 10:05:35	Custom scan	1	Immediately	22/09/2022 - 10:05:35	N/A	N/A	● Finished	
Task mai test immediately	root_test	22/09/2022 - 09:53:55	Custom scan	1	Immediately	22/09/2022 - 09:53:55	N/A	N/A	● Finished	
data 1	root_test	20/09/2022 - 17:42:46	Quick scan	1	Immediately	20/09/2022 - 17:42:46	N/A	N/A	● Finished	View report
test create	root_test	16/09/2022 - 15:04:59	Quick scan	0	Immediately	16/09/2022 - 15:04:59	N/A	N/A		View detail
create test agent edr test 2	root_test	14/09/2022 - 10:08:38	Custom scan	1	At 29/09/2022 - 10:10:42	29/09/2022 - 10:10:42	N/A	N/A		Duplicate this task
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A		Delete this task
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A		View detail
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	● Finished	View detail

- 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:

View task report

Task name: Task per: Created time: 14/09/2022 14:32:24
 Author: root_test Scan type: Custom scan

1 **2**  [Export to Excel](#) [View on Dashboard](#)

5 result(s)

Agent ID	Computer name	IP Address	Platform	Group	Status	Result
FC97D9289BFA70F681BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.1 36	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	● Scan skip	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule
524B30C4C568F59292D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	● Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0
F2AA317BE87690E505BF7D25CA6A7DC68D1FC37D	Blchpt3_Win10Test	192.168.255.1 38	Microsoft Windows 10 Pro	group_windows	● Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0

 [Back to top](#)

+ 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;

View task report

Task name: Task per: Created time: 14/09/2022 14:32:24
 Author: root_test Scan type: Custom scan

1 **2**  [Export to Excel](#) [View on Dashboard](#)

5 result(s)

Agent ID	Computer name	IP Address	Platform	Group	Status	Result
FC97D9289BFA70F681BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.1 36	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	● Scan skip	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule
524B30C4C568F59292D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	● Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0
F2AA317BE87690E505BF7D25CA6A7DC68D1FC37D	Blchpt3_Win10Test	192.168.255.1 38	Microsoft Windows 10 Pro	group_windows	● Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0

 [Back to top](#)

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.

View task report

Task name	Task per	Created time				
Author	root_test	Scan type				
fx		14/09/2022 14:32:24				
5 result(s)						
Agent ID	Computer name	IP Address	Platform	Group	Status	Result
FC97D9289BFA70F681BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.1 36	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	● Scan skip	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule
524B30C4C568F59292D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	● Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0
F2AA317BE87690E505BF7D25CA6A7DC68D1FC37D	Blchpt3_Win10Tes t	192.168.255.1 38	Microsoft Windows 10 Pro	group_windows	● Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0

Back to top

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

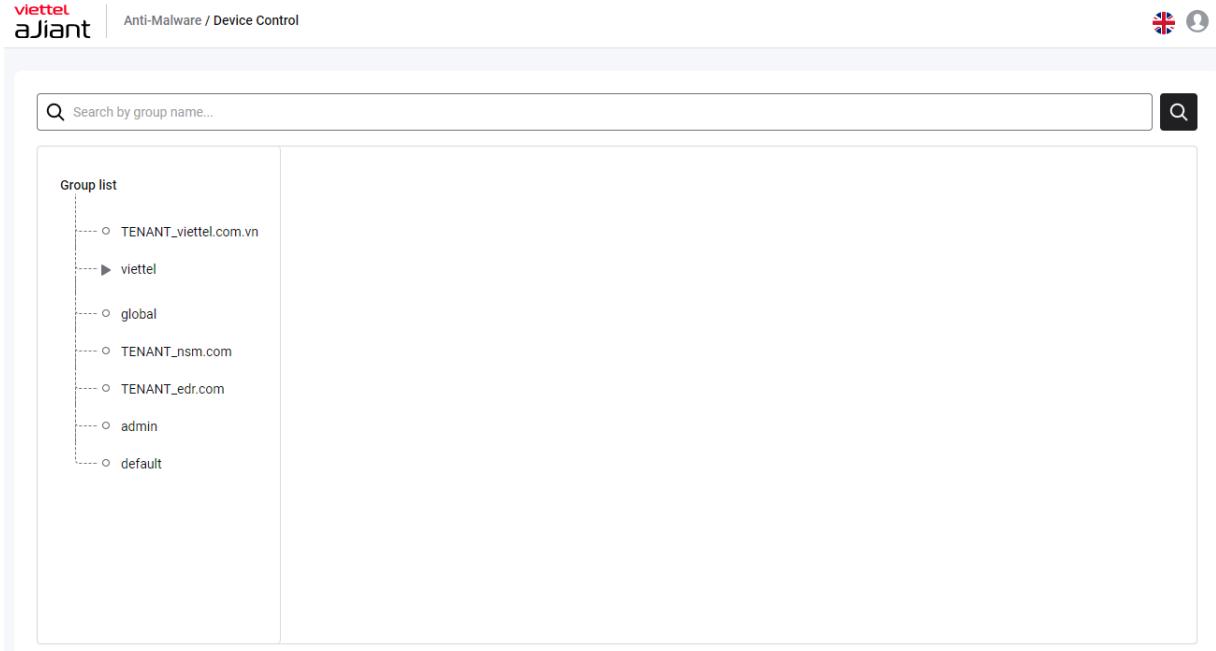
Function: Allows control and protection of important data through peripheral devices such as USB drives, Bluetooth devices, and writable CDs and DVDs.

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



The screenshot shows a web-based interface for managing device control. At the top, there is a header with the 'viettel' logo and the text 'Anti-Malware / Device Control'. On the right side of the header, there are icons for a user profile and a search function. Below the header is a search bar with the placeholder 'Search by group name...'. To the right of the search bar is a magnifying glass icon. The main content area is titled 'Group list' and displays a hierarchical tree structure of groups. The groups listed are: 'TENANT_viettel.com.vn', 'viettel' (which is expanded to show 'global', 'TENANT_ns.com', 'TENANT_edr.com', 'admin', and 'default').

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

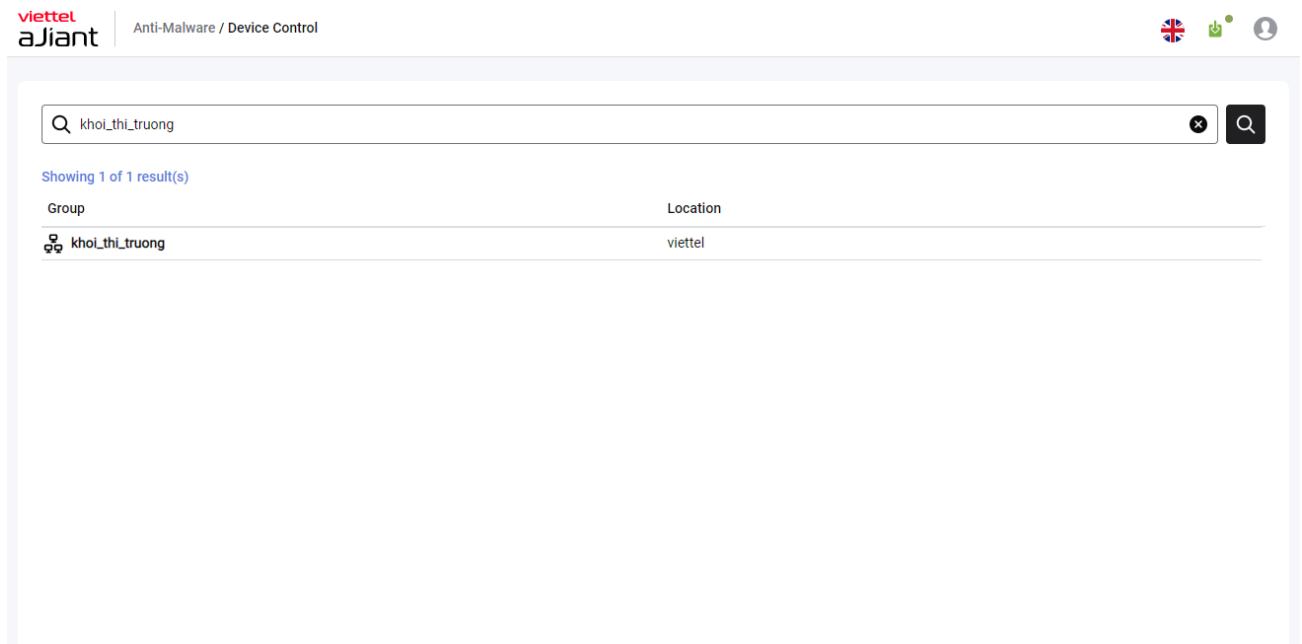


This screenshot shows the same interface as the previous one, but with a search term 'test_device_control' entered into the search bar. A dropdown menu below the search bar lists suggestions: 'TENANT_viettel.com.vn', 'anhnn_test', 'test_device_control' (which is highlighted with a red background), 'khoi_thi_truong', 'khoi_phu_thuoc', 'viettel', 'global', and 'TENANT_ns.com'. Below this dropdown, the 'Group list' tree is shown again, with the 'viettel' group expanded to show its sub-groups: 'TENANT_edr.com', 'admin', and 'default'. A red curved line is drawn from the bottom right corner of the image towards the bottom left corner, highlighting the search results area.

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.

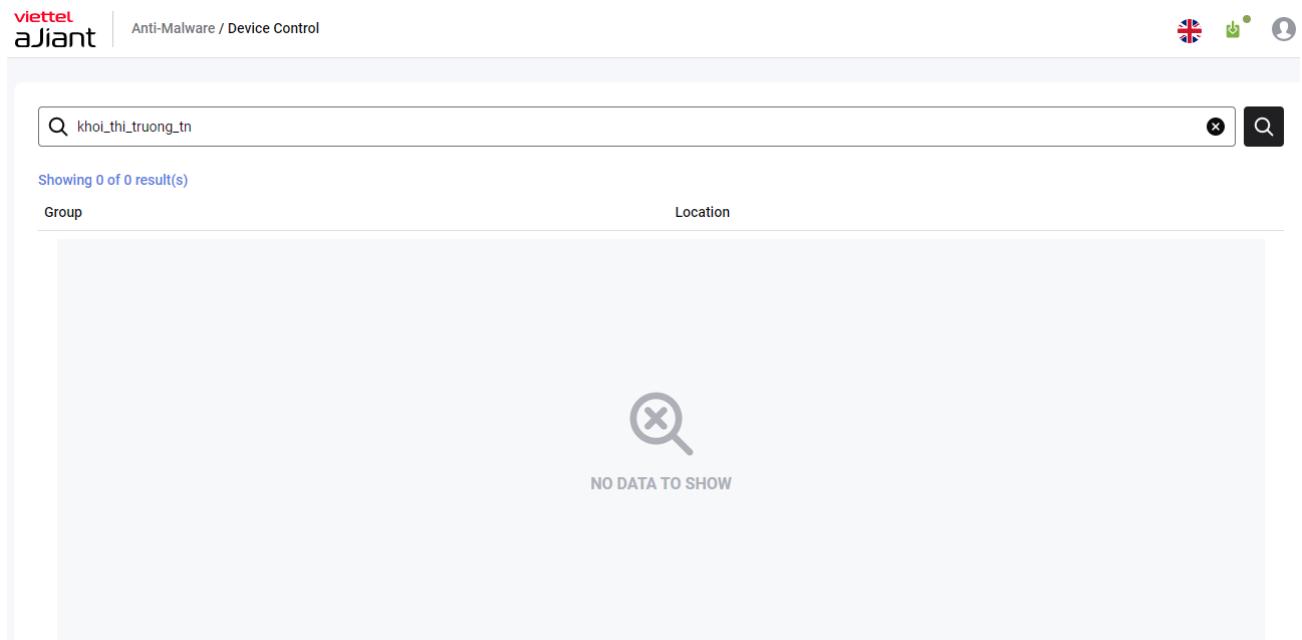
If there are results, they will be returned.



The screenshot shows a search interface with the following details:

- Search Bar:** The search term "khoi_thi_truong" is entered.
- Results Summary:** "Showing 1 of 1 result(s)"
- Table Headers:** "Group" and "Location"
- Table Data:** One row is shown, with "khoi_thi_truong" under the Group column and "viettel" under the Location column.

No results found for the search.



The screenshot shows a search interface with the following details:

- Search Bar:** The search term "khoi_thi_truong_tn" is entered.
- Results Summary:** "Showing 0 of 0 result(s)"
- Table Headers:** "Group" and "Location"
- Content Area:** A large "NO DATA TO SHOW" message with a magnifying glass icon containing an "X".

Device list of each group

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

There is a checkbox.

Inherited the status from the father group: liennt

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:

<input type="checkbox"/> Inherited the status from the father group: liennt	Device type	Status	Numbers of exception rules	Action
	Removable drives	<input type="checkbox"/> Block	0	
	Portable devices (MTP, PTP)	<input type="checkbox"/> Block	0	
	Network devices	<input type="checkbox"/> Block	0	
	Camera and scanners	<input type="checkbox"/> Block	0	
	Smart card devices	<input type="checkbox"/> Block	0	
	Other USB devices	<input checked="" type="checkbox"/> Allow	0	

- + 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

Detail - Removable drives X

Exception list

Q

Search

Showing 10 of 10 result(s) Add

Exception name	Description	Duration	Status	Action
zxczc	N/A	Forever	● Active	
teasd	vdvdv	Forever	● Active	
acca	N/A	18/05/2023 05:00:00 - 20/05/2023 14:30:00	● Active	
tasdasd	N/A	Forever	● Active	
tesda	N/A	Forever	● Active	
teasdasd	N/A	Forever	● Active	
yrdfds	N/A	Forever	● Active	
USB storage block forever	block forever	Forever	● Active	
test forever 2 USB storage	block USB Stor...	Forever	● Active	
test forever	N/A	Forever	● Active	

- 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).

Add exception

×

Exception name *

Rule 01

Permission

Allow

Description

Text description

0/100

Valid time

Forever

Choose time

09:00:00 23/05/2023 - 09:00:00 24/05/2023



Devices list (0)

Add device

Assignees

All agent(s)

Choose group(s) (0)

Choose agent(s) (0)

Cancel

Save

- 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)

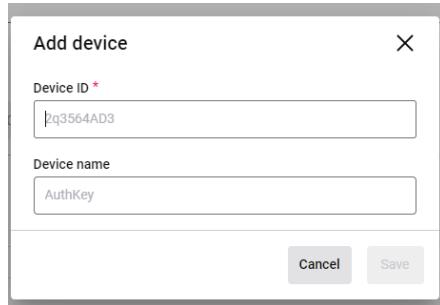
When there is no device: Only display the Add device button.

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.

Device list (1)			Add device
Device ID	Device name	Action	
Device USB 123	Thiết bị USB	 	  

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.)

Add agent(s)

<input type="checkbox"/> Agent ID	Computer name	IP Address	Group	Status
<input type="checkbox"/> 077278CE6797BB6B6395AB...	edr02_win10	192.168.40.129, 127....	vcs_anm	● Online
<input type="checkbox"/> 0EB4F0A2D2FE6432C50AFA...	ubuntu20	127.0.0.1, 10.0.2.15, 1...	vcs_anm	● Online
<input type="checkbox"/> 12CFB4DA48D28053302D14...	DESKTOP-7G2IBRE	192.168.56.1, 192.16...	vcs_anm	● Offline
<input type="checkbox"/> 15B2BBFFEB988C8080297...	JungJungJung	192.168.195.133, 127...	no_group	● Offline
<input type="checkbox"/> 1A2AA14691E192A4E1AF4A...	Win7x86	192.168.74.132, 127....	khoi_doc_lap	● Offline
<input type="checkbox"/> 1B0A66FD56EDD4C2C6D557...	DESKTOP-R2GBJEF	192.168.198.138, 127...	vcs_anm	● Offline
<input type="checkbox"/> 35BB40573301CD6ECD7194...	HuyenPT-Win7x86	192.168.131.129, 127...	vcs_anm	● Offline
<input type="checkbox"/> 44FF36ED36F0B20030539F5...	JUNGJU_JiuJiu	192.168.195.133, 127...	no_group	● Online

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.

Exception name *

◆ You can't leave this field blank.

Description

Description of this rule

Valid time

Forever

Choose time 16/05/2023 - 17:13:19 - 17/05/2023 - 17:03:19

Permission

Block

Device list (0)

Add device

Assignees

All agent(s)

Choose agent(s) (2)

Choose group(s) (4)

Add group

Group	Location	Action
TENANT_viettel.com.vn		
viettel		
global		
TENANT_nsrm.com		

<
1
>

Cancel Save

- 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;

Add group(s) X

Search

i **NOTE:** In this interface, users belonging to the parent group have full control over all the child groups of their parent group. [See more >>](#)

- TENANT_viettel.c...
- viettel >
- global
- TENANT_ns.com
- TENANT_edr.com

Selected (0)

Group	Location	Action
X		
NO DATA TO SHOW		

Cancel
Save

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.

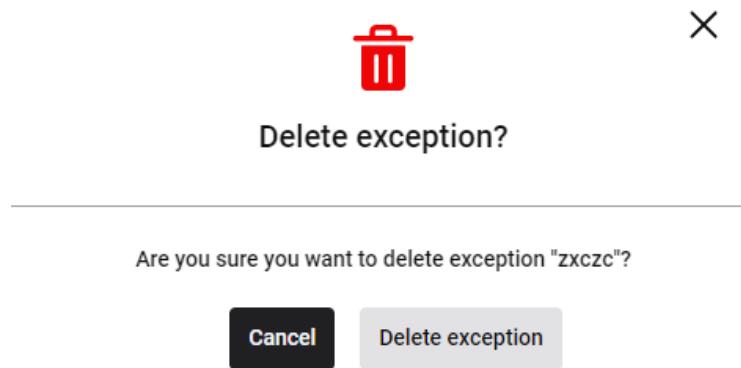
If you select the Edit icon, a similar screen will appear.

The screenshot shows the 'Add Exception' form. At the top right is a close button (X). The 'Exception name' field is filled with 'qwr'. The 'Permission' field is set to 'Block'. The 'Description' field contains 'wrqw'. The 'Valid time' section shows 'Forever' selected. Below that is a 'Choose time' button and a 'Select date...' button with a calendar icon. The 'Device list (0)' section has an 'Add device' button. The 'Assignees' section has a radio button for 'All agent(s)' which is selected, and two other options: 'Choose agent(s) (0)' and 'Choose group(s) (0)'. At the bottom are 'Cancel' and 'Save' buttons.

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.



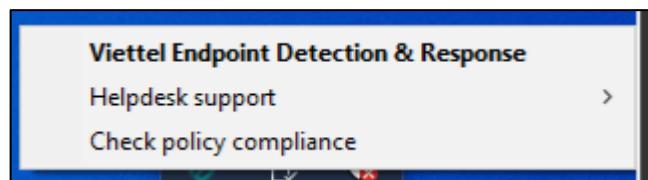
If the user selects the Delete Exception button, they agree to delete this exception. At this point, the portal will display a notification stating, "You have successfully deleted the exception."

Select Cancel to return to the Device list screen.

3.12 Main

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":



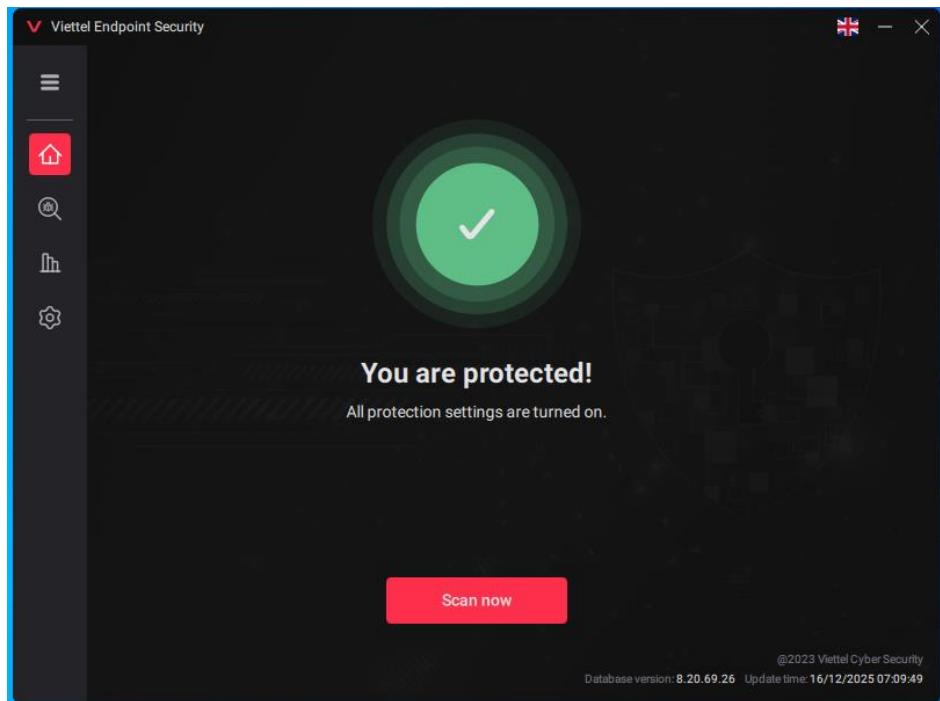
The system displays the following information:

- + 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 Protection

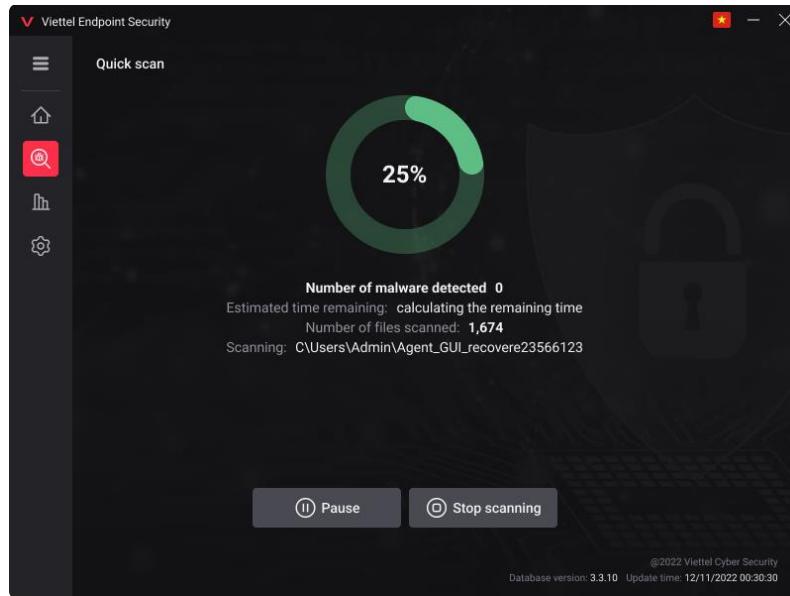
Purpose: to enable users to proactively use the system to scan and handle malware on their devices.

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:



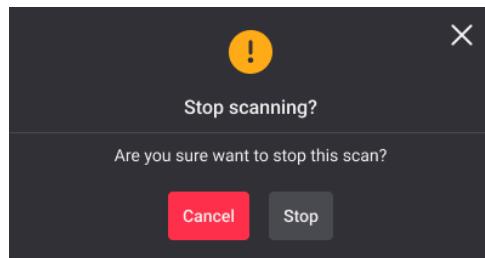
- + Display the total scan progress percentage
- + Display information on the number of detected malware samples
- + Display the estimated remaining time to complete the scan
- + Display the number of files that have been scanned
- + Display the file path being scanned

Support the following operations during scanning:

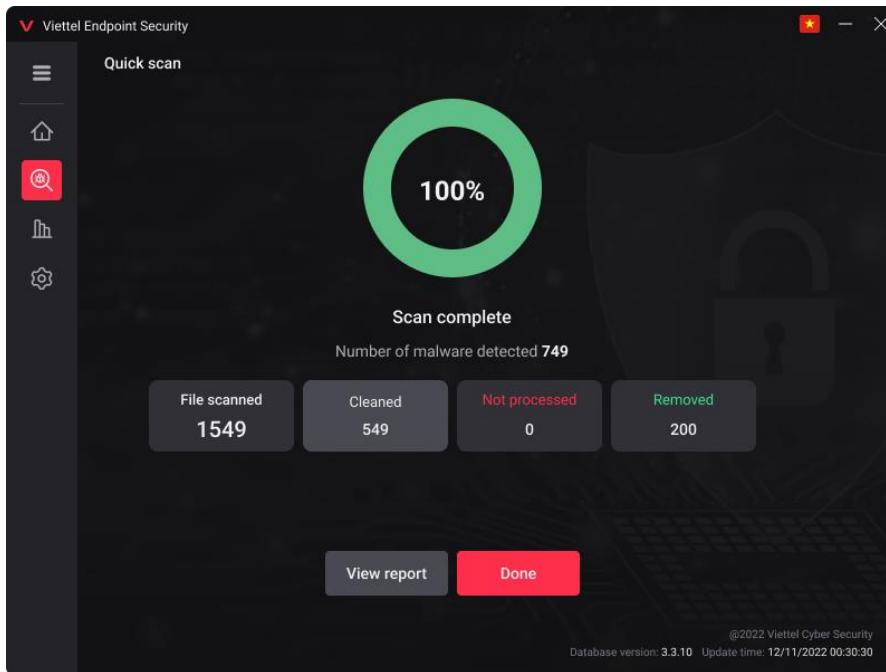
: Allow termination of the scanning process;

: 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.

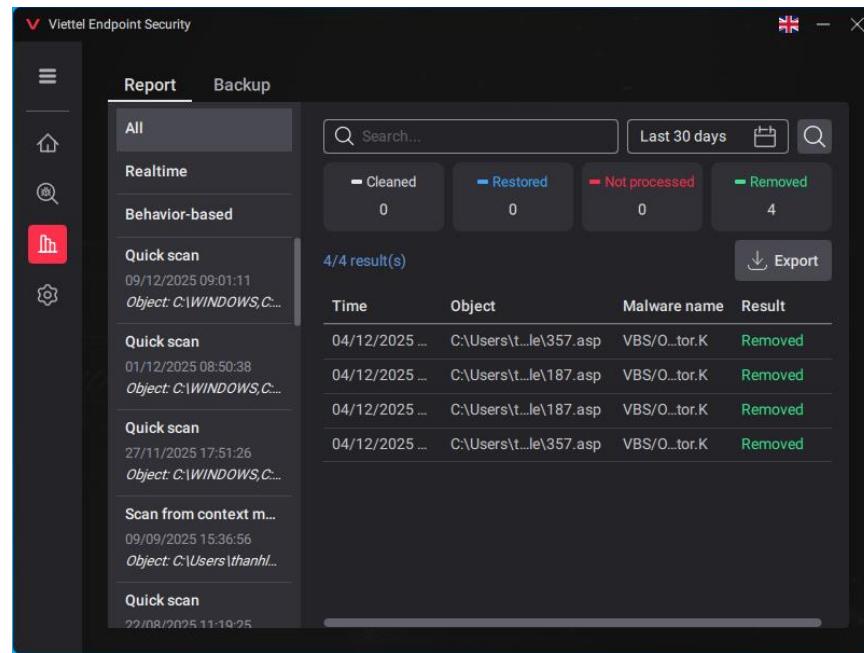
Click done to return to the main screen of Protection.

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.

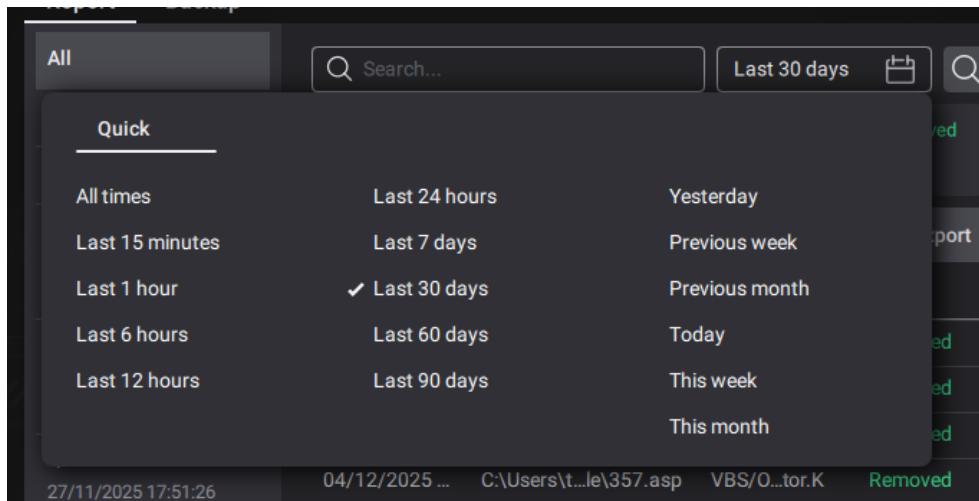
3.14 Report

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.



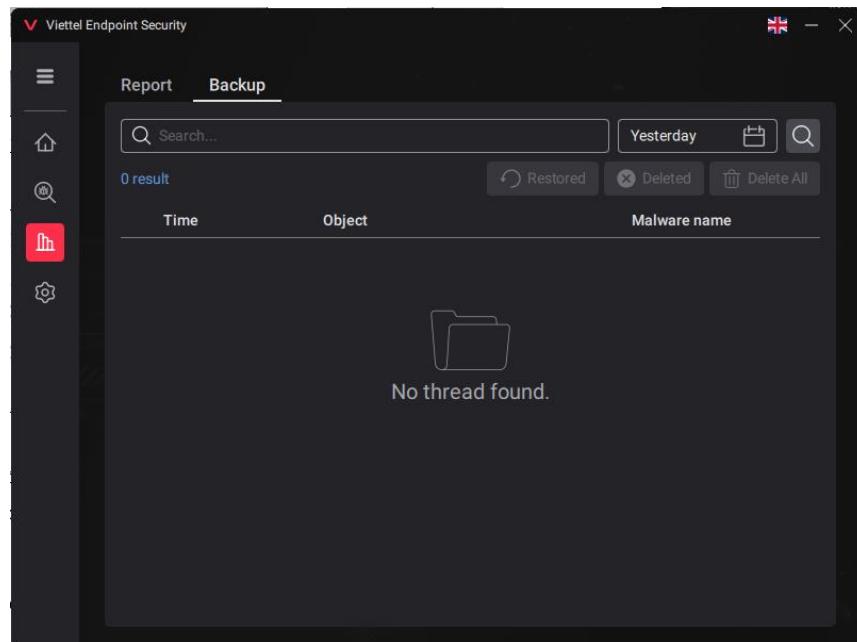
- Search by malware results

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."

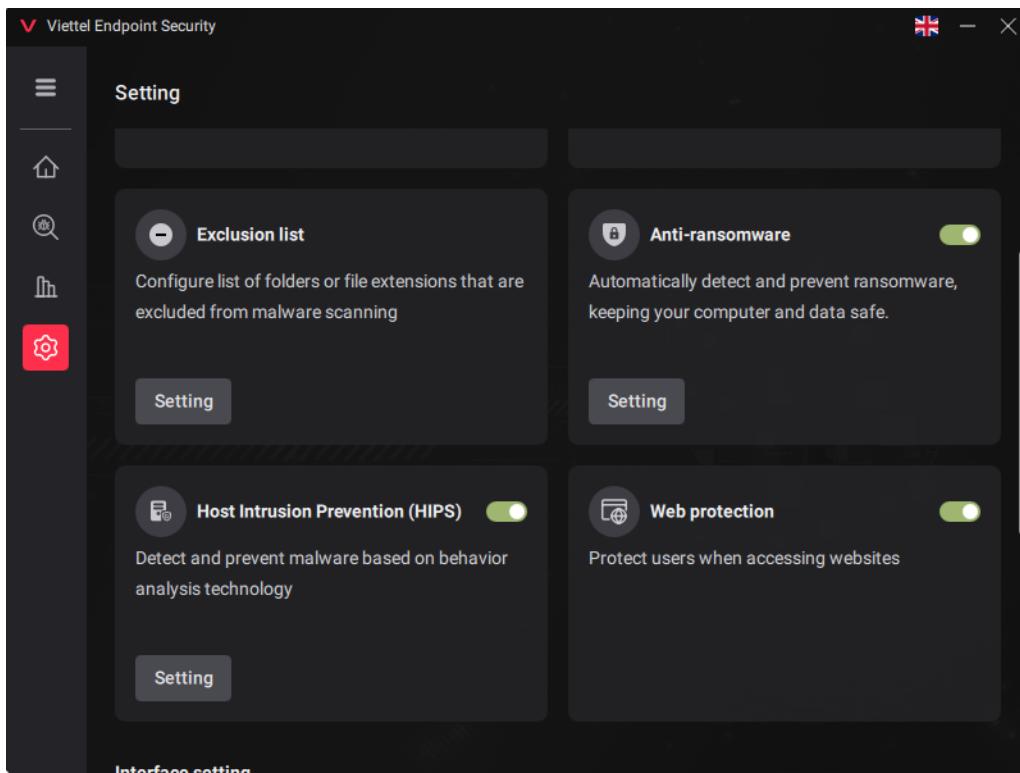
3.15 Setting

Purpose: Configuration settings on each agent machine

Allow searching all content within the settings page by keyword.

- 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



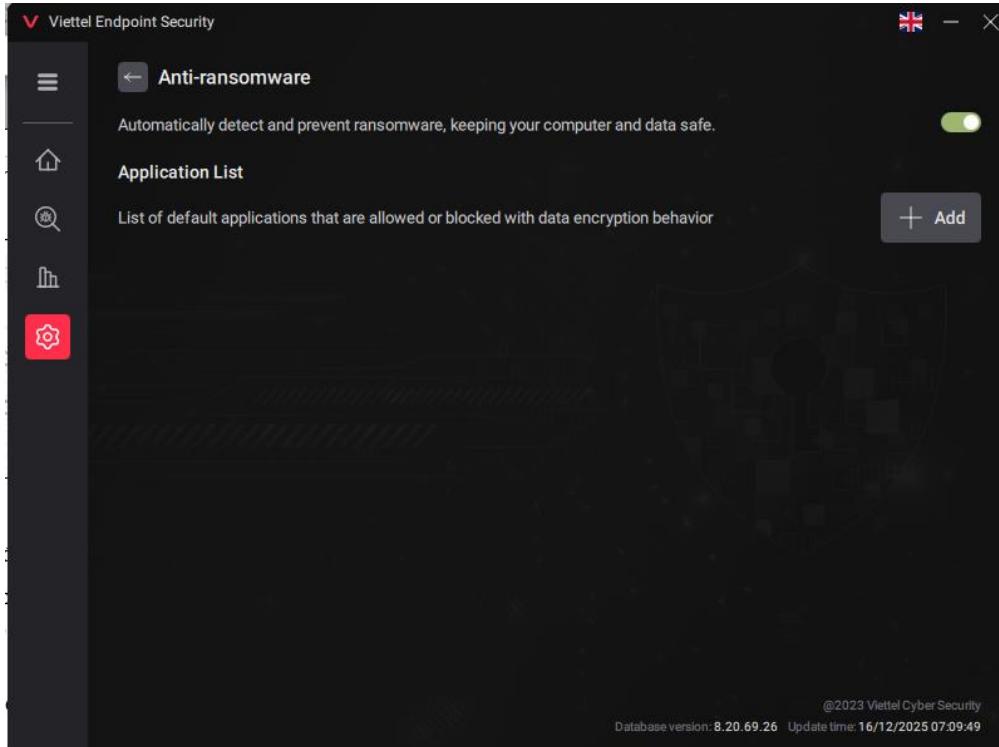
- Extension: Allows adding/editing Extensions (document file types) to be excluded (not scanned by Real-time Protection);

b. Interface setting

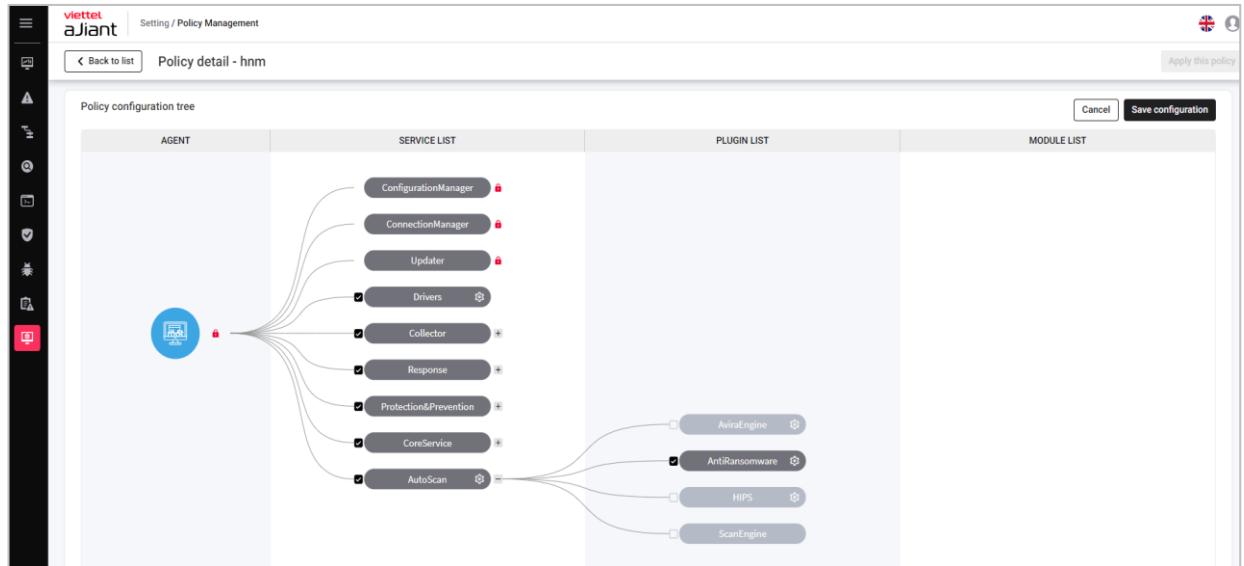
- Allow enabling/disabling Notifications → Display notifications on the device screen when a scan command is received from the system, upon detecting malware.
- Language: Allows selection of English/Vietnamese language

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 VESAutoScan

The command allows management of malware scanning, viewing reports, and backups of detected malware.

Run the command to list supported features.

```
$ 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 |
|-----+-----+-----+-----+-----+
|-----+
|     1 | 2025-07-10T17:46:32+07:00 | /usr,/home  | 30231 | 312,837      | 0   |
|-----+
|     2 | 2025-07-10T17:53:01+07:00 | /usr,/home  | 31795 | 312,838      | 0   |
|-----+
|-----+-----+-----+-----+-----+
|-----+
```

```
$ 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 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
```