



Certified Threat Intelligence
Analyst v2

CLASSROOM LAB SETUP GUIDE

EC-Council Official Curricula

Table of Contents

Classroom Setup Instructions: CTIAv2	4
Classroom Requirements	5
Hardware	6
Software	6
Classroom Connectivity	7
Configuration	7
Setup Document Overview	7
Training Room Environment	8
Instructor Computer	8
Student Workstations	9
Room Environment	10
Classroom Configuration	11
Computer Names	11
Network Topology	12
CTIA VM Setup on Instructor and Student Machines	13
Instructor Acceptance	13
Firewall Settings	13
Blackboard	14
Setup Checklist	14
Instructor Acceptance	15
Assistance	15
Detailed Setup Instructions — Configuration Tasks (CT)	16
CT#1: Install the Host Operating System	16
CT#2: Copy the Host Operating System Files	16
CT#3: Install WinRAR on Host Operating System	16
CT#4: Download the ISO File	17
CT#5: Install VMware Workstation Pro on Host Machine	17
CT#6: Configure a Virtual Network in VMware Virtual Network Editor	19
CT#7: Install Windows 11 Virtual Machine in VMware	24
CT#8: Create a Partition in the Windows 11 Virtual Machine	46

CT#9: Install Parrot Security Virtual Machine in VMware.....	51
CT#10: Turn Off Windows Defender Firewall on the Windows 11 Virtual Machine.....	64
CT#11: Configure Windows Components on the Windows 11 Virtual Machine.....	82
CT#12: Install WinRAR on the Windows 11 Virtual Machine.....	86
CT#13: Install MS Office on the Windows 11 Virtual Machine.....	86
CT#14: Download CTIA Tools on the Windows 11 Virtual Machine.....	86
CT#15: Adding .NET Framework in the Windows 11 Virtual Machine	87
CT#16: Install Java Runtime Environment and Java Development Kit in the Windows 11 Virtual Machine	87
CT#17: Share and Map CTIA-Tools Folder to Parrot Security Virtual Machine	88
CT#18: Install Adobe Acrobat Reader DC on the Windows 11 Virtual Machine.....	93
CT#19: Install Web Browsers on the Windows 11 Virtual Machine	94
CT#20: Install WinPcap on the Windows 11 Virtual Machine	94
CT#21: Turn Off Screen Savers on the Windows 11 Virtual Machine	94
CT#22: Ping Test Among Both Virtual Machines.....	97
CT#23: Take Snapshots of Virtual Machines	99

Classroom Setup Instructions: CTIAv2

This document contains setup instructions for the EC-Council Certified Threat Intelligence Analyst (CTIA) course. The course requires a standard modular classroom seating configuration, a computer for each student, a computer for the instructor, a dedicated hub or switch (hub preferred), a dedicated firewall, and an Internet connection. This class teaches threat intelligence methodology, which includes collection, analysis, reporting, and dissemination of intelligence. It is imperative that the network used for this class be separated both logically and physically from any other networks in the training facility to prevent students from “accidentally” conducting exploits on other computers within accessible networks.

Before beginning the class, install and configure all computers using the information and instructions that follow.

The information contained in this document is subject to change without notice. Unless otherwise noted, the names of companies, products, people, and data used in this document are fictional. Their use is not intended in any way to represent any real company, person, product, or event. Users of this document are responsible for compliance with all applicable copyright laws. No part of this document may be reproduced or transmitted by any means, electronic or mechanical, for any purpose, without the express written consent of the International Council of Electronic-Commerce Consultants, hereinafter referred to as the EC-Council. If, however, your only means of access is electronic, permission is hereby granted to print one copy.

The EC-Council may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering the material in this document. Except as expressly provided in any written license agreement from the EC-Council, providing this document does not give you any license to those patents, trademarks, copyrights, or other intellectual property.

Certified Threat Intelligence Analyst and CTIA are either registered trademarks or trademarks of the EC-Council in the USA and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Classroom Requirements

This section describes the classroom equipment required for the EC-Council Certified Threat Intelligence Analyst (CTIA) course.

Classroom Equipment

The following equipment is required for the general classroom setup:

- Climate control system, adjustable within the classroom
- Lighting controls, adjustable within the classroom
- Whiteboard, 3 feet × 6 feet (1 m × 2 m) or larger
- Markers of assorted colors and a whiteboard
- Eraser and whiteboard cleaner liquid (3 oz minimum)
- Towels and paper
- Easel with a flipchart or butcher paper pad, 24 in × 36 in
- Felt-tip pens with chisel tips (not fine point); blue and black are required, while other colors are optional
- Projection screen measuring 6 feet diagonally (a non-reflective whiteboard surface may be used as a substitute)
- Instructor station:
 - Ergonomic desk and chair
 - Power outlet
 - Network jack
 - LCD projector with a minimum resolution of 740 × 1280 pixels and all connecting cables
- Student station (per student):
 - Ergonomic chair
 - Workstation with a minimum horizontal workspace of 9 square feet (3 feet × 3 feet)
 - One power outlet
 - One network jack

Hardware

The hardware requirements for the instructor and student computers are identical:

- Intel Core i5 or equivalent CPU with a minimum clock speed of 3.2 GHz
- Minimum of 8 GB or more RAM
- Hard disk, 500 GB or higher and 7200 RPM or faster
- DVD drive (DVD R/W drive preferred)
- One network adapter (minimum of a 10/100 NIC, but a 10/100/1000 is preferred), full duplex (disable any additional network adapters installed)
- Monitor (minimum requirement is a 17-inch LCD monitor)
- Mouse or compatible pointing device and a sound card with amplified speakers
- Internet access
- Two wireless network adapters (PCI or USB)*

The following additional hardware is required:

- A switch with sufficient ports to allow the connection of all instructor and student workstations, in addition to at least five unused ports for connecting additional equipment or for use as “spares”

*If wireless network adapters are not available for all classroom machines, at least the instructor machine must be so equipped.

Software

All computers in the class require the following software:

- Any Windows/Linux/macOS operating system capable of running VMware Workstation Pro
- CTIA Tools downloadable from the Aspen portal
- VMware Workstation Pro v15.5.1 or later version
- Microsoft .NET Framework 6.0.415
- Adobe Acrobat Reader DC or later version
- WinRAR v6.24 or later version
- Web browsers: Microsoft Edge, Firefox, and Chrome
- WinPcap driver
- Microsoft Office 2016 or Open Office
- Java Runtime Environment v8u391 or later version

- Java Development Kit v8u171 or later version
- VMware Workstation Pro (built-in role in any Windows/Linux/macOS operating system capable of running VMware Workstation Pro)
 - Microsoft Windows 11 Enterprise or Professional (64-bit) with all patches applied
 - Parrot Security 5.0 Electric Ara (64 bit) with all patches applied

Note: All the above-mentioned tools, except the Windows operating system (Windows 11) and Parrot Security, are available in the CTIA Tools downloads from the Aspen portal.

Classroom Connectivity

As this class teaches network attack methodologies, the network for the class must be logically and physically separated from any other networks present in the training facility and must have its own Internet connection.

Configuration

This section describes the procedures for setting up the instructor and student computers, as well as general directions for the configuration of the firewall appliance.

This guide assumes that you will use disk-imaging software to create images of the classroom computers for future use. To that end, configuration tasks (CTs) common to all computers are presented first. Perform these tasks on the computer that will become the instructor computer. Create a disk image after setting up a single student computer. You may then deploy this image to the remaining classroom machines while completing configuration of the instructor computer.

Because the Instructor computer is configured as a dynamic host configuration protocol (DHCP) server that provides IP addresses to the student machines, the installation and configuration of the Instructor computer must be completed before the final configuration of the student machines can begin.

Setup Document Overview

This document provides background information for the technical staff responsible for setting up a training room facility for the CTIA course. This guide describes the requirements for the network equipment and computer stations that are installed and configured by the facility's personnel for the training courses.

Training Room Environment

The training room environment consists primarily of the following equipment:

- Instructor computer
- Student workstations

Equipment	Number (Class of 12 Students)	Operating System	Minimum System Requirements
Instructor Computer	1	Any Windows/Linux/macOS operating system	Intel Core i5 or equivalent PC with 500 GB free disk space, a minimum of 8 GB RAM (16 GB recommended), one NIC, 17-inch monitor, two wireless network adapters (PCI or USB), and one compatible mouse
Student Workstations	12	Any Windows/Linux/macOS operating system	Intel Core i5 or equivalent PC with 500 GB free disk space, a minimum of 8 GB RAM (16 GB recommended), one NIC, 17-inch monitor, one wireless network adapter (PCI or USB), and one compatible mouse

Instructor Computer

Perform the following tasks on the instructor computer:

- Install **any Windows/Linux/macOS operating system** capable of running VMware Workstation Pro, updated with the latest service packs and patches.
- Download the ISO file from Aspen (see [CT#4](#) in the Configuration Tasks section).
- Download all CTIA Tools from Aspen to the **E:\CTIA-Tools** folder on your hard drive for easy access (see [CT#14](#) in the Configuration Tasks section).
- Install VMware Workstation Pro on the host machine (see [CT#5](#) in the Configuration Tasks section).
- Configure a virtual network in the VMware Virtual Network Editor (see [CT#6](#) in the Configuration Tasks Section).
- Install guest operating systems (Windows 11) on VMware Workstation (see [CT#7](#) in the Configuration Tasks section).
- Create a partition in the Windows 11 virtual machine (see [CT#8](#) in the Configuration Tasks section).
- Install guest operating system (Parrot Security) on VMware Workstation (see [CT#9](#), in the Configuration Tasks section).
- Turn off the firewall on the Window 11 virtual machine (see [CT#10](#) in the Configuration Tasks section).

- Install Windows components in the Windows 11 virtual machine (see [CT#11](#) in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see [CT#12](#) and [CT#13](#) in the Configuration Tasks section).
- Have CTIA Tools shared as the **E:** drive on the Windows and Parrot Security machines (mapping the **E:** drive) (see [CT#17](#) in the Configuration Tasks section).
- Install Adobe Acrobat Reader DC on the Windows 11 virtual machine (see [CT#18](#) in the Configuration Tasks section).
- Install Web Browsers and WinPcap in the Windows 11 virtual machine (all software can be found in the **Lab Prerequisites** directory in the **E:\CTIA-Tools** folder) (see [CT#19](#), and [CT#20](#) in the Configuration Tasks section).
- Install .NET Framework on the Windows 11 virtual machine (see [CT#15](#) in the Configuration Tasks section).
- Install Java Runtime Environment and Java Development Kit on the Windows 11 virtual machine (see [CT#16](#) in the Configuration Tasks section).
- Turn off screen savers on the Windows 11 virtual machine (see [CT#21](#) in the Configuration Tasks section).
- Conduct a ping test between both the virtual machines in the network (see [CT#22](#) in the Configuration Tasks section).
- Take snapshots of the virtual machines (see [CT#23](#) in the Configuration Tasks section).
- Connect an LCD projector.

Student Workstations

Perform the following tasks on the student workstations:

- Install **any Windows/Linux/macOS operating system** capable of running VMware Workstation Pro, updated with the latest service packs and patches.
- Download the ISO file from Aspen (see [CT#4](#) in the Configuration Tasks section).
- Download all CTIA Tools from Aspen to the **E:\CTIA-Tools** folder on your hard drive for easy access (see [CT#14](#) in the Configuration Tasks section).
- Install VMware Workstation Pro on the host machine (see [CT#5](#) in the Configuration Tasks section).
- Configure a virtual network in the VMware Virtual Network Editor (see [CT#6](#) in the Configuration Tasks Section).
- Install guest operating systems (Windows 11) on VMware Workstation (see [CT#7](#) in the Configuration Tasks section).
- Create a partition in the Windows 11 virtual machine (see [CT#8](#) in the Configuration Tasks section).

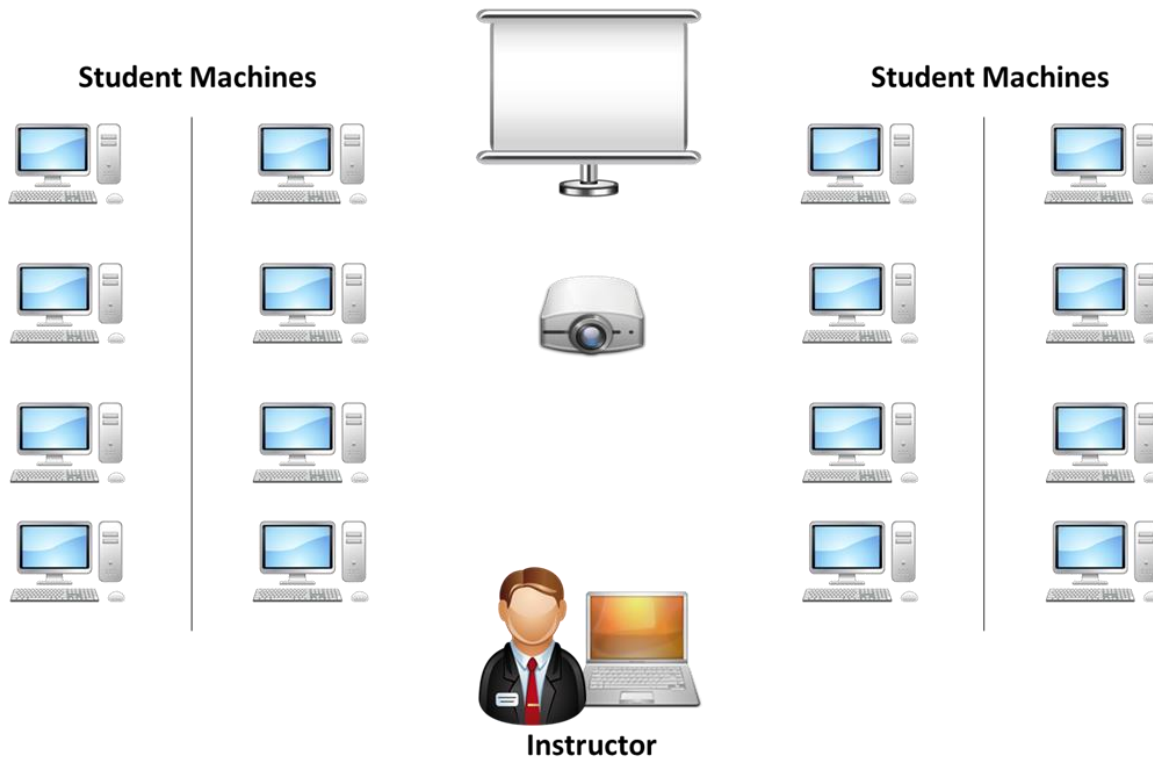
- Install guest operating system (Parrot Security) on VMware Workstation (see [CT#9](#), in the Configuration Tasks section).
- Turn off the firewall on the Windows 11 virtual machine (see [CT#10](#) in the Configuration Tasks section).
- Install Windows components in the Windows 11 virtual machine (see [CT#11](#) in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see [CT#12](#) and [CT#13](#) in the Configuration Tasks section).
- Have CTIA Tools shared as the **E:** drive on the Windows and Parrot Security machines (mapping the **E:** drive) (see [CT#17](#) in the Configuration Tasks section).
- Install Adobe Acrobat Reader DC on the Windows 11 virtual machine (see [CT#18](#) in the Configuration Tasks section).
- Install Web Browsers and WinPcap in the Windows 11 virtual machine (all software can be found in the **Lab Prerequisites** directory in the **E:\CTIA-Tools** folder) (see [CT#19](#), and [CT#20](#) in the Configuration Tasks section).
- Install .NET Framework on the Windows 11 virtual machine (see [CT#15](#) in the Configuration Tasks section).
- Install Java Runtime Environment and Java Development Kit on the Windows 11 virtual machine (see [CT#16](#) in the Configuration Tasks section).
- Turn off screen savers on the Windows 11 virtual machine (see [CT#21](#) in the Configuration Tasks section).
- Conduct a ping test between both the virtual machines in the network (see [CT#22](#) in the Configuration Tasks section).
- Take snapshots of the virtual machines (see [CT#23](#) in the Configuration Tasks section).

Room Environment

- The room must contain a whiteboard measuring a minimum of 1 yard by 2–3 yards (1 m by 2–3 m).
- The room should contain an easel and a large tablet (optional).
- The room must be equipped with legible black and blue felt-tip pens with chisel point tips (not fine tip).

Classroom Configuration

The configuration of this classroom is modular. Computers can be added or removed either by row or column, depending on the needs of the class. The following is a sample room setup that provides optimal support. This setup allows for ease of access to “*troublespots*” by the instructor and allows students to break into functional teams of varying sizes.

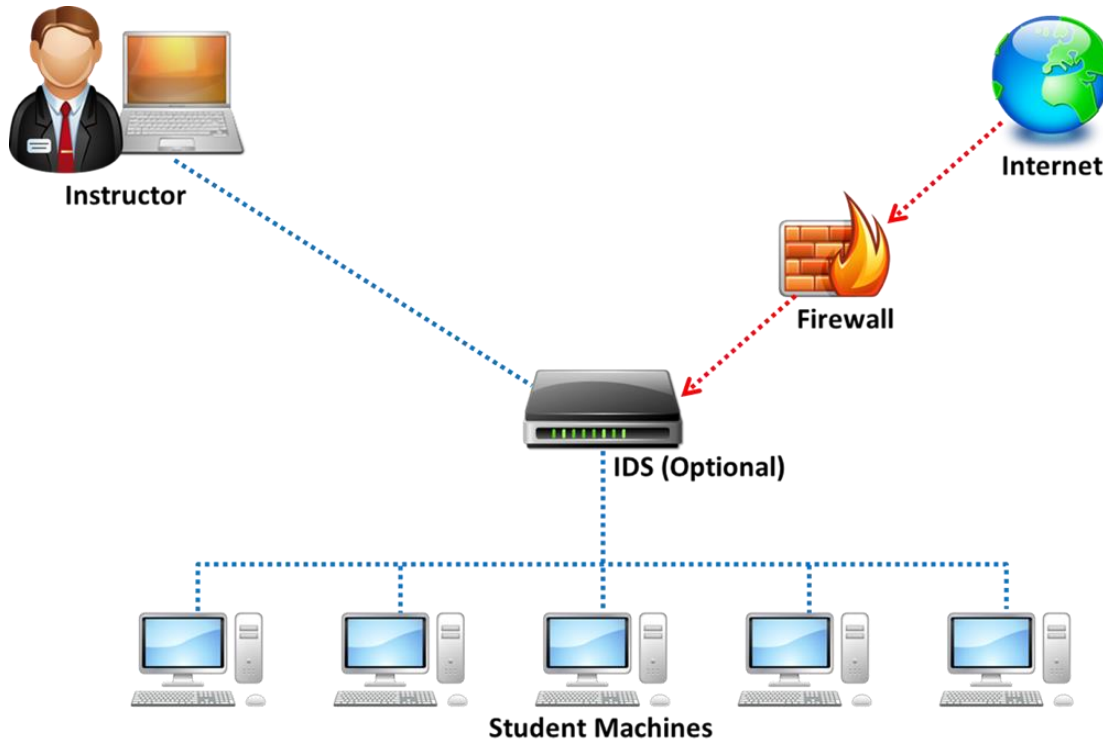


Computer Names

Assign computer names to student machines, such as CTIASTUDENT1, CTIASTUDENT2, CTIASTUDENT3. The instructor machine should be named INSTRUCTOR.

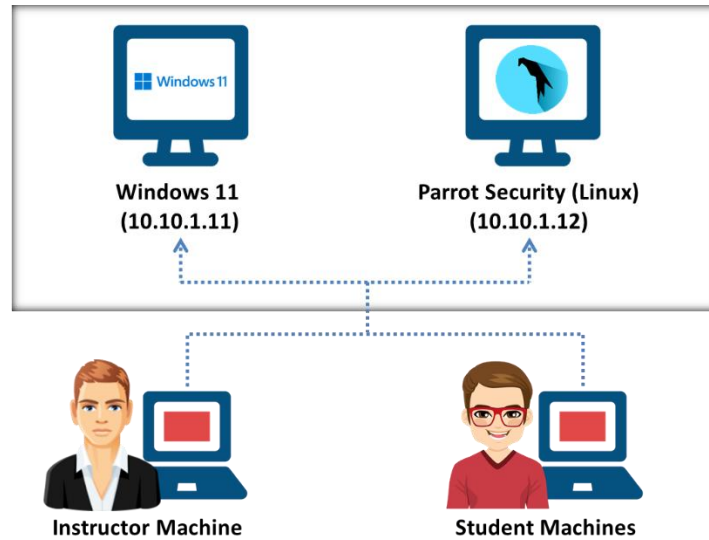
Network Topology

The training room must be physically isolated from any production network. Students must be able to access the Internet from their PCs. All computers are connected as one isolated network and domain. The common protocol is IP. All computers should have dynamic IP addresses using a DHCP server. Configure the DHCP server scope to 10.0.0.0/24 IP addresses. This reduces potential problems when booting the virtual machines. NICs can be of 10 Mbit or 100 Mbit (100 Mbit is recommended). Cables must be bundled and tied out of pathways and work areas and must be of sufficient length to avoid stress.



Set up the machines based on the classroom setup diagram. The lab exercises for the students are instructor led and they are based on the threat intelligence tools discussed in the trainer slides. The instructors are encouraged to demonstrate and guide the students on the use of threat intelligence tools. Please feel free to include your own exercises.

CTIA VM Setup on Instructor and Student Machines



Instructor and Student Machine Operating System: Any Operating System Capable of Running VMware (Fully Patched)

Instructor Acceptance

Before the scheduled start of the training class, the instructor should visit the training facility to inspect and approve the setup. The technical contact (system administrator) for the facility must be available to answer questions and correct any setup issues. Both the instructor and technical contact must ensure the completion of the following checklists before the training setup is deemed acceptable.

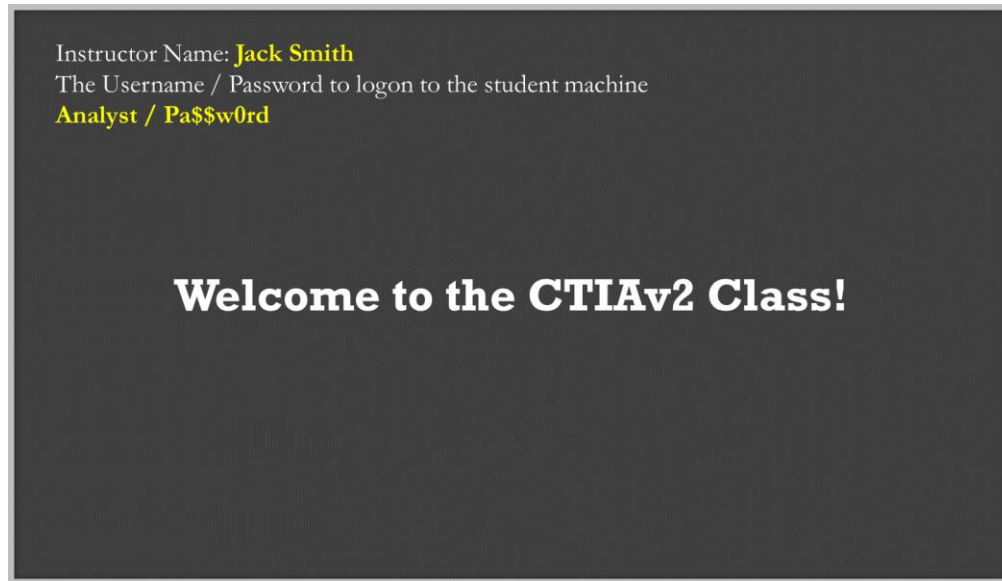
Firewall Settings

Do not block any ports while accessing the Internet through the firewall. You should be able to ping servers on the Internet.

Blackboard

Write the following in the top-left corner of the blackboard:

- Instructor name: <Name of the instructor>
- Username/Password to login to the student machine



Setup Checklist

The arrangement of items in the setup checklists is designed to validate the setup in the most efficient manner possible. Before beginning the setup checklist, log off any connected users.

Tick Here	List
<input type="checkbox"/>	Verify that VMware Workstation Pro is installed.
<input type="checkbox"/>	Verify that all CTIA tools are on the computer in the CTIA-Tools folder in the E: .
<input type="checkbox"/>	Verify that Internet access is available.
<input type="checkbox"/>	Visit https://www.eccouncil.org and view the page to check the Internet access.
<input type="checkbox"/>	Open Command Prompt and enter nslookup certifiedhacker.com to check for a connection to the server.
<input type="checkbox"/>	Verify that Acrobat Reader, WinRAR, WinPcap, and Command Prompt extensions are installed.
<input type="checkbox"/>	Verify that the web browsers (Google Chrome and Mozilla Firefox) are installed.
<input type="checkbox"/>	Verify that the instructor computer can display through the overhead projector.
<input type="checkbox"/>	Verify that each computer has 500 GB or more of free disk space.

<input type="checkbox"/>	Verify whether you can successfully boot the Windows 11 and Parrot Security virtual machines using VMware Workstation.
<input type="checkbox"/>	Confirm that the cable wiring is organized and labeled.
<input type="checkbox"/>	Confirm that the student workstation and chair are placed satisfactorily.
<input type="checkbox"/>	Confirm that the placement of the LCD (overhead) projector is appropriate.
<input type="checkbox"/>	Confirm that a whiteboard, dry erase markers, and erasers are available.
<input type="checkbox"/>	Confirm that the instructor's station is properly organized and oriented.
<input type="checkbox"/>	Confirm that computers are labeled with a client number.
<input type="checkbox"/>	Ensure that the EC-Council courseware (Official EC-Council CTIAv2 Box) is available to students.
<input type="checkbox"/>	Write down the phone number of the facility's technical contact person. Contact them in case of a network problem.
<input type="checkbox"/>	Confirm that the internal network adapter is configured for the virtual machines and host.

Instructor Acceptance

The technical contact (system administrator) for the facility must be available to answer questions and correct any setup issues.

The instructor should inspect both the classroom and the items covered in the setup checklist(s) to ensure that the classroom and setup meet EC-Council standards. Any deficiencies discovered by the instructor must be corrected before the scheduled start time of the class.

Assistance

If you have problems or require assistance in setting up the lab for your CTIA class, please e-mail partnersupport@eccouncil.org.

Detailed Setup Instructions — Configuration Tasks (CT)

CT#1: Install the Host Operating System

1. Install any **Windows/Linux/macOS** operating system capable of running VMware Workstation Pro using a DVD or USB drive.
2. Configure the hard disk to have one active primary partition (C:\ of 300 GB) and one extended logical partition (D:\ of 200 GB).
3. Check for updates and, if found, update the host operating system.
4. Install the wireless network adapters according to the manufacturer's instructions.

[\[Back to Configuration Task Outline\]](#)

CT#2: Copy the Host Operating System Files

1. Browse the installation DVD.
2. Copy all the source files from the DVD to the **SOURCES** folder in the drive's active primary partition (e.g., Active Drive Partition Name:\SOURCES).
3. When completed, close all windows to return to the **Desktop**.

[\[Back to Configuration Task Outline\]](#)

CT#3: Install WinRAR on Host Operating System

1. Download the latest version of **WinRAR** from the official WinRAR website (<https://www.winrar.com/download.html>).

Note: Download the latest version of WinRAR compatible with your host operating system from the official website (Here, we consider Windows to be the host OS).

2. Double-click on the **.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
3. The **WinRAR** setup window appears. Click **Install**.
4. Complete the installation by choosing the default settings.
5. After completing the installation, the installation location of the WinRAR files is automatically opened in an Explorer window; close the window.

[\[Back to Configuration Task Outline\]](#)

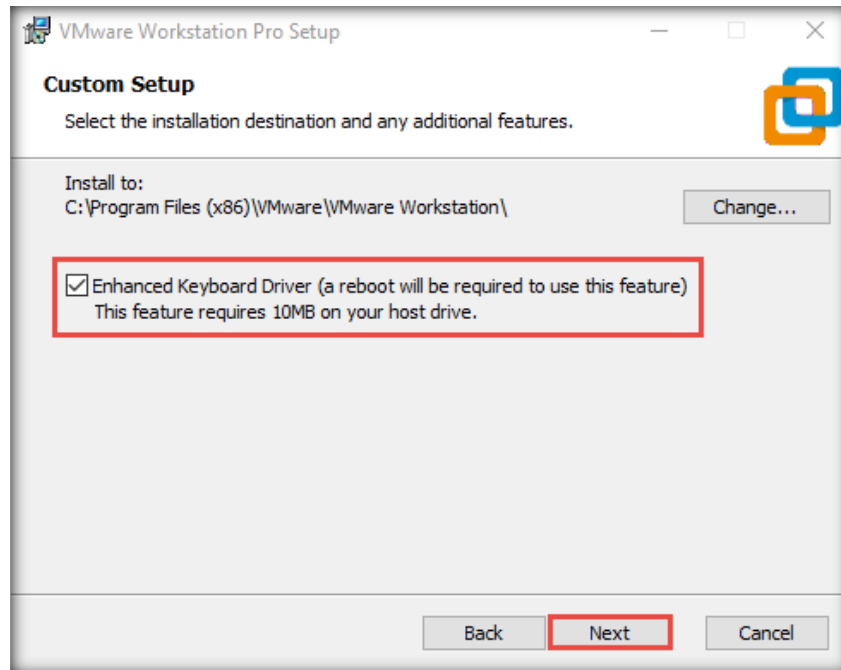
CT#4: Download the ISO File

1. Log in to your **Aspen** account (you will see your course listed under **My Courses**) → click the **TRAINING** button under the course to access the e-Courseware, Lab Manuals, and Tools in the **Training** area → click the **Download Tools** tab from the left-hand pane.
2. Click the **CTIAv2 ISO.zip** file from the right-hand pane to download the ISO files for the Parrot Security operating system.
3. Navigate to the location where you downloaded the **CTIAv2 ISO.zip** file, right-click the .zip files, and select the **Extract Here** option.

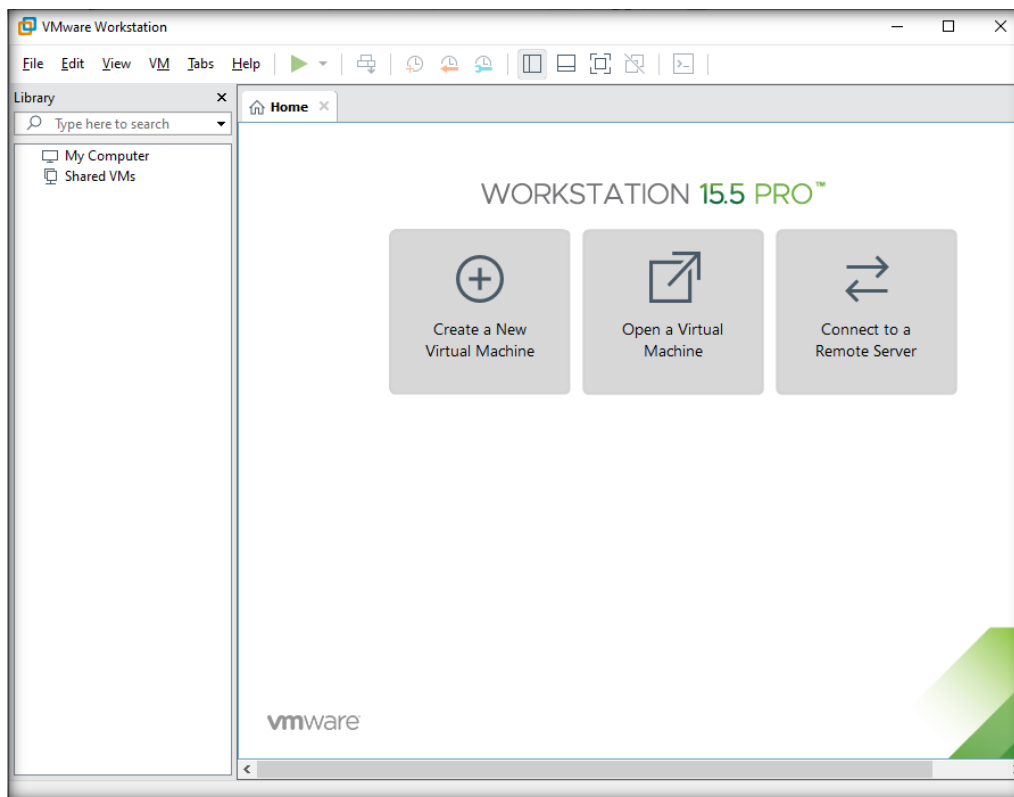
[\[Back to Configuration Task Outline\]](#)

CT#5: Install VMware Workstation Pro on Host Machine

1. In your host system, navigate to the location where you have extracted the **CTIAv2 ISO.zip** file and then to **CTIAv2 ISO\VMware Workstation Pro**.
2. Double-click the file **VMware-workstation-full-15.5.1-15018445.exe**.
Note: You can download the latest version of VMware Workstation Pro from <https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html>.
Note: If you decide to download the latest version, the screenshots in your lab environment might differ from those shown in this guide.
3. A **User Account Control** pop-up window appears. Click **Yes**.
Note: If a **VMware Product Installation** notification appears, click **Yes** to restart the system.
Note: After the system reboots, double-click the file **VMware-workstation-full-15.5.1-15018445.exe**.
4. VMware Workstation Pro initializes; in the installation wizard, click **Next**.
5. Accept the user agreement and click **Next**.
6. In the **Custom Setup** wizard, check the **Enhanced Keyboard Driver** option and click **Next**.
7. Follow the wizard-driven installation steps to install VMware Workstation Pro using the default settings.



8. On completion of the installation, the machine will restart.
9. Once the machine has rebooted, launch VMware Workstation Pro.

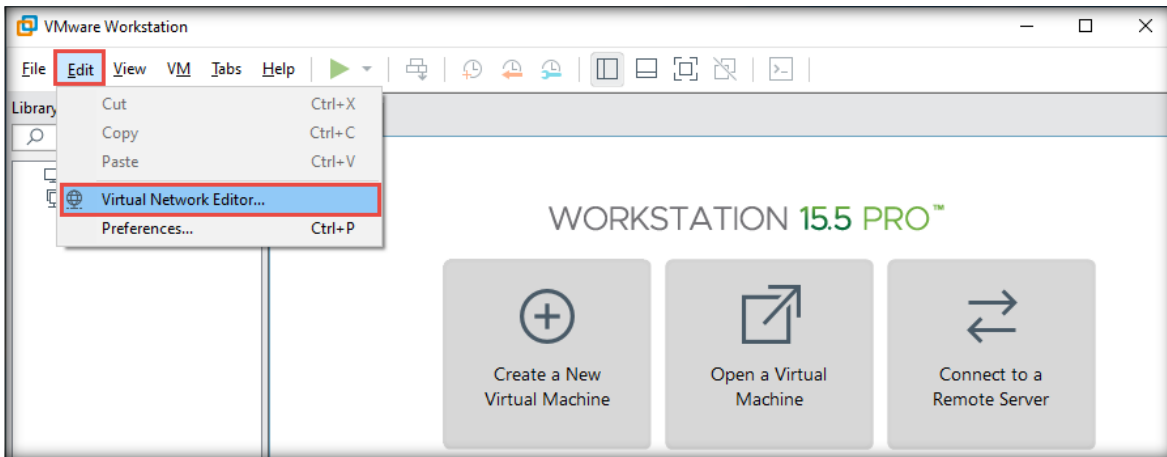


Note: If VMware Workstation Pro prompts for an activation key; provide it, if you have purchased one, or continue with the trial version.

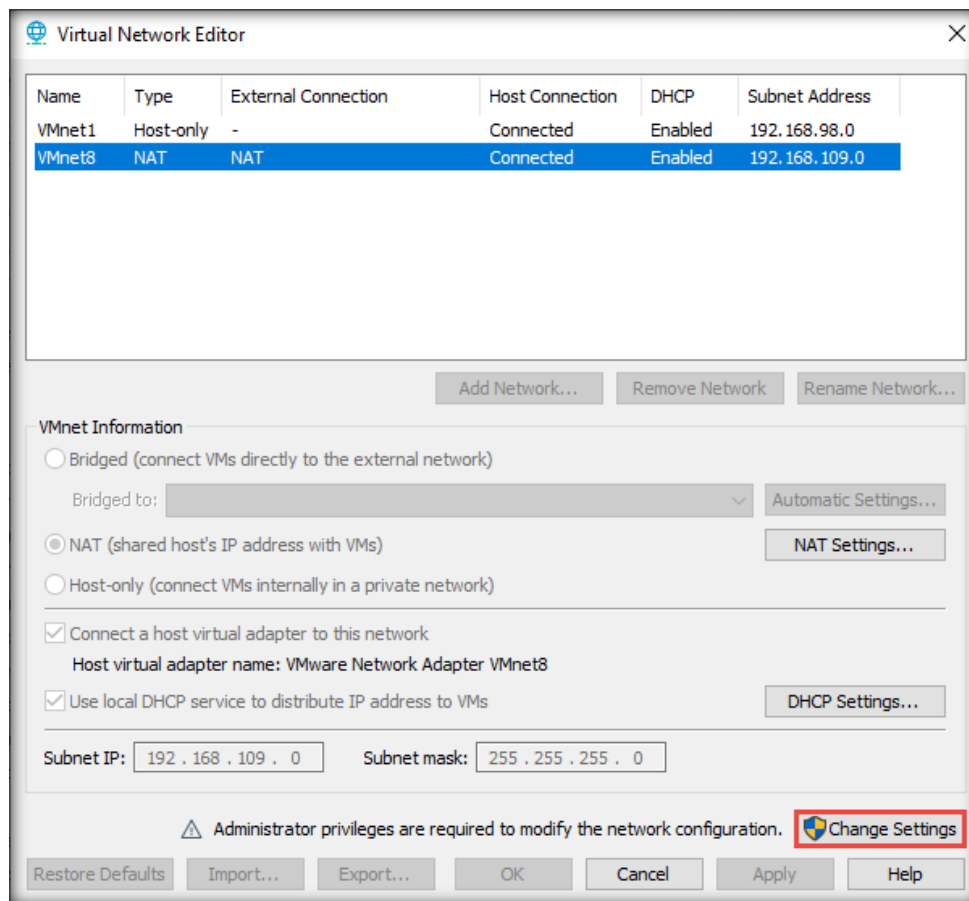
[\[Back to Configuration Task Outline\]](#)

CT#6: Configure a Virtual Network in VMware Virtual Network Editor

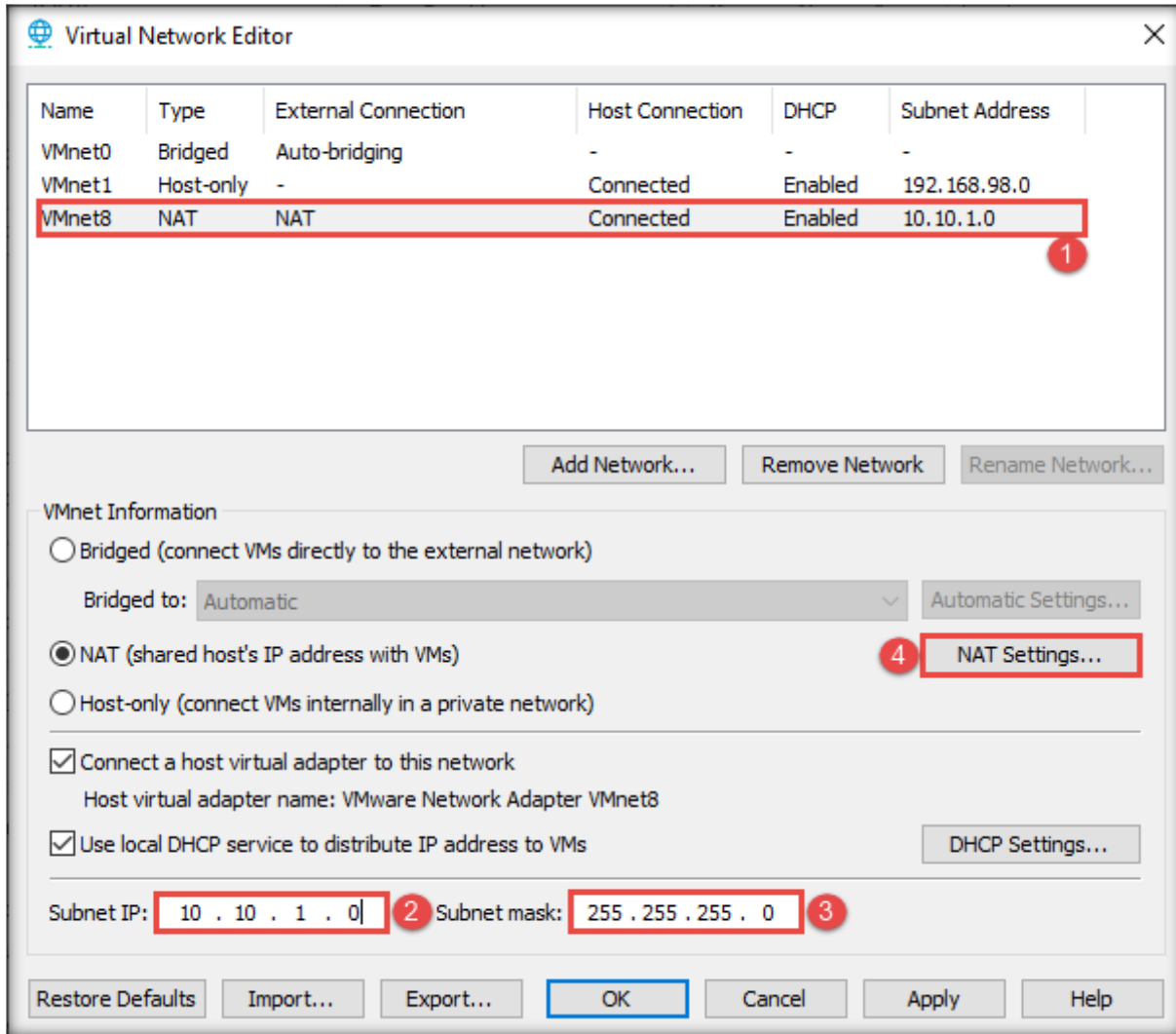
1. Launch **VMware Workstation Pro**.
2. Navigate to **Edit** and click **Virtual Network Editor...** as shown in the screenshot below.



3. The **Virtual Network Editor** window appears; choose the **VMnet8 NAT** network and click **Change Settings** from the lower-right section of the window.



4. If a **User Account Control** pop-up appears, click **Yes**.
5. In the **Virtual Network Editor** window, select **VMnet8** again in the lower section of the window, define **Subnet IP** as **10.10.1.0** and **Subnet mask** as **255.255.255.0**, and click **NAT Settings...**



6. The **NAT Settings** window appears; enter **10.10.1.2** as the **Gateway IP** and click **OK**.

The screenshot shows the NAT Settings dialog box with the following fields and options:

- Network: vmnet8
- Subnet IP: 10.10.1.0
- Subnet mask: 255.255.255.0
- Gateway IP: 10 . 10 . 1 | . 2

Port Forwarding

Host Port	Type	Virtual Machine IP Address	Description
-----------	------	----------------------------	-------------

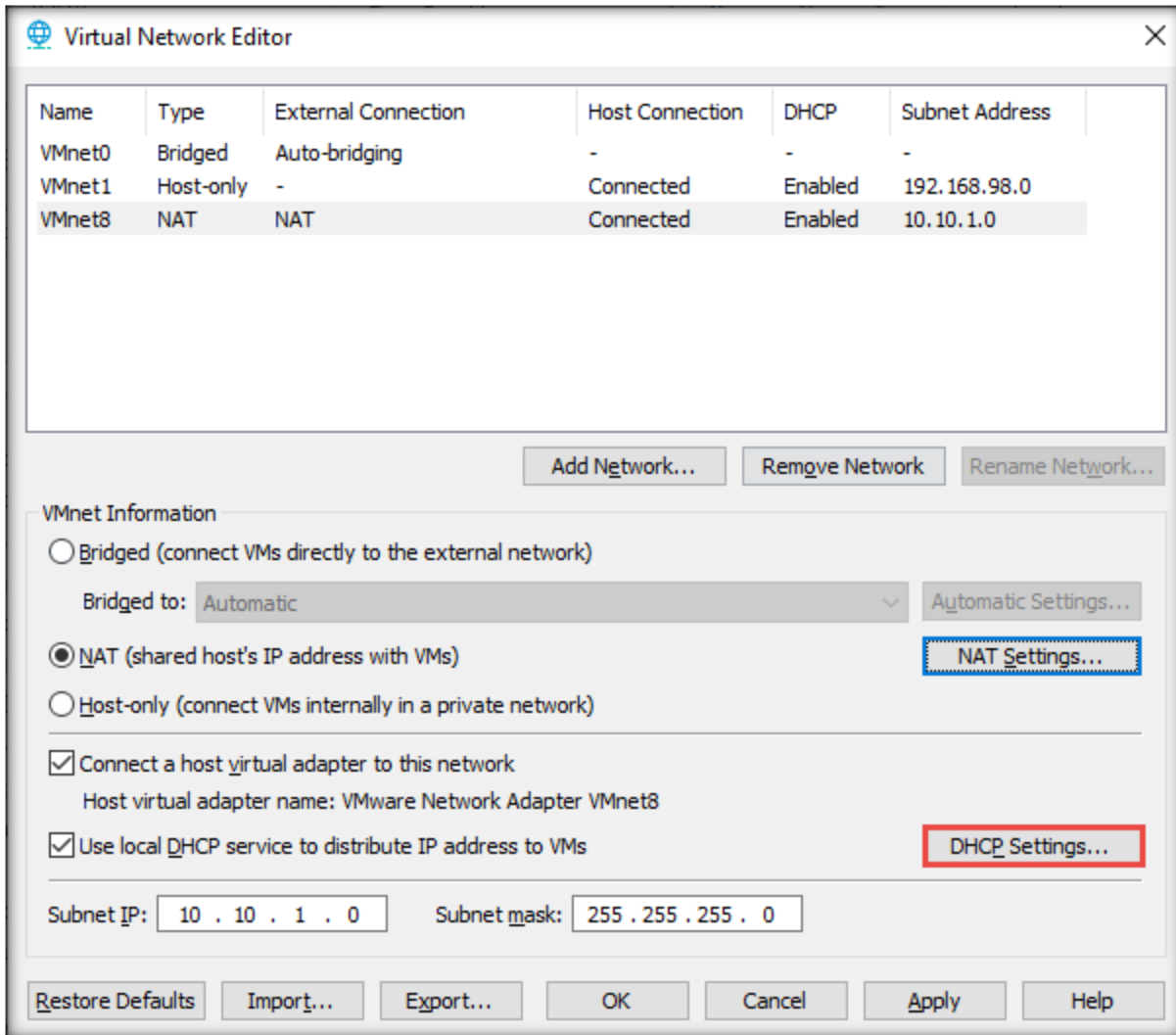
Buttons: Add... Remove Properties

Advanced

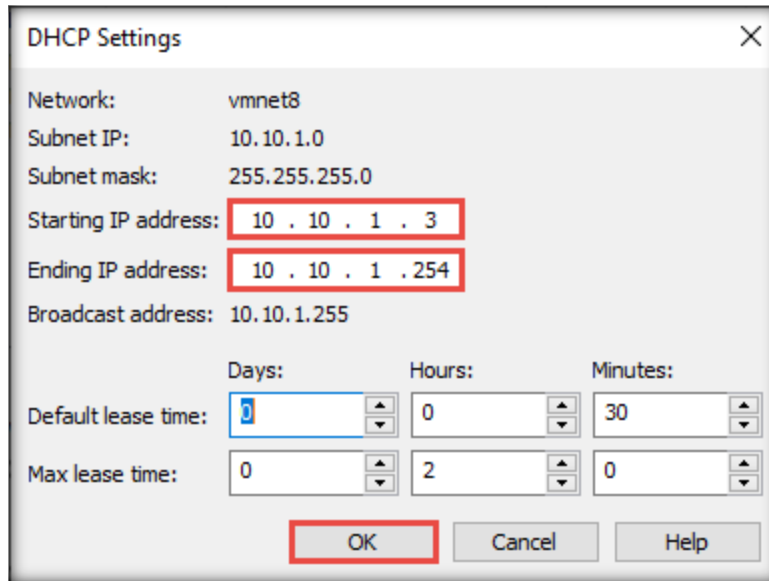
- Allow active FTP
- Allow any Organizationally Unique Identifier
- UDP timeout (in seconds): 30
- Config port: 0
- Enable IPv6
- IPv6 prefix: fd15:4ba5:5a2b:1008::/64

Buttons: DNS Settings... NetBIOS Settings... OK Cancel Help

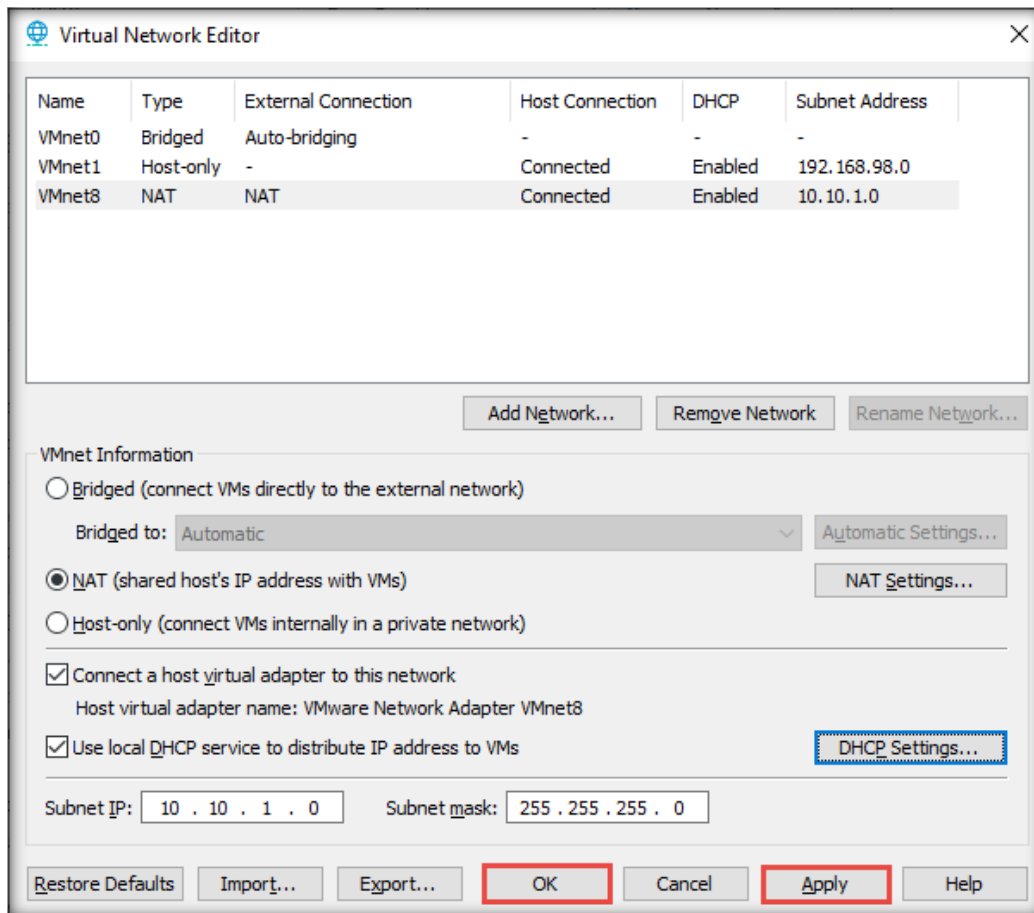
7. Now, keep **VMnet8** selected and click **DHCP Settings....**



- In the **DHCP Settings** window, define the **Starting IP address** as **10.10.1.3** and the **Ending IP address** as **10.10.1.254**. Click **OK**.



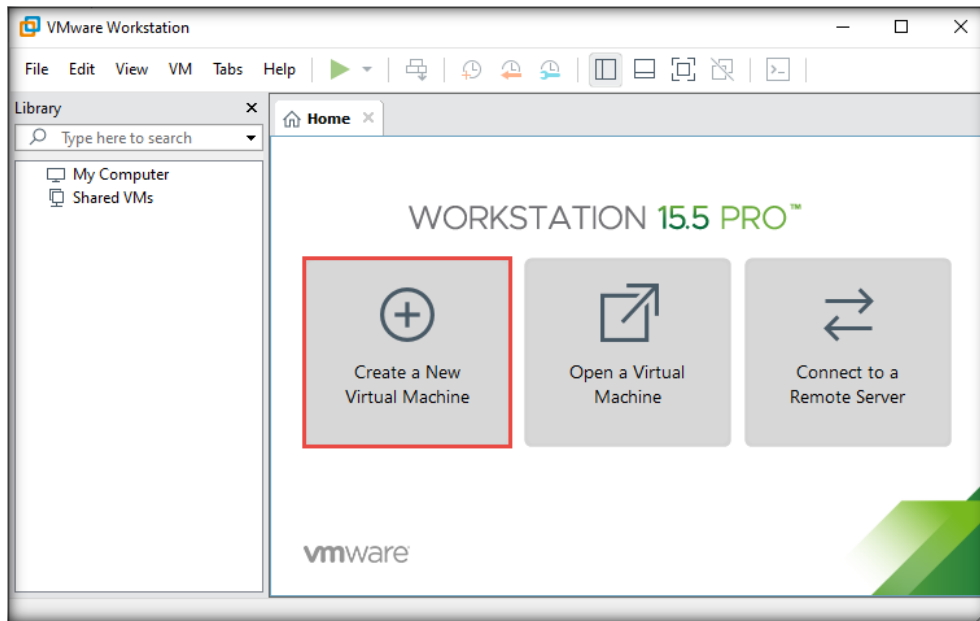
- Click **Apply** and **OK** in the **Virtual Network Editor** window to complete the configuration.



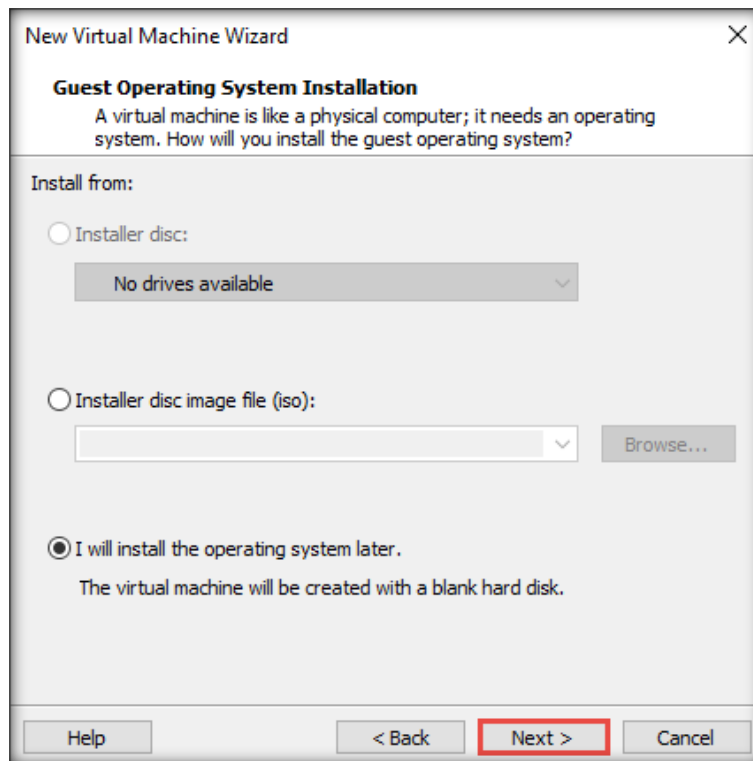
[\[Back to Configuration Task Outline\]](#)

CT#7: Install Windows 11 Virtual Machine in VMware

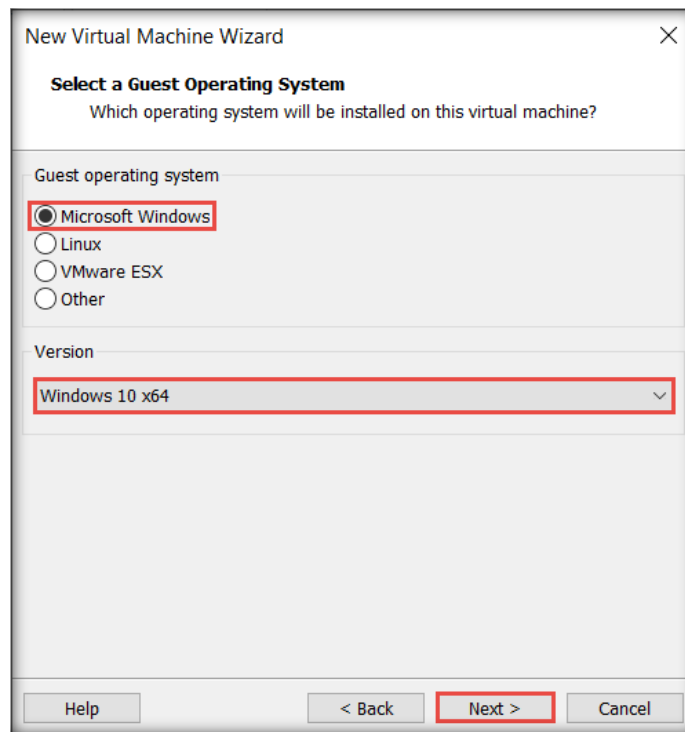
1. In the **VMware Workstation** window, click **Create a New Virtual Machine**.



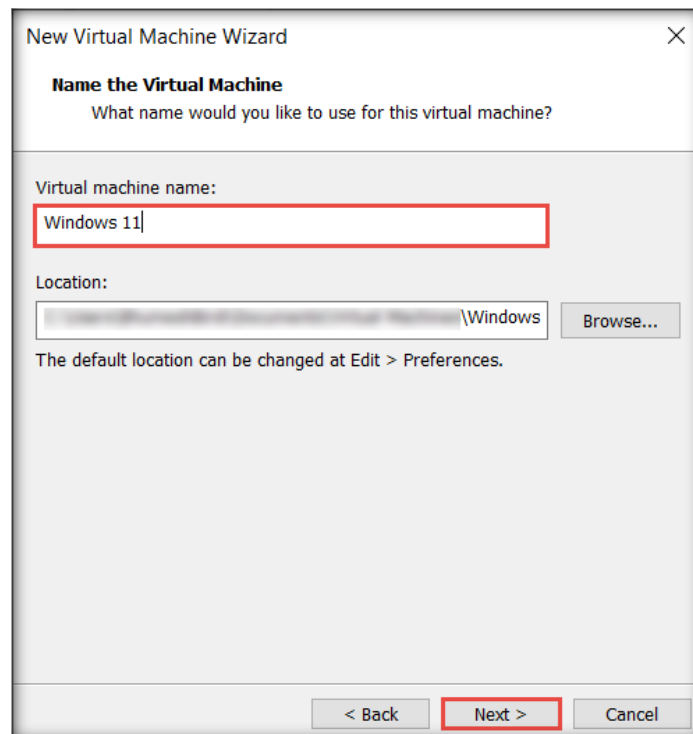
2. In the **New Virtual Machine Wizard** window, leave the settings to default (**Typical**) and click **Next**.
3. In the **Guest Operating System Installation** wizard, choose the **I will install the operating system later** radio button (if you have an ISO of **Windows 11**) and click **Next**.



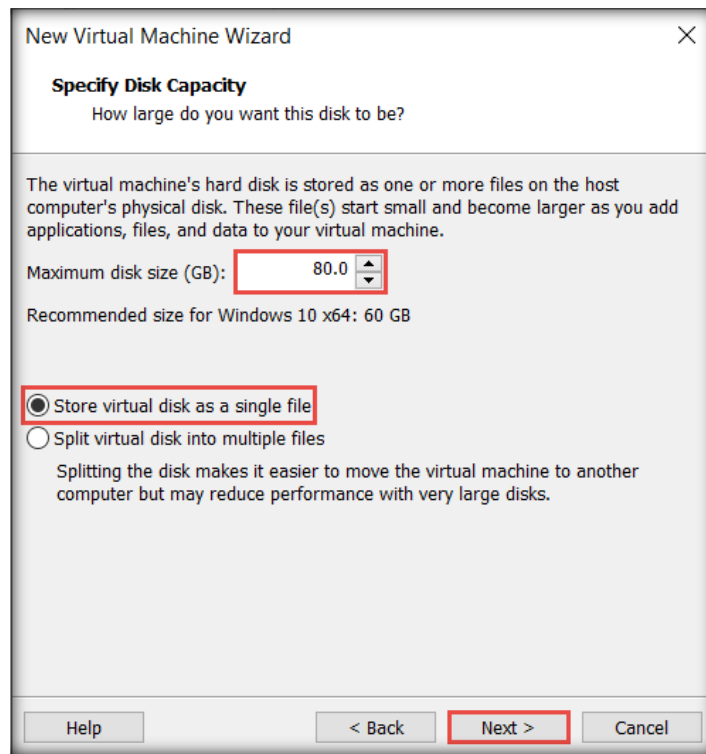
- In the **Select a Guest Operating System** wizard, ensure that the **Microsoft Windows** radio button is selected in the **Guest operating system** section and that **Windows 10 x64** is selected under **Version**. Click **Next**.



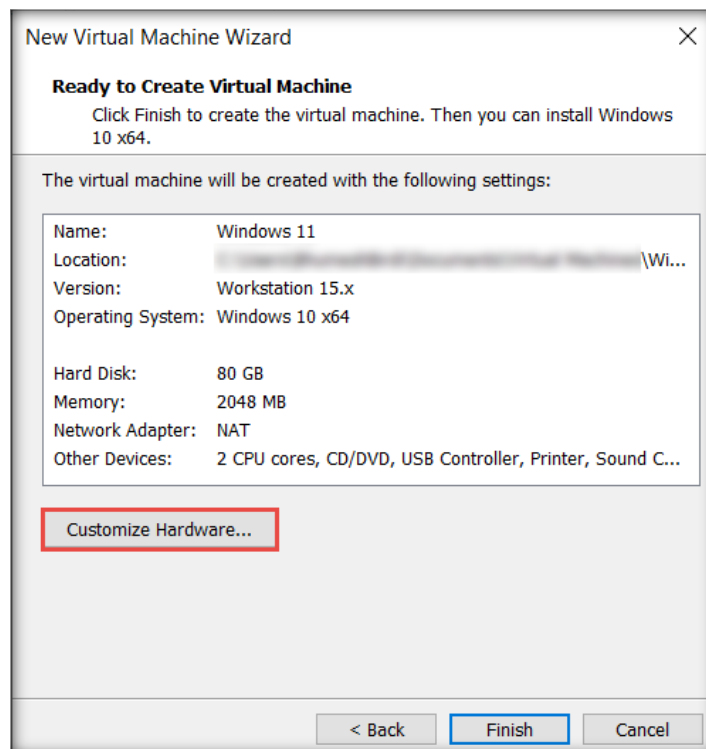
- The **Name the Virtual Machine** wizard appears; type **Windows 11** in the **Virtual machine name** field and click the **Browse** button to store the virtual hard disk. Choose your desired location to store the hard disk and then click **Next**.



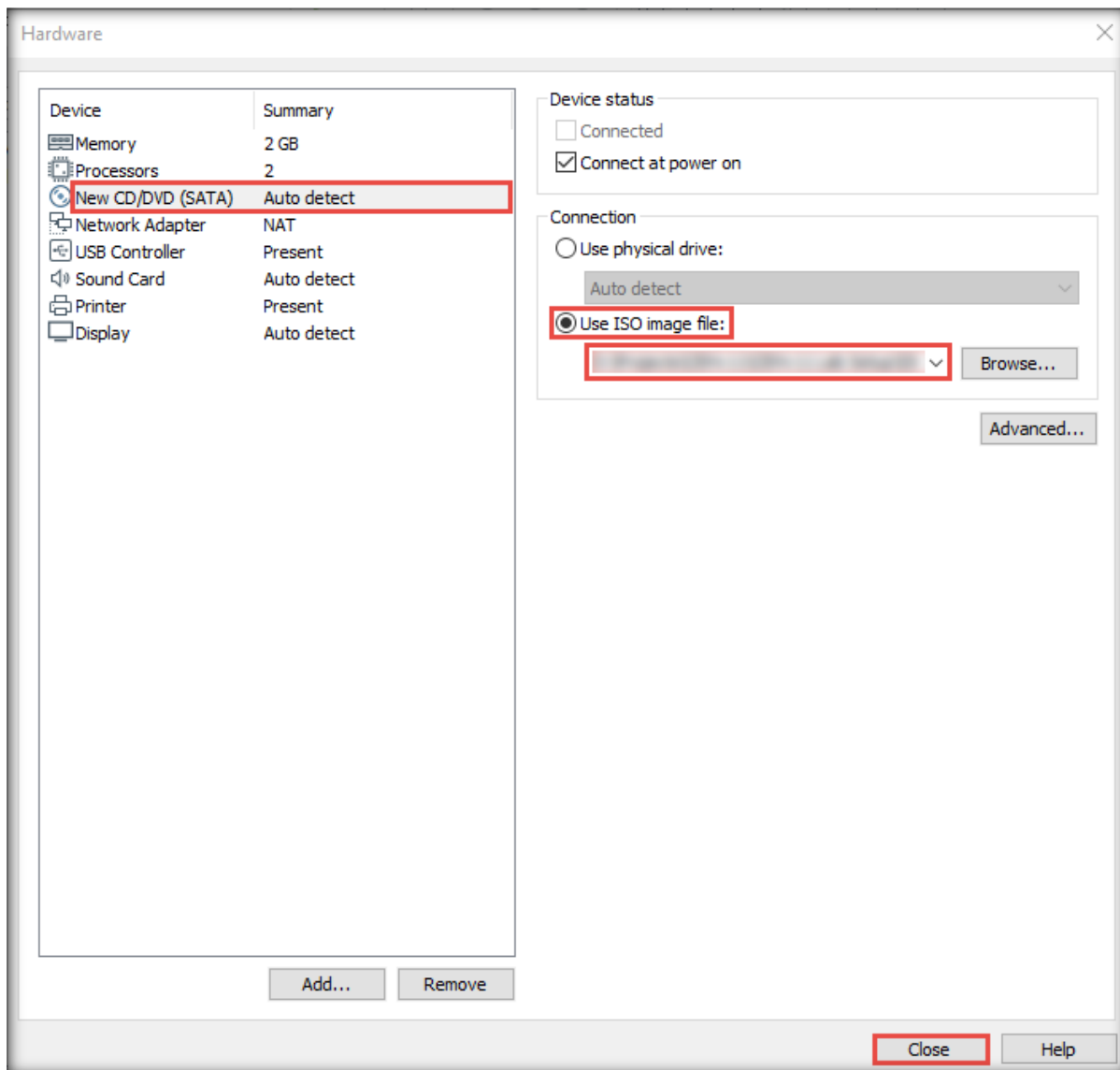
- The **Specify Disk Capacity** wizard appears. Leave the **Maximum disk size (GB)** to default (i.e., **80 GB**, recommended), select the **Store virtual disk as a single file** radio button, and click **Next**.



- The **Ready to Create Virtual Machine** wizard appears; confirm the settings and click the **Customize Hardware...** button.

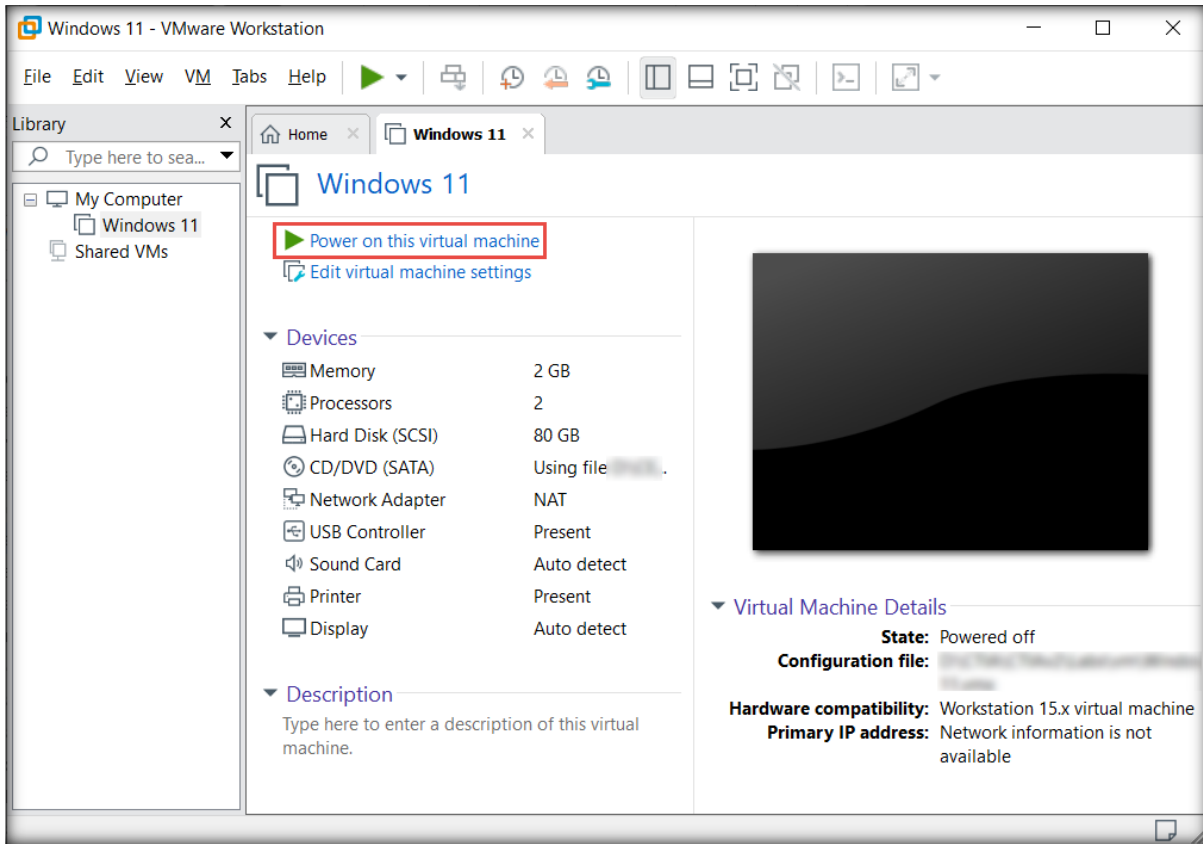


- The **Hardware** window appears; click the **New CD/DVD (SATA)** option from the left-hand pane. In the right-hand pane, select the **Use ISO image file** radio button and then click the **Browse...** button to provide the ISO path of Windows 11 ISO file. Click **Close**.

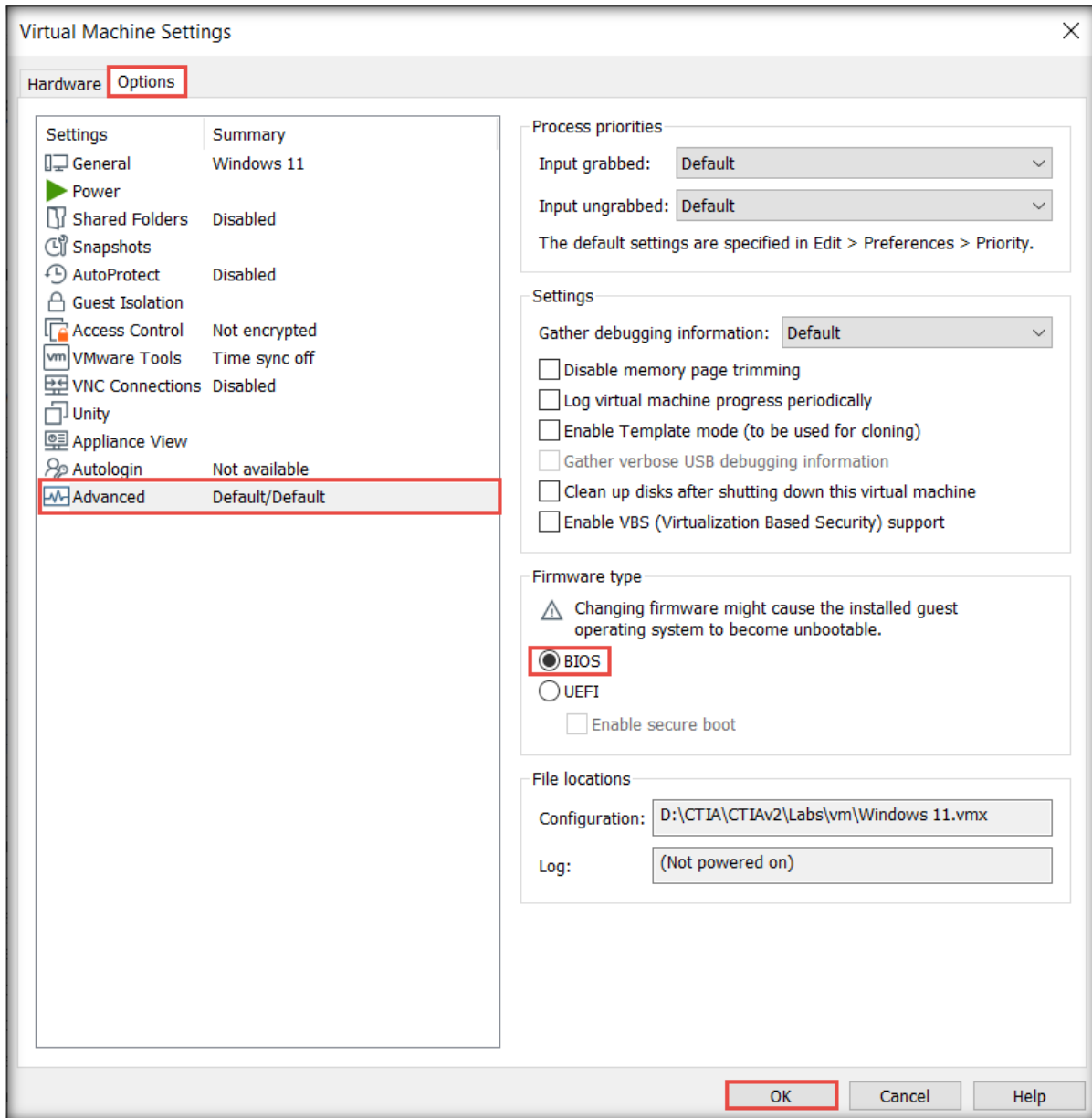


- In the **Ready to Create Virtual Machine** wizard, click **Finish**.

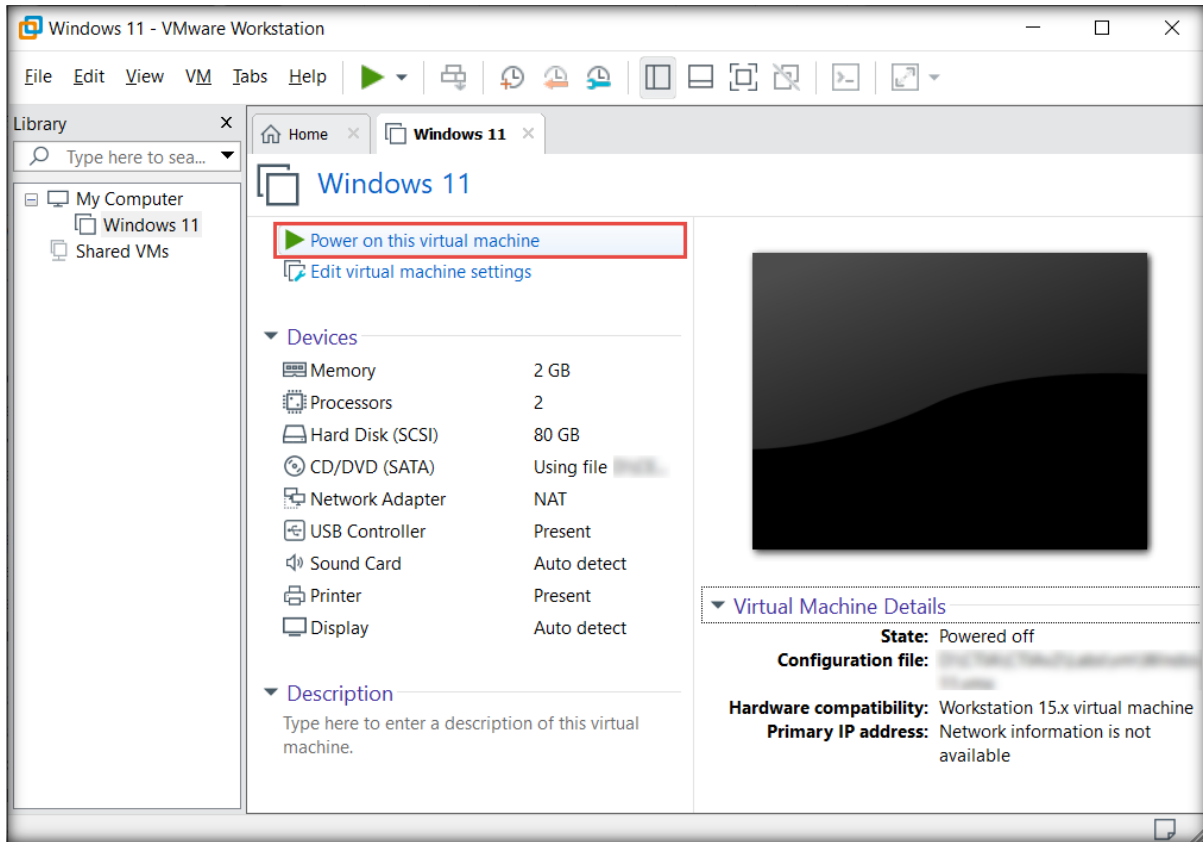
10. The **Windows 11** virtual machine appears; click the **Edit virtual machine settings** option.



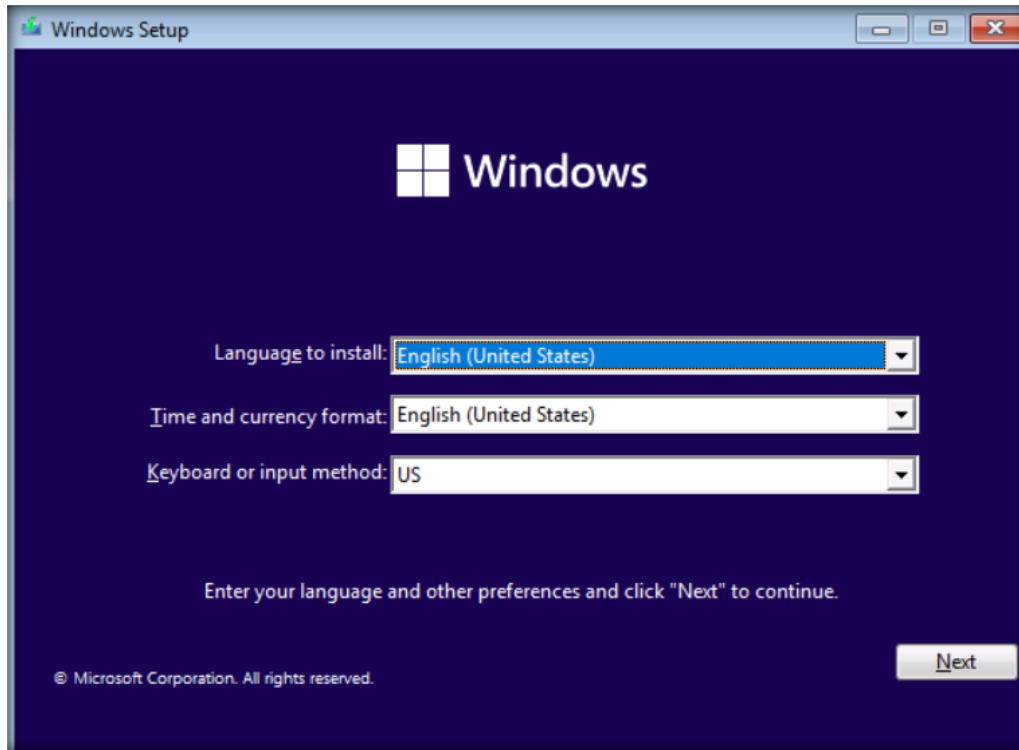
11. The **Virtual Machine Settings** window appears; click the **Options** tab.
12. In the **Options** tab, click the **Advanced** option from the left-hand pane.
13. Select the **BIOS** radio button under the **Firmware type** section in the **Advanced** options and click **OK**.



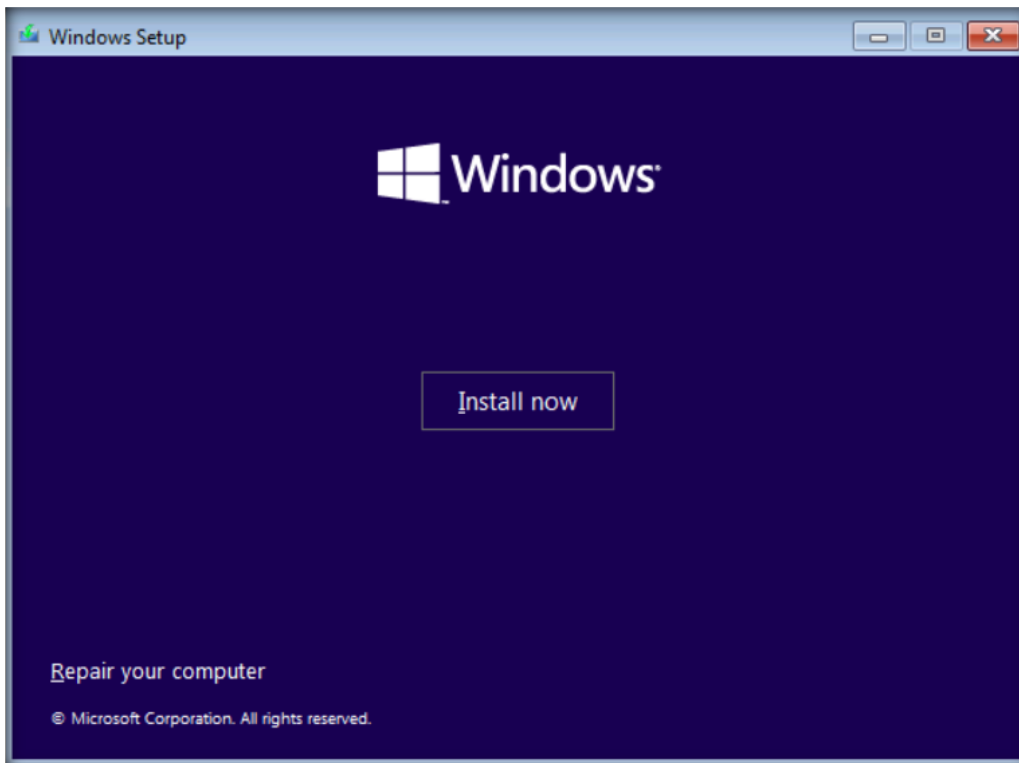
14. Click the **Power on this virtual machine** option to launch the **Windows 11** virtual machine.



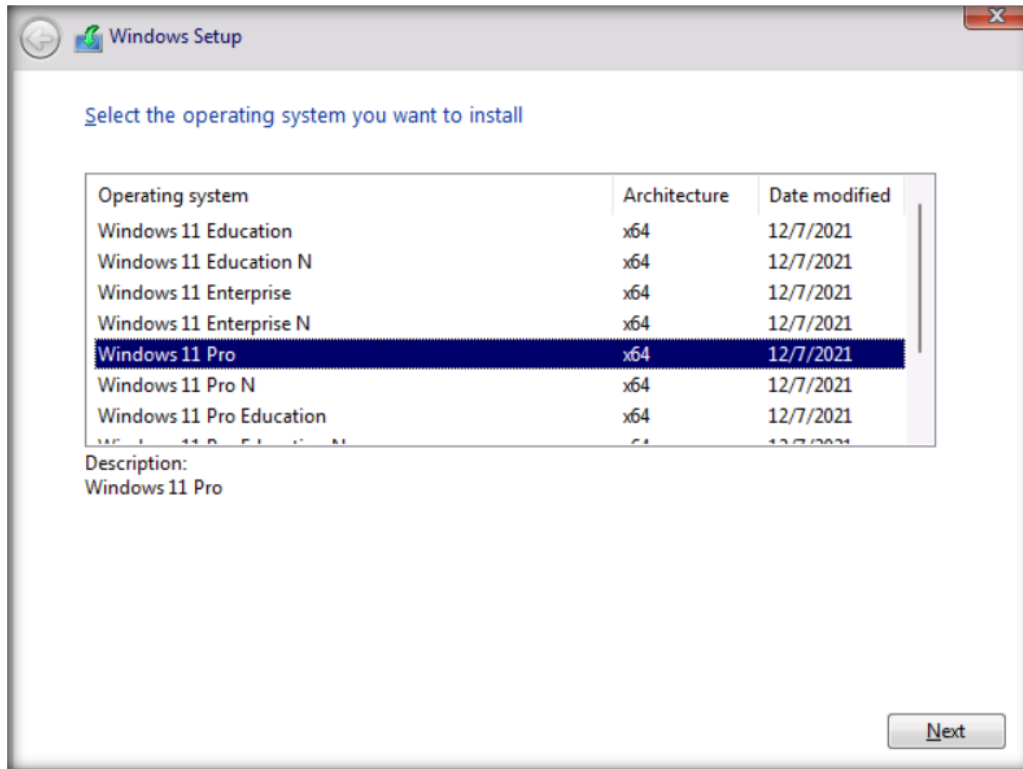
15. The virtual machine initializes, and the **Windows Setup** window appears. In the first window of the setup, leave the default settings and click **Next**.



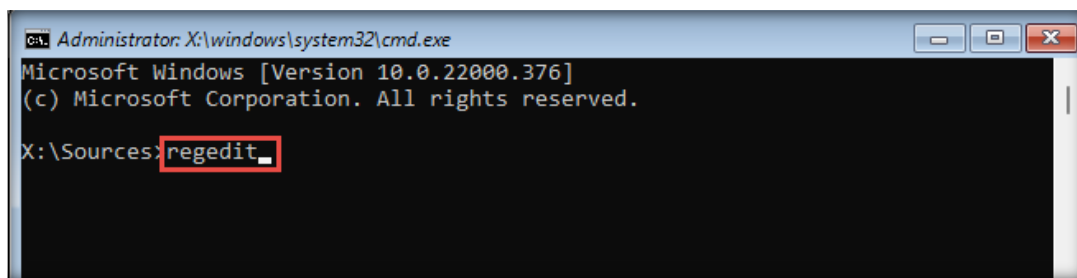
16. In the next window, click the **Install now** button to begin the installation.



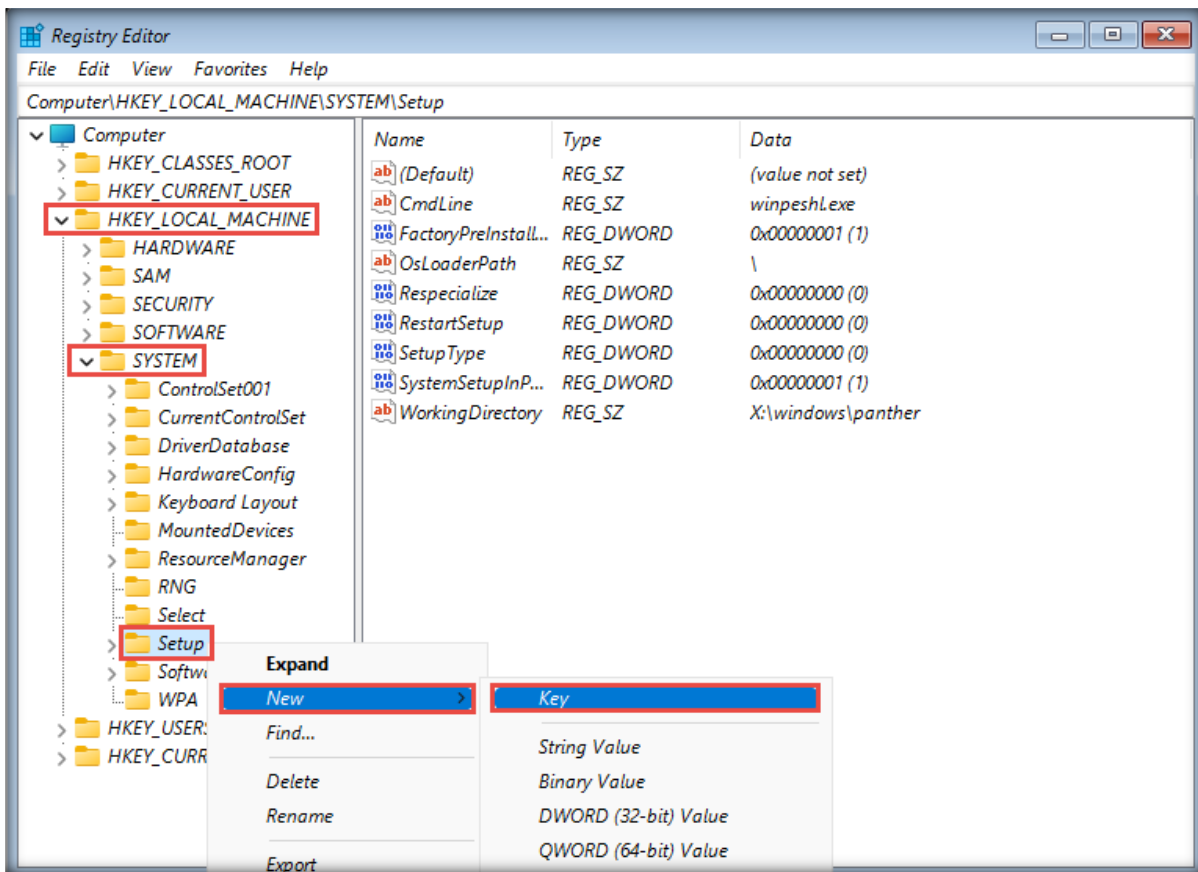
17. In the **Select the operating system you want to install** wizard, select **Windows 11 Pro** and click **Next**.



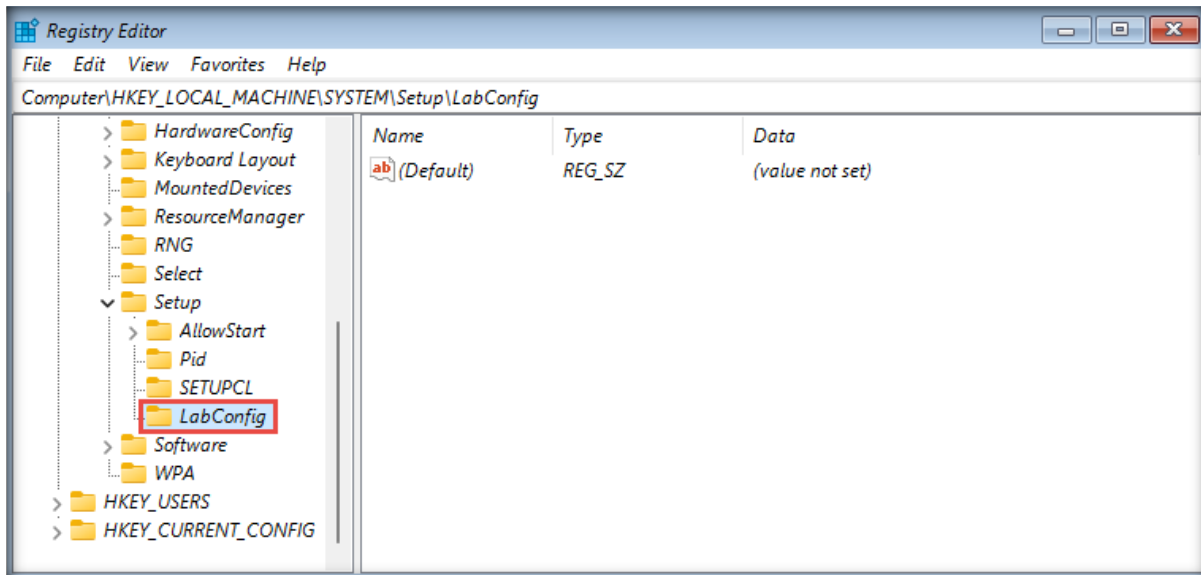
18. If **This PC can't run Windows 11** error appears, follow the below steps:
- Press **Shift+F10** and a **Command Prompt** window appears.
 - In the **Command Prompt** window, type **regedit** and press **Enter**.



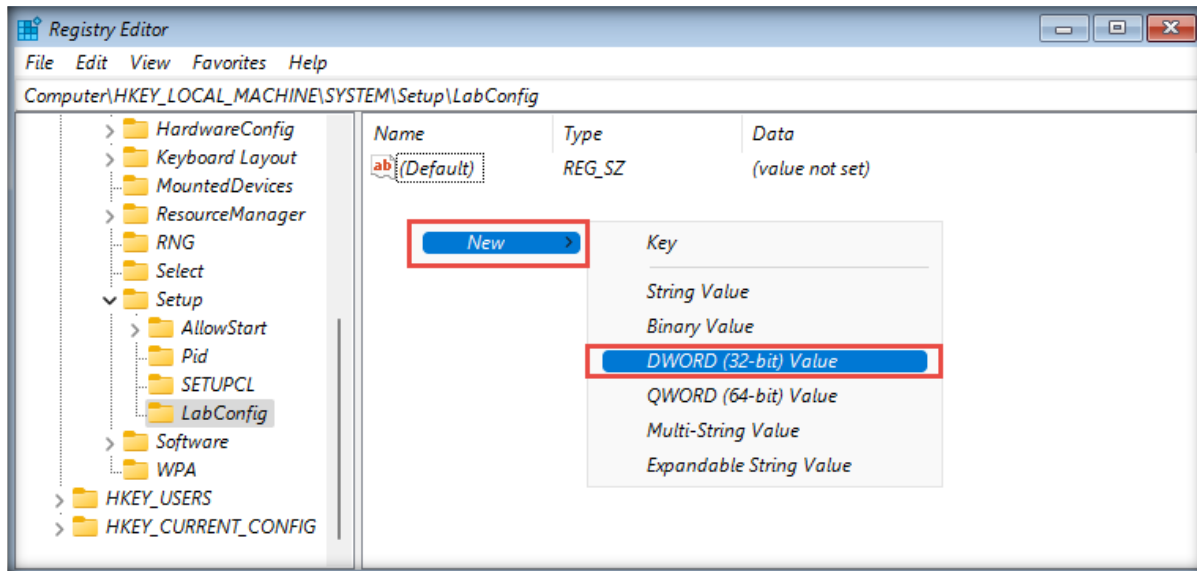
- The **Registry Editor** window appears, from the left-pane navigate to **HKEY_LOCAL_MACHINE** → **SYSTEM**. Right-click **Setup** node and navigate to **New** → **Key**.



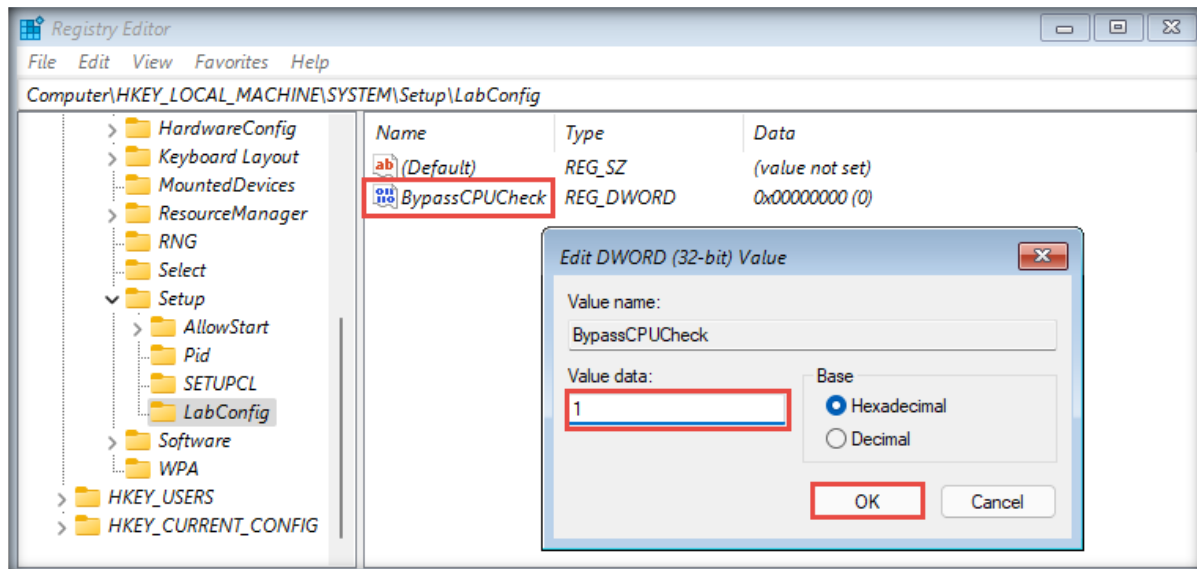
- A new key has been created, rename it as **LabConfig** and press **Enter**.



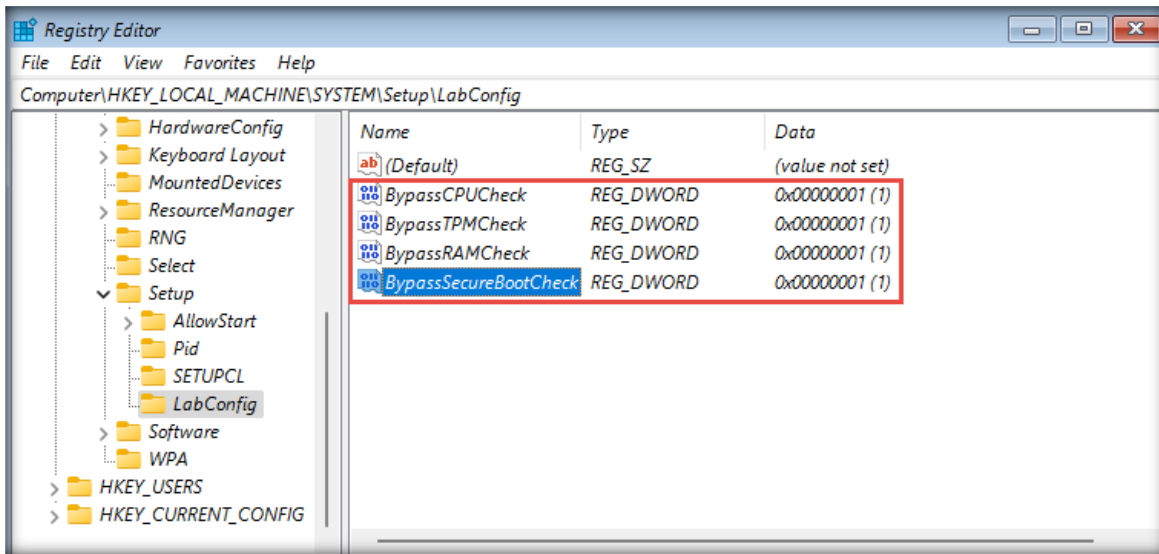
- Right-click anywhere in the right pane and navigate to **New** → **DWORD (32-bit) Value**.



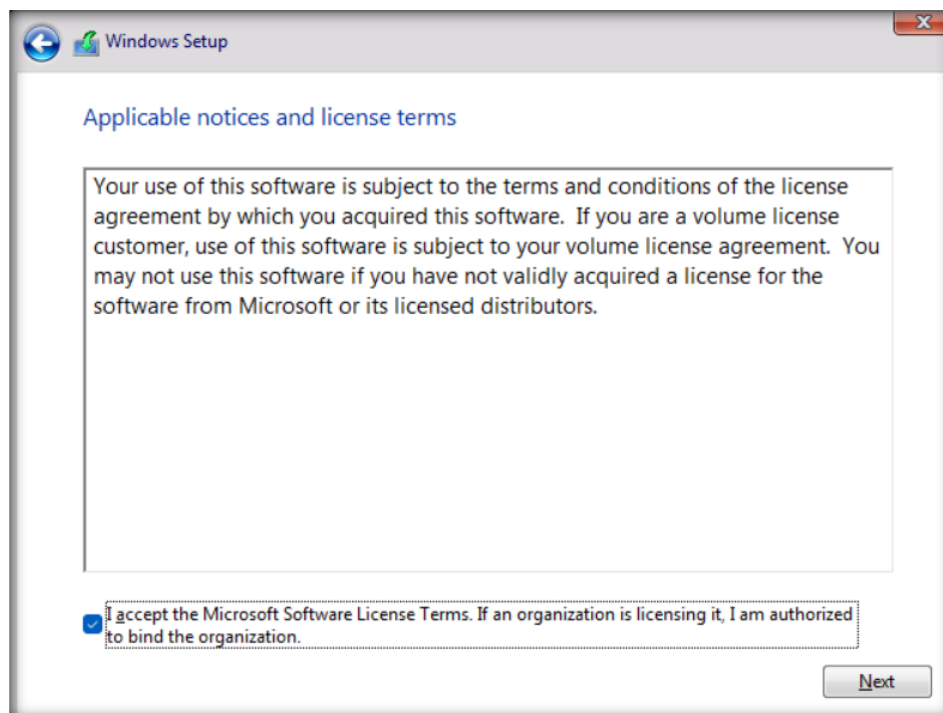
- Rename the value as **BypassCPUCheck** and press **Enter**.
- Now, right-click **BypassCPUCheck** value and select **Modify...** option.
- **Edit DWORD (32-bit Value)** pop-up appears, change the **Value data** to **1** and click **OK**.



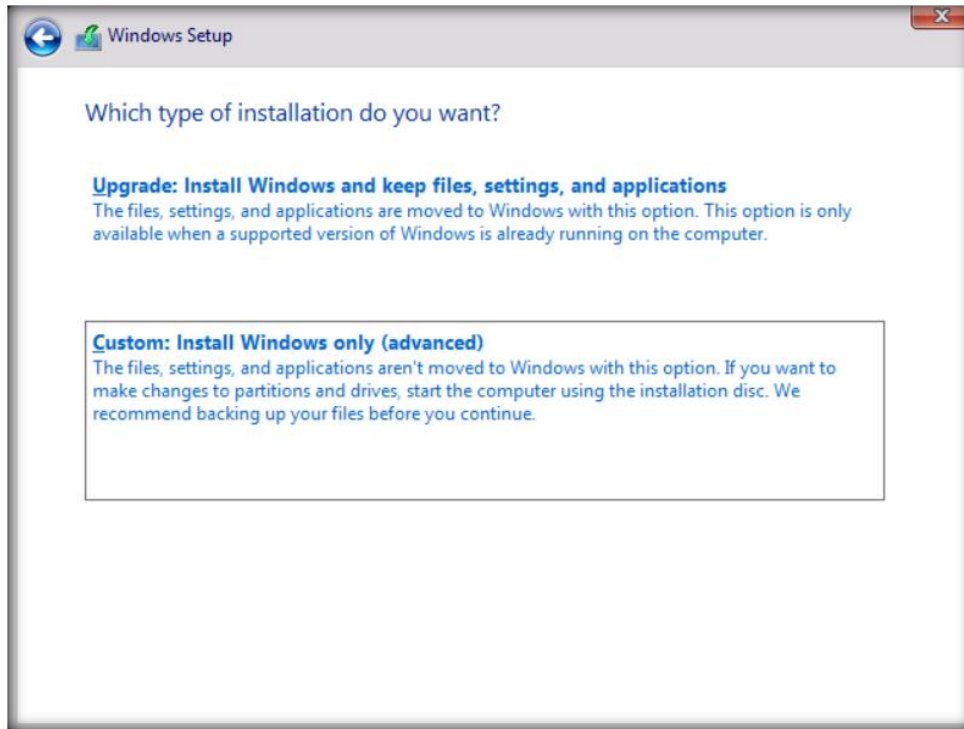
- Similarly, create **BypassTPMCheck**, **BypassRAMCheck**, and **BypassSecureBootCheck** values (for each value, set **Value data=1**).



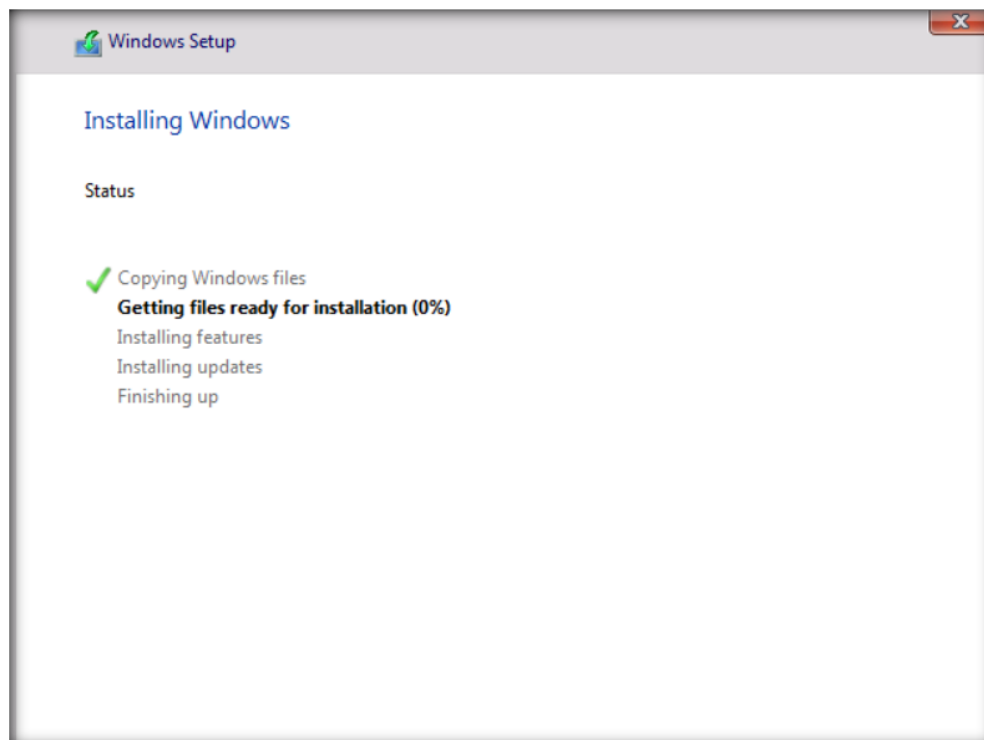
- Now, close all the windows (Registry Editor, Command Prompt and Error window).
 - In **Windows Setup** window, click **Yes**.
 - Click **Install Now** button.
19. The **Select the operating system you want to install** wizard appears again; select **Windows 11 Pro** and click **Next**.
 20. **Applicable notices and license terms** wizard appears, accept the license terms by clicking on **I accept...** checkbox and click **Next**.



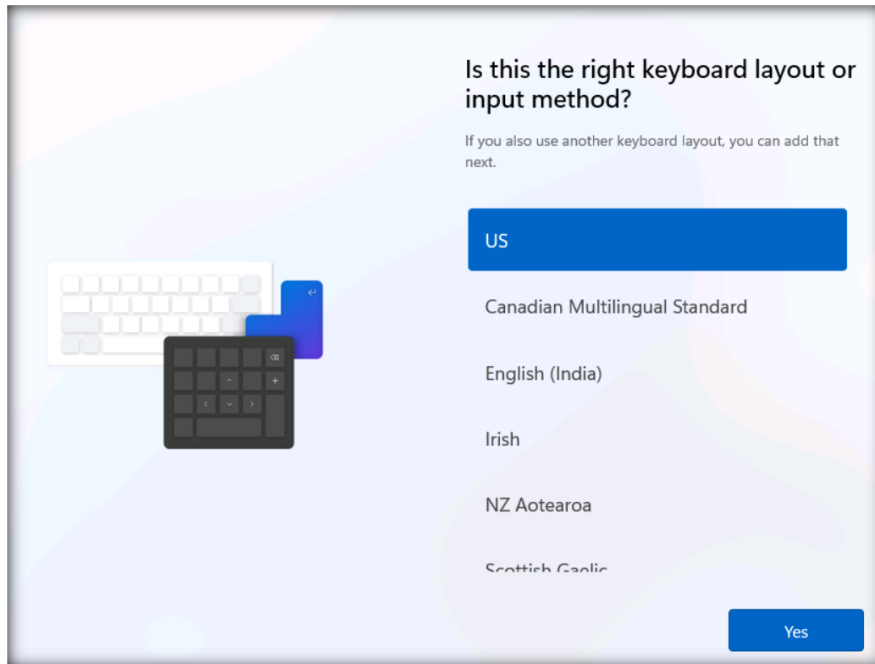
21. In the **Which type of installation do you want?** wizard, click the **Custom: Install Windows only (advanced)** option.



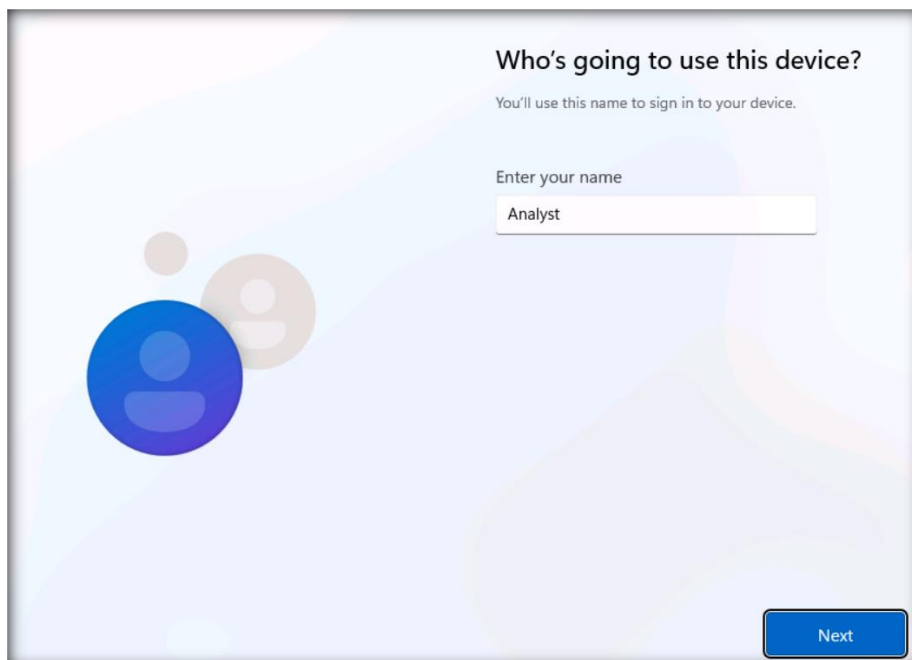
22. In the **Where do you want to install Windows?** wizard, click **Next**.
23. The installation of the Windows 11 operating system begins. The machine restarts once the installation has completed.

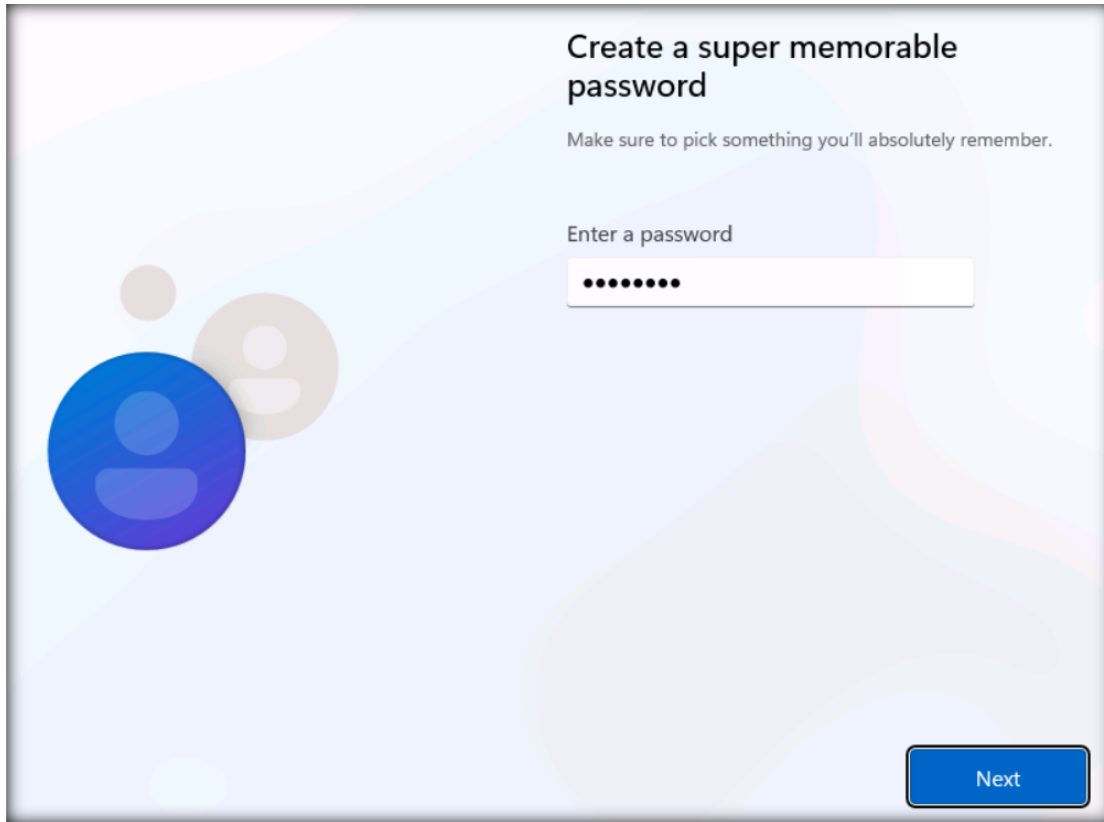


24. After completing the installation, an **Is this the right country or region?** wizard appears. Select your country and click **Yes**.
25. Similarly, select the preferred keyboard layout (here, **US**) in the next wizard and click **Yes**.



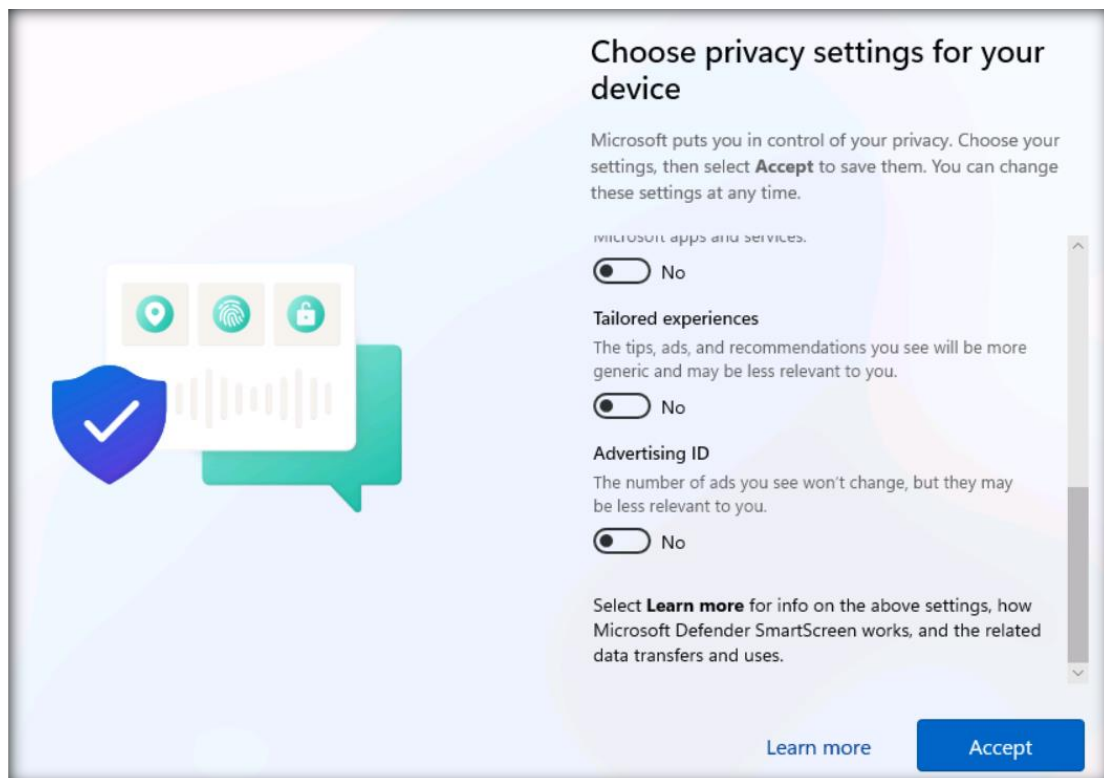
26. Skip the second keyboard option.
27. In the next wizard, select **Continue with limited setup**.
28. In the **Who's going to use this device?** wizard, enter **Analyst** and click **Next**. In the next wizard, set **Pa\$\$w0rd** as the password and click **Next**. Similarly, in the **Confirm password** wizard, enter the same password and click **Next**.



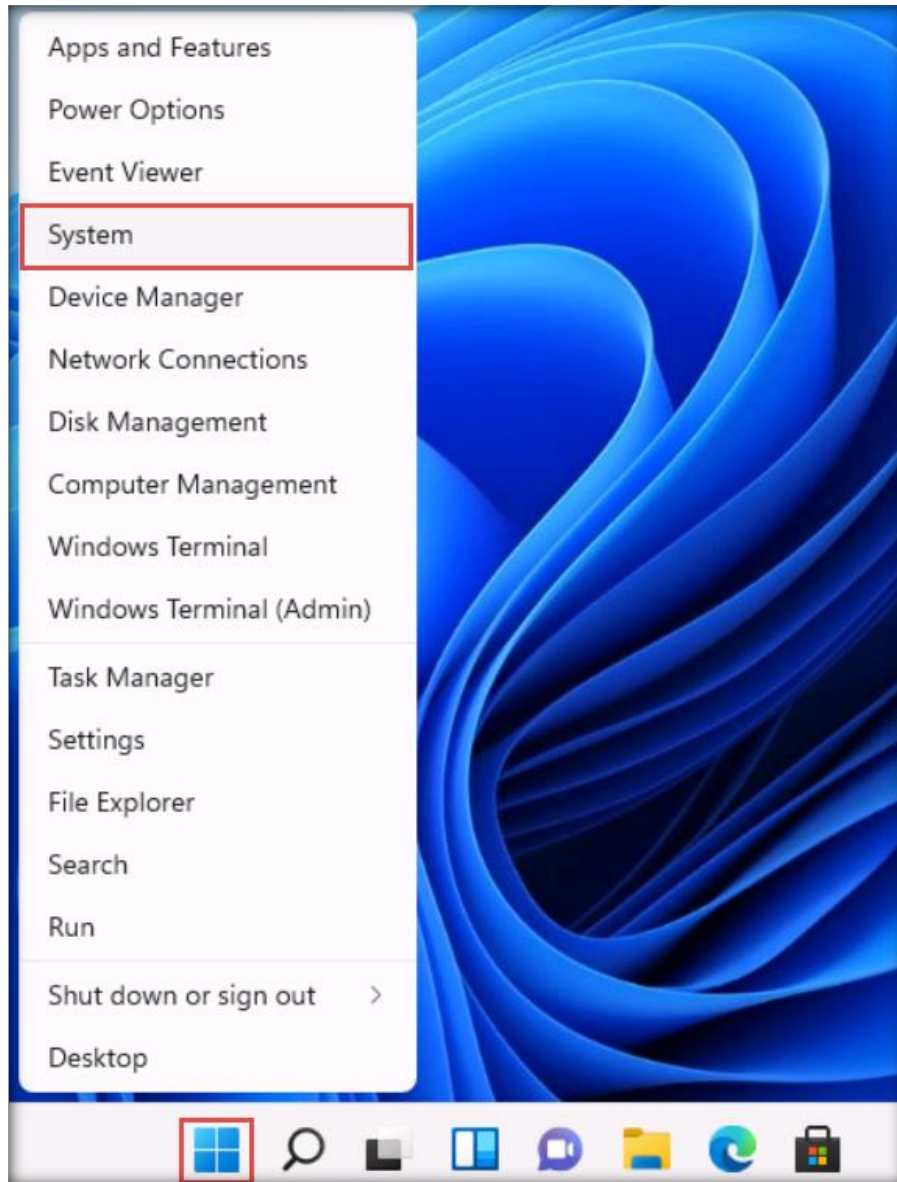


29. Add security questions in the next wizards.

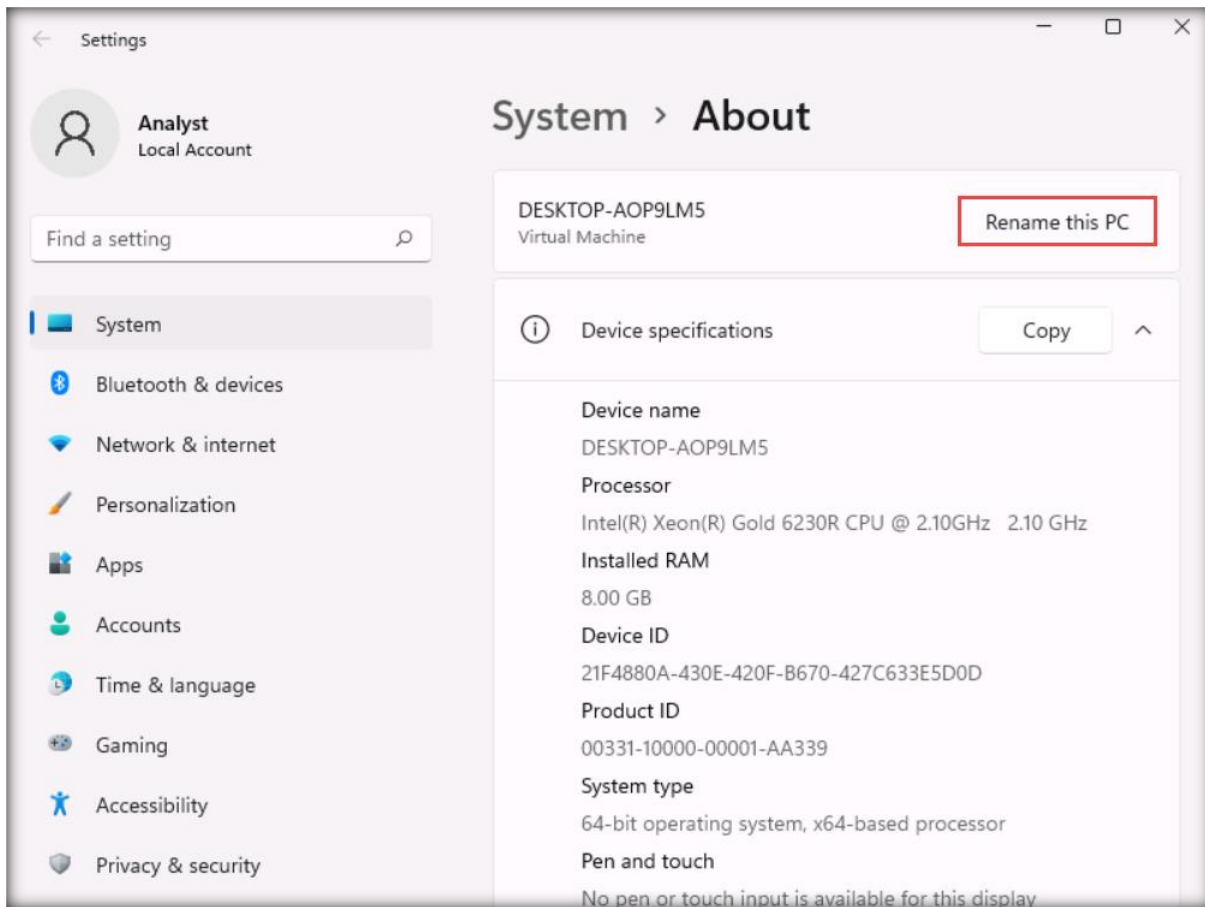
30. In the **Privacy settings** wizard, disable all the options and click **Accept**.



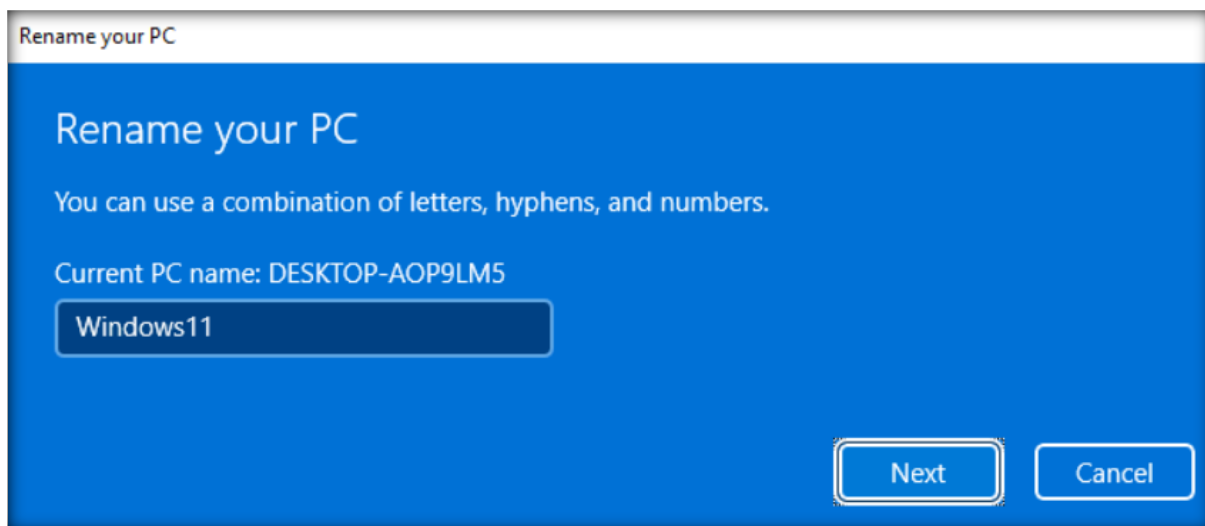
31. After Windows initializes, if an app window appears, close it.
32. Right-click on the **Start** icon and select **System** option from the list.



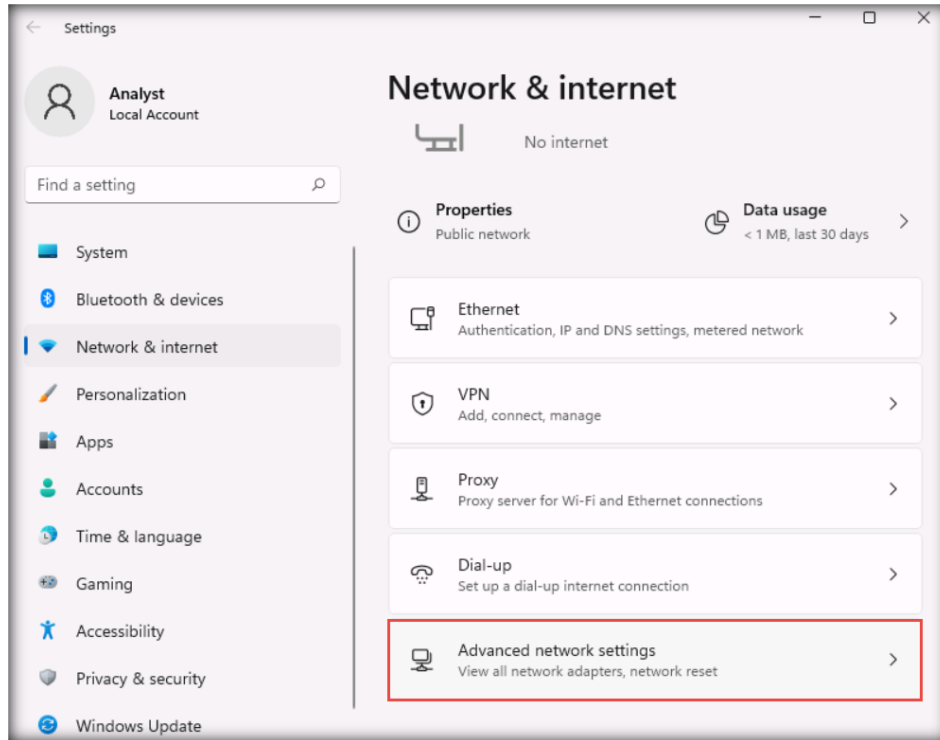
33. The **Settings** window appears, click **Rename this PC** button in the right pane.



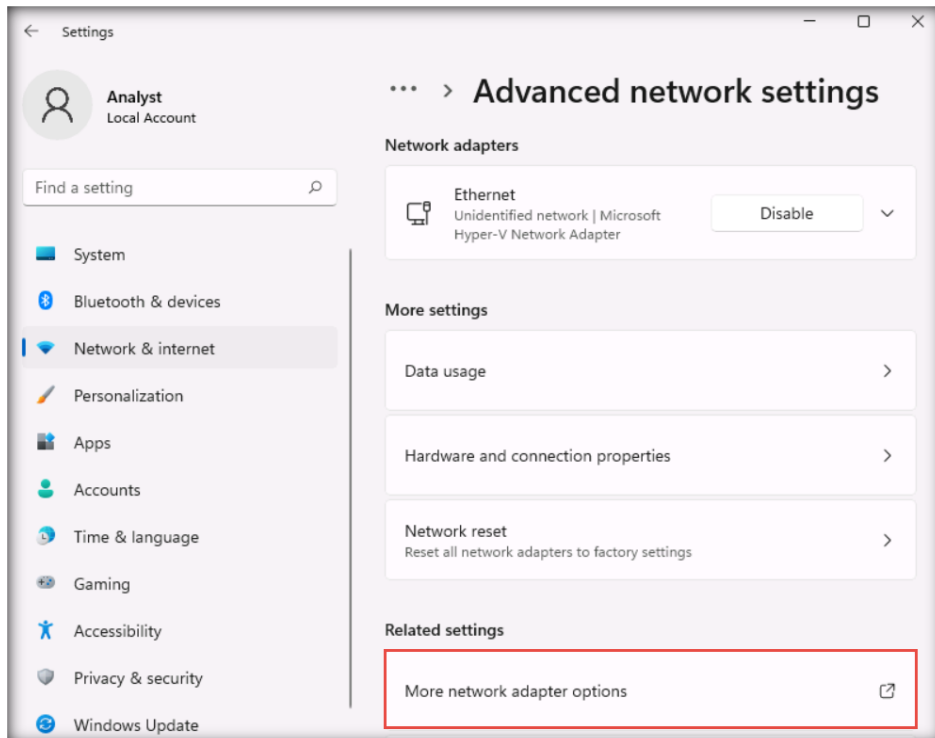
34. The **Rename your PC** pop-up window appears; type **Windows11** in the box and click **Next**.



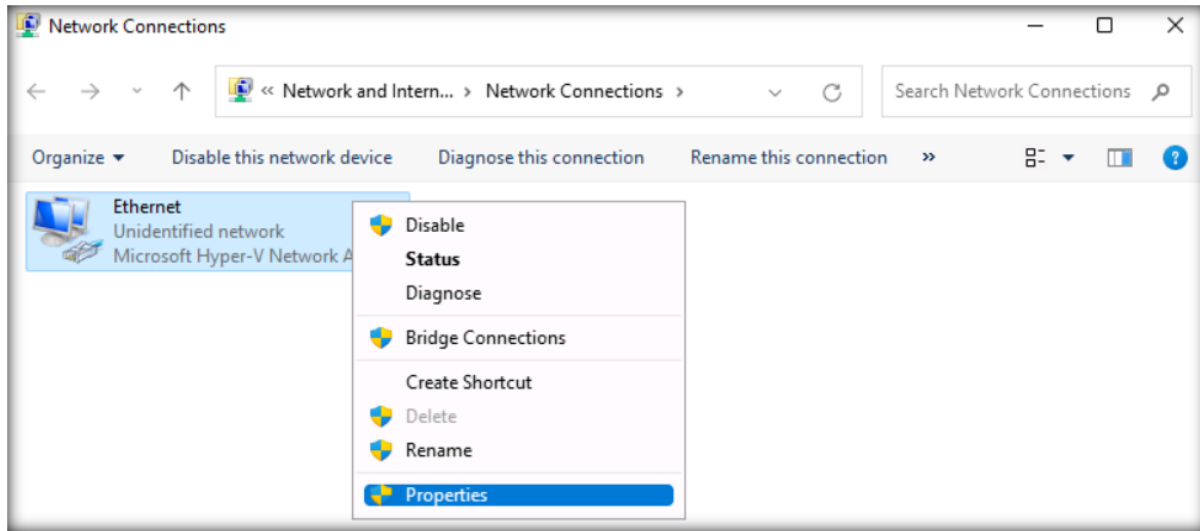
35. After the renaming process, click **Restart now** to apply the changes.
36. After the virtual machine restarts, log in to the virtual machine with the credentials **Analyst** and **Pa\$\$wOrd**. Open the **Network and Internet Settings** and select the **Advanced network settings**.



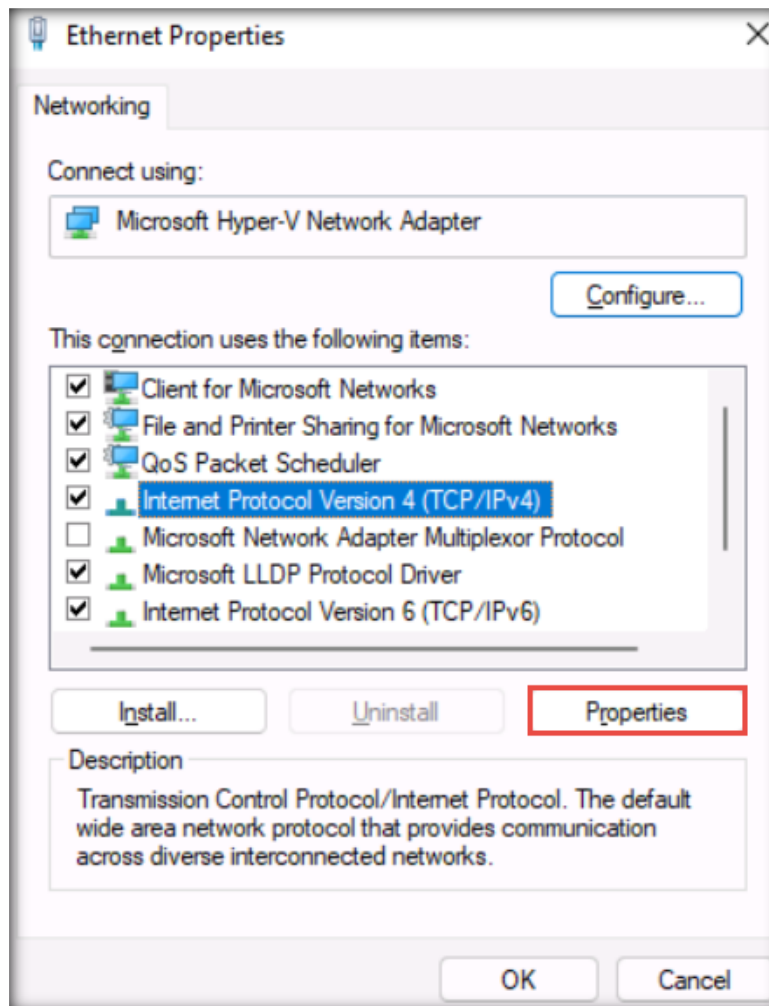
37. In the **Advanced network settings** window, select **More network adapter options**.



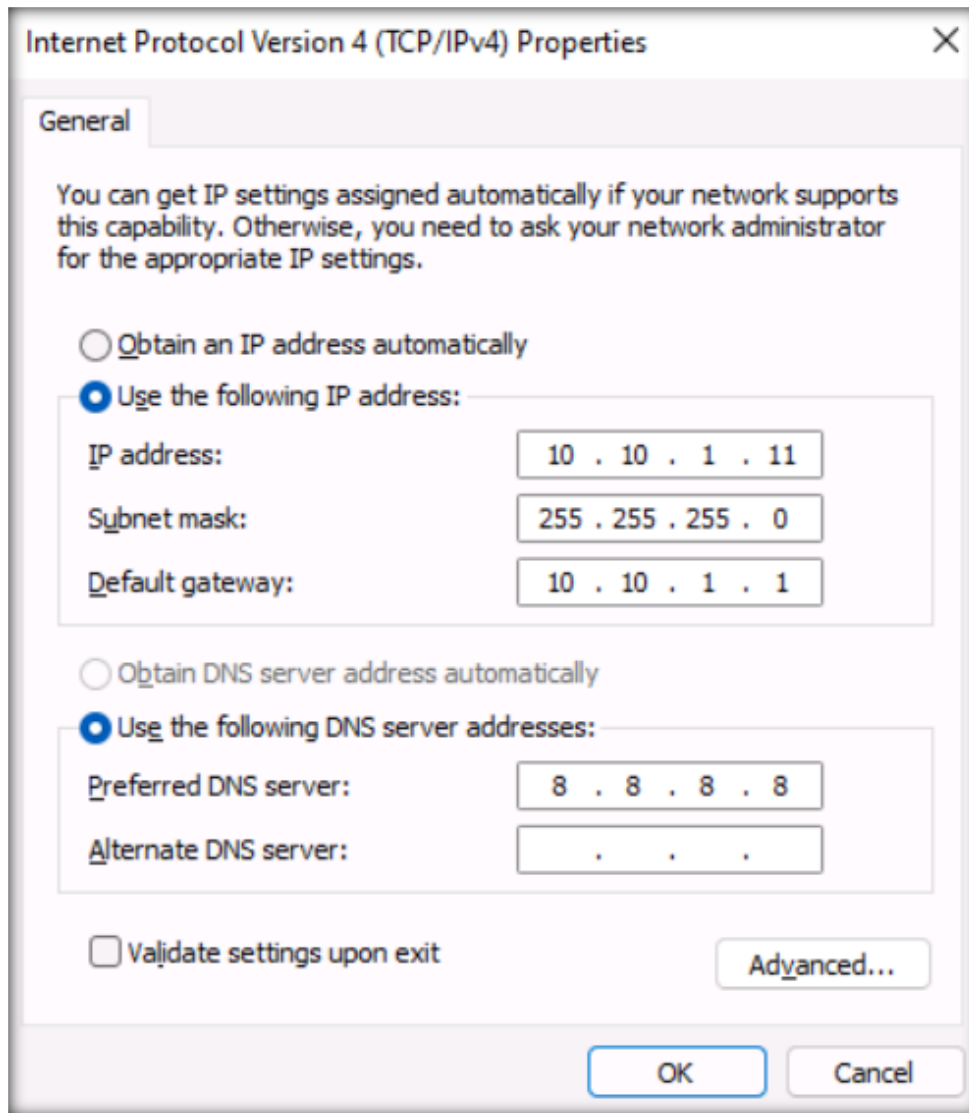
38. The **Network Connections** window appears. Right-click the network interface (here, **Ethernet**) and click **Properties**.



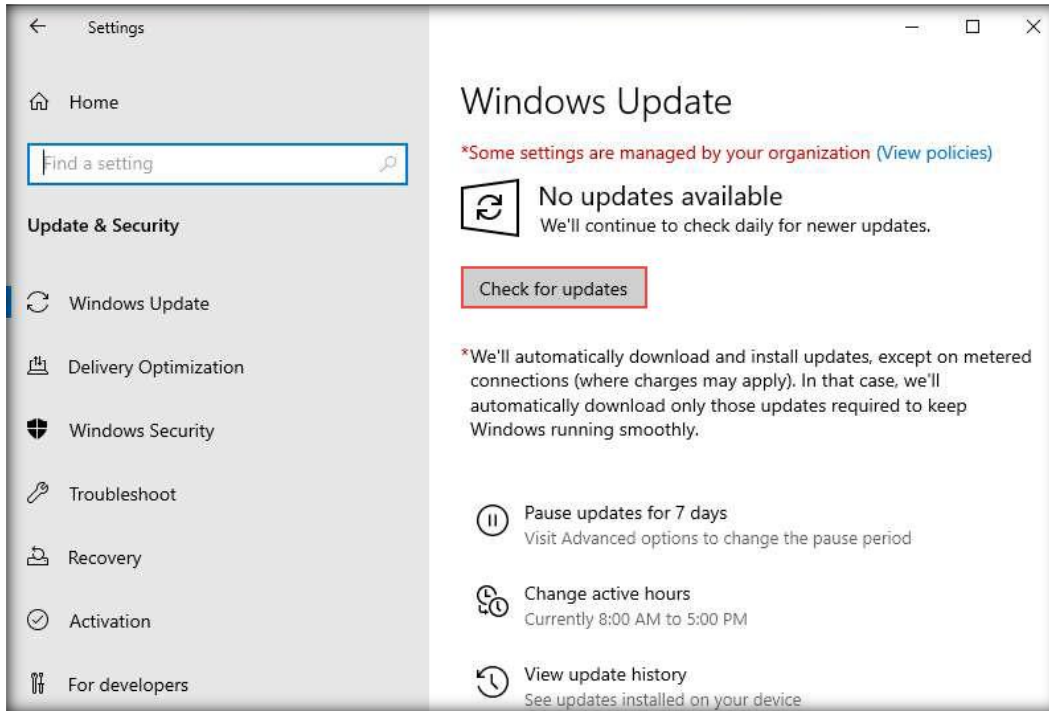
39. The **Ethernet Properties** window appears. Scroll down the list, select **Internet Protocol Version 4 (TCP/IPv4)**, and click on **Properties**.



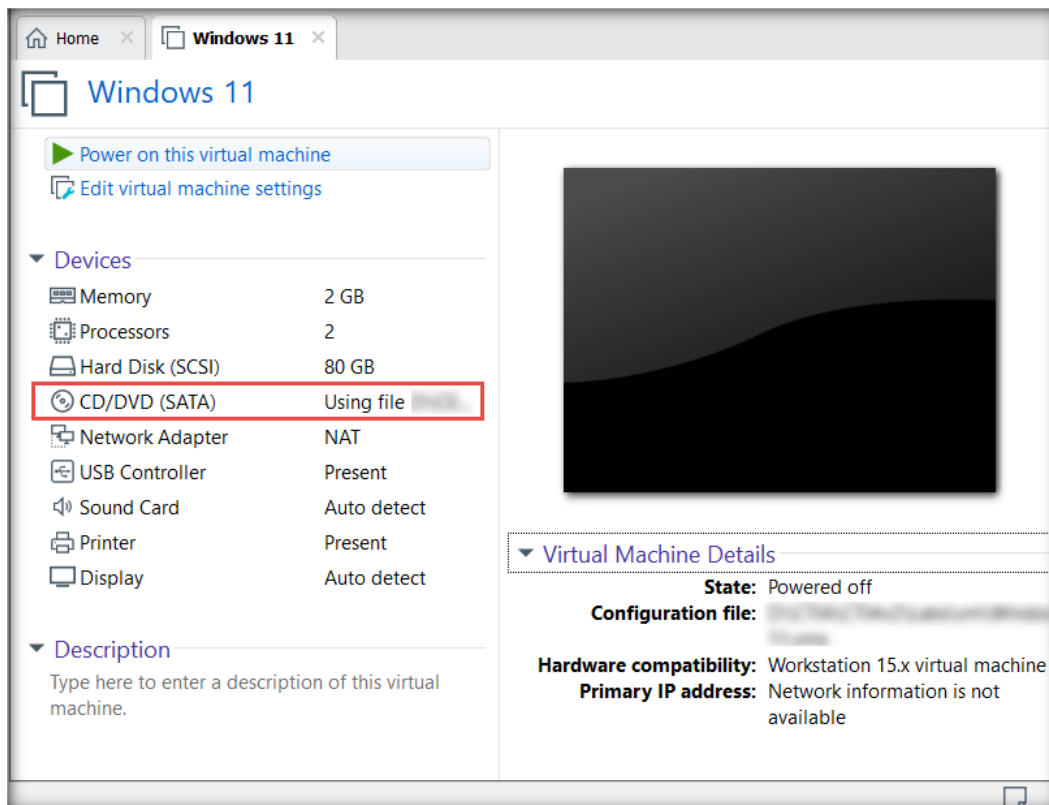
40. Select the **Use the following IP address** radio button. Assign **10.10.1.11** as the **IP address**, **255.255.255.0** as the **Subnet mask**, and **10.10.1.1** as the **Default gateway**.
41. Assign **8.8.8.8** as the **Preferred DNS server** address and click **OK**.



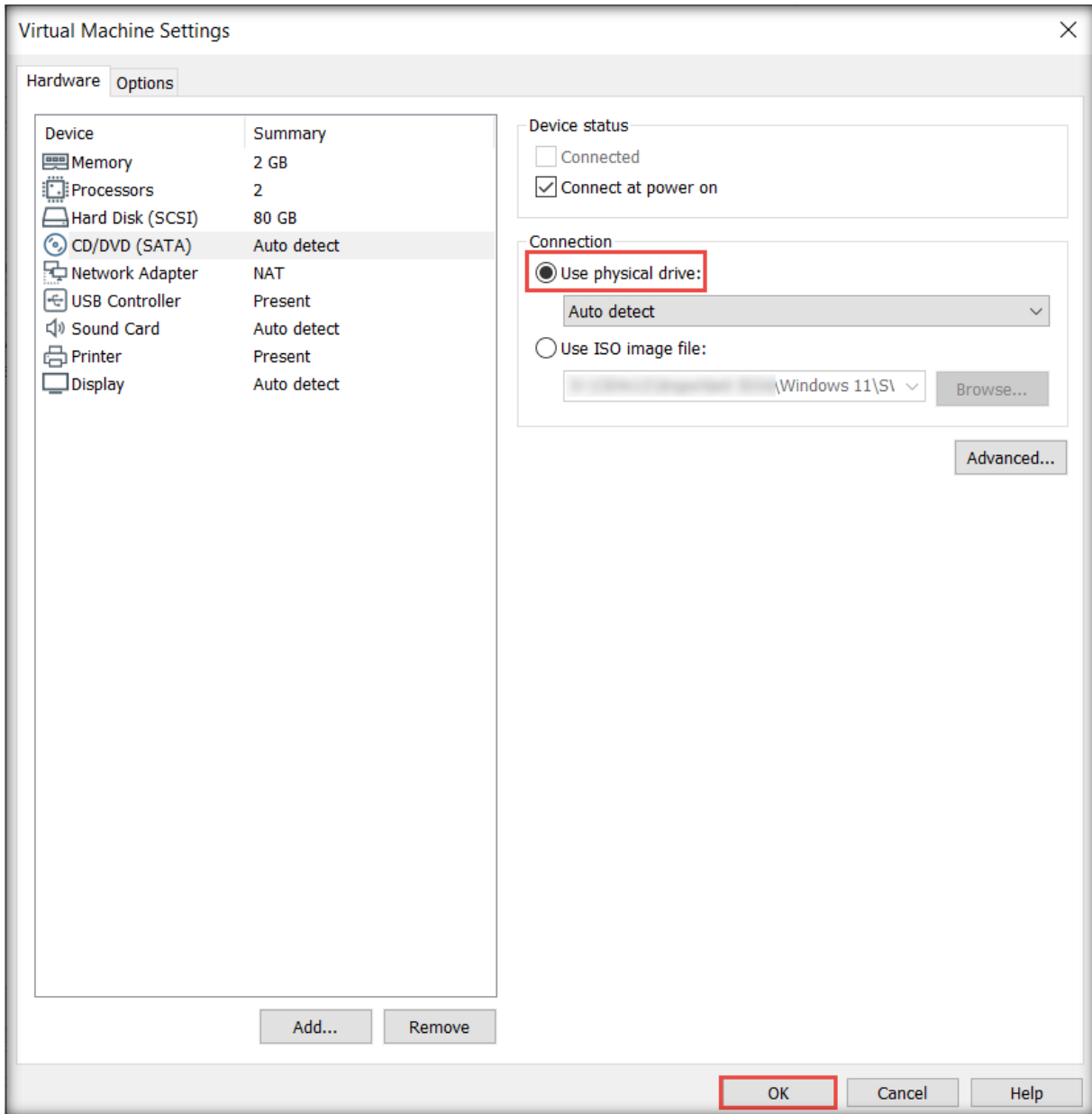
42. **Close** the **Ethernet Properties** window; then, close all open windows.
43. Right-click the **Windows** button in the lower-left corner of the screen and click **Settings**.
44. In the **Settings** window, click **Update & Security**.
45. Click **Check for updates** from the right-hand pane.



46. Check for and install the latest updates.
47. After installing all the updates, restart the machine.
48. Turn off the virtual machine. In the **Devices** section of the **Windows 11** tab, click **CD/DVD (SATA)**.



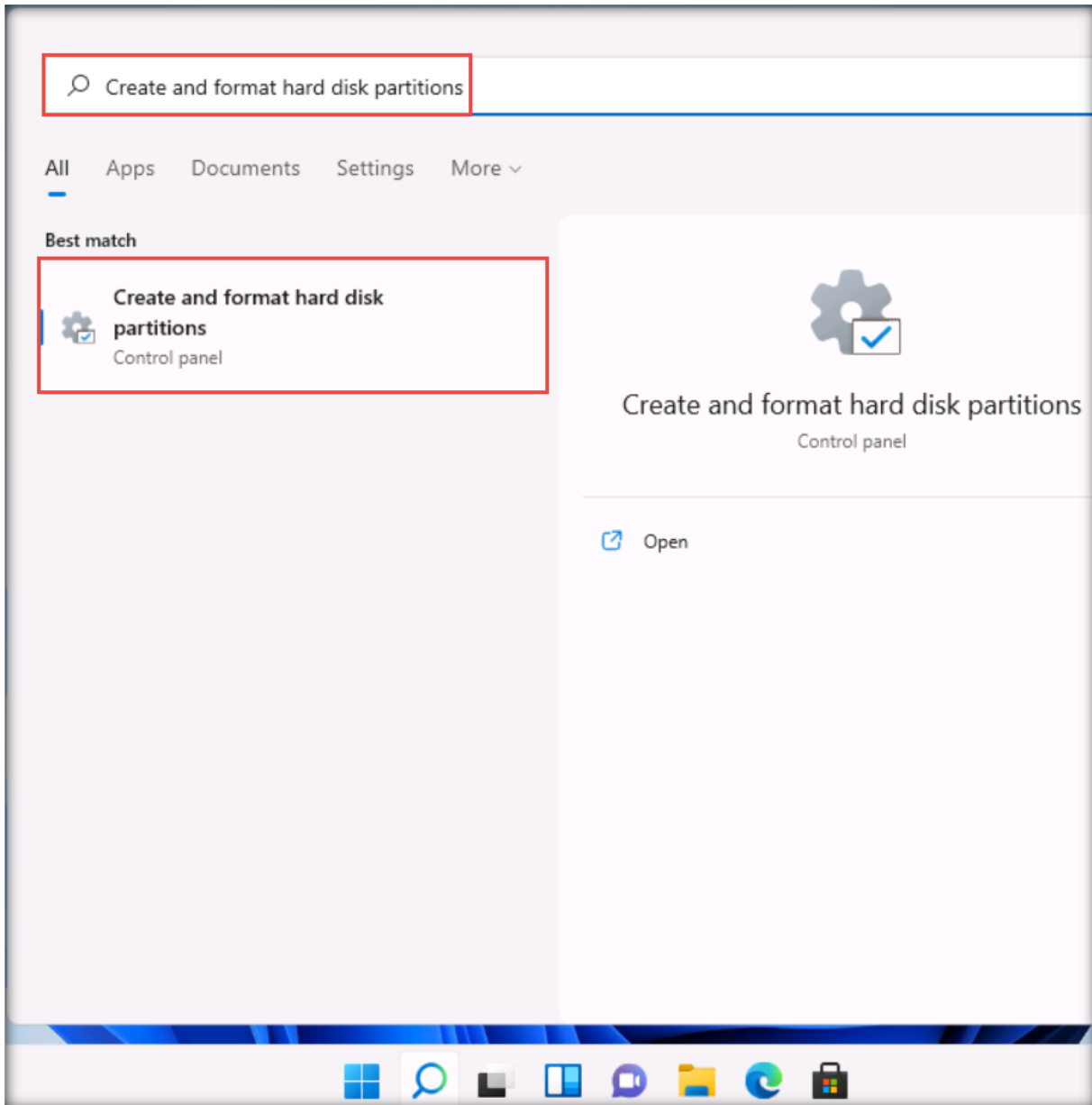
49. The **Virtual Machine Settings** window appears; choose the **Use physical drive:** radio button in the **Connection** section and click **OK**.



[\[Back to Configuration Task Outline\]](#)

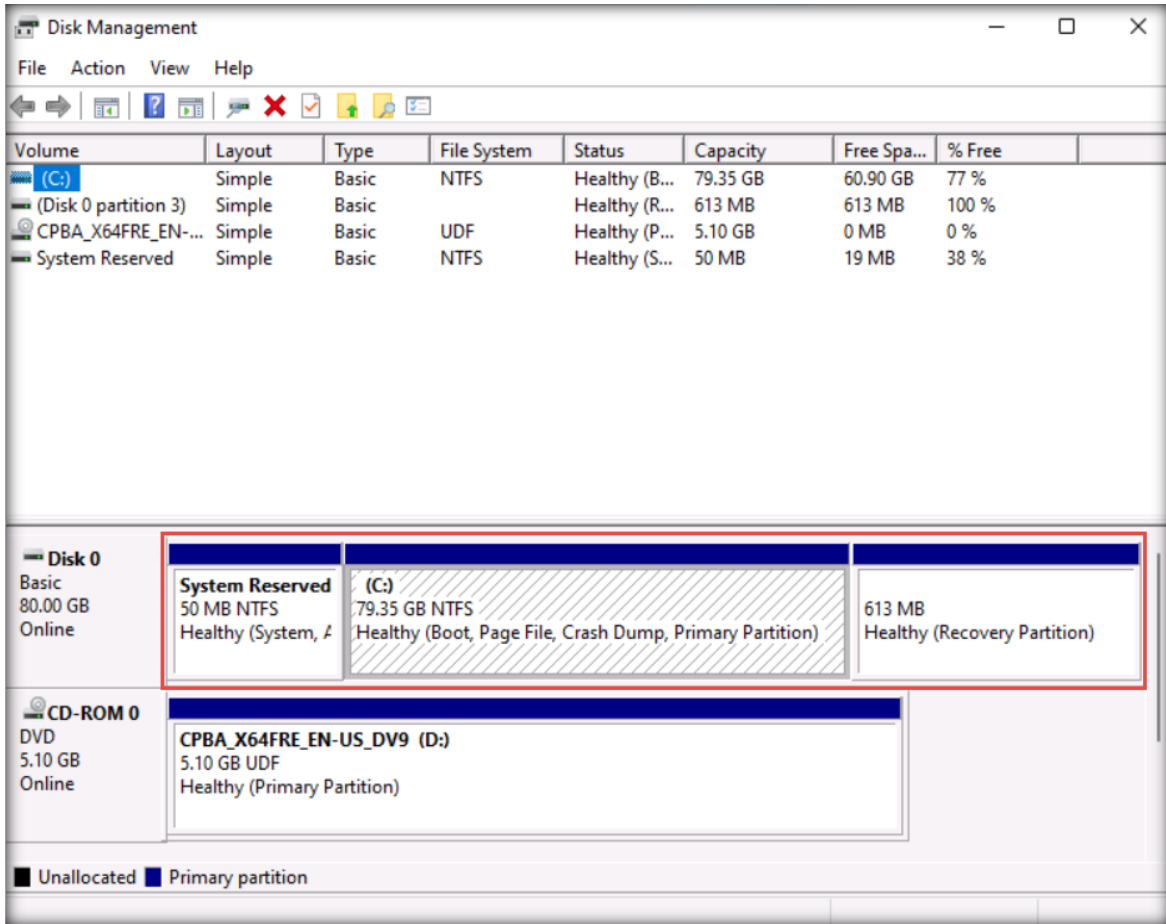
CT#8: Create a Partition in the Windows 11 Virtual Machine

1. In the search bar, type **create and format hard disk partitions** and select **Create and format hard disk partitions** from the search results.

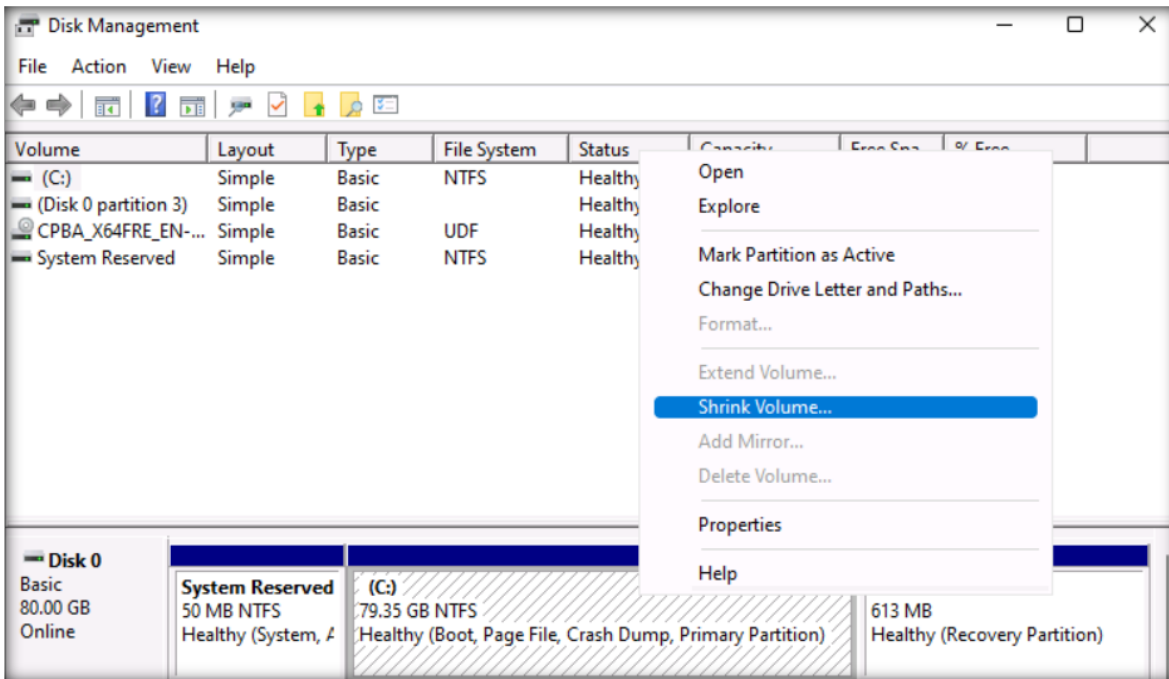


2. This will display the current disk partition, as shown in the screenshot below.

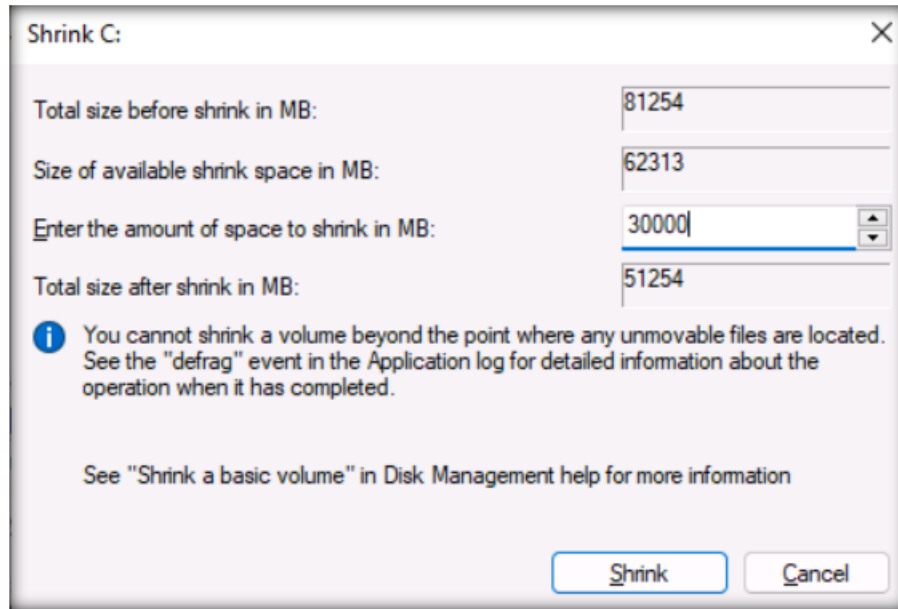
Note: While creating the Windows 11 virtual machine, we allocated a disk space of 80 GB. Here, we will create the partitions **E:** with a disk space of 30 GB, respectively.



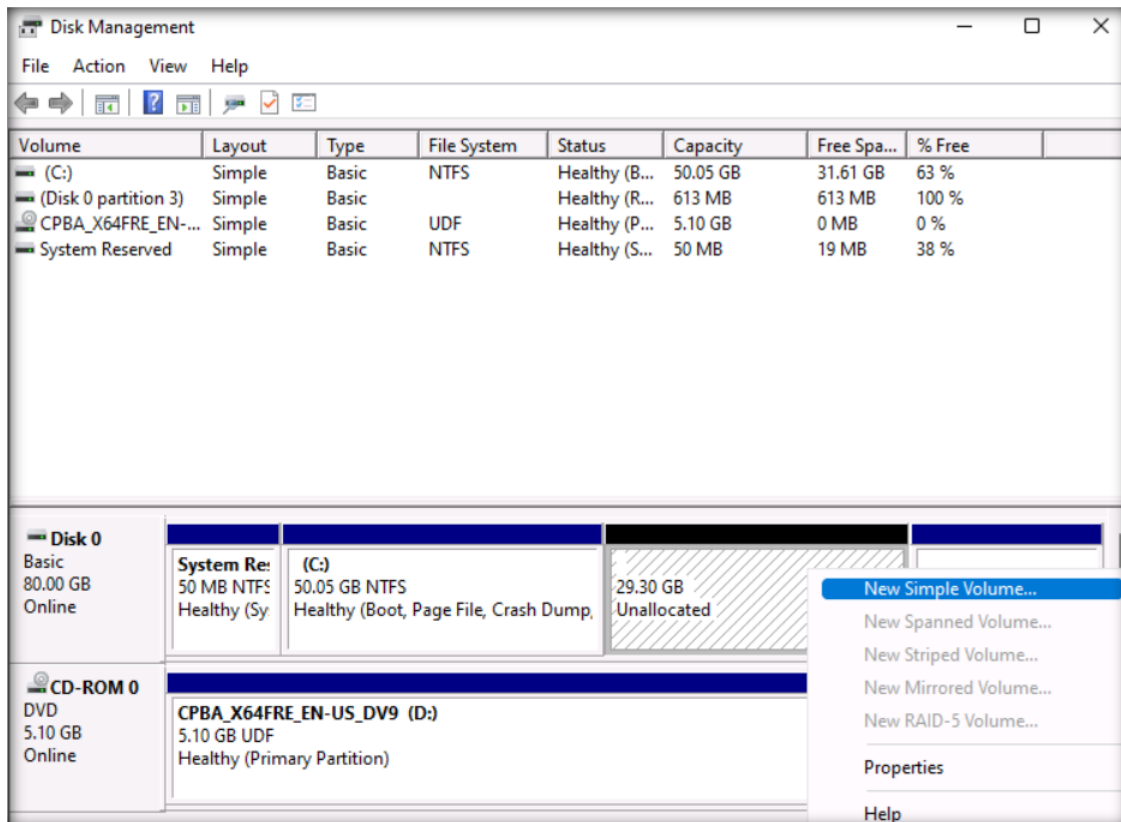
3. Select the drive from the middle pane (here, **C:**). Right-click the selected drive and click **Shrink Volume...**



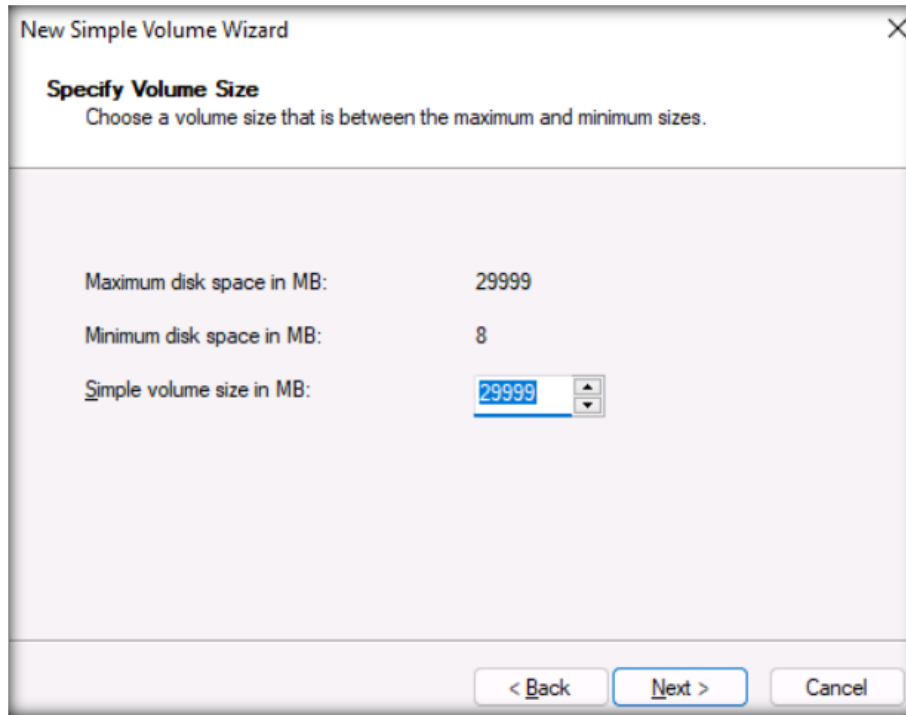
4. A **Shrink C:** window appears, showing the available shrink space. Enter **250000** (i.e., 250 GB) in the **Enter the amount of space to shrink in MB:** field and click **Shrink**.



5. The **Disk Management** window will display the newly created unallocated disk partition in the middle pane.
6. Select the **Unallocated** drive from the middle pane, right-click the selected drive, and click **New Simple Volume...**

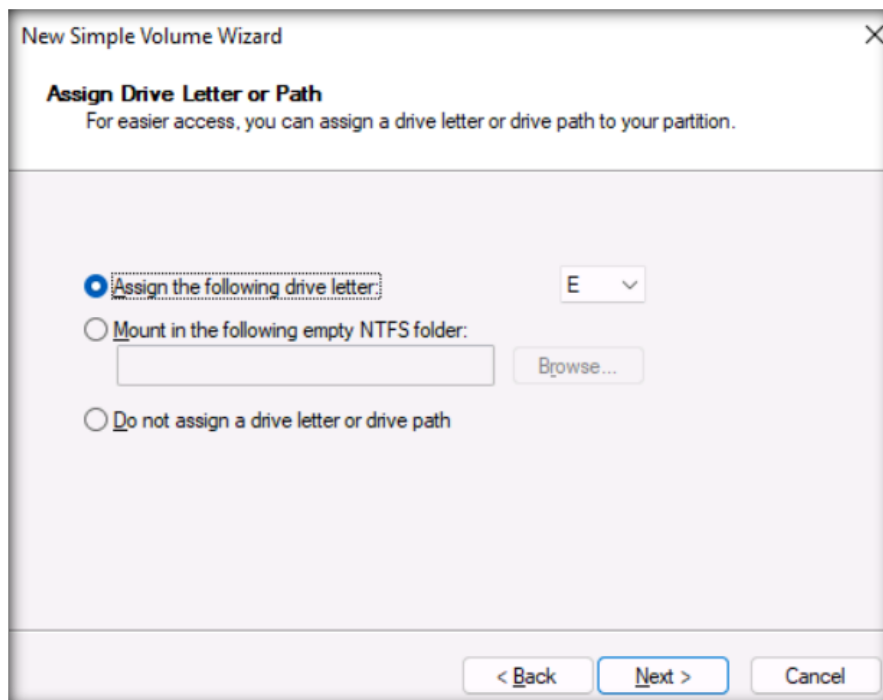


7. The **New Simple Volume Wizard** window appears; click **Next**.
8. In the **Specify Volume Size** wizard, leave the default settings and click **Next**.

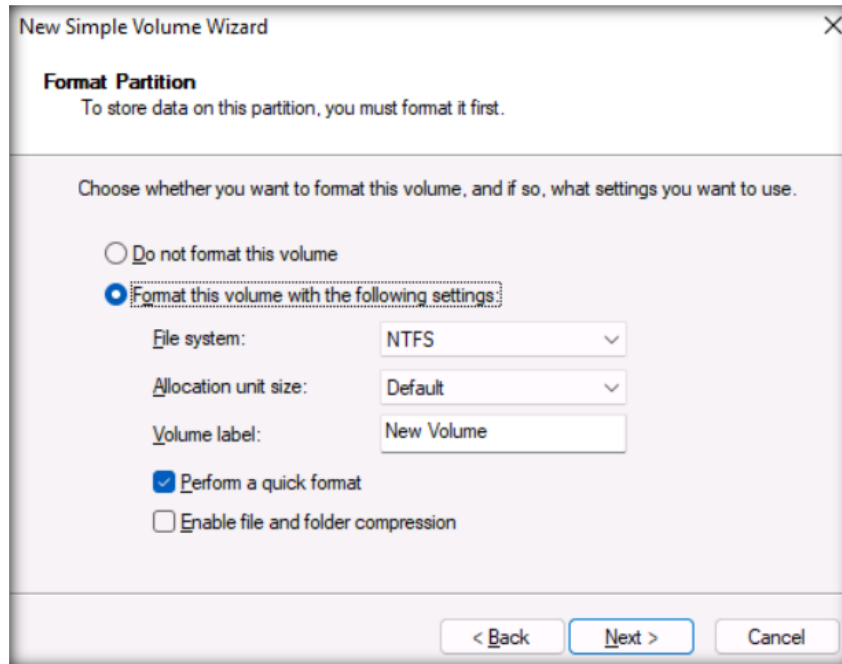


9. In the **Assign Drive Letter or Path** wizard, the letter **E** is selected by default in the **Assign the following drive letter** field; click **Next**.

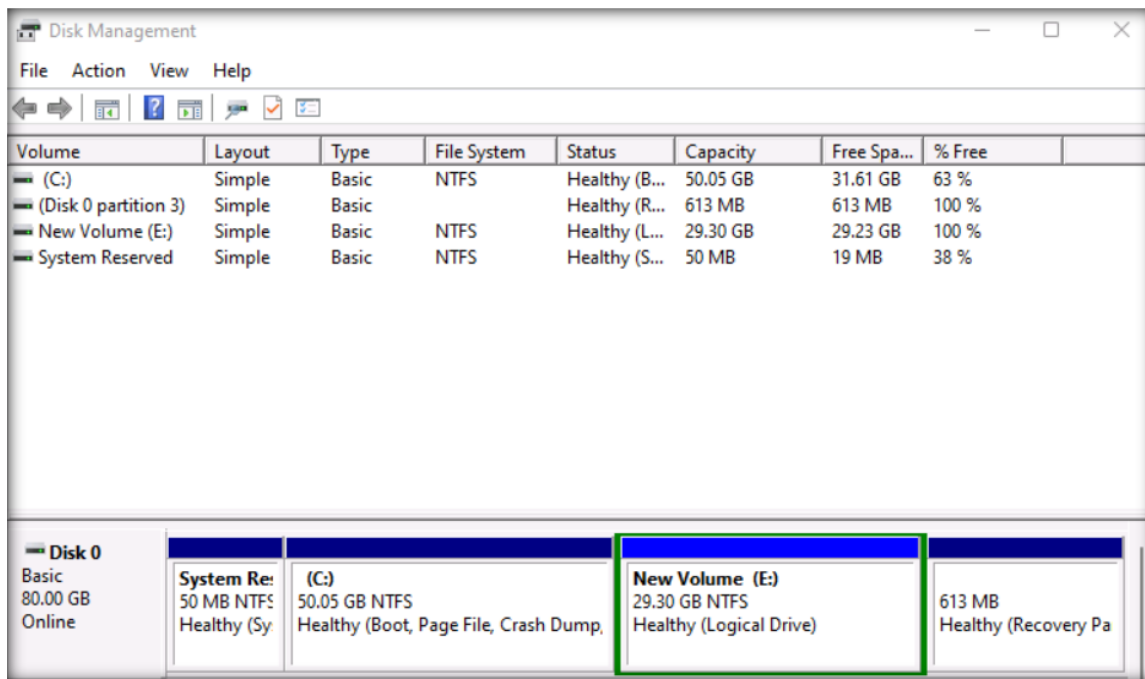
Note: If a letter other than **E** is selected in the **Assign the following drive letter** field, click on the drop-down menu and select **E**.



- In the **Format Partition** wizard, **NTFS** is the default selected file system to format the volume; click **Next**.



- In the next wizard, click **Finish**.
- The **Computer Management** window displays the newly created disk partition in the middle pane, as shown in the screenshot below.



- Close all windows and restart the **Windows 11** virtual machine.

[\[Back to Configuration Task Outline\]](#)

CT#9: Install Parrot Security Virtual Machine in VMware

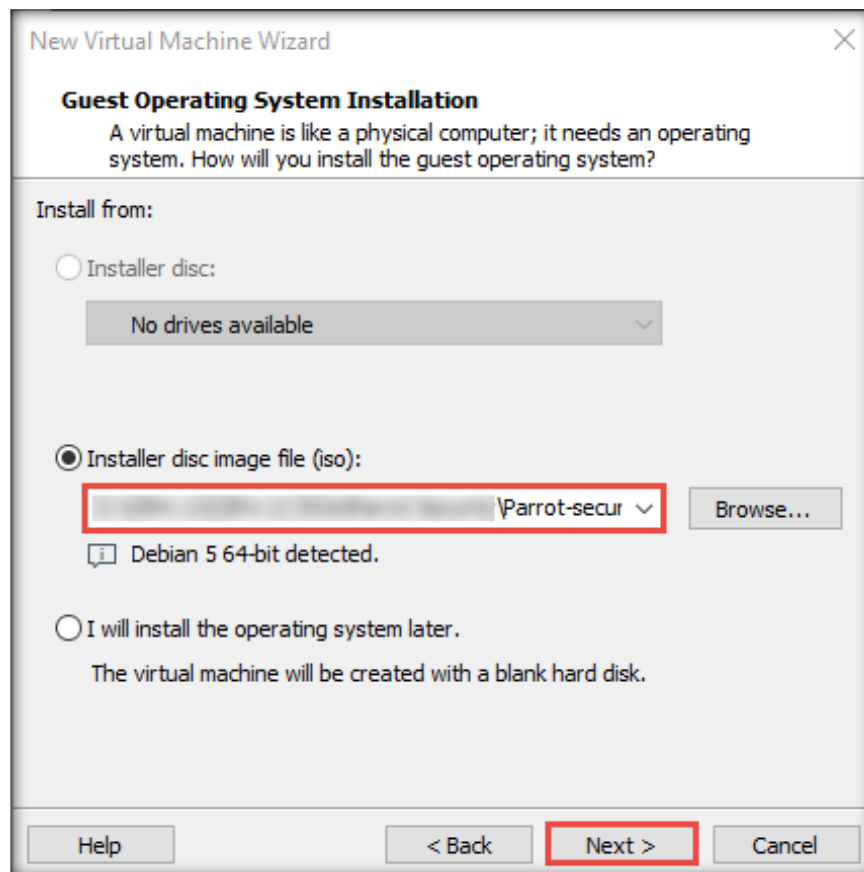
1. The next step is to set up the **Parrot Security** virtual machine in VMware Workstation Pro.
2. In the **VMware Workstation** window, click **Create a New Virtual Machine**.
3. In the **New Virtual Machine Wizard** window, leave the settings as their default (**Typical**) and click **Next**.
4. In the **Guest Operating System Installation** wizard, choose the **Installer disc image file (iso)**: radio button. Click **Browse** to provide the ISO path of the Parrot Security ISO file.

Note: Here, we have used the **Parrot Security (MATE)** .iso file **Parrot-security-5.0_amd64.iso** to create the **Parrot Security** virtual machine. Navigate to the location where you have extracted the **CTIAv2 ISO.zip** file and then to **CTIAv2 ISO\Parrot Security** to locate the Parrot Security ISO file.

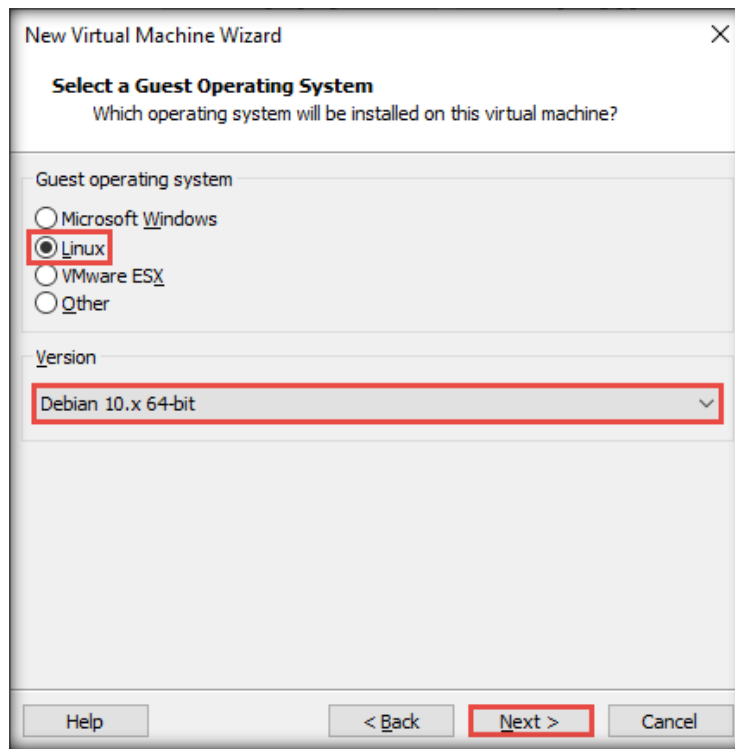
However, you can download the latest ISO file from <https://www.parrotsec.org/download/>.

Note: If you decide to download the latest version, the screenshots here might differ from what you see in your lab environment.

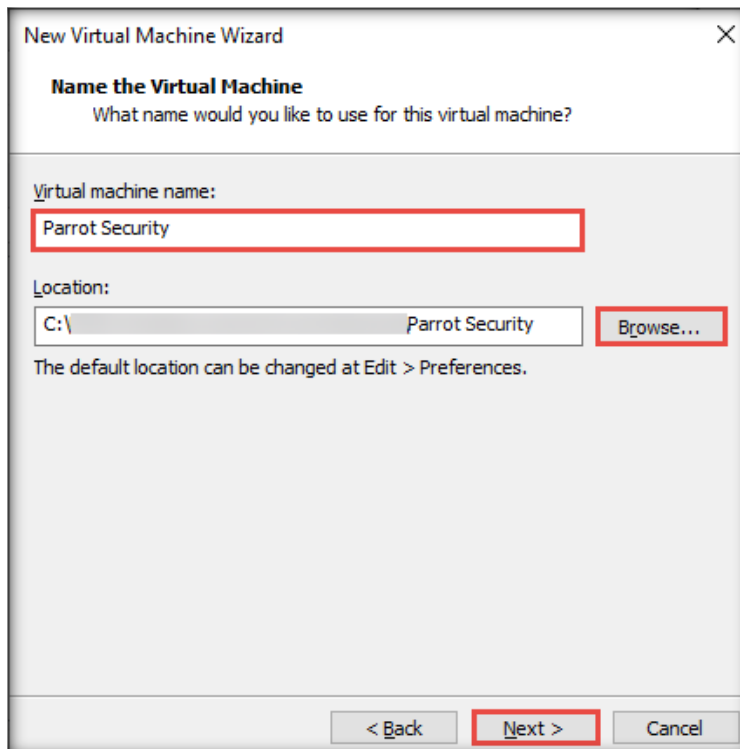
5. Then, select the Parrot Security ISO file and click **Open** to provide the ISO path. Finally, click **Next**.



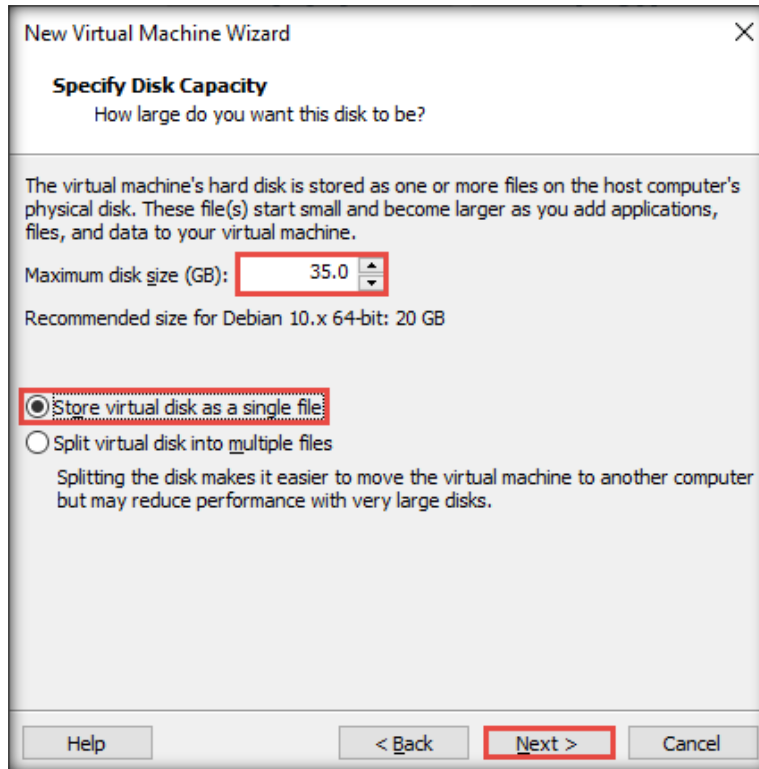
- The **Select a Guest Operating System** wizard appears. Choose the **Linux** radio button under the **Guest operating system** field and select **Debian 10.x 64-bit** in the **Version** drop-down box. Then, click **Next**.



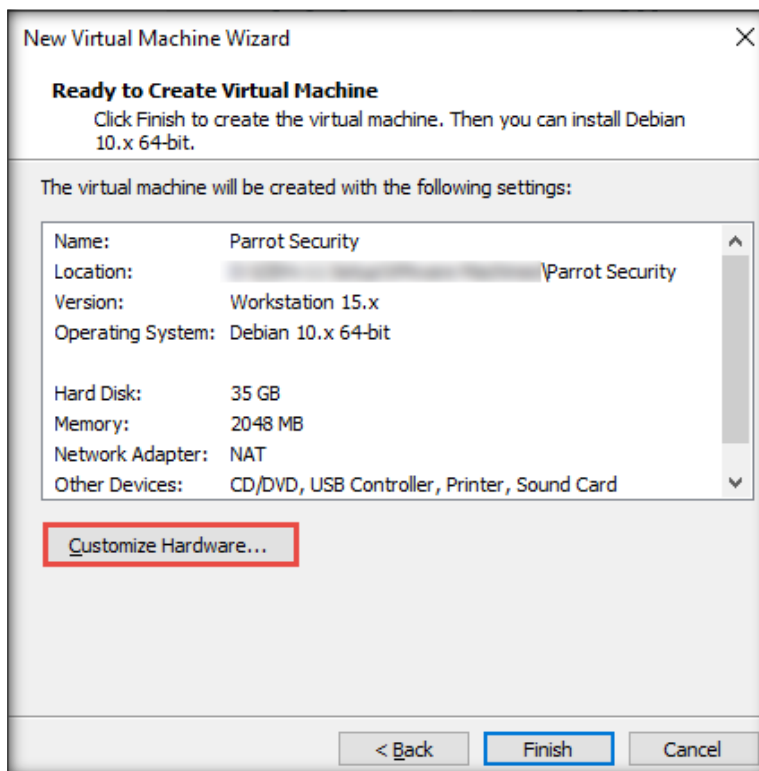
- The **Name the Virtual Machine** wizard appears. Type **Parrot Security** in the **Virtual machine name** field and click the **Browse** button to store the virtual hard disk. Then, click **Next**.



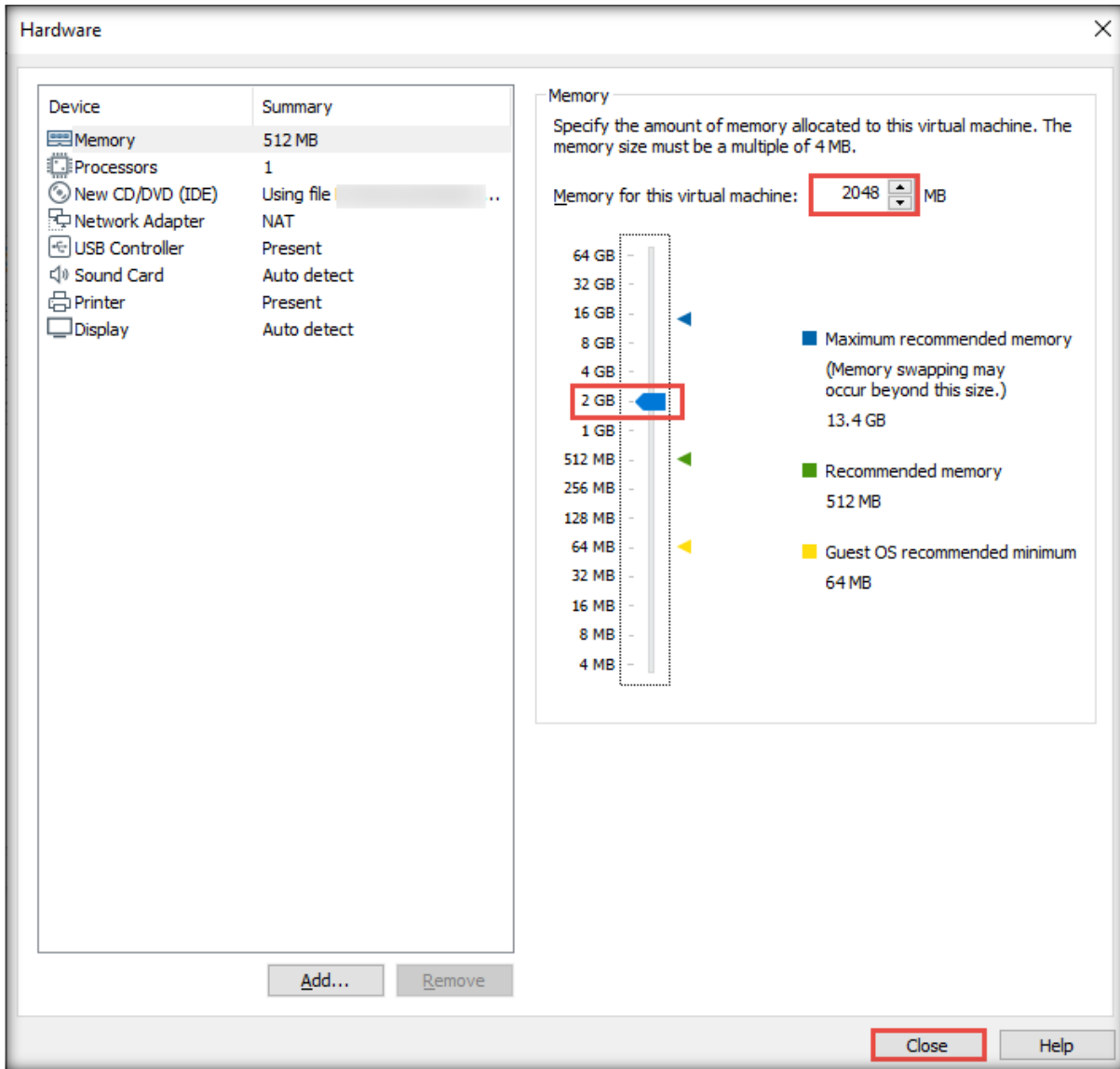
8. The **Specify Disk Capacity** wizard appears; type **35.0 GB** in the **Maximum disk size (GB)** field and choose the **Store virtual disk as a single file** radio button. Then, click **Next**.



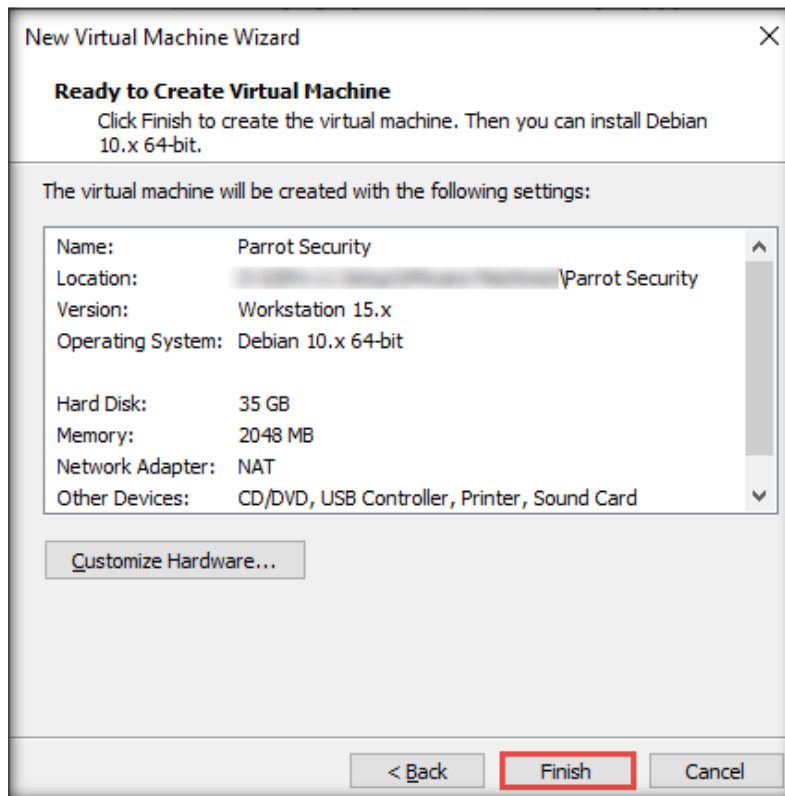
9. Click the **Customize Hardware...** button in the **Ready to Create Virtual Machine** wizard.



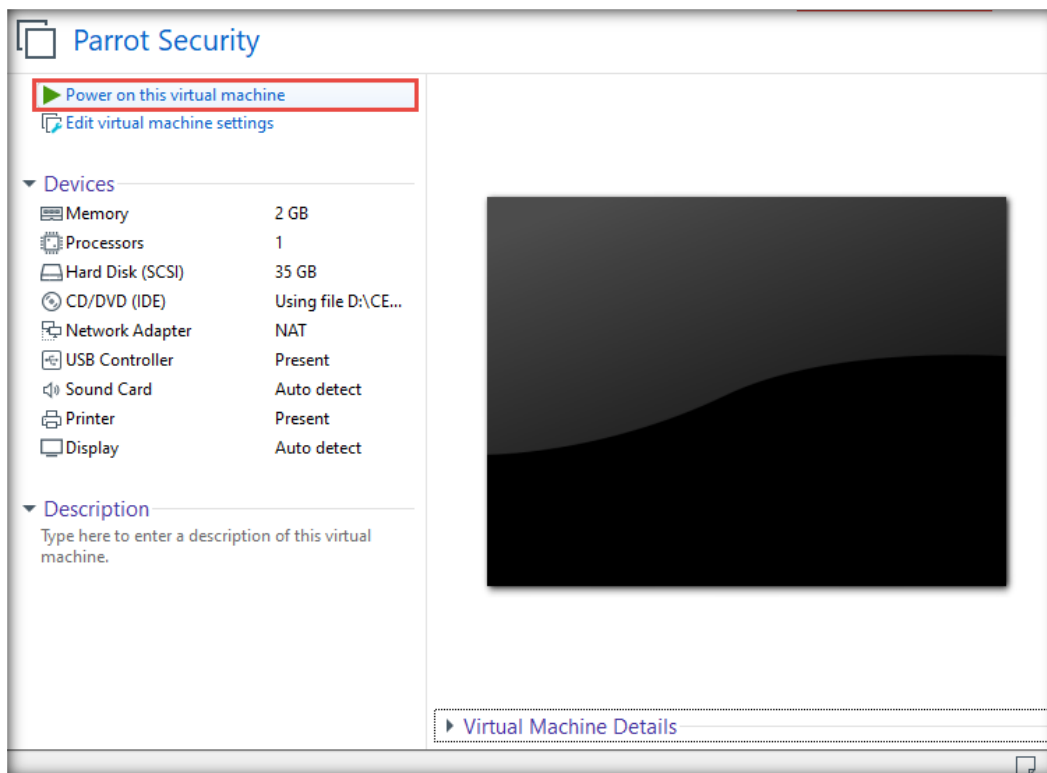
10. The **Hardware** window appears; ensure that **Memory** is assigned as **2 GB** or **2048 MB** and click **Close**.



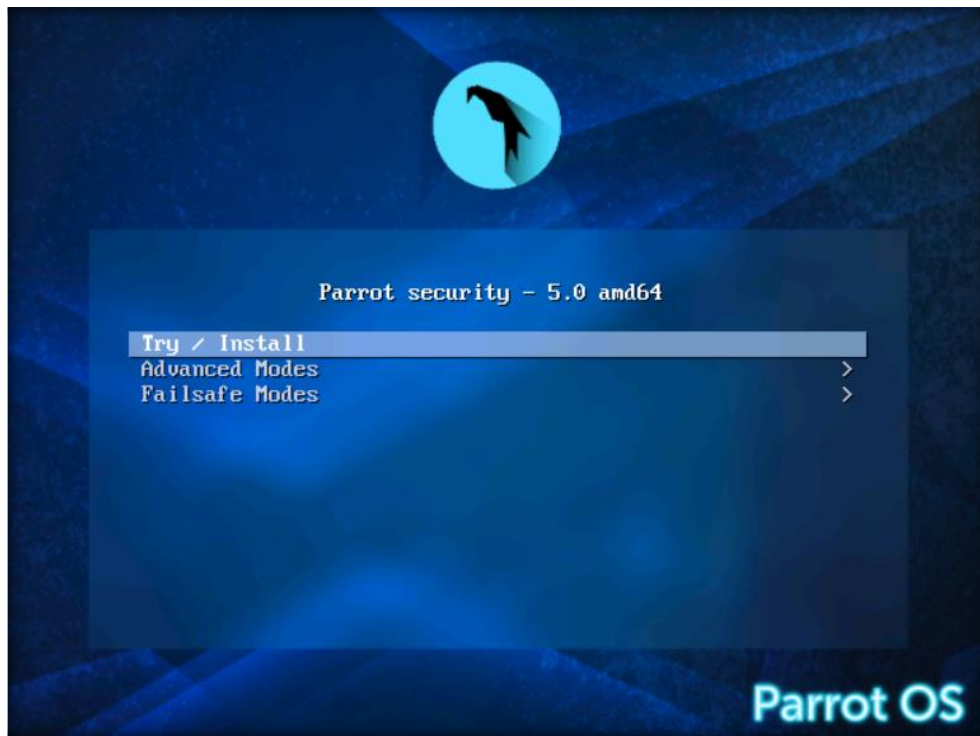
11. Click **Finish** in the **Ready to Create Virtual Machine** wizard.



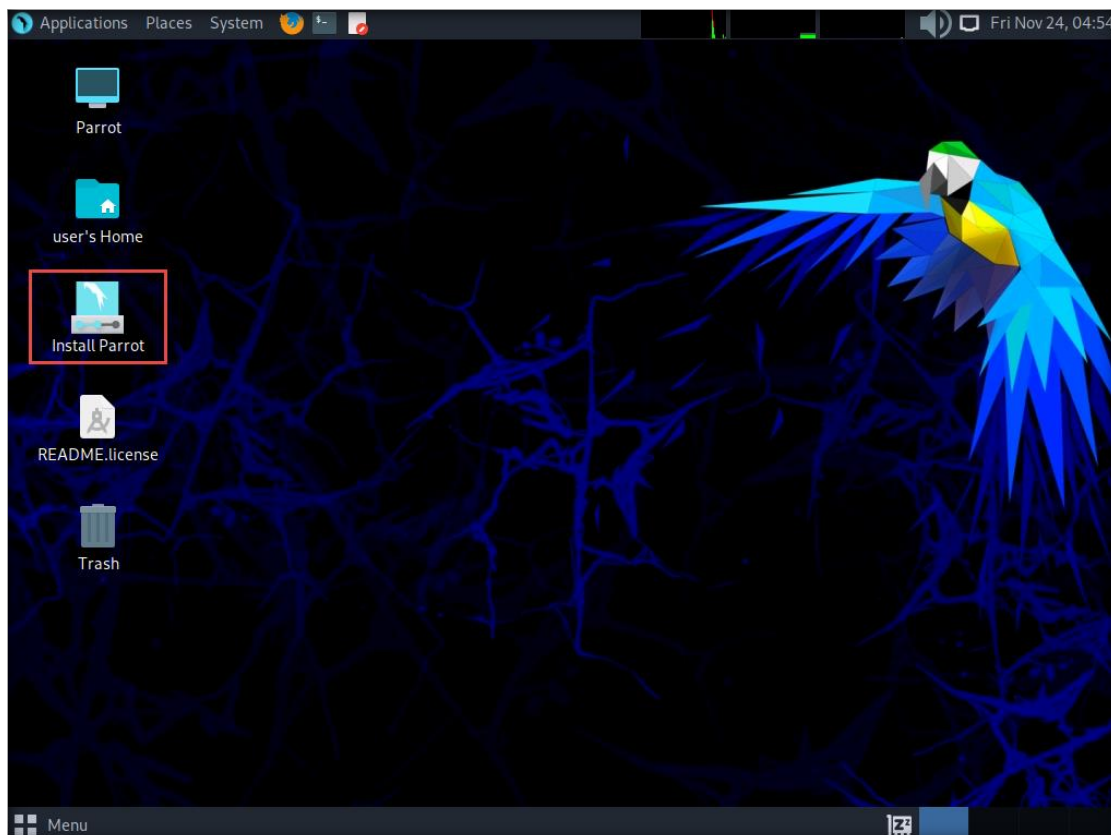
12. In the **Parrot Security** tab, click the **Power on this virtual machine** link.



13. The **Parrot security – 5.0 amd64** boot menu appears; select **Install** and press **Enter**.



14. The Parrot Security desktop appears. Double-click the **Install Parrot** shortcut to initialize the installation process.

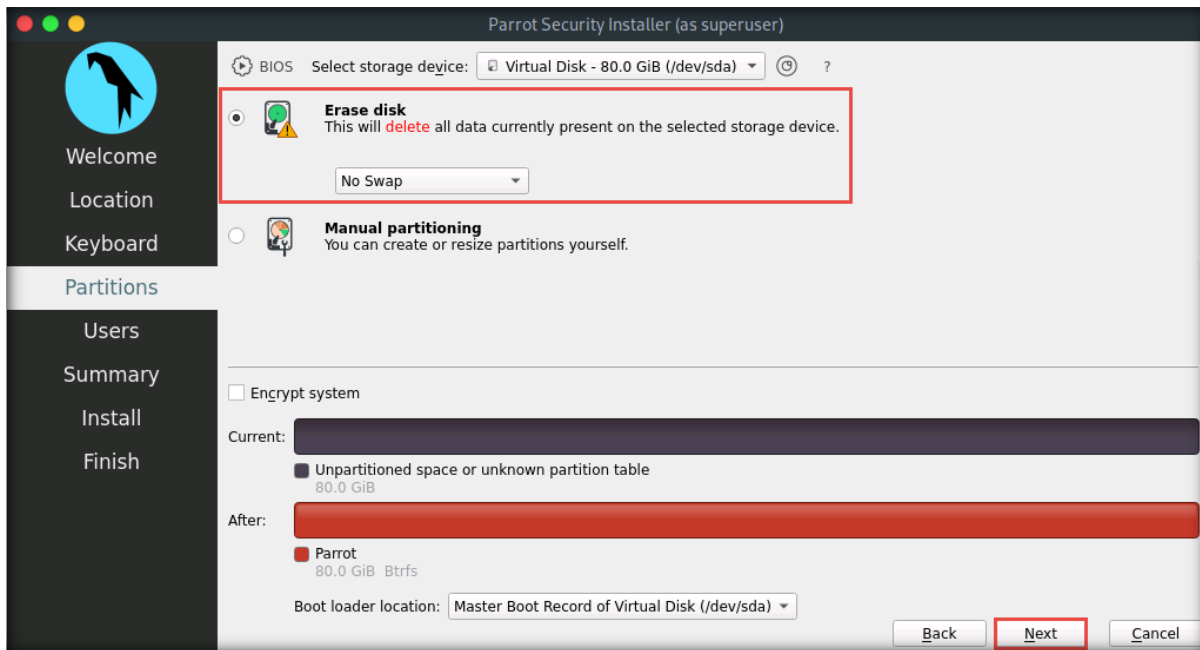


- A **Parrot OS Installer** window appears. In the **Welcome** wizard, leave default selected language as **American English**, and click **Next**.



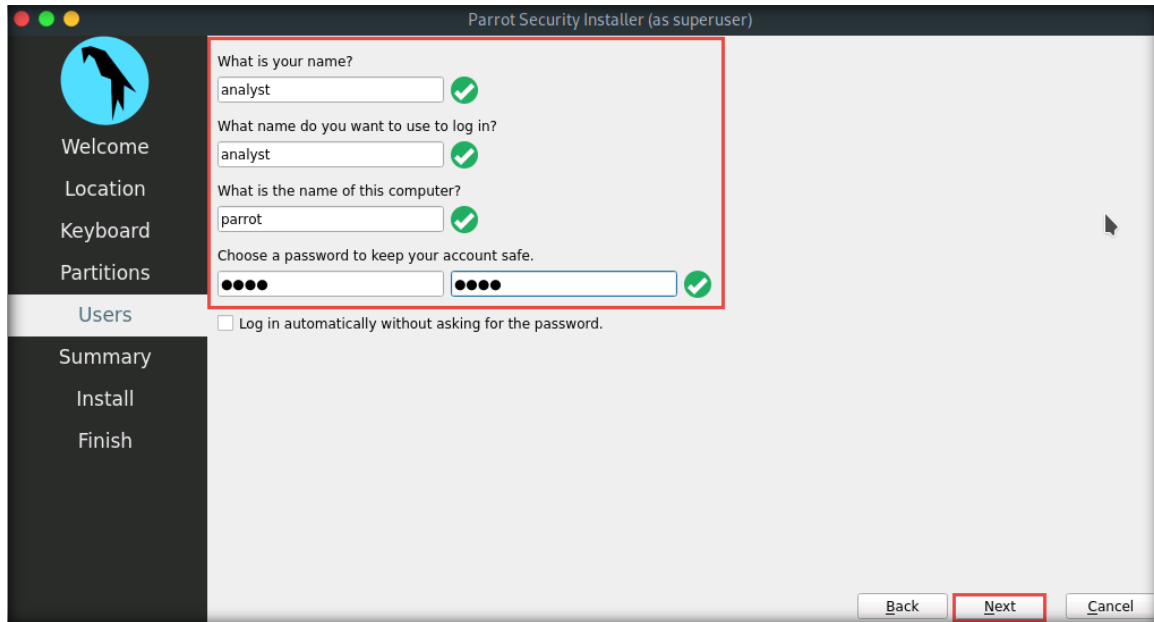
- In the **Location** wizard, leave default settings and click **Next**.
- In the **Keyboard** wizard, leave default settings and click **Next**.
- In the **Partitions** wizard, select the **Erase disk** checkbox and click **Next**.

Note: If the **Encrypt system** checkbox is selected, then unselect it.

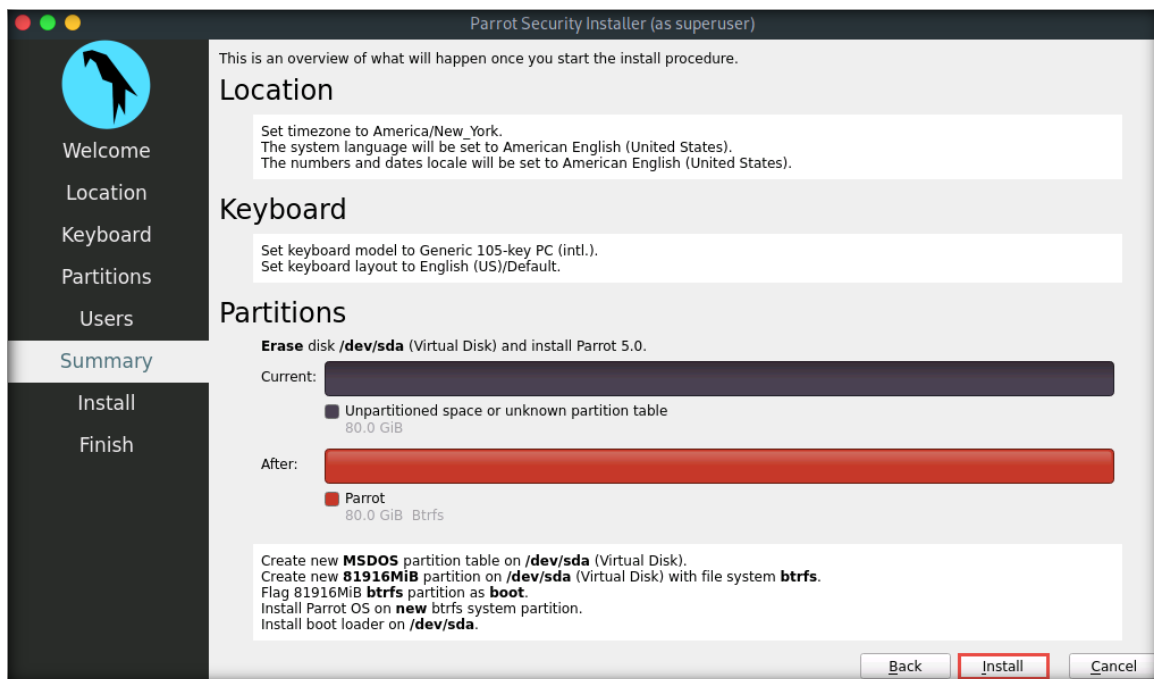


- In the **Users** wizard, enter **analyst** in the **What is your Name?** field. In the **What is the name of this computer?** field, enter **parrot**.

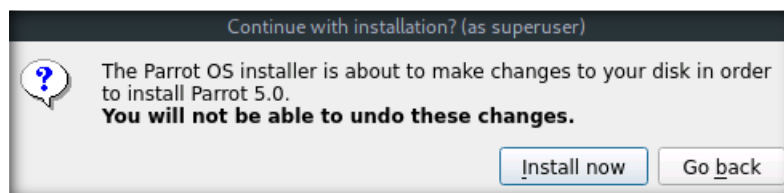
20. In the **Choose a password to keep your account safe** section, enter **toor** in both the **Password** and **Repeat Password** fields. Click **Next**.



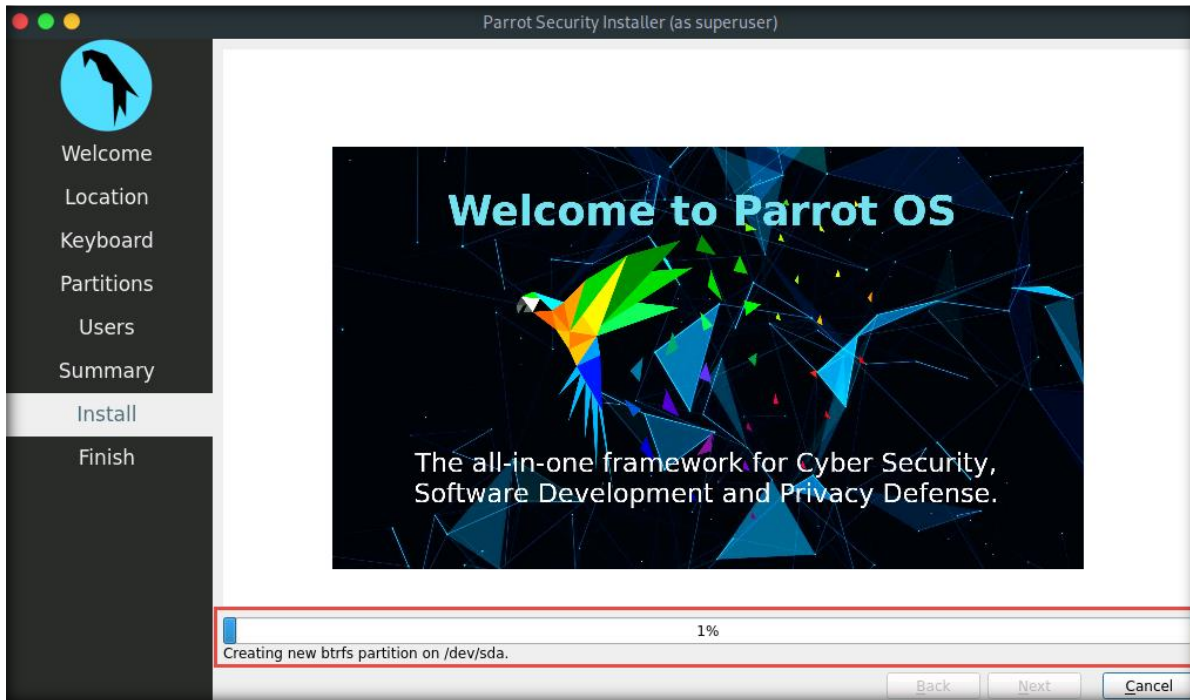
21. The **Summary** wizard appears. Check the settings and click **Install**.



22. In the **Continue with installation?** dialog box, click **Install Now**.

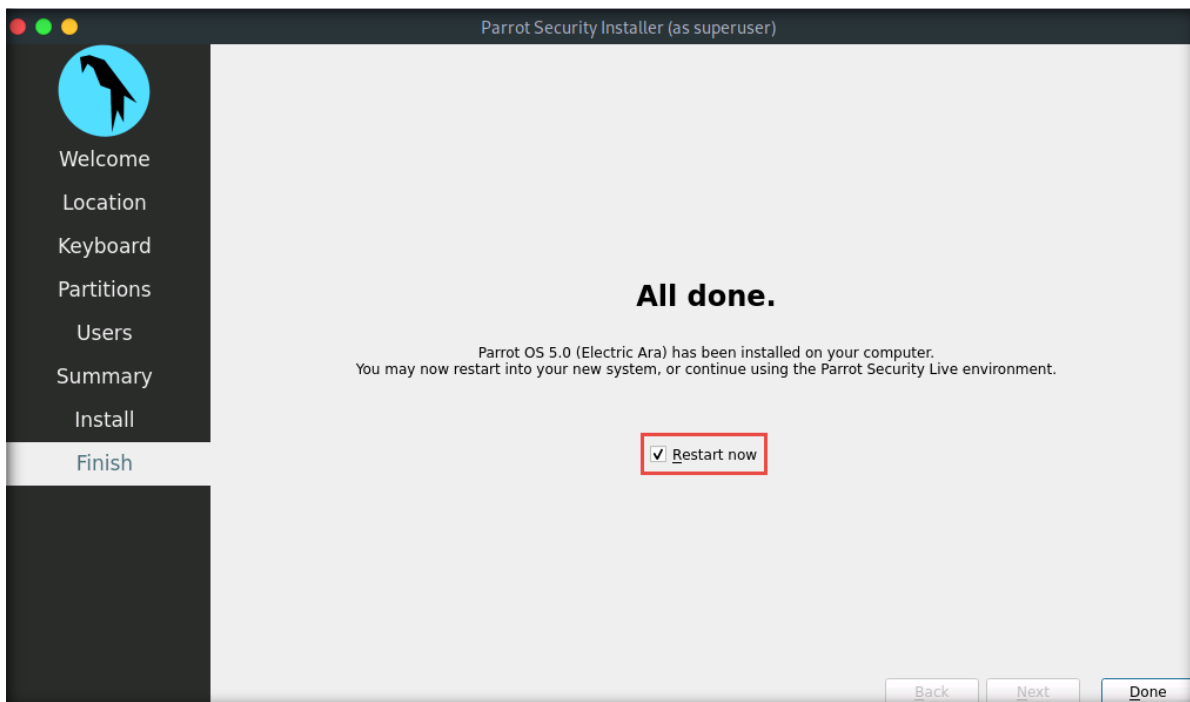


23. The installation process begins. Observe the status in the installation bar, as shown in the screenshot below.

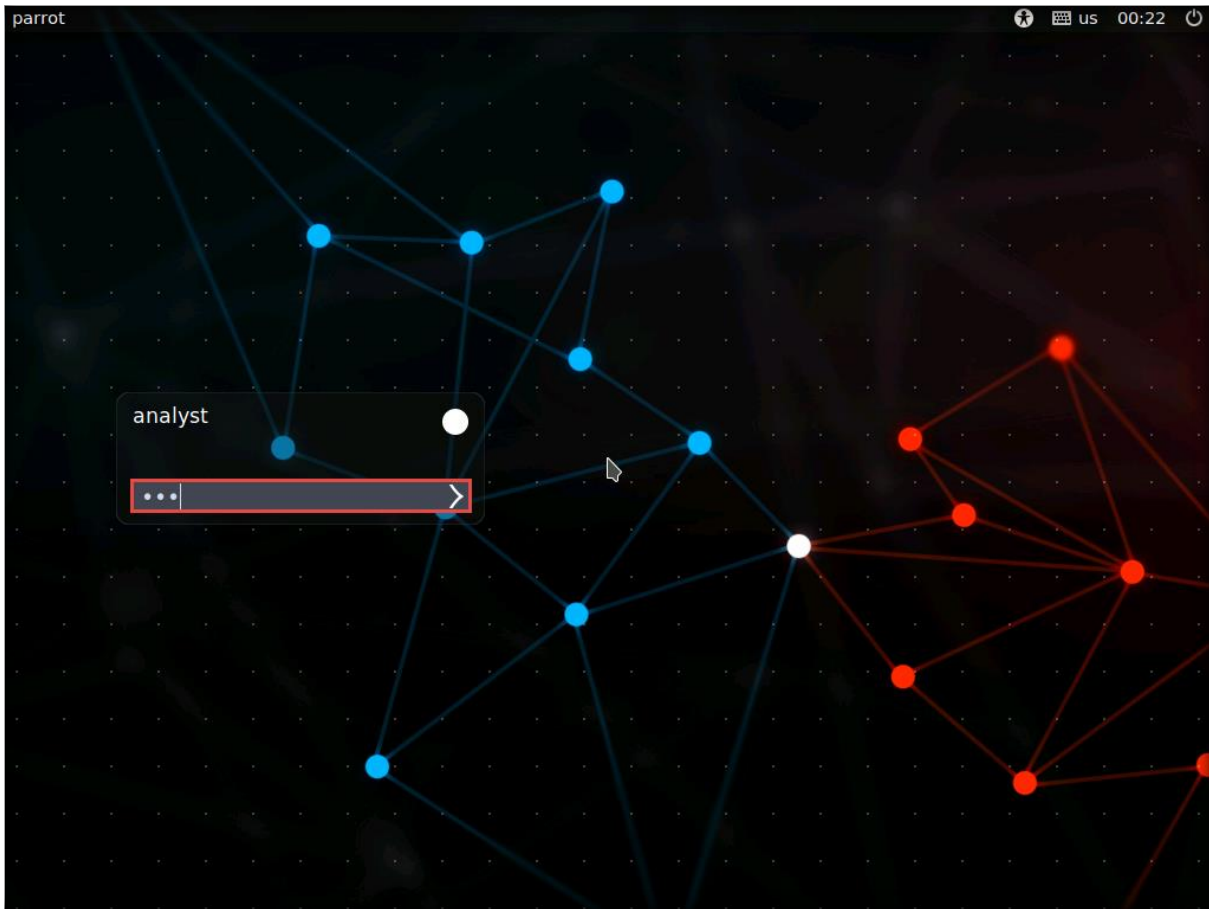


24. System installation will take some time.

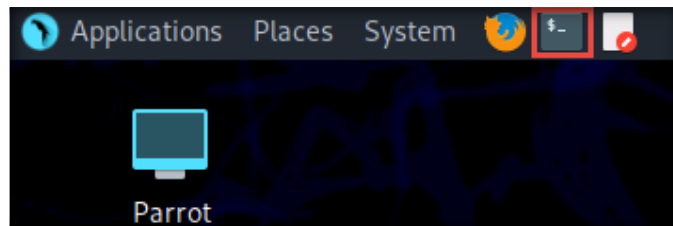
25. After the completion of the installation process, an **All done** message appears. Ensure that the **Restart now** check box is selected and click **Done**.



26. After the reboot, the **analyst** username is selected by default on the login screen. Enter **toor** in the **Password** field and press **Enter** to log in to the machine.



27. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



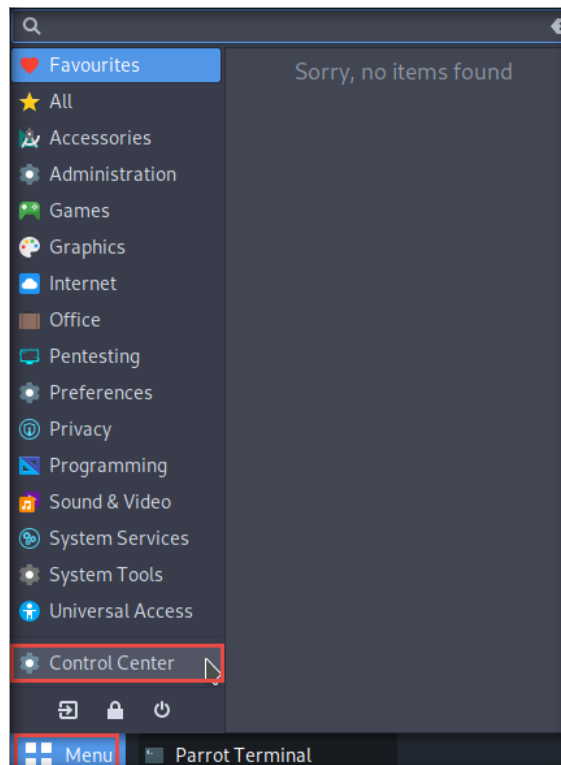
28. Now, verify the configured network adapter setting of the virtual machine. In the **Parrot Terminal** window, type **ifconfig** and press **Enter** to check the network adapter—here, it is **eth0** (this might differ in your lab environment). Close the Terminal window after noting the adapter.

```

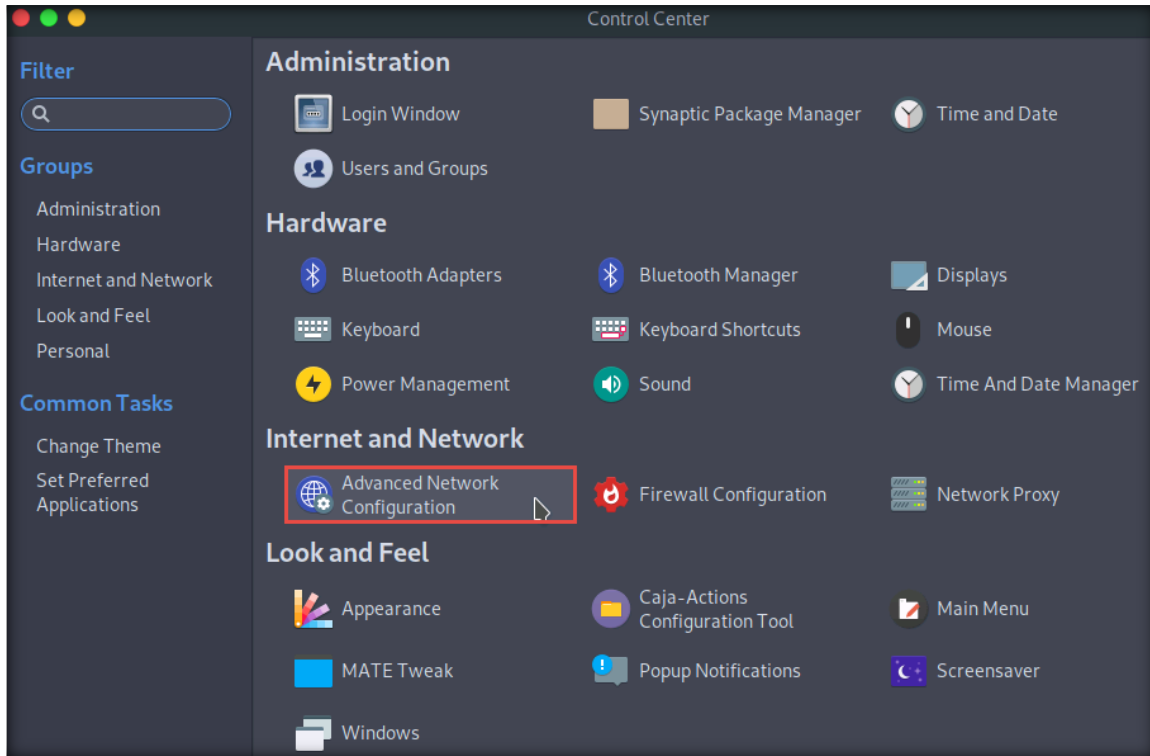
[analyst@parrot]-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.2 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::82f0:ae2f:de83:cedf prefixlen 64 scopeid 0x20<link>
    ether 02:15:5d:11:da:36 txqueuelen 1000 (Ethernet)
    RX packets 11 bytes 1926 (1.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 2518 (2.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  
```

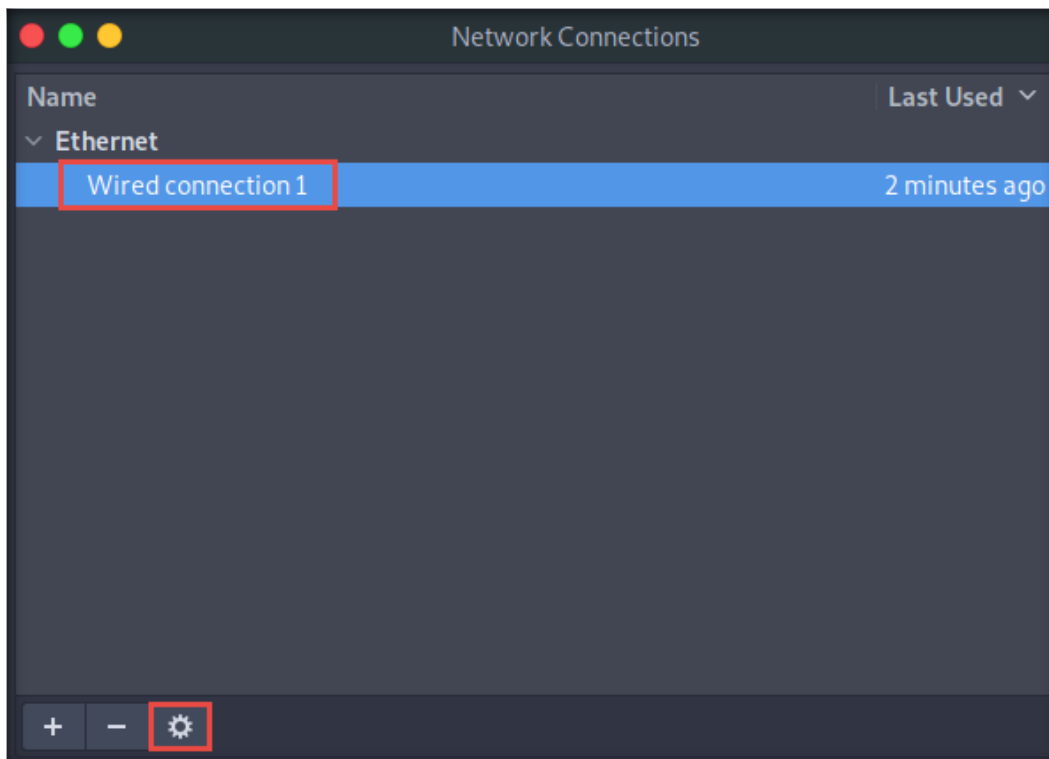
29. Since this adapter IP address has been assigned through DHCP, we must now configure the network adapter to static. To do so, navigate to **Menu** in the bottom-left corner of the **Desktop** and click **Control Center**.



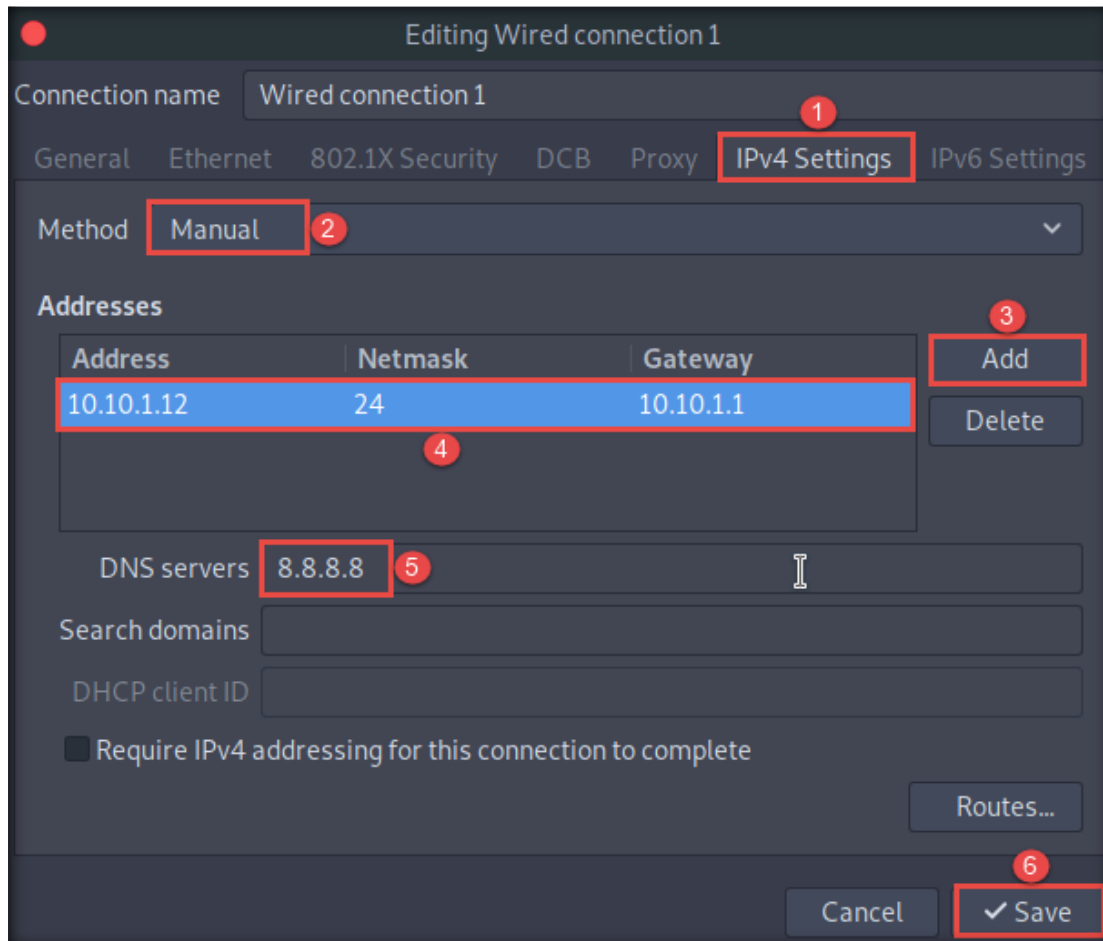
30. The **Control Center** window appears; click **Advanced Network Configuration** under the **Internet and Network** section.



31. A **Network Connections** window appears. Select **Wired connection 1** and click the **Settings** icon.



32. In the **Editing Wired connection 1** window, navigate to the **IPv4 Settings** tab. Select the **Manual** option from the **Method** drop-down box. In the **Addresses** section, click the **Add** button and add **10.10.1.12**, **255.255.255.0**, and **10.10.1.2** as the **Address**, **Netmask**, and **Gateway**. Type **8.8.8.8** in the **DNS servers** field and click **Save**.



33. Close all windows and **reboot** the virtual machine to enable the setting.
34. Once the machine has restarted, log in to the machine and open a **Terminal** window.

35. Type **ifconfig** and press **Enter** to verify the configured IP address. Then, type **ping www.eccouncil.org** to check Internet connectivity.

```

Parrot Terminal
File Edit View Search Terminal Help

[analyst@parrot]-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.12 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::82f0:ae2f:de83:cedf prefixlen 64 scopeid 0x20<link>
    ether 02:15:5d:11:da:36 txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 126 (126.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 2142 (2.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[analyst@parrot]-[~]
└─$ ping www.eccouncil.org
PING www.eccouncil.org (104.18.8.180) 56(84) bytes of data:
64 bytes from 104.18.8.180 (104.18.8.180): icmp_seq=1 ttl=58 time=2.38 ms
64 bytes from 104.18.8.180 (104.18.8.180): icmp_seq=2 ttl=58 time=2.41 ms
64 bytes from 104.18.8.180 (104.18.8.180): icmp_seq=3 ttl=58 time=2.31 ms
  
```

[\[Back to Configuration Task Outline\]](#)

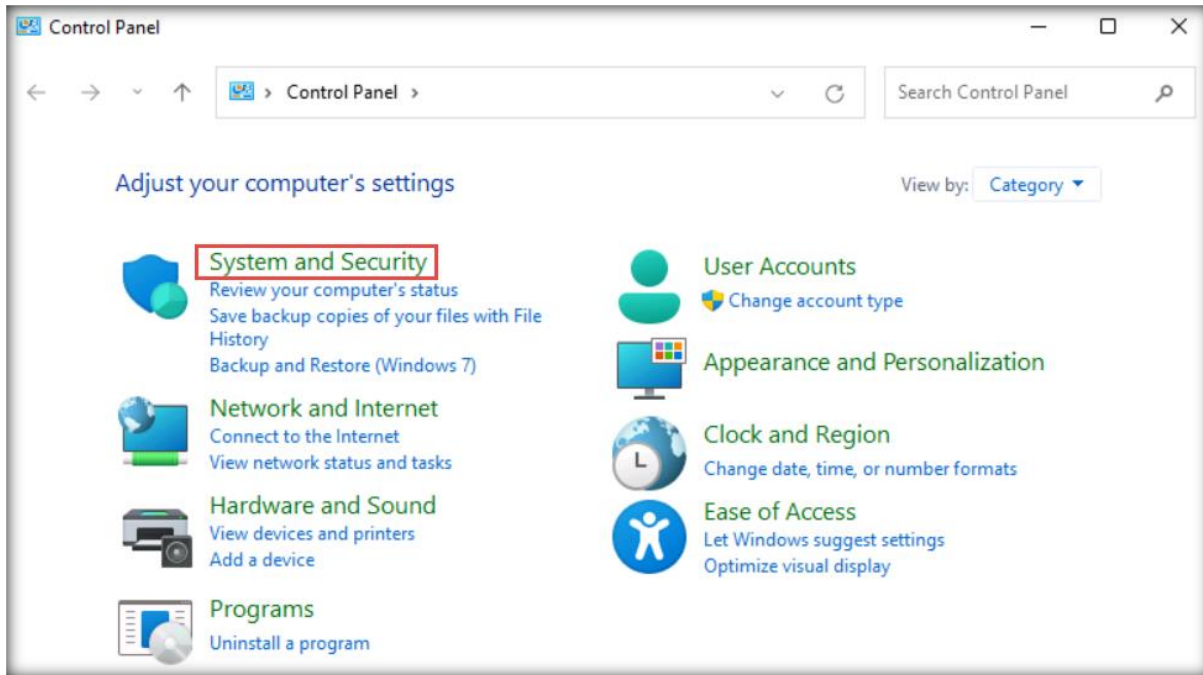
CT#10: Turn Off Windows Defender Firewall on the Windows 11 Virtual Machine

1. Turn on the **Windows 11** virtual machine, press any key, and log in with the credentials **Analyst** and **Pa\$\$w0rd**.

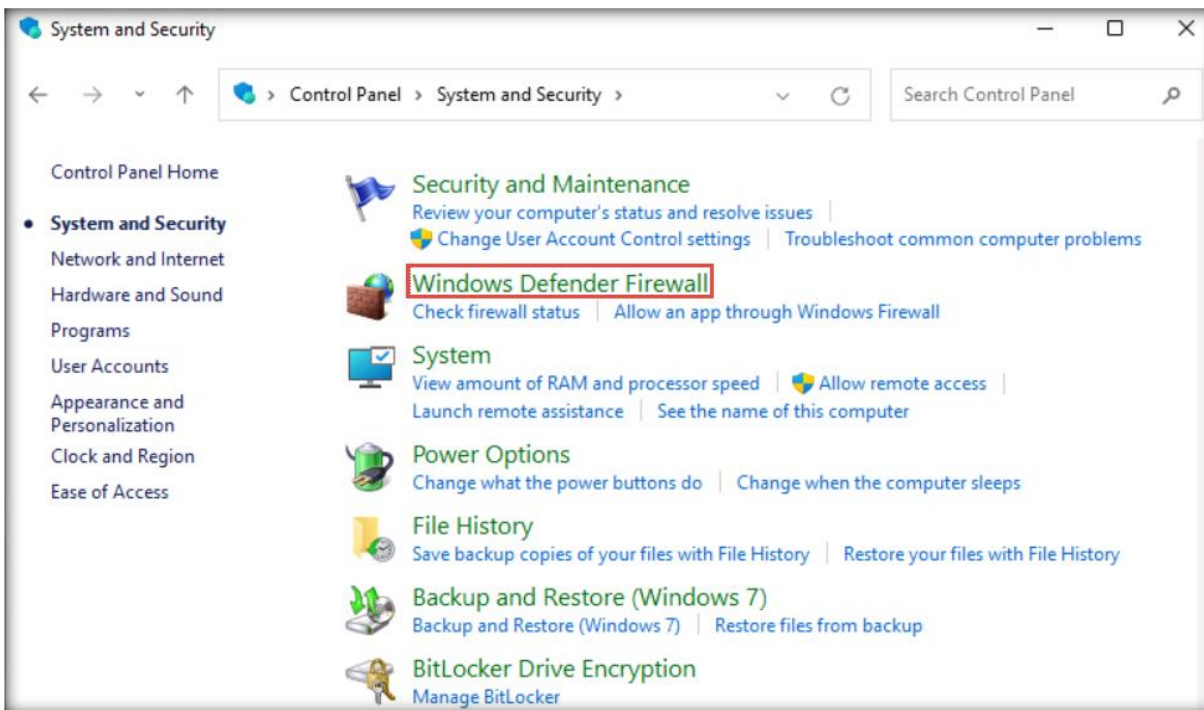
Note: If a **Windows 11 – VMware Workstation** pop-up appears, click **Yes**.

2. Click the **Type here to search** icon, type **control panel** and select **Control Panel** from the search results.

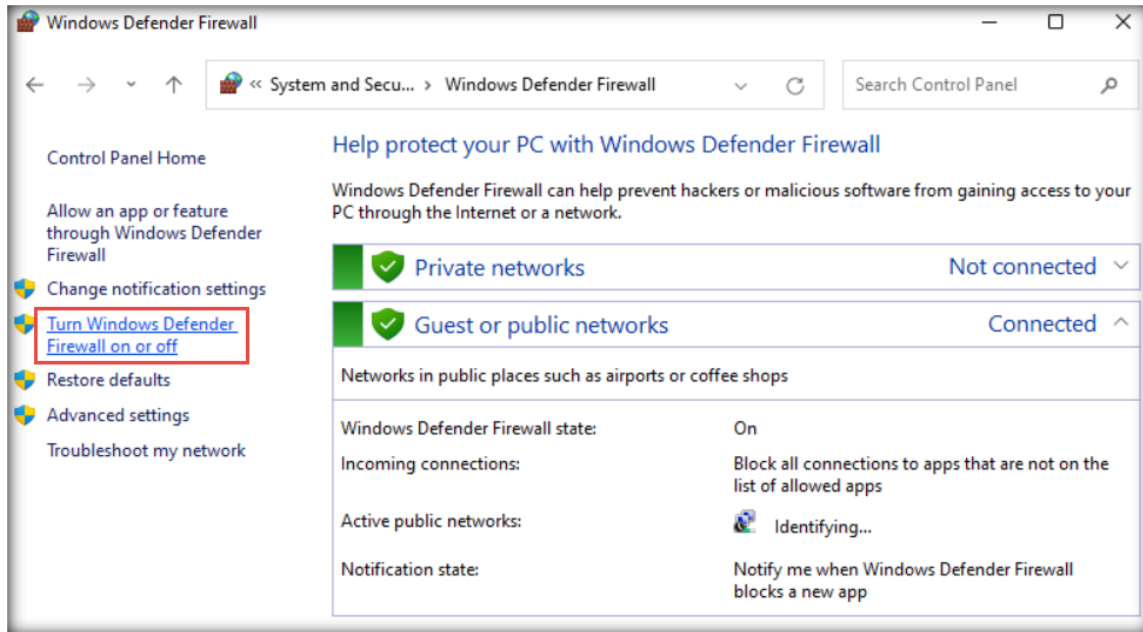
3. The **Control Panel** window appears; click the **System and Security** category.



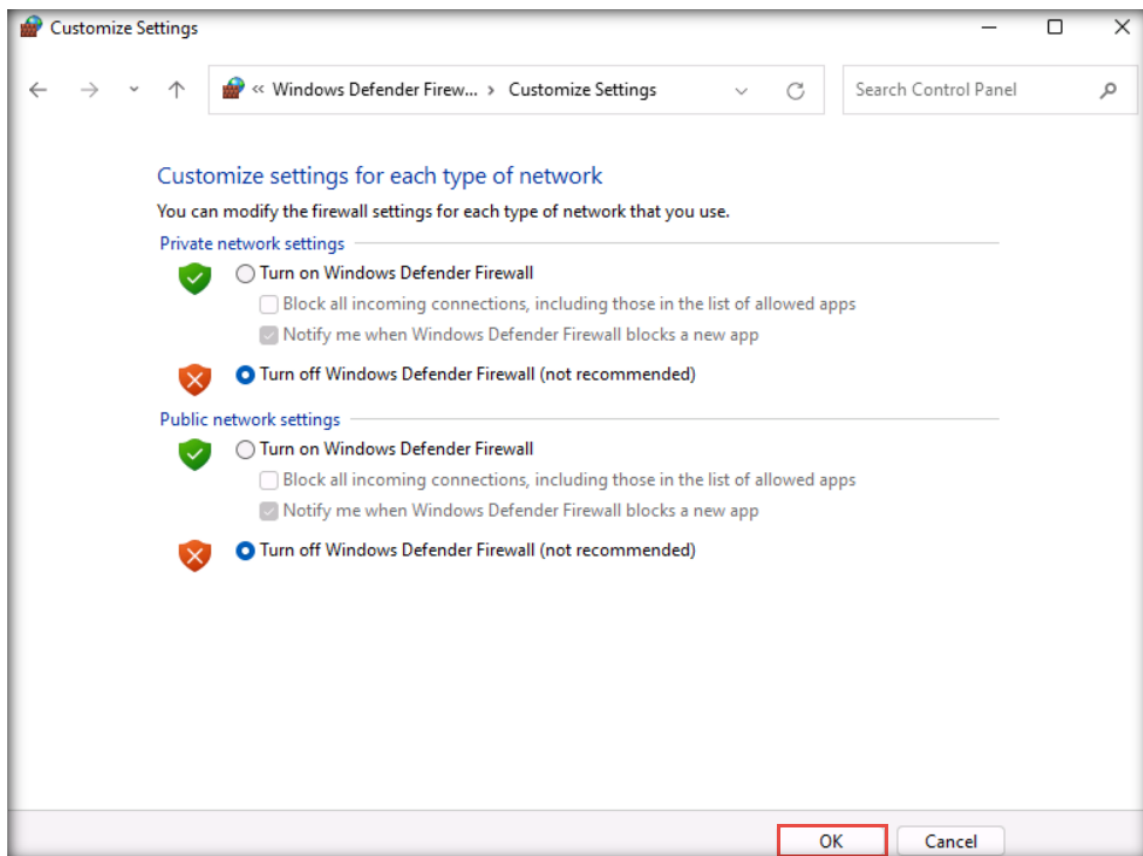
4. Click **Windows Defender Firewall** in the **System and Security** window.



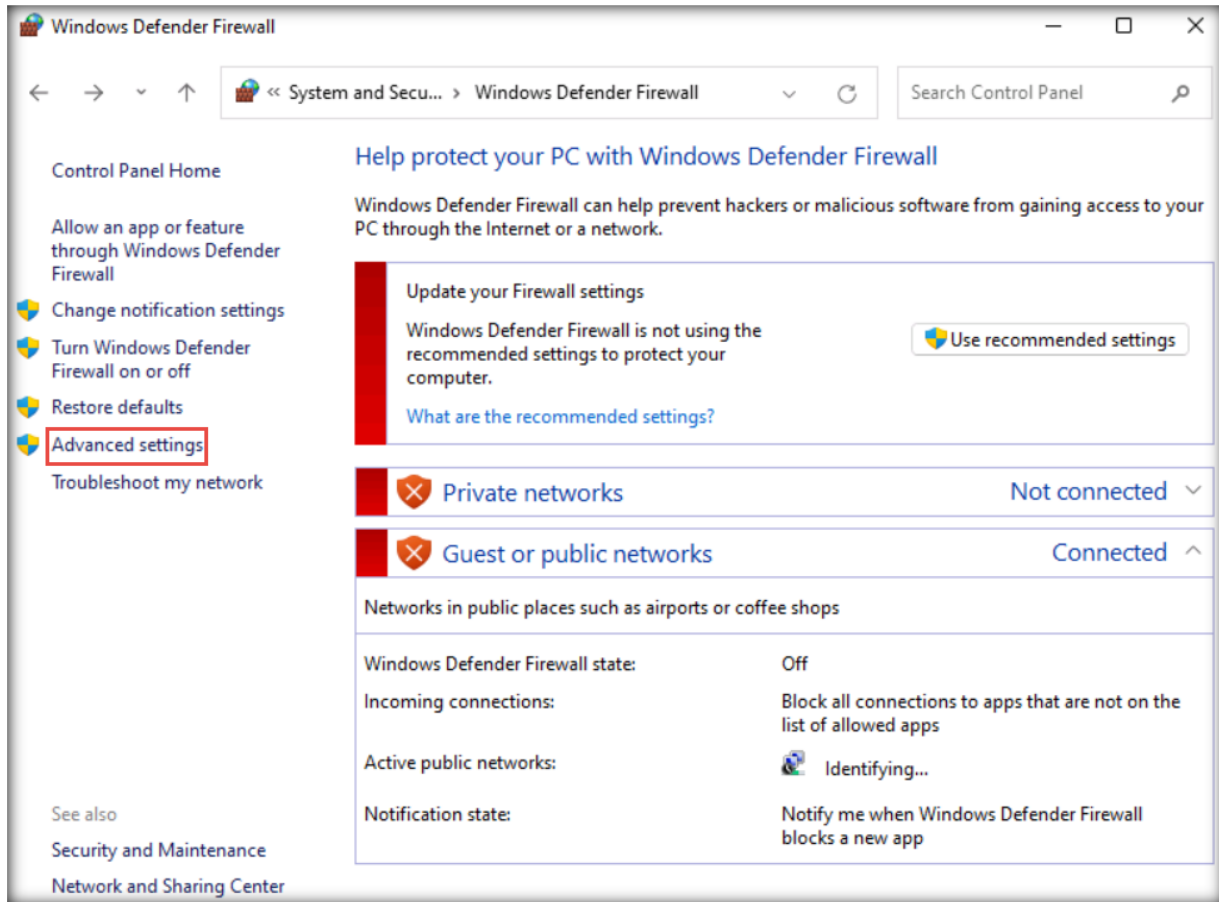
- In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left-hand pane.



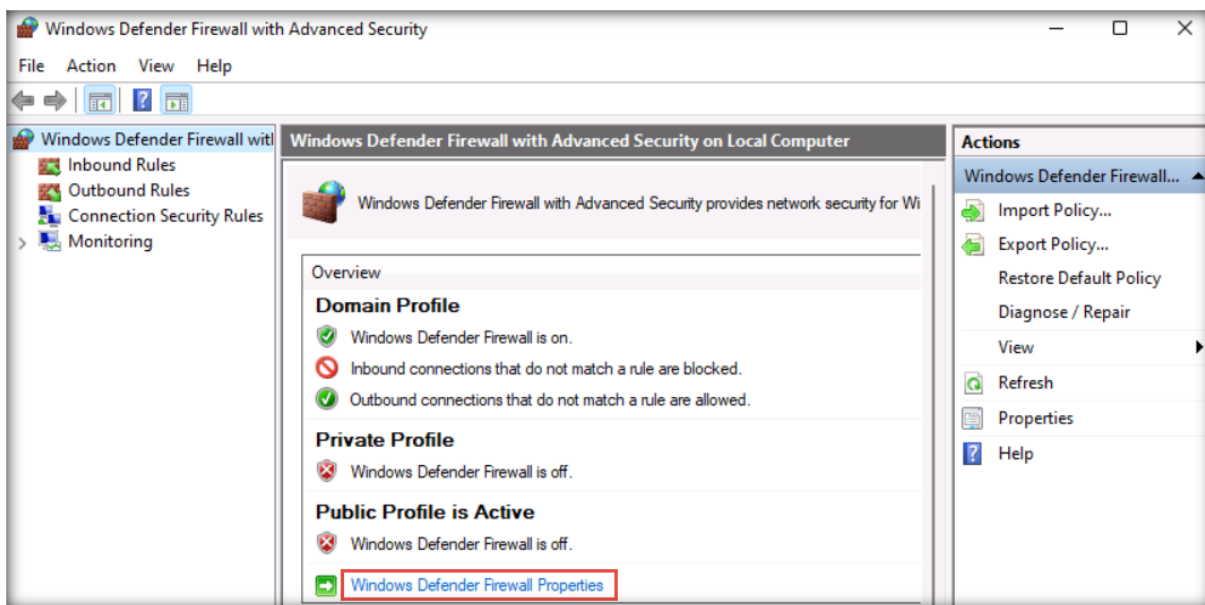
- In the **Customize Settings** window, select the **Turn off Windows Defender Firewall (not recommended)** radio button for all Domain, Private, and Public network settings and click **OK**.



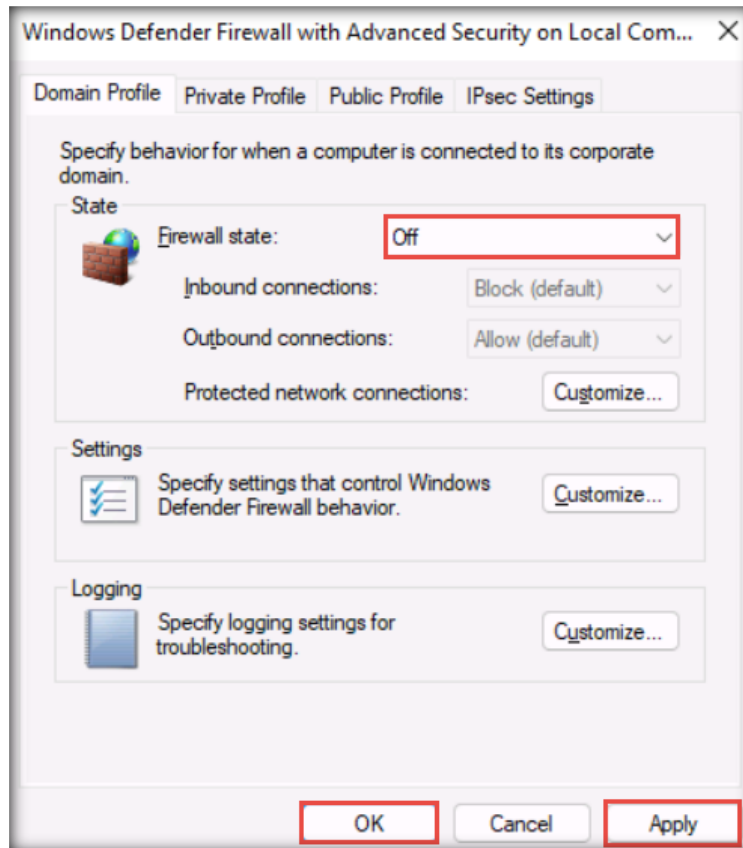
- Again, in the **Windows Defender Firewall** window, click the **Advanced settings** link in the left-hand pane.



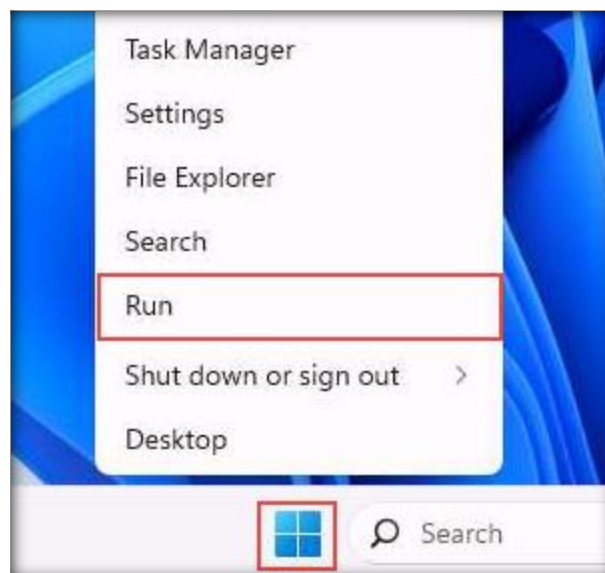
- Once the **Windows Defender Firewall with Advanced Security** window appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section.



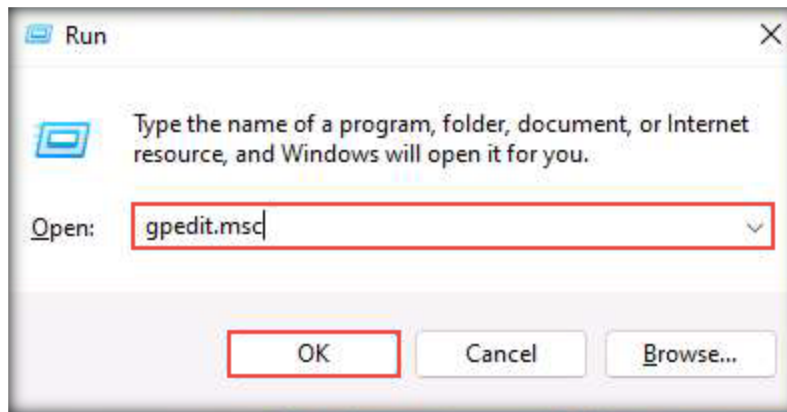
9. When the **Windows Defender Firewall with Advanced Security on Local Computer Properties** window appears, in the **Domain Profile** tab, choose **Off** from the **Firewall state** drop-down list. Then, navigate to the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply** and then **OK**.



10. Close all windows.
11. Right-click the **Windows** icon in the lower section of the screen and click **Run**.

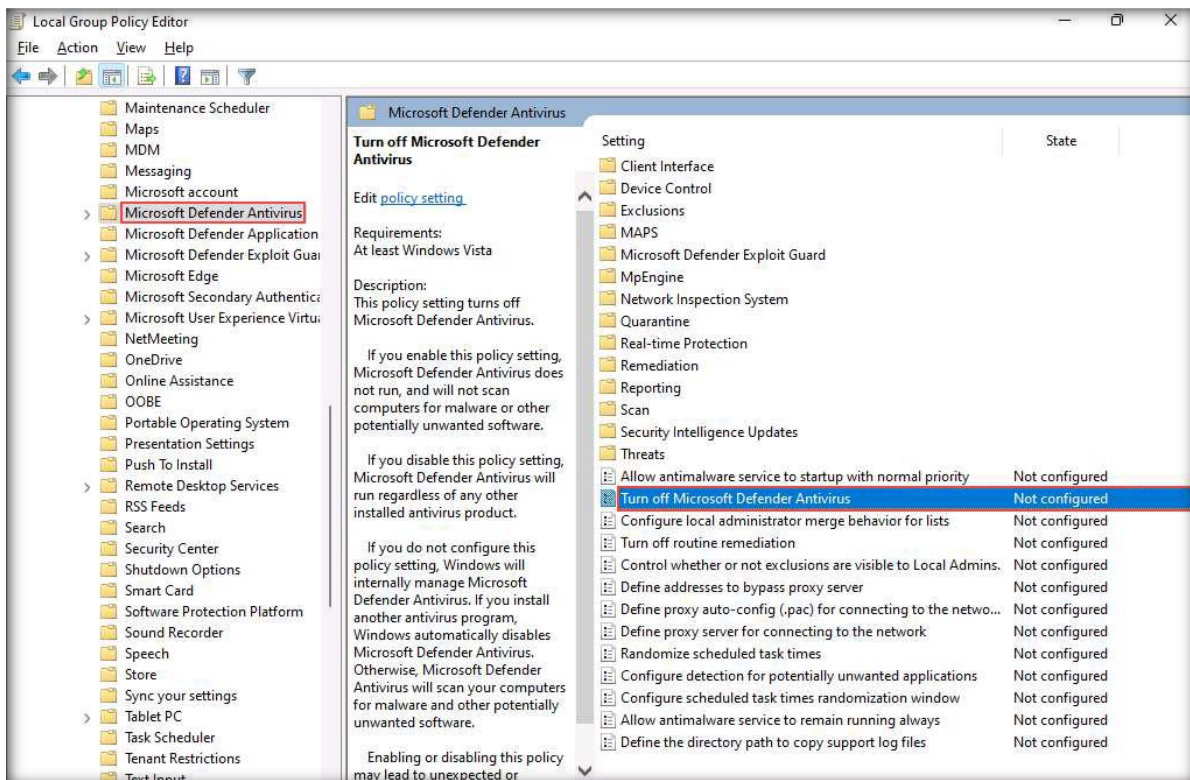


12. The **Run** window appears. Type **gpedit.msc** and click **OK**.

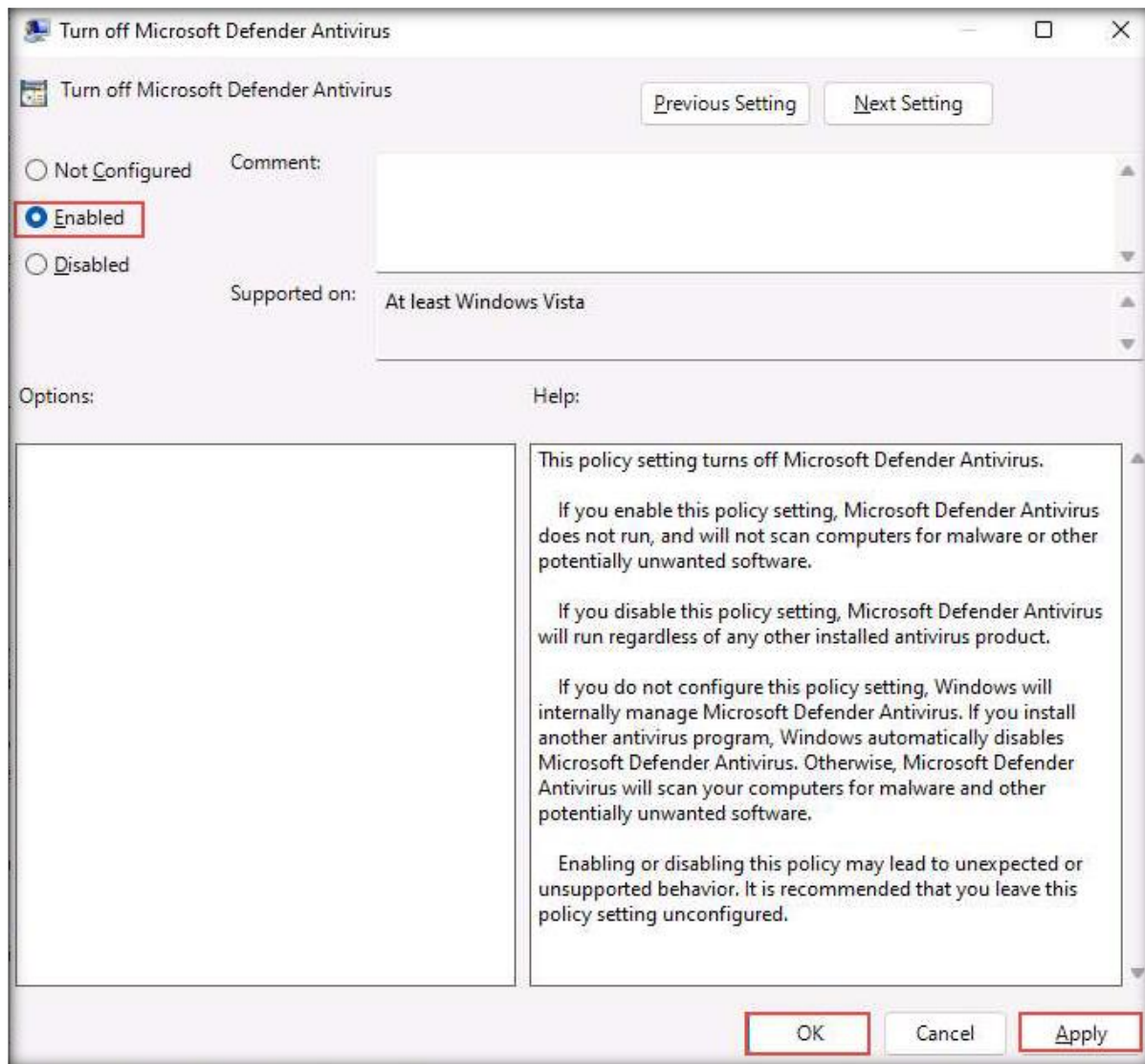


13. The **Local Group Policy Editor** window appears. In the left-hand pane, navigate to **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Microsoft Defender Antivirus**. Double-click the **Turn off Microsoft Defender Antivirus** policy in the right-hand pane of the window, as shown in the screenshot below.

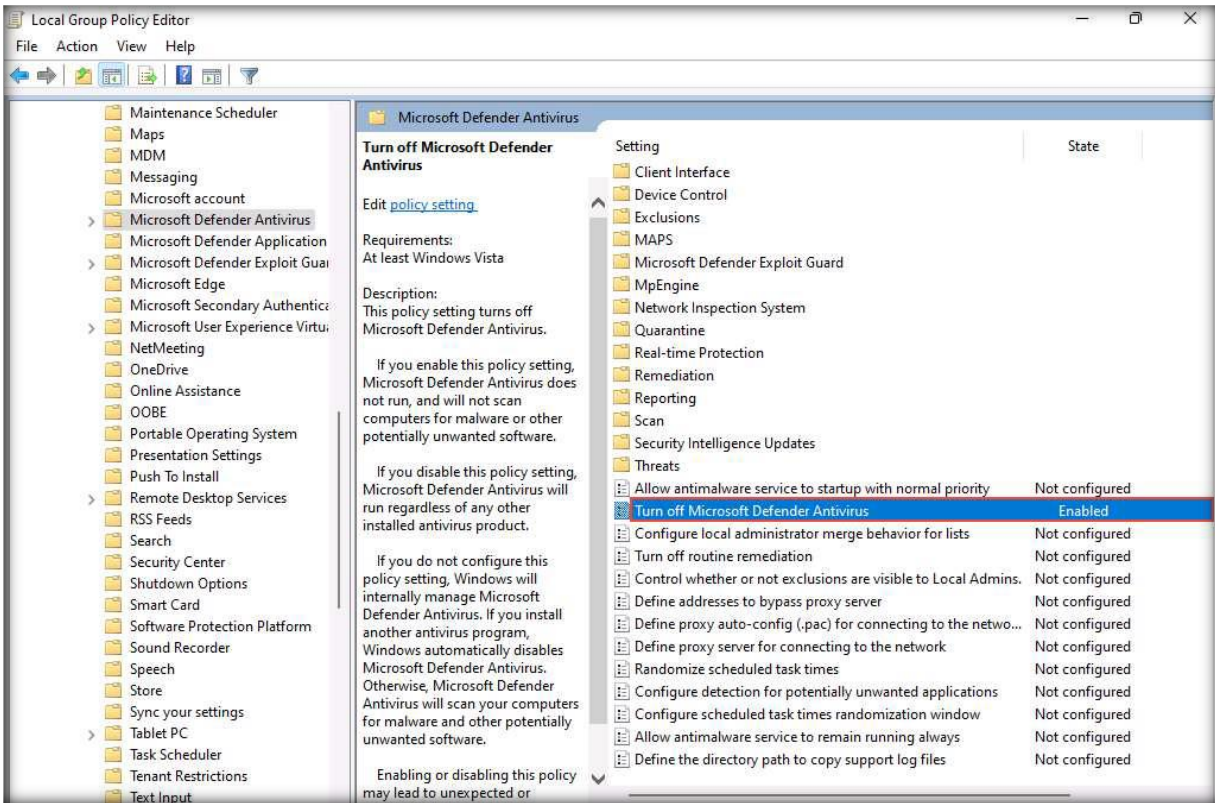
Note: If you are using an older version of **Windows**, you might see a **Windows Defender Antivirus** folder instead of **Microsoft Defender Antivirus**.



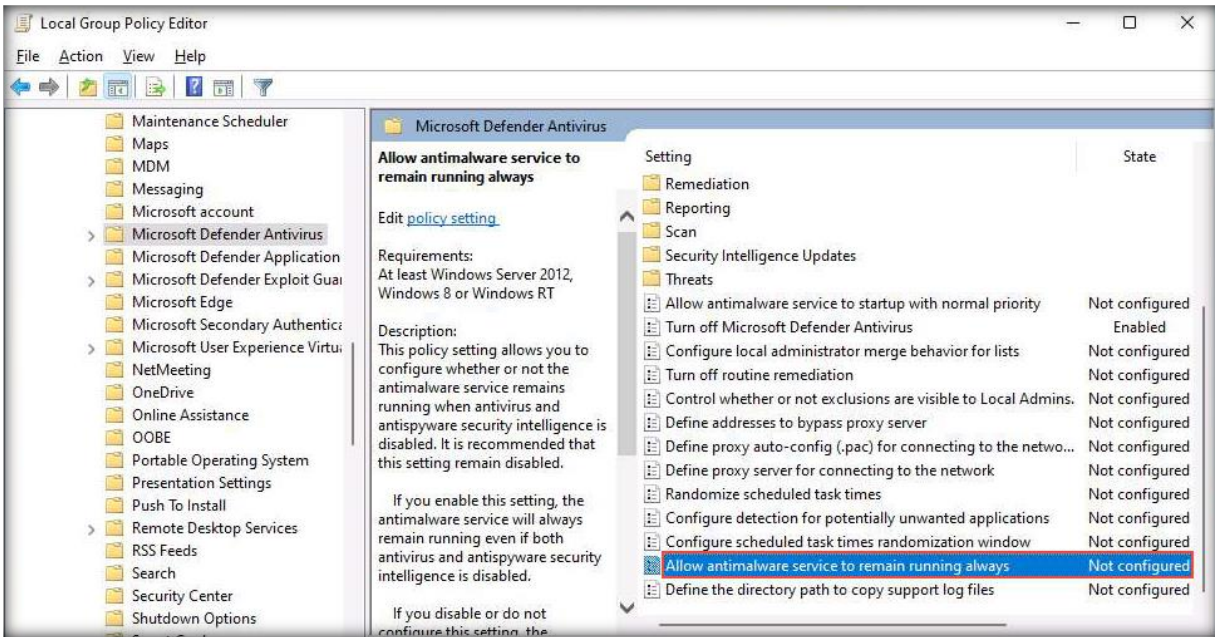
14. When the **Turn off Microsoft Defender Antivirus** window appears, select the **Enabled** radio button, click **Apply**, and then click **OK** to turn off **Microsoft Defender Antivirus**.



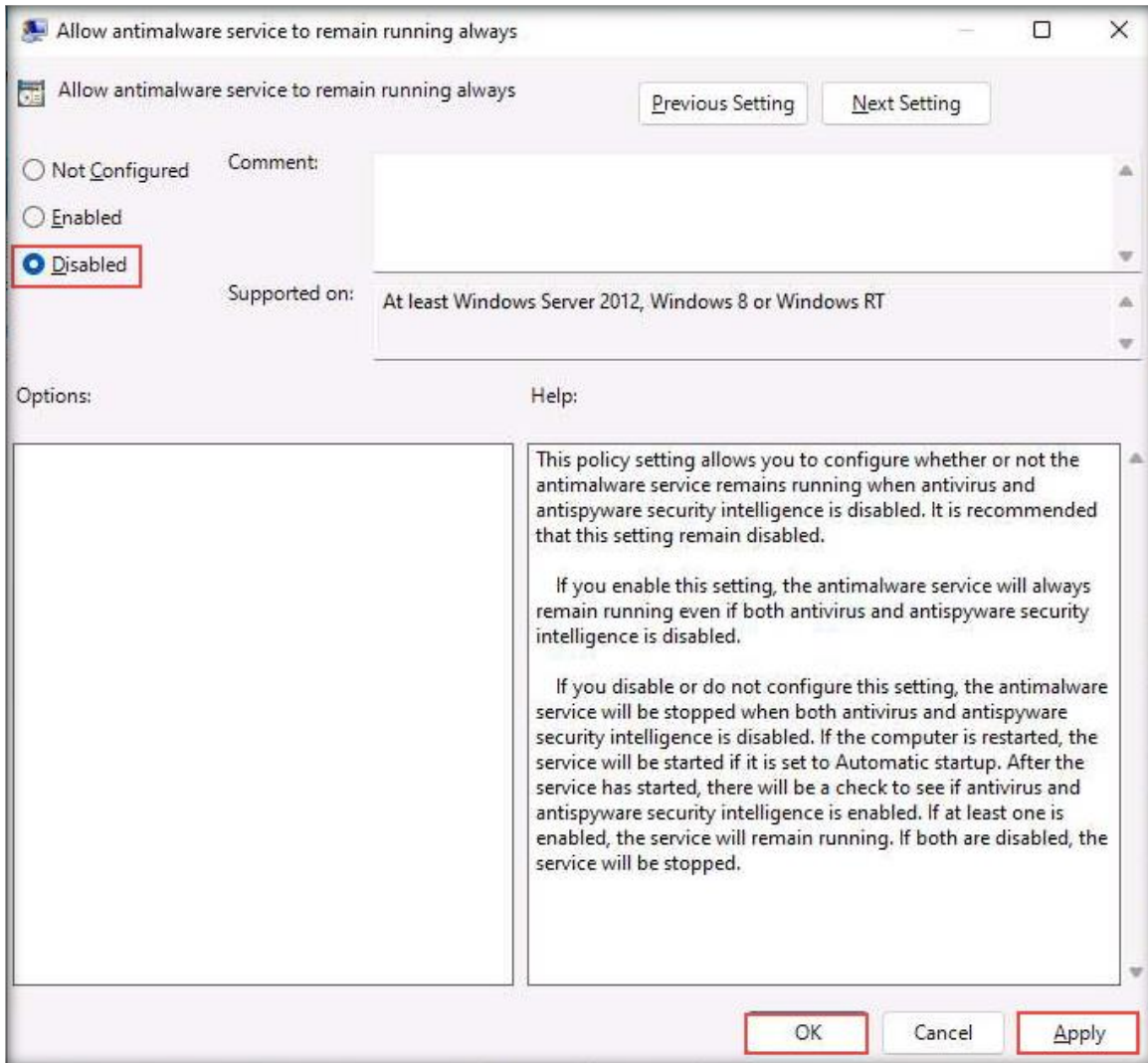
15. Microsoft Defender Antivirus is turned off.



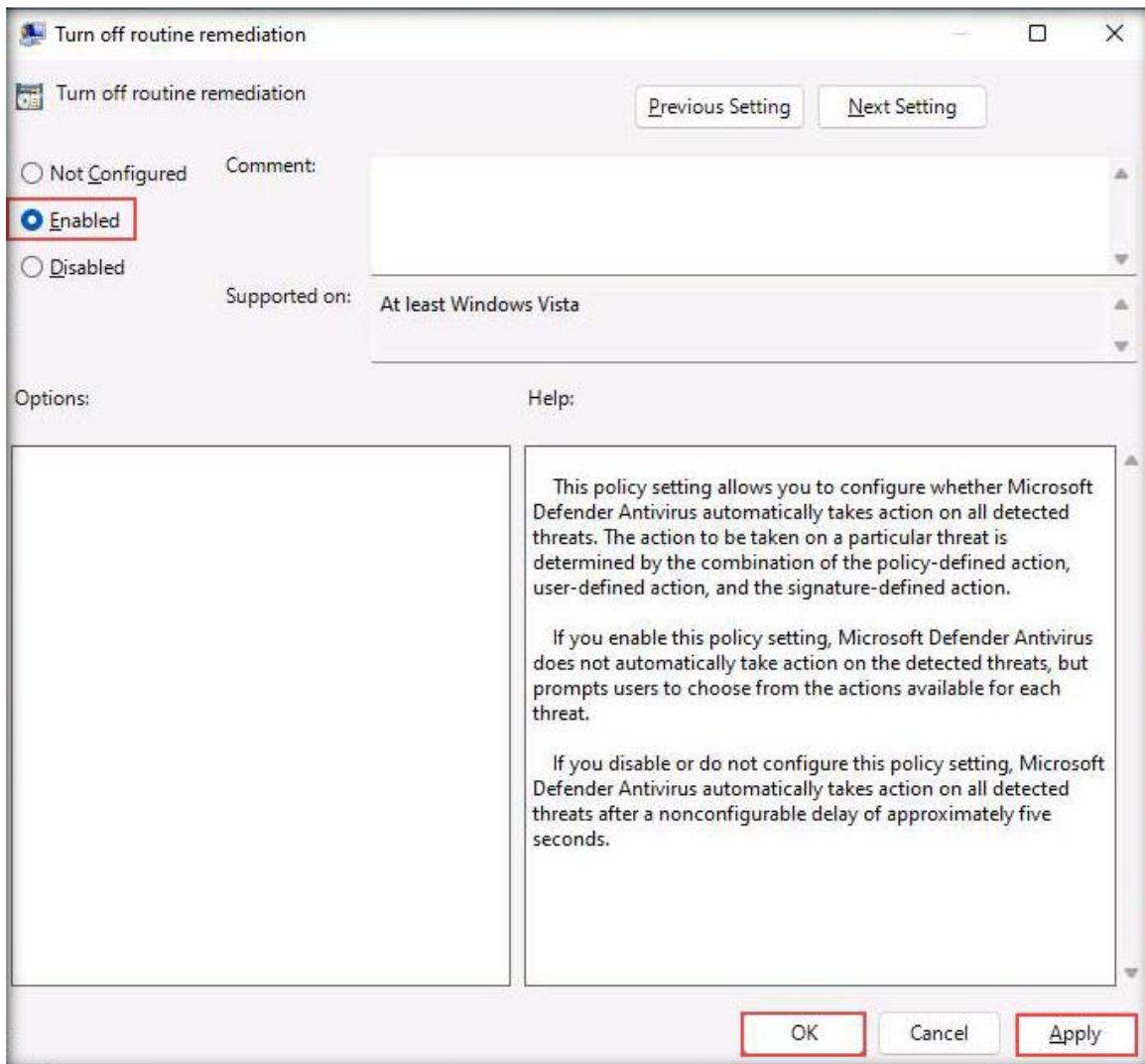
16. In the Local Group Policy Editor window, double-click Allow antimalware service to remain running always.



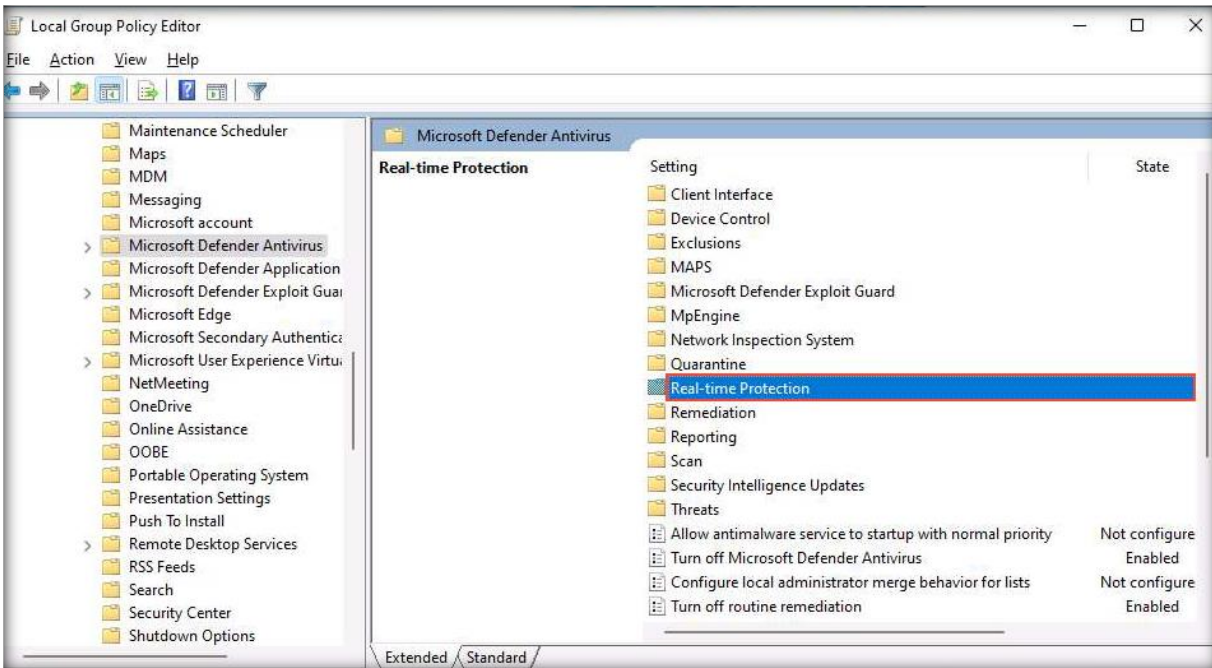
17. When the **Allow antimalware service to remain running always** window appears, select the **Disabled** radio button. Click **Apply** and then **OK**.



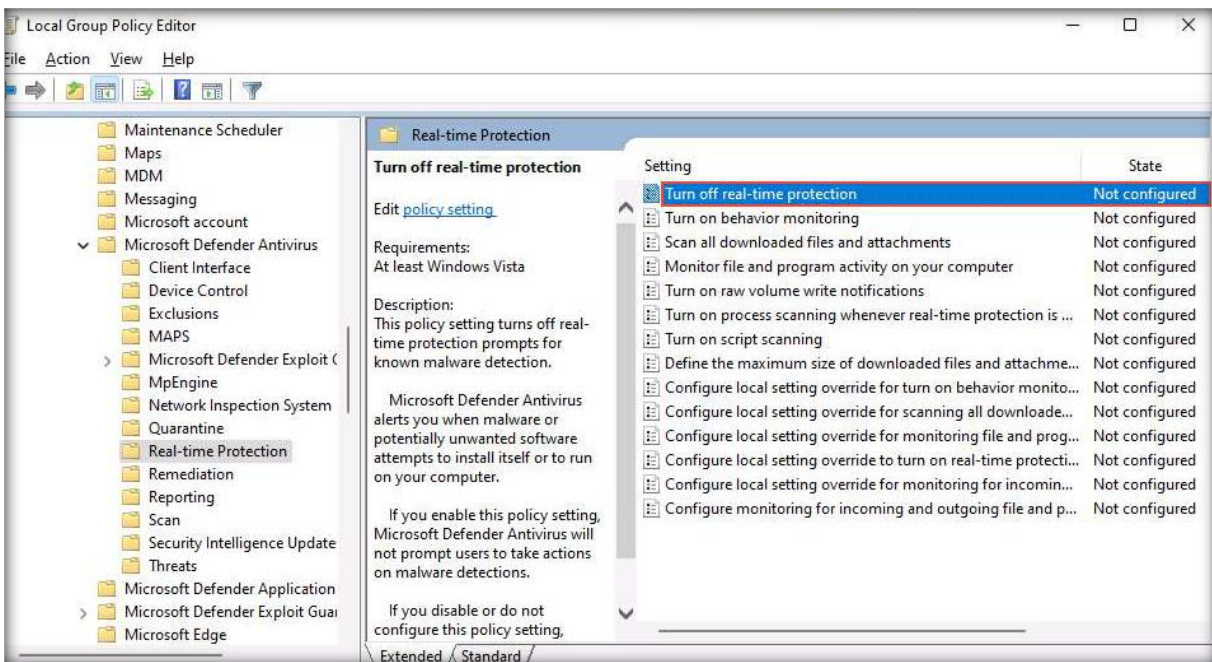
18. In the **Local Group Policy Editor** window, double-click **Turn off routing remediation**.
19. When the **Turn off routing remediation** window appears, select the **Enabled** radio button. Click **Apply** and then **OK**.



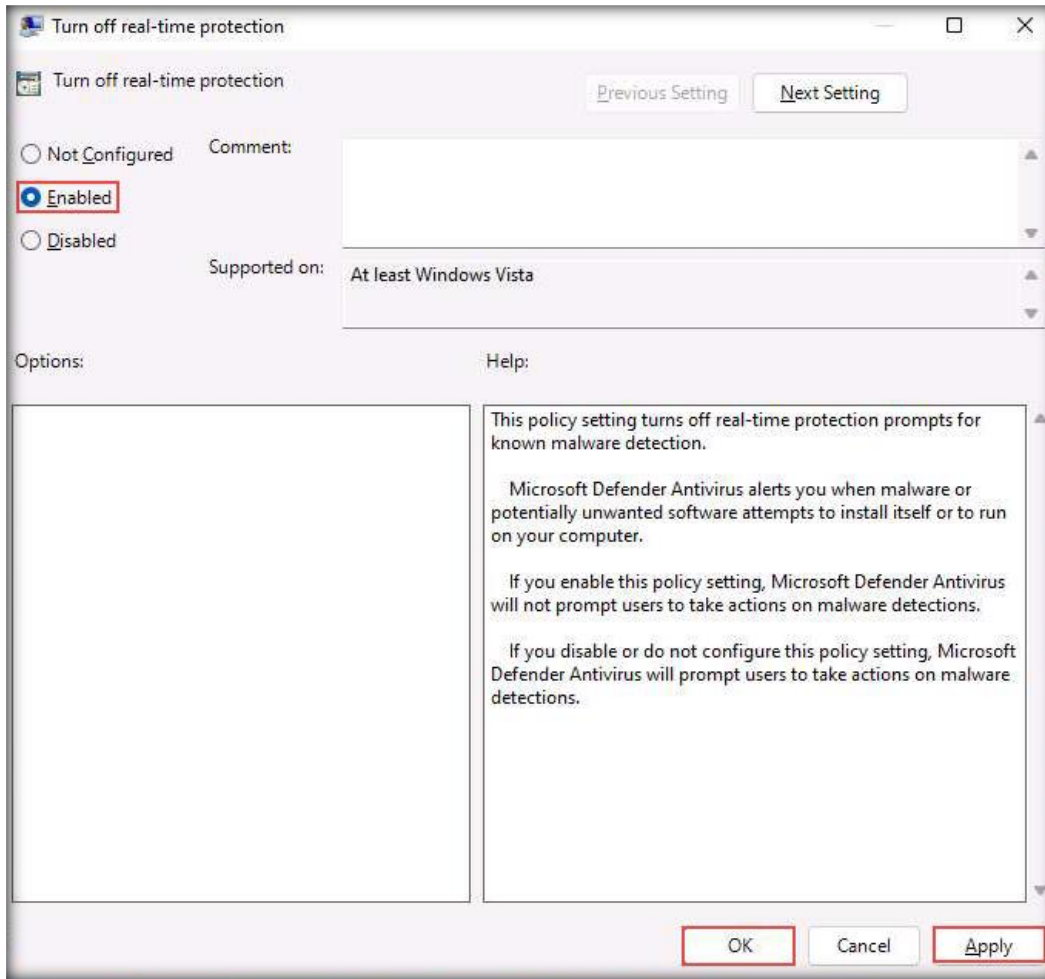
20. In the **Local Group Policy Editor** window, double-click the **Real-time Protection** folder.



21. In the **Real-time Protection** window, double-click **Turn off real-time protection**.



22. When the **Turn off real-time protection** window appears, select the **Enabled** radio button. Click **Apply** and then **OK**.

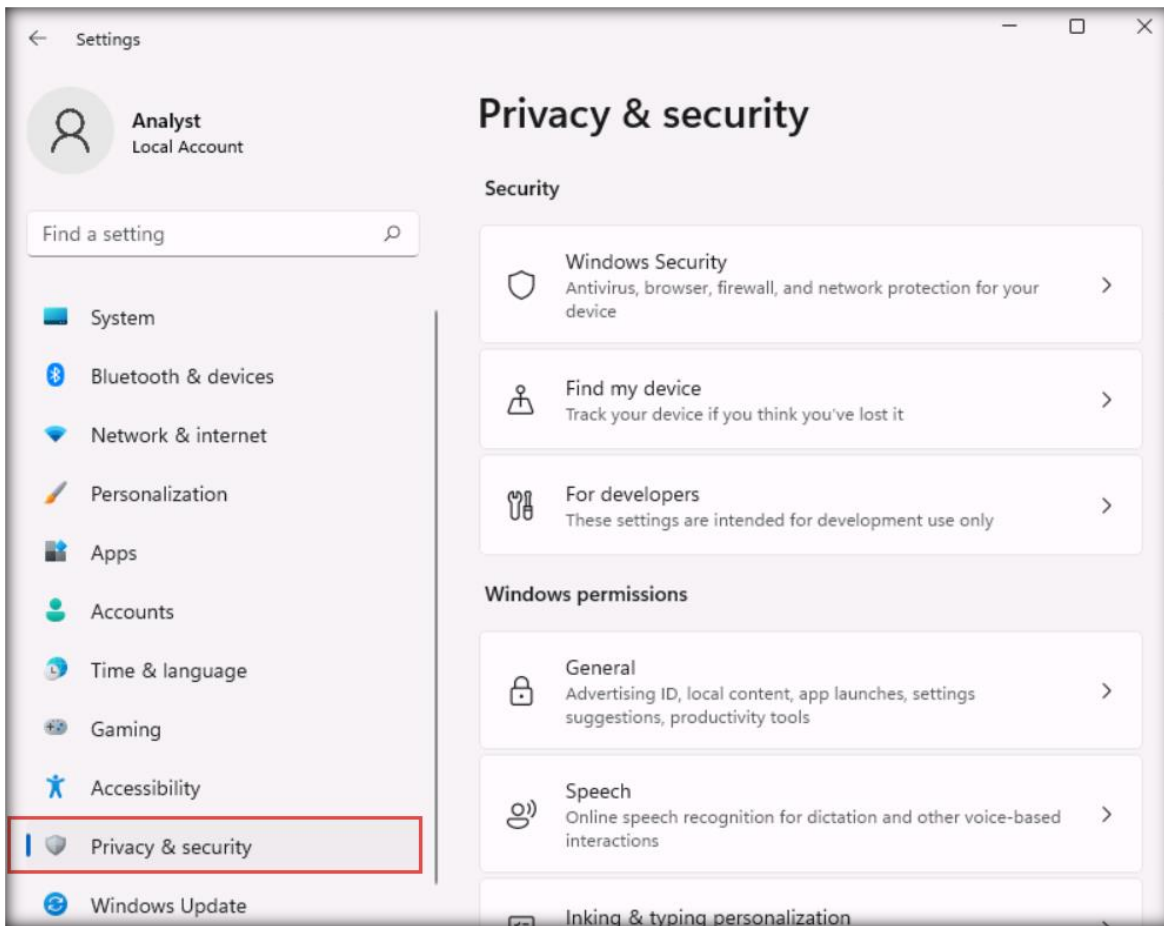


23. Close all windows.

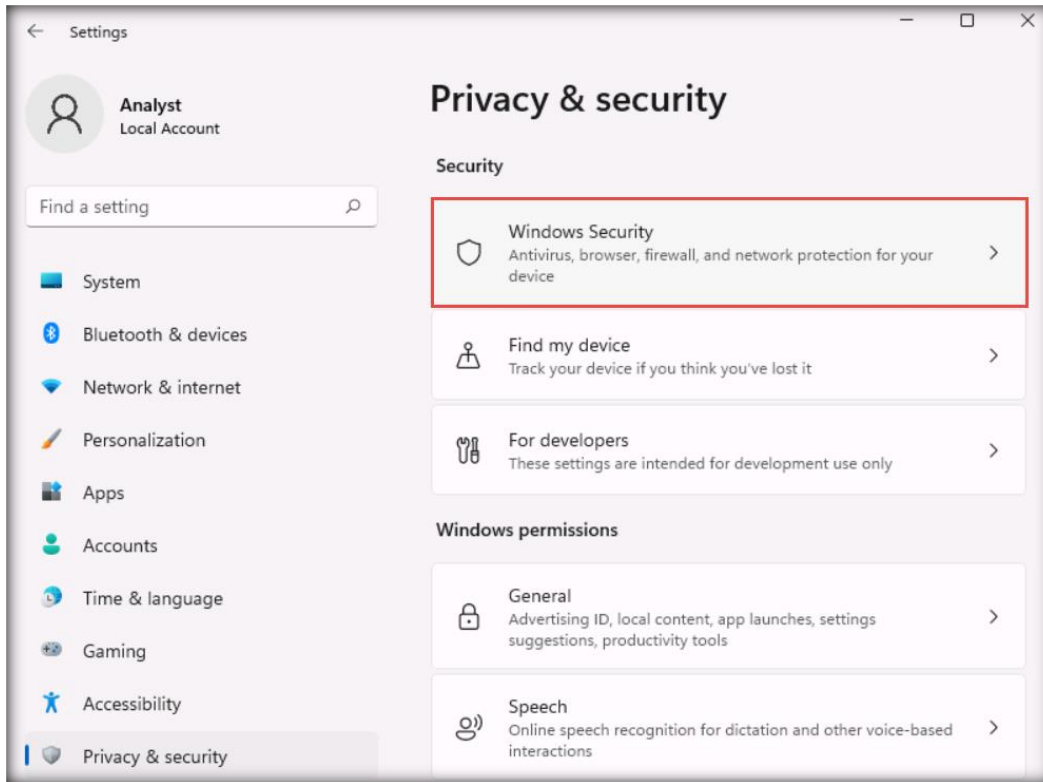
24. Right-click the **Windows** button in the lower-left corner of the screen and click **Settings**.



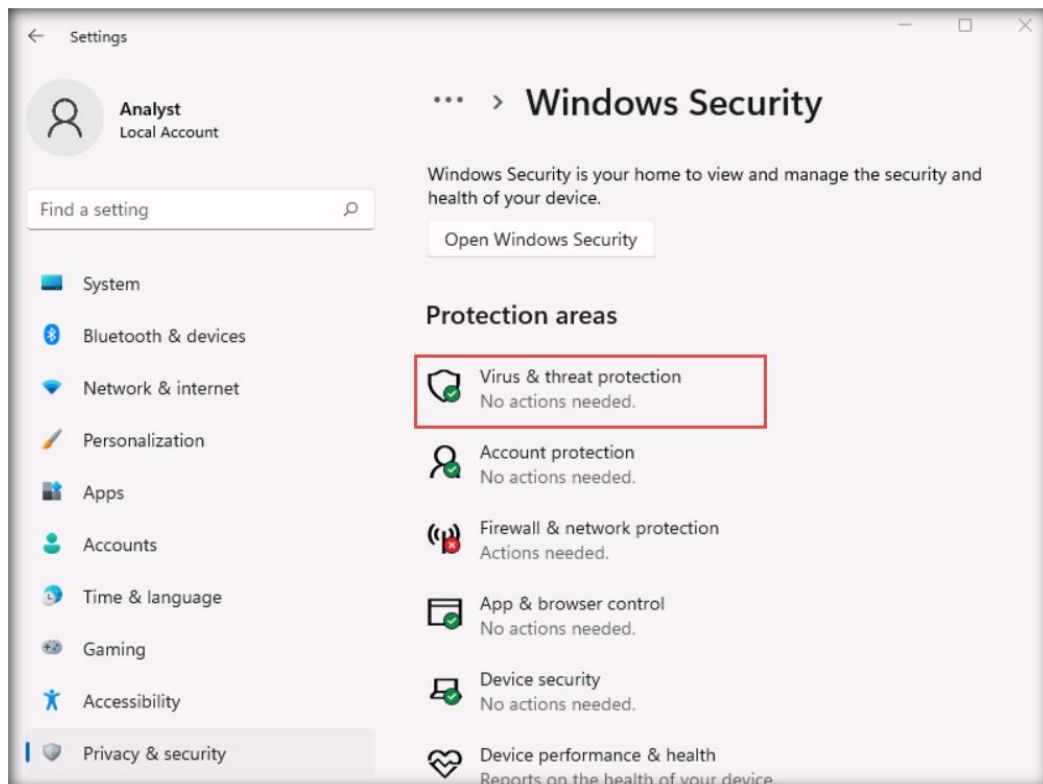
25. In the **Settings** window, click **Privacy & security** from the left-hand pane.



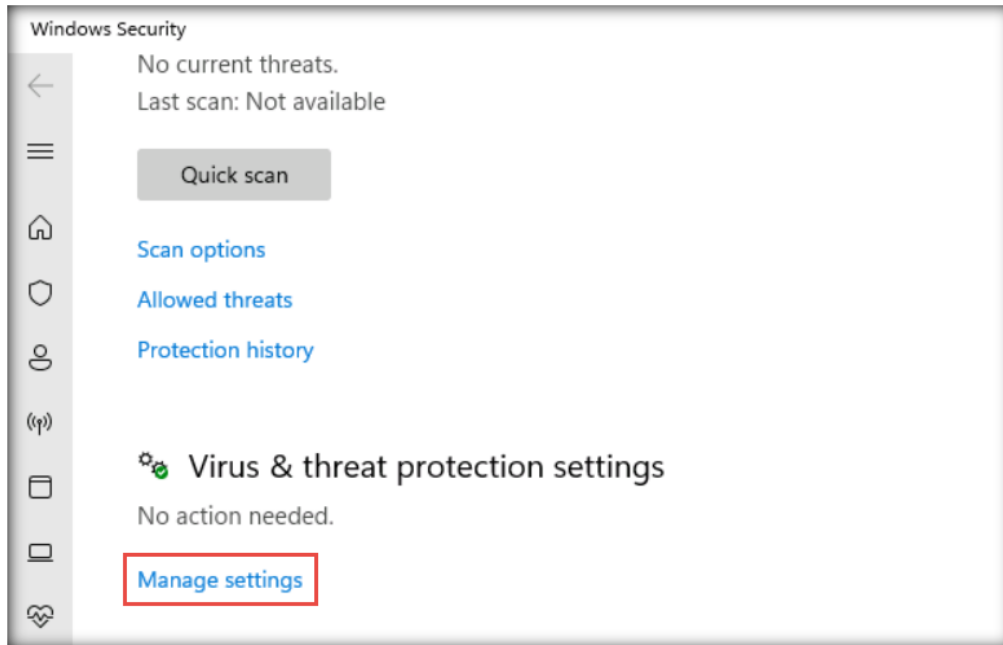
26. The **Privacy & security** settings appear in the right-hand pane. Then, click the **Windows Security** option.



27. In the **Windows Security** window, click **Virus & threat protection**.

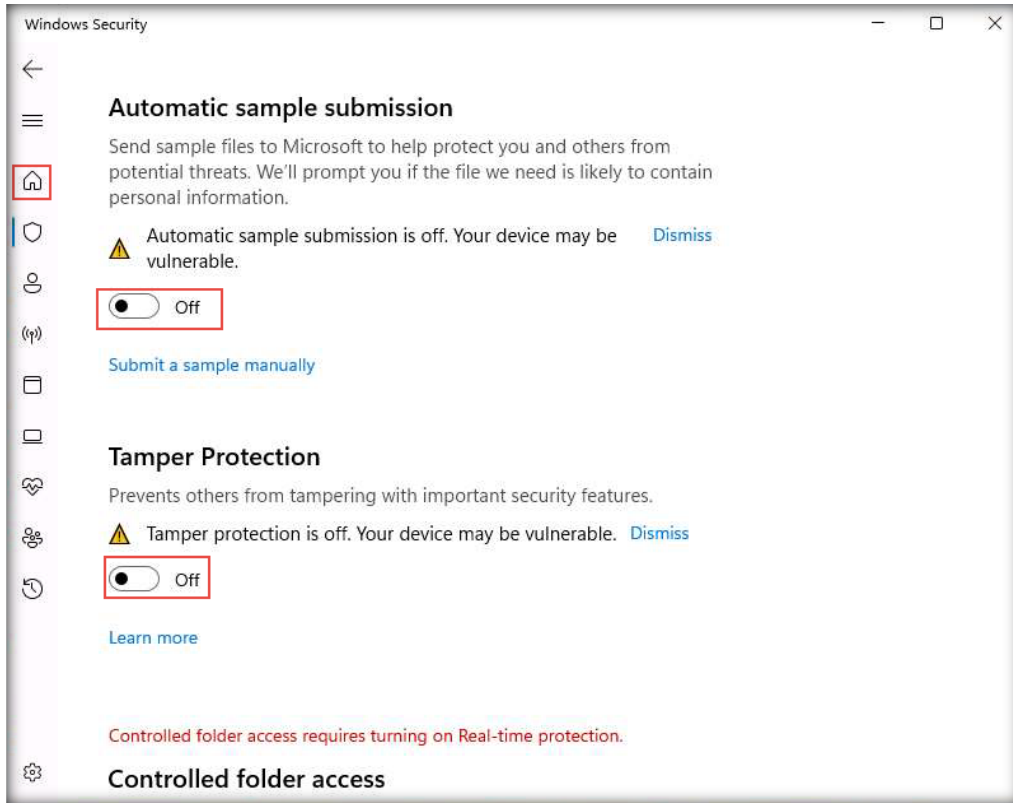


28. On the **Virus & threat protection** page, click **Manage settings** under **Virus & threat protection settings**.

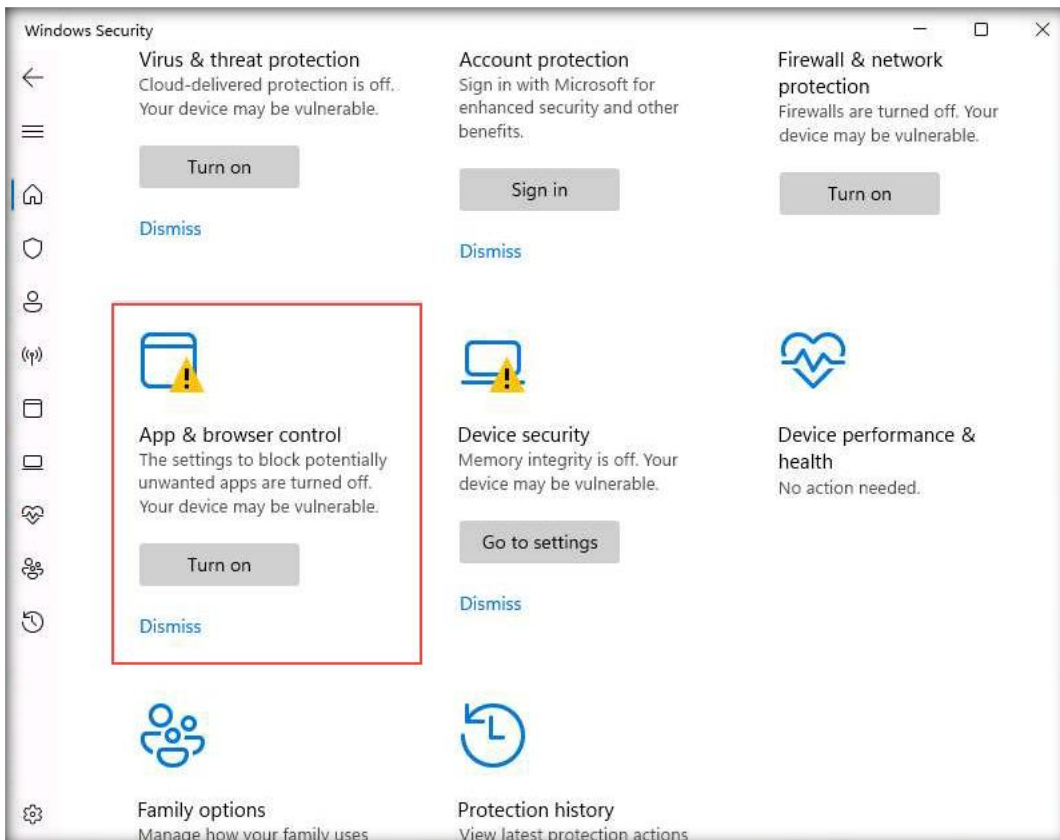


29. When the **Virus & threat protection settings** page appears, turn off **Real-time protection**, **Cloud-delivered protection**, **Automatic sample submission**, and **Tamper Protection**. If a **User Account Control** pop-up window appears, click **Yes**. After turning off the above-mentioned items, click the **Home** icon in the left menu bar.

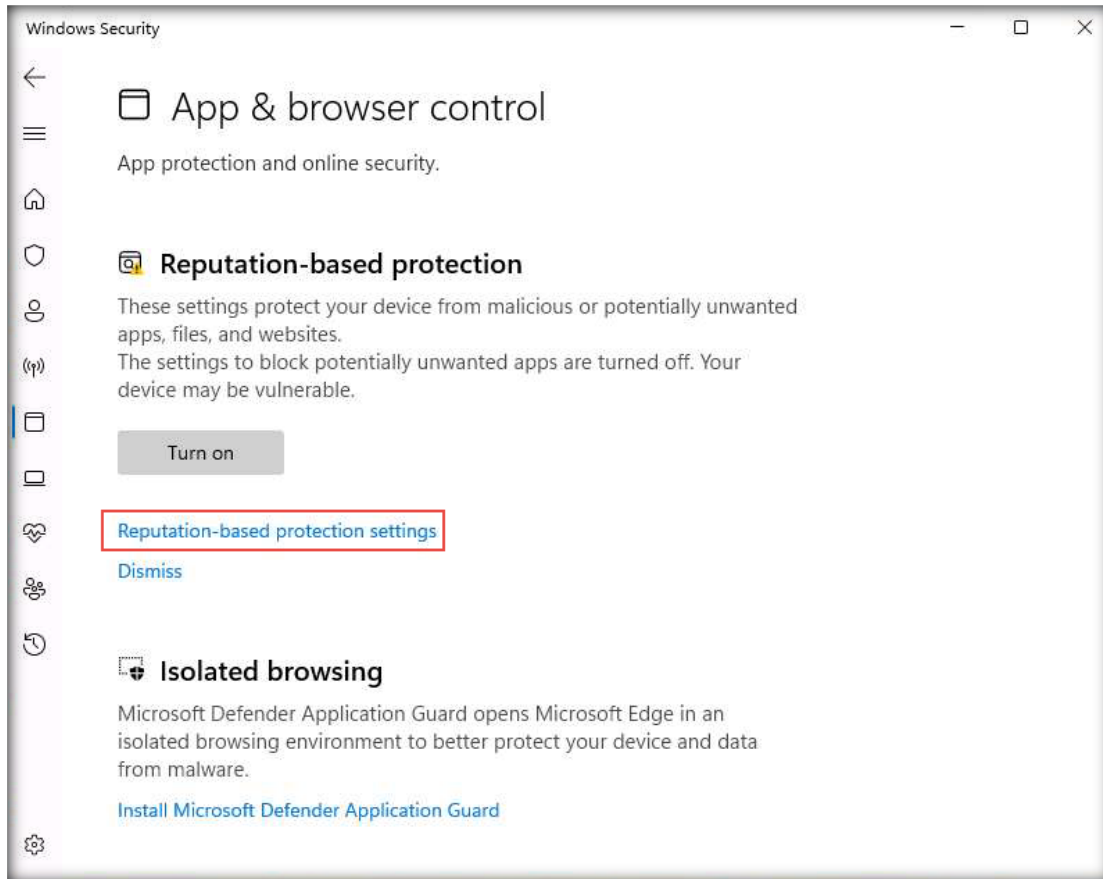




30. Next, click **App & browser control** in the **Windows Security** window.

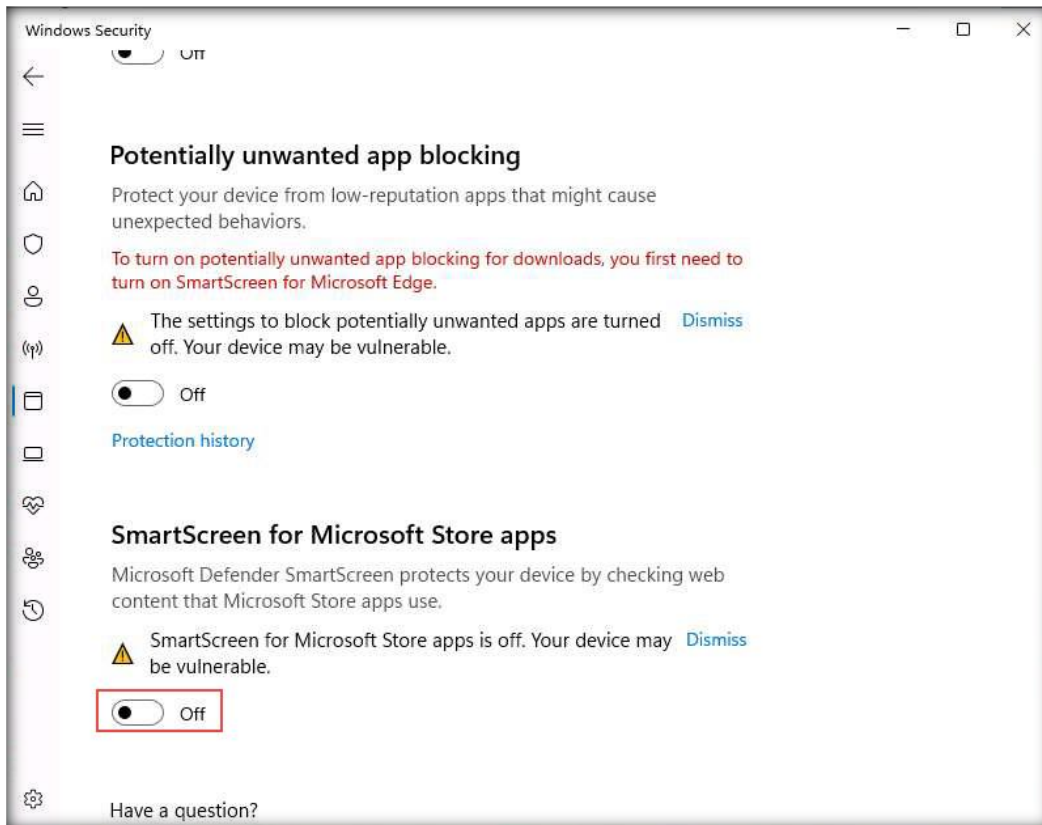
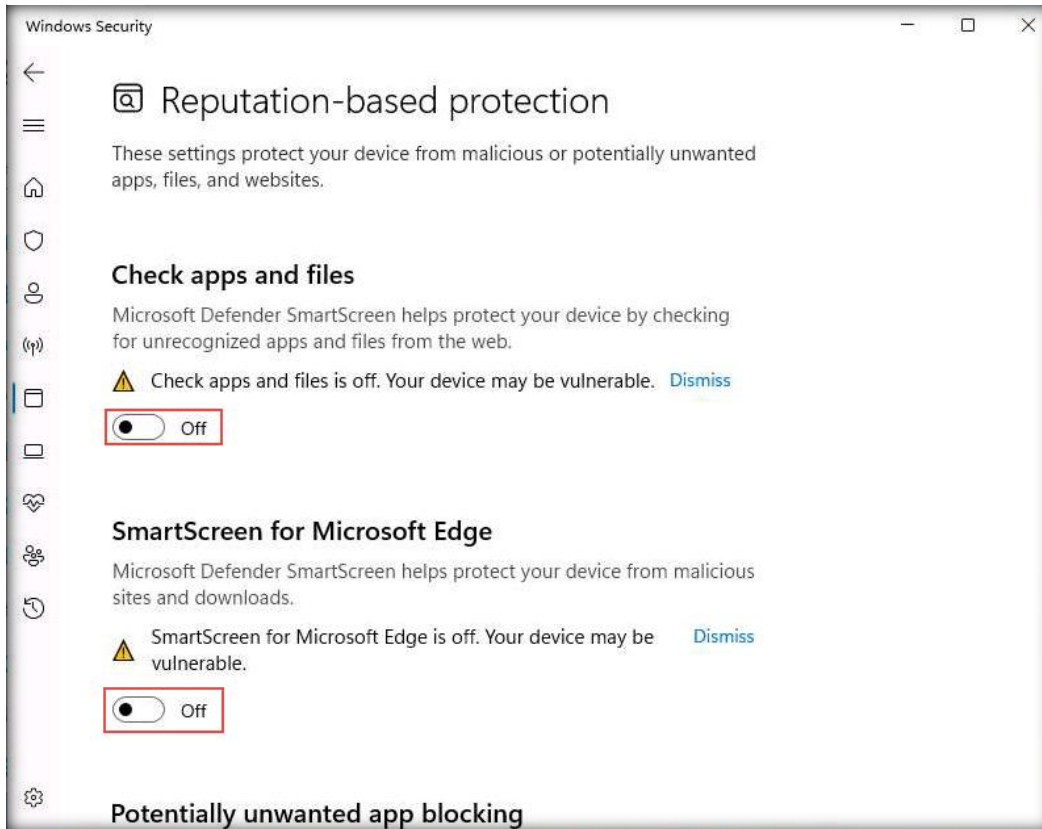


31. In the **App & browser control** page, click the **Reputation-based protection settings** link under **Reputation-based protection**.



32. The **Reputation-based protection** page appears. Select the **Off** radio buttons under **Check apps and files**, **SmartScreen for Microsoft Edge**, and **SmartScreen for Microsoft Store apps**. If a **User Account Control** pop-up window appears, click **Yes**.

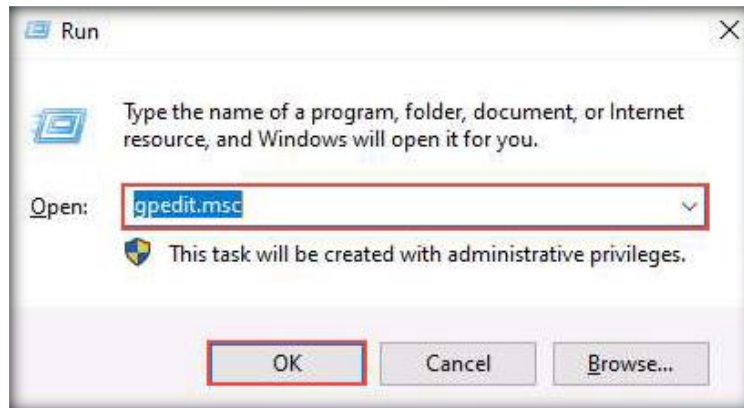
Note: If you are unable to turn off the **SmartScreen for Microsoft Edge** radio button, leave the setting for **SmartScreen for Microsoft Edge** radio button as it is, and continue with the setup.



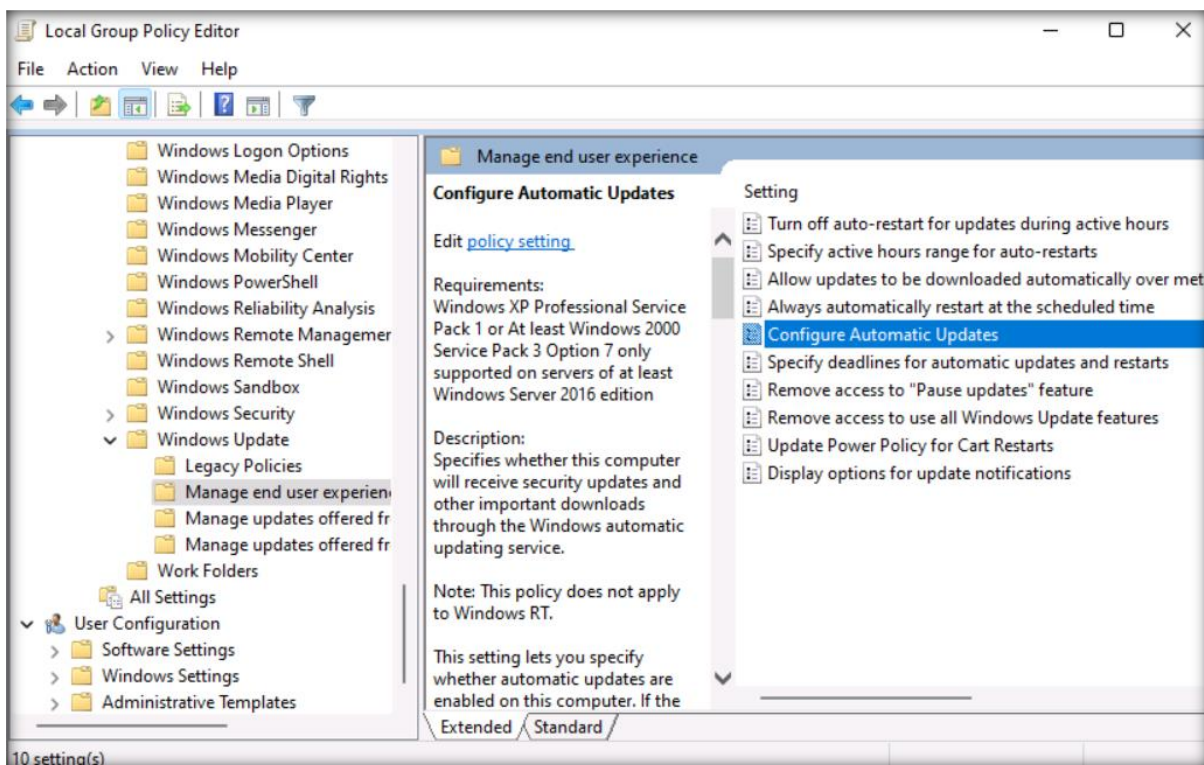
33. Close all windows.

CT#11: Configure Windows Components on the Windows 11 Virtual Machine

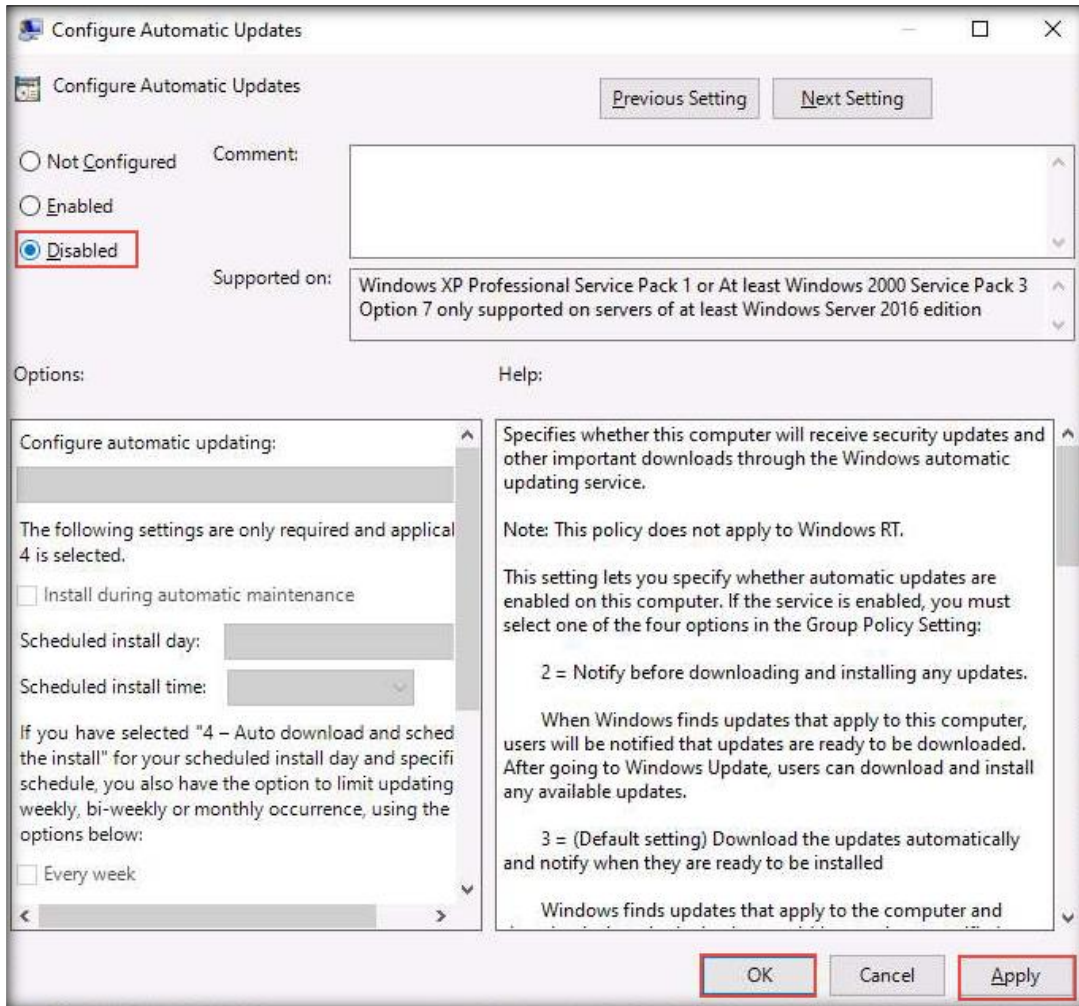
1. Log in to the **Windows 11** virtual machine. Right-click on **Start** and click **Run**.
2. The **Run** window appears; type **gpedit.msc** and click **OK**.



3. The **Local Group Policy Editor** window appears; expand **Administrative Templates** under **Computer Configuration** in the left pane.
4. In **Administrative Templates**, expand **Windows Components**, scroll down, click **Windows Update** in the left pane, and double-click **Manage end user experience**.
5. Under Manage end user experience, double-click **Configure Automatic Updates** in the right-hand pane, as shown in the screenshot below.

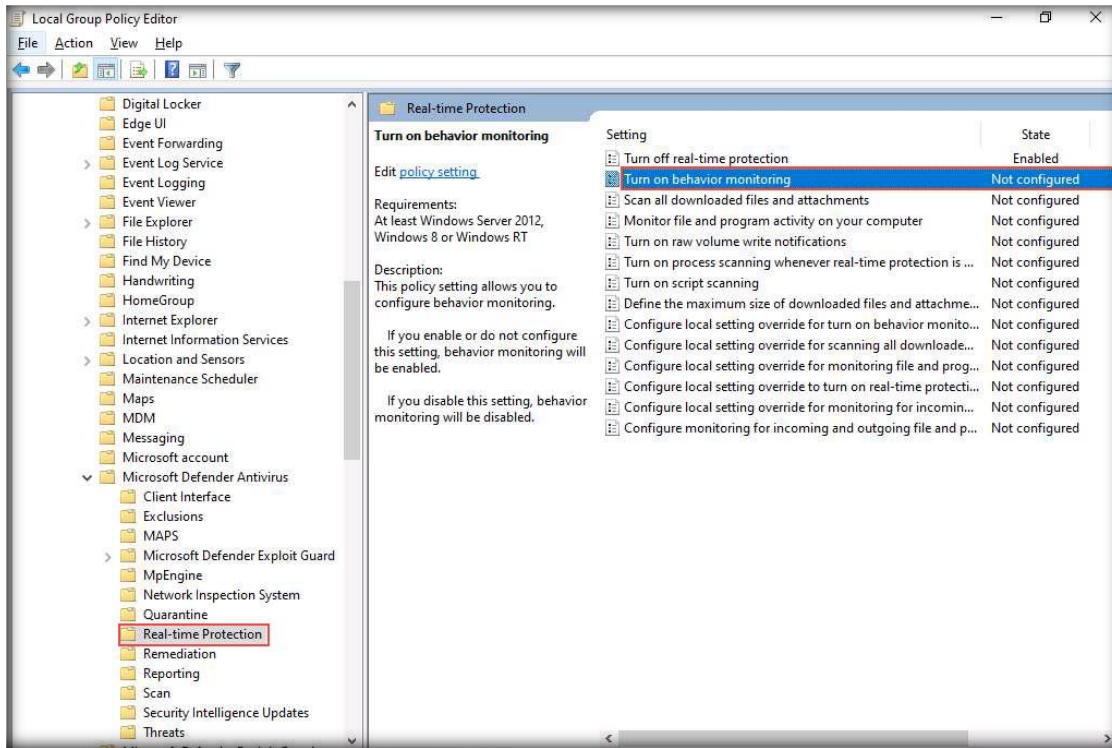


- The **Configure Automatic Updates** window appears; select the **Disabled** radio button. Click **Apply** and then **OK**.

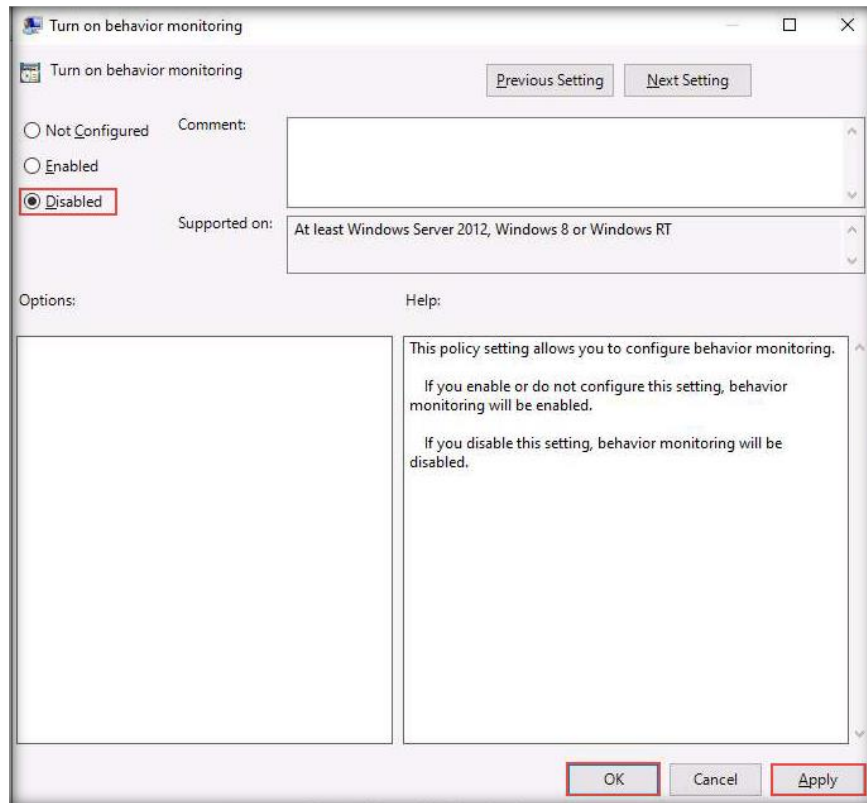


- In the left-hand pane, navigate to **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Windows Defender Antivirus** → **Real-time Protection**.

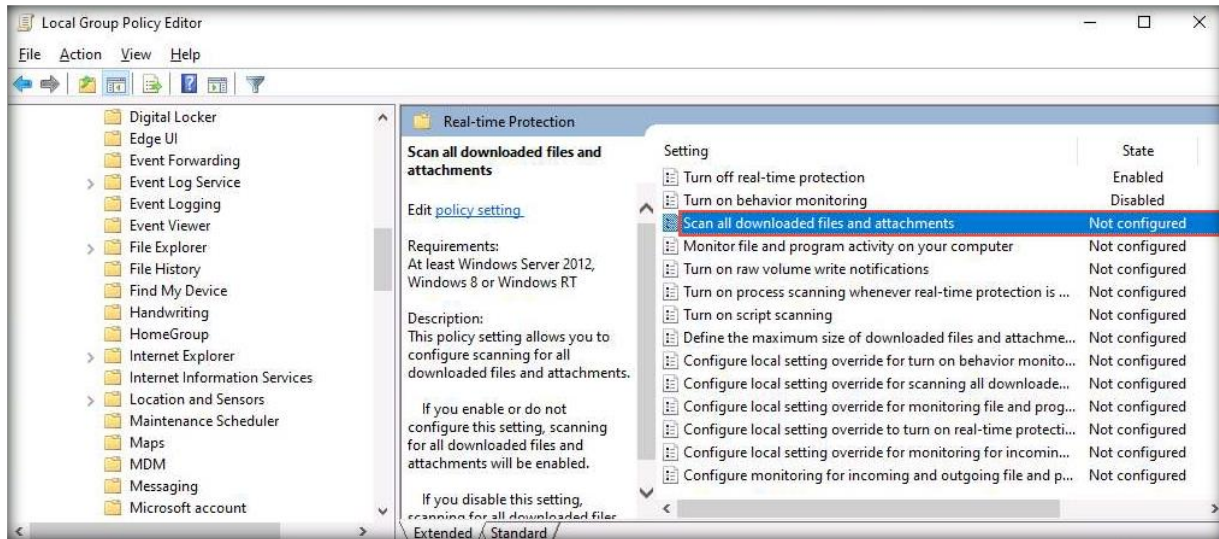
8. Double-click the **Turn on behavior monitoring** setting to configure its settings.



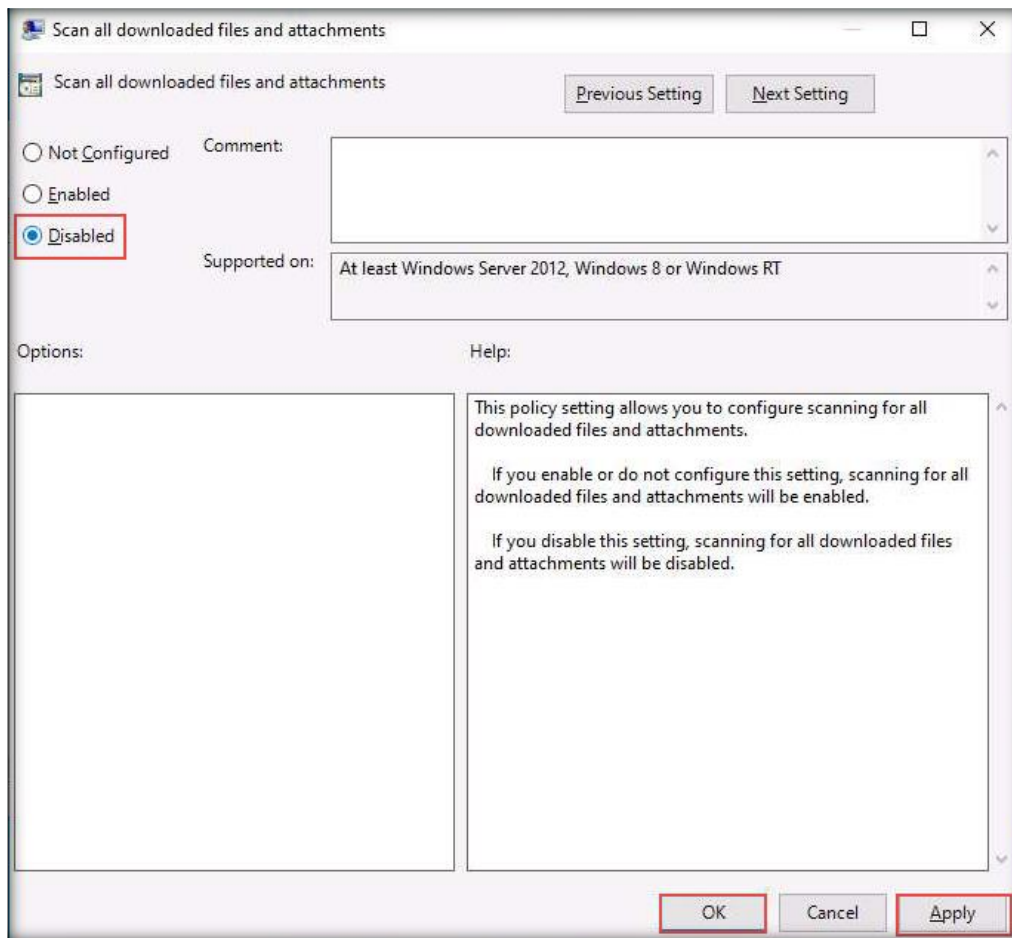
9. The **Turn on behavior monitoring** window appears. Select the **Disabled** radio button. Click **Apply** and then **OK**.



10. Double-click the **Scan all downloaded files and attachments** setting, as shown in the screenshot below.



11. The **Scan all downloaded files and attachments** window appears. Select the **Disabled** radio button. Click **Apply** and then **OK**.



[\[Back to Configuration Task Outline\]](#)

CT#12: Install WinRAR on the Windows 11 Virtual Machine

1. Log in to the **Windows 11** virtual machine with the credentials **Analyst** and **Pa\$\$w0rd**.
2. Download the latest version of **WinRAR** from the official WinRAR website (<https://www.rarlab.com/download.htm>).
Note: Download the 64-bit version of **WinRAR**.
3. Double-click on the **winrar-x64-624.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
4. The **WinRAR** setup window appears; click **Install**.
5. Complete the installation by choosing the default settings throughout the installation process.
6. After completing the installation, the **installation location of WinRAR files** window opens automatically; close the window.

[\[Back to Configuration Task Outline\]](#)

CT#13: Install MS Office on the Windows 11 Virtual Machine

1. Download the latest version of **MS Office** from the official Microsoft website (<https://www.microsoft.com>).
Note: Download the 64-bit version of **MS Office**.
2. Double-click on the setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
3. Accept the license terms and complete the installation by choosing the default settings throughout the installation process.

[\[Back to Configuration Task Outline\]](#)

CT#14: Download CTIA Tools on the Windows 11 Virtual Machine

1. Log in to the **Windows 11** virtual machine with the credentials **Analyst** and **Pa\$\$w0rd**.
2. Create a folder on drive **E:** named **CTIA-Tools**.
3. Log in to your **Aspen** account (you will see your course listed under **My Courses**). Click the **TRAINING** button under the course to access the e-Courseware, Lab Manuals, and tools in the **Training** area. → Click the **Download Tools** tab in the left-hand pane.

4. Click the module names in the right-hand pane (except CTIAv2 ISO.zip) and download all the **CTIA Tools** files to the **E:\CTIA-Tools** folder.
5. Right-click the .zip files in the **E:\CTIA-Tools** folder and select the **Extract Here** option.

[\[Back to Configuration Task Outline\]](#)

CT#15: Adding .NET Framework in the Windows 11 Virtual Machine

1. Log in to the **Windows 11** virtual machine using the credentials **Analyst** and **Pa\$\$w0rd**.
2. Navigate to the **E:\CTIA-Tools\CTIA Lab Prerequisites\.NET Framework** folder.
3. Alternatively, you may download the latest version of **.NET Framework** from the official website.
4. Double-click on the **dotNetFx35setup.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
5. The **.NET Framework** setup window appears; click **Install**.
6. Complete the installation by choosing the default options throughout.
7. Close the window.

[\[Back to Configuration Task Outline\]](#)

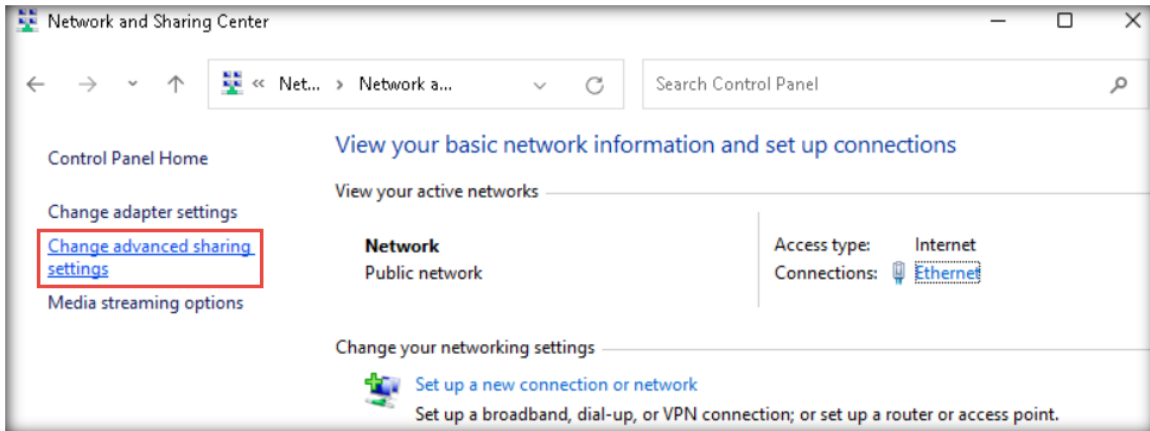
CT#16: Install Java Runtime Environment and Java Development Kit in the Windows 11 Virtual Machine

1. In the **Windows 11** virtual machine, navigate to **E:\CTIA-Tools\CTIA Lab Prerequisites**.
2. Open the **Java Runtime Environment** folder.
3. Double-click the **jre-8u391-windows-x64.exe** file and follow the **wizard-driven** installation steps to install Java Runtime Environment.
4. Similarly, navigate to **E:\CTIA-Tools\CTIA Lab Prerequisites\Java Development Kit** folder.
5. Double-click the **jdk-8u171-windows-i586.exe** file and follow the **wizard-driven** installation steps to install Java Development Kit.
6. You can also download the **latest versions** of Java Runtime Environment and Java Development Kit from the respective vendors.

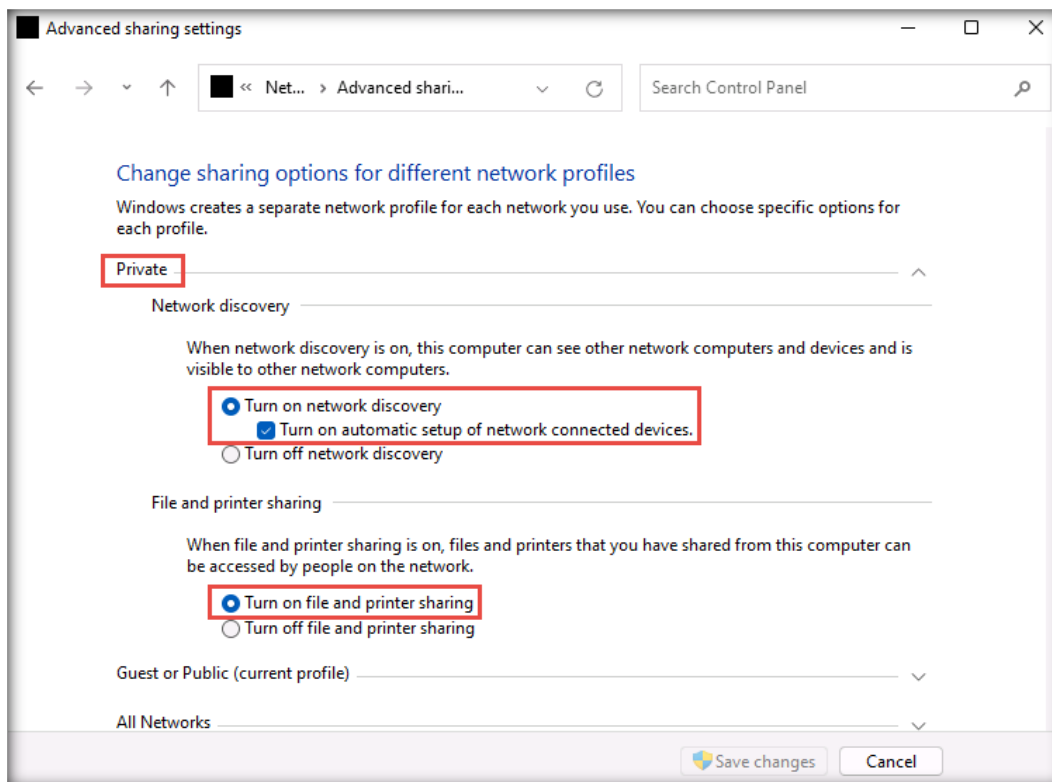
[\[Back to Configuration Task Outline\]](#)

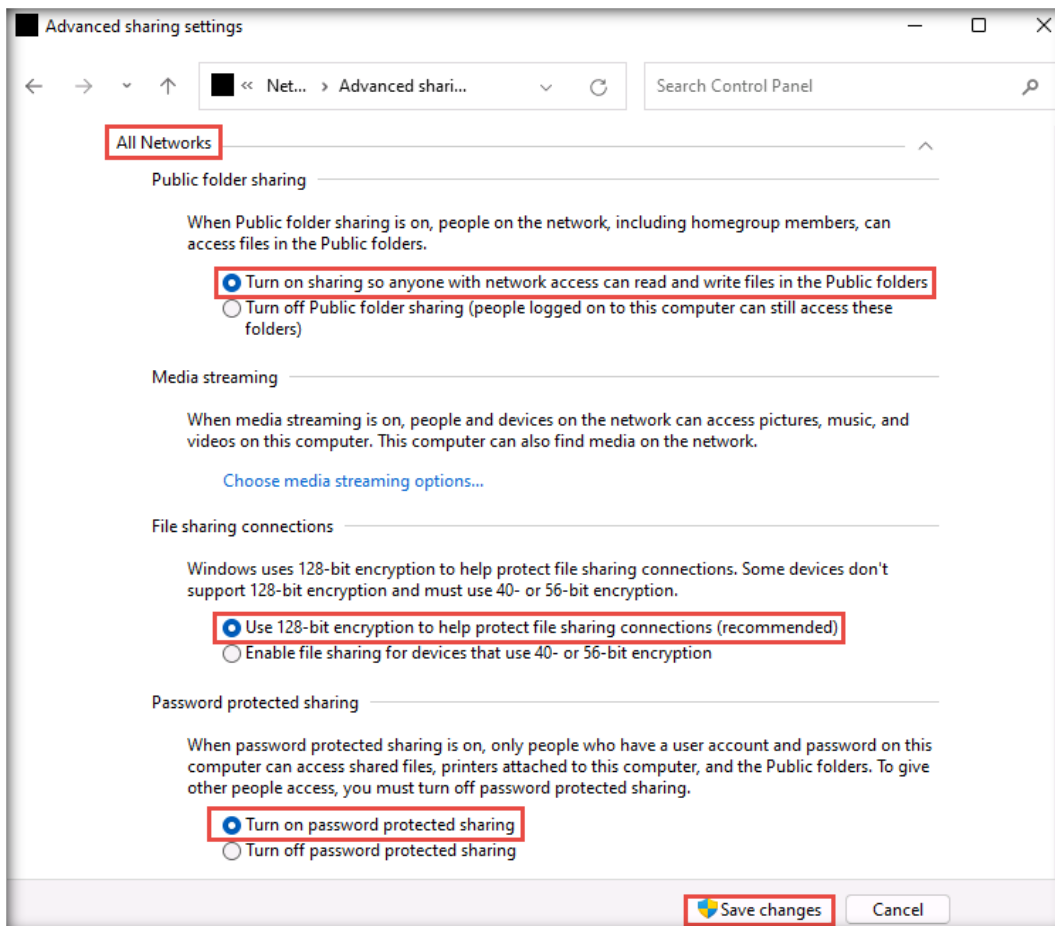
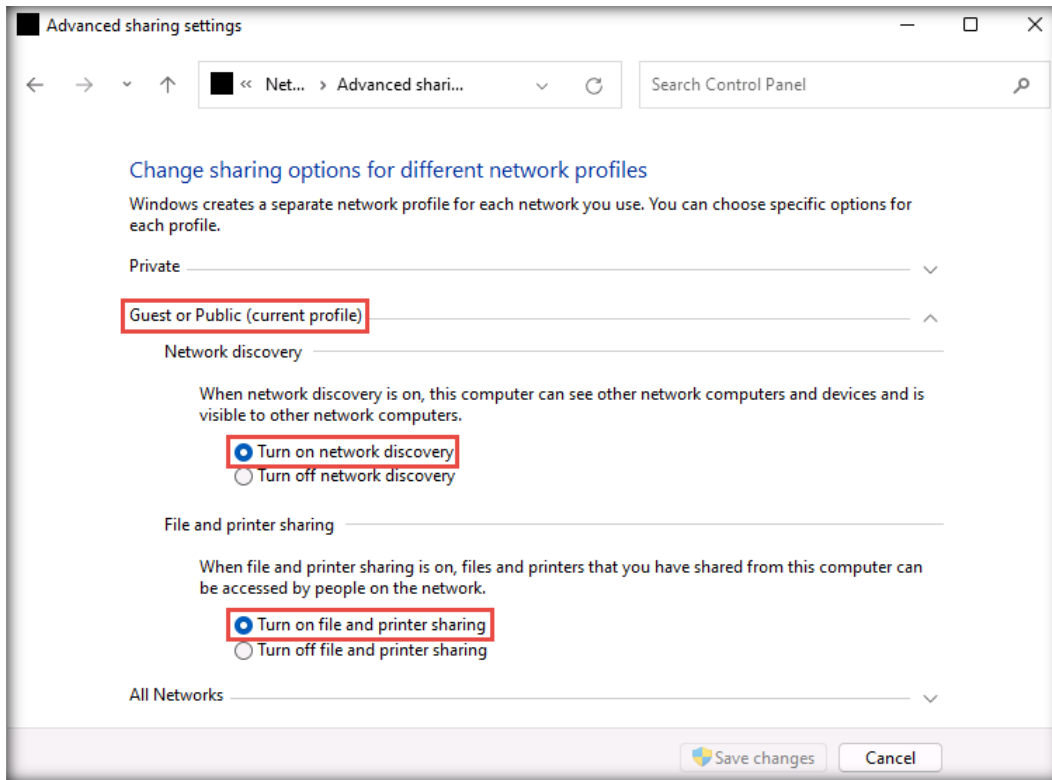
CT#17: Share and Map CTIA-Tools Folder to Parrot Security Virtual Machine

1. Log in to the **Windows 11** virtual machine with the credentials **Analyst** and **Pa\$\$w0rd**.
2. Open **Network and Sharing Center** by navigating to **Control Panel** → **Network and Internet** → **Network and Sharing Center**.
3. In the **Network and Sharing Center** window, click the **Change advanced sharing settings** link in the left pane.

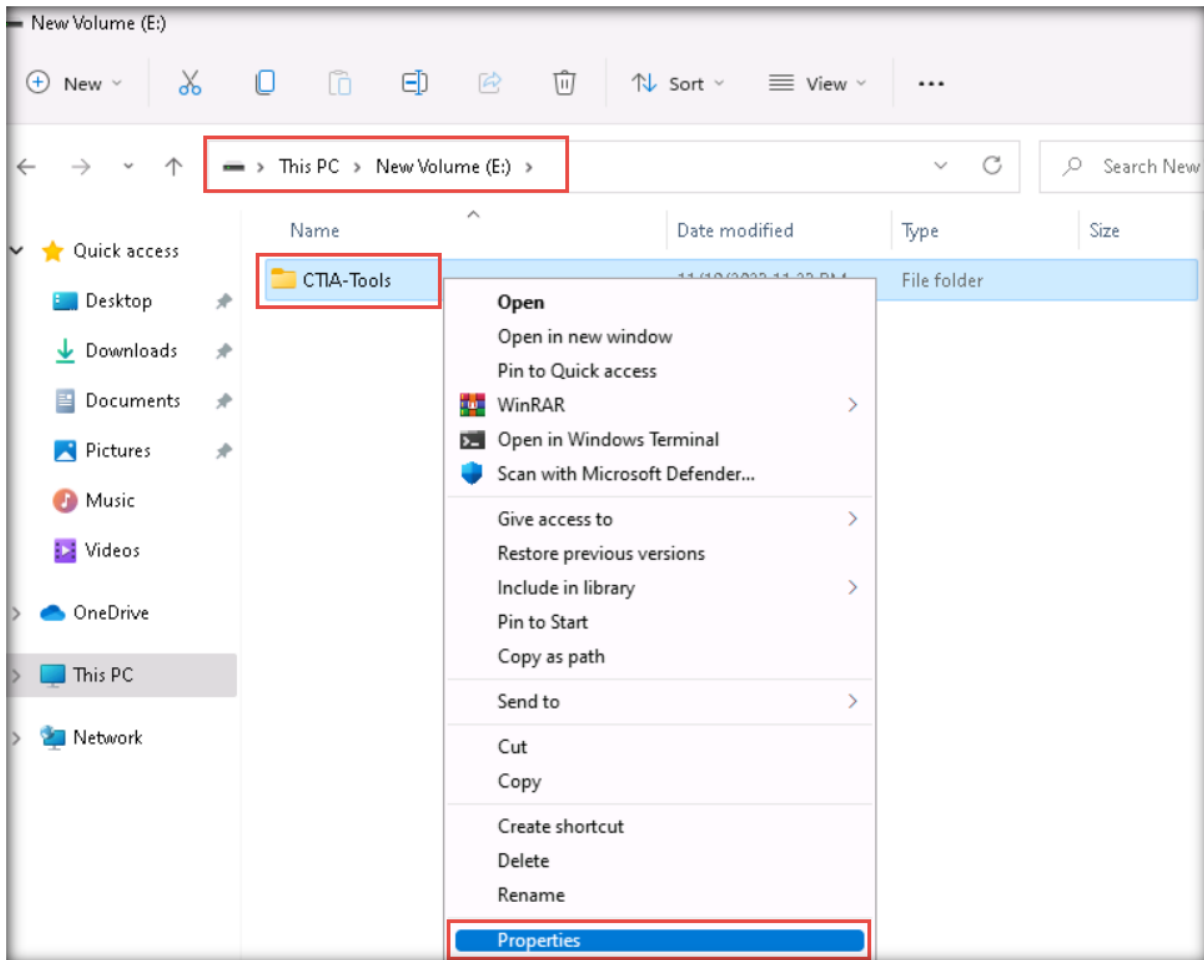


4. In the **Advanced sharing settings** window, turn on network discovery as well as file and printer sharing under **Private (current profile)**, **Guest or Public**, and **All Networks**, as shown in the screenshots below, and click **Save changes**.



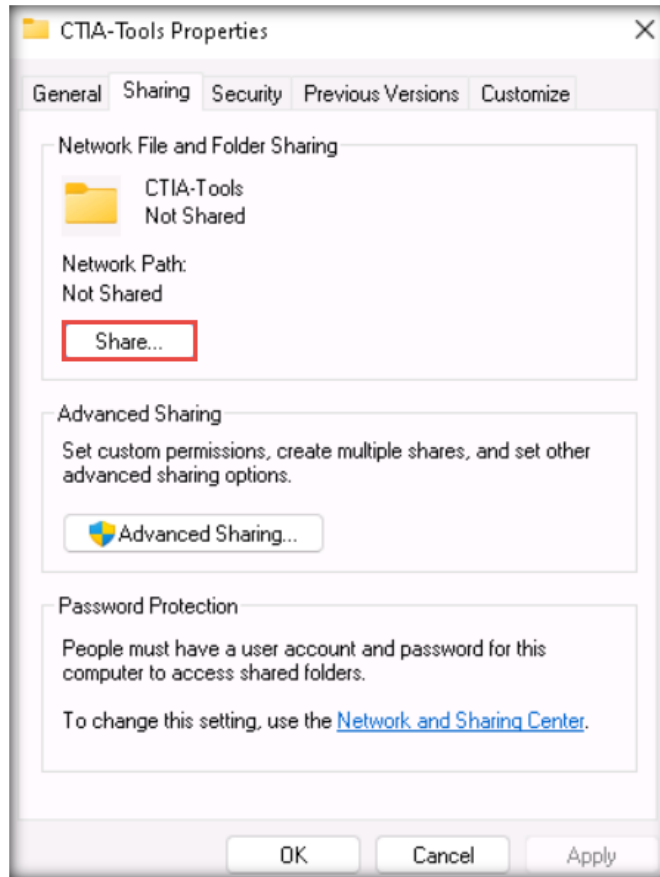


5. Close the **Network and Sharing Center** window.
6. Now, open a **File Explorer** window, navigate to the **E:** drive, right-click on the **CTIA-Tools** folder, and navigate to **Show more options** → **Properties** from the context menu.

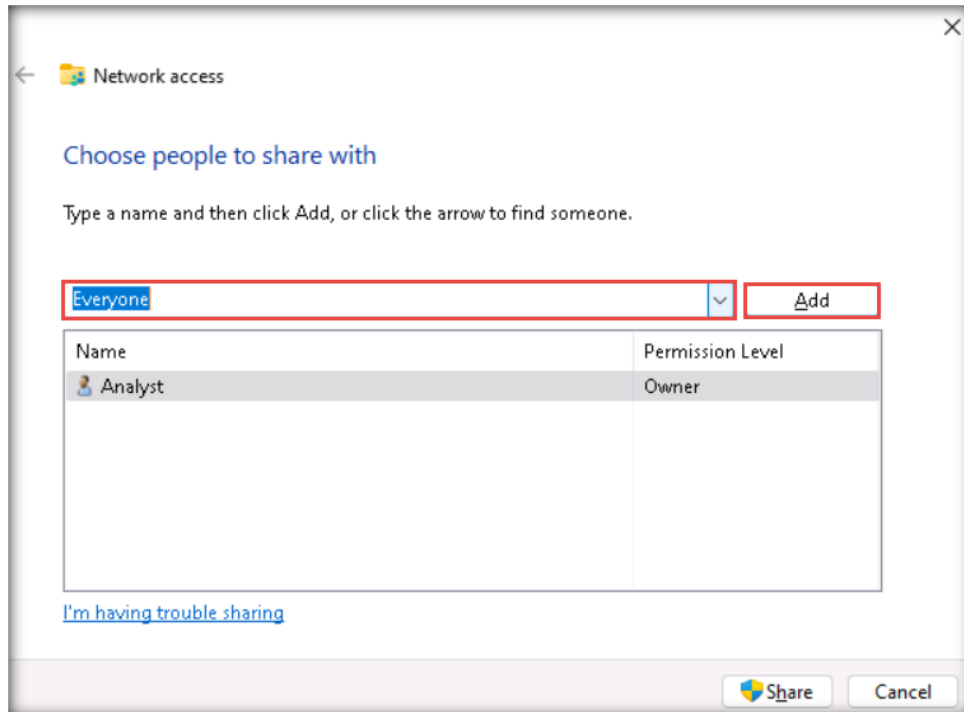


7. Select the **Sharing** tab from the **CTIA-Tools Properties** window to modify and display the current shared folder settings.

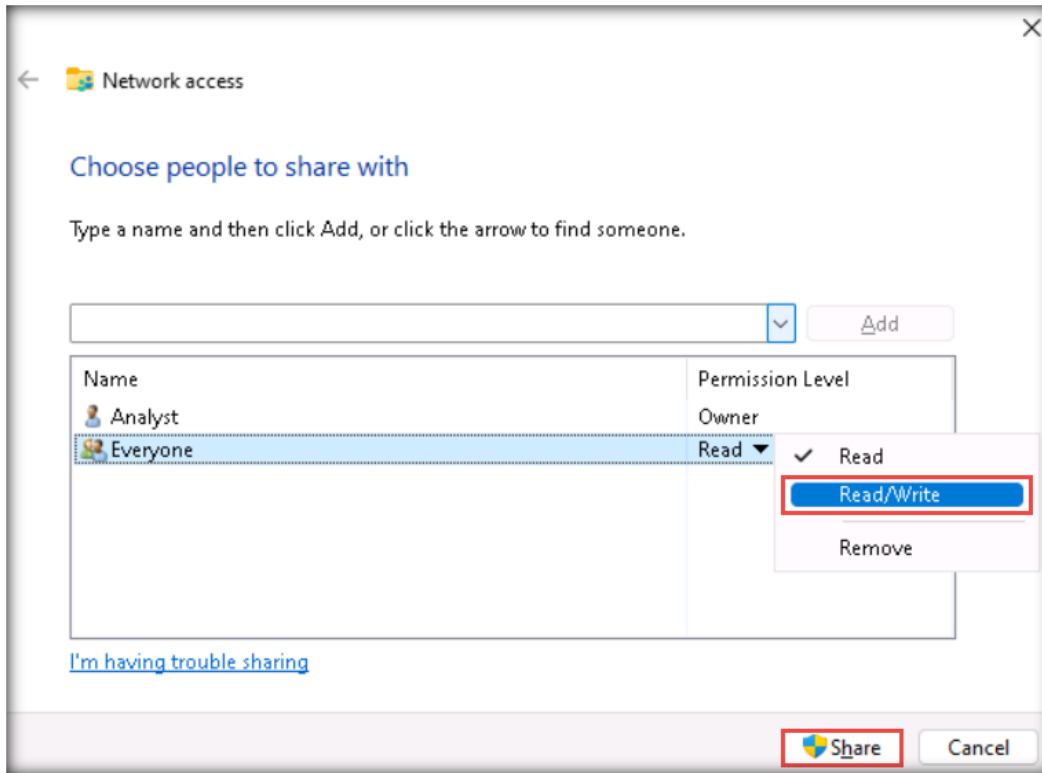
- 8. Click the **Share...** button to access the **File Sharing** options.



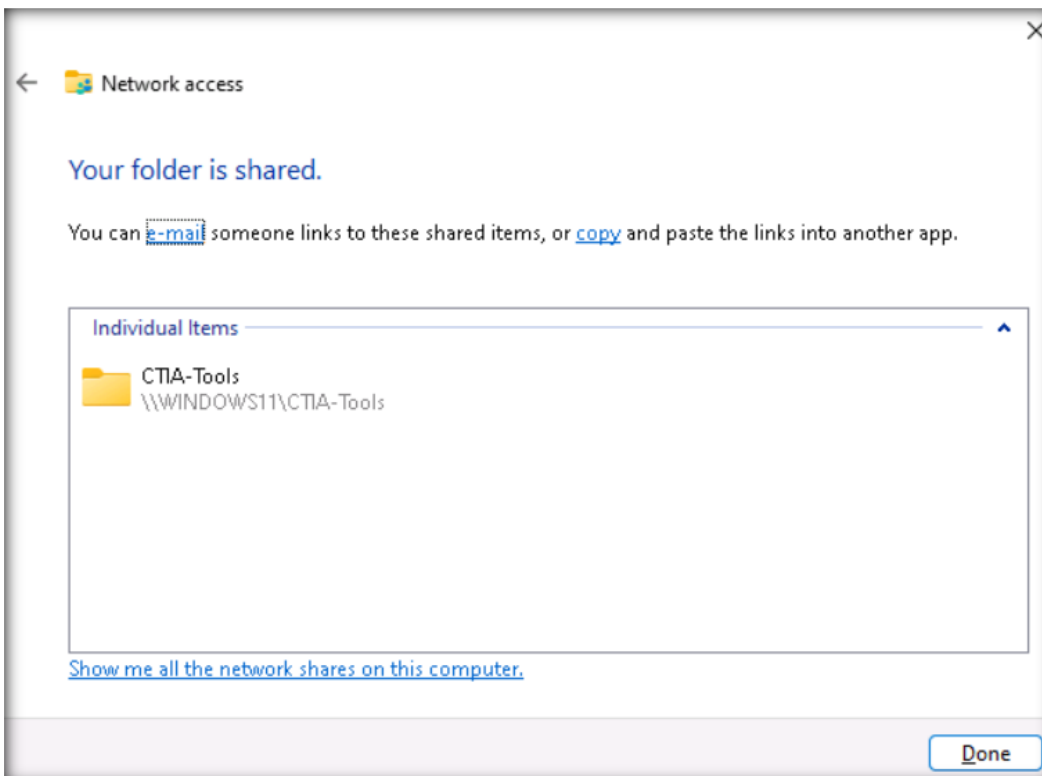
- 9. In the **File Sharing** wizard, select **Everyone** from the drop-down list and click **Add**.



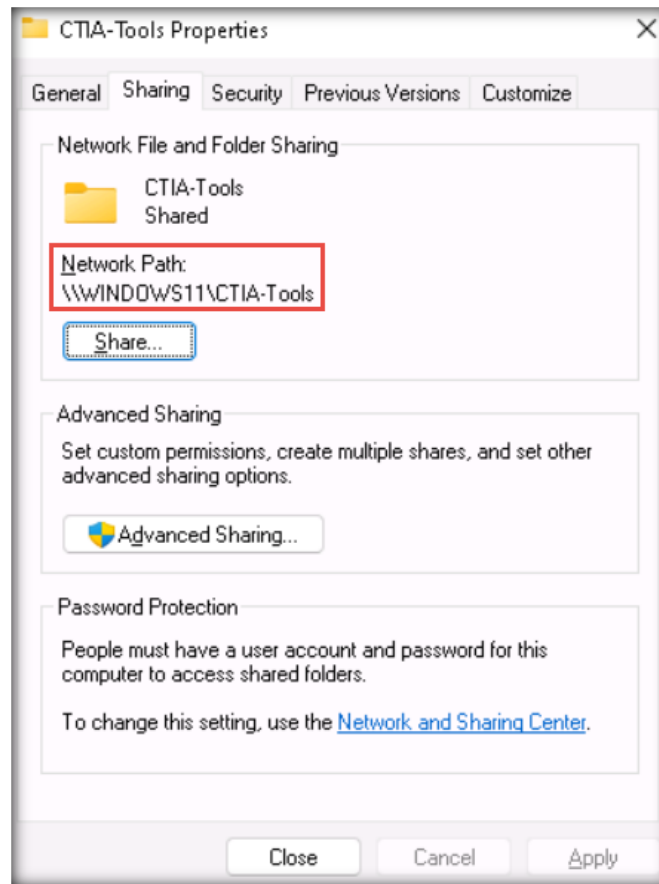
10. For the newly added users (**Everyone**), click the **Read** drop-down menu and click **Read/Write**.
11. Click **Share** to begin sharing with the added users.



12. Click **Done** on the confirmation page of the **File Sharing** wizard.



13. Close the **CTIA-Tools Properties** window.



14. Close all open windows.

[\[Back to Configuration Task Outline\]](#)

CT#18: Install Adobe Acrobat Reader DC on the Windows 11 Virtual Machine

1. Log in to the **Windows 11** virtual machine with the credentials **Analyst** and **Pa\$\$w0rd**.
2. Open a **File Explorer** window and navigate to the **E:\CTIA-Tools\CTIA Lab Prerequisites\Adobe Reader** folder.
3. Alternatively, you may download the latest version of **Adobe Acrobat Reader DC** from the official Adobe website.
4. Double-click the **Reader_Install_Setup.exe** file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
5. Follow the **wizard-driven** installation steps and complete the installation by choosing the default options throughout.
6. After the installation has completed, close all windows.

[\[Back to Configuration Task Outline\]](#)

CT#19: Install Web Browsers on the Windows 11 Virtual Machine

1. On the **Windows 11** virtual machine, navigate to the **E:\CTIA-Tools\CTIA Lab Prerequisites\Web Browsers** folder.
2. Follow the **wizard-driven** installation steps to install the **Google Chrome** and **Mozilla Firefox** web browsers.
3. You can also download the **latest** versions of these web browsers from their respective websites.

[\[Back to Configuration Task Outline\]](#)

CT#20: Install WinPcap on the Windows 11 Virtual Machine

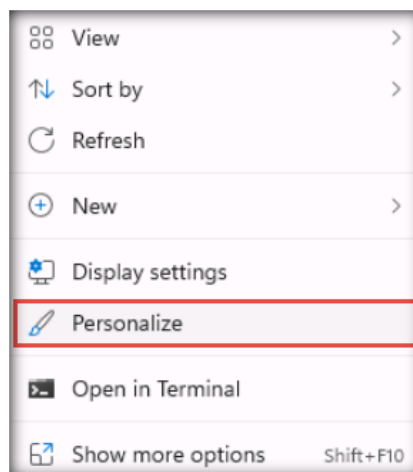
1. In the **Windows 11** virtual machine, navigate to **E:\CTIA-Tools\CTIA Lab Prerequisites**.
2. Open **WinPcap** folder.
3. Double-click the **WinPcap_4_1_3.exe** file and follow the **wizard-driven** installation steps to install WinPcap.
4. You can also download the **latest version** of WinPcap from the respective vendors.

[\[Back to Configuration Task Outline\]](#)

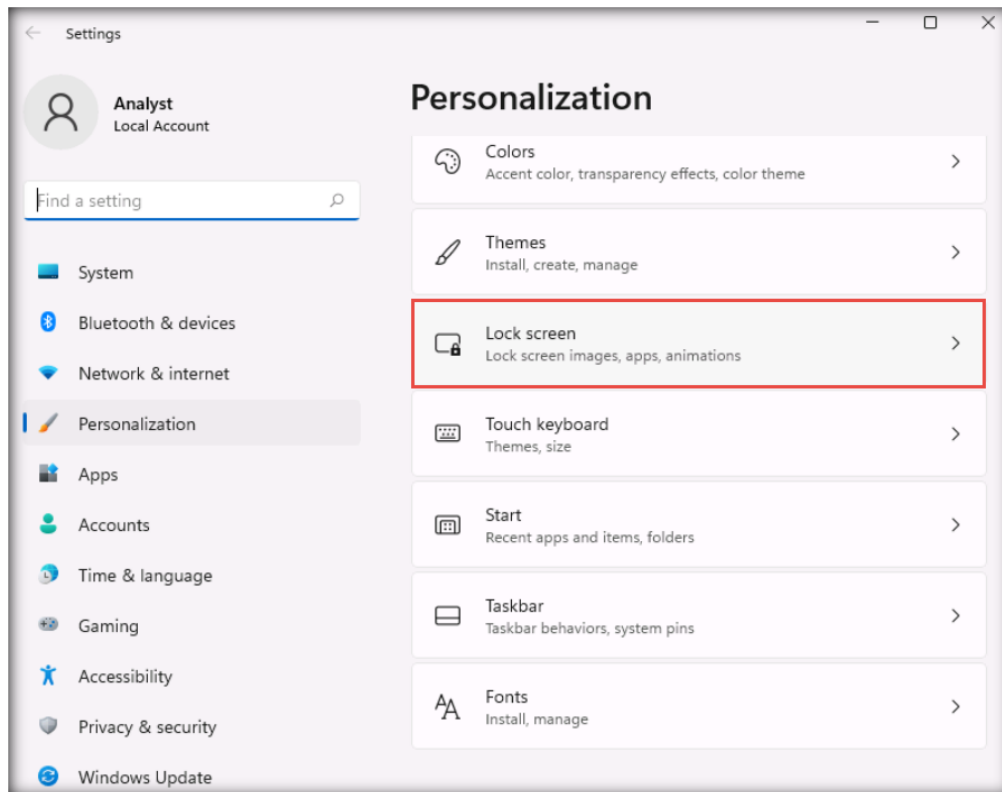
CT#21: Turn Off Screen Savers on the Windows 11 Virtual Machine

Note: Before performing this CT, you must activate the Windows 11 virtual machine.

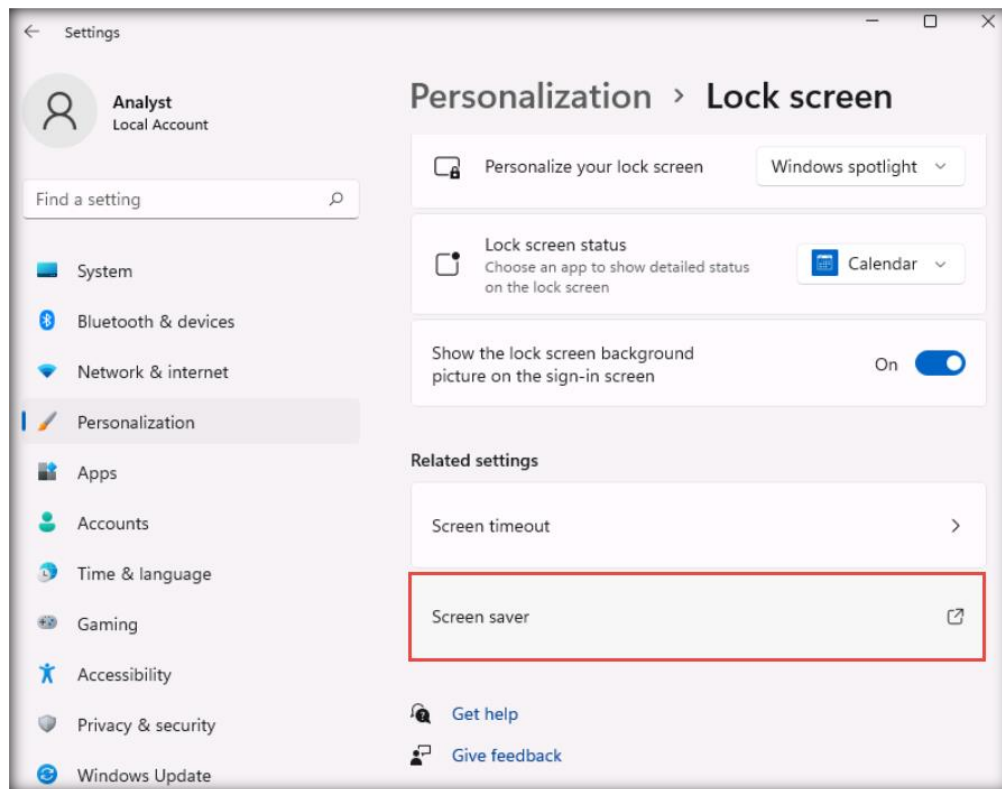
1. In the **Windows 11** virtual machine, right-click on the **Desktop** and select **Personalize** to open the personalization settings.



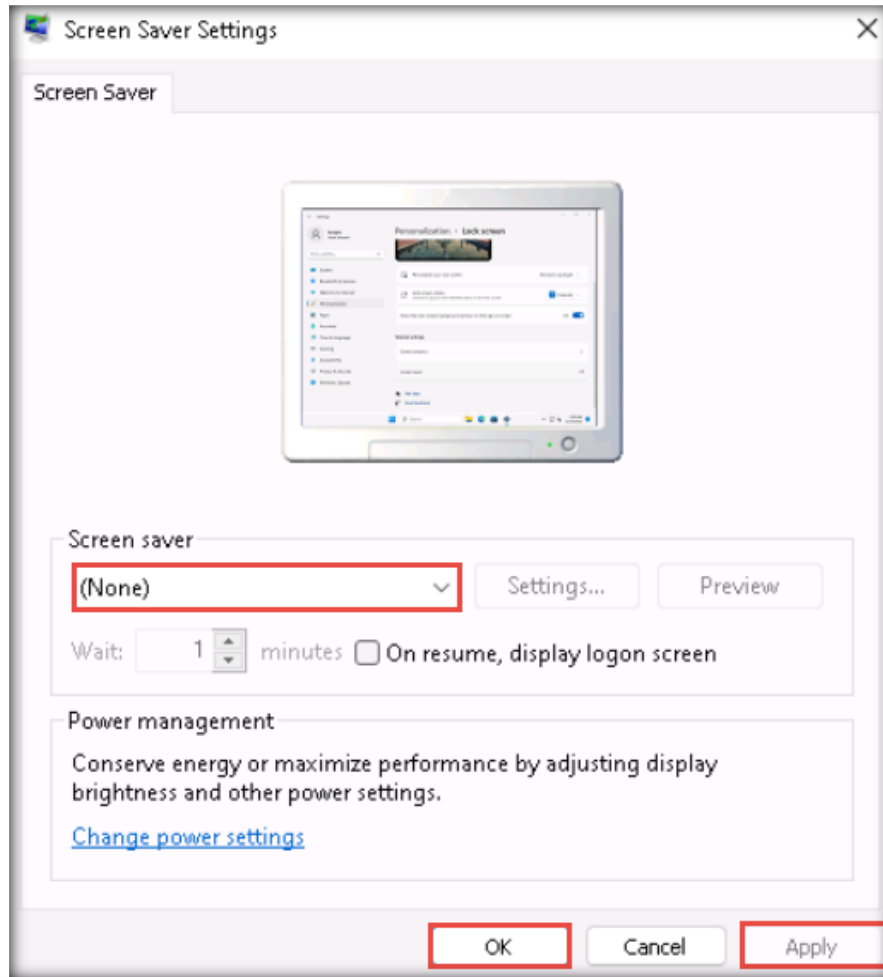
2. In the **Personalization** window scroll down and click **Lock screen** in the right pane.



3. The **Lock screen** settings page appears; scroll down and click **Screen saver**.



- The **Screen Saver Settings** window appears; ensure that the **(None)** option is selected from the drop-down list for **Screen saver**. Click **Apply** and then **OK**.

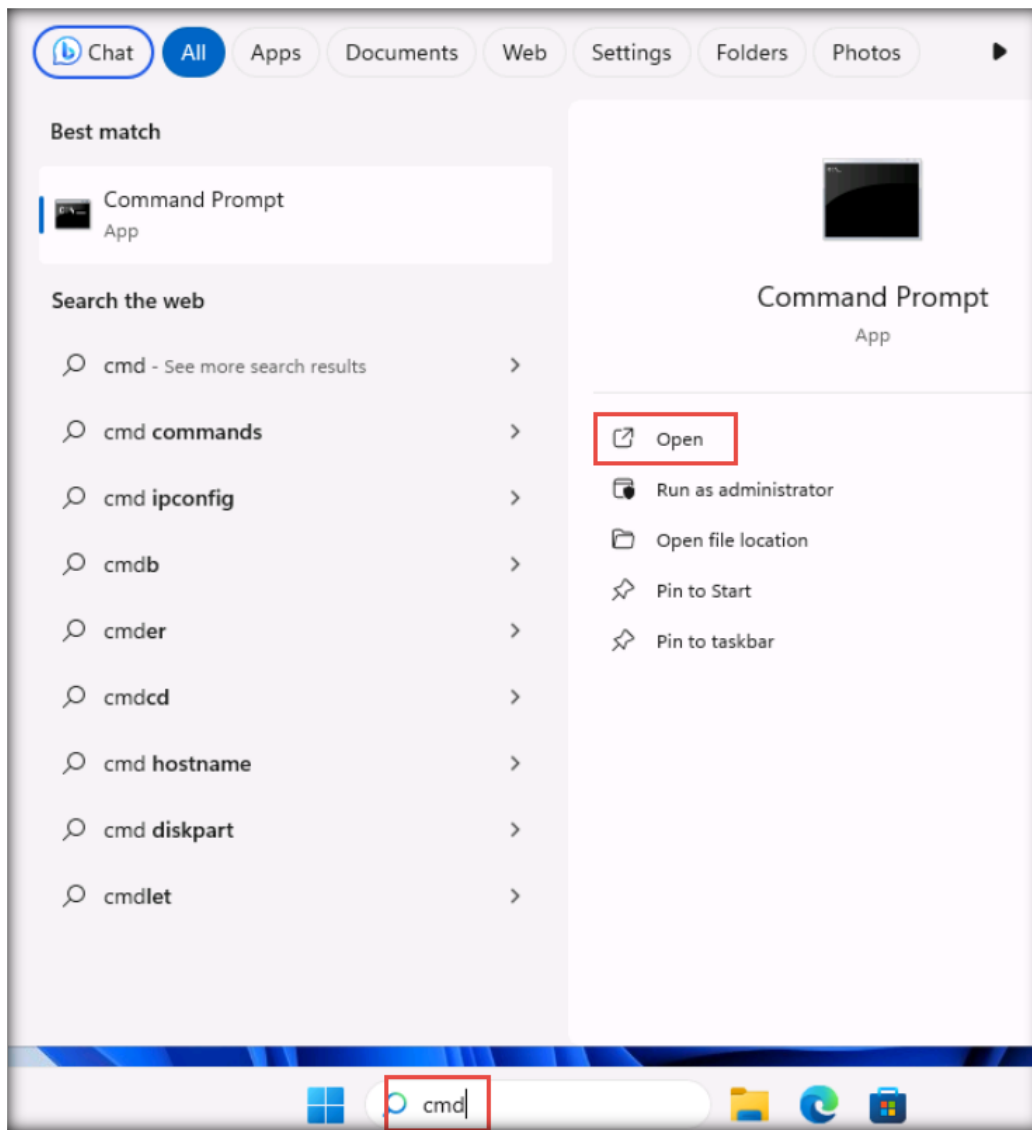


- Close all windows.

[\[Back to Configuration Task Outline\]](#)

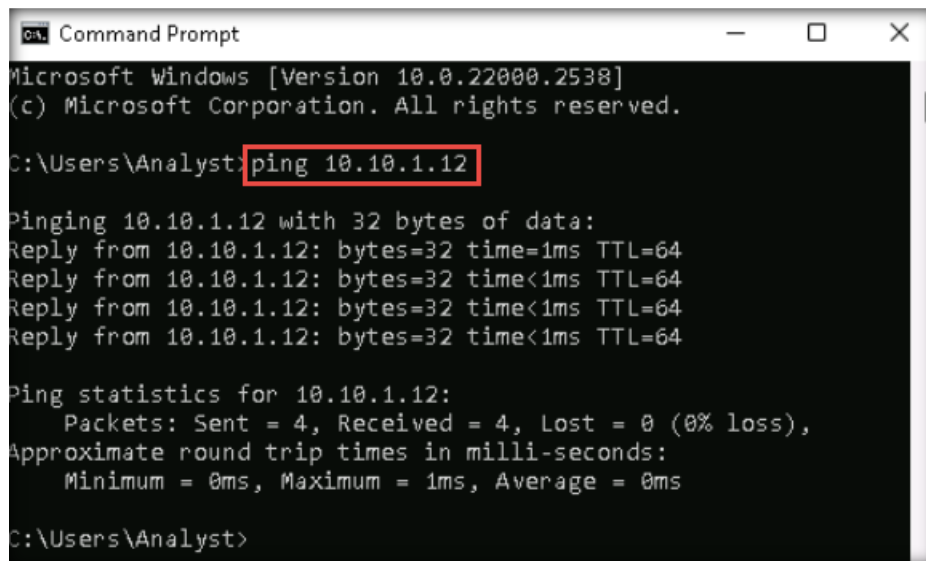
CT#22: Ping Test Among Both Virtual Machines

1. On the **Windows 11** virtual machine, open a **Command Prompt** window.



2. Before pinging the **Parrot Security** virtual machine, ensure that it is running.

3. Check for a reply from the virtual machine. Here, as an example, we are using the **Parrot Security** virtual machine with the IP address **10.10.1.12** (this IP address may be different in your lab network).



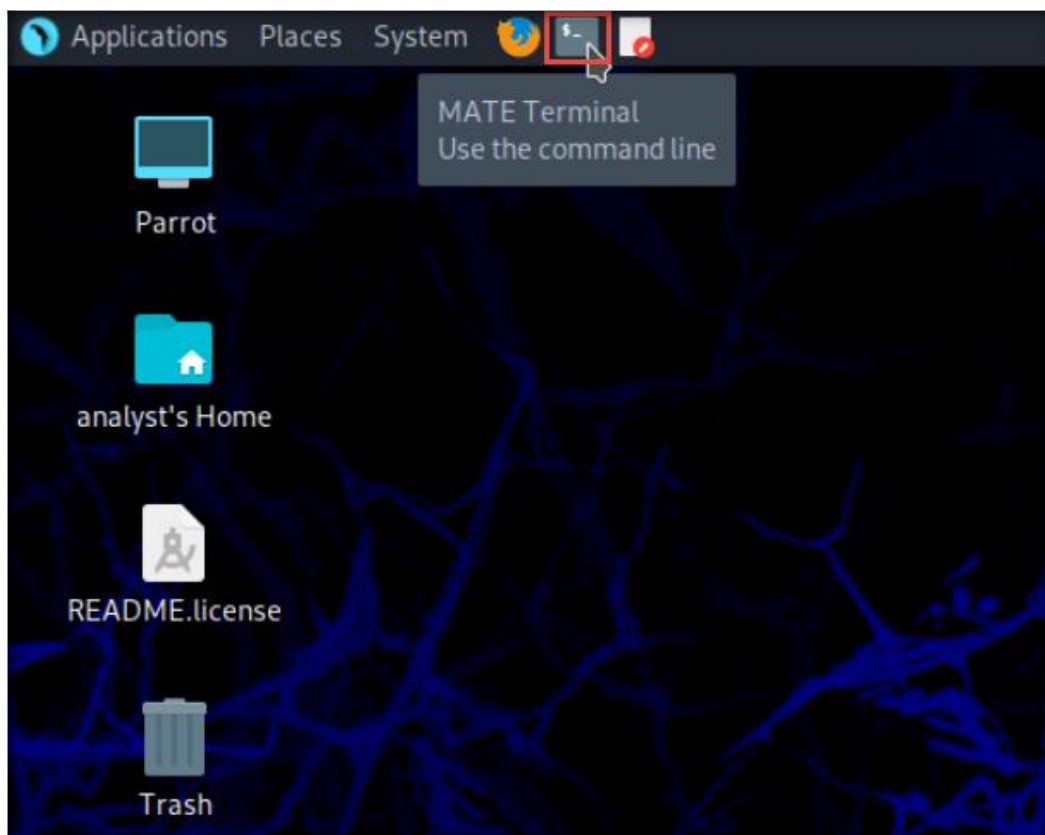
```
C:\Users\Analyst>ping 10.10.1.12

Pinging 10.10.1.12 with 32 bytes of data:
Reply from 10.10.1.12: bytes=32 time=1ms TTL=64
Reply from 10.10.1.12: bytes=32 time<1ms TTL=64
Reply from 10.10.1.12: bytes=32 time<1ms TTL=64
Reply from 10.10.1.12: bytes=32 time<1ms TTL=64

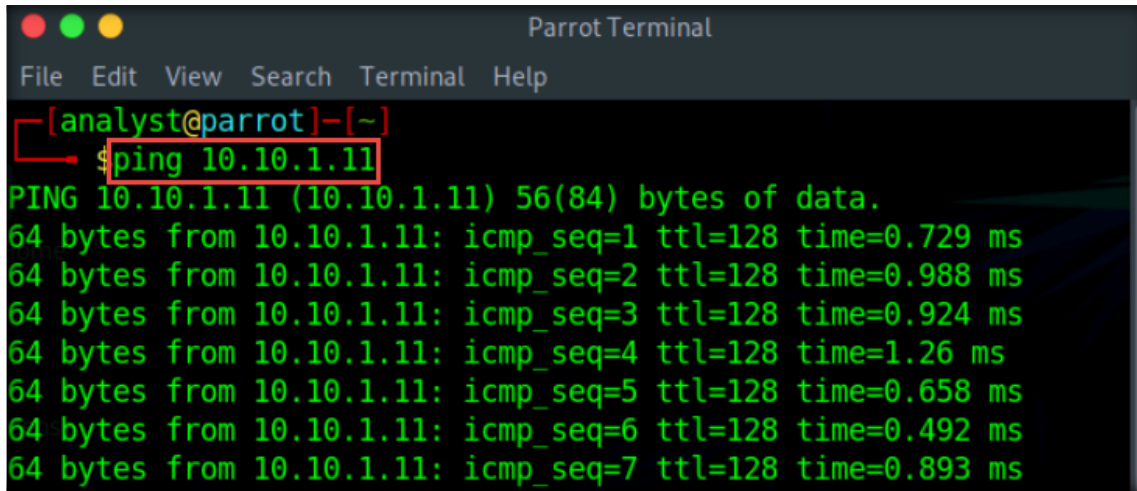
Ping statistics for 10.10.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Analyst>
```

4. Now, switch to the **Parrot Security** virtual machine and login using credentials **analyst/toor**.
5. Select the **MATE Terminal** icon available at the top section of the Desktop to launch Terminal window.



- In the **Terminal** window, type **ping 10.10.1.11** to ping the **Windows 11** virtual machine.

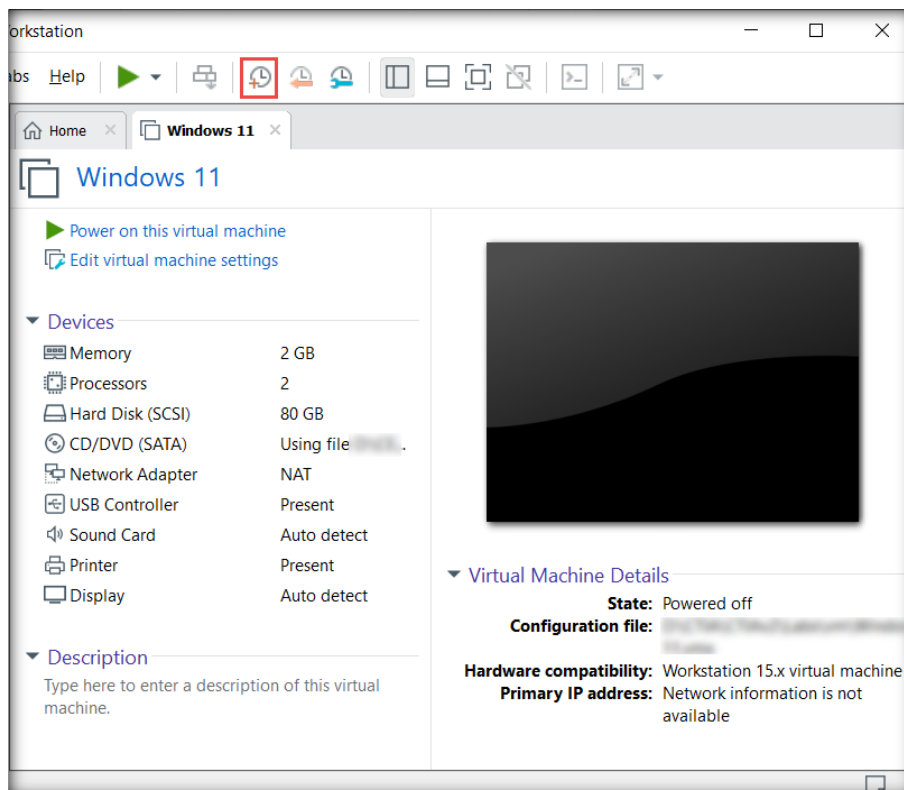


- This shows that both the virtual machines are interconnected.

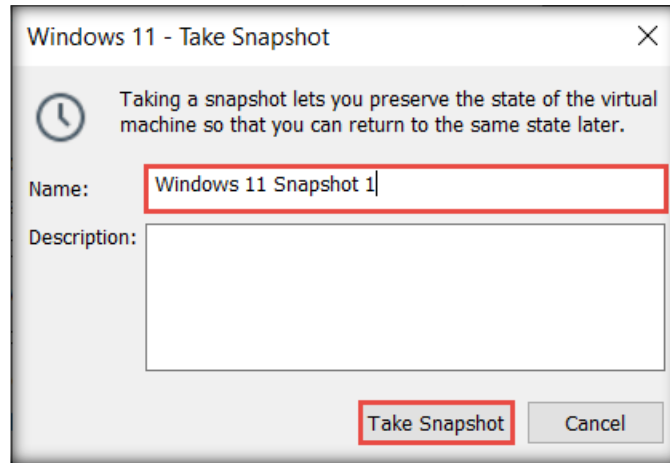
[\[Back to Configuration Task Outline\]](#)

CT#23: Take Snapshots of Virtual Machines

- Ensure that all the virtual machines are turned off.
- In the **VMware Workstation** window, click on **Windows 11** in the left pane and then the **Take a snapshot of this virtual machine** (🕒) icon, as shown in the screenshot.



3. The **Windows 11 – Take Snapshot** pop-up appears. Type a name for the snapshot in the **Name** field, retain the default description field, and click **Take Snapshot**.



4. Similarly, take a snapshot of the **Parrot Security** virtual machine once all the CTs have been completed.

[\[Back to Configuration Task Outline\]](#)

End of the Document

CITIA

Certified Threat Intelligence Analyst

EC-Council

Building A Culture Of Security

EC-Council Official Curricula