Viettel Endpoint Detection & Response (VCS-aJiant)

Version 3.3.0 EPP – 2021

Update date: 29 Nov. 2021

User Guide

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Table of Contents

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Glossary

Terms	Description
VCS-aJiant	Trade name of the Viettel Endpoint Detection & Response product

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

1. Introduction

1.1. Current Situation

Today, organizations and enterprises continue to face many difficulties with the detection, identification, investigation and minimization of advanced malware forms in the system. Traditional anti-malware technologies such as signature-based anti-virus are being intentionally bypassed by highly skilled professional attackers with attack kits and malware customized and targeted to specific objects. Many organizations have acknowledged that their traditional anti-malware defense methods have failed and a new strategy must be created to identify these breaches at the endpoint. A significant number of recent data breaches from advanced malware forms have made the customer interest increase in the Endpoint Detection and Response (EDR) Solutions, in which VCS-aJiant is one of them.

1.2. Technology Development

The technology of the VCS-aJiant Solution improves the shortcomings of signature-based technologies that organizations are using such as anti-virus or IPS/IDS to provide the ability to detect the behavior-based anomalies and the deep insight into specific information related to endpoint to detect and minimize the advanced threats.

1.3. VCS-aJiant

VCS-aJiant is able to provide detailed information on malware infections and lateral movement behaviors of attackers as they perform scans or use information stolen in the intranet for systems and applications.

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

1.4. Upgraded Information

Version 3.3.0 provides the following new features:

- Provide Dashboard feature: The product supports a separate Dashboard for data analyzed from AV engine.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- Improve Agent Management feature, provide version information for the agent and the Installation File Version information tab and allow looking up version information of the agent installer and detailed files in the installer.
- Provide an Agent-side interface to monitor the information security situation at the machine and proactively scan malware for processing.
- Improve issues in the old version to ensure stability.

2. Overview

2.1. Technologies

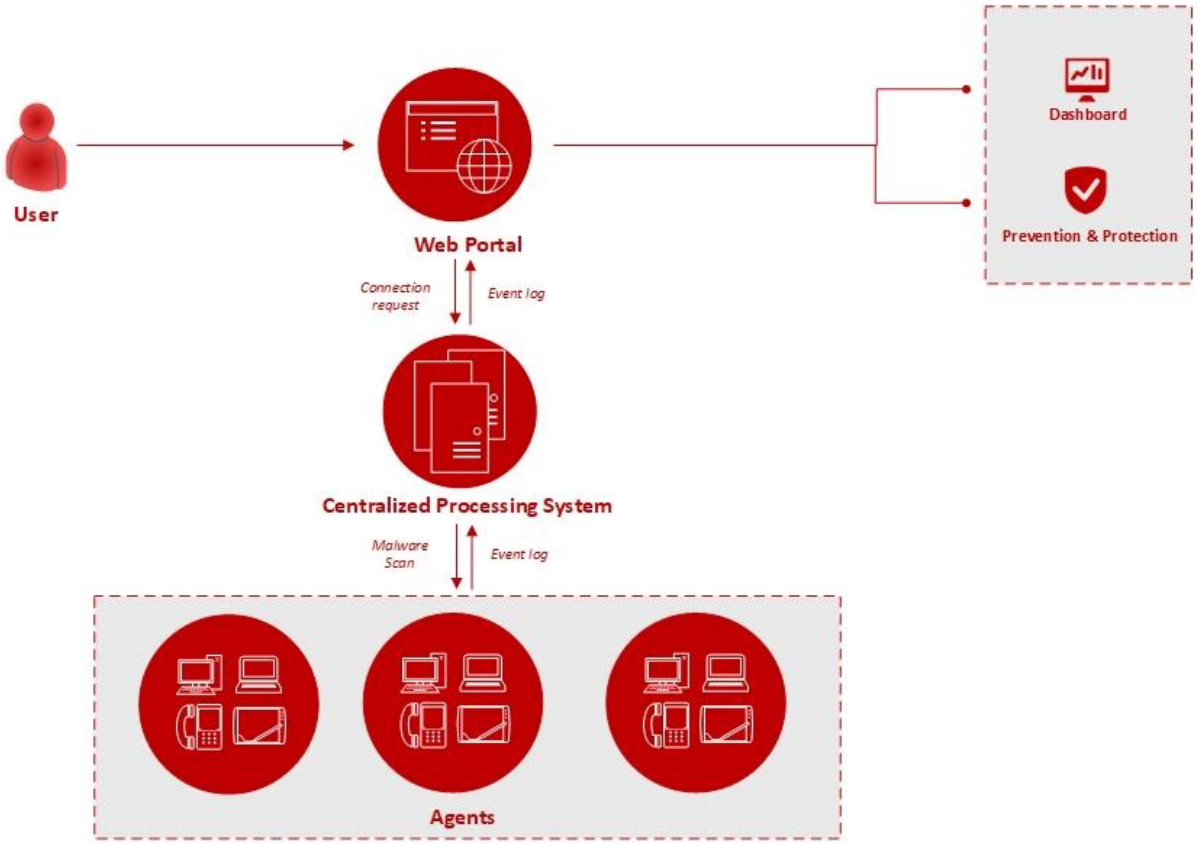
VCS-aJiant uses Filter Driver technology (allow to run and monitor at the Kernel-based level) to collect information, including Files, Processes, Registries, Networks on user computers and servers. The file signs include Modified, Delete and Changed attribute. The registry signs include Delete key/value, Set value, Rename key/value and Create key with suspicious access. The suspicious signs of Memory are periodically scanned. The behavior identified as Suspicious is pushed to the centralized analysis back-end system.

The attack investigation workflow is designed as a closed flow according to the incident response scenario (IR Flow) in order to support the detection and analysis of anomalous signs right on a single interface, provide deep investigation (Forensic) functions on Endpoint, support to get suspicious files (Get Artifact), push scanning tool (Tool Deployment), allow investigation implementation, provide evidence in real-time (Process Analysis and Live Response) and allow respond to a threat detected.

As soon as the anomaly is verified, Endpoint provides wide-ranging malware removal tools (Response Scenario), including: isolating the infected machine network (with network containment), killing process and deleting file/registry.

2.2. Infrastructure Architecture

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



There are 3 main components as follows:

- Agent: A component installed on each computer, responsible for monitoring abnormal signs, thoroughly preventing and removing malicious programs on the system and sending results to a centralized administration server.
- Cluster of servers for administration, centralized processing and storage: A component that processes data sent back from agents and plays a key role in data analysis and data processing in real time.
- Web-Portal interface: A component that the administrator will use to monitor and analyze the system's information.

2.3. Work with Admin Interface

Currently, VCS-aJiant provides 02 interfaces as follows:

- Web-portal interface: Include the following functional interfaces and processing flows:
  - Dashboard: Statistics and visual charts about the organization’s information security situation.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- Agent-side interface: Include the following functional interfaces and processing flows:
  - Main: A home page allows quickly viewing the information security status of agent installed machine
  - Reports: Reports on the situation of handling malware detected at the machine
  - Scan: Allow users to actively scan for malware with files and folders on the machine, including 3 mechanisms: Quick Scan, Full Scan and Custom Scan.
  - About: Provide version information and product support.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

3. Instruction to Use

3.1. WEB-PORTAL INTERFACE

3.1.1. Login

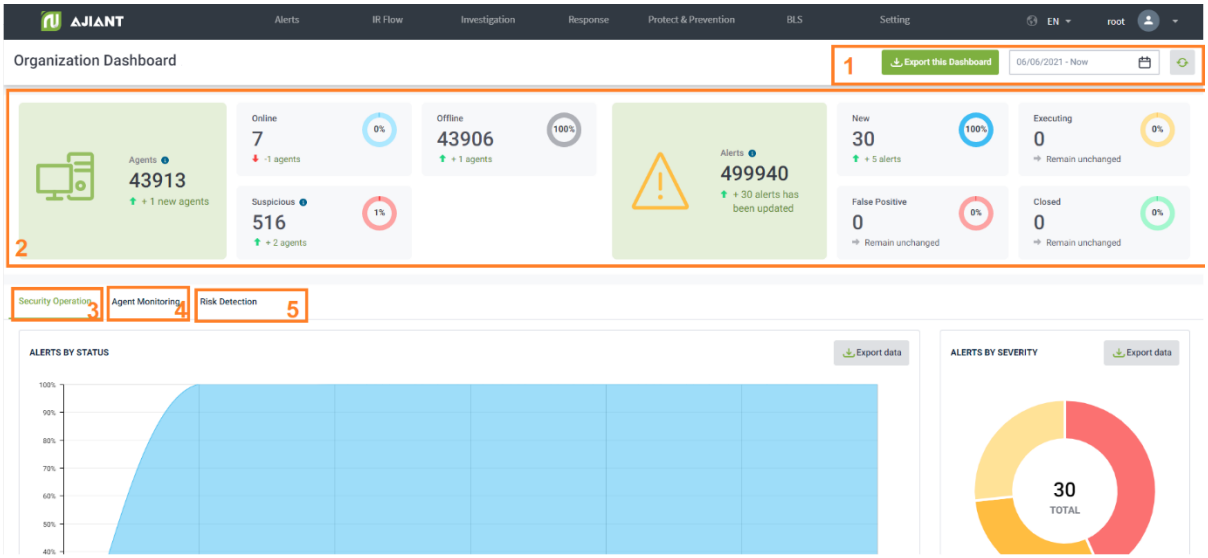
- Access the system at the provided address.

- Login with the provided user/password.

3.1.2. Dashboard VCS-aJiant (default)

- Main features include as follows:

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Action to data on Dashboard
  - Extract data on Dashboard
  - Search data up to the last 90 days
  - Refresh data.
- Overview: An overview statistics of the organization's information security situation (through agent and alert state).
- Security Operation: Monitor information security operation situation (through alert operation monitor).
- Agent Monitoring: Monitor installation state and agent state.
- Risk Detection: Track threats to the organization (through the statistics of the objects generating the most unprocessed alerts in the system).

- Data authorization at the features is as follows:
  - User login under root group: Display data of the entire system.
  - User login in 1 level group: Display data at all 1 level group and affiliated subgroups.
  - User login in 2 level group onwards: Display data at the entire 1 level group containing the group of the user login and the affiliated subgroups of the corresponding 1 level group.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

3.1.2.1. Action to Data

3.1.2.1.1. Export Data

Allow exporting the existing data on the Dashboard interface by selecting 

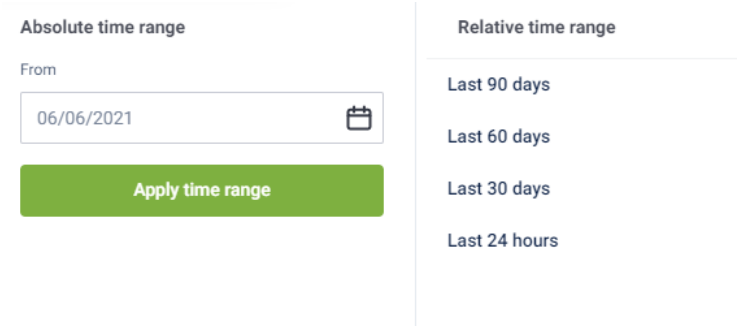
, in addition to adding the detailed data sheets to support reports.

- In case of connection failure or no data on all components of Dashboard, the export is not supported and the action will be hidden.
- In case of having data, support to export files in .xlsx format.

3.1.2.1.2. Search by Date

Allow adjusting the time range to monitor the information security situation up to the current time with the default time from the last day.

- To select the start-time range to monitor, enable to choose absolute or relative time range as follows:



  - Absolute time range: A specific start date value and up to 90 days from the current date supported.

For example, it is currently 3 am on 7 June 2021, select start date = "06/06/2021". → Monitoring period: 00:00 6 June 2021 to 03:00 6 July 2021.

  - Relative time range: A relative time range between the start date and the current date.

For example, it is currently 3 am on 7 June 2021, select start date = “Last 30 days”. The system automatically searches the last 30 days and starts counting from 00:00 of that day. → Monitoring period: 00:00 8 May 2021 to 03:00 7 June 2021.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- After selecting the time range to monitor, select 

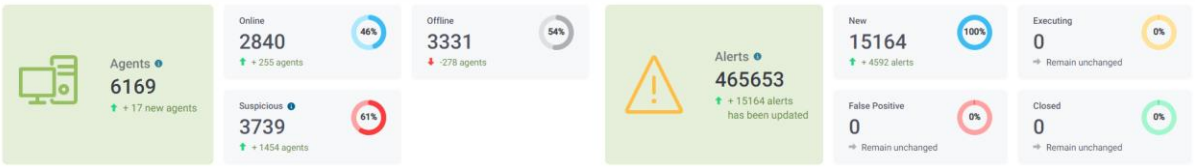
to reload the corresponding data.

3.1.2.1.3. Refresh Data

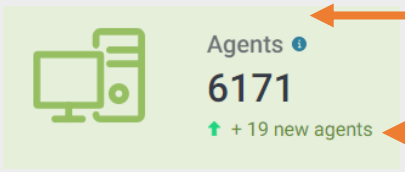
Allow refreshing manual data, select  to update the latest data up to the current time.

3.1.2.2. Overview Statistics

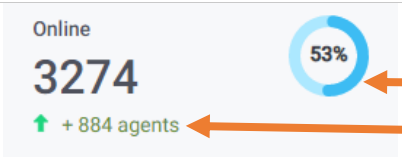
Allow quick statistics on the information security situation at the organization according to the selected time range in the search section.



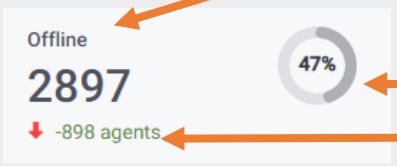
- Statistics related to agents

Statistics	Meaning
	Include 2 numbers as follows: Total number of machines with agent installed in the system (regardless of search time range) Total number of new machines with agent installed during the search time range (+: Newly installed machine, Remain unchanged: No newly installed machine during the search time range).
	Include 3 numbers as follows: Average number of online machines during the search time range (only counting working time during office hours from 08:00 - 18:00) Average number rate of online machines compared to the whole system

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

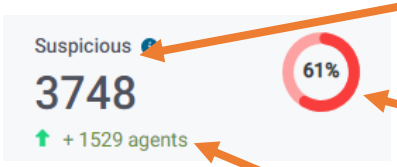


Average number of online machines different from the previous cycle.
(+: Average number of online machines increased compared to the previous time range, Remain unchanged: No difference).



Include 3 numbers as follows:

Average number of offline machines in the search time range (only counting working time during office hours from 08:00 - 18:00)
Average number rate of offline machines compared to the whole system
Average number of offline machines different from the previous cycle.
(+: Average number of offline machines increased compared to the previous time range, Remain unchanged: No difference).



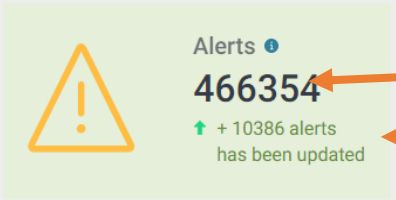
Include 3 numbers as follows:

Total number of machines with agent installed in the system (regardless of search time range) generating unprocessed alerts
Rate of machines generating alerts compared to the number of machines in the whole system (regardless of search time range)
Total number of machines generating alerts during the search time range
(+: New machines generating alerts, Remain unchanged: No new machine generating alerts during the search time range).

- Statistics related to alerts

Statistics	Meaning

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

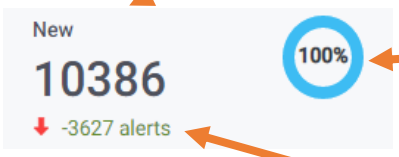


Include 2 numbers as follows:

Total number of alerts in whole system (regardless of search time range)

Total number of new alerts generated or updated during the search time range

(+: New alerts generated, Remain unchanged: No new alert generated during the search time range).



Include 3 numbers as follows:

Total number of new alerts generated or updated during the search time range and in the NEW state

Rate of new alerts generated or updated during the search time range in the NEW state compared to all new alerts generated or updated during the search period time range

Total number of new alerts generated or updated during the search time range and in the NEW state different from the previous cycle.

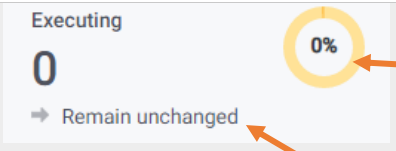
(+: Total number of new alerts increased from the previous time range, Remain unchanged: Total number of new alerts remained unchanged from the previous time range).

Include 3 numbers as follows:

Total number of new alerts generated or updated during the search time range and in the <> (NEW, FALSE POSITIVE, CLOSED) state

Rate of new alerts generated or updated during the search time range and in the <> (NEW, FALSE POSITIVE, CLOSED) state

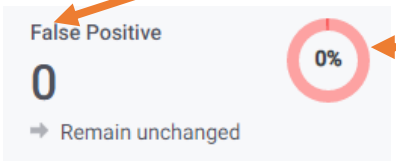
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



compared to all new alerts generated or updated during the search time range

Total number of new alerts generated or updated during the search time range and in the <> (NEW, FALSE POSITIVE, CLOSED) state different from the previous cycle.

(+: Total alert increased compared to the previous time range, Remain unchanged: Total number of alerts remained unchanged from the previous time range).



Include 3 numbers as follows:

Total number of new alerts generated or updated during the search time range and in the CLOSED state

Rate of new alerts generated or updated during the search time range and in the CLOSED state compared to all new alerts generated or updated during the search time range

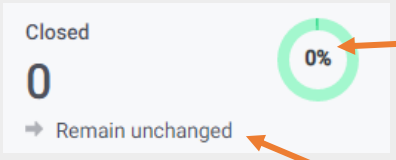
Total number of new alerts generated or updated during the search time range and in the CLOSED state different from the previous cycle

(+: Total alert increased compared to the previous time range, Remain unchanged: Total number of alerts remained unchanged from the previous time range).

Include 3 numbers as follows:

Total number of new alerts generated or updated during the search range time and in the FALSE POSITIVE state

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Rate of new alerts generated or updated during the search time range and in the FALSE POSITIVE state compared to all new alerts generated or updated during the search time range

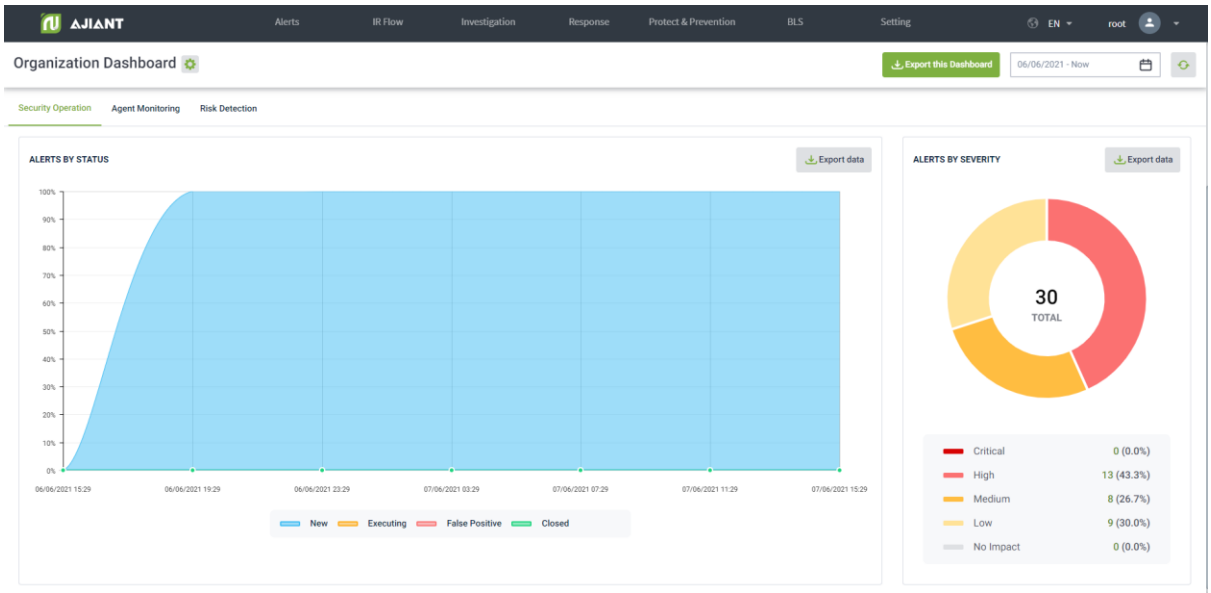
Total number of new alerts generated or updated during the search time range and in the FALSE POSITIVE state different from the previous cycle.

(+: Total alert increased compared to the previous time range, Remain unchanged: Total number of alerts remained unchanged from the previous time range).

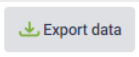
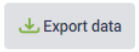
3.1.2.3. Monitor Security Operation

Allow monitoring the information security operation situation (through alert operation monitor) according to the selected time range in the search section, including:

- Statistic of alert process state by state
- Statistic of alert by severity
- Corresponding data export in the charts.



Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

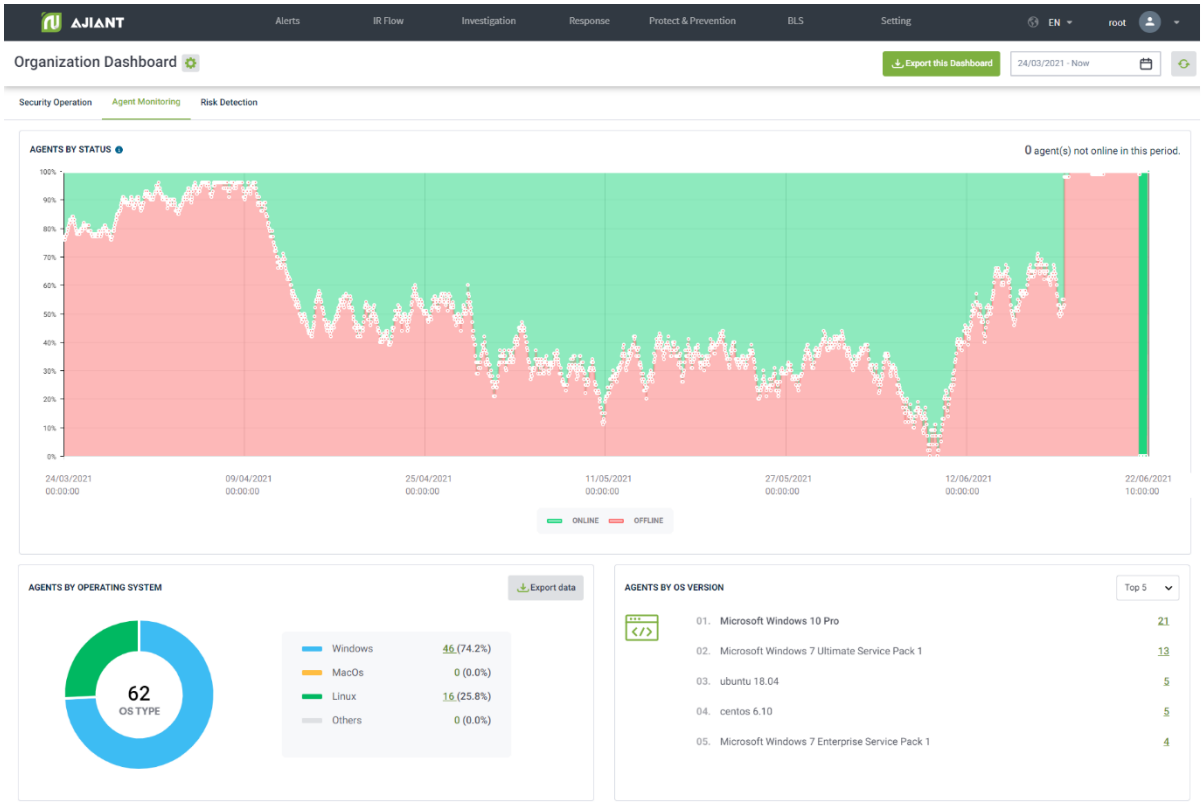
Charts/Statistics	Meaning
Alert by state	Domain chart: Monitor the state of newly recorded or updated alerts during the search time range, including: • X-axis: Time • Y-axis: Alert rate divided by 4 state groups (New, Executing, Closed and False Positive) • Allow selecting  to download alert lists sorted by state.
Alert by severity	Pie chart: Monitor the state of newly recorded or updated alerts by severity during the search time range, including: • Rate: Alert rate at each severity • Total number of new or updated alerts in a time range is displayed in the middle of the chart. • Allow selecting  to download alert lists sorted by severity.

3.1.2.4. Agent Monitoring

Allow statistics of agents by state and operating system information according to the selected time range in the search section, including:

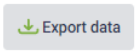
- Agent state statistics (online and offline)
- Agent statistics by operating system and operating system version
- Agent data export.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Charts/Statistics	Meaning
Agent by state	Domain chart: Monitor the state of machine recognition by state (Online/Offline) in the report cycle up to the current time, including: • Y-axis: Rate of machine divided by 2 state groups (Online and Offline) • X-axis: Statistical time • Display the number of machines that are not online at all (in case the machine is not online for more than 30 days, the machine is not automatically recognized).
Agent by operating system	Pie chart: Monitor the state of machine recognition by operating system (OS), including: • Rate: Machine rate at each OS

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

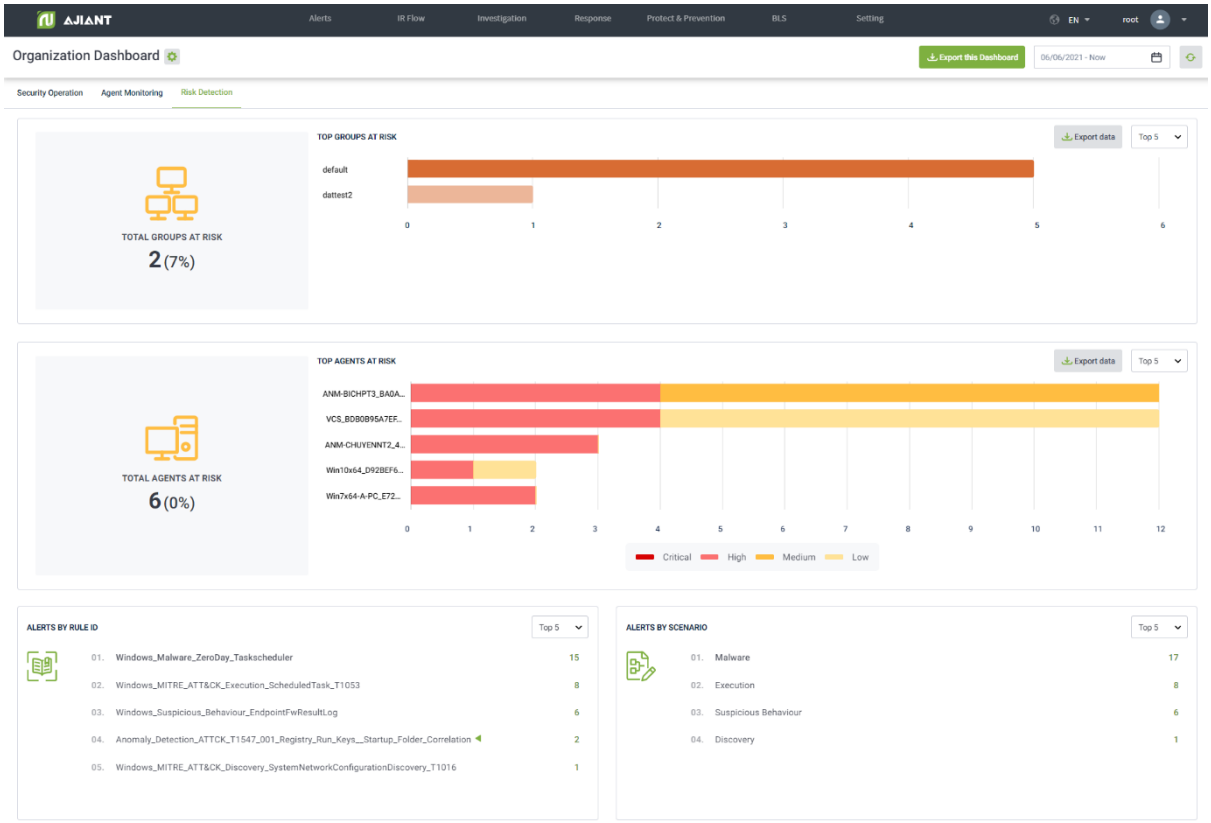
	• The notes section lists the OS list: Windows, MacOS, Linux and other operating systems. • Allow selecting  to download machine lists sorted by OS information.
Agent by OS version	Statistics on the top OS versions installed on the machines. • Allow changing the statistical period: Top 5, Top 10, Top 20, Top 50. Default is Top 5.

3.1.2.5. Monitor Risk Detection

Allow monitoring of threats to the organization (through the statistics of the objects that generate the most unprocessed alerts in the system), including:

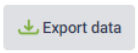
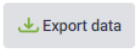
- Statistics of top groups that generate the most alerts.
- Statistics of top agents that generate the most alerts.
- Statistics of the top RuleIDs and scenarios that generate the most scenes.
- Export the information data according to dangerous objects.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Charts/Statistics	Meaning
Total groups at risk	Total number of groups containing computers with newly recorded or updated alerts (excluding false positive and closed alerts, excluding deleted groups) during the search time range. Rate of suspicious groups to the entire group in the system (excluding deleted groups).
Top groups at risk	Column chart: Statistic of top groups containing many computers with the most newly recorded or updated alerts (excluding false positive and closed alerts, excluding deleted groups) during the search time range, including: • X-axis: Number of machines generating multiple alerts in each group

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

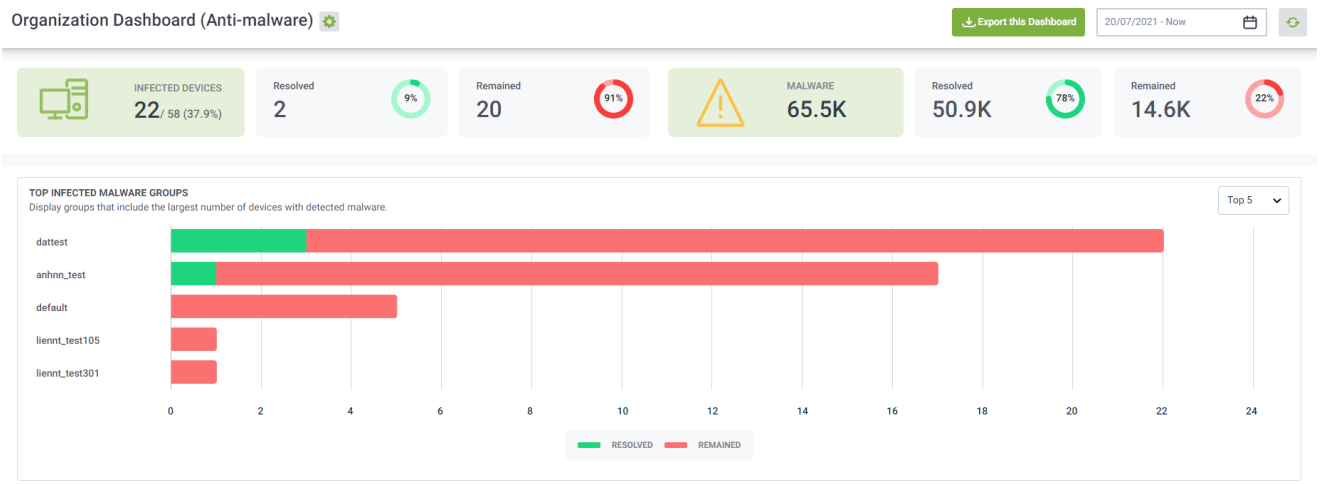
	• Y-axis: Corresponding group name • Allow changing the statistical interval: Top 5, Top 10, Top 20, Top 50. Default is Top 5. • Allow selecting  to download computer lists that generate alerts.
Total agents at risk	Total number of computers with newly recorded or updated alerts (excluding false positive and closed alerts, excluding computers that have been inactive for more than last 30 days) during the search time range. Rate of suspicious machines compared to all computers in the system (excluding computers that have been inactive for more than last 30 days).
Top agents at risk	Column chart: Statistic of top computers with the most newly recorded or updated alerts (excluding false positive and closed alerts) during the search time range, including: • X-axis: Number of alerts at each host, clearly divided by severity (Critical, High, Medium and Low) • Y-axis: Corresponding machine name • Allow changing the statistical period: Top 5, Top 10, Top 20, Top 50. Default is Top 5. • Allow selecting  to download computer lists that generate alerts.
Alerts by RuleID	Statistics of top RuleID with the most newly recorded or updated alerts during the search time range, including: • Allow changing the statistical period: Top 5, Top 10, Top 15, Top 20. Default is Top 5.
Alerts by Scenarios	Statistics of top Scenario with the most newly recorded or updated alerts in the report cycle up to the current time, including:

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

	• Allow changing the statistical period: Top 5, Top 10, Top 15, Top 20. Default is Top 5.

3.1.3. Anti-malware Dashboard

The function provides visual charts to monitor the organization's information security situation through data related to the removal of malware.



- Main features include a set of as follows:

  - Action to data on Dashboard
    - Export data on Dashboard
    - Search data up to the last 90 days
    - Refresh data.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- Overview: An overview of the organization's information security situation (through the device and threat state)
- Risk Detection: Track threats to the organization (through the statistics of objects that generate the most malware in the system).

- Data authorization at the feature is as follows:
  - Allow displaying all data, not by unit.

3.1.3.1. Action to Data

3.1.3.1.1. Export Data

Allow exporting the existing data on the Dashboard interface by selecting 

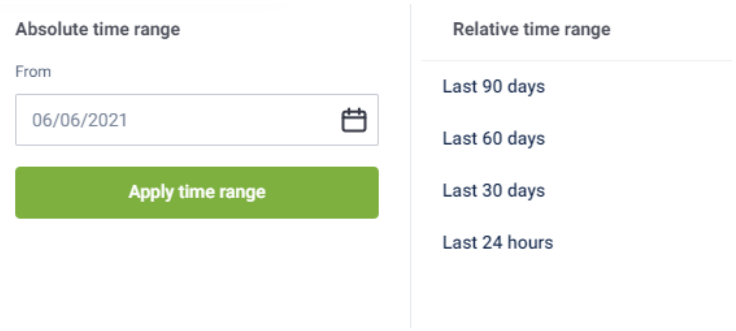
, in addition to adding the detailed data sheets to support reports.

- In case of connection failure or no data on all components of Dashboard, the export is not supported and the action will be hidden.
- In case of having data, support to export files in .xlsx format.

3.1.3.1.2. Search by Date

Allow adjusting the time range to monitor the information security situation up to the current time with the default time from the last day.

- To select the start-time range to monitor, enable to choose absolute or relative time range as follows



  - Absolute time range: A specific start date value and up to 90 days from the current date supported.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

For example, it is currently 3 am on 7 June 2021, select start date = "06/06/2021". → Monitoring period: 00:00 6 June 2021 to 03:00 6 July 2021.

- Relative time range: A relative time range between the start date and the current date.

For example, it is currently 3 am on 7 June 2021, select start date = “Last 30 days”. The system automatically searches the last 30 days and starts counting from 00:00 of that day. → Monitoring period: 00:00 8 May 2021 to 03:00 7 June 2021.

- After selecting the time range to monitor, select 

to reload the corresponding data.

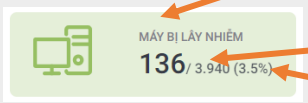
3.1.3.1.3. Refresh Data

Allow refreshing manual data, select  to update the latest data up to the current time.

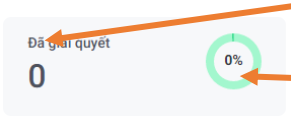
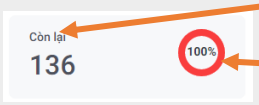
3.1.3.2. Overview Statistics

Allow quick statistics on the information security situation at the organization according to the selected time range in the search section.

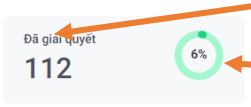
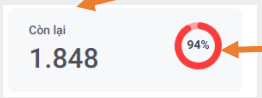
- Statistics related to agents

Statistics	Meaning
	Include 3 numbers as follows: Total number of infected machines in the system during the search range Total number of agent installed machines in the system (excluding search time range) Rate of infected machines compared to all agent installed machines in the system.
	Include 2 numbers as follows: Total number of infected machines in the system processed successfully

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

	Rate of infected machines processed successfully compared to all infected machines in the system.
	Include 2 numbers as follows: Total number of infected machines in the system failed to process Rate of infected machines failed to process compared to all infected machines in the system.

- Statistics related to alerts

Statistics	Meaning
	Include 1 number as follows: Total number of malware recorded in the entire system.
	Include 2 number as follows: Total number of malware in the system processed successfully Rate of malware processed successfully compared to all malware recorded on the system.
	Include 2 number as follows: Total number of malware in the system failed to process Rate of malware in the system failed to process compared to all malware recorded in the system.

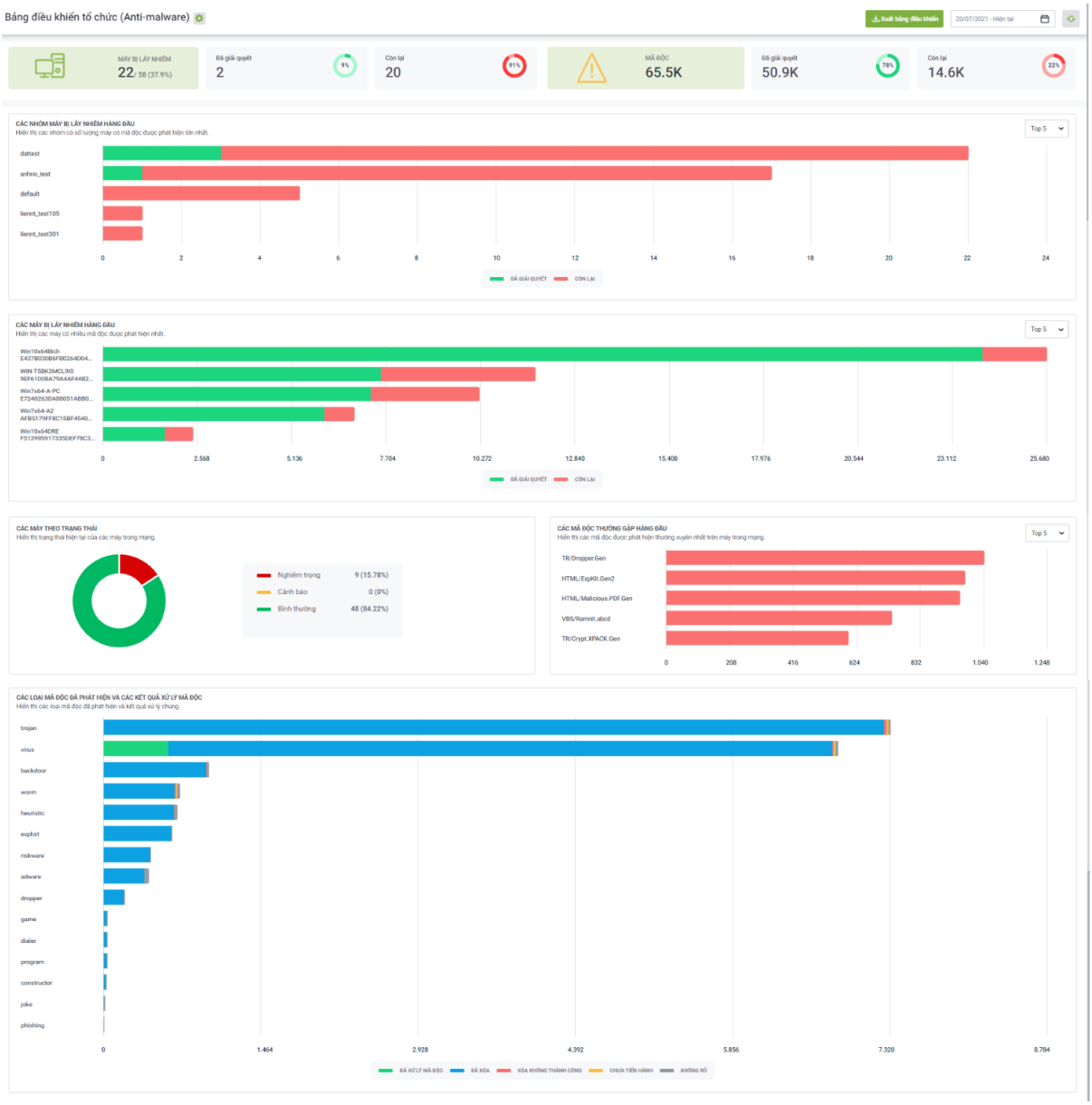
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

3.1.3.3. Monitor Risk Detection

Allow monitoring of threats to the organization (through the statistics of the most malware infected objects in the system).

- Statistics of top infected groups
- Statistics of top infected machines
- Statistics of machines by state
- Statistics of common malware
- Statistics of virus handling status

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Charts/Statistics	Meaning
Top infected device groups	Column chart: List the machine group with the most malware infected machines in the search time up to the present time, including: • X-axis: Number of infected machines in each group by processing state (Resolved - machine with all

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

	processed malware and Remain - machine with at least 1 unprocessed malware) • Y-axis: Name of the corresponding machine group • Allow to change the statistical interval: Top 5, Top 10, Top 20, Top 50. The default is Top 5.
Top infected devices	Column chart: List the most malware infected machines in the search time up to the present time, including: • X-axis: Number of infected malware by processing state (Resolved and Remain) • Y-axis: Name of the corresponding machine • Allow to change the statistical interval: Top 5, Top 10, Top 20 and Top 50. The default is Top 5.
Devices by status	Pie chart: Monitor the machine's status in the system according to the current status, including: • Rate: Rate of machines at each status compared to the total number of machines.
Top frequent threats	Column chart: List the most infected malware in the search time up to the present time, including: • X-axis: Number of generated malware • Y-axis: Name of malware • Allow to change the statistical interval: Top 5, Top 10, Top 20 and Top 50. The default is Top 5.
Types of detected viruses and disinfected results	Column chart: List viruses appearing in the search time up to the present time (sorted by the number of viruses in descending order), including: • X-axis: Number of viruses generated by processing status • Y-axis: Virus name.

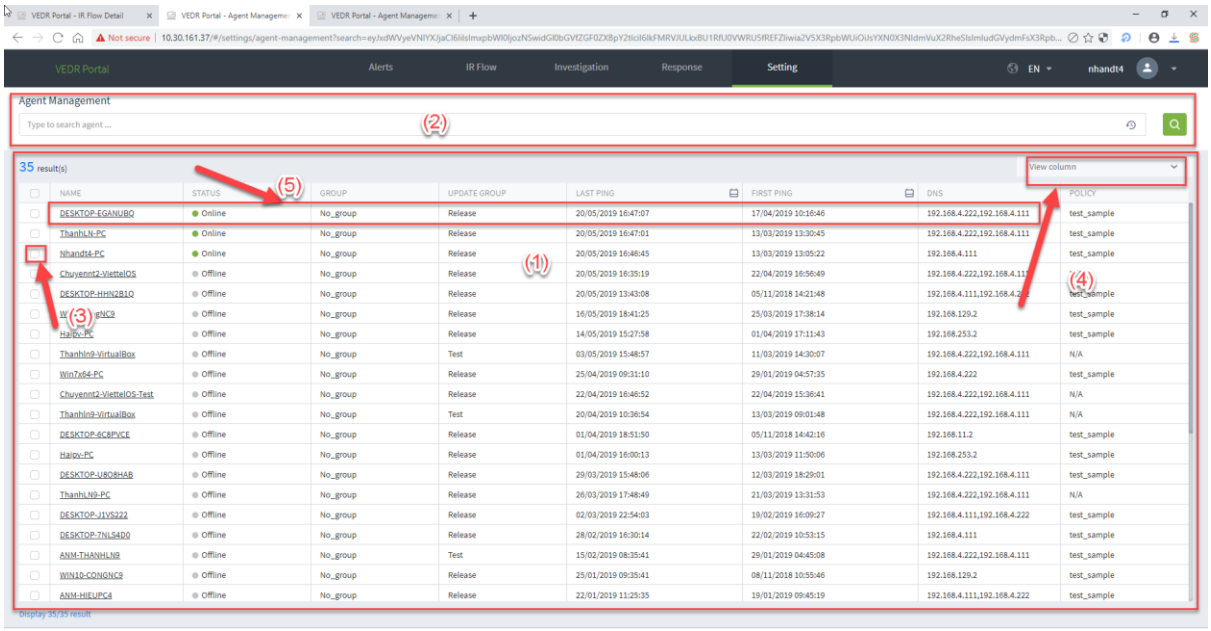
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

3.1.4. Setting Screen

3.1.4.1. Agent Management

Agent Management function supports administrators to manage installed agents, including:

- View Agent List and general information
- View details of Agent
- Quickly select Agents and set some settings (policy, update group).

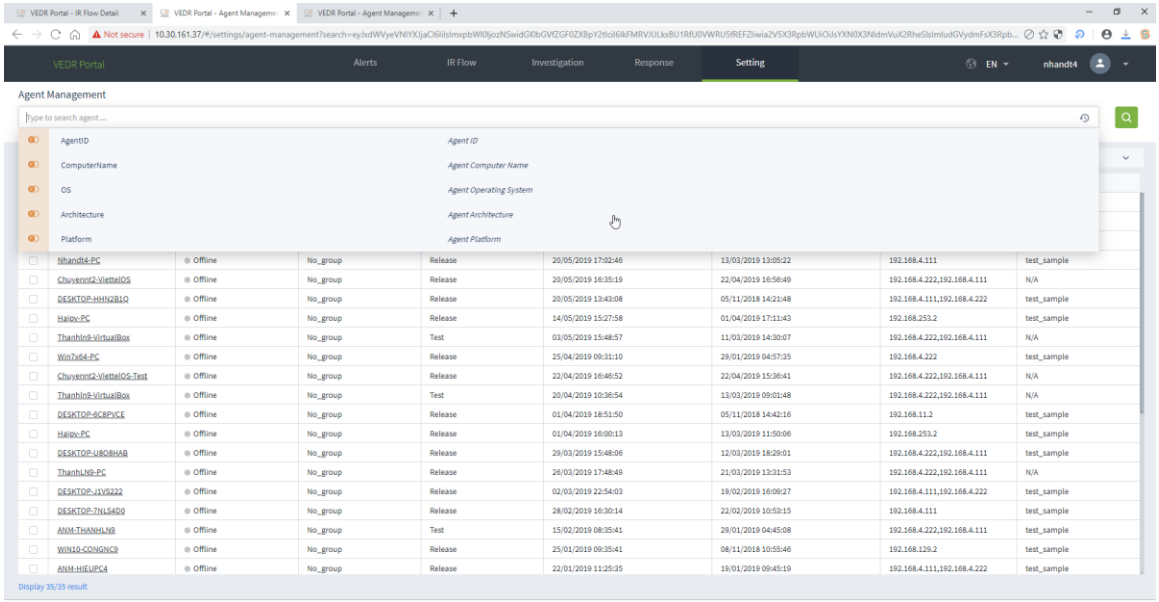


The system support performing the following features:

- View the Agent List installed on the system:
  - User login under root group: Display all Agents in active system < 30 days.
  - User login under default group: Display all Agents in the default group.
  - User login under parent-level group: Display all Agents in the group of the user logging in and the corresponding child-level group.
  - User login under a child-level group or many child-level groups: Display all Agents belonging to the group of the user logging in.
  - Each agent is displayed general information, including: Name, Status, Group, Update Group, Last Ping, First Ping, DNS, Policy, Agent ID, Platform, Platform Version, Architecture, DNS and Version.

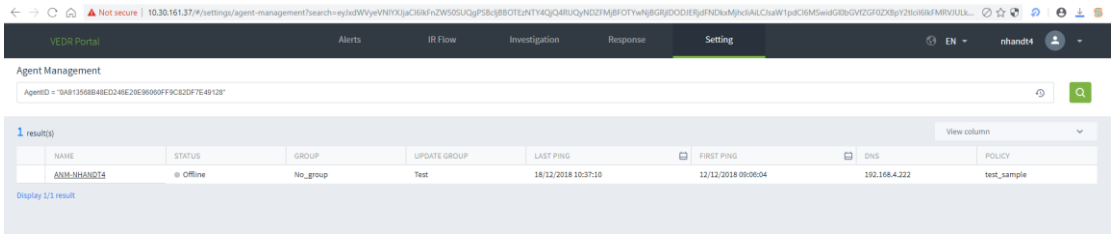
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- Support searching for Agent by Agent ID, ComputerName, OS, Architecture, Platform, Policy, IPDCN, Online, Update Group, Group ID, IP, Mac and Version. For each search criteria, search operators “=”, “!=” and “~” are supported.



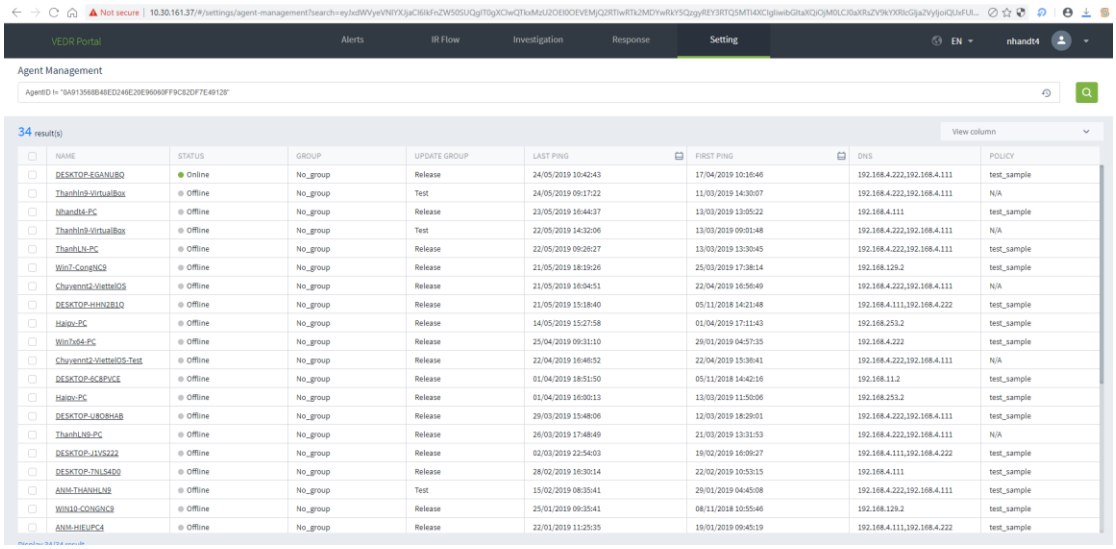
- Examples of search statements as follows:

Search by the condition “=”:

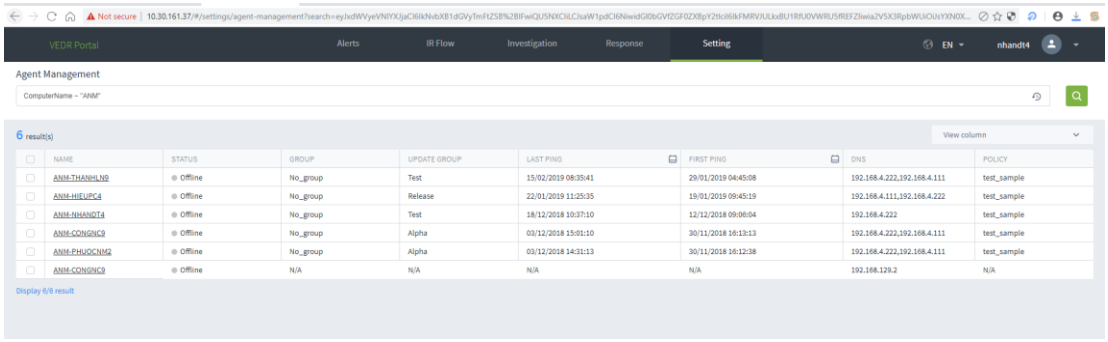


Search by the condition “!=”:

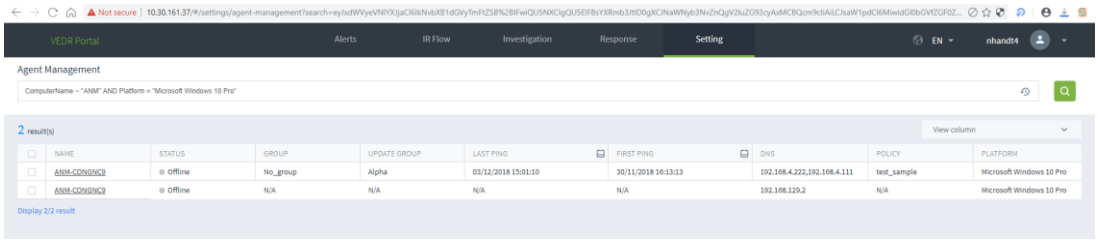
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Search by the condition “~”:

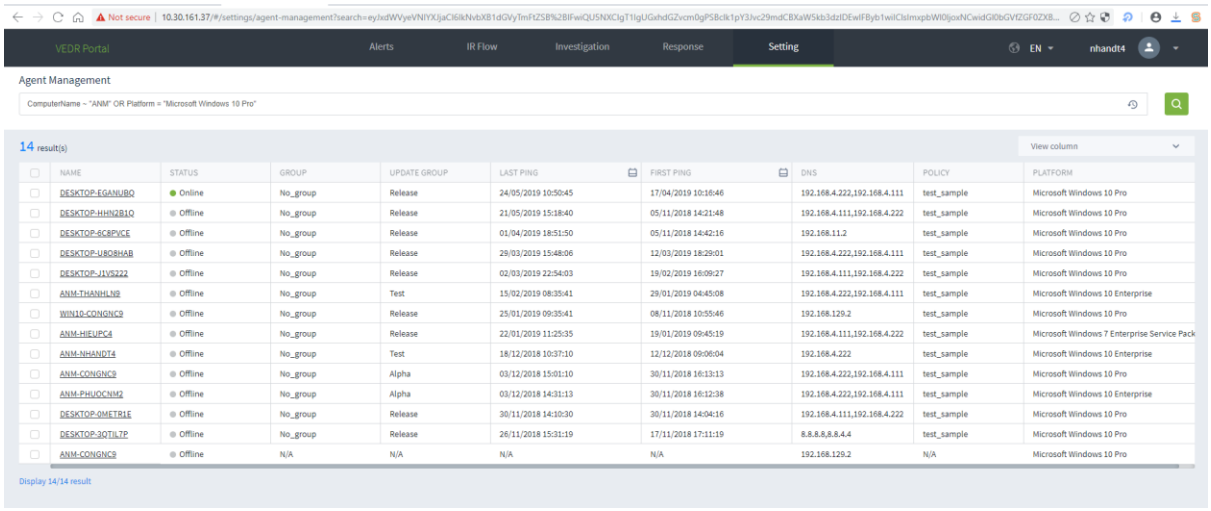


Search by AND match criteria:

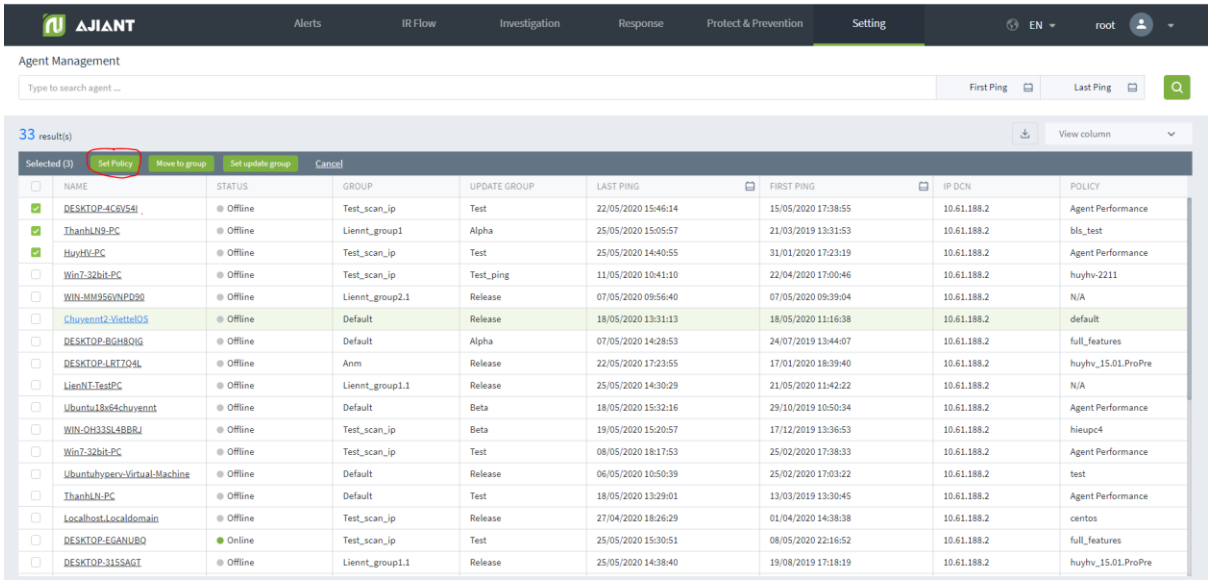


Search by OR match criteria:

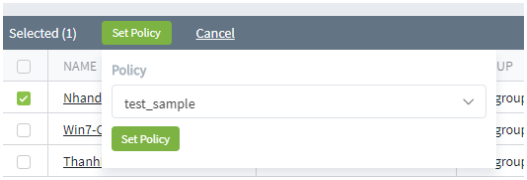
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Quickly select 1 agent/ 1 group of agents to set policy as follows:

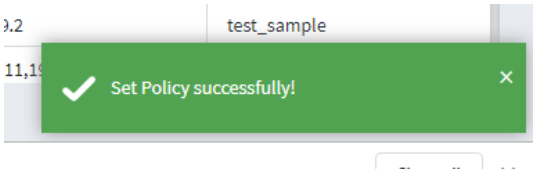


  - Tick to select 1 agent or multiple agents to enter the Multi-selected session.
  - Perform Set Policy.



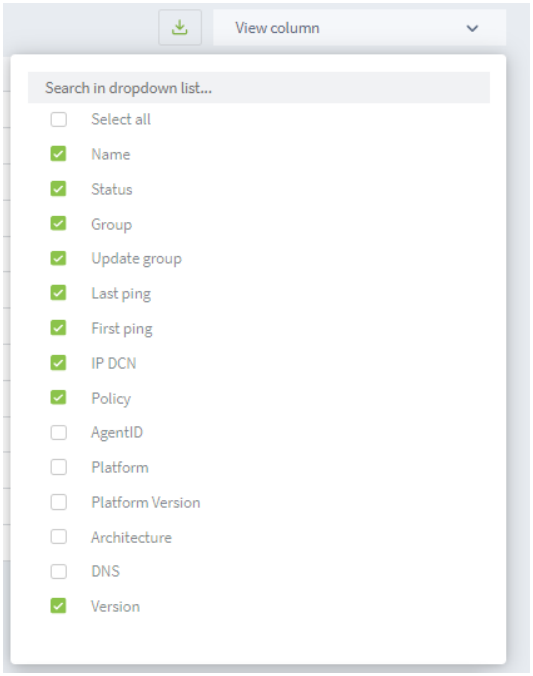
  - Result after setting policy:

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Delete the action on the Multi-selected screen

- View Column: Configure the display of columns at will:



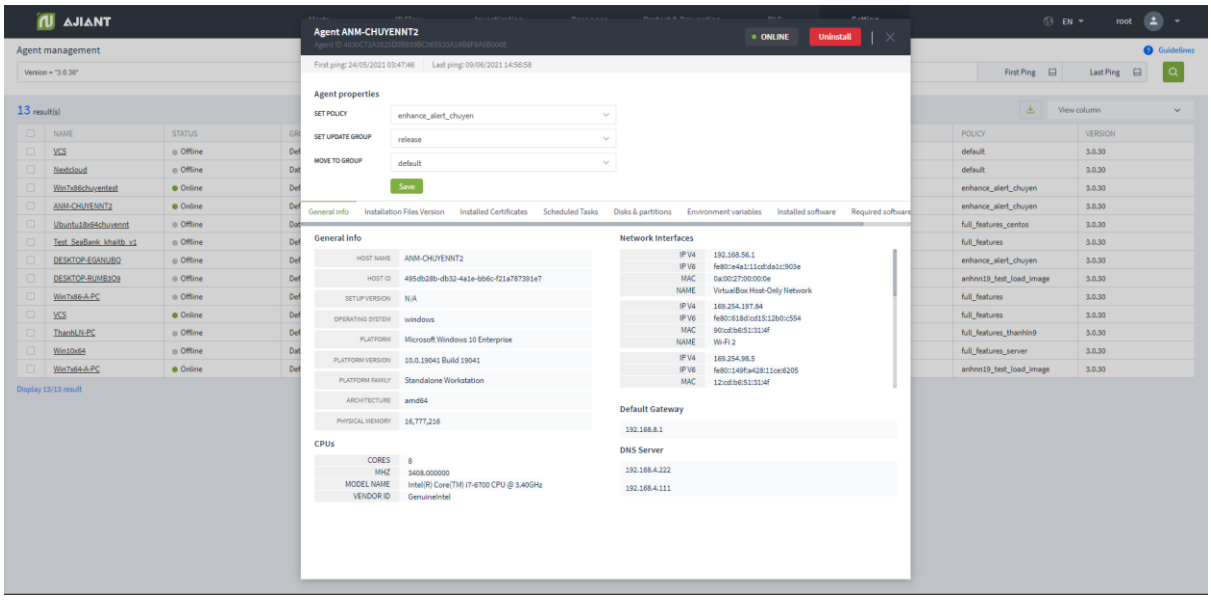
- View details of an agent by clicking duplicate the mouse on any row

The system supports users to perform Set Policy, Update Group and Move to group for Agent quickly.

- User login under root group: Display all Groups in the system.
- User login under default group: Display default Group.
- User login under parent-level group: Display all the Groups belonging to the user logging in and the users belonging to the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all Groups belonging to the user logging in.
    - Tab General Info Tab

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

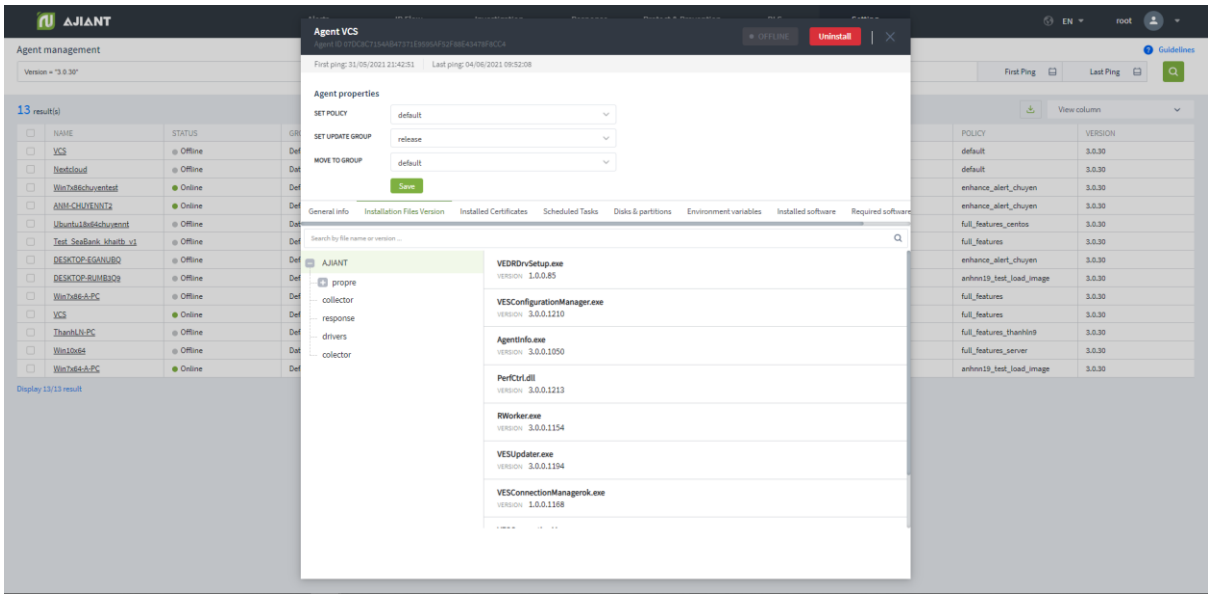
The system displays general information about the agent, including: General information, CPUs, Network Interfaces, Default Gateway and DNS Server.



- Installation Files Version Tap

Statistics of all agent installation files, including the following information: Name of folder containing installation file, File name and Version.

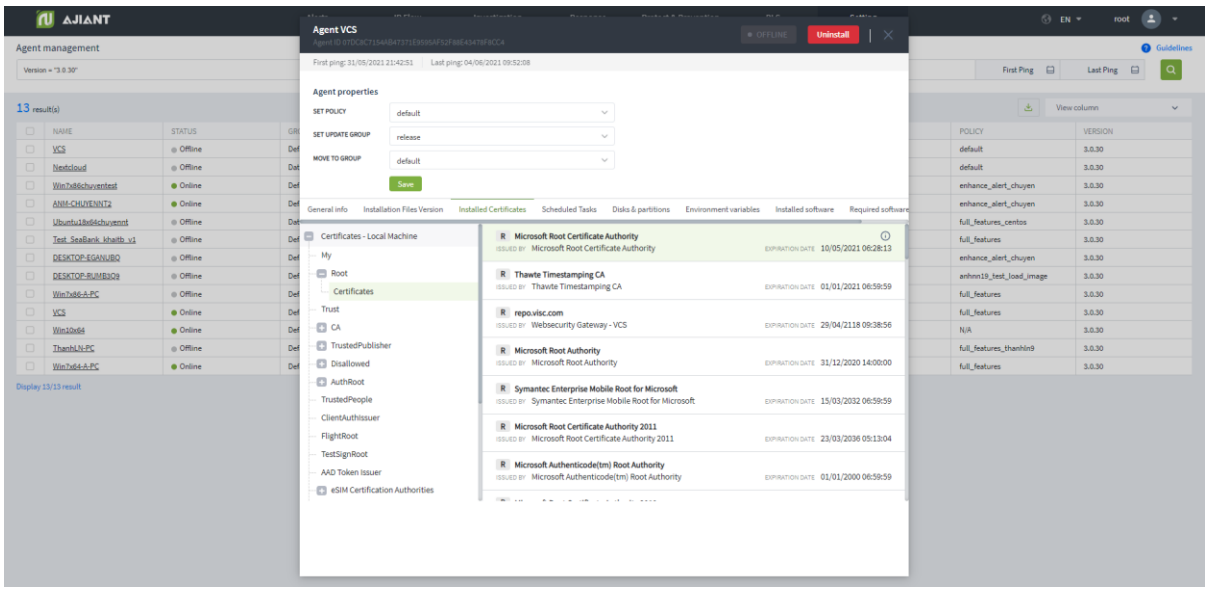
Support quick search by File name, Version in search text box.



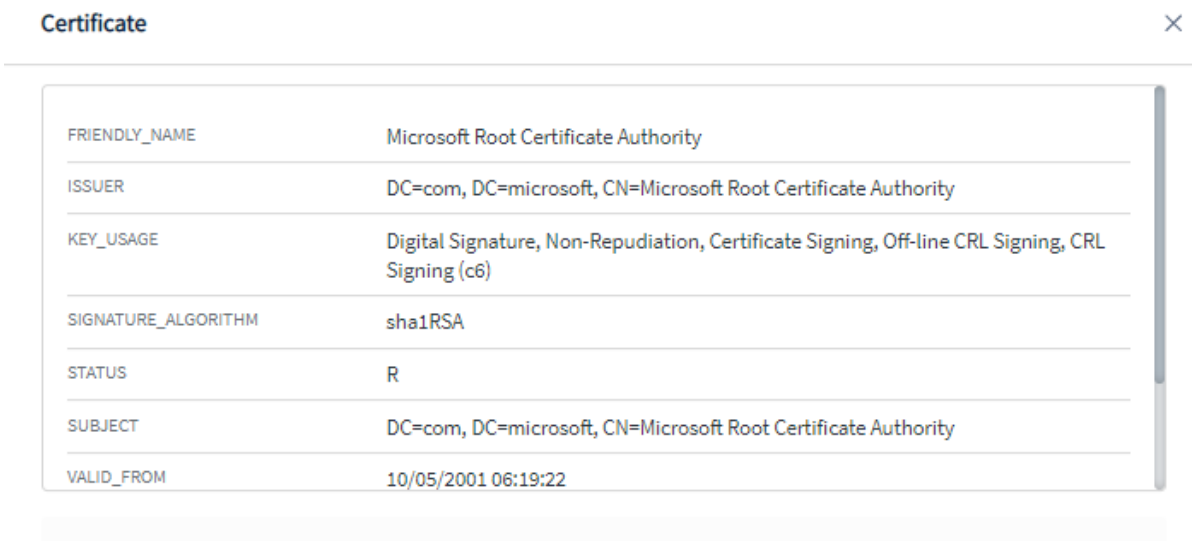
- Installed Certificates Tap

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

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 and Status.



In case of viewing details with more information, select , the screen is displayed as follows:

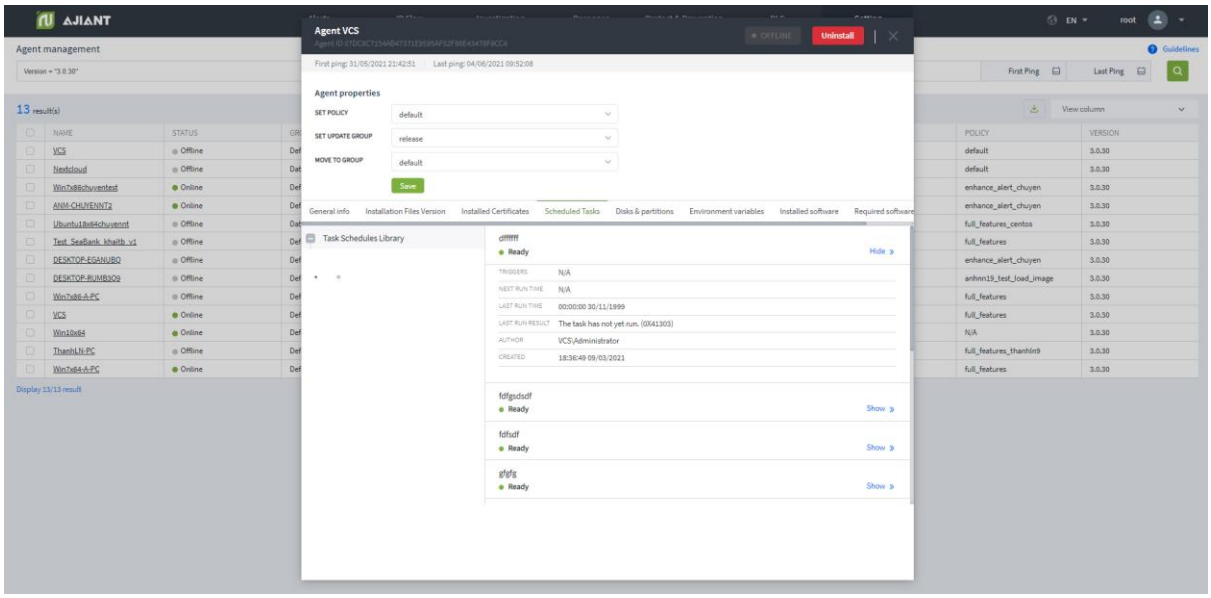


- Scheduled Tasks Tap

Statistics of all scheduled tasks on the agent installed machine, including information: List of scheduled tasks, Name, Status, Trigger, Next time run, Last time run, Author and Created.

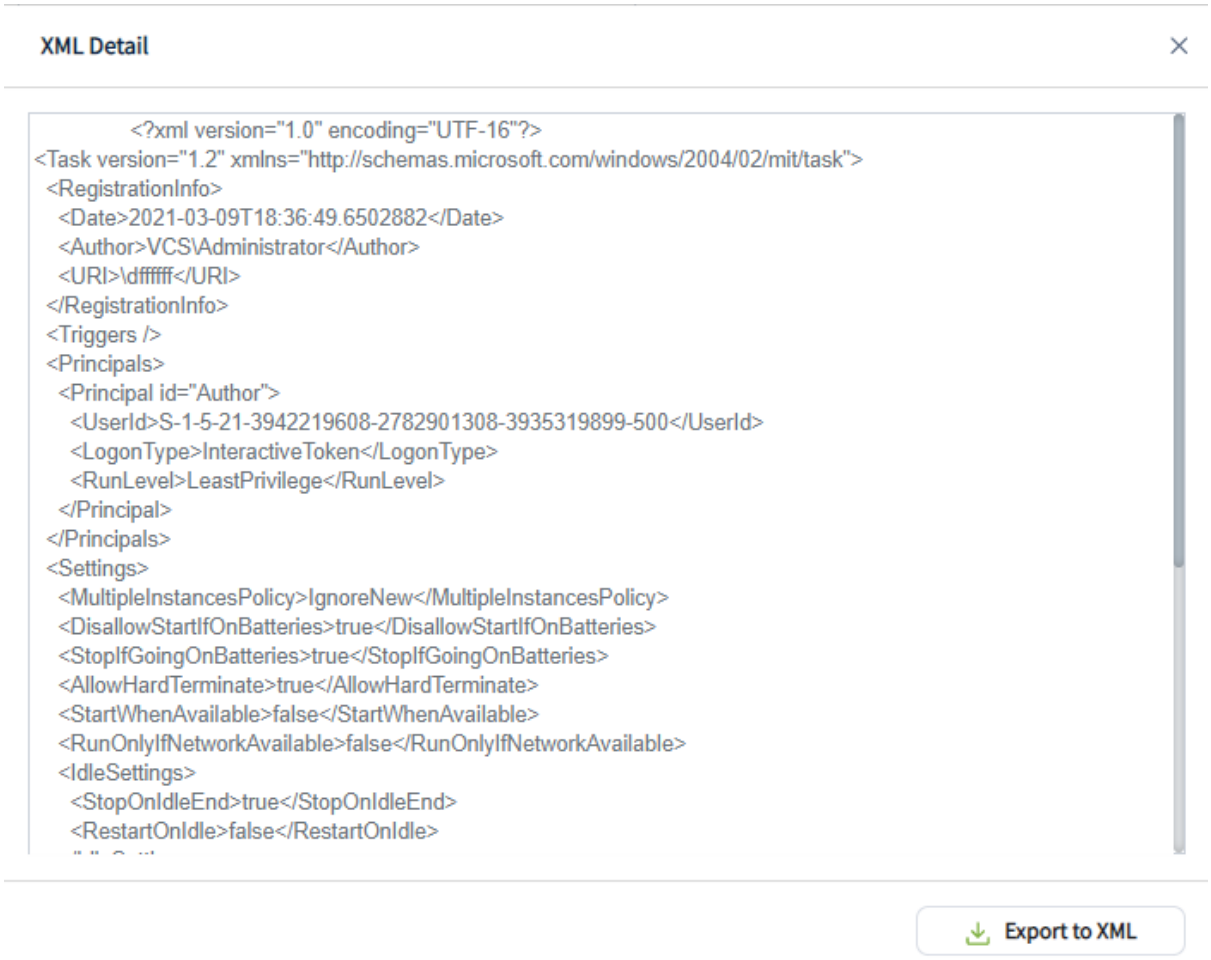
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

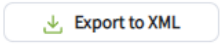
Select Show » or Hide » to customize the display of additional information for each task.



Hover over the task and select  to view the complete information of the task in .xml format.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Select 

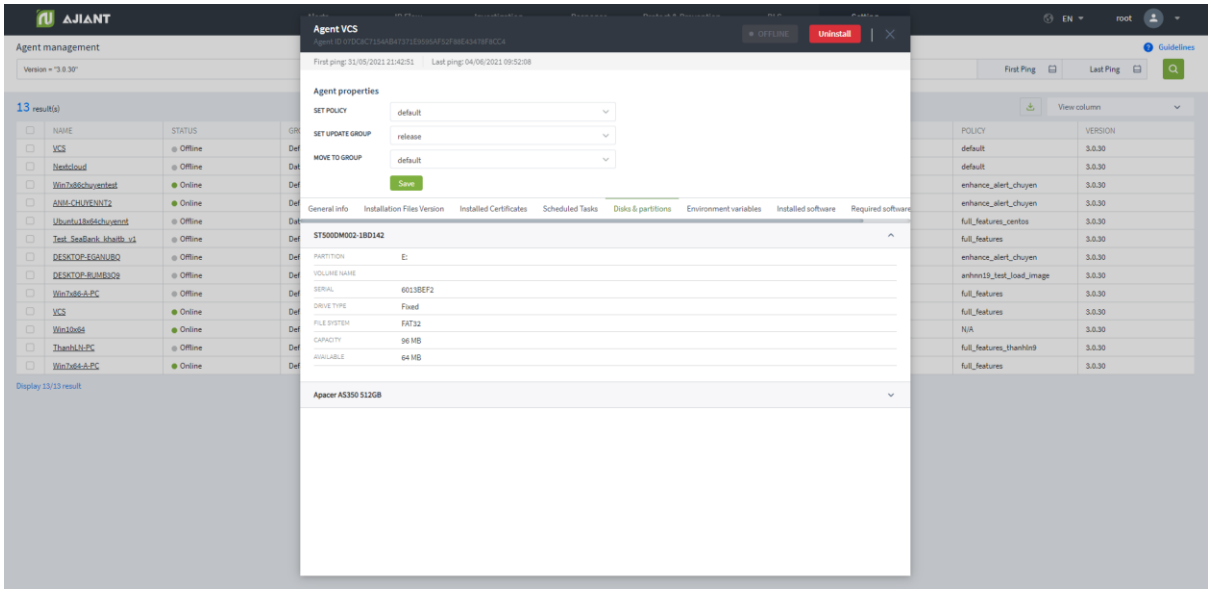
to download scheduled task information. The .xml format is supported.

- Disks & Partitions Tab

Statistics of all disks & partitions on the agent installed machine, including the following information: List of Disks, Partition, Volume name, Serial, Drive type, File system, Capacity and Available.

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

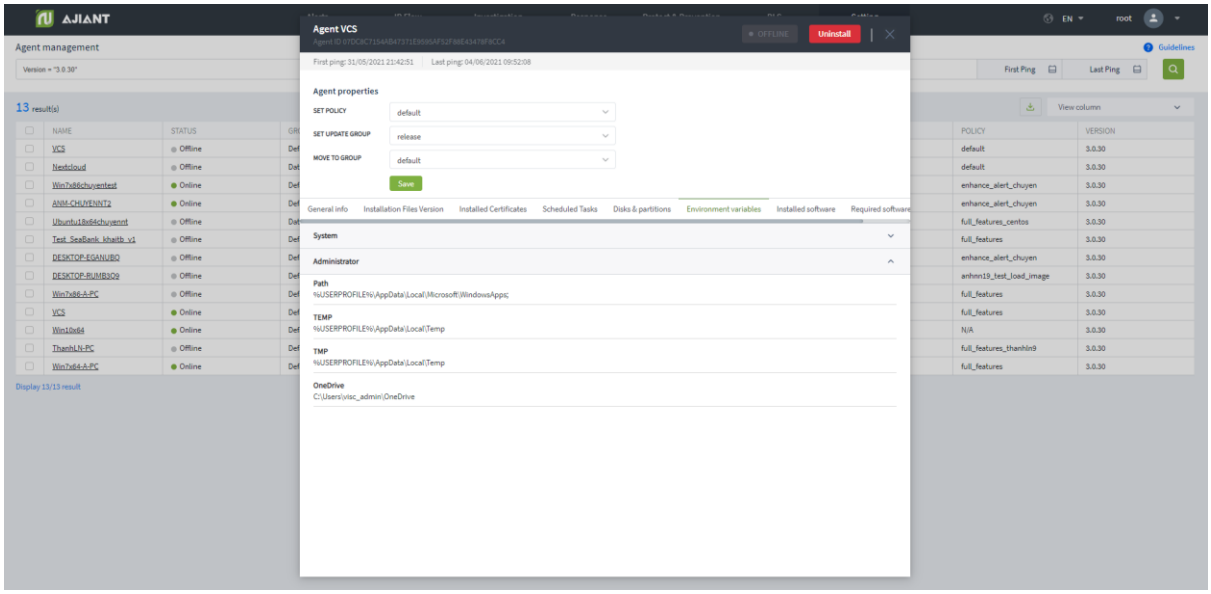
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Environment Variables Tab

Statistics of all environment variables on the agent installed machine, including the following information: List of system and users, variable name and values belonging to system or users.

Select ^ or v to customize the display of additional information for each disk.

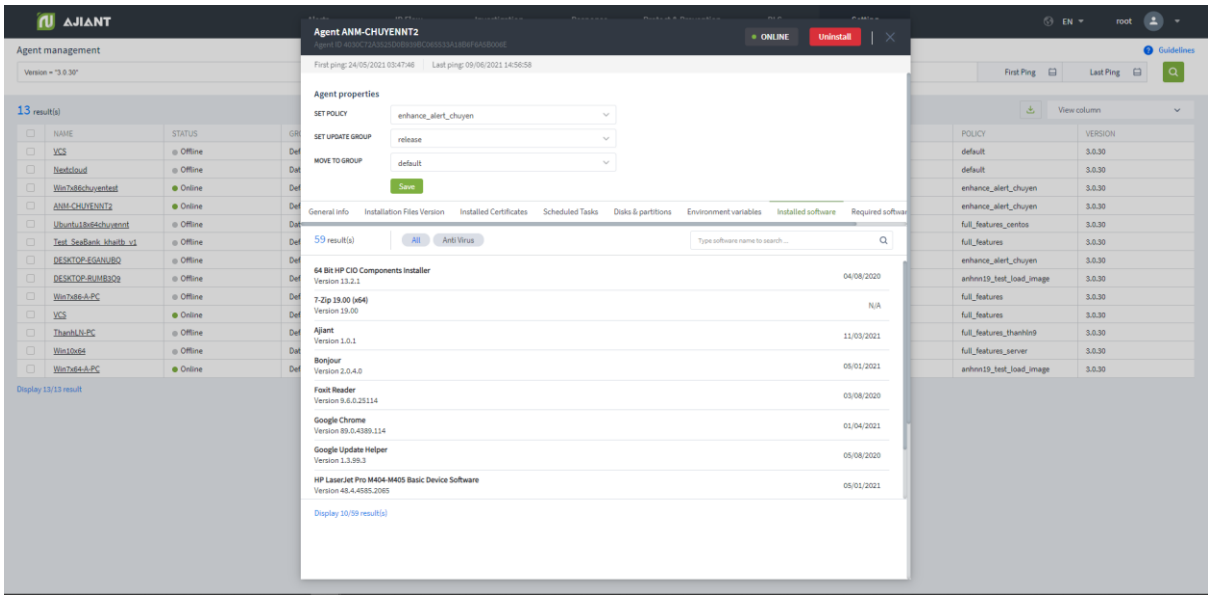


- Installed Software Tab

Statistics of all software installed in the agent, including information: Software name, installed version and installed date.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

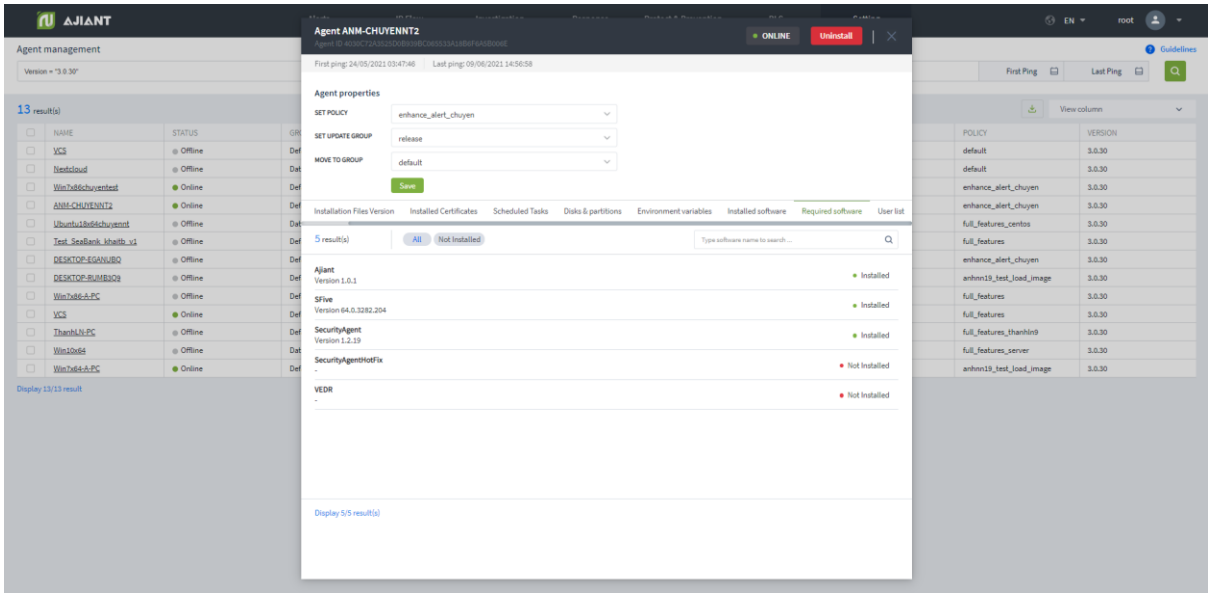
Support quickly searching for installed Antivirus software or entering the software name in the search text box.



- Required Software Tab

Statistics of all required software installed or not installed in the agent, including information: Software name, installed version and installed state.

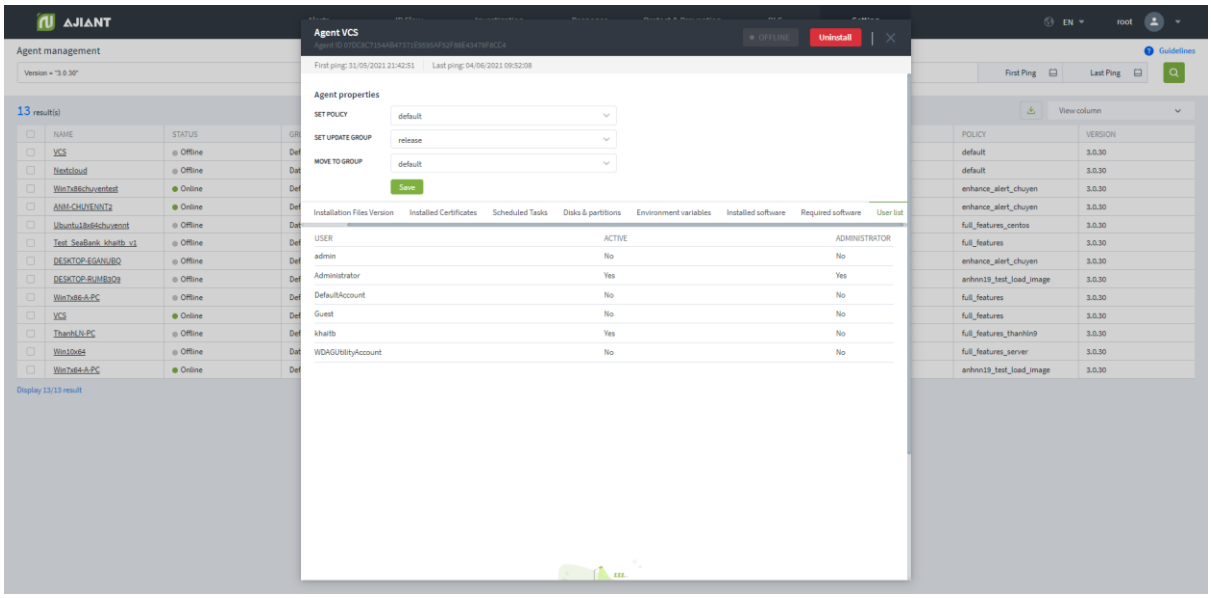
Support quickly searching for required software that is not installed on the machine or entering the name of the software in the search text box.



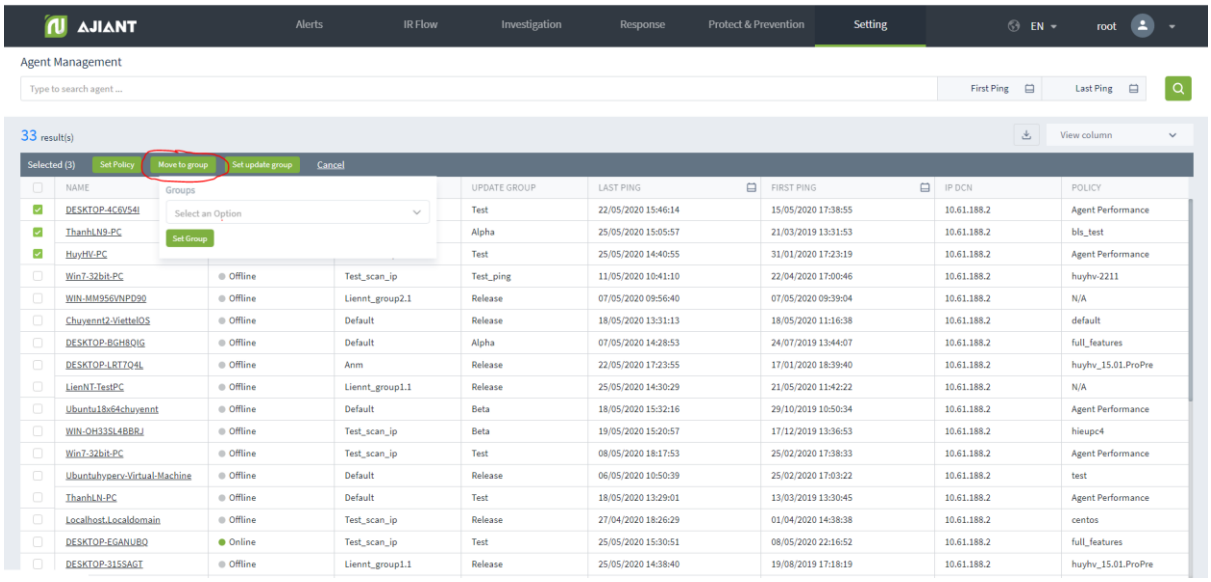
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- User List Tab

Statistics of all users logging in the agent, including information: Username, active and administrator.



- Quickly select 1 agent/ 1 group of agents to set up Move to group
  - Select 1 agent/multiple agents to enter the Multi-selected session



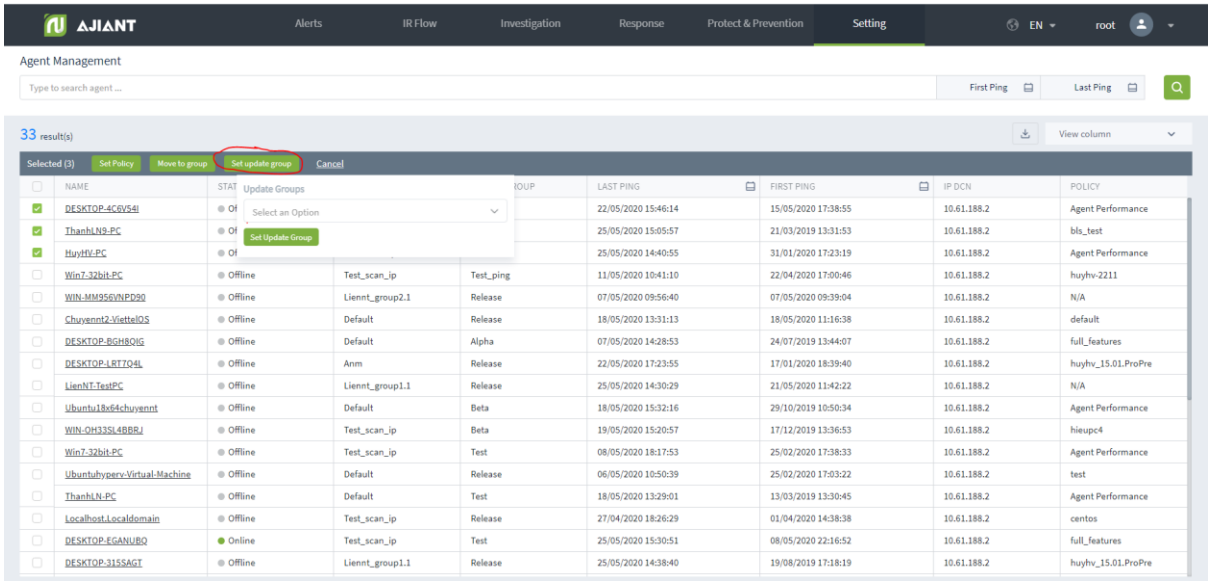
  - Perform Move to group

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Group list in the Move to group combo box

- User login under root group: Display all Groups in the system.
- User login under default group: Display default Group.
- User login under parent-level group: Display all the Groups belonging to the user logging in and the users belonging to the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all Groups belonging to the user logging in.

- Quickly select 1 agent/ 1 group of agents to set up Set update group
- Select 1 agent/multiple agents to enter the Multi-selected session.



- Perform Set update group.

Notes:

- Move to group: Move the agent to the groups in the Group Management screen
- Update group: Move the agent into groups that store files running under the agent, each group has different running files defined in the server.

3.1.4.2. Group Management

Configure the rule to automatically switch the Policy and group to the agents if the rule is satisfied on the Portal, reduce the time to switch the Policy and group for each agent and synchronize the Policy for the agents that satisfy the configured rule.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Key features on this monitor include as follows:

- (1) Manage groups by tree
- (2) Search group
- (3) Add a new group:
    - Create rules to automatically switch groups for agents
    - Options for group switch (All existing agents, New agents only, All existing and new agents) and Policy assignment (assign immediately, not assign).
- (4) Monitor the agents belonging to the group and the total number of agents belonging to the group
- (5) Edit group
- (6) Delete group and agent belonging to the group.

3.1.4.2.1. Manage groups by tree

- User login under root group: Display all groups in the system.
- User login under default group: Display default group.
- User login under parent-level group: Display the group belonging to the group of the user logging in and the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all groups belonging to the group of the user logging in.

The list of groups displayed in a tree form includes the root groups, and each root group includes child-level groups at level 1, level 2, etc.

Each group includes the group name, the group's configuration information (rule, policy and apply to), and a list of agents belonging to the group.

Group rules are independent among groups (no parent-child level group inheritance).

The group management by tree is for easier management when the number of agents is large and there is a hierarchy of agent management by company, department, etc.

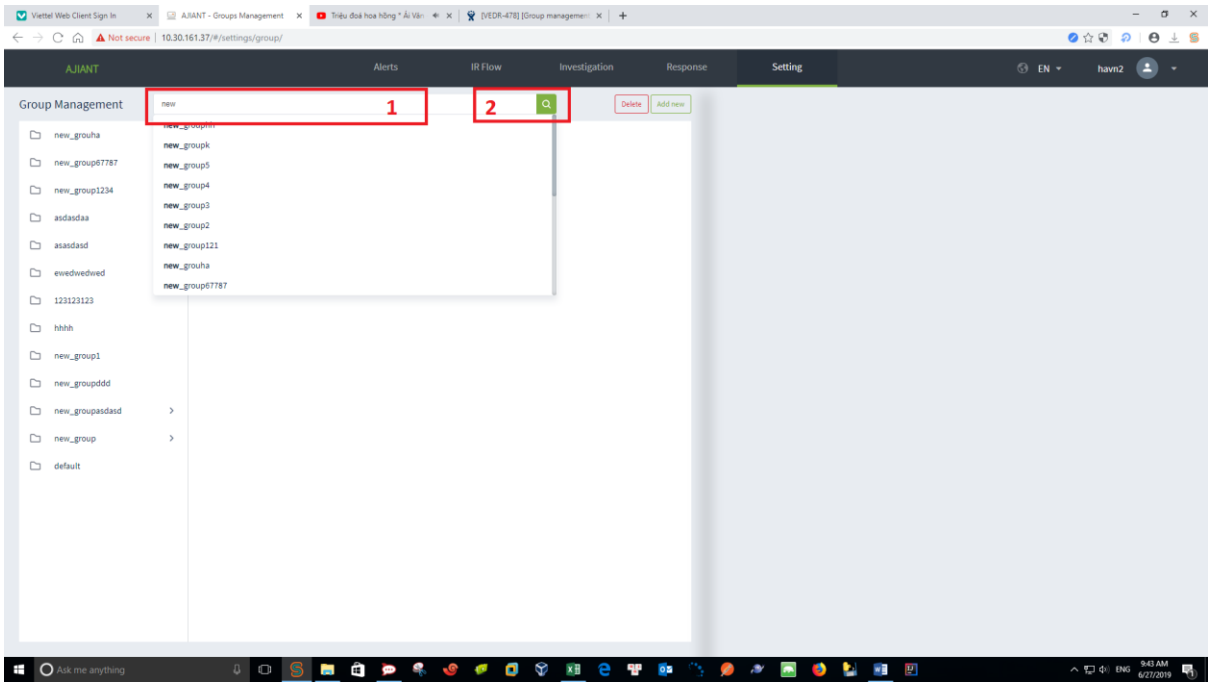
When the user belongs to a child-level group, if selecting a parent-level group, the group detail popup will not be seen.

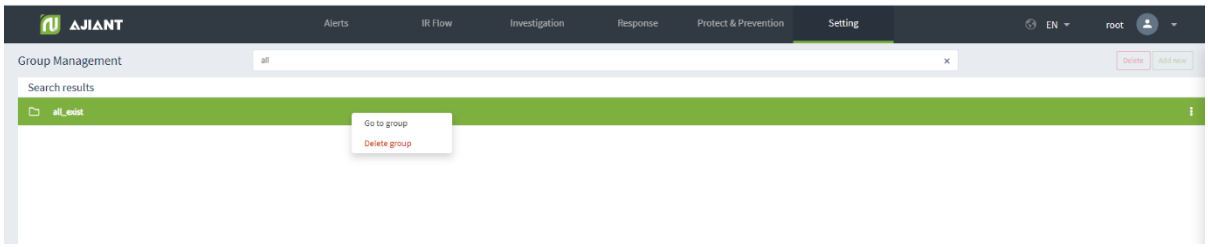
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

3.1.4.2.2. Search group

Method 1: Click on the Search textbox → A scrollable list of groups corresponding to the user logging in will be displayed → Select the group in the displayed list.

Method 2: Click on the Search textbox → Enter the search character into the textbox → The system automatically searches for records containing the entered characters → Select a suitable record in the suggested list or click Search or Enter, the list of satisfying records will be displayed.





- When double-clicking on a record will display detailed information of that record.
  - Detailed information tab is displayed as Detail and the data of that group is Rule, Policy and Apply to.
  - When selecting the Agent List tab, the agent information data matches that group.
- When right-clicking on a record, it will display 2 options: Go to group and Delete group.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- If selecting Go to group, then the user is taken to the location of that group on the tree
- If selecting Delete group, a confirmation popup to delete the group will be displayed.

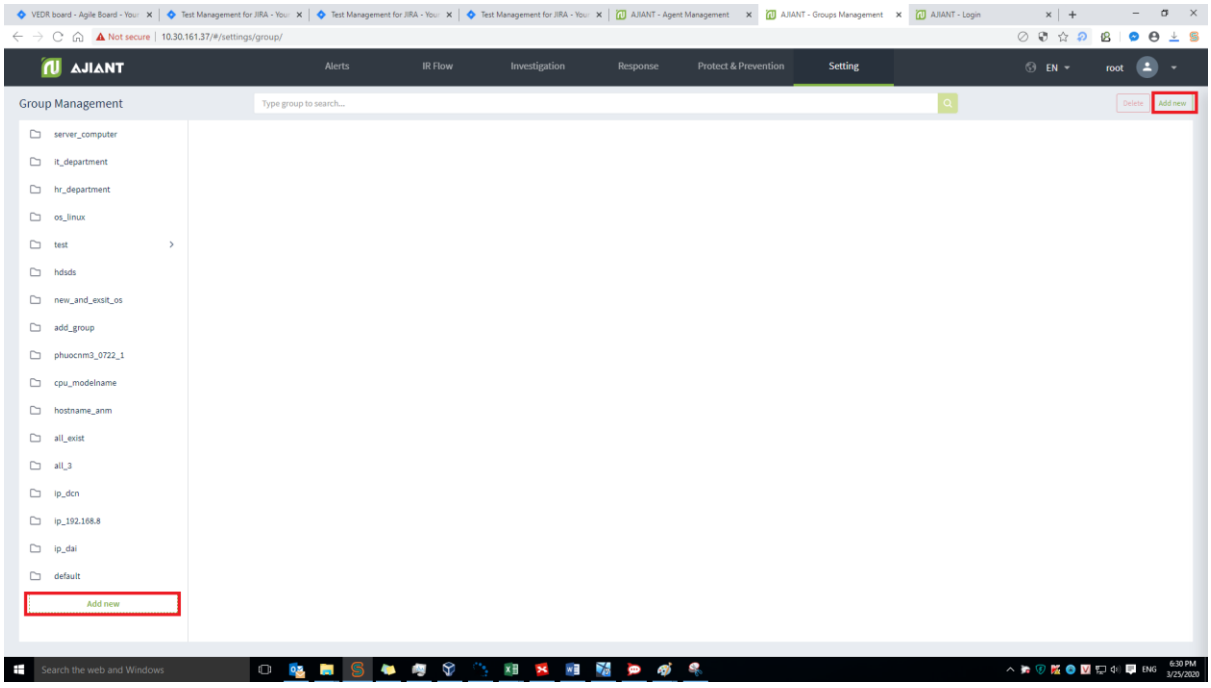
- When clicking on the menu in the right corner, each record also displays 2 options: Go to group and Delete group.

3.1.4.2.3. Add a new group

- User login under root group: Enable to add all new groups.
  User login under default group: Unable to add a new group.
- User login under parent-level group: Enable to add a new corresponding child-level group of the group belonging to the user logging in.
- User login under a child-level group or many child-level group: Enable to add a new corresponding child-level of the group belonging to the user logging in.

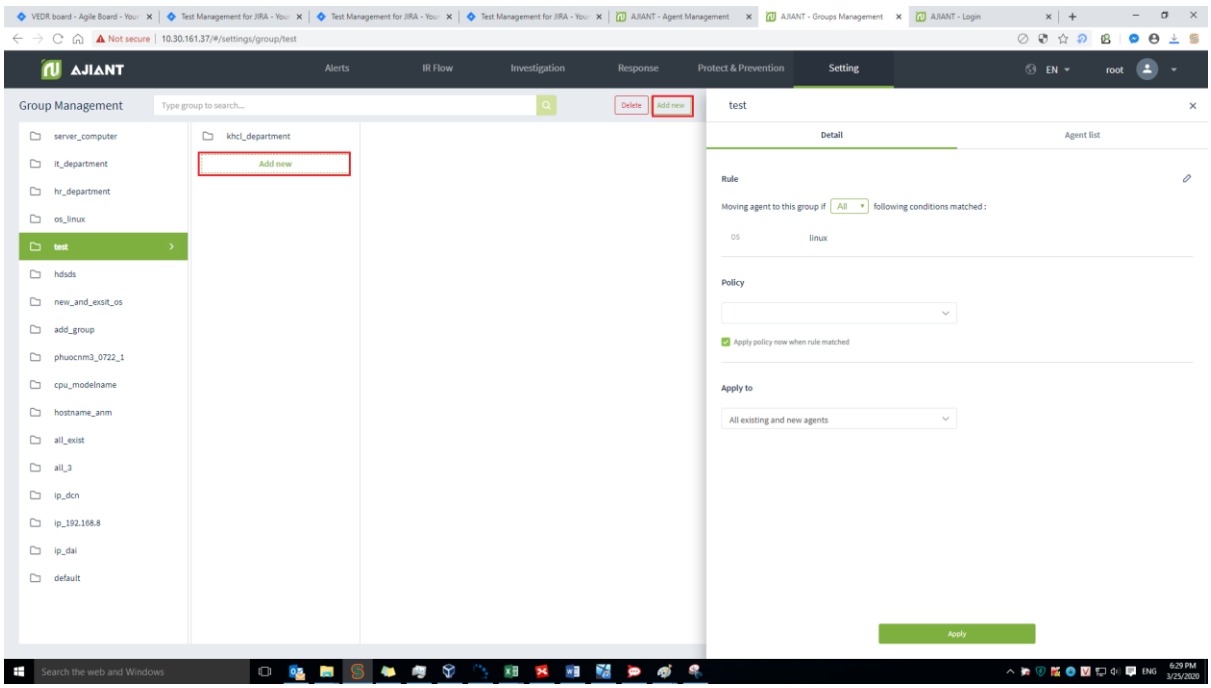
  - Step 1: Select the group location to create.

If creating a new group in the original group list, click the Add new button on the right corner of the screen or hover over the bottom of the original group list on the screen and click Add new.



Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

If creating a new group is a chil-level group in an original group or a group at level 1, level 2, etc, click on the parent-level group, then click Add new on the screen or hover over the bottom of the group list at the same level and click Add new.



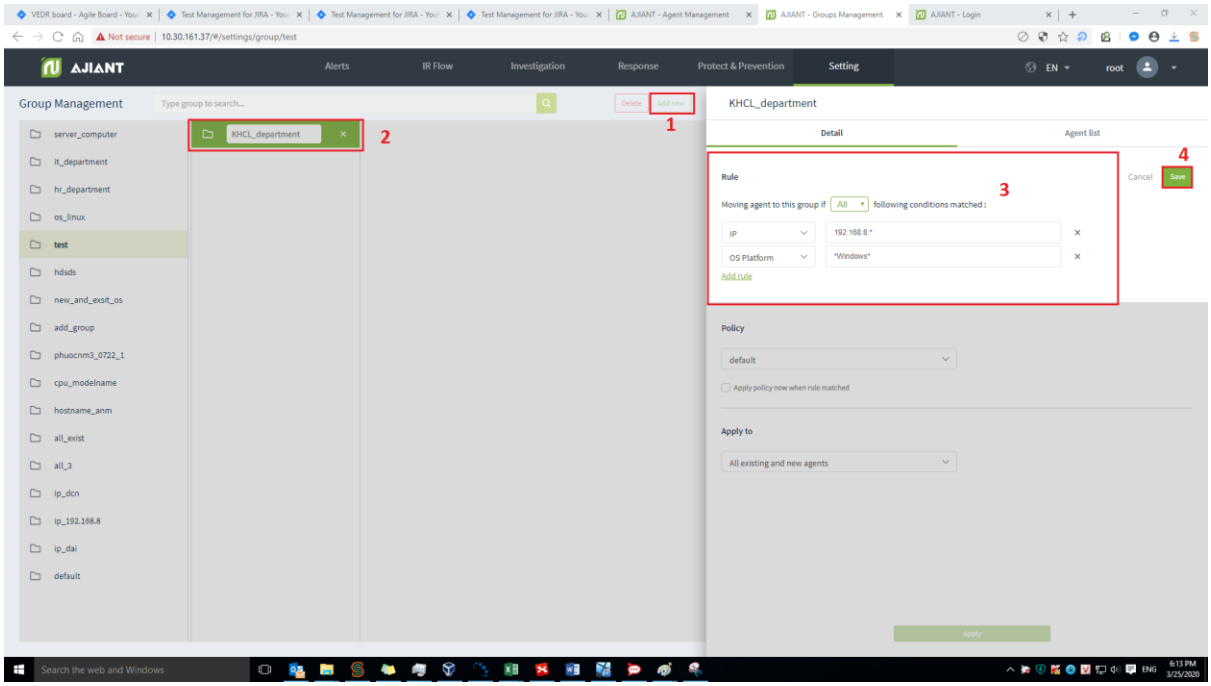
- Step 2: Enter the group name and configure the rule.

Notes: The name and configuration rule cannot be the same as the existing name and rule.

If the All operator is selected: The rule is satisfied when both fields are satisfied.

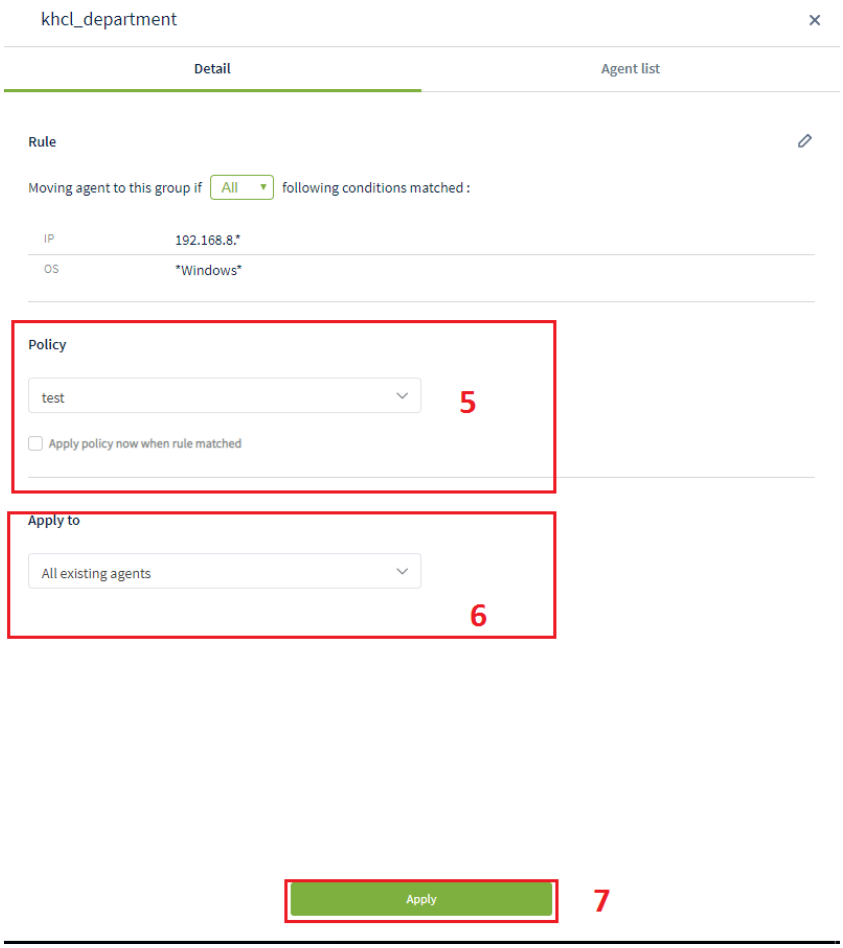
If the Any operator is selected: The rule is satisfied when one of the two or both fields is satisfied.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Step 3: Select the policy and the agent type to apply the policy if the rule is satisfied.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



After clicking Apply, check the agent switched to new group in the Agent List tab: The list of agents meets the rules and is switched to the newly added group. Depending on the option in the Apply to section to switch the group for agents in the system as follows:

- All existing agents: Switch groups for all existing agents in the system. For new agents installed after Apply, if they match the rule, groups are NOT switched.
- New agents only: Only switch groups for newly installed agents after Apply. For the existing agents on the system, if they match the rule, groups are NOT switched.
- All existing and new agents: Switch groups for all existing agents in the system and the newly installed agents after Apply if the rule is matched.

Notes:

- • If select the Apply policy now when rule matched checkbox, and click Apply, those selected agents will be checked the values. If they match the configured rule, they

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

will switch the policy for the agent to the selected policy at the Policy section, and switch groups.

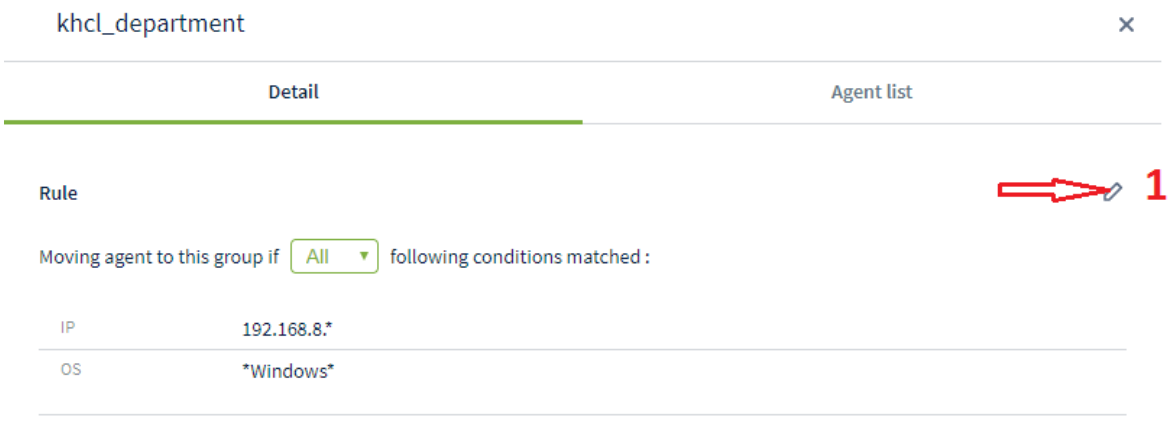
- In case the above checkbox is not selected, after Apply, those selected agents will be switched the group but not the policy. That is, the agents will keep the same policy while switching to the group with another policy. For newly installed agents, if the rule is matched, the group is switched and the default policy is applied. Because the checkbox is not selected, the default policy is applied.
- If the new agent matches the rules of many groups, it is prioritized to switch to the newly created group without counting the time to edit the group.

3.1.4.2.4. Edit group

Enable to choose to edit 1 or 2 or all 3 elements in a group, including: Rule, Policy and Apply to.

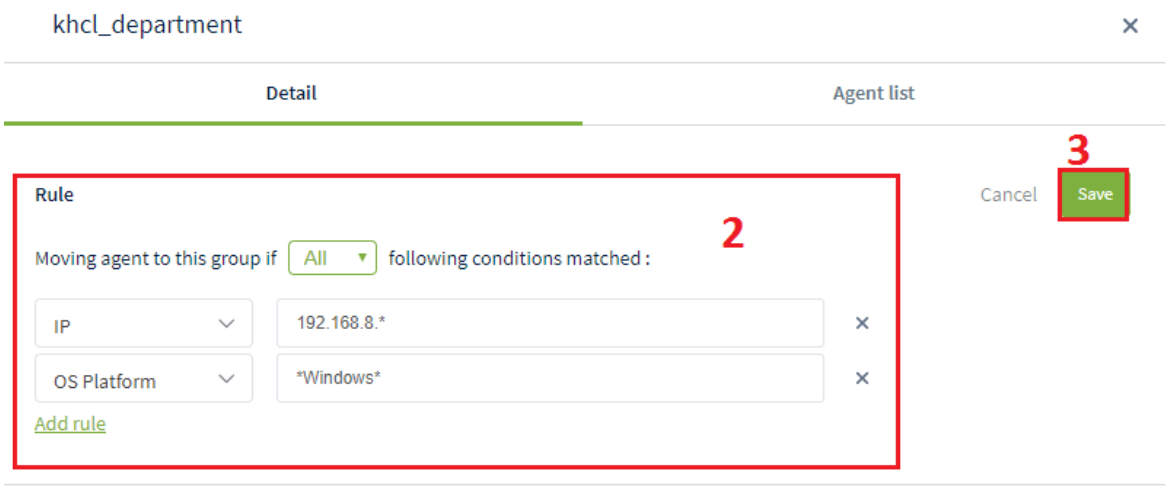
- User login under root group: Enable to edit all groups in the system.
- User login under default group: Unable to edit the default group.
- User login under parent-level group: Enable to edit all groups belonging to the user logging in/ and the child-level group whose role is also in the child-level role group of the user role logging in.
- User login under a child-level group or many child-level groups: Enable to edit all groups belonging to the user logging in.

To edit a Rule of a group, click the Edit icon.



Edit the group rule then click Save.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Then enable to edit in the Policy and Apply to sections, and click Apply.

Notes:

- In case of editing the elements of the group (Rule, Policy or Apply to) and do not click Apply, the edited content has been saved, but the Agent List is not updated. For newly installed Agents, perform the following:
  - Switch group: Depend on whether the new Agent is selected in the Apply to section. If selected, the Agent will be checked. If the rule of the group is matched, it will be switched to the group.
  - Apply policy: A policy of an agent depending on selecting the Apply policy now when rule matched checkbox. If the checkbox is selected, the group's policy will be applied. If it is not selected, the default policy will be applied. Because if the checkbox is not selected, the default policy will be applied.
- In case the components of the group are edited and then Apply is clicked, the edited content is saved. And if the All existing agents button in the Apply to section is selected, perform a scan of the entire agent information in the system and switch the group for the agent, then update the Agent List.

For new Agent, perform the same process as above.

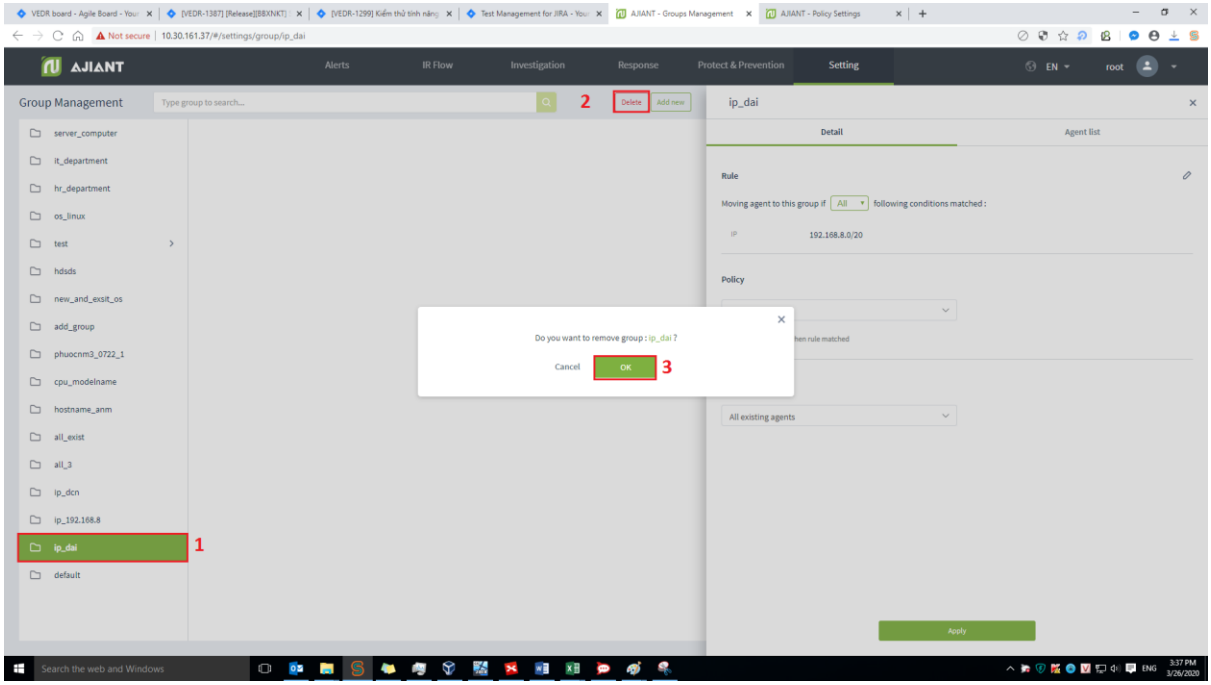
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

3.1.4.2.5. Delete group or remove agent from group

- User login under root group: Enable to delete all groups in the system.
- User login under default group: Unable to delete the default group
- User login under parent-level group: Enable to delete all groups belonging to the user logging in and the child-level group whose role is also in the child-level role group of the user role logging in.
- User login under a child-level group or many child-level groups: Enable to delete all groups belonging to the user logging in.

To delete a group, click on the group to delete, click Delete → OK on the confirmation screen.

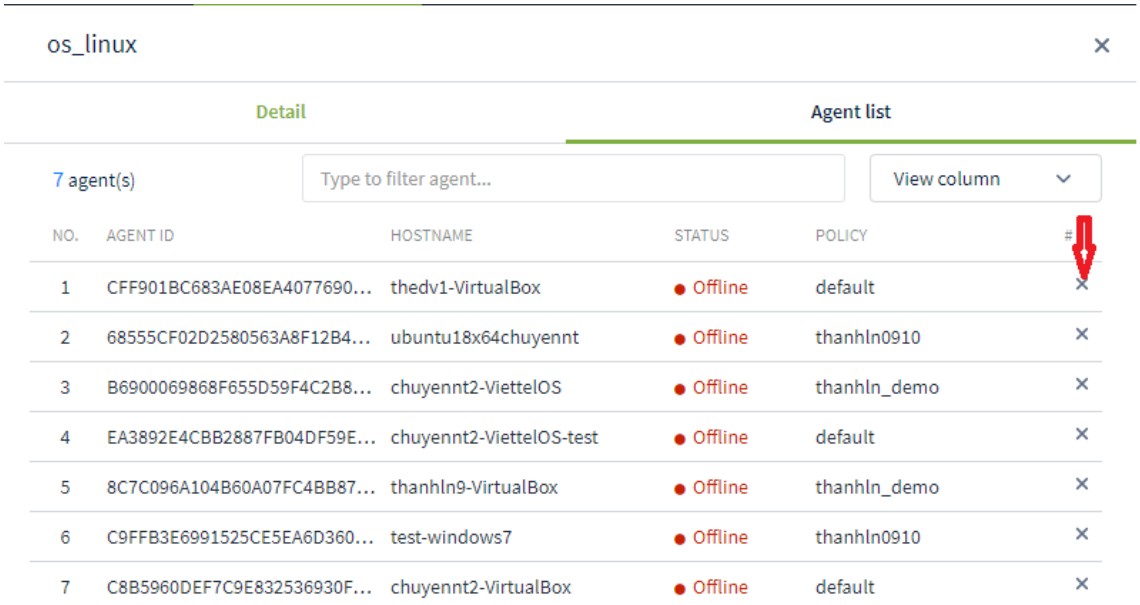
After deleting a group, the agents belonging to the group will be switched to the default group, while their policies will still remain.



To remove the agent from the group, click on the Agent List tab, click the x icon to remove the agent from the group.

After removing the agent from the group, the agent is switched to the default group, while its policy still remains.

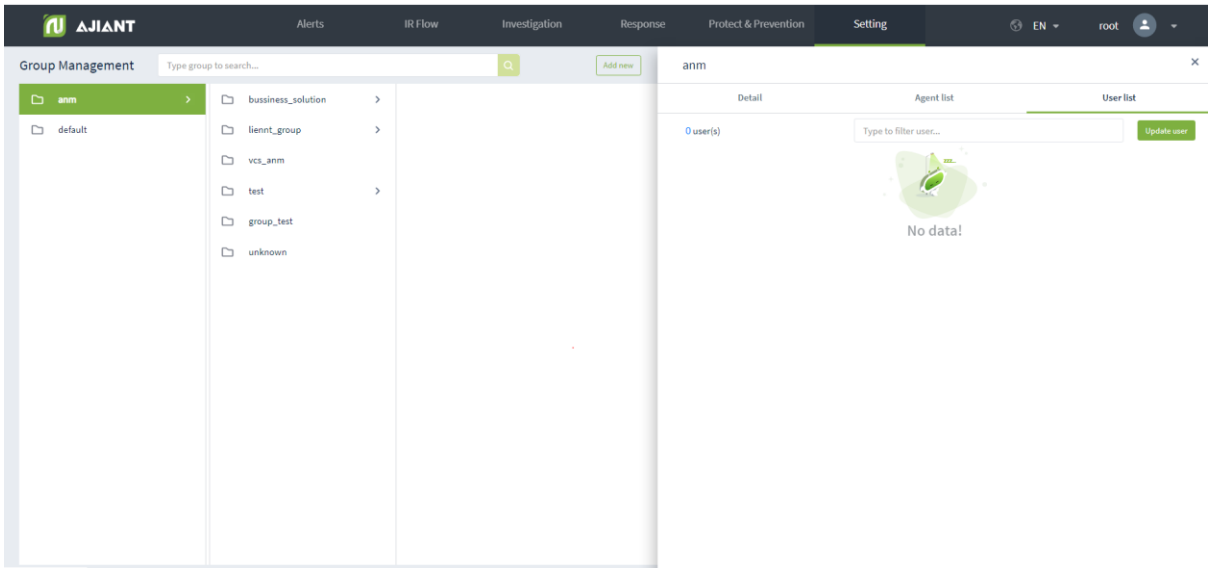
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



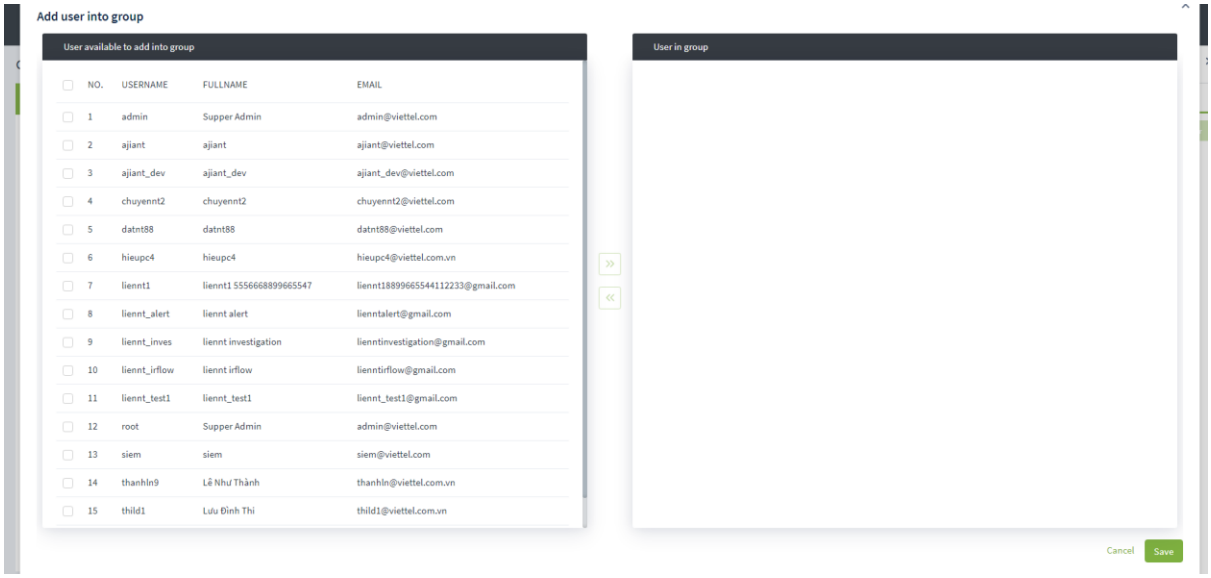
Notes: For deleting a parent-level group:

- Delete all child-level groups
- Switch all agents of the parent-level group and child-level groups to default group
- Maintain policy of agents in parent and child-level groups.

3.1.4.2.6. Add a new user to the group



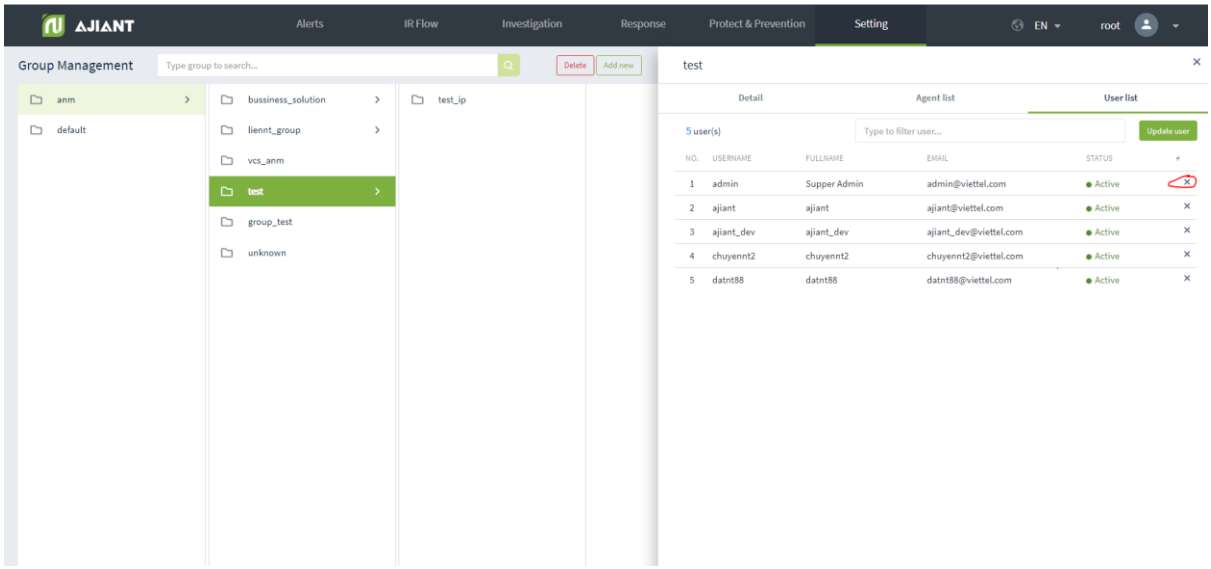
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



List of Users:

- User login under root group: Display all Users in the system.
- User login under default group: Display User only belonging to default group
- User login under parent-level group: Display the user logging in and the user belonging to the child-level group whose role is also in the child role group of the user role logging in.
- User login under a child-level group or many child-level groups: Display the user logging in.

3.1.4.2.7. Delete user



Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

3.1.4.3. Account Management

Manage accounts, permission and permission group of the portal system.

3.1.4.3.1. Permission management

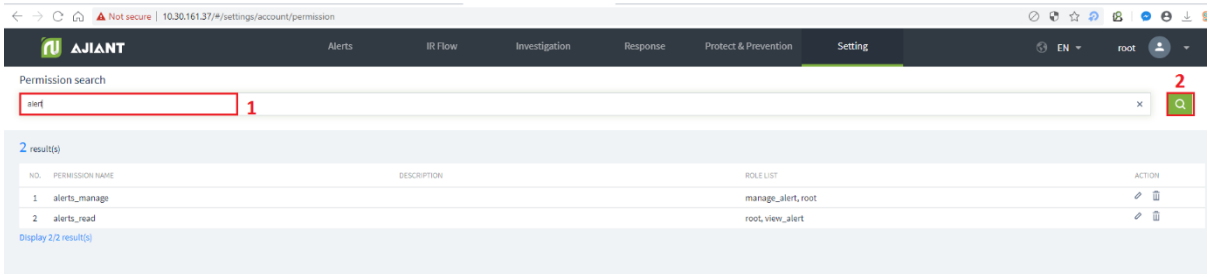
Manage access permission to system resources (APIs). A permission is access permission to a specific resource (API) of the system.

- The main functions on this screen, including:
  - (1) Manage permission
  - (2) Search permission
  - (3) Delete permission
- Manage permission

Display all system permission. In case the permission is deleted on this screen, when performing functions on the portal without permission, the deleted permission will automatically be added on the Permission Management screen.

- Search permission

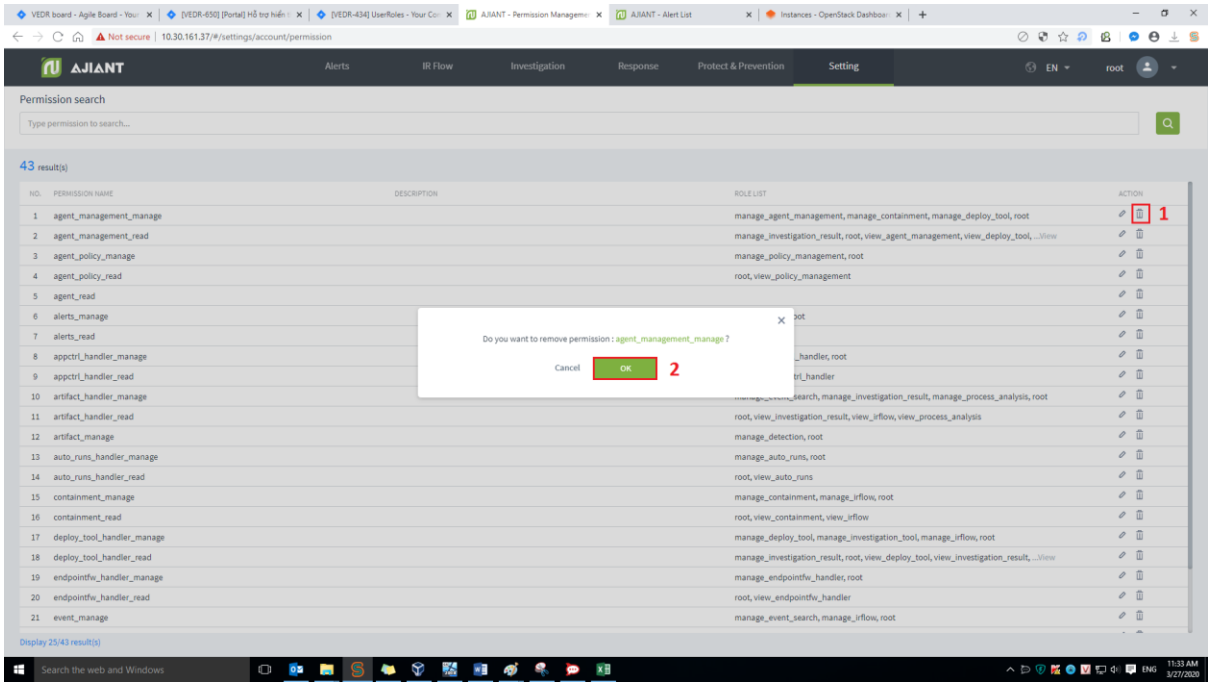
Enter the search character in the Search textbox → Click Enter or Search → A list of satisfied permission is displayed.



- Delete permission

Click the Delete icon → Click OK on confirmation screen to delete successfully.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



3.1.4.3.2. Role Management

Manage roles (permission group) of the system.

- Functions on this screen includes a set of as follows:
  - (1) Manage list of role
    - User login under root Role: Display all Roles in the system.
    - User login under default Role: Display default Role.
    - User login under parent-level Role: Display all the Roles belonging to the user logging in and the corresponding child-level group.
    - User login under a child-level Role or many child-level Roles: Display all Roles belonging to the role of the user logging in.
  - (2) Search role
  - (3) Add a new role
  - (4) Delete role
- Manage list of role

Manage the role list in the tree form. There are 2 built-in default root roles: Default and Root.

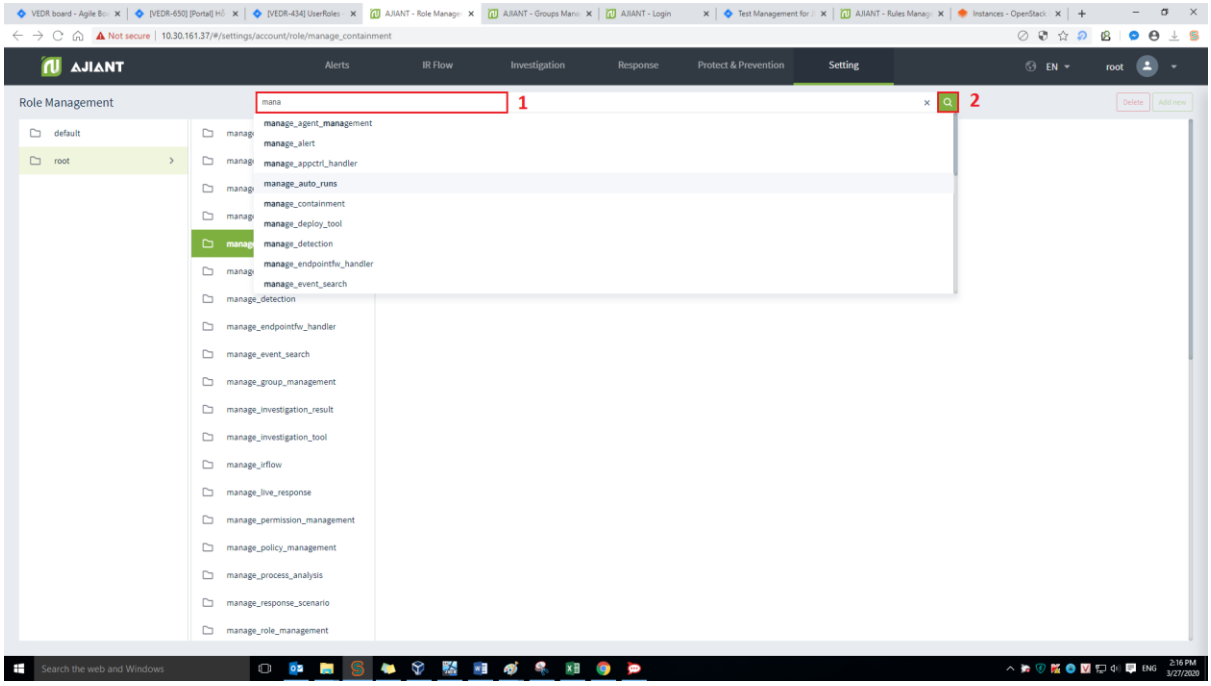
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Default role: User with Default permission only has permission to access to Portal, no permission to view data or perform the function.

Root role: Include all system roles. The user with Root role has full permission to use all functions on Portal.

Clicking on a role, the detailed information of the role will be displayed. A role will include information: role name, list of permission, list of users (accounts) containing role, parent-level role or list of child-level roles (if any).

- Search role
    - Method 1: Click on the Search textbox → The list of roles in the system is displayed and can be scrolled → Select the role in the list that is displayed.
    - Method 2: Click on the Search textbox → Enter the search character in the textbox → The system filters out the roles containing the search character → Select the role in the filtered list or click Enter or click the Search button.



    - When double-clicking on a record, the detailed information of that record will be displayed.
        - Detailed information tab is displayed as Detail. The role data includes role information and permission of that role.

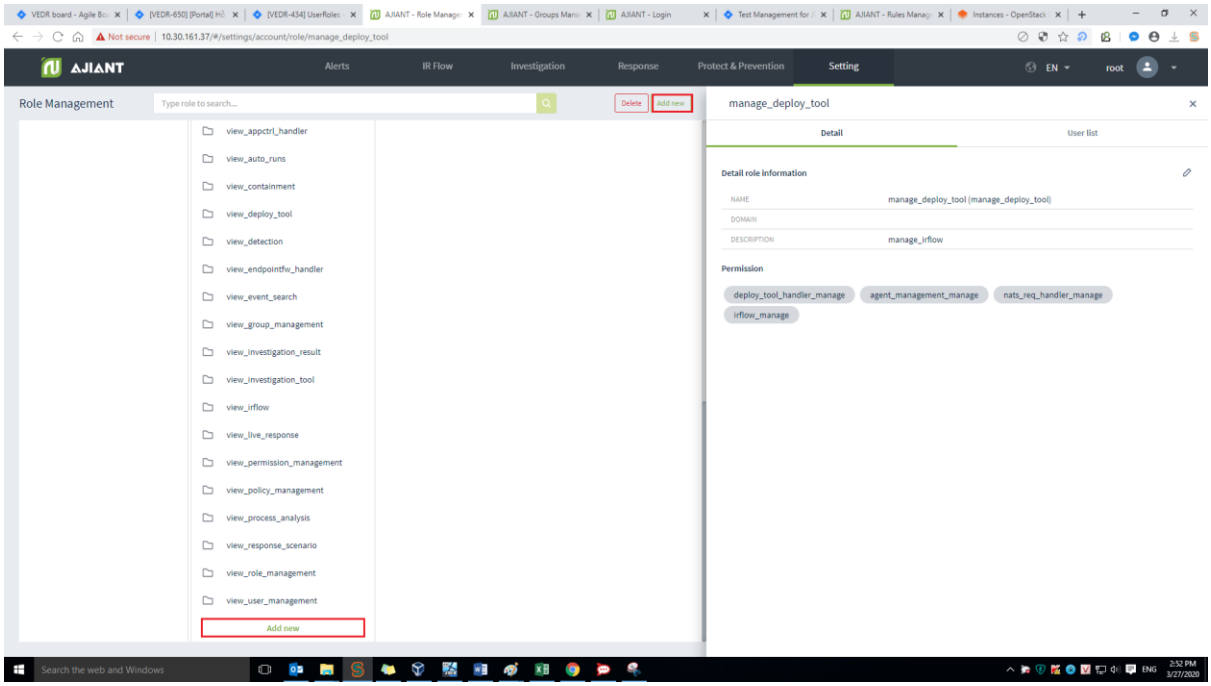
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

    - When selecting the User List tab, it means the user list containing the role is selected.
  - When right-clicking on a record, it will display Go to role. Click on Go to role to return to the original tree role list.
  - When clicking on the menu in the right corner, each record also displays the option: Go to role.

- Add a new role
  - User login under root group: Enable to add all new roles in the data tree.
  - User login under default group: Unable to add new.
  - User login under parent-level group: Enable to add a new corresponding child-level role of the group belonging to the user logging in. Unable to add a new role at the same level.
  - User login under a child-level group or many child-level groups: Enable to add a new corresponding child-level group of the group belonging to the user logging in.
    - Step 1: There are ways to create a new role as follows:
      - Click on a role then hover over the end of the role list and select Add new to create a role with the same level as the selected role.
      - Click Add new on the screen to create a child-level role of the selected role
      - Right-click on a column in the tree and select Add new role.

    Then, enter the role name that does not match the role name existed in the system.

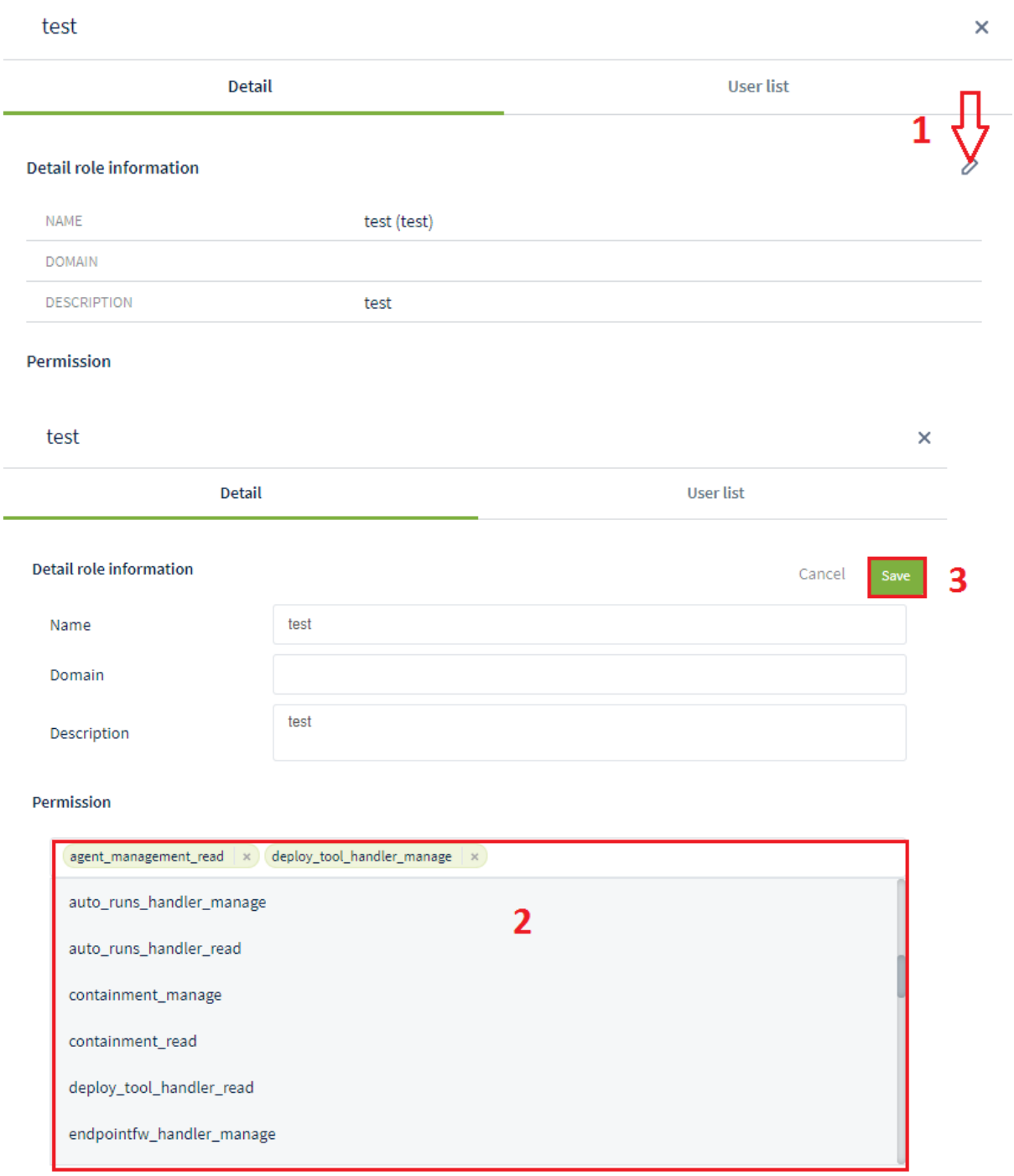
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Step 2: Click the Edit icon to add permission information for the role → Select permission to add to the role → Click Save.
  - User login under root group: Enable to edit all roles in the system.
  - User login under default group: Unable to edit default role.
  - User login under parent-level group: Enable to edit all the roles belonging to the user logging in and its child-level roles.
  - User login under a child-level group or many child-level groups: Enable to edit all roles belonging to the user logging in.

Notes: The permission list of child-level role is the parent-level role's subset. That is, when choosing the permission to assign to the child-level role, that role must belong to the permission list of the parent-level role.

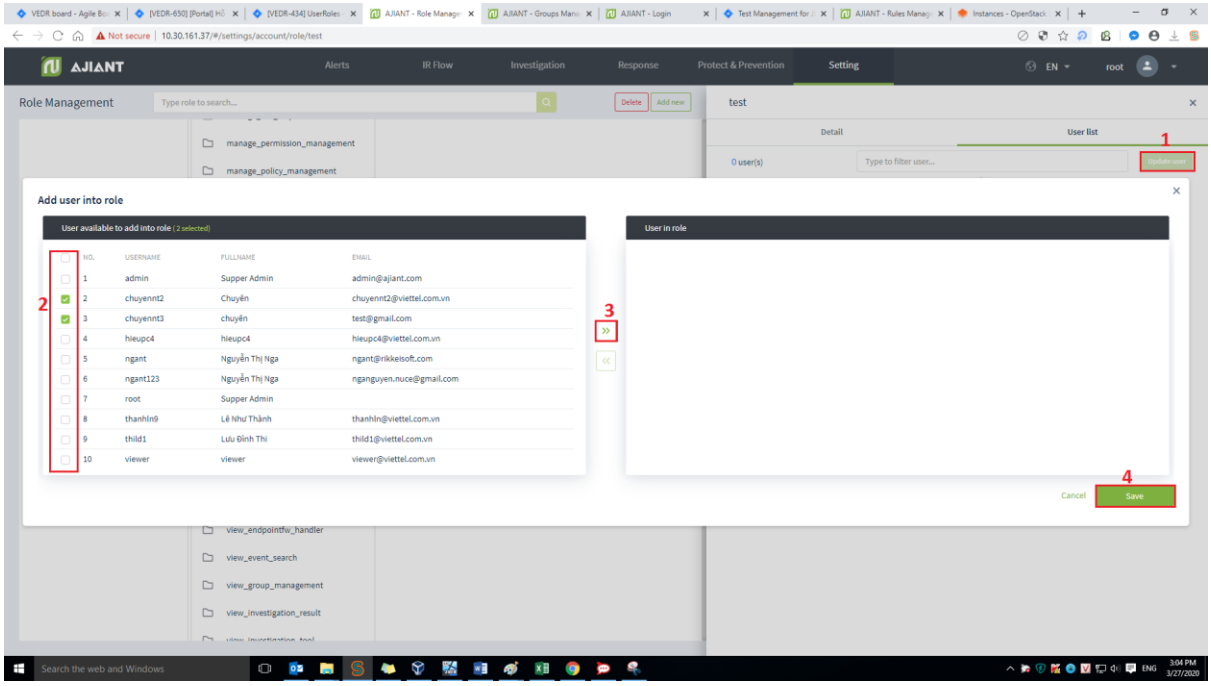
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Step 3: Switch to the User List tab to add a role to the User's role list.
  - User login under root group: Display all users in the system.
  - User login under default group: Display user only belongs to the default.

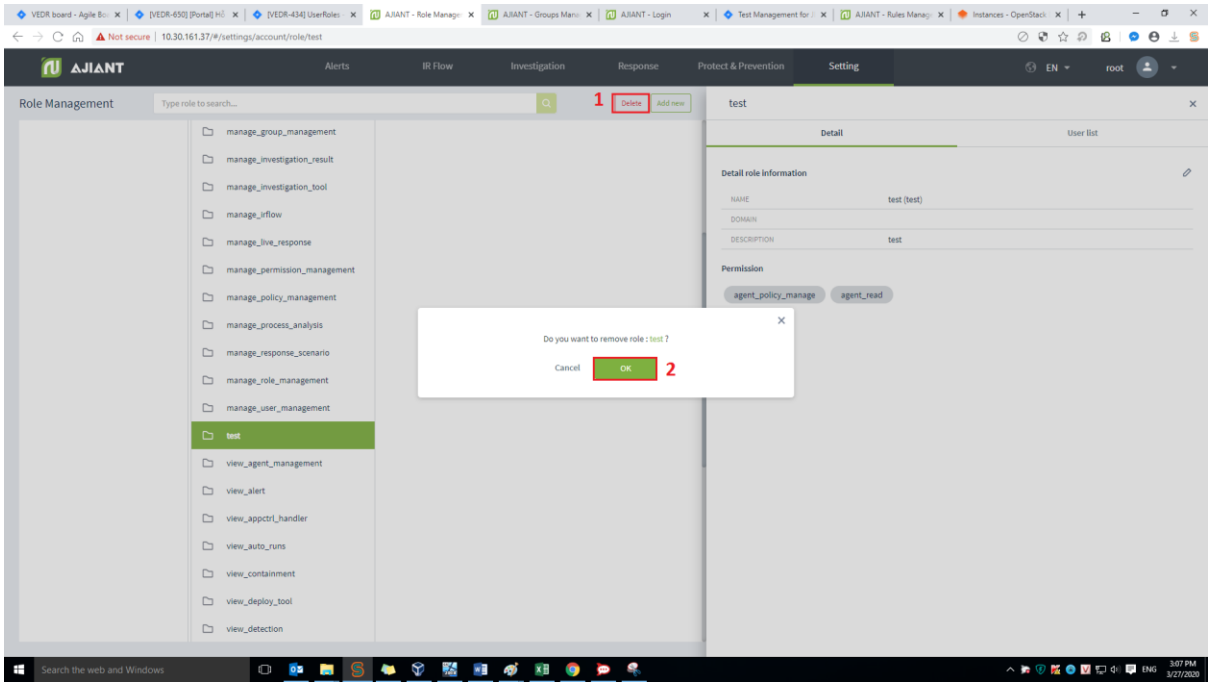
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- User login under parent-level group: Display the user logging in and the user in the child-level group whose role is also in the child-level role group of the user logging in.
- User login under a child-level group or many child-level groups: Display the user logging in.



- Delete role
  - Click on the role to delete, select Delete → Click OK on the confirmation screen.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Notes: After deleting a role, all users using this role are changed: If user X is in the deleted role and user X has only 1 role, user X is switched to the default role. Otherwise, if user X has many roles, only the deleted role is removed from user X's role list.

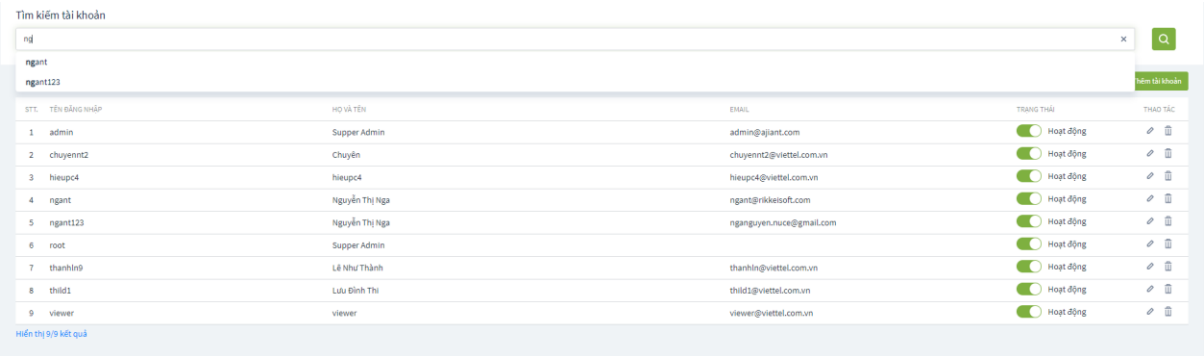
3.1.4.3.3. User management

Manage accounts logged into Portal VCS-aJiant system.

- The main functions on this screen include a set of as follows:
  - (1) Search account
  - (2) Add new account
  - (3) Edit account
  - (4) Delete account
- Search account

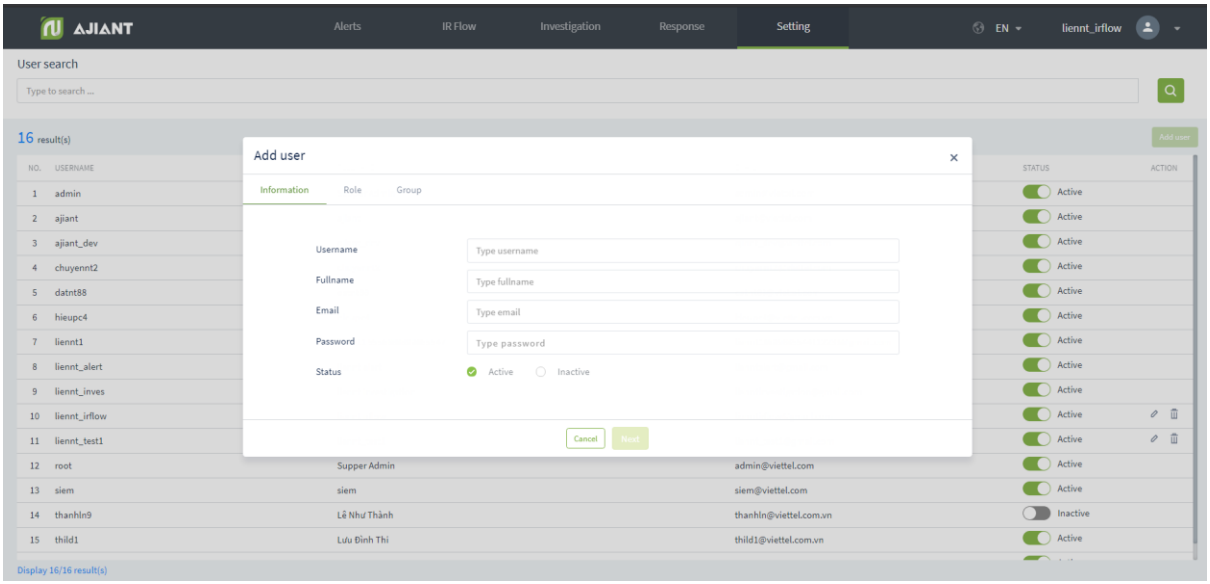
Click on the Search textbox → The list of accounts in the system is displayed → Select the account to search in the list or enter the <text> character in the textbox to filter out the accounts → Click Search or select the account to search from the list of filtered accounts.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



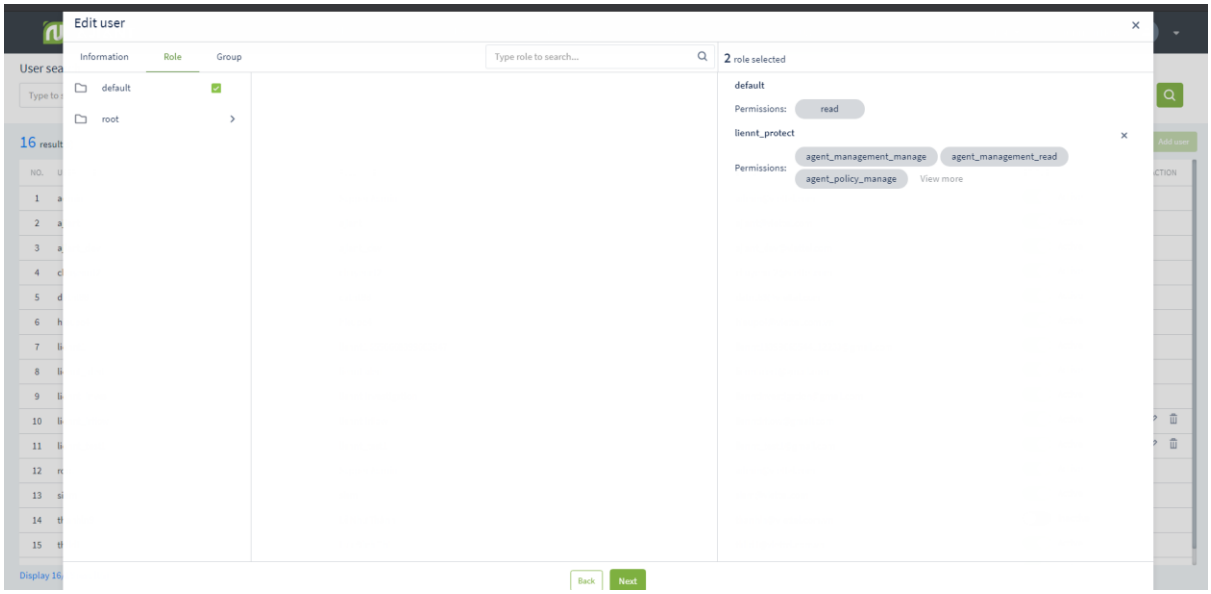
- Add new account

Click Add user → Enter information in the form that is displayed → Click Next.

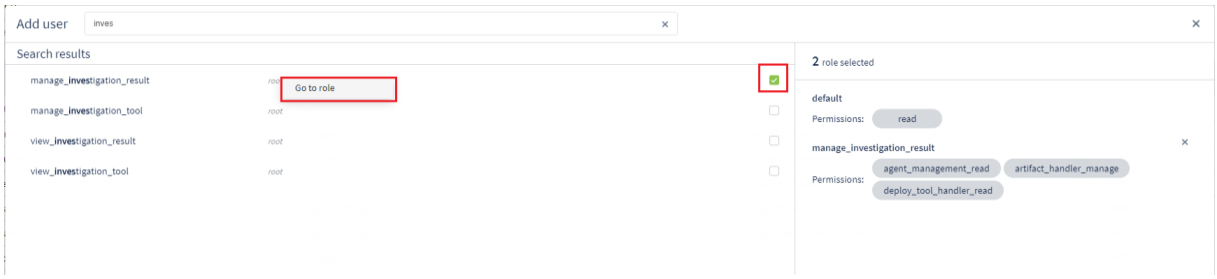


  - Select the role (permission group) to assign to the account, then click Next.
  - When clicking on the check box, each role will display the permission corresponding to that role:
    - User login under root Role: Display all Roles in the system.
    - User login under default Role: Display default Role.
    - User login under parent-level Role: Display all the Roles belonging to the user logging in and the corresponding child-level group.
    - User login under a child-level Role or many child-level Roles: Display all Roles belonging to the Role of the user logging in.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- On the Add role screen for user, the roles can be searched similar to the account search. After entering the search characters in the Search textbox → Click the Search icon or Enter to display the role screen that meets the search criteria.



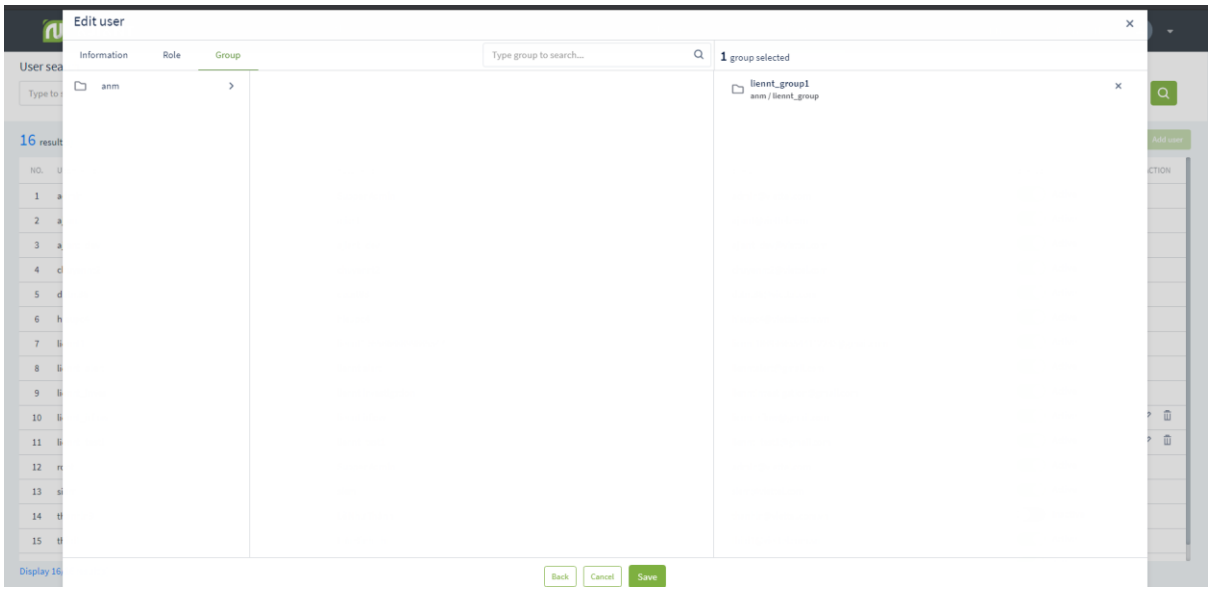
- Click the checkbox corresponding to the role to be added, and click Go to role to return to the original role list screen, then click Create to create an account.

Notes: The account that is logged in to create a new account can only create accounts containing child-level roles in the list of roles that the account logging in is granted.

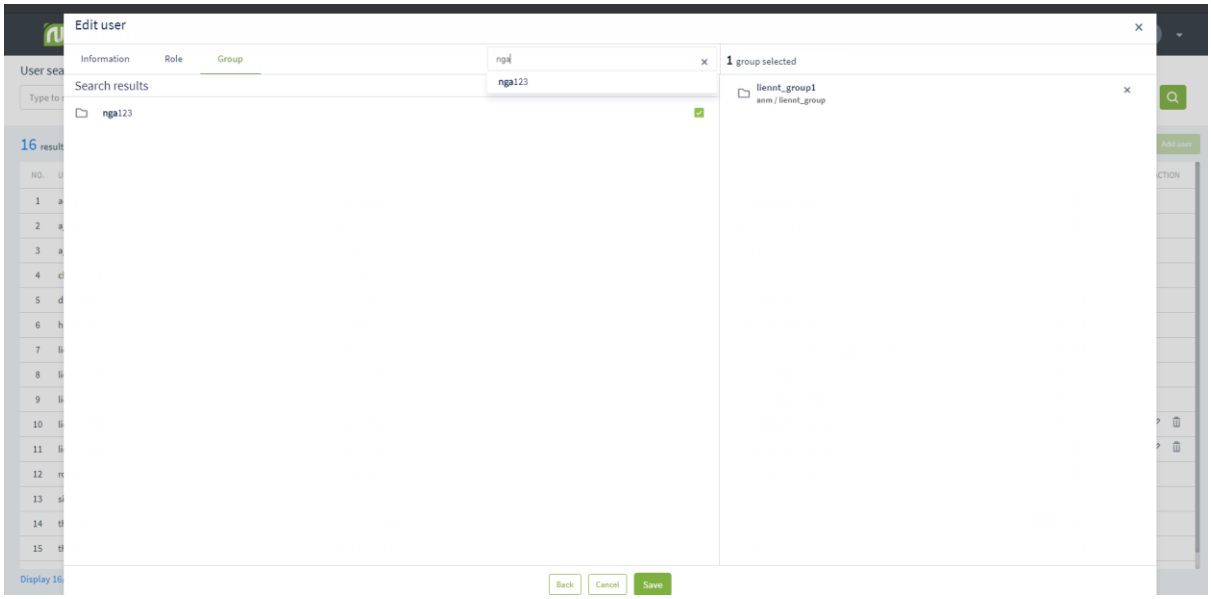
- Select the group to assign to the account, then click Create.
- When clicking on the check box, each role will display the permission corresponding to that role.
  - User login under root group: Display all groups in the system.
  - User login under default group: Display default group.
    User login under parent group: Display the group belonging to the group of the user logging in and the corresponding child-level group.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- User login under a child-level group or many child-level groups: Display all groups belonging to the group of the user logging in.



- Click the checkbox corresponding to the group to be added, and click Go to role to return to the original group list screen, then click Create to create an account.



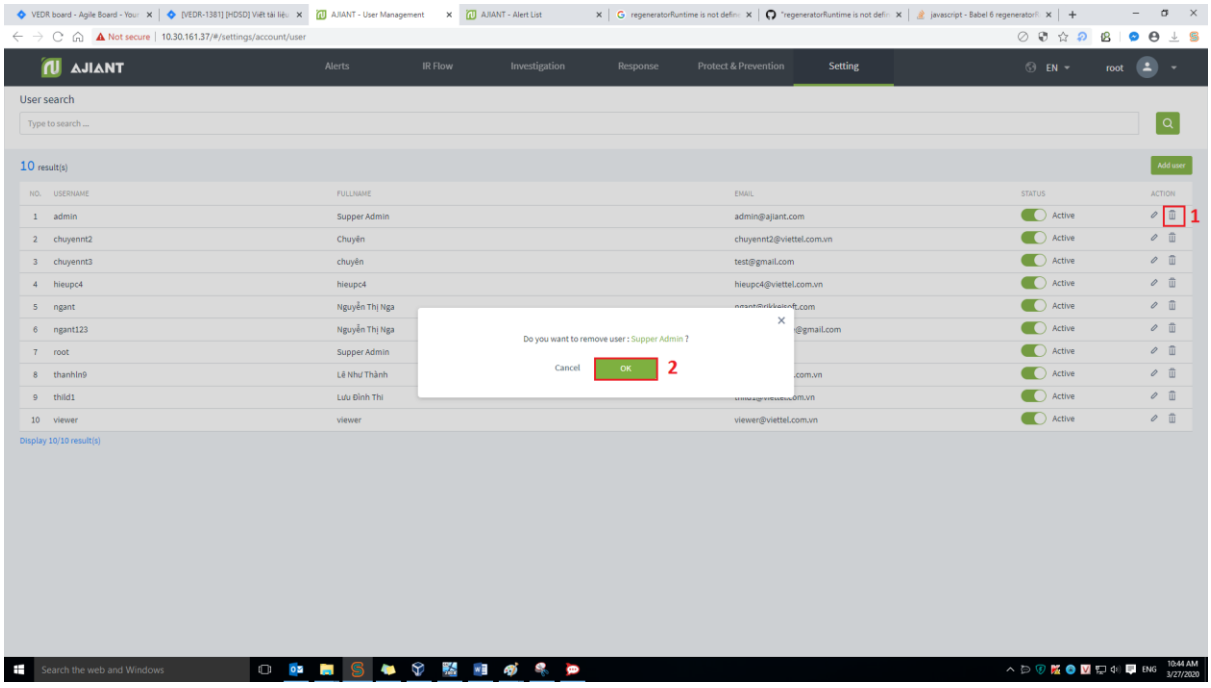
- Delete account

Click on the Delete icon, then click OK on confirmation screen.

Check the display of the Delete icon as follows:

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- User login under root group: Display all users in the system.
- User login under default group: Display user only belongs to default.
- User login under parent-level group: Display the user logging in and the user in the child-level group whose role is also in the child-level role group of the user logging in.

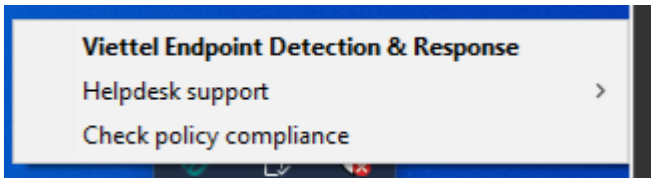


3.2. Agent Interface

3.2.1. Main

The function allows users to quickly view the information security status at the agent installed machines.

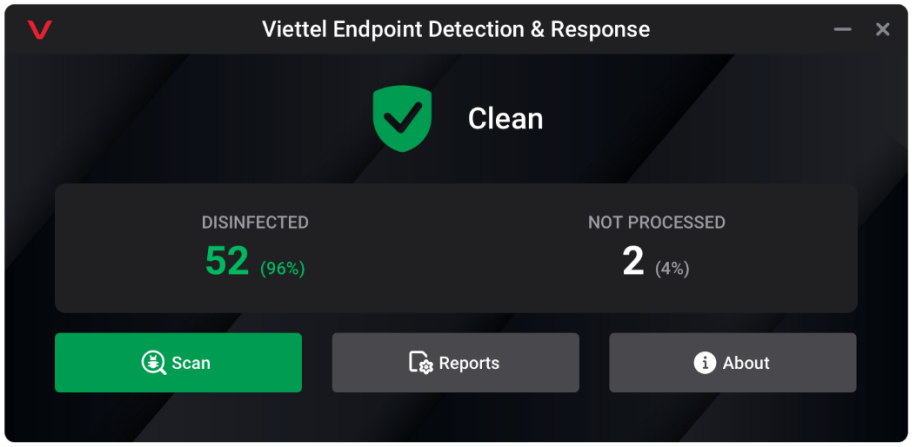
On the taskbar, find and double-click the  icon → Select Viettel Endpoint Detection & Response:



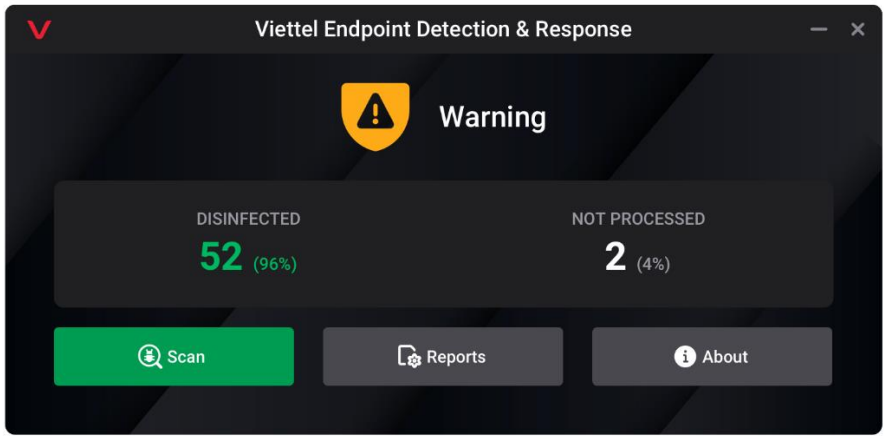
The system displays the information as follows:

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

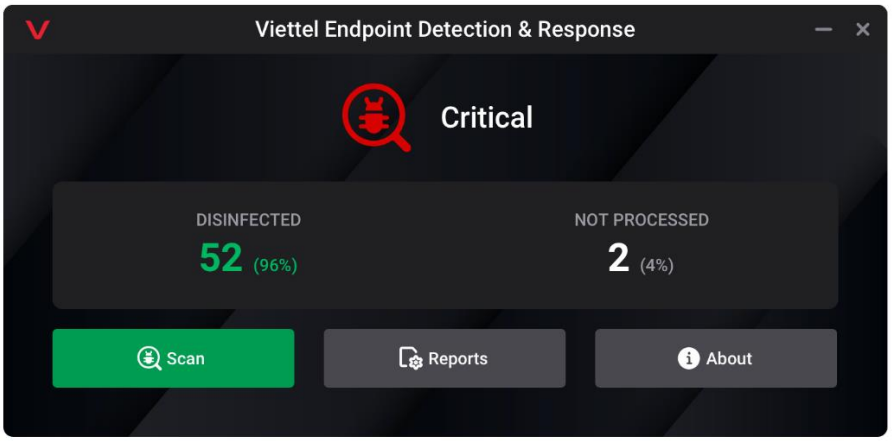
- In case the machine has no malware or all processed malware:



- In case the machine has at least 1 malware and no malware with a critical threat:



- In case the machine has at least 1 malware with critical threat:



Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- In addition, the system displays statistics related to the total number of detected malware as follows:
    - Disinfected: The total number and rate of detected and processed malware
    - Not processed: The total number and rate of detected and unprocessed malware.

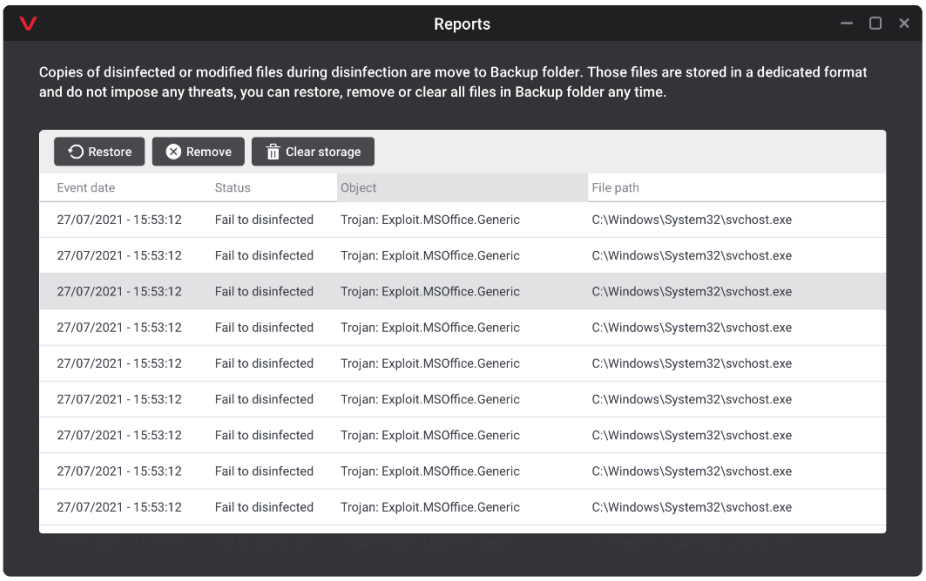
3.2.2. About

The function provides information about Agent version installed on user's machine and product support information.

3.2.3. Reports

The function collects a list of malware detected on the system and the processing status up to the present time.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



For the files containing malware, before they are processed, their originals are stored in the Backup folder. To clean the Backup folder or restore files, the product provides the following features:

Restore: Enable to select 1 file to restore

Remove: Enable to select 1 file to remove from Backup folder

Clear storage: Enable to quickly clean all existing files in the Backup folder.

3.2.4. Scan

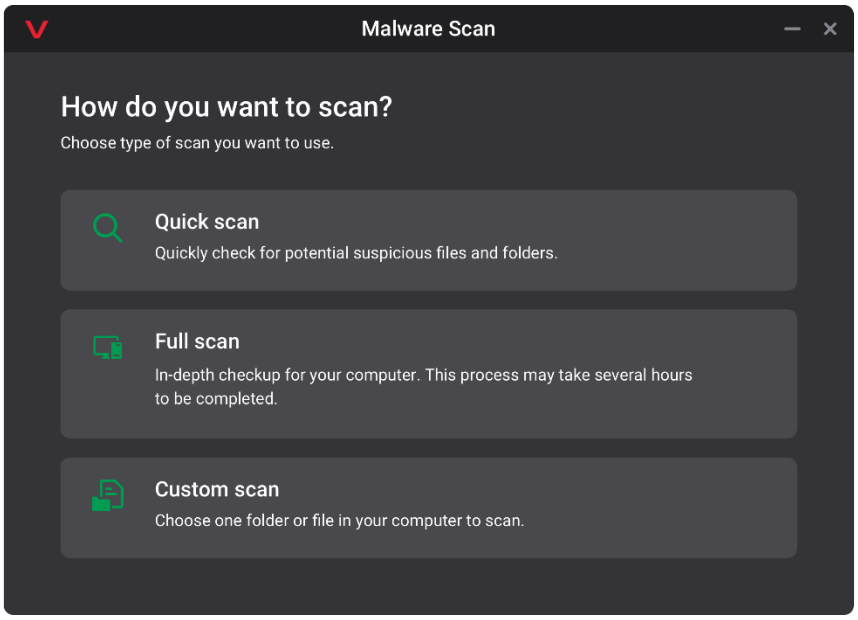
The function allows users to actively use the system to scan and handle malware on the machine.

The supported scanning methods include a set of as follows:

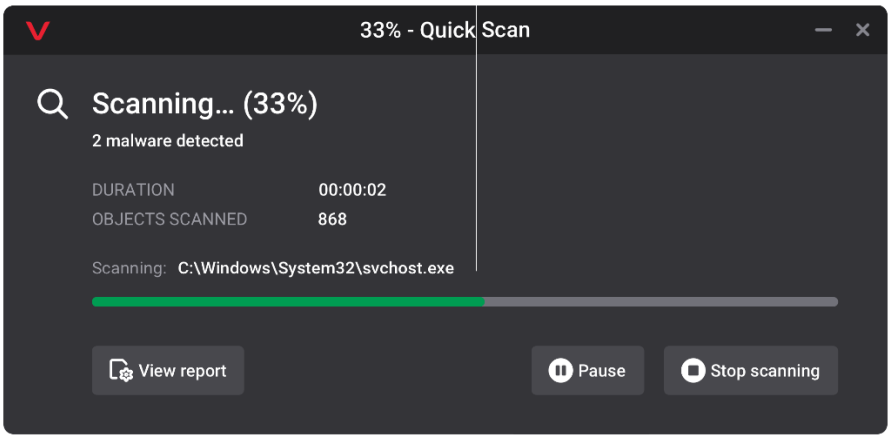
- Select directly from explorer file: Enable to select multiple files and folders, then right-click to select scan (Context scan)
- Select scan methods from agent interface:
  - Quick scan: Scan on a set of predefined folders where malware is frequently generated. When selected, all files and folders belonging to the selected folders will be scanned.
  - Full scan: Scan all files and folders on the user's computer.

Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

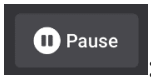
- Custom scan: Similar to Context scan, when this method is selected, the agent displays the explorer file in order to allow the user to select a file or folder to scan.



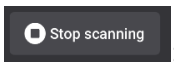
After selecting the appropriate method, the system scans and processes malware:



The following actions during scanning are supported:

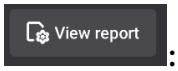


: Enable to pause the scanning process



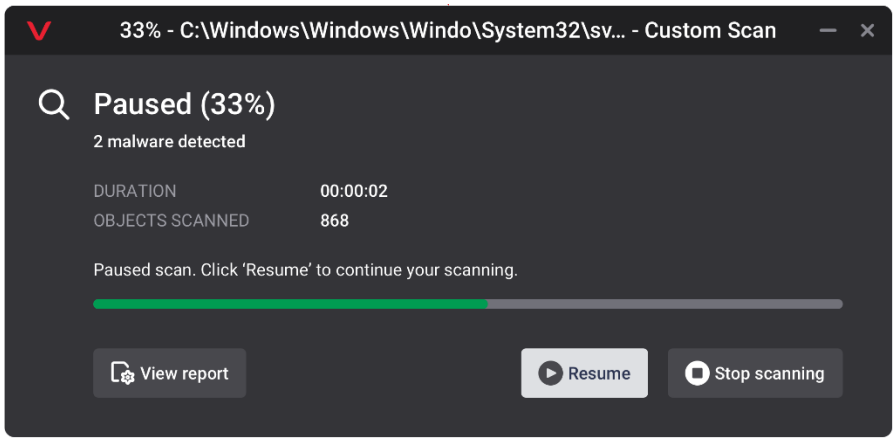
: Enable to stop the scanning process

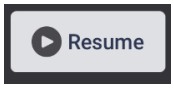
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

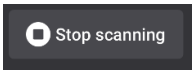


: In case at least one malware is detected, the quick view of the processing status is allowed at 3.14 Reports.

When user chooses to pause the scanning process, the screen is displayed as follows:

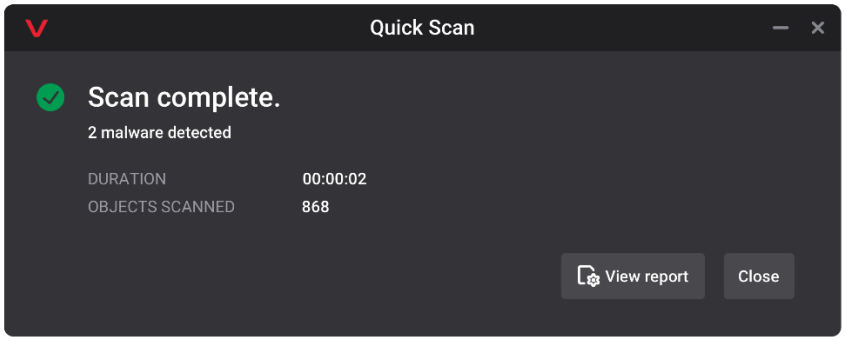


It is possible to select 

to continue scanning or 

to complete the scan process.

When the scan is completed, the result is displayed as follows:



Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com