

Viettel Endpoint Detection & Response

.

.

*

.

.

.

.

(VCS-aJiant)

Version 3.3.0 EPP - 2021

Update date: 29 Nov. 2021

User Guide





Table of Contents

Terms4
1. INTRODUCTION
1.1 Current Situation
1.2 Technology Development6
1.3 VCS-aJiant6
1.4 Upgraded Information6
2. OVERVIEW
2.1 Technologies7
2.2 Infrastructure Architecture7
2.3 Work with Admin Interface8
3. INSTRUCTION TO USE10
WEB-PORTAL INTERFACE10
3.1 Login10
3.2 Dashboard VCS-aJiant (default)10
3.2.1 Action to Data12
3.2.1.1 Export Data12
3.2.1.2 Search by Date12
3.3.1.3 Refresh Data13
3.2.2 Overview Statistics

	3.2.3 Monitor Security Operation17
	3.2.4 Agent Monitoring18
	3.2.5 Monitor Risk Detection
	3.3 Anti-malware Dashboard23
	3.3.1 Action to Data24
	3.3.1.1 Export Data24
	3.3.1.2 Search by Date24
	3.3.1.3 Refresh Data25
	3.3.2 Overview Statistics
	3.3.3 Monitor Risk Detection27
	3.4 Setting Screen
	3.4.1 Agent Management30
	3.4.2 Group Management42
	3.4.3 Account Management54
	3.4.3.1 Permission management54
	3.4.3.2 Role Management55
	3.4.3.3 User management61
ļ	GENT INTERFACE
	3.5 Main
	3.6 About

 Viettel Cyber Security
 Reangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
 3

 T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com
 3



3.7 Rep	orts	67
3.8	Scan	68



Glossary

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





1. Introduction

1.1. Current Situation

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

1.2. Technology Development

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

1.3. VCS-aJiant

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

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

1.4. Upgraded Information

Version 3.3.0 provides the following new features:

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

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

2. Overview

2.1. Technologies

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

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

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

Page

2.2. Infrastructure Architecture

 Viettel Cyber Security

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com





There are 3 main components as follows:

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

2.3. Work with Admin Interface

Currently, VCS-aJiant provides 02 interfaces as follows:

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

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



viettel security

3. Instruction to Use

3.1. WEB-PORTAL INTERFACE

3.1.1. Login

• Access the system at the provided address.

	English 🗸
3#E	
	Password Password Fortort your password? Sign in
	Version 3.8.122 (noter 1.2.1.6)
	remous au Log general, Suboy © 2021 Weter Opter Security - Branch of Weter Oroup

- Login with the provided user/password.
- 3.1.2. Dashboard VCS-aJiant (default)
- Main features include as follows:

παίζα 🔟	Alerts	IR Flow	Investigation	Response	Protect & Prevention	BLS	Setting		③ EN ▼	root 🔔 🔹
Organization Dashboard							1 Export	this Dashboard	06/06/2021 - Now	⊟ ↔
Agents •	Online 7 J -1 agents	0%	Offline 43906 t +1 agents	100%	Alerts •	New 30 1 + 5 alerts	100%	Executing O Remain unch	0%	
2	t + 1 new agents Suspicious • (1) 516 t + 2 agents	+ + 30 alerts has been updated	False Positive 0 ⇒ Remain unchang	ed of	Closed 0 ⇒ Remain unch	anged				
Security Operation	tection 5									
ALERTS BY STATUS							لعلى Export data	ALERTS BY SEV	ERITY	🕹 Export data
100%										
80% -										
70% - 60% -									30	
50% -									IUIAL	

- Action to data on Dashboard
 - Extract data on Dashboard
 - Search data up to the last 90 days
 - Refresh data.
- Overview: An overview statistics of the organization's information security situation (through agent and alert state).
- Security Operation: Monitor information security operation situation (through alert operation monitor).
- \circ Agent Monitoring: Monitor installation state and agent state.
- Risk Detection: Track threats to the organization (through the statistics of the objects generating the most unprocessed alerts in the system).
- Data authorization at the features is as follows:
 - User login under root group: Display data of the entire system.
 - User login in 1 level group: Display data at all 1 level group and affiliated subgroups.
 - User login in 2 level group onwards: Display data at the entire 1 level group containing the group of the user login and the affiliated subgroups of the corresponding 1 level group.



3.1.2.1. Action to Data

3.1.2.1.1. Export Data

Allow exporting the existing data on the Dashboard interface by selecting in addition to adding the detailed data sheets to support reports.

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

3.1.2.1.2. Search by Date

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

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

Absolute time range	Relative time range
From	Last 90 days
06/06/2021	Last 60 days
Apply time range	Last 30 days
	Last 24 hours

• 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". \rightarrow 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. \rightarrow Monitoring period: 00:00 8 May 2021 to 03:00 7 June 2021.



• After selecting the time range to monitor, select Apply time range to reload the corresponding data.

3.1.2.1.3. Refresh Data

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

3.1.2.2. Overview Statistics

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



• Statistics related to agents

Statistics	Meaning
Agents • 6171 • + 19 new agents	Include 2 numbers as follows: Total number of machines with agent installed in the system (regardless of search time range) Total number of new machines with agent installed during the search time range (+: Newly installed machine, Remain unchanged: No newly installed machine during the search time range).
	Include 3 numbers as follows: Average number of online machines during the search time range (only counting working time during office hours from 08:00 - 18:00) Average number rate of online machines compared to the whole system

 Viettel Cyber Security
 Page |

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
 13

 T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com
 13



Offline

2897

-898 agents.

Suspicious g

3748

+ 1529 agents



Average number of online machines different from the previous cycle.

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

Include 3 numbers as follows:

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

Average number rate of offline machines compared to the whole system

Average number of offline machines different from the previous cycle.

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

Include 3 numbers as follows:

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

• Statistics related to alerts

61%



Include 2 numbers as follows:

Alerts 0

New

10386

-3627 alerts

466354

+ 10386 alerts has been updated Total number of alerts in whole system (regardless of search time range) Total number of new alerts generated or updated during the search time range (+: New alerts generated, Remain unchanged: No new alert generated during the search time range).

Include 3 numbers as follows:

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

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

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

Include 3 numbers as follows:

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

Pagel

15



Executing

False Positive

0

Remain unchanged

0

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

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

Include 3 numbers as follows:

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

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

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

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

Include 3 numbers as follows:

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



N%

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 Page|

16

	Rate of new alerts generated or updated
Closed	during the search time range and in the FALSE
0%	POSITIVE state compared to all new alerts
Remain unchanged	generated or updated during the search time
· · · · · · · · · · · · · · · · · · ·	range
	Total number of new alerts generated or
	updated during the search time range and in
	the FALSE POSITIVE state different from the
	previous cycle.
	(+: Total alert increased compared to the
	previous time range, Remain unchanged:
	Total number of alerts remained unchanged
	from the previous time range).

3.1.2.3. Monitor Security Operation

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

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







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

3.1.2.4. Agent Monitoring

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

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



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

 Viettel Cyber Security
 Reangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
 19

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com
 19



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

3.1.2.5. Monitor Risk Detection

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

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





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





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

P a g e |

22

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

3.1.3. Anti-malware Dashboard

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

Organization I	Dashboard (Anti-r	malware) 🔅						± Export thi	s Dashboard	0/07/2021 - Now	⊕
	INFECTED DEVICES 22 / 58 (37.9%)	Resolved 2	9%	Remained 20	91%	Ň	MALWARE	Resolved 50.9K	78%	Remained	22%
TOP INFECTED MAI	LWARE GROUPS include the largest number of	devices with detected r	nalware.								Top 5 🗸
dattest											
anhnn_test											
default											
liennt_test105											
liennt_test301											
	0	2	4 6	8	10	12	14	16 18	20	22	24
					RESOLVED	REMAINED					

• Main features include a set of as follows:

Organization	Dashboard (Anti-ı	malware) 🔅						∎±¤ 1	port this Dashboard	20/07/2021 - Now	Ö
2	INFECTED DEVICES 22/58 (37.9%)	Resolved 2	95	Remained 20	012	Ŵ	MALWARE	Resolved	785	Remained 14.6K	22%
TOP INFECTED MA Display groups that	ALWARE GROUPS t include the largest number of	f devices with detected	malware.								Top 5 🗸
dattest											
anhnn_test											
default											
liennt_test105											
liennt_test301											
	0	2	4 6	8	10	12	14	16 18	20	22	24
3					RESOLVED	REMAINED					

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





- Overview: An overview of the organization's information security situation (through the device and threat state)
- Risk Detection: Track threats to the organization (through the statistics of objects that generate the most malware in the system).
- Data authorization at the feature is as follows:
 - Allow displaying all data, not by unit.

3.1.3.1. Action to Data

3.1.3.1.1. Export Data

Allow exporting the existing data on the Dashboard interface by selecting in addition to adding the detailed data sheets to support reports.

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

3.1.3.1.2. Search by Date

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

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

Absolute time range	Relative time range
From	Last 90 days
06/06/2021	Last 60 days
Apply time range	Last 30 days
	Last 24 hours

• 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". \rightarrow 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. \rightarrow Monitoring period: 00:00 8 May 2021 to 03:00 7 June 2021.

• After selecting the time range to monitor, select Apply time range to reload the corresponding data.

3.1.3.1.3. Refresh Data

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

3.1.3.2. Overview Statistics

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



• Statistics related to agents

Statistics	Meaning
ма́у ві Láy NHIÊM 136/ 3.940 (3.5%)	Include 3 numbers as follows: Total number of infected machines in the system during the search range Total number of agent installed machines in the system (excluding search time range) Rate of infected machines compared to all agent installed machines in the system.
	Include 2 numbers as follows: Total number of infected machines in the system processed successfully





Đã giải quyết O	Rate of infected machines processed successfully compared to all infected machines in the system.
	Include 2 numbers as follows: Total number of infected machines in the system failed to process
còn lại 136	Rate of infected machines failed to process compared to all infected machines in the system.

• Statistics related to alerts

Statistics	Meaning
MĂ ĐÔC 1.960	Include 1 number as follows: Total number of malware recorded in the entire system.
Dā giarquyēt 112	Include 2 number as follows: Total number of malware in the system processed successfully Rate of malware processed successfully compared to all malware recorded on the system.
còn lai 1.848	Include 2 number as follows: Total number of malware in the system failed to process Rate of malware in the system failed to process compared to all malware recorded in the system.

 Viettel Cyber Security
 Page]

 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
 26

 T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com
 26

3.1.3.3. Monitor Risk Detection

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

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







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

 Viettel Cyber Security
 Reangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi
 28

 T: (+84) 971 360 360
 E: vcs.sales@viettel.com.vn
 W: www.viettelcybersecurity.com

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



3.1.4. Setting Screen

3.1.4.1. Agent Management

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

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

vedr →	Portal - IR Flow Detail X	VEDR Portal - Agent Managemer X 1.30.161.37/#/settings/agent-manage	VEDR Portal - Agent Manageme ement?search=eyJxdWVyeVNIYX.	≈ × + IjaCl6lilsImxpbWl0ljozNSwidGl0b	GVfZGF0ZXBpY2tlcil6lkFMRVJULlcxBU1RfU0V	WRU5fREFZIiwia2V5X3RpbWUiOiJsYXN	10X3NIdmVuX2RheSIsImIudGVydmFsX3Rpb.	୍ - ଟ ଚନ୍ତି ଚ ାପ :
	VEDR Portal		Alerts	IR Flow Inv	vestigation Response	Setting	⊕ en -	nhandt4 😩
ent l	Management o search agent		(2	2)				9
5 resu	ult(s)	(5)					View co	lumn
0	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	DNS	POLICY
	DESKTOP-EGANUBQ	Online	No_group	Release	20/05/2019 16:47:07	17/04/2019 10:16:46	192.168.4.222,192.168.4.111	test_sample
	ThanhLN-PC	Online	No_group	Release	20/05/2019 16:47:01	13/03/2019 13:30:45	192.168.4.222,192.168.4.111	test_sample
	Nhandt4-PC	 Online 	No_group	Release (1)	20/05/2019 16:46:45	13/03/2019 13:05:22	192.168.4.111	test_sample
A	Chuyennt2-ViettelOS	Offline	No_group	Release	20/05/2019 16:35:19	22/04/2019 16:56:49	192.168.4.222,192.168.4.11	(4)
	DESKTOP-HHN2B1Q	Offline	No_group	Release	20/05/2019 13:43:08	05/11/2018 14:21:48	192.168.4.111,192.168.4.2	test_sample
	W(3) gNC9	Offline	No_group	Release	16/05/2019 18:41:25	25/03/2019 17:38:14	192.168.129.2	test_sample
	Halpy-PC	Offline	No_group	Release	14/05/2019 15:27:58	01/04/2019 17:11:43	192.168.253.2	test_sample
	Thanhln9-VirtualBox	Offline	No_group	Test	03/05/2019 15:48:57	11/03/2019 14:30:07	192.168.4.222,192.168.4.111	N/A
	Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10	29/01/2019 04:57:35	192.168.4.222	test_sample
	Chuyennt2-ViettelOS-Test	Offline	No_group	Release	22/04/2019 16:46:52	22/04/2019 15:36:41	192.168.4.222,192.168.4.111	N/A
	Thanhin9-VirtualBox	Offline	No_group	Test	20/04/2019 10:36:54	13/03/2019 09:01:48	192.168.4.222,192.168.4.111	N/A
	DESKTOP-6C8PVCE	Offline	No_group	Release	01/04/2019 18:51:50	05/11/2018 14:42:16	192.168.11.2	test_sample
	Halpv-PC	Offline	No_group	Release	01/04/2019 16:00:13	13/03/2019 11:50:06	192.168.253.2	test_sample
	DESKTOP-U808HAB	Offline	No_group	Release	29/03/2019 15:48:06	12/03/2019 18:29:01	192.168.4.222,192.168.4.111	test_sample
	ThanhLN9-PC	Offline	No_group	Release	26/03/2019 17:48:49	21/03/2019 13:31:53	192.168.4.222,192.168.4.111	N/A
	DESKTOP-J1VS222	Offline	No_group	Release	02/03/2019 22:54:03	19/02/2019 16:09:27	192.168.4.111,192.168.4.222	test_sample
	DESKTOP-7NLS4D0	Offline	No_group	Release	28/02/2019 16:30:14	22/02/2019 10:53:15	192.168.4.111	test_sample
	ANM-THANHLN9	Offline	No_group	Test	15/02/2019 08:35:41	29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample
	WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41	08/11/2018 10:55:46	192.168.129.2	test_sample
	ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35	19/01/2019 09:45:19	192.168.4.111,192.168.4.222	test_sample

The system support performing the following features:

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

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

	🖸 VIDA Rond - IA Rov Deal x 🔯 VIDA Rond - Agent Manageme: x 👔 VIDA Rond - Agent Manageme: x 🕴 + - 🗸 🖉										
\leftarrow		C 🞧 🔺 Not secure 10.30	0.161.37/#/settings/agent-manage	ement?search=eyJxdWVyeVNIYXJ	jaCl6lilsImxpbWl0ljozNSwidGl0b	GVfZGF0ZXBpY2tlcil6lk	FMRVJULIxxBU1RfU0VV	VRU5fREFZliwia2V5X3RpbWUiOiJsYXN	X3NIdmVuX2RheSIsImIudGVydmFsX3Rpb	O 🕁 😍 🧔	Θ 🛓 😫
								Setting		nhandt4	. -
Ag	ent M	lanagement					-				
h	ypeto	search agent								0	Q
	D	AgentID			Agent ID						
											~
	e la compañía de la c	ComputerName			Agent Computer Name						
•	BD	OS			Agent Operating System						1.1
•		Architecture			Agent Architecture	"Ռոյ					
	Ð	Platform			Agent Platform	0					
		Nhandt4-PC	Offline	No_group	Release	20/05/2019 17:02:46		13/03/2019 13:05:22	192.168.4.111	test_sample	
		Chuyennt2-ViettelOS	Offline	No_group	Release	20/05/2019 16:35:19		22/04/2019 16:56:49	192.168.4.222,192.168.4.111	N/A	
		DESKTOP-HHN2B1Q	Offline	No_group	Release	20/05/2019 13:43:08		05/11/2018 14:21:48	192.168.4.111,192.168.4.222	test_sample	
		Hajpy-PC	Offline	No_group	Release	14/05/2019 15:27:58		01/04/2019 17:11:43	192.168.253.2	test_sample	
		Thanhing-VirtualBox	Offline	No_group	Test	03/05/2019 15:48:57		11/03/2019 14:30:07	192.168.4.222,192.168.4.111	N/A	
		Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10		29/01/2019 04:57:35	192.168.4.222	test_sample	
		Chuyennt2-ViettelOS-Test	Offline	No_group	Release	22/04/2019 16:46:52		22/04/2019 15:36:41	192.168.4.222,192.168.4.111	N/A	
		Thanhing-VirtualBox	Offline	No_group	Test	20/04/2019 10:36:54		13/03/2019 09:01:48	192.168.4.222,192.168.4.111	N/A	
		DESKTOP-6C8PVCE	Offline	No_group	Release	01/04/2019 18:51:50		05/11/2018 14:42:16	192.168.11.2	test_sample	_
		Haipy-PC	Offline	No_group	Release	01/04/2019 16:00:13		13/03/2019 11:50:06	192.168.253.2	test_sample	
		DESKTOP-USOBHAB	Offline	No_group	Release	29/03/2019 15:48:06		12/03/2019 18:29:01	192.168.4.222,192.168.4.111	test_sample	
		ThanhLN9-PC	Offline	No_group	Release	26/03/2019 17:48:49		21/03/2019 13:31:53	192.168.4.222,192.168.4.111	N/A	
		DESKTOP-J1VS222	Offline	No_group	Release	02/03/2019 22:54:03		19/02/2019 16:09:27	192.168.4.111,192.168.4.222	test_sample	
		DESKTOP-7NLS4D0	Offline	No_group	Release	28/02/2019 16:30:14		22/02/2019 10:53:15	192.168.4.111	test_sample	
		ANM-THANHLN9	Offline	No_group	Test	15/02/2019 08:35:41		29/01/2019 04:45:08	192.168.4.222,192.168.4.111	test_sample	
		WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41		08/11/2018 10:55:46	192.168.129.2	test_sample	
		ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35		19/01/2019 09:45:19	192.168.4.111,192.168.4.222	test_sample	
Dis	play 3	5/35 result									

• Examples of search statements as follows:

Search by the condition "=":

$\in \ \ni$	C 🕞 🔺 Not secur	re 10.30.161.37/#/settings/agent-mana	gement?search=ey/xdWV/yeVNIY	XJjaCl6lkFnZW50SUQgPSB	clj8BOTEzNTY4QjQ4RUQyNDZI	MjBFOTYwNjBGRjIDOI	DJERjdFNDkxMjhcliAiLCJsaW	/1pdCl6MSwidGl0bGVfZGF0ZX8pY2tlcil6lk	FMRVJULk	⊘☆♥ 👂	θ	· 🔟 🧧
						Response	Setting			nhandt4	٠	
Agent	Management											
Agenti	D = "0A913568B48ED246E2	20E96060FF9C82DF7E49128*								4	9	Q
1 result	t(s)								View colu	umn		~
	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	E	FIRST PING	DNS		POLICY		
	ANM-NHANDT4	Offline	No_group	Test	18/12/2018 10:37:10		12/12/2018 09:06:04	192.168.4.222		test_sample		
Display	1/1 result											

Search by the condition "!=":





$\in \ \rightarrow$	C 🝙 🔺 Not secure 10	.30.161.37/#/settings/agent-ma	nagement?search=eyJxdWVyeVNN	XJjaCl6lkFnZW50SUQgIT0	lgXClwQTlotMzU2OEl0OEVEMj	Q2RTIwRTk2MDYwRkY5	QzgyREY3RTQ5MTI4XCIgIi	wibGltaXQiOjM0LCJ	0aXRsZV9kYXRlcGljaZVyljoiQUxFL	🗆 🛇 会 👽 👂 🛛 🖯 🔶 🛓 😫
							Setting			nhandt4 👱 👻
Agent	Management					***				
Agenti	D != "0A913568B48ED246E20E960	50FF9C82DF7E49128"								0
34 res	ult(s)								View	column 🗸
	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	6	FIRST PING		DNS	POLICY
	DESKTOP-EGANUBQ	Online	No_group	Release	24/05/2019 10:42:43		17/04/2019 10:16:46		192.168.4.222,192.168.4.111	test_sample
	Thanhin9-VirtualBox	Offline	No_group	Test	24/05/2019 09:17:22		11/03/2019 14:30:07		192.168.4.222,192.168.4.111	N/A
	Nhandt4-PC	Offline	No_group	Release	23/05/2019 16:44:37		13/03/2019 13:05:22		192.168.4.111	test_sample
	Thanhin9-VirtualBox	Offline	No_group	Test	22/05/2019 14:32:00		13/03/2019 09:01:48		192.168.4.222,192.168.4.111	N/A
	ThanhLN-PC	Offline	No_group	Release	22/05/2019 09:26:27		13/03/2019 13:30:45		192.168.4.222,192.168.4.111	test_sample
	Win7-CongNC9	Offline	No_group	Release	21/05/2019 18:19:26		25/03/2019 17:38:14		192.168.129.2	test_sample
	Chuyennt2-ViettelOS	Offline	No_group	Release	21/05/2019 16:04:51		22/04/2019 16:56:49		192.168.4.222,192.168.4.111	N/A
	DESKTOP-HHN2B1Q	Offline	No_group	Release	21/05/2019 15:18:40		05/11/2018 14:21:48		192.168.4.111,192.168.4.222	test_sample
	Haipv-PC	Offline	No_group	Release	14/05/2019 15:27:58		01/04/2019 17:11:43		192.168.253.2	test_sample
	Win7x64-PC	Offline	No_group	Release	25/04/2019 09:31:10		29/01/2019 04:57:35		192.168.4.222	test_sample
	Chuyennt2-ViettelOS-Test	Offline	No_group	Release	22/04/2019 16:46:52		22/04/2019 15:36:41		192.168.4.222,192.168.4.111	N/A
	DESKTOP-6C8PVCE	Offline	No_group	Release	01/04/2019 18:51:50		05/11/2018 14:42:16		192.168.11.2	test_sample
	Haipy-PC	Offline	No_group	Release	01/04/2019 16:00:13		13/03/2019 11:50:06		192.168.253.2	test_sample
	DESKTOP-U808HAB	Offline	No_group	Release	29/03/2019 15:48:06		12/03/2019 18:29:01		192.168.4.222,192.168.4.111	test_sample
	ThanhLN9-PC	Offline	No_group	Release	26/03/2019 17:48:49		21/03/2019 13:31:53		192.168.4.222,192.168.4.111	N/A
	DESKTOP-J1VS222	Offline	No_group	Release	02/03/2019 22:54:03		19/02/2019 16:09:27		192.168.4.111,192.168.4.222	test_sample
	DESKTOP-7NLS4D0	Offline	No_group	Release	28/02/2019 16:30:14		22/02/2019 10:53:15		192.168.4.111	test_sample
	ANM-THANHLN9	Offline	No_group	Test	15/02/2019 08:35:41		29/01/2019 04:45:08		192.168.4.222,192.168.4.111	test_sample
	WIN10-CONGNC9	Offline	No_group	Release	25/01/2019 09:35:41		08/11/2018 10:55:46		192.168.129.2	test_sample
	ANM-HIEUPC4	Offline	No_group	Release	22/01/2019 11:25:35		19/01/2019 09:45:19		192.168.4.111,192.168.4.222	test_sample

Search by the condition "~":

🗧 🔿 🖸 🎧 🚺 NO 1800/ 1030.16137/9/settings/spect-management/search-syludWys/NRVS_CIGNMARX8160/y1RrZ581288%-CUSMCICCoaW1p3C16Maid60804/2C0289/28086AfMRVULubU1RDWRUSEUS728ab2533bbWUOU0000000C 🖉 🖓 👂 😝 🔒 😆												
							Setting				nhandt4	•
Agent M	Management											
Compu	iterName ~ "ANM"										9	Q
6 result	:(s)									View colur	mn	~
	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	0	FIRST PING		DNS		POLICY	
	ANM-THANHLN9	Offline	No_group	Test	15/02/2019 08:35:41		29/01/2019 04:45:08		192.168.4.222,192.168.4.1	11	test_sample	
	ANM-HIEUPC4	 Offline 	No_group	Release	22/01/2019 11:25:35		19/01/2019 09:45:19		192.168.4.111,192.168.4.2	22	test_sample	
	ANM-NHANDT4	Offline	No_group	Test	18/12/2018 10:37:10		12/12/2018 09:06:04		192.168.4.222		test_sample	
	ANM-CONGNC9	Offline	No_group	Alpha	03/12/2018 15:01:10		30/11/2018 16:13:13		192.168.4.222,192.168.4.1	.11	test_sample	
	ANM-PHUOCNM2	Offline	No_group	Alpha	03/12/2018 14:31:13		30/11/2018 16:12:38		192.168.4.222,192.168.4.1	11	test_sample	
	ANM-CONGNC9	Offline	N/A	N/A	N/A		N/A		192.168.129.2		N/A	
Display 6	5/6 result											
Display 6	ANM-CONGNC9 5/6 result	Offline	N/A	N/A	N/A		N/A		192.168.129.2		N/A	

Search by AND match criteria:

$ \in \rightarrow $	C 🞧 🔺 Not secur	e 10.30.161.37/#/settings/	/agent-management?search	i=eyJxd₩VyeVNIYX	JjaCl6lkNvbX81dGV	yTmFtZSB%2BIFwiQU5NXClgQ	QU5EIFBsYX	Rmb3JtlD0gXCJN	aWNyb3NvZnQgV2luZ	393 cy AxMCBQ cm9cliAiLCJ saW1p	dCI6MiwidGI0b	GVIZGFOZ (0 1 1 1	θ	± 8
								sponse	Setting				nhandt4		
Agent	Management														
Comp	terName ~ "ANM" AND Plat	form = "Microsoft Windows 10 Pr	0"										-3		Q
2 result	(\$)											View colum	n		~
	NAME	STATUS	GROUP	UPDATE	GROUP	LAST PING		FIRST PING		DNS	POLICY		PLATFORM		
	ANM-CONGNC9	Offline	No_group	Alpha		03/12/2018 15:01:10		30/11/2018 16:1	3:13	192.168.4.222,192.168.4.111	test_sample		Microsoft Wine	dows 10 P	Pro
	ANM-CONGNC9	Offline	N/A	N/A		N/A		N/A		192.168.129.2	N/A		Microsoft Wint	dows 10 P	ro
Display	l/2 result														
Display	l/2 result														

Search by OR match criteria:



									Settin	g			nhandt4	
ent N	lanagement													
omput	erName ~ "ANM" OR Platforr	n = "Microsoft Windows 10	Pro*										Ð	0
resu	it(s)											View column	1	
	NAME	STATUS	GROUP	UPDATE GROUP	D LAST P	ING	E F	IRST PING		DNS	POLICY	PLATFORM		
	DESKTOP-EGANUBQ	Online	No_group	Release	24/05/2	019 10:50:45	1	7/04/2019 10:16:46		192.168.4.222,192.168.4.111	test_sample	Microsoft W	indows 10 Pro	
	DESKTOP-HHN2B1Q	Offline	No_group	Release	21/05/2	019 15:18:40	0	15/11/2018 14:21:48		192.168.4.111,192.168.4.222	test_sample	Microsoft W	indows 10 Pro	
	DESKTOP-6C8PVCE	Offline	No_group	Release	01/04/2	019 18:51:50	0	15/11/2018 14:42:16		192.168.11.2	test_sample	Microsoft W	indows 10 Pro	
	DESKTOP-U808HAB	Offline	No_group	Release	29/03/2	019 15:48:06	1	2/03/2019 18:29:01		192.168.4.222,192.168.4.111	test_sample	Microsoft W	indows 10 Pro	
	DESKTOP-J1VS222	Offline	No_group	Release	02/03/2	019 22:54:03	1	9/02/2019 16:09:27		192.168.4.111,192.168.4.222	test_sample	Microsoft W	indows 10 Pro	
	ANM-THANHLN9	Offline	No_group	Test	15/02/2	019 08:35:41	2	9/01/2019 04:45:08		192.168.4.222,192.168.4.111	test_sample	Microsoft W	indows 10 Enterp	rise
	WIN10-CONGNC9	Offline	No_group	Release	25/01/2	019 09:35:41	0	08/11/2018 10:55:46		192.168.129.2	test_sample	Microsoft W	indows 10 Pro	
	ANM-HIEUPC4	Offline	No_group	Release	22/01/2	019 11:25:35	1	9/01/2019 09:45:19		192.168.4.111,192.168.4.222	test_sample	Microsoft W	indows 7 Enterpr	ise Serv
	ANM-NHANDT4	Offline	No_group	Test	18/12/2	018 10:37:10	1	2/12/2018 09:06:04		192.168.4.222	test_sample	Microsoft W	indows 10 Enterp	rise
	ANM-CONGNC9	Offline	No_group	Alpha	03/12/2	1018 15:01:10	3	0/11/2018 16:13:13		192.168.4.222,192.168.4.111	test_sample	Microsoft W	indows 10 Pro	
	ANM-PHUOCNM2	Offline	No_group	Alpha	03/12/2	018 14:31:13	3	0/11/2018 16:12:38		192.168.4.222,192.168.4.111	test_sample	Microsoft W	indows 10 Enterp	rise
	DESKTOP-OMETRIE	Offline	No_group	Release	30/11/2	018 14:10:30	3	0/11/2018 14:04:16		192.168.4.111,192.168.4.222	test_sample	Microsoft W	indows 10 Pro	
	DESKTOP-3QTIL7P	Offline	No_group	Release	26/11/2	018 15:31:19	1	7/11/2018 17:11:19		8.8.8.8,8.8.4.4	test_sample	Microsoft W	indows 10 Pro	
	ANM-CONGNC9	Offline	N/A	N/A	N/A			4/A		192.168.129.2	N/A	Microsoft W	indows 10 Pro	

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

1	U AJIANT			Investigation		evention Setting	😚 EN 🕶	root 💄 🗸
Agent I	Management							
Type to	o search agent						First Ping 🔛	Last Ping 🖨 📿
33 resu	ilt(s)						÷	View column 🗸
Selecte	rd (3) Set Policy Move to group	Set update group Can	cel					
	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY
	DESKTOP-4C6V54I	Offline	Test_scan_ip	Test	22/05/2020 15:46:14	15/05/2020 17:38:55	10.61.188.2	Agent Performance
	ThanhLN9-PC	Offline	Liennt_group1	Alpha	25/05/2020 15:05:57	21/03/2019 13:31:53	10.61.188.2	bls_test
	HuyHV-PC	Offline	Test_scan_ip	Test	25/05/2020 14:40:55	31/01/2020 17:23:19	10.61.188.2	Agent Performance
	Win7-32bit-PC	Offline	Test_scan_ip	Test_ping	11/05/2020 10:41:10	22/04/2020 17:00:46	10.61.188.2	huyhv-2211
	WIN-MM956VNPD90	Offline	Liennt_group2.1	Release	07/05/2020 09:56:40	07/05/2020 09:39:04	10.61.188.2	N/A
	Chuyennt2-ViettelOS	Offline	Default	Release	18/05/2020 13:31:13	18/05/2020 11:16:38	10.61.188.2	default
	DESKTOP-BGH8QIG	Offline	Default	Alpha	07/05/2020 14:28:53	24/07/2019 13:44:07	10.61.188.2	full_features
	DESKTOP-LRT7Q4L	Offline	Anm	Release	22/05/2020 17:23:55	17/01/2020 18:39:40	10.61.188.2	huyhv_15.01.ProPre
	LienNT-TestPC	Offline	Liennt_group1.1	Release	25/05/2020 14:30:29	21/05/2020 11:42:22	10.61.188.2	N/A
	Ubuntu18x64chuyennt	Offline	Default	Beta	18/05/2020 15:32:16	29/10/2019 10:50:34	10.61.188.2	Agent Performance
	WIN-OH33SL4BBRJ	 Offline 	Test_scan_ip	Beta	19/05/2020 15:20:57	17/12/2019 13:36:53	10.61.188.2	hieupc4
	Win7-32bit-PC	Offline	Test_scan_ip	Test	08/05/2020 18:17:53	25/02/2020 17:38:33	10.61.188.2	Agent Performance
	Ubuntuhyperv-Virtual-Machine	Offline	Default	Release	06/05/2020 10:50:39	25/02/2020 17:03:22	10.61.188.2	test
	ThanhLN-PC	Offline	Default	Test	18/05/2020 13:29:01	13/03/2019 13:30:45	10.61.188.2	Agent Performance
	Localhost.Localdomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29	01/04/2020 14:38:38	10.61.188.2	centos
	DESKTOP-EGANUBQ	Online	Test_scan_ip	Test	25/05/2020 15:30:51	08/05/2020 22:16:52	10.61.188.2	full_features
	DESKTOP-315SAGT	Offline	Liennt_group1.1	Release	25/05/2020 14:38:40	19/08/2019 17:18:19	10.61.188.2	huyhv_15.01.ProPre

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

Selecte	ed (1)	Set Policy <u>Cancel</u>	
	NAME	Policy	UP
	Nhand	test_sample	group
	Win7-C	Set Policy	group
	<u>Thanh</u>		group

• Result after setting policy:







- Delete the action on the Multi-selected screen
- View Column: Configure the display of columns at will:

	4	6	View column	~
0				
Searc	n in dropdown l	ISt		
	Select all			
~	Name			
\checkmark	Status			
\checkmark	Group			
\checkmark	Update group			
\checkmark	Last ping			
~	First ping			
~	IP DCN			
\checkmark	Policy			
	AgentID			
	Platform			
	Platform Versi	on		
	Architecture			
	DNS			
~	Version			

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

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

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



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

TIANT 🚺	📶 AJIANT			n		() en	i + root 😩 +	
Agent management			Agent ID 4030C72A35250	00B939BC065533A18B6F6A5B006E				Guidelines
Version = "3.0.30"			First ping: 24/05/2021 03	:47:46 Last ping: 09/06/2021 14:56:58			First Ping	Last Ping 🖨 📿
			Agent properties					
13 result(s)			SET POLICY	enhance alert chuven	~		🛃 Vier	w column 🗸 🗸
NAME	STATUS	GRO	SET LIPOATE GROUP				POLICY	VERSION
C VCS	Offline	Def	SET OF BATE GID OF	release	~		default	3.0.30
Nextcloud	Offline	Dat	MOVE TO GROUP	default	~		default	3.0.30
Win7x86chuyentest	Online	Def		Save			enhance_alert_chuyen	3.0.30
ANM-CHUVENNT2	Online	Def	General info Installati	on Files Version Installed Certificates Scheduled Tasks	Disks & partitions Environm	ment variables installed software Required software	enhance_alert_chuyen	3.0.30
Ubuntu18x64chuye	nnt © Offline	Date	General Into Installato	Streament installed Certificates Scheduled lasts	oraka er partitiona environi	Prene variablea instance abrevare insequires abrevare	full_features_centos	3.0.30
Test SeaBank khai	t <u>b_v1</u> ⊚ Offline	Def	General info		Network Interfaces		full_features	3.0.30
DESKTOP-EGANUB	© Offline	Def	HOST NAME	ANM-CHUYENNT2	IP V4	192.168.56.1 fe80:re4a1:11cd:da1c:903e	enhance_alert_chuyen	3.0.30
DESKTOP-RUMB30	© Offline	Def	HOSTID	495db28b-db32-4a1e-bb6c-f21a787391e7	MAC	0a:00:27:00:00:0e	anhnn19_test_load_image	3.0.30
Win7x86-A-PC	 Offline 	Def	SETUP VERSION	N/A	NAME	VirtualBox Host-Only Network	full_features	3.0.30
	Online	Def	OPERATING SYSTEM	windows	IP V4 IP V6	fe80:618d:od15:12b0:c554	full_features	3.0.30
ThanhLN-PC	Offline	Def	PLATFORM	Microsoft Windows 10 Enterprise	MAC	90cdtb6(51:31:4f	full_features_thanhin9	3.0.30
<u>Win10x64</u>	Offline	Dat	The ATTOONN OF THE OWNER	to a topat Rudul topat	IP V4	160 254 08 5	full_features_server	3.0.30
Win7x64-A-PC	Online	Def	POR PORM VERSION	200.13041 0010 13041	IP V6	fe80::149f:a428:11ce:6205	anhnn19_test_load_image	3.0.30
Display 13/13 result			PLATFORM FAMILY	Standaione Workstation	MAC	12:od:b6:51:31:4f		
			ARCHITECTURE	amd64	Default Gateway			
			PHYSICAL MEMORY	16,777,216	192.168.8.1			
			CPUs		DNS Server			
			CORES	8	192.168.4.222			
			MODEL NAME	1408.000000 Intel(R) Core(TM) 17-6700 CPU @ 3.40GHz	192 168 4 111			
			VENDOR ID	GenuineIntel				

Installation Files Version Tap

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

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

📶 АЈІАНТ		Agent VCS				
Agent management		Agent ID 07DC8C7154AB473	371E9595AF52F88E43478F8CC4	Vierblate Vierblate A		Guidelines
Version = "3.0.30"		First ping: 31/05/2021 21:42	Last ping: 04/06/2021 09:52:08		First Ping	Last Ping 🖨 🔍
		Agent properties				
13 result(s)		SET POLICY	efault		速 Vie	w column 🗸 🗸
NAME	STATUS	GRC SET LIPDATE GROUP			POLICY	VERSION
	Offline	Def	nease "		default	3.0.30
Nextcloud	Offline	Dat MOVE TO GROUP de	efsult ~		default	3.0.30
Win7x86chuyentest	Online	Def	ave		enhance_alert_chuyen	3.0.30
ANM-CHUYENNT2	Online	Def General info Installation	Files Version Installed Certificates Scheduled Tasks Disks & partitions	Environment variables Installed software Required software	enhance_alert_chuyen	3.0.30
Ubuntu18x64chuyen	nt © Offline	Dat			full_features_centos	3.0.30
Test SeaBank khait	o v1 ⊕ Offline	Def Search by file name or version		٩	full_features	3.0.30
DESKTOP-EGANUBO	Offline	Def 🚍 AJIANT	VEDRDrvSetup.exe		enhance_alert_chuyen	3.0.30
DESKTOP-RUMB3Q9	Offline	Def propre	VERSION 1.0.0.85		anhnn19_test_load_image	3.0.30
Win7x86-A-PC	Offline	Def collector	VESConfigurationManager.exe		full_features	3.0.30
	Online	Def response	VERSION 3.0.0.1210		full_features	3.0.30
ThanhLN-PC	Offline	Def drivers	Agentinfo.exe		full_features_thanhin9	3.0.30
<u>Win10x64</u>	Offline	Dat colector	VERSION 3.0.0.1050		full_features_server	3.0.30
Win7x64-A-PC	Online	Def	PerfCtri dil		anhnn19_test_load_image	3.0.30
Display 13/13 result			VERSION 3.0.0.1213			
			RWorker.exe VERSION 3.0.0.1154			
			VESUpdater.exe VERSION 3.0.0.1194			
			VESConnectionManagerok.exe Version 1.0.0.1168			

Installed Certificates Tap





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

τιαίζα 🔟		Agent VCS	hannad hand an Anna an		© E1	root 😩 👻
Agent management		Agent ID 07DC8C7154A847371E9595AF52F88E434	178F8CC4			Ø Guidelines
Version = "3.0.30"		First ping: 31/05/2021 21:42:51 Last ping: 04/	06/2021 09:52:08		First Ping	Last Ping 🖨 🔍
		Agent properties				_
13 result(s)		SET POLICY default	~		📩 Vie	w column 🗸 🗸
NAME	STATUS	GRU SET UPDATE GROUP			POLICY	VERSION
	Offline	Def	*		default	3.0.30
Nextcloud	Offline	Dat MOVE TO GROUP default	~		default	3.0.30
Win7x86chuyentest	Online	Def			enhance_alert_chuyen	3.0.30
ANM-CHUYENNT2	Online	Def General info Installation Files Version Insta	Iled Certificates Scheduled Tasks Disks & partitions Environment variable	es Installed software Required software	enhance_alert_chuyen	3.0.30
Ubuntu18x64chuyennt	Offline	Dat	1		full_features_centos	3.0.30
Test SeaBank khaitb v1	Offline	Def Certificates - Local Machine	R Microsoft Root Certificate Authority	0 EVERATION OUTE 10/05/2021 05/28-12	full_features	3.0.30
DESKTOP-EGANUEQ	Offline	Def - My	asses of the contract of an are plantery		enhance_alert_chuyen	3.0.30
DESKTOP-RUMB3Q9	Offline	Def Root	R Thawte Timestamping CA		anhnn19_test_load_image	3.0.30
Uin7x86-A-PC	Offline	Def Certificates	Issued by Thawke Timestamping CA	EXPRATION DATE: 01/01/2021 06:59:59	full_features	3.0.30
	Online	Def Trust	R repolvisc.com		full_features	3.0.30
U Win10x64	Online	Def CA	Issued BY Websecurity Gateway - VCS	EXPIRATION DATE 29/04/2118 09:38:56	N/A	3.0.30
ThanhLN-PC	Offline	Def TrustedPublisher	R Microsoft Root Authority		full_features_thanhln9	3.0.30
Win7x64-A-PC	Online	Def Disallowed	issued by Microsoft Root Authority	EXPIRATION DATE 31/12/2020 14:00:00	full_features	3.0.30
Display 13/13 result		TrustedPeople	R Symantec Enterprise Mobile Root for Microsoft ISSUED BY Symantec Enterprise Mobile Root for Microsoft	EXPIRATION DATE 15/03/2032 06:59:59		
		- ClientAuthissuer - FlightRoot	R Microsoft Root Certificate Authority 2011	EXPIRATION DATE 23/03/2036 05:13:04		
		- TestsignRoot	R Microsoft Authenticode(tm) Root Authority ISSUED BY Microsoft Authenticode(tm) Root Authority	EXPIRATION DATE 01/01/2000 06:59:59		
		esim Certification Authorities	The second se			

In case of viewing details with more information, select ⁽¹⁾, the screen is displayed as follows:

rtificate	
RIENDLY_NAME	Microsoft Root Certificate Authority
SSUER	DC=com, DC=microsoft, CN=Microsoft Root Certificate Authority
KEY_USAGE	Digital Signature, Non-Repudiation, Certificate Signing, Off-line CRL Signing, CRL Signing (c6)
SIGNATURE_ALGORITHM	sha1RSA
STATUS	R
UBJECT	DC=com, DC=microsoft, CN=Microsoft Root Certificate Authority
ALID_FROM	10/05/2001 06;19:22

Scheduled Tasks Tap

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



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

📶 AJIANT		Agent VCS	NAL INTERNET PROVIDE RECEIPTION OF PROVIDE	~) EN * root 😩 *		
Agent management		Agent ID IITDOSCT15	darantessisArsarantesica	^	😗 Guidelines		
Version = "3.0.30"		First ping: 31/05/202	21:42:51 Last ping: 04/06/2021 09:52:08	First Ping	First Ping 🖾 Last Ping 🖾 📿		
13 result(s)		Agent properties SET POLICY	default.	ى	View column 👻		
NAME	STATUS	GRI SET UPDATE GROUP	release	POLICY	VERSION		
	Offline	Def MOVE TO GROUP	Ada-B V	default	3.0.30		
Nextcloud	Offline	Dat		default	3.0.30		
Win7x86chuyentest	Online	Def	Save	enhance_alert_chuyen	3.0.30		
ANM-CHUYENNT2	Online	Def General Info Insta	tion Files Version Installed Certificates Scheduled Tasks Disks & partitions Environment variables Installed software Required	software enhance_alert_chuyen	3.0.30		
Ubuntu18x64chuvennt	Offline	Dat		full_features_centos	3.0.30		
Test SeaBank khaitb vi	 Offline 	Def 📮 Task Schedules I	e Ready Hide	full_features	3.0.30		
DESKTOP-EGANUBO	Offline	Def	TRUNCTURE ALLA	enhance_alert_chuyen	3.0.30		
DESKTOP-RUMB309	© Offline	Def • °	NETRICIAL MA	anhinn19_test_load_image	3.0.30		
<u>Win7x86-A-PC</u>	@ Offline	Def	LAST BUILTING PROVING TO JIN (1966)	full_features	3.0.30		
O YCS	Online	Def	LAST RUN RESULT. The task has not used runs. (0X41303)	full_features	3.0.30		
Win10x64	e Online	Def	AUTHOR VCSIAdministrator	N/A	3.0.30		
ThanhLN-PC	Offline	Def	CREATED 18:36:49 09/03/2021	full_features_thanhin9	3.0.30		
WinZx64-A-PC	Online	Def		full_features	3.0.30		
Doplay 33/13 result			Infiguidad Show Infiguidad Show Infiguidad Show Show Show Show Infiguidad Show Show Infiguidad Show Infiguidad Show	3 3 3			

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





XML Detail

ml version="1.0" encoding="UTE-16"?	
<task version="1 2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"></task>	
<registrationinfo></registrationinfo>	
<date>2021-03-09T18:36:49 6502882</date>	
<author>VCS\Administrator</author>	
<uri>/dfffff</uri>	
<triagers></triagers>	
<principale></principale>	
<principal id="Author"></principal>	
< http://www.sectors.com/sectors/se	
<logontype>InteractiveToken</logontype>	
<punl evel="">l exetPrivilege</punl>	
<td></td>	
<pre>Settings></pre>	
Setunys	
ChicallowStartIfOnBattericeStruct/DisallowStartIfOnBattericeS	
<pre>StanlfCaingOnPattorios>true</pre> /StanlfCaingOnPattorios>	
<nlowhardtorminate>true</nlowhardtorminate>	
< Allow Hard Terminate>rrue Allow Hard Terminate	
<stattymenavailable>talse<stattymenavailable></stattymenavailable></stattymenavailable>	
<runoniyinvetworkavailable>laise</runoniyinvetworkavailable>	
<iol> Chan On Julia Fands taxes </iol>	
<stoponialeena>true</stoponialeena>	
<restartonidie>talse</restartonidie>	
	.↓. Export to XML

 \times

Select <u>Export to XML</u> to download scheduled task information. The .xml format is supported.

Disks & Partitions Tab

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

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

Ĩ	U AJIANT			Agent VCS	In Plans Excertification Processes Product & Proceedings IN P. Paddan	() P	i * root 主 *		
Agent	nanagement				IB47371E9595AF52F88E43478F8CC4		Guidelines		
Version	- "3.0.30"			First ping: 31/05/2021	21:42:51 Last ping: 04/06/2021 09:52:08	First Pine 🗂	First Pine 🖂 Last Pine 🛱 🔘		
			_			intering to			
13	.8(a)			Agent properties			w column		
10 161	nu(s)			SETPOLICY	default ~				
	NAME	STATUS	GR	SET UPDATE GROUP	release \vee	POLICY	VERSION		
	VCS	Offline	Def	MOVE TO GROUP	default ~	default	3.0.30		
	Nextcloud	Offline	Dat			default	3.0.30		
	Win7x86chuyentest	Online	Def		Sive	enhance_alert_chuyen	3.0.30		
	ANM-CHUYENNTZ	Online	Det	General info Installa	tion Files Version Installed Certificates Scheduled Tasks Disks & partitions Environment variables Installed software Required softw	re enhance_alert_chuyen	3.0.30		
	Ubuntu18x64chuyennt	© Offline	Dat	ST500DM002-18D142	^	full_features_centos	3.0.30		
	Test Seabank knaith VI	© Offline	Der	2407/7/24		Tul_peatures	3.0.30		
	DESKTOP-EGANOBO	© Offline	Def	VOLUME NAME	E	ennance_aiert_cnuyen	3.0.30		
	DESKTOP-RUMBSUS	© Offine	Def	SERIAL	60138EF2	annin19_test_load_image	3.0.30		
	WILLIOD-R-FL	© Ontine	Der	DRIVE TYPE	Fixed	foil_features	3.0.30		
	Yu2 Win10x44	Online	Def	FILE SYSTEM	FAT32	N/A	3.0.30		
	Thanki M.P.	© Offline	Def	CAPACITY	96 MB	full features thanking	3.0.30		
	Martinettes	© Online	Def	AVAILABLE	64 MB	full features	2.0.20		
	HILLING COLS	• Onane	Det			TUIL_TEALUTES	3.0.30		
Display :	3/13 result			Apacer AS350 512GB	v				

Environment Variables Tab

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

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

10 ΑΙΙΔΝΤ				Agent VCS					
Agent	management			Agent ID 07DC8C7154	(647371E9595AF52F88E43478F8CC4			Guidelines	
Version	n = "3.0.30"			First ping: 31/05/2021	21:42:51 Last ping: 04/06/2021 09:52:08		First Ping 🖨	Last Ping 🖨 🔍	
				Agent properties					
13 res	ult(s)			SET POLICY	default ~		📩 Vie	w column 🗸	
	NAME	STATUS	GRO	SET UPDATE GROUP			POLICY	VERSION	
	VCS	Offine	Def		researe		default	3.0.30	
	Nextcloud	Offine	Dat	MOVE TO GROUP	default ~		default	3.0.30	
	Win7x86chuyentest	Online	Def		Save		enhance_alert_chuyen	3.0.30	
	ANM-CHUYENNT2	Online	Def	General info Installa	ation Files Version Installed Certificates Scheduled Tasks Disks & partitions Environment va	ariables Installed software Required software	enhance_alert_chuyen	3.0.30	
	Ubuntu18x64chuyennt	Offline	Dat				full_features_centos	3.0.30	
	Test SeaBank khaitb v1	Offline	Def	System		~	full_features	3.0.30	
	DESKTOP-EGANUEQ	 Offline 	Def	Administrator		^	enhance_alert_chuyen	3.0.30	
	DESKTOP-RUMB3Q9	Offine	Def	Path			anhnn19_test_load_image	3.0.30	
	Win7x86-A-PC	Offline	Def	%USERPROFILE%(App	aData\Local\Microsoft(WindowsApps;	full_features	3.0.30		
	VCS	Online	Def	TEMP			full_features	3.0.30	
	Win10x64	 Online 	Def	96USERPROFILE96\App	;Data\Local\Temp		N/A	3.0.30	
	ThanhLN-PC	 Offline 	Def	ТМР			full_features_thanhin9	3.0.30	
	Win7x64-A-PC	Online	Def	%USERPROFILE%\App	JData)Local(Temp		full_features	3.0.30	
Display :	33/35 result			OneDrive C'(Users)viscadmin)(hebhe				

Installed Software Tab

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





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

Î	🚺 ΔΙΙΔΝΤ		1	Agent ANM-CHUYENNT2 • ONLINE Uninetal				() EI	e 🖛 root 🖭 📼
Agent	management			Agent ID 4030C72A3S	25D0B939BC065533A18B6F6A5B006E	• 04			Guidelines
Versic	on = "3.0.30"			First ping: 24/05/2021	103:47:46 Last ping: 09/06/2021 14:56:58	First Ping 🖨 Last Ping 🖨 📿			
				Agent properties					
13 res	sult(s)			SET POLICY	enhance_alert_chuyen	± Vie	w column 🗸 🗸		
	NAME	STATUS	GRO	SET UPDATE GROUP	miana			POLICY	VERSION
	VCS	 Offline 	Def		100000			default	3.0.30
	Nextcloud	 Offline 	Dat	MOVE TO GROUP	default ~			default	3.0.30
	Win7x86chuyentest	Online	Def		Save			enhance_alert_chuyen	3.0.30
	ANM-CHUYENNT2	Online	Def	General info Install	ation Files Version Installed Certificates Scheduled Tasks	Disks & partitions Environment variables	Installed software Required software	enhance_alert_chuyen	3.0.30
	Ubuntu18x64chuyennt	Offline	Date					full_features_centos	3.0.30
	Test SeaBank khaitb v1	Offline	Def	59 result(s)	All Anti Virus	Type software name to sea	arch Q	full_features	3.0.30
	DESKTOP-EGANUBQ	Offline	Def	CA Bis UD CIO Comerci	erete installer			enhance_alert_chuyen	3.0.30
	DESKTOP-RUMB3Q9	Offline	Def	Version 13.2.1	nents installer		04/08/2020	anhnn19_test_load_image	3.0.30
	Win7x86-A-PC	Offline	Def	7-Zip 19.00 (x64)			N/A	full_features	3.0.30
	VCS	Online	Def	Version 19.00		full_features	3.0.30		
	ThanhLN-PC	o Offline	Def	Ajiant Version 1.0.1			11/03/2021	full_features_thanhin9	3.0.30
	Win10x64	offline	Dat	Beeleur				full_features_server	3.0.30
	Win7x64-A-PC	Online	Def	Version 2.0.4.0			05/01/2021	anhnn19_test_load_image	3.0.30
Display	13/13 result			Foxit Reader Version 9.6.0.25114			03/08/2020		
				Google Chrome Version 89.0.4389.114			01/04/2021		
				Google Update Helpe Version 1.3.99.3	r		05/08/2020		
				HP LaserJet Pro M404 Version 48.4.4585.206	- M405 Basic Device Software		05/01/2021		
				Display 10/59 result(s	a				

Required Software Tab

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

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

Î	ΠΔΙΑΝΤ			Agent ANM-CHUYENNT2 • ONLINE Uninstall X				③EN ♥ root 😩 ♥				
Agent	management			Agent ID 4030C72A35	25D0B939BC065533A18B6F6A5B006E	- Untant			Guidelines			
Versio	n = "3.0.30"			First ping: 24/05/202:	1 03:47:46 Last ping: 09/06/2021 14:56:58			First Ping 🔛	Last Ping 🖨 🔍			
				Agent properties								
13 res	ult(s)			SET POLICY	enhance_alert_chuyen			خ. Vie	v column 🗸 🗸			
	NAME	STATUS	GR	SET UPDATE GROUP	release V			POLICY	VERSION			
	XCS	Offline	Def		release			default	3.0.30			
	Nextcloud	Offline	Dat	MOVE TO GROUP	default ~			default	3.0.30			
	Win7x86chuyentest	Online	Def		Save			enhance_alert_chuyen	3.0.30			
	ANM-CHUYENNT2	Online	Def	Installation Files Versi	ion Installed Certificates Scheduled Tasks Disks & partitic	ons Environment variables Installed software	Required software User list	enhance_alert_chuyen	3.0.30			
	Ubuntu18x64chuyennt	Offline	Dat					full_features_centos	3.0.30			
	Test SeaBank khaitb v1	Offline	Def	5 result(s)	All Not Installed	Type software name to search	Q.	full_features	3.0.30			
	DESKTOP-EGANUBQ	Offline	Def					enhance_alert_chuyen	3.0.30			
	DESKTOP-RUMB3Q9	Offline	Def	Agant Version 1.0.1			 Installed 	anhnn19_test_load_image	3.0.30			
	Win7x86-A-PC	Offline	Def	SFive			- Installed	full_features	3.0.30			
	VCS	Online	Def	Version 64.0.3282.204	4		• Instanted	full_features	3.0.30			
	ThanhLN-PC	Offline	Def	SecurityAgent			Installed	full_features_thanhin9	3.0.30			
	Win10x64	Offline	Dat	Constitution of the second sec				full_features_server	3.0.30			
	Win7x64-A-PC	Online	Def	-			 Not Installed 	anhnn19_test_load_image	3.0.30			
Display	13/13) result			VEDR - Display 5/5 result(s)			Not installed					

	Page
Viettel Cyber Security	
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi	40
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn W: www.viettelcybersecurity.com	
/	

User List Tab

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

Î	1 AJIANT			Agent VCS			e						
Agent	management			Agent ID 07DC8C7154	AB47371E9595AF52F88E434	78F8CC4			• OFFLINE	Uninstan	<u> </u>		😗 Guidelines
Versio	a = "3.0.30"			First ping: 31/05/2021 21:42:51 Last ping: 04/05/2021 09:52:08							First Ping 📋 Last Ping 🛱 📿		
13	.14(e)			Agent properties							. Viewcolume		
1016				SETPOLICY	default		~						
	NAME	STATUS	GRO	SET UPDATE GROUP	release		~					POLICY	VERSION
	VL2 National	© Offine	Det	MOVE TO GROUP	default		~					default	3.0.30
	Westcooo	© Online	Dat		See							oelault	3.0.30
	ANM_CHINENATS	Online	Def		June						_	enhance_alert_chuyen	3.0.30
	Ubustu 18x64cb usent	© Office	Dat	Installation Files Versio	on Installed Certificates	Scheduled Tasks	Disks & partitions	Environment variables	Installed software	Required software	User list	full features centres	3.0.30
	Test SeaBank khaith v1	© Offline	Def	USER			ACTIVE			ADMINISTRA	TOR	full_features	3.0.30
	DESKTOP-EGANUBO	© Offline	Def	admin			No			No		enhance alert chuven	3.0.30
	DESKTOP-RUMB309	© Offline	Def	Administrator			Yes			Yes		anhnn19 test load im	age 3.0.30
	Win7x86-A-PC	Offline	Def	DefaultAccount			No			No		full_features	3.0.30
	VCS	Online	Def	Guest			No			No		full_features	3.0.30
	ThanhLN-PC	Offline	Def	khaitb			Yes			No		full_features_thanhin9	3.0.30
	Win10x64	Offline	Dat	WDAGUtilityAccount			No			No		full_features_server	3.0.30
	Win7x64-A-PC	Online	Def								-	anhnn19_test_load_im	age 3.0.30
Display :	3/3 meułt												

- 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

í	U ΔJIANT			Investigation		revention Setting			∋ en -	root		
Agent	Management											
Type t	o search agent							First Ping		Last Ping		Q
												_
33 res	ult(s)								*	View column		~
Select	ed (3) Set Policy Move to gro	up Set update group Can	ncel									
	NAME Groups			UPDATE GROUP	LAST PING	FIRST PING	🖨 IP D	CN		POLICY		
	DESKTOP-4C6V54I Select	an Option	~	Test	22/05/2020 15:46:14	15/05/2020 17:38:55	10.6	1.188.2		Agent Perfor	mance	
	ThanhLN9-PC Set Gro	up		Alpha	25/05/2020 15:05:57	21/03/2019 13:31:53	10.6	1.188.2		bls_test		
2	HuyHV-PC			Test	25/05/2020 14:40:55	31/01/2020 17:23:19	10.6	1.188.2		Agent Perfor	mance	
	Win7-32bit-PC	Offline	Test_scan_ip	Test_ping	11/05/2020 10:41:10	22/04/2020 17:00:46	10.6	1.188.2		huyhv-2211		
	WIN-MM956VNPD90	Offline	Liennt_group2.1	Release	07/05/2020 09:56:40	07/05/2020 09:39:04	10.6	1.188.2		N/A		
	Chuyennt2-ViettelOS	Offline	Default	Release	18/05/2020 13:31:13	18/05/2020 11:16:38	10.6	1.188.2		default		
	DESKTOP-BGH8QIG	Offline	Default	Alpha	07/05/2020 14:28:53	24/07/2019 13:44:07	10.6	1.188.2		full_features		
	DESKTOP-LRT7Q4L	Offline	Anm	Release	22/05/2020 17:23:55	17/01/2020 18:39:40	10.6	1.188.2		huyhv_15.01	.ProPre	
	LienNT-TestPC	Offline	Liennt_group1.1	Release	25/05/2020 14:30:29	21/05/2020 11:42:22	10.6	1.188.2		N/A		
	Ubuntu18x64chuyennt	Offline	Default	Beta	18/05/2020 15:32:16	29/10/2019 10:50:34	10.6	1.188.2		Agent Perfor	mance	
	WIN-OH33SL4BBRJ	Offline	Test_scan_ip	Beta	19/05/2020 15:20:57	17/12/2019 13:36:53	10.6	1.188.2		hieupc4		
	Win7-32bit-PC	Offline	Test_scan_ip	Test	08/05/2020 18:17:53	25/02/2020 17:38:33	10.6	1.188.2		Agent Perfor	mance	
	Ubuntuhyperv-Virtual-Machine	Offline	Default	Release	06/05/2020 10:50:39	25/02/2020 17:03:22	10.6	1.188.2		test		
	ThanhLN-PC	Offline	Default	Test	18/05/2020 13:29:01	13/03/2019 13:30:45	10.6	1.188.2		Agent Perfor	mance	
	Localhost.Localdomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29	01/04/2020 14:38:38	10.6	1.188.2		centos		
	DESKTOP-EGANUBQ	Online	Test_scan_ip	Test	25/05/2020 15:30:51	08/05/2020 22:16:52	10.6	1.188.2		full_features		
	DESKTOP-315SAGT	Offline	Liennt_group1.1	Release	25/05/2020 14:38:40	19/08/2019 17:18:19	10.6	1.188.2		huyhv_15.01	.ProPre	

 $\circ \quad \text{Perform Move to group} \\$





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.

Ĩ	U AJIANT	Alerts	IR Flow	Investigation	Response	Protect & Prevention	Setting	😌 EN 🕶	root 😦 🗸
Agent	Management								
Type t	o search agent							First Ping 📋	Last Ping 📋 📿
33 resi	ult(s)							Ł	View column 🗸
Selecto	ed (3) Set Policy Move to group	p Set update group Can	cel						
0	NAME	STAT Update Groups		loup	LAST PING	E FIRST PIN	G 🗖	IP DCN	POLICY
	DESKTOP-4C6V54I	Of Select an Option		~	22/05/2020 15:46:14	15/05/202	0 17:38:55	10.61.188.2	Agent Performance
	ThanhLN9-PC	Of Set Update Group			25/05/2020 15:05:57	21/03/20	9 13:31:53	10.61.188.2	bls_test
	HuyHV-PC	e of			25/05/2020 14:40:55	31/01/202	10 17:23:19	10.61.188.2	Agent Performance
	Win7-32bit-PC	Offline	Test_scan_ip	Test_ping	11/05/2020 10:41:10	22/04/202	17:00:46	10.61.188.2	huyhv-2211
	WIN-MM956VNPD90	Offline	Liennt_group2.1	Release	07/05/2020 09:56:40	07/05/202	0 09:39:04	10.61.188.2	N/A
	Chuyennt2-ViettelOS	Offline	Default	Release	18/05/2020 13:31:13	18/05/202	0 11:16:38	10.61.188.2	default
	DESKTOP-BGH8QIG	Offline	Default	Alpha	07/05/2020 14:28:53	24/07/201	9 13:44:07	10.61.188.2	full_features
	DESKTOP-LRT7Q4L	Offline	Anm	Release	22/05/2020 17:23:55	17/01/202	18:39:40	10.61.188.2	huyhv_15.01.ProPre
	LienNT-TestPC	Offline	Liennt_group1.1	Release	25/05/2020 14:30:29	21/05/202	11:42:22	10.61.188.2	N/A
	Ubuntu18x64chuyennt	Offline	Default	Beta	18/05/2020 15:32:16	29/10/201	9 10:50:34	10.61.188.2	Agent Performance
	WIN-OH33SL4BBRJ	Offline	Test_scan_ip	Beta	19/05/2020 15:20:57	17/12/201	9 13:36:53	10.61.188.2	hieupc4
	Win7-32bit-PC	Offline	Test_scan_ip	Test	08/05/2020 18:17:53	25/02/202	0 17:38:33	10.61.188.2	Agent Performance
	Ubuntuhyperv-Virtual-Machine	Offline	Default	Release	06/05/2020 10:50:39	25/02/202	0 17:03:22	10.61.188.2	test
	ThanhLN-PC	Offline	Default	Test	18/05/2020 13:29:01	13/03/201	9 13:30:45	10.61.188.2	Agent Performance
	Localhost.Localdomain	Offline	Test_scan_ip	Release	27/04/2020 18:26:29	01/04/202	0 14:38:38	10.61.188.2	centos
	DESKTOP-EGANUBQ	Online	Test_scan_ip	Test	25/05/2020 15:30:51	08/05/202	0 22:16:52	10.61.188.2	full_features
	DESKTOP-315SAGT	Offline	Liennt_group1.1	Release	25/05/2020 14:38:40	19/08/20:	9 17:18:19	10.61.188.2	huyhv_15.01.ProPre

• Perform Set update group.

Notes:

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

3.1.4.2. Group Management

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

Key features on this monitor include as follows:

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

3.1.4.2.1. Manage groups by tree

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

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

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

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

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

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

Pagel

43



3.1.4.2.2. Search group

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

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



- When double-clicking on a record will display detailed information of that record.
 - Detailed information tab is displayed as Detail and the data of that group is Rule, Policy and Apply to.
 - \circ 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
- $\circ~$ If selecting Delete group, a confirmation popup to delete the group will be displayed.
- When clicking on the menu in the right corner, each record also displays 2 options: Go to group and Delete group.

3.1.4.2.3. Add a new group

- User login under root group: Enable to add all new groups. User login under default group: Unable to add a new group.
- User login under parent-level group: Enable to add a new corresponding child-level group of the group belonging to the user logging in.
- User login under a child-level group or many child-level group: Enable to add a new corresponding child-level of the group belonging to the user logging in.
 - Step 1: Select the group location to create.

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

💠 VEDR board - Agile Board - Your 🗙 🛛 💠 Test Management fo	ir JIRA - Your 🗙 🛛 💠 Test Management fo	r JIRA - Your 🗙 💠 Te	st Management for JIRA - Your 🗙	AJIANT - Agen	t Management 🗙 🔃 AJIAN	IT - Groups Management	× AJIANT - Login	× +	-	$\sigma \times$
\leftrightarrow \rightarrow \bigcirc \bigcirc \land Not secure 10.30.161.37/#/setting	s/group/							0 🕄 🟠 🔊	路 😒	θ 🛓 😫
📶 ΑJIANT	Alerts	IR Flow	Investigation	Response	Protect & Prevention	Setting		© EN ₹	root	•
Group Management	Type group to search						Q			Add new
server_computer										
it_department										
hr_department										
C os_linux										
□ test >										
🗅 hdsds										
new_and_exsit_os										
C add_group										
phuocnm3_0722_1										
C1 cpu_modelname										
C hostname_anm										
all_exist										
🗅 all_3										
D Ip_dcn										
D ip_192.168.8										
🗅 ip_dai										
🗅 default										
Add new										
Search the web and Windows	o 💁 🖬 S 🍬	🧧 😵 🕒	xii 🔀 📓	a 🍋 🐗	4			^ 🍺 🐨 🔣 💿 💟	🗊 di) 💷 B	6:30 PM 3/25/2020





Kear T: (+

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.

VEDR board - Agile Board - Your	🗙 📔 💠 Test Management for JIRA - Your 🗙	🔷 Test Management for JIRA - Your	🗙 🛛 🔷 Test Management for JIRA - Your	🗙 📔 📶 AJIANT - Agent Man	agement 🗙 🔃 AJIANT - Groups Managemen	AJIANT - Login	× +	- a ×
\leftrightarrow \rightarrow \bigcirc \bigcirc \land Not secu	re 10.30.161.37/#/settings/group/test						⊘ € ☆ ⊅ 😫 🤇	● 🛓 😫
📶 ΔΙΙΔΝΤ		Alerts IR Fi	ow Investigation	Response I	Protect & Prevention Setting		⊙ EN ≠ root	-
Group Management	Type group to search		Q	Delete Add new	test			×
Server_computer	L khcl_department				Detail		Agent list	
it_department	Add new				Rule			0
hr_department					Moving agent to this group if All v fo	llowing conditions matched :		
C os_linux					os linux			
	>							
hasas					Policy			
add group						~		
phuocnm3_0722_1					Apply policy now when rule matched			
C cpu_modelname					Apply to			
🗅 hostname_anm					All existing and new agents	~		
🗅 all_exist								
🗅 all_3								
🗅 lp_dcn								
□ ip_192.168.8								
🗅 ip_dai								
🗅 default								
							_	
_						жарау		
Search the web and Win	idows 🔲 🔯	📒 S 🔌 🦉	🛇 🕒 🗷 🖉	M 🍋 🍕 👫	6	,	^ 🍺 😨 🐹 💿 💟 🛒 🕸 🛡	ENG 3/25/2020

• 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.



Step 3: Select the policy and the agent type to apply the policy if the rule is satisfied. 0





khcl_department	_department Agent list	×	
Detail		Agent list	
Rule			0
Moving agent to this group if All v following conditions mat	ched :		
IP 192.168.8.*			
OS *Windows*			
Policy			
test 🗸	5		
Apply policy now when rule matched	5		
Apply to			
All existing agents \checkmark			
	6		
Appl	y	7	

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

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

Notes:

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



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

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

3.1.4.2.4. Edit group

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

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

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

khcl_dep	artment			×
	Detail		Agent list	
Rule				→ 1
Moving agent	to this group if A	following conditions matche	:d :	
IP	192.168.8	*		
OS	*Window	5*		

Edit the group rule then click Save.





		Detail	Agent list	
ule			Can	cel Save
loving agent to t	this group i	if All • following conditions matched :	2	
loving agent to t IP	this group i	f All following conditions matched :	×	

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.

Pagel Viettel Cyber Security 50 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

3.1.4.2.5. Delete group or remove agent from group

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

To delete a group, click on the group to delete, click Delete \rightarrow 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.

VEDR board - Agile Board - Your	× 💠 [VEDR-1387] [Release][B8XNKT	🗆 🗙 🛛 💠 [VEDR-1299] Kiếm thử tế	nh năng 🗙 💠 Test Management for JIRA - You: 🗙	AJIANT - Groups Mana	agement × 🔃 AJIANT - Policy Settings	× +	- σ ×
← → C ⋒ ▲ Not secur	e 10.30.161.37/#/settings/group/i	p_dai				Q) 🕏 🏠 🔊 🙆 🔍 😂 😫
🔃 ΔΙΙΔΝΤ		Alerts	IR Flow Investigation	Response Pr	rotect & Prevention Setting		🚱 EN 👻 🛛 root 🚨 👻
Group Management	Type group to search		Q 2	Delete Add new	ip_dai		×
server_computer					Detail		Agent list
it_department							
hr_department					Rule		0
🗅 os_linux					Moving agent to this group if All v fo	llowing conditions matched :	
🗅 test	>				IP 192.168.8.0/20		
🗅 hdsds					Policy		
new_and_exsit_os					,		
add_group			Do unu unot to rer	noue group Lin, dai 2	×		
phuocnm3_0722_1			bo you want to fer	and group the cart	nen ruie matched		
C cpu_modelname			Cancel	ок 3			
🗅 hostname_anm					All existing agents	~	
🗅 all_exist							
🗅 all_3							
D Ip_dcn							
□ ip_192.168.8							
🗅 ip_dai	1						
🗅 default							
						Apply	
Search the web and Wind	lows	📴 🔚 🖇 💌	🧶 🗘 🔛 🔀 🛤 🕅 🤅	o 🧑 🤻		^	© 😥 😋 💟 💭 di) 💭 ENG 3/37.PM 3/26/2020

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.





0	s_li	nux					×
		Detai	l		Agent list		
7	age	nt(s)	Type to	filter agent		View column	~
N	10.	AGENT ID		HOSTNAME	STATUS	POLICY	#
	1	CFF901BC683AE08EA40	77690	thedv1-VirtualBox	• Offline	default	×
	2	68555CF02D2580563A8	F12B4	ubuntu18x64chuyennt	• Offline	thanhln0910	×
:	3	B6900069868F655D59F4	4C2B8	chuyennt2-ViettelOS	Offline	thanhln_demo	×
	4	EA3892E4CBB2887FB04	DF59E	chuyennt2-ViettelOS-test	Offline	default	×
1	5	8C7C096A104B60A07FC	4BB87	thanhln9-VirtualBox	• Offline	thanhln_demo	×
	6	C9FFB3E6991525CE5EA	6D360	test-windows7	• Offline	thanhln0910	×
	7	C8B5960DEF7C9E83253	6930F	chuyennt2-VirtualBox	Offline	default	×

Notes: For deleting a parent-level group:

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

3.1.4.2.6. Add a new user to the group

ΤΙΔΙΈΑ 🚺					Investigation		Protect & Prevention	Setting	😚 EN 🕶	root	• •
Group Management	Type group	o to sear	rch		٩	Add new	anm				×
🗅 anm			bussiness_solution	>			Detail	Agent l	ist	User li	st
C default			liennt_group	>			0 user(s)	Type to filter user			Update user
			vcs_anm						<u>.</u>		
			test	>							
			group_test					No da	ta!		
			unknown								



User	availab	le to add into grou	P		User in group
	NO.	USERNAME	FULLNAME	EMAIL	
	1	admin	Supper Admin	admin@viettel.com	
	2	ajiant	ajiant	ajiant@viettel.com	
	3	ajiant_dev	ajiant_dev	ajiant_dev@viettel.com	
	4	chuyennt2	chuyennt2	chuyennt2@viettel.com	
	5	datnt88	datnt88	datnt88@viettel.com	
	6	hieupc4	hieupc4	hieupc4@viettel.com.vn	»
	7	liennt1	liennt1 5556668899665547	liennt18899665544112233@gmail.com	
	8	liennt_alert	liennt alert	lienntalert@gmail.com	
	9	liennt_inves	liennt investigation	lienntinvestigation@gmail.com	
	10	liennt_irflow	liennt irflow	lienntirflow@gmail.com	
	11	liennt_test1	liennt_test1	liennt_test1@gmail.com	
	12	root	Supper Admin	admin@viettel.com	
	13	siem	siem	siem@viettel.com	
	14	thanhln9	Lê Như Thành	thanhln@viettel.com.vn	
	15	thild1	Lưu Đình Thi	thild1@viettel.com.vn	

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.

📶 AJIANT						Investiga						Setting		EN 👻	root	- 1
Group Management	Type grou	ip to sear	ch			٩	Delet	e Add new	test							3
🗅 anm	>		bussiness_solution	>	🗅 test_ip					Detail		Agent	list		User li	st
🗅 default			liennt_group	>					5 us	er(s)		Type to filter user				Update user
			vcs_anm						NO.	USERNAME	FULLNAME	EMA	AIL		STATUS	
			test	>					1	admin	Supper Adr	nin adr	min@viettel.com		 Active 	×
			group_test						2	ajiant	ajiant	ajia	ant@viettel.com		 Active 	×
		~							3	ajiant_dev	ajiant_dev	ajia	ant_dev@viettel.con		 Active 	×
			unknown						4	chuyennt2	chuyennt2	chu	Jyennt2@viettel.con		Active	×
									5	datntoo	datntee	dat	ntoo@viettel.com		 Active 	
													D	ъс	۱۵	
														чy	~ I	
Viette	el Cybe	r Se	curity										/ E			
1/					and Marry T	. Disconstation		- :					/_ 0.	2		

3.1.4.2.7. Delete user

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



3.1.4.3. Account Management

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

3.1.4.3.1. Permission management

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

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

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

• Search permission

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

\leftarrow \rightarrow C $_{\mathrm{fit}}$ A Not secure 10.30.161.37/#/settings/accord	unt/permission					0 🕄 🟠 🔊	12 🗢 \varTheta 坐 🧯
📶 ΔΙΙΔΝΤ			Investigation	Protect & Prevention	Setting		root 👱 👻
Permission search							2
alert 1							×Q
2 result(s)							
ND. PERNISSION NAME		DESCRIPTION		ROLE LIST			ACTION
1 alerts_manage				manage_alert, roo	t		∅ 11
2 alerts_read				root, view_alert			Ø 🗓
Display 2/2 result(s)							

• Delete permission

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

→ C (m) ▲ Not secure 10.30.161.37/#/setting	s/account/permission						0014	8 9 0	9
📶 ΔJIANT						Setting		root 🕒	
ermission search									
ype permission to search									9
3 result(s)									
NO. PERMISSION NAME	DE	SCRIPTION			ROLE LIST			ACTION	
1 agent_management_manage					manage_agent	_management, manage_containment, mana	ge_deploy_tool, root	0 1	1
2 agent_management_read					manage_invest	igation_result, root, view_agent_manageme	nt, view_deploy_tool,View	0 11	
agent_policy_manage					manage_policy	_management, root		0 11	
agent_policy_read					root, view_polie	cy_management		0 🗓	
agent_read								0 🗓	
alerts_manage					×	pot		0 Û	
alerts_read			Do you want to remove permission	on : agent_management_mar	nage?			0 🗓	
appctrl_handler_manage						_handler, root		0 🗓	
appctrl_handler_read			Cancel	ок 2		trl_handler		0 🗓	
0 artifact_handler_manage		-				search, manage_investigation_result, mana	ge_process_analysis, root	0 🗓	
1 artifact_handler_read					root, view_inve	stigation_result, view_irflow, view_process_i	analysis	0 11	
2 artifact_manage					manage_detect	tion, root		0 11	
auto_runs_handler_manage					manage_auto_i	runs, root		0 11	
auto_runs_handler_read					root, view_auto	_runs		0 11	
5 containment_manage					manage_contai	inment, manage_irflow, root		0 🗓	
6 containment_read					root, view_cont	tainment, view_irflow		0 🗓	
7 deploy_tool_handler_manage					manage_deploy	y_tool, manage_investigation_tool, manage_	_irflow, root	0 Û	
8 deploy_tool_handler_read					manage_invest	igation_result, root, view_deploy_tool, view_	investigation_result,View	0 11	
9 endpointfw_handler_manage					manage_endpo	pintfw_handler, root		0 🗓	
0 endpointfw_handler_read					root, view_end	pointfw_handler		0 🗓	
1 event_manage					manage_event	_search, manage_irflow, root		0 11	

3.1.4.3.2. Role Management

Manage roles (permission group) of the system.

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

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



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

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

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

- Search role
 - Method 1: Click on the Search textbox \rightarrow The list of roles in the system is displayed and can be scrolled \rightarrow 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.

💠 VEDR board - Agile Box 🗙 🔷 [VEDR-650] [Porta	ual) Hő 🗙 🛛 🔇	VEDR-434] UserRoles · ×	🔃 AJIANT - Role Manager 🗙	🚺 AJIANT - Groups Mana 🗙	AJIANT - Login	🗙 🛛 💠 Test Management f	for J 🗙 🛛 📶 AJIANT -	Rules Manage 🗙 🌻 Instan	ices - OpenStack 🗙 🕂	- o	×
← → C (n) ▲ Not secure 10.30.161.37	7/#/settings/a	account/role/manage_contair	nment						0 🕄 🕁 🔊	🛚 🗢 🕒 🕹	5
📶 ΔΙΙΔΝΤ		Alerts	IR Flow	Investigation	Response	Protect & Prevention	Setting		③ EN *	root 💶 👻	
Role Management		mana		1				× Q 2			
🗅 default	🗅 manage	manage_agent_managemen	t								
C1 root → C	manage	manage_alert									
	_	manage_auto_runs									
	manage	manage_containment									
C	🗅 managi	manage_deploy_tool									
C	🗅 managi	manage_detection									
C	🗅 manage	manage_endpointfw_handle	r								
C	🗅 manage,	_detection									
C	🗅 manage	_endpointfw_handler									H
C	🗅 manage	_event_search									
C	🗅 manage,	_group_management									
C	🗅 manage,	_investigation_result									
C	🗅 manage	_investigation_tool									
C	🗅 manage,	_irflow									
C	🗅 manage,	_live_response									
C	🗅 manage	_permission_management									
C	🗅 manage	_policy_management									
C	🗅 manage,	_process_analysis									
C	🗅 manage	_response_scenario									
C	🗅 manage	_role_management									U
Search the web and Windows		0 🙋 🗖 S	🍬 😵 🔣	i 🛷 条 📧	9				^ 🍺 🖗 🔣	売 (4) ■ ENG 3/27/2	PM 2020

- 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.



- $\circ~$ When selecting the User List tab, it means the user list containing the role is selected.
- When right-clicking on a record, it will display Go to role. Click on Go to role to return to the original tree role list.
- When clicking on the menu in the right corner, each record also displays the option: Go to role.
- Add a new role
 - User login under root group: Enable to add all new roles in the data tree.
 - User login under default group: Unable to add new.
 - User login under parent-level group: Enable to add a new corresponding child-level role of the group belonging to the user logging in. Unable to add a new role at the same level.
 - User login under a child-level group or many child-level groups: Enable to add a new corresponding child-level group of the group belonging to the user logging in.
 - Step 1: There are ways to create a new role as follows:
 - Click on a role then hover over the end of the role list and select Add new to create a role with the same level as the selected role.
 - Click Add new on the screen to create a child-level role of the selected role
 - Right-click on a column in the tree and select Add new role.

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



VEDR board - Agile Bor × S [VED	R-650] [Portal] Hồ 🗙 🔷 [VEDR-434] UserRoles - 🗙 📶	AJIANT - Role Manage: X 🔃 AJIANT - Groups Ma	ne: 🗙 🔃 AJIANT - Login	🗙 🛛 🔷 Test Management for J 🗙 🛛 📶 AJIANT - Rules Manage 🗙	Instances - OpenStack: X + - 0 X
	0.30.161.37/#/settings/account/role/manage_deploy_too	10 Plana tanatanta	0	Best of A Descention	
🔟 AJIANT	Alerts	IR Flow Investigation	Response	Protect & Prevention Setting	😒 EN 👻 root 🖆 👻
Role Management	ype role to search	٩	Delete Add new	manage_deploy_tool	×
	view_appctrl_handler			Detail	User list
	view_auto_runs			Detail role information	0
	view_containment			NAME manage deploy :	tool (manage deploy tool)
	view_deploy_tool			DOMAIN	
	view_detection			DESCRIPTION manage_irflow	
	view_endpointfw_handler			Permission	
	view_event_search			deploy_tool_handler_manage agent_management_m	nanage nats_req_handler_manage
	view_group_management			irflow_manage	
	view_investigation_result				
	view_investigation_tool				
	view_irflow			1	
	view_live_response				
	view_permission_management				
	view_policy_management				
	view_process_analysis				
	view_response_scenario				
	view_role_management				
	view_user_management				
	Add new				
Search the web and Windows	0 6 5 4	> 😯 🔣 🖬 🛷 🕅 () 🍋 🔍	1	へ 🍺 🕖 👯 🌚 💟 💭 dii 💭 ENG 🛛 252 PM

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

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

	Page	9
/iettel Cyber Security		
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi	58	
: (+84) 971 360 360 E: vcs.sales@viettel.com.vn W: www.viettelcybersecurity.com		

test

Detail		_	User list		п
Detail role information				1	١Ŷ
NAME	test (test)				
DOMAIN					
DESCRIPTION	test				
Permission					
test					×
Detail			User list		
Detail role information			Ca	ancel Save	3
Name	test				
Domain					
Description	test				
Permission					
agent_management_read ×	deploy_tool_handler_manage ×				
auto_runs_handler_manage		2		1	
auto_runs_handler_read		2			
containment_manage					
containment_read					
deploy_tool_handler_read					
endpointfw_handler_manage	2				

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

	Page
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	, 59

×



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

VED	R board	- Agile Bor	× 🔷 [VEDR-65	i0] [Portal] Hỗ 🗙 🛛 💠 [VEDR-434] UserRole	s · 🗙 📶 AJIANT - Role Manager 🗙	AJIANT - Groups Mana	× AJIANT - Login	🗙 🛛 💠 Test Management fo	r J 🗙 📶 AJIANT - Rules Manage 🗙 🌻	instances - OpenStack + - 🛛 🗙
$\leftarrow \rightarrow$	C	۵ ا	Not secure 10.30	0.161.37/#/settings/account/role/test						🖉 🛠 🏠 🔊 🙆 । 😒 🤁 날 😂
í	10	مالم	п	Ale	rts IR Flow	Investigation	Response	Protect & Prevention	Setting	ⓒ EN 👻 root 😩 👻
Role	Mana	gement	t Туре	role to search			Delete Add new	test		×
									Detail	User list
				manage_permission_manage	ment			-		1
				manage_policy_management				0 user(s)	Type to filter user	Update user
A	dd use	er into ro	ole							×
							Lines in sele			
1.1	USA	er avaitable	e to add into role (2	selected)			User in role			
	0	NO.	USERNAME	FULLNAME	EMAIL					
	0	1	admin	Supper Admin	admin@ajiant.com					
2		2	chuyennt2	Chuyển	chuyennt2@viettel.com.vn		3			
		3	chuyennt3	chuyên	test@gmail.com		×			
		4	hieupc4	hleupc4	hieupc4@viettel.com.vn					
	0	5	ngant	Nguyên Thị Nga	ngant@rikkelsoft.com					
		6	ngant123	Nguyên Thị Nga	nganguyen.nuce@gmail.com					
		7	root	Supper Admin						
		8	thanhln9	Lê Như Thành	thanhln@viettel.com.vn					
	<u> </u>	9	thild1	Lưu Định Thị	thild1@vietteLcom.vn					
	U	10	viewer	viewer	viewer@viettel.com.vn					4
										Cancel Save
				view_endpointfw_handler						
				view_event_search						
				view group management						
				view_investigation_result						
				Pa view investigation tool						
::	earch t	the web a	ind Windows	O 📴 딇	S 🔷 🛠 🔣	📲 🛷 📧 🌍	>			∧ 🍃 (9) 🙀 (0) 1 등 (1) 1 등 ENG 3/27/2020

- Delete role
 - \circ Click on the role to delete, select Delete \rightarrow 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.

3.1.4.3.3. User management

Manage accounts logged into Portal VCS-aJiant system.

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

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



Tìm kiếm tài khoản				
ng				×Q
ngant				
ngant123				'hêm tài khoản
STT. TÊN ĐĂNG NHẬP	HỌ VÀ TÊN	EMAIL	TRẠNG THẢI	THAD TÁC
1 admin	Supper Admin	admin@ajiant.com	🚺 Hoạt động	0
2 chuyennt2	Chuyển	chuyennt2@viettel.com.vn	🚺 Hoạt động	/ 1
3 hieupc4	hieupc4	hieupc4@viettel.com.vn	🚺 Hoạt động	0
4 ngant	Nguyễn Thị Nga	ngant@rikkeisoft.com	🚺 Hoạt động	0
5 ngant123	Nguyễn Thị Nga	nganguyen.nuce@gmail.com	Hoạt động	0
6 root	Supper Admin		🗾 Hoạt động	0
7 thanhln9	Lê Như Thành	thanhIn@vietteLcom.vn	Hoạt động	0
8 thild1	Lưu Đình Thi	thild1@viettel.com.vn	🗾 Hoạt động	0
9 viewer	viewer	viewer@viettel.com.vn	Hoạt động	0
Hiến thị 9/9 kết quả				

• Add new account

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

📶 ΔJIΔΝΤ				Setting			liennt_irflow	
User search								
Type to search								Q
16 result(s)	Adduser							
NO. USERNAME	Add user				×	STATUS		ACTION
1 admin	Information Role Group						Active	
2 ajiant) Active	
3 ajiant_dev	Username	Type usern	ame				Active	
4 chuyennt2	Fullname	Time fuller					Active	
5 datnt88		Type tutina	me				Active	
6 hieupc4	Email	Type email					Active	
7 liennt1	Password	Type pass	sword				Active	
8 liennt_alert	Status	Active	 Inactive 				Active	
9 liennt_inves							Active	
10 liennt_irflow							Active	0 11
11 liennt_test1			Cancel N) Active	0 11
12 root	Supper Admin			admin@viettel.com			Active	
13 siem	siem			siem@viettel.com			Active	
14 thanhin9	Lê Như Thành			thanhln@viettel.com.vn			Inactive	
15 thild1	Lưu Đình Thi			thild1@viettel.com.vn) Active	
Display 16/16 result(s)								

- \circ 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.



(I)	Edit user						×	
Liser sea	Information Role	Group	Type role to search Q	2 role selected				
Type to a	🗅 default			default				0
	🗅 root	>		Permissions:	read			
16 result				liennt_protect		×	- 1	
NO. U				Permissions:	agent_management_manage agent_managemen	t_read	G	TION
1 a					agencponcy_manage		- 1	
2 a.							- 1	
3 a.								
4 cl								
5 d								
6 h								
7 li-								
8 li-								
9 li-								-
10 li-							2	-
11 6								-
12 rd								
14 th							- 1	
15 tł							- 1	
Display 16			Back Next					

 \circ 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.

Add user inves		×	×
Search results			2 role selected
manage_investigation_result	⁷⁰⁰ Go to role		default
manage_investigation_tool	root		Permissions: read
view_investigation_result	root		manage_investigation_result ×
view_investigation_tool	raot		Permissions: deploy_tool_handler_read

• 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.

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

Page Viettel Cyber Security 63 Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



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

٦Ì	Edit user			×) -
User sea	Information Role Group	Type group to search Q	1 group selected		
Type to :	□ anm >		Liennt_group1 anm / liennt_group	×	٩
16 result					Add user
NO. U					CTION
1 a					
2 a					
3 а					
4 c					
5 d					
6 h					
7 li					
8 li					
9 li					
10 li					2 🗊
11 li					2 🗊
12 m					
13 si					
14 ti					
15 ti					
Display 16		Back Cancel Save			

• 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.

n	Edit user			×		
Liser sea	Information Role Group	nga ×	1 group selected			
Turns to r	Search results	nga123	liennt_group1	×		
	🗅 nga123	2	anm / liennt_group		~	•
16 result					Add v	
NO. U					CTION	
1 a						
2 a,						
3а,						
4 c						
5 d						
6 h						
7 li						
8 li						
9 li						
10 li					2	
11 li					2 1	
12 m						
13 si						
14 tł						
15 tł						
Display 16		Back Cancel Save				

• Delete account

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

Check the display of the Delete icon as follows:



- \circ 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.

🔷 VEDR board - Agile Board - Your 🗙 🛛 💠 [VEDR-1381] [HDSD] Viët tái liệu 🗙	AJIANT - User Manager	ment × 🔟	AJIANT - Alert List 🗙 📔	G regeneratorRuntim	e is not define 🗙 🛛 🗛 "reg	eneratorRuntime is not defin 🗙	🐊 javascript - Babel 6 regene	ratorR × +	-	$\sigma \ \times$
← → C (m) ▲ Not secure 10.30.161.37/#/settings/account/use	r							0 🕄 🏠 🔊	ଥ ໑ €	9 ± §
παιία 🔟						Setting			root 🛓	
User search										
Type to search										Q
10 result(s)									1	Add user
NO. USERNAME	FULLNAME				EMAIL			STATUS	4	CTION
1 admin	Supper Admin				admin@ajiant.c	m		Active	4	۵ 🗊 ۱
2 chuyennt2	Chuyên				chuyennt2@viet	tel.com.vn		Active	6	۶ û
3 chuyennt3	chuyên				test@gmail.com			Active	l	۶ 🗊
4 hieupc4	hieupc4				hieupc4@viettel	.com.vn		Active	l	2 🗊
5 ngant	Nguyễn Thị Nga	_			nasnt@rikkeico	t.com		C Active	6	2 🗊
6 ngant123	Nguyễn Thị Nga		Do you want to remove use	o remove user - Sunner Admin ?	~	@gmail.com		Active	l	2 🗊
7 root	Supper Admin							C Active	6	۶ 🗊
8 thanhin9	Lê Như Thành		Cancel	а ок 2		.com.vn		Active	l	۵ 🗊
9 thild1	Lưu Đình Thi				unio 1 morte viene co	om.vn		C Active	6	۶ 🗊
10 viewer	viewer				viewer@viettel.4	om.vn		Active	6	۶ 🗊
Dopley 10/15 result(s)										
E Search the web and Windows	S	V 🔣 🛚	1 🧔 条 应				^	Þ 🤋 🐹 💿 V	도 4) 🗊 EN	3 10:44 AM 3/27/2020

3.2. Agent Interface

3.2.1. Main

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

On the taskbar, find and double-click the **select** icon \rightarrow Select Viettel Endpoint Detection & Response:



The system displays the information as follows:





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



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

V Viette	el Endpoint Detection & Resp	oonse – ×
	A Warning	
disinfected 52 (96%)	Ν	DOT PROCESSED 2 (4%)
🛞 Scan	Reports	i About

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

V	Viettel	Endpoint Detection & Resp	oonse – ×
		Critical	
	DISINFECTED 52 (96%)	٩	NOT PROCESSED 2 (4%)
	😫 Scan	Reports	i About

	Page
Viettel Cyber Security /	
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi	66
T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn W: www.viettelcybersecurity.com	

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

3.2.2. About

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

V About		×
_{viettel} ajiant	Viettel Endpoint Detection & Response VERSION 11.0.2215	
	OPERATION SYSTEM Microsoft Windows 10 x64	
	For more detail, please contact us via <u>cskh_anm@viettel.com.</u> © 2021 Viettel Cyber Security - Branch of Viettel Group	<u>vn</u> .

3.2.3. Reports

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



viettel	
security	

		Reports	– c
Copies of disinfected or and do not impose any tl	modified files during nreats, you can resto	disinfection are move to Backup fol re, remove or clear all files in Backup	der. Those files are stored in a dedicated format folder any time.
🔿 Restore 🛛 😣 Re	emove 🗍 🛅 Clear s	torage	
Event date	Status	Object	File path
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit.MSOffice.Generic	C:\Windows\System32\svchost.exe
27/07/2021 - 15:53:12	Fail to disinfected	Trojan: Exploit MSOffice.Generic	C\\Windows\System32\svchost.exe

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

• Restore : Enable to select 1 file to restore

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

th Clear storage</sup>: Enable to quickly clean all existing files in the Backup folder.

3.2.4. Scan

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

The supported scanning methods include a set of as follows:

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

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



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



The following actions during scanning are supported:



Enable to stop the scanning process





🄓 View report

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

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



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

V		Quick Scan		– ×	
V	Scan complete. 2 malware detected				
	DURATION OBJECTS SCANNED	00:00:02 868			
			🔓 View report	Close	

