Table of contents

Introduction to Active Response in Cybersecurity

Highlight the challenges faced by security teams during incident response, including delayed responses to high-severity events and difficulties in collecting relevant information in real time.

Role of Wazuh SIEM and XDR Platform

Explain how Wazuh improves incident response through real-time visibility, reducing alert fatigue, automating response actions, and providing ready-to-use response scripts.

Introduction to Invinsense Custom Active Response Module

Describe the module's capability to automate response actions based on specific triggers, aiding security teams in managing incidents effectively.

Work Flow

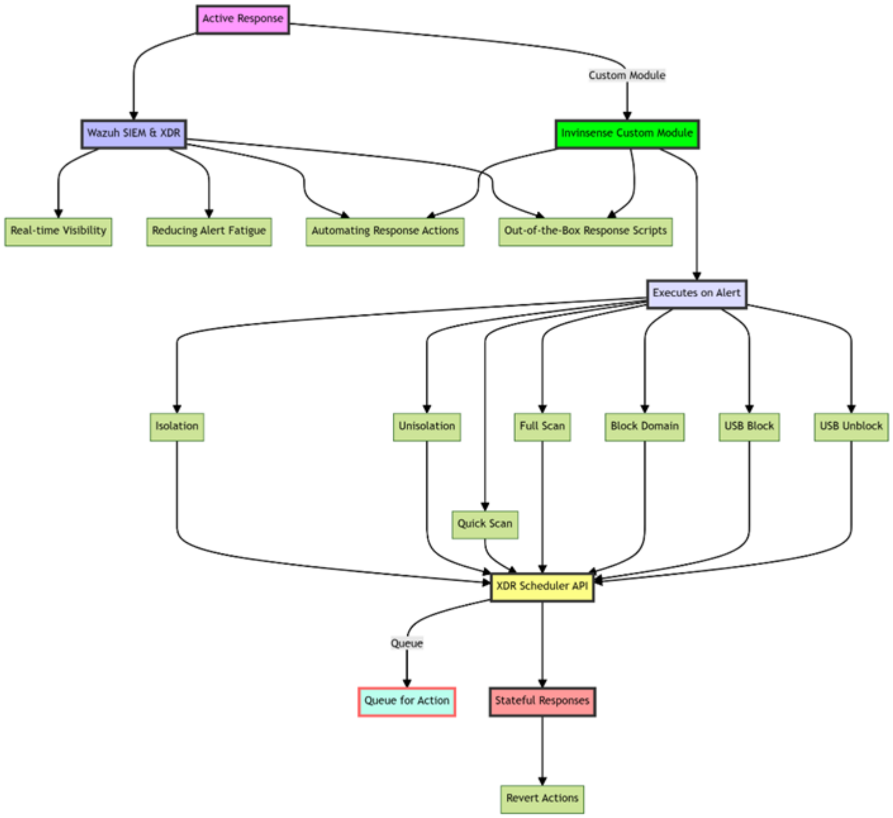


image.png

Types of Custom Active Responses

List and briefly describe each type of custom active response, including isolation, unisolation, quick scan, full scan, block domain, USB block, and USB unblock.

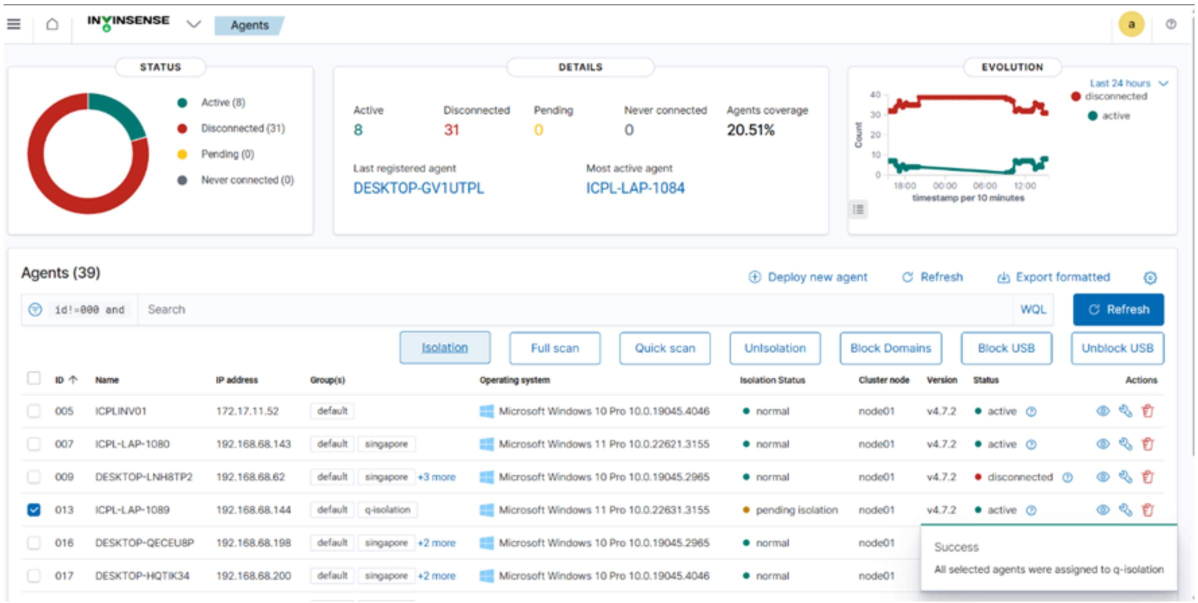
What is Isolation? How it works?

What is Isolation

Isolation refers to a security practice employed in server-side monitoring, wherein the system actively detects any unusual or suspicious activities on the internet. When such activities are identified, the administrator or the personnel responsible for managing the server isolate the affected machine. This isolation entails restricting the device's access to the internet, preventing any further communication with external networks.

How to Isolate the machine

Navigate to the Invinsense dashboard, locate the device you wish to isolate, and click on it. Subsequently, select the 'Isolation' option to initiate the isolation process.



Active	Disconnected	Pending	Never connected	Agents coverage
8	31	0	0	20.51%

Last registered agent DESKTOP-GV1UTPL

Most active agent ICPL-LAP-1084

Agents (39)

id!=000 and Search

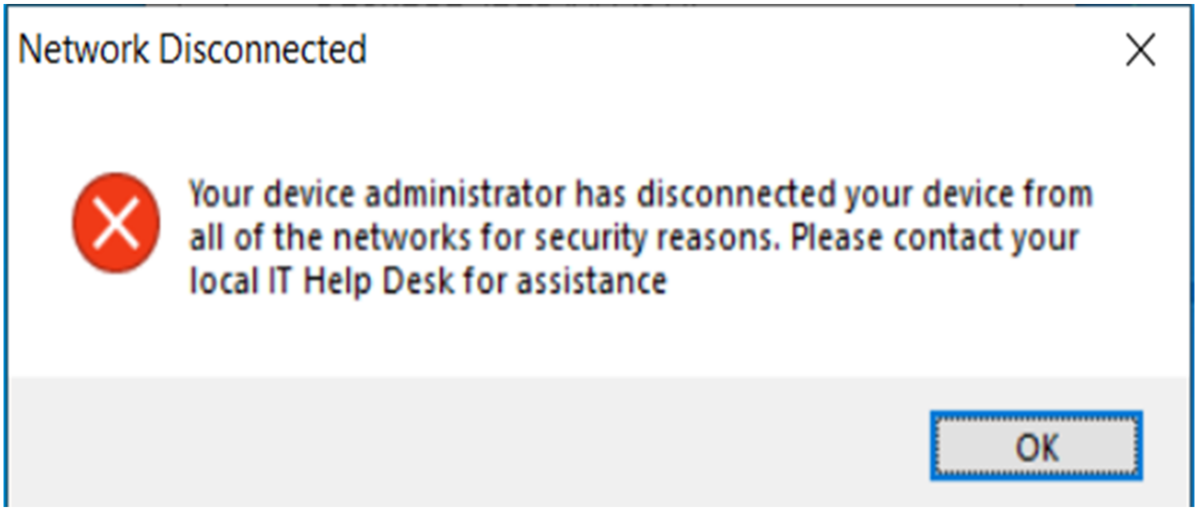
☐	ID ↑	Name	IP address	Group(s)	Operating system	Isolation Status	Cluster node	Version	Status	Actions
☐	005	ICPLINV01	172.17.11.52	default	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	● active	
☐	007	ICPL-LAP-1080	192.168.68.143	default singapore	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active	
☐	009	DESKTOP-LNH8TP2	192.168.68.62	default singapore +3 more	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	● disconnected	
☑	013	ICPL-LAP-1089	192.168.68.144	default q-isolation	Microsoft Windows 11 Pro 10.0.22631.3155	● pending isolation	node01	v4.7.2	● active	
☐	016	DESKTOP-QECEU8P	192.168.68.198	default singapore +2 more	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01			
☐	017	DESKTOP-HQTIK34	192.168.68.200	default singapore +2 more	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01			

Success

All selected agents were assigned to q-isolation

image_1.png

Isolated machine or machines receive a pop-up notification

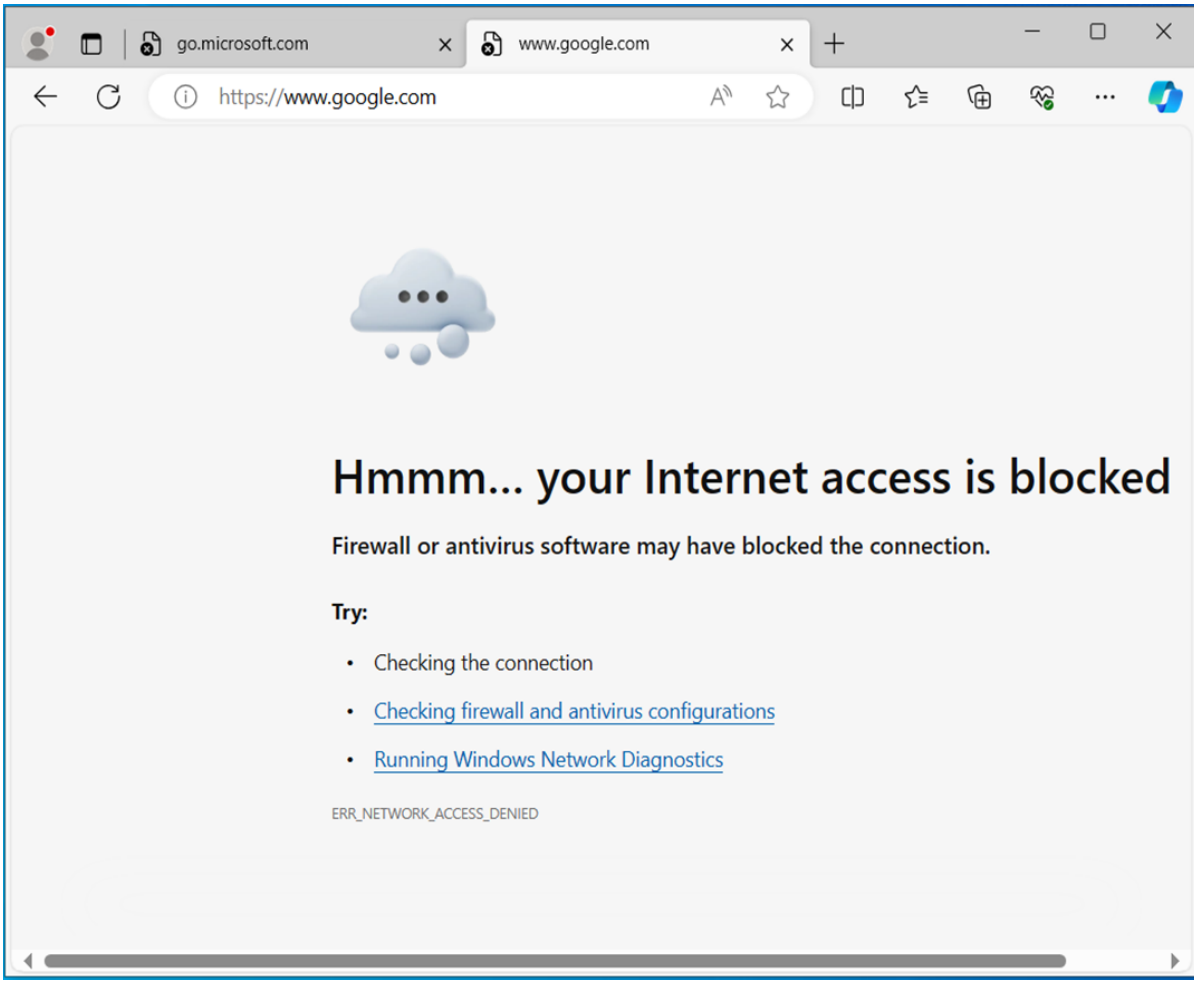


Network Disconnected

Your device administrator has disconnected your device from all of the networks for security reasons. Please contact your local IT Help Desk for assistance

image_2.png

Now, you can observe on that machine or those machines that they do not have access to the internet



Hmmm... your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

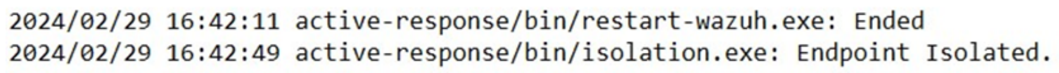
Try:

- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

ERR_NETWORK_ACCESS_DENIED

image_3.png

You can find a log in the Active Response folder at C:\Program Files (x86) \ossec-agent\active-response.



```
2024/02/29 16:42:11 active-response/bin/restart-wazuh.exe: Ended
2024/02/29 16:42:49 active-response/bin/isolation.exe: Endpoint Isolated.
```

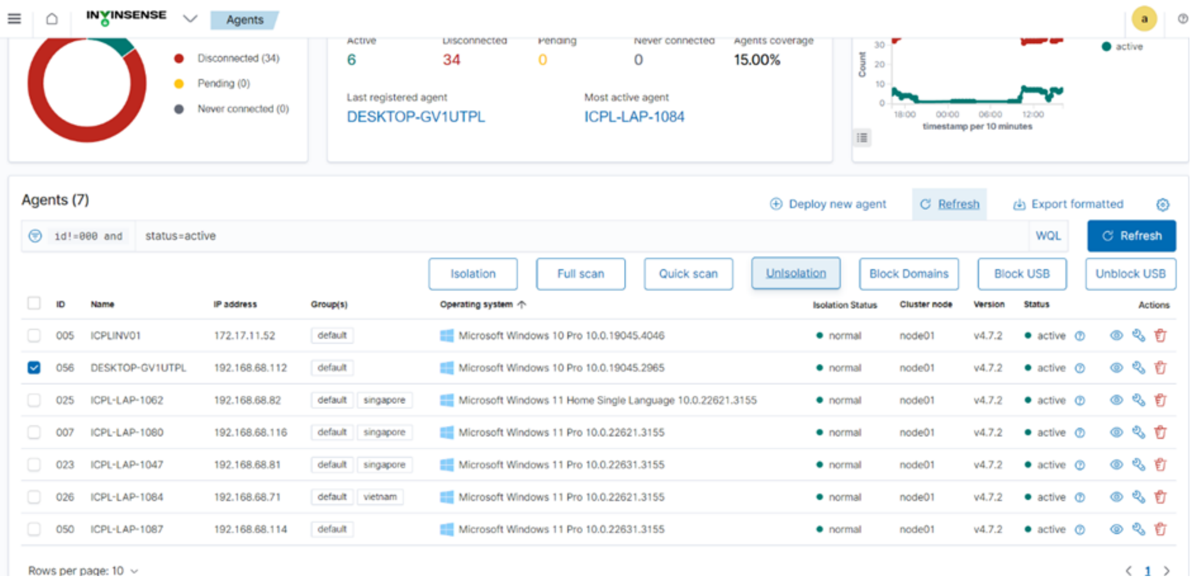
image_4.png

What is Unisolation? How it works?

What is Unisolation

Unisolation is the procedure of reintegrating or reconnecting someone or something that was previously isolated. This involves bringing them back into contact with others or the outside world. This process is crucial for restoring connectivity and allowing the reintegration of the isolated entity into its broader environment. Unisolation is often employed after a period of isolation, ensuring a smooth transition back into regular interactions and activities.

On the Invinsense dashboard, select the device or devices to initiate the unisolation process



Active 6 | Disconnected 34 | Pending 0 | Never connected 0 | Agents coverage 15.00%

Last registered agent DESKTOP-GV1UTPL

Most active agent ICPL-LAP-1084

Agents (7)

Deploy new agent | Refresh | Export formatted

id!=000 and status=active | WQL | Refresh

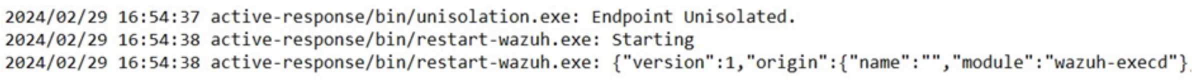
Isolation | Full scan | Quick scan | Unisolation | Block Domains | Block USB | Unblock USB

☐	ID	Name	IP address	Group(s)	Operating system ↑	Isolation Status	Cluster node	Version	Status	Actions
☐	005	ICPLINV01	172.17.11.52	default	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	● active	
☑	056	DESKTOP-GV1UTPL	192.168.68.112	default	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	● active	
☐	025	ICPL-LAP-1062	192.168.68.82	default singapore	Microsoft Windows 11 Home Single Language 10.0.22621.3155	● normal	node01	v4.7.2	● active	
☐	007	ICPL-LAP-1080	192.168.68.116	default singapore	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active	
☐	023	ICPL-LAP-1047	192.168.68.81	default singapore	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active	
☐	026	ICPL-LAP-1084	192.168.68.71	default vietnam	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active	
☐	050	ICPL-LAP-1087	192.168.68.114	default	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active	

Rows per page: 10 ⌄ ‹ 1 ›

image_5.png

You can find a log in the Active Response folder at C:\Program Files (x86) \ossec-agent\active-response.



```
2024/02/29 16:54:37 active-response/bin/unisolation.exe: Endpoint Unisolated.
2024/02/29 16:54:38 active-response/bin/restart-wazuh.exe: Starting
2024/02/29 16:54:38 active-response/bin/restart-wazuh.exe: {"version":1,"origin":{"name":"","module":"wazuh-execd"}
```

image_6.png

What is Quick Scan? How it works?

Introduction

Welcome to the Quick Scan Documentation. This guide provides an overview of the quick scan process in computing, outlining its purpose, usage.

Purpose

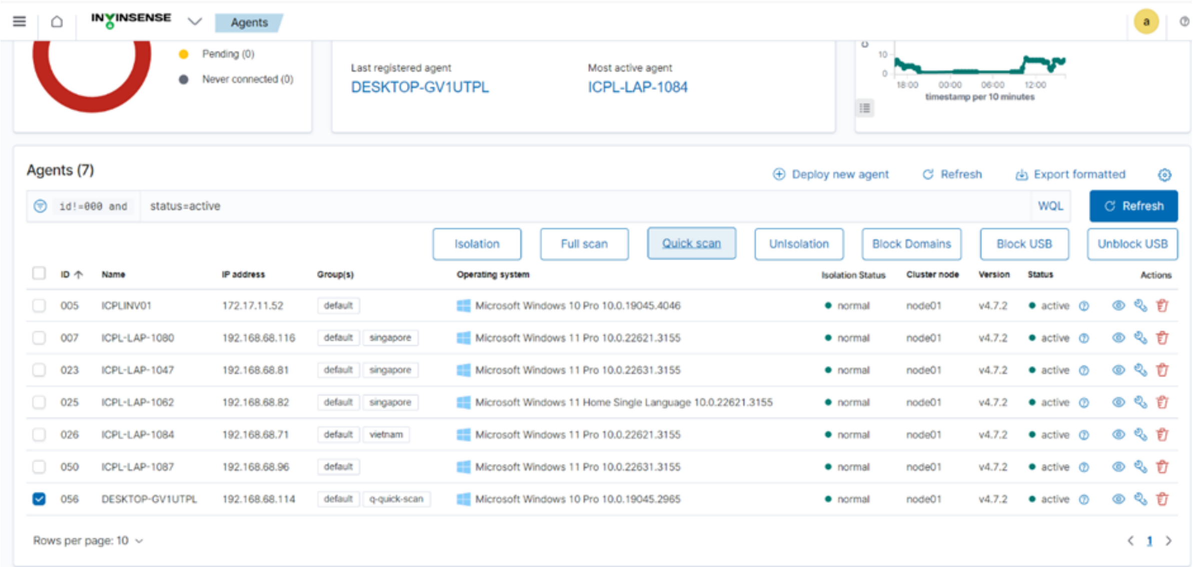
The primary purpose of a quick scan is to rapidly assess key areas or components of a system for potential issues or threats. This expedited process is designed to save time by prioritizing critical parts while potentially skipping less crucial elements.

Key Components

Identify the main components or areas typically examined during a quick scan. These may include critical system files, essential applications, network configurations, and other high-priority elements.

How it works?

On the Invensense dashboard, select the device or devices and initiate a quick scan



Last registered agent: DESKTOP-GV1UTPL

Most active agent: ICPL-LAP-1084

Agents (7)

`id!=000 and` status=active

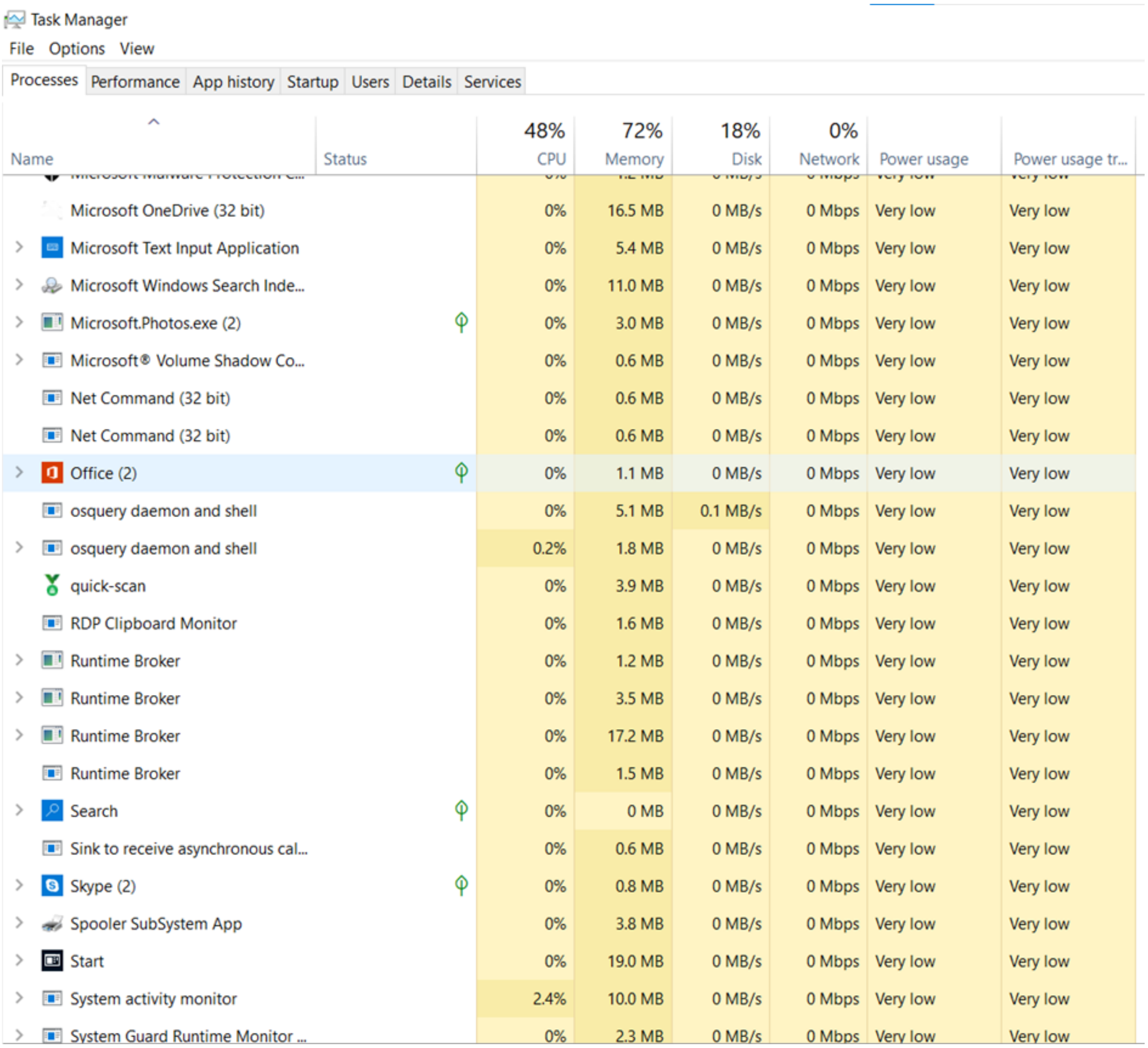
	ID ↑	Name	IP address	Group(s)	Operating system	Isolation Status	Cluster node	Version	Status
□	005	ICPLINV01	172.17.11.52	default	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	● active
□	007	ICPL-LAP-1080	192.168.68.116	default singapore	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active
□	023	ICPL-LAP-1047	192.168.68.81	default singapore	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active
□	025	ICPL-LAP-1062	192.168.68.82	default singapore	Microsoft Windows 11 Home Single Language 10.0.22621.3155	● normal	node01	v4.7.2	● active
□	026	ICPL-LAP-1084	192.168.68.71	default vietnam	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active
□	050	ICPL-LAP-1087	192.168.68.96	default	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active
☑	056	DESKTOP-GV1UTPL	192.168.68.114	default q-quick-scan	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	● active

Rows per page: 10

1

image_7.png

Now, you can check the taskbar on the endpoint device where the quick scan is running in the background.

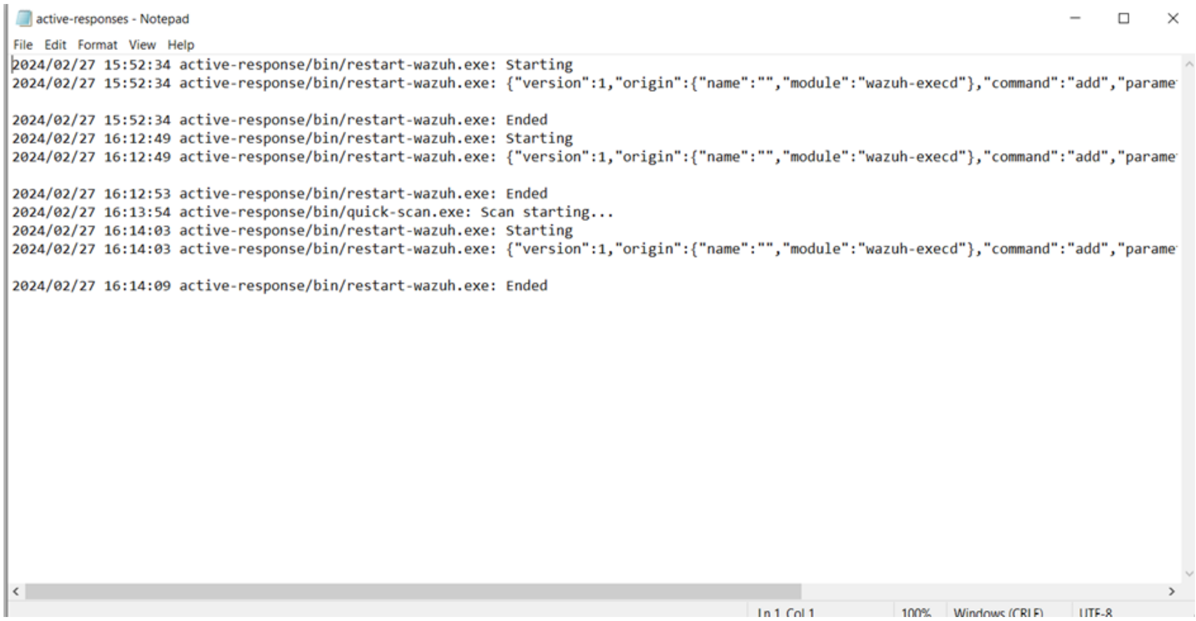


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	Status	48% CPU	72% Memory	18% Disk	0% Network	Power usage	Power usage tr...
Microsoft Malware Protection C...		0%	1.2 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft OneDrive (32 bit)		0%	16.5 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Text Input Application		0%	5.4 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Windows Search Inde...		0%	11.0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft.Photos.exe (2)	🌱	0%	3.0 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft® Volume Shadow Co...		0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
Net Command (32 bit)		0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
Net Command (32 bit)		0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
Office (2)	🌱	0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
osquery daemon and shell		0%	5.1 MB	0.1 MB/s	0 Mbps	Very low	Very low
osquery daemon and shell		0.2%	1.8 MB	0 MB/s	0 Mbps	Very low	Very low
quick-scan		0%	3.9 MB	0 MB/s	0 Mbps	Very low	Very low
RDP Clipboard Monitor		0%	1.6 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker		0%	1.2 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker		0%	3.5 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker		0%	17.2 MB	0 MB/s	0 Mbps	Very low	Very low
Runtime Broker		0%	1.5 MB	0 MB/s	0 Mbps	Very low	Very low
Search	🌱	0%	0 MB	0 MB/s	0 Mbps	Very low	Very low
Sink to receive asynchronous cal...		0%	0.6 MB	0 MB/s	0 Mbps	Very low	Very low
Skype (2)	🌱	0%	0.8 MB	0 MB/s	0 Mbps	Very low	Very low
Spooler SubSystem App		0%	3.8 MB	0 MB/s	0 Mbps	Very low	Very low
Start		0%	19.0 MB	0 MB/s	0 Mbps	Very low	Very low
System activity monitor		2.4%	10.0 MB	0 MB/s	0 Mbps	Very low	Very low
System Guard Runtime Monitor ...		0%	2.3 MB	0 MB/s	0 Mbps	Very low	Very low

image_8.png

You can find a log in the Active Response folder at C:\Program Files (x86) \ossec-agent\active-response.



```
2024/02/27 15:52:34 active-response/bin/restart-wazuh.exe: Starting
2024/02/27 15:52:34 active-response/bin/restart-wazuh.exe: {"version":1,"origin":{"name":"","module":"wazuh-execd"},"command":"add","parame

2024/02/27 15:52:34 active-response/bin/restart-wazuh.exe: Ended
2024/02/27 16:12:49 active-response/bin/restart-wazuh.exe: Starting
2024/02/27 16:12:49 active-response/bin/restart-wazuh.exe: {"version":1,"origin":{"name":"","module":"wazuh-execd"},"command":"add","parame

2024/02/27 16:12:53 active-response/bin/restart-wazuh.exe: Ended
2024/02/27 16:13:54 active-response/bin/quick-scan.exe: Scan starting...
2024/02/27 16:14:03 active-response/bin/restart-wazuh.exe: Starting
2024/02/27 16:14:03 active-response/bin/restart-wazuh.exe: {"version":1,"origin":{"name":"","module":"wazuh-execd"},"command":"add","parame

2024/02/27 16:14:09 active-response/bin/restart-wazuh.exe: Ended
```

image_9.png

What is Full Scan? How it works?

Introduction

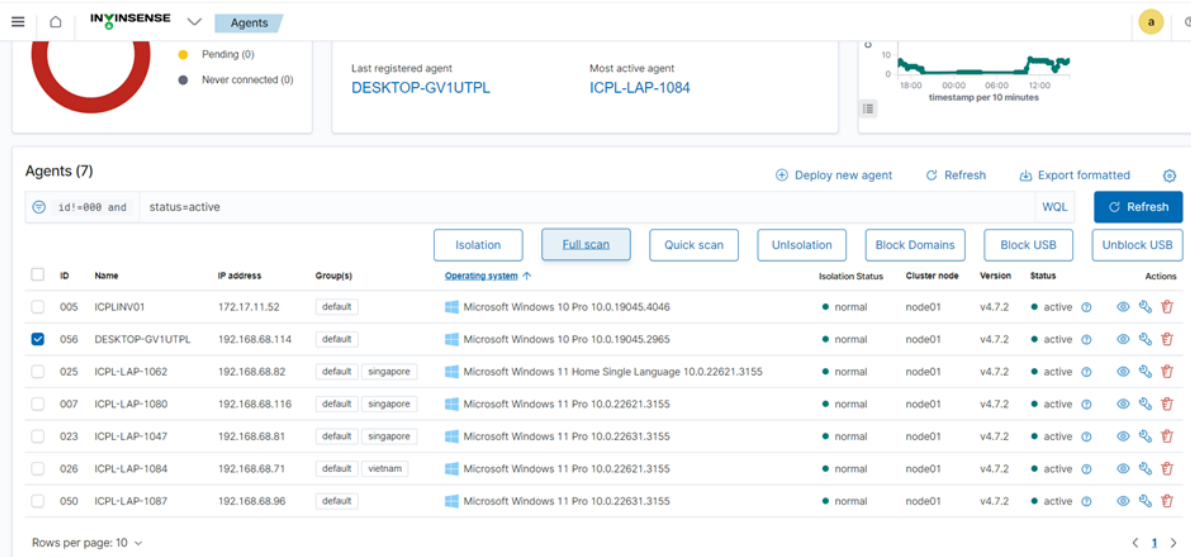
Welcome to the Full Scan Documentation. This comprehensive guide offers an in-depth exploration of the full scan process in computing, serving as a valuable resource for both beginners and seasoned users alike.

What is Full scan?

Which is a function of Invinsense which checks every area of the computer, including memory, hard drives and sometimes any external devices connected to the computer, like external hard drives and USB flash drives. Because the full scan checks everything, it takes longer to perform the scan. A full scan is a comprehensive process in computing that thoroughly examines and analyzes all elements within a system without skipping any part. This detailed assessment ensures a comprehensive evaluation of the entire system for potential issues or threats.

How it Works?

On a invinsense dashboard tick device/devices for a Full scan



Last registered agent DESKTOP-GV1UTPL

Most active agent ICPL-LAP-1084

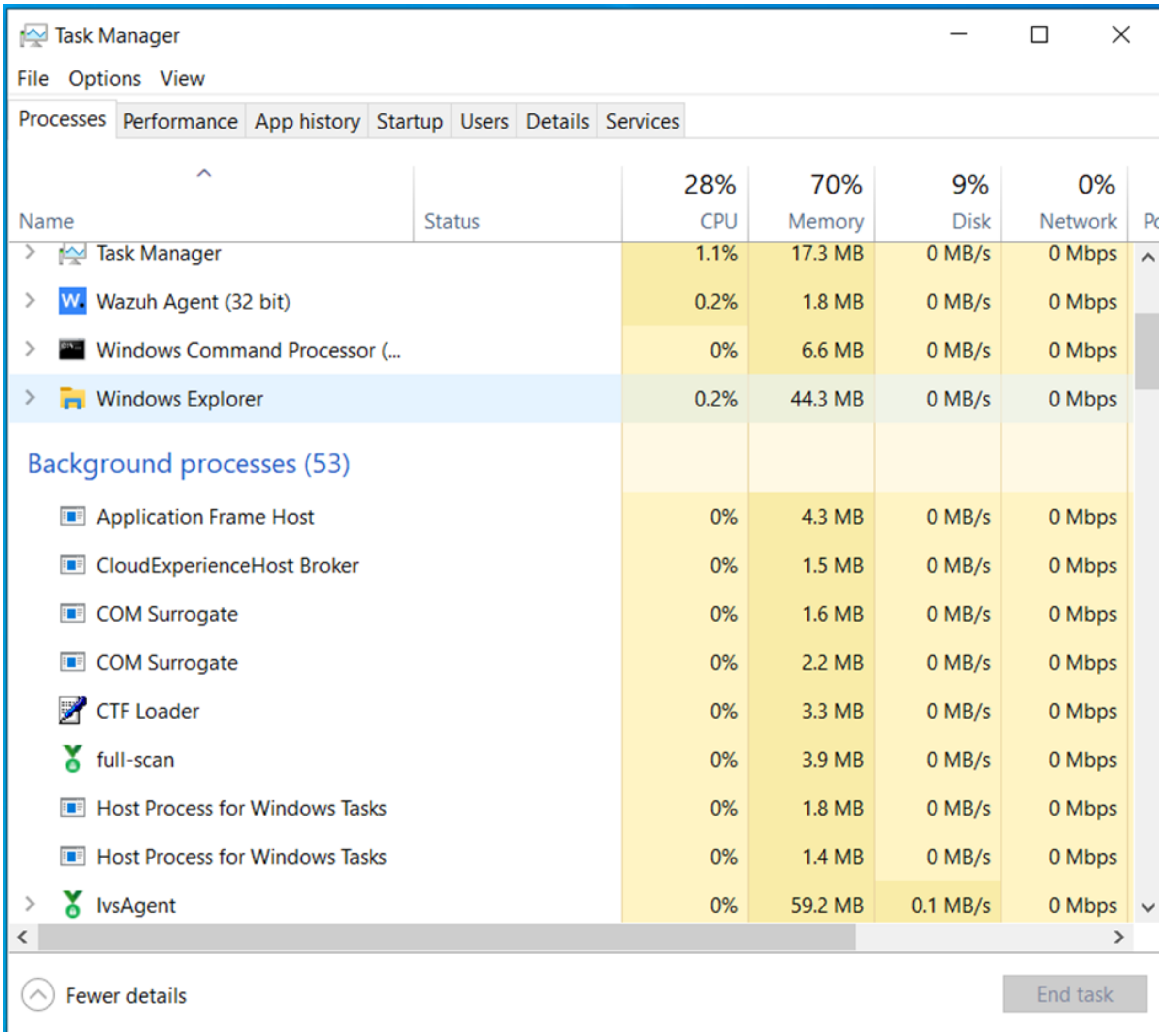
Agents (7)

id!=000 and status=active

	ID	Name	IP address	Group(s)	Operating system	Isolation Status	Cluster node	Version	Status	Actions
□	005	ICPLINV01	172.17.11.52	default	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	● active	
☑	056	DESKTOP-GV1UTPL	192.168.68.114	default	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	● active	
□	025	ICPL-LAP-1062	192.168.68.82	default singapore	Microsoft Windows 11 Home Single Language 10.0.22621.3155	● normal	node01	v4.7.2	● active	
□	007	ICPL-LAP-1080	192.168.68.116	default singapore	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active	
□	023	ICPL-LAP-1047	192.168.68.81	default singapore	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active	
□	026	ICPL-LAP-1084	192.168.68.71	default vietnam	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active	
□	050	ICPL-LAP-1087	192.168.68.96	default	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active	

image_10.png

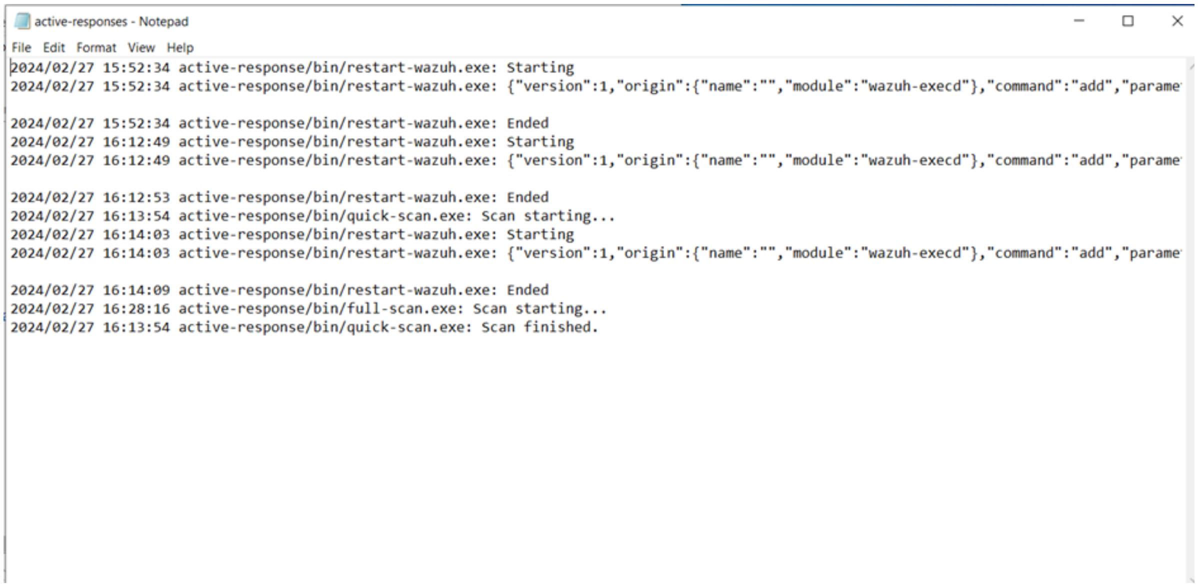
Now, you can check the taskbar on the endpoint device where the full scan is running in the background


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

Name	Status	28% CPU	70% Memory	9% Disk	0% Network	Pc
Task Manager		1.1%	17.3 MB	0 MB/s	0 Mbps	
Wazuh Agent (32 bit)		0.2%	1.8 MB	0 MB/s	0 Mbps	
Windows Command Processor (...		0%	6.6 MB	0 MB/s	0 Mbps	
Windows Explorer		0.2%	44.3 MB	0 MB/s	0 Mbps	
Background processes (53)						
Application Frame Host		0%	4.3 MB	0 MB/s	0 Mbps	
CloudExperienceHost Broker		0%	1.5 MB	0 MB/s	0 Mbps	
COM Surrogate		0%	1.6 MB	0 MB/s	0 Mbps	
COM Surrogate		0%	2.2 MB	0 MB/s	0 Mbps	
CTF Loader		0%	3.3 MB	0 MB/s	0 Mbps	
full-scan		0%	3.9 MB	0 MB/s	0 Mbps	
Host Process for Windows Tasks		0%	1.8 MB	0 MB/s	0 Mbps	
Host Process for Windows Tasks		0%	1.4 MB	0 MB/s	0 Mbps	
IvsAgent		0%	59.2 MB	0.1 MB/s	0 Mbps	

image_11.png

You can find a log in the Active Response folder at C:\Program Files (x86) \ossec-agent\active-response.



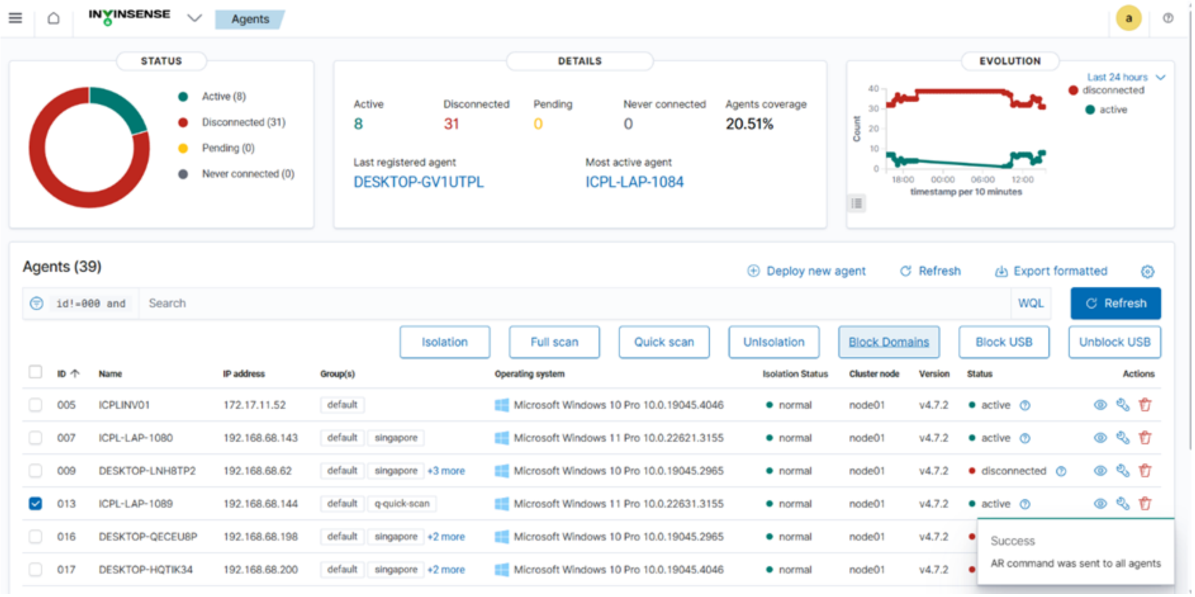
```
2024/02/27 15:52:34 active-response/bin/restart-wazuh.exe: Starting
2024/02/27 15:52:34 active-response/bin/restart-wazuh.exe: {"version":1,"origin":{"name":"","module":"wazuh-execd"},"command":"add","parame

2024/02/27 15:52:34 active-response/bin/restart-wazuh.exe: Ended
2024/02/27 16:12:49 active-response/bin/restart-wazuh.exe: Starting
2024/02/27 16:12:49 active-response/bin/restart-wazuh.exe: {"version":1,"origin":{"name":"","module":"wazuh-execd"},"command":"add","parame

2024/02/27 16:12:53 active-response/bin/restart-wazuh.exe: Ended
2024/02/27 16:13:54 active-response/bin/quick-scan.exe: Scan starting...
2024/02/27 16:14:03 active-response/bin/restart-wazuh.exe: Starting
2024/02/27 16:14:03 active-response/bin/restart-wazuh.exe: {"version":1,"origin":{"name":"","module":"wazuh-execd"},"command":"add","parame

2024/02/27 16:14:09 active-response/bin/restart-wazuh.exe: Ended
2024/02/27 16:28:16 active-response/bin/full-scan.exe: Scan starting...
2024/02/27 16:13:54 active-response/bin/quick-scan.exe: Scan finished.
```

image_12.png

What is Block Domain? How it works?

Block Domains

A block domain is a website address that has been restricted or prevented from being accessed by users,typically by network administrators or software filters,due to various reason such as security concerns,inappropriate content,or company policies.



Active	Disconnected	Pending	Never connected	Agents coverage
8	31	0	0	20.51%

Last registered agent: DESKTOP-GV1UTPL

Most active agent: ICPL-LAP-1084

Agents (39)

id!=000 and Search

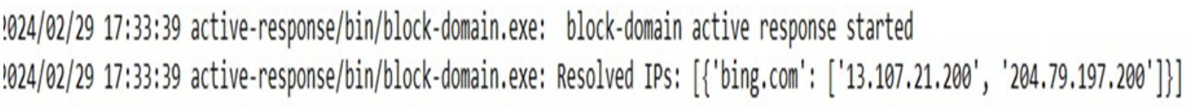
	ID ↑	Name	IP address	Group(s)	Operating system	Isolation Status	Cluster node	Version	Status	Actions
□	005	ICPLINV01	172.17.11.52	default	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	● active	
□	007	ICPL-LAP-1080	192.168.68.143	default singapore	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active	
□	009	DESKTOP-LNH8TP2	192.168.68.62	default singapore +3 more	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	● disconnected	
☑	013	ICPL-LAP-1089	192.168.68.144	default q-quick-scan	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active	
□	016	DESKTOP-QECEU8P	192.168.68.198	default singapore +2 more	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	●	
□	017	DESKTOP-HQTIK34	192.168.68.200	default singapore +2 more	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	●	

Success

AR command was sent to all agents

image_13.png

You can find a log in the Active Response folder at C:\Program Files (x86) \ossec-agent\active-response.



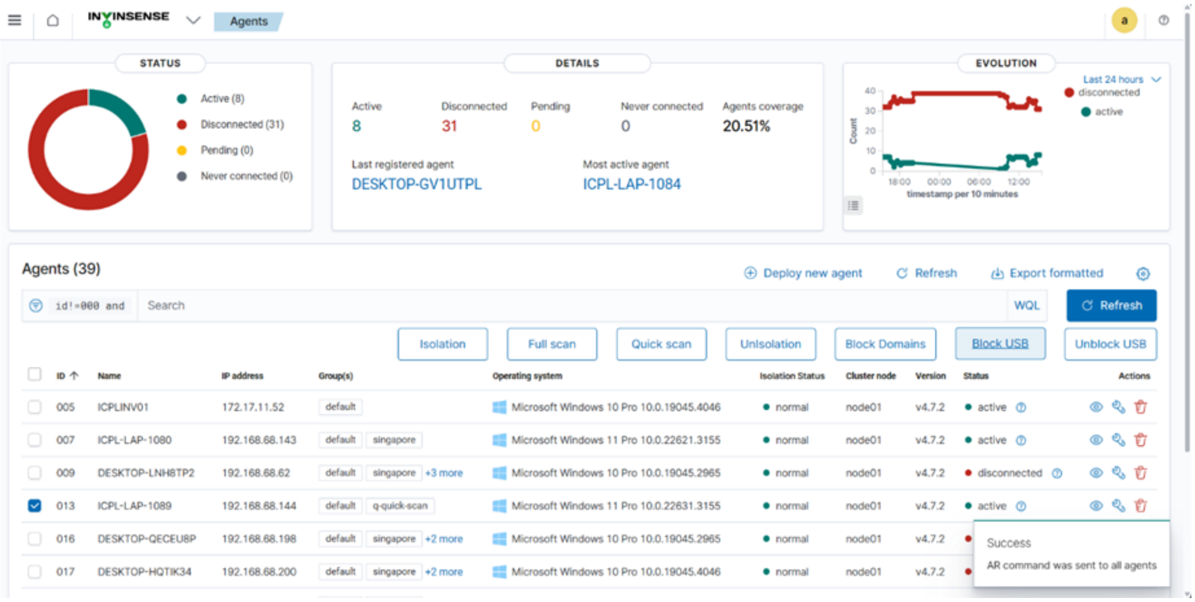
```
2024/02/29 17:33:39 active-response/bin/block-domain.exe:  block-domain active response started
2024/02/29 17:33:39 active-response/bin/block-domain.exe: Resolved IPs: [{'bing.com': ['13.107.21.200', '204.79.197.200']}]
```

image_14.png

What is Block USB? How it works?

Block USB

Blocking USB refers to restricting or disabling the use of USB ports on a computer or device,usually done to prevent unauthorized data transfer, malware infection, or to enforce security policies.



DETAILS

Active 8
Disconnected 31
Pending 0
Never connected 0
Agents coverage 20.51%

Last registered agent DESKTOP-GV1UTPL
Most active agent ICPL-LAP-1084

Agents (39)

id!=000 and Search

□	ID	Name	IP address	Group(s)	Operating system	Isolation Status	Cluster node	Version	Status	Actions
□	005	ICPLINV01	172.17.11.52	default	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	● active	
□	007	ICPL-LAP-1080	192.168.68.143	default singapore	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active	
□	009	DESKTOP-LNH8TP2	192.168.68.62	default singapore +3 more	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	● disconnected	
☑	013	ICPL-LAP-1089	192.168.68.144	default q-quick-scan	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active	
□	016	DESKTOP-QECEU8P	192.168.68.198	default singapore +2 more	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	●	
□	017	DESKTOP-HQTIK34	192.168.68.200	default singapore +2 more	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	●	

Success
AR command was sent to all agents

image_15.png

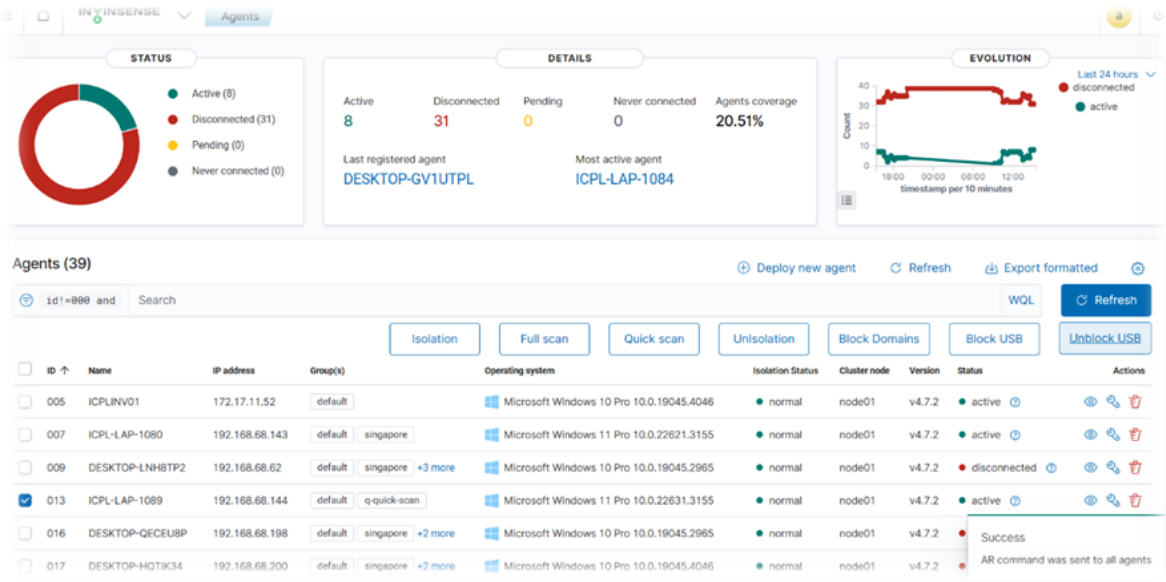
You can find a log in the Active Response folder at C:\Program Files (x86) \ossec-agent\active-response.

```
2024/02/29 17:33:52 active-response/bin/block-usb.exe: USB blocked on the endpoint.
2024/02/29 17:33:53 active-response/bin/block-usb.exe: USB blocked on the endpoint.
```

What is Unblock USB? How it works?

Unblock USB

Unblocking USB involves enabling or allowing the use of USB ports on a computer or device after they have been previously restricted or disabled, typically done to restore functionality or accommodate legitimate usage.



DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
8	31	0	0	20.51%

Last registered agent: DESKTOP-GV1UTPL

Most active agent: ICPL-LAP-1084

Agents (39)

	ID	Name	IP address	Group(s)	Operating system	Isolation Status	Cluster node	Version	Status	Actions
□	005	ICPLINV01	172.17.11.52	default	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	● active	
□	007	ICPL-LAP-1080	192.168.68.143	default singapore	Microsoft Windows 11 Pro 10.0.22621.3155	● normal	node01	v4.7.2	● active	
□	009	DESKTOP-LNH8TP2	192.168.68.62	default singapore +3 more	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	● disconnected	
☑	013	ICPL-LAP-1089	192.168.68.144	default q-quick-scan	Microsoft Windows 11 Pro 10.0.22631.3155	● normal	node01	v4.7.2	● active	
□	016	DESKTOP-QECEU8P	192.168.68.198	default singapore +2 more	Microsoft Windows 10 Pro 10.0.19045.2965	● normal	node01	v4.7.2	●	
□	017	DESKTOP-HQTIK34	192.168.68.200	default singapore +2 more	Microsoft Windows 10 Pro 10.0.19045.4046	● normal	node01	v4.7.2	●	

Success

AR command was sent to all agents

image_17.png

You can find a log in the Active Response folder at C:\Program Files (x86) \ossec-agent\active-response.

```
2024/02/29 17:33:54 active-response/bin/block-domain.exe: DNS cache has been flushed successfully.
2024/02/29 17:38:02 active-response/bin/unblock-usb.exe: USB unblocked on the endpoint.
```