EC-Council

C|SA™

Certified SOC Analyst

Classroom Lab Setup Guide

www.eccouncil.org

Table of Contents

Classroom Setup Instructions: CSA

This document contains setup instructions for the Certified SOC Analyst (CSA) course. The course requires a standard modular classroom seating configuration, one computer for each student, one computer for the instructor, a dedicated switch, dedicated firewall, and Internet connection. This class teaches SOC processes.

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

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

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

Certified SOC Analyst and CSA are either registered trademarks or trademarks of the EC-Council in the USA and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

Classroom Requirements

This section describes classroom equipment required for the Certified SOC Analyst (CSA) 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 X 6 feet (1m X 2m) or larger
- Markers, whiteboard, assorted colors
- Eraser, whiteboard cleaner liquid
- Easel with flipchart or butcher paper pad, 24 inches X 36 inches
- Felt tip pens, blue and black required, other colors optional, chisel tip (not fine-point)
- Screen, projection, 6 feet diagonal measurement (non-reflective whiteboard surface may be substituted)
- Instructor station:

    - Desk, chair, and ergonomic keyboard
    - Power outlet
    - Network jack
    - Projector, LCD, capable of 740 X 1280 pixels minimum w/ all connecting cables
- Student station (per student):
    - Chair, ergonomic keyboard
    - Workstation, minimum horizontal workspace 9 square feet (3 feet X 3 feet)
    - Power outlet, one per student station
    - Network jack, one per student station

Hardware

Hardware requirements for instructor, student and victim computers are identical:

- Intel Core i5 or equivalent CPU with minimum CPU speed of 3.2 GHz
- Minimum 16 GB RAM (16 GB is recommended)
- Hard disk, 500 GB or larger, 7200 RPM or faster
- DVD drive (DVD R/W drive preferred)
- One Network adapters (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 17-inch LCD
- Mouse or compatible pointing device, and sound card with amplified speakers
- Internet access

The following additional hardware is also required:

- An unmanaged switch, with sufficient ports to allow connection of all instructor and student workstations plus at least 5 additional, unused ports for connection of additional equipment or for use as “spares.”

Software

All computers in the class require the following software:

- Microsoft Windows 10 Enterprise or Professional (64-bit) fully patched
- Adobe Acrobat Reader DC or later version
- WinRAR v5.60 or later version
- Web browsers: Internet Explorer, Firefox, and Chrome
- Word, Excel, and PowerPoint Viewers or Microsoft Office 2016/Open Office

- Hyper-V (built-in role in Windows 10 Enterprise or Professional (64 bit))
    - Microsoft Windows Server 2016 Standard (64-bit)
    - Microsoft Windows Server 2012 R2 Standard (64-bit)
    - Microsoft Windows 10 Enterprise (64-bit)
    - AlienVault_OSSIM_64bits_5.3.0.iso (downloadable at http://downloads.alienvault.com/c/download?version=current_ossim_iso)
    - Kali Linux (64 bit)
    - SOC-Tools downloadable from Aspen portal.

Setup Document Overview

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

Training Room Environment

The training room environment consists primarily of the following equipment:

- Instructor's Computer
- Student Workstation

Equipment	Number (Class of 12 Students)	Operating System	Minimum System Requirements
Instructor's Computer	1	Microsoft Windows 10 enterprise or Professional (64-bit) fully patched	Intel Core i5 or equivalent PC with 200 GB free disk space (with two logical partitions C: and D:), minimum of 16 GB RAM, 1 NIC (disable or unplug extras), 17-inch monitor, and compatible mouse
Student Workstations	12	Microsoft Windows 10 Enterprise or Professional (64-bit) fully patched	Intel Core i5 or equivalent PC with 200 GB free disk space (with two logical partitions C: and D:), minimum of 16 GB RAM, 1 NIC (disable or unplug extras), 17-inch monitor, and compatible mouse

Instructor's Computer

The instructor's computer must:

- Be installed with **Windows 10 Enterprise or Professional (64 bit),** later service packs and full patches applied
- Have Microsoft Office/Open Office or PowerPoint, Word, and Excel Viewers installed
- Be running IP protocol
- Have all SOC Essential Tools downloaded from Aspen to the hard drive in D:\SOC-Tools folder for easy access (See CT#3 in Configuration Task section)
- Be installed with **Hyper-V** in Windows 10 host machine (see CT#4 in Configuration Task section)
- Configuring Internal Network for Hyper-V (See Configuration Task CT#5)
- Be configured with Hyper-V VMs and guest operating systems
  - Create and Configure Windows Server 2016 Standard Virtual Machine (See Configuration Task CT#6)
    - Create a Virtual Machine and Install Windows Server 2016 Standard (See Configuration Task CT#6.1)
    - Change the Computer Name of Windows Server 2016 Virtual Machine (See Configuration Task CT#6.2)
    - Configure Static IP address for Windows Server 2016 Virtual Machine (See Configuration Task CT#6.3)
    - Share SOC-Tools Folder from Host Machine and Map to Windows Server 2016 Virtual Machine (See Configuration Task CT#6.4)
    - Install WinRAR in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.5)
    - Install Web Browsers in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.6)
    - Install Notepad++ in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.7)
    - Install Java Development Kit 8u (JDK 8u) in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.8)
    - Install Splunk Enterprise in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.9)
    - Install .Net Framework 3.5 (Includes .Net 2.0 and 3.0) in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.10)
  - Create and Configure Windows Server 2012 Virtual Machine (See Configuration Task CT#7)

    - Create a Virtual Machine and Install Windows Server 2012 R2 Standard OS (See Configuration Task CT#7.1)
    - Change the Computer Name of Windows Server 2012 Virtual Machine (See Configuration Task CT#7.2)
    - Configure Static IP address for Windows Server 2012 Virtual Machine (See Configuration Task CT#7.3)
    - Add IIS roles in Server Manager of Windows Server 2012 Virtual Machine (See Configuration Task CT#7.4)
    - Share SOC-Tools Folder from Host Machine and Map to Windows Server 2012 Virtual Machine (See Configuration Task CT#7.5)
    - Install MS SQL Server 2016 Express Edition on Windows Server 2012 Virtual Machine (See Configuration Task CT#7.6)
    - Install Microsoft SQL Server Management Studio on Windows Server 2012 Virtual Machine (See Configuration Task CT#7.7)
    - Install Notepad++ in Windows Server 2012 Virtual Machine (See Configuration Task CT#7.8)
    - Install Web Browser in Windows Server 2012 Virtual Machine (See Configuration Task CT#7.9)
    - Configure the LuxuryTreats Website in Windows Server 2012 Virtual Machine (See Configuration Task CT#7.10)
    - Configure Host File in Windows Server 2012 Virtual Machine (See Configuration Task CT#7.11)
    - Setup FTP Site on Windows Server 2012 Virtual Machine (See Configuration Task CT#7.12)
    - Install WinPcap on Windows Server 2012 Virtual Machine (See Configuration Task CT#7.13)
  - Create and Configure Windows 10 Virtual Machine (See Configuration Task CT#8)
    - Create a Virtual Machine and Install Windows 10 Guest OS (See Configuration Task CT#8.1)
    - Create New User Account in Windows 10 Virtual Machine (See Configuration Task CT#8.2)
    - Change the Computer Name in Windows 10 Virtual Machine (See Configuration Task CT#8.3)
    - Configure Static IP Address for Windows 10 Virtual Machine (See Configuration Task CT#8.4)
    - Share SOC-Tools Folder from Host Machine and Map to Windows 10 Virtual Machine (See Configuration Task CT#8.5)

        - Install Web Browsers in Windows 10 Virtual Machine (See Configuration Task CT#8.6)
        - Install FTP Client in Windows 10 Virtual Machine (See Configuration Task CT#8.7)
        - Turn off the Windows Defender Firewall in Windows 10 Virtual Machine (See Configuration Task CT#8.8)
    - Create and Configure kali Linux Virtual Machine (See Configuration Task CT#9)
        - Create a Virtual Machine and Install Kali Linux OS (See Configuration Task CT#9.1)
        - Configure Host File in Kali Linux (See Configuration Task CT#9.2)
        - Updating Kali Linux (See Configuration Task CT#9.3)
    - Install and Configure AlienVault OSSIM (See Configuration Task CT#10)
    - Create and Configure Windows 10 Virtual Machine (SIEM2) (See Configuration Task CT#11)
    - Setting Checkpoints of Virtual Machines (See Configuration Task CT#12)
    - Setting Time Zone of Virtual Machines (See Configuration Task CT#13)
    - Has an LCD projector connected to an instructor's machine?
    - Use ghost images (recommended) to reduce the setup time in case of computer failure

Student Workstations

Student workstations must:

- Be installed with **Windows 10 Enterprise or Professional (64 bit),** later service packs and full patches applied
- Have Microsoft Office/Open Office or PowerPoint, Word, and Excel Viewers installed
- Be running IP protocol
- Have all SOC Essential Tools downloaded from Aspen to the hard drive in D:\SOC-Tools folder for easy access (See CT#3 in Configuration Task section)
- Be installed with **Hyper-V** in Windows 10 host machine (see CT#4 in Configuration Task section)
- Configuring Internal Network for Hyper-V (See Configuration Task CT#5)
- Be configured with Hyper-V VMs and guest operating systems
    - Create and Configure Windows Server 2016 Standard Virtual Machine (See Configuration Task CT#6)
        - Create a Virtual Machine and Install Windows Server 2016 Standard (See Configuration Task CT#6.1)
        - Change the Computer Name of Windows Server 2016 Virtual Machine (See

    Configuration Task CT#6.2)
    - Configure Static IP address for Windows Server 2016 Virtual Machine (See Configuration Task CT#6.3)
    - Share SOC-Tools Folder from Host Machine and Map to Windows Server 2016 Virtual Machine (See Configuration Task CT#6.4)
    - Install WinRAR in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.5)
    - Install Web Browsers in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.6)
    - Install Notepad++ in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.7)
    - Install Java Development Kit 8u (JDK 8u) in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.8)
    - Install Splunk Enterprise in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.9)
    - Install .Net Framework 3.5 (Includes .Net 2.0 and 3.0) in Windows Server 2016 Virtual Machine (See Configuration Task CT#6.10)
  - Create and Configure Windows Server 2012 Virtual Machine (See Configuration Task CT#7)
    - Create a Virtual Machine and Install Windows Server 2012 R2 Standard OS (See Configuration Task CT#7.1)
    - Change the Computer Name of Windows Server 2012 Virtual Machine (See Configuration Task CT#7.2)
    - Configure Static IP address for Windows Server 2012 Virtual Machine (See Configuration Task CT#7.3)
    - Add IIS roles in Server Manager of Windows Server 2012 Virtual Machine (See Configuration Task CT#7.4)
    - Share SOC-Tools Folder from Host Machine and Map to Windows Server 2012 Virtual Machine (See Configuration Task CT#7.5)
    - Install MS SQL Server 2016 Express Edition on Windows Server 2012 Virtual Machine (See Configuration Task CT#7.6)
    - Install Microsoft SQL Server Management Studio on Windows Server 2012 Virtual Machine (See Configuration Task CT#7.7)
    - Install Notepad++ in Windows Server 2012 Virtual Machine (See Configuration Task CT#7.8)
    - Install Web Browser in Windows Server 2012 Virtual Machine (See Configuration Task CT#7.9)

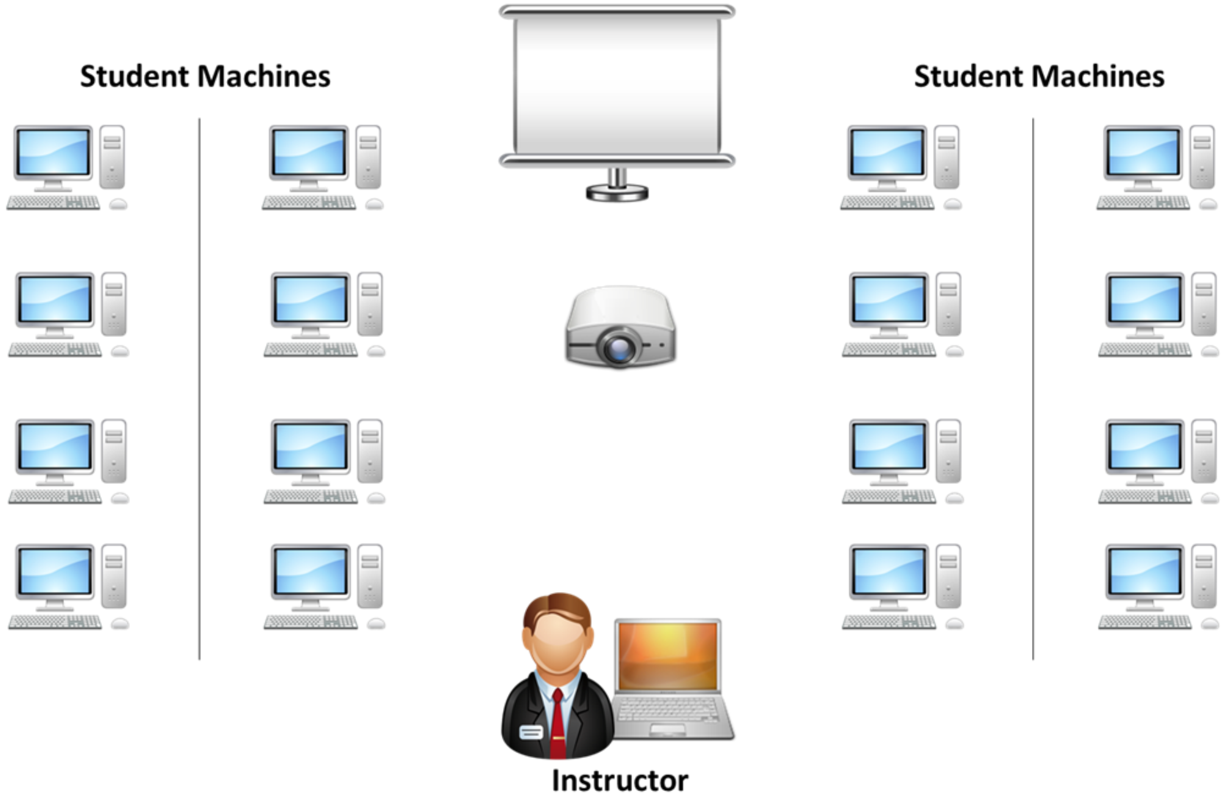
    - Configure the LuxuryTreats Website in Windows Server 2012 Virtual Machine (See Configuration Task CT#7.10)
    - Configure Host File in Windows Server 2012 Virtual Machine (See Configuration Task CT#7.11)
    - Setup FTP Site on Windows Server 2012 Virtual Machine (See Configuration Task CT#7.12)
    - Install WinPcap on Windows Server 2012 Virtual Machine (See Configuration Task CT#7.13)
- Create and Configure Windows 10 Virtual Machine (See Configuration Task CT#8)
    - Create a Virtual Machine and Install Windows 10 Guest OS (See Configuration Task CT#8.1)
    - Create New User Account in Windows 10 Virtual Machine (See Configuration Task CT#8.2)
    - Change the Computer Name in Windows 10 Virtual Machine (See Configuration Task CT#8.3)
    - Configure Static IP Address for Windows 10 Virtual Machine (See Configuration Task CT#8.4)
    - Share SOC-Tools Folder from Host Machine and Map to Windows 10 Virtual Machine (See Configuration Task CT#8.5)
    - Install Web Browsers in Windows 10 Virtual Machine (See Configuration Task CT#8.6)
    - Install FTP Client in Windows 10 Virtual Machine (See Configuration Task CT#8.7)
    - Turn off the Windows Defender Firewall in Windows 10 Virtual Machine (See Configuration Task CT#8.8)
- Create and Configure kali Linux Virtual Machine (See Configuration Task CT#9)
    - Create a Virtual Machine and Install Kali Linux OS (See Configuration Task CT#9.1)
    - Configure Host File in Kali Linux (See Configuration Task CT#9.2)
    - Updating Kali Linux (See Configuration Task CT#9.3)
- Install and Configure AlienVault OSSIM (See Configuration Task CT#10)
- Create and Configure Windows 10 Virtual Machine (SIEM2) (See Configuration Task CT#11)
- Setting Checkpoints of Virtual Machines (See Configuration Task CT#12)

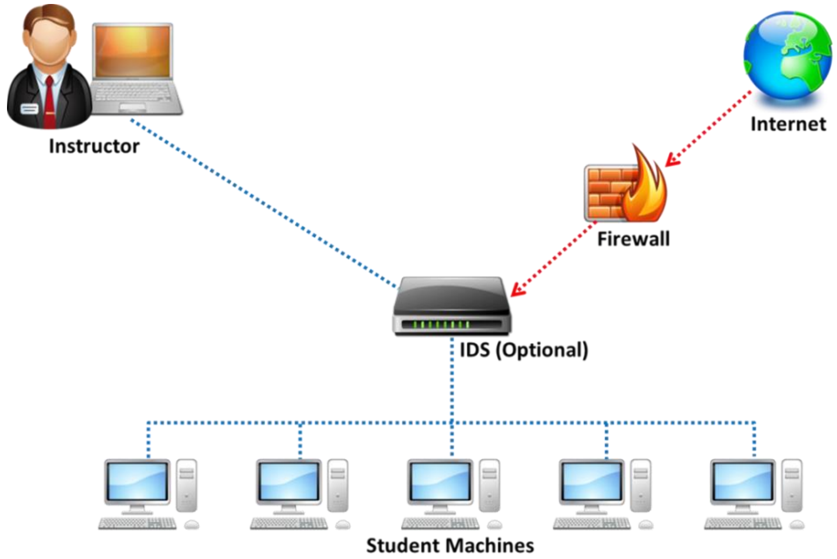
Room Environment

- The room must contain a whiteboard measuring a minimum of 1 yard by 2-3 yards in length (1 meter by 2-3 meters)
- The room should contain an easel and large tablet (optional)
- The room must be equipped with legible black and blue felt tip pens

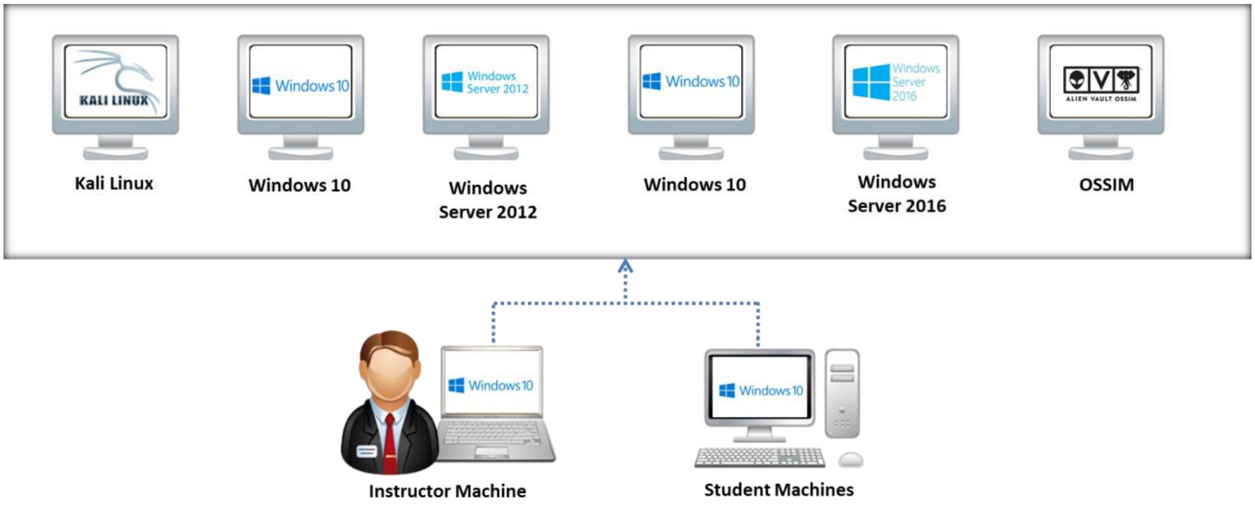
Classroom Configuration

The configuration of this classroom is modular. Computers can be added or removed by either row or column, depending on the needs of the particular 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 small and larger teams.





Set up the machines based on the classroom setup diagram. The lab exercises for the students are instructor led and they are based on the network security tools in the trainer slides.



Instructor and Student Machine Operating System: Windows 10 (Fully Patched)

Computer Names

Assign computer names to student machines like CSASTUDENT1, CSASTUDENT2, CSASTUDENT3, and so on. Instructor machine should be named as INSTRUCTOR.

Instructor Acceptance

Before the training class is scheduled to begin, the instructor will visit the training facility to inspect and accept 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 the facility technical contact will ensure completion of the following checklists before the training setup is deemed acceptable.

Firewall Settings

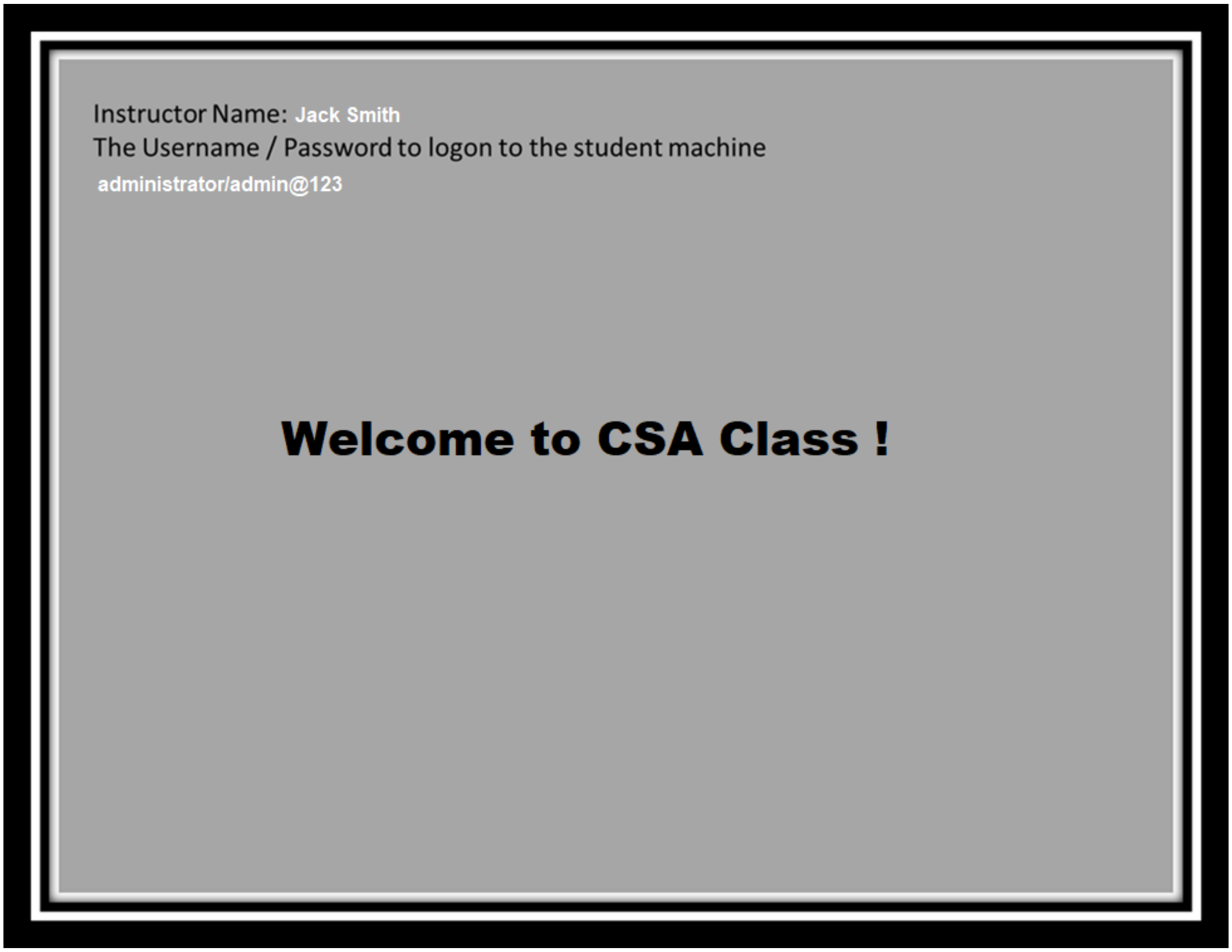
Do not block any ports while accessing the Internet through the firewall. You should be able to ping servers on the Internet.

Block the firewall in all the configured machines.

Blackboard

- Write the following on the blackboard top left corner
  - Instructor name: <Name of the instructor>
  - The username/password to logon to the student machine
- At the center of the board write the following letters in bold

Welcome to CSA Class!



Instructor Name: Jack Smith
The Username / Password to logon to the student machine
administrator/admin@123

Welcome to CSA Class !

Setup Checklist

The arrangement of items in the setup checklists is designed to allow the process to be completed in the most efficient manner possible and validate that the setup has been done correctly. Before beginning the setup checklist, log off any connected users.

Tick Here	List
□	Open Network. Verify that all classroom computers are visible in Network
□	Verify that the SOC tools are on the computer in SOC-Tools folder in the D:\ drive
□	Verify that Internet access is available
□	Visit https://www.eccouncil.org to check the Internet access
□	Verify each computer has 200 GB or more free disk space
□	Verify Microsoft PowerPoint, Word, and Excel viewer are installed (or Microsoft office/Open Office is installed)
□	Verify if you can successfully boot Windows Server 2012, Windows 10, Windows Server 2016, OSSIM, virtual machines
□	Verify that all the VMs are configured as per the configuration tasks
□	Verify that the Instructor computer can image through the overhead projector
□	Placement of LCD (overhead) projector is appropriate
□	Cable wiring organized and labeled
□	Student workstations and chair placement is satisfactory
□	Whiteboard and dry erase markers and erasers are available
□	Instructor station is properly organized and oriented
□	Computers are labeled with client number
□	EC-Council courseware (Official EC-Council CSA Box) is available for students
□	Write down the facility's technical contact person's mobile phone number. Contact him in case of network problem

Instructor Acceptance

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

The Instructor will 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 for the class.

Assistance

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

Detailed Configuration Tasks (CT)

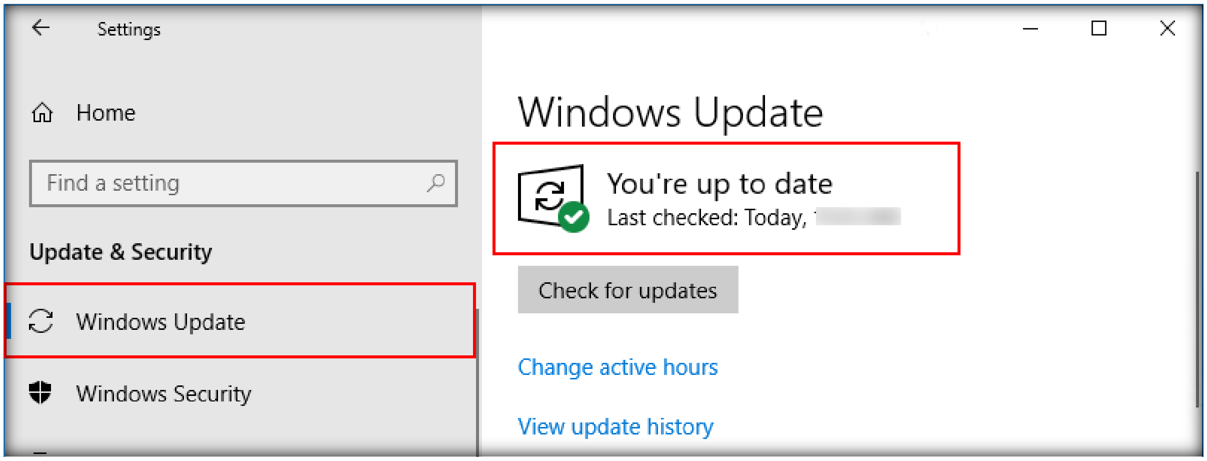
CT#1: Set Up Hardware

1. Set the computer's BIOS to start first from the **DVD-ROM** drive and then from the hard drive (Drive C:\).
2. Now keep **Windows 10 DVD** in the **DVD-ROM.**
3. Configure the hard disk to have one **active primary partition** (C:\ of 300 GB) and one **extended logical partition** (D:\ of 200 GB).
4. Follow the steps to install **Windows 10.**
5. Once installed, check for updates and, if found any, update the **Windows 10** host machine.
6. Install the **wireless network adapters** according to the manufacturer's instructions.

CT#2: Turn Off the Windows Defender Firewall in Host Machine

1. Now, check for the system updates and if found any, update the **Windows 10** virtual machine to the latest.

   Note: Installing the updates might take some time.



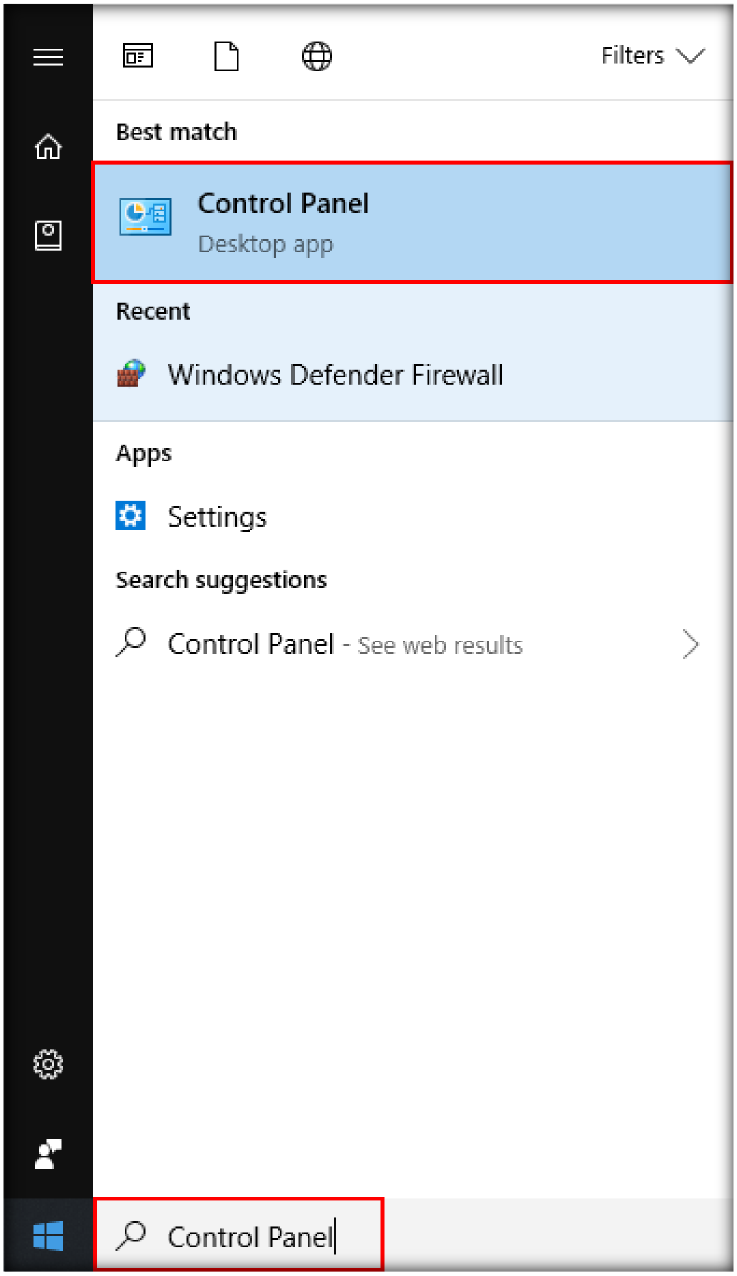
Windows Update

You're up to date

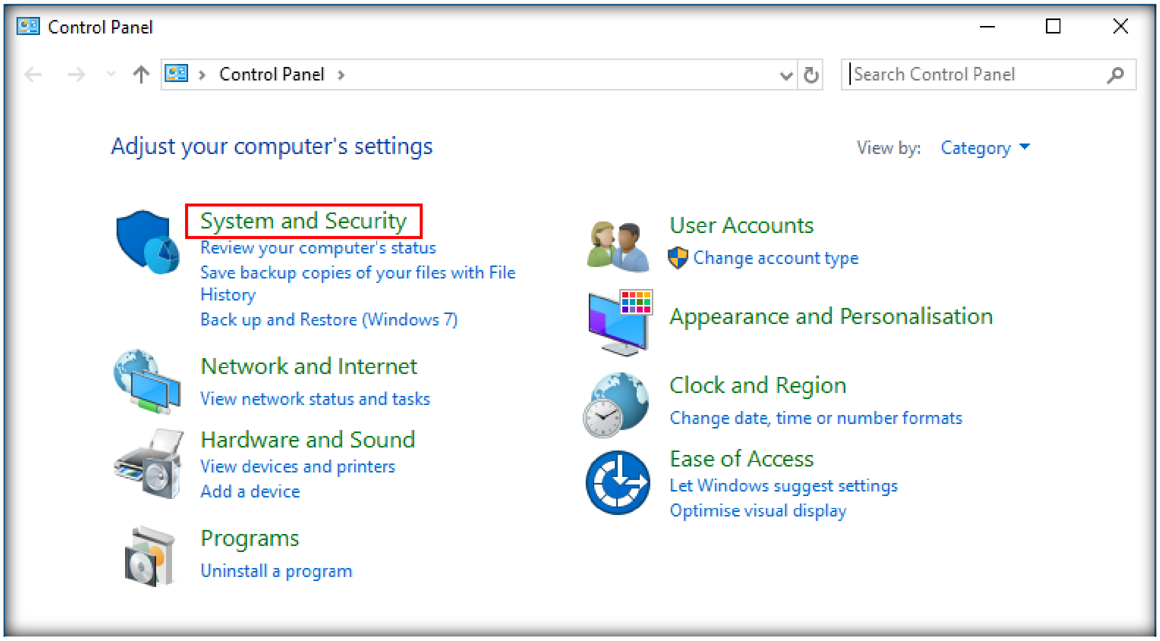
Last checked: Today, [redacted]

2. Turn on the machine and log in with credentials.

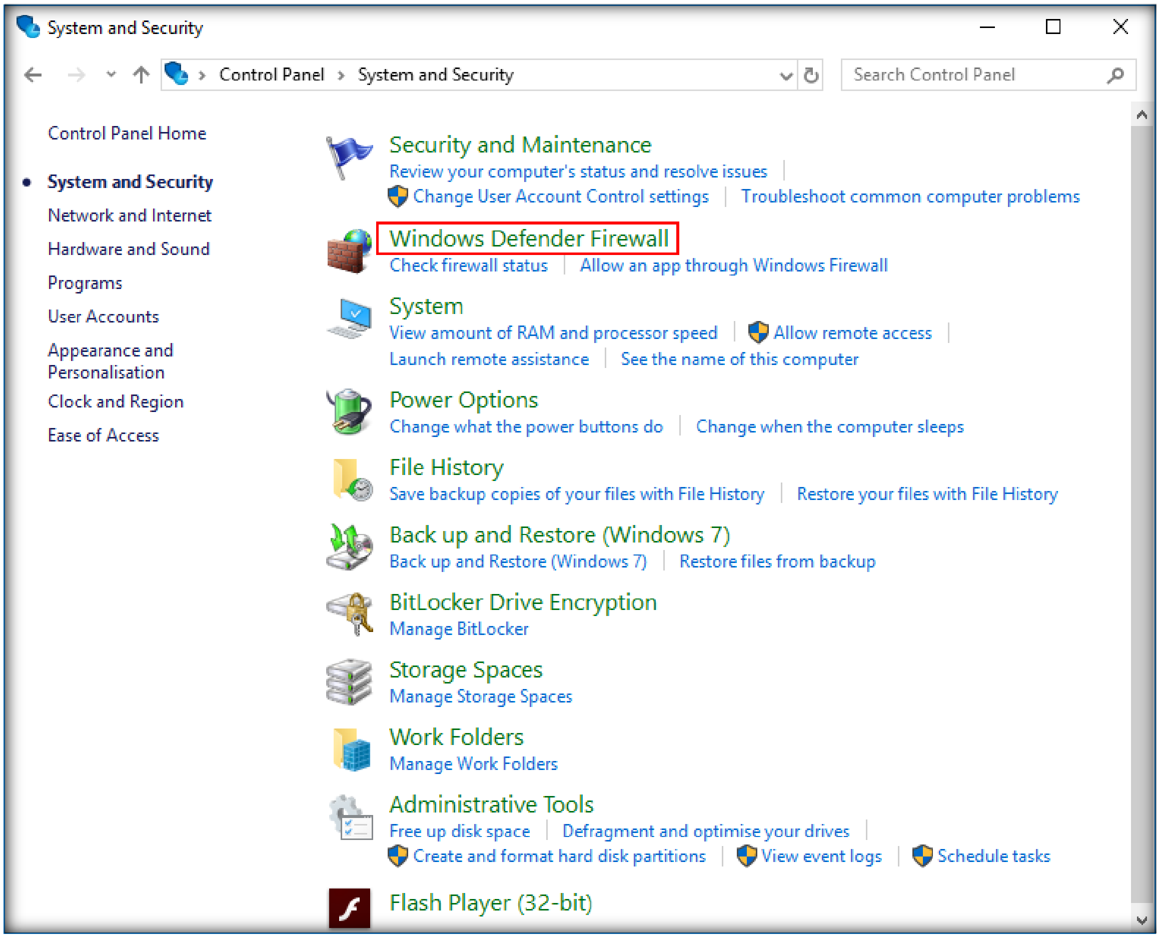
3. In the **Type here to search** field present at the lower left corner of the screen, type **Control Panel**. A search result containing **Control Panel** desktop app appears. Click **Control Panel**.



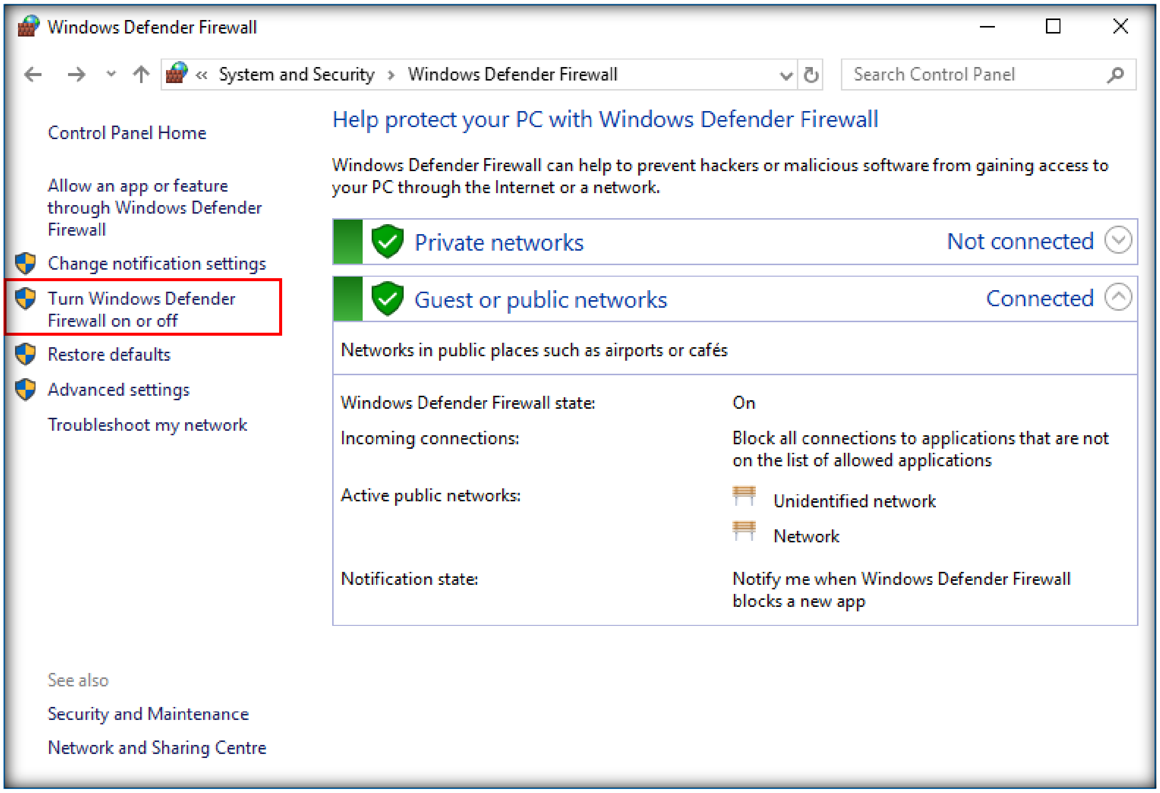
4. In the **Control Panel** window, click **System and Security**.


Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Back up and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalisation
Clock and Region
Change date, time or number formats
Ease of Access
Let Windows suggest settings
Optimise visual display

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


System and Security
Control Panel › System and Security
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalisation
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Power Options
Change what the power buttons do
Change when the computer sleeps
File History
Save backup copies of your files with File History
Restore your files with File History
Back up and Restore (Windows 7)
Back up and Restore (Windows 7)
Restore files from backup
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Free up disk space
Defragment and optimise your drives
Create and format hard disk partitions
View event logs
Schedule tasks
Flash Player (32-bit)

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



Windows Defender Firewall

« System and Security › Windows Defender Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Security and Maintenance

Network and Sharing Centre

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help to prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

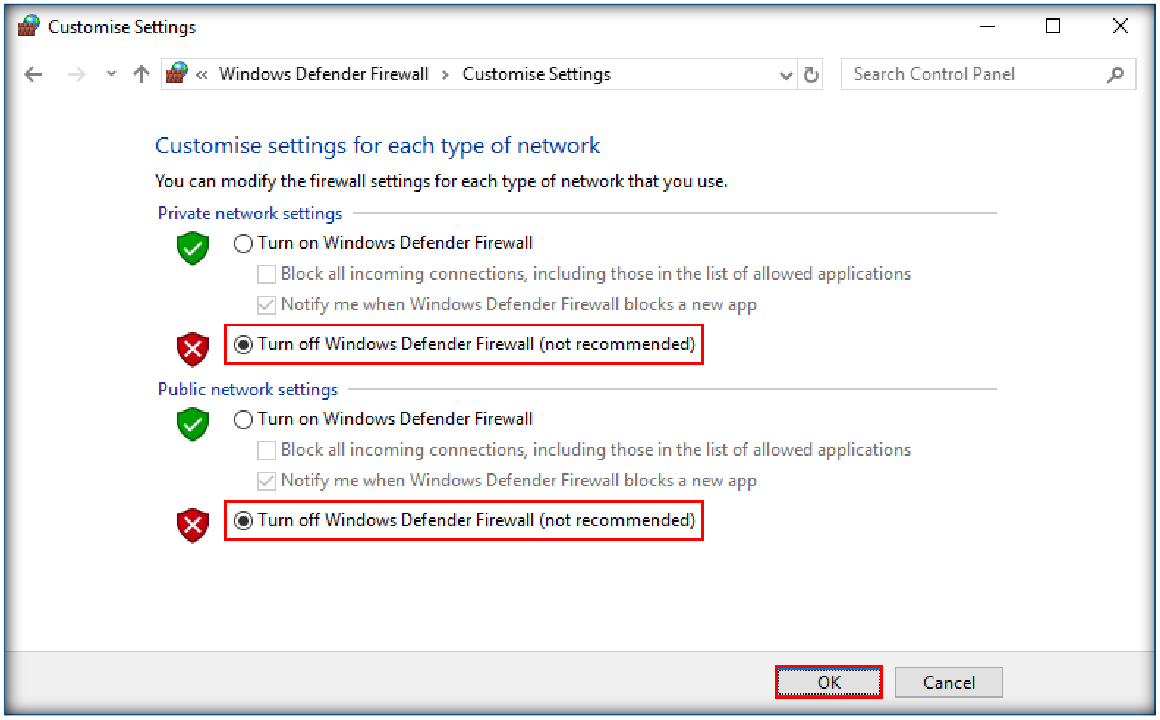
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or cafés

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to applications that are not on the list of allowed applications
Active public networks:	Unidentified network Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

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



Customise Settings

« Windows Defender Firewall › Customise Settings

Search Control Panel

Customise settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed applications

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

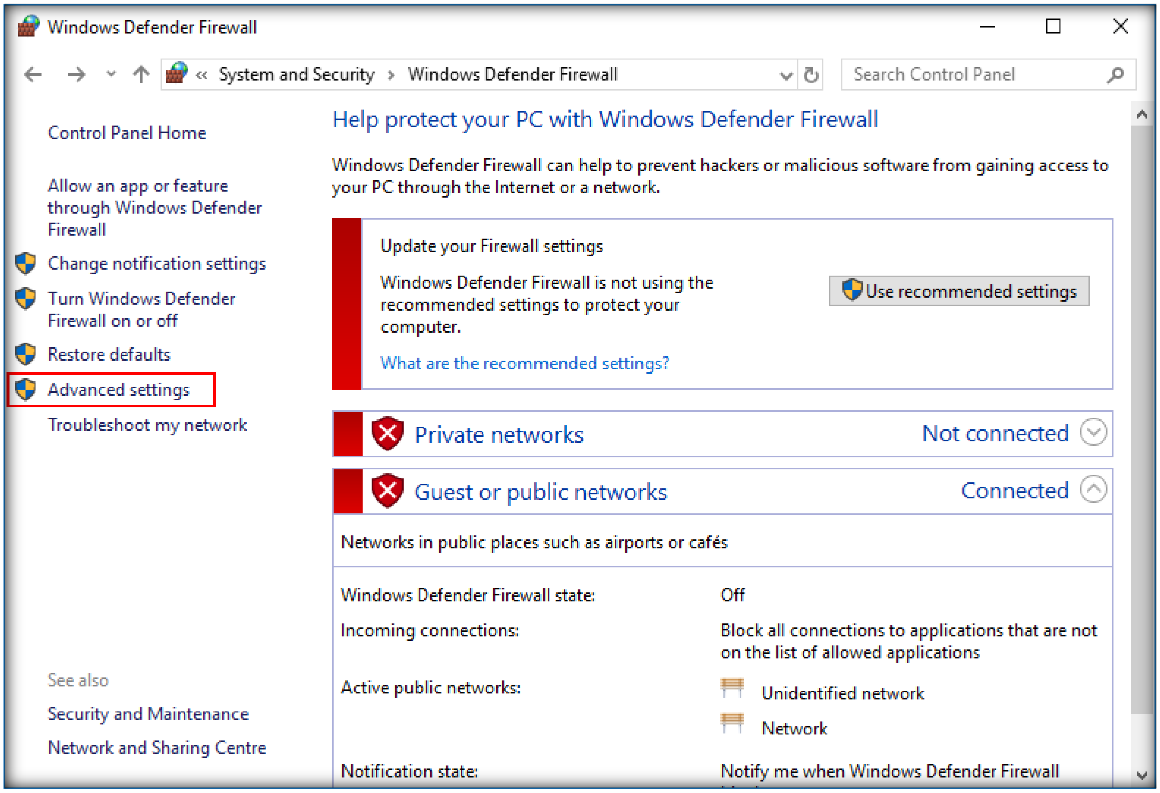
○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed applications

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

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



Windows Defender Firewall
System and Security > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Centre

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help to prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

Use recommended settings

What are the recommended settings?

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or cafés

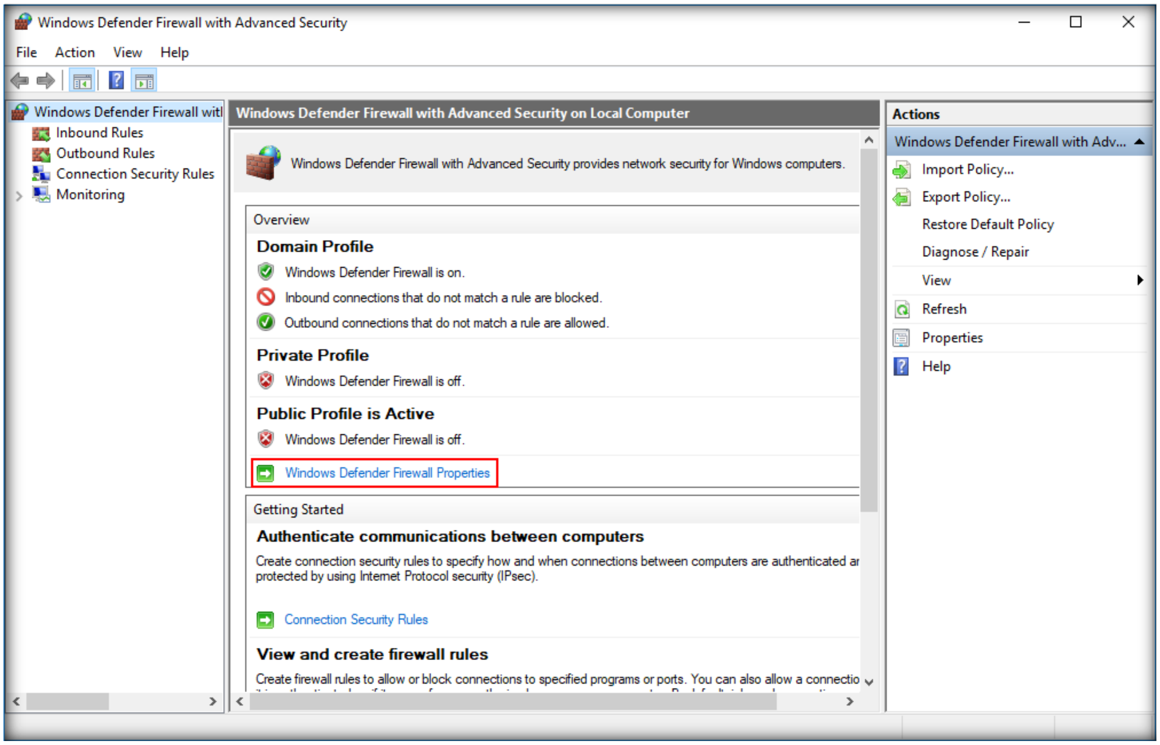
Windows Defender Firewall state: Off

Incoming connections: Block all connections to applications that are not on the list of allowed applications

Active public networks: Unidentified network; Network

Notification state: Notify me when Windows Defender Firewall

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



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

Windows Defender Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Private Profile

Windows Defender Firewall is off.

Public Profile is Active

Windows Defender Firewall is off.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

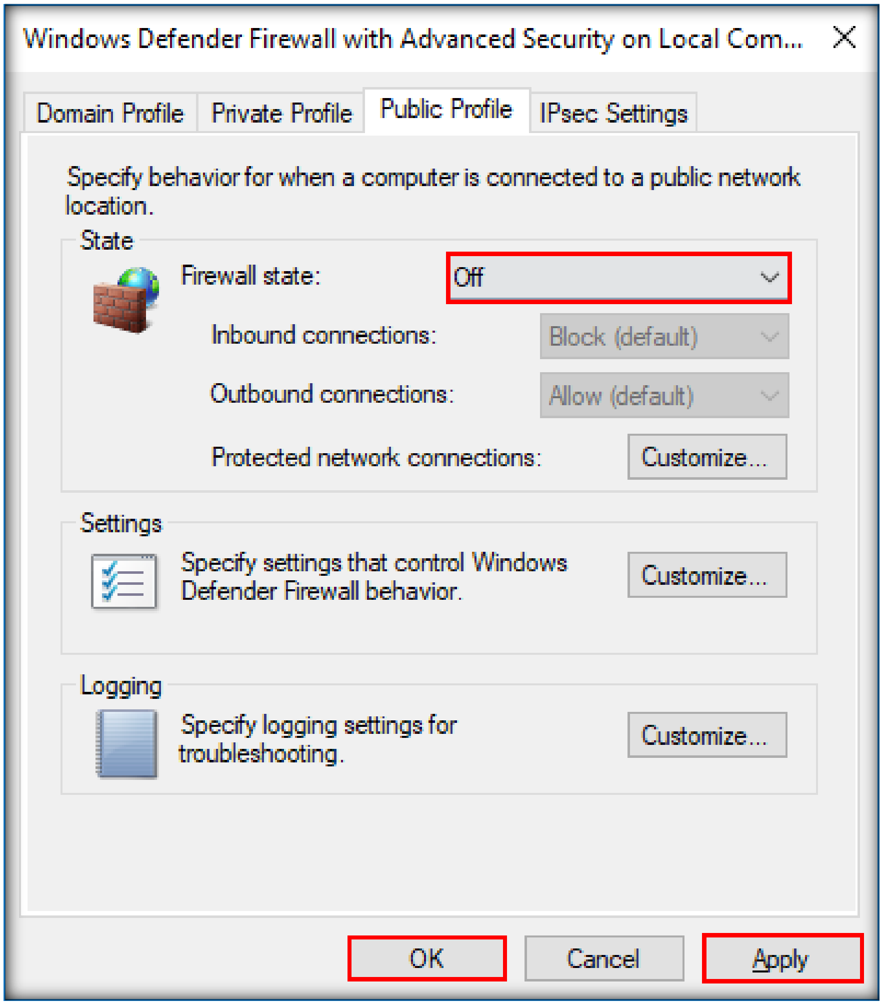
Create connection security rules to specify how and when connections between computers are authenticated ar protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connectio

10. 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 **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply** and then click **OK**.



Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

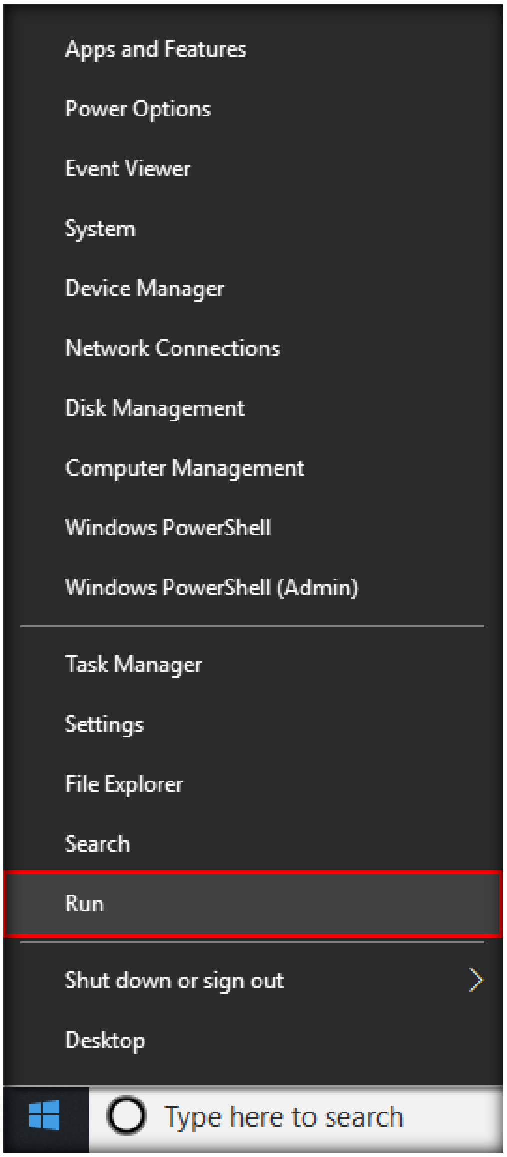
Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

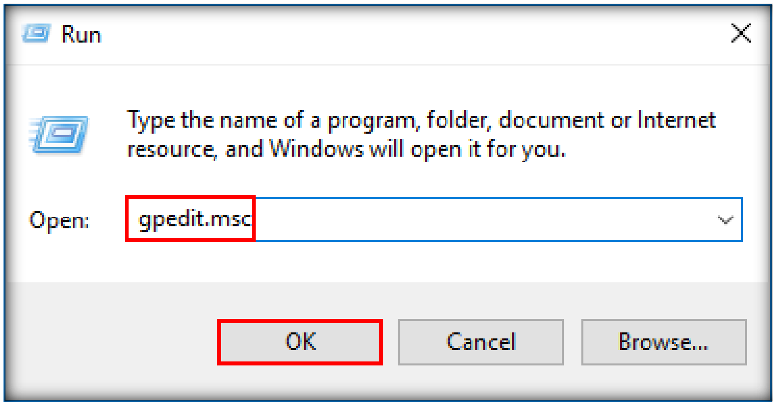
Specify logging settings for troubleshooting. Customize...

11. Close all the windows.

12. Right-click the **Windows** button at the lower left corner of the screen and click **Run**.



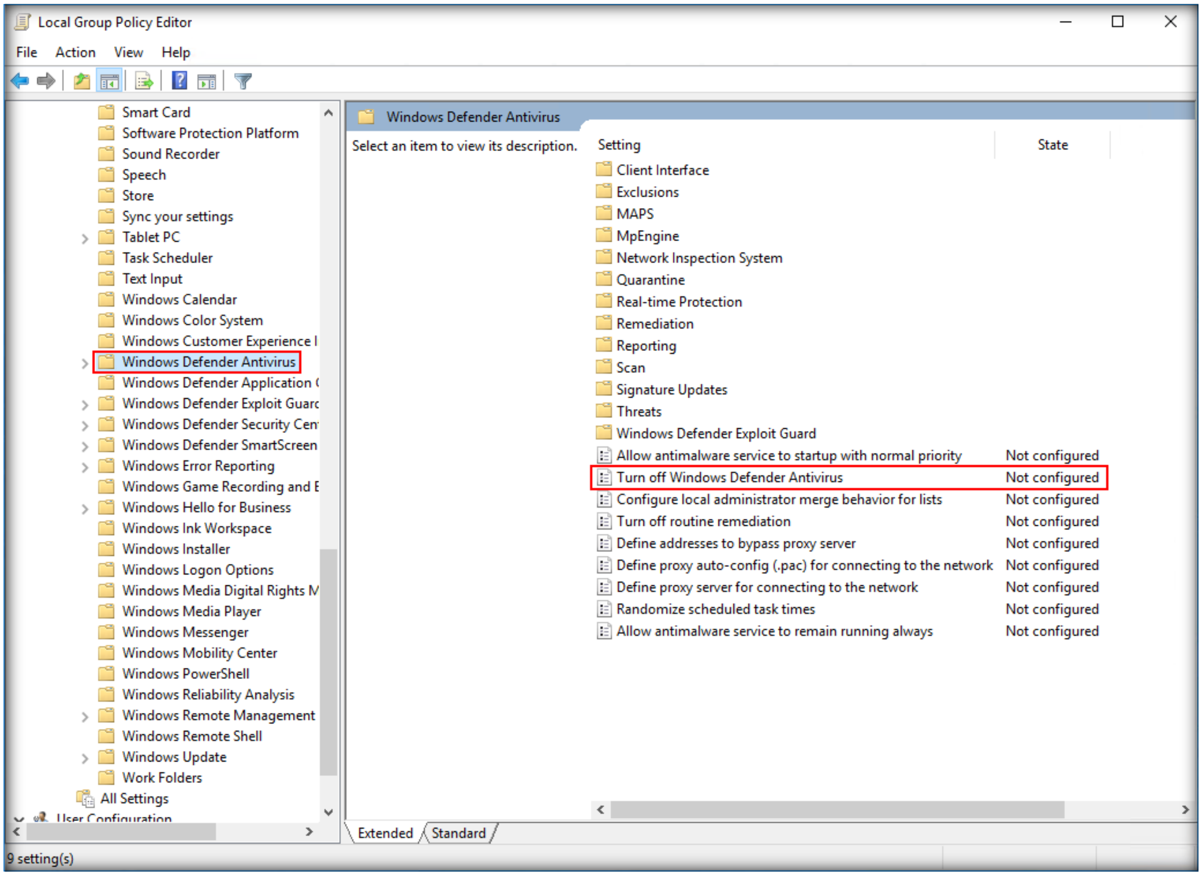
13. **Run** window appears, type **gpedit.msc** and click **OK**.



Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

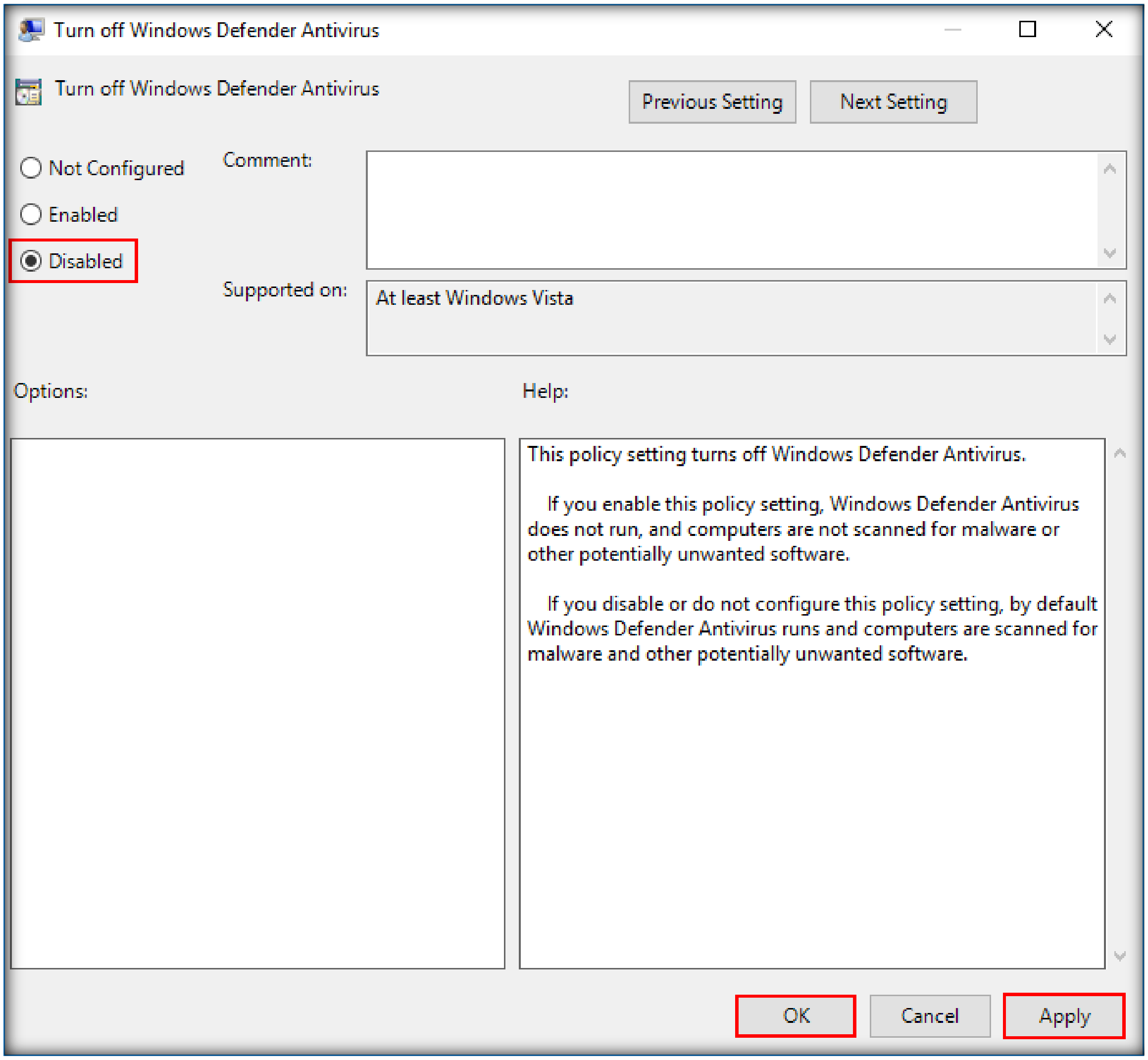
Open: gpedit.msc

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


Local Group Policy Editor
File
Action
View
Help
Smart Card
Software Protection Platform
Sound Recorder
Speech
Store
Sync your settings
Tablet PC
Task Scheduler
Text Input
Windows Calendar
Windows Color System
Windows Customer Experience I
Windows Defender Antivirus
Windows Defender Application (
Windows Defender Exploit Guarc
Windows Defender Security Cen
Windows Defender SmartScreen
Windows Error Reporting
Windows Game Recording and E
Windows Hello for Business
Windows Ink Workspace
Windows Installer
Windows Logon Options
Windows Media Digital Rights M
Windows Media Player
Windows Messenger
Windows Mobility Center
Windows PowerShell
Windows Reliability Analysis
Windows Remote Management
Windows Remote Shell
Windows Update
Work Folders
All Settings
User Configuration
Windows Defender Antivirus
Select an item to view its description.
Extended
Standard
9 setting(s)

Setting	State
Client Interface	
Exclusions	
MAPS	
MpEngine	
Network Inspection System	
Quarantine	
Real-time Protection	
Remediation	
Reporting	
Scan	
Signature Updates	
Threats	
Windows Defender Exploit Guard	
Allow antimalware service to startup with normal priority	Not configured
Turn off Windows Defender Antivirus	Not configured
Configure local administrator merge behavior for lists	Not configured
Turn off routine remediation	Not configured
Define addresses to bypass proxy server	Not configured
Define proxy auto-config (.pac) for connecting to the network	Not configured
Define proxy server for connecting to the network	Not configured
Randomize scheduled task times	Not configured
Allow antimalware service to remain running always	Not configured

15. When the **Turn off Windows Defender Antivirus** window appears, choose the **Disabled** radio button and click **Apply** and **OK** to turn off Windows Defender Antivirus.



Turn off Windows Defender Antivirus

○ Not Configured

○ Enabled

● Disabled

Comment:

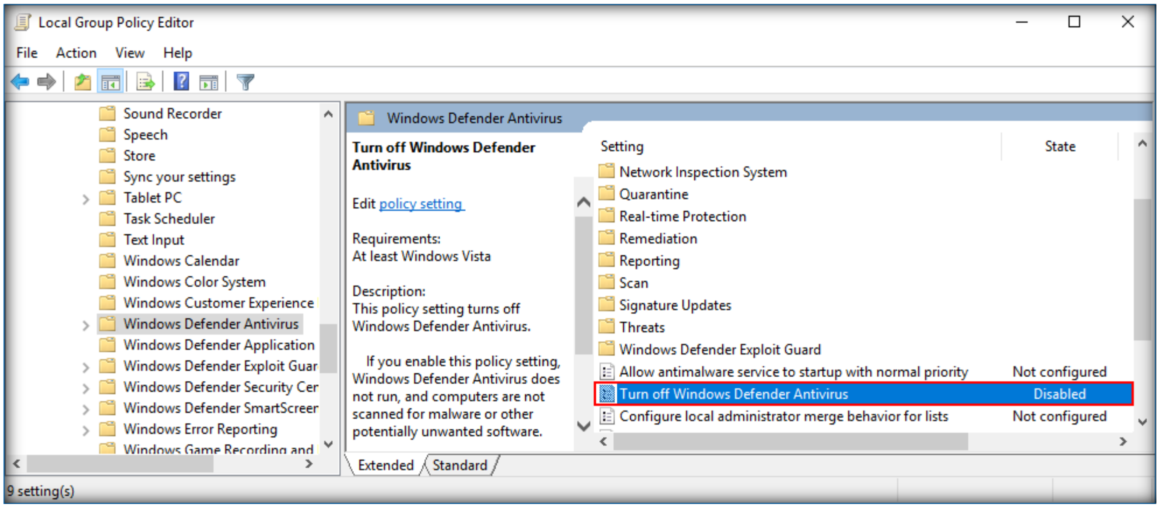
Supported on: At least Windows Vista

This policy setting turns off Windows Defender Antivirus.

If you enable this policy setting, Windows Defender Antivirus does not run, and computers are not scanned for malware or other potentially unwanted software.

If you disable or do not configure this policy setting, by default Windows Defender Antivirus runs and computers are scanned for malware and other potentially unwanted software.

16. **Windows Defender Antivirus** is turned off.


Local Group Policy Editor
File
Action
View
Help
Sound Recorder
Speech
Store
Sync your settings
Tablet PC
Task Scheduler
Text Input
Windows Calendar
Windows Color System
Windows Customer Experience
Windows Defender Antivirus
Windows Defender Application
Windows Defender Exploit Guar
Windows Defender Security Cer
Windows Defender SmartScreer
Windows Error Reporting
Windows Game Recording and
Extended
Standard
9 setting(s)

Windows Defender Antivirus

Turn off Windows Defender Antivirus

Edit policy setting

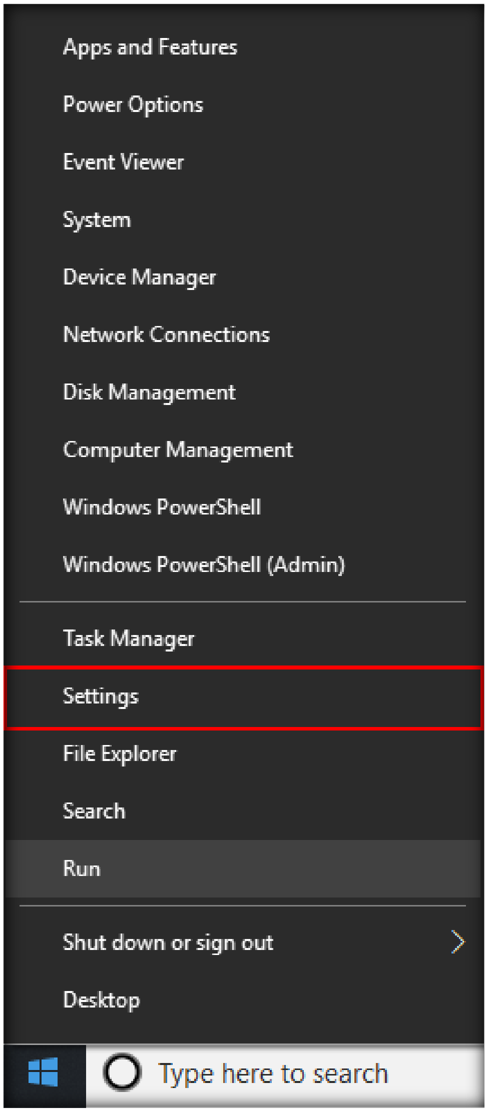
Requirements:
At least Windows Vista

Description:
This policy setting turns off Windows Defender Antivirus.

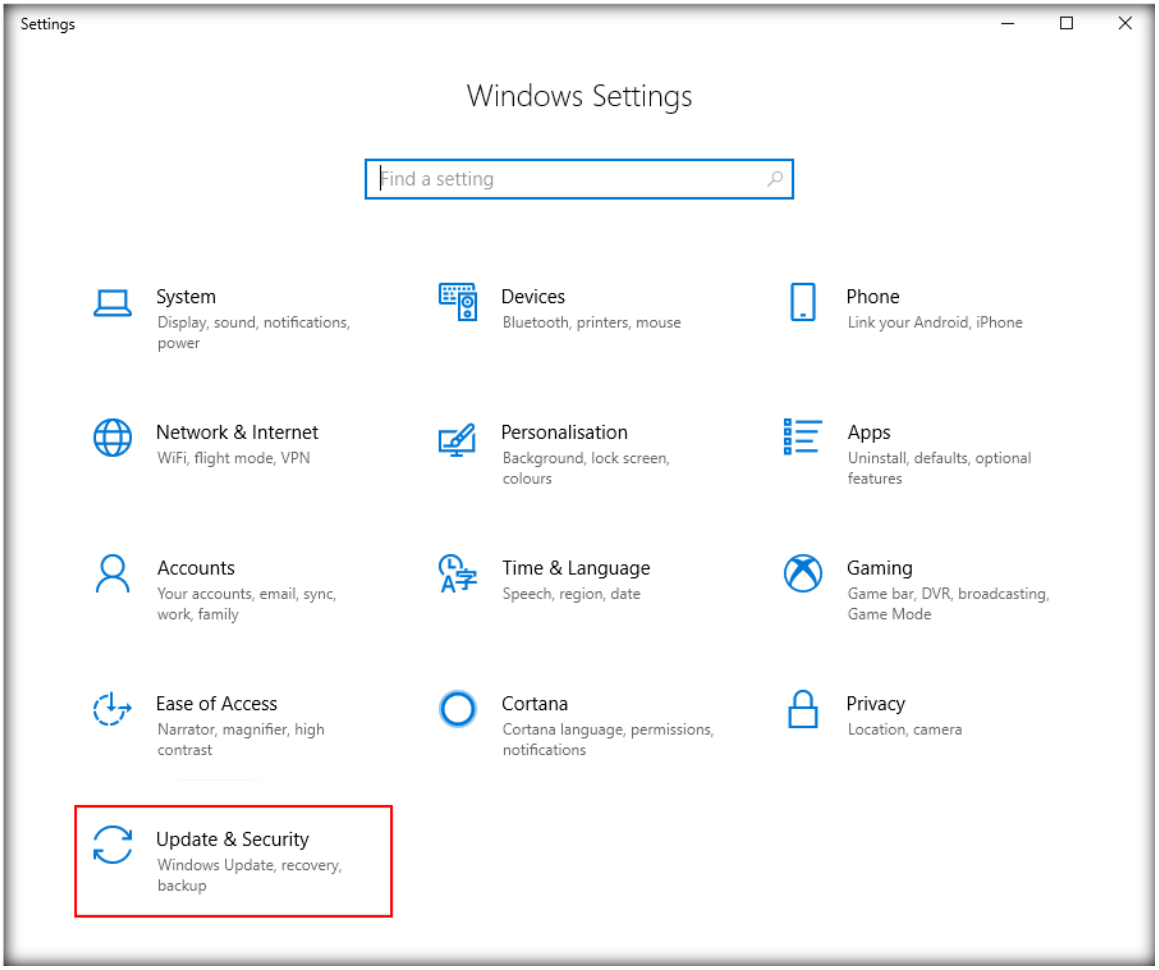
If you enable this policy setting, Windows Defender Antivirus does not run, and computers are not scanned for malware or other potentially unwanted software.

Setting	State
Network Inspection System	
Quarantine	
Real-time Protection	
Remediation	
Reporting	
Scan	
Signature Updates	
Threats	
Windows Defender Exploit Guard	
Allow antimalware service to startup with normal priority	Not configured
Turn off Windows Defender Antivirus	Disabled
Configure local administrator merge behavior for lists	Not configured

17. Close all the windows.
18. Right-click **Windows** button at the lower left corner of the screen and click **Settings**.



19. In the **Settings** window, click **Update & Security**.



Settings

Windows Settings

Find a setting

System
Display, sound, notifications, power

Devices
Bluetooth, printers, mouse

Phone
Link your Android, iPhone

Network & Internet
WiFi, flight mode, VPN

Personalisation
Background, lock screen, colours

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, family

Time & Language
Speech, region, date

Gaming
Game bar, DVR, broadcasting, Game Mode

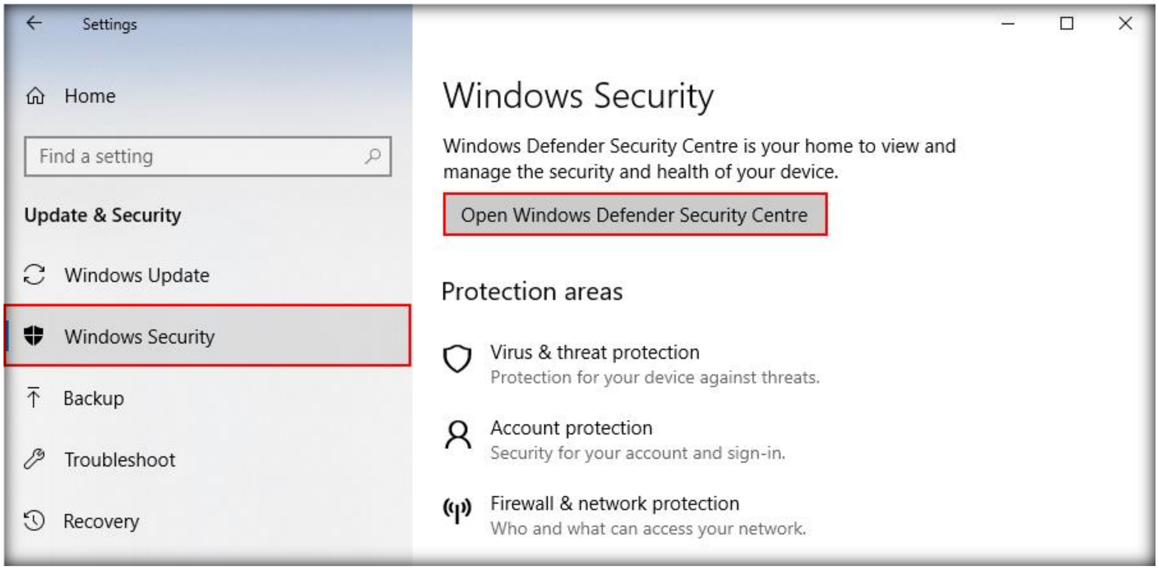
Ease of Access
Narrator, magnifier, high contrast

Cortana
Cortana language, permissions, notifications

Privacy
Location, camera

Update & Security
Windows Update, recovery, backup

20. In the **Settings** window, **Update & Security** settings will be available in the left-pane. Click **Windows Security.** This page appears in the right-pane. Click **Open Windows Defender Security Center** button as shown in the screenshot.



Settings

Home

Find a setting

Update & Security

Windows Update

Windows Security

Backup

Troubleshoot

Recovery

Windows Security

Windows Defender Security Centre is your home to view and manage the security and health of your device.

Open Windows Defender Security Centre

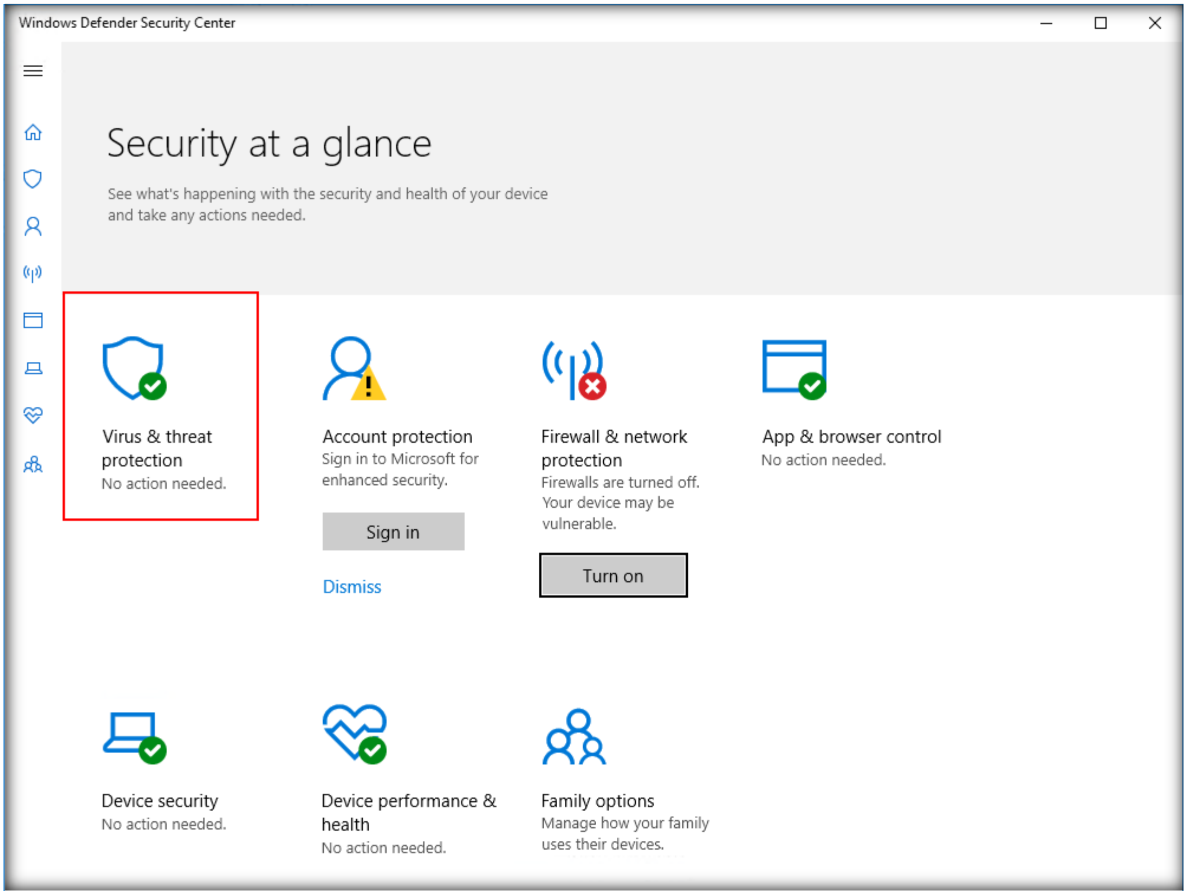
Protection areas

Virus & threat protection
Protection for your device against threats.

Account protection
Security for your account and sign-in.

Firewall & network protection
Who and what can access your network.

21. In the **Windows Defender Security Center** window, click **Virus & threat protection**.



Windows Defender Security Center

Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
Sign in to Microsoft for enhanced security.

Sign in

Dismiss

Firewall & network protection
Firewalls are turned off. Your device may be vulnerable.

Turn on

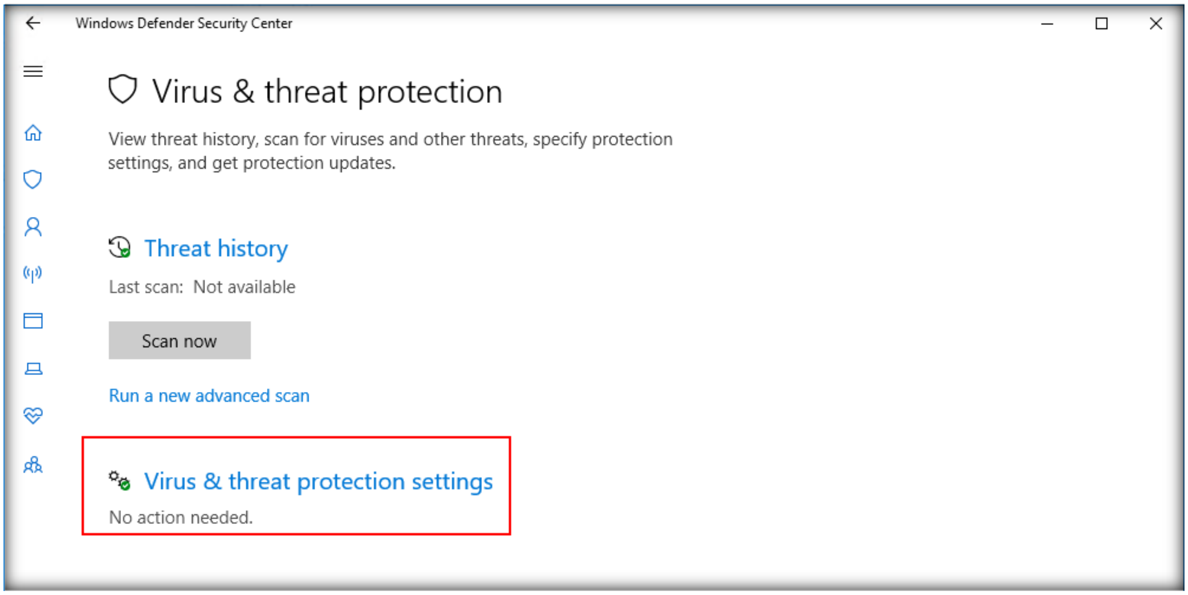
App & browser control
No action needed.

Device security
No action needed.

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

22. In the **Virus & threat protection** page, click **Virus & threat protection settings**.



Windows Defender Security Center

Virus & threat protection

View threat history, scan for viruses and other threats, specify protection settings, and get protection updates.

Threat history

Last scan: Not available

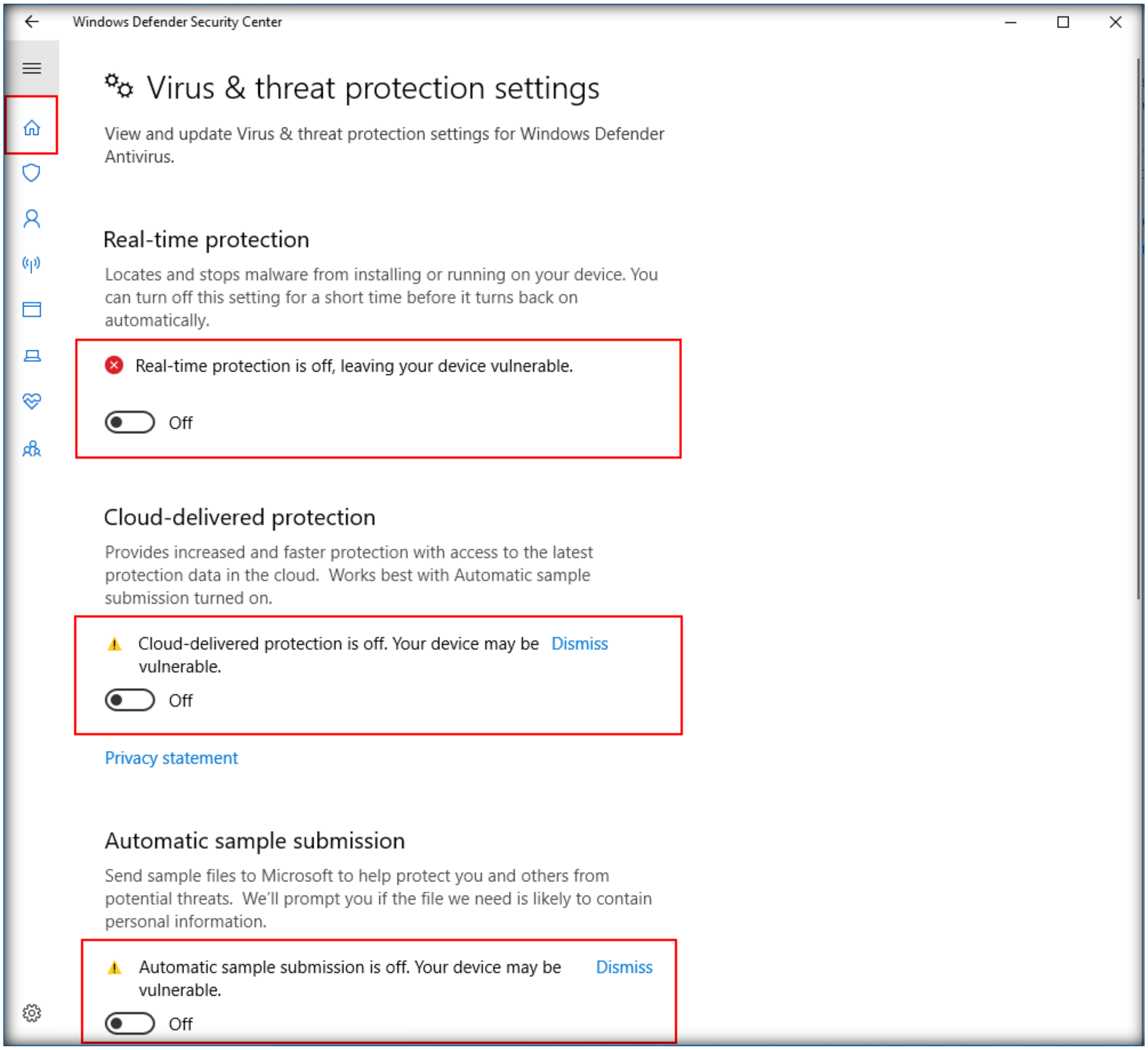
Scan now

Run a new advanced scan

Virus & threat protection settings

No action needed.

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



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

Off

Privacy statement

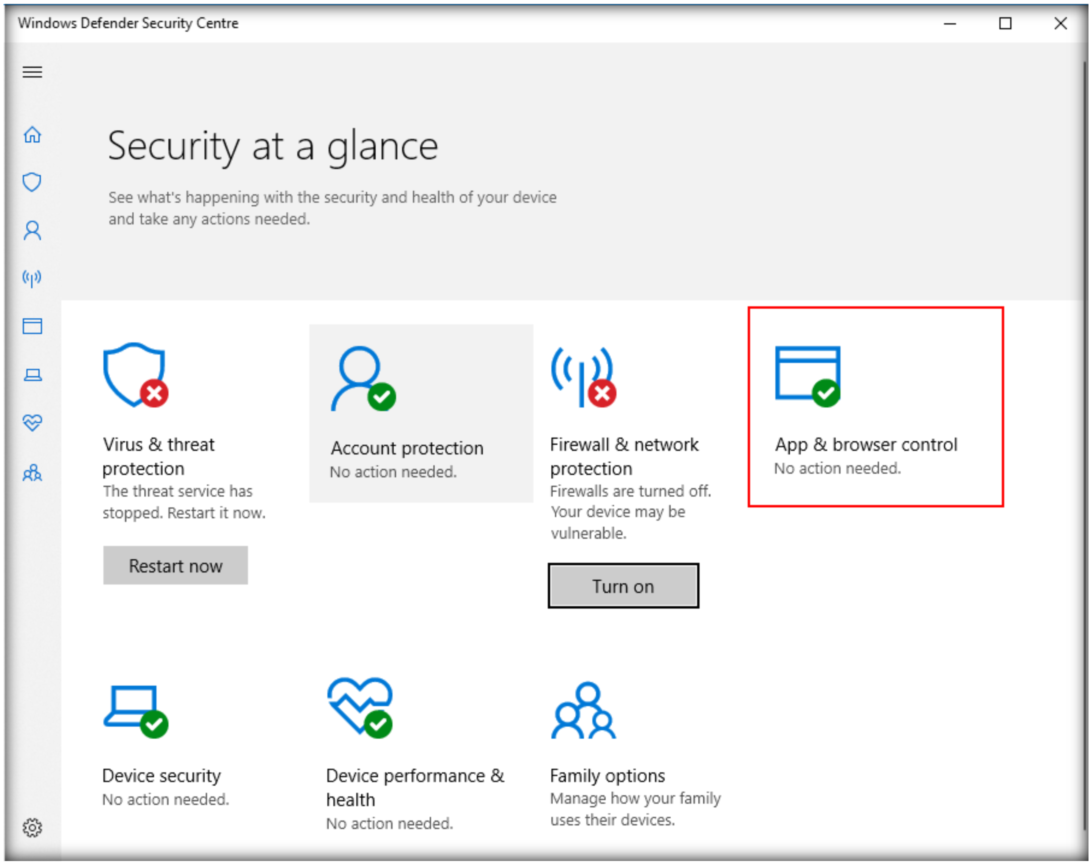
Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable. Dismiss

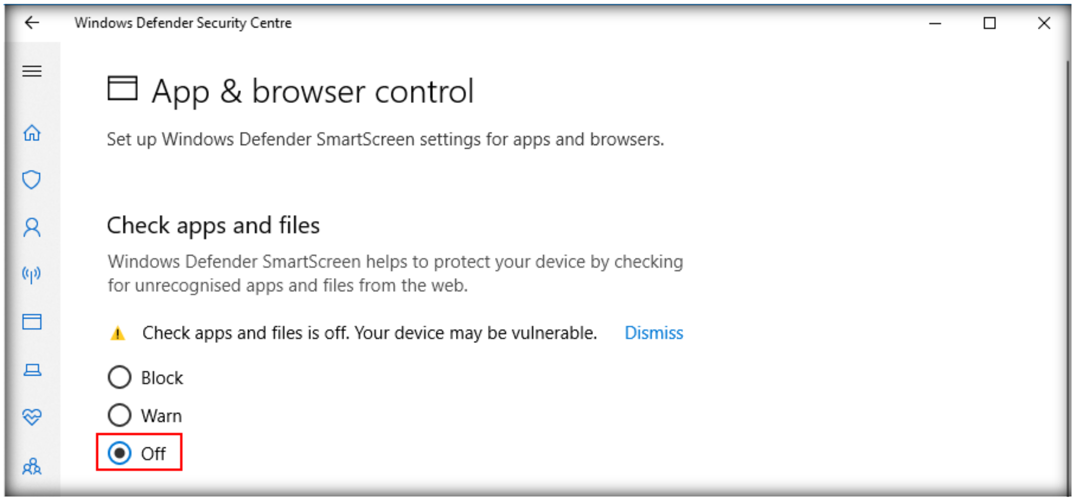
Off

24. Then, click **App & browser control** in the **Windows Defender Security Center** window.


Windows Defender Security Centre
Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Virus & threat protection
The threat service has stopped. Restart it now.
Restart now
Account protection
No action needed.
Firewall & network protection
Firewalls are turned off. Your device may be vulnerable.
Turn on
App & browser control
No action needed.
Device security
No action needed.
Device performance & health
No action needed.
Family options
Manage how your family uses their devices.

25. In the **App & browser control** page, select the **Off** radio button 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.


Windows Defender Security Centre
App & browser control
Set up Windows Defender SmartScreen settings for apps and browsers.
Check apps and files
Windows Defender SmartScreen helps to protect your device by checking for unrecognised apps and files from the web.
Check apps and files is off. Your device may be vulnerable.
Dismiss
○ Block
○ Warn
● Off

26. Close all the windows.

CT#3: Download SOC Tools

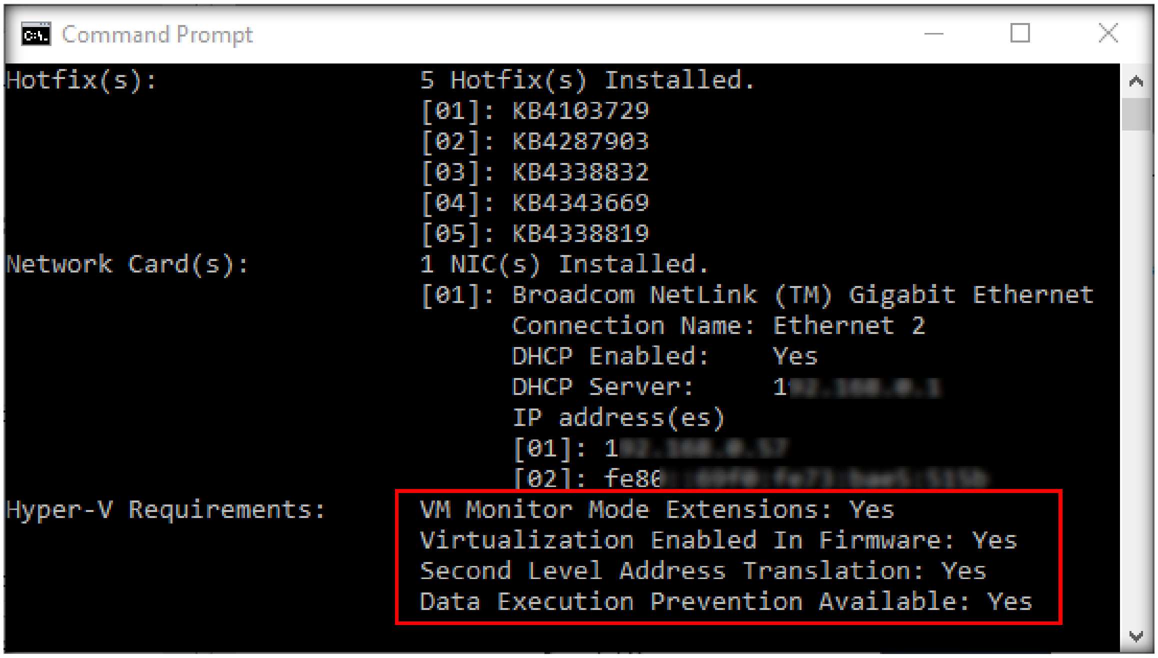
1. In the **host** machine, create a folder in the Drive **D:** named **SOC-Tools**.
2. Log in to your **Aspen** account. (You will see your course listed under **My Courses**.) → Click **TRAINING** button under the course to access the e-Courseware, Lab Manuals, and Tools in the **Training** area → Click **Download Tools** tab from the left-pane.
3. Click the module names from the right-pane and download all the **SOC Tools** files to the **D:\SOC-Tools** folder.
4. Right-click the .zip files in the **D:\SOC-Tools** folder and select the **Extract Here** option.

CT#4: Install Hyper-V role in Windows 10 Host Machine

Note: Hardware Requirements for installing Hyper-V

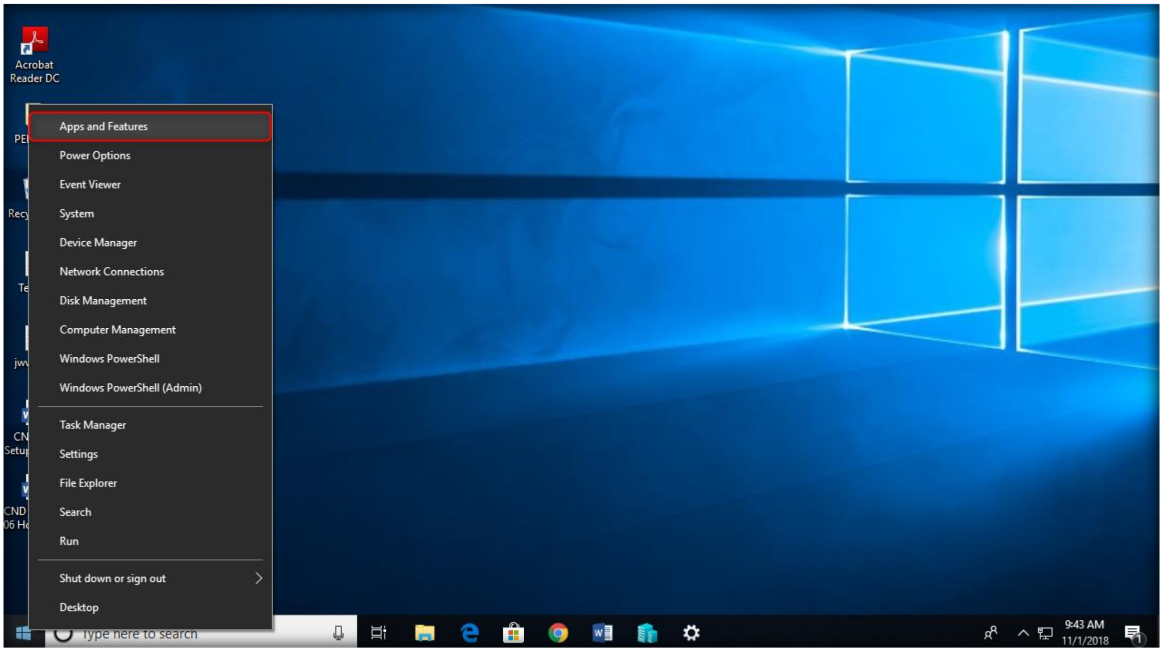
- A 64-bit processor with second-level address translation (SLAT).
- CPU support for Virtual Machine Monitor Mode Extension (VT-c on Intel CPU's).
- Virtualization technology may have a different label based on the motherboard manufacturer.
- Hardware-enforced data execution prevention.

1. Login to the **Windows 10** host machine. To verify compatibility, open up **PowerShell** or a **Command Prompt (cmd.exe)** and type **systeminfo.exe**. This returns information about Hyper-V compatibility. If all listed Hyper-V requirements have a value of **Yes**, your system can run the Hyper-V role. Close the **Command Prompt**.

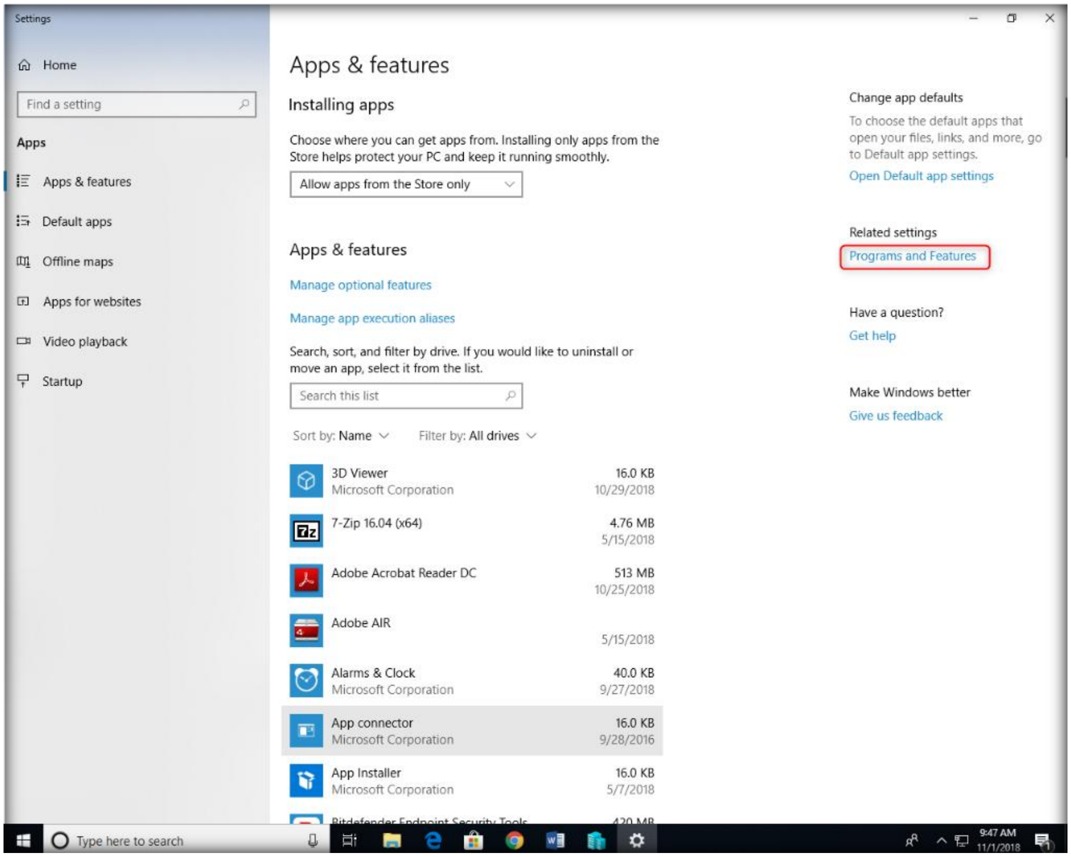


```
Hotfix(s):                     5 Hotfix(s) Installed.
                               [01]: KB4103729
                               [02]: KB4287903
                               [03]: KB4338832
                               [04]: KB4343669
                               [05]: KB4338819
Network Card(s):               1 NIC(s) Installed.
                               [01]: Broadcom NetLink (TM) Gigabit Ethernet
                                     Connection Name: Ethernet 2
                                     DHCP Enabled:    Yes
                                     DHCP Server:     1[redacted]
                                     IP address(es)
                                     [01]: 1[redacted]
                                     [02]: fe80[redacted]
Hyper-V Requirements:          VM Monitor Mode Extensions: Yes
                               Virtualization Enabled In Firmware: Yes
                               Second Level Address Translation: Yes
                               Data Execution Prevention Available: Yes
```

2. Right-click on the windows start button icon and select **Apps and Features**.



3. The **App and Features** window appears; click on **Programs and Features** link as shown in following screenshot.



Choose where you can get apps from. Installing only apps from the Store helps protect your PC and keep it running smoothly.

Allow apps from the Store only

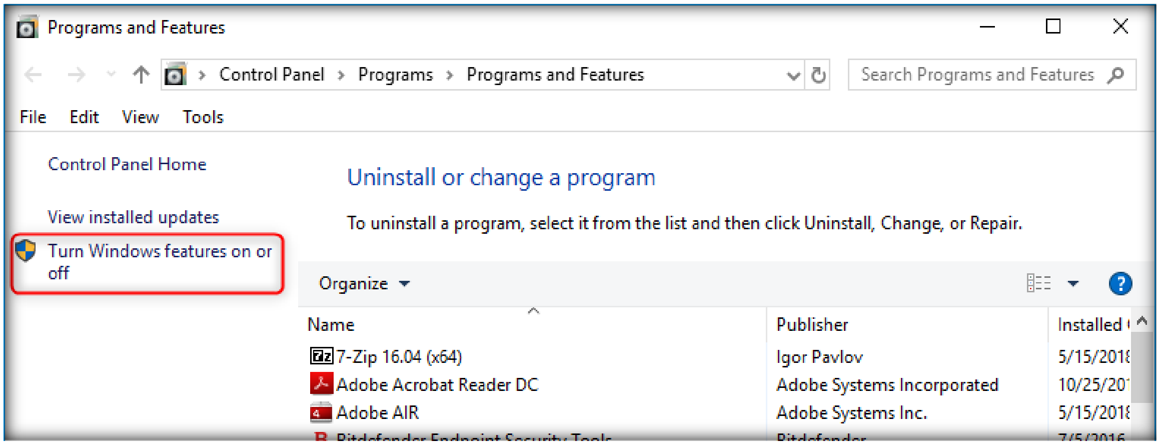
Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

Sort by: Name   Filter by: All drives

To choose the default apps that open your files, links, and more, go to Default app settings.

3D Viewer Microsoft Corporation	16.0 KB 10/29/2018
7-Zip 16.04 (x64)	4.76 MB 5/15/2018
Adobe Acrobat Reader DC	513 MB 10/25/2018
Adobe AIR	5/15/2018
Alarms & Clock Microsoft Corporation	40.0 KB 9/27/2018
App connector Microsoft Corporation	16.0 KB 9/28/2016
App Installer Microsoft Corporation	16.0 KB 5/7/2018
Bitdefender Endpoint Security Tools	420 MB

4. The **Program and Features** window appears, click **Turn Windows features on or off.**



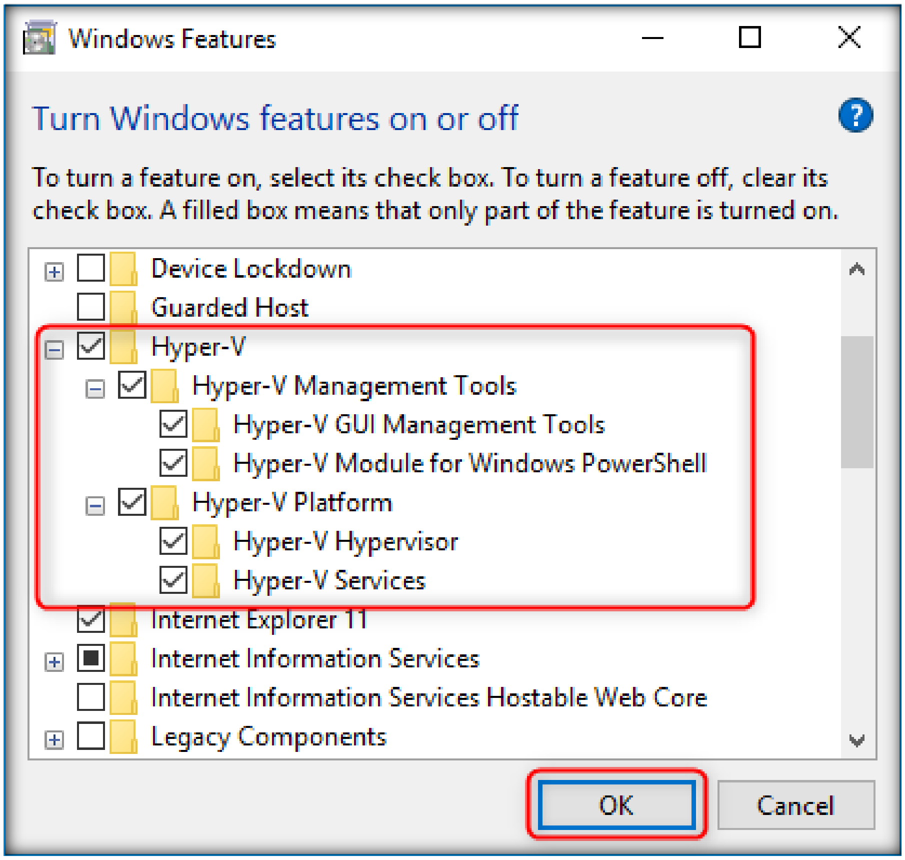
Programs and Features
Control Panel › Programs › Programs and Features
Search Programs and Features
File Edit View Tools
Control Panel Home
View installed updates
Turn Windows features on or off
Organize

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed
7-Zip 16.04 (x64)	Igor Pavlov	5/15/201
Adobe Acrobat Reader DC	Adobe Systems Incorporated	10/25/20
Adobe AIR	Adobe Systems Inc.	5/15/201
Bitdefender Endpoint Security Tools	Bitdefender	7/5/2016

5. The **Windows Features** list will appear, check the **Hyper-V** feature as shown in the screenshot. Click **OK.**



Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Device Lockdown
- □ Guarded Host
- ☑ Hyper-V
  - ☑ Hyper-V Management Tools
    - ☑ Hyper-V GUI Management Tools
    - ☑ Hyper-V Module for Windows PowerShell
  - ☑ Hyper-V Platform
    - ☑ Hyper-V Hypervisor
    - ☑ Hyper-V Services
- ☑ Internet Explorer 11
- ■ Internet Information Services
- □ Internet Information Services Hostable Web Core
- □ Legacy Components

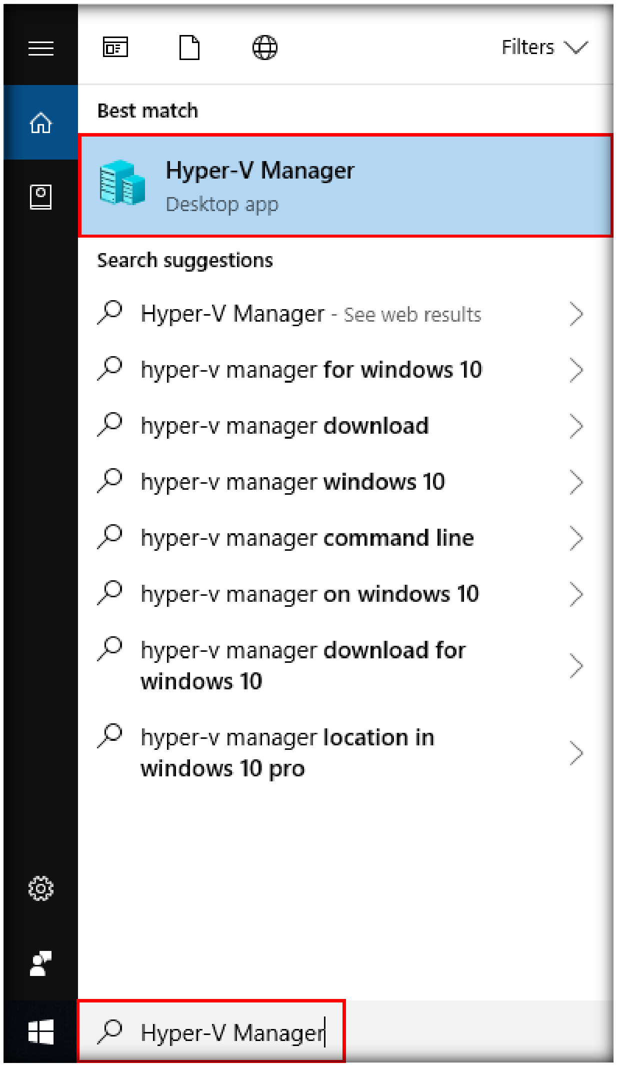
6. After applying the requested changes with regard to Hyper-V feature, click **Restart now**.

7. Once the system reboots, launch the Hyper-V Manager. This can be done in two ways:

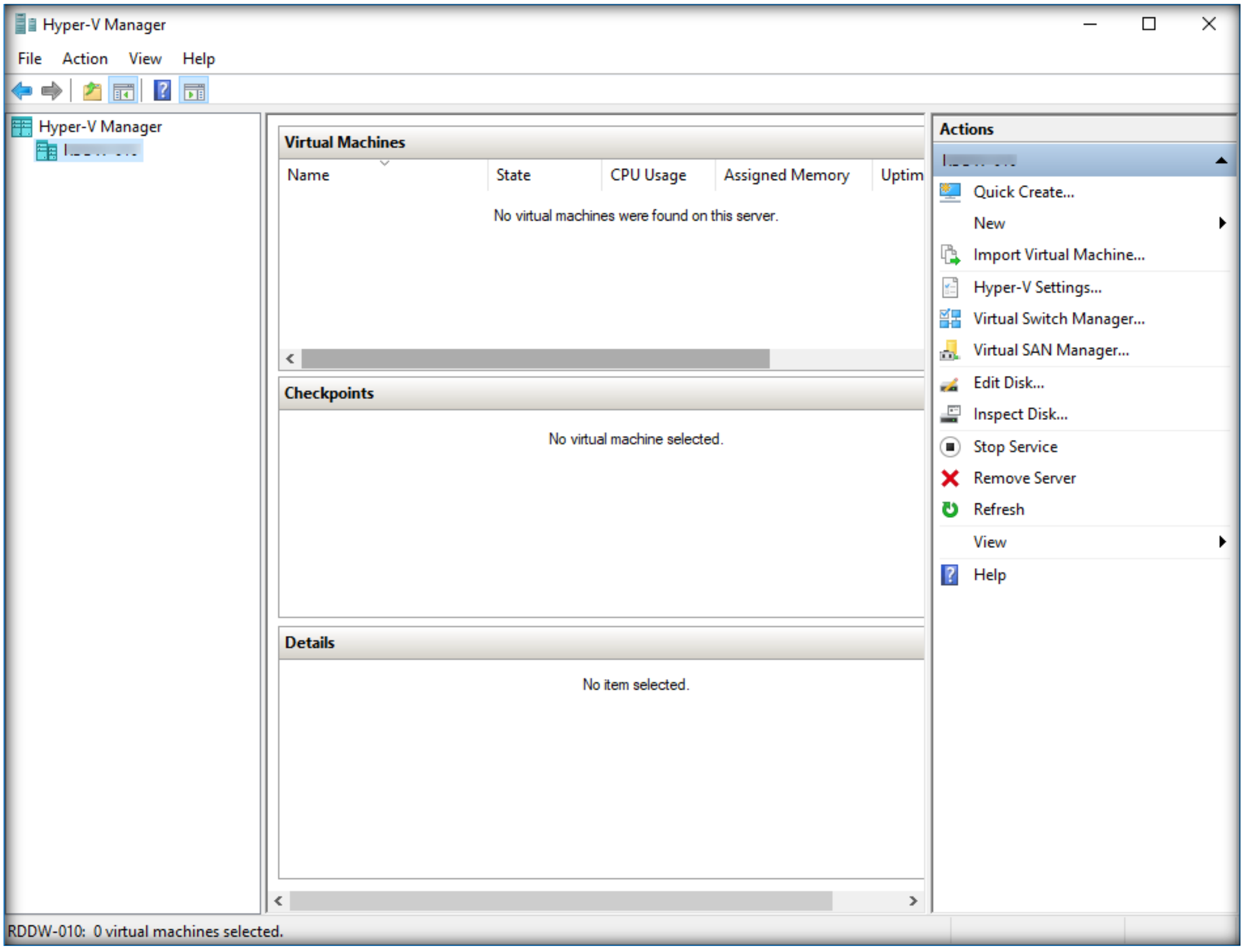
   By typing **Hyper-V Manager** in the **Type here to search** field at the lower left corner of window and clicking on **Hyper-V Manager.**

   (or)

   Click the **Windows** icon present at the lower left corner of the window, navigate down and expand the **Window Administrative Tools** folder to find the **Hyper-V Manager** icon. Click **Hyper-V Manager**.


Filters
Best match
Hyper-V Manager
Desktop app
Search suggestions
Hyper-V Manager - See web results
hyper-v manager for windows 10
hyper-v manager download
hyper-v manager windows 10
hyper-v manager command line
hyper-v manager on windows 10
hyper-v manager download for windows 10
hyper-v manager location in windows 10 pro
Hyper-V Manager

8. **Hyper-V Manager** window appears along with the current machine's name in the left-pane as shown in the screenshot.



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptim

No virtual machines were found on this server.

Checkpoints

No virtual machine selected.

Details

No item selected.

RDDW-010: 0 virtual machines selected.

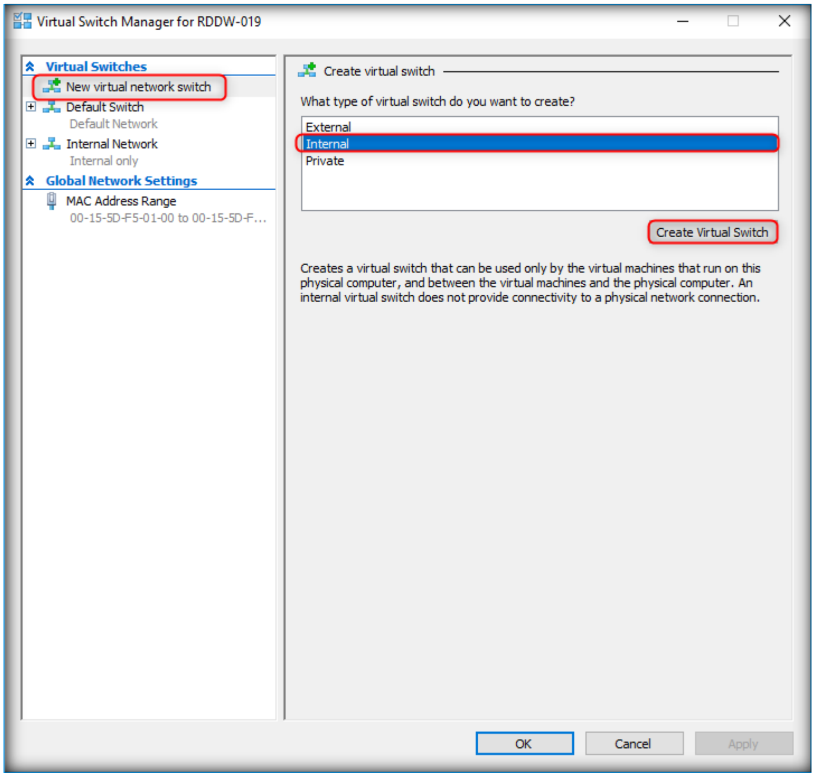
9. Hyper-V has been successfully installed in the **Window 10** host machine.

CT#5: Configuring Network for Hyper-V

CT#5.1: Configuring Internal Network for Hyper-V

1. Launch **Hyper-V** Manager.
2. Click **Virtual Switch Manager** in the right pane **of Hyper-V Manager**. The **Virtual Switch Manager** window appears.
3. Select **New virtual network switch** from left pane, and select **Internal** as the network type in the pane of the window.

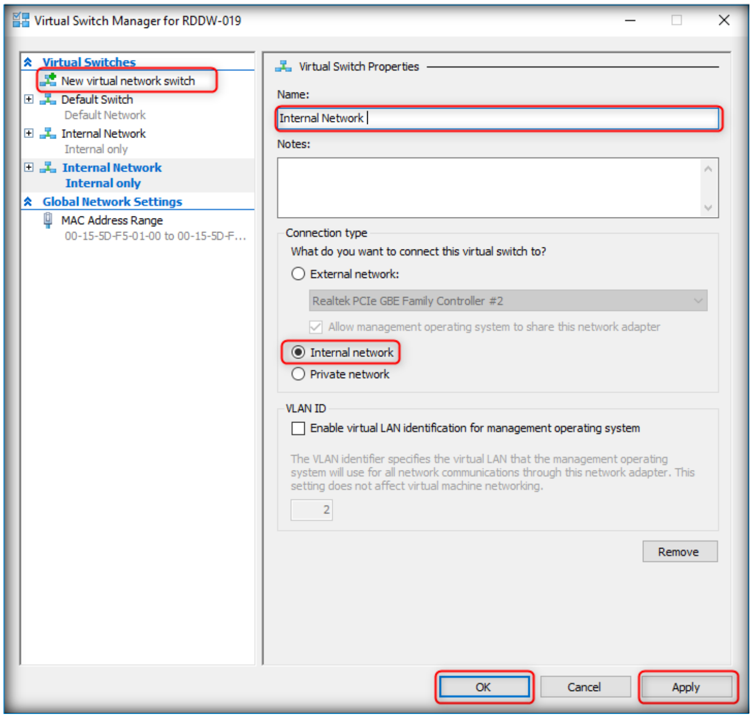
4. Click **Create Virtual Switch** button.



What type of virtual switch do you want to create?

Creates a virtual switch that can be used only by the virtual machines that run on this physical computer, and between the virtual machines and the physical computer. An internal virtual switch does not provide connectivity to a physical network connection.

5. The newly created virtual switch appears in the left pane. Enter the name of the virtual switch as **Internal Network** under the **Name** field, select **Internal network** radio button, click **Apply** and then click **OK.**



Name: Internal Network

Notes:

Connection type

What do you want to connect this virtual switch to?

○ External network:

Realtek PCIe GBE Family Controller #2

☑ Allow management operating system to share this network adapter

● Internal network

○ Private network

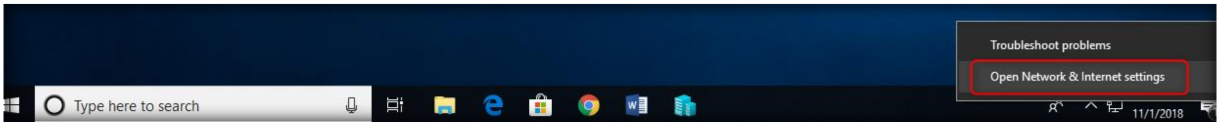
VLAN ID

□ Enable virtual LAN identification for management operating system

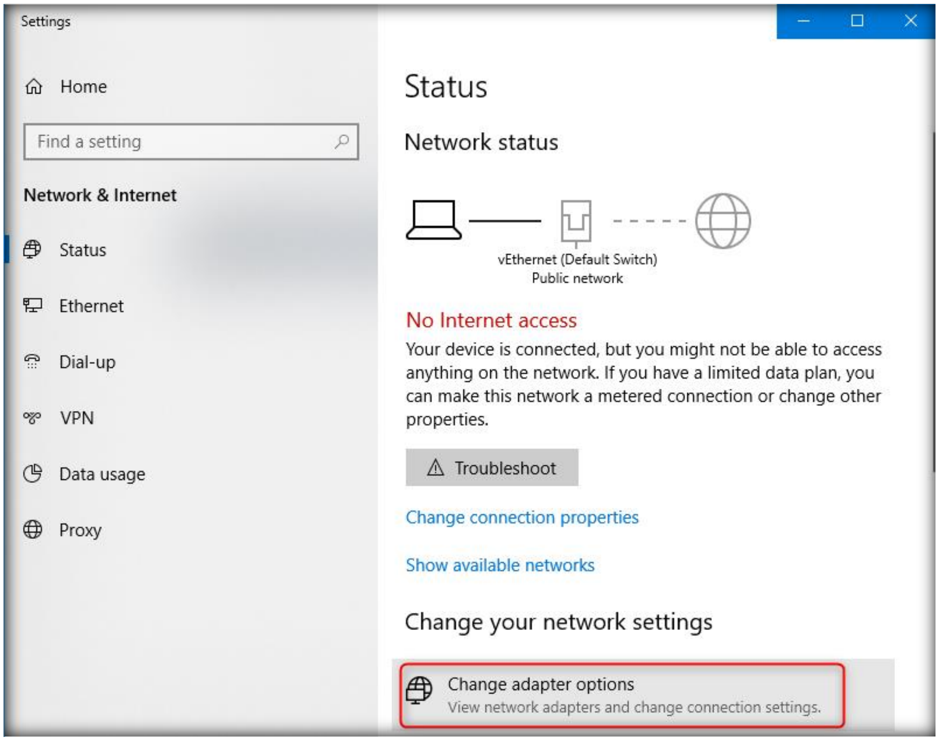
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

6. Right-click on Network icon (lower right corner of the desktop), and click **Open Network and Internet Setting** from the context menu.



7. The **Settings** window appears. In the Settings window, click on **Change adaptor options**.

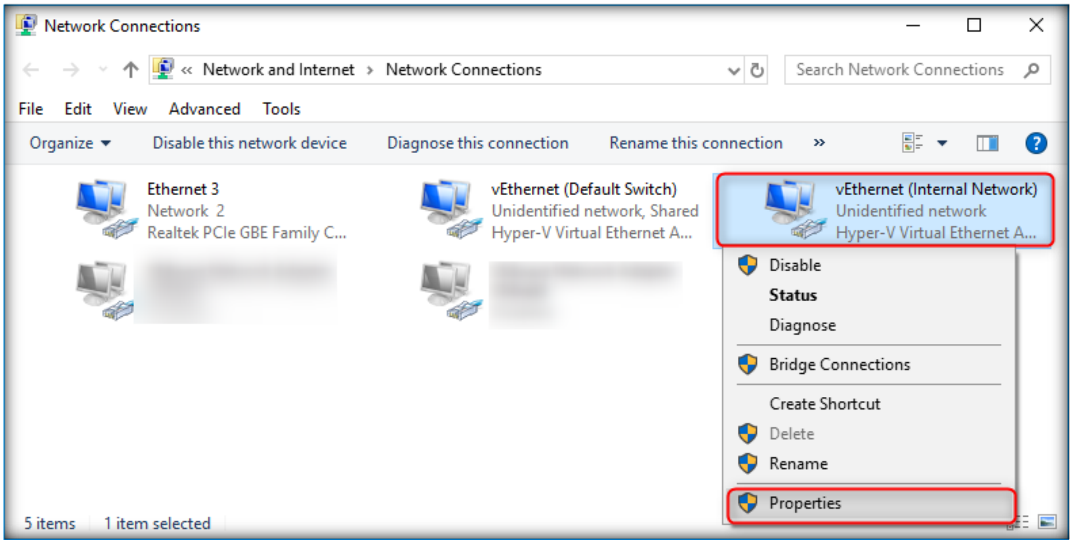


No Internet access

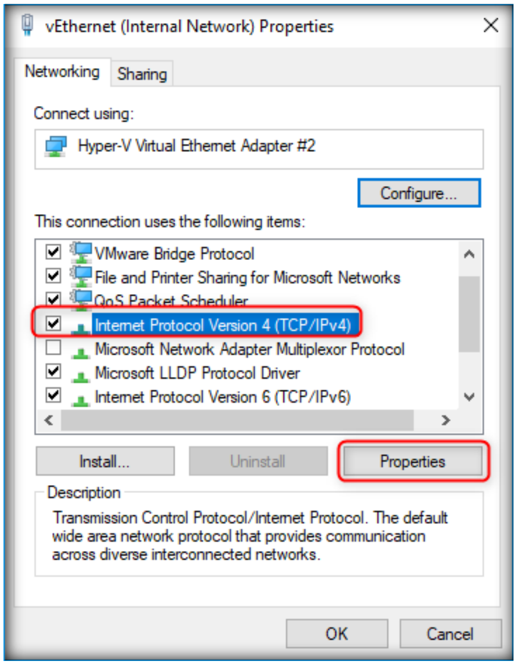
Your device is connected, but you might not be able to access anything on the network. If you have a limited data plan, you can make this network a metered connection or change other properties.

Troubleshoot
Change connection properties
Show available networks
Change your network settings
Change adapter options
View network adapters and change connection settings.

8. In the **Network Connections** window, right-click on created **Internal Network** switch; and click **Properties** from the context menu.


Network Connections
« Network and Internet › Network Connections
Search Network Connections
File Edit View Advanced Tools
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
»
Ethernet 3
Network 2
Realtek PCIe GBE Family C...
vEthernet (Default Switch)
Unidentified network, Shared
Hyper-V Virtual Ethernet A...
vEthernet (Internal Network)
Unidentified network
Hyper-V Virtual Ethernet A...
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
5 items
1 item selected

9. Internal Network adapter properties window appears, scroll down and select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



vEthernet (Internal Network) Properties

Networking | Sharing

Connect using:

Hyper-V Virtual Ethernet Adapter #2

Configure...

This connection uses the following items:

☑ VMware Bridge Protocol
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Install... | Uninstall | Properties

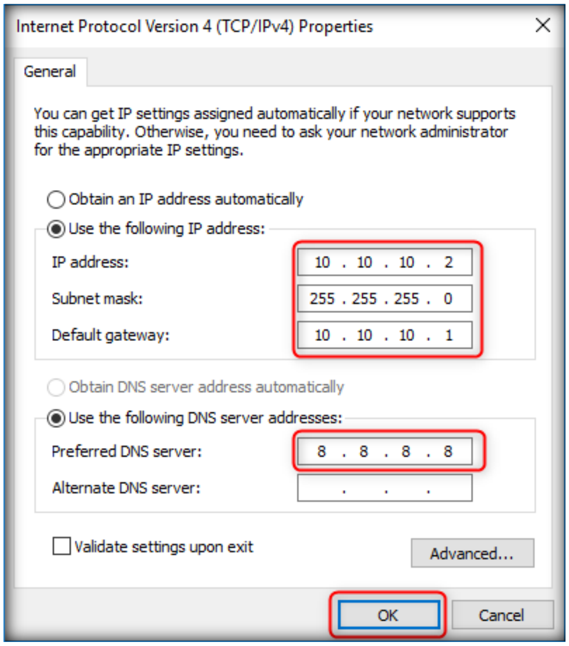
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

10. Select **Use the following IP address** radio button, and type the following values as shown in the screenshot and click **OK**.

   - IP address: **10.10.10.2**
   - Subnet mask: **255.255.255.0**
   - Default gateway: **10.10.10.1**
   - Preferred DNS server: **8.8.8.8**



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 10 . 10 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 10 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

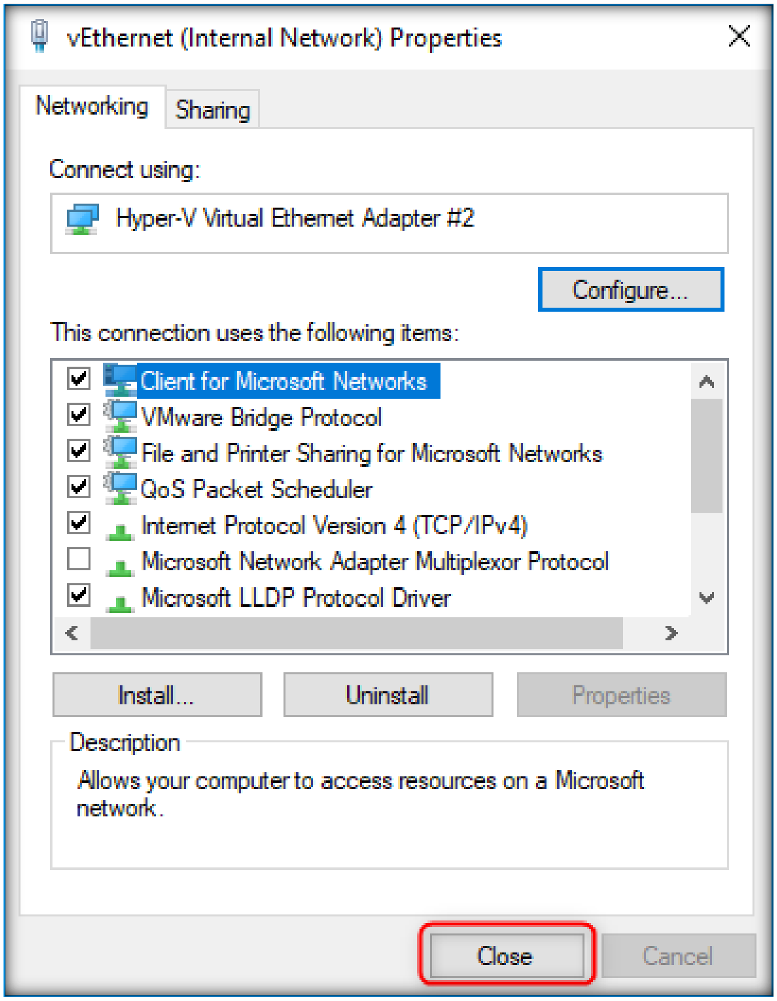
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

OK | Cancel

11. Close the **Properties** window, and other windows that were open except Hyper-V Manager.



vEthernet (Internal Network) Properties

Connect using:

Hyper-V Virtual Ethernet Adapter #2

This connection uses the following items:

☑ Client for Microsoft Networks
☑ VMware Bridge Protocol
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver

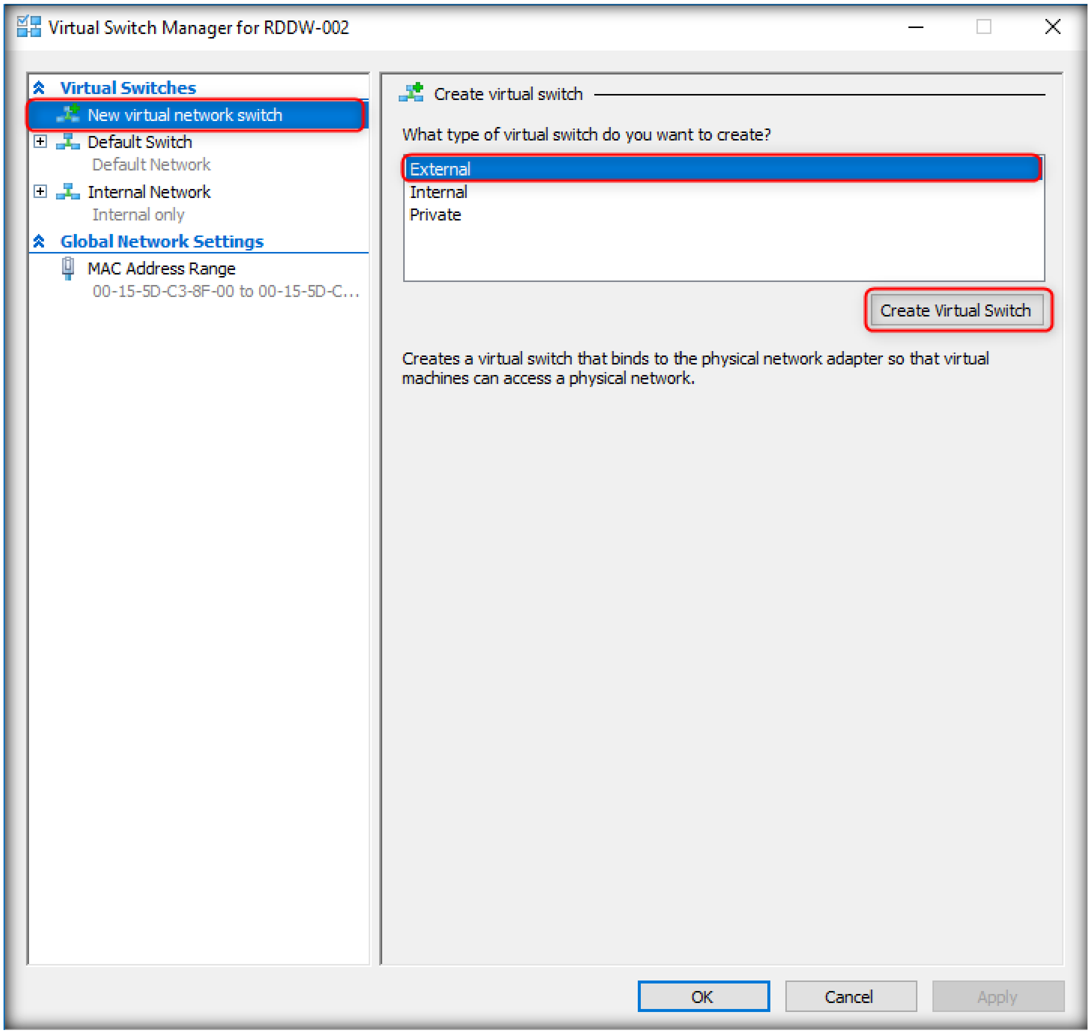
Description

Allows your computer to access resources on a Microsoft network.

CT#5.2: Configuring External Network for Hyper-V

1. Launch **Hyper-V** Manager.
2. Click **Virtual Switch Manager** in the right pane **of Hyper-V Manager**. The **Virtual Switch Manager** window appears.

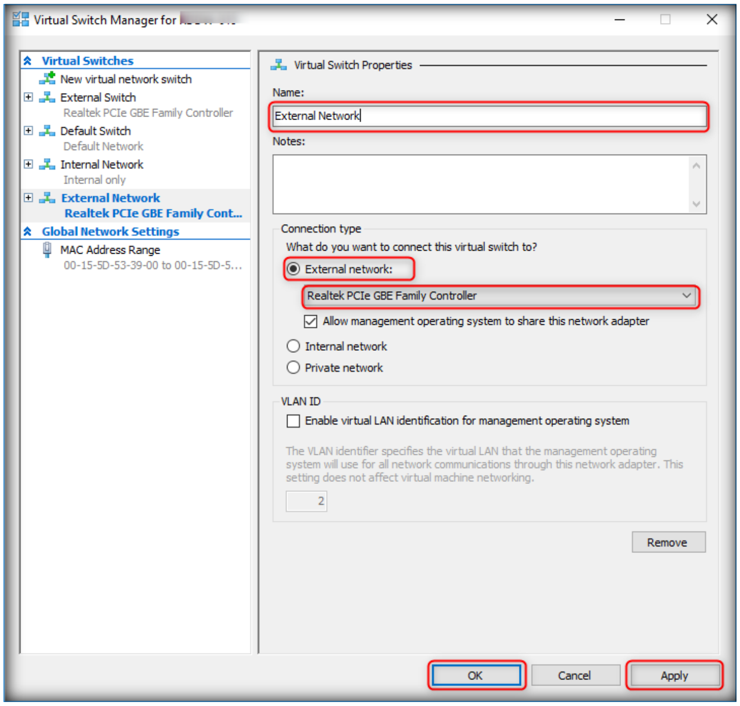
3. Select **New virtual network switch** from left pane and select **External** as the network type in the pane of the window. Click **Create Virtual Switch** button.



What type of virtual switch do you want to create?

Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.

4. The newly created virtual switch appears in the left pane. Enter the name of the virtual switch as **External Network** under the **Name** field, select **External network** radio button, click **Apply** and then click **OK**.



Virtual Switch Manager for [redacted]

Virtual Switches
New virtual network switch
External Switch
Realtek PCIe GBE Family Controller
Default Switch
Default Network
Internal Network
Internal only
External Network
Realtek PCIe GBE Family Cont...
Global Network Settings
MAC Address Range
00-15-5D-53-39-00 to 00-15-5D-5...
Virtual Switch Properties

Name: External Network

Notes:

Connection type

What do you want to connect this virtual switch to?

● External network:

Realtek PCIe GBE Family Controller

☑ Allow management operating system to share this network adapter

○ Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

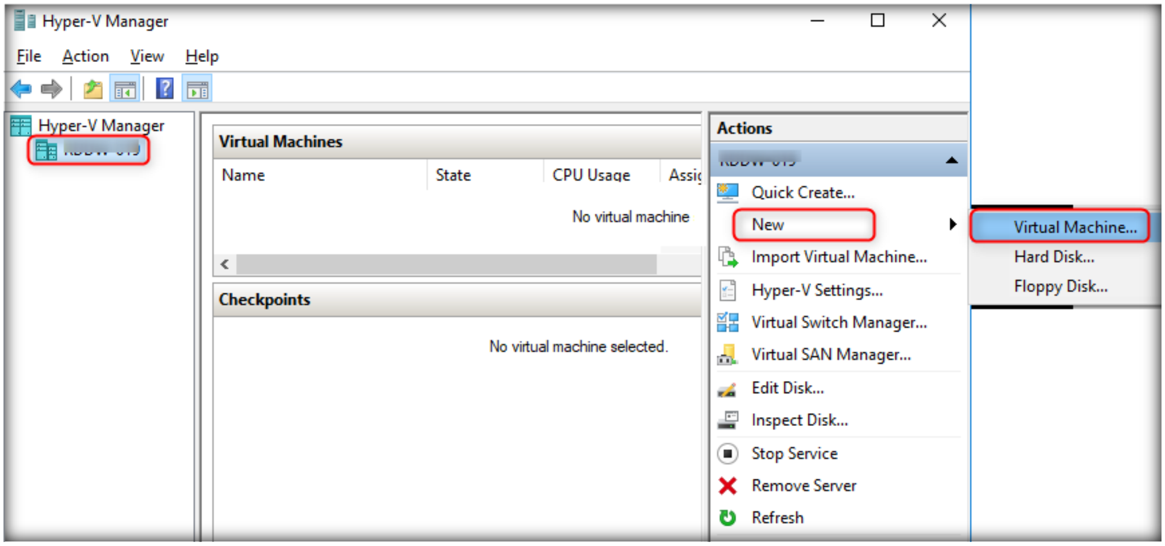
2

CT#6: Creating and Configuring Windows Server 2016 Virtual Machine

CT#6.1: Creating a Virtual Machine and Installing Windows Server 2016 Standard Guest OS

1. Launch **Hyper-V Manager**. If already launched, skip to step two.

2. Select your local machine in the left pane, then click **New** in the **Actions** pane, and then click **Virtual Machine…** in the **right pane** as shown in the screen shot.

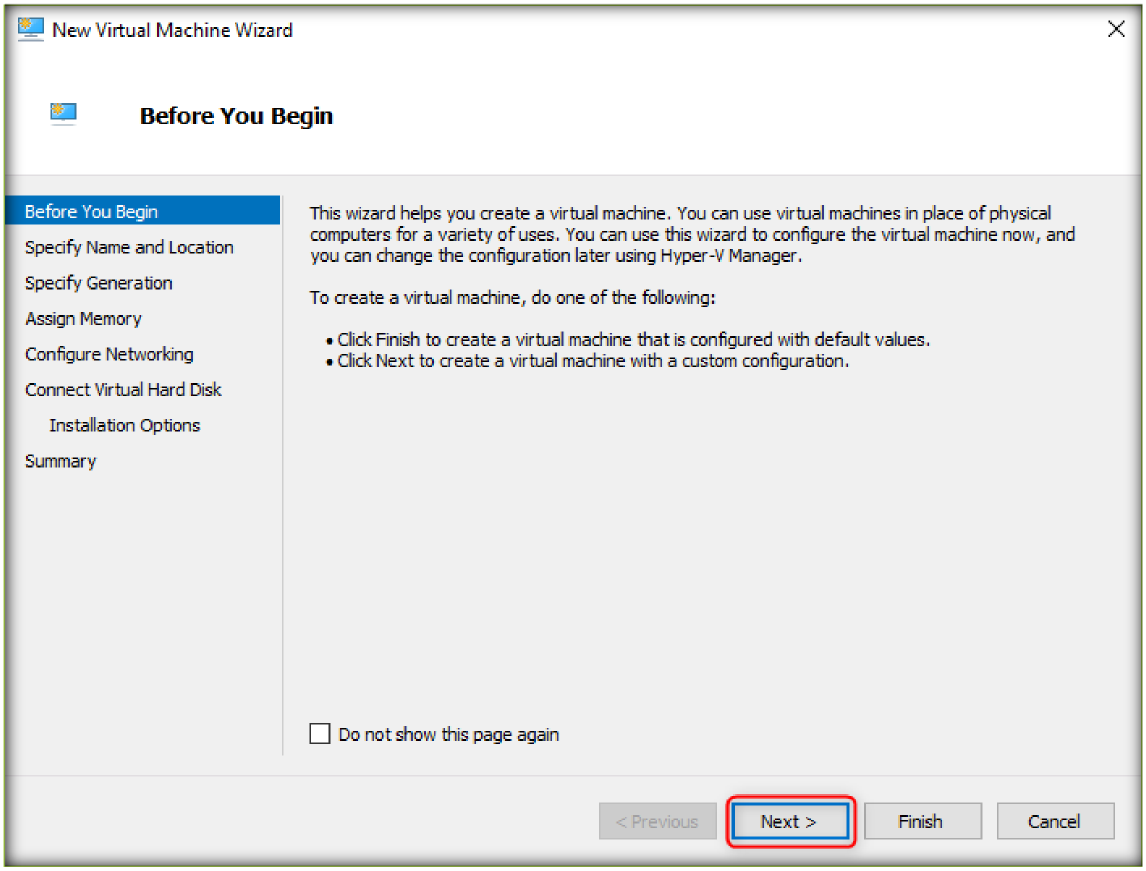


No virtual machine

No virtual machine selected.

Note: Every machine has a unique name, so the name of your machine differs from the name shown in the above screenshot.

3. **New Virtual Machine Wizard** window appears, click **Next** button.



This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

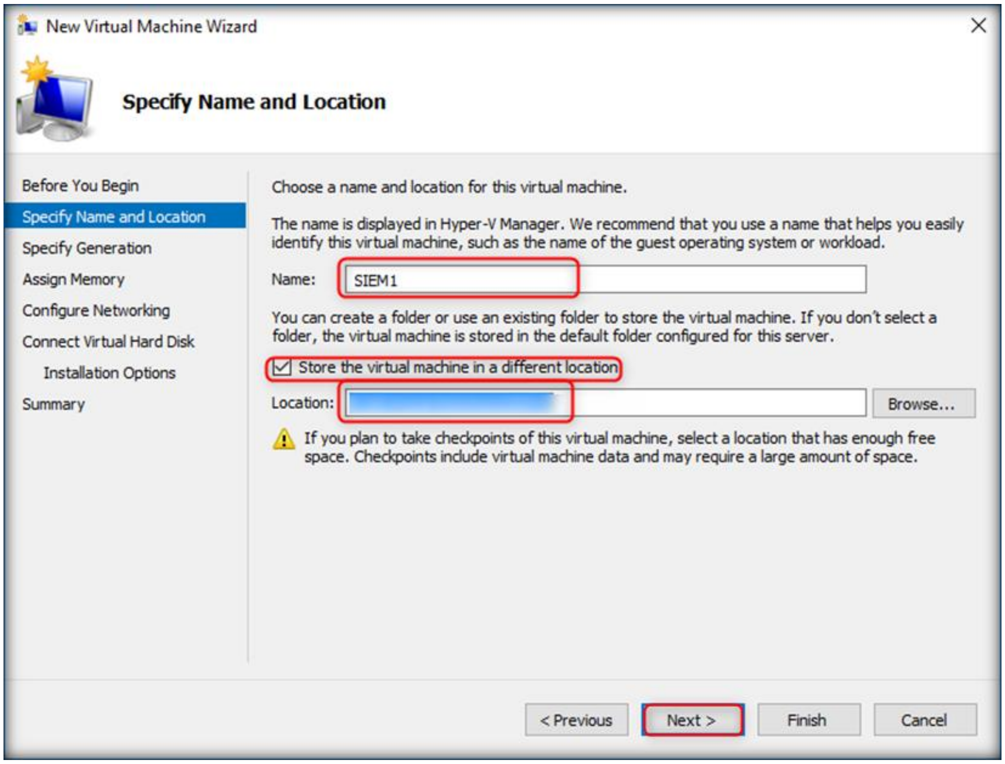
To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

☐ Do not show this page again

4. Specify **Name** and **location** of new virtual machine. Assign the name of the virtual machine as **SIEM1**.
5. The default location for storing the virtual machine is **C:\ProgramData\Microsoft\Windows\Hyper-V\.**
6. Click check box to store virtual machine in different location or set it to default location.
7. Click **Next**.

   Note: You can specify the location either in the **Specify Name and Location** section or in the forthcoming **Connect Virtual Hard Disk** section.



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: SIEM1

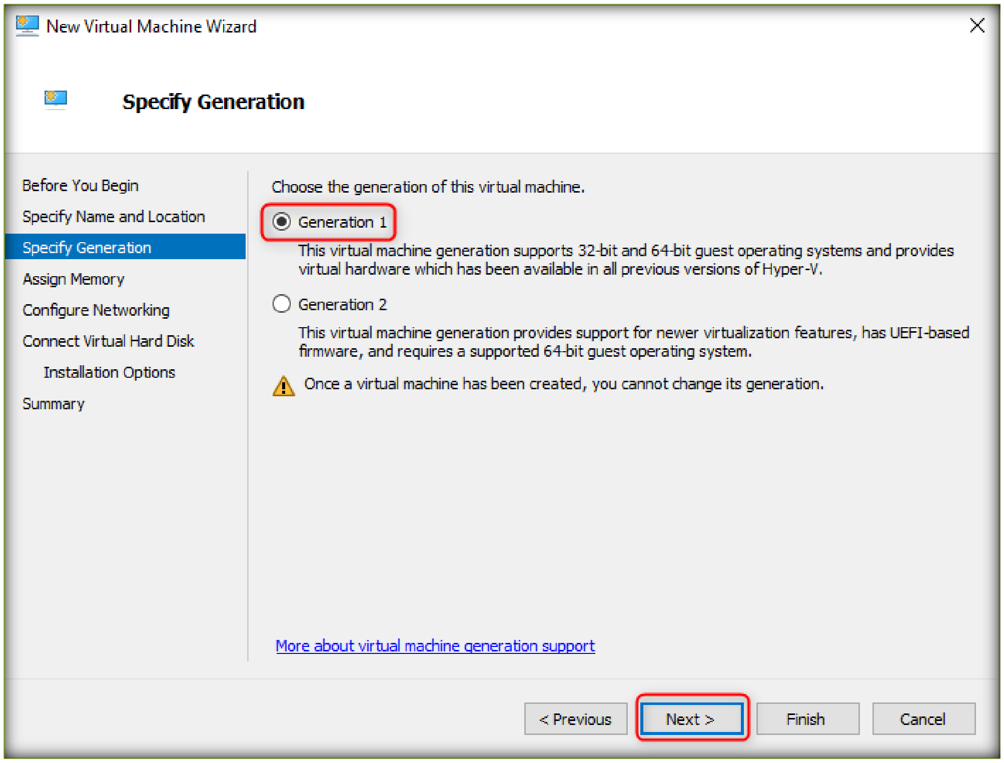
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

Location: [redacted]

⚠ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

8. Choose the generation of the virtual machine and click **Next**.


New Virtual Machine Wizard

Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

○ Generation 2

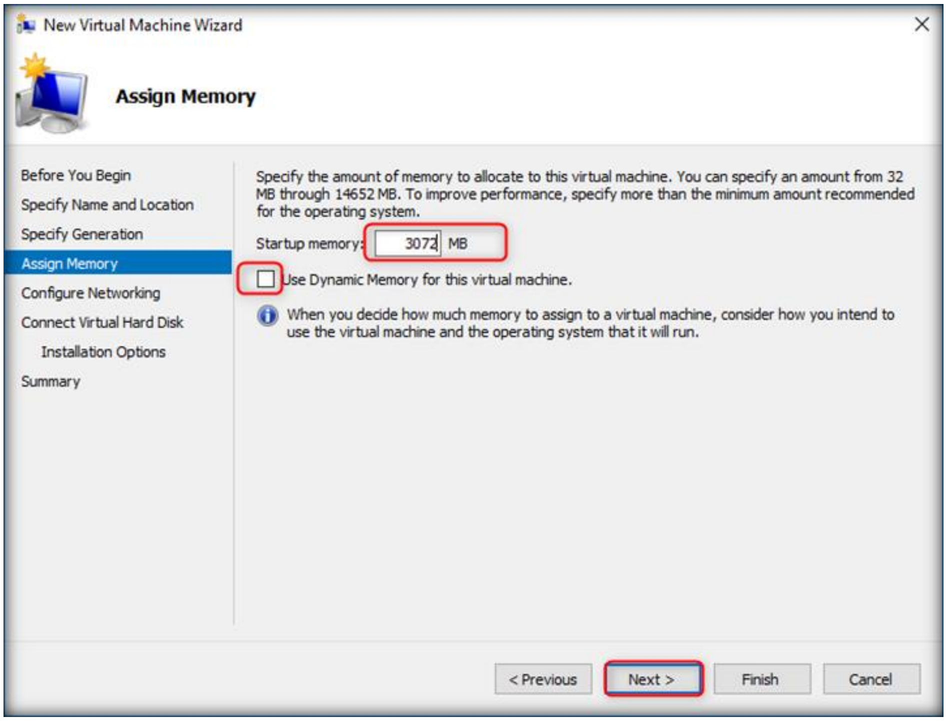
This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

Once a virtual machine has been created, you cannot change its generation.

More about virtual machine generation support

9. Assign the amount of Startup memory to allocate to this virtual machine in MB (here, 3072) and uncheck Use Dynamic memory for the virtual machine.

10. Click **Next**.


New Virtual Machine Wizard

Assign Memory

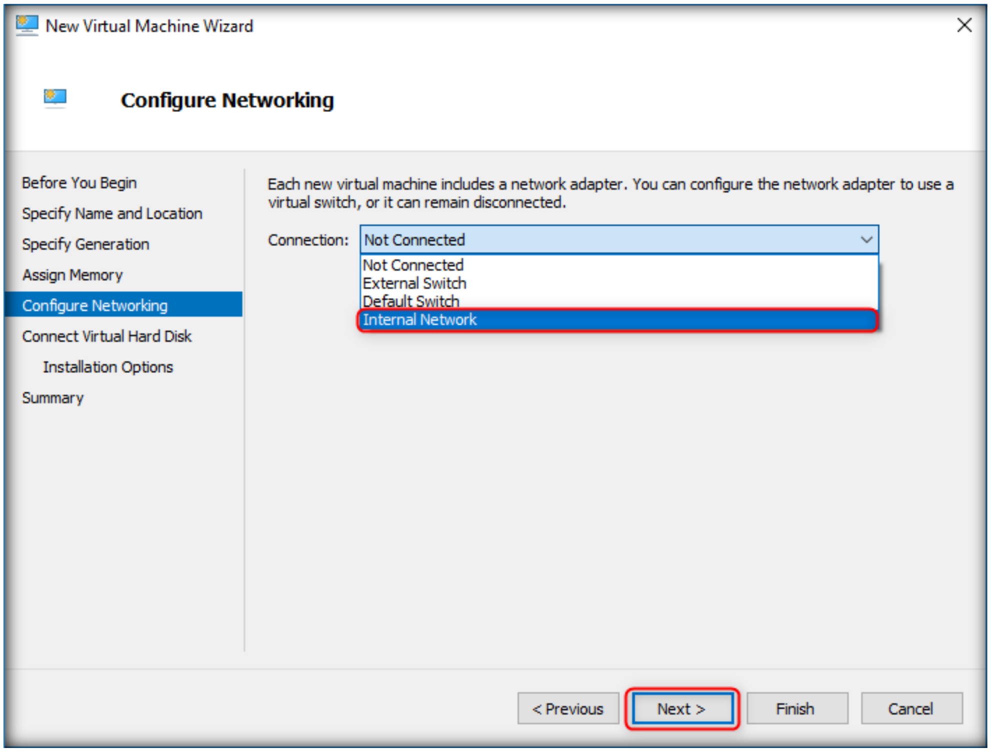
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 14652 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 3072 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

11. In the next step, Configuring Network, select **Internal Network** adaptor from **Connection** drop-down list and click **Next**.



New Virtual Machine Wizard

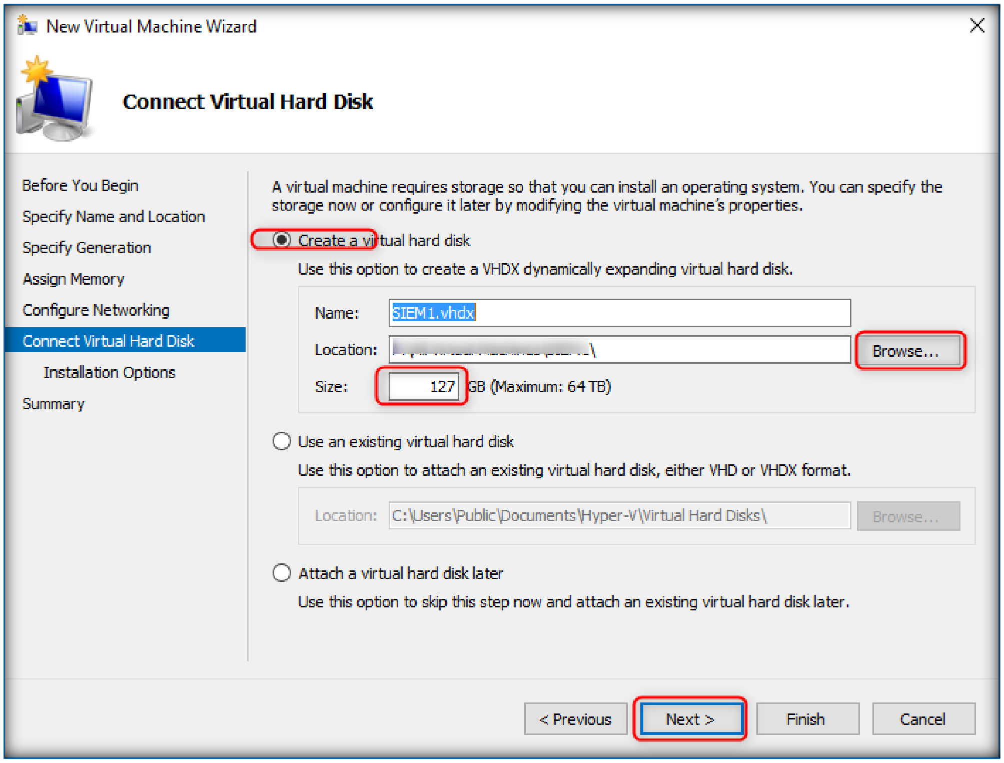
Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

- Not Connected
- External Switch
- Default Switch
- Internal Network

12. In **Connect Virtual Hard Disk** step, allocate **127 GB** default space for hard disk and click **Next**.



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: SIEM1.vhdx

Location: [redacted]

Size: 127 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

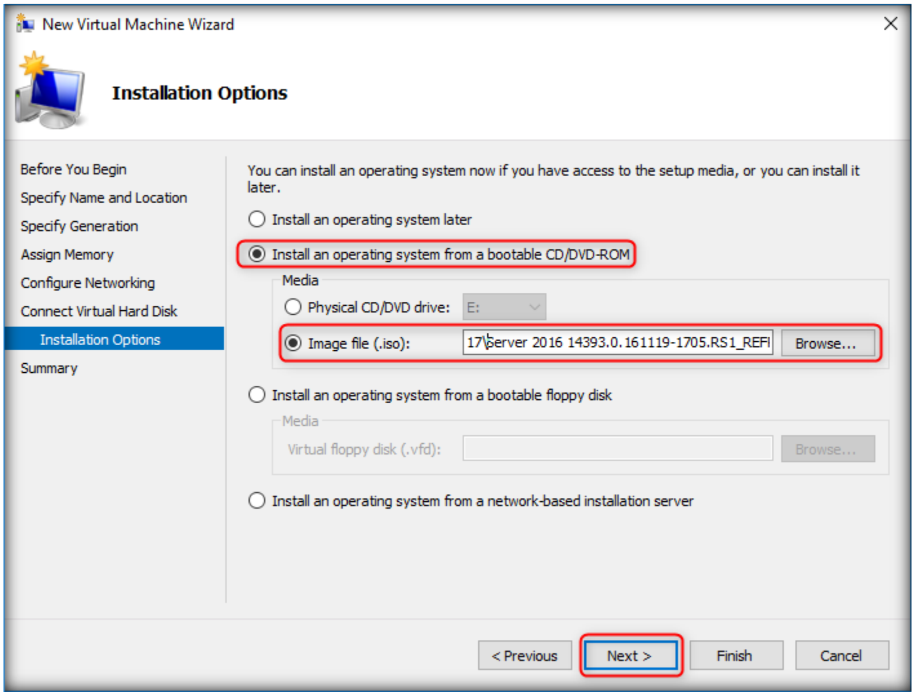
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

13. The **installation options** section appears, select **Install an operating system from a bootable CD/DVD-ROM** radio button.

    - If you have a Windows Server 2016 DVD choose Physical CD/DVD drive radio button and then click **Next**.
    - If you have a Windows Server 2016 ISO file, then choose Image file (.iso) radio button and click browse button to provide the path of ISO file and click **Next**.



Installation Options

You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a bootable CD/DVD-ROM

Media

○ Physical CD/DVD drive: E:

● Image file (.iso): 17\Server 2016 14393.0.161119-1705.RS1_REFI

○ Install an operating system from a bootable floppy disk

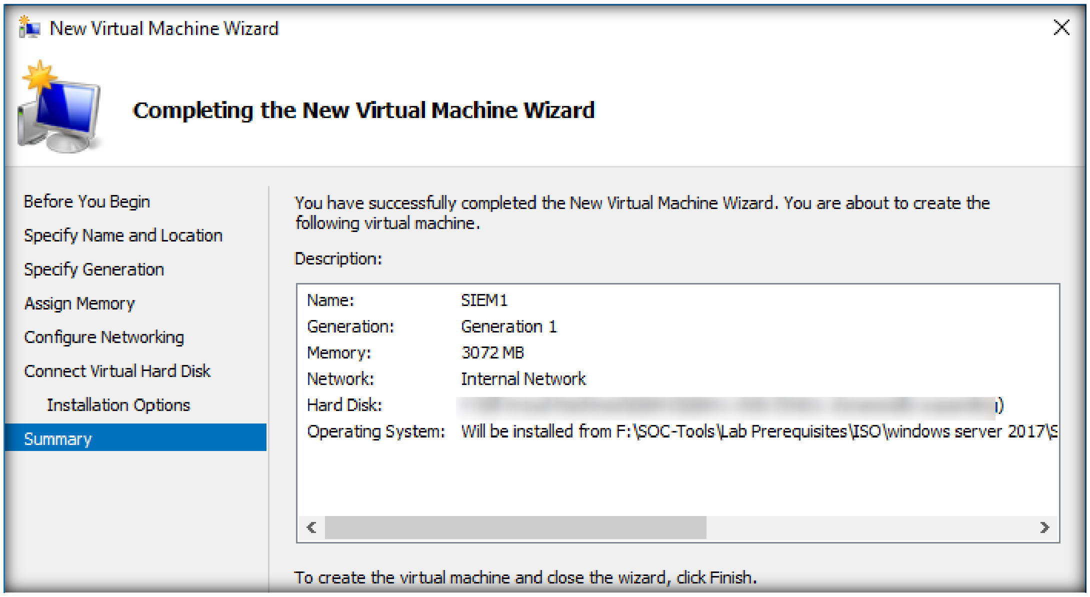
Media

Virtual floppy disk (.vfd):

○ Install an operating system from a network-based installation server

14. **New Virtual Machine** Wizard appears with summary information.

15. Click **Finish**.



Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

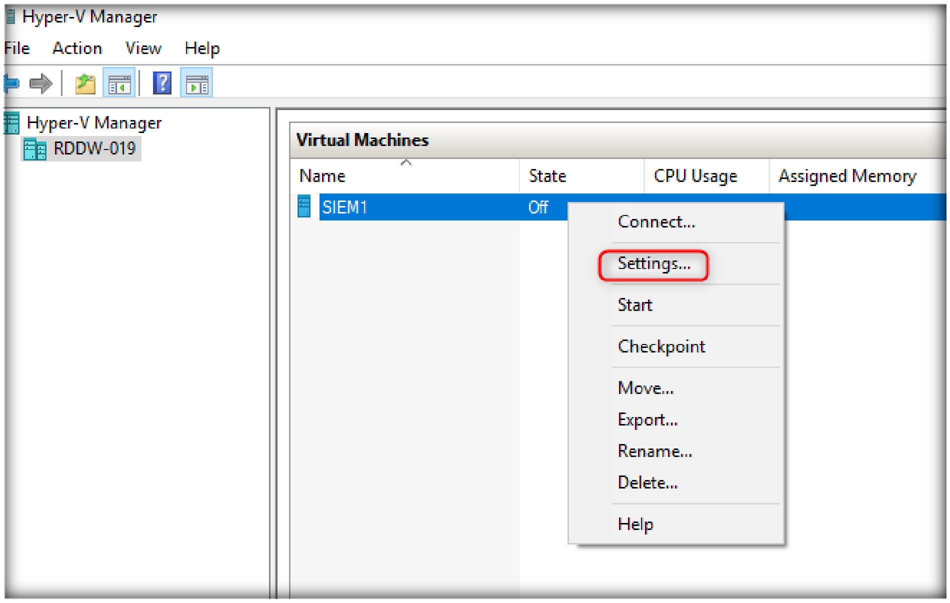
Description:

Name:	SIEM1
Generation:	Generation 1
Memory:	3072 MB
Network:	Internal Network
Hard Disk:	[redacted]
Operating System:	Will be installed from F:\SOC-Tools\Lab Prerequisites\ISO\windows server 2017\S

To create the virtual machine and close the wizard, click Finish.

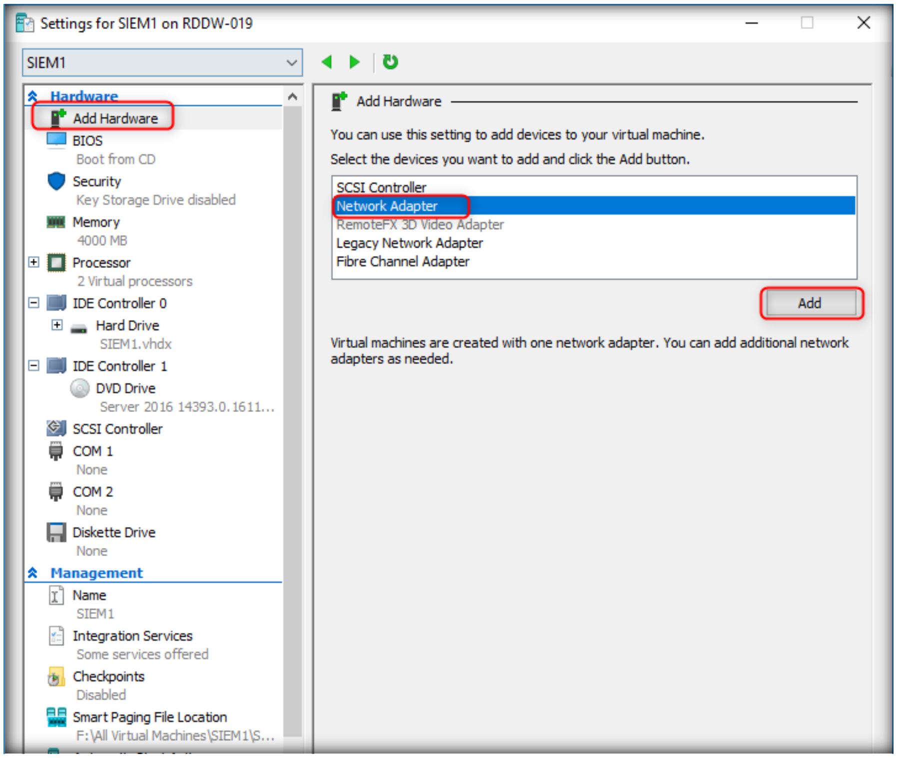
16. Hyper-V Manager creates **SIEM1** virtual machine profile.

17. In **Hyper-V Manager** main window, you see a new virtual machine named **SIEM1**. Right-click on the newly created virtual machine and click **Settings** from the context menu.



Name	State	CPU Usage	Assigned Memory
SIEM1	Off		

18. Setting for **SIEM1** window will open click on **Add Hardware** and select **Network Adapter** click **Add** button.

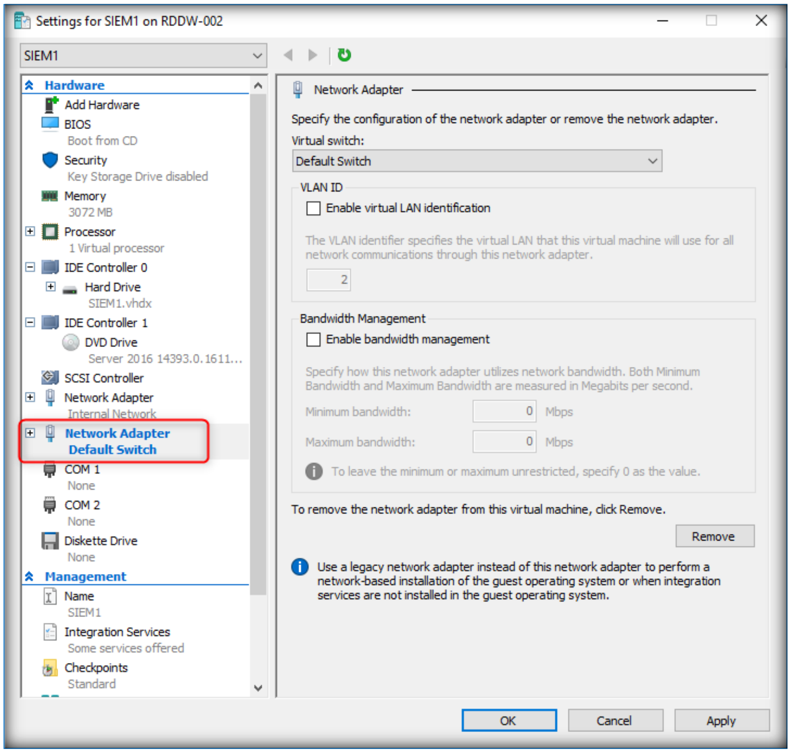


You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

Virtual machines are created with one network adapter. You can add additional network adapters as needed.

19. Select **Default Switch** from the **Virtual switch** dropdown. You will see **Network Adaptor Default Switch** added for **SIEM1**.



Settings for SIEM1 on RDDW-002

SIEM1

Hardware
- Add Hardware
- BIOS — Boot from CD
- Security — Key Storage Drive disabled
- Memory — 3072 MB
- Processor — 1 Virtual processor
- IDE Controller 0
  - Hard Drive — SIEM1.vhdx
- IDE Controller 1
  - DVD Drive — Server 2016 14393.0.1611...
- SCSI Controller
- Network Adapter — Internal Network
- **Network Adapter — Default Switch**
- COM 1 — None
- COM 2 — None
- Diskette Drive — None

Management
- Name — SIEM1
- Integration Services — Some services offered
- Checkpoints — Standard

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Default Switch

VLAN ID

□ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

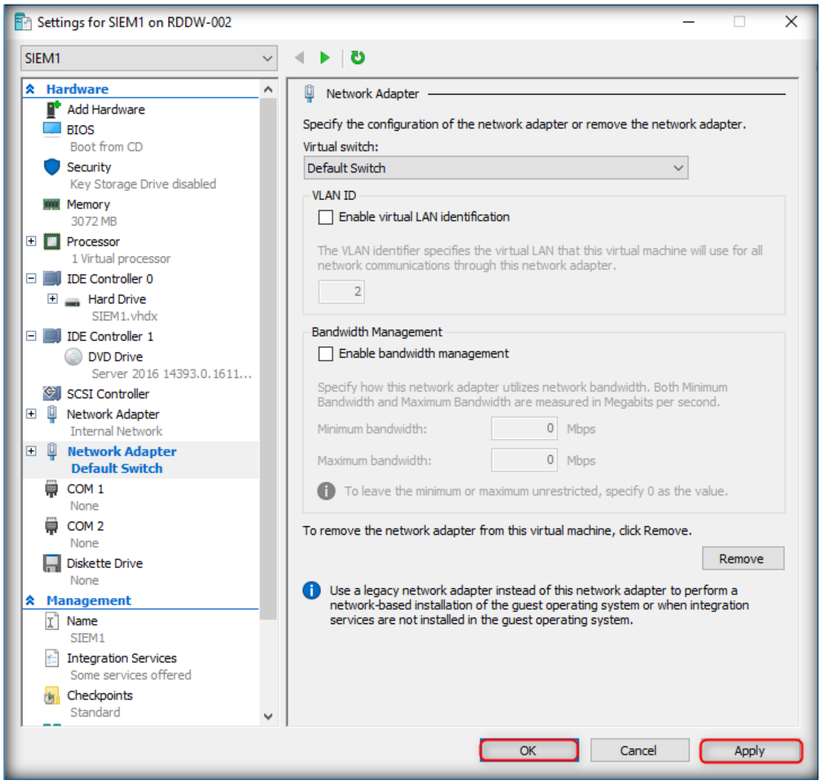
To remove the network adapter from this virtual machine, click Remove.

Remove

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

OK Cancel Apply

20. Click **Apply** and **OK**.



Settings for SIEM1 on RDDW-002

SIEM1

Hardware
- Add Hardware
- BIOS — Boot from CD
- Security — Key Storage Drive disabled
- Memory — 3072 MB
- Processor — 1 Virtual processor
- IDE Controller 0
  - Hard Drive — SIEM1.vhdx
- IDE Controller 1
  - DVD Drive — Server 2016 14393.0.1611...
- SCSI Controller
- Network Adapter — Internal Network
- **Network Adapter — Default Switch**
- COM 1 — None
- COM 2 — None
- Diskette Drive — None

Management
- Name — SIEM1
- Integration Services — Some services offered
- Checkpoints — Standard

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Default Switch

VLAN ID

□ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

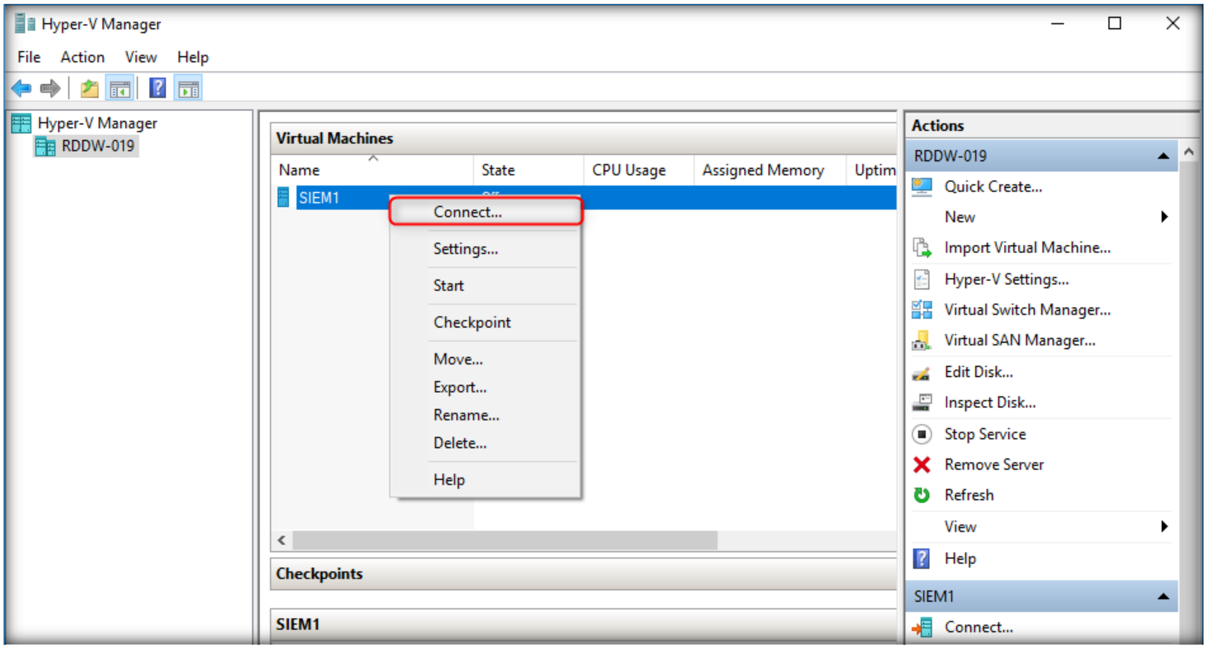
To remove the network adapter from this virtual machine, click Remove.

Remove

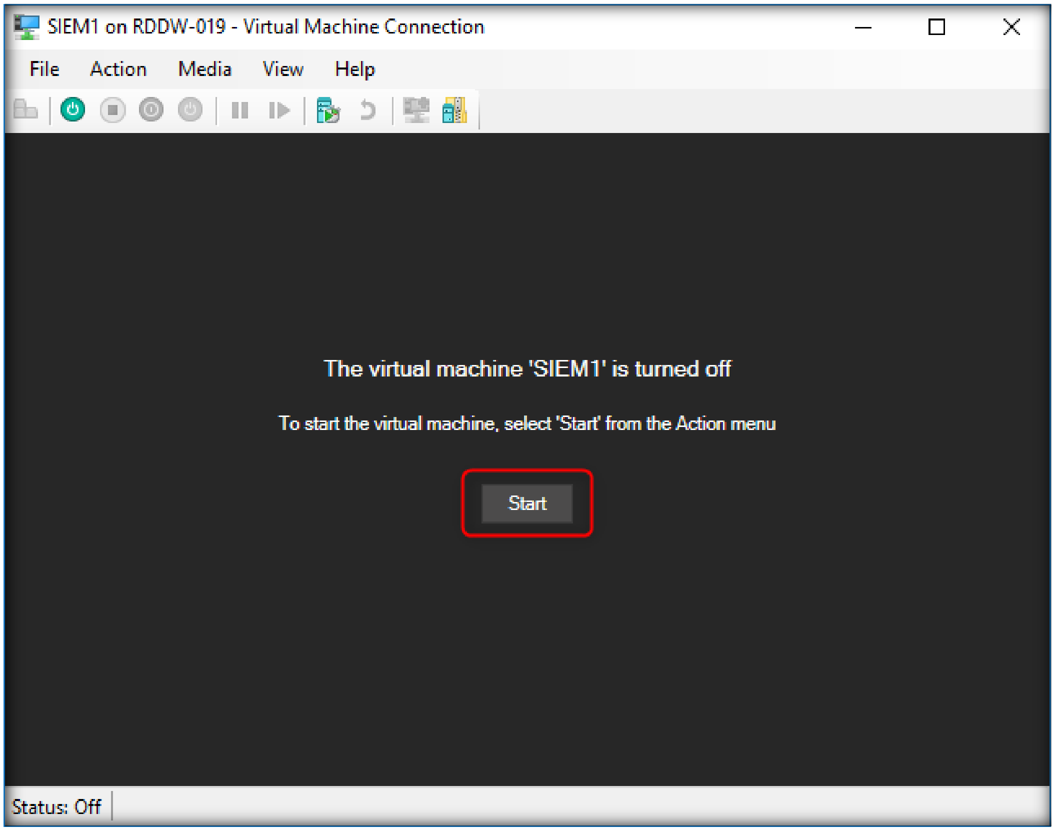
Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

OK Cancel Apply

21. In **Hyper-V Manager** main window, right-click **SIEM1** virtual machine and click **Connect** from the context menu.



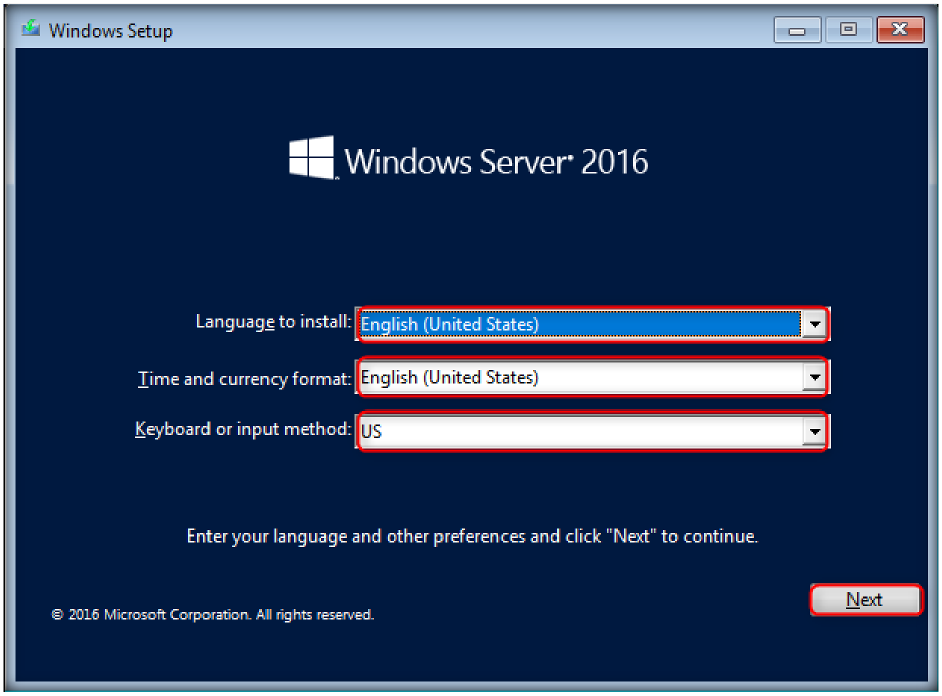
22. **SIEM1** Virtual Machine window appears click **Start** button as shown in the screenshot.


SIEM1 on RDDW-019 - Virtual Machine Connection
File Action Media View Help
Start
Status: Off

The virtual machine 'SIEM1' is turned off

To start the virtual machine, select 'Start' from the Action menu

23. When **SIEM1** virtual machine is turned on, **Windows Setup** window will appear. Fill the required details and click **Next**.



Language to install: English (United States)

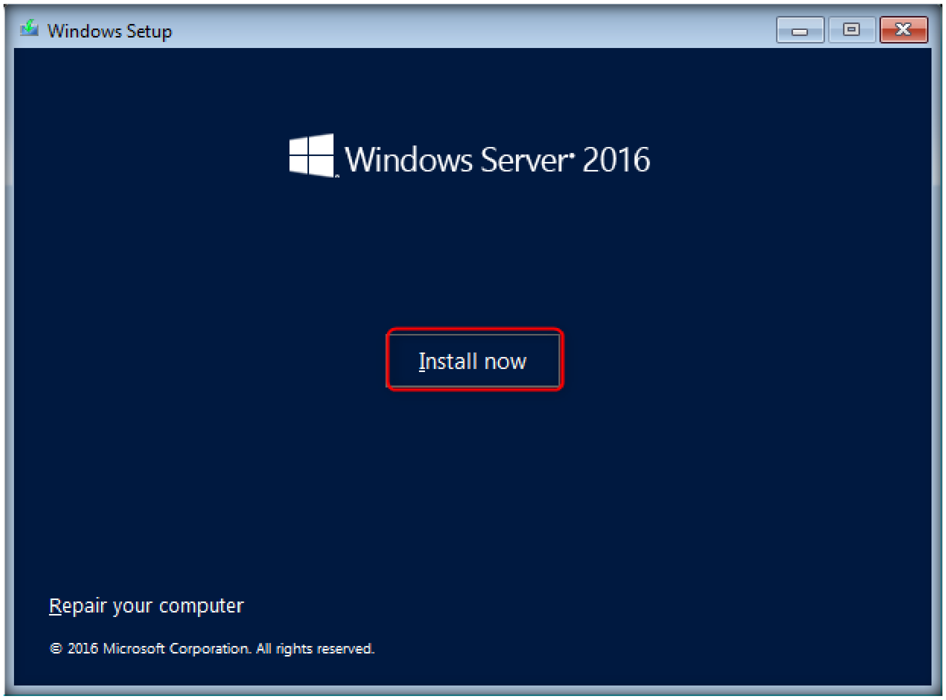
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

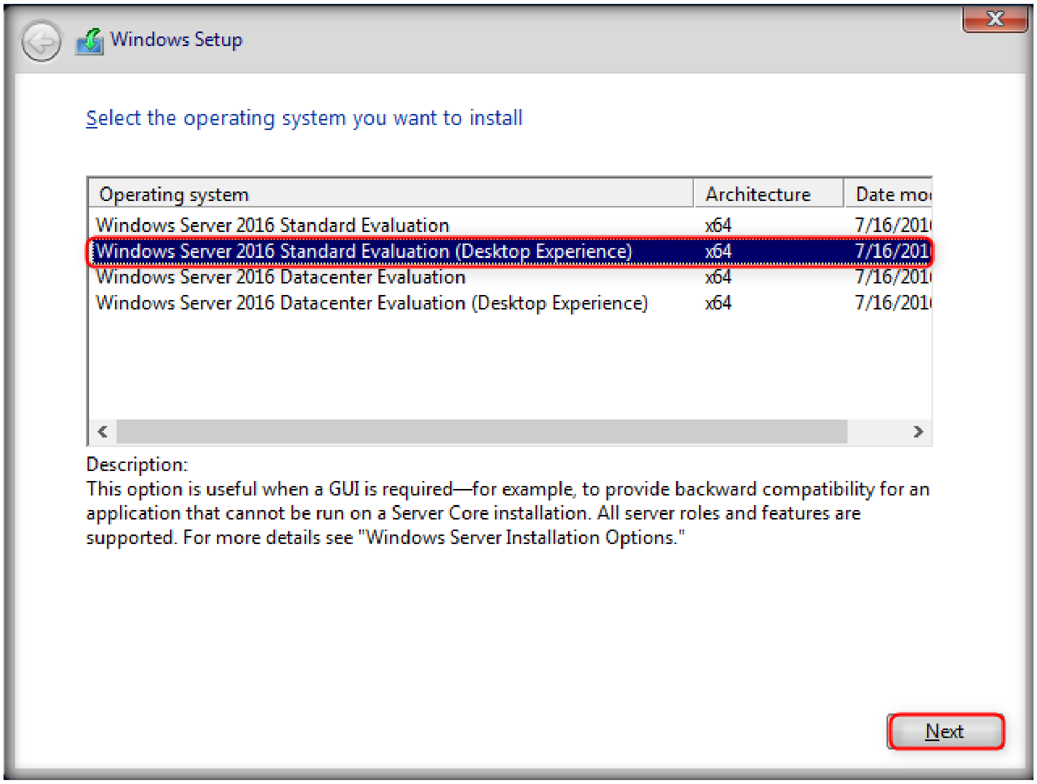
© 2016 Microsoft Corporation. All rights reserved.

24. Click **Install Now** in the Windows Setup to continue installation.



© 2016 Microsoft Corporation. All rights reserved.

25. In the **Select the operating system you want to install** select **Windows Server 2016 Standard Evaluation (Desktop Experience)** option and click **Next**.

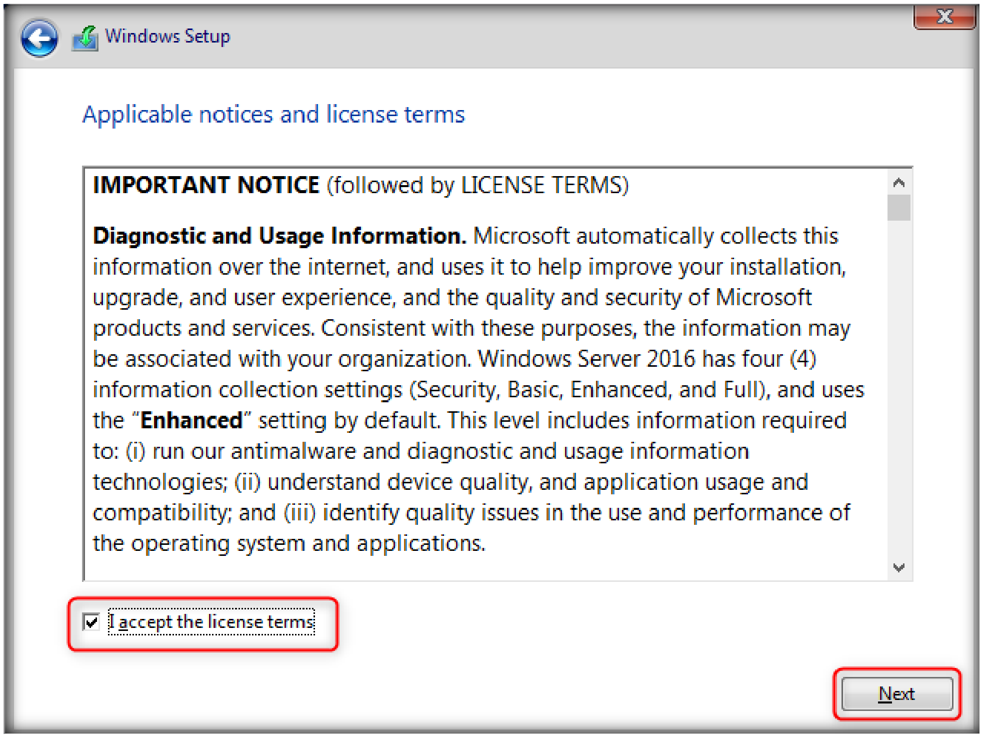


Select the operating system you want to install

Operating system	Architecture	Date mo
Windows Server 2016 Standard Evaluation	x64	7/16/201
Windows Server 2016 Standard Evaluation (Desktop Experience)	x64	7/16/201
Windows Server 2016 Datacenter Evaluation	x64	7/16/201
Windows Server 2016 Datacenter Evaluation (Desktop Experience)	x64	7/16/201

Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."

26. Check **I accept the license terms** and click **Next**.



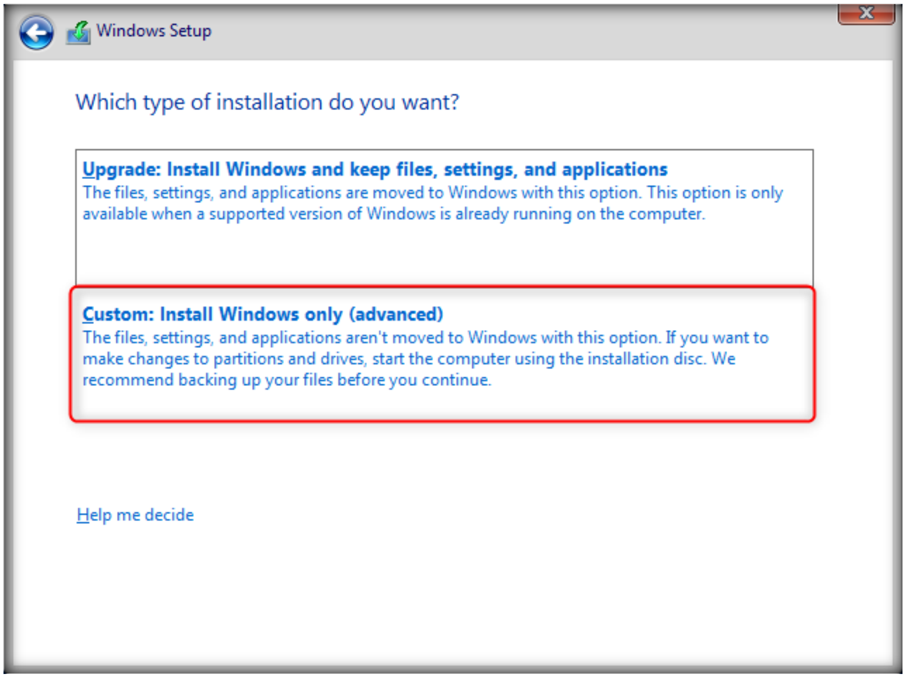
Applicable notices and license terms

IMPORTANT NOTICE (followed by LICENSE TERMS)

Diagnostic and Usage Information. Microsoft automatically collects this information over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Consistent with these purposes, the information may be associated with your organization. Windows Server 2016 has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "**Enhanced**" setting by default. This level includes information required to: (i) run our antimalware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.

☑ I accept the license terms

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

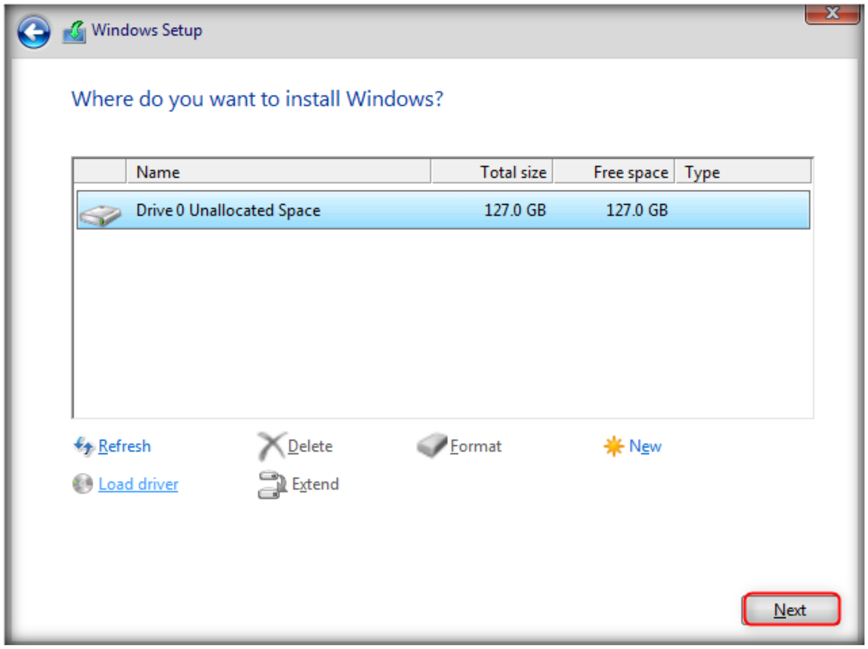


Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

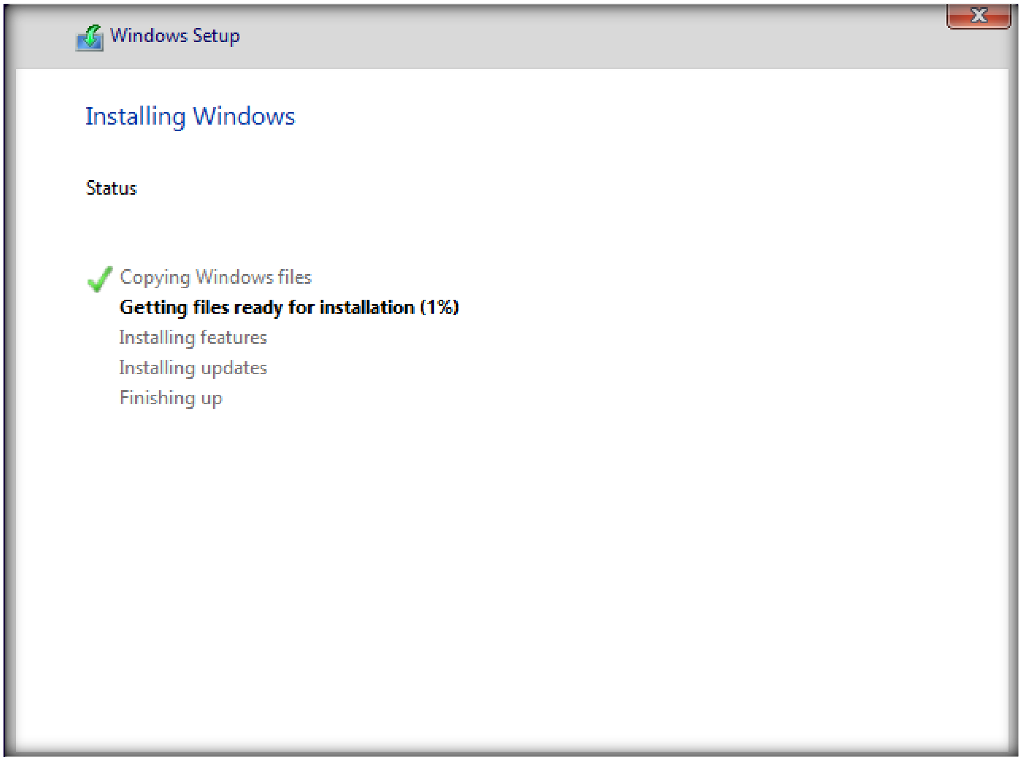
28. Click **Next**.



Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	127.0 GB	127.0 GB	

29. **Installing Windows** screen appears; wait until it completes the installation.



Windows Setup

Installing Windows

Status

✓ Copying Windows files

Getting files ready for installation (1%)

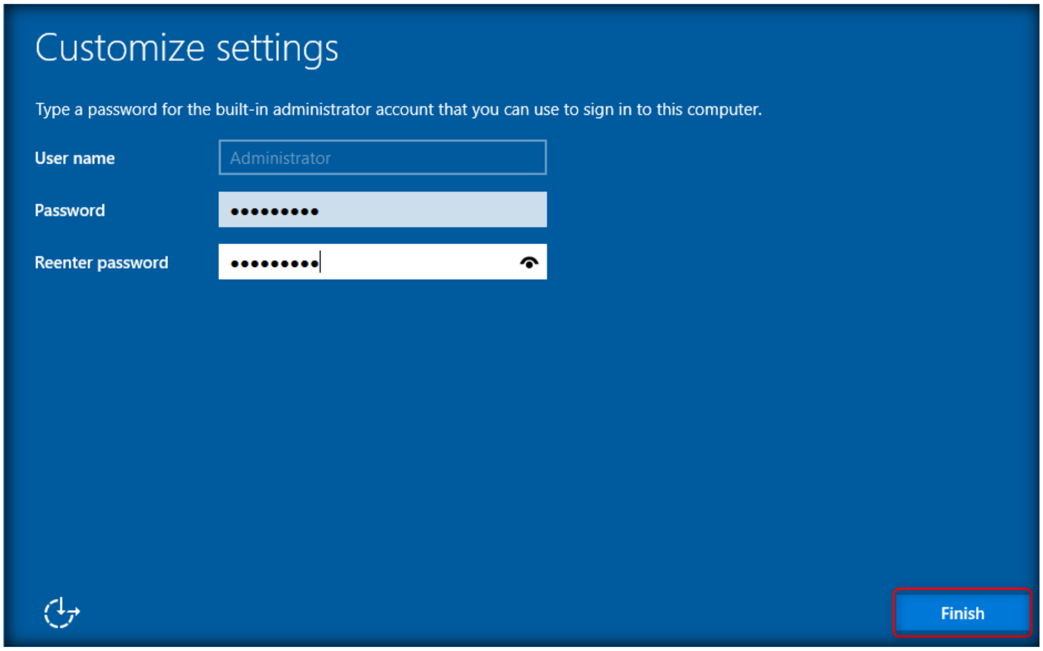
Installing features

Installing updates

Finishing up

30. Once the installation is completed machine will restart.

31. Customize settings window will appear, then enter **admin@123** as Password and Reenter password for the Administrator account and click **Finish**.



Customize settings

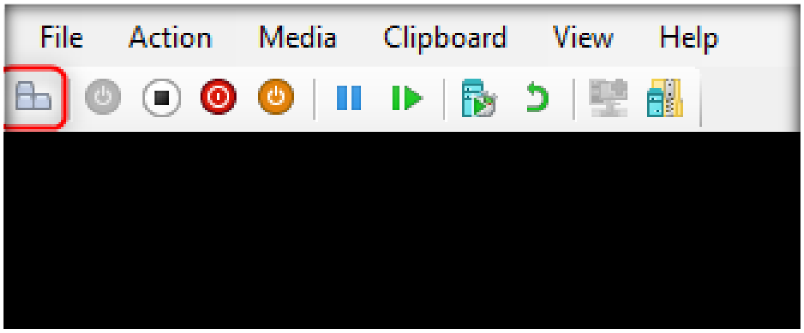
Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

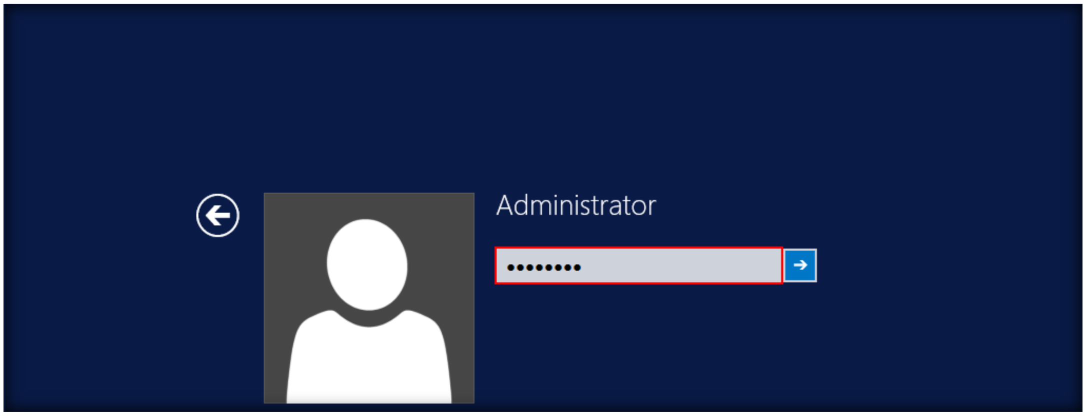
Password: •••••••••

Reenter password: •••••••••

32. Click **Ctrl+Alt+Delete** icon from the menu to login to **SIEM1**.

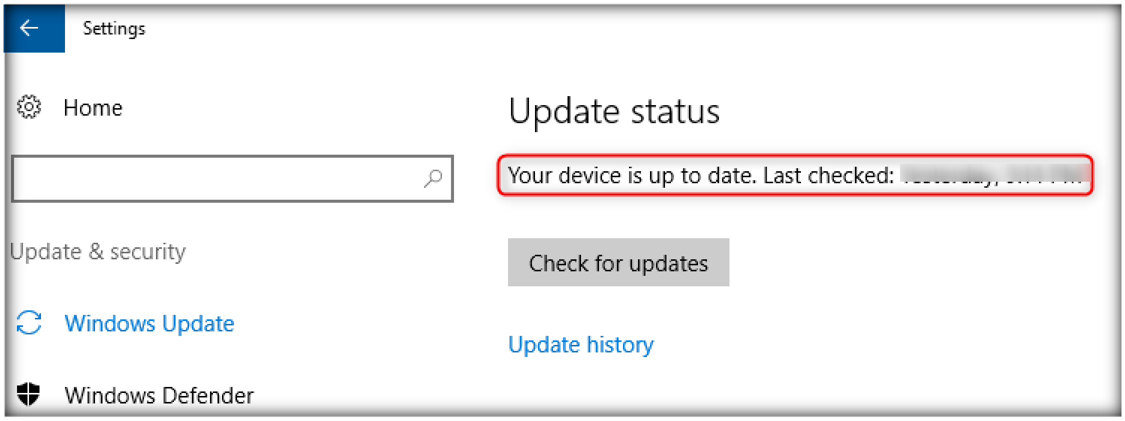


33. Login screen appears. Type the password **(admin@123)** and press **Enter**.



34. Now, check for the system updates and if found any, update the **Windows Server 2016** virtual machine to the latest.

    Note: Installing the updates might take some time.

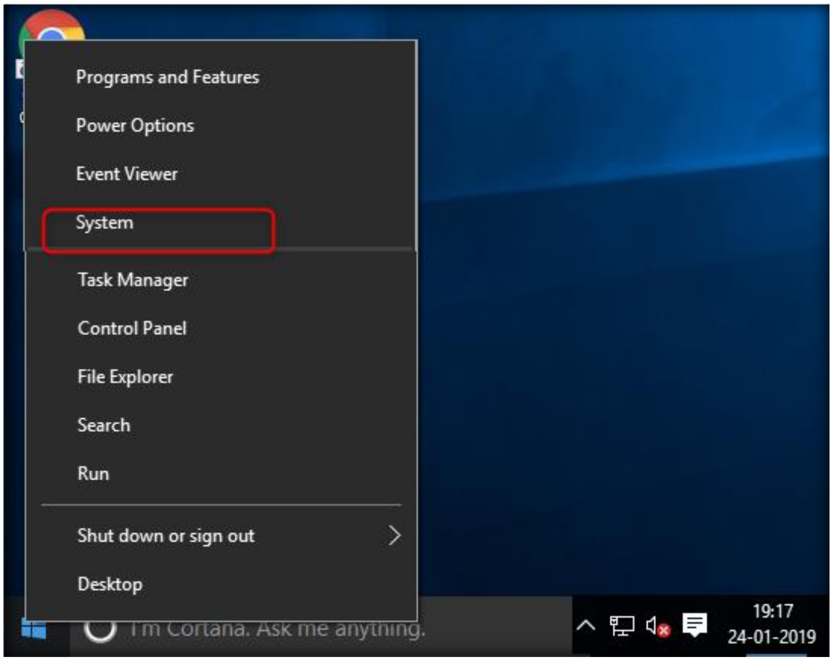


Update status

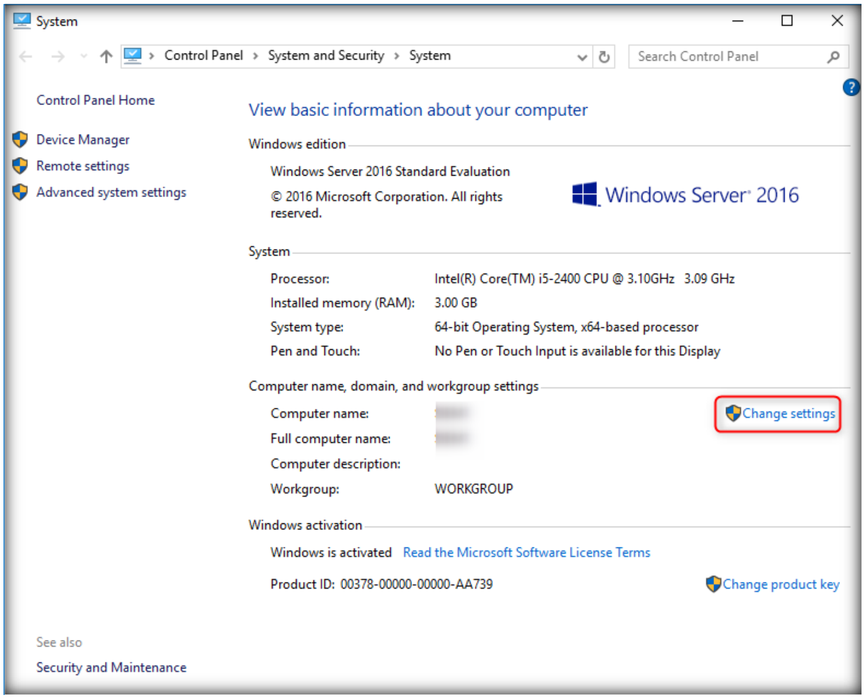
Your device is up to date. Last checked: [redacted]

CT#6.2: Changing the Computer Name

1. Close the **Server Manager** window. Right-click **Start** button and click on **System**.



2. In the System window, click **Change settings**.



View basic information about your computer

Windows edition

Windows Server 2016 Standard Evaluation

© 2016 Microsoft Corporation. All rights reserved.

Windows Server 2016

System

Processor: Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz 3.09 GHz

Installed memory (RAM): 3.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: [redacted]

Full computer name: [redacted]

Computer description:

Workgroup: WORKGROUP

Change settings

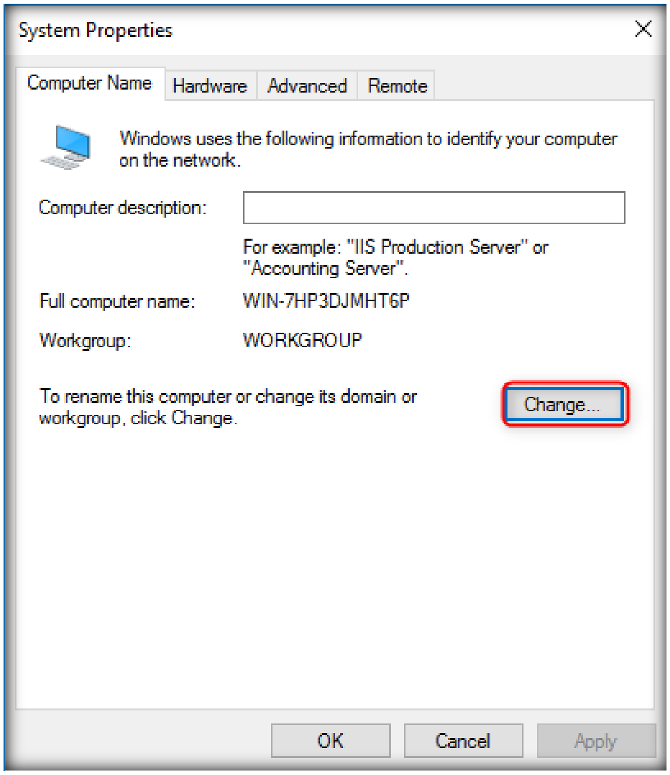
Windows activation

Windows is activated Read the Microsoft Software License Terms

Product ID: 00378-00000-00000-AA739

Change product key

3. In the **Computer Name** tab of the System Properties window, click **Change.**



Windows uses the following information to identify your computer on the network.

Computer description:

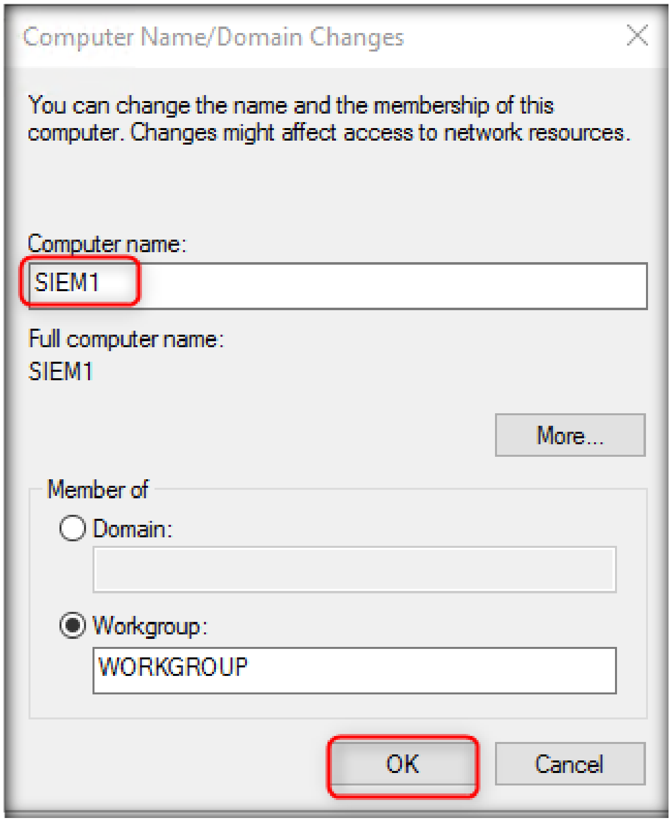
For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-7HP3DJMHT6P

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

4. Type **SIEM1** in the **Computer name** field and click **OK**.



You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: SIEM1

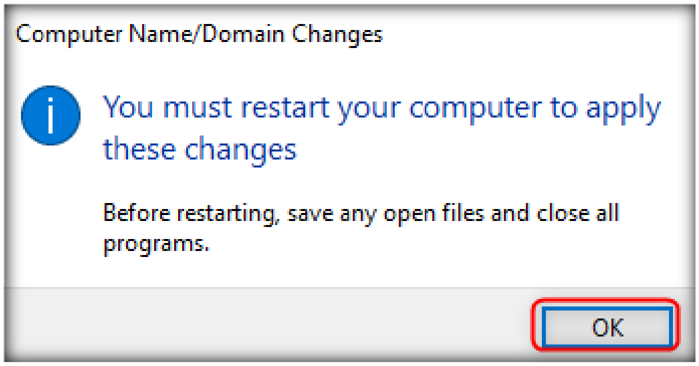
Full computer name: SIEM1

Member of

○ Domain:

● Workgroup: WORKGROUP

5. Alert will be prompted to restart the system, click **OK.**

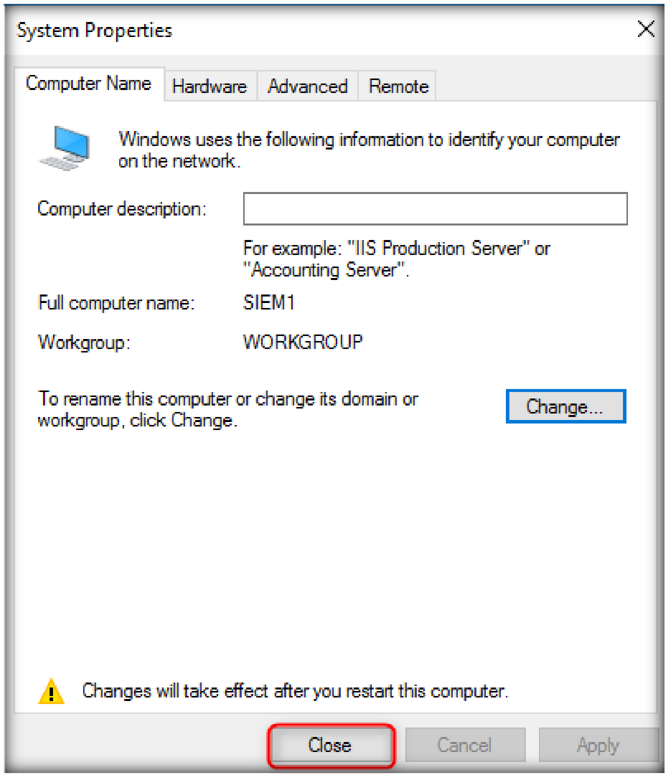


Computer Name/Domain Changes

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

6. You will be return back to System Properties window, click **Close**.



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

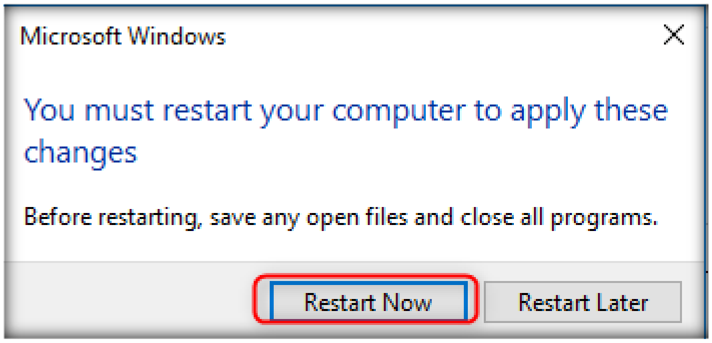
Full computer name: SIEM1

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

Changes will take effect after you restart this computer.

7. You will be prompted to restart the system, click **Restart Now**.



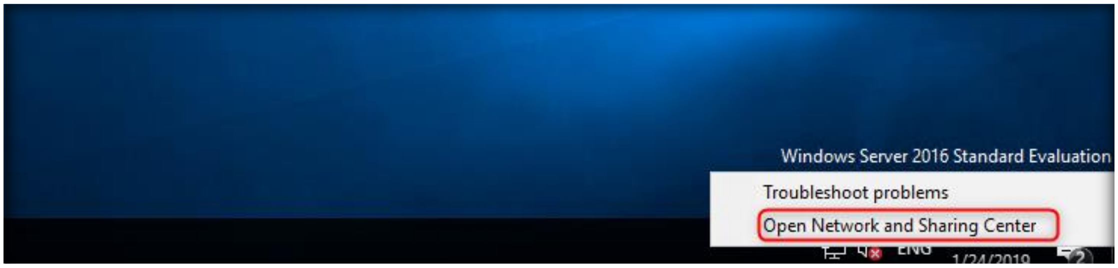
Microsoft Windows

You must restart your computer to apply these changes

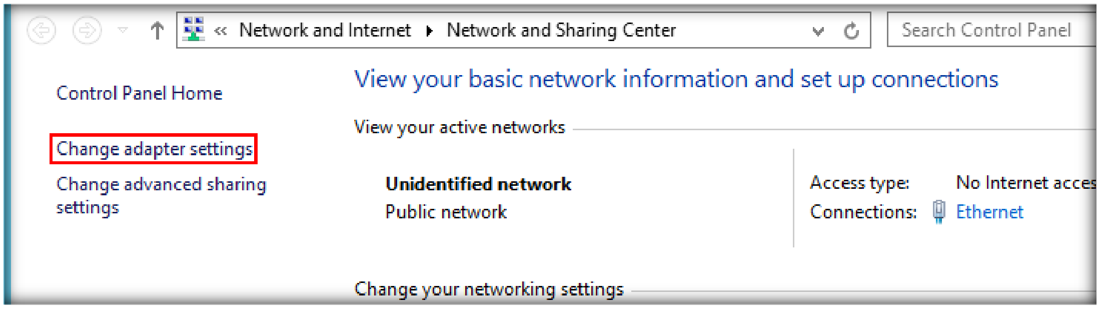
Before restarting, save any open files and close all programs.

CT#6.3: Configuring Static IP Address

1. Login as Administrator. Close the **Server Manager** window that opens after successful sign in, right-click on **Network** icon (lower right corner of the desktop) and click **Open Network and Sharing Center** from the context menu.

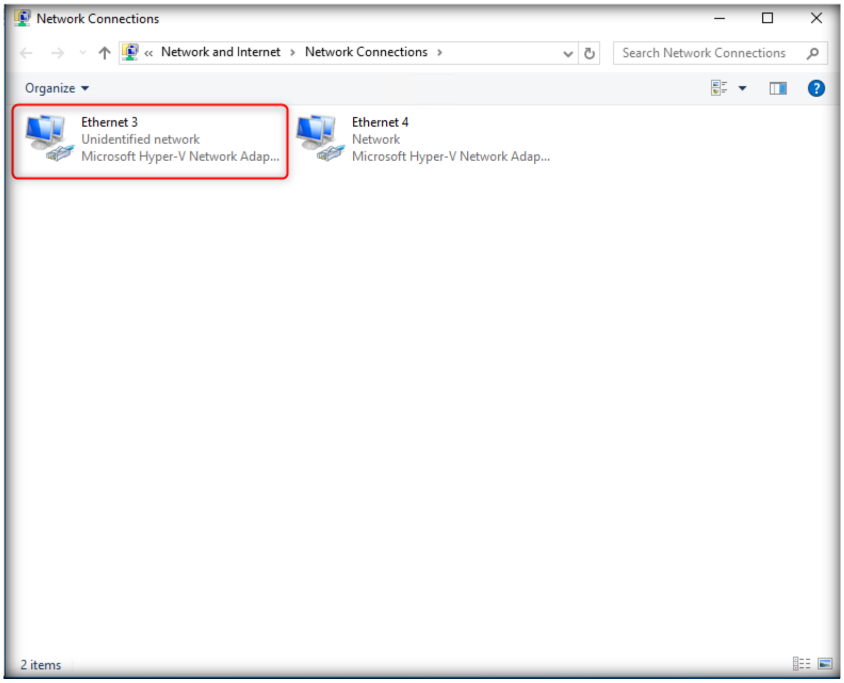

Windows Server 2016 Standard Evaluation
Troubleshoot problems
Open Network and Sharing Center
ENG
1/24/2019

2. Network and Sharing Center window appear, click **Change adapter settings** link from the left pane.

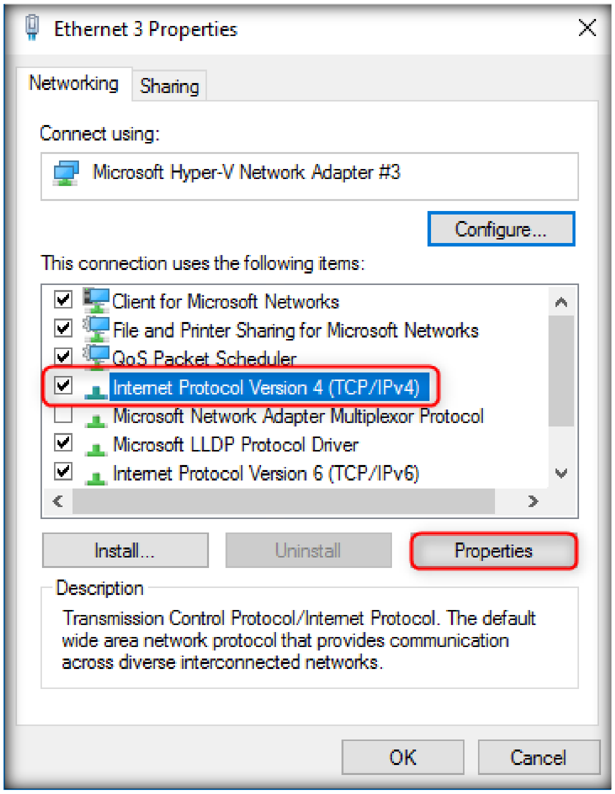

« Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Unidentified network
Public network
Access type: No Internet acces
Connections: Ethernet
Change your networking settings

3. In the Network Connections window, right-click on Unidentified network (**Ethernet** 3) adapter and click **Properties** from the context menu.

Note: The Name of Unidentified network may vary.


Network Connections
« Network and Internet › Network Connections ›
Search Network Connections
Organize ▾
Ethernet 3
Unidentified network
Microsoft Hyper-V Network Adap...
Ethernet 4
Network
Microsoft Hyper-V Network Adap...
2 items

4. Ethernet adapter Properties window appears; and select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



Ethernet 3 Properties

Networking | Sharing

Connect using:

Microsoft Hyper-V Network Adapter #3

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

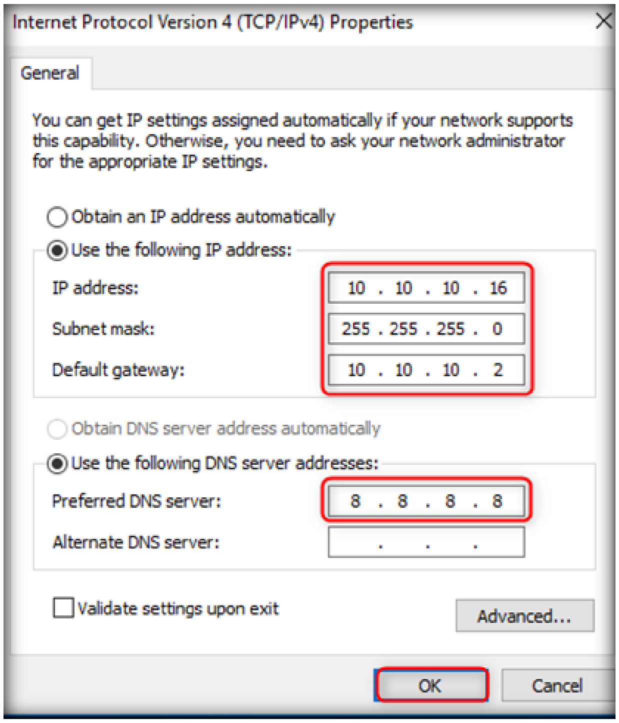
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select **Use the following IP address** and **Use the following DNS server addresses** radio buttons, and type the following values as shown in the screenshot and click **OK**.

   - IP address: **10.10.10.16**
   - Subnet mask: **255.255.255.0**
   - Default gateway: **10.10.10.2**
   - Preferred DNS server: **8.8.8.8**

   Note: Once you click on **OK** button, Networks section pane appears on the right side of the desktop screen, then click **Yes**.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 16

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 10 . 10 . 2

○ Obtain DNS server address automatically

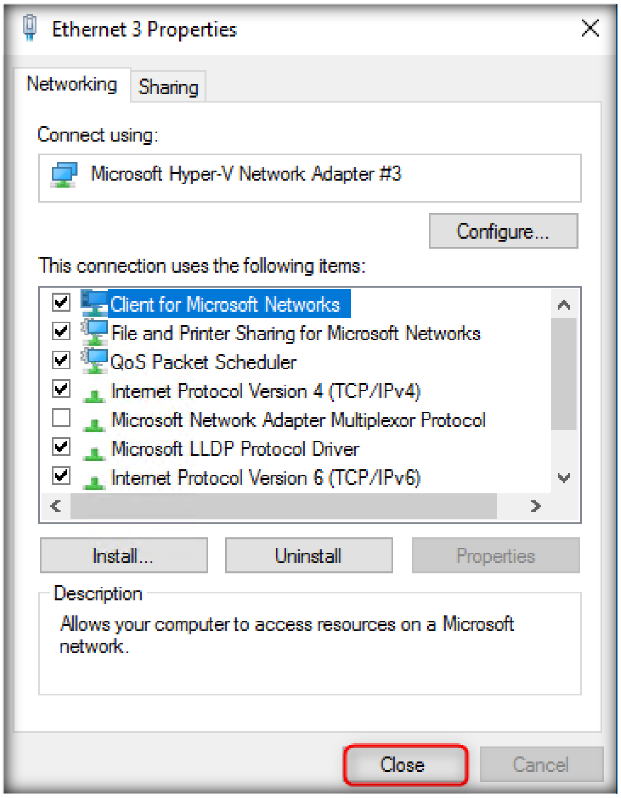
● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: . . .

□ Validate settings upon exit

6. Click **Close** to close the Ethernet Properties window.



Ethernet 3 Properties

Networking | Sharing

Connect using:

Microsoft Hyper-V Network Adapter #3

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Install... | Uninstall | Properties

Description

Allows your computer to access resources on a Microsoft network.

Close | Cancel

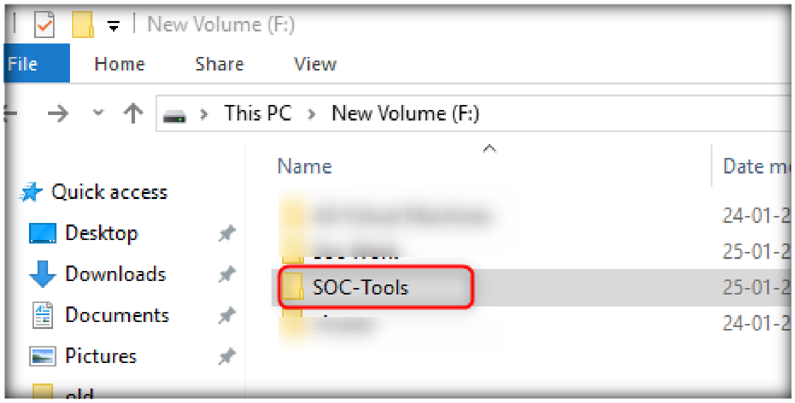
7. Now, check whether Windows Server 2016 is installed and working properly and check whether Internet is accessible.

CT#6.4: Sharing SOC-Tools Folder from Host Machine and Mapping to Windows Server 2016 VM

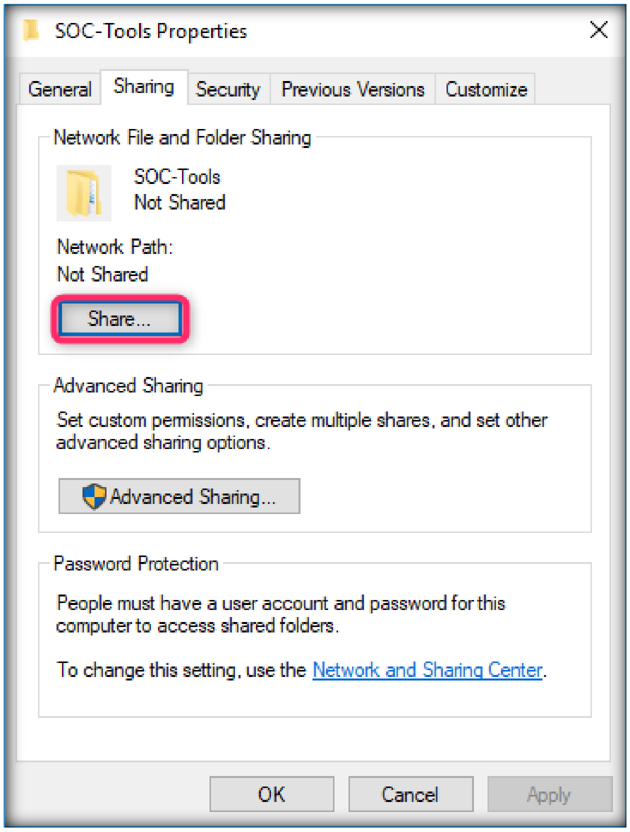
1. Navigate to **D:\** (where SOC-Tools) folder is located, in your host machine.

2. Right-click on **SOC-Tools** folder and click **Properties** from the context menu.

   Note: If you have placed **SOC-Tools** in a different drive then screenshots may differ in your lab environment.



3. **SOC-Tools** Properties window appears, click **Sharing** tab, and then click **Share** button as shown in the screenshot.



SOC-Tools Properties

General | Sharing | Security | Previous Versions | Customize

Network File and Folder Sharing

SOC-Tools
Not Shared

Network Path:
Not Shared

Share...

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

Advanced Sharing...

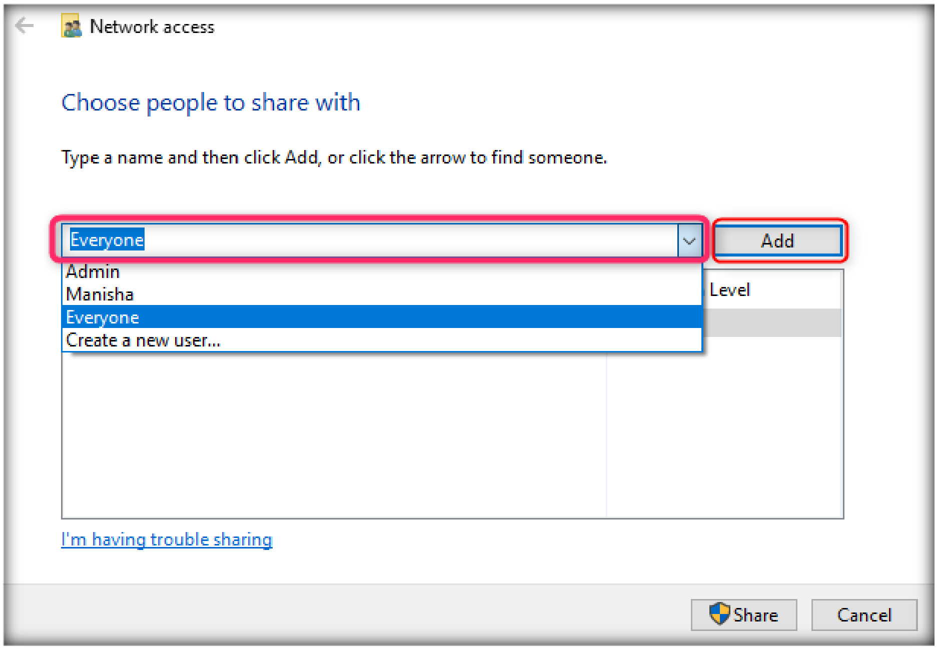
Password Protection

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.

OK | Cancel | Apply

4. File Sharing window appears, select **Everyone** from drop-down list and click **Add** in Choose people to share with wizard.



Network access

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Everyone

Add

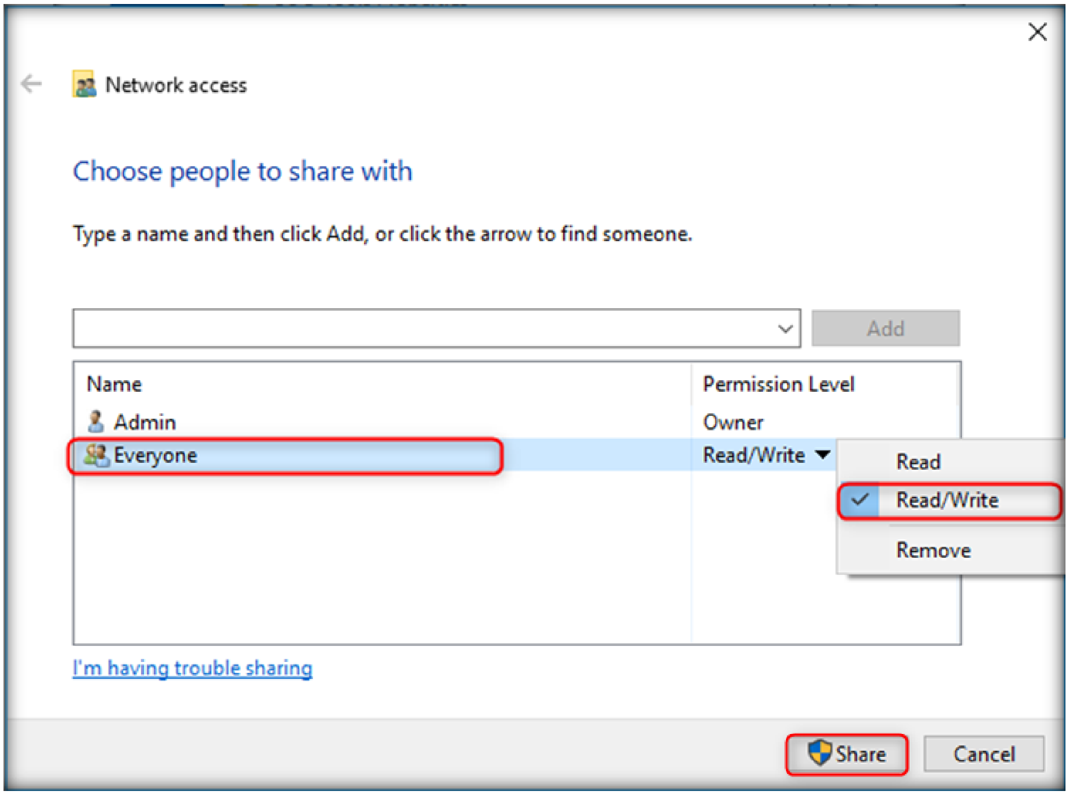
Admin
Manisha
Everyone
Create a new user...

Level

I'm having trouble sharing

Share | Cancel

5. Everyone will be added to the list. Click **Everyone** from the list and select **Read/Write** option from the dropdown menu. Click **Share** button.



Network access

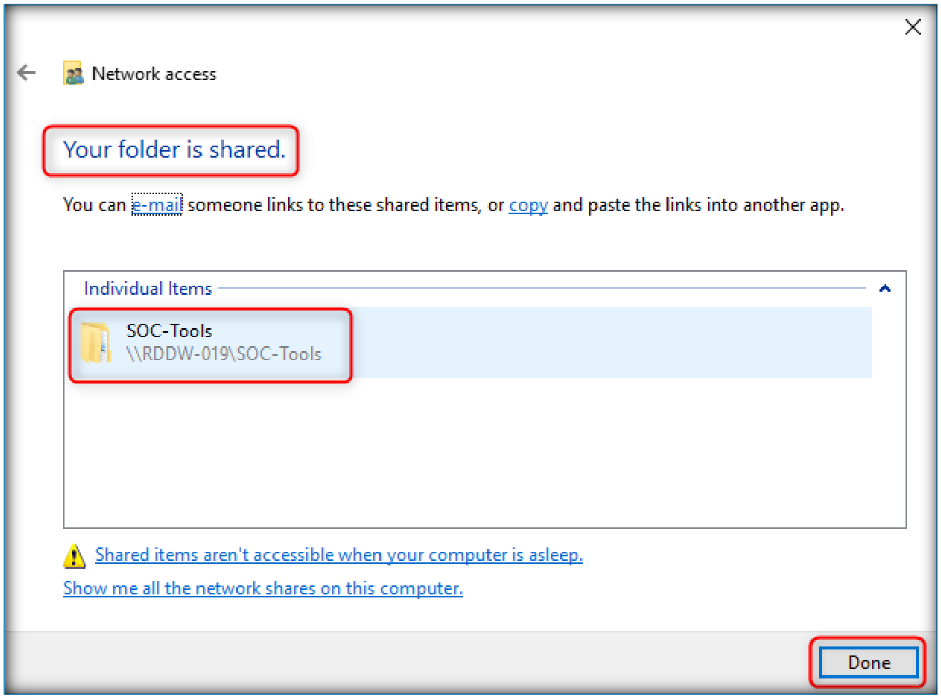
Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Admin	Owner
Everyone	Read/Write

6. Your folder is shared screen appears, click **Done** button as shown in the screenshot.

Note: Your local host machine name will differ in your lab environment.



Network access

Your folder is shared.

You can e-mail someone links to these shared items, or copy and paste the links into another app.

Individual Items

SOC-Tools
\\RDDW-019\SOC-Tools

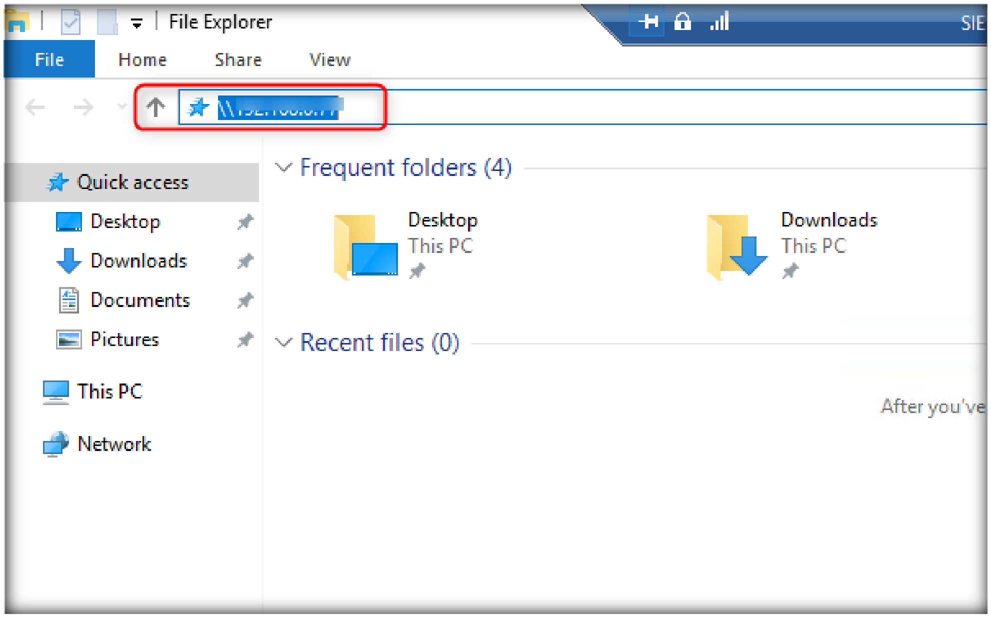
Shared items aren't accessible when your computer is asleep.

Show me all the network shares on this computer.

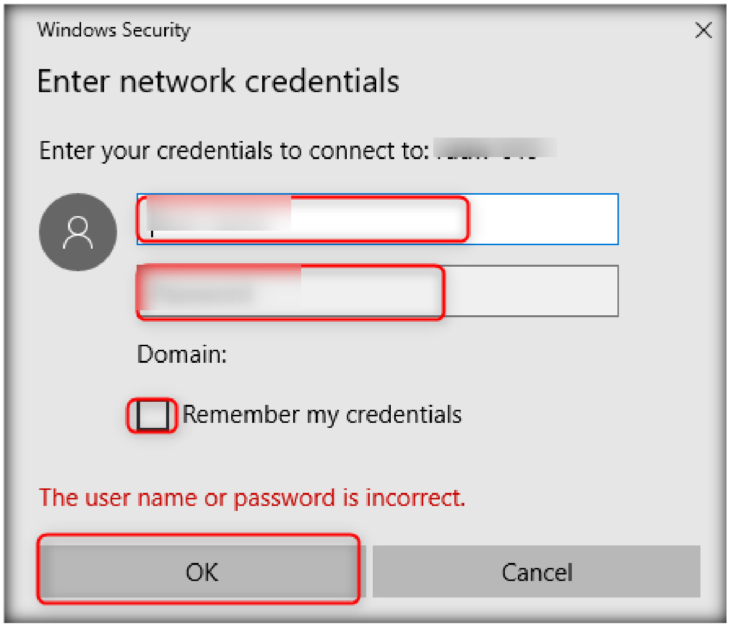
7. Close all the windows that were open in your host machine.

8. Switch to **SIEM1** virtual machine, if it is turned off then turn on the machine, and login with the administrator credentials (username: Administrator and Password: admin@123). Once logged in, close the **Server Manager** window.

9. Open File Explorer, and type **[IP Address OR Host Name of your host machine]** in the address bar and press **Enter**.



10. Windows Security pop-up will appear, type your Host machine credentials, check the **Remember my credentials** check box and click **OK**.



Windows Security

Enter network credentials

Enter your credentials to connect to: [redacted]

[redacted]

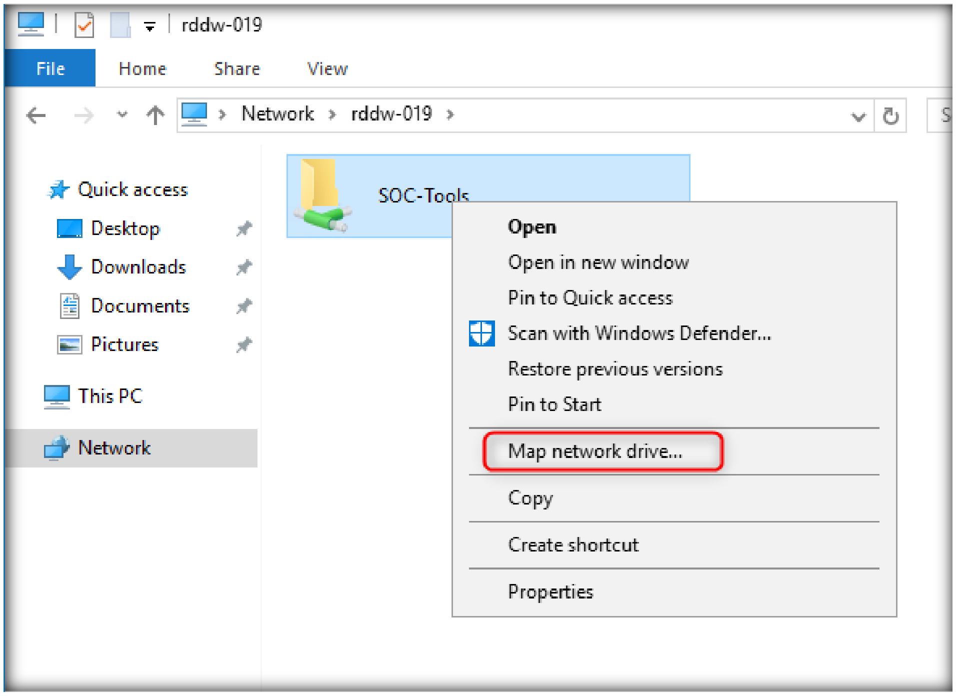
[redacted]

Domain:

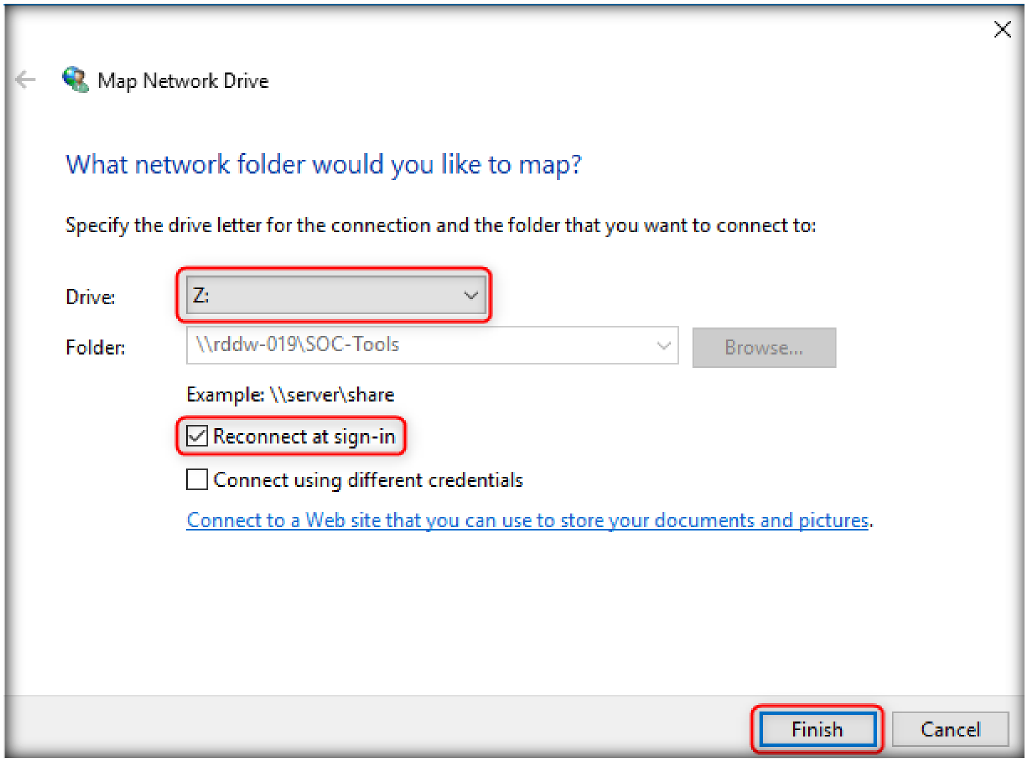
□ Remember my credentials

The user name or password is incorrect.

11. Right-click on **SOC-Tools** shared folder and click Map network drive from the context menu as shown in the screenshot.



12. Map Network Drive window appears, assign drive letter as **Z:\,** make sure that Reconnect at sign-in option is checked and click **Finish**.


Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\rddw-019\SOC-Tools

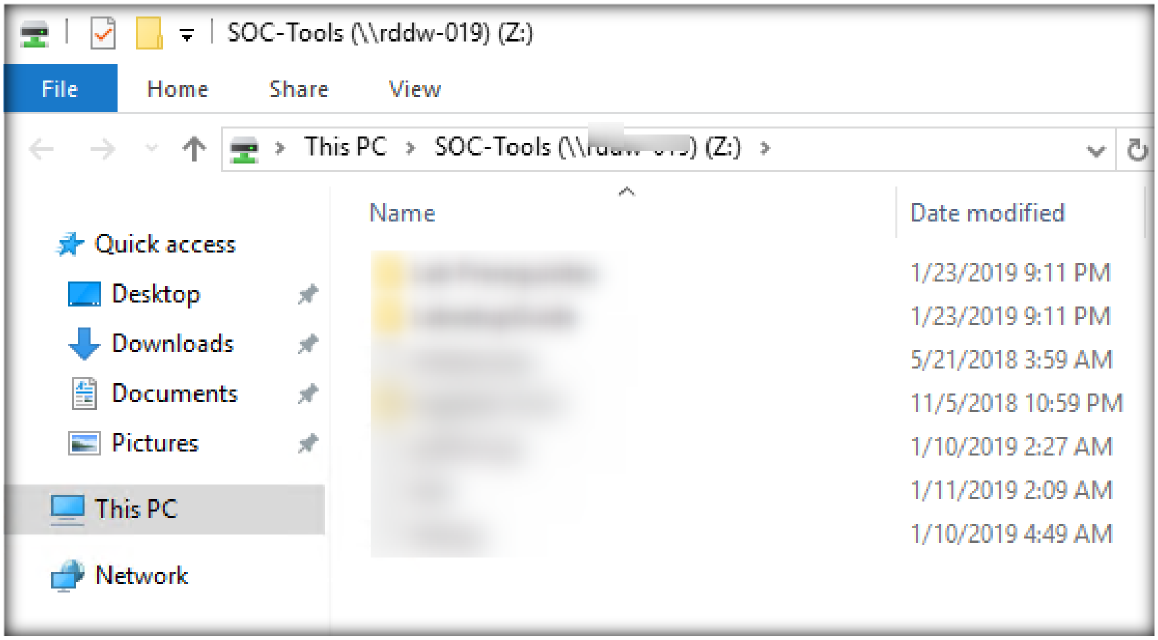
Example: \\server\share

☑ Reconnect at sign-in

☐ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

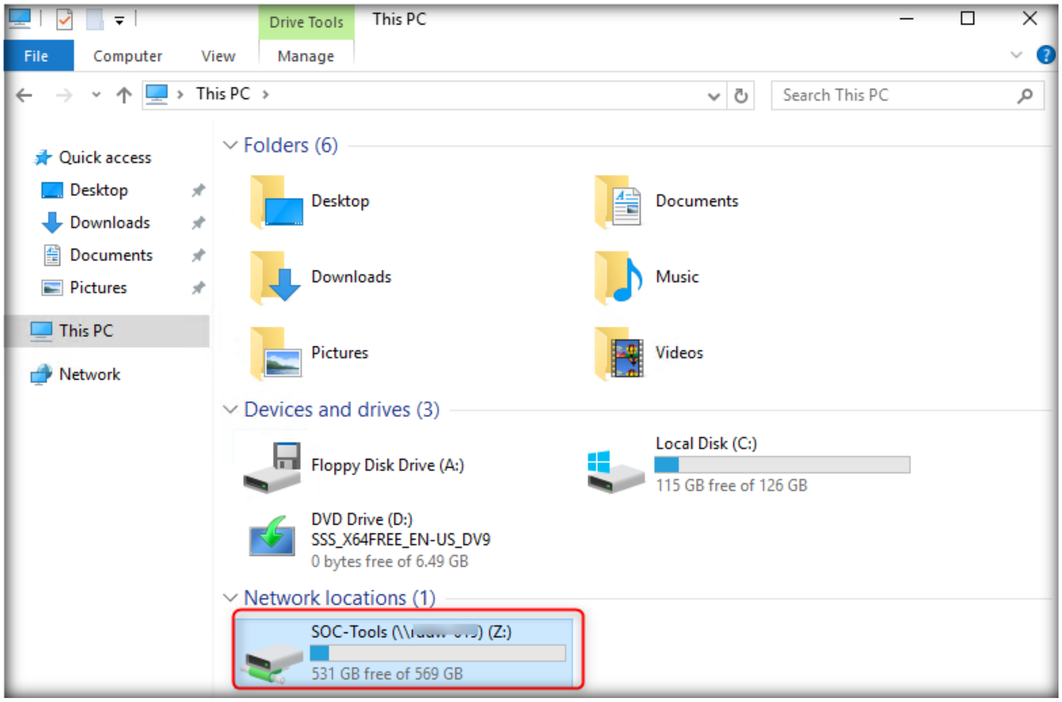
13. SOC-Tools mapped network drive appears in the File Explorer view, click **This-PC** from the left pane to confirm.



Name	Date modified
[redacted]	1/23/2019 9:11 PM
[redacted]	1/23/2019 9:11 PM
[redacted]	5/21/2018 3:59 AM
[redacted]	11/5/2018 10:59 PM
[redacted]	1/10/2019 2:27 AM
[redacted]	1/11/2019 2:09 AM
[redacted]	1/10/2019 4:49 AM

14. Now you can see that **SOC-Tools** directory is mapped to your **SIEM1** machine as shown in the screenshot.

Note: Throughout this configuration, the IP address of the host machine will differ in your lab environment.



CT#6.5: Installing WinRAR in Windows Server 2016 VM

1. Navigate to **Z:\SOC-Tools\Lab Prerequisites\WinRAR** folder.
2. Alternatively, you can also download the latest version of **WinRAR** from **Vendor**.
3. Double click on **winrar-x64-540.exe** to begin the installation.
4. **WinRAR setup** window appears.
5. In the **WinRAR 5.10** setup window, click **Install.**
6. Complete the **install** by choosing **defaults** throughout the installation process.
7. After completing the installation, the installation **location** of WinRAR files window opens **automatically.**
8. Close the window.

CT#6.6: Installing Web Browsers in Windows Server 2016 VM

1. Navigate to **Z:\SOC-Tools\Lab Prerequisites** in guest operating systems.
2. Open **Web Browsers** folder.
3. Follow **wizard-driven** installation steps and install **Firefox** and **Chrome** web browsers.
4. You can also download **latest** version of web browsers from respective **vendors**.

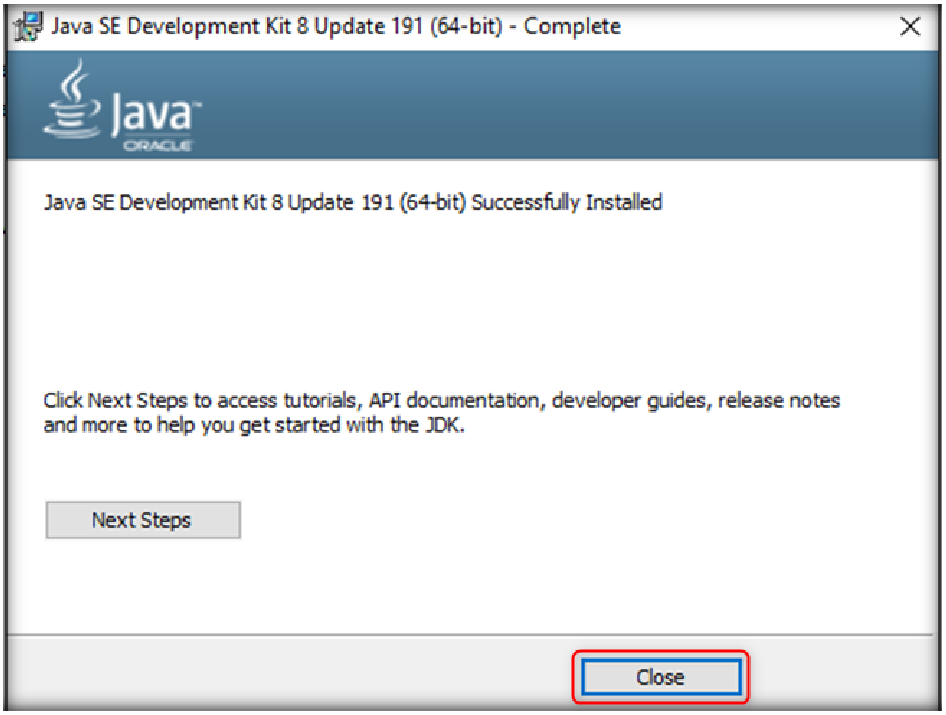
CT#6.7: Installing Notepad++ in Windows Server 2016 VM

1. Navigate to **Z:\SOC-Tools\Lab Prerequisites** in guest operating systems.
2. Open **Notepad++** folder and double-click **npp.7.3.2.Installer**.
3. Follow the wizard-driven installation steps, to install **Notepad++**.
4. You can also download latest version of Notepad++ from its vendor site.

CT#6.8: Installing Java Development Kit 8u (JDK 8u) in Windows Server 2016 VM

1. Navigate to **Z:\SOC-Tools\SOC Lab Prerequisites** in guest operating systems.
2. Open JDK Folder and double-click **jdk-8u191-windows-x64.exe**.
3. Follow the wizard-driven installation steps to install JDK.

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

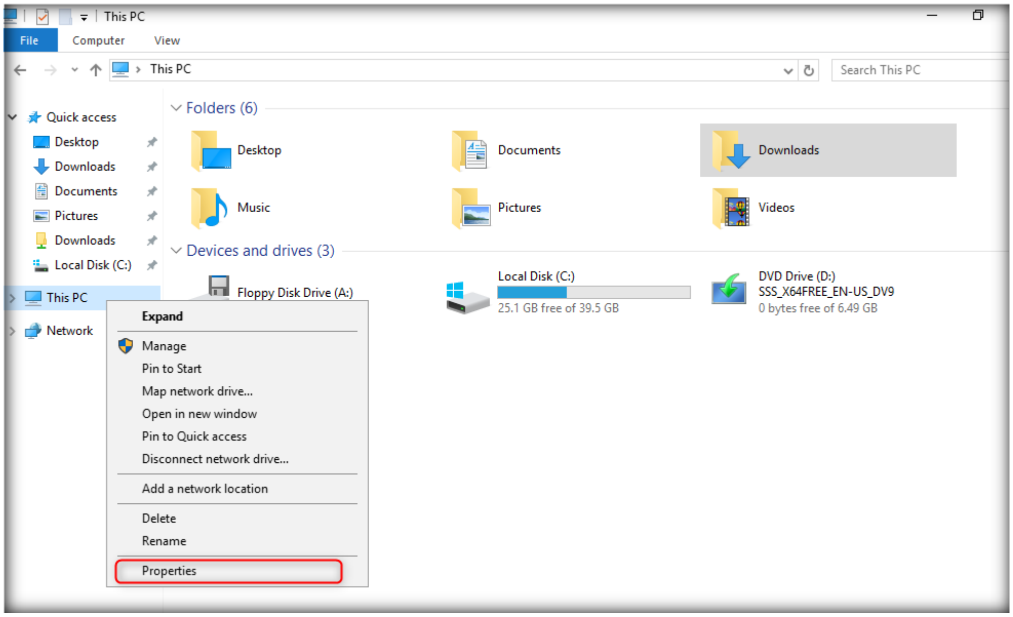


Java SE Development Kit 8 Update 191 (64-bit) - Complete

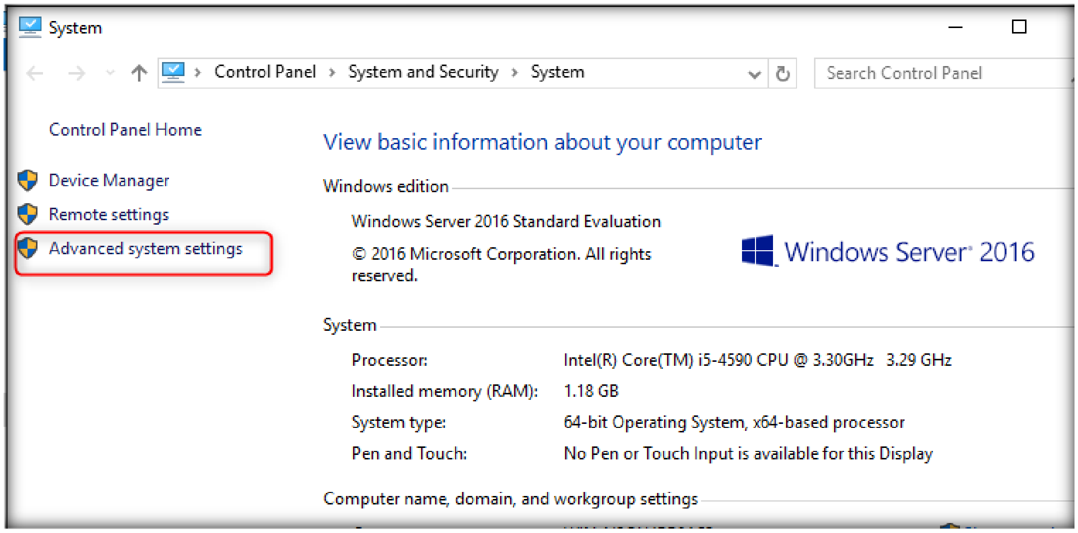
Java SE Development Kit 8 Update 191 (64-bit) Successfully Installed

Click Next Steps to access tutorials, API documentation, developer guides, release notes and more to help you get started with the JDK.

5. For Setting-up **JAVA_HOME** System Variable, open **File Explorer** and right-click on **This PC** and select **Properties** option from the context menu.



6. **System** window will appear, click on **Advanced system settings** option.



View basic information about your computer

Windows edition

Windows Server 2016 Standard Evaluation

© 2016 Microsoft Corporation. All rights reserved.

Windows Server 2016

System

Processor: Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 3.29 GHz

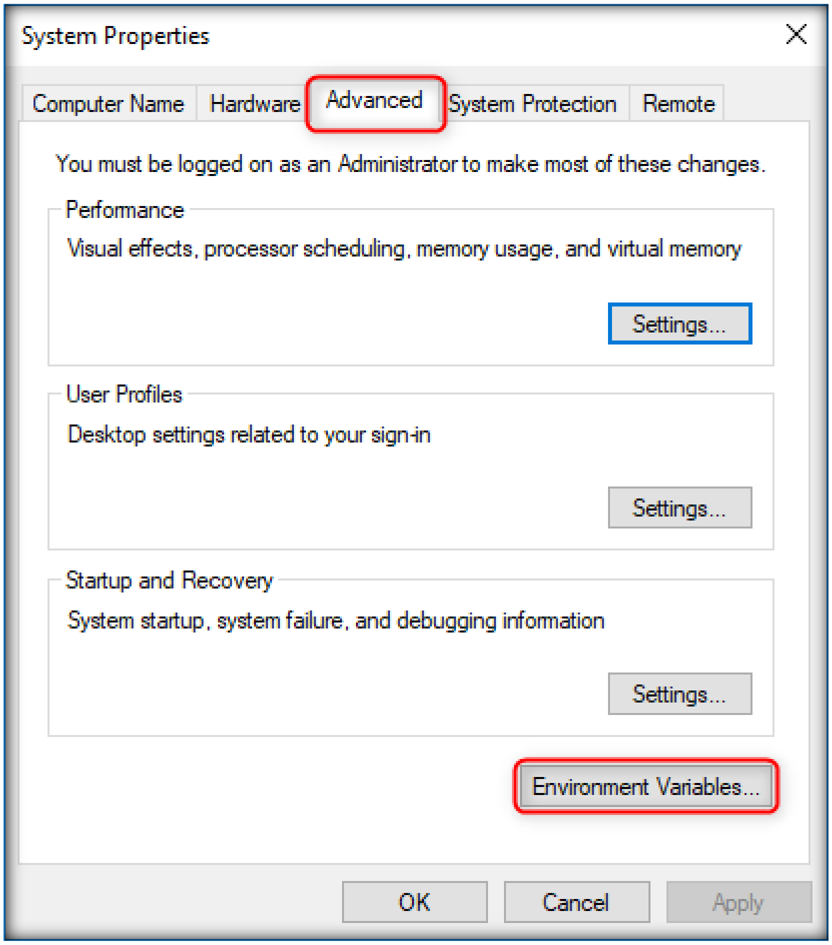
Installed memory (RAM): 1.18 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

7. System Properties window will appear, Navigate to **Advanced** Tab. Click **Environment Variables…** button.



You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

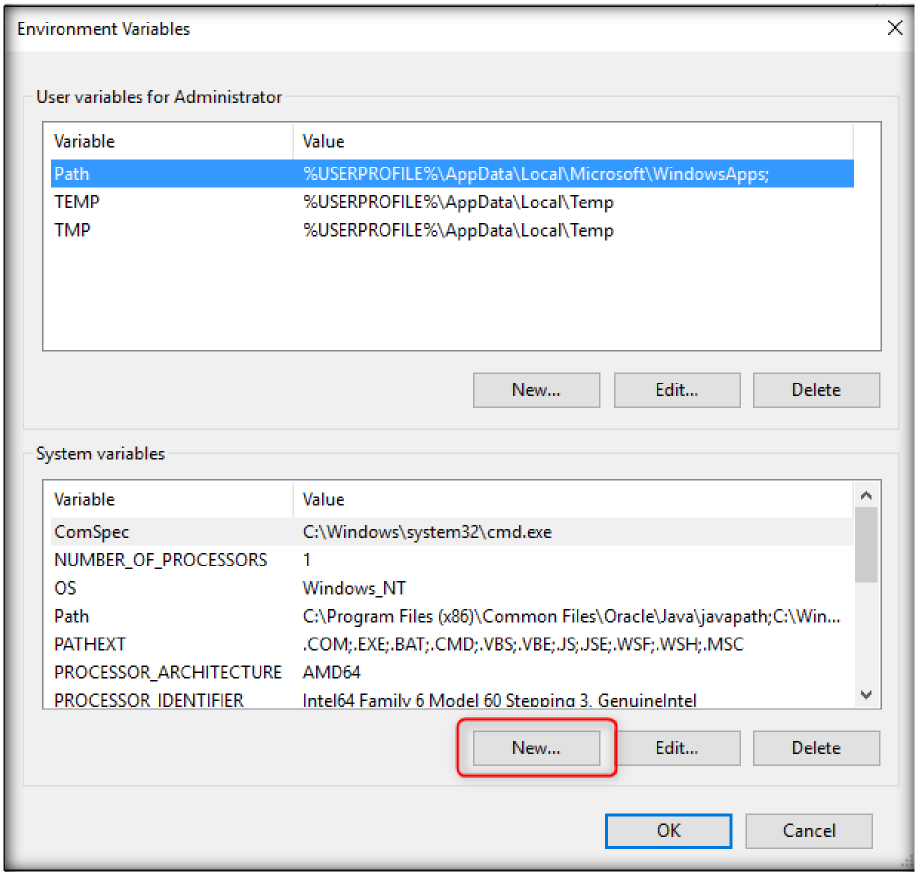
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

8. **Environment Variables** window will appear, click on **New…** button in under **System variables** pane.



Environment Variables

User variables for Administrator

Variable	Value
Path	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

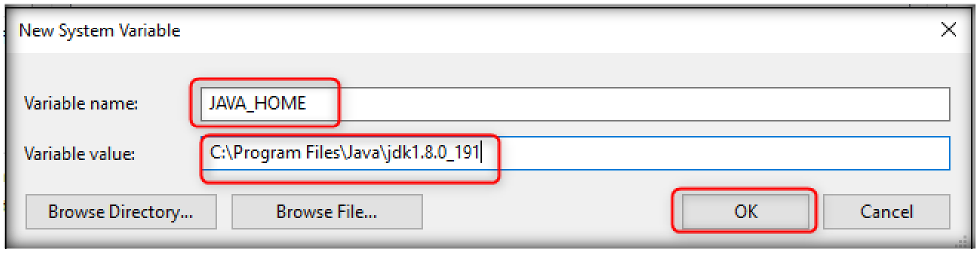
Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
NUMBER_OF_PROCESSORS	1
OS	Windows_NT
Path	C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Win...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 60 Stepping 3, GenuineIntel

9. New System variable window will appear, enter details given below.

   Variable Name: **JAVA_HOME**

   Variable value: **C:\Program Files\Java\jdk1.8.0_191** (if you did not change the path while installing JDK).

   Note: if you have changed the Path while installing JDK, locate Java installation directory and enter the path of Java installation directory as Variable value. Click **OK** button.

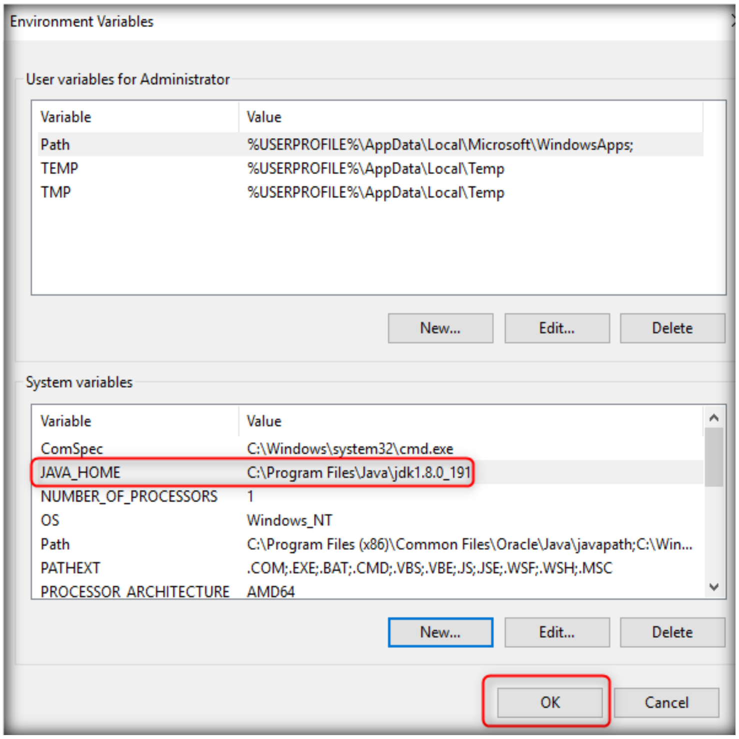


New System Variable

Variable name: JAVA_HOME

Variable value: C:\Program Files\Java\jdk1.8.0_191

10. You will see **JAVA_HOME** variable listed under **System variables** pane. Click **OK.**



Environment Variables

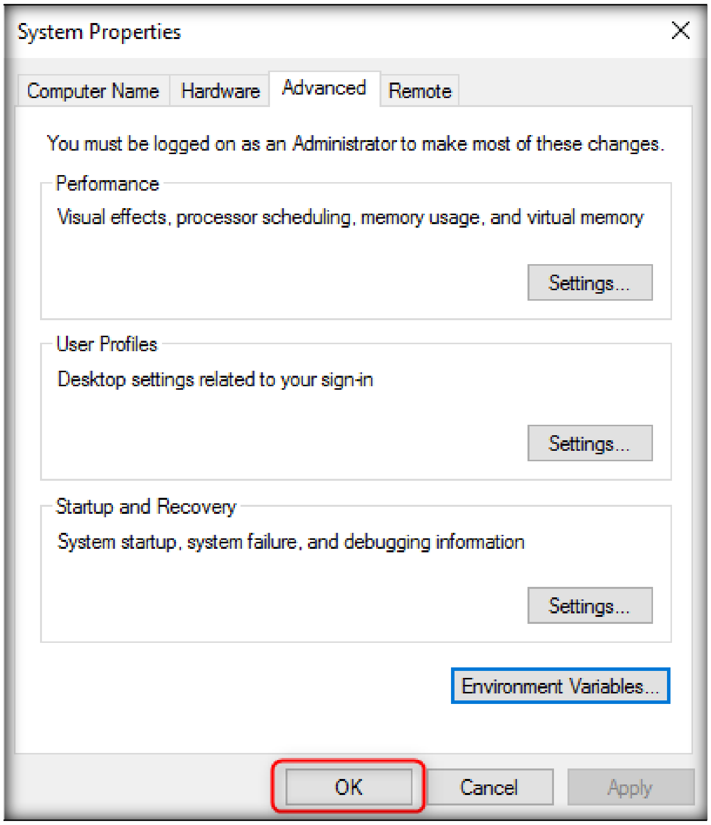
User variables for Administrator

Variable	Value
Path	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
JAVA_HOME	C:\Program Files\Java\jdk1.8.0_191
NUMBER_OF_PROCESSORS	1
OS	Windows_NT
Path	C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Win...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64

11. Click **OK** button in the **System Properties** Window. Restart the system to complete the java installation.



System Properties

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

Desktop settings related to your sign-in

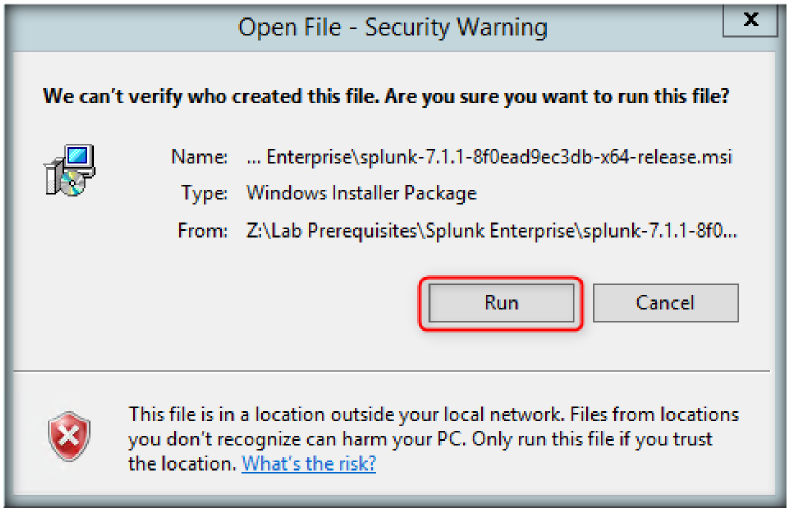
Startup and Recovery

System startup, system failure, and debugging information

CT#6.9: Installing Splunk Enterprise in Windows Server 2016 VM

1. Launch **SIEM1**.
2. Login as Administrator (Username: Administrator and Password: admin@123).
3. Navigate to **Z:\SOC-Tools\Lab Prerequisites\Splunk Enterprise**.

   (Ensure you have installed google chrome in windows server 2016 before installing Splunk Enterprise).
4. Double click **splunk-7.1.1-8f0ead9ec3db-x64-release.msi** to start the installation. If the Open File - Security Warning window pops up appears, click Run**.** **Note:** If a notification appears stating the "SmartScreen has prevented the app from running", click More info, and then click Run anyway.



Open File - Security Warning

We can't verify who created this file. Are you sure you want to run this file?

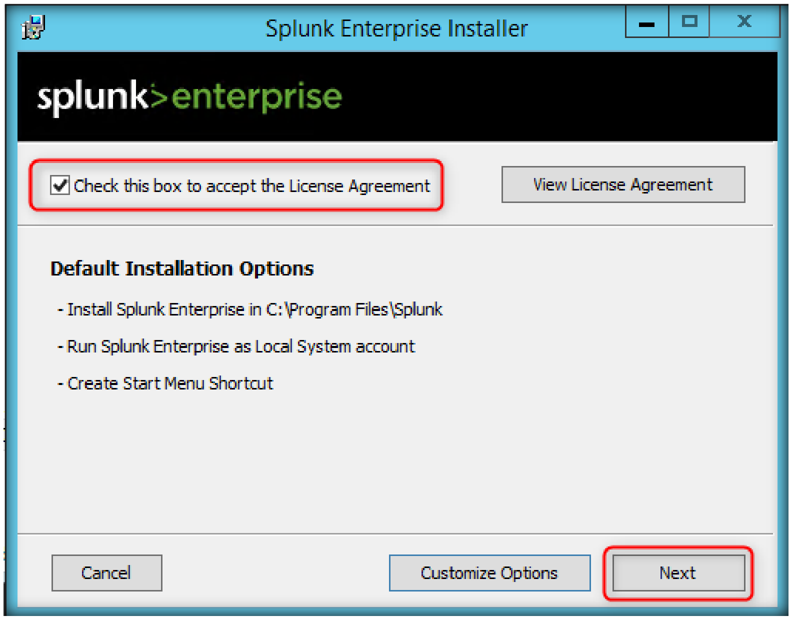
Name: ... Enterprise\splunk-7.1.1-8f0ead9ec3db-x64-release.msi

Type: Windows Installer Package

From: Z:\Lab Prerequisites\Splunk Enterprise\splunk-7.1.1-8f0...

This file is in a location outside your local network. Files from locations you don't recognize can harm your PC. Only run this file if you trust the location. What's the risk?

5. The Splunk Enterprise Installer window appears. Accept the license agreement and click **Next**.



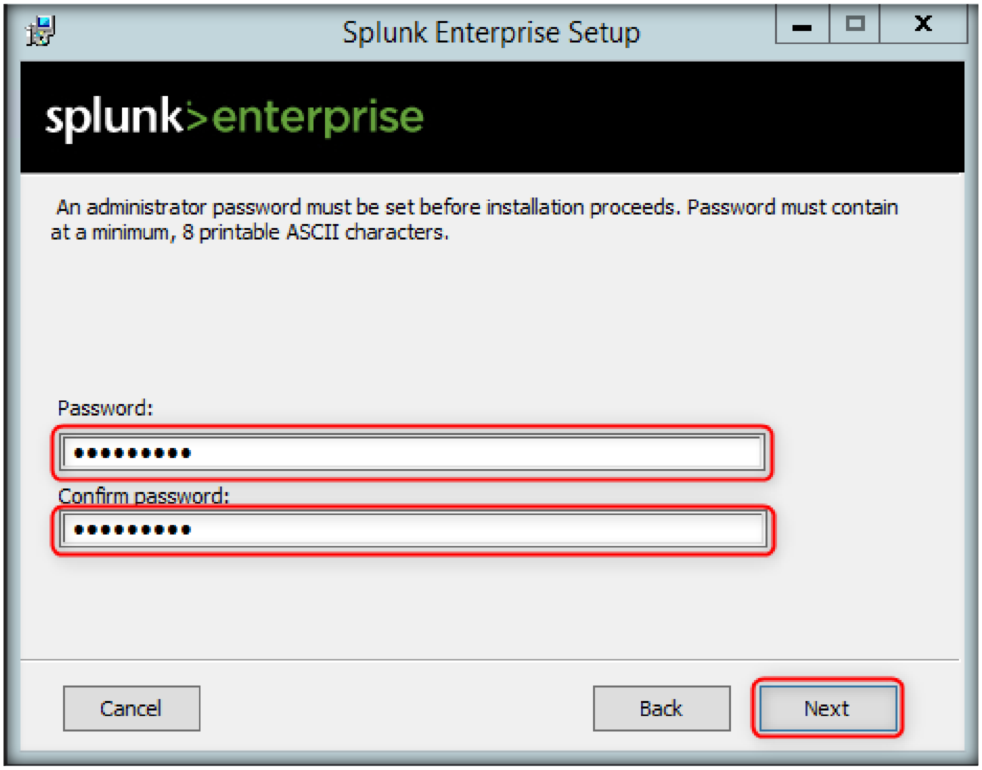
Splunk Enterprise Installer

☑ Check this box to accept the License Agreement

Default Installation Options

- Install Splunk Enterprise in C:\Program Files\Splunk
- Run Splunk Enterprise as Local System account
- Create Start Menu Shortcut

6. Set administrator password for Splunk Enterprise by giving a password (**admin@123**).

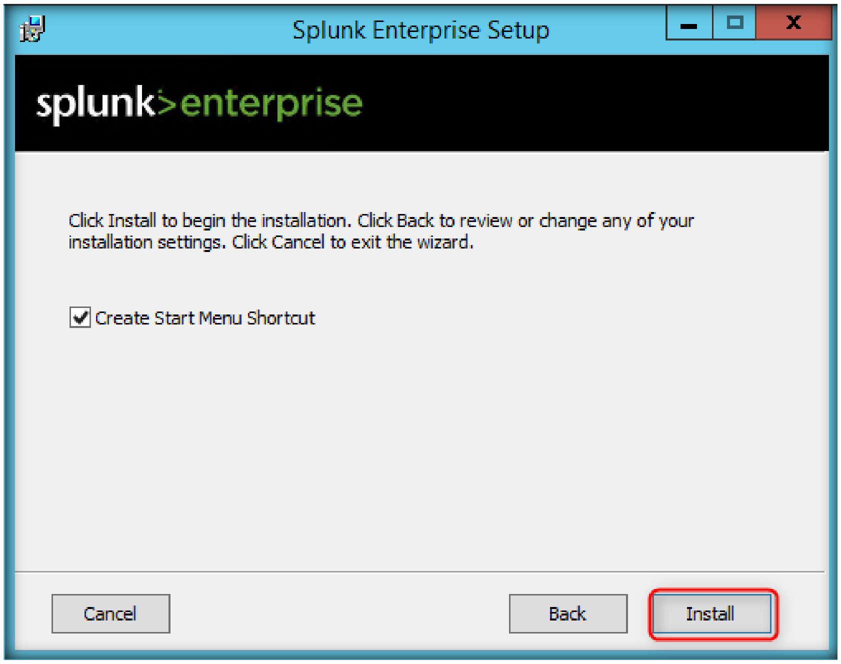


An administrator password must be set before installation proceeds. Password must contain at a minimum, 8 printable ASCII characters.

Password: •••••••••

Confirm password: •••••••••

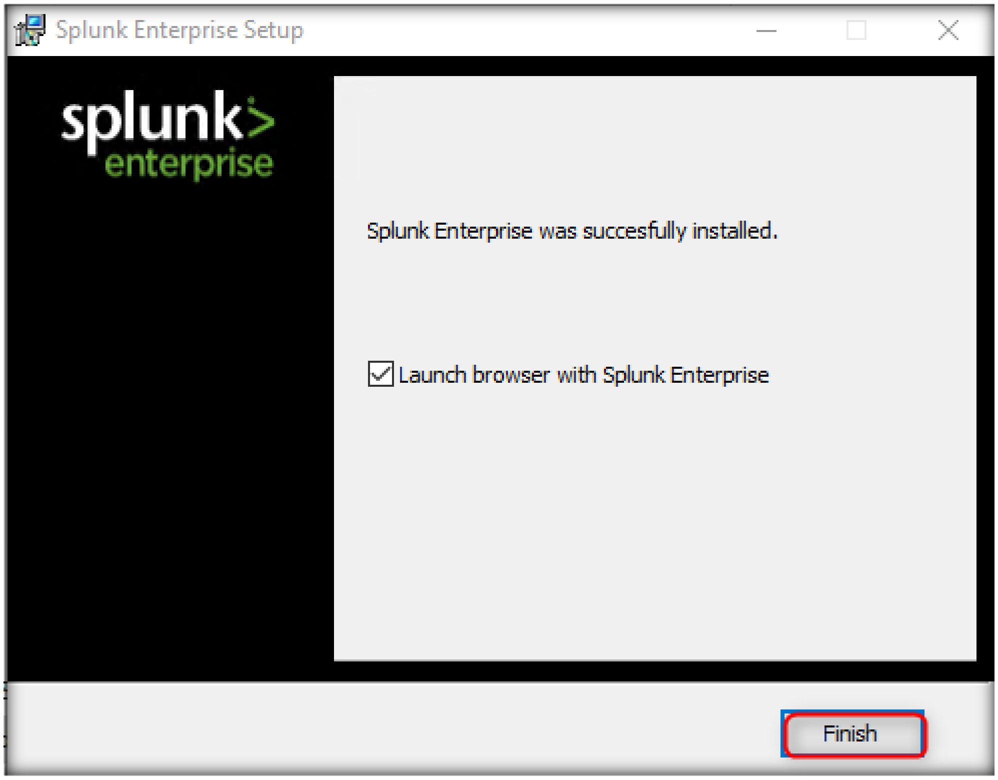
7. Click **Install** to install Splunk Enterprise.



Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

☑ Create Start Menu Shortcut

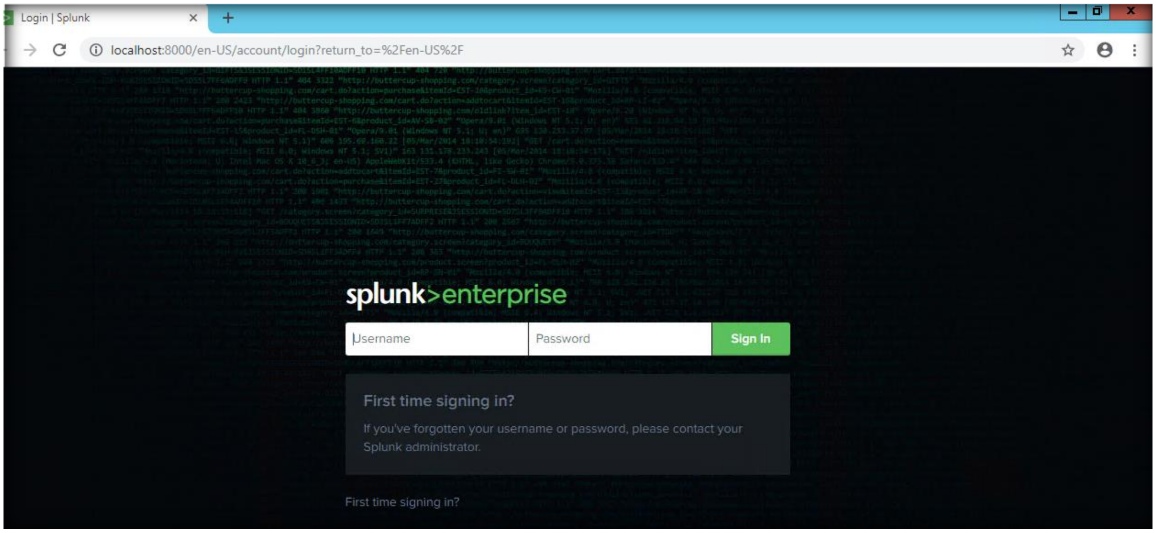
8. Wait for the installation to complete. Click **Finish** to complete Splunk enterprise setup.



Splunk Enterprise was succesfully installed.

☑ Launch browser with Splunk Enterprise

9. Splunk Enterprise launches in your default browser. The **First time signing in?** page appears. Enter the **username (admin)** and **password** (provided while installation (**admin@123**) in their respective fields and click **Sign in**.

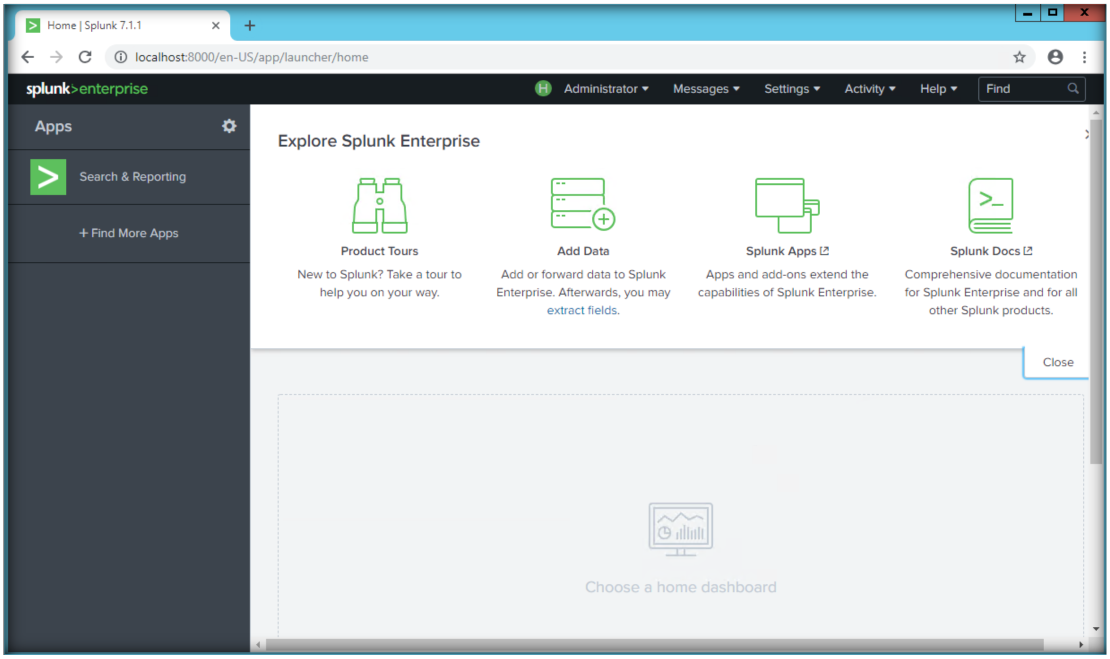


localhost:8000/en-US/account/login?return_to=%2Fen-US%2F

First time signing in?

If you've forgotten your username or password, please contact your Splunk administrator.

10. You will be successfully logged in to Splunk Enterprise.



Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

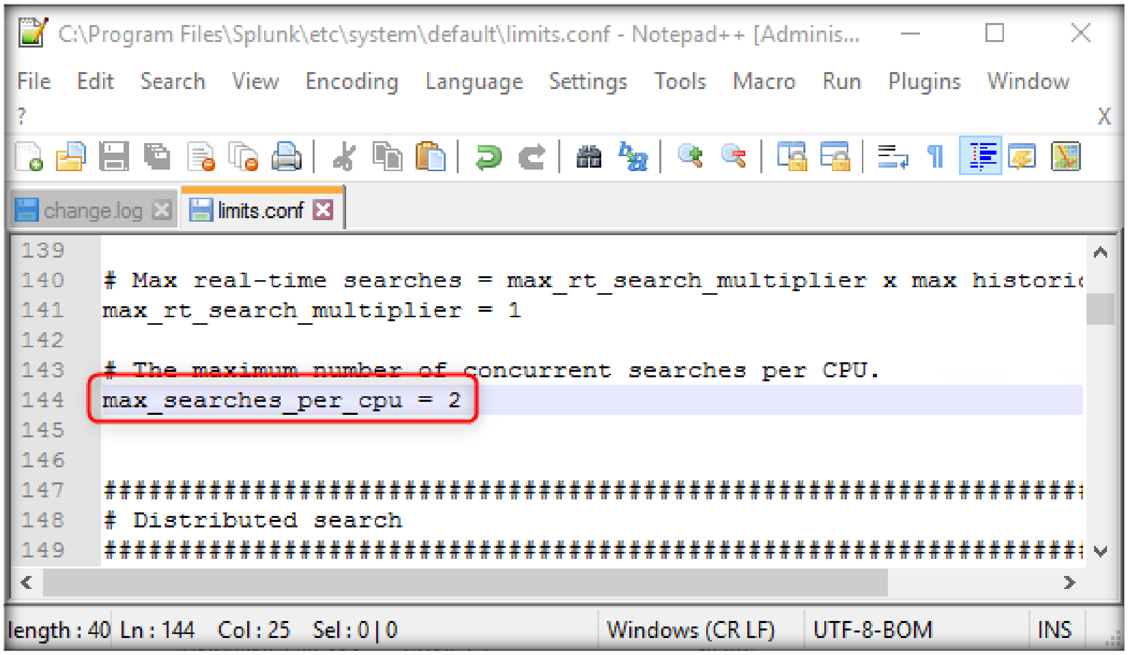
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

Choose a home dashboard

11. To increase default maximum number of concurrent of searches per CUP in Splunk Enterprise, navigate to **c:\Program Files\Splunk\etc\system\default** and open file **limits.conf** with **Notepad++.**

12. Go to line no 144 and set **max_searches_per_cpu=2**, click save and close the file.

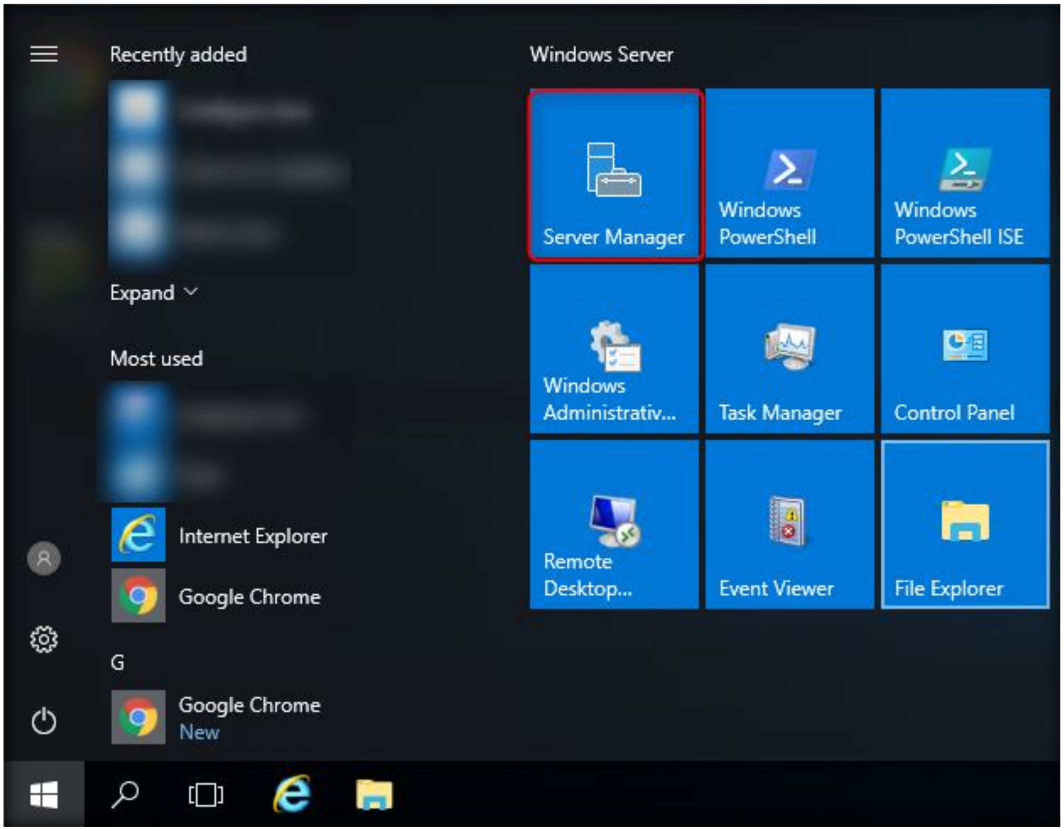


```
139
140 # Max real-time searches = max_rt_search_multiplier x max historic
141 max_rt_search_multiplier = 1
142
143 # The maximum number of concurrent searches per CPU.
144 max_searches_per_cpu = 2
145
146
147 ####################################################################
148 # Distributed search
149 ####################################################################
```

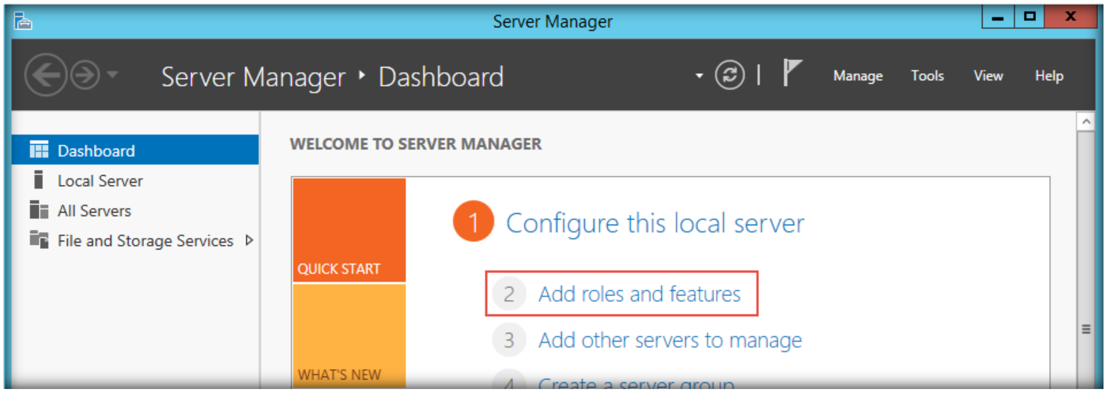
length : 40 Ln : 144 Col : 25 Sel : 0 | 0 Windows (CR LF) UTF-8-BOM INS

CT#6.10: Installing .Net Framework 3.5 (Includes .Net 2.0 and 3.0)

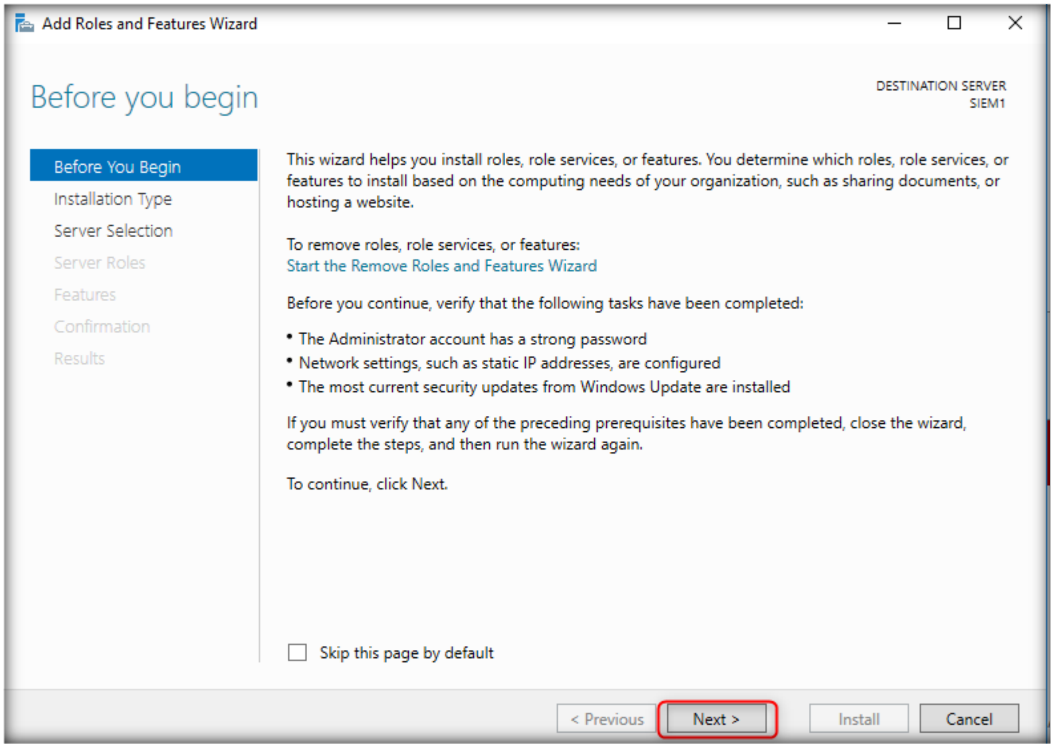
1. To open Server Manager, click **Start** → **Server Manager** icon.
2. To open Server Manager, click **Start** → **Server Manager** icon.



3. Click **Add roles and features** as shown in the screenshot.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group

4. **Add Roles and Features Wizard** appears, by default Before You Begin section selected, click **Next**.



Before you begin

DESTINATION SERVER
SIEM1

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

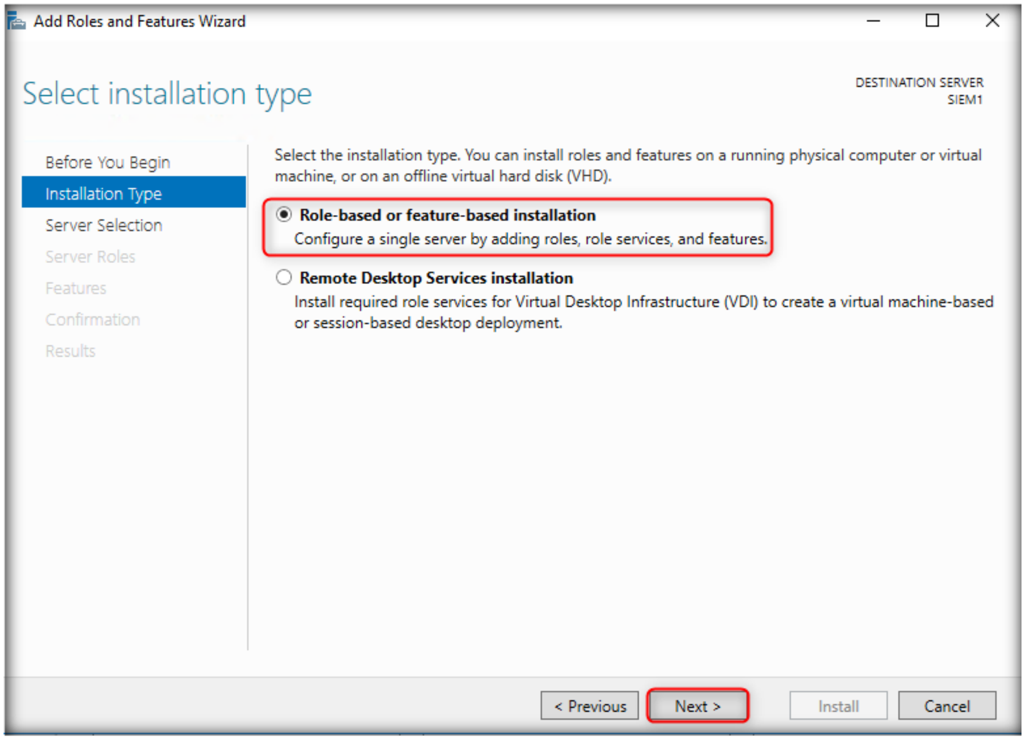
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

5. In Installation Type section leave the selection to default, click **Next**.



Select installation type

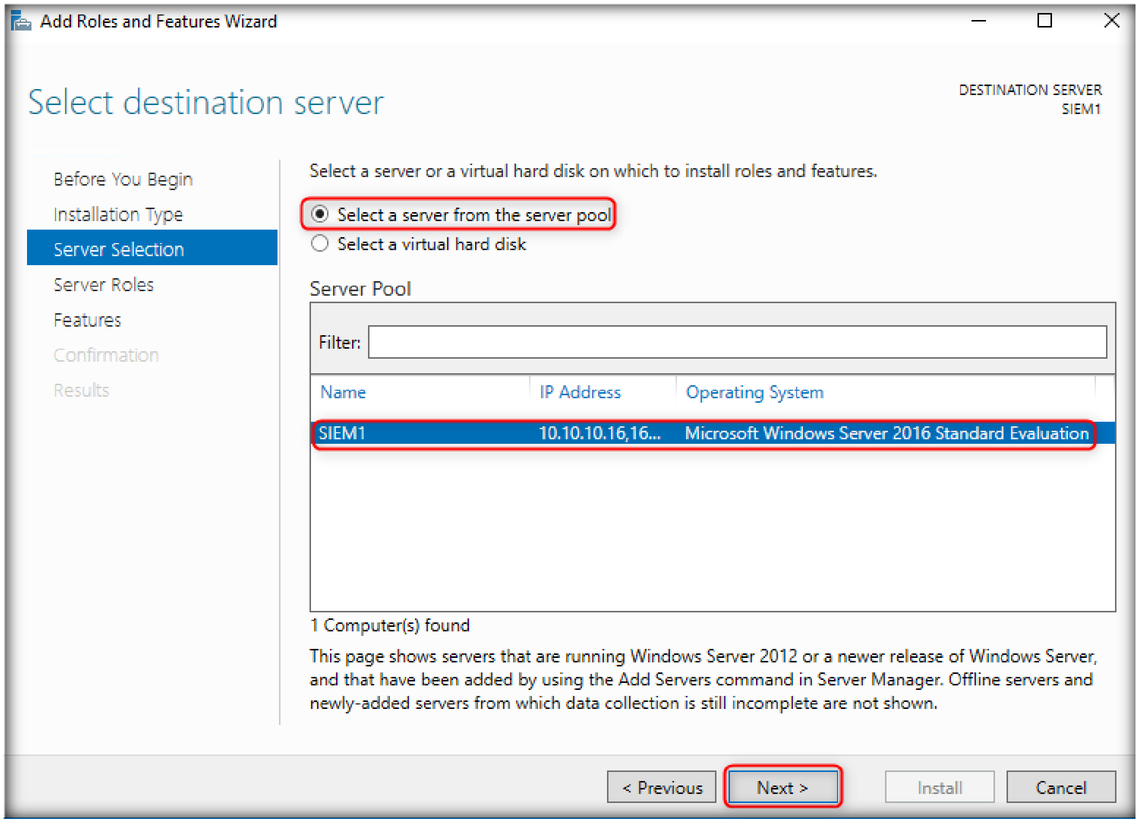
DESTINATION SERVER
SIEM1

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

6. In Server Selection section, leave the settings to default and click **Next**.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
SIEM1

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

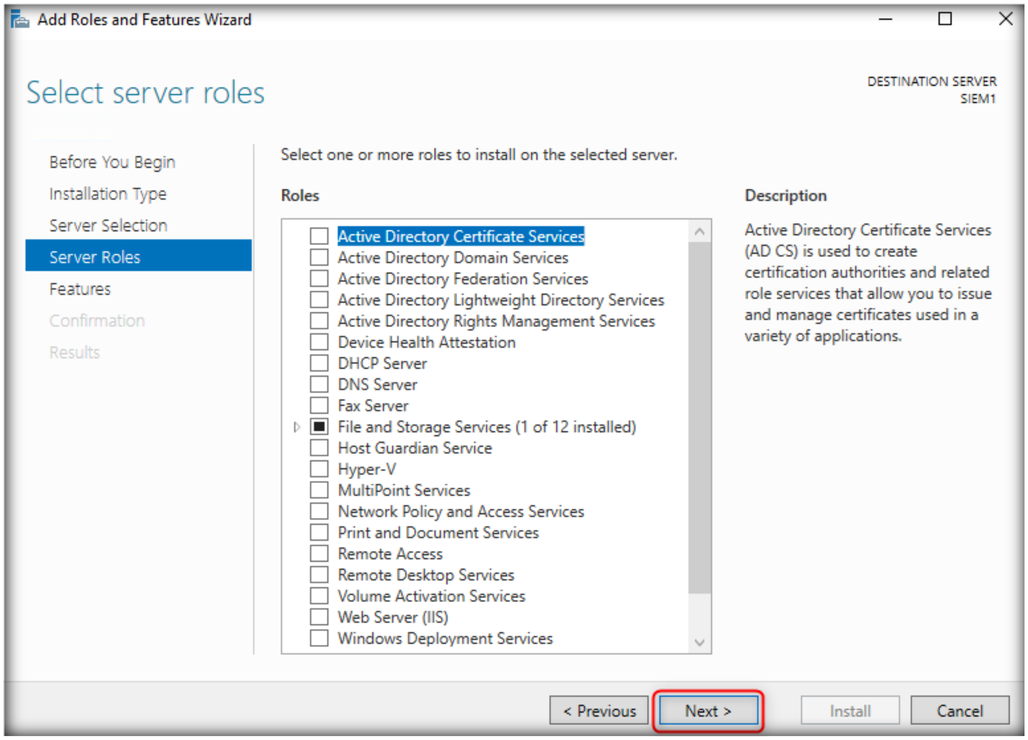
Filter:

Name	IP Address	Operating System
SIEM1	10.10.10.16,16...	Microsoft Windows Server 2016 Standard Evaluation

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

7. In Server Roles section, click **Next**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
SIEM1

Select one or more roles to install on the selected server.

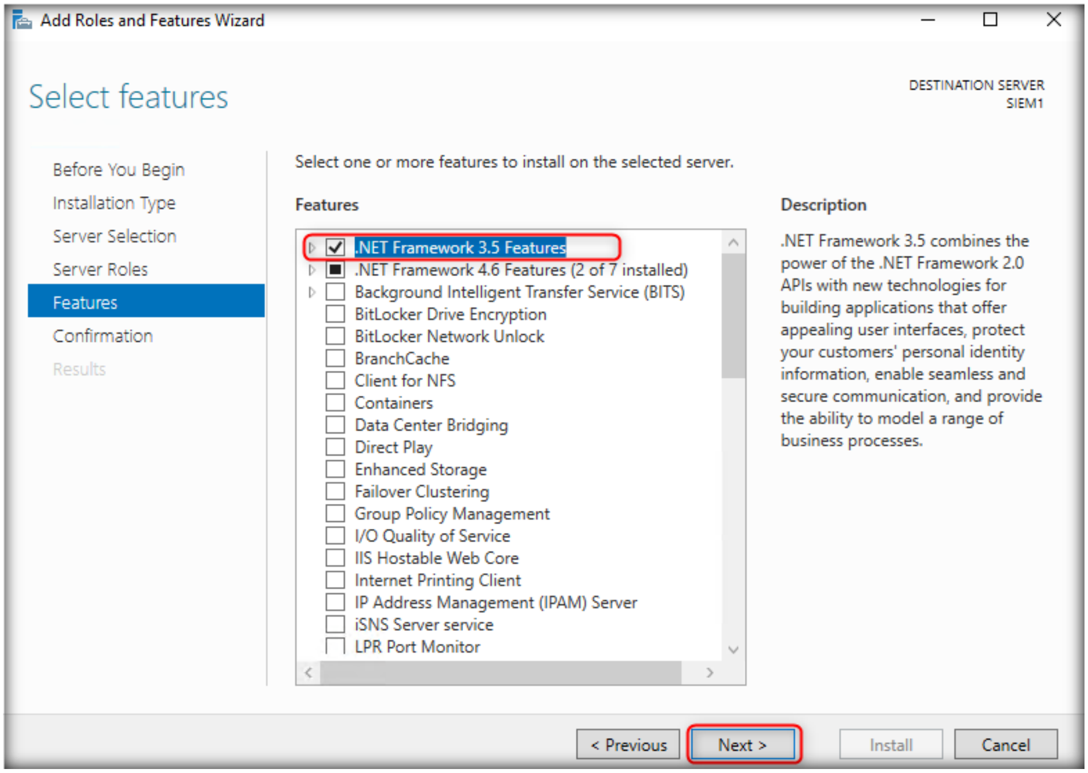
Roles

□ Active Directory Certificate Services
□ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Device Health Attestation
□ DHCP Server
□ DNS Server
□ Fax Server
■ File and Storage Services (1 of 12 installed)
□ Host Guardian Service
□ Hyper-V
□ MultiPoint Services
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
□ Web Server (IIS)
□ Windows Deployment Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

8. In **Select features** section, check **.NET Framework 3.5 Features** check box, and click **Next**.



Add Roles and Features Wizard

Select features

DESTINATION SERVER
SIEM1

Select one or more features to install on the selected server.

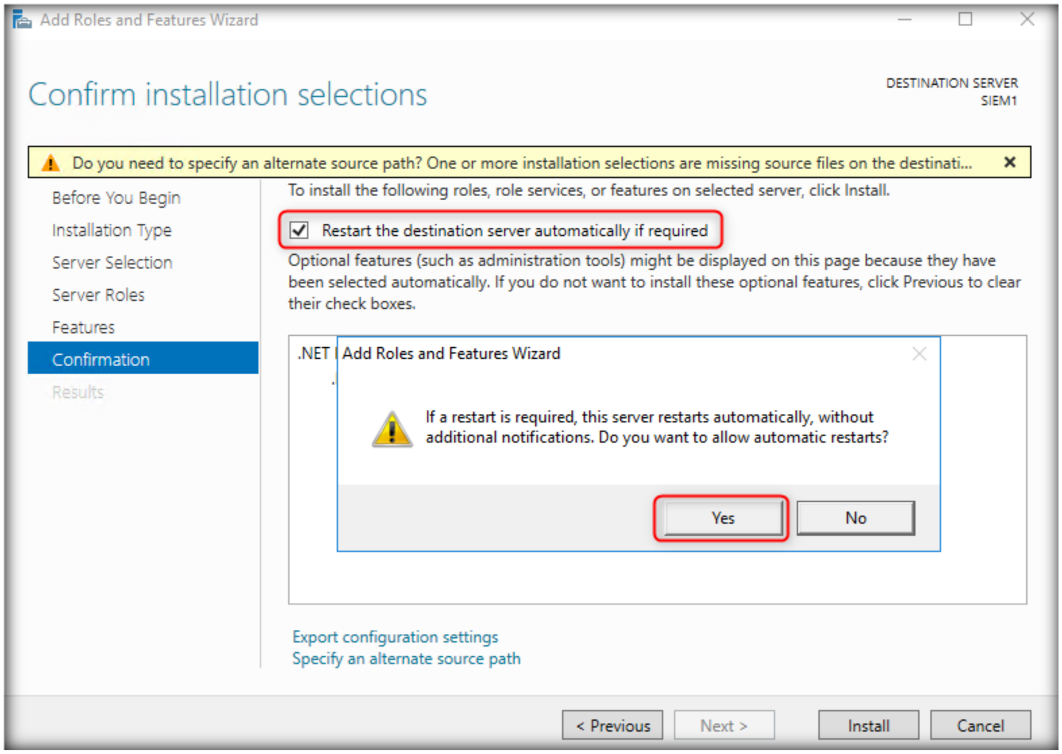
Features

- ☑ .NET Framework 3.5 Features
- ■ .NET Framework 4.6 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service
- □ LPR Port Monitor

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

9. In **Confirm installation selections**, check **Restart the destination server automatically if required** option. Add Roles and Features Wizard pop-up appears click **Yes**.



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
SIEM1

Do you need to specify an alternate source path? One or more installation selections are missing source files on the destinati...

To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

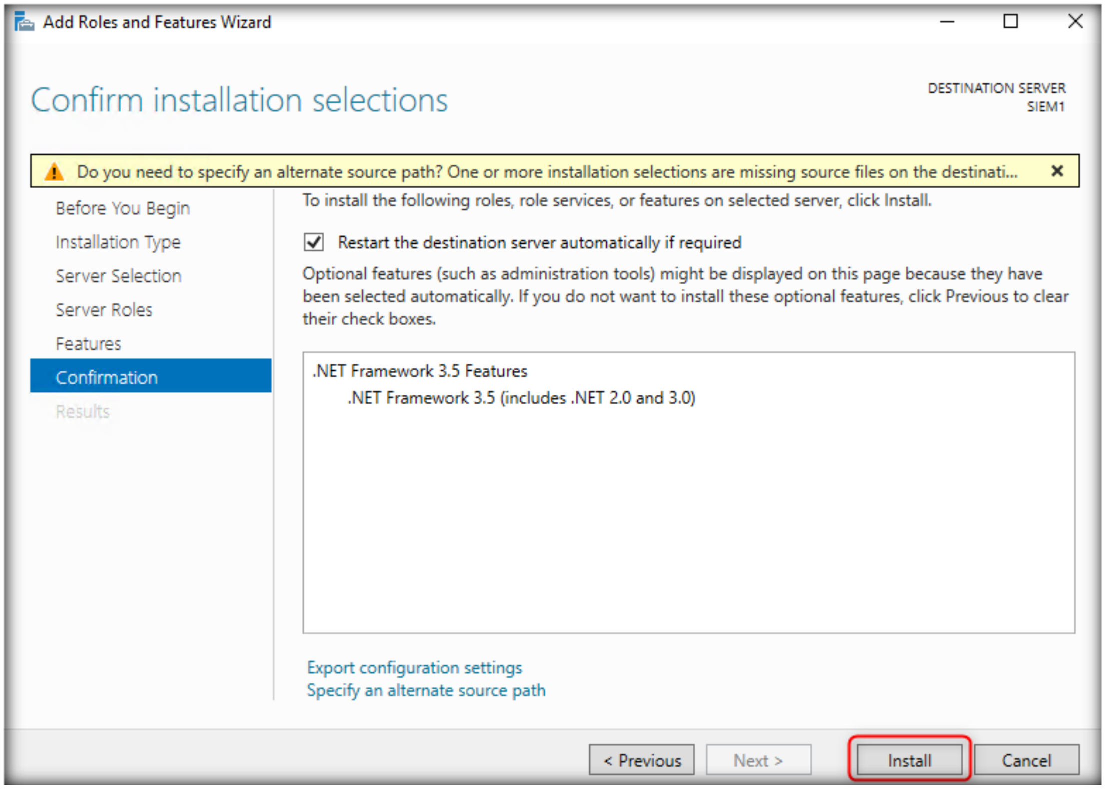
.NET

Add Roles and Features Wizard

If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Yes
No
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

10. Click **Install** button to proceed for the selected features installation.



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
SIEM1

⚠ Do you need to specify an alternate source path? One or more installation selections are missing source files on the destinati...

To install the following roles, role services, or features on selected server, click Install.

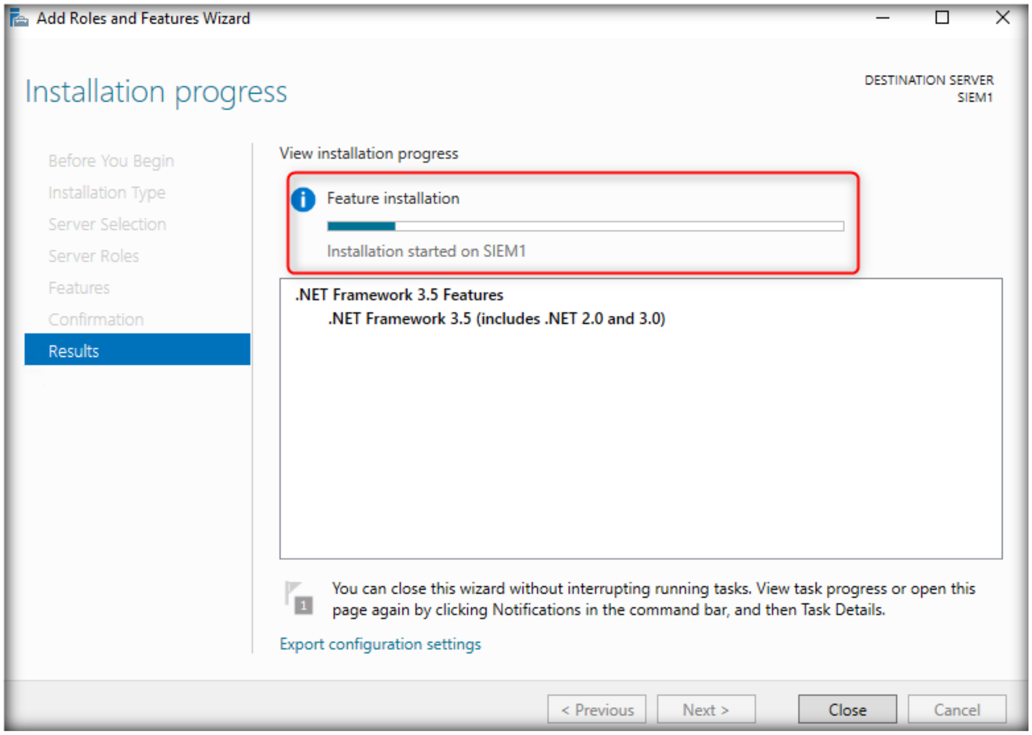
☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

11. Wait until the installation is completed.



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
SIEM1

View installation progress

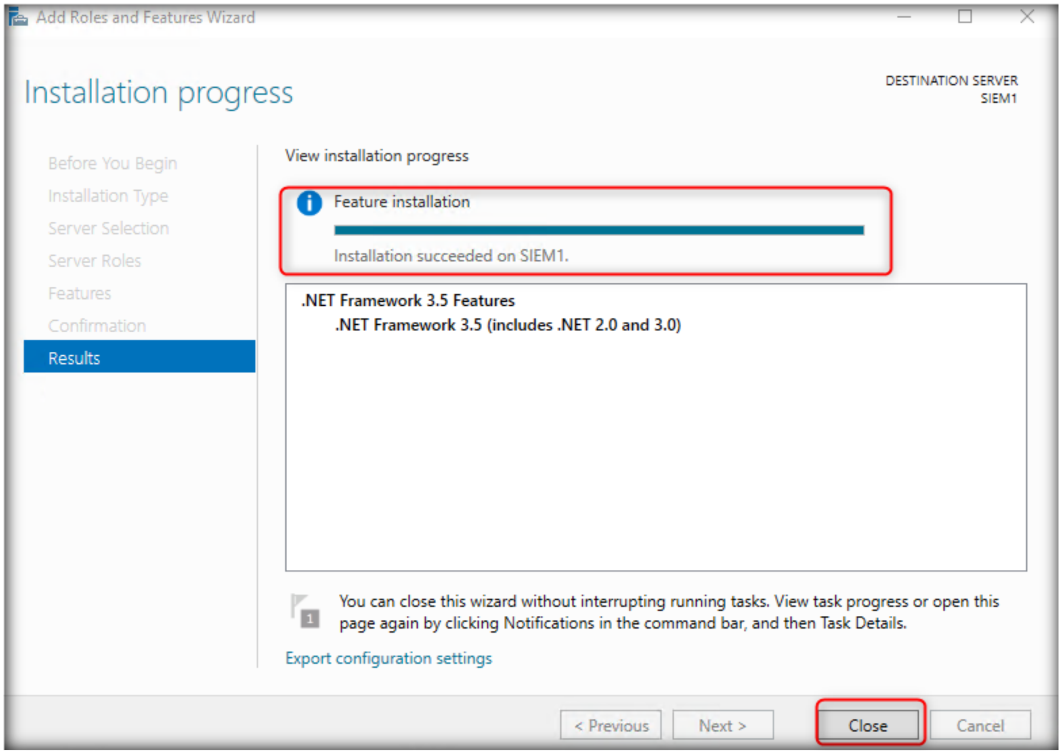
Feature installation

Installation started on SIEM1

.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

12. Once the installation is completed, you can see the message as Installation Succeeded as shown in the screenshot, click **Close** button. If restart is required, restart the machine.



Installation succeeded on SIEM1.

.NET Framework 3.5 Features
.NET Framework 3.5 (includes .NET 2.0 and 3.0)

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

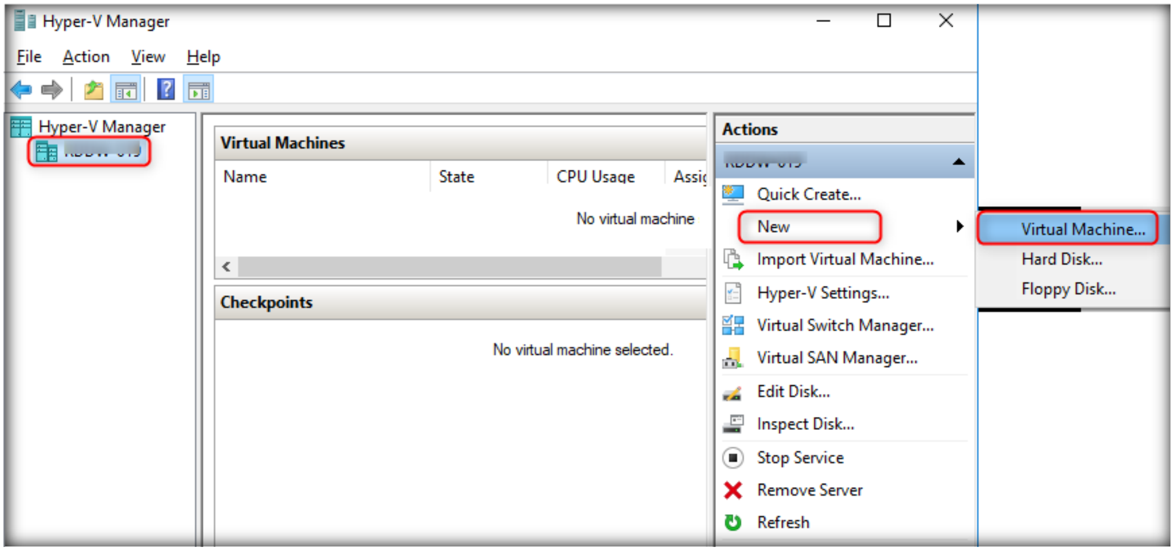
CT#6.11: Turn off Windows Firewall in Windows Server 2016 VM

1. Follow the step 3 to 11 of CT#2, to turn off firewall Windows Server 2016.

CT#7: Creating and Configuring Windows Server 2012 Virtual Machine

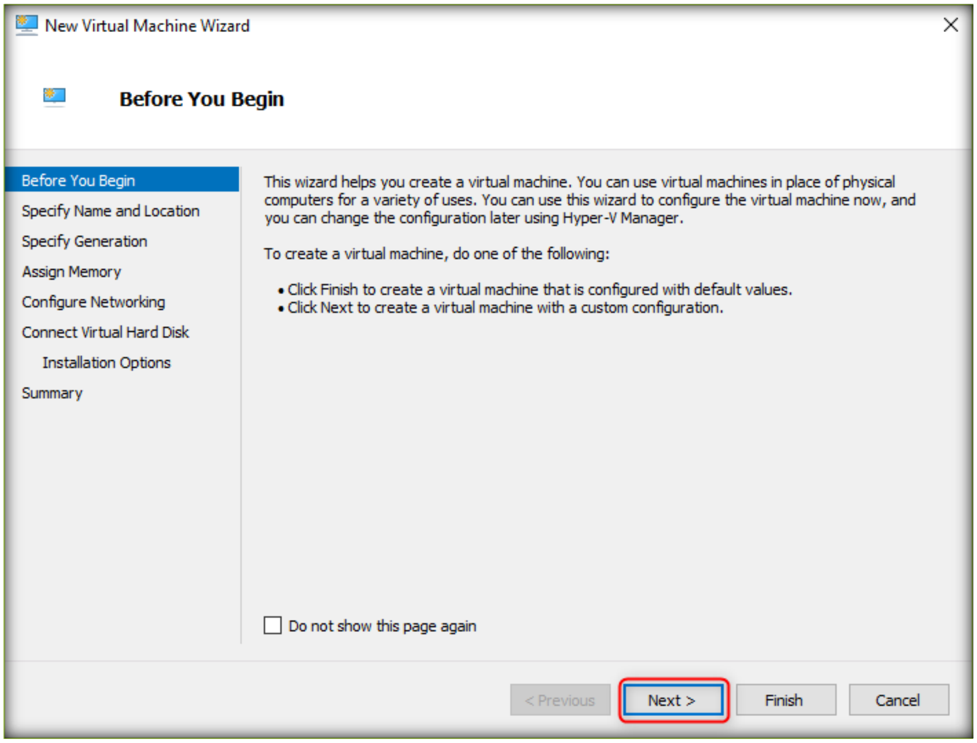
CT#7.1: Creating a Virtual Machine and Installing Windows Server 2012 R2 Standard Guest OS

1. Launch Hyper-V Manager. If already launched, skip to step two.
2. Select your local machine in the left pane, then click **New** under **Actions** pane, and then click **Virtual Machine** in the right pane as shown in the screen shot.



Note: Every machine has a unique name, so the name of your machine differs from the name shown in the above screenshot.

3. **New Virtual Machine Wizard** window appears, click **Next** button.



This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

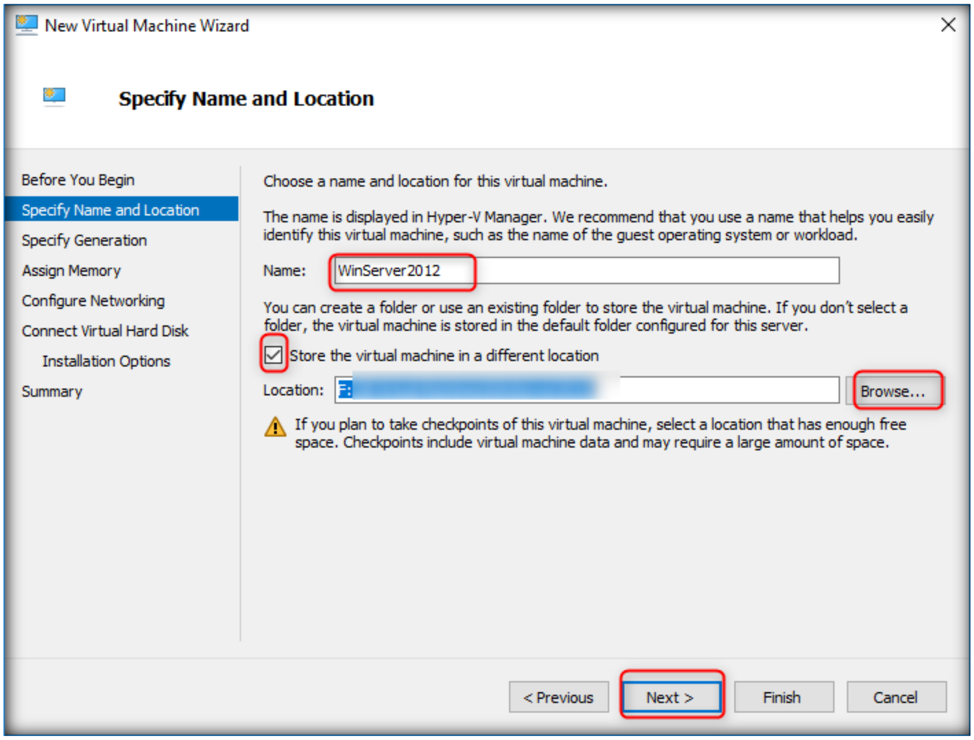
☐ Do not show this page again

4. Specify **Name WinServer2012** and **location** of new virtual machine. Assign the name of the virtual machine as **Windows Server 2012**.

5. The default location for storing the virtual machine is **C:\ProgramData\Microsoft\Windows\Hyper-V\.** You can choose different location to store the VM's or set it to default location.

6. Click **Next**.

   Note: You can specify the location either in the **Specify Name and Location** section or in the forthcoming **Connect Virtual Hard Disk** section.



Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: WinServer2012

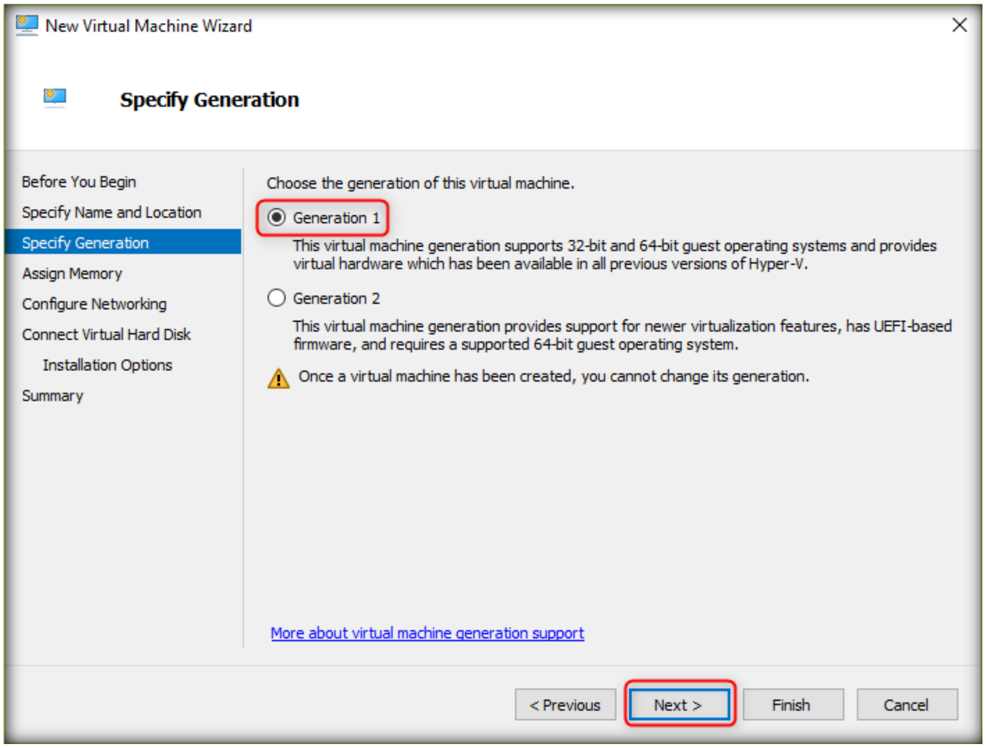
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

Location: F:[redacted]

⚠ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

7. Choose the generation of the virtual machine (here, **Generation 1**) and click **Next**.



Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

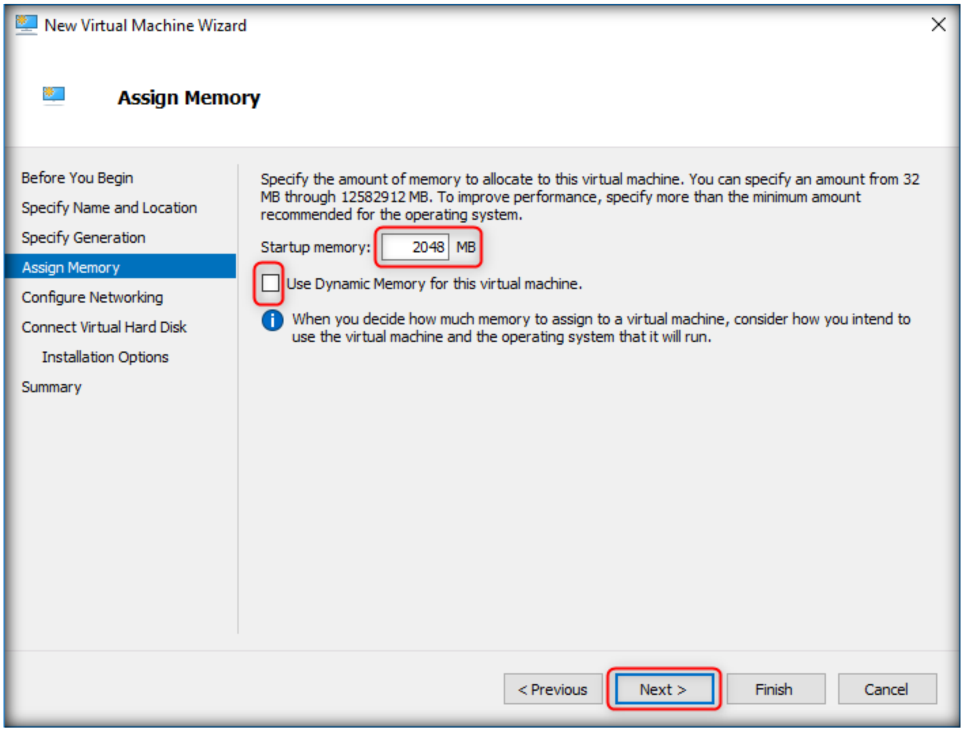
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

8. Assign the amount of Startup memory to allocate to this virtual machine in MB (here, 2048) and uncheck Use Dynamic Memory for this virtual machine.

9. Click **Next**.



New Virtual Machine Wizard

Assign Memory

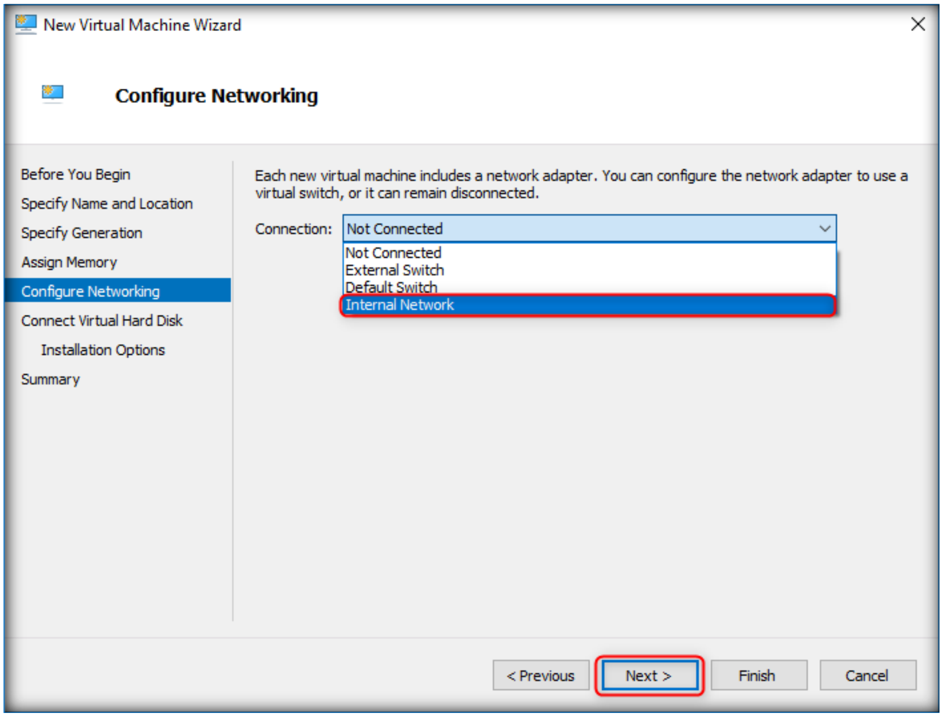
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 2048 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

10. In the next step, Configuring Network, select **Internal Network** adaptor from **Connection** drop-down list and click **Next**.



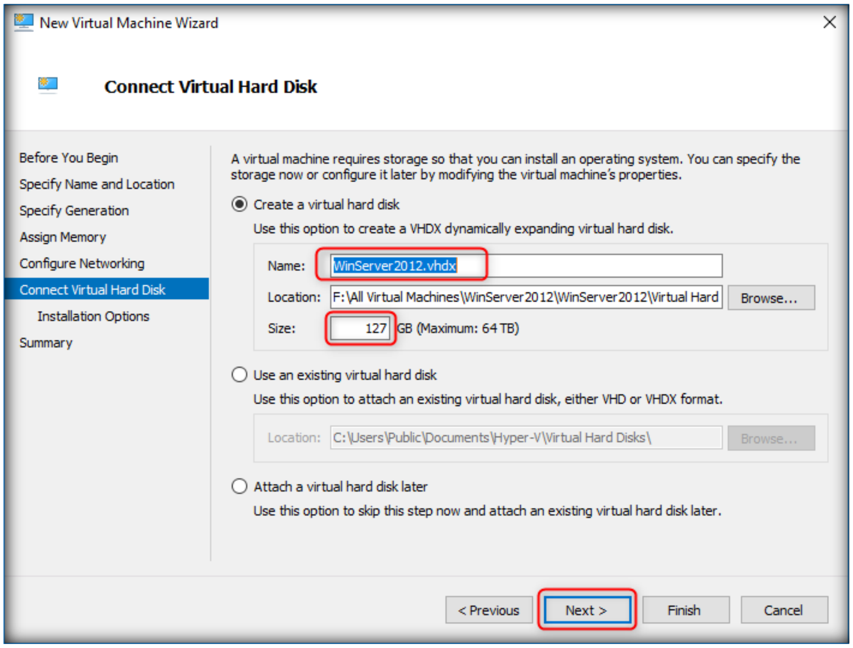
New Virtual Machine Wizard

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

11. Connect Virtual Hard Disk section appears, allocate default **127 GB** space for hard disk and click **Next**.



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: WinServer2012.vhdx

Location: F:\All Virtual Machines\WinServer2012\WinServer2012\Virtual Hard

Size: 127 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

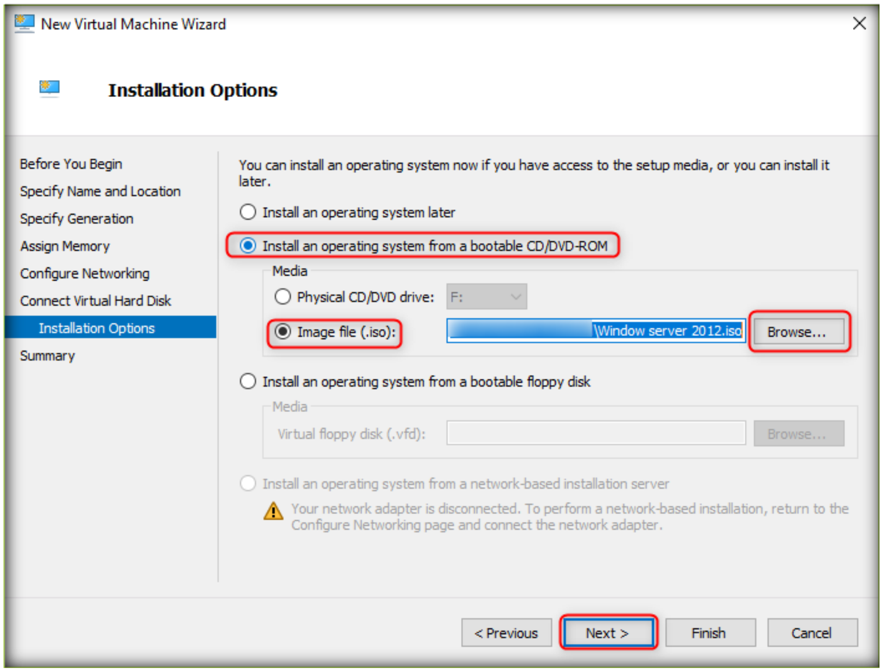
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

12. The **installation options** section appears, select **Install an operating system from a bootable CD/DVD-ROM** radio button.

- ○ If you have a Windows Server 2012 DVD choose Physical CD/DVD drive radio button and then click **Next**.
- ○ If you have a Windows Server 2012 ISO file, then choose Image file (.iso) radio button and click browse button to provide the path of ISO file and click **Next**.



New Virtual Machine Wizard

Installation Options

You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a bootable CD/DVD-ROM

Media

○ Physical CD/DVD drive: F:

● Image file (.iso): Window server 2012.iso

○ Install an operating system from a bootable floppy disk

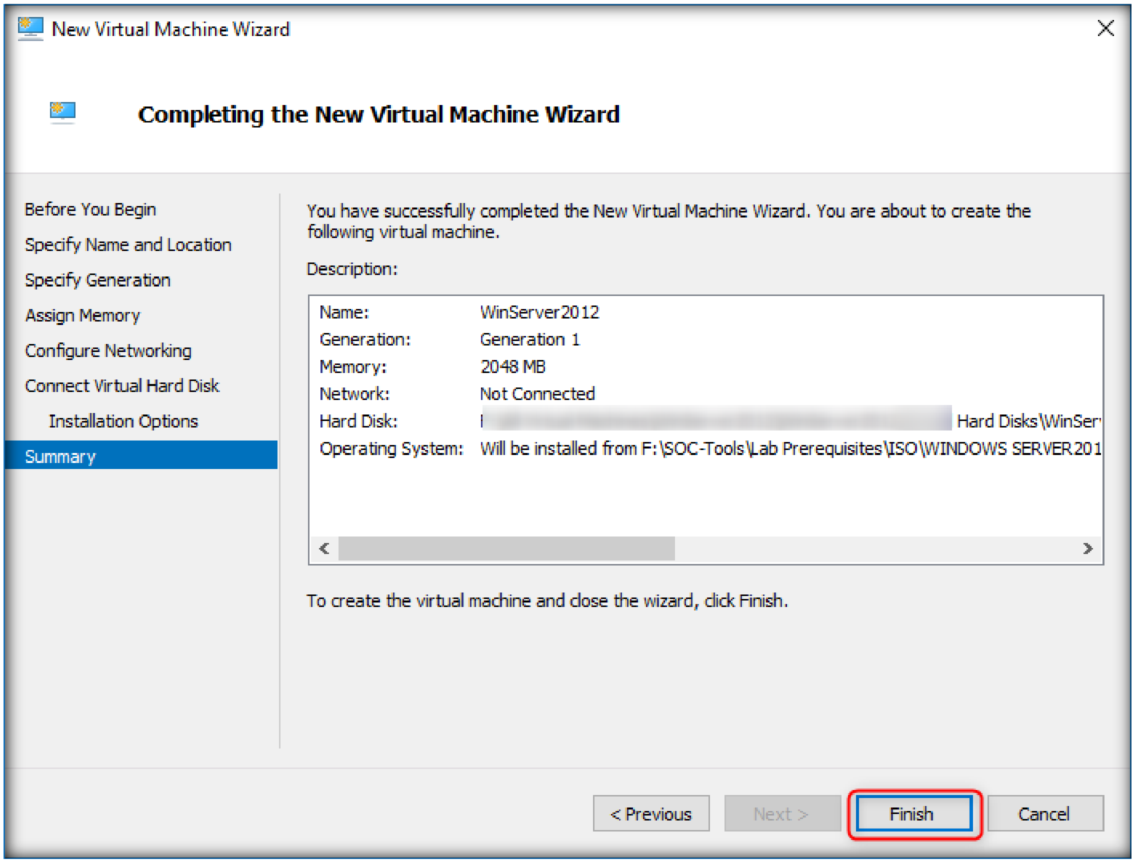
Media

Virtual floppy disk (.vfd):

○ Install an operating system from a network-based installation server

⚠ Your network adapter is disconnected. To perform a network-based installation, return to the Configure Networking page and connect the network adapter.

13. New Virtual Machine Wizard appears with summary information. Click **Finish**.



You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

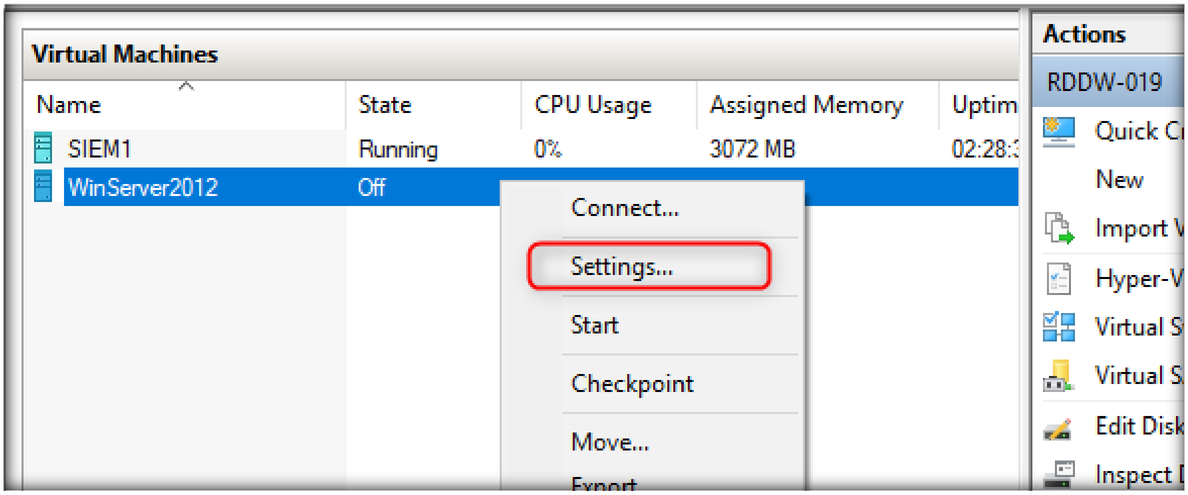
Description:

Name:	WinServer2012
Generation:	Generation 1
Memory:	2048 MB
Network:	Not Connected
Hard Disk:	I [redacted] Hard Disks\WinSer
Operating System:	Will be installed from F:\SOC-Tools\Lab Prerequisites\ISO\WINDOWS SERVER201

To create the virtual machine and close the wizard, click Finish.

14. Hyper-V Manager creates **Windows Server 2012** virtual machine profile.

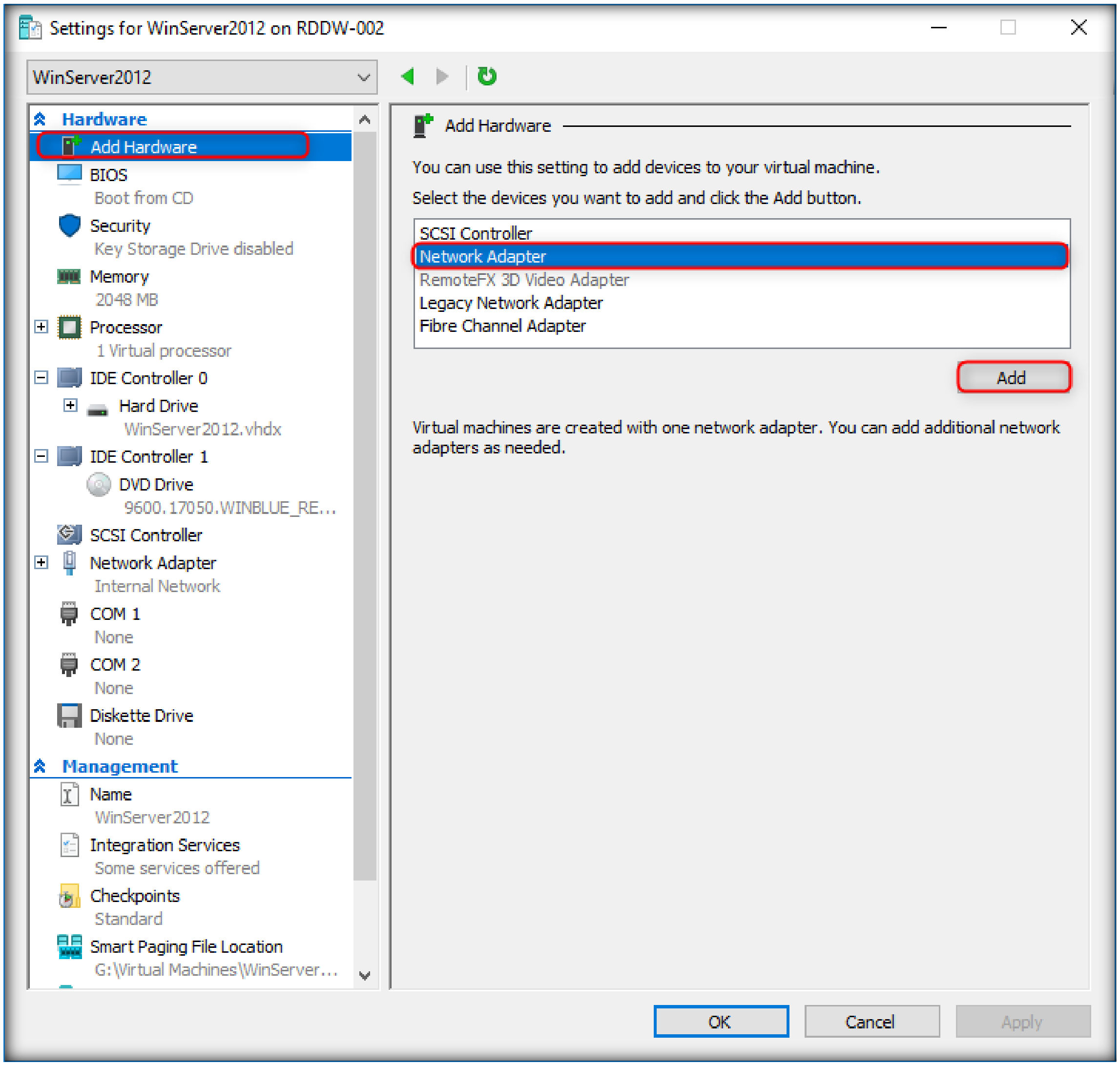
15. In **Hyper-V Manager** main window, you see a new virtual machine named **WinServer2012**. Right-click on the newly created virtual machine and click **Settings** from the context menu.



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptim
SIEM1	Running	0%	3072 MB	02:28:3
WinServer2012	Off			

16. Setting for **WinServer2012** window will open, click on **Add Hardware** and select **Network Adapter**, then click **Add**.



Settings for WinServer2012 on RDDW-002

Add Hardware

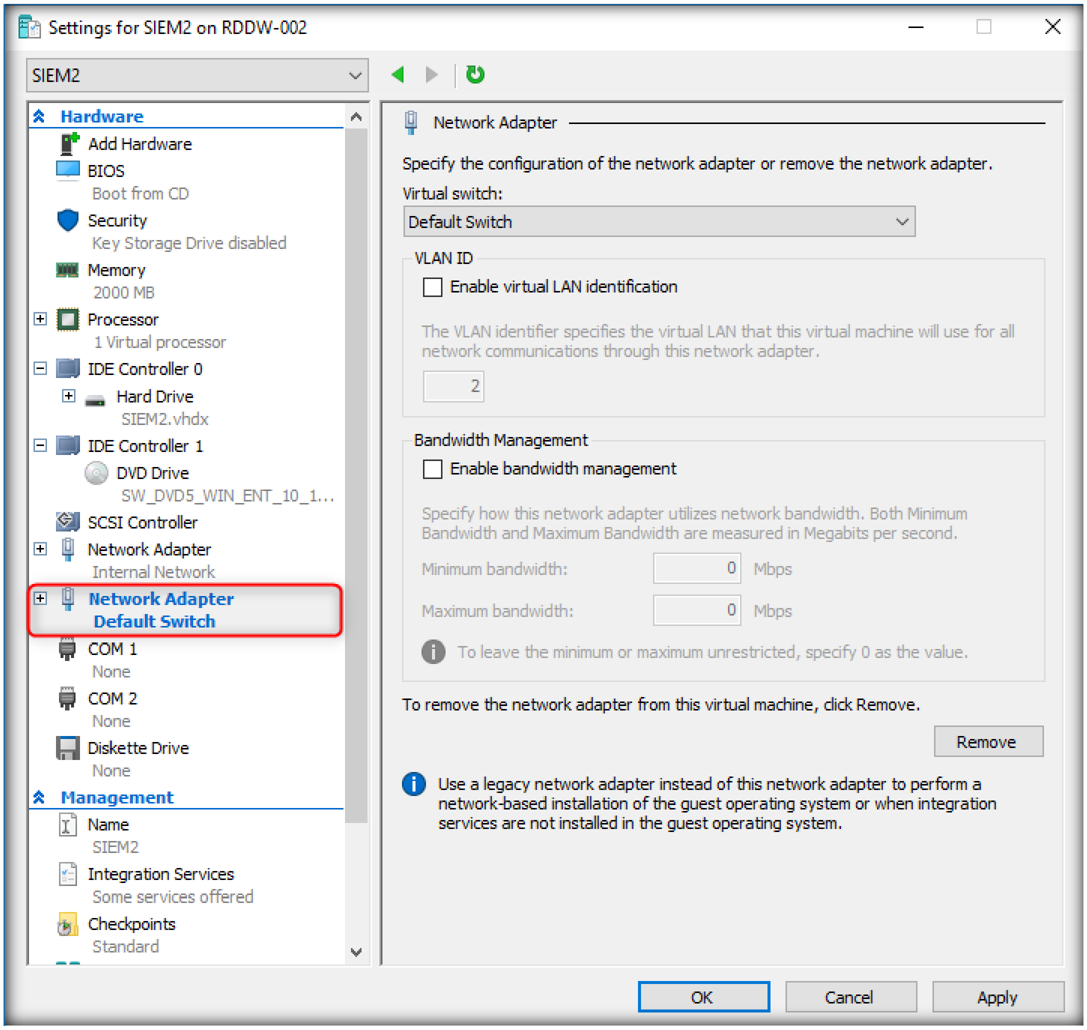
You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

SCSI Controller
Network Adapter
RemoteFX 3D Video Adapter
Legacy Network Adapter
Fibre Channel Adapter

Virtual machines are created with one network adapter. You can add additional network adapters as needed.

17. Select **Default Switch** from the **Virtual switch** dropdown. You will see **Default Switch Network Adaptor** added for **WinServer2012**.



Settings for SIEM2 on RDDW-002

SIEM2

Hardware

- Add Hardware
- BIOS
  Boot from CD
- Security
  Key Storage Drive disabled
- Memory
  2000 MB
- Processor
  1 Virtual processor
- IDE Controller 0
  - Hard Drive
    SIEM2.vhdx
- IDE Controller 1
  - DVD Drive
    SW_DVD5_WIN_ENT_10_1...
- SCSI Controller
- Network Adapter
  Internal Network
- **Network Adapter**
  Default Switch
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management

- Name
  SIEM2
- Integration Services
  Some services offered
- Checkpoints
  Standard

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch:
Default Switch

VLAN ID

□ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

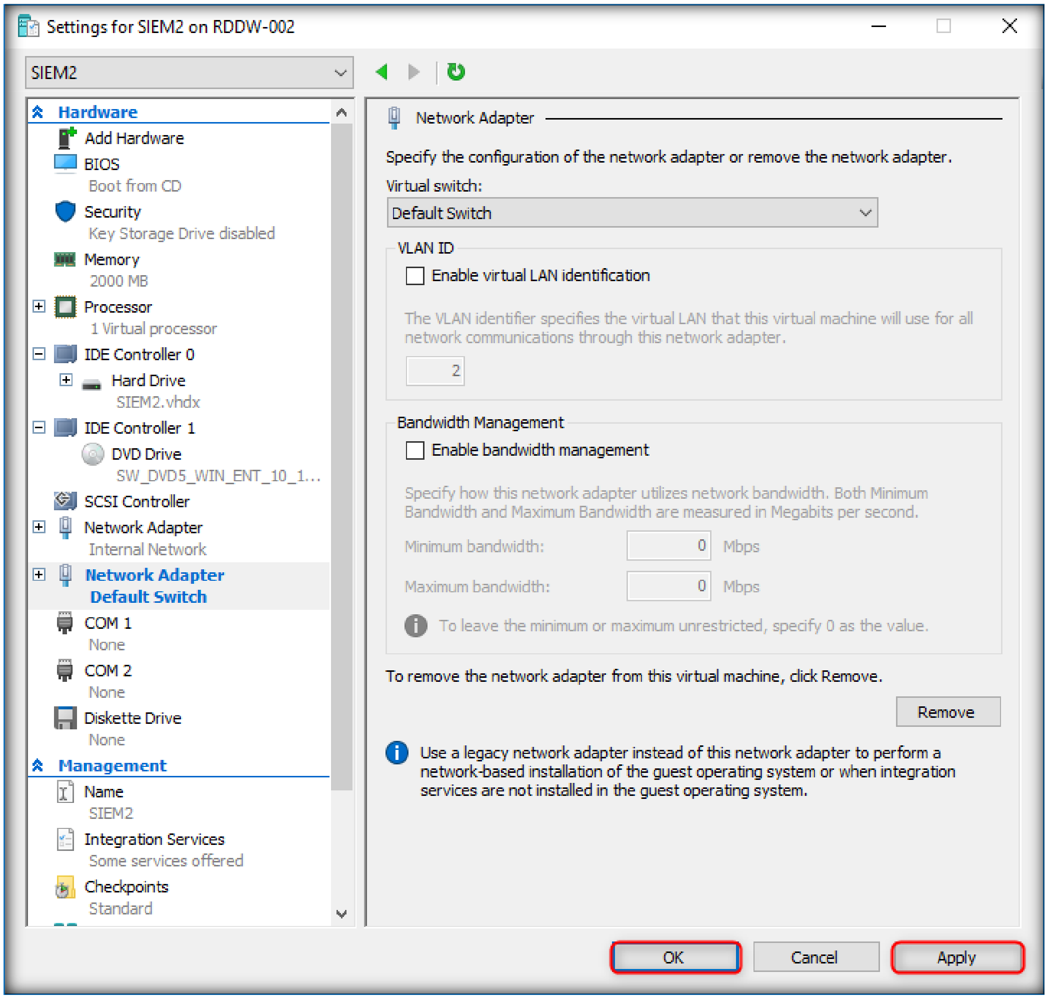
Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

18. Click **Apply** and **OK**.



Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Default Switch

VLAN ID

☐ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

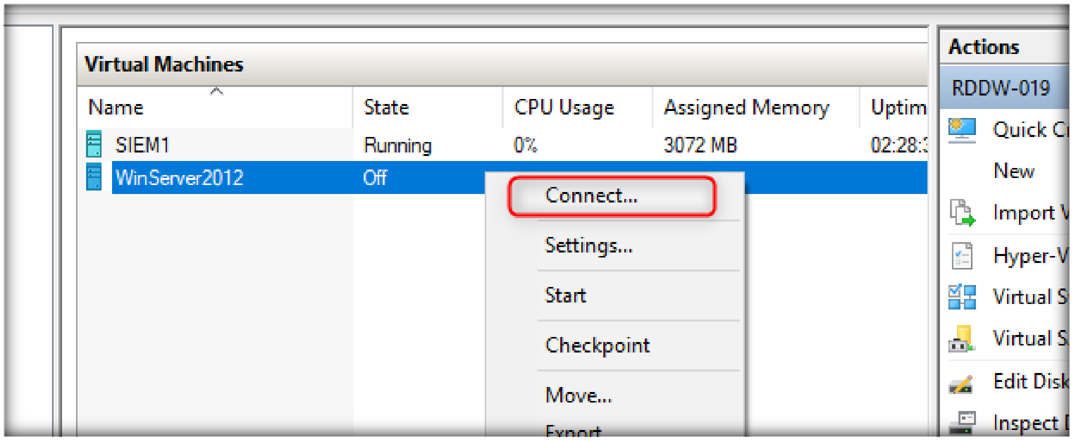
Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

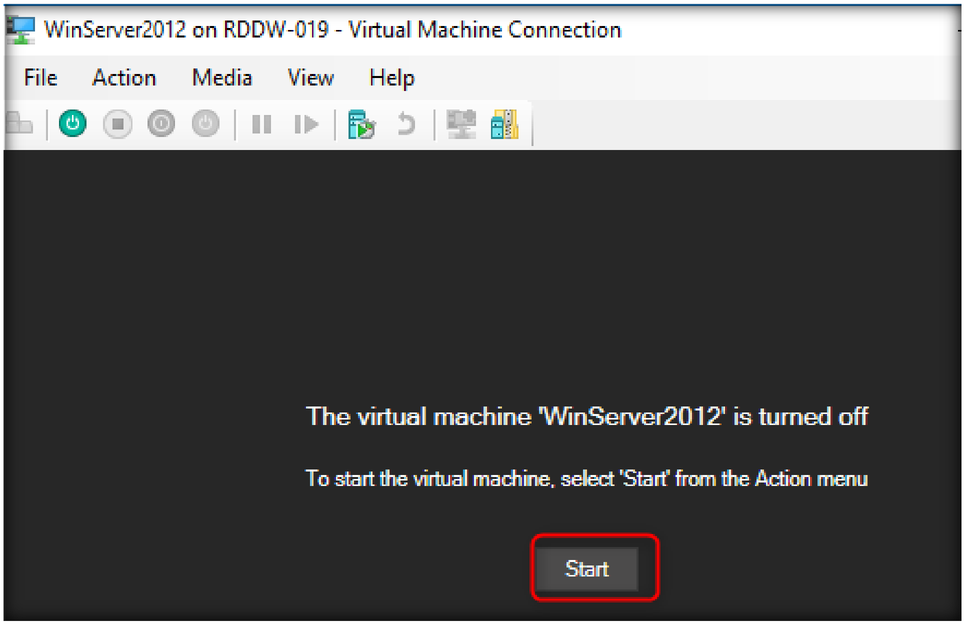
19. In **Hyper-V Manager** main window, you see a new virtual machine named **WinServer2012.** Right-click on the newly created virtual machine and click **Connect** from the context menu.



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptim
SIEM1	Running	0%	3072 MB	02:28::
WinServer2012	Off			

20. **WinServer2012** Virtual Machine window appears, click **Start** button as shown in the screenshot.

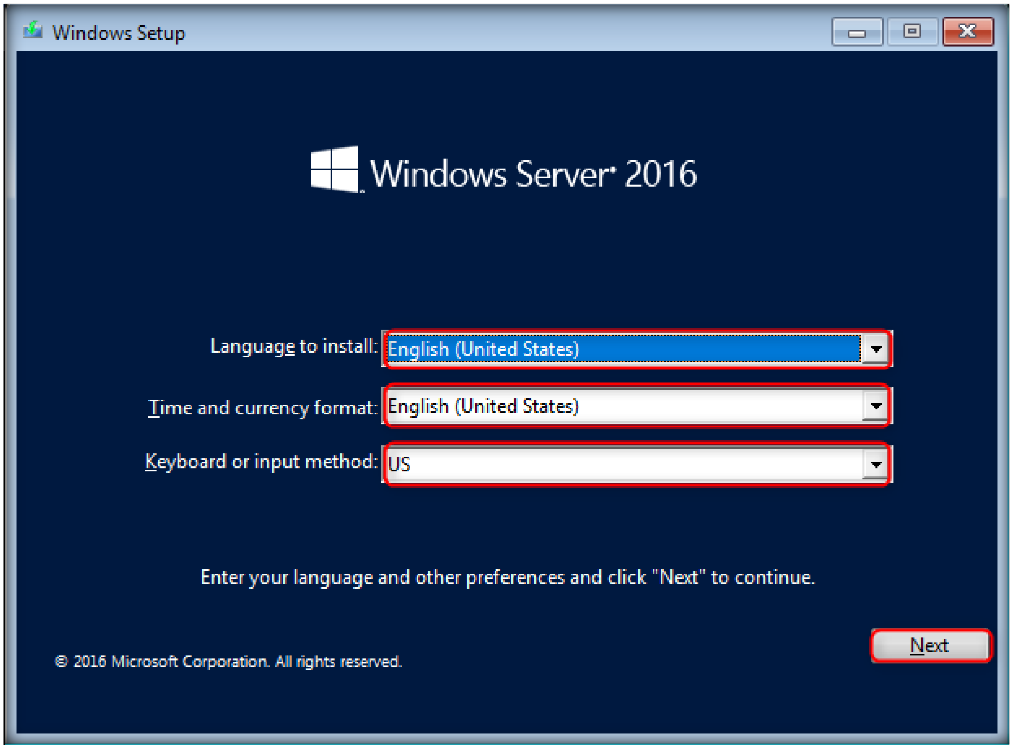


WinServer2012 on RDDW-019 - Virtual Machine Connection

The virtual machine 'WinServer2012' is turned off

To start the virtual machine, select 'Start' from the Action menu

21. When WinServer2012 virtual machine is turned on, **Windows Setup** window will appear. Fill the required details and click **Next**.



Windows Setup

Language to install: English (United States)

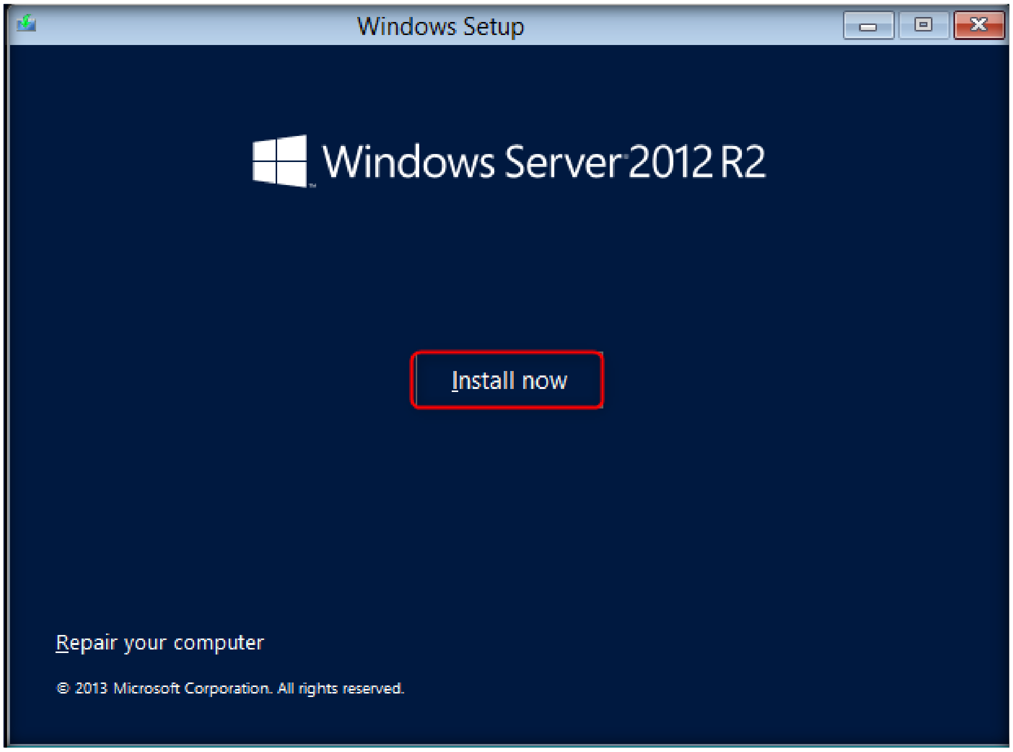
Time and currency format: English (United States)

Keyboard or input method: US

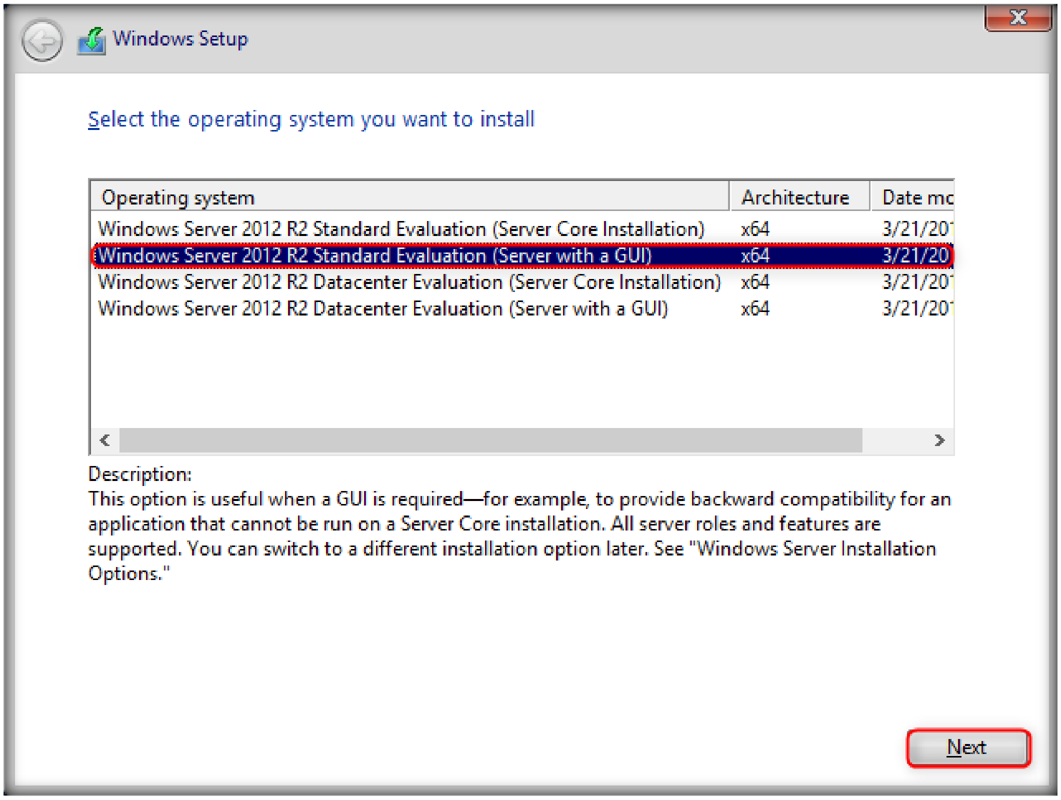
Enter your language and other preferences and click "Next" to continue.

© 2016 Microsoft Corporation. All rights reserved.

22. Click **Install Now** in the Windows Setup to continue installation.



23. In the **Select the operating system you want to install** select **Windows Server 2012 R2 Standard Evaluation (Server with a GUI)** option and click **Next**.

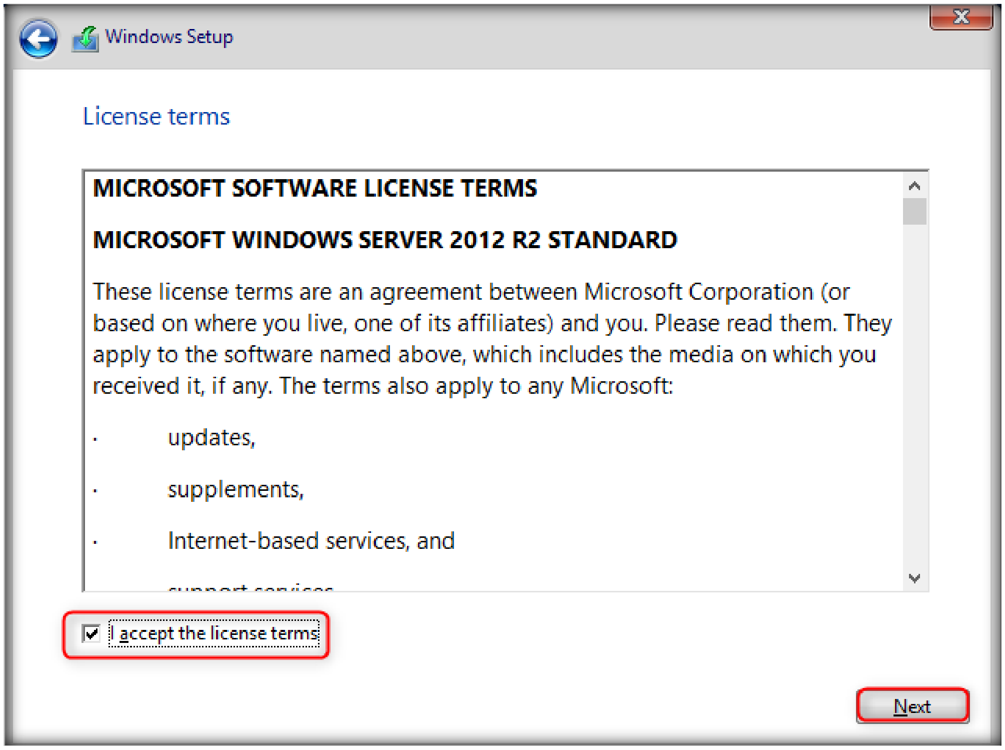


Select the operating system you want to install

Operating system	Architecture	Date mc
Windows Server 2012 R2 Standard Evaluation (Server Core Installation)	x64	3/21/20
Windows Server 2012 R2 Standard Evaluation (Server with a GUI)	x64	3/21/20
Windows Server 2012 R2 Datacenter Evaluation (Server Core Installation)	x64	3/21/20
Windows Server 2012 R2 Datacenter Evaluation (Server with a GUI)	x64	3/21/20

Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. You can switch to a different installation option later. See "Windows Server Installation Options."

24. Check **I accept the license terms** and click **Next**.



Windows Setup

License terms

MICROSOFT SOFTWARE LICENSE TERMS

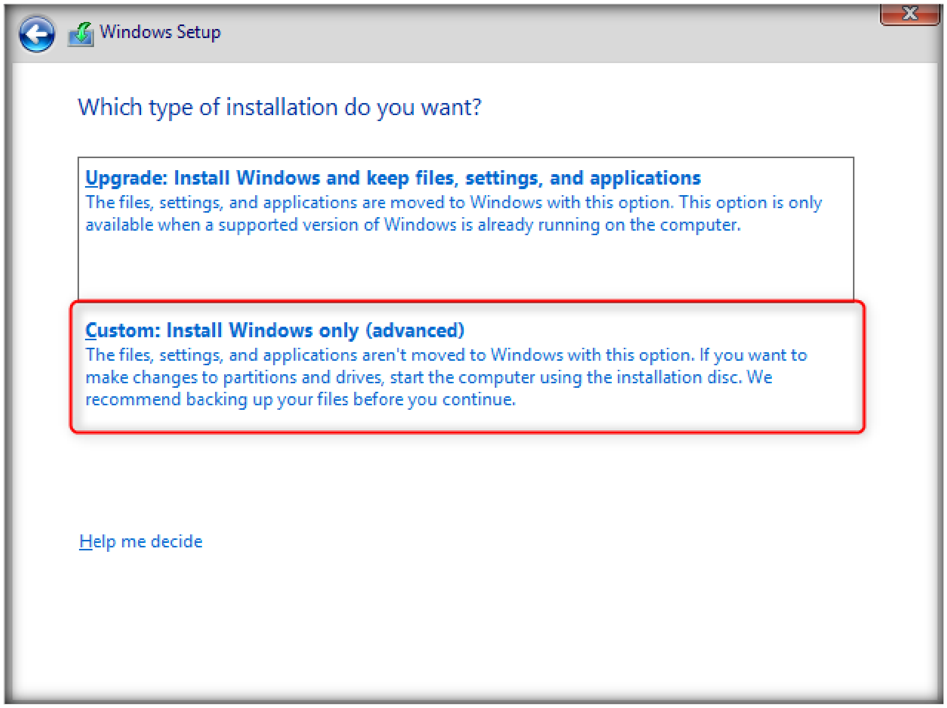
MICROSOFT WINDOWS SERVER 2012 R2 STANDARD

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft:

- updates,
- supplements,
- Internet-based services, and
- support services

☑ I accept the license terms

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



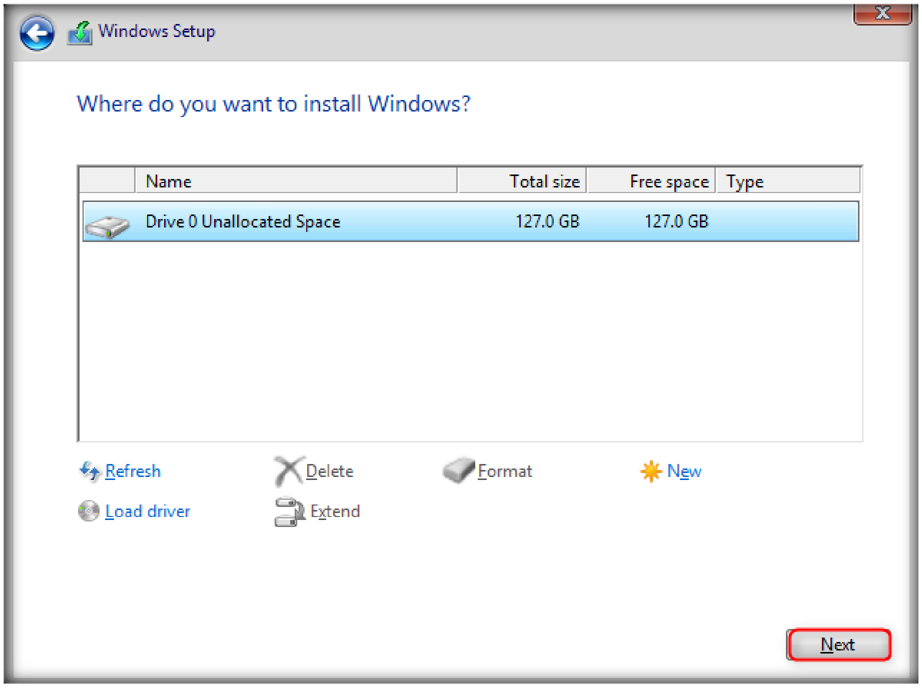
Windows Setup

Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

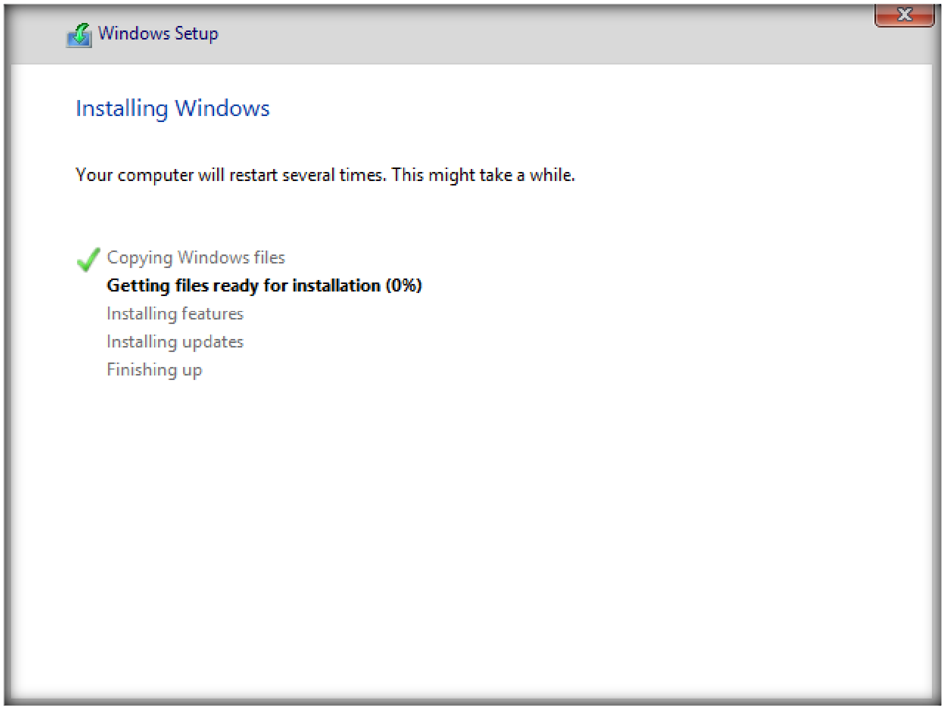
26. Click **Next**.



Where do you want to install Windows?

	Name	Total size	Free space	Type
	Drive 0 Unallocated Space	127.0 GB	127.0 GB	

27. Installing Windows screen appears; wait until it completes the installation.



Installing Windows

Your computer will restart several times. This might take a while.

✓ Copying Windows files

Getting files ready for installation (0%)

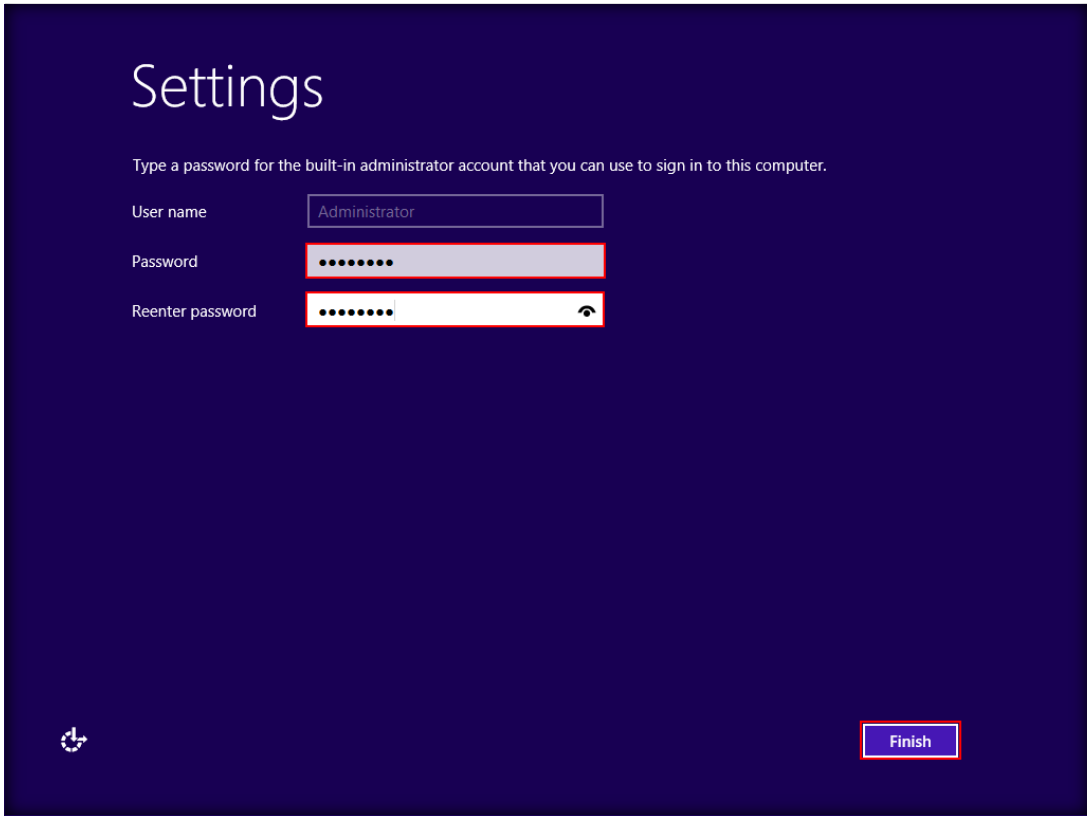
Installing features

Installing updates

Finishing up

28. Once the installation is completed machine will restart.

29. Settings window will appear, enter **admin@123** as **Password** and **Reenter password** for the Administrator account, and click **Finish.**



Settings

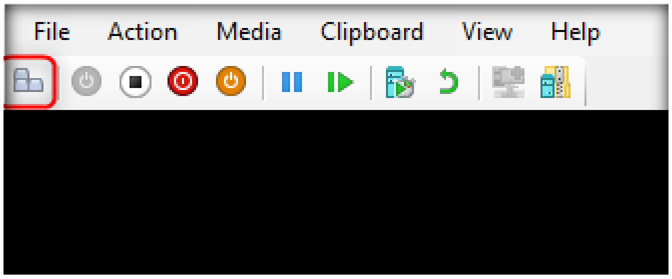
Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

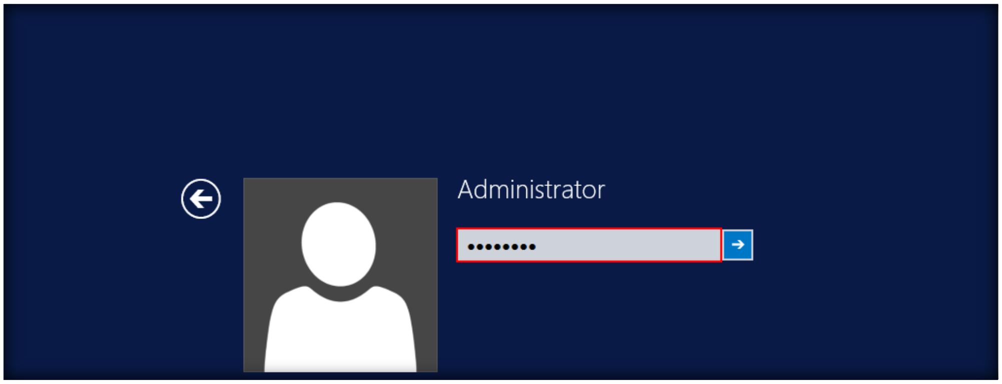
Password: ••••••••

Reenter password: ••••••••

30. Click **Ctrl+Alt+Delete** icon from the menu to login to **WinServer2012**.



31. Login screen appears. Type the password (**admin@123**) and press **Enter**.

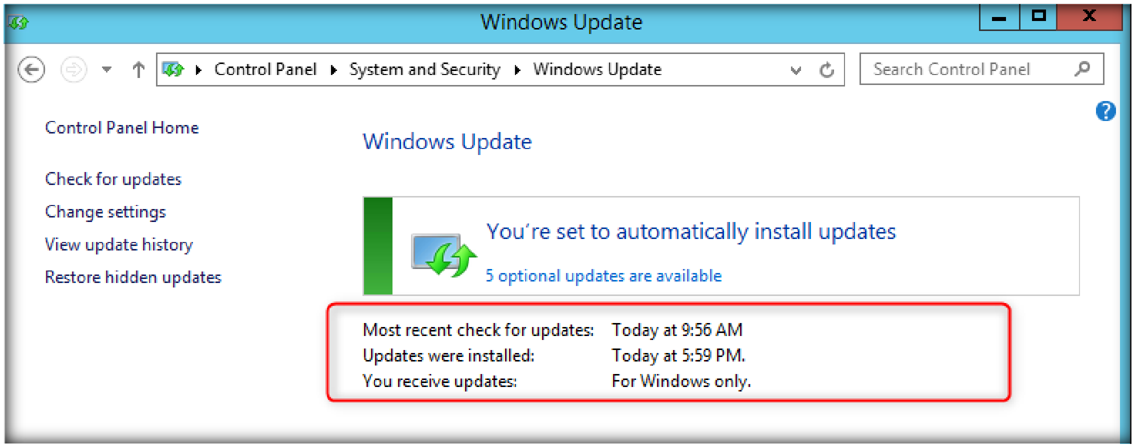


Administrator

••••••••

32. Now, check for the system updates and if found any, update the **Windows Server 2012** virtual machine to the latest.

    Note: Installing the updates might take some time.



You're set to automatically install updates

5 optional updates are available

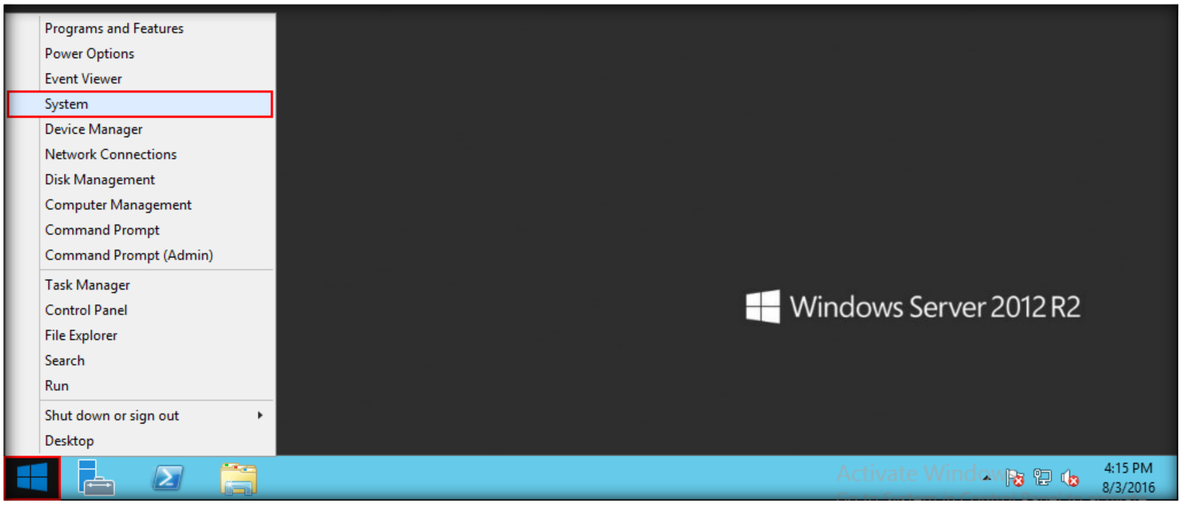
Most recent check for updates: Today at 9:56 AM

Updates were installed: Today at 5:59 PM.

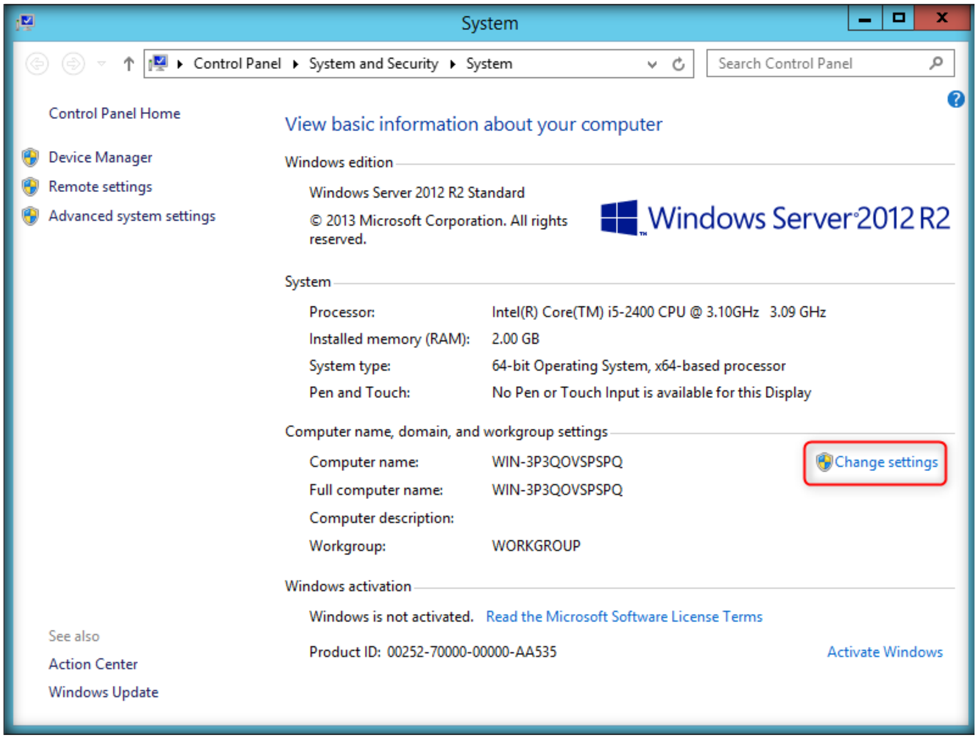
You receive updates: For Windows only.

CT#7.2: Changing the Computer Name

1. Close the Server Manager window that opens. Right-click **Start** icon and click on **System**.



2. In the System window, click **Change settings**.



System

Control Panel ▸ System and Security ▸ System

Search Control Panel

Control Panel Home

Device Manager

Remote settings

Advanced system settings

View basic information about your computer

Windows edition

Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

System

Processor: Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz 3.09 GHz

Installed memory (RAM): 2.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: WIN-3P3QOVSPSPQ

Full computer name: WIN-3P3QOVSPSPQ

Computer description:

Workgroup: WORKGROUP

Change settings

Windows activation

Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00252-70000-00000-AA535

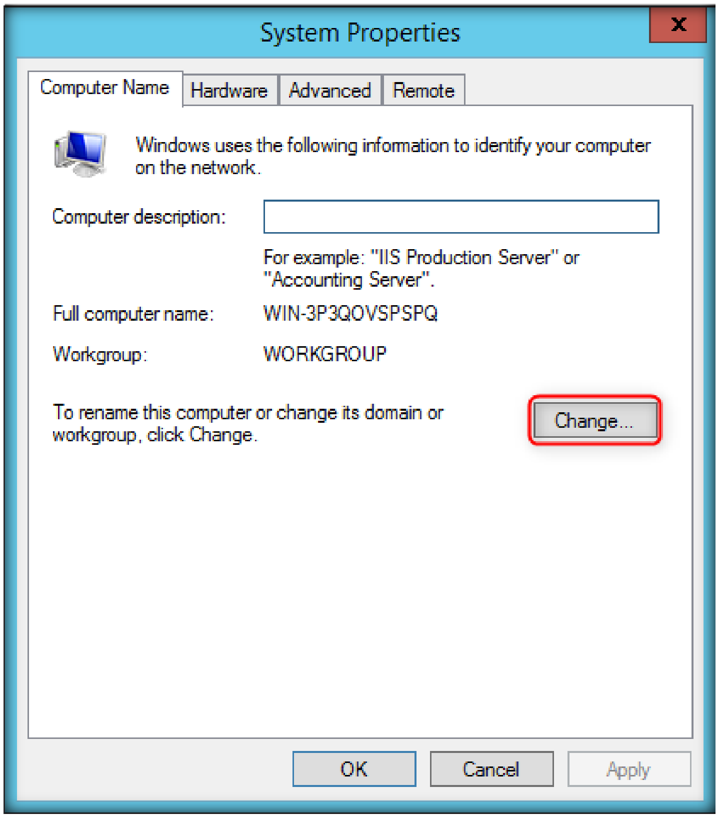
Activate Windows

See also

Action Center

Windows Update

3. In the **Computer Name** tab of the System Properties window, click **Change**.



System Properties

Computer Name | Hardware | Advanced | Remote

Windows uses the following information to identify your computer on the network.

Computer description:

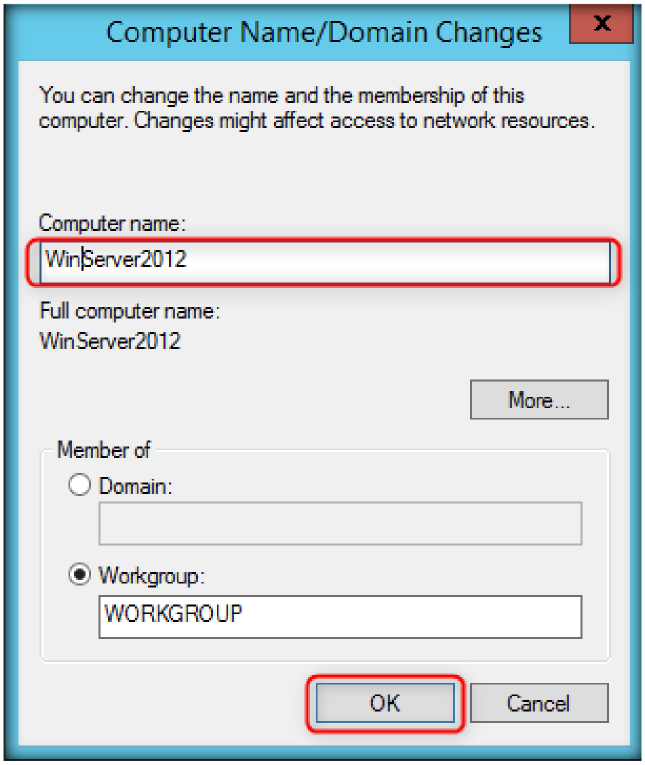
For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-3P3QOVSPSPQ

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

4. In the **Computer name** field, enter **WinServer2012** and click **OK**.



Computer Name/Domain Changes

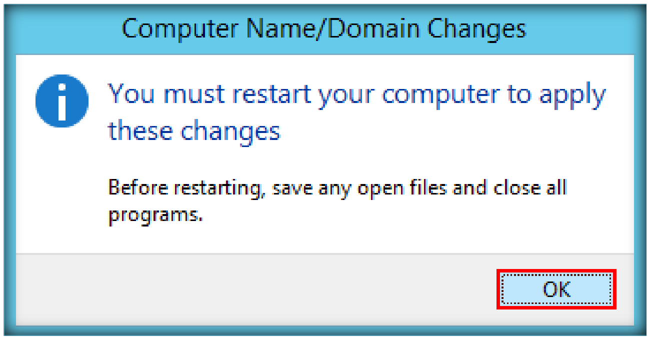
You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
WinServer2012

Full computer name:
WinServer2012

Member of
○ Domain:
● Workgroup:
WORKGROUP

5. When prompted to restart the system, click **OK**.

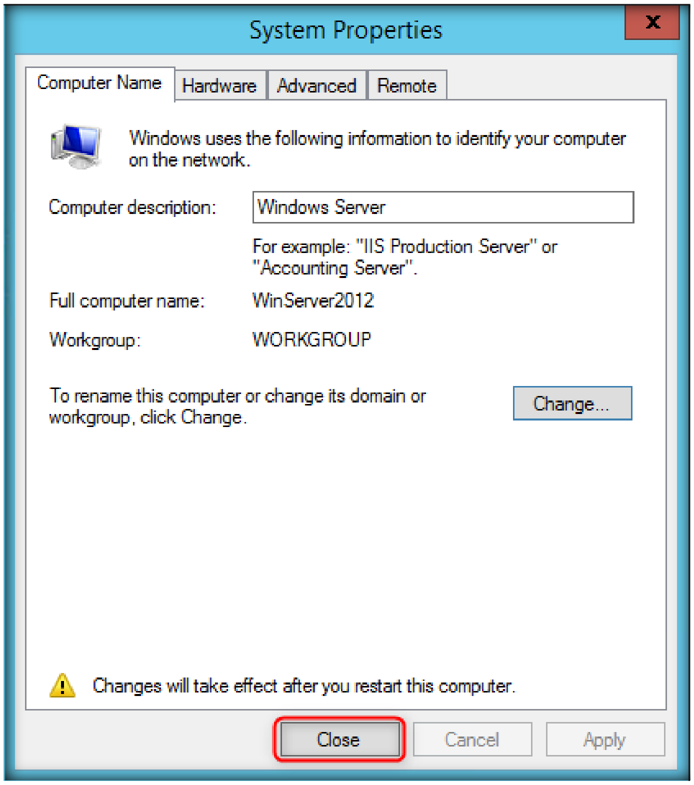


Computer Name/Domain Changes

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

6. You will be returned to System Properties window, click **Close**.



Windows uses the following information to identify your computer on the network.

Computer description: Windows Server

For example: "IIS Production Server" or "Accounting Server".

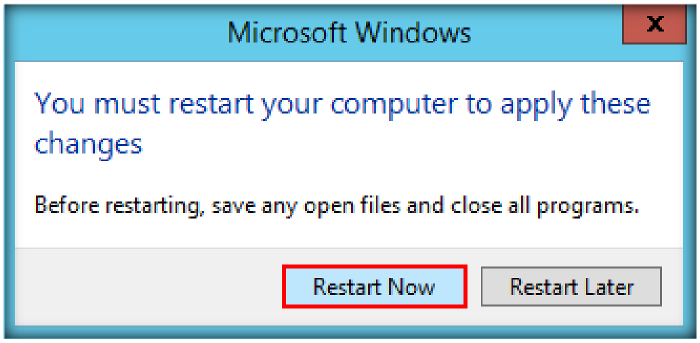
Full computer name: WinServer2012

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

Changes will take effect after you restart this computer.

7. You will be prompted to restart the system, click **Restart Now**.

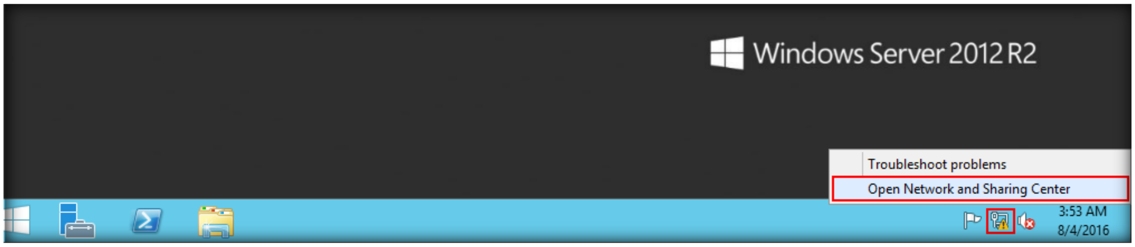


You must restart your computer to apply these changes

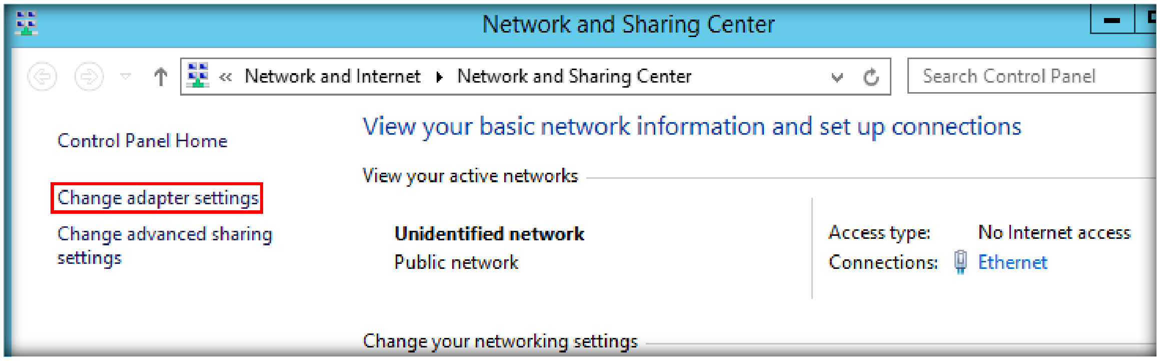
Before restarting, save any open files and close all programs.

CT#7.3: Configuring Static IP Address

1. Login as Administrator. Close the **Server Manager** window that opens after successful sign in, right-click on **Network** icon (lower right corner of the desktop) and click **Open Network and Sharing Center** from the context menu.

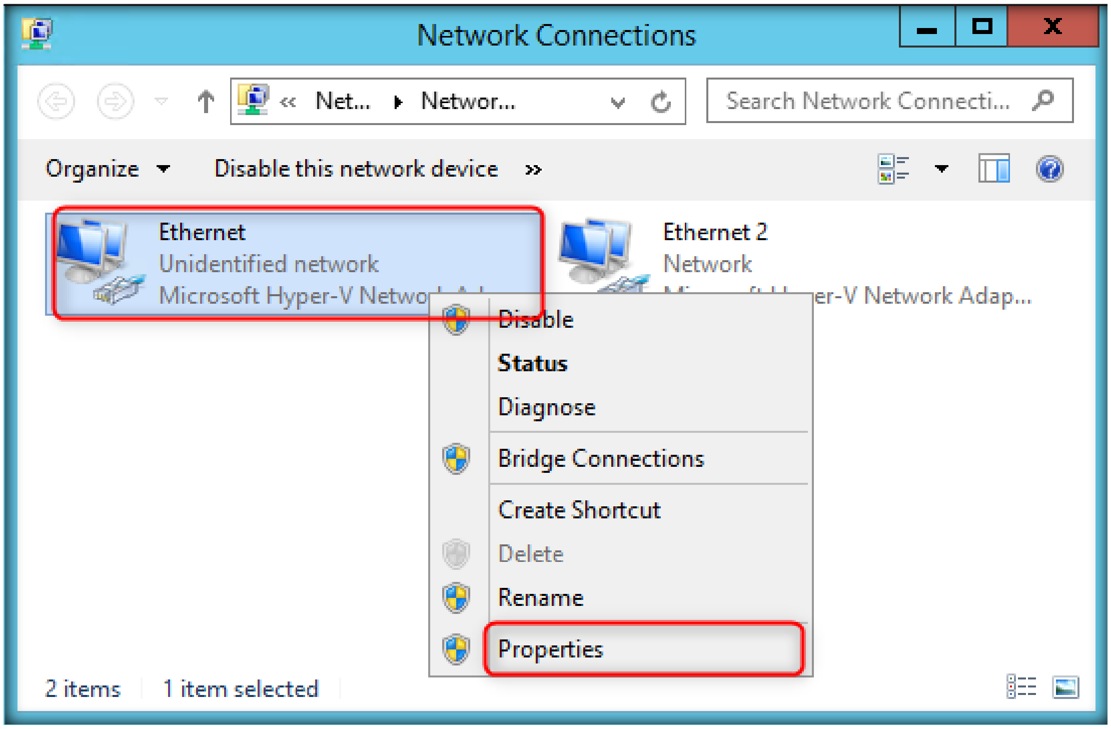


2. Network and Sharing Center window appear, click **Change adapter settings** link from the left pane.

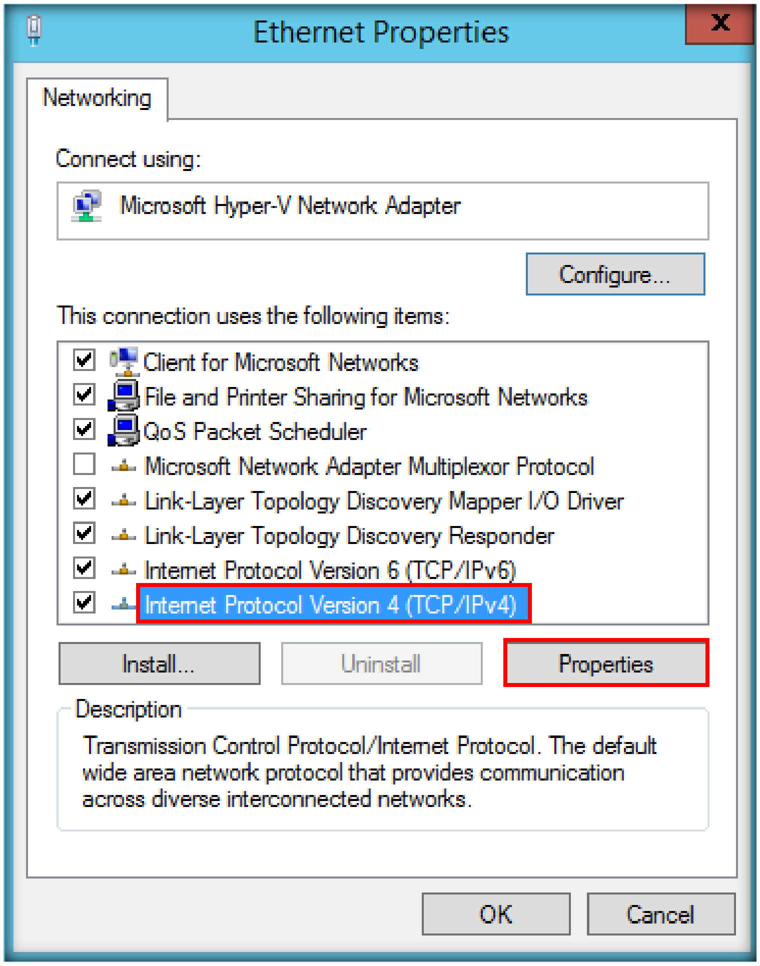

Network and Sharing Center
« Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Unidentified network
Public network
Access type: No Internet access
Connections: Ethernet
Change your networking settings

3. In the Network Connections window, right-click on Unidentified network (**Ethernet**) adapter and click **Properties** from the context menu.

   Note: The Name of Unidentified network may vary.



4. Ethernet adapter Properties window appears; and select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties.**

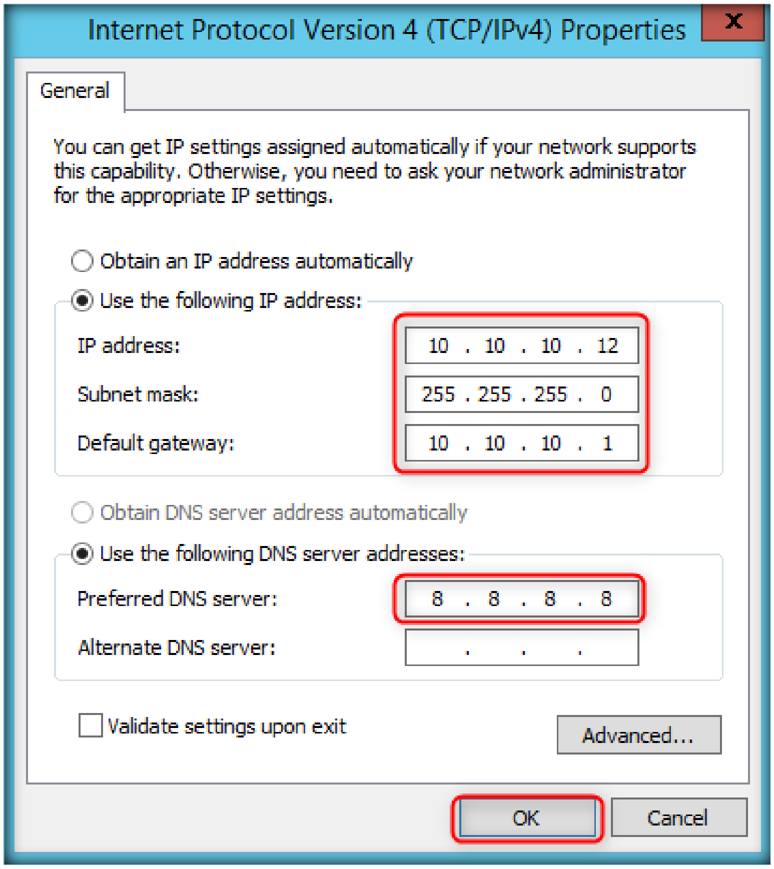


Ethernet Properties
Networking
Connect using:
Microsoft Hyper-V Network Adapter
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
Install...
Uninstall
Properties
Description
OK
Cancel

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select **Use the following IP address** and **Use the following DNS server addresses** radio buttons, and type the following values as shown in the screenshot and click **OK**.
    - IP address: **10.10.10.12**
    - Subnet mask: **255.255.255.0**
    - Default gateway: **10.10.10.2**
    - Preferred DNS server: **8.8.8.8**

   Note: Once you click on **OK** button if Networks section appears on the right side of the desktop screen, and then click **Yes**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	10 . 10 . 10 . 12
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 10 . 10 . 1

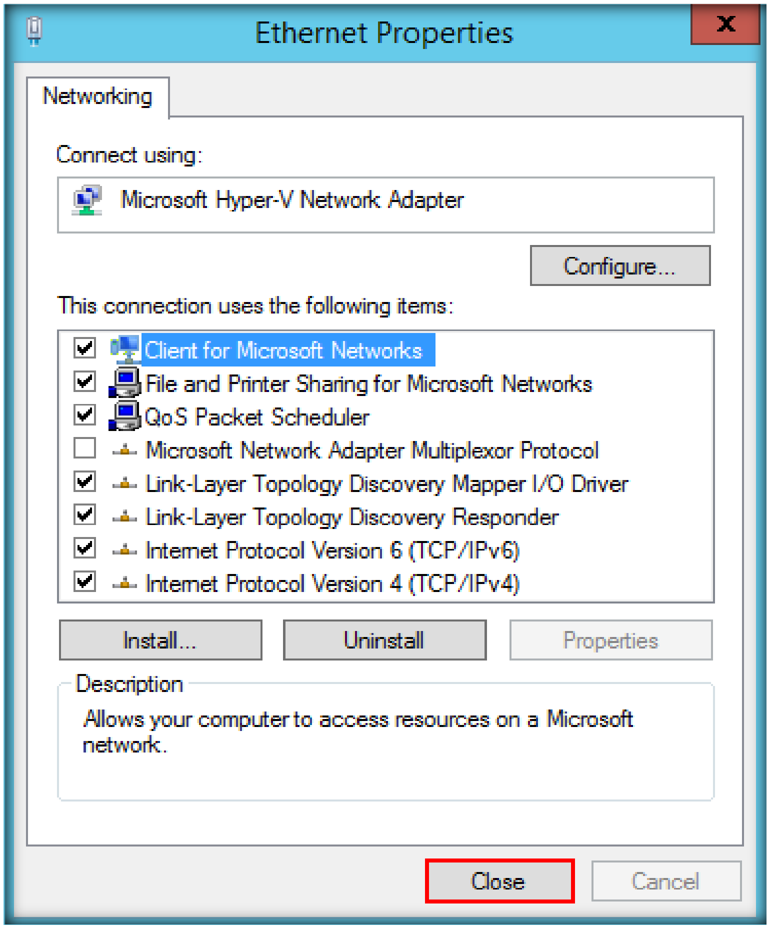
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	. . .

□ Validate settings upon exit

6. Click **Close** to close the Ethernet Properties window.



Connect using:

Microsoft Hyper-V Network Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

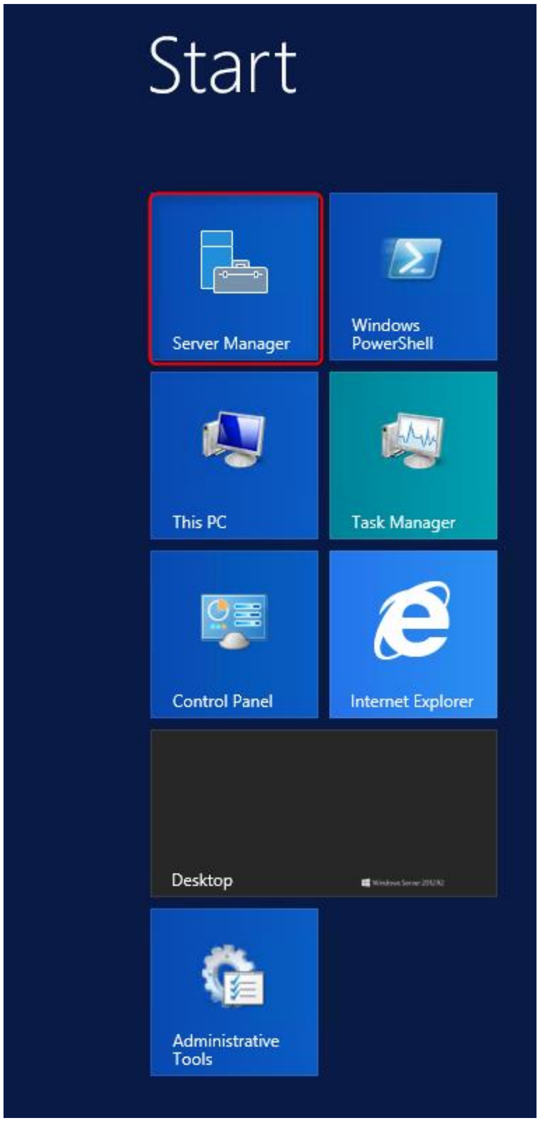
Description

Allows your computer to access resources on a Microsoft network.

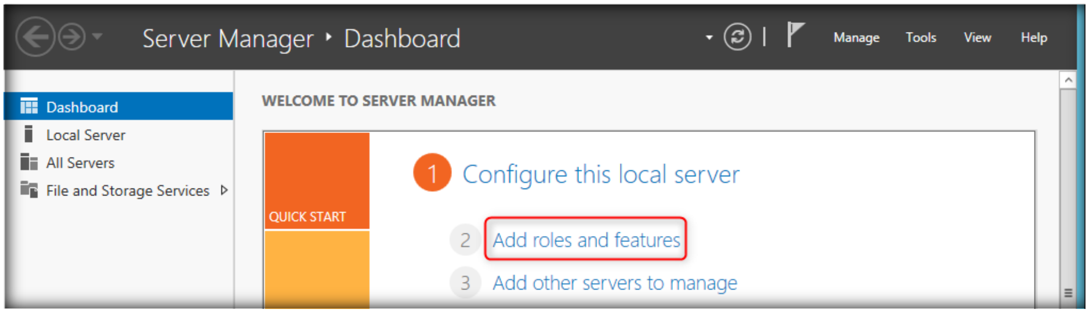
7. Now, check whether Windows Server 2012 is installed and working properly.

CT#7.4: Adding IIS (Internet Information Services) roles in Server Manager

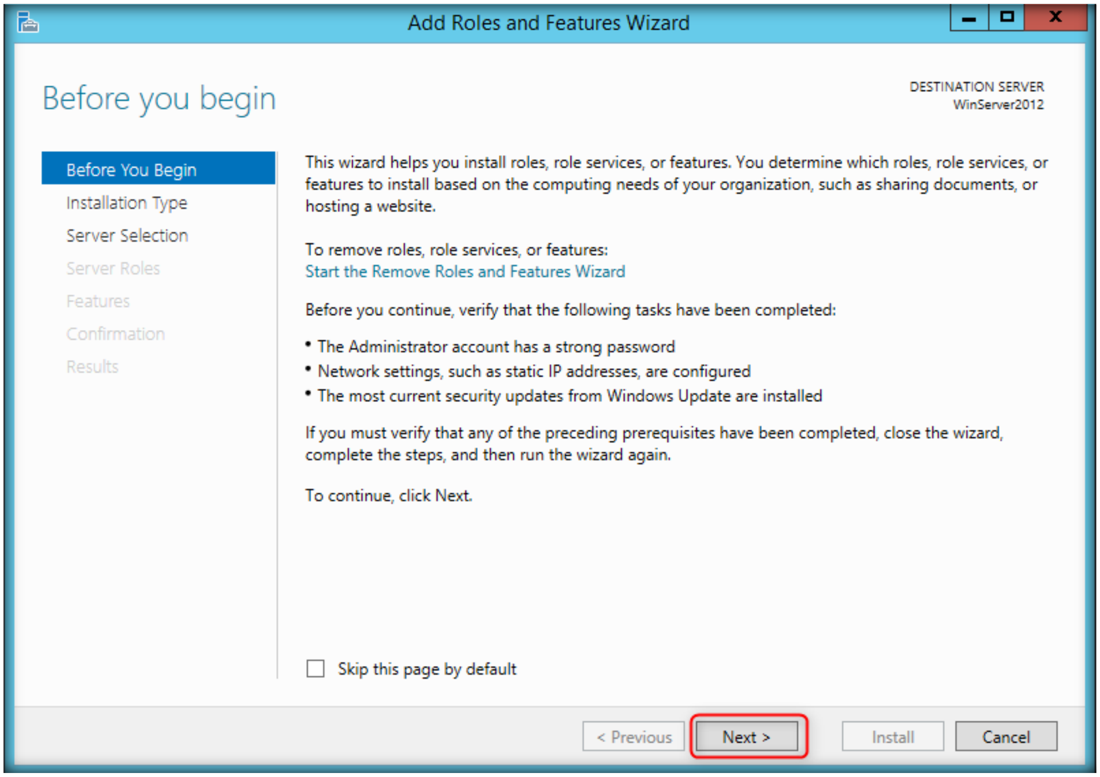
1. To open Server Manager, click **Start → Server Manager** icon.



2. In Server Manager **Dashboard**, click **Add Roles and Features.**


Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
1 Configure this local server
2 Add roles and features
3 Add other servers to manage

3. **Add Roles and Features Wizard** appears, click **Next**.



Before you begin

DESTINATION SERVER
WinServer2012

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

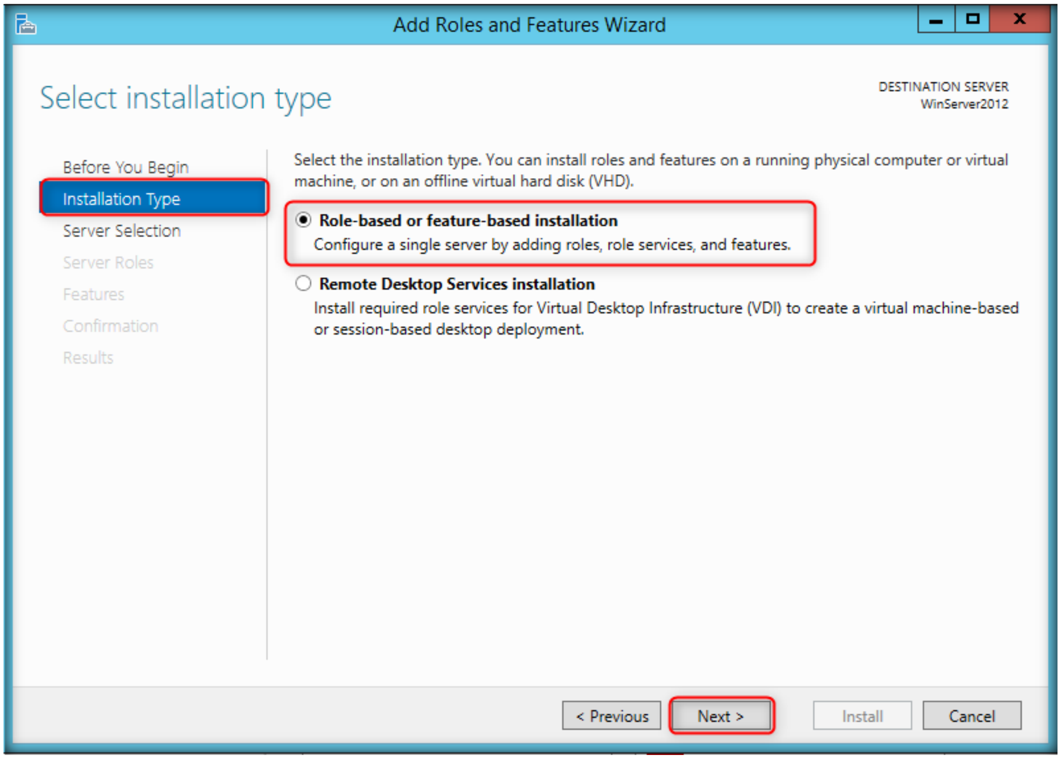
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

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



Select installation type

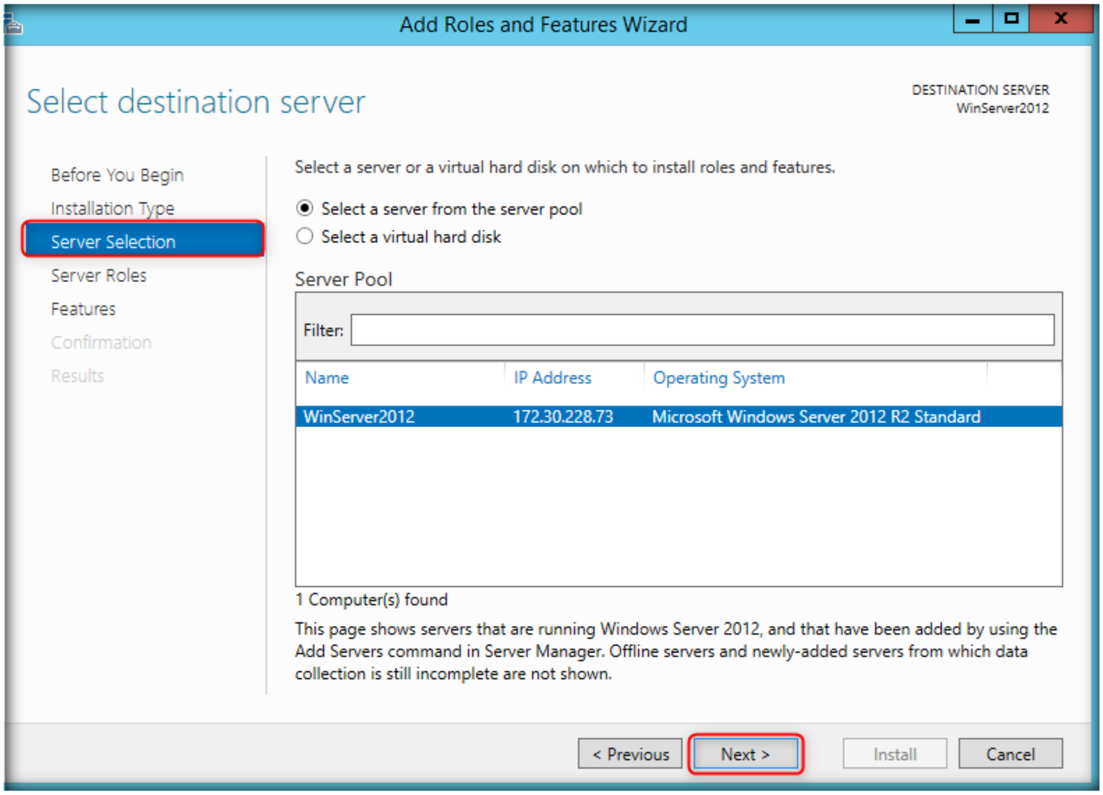
DESTINATION SERVER
WinServer2012

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

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



Select destination server

DESTINATION SERVER
WinServer2012

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

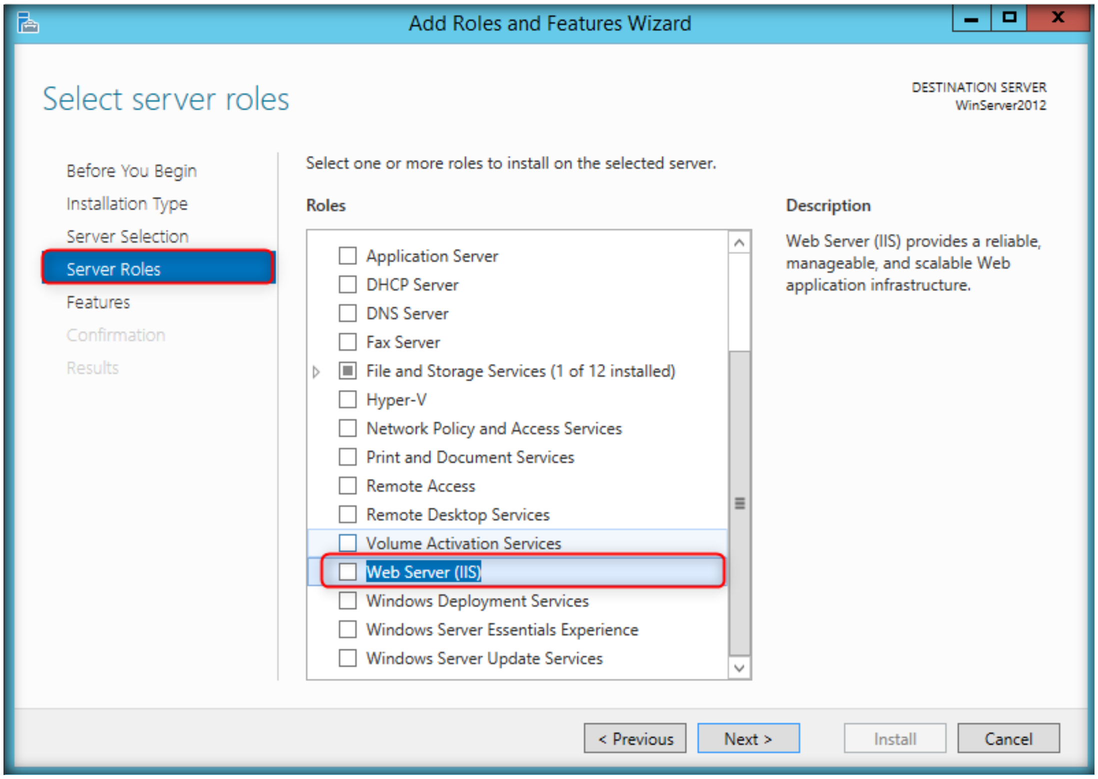
Filter:

Name	IP Address	Operating System
WinServer2012	172.30.228.73	Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

6. **Server Roles** section appears, click the check box of **Web Server (IIS)** role.



Select server roles

DESTINATION SERVER
WinServer2012

Select one or more roles to install on the selected server.

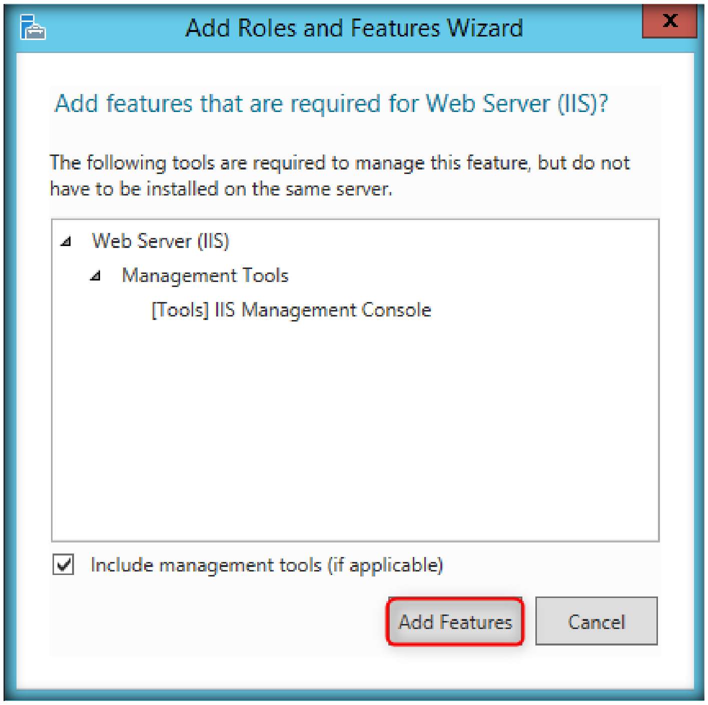
Roles

- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

7. **Add Roles and Features Wizard** window appears, click **Add Features**.



Add Roles and Features Wizard

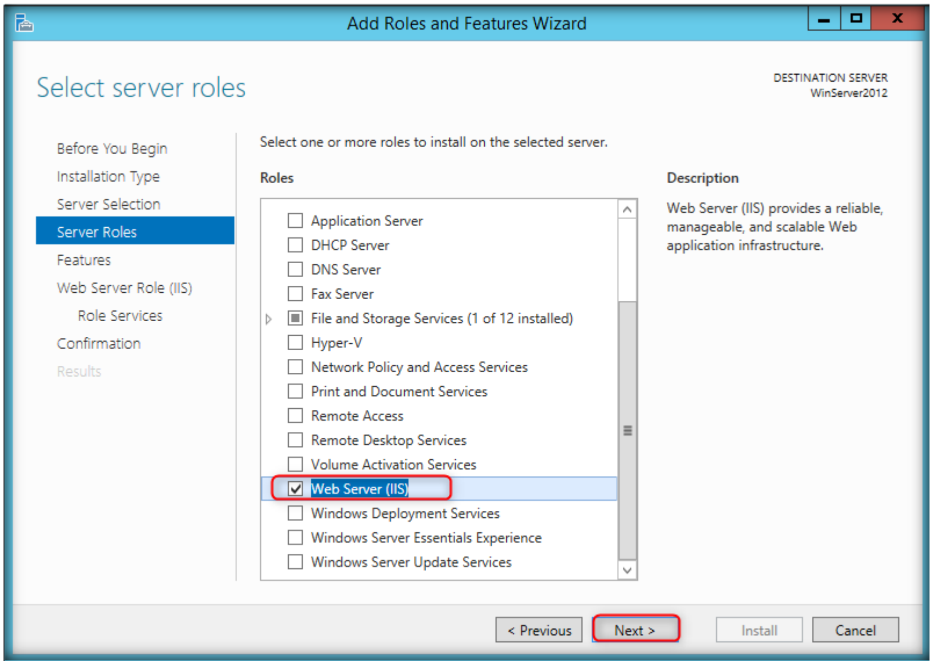
Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)

8. In the **Server Roles** section, you will observe the Web Server (IIS) option is checked. Click **Next**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WinServer2012

Select one or more roles to install on the selected server.

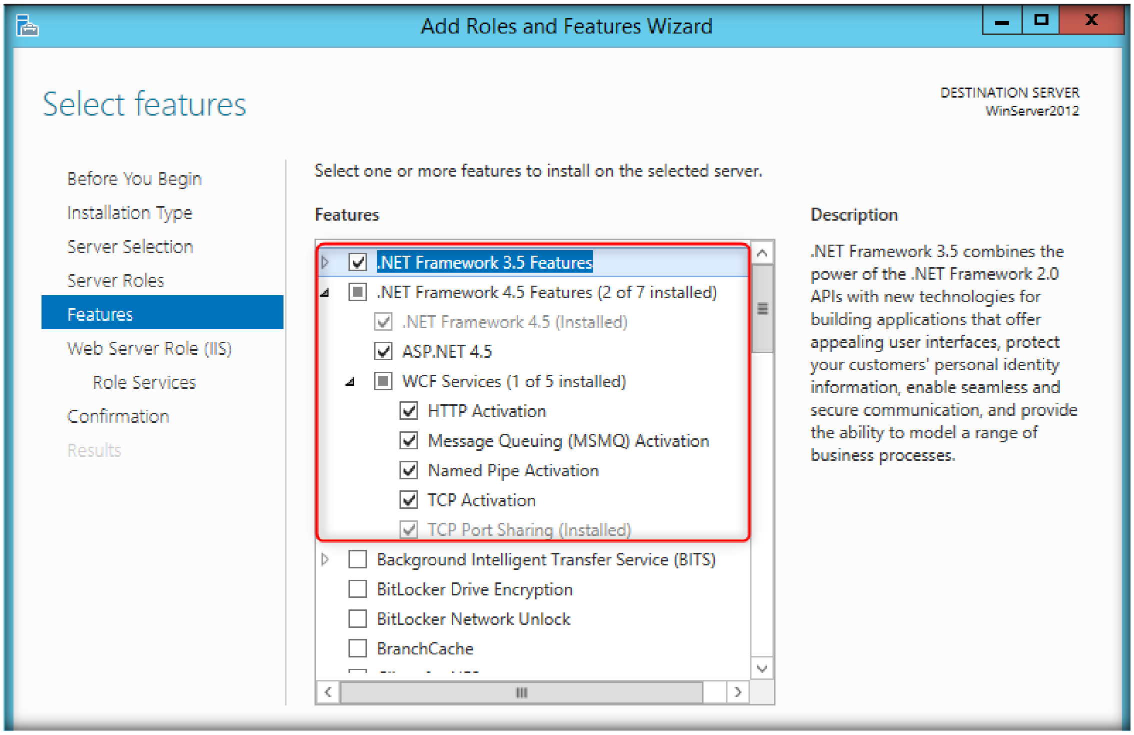
Roles

- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☑ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

9. **Features** section appears, select the checkboxes for **.NET Framework 3.5** feature, as well as all the checkboxes under **.NET Framework 4.6** Features.



Select features

DESTINATION SERVER
WinServer2012

Select one or more features to install on the selected server.

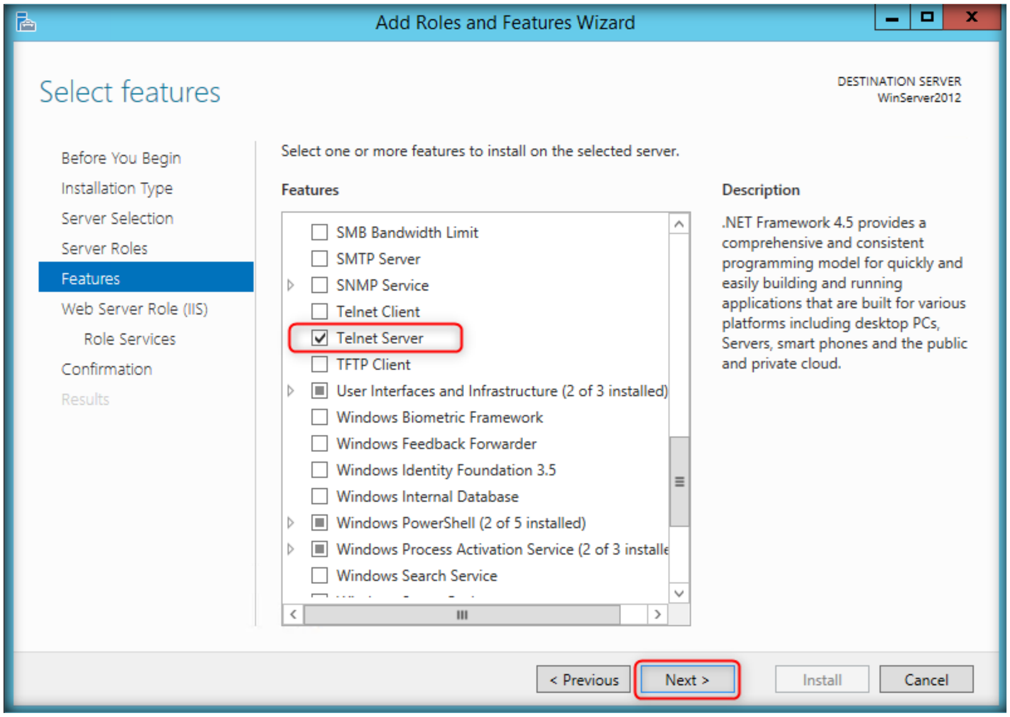
Features

- ☑ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
  - ☑ .NET Framework 4.5 (Installed)
  - ☑ ASP.NET 4.5
  - ▣ WCF Services (1 of 5 installed)
    - ☑ HTTP Activation
    - ☑ Message Queuing (MSMQ) Activation
    - ☑ Named Pipe Activation
    - ☑ TCP Activation
    - ☑ TCP Port Sharing (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

10. Scroll down and check **Telnet Server** feature option Click **Next**.



Select features

DESTINATION SERVER
WinServer2012

Select one or more features to install on the selected server.

Features

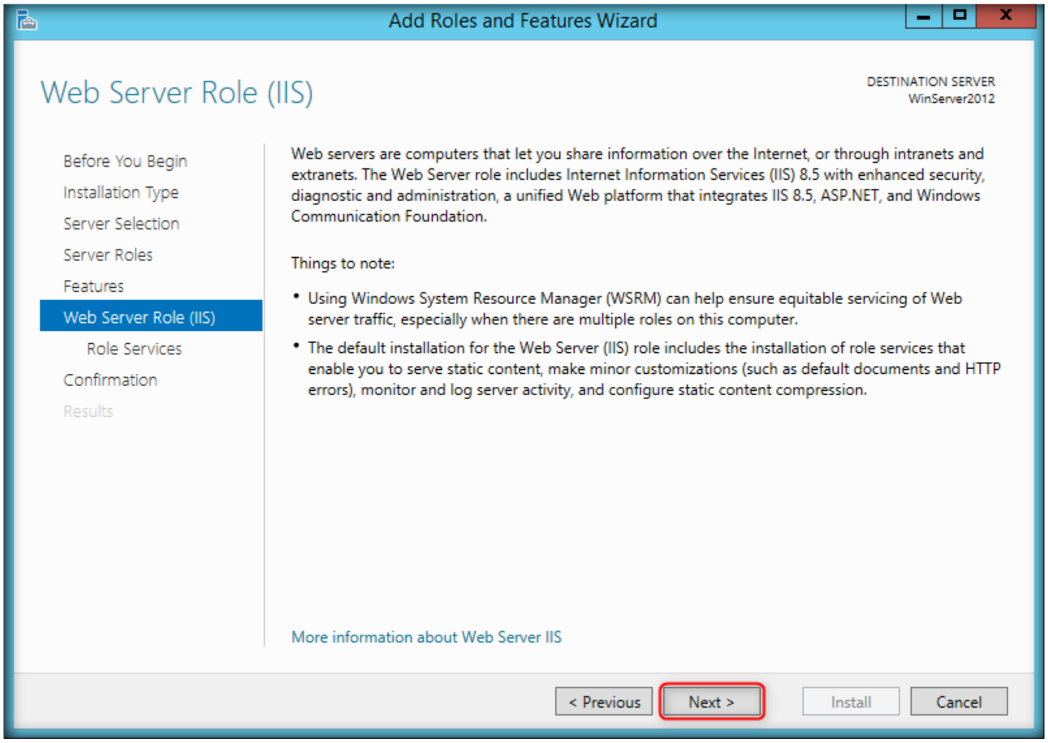
- □ SMB Bandwidth Limit
- □ SMTP Server
- □ SNMP Service
- □ Telnet Client
- ☑ Telnet Server
- □ TFTP Client
- ▣ User Interfaces and Infrastructure (2 of 3 installed)
- □ Windows Biometric Framework
- □ Windows Feedback Forwarder
- □ Windows Identity Foundation 3.5
- □ Windows Internal Database
- ▣ Windows PowerShell (2 of 5 installed)
- ▣ Windows Process Activation Service (2 of 3 installe
- □ Windows Search Service

Description

.NET Framework 4.5 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.

11. Click **Add Features** button if you get a prompt for the features to be added, while selecting any features. Click **Next**.

12. **Web Server Role (IIS)** section appears in the wizard, click **Next**.

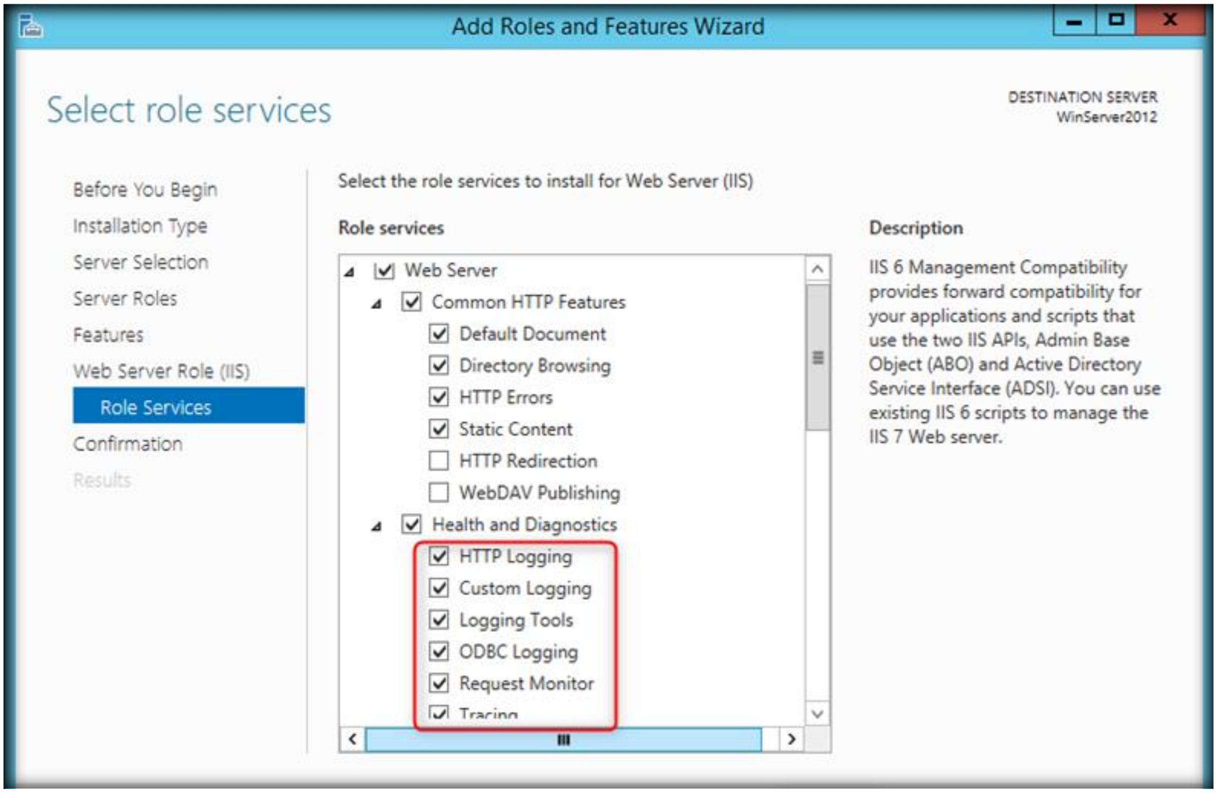


Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 8.5 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 8.5, ASP.NET, and Windows Communication Foundation.

Things to note:

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

13. **Selected Role Services** section appears in the wizard. Check all features under **Health and Diagnostics**.



Select the role services to install for Web Server (IIS)

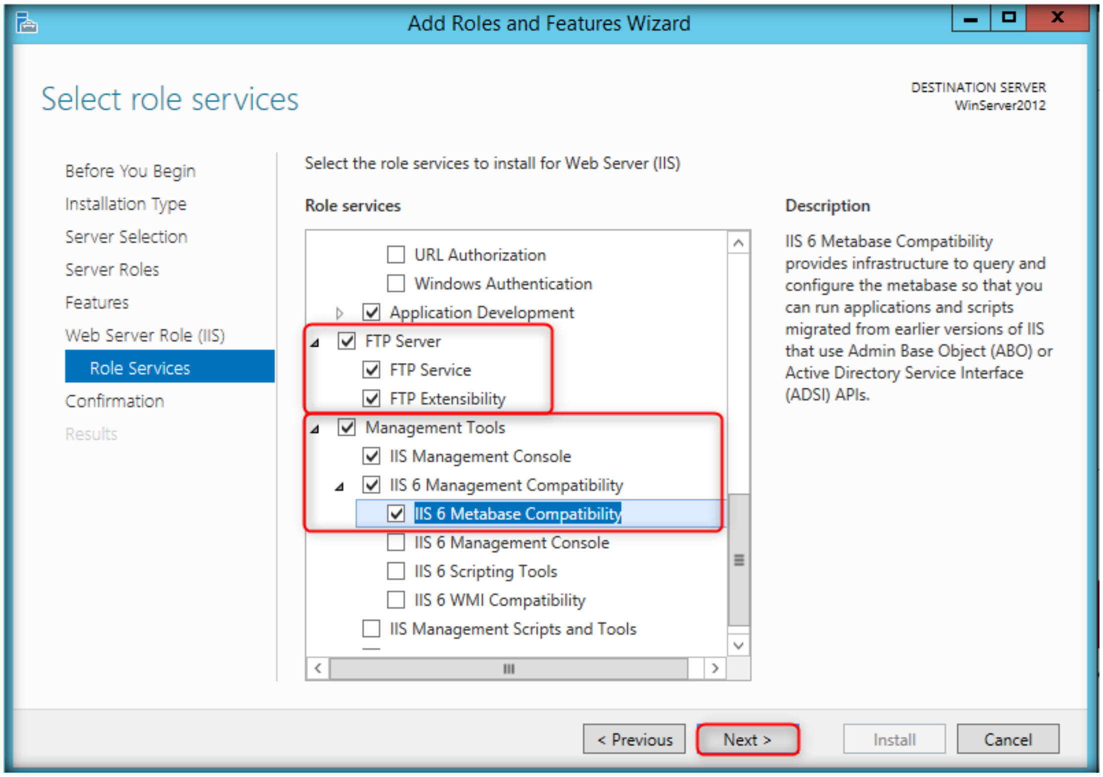
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - ☑ Custom Logging
    - ☑ Logging Tools
    - ☑ ODBC Logging
    - ☑ Request Monitor
    - ☑ Tracing

Description

IIS 6 Management Compatibility provides forward compatibility for your applications and scripts that use the two IIS APIs, Admin Base Object (ABO) and Active Directory Service Interface (ADSI). You can use existing IIS 6 scripts to manage the IIS 7 Web server.

14. Scroll down and Check **FTP Server→ FTP Service, Management Tools→ IIS Management Console, IIS 6 Metabase Compatability → IIS 6 Metabase Compatability**. Click **Next**.



Select role services

DESTINATION SERVER
WinServer2012

Select the role services to install for Web Server (IIS)

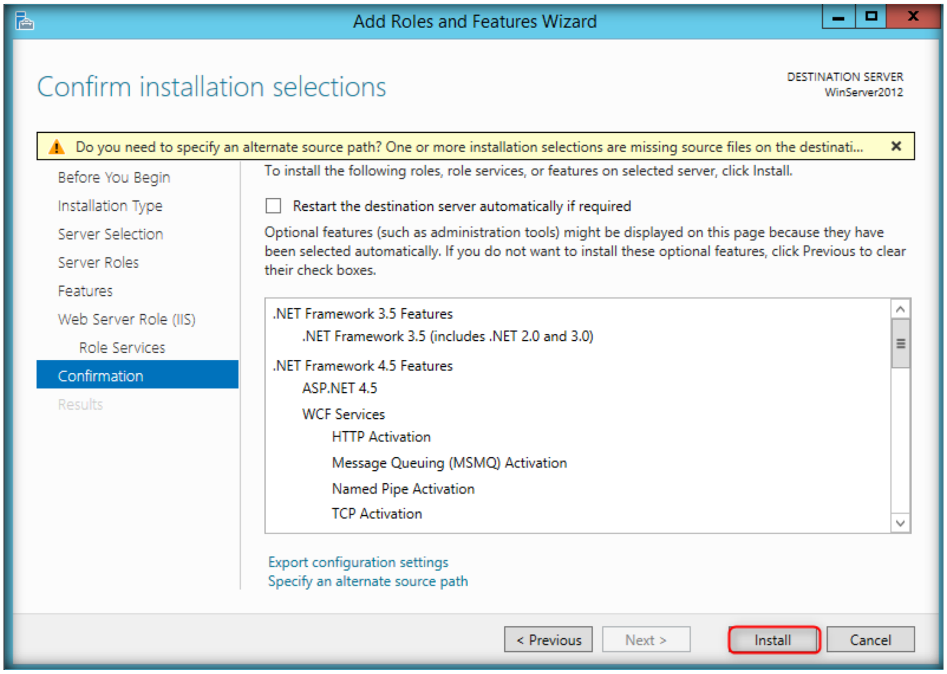
Role services

- ☐ URL Authorization
- ☐ Windows Authentication
- ☑ Application Development
- ☑ FTP Server
  - ☑ FTP Service
  - ☑ FTP Extensibility
- ☑ Management Tools
  - ☑ IIS Management Console
  - ☑ IIS 6 Management Compatibility
    - ☑ IIS 6 Metabase Compatibility
    - ☐ IIS 6 Management Console
    - ☐ IIS 6 Scripting Tools
    - ☐ IIS 6 WMI Compatibility
  - ☐ IIS Management Scripts and Tools

Description

IIS 6 Metabase Compatibility provides infrastructure to query and configure the metabase so that you can run applications and scripts migrated from earlier versions of IIS that use Admin Base Object (ABO) or Active Directory Service Interface (ADSI) APIs.

15. In Confirm installation section wizard, click **Install** (Ignore the warning under the Custom installation selections wizard).



Confirm installation selections

DESTINATION SERVER
WinServer2012

⚠ Do you need to specify an alternate source path? One or more installation selections are missing source files on the destinati... ×

To install the following roles, role services, or features on selected server, click Install.

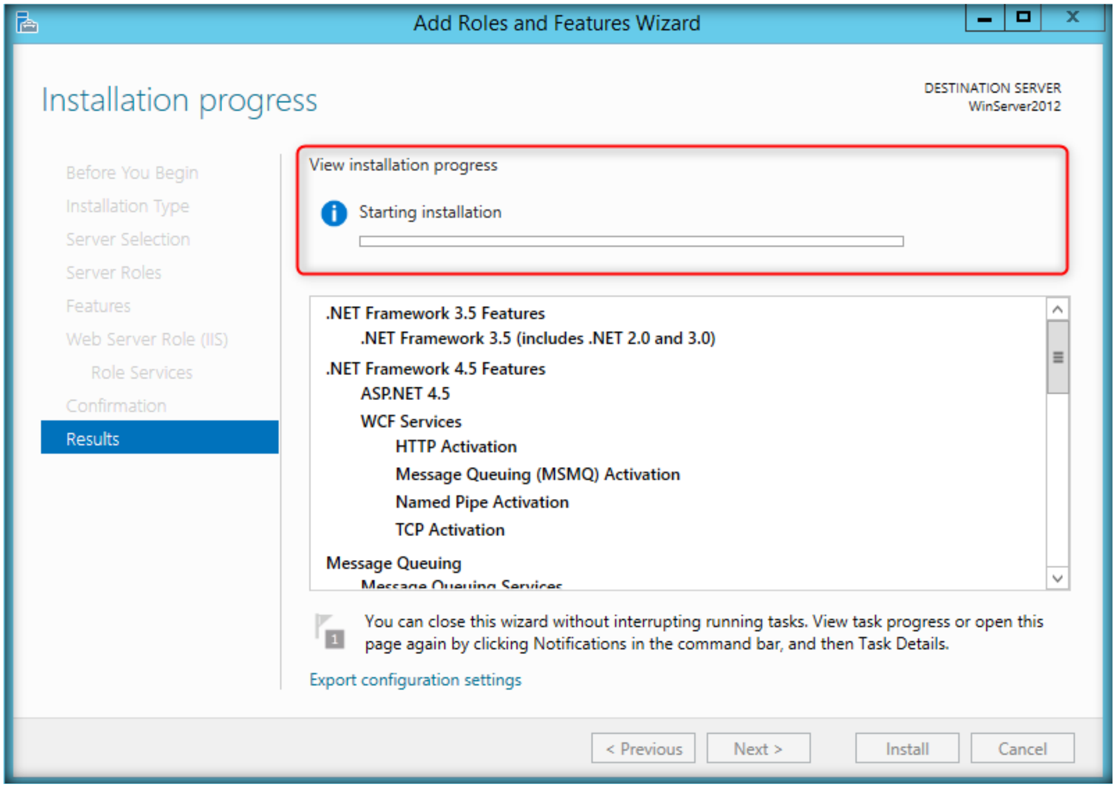
☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

.NET Framework 3.5 Features
  .NET Framework 3.5 (includes .NET 2.0 and 3.0)
.NET Framework 4.5 Features
  ASP.NET 4.5
  WCF Services
    HTTP Activation
    Message Queuing (MSMQ) Activation
    Named Pipe Activation
    TCP Activation

Export configuration settings
Specify an alternate source path

16. **Add Roles and Features Wizard** will show the installation progress of the features. It will take a while to **complete** the installation of selected roles.

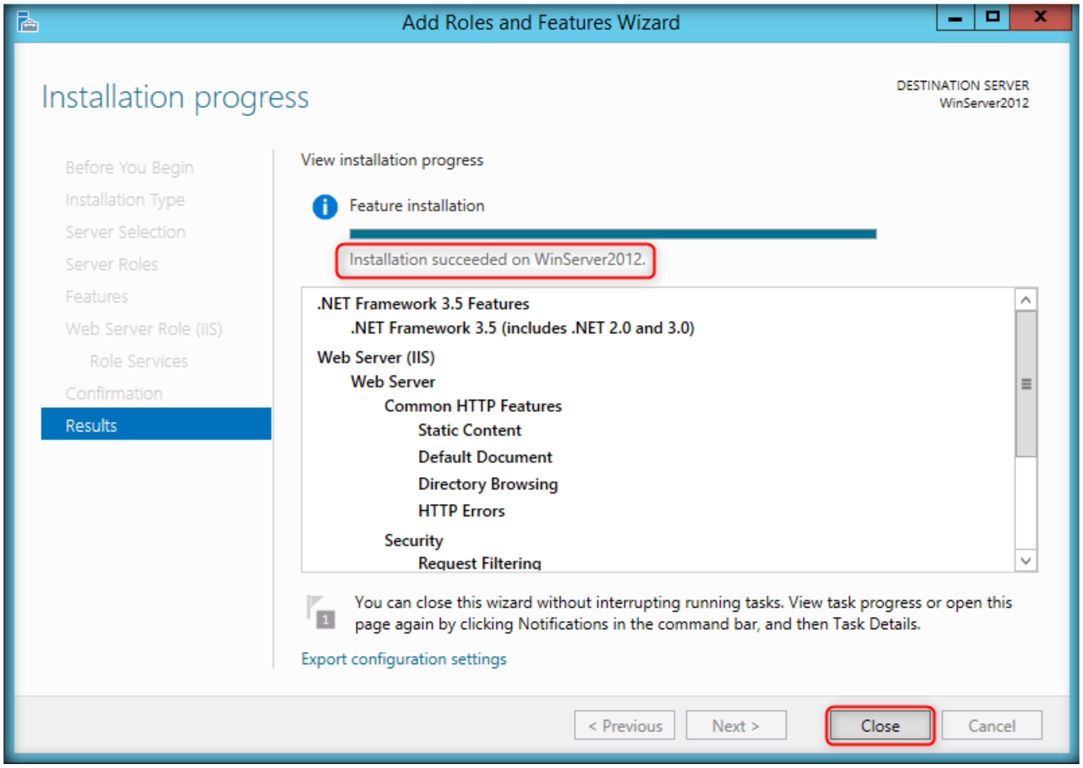


.NET Framework 3.5 Features
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
.NET Framework 4.5 Features
ASP.NET 4.5
WCF Services
HTTP Activation
Message Queuing (MSMQ) Activation
Named Pipe Activation
TCP Activation
Message Queuing
Message Queuing Services

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

17. After the completion of installation, click **Close** button and restart the machine.



Installation succeeded on WinServer2012.

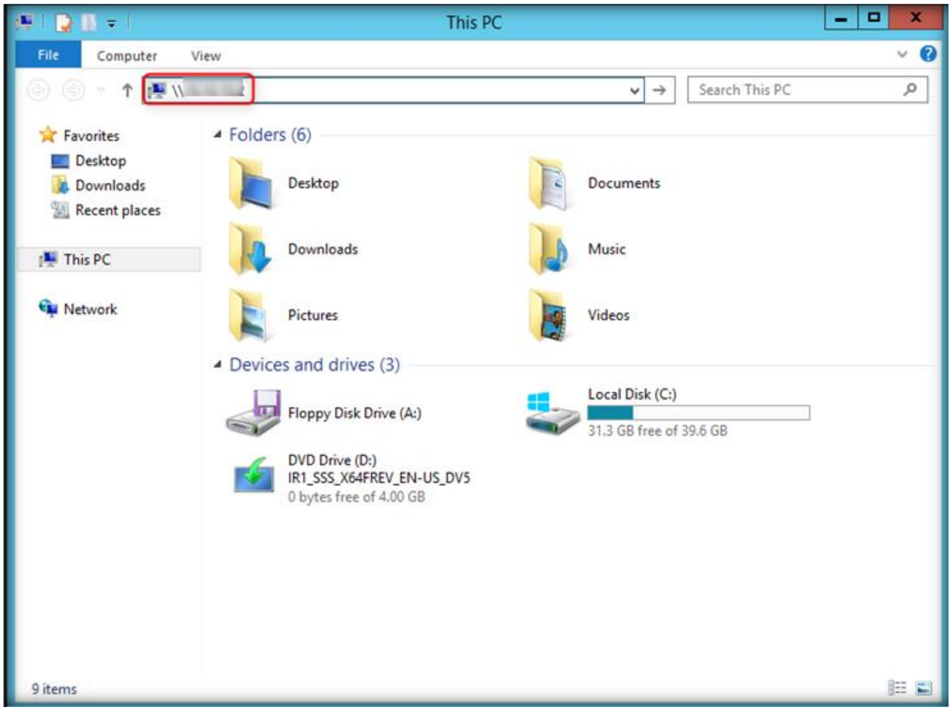
.NET Framework 3.5 Features
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
Web Server (IIS)
Web Server
Common HTTP Features
Static Content
Default Document
Directory Browsing
HTTP Errors
Security
Request Filtering

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

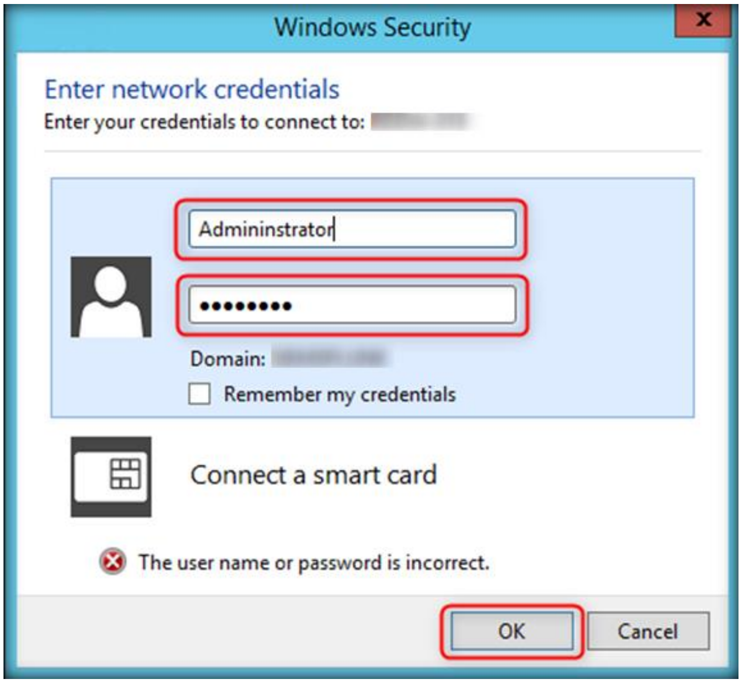
Export configuration settings

CT#7.5: Sharing SOC-Tools Folder from Host Machine and Mapping to Windows Server 2012 VM

1. Open File Explorer, and type **[IP Address of your host machine]** in the address bar and press **Enter.**



2. Type your Host machine credentials, check the Remember my credentials check box and click **OK**, in the Windows Security pop-up that appears.


Windows Security

Enter network credentials

Enter your credentials to connect to: [redacted]

Admininstrator

•••••••••

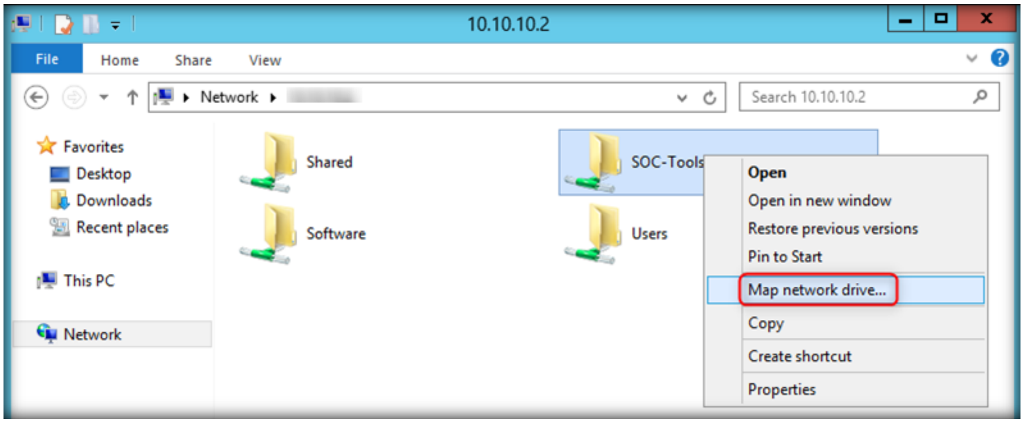
Domain: [redacted]

☐ Remember my credentials

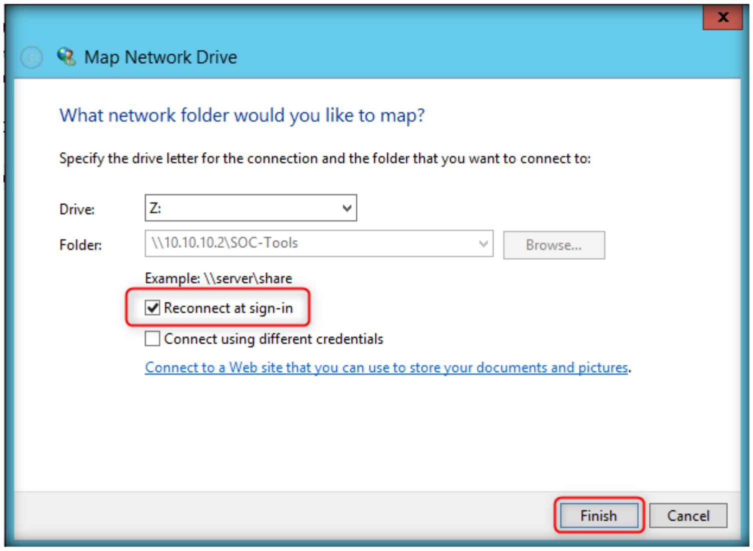
Connect a smart card

The user name or password is incorrect.

3. Right-click on SOC-Tools shared folder and click Map network drive from the context menu as shown in the screenshot.



4. Map Network Drive window appears, assign drive letter as **Z:\**, make sure that Reconnect at sign-in option is checked and click **Finish.**


Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\10.10.10.2\SOC-Tools

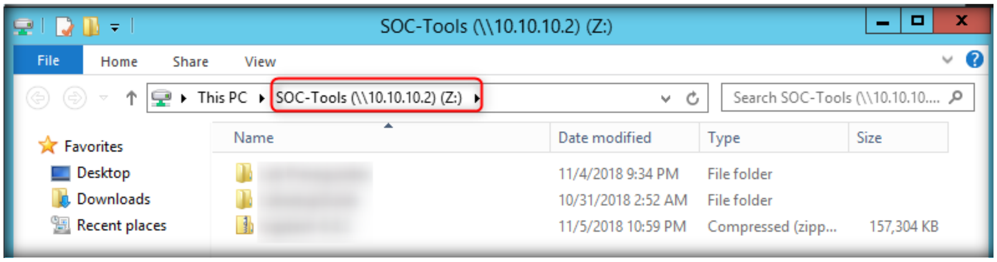
Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

Browse...
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel

5. SOC-Tools mapped network drive appears in the File Explorer view, click **This-PC** from the left pane to confirm.

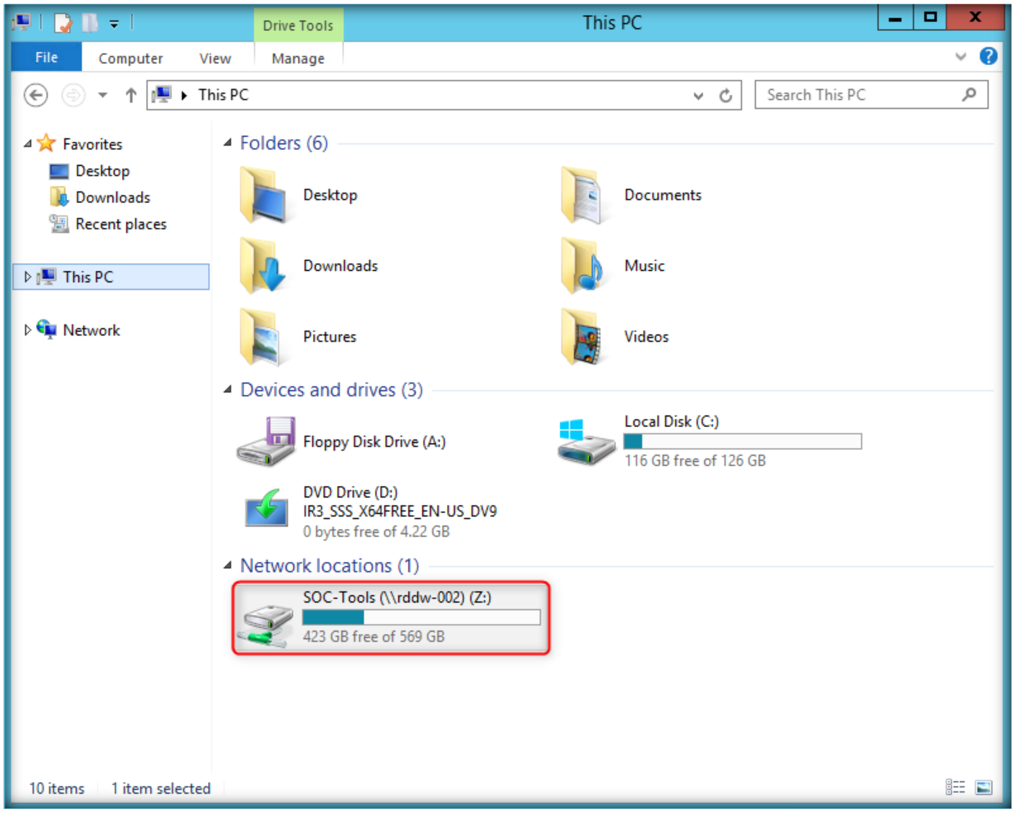

SOC-Tools (\\10.10.10.2) (Z:)

This PC ▸ SOC-Tools (\\10.10.10.2) (Z:)

Name	Date modified	Type	Size
[redacted]	11/4/2018 9:34 PM	File folder	
[redacted]	10/31/2018 2:52 AM	File folder	
[redacted]	11/5/2018 10:59 PM	Compressed (zipp...	157,304 KB

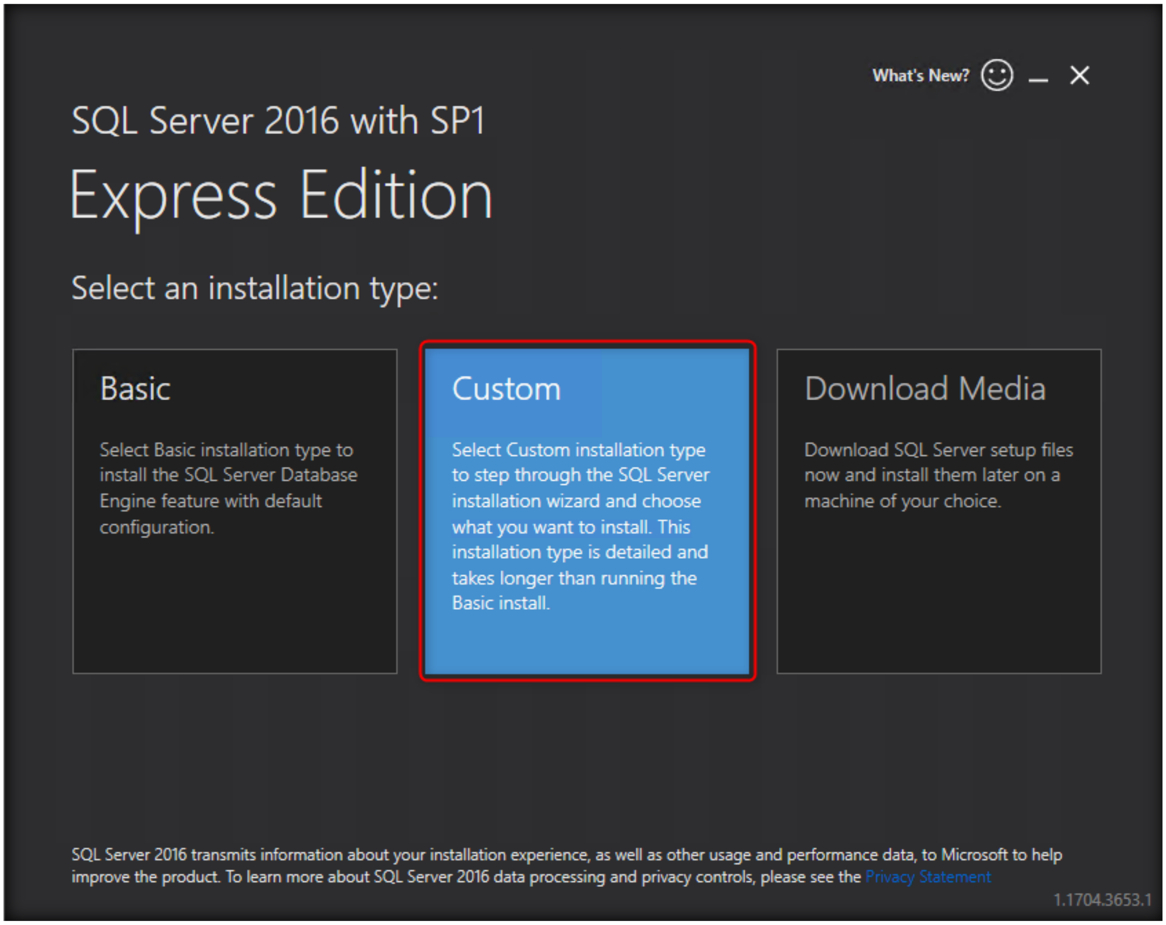
6. Now you can see that **SOC-Tools** directory is mapped to your Windows Server 2012 machine as shown in the screenshot.

   Note: Throughout this configuration, the IP address of the host machine will differ in your lab environment.



CT#7.6: Install MS SQL Server 2016 Express Edition on Windows Server 2016 Virtual Machine

1. Navigate to **Z:\ SOC-Tools\Lab Prerequisites\SQL Server 2016** and double-click **SQLServer2016-SSEI-Expr.exe**.
2. If Open File -Security warning pop-up appears, click **Run**.
3. SQL Server 2016 window appears click **Custom**.



SQL Server 2016 with SP1

Express Edition

Select an installation type:

Basic

Select Basic installation type to install the SQL Server Database Engine feature with default configuration.

Custom

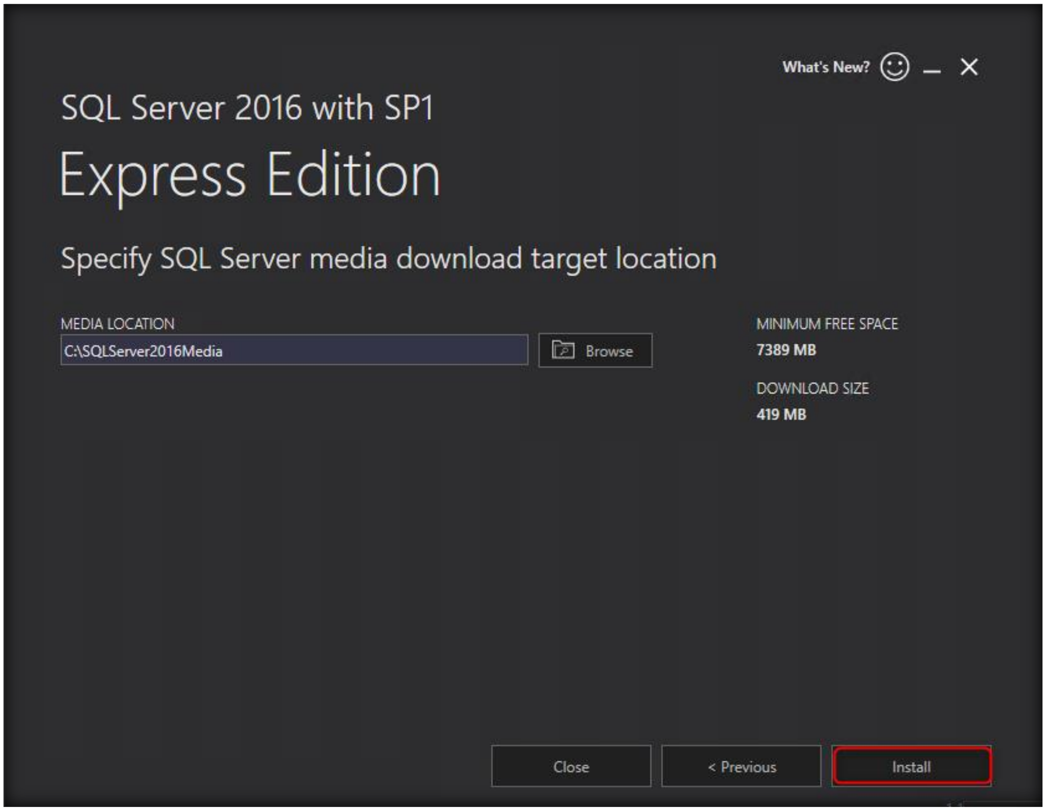
Select Custom installation type to step through the SQL Server installation wizard and choose what you want to install. This installation type is detailed and takes longer than running the Basic install.

Download Media

Download SQL Server setup files now and install them later on a machine of your choice.

SQL Server 2016 transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about SQL Server 2016 data processing and privacy controls, please see the Privacy Statement

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



SQL Server 2016 with SP1

Express Edition

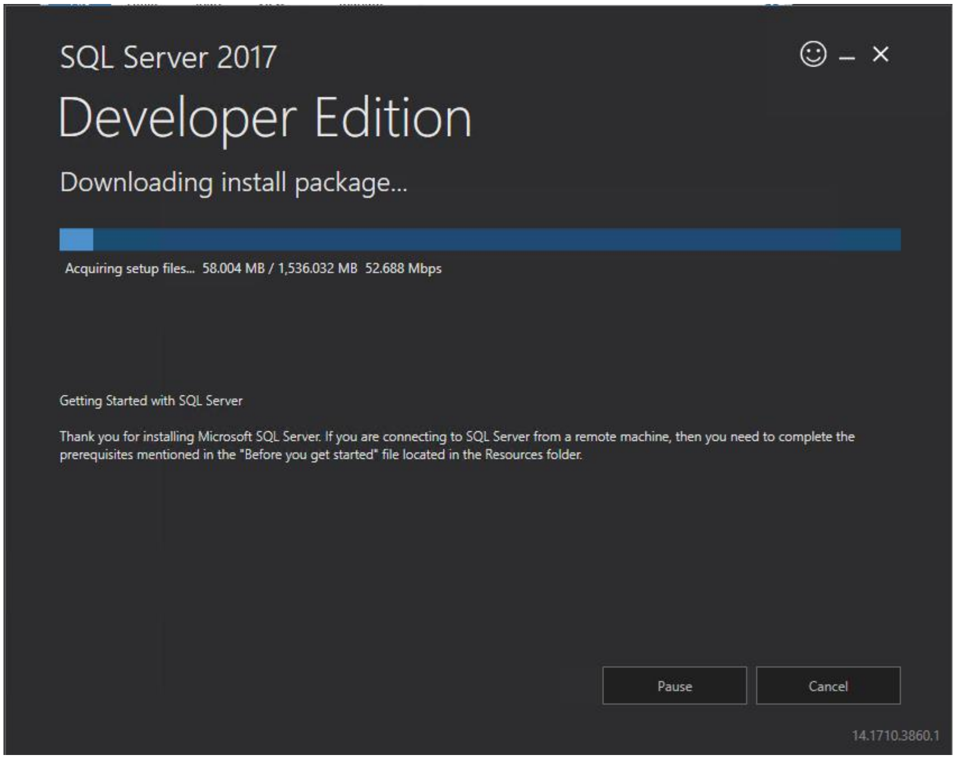
Specify SQL Server media download target location

MEDIA LOCATION
C:\SQLServer2016Media

MINIMUM FREE SPACE
7389 MB

DOWNLOAD SIZE
419 MB

5. The program starts downloading the setup files, wait for the Installation Center to launch.



SQL Server 2017

Developer Edition

Downloading install package...

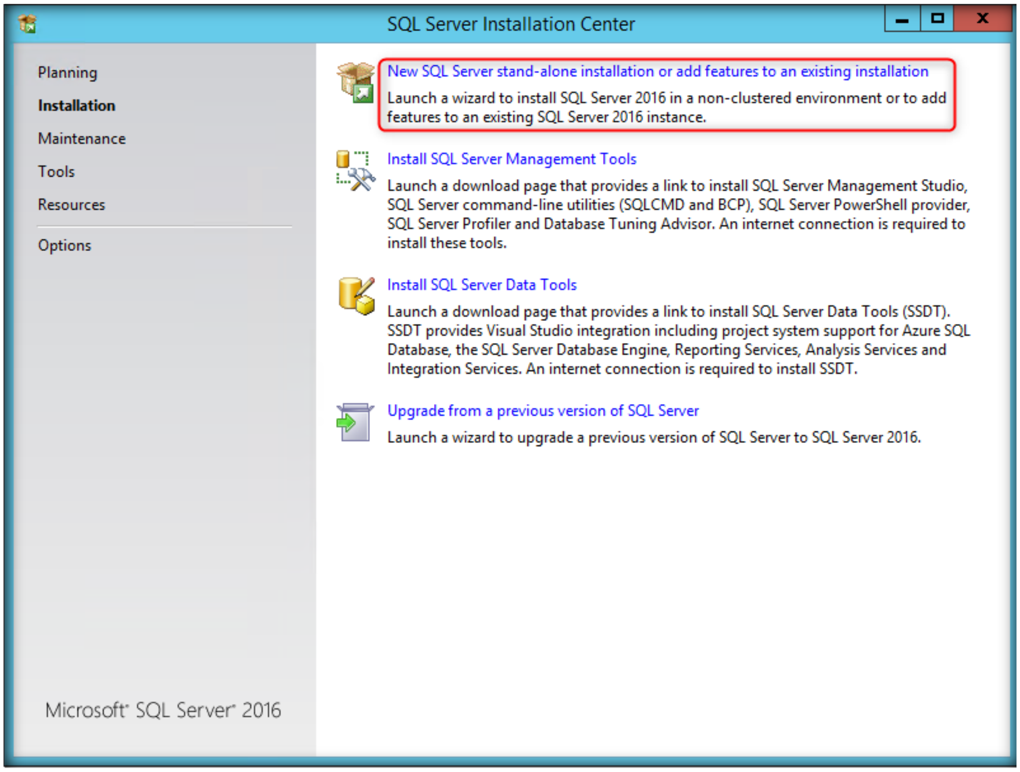
Acquiring setup files... 58.004 MB / 1,536.032 MB 52.688 Mbps

Getting Started with SQL Server

Thank you for installing Microsoft SQL Server. If you are connecting to SQL Server from a remote machine, then you need to complete the prerequisites mentioned in the "Before you get started" file located in the Resources folder.

14.1710.3860.1

6. SQL Server Installation Center window appears with **Installation** section displayed by default, click **New SQL Server stand-alone installation or add features to an existing installation** link and wait for some time.



SQL Server Installation Center

New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2016 in a non-clustered environment or to add features to an existing SQL Server 2016 instance.

Install SQL Server Management Tools

Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.

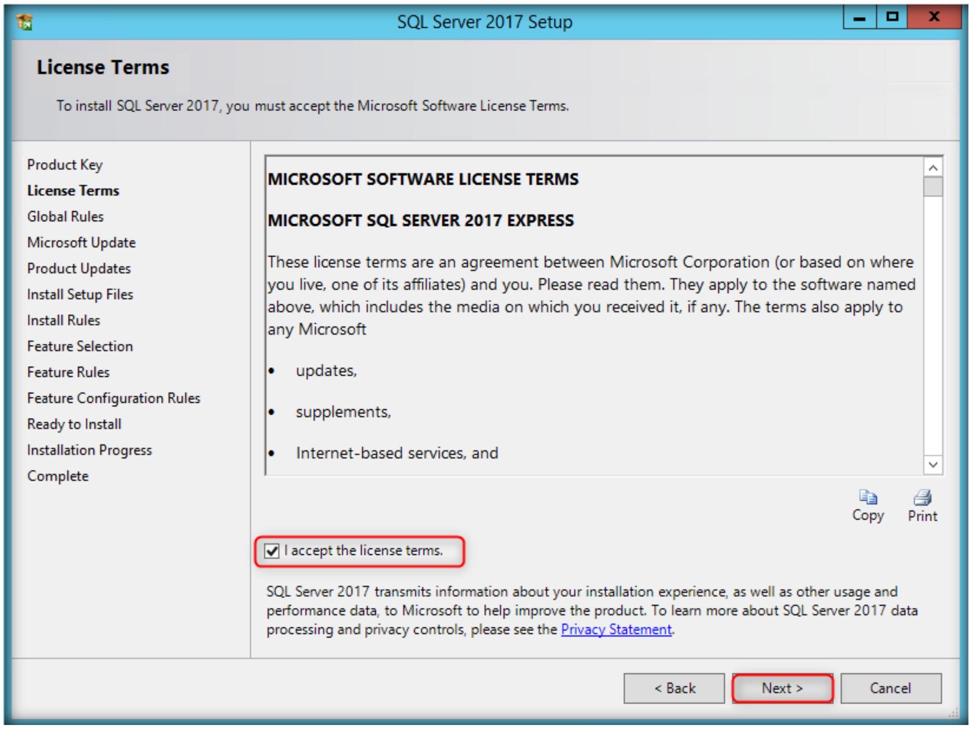
Install SQL Server Data Tools

Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.

Upgrade from a previous version of SQL Server

Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2016.

7. Read the Software License Terms in the **License Terms** section, check the option **I accept the license terms** and click **Next**.



SQL Server 2017 Setup

License Terms

To install SQL Server 2017, you must accept the Microsoft Software License Terms.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2017 EXPRESS

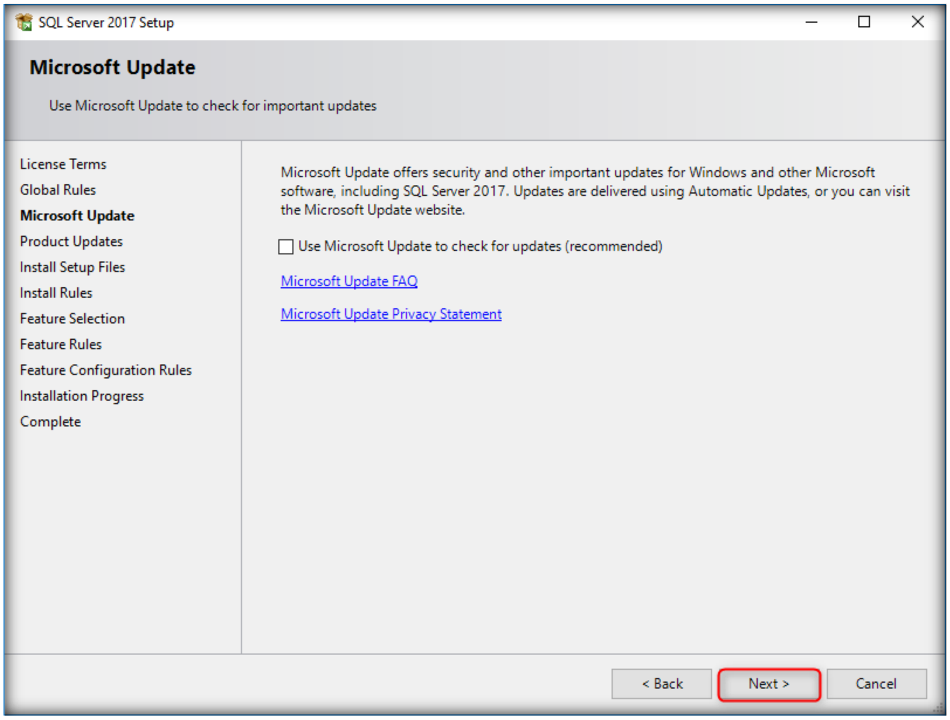
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and

☑ I accept the license terms.

SQL Server 2017 transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about SQL Server 2017 data processing and privacy controls, please see the Privacy Statement.

8. SQL Server 2017 Setup **Microsoft Update** section appears, click **Next**.



SQL Server 2017 Setup

Microsoft Update

Use Microsoft Update to check for important updates

Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2017. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.

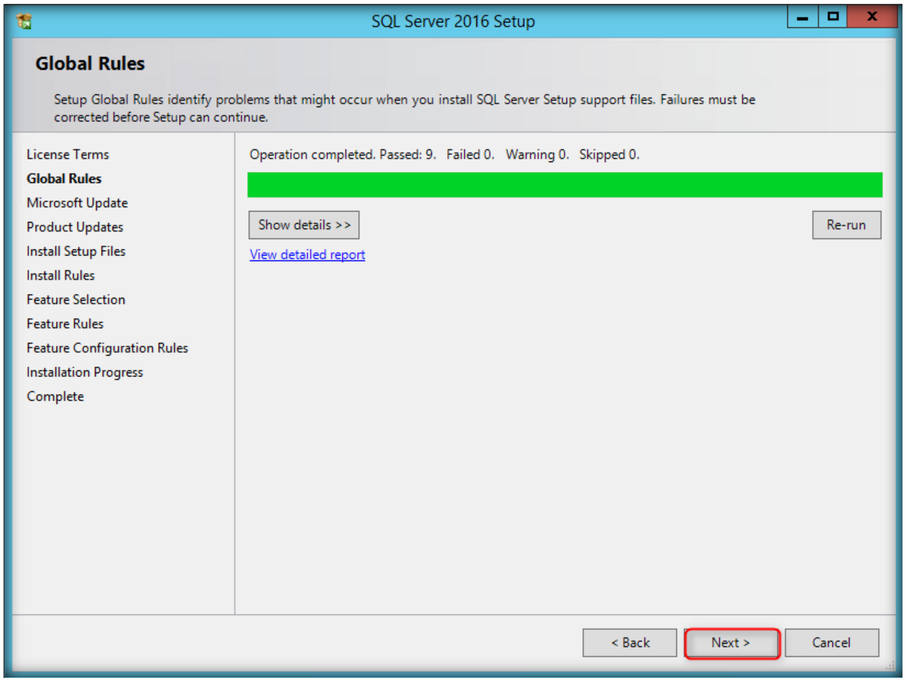
□ Use Microsoft Update to check for updates (recommended)

Microsoft Update FAQ

Microsoft Update Privacy Statement

9. The **Install Rules** verifies the system state of your computer before Setup continues.

10. After verification is finished, click **Next**.



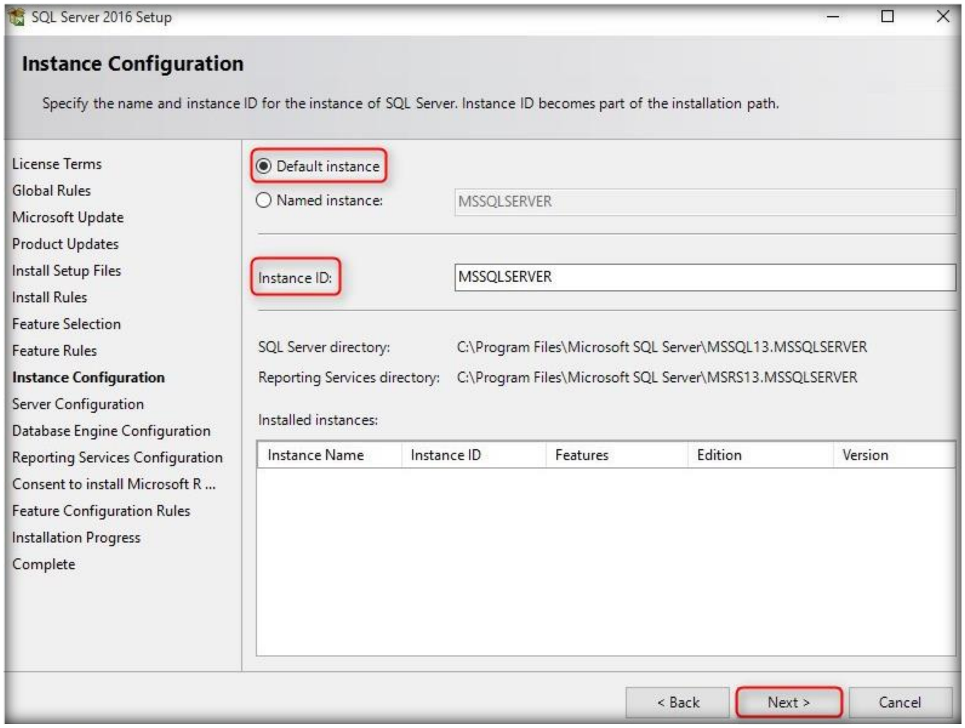
SQL Server 2016 Setup

Global Rules

Setup Global Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

Operation completed. Passed: 9. Failed 0. Warning 0. Skipped 0.

11. The **Feature Rules** gets installed and **Instance Configuration** window appears.
12. In the **Instance Configuration** window, select **Default instance** that gives the **Instance ID** as **MSSQLSERVER**. Click **Next**.



SQL Server 2016 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

● Default instance

○ Named instance: MSSQLSERVER

Instance ID: MSSQLSERVER

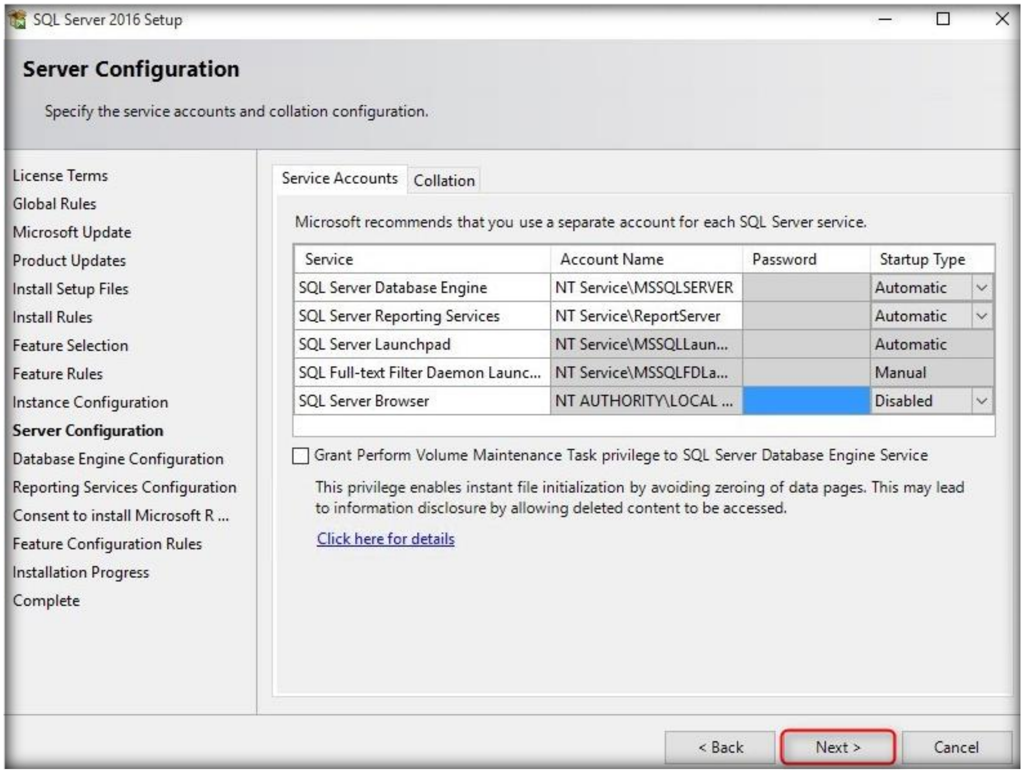
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER

Reporting Services directory: C:\Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

13. The **Server Configuration** window appears. Click **Next**.



SQL Server 2016 Setup

Server Configuration

Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

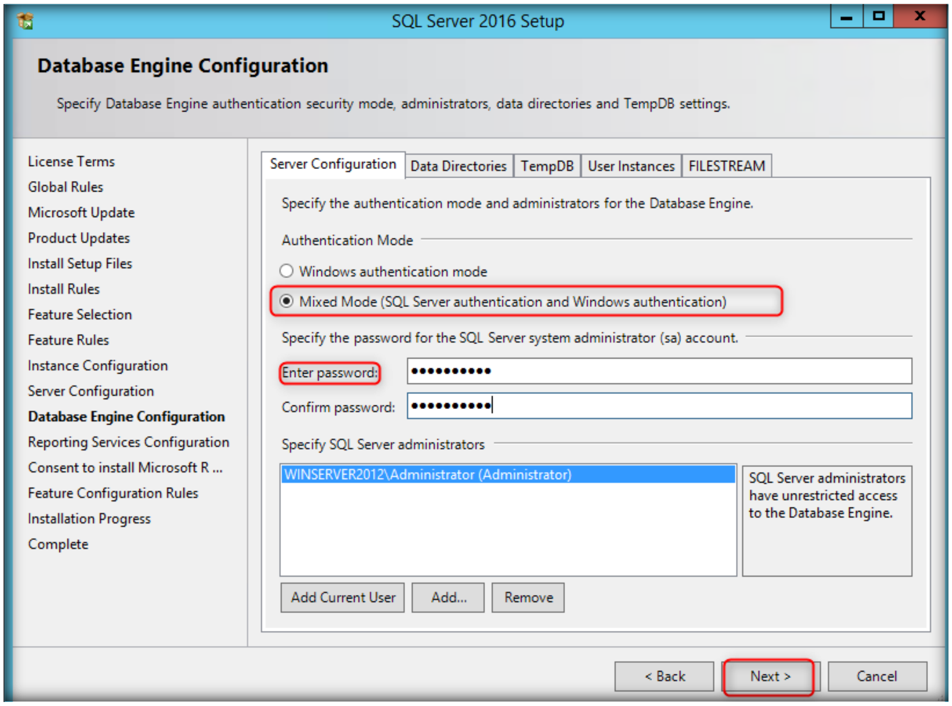
Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT Service\MSSQLSERVER		Automatic
SQL Server Reporting Services	NT Service\ReportServer		Automatic
SQL Server Launchpad	NT Service\MSSQLLaun...		Automatic
SQL Full-text Filter Daemon Launc...	NT Service\MSSQLFDLa...		Manual
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled

☐ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

Click here for details

14. In the **Database Engine Configuration** window, select **Mixed Mode (SQL Server authentication and Windows authentication).** In **Enter password** field specify the password **qwerty@123**. Click **Next**.



Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: ••••••••••

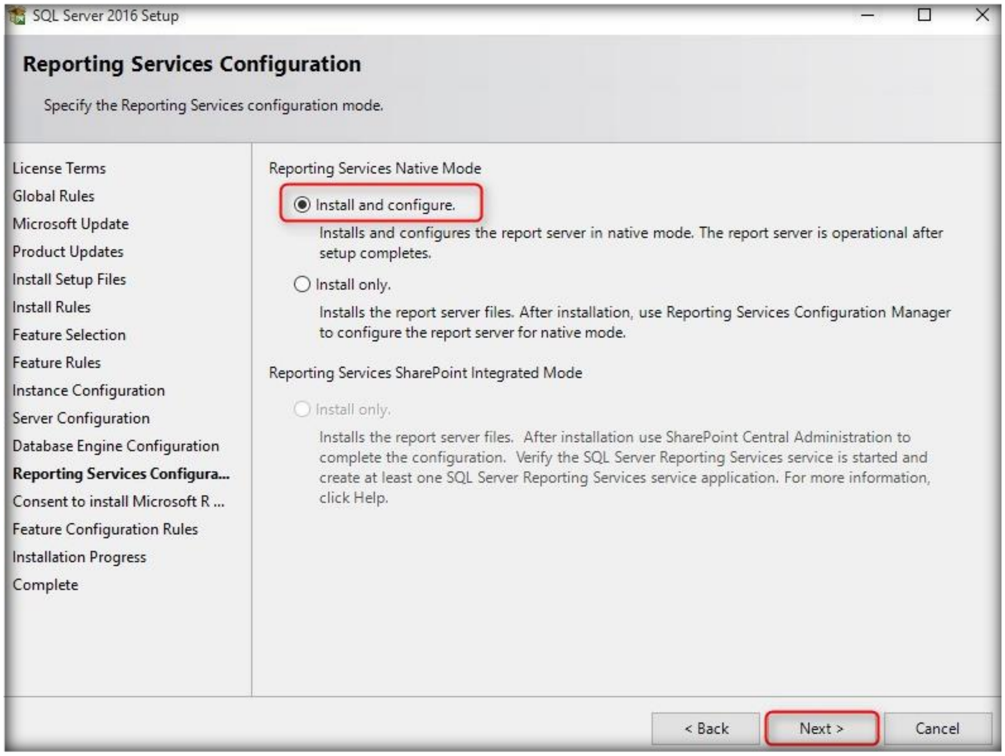
Confirm password: ••••••••••

Specify SQL Server administrators

WINSERVER2012\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

15. In the **Reporting Services Configuration** window, select **Install and configure**. Click **Next**.



Reporting Services Configuration

Specify the Reporting Services configuration mode.

Reporting Services Native Mode

● Install and configure.

Installs and configures the report server in native mode. The report server is operational after setup completes.

○ Install only.

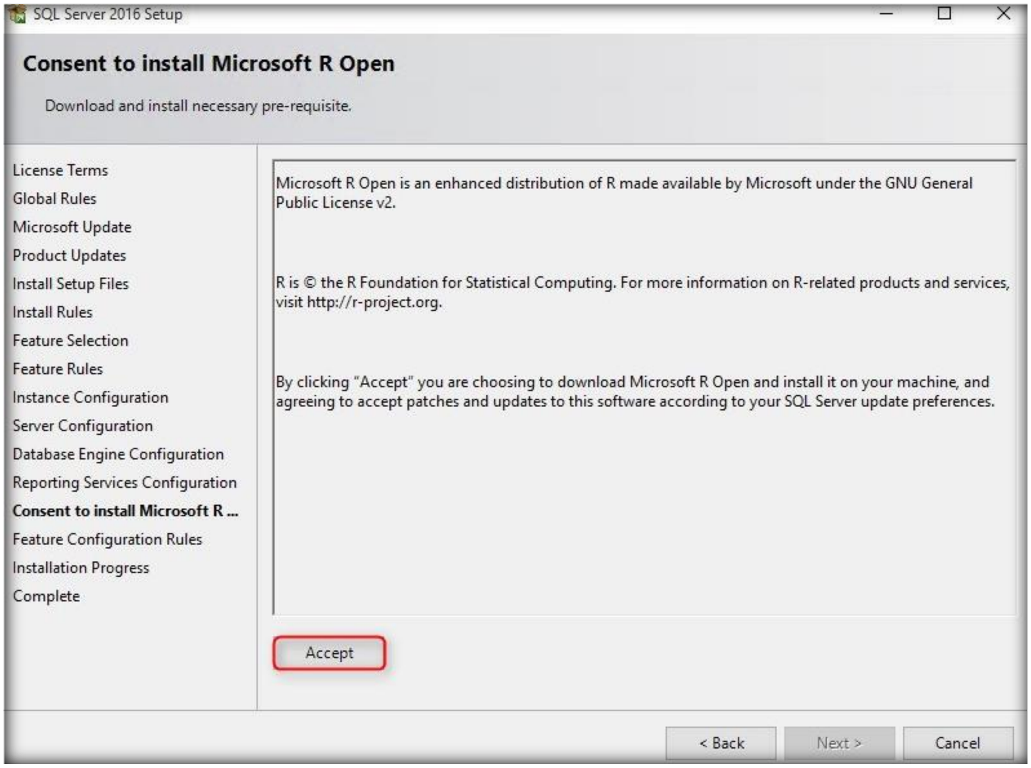
Installs the report server files. After installation, use Reporting Services Configuration Manager to configure the report server for native mode.

Reporting Services SharePoint Integrated Mode

○ Install only.

Installs the report server files. After installation use SharePoint Central Administration to complete the configuration. Verify the SQL Server Reporting Services service is started and create at least one SQL Server Reporting Services service application. For more information, click Help.

16. **Consent to install Microsoft R Open** window appears. Click **Accept** to download Microsoft R Open.



Consent to install Microsoft R Open

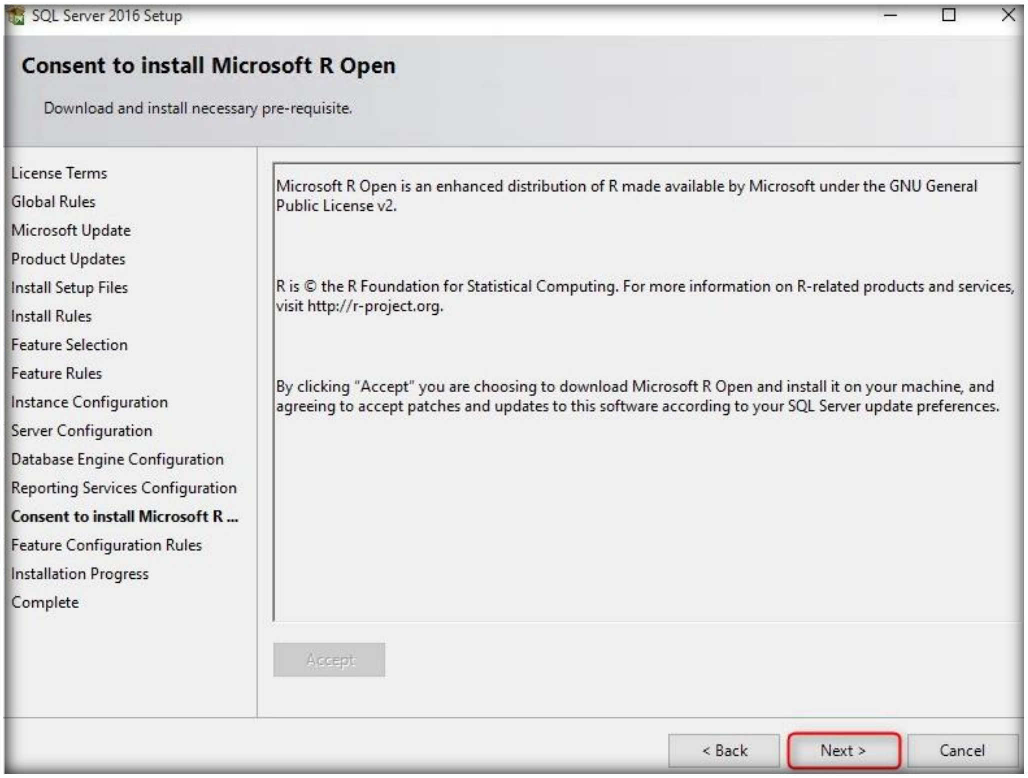
Download and install necessary pre-requisite.

Microsoft R Open is an enhanced distribution of R made available by Microsoft under the GNU General Public License v2.

R is © the R Foundation for Statistical Computing. For more information on R-related products and services, visit http://r-project.org.

By clicking "Accept" you are choosing to download Microsoft R Open and install it on your machine, and agreeing to accept patches and updates to this software according to your SQL Server update preferences.

17. Click **Next**.



Consent to install Microsoft R Open

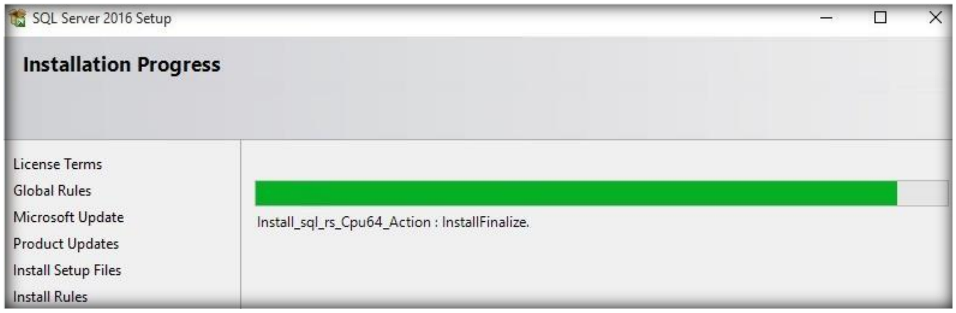
Download and install necessary pre-requisite.

Microsoft R Open is an enhanced distribution of R made available by Microsoft under the GNU General Public License v2.

R is © the R Foundation for Statistical Computing. For more information on R-related products and services, visit http://r-project.org.

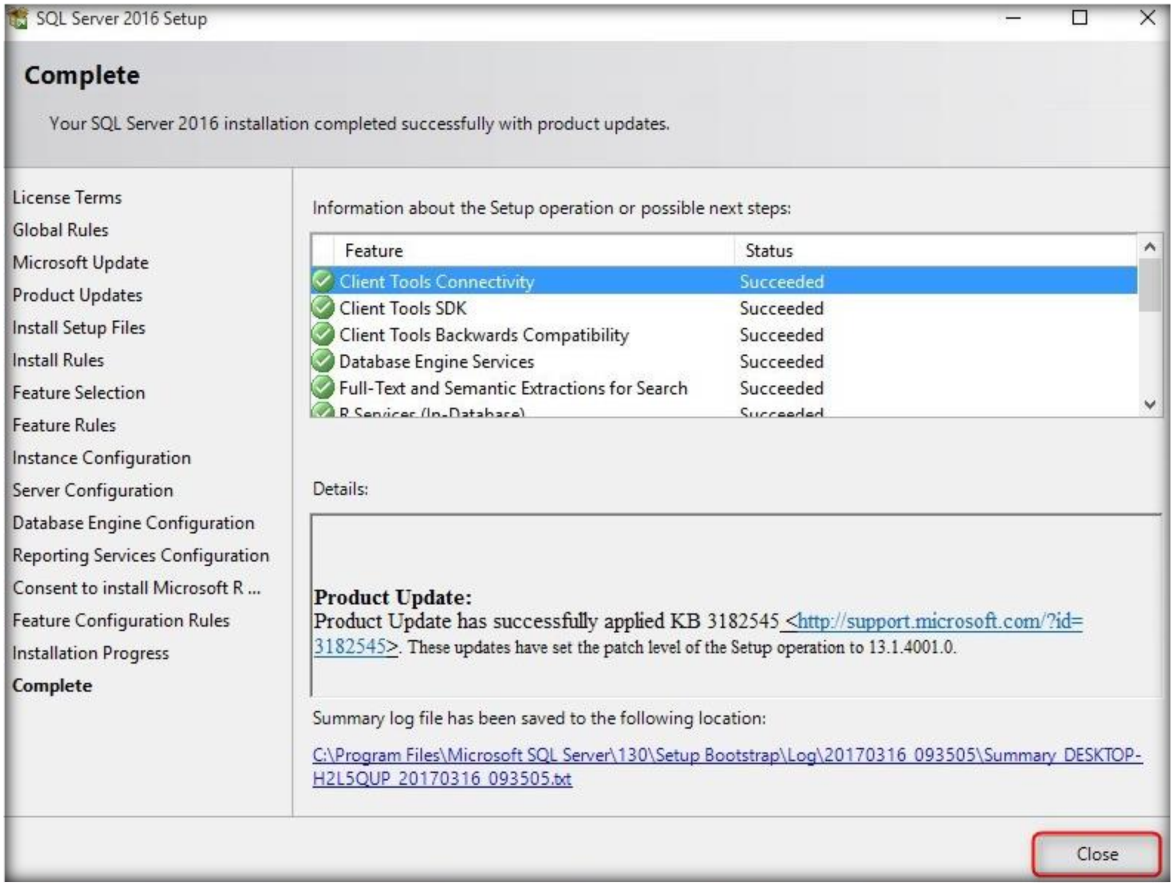
By clicking "Accept" you are choosing to download Microsoft R Open and install it on your machine, and agreeing to accept patches and updates to this software according to your SQL Server update preferences.

18. **Feature Configuration Rules** installation occurs after the pre-requisite installation of **Microsoft R Open**.
19. **Installation Progress** window appears. During installation, the Installation Progress page provides **status** so that you can monitor installation **progress** as Setup continues.
20. After the installation completes click **Next** or the **Complete** page appears automatically.



Install_sql_rs_Cpu64_Action : InstallFinalize.

21. **Complete page** appears.
22. The Complete page provides a link to the **summary log file** for the installation and other **important notes**.
23. Click **Close**.



Your SQL Server 2016 installation completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
Client Tools Connectivity	Succeeded
Client Tools SDK	Succeeded
Client Tools Backwards Compatibility	Succeeded
Database Engine Services	Succeeded
Full-Text and Semantic Extractions for Search	Succeeded
R Services (In-Database)	Succeeded

Details:

Product Update:
Product Update has successfully applied KB 3182545 <http://support.microsoft.com/?id=3182545>. These updates have set the patch level of the Setup operation to 13.1.4001.0.

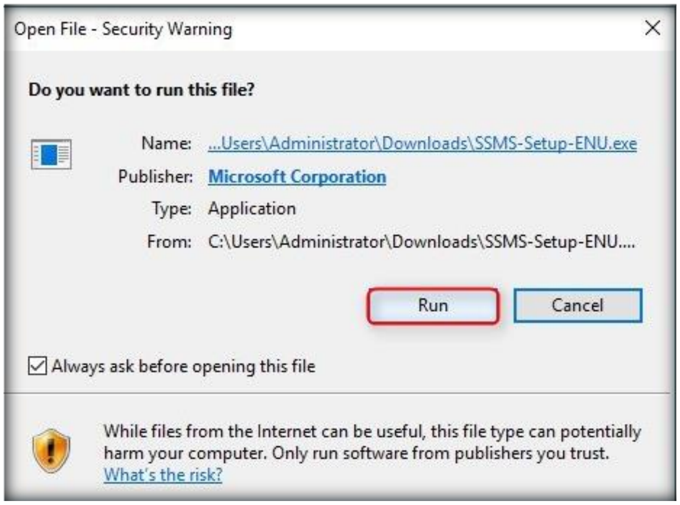
Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20170316_093505\Summary_DESKTOP-H2L5QUP_20170316_093505.txt

24. You are instructed to **restart** the computer. **Save** your work before you restart the computer.
25. You must read the **message** from the **Installation Wizard** when you finish Setup.

CT#7.7: Install Microsoft SQL Server Management Studio on Windows Server 2012 Virtual Machine

1. Navigate the **D:\SOC-Tools\Lab Prerequisites\SQL Server Management Studio** Double-click on SSMS-Setup-ENU.exe.
2. Click **Run** if security waring pop-up appears.



Open File - Security Warning

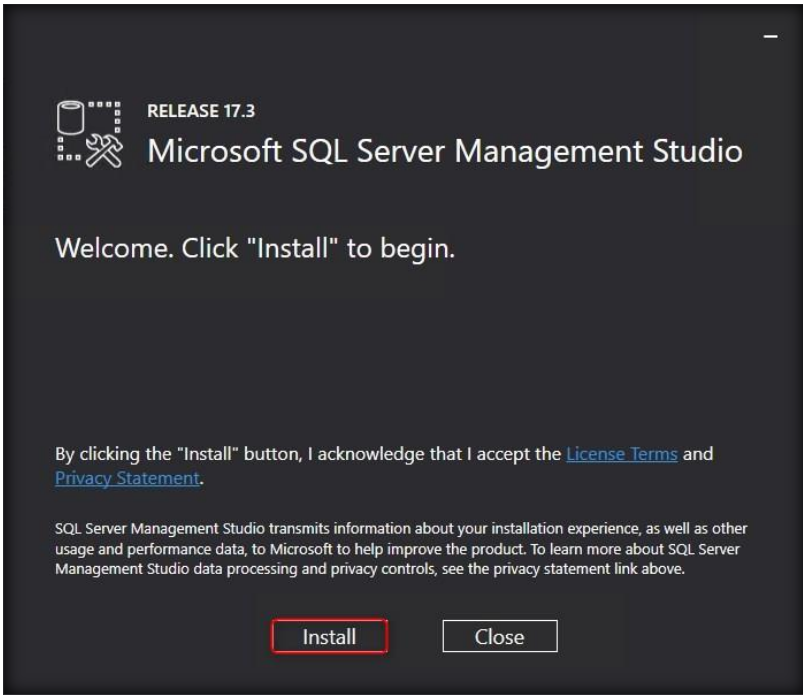
Do you want to run this file?

Name: ...Users\Administrator\Downloads\SSMS-Setup-ENU.exe
Publisher: Microsoft Corporation
Type: Application
From: C:\Users\Administrator\Downloads\SSMS-Setup-ENU....

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

3. Microsoft SQL Server Management Studio welcome screen appears, click **Install** to begin the setup.



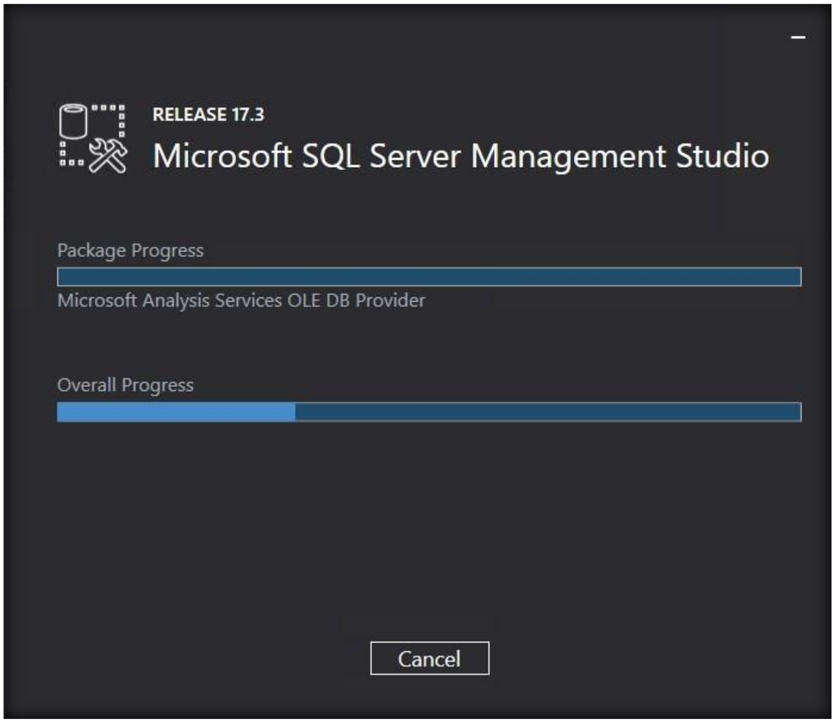
RELEASE 17.3
Microsoft SQL Server Management Studio

Welcome. Click "Install" to begin.

By clicking the "Install" button, I acknowledge that I accept the License Terms and Privacy Statement.

SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about SQL Server Management Studio data processing and privacy controls, see the privacy statement link above.

4. Microsoft SQL Server Management Studio begins the setup. Wait for the setup to finish.



RELEASE 17.3

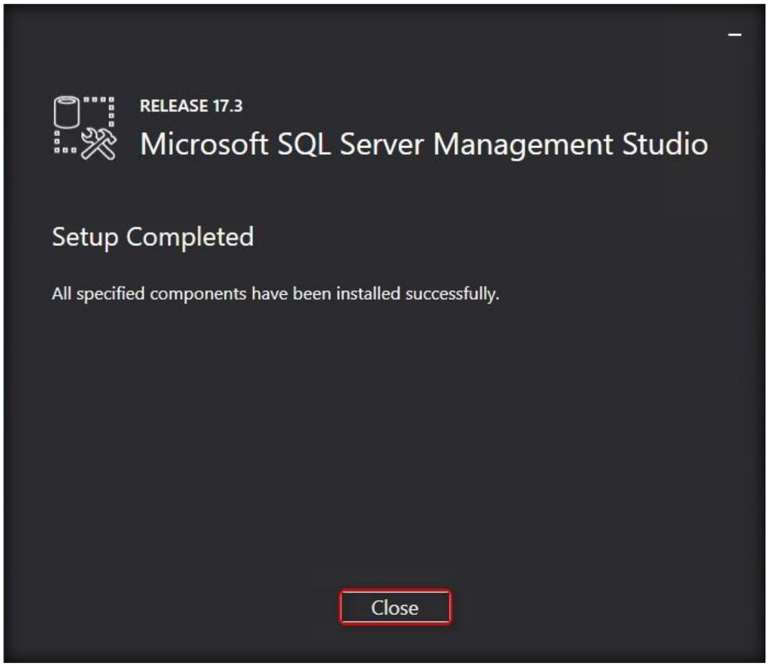
Microsoft SQL Server Management Studio

Package Progress

Microsoft Analysis Services OLE DB Provider

Overall Progress

5. Microsoft SQL Server Management Studio Setup Completed screen appears, click **Close** to finish.



RELEASE 17.3

Microsoft SQL Server Management Studio

Setup Completed

All specified components have been installed successfully.

6. Close the **SQL Server Installation Center** window.

CT#7.8: Installing Notepad++ in Windows Server 2012 VM

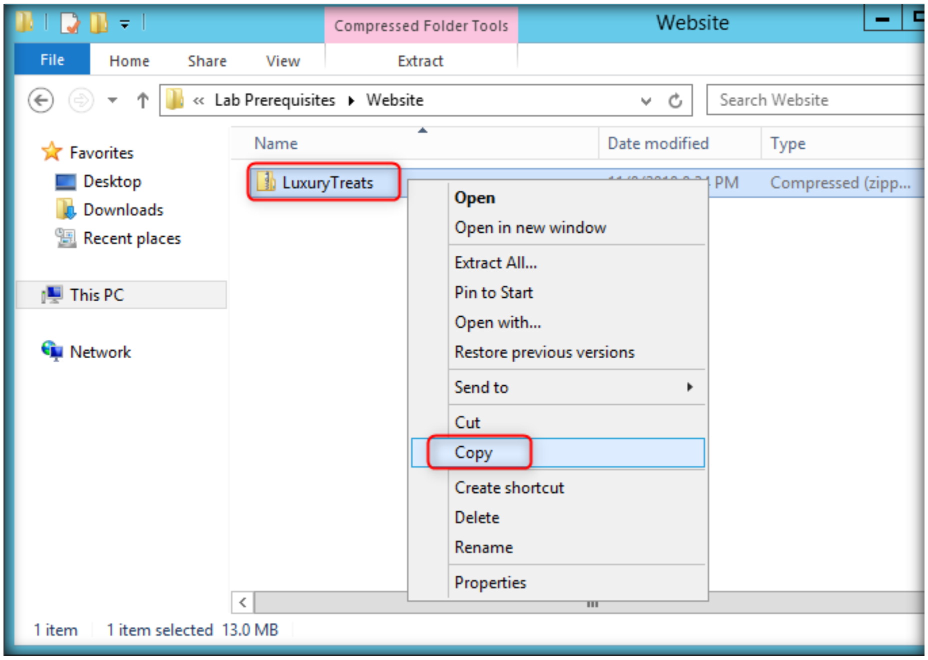
1. Navigate to **Z:\SOC-Tools\Lab Prerequisites** in guest operating systems.
2. Open **Notepad++** folder and double-click **npp.7.3.2.Installer**.
3. Follow the wizard-driven installation steps, to install **Notepad++**.
4. You can also download latest version of Notepad++ from its vendor site.

CT#7.9: Installing Web Browsers in Windows Server 2012 VM

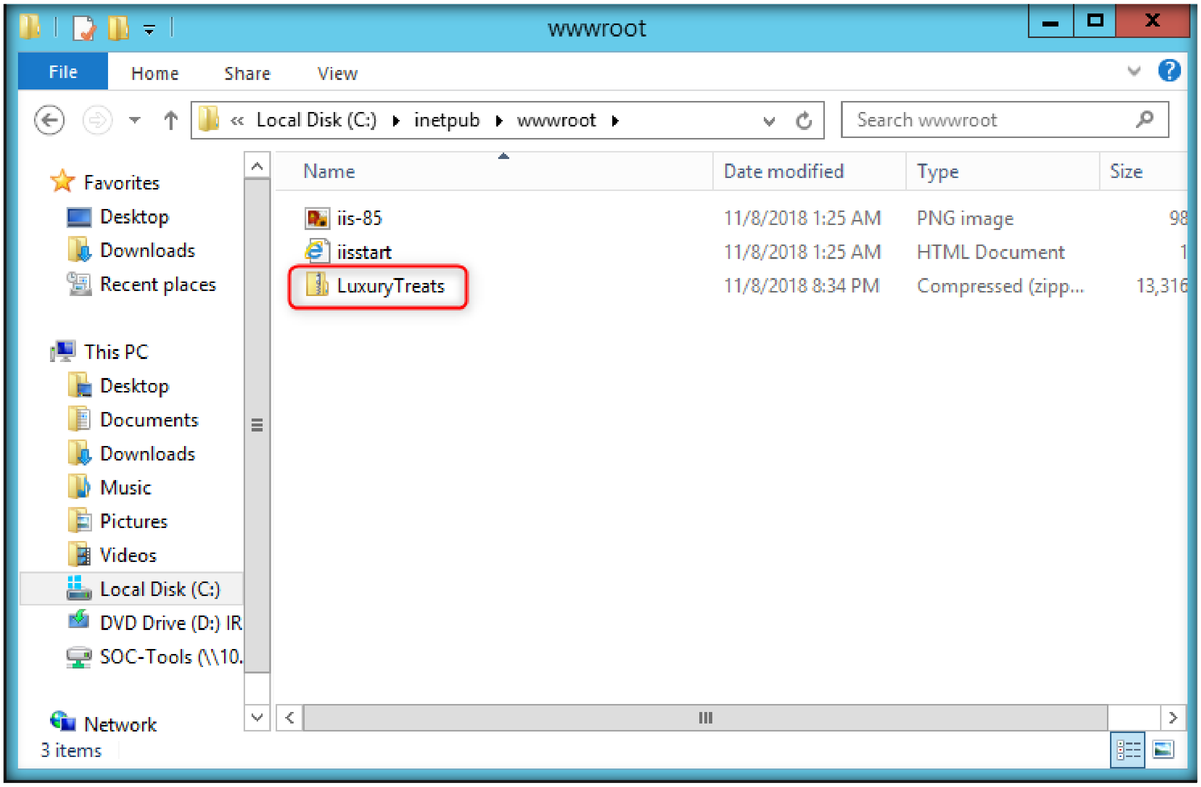
1. Navigate to **Z:\SOC-Tools\Lab Prerequisites** in guest operating systems.
2. Open **Web Browsers** folder.
3. Follow **wizard-driven** installation steps and install **Firefox** and **Chrome** web browsers.
4. You can also download **latest** version of web browsers from respective **vendors**.

CT#7.10: Configure the LuxuryTreats Website in Windows Server 2012 (Virtual Machine)

1. Navigate to **Z:\SOC-Tools\Lab Prerequisites\Websites**.
2. Right-click the **LuxuryTreats.zip** file select copy from the context menu to copy the file.

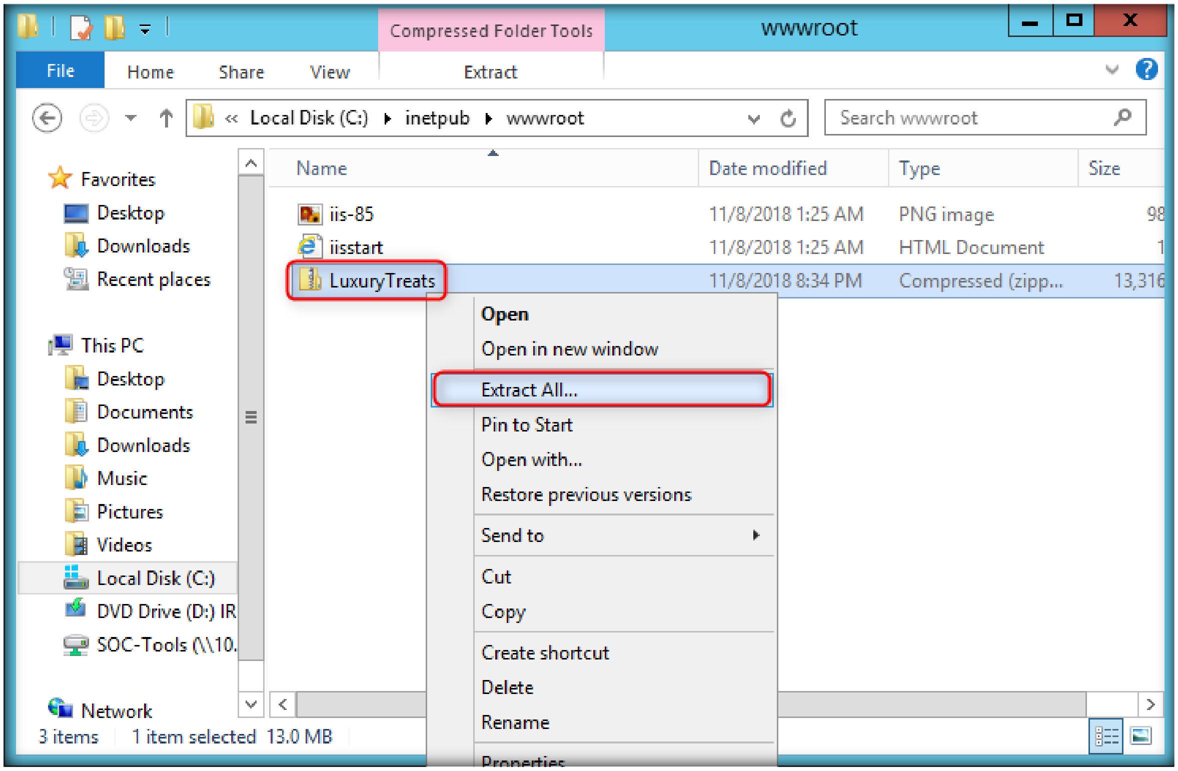


3. Navigate to **C:\inetpub\wwwroot** folder and past the copied LuxuryTreats.zip file.



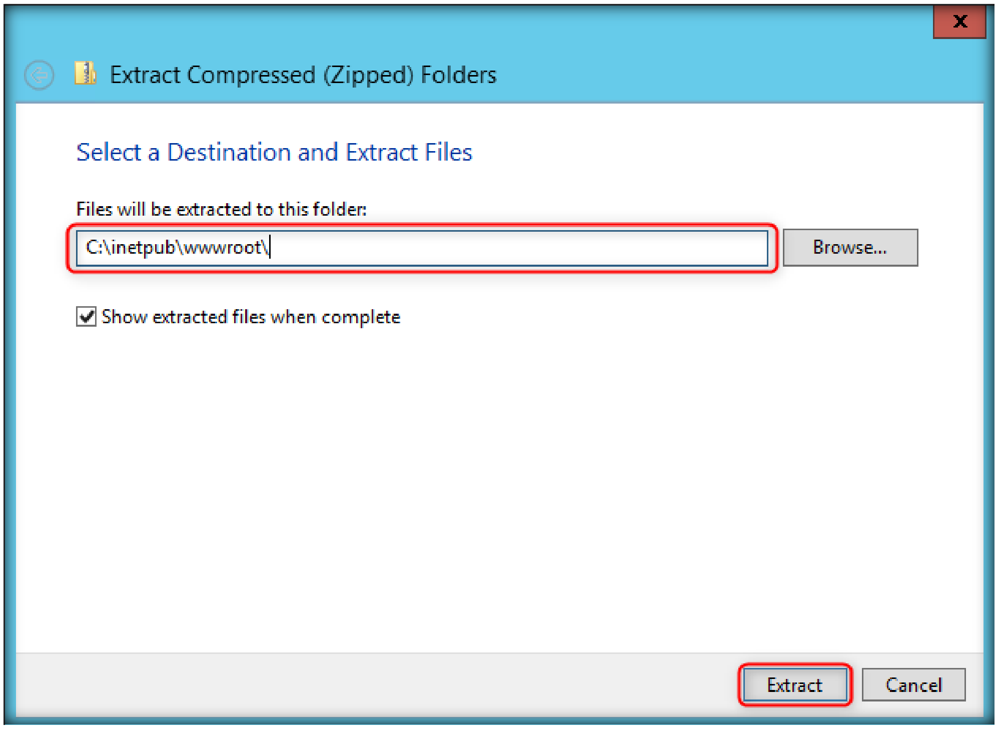
Name	Date modified	Type	Size
iis-85	11/8/2018 1:25 AM	PNG image	98
iisstart	11/8/2018 1:25 AM	HTML Document	1
LuxuryTreats	11/8/2018 8:34 PM	Compressed (zipp...	13,316

4. Right-click the **LuzuryTreats.zip** file and click **Extract All** option from the context menu.



Name	Date modified	Type	Size
iis-85	11/8/2018 1:25 AM	PNG image	98
iisstart	11/8/2018 1:25 AM	HTML Document	1
LuxuryTreats	11/8/2018 8:34 PM	Compressed (zipp...	13,316

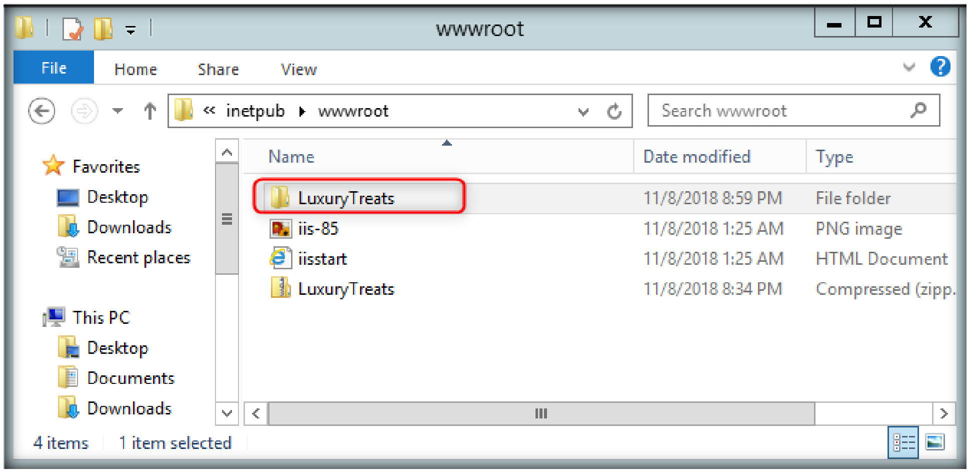
5. Change the Destination folder to **C:/inetpub/wwwroot/** and click **Extract**.


Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Browse...
Extract
Cancel

Files will be extracted to this folder:
C:\inetpub\wwwroot\

☑ Show extracted files when complete

6. LuxuryTreats.zip file will be extracted, and you will see a **LuxuryTreats** folder created in **C:/inetpub/wwwroot. Delete** the LuxuryTreats.zip file. After extracting the LuxuryTreats folder delete the LuxuryTreats.zip file.



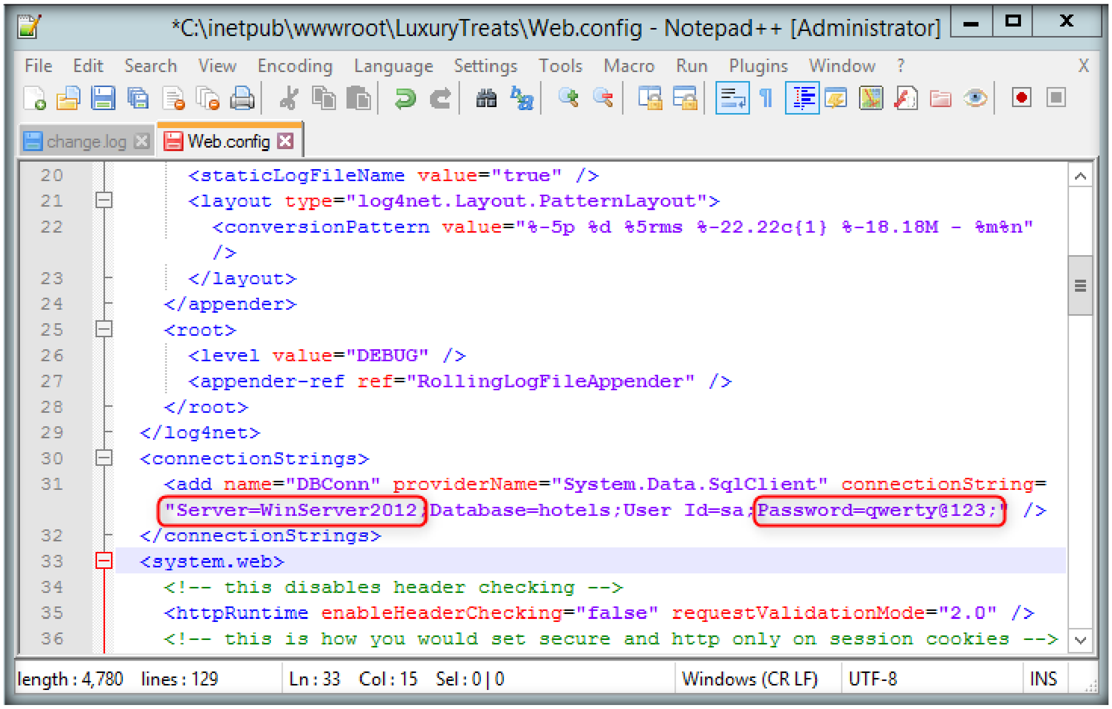
Name	Date modified	Type
LuxuryTreats	11/8/2018 8:59 PM	File folder
iis-85	11/8/2018 1:25 AM	PNG image
iisstart	11/8/2018 1:25 AM	HTML Document
LuxuryTreats	11/8/2018 8:34 PM	Compressed (zipp.

4 items 1 item selected

7. Open **LuxuryTreats** folder from **C:\inetpub\wwwroot\** and open **Web.config** file in notepad++ or in notepad.

8. Scroll down to **connectionStrings** tag, Replace Server with your machine's name in the **connectionString** property of DBConn connection string as shown in the screenshot.

   Note: If you have changed the password of sa user while installing SQL Server, change the password in the connection string to given password for SQL Server **sa** user while installing SQL Server.

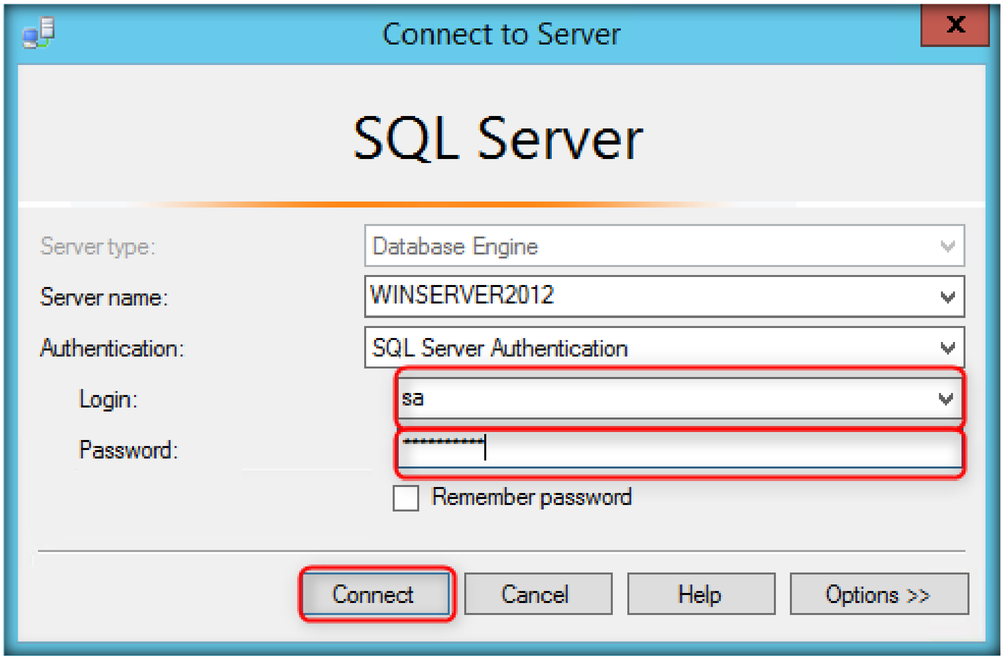


*C:\inetpub\wwwroot\LuxuryTreats\Web.config - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
Web.config
length : 4,780 lines : 129
Ln : 33 Col : 15 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS

```
      <staticLogFileName value="true" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%-5p %d %5rms %-22.22c{1} %-18.18M - %m%n"
        />
      </layout>
    </appender>
    <root>
      <level value="DEBUG" />
      <appender-ref ref="RollingLogFileAppender" />
    </root>
  </log4net>
  <connectionStrings>
    <add name="DBConn" providerName="System.Data.SqlClient" connectionString=
    "Server=WinServer2012;Database=hotels;User Id=sa;Password=qwerty@123;" />
  </connectionStrings>
  <system.web>
    <!-- this disables header checking -->
    <httpRuntime enableHeaderChecking="false" requestValidationMode="2.0" />
    <!-- this is how you would set secure and http only on session cookies -->
```

9. **Save** the file and **close** it.

10. Now, **launch** SQL Server 2016 Management Studio and click **Connect.**



Server type: Database Engine

Server name: WINSERVER2012

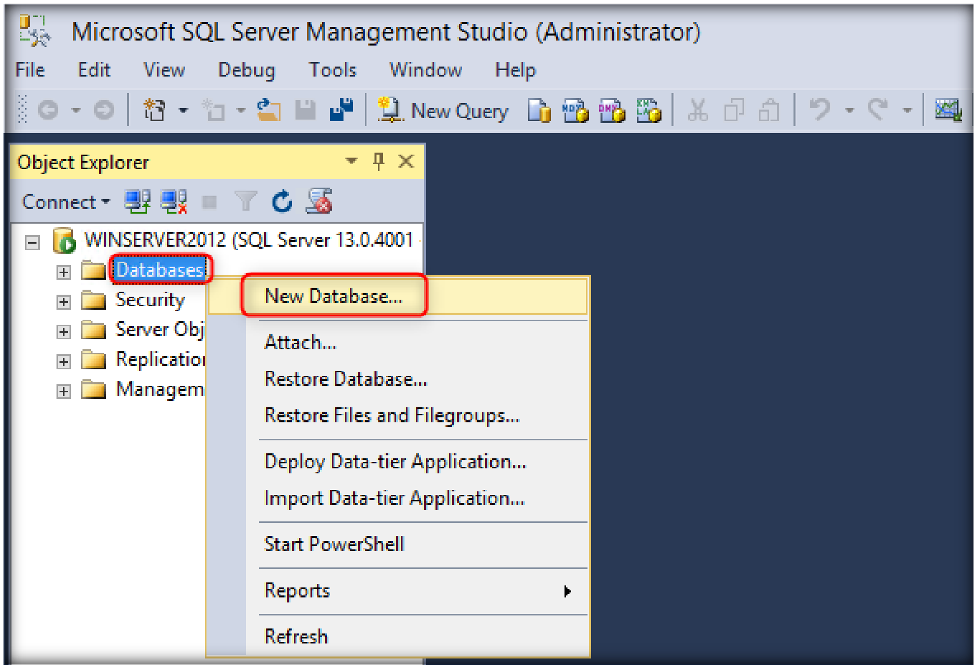
Authentication: SQL Server Authentication

Login: sa

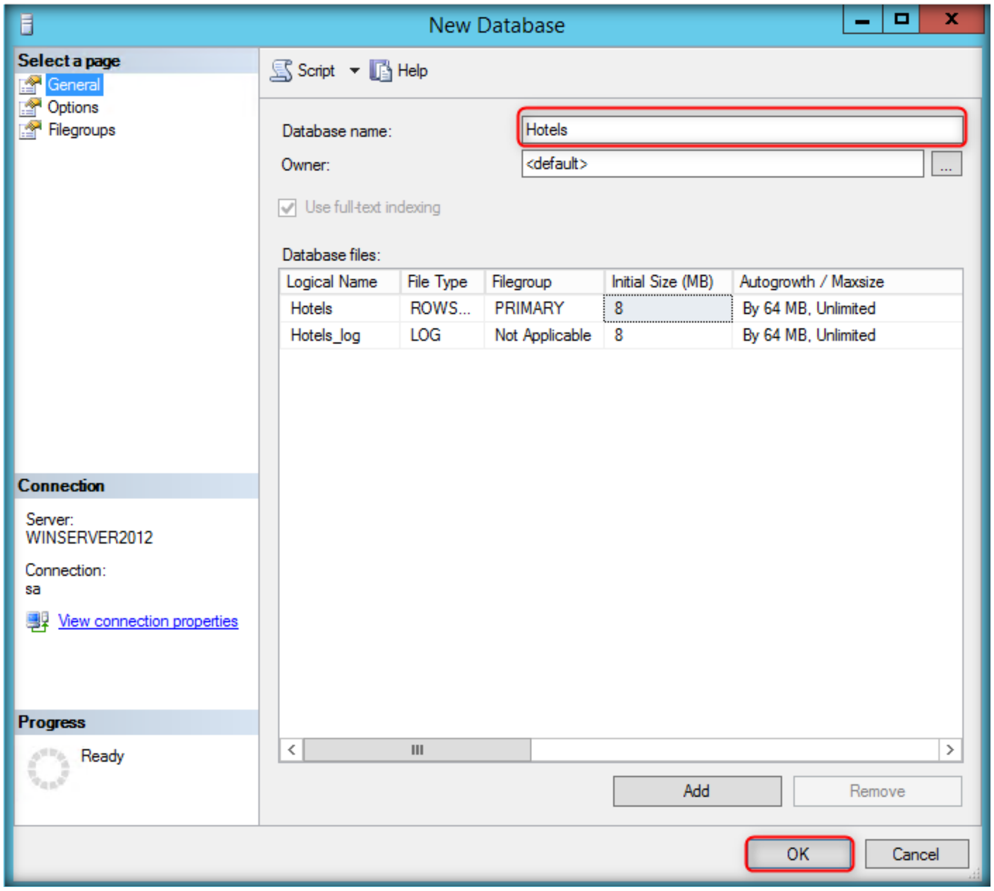
Password: ************

□ Remember password

11. **Microsoft SQL Server Management Studio** window, right-click on **Databases** and select **New Database.**


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
WINSERVER2012 (SQL Server 13.0.4001
Databases
Security
Server Obj
Replicatio
Managem
New Database...
Attach...
Restore Database...
Restore Files and Filegroups...
Deploy Data-tier Application...
Import Data-tier Application...
Start PowerShell
Reports
Refresh

12. **New Database** window appears, specify **Database name** as **Hotels** and click **OK**.



Database name: Hotels

Owner: <default>

☑ Use full-text indexing

Server: WINSERVER2012

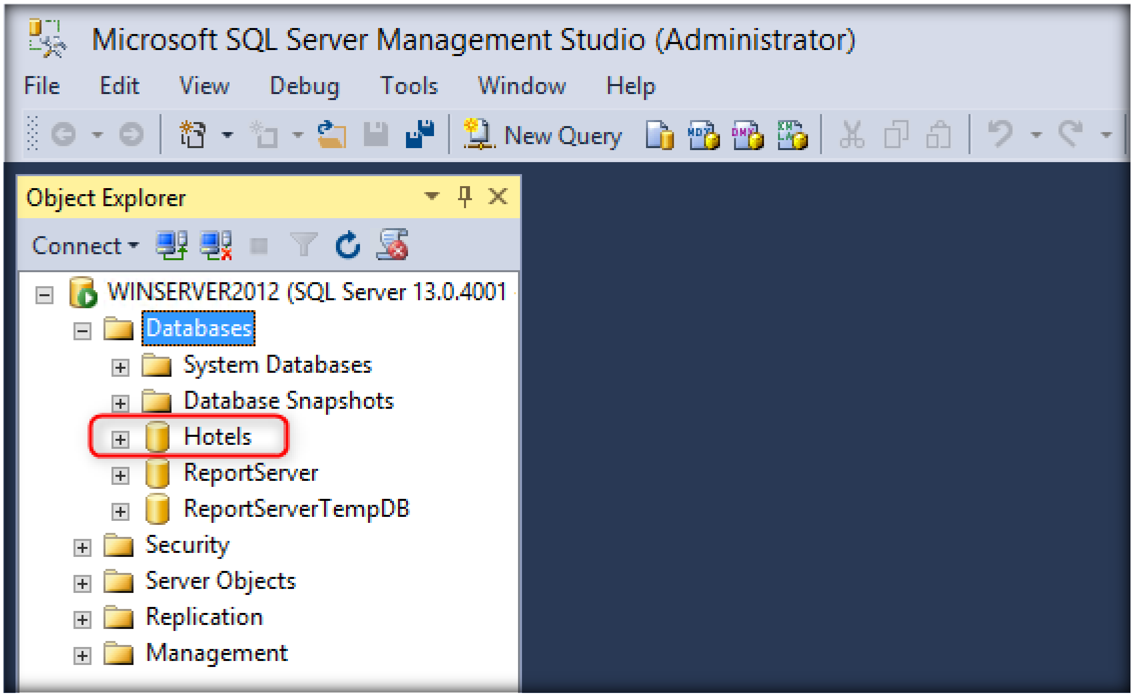
Connection: sa

View connection properties

Database files:

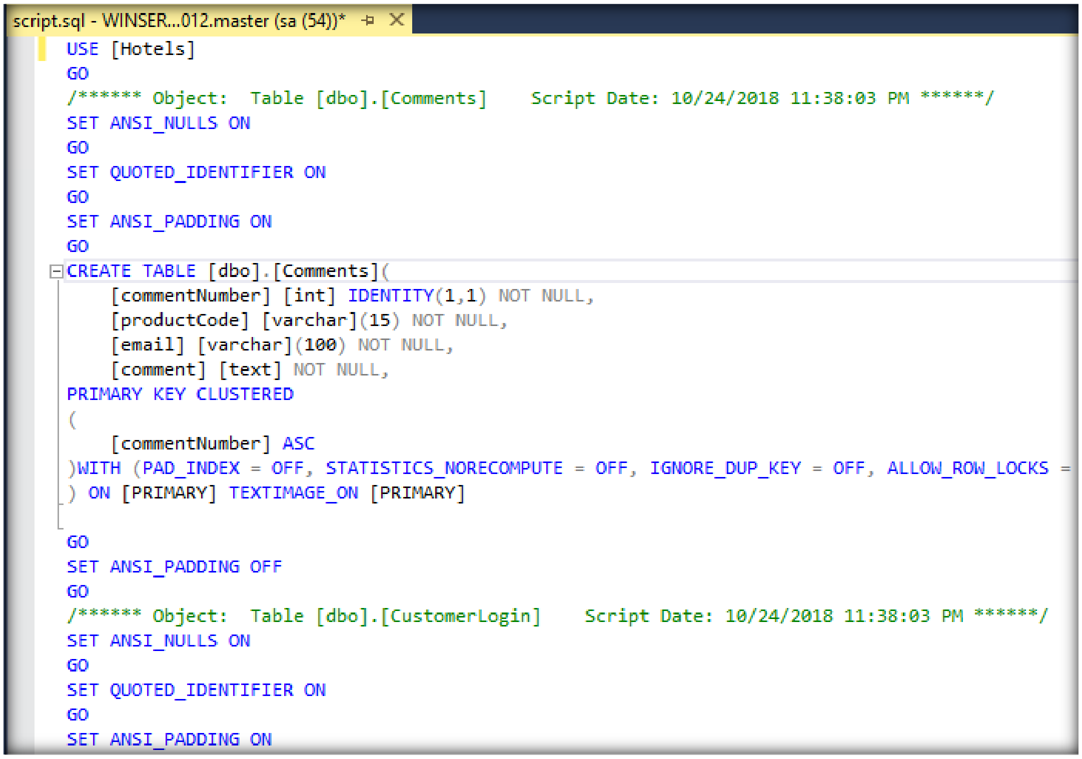
Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Maxsize
Hotels	ROWS...	PRIMARY	8	By 64 MB, Unlimited
Hotels_log	LOG	Not Applicable	8	By 64 MB, Unlimited

13. Now expand the **Databases** node. You will observe that Hotels database appears under the **Object Explorer** section, which implies that Hotels database has been **successfully** created.



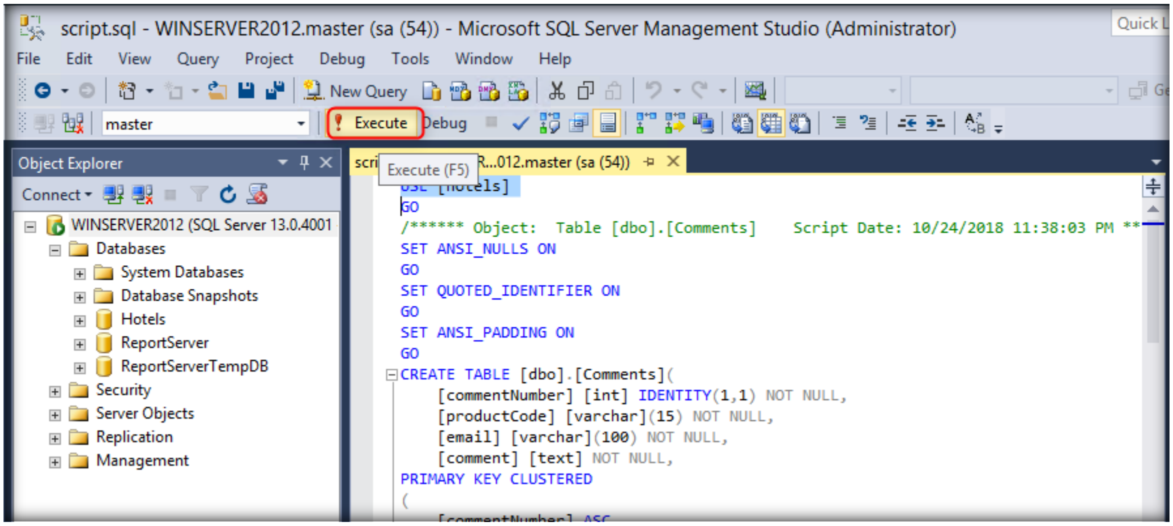
14. Navigate to **Z:\Lab Prerequisites\Website\DBScript**.

15. Double-click **Script.sql** file, it will open in **SQL Server Management Studio** Editor.If you are not connected to the database server Connect to Server Window appears give the username and password and connect to the database server.



```
USE [Hotels]
GO
/****** Object:  Table [dbo].[Comments]    Script Date: 10/24/2018 11:38:03 PM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
SET ANSI_PADDING ON
GO
CREATE TABLE [dbo].[Comments](
    [commentNumber] [int] IDENTITY(1,1) NOT NULL,
    [productCode] [varchar](15) NOT NULL,
    [email] [varchar](100) NOT NULL,
    [comment] [text] NOT NULL,
PRIMARY KEY CLUSTERED
(
    [commentNumber] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS =
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

GO
SET ANSI_PADDING OFF
GO
/****** Object:  Table [dbo].[CustomerLogin]    Script Date: 10/24/2018 11:38:03 PM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
SET ANSI_PADDING ON
```

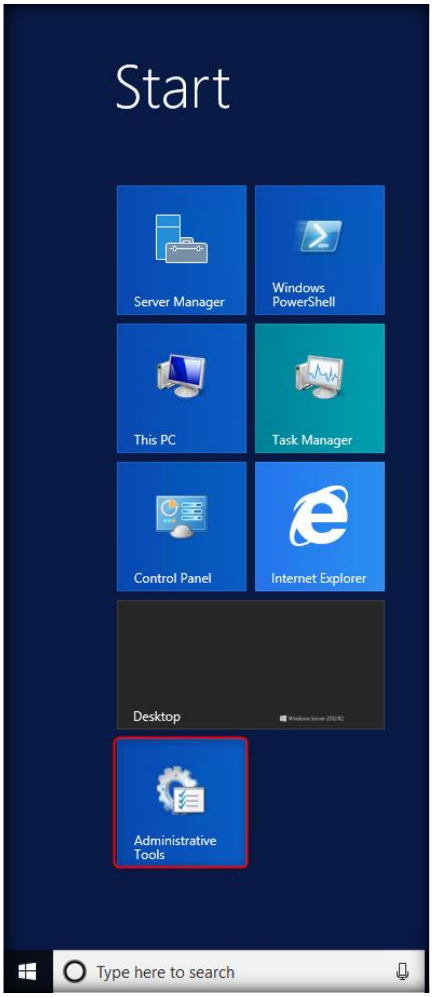
16. Now click Execute on the task bar.



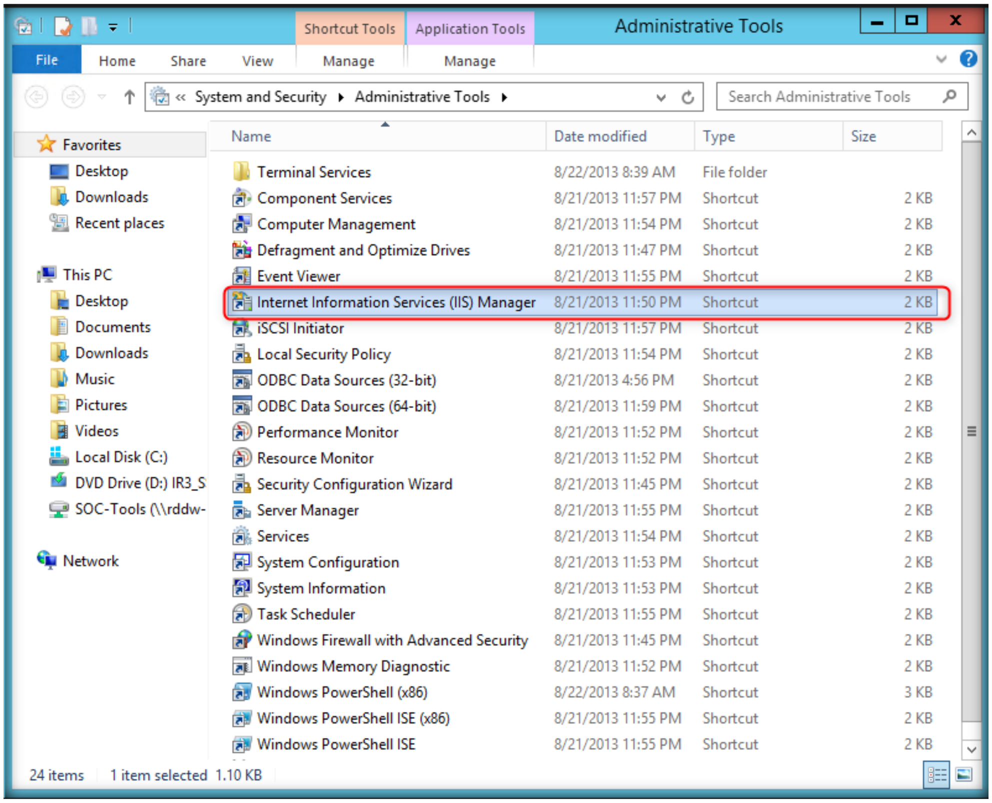
```
USE [Hotels]
GO
/****** Object:  Table [dbo].[Comments]    Script Date: 10/24/2018 11:38:03 PM **
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
SET ANSI_PADDING ON
GO
CREATE TABLE [dbo].[Comments](
    [commentNumber] [int] IDENTITY(1,1) NOT NULL,
    [productCode] [varchar](15) NOT NULL,
    [email] [varchar](100) NOT NULL,
    [comment] [text] NOT NULL,
PRIMARY KEY CLUSTERED
(
    [commentNumber] ASC
```

17. This process will create **necessary tables** in the **Hotels** database.

18. Now click **Start** menu button, click **Administrative Tools.**



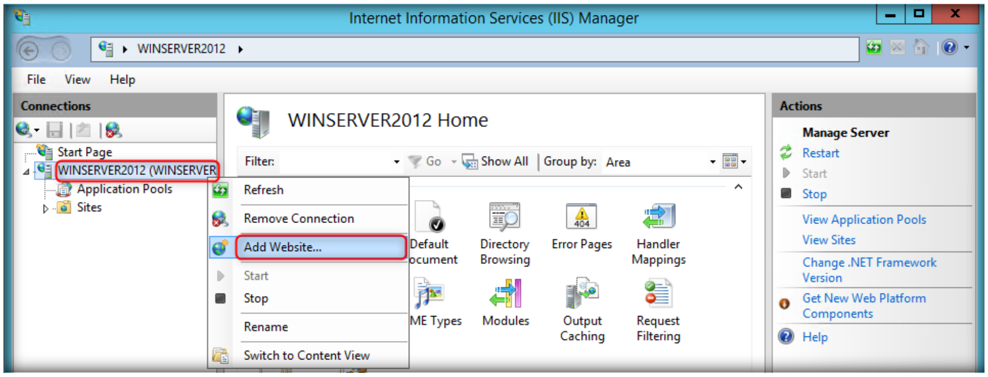
19. Double-click **on Internet Information Services (IIS) Manager**.



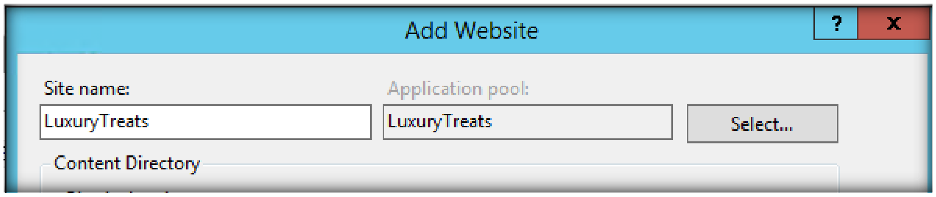
Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
Internet Information Services (IIS) Manager	8/21/2013 11:50 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB
Local Security Policy	8/21/2013 11:54 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/21/2013 4:56 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/21/2013 11:59 PM	Shortcut	2 KB
Performance Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Resource Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Security Configuration Wizard	8/21/2013 11:45 PM	Shortcut	2 KB
Server Manager	8/21/2013 11:55 PM	Shortcut	2 KB
Services	8/21/2013 11:54 PM	Shortcut	2 KB
System Configuration	8/21/2013 11:53 PM	Shortcut	2 KB
System Information	8/21/2013 11:53 PM	Shortcut	2 KB
Task Scheduler	8/21/2013 11:55 PM	Shortcut	2 KB
Windows Firewall with Advanced Security	8/21/2013 11:45 PM	Shortcut	2 KB
Windows Memory Diagnostic	8/21/2013 11:52 PM	Shortcut	2 KB
Windows PowerShell (x86)	8/22/2013 8:37 AM	Shortcut	3 KB
Windows PowerShell ISE (x86)	8/21/2013 11:55 PM	Shortcut	2 KB
Windows PowerShell ISE	8/21/2013 11:55 PM	Shortcut	2 KB

24 items 1 item selected 1.10 KB

20. Internet Information Services (IIS) Manager main window appears, now in Connections pane of the IIS Manager, right-click the **Machine Name** and click **Add Website** from context menu.



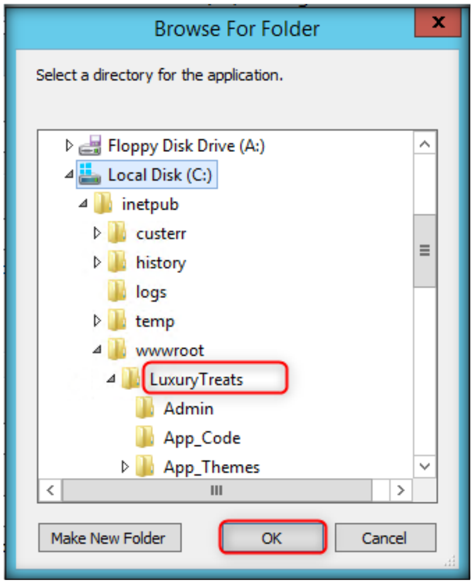
21. Add Website wizard appears, type the **Site** name in **Site name**: field and click on **Browse** button near **Physical path**: section. Here we are installing LuxuryTreats site, so we have provided **LuxuryTreats** in the Site name: field.



Site name: LuxuryTreats

Application pool: LuxuryTreats

22. **Browse** for Folder pop-up appears, navigate to C:\inetpub\wwwroot and choose **LuxuryTreats** folder and click **OK**.

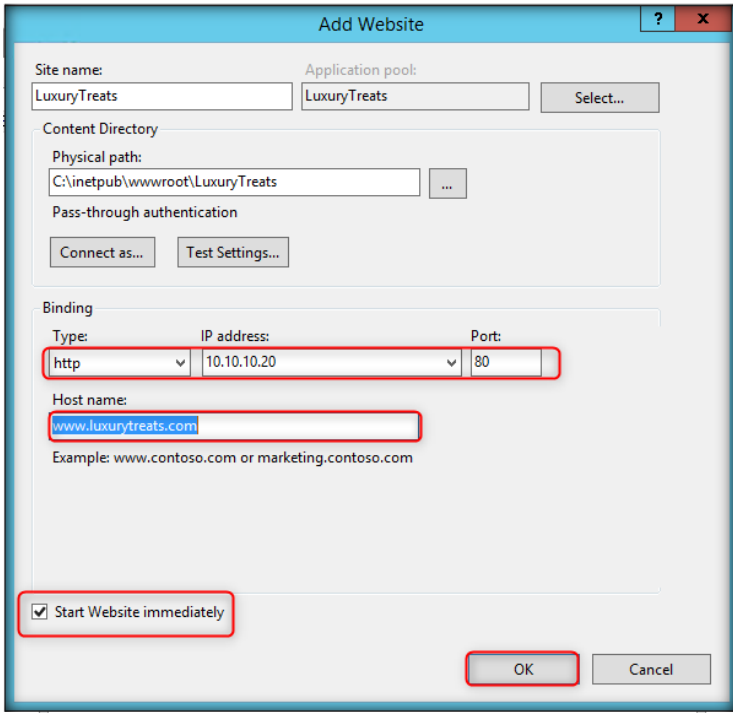


Browse For Folder

Select a directory for the application.

23. Now in Binding section choose **http** in Type: field. Choose the **Host machine IP address** (Internal adaptor - 10.10.10.12) from IP address: field, and choose **80** in Port: field.

24. Type www.luxurytreats.com in Hostname: field, make sure that **Start Website immediately** is checked and click **OK**.



Add Website

Site name: LuxuryTreats

Application pool: LuxuryTreats

Content Directory

Physical path: C:\inetpub\wwwroot\LuxuryTreats

Pass-through authentication

Binding

Type: http

IP address: 10.10.10.20

Port: 80

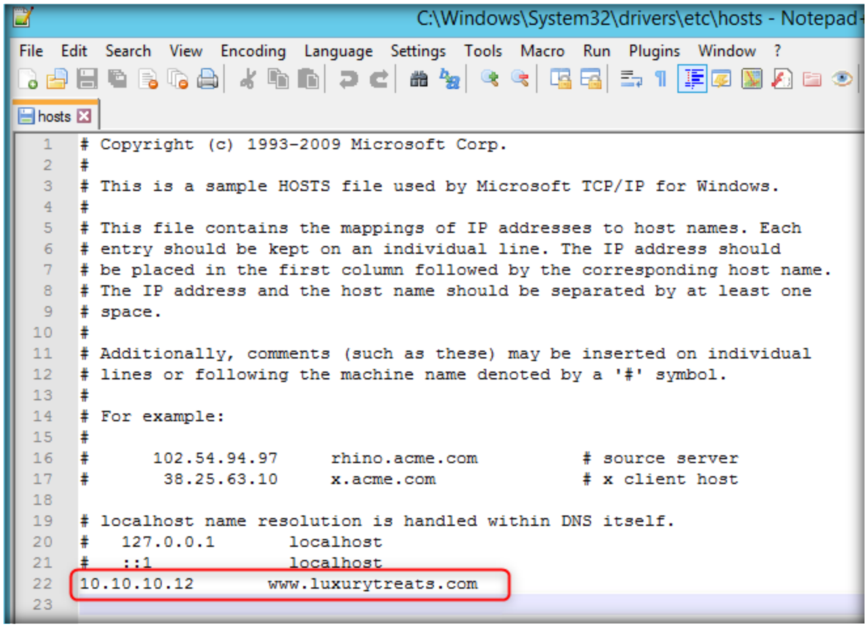
Host name: www.luxurytreats.com

Example: www.contoso.com or marketing.contoso.com

☑ Start Website immediately

CT#7.11: Configuring Host File in Windows Server 2012

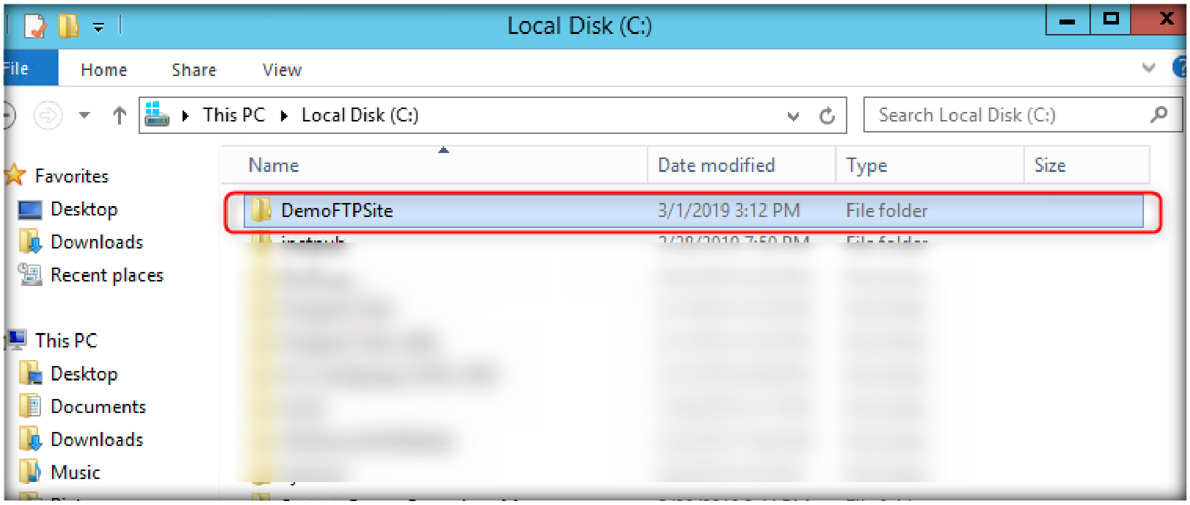
1. In Windows Server 2012 navigate to **C:\Windows\System32\drivers\etc** and right click on **hosts** file and click **Edit with Notepad++** from context menu.
2. Hosts file opens in Notepad++ type **<IP Address of the Windows Server 2012>** www.luxurytreats.com and click **Save** button and close the Notepad++ window.


C:\Windows\System32\drivers\etc\hosts - Notepad
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#    127.0.0.1       localhost
#    ::1             localhost
10.10.10.12        www.luxurytreats.com

```

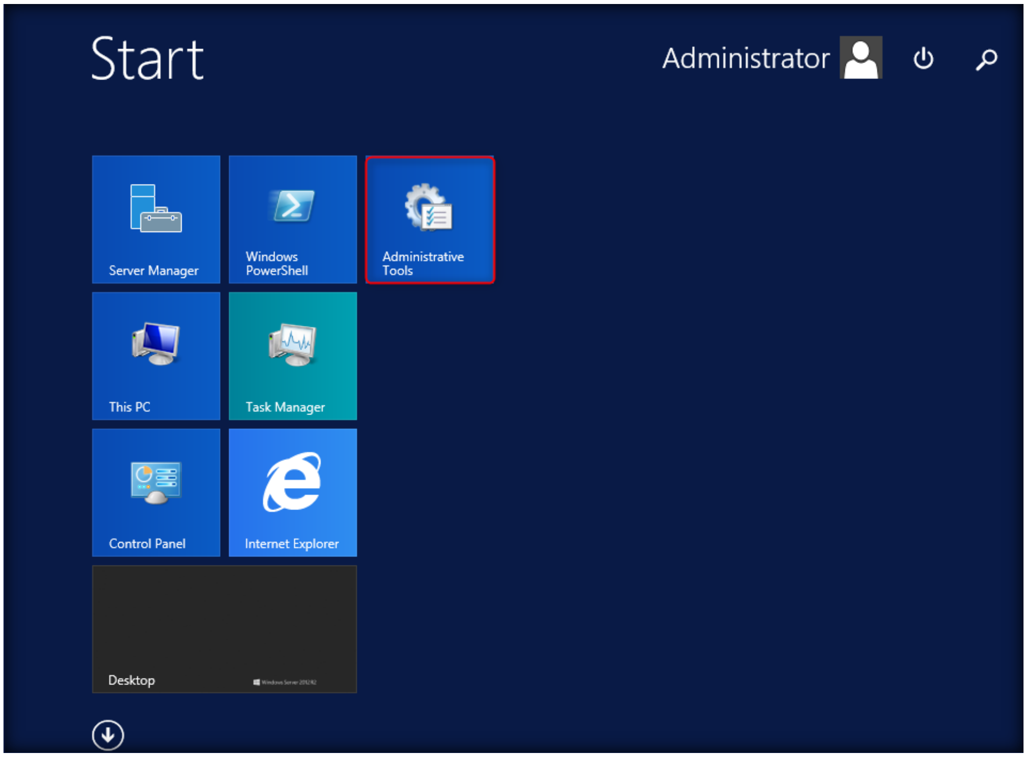
CT#7.12: Setting up FTP Site in Windows 2012

1. Navigate to **Z:\Lab Prerequisites\Website** and copy the **DemoFTPSite** in to C: drive.

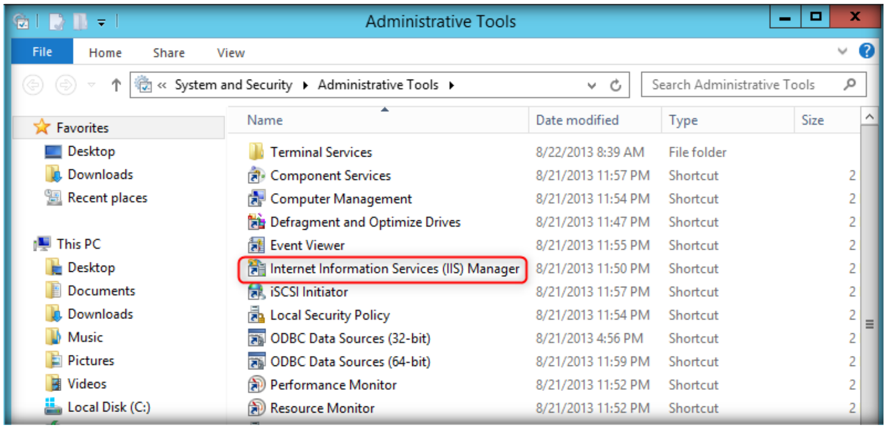


Name	Date modified	Type	Size
DemoFTPSite	3/1/2019 3:12 PM	File folder	

2. Click on **Windows Start** button →**Administrative Tools**.

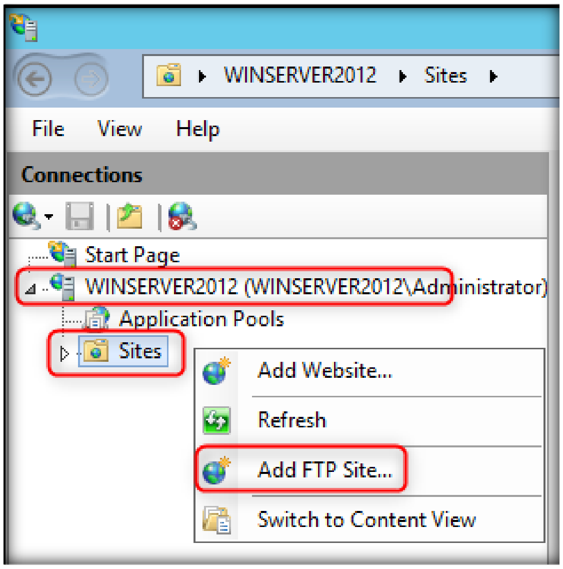

Start
Administrator
Server Manager
Windows PowerShell
Administrative Tools
This PC
Task Manager
Control Panel
Internet Explorer
Desktop

3. Double-Click on **Internet Information Services (IIS) Manager**.

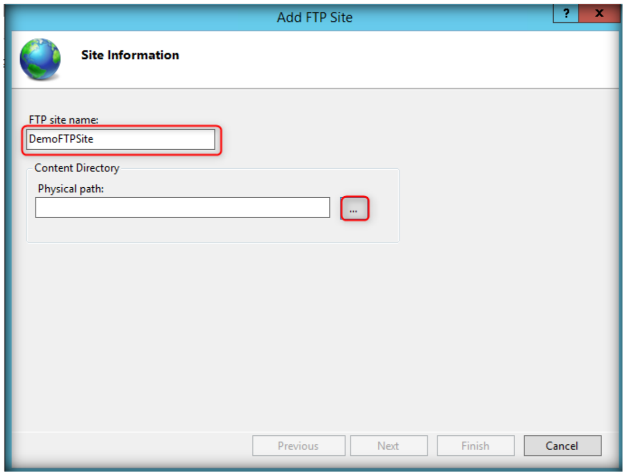


Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Component Services	8/21/2013 11:57 PM	Shortcut	2
Computer Management	8/21/2013 11:54 PM	Shortcut	2
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2
Event Viewer	8/21/2013 11:55 PM	Shortcut	2
Internet Information Services (IIS) Manager	8/21/2013 11:50 PM	Shortcut	2
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2
Local Security Policy	8/21/2013 11:54 PM	Shortcut	2
ODBC Data Sources (32-bit)	8/21/2013 4:56 PM	Shortcut	2
ODBC Data Sources (64-bit)	8/21/2013 11:59 PM	Shortcut	2
Performance Monitor	8/21/2013 11:52 PM	Shortcut	2
Resource Monitor	8/21/2013 11:52 PM	Shortcut	2

4. In the IIS Manager window expand **WINSERVER2012.** Right-click on **Sites** and click on **Add FTP Site** from the context menu.



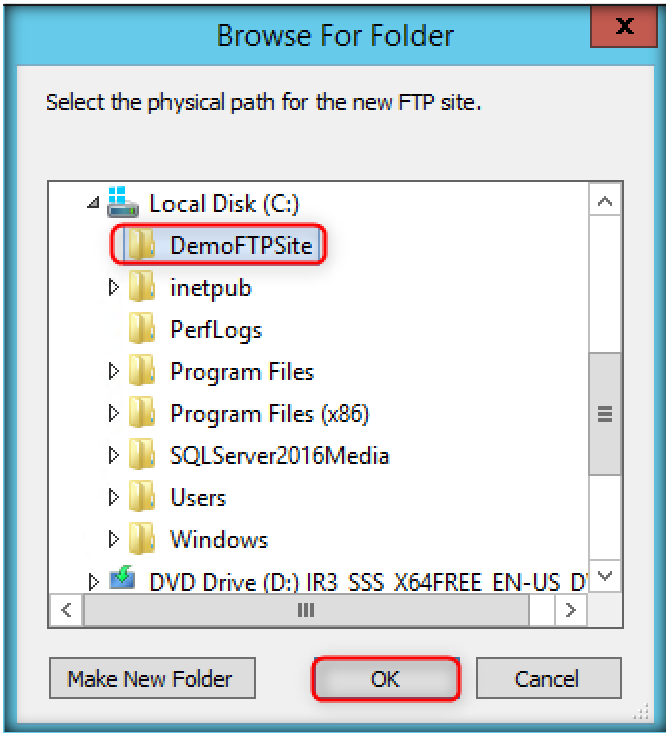
5. Give FTP site name as **DemoFTPSite. Click … ellipse button.**



FTP site name: DemoFTPSite

Physical path:

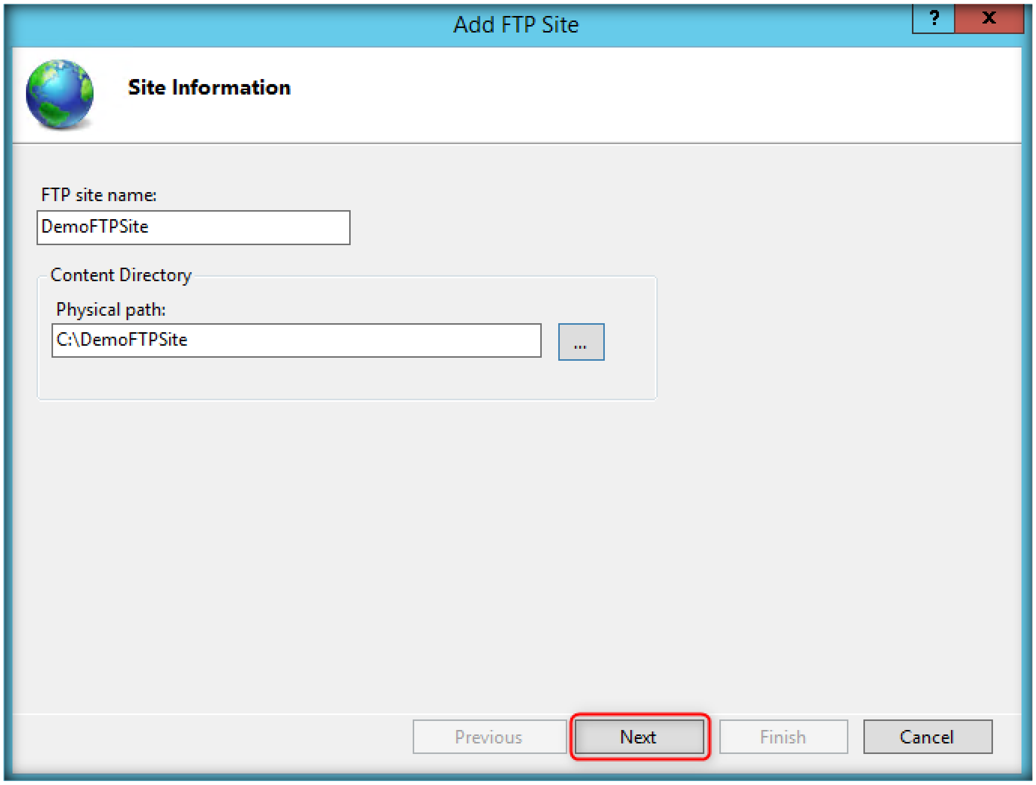
6. **Browse for folder** dialog box appears, navigate to **C:\DemoFTPSite and** click **OK**.



Browse For Folder

Select the physical path for the new FTP site.

7. The physical path will be set to C:\DemoFTPSite. Click **Next.**



Add FTP Site

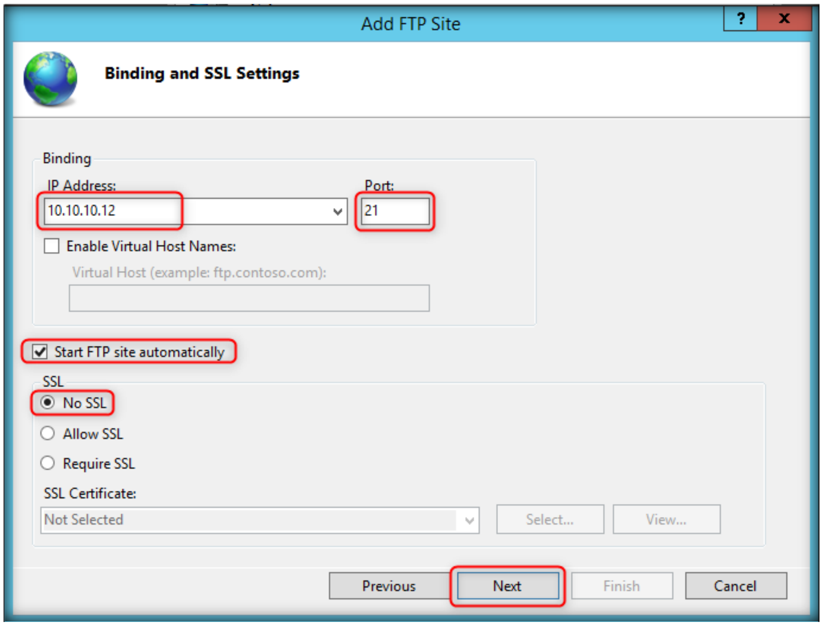
Site Information

FTP site name: DemoFTPSite

Content Directory

Physical path: C:\DemoFTPSite

8. Select IP Address **10.10.10.12** from the IP Address dropdown Port: **21** and check **Start FTP site automatically**. Select **No SSL** as **SLL** option and click **Next.**



Add FTP Site

Binding and SSL Settings

Binding

IP Address: 10.10.10.12

Port: 21

□ Enable Virtual Host Names:

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

☑ Start FTP site automatically

SSL

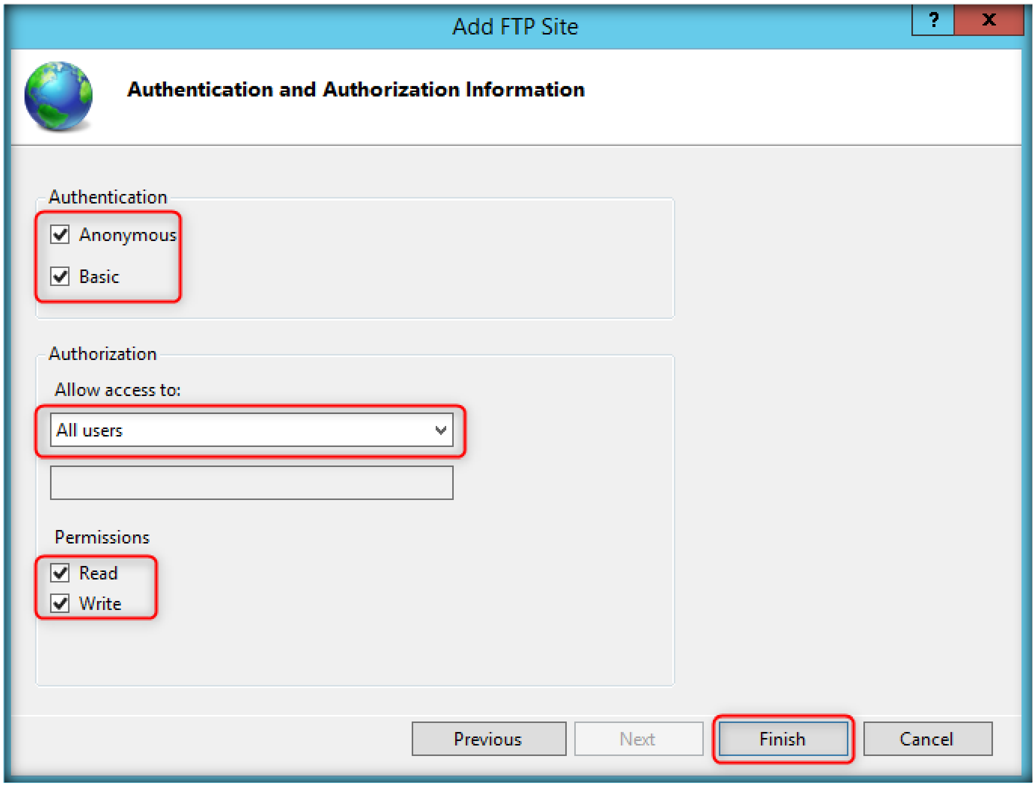
● No SSL

○ Allow SSL

○ Require SSL

SSL Certificate: Not Selected

9. Check **Anonymous** and **Basic** for Authentication. Select **Allow access to: All users** as Authorization and check Permissions: **Read and Write** click **Finish.**



Add FTP Site

Authentication and Authorization Information

Authentication

☑ Anonymous

☑ Basic

Authorization

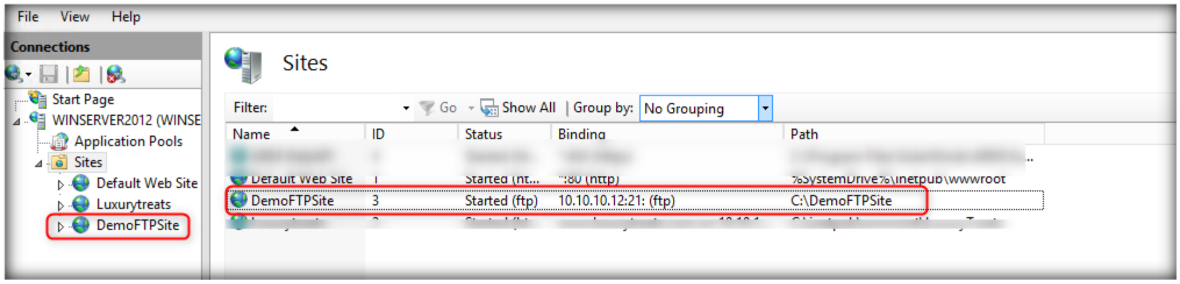
Allow access to: All users

Permissions

☑ Read

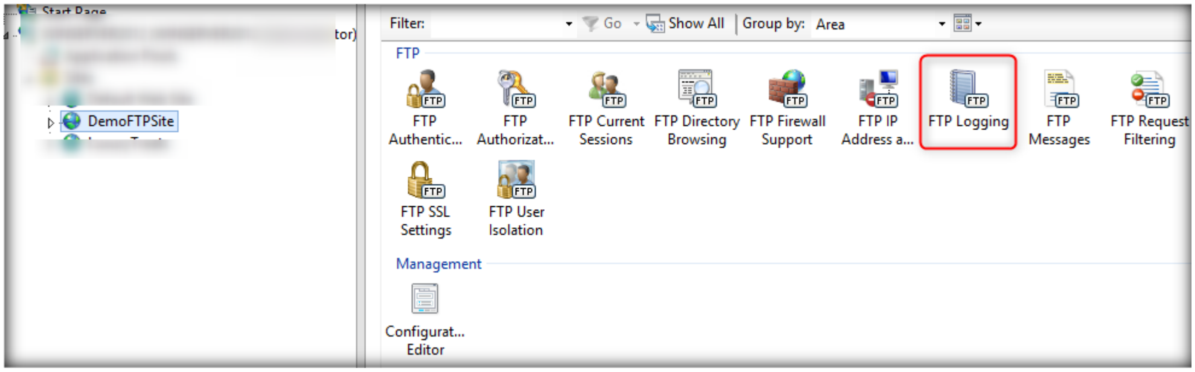
☑ Write

10. You will see that **DemoFTPSite** will be successfully created in IIS Manager.

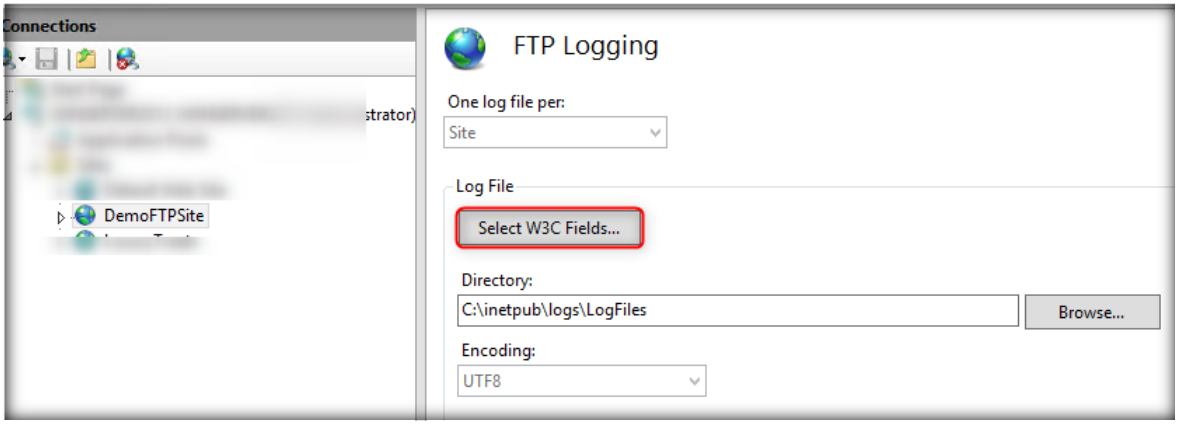


Name	ID	Status	Binding	Path
Default Web Site	1	Started (ht...	*:80 (http)	%SystemDrive%\inetpub\wwwroot
DemoFTPSite	3	Started (ftp)	10.10.10.12:21: (ftp)	C:\DemoFTPSite

11. Click on **DemoFTPSite** and double-click on **FTP Logging** as shown in following screenshot.



12. Click on **Select W3C Fields…** button.



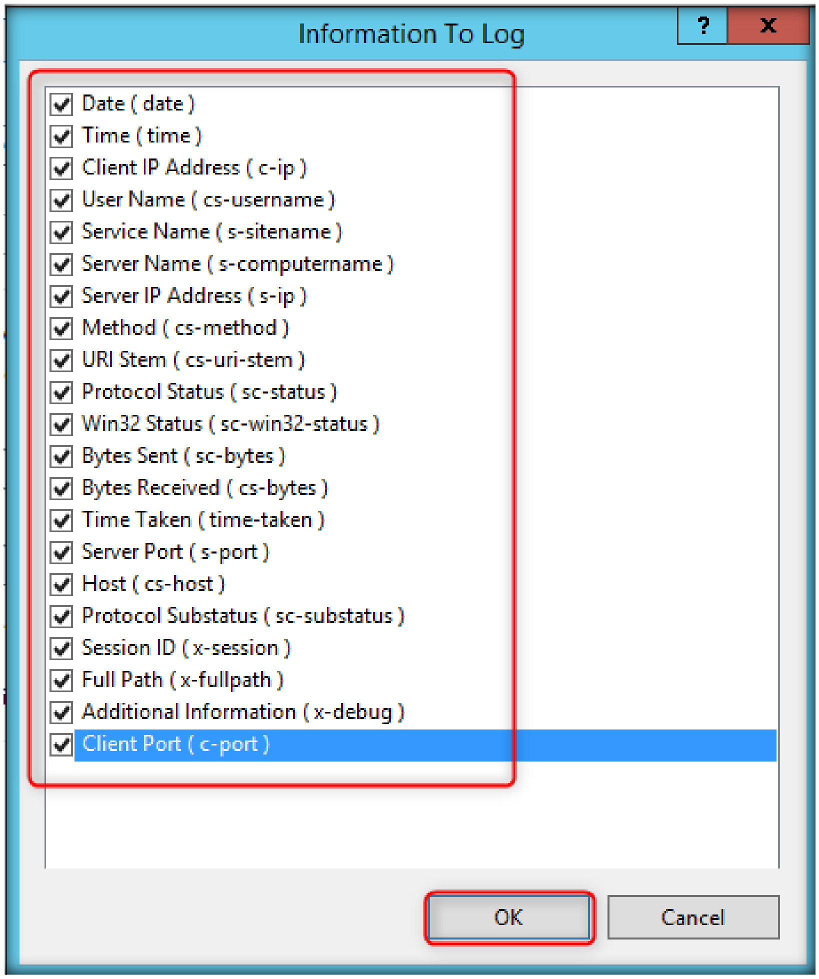
One log file per: Site

Log File

Directory: C:\inetpub\logs\LogFiles

Encoding: UTF8

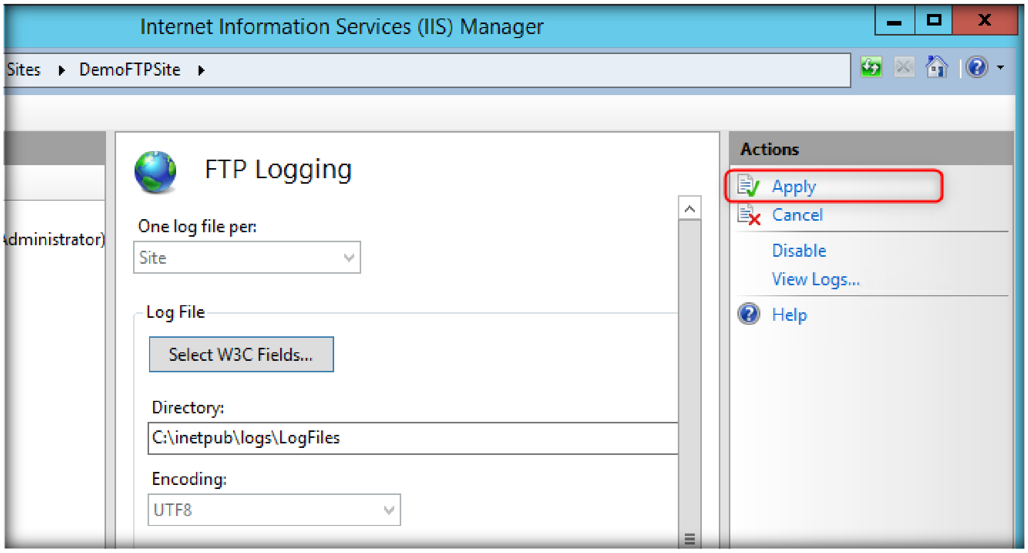
13. Tick All check boxes available in **Information to Log** window and click OK.



Information To Log

- ☑ Date (date)
- ☑ Time (time)
- ☑ Client IP Address (c-ip)
- ☑ User Name (cs-username)
- ☑ Service Name (s-sitename)
- ☑ Server Name (s-computername)
- ☑ Server IP Address (s-ip)
- ☑ Method (cs-method)
- ☑ URI Stem (cs-uri-stem)
- ☑ Protocol Status (sc-status)
- ☑ Win32 Status (sc-win32-status)
- ☑ Bytes Sent (sc-bytes)
- ☑ Bytes Received (cs-bytes)
- ☑ Time Taken (time-taken)
- ☑ Server Port (s-port)
- ☑ Host (cs-host)
- ☑ Protocol Substatus (sc-substatus)
- ☑ Session ID (x-session)
- ☑ Full Path (x-fullpath)
- ☑ Additional Information (x-debug)
- ☑ Client Port (c-port)

14. Click **Apply** in right side **Action** pane.



Internet Information Services (IIS) Manager

Sites ▸ DemoFTPSite ▸

FTP Logging

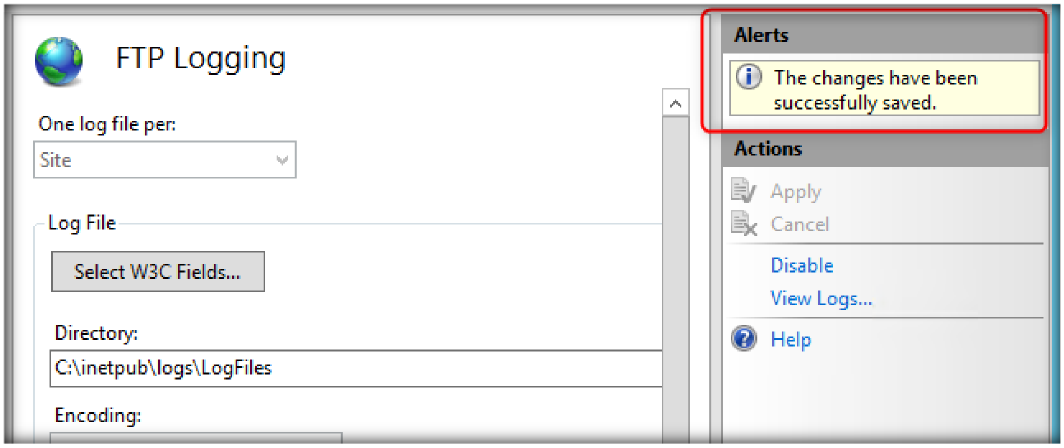
One log file per: Site

Log File

Directory: C:\inetpub\logs\LogFiles

Encoding: UTF8

15. You will see Alerts **The changes have been successfully saved**.



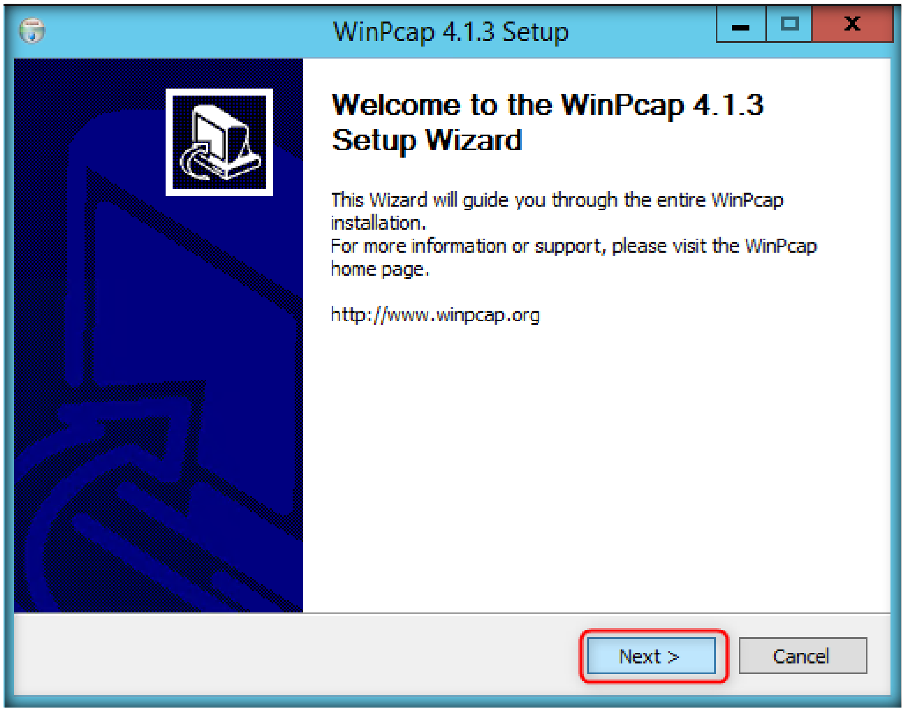
C:\inetpub\logs\LogFiles

The changes have been successfully saved.

16. Close all open windows.

CT#7.13: Installing WinPcap on Windows Server 2012

1. To install WinPcap, navigate to Z:\SOC-Tools\Prerequisite\WinPcap.
2. Double-click the **WinPcap_4_1_3.exe** file. **WinPcap 4.1.3 Setup** wizard will appear.
3. click **Next**.

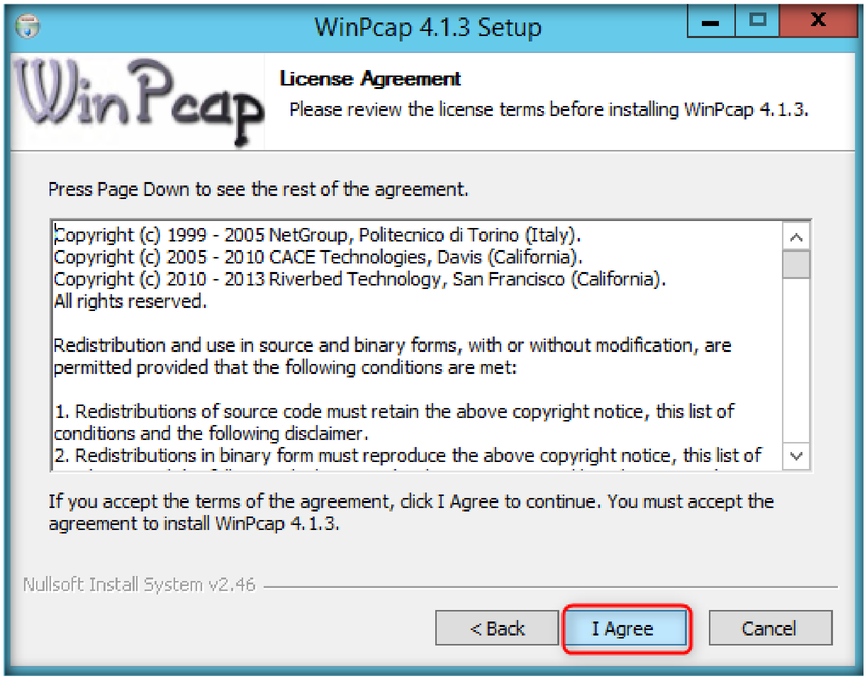


Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

4. Accept the **License Agreement**, and install WinPcap by selecting the options that appear **I Agree** in the wizard.



License Agreement

Please review the license terms before installing WinPcap 4.1.3.

Press Page Down to see the rest of the agreement.

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.

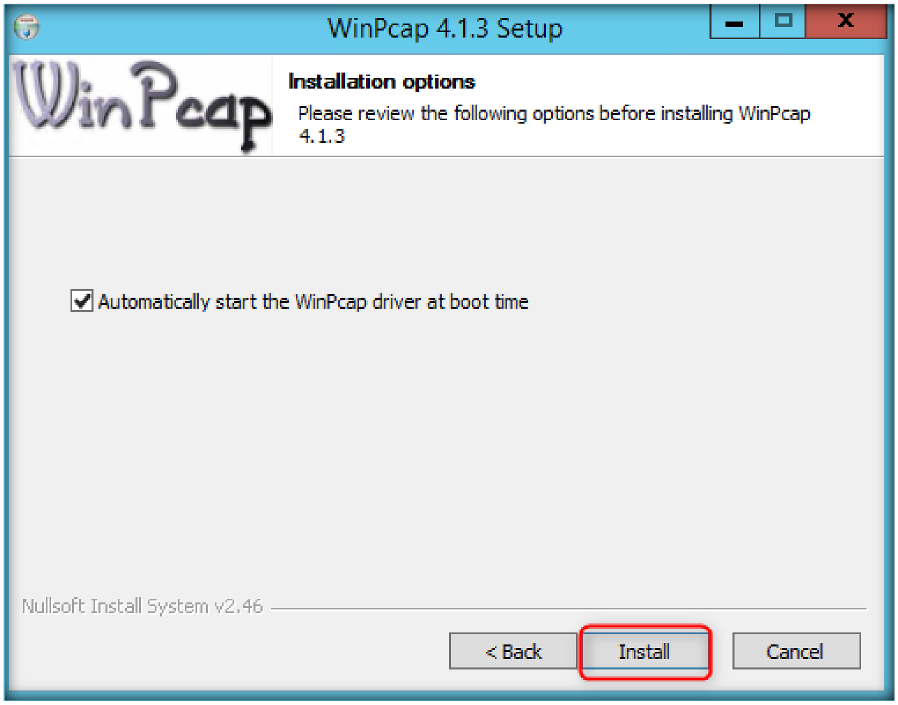
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.

Nullsoft Install System v2.46

5. Click on **Install** button.



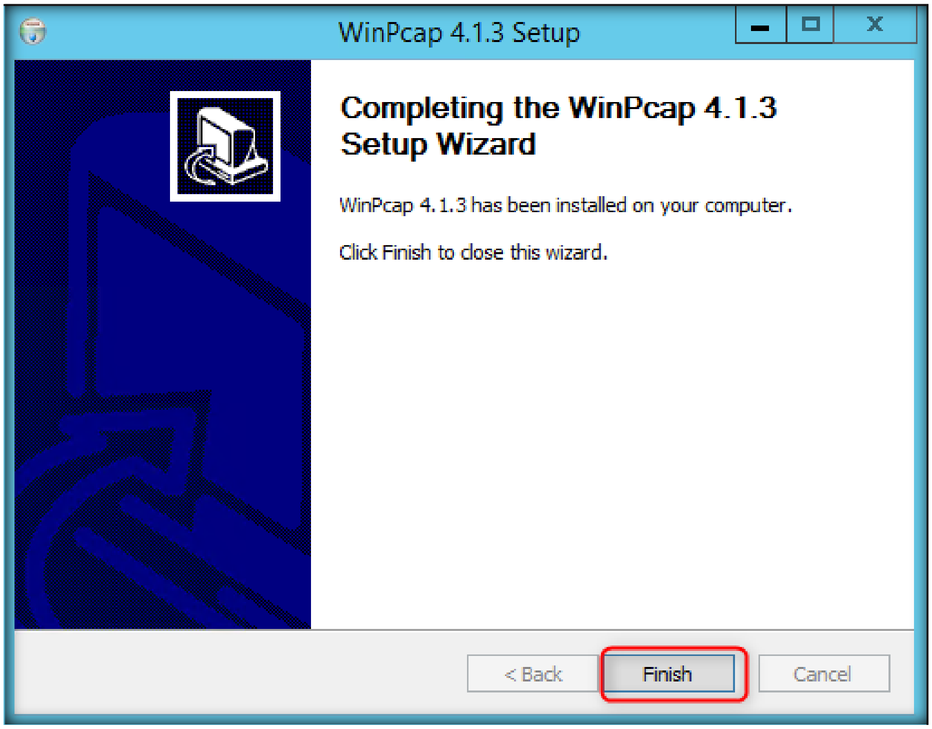
Installation options

Please review the following options before installing WinPcap 4.1.3

☑ Automatically start the WinPcap driver at boot time

Nullsoft Install System v2.46

6. Once Installation Complete Click Finish button to close this Wizard.



WinPcap 4.1.3 Setup

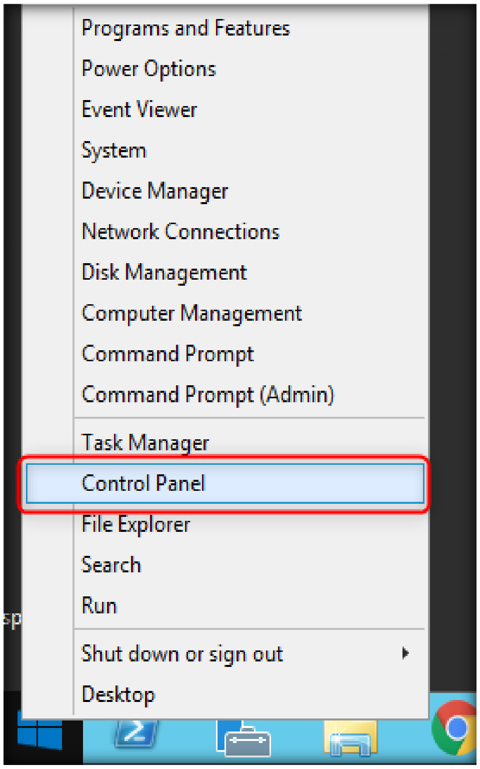
Completing the WinPcap 4.1.3 Setup Wizard

WinPcap 4.1.3 has been installed on your computer.

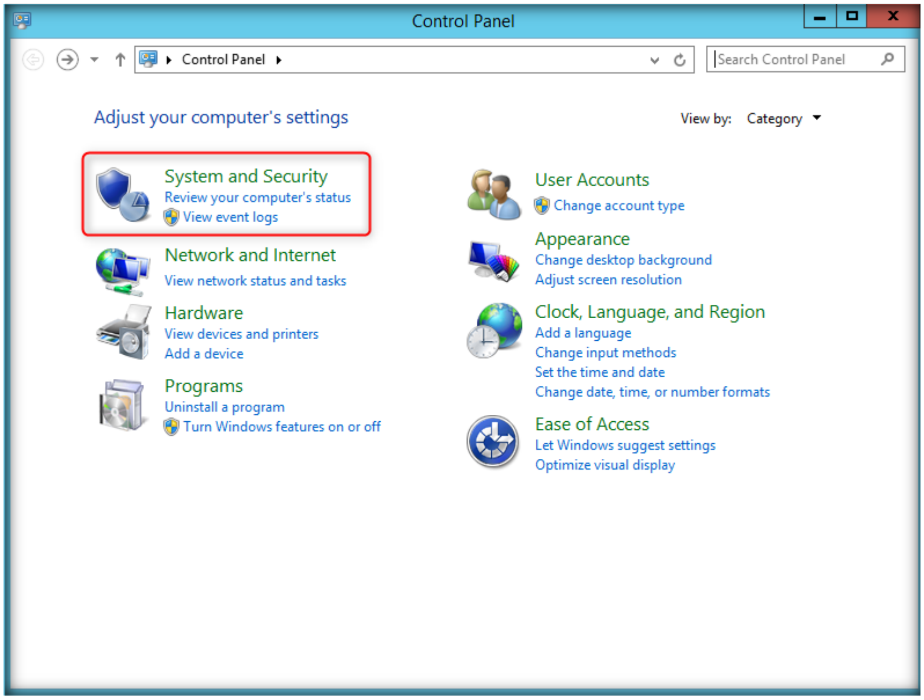
Click Finish to close this wizard.

CT#7.14: Turn off Windows Firewall in WinServer2012

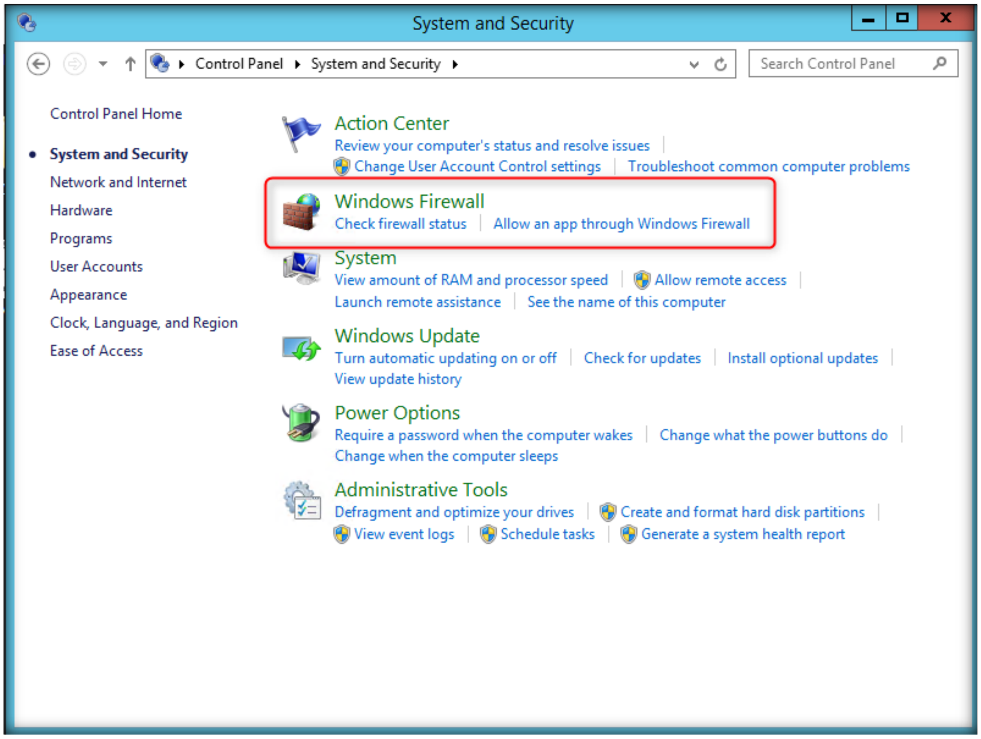
1. Right-click on Windows start button and click **Control Panel**.



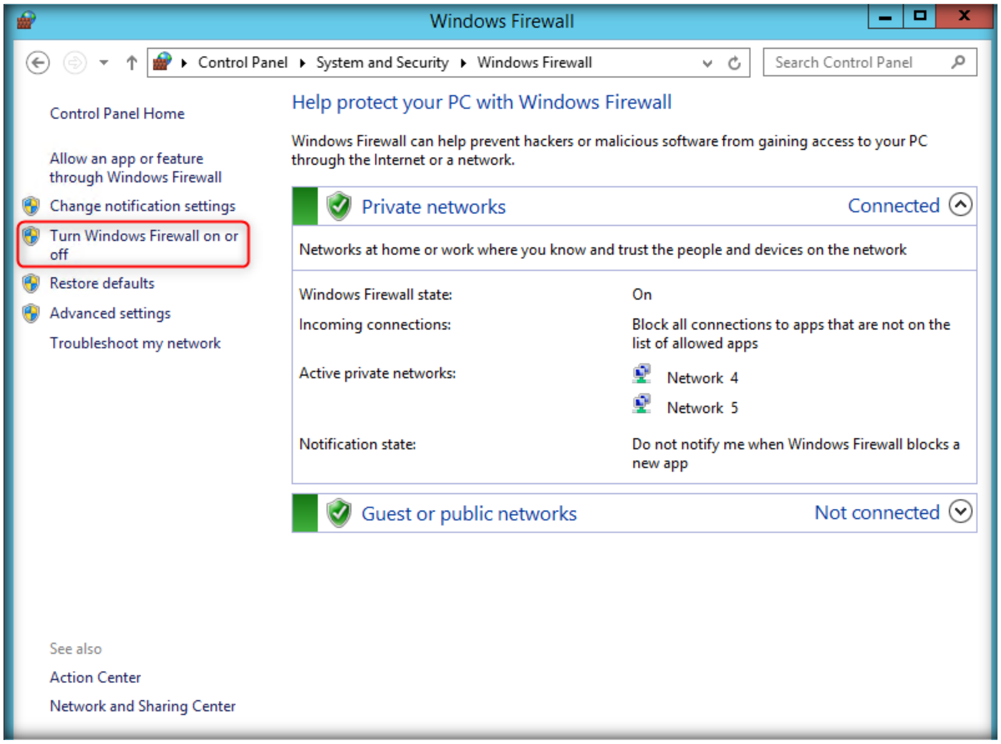
2. In the **Control Panel** window, click **System and Security**.



3. Click the **Windows Firewall** in the **System and Security** window.


System and Security
Control Panel
System and Security
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance
Clock, Language, and Region
Ease of Access
Action Center
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Windows Update
Turn automatic updating on or off
Check for updates
Install optional updates
View update history
Power Options
Require a password when the computer wakes
Change what the power buttons do
Change when the computer sleeps
Administrative Tools
Defragment and optimize your drives
Create and format hard disk partitions
View event logs
Schedule tasks
Generate a system health report

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


Windows Firewall
Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

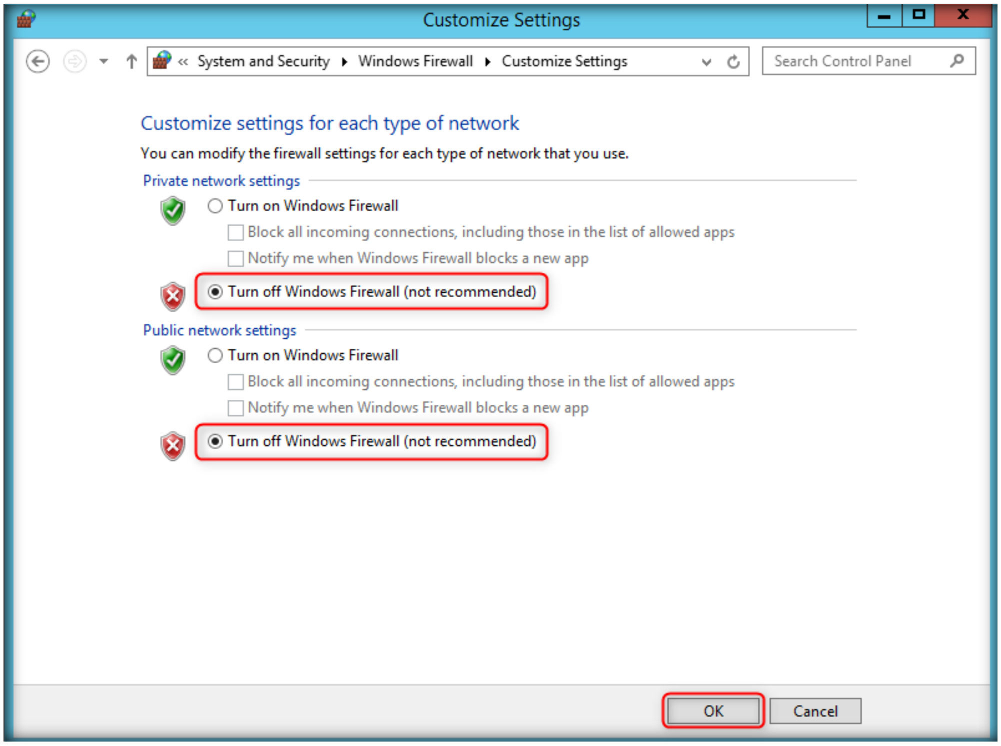
Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network 4 Network 5
Notification state:	Do not notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

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


Customize Settings
« System and Security ▸ Windows Firewall ▸ Customize Settings
Search Control Panel
OK
Cancel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

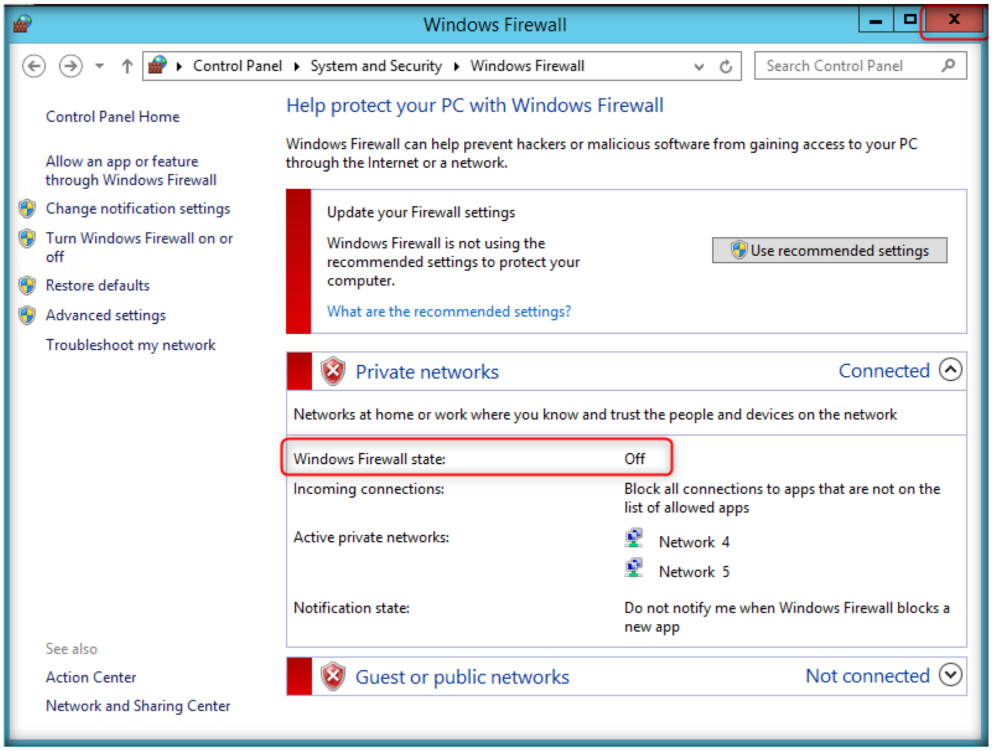
○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

6. You will see status of windows firewall is off, close the **Windows Firewall** window.


Windows Firewall
Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Use recommended settings
What are the recommended settings?
Private networks
Connected
Guest or public networks
Not connected

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

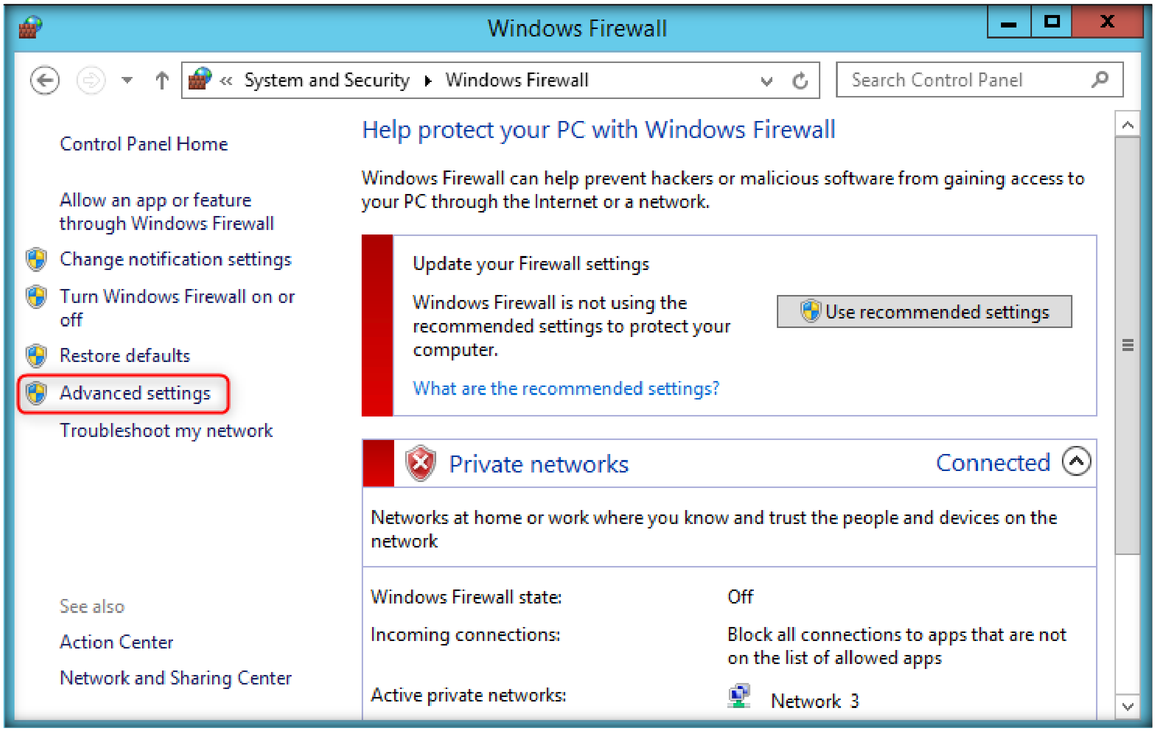
Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network 4 Network 5
Notification state:	Do not notify me when Windows Firewall blocks a new app

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


Windows Firewall
« System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Use recommended settings
What are the recommended settings?
Private networks
Connected

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

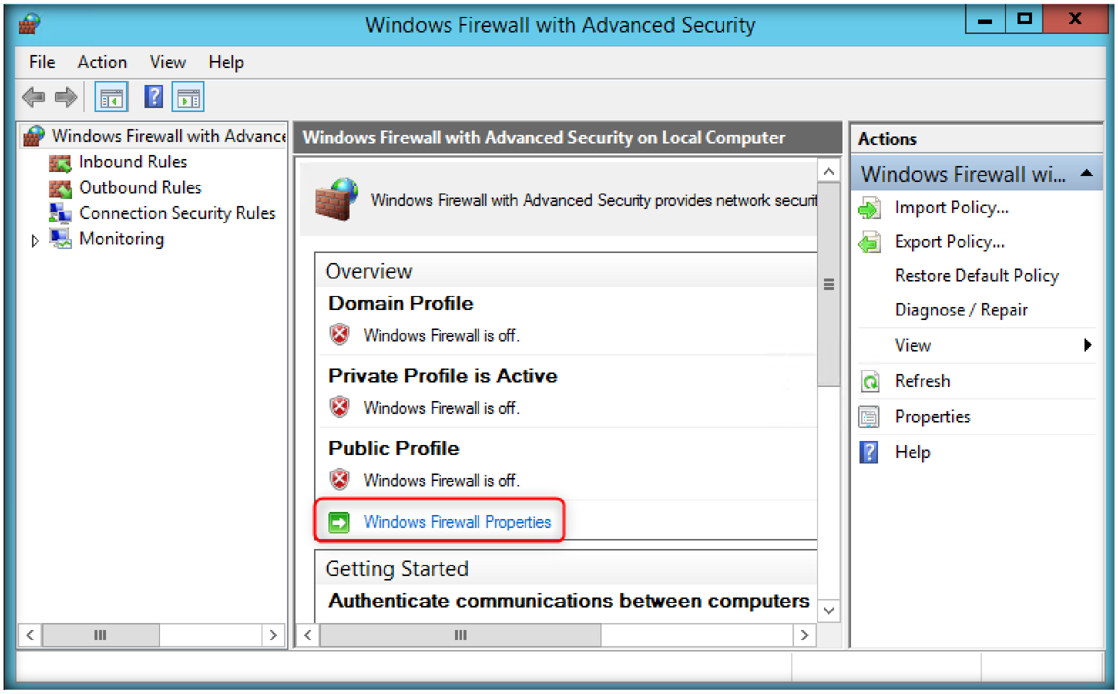
Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network 3

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



Windows Firewall with Advanced Security provides network securit

Overview

Domain Profile

Windows Firewall is off.

Private Profile is Active

Windows Firewall is off.

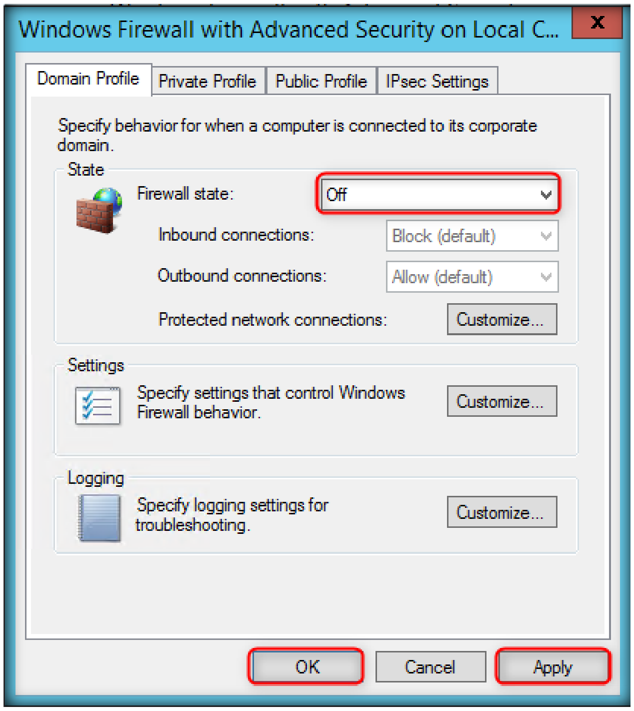
Public Profile

Windows Firewall is off.

Getting Started

Authenticate communications between computers

9. When the **Windows 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 **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply** and then click **OK**.



Specify behavior for when a computer is connected to its corporate domain.

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections:

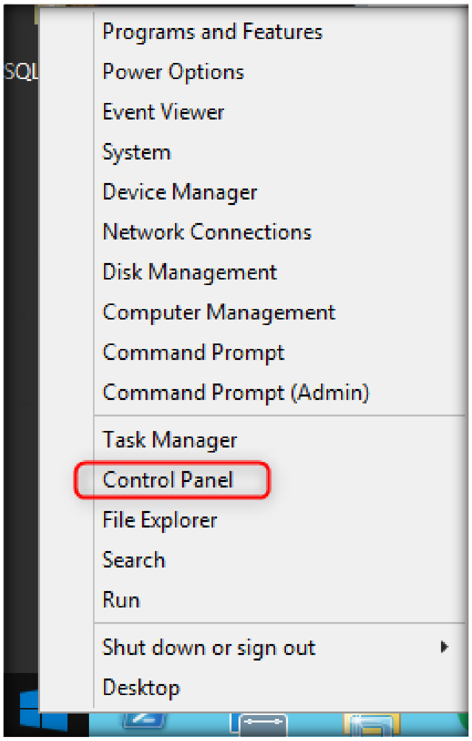
Specify settings that control Windows Firewall behavior.

Specify logging settings for troubleshooting.

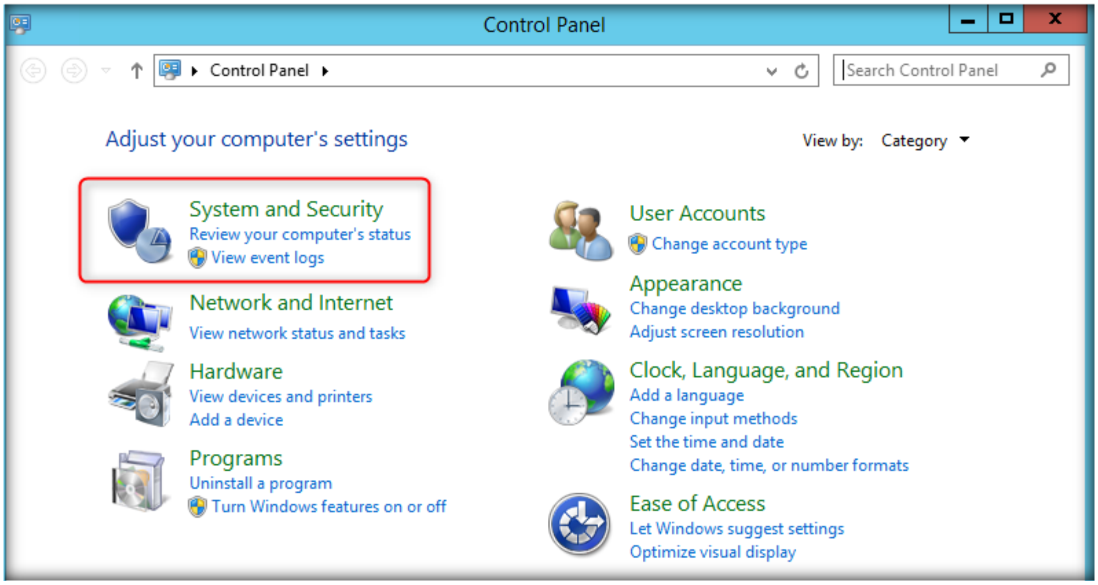
10. Close all the windows.

CT#7.15: Change User Account Settings to disable notification on System Changes

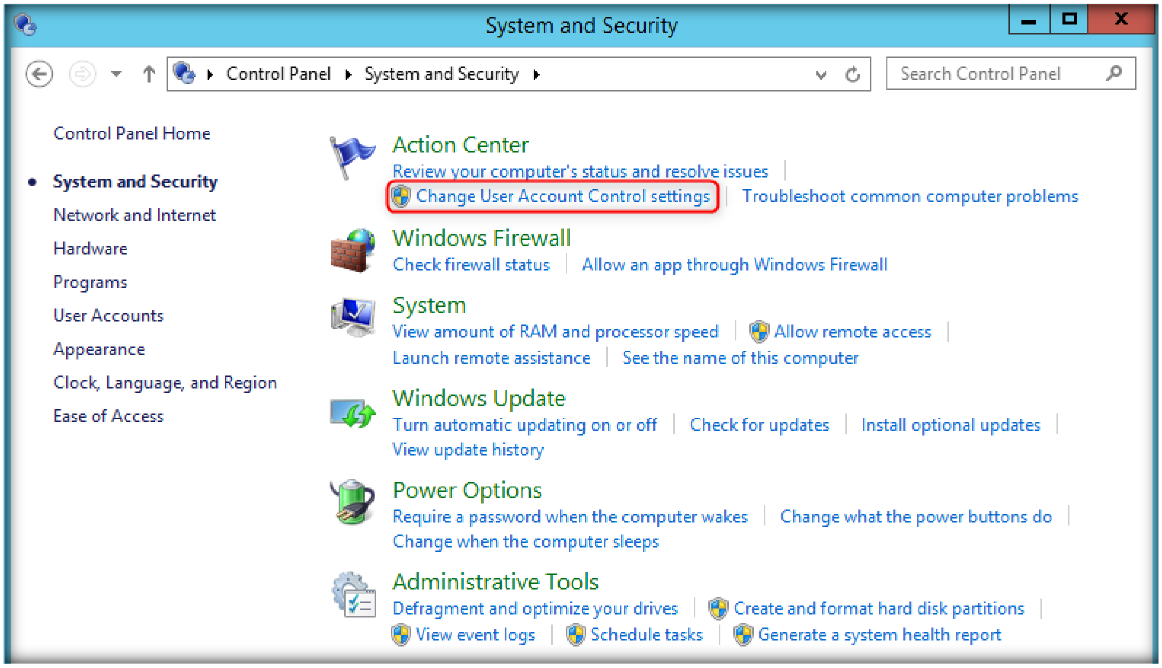
1. Right-click on Windows Start Button and Select **Control Panel**.



2. Control Panel will open click on **System and Security**.



3. Click on **Change User Account Control setting** link.



System and Security

Control Panel ▸ System and Security ▸

Search Control Panel

Control Panel Home

- **System and Security**

Network and Internet

Hardware

Programs

User Accounts

Appearance

Clock, Language, and Region

Ease of Access

Action Center

Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

Windows Firewall

Check firewall status | Allow an app through Windows Firewall

System

View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer

Windows Update

Turn automatic updating on or off | Check for updates | Install optional updates | View update history

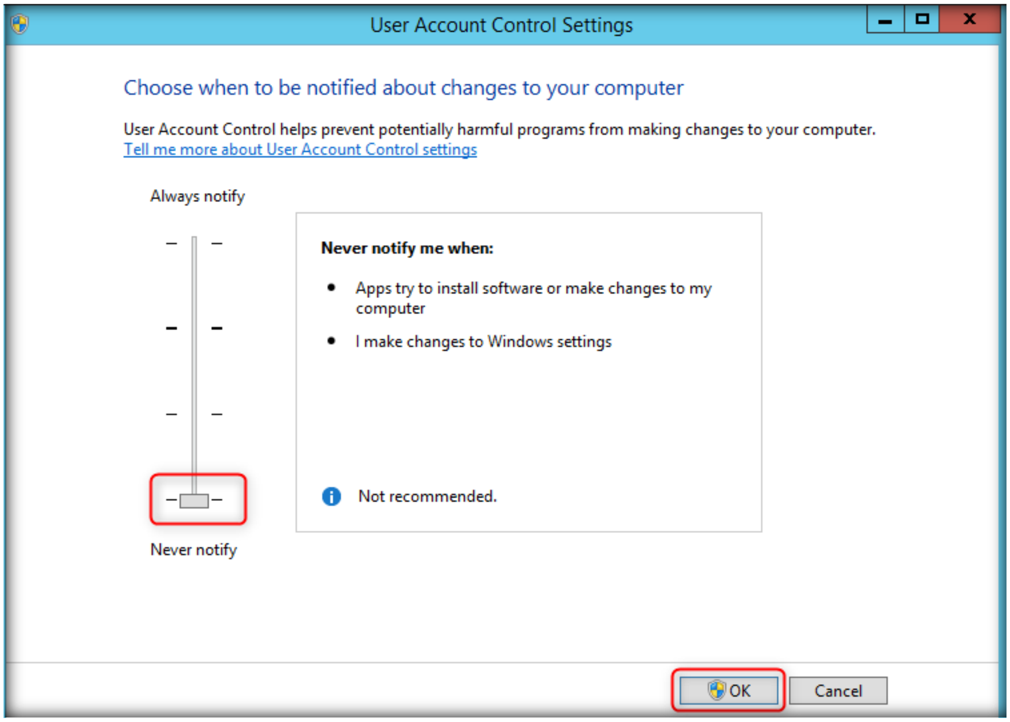
Power Options

Require a password when the computer wakes | Change what the power buttons do | Change when the computer sleeps

Administrative Tools

Defragment and optimize your drives | Create and format hard disk partitions | View event logs | Schedule tasks | Generate a system health report

4. Drag the scroll bar down **Always notify** to **Never notify** and click **OK**.



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Never notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Not recommended.

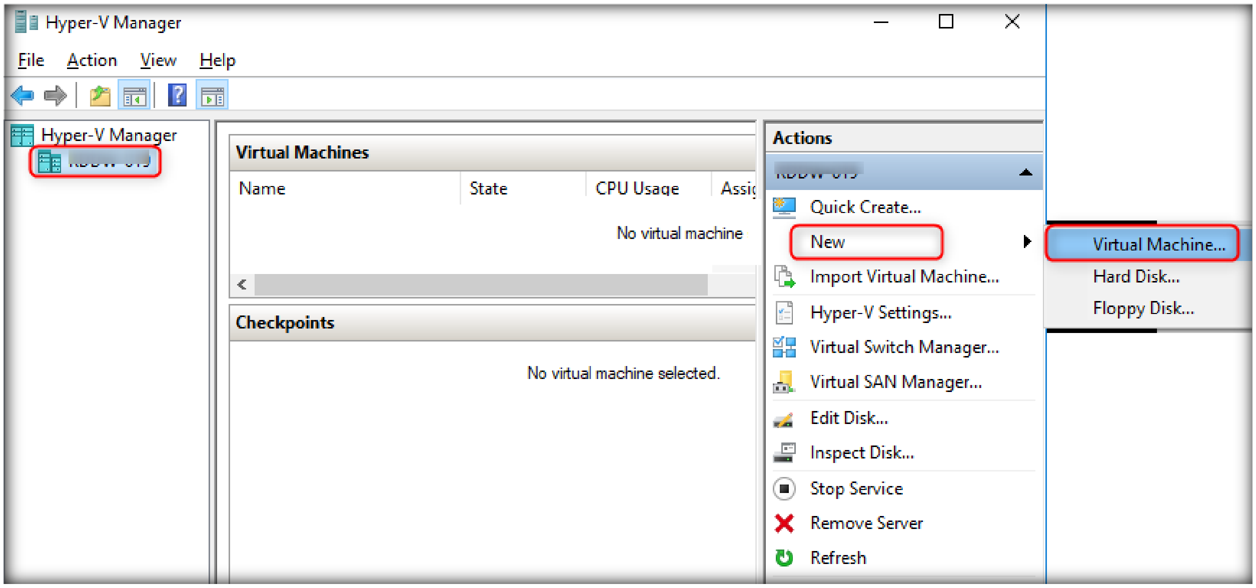
Never notify

OK Cancel

CT#8: Creating and Configuring Windows 10 Virtual Machine

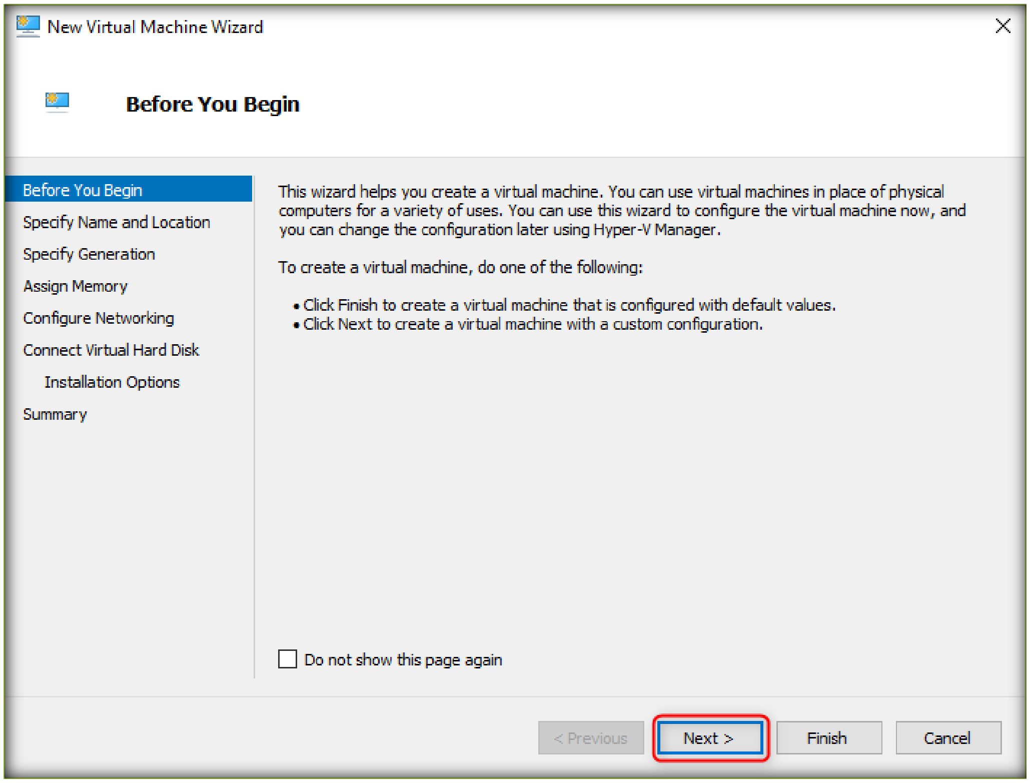
CT#8.1: Creating a Virtual Machine and Installing Windows 10 Guest OS

1. Launch Hyper-V Manager. If already launched, skip to step two.
2. Select your local machine in the left pane, then click **New**, and then click **Virtual Machine…** in the right pane as shown in the screen shot.



Note: Every machine has a unique name, so the name of your machine differs from the name shown in the above screenshot.

3. **New Virtual Machine Wizard** window appears, click **Next** button.



New Virtual Machine Wizard

Before You Begin

This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

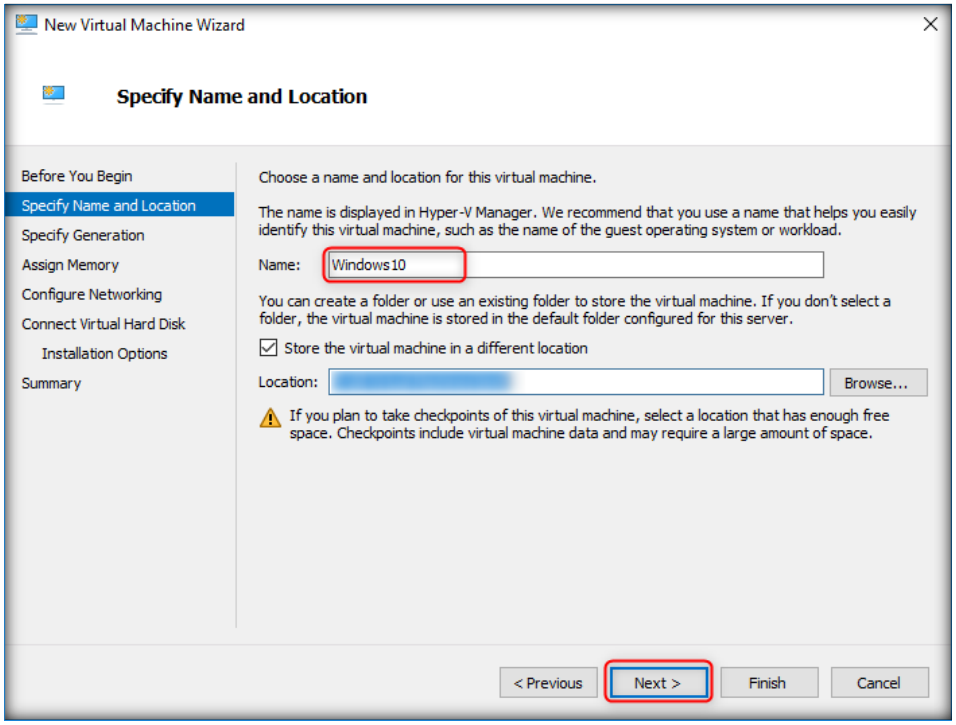
□ Do not show this page again

4. Specify **Name** and **location** of new virtual machine. Assign the name of the virtual machine as **Windows10.**

5. The default location for storing the virtual machine is **C:\ProgramData\Microsoft\Windows\Hyper-V\.** You can choose different location to store the VM's or set it to default location.

6. Click **Next**.

   Note: You can specify the location either in the **Specify Name and Location** section or in the forthcoming **Connect Virtual Hard Disk** section.



New Virtual Machine Wizard

Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Windows10

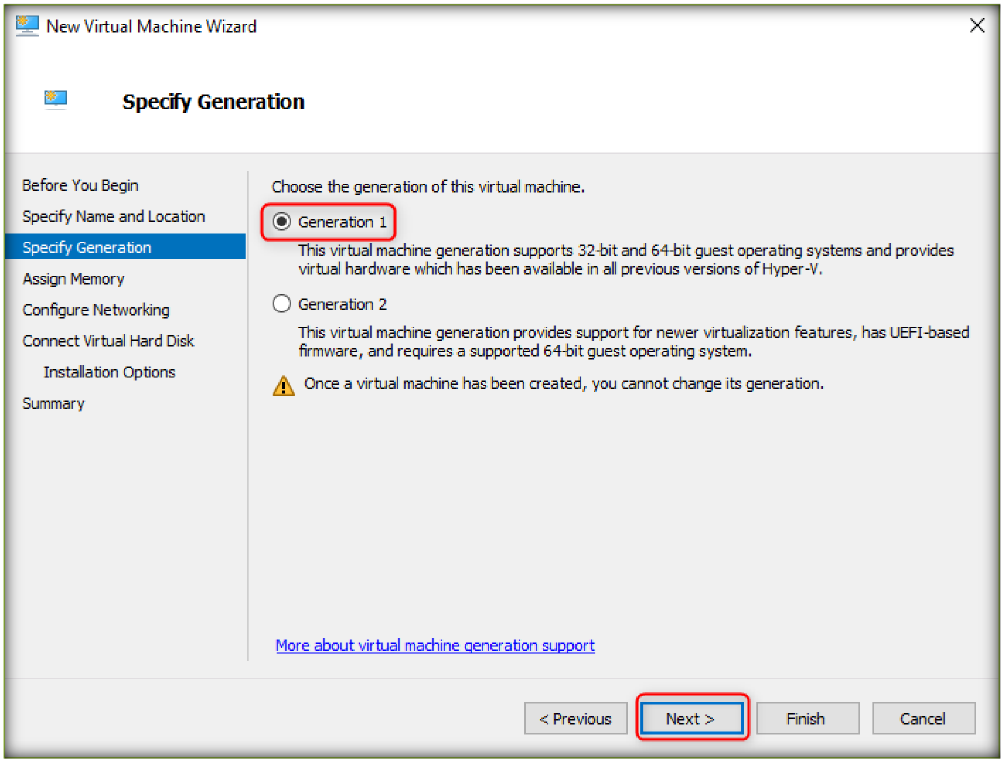
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

Location: [redacted]

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

7. Choose the generation of the virtual machine (here, **Generation** 1) and click **Next**.



New Virtual Machine Wizard

Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

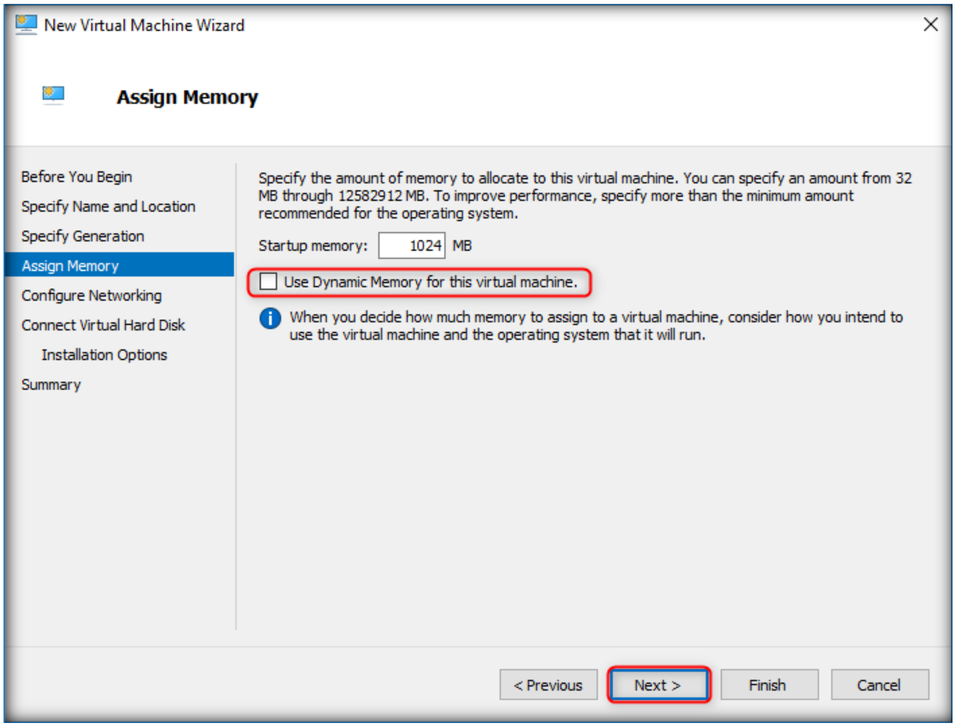
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

Once a virtual machine has been created, you cannot change its generation.

8. Assign the amount of Startup memory to allocate to this virtual machine in MB (here, 3072) and uncheck Use Dynamic memory for the virtual machine.

9. Click **Next**.



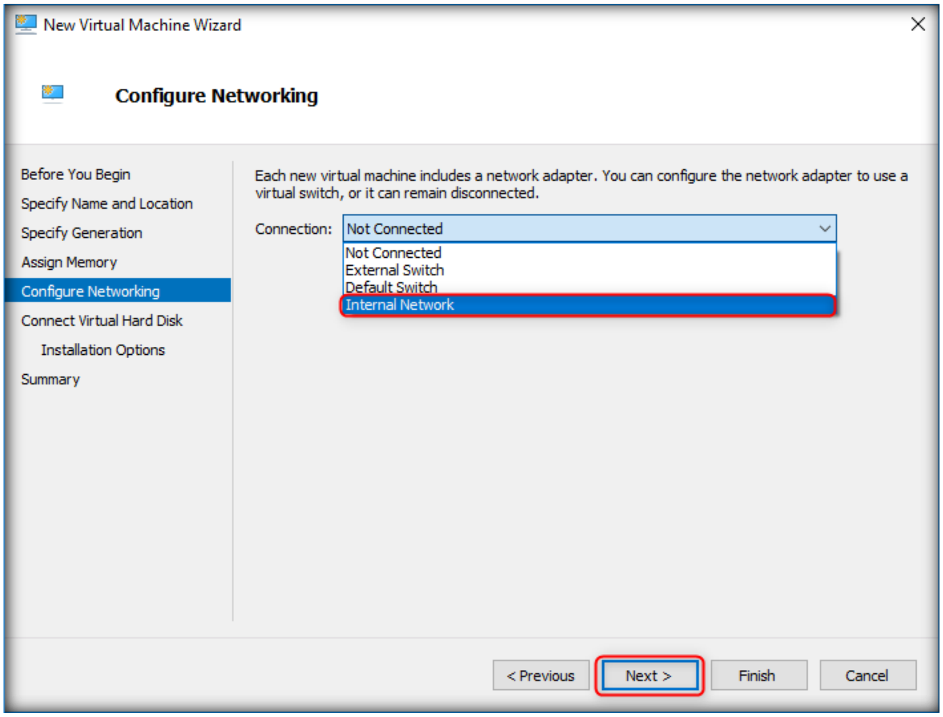
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 1024 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

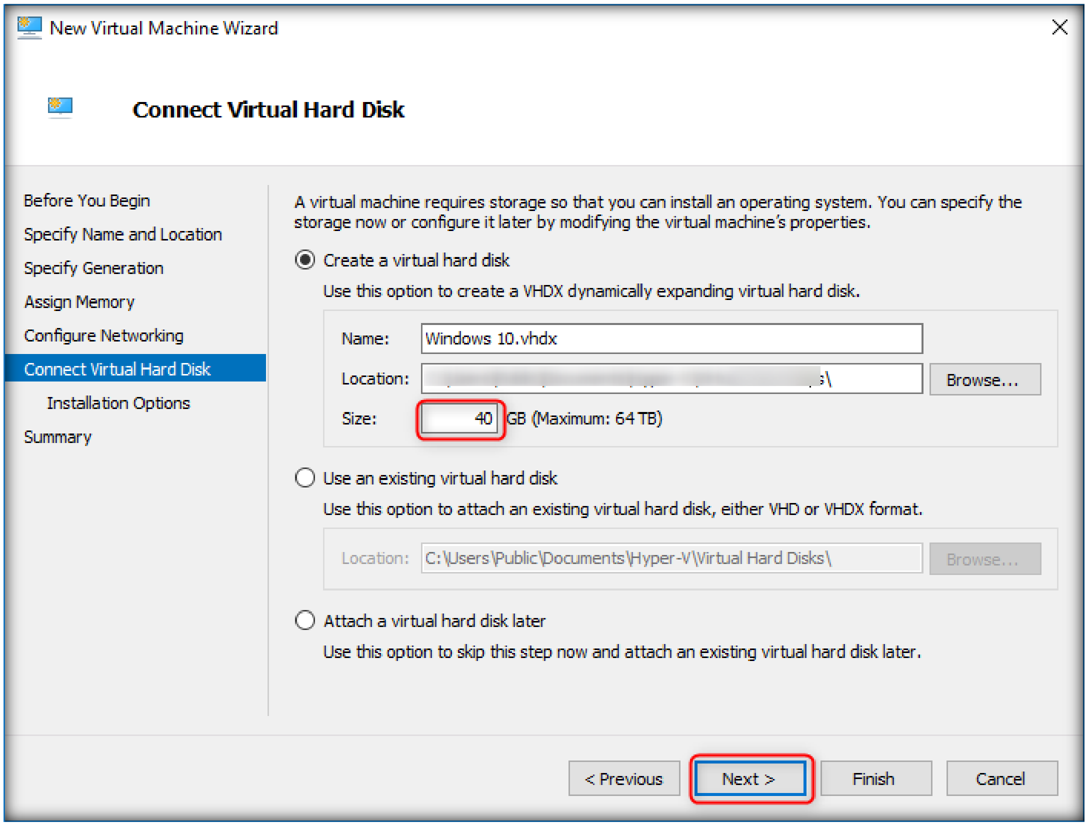
10. In the Configure Networking step, select **Internal Network** from Connection drop-down list and click **Next**.



Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

11. Connect Virtual Hard Disk section appears, allocate **40 GB** default space for hard disk and click **Next**.



Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: Windows 10.vhdx

Location: [redacted]s\

Size: 40 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

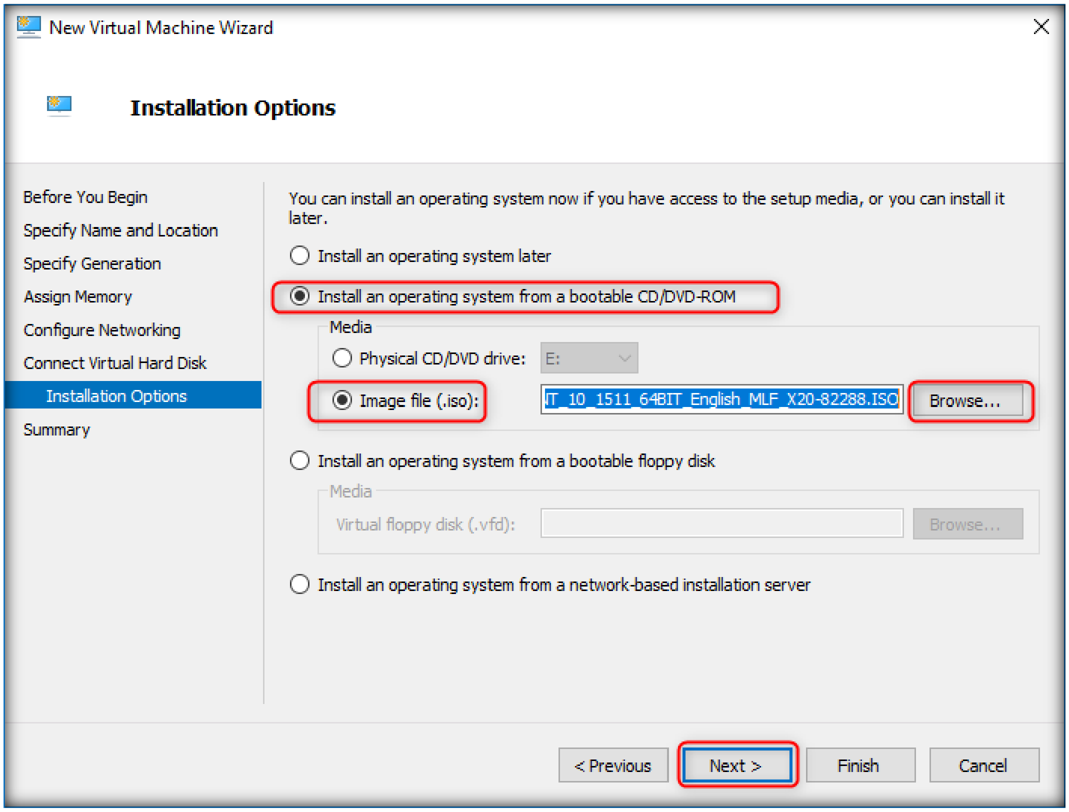
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

12. The **installation options** section appears, select **Install an operating system from a bootable CD/DVD-ROM** radio button.
    - If you have a Windows 10 DVD choose Physical CD/DVD drive radio button and then click **Next**.
    - If you have a Windows 10 file, then choose Image file (.iso) radio button and click browse button to provide the path of ISO file and click **Next**.



New Virtual Machine Wizard

Installation Options

You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a bootable CD/DVD-ROM

Media

○ Physical CD/DVD drive: E:

● Image file (.iso): T_10_1511_64BIT_English_MLF_X20-82288.ISO

○ Install an operating system from a bootable floppy disk

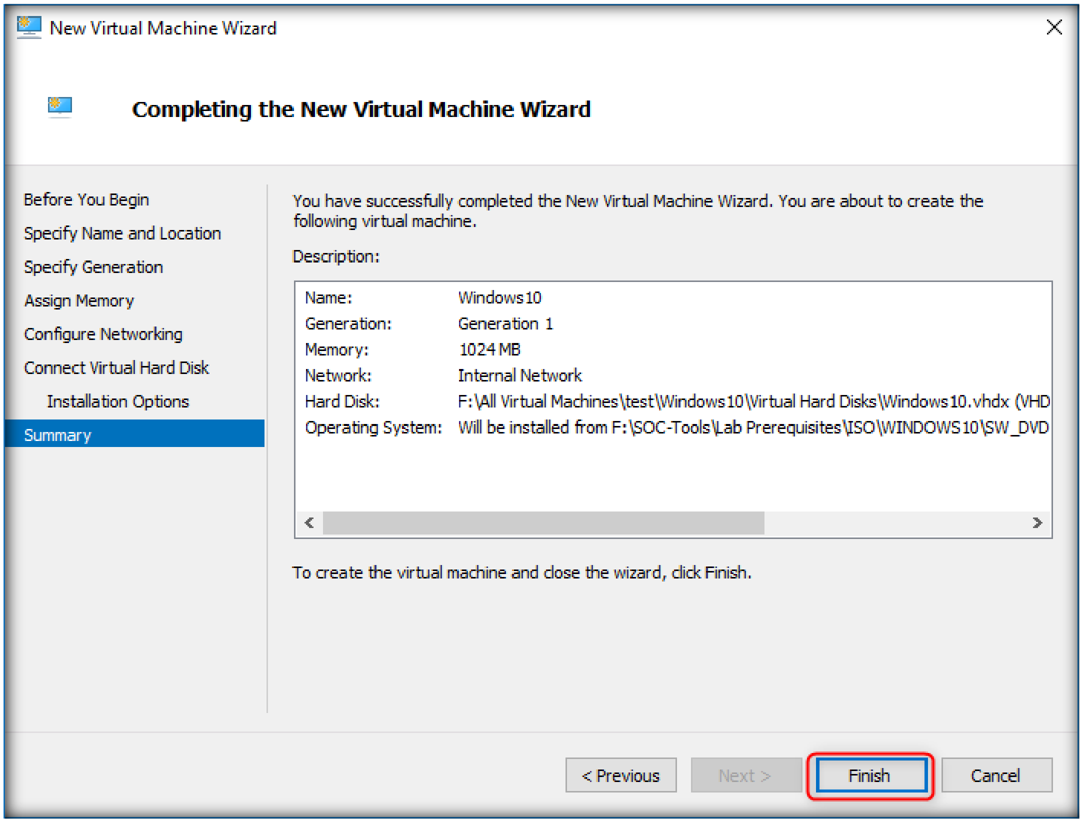
Media

Virtual floppy disk (.vfd):

○ Install an operating system from a network-based installation server

13. Virtual machine wizard appears with summary information.

14. Click **Finish**.



Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

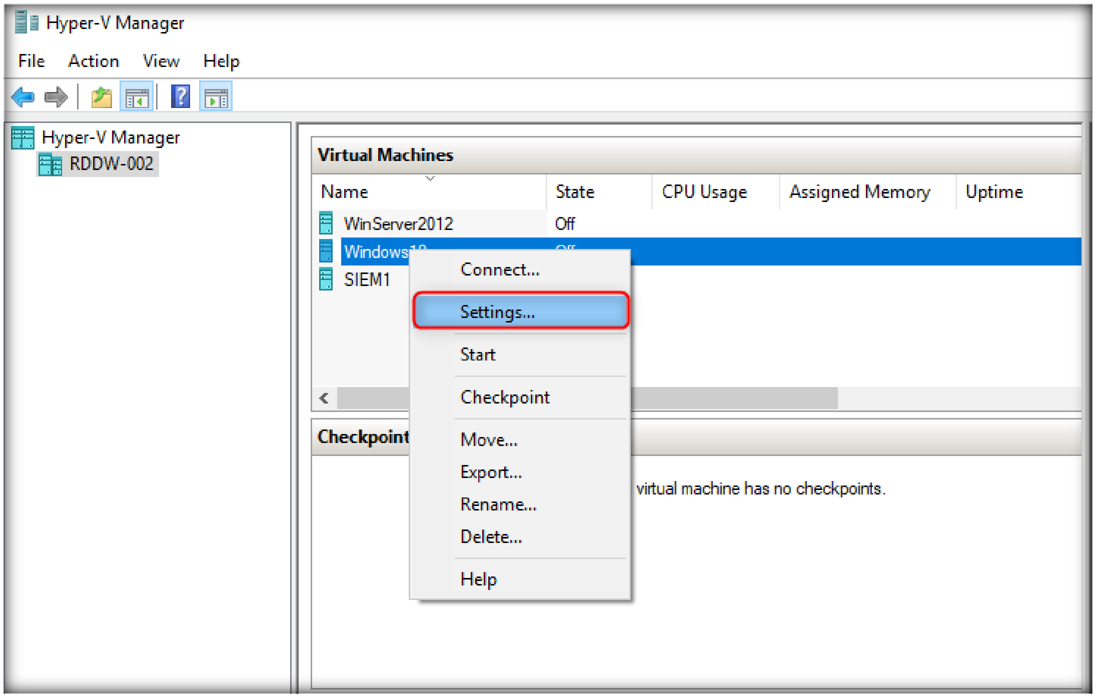
Description:

Name:	Windows10
Generation:	Generation 1
Memory:	1024 MB
Network:	Internal Network
Hard Disk:	F:\All Virtual Machines\test\Windows10\Virtual Hard Disks\Windows10.vhdx (VHD
Operating System:	Will be installed from F:\SOC-Tools\Lab Prerequisites\ISO\WINDOWS10\SW_DVD

To create the virtual machine and close the wizard, click Finish.

15. Hyper-V Manager creates **Windows10** virtual machine profile.

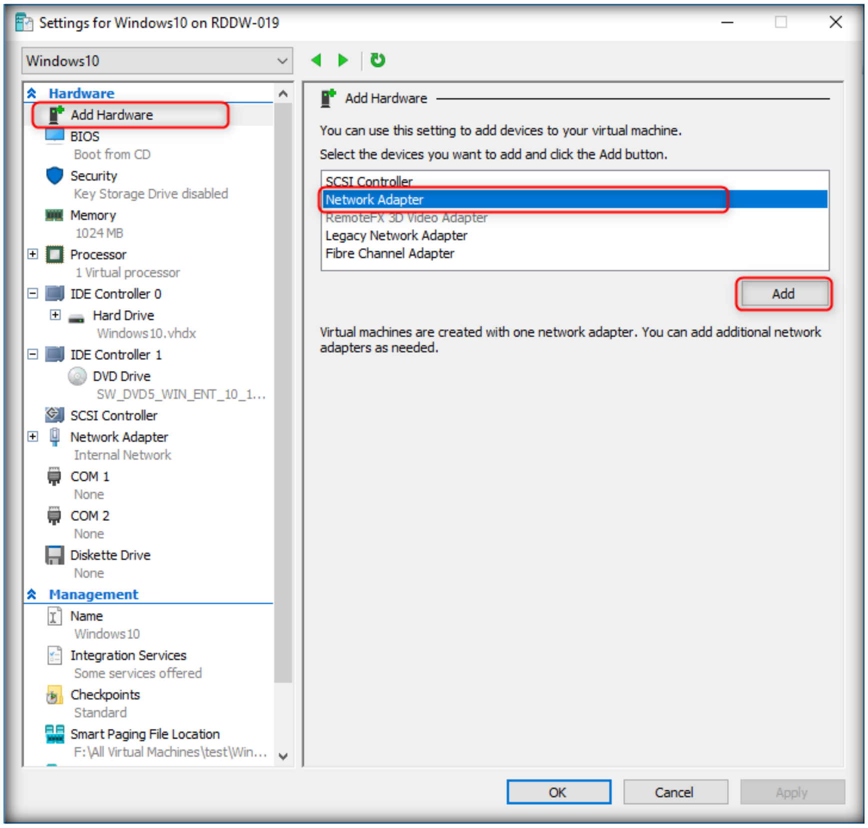
16. In **Hyper-V Manager** main window, you see a new virtual machine named **Windows10**. Right-click on the newly created virtual machine and click **Settings** from the context menu.



Name	State	CPU Usage	Assigned Memory	Uptime
WinServer2012	Off			
Windows10	Off			
SIEM1				

virtual machine has no checkpoints.

17. Setting for **Windows10** window will open click on **Add Hardware** and select **Network Adapter** click **Add** button finally click **OK** button.



BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
1024 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
Windows10.vhdx
IDE Controller 1
DVD Drive
SW_DVD5_WIN_ENT_10_1...
SCSI Controller
Network Adapter
Internal Network
COM 1
None
COM 2
None
Diskette Drive
None

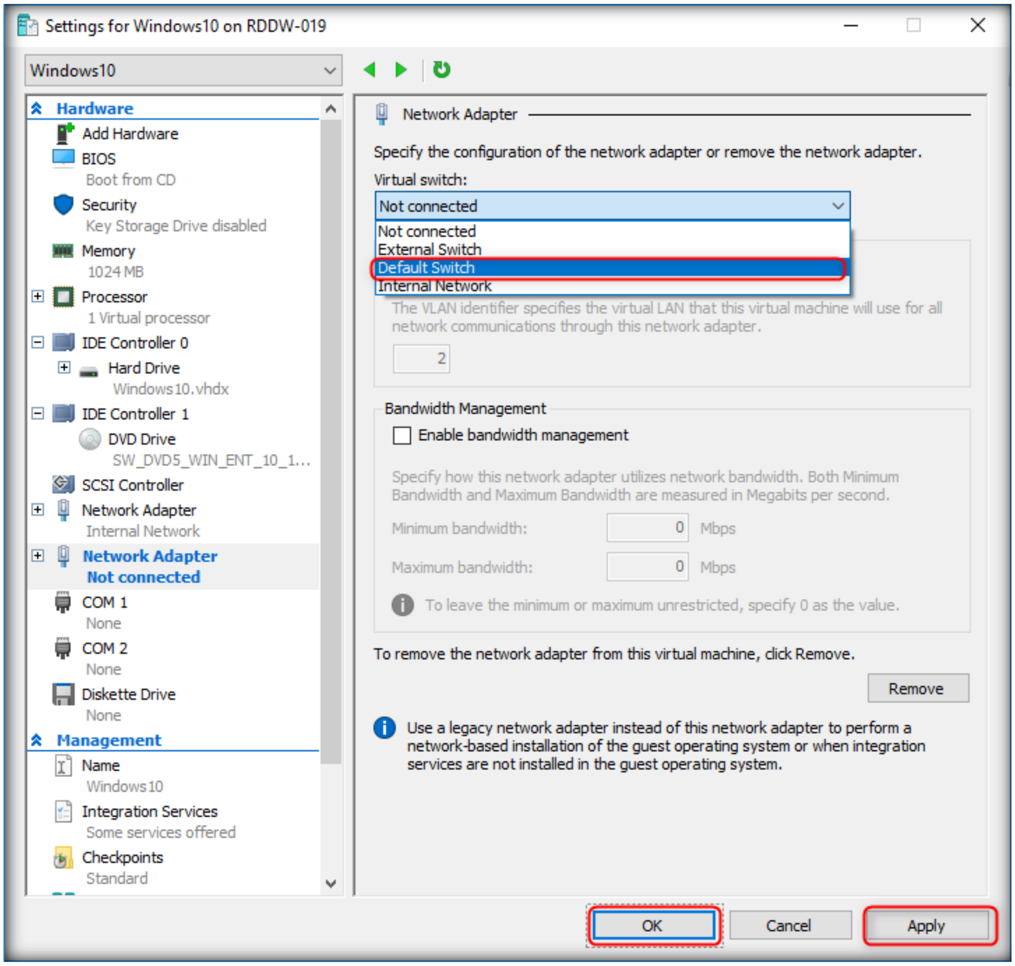
Name
Windows10
Integration Services
Some services offered
Checkpoints
Standard
Smart Paging File Location
F:\All Virtual Machines\test\Win...

You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

Virtual machines are created with one network adapter. You can add additional network adapters as needed.

18. You will see **Network Adaptor** added in setting list, select virtual switch as **Default Switch** click **Apply** and click **OK**.



Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Not connected

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

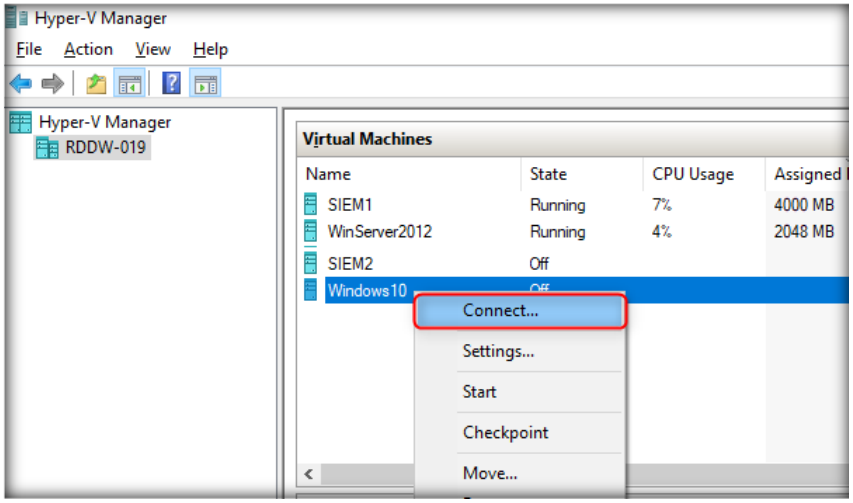
Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

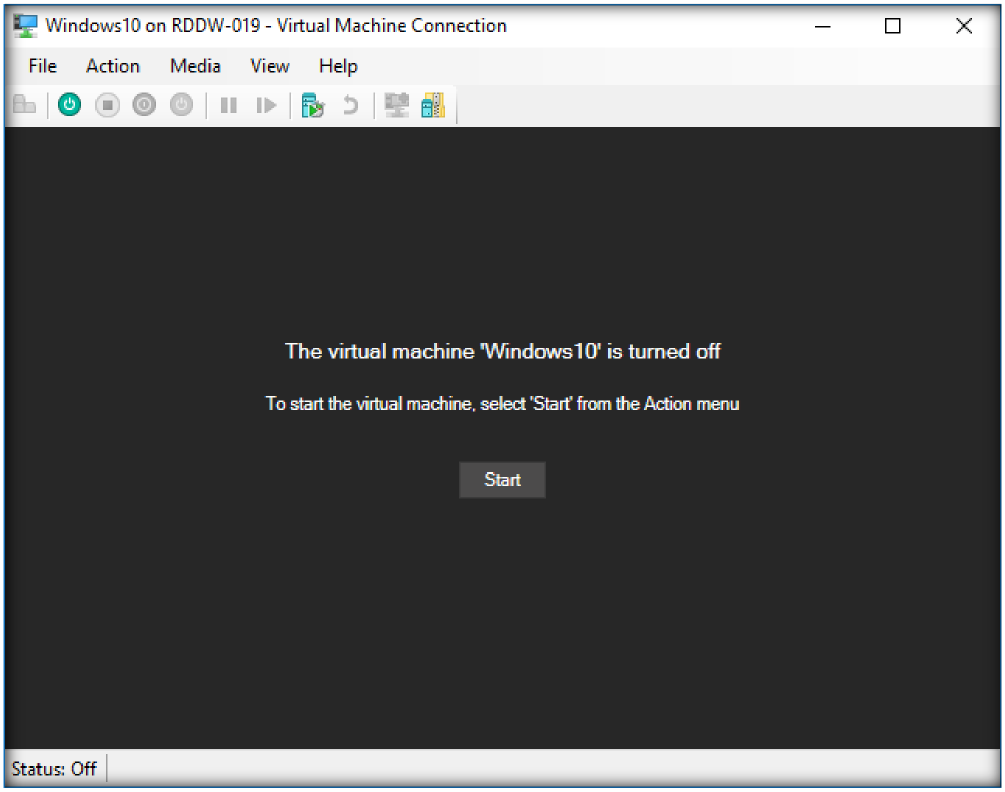
Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

19. In **Hyper-V Manager** main window, you see a new virtual machine named **Windows10**. Right-click on the newly created virtual machine and click **Connect** from the context menu.



Name	State	CPU Usage	Assigned
SIEM1	Running	7%	4000 MB
WinServer2012	Running	4%	2048 MB
SIEM2	Off		
Windows10	Off		

20. **Windows10** Virtual Machine window appears click **Start** button as shown in the screenshot.



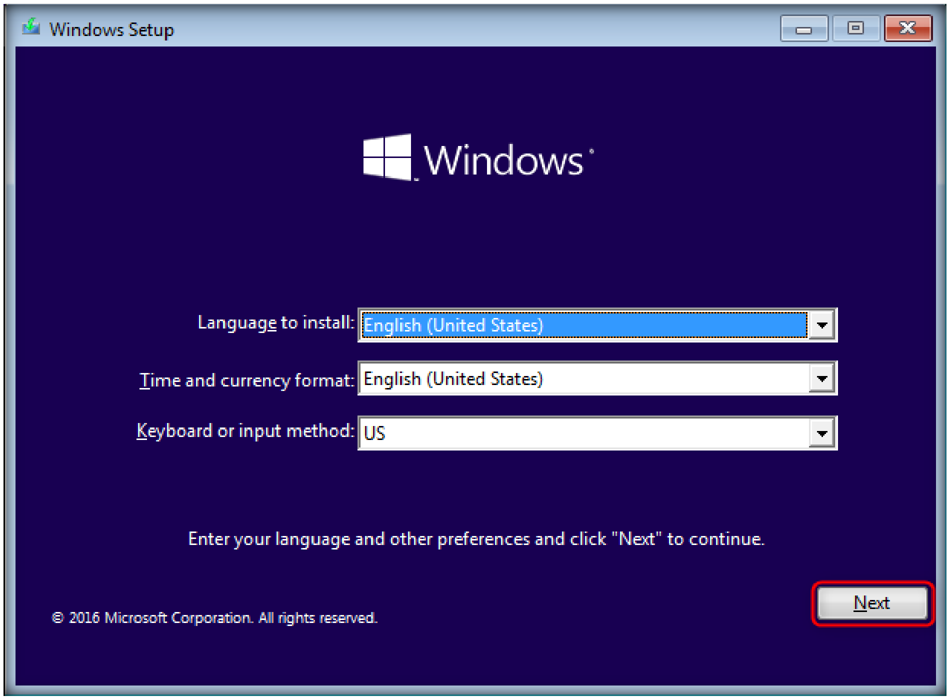
Windows10 on RDDW-019 - Virtual Machine Connection

The virtual machine 'Windows10' is turned off

To start the virtual machine, select 'Start' from the Action menu

Status: Off

21. Windows Setup screen appears, in Windows Setup screens choose the **Language** and other preferences then click **Next**.



Language to install: English (United States)

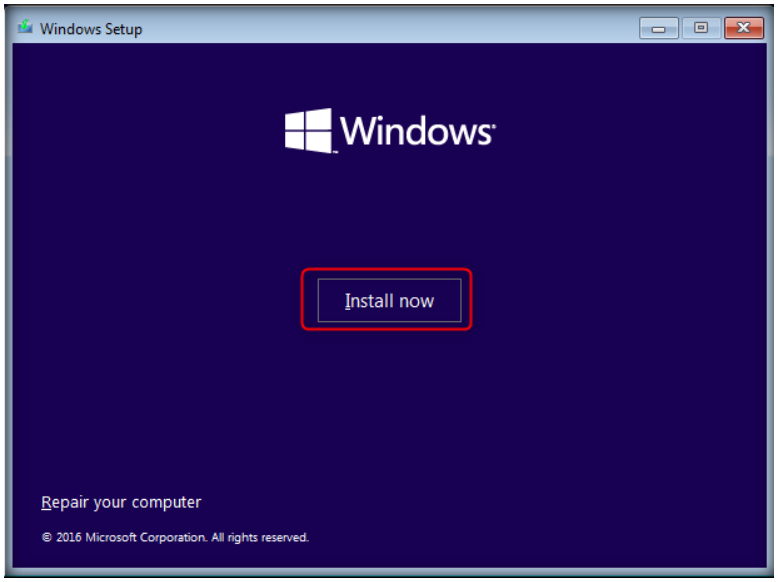
Time and currency format: English (United States)

Keyboard or input method: US

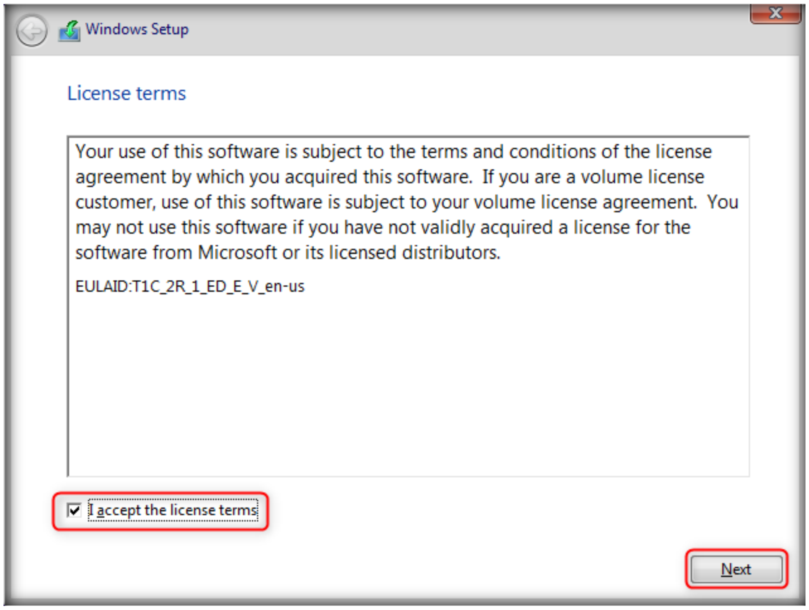
Enter your language and other preferences and click "Next" to continue.

© 2016 Microsoft Corporation. All rights reserved.

22. Click **Install now** button to start the installation process of Windows 10.



23. License terms wizard appears, check **I accept the license terms** check and box and click **Next**.



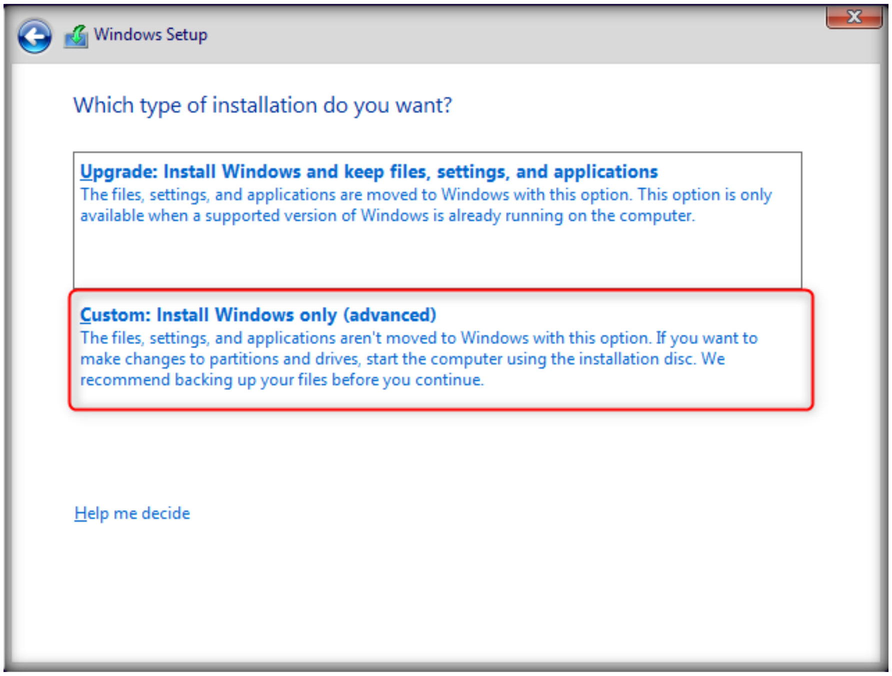
License terms

Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. If you are a volume license customer, use of this software is subject to your volume license agreement. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.

EULAID:T1C_2R_1_ED_E_V_en-us

☑ I accept the license terms

24. Click **Custom: Install Windows only (advanced)** option to proceed with the installation.

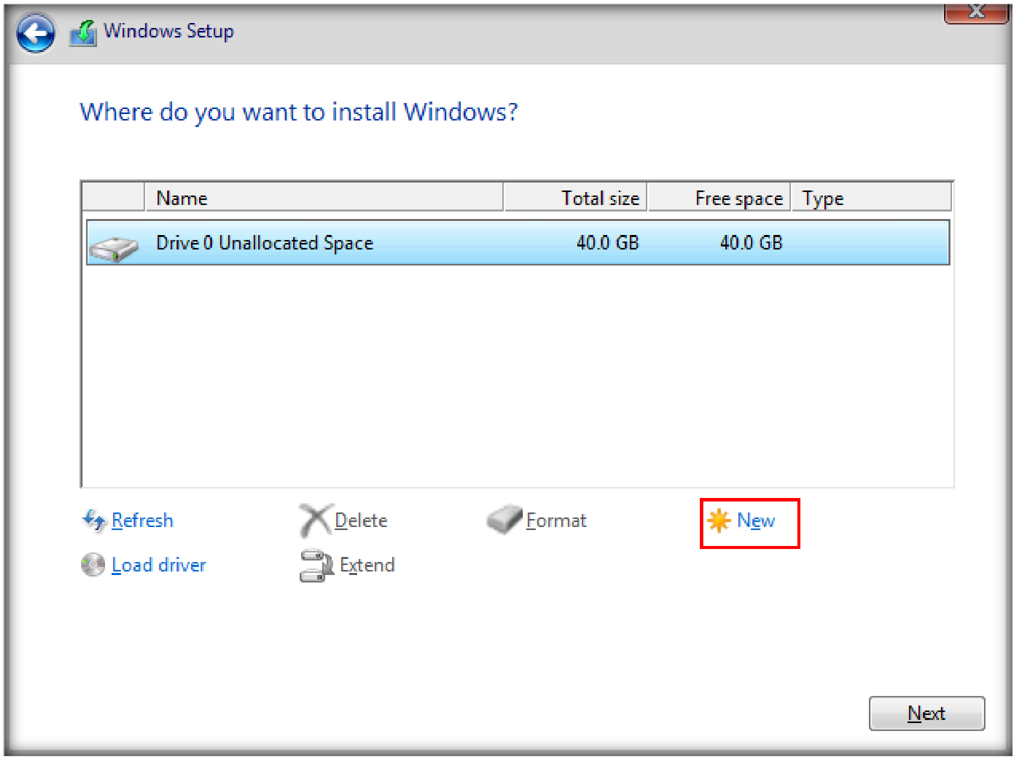


Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

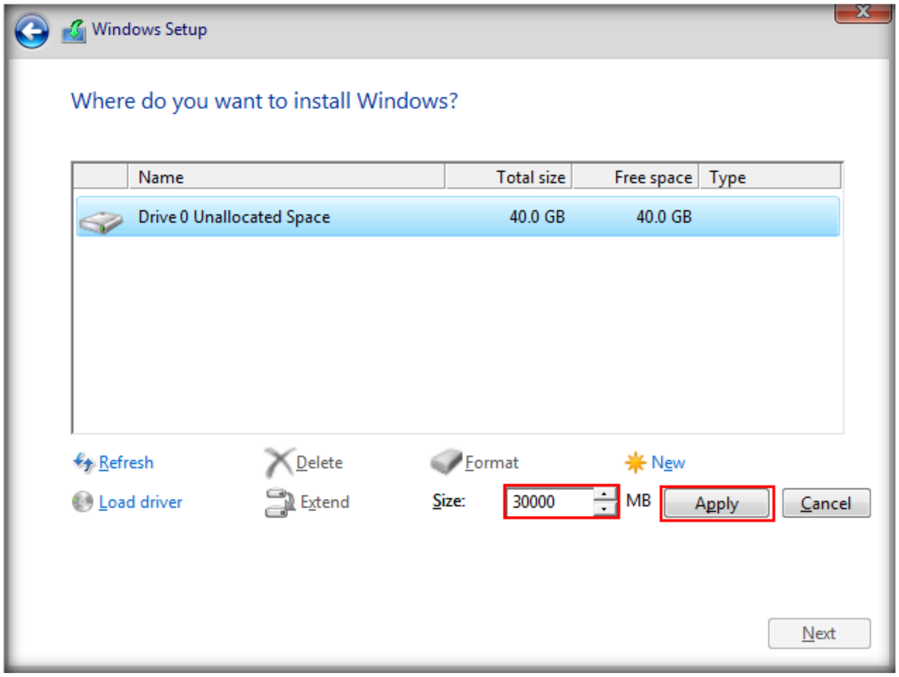
25. Where do you want to install Windows? wizard appears, click **New** to create a partition.



Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	40.0 GB	40.0 GB	

26. Provide **30000 MB** in the Size field and click **Apply**.



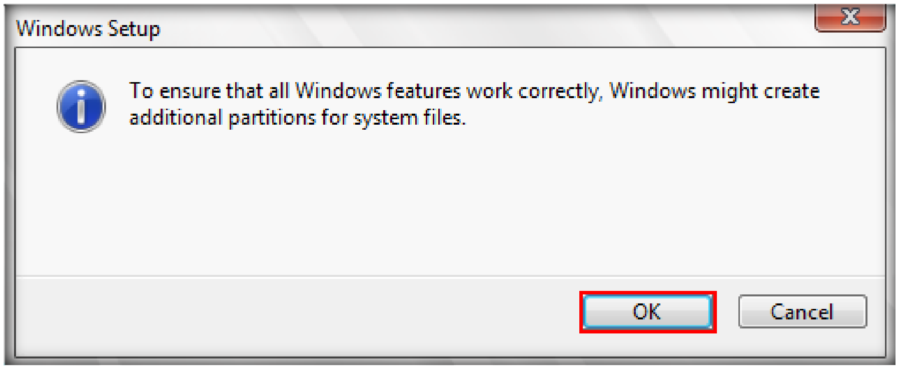
Windows Setup

Where do you want to install Windows?

	Name	Total size	Free space	Type
	Drive 0 Unallocated Space	40.0 GB	40.0 GB	

Size: 30000 MB

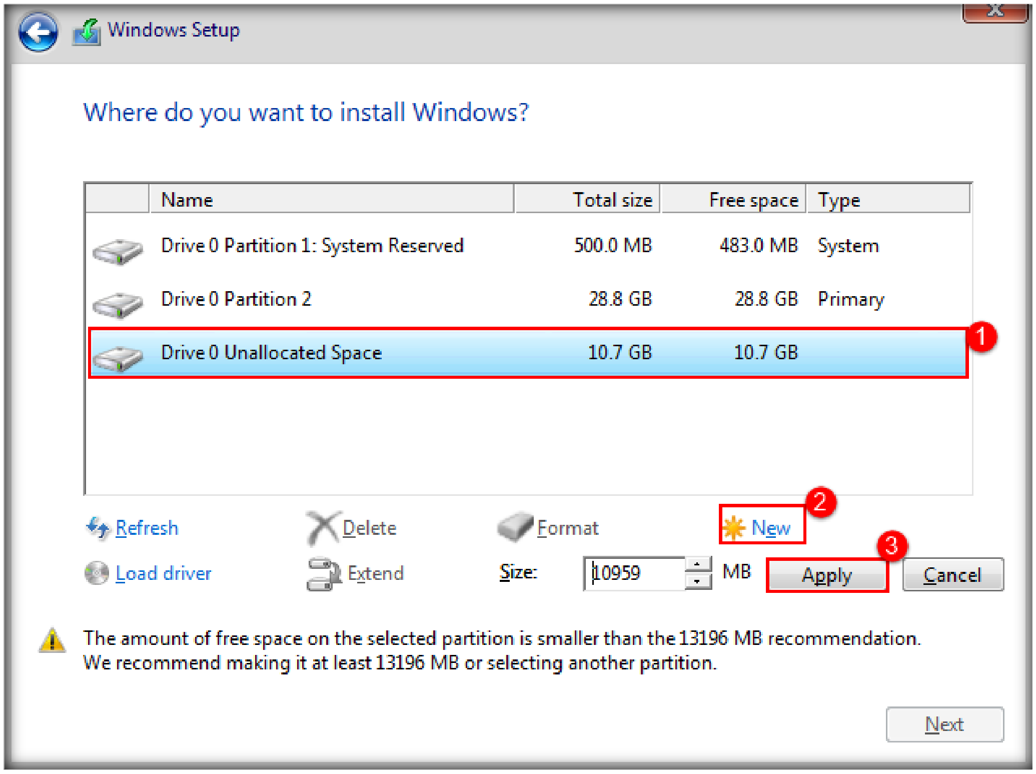
27. Windows Setup pop-up appears, click **OK**.



Windows Setup

To ensure that all Windows features work correctly, Windows might create additional partitions for system files.

28. Click Unallocated Space partition, then click on **New**, and then leave the size to default and then click **Apply**.



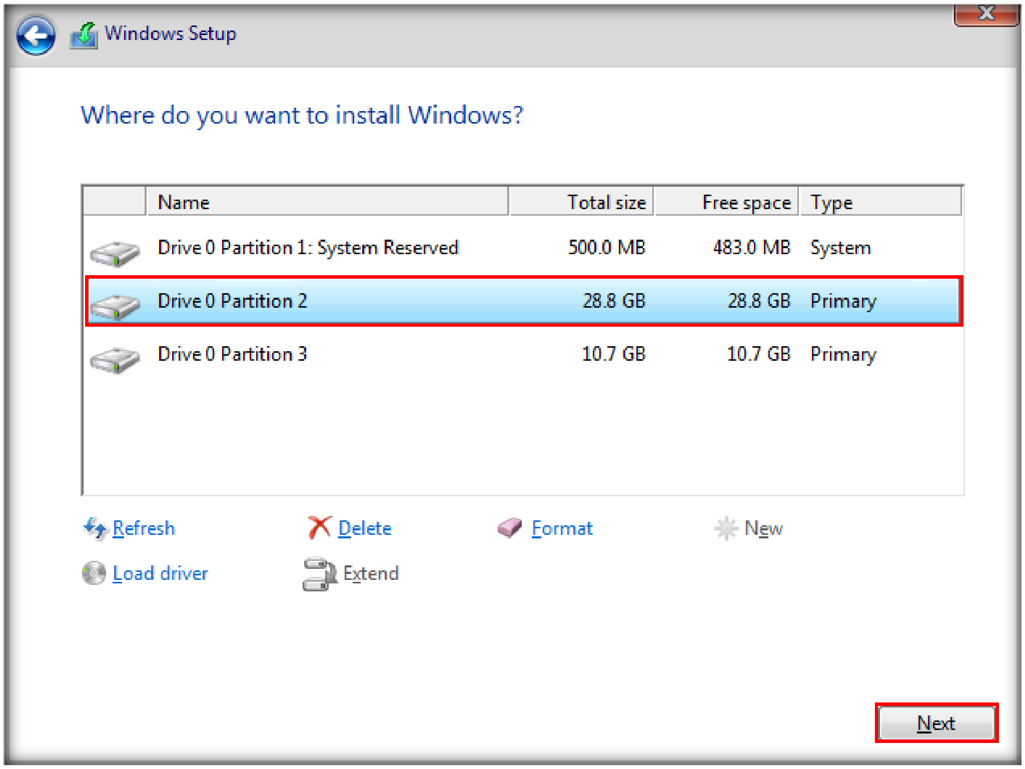
Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Partition 1: System Reserved	500.0 MB	483.0 MB	System
Drive 0 Partition 2	28.8 GB	28.8 GB	Primary
Drive 0 Unallocated Space	10.7 GB	10.7 GB	

Size: 10959 MB

⚠ The amount of free space on the selected partition is smaller than the 13196 MB recommendation. We recommend making it at least 13196 MB or selecting another partition.

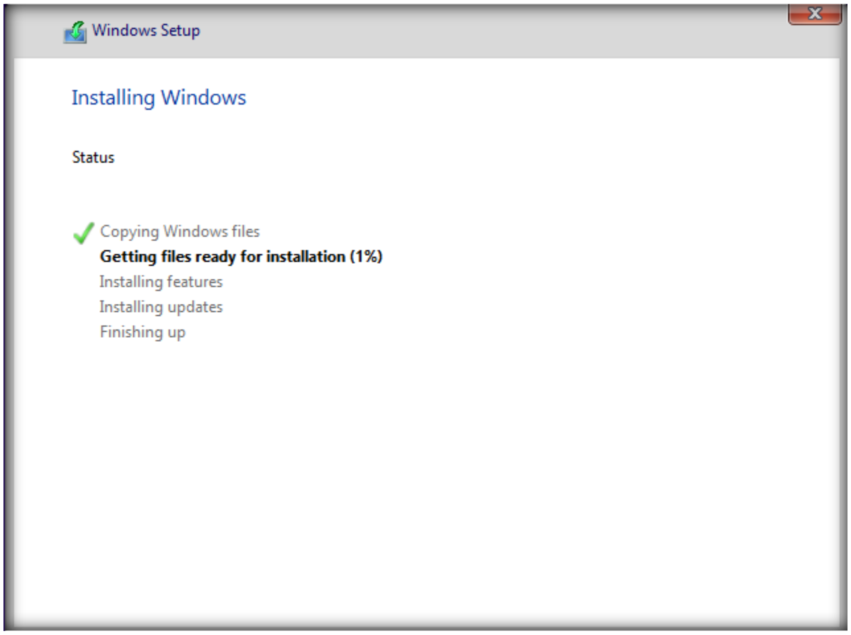
29. After partitions are created, choose the partition to install Windows 10, and click **Next**.



Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Partition 1: System Reserved	500.0 MB	483.0 MB	System
Drive 0 Partition 2	28.8 GB	28.8 GB	Primary
Drive 0 Partition 3	10.7 GB	10.7 GB	Primary

30. Installing Windows screen appears; wait until it completes the installation.



Windows Setup

Installing Windows

Status

✓ Copying Windows files

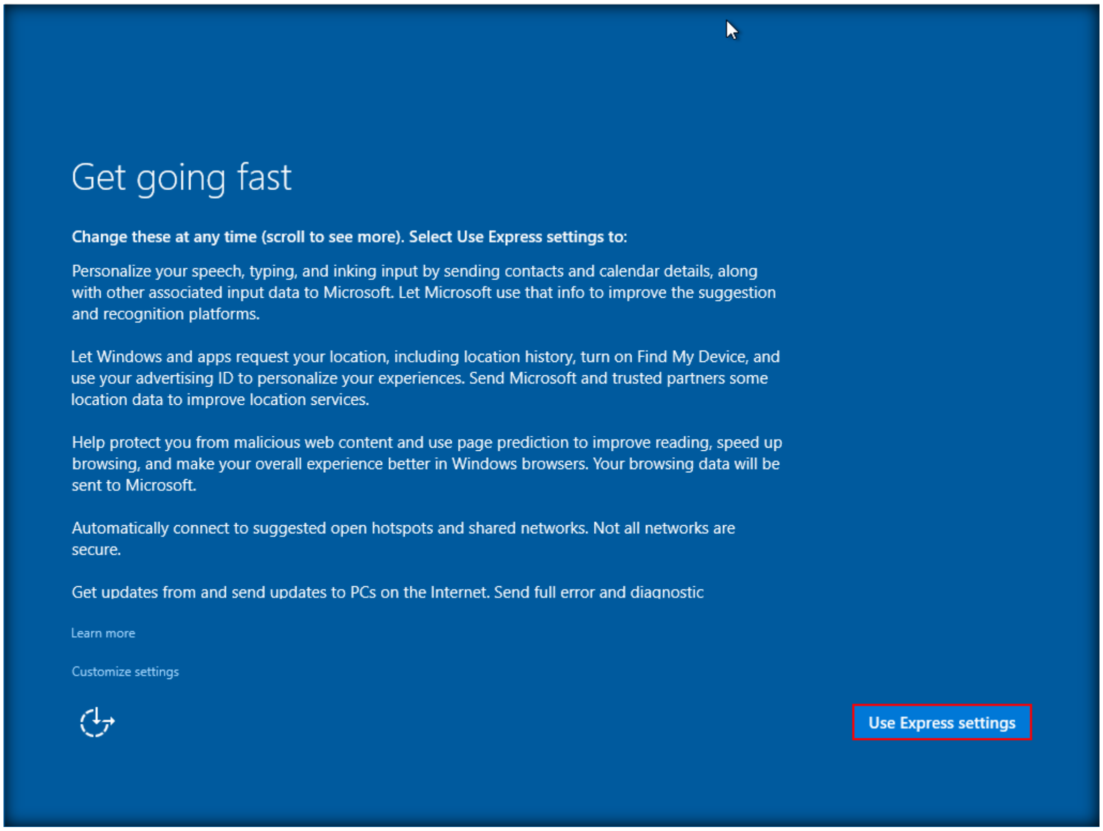
Getting files ready for installation (1%)

Installing features

Installing updates

Finishing up

31. Once the installation is completed machine will restart, and you will see the Get going fast screen. Click **Use Express settings** button.



Get going fast

Change these at any time (scroll to see more). Select Use Express settings to:

Personalize your speech, typing, and inking input by sending contacts and calendar details, along with other associated input data to Microsoft. Let Microsoft use that info to improve the suggestion and recognition platforms.

Let Windows and apps request your location, including location history, turn on Find My Device, and use your advertising ID to personalize your experiences. Send Microsoft and trusted partners some location data to improve location services.

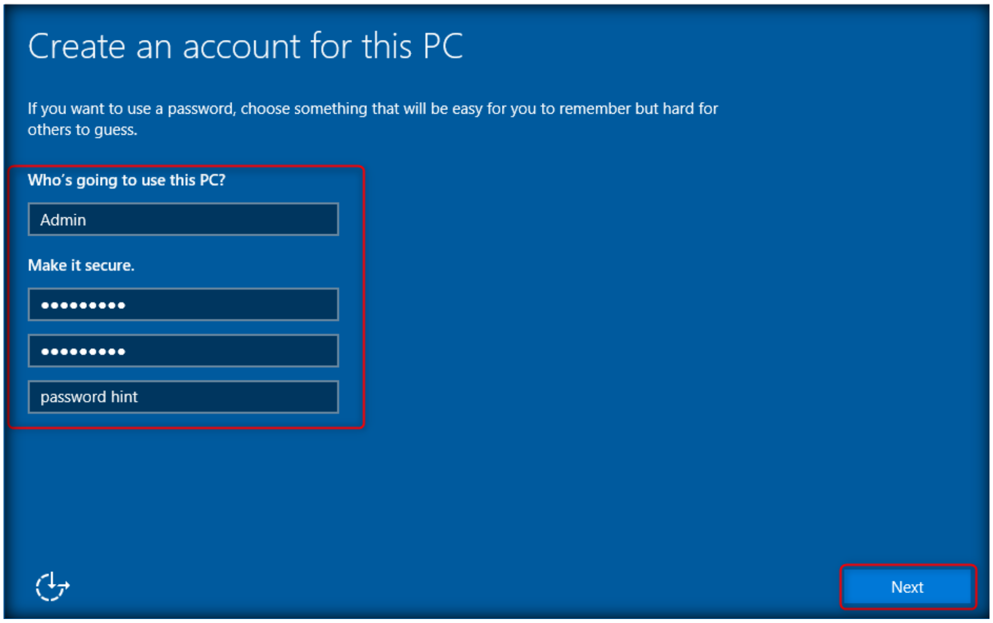
Help protect you from malicious web content and use page prediction to improve reading, speed up browsing, and make your overall experience better in Windows browsers. Your browsing data will be sent to Microsoft.

Automatically connect to suggested open hotspots and shared networks. Not all networks are secure.

Get updates from and send updates to PCs on the Internet. Send full error and diagnostic

32. Create an account for this PC screen appears, fill the following details:
    - Username: **Admin**
    - Password: **admin@123**

    Hint field need to be filled mandatory, you can fill with the desired hint, and click **Next**.



Create an account for this PC

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?

Admin

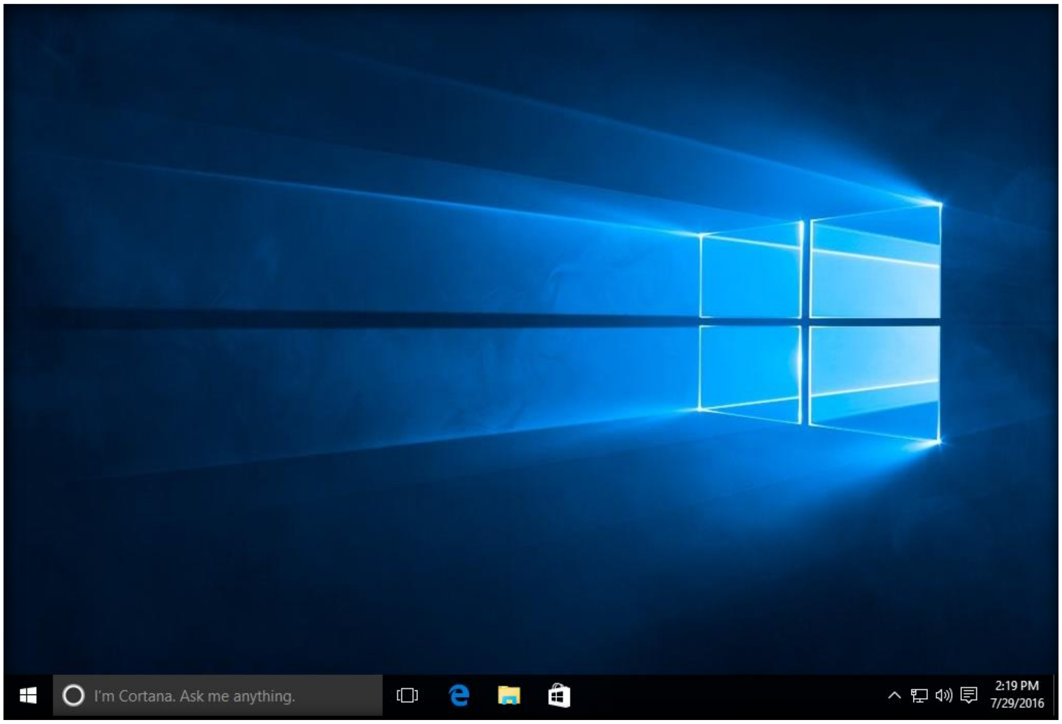
Make it secure.

••••••••••

••••••••••

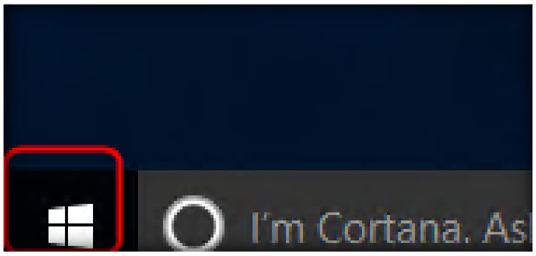
password hint

33. Windows 10 machine is ready as shown in the screenshot.

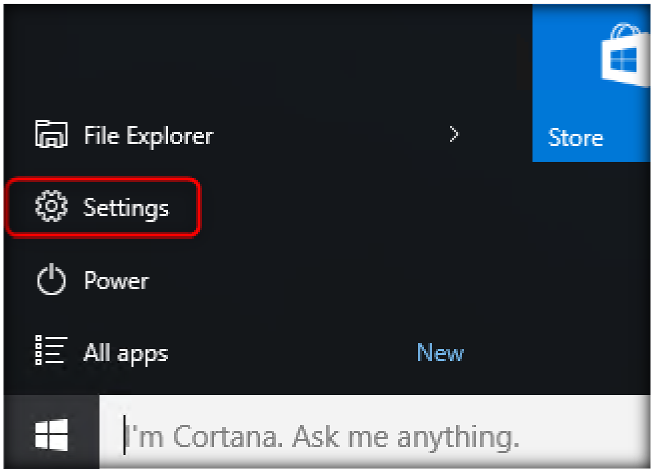


CT#8.2: Creating New User Account in Windows 10 Virtual Machine

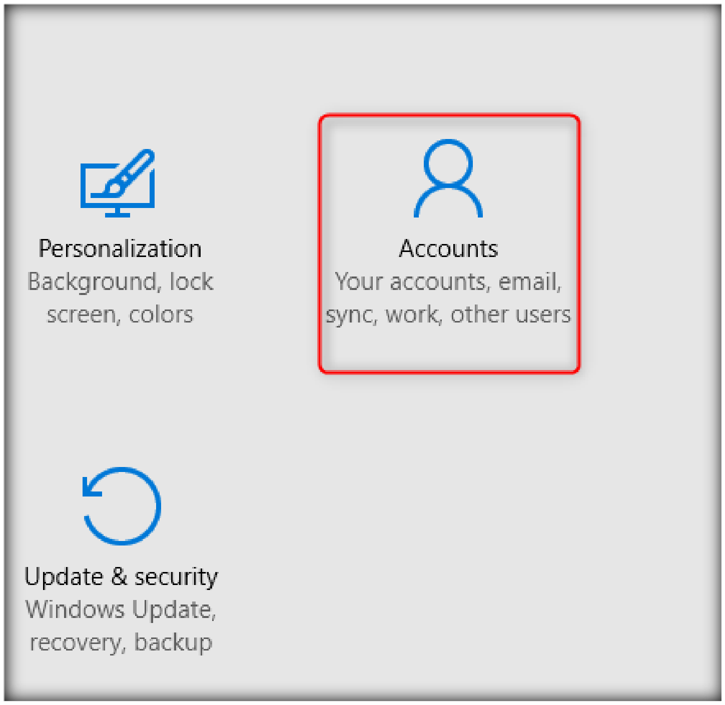
1. Click windows **Start** button Icon.



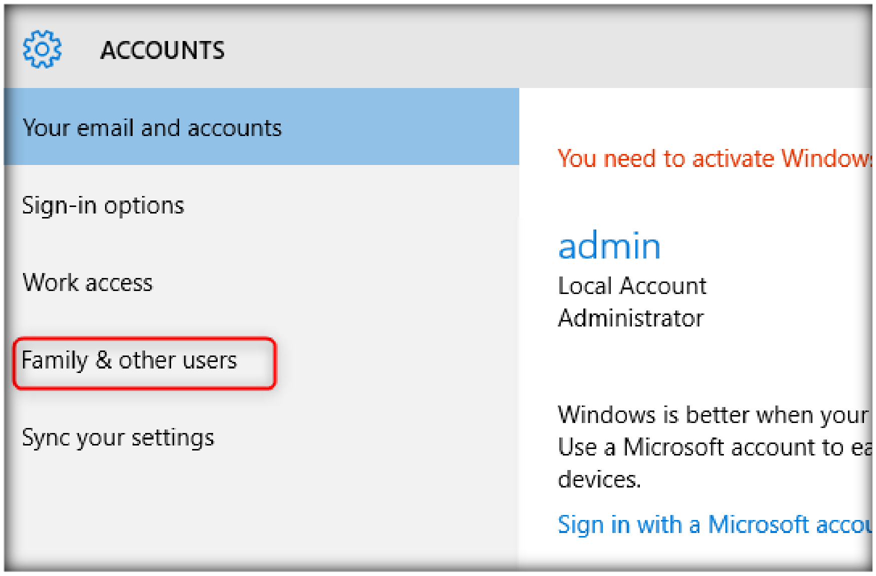
2. Click **Settings**.



3. Click on **Accounts**.


Personalization
Background, lock screen, colors
Accounts
Your accounts, email, sync, work, other users
Update & security
Windows Update, recovery, backup

4. Select option **Family & Other users**.

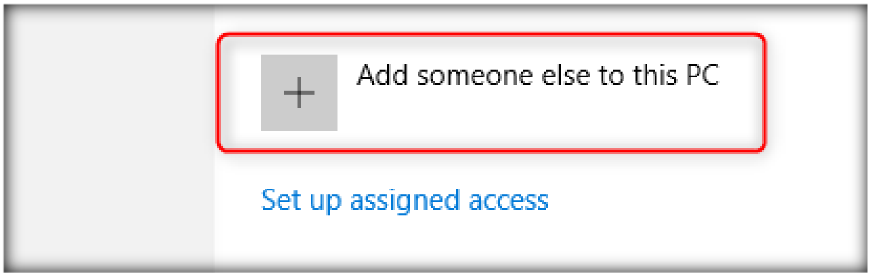


You need to activate Window

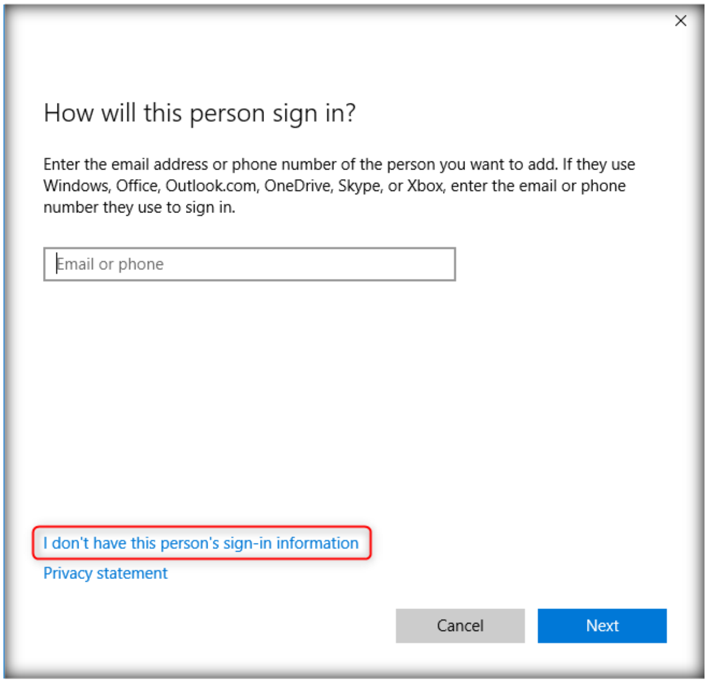
admin
Local Account
Administrator

Windows is better when your
Use a Microsoft account to ea
devices.

5. Click **Add someone else to this PC** button.

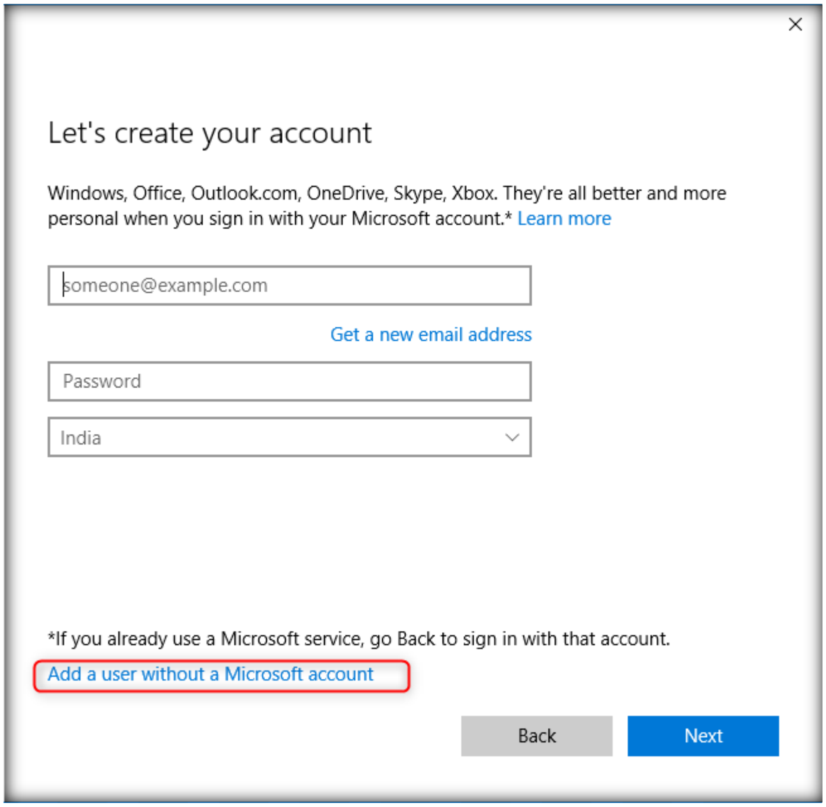


6. Click **I don't have this person's sign-in information** link.


How will this person sign in?

Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

7. Click **Add a user without Microsoft account** link.

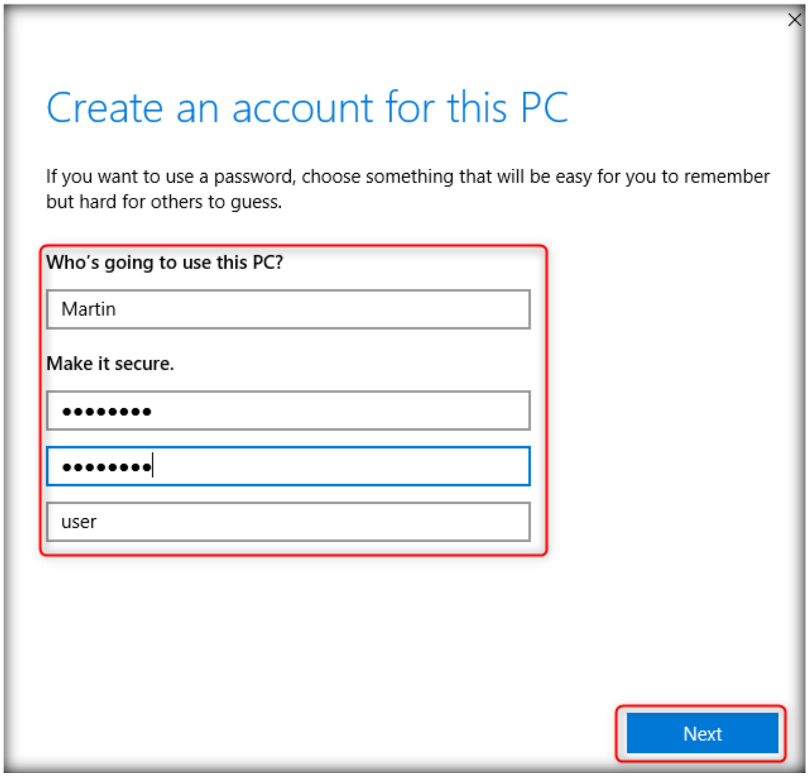


Let's create your account

Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more personal when you sign in with your Microsoft account.* Learn more

*If you already use a Microsoft service, go Back to sign in with that account.

8. Type username as **Martin** and password as **user@123** type confirmed password and password hint as **user** click **Next**.



Create an account for this PC

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?

Martin

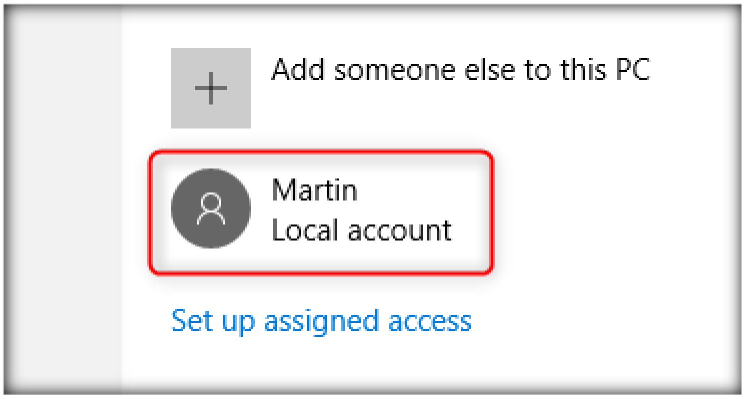
Make it secure.

••••••••

••••••••

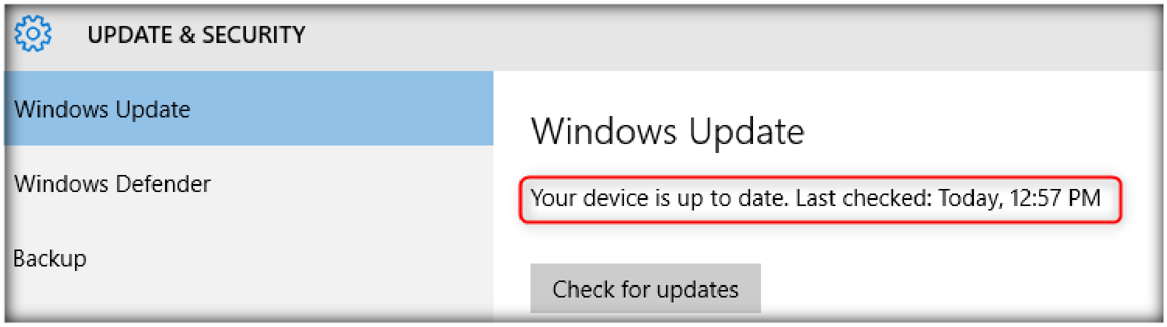
user

9. User Martin will be created as shown following screenshot.



10. Now, check for the system updates and if found any, update the **Windows 10** virtual machine to the latest.

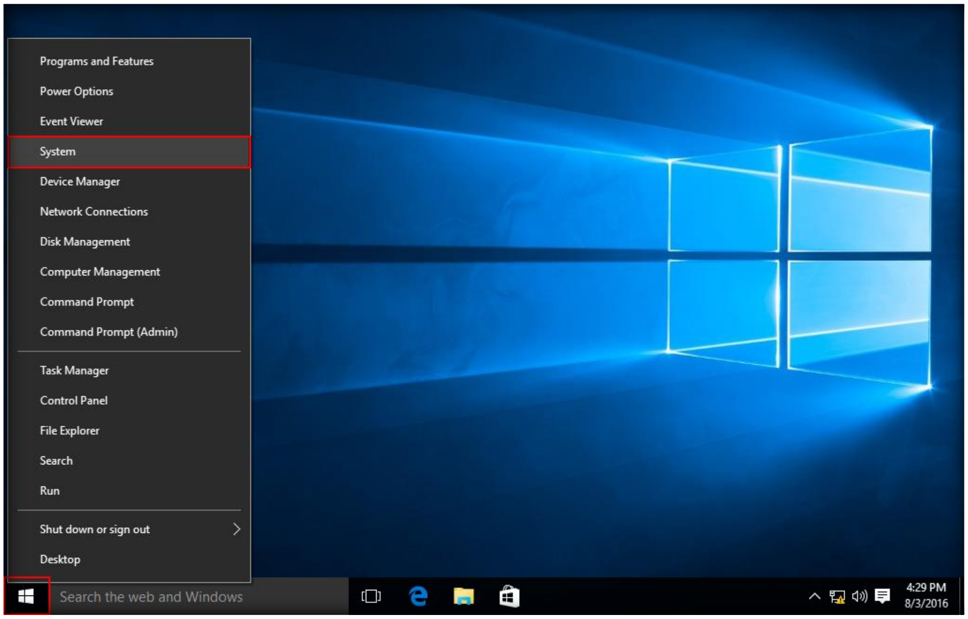
    Note: Installing the updates might take some time.



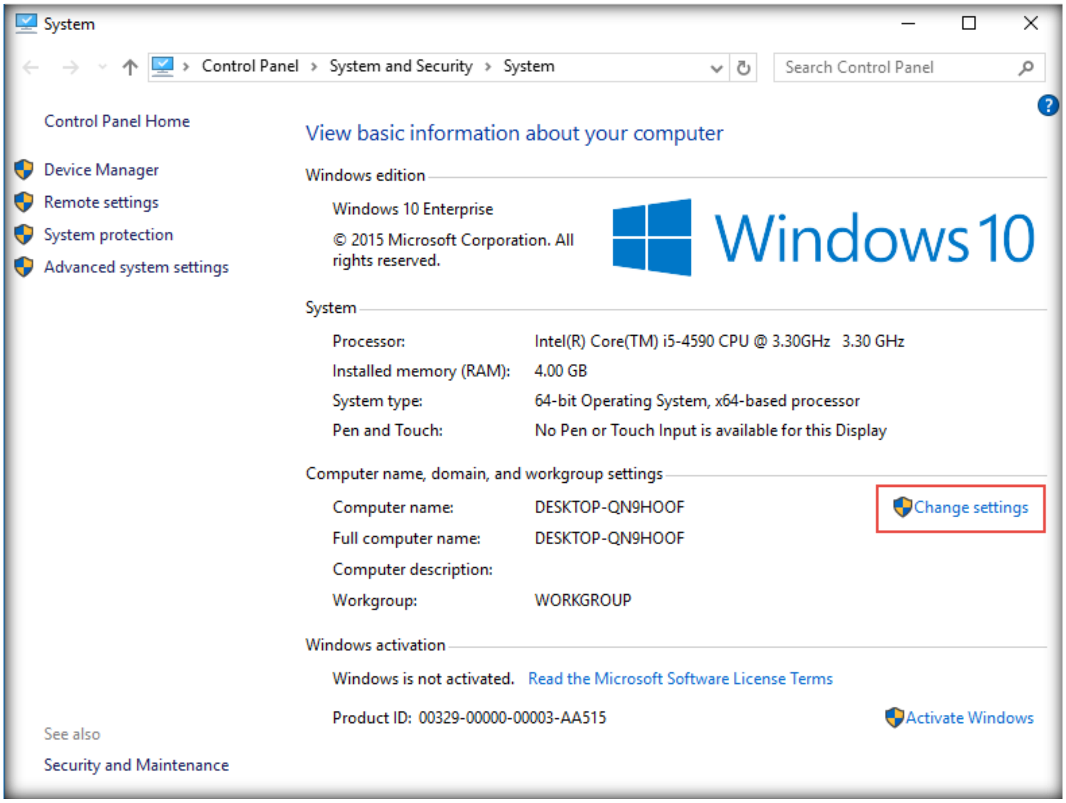
Your device is up to date. Last checked: Today, 12:57 PM

CT#8.3: Change the Computer Name

1. Right-click **Start** icon and click on **System**.



2. In the System window, click **Change settings**.



View basic information about your computer

Windows edition

Windows 10 Enterprise

© 2015 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 3.30 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

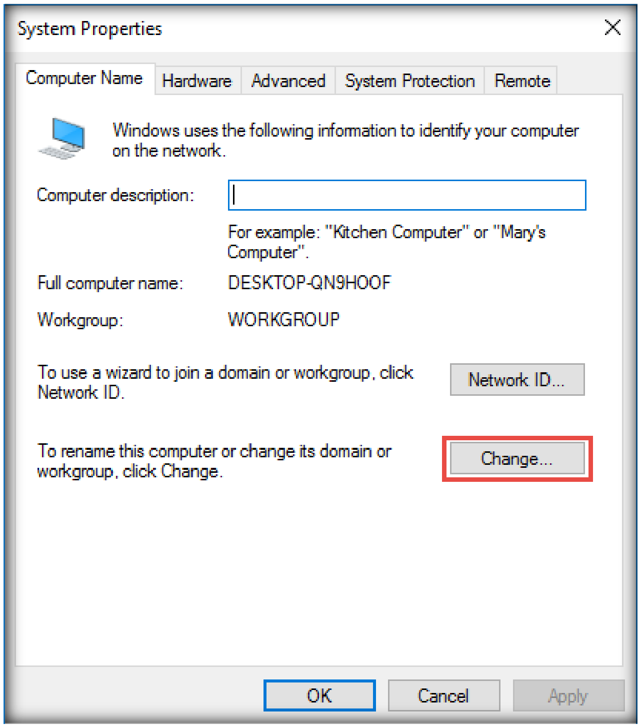
Computer name:	DESKTOP-QN9HOOF	Change settings
Full computer name:	DESKTOP-QN9HOOF	
Computer description:		
Workgroup:	WORKGROUP	

Windows activation

Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00329-00000-00003-AA515 Activate Windows

3. In the Computer Name tab of the System Properties window, click **Change**.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

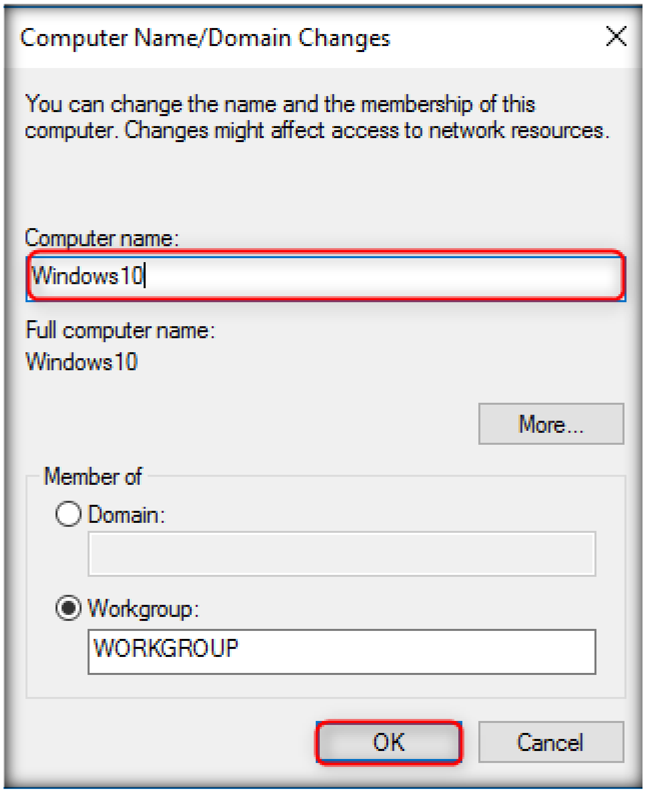
Full computer name: DESKTOP-QN9HOOF

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

4. In the Computer Name field, enter **Windows10** and click OK.



You can change the name and the membership of this computer. Changes might affect access to network resources.

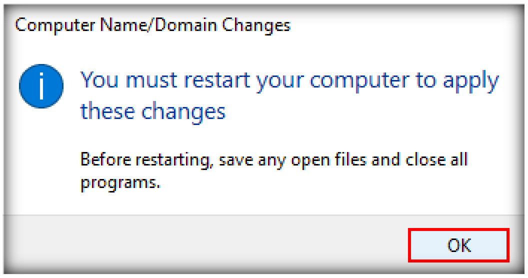
Computer name: Windows10

Full computer name:
Windows10

○ Domain:

● Workgroup: WORKGROUP

5. When prompted to restart the system, click **OK.**

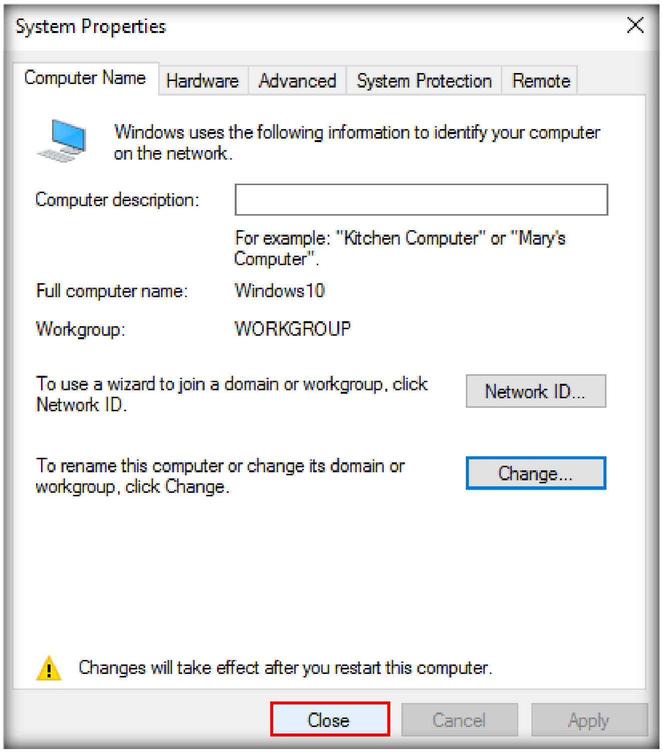


Computer Name/Domain Changes

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

6. You will be returned back to System Properties window, click **Close**.



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Windows10

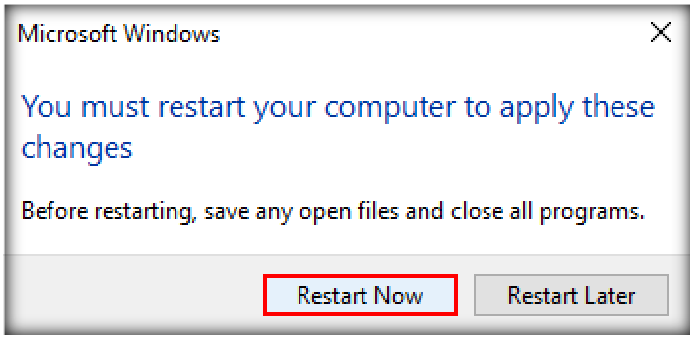
Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Changes will take effect after you restart this computer.

7. You will be prompted to restart the system, click **Restart Now**.



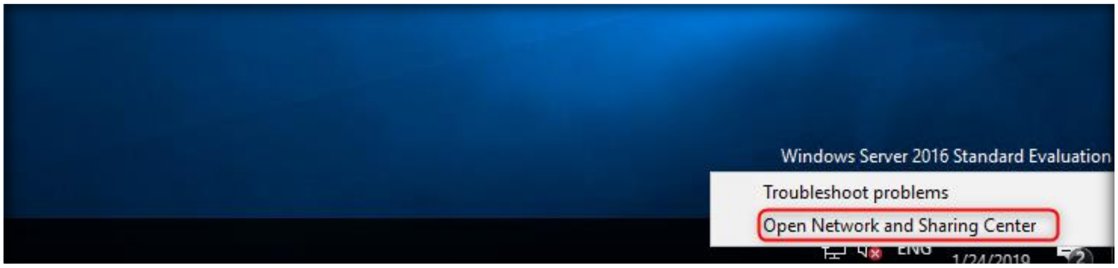
Microsoft Windows

You must restart your computer to apply these changes

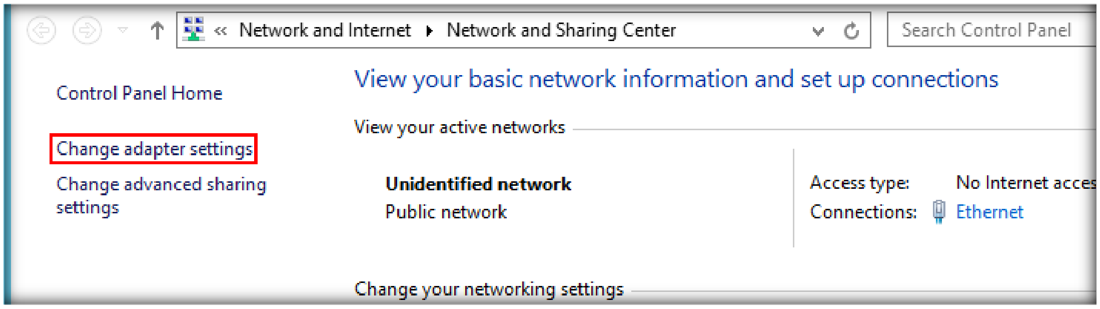
Before restarting, save any open files and close all programs.

CT#8.4: Configuring Static IP Address

1. Login as Administrator (Username : Admin Password: admin@123). ight-click on **Network** icon (lower right corner of the desktop) and click **Open Network and Sharing Center** from the context menu.

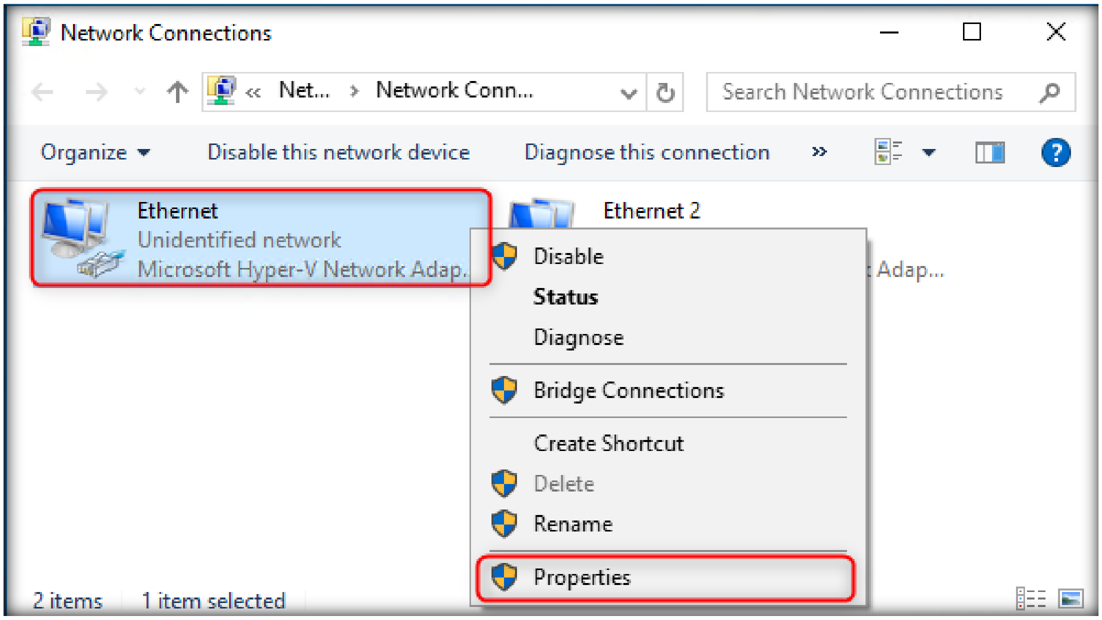

Windows Server 2016 Standard Evaluation
Troubleshoot problems
Open Network and Sharing Center
ENG
1/24/2019

2. Network and Sharing Center window appear, click **Change adapter settings** link from the left pane.

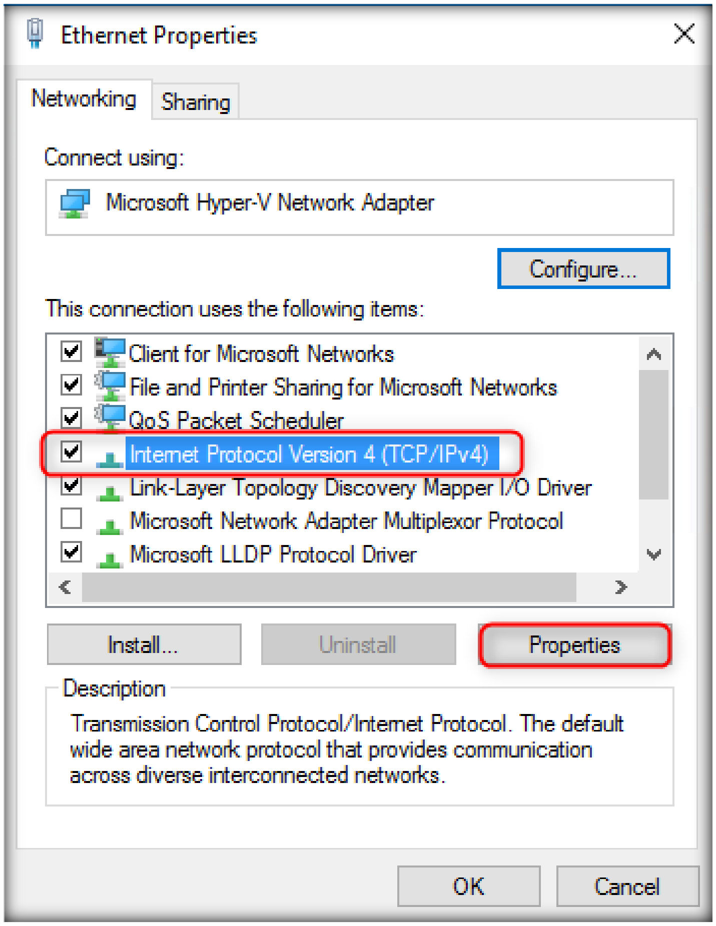

« Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Unidentified network
Public network
Access type: No Internet acces
Connections: Ethernet
Change your networking settings

3. In the Network Connections window, right-click on Unidentified network (**Ethernet**) adapter and click **Properties** from the context menu.

Note: The Name of Unidentified network may vary.



4. Ethernet adapter Properties window appears; and select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



Ethernet Properties

Connect using:

Microsoft Hyper-V Network Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

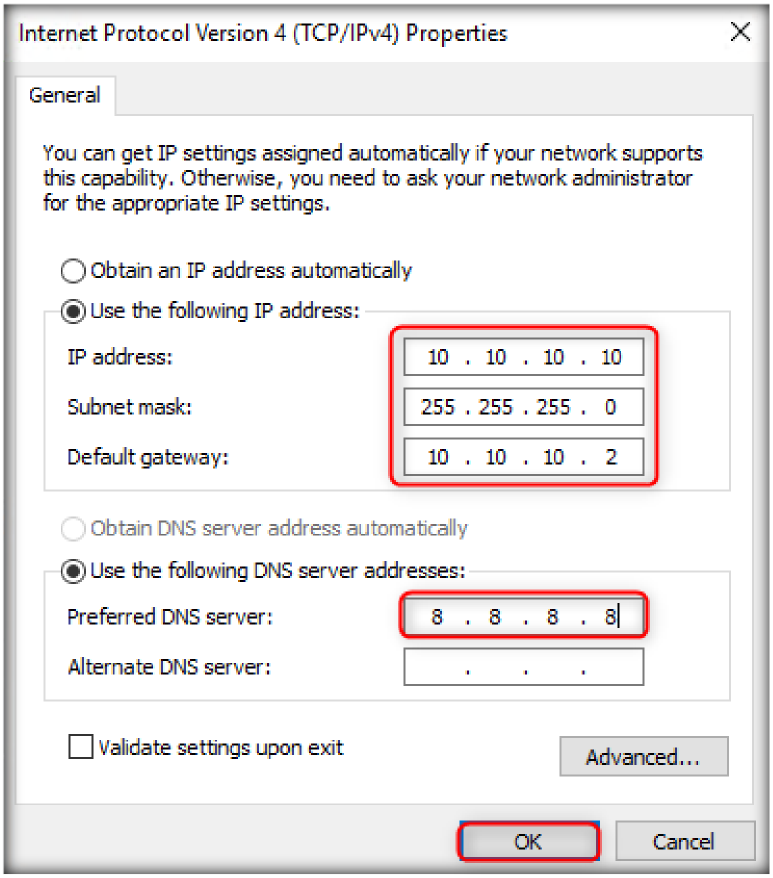
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select **Use the following IP address** and **Use the following DNS server addresses** radio buttons, and type the following values as shown in the screenshot and click **OK**.

   - IP address: **10.10.10.10**
   - Subnet mask: **255.255.255.0**
   - Default gateway: **10.10.10.2**
   - Preferred DNS server: **8.8.8.8**

   Note: Once you click on **OK** button if Networks section appears on the right side of the desktop screen, and then click **Yes**.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 10 . 10 . 2

○ Obtain DNS server address automatically

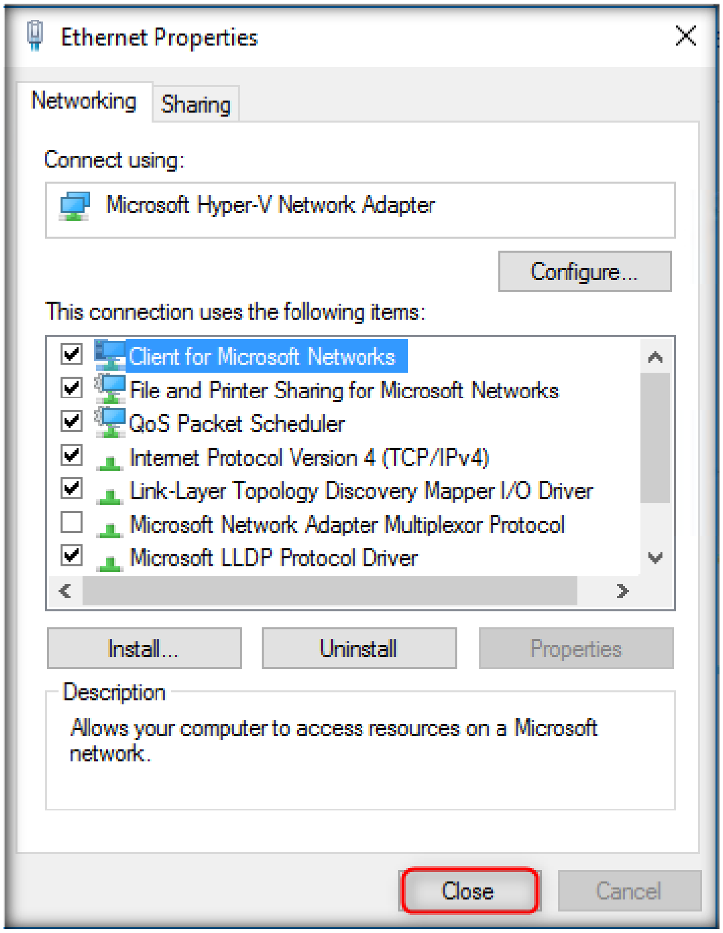
● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: . . .

□ Validate settings upon exit

6. Click **Close** to close the Ethernet Properties window.



Connect using:

Microsoft Hyper-V Network Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver

Description

Allows your computer to access resources on a Microsoft network.

CT#8.5: Sharing SOC-Tools Folder from Host Machine and Mapping to Windows 10 VM

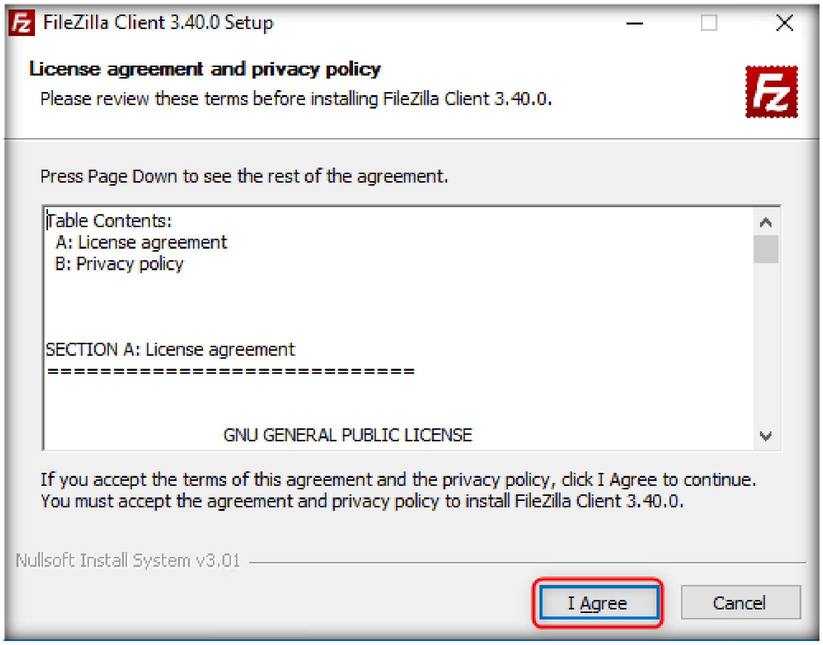
1. Follow CT#6.4, to share **SOC-Tools** directory in Windows10 VM.

CT#8.6: Installing Web Browsers

1. Follow CT#6.6, to install web browser.

CT#8.7: Installing FTP Client

1. Navigate to **Z:\Lab Prerequisites\FileZilla** folder.
2. Double click on **FileZilla_3.40.0_win64-setup_bundled.exe** to begin the installation.
3. If the **Open - File Security Warning** pop-up appears, click **Run**.
4. Follow the wizard steps (by selecting default options) to install FileZilla.
5. Click **I Agree**.



FileZilla Client 3.40.0 Setup

License agreement and privacy policy

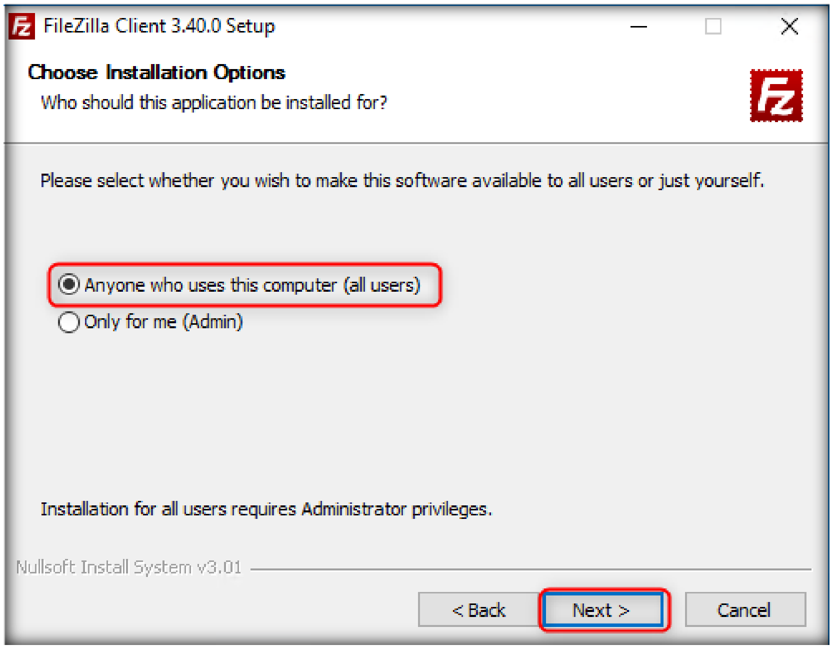
Please review these terms before installing FileZilla Client 3.40.0.

Press Page Down to see the rest of the agreement.

```
Table Contents:
  A: License agreement
  B: Privacy policy


SECTION A: License agreement
============================


                     GNU GENERAL PUBLIC LICENSE
```

If you accept the terms of this agreement and the privacy policy, click I Agree to continue. You must accept the agreement and privacy policy to install FileZilla Client 3.40.0.

6. Leave default option as it is click **Next**.



FileZilla Client 3.40.0 Setup

Choose Installation Options

Who should this application be installed for?

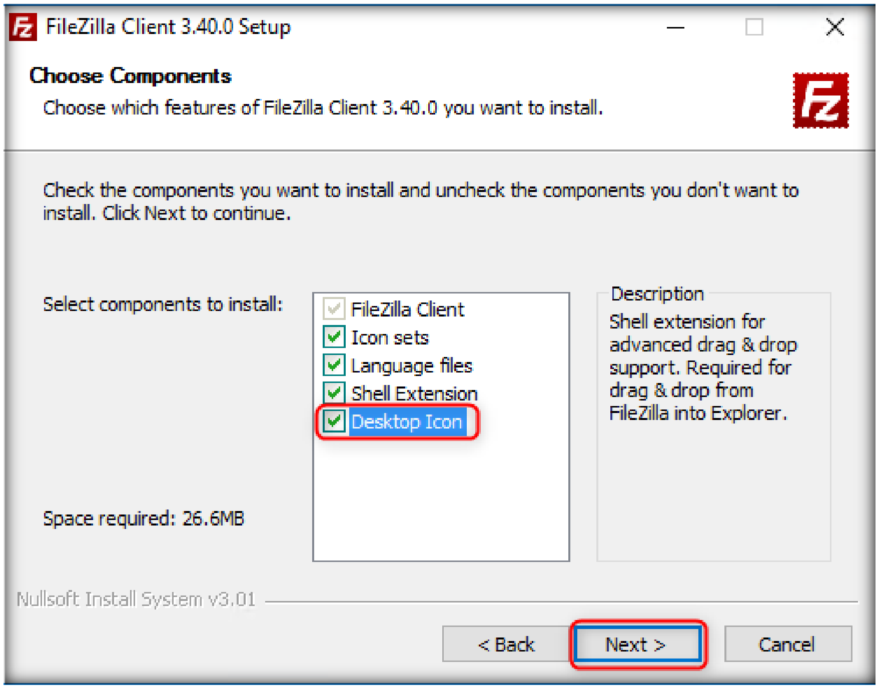
Please select whether you wish to make this software available to all users or just yourself.

● Anyone who uses this computer (all users)

○ Only for me (Admin)

Installation for all users requires Administrator privileges.

7. Check **Desktop Icon** option from list and click **Next.**



FileZilla Client 3.40.0 Setup

Choose Components

Choose which features of FileZilla Client 3.40.0 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

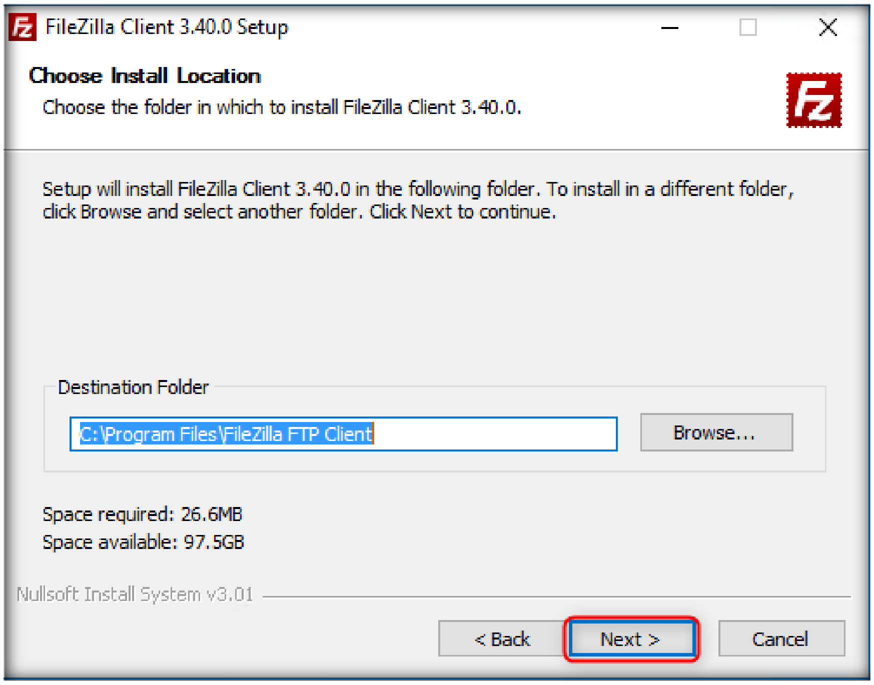
- ☑ FileZilla Client
- ☑ Icon sets
- ☑ Language files
- ☑ Shell Extension
- ☑ Desktop Icon

Description

Shell extension for advanced drag & drop support. Required for drag & drop from FileZilla into Explorer.

Space required: 26.6MB

8. Choose default installation location and Click **Next**.



FileZilla Client 3.40.0 Setup

Choose Install Location

Choose the folder in which to install FileZilla Client 3.40.0.

Setup will install FileZilla Client 3.40.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

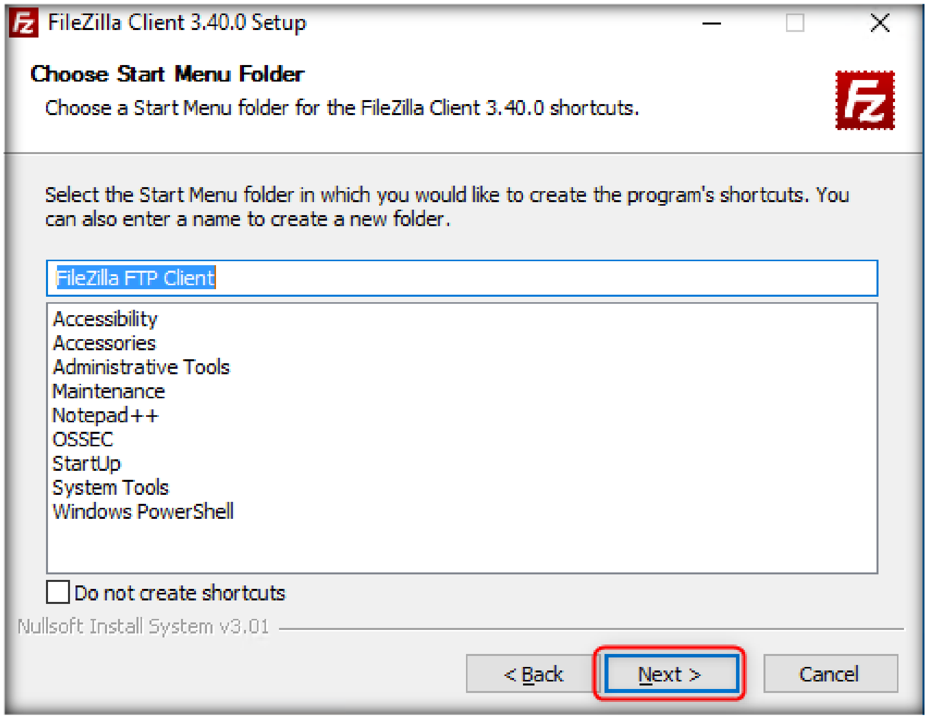
Destination Folder

C:\Program Files\FileZilla FTP Client

Space required: 26.6MB

Space available: 97.5GB

9. Click **Next**.



FileZilla Client 3.40.0 Setup

Choose Start Menu Folder

Choose a Start Menu folder for the FileZilla Client 3.40.0 shortcuts.

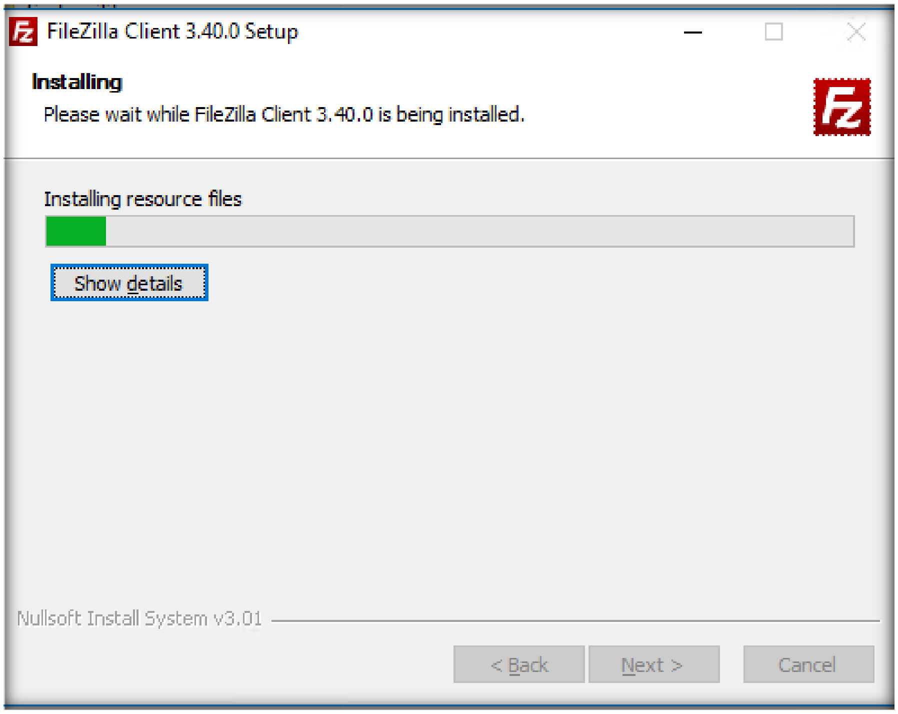
Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

FileZilla FTP Client

Accessibility
Accessories
Administrative Tools
Maintenance
Notepad++
OSSEC
StartUp
System Tools
Windows PowerShell

□ Do not create shortcuts

10. Installation will start.



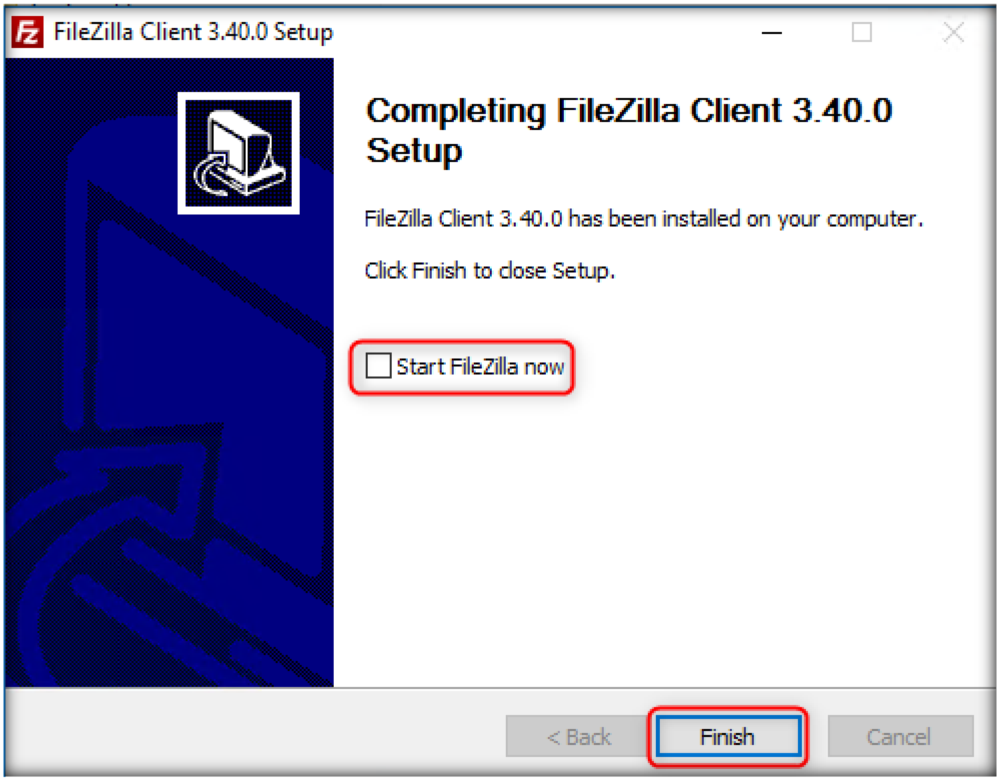
FileZilla Client 3.40.0 Setup

Installing

Please wait while FileZilla Client 3.40.0 is being installed.

Installing resource files

11. Uncheck **Start FileZilla now** option and click **Finish** button to complete filezilla installation.



Completing FileZilla Client 3.40.0 Setup

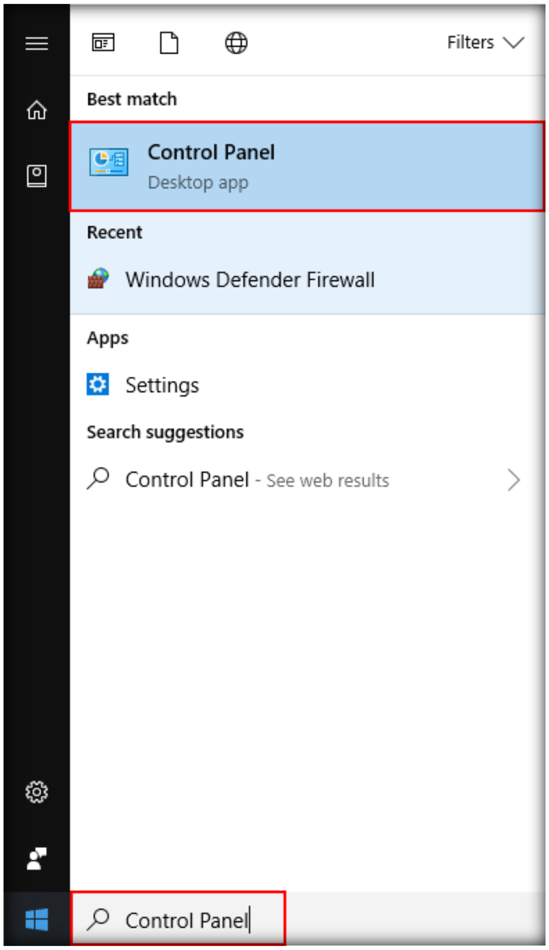
FileZilla Client 3.40.0 has been installed on your computer.

Click Finish to close Setup.

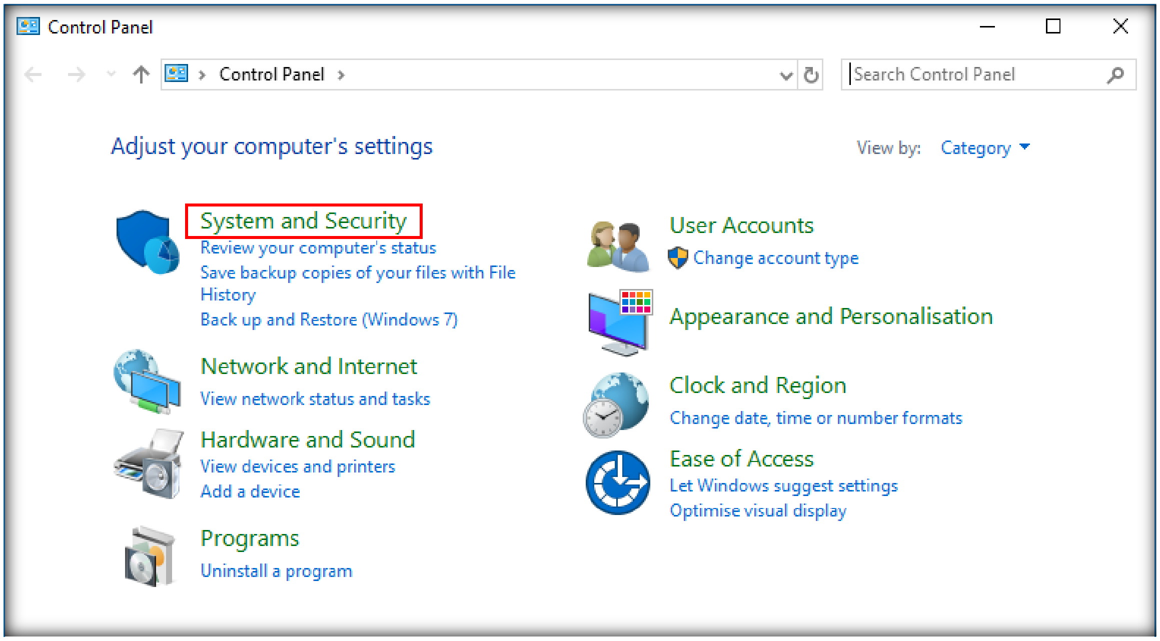
☐ Start FileZilla now

CT#8.8: Turn Off the Windows Defender Firewall

1. In the **Type here to search** field present at the lower left corner of the screen, type **Control Panel**. A search result containing **Control Panel** desktop app appears. Click **Control Panel**.

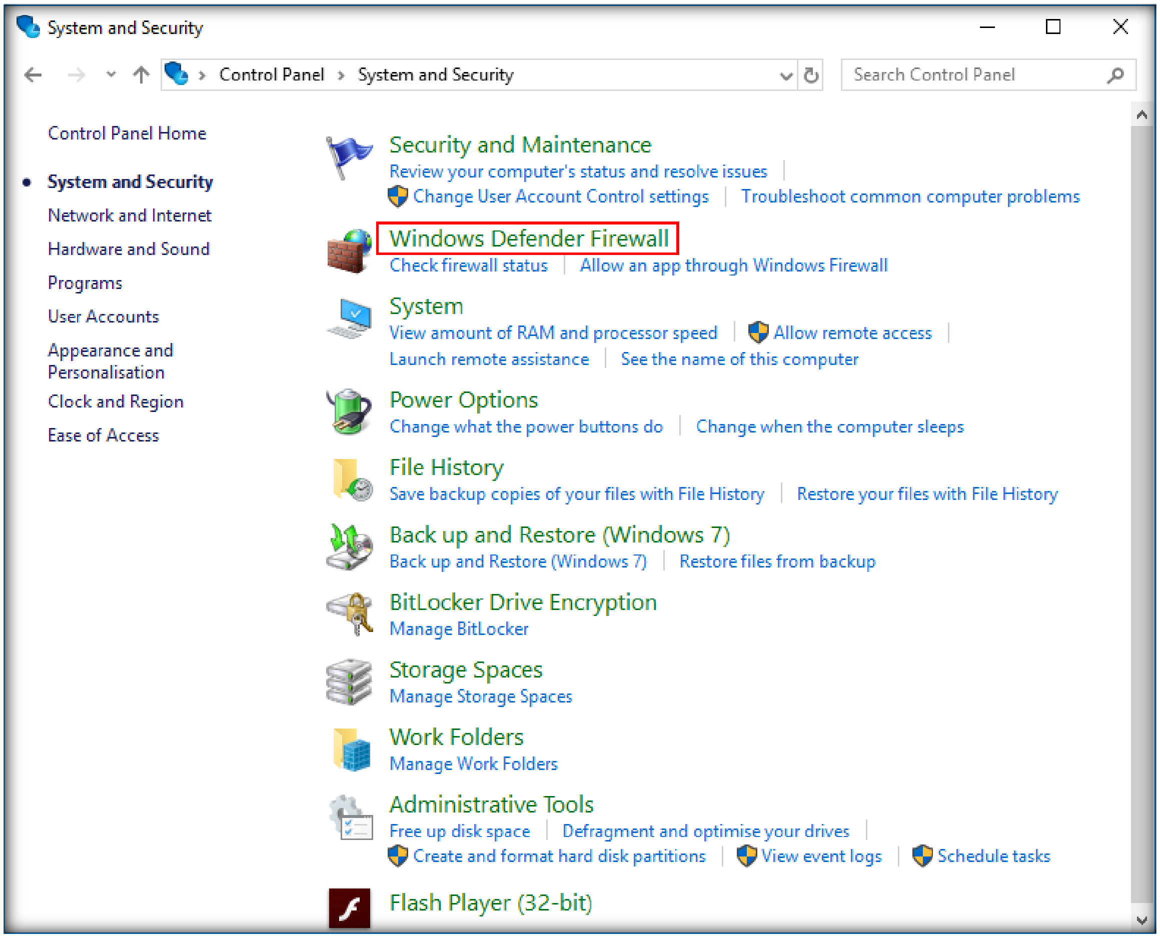


2. In the **Control Panel** window, click **System and Security**.



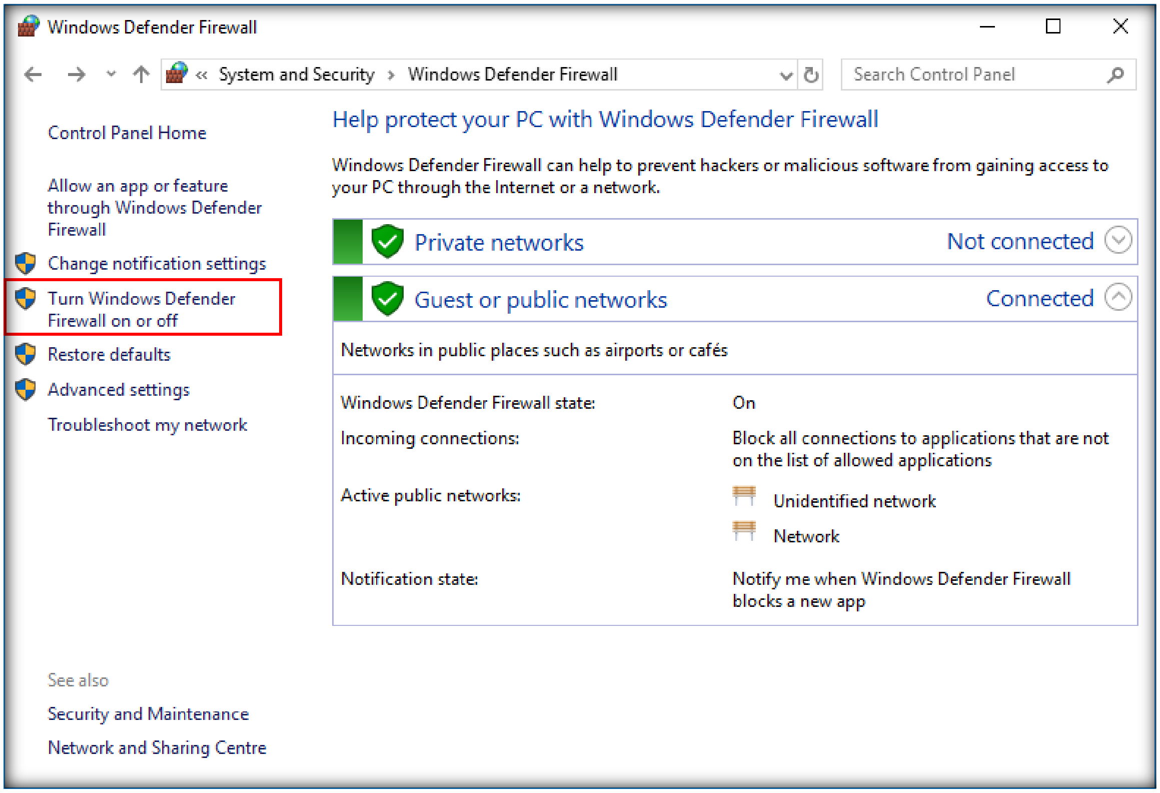
Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Back up and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalisation
Clock and Region
Change date, time or number formats
Ease of Access
Let Windows suggest settings
Optimise visual display

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



System and Security
Control Panel › System and Security
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalisation
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Power Options
Change what the power buttons do
Change when the computer sleeps
File History
Save backup copies of your files with File History
Restore your files with File History
Back up and Restore (Windows 7)
Back up and Restore (Windows 7)
Restore files from backup
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Free up disk space
Defragment and optimise your drives
Create and format hard disk partitions
View event logs
Schedule tasks
Flash Player (32-bit)

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


Windows Defender Firewall
« System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Centre

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help to prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

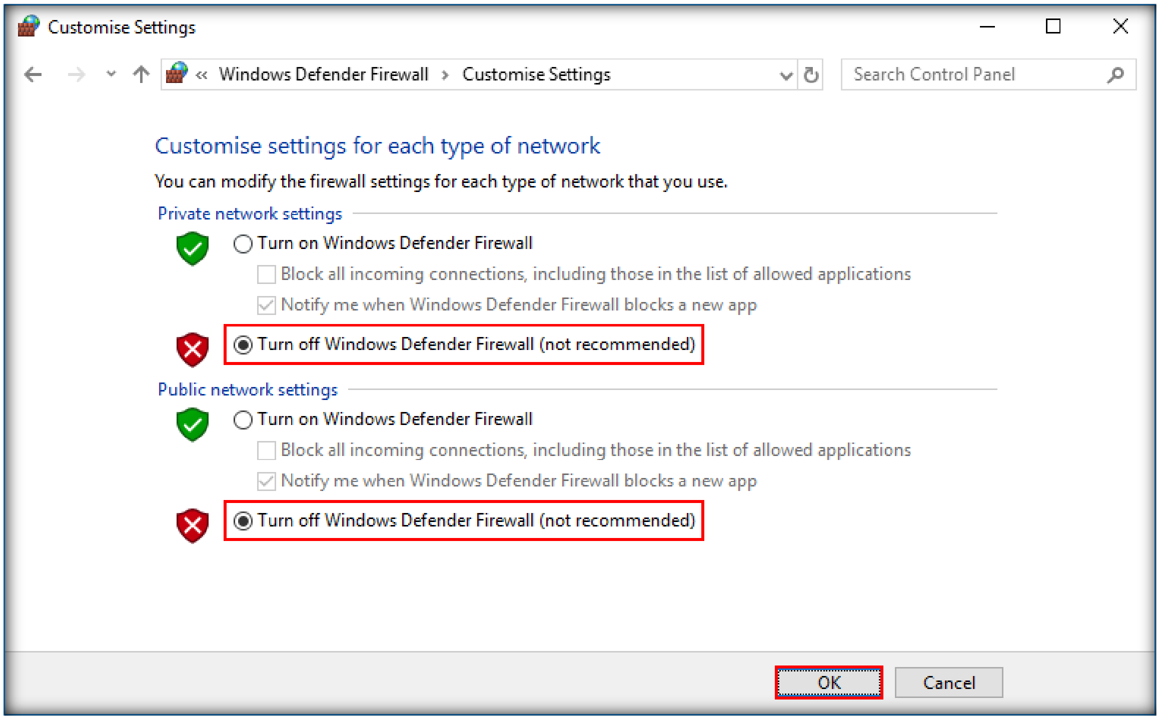
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or cafés

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to applications that are not on the list of allowed applications
Active public networks:	Unidentified network Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

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



Customise settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed applications

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

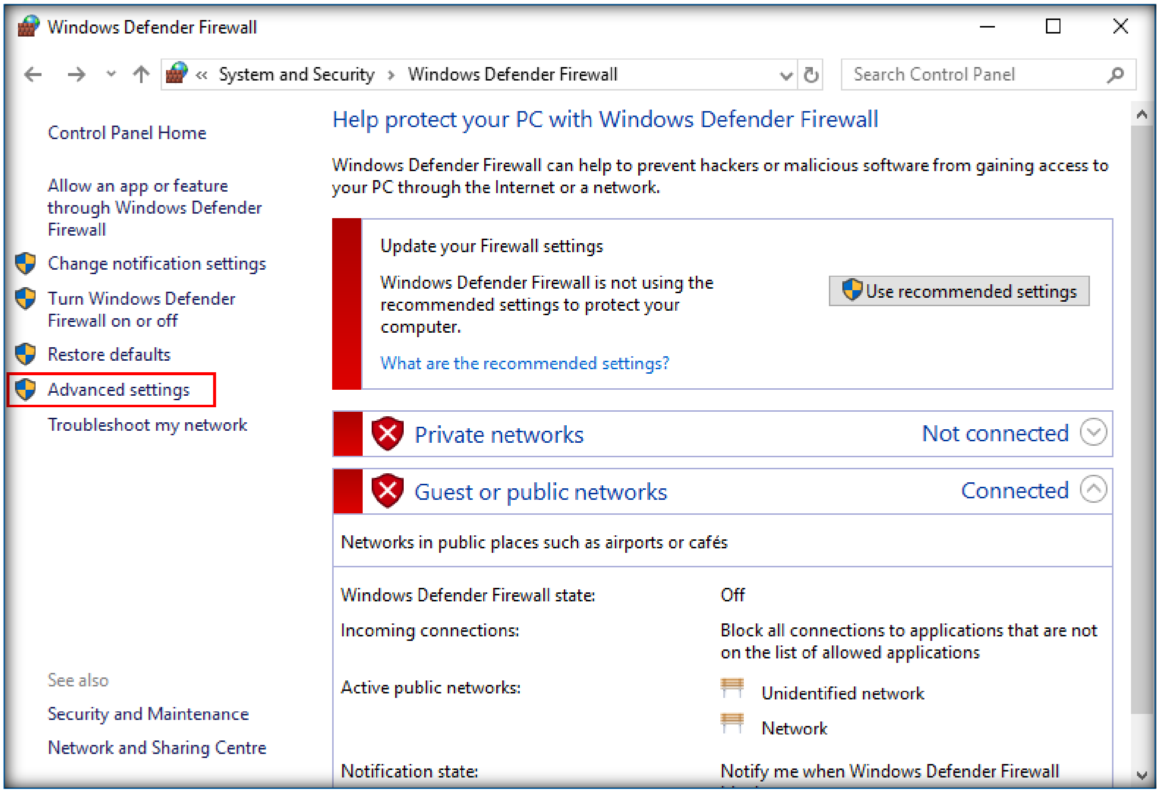
○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed applications

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

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



Windows Defender Firewall

System and Security > Windows Defender Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Security and Maintenance

Network and Sharing Centre

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help to prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

Use recommended settings

What are the recommended settings?

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or cafés

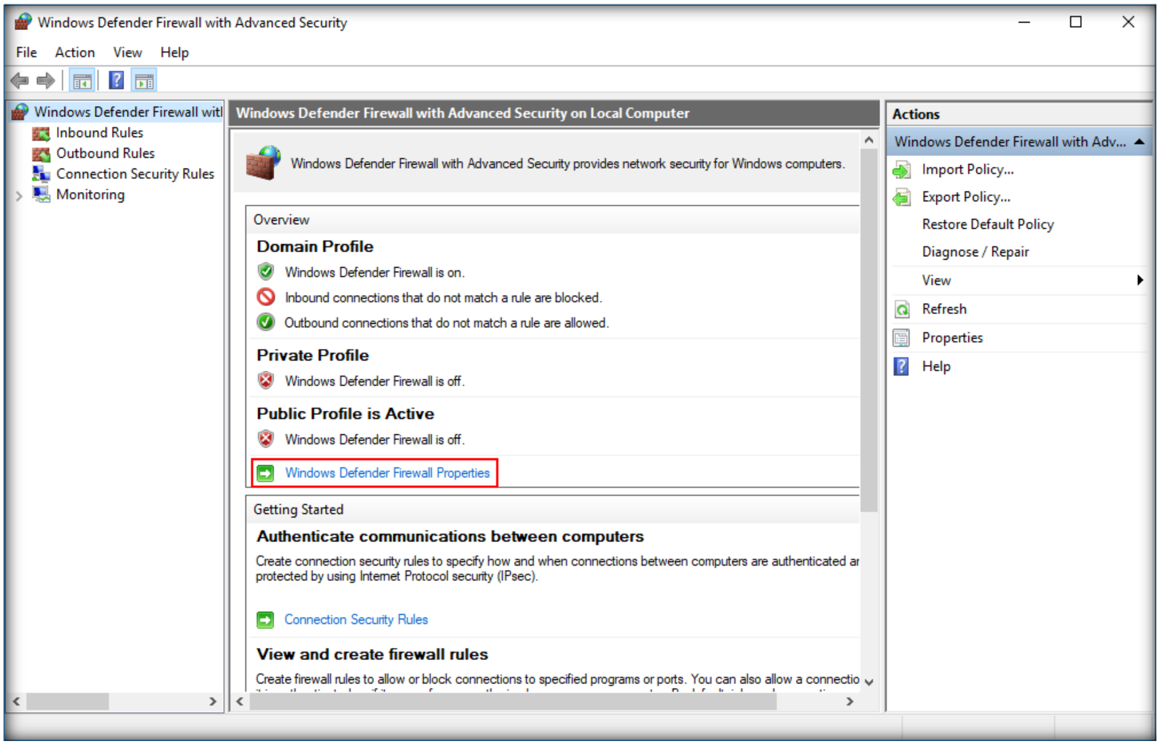
Windows Defender Firewall state: Off

Incoming connections: Block all connections to applications that are not on the list of allowed applications

Active public networks: Unidentified network; Network

Notification state: Notify me when Windows Defender Firewall

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



Windows Defender Firewall with Advanced Security

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is off.

Public Profile is Active

- Windows Defender Firewall is off.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

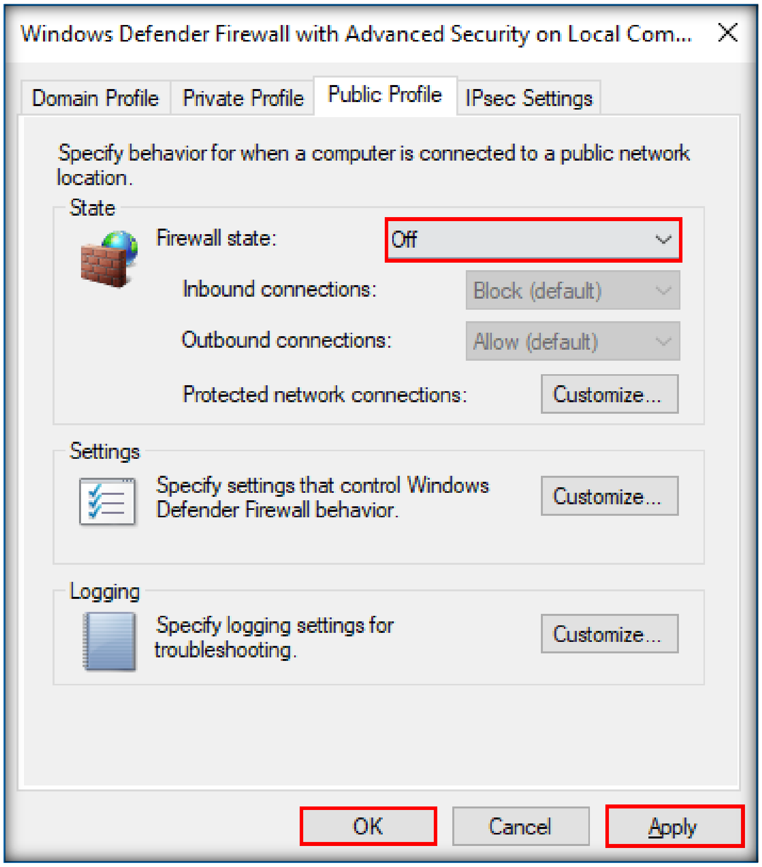
Create connection security rules to specify how and when connections between computers are authenticated ar protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connectio

8. 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 **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply** and then click **OK**.



Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

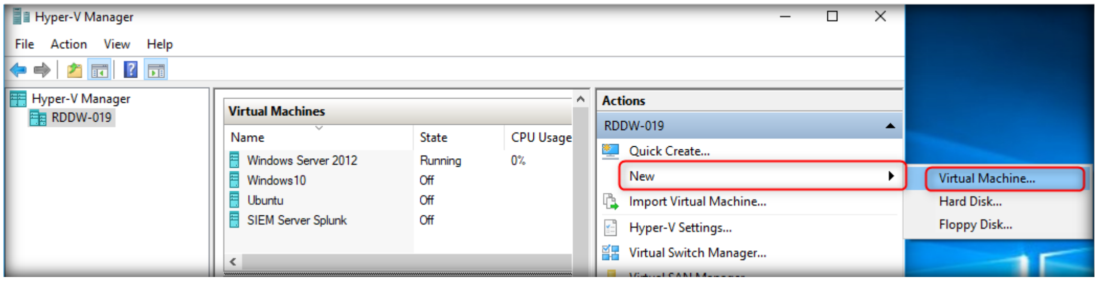
OK Cancel Apply

9. Close all the windows.

CT#9: Creating and Configuring Kali Linux Virtual Machine

CT#9.1: Creating a Virtual Machine and Installing Kali Linux OS

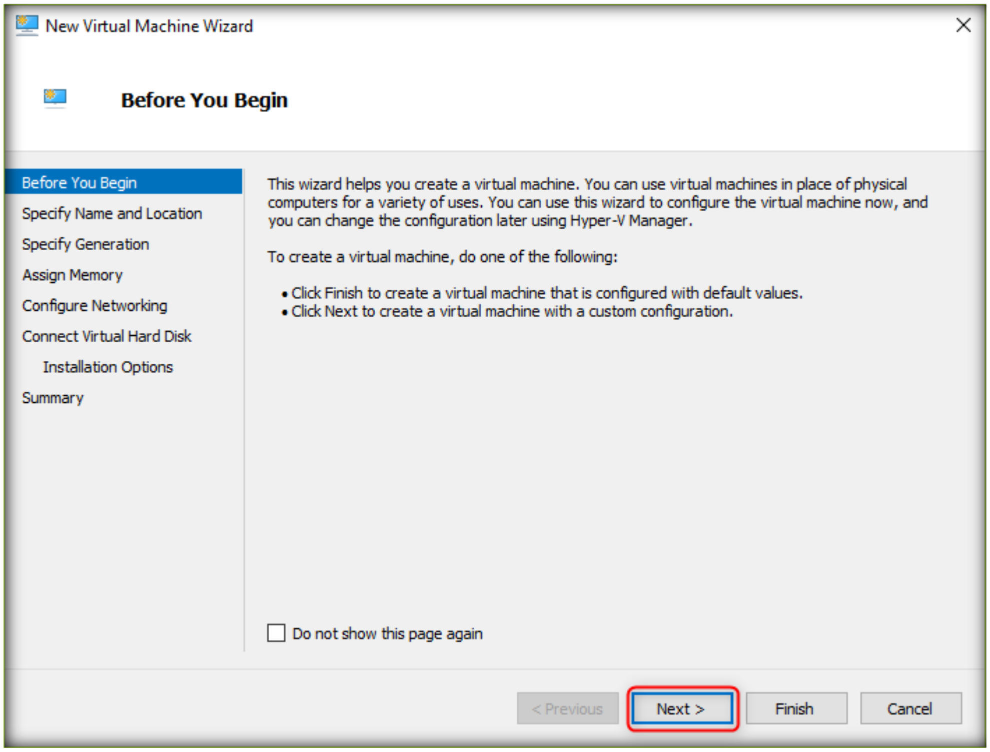
1. Launch Hyper-V Manager. If already launched, skip to step two.
2. Select your local machine in the left pane, then click **New**, and then click **Virtual Machine…** in the right pane as shown in the screen shot.



Name	State	CPU Usage
Windows Server 2012	Running	0%
Windows10	Off	
Ubuntu	Off	
SIEM Server Splunk	Off	

Note: Every machine has a unique name, so the name of your machine differs from the name shown in the above screenshot.

3. **New Virtual Machine Wizard** window appears, click **Next** button.



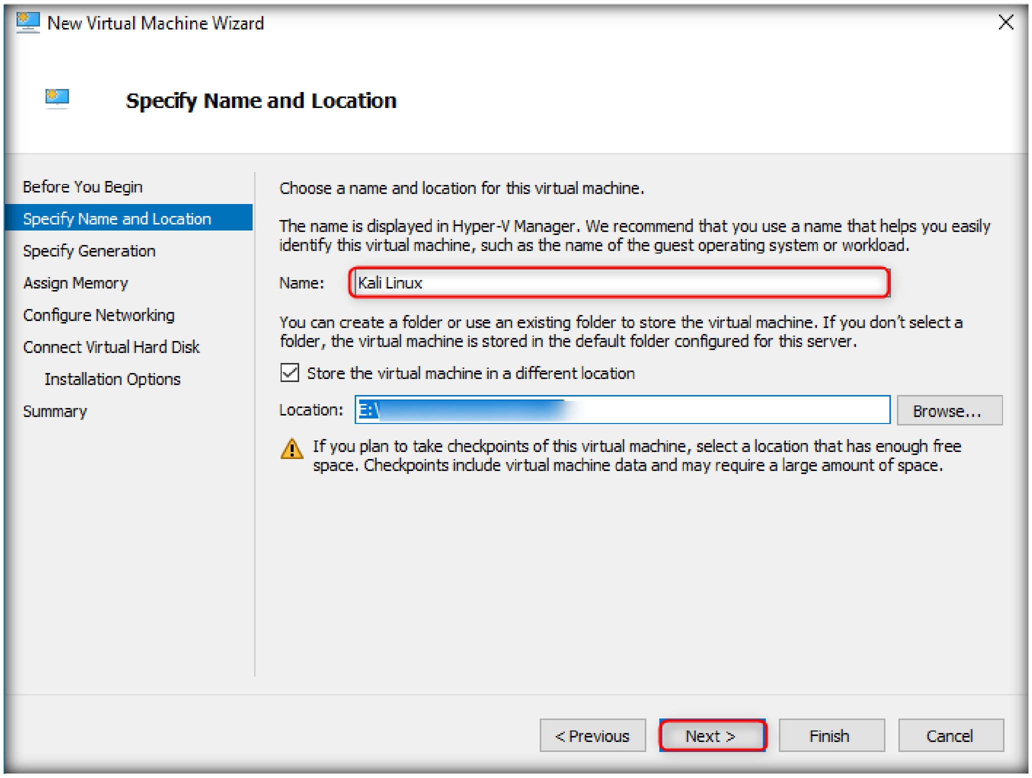
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

4. Specify **Name** and **location** of new virtual machine. Assign the name of the virtual machine as **Kali Linux**.
5. The default location for storing the virtual machine is **C:\ProgramData\Microsoft\Windows\Hyper-V\.** You can choose different location to store the VM's or set it to default location.
6. Click **Next.**

   Note: You can specify the location either in the **Specify Name and Location** section or in the forthcoming **Connect Virtual Hard Disk** section.



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Kali Linux

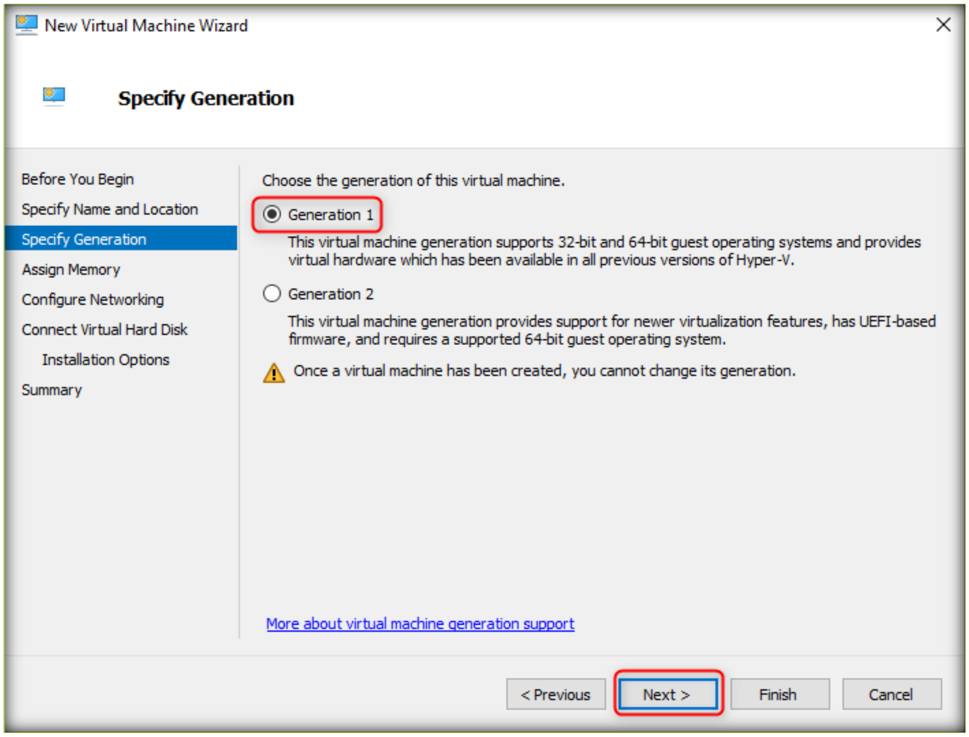
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

Location: E:\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

7. Choose the generation of the virtual machine (here, **Generation 1**) and click **Next.**



Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

○ Generation 2

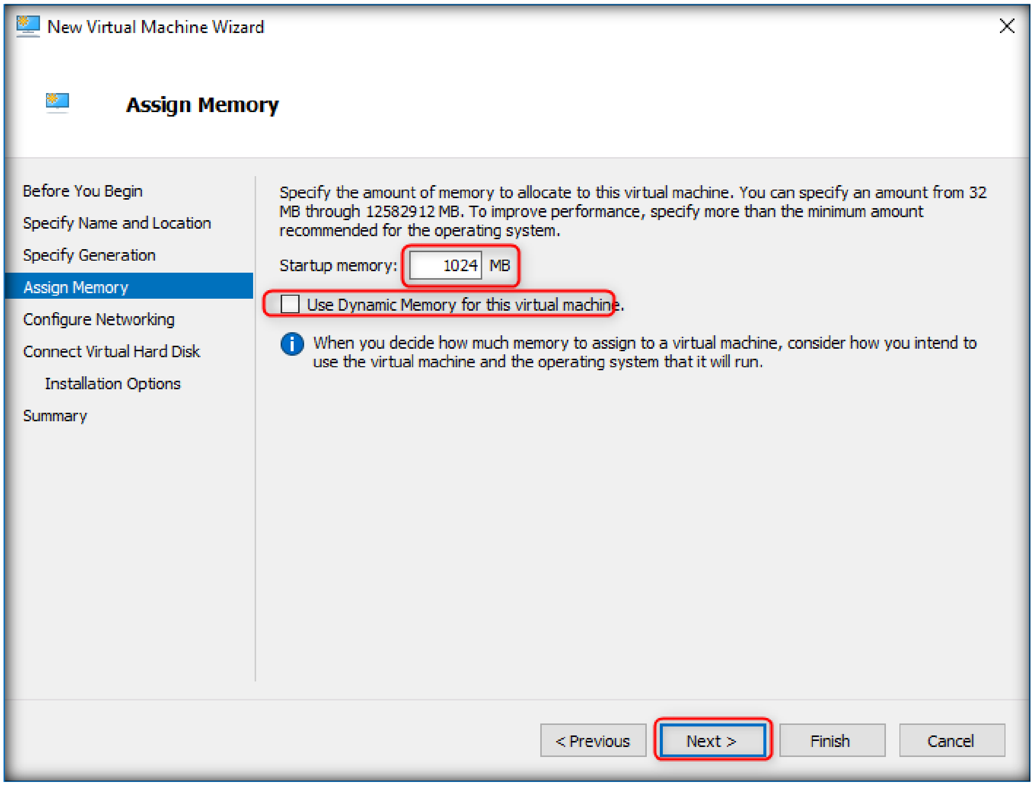
This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

More about virtual machine generation support

8. Assign the amount of Startup memory to allocate to this virtual machine in MB (here, 1024).

9. Click **Next.**



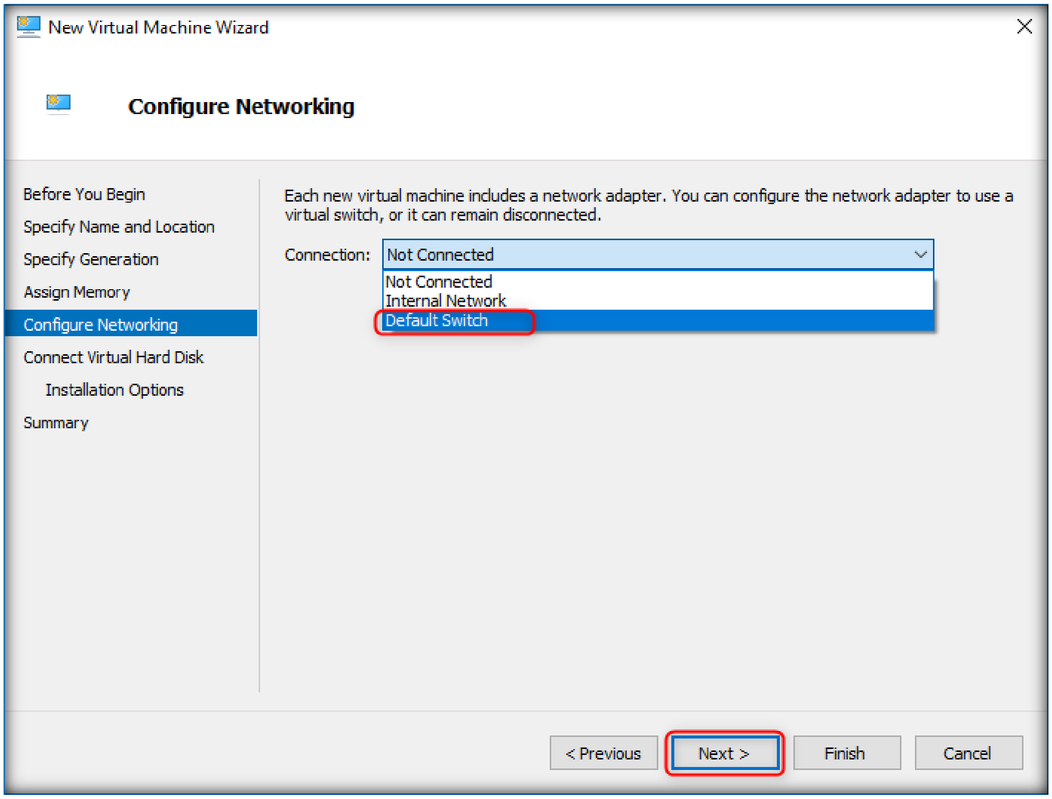
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 1024 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

10. In the next step, select **network adapter** as **Default Switch** from connection drop-down list and click **Next.**



New Virtual Machine Wizard

Configure Networking

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

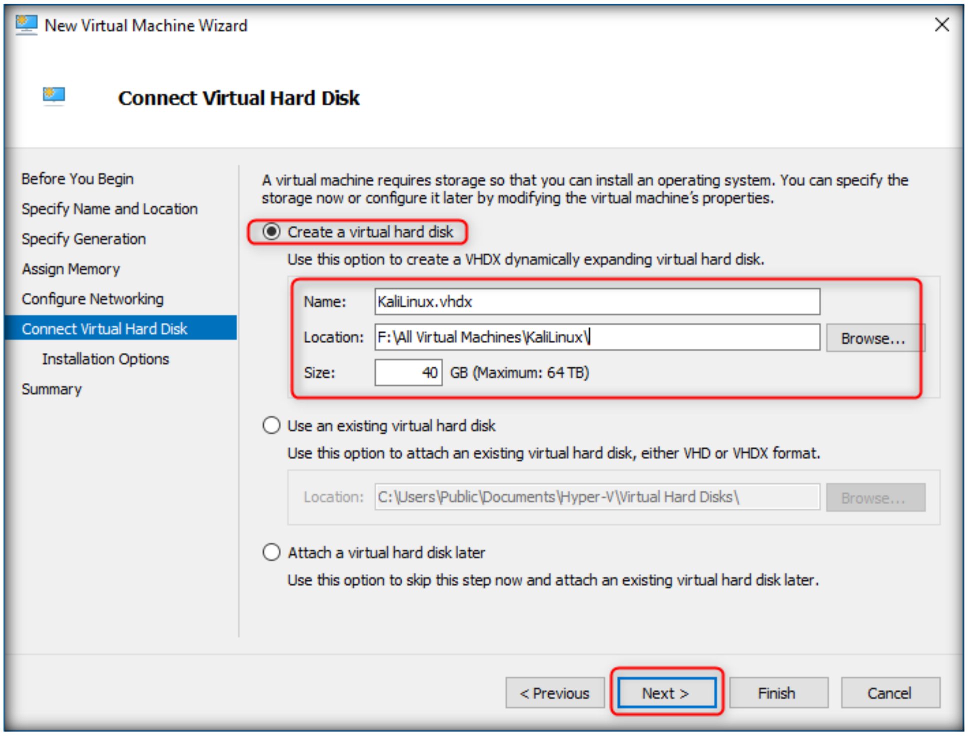
Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

Not Connected
Internal Network
Default Switch

< Previous | Next > | Finish | Cancel

11. Connect Virtual Hard Disk section appears, allocate **40 GB** space for hard disk and click **Next.**



New Virtual Machine Wizard

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: KaliLinux.vhdx

Location: F:\All Virtual Machines\KaliLinux\ Browse...

Size: 40 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...

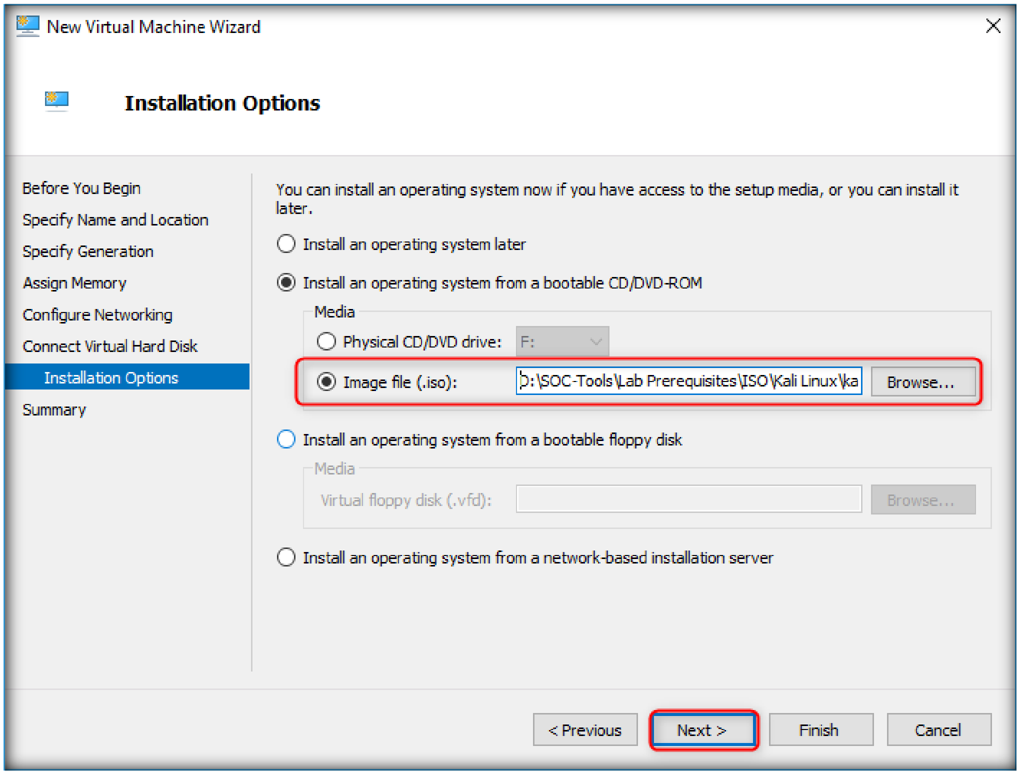
○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous | Next > | Finish | Cancel

12. The **installation options** section appears, select **Install an operating system from a bootable CD/DVD-ROM** radio button.

   - **If** you have a Kali Linux choose Physical CD/DVD drive radio button and then click **Next**.
   - If you have a Kali Linux file, then choose Image file (.iso) radio button and click browse button to provide the path of ISO file and click **Next**.


New Virtual Machine Wizard

Installation Options

You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a bootable CD/DVD-ROM

Media

○ Physical CD/DVD drive: F:

● Image file (.iso): D:\SOC-Tools\Lab Prerequisites\ISO\Kali Linux\ka

○ Install an operating system from a bootable floppy disk

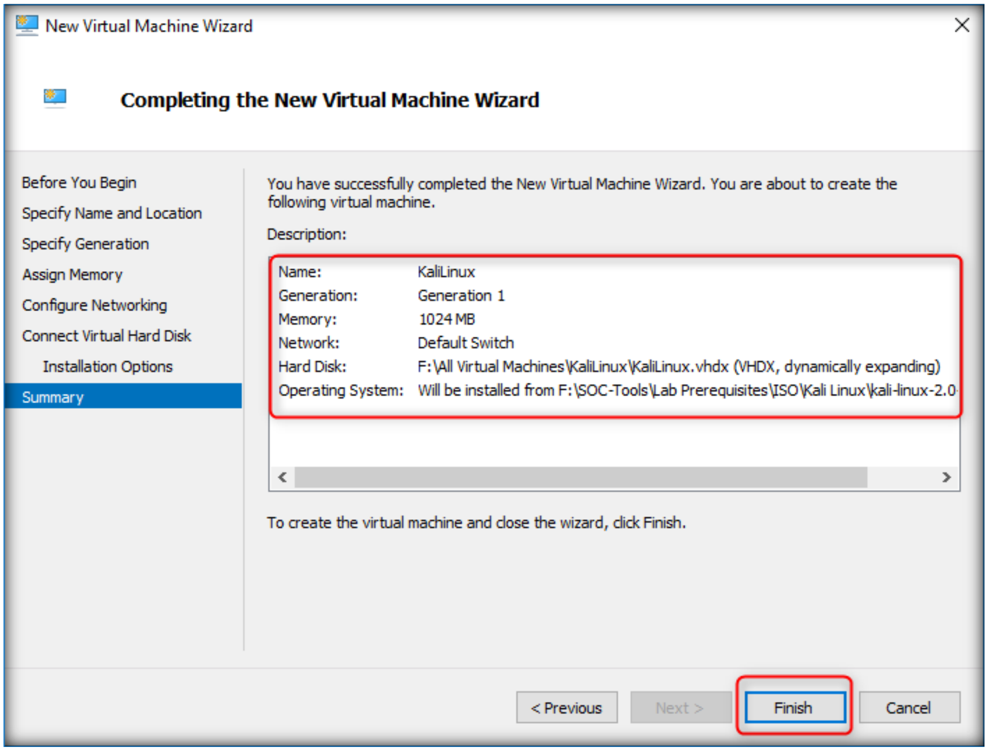
Media

Virtual floppy disk (.vfd):

○ Install an operating system from a network-based installation server

13. Virtual machine wizard appears with summary information.

14. Click **Finish.**



Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

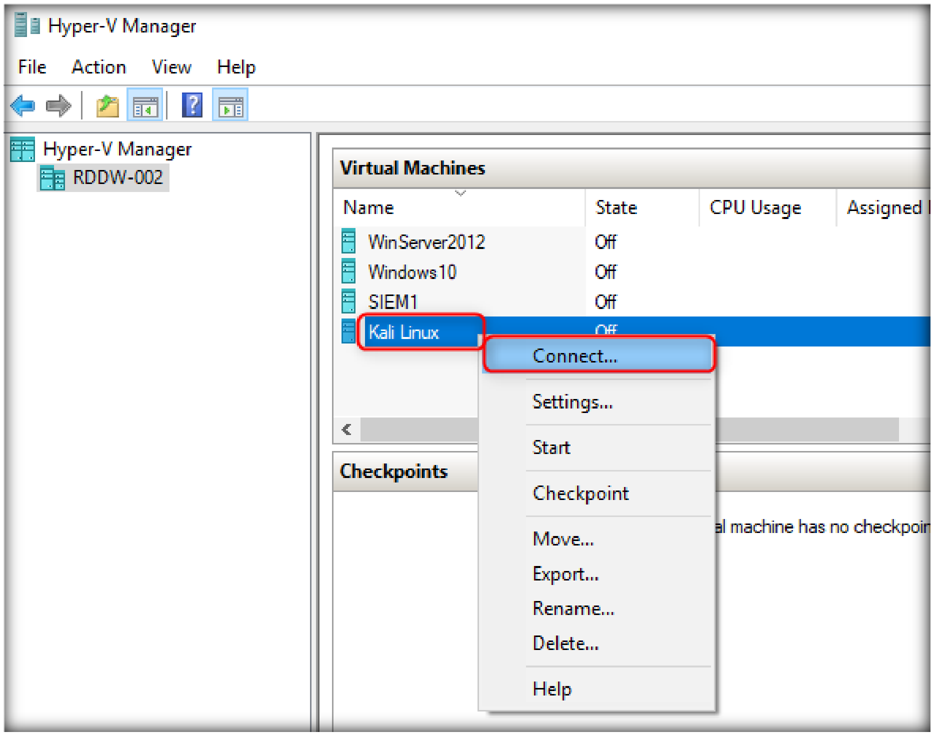
Description:

```
Name:              KaliLinux
Generation:        Generation 1
Memory:            1024 MB
Network:           Default Switch
Hard Disk:         F:\All Virtual Machines\KaliLinux\KaliLinux.vhdx (VHDX, dynamically expanding)
Operating System:  Will be installed from F:\SOC-Tools\Lab Prerequisites\ISO\Kali Linux\kali-linux-2.0
```

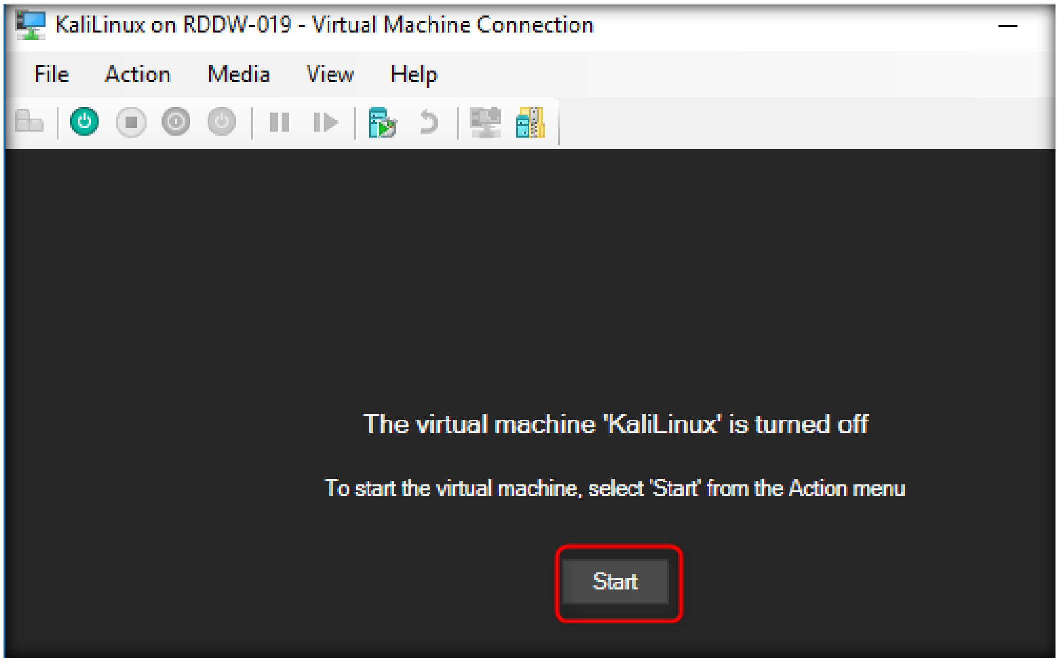
To create the virtual machine and close the wizard, click Finish.

15. Hyper-V Manager creates **Kali Linux** virtual machine profile.

16. In **Hyper-V Manager** main window, you see a new virtual machine named **Kali Linux**. Right-click on the newly created virtual machine and click **Connect** from the context menu.



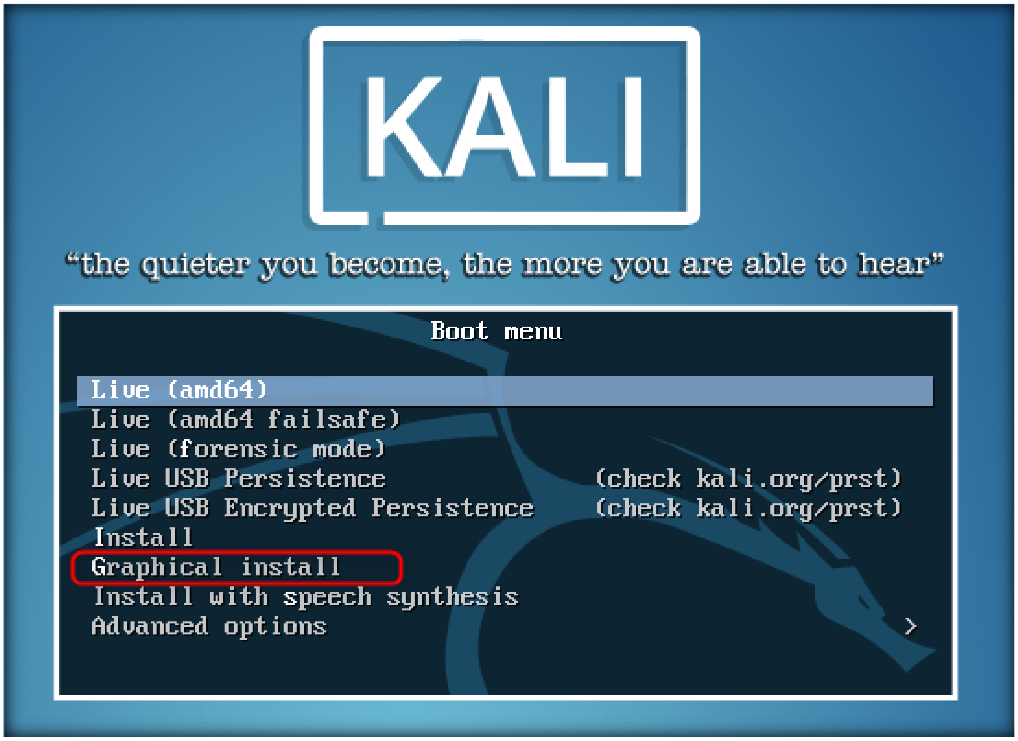
17. Kali Linux Virtual Machine window appears click **Start** button as shown in the screenshot.



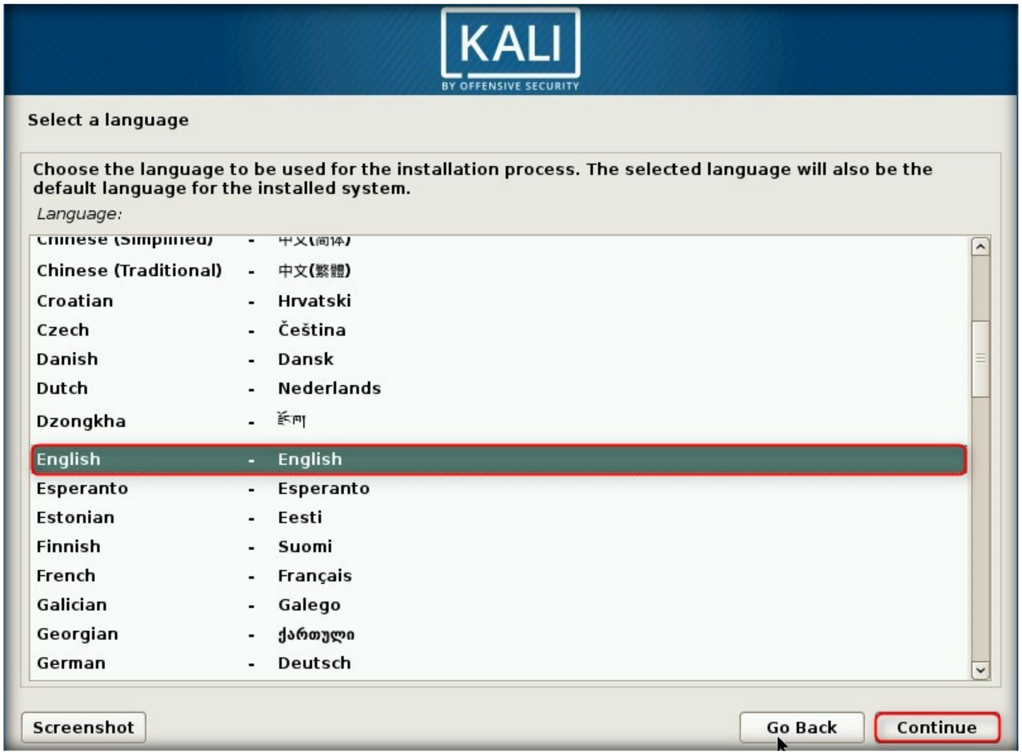
The virtual machine 'KaliLinux' is turned off

To start the virtual machine, select 'Start' from the Action menu

18. Kali Linux **Boot menu** appears, select **Graphical install** and press **Enter**.


KALI
"the quieter you become, the more you are able to hear"
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options >

19. **Select a language** window appears, choose a language (here, **English**) and click **Continue**.



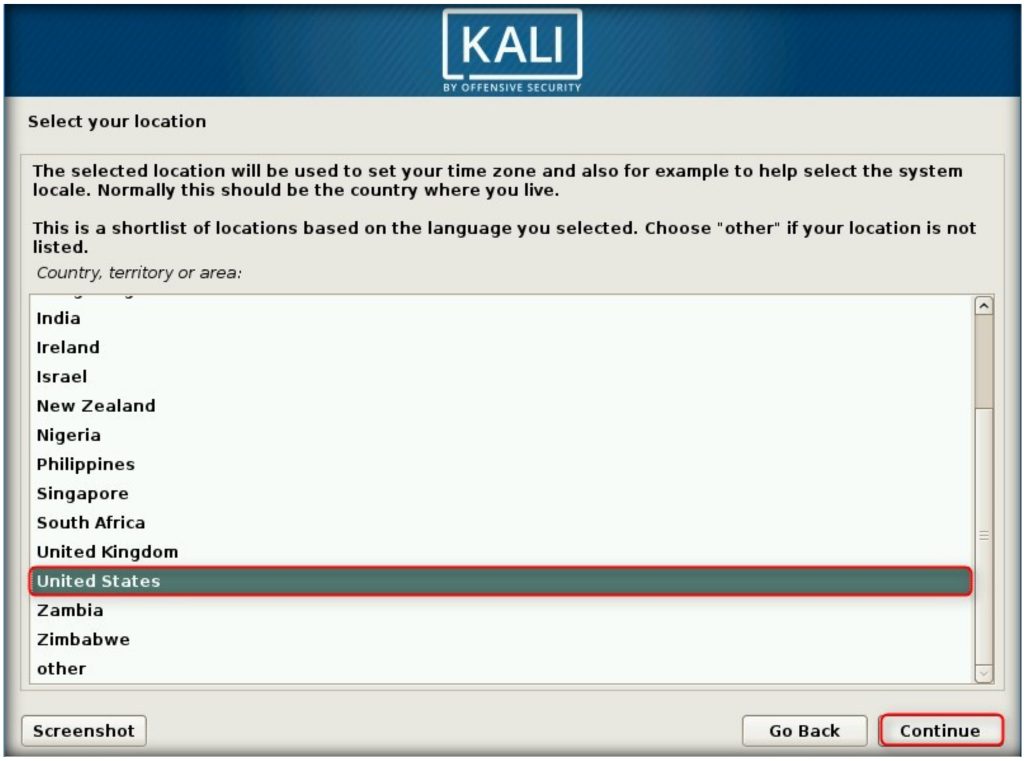
Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

20. In the **Select your location** section, choose a location (here, **United States**) and click **Continue**.



Select your location

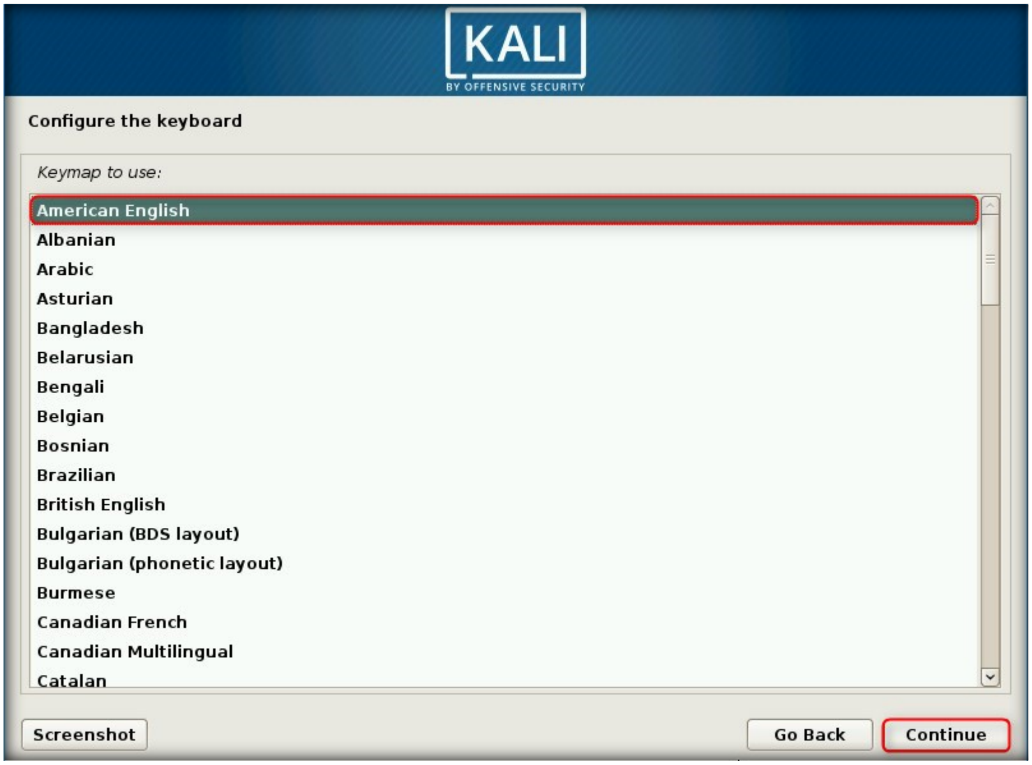
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

India
Ireland
Israel
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

21. **Configure the keyboard** section appears, choose a language (here, **American English**) and click **Continue.**

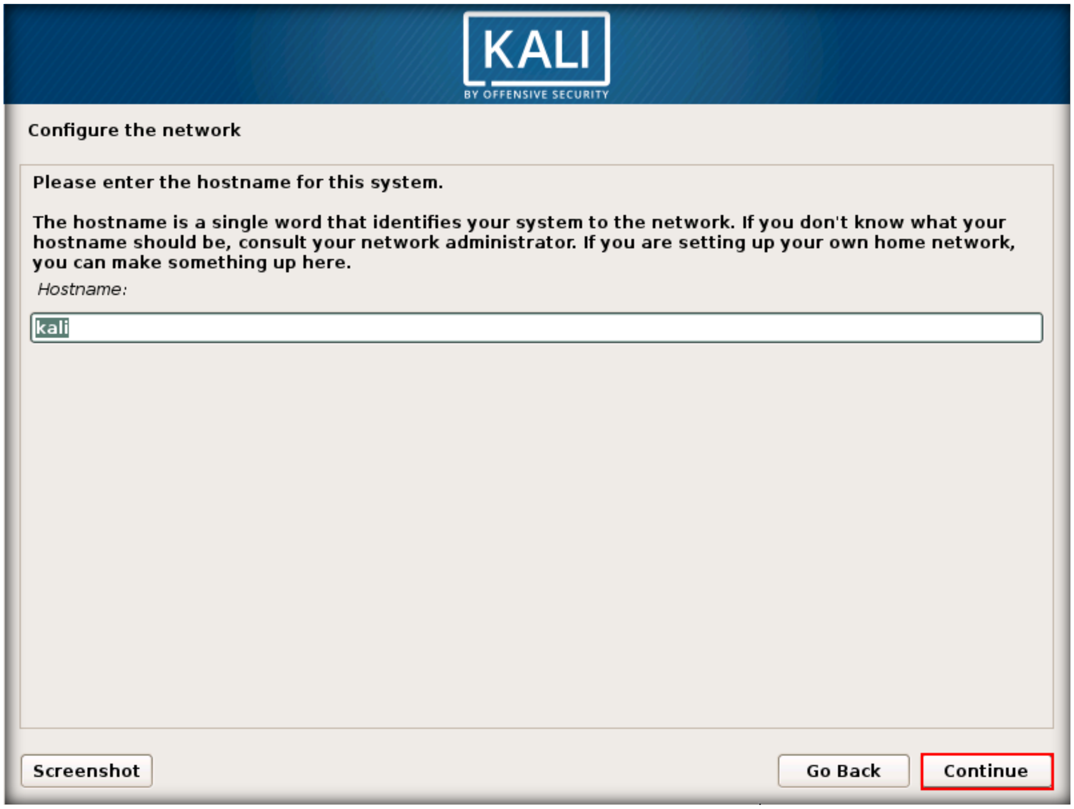


Configure the keyboard

Keymap to use:

American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian (BDS layout)
Bulgarian (phonetic layout)
Burmese
Canadian French
Canadian Multilingual
Catalan

22. **Configure the network** section appears, leave the Hostname to default and click **Continue.**



Configure the network

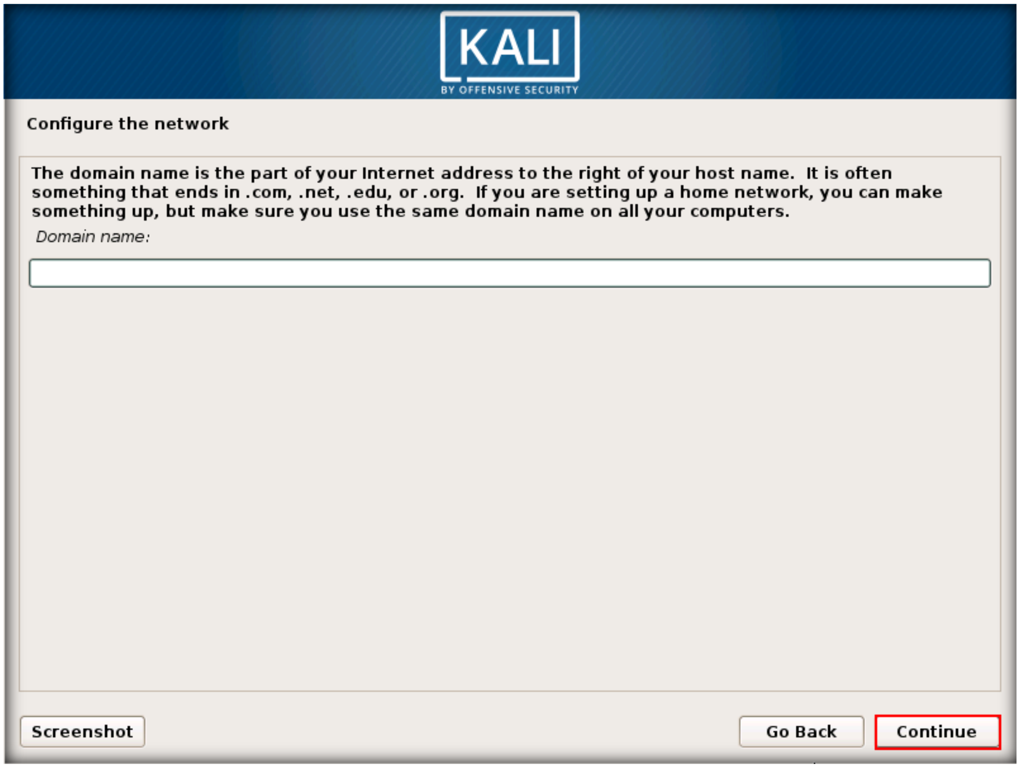
Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

kali

23. **Configure the network** section appears, leave the Domain name: field blank and click **Continue.**

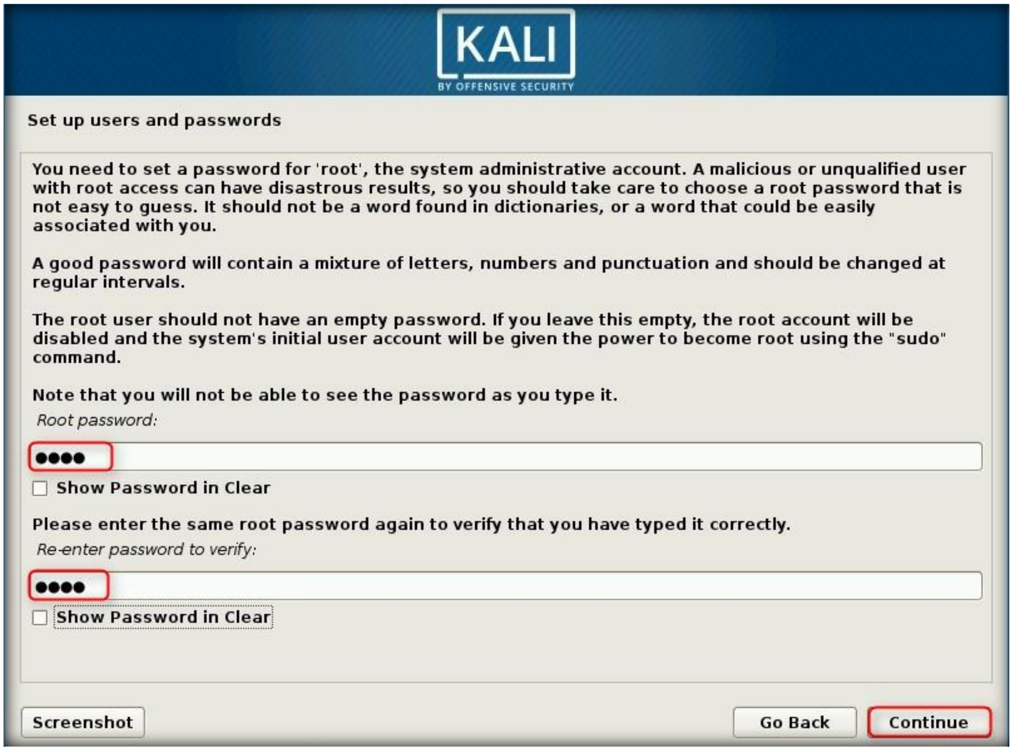


Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

24. **Set up users and passwords** section appears, enter **toor** in both the **Root password** as well as **re-enter password to verify** fields and click **Continue.**



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

●●●●

□ Show Password in Clear

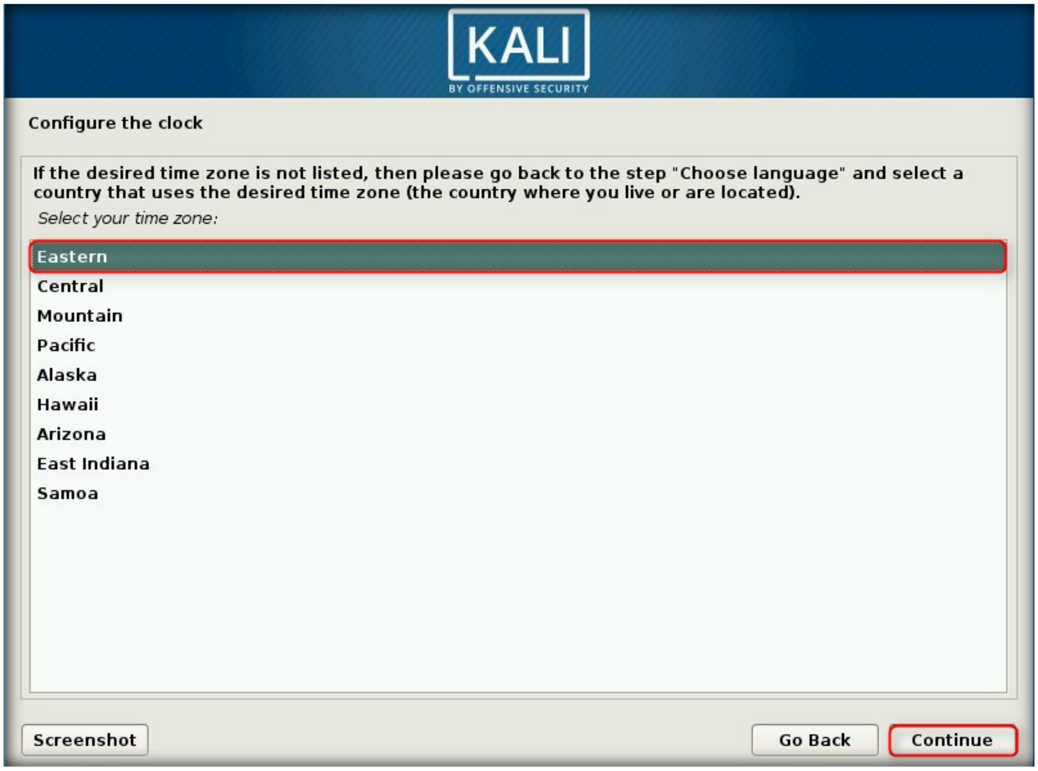
Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●

□ Show Password in Clear

25. In **Configure the clock** window, choose the time zone (here, **Eastern**) and click **Continue Wait** until the installer fetches time from the network time server.



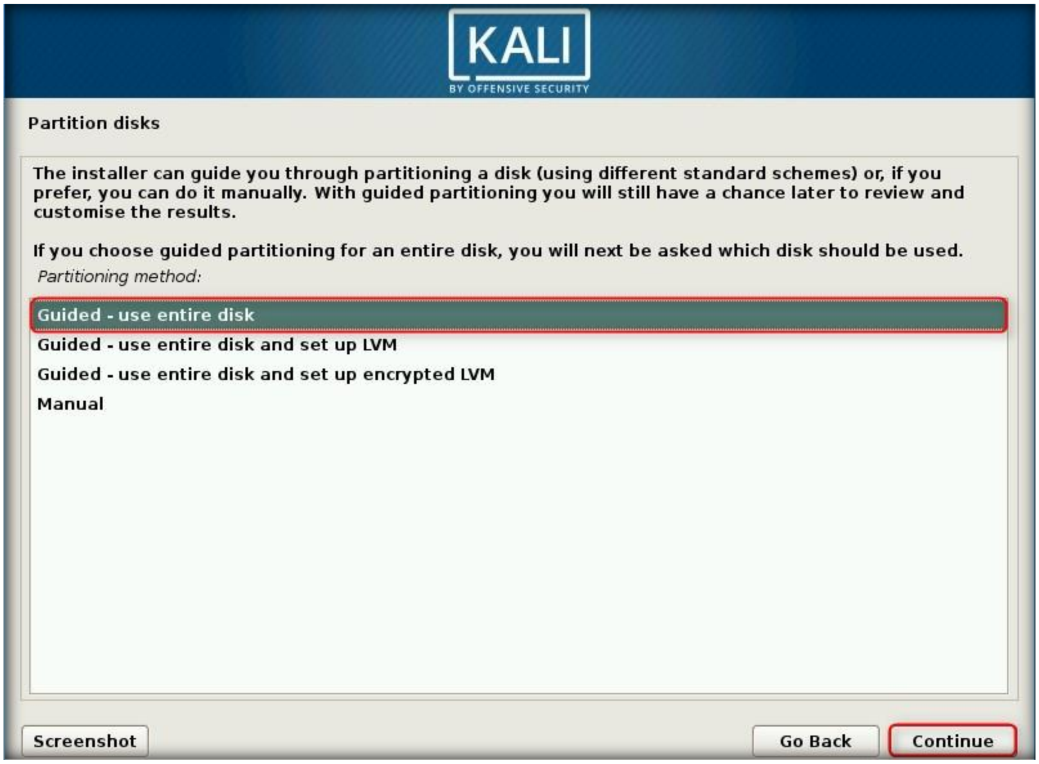
Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa

26. **Partition disks** window appears, choose the Partitioning method: **Guided – use entire disk** and click **Continue**.



Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

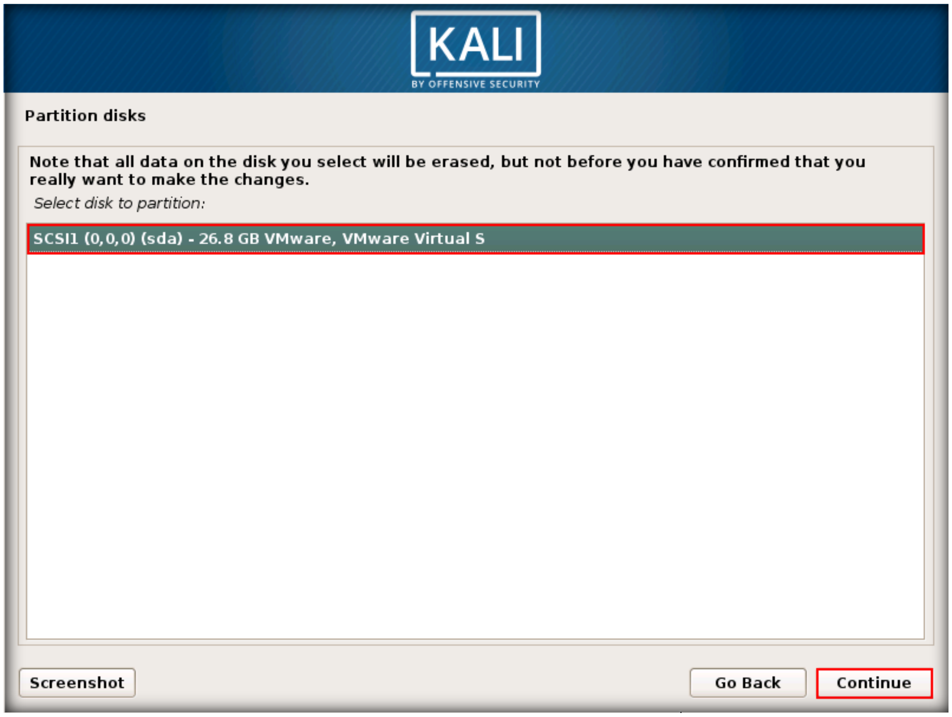
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual

27. Another **Partition disks** window appears, select the disk **SCSI1 (0,0,0) (sda) – 26.8 GB VMware, VMware Virtual S** and click **Continue.**

Note: The size of the disk (**26.8 GB**) may vary in your lab environment.



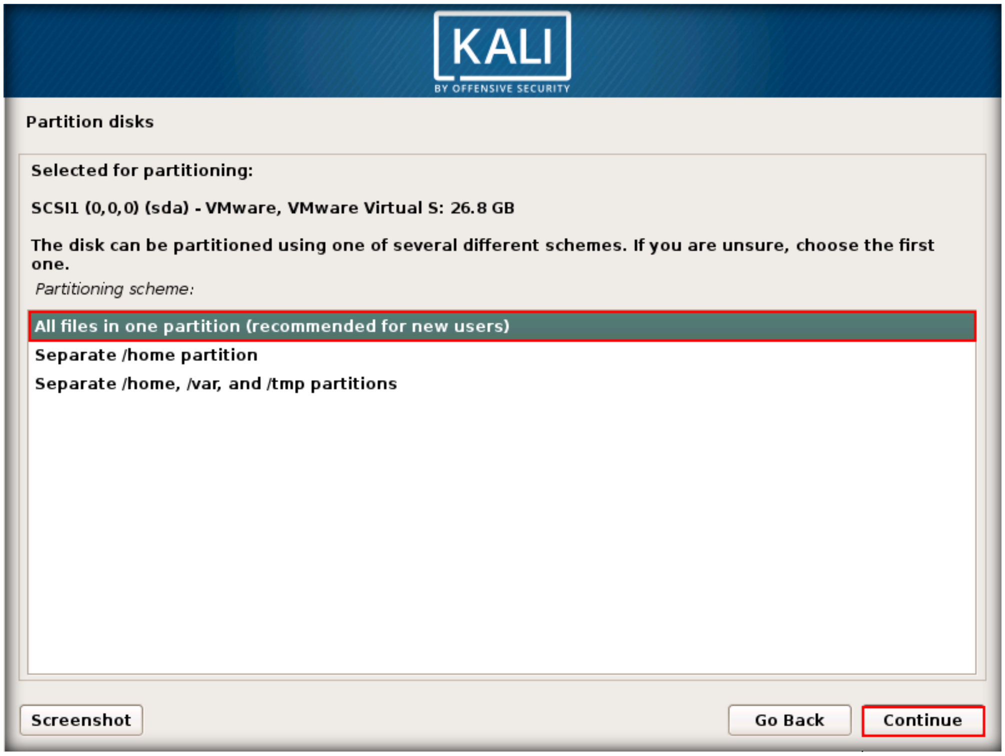
Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

SCSI1 (0,0,0) (sda) - 26.8 GB VMware, VMware Virtual S

28. In the **Partition disks** window, choose the Partitioning scheme: **All files in one partition (recommended for new users)** and click **Continue**.



Partition disks

Selected for partitioning:

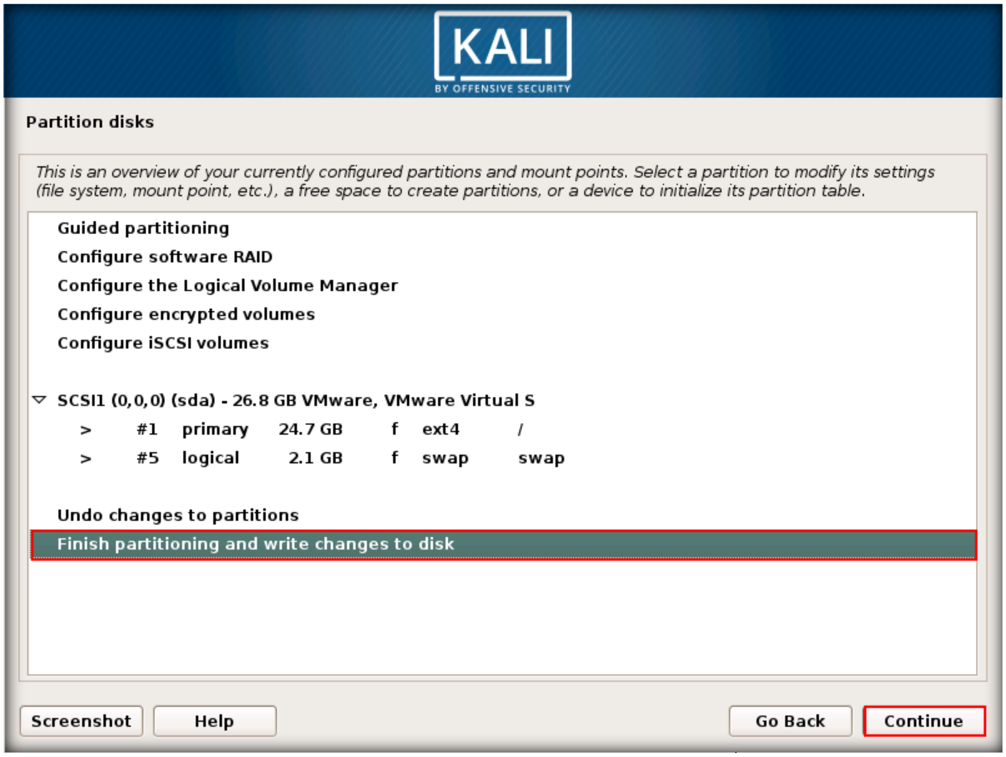
SCSI1 (0,0,0) (sda) - VMware, VMware Virtual S: 26.8 GB

The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

Partitioning scheme:

All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions

29. **Partition disks** window appears displaying the overview of your currently configured partitions, choose **Finish partitioning and write changes to disk** and click **Continue**.

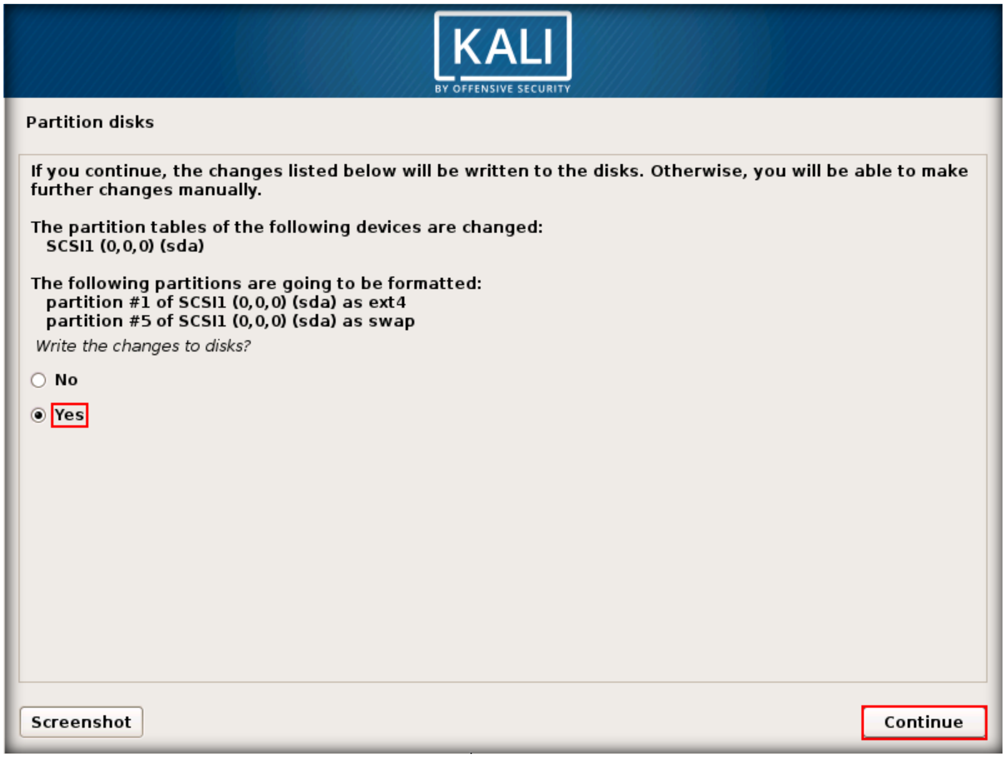


Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

```
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

▽ SCSI1 (0,0,0) (sda) - 26.8 GB VMware, VMware Virtual S
     >    #1   primary   24.7 GB    f   ext4     /
     >    #5   logical    2.1 GB    f   swap     swap

Undo changes to partitions
Finish partitioning and write changes to disk
```

30. A **Partition disks** window appears stating that the changes will be written to the disk, select **Yes** and click **Continue**.



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
  SCSI1 (0,0,0) (sda)

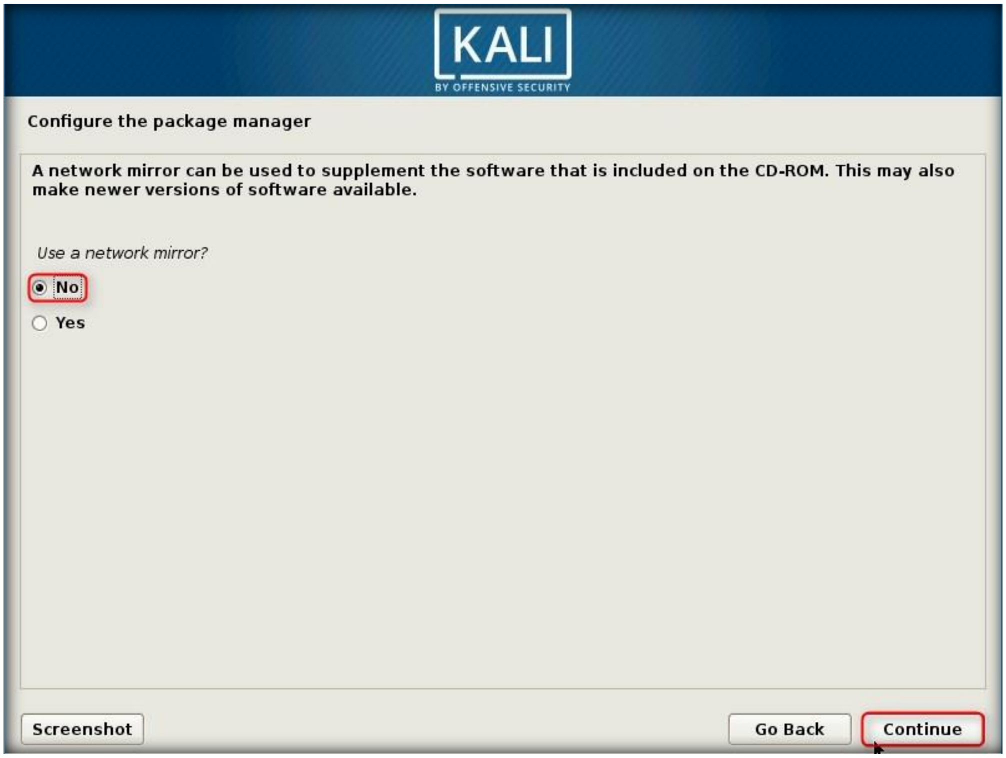
The following partitions are going to be formatted:
  partition #1 of SCSI1 (0,0,0) (sda) as ext4
  partition #5 of SCSI1 (0,0,0) (sda) as swap

Write the changes to disks?

○ No

● Yes

31. On completion of installation, **Configure the package manager** window appears, select **No** and click **Continue**.



Configure the package manager

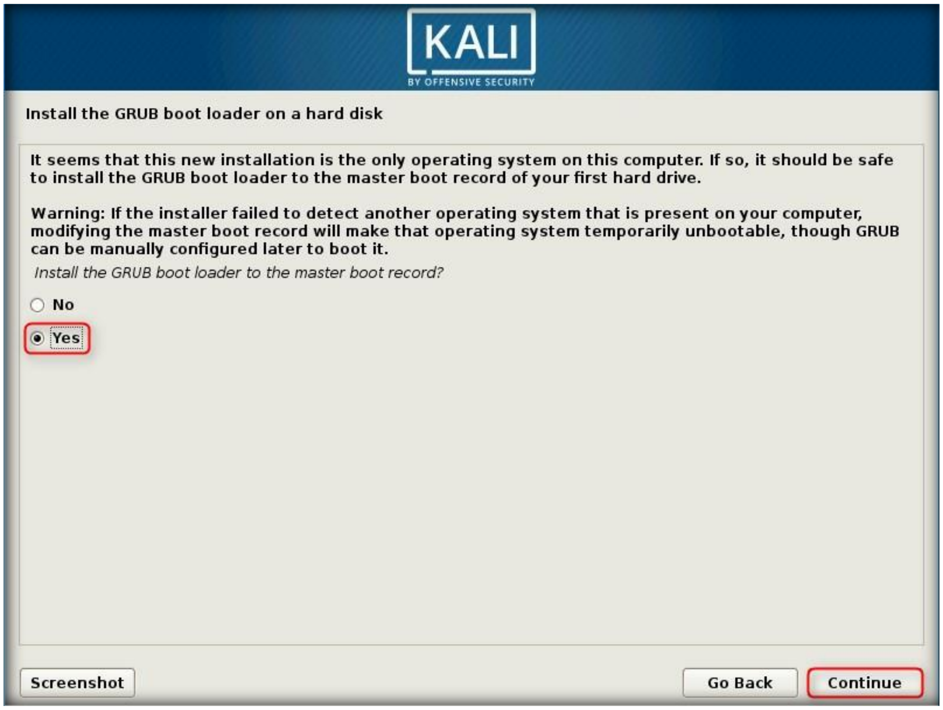
A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.

Use a network mirror?

● No

○ Yes

32. Install the GRUB boot loader on a hard disk window appears, select Yes in order to install the GRUB boot loader to the master boot record and click **Continue**.



Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

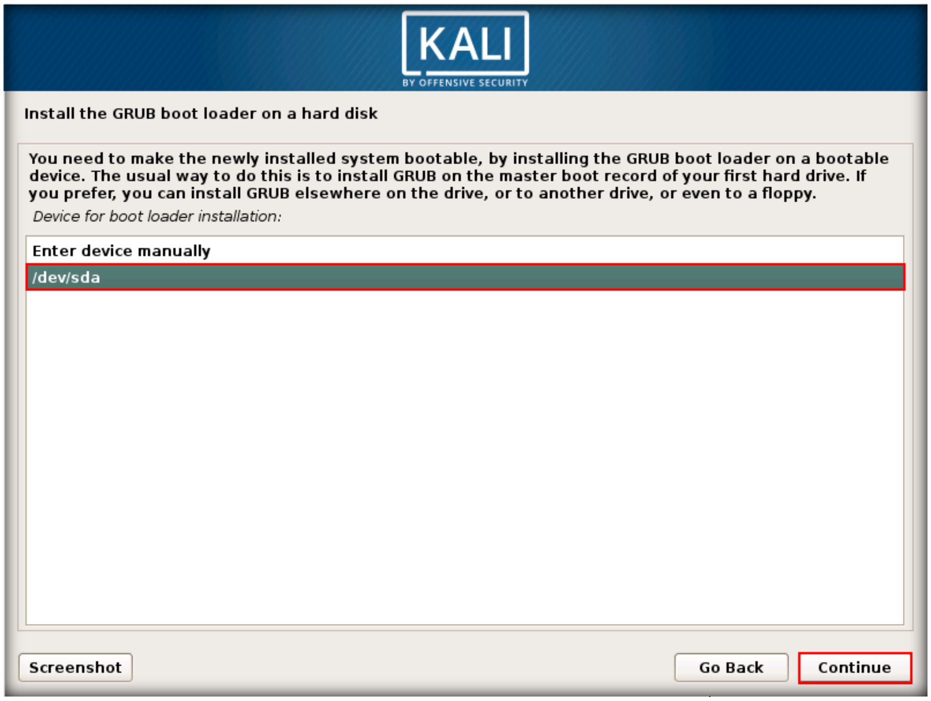
Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

○ No

● Yes

33. Select the available device in Device for boot loader installation (here, **/dev/sda**) and click **Continue**. Wait until the GRUB boot loader is installed.



Install the GRUB boot loader on a hard disk

You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB on the master boot record of your first hard drive. If you prefer, you can install GRUB elsewhere on the drive, or to another drive, or even to a floppy.

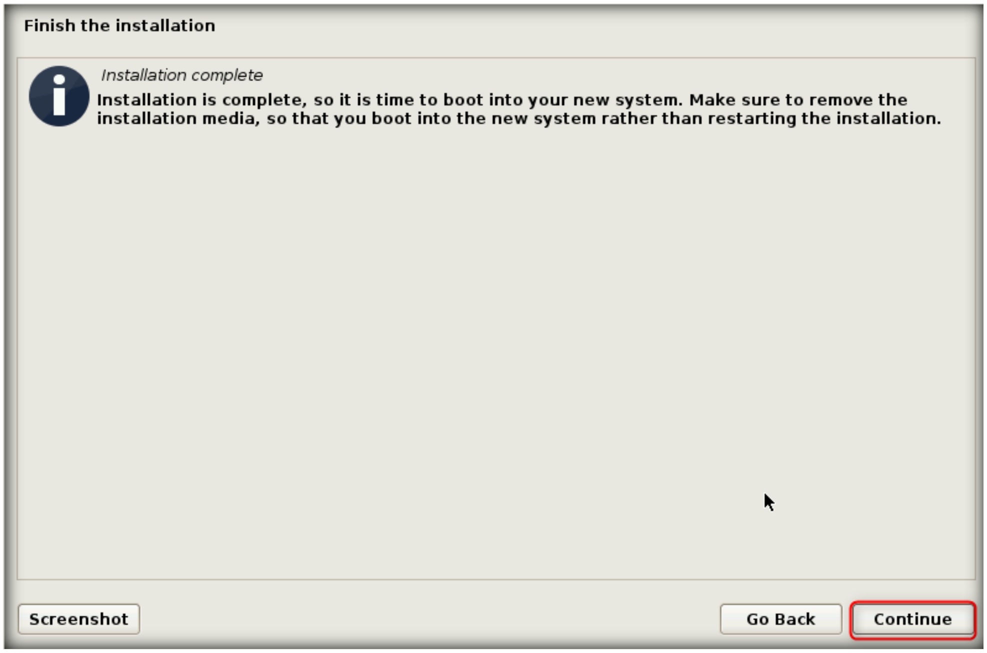
Device for boot loader installation:

Enter device manually

/dev/sda

34. Wait until the partitions are formatted and the operating system is installed.

35. It takes some time for the installation to complete. Finish the installation window appears, click **Continue.**

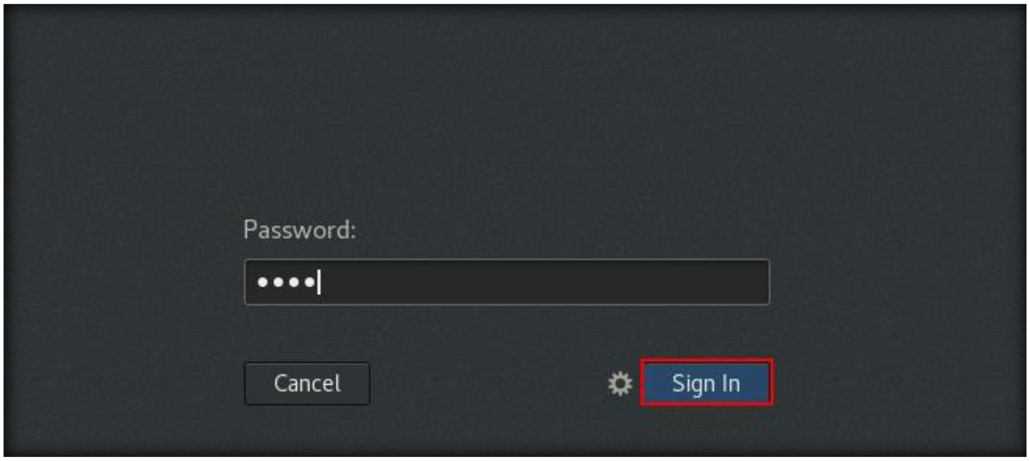


Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.

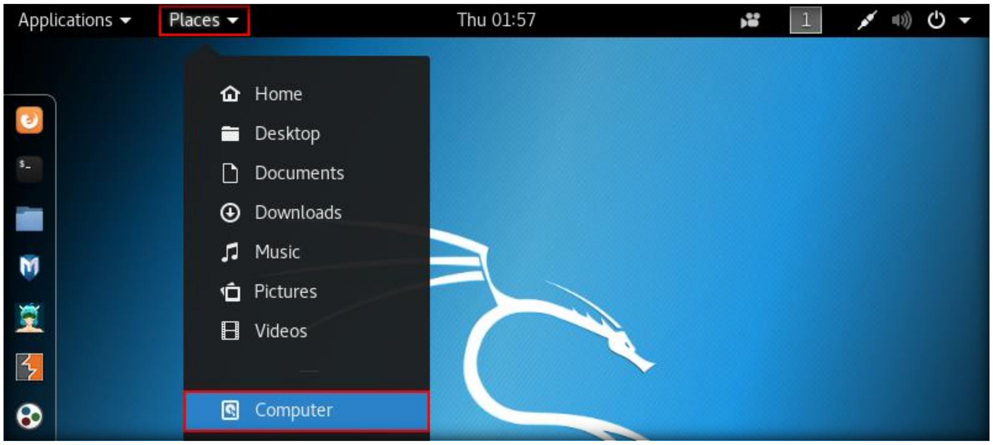
36. Once the installation is finished the machine will get restarted, and after the restart it will come to the login screen. Login to the machine with Username: **root** and Password: **toor**.



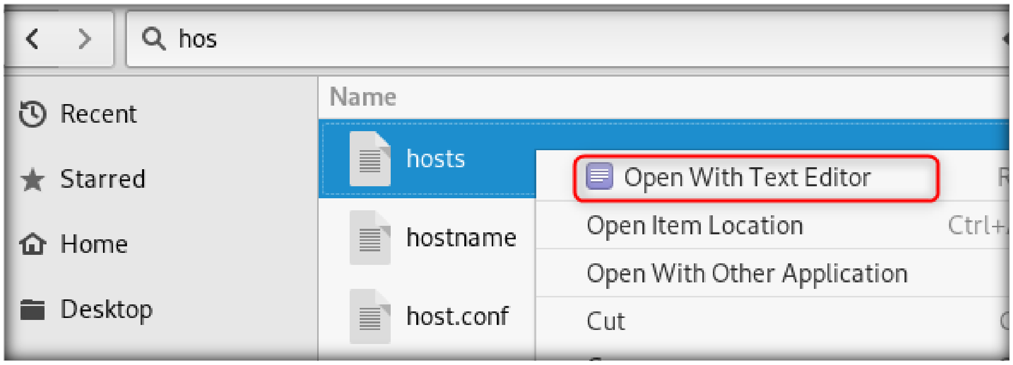
Password: ••••

CT#9.2 Configuring Host File in Kali Linux

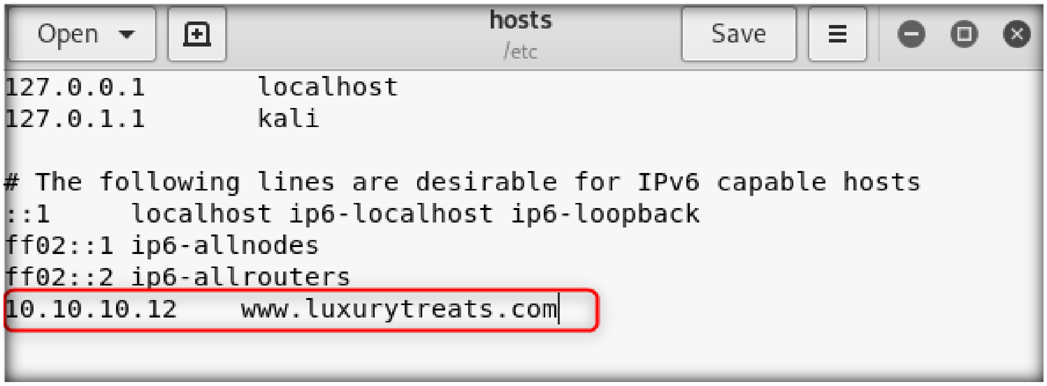
1. To add **www.luxurytreats.com** website to the host file, navigate to **Places → Computer.**



2. Navigate to **etc** folder then search for **hosts** file → right click on file and open with Text Editor.



3. Add IP **10.10.10.12** address and url **www.luxurytreats.com** at the end of the file. Click **Save** close the text editor.

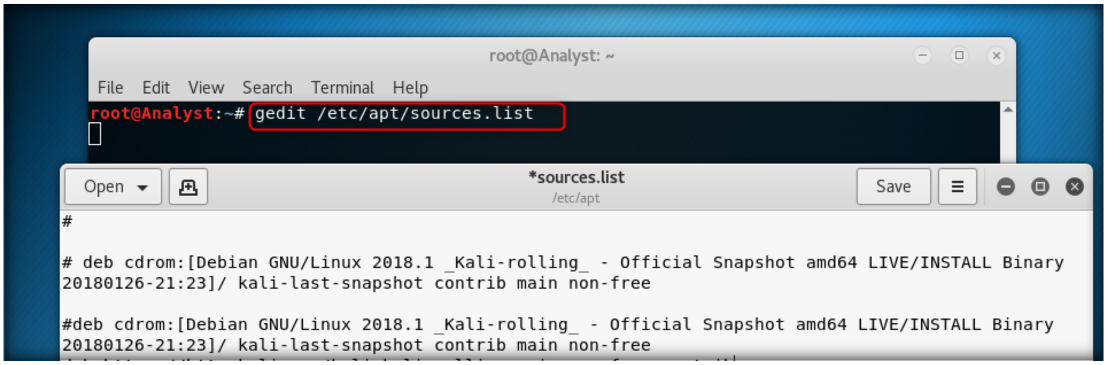


```
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.10.12     www.luxurytreats.com
```

4. Open browser and type www.luxurytreats.com in url and press **Enter**, you will navigate to luxuryTreats website.

CT#9.3 Updating Kali Linux

1. Open **terminal** and type **gedit /etc/apt/sources.list. sources.list** file will open in the **geditor.**



```
root@Analyst:~# gedit /etc/apt/sources.list
```

```
#

# deb cdrom:[Debian GNU/Linux 2018.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary
20180126-21:23]/ kali-last-snapshot contrib main non-free

#deb cdrom:[Debian GNU/Linux 2018.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary
20180126-21:23]/ kali-last-snapshot contrib main non-free
```

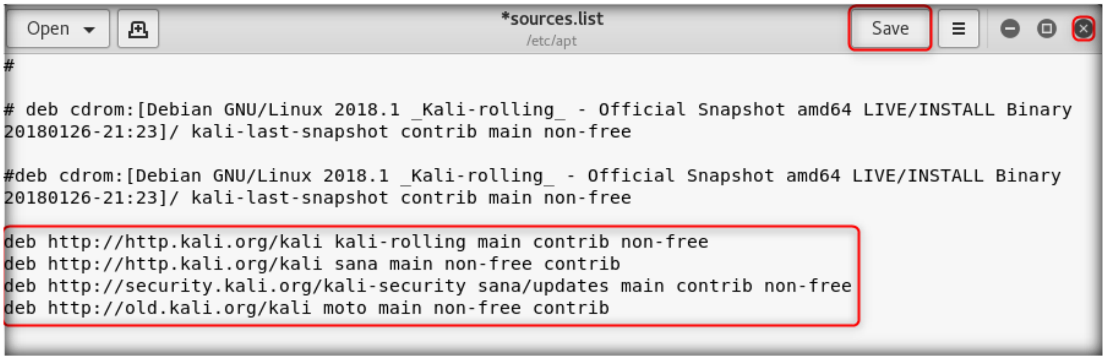
2. Add following line of code at the end of the **sources.list** file. Click **Save** to save the file. close the **sources.list** file.

   deb http://http.kali.org/kali kali-rolling main contrib non-free

   deb http://http.kali.org/kali sana main non-free contrib

   deb http://security.kali.org/kali-security sana/updates main contrib non-free

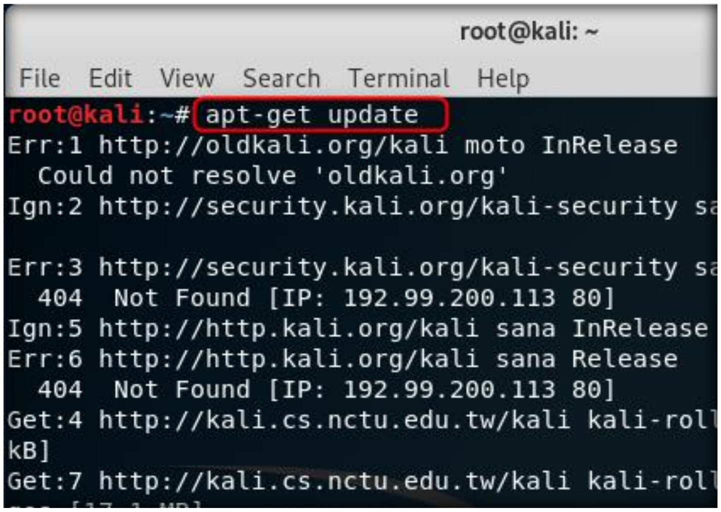
   deb http://old.kali.org/kali moto main non-free contrib



```
#

# deb cdrom:[Debian GNU/Linux 2018.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary
20180126-21:23]/ kali-last-snapshot contrib main non-free

#deb cdrom:[Debian GNU/Linux 2018.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary
20180126-21:23]/ kali-last-snapshot contrib main non-free

deb http://http.kali.org/kali kali-rolling main contrib non-free
deb http://http.kali.org/kali sana main non-free contrib
deb http://security.kali.org/kali-security sana/updates main contrib non-free
deb http://old.kali.org/kali moto main non-free contrib
```

3. Type apt-get update to update the **Kali Linux** virtual machine.

   Note: If not up-to-date, a prompt appears, asking for a user input as **Y/N**. Type **Y** and press **Enter** to continue the process.

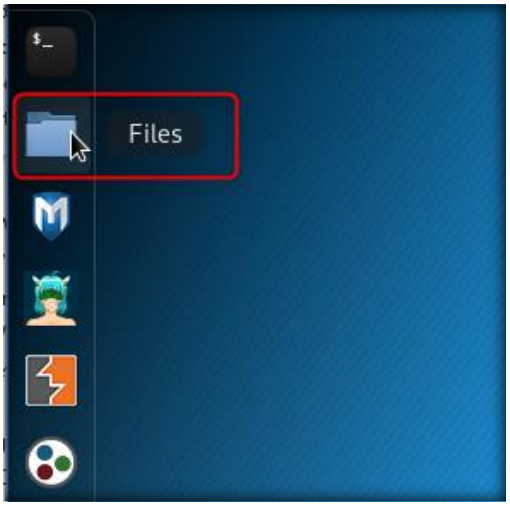


```
root@kali:~# apt-get update
Err:1 http://oldkali.org/kali moto InRelease
  Could not resolve 'oldkali.org'
Ign:2 http://security.kali.org/kali-security sa

Err:3 http://security.kali.org/kali-security sa
  404  Not Found [IP: 192.99.200.113 80]
Ign:5 http://http.kali.org/kali sana InRelease
Err:6 http://http.kali.org/kali sana Release
  404  Not Found [IP: 192.99.200.113 80]
Get:4 http://kali.cs.nctu.edu.tw/kali kali-roll
kB]
Get:7 http://kali.cs.nctu.edu.tw/kali kali-roll
```

4. Type **apt-get install ftp** in terminal and press **Enter** to install **ftp Client**.

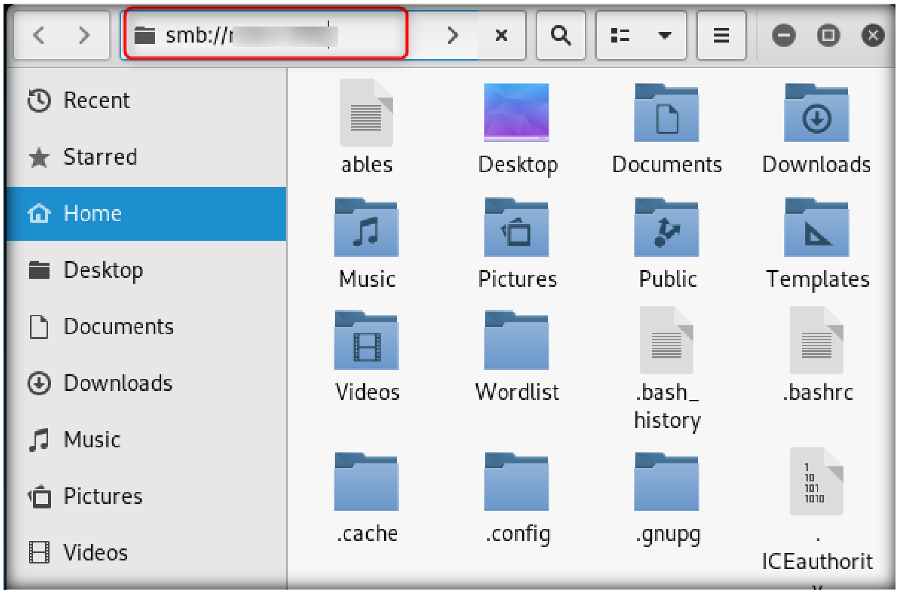
CT#9.4 Sharing SOC-Tools Folder from Host Machine

1. Click Files icon from the taskbar menu as shown in the screenshot.



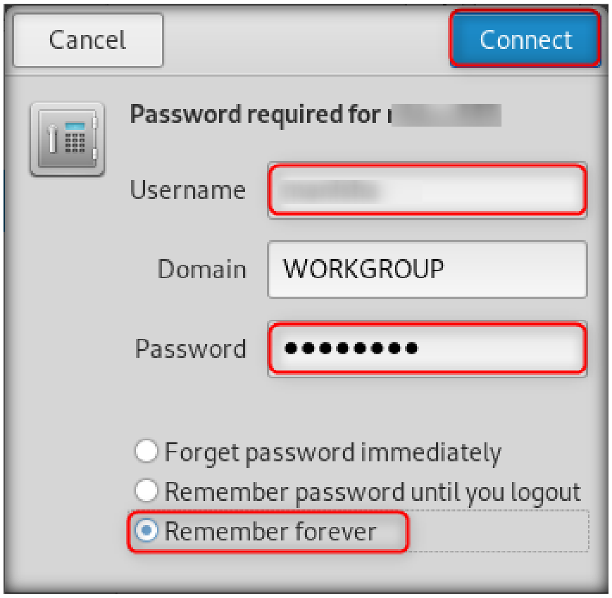
2. In the Explorer window, Press Ctrl + L and type smb://**[IP address of your host machine]** in the address bar and press **Enter**.

   Note: IP address will differ in your lab environment.



smb://[redacted]

3. Password required for [IP address of your host machine] pop-up appears, type credentials of your host machine, select Remember forever radio button and click **Connect.**



Password required for [redacted]

Username [redacted]

Domain WORKGROUP

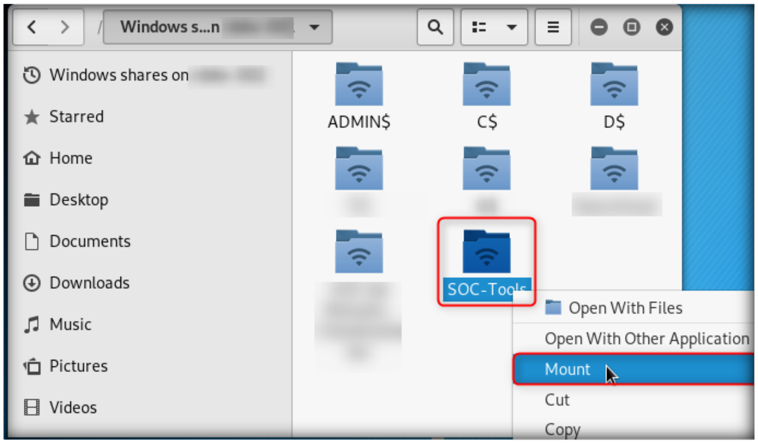
Password ●●●●●●●●●

○ Forget password immediately

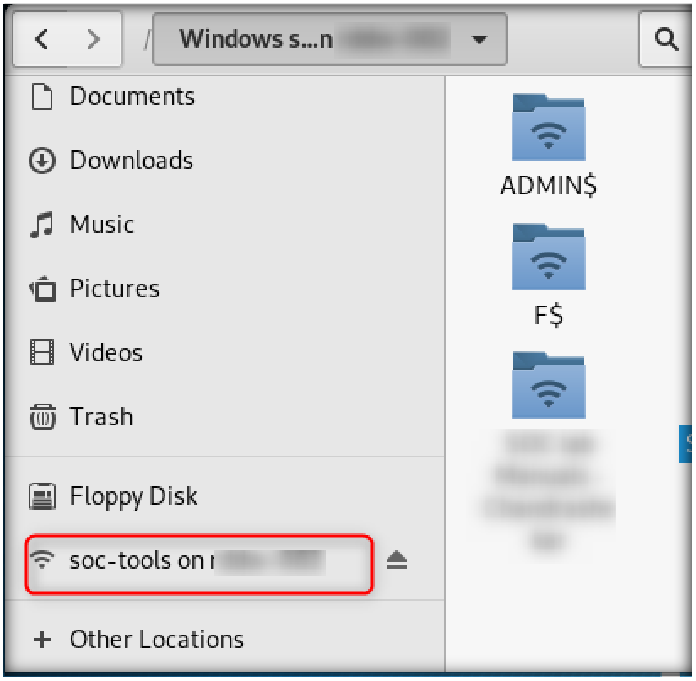
○ Remember password until you logout

● Remember forever

4. Shared SOC-Tools directory appears. Right-click the SOC-Tools directory and click **Mount**.



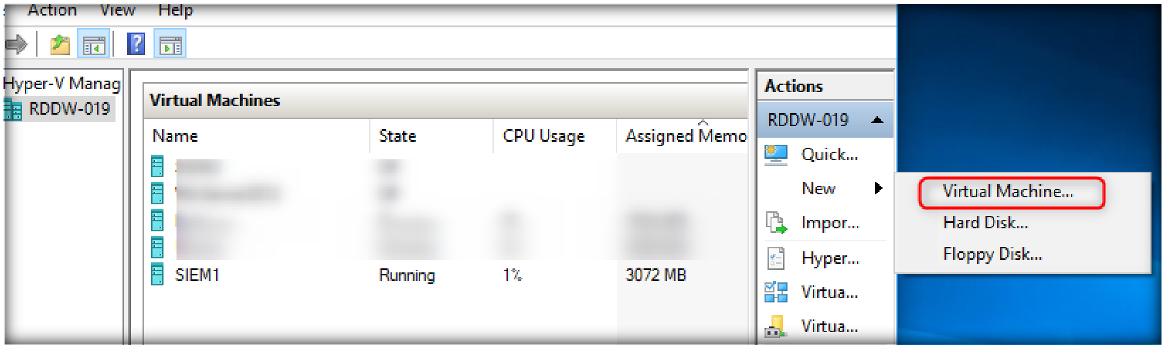
5. Scroll down and you will see host machine's soc-tools shared folder mounted.



CT#10: Installing and Configuring AlienVault OSSIM

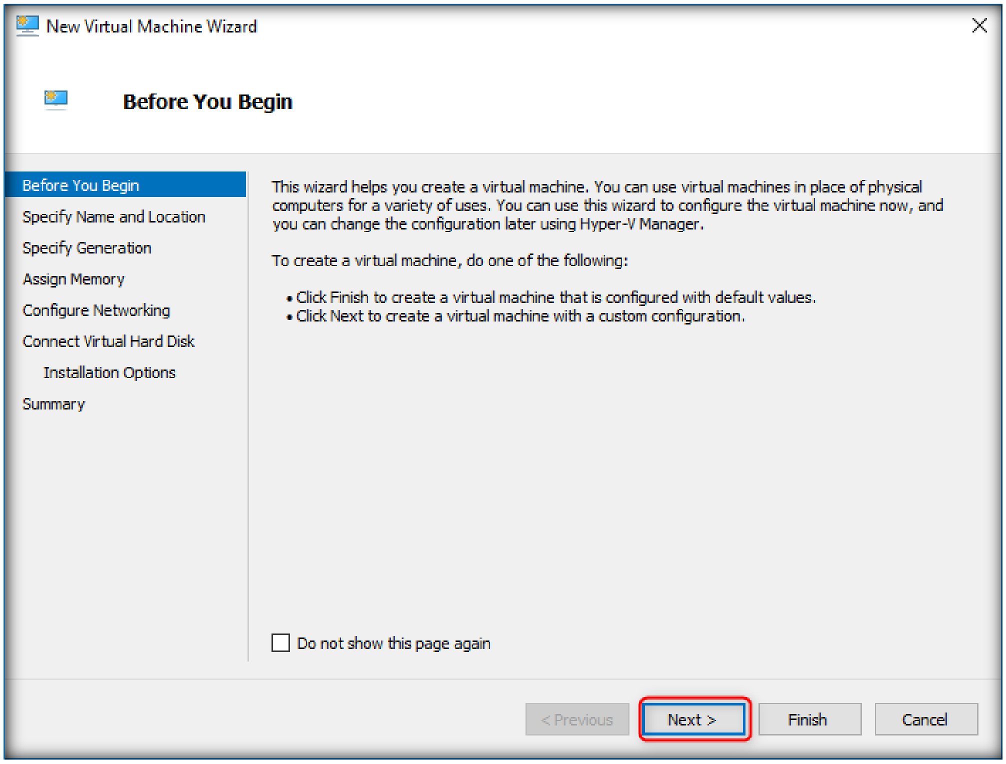
It is recommended that you have a system with at least **16 GB** of RAM. Before starting installation of OSSIM virtual machine, ensure that you have set RAM to **8000 MB**, no. of virtual CPU to 2, network interface to Internal.

1. Launch Hyper-V Manager. If already launched, skip to step two.
2. Select your local machine in the left pane, then click **New**, and then click **Virtual Machine…** in the right pane as shown in the screen shot.



Name	State	CPU Usage	Assigned Memo
SIEM1	Running	1%	3072 MB

3. **New Virtual Machine Wizard** window appears, click **Next** button.



This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

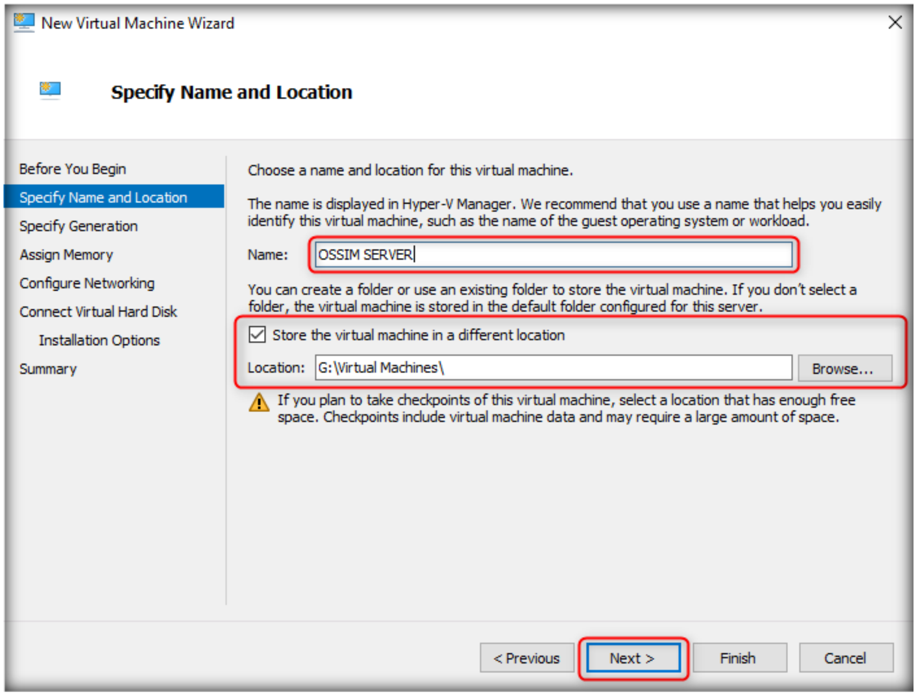
To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

☐ Do not show this page again

4. Specify **Name** and **location** of new virtual machine. Assign the name of the virtual machine as **OSSIM SERVER**. The default location for storing the virtual machine is **C:\ProgramData\Microsoft\Windows\Hyper-V\.** You can choose different location to store the VM's or set it to default location. Click **Next**.

   Note: You can specify the location either in the **Specify Name and Location** section or in the forthcoming **Connect Virtual Hard Disk** section.



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: OSSIM SERVER

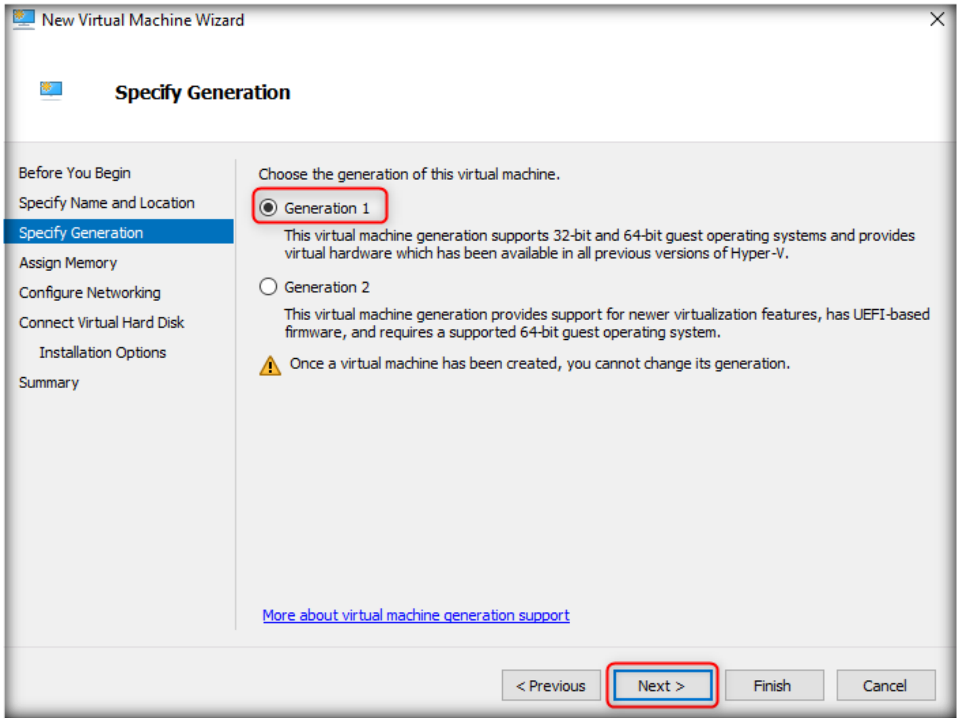
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

Location: G:\Virtual Machines\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

5. Choose the generation of the virtual machine (here, **Generation 1**) and click **Next**.



Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

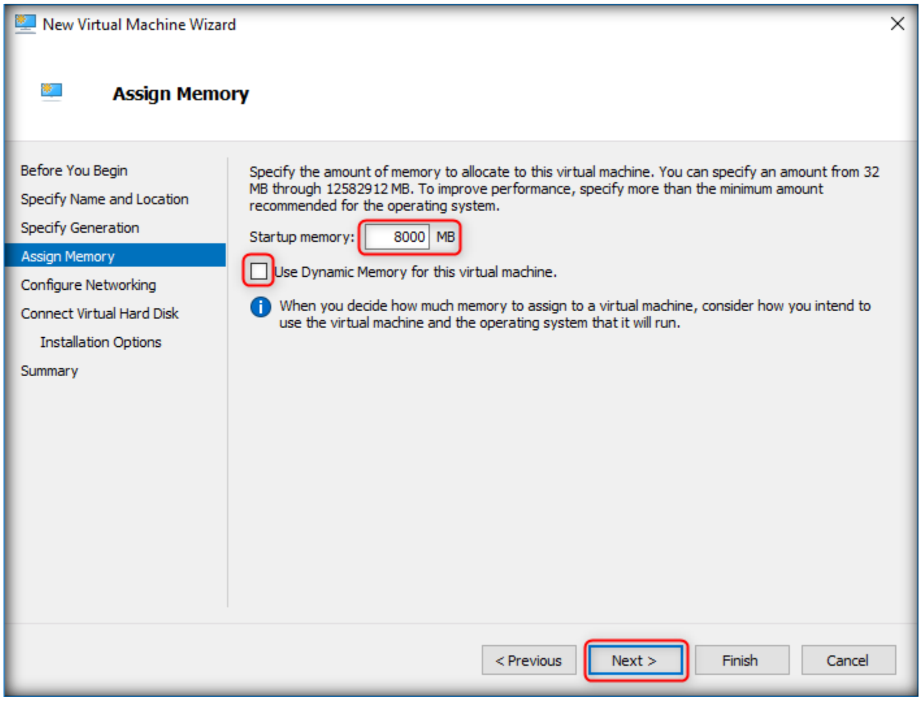
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

Once a virtual machine has been created, you cannot change its generation.

6. Assign the amount of **Startup memory** to allocate to this virtual machine in MB (here, **8000**)

7. Click **Next**.



New Virtual Machine Wizard

Assign Memory

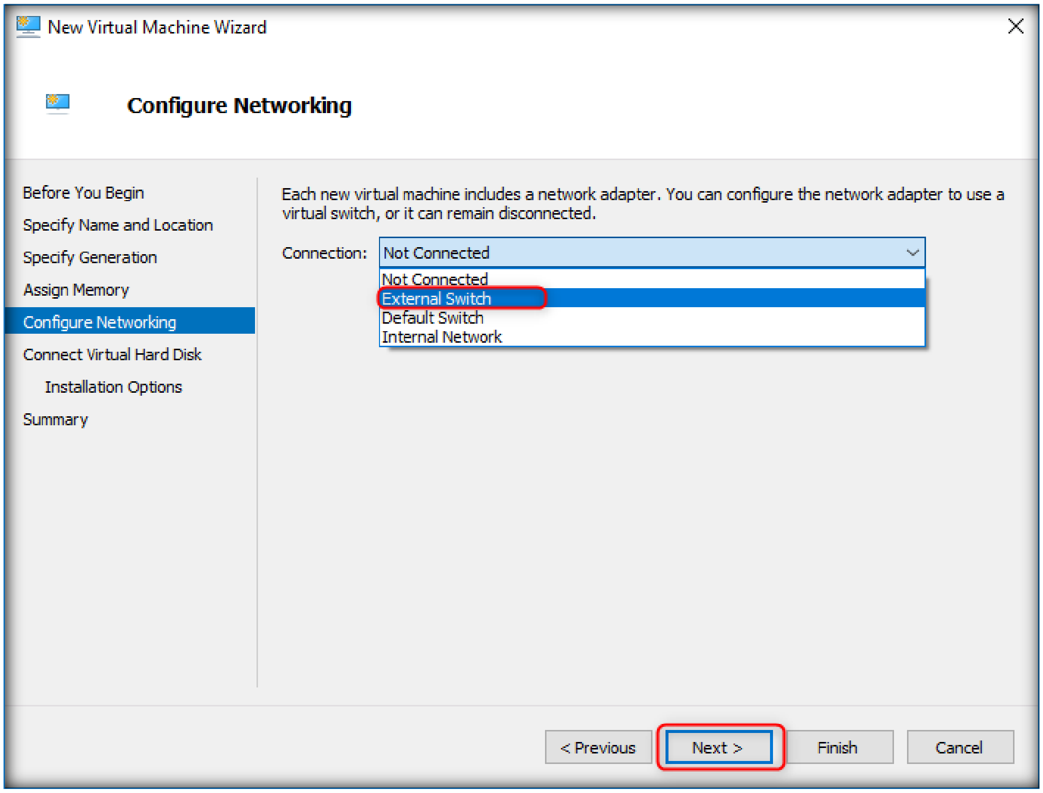
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 8000 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

8. In the next step, select **network adapter** as **Internal Network** from connection drop-down list and click **Next**.



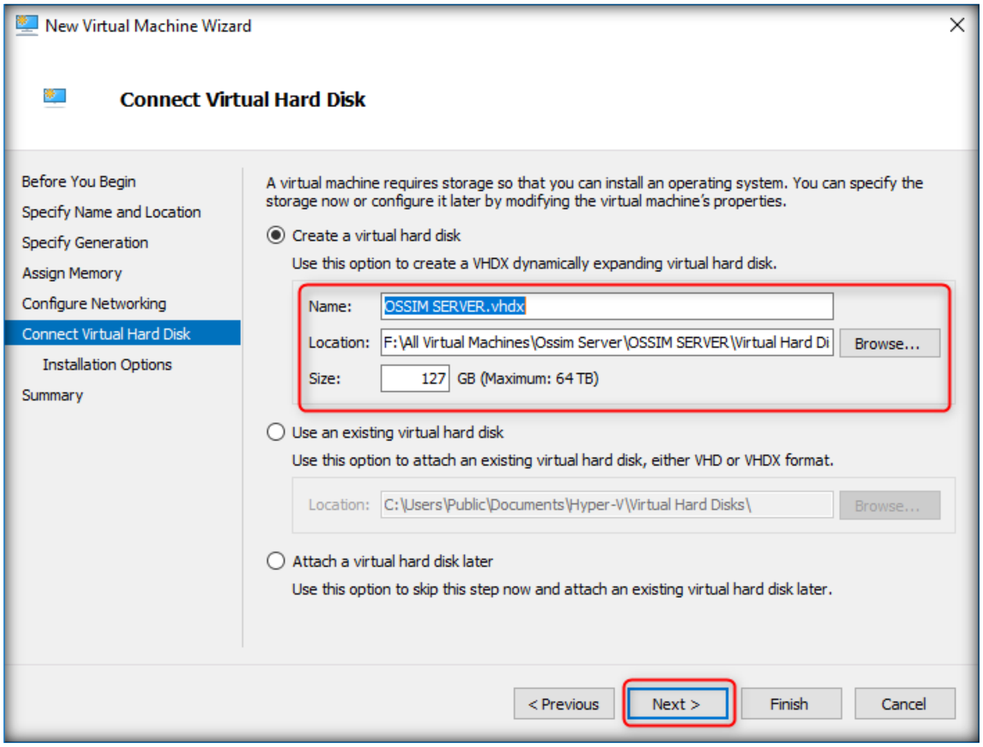
New Virtual Machine Wizard

Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

9. Connect Virtual Hard Disk section appears click **Next**.



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: OSSIM SERVER.vhdx

Location: F:\All Virtual Machines\Ossim Server\OSSIM SERVER\Virtual Hard Di

Size: 127 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

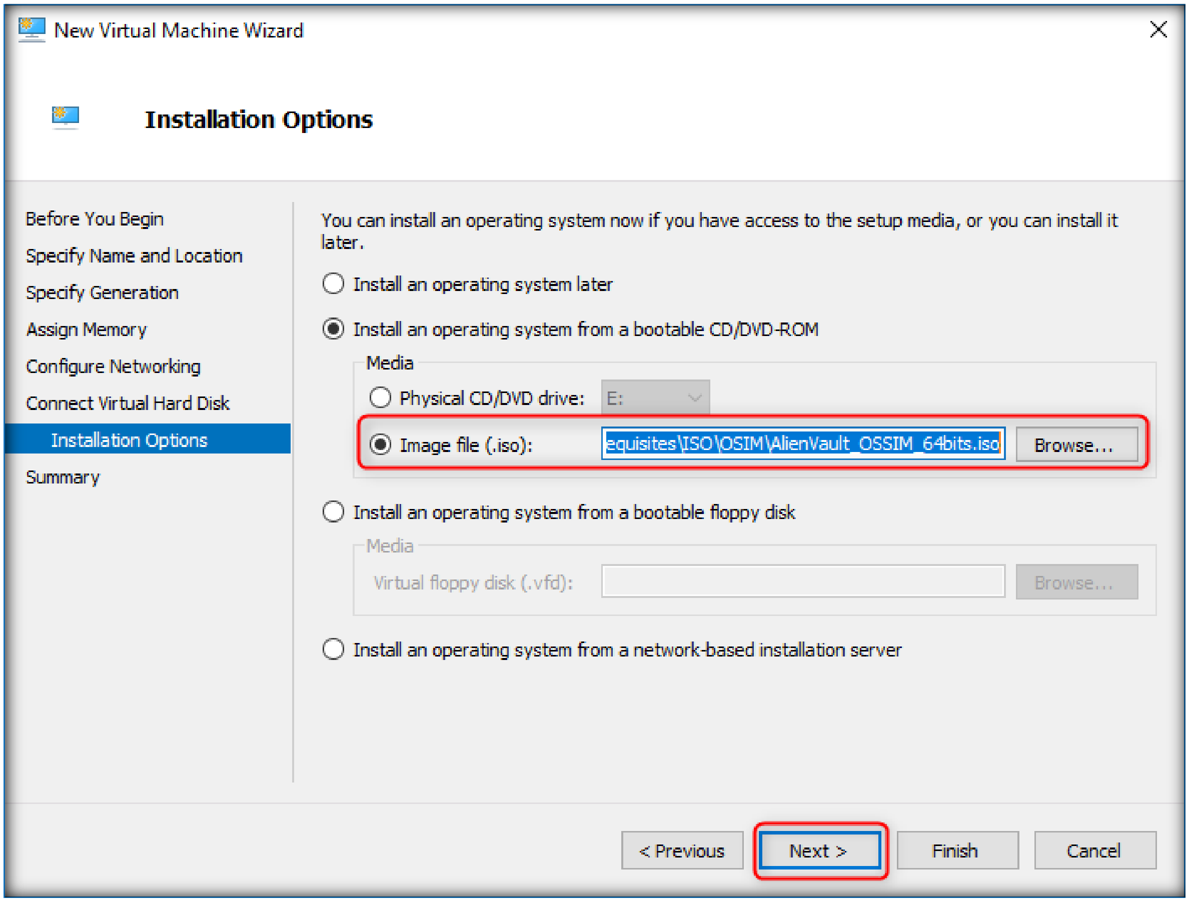
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

10. The **installation options** section appears, select **Install an operating system from a bootable CD/DVD-ROM** radio button.

    - If you have an OSSIM DVD choose Physical CD/DVD drive radio button and then click **Next**.
    - If you have an OSSIM ISO file, then choose Image file (.iso) radio button and click browse button to provide the path of ISO file and click **Next**.



You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a bootable CD/DVD-ROM

Media

○ Physical CD/DVD drive: E:

● Image file (.iso): equisites\ISO\OSIM\AlienVault_OSSIM_64bits.iso Browse...

○ Install an operating system from a bootable floppy disk

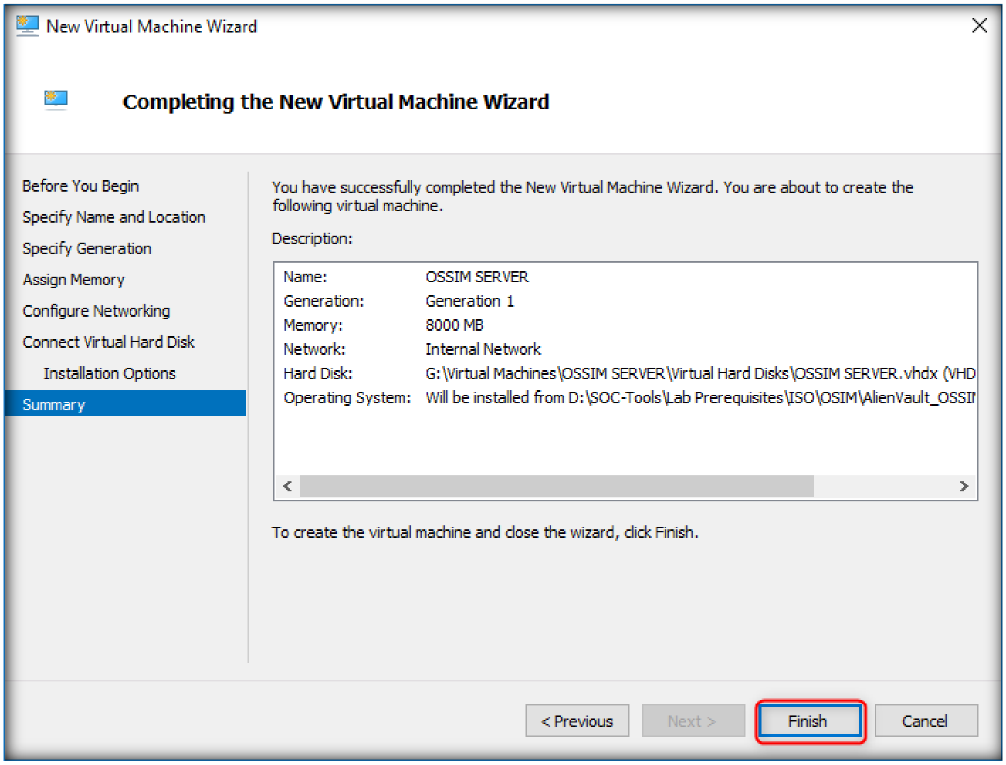
Media

Virtual floppy disk (.vfd): Browse...

○ Install an operating system from a network-based installation server

11. Virtual machine wizard appears with summary information.

12. Click **Finish**.



New Virtual Machine Wizard

Completing the New Virtual Machine Wizard

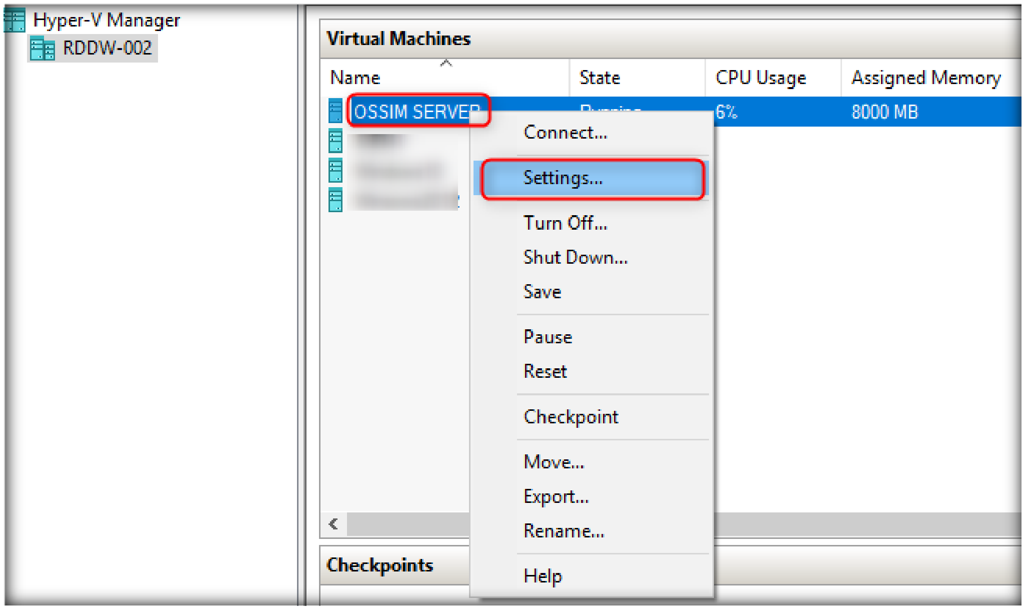
You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name:	OSSIM SERVER
Generation:	Generation 1
Memory:	8000 MB
Network:	Internal Network
Hard Disk:	G:\Virtual Machines\OSSIM SERVER\Virtual Hard Disks\OSSIM SERVER.vhdx (VHD
Operating System:	Will be installed from D:\SOC-Tools\Lab Prerequisites\ISO\OSIM\AlienVault_OSSI

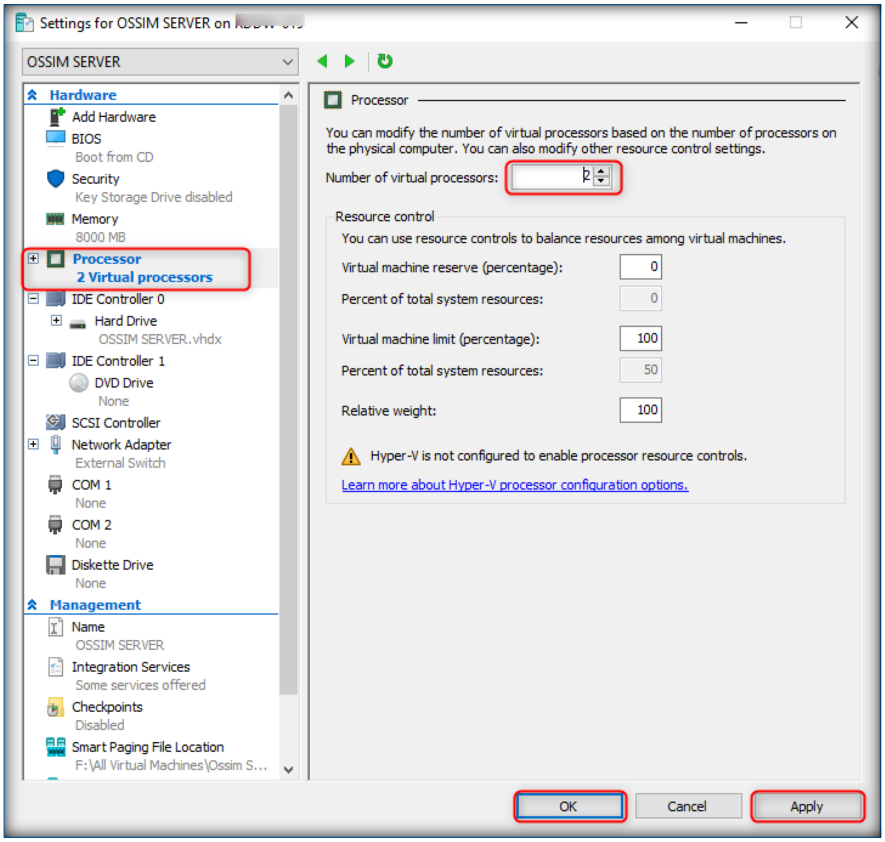
To create the virtual machine and close the wizard, click Finish.

13. In Hyper-V Manager window right-click on created OSSIM virtual machine and click Settings from the context menu.



Name	State	CPU Usage	Assigned Memory
OSSIM SERVER	Running	6%	8000 MB

14. Settings for OSSIM SERVER window appears, click **Processor** from left pane and type **2** in Number of virtual processors field, and click **Apply** and then **OK**.



Settings for OSSIM SERVER on [redacted]

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 2

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 0

Percent of total system resources: 0

Virtual machine limit (percentage): 100

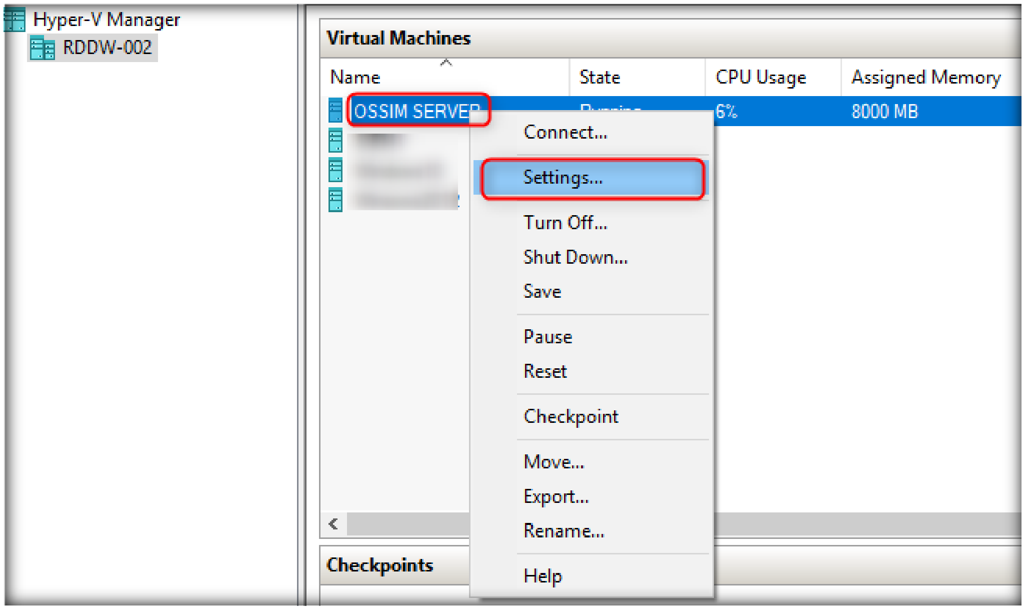
Percent of total system resources: 50

Relative weight: 100

Hyper-V is not configured to enable processor resource controls.

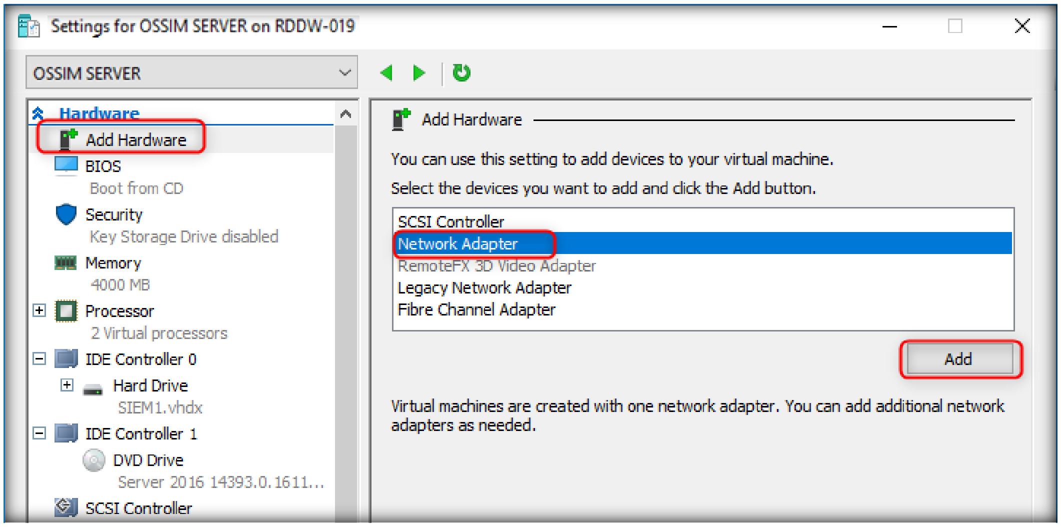
Learn more about Hyper-V processor configuration options.

15. In Hyper-V Manager window right-click on created OSSIM virtual machine and click Settings from the context menu.



Name	State	CPU Usage	Assigned Memory
OSSIM SERVER	Running	6%	8000 MB
[redacted]			
[redacted]			
[redacted]			

16. Click **Add Hardware** Select **Network Adapter** Click **Add** button.



Settings for OSSIM SERVER on RDDW-019

OSSIM SERVER

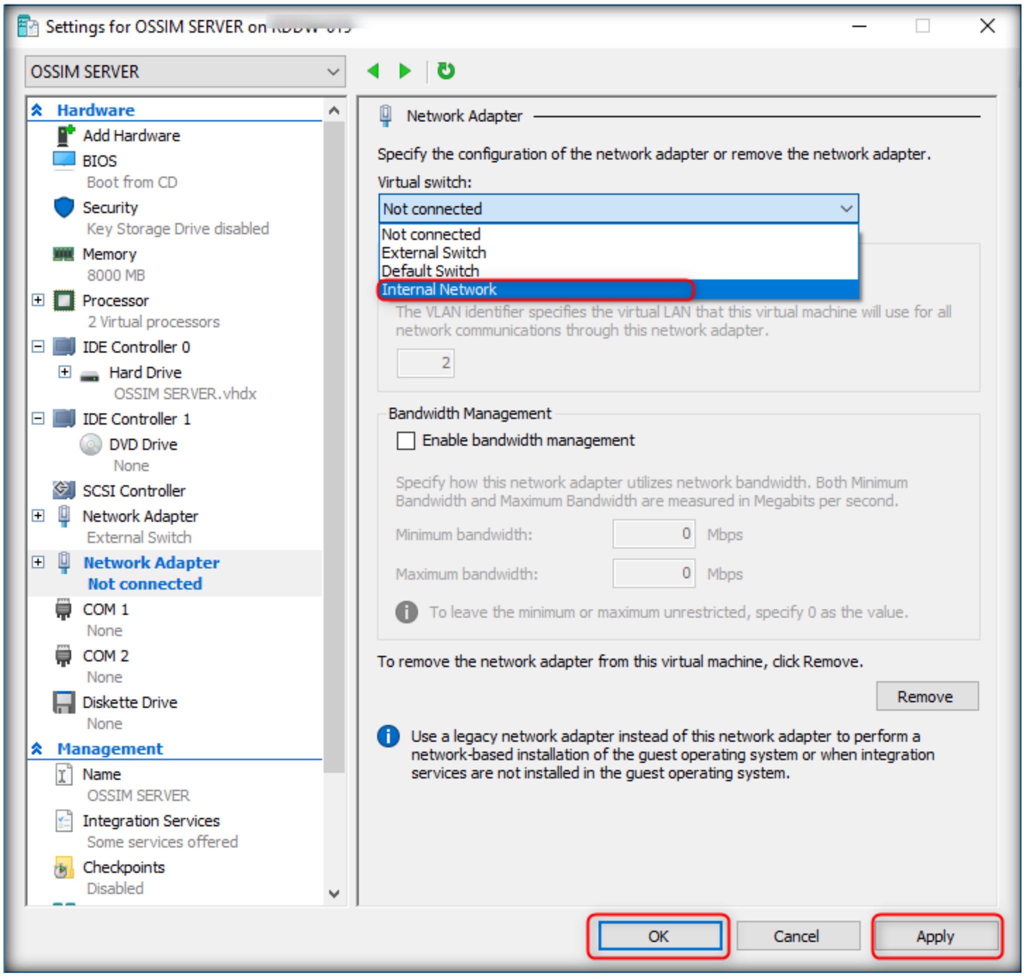
Add Hardware

You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

Virtual machines are created with one network adapter. You can add additional network adapters as needed.

17. Select **Network Adapter** select **External Network**.



Settings for OSSIM SERVER on

OSSIM SERVER

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch:

Not connected

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

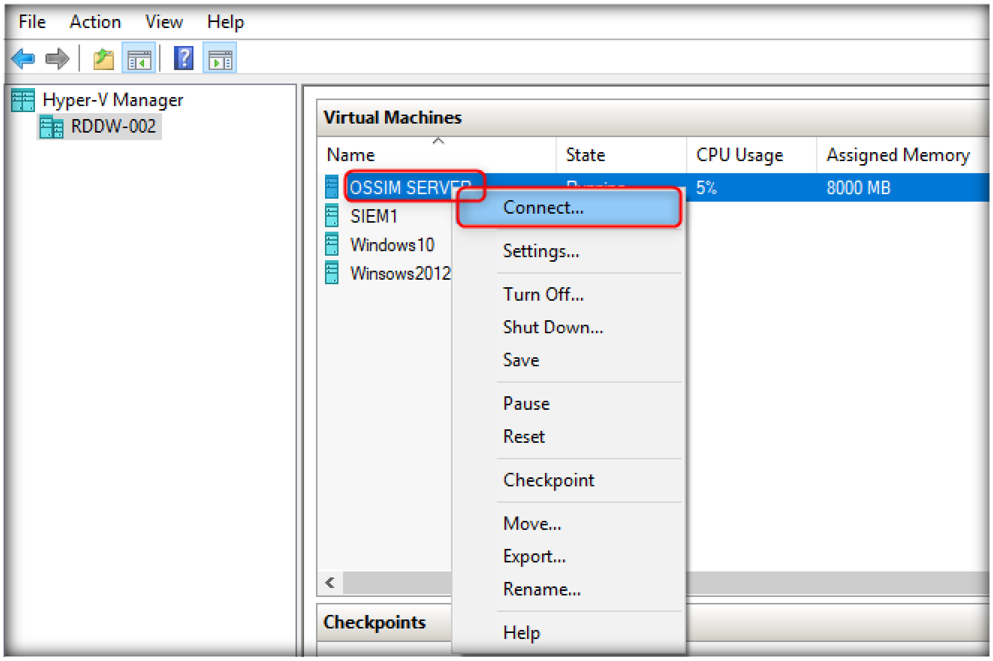
Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

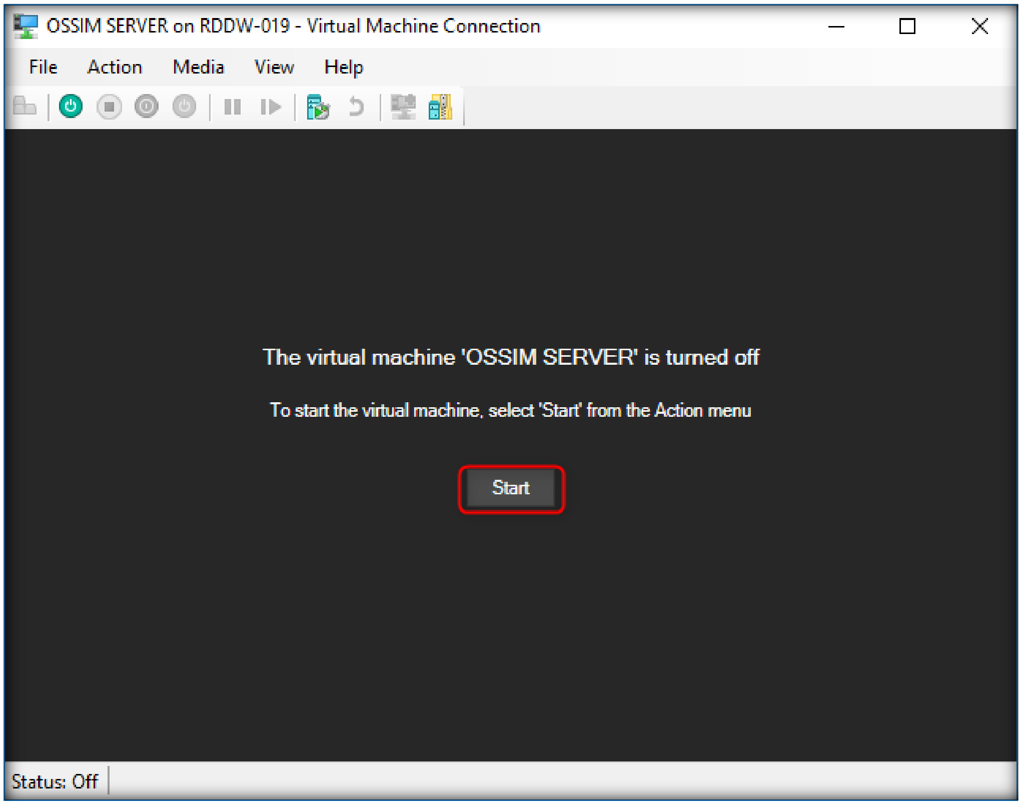
To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

18. In **Hyper-V Manager** main window, right-click on **OSSIM** newly created virtual machine and click **Connect** from the context menu.



19. OSSIM Virtual Machine window appears click **Start** button as shown in the screenshot.



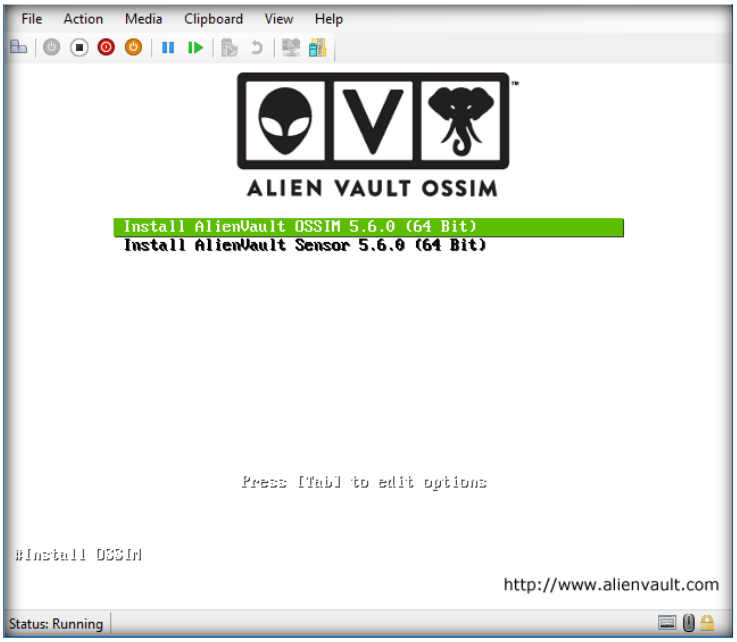
The virtual machine 'OSSIM SERVER' is turned off

To start the virtual machine, select 'Start' from the Action menu

20. OSSIM virtual machine starts booting with the provided source.

21. ALIEN VAULT OSSIM setup wizard appears, choose **AlienVault OSSIM 5.6.0 (64 Bit)** option and press **Enter**.

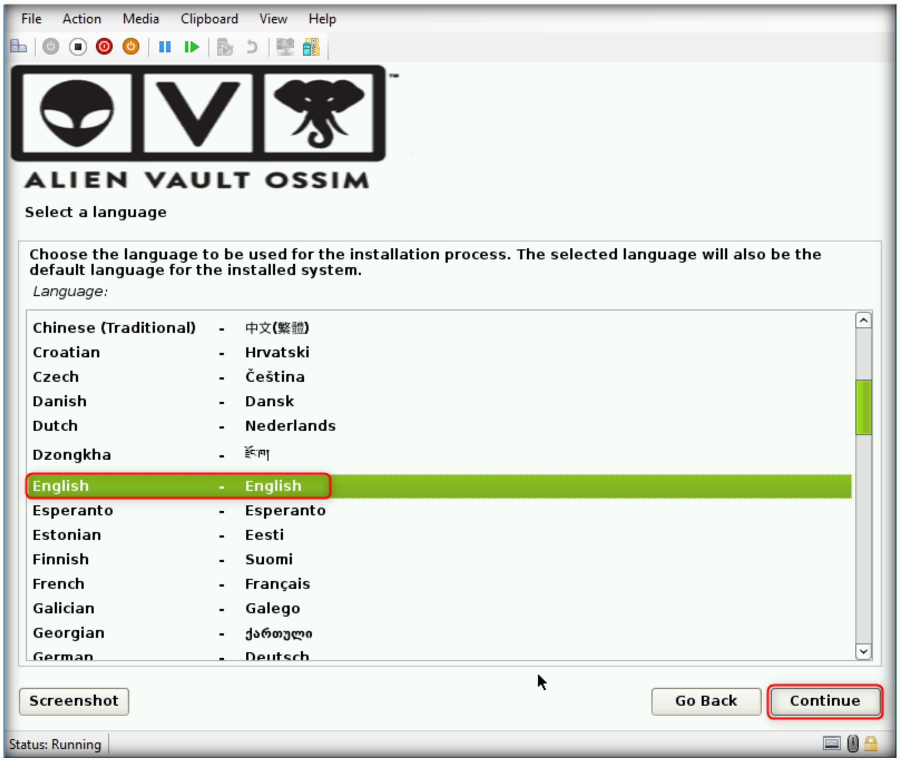
    Note: The screenshots might differ if you have downloaded the latest version of AlienVault OSSIM.



```
Install AlienVault OSSIM 5.6.0 (64 Bit)
Install AlienVault Sensor 5.6.0 (64 Bit)

Press [Tab] to edit options

#Install OSSIM
```

http://www.alienvault.com

22. Select a language screen appears. Select your language and click **Continue**.



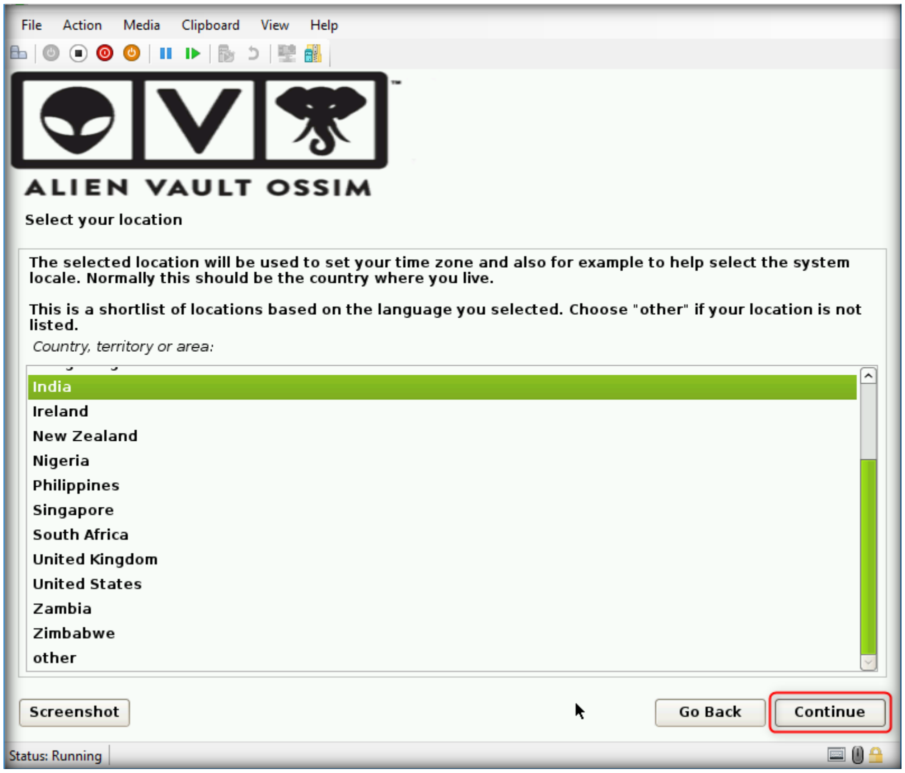
Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

23. Select your location screen appears. Select your country and click **Continue**.



Select your location

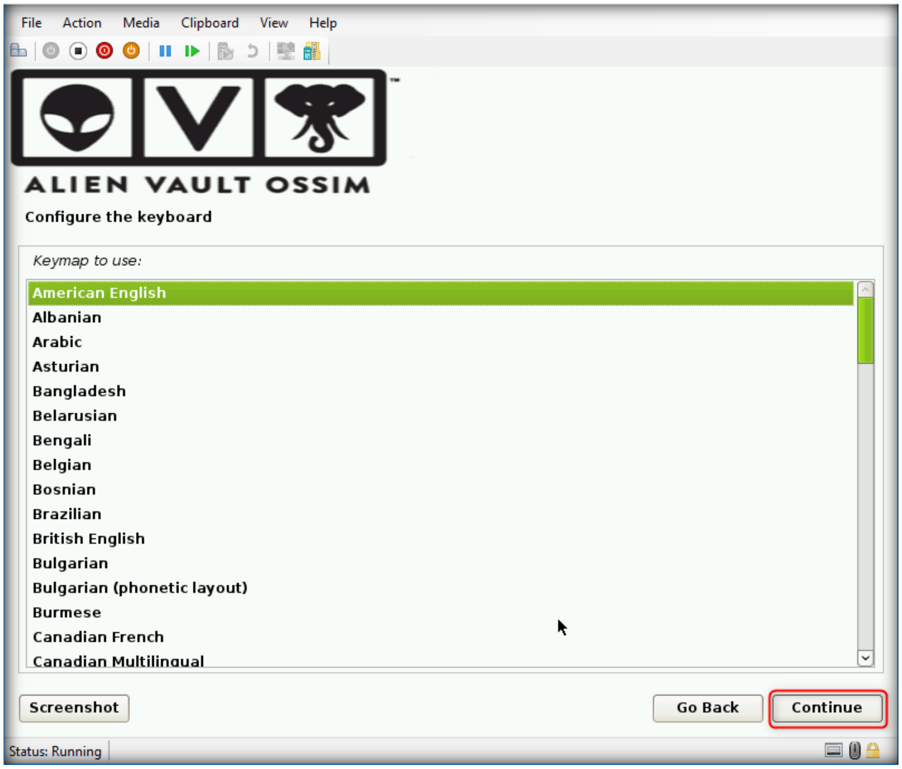
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

24. Configure the keyboard window appears. Select your preferred language and click **Continue**.



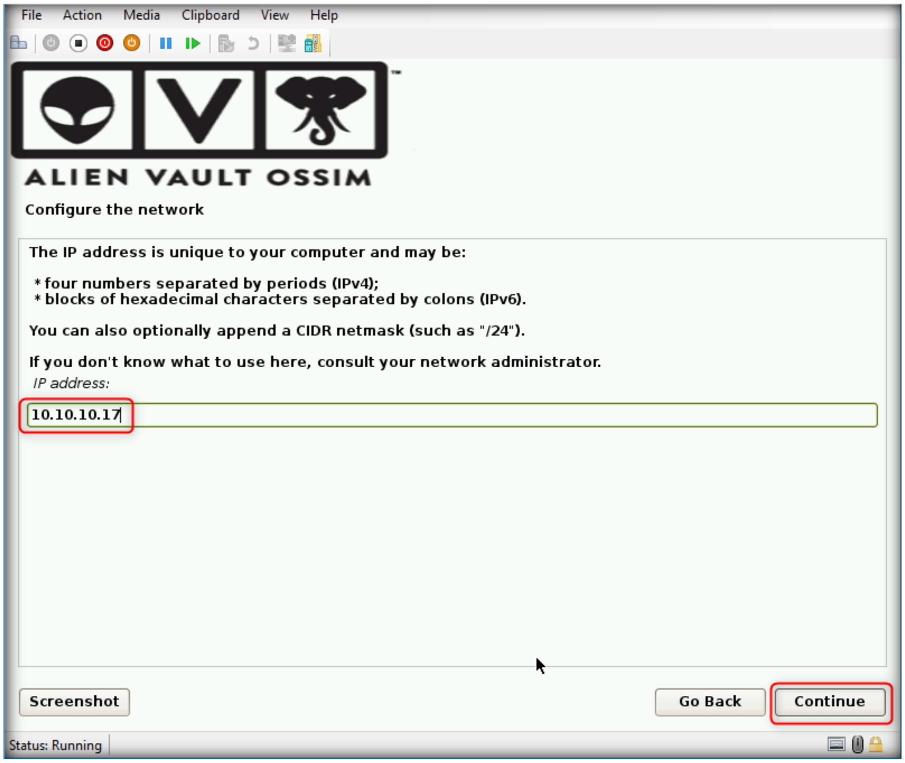
Configure the keyboard

Keymap to use:

American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian
Bulgarian (phonetic layout)
Burmese
Canadian French
Canadian Multilingual

25. Configure the network window appears. Enter **10.10.10.17** in the IP address: field and click **Continue**.

    Note: IP may differ if you have chosen a different IP while configuring OSSIM.



Configure the network

The IP address is unique to your computer and may be:

* four numbers separated by periods (IPv4);
* blocks of hexadecimal characters separated by colons (IPv6).

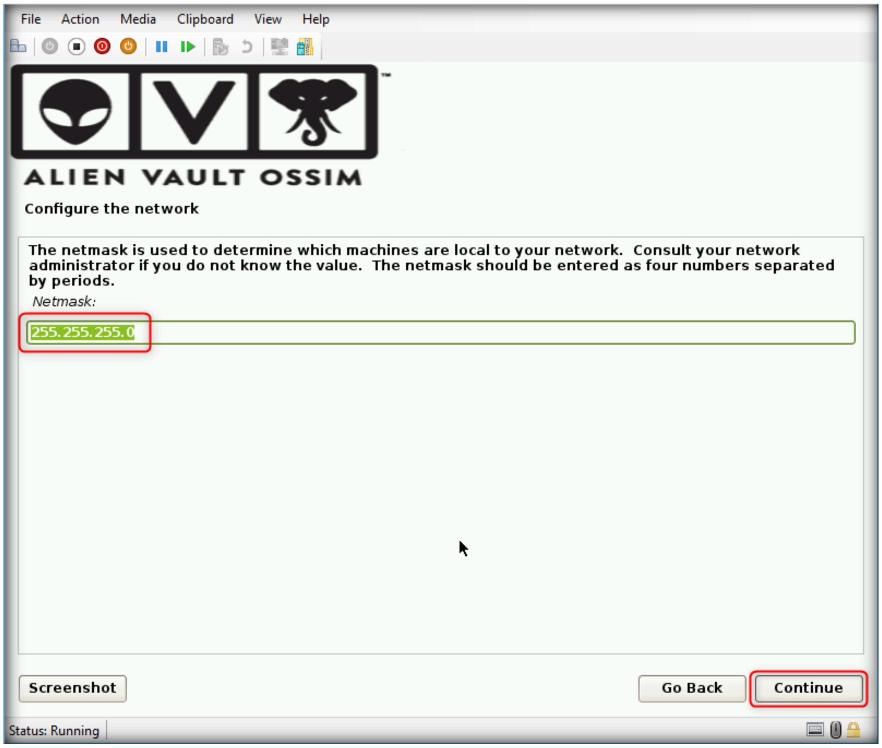
You can also optionally append a CIDR netmask (such as "/24").

If you don't know what to use here, consult your network administrator.

IP address:

10.10.10.17

26. Netmask: screen appears. Ensure the mask is set to **255.255.255.0** and click **Continue**.



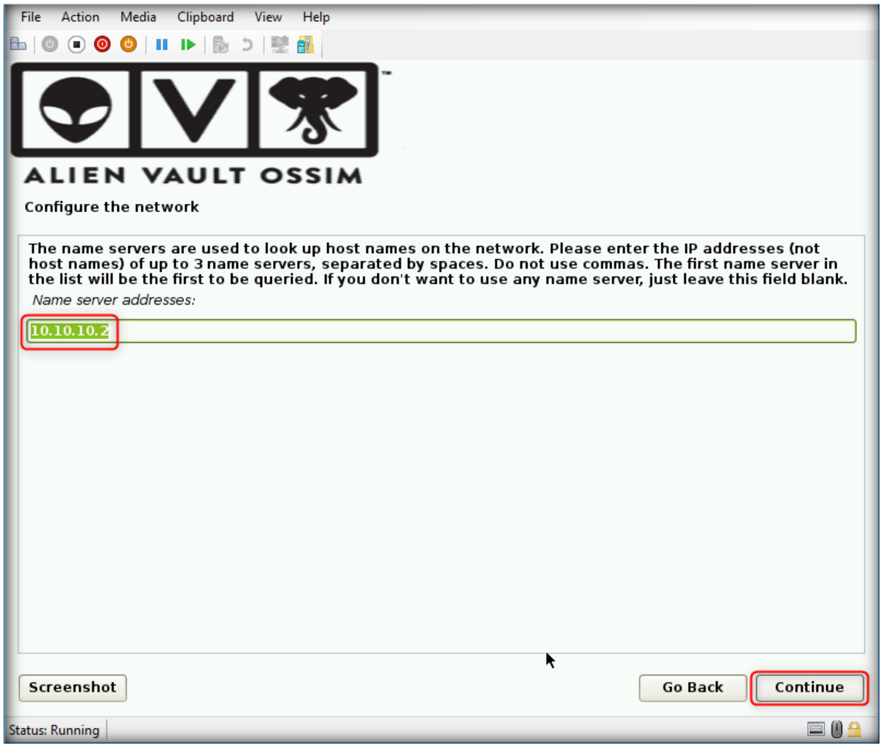
Configure the network

The netmask is used to determine which machines are local to your network. Consult your network administrator if you do not know the value. The netmask should be entered as four numbers separated by periods.

Netmask:

255.255.255.0

27. Gateway: screen appears. Ensure that gateway is set to **10.10.10.2** and click **Continue**.



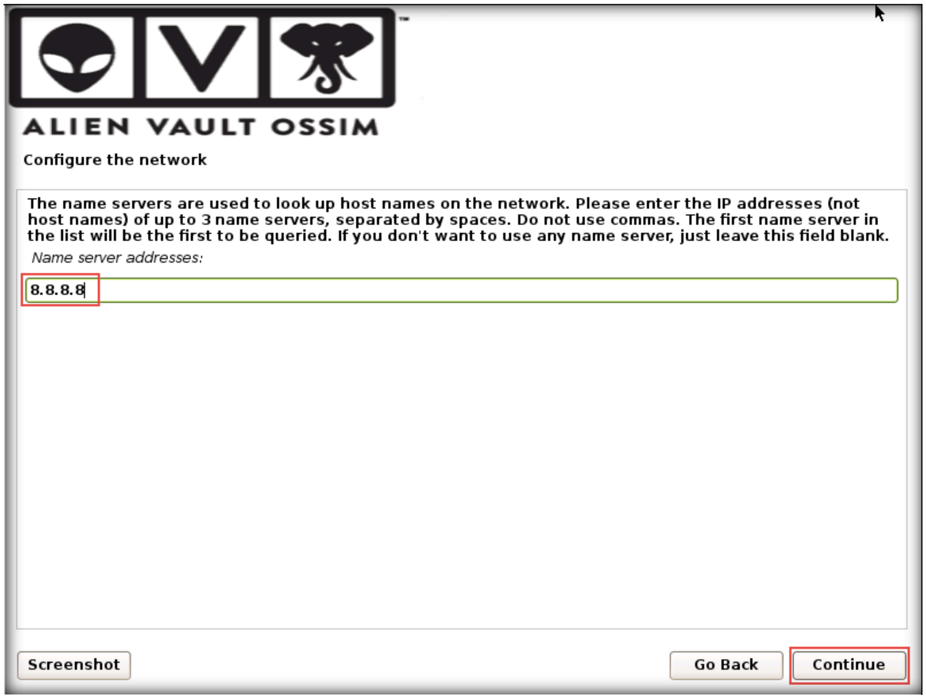
Configure the network

The name servers are used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.

Name server addresses:

10.10.10.2

28. Name server addresses: screen appears. You can enter the **DNS** server address, or you can leave the field default and click **Continue**.



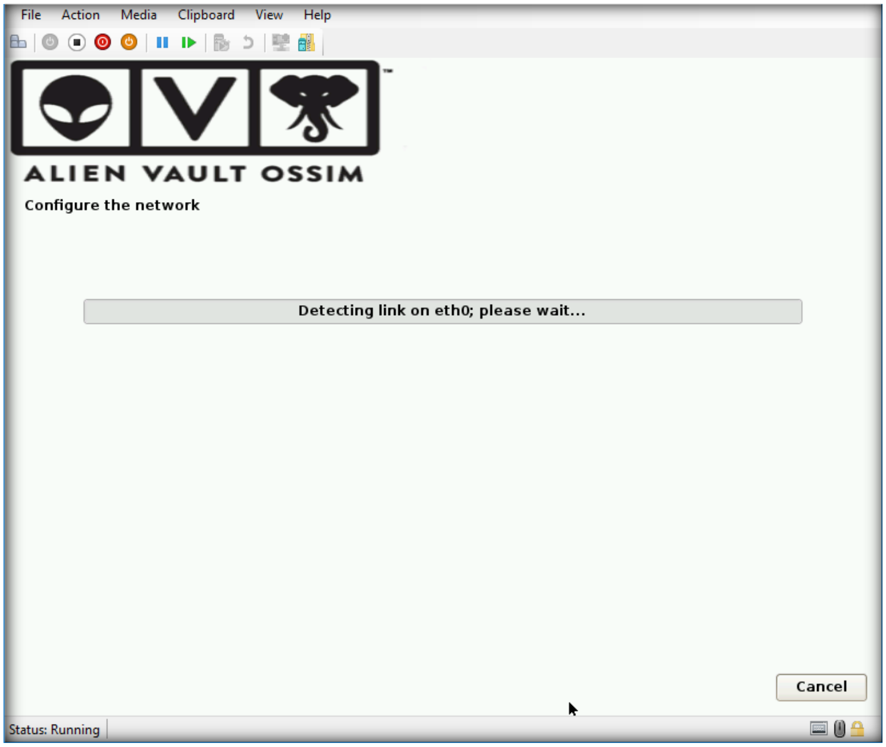
Configure the network

The name servers are used to look up host names on the network. Please enter the IP addresses (not host names) of up to 3 name servers, separated by spaces. Do not use commas. The first name server in the list will be the first to be queried. If you don't want to use any name server, just leave this field blank.

Name server addresses:

8.8.8.8

29. Wait until the network configuration is completed.

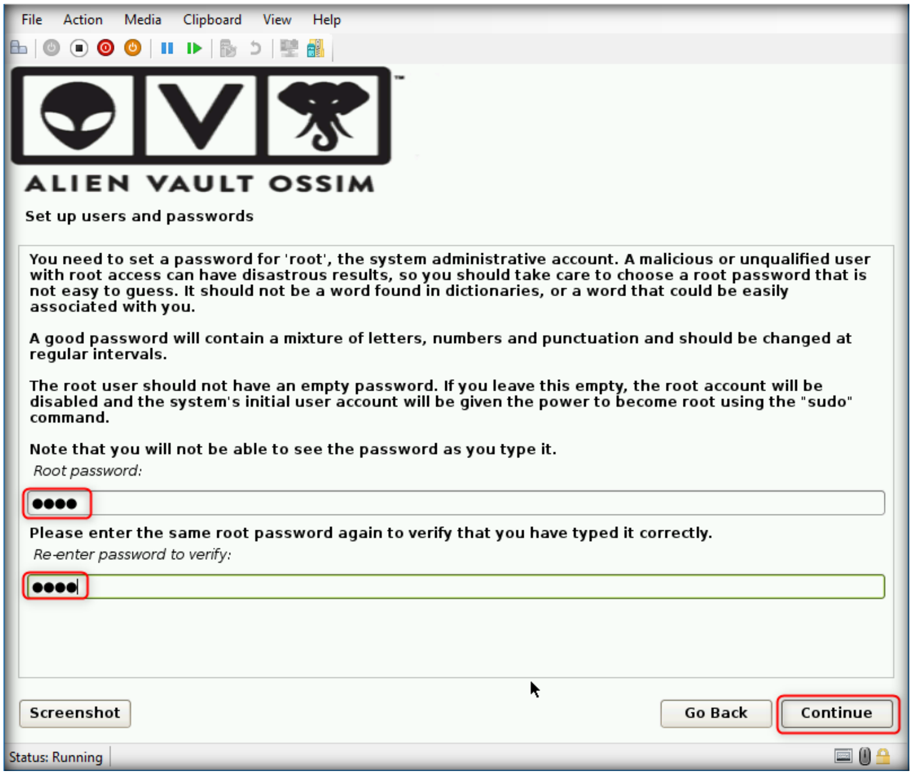


Configure the network

Detecting link on eth0; please wait...

30. Set up users and passwords screen appear. Enter **toor** in Root password: and Re-enter password to verify fields and click **Continue**.

Note: You can type any password of your choice.



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

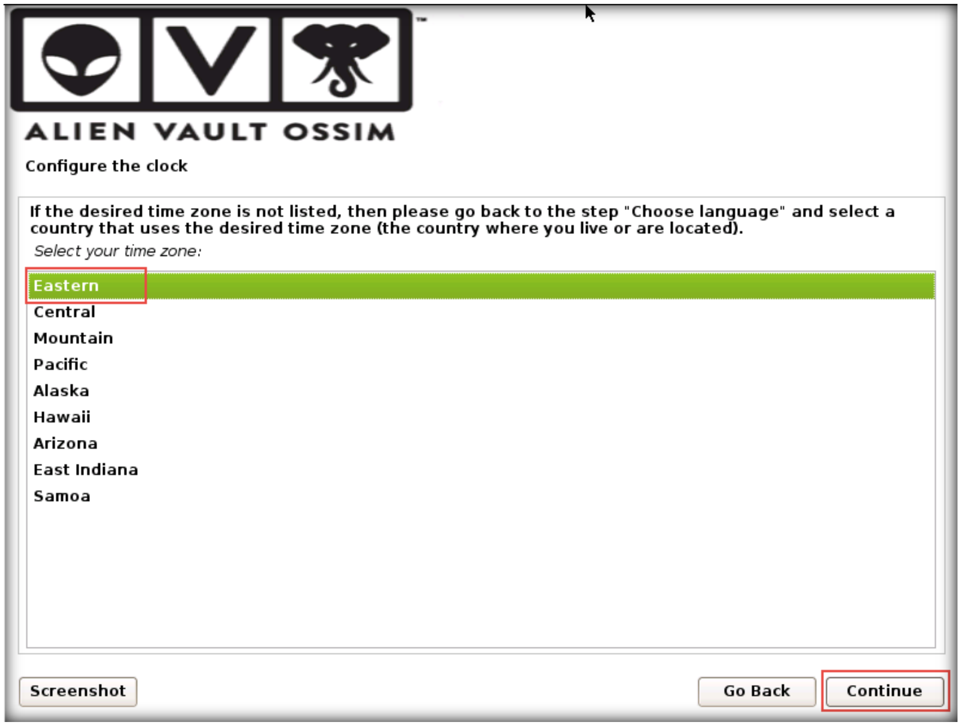
●●●●

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●

31. Configure the clock screen appears. Select your preferred time zone and click **Continue**.



ALIEN VAULT OSSIM

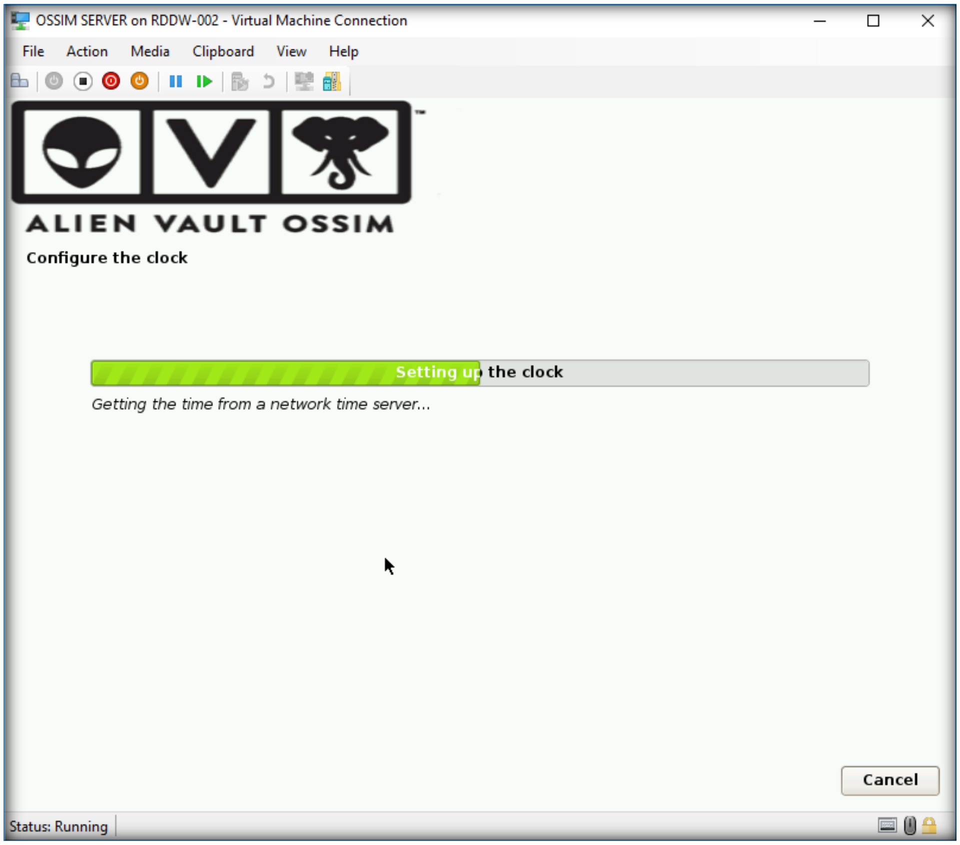
Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa

32. It will take some time to complete the configuration, wait until it finishes.



OSSIM SERVER on RDDW-002 - Virtual Machine Connection

ALIEN VAULT OSSIM

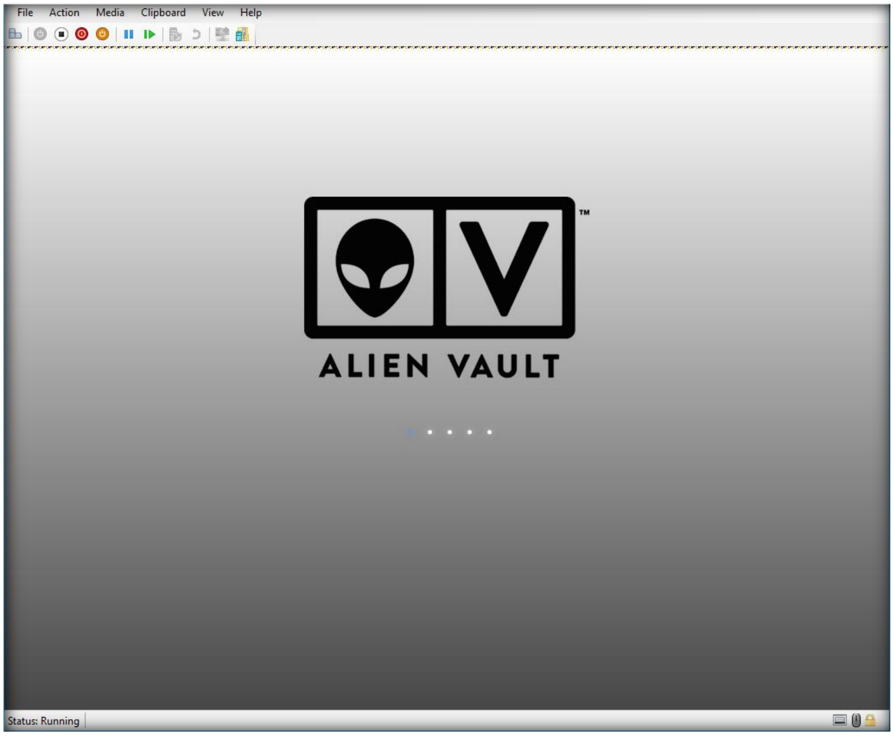
Configure the clock

Setting up the clock

Getting the time from a network time server...

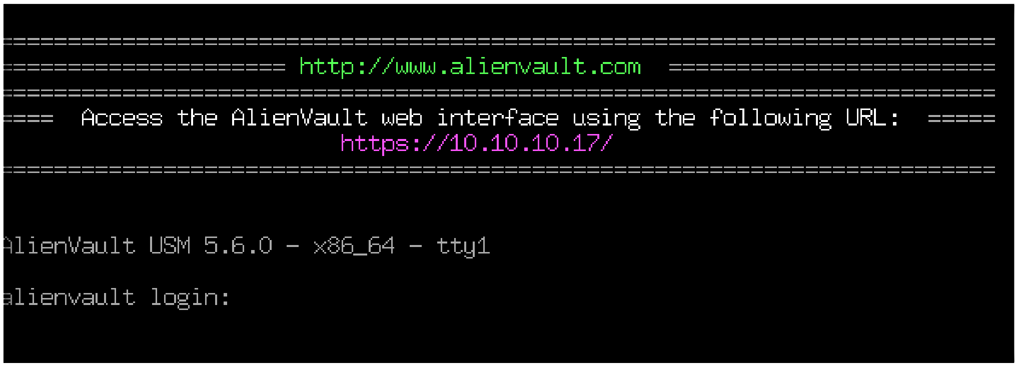
Status: Running

33. Once configurations are completed, the ALIEN VAULT screen appears as shown in the screenshot. **Restart** the machine.



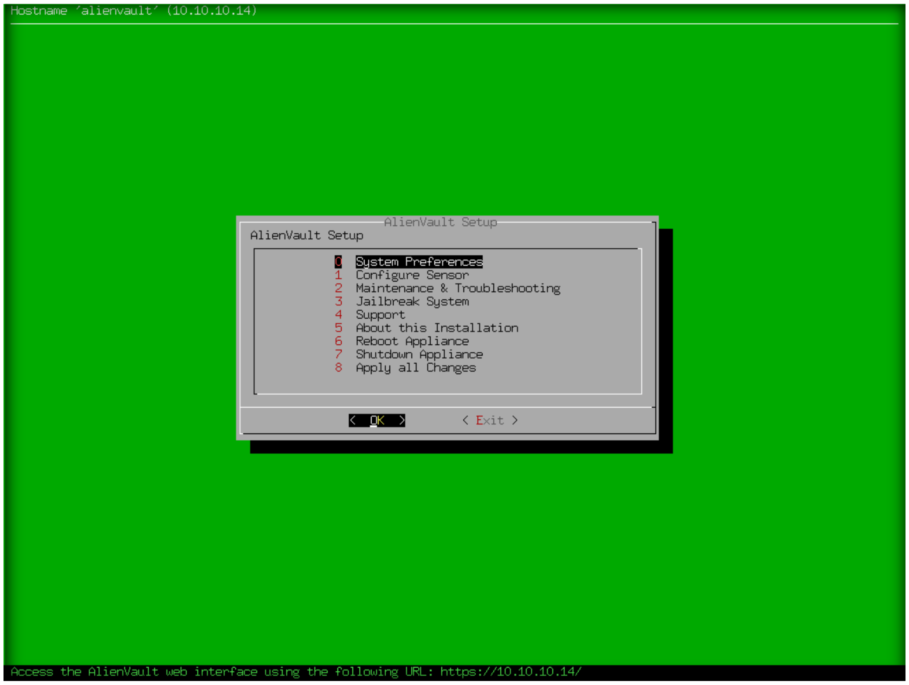
34. After restart wait for the login screen to appear and enter **root** as the username and press **Enter** key then type **toor** as password and press **Enter**.

Note: The password that you have set at **step 30** in this Configuration Task.



```
==========================================================================
===================== http://www.alienvault.com  ========================
==========================================================================
====  Access the AlienVault web interface using the following URL:  =====
                          https://10.10.10.17/
==========================================================================


AlienVault USM 5.6.0 - x86_64 - tty1

alienvault login:
```

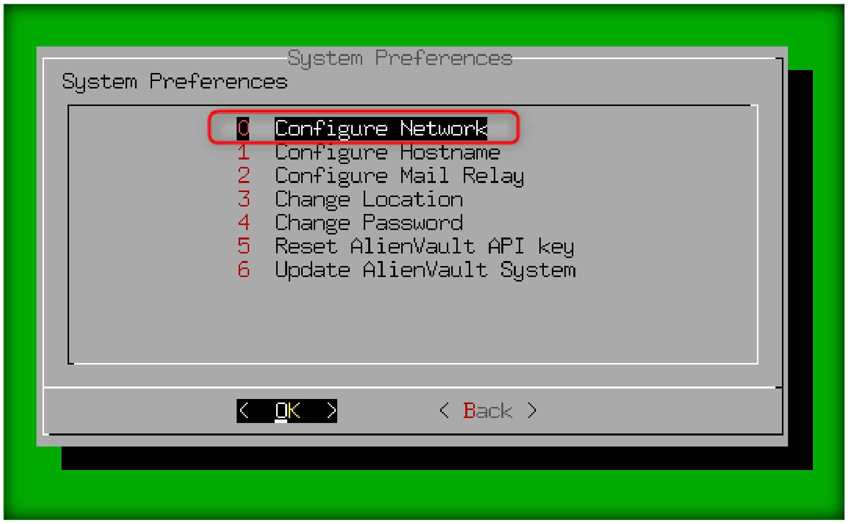
35. AlienVault Setup screen appears as shown in the screenshot.



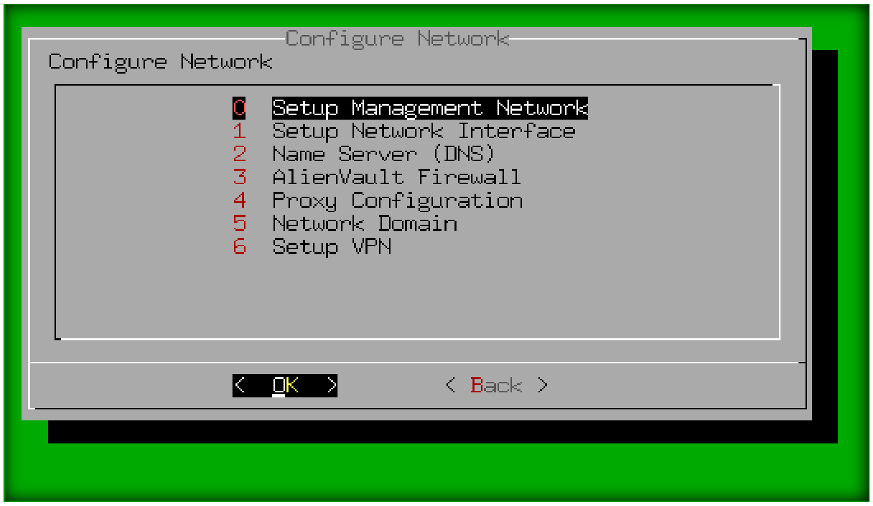
Hostname 'alienvault' (10.10.10.14)

Access the AlienVault web interface using the following URL: https://10.10.10.14/

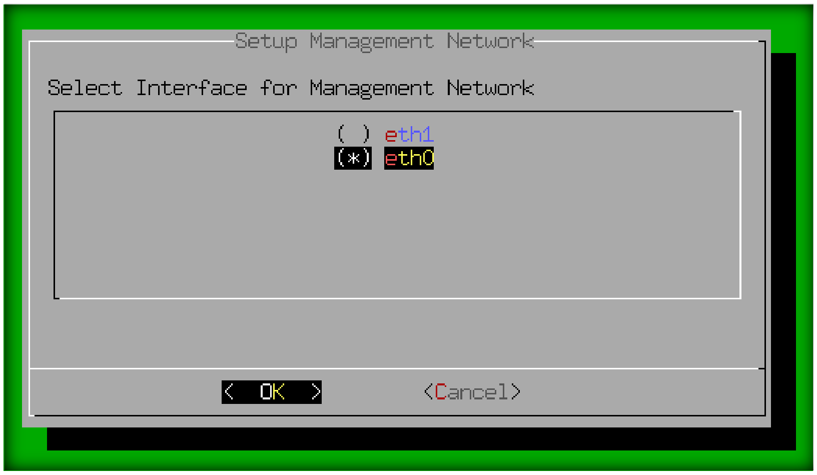
36. To setup **Management Network,** select **Configure Network** from **System Preferences** screen.



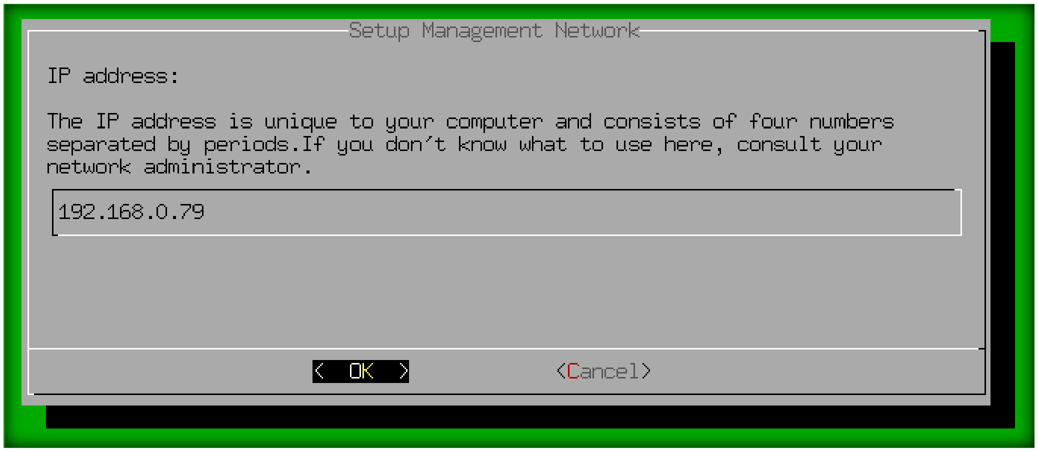
37. In the Configure Network screen, select **Setup Management Network**.



38. In the Select Interface for Management Network screen, select **eth0** (Default adaptor).

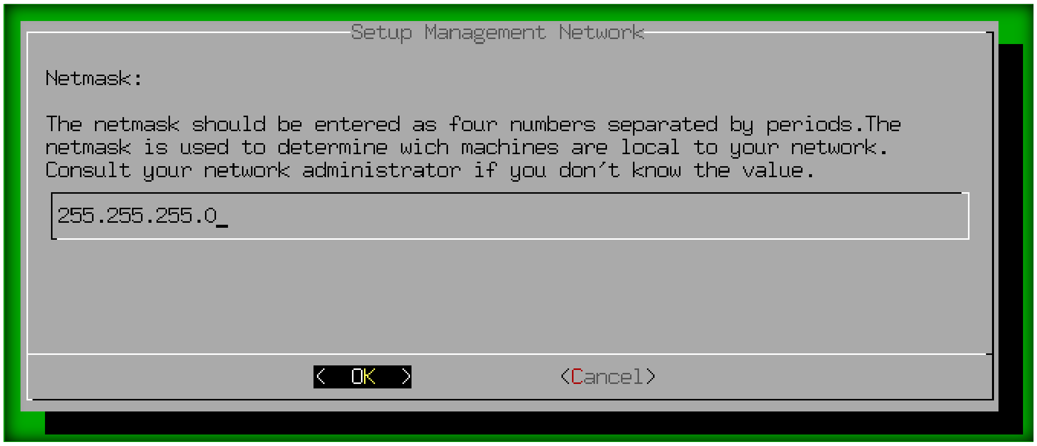


39. In the Setup Management Network, type IP **192.168.0.79** address and select **OK**.



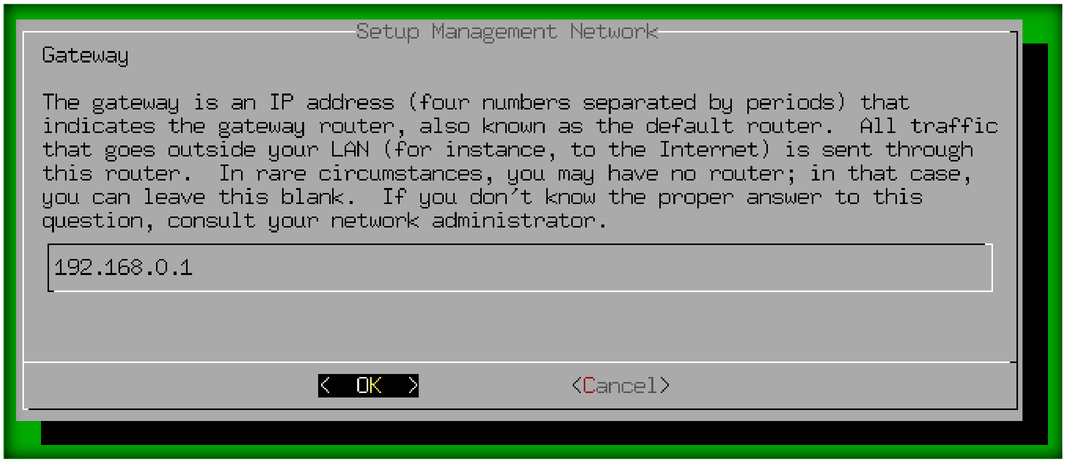
```
IP address:

The IP address is unique to your computer and consists of four numbers
separated by periods.If you don't know what to use here, consult your
network administrator.

192.168.0.79
```

40. In the Netmask screen, type IP **255.255.255.0** as netmask and select **OK**.



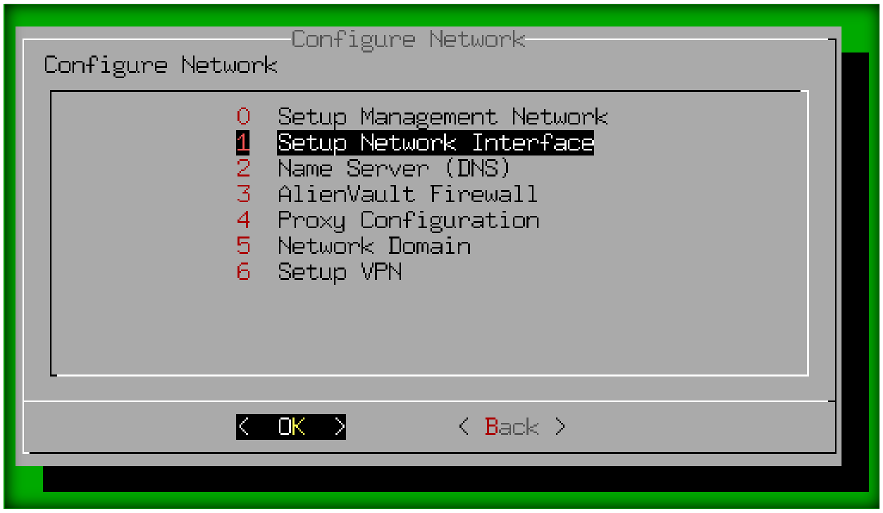
```
Setup Management Network

Netmask:

The netmask should be entered as four numbers separated by periods.The
netmask is used to determine wich machines are local to your network.
Consult your network administrator if you don't know the value.

255.255.255.0_

< OK >          <Cancel>
```

41. In the Gateway screen, type **192.168.0.1** as Gateway and select **OK**.



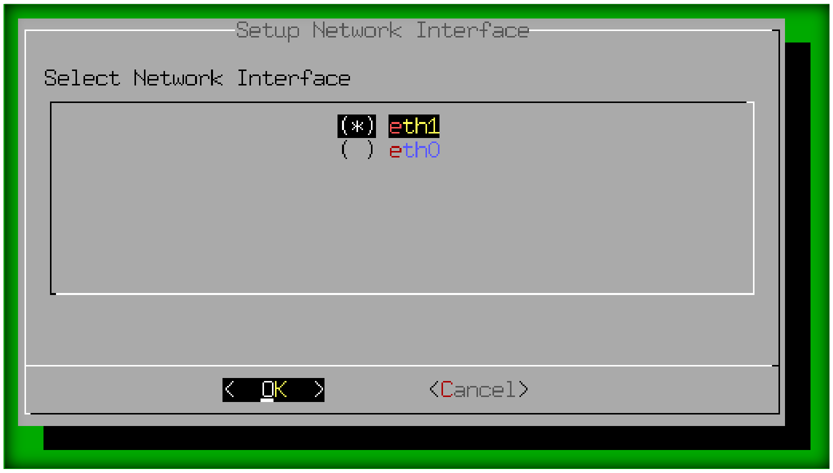
```
Setup Management Network
Gateway

The gateway is an IP address (four numbers separated by periods) that
indicates the gateway router, also known as the default router.  All traffic
that goes outside your LAN (for instance, to the Internet) is sent through
this router.  In rare circumstances, you may have no router; in that case,
you can leave this blank.  If you don't know the proper answer to this
question, consult your network administrator.

192.168.0.1

< OK >          <Cancel>
```

42. To setup **Network Interface,** Select **Setup Network Interface** option and click **OK**.



```
Configure Network
Configure Network

        0  Setup Management Network
        1  Setup Network Interface
        2  Name Server (DNS)
        3  AlienVault Firewall
        4  Proxy Configuration
        5  Network Domain
        6  Setup VPN

< OK >          < Back >
```

43. In the Setup Network Interface screen, select **eth1** option and click **OK**.

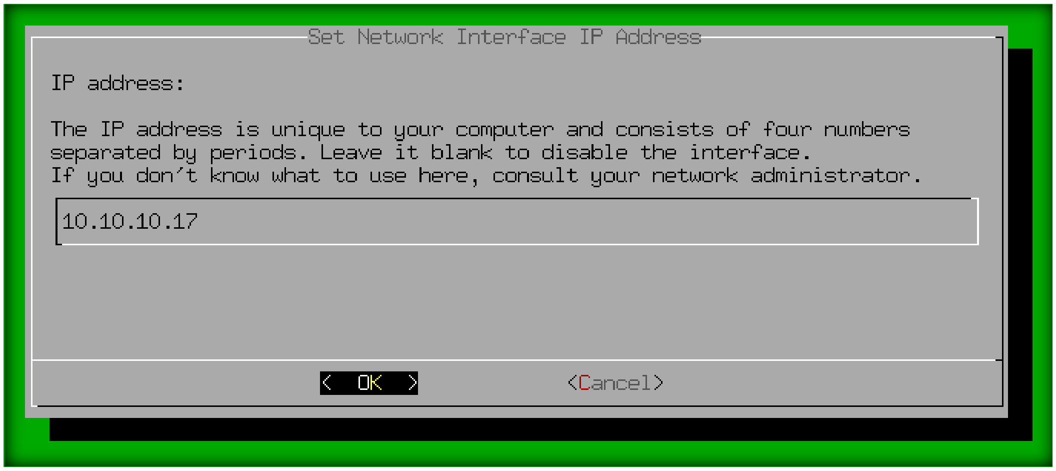


Setup Network Interface

Select Network Interface

```
(*) eth1
( ) eth0
```

44. In the Set Network Interface IP address screen, type **10.10.10.17** and select **OK**.



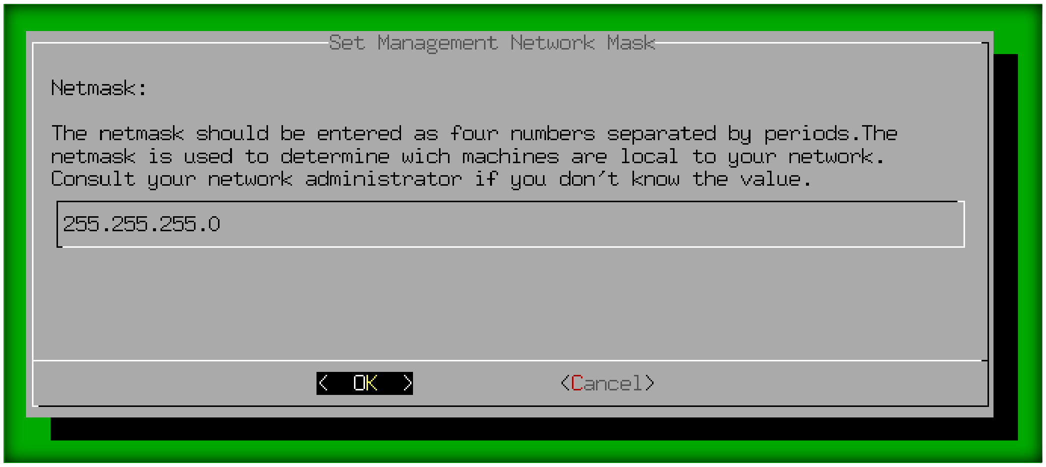
Set Network Interface IP Address

IP address:

The IP address is unique to your computer and consists of four numbers
separated by periods. Leave it blank to disable the interface.
If you don't know what to use here, consult your network administrator.

```
10.10.10.17
```

45. In the Set Management Network Mask screen, type **255.255.255.0** and select **OK.**



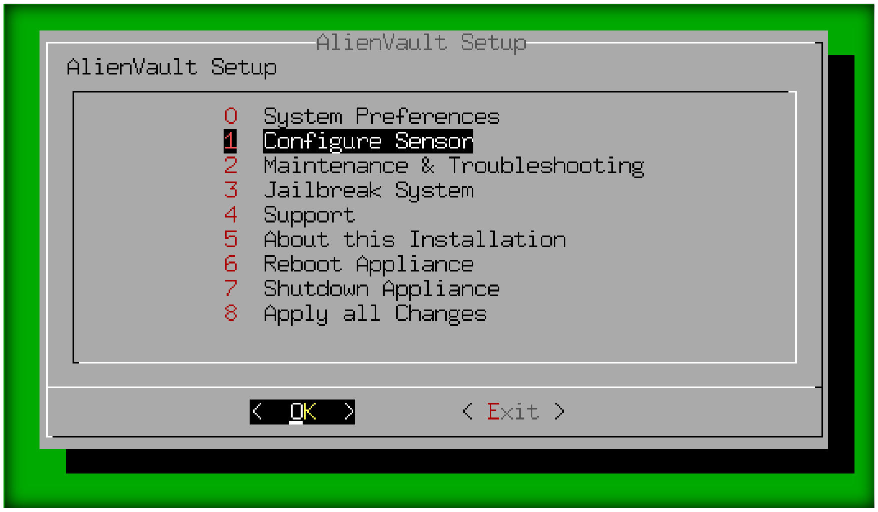
Set Management Network Mask

Netmask:

The netmask should be entered as four numbers separated by periods.The
netmask is used to determine wich machines are local to your network.
Consult your network administrator if you don't know the value.

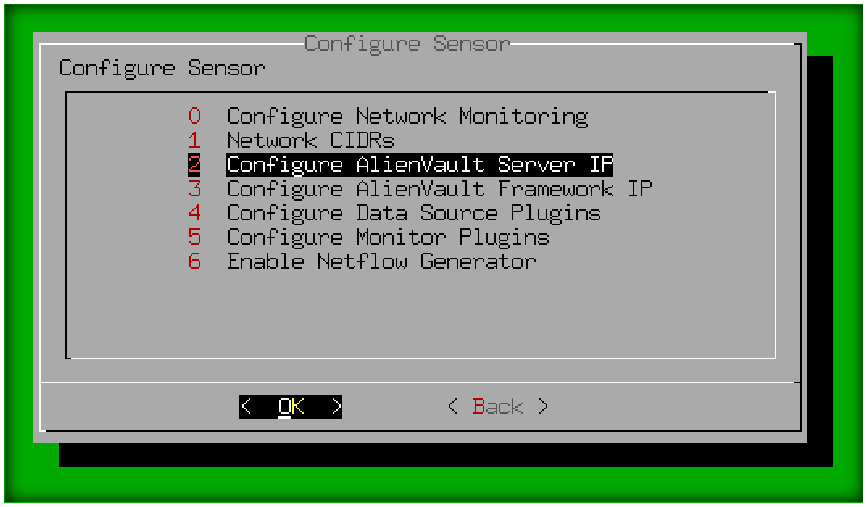
```
255.255.255.0
```

46. Select **Back** until you view the AlienVault Setup Screen. Select **Configure Sensor** option and click **OK**.



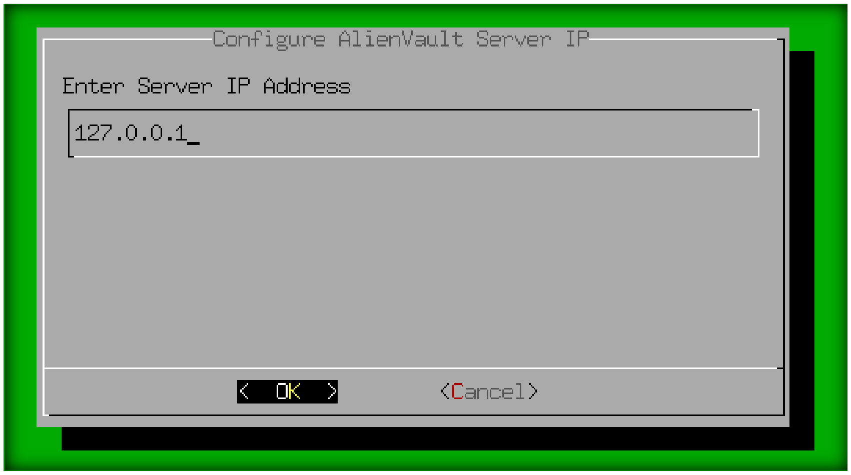
```
AlienVault Setup
AlienVault Setup

        0  System Preferences
        1  Configure Sensor
        2  Maintenance & Troubleshooting
        3  Jailbreak System
        4  Support
        5  About this Installation
        6  Reboot Appliance
        7  Shutdown Appliance
        8  Apply all Changes

        <  OK  >          < Exit >
```

47. In the **Configure Sensor** screen, select Configure AlienVault Server IP and select **OK**.



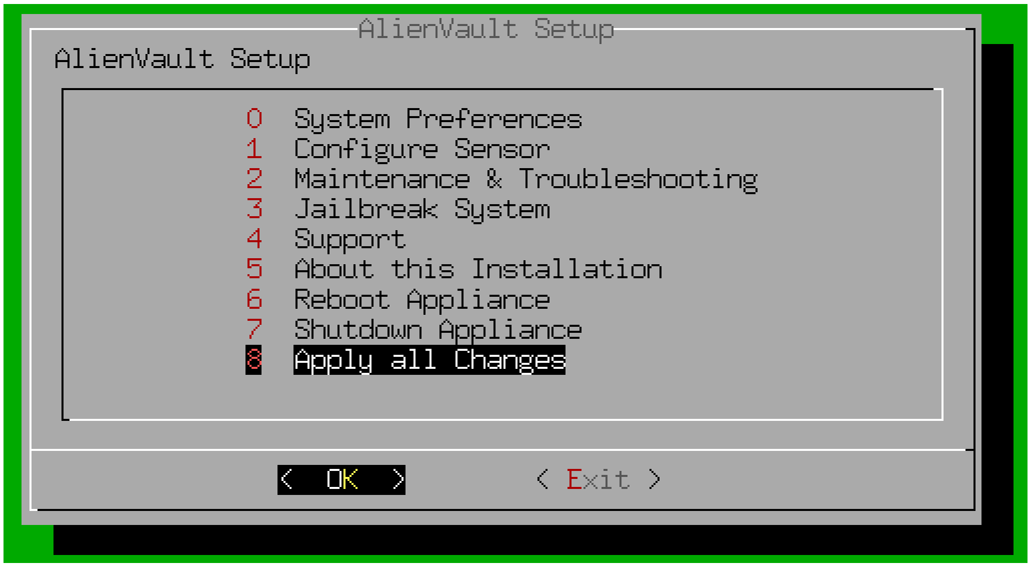
```
Configure Sensor
Configure Sensor

      0  Configure Network Monitoring
      1  Network CIDRs
      2  Configure AlienVault Server IP
      3  Configure AlienVault Framework IP
      4  Configure Data Source Plugins
      5  Configure Monitor Plugins
      6  Enable Netflow Generator

        <  OK  >          < Back >
```

48. In the **Configure Alienvault Server IP,** enter **127.0.0.1** and select **OK**.



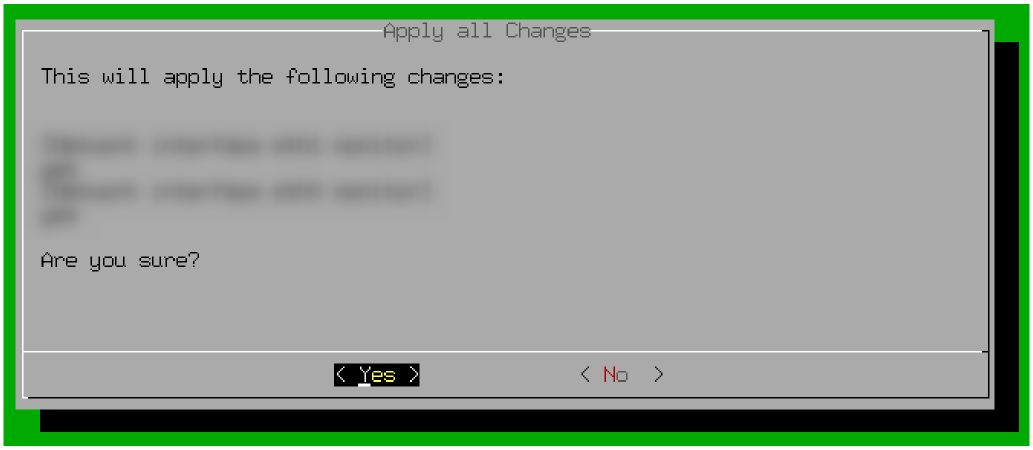
```
Configure AlienVault Server IP

Enter Server IP Address
127.0.0.1_

        <  OK  >          <Cancel>
```

49. Select **Back** until you view the AlienVault Setup Screen. Select **Apply all Changes** option and click **OK**.



AlienVault Setup

50. Apply all Changes screen will appear Select **Yes**.

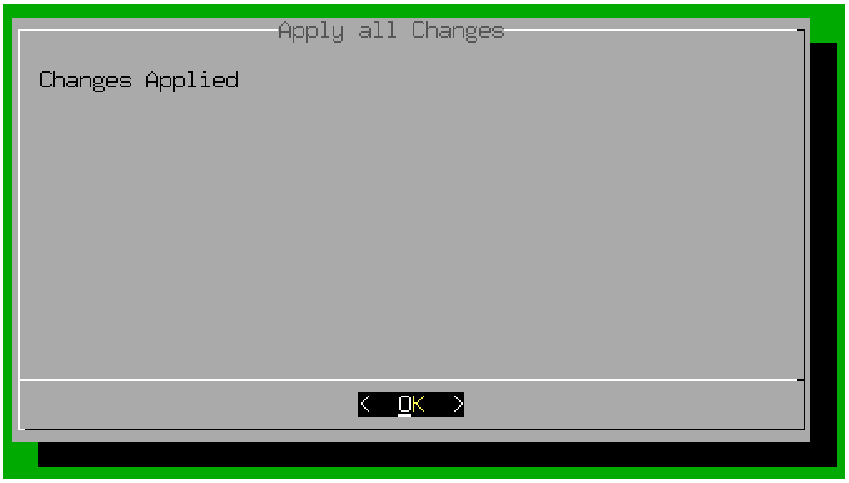


This will apply the following changes:

[redacted]

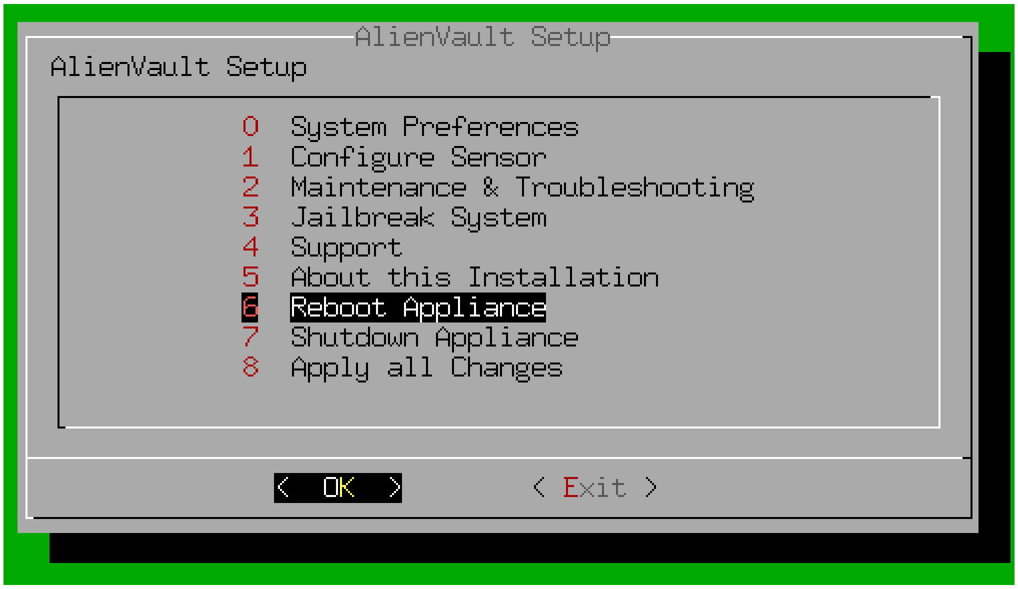
Are you sure?

51. Once all changes are applied select the **OK.**



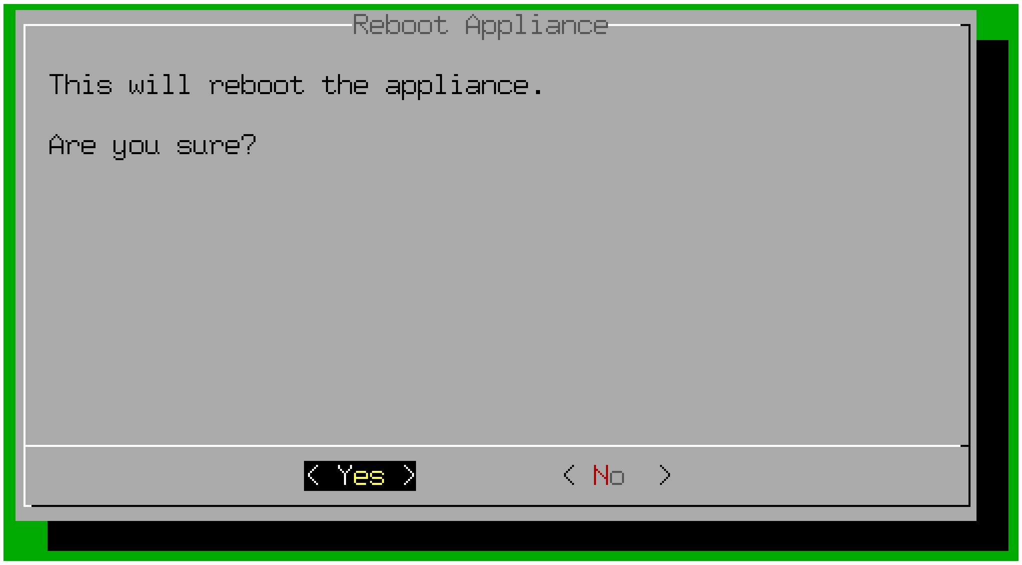
Changes Applied

52. Select **Reboot Appliance** option and press **Enter**.



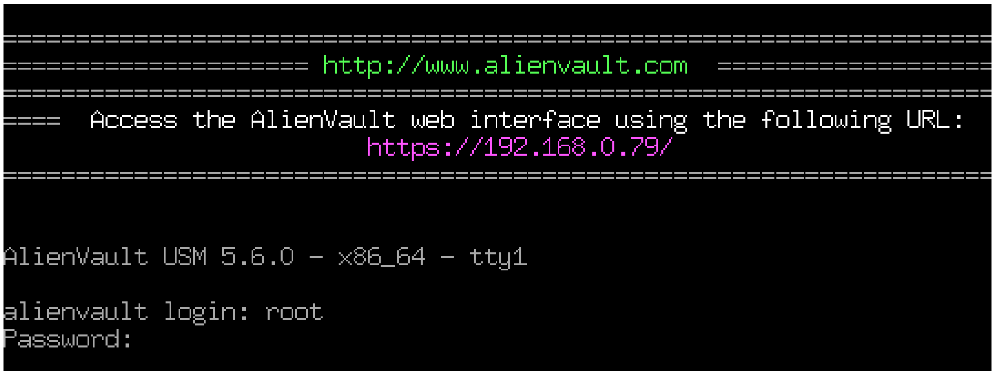
```
AlienVault Setup
AlienVault Setup

        0  System Preferences
        1  Configure Sensor
        2  Maintenance & Troubleshooting
        3  Jailbreak System
        4  Support
        5  About this Installation
        6  Reboot Appliance
        7  Shutdown Appliance
        8  Apply all Changes

        <  OK  >           < Exit >
```

53. Select **Yes** to Reboot Appliance.



```
Reboot Appliance

This will reboot the appliance.

Are you sure?

        < Yes >           < No  >
```

54. After reboot wait for the login screen to appear and enter **root** as the username and press **Enter** key then type **toor** as password and press **Enter**.



```
=====================================================================
==================== http://www.alienvault.com  ===================
=====================================================================
====  Access the AlienVault web interface using the following URL:
                       https://192.168.0.79/
=====================================================================


AlienVault USM 5.6.0 - x86_64 - tty1

alienvault login: root
Password:
```

CT#11: Creating and Configuring Windows 10 Virtual Machine (SIEM2)

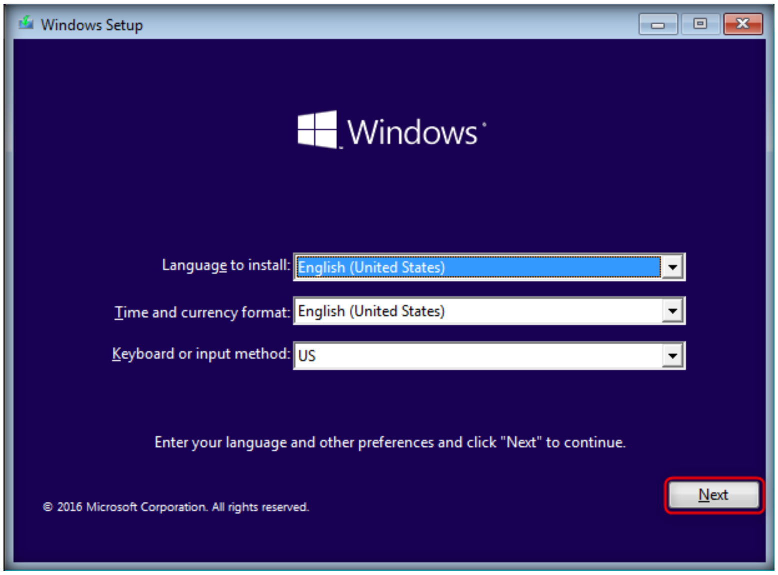
CT#11.1: Creating a Virtual Machine and Installing Windows 10 Enterprise Guest OS

Follow the steps of CT#5.1, to create a VM and install **Windows 10** guest OS.

Virtual Machine Name: **SIEM2.**

RAM: **2000 MB**

1. Wait until Windows Setup screen appears, in Windows Setup screens choose the **Language** and other preferences then click **Next**.



Language to install: English (United States)

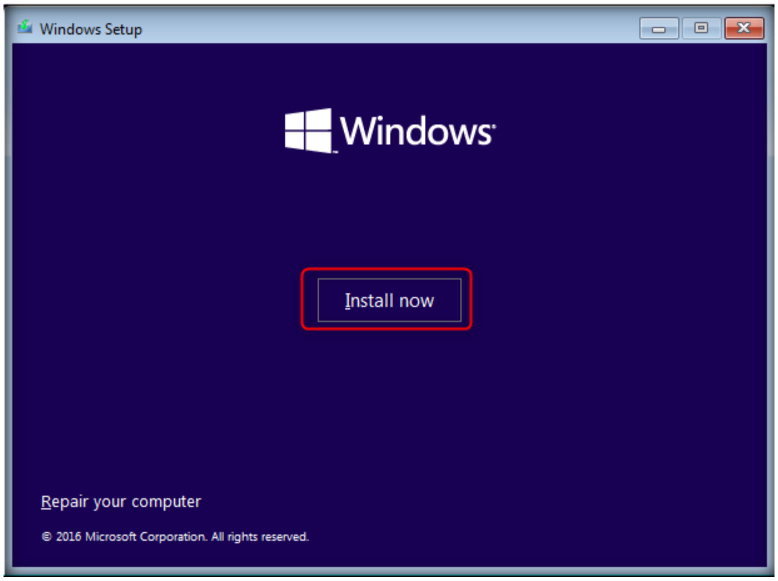
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

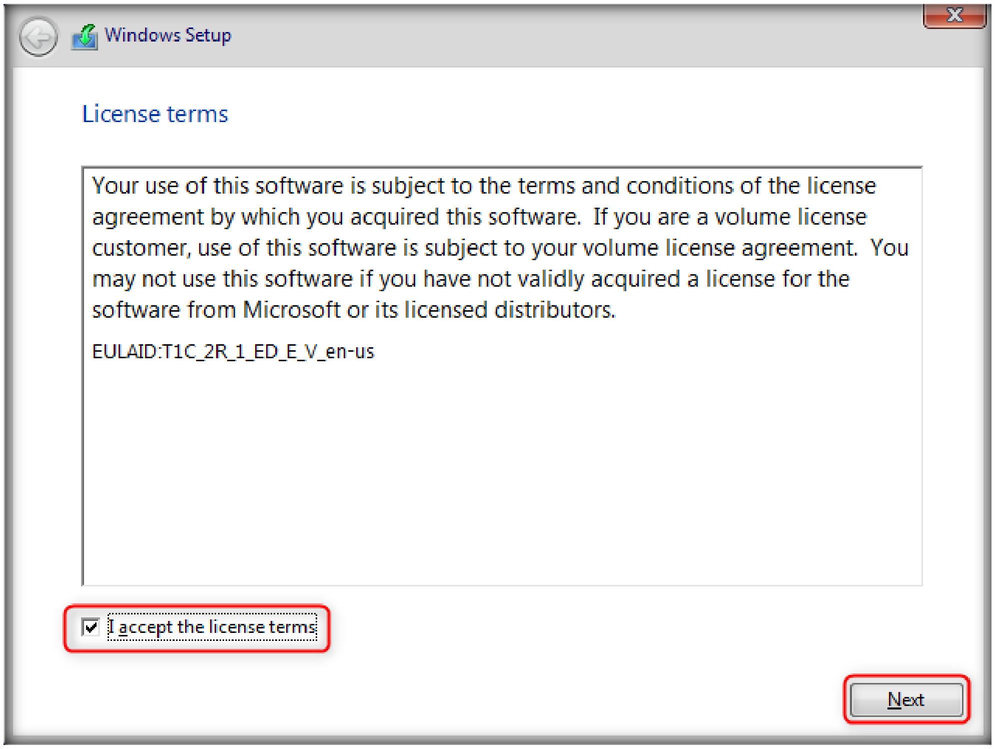
© 2016 Microsoft Corporation. All rights reserved.

2. Click **Install now** button to start the installation process of Windows 10.



© 2016 Microsoft Corporation. All rights reserved.

3. License terms wizard appears, check I accept the license terms check and box and click **Next**.



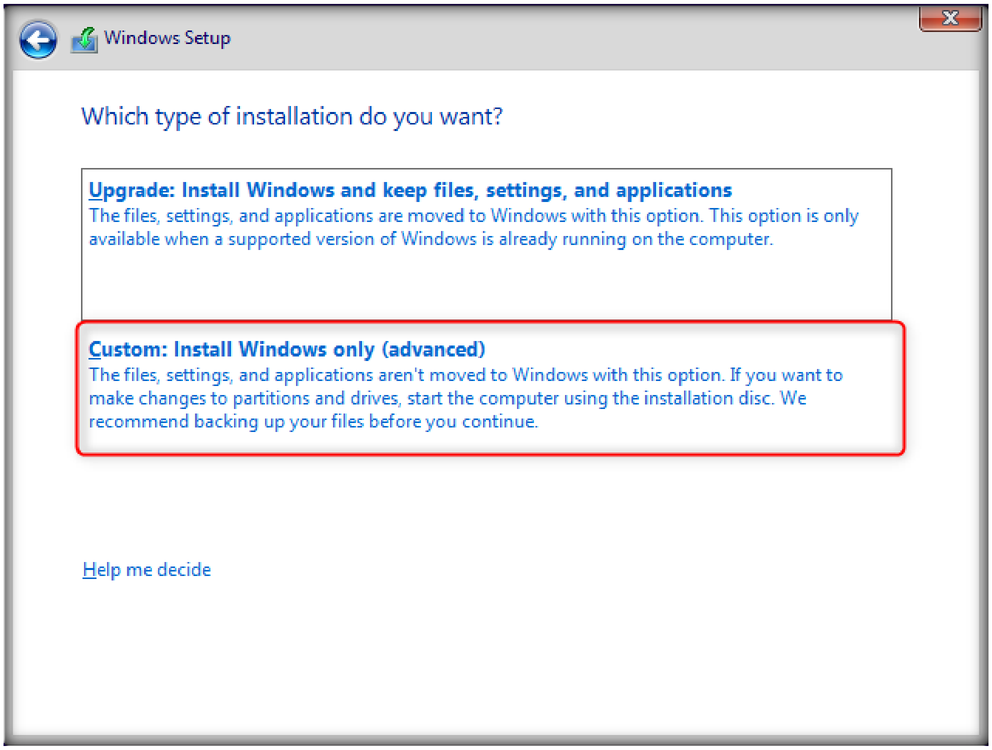
License terms

Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. If you are a volume license customer, use of this software is subject to your volume license agreement. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.

EULAID:T1C_2R_1_ED_E_V_en-us

☑ I accept the license terms

4. Click **Custom: Install Windows only (advanced)** option to proceed with the installation.

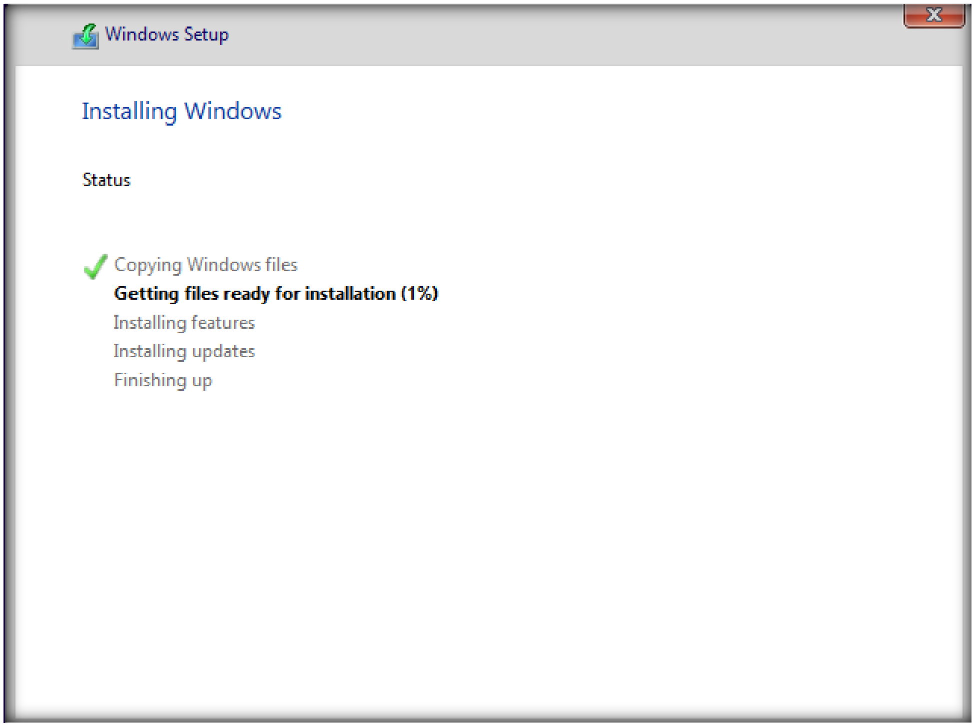


Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

5. Installing Windows screen appears; wait until it completes the installation.



Installing Windows

Status

✓ Copying Windows files

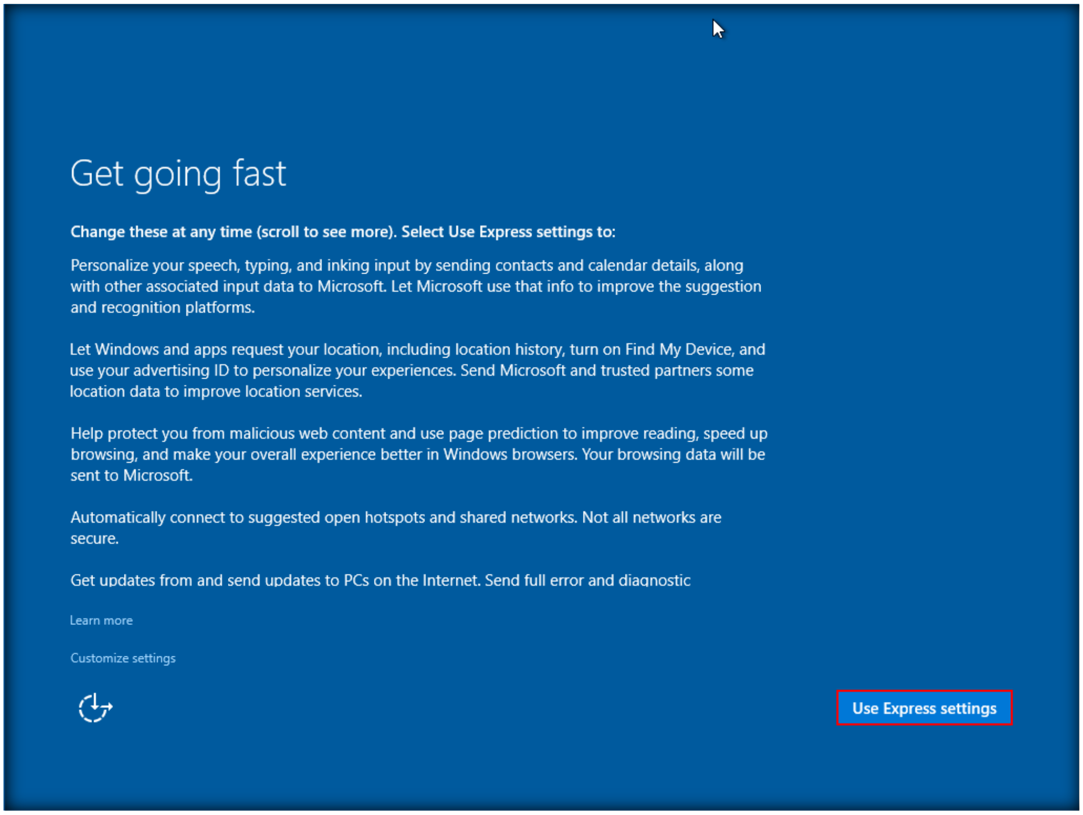
Getting files ready for installation (1%)

Installing features

Installing updates

Finishing up

6. Once the installation is completed machine will restart, and you will see the Get going fast screen. Click **Use Express settings** button.



Get going fast

Change these at any time (scroll to see more). Select Use Express settings to:

Personalize your speech, typing, and inking input by sending contacts and calendar details, along with other associated input data to Microsoft. Let Microsoft use that info to improve the suggestion and recognition platforms.

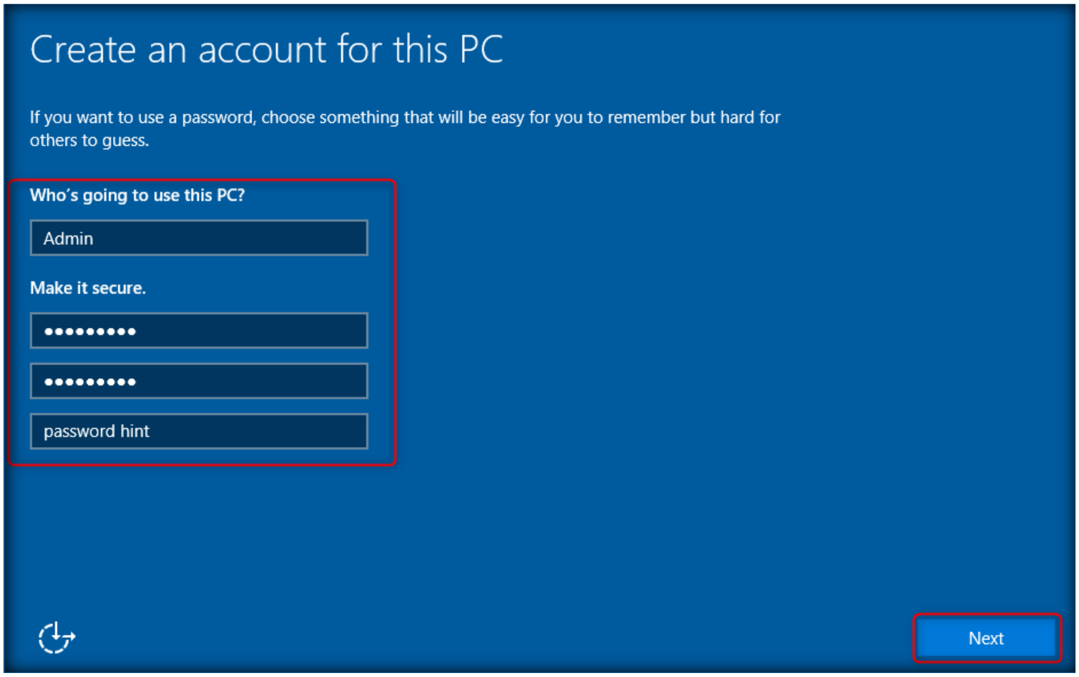
Let Windows and apps request your location, including location history, turn on Find My Device, and use your advertising ID to personalize your experiences. Send Microsoft and trusted partners some location data to improve location services.

Help protect you from malicious web content and use page prediction to improve reading, speed up browsing, and make your overall experience better in Windows browsers. Your browsing data will be sent to Microsoft.

Automatically connect to suggested open hotspots and shared networks. Not all networks are secure.

Get updates from and send updates to PCs on the Internet. Send full error and diagnostic

7. Create an account for this PC screen appears, fill the following details:
   - Username: **admin**
   - Password: **admin@123**
   - Hint field need to be filled mandatory, you can fill with the desired hint, and click **Next**.



Create an account for this PC

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?

Admin

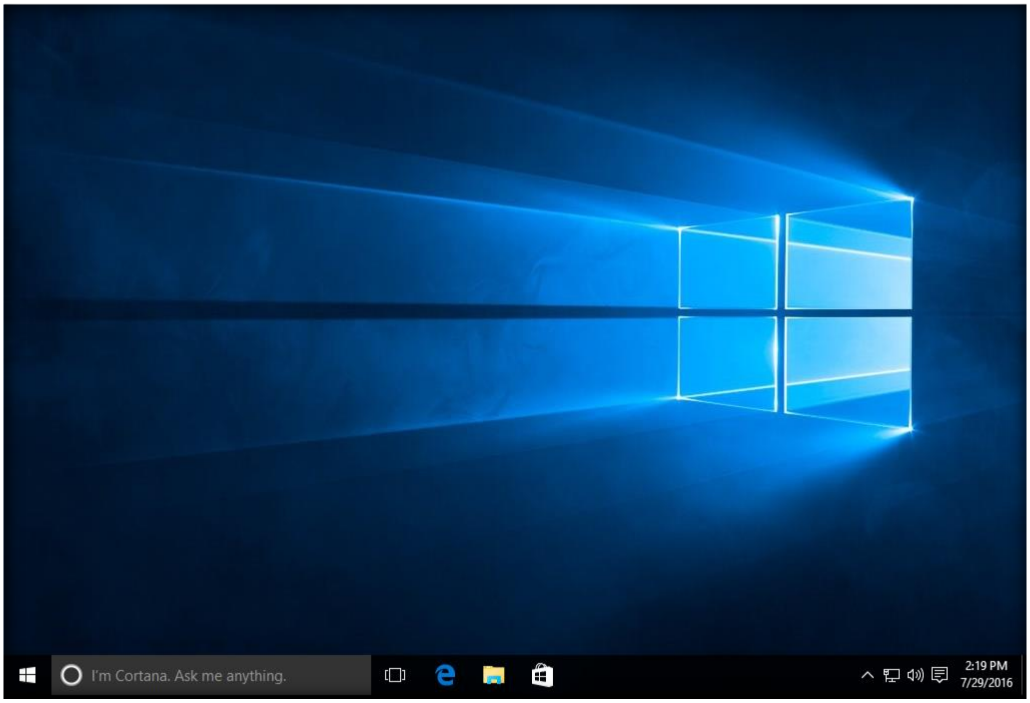
Make it secure.

••••••••••

••••••••••

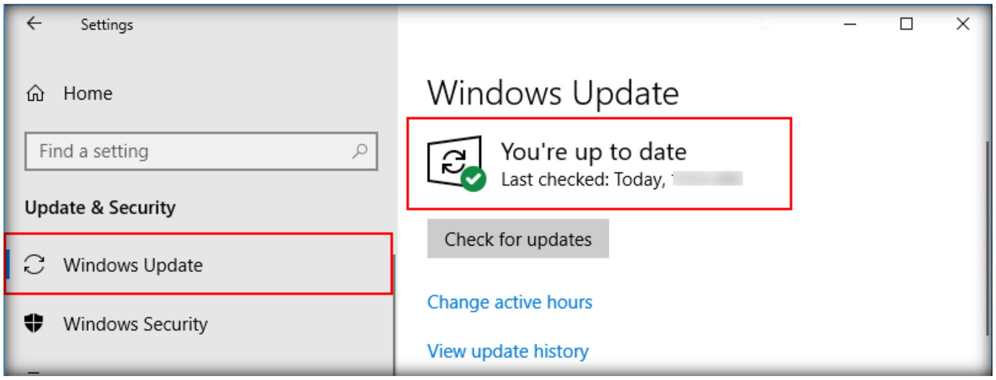
password hint

8. Windows 10 machine is ready as shown in the screenshot.



9. Now, check for the system updates and if found any, update the **Windows 10 (SIEM2)** virtual machine to the latest.

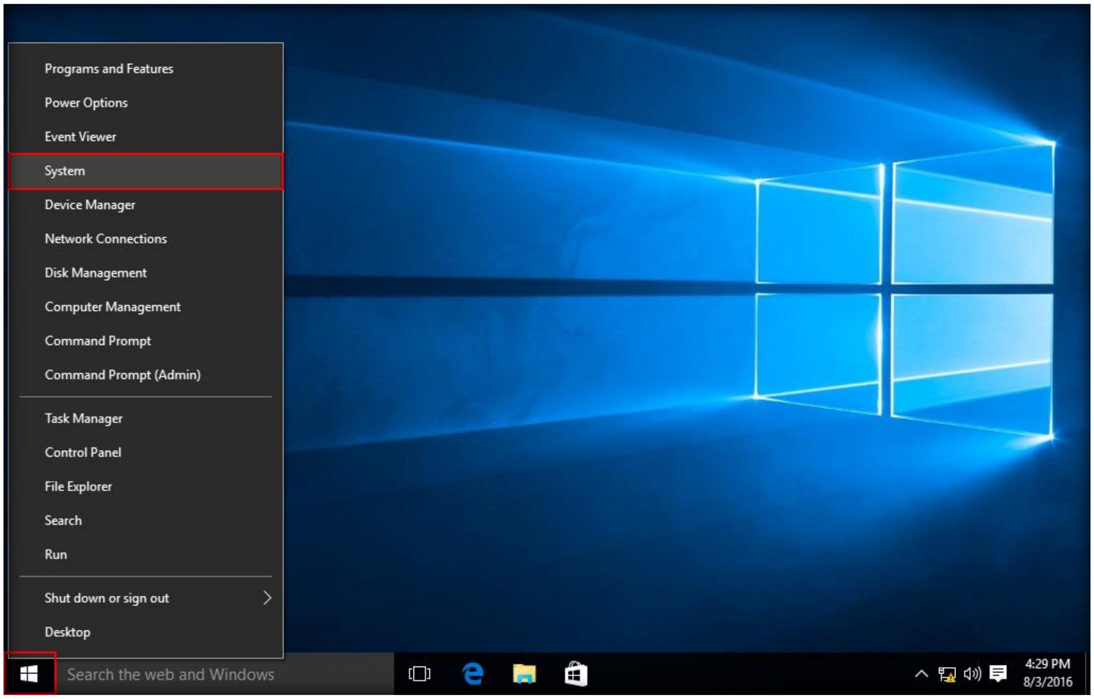
   Note: Installing the updates might take some time.



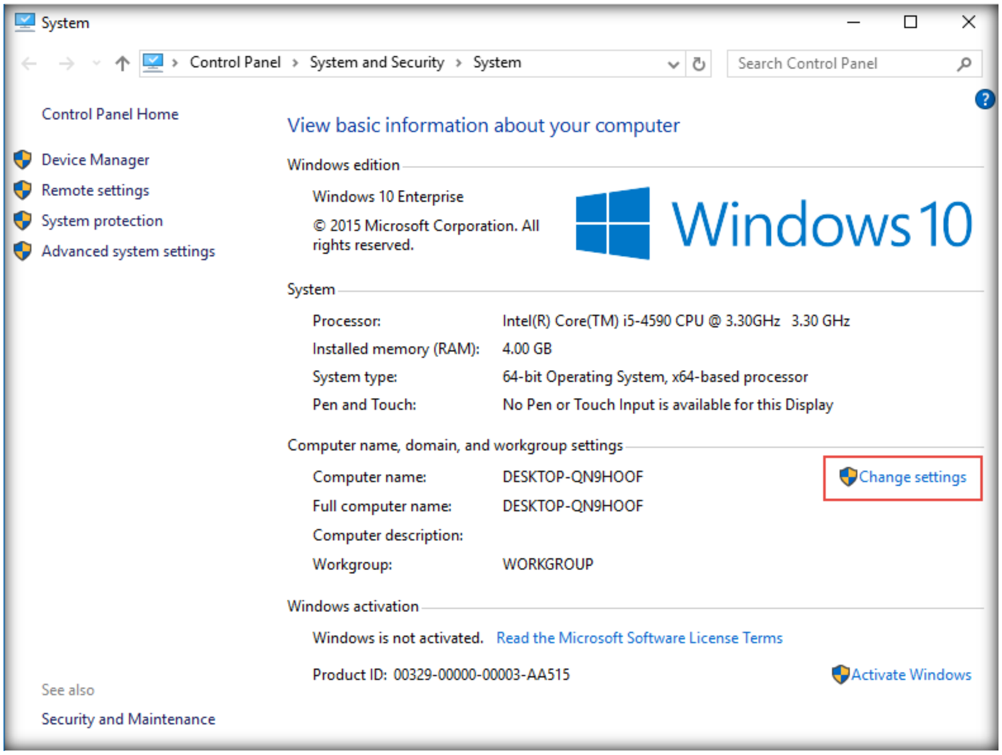
You're up to date
Last checked: Today, [redacted]

CT#11.2: Change the Computer Name

1. Right-click **Start** icon and click on **System**.



2. In the System properties window, click **Change settings**.



View basic information about your computer

Windows edition

Windows 10 Enterprise

© 2015 Microsoft Corporation. All rights reserved.

Windows 10

System

Processor: Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 3.30 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: DESKTOP-QN9HOOF

Full computer name: DESKTOP-QN9HOOF

Computer description:

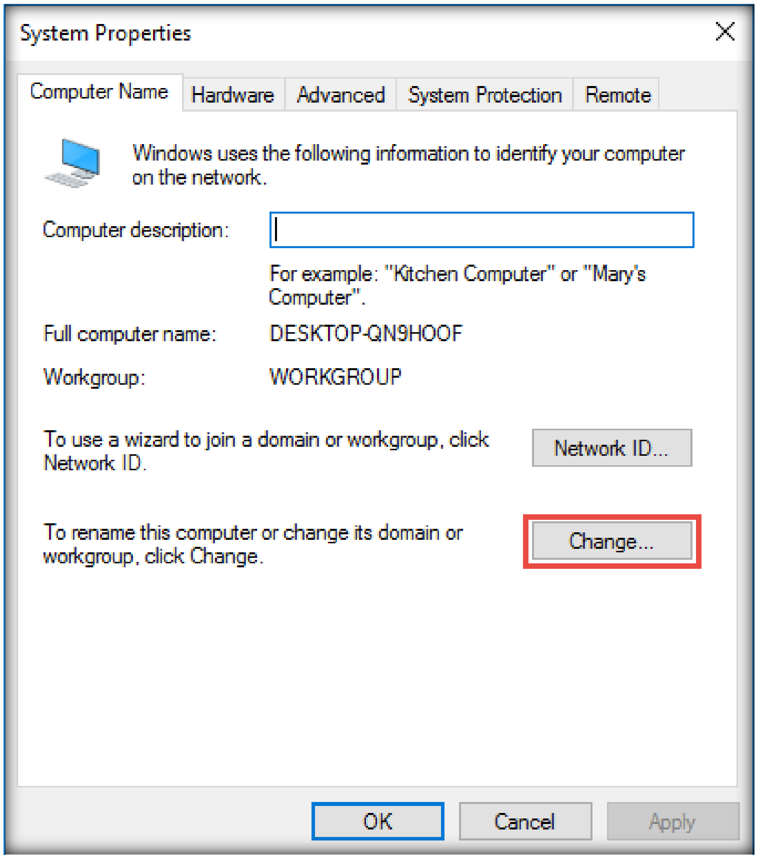
Workgroup: WORKGROUP

Windows activation

Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00329-00000-00003-AA515

3. In the Computer Name tab of the System Properties window, click **Change**.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

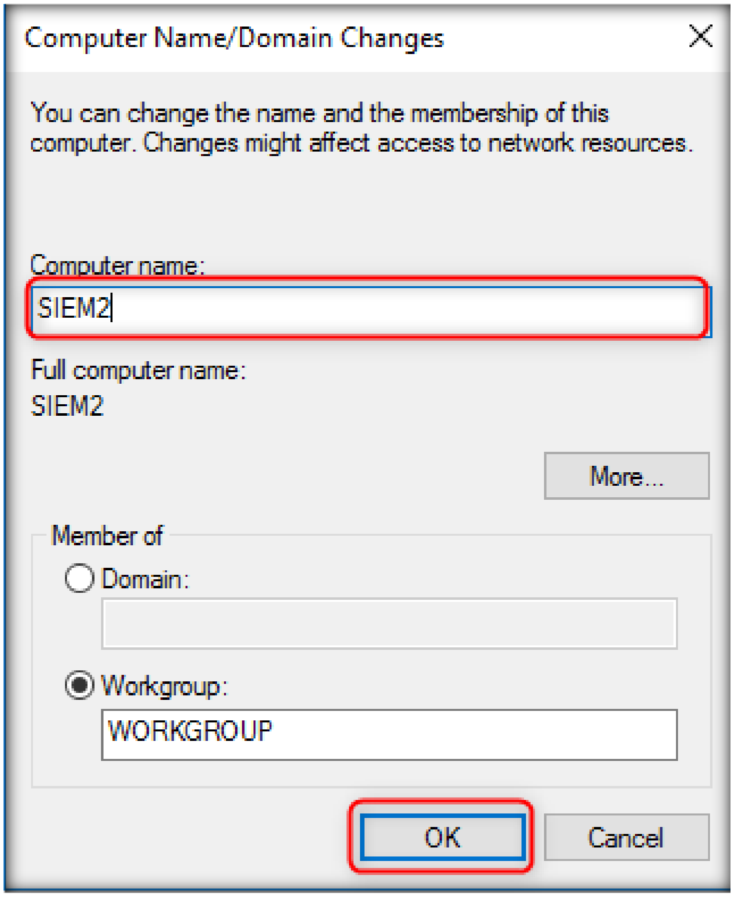
Full computer name: DESKTOP-QN9HOOF

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

4. In the Computer Name field enter **SIEM2** and click **OK**.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: SIEM2

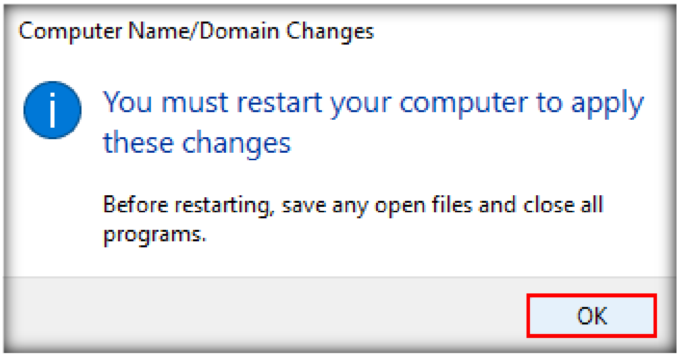
Full computer name:
SIEM2

Member of

○ Domain:

● Workgroup: WORKGROUP

5. When prompted to restart the system, click **OK**.

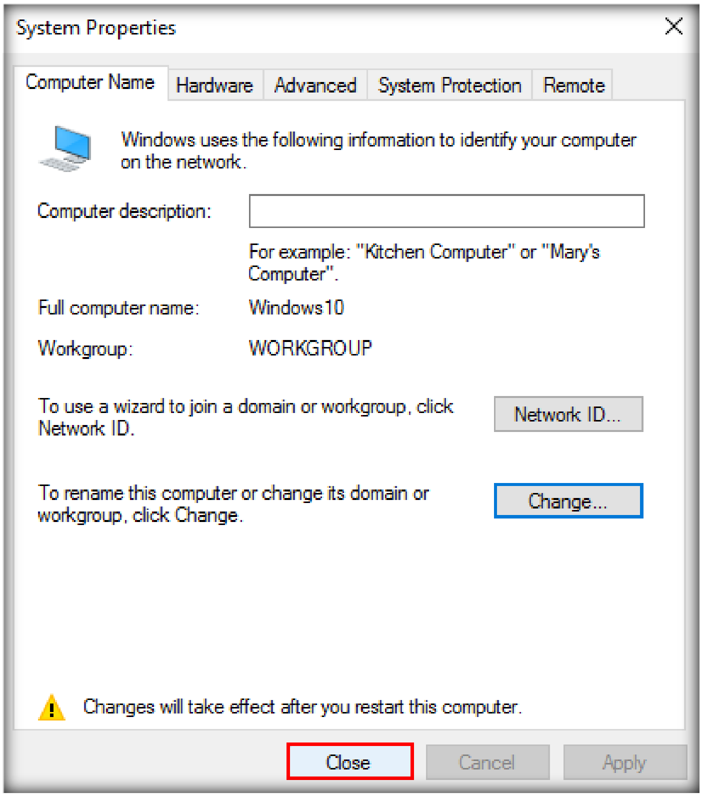


Computer Name/Domain Changes

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

6. You will be returned back to System Properties window, click **Close**.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Windows10

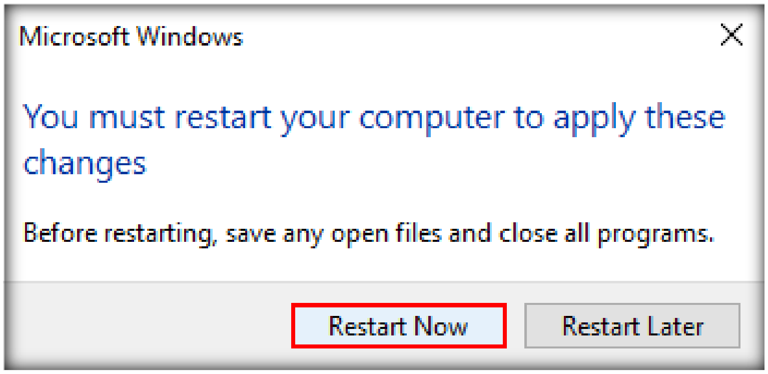
Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Changes will take effect after you restart this computer.

7. You will be prompted to restart the system, click **Restart Now**.



You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

CT#11.3: Configuring Static IP Address

1. Follow the steps as in the above Configuration Task, CT#8.4, to configure IPv4 address in the Windows 10 VM with the following values:
   - IP Address: **10.10.10.10**
   - Subnet Mask: **255.255.255.0**
   - Default Gateway: **10.10.10.2**
   - Preferred DNS server**: 8.8.8.8**

CT#11.4: Mapping SOC-Tools Folder from Host Machine to Windows 10 VM

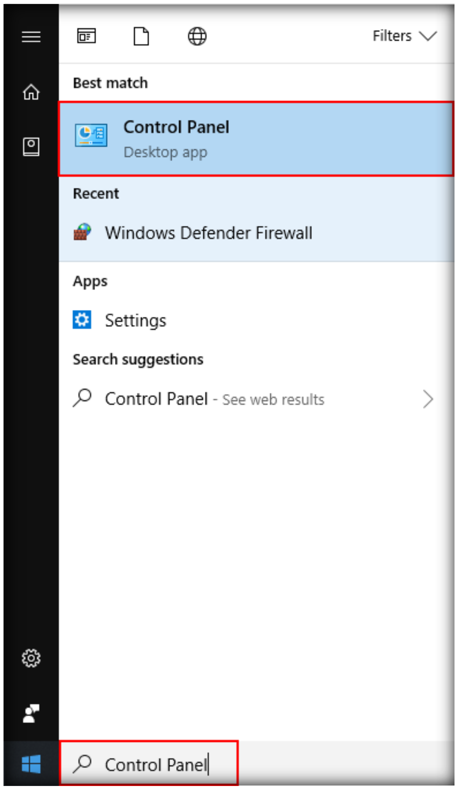
1. Follow CT#6.4, to share SOC-Tools directory in SIEM1 VM.

CT#11.5: Installing Web Browsers

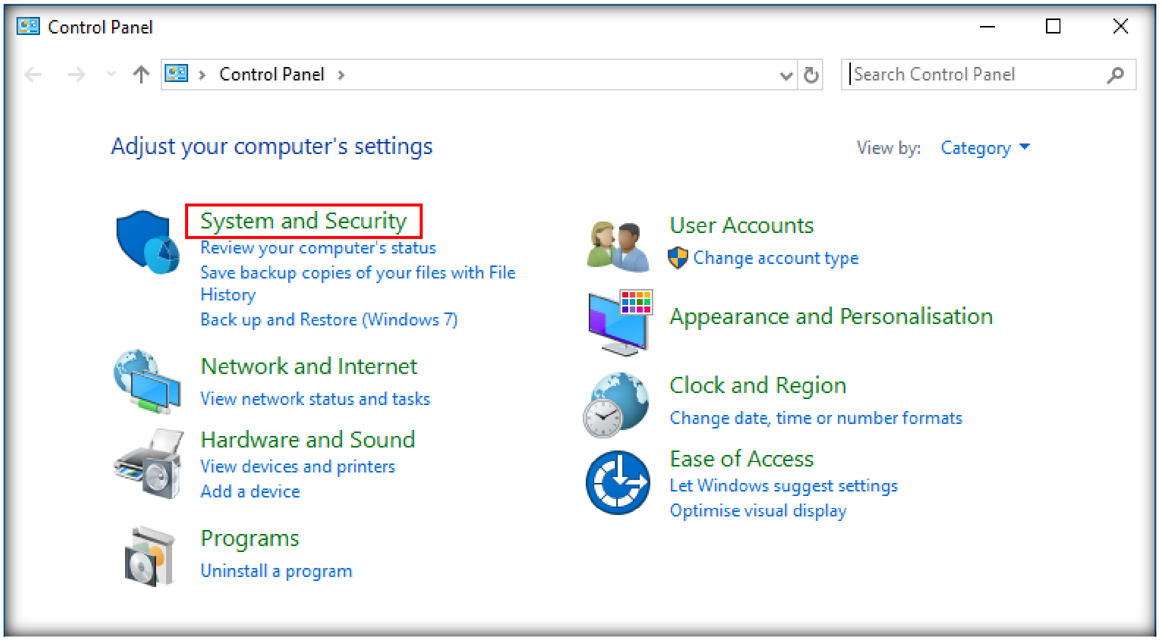
1. Follow the steps 1 to 4 of CT#6.6, to install web browser.

CT#11.6: Turn Off the Windows Defender Firewall

1. In the **Type here to search** field present at the lower left corner of the screen, type **Control Panel**. A search result containing **Control Panel** desktop app appears. Click **Control Panel**.

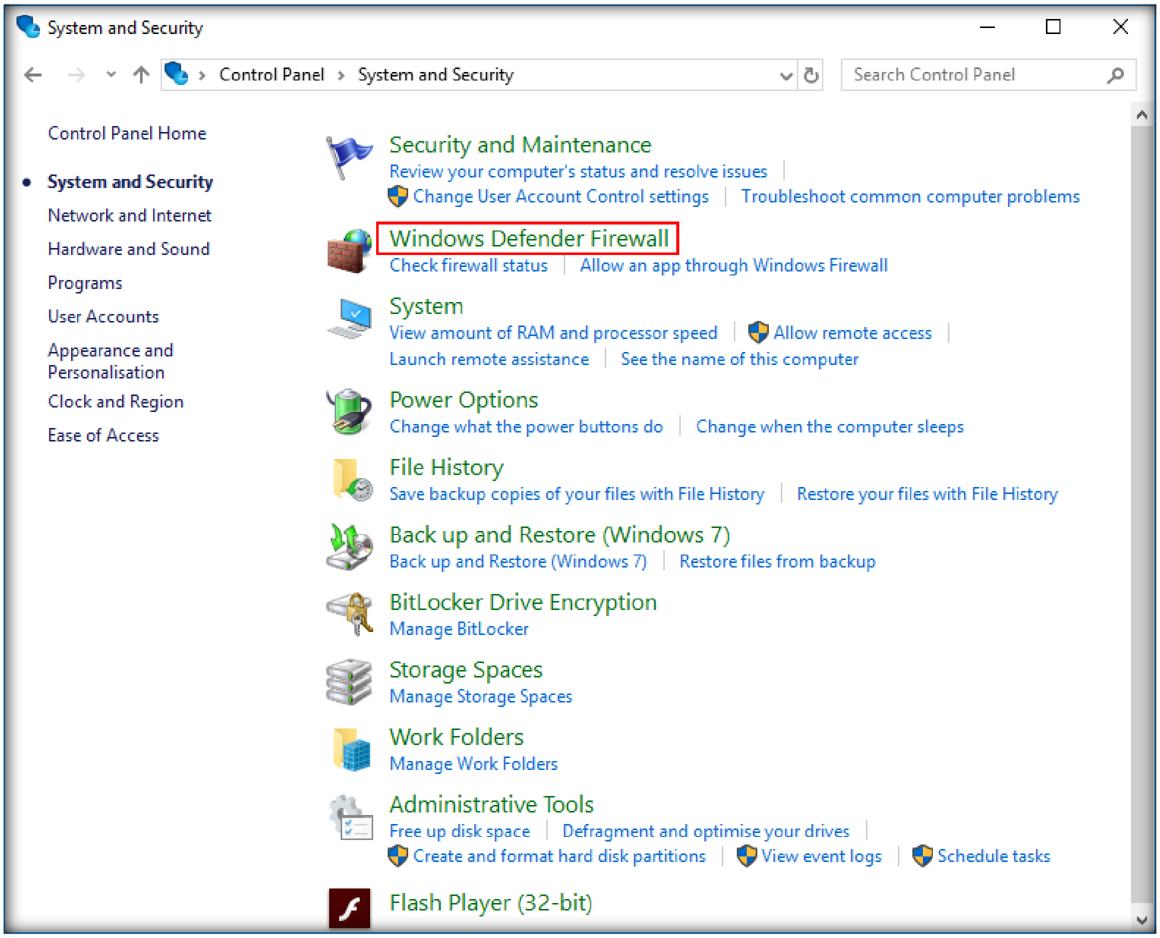


2. In the **Control Panel** window, click **System and Security**.



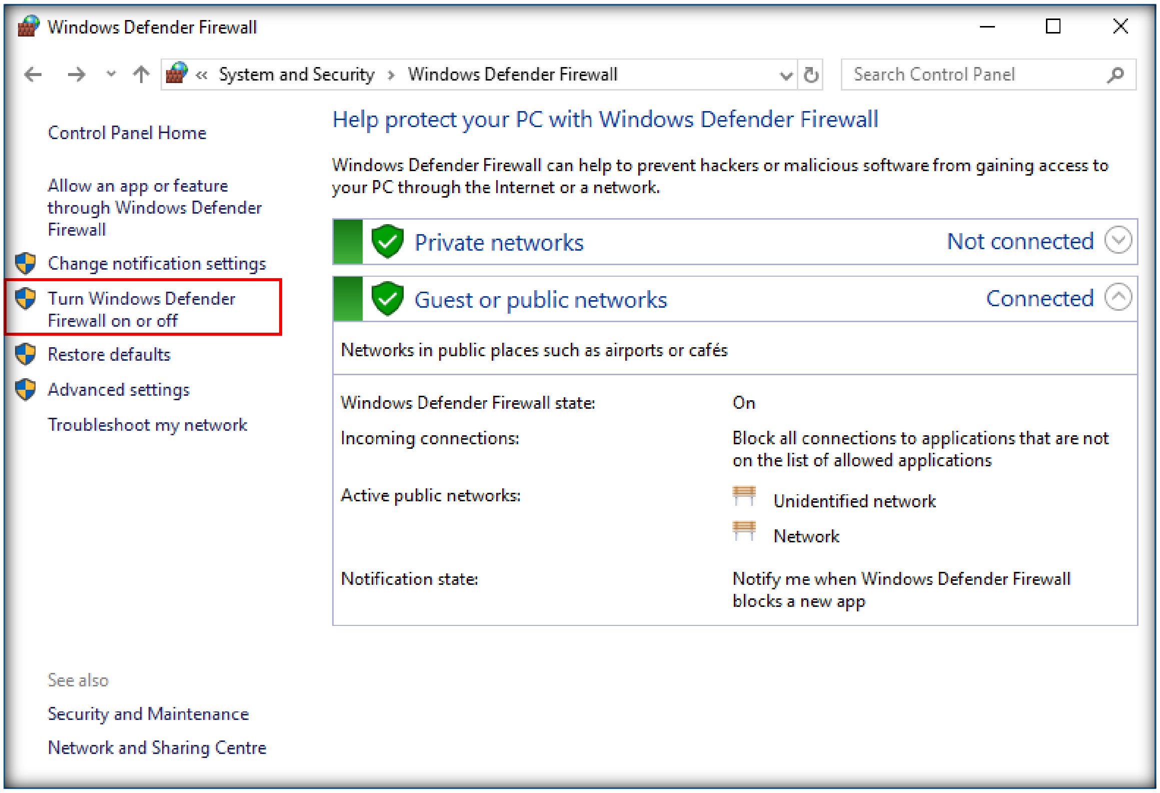
Control Panel
Control Panel ›
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Back up and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalisation
Clock and Region
Change date, time or number formats
Ease of Access
Let Windows suggest settings
Optimise visual display

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



System and Security
Control Panel › System and Security
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalisation
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Power Options
Change what the power buttons do
Change when the computer sleeps
File History
Save backup copies of your files with File History
Restore your files with File History
Back up and Restore (Windows 7)
Back up and Restore (Windows 7)
Restore files from backup
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Free up disk space
Defragment and optimise your drives
Create and format hard disk partitions
View event logs
Schedule tasks
Flash Player (32-bit)

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



Windows Defender Firewall
« System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Centre

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help to prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

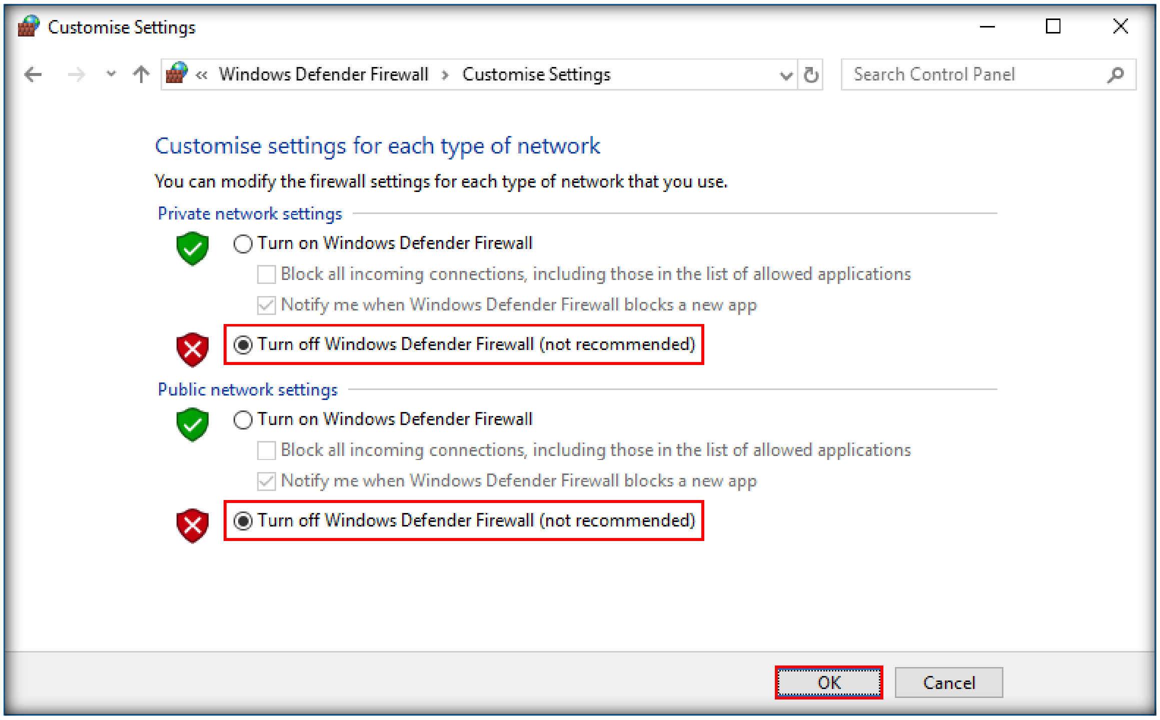
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or cafés

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to applications that are not on the list of allowed applications
Active public networks:	Unidentified network Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

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



Customise settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed applications

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

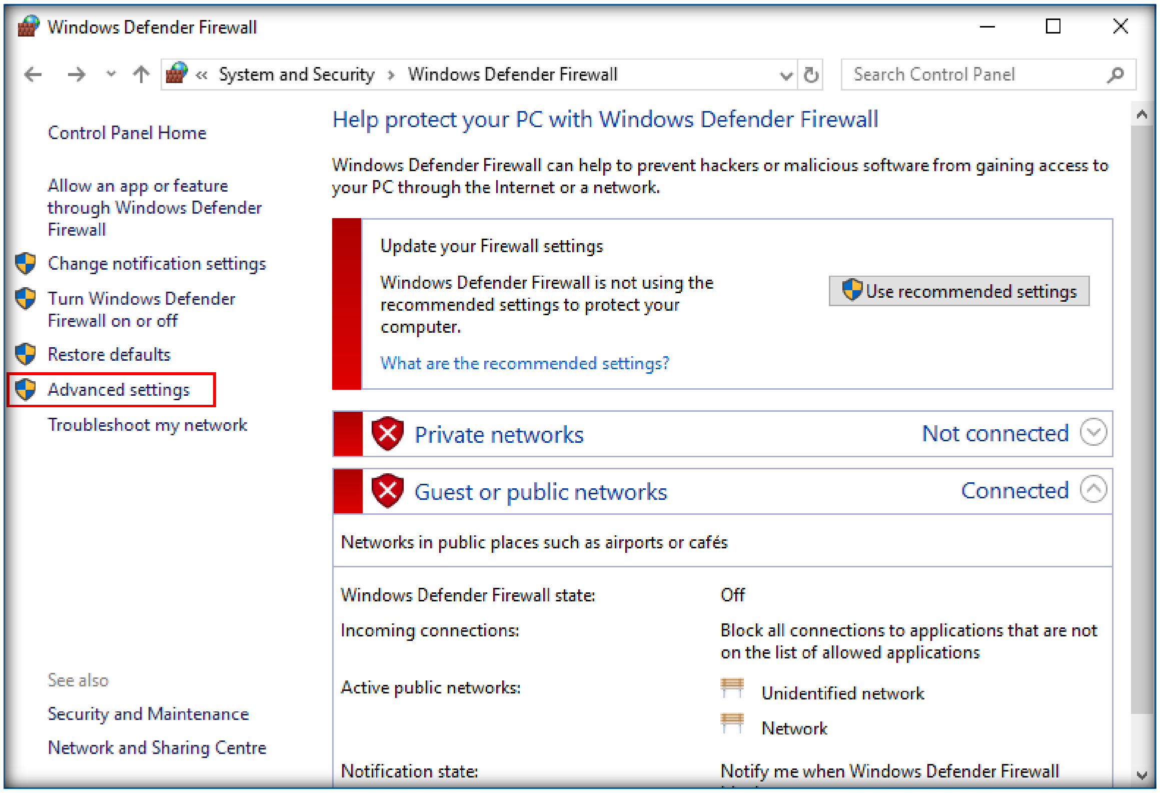
○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed applications

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

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


Windows Defender Firewall
System and Security > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Centre
Use recommended settings
What are the recommended settings?

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help to prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or cafés

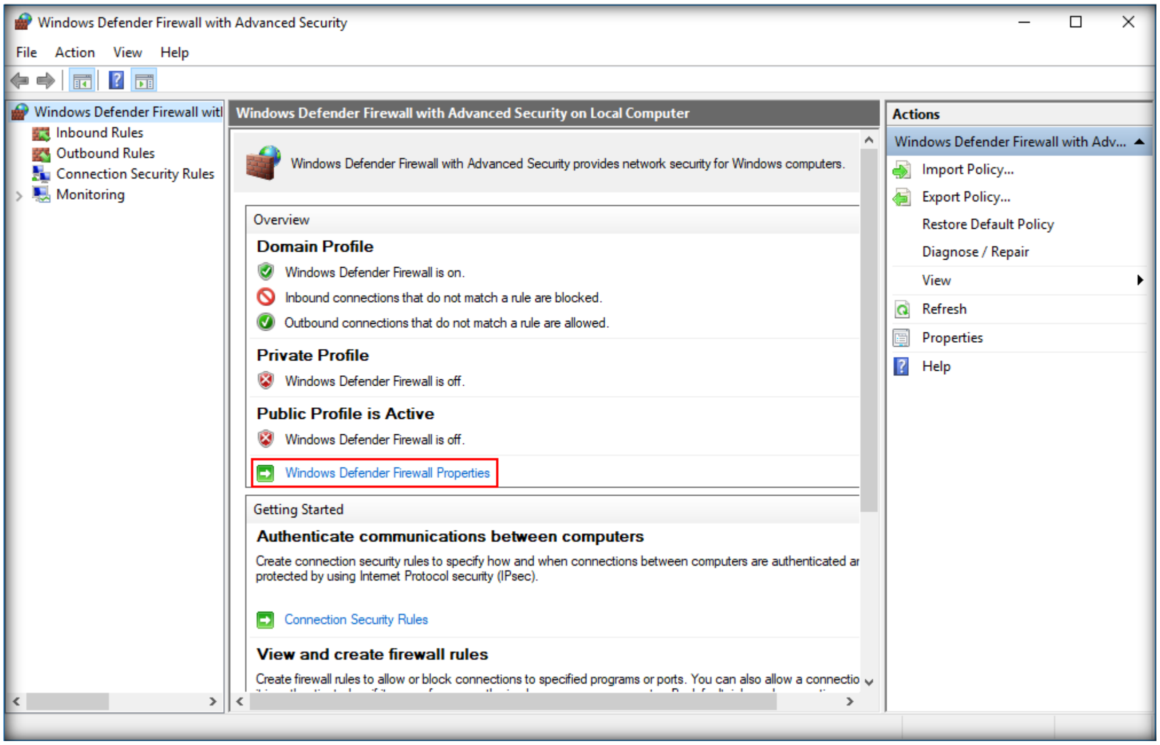
Windows Defender Firewall state: Off

Incoming connections: Block all connections to applications that are not on the list of allowed applications

Active public networks: Unidentified network; Network

Notification state: Notify me when Windows Defender Firewall

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


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Windows Defender Firewall with Adv...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
Windows Defender Firewall Properties
Connection Security Rules

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is off.

Public Profile is Active

- Windows Defender Firewall is off.

Getting Started

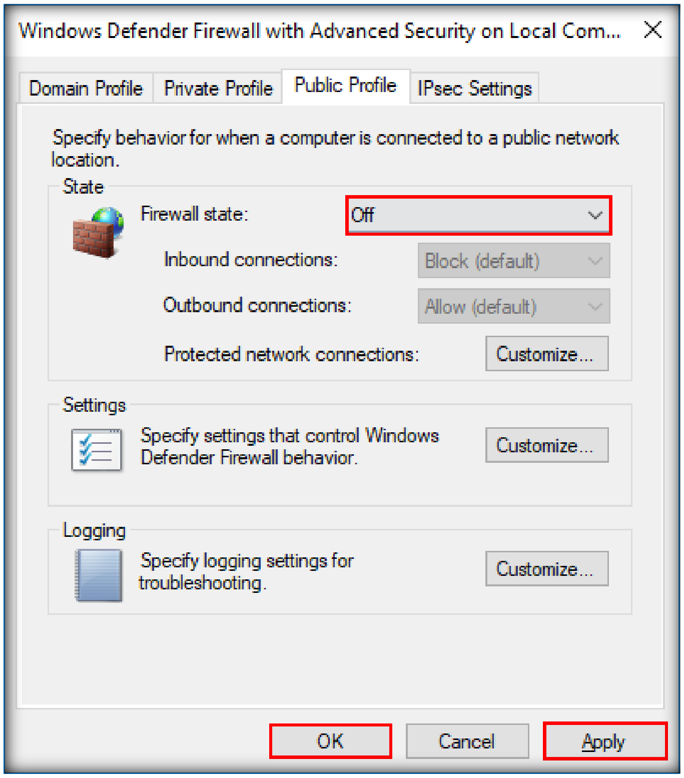
Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated ar protected by using Internet Protocol security (IPsec).

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connectio

8. 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 **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply** and then click **OK**.



Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior.

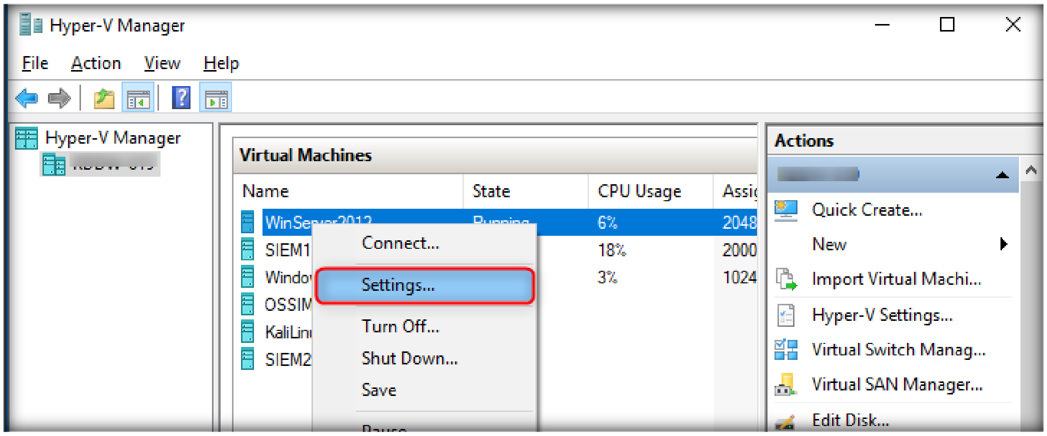
Logging

Specify logging settings for troubleshooting.

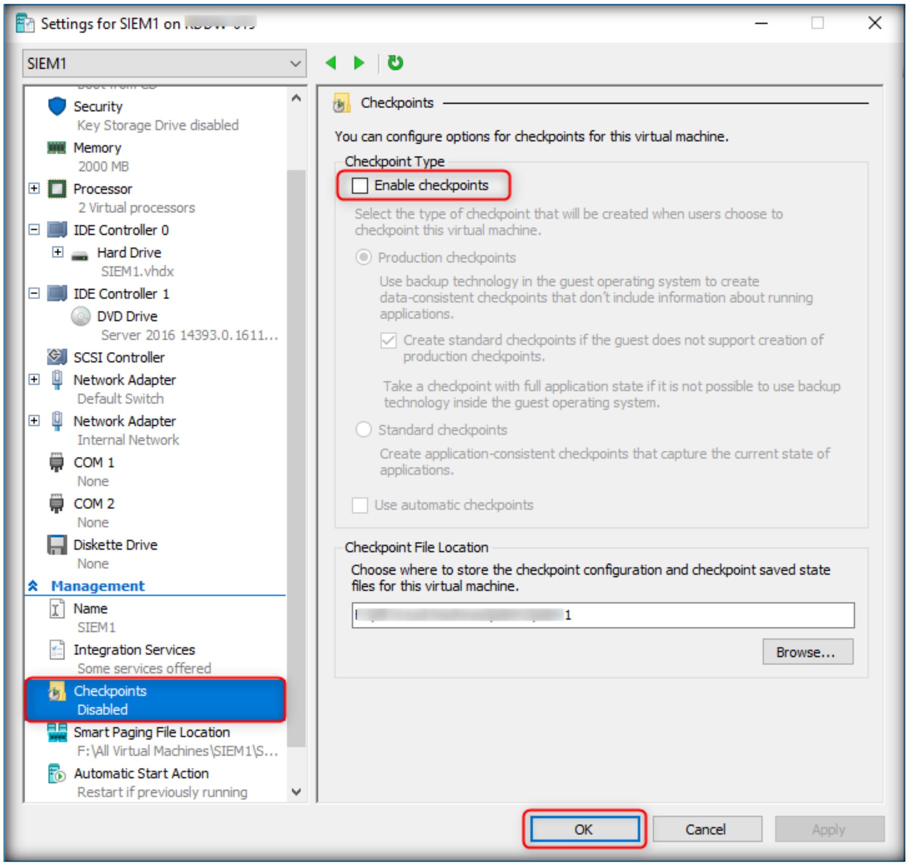
9. Close all the windows.

CT#12: Setting Checkpoints of Virtual Machines

1. After installing and configuring all the guest operating systems on virtual machines, set **disable Checkpoints** for all these virtual machines.
2. Open **Hyper-V Manager** right click on a virtual machine and click **Settings…**.



3. Click **Checkpoints** in left side pane then uncheck the **Enable checkpoints** check box, click **OK**.


Settings for SIEM1 on [redacted]

Checkpoints

You can configure options for checkpoints for this virtual machine.

Checkpoint Type

□ Enable checkpoints

Select the type of checkpoint that will be created when users choose to checkpoint this virtual machine.

● Production checkpoints

Use backup technology in the guest operating system to create data-consistent checkpoints that don't include information about running applications.

☑ Create standard checkpoints if the guest does not support creation of production checkpoints.

Take a checkpoint with full application state if it is not possible to use backup technology inside the guest operating system.

○ Standard checkpoints

Create application-consistent checkpoints that capture the current state of applications.

□ Use automatic checkpoints

Checkpoint File Location

Choose where to store the checkpoint configuration and checkpoint saved state files for this virtual machine.

[redacted]1

4. Perform this action for **all** the installed virtual machines.

CT#13: Setting Time Zone of Virtual Machines

1. Navigate to Date and Time Settings to ensure that all virtual machines Time zone configuration is same.

End of the Document