Linux Ubuntu 24.04 LTS: How to Customize.

How to Install Linux Ubuntu 24.04 LTS, Ubuntu 24.04 LTS is the latest Long-Term Support release of Ubuntu, launched in April 2024. It's the most recommended version for stability and long-term use, Codename: Noble Numbat. Information:

- Codename: Noble Numbat
- Release date: April 2024
- Support:
- 5 years (until April 2029)
- Up to 10–15 years with Ubuntu Pro
- Type: LTS (Long-Term Support)

Ubuntu 24.04 LTS was smooth,

Main Features

- **Linux Kernel 6.8 (initial release)**
- **GNOME 46 desktop (modern, smoother UI)**
- **Improved performance (better graphics handling & power efficiency)**
- **More stable and secure**

Who was it for?

- Linux beginners
- Developers / programmers
- Server administrators
- Everyday desktop users

Recommended System Requirements

- RAM: 4–8 GB (16 GB recommended)
- Storage: at least 251 GB
- CPU: dual-core or better

This recommended for Developers / programmers AND Everyday desktop users.Great— Ubuntu 24.04 LTS is an excellent choice for both **developers** and **server administrators** too.

Quick setup commands:

Terminal$ sudo su -
apt update # sudo apt upgrade -y

Essentials
apt install -y build-essential vim git curl wget
$ Gnome Smooth
# apt -y install gedit bluefish

How to Customize:

For Server Administrators

Why it's good

- Long-term security updates (5+ years)
- Reliable for production environments
- Strong community + enterprise support

Typical server roles

- Web server (Apache)
- Database (MySQL / MariaDB)
- File server / backup system

Basic server setup:
apt install openssh-server -y
apt install ufw -y
ufw allow OpenSSH
ufw enable

Must-do security steps (very important):
vim /etc/ssh/sshd_config
 # Set: PermitRootLogin no
 # PasswordAuthentication no
Esc:wq

Configure Firewall (UFW)
apt install ufw -y
ufw allow OpenSSH
ufw allow 80
ufw allow 443
ufw enable

Real production-ready server
apt install exfatprogs -yInstalls **exfatprogs**, which is used to manage **exFAT filesystem** (common for USB drives, SD cards, external disks).

After installing, your system can: Read/write exFAT drives, Format exFAT disks, Check and repair exFAT filesystem.
Production Advice
For servers:
- exFAT is **not recommended for main storage**
- Use:
  - ext4 (default Linux)
  - xfs (for large data)

exFAT is only for: ✔ USB / portable devices × Server database or system disk.

Next Step (Recommended):
apt install curl wget git -y

How to Customize:

Good step: you'll've next install Apache HTTP Server on Ubuntu 24.04 LTS:
apt install apache2 -y
ufw allow "Apache Full"
systemctl start apache2
systemctl stop apache2
systemctl restart apache2
systemctl enable apache2

Test in Browser Mozilla Firefox Open: http://localhost/ or http://127.0.0.1/

You should see: **Apache2 Ubuntu Default Page**.
Default Web Directory
ls –la /var/www/html

Recommended Next Command
Install PHP + MariaDB support:
pwd
apt install php libapache2-mod-php php-cli php-common php-mysql php-curl php-mbstring php-xml php-zip php-gd php-intl php-bcmath mariadb-server mariadb-client -y

Check now:
mysql --version
systemctl status mysql
systemctl status mariadb

Secure MariaDB
Run:
mysql_secure_installation
Recommended answers:
- Set root password → YES
- Remove anonymous users → YES
- Disallow remote root login → YES
- Remove test database → YES

Reload privilege tables → YES

Your Step: Secure production server.
apt update -y
apt upgrade -y
apt autoremove -y
apt autoclean

Enable automatic security updates:
apt install -y unattended-upgrades
dpkg-reconfigure unattended-upgrades

Firewall (UFW): Only expose what you need.
ufw default deny incoming
ufw default allow outgoing
ufw allow OpenSSH
ufw allow "Apache Full" //# ports 80 + 443
ufw enable
ufw status

SSH Hardening (critical):
ufw default deny incoming
ufw default allow outgoing
ufw allow OpenSSH
ufw allow "Apache Full"   # ports 80 + 443
ufw enable
ufw status

vim /etc/ssh/sshd_config
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
AllowUsers deploy
X11Forwarding no

systemctl restart ssh **Apache Security Tuning: .htaccess**
a2enmod headers rewrite ssl
systemctl restart apache2

vim /etc/apache2/conf-available/security.conf
ServerTokens Prod
ServerSignature Off
TraceEnable Off

Reload: Apache
systemctl reload apache2

Database Security:
+ Remove test DB
+ Disable remote root# vim /etc/mysql/mysql.conf.d/mysqld.cnf
bind-address = 127.0.0.1
systemctl restart mysql**Monitoring & Logs Apache:**
cat /var/log/apache2/access.log > /var/www/html/WebLogsLite/03.httpd.access.log# /bin/cat /var/log/apache2/access.log | grep $CURRENT_DATE > /var/www/html/WebLogsLite/04.httpd.access.txt# /bin/cat /var/log/apache2/access.log | grep *02/May/2026* > /var/www/html/WebLogsLite/03.httpd.access.txt **Backup Strategy (DON'T SKIP):**
mysqldump -u root -p appdb > backup.sql

Files: www/html
tar -czf backup.tar.gz /var/www/html

How to Customize:

Final Production Checklist:

✔ SSH key-only login ✔ Firewall active ✔ HTTPS enforced ✔ MySQL local-only ✔ Apache hardened ✔ Auto updates enabled ✔ Backups working

What This Command Does: # hw-probe -all -upload

- Scans:
  - CPU, RAM, disk, GPU, network
- Detects:
  - drivers and compatibility
- Uploads:
  - **public report online**
- Returns:
  - A **URL link** to your hardware profile

hw-probe -all -upload

Add Extra Login Protection (VERY IMPORTANT)

apt install apache2-utils -y
htpasswd -c /etc/phpmyadmin/password/.htpasswd001 admin

vim /var/www/html/login/.htaccessAuthType Basic
AuthName "Restricted Access"
AuthUserFile /etc/phpmyadmin/password/.htpasswd001
Require valid-user

Clean Server/Desktop Production Firewall:
22/tcp → SSH (restricted)
80/tcp → HTTP
443/tcp → HTTPS

First — Important Truth
! Renaming /phpmyadmin alone is **NOT real security**

Bots can still find it.
☞ We will do:

- ✔ Rename path
- ✔ Add authentication
- ✔ Restrict access

Remember command:
ufw status verbose

by: piasDraco [/pias : pias25]