Guide to Integrate Wazuh with Antivirus Software

Author: Joshua Robertson

# Introduction

This guide will provide instructions for how to integrate Wazuh with antivirus software on Windows and Ubuntu operating systems. Wazuh agents can be configured to collect logs from Windows Defender for Windows and ClamAV for Linux operating systems. Wazuh includes out-of-the-box decoders for Windows Defender and ClamAV logs. Decoders are necessary to extract the information from received events and prepare them for subsequent analysis. In addition, the Wazuh server also includes rules for Windows Defender and ClamAV. A rule instructs the Wazuh server to generate an alert when all specified conditions within the rule are meet.

# Windows Defender

Windows Defender provides virus and threat protection on Windows operating systems. Wazuh agents installed on Windows endpoints can be configured to collect Windows Defender logs. This enhances the ability of Wazuh to provide real-time monitoring and threat detection on Windows endpoints.

## Configuration

The first step is to configure the Wazuh agent to collect Windows Defender logs. This can be accomplished using centralised configuration or local configuration. This guide will use local configuration.

1. Run notepad as administrator on the Windows endpoint (Figure 1).

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Run notepad as administrator

1. Open the local configuration file on the Windows agent (Figure 2):

C:\Program Files (x86)\ossec-agent\ossec.conf

A screenshot of a computer

AI-generated content may be incorrect.

Figure : Open the local configuration file

1. Add the following code block to the configuration file (Figure 3):

<localfile>

<location>Microsoft-Windows-Windows Defender/Operational</location>

<log\_format>eventchannel</log\_format>

</localfile>

A screenshot of a computer program

AI-generated content may be incorrect.

Figure : Add the code block

1. Save the file.

## Decoders and Rules

Rules for Windows Defender can be found in the following file on the Wazuh server:

/var/ossec/ruleset/rules/0600-win-wdefender\_rules.xml

## Alert sample

The below data is an example of a Windows Defender alert. Alerts can be triggered by both user and malware activity on monitored endpoints. Alerts can be found in the following files on the Wazuh server:

/var/ossec/logs/alerts/alerts.log

/var/ossec/logs/alerts/alerts.json

Alert created when Windows Defender protection is disabled:

\*\* Alert 1755504046.9349977: - windows,windows\_defender,pci\_dss\_5.1,pci\_dss\_10.2.6,pci\_dss\_10.6.1,gpg13\_4.14,gpg13\_10.1,gdpr\_IV\_35.7.d,hipaa\_164.312.b,nist\_800\_53\_SI.3,nist\_800\_53\_AU.14,nist\_800\_53\_AU.5,nist\_800\_53\_AU.6,tsc\_A1.2,tsc\_CC6.8,tsc\_CC7.2,tsc\_CC7.3,

2025 Aug 18 08:00:46 (wazuh03) 20.92.162.94->EventChannel

Rule: 62152 (level 5) -> 'Windows Defender: Antivirus real-time protection is disabled'

{"win":{"system":{"providerName":"Microsoft-Windows-Windows Defender","providerGuid":"{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}","eventID":"5001","version":"0","level":"4","task":"0","opcode":"0","keywords":"0x8000000000000000","systemTime":"2025-08-18T08:00:45.7265153Z","eventRecordID":"418","processID":"3640","threadID":"3476","channel":"Microsoft-Windows-Windows Defender/Operational","computer":"wazuh03","severityValue":"INFORMATION","message":"\"Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.\""},"eventdata":{"product Name":"Microsoft Defender Antivirus","product Version":"4.18.25070.5"}}}

win.system.providerName: Microsoft-Windows-Windows Defender

win.system.providerGuid: {11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}

win.system.eventID: 5001

win.system.version: 0

win.system.level: 4

win.system.task: 0

win.system.opcode: 0

win.system.keywords: 0x8000000000000000

win.system.systemTime: 2025-08-18T08:00:45.7265153Z

win.system.eventRecordID: 418

win.system.processID: 3640

win.system.threadID: 3476

win.system.channel: Microsoft-Windows-Windows Defender/Operational

win.system.computer: wazuh03

win.system.severityValue: INFORMATION

win.system.message: "Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled."

win.eventdata.product Name: Microsoft Defender Antivirus

win.eventdata.product Version: 4.18.25070.5

# ClamAV

ClamAV is an open source antivirus toolkit developed by Cisco. ClamAV can provide real-time protection on Linux systems and email scanning. ClamAV can be configured to forward its logs to the syslog which will be read by the Wazuh agent. This enhances the ability of Wazuh to provide real-time monitoring and threat detection on Linux endpoints.

## Configuration

The first step is to install ClamAV because it is not included in Ubuntu – the Linux distribution that we are using for our project.

1. Get the latest packages:

sudo apt update

1. Install ClamAV and ClamAV daemon:

sudo apt install clamav clamav-daemon

1. Update the virus database:

sudo freshclam

The next step is to configure ClamAV to forward its logs to the syslog file.

1. Open the clamd.conf file:

/etc/clamav/clamd.conf

1. Add the following statement (Figure 4):

LogSyslog true

A screenshot of a computer

AI-generated content may be incorrect.

Figure : clamd.conf

1. Save the file.

Now we will verify that ClamAV is forwarding logs to syslog and that the Wazuh agent is reading them.

1. Create the EICAR test file:

set +H

echo "X5O!P%@AP[4\\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*" > ~/eicar.com

1. Scan the file:

clamdscan --fdpass ~/eicar.com

1. Check the log files:

sudo cat /var/log/clamav/clamav.log

/var/log/syslog

## Decoders and rules

Rules for ClamAV can be found in the following file on the Wazuh server:

/var/ossec/ruleset/rules/0320-clam\_av\_rules.xml

## Alert sample

The below data is an example of a ClamAV alert. Alerts can be found in the following files on the Wazuh server:

/var/ossec/logs/alerts/alerts.log

/var/ossec/logs/alerts/alerts.json

Alert created when ClamAV detects malware:

\*\* Alert 1756794767.2189018: mail - clamd,freshclam,virus,pci\_dss\_5.1,pci\_dss\_5.2,pci\_dss\_11.4,gpg13\_4.2,gdpr\_IV\_35.7.d,nist\_800\_53\_SI.3,nist\_800\_53\_SI.4,tsc\_A1.2,tsc\_CC6.1,tsc\_CC6.8,tsc\_CC7.2,tsc\_CC7.3,

Sep 02 06:32:47 wazuh04 clamd[2530]: Tue Sep 2 06:32:47 2025 -> /home/josh/eicar.com: Eicar-Signature(69630e4574ec6798239b091cda43dca0:69) FOUND

\*\* Alert 1756794767.2189475: mail - clamd,freshclam,virus,pci\_dss\_5.1,pci\_dss\_5.2,pci\_dss\_11.4,gpg13\_4.2,gdpr\_IV\_35.7.d,nist\_800\_53\_SI.3,nist\_800\_53\_SI.4,tsc\_A1.2,tsc\_CC6.1,tsc\_CC6.8,tsc\_CC7.2,tsc\_CC7.3,

Sep 02 06:32:47 wazuh04 clamd[2530]: /home/josh/eicar.com: Eicar-Signature(69630e4574ec6798239b091cda43dca0:69) FOUND

# Bibliography

Cisco n.d., *Introduction – ClamAV Documentation*, 19 August 2025, <https://docs.clamav.net/>

Ubuntu Community Help Wiki 2017, *ClamAV*, wiki, viewed 19 August 2025, <https://help.ubuntu.com/community/ClamAV>

Wazuh 2025, *ClamAV logs collection*, viewed 19 August 2025, <https://documentation.wazuh.com/4.12/user-manual/capabilities/malware-detection/clam-av-logs-collection.html>

Wazuh 2025, *Decoders syntax*, viewed 14 September 2025, <https://documentation.wazuh.com/4.12/user-manual/ruleset/ruleset-xml-syntax/decoders.html>

Wazuh 2025, *Rules syntax*, viewed 14 September 2025, <https://documentation.wazuh.com/4.12/user-manual/ruleset/ruleset-xml-syntax/rules.html>

Wazuh 2025, *Windows Defender logs collection*, viewed 18 August 2025, <https://documentation.wazuh.com/4.12/user-manual/capabilities/malware-detection/win-defender-logs-collection.html>