

IBM Project Report

On

Develop an application to facilitate IPR filing for the grassroots community

Developed By:

Rishabh Patel (19162171034)
Sahil Patel (20162172004)
Smit Patel (19162121031)

Guided By:

Prof. Umesh Lakhtariya (Internal)
Mr. Anoj Dixit (External guide)

Submitted to

Department of Computer Science & Engineering
Institute of Computer Technology



Year: 2023



CERTIFICATE

This is to certify that the **IBM** Project work entitled “Develop an application to facilitate IPR filing for the grassroots community” by Rishabh Patel (Enrolment No.19162171034), Sahil Patel (Enrolment No.20162172007) and Smit Patel (EnrolmentNo.19162121031) of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by them in the CSE(CS/BDA) Department at Elegant Microweb Pvt. Ltd. The results/findings contained in this Project have not been submitted in part or full to any other University / Institute for award of any other Degree.

Name & Signature of Internal Guide

Name & Signature of Head

Place: ICT - GUNI

Date:

ACKNOWLEDGEMENT

IBM Internship project is a golden opportunity for learning and self-development. I consider myself very lucky and honored to have so many wonderful people lead me through in completion of this project. First and foremost, I would like to thank Dr. Hemal Shah, Principal, ICT, and Prof. Dharmesh Darji, Head, ICT who gave us an opportunity to undertake this project. My grateful thanks to Prof. Umesh Lakhtariya & Mr. Anoj Dixit (Internal & External Guides) for their guidance in project work Develop an application to facilitate IPR filing for the grassroots community, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where would have been without his/her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

Rishabh Patel (Enrollment No:19162171034)

Sahil Patel (Enrollment No: 20162172007)

Smit Patel (Enrollment No:19162121031)

ABSTRACT

The development of an application to facilitate IPR filing for the grassroots community aims to address the challenges faced by individuals and small organizations in navigating the complex and often costly process of obtaining intellectual property rights. By providing a user-friendly platform with step-by-step guides, document templates, and the ability to submit applications electronically, the application aims to make the IPR filing process more accessible and efficient for those with limited resources. Additionally, the application would provide information and resources on different types of IPR, such as patents, trademarks, and copyrights, to assist users in understanding the process and making informed decisions. Overall, the application aims to empower the grassroots community to protect their intellectual property and support their growth and development.

INDEX

Chapter	Title	Page No
1	Introduction	01
2	Project Scope	03
3	Software and Hardware requirement	05
4	Process Model	07
5	Project Plan	10
6	Implementation Details	12
7	Conclusion and future work	14
8	References	16

CHAPTER: 1 INTRODUCTION

CHAPTER 1 INTRODUCTION

An application to facilitate IPR filing for the grassroots community would likely be a software tool or platform that makes it easier for individuals or small organizations with limited resources to file for intellectual property rights. This could include features such as step-by-step guides, document templates, and the ability to submit applications electronically. The application could also provide resources and information on different types of IPR, such as patents, trademarks, and copyrights. The goal of such an application would be to make the IPR filing process more accessible and user-friendly for those who may not have the knowledge or resources to navigate the process on their own.

CHAPTER: 2 PROJECT SCOPE

CHAPTER 2 PROJECT SCOPE

The scope of a project to develop an application to facilitate IPR filing for the grassroots community would include the following:

Research and analysis: This would involve researching the current IPR filing process, identifying the challenges faced by the grassroots community, and determining the features and functionality that would be most useful in addressing these challenges.

Design and development: This would involve creating the user interface and features of the application, such as step-by-step guides, document templates, and the ability to submit applications electronically.

▲ CHAPTER: 3 SOFTWARE AND HARDWARE REQUIREMENTS

Minimum Hardware Requirements



Processor	2.0 GHz
RAM	4GB
HDD	40GB



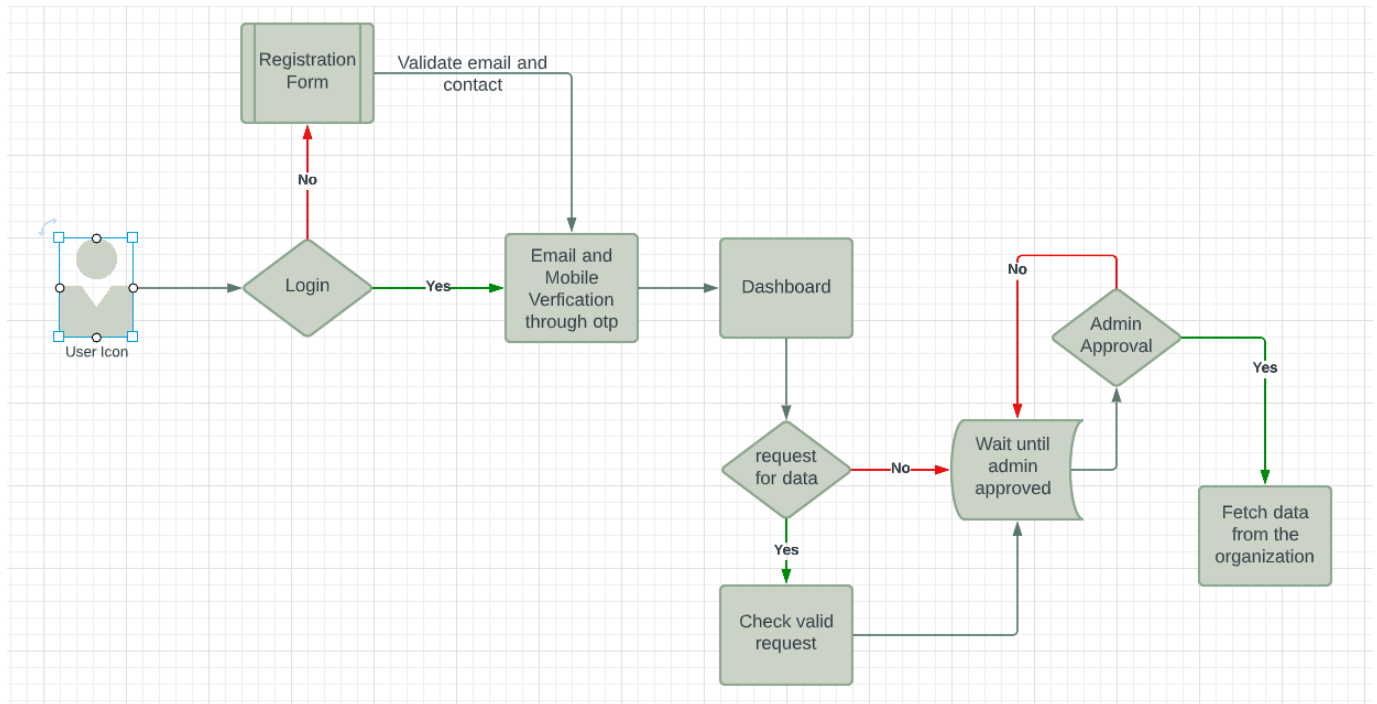
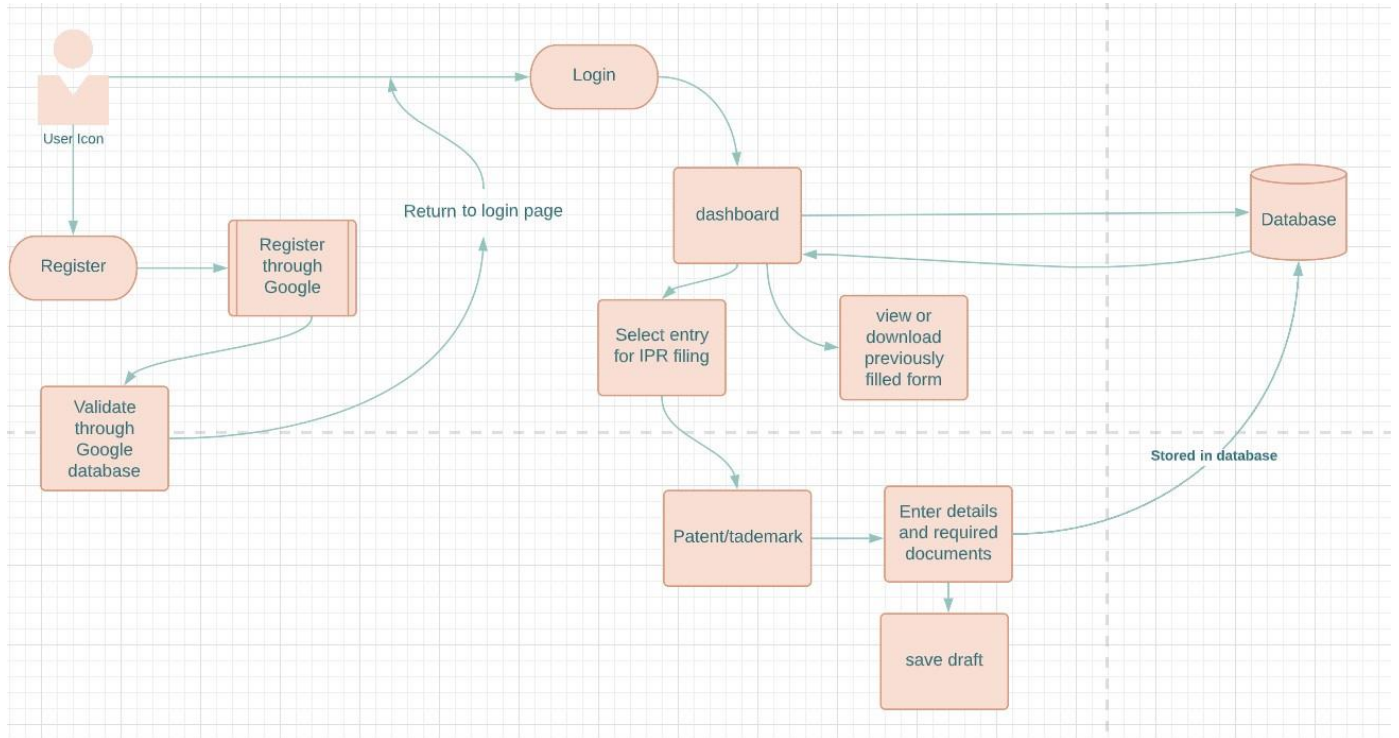
Table 3.1 Minimum Hardware Requirements

Minimum Software Requirements

Operating System	Any operating system which can support an internet browser.
Programming language	-
Other tools & tech	Internet browser

Table 3.2 Minimum Software Requirements

CHAPTER: 4 PROCESS MODEL |



CHAPTER: 5 PROJECT PLAN

CHAPTER 5 PROJECT PLAN

A project plan for developing an application to facilitate IPR filing for the grassroots community could include the following steps:

Kick-off meeting: Hold a meeting with the project team to discuss the project scope, goals, and timelines.

Research and analysis: Conduct research on the current IPR filing process and identify the challenges faced by the grassroots community. Determine the features and functionality that would be most useful in addressing these challenges.

Design and development: Create the user interface and features of the application, such as step-by-step guides, document templates, and the ability to submit applications electronically.

Testing and quality assurance: Test the application to ensure it is user-friendly and functions as intended, and make any necessary adjustments before launch.

Deployment and maintenance: Deploy the application and provide ongoing maintenance and support to ensure it continues to function effectively.

Training: Provide training to end-users on how to use the application and navigate the IPR filing process.

Monitoring and evaluation: Monitor the usage of the application and gather feedback from the end-users to evaluate the effectiveness of the application and identify areas for improvement.

Close project: Close the project and document the lessons learned.

It is important to establish clear milestones and deadlines for each step, and to regularly review the progress of the project to ensure it stays on track. Also, this plan should be flexible enough to accommodate any changes or unforeseen challenges that may arise during the course of the project.

CHAPTER: 6 IMPLEMENTATION DETAILS

CHAPTER 6 IMPLEMENTATION DETAIL

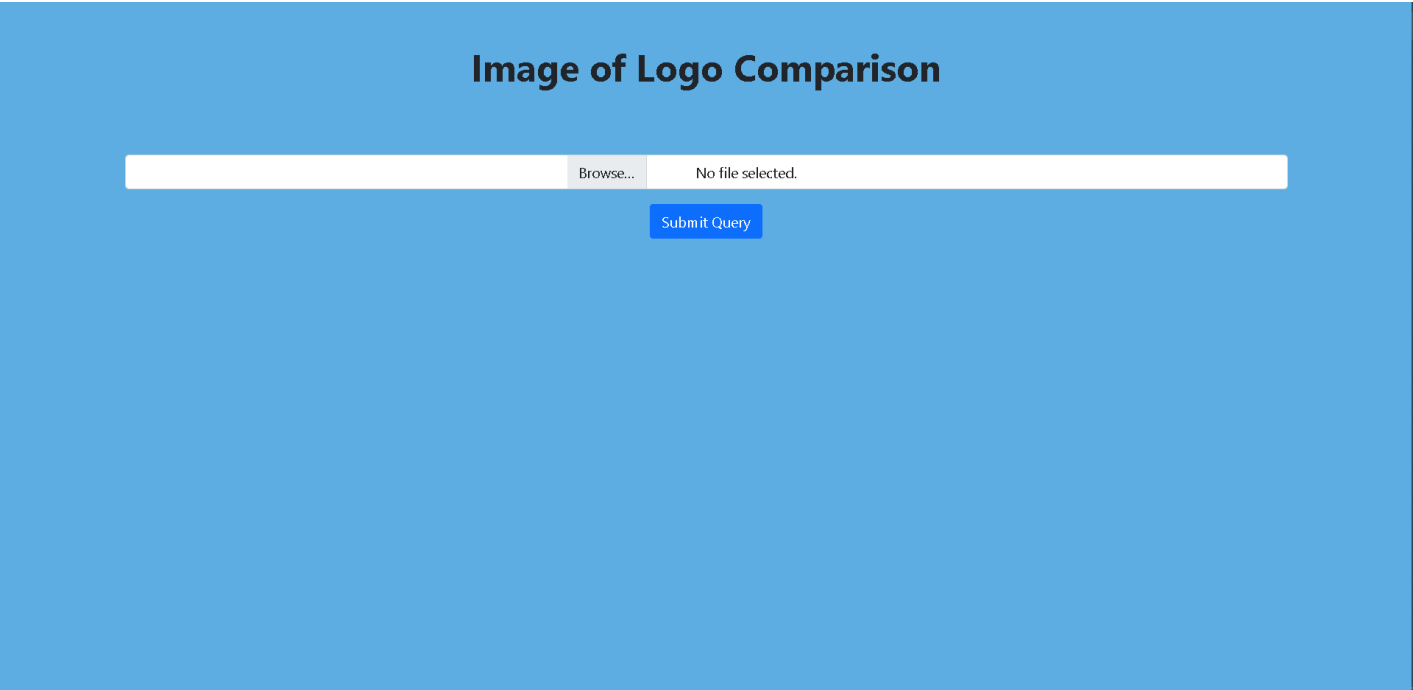
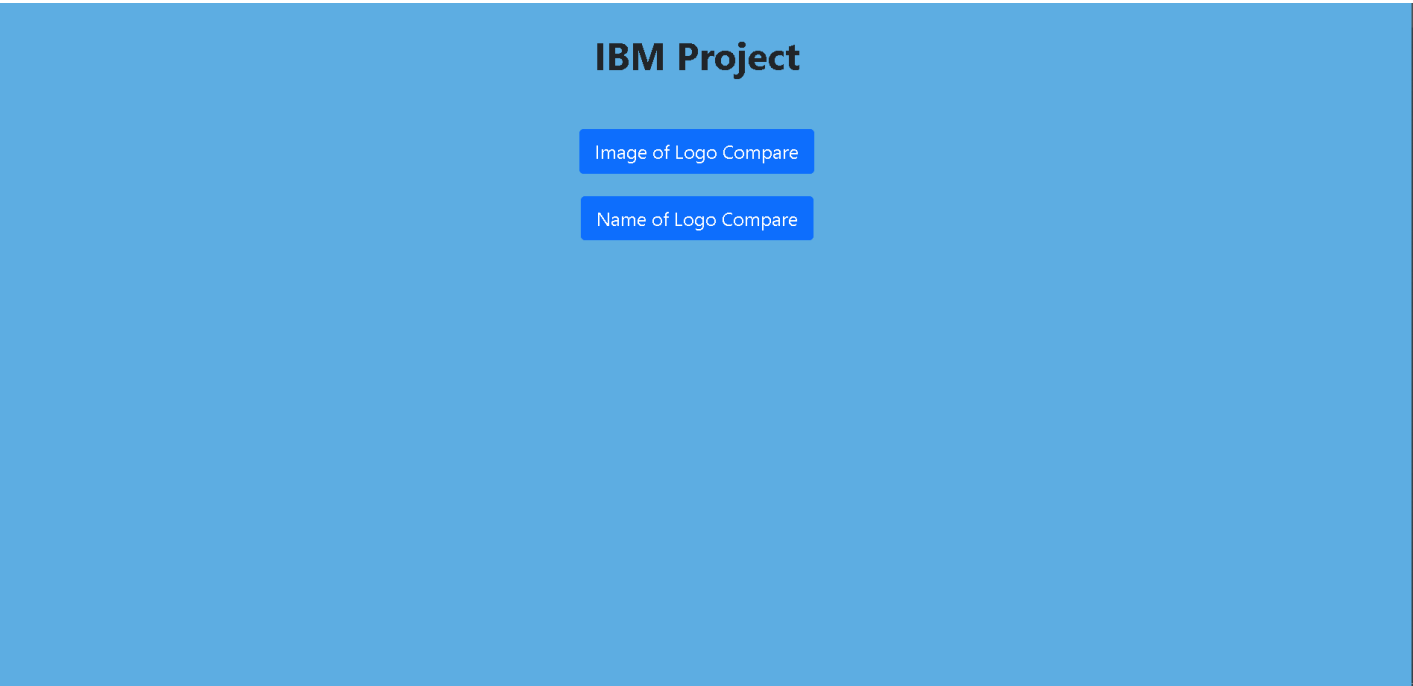


Image of Logo Comparison

	Browse...	img4.jpg
<input type="button" value="Submit Query"/>		

Result

This logo Image is already Patent, Please choose another logo!!!

Logo of Name Compare

Enter a Logo Name :

Submit Query

Result

This name already Patent : YOUTUBEplease choose another name!!!

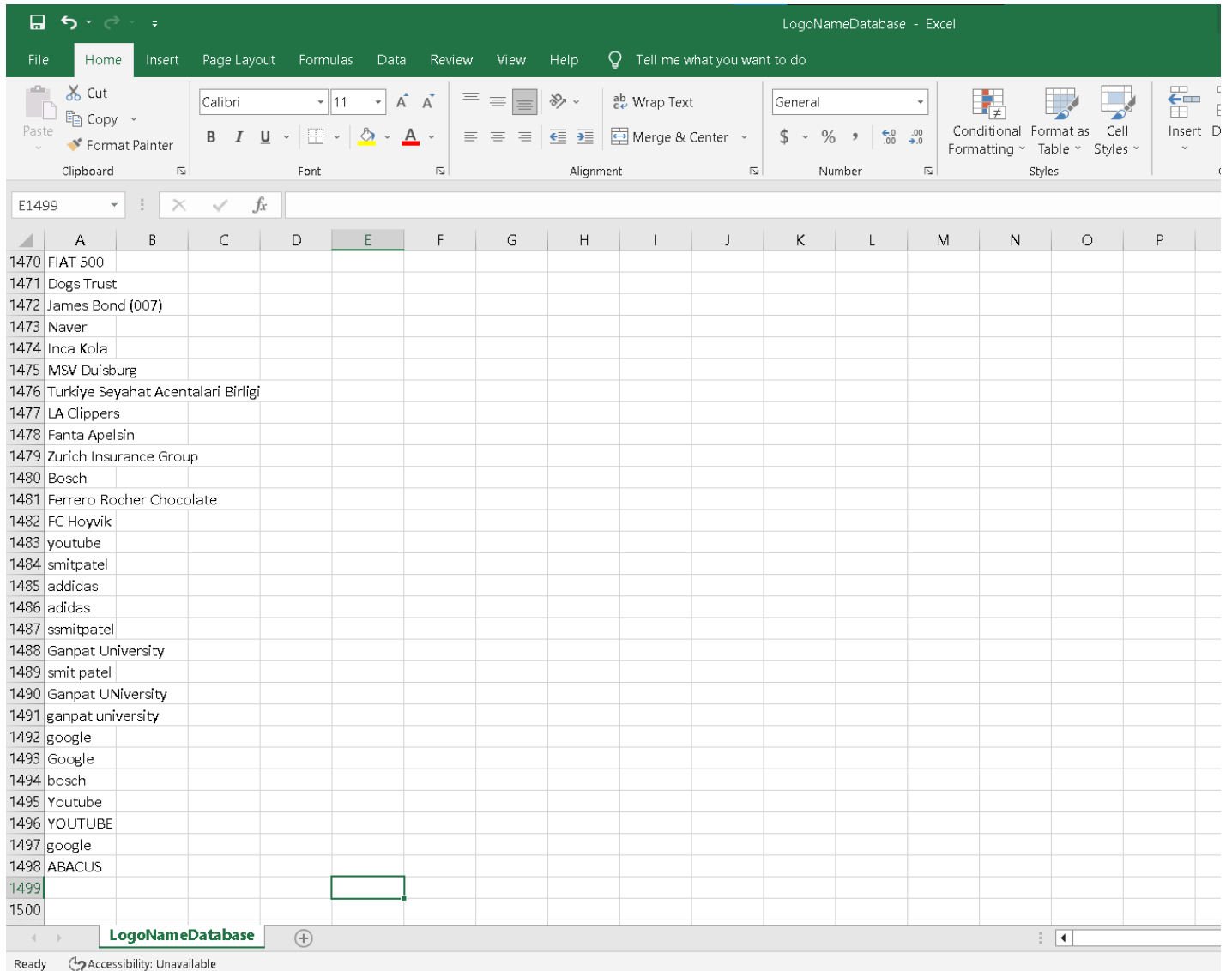
Logo of Name Compare

Enter a Logo Name :

Submit Query

Result

This name is unique : ABACUSnow saved in our database.



4.1. Ubuntu server installation.

Move to Ubuntu official web side and download the server file form the download tab.

CANONICAL

ubuntu®Enterprise ▾Developer ▾Community ▾Download ▾

We are hiringProducts ▾

Search 🔍Sign in

Ubuntu Desktop ▸

Download Ubuntu desktop and replace your current operating system whether it's Windows or Mac OS, or, run Ubuntu alongside it.

22.04 LTS22.10

Ubuntu Server ▸

The most popular server Linux in the cloud and data centre, you can rely on Ubuntu Server and its five years of guaranteed free upgrades.

Get Ubuntu Server

Mac and WindowsARMIBM Powers390x

Ubuntu for IoT ▸

Are you a developer who wants to try snappy Ubuntu Core or classic Ubuntu on an IoT board?

Raspberry PiIntel IoT platformsIntel NUCKVMQualcomm Dragonboard 410cIntel IEI TANK 870AMD-Xilinx Evaluation kits & SOMsRISC-V platforms

Ubuntu Cloud ▸

Use Ubuntu optimised and certified server images on most major clouds.

Get started on Amazon AWS, Microsoft Azure, Google Cloud Platform and more...Download cloud images for local development and testing

TUTORIALS

If you are already running Ubuntu - you can upgrade with the Software Updater

Burn a DVD on Ubuntu, macOS, or Windows. Create a bootable USB stick on Ubuntu, macOS, or Windows

Installation guides for [Ubuntu Desktop](#) and [Ubuntu Server](#)

You can learn how to [try Ubuntu before you install](#)

READ THE DOCS

Read the official docs for [Ubuntu Desktop](#), [Ubuntu Server](#), and [Ubuntu Core](#)

UBUNTU APPLIANCES

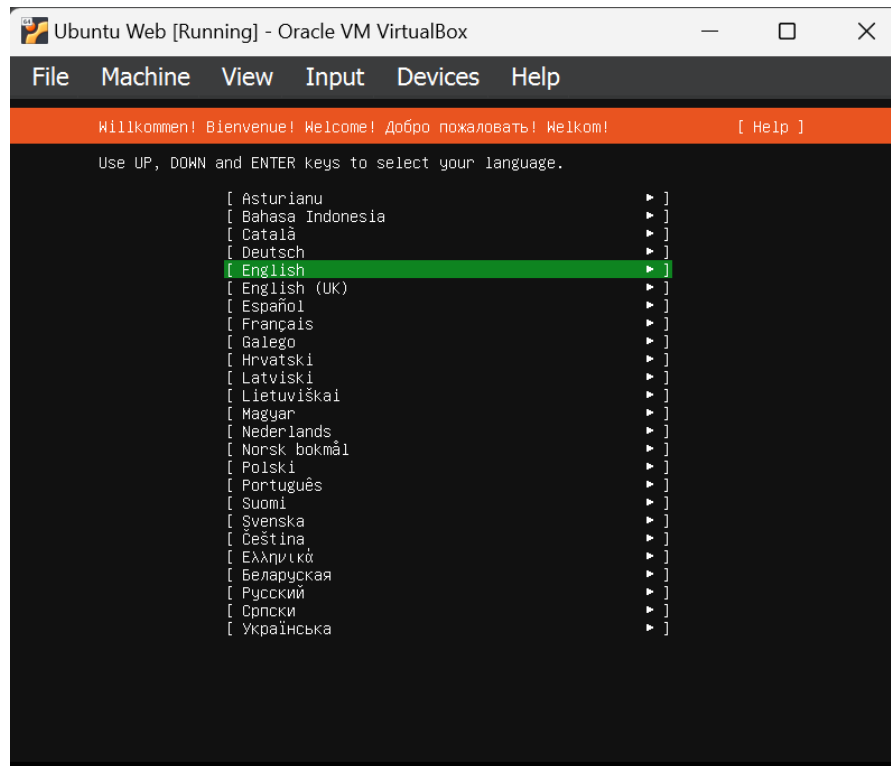
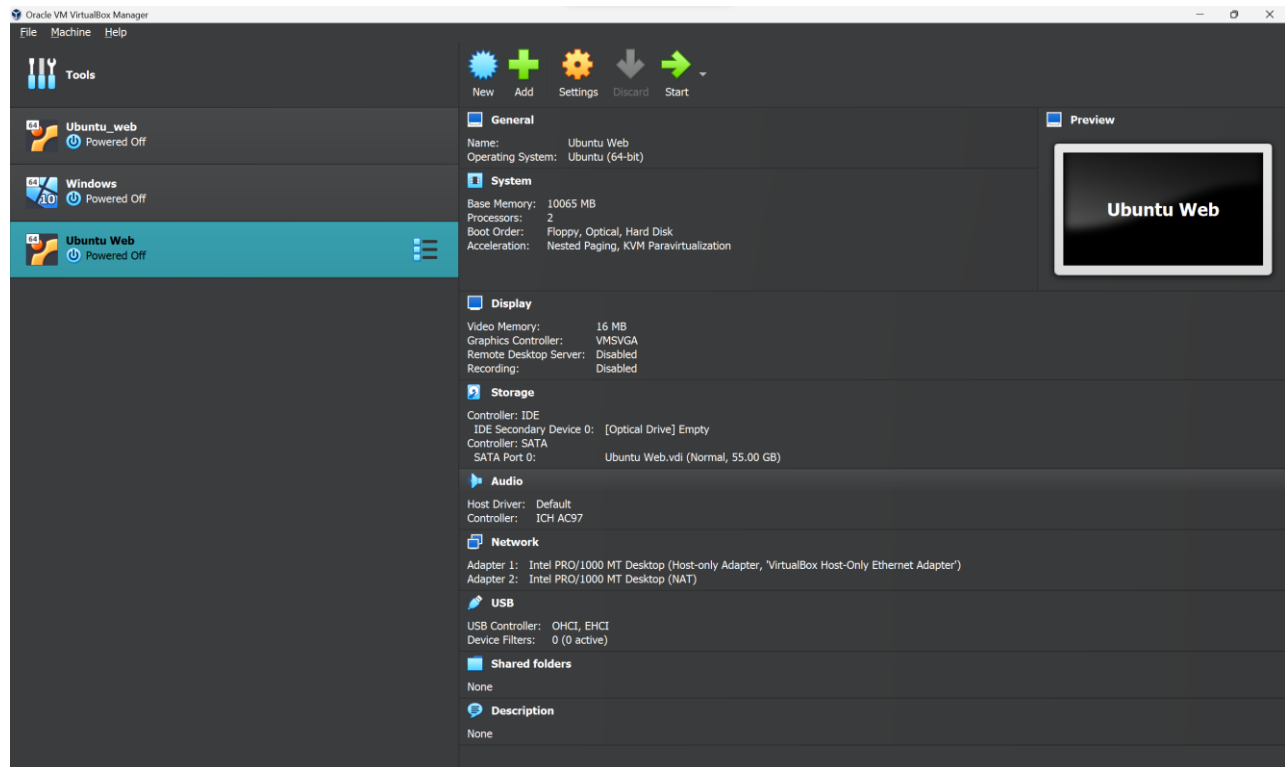
An [Ubuntu Appliance](#) is an official system image which blends a single application with Ubuntu Core. Certified to run on Raspberry Pi and PC boards.

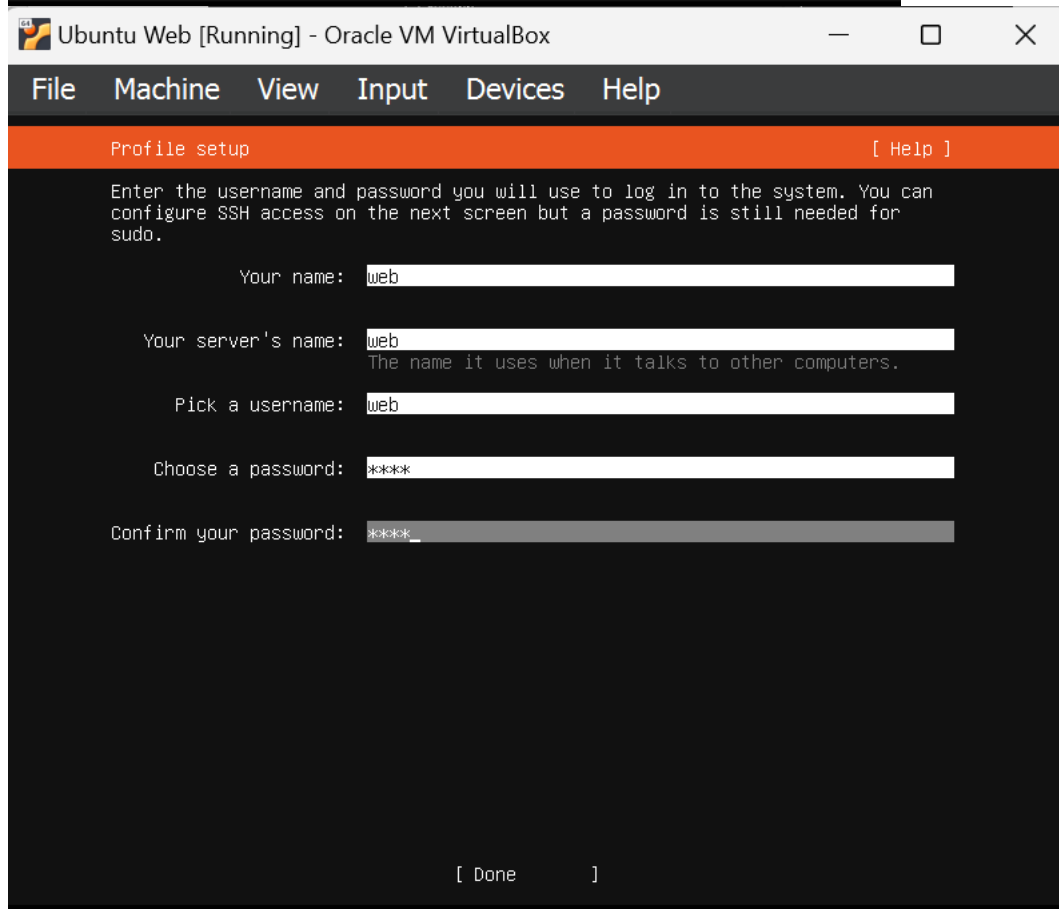
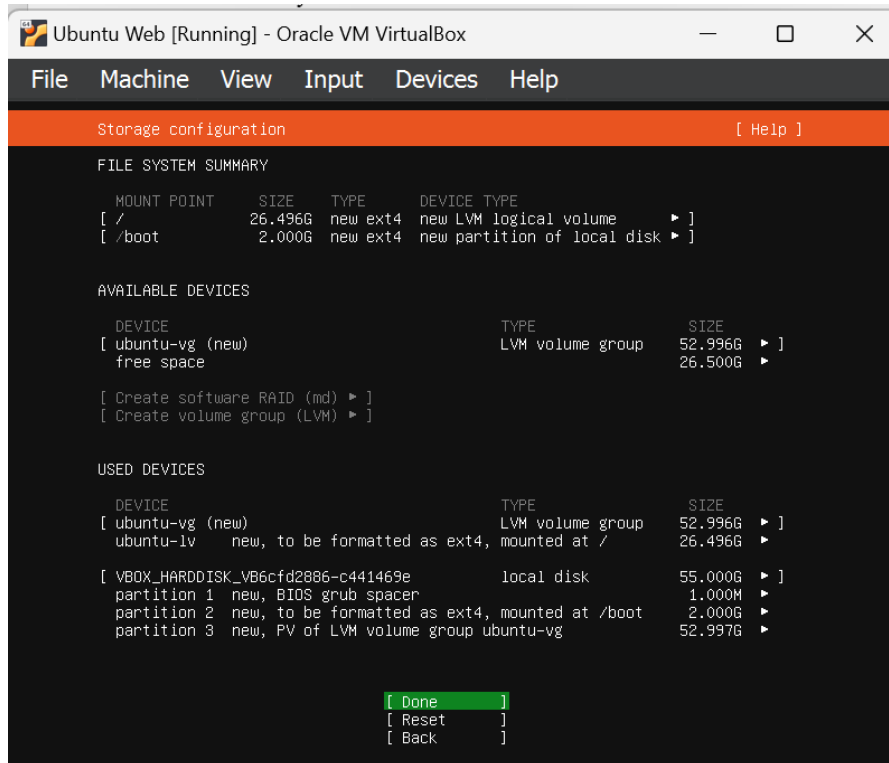
OTHER WAYS TO DOWNLOAD

Click on these to download the server file.

UBUNTU LIAISON

[Ubuntu](#)[Ubuntu Studio](#)[Ubuntu Budgie](#)[Xubuntu](#)[Ubuntu Kylin](#)





```
Ubuntu Web [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Installing system [ Help ]

configuring disk: disk-sda
configuring partition: partition-0
configuring partition: partition-1
configuring format: format-0
configuring partition: partition-2
configuring lvm_volgroup: lvm_volgroup-0
configuring lvm_partition: lvm_partition-0
configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
executing curtin install extract step
curtin command install
writing install sources to disk
running 'curtin extract'
curtin command extract
acquiring and extracting image from cp:///tmp/tmpjv49c4_z/mount
executing curtin install curthooks step
curtin command install
configuring installed system
running 'mount --bind /cdrom /target/cdrom'
running 'curtin in-target -- setupcon --save-only'
curtin command in-target
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
configuring iscsi service
configuring raid (mdadm) service
installing kernel \

[ View full log ]
```

```
webserver@webserver:~$ mkdir wazuh
webserver@webserver:~$ mkdir backup
```

```
webserver@webserver:~/wazuh$ curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
webserver@webserver:~/wazuh$
```

```
webserver@webserver:~/wazuh$
webserver@webserver:~/wazuh$ curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
webserver@webserver:~/wazuh$ chmod 744 wazuh-install.sh
webserver@webserver:~/wazuh$ ./wazuh-install.sh -d wazuh
./wazuh-install.sh line 2197: /var/log/wazuh-install.log: Permission denied
27/03/2023 11:46:35 INFO: Starting Wazuh installation assistant. Wazuh version: 4.3.10
27/03/2023 11:46:35 INFO: Verbose logging redirected to /var/log/wazuh-install.log
27/03/2023 11:46:40 INFO: -- Download Packages --
27/03/2023 11:46:40 INFO: Starting Wazuh packages download.
27/03/2023 11:46:40 INFO: Downloading Wazuh deb packages for x86_64.
27/03/2023 11:47:18 INFO: The manager package was downloaded.
27/03/2023 11:47:19 INFO: The filebeat package was downloaded.
27/03/2023 11:47:35 INFO: The indexer package was downloaded.
27/03/2023 11:47:40 INFO: The dashboard package was downloaded.
27/03/2023 11:47:40 INFO: The packages are in wazuh-offline/wazuh-packages
27/03/2023 11:47:40 INFO: Downloading configuration files and assets.
27/03/2023 11:47:40 INFO: The resource https://packages.wazuh.com/key/GPG-KEY-WAZUH was downloaded.
27/03/2023 11:47:40 INFO: The resource https://packages.wazuh.com/4.3/cpl/wazuh/filebeat/filebeat.yml was downloaded.
27/03/2023 11:47:41 INFO: The resource https://raw.githubusercontent.com/wazuh/wazuh/4.3/extensions/elasticsearch/7.x/wazuh-template.json was downloaded.
27/03/2023 11:47:41 INFO: The resource https://packages.wazuh.com/4.3/filebeat/wazuh-filebeat-0.2.tar.gz was downloaded.
27/03/2023 11:47:41 INFO: The configuration files and assets are in wazuh-offline/wazuh-files
27/03/2023 11:47:55 INFO: You can follow the installation guide here https://documentation.wazuh.com/current/installation-guide/more-installation-alternatives/offline-installation.html
webserver@webserver:~/wazuh$
```

```
webserver@webserver:~/wazuh$ curl -sO https://packages.wazuh.com/4.3/config.yml
webserver@webserver:~/wazuh$ ls
config.yml wazuh-install.sh wazuh-offline.tar.gz
webserver@webserver:~/wazuh$
```

```
root@webserver: /home/webserver/wazuh
GNU nano 6.2
nodes:
# Wazuh indexer nodes
indexer:
- name: node-1
  ip: 192.168.1.10
#- name: node-2
# ip: <indexer-node-ip>
#- name: node-3
# ip: <indexer-node-ip>

# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
- name: wazuh-1
  ip: 192.168.1.10
# node_type: master
#- name: wazuh-2
# ip: <wazuh-manager-ip>
# node_type: worker
#- name: wazuh-3
# ip: <wazuh-manager-ip>
# node_type: worker

# Wazuh dashboard nodes
dashboard:
- name: dashboard
  ip: 192.168.1.10
```

```

root@webserver:/home/webserver/wazuh# cat config.yml
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: 192.168.1.10
    #- name: node-2
    # ip: <indexer-node-ip>
    #- name: node-3
    # ip: <indexer-node-ip>

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: 192.168.1.10
    # node_type: master
    #- name: wazuh-2
    # ip: <wazuh-manager-ip>
    # node_type: worker
    #- name: wazuh-3
    # ip: <wazuh-manager-ip>
    # node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: 192.168.1.10

```

```

root@webserver:/home/webserver/wazuh# ls
config.yml wazuh-certificates wazuh-certs-tool.sh wazuh-install.sh wazuh-offline.tar.gz
root@webserver:/home/webserver/wazuh#

```

```

root@webserver:/home/webserver/wazuh# scp -r wazuh-offline.tar.gz webserver@192.168.1.10:/home/webserver/
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ED25519 key fingerprint is SHA256:owokQe7hy7nD0eXTeWl0dWlcaLp+BMHogdFYys.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.10' (ED25519) to the list of known hosts.
webserver@192.168.1.10's password:
wazuh-offline.tar.gz
root@webserver:/home/webserver/wazuh# scp -r wazuh-certificates webserver@192.168.1.10:/home/webserver/
webserver@192.168.1.10's password:
root-ca.pem
wazuh-1.pem
dashboard-key.pem
node-1-key.pem
admin-key.pem
root-ca.key
wazuh-1-key.pem
node-1.pem
admin.pem
dashboard.pem
root@webserver:/home/webserver/wazuh#

```

```

100% 599MB 384.7MB/s 00:01
100% 1204 1.3MB/s 00:00
100% 1277 1.4MB/s 00:00
100% 1704 1.5MB/s 00:00
100% 1700 1.5MB/s 00:00
100% 1704 2.5MB/s 00:00
100% 1704 2.3MB/s 00:00
100% 1704 1.5MB/s 00:00
100% 1277 1.6MB/s 00:00
100% 1119 764.0KB/s 00:00
100% 1251 1.5MB/s 00:00

```

```

webserver@webserver:~$ ls
backup wazuh wazuh-certificates wazuh-offline.tar.gz
webserver@webserver:~$ sudo su
[sudo] password for webserver:
root@webserver:/home/webserver# mv wazuh-certificates /home/webserver/backup/
root@webserver:/home/webserver# ls
backup wazuh wazuh-offline.tar.gz
root@webserver:/home/webserver# mv wazuh-offline.tar.gz /home/webserver/backup/
root@webserver:/home/webserver# ls
backup wazuh
root@webserver:/home/webserver#

```

```
root@webserver:/home/webserver# cd backup/
root@webserver:/home/webserver/backup# ls
wazuh-certificates  wazuh-offline.tar.gz
root@webserver:/home/webserver/backup# ls -l
total 613844
drwxr--r-- 2 webserver webserver      4096 Mar 27 12:00 wazuh-certificates
-rw----- 1 webserver webserver 628567785 Mar 27 11:59 wazuh-offline.tar.gz
root@webserver:/home/webserver/backup#
```

```
root@webserver:/home/webserver/wazuh# tar xf wazuh-offline.tar.gz
root@webserver:/home/webserver/wazuh#
```

```
root@webserver:/home/webserver/wazuh# dpkg -i ../wazuh-offline/wazuh-packages/wazuh-indexer*.deb
Selecting previously unselected package wazuh-indexer.
(Reading database ... 73929 files and directories currently installed.)
Preparing to unpack ../wazuh-indexer_4.3.10-1_amd64.deb ...
Creating wazuh-indexer group... OK
Creating wazuh-indexer user... OK
Unpacking wazuh-indexer (4.3.10-1) ...
Setting up wazuh-indexer (4.3.10-1) ...
Created opensearch keystore in /etc/wazuh-indexer/opensearch.keystore
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
root@webserver:/home/webserver/wazuh#
```

```
root@webserver:/home/webserver/wazuh# systemctl daemon-reload
root@webserver:/home/webserver/wazuh# systemctl enable wazuh-indexer
Synchronizing state of wazuh-indexer.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-indexer
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-indexer.service -> /lib/systemd/system/wazuh-indexer.service.
root@webserver:/home/webserver/wazuh# systemctl start wazuh-indexer
root@webserver:/home/webserver/wazuh#
```

```
root@webserver:/home/webserver/wazuh# systemctl daemon-reload
root@webserver:/home/webserver/wazuh# systemctl enable wazuh-manager
Synchronizing state of wazuh-manager.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-manager
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service -> /lib/systemd/system/wazuh-manager.service.
root@webserver:/home/webserver/wazuh# systemctl start wazuh-manager
root@webserver:/home/webserver/wazuh#
```

```

root@webserver:/home/webserver/wazuh# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-03-27 12:18:49 UTC; 23s ago
     Process: 40542 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 133 (limit: 20362)
   Memory: 580.2M
      CPU: 20.715s
   CGroup: /system.slice/wazuh-manager.service
           └─40595 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             └─40634 /var/ossec/bin/wazuh-authd
               └─40650 /var/ossec/bin/wazuh-db
                 └─40664 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
                   └─40667 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
                     └─40679 /var/ossec/bin/wazuh-execd
                       └─40693 /var/ossec/bin/wazuh-analysisd
                         └─40754 /var/ossec/bin/wazuh-syscheckd
                           └─40773 /var/ossec/bin/wazuh-remoted
                             └─40805 /var/ossec/bin/wazuh-logcollector
                               └─40827 /var/ossec/bin/wazuh-monitord
                                 └─40849 /var/ossec/bin/wazuh-modulesd

Mar 27 12:18:40 webserver env[40542]: Started wazuh-db...
Mar 27 12:18:41 webserver env[40542]: Started wazuh-execd...
Mar 27 12:18:42 webserver env[40542]: Started wazuh-analysisd...
Mar 27 12:18:43 webserver env[40542]: Started wazuh-syscheckd...
Mar 27 12:18:44 webserver env[40542]: Started wazuh-remoted...
Mar 27 12:18:46 webserver env[40542]: Started wazuh-logcollector...
Mar 27 12:18:47 webserver env[40542]: Started wazuh-monitord...
Mar 27 12:18:47 webserver env[40542]: Started wazuh-modulesd...
Mar 27 12:18:49 webserver env[40542]: Completed.
Mar 27 12:18:49 webserver systemd[1]: Started Wazuh manager.
root@webserver:/home/webserver/wazuh#

```

```

root@webserver:/home/webserver/wazuh# dpkg -i ./wazuh-offline/wazuh-packages/filebeat*.deb
Selecting previously unselected package filebeat.
(Reading database ... 93565 files and directories currently installed.)
Preparing to unpack .../filebeat-oss-7.10.2-amd64.deb ...
Unpacking filebeat (7.10.2) ...
Setting up filebeat (7.10.2) ...
root@webserver:/home/webserver/wazuh#

```

```

root@webserver:/home/webserver/wazuh# cp ./wazuh-offline/wazuh-files/filebeat.yml /etc/filebeat/ &&\
cp ./wazuh-offline/wazuh-files/wazuh-template.json /etc/filebeat/ &&\
chmod go+r /etc/filebeat/wazuh-template.json
root@webserver:/home/webserver/wazuh#
root@webserver:/home/webserver/wazuh# dpkg -i ./wazuh-offline/wazuh-packages/wazuh-dashboard*.deb
Selecting previously unselected package wazuh-dashboard.
(Reading database ... 93884 files and directories currently installed.)
Preparing to unpack .../wazuh-dashboard_4.3.10-1_amd64.deb ...
Creating wazuh-dashboard group... OK
Creating wazuh-dashboard user... OK
Unpacking wazuh-dashboard (4.3.10-1) ...
Setting up wazuh-dashboard (4.3.10-1) ...
root@webserver:/home/webserver/wazuh#

```

```

root@webserver:/home/webserver/wazuh# NODE_NAME=dashboard
root@webserver:/home/webserver/wazuh# mkdir /etc/wazuh-dashboard/certs
root@webserver:/home/webserver/wazuh# mv -n wazuh-certificates/$NODE_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem
root@webserver:/home/webserver/wazuh# mv -n wazuh-certificates/$NODE_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
root@webserver:/home/webserver/wazuh# cp wazuh-certificates/root-ca.pem /etc/wazuh-dashboard/certs/
root@webserver:/home/webserver/wazuh# chmod 500 /etc/wazuh-dashboard/certs/
root@webserver:/home/webserver/wazuh# chmod 400 /etc/wazuh-dashboard/certs/*
root@webserver:/home/webserver/wazuh# chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
root@webserver:/home/webserver/wazuh#

```

```

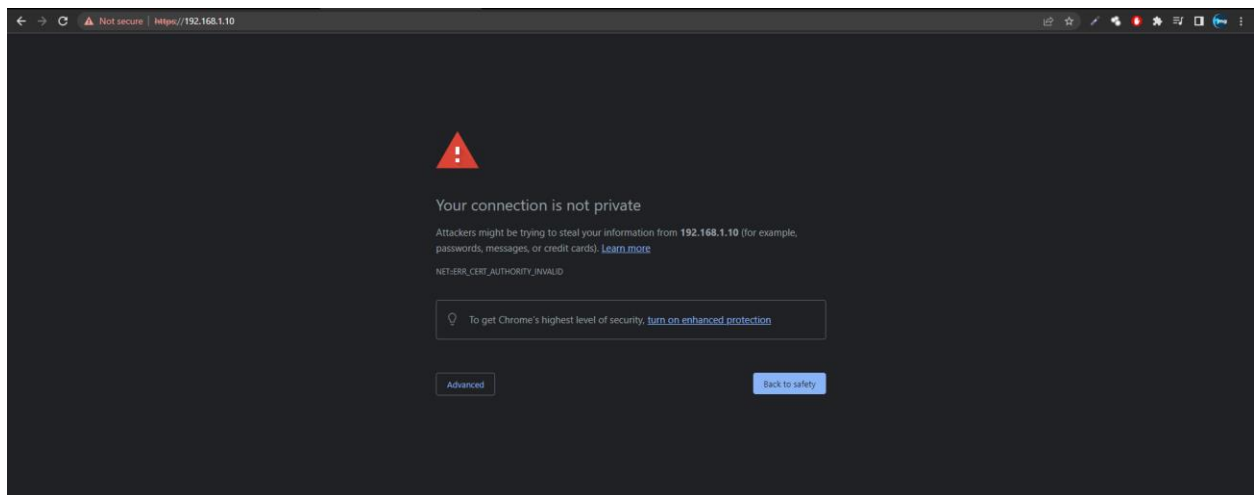
root@webserver:/home/webserver/wazuh
GNU nano 6.2
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://192.168.1.10:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersWhitelist: ["securitytenant","Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wazuh

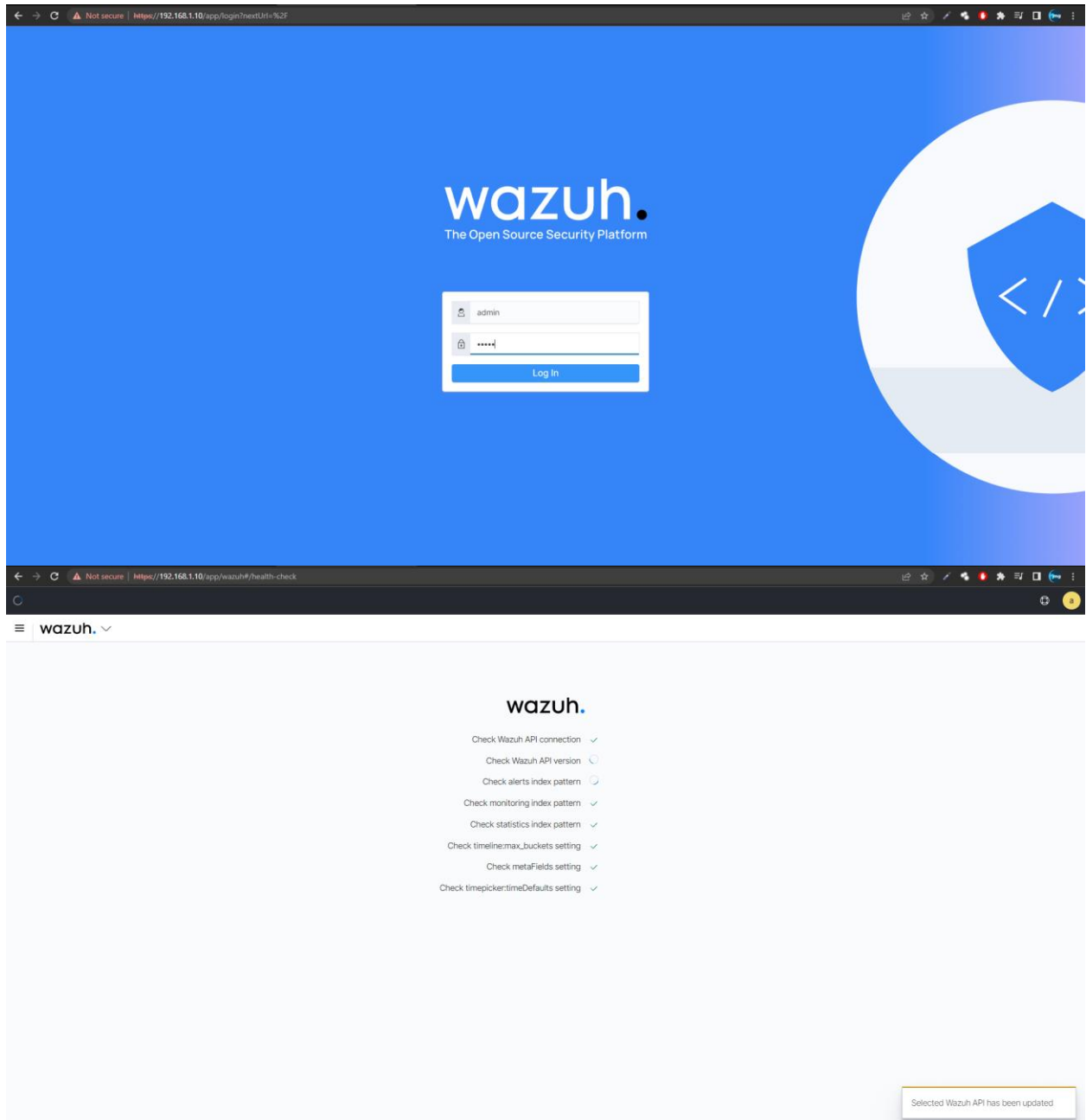
```

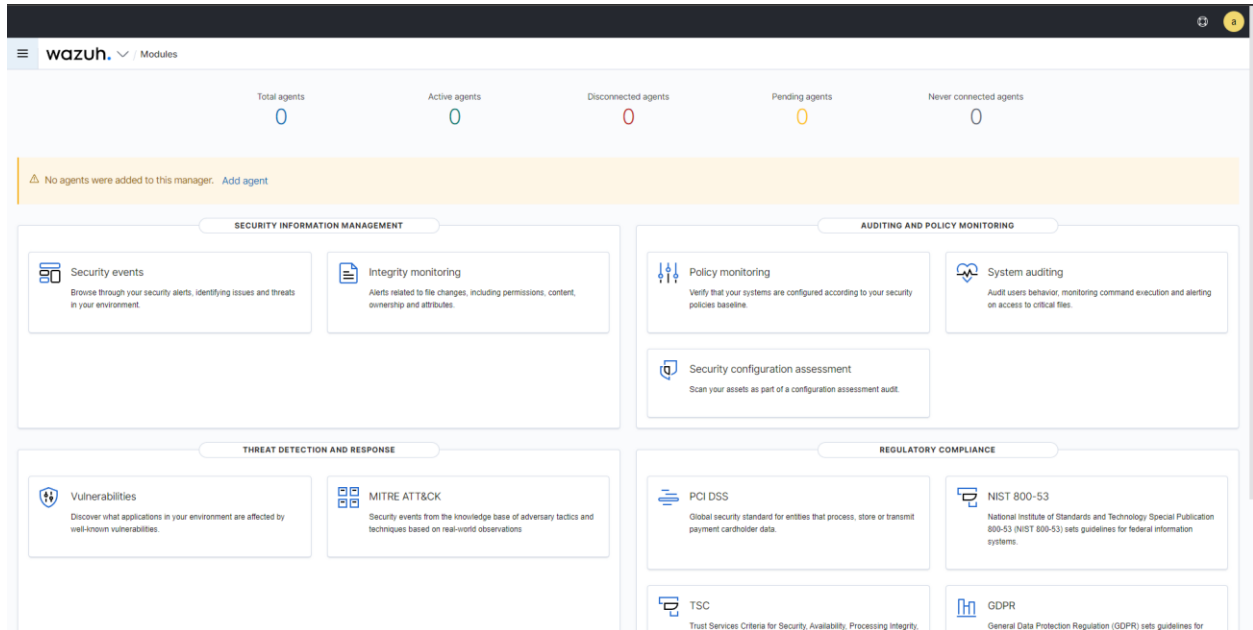
```

root@webserver:/home/webserver/wazuh# systemctl daemon-reload
root@webserver:/home/webserver/wazuh# systemctl enable wazuh-dashboard
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-dashboard.service → /etc/systemd/system/wazuh-dashboard.service.
root@webserver:/home/webserver/wazuh# systemctl start wazuh-dashboard
root@webserver:/home/webserver/wazuh#

```







wazuh. Platform Cloud Services Partners Blog Company

Search

Getting started
Quickstart
Installation guide
Wazuh indexer
Wazuh server
Wazuh dashboard
Wazuh agent
Linux

Installation guide / Wazuh agent / Installing Wazuh agents on Windows endpoints

Installing Wazuh agents on Windows endpoints

The agent runs on the endpoint you want to monitor and communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel. Monitor your Windows systems with Wazuh, from Windows XP to the latest available versions including Windows 11 and Windows Server 2022.

Note To perform the installation, administrator privileges are required.

1. To start the installation process, download the [Windows installer](#).
2. Select the installation method you want to follow: command line interface (CLI) or graphical user interface (GUI).

```
root@webserver:/home/webserver/wazuh# cd /var/ossec/bin/
root@webserver:/var/ossec/bin# ls
agent_control  agent_upgrade  cluster_control  verify-agent-conf  wazuh-analysisd  wazuh-authd  wazuh-control  wazuh-db  wazuh-execd  wazuh-logcollector  wazuh-logtest-legacy  wazuh-
agent_groups  clear_state    manage_agents    wazuh-agentlessd  wazuh-apid      wazuh-clusterd  wazuh-csyslogd  wazuh-dbd  wazuh-integratord  wazuh-logtest     wazuh-maild  wazuh-
```

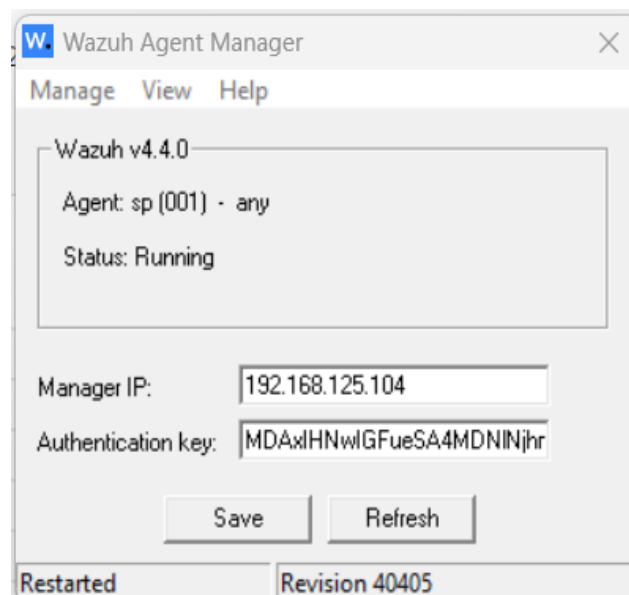
```

(Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
    * A name for the new agent: sahil
    * The IP Address of the new agent: any
Confirm adding it?(y/n): y
2023/04/06 14:00:56 manage_agents: WARNING: 9008: Duplicate name

*****
* Wazuh v4.4.0 Agent manager.                *
* The following options are available:        *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: 

```





STATUS



- Active (1)
- Disconnected (0)
- Pending (0)
- Never connected (0)

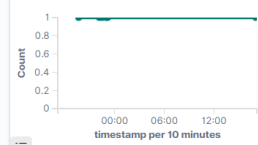
DETAILS

Active 1 Disconnected 0 Pending 0 Never connected 0 Agents coverage 100.00%

Last registered agent
sp

Most active agent
sp

EVOLUTION



Last 24 hours ▾

● active

status=active × Filter or search agent

Refresh

Agents (1)

⊕ Deploy new agent

📄 Export formatted



ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	sp	192.168.31.30	default	🖥️ Microsoft Windows 11 Home Single Language 10.0.22621.1413	node01	v4.4.0	● active	👁️ 🔗

Sysinternals Downloads Community Resources

Filter by title

Home

Downloads

Downloads

> File and Disk Utilities

> Networking Utilities

> Process Utilities

> Security Utilities

Security Utilities

Autologon

LogonSessions

NewSID

PsLoggedOn

PsList

RootkitRevealer

Sysmon

> System Information

> Miscellaneous

Sysinternals Suite

Microsoft Store

Learn / Sysinternals / Downloads /

Sysmon v14.14

Article • 01/26/2023 • 15 minutes to read • 9 contributors

By Mark Russinovich and Thomas Garnier

Published: January 25, 2023

Download Sysmon ^{if} (4.6 MB)

Download Sysmon for Linux (GitHub) ^{if}

Feedback

In this article

- Introduction
- Overview of Symon Capabilities
- Screenshots
- Usage

Show more

Introduction

System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection ^{if} or SIEM ^{if} agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Note that Sysmon does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

sysmonconfig-export 10/17/2021 6:49 AM Microsoft Edge H... 121 KB

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
PS C:\WINDOWS\system32> cd ../
PS C:\WINDOWS> cd
PS C:\WINDOWS> cd ../
PS C:\> cd .\Users\Hulk\Sysmon
PS C:\Users\Hulk\Sysmon> .\Sysmon64.exe -accepteula -i sysmonconfig-export.xml
.\Sysmon64.exe :
At line:1 char:1
+ .\Sysmon64.exe -accepteula -i sysmonconfig-export.xml
+ ~~~~~
+ CategoryInfo          : NotSpecified: (String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError

System Monitor v14.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.83
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\Hulk\Sysmon>
```

Event Viewer

File Action View Help

Security-LessPrivilegedAppCo
 Security-Mitigations
 Security-Netlogon
 Security-SPP-UI-GenuineCent
 Security-SPP-UI-Notifications
 Security-UserConsentVerifier
 SecurityMitigationBroker
 ServiceReportingAPI
 SettingsSync
 SettingsSync-Azure
 SettingsSync-OneDrive
 Shell-ConnectedAccountState
 Shell-Core
 ShellCommon-StartLayoutPop
 SmartCard-Audit
 SmartCard-DeviceEnum
 SmartCard-TPM-VCARD-Modu
 SmartScreen
 SMBClient
 SMBServer
 SMBWitnessClient
 StateRepository
 Storage-Telemetry
 StorageManagement
 StorageManagement-Partitbl
 StorageSettings
 StorageSpaces-Api
 StorageSpaces-Driver
 StorageSpaces-ManagementA
 StorageSpaces-Parser
 StorageSpaces-SpaceManager
 StorDiag
 Store
 StorPort
 StorSvc
 Sysmon
 System
 SystemSettings-Threshold
 TaskScheduler
 TCP/IP
 TerminalServices-ClientActiveD
 TerminalServices-ClientUSDe
 TerminalServices-LocalSession
 TerminalServices-PnPDevices
 TerminalServices-Printers
 TerminalServices-RamoteConn
 Time-Service
 Time-Service-PTP-Provider
 Troubleshooting-Recommend
 TZSync
 TZUI

Operational - Number of events: 32 (3 New events available)

Level	Date and Time	Source	Event ID	Task Ca...
Information	4/7/2023 1:34:58 AM	Sysmon	3	Network...
Information	4/7/2023 1:34:58 AM	Sysmon	3	Network...
Information	4/7/2023 1:34:58 AM	Sysmon	3	Network...
Information	4/7/2023 1:34:49 AM	Sysmon	1	Process...
Information	4/7/2023 1:34:41 AM	Sysmon	22	Dns qu...
Information	4/7/2023 1:34:40 AM	Sysmon	3	Network...
Information	4/7/2023 1:34:37 AM	Sysmon	22	Dns qu...
Information	4/7/2023 1:34:29 AM	Sysmon	1	Process...
Information	4/7/2023 1:34:26 AM	Sysmon	22	Dns qu...
Information	4/7/2023 1:34:25 AM	Sysmon	22	Dns qu...
Information	4/7/2023 1:34:24 AM	Sysmon	1	Process...
Information	4/7/2023 1:34:24 AM	Sysmon	1	Process...
Information	4/7/2023 1:34:09 AM	Sysmon	1	Process...
Information	4/7/2023 1:33:49 AM	Sysmon	1	Process...
Information	4/7/2023 1:33:35 AM	Sysmon	5	Process...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...
Information	4/7/2023 1:33:35 AM	Sysmon	13	Registr...

Event 3, Sysmon

General Details

Network connection detected

RuleName: -

UtcTime: 2023-04-06 20:04:56.423

ProcessGuid: {c17ee68-0716-642f-0201-000000000700}

ProcessId: 7976

Image: C:\Program Files\UEMS_CentralServer\jre\bin\java.exe

Log Name: Microsoft-Windows-Sysmon Operational

Source: Sysmon

Event ID: 3

Level: Information

User: SYSTEM

OpCode: Info

Task Category: Network connection detected (rule: NetworkConnect)

Keywords: DESKTOP-LSUC0U6

More Information: [Event Log Online Help](#)

Actions

Operational

Open Saved Log...

Create Custom View...

Import Custom View...

Clear Log...

Filter Current Log...

Properties

Disable Log

Find...

Save All Events As...

Attach a Task To This Log...

View

Refresh

Help

Event 3, Sysmon

Event Properties


Attach Task To This Event...

Copy

Save Selected Events...

Refresh

Help

 Management / Groups

< agent.conf of default group

Save

```
1 <agent_config>
2   <!-- Shared agent configuration here -->
3   <client_buffer>
4     <!-- Agent buffer options -->
5     <disable>no</disable>
6     <queue_size>100000</queue_size>
7     <events_per_second>1000</events_per_second>
8   </client_buffer>
9   <localfile>
10    <location>Microsoft-Windows-Windows Defender/Operational</location>
11    <log_format>eventchannel</log_format>
12    <location>Security</location>
13    <log_format>eventlog</log_format>
14    <location>Microsoft-Windows-Sysmon/Operational</location>
15    <log_format>eventchannel</log_format>
16  </localfile>
17 </agent_config>
```

▲ CHAPTER: 8 REFERENCES

CHAPTER 8 REFERENCES

- <https://www.ipindia.gov.in/>
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3217699/>
- <https://www.ies.gov.in/pdfs/why-India-needs-to-urgently-invest-in-its-IPR-ecosystem-16th-Aug-2022.pdf>
- <http://www.sric.iitkgp.ac.in/docss/iitkgpipguide.pdf>

