viettel
security

Viettel Endpoint Detection & Response (VCS-aJiant)

Version 3.3.0 EDR – 2021

Update date: 29 Nov. 2021

User Guide

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
IR Flow	Incident Response Flow: A operational flow to handle alerts, investigations and responses
Artifact	Alert-related investigation objects, such as path file/registry/process
Detection	Object detection related to alerts
Containment	Process isolation in computer, such as network isolation and process suspension
Investigation	Investigation process: Based on event logs or active investigation using tools on the users' machine. The below investigation methods with investigation tools including auto runs and listdlls are supported: • Process Analysis • Search event logs.
Response	Response process: From the investigation results, the operator processes them in the following ways: • Response Scenario • Live Response.
Timeline	A timeline to show activities in IR Flow, including: • Create IR Flow • Create/close Process Analysis session • Create/close Live Response session. • Close IR Flow.

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:

- Improve Login and Process Analysis features according to new interface design
- Improve user experience and add necessary process information to support users in the investigation process
- Improve issues in the old version to ensure stability.

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

2. Overview

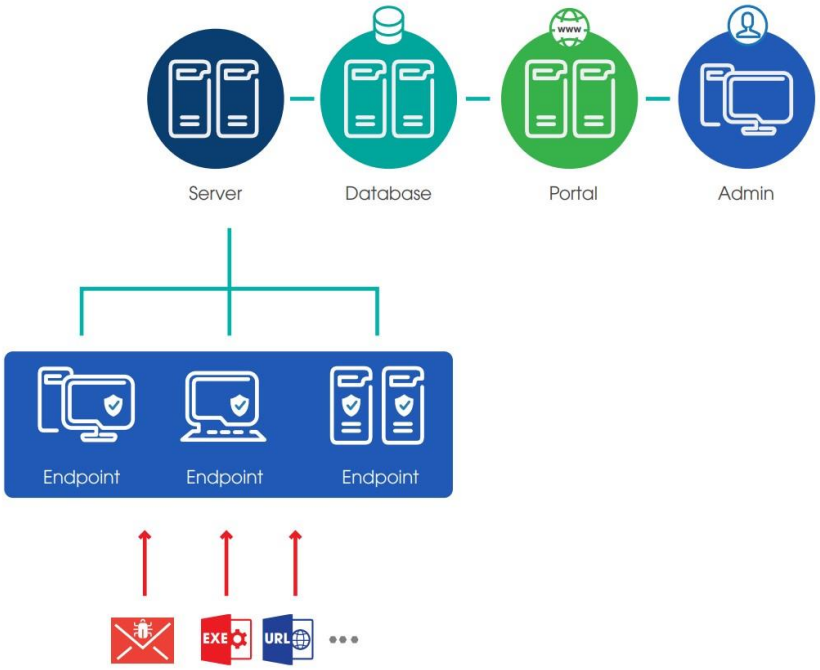
2.1. Technologies

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 IR Flow scenario 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



VCS-aJiant system includes 03 main components:

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

- Agents: A component installed on each computer, responsible for monitoring abnormal signs on the computer and sending logs to a centralized server.
- Cluster of servers for centralized processing and storage: A data processing component, playing a key role in analyzing and processing data sent by the Agent in real time.
- Web Portal: A component for administrators, used to monitor and analyze system information.

2.3. Work with Admin Interface

The Web-portal interface includes the following functional interfaces and processing flows:

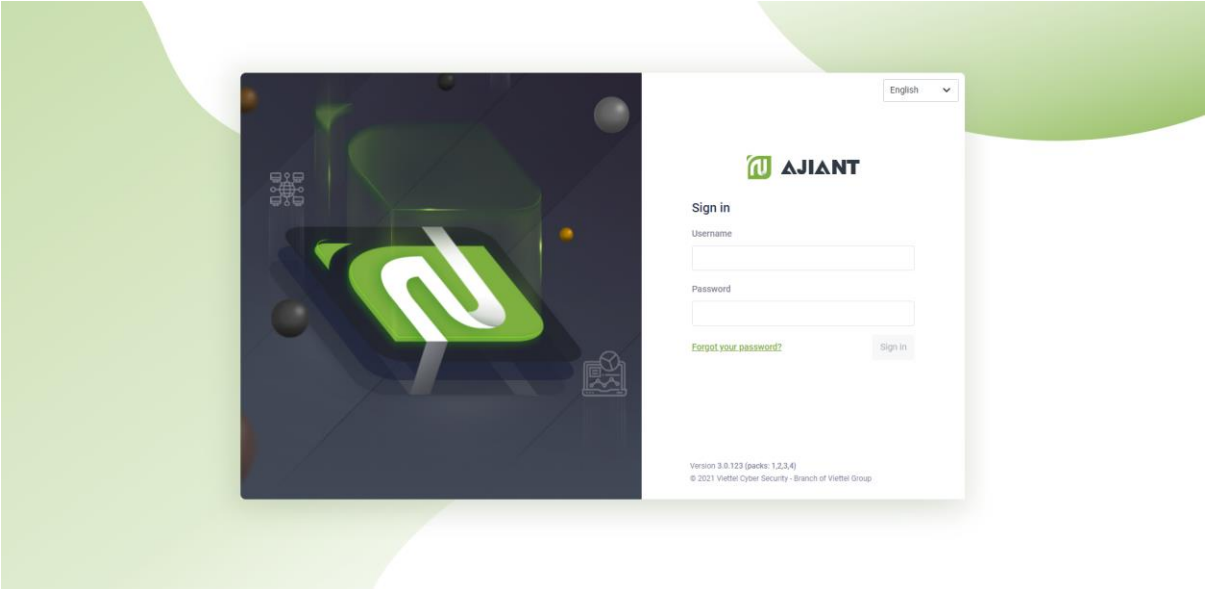
- Dashboard: Statistics and visual charts about the organization's information security situation.
- Alert management: An alert list about signs of malware appearing on the user's computer.
- IR Flow management: A list of IR Flows created by the administrator during the investigation. The flow includes a set of Detection, Containment, Investigation and Response.
- Investigation: A tool list for investigation (Process Analysis, Event search and Deploy tools).
- Response: A tool list for response and incident response (Live response)
- Protect & Prevention: A list of workstation protection and prevention features (Application control and Endpoint firewall)
- Setting: A list of system setting functions (Policy management, Agent management, Group management, Rule correlation and Account management: User, Role, Permission management).

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. Login

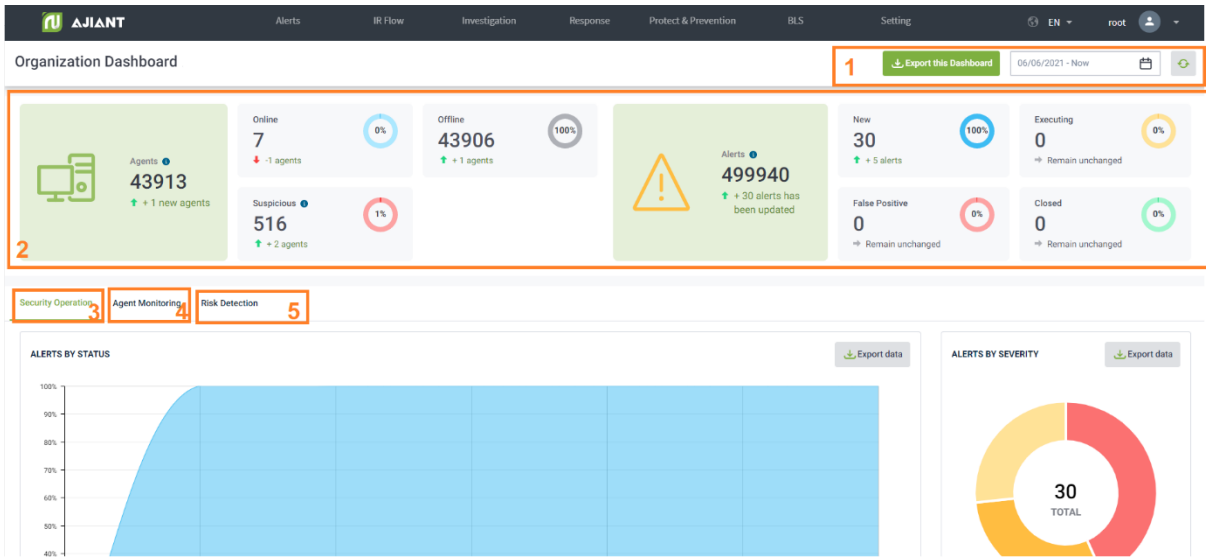
- Access the system at the provided address.



- Login with the provided user/password.

3.2. Dashboard VCS-aJiant

- Main features include as follows:



- Operations with data on Dashboard
  - Export data on Dashboard
  - Search data up to the last 90 days

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

    - 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 child-level groups.
  - 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 child-level groups of the corresponding 1 level group.

3.2.1. Action to Manipulating Data

3.2.1.1. Export Data

This function allows to export the existing data on the Dashboard interface by selecting 

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

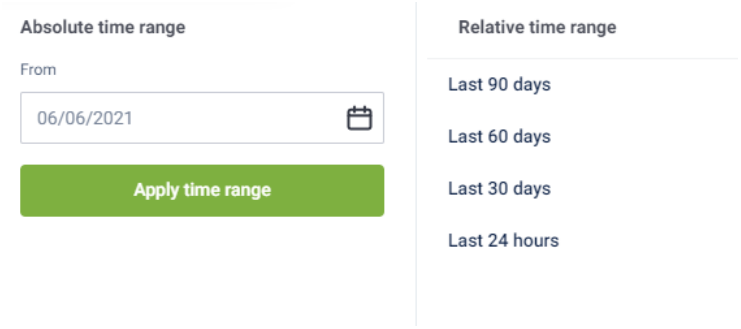
- In case of connection failure or no data on all components of Dashboard, the export is not supported and the action will be hidden.
- In case of having data, support to export files in .xlsx format.

3.2.1.2. Search by Date

This function allows to adjust the time period 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

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



- 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.

- After selecting the time range to monitor, select 

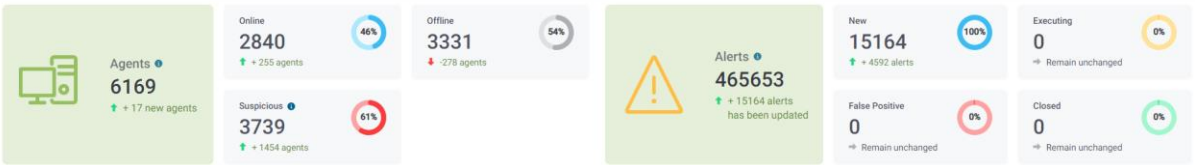
to reload the corresponding data.

3.2.1.3. Refresh Data

This function allows to refresh manual data, select  to update the latest data up to the current time.

3.2.2. Overview Statistics

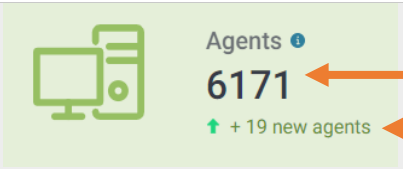
This function allows to quick statistics on the information security situation at the organization according to the selected time range in the search section.



3.2.2.1. Statistics Related to Agents

Statistics	Meaning
	Include 2 numbers 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

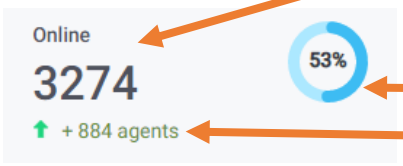


Total number of machines with agent installed in the system (regardless of search time range)

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:



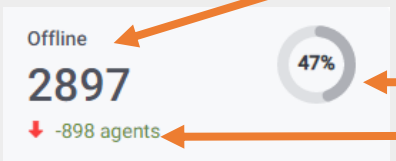
Average number of online machines during the search time range (only counting working time during office hours from 08:00 - 18:00)

Average number rate of online machines compared to the whole system

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)

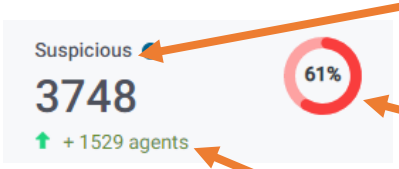
Average number rate of offline machines compared to the whole system

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:

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



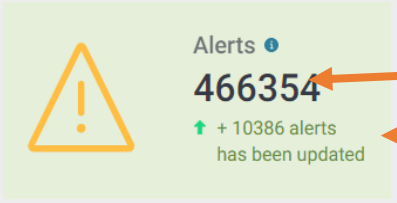
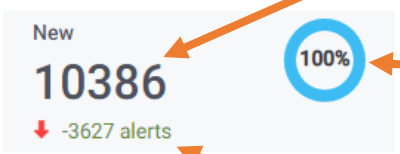
Total number of machines with agent installed in the system (regardless of search time range) generating unprocessed alerts

Rate of machines generating alerts compared to the number of machines in the whole system (regardless of search time range)

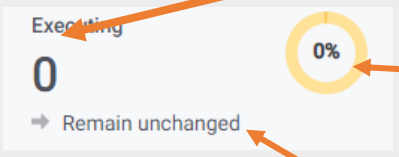
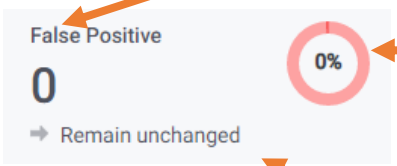
Total number of machines generating alerts during the search time range

(+: New machines generating alerts, Remain unchanged: No new machine generating alerts during the search time range).

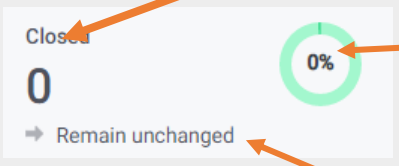
3.2.2.2. Statistics Related to Alerts

Statistics	Meaning
	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

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 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 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

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

	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 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).

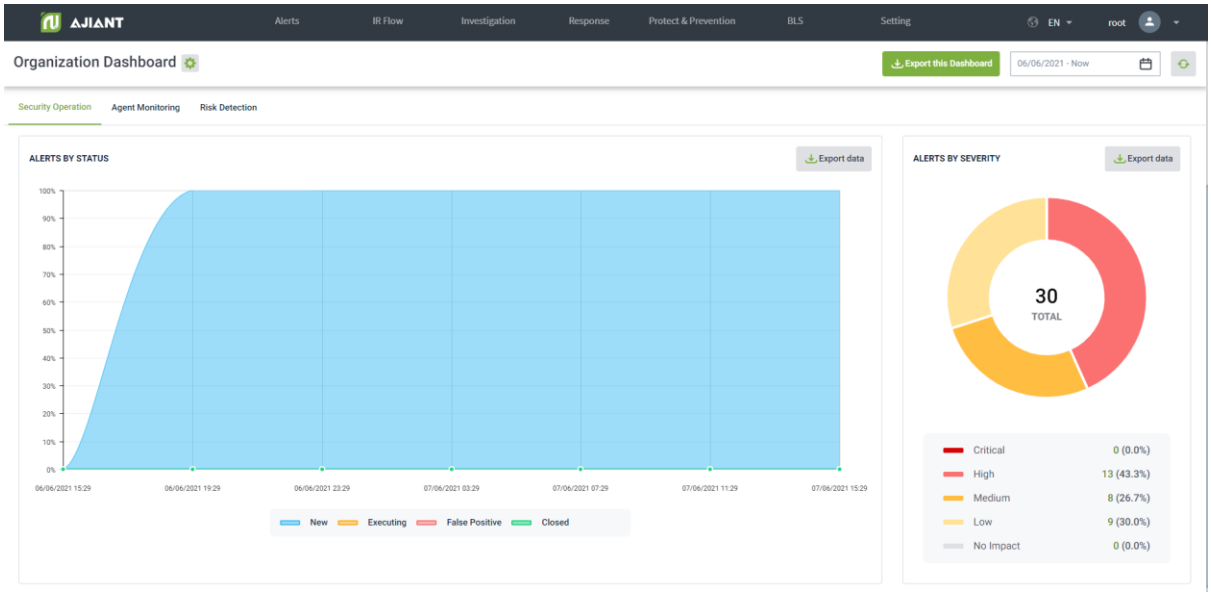
3.2.3. Monitor Security Operation

This function allows to monitor 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

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

- Corresponding data export in the charts.



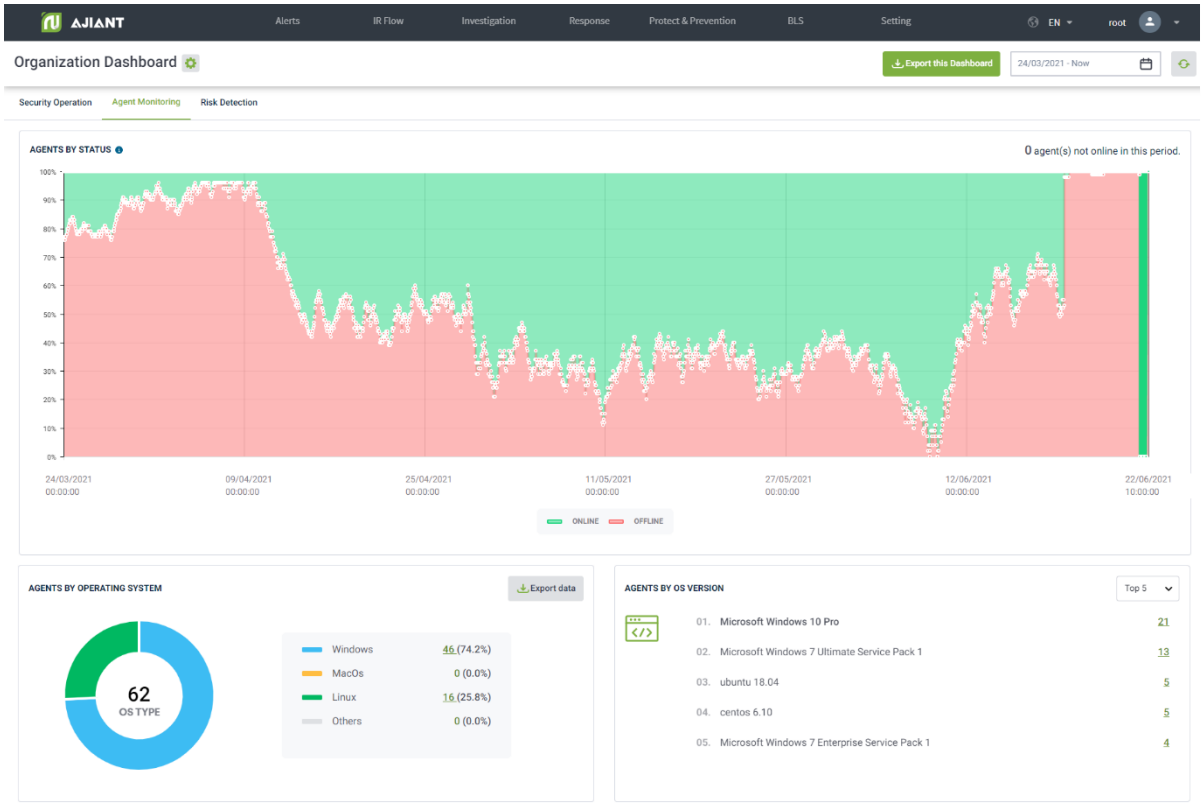
Charts/Statistics	Meaning
Alert by state	Domain chart: Monitor the state of newly recorded or updated alerts during the search time range, including: • X-axis: Time • Y-axis: Alert rate divided by 4 state groups (New, Executing, Closed and False Positive) • Allow selecting Export data to download alert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

3.2.4. Agent Monitoring

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

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



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:

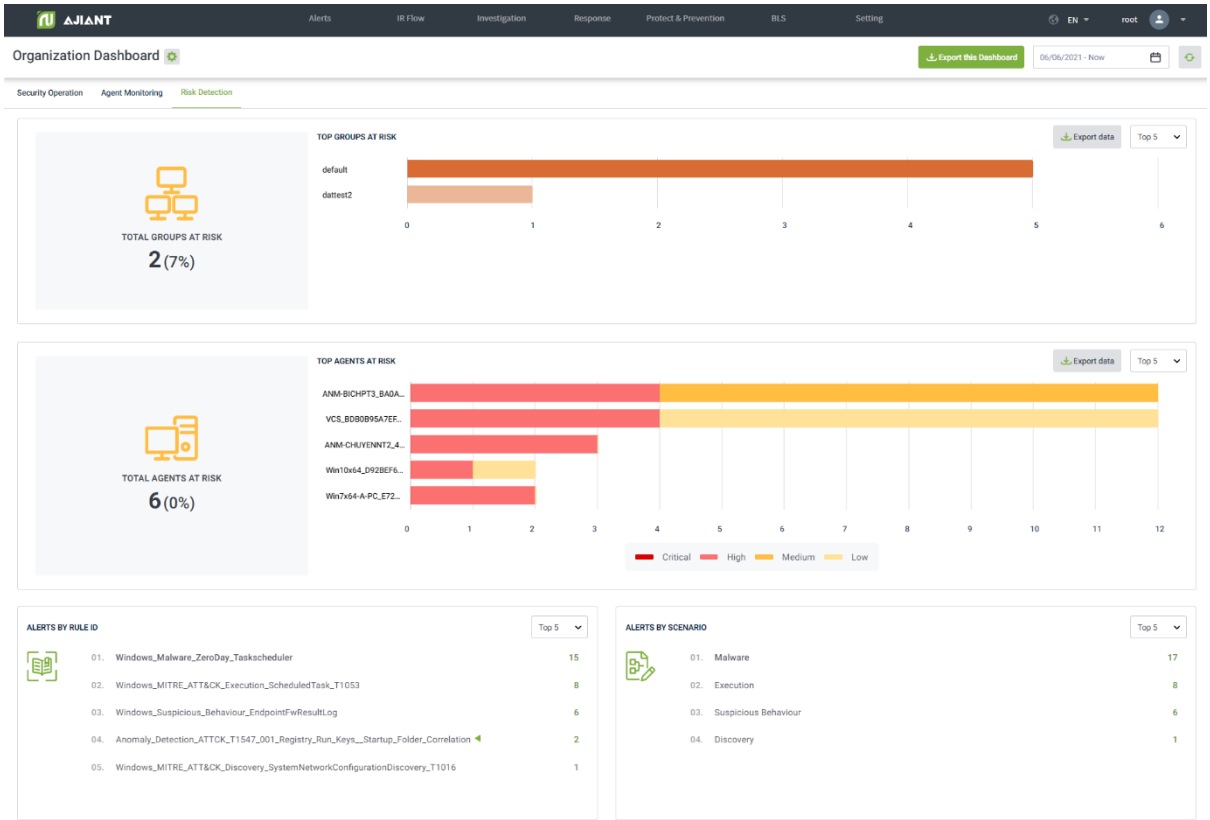
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

	• Rate: Machine rate at each OS • The notes section lists the OS list: Windows, MacOS, Linux and other operating systems. • Allow selecting Export data to download machine lists sorted by OS information.
Agent by OS version	Statistic 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.

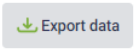
3.2.5. Monitor Risk Detection

This function allows to monitor threats to the organization (through the statistic of the objects that generate the most unprocessed alerts in the system), including:

- Statistic of top groups that generate the most alerts.
- Statistic of top agents that generate the most alerts.
- Statistic 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

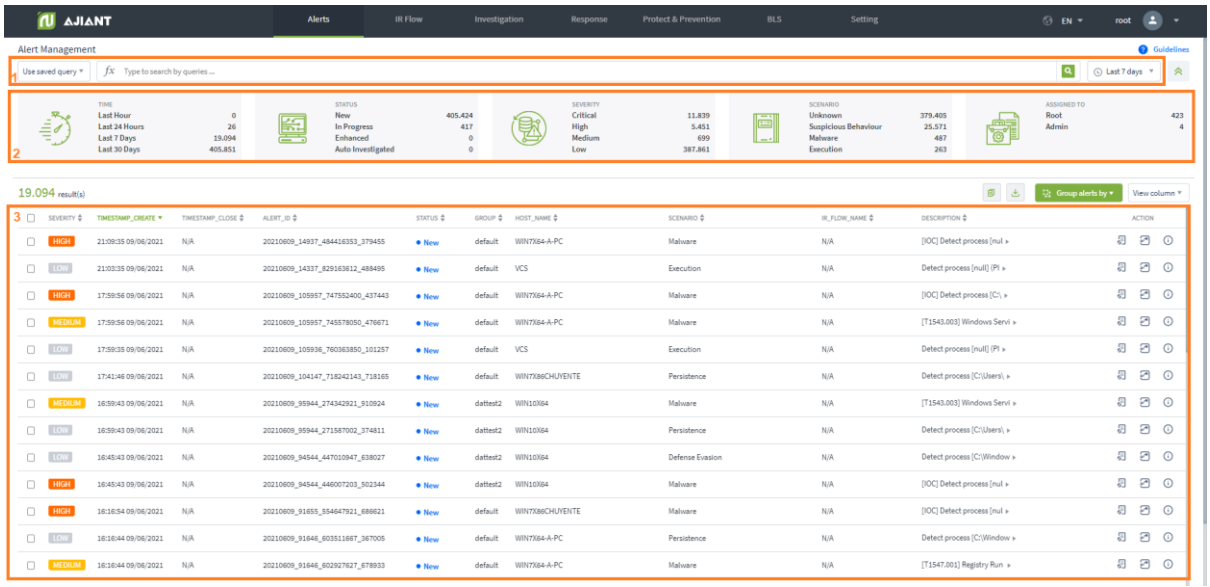
Charts/Statistics	Meaning
Total groups at risk	Total number of groups containing computers with newly recorded or updated alerts (excluding false positive and closed alerts, excluding deleted groups) during the search time range. Rate of suspicious groups to the entire group in the system (excluding deleted groups).
Top groups at risk	Column chart: Statistics 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 • 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: Statistics 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

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 20, Top 50. Default is Top 5. • Allow selecting Export data 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: • Allow changing the statistical period: Top 5, Top 10, Top 15, Top 20. Default is Top 5.

4. Manage Alerts

- Main features include as follows:



  - Search data by query and time
    - Search data by query command and use stored query commands
    - Search data by 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

- Quick search
- Alert list and actions with alert
  - View alert list
  - Group alert
  - View alert summary
  - View 1 alert details
  - View Investigation Graph
  - Mark not dangerous (Set False Positive) for 1 or many alerts
  - Create IR flow from 1 or many alerts
  - Add 1 or many alerts to IR flow

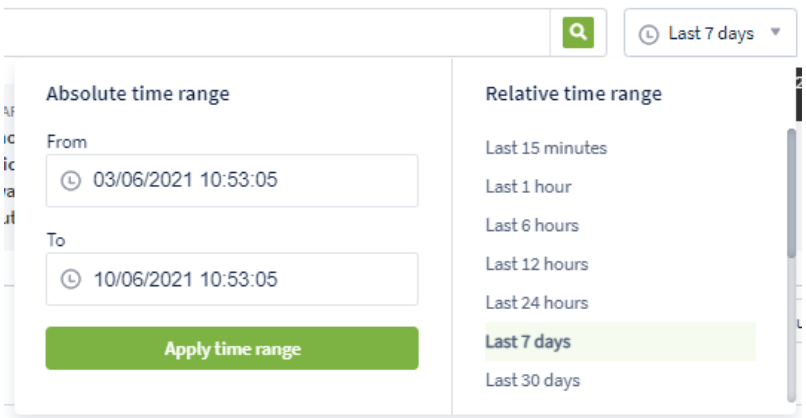
- Data authorization at the following features:
  - User login under root group: Display all alerts in the system.
  - User login under default group: Display all alerts belonging to the default group.
  - User login under parent group: Display all alerts belonging to the group of the user logging in and the corresponding child-level group.
  - User login under a group with one child-level group or many child-level groups: Display all alerts belonging to the group of the user logging in.

4.1.1. Search Alerts

Allow creating a query command, using a stored query command or quickly searching to search for an alert by the time that the alert was generated.

4.1.1.1. Search by Time

- Default when accessing the system, search alert according to the last 7 days.



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 time value by selecting absolute time or relative time
  - Absolute time: A specific start time - end time value, which allows entering or choosing from the calendar and supports dd/mm/yy, hh:mm:ss format.
  - Relative time: A relative time between the start time and current time.

For example, it is currently 3 am on 07/06/2021, select start date is “Last 30 days”. The system automatically searches the last 30 days and starts from 03:00 hour of that day. → Monitoring period: 03:00 08/05/2021 to 03:00 07/06/2021.

4.1.1.2. Quick Search

Quick Search supports quick alert search by fields:

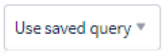
- Time: Time to generate alert
- State: The state of the alert
- Severity: The severity of the alert
- Scenario: The scenario that generates the alert.
- Assigned to: The person assigned to handle the alert.

4.1.1.3. Search by Query

This function allows to search by query in 2 below ways:

- Use the previously saved query to search
- Enter the query to search

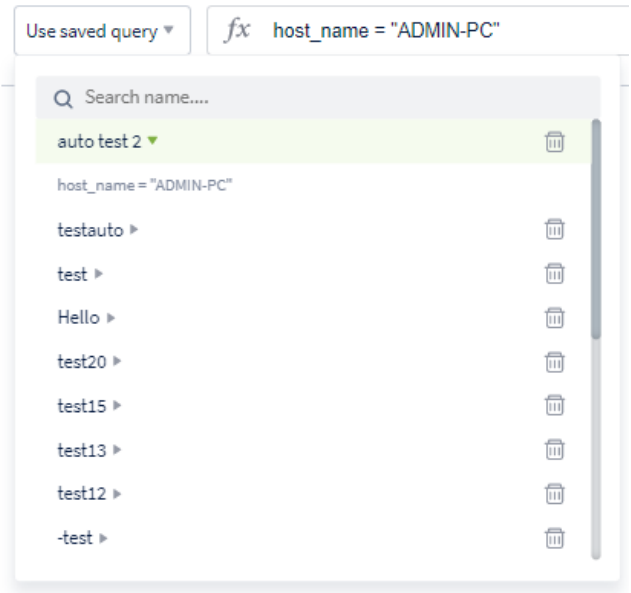
4.1.1.3.1. Use Previously Saved Query to Search

- Step 1: Select the previously saved query at the 

combo box.
- Step 2: Review the query content before selecting by selecting .

  In case of deleting the old query, move the cursor to the record to delete and select  .
- Step 3: Click on the record to use in order to query, the old query content is displayed in the query input 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



In case of adding or editing the query content, enable to enter right on the query box and select Save query to save.

Notes: The Save query button is only displayed when the query has correct structure.

4.1.1.3.2. Enter a query to search

- Step 1: Enter query into the Search textbox with the following format:

<field_name> <operator> “<value>” AND/OR <field_name> <operator> “<value>”

In which:

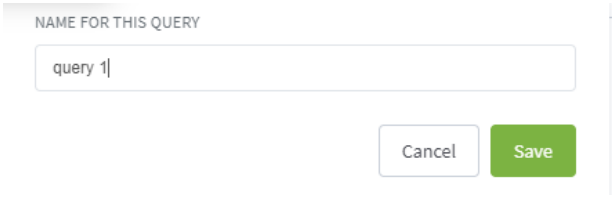
- <field_name> are the following values:
  - Severity: The severity of the alert.
  - Alert_id: Alert code.
  - State: The state of the alert.
  - Group: The group of the event that generates the alert.
  - Hostname: Name of the workstation.
  - Scenario: The scenario that generates an alert based on MITER ATT&CK.
  - Ir_flow_name: The name of the IR flow to which the alert belongs to that IR flow.
  - Assignee: The person assigned to handle the alert.
  - Signature_id: Event code that generates the alert.

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

- Rule_id: Code of the rules generating alerts
- Description: Describe the context information the alert generated.

  - <operator> are the following values:
    - =: Find an exact value as the value
    - !=: Find a value other than the value
    - ~: Find a value including the value
    - AND/OR: Combination operators to combine 2 queries.

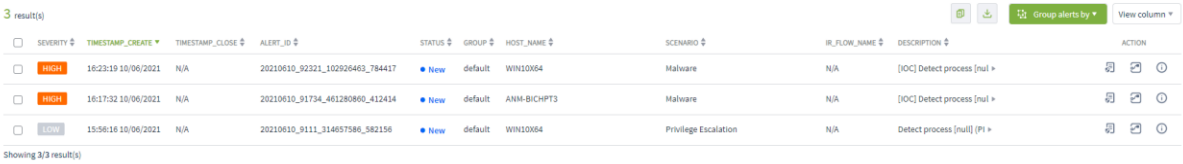
- Step 2: Click on Search.
  - In case there is no matched result, the system will display the notification as No data.
  - In case there is a matched result, the system defaults to display 50 records in descending order by time. To view more records, scroll the data to the bottom of the page, the system will load the next 50 records.
- Step 3: In case the query has the correct structure to save it for future usage, select Save query and enter a name to remind the query:



Notes: The Save query button is only displayed when the query has correct structure.

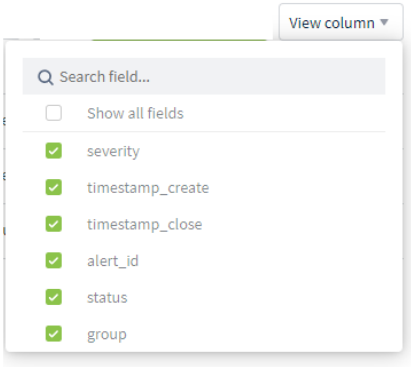
4.1.2. Alert List

This function allows to view a list of alerts that meet the search condition.



- Step 1: Select View column to select the fields to display on the Alert List.

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

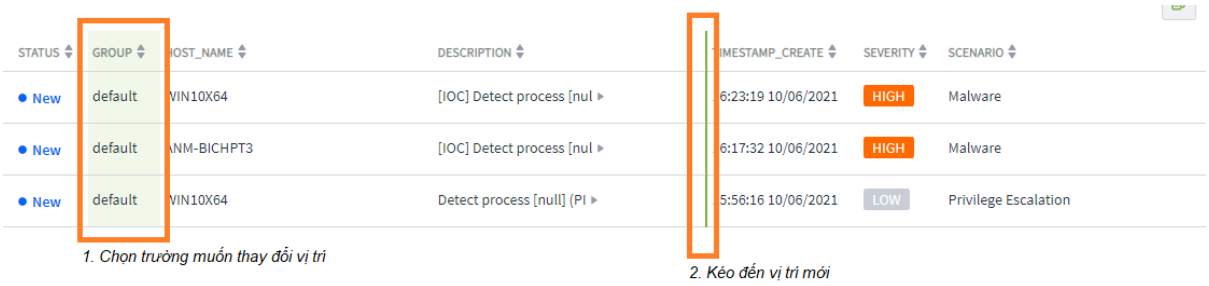


Here, searching information fields by field name is allowed and select/deselect all fields are supported.

- Step 2: On the list, the operations are supported as follows:
  - Sort by data in each column

For example, to sort the data by the creation time field, click TIMESTAMP_CREATE the first time at the field name to sort by the ascending creation time, click TIMESTAMP_CREATE the second time to sort by the descending creation time, click the third time to remove the sort and return to original state TIMESTAMP_CREATE .

  - Drag and drop the information field to the desired position



    - Click once to view summary information, view details at section 3.3.4 View Alert Summary.
    - Click twice or select to view detailed information, view details at section 3.3.4 View Alert Summary.
  - Select to mark Not Dangerous for alert, view the marked case of 1 alert at section 3.3.5 Mark Not Dangerous for 1 Alert/Multi-Alerts or Alert Group.
  - Select to insert alert into IR Flow, view the inserted case of 1 alert into an existed IR Flow at section 3.3.7 Add 1 Alert/Multi-Alerts or Alert Group into an Existed IR FLow or into a new IR Flow at section 3.3.6 Create a New IR Flow from 1 Alert/Multi-Alerts or Alert 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

- Select to view the reason for marking Not Dangerous in alerts that are in the FALSE POSITIVE state.

- Step 3: After completing the actions on the records, selecting one or more records is allowed by clicking at the top of each alert to continue performing next actions with the below supported actions.

  - Select Add to IRFlow to add the selected alert to the IR Flow for processing.

Notes: This action is only applied when all selected alerts are in NEW state. If there is at least one alert in state different from NEW, the action will be hidden the Add to IRFlow button. View details in case of adding 1 alert to a new IR Flow at section 3.3.6 Create a New IR Flow from 1 Alert/Multi-Alerts or Alert Group or add to an existing IR Flow at section 3.3.7 Add 1 Alert/Multi-Alerts or Alert Group into an Existed IR FLow.

  - Select Set false positive to mark Not Dangerous for alert.

Notes: This action is only applied when all selected alerts are in NEW state. If there is at least one alert in state different from NEW, the action will be hidden the Set false positive button. View details in case of marking Not dangerous 1 alert at section 3.3.5 Mark Not Dangerous for 1 Alert/Multi-Alerts or Alert Group.

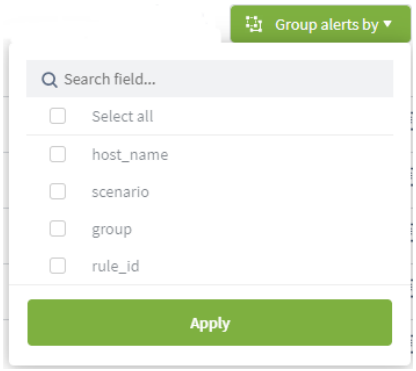
  - Select Export selected alert(s) to export the currently selected alert.

4.1.3. Group Alert

This function allows to group alerts by one or more criteria, including: hostname, scenario, group and RuleID.

- Step 1: After searching, alerts can be grouped by selecting Group alerts by to select the criteria to use as alert grouping criteria.

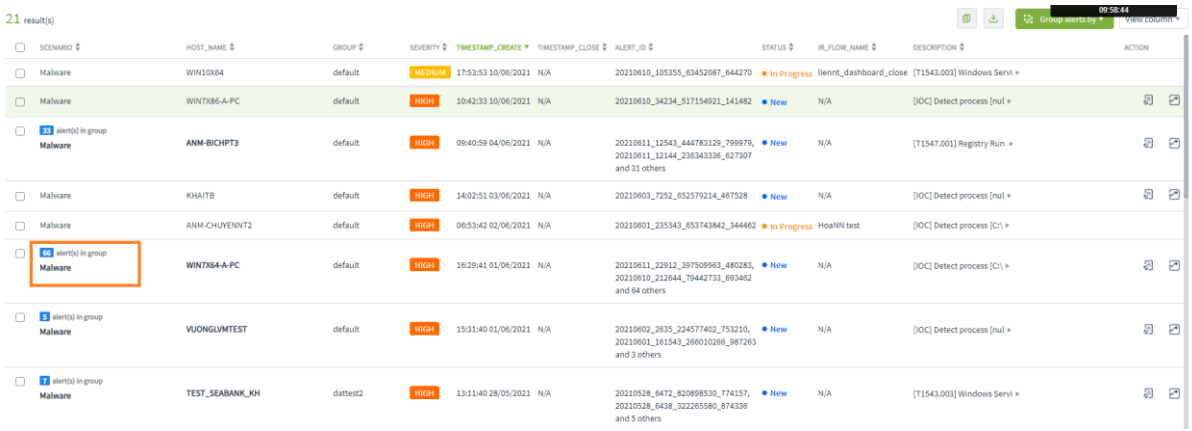
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Support searching by criteria name and selecting 1 or more criteria to group

- Step 2: Select  to apply.

Alerts that have the same selected criteria and same state and are in the same IR Flow (if any) will be grouped into 1 row in the result list.

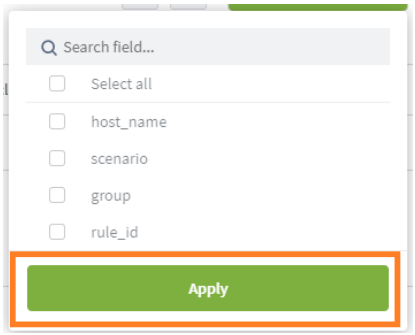


In which:

- Fields used as grouping criteria will be bolded.
- The number of grouped alerts is displayed at the selected criteria.

- Step 3: To ungroup, perform the same actions but do not select any criteria and select Apply only.

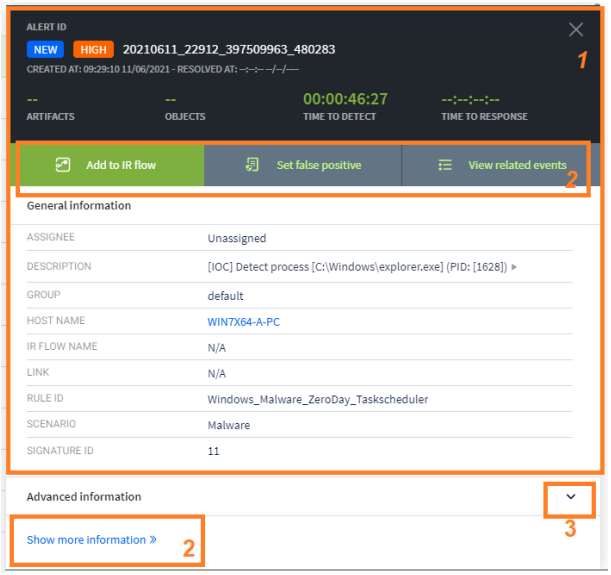
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



4.1.4. View Alert Summary

This function allows to quickly view the alert summary information.

- Step 1: Click once on the alert to view the summary, the following information is displayed:

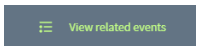


  - General information group of alert, in which:
    - Artifacts: List of suspicious objects automatically/ manually marked in alert.
    - Objects: List of objects in alert.
    - Time to detect: Total time to detect and investigate alert, from when the alert is generated to when it is inserted into the IR Flow or marked FALSE POSITIVE.
    - Time to response: Total alert processing time, from when the alert is inserted into IR Flow to when IR Flow is closed.
  - Group actions with alert

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 

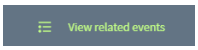
to insert alert into IR Flow, view the case of inserting 1 alert into an existed IR Flow at section 3.3.7 Add 1 Alert/Multi-Alerts or Alert Group into an Existed IR FLow or into a new IR Flow section 3.3.6 Create a New IR Flow from 1 Alert/Multi-Alerts or Alert Group.
- Select 

to mark Not dangerous for alert, view the case of marking 1 alert at section 3.3.5 Mark Not Dangerous for 1 Alert/Multi-Alerts or Alert Group.
- Select 

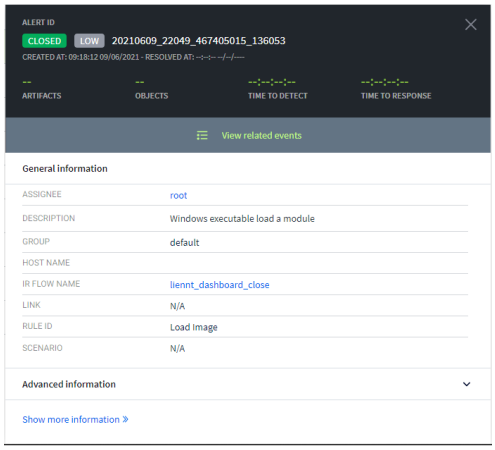
to switch to the Event Search feature with the default time of last 4 hours and after the time the alert generated.

Notes: The action of 

and 

is only displayed for the alert in the NEW state, in case the alert is different from NEW, only the following 

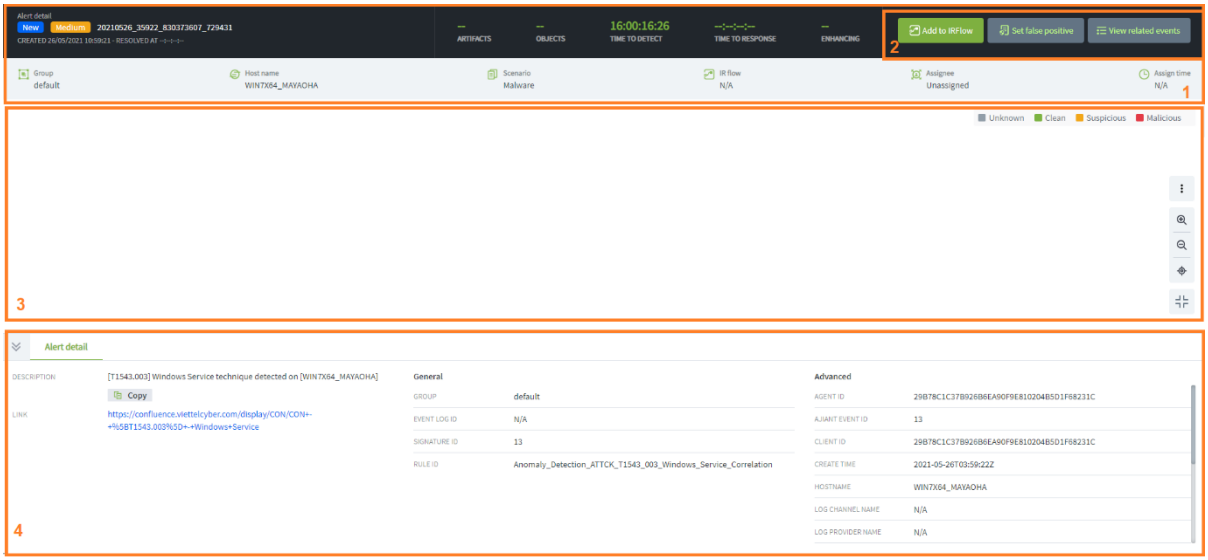
button is displayed:



4.1.5. View Alert Details

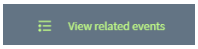
This function allows to view detailed alert information, support automatic information enrichment by automatically collecting information about events related to the alert that has just arisen, and provide a visual chart to quickly view the relationship between objects included in the alert.

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



- General information group of alert, in which:
  - Artifacts: List of suspicious objects automatically/ manually marked in alert
  - Objects: List of objects in alert
  - Time to detect: Total time to detect and investigate alert, from when the alert is generated to when it is inserted into the IR Flow or marked FALSE POSITIVE.
  - Time to response: Total alert processing time, from when the alert is inserted into IR Flow to when IR Flow is closed.
  - Enhancing: The completion rate of the system's automatic information enrichment process.
- Group actions with alert
  - Select 

to insert alert into IR Flow, view the case of inserting 1 alert into an existed IR Flow at section 3.3.7 Add 1 Alert/Multi-Alerts or Alert Group into an Existed IR FLow or into a new IR Flow at section 3.3.6 Create a New IR Flow from 1 Alert/Multi-Alerts or Alert Group.
  - Select 

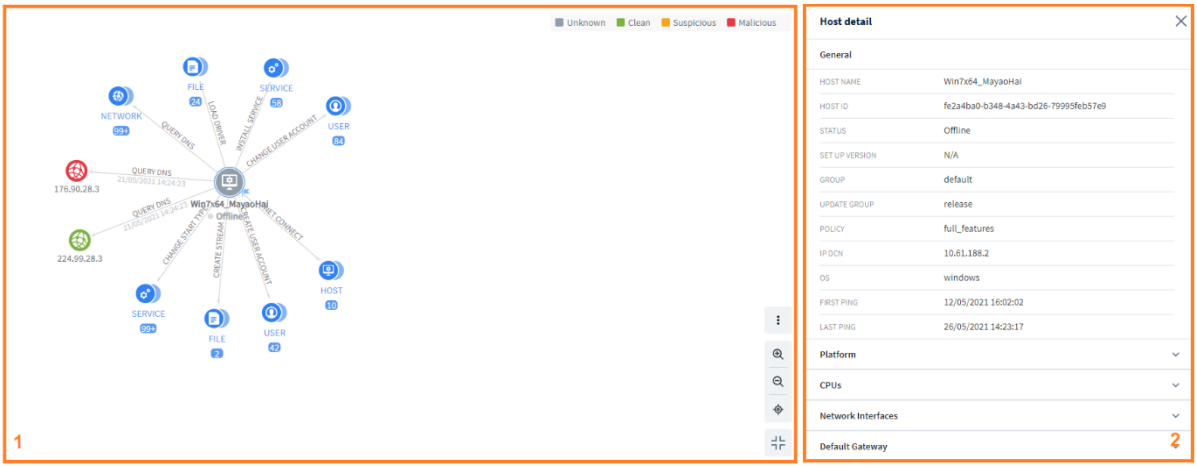
to mark Not dangerous for alert, view the case of marking 1 alert at section 3.3.5 Mark Not Dangerous for 1 Alert/Multi-Alerts or Alert Group.
  - Select 

to switch to the Event Search feature with the default time of last 4 hours and after the time the alert generated.
- Investigation Graph: View details at section 3.3.5 Investigation Graph.
- Information tab related to alert: Currently only Alert Detail is 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

4.1.6. Investigation Graph

This function allows to display the object relationship in the alert, view the object details and support the spill investigation based on the set of events collected in the system.

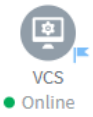


1 - Graph display area and graph actions

2 - Detailed information display area of objects on the graph

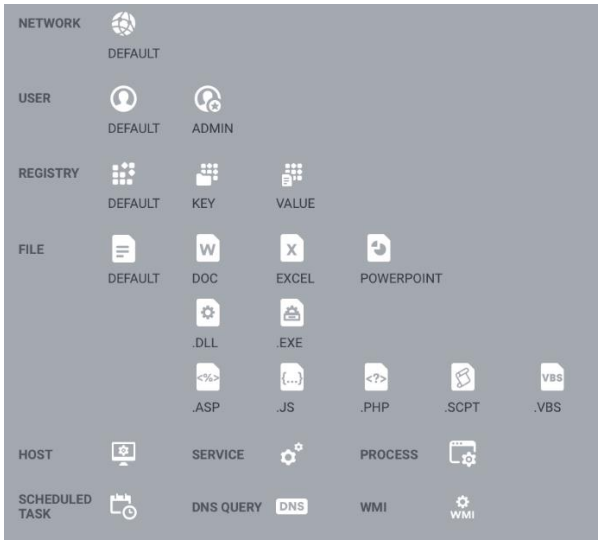
4.1.6.1. Graph Display Area and Graph Actions

- This function allows to visually display the objects in the alert for information view and investigation.
- By default, when accessing, the graph displays information related to the original machine that generates an alert, specifically as follows:



- In the graph, there is always a flagged machine to mark the original machine that generates the alert, and by default, each machine always comes with the objects that have a direct relationship with the original machine within 1 day from the time the alert is generated. The list of objects includes 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



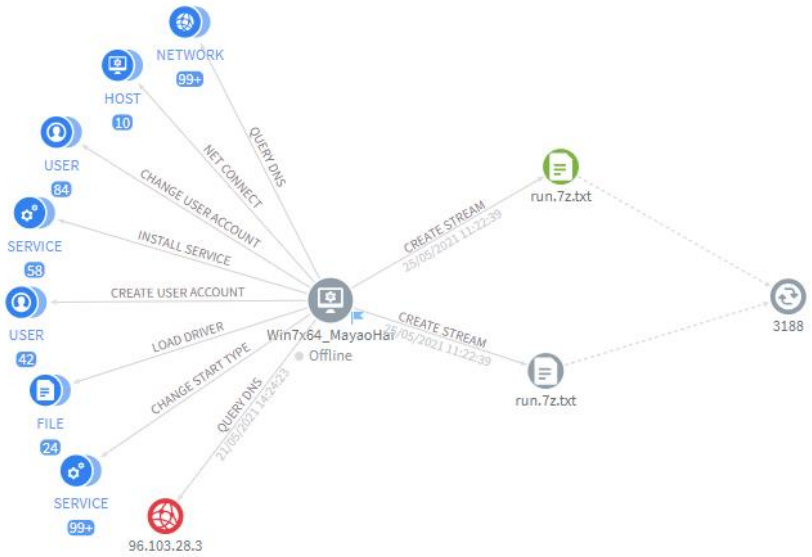
- Each object includes the following state: 

- Among objects, the relationships are displayed, including:
  - Relationship: The relationship is defined according to the events arising within 1 day from the time the alert is generated (where the relationship name is above the solid line arrow connecting 2 objects.):

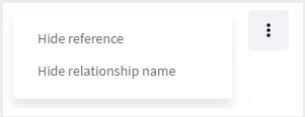
  - Reference: Reference relationship, which is other objects recorded in the main event that generated the object (shown by a dashed line arrow and without a specific relationship name):

For example:

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



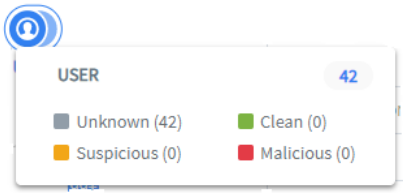
- Actions to support graph display, including:

Display support actions	Meaning
	Enable to hide/show information on the graph, including: • Reference: When selected, enable to hide/ show reference information, including dashed line arrow and reference object at all existing objects on the graph. • Relationship name: When selected, enable to hide/ show the relationship name information above all existing solid line arrows on the graph.
	Enable to zoom in/ zoom out the corresponding graph at the position of the pointed cursor. In addition, enable to roll the cursor the desired position to zoom in/ zoom out for quick action.
	Enable to return to the graph center (original machine).
	Enable to zoom in the maximum screen in order to view graph and perform action on it.

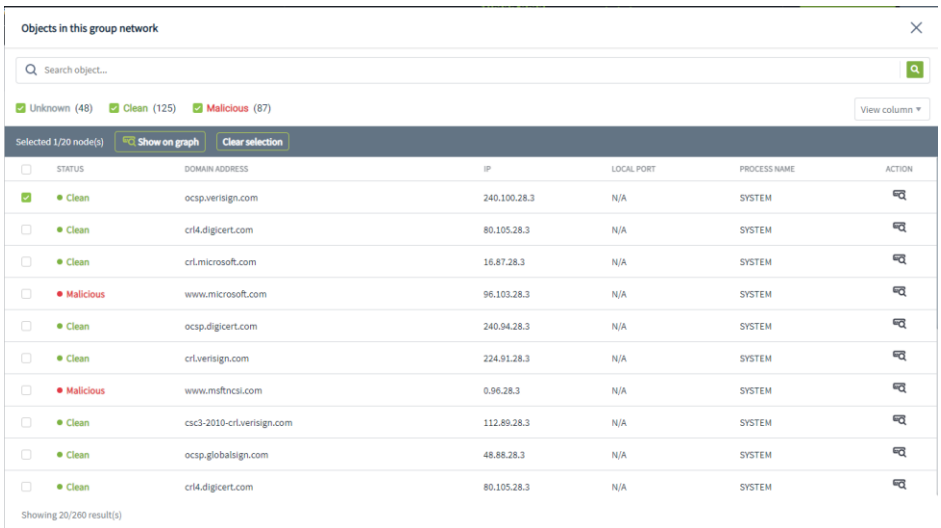
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- An example of a default graph as follows:

- In case each object type has more than 1 dependent object, the objects will be automatically grouped.
- Hover to view quick statistics at each object group as follows:

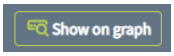


- From here, for further spill investigation to the objects, perform the following steps:
  - Step 1: Click on the group of objects to view, the interface is displayed as follows:



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

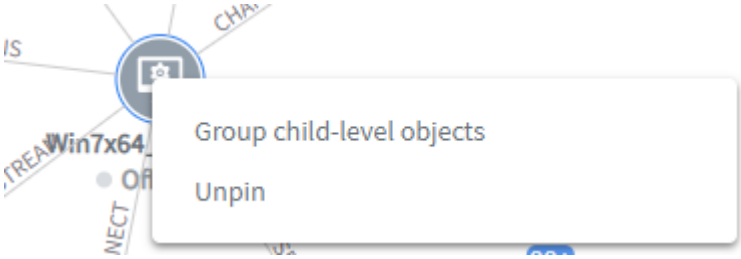
- Enable to filter objects in the group by state

or quickly search by entering the data to search in all fields.
- When a suitable object selected, select  to display 1 object on the graph or select 

to select up to 20 objects on the graph.

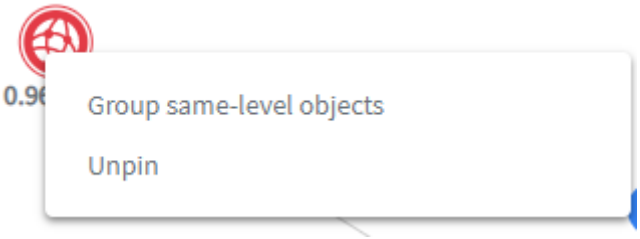
Notes: If the expanded object is a computer, when the object is displayed by default, the objects that have direct relationships to the computer within 1 day from the time the alert generated are also automatically displayed.

- Step 2: After displaying the objects to be investigated on the graph, the below support actions enable to expand/ collapse are displayed:
  - At the original machine/ normal computer: Support collapsing objects to the default state when displaying the machine (Only include objects that have a direct relationship with the machine and for each object type if there is more than 1 object inside, a group form is displayed) by right-clicking on the object, then selecting Group child-level objects.



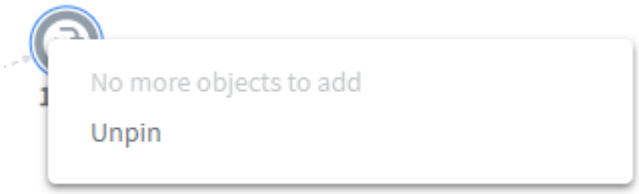
  - At other objects: Support collapsing by grouping by object type and relationship type with objects of the same level by right-clicking on the object, then selecting Group same-level objects.

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

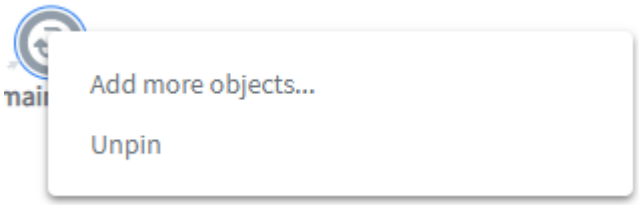


- At the object is a process, allow expanding for spill investigation by right-clicking on the object,

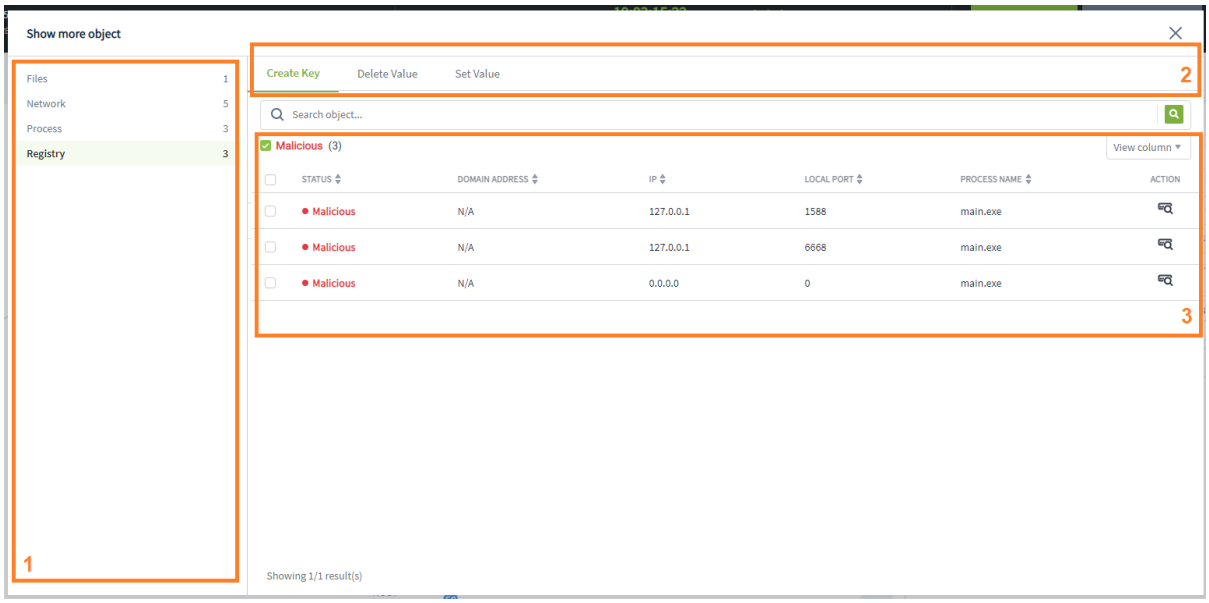
In case it is not possible to continue the spill, the following is displayed:



In case of the spill, select Add more objects...



The interface that allows selecting the object to be spilled is displayed as follows:



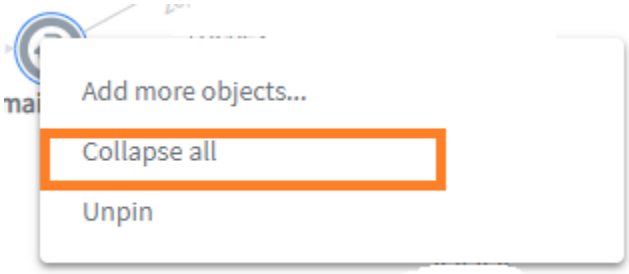
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- Select object type
- Select the relationship type from process to object
- Directly select the object to display. Support searching by object's Malicious or Clean state or searching by content in the object's information fields.

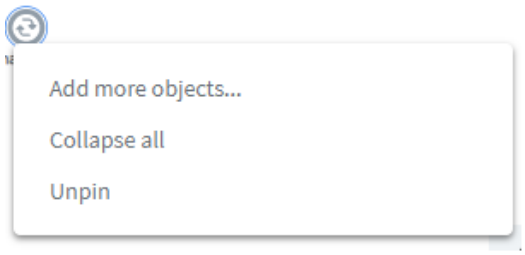
Select View column to select the display information fields or use the feature to sort information in the list.

When a suitable object is selected, select to display 1 object on the graph or select Show on graph to select up to 20 objects on the graph.

- At the object which is a process, when there are objects being expanded, it is allowed to collapse by right-clicking on the object as follows:



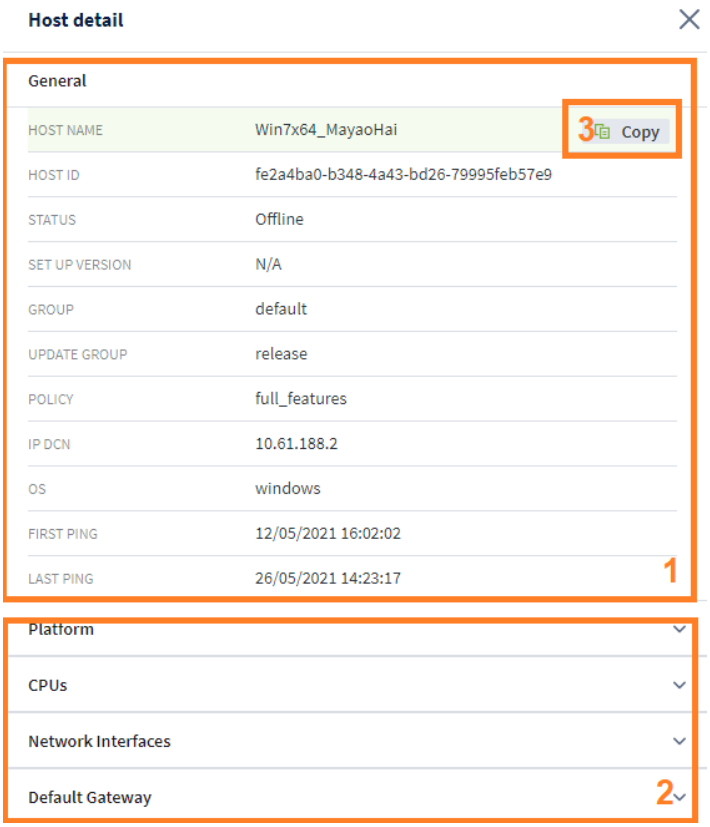
- By default, in the graph, objects automatically run and keep their distance from each other when moved. In case of using the cursor to select and drag and drop objects, after removing the cursor, the object is automatically pinned to a new position. To cancel the Pin action, select Unpin.



4.1.6.2. Detailed Information Display Area

As an additional feature of the graph, allow displaying detailed element information in the graph (including objects and relationships in the graph).

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

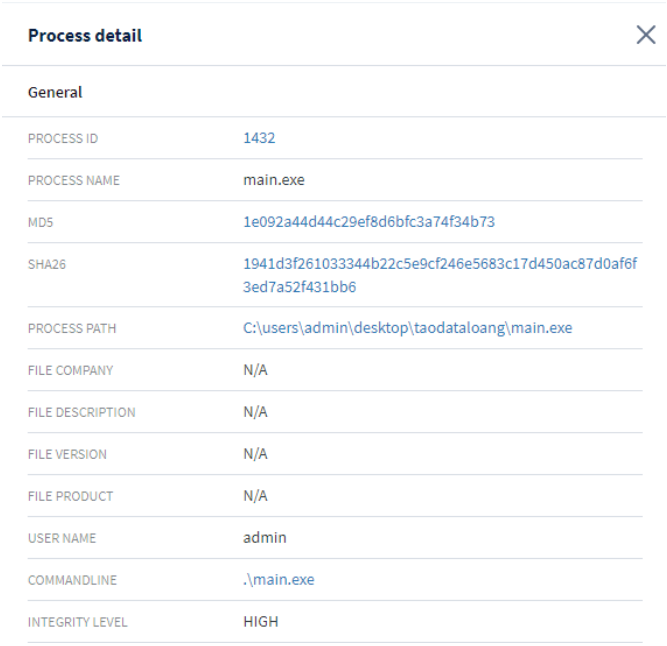


- Group of general information: Including general information/identifying information of the object and always displayed when accessing.
- Detailed information group: Include detailed information of object classified into different information groups which will be closed by default, select ˅ to expand and display the information group.

The Copy action supports copying the information field content.

Notes: Some object identifying information fields allow quickly linking to look up in Event Search or Agent Management.

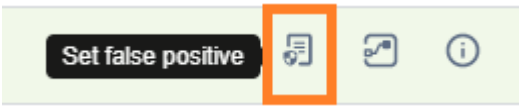
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



4.1.7. Mark Not Dangerous for 1 Alert/Multi-Alert or Alert Group

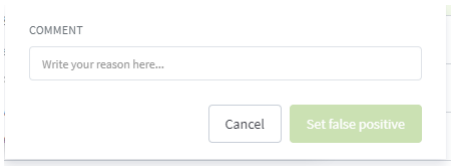
This function allows to mark alert as Not dangerous and Not continue processing as follows:

- Step 1: Select 1 alert or multi-alerts to mark as Not dangerous.
- Step 2: Click on the Set False Positive button (Set False Positive button is only displayed in record with the NEW state as or all selected records are in NEW state.)



- Step 3: Enter the reason for marking Not dangerous and select 

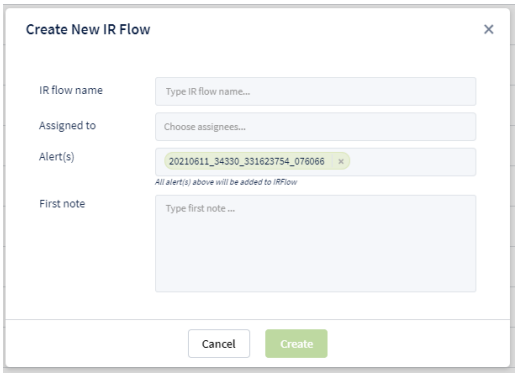
.



4.1.8. Create IR Flow from 1 Alert/Multi-Alert or Alert Group

- Step 1: Select 1 alert/multi-alerts to create IR Flow.
- Step 2: Enter the information and create IR Flow.

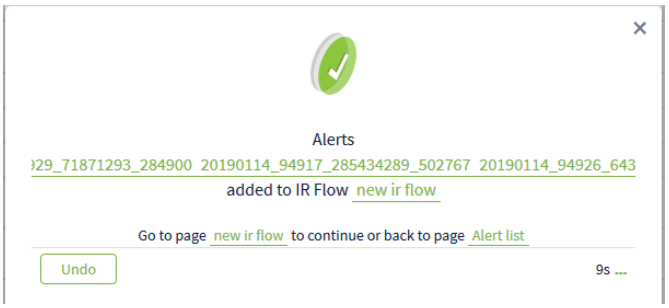
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



The data displayed in the Assigned to combo box include as follows:

- User login under root group: Display all user names in the system.
- User login under default group: Display the username of the current user login.
- User login under parent-level group: Display all user names belonging to the child-level group of the current user login and the own current user login.
- User login under a group of one or more child-level group: Display the username of the current user login.

- Step 3: After creating, the following window displayed to be able to undo in 10s:

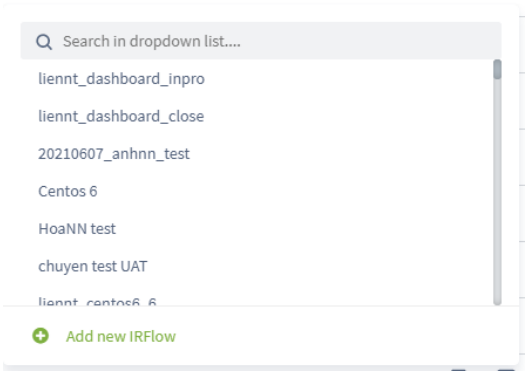


- To undo: Select Undo for 10 seconds.
- To create an IR Flow immediately and switch to the IR Flow screen, select the name of the newly created IR Flow and then select New IR Flow.
- To back to the alert screen, select Alert List.

4.1.9. Add 1 Alert/Multi-Alert or Alert Group into Existed IR Flow

Same as the 3.3.5 section but do not select Add new IR Flow and select an existed IR Flow from the drop-down list only:

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

5. IR Flow Screen

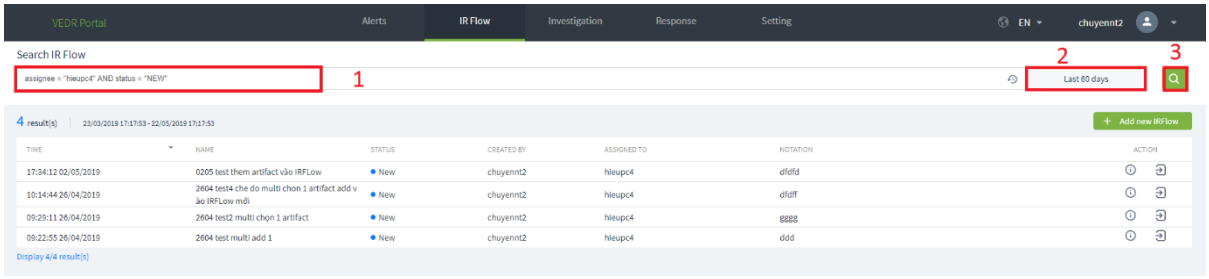
5.1.1. Display List

- User login under root group: Display all IR Flow in the system.
- User login under default group: Display all IR Flow assigned to the current user login.
- User login under parent-level group: Display all IR Flow assigned to the user login and the users belonging to the respective child-level group.
- User login under a group of one or more child-level group: Display all IR Flow assigned to the current user login.

5.1.2. Search IR Flow

Only the records corresponding to the current user login can be searched.

Similar to the Search function in the Alert screen, the IR Flow screen supports searching by query as follows:



- Step 1: Enter into the Search query textbox with the following format:

<field_name> <operator> “<value>” AND/OR <field_name> <operator> “<value>”

In which:

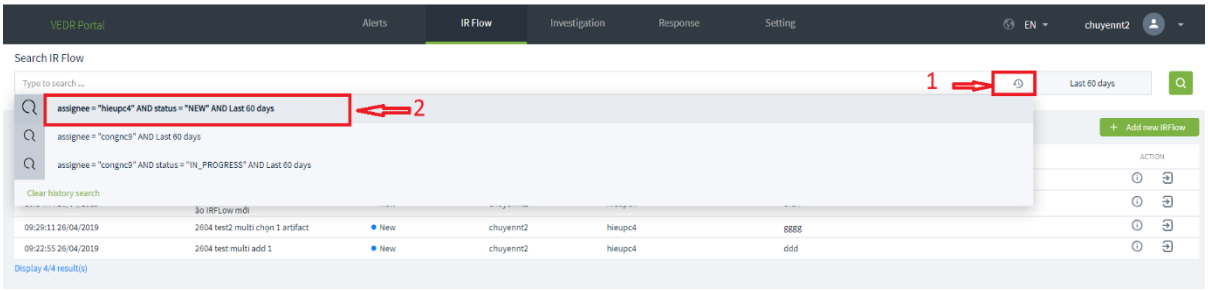
  - <field_name> are the following values:
    - Assignee: The person assigned to handle the alert.
    - Created_by: Account to create IR Flow
    - Name: Name of IR Flow
    - Notation: IRFlow's note
    - State: State of IR Flow
  - <operator> are the following values:

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

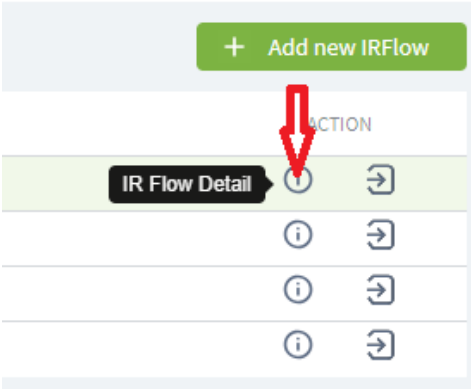
- =: Find an exact value as the value
- !=: Find a value other than the value
- ~: Find a value including the value
- AND/OR: Combination operator to combine 2 queries.

- Step 2: Select the search period by clicking the Date & Time button and select an arbitrary time period. If not selected, the default is Last 7 days.
- Step 3: Click on Search.

In addition, search by history is also supported.



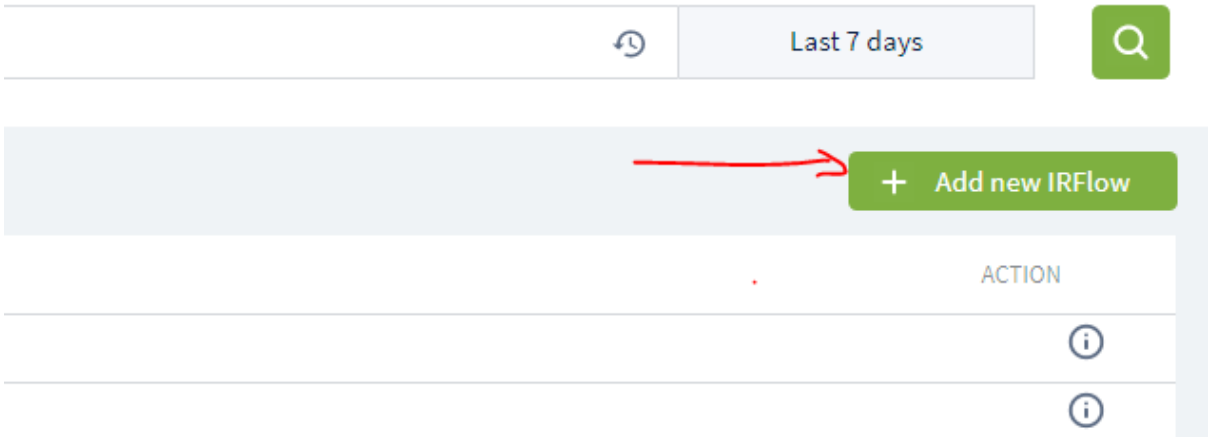
To view detailed information of 1 IR Flow and perform investigation and process, select IR Flow Detail.



5.1.3. How to Create a IR Flow?

- Step 1: Click Add new IR Flow.

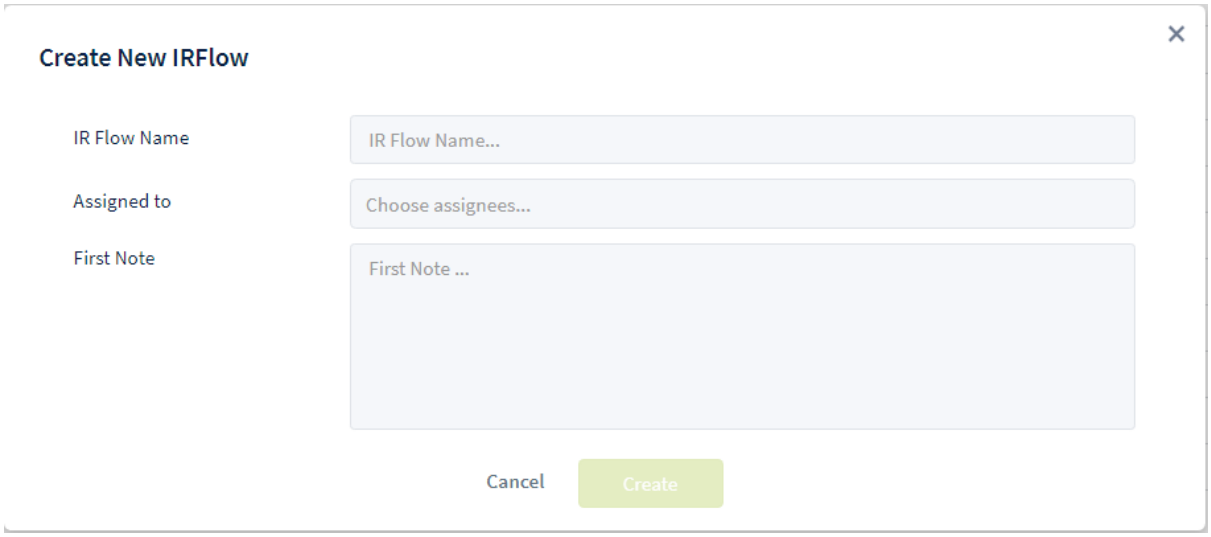
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Step 2: Enter valid information.

The data displayed in the Assigned to combo box include as follows:

- User login under root group: Display all user names in the system.
- User login under default group: Display the username of the user logging in.
- User login under parent-level group: Display all usernames belonging to the child-level group of the user logging in and the user logging in.
- User login under a group of one or more child-level groups: Display the username of the user logging in.



- Step 3: Click the Create button → the newly created IR Flow is displayed on the IR Flow Screen

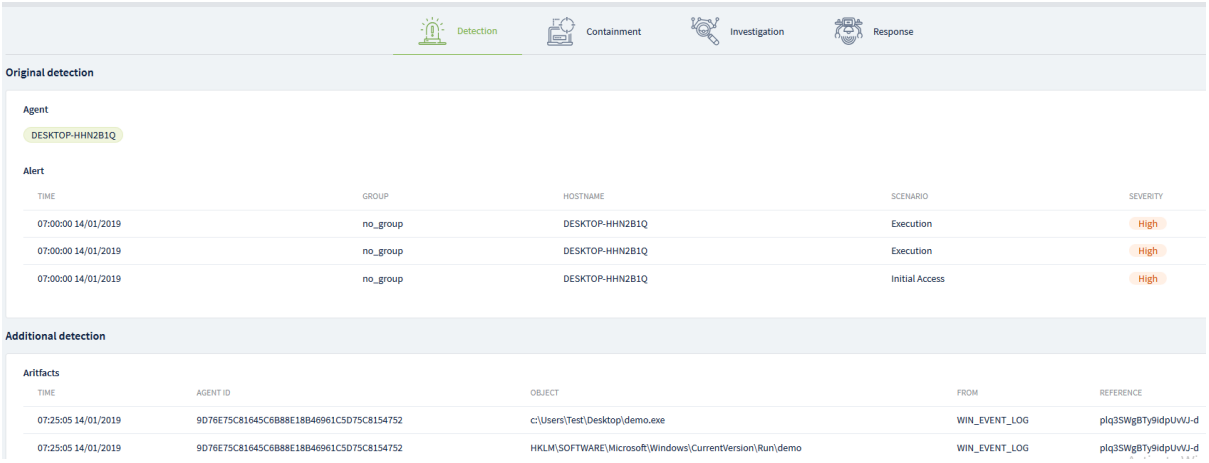
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

5.1.4. Steps to Perform in IR Flow

- After creating IR Flow from alerts or pushing alerts into IR Flow, operator will go to IR Flow page to perform following actions:
  - View information to investigate: Alert list, computer with alert, related objects (file/registry/process).
  - Isolate alert generating computers: Isolate the network and process.
  - Investigate and detect alert-related objects (artifacts).
  - Response: Process the investigated results. For example, kill the malicious processes, delete malicious files, delete registry entries generated by malwares, etc.
  - Investigation close: Close IR Flow, stop isolating machine and close Process Analysis and Live Response sessions.

5.1.5. IRFLow - Detection

- Detection tab displays alert-related objects, such as:
  - Computer list with alert.
  - Alert list.
  - List of artifacts discovered during investigation.



- Objects in the Original Detection section: Be as initial alerts (Alert) and computers (Agent) when IR Flow is created.
- As for the objects in the Additional Detection section: As the alerts, computers, artifacts added at the investigation step (Investigation).
- Meaning of some fields on the Detection 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

- Time: Time to add agent/artifact to the Detection screen.
- Object: File/registry path of artifact.
- From: Source of generating artifact (Event log or Process Analysis).
- Reference: ID of event log or ID of Process Analysis connection session.

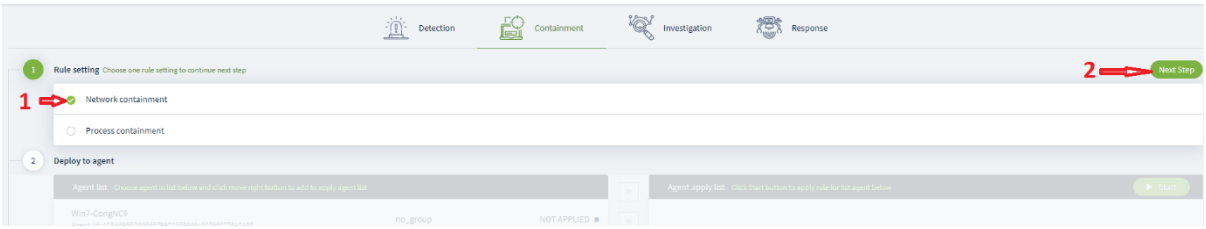
5.1.6. IRFlow - Containment

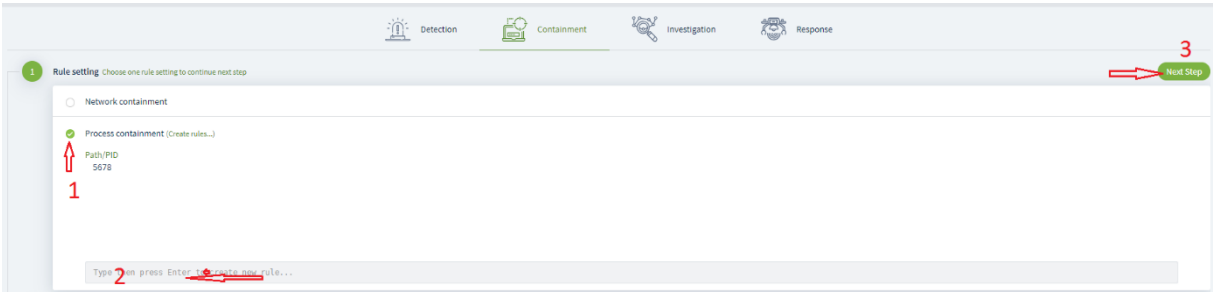
Containment tab allows isolating 1 or more computers in the Detection or Suspend tab the process in the alert located in IR Flow.

Containment state includes as follows:

- NOT APPLIED: The command to agent is not sent.
- APPLYING: The command to agent is being sent.
- APPLIED: The isolation command is sent successfully.
- STOPPING: The isolation stop command is being sent.
- STOPPED: The stop isolation command is sent successfully.

- Step 1: Select the investigation method: Isolate the network or suspend the process and then select Next Step.

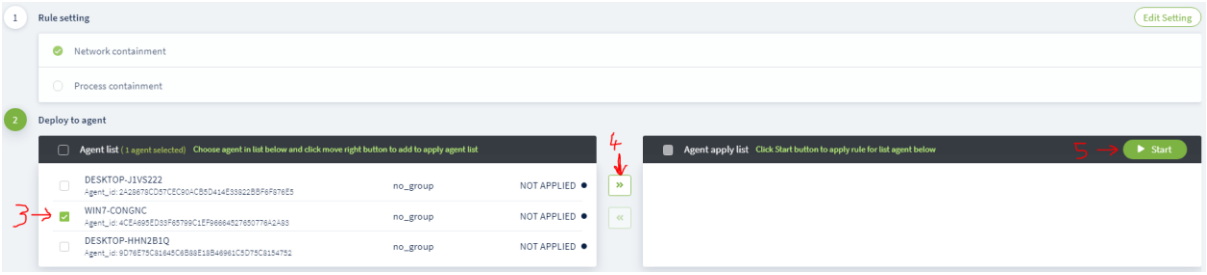




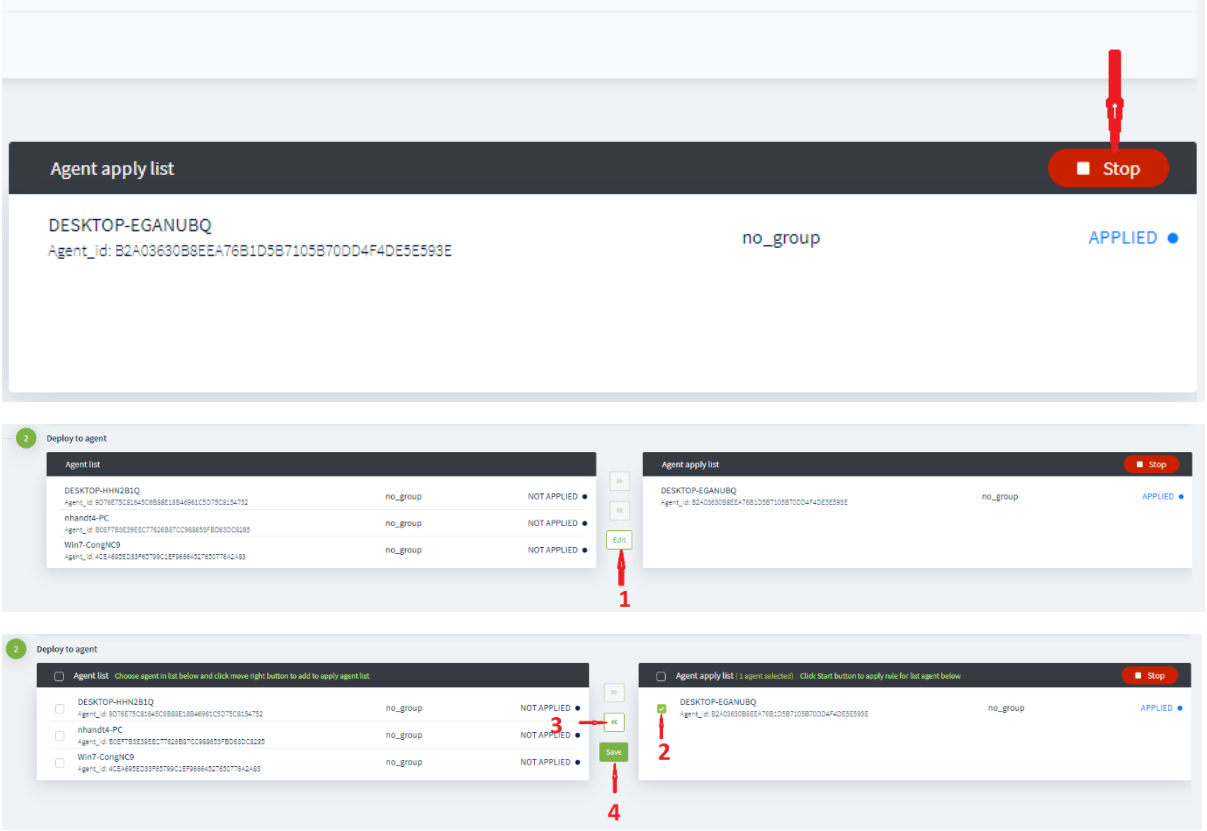
Notes: After entering Path/PID, the Enter button must be pressed to save the configuration. The multiple processes can be suspended at the same time.

- Step 2: Select the list of Agents to isolate and select Start to start isolating.

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: To stop isolating, click Stop or select agent in the Agent apply list button and switch back to Agent List.



In case the administrator does not actively stop the isolation on the Portal, after the default time (24h), the Agent will also automatically remove the isolation under the Agent.

5.1.7. IRFLow - Investigation

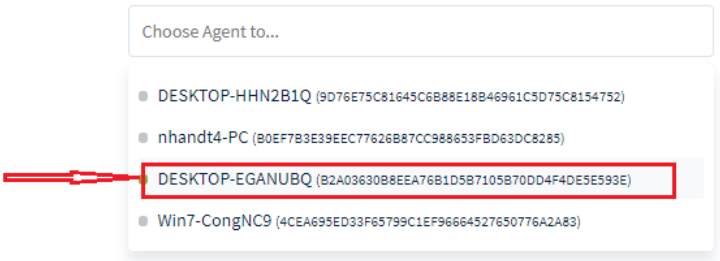
5.1.7.1. Process Analysis

5.1.7.1.1. View Process Information

This is the process of analyzing the processes on the user's machine in the Detection tab in real time to look for anomalies.

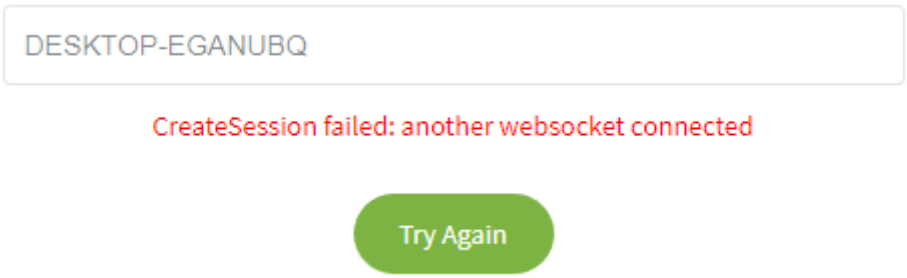
Step 1: Select the agent to connect, then click Start. Agent List is Agents in IR Flow.

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

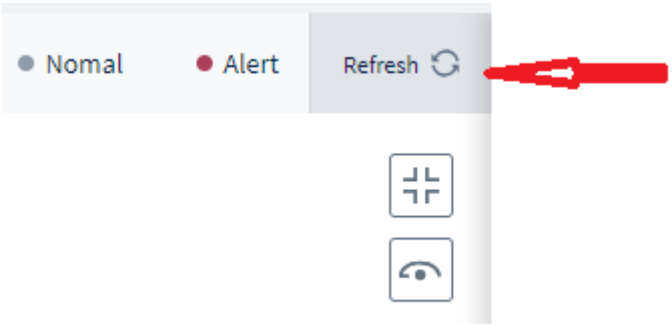


Notes:

- Timeout to create a connection is 60s. After 60 seconds, if the Agent cannot be connected, it needs to be reconnected.
- At a time in 1 IR Flow, only 1 connection to the Agent can be created. In case there is another account connecting to the Agent in the same IR Flow, an error notification will be displayed.

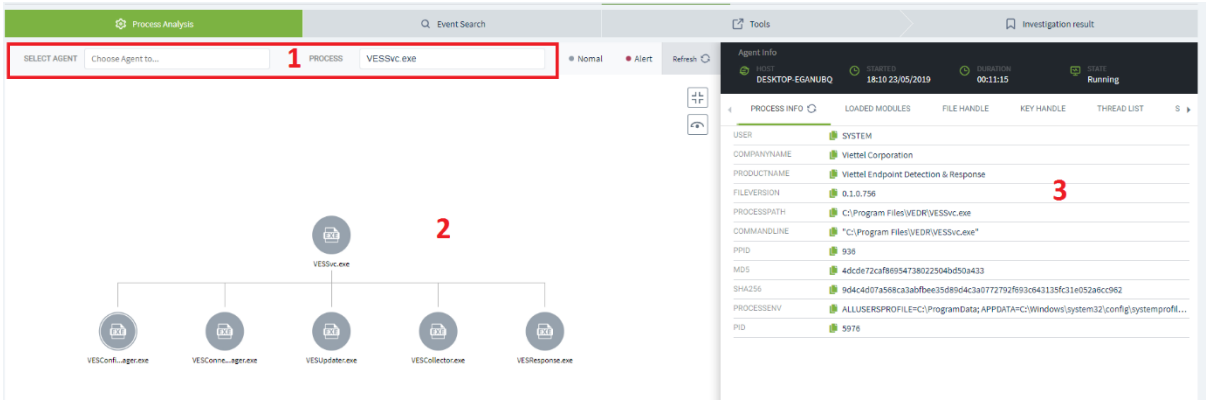


- Step 2: Click Refresh to get the latest process list under Agent.



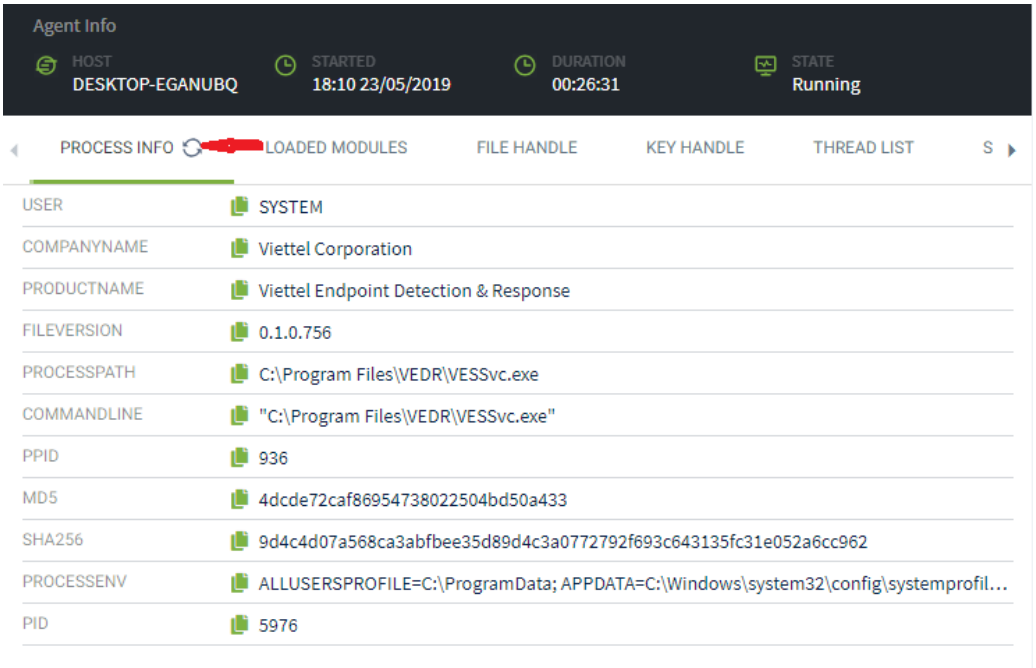
- Step 3: Select the process in the process list to view detailed information

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



- Area 1: Select agent and process.
- Area 2: Display process tree information. The default displays 1 parent level and 1 child level. Allow expanding/collapsing the levels when clicking on a process in the tree. Processes that is focused in the tree will display an icon different from the process that is not focused.
- Area 3: Display focused process information in the tree, including information on tabs: Process info, Modules (loaded dll), File handles, Key handles, Thread List, Section handles and Network Connection.

- Step 4: To get the latest information of the process, click the Refresh icon on each tab.



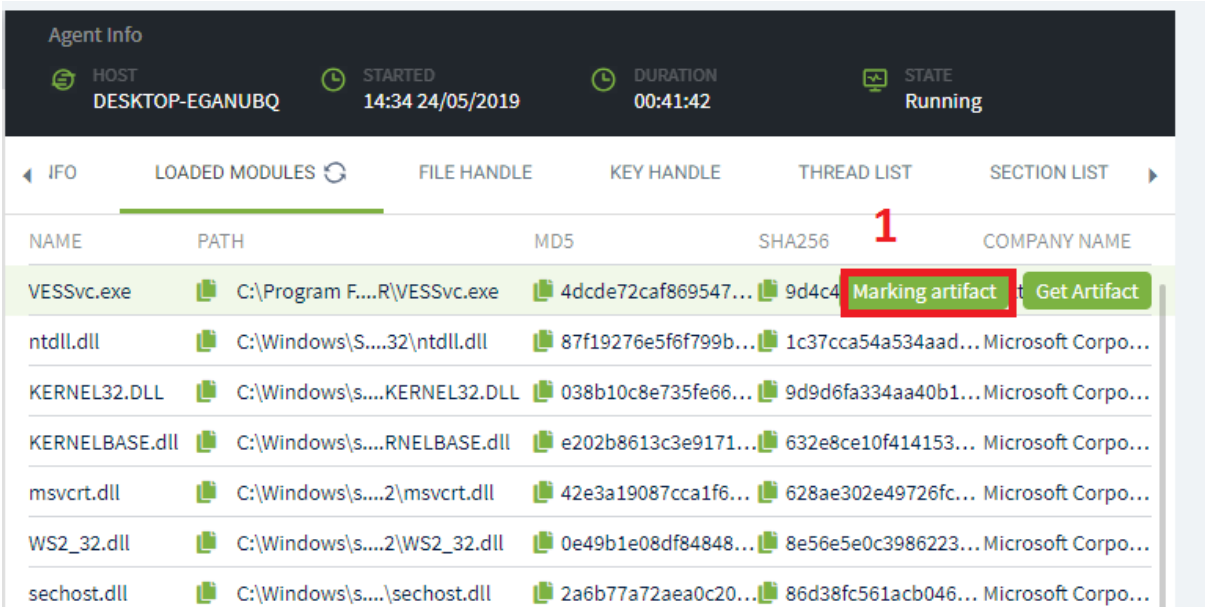
Notes:

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 switching sub-tabs in Investigation, such as Event Search, Tools and Investigation Result, the connection session with Agent is kept and no need to reconnect.
- When switching to other tabs, such as Detection, Containment, Response, Alert, Setting, etc. or F5, Logout, etc., the connection session with Agent needs to be reconnected.
- The Process Analysis connection session in IR Flow only closes when the administrator closes IR Flow. That is, if the IR Flow is not closed, every time when entering IR Flow and connecting to the Agent, the ID of the connection session does not change.

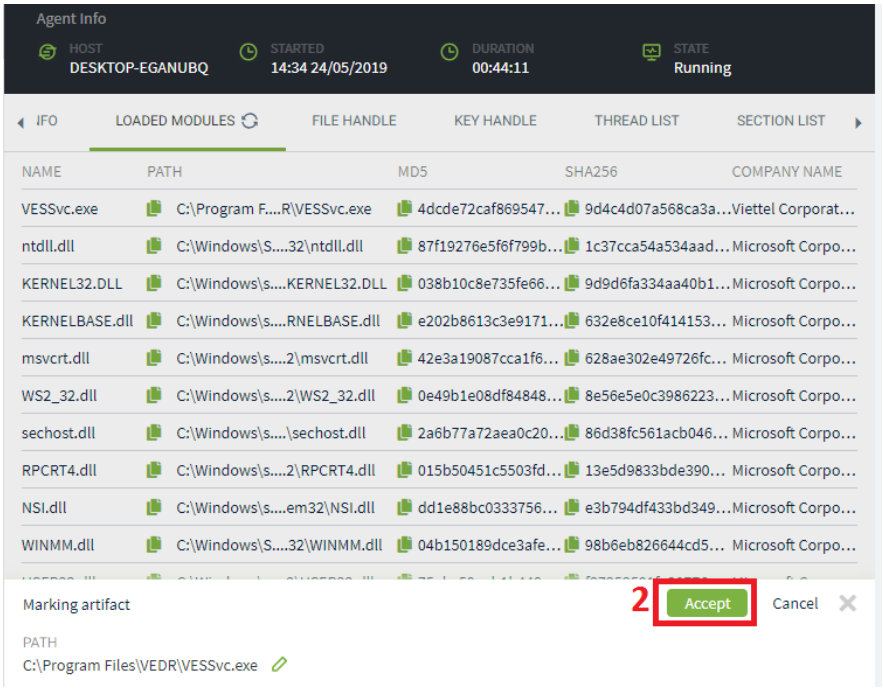
5.1.7.1.2. Marking/Get Artifact

- Marking artifact function allows marking the artifact to be tracked. The following data can be marked:
  - Process Info: Process Path
  - Loaded module: Path
  - File Handle: Path
  - Key Handle: Key path and Value
- Step 1: Select any record and hover over that record. Click on the Marking artifact button.

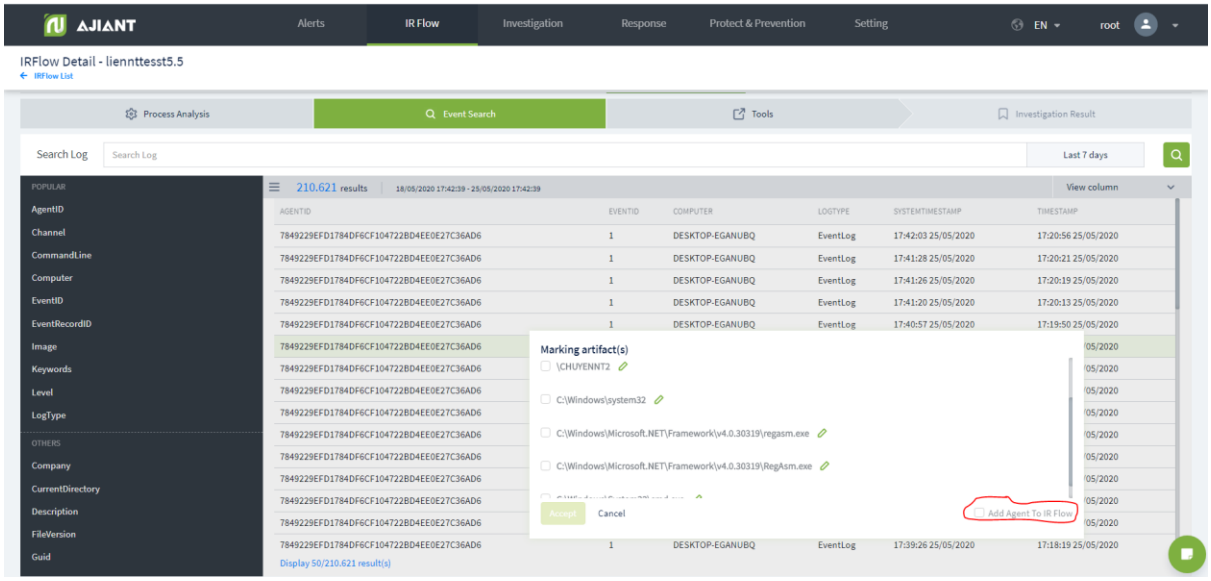


- Step 2: Click the Accept button, enable to edit the file path when clicking on the Edit icon.

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

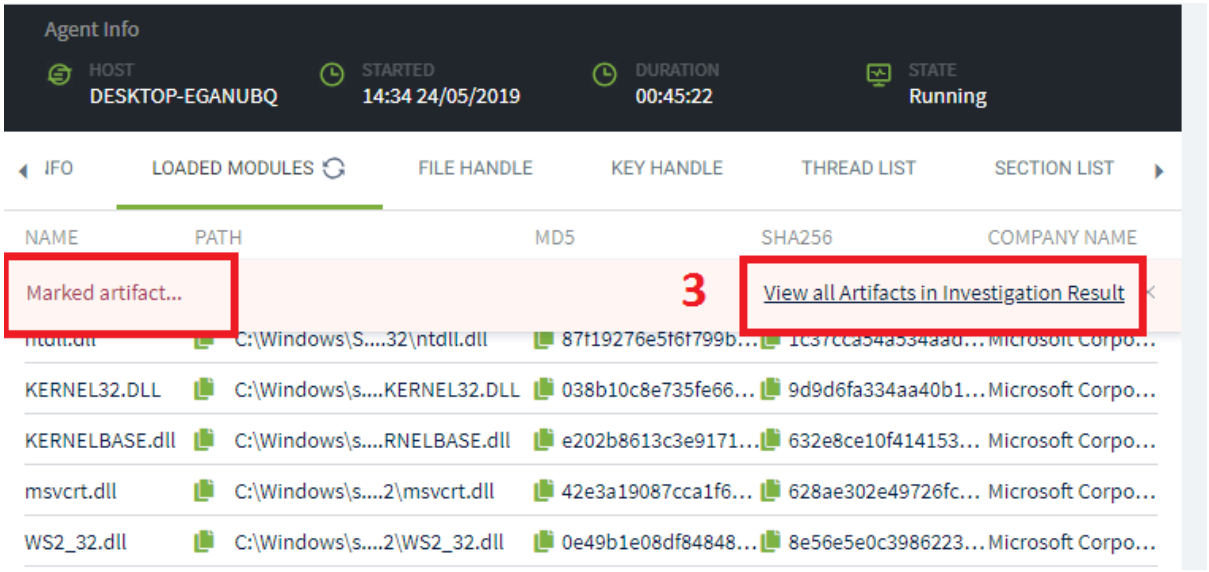


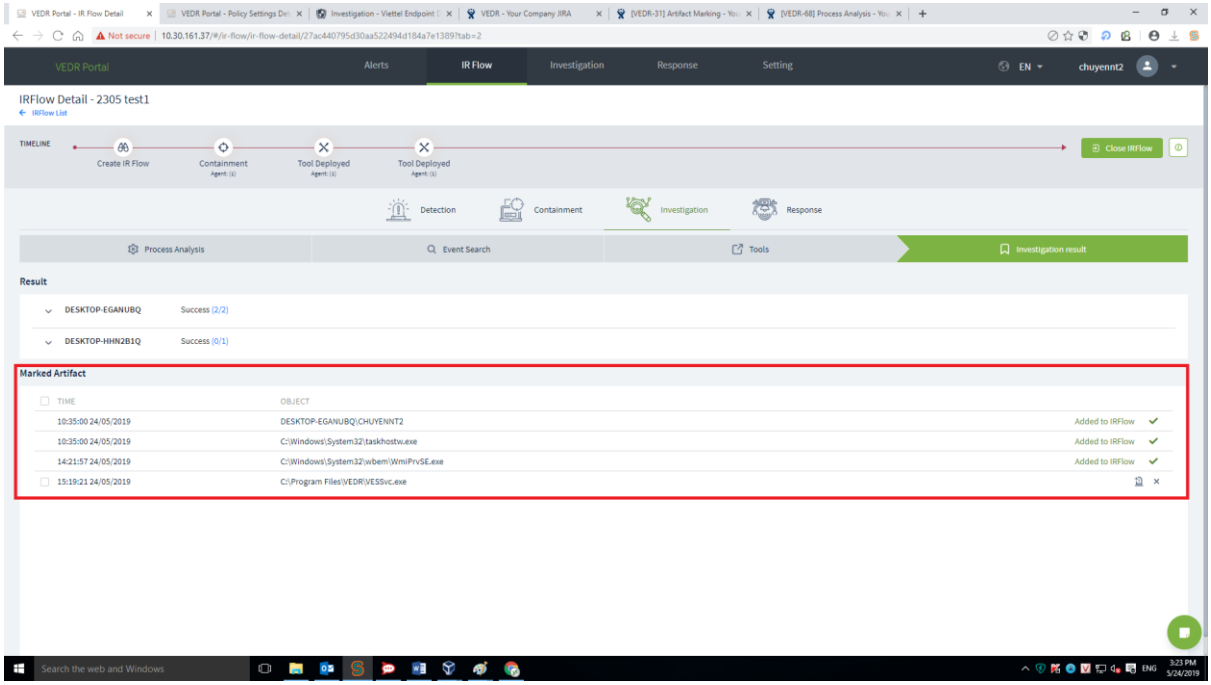
In case of selecting a record with an Agent that does not exist in Detection, there will be an Add Agent to IR Flow check box. When performing Accept, the corresponding Agent will be added to Detection.



- After marked successfully, the notification is displayed. Click the View all artifacts in Investigation Result button to go to the Investigation Result screen. Artifact marked will be displayed on this screen.

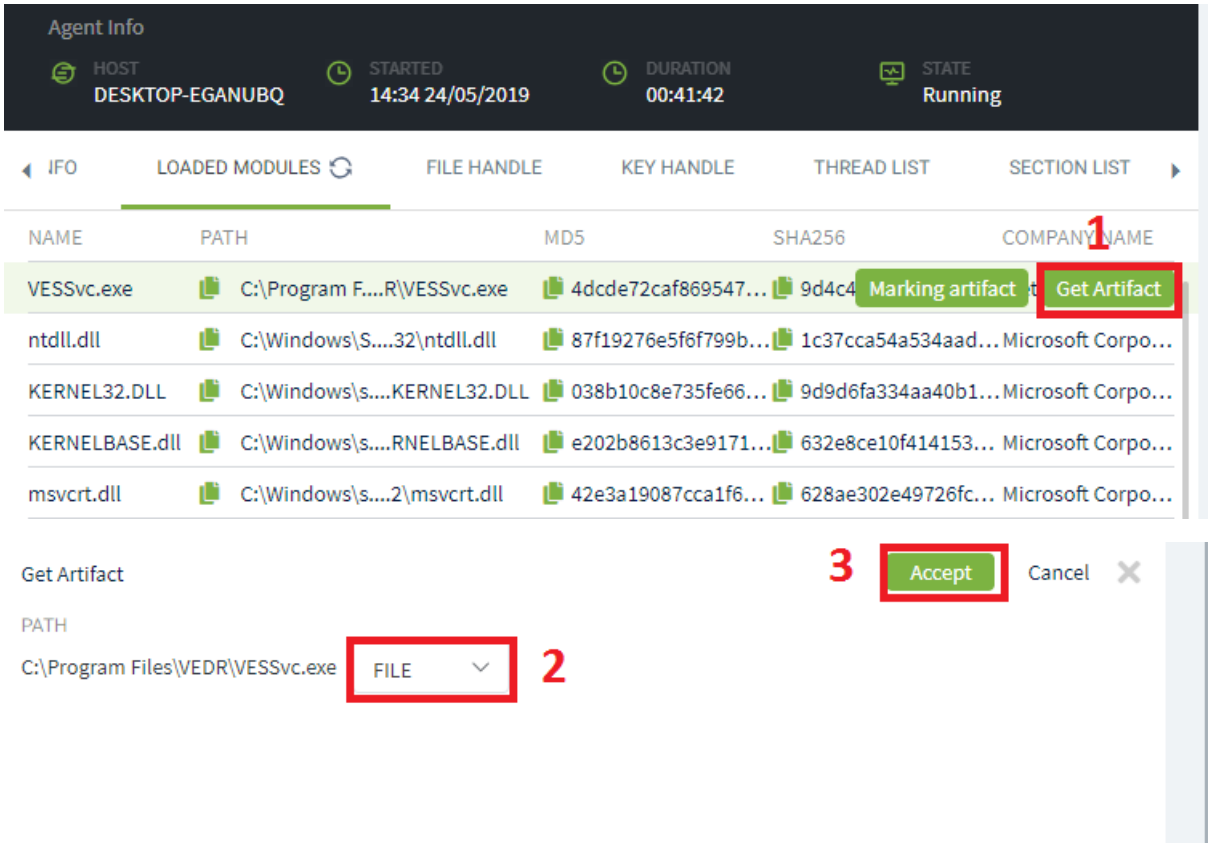
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com





- Get Artifact function allows getting file/registry information under Agent for investigation.
- Select a record and hover over that record. Click Get artifact button → Select artifact type (File/Registry) → Click Accept. Then check the result of performing Get artifact on the Investigation Result 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

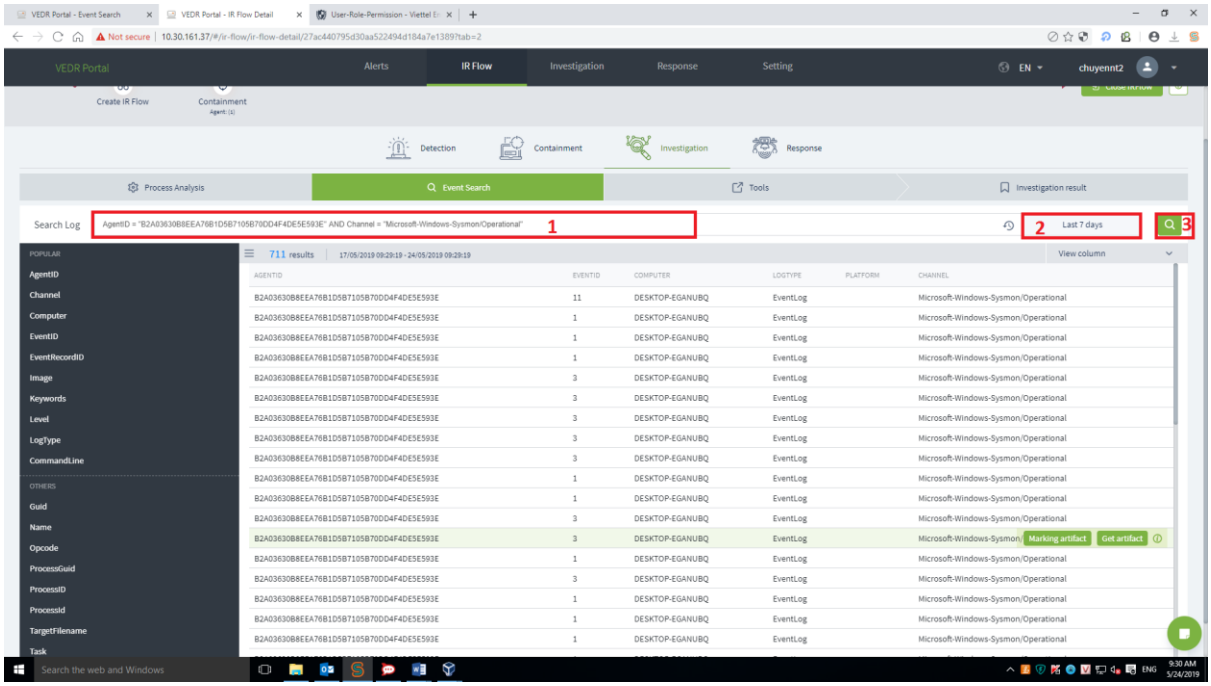


5.1.7.2. Event Search

This is the process of finding objects based on event logs. Unlike other tabs in IR Flow that only display information about Agents added to IR Flow, this tab displays all events of all Agents in the system.

5.1.7.2.1. Event Search

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 1: Enter query into the Search textbox with the following format:

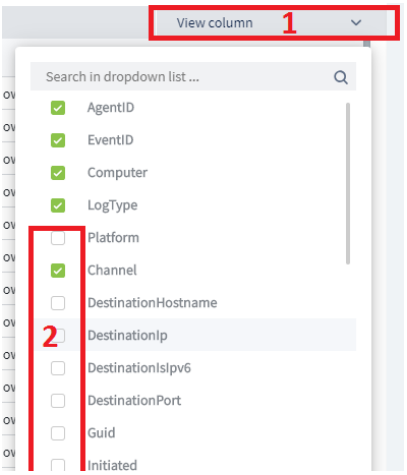
<field_name> <operator> “<value>” AND/OR <field_name> <operator> “<value>”

In which:

  - <field_name> are the following values:
    - AgentID: ID of the agent
    - EventID: ID of the event
    - Computer: Name of the computer
    - LogType: Type of log
    - Channel: Channel of the event.
  - <operator> are the following values:
    - =: Find an exact value as the value
    - !=: Find a value different from the value
    - ~: Find a value including the value
    - AND/OR: Combination operator to combine 2 queries.
- Step 2: Select the search range by clicking the Date & Time button and choosing an arbitrary time. If no time is selected, the system defaults to Last 7 days.
- Step 3: Click on Search.

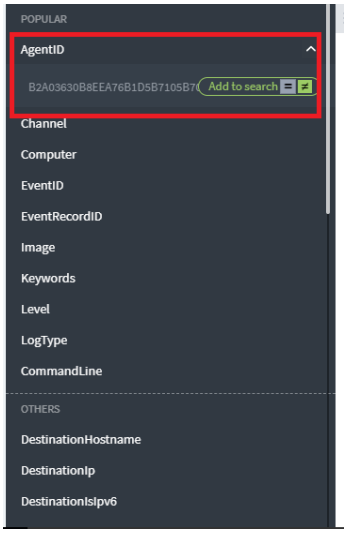
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- In case there are no matching results, the system will display the notification: No data.
- In case there is a match, the system will default to 50 records in descending order of time with 5 default display columns, including: AgentID, EventID, Computer, LogType, Channel.
- To add a display column, click on View Column and tick to select the necessary fields.



- In addition, users can search for fields in the Popular and Others section by showing the values of the fields and hovering over the value in Popular/Others, that record will display 2 icons: “=” and “!=".
  - If the user selects "=", the Search textbox will display the query corresponding to the "=" operator.
  - If the user selects "!=", the Search textbox will display the query corresponding to the "!=" operator.
  - If there is data in the Search textbox and the user chooses to add values in the Popular/Others section, the two sides of the query are connected by the AND operator.

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

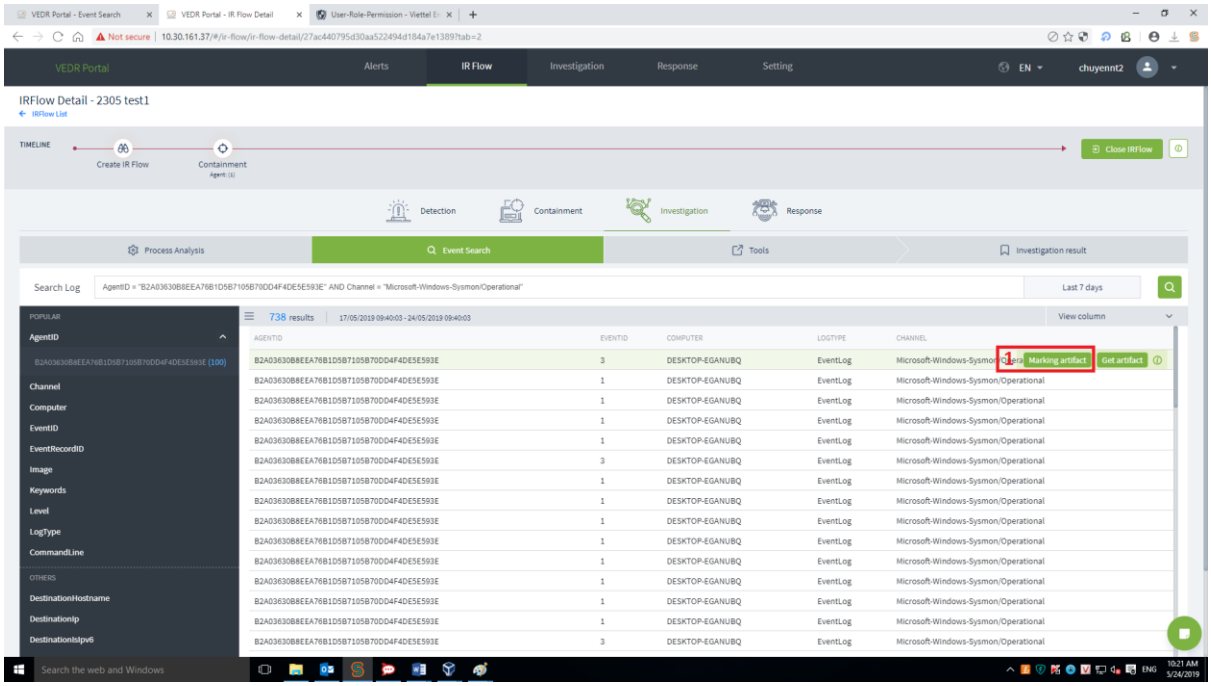


- In the Others section, all fields of the log are displayed.
- When performing show/hide 1 field, 5 fields with the highest number of records sorted from highest to lowest will be displayed.
- When the user loads more, each record of field will be updated according to the number of records displayed on the screen.
    - In the Popular section, 10 popular fields of the most searched log are displayed.
    - If there are >= 10 fields, the 10 fields with the highest number of searches will be displayed, if there are less than 10 fields, all those fields will be displayed.
- When performing show/hide 1 field, 5 fields with the highest number of records sorted from highest to lowest will be displayed.
- When the user loads more, each record of field will be updated according to the number of records displayed on the screen.
- When double-clicking on a record, the detailed information of that record will be displayed.
    - The detailed information tab is displayed as a Table type, the data is displayed in the form of a table
    - When selecting the JSON tab, the data is displayed as .JSON format.

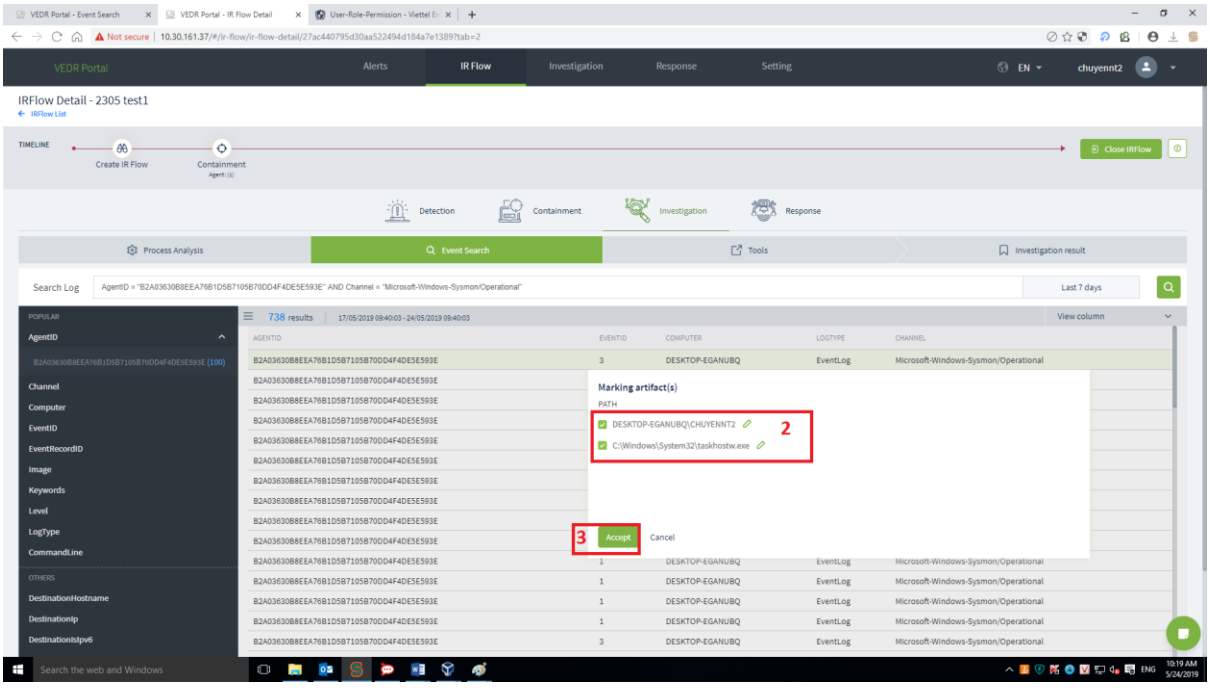
5.1.7.2.2. Event Handle

Marking artifact: The artifact is marked.

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 1: Select any record and hover over that record. Click on the Marking artifact button. A popup will appear on the screen as follows:

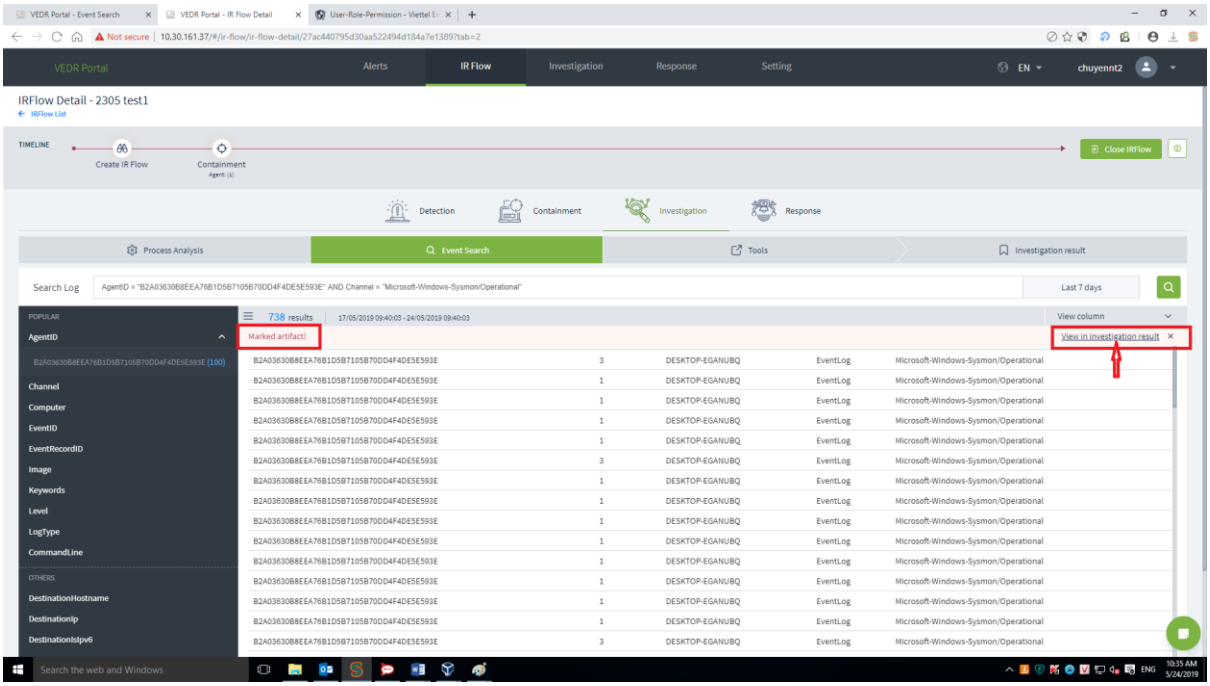


In case of selecting the event of the Agent that is not part of IR Flow, there will be an option for the user to add the Agent to IR Flow. Agent will be added to the Detection screen of the active IR Flow.

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: Choose a suitable path for marking artifact. Then click Accept to perform marking. If Cancel is selected, the marking artifact will be delayed.

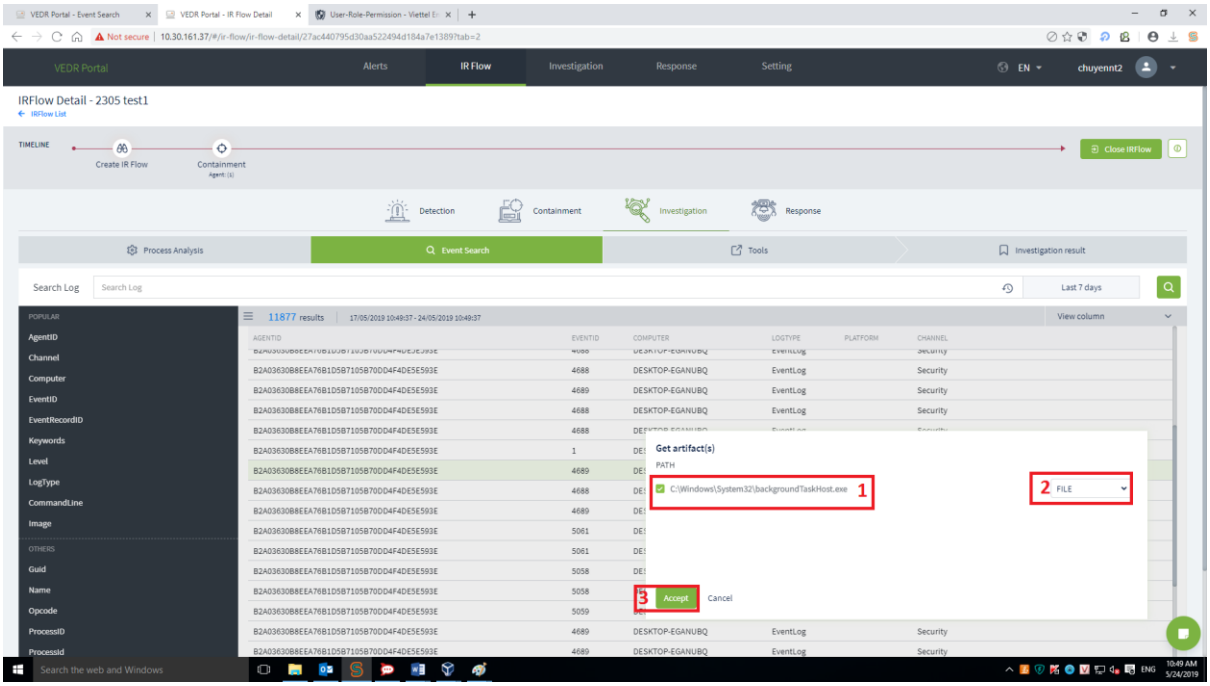
When the marking artifact is successful, the screen will display a notification. Click on View in investigation result to go to the Investigation Result screen and the marked event will be moved to this tab.



Get artifact: Perform get file/registry under Agent to server to serve the investigation process.

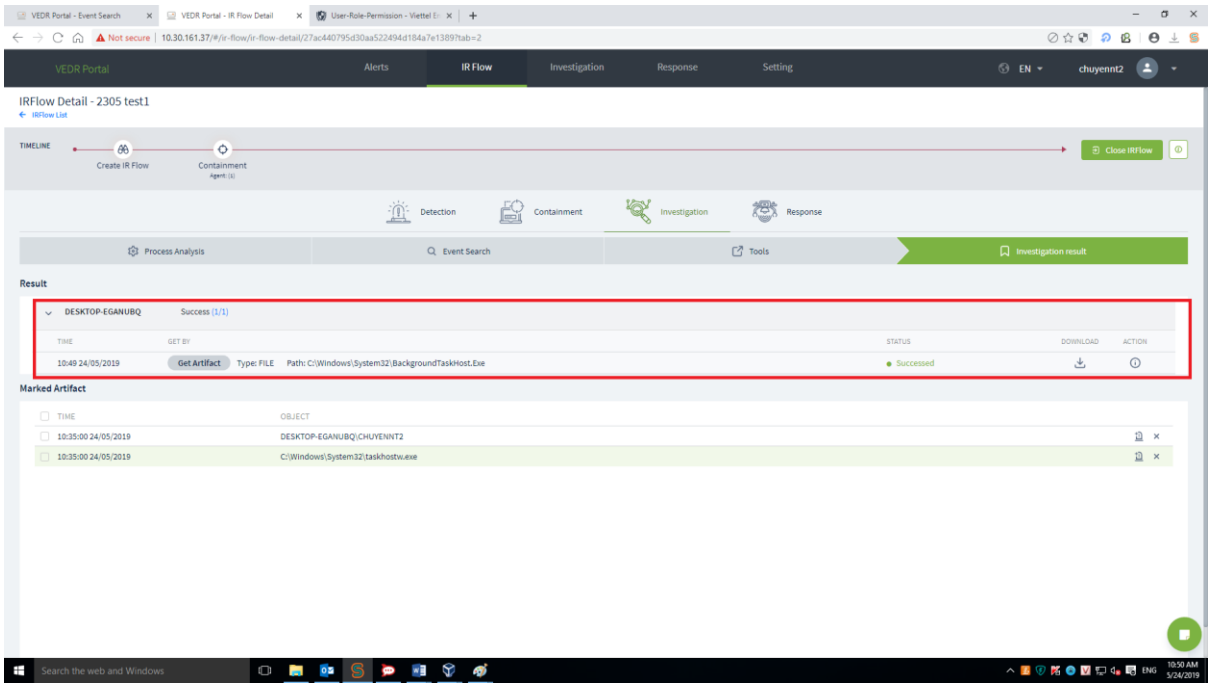
- Step 1: Select any record and hover over that record. Click on the Get artifact button, a popup will be appeared on the screen as follows:

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



- Step 2: Select artifact, then select artifact type (File/Registry) and click Accept.

When the marking artifact is successful, the screen will display a notification. Click on View in investigation result to go to the Investigation Result screen. The result of Get artifact will be displayed on this tab.



View event details: Select any record and hover on that record, click on the View details icon.

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

5.1.7.2.3. Deploy Tools

This is the process of pushing the tool down to the Agent to get information for investigation. Information about some tools available on the system as follows:

For a Windows agent:

- Listdlls: Get information about processes and dlls being loaded.
- Autorunsc: Get information about processes and services that start with the system.

For a Linux agent:

- ListService: Get the list of services under the agent machine.

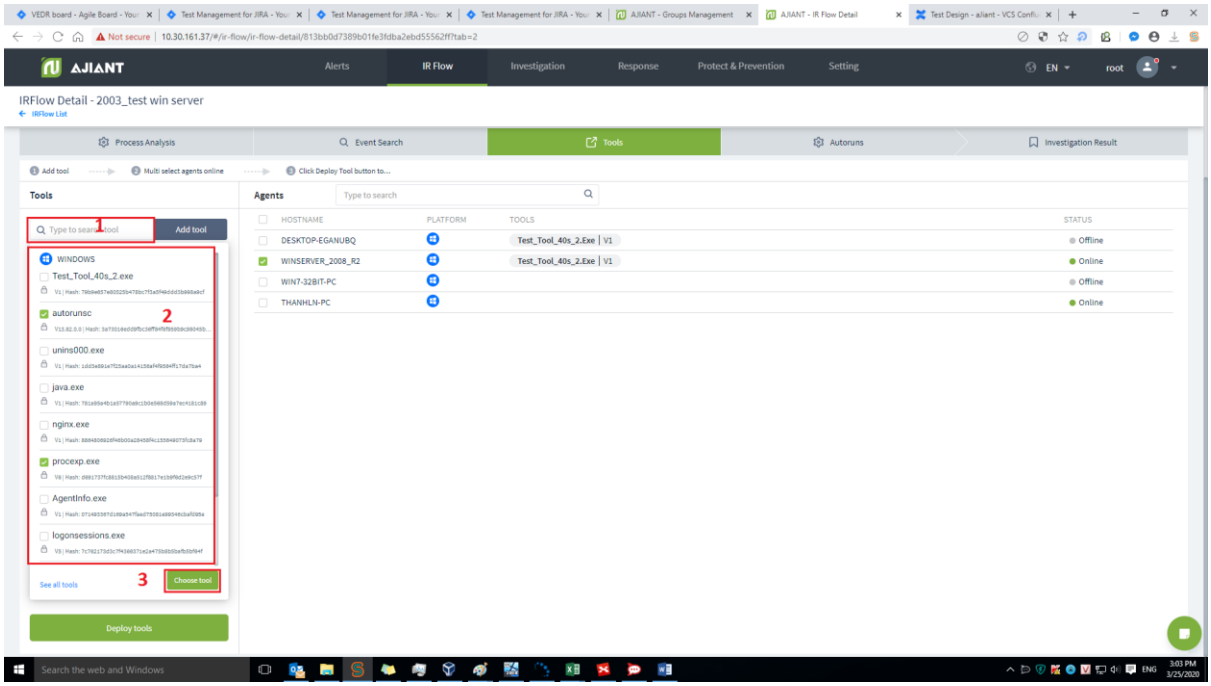
The flow that implements this function is as follows:

Make tool selection → Select agent → Click Deploy tools.

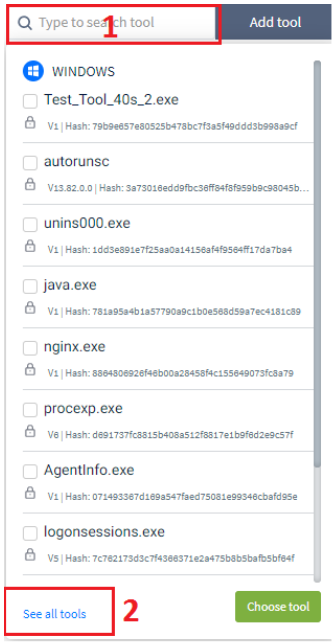
To choose the appropriate tool, there are two ways:

  - Method 1: Click on the Search tool textbox → Click the tool to deploy → Click Choose tool.

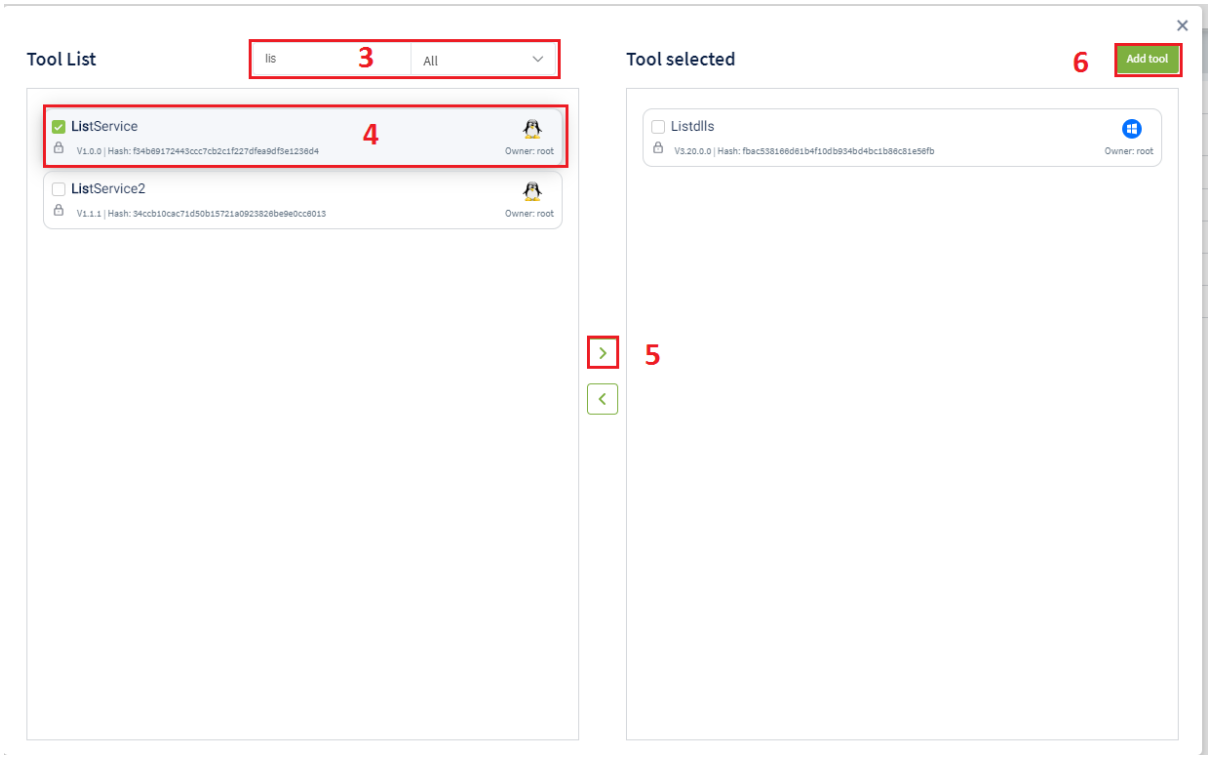
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



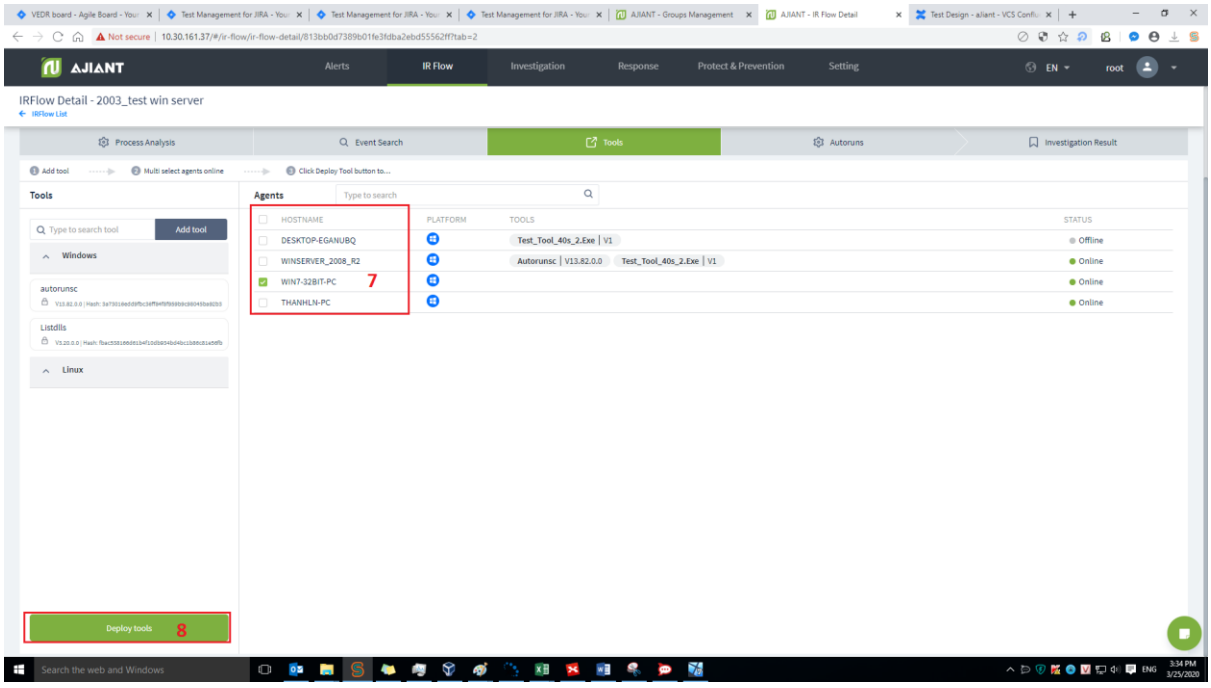
- Method 2: Click on the Search tool textbox → Click See all tools → Display the full tool list screen → Search and select the tool to deploy → Click Add tool.



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

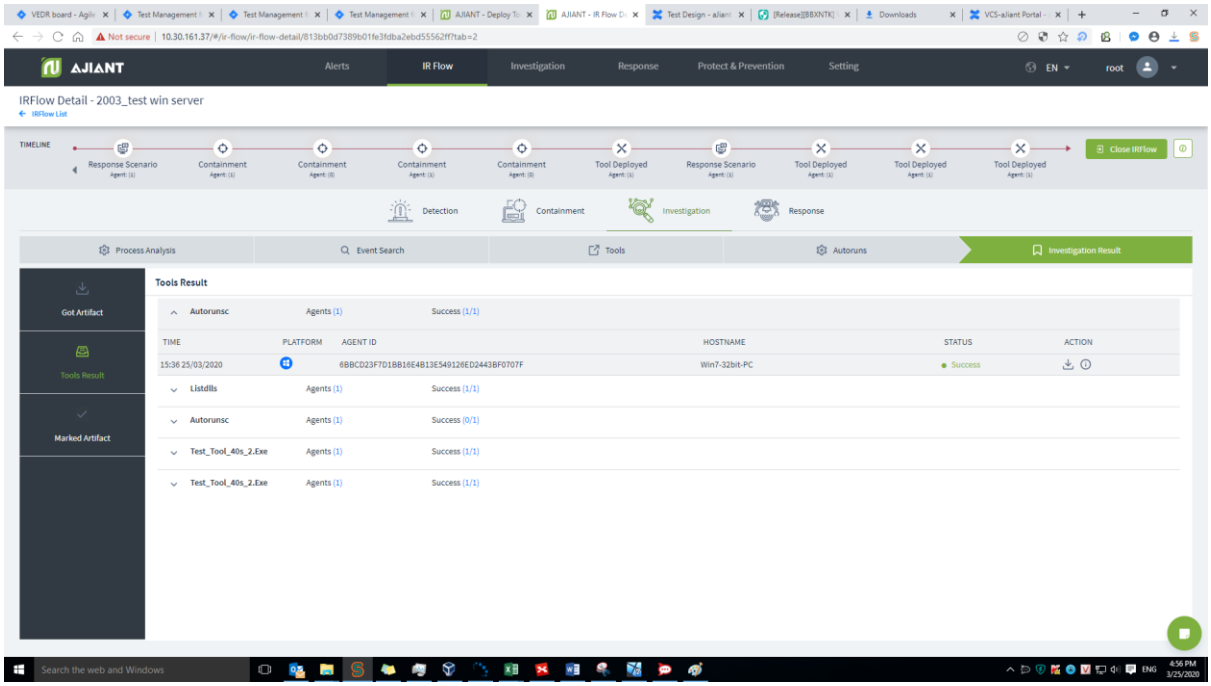


- After searching for tools, select an agent and click Deploy tools.



- After deploying the tool, view the results in the Investigation Result and Tools Result 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



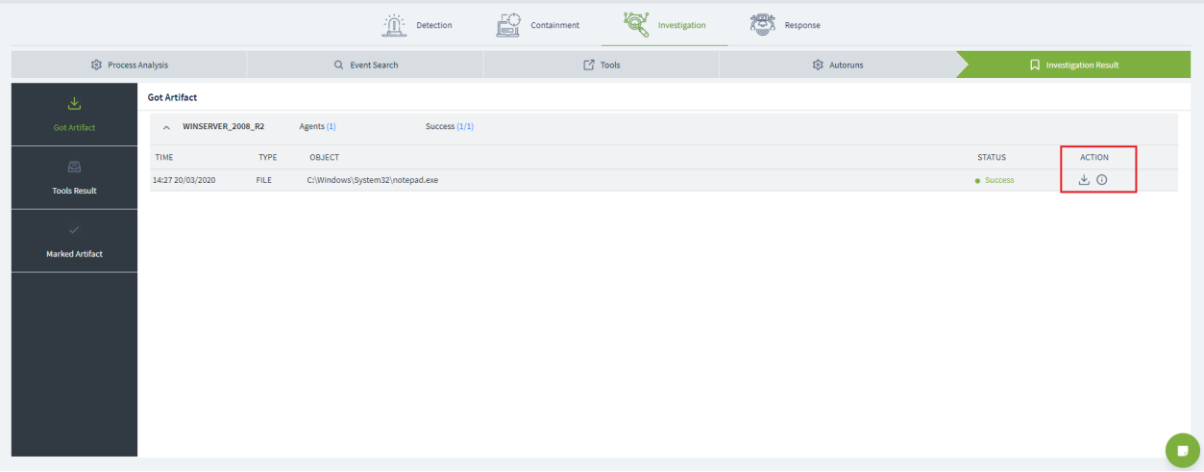
5.1.7.2.4. Handle Event

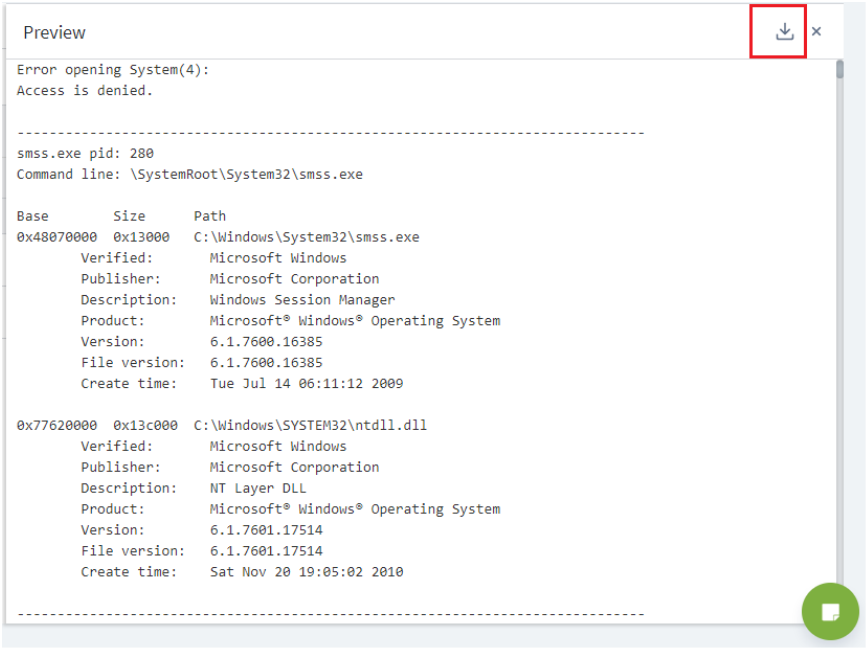
This is the screen displaying information about Deploy tool, Marking/Get Artifact results in 3 tabs: Process Analysis, Event search and Tools.

- Got Artifact: The result of executing the Get Artifact command.
- Tool Results: The results of executing the Deploy tools command.
- Marked Artifact: The artifacts are marked.

- In the Got Artifact and Tool Results tabs, the following actions can be performed:
  - View the detailed content of the taken artifact or the result of running the tool under the agent. If the data is text, it can be viewed directly on the interface. If the data is an executable file (.exe), it needs to be downloaded to the local machine to check.
  - Download the artifact or tool run results. There are 2 ways to download: Click the Download icon on the interface or click the View details icon → Click the Download icon on this screen.

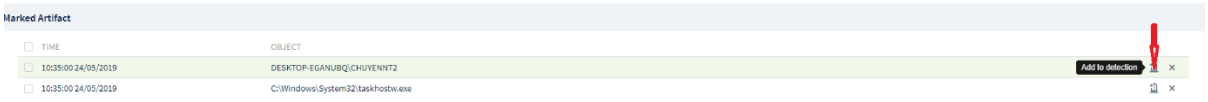
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com





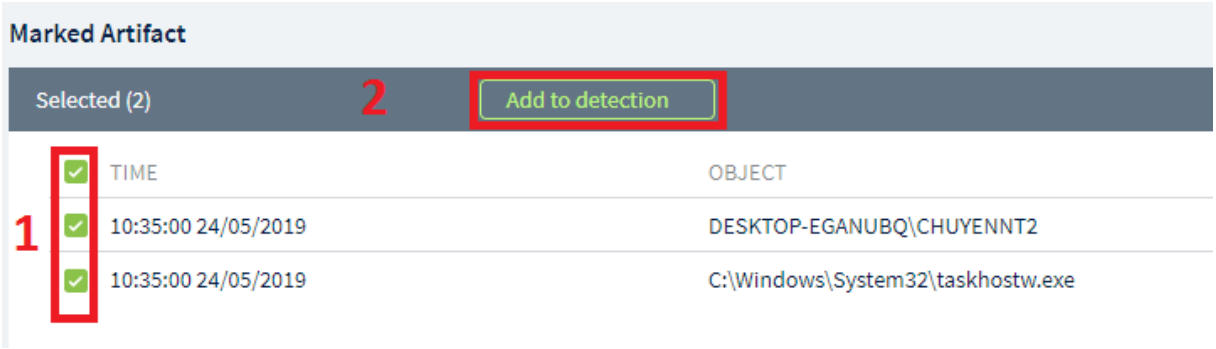
- In the Marked artifact tab, select the artifact to add to the Detection screen as follows:

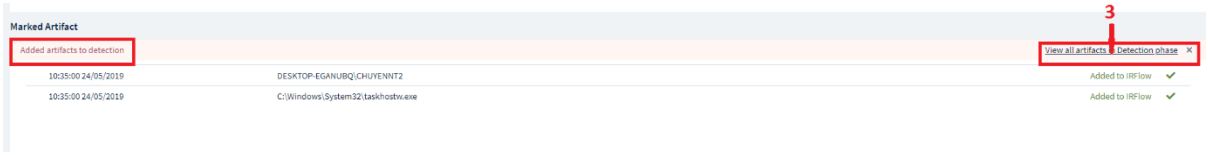
Select an artifact and click Add to detection:



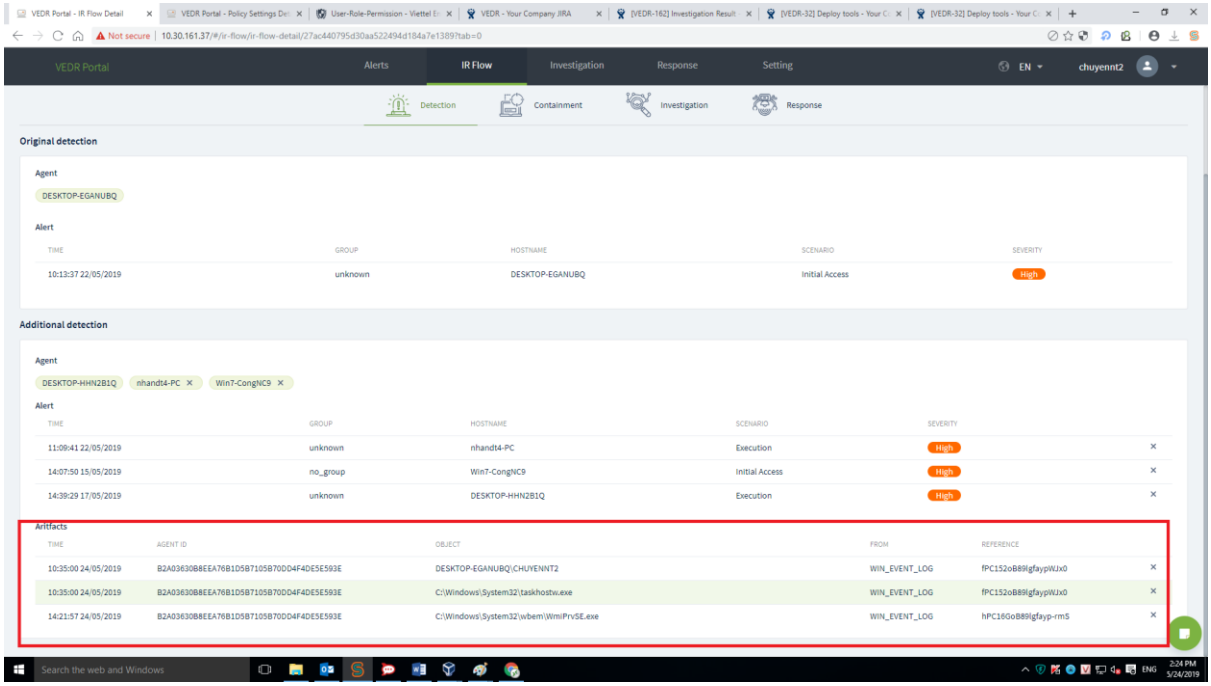
Select multiple artifacts and click Add to detection:

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 adding successfully, a notification will be displayed, click on View all artifacts in Detection phase to go to Detection screen. The artifacts are added to Additional detection on the Detection screen.



5.1.8. IR Flow - Response

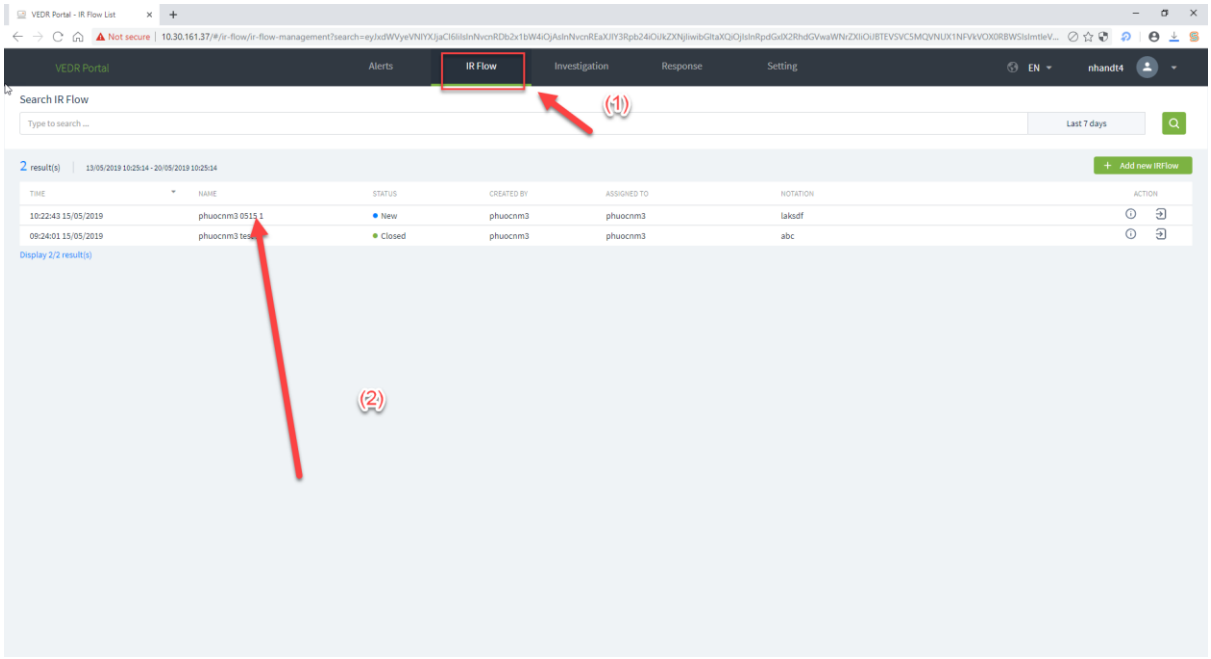
5.1.8.1. Live Response

The Live response function provides the ability to process a set of remote commands according to the working session to provide information or handle requests on the host.

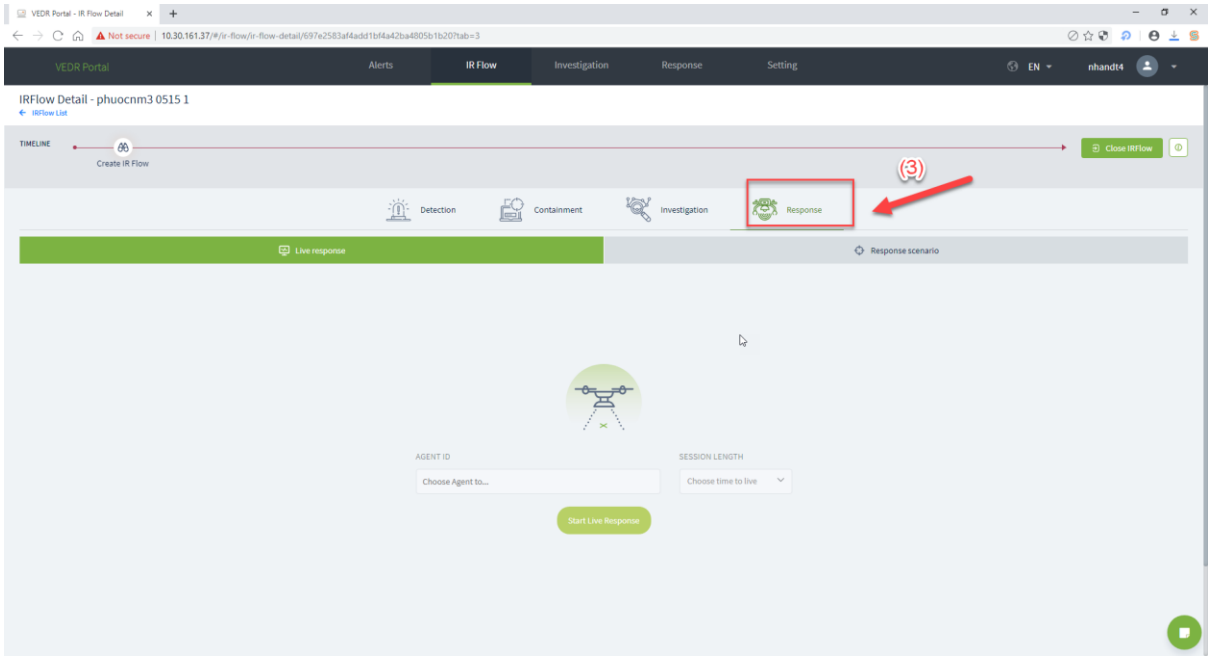
Steps to implement Live Response function in IR Flow as follows:

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

- Step 1: Click the IR Flow tab.
- Step 2: Click duplicate on a record in the list of records (Notes: Select the correct IR Flow record containing the Agent that needs to perform the Live Response.)



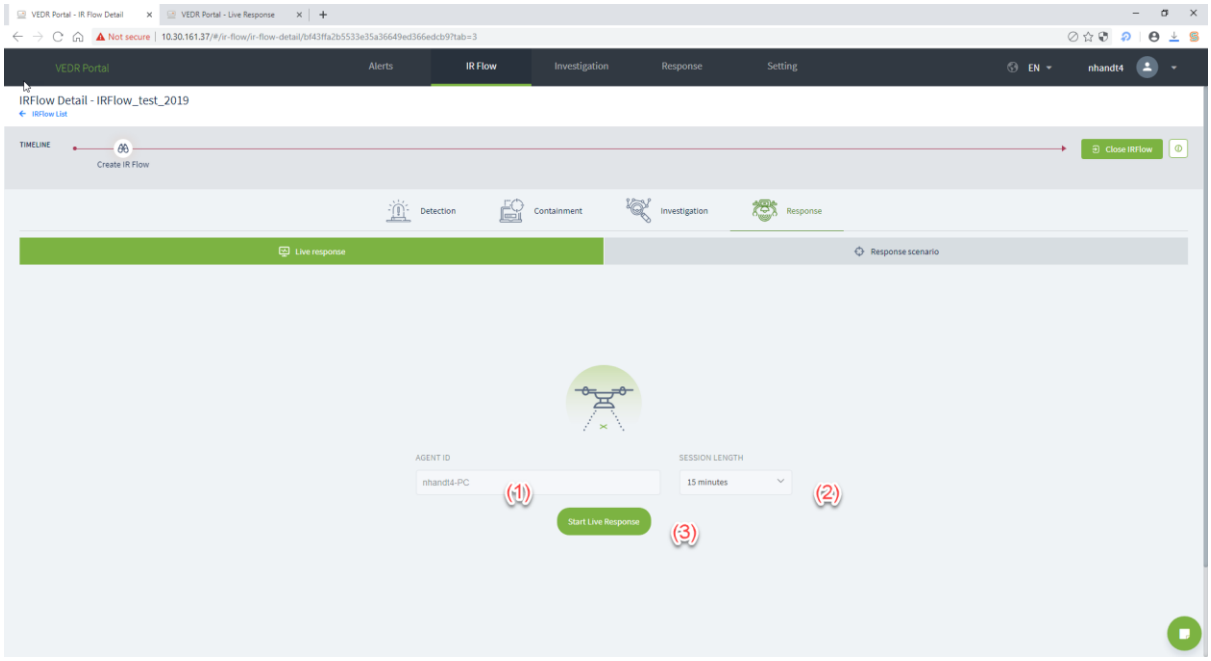
- Step 3: Click the Response sub-tap.



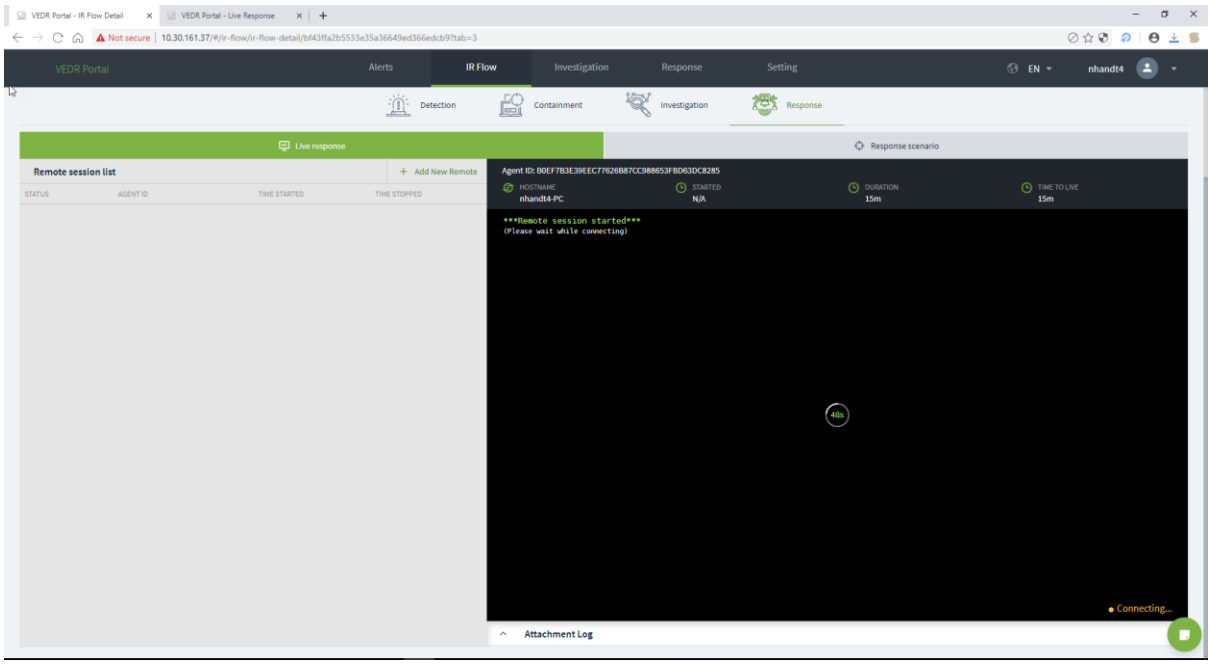
- Step 4: Select Agent and time range (5 minutes/ 15 minutes/ 1 hour/ 3 hours) to perform Live Response and press the Start Live Response button.

The list of Agents displayed in the combo box is all the agents displayed in the Detection 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



After that, the user needs to wait 1 minute for the system to connect to the agent. The system state is Connecting.

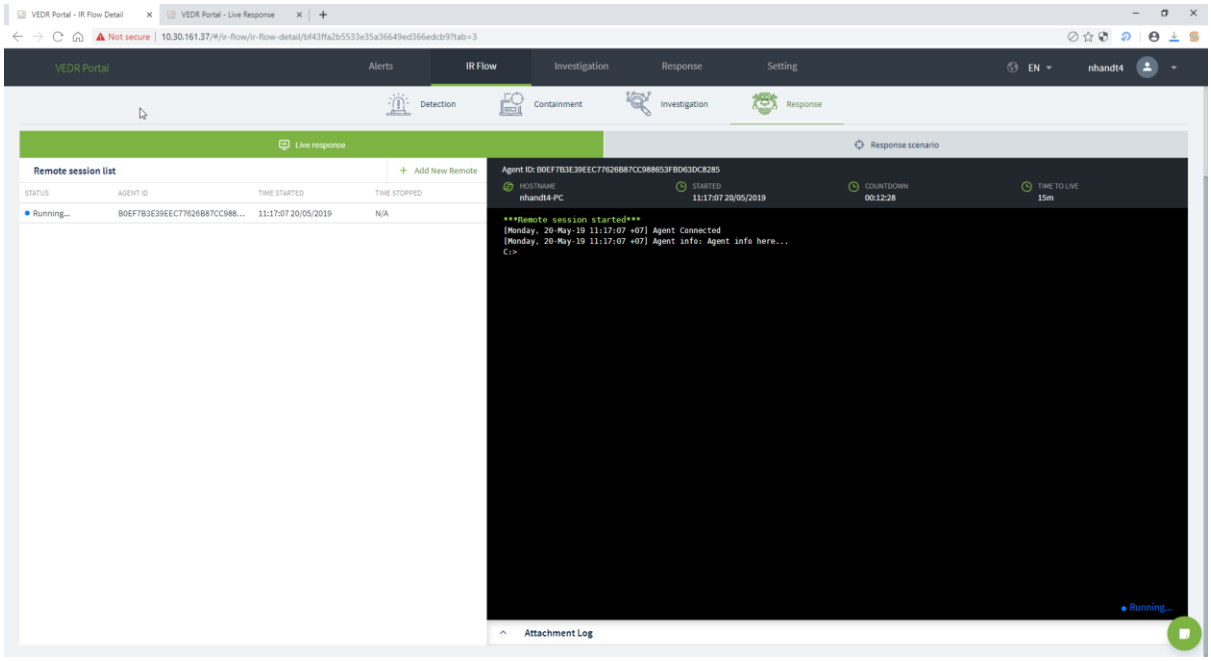


- Step 5: When the connection is successful, the system displays a record in the Remote Session List and the console screen has information about the connection and displays the Running state.

(Remote Session List: Display a list of IR Flow's Live response sessions that have been performed.)

Notes: Each agent at a time has only 1 working session of Live response.

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



Users can execute commands at the console screen as follows:

No.	Commands	Parameters	Description
1	cd	cd <dirpath>	Change current working folder
2		cd.. or cd ..	Switch back to parent-level folder
3	pwd		Print current working folder
4	dir		List files/sub-level folders in the current folder
5	delete	delete -file <path> For example: delete -file "c:\temp\run path.exe"	Delete 1 file
		delete -folder <folderpath> For example: delete -folder temp\axvers	Delete 1 folder

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 -all <folderpath> For example: delete -all c:\temp	Delete all files/sub-folders in the folder (but do not delete the folder)
6	viewfile	<filepath><sizeinbytes>	Display data in file (file size limit)
7	get	<filepath>	Upload 1 file from host to server
8	put	<url><folderpath>	Download 1 file to host machine
9	mkdir	<dir name>	Create 1 folder
10	reg		Commands related to Registry
		query <keyname> -v <valuename> For example: reg -query "HKLM\Software\abc xyz" -v "run path"	Query the value data of a key
		query <keyname> -s For example: reg -query "HKLM\Software\abc xyz" -s	Query all sub keys, values and data
		add <keyname> For example: reg -add "HKLM\software\abc xyz"	Add 1 key
		add <keyname> -v <valuename> -t <type> -d <data> For example: reg -add "HKLM\software\abc xyz" -v	Add 1 value

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

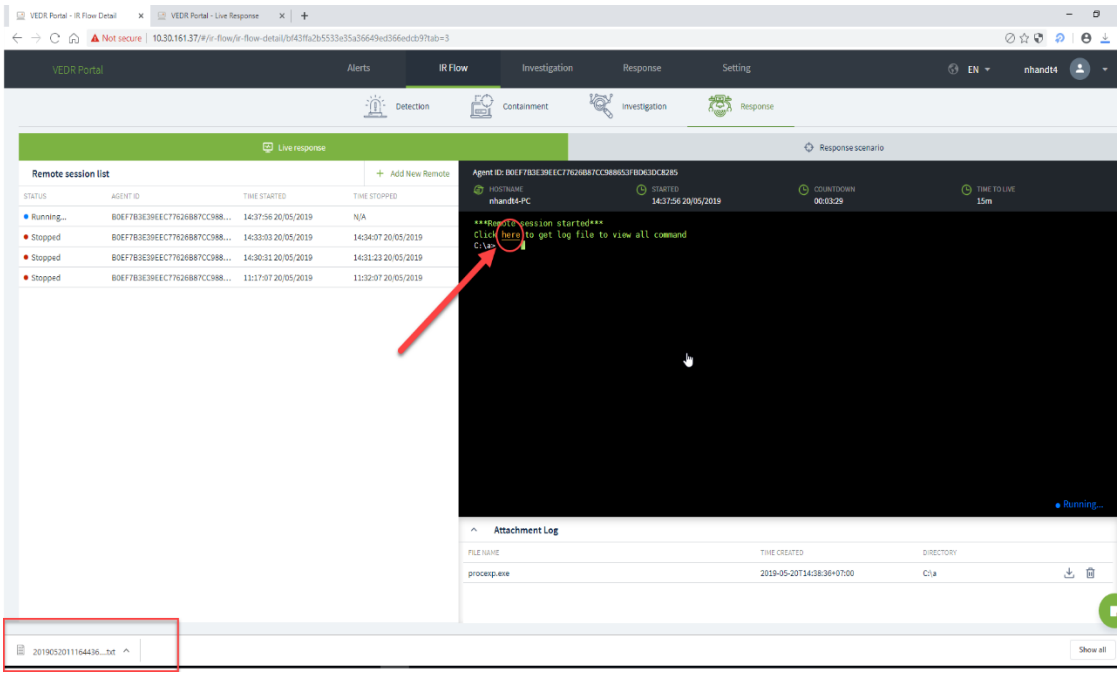
		"run path" -t REG_SZ -d "c:\temp\bin.exe"	
		delete <keyname> For example: reg -delete HKU\S-1-5-21-3791698801-2327923109-636705026-2080\Software\Test	Delete 1 key and all sub keys and value
		delete <keyname> -v <valuename>	Delete 1 key value
		import <filename>	Import 1 file .reg
		export <keyname> <filename>	Export 1 file .reg
11	process		Commands related to process
		-t <processid>	Turn off a running process by process ID
		-s <processid>	Pause a process
		-r <processid>	Recover a previously paused process
		-l -a	List all processes of all users
		-l -u <username>	List all processes of an user
12	service		Commands related to service
		-query	List the services running on the host machine
		-start <servicename>	Start 1 service
		-stop <servicename>	Stop 1 service

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

13	user	-list	List the users on the machine
		-sid<username>	Get sid of username
14	cls		Delete the console screen
15	help		Help command

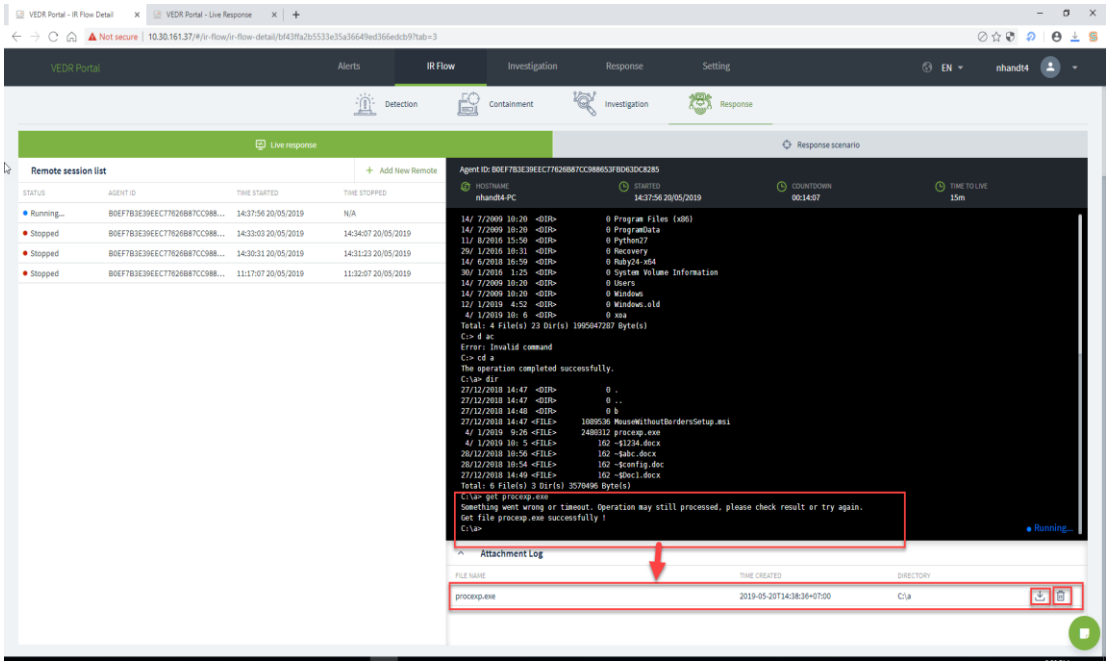
Some notes when working with commands on the console screen as follows:

- Clear command: After executing the Clear command, the system will support the user to download the entire log made on the previous console screen, by clicking on the here link.

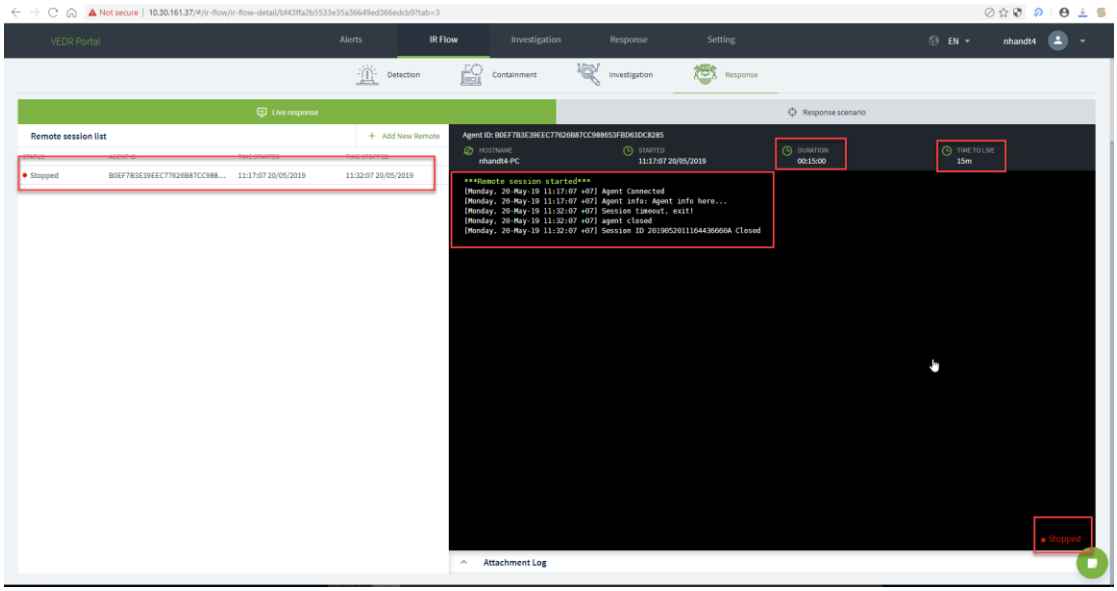


- Get <filepath> command: For example, get procexp.exe in the console screen, the result of getting the file is displayed in the Attachment Log screen at the bottom right corner of the screen. Users are allowed to download files to the browser or delete the downloaded files to the server.

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

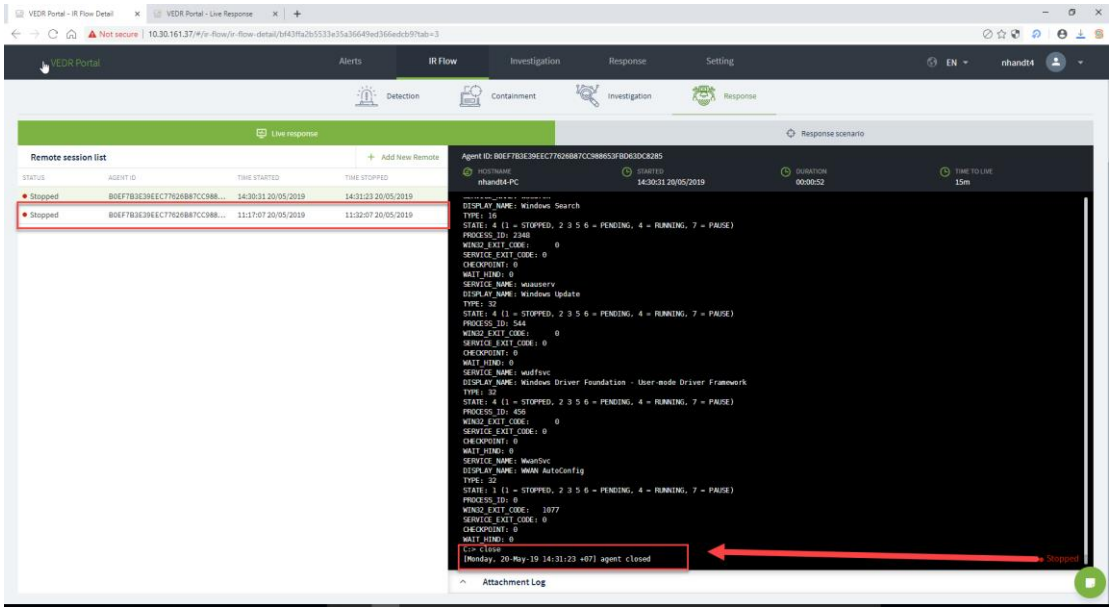


- Step 6: The Live Response session ends when:
  - Time of session expires: When the time of Duration field is equal to the time of Time to Live field.

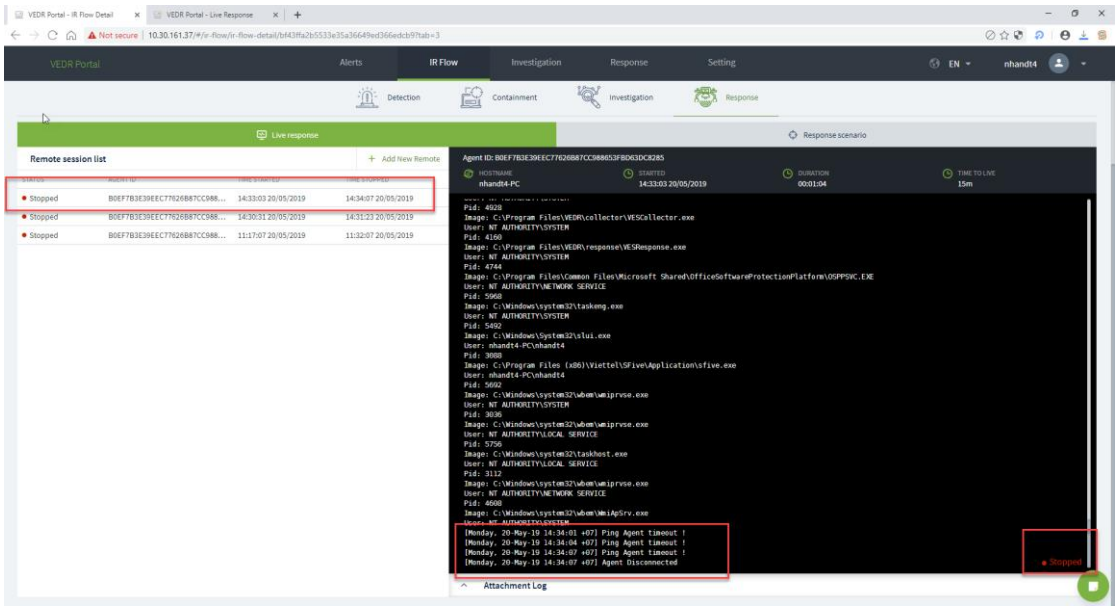


  - The user actively requests to close the connection with the Close command.

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

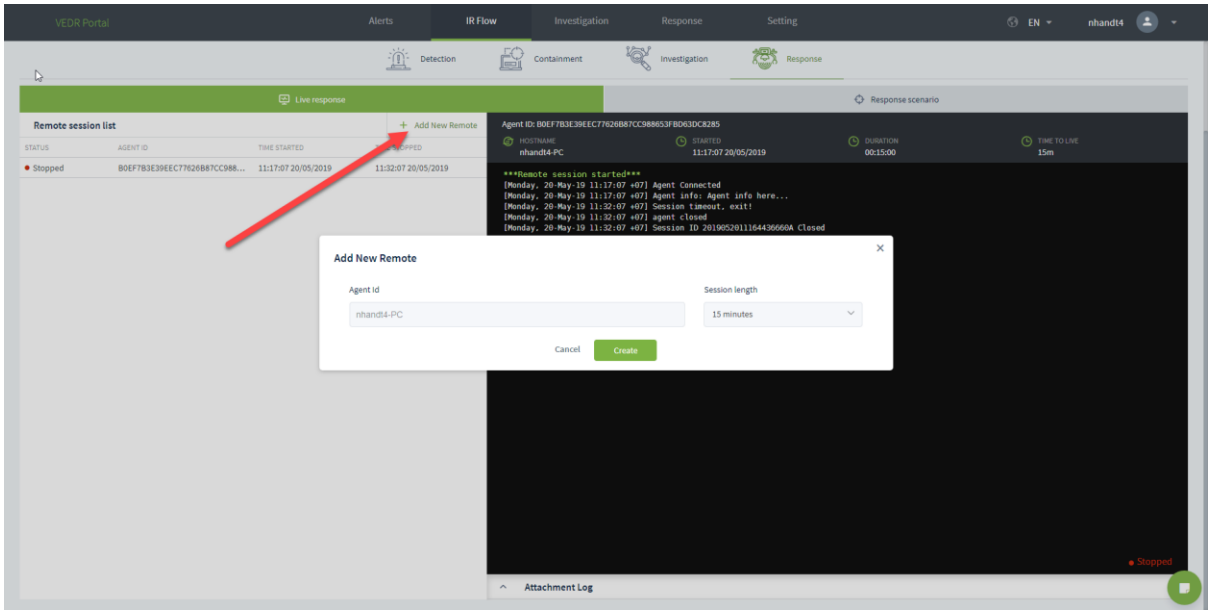


When the connection with the agent is lost, the server performs ping/pong failed more than 3 times.



In addition, users can click the + Add New Remote button to create a new live response session:

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

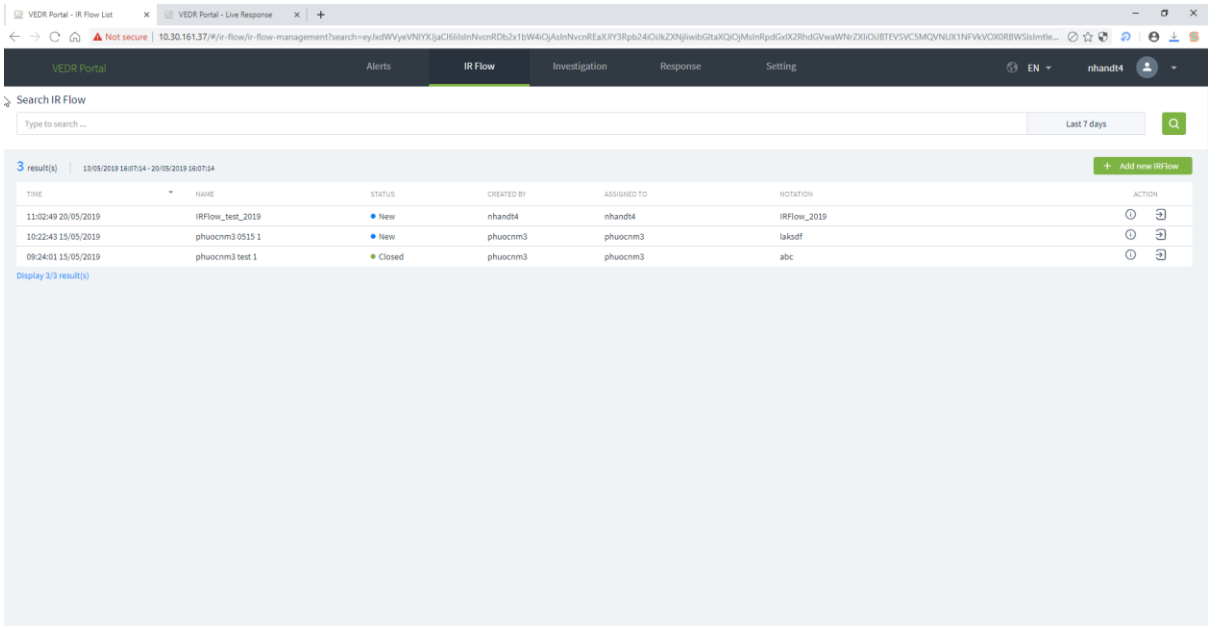


5.1.8.2. Response Scenario

The Response scenario function provides the ability to set up a Response scenario and execute the response on one or more Agents.

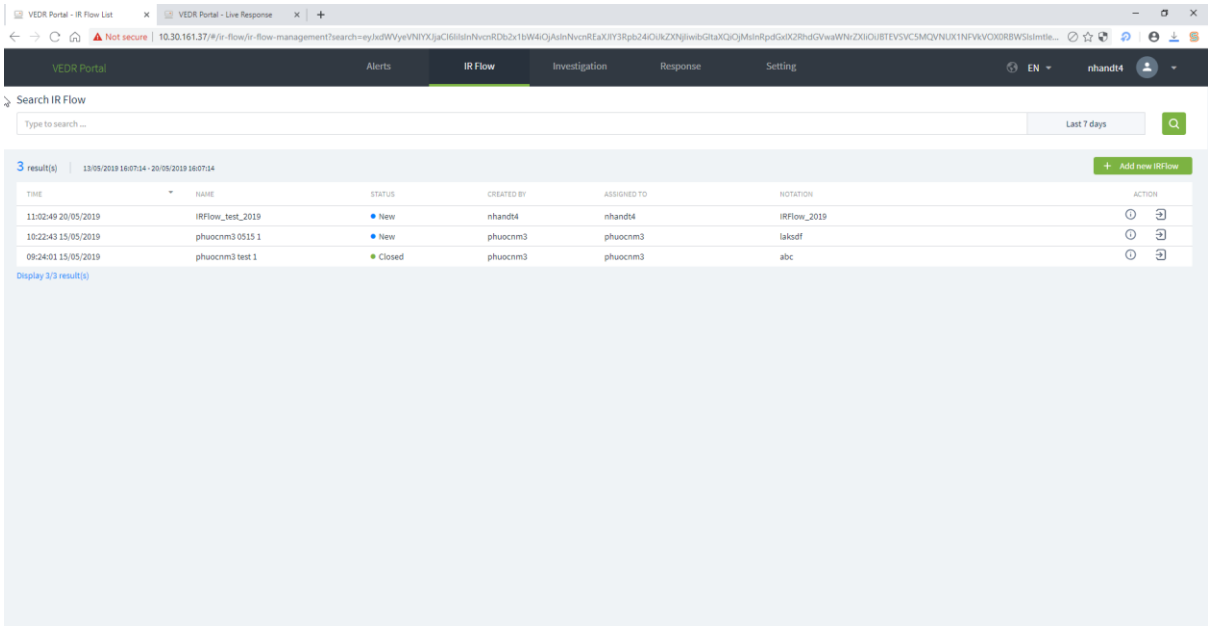
Steps to implement Response Scenario function in IR Flow as follows:

- Step 1: Click the IR Flow tab.

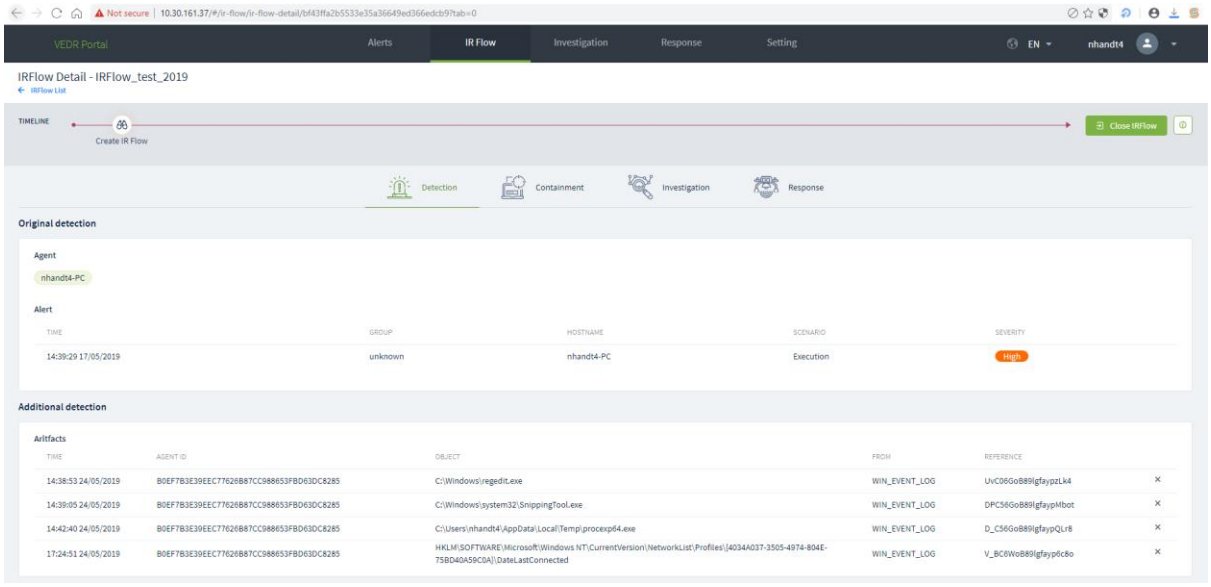


- Step 2: Click duplicate on a record in the list of records (Notes: Select the correct IR Flow record containing the Agent that needs to perform Response Scenario.).

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

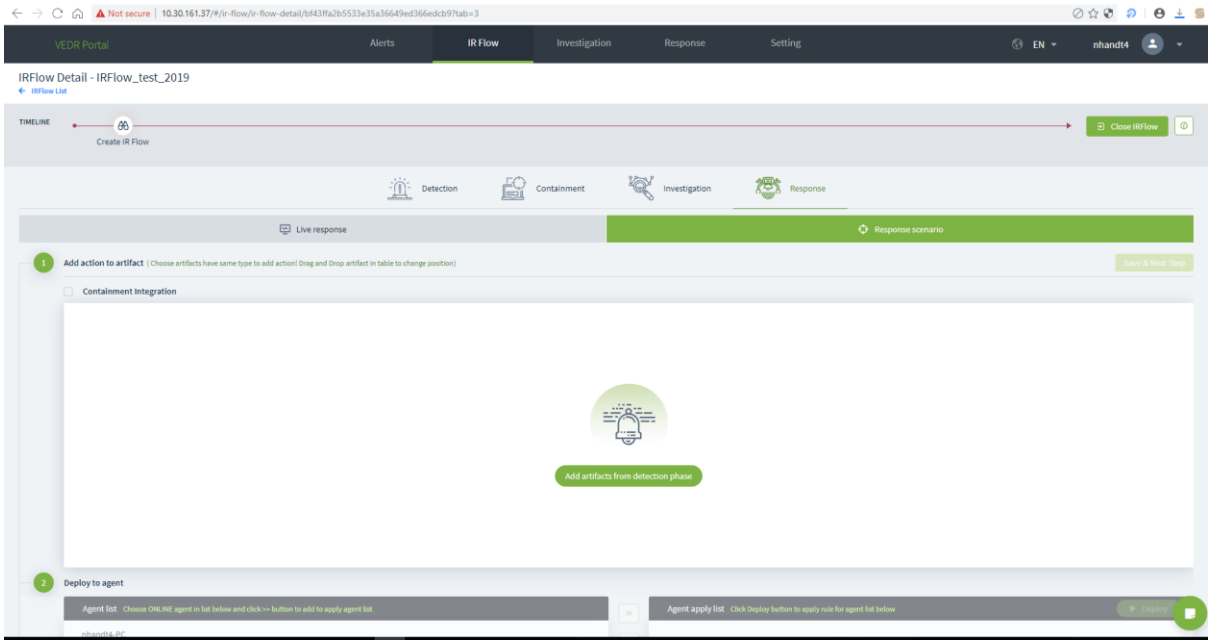


Notes: To perform the reaction scenarios, the administrator must add the Artifacts in the Detection section as shown below:

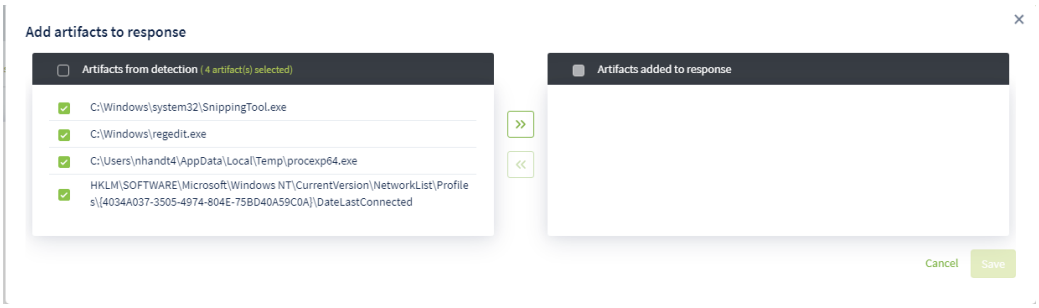


- Step 3: Click Response Tab → Response Scenario.

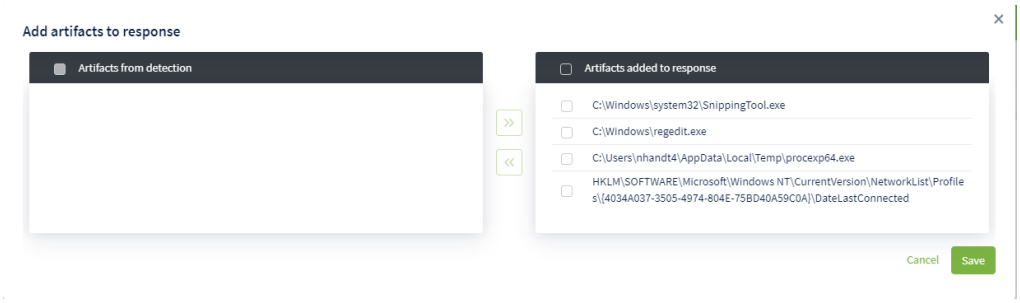
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Step 4: Perform detailed configurations as follows:
  - Add action to Artifact
    - Click the Add artifacts from detection phase button to start adding Artifacts to Response scenario.
    - Artifact List visible from the Detection tab

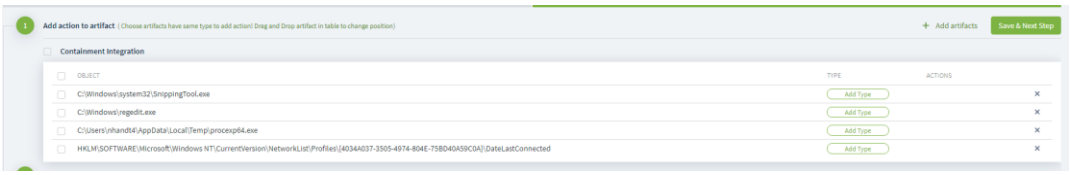


    - Click the » button to switch to the Artifact section in the Response scenario.



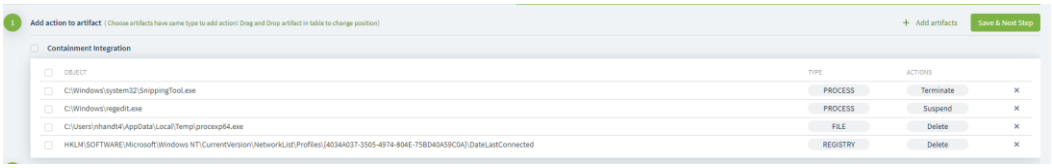
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- Click Save to save the selected Artifact List or Cancel to cancel the above selection.



- Select Type for Artifacts

The system supports assigning 1 Type/Action to 1 Artifact or 1 Type/Action to many Artifacts. There are 3 types, including: File, Process, Registry. Each Type has its own Action.

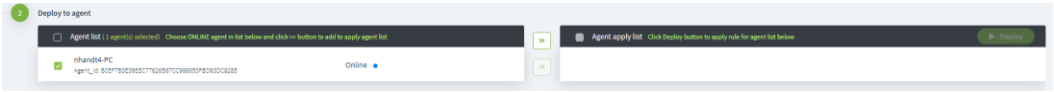


After completing the assignment of Type and Action, Click Save & Next Step to save and move to the next step or Click + Add artifacts to continue adding Artifact.

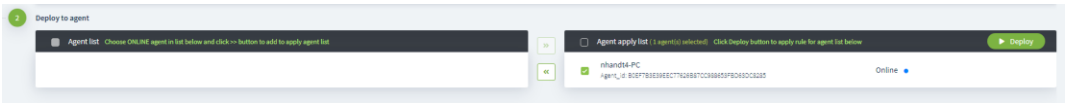
- Deploy to Agent

Agent List is obtained from the Detection tab

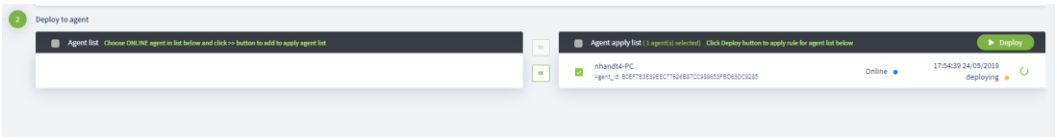
- Tick to select the Agent that is online in the Agent List of IR Flow to switch to the List of agents that execute the Response scenario.



- Click » to switch to list of deployable agents.
- Tick to select Agent to deploy.

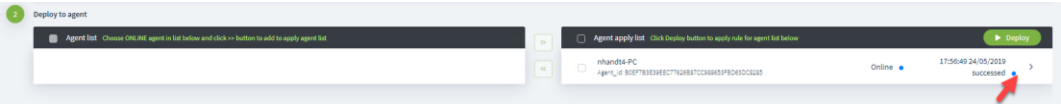


- Click the Deploy button
- After clicking the Deploy button, there are below states:
- Deploying

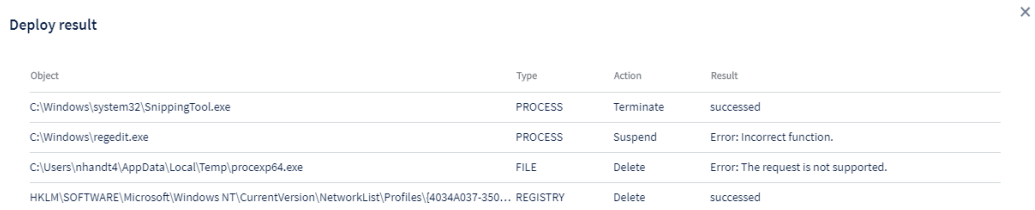


Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- Successes

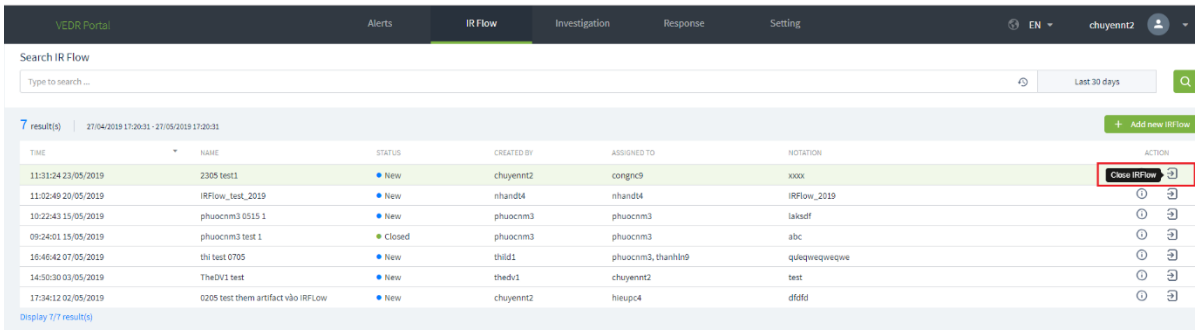


- Click on the details to view the scenario implementation results

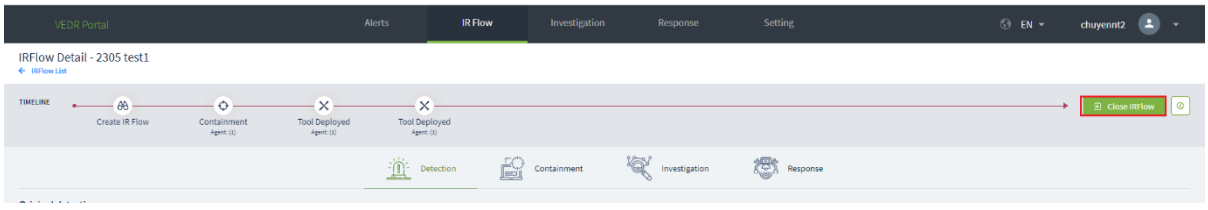


5.1.9. Close IR Flow

- Close IR Flow after investigation and process is complete.
- To close IR Flow click Close IR Flow on IR Flow List screen.

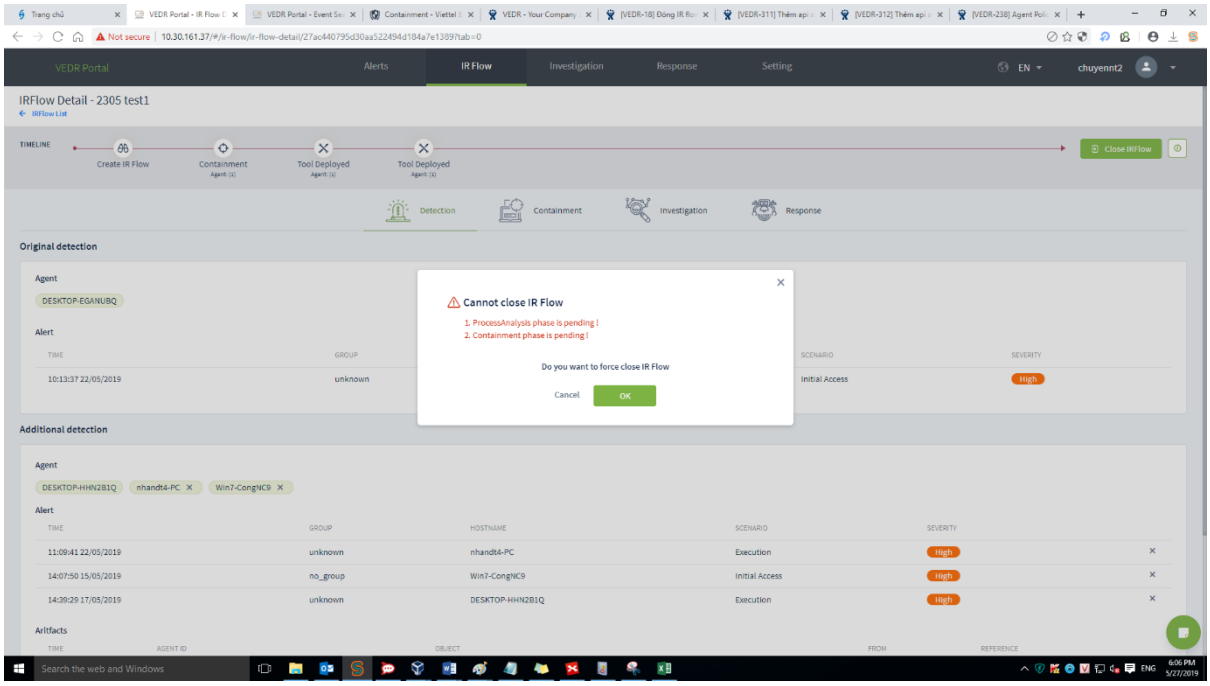


- Or click Close IR Flow on the timeline at any phase in IR Flow, such as Detection, Containment, Investigation, Response.

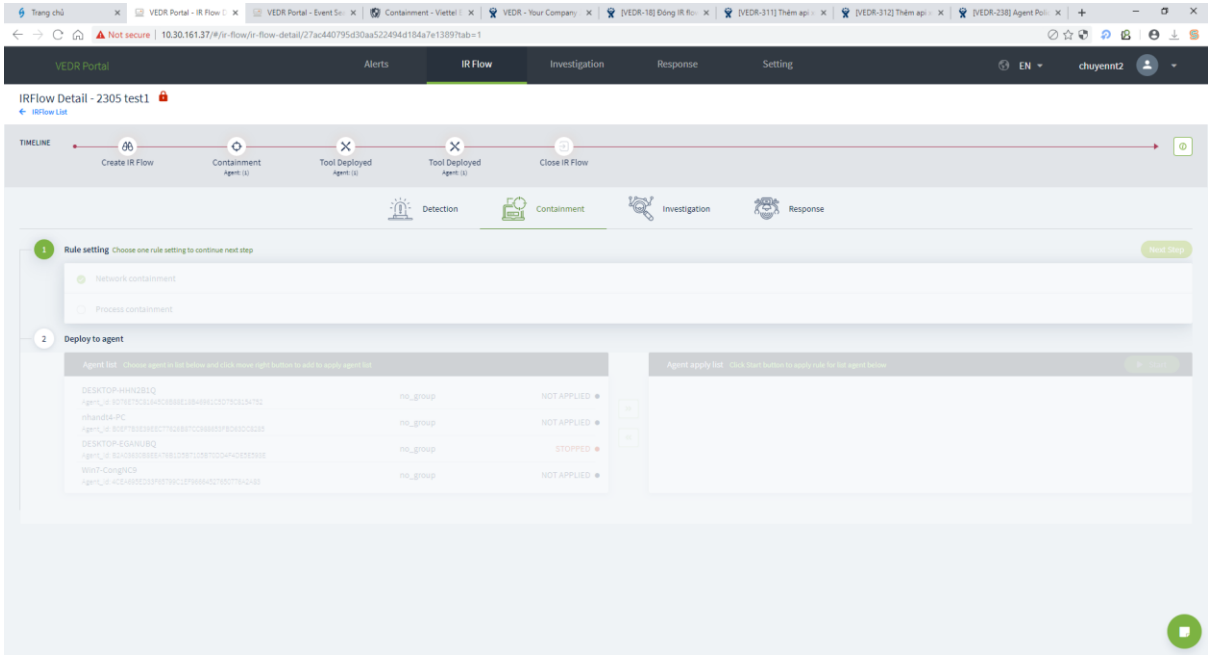


  - If when selecting Close IR Flow, there are unfinished tasks, such as: Containment, Live Response, Response Scenario, Deployment tool, etc., a notification will be displayed to ask the user as follows:

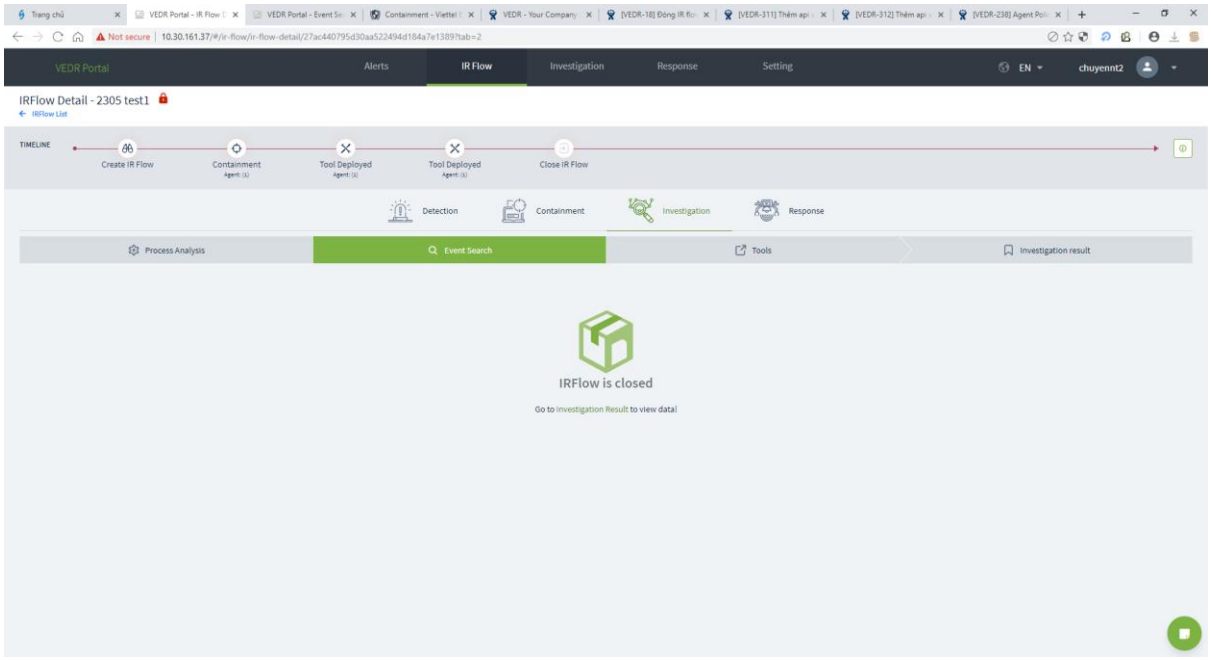
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

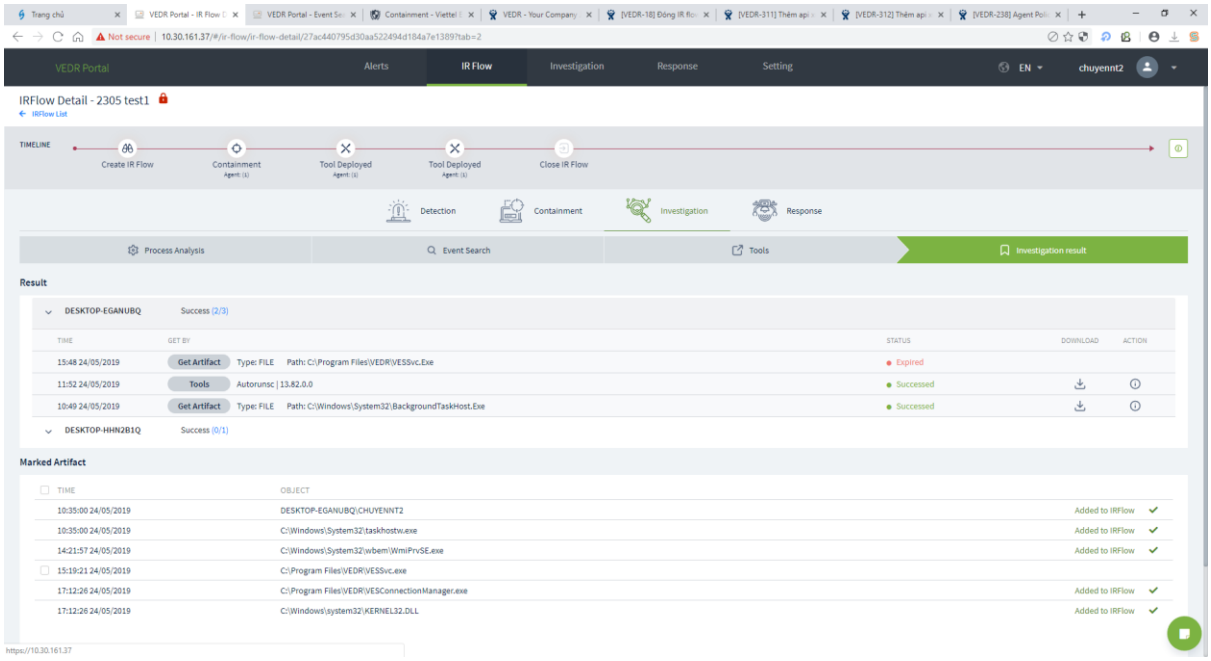


- When the user selects OK, it will close all connections to the Agent in IR Flow.
- When entering the closed IR Flow, information in only 2 tabs of Detection and Investigation Result can be viewed, other tabs with different function will be disabled or will not display data.



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





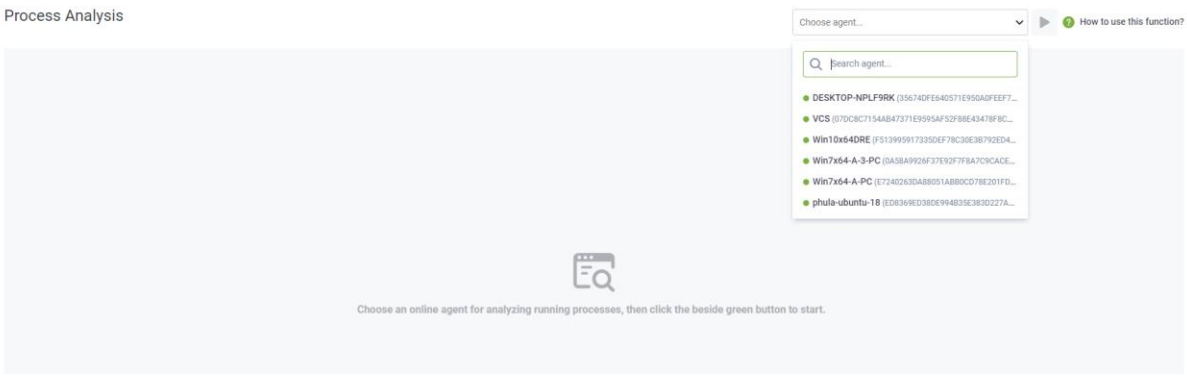
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

6. Investigation Screen

The Investigation screen includes a number of small tabs, which are Process Analysis, Event Search, and Deploy Tools. In terms of operation, these two functions are not much different from those in IR Flow, however, there are some other points that will be described in details as follows:

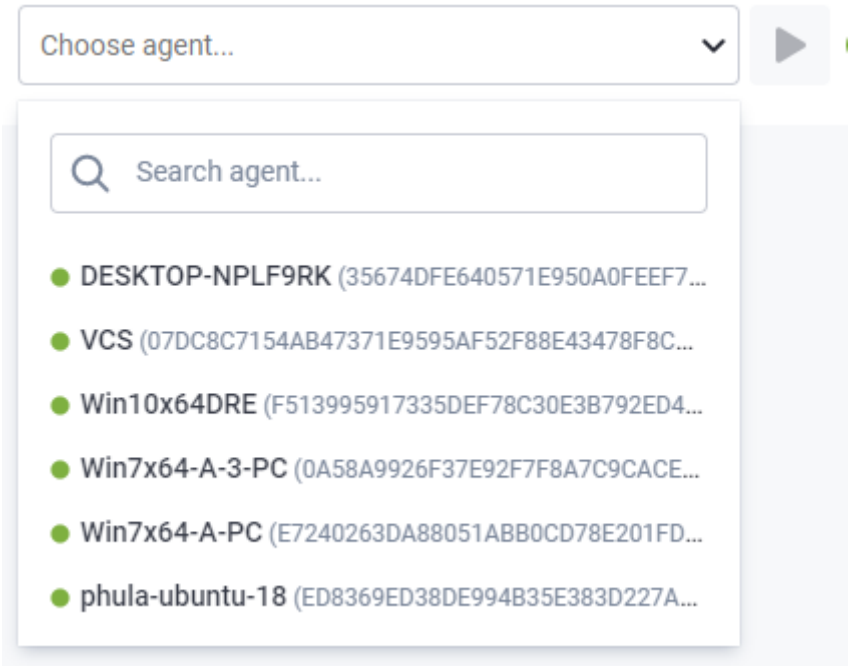
6.1.1. Investigation Process Analysis

The function allows the user to create a connection and check the process state under the user's machine. In which:

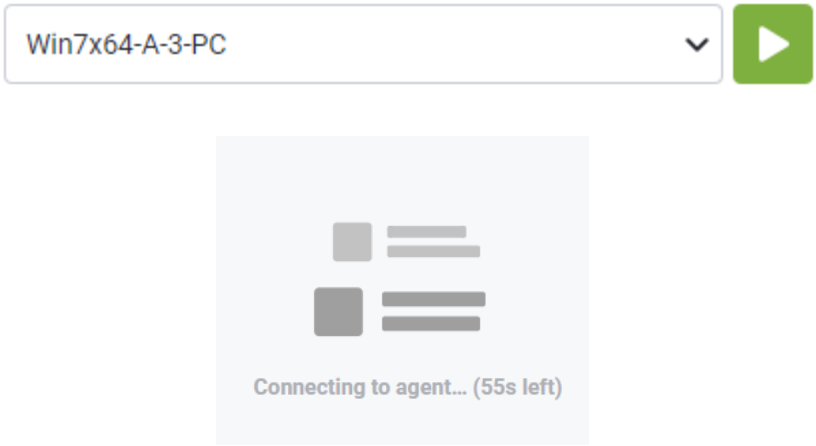


- List of user machines:
  - User login under root group: Display all Agents in the active system < 30 days.
  - User login under default group: Display all Agents in the default group.
  - User login under parent-level group: Display all Agents in the group of the user logging in and the corresponding 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.
- Step 1: Search and select Agent to connect (Notes: To make sure to connect, the list only displays the online machines.)

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

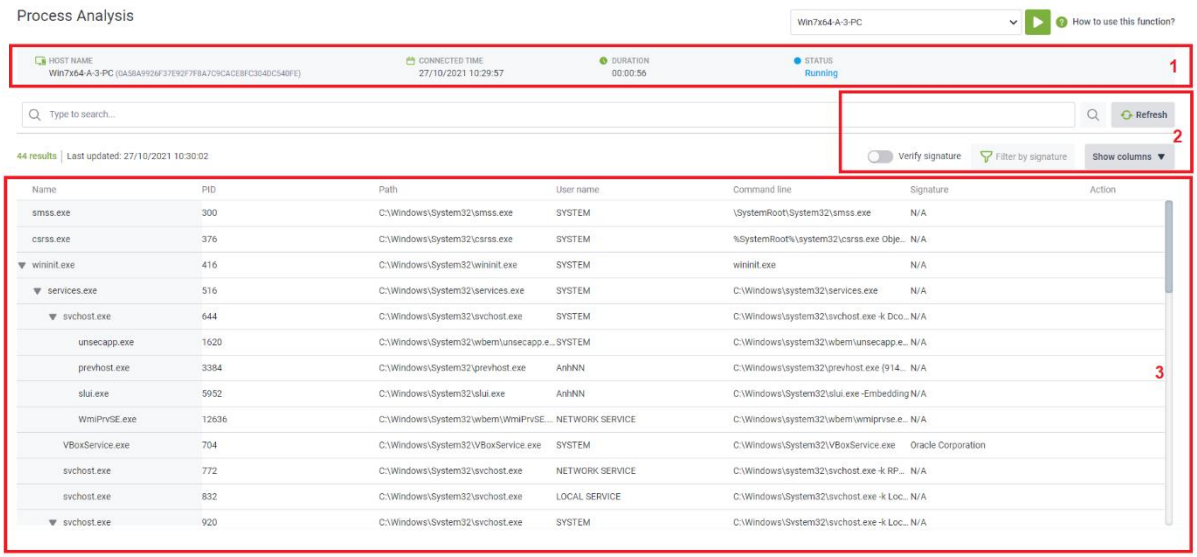


Select 1 machine and click  to make the connection (connection can take up to 60 seconds.)



- Step 2: View the list of active processes at the user's machine.

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



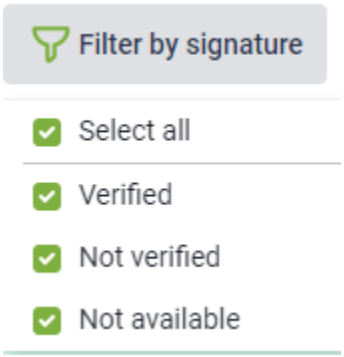
In which, the interface is divided into below information groups:

- (1) The information group related to the connection, including: The connecting machine, the time of creating the connection, the duration of the connection to the present and the connection state.
- (2) The information group supports searching/refreshing and filtering data in the list, including the following actions:

: Allow searching by keyword of the data currently displayed in all fields on the list.

Refresh : Allow refreshing data (still hold the the search conditions and filter conditions in use, only get the latest data from the user's machine to display).

Verify signature : Enable/disable to obtain digital signature information for processes. In case this configuration is enabled, the progress data by digital signature is enabled to filter.



The digital signature states will specify the color of the corresponding record.

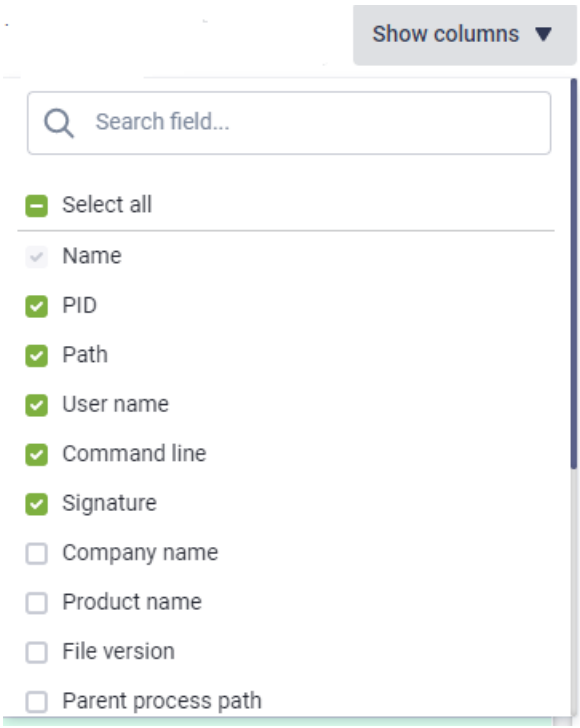
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

CRYPTSP.dll	C:\Windows\system3...	d0c2fbb6d97416b01...	7eab6c37f0a845e64...	Microsoft Corporation	Microsoft Windows
GDI32.dll	C:\Windows\system3...	1084aa52ccc324ea5...	6e972cf624f7c0de81...	Microsoft Corporation	Microsoft Windows
IMM32.DLL	C:\Windows\system3...	aa2c08ce85653b1a0...	83dfd0c119b20aedb...	Microsoft Corporation	Microsoft Windows
KERNELBASE.dll	C:\Windows\system3...	da68c291b4ef2dec9c...	21aa4779fc21e7621...	Microsoft Corporation	Microsoft Windows
LPK.dll	C:\Windows\system3...	d202223587518b13d...	9db971b866d058adb...	Microsoft Corporation	Microsoft Windows
MSCTF.dll	C:\Windows\system3...	c431eaf5caa1c82cac...	addf850128dc675e6...	Microsoft Corporation	Microsoft Windows
NSI.dll	C:\Windows\system3...	044fe45ffd6ad40e3b...	a1688a5e6e0f7037c...	Microsoft Corporation	Microsoft Windows
PerfCtrl.dll	C:\Program Files\Ajia...	a8a221af714077ec8...	e11aec935d0a34766...	Viettel Corporation	Viettel Group
RPCRT4.dll	C:\Windows\system3...	0611473c1ad9e2d99...	90afcc2a60350ece27...	Microsoft Corporation	Microsoft Windows
USER32.dll	C:\Windows\system3...	fe70103391a64039a...	f7d219d75037bc98f6...	Microsoft Corporation	Microsoft Windows
USP10.dll	C:\Windows\system3...	2f8b1e3ee3545d3b5...	2a3ec01f3bafe7d7d6...	Microsoft Corporation	Microsoft Windows
VESSvc.exe	C:\Program Files\Ajia...	e381c58f04dae8f2a2...	c6510091a2433f918f...	N/A	N/A
advapi32.dll	C:\Windows\system3...	6df46d2bd74e3da1b...	2dc945f6f2c4a82189...	Microsoft Corporation	Microsoft Windows

- Verified: Green - with digital signature and still valid
- Not verified: Red - no digital signature or expired digital signature
- N/A: White - no digital signature information found.

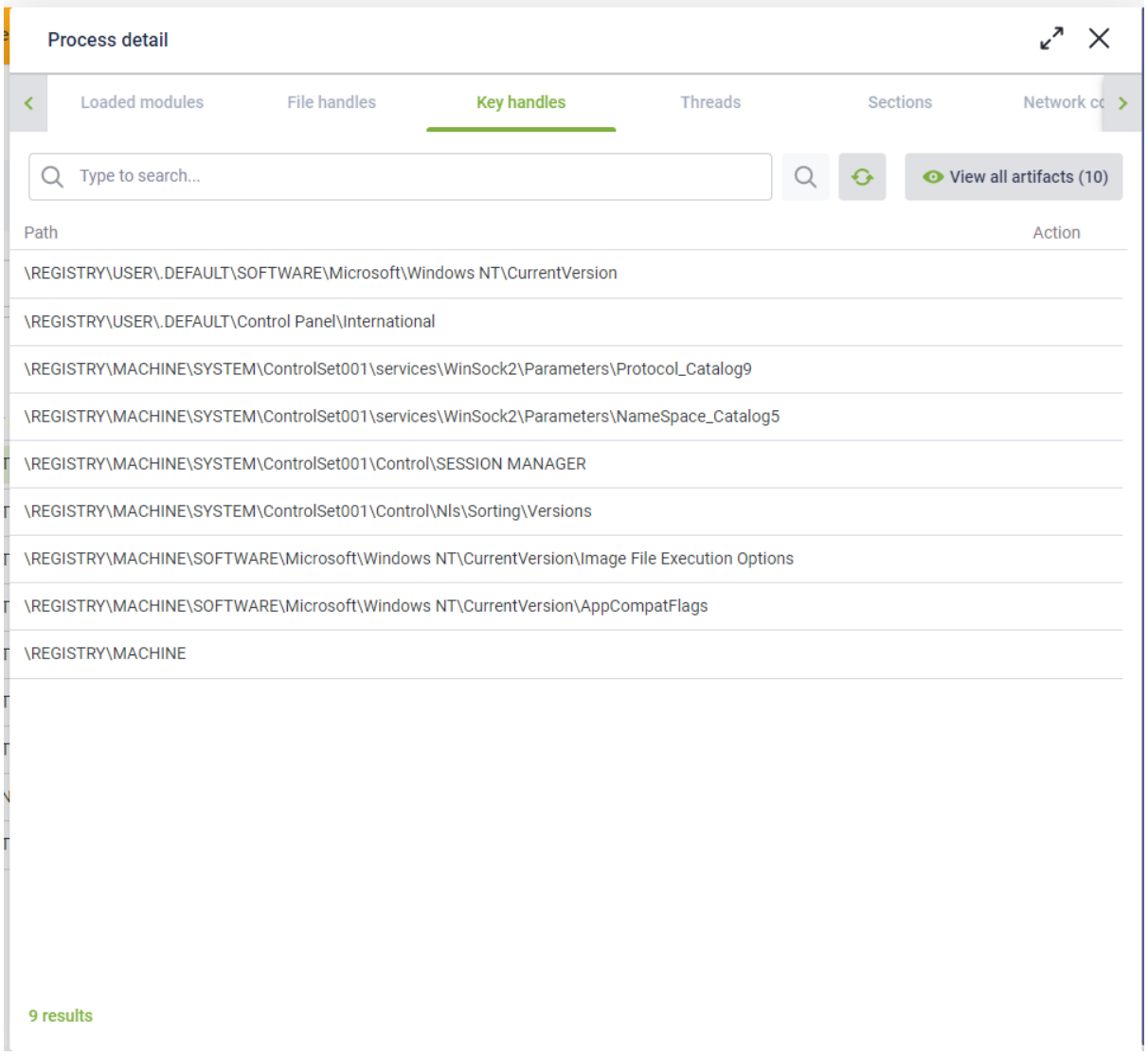
Show columns ▼ : Allow adjusting the display field on the progress list.

On the list, except the Name field, which is always displayed permanently, the remaining fields can be optionally displayed or not displayed.



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) Process list: Display current progress data on user machine with selected information fields in Show column section. At each record, double click to view progress details.



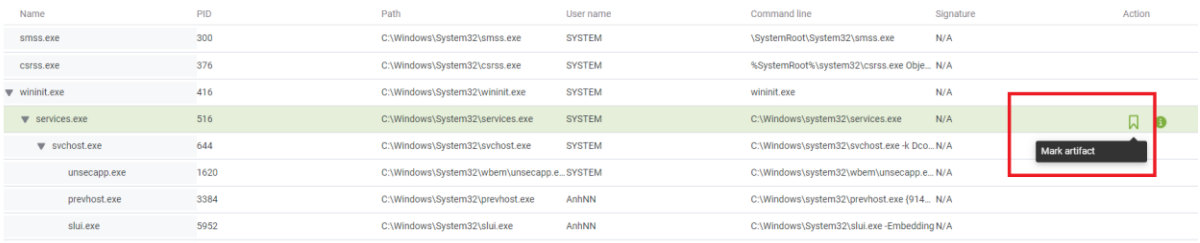
Progress details are divided into tabs. For each tab, a corresponding list of information is displayed.

- Step 3: Marking artifact

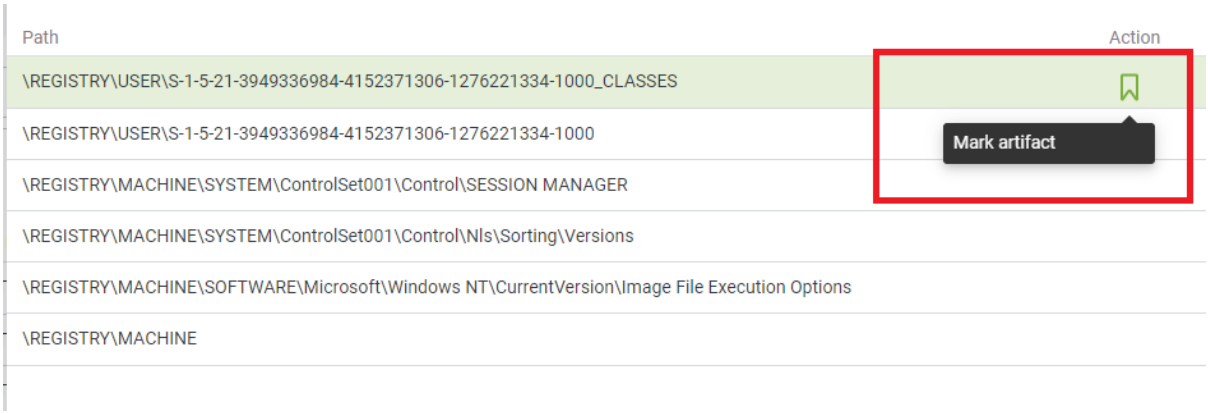
Similar to the Process Analysis function in IR Flow, this screen also provides marking of artifacts for investigation.

User can select progress outside the list to mark.

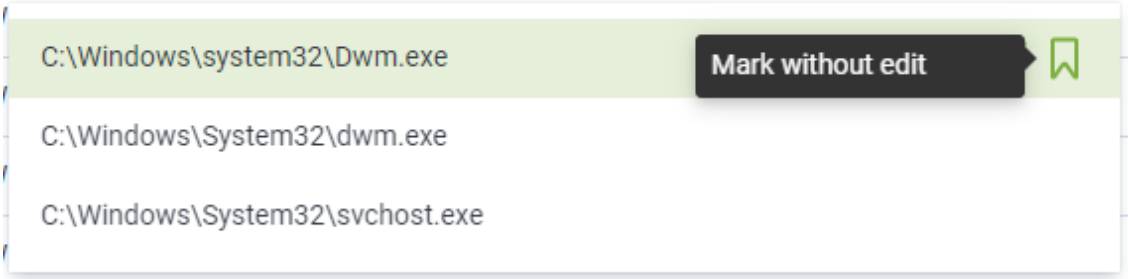
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



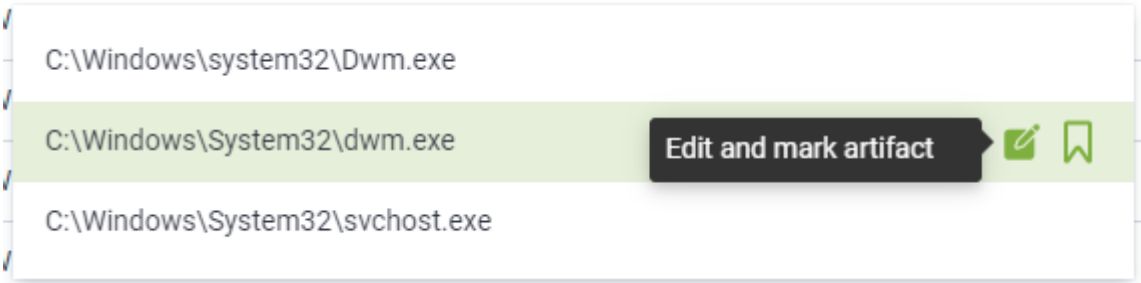
Or mark suspicious objects in process details.



For each selected object, select Mark with edit - mark the current content directly.



Or users can edit object content before marking.

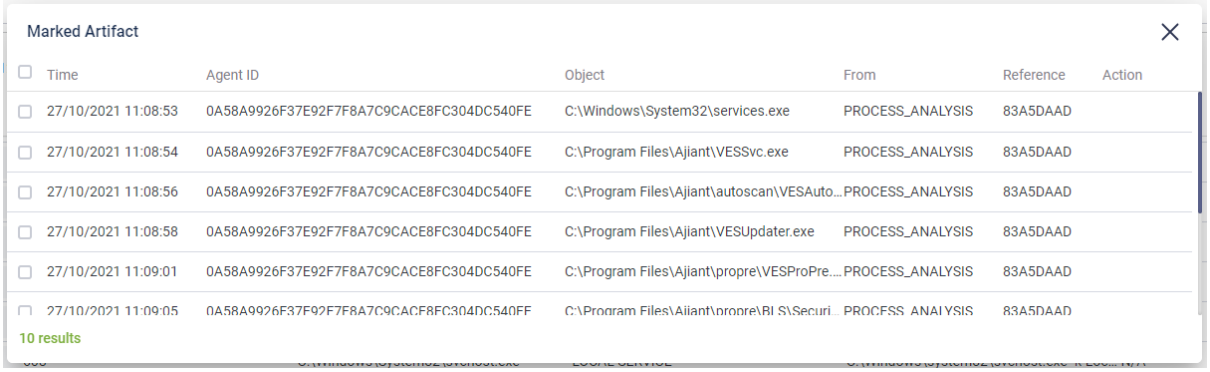


After marking, to review the list by clicking 

.

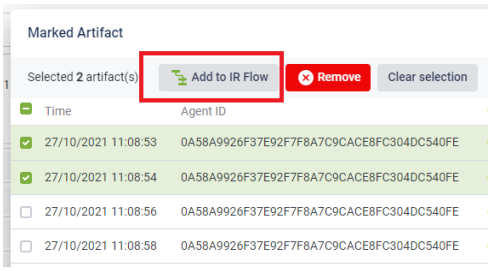
Notes: This button is only displayed when at least 1 artifact is marked.

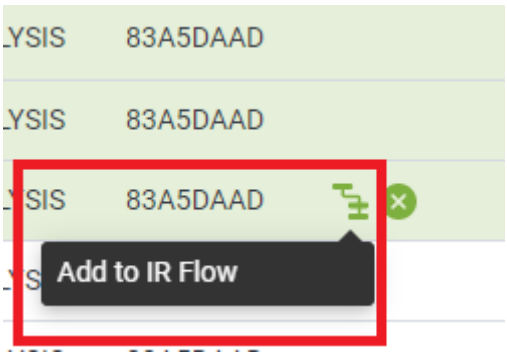
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



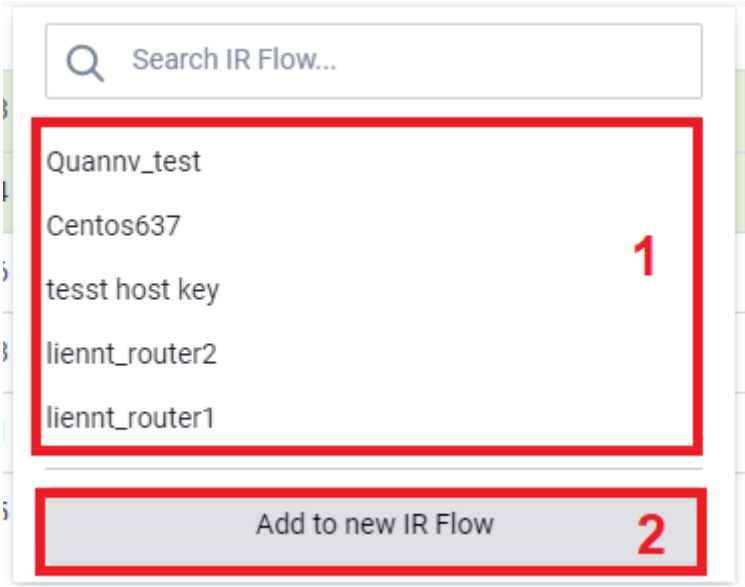
- Step 4: Add artifact to IR Flow

On the Marked artifact tab, click Add to IR Flow on a record or select multiple artifacts in multi-select mode and click Add to IR Flow.





Choose from a ready-made IR Flow or create a new IR Flow.

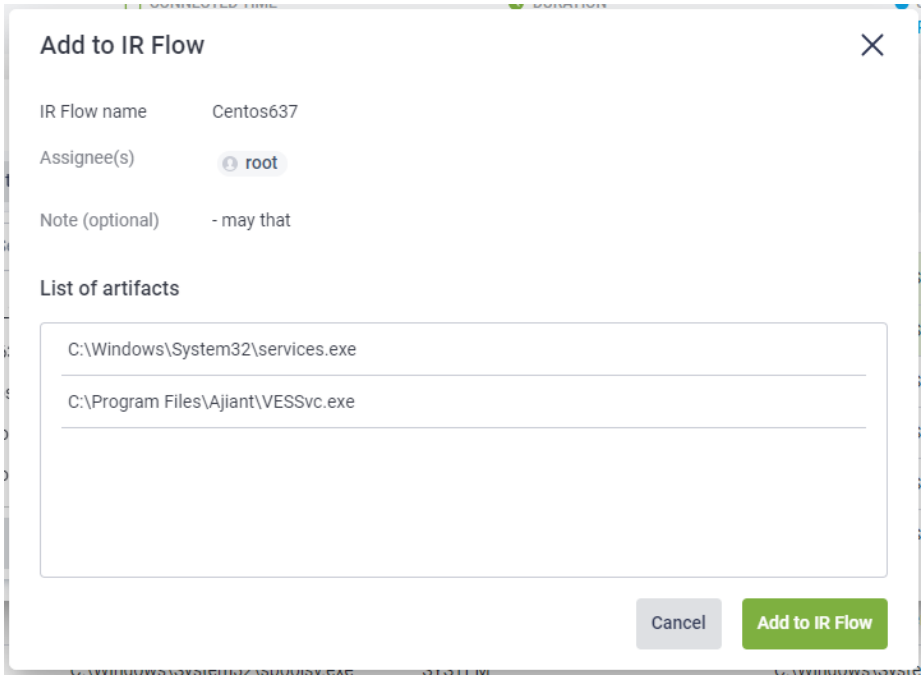


(1) Ready-made IR Flow list:

- User login under root group: Display all IR Flow 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

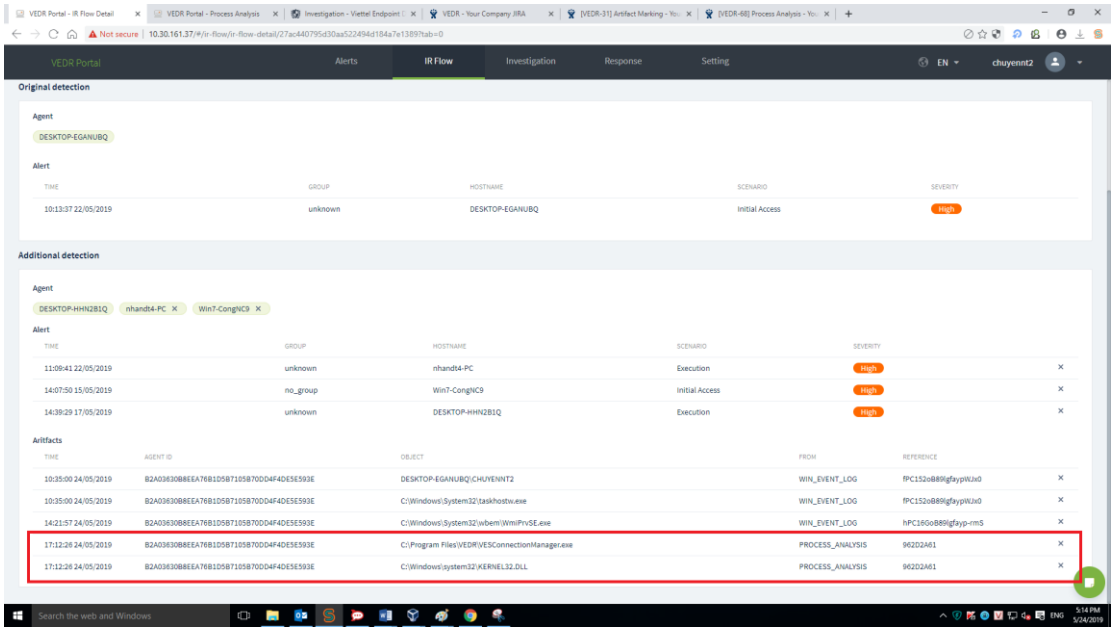
- User login under default group: Display all IR Flow assigned to the user logging in.
- User login under parent-level group: Display all IR Flow assigned to the user logging in and the users belonging to the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all IR Flow assigned to the user logging in.



The assigned to list when creating a new IR Flow

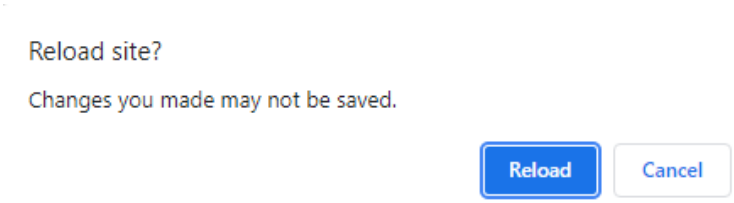
- User login under root group: Display all usernames in the system.
- User login under default group: Display the username of the user logging in.
- User login under parent-level group: Display all usernames belonging to the child-level group of the user logging in and the user logging in.
- User login under a child-level group or many child-level groups: Display the name of user logging in.
  - If choose to add into an existed IR Flow, when moving to the Detection artifact screen, it will be added to the Additional detection section.
  - If choose to add a new IR Flow, when moving to the Detection artifact screen, it will be added to the Original detection section.

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:

Artifact data will not be lost if the connection is transferred to different machines or in case the current machine loses connection, the user reloads the page or navigates to another page, the system asks for confirmation as follows:



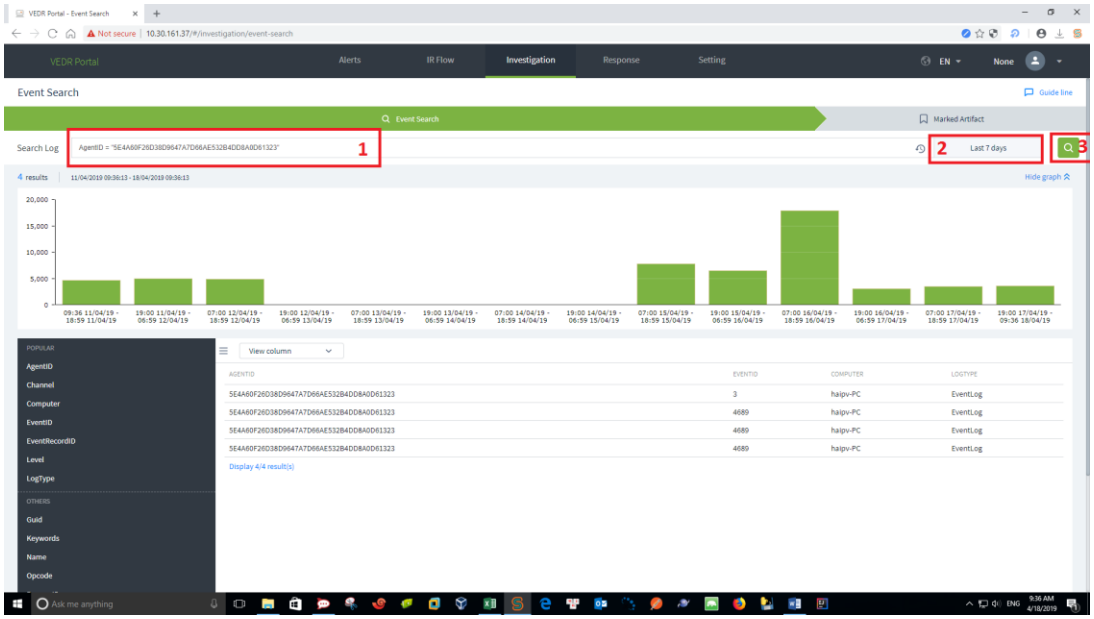
6.1.2. Investigation Event Search

6.1.2.1. Event Search

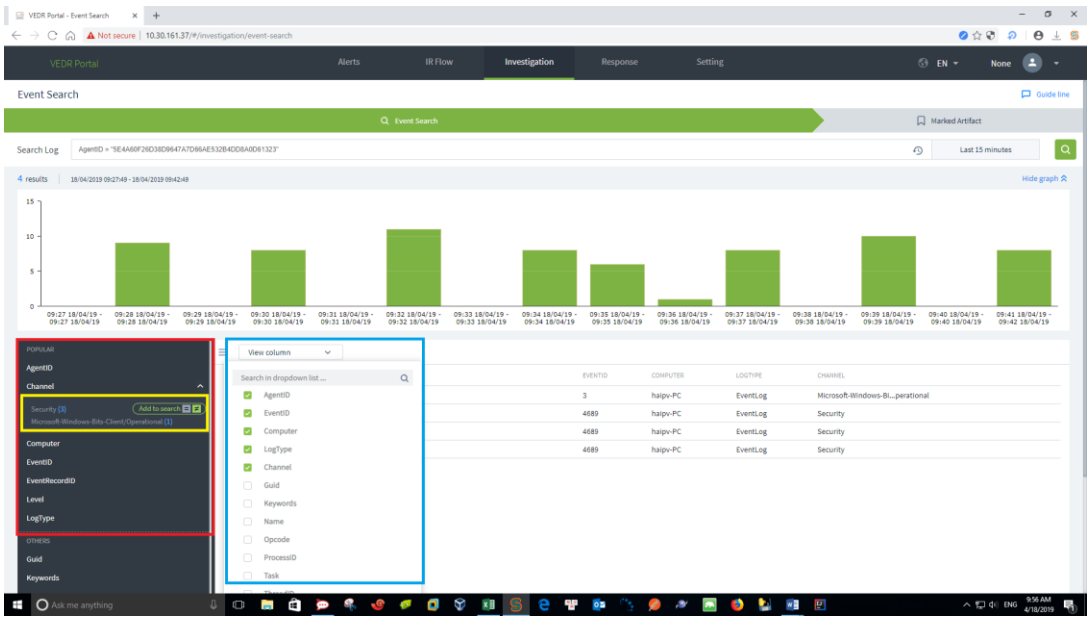
This function is similar to the IR Flow's Event Search.

- Step 1: Enter the query → Select a time range → Click Search.

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

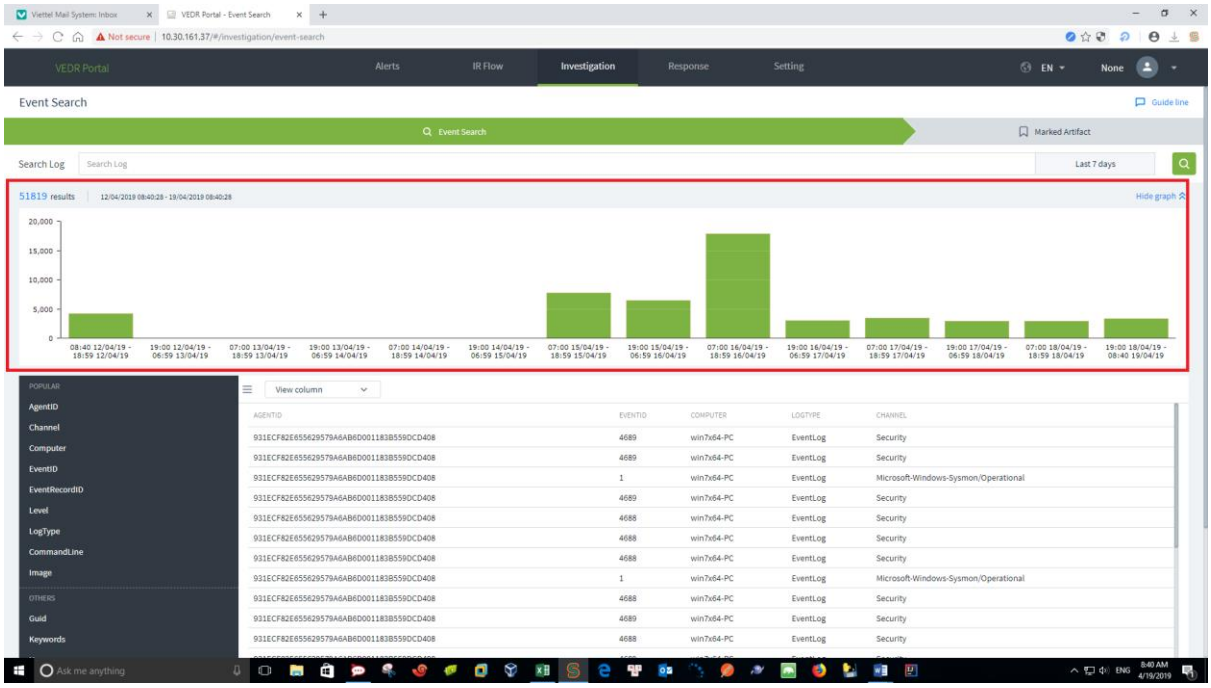


- Step 2: Add search fields to the query with Popular and Others fields.



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

6.1.2.2. Chart



- Step 1: Perform a search same with the Event Search.
- Step 2: The chart displays statistics according to the search time range. The way to divide the time range corresponding to the columns on the chart is as follows:
  - Statistics for >= 90 days: Divide into 30 statistical intervals.
  - Statistics of events in the last 60 days: Divide into 20 intervals, 3 days/each interval.
  - Statistics for 30 days: Divide into 15 intervals, 2 days/each interval.
  - Statistics for 7 days: Divide into 14 intervals, 12 hours/ each interval.
  - Statistics for 1 day: Divide into 24 intervals, 1 hour/ each interval.
  - Statistics for 12 hours: Divide into 12 intervals, 1 hour/ each interval.
  - Statistics for 6 hours: Divide into 12 intervals, 30 minutes/ each interval.
  - Statistics for 1 hour: Divide into 12 intervals, 5 minutes/ each interval.
  - Statistics for 30 minutes: Divide into 15 intervals, 2 minutes/ each interval.
  - Statistics for under 30 minutes: Divide into 1-minute intervals.

When hovering over each column, the time range and the number of records searched during that period will be will displayed.

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: The timelines on the chart are the timelines calculated in round days/hours/minutes to suit the long or short statistical period.

6.1.2.3. Event Handle

- View event details: Double click on a record or hover over a record and click the View details icon.

- Marking artifact: Hover over a record and select Marking artifact.

- Select path and click Accept.

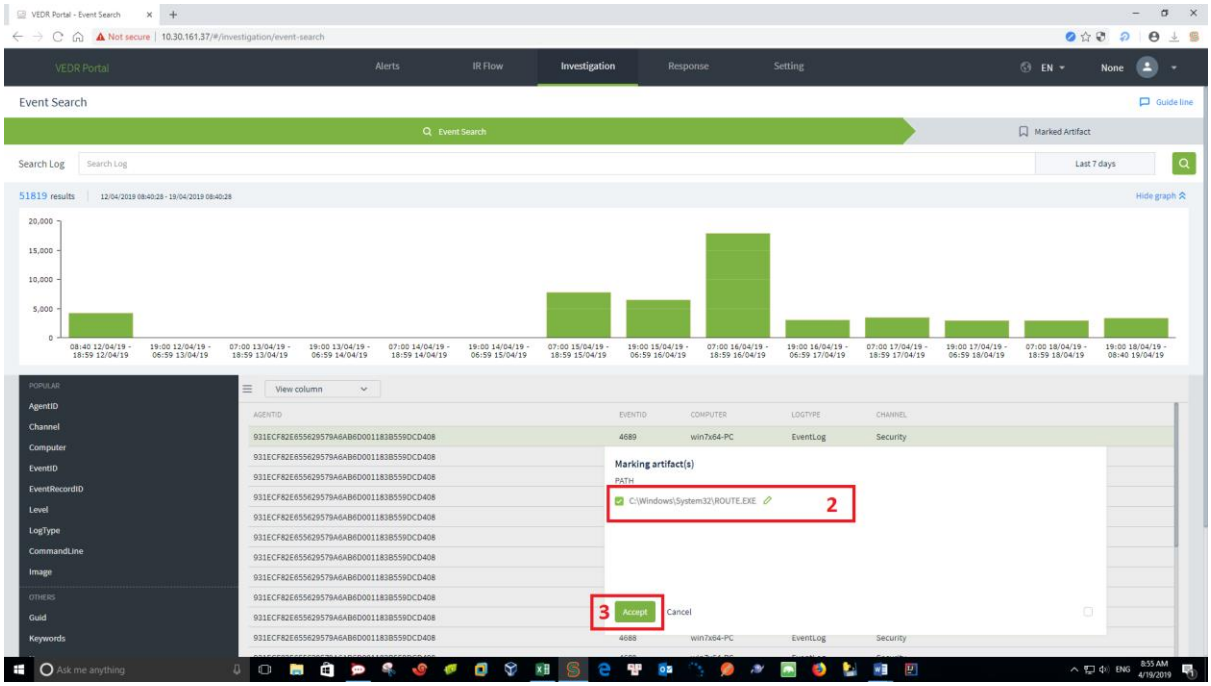
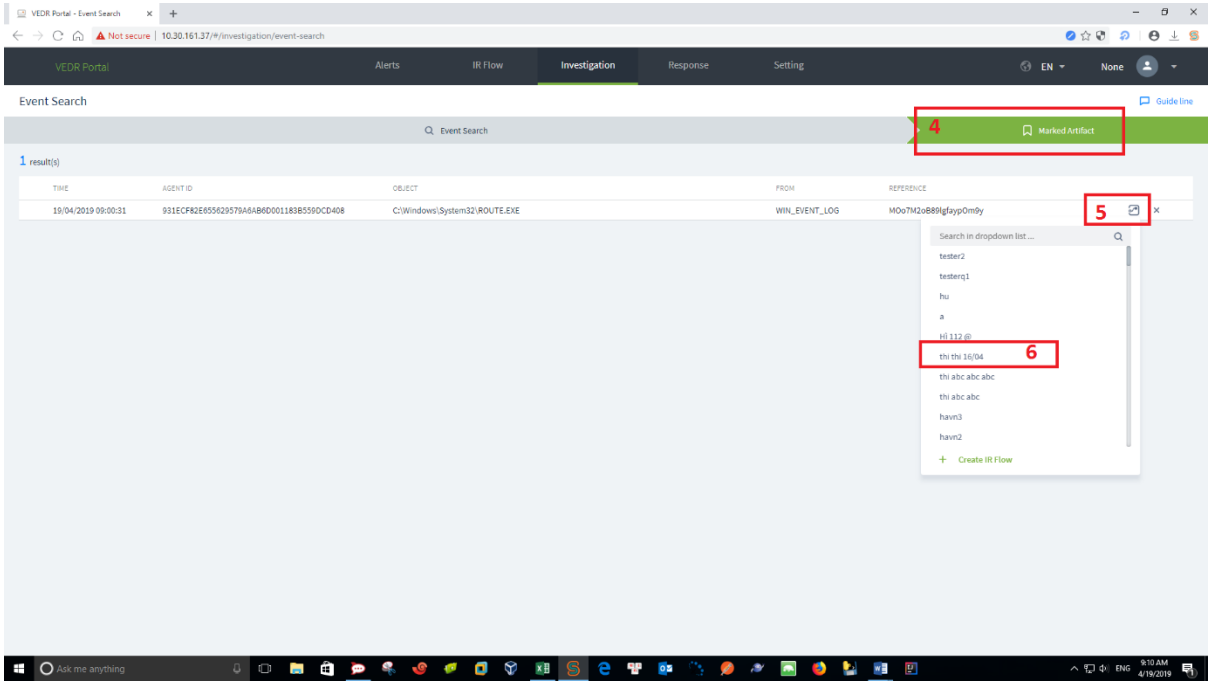
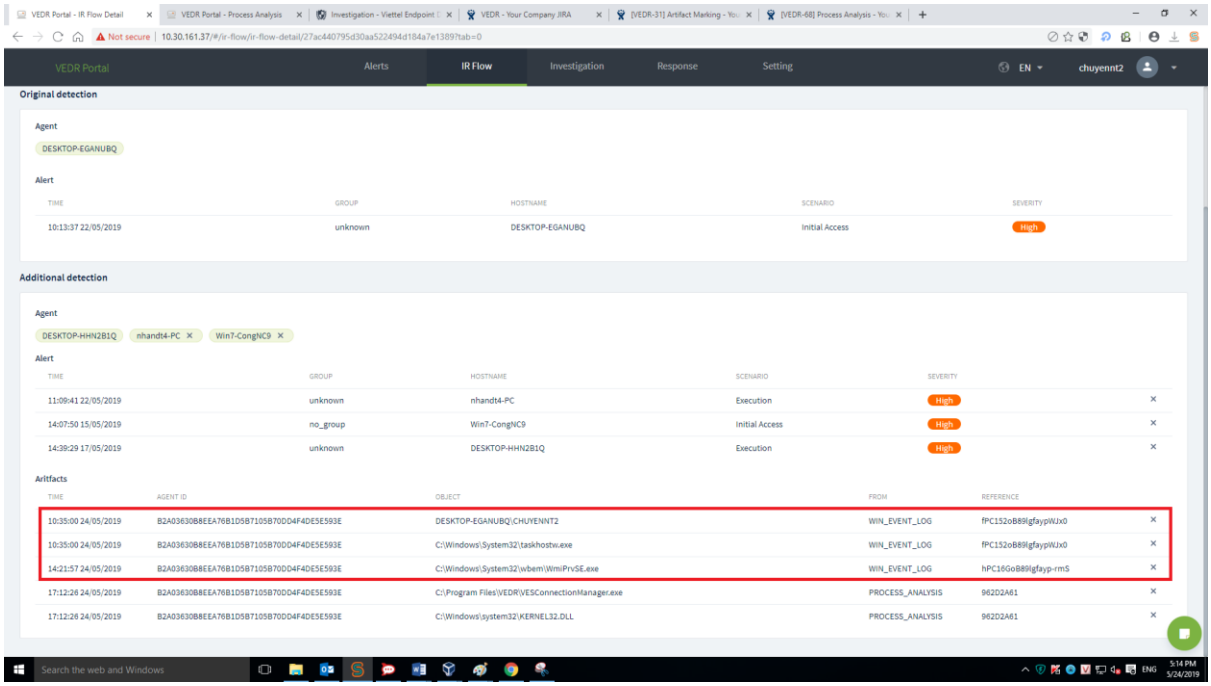


Figure 2: Investigation/Event Search Marking artifact

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 IR Flow and add that artifact to IR Flow.





- Similar to the Process Analysis function, there are also some notes as follows:
  - If switching tabs between Event Search and Marked artifact, the data in Marked artifact screen will not be lost.
  - If switching to the big tabs, such as Alert, IR Flow, Response and Setting, the data in Marked artifact screen will be lost.

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

6.1.3. Investigation Deploy Tools

6.1.3.1. Tool Management

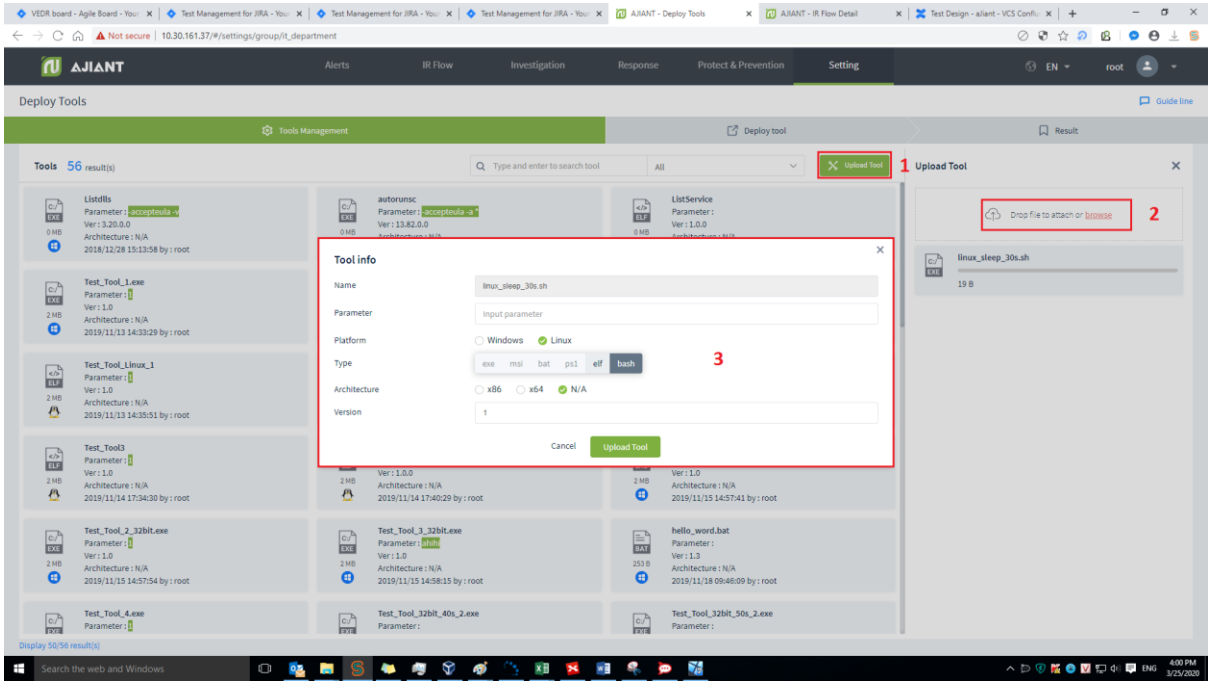
Purpose: Manage all tools of the system. Users can add/delete tools on this screen.

Features on this screen include as follows:

- Display tool list with detailed information of the tool, including: Name, Parameter, Version, Architecture, Upload User, Platform and Hash code.
- Search tool: Search by many criteria, such as All (all data fields), Name (tool name), Tool ID, Version, SHA1, Upload User and Platform.
- Upload tool: Upload tool running on Windows and Linux agents with a maximum capacity of 10MB.

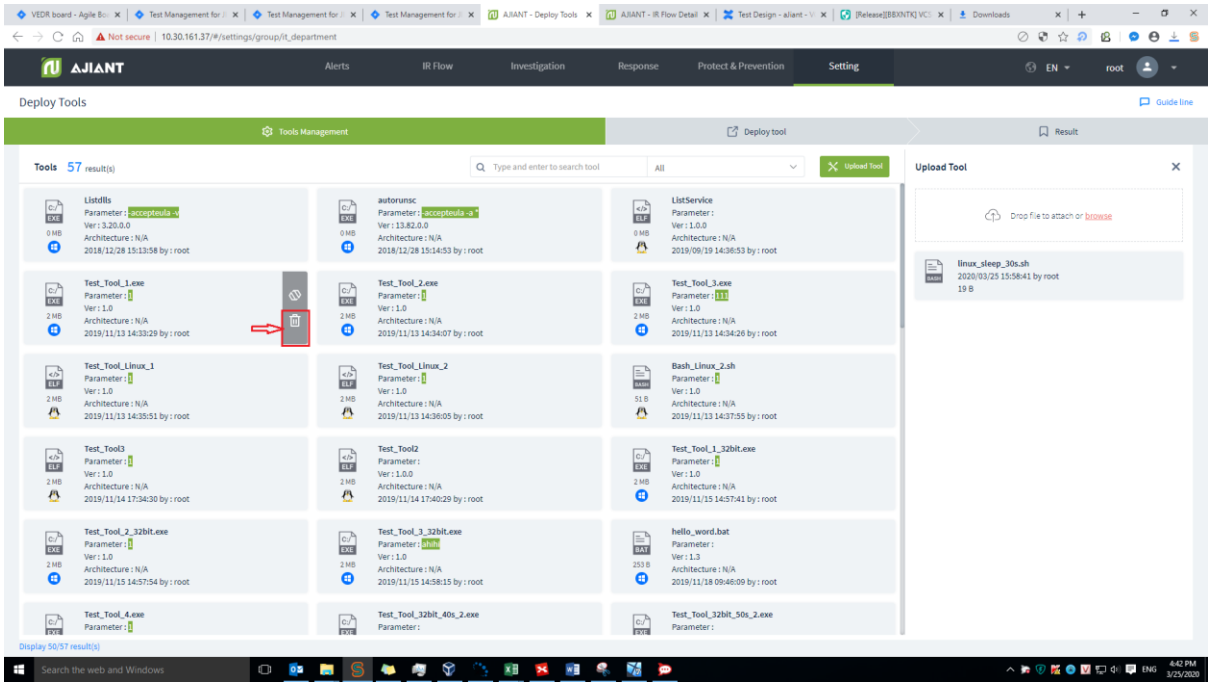
For the Upload tool feature, perform the following steps:

- Click Upload tool → Select the path to the tool to upload or drag and drop the tool into the interface → Enter information in the Tool info popup → Click Upload tool.



For the Delete tool feature, hover the mouse over the tool to delete → Select Delete.

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



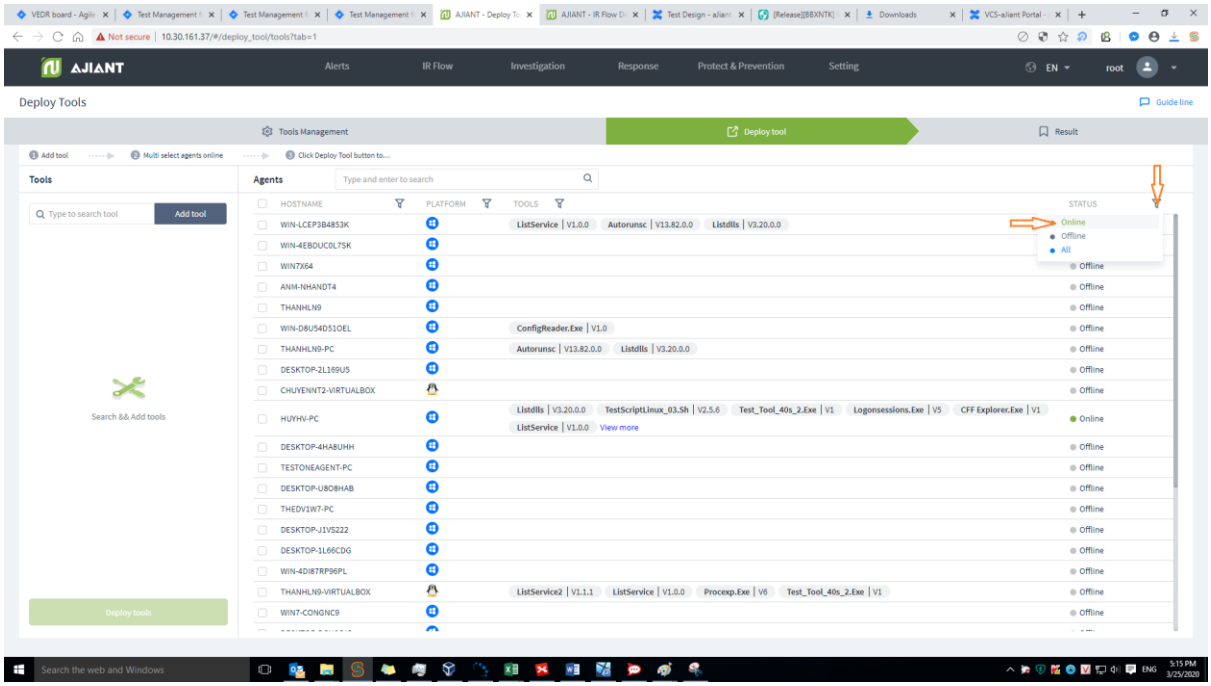
6.1.3.2. Deploy tool

The actions are similar to the Deploy tool function in IR Flow in section 3.4.4.3. However, there are a few other points as follows:

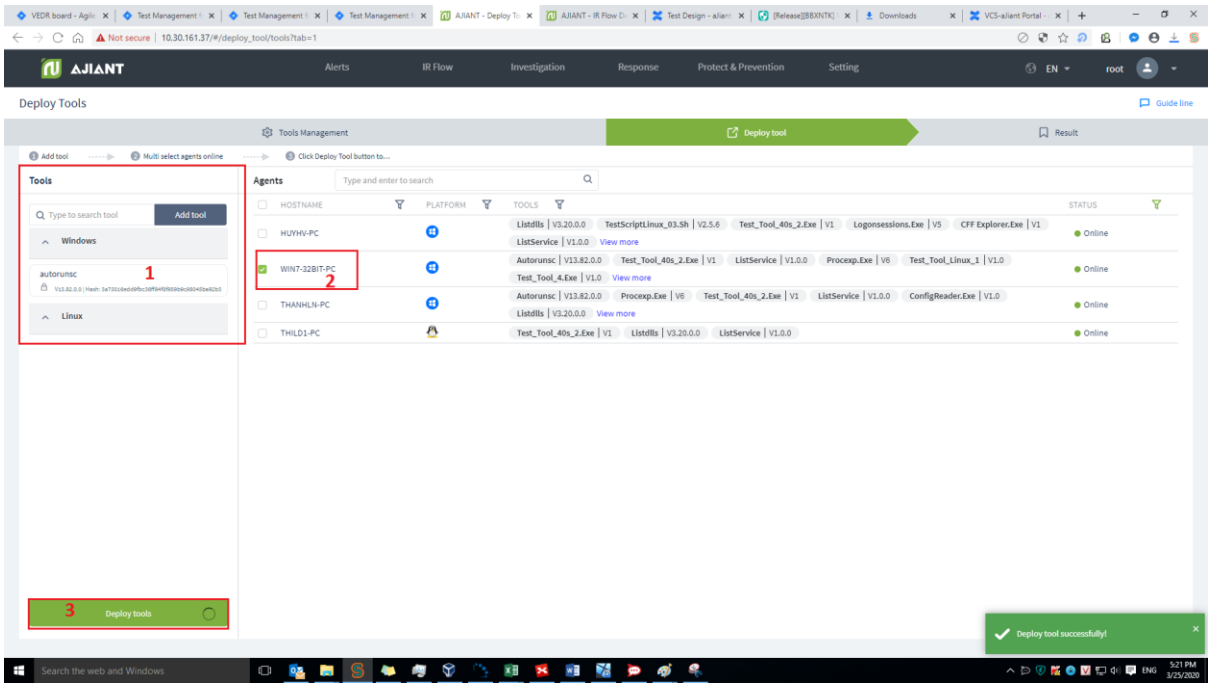
- User login under root group: Display all Agents in active system < 30 days.
- User login under default group: Display all Agents in the default group.
- User login under parent-level group: Display all Agents in the group user logging in and the corresponding child-level group.
- User login under a child-level group or many child-level groups: Display all Agents belonging to the group of the user logging in.

Enable to filter online agents, then search for agents.

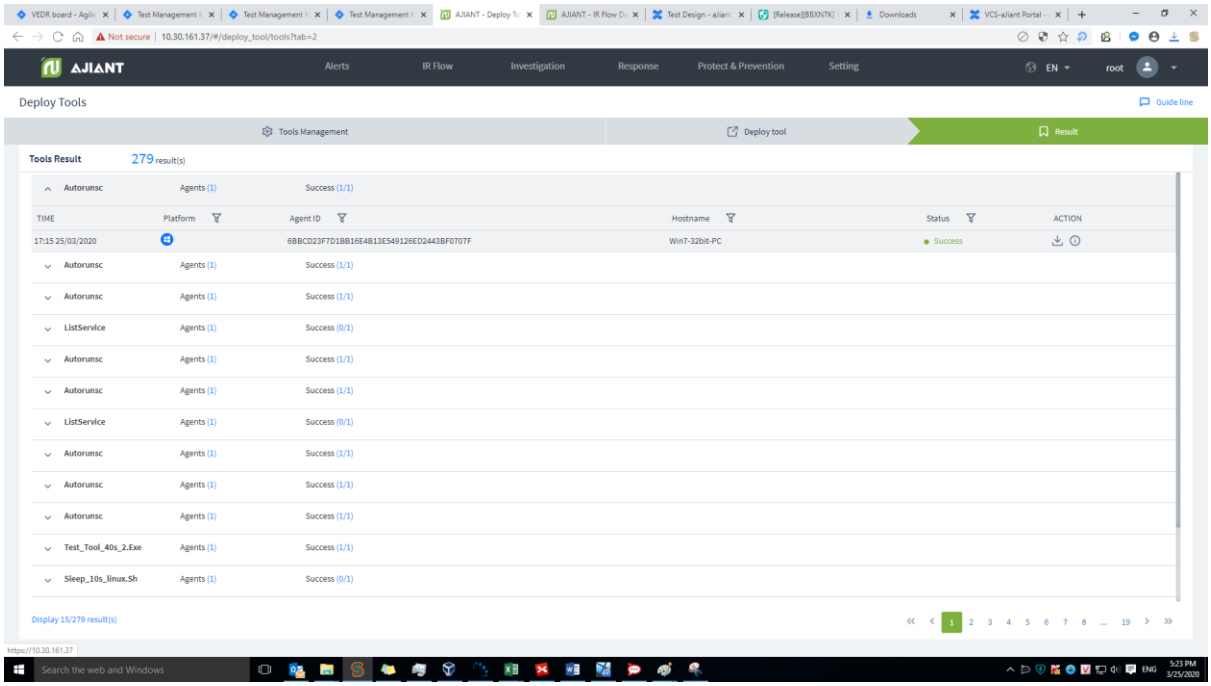
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



After selecting the tool and agent to deploy, check the results on the Result tab. On this screen, the results of running the tool under the agent also can be viewed or downloaded to the local machine similar to IR Flow.



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



7. Response Screen

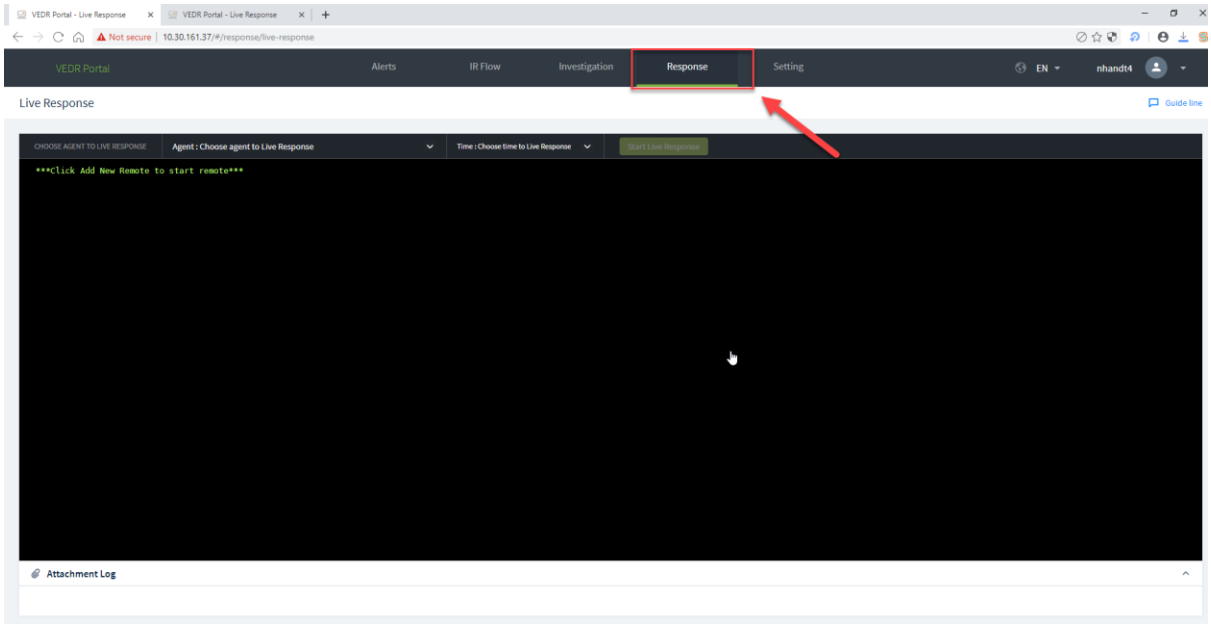
7.1.1. Response Live Response

Purpose: The Live Response function provides the ability to process a set of remote commands according to the working session to provide information or process requests on the host.

Steps to implement Live Response function as follows:

- Step 1: Click the Response tab and select Live Response.

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: Create a new Live Response session

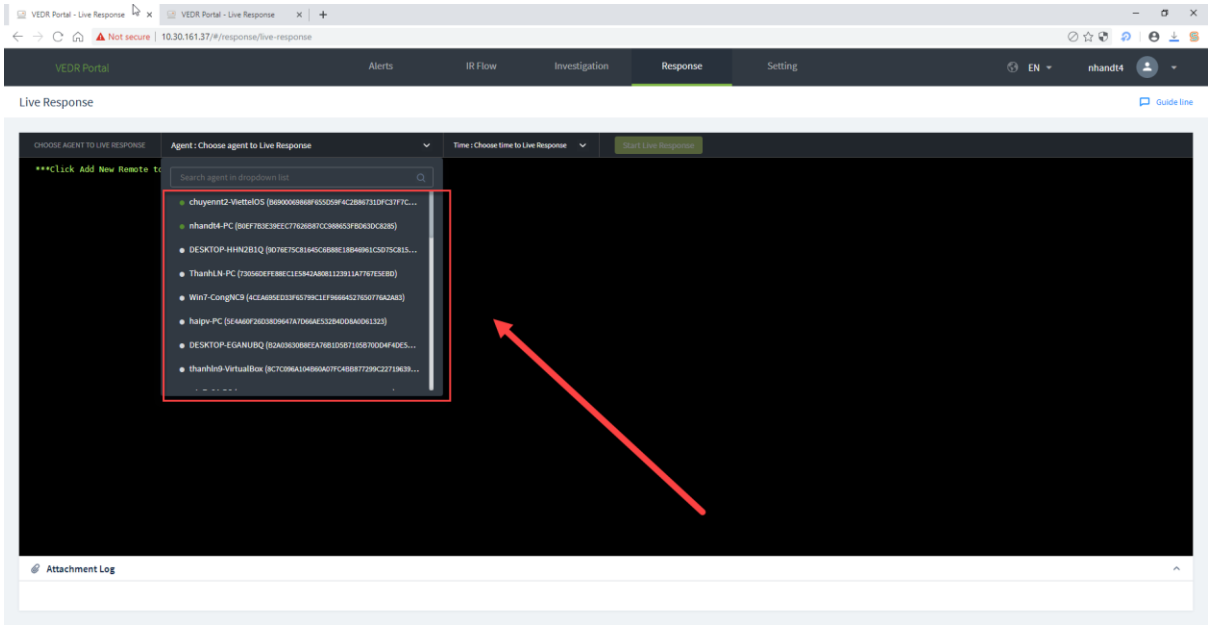
Select Agent: Display the list of agents:

- 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 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.

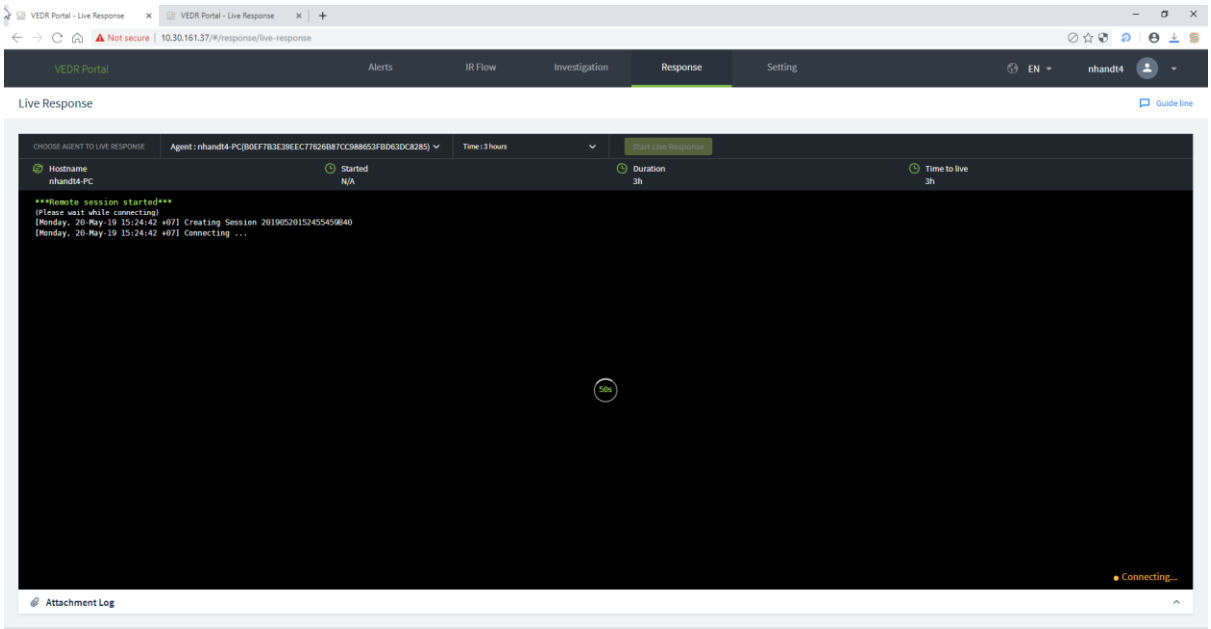
Users can only perform Live Response command with agents that are online ( ).

- Select Time: There are intervals of 5 minutes, 15 minutes, 1 hour and 3 hours.
- Click Start Live Response button.

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



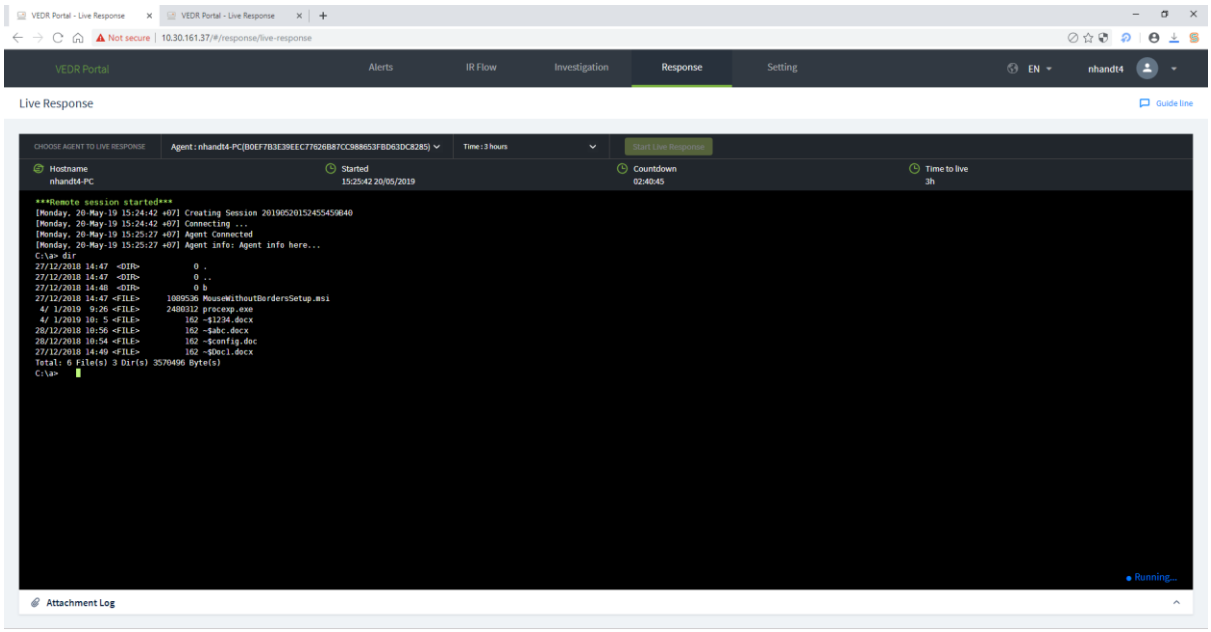
- Step 3: Wait for 1 minute for the system to connect to the agent, the system state is Connecting.



- Step 4: When the connection is successful, the user is allowed to execute commands at the console screen and the state of the Live Response session is Running.

Notes: Each agent at a time has only 1 working session of Live Response.

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



Users can execute commands at the console screen as follows:

No.	Commands	Parameters	Description
1	cd	cd <dirpath>	Change current working folder
2		cd.. or cd ..	Switch back to parent-level folder
3	pwd		Print current working folder
4	dir		List files/sub-level folders in the current folder
5	delete	delete -file <path> For example: delete -file "c:\temp\run path.exe"	Delete 1 file
		delete -folder <folderpath> For example: delete -folder temp\axvers	Delete 1 folder

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 -all <folderpath> For example: delete -all c:\temp	Delete all files/sub-folders in the folder (but do not delete the folder)
6	viewfile	<filepath><sizeinbytes>	Display data in file (file size limit)
7	get	<filepath>	Upload 1 file from host to server
8	put	<url><folderpath>	Download 1 file to host machine
9	mkdir	<dir name>	Create 1 folder
10	reg		Commands related to Registry
		query <keyname> -v <valuename> For example: reg -query "HKLM\Software\abc xyz" -v "run path"	Query the value data of a key
		query <keyname> -s For example: reg -query "HKLM\Software\abc xyz" -s	Query all sub keys, values and data
		add <keyname> For example: reg -add "HKLM\software\abc xyz"	Add 1 key
		add <keyname> -v <valuename> -t <type> -d <data> For example: reg -add "HKLM\software\abc xyz" -v	Add 1 value

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

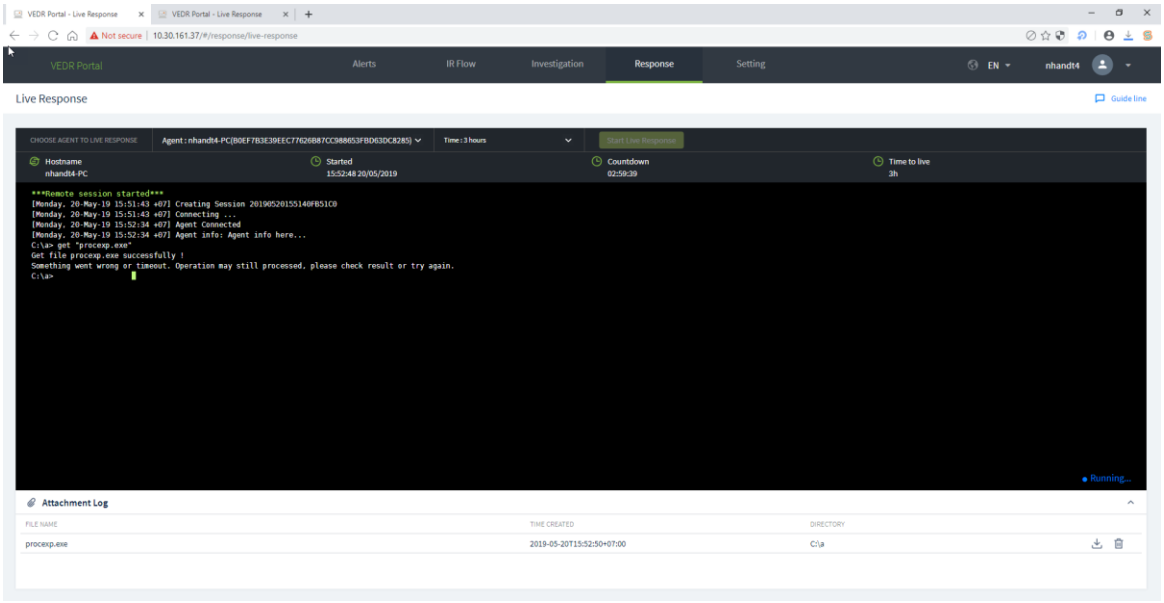
		"run path" -t REG_SZ -d "c:\temp\bin.exe"	
		delete <keyname> For example: reg -delete HKU\S-1-5-21-3791698801-2327923109-636705026-2080\Software\Test	Delete 1 key and all sub keys and value
		delete <keyname> -v <valuename>	Delete 1 key value
		import <filename>	Import 1 file .reg
		export <keyname> <filename>	Export 1 file .reg
11	process		Commands related to process
		-t <processid>	Turn off a running process by process ID
		-s <processid>	Pause a process
		-r <processid>	Recover a previously paused process
		-l -a	List all processes of all users
		-l -u <username>	List all processes of an user
12	service		Commands related to service
		-query	List the services running on the host machine
		-start <servicename>	Start 1 service
		-stop <servicename>	Stop 1 service

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

13	user	-list	List the users on the machine
		-sid<username>	Get sid of username
14	cls		Delete the console screen
15	help		Help command

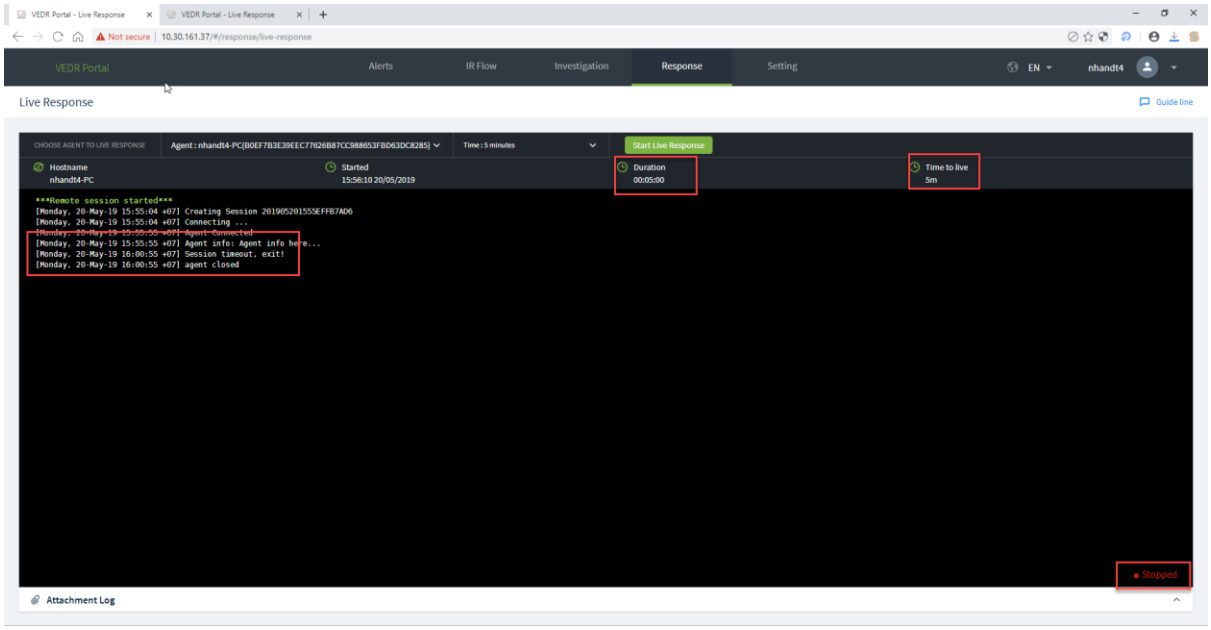
Some notes when working with commands on the console screen as follows:

- Clear command: After executing the Clear command, the system will support the user to download the entire log made on the previous console screen, by clicking on the here link.
- Get <filepath> command: For example, get procexp.exe in the console screen, the result of getting the file is displayed in the Attachment Log screen at the bottom right corner of the screen. Users are allowed to download files to the browser or delete the downloaded files to the server.

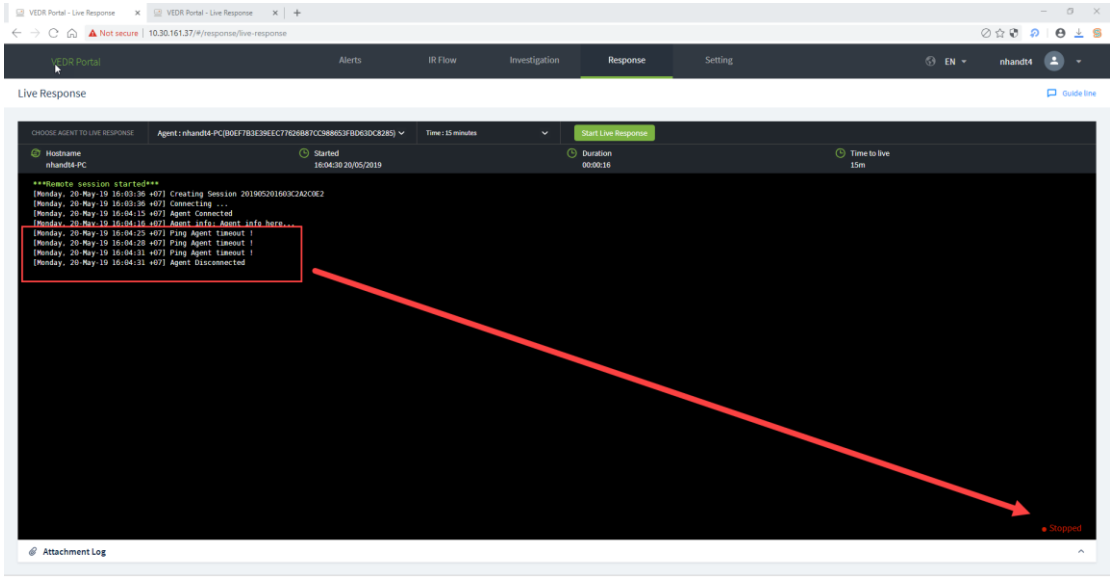


- Step 6: The Live Response session ends when:
  - Time of session expires: When the time of Duration field is equal to the time of the Time to Live field.

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 user actively requests to close the connection with the Close command.
- When the connection with the agent is lost, the server performs ping/pong failed more than 3 times.



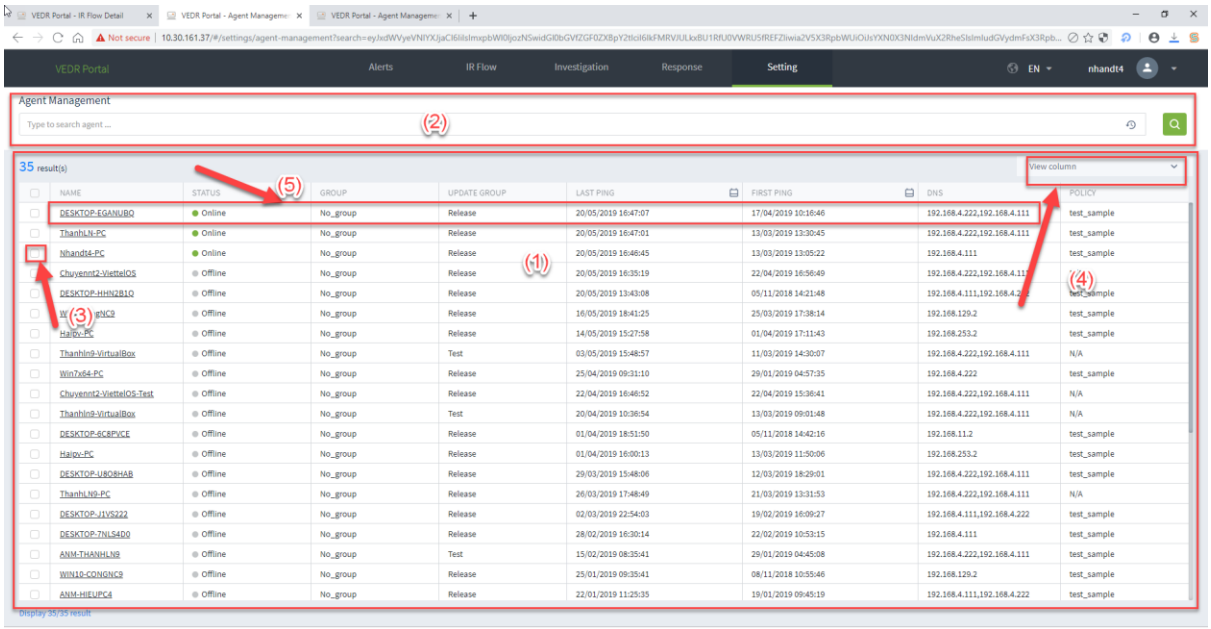
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

8. Setting Screen

8.1.1. 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).



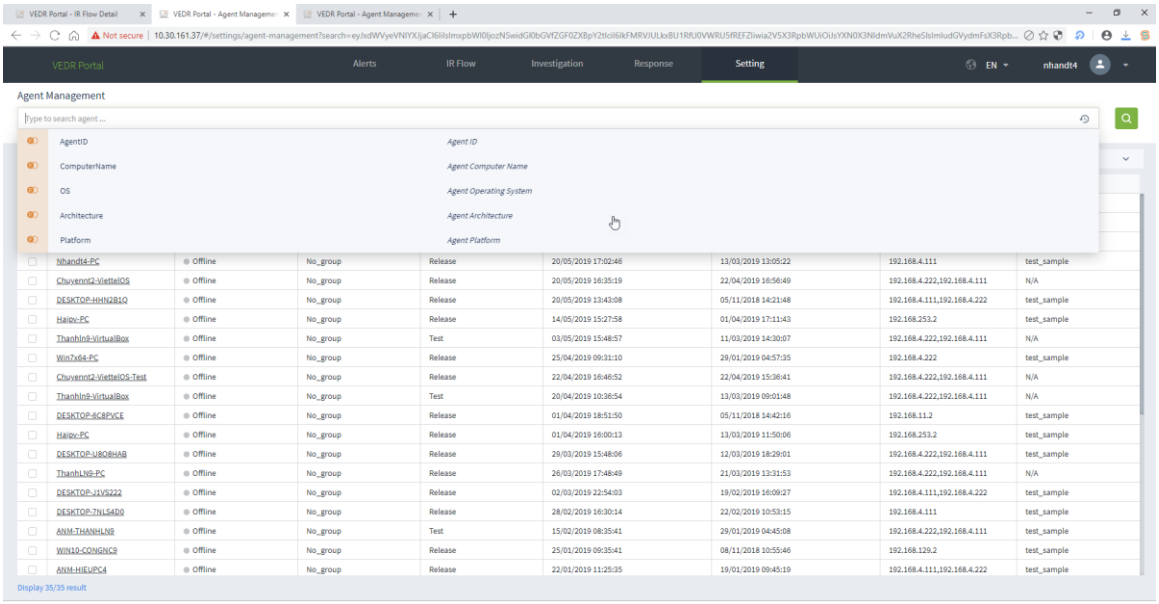
The system support performing the following features:

(1) 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 user 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 user.
- Each agent is displayed general information, including: Name, State, Group, Update Group, Last Ping, First Ping, DNS, Policy, AgentID, Platform, Platform Version, Architecture, DNS and Version.

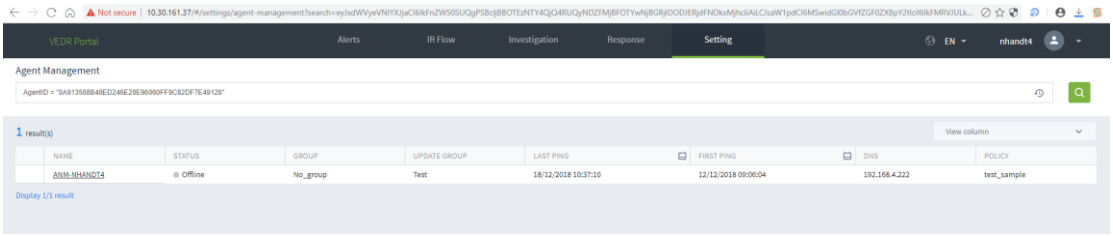
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

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

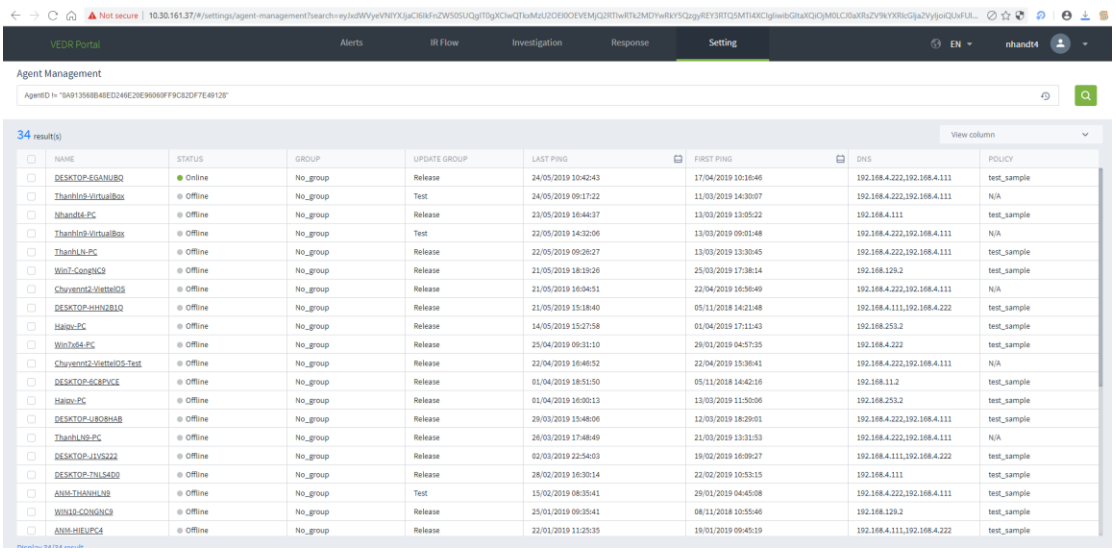


Examples of search statements as follows:

Search by the condition “=”:

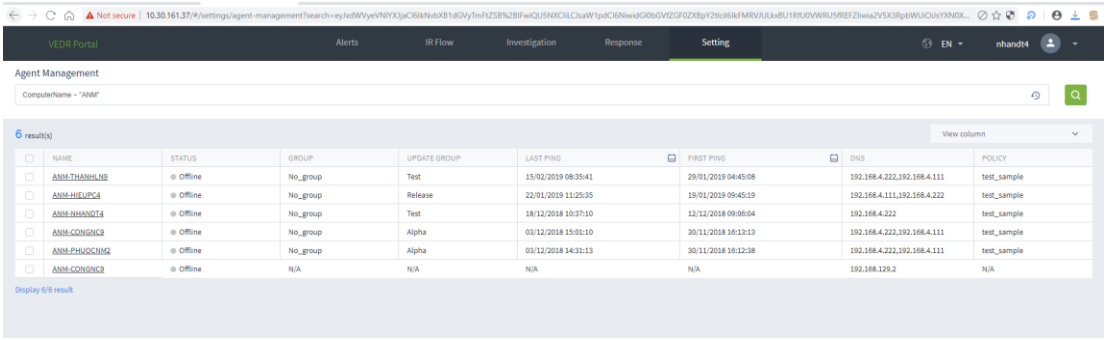


Search by the condition “!=”:

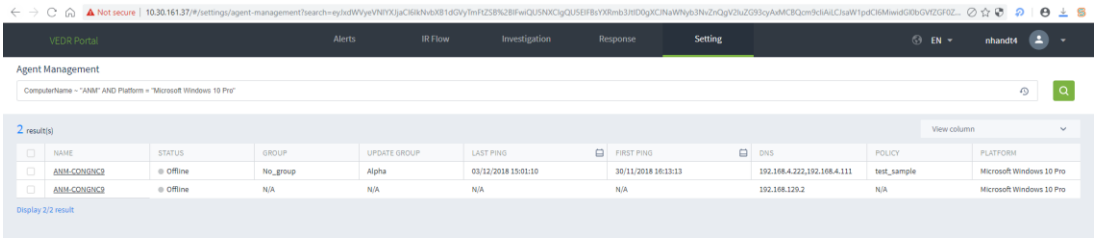


Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

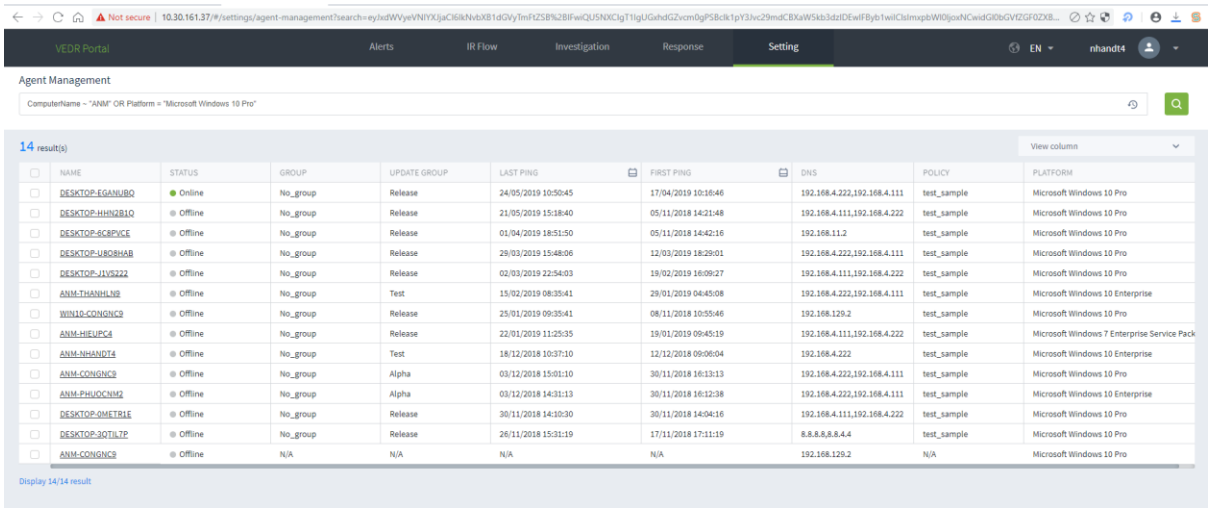
Search by the condition "~":



Search by AND match criteria:

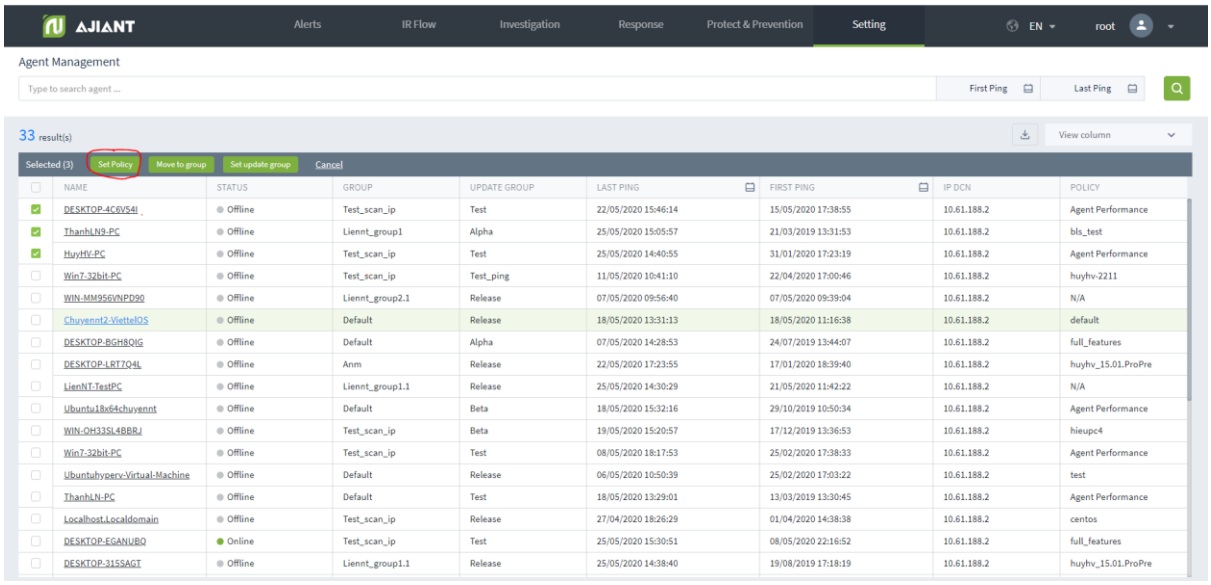


Search by OR match criteria:

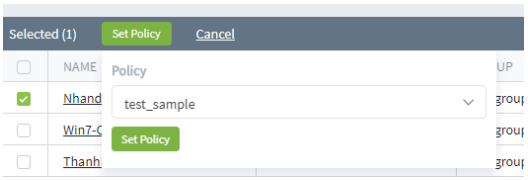


(3) Quickly select 1 agent/ 1 group of agents to set policy as follows:

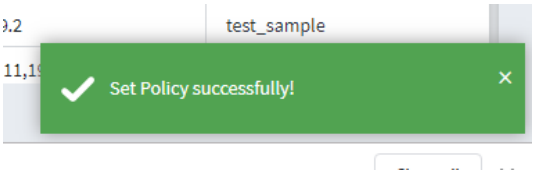
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



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



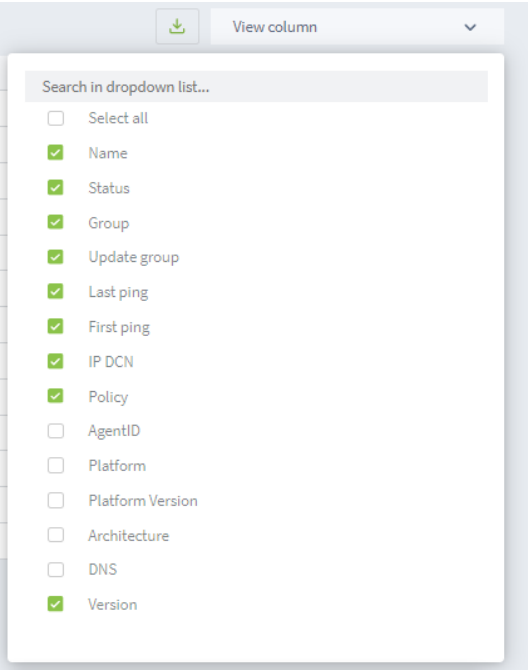
- Result after setting policy:



- Delete the action on the Multi-selected screen

(4) View Column: Configure the display of columns at will:

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



(5) View details of an agent by clicking duplicate the mouse on any row

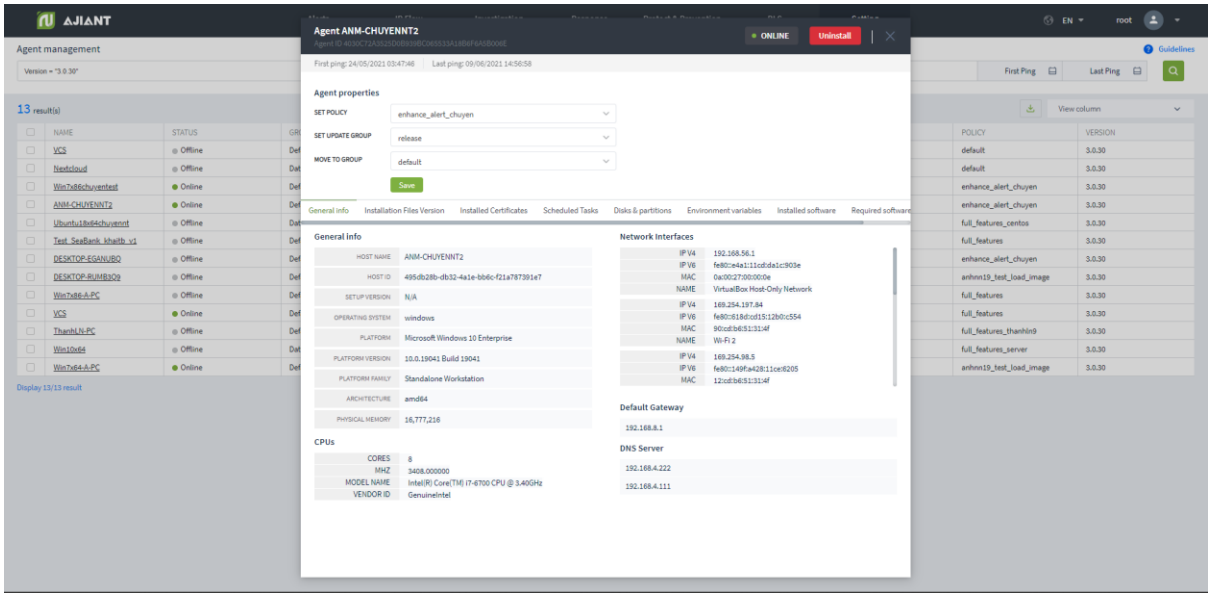
The system supports users to perform Set Policy, Update Group and Move to group for Agent quickly.

- 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.

- General Info Tab

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

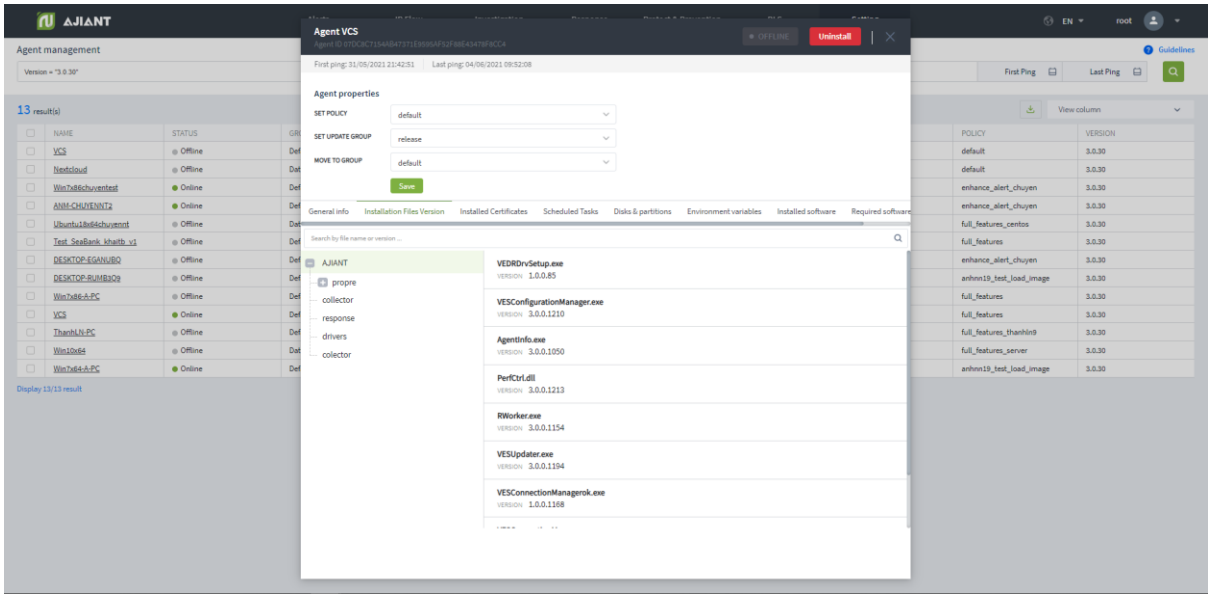
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Installation Files Version Tab

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

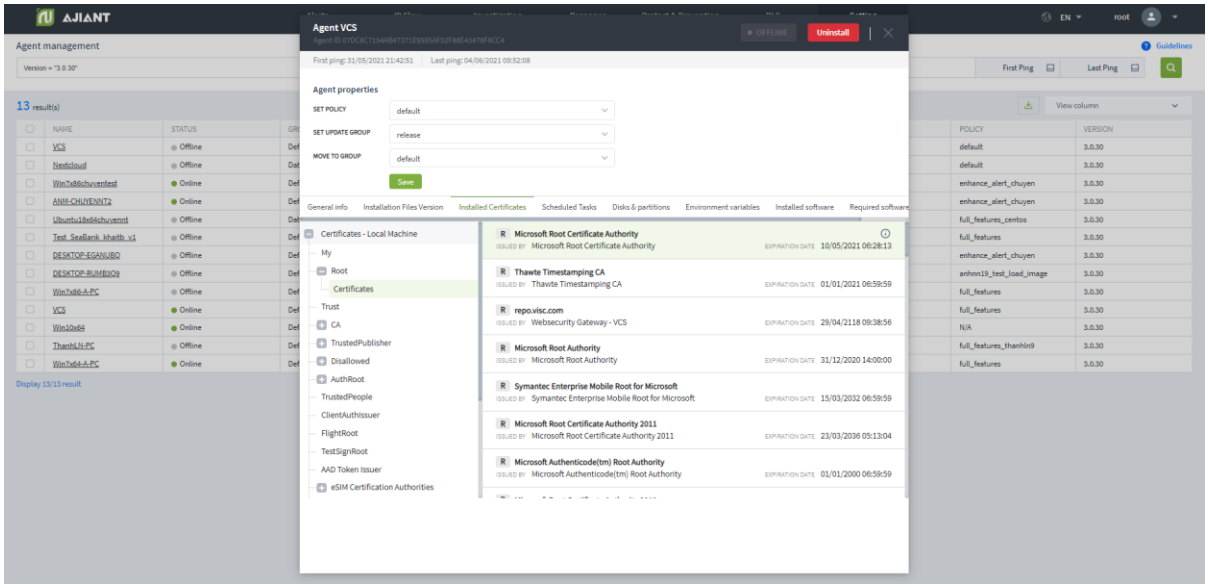
Support quick search by File name, Version in search text box.



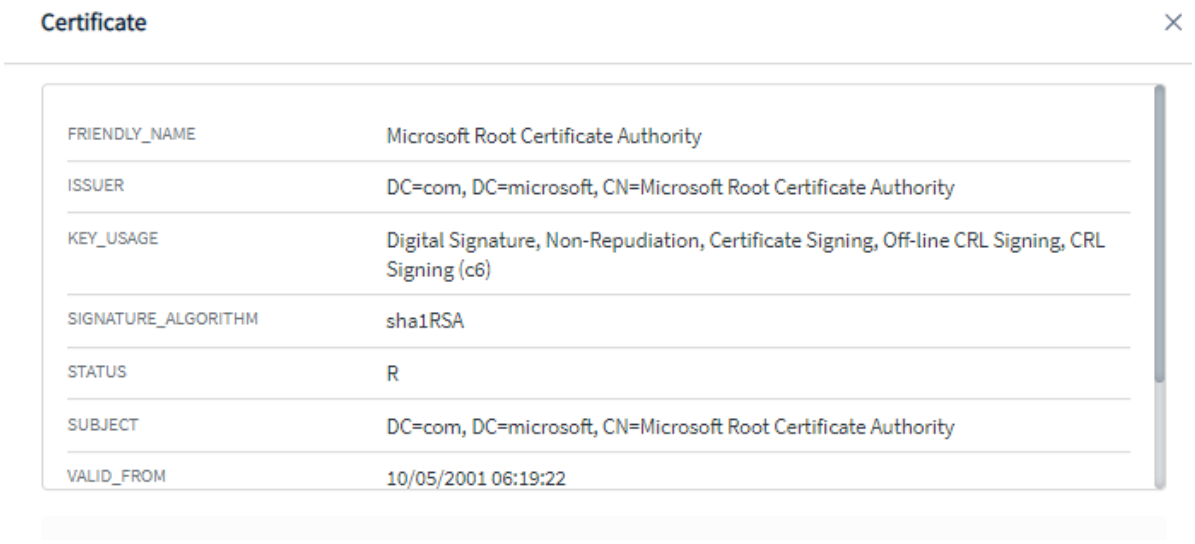
- Installed Certificates Tab

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 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



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

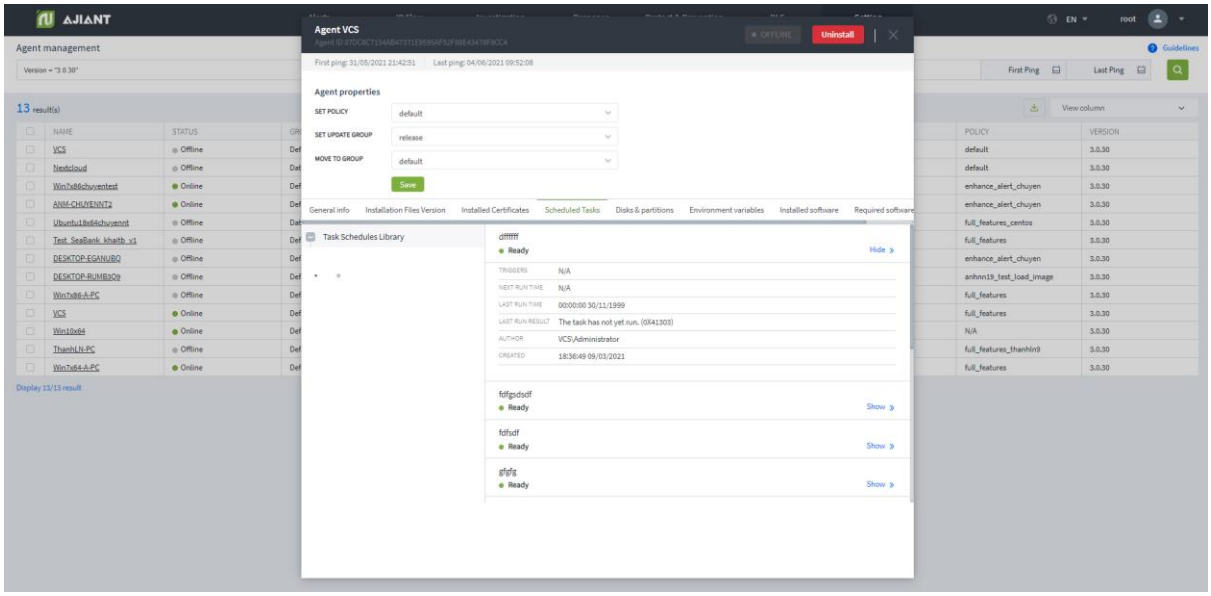


- Scheduled Tasks Tab

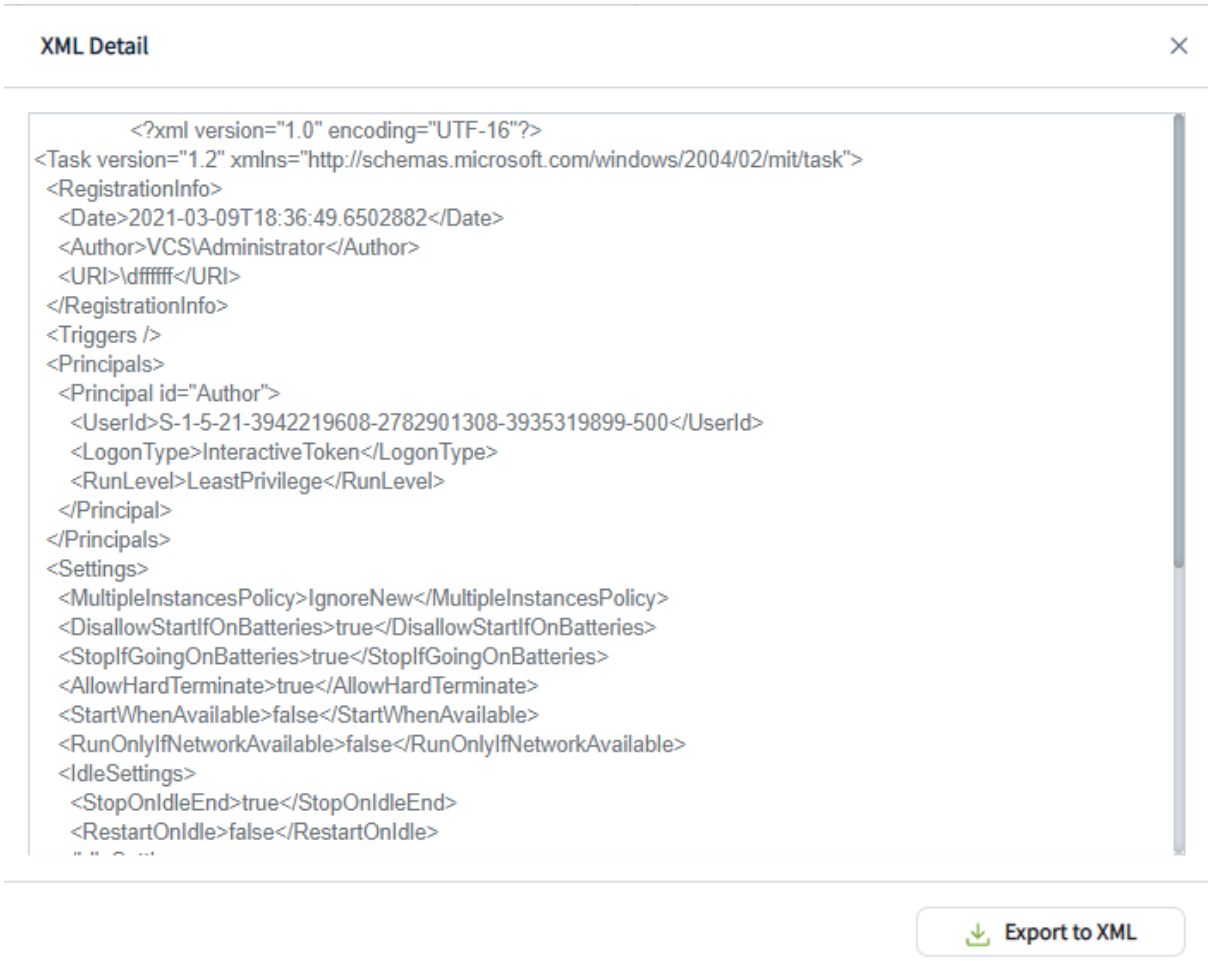
Statistics of all scheduled tasks on the agent installed machine, including information: List of scheduled tasks, Name, State, Trigger, Next time run, Last time run, Author and Created.

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

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



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



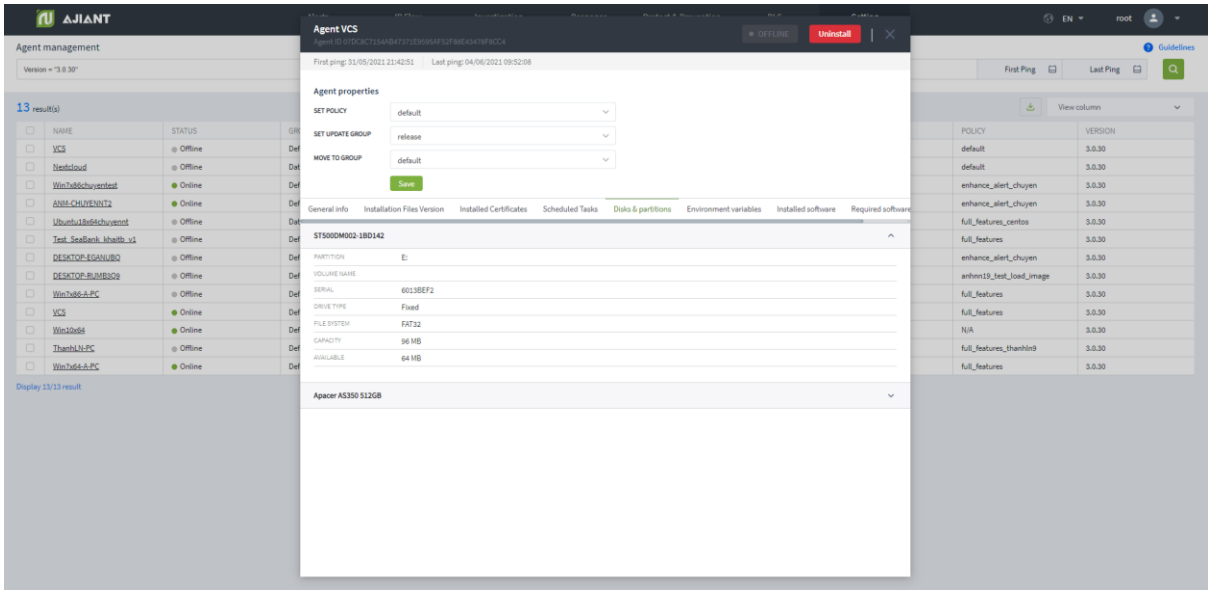
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- Select Export to XML 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 Disks, Partition, Volume name, Serial, Drive type, File system, Capacity and Available.

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

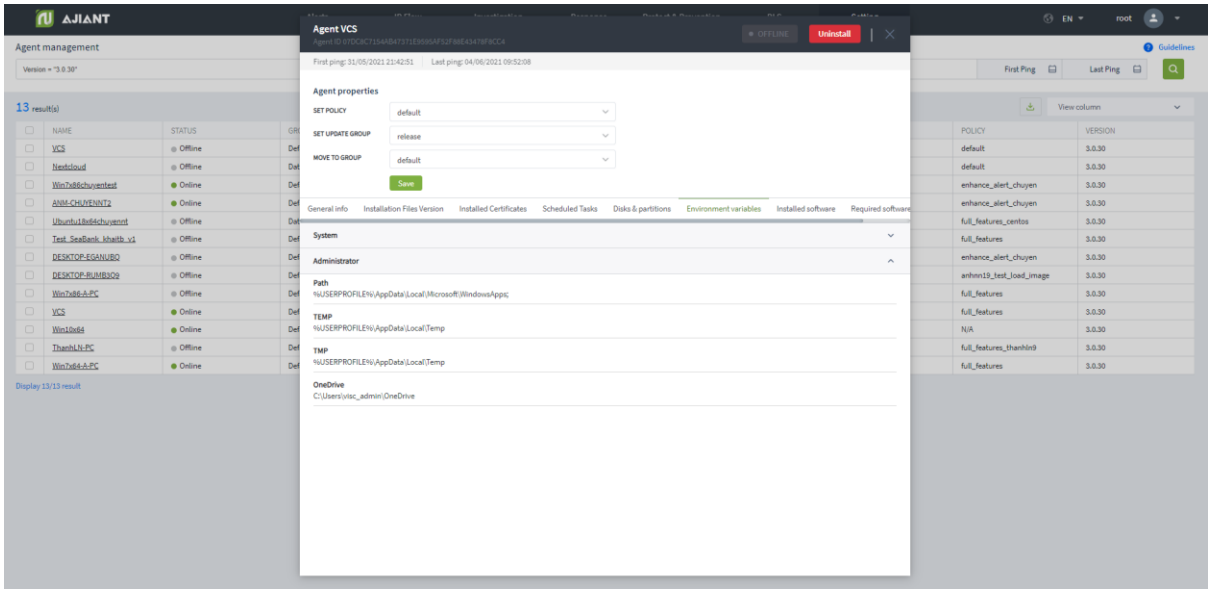


- Environment Variables Tab

Statistics of all environment variables on the machine where the agent is installed, 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.

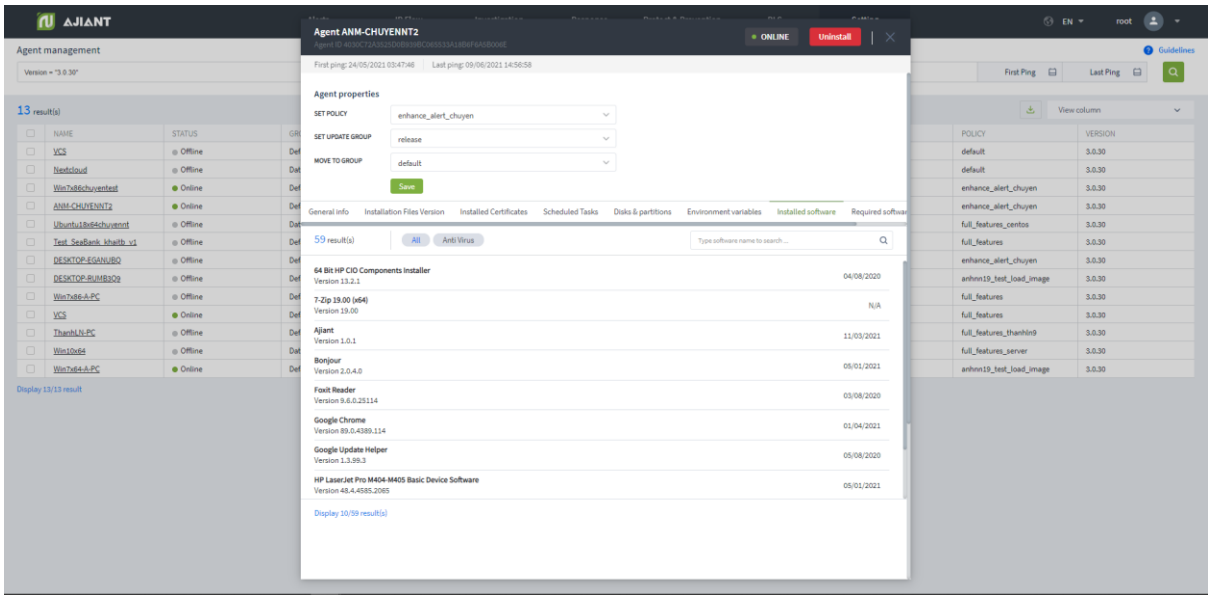
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Installed Software Tab

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

  - Support quick search for installed Antivirus software or enter the software name in the search text box.

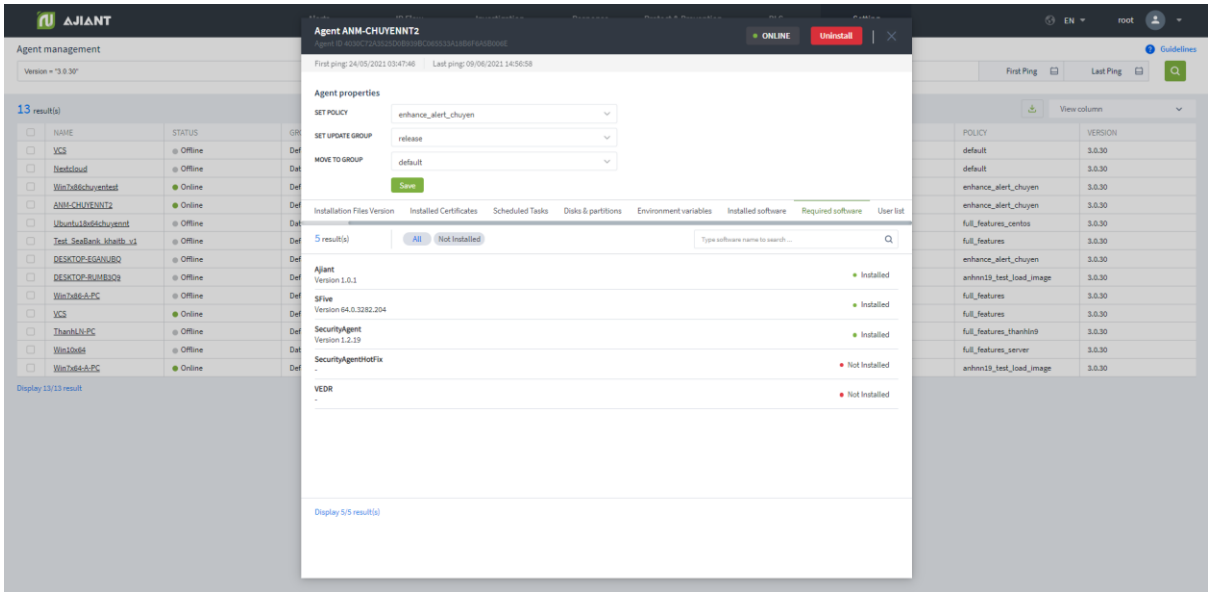


- Required Software Tab

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

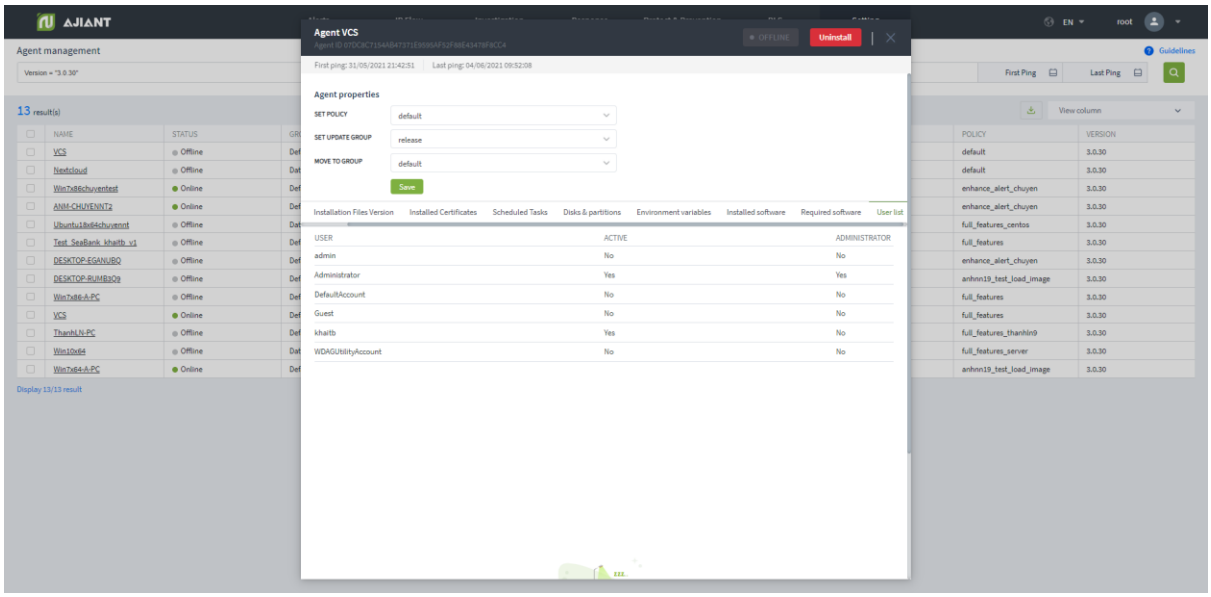
  - Support quick search for required software that is not installed on the machine or enter the name of the software in the search text box.

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

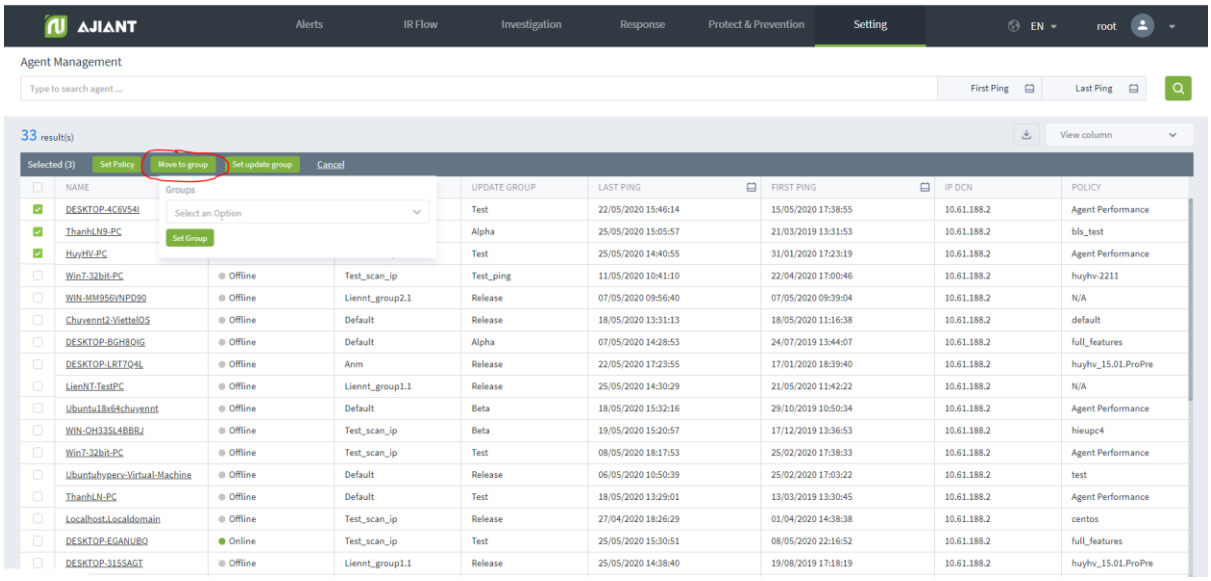
Statistics of all logged in users in the agent, including information: Username, active and administrator.



(6) 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

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



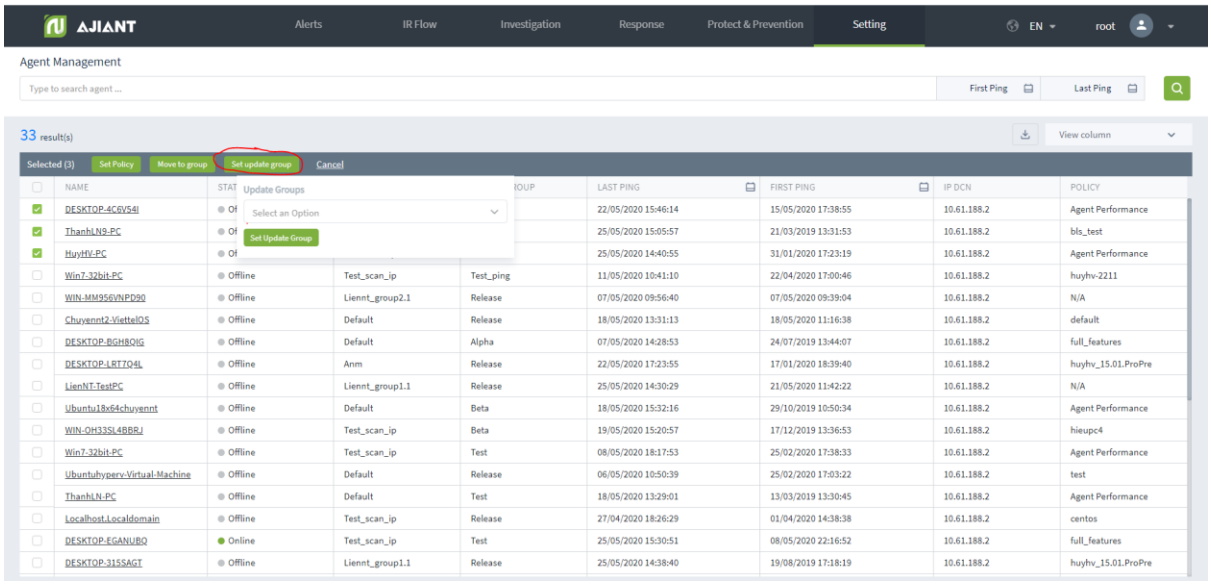
- Perform Move to group

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.

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



- Perform Set update group.

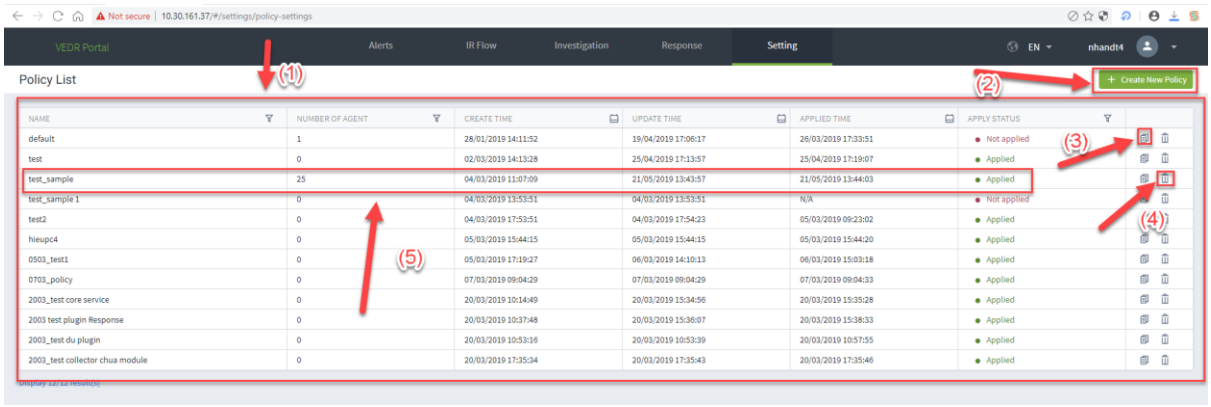
Notes:

- 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.

8.1.2. Policy Setting

Purpose: Support users to manage the list of policies set up for Agents.

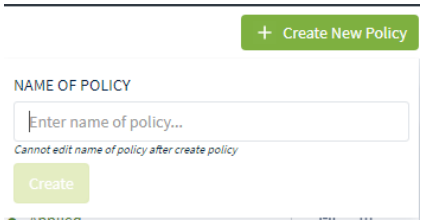
Interface screen when users access Setting >> Policy Setting as follows:



(1) Display the list of Policies that have been created on the system. Each Policy includes the following information: name, number of Agents to which the Policy is applied, creation time, update time, time of Policy application and state (there are 2 states: Applied and Not Applied).

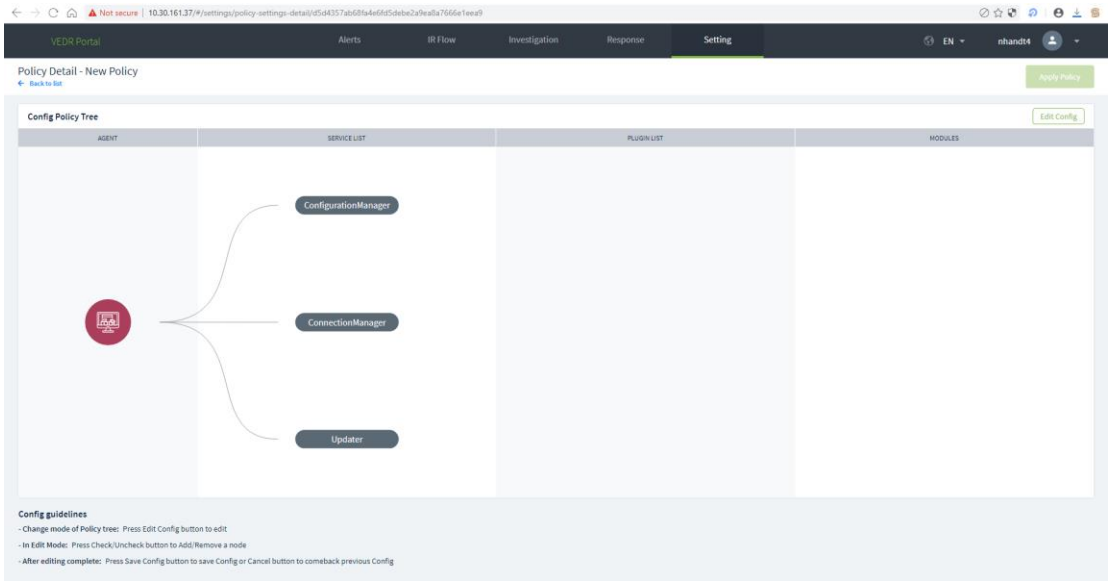
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

(2) Create a new Policy: Click on the + Create New Policy button, the system displays a popup to create a new Policy as follows:



Notes: When creating a new Policy, the Policy name cannot be the same as previously created Policy.

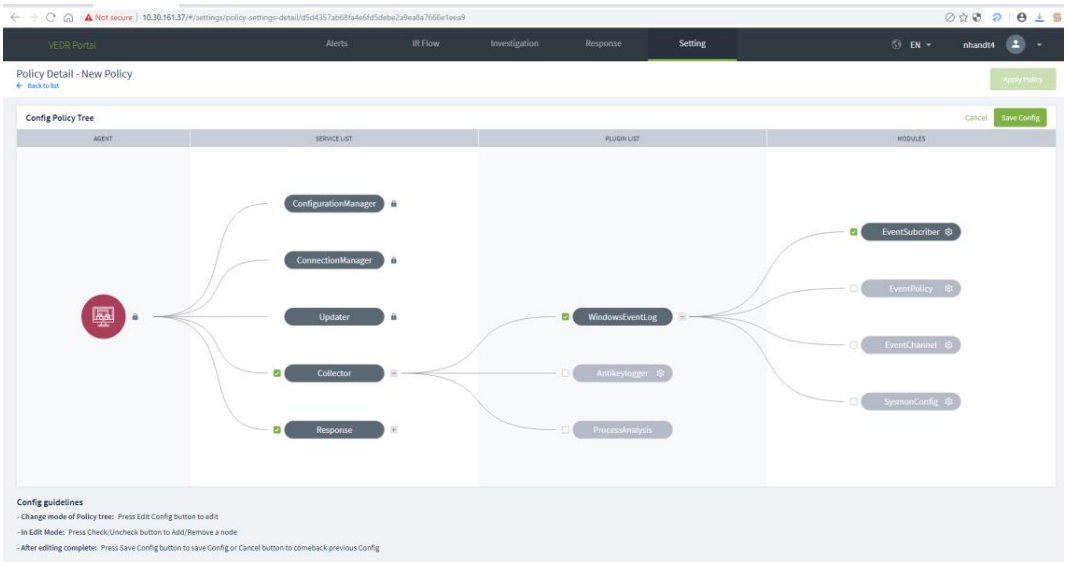
After creating a new Policy successfully, the system will display a detailed screen of a Policy as follows:



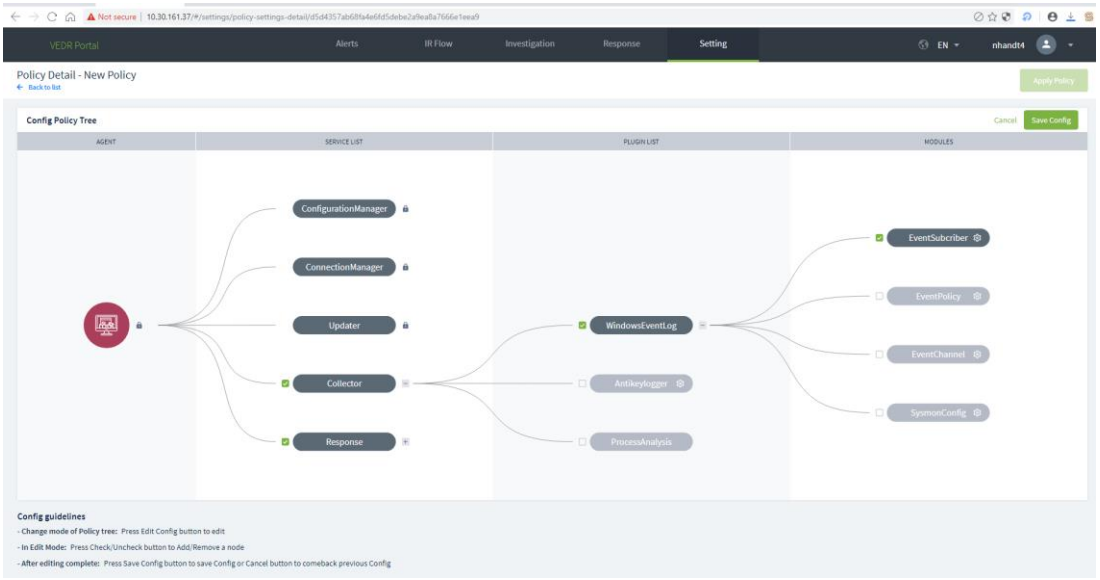
Each created Policy usually has 3 default core services, including: ConfigurationManager, ConnectionManager and Updater. Note that these 3 services are not allowed to be deleted from the system. Steps to configure a Policy as follows:

- Step 1: Click the Edit Config button to change the Policy tree.
- Step 2: When in Edit mode, users are allowed to Check/Uncheck to Add/Remote other services.

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: After completing the Edit mode: Users click the Save config button to save the changes or click the Cancel button to return to the previous configuration.



- Step 4: Click the  icon to perform detailed configuration for each Module/Plugin of the Services.
  - WindowsEventLog: Configure the log sources obtained under Agent.
  - EventSubscriber: Specify channels to get log.

Data request:

  - Event_filter field (filter by Event ID): Substrings separated by comma (,)

For example:

“4”: filter events with EventID = 4

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

"-689": filter events with EventID #689

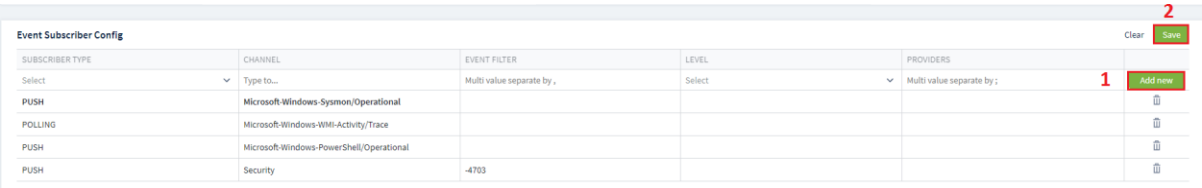
- Providers field: Substrings separated by semicolons (;)
- Fields require to have subs_type and channel.
- Channel: A log source
- Sub_type:

PUSH: When there is a new event → call the function of VCS-aJiant to handle it.

POLLING: VCS-aJiant after a time period of actively taking the log.

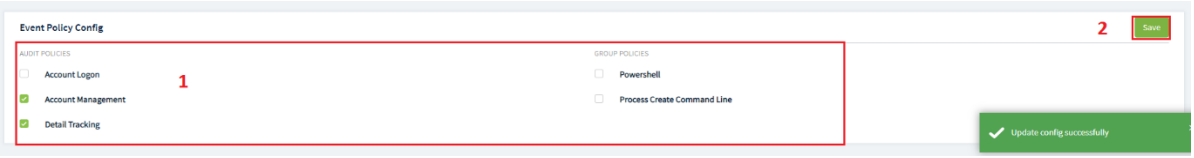
PULL: VCS-aJiant actively takes the log after a time.

After the configuration is complete, it is required to be saved.



- EventPolicy: Set Policy to enable/disable some log types that the system does not have by default.

Requirement: At least 1 field selected.



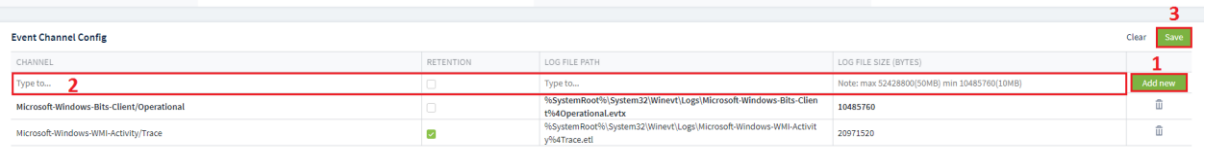
- EventChannel: Detailed configuration of some log sources as follows:

Retention: Whether to save the log rotation or not (If the Retention is selected, when the log file is full, the new log will overwrite the oldest log.)

Log file path: A log file path

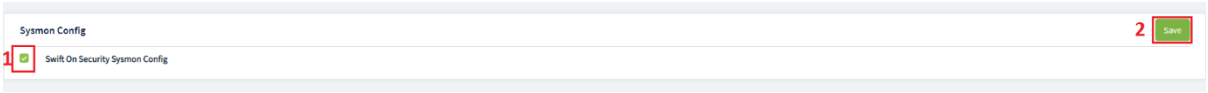
Log file size: A log file size

Requirements: All data must be filled in.



- SysmonConfig: Enable/disable sysmon tool on Agent to get a sysmon log: Microsoft-Windows-Sysmon/Operational

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



- Antikeylogger: Be as a SelfRun Plugin of VCS-aJiant, has the task that periodically scans the entire machine to find out the KeyLogger running on the machine if any.
- Scan settings: Configure the types of KeyLogger to scan

Requirements:

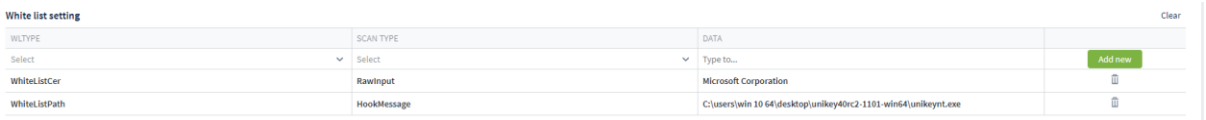
Scan cycle: Min is 1 minute and max is 180 minutes.

Choose at least 1 type of KeyLogger

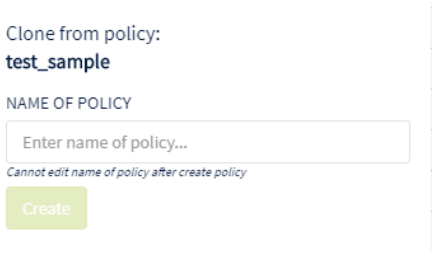
- Whitelist setting: Configure the whitelist of some software according to the file path on the drive or according to the digital signature (cert) of the file running the KeyLogger.

Requirement: Fill out all fields.

After entering, the configuration is required to be saved.

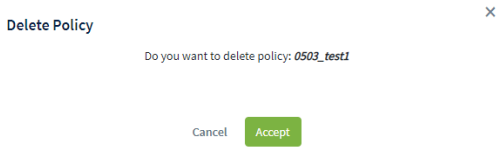


- Step 5: Click the Apply Policy button to set the newly configured Policy for Agent.
  - Clone new Policy: Click the button, the system copies all details of the cloned Policy, except for the Policy name.

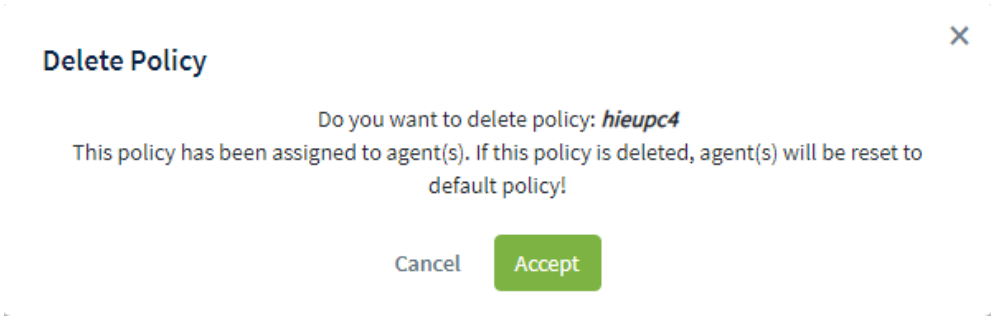


  - Delete Policy: Click on the button, the system displays a popup for the user to make a decision whether to delete Policy or not.

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 Policy already has an applied agent, after deleting it, the system automatically assigns default policy to that agent.



- When clicking duplicate on each record, the system will forward to the detail page of a Policy for users to view/change the configuration for the Policy.

8.1.3. 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.

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.

8.1.3.1. Manage groups by tree

- User login under root group: Display all groups 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

- 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.

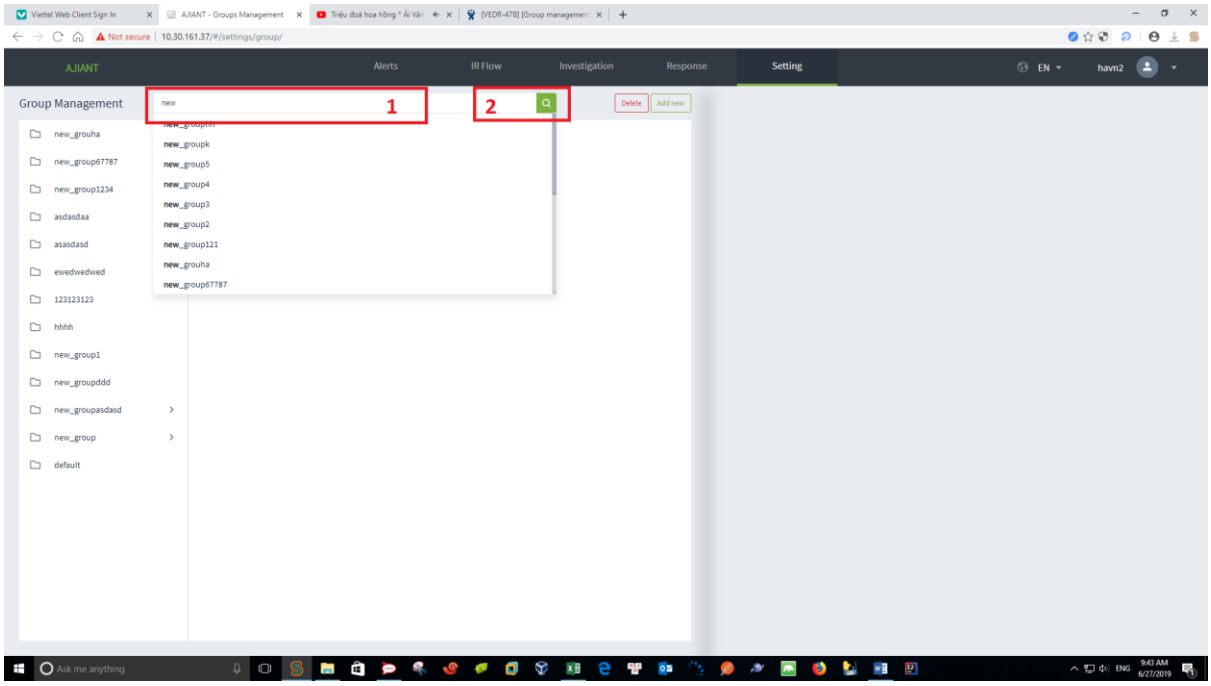
When the user belongs to a child-level group, if selecting a parent-level group, the group detail popup will not be seen.

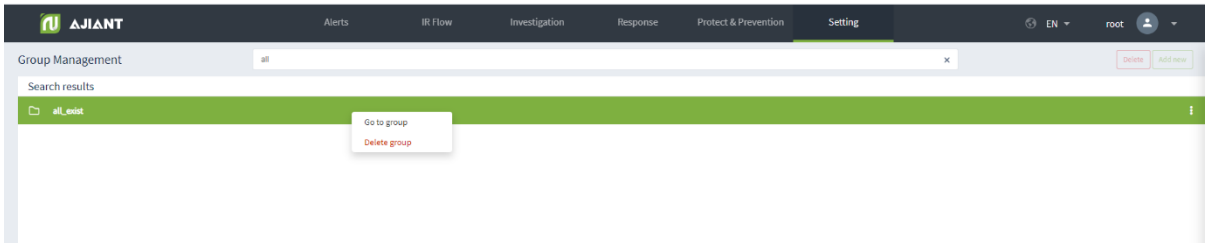
8.1.3.2. Search group

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.

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





- 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.
  - 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.

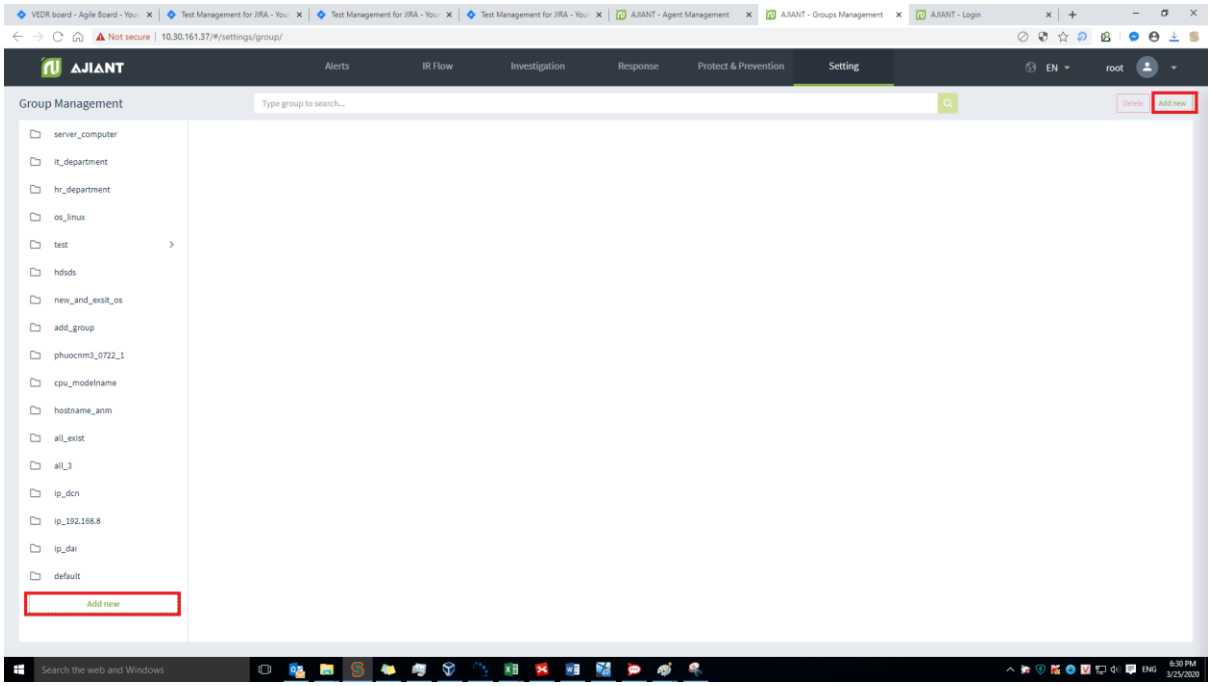
8.1.3.3. Add a new group

- User login under root group: Enable to add all new groups.

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

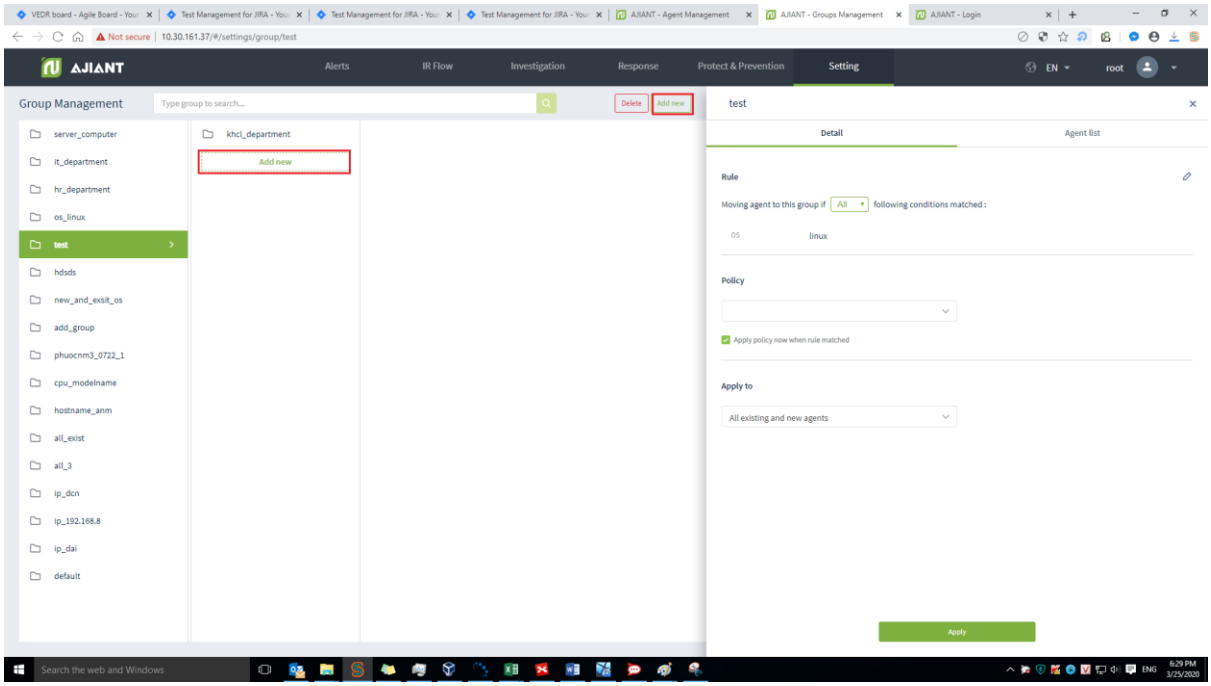
- User login under default group: Unable to add a new group.
- User login under parent-level group: Enable to add a new corresponding child-level group of the group belonging to the user logging in.
- User login under a child-level group or many child-level groups: Enable to add a new corresponding child-level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



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.

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

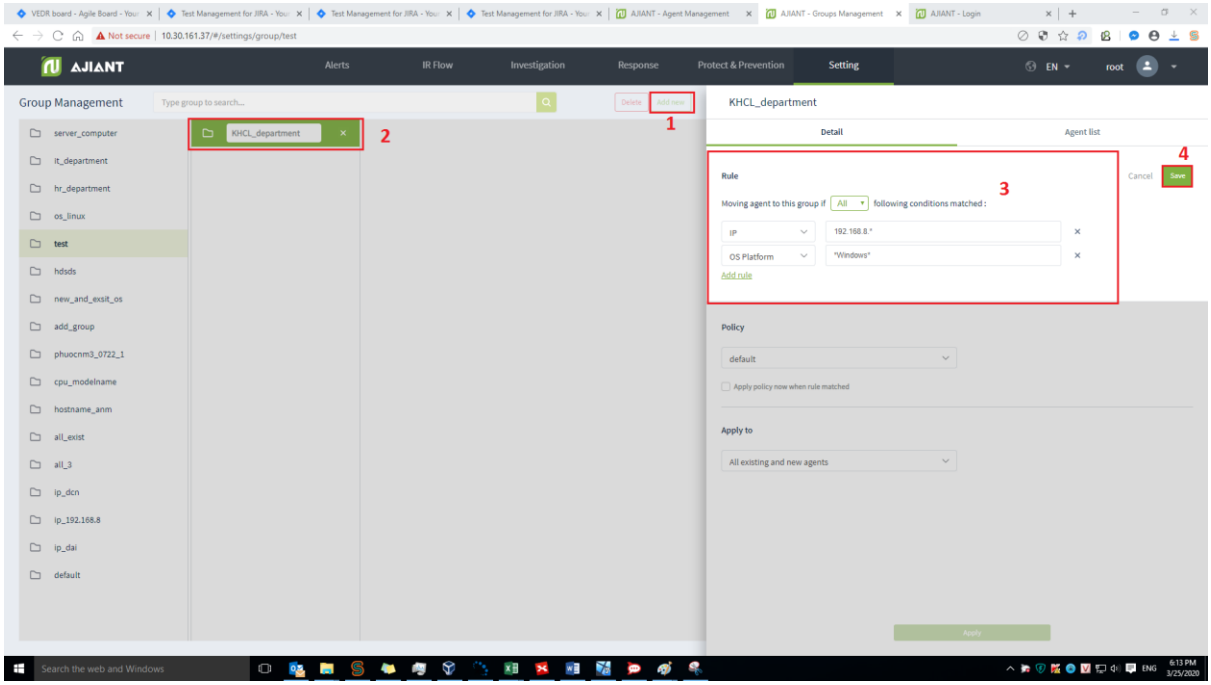


- Step 2: Enter the group name and configure the rule.

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

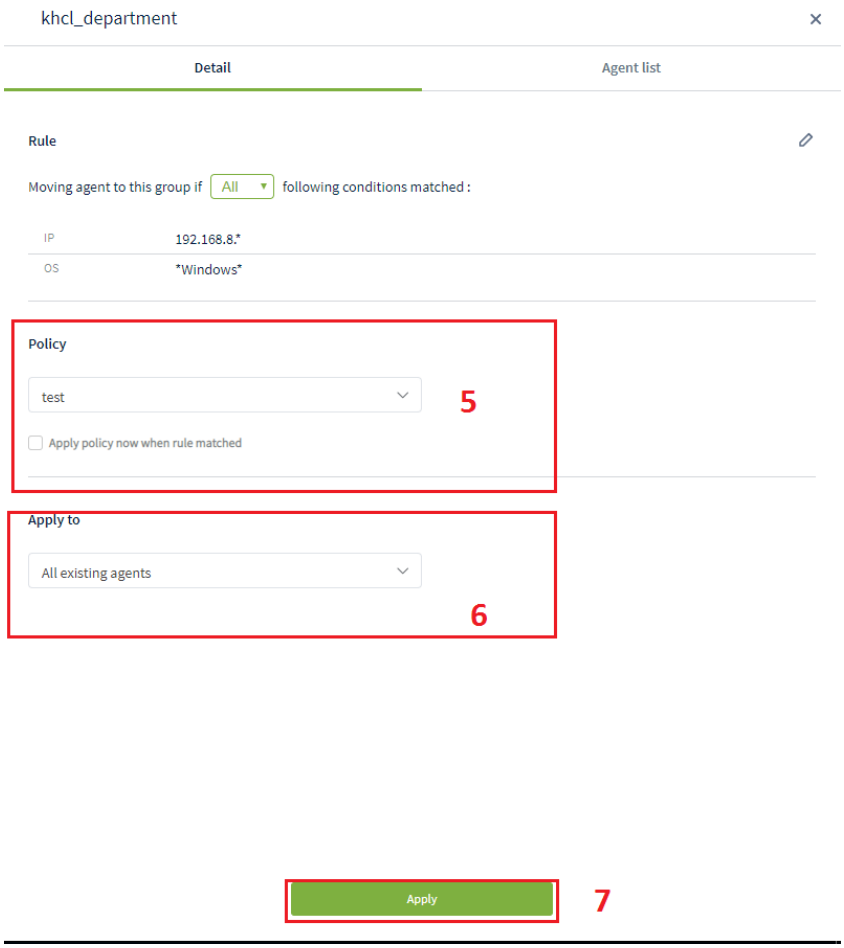
If the All operator is selected: The rule is satisfied when both fields are satisfied.

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.



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:

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

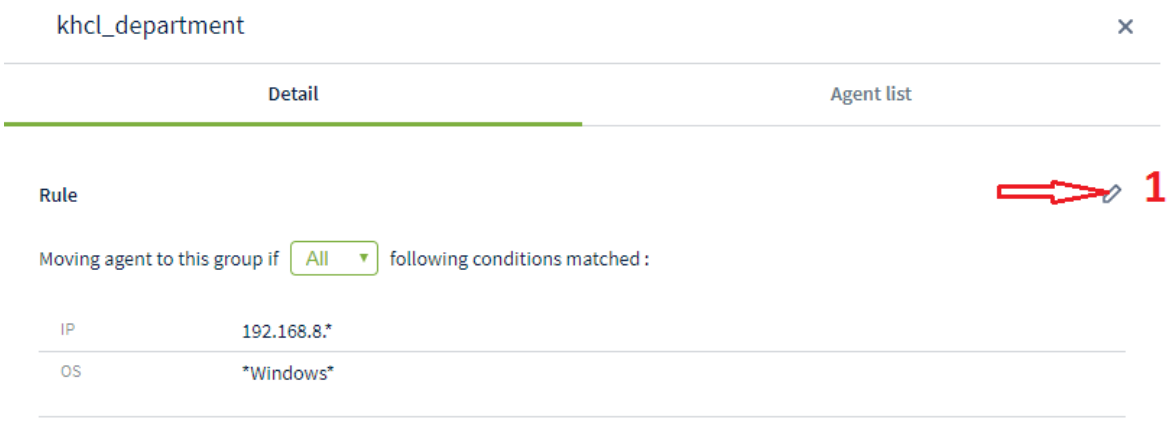
- If select the Apply policy now when rule matched checkbox, and click Apply, those selected agents will be checked the values. If they match the configured rule, they will switch the policy for the agent to the selected policy at the Policy section, and switch groups.
- In case the above checkbox is 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.

8.1.3.4. Edit group

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

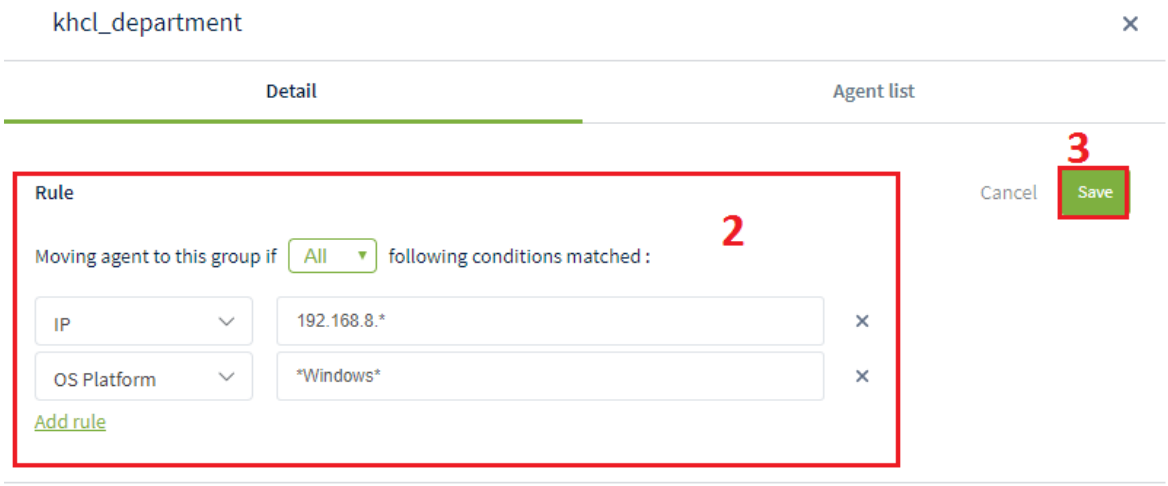
- User login under root group: Enable to edit all groups in the system.
- User login under default group: Unable to edit the default group.
- User login under parent-level group: Enable to edit all groups belonging to the user logging in/ and the child-level group whose role is also in the child-level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

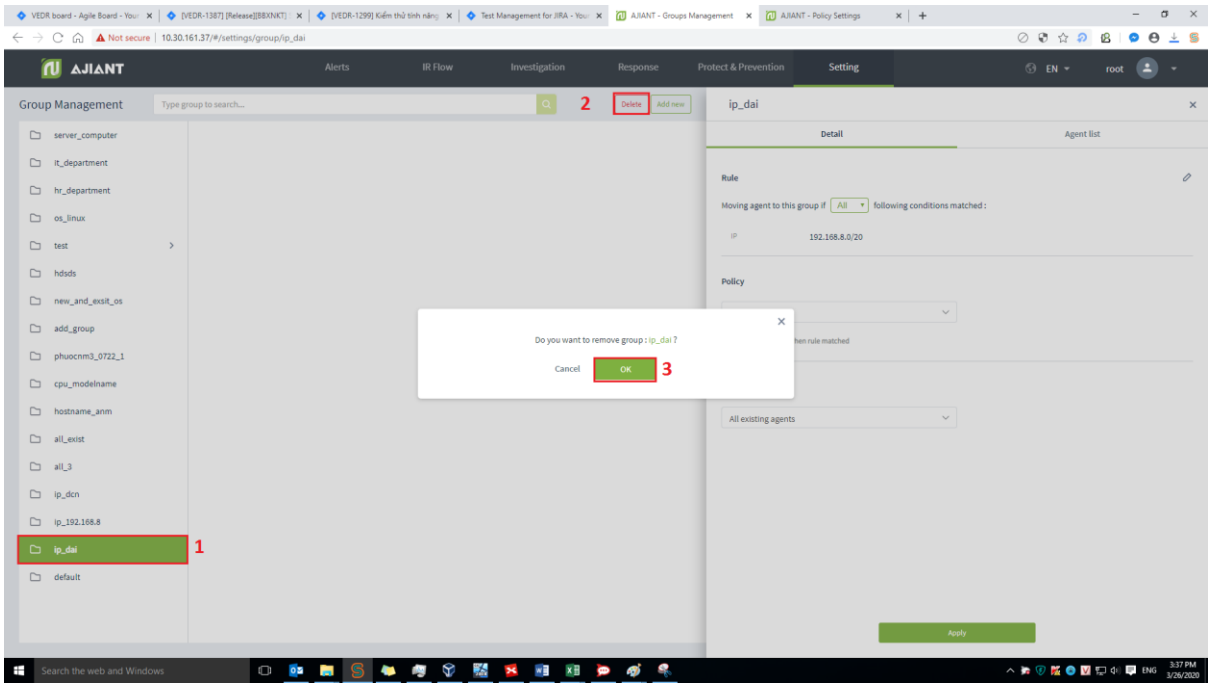
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

8.1.3.5. 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.

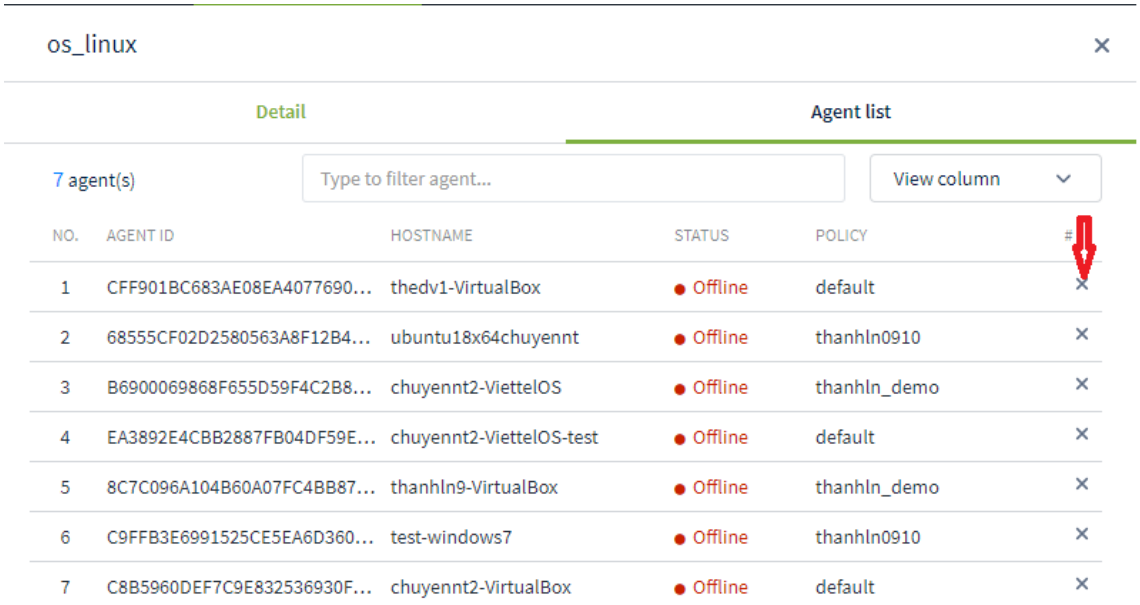
After deleting a group, the agents belonging to the group will be switched to the default group, while their policies will still remain.



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.

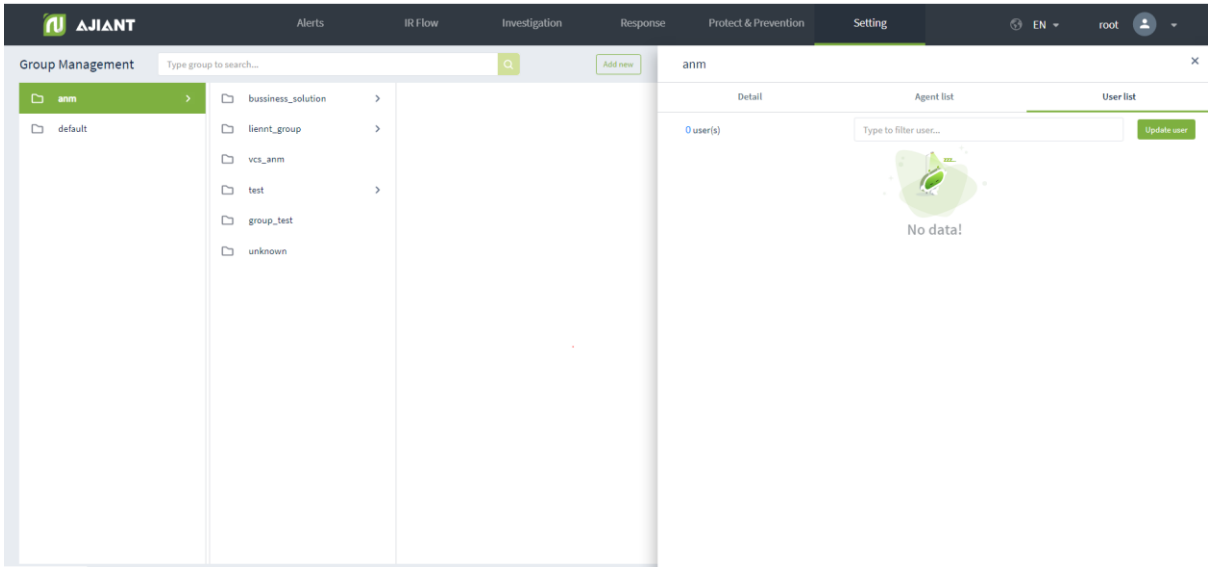
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



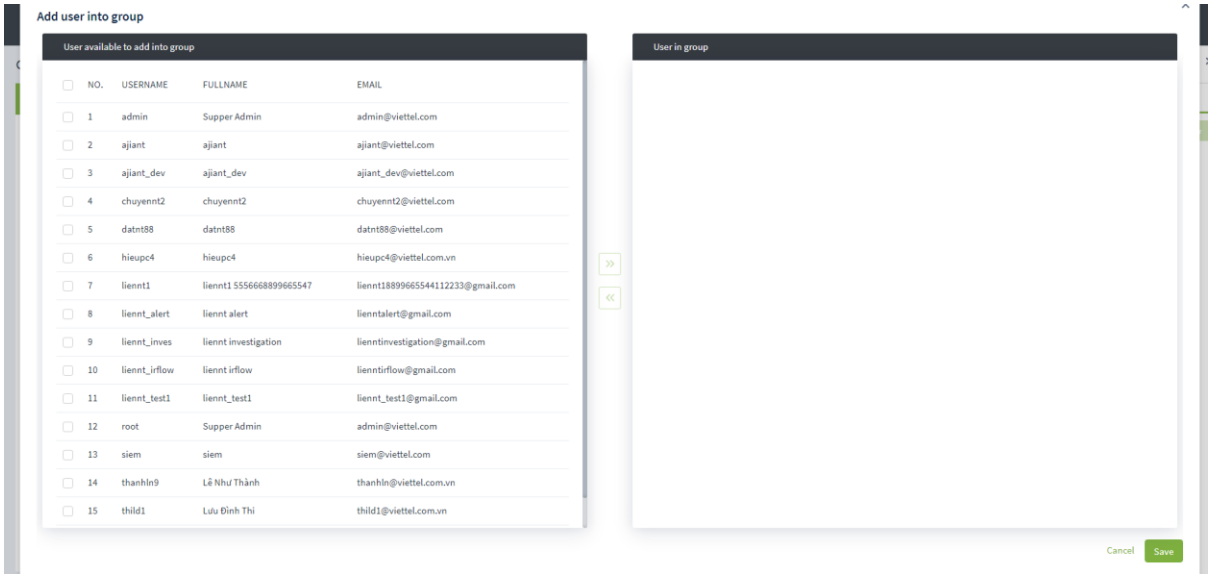
Notes: For deleting a parent-level group:

- 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.

8.1.3.6. Add a new user to the group



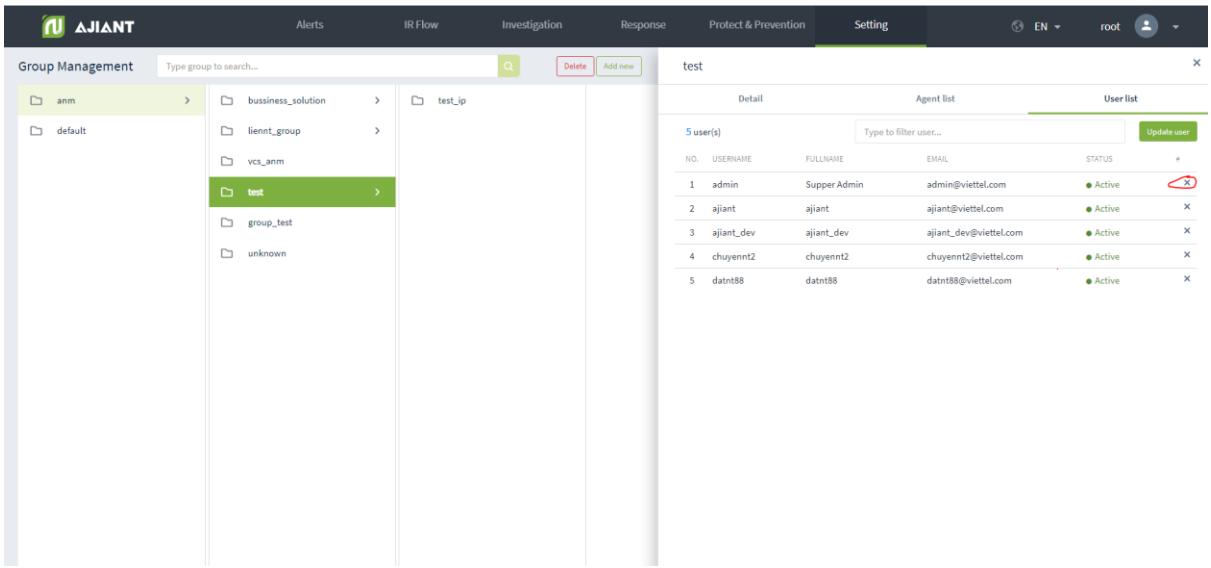
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



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.

8.1.3.7. 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

8.1.4. Account Management

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

8.1.4.1. 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

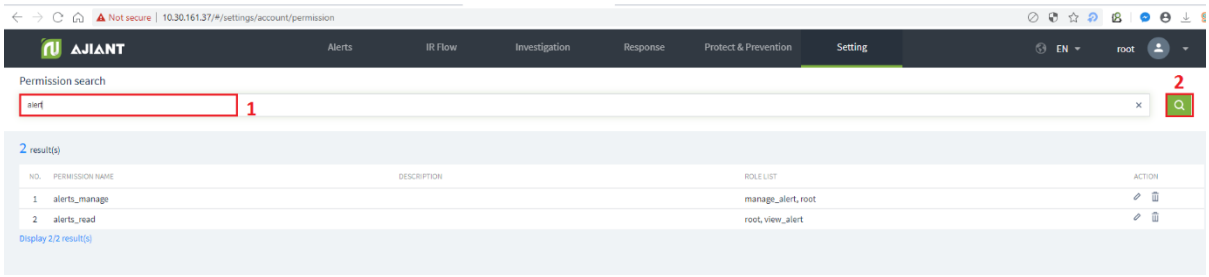
(3) Delete permission

8.1.4.1.1. 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.

8.1.4.1.2. Search permission

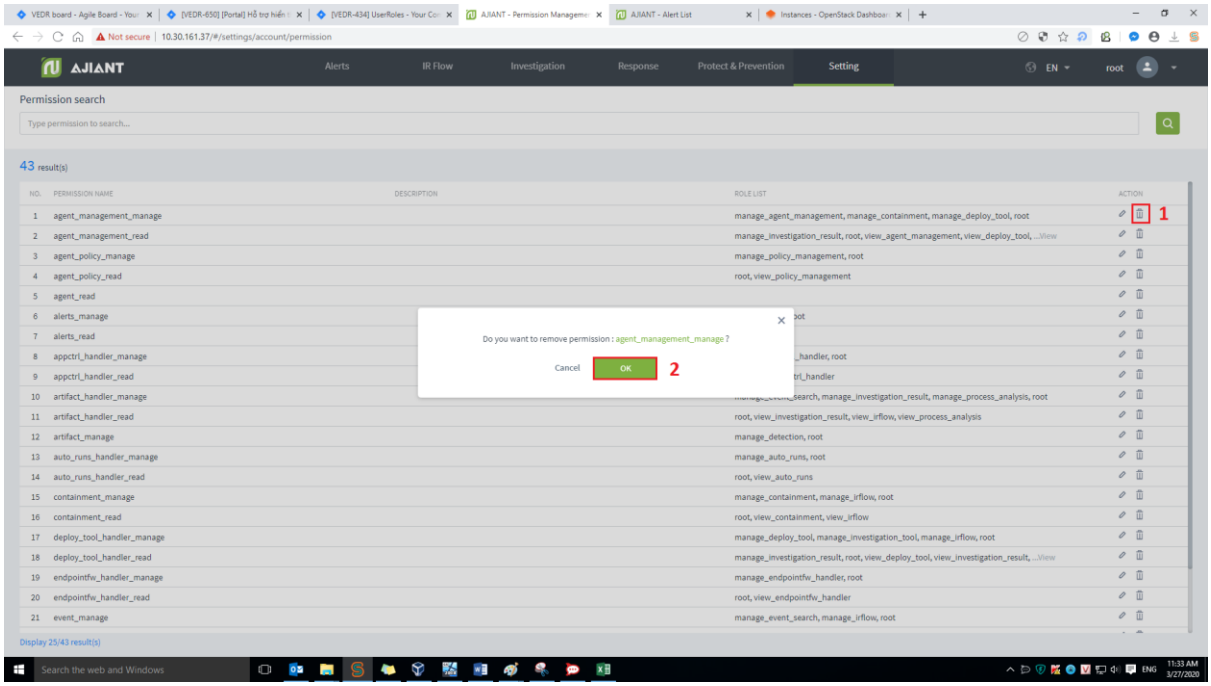
Enter the search character in the Search textbox → Click Enter or Search → A list of satisfied permission is displayed.



8.1.4.1.3. 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



8.1.4.2. 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

8.1.4.2.1. Manage list of role

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

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

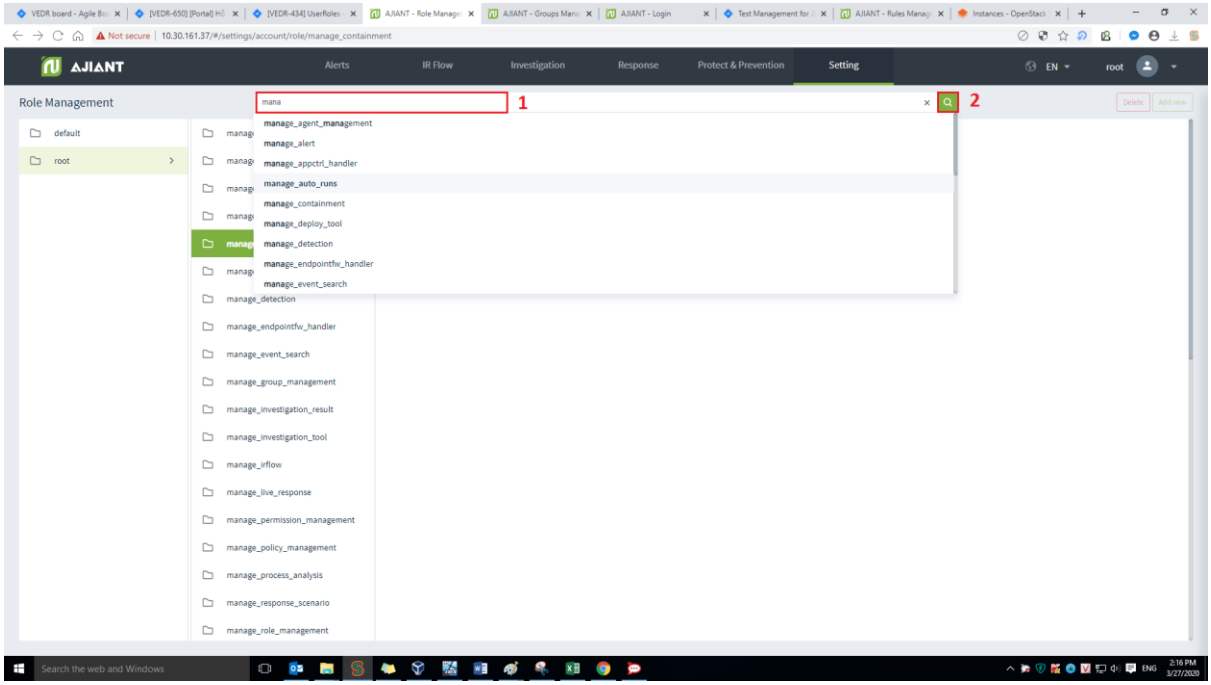
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

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).

8.1.4.2.2. 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.
    - 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.

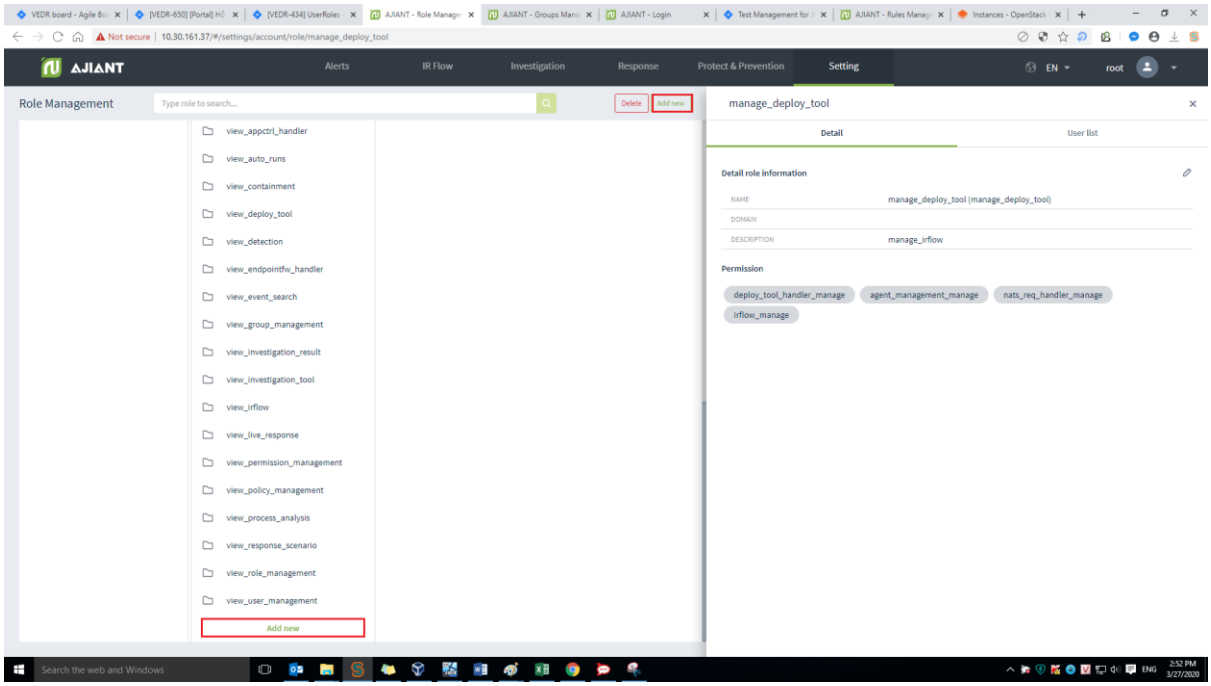
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- When clicking on the menu in the right corner, each record also displays the option: Go to role.

8.1.4.2.3. 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 group: 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.



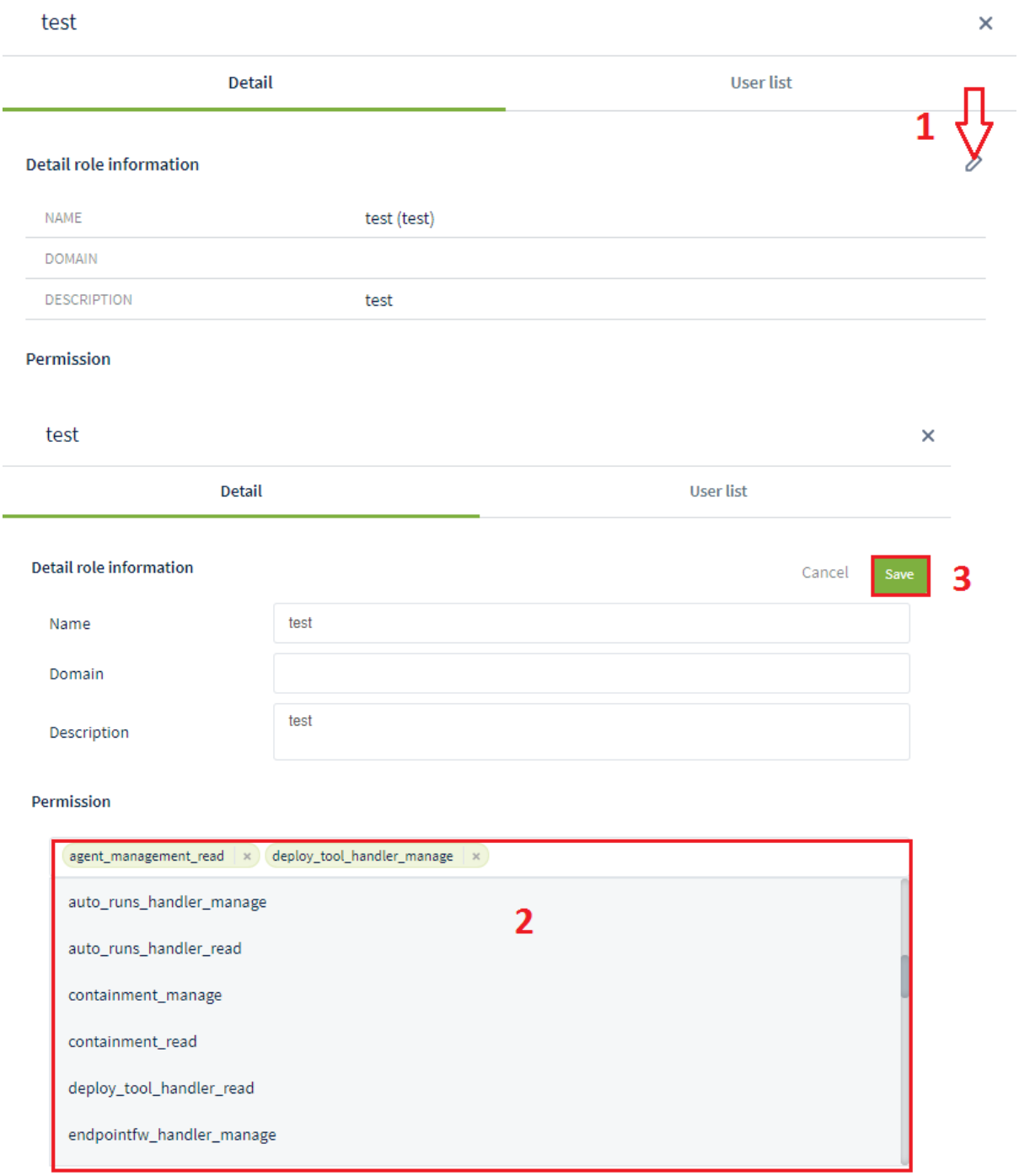
  - Step 2: Click the Edit icon to add permission information for the role → Select permission to add to the role → Click Save.
- User login under root group: Enable to edit all roles in the system.

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 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 group: 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.

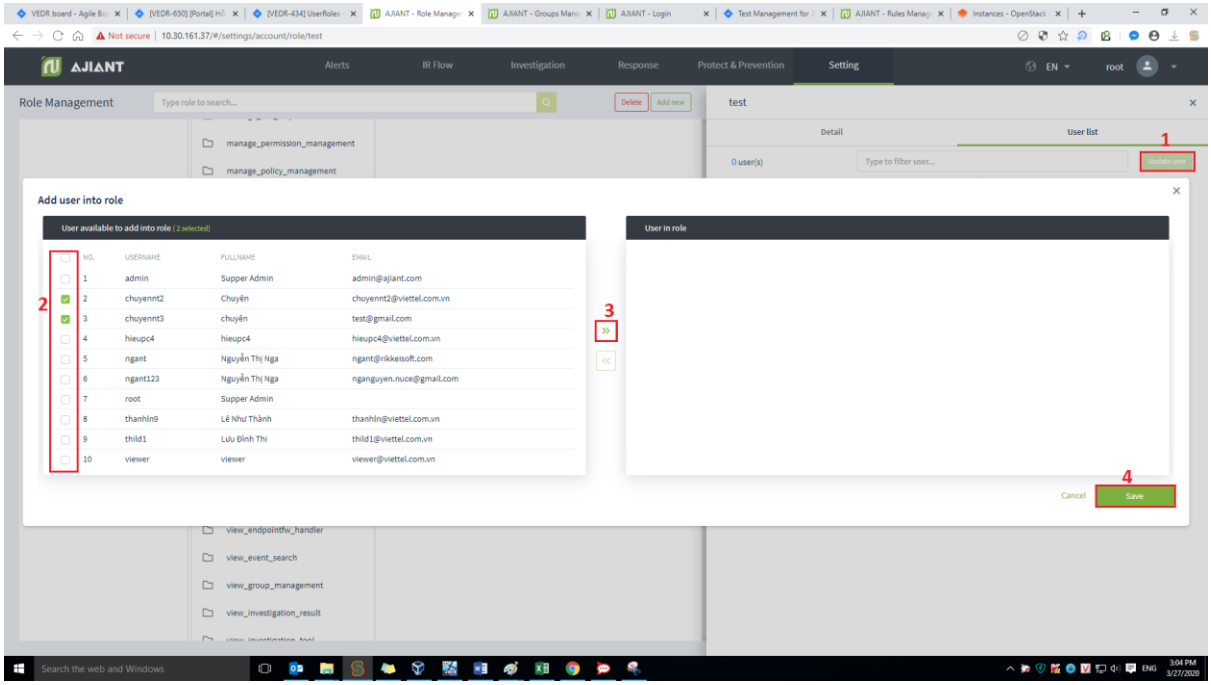
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- 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

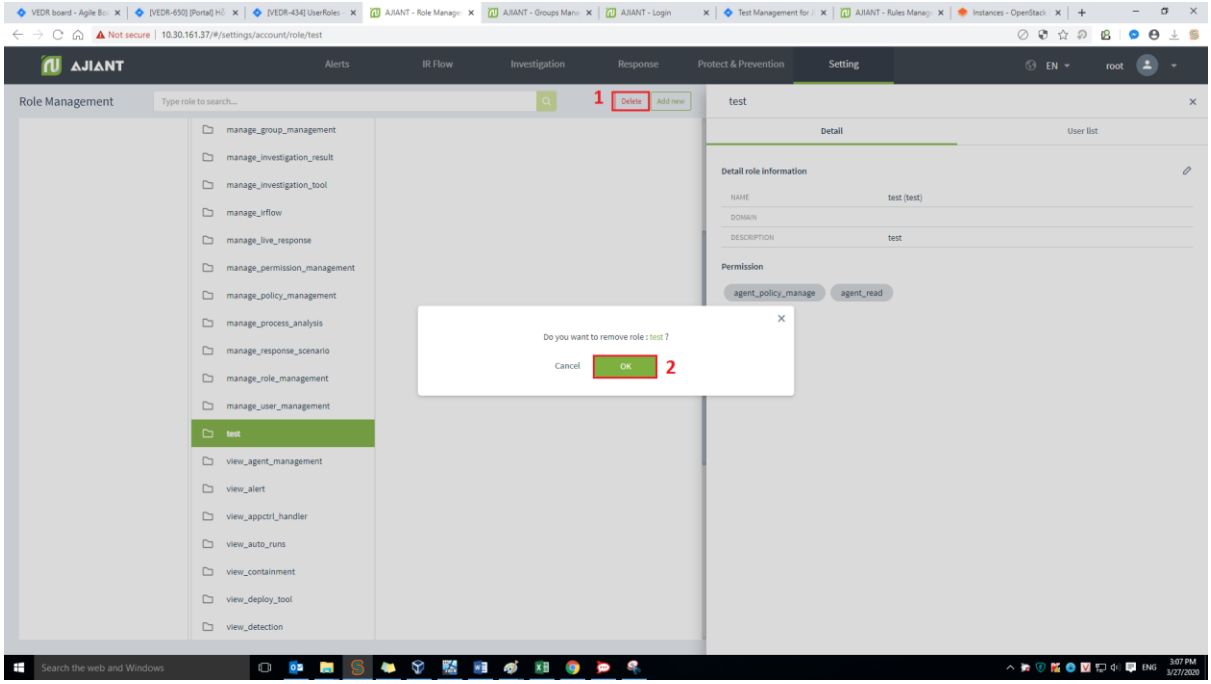
- User login under parent-level group: Display the user logging in and the user in the child-level group whose role is also in the child-level role group of the user logging in.
- User login under a child-level group or many child-level groups: Display the user logging



8.1.4.2.4. Delete 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

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



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.

8.1.4.3. 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

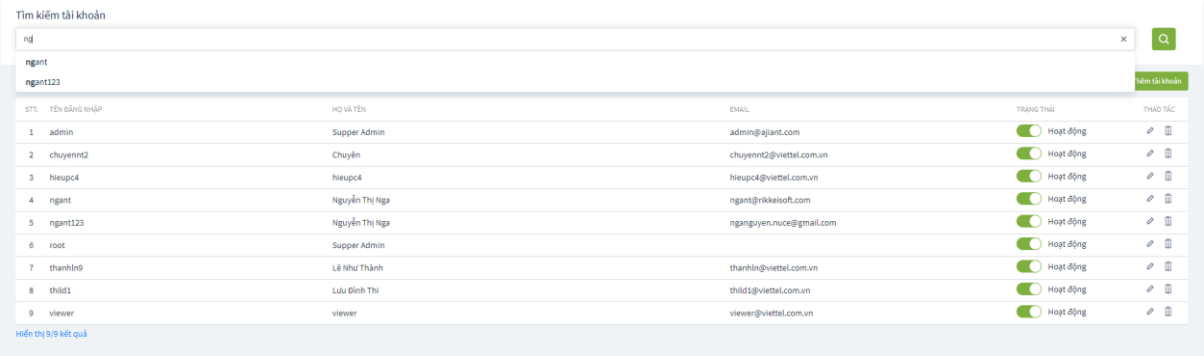
(3) Edit account

(4) Delete account

8.1.4.3.1. Search account

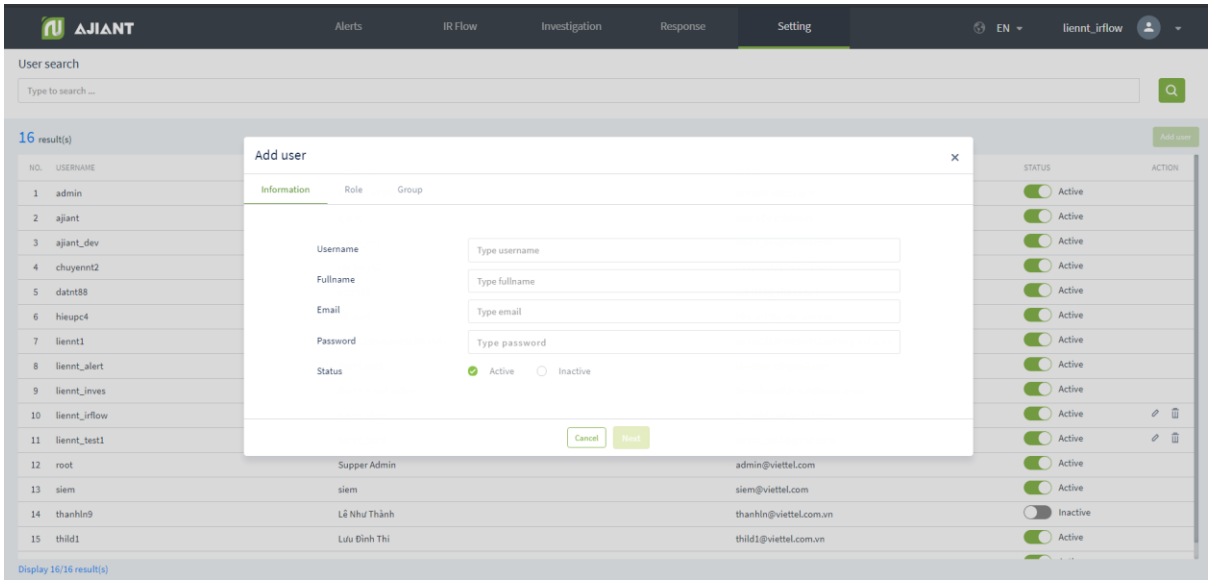
Click on the Search textbox → The list of accounts in the system is displayed → Select the account to search in the list or enter the <text> character in the textbox to filter out the accounts → Click Search or select the account to search from the list of filtered accounts.

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



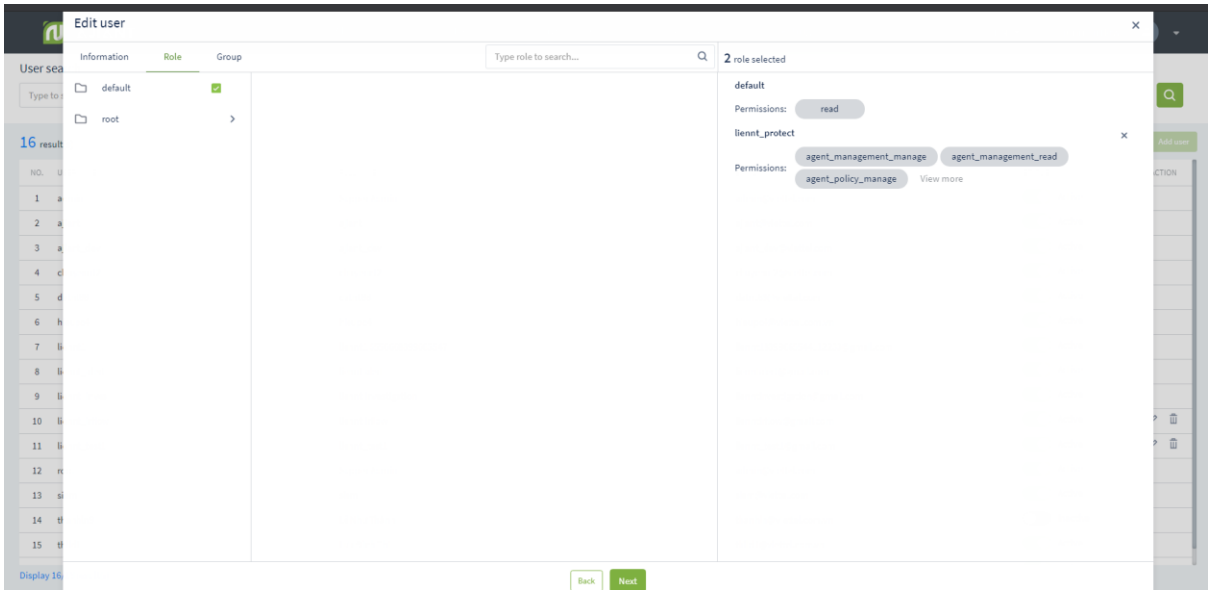
8.1.4.3.2. Add new account

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

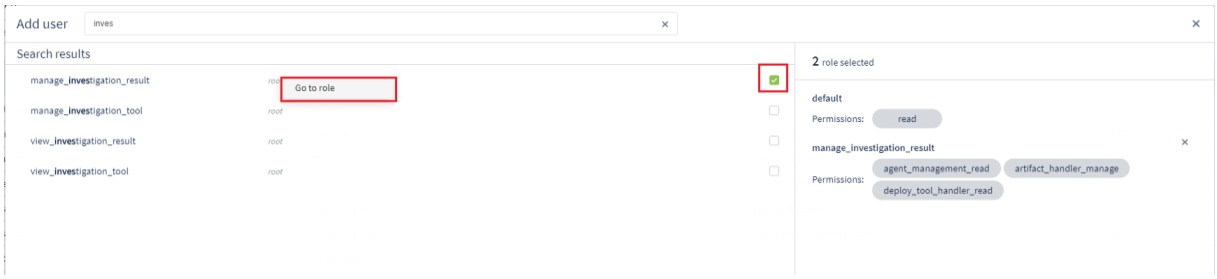


- Select the role (permission group) to assign to the account, then click Next.
- When clicking on the check box, each role will display the permission corresponding to that role:
  - User login under root role: Display all roles in the system.
  - User login under default role: Display default role.
  - 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.

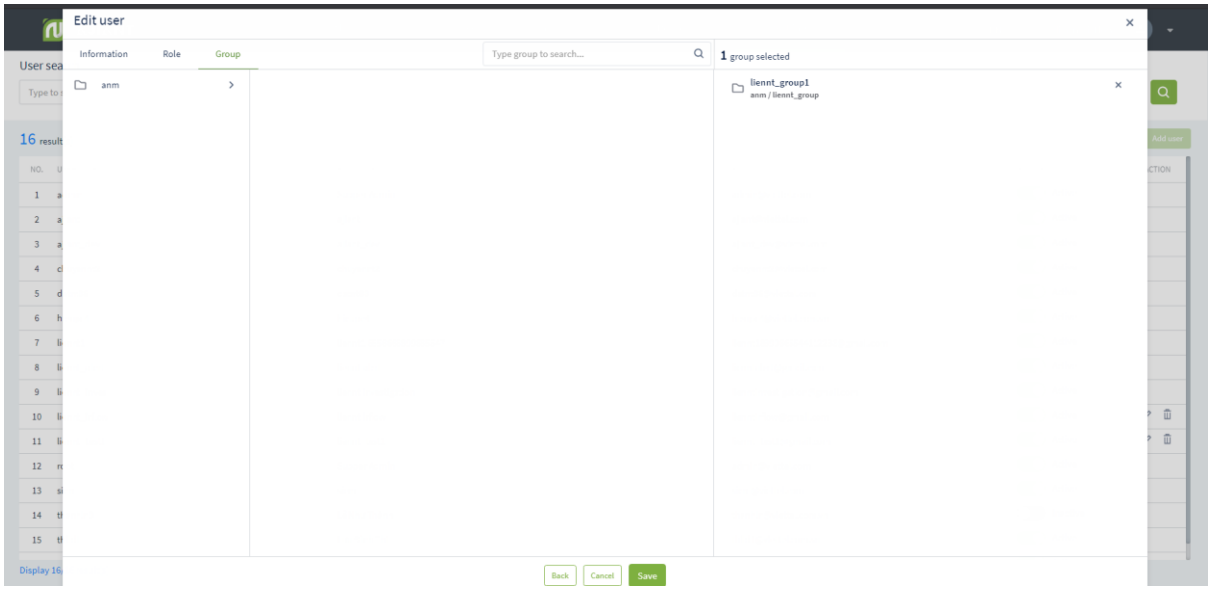


- Click the checkbox corresponding to the role to be added, and click Go to role to return to the original role list screen, then click Create to create an account.

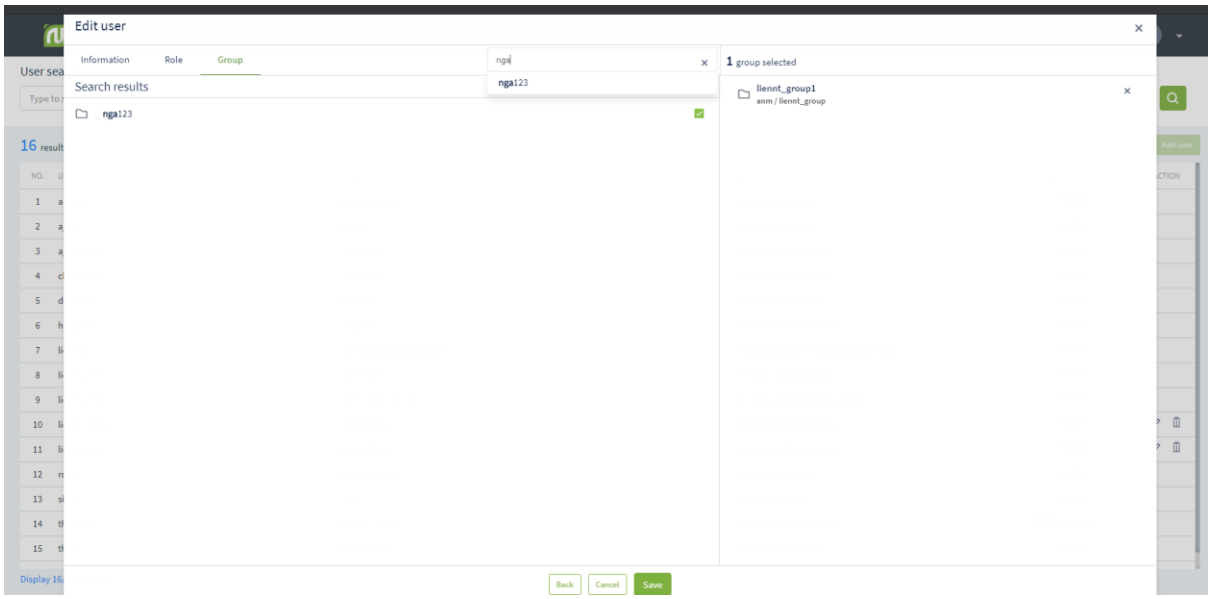
Notes: The account that is logged in to create a new account can only create accounts containing child-level roles in the list of roles that the account logging in is granted.

- 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-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.

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



- 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.



8.1.4.3.3. Delete account

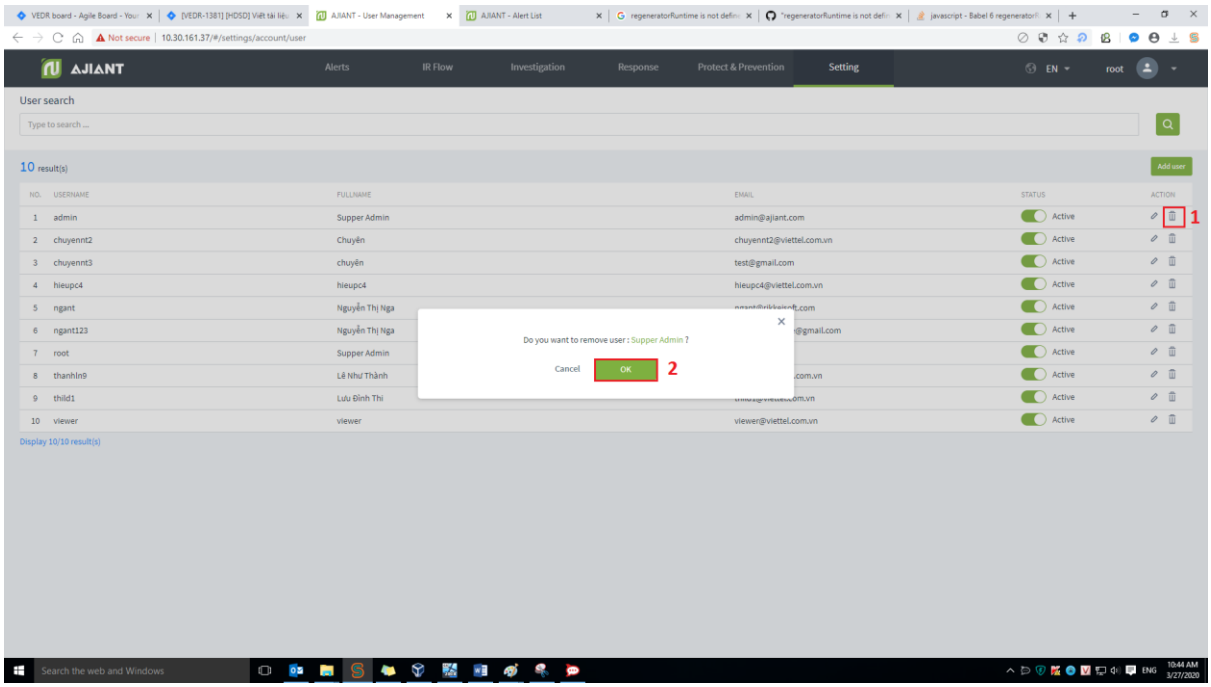
Click on the Delete icon, then click OK on confirmation screen.

Check the display of the Delete icon as follows:

- 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.

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 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

9. BLS Screen

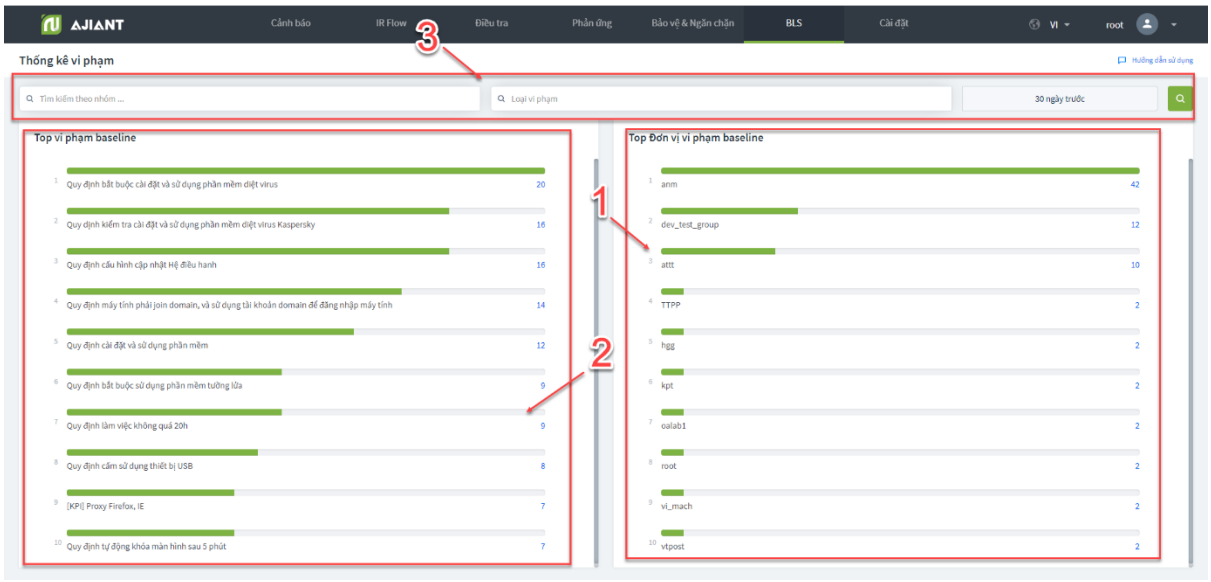
9.1.1. Violation statistics

The function of Violation statistics supports the administrator to make statistics about the violations of the installed agent, including:

- Top base line violations and top baseline violation units
- View the list of violations and the list of violation agents in each unit
- View the list of violation units and the list of violations in each unit
- View details of Agent
- Export violation
- Report violation.

Click on the BLS tab >> Violation statistics.

3.9.1.1Violation Statistics Screen



The system supports performing the following features:

(1) Statistics of Top 10 most base line violations arranged in descending order

Each record is displayed with information, including: violation content and number of violation machines.

Select any record in the Top baseline violation, the system will move to the detail screen corresponding to the selected violation.

(2) Statistics of Top 10 units violating the most base-line arranged in descending order

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

Each record is displayed with information, including: name of violation unit and number of violation machines.

Select any record in the Top unit violating the baseline, the system will move to the detail screen corresponding to the selected unit.

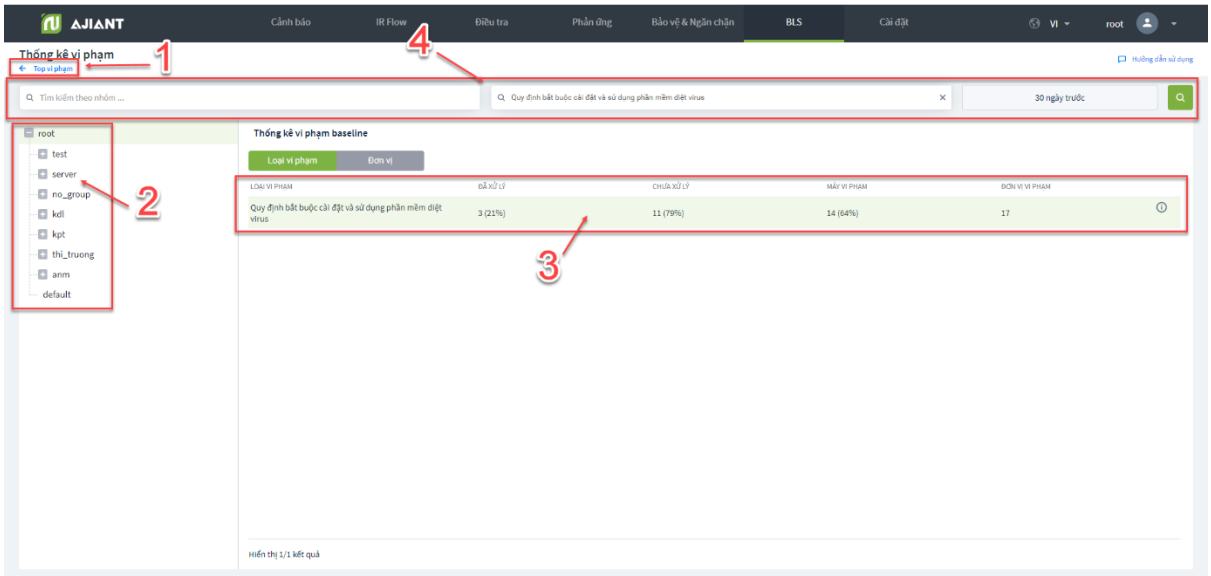
(3) Search

Individual search:

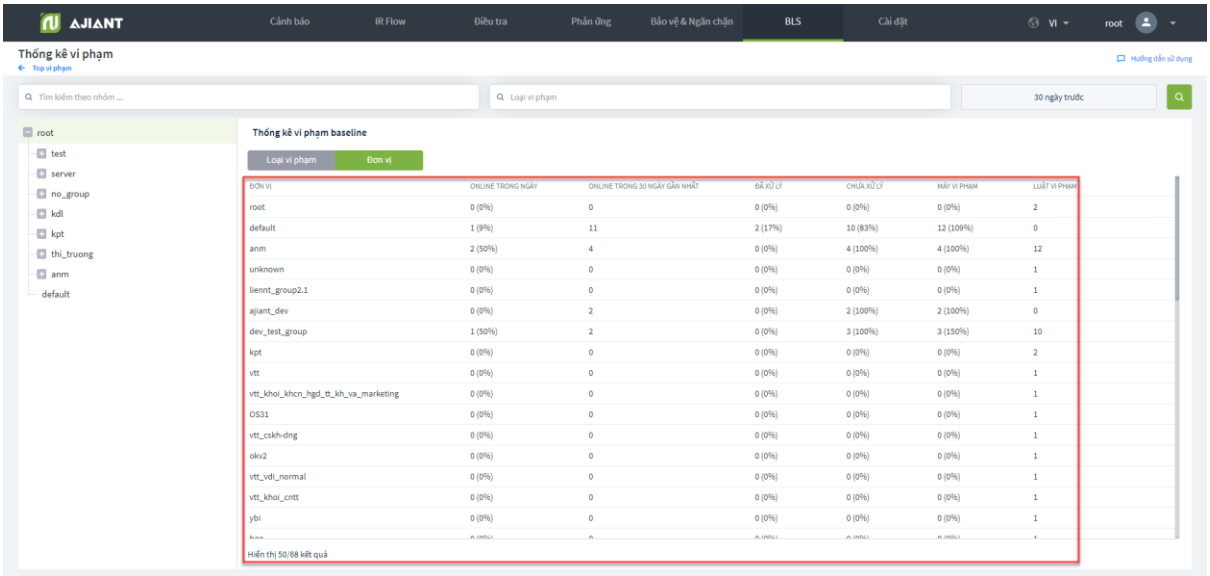
- Search by unit
  - Top violation units: Display the units entered and the list of corresponding child-level units (if any).
  - Top violations: Display the violations of the unit and corresponding child-level unit (if any).
- Violation type
  - Top violation units: Display a list of violation units and selected violation type.
  - Top violations: Display the selected violation.
- Violated time

Combination search: When entering 2 or more search conditions, the search will be performed according to the AND condition.

3.9.1.2Violation Type 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 supports performing the following features:

(1) Select the Top violation links

Move to the Dashboard screen, the list of top violations and top violating units.

(2) The unit data tree of system

Display all system units with the parent-child hierarchy.

Enable to select units on the unit data tree to filter violations.

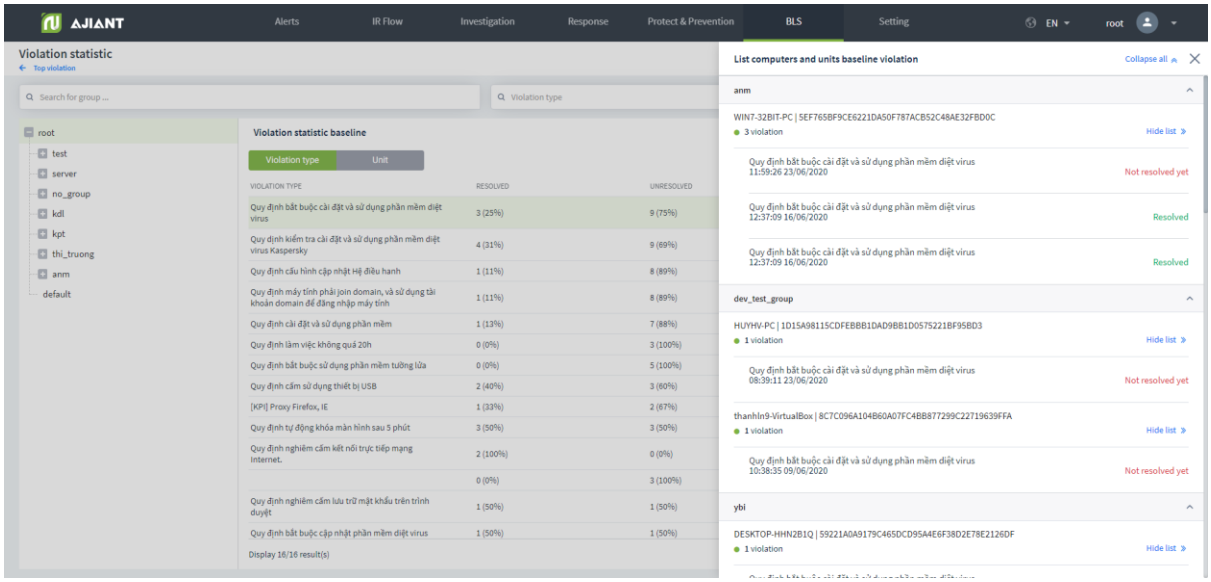
(3) Violation Type tab

Each Violation Type is displayed with general information, including: Violation type, Resolved, Unresolved, Violation Computer and Violation unit.

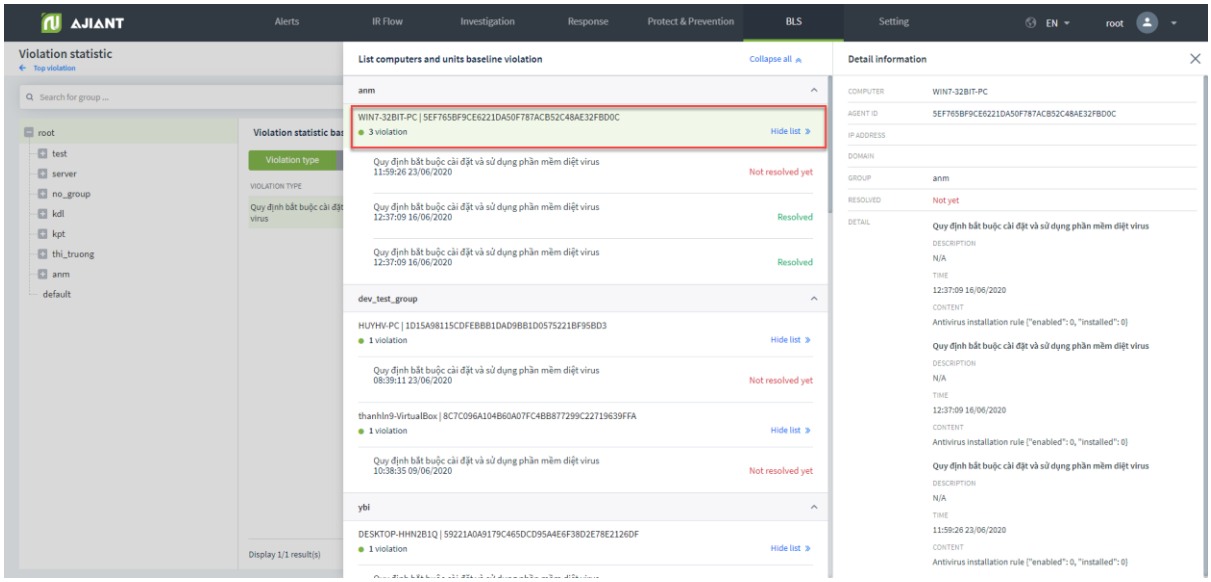
Select the Violation Type record on the list: Display a list of computers in each violation unit.

Select computer: Display detailed computer information and the corresponding violation list of the 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



Select a computer on 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 of the machine).



(4) Search

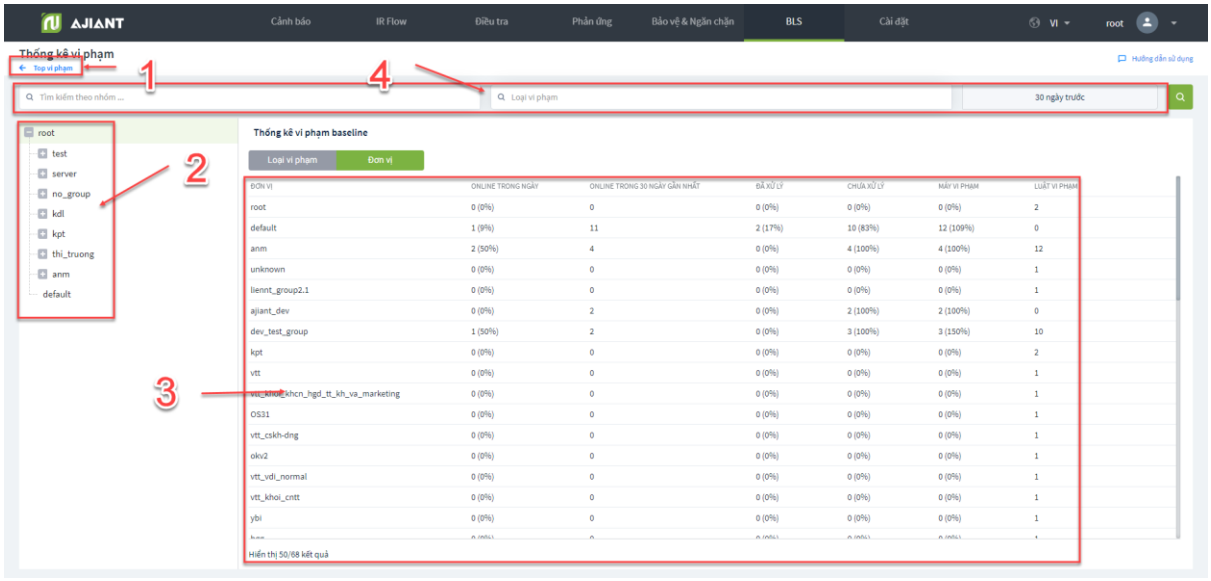
Individual search:

- Search by Unit: Display the entered unit and the list of corresponding child-level units.
- Violation type: Display the selected violation.
- Violated 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

Combination search: When entering 2 or more search conditions, the search will be performed according to the AND condition.

3.9.1.3Unit Tab



The system supports performing the following features:

(1) Select the Top unit links

Move to Dashboard screen, list of top violations and top violation units

(2) The unit data tree of system

Display all system units with the parent-child hierarchy.

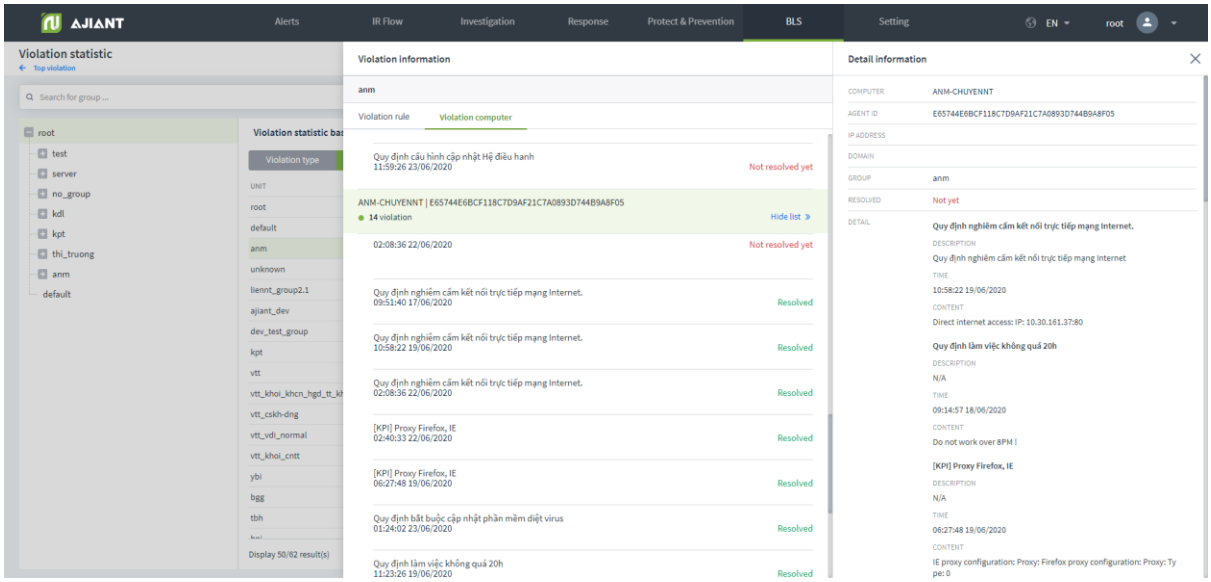
Enable to select units on the unit data tree to filter parent-child violation units.

(3) Unit Tab

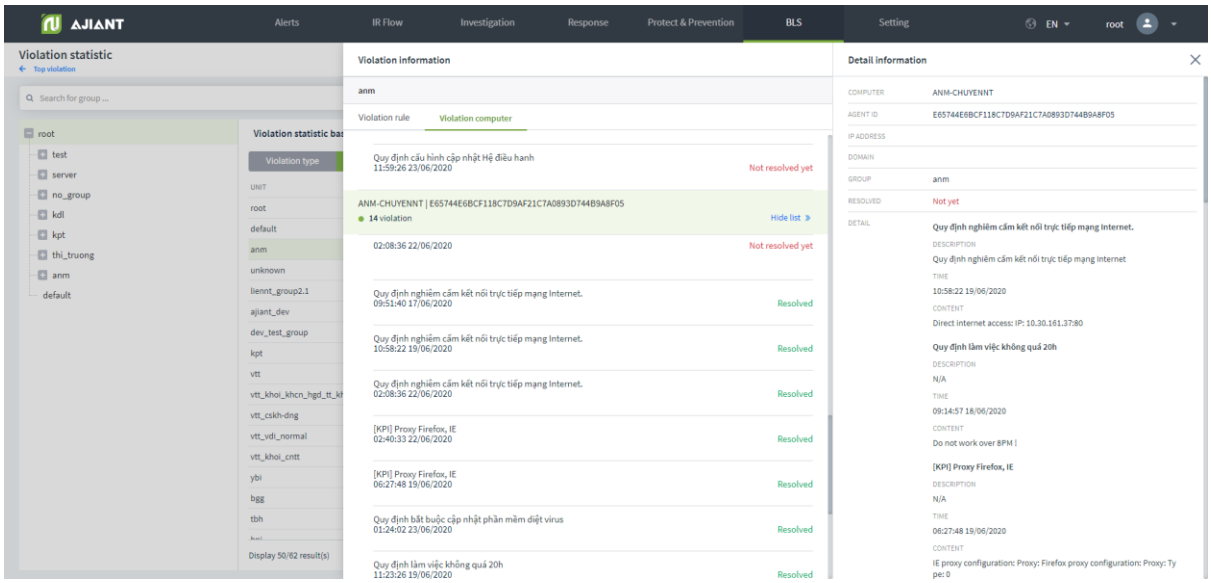
Each type of violation is displayed with general information, including: Unit, Online in day, Online in last 30 days, Resolved, Unresolved, Violation computer and Violation rule.

Select the detail icon of the violation computer column on the list: A list of computers in each violation unit is displayed, including: unit name, computer name|Agent ID, violation list of each machine, violation time, violation state (violation fixed or not fixed).

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

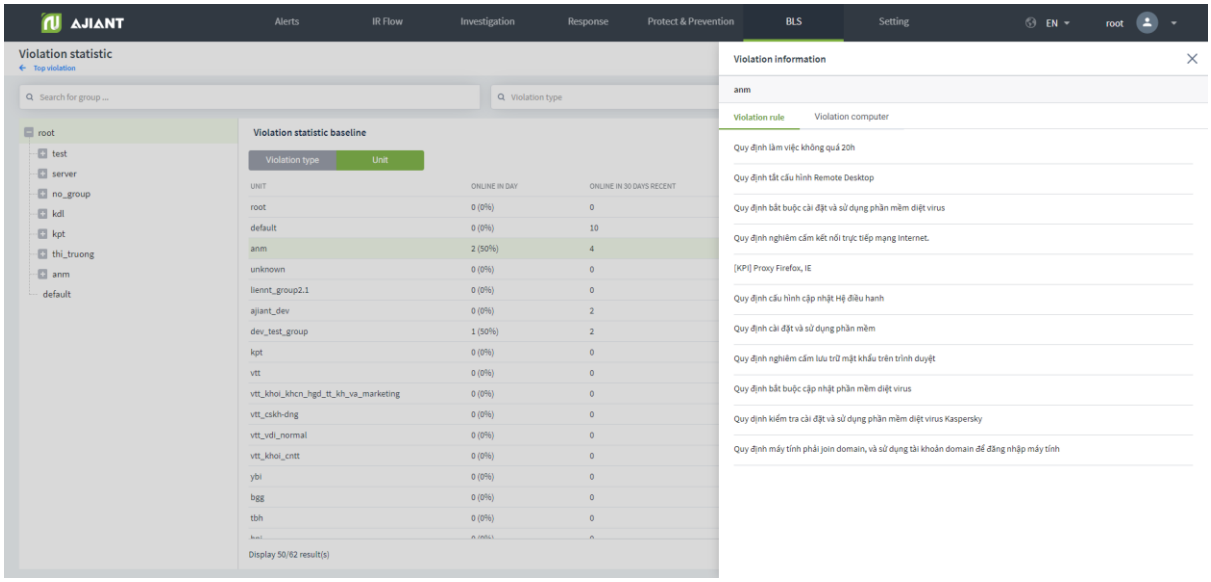


Select a computer on the Computer List popup: A popup with detailed computer information is displayed, including: Computer, AgentID, IP Address, Domain, Group, Resolved, Detail (all types of violations of the machine).



Select the icon detail of the rule violation column on the list: A violation list of the unit is displayed.

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



(4) Search

Individual search:

- Search by Unit: Display the entered unit and the list of corresponding child-level units.
- Violation time: Display the selected violation.
- Violated time

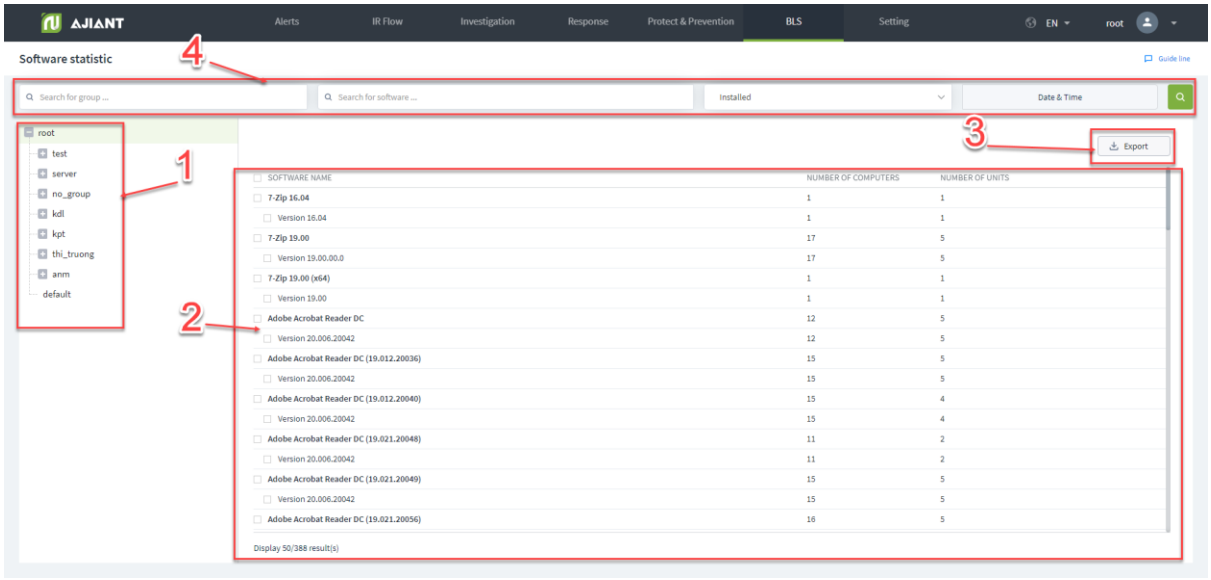
Combination search: When entering 2 or more search conditions, the search will be performed according to the AND condition.

9.1.2. Software statistics

The function of Software Statistics supports administrators to make statistics of installed software in a unit, including:

- View a list of installed software in a selected unit
- View details of Agent
- Export software.

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 supports performing the following features:

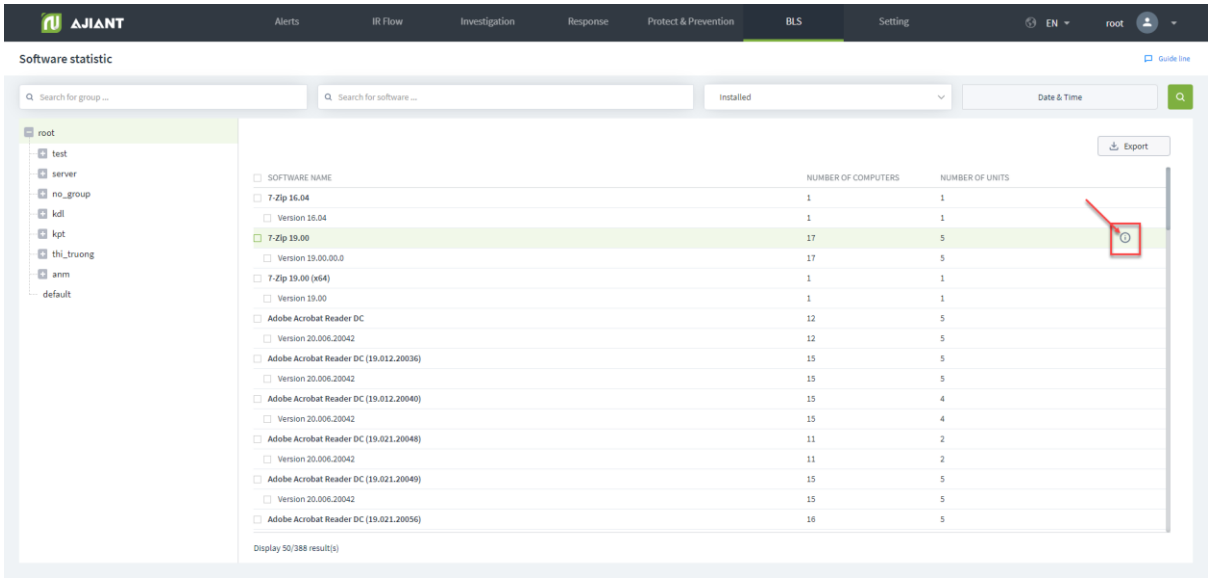
(1) The unit data tree of system

Display all system units with the parent-child hierarchy.

Enable to select units on the unit data tree to filter software.

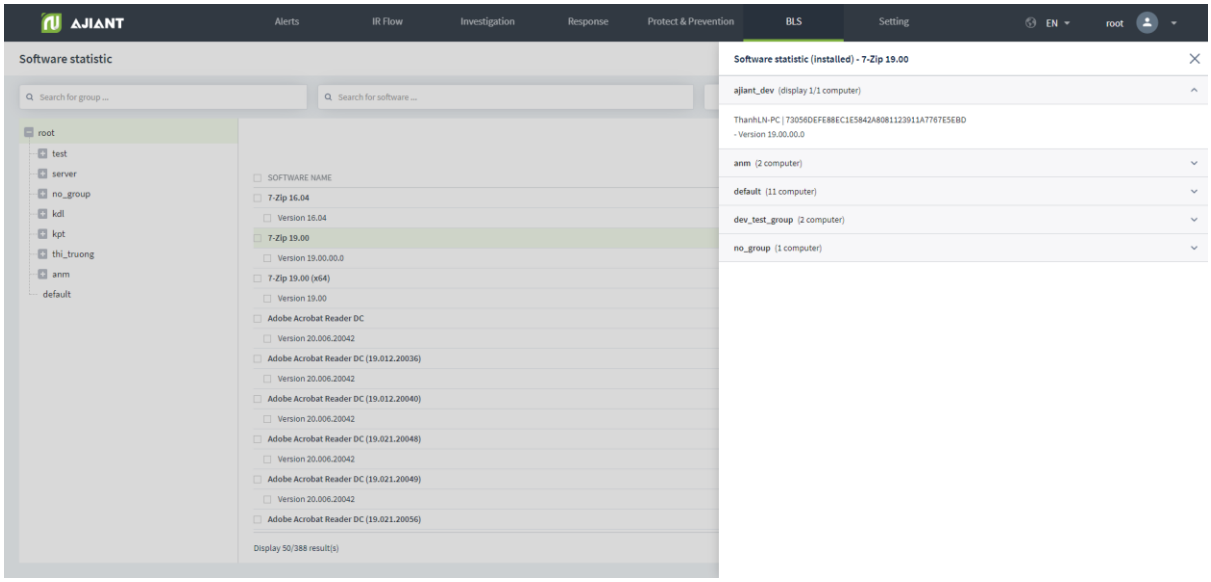
(2) Software list

Each software is displayed with general information, including: Software name, computer number and unit number.

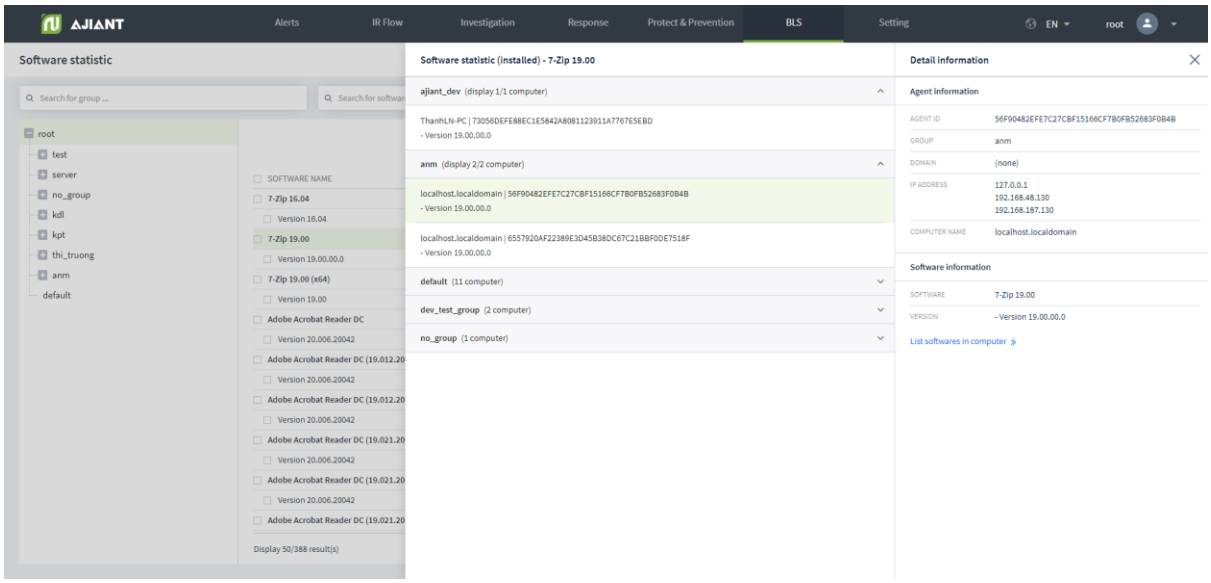


Select the icon detail of the violation computer column on the list: Display a list of computers in each unit, including: Unit Name, Computer Name|Agent ID and Version.

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

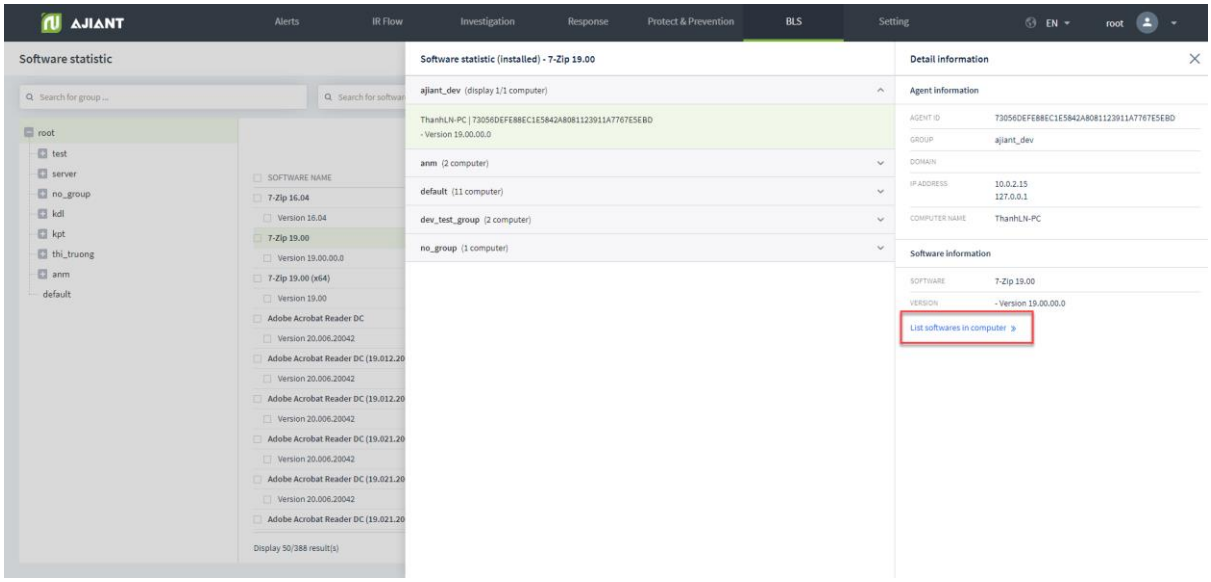


Select a computer on the Computer List popup: Display a popup with detailed computer information, including: Computer, AgentID, IP Address, Domain, Group and Software information (software name, version).



Select the link [Software list in computer]: The system goes to the Agent Management screen and the popup of corresponding computer details is displayed.

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) Search

Individual search:

- Search by Unit: Display the installed software in the unit.
- Software name: Display the list of entered software.
- Search by state: Installed and uninstalled.
- Installation time.

Combination search: When entering 2 or more search conditions, the search will be performed according to the AND condition.

(4) Export

Select Export: The system will download the Export file with the same data as the one displayed on the 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

10. Rules Correlation

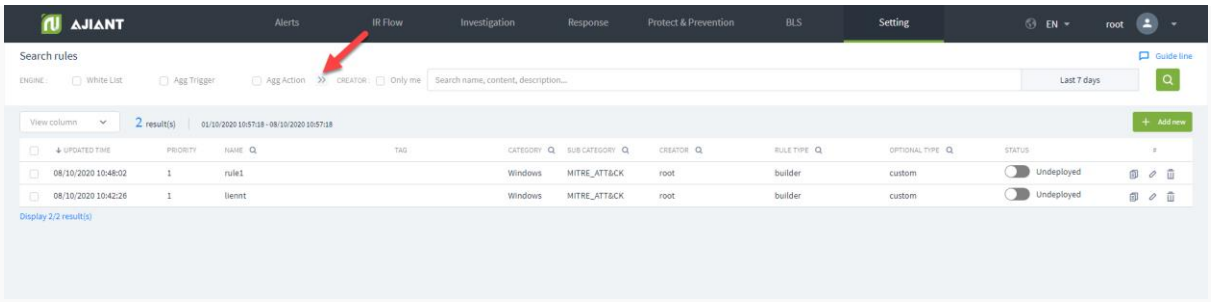
10.1.1. Display List

The function allows users to enter or select search conditions to search for existing rules on the system and quickly deploy/undeploy/delete with rules.

- FILTER
- FILTER includes:
  - 6 Engines: Whitelist, Agg Trigger, Agg Action, Filter, Indicator and False-Positive.
  - Search textbox by fields: Name, content and description.
  - Update time
  - Created by me

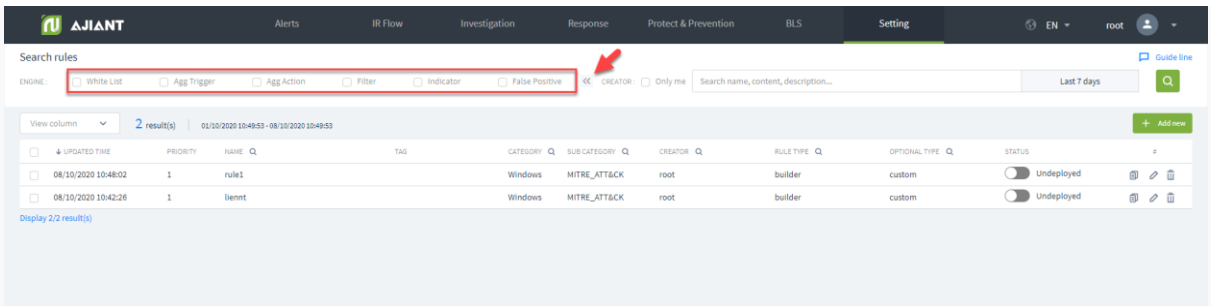
10.1.1.1. Filter by Engine

- Step 1: Choose 1 or more default Engines as follows:



Screen: Search rule

- Step 2: Select Expand to add the Engine to filter.

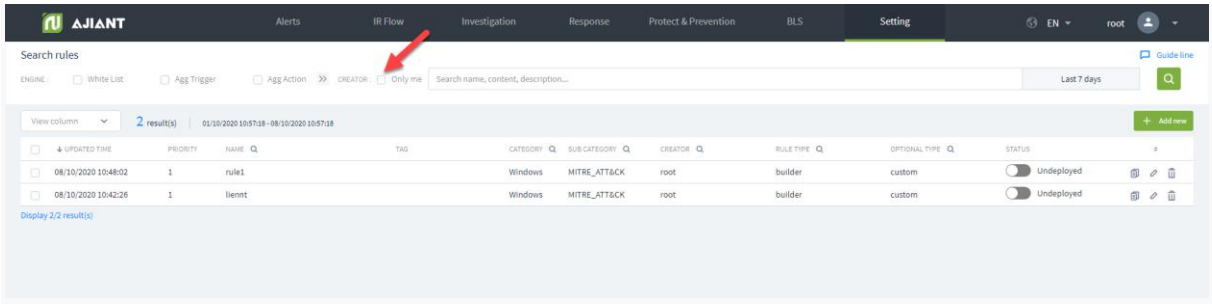


Screen: Expand search conditions

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

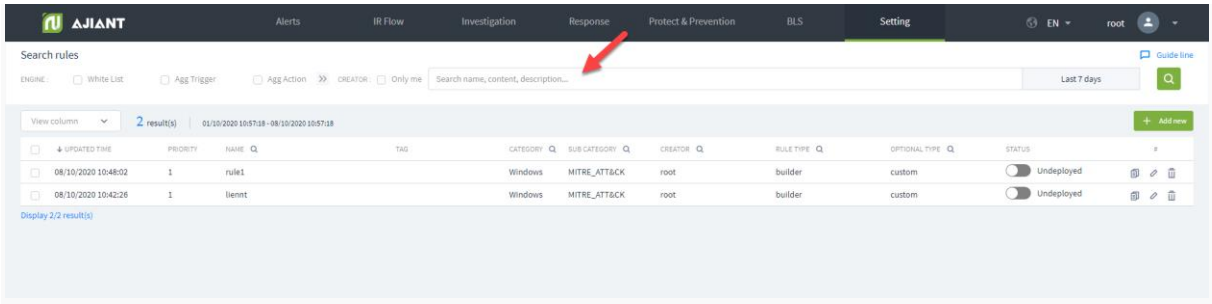
When 2 or more Engines are selected, the display screen returns results filtered by the AND operation.

- Step 3: Check the Rule creator who is the user logging in the system.



Screen: Filter by Creator

- Step 4: Enter the name, content and description to search into the textbox.



- Step 5: Enter the information to search.
- Step 6: Click Search to display search results.

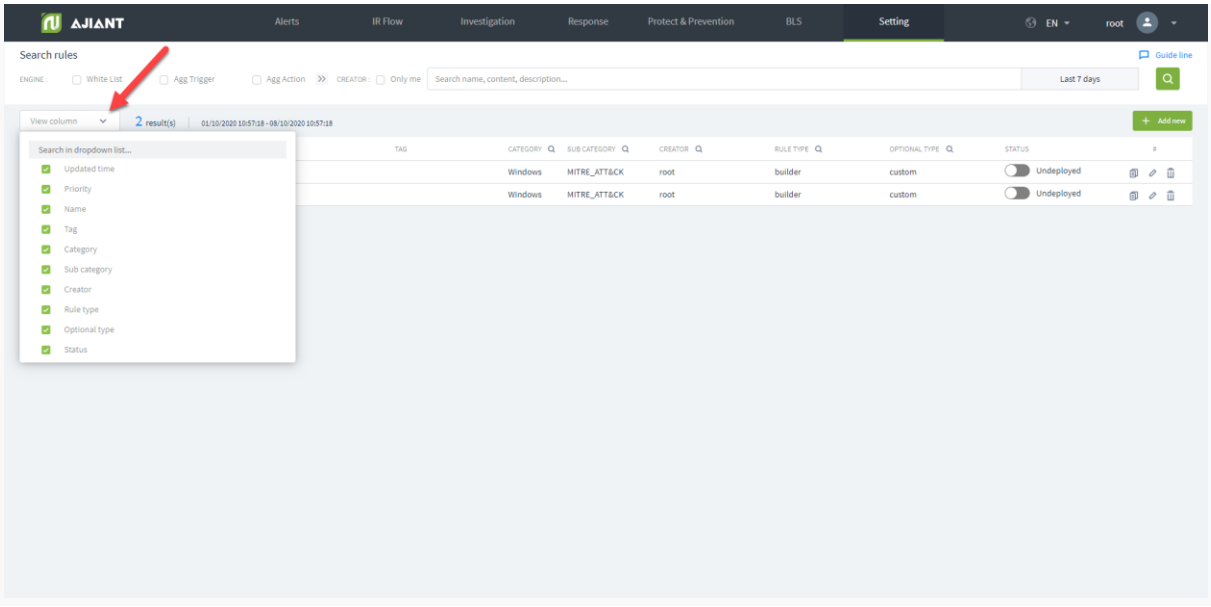
10.1.1.2. Select Column

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

Perform the following steps:

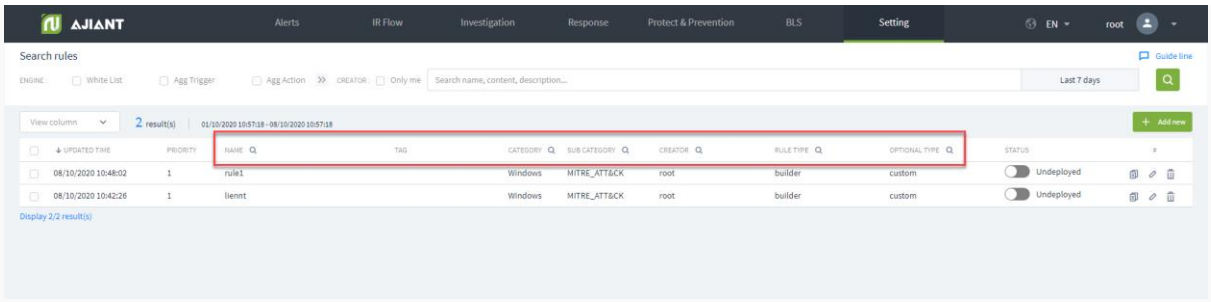
- Step 1: Click the View column combo box. The screen displays a list of selected columns in the form of a check box.
- Step 2: Click Select to the column names to display.

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



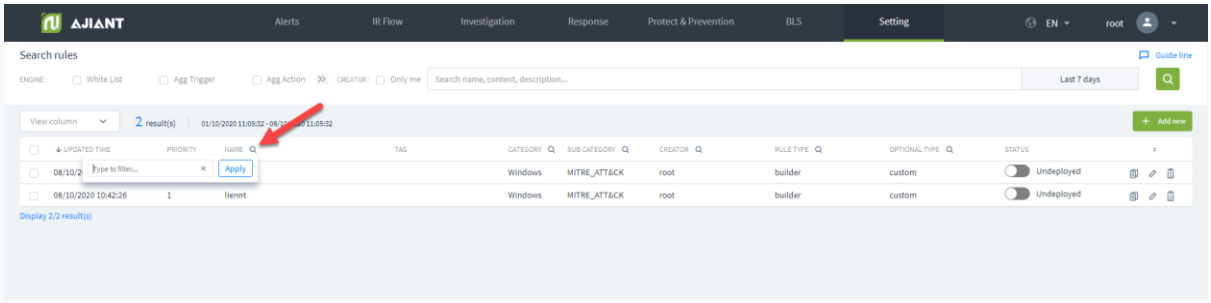
Screen: Options to add more columns

10.1.1.3. Quick Search Support



Search by rule name

- Step 1: Click the  icon to display the search bar.



Screen: Quick search by rule name

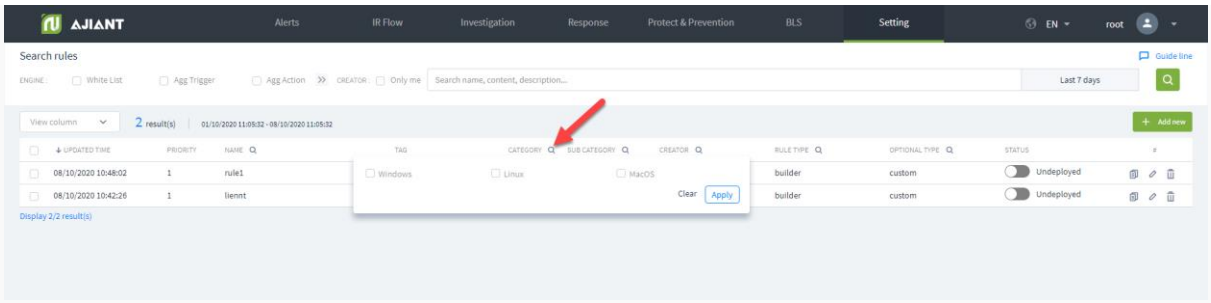
- Step 2: Enter the rule name to search.
- Step 3: Click Enter to display the search results.

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

10.1.1.4. Search by Category

Support quick search with 3 default types: Windows, Linux, and MacOS.

- Step 1: Click the icon to display a list of Category.



Screen: Quick search by Category

- Step 2: Select the category to search.
- Step 3: Click Apply.

10.1.1.5. Search Sub Category

Support quick search by deployment type, including 3 default types: Metre ATT&CK, Malware, and Suspicious Behavior.

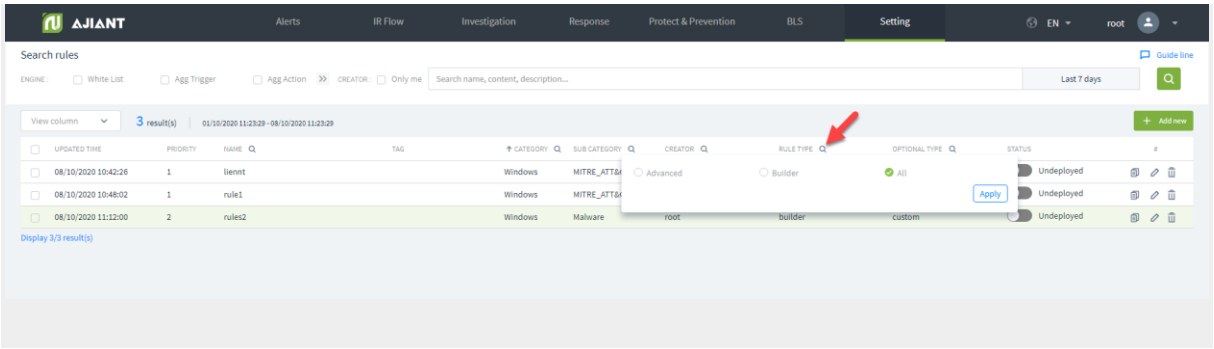
- Step 1: Click the icon to display the search bar.
- Step 2: Select the sub category to search.
- Step 3: Click Apply.

10.1.1.6. Search Creator

- Step 1: Click the icon to display the search bar.
- Step 2: Enter the creator name to search.
- Step 3: Click Apply.

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

10.1.1.7. Search Rule type

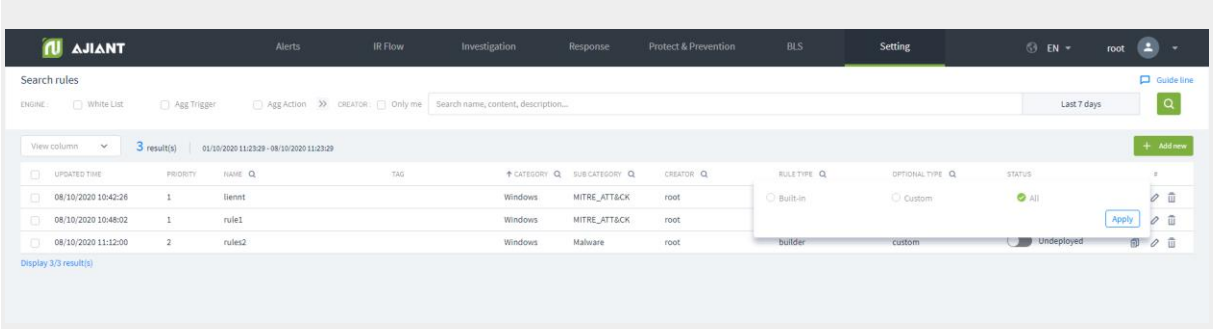


Support quick search with 3 default types: Advanced, Builder and All.

- Step 1: Click the icon to display the list of Rule types.
- Step 2: Click on the Rule type to search.
- Step 3: Click Apply.

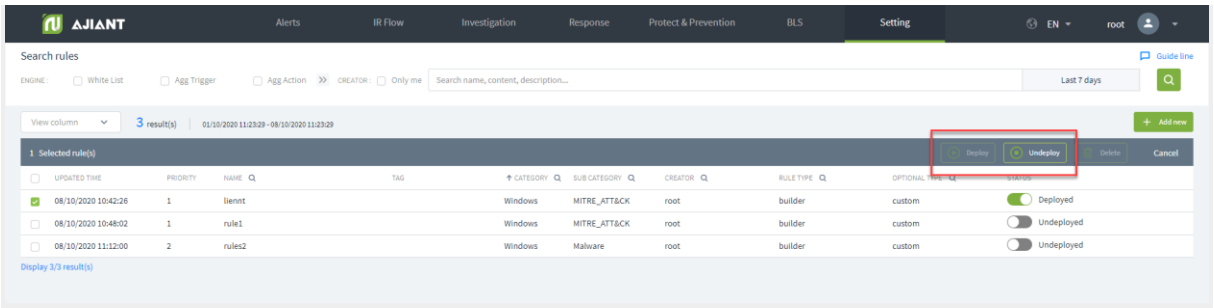
10.1.1.8. Search Optional Type

Quick search support includes 3 default types: Built-in, Custom, All.



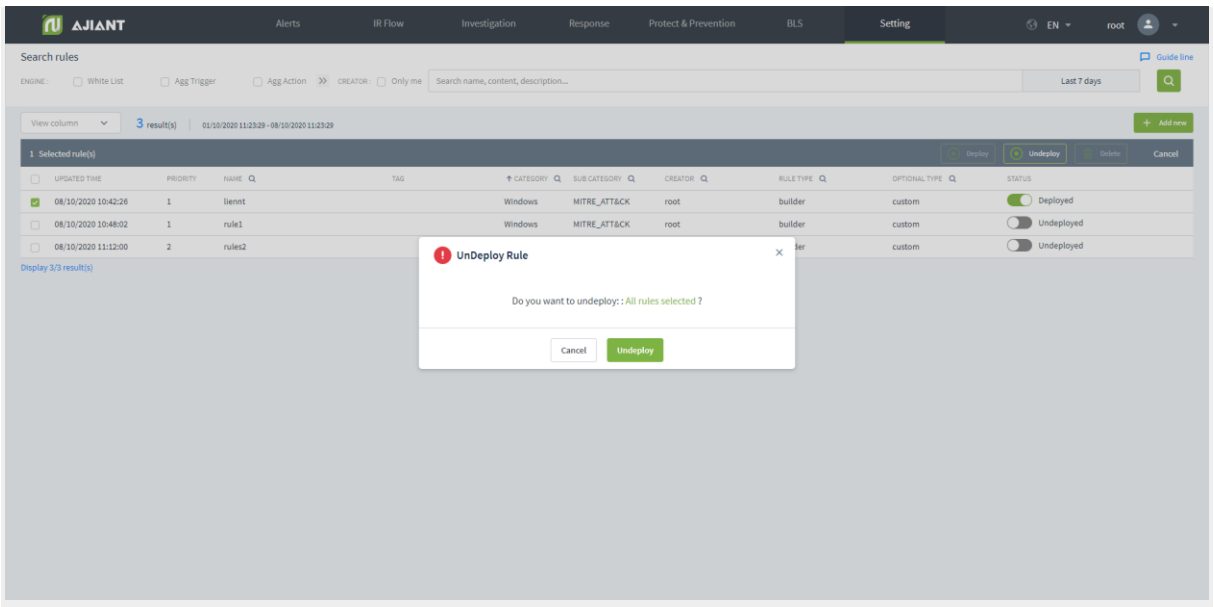
- Step 1: Click the icon to display the list of Optional types.
- Step 2: Click Optional type to search.
- Step 3: Click Apply.

10.1.1.9. Support Deploy/Undeploy for Multiple Rules



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 1: Click on multiple check boxes with the same state as Deploy or Undeploy.
- Step 2: Click the Deploy/Undeploy button.
- Step 3: Select Deploy/Undeploy on the popup displayed to perform Deploy/Undeploy.



10.1.2.Add New Rules Correlation

The function allows the user to configure a complete new correlation rule.

10.1.2.1. Overview

* Engine: It includes 6 engines with detailed information respectively as follows:
    - Whitelist is a Stateless Engine to quickly remove events that the system does not need to handle. Events that match the whitelist rule will be dropped from the traffic.
    - Agg_trigger and Agg_action is a Stateful Engine that performs group of similar events. Each aggregate rule contains information about the clustering condition (similar event definitions) and aggregation interval (e.g. 30s, 1 minute, 2 minutes, etc.). Events that match the group condition are stored and only return an event with the quantity after a time interval. Events that do not match the group condition are returned immediately with a quantity of 1.
    - Filter is a Stateless Engine that filters the conditions to input into the indicator.
    - Indicator is a Stateful Engine that performs checks and statistics on events that satisfy the Filter. Indicator inputs are events that satisfy the Filter, and outputs are Indicator Events or Alert Events. Indicator supports operation of count

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 in a unit of time (time. windows) of the same object, without repeating alerts for the same object in a predefined period of time. Each rule indicator only considers conditions of the same type, on the same system.

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

- Debug/ Not Debug are two states of the engine. When performing a debug action, the returned log that is satisfied with the engine condition will be displayed on the Debug Correlation screen.
- Conditions: Each engine will support different conditions of Event, not Event, Alert Event, not Alert Event, Accumulate, Function and not Function. Details of conditions and use as follows:
  - Event: Used for event fields.
  - Not Event: Only created if there is an event.
  - Alert: Used for alert fields.
  - Not Alert: Consider how long there is no alert event.
  - Accumulate: Perform grouping of event conditions that satisfy the number of events which can create an alert.
  - Function: Be as functions. Notes: For boolean functions, the return value is True or False.
  - Not Function: For Not Function, the functions used are the same as Function. However, the return value will have True/False opposition results.
- Operator:
  - Basic operators include: =, !=, >, <, >=, <= .
  - Print: Check if a field's value is in the list.
    - On the left side of the operator: Name of field to be checked.
    - On the right side of the operator: List of values to be checked is separated by ",".
  - Contains: Check the value of a field that contains the value to be checked.
    - On the left side of the operator: Name of the field to be checked (this field needs to have an array or string value).
    - On the right side of operator: Value to be checked.
  - Assign: Assign the value of a field to a variable.
    - On the left side of the operator: Name of the field to be assigned.
    - On the right side of the operator: Name of the variable to be assigned.
  - Matches: Check if the value of a field matches a regex string.

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 left side of the operator: Name of the field to be checked.
- On the right side of the operator: Regex string.

- Time configuration: Check the condition for a time interval, only in the Agg_trigger, Agg_action and Indicator engines.
- Count: Check if the number of events counted in a time interval satisfies the condition.

- Group/Ungroup: Allow user to quickly group or ungroup conditions in an AND or OR operator.

  Instruction to Group/Ungroup:

  - Group
    - Step 1: Click on the field to be grouped
    - Step 2: Select Group to detailed screen of the steps to perform grouping.
  - Ungroup
    - Step 1: Click on the items to be groupe
    - Step 2: Select Ungroup to detailed screen of the steps to perform ungrouping.
- Restore: Automatically reset to the latest SAVE.
- Reset: Reset conditions (to the original state).
- Delete: Delete Condition that is in focus.

10.1.2.2. Instruction to add new correlation rule:

- Step 1: At the Correlation screen, select the Add New button → System displays the new rule creation 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

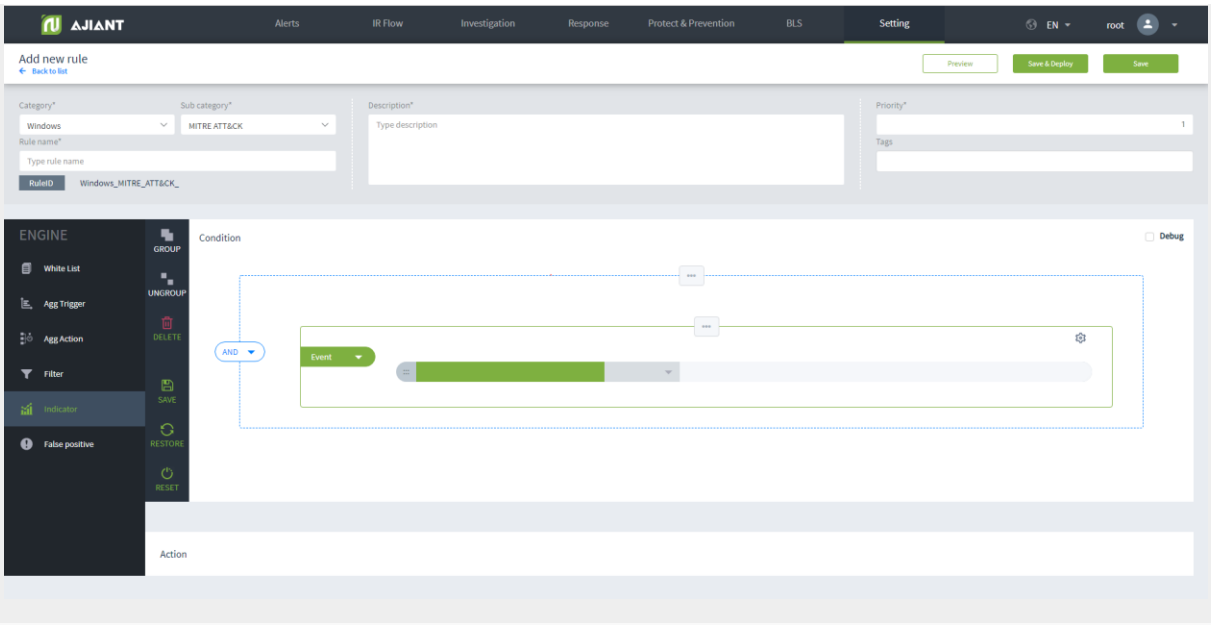
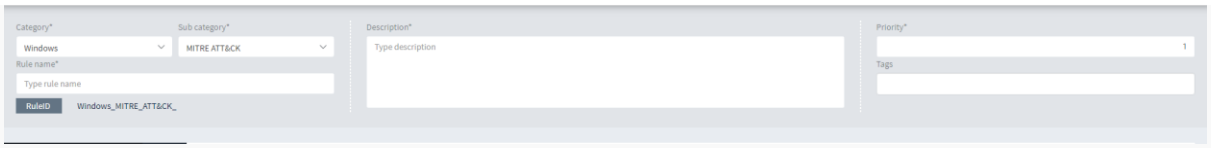


Figure 1: Screen of new Rule correlation creation

- Step 2: Enter the information of the rule.



Notes: Fields with the mark ⭐ are required fields.

- Step 3: Select Engine, enter conditions for Event, Not Event, Alert, Not Alert, Accumulate and Function respectively.

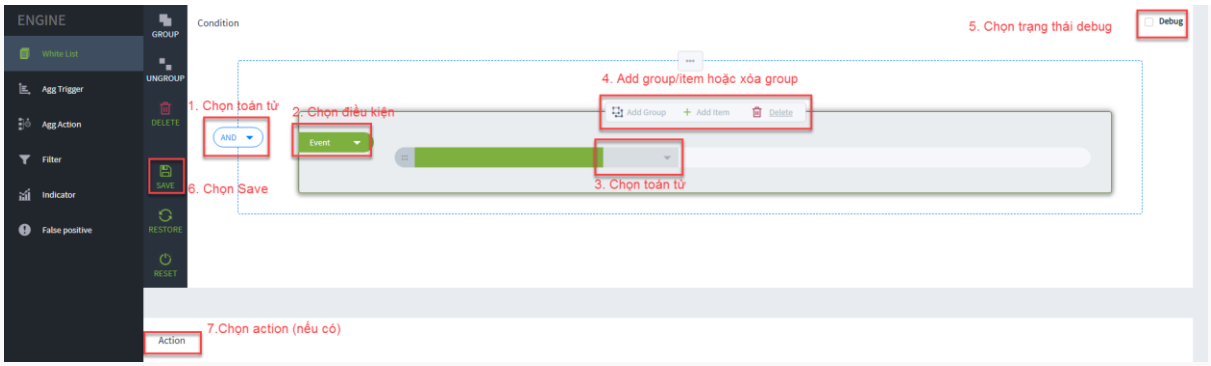


Figure 2: Detailed screen of new rule creation

- Step 4: Click on Save to save the condition or click on Cancel to return right after the newly saved step.
- Step 5: At Action, select the action to take on that engine.

Instruction to perform additional actions corresponding to each 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

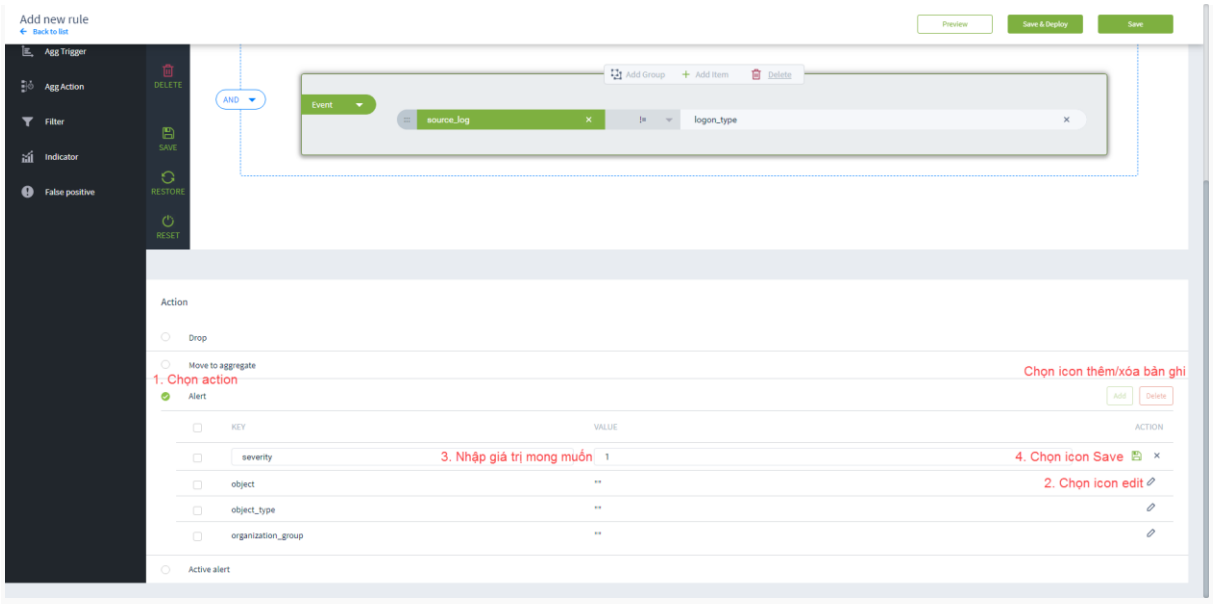
When the user completes the steps of condition creation and clicks Save, the screen will show the actions for each engine. Each engine will include corresponding actions. Agg_trigger engine will have no action.

Whitelist: Include 4 actions in the form of a check box, such as Drop, Switch to aggregate, Alert and Active List. The user is required to select 1 of these 4 actions. When the push log meets the condition, it will perform 1 of 4 actions that the user has selected. Function details of 4 actions as follows:

- Drop: Push logs that satisfy the condition will be dropped from the traffic.
- Switch to aggregate: Push logs that meet the conditions will be transferred to the aggregate engine for further processing.
- Alert: When adding key and value fields for alert, the push logs that meet the condition will display the alert in the Alert Management screen.
- Active list: The values of the active list will be added to the list displayed on the Active List screen.

Instruction to add fields for Alert/Active List action:

- Step 5.1: Click to select the action to add.
- Step 5.2: Click on the Edit button to enter the value for the field.
- Step 5.3: Enter a value for the field
- Step 5.4: Click on Save
- Step 5.5: Click on the Add icon to add a new field to the alert.



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

Figure 3: Screen of new action creation for rule correlation

To delete the action just created, click on the Delete icon.

To edit the action, click on the Edit icon.

Notes: It is possible to create multiple actions with different fields depending on the purpose of the user.
Agg_ation: At this engine, user can perform actions to add code.

Instruction to add a field for the actions of adding code:

- Step 5.1: Enter all conditions and operators. Click Save.
- Step 5.2: In the Action section, click the Enable action icon.
- Step 5.3: Enter the code content.
- Step 5.4: Select the Clear button → The input of the code will be deleted totally.

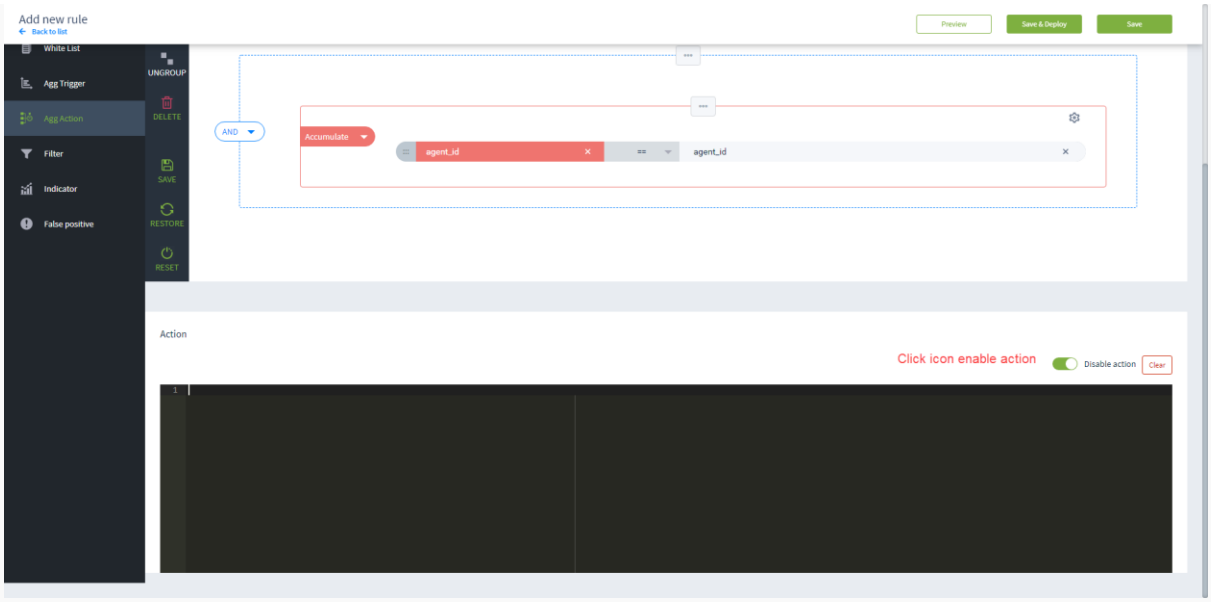


Figure 4: Screen of new Code creation by Agg_action engine

Filter: Consist of 3 actions: Alert, Enrichment and Active List. The user can have one or more actions in the same engine. Function details of 3 actions as follows:

- Enrichment: Add field to Alert.
- Alert and Active List (same with Whitelist engine).

The Add, Edit and Delete actions for the Filter engine actions are similar to new addition of fields for the Whitelist 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

Indicator: Be as Alert action. The Add, Edit and Delete actions for the Indicator engine actions are similar to new addition of fields for the Whitelist engine.

FalsePositive: Be as Enrichment Action. The Add, Edit and Delete actions for the FalsePositive engine actions are similar to new addition of fields for the Whitelist engine.

- Step 6: Click Save to save rule on the system. When the user wants to save on the system and deploy to correlation engine at the same time, click Save & Deploy.

Notes: When there is an error, user can click on Preview to view it.

10.1.3.Edit Correlation Rules

It allows user to edit the created rules with below implementation steps:

- Step 1: At the Rule Management screen, click on the Edit icon of the rule to edit.

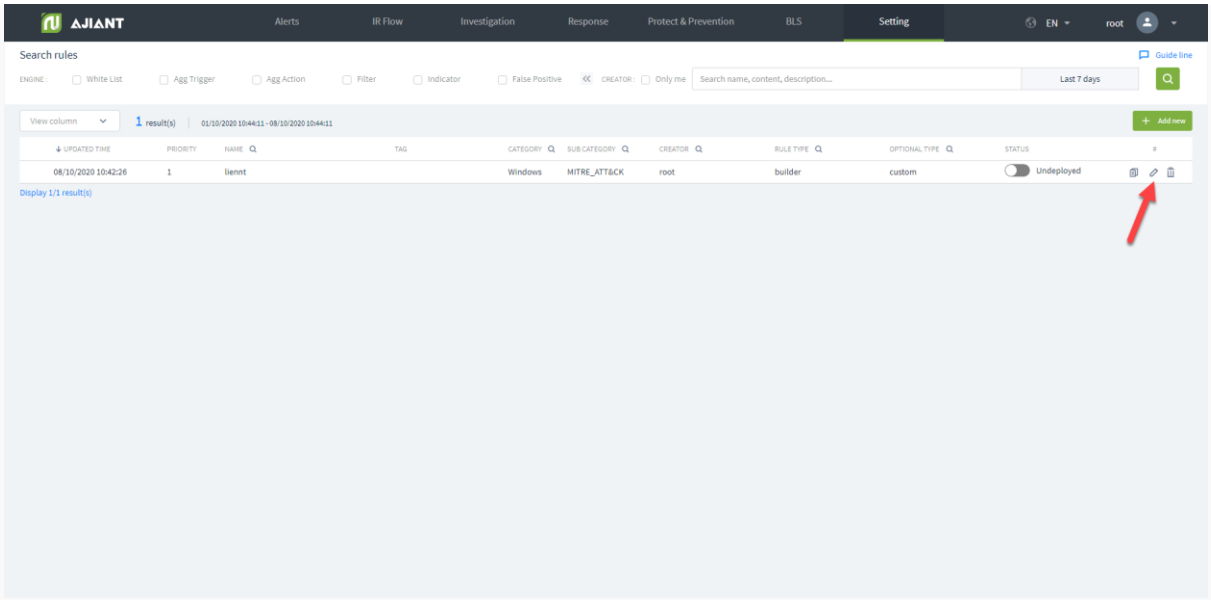


Figure 5: Screen of rule management

- Step 2: At the Edit screen, enter the information to be edited.

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

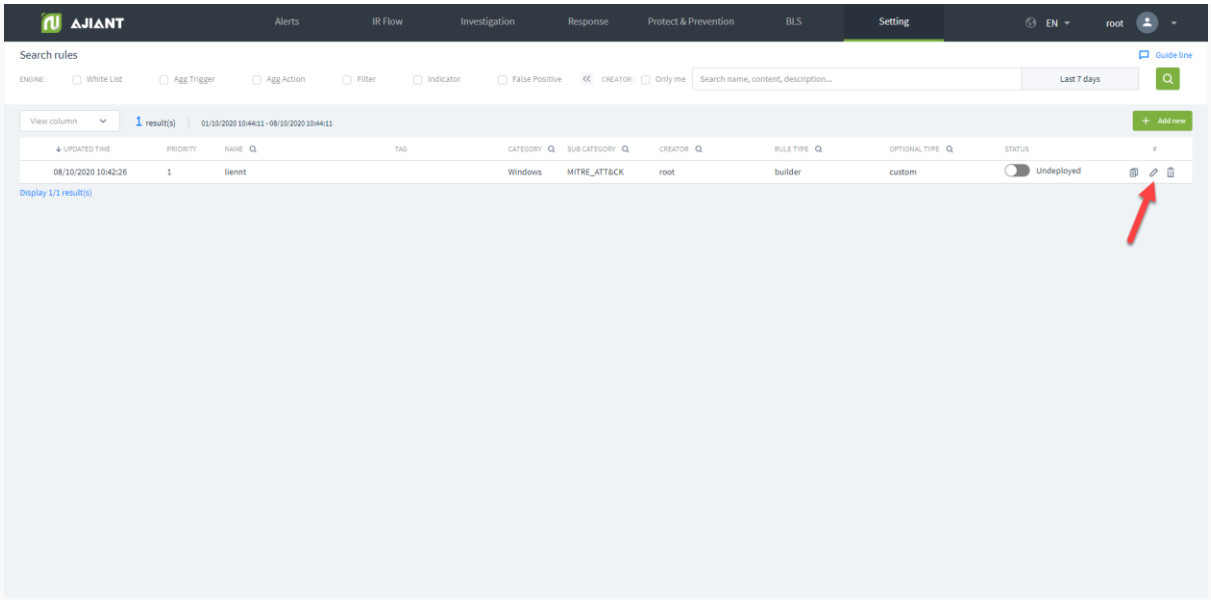


Figure 6: Detailed information screen of rule

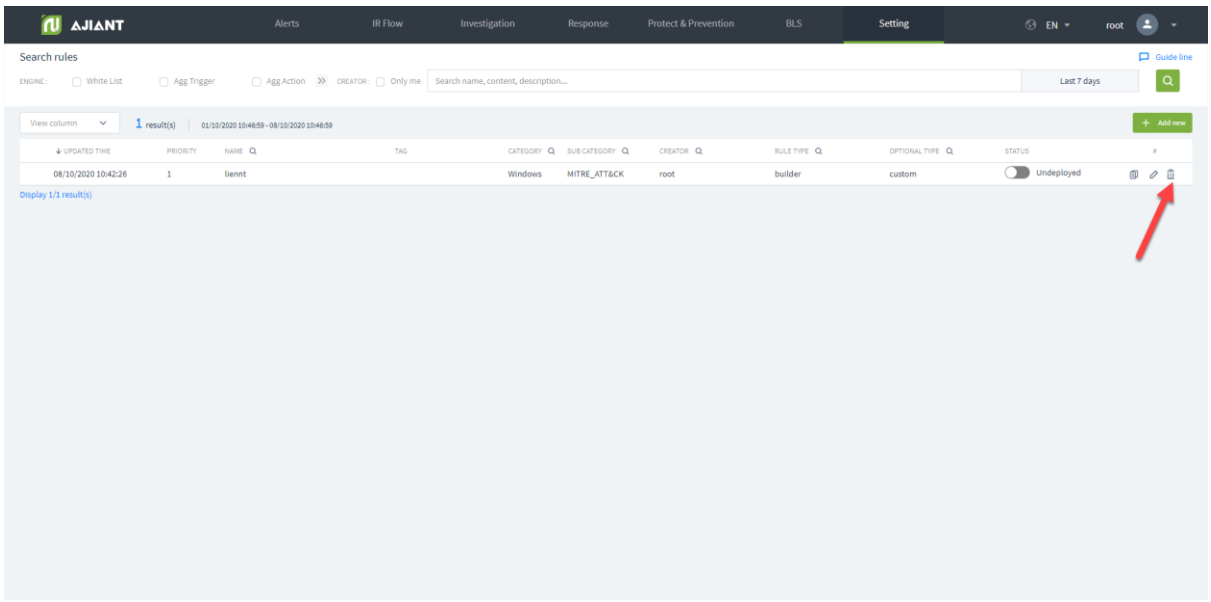
Notes: The fields of rule name, category and subcategory are non-editable fields.

- Step 3: Click on Save to save the rule on the system. When the user wants to save on the system and deploy to correlation engine at the same time, click on Save & Deploy.

For edit rules but only Save, user must click on Redeploy at the Rule Management screen for the new rule to take effect on the system.

Notes: When there is an error, user can click on Preview to view it.

10.1.4. Delete Correlation Rule



Instructions to delete a rule 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

- Step 1: Click on the Delete icon at the rule to delete.
- Step 2: The screen displays a confirmation notification to delete, select CANCEL/OK.

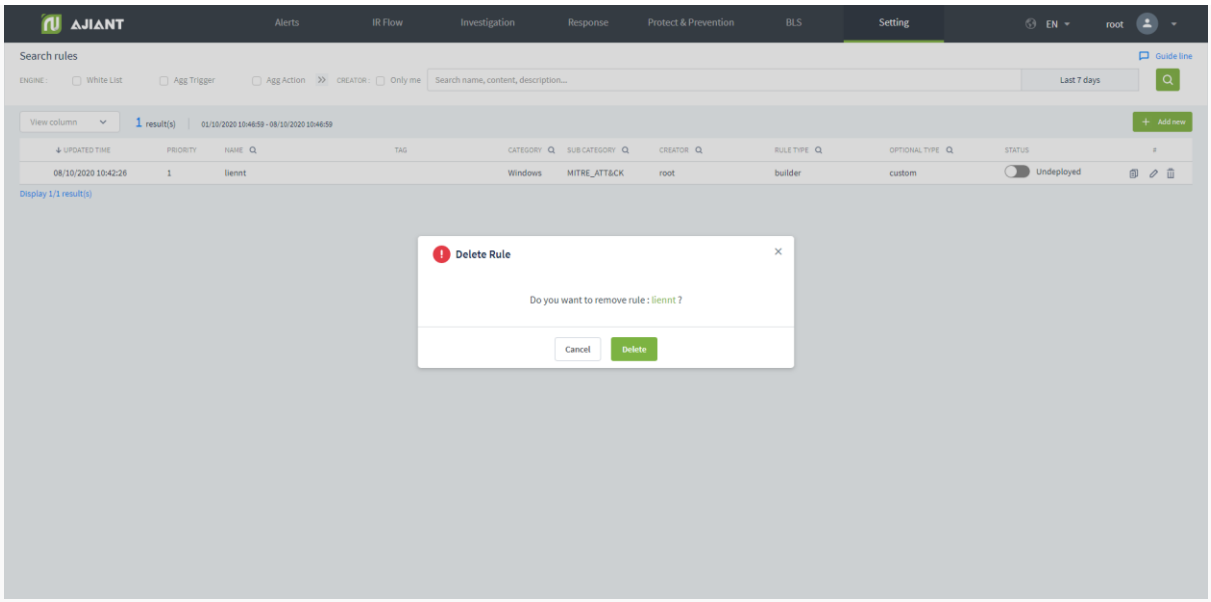


Figure 7: Confirmation popup to delete rule

If OK is selected, the selected rule will disappear from the display screen.

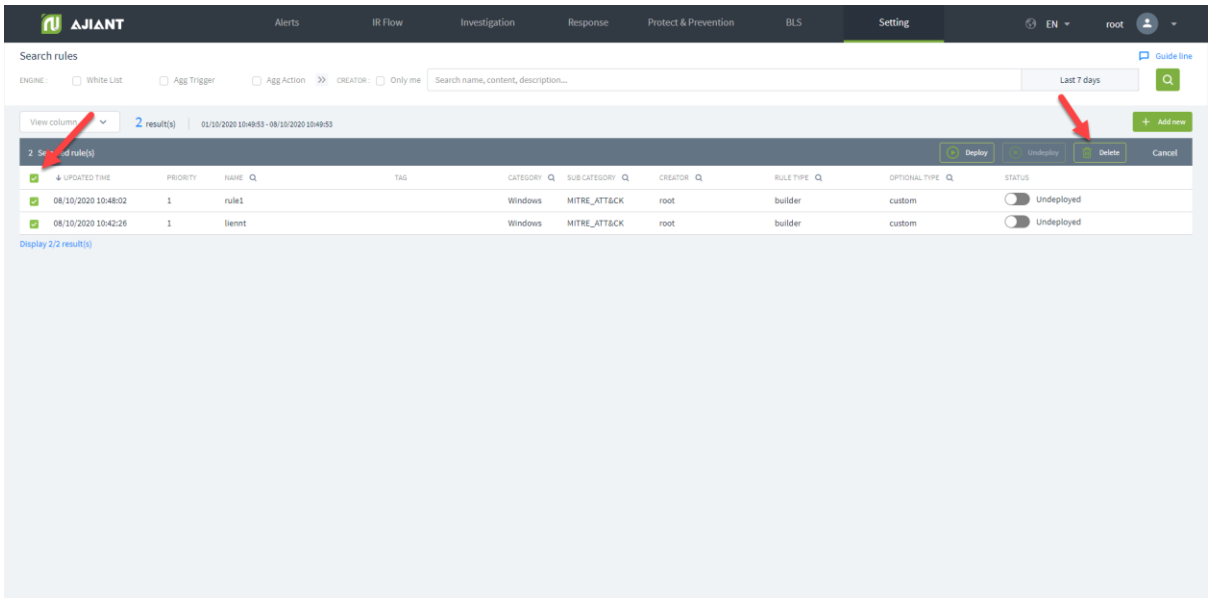


Figure 8: Screen of function to delete multiple rules at the same time

Instructions to delete multiple rules:

- Step 1: Click on the rules to delete (It is possible to delete all by clicking on Select all rules).

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: The screen displays a confirmation notification to delete, select CANCEL/OK.

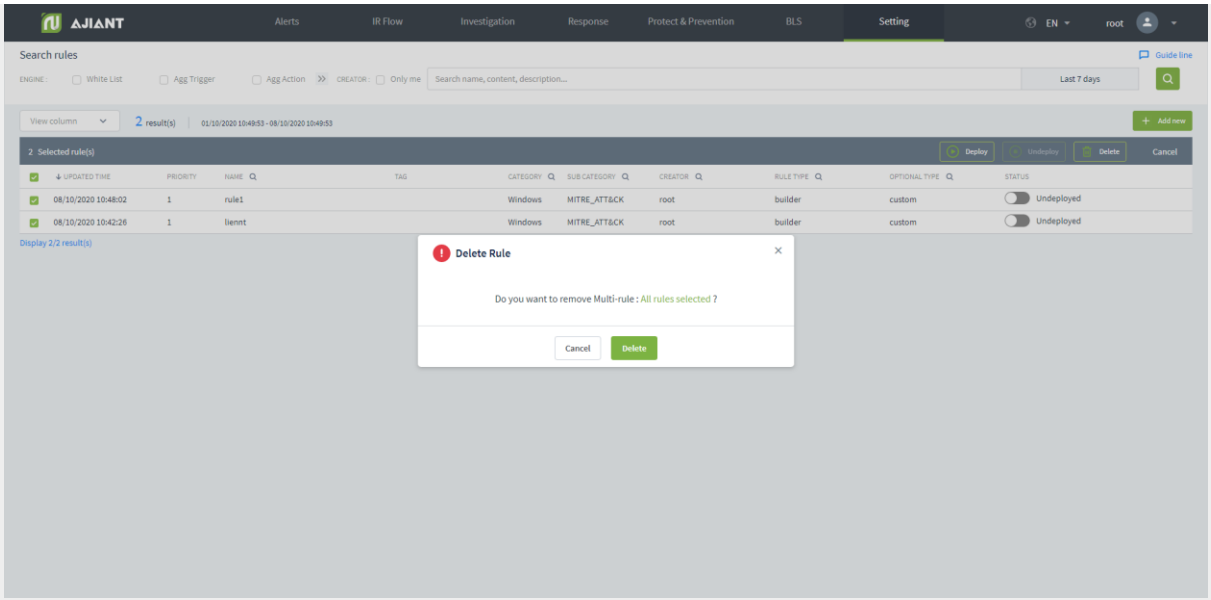


Figure 9: Confirmation screen to delete

Select OK, all rules will be removed from the display screen. Select CANCEL, the selected action will be cancelled.

3.10 Protect & Prevention

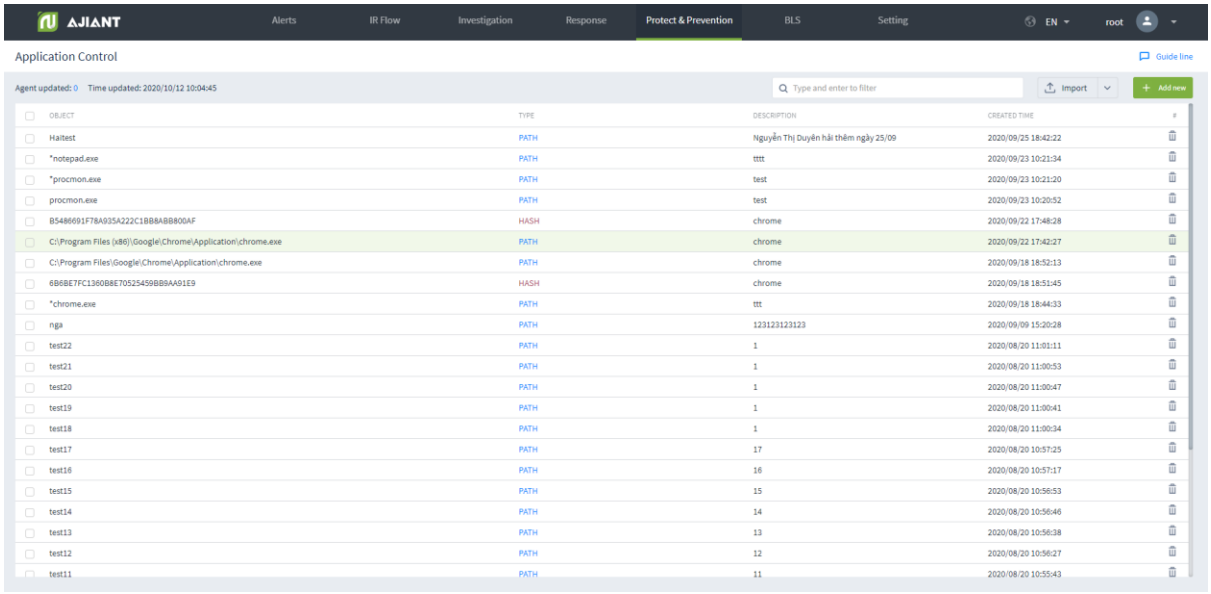
10.1.5. Application Control

The Application Control function allows configuring apps/ processes that will be blocked under the user's machine and do not allow executing. The app/process is identified based on the hash (MD5, SHA1 and SHA256) or the path.

10.1.6. Display list of blocked apps/ processes

Click on the Protect & Prevention tab → select Application control to display all applications/processes under the user's machine and not allowed to be used.

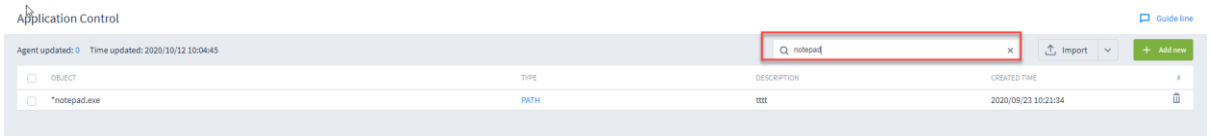
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Screen of blocked app/ process list

10.1.6.1. Search for blocked apps/processes

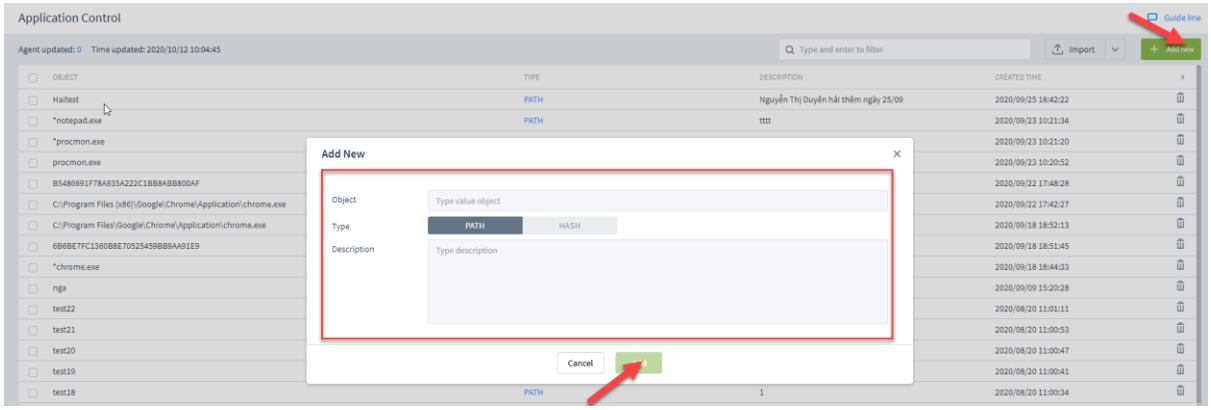
User can search by hash code or path of blocked apps.



Screen of searching for blocked apps/ processes

10.1.6.2. Add new blocked apps/ processes

Click on Add new to add a new blocked app/ process. The user can choose to block by path or hash code (MD5, SHA1, SHA256).



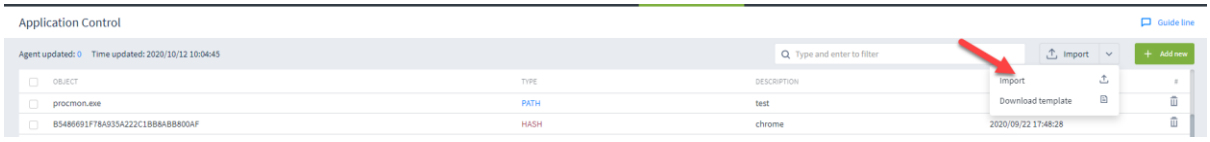
Screen of adding new blocked apps/ processes

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

10.1.6.3. Add new app/ process from existing file

Users can add new blocked applications/processes from the .csv file according to the available template to the current application list.

Click Import, select the path to the file to upload and click Open, the system will automatically add a list of applications to block on the system.

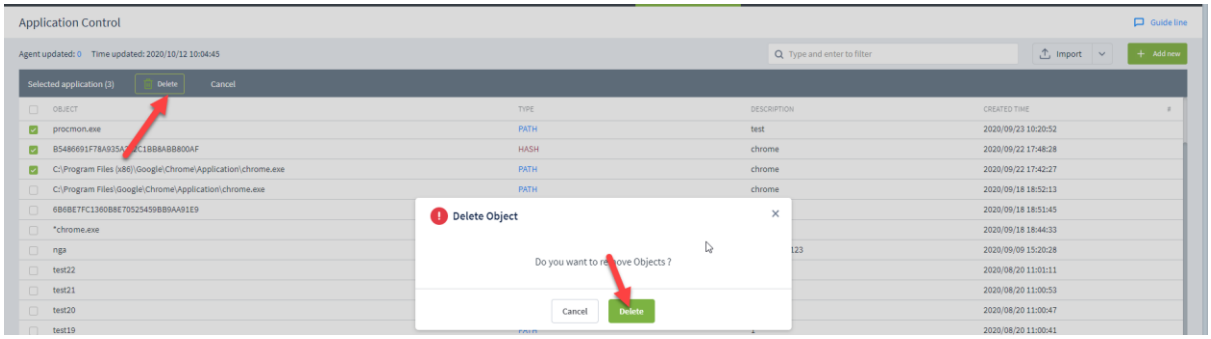


Screen of adding new apps/ processes from the existing file

10.1.6.4. Remove blocked apps/ processes from the list

The system supports deleting 1 or more blocked applications.

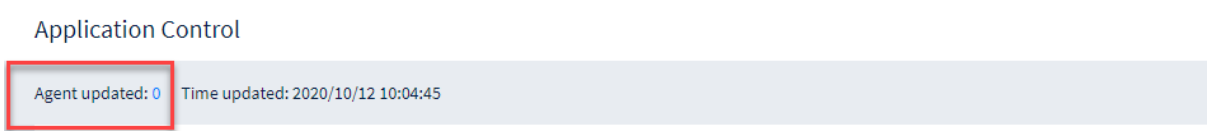
Click on each application to delete and click the Delete icon, or click the checkbox at the top of each application and click the Delete button.



Screen of removing blocked apps/ processes

10.1.6.5. Update stream to the number of agent machines with the new list successfully updated

After the user adds/modifies/deletes the list of processes on the interface, the system will update this list below agents according to the agent file update stream (every 3-minute interval). The agent receives the new configuration, generates a log with eventID = 101 and pushes it to the server, displayed on the Event Search screen. Then the system will automatically update the number of agents that have updated the new configuration list on the Application Control screen.



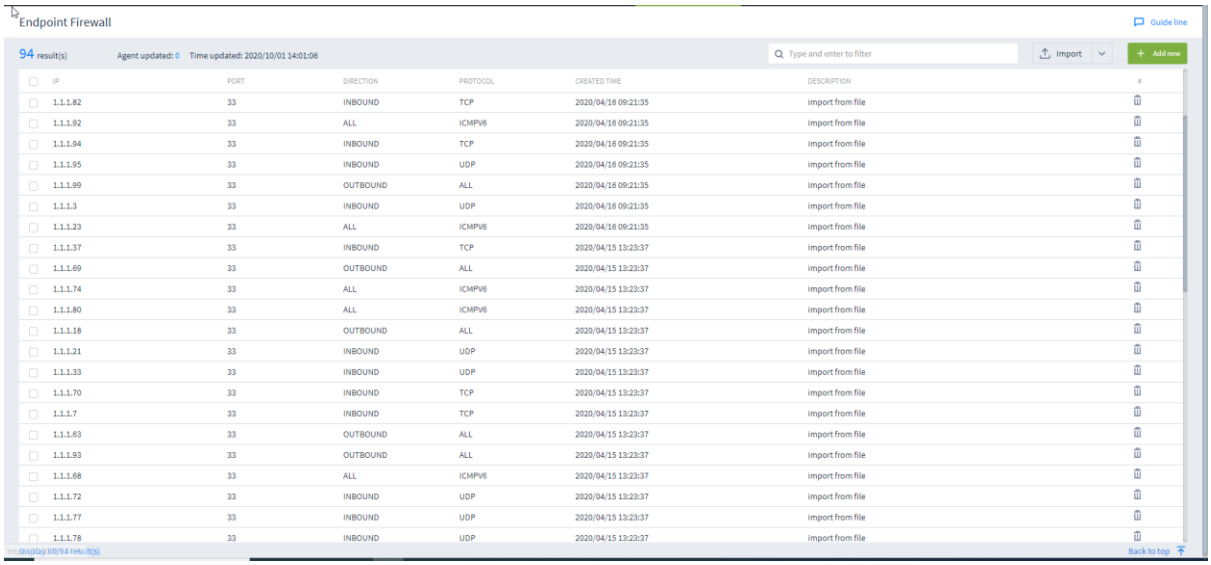
Viettel Cyber Security
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

10.1.6.6. Endpoint Firewall

Purpose: The Endpoint Firewall function allows configuring connections that will be blocked under the user's machine, including blocking by ip, port, or both ip and port, supports TCP, UDP and ICMP protocols, IPv4, IPv6, inbound and outbound connection.

10.1.6.7. Display list of blocked connections

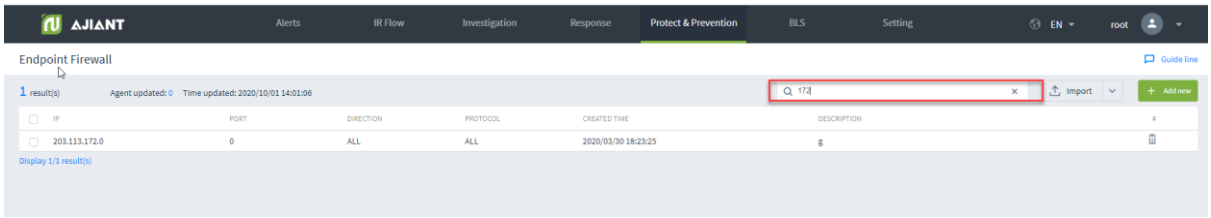
Click on the Protect & Prevention tab → Select Endpoint Firewall to display the entire list of blocked connections.



Screen of blocked connection list

10.1.6.8. Search blocked connections

Users can search by IP address and built-in port.



Screen of searching for blocked connections

10.1.6.9. Add new blocked connections

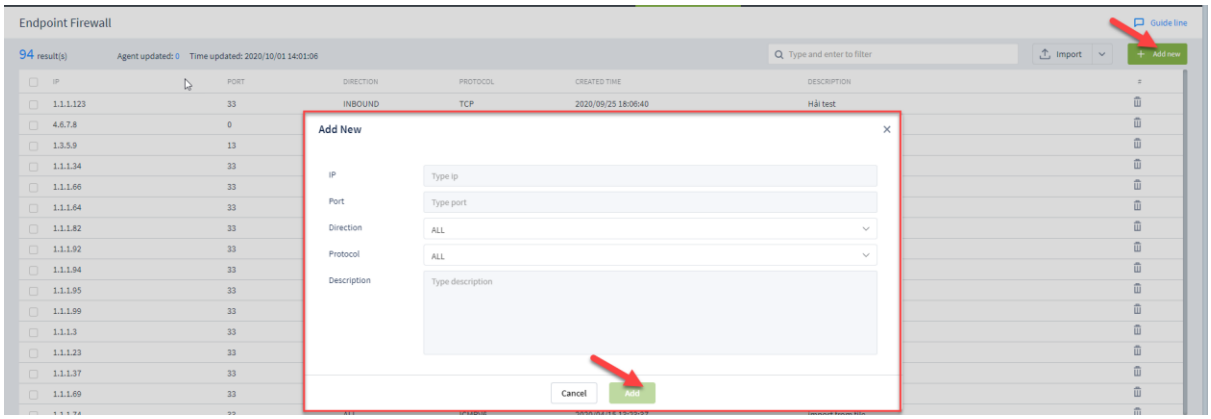
Click the Add new button, enter the information on the popup to add a new blocked connection with the following:

- IP: IP address to block
- Port: Port to block, if blocking all ports, enter 0

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

Direction: Inbound, outbound and All (block both directions)

Protocols: ICMP, TCP, UDP, ICMPV6 and ALL.

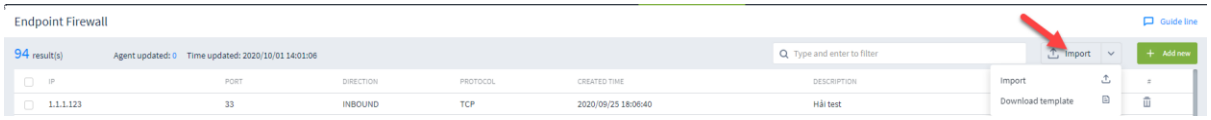


Screen of adding new blocked connection address

10.1.6.10. Add new blocked connection from existing file

Users can add new blocked apps/ processes from the .csv file according to the available template to the current application list.

Click Import, select the path to the file to upload and click Open, the system will automatically add a list of applications to block on the system.

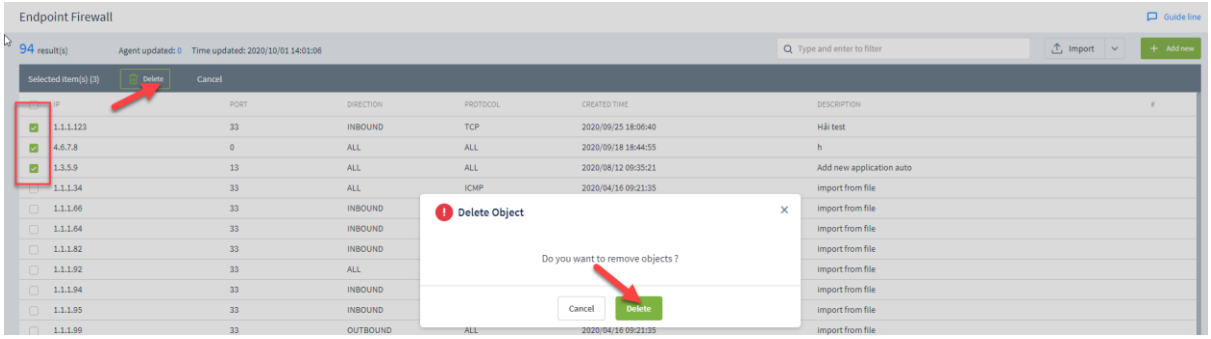


Screen of adding new apps/ processes from existing file

10.1.6.11. Delete blocked connection from the list

The system supports deleting 1 or more blocked connections.

Click on each connection to delete and click the Delete icon, or click on the checkbox at the top of each connection and click the Delete button.



Screen of deleting blocked connection

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

10.1.6.12. Update stream to the number of agent machines with the new list successfully updated

After the user adds/modifies/deletes the list of connections on the interface, the system will update this list below agents according to the agent file update stream (every 3-minute interval). The agent receives the new configuration, generates a log with eventID = 201 and pushes it to the server, displayed on the Event Search screen. Then the system will automatically update the number of agents that have updated the new configuration list on the Application Control 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