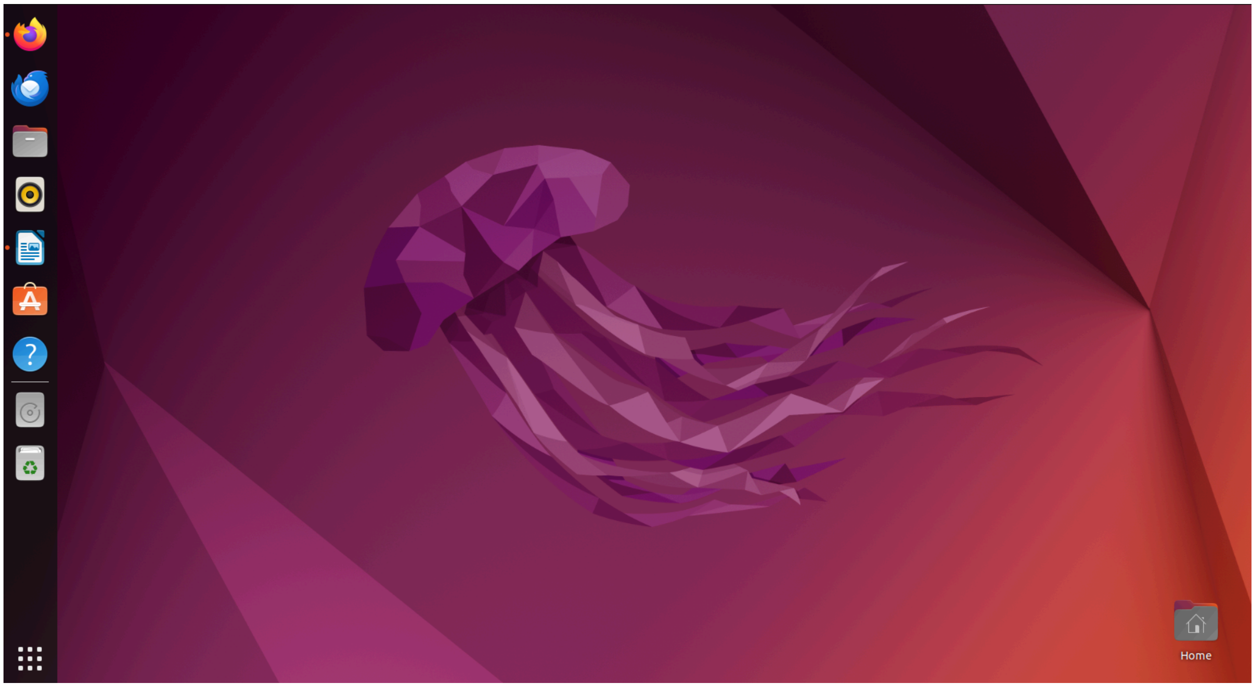
Wazuh Server Installation(Final Year Project)

Introduction

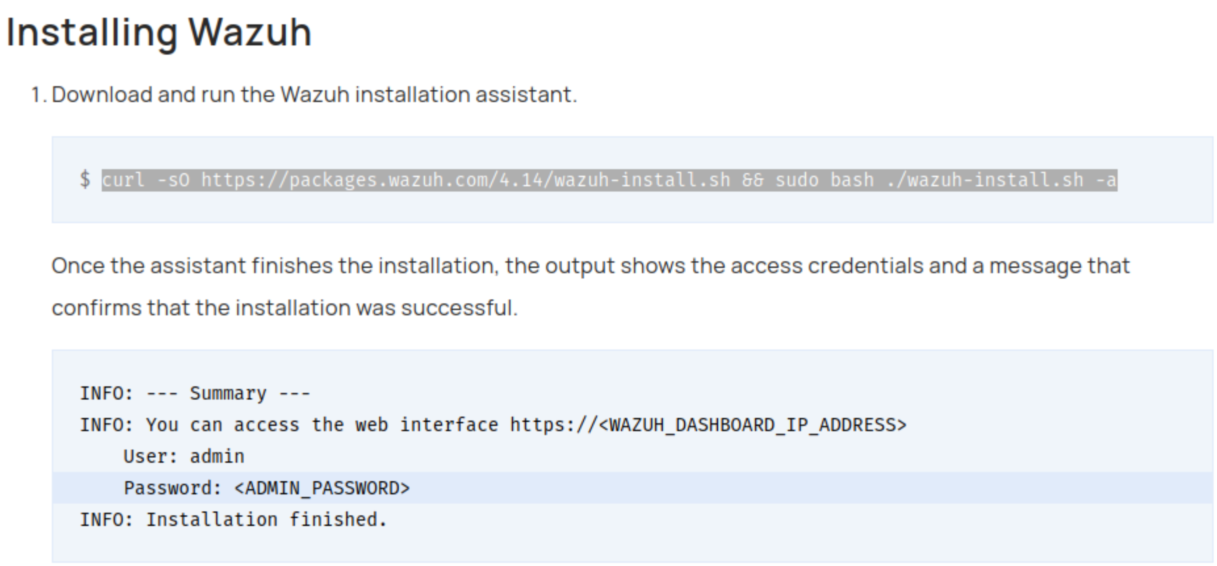
Our project starts with the complete and basic setup of Wazuh as it serves as the central monitoring and security management system for all components that we build later in the project. First, we installed the Wazuh Manager along with all of its essential components in our environment. We installed it on the Ubuntu operating system.



Installing Wazuh:

We installed the latest available version of Wazuh, **version 4.14**, by following the official documentation provided on the Wazuh website:

https://documentation.wazuh.com/current/quickstart.html



Installing Wazuh

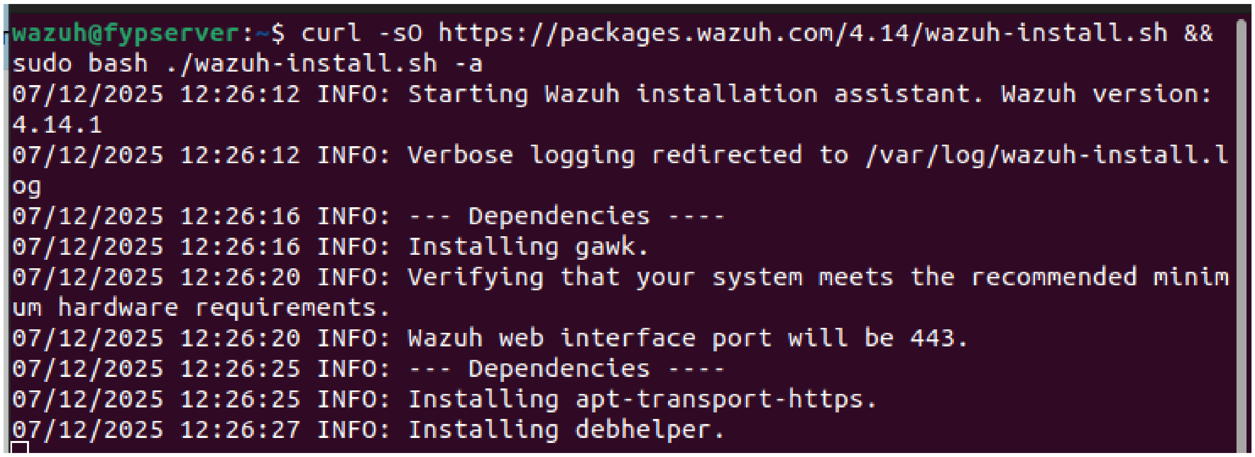
1. Download and run the Wazuh installation assistant.

```
$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

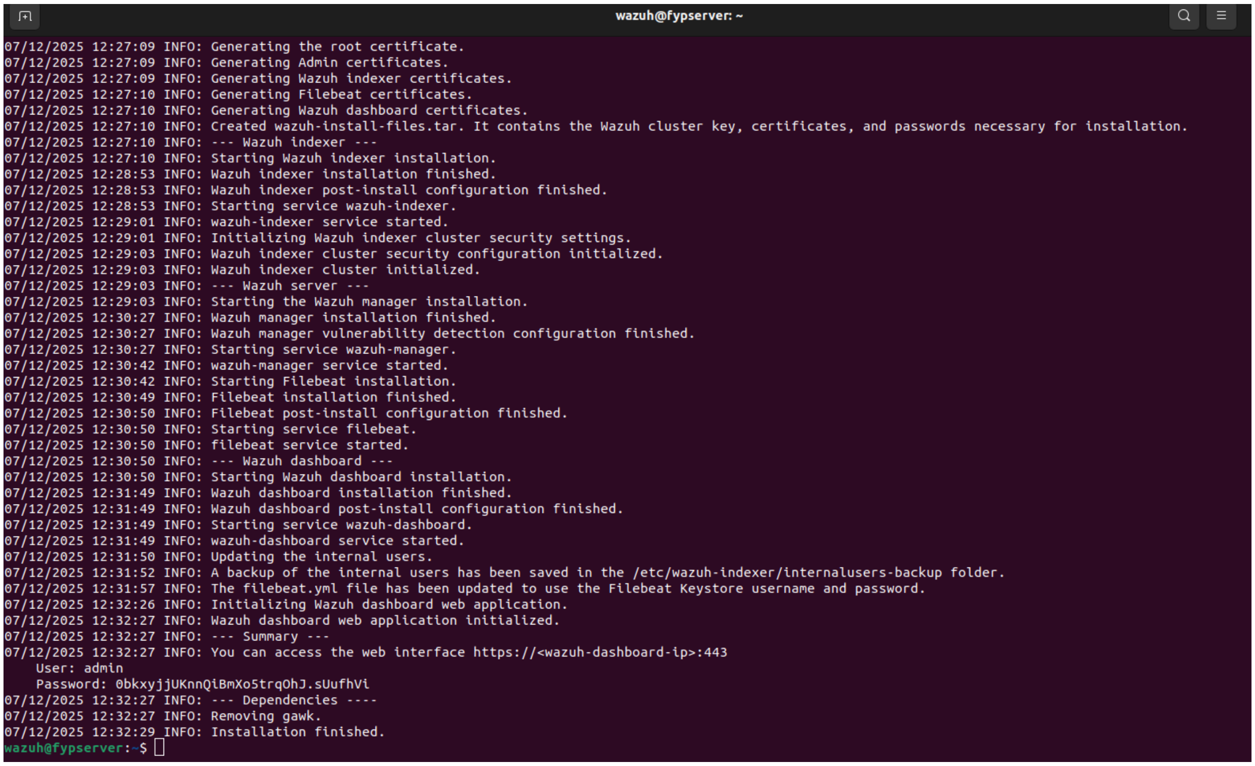
Once the assistant finishes the installation, the output shows the access credentials and a message that confirms that the installation was successful.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<WAZUH_DASHBOARD_IP_ADDRESS>
    User: admin
    Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

Copy this command and run it on the Ubuntu system terminal.
For our project we use the All-in-One Installation Method which installs and configures the core components automatically. Such as Wazuh Indexer, Wazuh Server and Wazuh Dashboard.

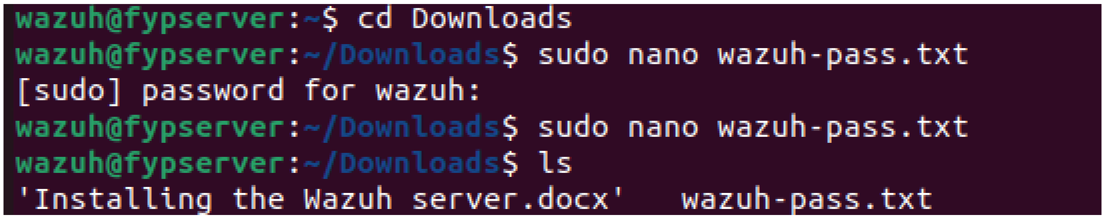


```
wazuh@fypserver:~$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh &&
sudo bash ./wazuh-install.sh -a
07/12/2025 12:26:12 INFO: Starting Wazuh installation assistant. Wazuh version:
4.14.1
07/12/2025 12:26:12 INFO: Verbose logging redirected to /var/log/wazuh-install.l
og
07/12/2025 12:26:16 INFO: --- Dependencies ----
07/12/2025 12:26:16 INFO: Installing gawk.
07/12/2025 12:26:20 INFO: Verifying that your system meets the recommended minim
um hardware requirements.
07/12/2025 12:26:20 INFO: Wazuh web interface port will be 443.
07/12/2025 12:26:25 INFO: --- Dependencies ----
07/12/2025 12:26:25 INFO: Installing apt-transport-https.
07/12/2025 12:26:27 INFO: Installing debhelper.
```



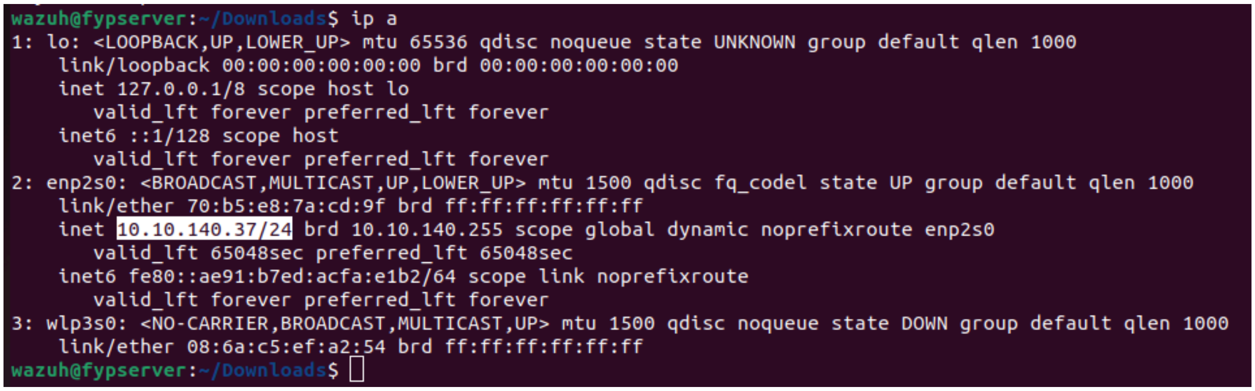
```
wazuh@fypserver: ~
07/12/2025 12:27:09 INFO: Generating the root certificate.
07/12/2025 12:27:09 INFO: Generating Admin certificates.
07/12/2025 12:27:09 INFO: Generating Wazuh indexer certificates.
07/12/2025 12:27:10 INFO: Generating Filebeat certificates.
07/12/2025 12:27:10 INFO: Generating Wazuh dashboard certificates.
07/12/2025 12:27:10 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
07/12/2025 12:27:10 INFO: --- Wazuh indexer ---
07/12/2025 12:27:10 INFO: Starting Wazuh indexer installation.
07/12/2025 12:28:53 INFO: Wazuh indexer installation finished.
07/12/2025 12:28:53 INFO: Wazuh indexer post-install configuration finished.
07/12/2025 12:28:53 INFO: Starting service wazuh-indexer.
07/12/2025 12:29:01 INFO: wazuh-indexer service started.
07/12/2025 12:29:01 INFO: Initializing Wazuh indexer cluster security settings.
07/12/2025 12:29:03 INFO: Wazuh indexer cluster security configuration initialized.
07/12/2025 12:29:03 INFO: Wazuh indexer cluster initialized.
07/12/2025 12:29:03 INFO: --- Wazuh server ---
07/12/2025 12:29:03 INFO: Starting the Wazuh manager installation.
07/12/2025 12:30:27 INFO: Wazuh manager installation finished.
07/12/2025 12:30:27 INFO: Wazuh manager vulnerability detection configuration finished.
07/12/2025 12:30:27 INFO: Starting service wazuh-manager.
07/12/2025 12:30:42 INFO: wazuh-manager service started.
07/12/2025 12:30:42 INFO: Starting Filebeat installation.
07/12/2025 12:30:49 INFO: Filebeat installation finished.
07/12/2025 12:30:50 INFO: Filebeat post-install configuration finished.
07/12/2025 12:30:50 INFO: Starting service filebeat.
07/12/2025 12:30:50 INFO: filebeat service started.
07/12/2025 12:30:50 INFO: --- Wazuh dashboard ---
07/12/2025 12:30:50 INFO: Starting Wazuh dashboard installation.
07/12/2025 12:31:49 INFO: Wazuh dashboard installation finished.
07/12/2025 12:31:49 INFO: Wazuh dashboard post-install configuration finished.
07/12/2025 12:31:49 INFO: Starting service wazuh-dashboard.
07/12/2025 12:31:49 INFO: wazuh-dashboard service started.
07/12/2025 12:31:50 INFO: Updating the internal users.
07/12/2025 12:31:52 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
07/12/2025 12:31:57 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
07/12/2025 12:32:26 INFO: Initializing Wazuh dashboard web application.
07/12/2025 12:32:27 INFO: Wazuh dashboard web application initialized.
07/12/2025 12:32:27 INFO: --- Summary ---
07/12/2025 12:32:27 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: 0bkxyjjUKnnQiBmXo5trqOhJ.sUufhVi
07/12/2025 12:32:27 INFO: --- Dependencies ----
07/12/2025 12:32:27 INFO: Removing gawk.
07/12/2025 12:32:29 INFO: Installation finished.
wazuh@fypserver:~$ 
```

Save the password in a secure position as this is required for Wazuh login interface.



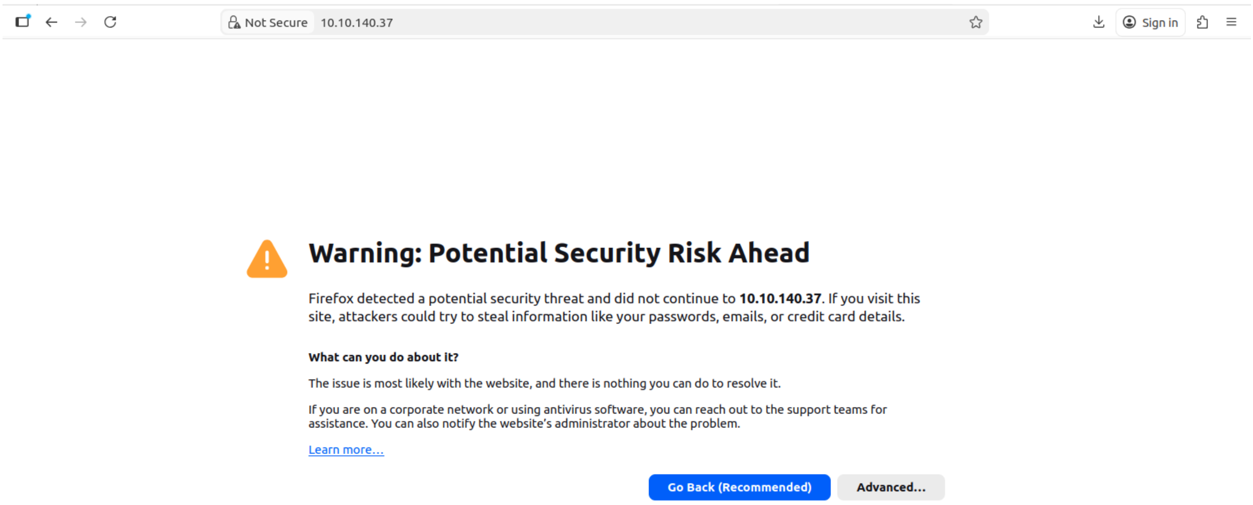
```
wazuh@fypserver:~$ cd Downloads
wazuh@fypserver:~/Downloads$ sudo nano wazuh-pass.txt
[sudo] password for wazuh:
wazuh@fypserver:~/Downloads$ sudo nano wazuh-pass.txt
wazuh@fypserver:~/Downloads$ ls
'Installing the Wazuh server.docx'   wazuh-pass.txt
```

Now we checked the IP on terminal to access the Wazuh web interface from a browser.



```
wazuh@fypserver:~/Downloads$ 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: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 70:b5:e8:7a:cd:9f brd ff:ff:ff:ff:ff:ff
    inet 10.10.140.37/24 brd 10.10.140.255 scope global dynamic noprefixroute enp2s0
       valid_lft 65048sec preferred_lft 65048sec
    inet6 fe80::ae91:b7ed:acfa:e1b2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 08:6a:c5:ef:a2:54 brd ff:ff:ff:ff:ff:ff
wazuh@fypserver:~/Downloads$ 
```

Now we access the web interface of Wazuh on the browser using IP.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **10.10.140.37**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

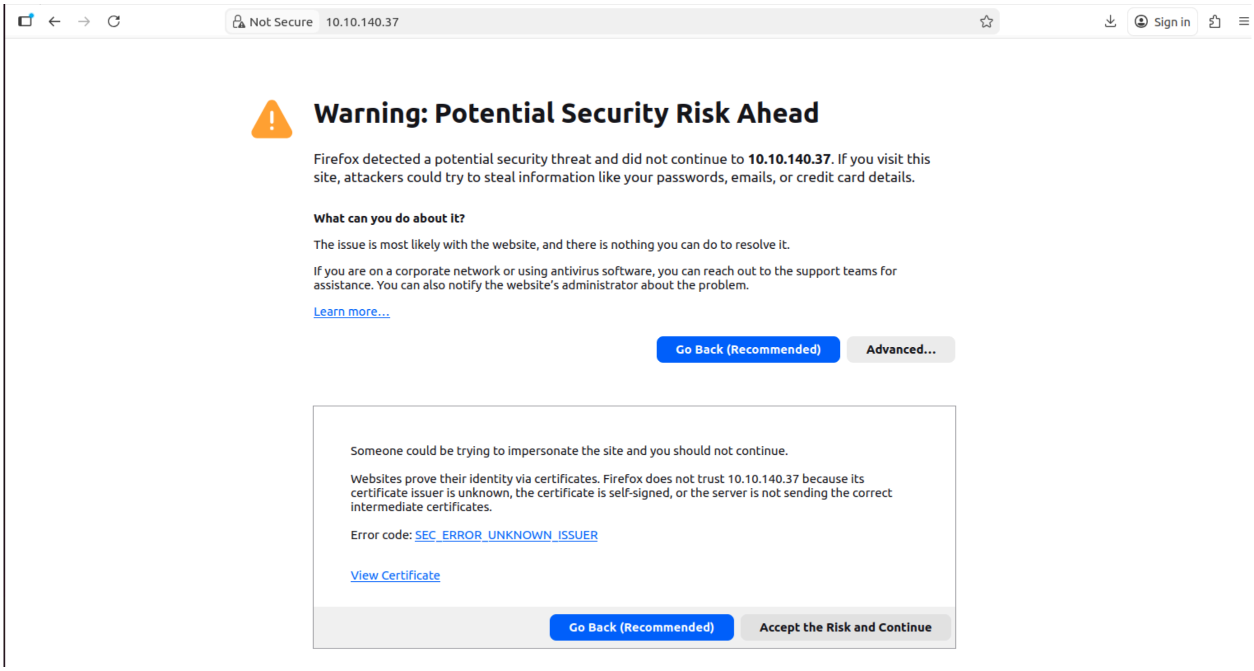
What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more…

Click on advanced option and then click on “Accept the Risk and Continue”



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **10.10.140.37**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more…

Someone could be trying to impersonate the site and you should not continue.

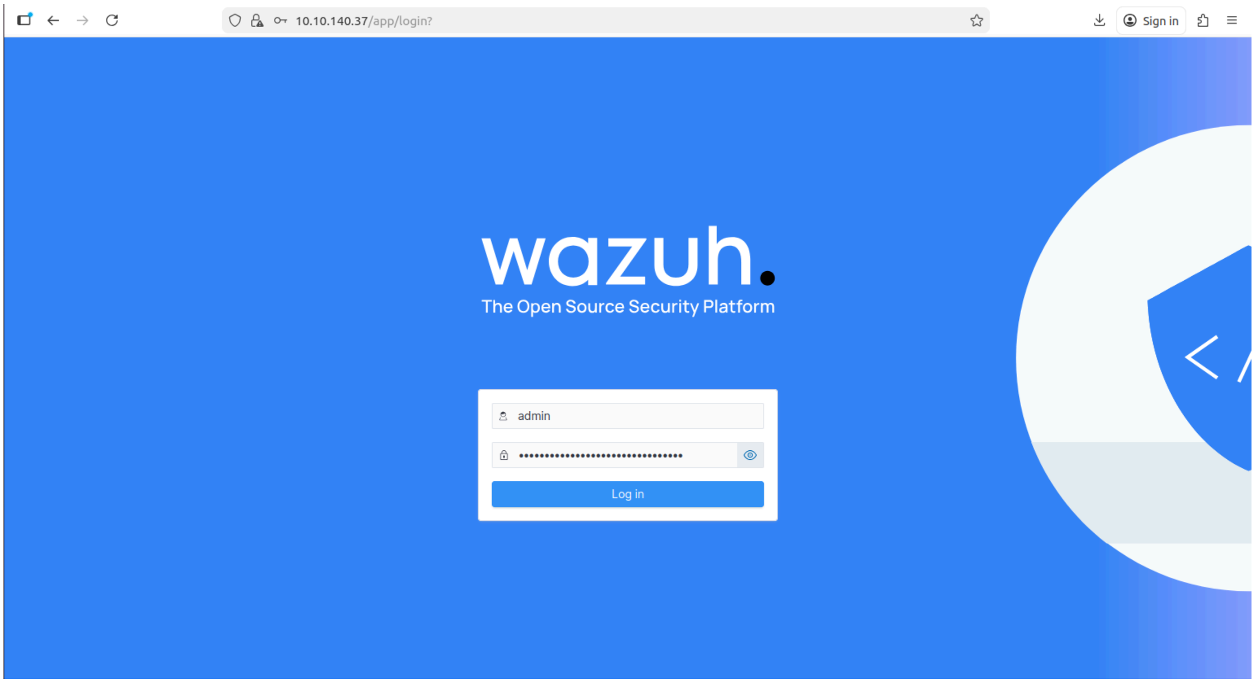
Websites prove their identity via certificates. Firefox does not trust 10.10.140.37 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

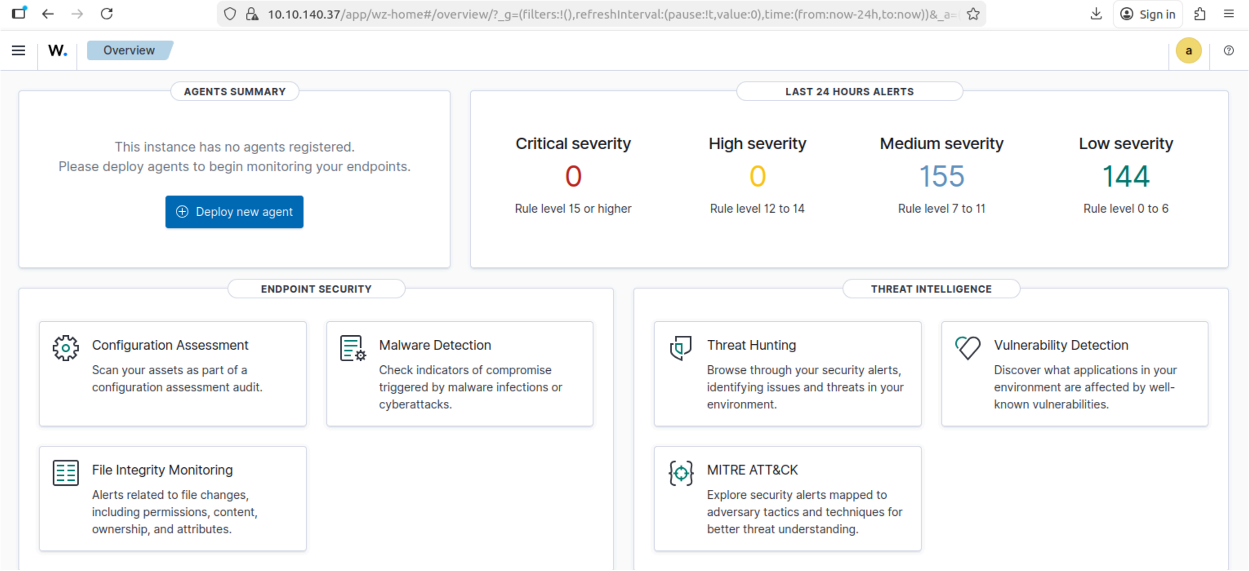
Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

After accepting the security warning, the Wazuh Dashboard loaded successfully.

Now we see the interface.




10.10.140.37/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a
Sign in
W.
Overview
a

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	155	144
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

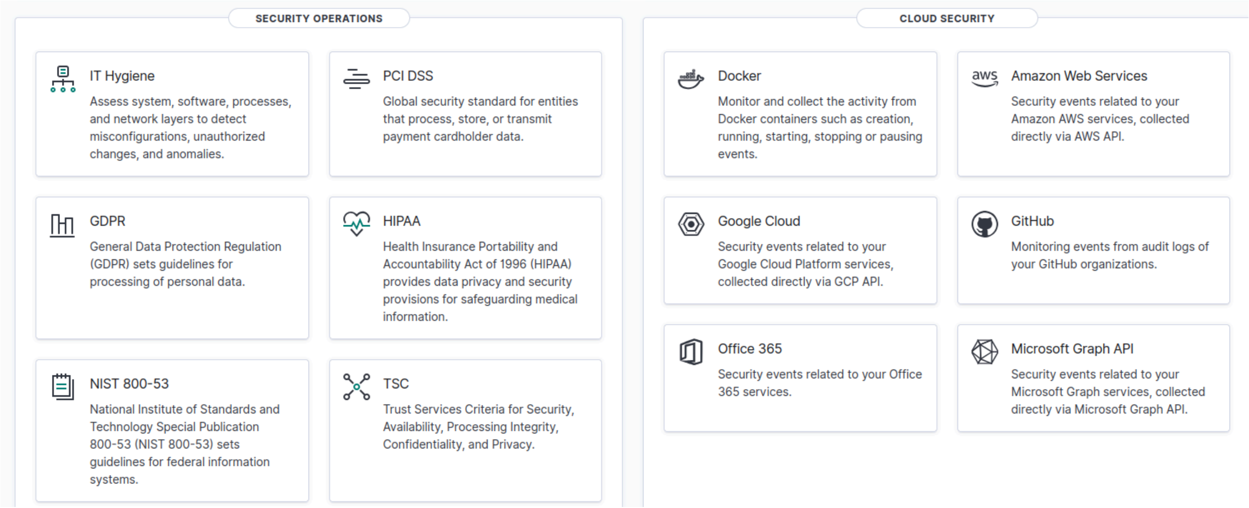
File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.



SECURITY OPERATIONS

IT Hygiene

Assess system, software, processes, and network layers to detect misconfigurations, unauthorized changes, and anomalies.

PCI DSS

Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

TSC

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

CLOUD SECURITY

Docker

Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services

Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud

Security events related to your Google Cloud Platform services, collected directly via GCP API.

GitHub

Monitoring events from audit logs of your GitHub organizations.

Office 365

Security events related to your Office 365 services.

Microsoft Graph API

Security events related to your Microsoft Graph services, collected directly via Microsoft Graph API.

Conclusion:

We successfully installed the Wazuh Manager with all its essential components using the All-in-One Installation Method. This provides the foundation for building our security monitoring system.