# FAQ



## How often does syscheck run?

Syscheck frequency is configurable by the user with frequency. By default is configured to run every 6 hours.

## What is the CPU usage like on the agents?

Syscheck scans are designed to run slowly to avoid too much CPU or memory use.

## Where are all the checksums stored?

All the checksums are stored on the manager `/var/ossec/queue/syscheck`

## Can I ignore files in a directory?

Yes, you can use the ignore option to avoid false positives. Example: ignore-false-positives

## Can Wazuh report changes in the content of a text file?

Yes, this is posible with the `report_changes` option. For `directories` only. This option gives us the exact content that has been changed in a text file. Be selective about which folders you use `report_changes` on, because this requires syscheck to copy every single file you want to monitor with `report_changes` to a private location for comparison purposes. Example: report changes

## How does Wazuh verify the integrity of files?

Wazuh manager stores and looks for modifications to all the checksums and file attributes received from the agents for the monitored files. Wazuh manager compares the new checksums/attributes against the stored ones. An alert is generated if anything changes.

## Does Wazuh monitor any directories by default?

Yes. By default Wazuh monitors `/etc`, `/usr/bin`, `/usr/sbin`, `/bin` and `/sbin` on Unix-like systems and `C:\Windows\System32` on Windows.

## Can I force an immediate syscheck scan?

**Yes, you can force an agent to perform a system integrity check with ::**

/var/ossec/bin/agent_control -r -a /var/ossec/bin/agent_control -r -u <agent_id>

More info at Ossec control section

## Does Syscheck start when Wazuh start?

By default syscheck scan when Wazuh start, but you can change this with the scan_on_start option

## Does Wazuh alert when a new file is created?

Yes, but you need to configure it. Use the alert_new_files option