

# **Wazuh File Integrity Monitoring**

## **Introduction**

File Integrity Monitoring is an important security feature that checks the integrity of files and directories on a system. It helps to ensure that no file is changed, deleted or created without proper authorization. Even a small unauthorized change in system files can cause security risks, system failures or potential attacks.

Wazuh, an open-source security monitoring platform, provides FIM capabilities. By using this we can continuously monitor critical system files and receive alerts whenever unauthorized changes occur.

## **What We Achieved**

By enabling FIM on Ubuntu Agent and Windows Agent and connecting them with Wazuh Manager we achieve:

Continuous monitoring of important system files.

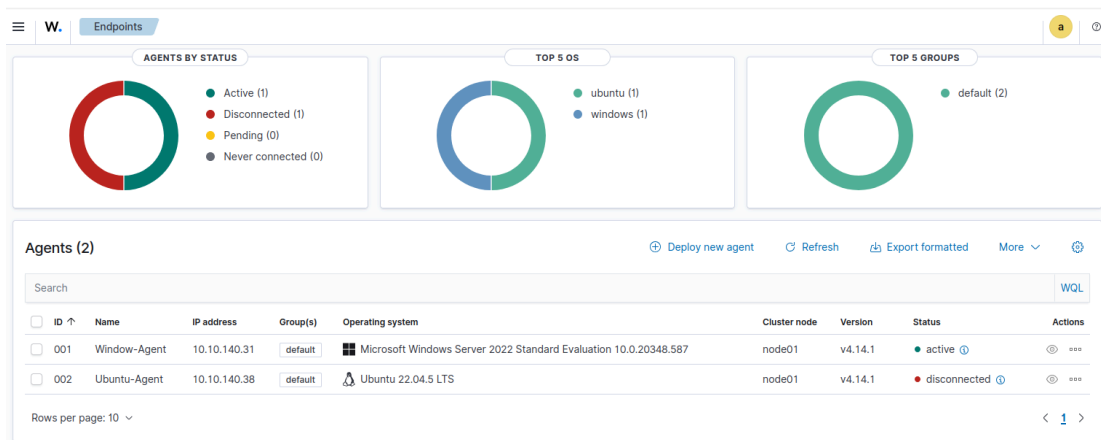
Real-time alerts whenever files are modified, deleted, or created without permission.

Centralized monitoring through Wazuh Dashboard, allowing us to view all file changes from a single place.

Early detection of potential attacks such as malware modifying system files.

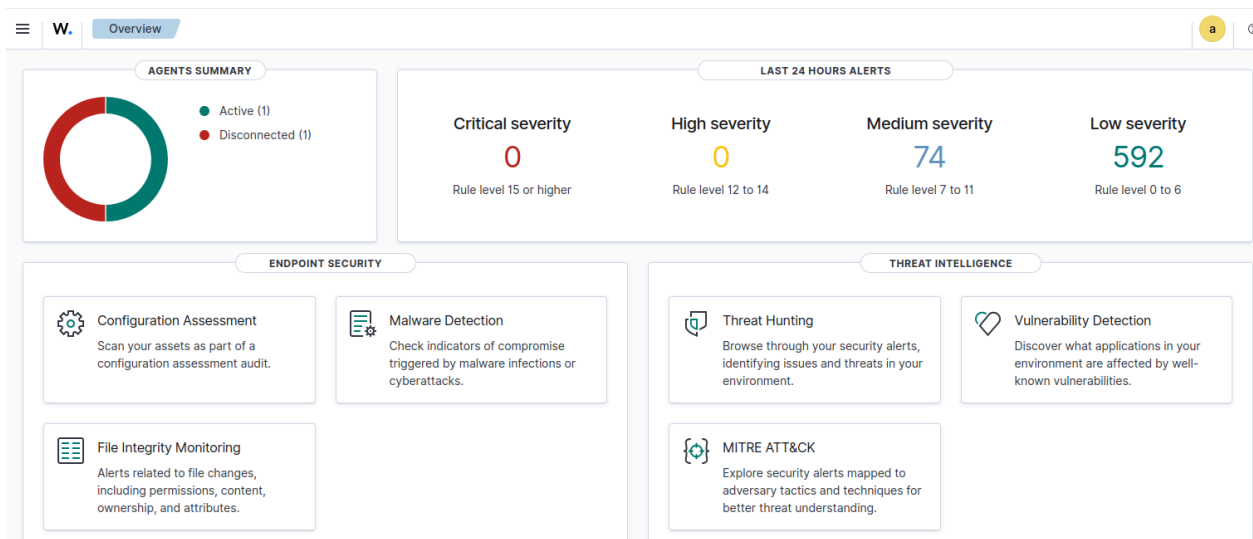
## Windows FIM

In our lab environment Wazuh Server and Window Agent are now in running state so first we implement the FIM in the Windows system.  
Dashboard of Wazuh Server:

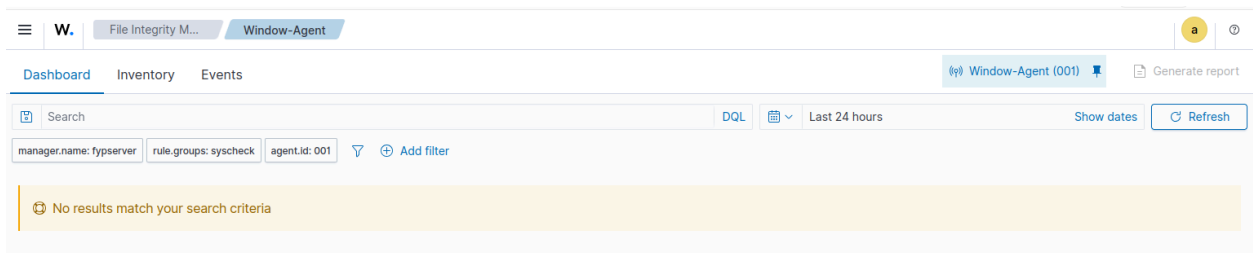


In Dashboard there are a total two agents but now only one Agent is active and that is Windows Agent which is in running state.

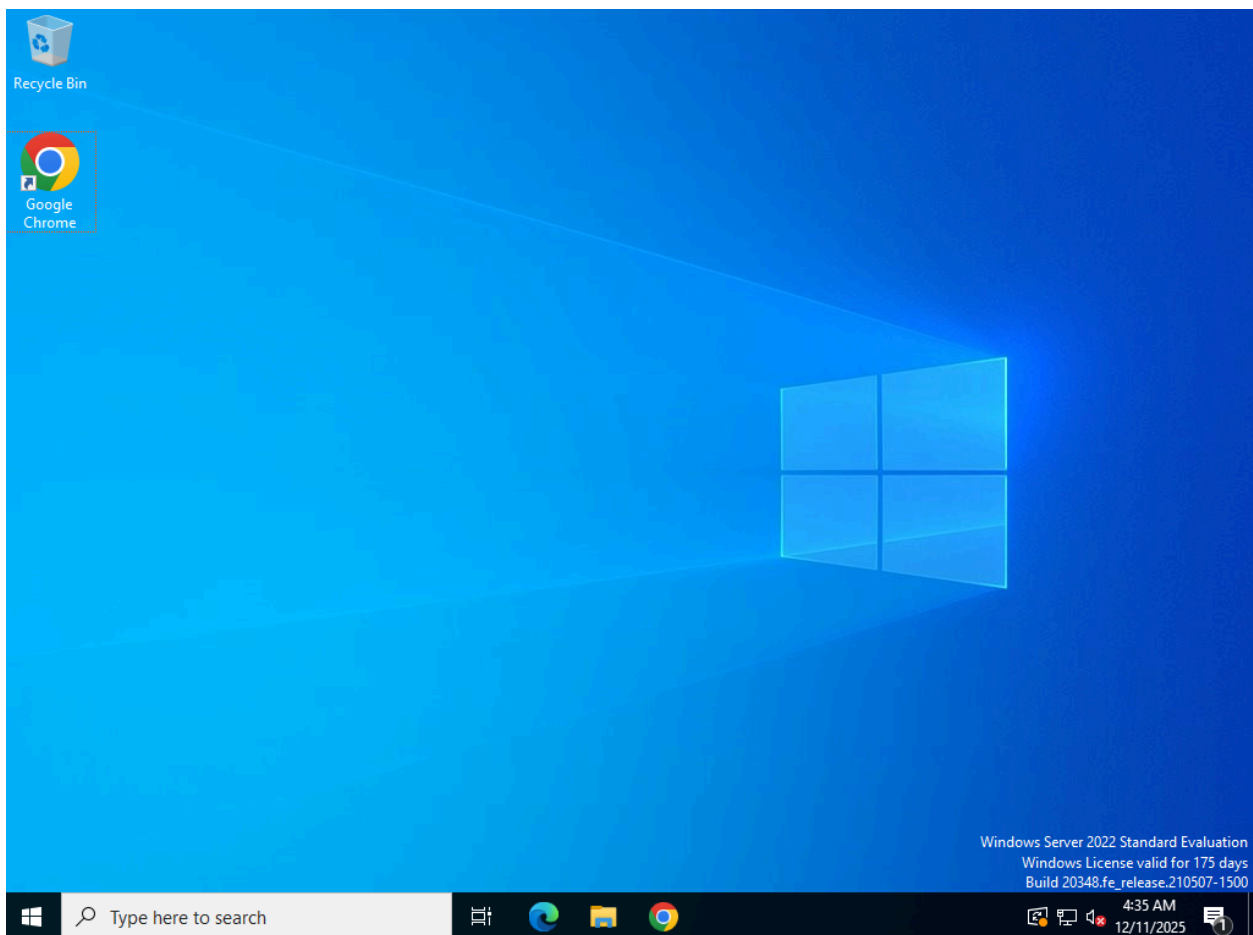
In Dashboard there is a section of Endpoint Security where you can see the “File Integrity Monitoring” click on it and go into this section and select the Agent.



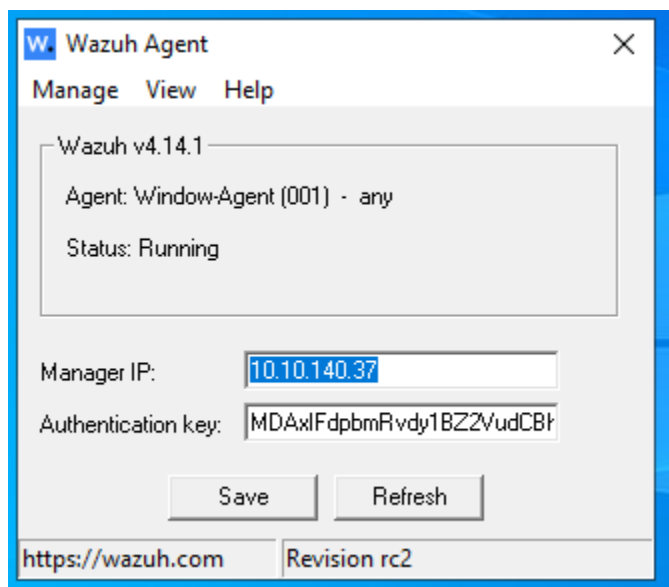
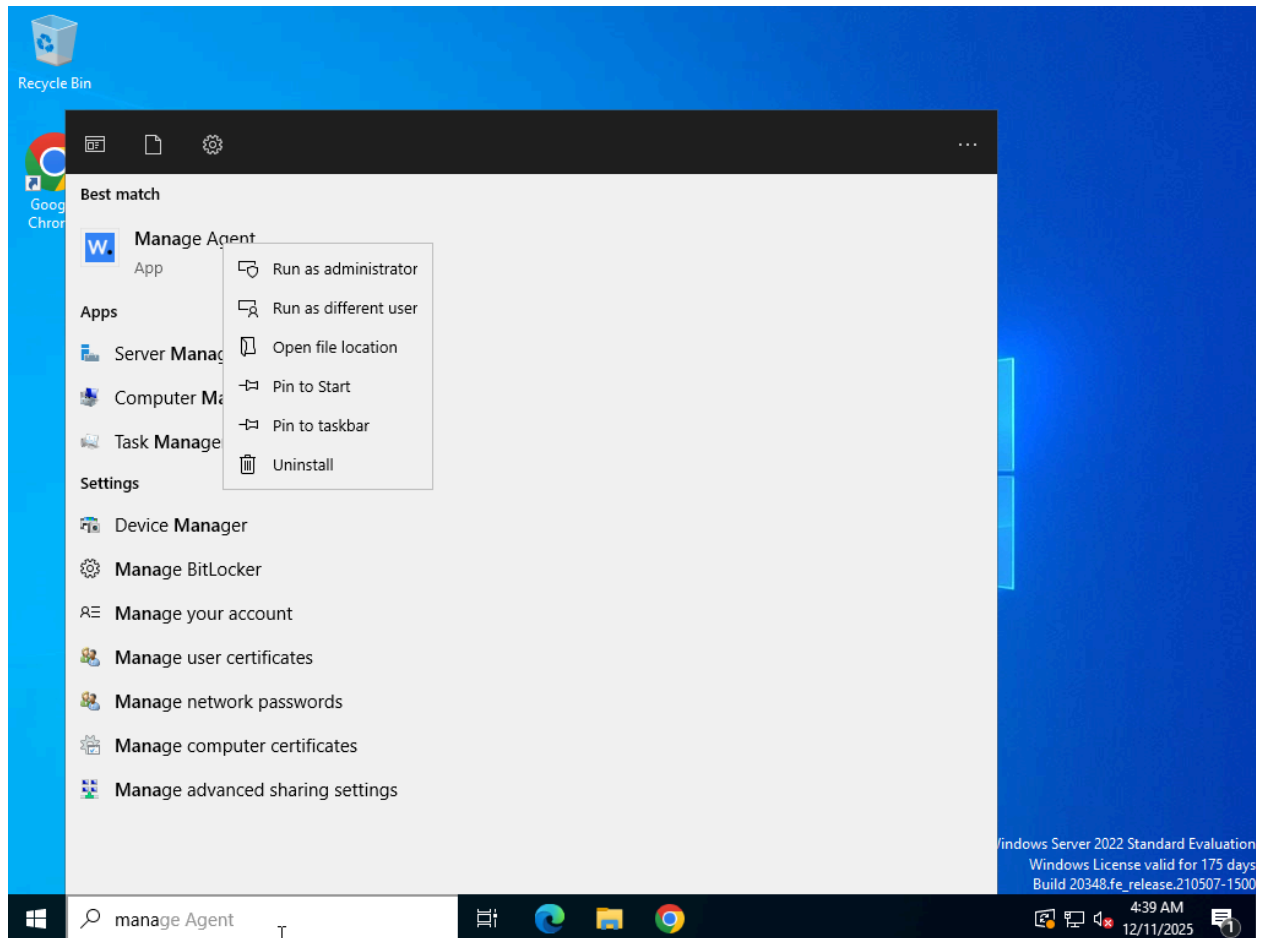
And we see there is no data as no FIM module is configured. So we configured it.



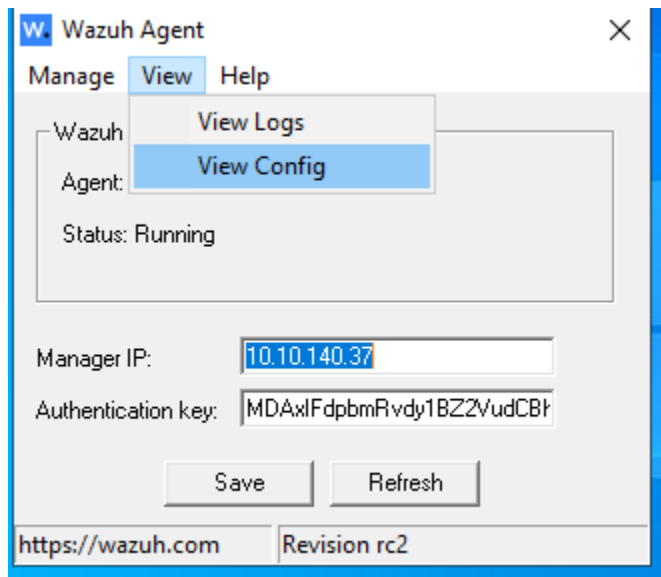
Now, first we go into the Windows Machines where Agent is installed and perform the configurations.



Search Agent in the menu bar and select it with Administration.



Now Wazuh Agent is launched and goes to view and selects “view config” for configuration.



Now we are in the configuration file where we add the path for directories which we want to monitor.

A screenshot of a Notepad window titled 'ossec.conf - Notepad'. The window shows the XML configuration for Wazuh. The configuration includes sections for Policy monitoring, Security Configuration Assessment (sca), and File integrity monitoring (syscheck). The syscheck section is highlighted in blue. The configuration is as follows:

```
<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
  <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

<!-- Security Configuration Assessment -->
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>

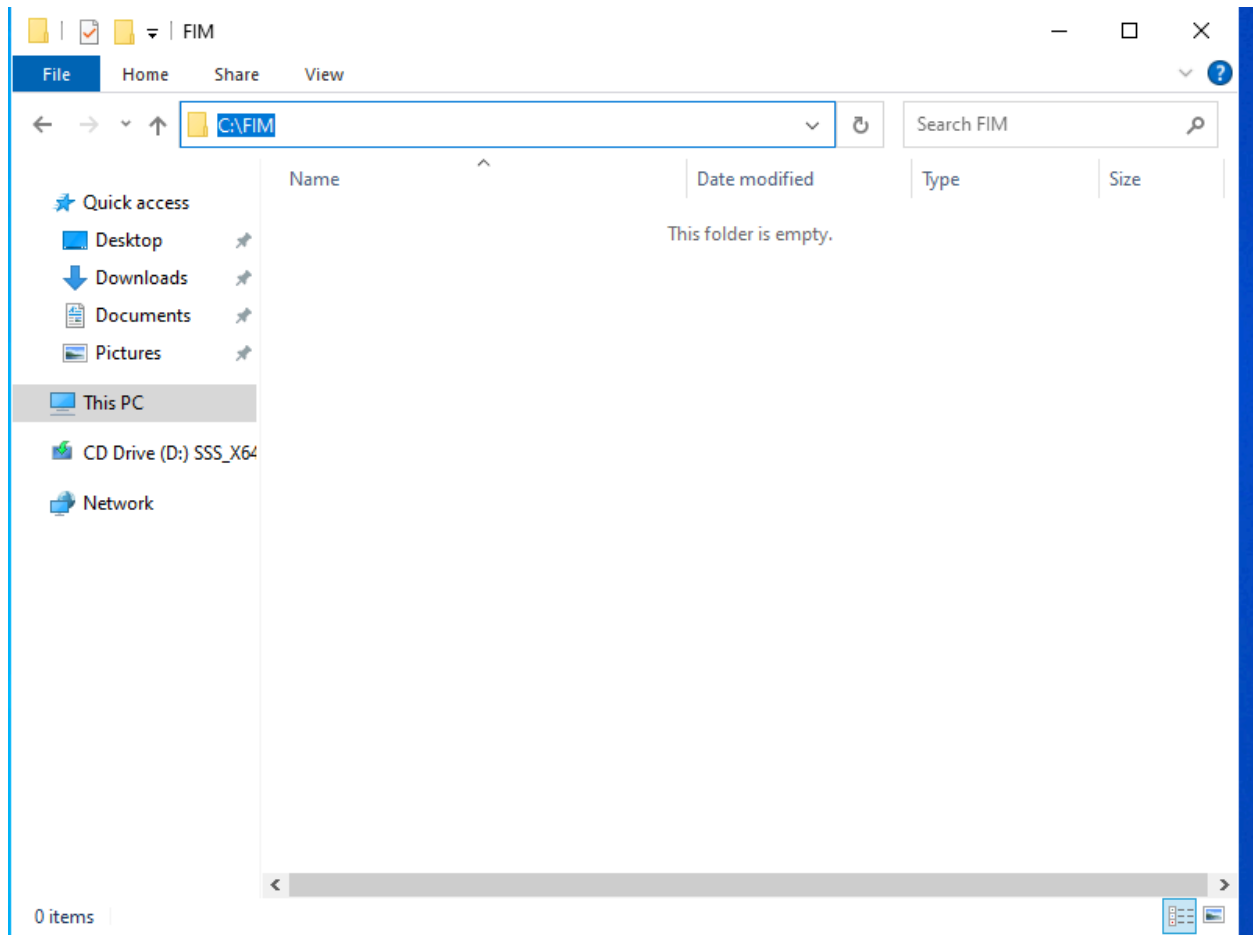
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored -->
```

The status bar at the bottom shows 'Ln 73, Col 3', '100%', 'Windows (CRLF)', and 'UTF-8'.

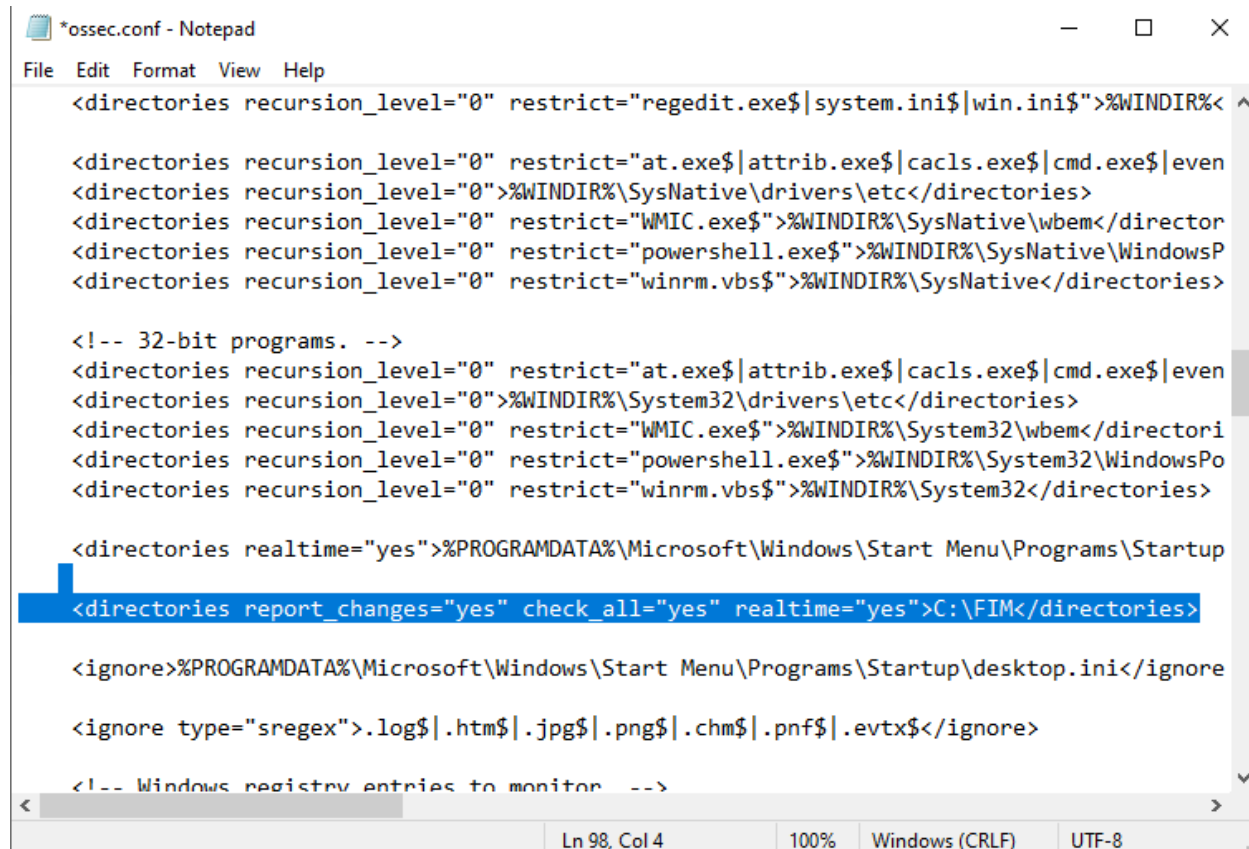
As we want to monitor the “C://FIM” folder so we add the path for this directory in the configuration file.



Copy this path and add it.

Add this line:

```
<directories report_changes="yes"check_all="yes" realtime="yes">C:\FIM</directories>
```



```
*ossec.conf - Notepad
File Edit Format View Help

<directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$" %WINDIR%<
^

<directories recursion_level="0" restrict="at.exe$|attrib.exe$|caccls.exe$|cmd.exe$|even
<directories recursion_level="0" %WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\SysNative\wbem</director
<directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\SysNative\WindowsP
<directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\SysNative</directories>

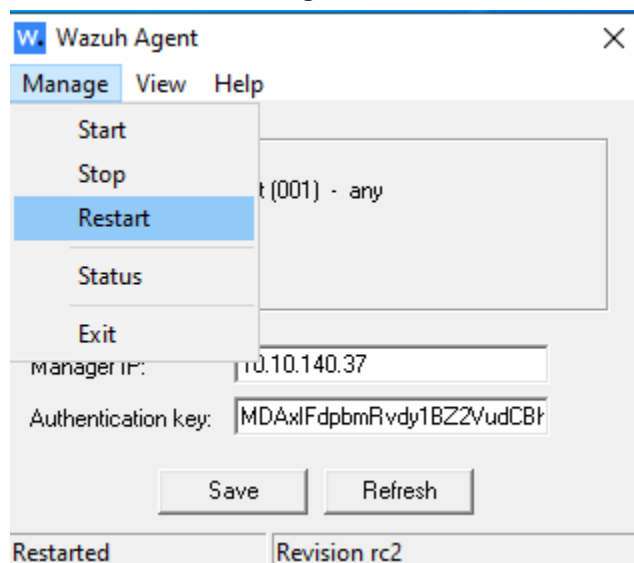
<!-- 32-bit programs. -->
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|caccls.exe$|cmd.exe$|even
<directories recursion_level="0" %WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\System32\wbem</director
<directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\System32\WindowsPo
<directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\System32</directories>

<directories realtime="yes" %PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup
<directories report_changes="yes" check_all="yes" realtime="yes" C:\FIM</directories>
<ignore %PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

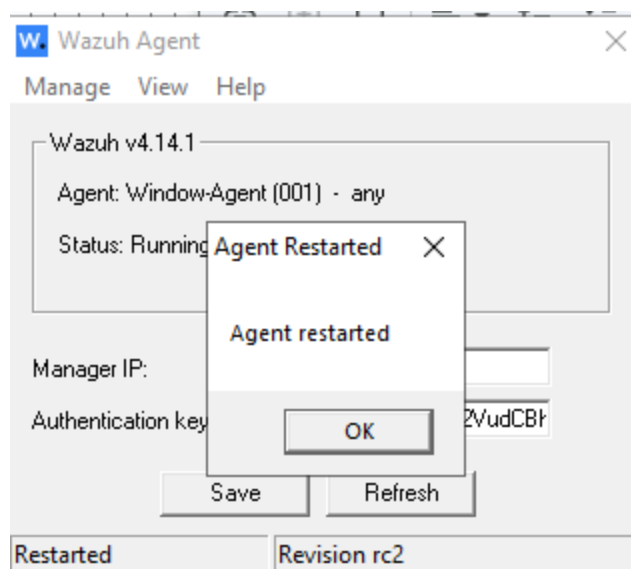
<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>

<!-- Windows registry entries to monitor -->
```

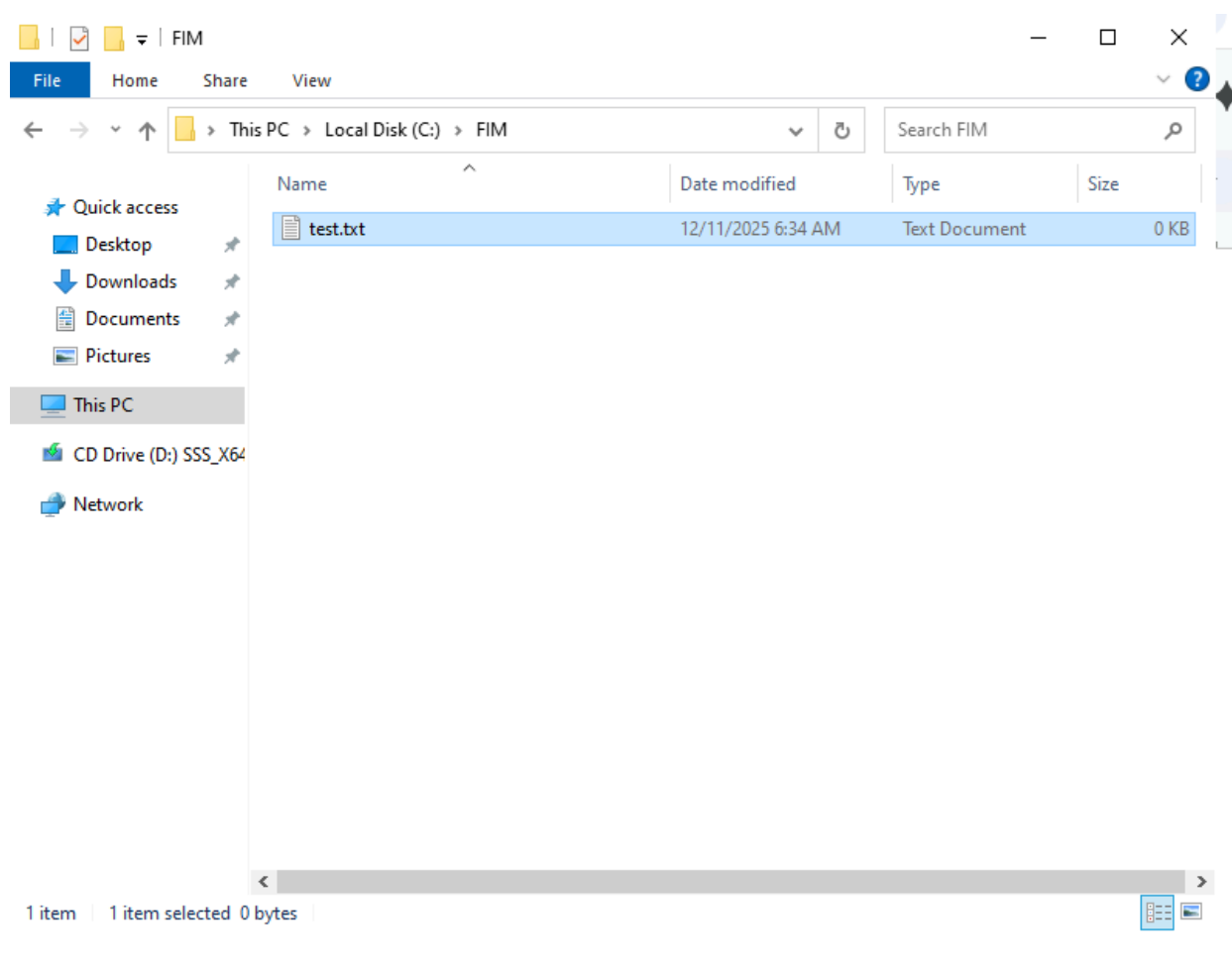
Save the changes and close the “ ossec.conf ” file.  
Restart the Wazuh Agent.



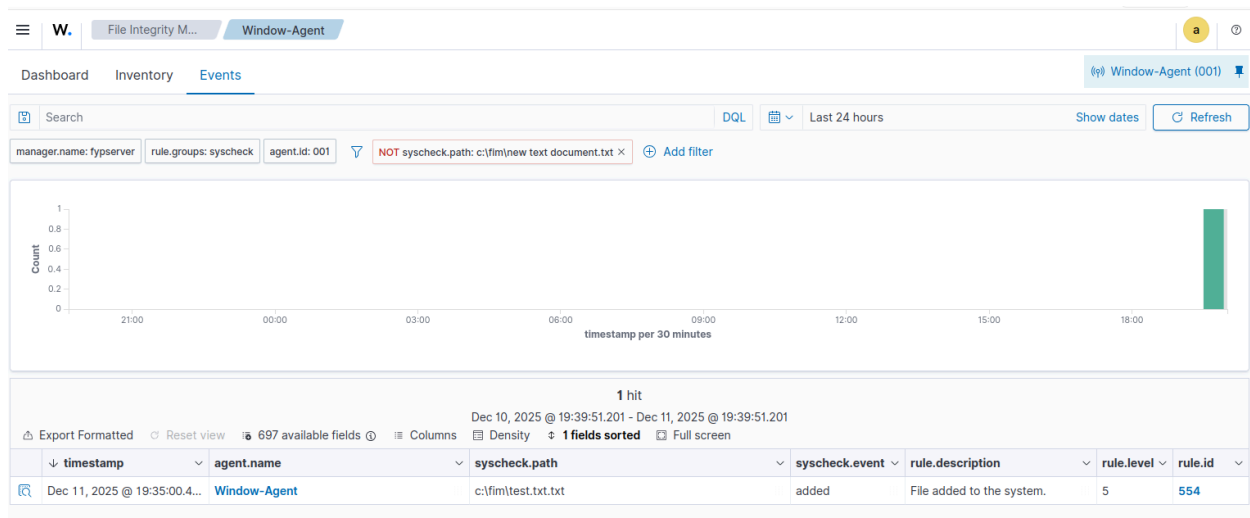
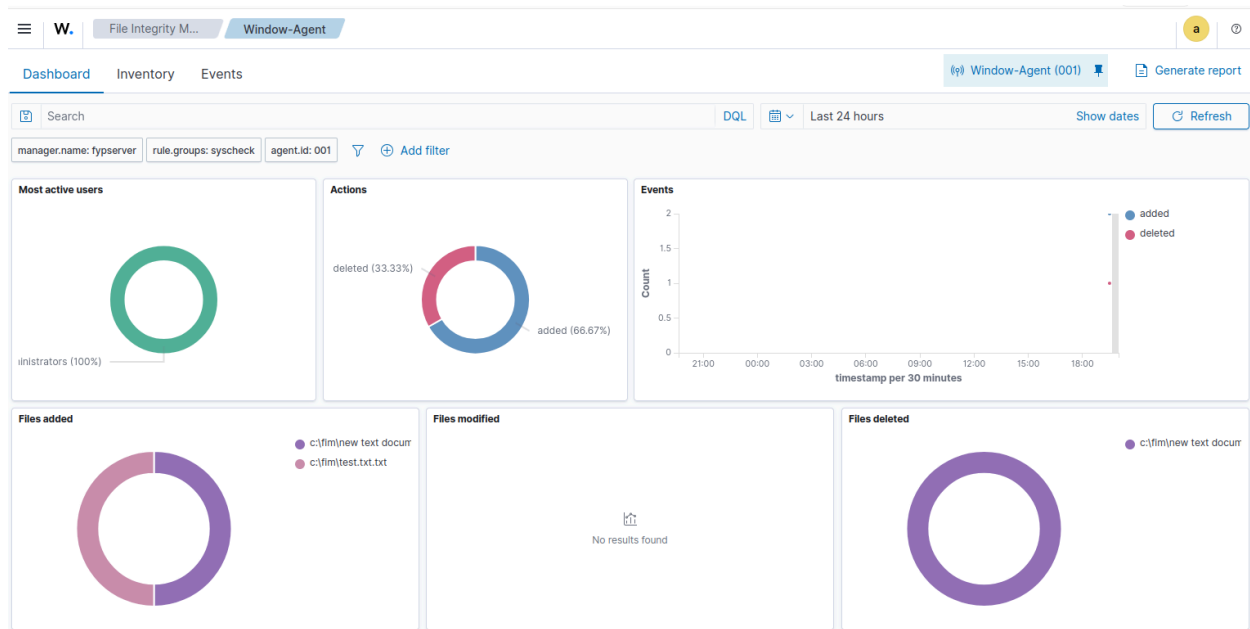
Click ok.



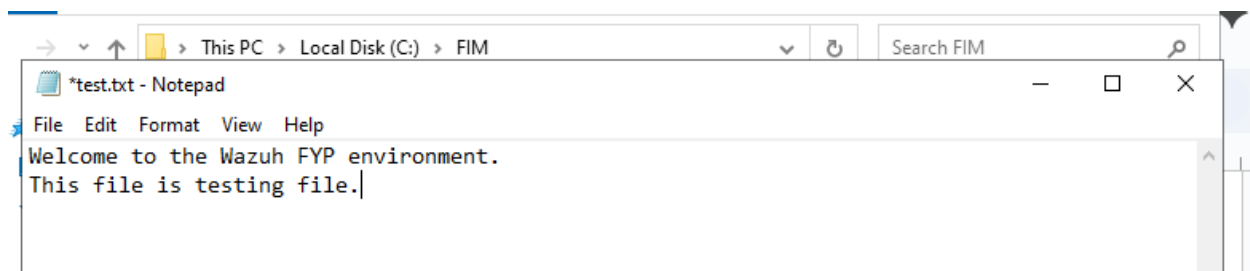
Now we create a test file for the testing purpose in the monitoring directory.



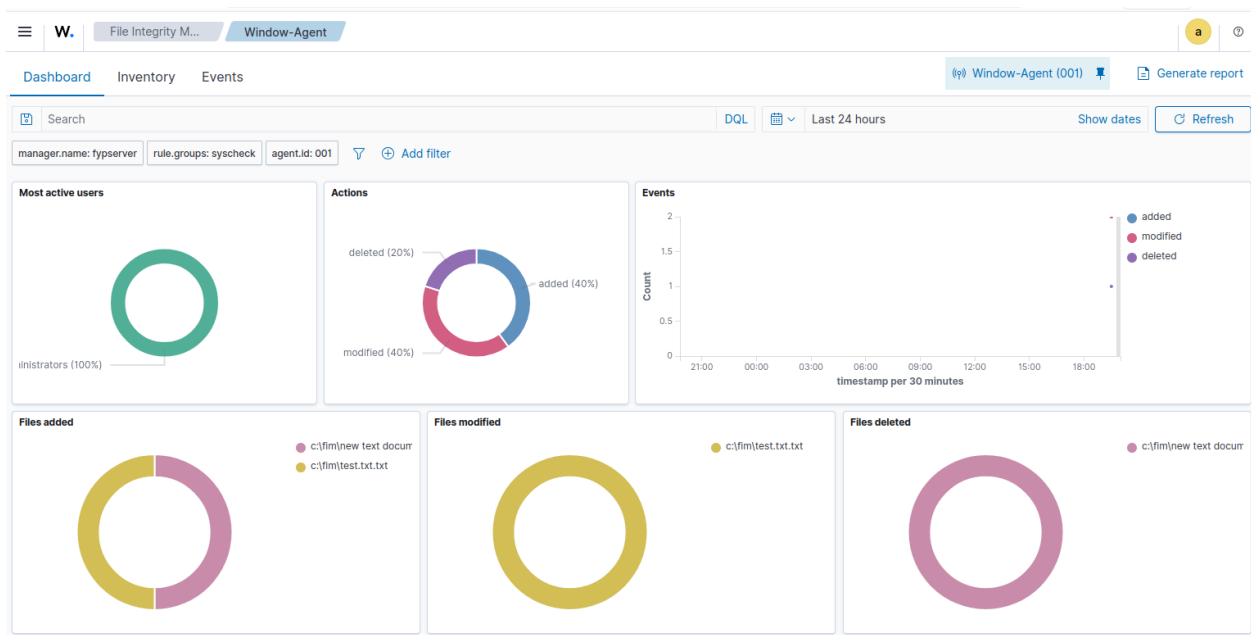
When we create a file then a real-time alerts will show in the Wazuh Dashboard.



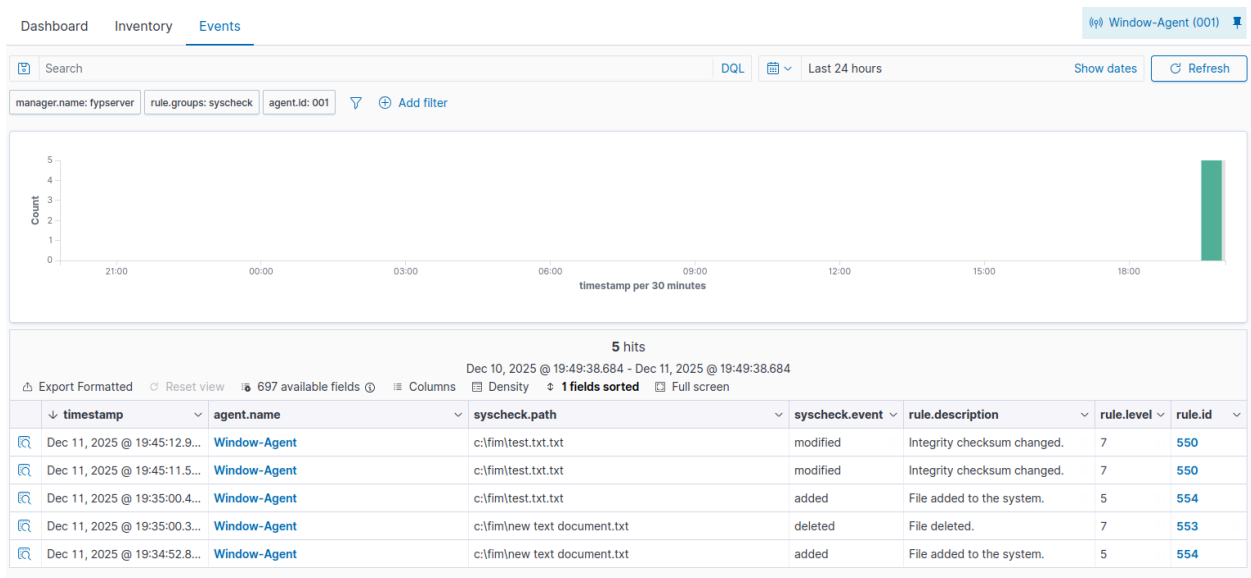
Now perform the modification in file for modification alerts.



Save this file and refresh the Wazuh Dashboard and now we see the modification alerts on it.



And we can also see the alerts in the events section.



Now click on any events and see the details of alerts.

## Document Details

[View surrounding documents](#)[View single document](#)

**Table** JSON

t _index	wazuh-alerts-4.x-2025.12.11
t agent.id	001
t agent.ip	10.10.140.31
t agent.name	Window-Agent
t decoder.name	syscheck_new_entry
t full_log	File 'c:\fim\test.txt.txt' added Mode: realtime
t id	1765463700.444566
t input.type	log
t location	syscheck
t manager.name	fypserver
t rule.description	File added to the system.
# rule.firedtimes	2
t rule.gdpr	II_5.1.f
t rule.gpg13	4.11
t rule.groups	ossec, syscheck, syscheck_entry_added, syscheck_file
t rule.hipaa	164.312.c.1, 164.312.c.2
t rule.id	554
# rule.level	5
rule.mail	false

## Document Details

[View surrounding documents](#)[View single document](#)

**Table** JSON

t _index	wazuh-alerts-4.x-2025.12.11
t agent.id	001
t agent.ip	10.10.140.31
t agent.name	Window-Agent
t decoder.name	syscheck_integrity_changed
t full_log	File 'c:\fim\test.txt.txt' modified Mode: realtime Changed attributes: mtime Old modification time was: '1765464311', now it is '1765464312'
t id	1765464312.466576
t input.type	log
t location	syscheck
t manager.name	fypserver
t rule.description	Integrity checksum changed.
# rule.firedtimes	2
t rule.gdpr	II_5.1.f
t rule.gpg13	4.11
t rule.groups	ossec, syscheck, syscheck_entry_modified, syscheck_file
t rule.hipaa	164.312.c.1, 164.312.c.2
t rule.id	550
# rule.level	7

t syscheck.event	modified
t syscheck.md5_after	d0e38d8842363f251b6078abf8f80579
t syscheck.md5_before	d41d8cd98f00b204e9800998ecf8427e
t syscheck.mode	realtime
📅 syscheck.mtime_after	Dec 12, 2025 @ 00:45:11.000
📅 syscheck.mtime_before	Dec 12, 2025 @ 00:34:52.000
t syscheck.path	c:\fim\test.txt.txt
t syscheck.sha1_after	09e381945b3a1910f38fc01d3cf71ac3b5b4822c
t syscheck.sha1_before	da39a3ee5e6b4b0d3255bfef95601890afd80709
t syscheck.sha256_after	ddbfb8937073ff33d434b2214eddec5978bd885b98b8fbcc354ced959560fae1e
t syscheck.sha256_before	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
# syscheck.size_after	65
# syscheck.size_before	0
t syscheck.uid_after	S-1-5-32-544
t syscheck.uname_after	Administrators
t syscheck.win_perm_after.allowed	DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, DELETE, READ_CONTROL, WRITE_DAC, WRITE_OWNER, SYNCHRONIZE, READ_DATA, WRITE_DATA, APPEND_DATA, READ_EA, WRITE_EA, EXECUTE, READ_ATTRIBUTES, WRITE_ATTRIBUTES, READ_CONTROL, SYNCHRONIZE, READ_DATA, READ_EA, EXECUTE, READ_ATTRIBUTES
t syscheck.win_perm_after.name	SYSTEM, Administrators, Users
📅 timestamp	Dec 11, 2025 @ 19:45:11.546

Now we successfully configured the FIM module and see the related alerts.

## Document Details

[View surrounding documents](#)

[View single document](#)



**Table**   JSON

t _index	wazuh-alerts-4.x-2025.12.11
t agent.id	001
t agent.ip	10.10.140.31
t agent.name	Window-Agent
t decoder.name	syscheck_deleted
t full_log	File 'c:\fim\new text document.txt' deleted Mode: realtime
t id	1765463700.443443
t input.type	log
t location	syscheck
t manager.name	fypserver
t rule.description	File deleted.
# rule.firedtimes	1
t rule.gdpr	II_5.1.f
t rule.gpg13	4.11
t rule.groups	ossec, syscheck, syscheck_entry_deleted, syscheck_file
t rule.hipaa	164.312.c.1, 164.312.c.2
t rule.id	553
# rule.level	7
rule.mail	false

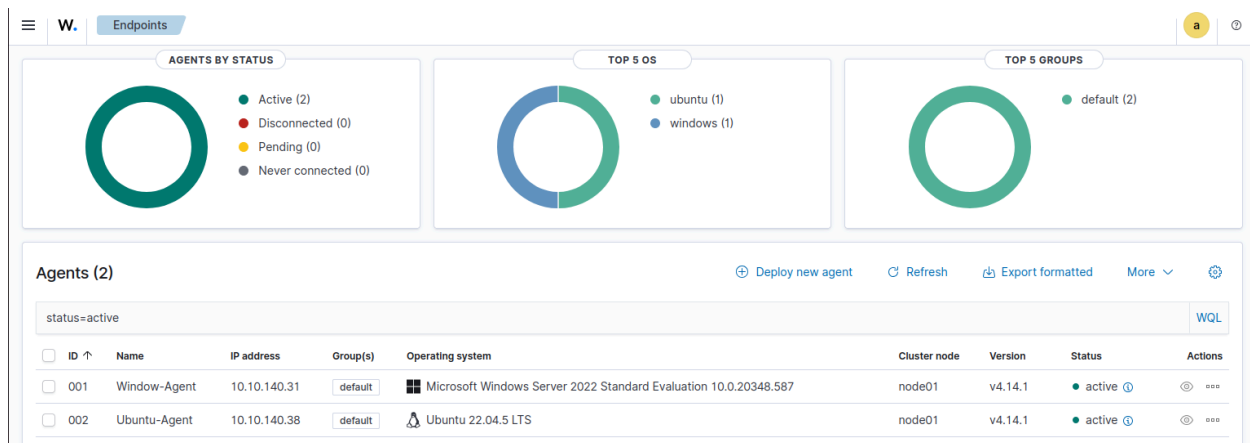
Now we successfully configured the FIM module and see the related alerts.

## Ubuntu FIM

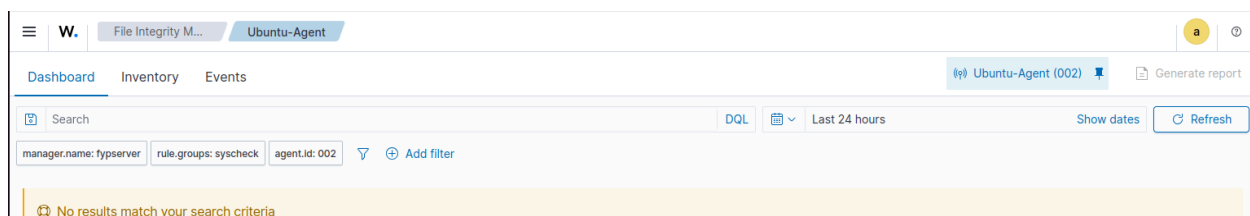
Now we configure the FIM in Ubuntu Machine where my Wazuh Agent is installed.

```
ubuntu@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ea:49:f9 brd ff:ff:ff:ff:ff:ff
    inet 10.10.140.38/24 brd 10.10.140.255 scope global dynamic noprefixroute enp0s3
        valid_lft 64900sec preferred_lft 64900sec
    inet6 fe80::938e:c0cc:c16c:736d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$
```

Now we go to Wazuh Dashboard and see the both Agents are active .



Select the Ubuntu Agent and we see there is no FIM alerts

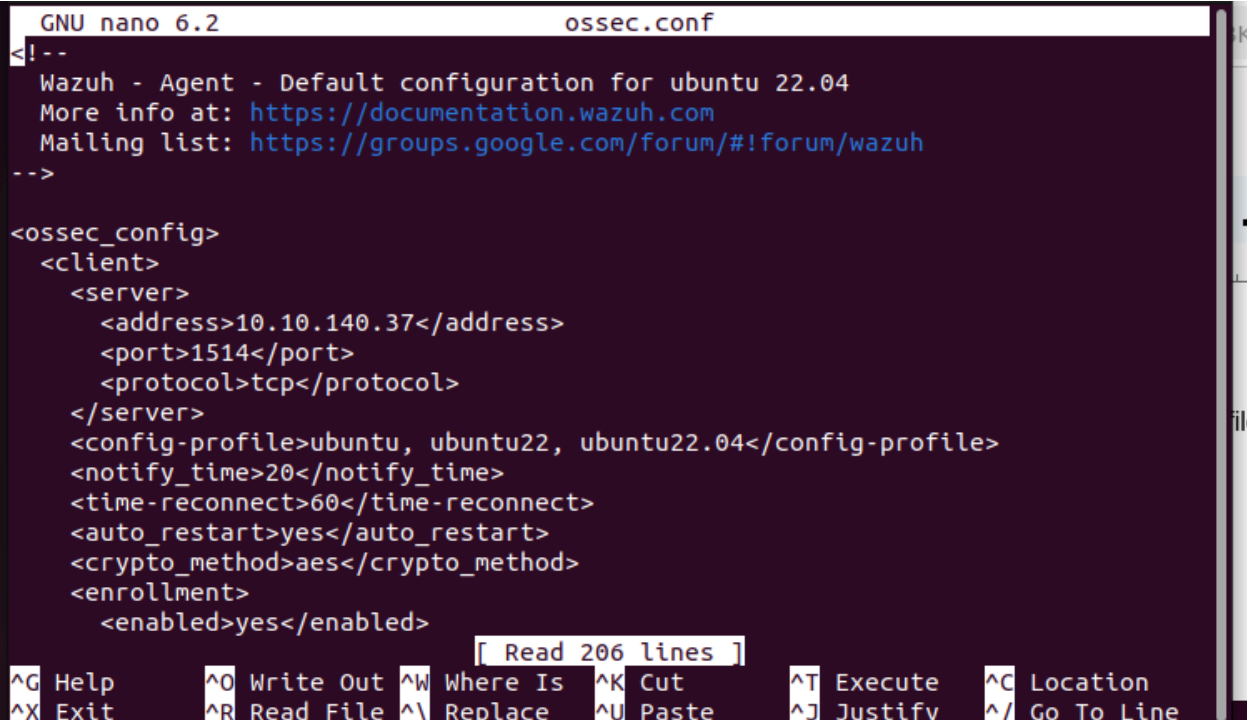


Now we are going to the Ubuntu machine to configure the ossec.conf file to monitor the critical directories.

By following command we see the configuration file:

```
sudo -i
cd /var/ossec/etc
nano ossec.conf
```

```
ubuntu@ubuntu:~$ sudo -i
root@ubuntu:~# cd /var/ossec/etc
root@ubuntu:/var/ossec/etc# ls
client.keys          local_internal_options.conf  ossec.conf  wpk_root.pem
internal_options.conf localtime                  shared
root@ubuntu:/var/ossec/etc# nano ossec.conf
```



```
GNU nano 6.2 ossec.conf
<!--
Wazuh - Agent - Default configuration for ubuntu 22.04
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>10.10.140.37</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu22, ubuntu22.04</config-profile>
    <notify_time>20</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
    <enrollment>
      <enabled>yes</enabled>
    </enrollment>
  </client>
</ossec_config>

[ Read 206 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Now add the path for which directories we want to monitor.

```
GNU nano 6.2                                ossec.conf

<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>
```

```
ubuntu@ubuntu:~$ cd /home/ubuntu/Documents
ubuntu@ubuntu:~/Documents$ cd /home/ubuntu/Downloads
ubuntu@ubuntu:~/Downloads$ cd test
ubuntu@ubuntu:~/Downloads/test$
```

```
<directories report_changes="yes" check_all="yes"
realtime="yes">/home/ubuntu/Documents</directories>
<directories report_changes="yes" check_all="yes"
realtime="yes">/home/ubuntu/Downloads</directories>
<directories report_changes="yes" check_all="yes"
realtime="yes">/home/ubuntu/Downloads/test</directories>
```

```
GNU nano 6.2                                /var/ossec/etc/ossec.conf *

<!-- Database synchronization settings -->
<synchronization>
  <max_eps>10</max_eps>
</synchronization>
</wodle>

<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>
  <!-- FIM directories which we want to monitor -->
  <directories report_changes="yes" check_all="yes" realtime="yes">/home/ubuntu/Documents</directories>
  <directories report_changes="yes" check_all="yes" realtime="yes">/home/ubuntu/Downloads</directories>
  <directories report_changes="yes" check_all="yes" realtime="yes">/home/ubuntu/Downloads/test</directories>
```

Saved the changes and restarted Wazuh Agent.

sudo systemctl restart wazuh-agent

```
ubuntu@ubuntu:~$ sudo systemctl restart wazuh-agent
ubuntu@ubuntu:~$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2025-12-11 21:05:32 PKT; 12s ago
     Process: 7390 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 35 (limit: 6287)
   Memory: 27.8M
      CPU: 11.931s
   CGroup: /system.slice/wazuh-agent.service
           └─7412 /var/ossec/bin/wazuh-execd
             └─7423 /var/ossec/bin/wazuh-agentd
               └─7437 /var/ossec/bin/wazuh-syscheckd
                 └─7447 /var/ossec/bin/wazuh-logcollector
                   └─7461 /var/ossec/bin/wazuh-modulesd

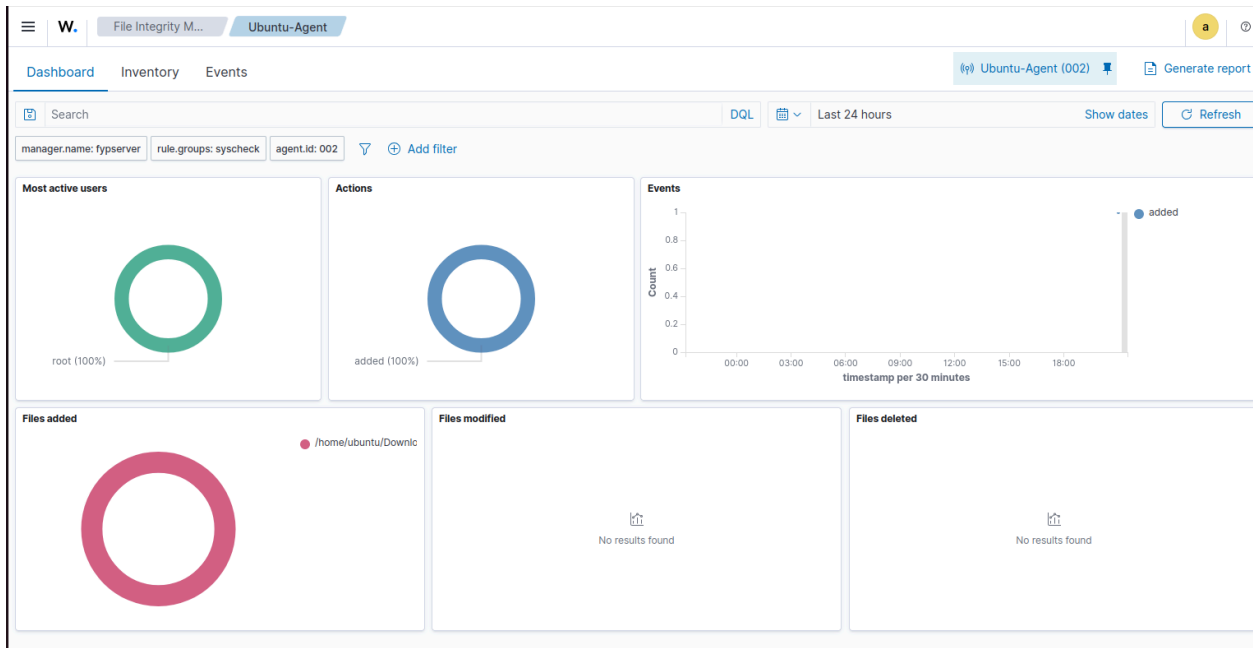
21:05:28 11 سمير ubuntu systemd[1]: Starting Wazuh agent...
21:05:28 11 سمير ubuntu env[7390]: Starting Wazuh v4.14.1...
21:05:29 11 سمير ubuntu env[7390]: Started wazuh-execd...
21:05:30 11 سمير ubuntu env[7390]: Started wazuh-agentd...
21:05:30 11 سمير ubuntu env[7390]: Started wazuh-syscheckd...
21:05:30 11 سمير ubuntu env[7390]: Started wazuh-logcollector...
21:05:30 11 سمير ubuntu env[7390]: Started wazuh-modulesd...
21:05:32 11 سمير ubuntu env[7390]: Completed.
21:05:32 11 سمير ubuntu systemd[1]: Started Wazuh agent.
ubuntu@ubuntu:~$
```

Now we create a test file for monitoring and testing purposes.

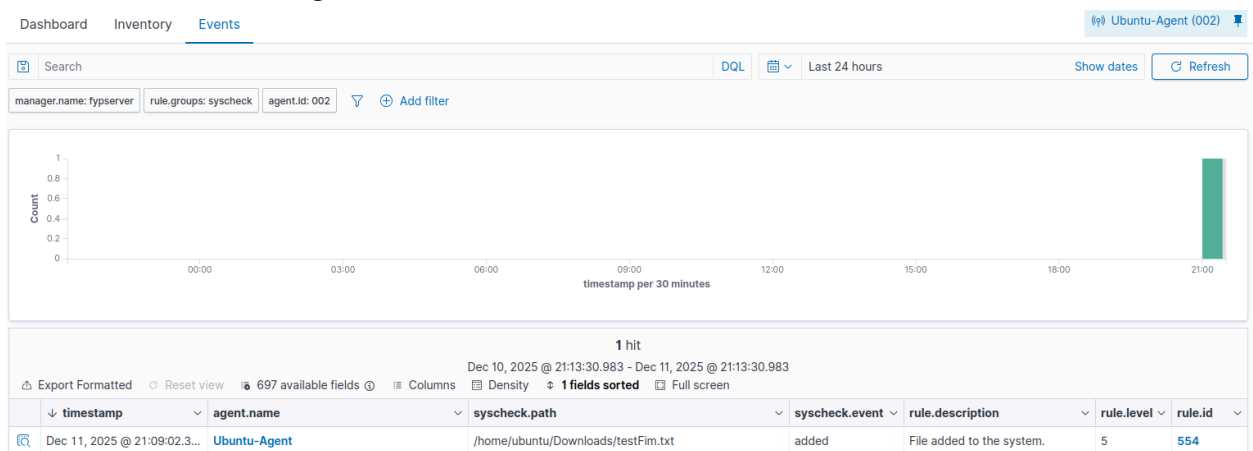
```
GNU nano 6.2 testFim.txt *
Welcome to our fyp FIM test.
This is our File Integrity Testing phase.
```

```
ubuntu@ubuntu:~/Downloads$ sudo nano testFim.txt
ubuntu@ubuntu:~/Downloads$
```

Now, we can see the alerts in the Wazuh Dashboard that are related to file integrity monitoring.

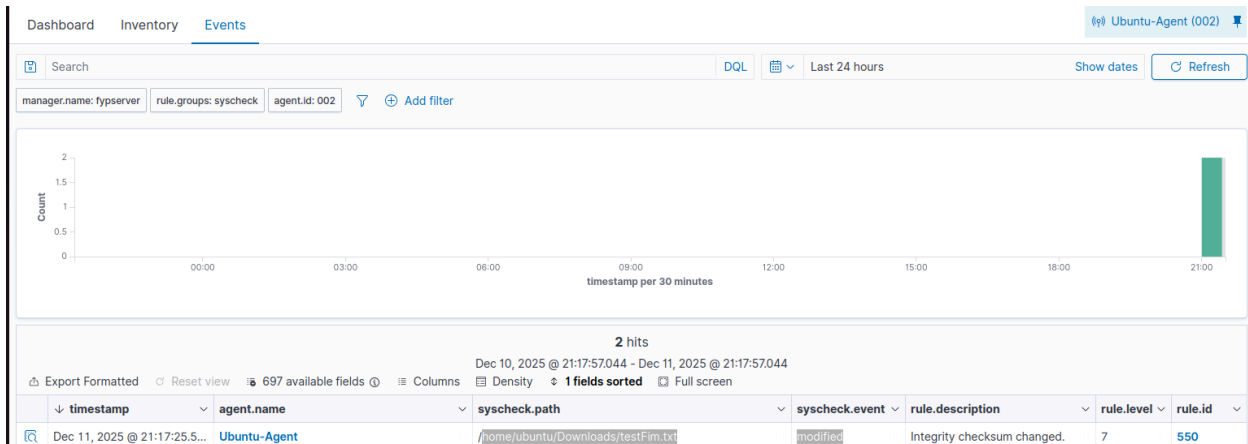


Now go to the events section and see the events, as we created the file so we see the alerts related to adding a file.

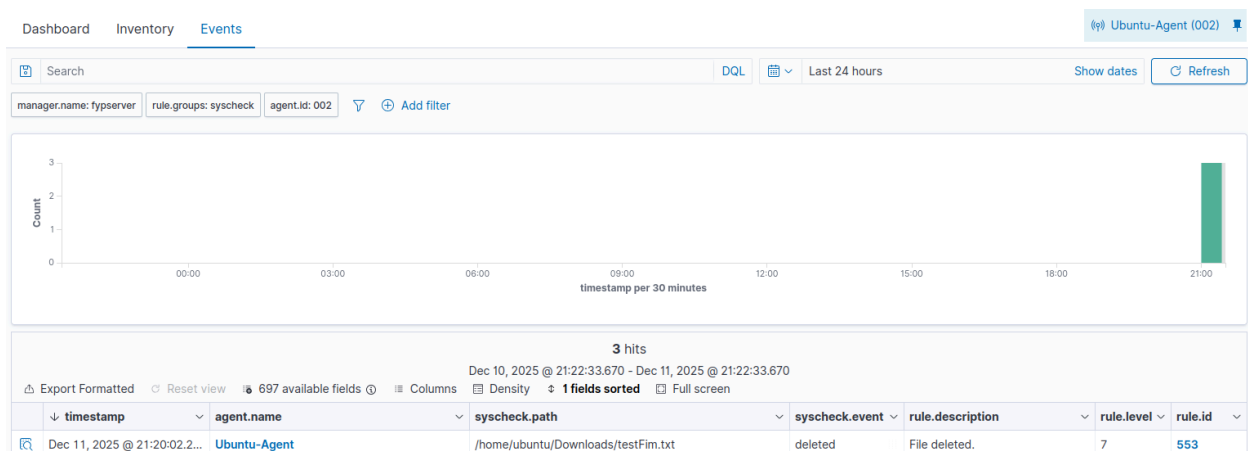


Now, modify the file and see the modified alerts in the events section.

```
GNU nano 6.2 testFim.txt *
Welcome to our fyp FIM test.
This is our File Integrity Testing phase.
Here we modified the file.
```



Now we delete a file “testFim” from the download directory and there is no file exist in downloads directory and we see their alerts in Dashboard in real time.



Now click on any events and see their details.  
So, first we click on the modified events see their details,

## Document Details

[View surrounding documents](#)[View single document](#)

**Table** JSON

t _index	wazuh-alerts-4.x-2025.12.11
t agent.id	002
t agent.ip	10.10.140.38
t agent.name	Ubuntu-Agent
t decoder.name	syscheck_integrity_changed
t full_log	File '/home/ubuntu/Downloads/testFim.txt' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '71' to '97' Old modification time was: '1765469342', now it is '1765469845' Old md5sum was: '5070edb38ca4e77ca2f1c93c695b11cf' Now md5sum is: '6807d0cf31f0a3a100707b00033c1a06'
t id	1765469845.769875
t input.type	log
t location	syscheck
t manager.name	fypserver
t rule.description	Integrity checksum changed.
# rule.firedtimes	1
t rule.gdpr	II_5.1.f
t rule.gpg13	4.11
t rule.groups	ossec, syscheck, syscheck_entry_modified, syscheck_file
t rule.hipaa	164.312.c.1, 164.312.c.2

Now, we see the details of delete events.

🔍 rule.mail	false
† rule.mitre.id	T1070.004, T1485
† rule.mitre.tactic	Defense Evasion, Impact
† rule.mitre.technique	File Deletion, Data Destruction
† rule.nist_800_53	SI.7
† rule.pci_dss	11.5
† rule.tsc	PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3
† syscheck.event	deleted
† syscheck.gid_after	0
† syscheck.gname_after	root
† syscheck.inode_after	3807634
† syscheck.md5_after	6807dcf34fea3a199707b090333c4e96
† syscheck.mode	realtime
📅 syscheck.mtime_after	Dec 12, 2025 @ 02:17:25.000
† syscheck.path	/home/ubuntu/Downloads/testFim.txt
† syscheck.perm_after	rw-r--r--
† syscheck.sha1_after	72c2bc97b145237ed005f3a9a792f2433c51109a
† syscheck.sha256_after	a540a1843c5e156bc727348935cf42c41222cce661784524ef01e8ddccb4e328
# syscheck.size_after	97
† syscheck.uid_after	0
† syscheck.uname_after	root
📅 timestamp	Dec 11, 2025 @ 21:20:02.234

Table JSON

📅 @timestamp	Dec 11, 2025 @ 21:20:02.234
† _index	wazuh-alerts-4.x-2025.12.11
† agent.id	002
† agent.ip	10.10.140.38
† agent.name	Ubuntu-Agent
† decoder.name	syscheck_deleted
† full_log	File '/home/ubuntu/Downloads/testFim.txt' deleted Mode: realtime
† id	1765470002.780772
† input.type	log
† location	syscheck
† manager.name	fypserver
† rule.description	File deleted.
# rule.firedtimes	1
† rule.gdpr	II_5.1.f
† rule.gpg13	4.11
† rule.groups	ossec, syscheck, syscheck_entry_deleted, syscheck_file
† rule.hipaa	164.312.c.1, 164.312.c.2
† rule.id	553

**Summary:**

We successfully configured the File Integrity Module( FIM) module on both Ubuntu and Window Machines. After the setup, Wazuh started detecting all configured directories activities and alerts are now visible in Wazuh Dashboard which confirms that FIM is working correctly on both systems.