



## **Agents configuration report**

**SAMEER HASSAN**

**Wazuh lab**

**Github-link:** [GitHub - sameerhassancode/Wazuh-labs](https://github.com/sameerhassancode/Wazuh-labs)

**Linkedin:** <https://www.linkedin.com/in/sameer-hassan-15a428255/>

## What is Wazuh?

**Wazuh** is a free and open-source security platform used for threat detection, compliance monitoring, and incident response. It helps organizations monitor their infrastructure in real-time by collecting and analyzing data from endpoints (like servers, desktops, or cloud instances). Wazuh works as a **SIEM (Security Information and Event Management)** and **XDR (Extended Detection and Response)** solution.

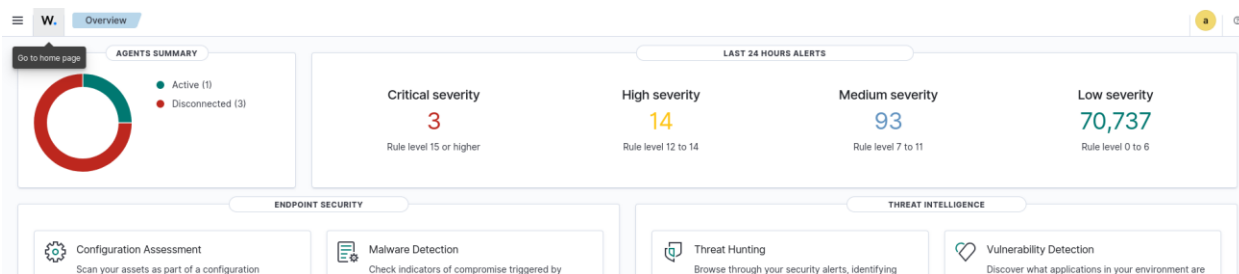
## What is the Wazuh Agent?

The **Wazuh Agent** is a lightweight piece of software installed on endpoints (such as Linux, Windows, or macOS machines). Its primary job is to:

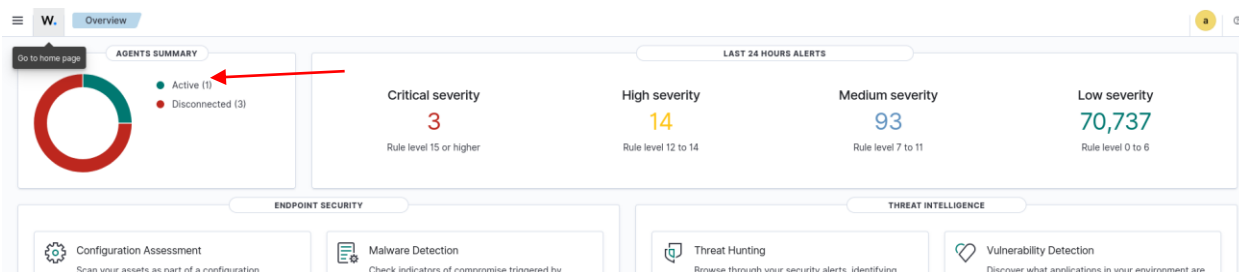
- **Collect system data** (logs, events, file changes, etc.)
- **Send that data** securely to the Wazuh Manager
- **Enforce active response rules** (like blocking malicious IPs or restarting services)

Each endpoint you want to monitor needs to have the Wazuh agent installed and configured.

## Wazuh-Dashboard:



## Click on active



It's showing 1 active agent.

Agents (1) ☐ Show only outdated Deploy new agent Refresh Export formatted More

status=active WQL

<input type="checkbox"/>	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
<input type="checkbox"/>	001	Win-001	192.168.0.105	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	active	

Rows per page: 10 < 1 >

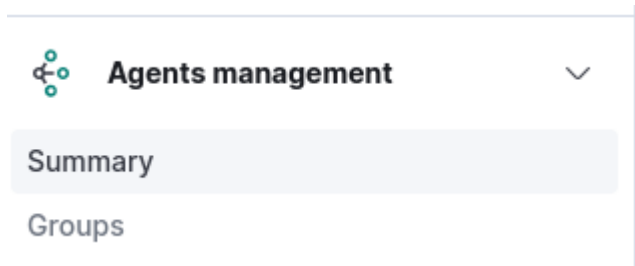
Now click on hamburger icon on the top left

The screenshot shows the Wazuh dashboard interface. At the top left, there is a hamburger menu icon (three horizontal lines) next to the 'W.' logo and the 'Endpoints' tab. A red arrow points to this icon. The dashboard displays three donut charts: 'AGENTS BY STATUS' (Active: 1, Disconnected: 3, Pending: 0, Never connected: 0), 'TOP 5 OS' (windows: 2, kali: 1, bsd: 1), and 'TOP 5 GROUPS' (default: 4). Below these charts is a table with columns: ID, Name, IP address, Group(s), Operating system, Cluster node, Version, Status, and Actions. The table shows one active agent with ID 001, Name Win-001, IP address 192.168.0.105, Group(s) default, and Operating system Microsoft Windows 11 Pro 10.0.26100.4351. The Status is active.

Now click on agents managements:

The screenshot shows the Wazuh dashboard interface with the left sidebar expanded. The 'Agents management' option is highlighted with a red arrow. The sidebar contains the following options: Recently viewed, Home, Explore, Endpoint security, Threat intelligence, Security operations, Cloud security, Agents management, Server management, Indexer management, Dashboard management, and Dock navigation. The main content area shows the same dashboard as the previous screenshot, with the 'Agents management' option highlighted in the sidebar.

After clicking it will show two sub types:



Click on Summary and it will redirect to page showing all agents:

Agents (4) Show only outdated Deploy new agent Refresh Export formatted More WQL

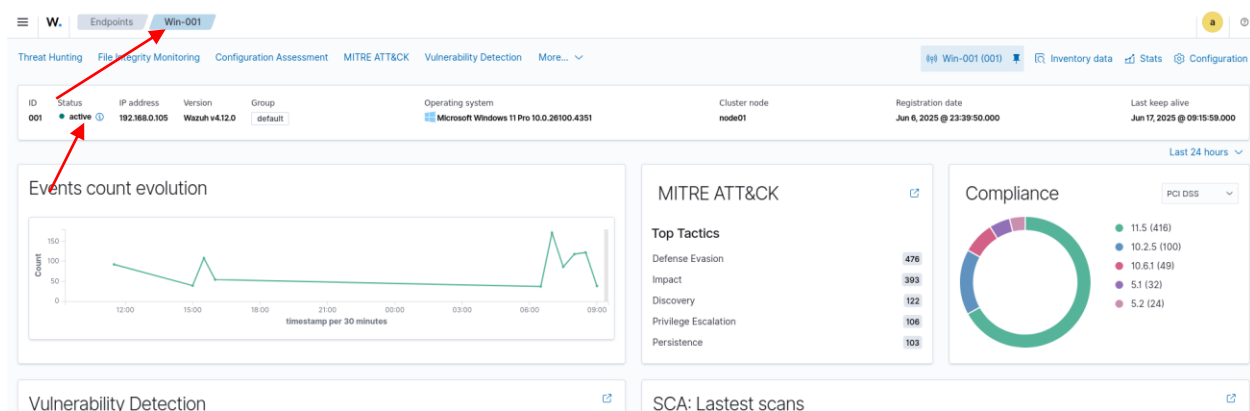
Search

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Win-001	192.168.0.105	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	active	
002	win-002	192.168.0.110	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	disconnected	
004	kali-001	192.168.0.117	default	Kali GNU/Linux 2025.1	node01	v4.12.0	disconnected	
005	pfSense.home.arpa	192.168.0.117	default	BSD 15.0	node01	v4.12.0	disconnected	

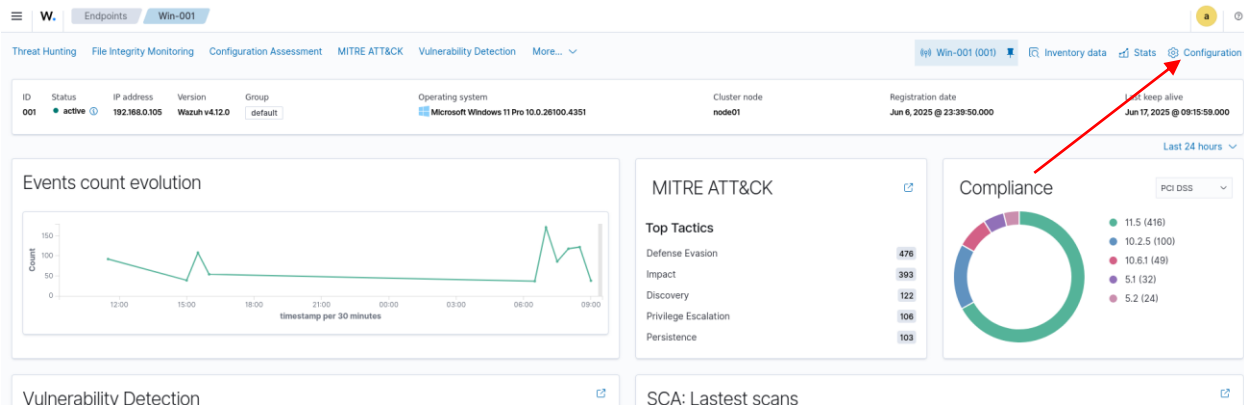
Rows per page: 10

Click on any agent you want to generate report I am selecting active agent:

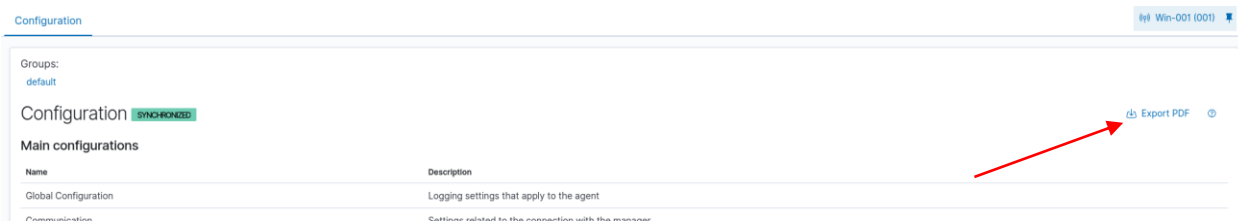
After selecting agent it will show you this page



Now click on configuration icon:

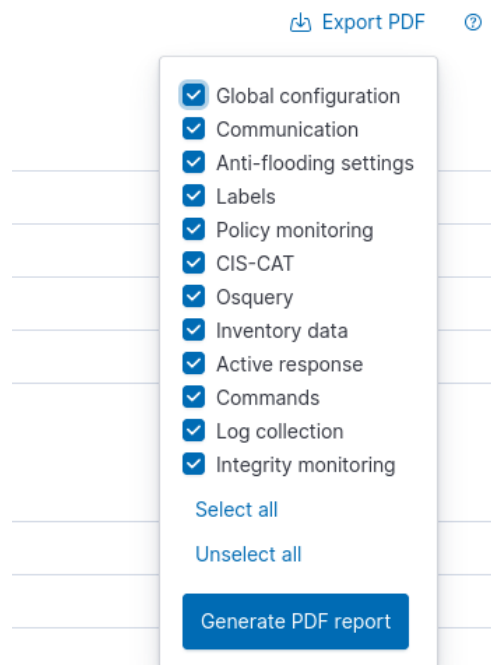


Now it you can see the option to generate the report:



Click export PDF:

Check the options and generate pdf report



Report is successfully generated:



[info@wazuh.com](mailto:info@wazuh.com)  
<https://wazuh.com>

## Agent 001 configuration

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	Win-001	192.168.0.105	Wazuh v4.12.0	wazuh-server	Microsoft Windows 11 Pro 10.0.26100.4351	Jun 7, 2025 @ 03:39:50.000	Jun 17, 2025 @ 13:20:07.000

Group: default

## Main configurations

### Global configuration

Logging settings that apply to the agent

Write internal logs in plain text    yes

Write internal logs in JSON format    no

### Communication

Settings related to the connection with the manager

Showing all the configuration details

## system threats and incident response

### Osquery

Expose an operating system as a high-performance relational database

Osquery integration disabled	yes
Auto-run the Osquery daemon	yes
Use defined labels as decorators	yes
bin_path	C:\Program Files\osquery\osqueryd
Path to the Osquery results log file	C:\Program Files\osquery\log\osqueryd.results.log
Path to the Osquery configuration file	C:\Program Files\osquery\osquery.conf

### Inventory data

Gather relevant information about the operating system, hardware, networking and packages

Syscollector integration disabled	no
Scan on start	yes
Interval between system scans	3600
Scan network interfaces	yes
Scan operating system info	yes
Scan hardware info	yes
Scan installed packages	yes
Scan listening network ports	yes
Scan all network ports	no
Scan current processes	yes
hotfixes	yes
sync_max_eps	10

## Summary:

Viewing or generating a Wazuh agent configuration report provides critical visibility into the security posture of an endpoint. It ensures the agent is properly connected to the Wazuh manager, verifies that essential modules like file integrity monitoring, vulnerability detection, and system inventory are enabled, and confirms that the setup complies with organizational or regulatory standards. This information is valuable for auditing, documentation, and troubleshooting, allowing security teams to quickly identify misconfigurations, coverage gaps, or disabled features. Overall, it strengthens endpoint monitoring and supports proactive threat detection and response.

**Need training on Wazuh ?**

Contact number: +923355345678

Email: [sameeerishassan@gmail.com](mailto:sameeerishassan@gmail.com)

LinkedIn: <https://pk.linkedin.com/in/sameer-hassan-15a428255>

## Other SIEM

1. IBM Qradar
2. Splunk
3. Azure Sentinel