



AGENT CONFIGURATION REPORT

What is Wazuh?

Wazuh is a free and open source security platform used for threat detection , complaince monitoring, and incident response. It helps organizations to monitor their infrastructure in real-time by collecting and analyzing data from end points (like servers, desktops or cloud instances).

Wazuh works as a **SIEM (Security Information and Event Management)** and **XDR (Extended Detection and Response)** solution.

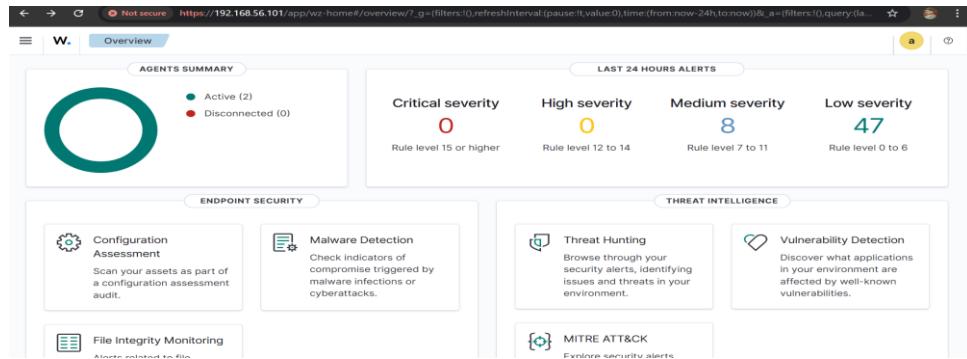
What is Wazuh agent?

The **wazuh agent** is lightweight piece of software installed on endpoints (such as Linux, Windows, or macOS machines). Its primarily job to:

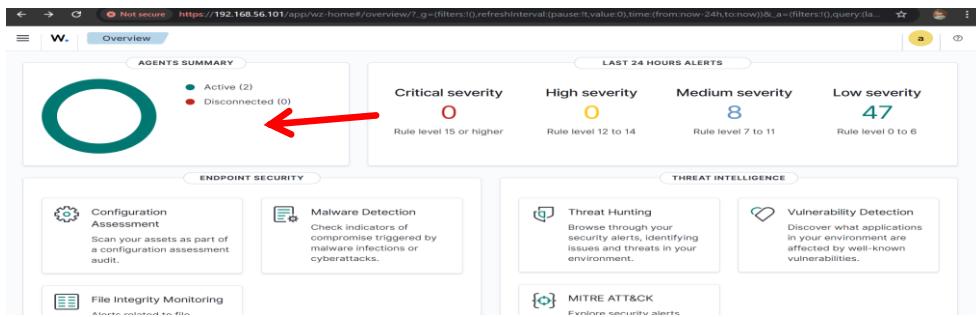
- **Collect system data** (logs, events, file changes etc)
- **Send that data** securely to the Wazuh Manager
- **Enforce active response rules** (like blocking malicious IPs or restarting services)

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

Wazuh Dashboard:



Click On the Active:



It's Showing 2 Active Agent:

Agents (2)								
Deploy new agent Refresh Export formatted More WQL								
status=active								
ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	WinDows11	192.168.56.1	default	Microsoft Windows 11 Pro 10.0.22000.2538	node01	v4.14.1	active ⓘ	...
002	kali-vm	10.0.2.15	default	Kali GNU/Linux 2025.3	node01	v4.14.1	active ⓘ	...

Rows per page: 10 < 1 >

Click On the Menu:

The screenshot shows the main dashboard with a red arrow pointing to the three-line menu icon in the top-left corner. The dashboard includes sections for AGENTS SUMMARY (Active: 2, Disconnected: 0), LAST 24 HOURS ALERTS (Critical: 0, High: 1, Medium: 9, Low: 47), and various threat intelligence modules like Malware Detection, Threat Hunting, and Vulnerability Detection.

The screenshot shows the main dashboard with a red arrow pointing to the 'Agents management' item in the 'Recently viewed' dropdown menu. The dashboard layout remains the same as the previous screenshot.

Click on Agents Management:

The screenshot shows the main dashboard with a red arrow pointing to the 'Summary' link under the 'Agents management' item in the 'Recently viewed' dropdown menu. The dashboard layout remains the same as the previous screenshots.

Click on the Summary It will redirect to page showing all the agents:

Agents (2)								
Deploy new agent Refresh Export formatted More WQL								
<input type="text" value="Search"/>								
ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	WinDows11	192.168.56.1	default	Microsoft Windows 11 Pro 10.0.22000.2538	node01	v4.14.1	active	...
002	kali-vm	10.0.2.15	default	Kali GNU/Linux 2025.3	node01	v4.14.1	active	...

Rows per page: 10 < 1 >

Click on any agent you want to generate report I am selecting active agent (WinDows11)

After selecting It will show you:

The screenshot shows the Wazuh interface with the 'Endpoints' tab selected. A red arrow points to the 'active' status indicator for the agent '001 WinDows11'. Below the list, there are three main cards: 'Events count evolution' (a line chart), 'MITRE ATT&CK' (a card with top tactics like Defense Evasion, Privilege Escalation, Initial Access, Persistence), and 'Compliance' (a donut chart showing counts for different PCI DSS levels).

Now click the Configuration icon:

The screenshot shows the Wazuh interface with the 'Configuration' icon highlighted by a red arrow. Below the configuration section, there are three cards: 'System inventory' (showing details like cores, memory, CPU, host name, and serial number), 'Events count evolution' (a line chart), and 'Compliance' (a donut chart).

There you can see the option to generate the report:

The screenshot shows the Wazuh Configuration interface. At the top, there are tabs for 'Endpoints', 'WinDows11', and 'Configuration'. Below this, a 'Groups' section lists 'default'. Under 'Main configurations', there is a table with columns 'Name' and 'Description'. The table includes rows for 'Global Configuration', 'Communication', 'Anti-flooding settings', and 'Labels'. On the right side of the configuration table, there is a blue 'Export PDF' button with a red arrow pointing to it.

**Click the export PDF
Check the option and generate the report:**

This screenshot shows a sidebar titled 'Select configurations' containing a list of monitoring modules, each with a checked checkbox icon. The listed items include: Global configuration, Communication, Anti-flooding settings, Labels, Policy monitoring, CIS-CAT, Osquery, Inventory data, Active response, Commands, Log collection, and Integrity monitoring. Below this list are two buttons: 'Select all' and 'Unselect all'. At the bottom is a large blue 'Generate PDF report' button.

This screenshot shows a generated PDF report titled 'wazuh. Agent 001 configuration'. The report includes a header with the Wazuh logo and contact information: 'info@wazuh.com' and 'https://wazuh.com'. The main content of the report is titled 'Agent 001 configuration' and displays the following details:

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keepalive
001	WinDows11	192.168.56.1	Wazuh v4.14.1	wazuh server	Microsoft Windows 11 Pro	Dec 1, 2025 @ 05:32:36.000	Feb 12, 2026 @ 10:36:15.000

The report also includes sections for 'Main configurations' (Global configuration and Communication) and 'Logs' (with a preview of log entries).

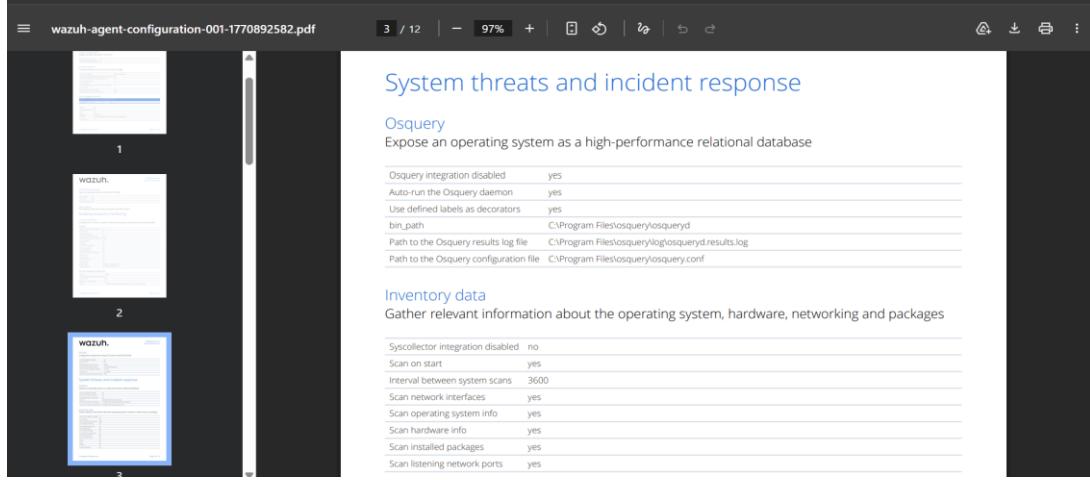
Report is successfully generated:

This screenshot shows a generated PDF report titled 'wazuh. Agent 001 configuration'. The report includes a header with the Wazuh logo and contact information: 'info@wazuh.com' and 'https://wazuh.com'. The main content of the report is titled 'Agent 001 configuration' and displays the following details:

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keepalive
001	WinDows11	192.168.56.1	Wazuh v4.14.1	wazuh server	Microsoft Windows 11 Pro	Dec 1, 2025 @ 05:32:36.000	Feb 12, 2026 @ 10:36:15.000

The report also includes sections for 'Main configurations' (Global configuration and Communication) and 'Logs' (with a preview of log entries).

Showing all the configuration details



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 organization or regulatory standards. This information is valuable for auditing, documentation, and troubleshooting, allowing security teams to quickly identify misconfiguration, coverage gaps or, disabled features. Overall, it strengthens endpoint monitoring and supports proactive threat detection and response.

Other SIEM:

Splunk

IBM QRadar

Azure Sentinel