BiT

Bahir Dar Institute Of Technology

ባሕር ዳር ቴክኖሎጂ ኢንስቲትዩት

Bahir Dar University

ባሕር ዳር ዩኒቨርሲቲ

OPERATING SYSTEM AND SYSTEM PROGRAMMIG

INDIVIDUAL ASSIGNMENT

INSTALLING TAILS OS

Name:- Eyob Molla

ID NO:- BDU1601462

Section:- A

Submitted to: - Lec. Wendimu Baye

Submission date: -16/08/2017 EC.

Contents

Introduction to Tails OS

Tails OS (The Amnesic Incognito Live System) is a privacy-focused, open-source operating system designed to protect user anonymity and security. Based on Debian Linux, it runs directly from a USB stick or DVD without installing anything on the host computer, ensuring no traces are left behind. A key feature of Tails is its amnesic nature unless configured with Persistent Storage, all data, including temporary files and browsing history, is erased after shutdown. To safeguard privacy, Tails routes all internet traffic through the Tor network, masking the user's location and identity while blocking non-Tor connections to prevent accidental leaks.

The OS comes pre-installed with essential privacy tools, such as the Tor Browser for anonymous web browsing, Thunderbird with Enigmail for encrypted email, KeePassXC for password management, OnionShare for secure file sharing, and MAT (Metadata Anonymization Toolkit) for removing metadata from files. Additionally, Tails incorporates strong security measures like Linux-based protections and Mandatory Access Control (MAC) to defend against malware and surveillance. It is compatible with most computers, making it accessible for users who need a portable, secure system. Tails is widely used by journalists, whistleblowers (like Edward Snowden), activists, and privacy-conscious individuals who want to avoid tracking and censorship. Getting started involves downloading the ISO from the official website, verifying its authenticity, creating a bootable USB, and booting from it.

While Tails offers strong anonymity, it has some limitations, such as slower internet speeds due to Tor routing and incompatibility with high-performance tasks like gaming or video editing. Despite these trade-offs, Tails remains a trusted tool for digital privacy, making it an excellent choice for those seeking secure, untraceable computing.

The History of Tails Operating System

The Amnesic Incognito Live System, more commonly known as Tails**,** is a securityfocused Linux distribution developed to preserve privacy and anonymity. Officially released on June 23, 2009, Tails was born out of the merging of two earlier privacy projects: Incognito and Amnesia. Incognito was a Gentoo-based Linux distribution centered on anonymous web browsing, but it was eventually discontinued. Amnesia, the original name for what would become Tails, merged with Incognito to form a new, more robust privacy-centric operating system.

From its inception, Tails aimed to provide users with a portable and secure computing environment that could be booted from a USB stick or DVD, leaving no trace on the host system. Its defining feature is its integration with **Tor**, the anonymity network that routes internet traffic through multiple servers to conceal users' identities and locations. Early in its development, the Tor Project offered financial support, helping to solidify Tails' foundational ties with the Tor network.

Over time, Tails gained additional funding and institutional backing from organizations committed to digital freedom and open technology. Notable contributors included the Open Technology Fund, Mozilla, and the Freedom of the Press Foundation. These partnerships helped sustain and expand Tails' development, ensuring that it remained an up-to-date and trustworthy tool for users in need of secure communication and privacy.

Tails gained international attention due to its role in investigative journalism and whistleblower communication. Journalists such as Laura Poitras, Glenn Greenwald, Bruce Schneier, and Barton Gellman all publicly credited Tails as a vital tool in their work with Edward Snowden, the former NSA contractor who leaked classified documents in 2013. Its ability to operate as a live system that leaves no digital footprint made it ideal for sensitive, high-risk work where confidentiality was paramount.

As technology progressed, Tails also evolved to stay current. In 2017, with the release **of** version 3.0, Tails dropped support for 32-bit processors, requiring users to have a 64-bit system. This move improved system performance and enhanced overall security, reflecting the project's commitment to remaining a modern and effective platform.

A significant development in Tails' organizational history occurred in 2023, when the Tails Project proposed a formal merger with The Tor Project. The merger was officially completed on September 26, 2024, with the aim of unifying efforts and allowing the Tails team to focus more closely on their core mission. In a public statement, the Tails Project noted that, "By joining forces, the Tails team can now focus on their core mission of maintaining and improving Tails OS, exploring more and complementary use cases while benefiting from the larger organizational structure of The Tor Project."

Today, Tails continues to serve as a critical tool for journalists, activists, and anyone needing to protect their privacy in an increasingly monitored digital world. From its early days as a combination of Incognito and Amnesia to its current home under the Tor Project's umbrella, Tails has consistently upheld its mission to provide secure, anonymous computing for all.

Motivation to The Development of Tails OS

The development of Tails was primarily motivated by the growing need for privacy, anonymity, and security in the digital age. As internet surveillance, censorship, and data collection became more widespread, users—especially journalists, activists, whistleblowers, and political dissidents—needed tools to protect their communications and identities.

One of the major driving forces was the realization that standard operating systems leave traces of activity on computers. Temporary files, browsing history, logs, and metadata could easily be recovered—even after deletion—making users vulnerable to tracking or forensic analysis. Tails was created as a live operating system that runs entirely in memory and leaves no trace on the host machine after shutdown.

Another major motivation was to integrate the Tor network natively into an operating system to ensure all network traffic was anonymized. While Tor could be installed separately on other systems, this approach was often too technical or inconsistent. Tails ensures that every internet connection is routed through Tor by default, offering a turnkey solution for anonymous browsing and secure communication.

Additionally, the rise of repressive regimes and mass surveillance programs (such as those revealed by Edward Snowden) highlighted the urgent need for a portable, censorship-resistant operating system. The creators of Tails aimed to empower individuals in such environments by providing a system that could be booted from a USB stick or DVD on almost any computer, without needing installation or leaving evidence behind.

Generally, the motivation behind Tails was to build a secure, anonymous, and portable computing environment that anyone could use regardless of their technical skill level to communicate and work safely under the threat of surveillance, censorship, or persecution

Objectives of tails OS

Tails OS (The Amnesic Incognito Live System) is a Debian-based Linux distribution designed to prioritize user privacy and anonymity. The primary objectives of Tails OS include the following.

1. **Preserving User Privacy and Anonymity**: Tails routes all internet connections through the Tor network, ensuring that users' locations and identities are concealed. It blocks all non-anonymous connections to prevent accidental data leaks.
2. **Amnesic Operation**: By default, Tails runs in the computer's RAM and does not write to the hard drive, leaving no trace of the user's activities after shutdown. This design ensures that sensitive data is not stored on the device.
3. **Portable and Live System**: Tails is designed to be booted from a USB stick or DVD, allowing users to operate it on almost any computer without installation. This portability enables users to maintain privacy on shared or public machines.
4. **Secure Communication Tools**: Tails comes pre-installed with applications like the Tor Browser for anonymous web browsing, Thunderbird with Enigmail for encrypted emails, and Pidgin with OTR for secure instant messaging, facilitating confidential communication.

5. **Protection Against Surveillance and Censorship**: By leveraging the Tor network and providing tools for encrypted communication, Tails helps users circumvent censorship and protect against surveillance, making it valuable for journalists, activists, and individuals in repressive regimes.

And also We can see four additional objectives of Tails OS that enhance its privacy and security features:

1. **Secure and Encrypted File Storage**

   Tails allows users to create an optional encrypted Persistent Storage on the USB stick. This enables the secure storage of specific files and settings across sessions, such as documents, Wi-Fi configurations, and additional software, without compromising the system's amnesic nature.

2. **Inclusion of Comprehensive Privacy Tools**

   Tails comes pre-installed with a suite of privacy-focused applications, including:

   I. **Tor Browser** for anonymous web browsing
   II. **Thunderbird** with Enigmail for encrypted email communication
   III. **KeePassXC** for secure password management
   IV. **OnionShare** for anonymous file sharing

Requirements to install tails OS on VMware

Running Tails OS within VMware is feasible, but it's important to understand that doing so may compromise some of Tails' core privacy and security features. Tails is designed to run as a live system from a USB stick or DVD, ensuring that no traces are left on the host compute.

Hardware Requirements

While Tails does not officially support running in virtual machines like on VMware, but the following hardware specifications can help ensure smooth operation:

I. **Processor**: 64-bit Intel or AMD processor but Tails does not support ARM or PowerPC architectures.
II. **Memory**: At least 2 GB of RAM allocated to the virtual machine.
III. **Storage**: VMware installation and Tails ISO image storage. Note that Tails is designed to run without persistent storage, so no virtual hard disk is necessary.
IV. **Network Adapter**: Dedicated USB network interface controllers (NICs) are recommended for enhanced privacy.

V. **internet Connection** : An internet connection is necessary to access the Tor network and use Tails' online features. It's recommended to connect via Ethernet for more reliable network connectivity.

Software Requirements

A. Host Operating System: Windows 7 or Later

Windows 7+ ?

I. Tails is designed to work on modern systems, and Windows 7 (released in 2009) is the oldest version but it is still compatible with current VMware software.

II. Older Windows versions lack driver support for virtualization and USB 3.0, which Tails may require.

64-bit vs. 32-bit ?

I. Tails 3.0+ requires a 64-bit host OS because it no longer supports 32bit processors.

B. Virtualization Software: VMware Workstation or Player

i. **VMware Workstation Pro :** it is Best for advanced user.

Why VMware?

VMware is more stable for Tails than VirtualBox because of it's better network & USB passthrough.

- Supports UEFI/legacy BIOS modes and this model is needed for Tails booting.

C. Tails ISO Image

- Must be downloaded from the official site: https://tails.boum.org.

Why verify the ISO?

- To Ensures the file wasn't corrupted.
- Prevents malware-infected versions from being installed.

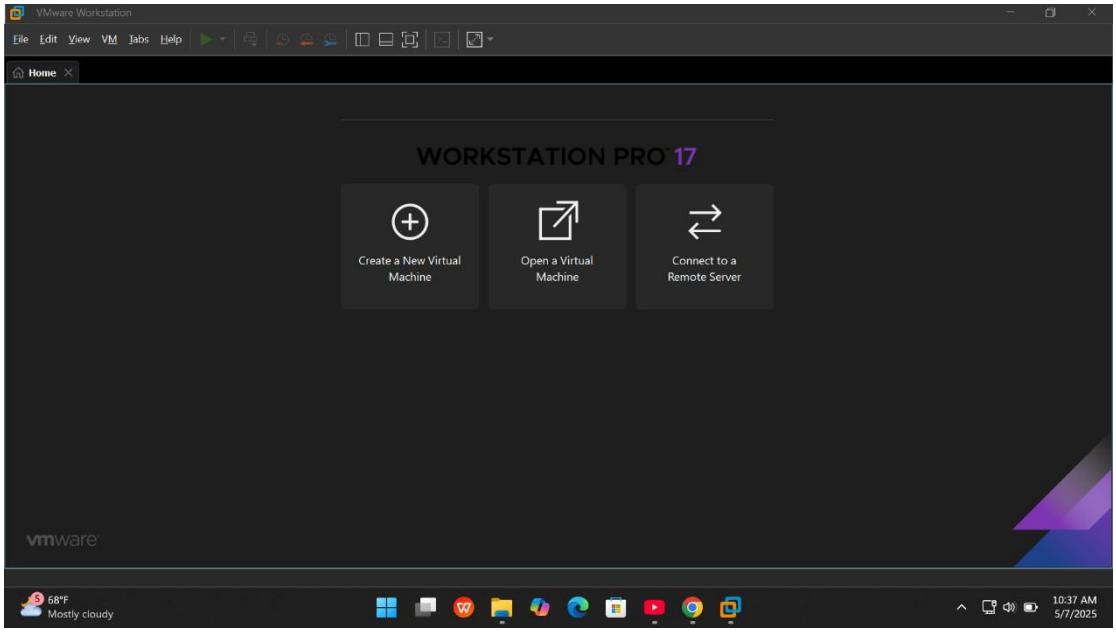
Minimum 8GB?

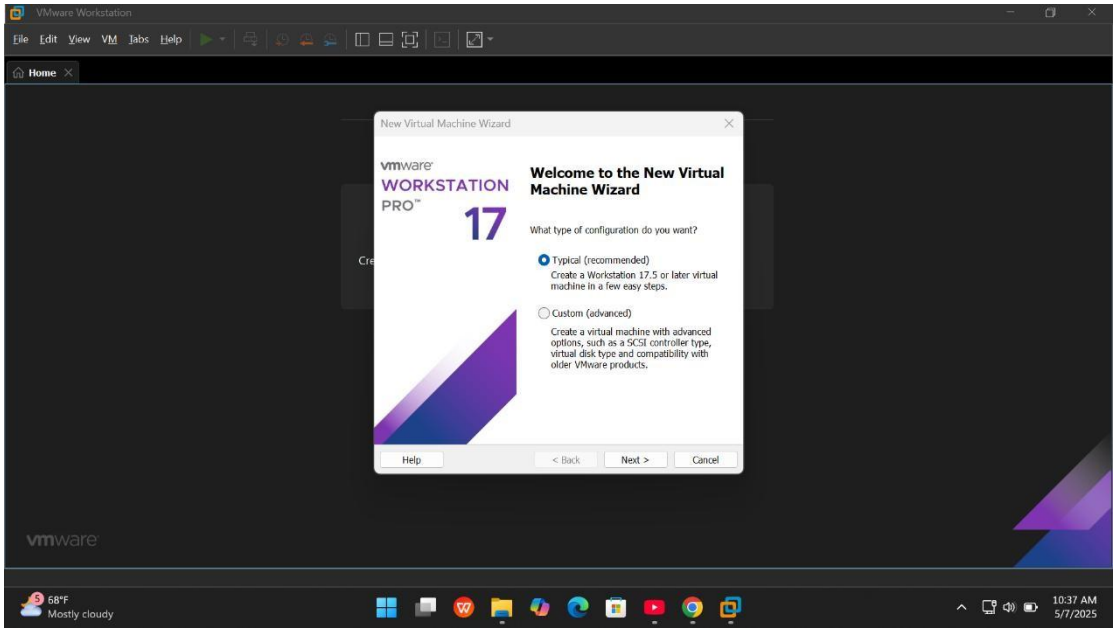
- Tails itself takes ~4GB, leaving space for encrypted storage.

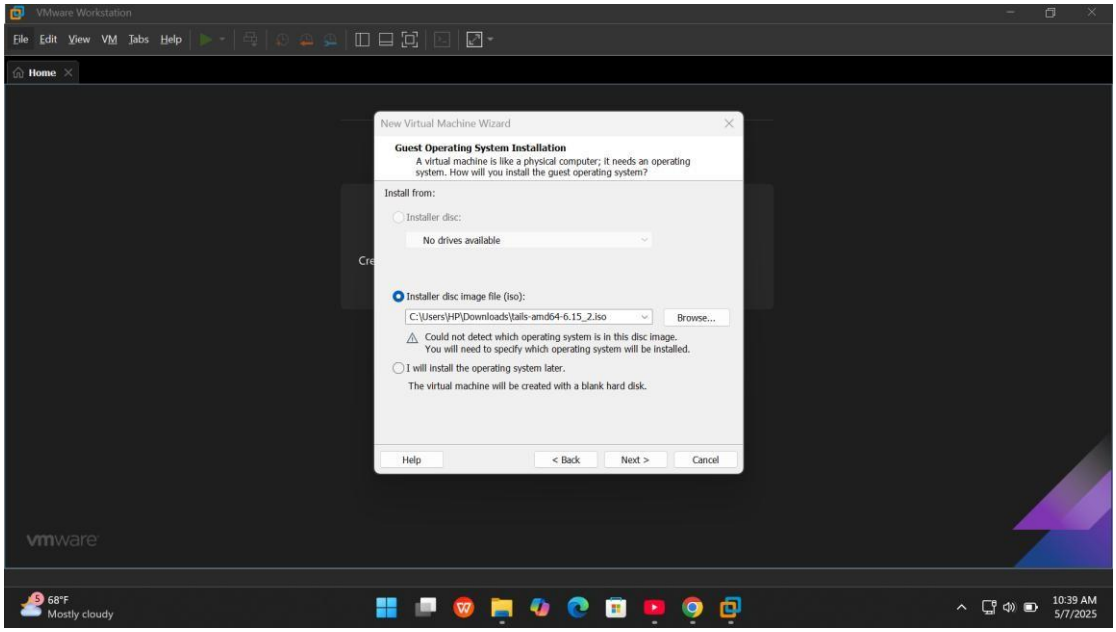
Installation Process

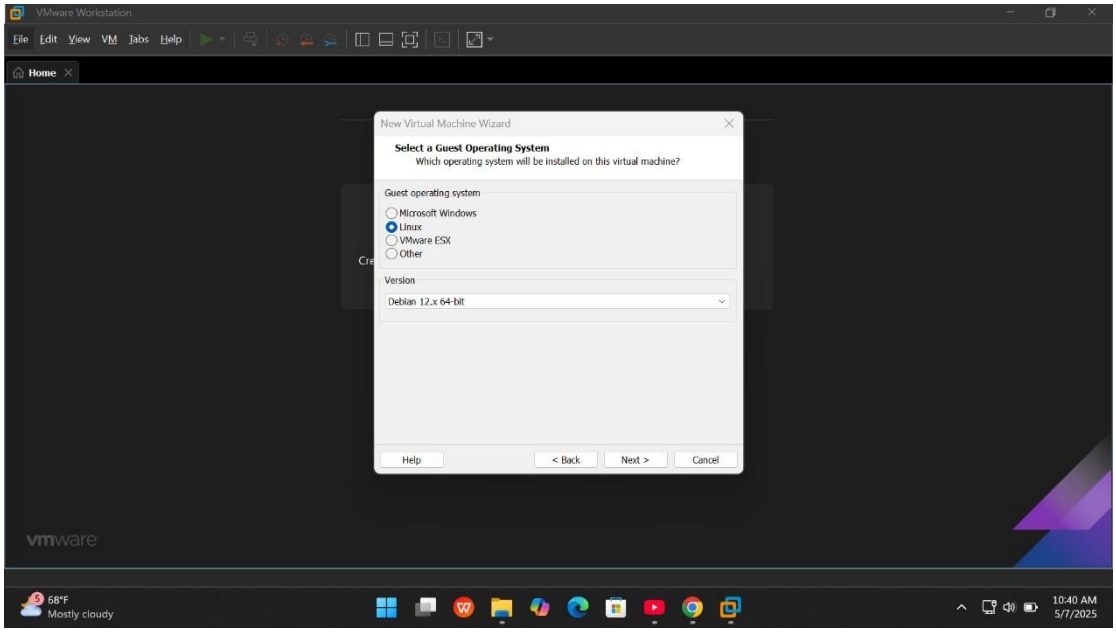
During the installation process of Tails OS I am going to follow the following steps to install tails OS on VMware .

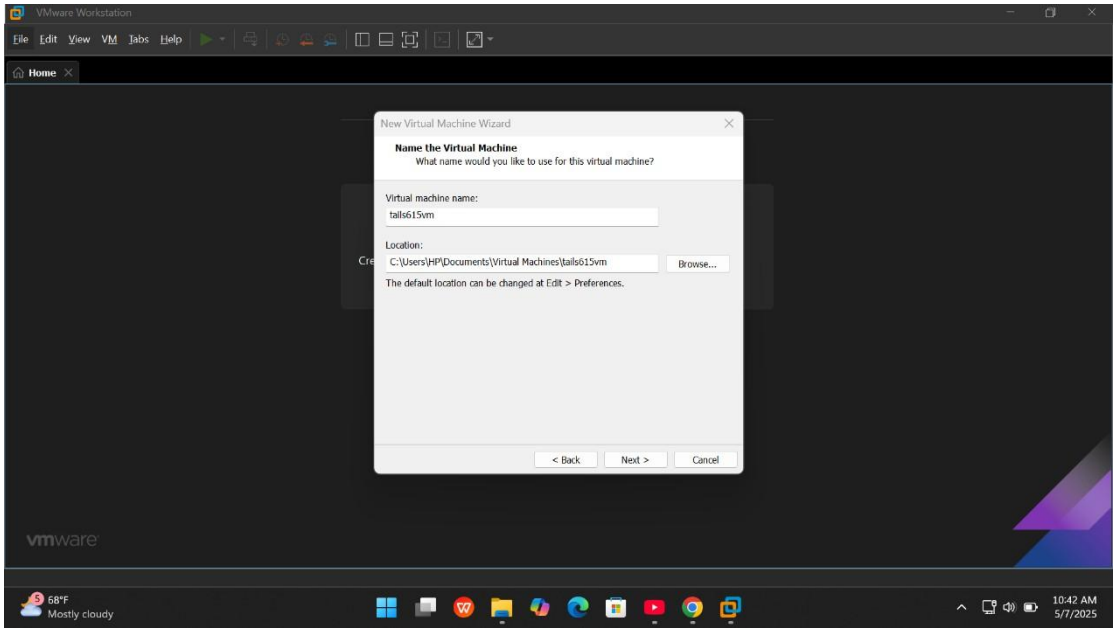
- **Download the Tails ISO:**
  first of all I will Go to the official Tails website (install tails.net/ /) and I will download the latest Tails ISO image and I am going to verify it to check if it is the latest one.
- **Open VMware Workstation:**
  After I download and installed my VMware I going to Launch VMware Workstation Player or Workstation.
- **Create a New Virtual Machine:** and then Click "Create a New Virtual Machine". I will Choose "Installer disk image" and browse for the Tails ISO I downloaded.
- **Specify Guest Operating System:**
  Select "Linux" as the guest operating system type and I choose Debian 12.x 64 bit but another version is also possible like "Other Linux 5.x 64 bit".
- **Configure Memory:**
  Allocate at least 2048 MB (2 GB) of RAM to the virtual machine.
- **Choose Hard Drive Option:**
  Select "Do not add a virtual hard drive".
  Proceed with the warning dialog about creating a VM without a hard drive.
- **Boot from the Tails ISO:** and then Power on the virtual machine. The VM will boot from the Tails ISO, and the Tails installation process will start.
- **Wait for Tails to Load:**
  Once the VM boots, Tails will load into the Welcome to Tails screen.
  This might take a minute depending on my system.
- **Configure Tails Settings (Optional):**
  At the Welcome screen, you can choose additional settings such as language, keyboard layout, and MAC address spoofing.
  Click **"Start Tails"** to continue with default or customized settings.
- **Tails Desktop Loads:**
  After a short loading period, you'll be presented with the Tails desktop environment, which runs entirely from memory.
- **Use Tails in Live Mode:**
  Tails is a live operating system and does not store data permanently. You can browse the internet, use included applications (like Tor Browser, KeePassXC, LibreOffice), or plug in a USB drive for persistent storage.
- **Shut Down Tails Safely:**
  When finished, click the **power icon** in the top right corner and choose **"Shutdown"**.
  Tails will erase all memory and shut down secure .
  Now I going to show the above steps in practice

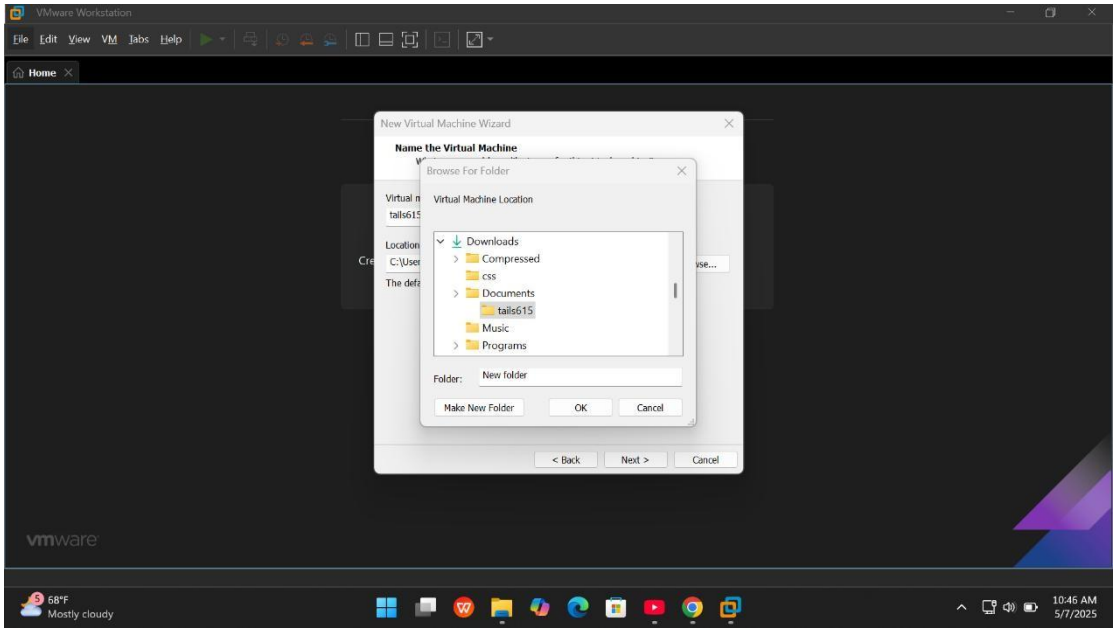

VMware Workstation
File Edit View VM Tabs Help
Home
WORKSTATION PRO 17
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
vmware
68°F
Mostly cloudy
10:37 AM
5/7/2025

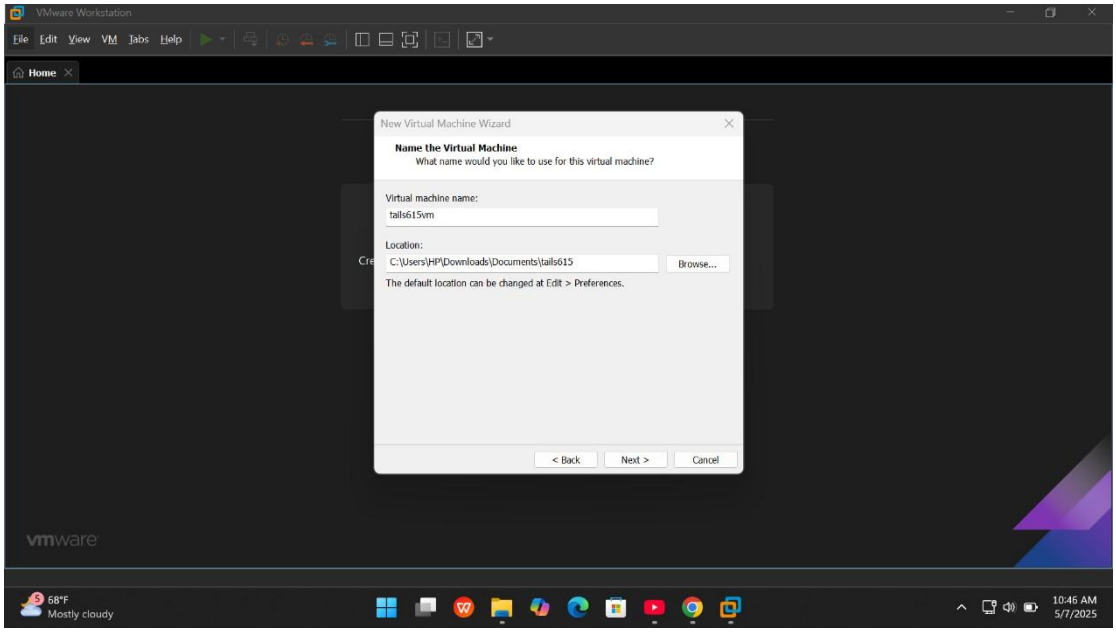

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
vmware
WORKSTATION
PRO™
17
Welcome to the New Virtual Machine Wizard
What type of configuration do you want?
Typical (recommended)
Create a Workstation 17.5 or later virtual machine in a few easy steps.
Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.
Help
< Back
Next >
Cancel
vmware
68°F
Mostly cloudy
10:37 AM
5/7/2025

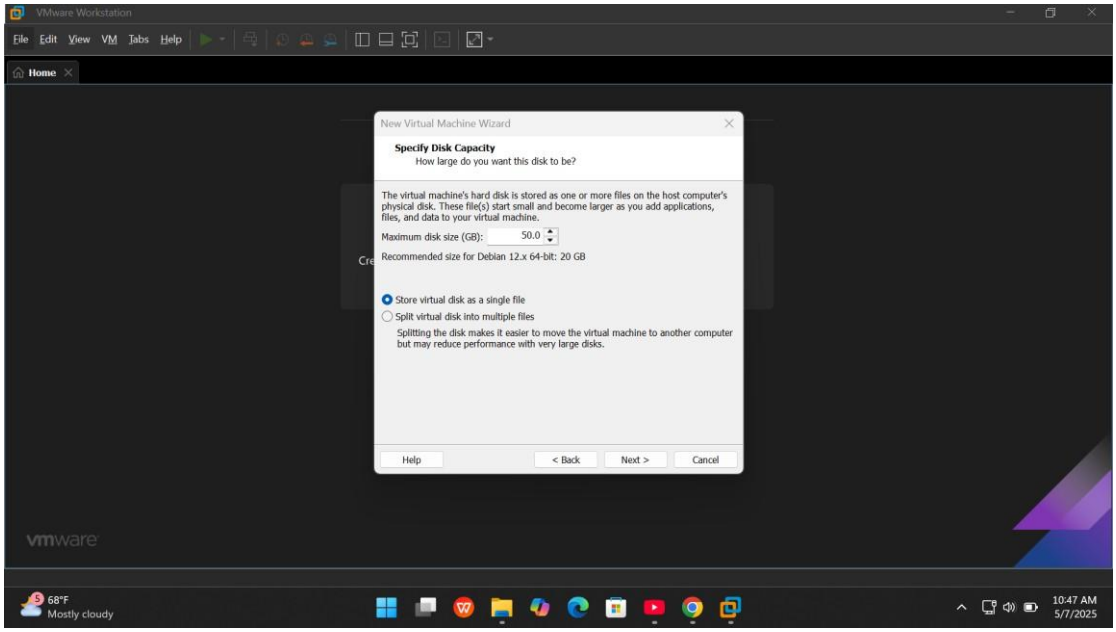

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
No drives available
Installer disc image file (iso):
C:\Users\HP\Downloads\tails-amd64-6.15_2.iso
Browse...
Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel
vmware
68°F
Mostly cloudy
10:39 AM
5/7/2025

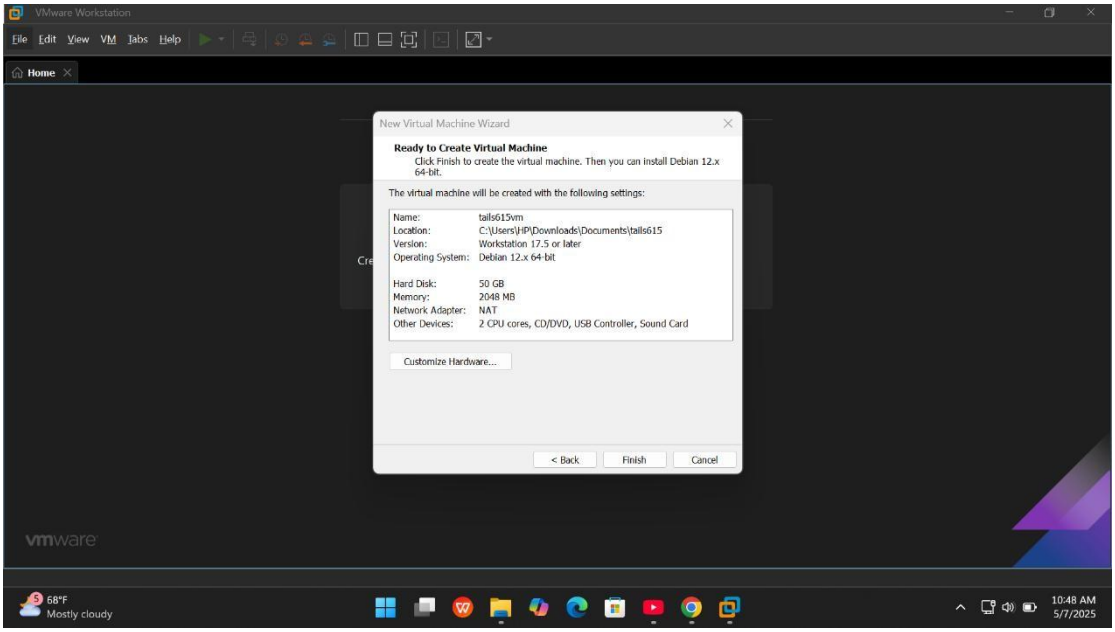

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
Select a Guest Operating System
Which operating system will be installed on this virtual machine?
Guest operating system
Microsoft Windows
Linux
VMware ESX
Other
Version
Debian 12.x 64-bit
Help
< Back
Next >
Cancel
vmware
68°F
Mostly cloudy
10:40 AM
5/7/2025

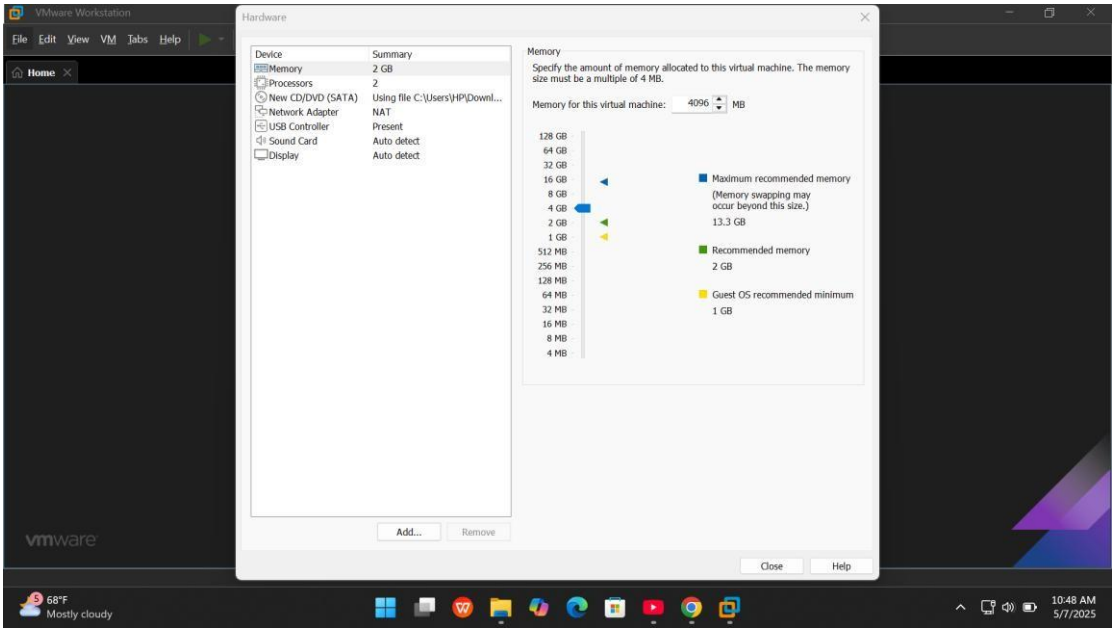

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
tails615vm
Location:
C:\Users\HP\Documents\Virtual Machines\tails615vm
Browse...
The default location can be changed at Edit > Preferences.
< Back
Next >
Cancel
vmware
68°F
Mostly cloudy
10:42 AM
5/7/2025

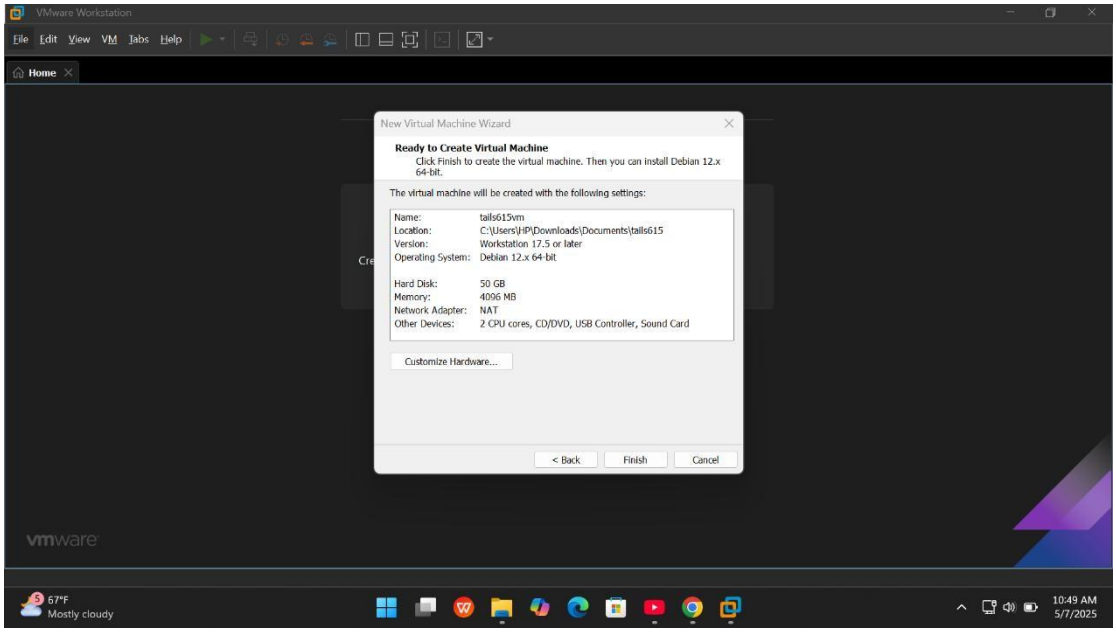

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
Name the Virtual Machine
Browse For Folder
Virtual Machine Location
Downloads
Compressed
css
Documents
tails615
Music
Programs
Folder:
New folder
Make New Folder
OK
Cancel
< Back
Next >
Cancel
vmware
68°F
Mostly cloudy
10:46 AM
5/7/2025

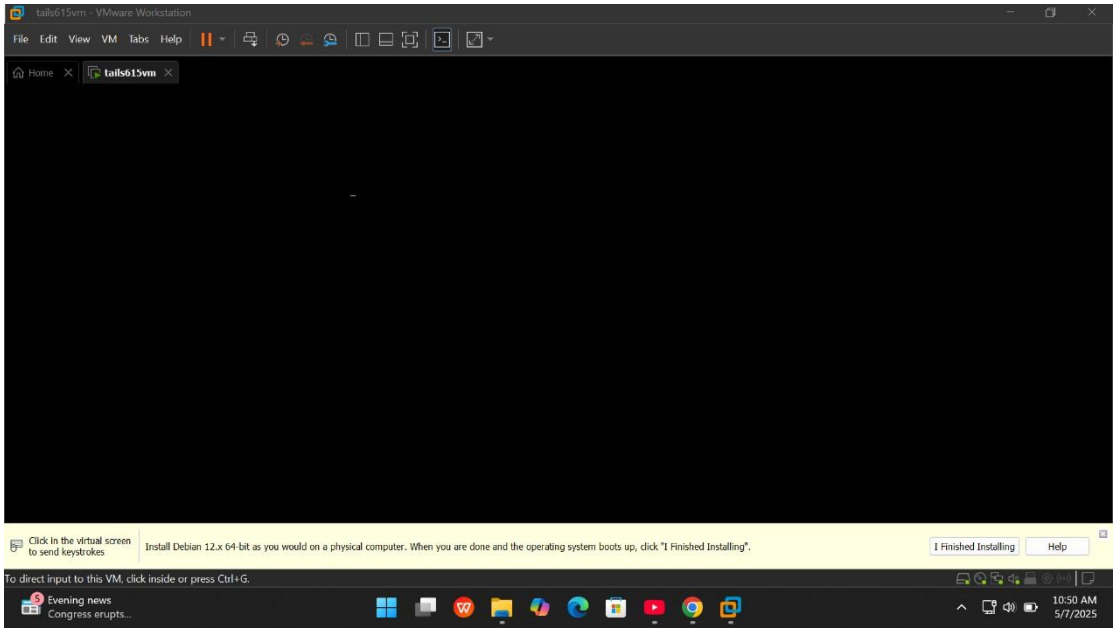

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
tails615vm
Location:
C:\Users\HP\Downloads\Documents\tails615
Browse...
The default location can be changed at Edit > Preferences.
< Back
Next >
Cancel
vmware
68°F
Mostly cloudy
10:46 AM
5/7/2025

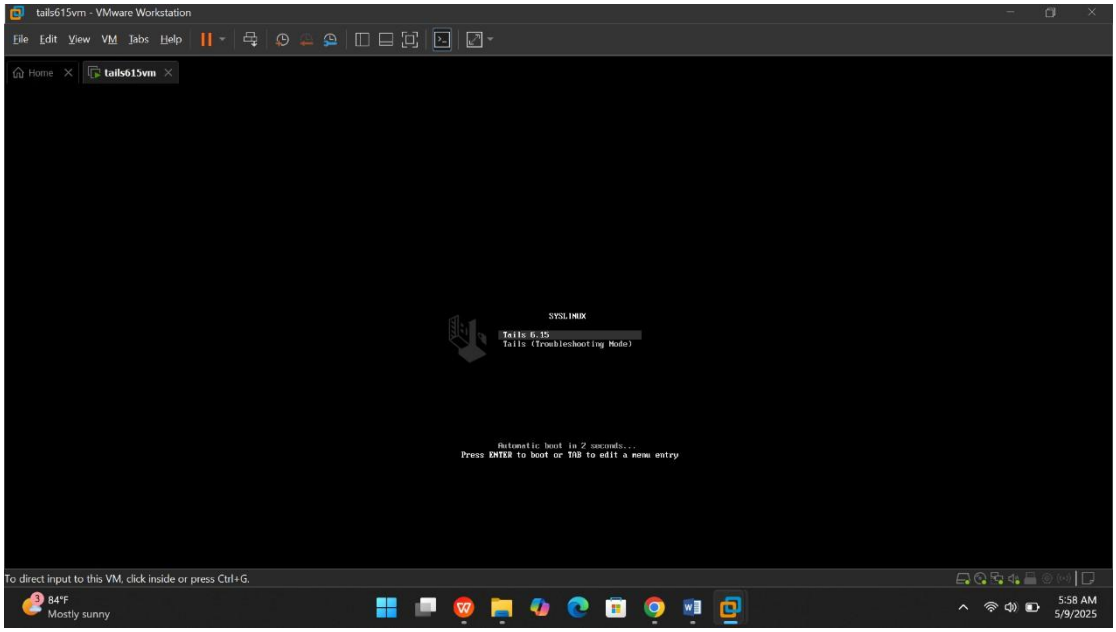

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
50.0
Recommended size for Debian 12.x 64-bit: 20 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel
vmware
68°F
Mostly cloudy
10:47 AM
5/7/2025

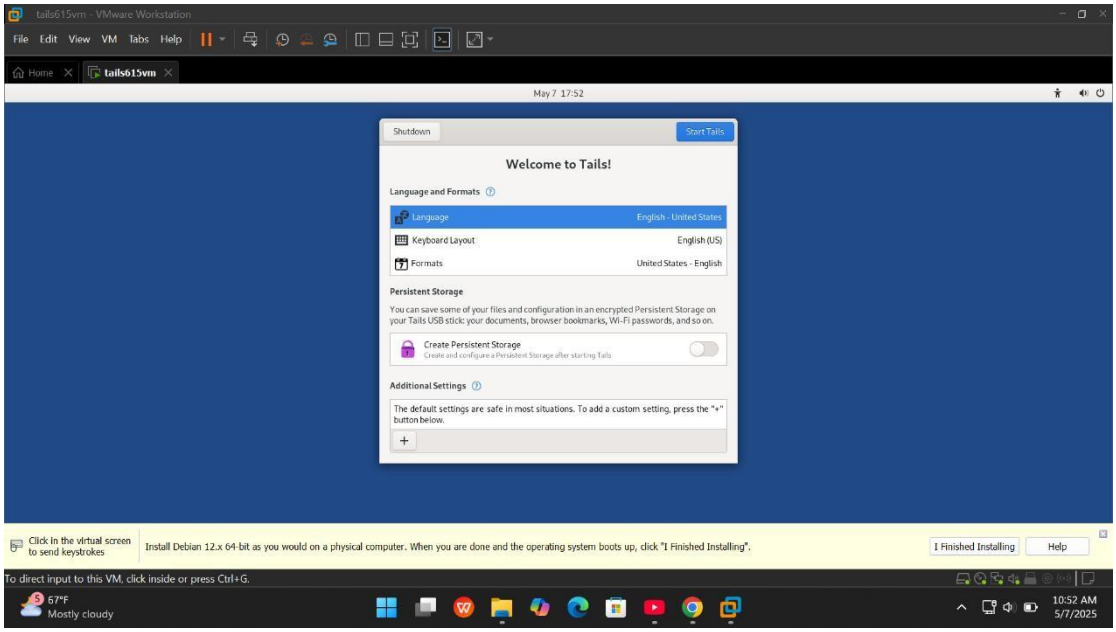

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Debian 12.x 64-bit.
The virtual machine will be created with the following settings:
Name: tails615vm
Location: C:\Users\HP\Downloads\Documents\tails615
Version: Workstation 17.5 or later
Operating System: Debian 12.x 64-bit
Hard Disk: 50 GB
Memory: 2048 MB
Network Adapter: NAT
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Sound Card
Customize Hardware...
< Back
Finish
Cancel
vmware
68°F
Mostly cloudy
10:48 AM
5/7/2025

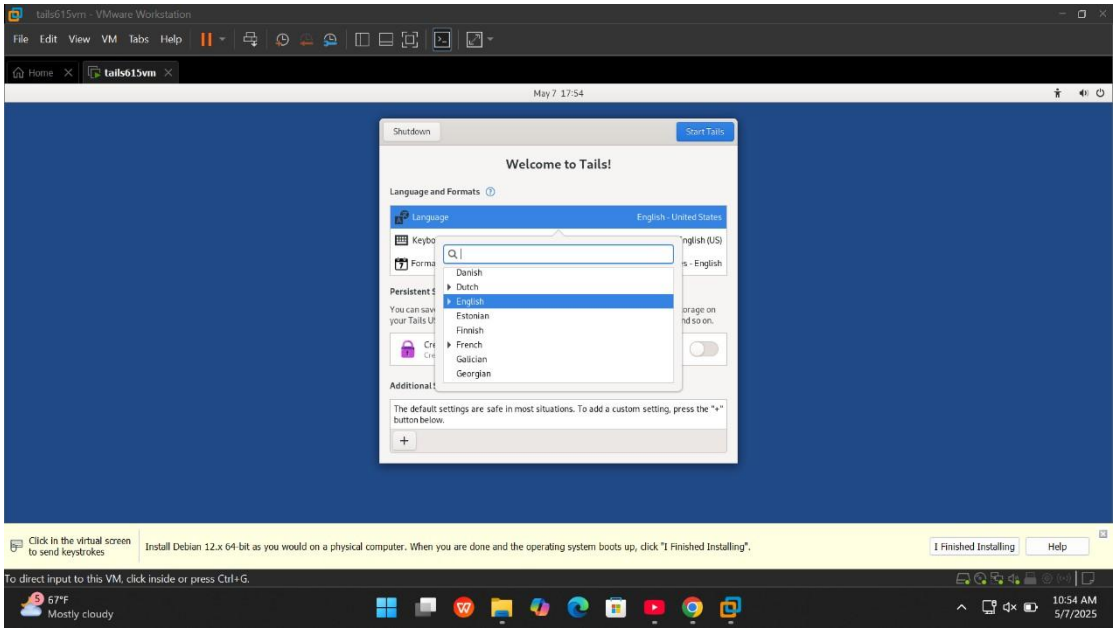

VMware Workstation
File Edit View VM Tabs Help
Home
Hardware
Device Summary
Memory 2 GB
Processors 2
New CD/DVD (SATA) Using file C:\Users\HP\Downl...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect
Add...
Remove
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine: 4096 MB
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory
(Memory swapping may occur beyond this size.)
13.3 GB
Recommended memory
2 GB
Guest OS recommended minimum
1 GB
Close
Help
vmware
68°F
Mostly cloudy
10:48 AM
5/7/2025

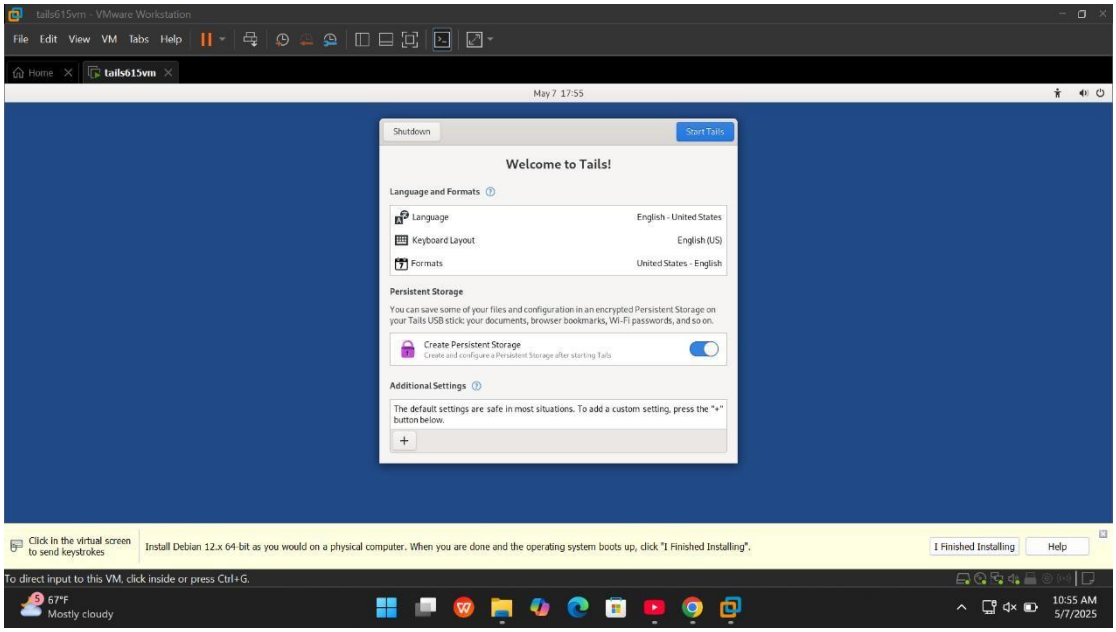

VMware Workstation
File Edit View VM Tabs Help
Home
New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Debian 12.x 64-bit.
The virtual machine will be created with the following settings:
Name: tails615vm
Location: C:\Users\HP\Downloads\Documents\tails615
Version: Workstation 17.5 or later
Operating System: Debian 12.x 64-bit
Hard Disk: 50 GB
Memory: 4096 MB
Network Adapter: NAT
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Sound Card
Customize Hardware...
< Back
Finish
Cancel
vmware
67°F
Mostly cloudy
10:49 AM
5/7/2025

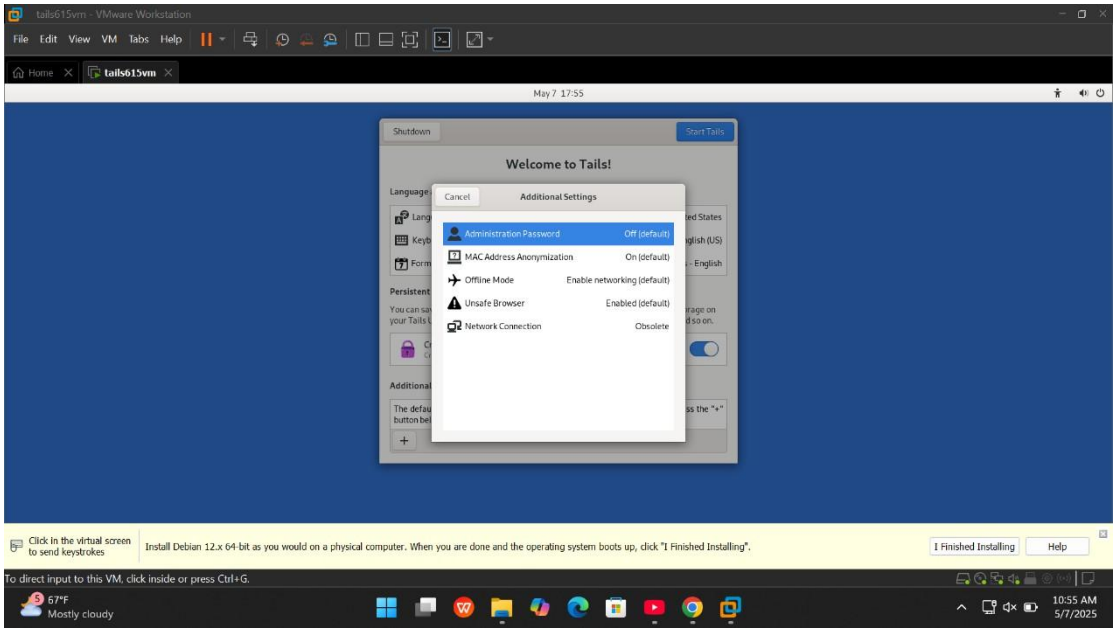

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Click in the virtual screen to send keystrokes
Install Debian 12.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, click inside or press Ctrl+G.
Evening news
Congress erupts...
10:50 AM
5/7/2025

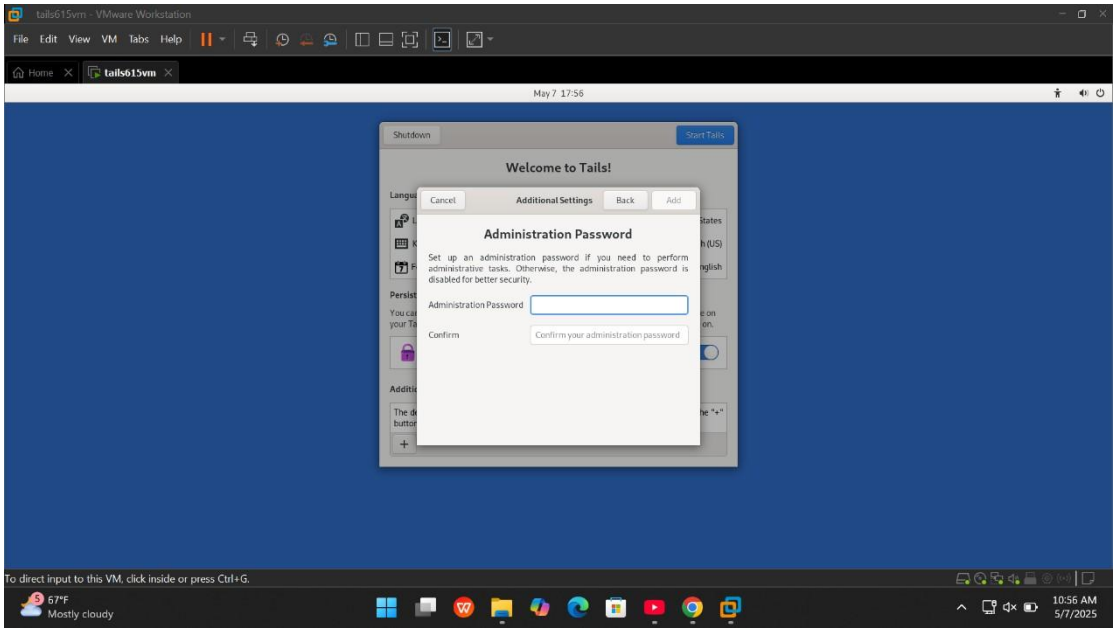

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
SYSLINUX
Tails 6.15
Tails (Troubleshooting Mode)
Automatic boot in 2 seconds...
Press ENTER to boot or TAB to edit a menu entry
To direct input to this VM, click inside or press Ctrl+G.
84°F
Mostly sunny
5:58 AM
5/9/2025

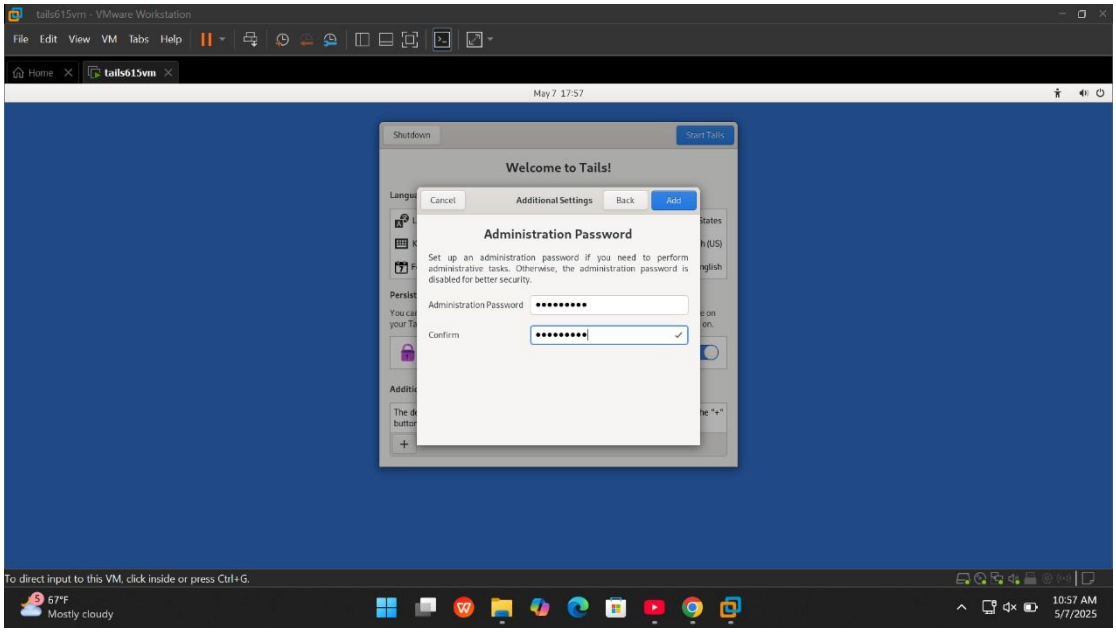

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
May 7 17:52
Shutdown
Start Tails
Welcome to Tails!
Language and Formats
Language
English - United States
Keyboard Layout
English (US)
Formats
United States - English
Persistent Storage
You can save some of your files and configuration in an encrypted Persistent Storage on your Tails USB stick: your documents, browser bookmarks, Wi-Fi passwords, and so on.
Create Persistent Storage
Create and configure a Persistent Storage after starting Tails
Additional Settings
The default settings are safe in most situations. To add a custom setting, press the "+" button below.
Click in the virtual screen to send keystrokes
Install Debian 12.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:52 AM
5/7/2025

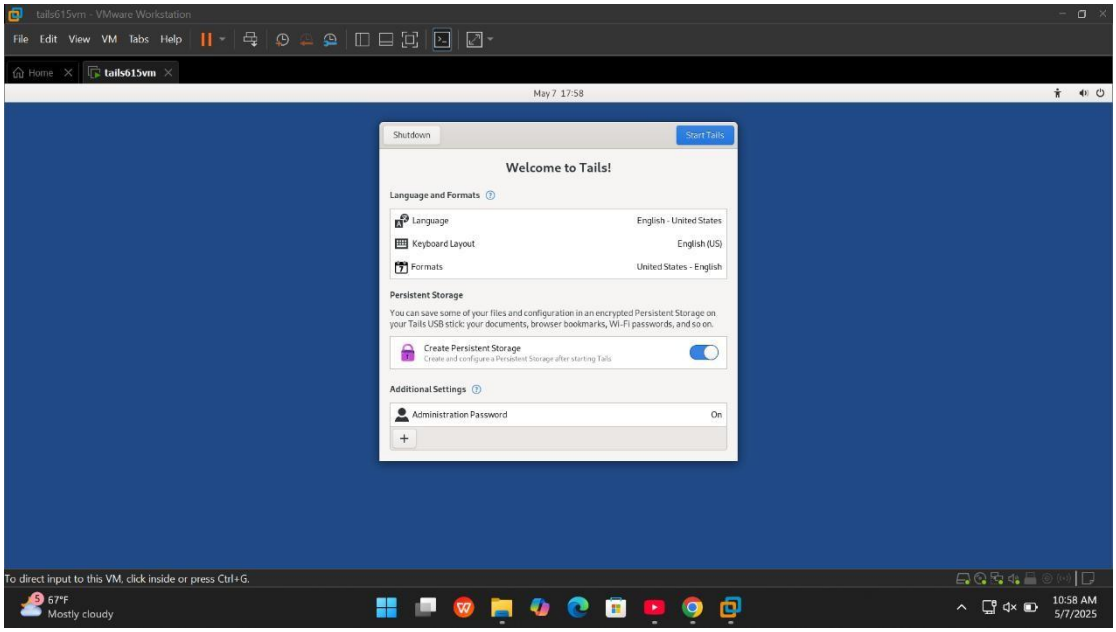

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
May 7 17:54
Shutdown
Start Tails
Welcome to Tails!
Language and Formats
Language
English - United States
Danish
Dutch
English
Estonian
Finnish
French
Galician
Georgian
The default settings are safe in most situations. To add a custom setting, press the "+" button below.
Click in the virtual screen to send keystrokes
Install Debian 12.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:54 AM
5/7/2025

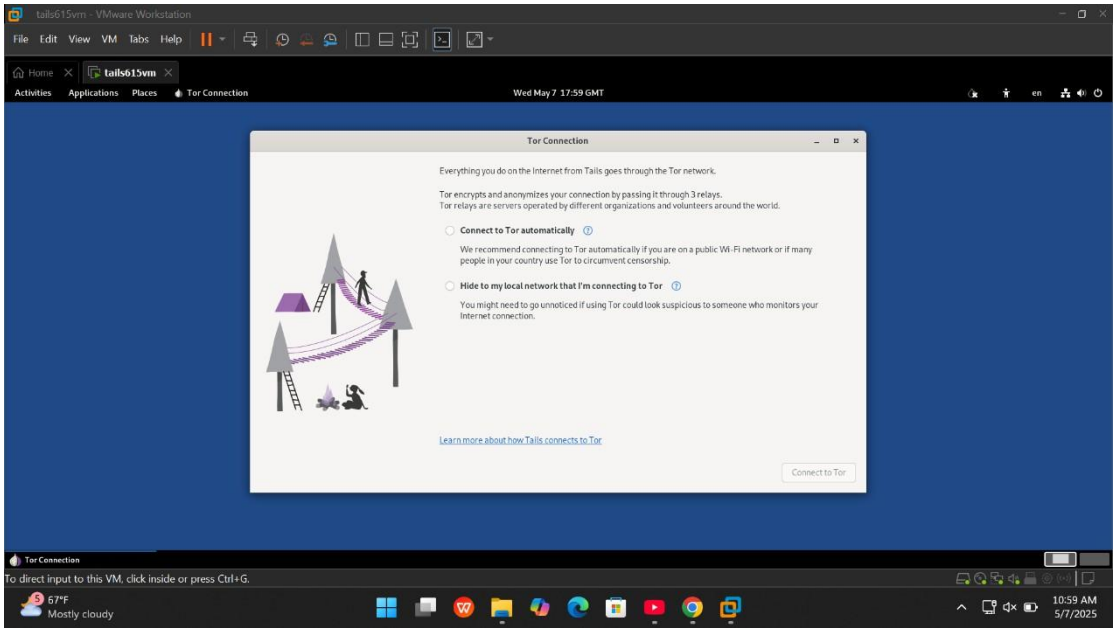

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
May 7 17:55
Shutdown
Start Tails
Welcome to Tails!
Language and Formats
Language
English - United States
Keyboard Layout
English (US)
Formats
United States - English
Persistent Storage
You can save some of your files and configuration in an encrypted Persistent Storage on your Tails USB stick: your documents, browser bookmarks, Wi-Fi passwords, and so on.
Create Persistent Storage
Create and configure a Persistent Storage after starting Tails
Additional Settings
The default settings are safe in most situations. To add a custom setting, press the "+" button below.
Click in the virtual screen to send keystrokes
Install Debian 12.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:55 AM
5/7/2025

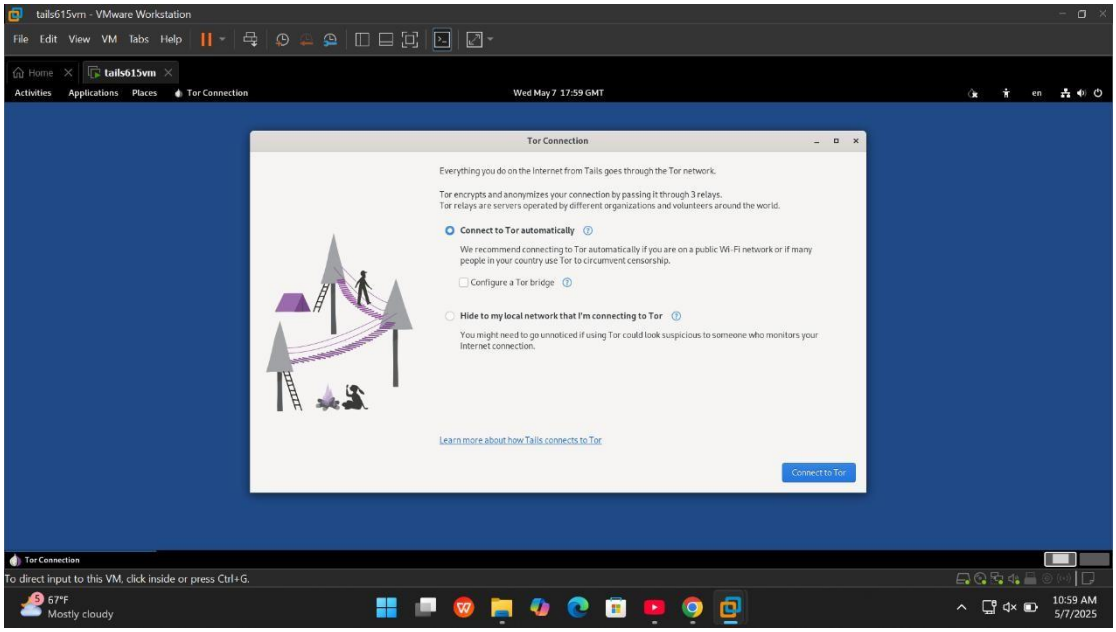

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
May 7 17:55
Shutdown
Start Tails
Welcome to Tails!
Cancel
Additional Settings
Administration Password
Off (default)
MAC Address Anonymization
On (default)
Offline Mode
Enable networking (default)
Unsafe Browser
Enabled (default)
Network Connection
Obsolete
Click in the virtual screen to send keystrokes
Install Debian 12.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:55 AM
5/7/2025

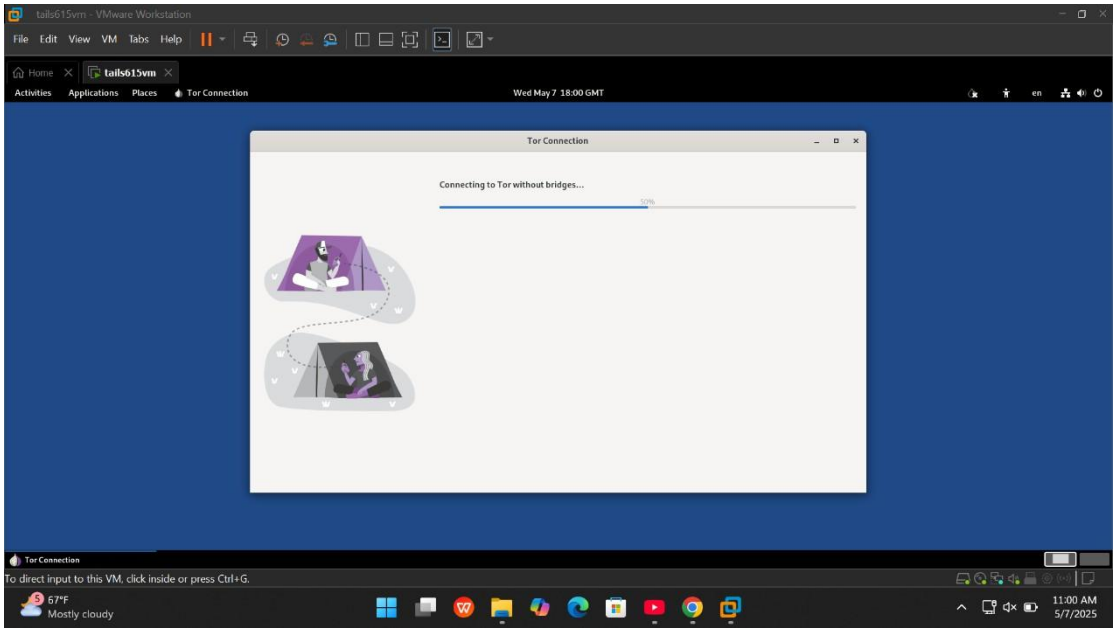

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
May 7 17:56
Shutdown
Start Tails
Welcome to Tails!
Cancel
Additional Settings
Back
Add
Administration Password
Set up an administration password if you need to perform administrative tasks. Otherwise, the administration password is disabled for better security.
Administration Password
Confirm
Confirm your administration password
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:56 AM
5/7/2025

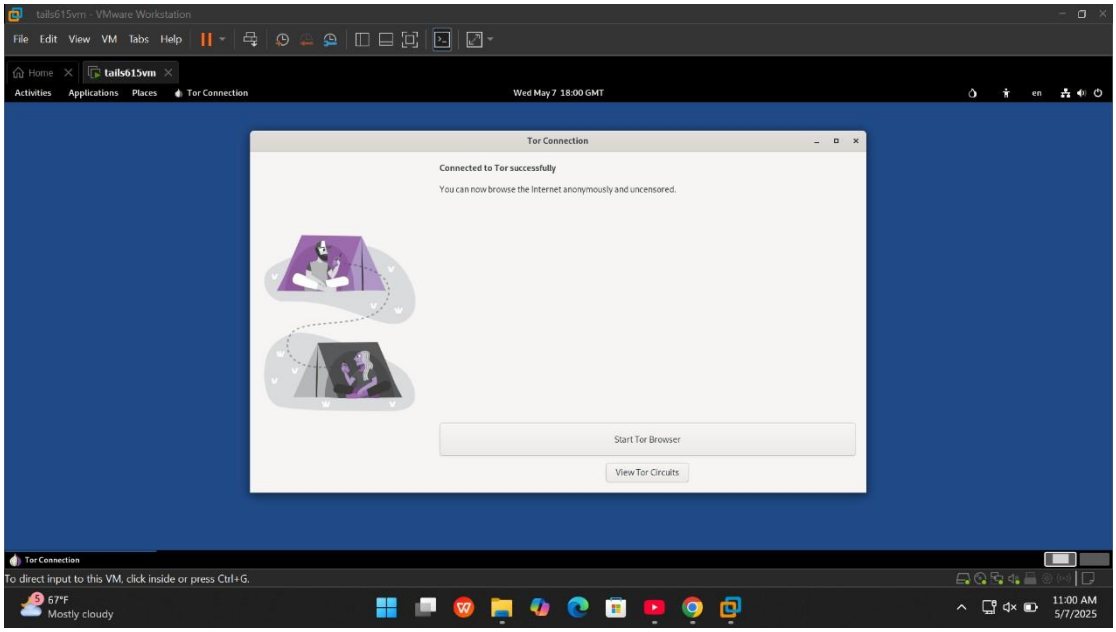

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
May 7 17:57
Shutdown
Start Tails
Welcome to Tails!
Cancel
Additional Settings
Back
Add
Administration Password
Set up an administration password if you need to perform administrative tasks. Otherwise, the administration password is disabled for better security.
Administration Password
Confirm
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:57 AM
5/7/2025

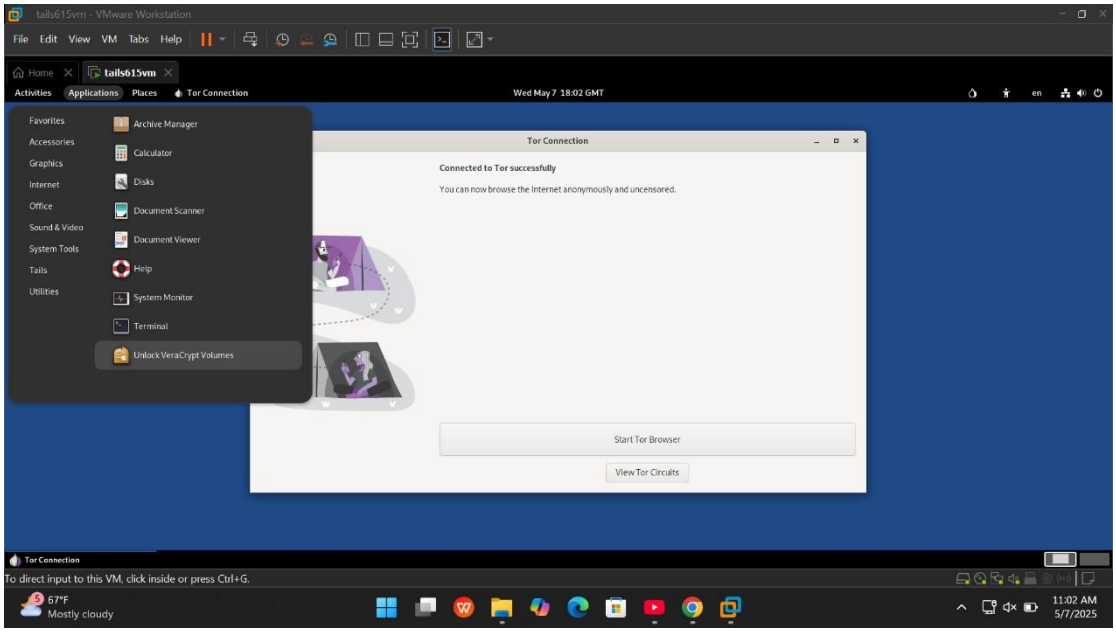

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
May 7 17:58
Shutdown
Start Tails
Welcome to Tails!
Language and Formats
Language
English - United States
Keyboard Layout
English (US)
Formats
United States - English
Persistent Storage
You can save some of your files and configuration in an encrypted Persistent Storage on your Tails USB stick: your documents, browser bookmarks, Wi-Fi passwords, and so on.
Create Persistent Storage
Create and configure a Persistent Storage after starting Tails
Additional Settings
Administration Password
On
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:58 AM
5/7/2025

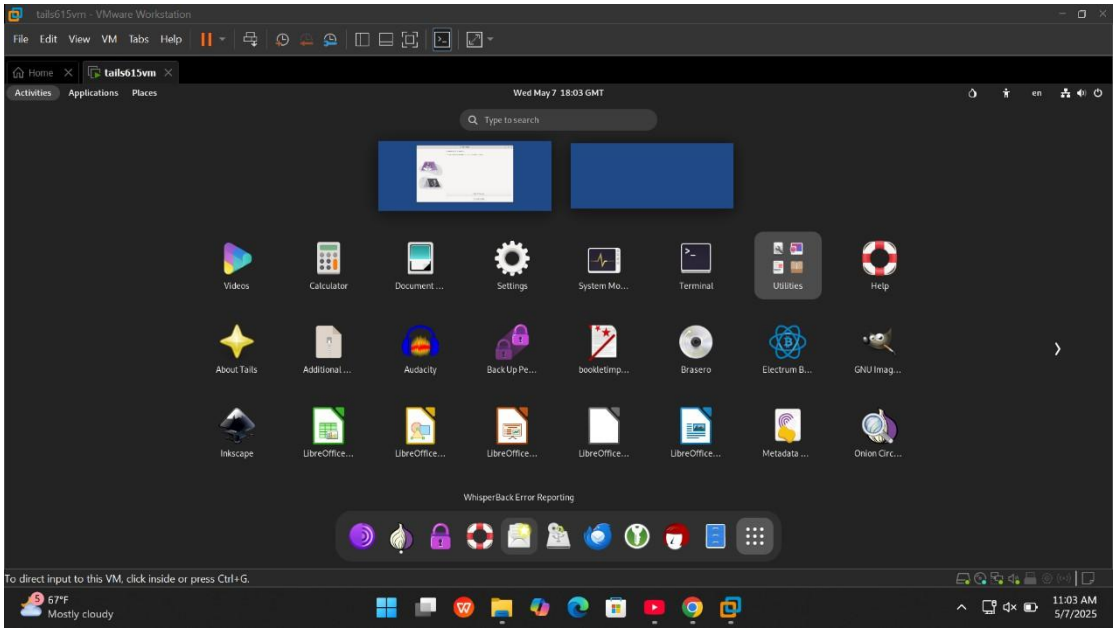

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Tor Connection
Wed May 7 17:59 GMT
en
Tor Connection
Everything you do on the Internet from Tails goes through the Tor network.
Tor encrypts and anonymizes your connection by passing it through 3 relays.
Tor relays are servers operated by different organizations and volunteers around the world.
Connect to Tor automatically
We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.
Hide to my local network that I'm connecting to Tor
You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.
Learn more about how Tails connects to Tor
Connect to Tor
Tor Connection
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:59 AM
5/7/2025

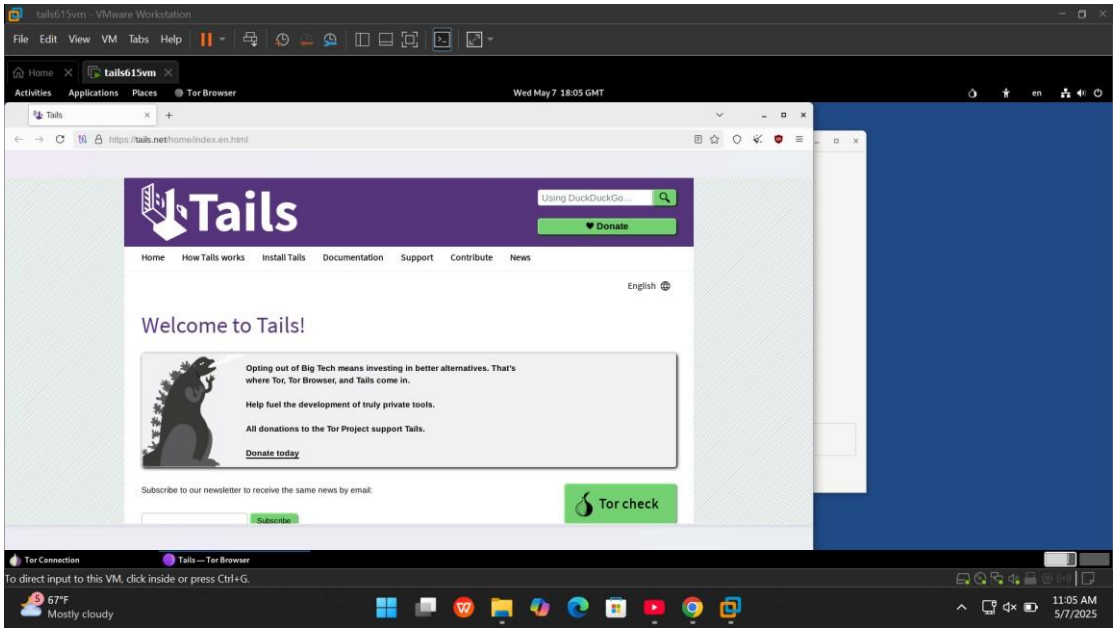

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Tor Connection
Wed May 7 17:59 GMT
en
Tor Connection
Everything you do on the Internet from Tails goes through the Tor network.
Tor encrypts and anonymizes your connection by passing it through 3 relays.
Tor relays are servers operated by different organizations and volunteers around the world.
Connect to Tor automatically
We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.
Configure a Tor bridge
Hide to my local network that I'm connecting to Tor
You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.
Learn more about how Tails connects to Tor
Connect to Tor
Tor Connection
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
10:59 AM
5/7/2025

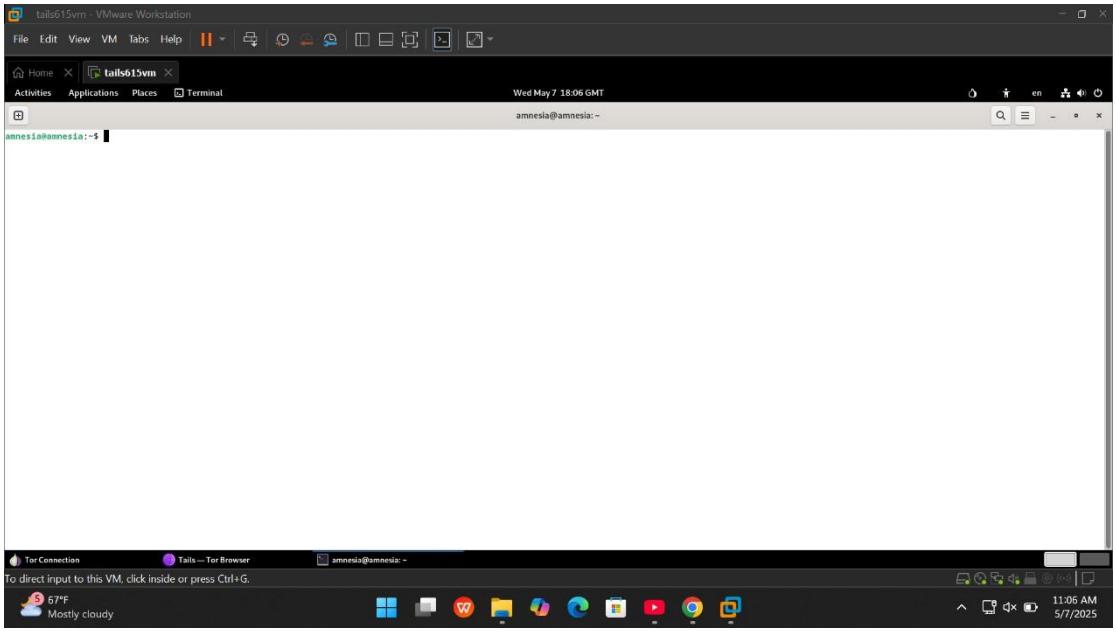

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Tor Connection
Wed May 7 18:00 GMT
en
Tor Connection
Connecting to Tor without bridges...
50%
Tor Connection
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
11:00 AM
5/7/2025

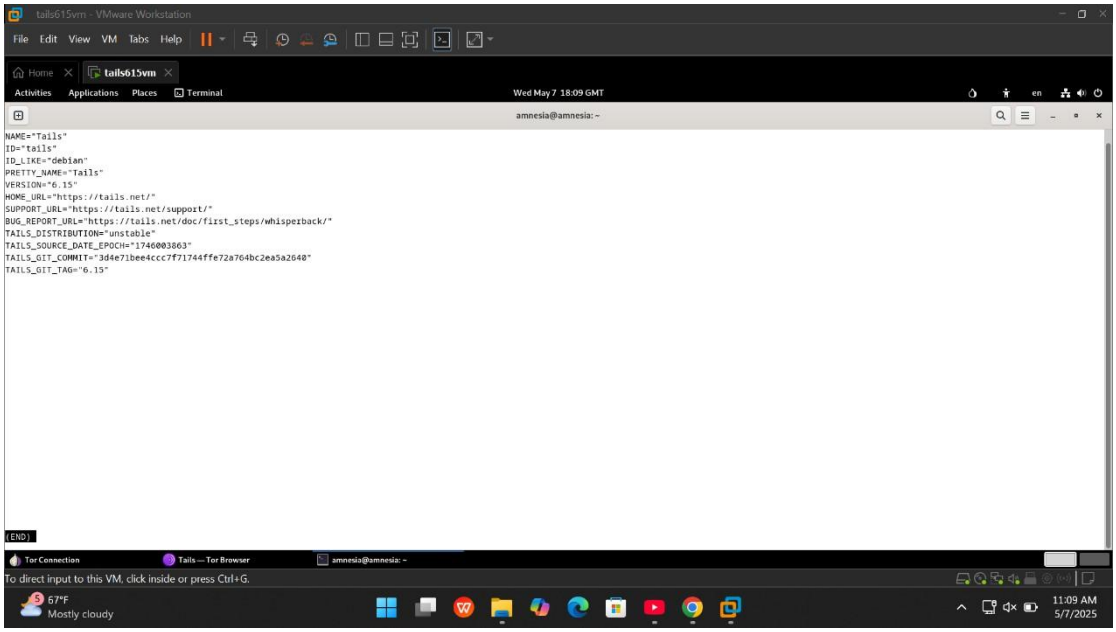

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Tor Connection
Wed May 7 18:00 GMT
en
Tor Connection
Connected to Tor successfully
You can now browse the Internet anonymously and uncensored.
Start Tor Browser
View Tor Circuits
Tor Connection
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
11:00 AM
5/7/2025

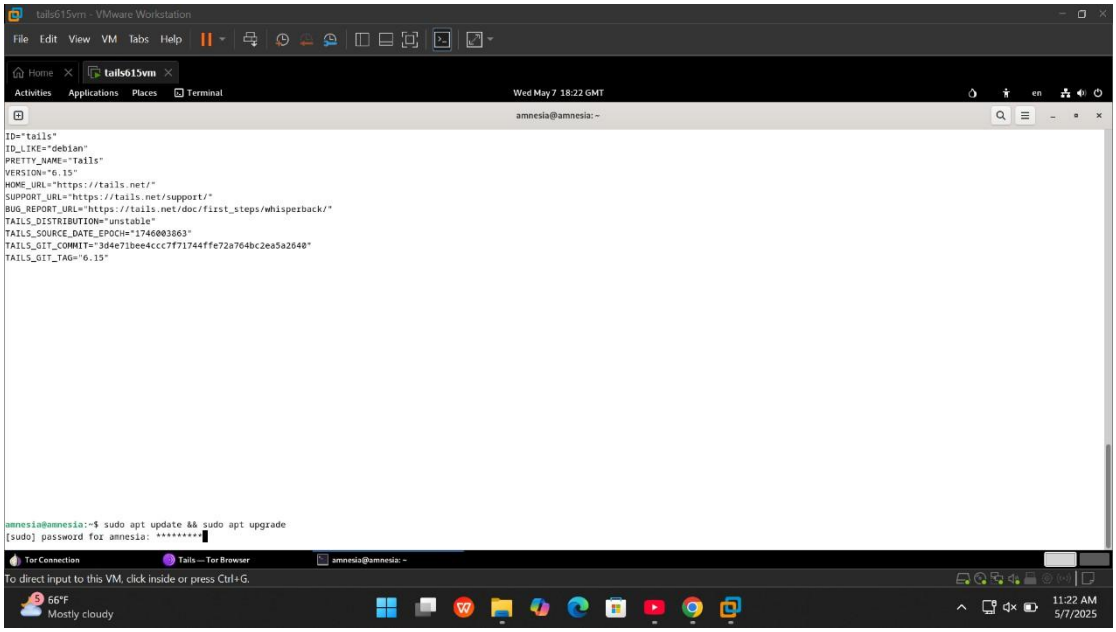

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities
Applications
Places
Tor Connection
Wed May 7 18:02 GMT
en
Favorites
Accessories
Graphics
Internet
Office
Sound & Video
System Tools
Tails
Utilities
Archive Manager
Calculator
Disks
Document Scanner
Document Viewer
Help
System Monitor
Terminal
Unlock VeraCrypt Volumes
Tor Connection
Connected to Tor successfully
You can now browse the Internet anonymously and uncensored.
Start Tor Browser
View Tor Circuits
Tor Connection
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
11:02 AM
5/7/2025

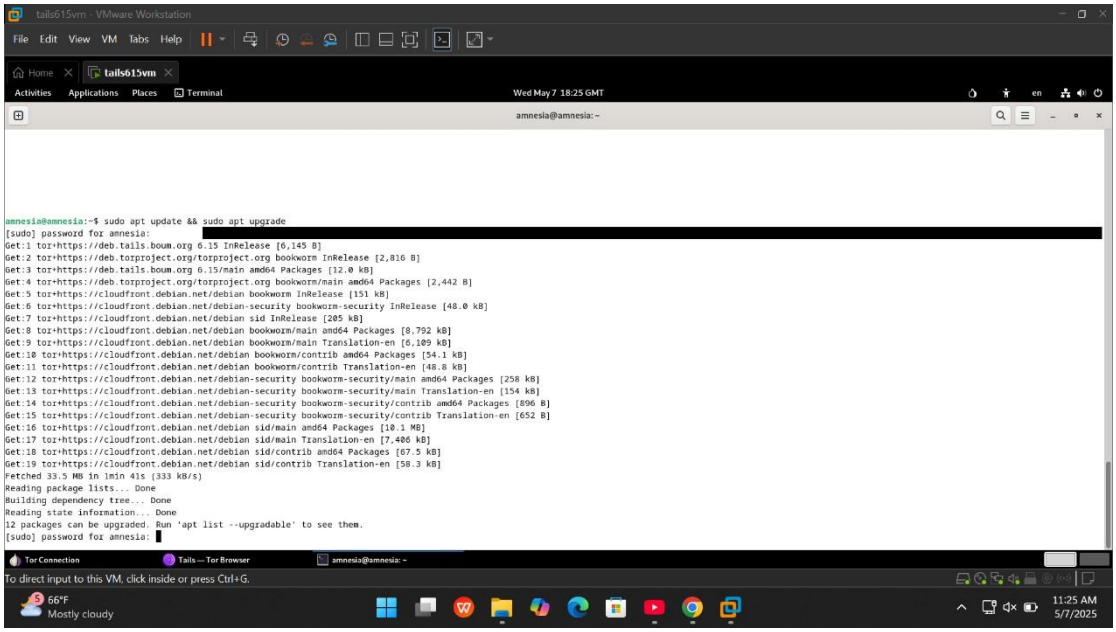

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities
Applications
Places
Wed May 7 18:03 GMT
en
Type to search
Videos
Calculator
Document ...
Settings
System Mo...
Terminal
Utilities
Help
About Tails
Additional ...
Audacity
Back Up Pe...
booklettimp...
Brasero
Electrum B...
GNU Imag...
Inkscape
LibreOffice...
LibreOffice...
LibreOffice...
LibreOffice...
LibreOffice...
Metadata ...
Onion Circ...
WhisperBack Error Reporting
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
11:03 AM
5/7/2025

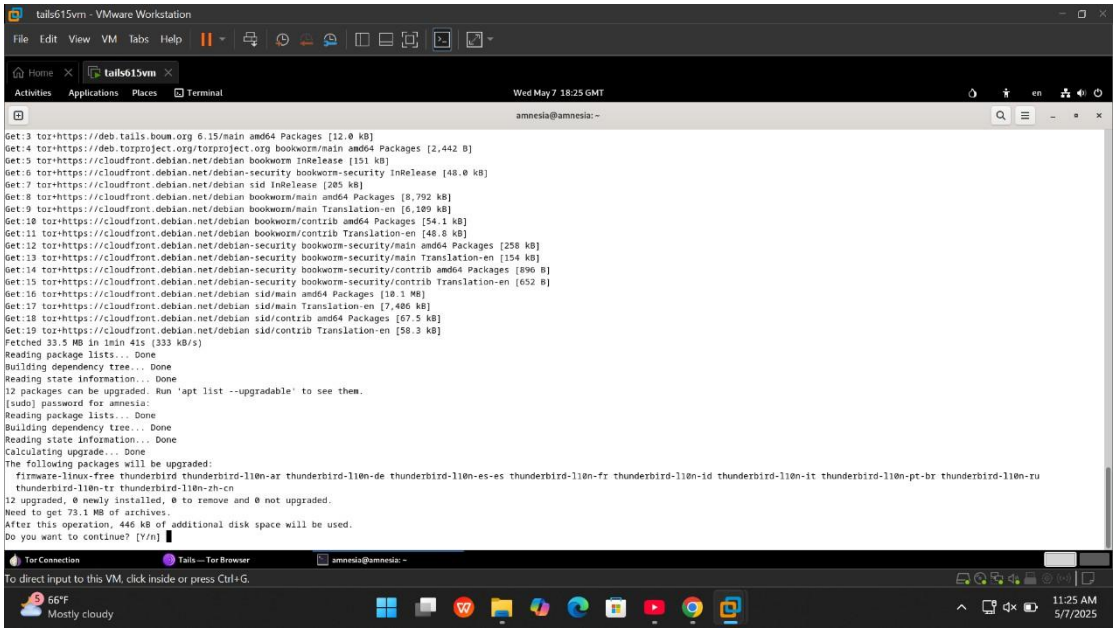

tails615vm - VMware Workstation
File Edit View VM Tabs Help
tails615vm
Activities Applications Places Tor Browser
Wed May 7 18:05 GMT
Tails
https://tails.net/home/index.en.html
Tails
Using DuckDuckGo...
Donate
Home How Tails works Install Tails Documentation Support Contribute News
English
Welcome to Tails!
Opting out of Big Tech means investing in better alternatives. That's where Tor, Tor Browser, and Tails come in.
Help fuel the development of truly private tools.
All donations to the Tor Project support Tails.
Donate today
Subscribe to our newsletter to receive the same news by email:
Subscribe
Tor check
Tor Connection
Tails — Tor Browser
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
11:05 AM
5/7/2025

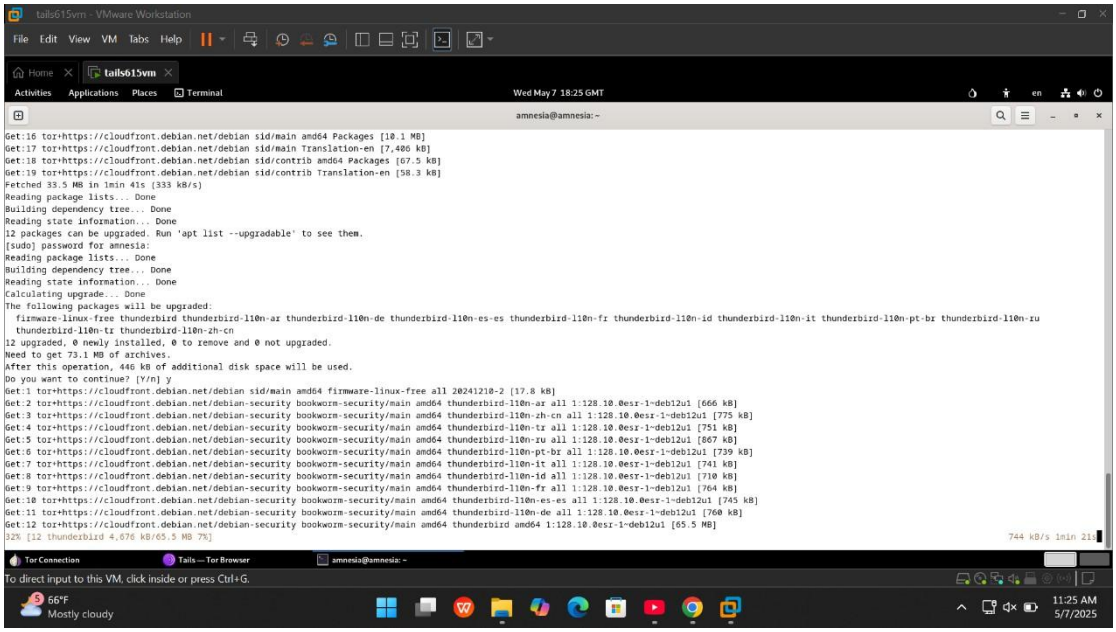

tails615vm - VMware Workstation
File Edit View VM Tabs Help
tails615vm
Activities Applications Places Terminal
Wed May 7 18:06 GMT
amnesia@amnesia: ~
amnesia@amnesia:~$
Tor Connection
Tails — Tor Browser
amnesia@amnesia: ~
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
11:06 AM
5/7/2025

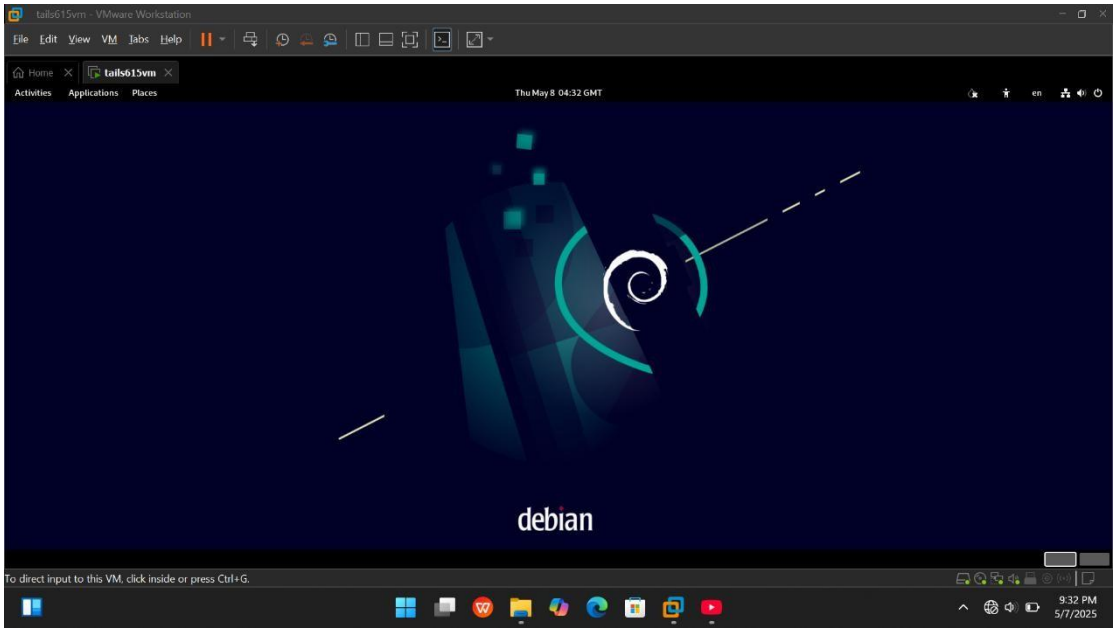

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Terminal
Wed May 7 18:09 GMT
en
amnesia@amnesia: ~
NAME="Tails"
ID="tails"
ID_LIKE="debian"
PRETTY_NAME="Tails"
VERSION="6.15"
HOME_URL="https://tails.net/"
SUPPORT_URL="https://tails.net/support/"
BUG_REPORT_URL="https://tails.net/doc/first_steps/whisperback/"
TAILS_DISTRIBUTION="unstable"
TAILS_SOURCE_DATE_EPOCH="1746003863"
TAILS_GIT_COMMIT="3d4e71bee4ccc7f71744ffe72a764bc2ea5a2640"
TAILS_GIT_TAG="6.15"
(END)
Tor Connection
Tails — Tor Browser
amnesia@amnesia: ~
To direct input to this VM, click inside or press Ctrl+G.
67°F
Mostly cloudy
11:09 AM
5/7/2025

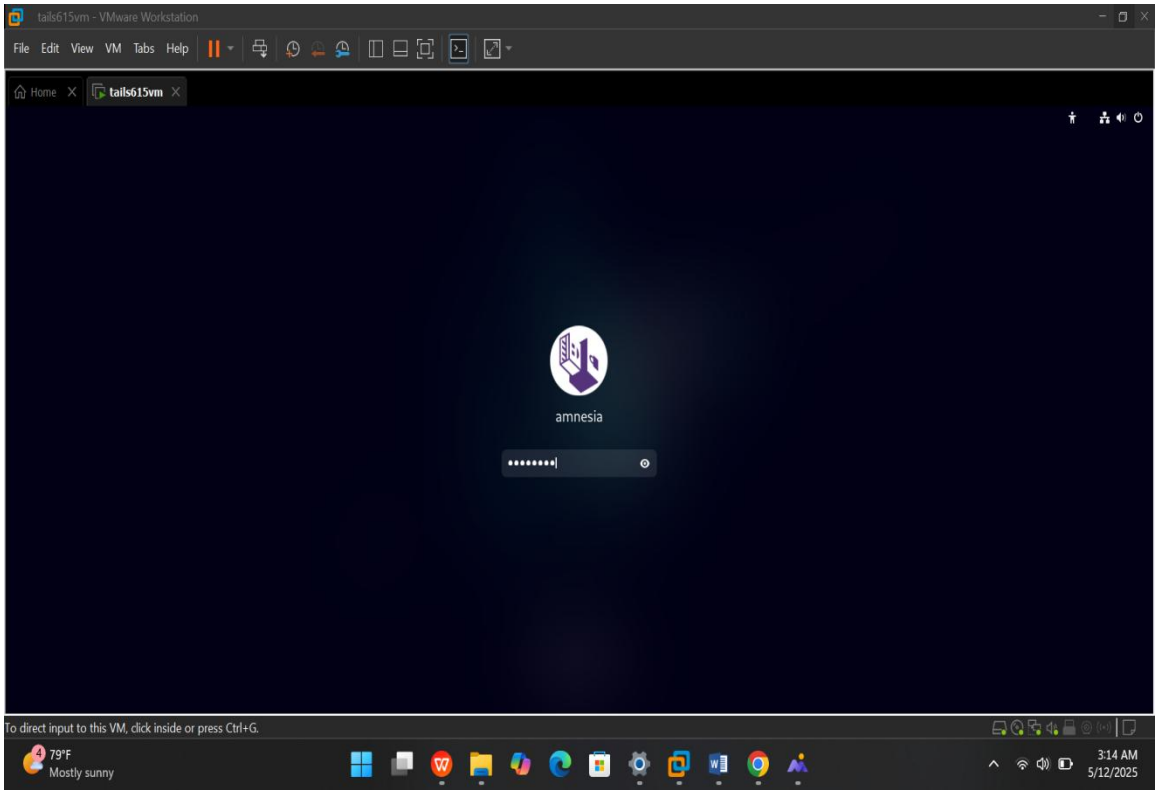

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Terminal
Wed May 7 18:22 GMT
en
amnesia@amnesia: ~
ID="tails"
ID_LIKE="debian"
PRETTY_NAME="Tails"
VERSION="6.15"
HOME_URL="https://tails.net/"
SUPPORT_URL="https://tails.net/support/"
BUG_REPORT_URL="https://tails.net/doc/first_steps/whisperback/"
TAILS_DISTRIBUTION="unstable"
TAILS_SOURCE_DATE_EPOCH="1746003863"
TAILS_GIT_COMMIT="3d4e71bee4ccc7f71744ffe72a764bc2ea5a2640"
TAILS_GIT_TAG="6.15"
amnesia@amnesia:~$ sudo apt update && sudo apt upgrade
[sudo] password for amnesia: *********
Tor Connection
Tails — Tor Browser
amnesia@amnesia: ~
To direct input to this VM, click inside or press Ctrl+G.
66°F
Mostly cloudy
11:22 AM
5/7/2025

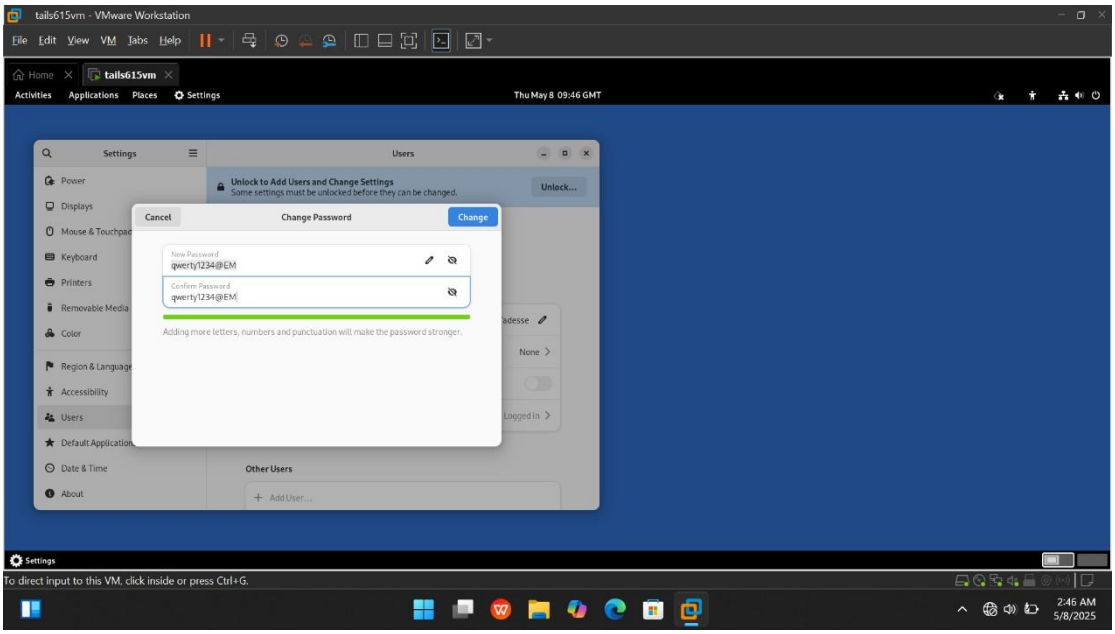

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Terminal
Wed May 7 18:25 GMT
en
amnesia@amnesia: ~
amnesia@amnesia:~$ sudo apt update && sudo apt upgrade
[sudo] password for amnesia:
Get:1 tor+https://deb.tails.boum.org 6.15 InRelease [6,145 B]
Get:2 tor+https://deb.torproject.org/torproject.org bookworm InRelease [2,816 B]
Get:3 tor+https://deb.tails.boum.org 6.15/main amd64 Packages [12.0 kB]
Get:4 tor+https://deb.torproject.org/torproject.org bookworm/main amd64 Packages [2,442 B]
Get:5 tor+https://cloudfront.debian.net/debian bookworm InRelease [151 kB]
Get:6 tor+https://cloudfront.debian.net/debian-security bookworm-security InRelease [48.0 kB]
Get:7 tor+https://cloudfront.debian.net/debian sid InRelease [205 kB]
Get:8 tor+https://cloudfront.debian.net/debian bookworm/main amd64 Packages [8,792 kB]
Get:9 tor+https://cloudfront.debian.net/debian bookworm/main Translation-en [6,109 kB]
Get:10 tor+https://cloudfront.debian.net/debian bookworm/contrib amd64 Packages [54.1 kB]
Get:11 tor+https://cloudfront.debian.net/debian bookworm/contrib Translation-en [48.8 kB]
Get:12 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 Packages [258 kB]
Get:13 tor+https://cloudfront.debian.net/debian-security bookworm-security/main Translation-en [154 kB]
Get:14 tor+https://cloudfront.debian.net/debian-security bookworm-security/contrib amd64 Packages [896 B]
Get:15 tor+https://cloudfront.debian.net/debian-security bookworm-security/contrib Translation-en [652 B]
Get:16 tor+https://cloudfront.debian.net/debian sid/main amd64 Packages [18.1 MB]
Get:17 tor+https://cloudfront.debian.net/debian sid/main Translation-en [7,406 kB]
Get:18 tor+https://cloudfront.debian.net/debian sid/contrib amd64 Packages [67.5 kB]
Get:19 tor+https://cloudfront.debian.net/debian sid/contrib Translation-en [58.3 kB]
Fetched 33.5 MB in 1min 41s (333 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
12 packages can be upgraded. Run 'apt list --upgradable' to see them.
[sudo] password for amnesia:
Tor Connection
Tails — Tor Browser
amnesia@amnesia: ~
To direct input to this VM, click inside or press Ctrl+G.
66°F
Mostly cloudy
11:25 AM
5/7/2025

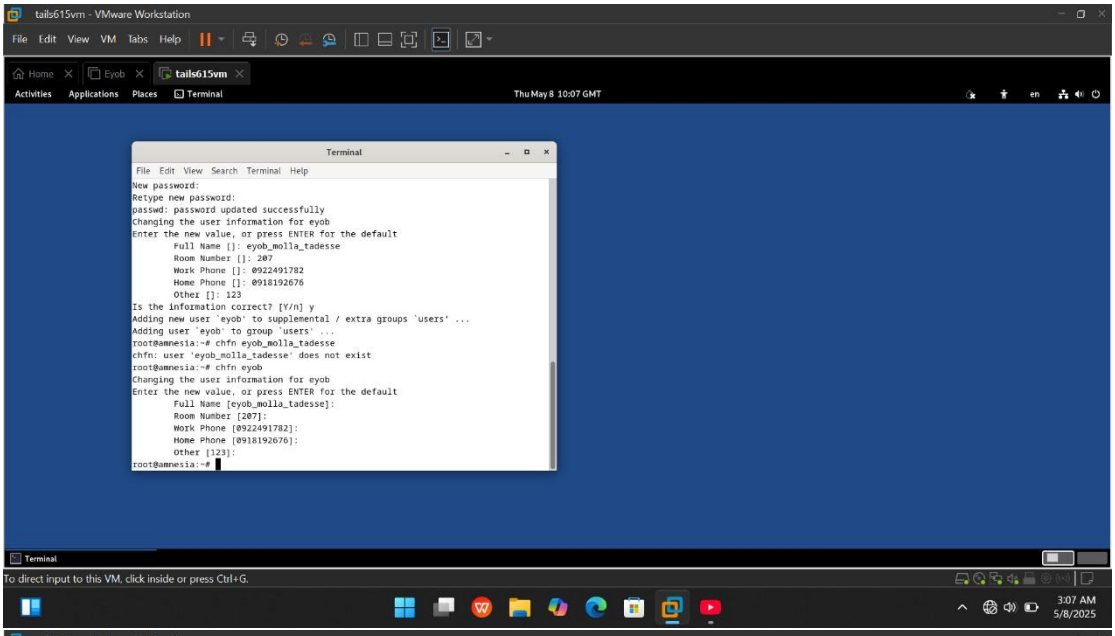

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Terminal
Wed May 7 18:25 GMT
en
amnesia@amnesia: ~
Get:3 tor+https://deb.tails.boum.org 6.15/main amd64 Packages [12.0 kB]
Get:4 tor+https://deb.torproject.org/torproject.org bookworm/main amd64 Packages [2,442 B]
Get:5 tor+https://cloudfront.debian.net/debian bookworm InRelease [151 kB]
Get:6 tor+https://cloudfront.debian.net/debian-security bookworm-security InRelease [48.0 kB]
Get:7 tor+https://cloudfront.debian.net/debian sid InRelease [205 kB]
Get:8 tor+https://cloudfront.debian.net/debian bookworm/main amd64 Packages [8,792 kB]
Get:9 tor+https://cloudfront.debian.net/debian bookworm/main Translation-en [6,109 kB]
Get:10 tor+https://cloudfront.debian.net/debian bookworm/contrib amd64 Packages [54.1 kB]
Get:11 tor+https://cloudfront.debian.net/debian bookworm/contrib Translation-en [48.8 kB]
Get:12 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 Packages [258 kB]
Get:13 tor+https://cloudfront.debian.net/debian-security bookworm-security/main Translation-en [154 kB]
Get:14 tor+https://cloudfront.debian.net/debian-security bookworm-security/contrib amd64 Packages [896 B]
Get:15 tor+https://cloudfront.debian.net/debian-security bookworm-security/contrib Translation-en [652 B]
Get:16 tor+https://cloudfront.debian.net/debian sid/main amd64 Packages [18.1 MB]
Get:17 tor+https://cloudfront.debian.net/debian sid/main Translation-en [7,406 kB]
Get:18 tor+https://cloudfront.debian.net/debian sid/contrib amd64 Packages [67.5 kB]
Get:19 tor+https://cloudfront.debian.net/debian sid/contrib Translation-en [58.3 kB]
Fetched 33.5 MB in 1min 41s (333 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
12 packages can be upgraded. Run 'apt list --upgradable' to see them.
[sudo] password for amnesia:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
firmware-linux-free thunderbird thunderbird-l10n-ar thunderbird-l10n-de thunderbird-l10n-es-es thunderbird-l10n-fr thunderbird-l10n-id thunderbird-l10n-it thunderbird-l10n-pt-br thunderbird-l10n-ru
thunderbird-l10n-tr thunderbird-l10n-zh-cn
12 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 73.1 MB of archives.
After this operation, 446 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Tor Connection
Tails — Tor Browser
amnesia@amnesia: ~
To direct input to this VM, click inside or press Ctrl+G.
66°F
Mostly cloudy
11:25 AM
5/7/2025

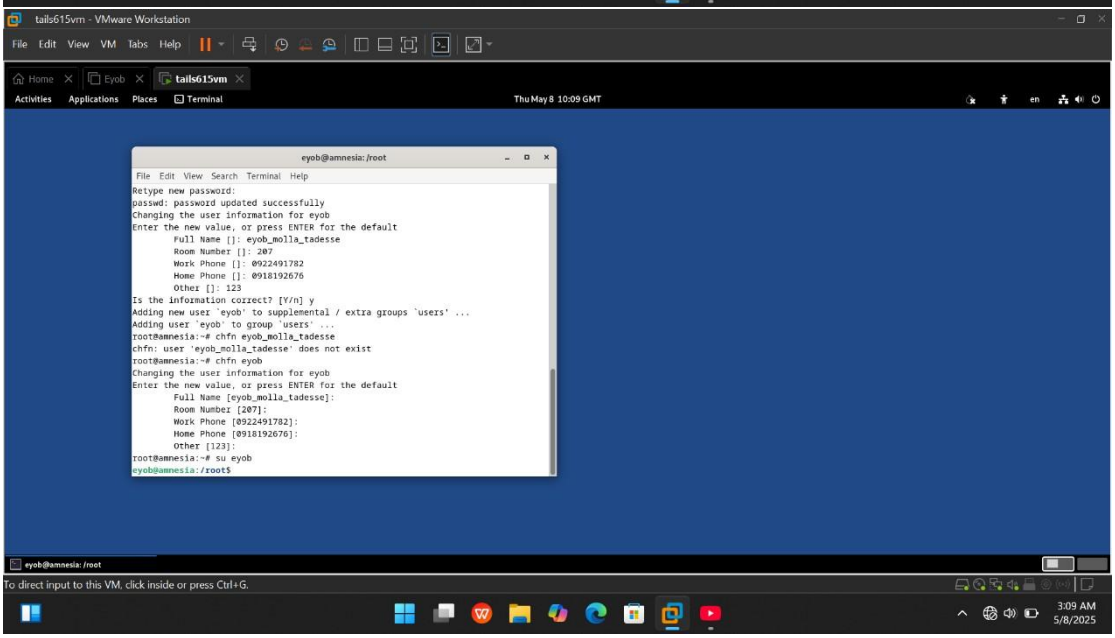

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Terminal
Wed May 7 18:25 GMT
en
amnesia@amnesia: ~
Get:16 tor+https://cloudfront.debian.net/debian sid/main amd64 Packages [10.1 MB]
Get:17 tor+https://cloudfront.debian.net/debian sid/main Translation-en [7,406 kB]
Get:18 tor+https://cloudfront.debian.net/debian sid/contrib amd64 Packages [67.5 kB]
Get:19 tor+https://cloudfront.debian.net/debian sid/contrib Translation-en [58.3 kB]
Fetched 33.5 MB in 1min 41s (333 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
12 packages can be upgraded. Run 'apt list --upgradable' to see them.
[sudo] password for amnesia:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
firmware-linux-free thunderbird thunderbird-l10n-ar thunderbird-l10n-de thunderbird-l10n-es-es thunderbird-l10n-fr thunderbird-l10n-id thunderbird-l10n-it thunderbird-l10n-pt-br thunderbird-l10n-ru
thunderbird-l10n-tr thunderbird-l10n-zh-cn
12 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 73.1 MB of archives.
After this operation, 446 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 tor+https://cloudfront.debian.net/debian sid/main amd64 firmware-linux-free all 20241210-2 [17.8 kB]
Get:2 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-ar all 1:128.10.0esr-1~deb12u1 [666 kB]
Get:3 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-zh-cn all 1:128.10.0esr-1~deb12u1 [775 kB]
Get:4 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-tr all 1:128.10.0esr-1~deb12u1 [751 kB]
Get:5 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-ru all 1:128.10.0esr-1~deb12u1 [867 kB]
Get:6 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-pt-br all 1:128.10.0esr-1~deb12u1 [739 kB]
Get:7 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-it all 1:128.10.0esr-1~deb12u1 [741 kB]
Get:8 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-id all 1:128.10.0esr-1~deb12u1 [710 kB]
Get:9 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-fr all 1:128.10.0esr-1~deb12u1 [764 kB]
Get:10 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-es-es all 1:128.10.0esr-1~deb12u1 [745 kB]
Get:11 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird-l10n-de all 1:128.10.0esr-1~deb12u1 [760 kB]
Get:12 tor+https://cloudfront.debian.net/debian-security bookworm-security/main amd64 thunderbird amd64 1:128.10.0esr-1~deb12u1 [65.5 MB]
32% [12 thunderbird 4,676 kB/65.5 MB 7%]
744 kB/s 1min 21s
Tor Connection
Tails — Tor Browser
amnesia@amnesia: ~
To direct input to this VM, click inside or press Ctrl+G.
66°F
Mostly cloudy
11:25 AM
5/7/2025

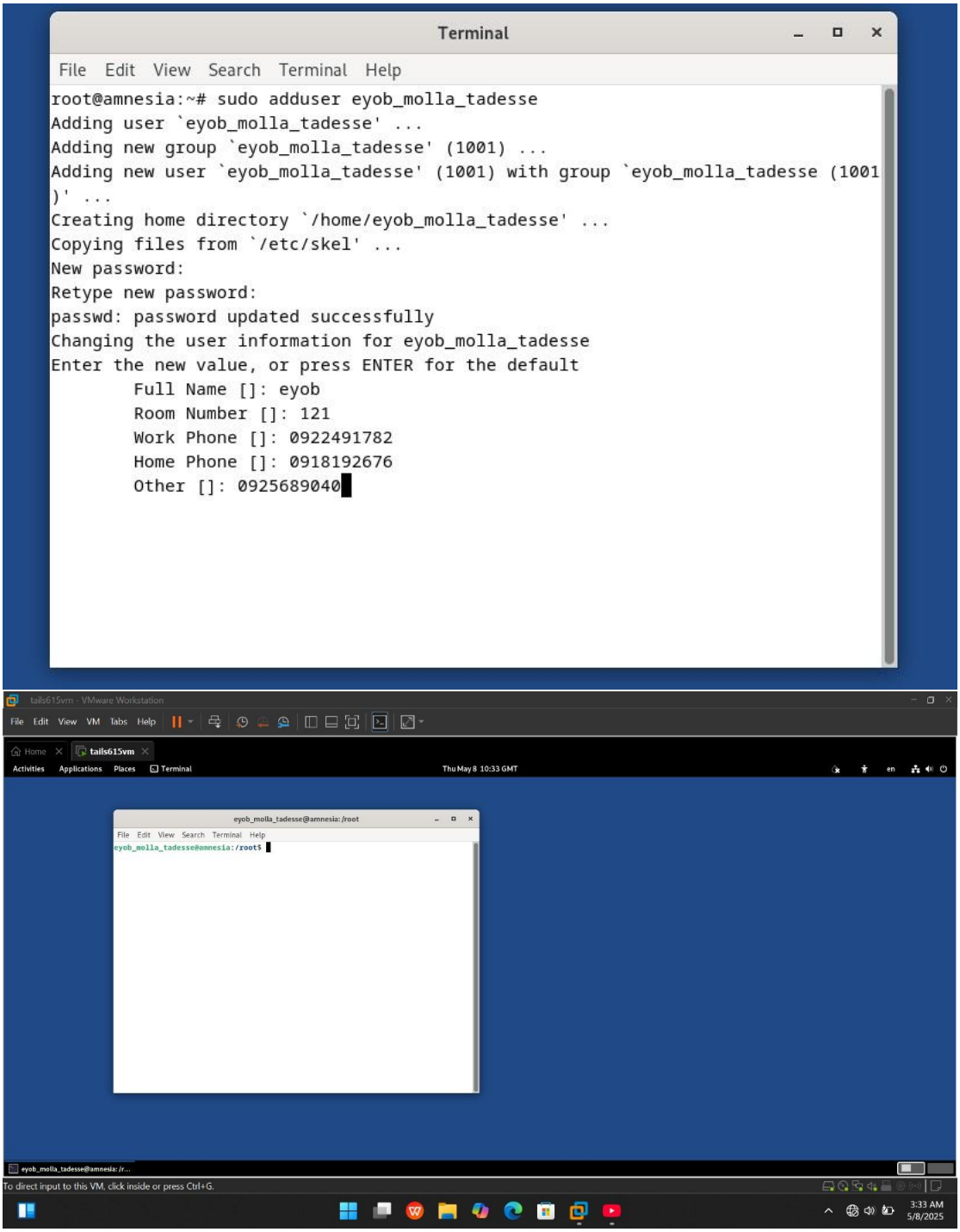

tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places
Thu May 8 04:32 GMT
en
debian
To direct input to this VM, click inside or press Ctrl+G.
9:32 PM
5/7/2025


tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
amnesia
To direct input to this VM, click inside or press Ctrl+G.
79°F
Mostly sunny
3:14 AM
5/12/2025


tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
tails615vm
Activities Applications Places Settings
Thu May 8 09:46 GMT
Settings
Users
Unlock to Add Users and Change Settings
Some settings must be unlocked before they can be changed.
Unlock...
Cancel
Change Password
Change
New Password
qwerty1234@EM
Confirm Password
qwerty1234@EM
Adding more letters, numbers and punctuation will make the password stronger.
Power
Displays
Keyboard
Printers
Removable Media
Color
Region & Language
Accessibility
Users
Default Applications
Date & Time
About
Other Users
Add User...
None
Logged In
To direct input to this VM, click inside or press Ctrl+G.
2:46 AM
5/8/2025


tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
Eyob
tails615vm
Activities
Applications
Places
Terminal
Thu May 8 10:07 GMT
en
Terminal
File Edit View Search Terminal Help
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for eyob
Enter the new value, or press ENTER for the default
Full Name []: eyob_molla_tadesse
Room Number []: 207
Work Phone []: 0922491782
Home Phone []: 0918192676
Other []: 123
Is the information correct? [Y/n] y
Adding new user `eyob' to supplemental / extra groups `users' ...
Adding user `eyob' to group `users' ...
root@amnesia:~# chfn eyob_molla_tadesse
chfn: user 'eyob_molla_tadesse' does not exist
root@amnesia:~# chfn eyob
Changing the user information for eyob
Enter the new value, or press ENTER for the default
Full Name [eyob_molla_tadesse]:
Room Number [207]:
Work Phone [0922491782]:
Home Phone [0918192676]:
Other [123]:
root@amnesia:~#
Terminal
To direct input to this VM, click inside or press Ctrl+G.
3:07 AM
5/8/2025


tails615vm - VMware Workstation
File Edit View VM Tabs Help
Home
Eyob
tails615vm
Activities
Applications
Places
Terminal
Thu May 8 10:09 GMT
en
eyob@amnesia: /root
File Edit View Search Terminal Help
Retype new password:
passwd: password updated successfully
Changing the user information for eyob
Enter the new value, or press ENTER for the default
Full Name []: eyob_molla_tadesse
Room Number []: 207
Work Phone []: 0922491782
Home Phone []: 0918192676
Other []: 123
Is the information correct? [Y/n] y
Adding new user `eyob' to supplemental / extra groups `users' ...
Adding user `eyob' to group `users' ...
root@amnesia:~# chfn eyob_molla_tadesse
chfn: user 'eyob_molla_tadesse' does not exist
root@amnesia:~# chfn eyob
Changing the user information for eyob
Enter the new value, or press ENTER for the default
Full Name [eyob_molla_tadesse]:
Room Number [207]:
Work Phone [0922491782]:
Home Phone [0918192676]:
Other [123]:
root@amnesia:~# su eyob
eyob@amnesia:/root$
eyob@amnesia: /root
To direct input to this VM, click inside or press Ctrl+G.
3:09 AM
5/8/2025



NB:-

Tails OS is a privacy-focused Linux distribution that runs entirely from a USB stick or DVD.
It uses the system's RAM (not the hard drive) for all operations, making it "amnesic."
When I shut down and start , all data stored in RAM is automatically wiped, erasing any trace of the session so everything I made change above will be erased after I restart.

Issues faced during installing tails OS

1. VMware Compatibility Issues

A. Unsupported VMware Version

Problem: Older versions of VMware may not fully support Tails OS, leading to installation failures or system instability.

Symptoms:

- Installation process freezes or crashes unexpectedly.
- Certain hardware components, such as network adapters or storage controllers, may not function correctly.

Solution:

- Ensure you're using the latest version of VMware Workstation or Player.
- Check the Tails documentation for any specific VMware version recommendations.

B. Incorrect Guest Operating System Selection

Problem: Selecting the wrong guest OS type during VM setup can lead to improper hardware emulation.

Symptoms:

- Tails installer fails to boot or crashes during installation.
- Post-installation performance issues, such as slow disk I/O or unresponsive network interfaces.

Solution:

- During VM creation, select "Linux" as the guest operating system.
- If available, choose "Debian" as the specific version.
- Ensure the system architecture (32-bit or 64-bit) matches your installation medium.

C. Virtual Hardware Configuration Problems

Problem: Inadequate allocation of virtual resources can hinder the installation process.

Symptoms:

- Installation stalls or crashes during package extraction or kernel compilation.

- "Out of memory" errors or failure to detect available disk space.

Solution:

- Allocate at least 1 GB of RAM for smoother installation and operation.
- Assign at least 10 GB of virtual hard drive space, especially if additional packages or graphical environments will be installed later.

2. Booting and USB Issues

A. Booting from USB in VMware

Problem: VMware may not recognize USB devices correctly, preventing Tails from booting.

Solution:

- Create a VM, delete the hard drive added in the wizard, and then add the USB as an IDE Drive.
- Ensure that the USB device is properly connected and recognized by the host system.

3. Networking Issue

A. No Network Interface Detected

Problem: Tails may fail to detect VMware's default virtual network adapters, leading to a lack of network connectivity.

Symptoms:

- Network interface not listed during the installation’s network configuration step.
- Post-installation, ifconfig shows no network interfaces or the available interface does not connect to the network.

Solution:

- Ensure the virtual machine is set to use the correct network adapter type. VMware typically supports VMXNET or E1000 virtual NICs for Tails OS. The E1000 adapter is known for its compatibility with a wide range of operating systems.
- If the network adapter is not detected, manually configure the network interface using Tails' installer or via the terminal after installation.

- Verify that the VMware network adapter is correctly set up and that the host machine’s network settings are configured properly to pass traffic through to the virtual machine.

4. Display and Graphics Issues

A. Display Color Mode Mismatch

Problem: A mismatch between the virtual machine's display settings and the guest operating system's capabilities can cause display issues.

Symptoms:

- Error messages related to color depth, such as "The virtual machine window is optimized to work in 32-bit color mode but the virtual display is currently set to 24-bit."

Solution:

- Adjust the virtual machine's display settings to match the guest OS's capabilities.
- If using a Linux-based guest OS like Tails, ensure that the display settings are compatible with the guest's requirements.

File system support

Supported Filesystems in Tails OS

1. ext4 (Live System)

- **Usage**: The live operating system runs from an ext4 partition.
- **Why ext4?**: Ext4 is a robust, journaling filesystem native to Linux, offering reliability and efficiency.

2. Encrypted ext4 (Persistent Storage)

- **Usage**: For storing persistent data across sessions, Tails uses an encrypted ext4 partition secured with LUKS and dm-crypt.
- **Why Encrypted ext4?**: It provides strong encryption for sensitive data while maintaining compatibility with Linux systems.

3. FAT32 (USB Drive)

- **Usage**: The USB drive containing Tails is typically formatted with FAT32.
- **Why FAT32?**: Ensures compatibility across various operating systems, facilitating the creation and maintenance of the Tails live system.

Unsupported or Not Recommended Filesystems

1. NTFS

- **Why Not Recommended?**: NTFS is a proprietary filesystem developed by Microsoft. Its support in Linux is available but not optimal, and it lacks features like journaling, which are crucial for system integrity.

2. exFAT

- **Why Not Recommended?**: exFAT is designed for flash drives and SD cards. While supported in Linux, it's not ideal for system installations due to potential reliability issues and lack of journaling.

3. Btrfs

- **Why Not Recommended?**: Btrfs is an advanced filesystem with features like snapshots and compression. However, it's considered less stable and mature compared to ext4, making it unsuitable for the critical environment of Tails.

4. ZFS

- **Why Not Recommended?**: ZFS is a high-performance filesystem with advanced features, but it has licensing issues and is not natively supported in Linux distributions like Tails.

5. HFS+ and APFS

- **Why Not Recommended?**: These are Apple filesystems. Tails is not designed to interact with macOS-specific filesystems, leading to potential compatibility and stability issues.

Advantage of tails OS

1. Enhanced Privacy

- **Tor Network Integration:** The cornerstone of Tails' privacy is its seamless integration with the Tor network. All your internet traffic gets routed through a series of relays, obfuscating your origin and making it incredibly difficult to track your online activity. This protects you from potential surveillance by governments, corporations, or even hackers.
- **Pre-configured Anonymity Tools:** Tails comes pre-loaded with various anonymity tools right out of the box. This includes the Tor Browser, which is specifically designed to function within the Tor network for maximum anonymity. Additionally, tools like "Disconnection Keeper" automatically disconnect your internet connection if the Tor network loses connection, preventing accidental leaks of your real IP address.
- **Fingerprint Reduction:** Modern web browsers can reveal a lot about your system through "fingerprinting" techniques. Tails employs various countermeasures to

reduce your browser fingerprint, making it harder to identify your unique system configuration and differentiate you from other users.

2. Improved Security

- **Pre-installed Security Applications:** Tails goes beyond anonymity by providing a robust security suite. This includes tools like "GnuPG" for encrypting emails and files, "LUKS" for encrypting entire hard drives (on persistent storage), and "KeePassXC" for managing strong and unique passwords for all your online accounts.
- **Amnesiac Behavior:** One of Tails' most distinctive features is its "amnesiac" nature. By default, Tails doesn't store any data on the local hard drive. Once you shut down the system, everything you've done – browsing history, downloads, files created is wiped clean. This significantly reduces the risk of malware infection or data breaches, especially when using a public or untrusted computer.
- **Regular Security Updates:** The Tails development team is committed to keeping the operating system secure by releasing regular updates that patch vulnerabilities and address potential security risks.

3. Portability and Discreet Use

- **USB Drive Convenience:** Tails runs entirely from a live USB drive. This makes it incredibly portable and allows you to use it on any computer without leaving a trace on the local storage. You can carry your anonymity and security tools in your pocket, ready to be deployed whenever needed.
- **No Installation Required:** There's no need to install Tails on your computer's hard drive. Simply boot your computer from the USB drive, and you're ready to go. This eliminates the risk of modifying your primary operating system or leaving any residual files behind.

4. Free and Open-Source

- **Cost-Effective Solution:** Tails is completely free to download and use. There are no hidden costs or subscriptions involved.
- **Transparency and Community Support:** Being open-source means the underlying code of Tails is publicly available for anyone to inspect. This fosters transparency and allows the security community to collaborate on improvements and identify potential vulnerabilities. Additionally, a vibrant community of Tails users and developers exists online, offering support and resources for those encountering any difficulties.

Disadvantage of tails OS

- Limited Usability for Daily Tasks Tails is not designed for regular use like Windows or macOS. It's meant for specific privacy-focused tasks (e.g., whistleblowing, journalism, activism). Lack of persistent storage (by default) means you must reconfigure settings and reinstall software each session.
- Slow Performance Runs from a USB drive, which is slower than an SSD/HDD. Encryption and Tor routing add latency, making browsing and downloads slower.

- No Native Support for Some Hardware Limited drivers for Wi-Fi, GPU, and peripherals (some may not work). Issues with newer MacBooks and certain hardware.
- . Tor Dependency (Can Be a Weakness) All traffic goes through Tor, which can be slow or blocked in some countries. Some websites block Tor exit nodes, limiting access.
- No Persistent User Accounts By default, all data is wiped after shutdown (unless manually saved to an encrypted Persistent Storage). Installing software or saving files requires extra steps.
- Not Ideal for High-Risk Scenarios Against Powerful Adversaries While Tails is strong against surveillance, it may not protect against advanced adversaries (e.g., nation-state actors with zero-day exploits). If compromised while running, forensic traces might remain on RAM (though unlikely).
- Learning Curve Requires basic Linux knowledge for advanced customization. Some features (like Persistent Storage setup) may confuse beginners.
- Limited Software Availability Only includes pre-installed privacy tools (e.g., Tor Browser, KeePassXC, LibreOffice). Installing additional software is possible but cumbersome.
- Susceptibility to Evil Maid Attacks If an attacker gains physical access to your Tails USB, they could modify it (though Verified Boot helps mitigate this).
- Not Fully Anonymous by Default User mistakes (e.g., logging into personal accounts, using non-Tor connections) can break anonymity.

conclusion

Tails OS (The Amnesic Incognito Live System) is a uniquely designed Linux distribution aimed at preserving user privacy, maintaining anonymity, and protecting against surveillance and censorship. Built on top of Debian, Tails is a live operating system that runs entirely from removable media such as a USB stick or DVD, and deliberately avoids interacting with the computer's internal storage. This ensures that no traces of user activity are left behind after the session ends, aligning perfectly with its core philosophy of amnesia and privacy.

The installation process of Tails is intentionally different from traditional Linux distributions. It is not installed in the typical sense but is instead written to a bootable USB device using tools like Etcher or the Tails Installer.

Tails also supports specific filesystems in line with its security goals. The live environment primarily runs in RAM and utilizes the SquashFS (Squashed File System) format for its compressed read-only system files, ensuring integrity and preventing modification during use. When persistent storage is enabled, it uses ext4 with LUKS encryption. This setup ensures both performance and security—ext4 being a stable, journaled filesystem and LUKS offering full-disk encryption to protect against data recovery or unauthorized access. However, users are limited to the filesystems and

formats explicitly supported for encrypted volumes and temporary file handling, reinforcing Tails' minimal attack surface.

Tails comes pre-equipped with a collection of privacy and security tools, including the **Tor Browser**, **KeePassXC**, **Electrum Bitcoin Wallet**, and **MAT2** (Metadata Anonymization Toolkit). All network connections are automatically routed through the **Tor network**, and any attempt to bypass this configuration is blocked. This guarantees that the user's IP address and online activities remain hidden. These tools are configured to be secure by default, minimizing user error and maximizing protection against threats such as tracking, malware, or surveillance.

Running Tails on virtual machines such as **VMware** provides a useful way for users to test or become familiar with the operating system in a controlled environment. The process involves downloading the official ISO, creating a new virtual machine with suitable RAM (2 GB minimum), and booting the ISO as a live session. However, while the interface and tools work properly, virtualization does not offer the full security that Tails is designed for. A virtual machine shares resources with the host system, which may log activity, cache memory data, or expose the Tails environment to potential compromise. For this reason, virtualized usage should be limited to learning and experimentation, and not for real-world anonymous or secure communication.

Future Outlook and Recommendations for Tails OS

As digital privacy becomes an increasingly urgent concern in the modern world, the significance of projects like Tails OS continues to grow. With expanding surveillance technologies, data collection practices, and censorship across many regions, Tails remains one of the most critical tools for individuals seeking to preserve anonymity and resist monitoring. Its role in journalism, activism, whistleblowing, and privacy advocacy is already well-established, and the future holds both challenges and opportunities for its evolution.

From a technical perspective, future development of Tails OS should continue to focus on increasing hardware compatibility and usability without compromising its core principles. Improvements in support for modern hardware drivers, such as Wi-Fi cards, GPUs, and touchpads, would enhance user experience, especially as newer systems become the norm. Additionally, better integration with UEFI and Secure Boot—now standard on most systems—would further reduce the friction of using Tails on current hardware.

Security is always evolving, and Tails must adapt to emerging threats. Enhancements such as automatic updates over Tor, improved sandboxing of applications, and integration with next-generation anonymization networks could further reinforce its resilience. As more users adopt privacy-focused practices, there is also a need for enhanced user education within Tails itself—perhaps through interactive tutorials or built-in threat modeling guidance—to ensure users understand how to use the system securely.

On the usability and accessibility front, simplifying the onboarding process for nontechnical users is critical. Despite its powerful privacy tools, Tails can be intimidating for beginners. Streamlined installation steps, friendlier interface elements, and clearer documentation could help bridge this gap and encourage broader adoption. Providing language support for underrepresented regions could also empower users in countries where digital repression is high.

In terms of recommendations, users should be encouraged to:

1. **Run Tails from a USB on trusted hardware** rather than in a virtual machine when privacy is a real concern.
2. **Regularly update** to the latest version, as security patches are essential in a system designed to resist surveillance.
3. **Understand their threat model** and use Tails accordingly—knowing when and how to use persistence, what information to store, and how to manage identity separation online.
4. **Engage with the Tails community**, provide feedback, and contribute to its development, especially if they have technical skills or localized knowledge.

Finally , Tails should continue to work closely with organizations like the **Tor Project**, **EFF**, and other open-source security communities. These collaborations can help Tails stay aligned with broader privacy initiatives and ensure it remains a trusted, cuttingedge tool in the fight for digital freedom.

About virtualization

What is virtualization?

Virtualization is the creation of a virtual version of an actual piece of technology, such as an operating system (OS), a server, a storage device or a network resource. Virtualization uses software that simulates hardware functionality to create a virtual system.

This practice lets IT organizations run multiple OS, more than one virtual system and various applications on a single server. The benefits of virtualization include greater efficiency and economies of scale.

OS virtualization uses software that enables a piece of hardware to run multiple operating system images at the same time. The technology got its start on mainframes decades ago to save on expensive processing power.

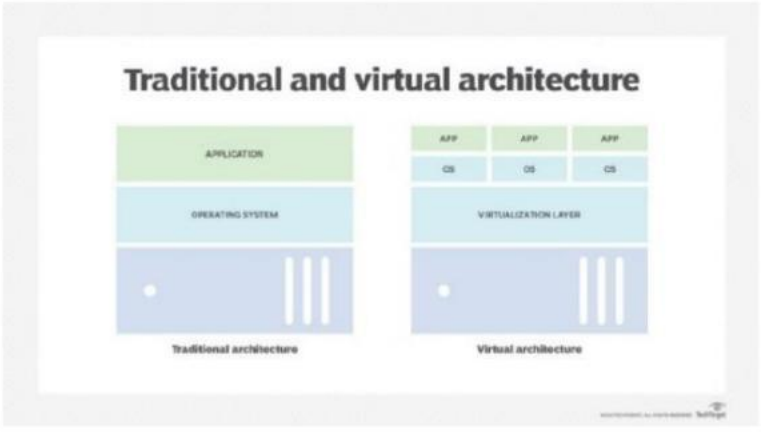
Why Use Virtualization?

1. Resource Optimization: Virtualization allows multiple workloads to run on a single physical machine, maximizing hardware usage and reducing costs associated with purchasing and maintaining physical servers.
2. Scalability: It makes it easier to scale resources up or down based on demand, facilitating rapid deployment of applications and services.

3. Isolation: Virtual machines (VMs) are isolated from one another, enhancing security and stability. If one VM fails, it does not affect others.
4. Simplified Management: Centralized management tools allow for easier monitoring, backup, and disaster recovery processes.
5. Testing and Development: Virtualization provides safe environments for testing applications without affecting the production system, allowing for quick iterations and experimentation.

How virtualization works?

Virtualization technology abstracts an application, guest operating system or data storage away from its underlying hardware or software.
Organizations that divide their hard drives into different partitions already engage in virtualization. A partition is the logical division of a hard disk drive that, in effect, creates two 46 separate hard drives. Server virtualization is a key use of virtualization technology. It uses a software layer called a hypervisor to emulate the underlying hardware. This includes the central processing units (CPU's) memory, input/output and network traffic. Hypervisors take the physical resources and separate them for the virtual environment.
They can sit on top of an OS or be directly installed onto the hardware. Xen hypervisor is an open source software program that manages the low-level interactions that occur between virtual machines (VMs) and physical hardware. It enables the simultaneous creation, execution and management of various
VMs in one physical environment. With the help of the hypervisor, the guest OS, which normally interacts with true hardware, does so with a software emulation of that hardware.
Although OS running on true hardware often outperform those running on virtual systems, most guest OS and applications don't fully use the underlying hardware. Virtualization removes dependency on a given hardware platform, creating greater flexibility, control and isolation for environments. Plus, virtualization has spread beyond servers to include applications, networks, data management and desktops.



A side-by-side view of a traditional vs. virtual architecture shows their differences.

The virtualization process follows these steps:

1. Hypervisors detach physical resources from their physical environments.

2. Resources are taken from the physical environment and divided among various virtual environments.
3. System users work with and perform computations within the virtual environment. Once the virtual environment is running, a user or program can send an instruction that requires extra resources from the physical environment. In response, the hypervisor relays the message to the physical machine and stores the changes. The virtual environment is often referred to as a guest machine or virtual machine. The VM acts like a single data file that can be transferred from one computer to another and opened in both. It should perform the same way on every computer.

Types of virtualizations

Hypervisors are the technology that enables virtual abstraction. Type 1, the most common hypervisor, sits directly on bare metal and virtualizes the hardware platform. KVM virtualization is an open source, Linux kernel-based hypervisor that provides Type 1 virtualization benefits. A Type 2 hypervisor requires a host operating system and is more often used for testing and labs.

There are six areas of IT where virtualization is frequently used:

1) Network virtualization combines the available resources in a network by splitting up the available bandwidth into connectivity channels, each of which runs independently from the others. With virtual network, each channel can be assigned or reassigned to a particular server or device in real time. Much like a partitioned hard drive, virtualization separates the network into manageable parts, disguising the true complexity of the network.

2) Storage virtualization pools physical storage from multiple network storage devices into a centrally managed console. Storage virtualization is commonly used in storage area networks.

3) Server virtualization hides server resources, including the number and identity of individual physical servers, CPUs and OSes, from users. Virtual servers spare users from having to manage the complicated details of server resources. They also increase server, processor and OS sharing as well as resource use and expansion capacity.

4) Data virtualization abstracts the technical details of data and data management, such as location, performance and format. Instead, data virtualization focuses on broader access and resiliency.

5) Desktop virtualization virtualizes a workstation load rather than a server. This lets the user access a desktop remotely, typically using a thin client at the desk. With virtual desktop infrastructure, the workstation essentially runs in a data center server and access is more secure and portable. However, the OS license and infrastructure still must be accounted for.

5) Application virtualization abstracts the application layer away from the OS. This lets the application run in an encapsulated form without dependence on the underlying OS.

Advantages of virtualization

The overall benefit of virtualization is that it helps organizations maximize output.
More specific.
advantages include the following:

a) Lower costs: Virtualization reduces the amount of hardware servers companies and data centers require. This lowers the overall cost of buying and maintaining large amounts of hardware.

b) Easier disaster recovery: DR is simple in a virtualized environment. Regular snapshots provide up-to-date data, letting organizations easily back up and recover VMs, avoiding unnecessary downtime. In an emergency, a virtual machine can migrate to a new location within minutes.

c) Easier testing: Testing is less complicated in a virtual environment. Even in the event of a large mistake, the test can continue without stopping and returning to the beginning. The test simply returns to the previous snapshot and proceeds.

d) Faster backup: Virtualized environments take automatic snapshots throughout the day to guarantee all data is up to date. VMs can easily migrate between host machines and be efficiently redeployed.

e) Improved productivity:. Virtualized environments require fewer physical resources, which results in less time spent managing and maintaining servers. Tasks that take days or weeks in physical environments are done in minutes. This lets staff members spend their time on more productive tasks, such as raising revenue and facilitating business initiatives

f) Single-minded servers: Virtualization provides a cost-effective way to separate email, database and web servers, creating a more comprehensive and dependable system.

g) Optimize deployment and redeployment: When a physical server crashes, the backup server might not always be ready or up to date. If this is the case, then the 4849 redeployment process can be time-consuming and tedious. However, in a virtualized data center, virtual backup tools expedite the process to minutes.

h) Reduced heat and improved energy savings: Companies that use a lot of hardware servers risk overheating their physical computing resources. Virtualization decreases the number of servers used for data management.

Limitations of virtualization

Before converting to a virtualized environment, organizations should consider the various limitations:

a) Cost: The investment required for virtualization software and hardware can be expensive. If the existing infrastructure is more than five years old, organizations should consider an initial renewal budget. Many businesses work with a managed service provider to offset costs with monthly leasing and other purchase options.

b) Software licensing considerations: Vendors view software use within a virtualized environment in different ways. It's important to understand how a specific vendor does this.

c) Time and effort: Converting to virtualization takes time and has a learning curve that requires IT staff to be trained in virtualization. Furthermore, some applications don't adapt well to a virtual environment. IT staff must be prepared to face these challenges and address them prior to converting.

d) Security: Virtualization comes with unique security risks. Data is a common target for attacks, and the chance of a data breach increases with virtualization.

e) Complexity: In a virtual environment, users can lose control of what they can do because several parts of the environment must collaborate to perform the same task. If any part doesn't work, the entire operation can fail.

Reference

1.https://tails.net/install/index.en.htm
2.https://www.techspot.com/downloads/6518-tails.html