



CHFI

Classroom Lab Setup Guide

Table of Contents

Classroom Setup Instructions: CHFiv9	4
Classroom Requirements	5
Hardware.....	6
Software.....	7
Classroom Connectivity	8
Configuration.....	8
Setup Document Overview	8
Training Room Environment	8
Instructor's Computer.....	10
Student Workstations	12
Room Environment	13
Classroom Configuration.....	14
Network Topology	17
Computer Names.....	17
Instructor Acceptance	17
Firewall Settings	18
Blackboard	18
Setup Checklist	20
Instructor Acceptance	23
Assistance.....	23
Detailed Setup Instructions: Configuration Tasks (CT).....	24
CT#1: Set up Hardware.....	24
CT#2: Adding Hyper-V role in Server Manager of Windows Server 2012 Host Machine.....	25
CT#3: Configure Internal Network for Hyper-V.....	39
CT#4: Create a New Virtual Machine in Hyper-V.....	49

CT#5: Install Windows Server 2012 Operating System in Hyper-V	63
CT#6: Configure Internet Explorer (IE) Enhanced Security Configuration in Windows Server 2012 Virtual Machine	78
CT#7: Disable DEP in Windows Server 2012 Virtual Machine	81
CT#8: Configure Windows Explorer in Windows Server 2012 Virtual Machine	82
CT#9: Adding .NET Framework and Telnet Roles in Windows Server 2012 Virtual Machine	83
CT#10: Disable Server Manager in Windows Server 2012 Virtual Machine.....	94
CT#11: Install a Web Browser in Windows Server 2012 Virtual Machine	96
CT#12: Install WinRAR in Windows Server 2012 Virtual Machine	96
CT#13: Download CHFI Tools in Windows Server 2012 Virtual Machine	96
CT#14: Install Adobe Reader v11.0.10	97
CT#15: Install WinPcap 4.1.3 in Windows Server 2012 Virtual Machine	97
CT#16: Install Java SE Development Kit in Windows Server 2012 Virtual Machine.....	97
CT#17: Install Java SE Run Time Environment in Windows Server 2012 Virtual Machine	97
CT#18: Install and configure Android SDK Tools on Windows Server 2012 Virtual Machine.....	98
CT#19: Turn off Firewall in Windows Server 2012 and Windows 10 Virtual Machines	152
CT#20: Share CHFI-Tools folder as 'Z:\' drive (Mapping Z:\ drive).....	169
CT#21: Install Kali Linux in Hyper-V	184
CT#22: Install Ubuntu in Hyper-V	219
CT#23: Test for Pinging Each Other.....	241
CT#24: Create Checkpoints for all Virtual Machines	242

Classroom Setup Instructions: CHFIV9

This document contains setup instructions for the EC-Council Computer Hacking Forensic Investigator (CHFI) course. The course requires a standard modular classroom seating configuration, one computer for each student, one computer for the instructor, a dedicated hub or switch (hub preferred), dedicated firewall, and Internet connection. This class teaches computer forensics investigation methodologies. It is imperative that the network used for this class be separated both logically and physically from any other networks in the training facility to preclude students “accidentally” conducting exploits on other computers within accessible networks.

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

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

EC-Council Computer Hacking Forensic Investigator and CHFI 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 EC-Council Computer Hacking Forensic Investigator (CHFI) 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 (1 m x 2 m), or larger
- Markers, whiteboard, assorted colors
- Eraser, whiteboard cleaner liquid (3 oz minimum)
- Paper towels
- 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 and chair, ergonomic
 - Power outlet
 - Network jack
 - Projector, LCD, capable of 740 x 1280 pixels minimum w/all connecting cables
- Student station (per student)
 - Chair, ergonomic
 - 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 and student computers are identical:

- Intel® Core™ i5 or equivalent CPU with minimum CPU speed of 3.90 GHz
- 16 GB or more RAM
- Hard disk, 300 GB or larger, 7200 RPM or faster
- DVD drive (DVD R/W drive preferred)
- Two network adapters, 10/100 Mbps required, full duplex (disable any additional network adapters installed)
- Super VGA (SVGA) monitor, minimum 18.5-inch
- Mouse or compatible pointing device
- Sound card with amplified speakers
- Internet access
- BIOS boot up configuration set to DVD-ROM, hard disk 1 (C:\ drive)
- Wireless network adapter (PCI or USB)*

The following additional hardware is also required:

- Hub or unmanaged switch (hub preferred), 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.”
- Hardware firewall appliance (Cisco PIX, ASA, or equivalent)**

Software

All computers in the class require the following software:

- Windows Server 2012 R2 or later* (Standard Edition with GUI), fully patched
- MS Internet Information Server 8
- Microsoft .NET Framework 4.5
- Adobe Reader 11.0.10 or later version
- winrar-x64-54b1 or later version
- Web browsers: Internet Explorer, Firefox and Chrome
- WinPcap driver
- Word, Excel, and PowerPoint Viewers or Microsoft Office 2016
- Notepad++
- Java SE Run Time Environment
- Java SE Development Toolkit
- Android Software Development Toolkit
- Hyper-V (built-in role in **Windows Server 2012 R2** or later)
 - Microsoft Windows 10 with full patches applied
 - Kali Linux 2016 Rolling Release (x64) (downloadable at <http://cdimage.kali.org/kali-2016.1/kali-linux-2016.1-amd64.iso>)
 - Ubuntu Linux 16.04 LTS (x64) (downloadable at <http://ubuntu.excellmedia.net/releases/16.04.1/ubuntu-16.04.1-desktop-amd64.iso>)

*Hyper-V runs only on a **Windows Server 2012** 64-bit box

Classroom Connectivity

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

Configuration

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

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

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

Setup Document Overview

This document provides background information for technical staff responsible for setting up a training room facility for the CHFI 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	Windows Server 2012 R2 or later (Standard Edition with GUI)	Intel Core i5 CPU with 300 GB free disk space, 16 GB RAM, 2 NICs (disable or unplug extras), 18.5-inch monitor and cards to drive at 1366 x 768 (or at monitor's native resolution) and configured at 16 million colors, compatible mouse, and wireless card for Wi-Fi access
Student workstations	12	Windows 2012 Server R2 or later (Standard Edition with GUI)	Intel Core i5 CPU with 300 GB free disk space, 16 GB RAM, 2 NICs (disable or unplug extras), 18.5-inch monitor and cards to drive at 1366 x 768 (or at monitor's native resolution) and configured at 16 million colors, compatible mouse, and wireless card for Wi-Fi access

Instructor's Computer

The Instructor's computer must:

- Be installed with **Windows Server 2012 R2** or later (Enterprise Edition) with the latest service packs and full patches applied
- Be running **IP protocol**
- Configure the **logon account** with username: *Administrator*, password: *qwert@123* (lowercase)
- Configure **Hyper-V**, create **virtual machines** in Hyper-V, and install **guest operating systems: Windows Server 2012** (fully patched), **Windows 10** (fully patched), **Kali Linux 2016 rolling release** and **Ubuntu 16.04** (See [CT#2](#), [CT#4](#), [CT#5](#), [CT#21](#), and [CT#22](#) in the Configuration Tasks section)
- Have **PowerPoint**, **Word**, and **Excel Viewers** installed, or be installed with **Microsoft Office 2016** or later version in Windows Server 2012 virtual machine
- Be installed with a **wireless card** (USB or PCI)
- Have an **LCD projector** connected
- Have **internal switch** added and in Hyper-V Manager and configure the internal adapter (See [CT#3](#) in the Configuration Tasks section)
- Configure the default **Internet Explorer Enhanced Security Configuration** utility in **Start → All Programs → Administrative Tools → Server Manager** (See [CT#6](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Disable **DEP** in **Control Panel → System → Advanced System Settings → Performance Settings → Data Execution Prevention** (See [CT#7](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Set **Windows Explorer** in Windows Server 2012 and Windows 10 VMs to show all files, file types, and extensions (See [CT#8](#) in the Configuration Tasks section)
- Be installed with **Microsoft .Net Framework 4.5** or later version and Telnet roles in Windows Server 2012 virtual machine (See [CT#9](#) in the Configuration Tasks section)
- Disable Server Manager in Windows Server 2012 Virtual Machine (See [CT#10](#) in the Configuration Tasks section)
- Have installed the latest versions of a **web browser** (See [CT#11](#) in the Configuration Tasks section) in both Windows Server 2012 virtual machine

- Have **Adobe Reader 11.0.10** or later version and **winrar** latest version installed (both can be found in the **CHFIv9 Lab Prerequisites** directory in the **C:\CHFI-Tools** folder) (See [CT#14](#) and [CT#12](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Download CHFI Tools in Windows Server 2012 Virtual Machine (See [CT#13](#) in the Configuration Tasks section)
- Be installed with **WinPcap** drivers (See [CT#15](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Be installed with **Java SE Development Toolkit** (See [CT#16](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Be installed with **Java SE Run Time Environment** (See [CT#17](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Have Android SDK installed and configured in Windows Server 2012 virtual machine (See [CT#18](#) in the Configuration Tasks section) on Windows Server 2012 Virtual Machine
- Have the **firewall** turned off in all the Windows based machines (See [CT#19](#) in the Configuration Tasks section)
- Share **CHFI - Tools** folder in **C:** as the “**Z:**” drive (map Z:\ drive) (See [CT#20](#) in the Configuration Tasks section)
- Verify the Ping test between all the machines in your network (See [CT#23](#) in the Configuration Tasks section)
- Create Checkpoints for all Virtual Machines (See [CT#24](#) in the Configuration Tasks section)

Note: The use of ghost images is recommended to reduce setup time if computer failure occurs.

Student Workstations

The Student workstations must:

- Be installed with **Windows Server 2012 R2** or later (Enterprise Edition) with the latest service packs and full patches applied
- Be running **IP protocol**
- Configure the **logon account** with username: *Administrator*, password: *qwert@123* (lowercase)
- Configure **Hyper-V**, create **virtual machines** in Hyper-V, and install **guest operating systems: Windows Server 2012** (fully patched), **Windows 10** (fully patched), **Kali Linux 2016 rolling release** and **Ubuntu 16.04** (See [CT#2](#), [CT#4](#), [CT#5](#), [CT#21](#), and [CT#22](#) in the Configuration Tasks section)
- Have **PowerPoint**, **Word**, and **Excel Viewers** installed, or be installed with **Microsoft Office 2016** or later version in Windows Server 2012 virtual machine
- Be installed with a **wireless card** (USB or PCI)
- Have an **LCD projector** connected
- Have **internal switch** added and in Hyper-V Manager and configure the internal adapter (See [CT#3](#) in the Configuration Tasks section)
- Configure the default **Internet Explorer Enhanced Security Configuration** utility in **Start → All Programs → Administrative Tools → Server Manager** (See [CT#6](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Disable **DEP** in **Control Panel → System → Advanced System Settings → Performance Settings → Data Execution Prevention** (See [CT#7](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Set **Windows Explorer** in Windows Server 2012 and Windows 10 virtual machines to show all files, file types, and extensions (See [CT#8](#) in the Configuration Tasks section)
- Be installed with **Microsoft .Net Framework 4.5** or later version and Telnet roles in Windows Server 2012 virtual machine (See [CT#9](#) in the Configuration Tasks section)
- Disable Server Manager in Windows Server 2012 Virtual Machine (See [CT#10](#) in the Configuration Tasks section)
- Have installed the latest versions of a **web browser** (See [CT#11](#) in the Configuration Tasks section) in both Windows Server 2012 virtual machine
- Have **Adobe Reader 11.0.10** or later version and **winrar** latest version installed (both can be found in the **CHFIv9 Lab**)

Prerequisites directory in the **C:\CHFI-Tools** folder) (See [CT#14](#) and [CT#12](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine

- Download CHFI Tools in Windows Server 2012 Virtual Machine (See [CT#13](#) in the Configuration Tasks section)
- Be installed with **WinPcap** drivers (See [CT#15](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Be installed with **Java SE Development Toolkit** (See [CT#16](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Be installed with **Java SE Run Time Environment** (See [CT#17](#) in the Configuration Tasks section) in Windows Server 2012 virtual machine
- Have Android SDK installed and configured in Windows Server 2012 virtual machine (See [CT#18](#) in the Configuration Tasks section) on Windows Server 2012 Virtual Machine
- Have the **firewall** turned off in all the Windows based machines (See [CT#19](#) in the Configuration Tasks section)
- Share **CHFI - Tools** folder in **C:** as the “**Z:**” drive (map Z:\ drive) (See [CT#20](#) in the Configuration Tasks section)
- Verify the Ping test between all the machines in your network (See [CT#23](#) in the Configuration Tasks section)
- Create Checkpoints for all Virtual Machines (See [CT#24](#) in the Configuration Tasks section)

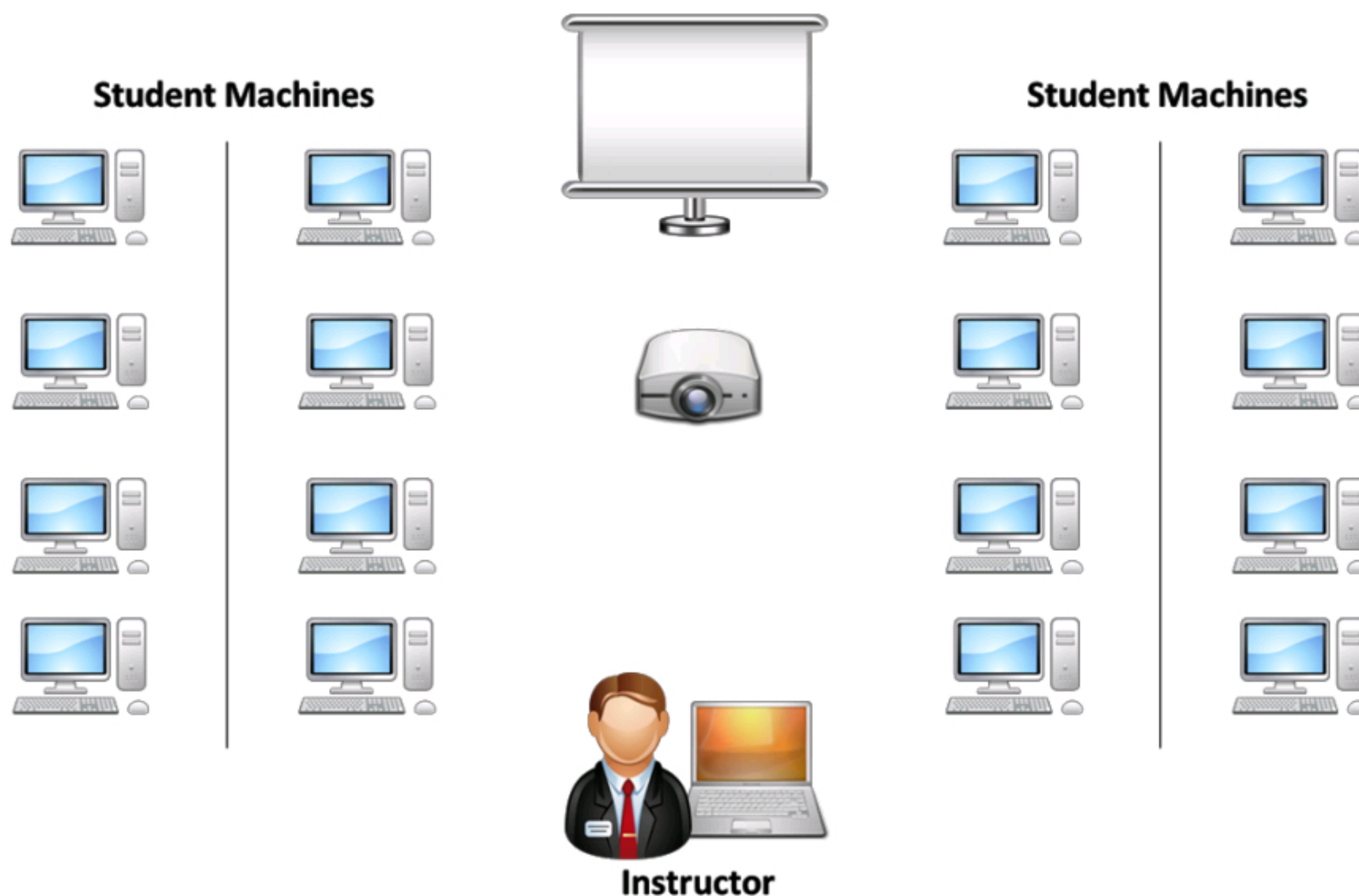
Note: The use of ghost images is recommended to reduce setup time if computer failure occurs.

Room Environment

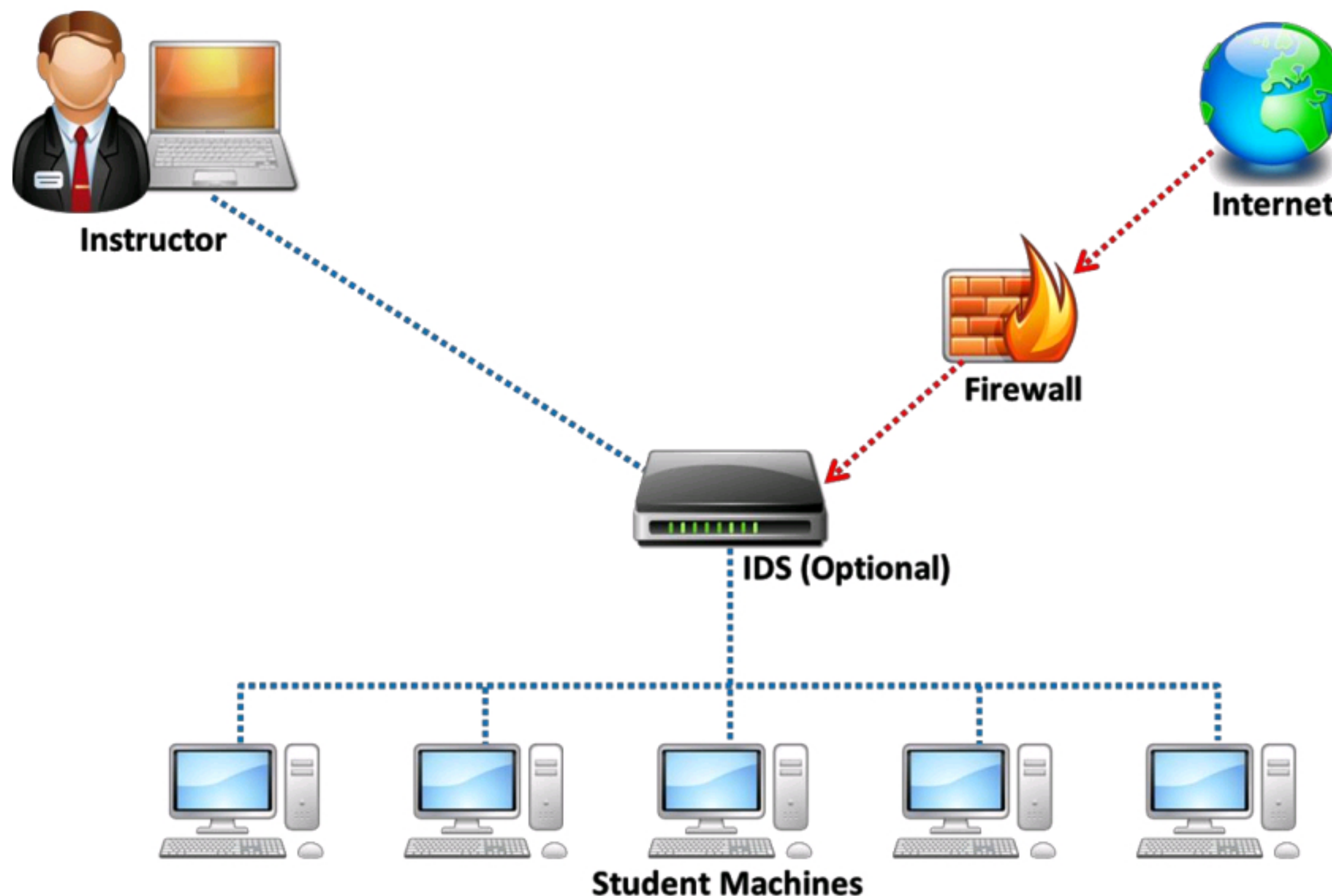
- The room must contain a whiteboard measuring a minimum of 3 feet by 6 feet in length (1 meter by 2 meters)
- The room should contain an easel and large tablet (optional)
- The room must be equipped with legible black and blue felt-tip pens (chisel tip, not fine-point)

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 the instructor easy access to “trouble spots,” and allows students to break into functional small and large teams.

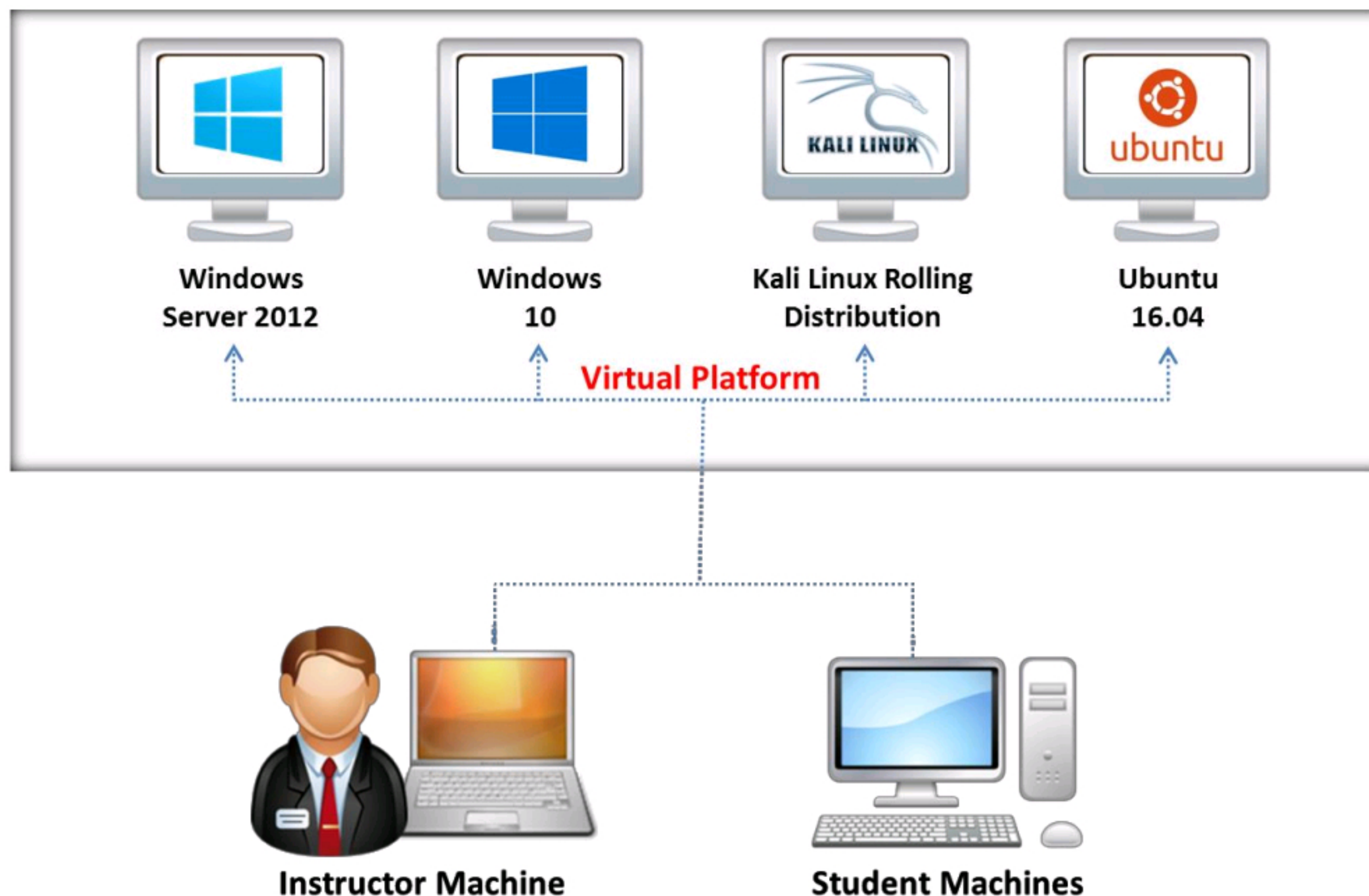


Instructor and Student Machine Operating System: Windows Server 2012 (Fully Patched)



Instructor and Student Machine Operating System: Windows Server 2012 (Fully Patched)

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 forensics tools in the trainer slides. The instructors are encouraged to demonstrate and guide the students on the use of the forensics tools. Please feel free to include your own exercises.



Instructor and Student Machine Operating System: Windows Server2012 (Fully Patched)

Network Topology

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

The training room must also have a wireless network to demonstrate wireless labs. The wireless network should be configured to use WEP keys for demonstration purposes. This network could be a part of the above network subnet. Configure the wireless router for DHCP server scope.

Computer Names

Assign computer names to student machines like CHFISTUDENT1, CHFISTUDENT2, CHFISTUDENT3, and so on. Name the instructor machine 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 checklist before the training setup is deemed acceptable.

Firewall Settings

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

Blackboard

- Write the following on the blackboard in the 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, in bold:

Welcome to CHFIv9 Class!

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

Welcome to CHFIv9 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 also validate that the setup has been done correctly. Before beginning the setup checklist, log off any connected users.

Check Here	Setup Verification Tasks
<input type="checkbox"/>	Open Network Neighborhood and verify that all classroom computers are visible in Network Neighborhood
<input type="checkbox"/>	Verify that the Instructor computer can display through the overhead projector
<input type="checkbox"/>	Cable wiring is organized and labeled
<input type="checkbox"/>	Student workstations and chair placement are satisfactory
<input type="checkbox"/>	Placement of LCD (overhead) projector is appropriate
<input type="checkbox"/>	Whiteboard and dry erase markers and erasers are available
<input type="checkbox"/>	Instructor station is properly organized and oriented
<input type="checkbox"/>	Computers are labeled with client numbers
<input type="checkbox"/>	EC-Council Courseware (Official EC-Council CHFIv9 box) is available for students
<input type="checkbox"/>	Write down the facility's technical contact person's phone number to call in the event of a network problem
<input type="checkbox"/>	Verify each computer has 300 GB or more free disk space
<input type="checkbox"/>	Verify that every host machine in the classroom has four VMs installed and configured
<input type="checkbox"/>	Verify that internal network adapter is configured on host machine and virtual machines
<input type="checkbox"/>	Verify you can successfully boot the virtual machines in Hyper-V
<input type="checkbox"/>	Verify that the forensics tools are on the Windows Server 2012 VM in C:\CHFI-Tools folder
<input type="checkbox"/>	Verify that Internet Explorer Enhanced Security Configuration is removed from Server Manager of Windows Server 2012 VM
<input type="checkbox"/>	Verify that DEP in Control Panel is disabled in Windows Server 2012 VM

<input type="checkbox"/>	Verify that Windows Explorer is set to show all files and file types, including hidden files and extensions in Windows Server 2012 and Windows 10 VMs
<input type="checkbox"/>	Verify that .NET Framework is installed and Telnet roles are added in Windows Server 2012 virtual machine
<input type="checkbox"/>	Verify that Server Manager is disabled in Windows Server 2012 virtual machine
<input type="checkbox"/>	Verify that Internet access is available in the virtual machines
<input type="checkbox"/>	Verify that a web browser is installed in Windows Server 2012 virtual machine
<input type="checkbox"/>	Visit https://www.eccouncil.org and view the page to check Internet access
<input type="checkbox"/>	Open Command Prompt and type nslookup certifiedhacker.com and look for connection to the server
<input type="checkbox"/>	Verify that WinRAR is installed in Windows Server 2012 virtual machine
<input type="checkbox"/>	Download CHFI-Tools to C:\ in Windows Server 2012 virtual machine
<input type="checkbox"/>	Verify Microsoft PowerPoint, Word, and Excel Viewers are installed (or Microsoft Office 2016 is installed)
<input type="checkbox"/>	Verify Adobe Reader, Java SE Development Toolkit and Java SE Run Time Environment are installed in Windows Server 2012 virtual machine
<input type="checkbox"/>	Verify WinPcap drivers are installed in Windows Server 2012 virtual machine
<input type="checkbox"/>	Install and Configure Android SDK in Windows Server 2012 virtual machine
<input type="checkbox"/>	Verify the firewall is turned off in all the Windows machines
<input type="checkbox"/>	Share CHFI-Tools folder as 'Z:\' drive (Mapping Z:\ drive)
<input type="checkbox"/>	Test for Pinging Each Other
<input type="checkbox"/>	Create Checkpoints for all Virtual Machines

Notes:

- You might want to create ghost images of the instructor and student machines so that the future installations become easier.
- You can restore checkpoint anytime during the class. Many Trojans and rootkits replace the system files, and you will need to restore by restoring the checkpoint.
- Have one additional student machine available as a standby. If a student computer cannot boot up because of a virus/Trojan infection, then you will be able to replace the student machine with this backup.

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 to ensure that the classroom and setup meet EC-Council standards. Any deficiencies the instructor discovers 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 CHFI class, please email partnersupport@eccouncil.org.

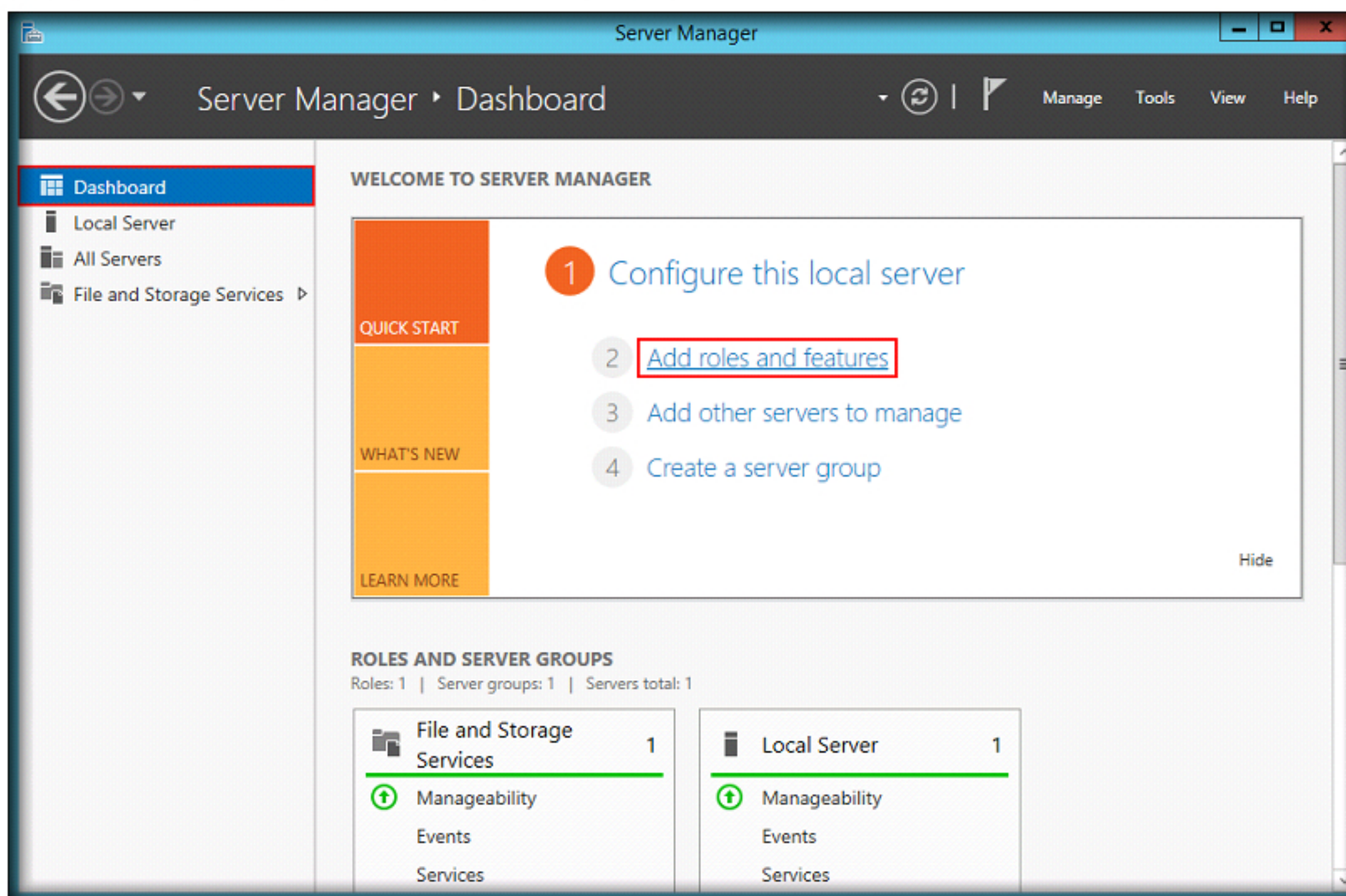
Detailed Setup Instructions: Configuration Tasks (CT)

CT#1: Set up Hardware

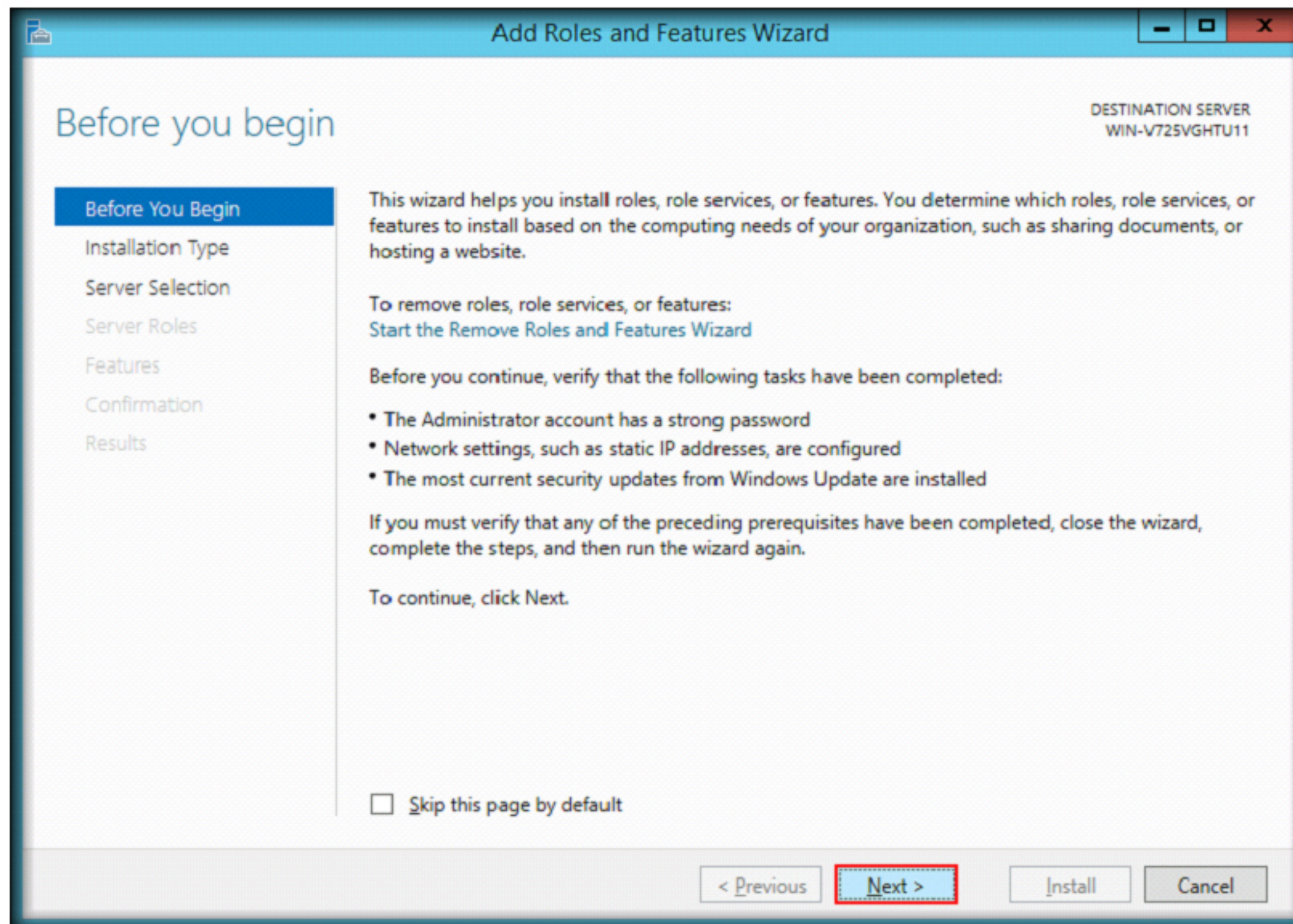
1. Set the computer's BIOS to start first from the **DVD-ROM** drive then hard drive (Drive C:\)
2. Now keep Windows Server 2012 DVD in the DVD-ROM
3. Configure the hard disk to have one **active primary partition** (C:\ of 50 GB) and two **extended logical partitions** (D:\ of 50GB and E:\ of 200GB)
4. Follow the steps to install Windows Server 2012
5. Install the **wireless network adapters** according to manufacturer's instructions

CT#2: Adding Hyper-V role in Server Manager of Windows Server 2012 Host Machine

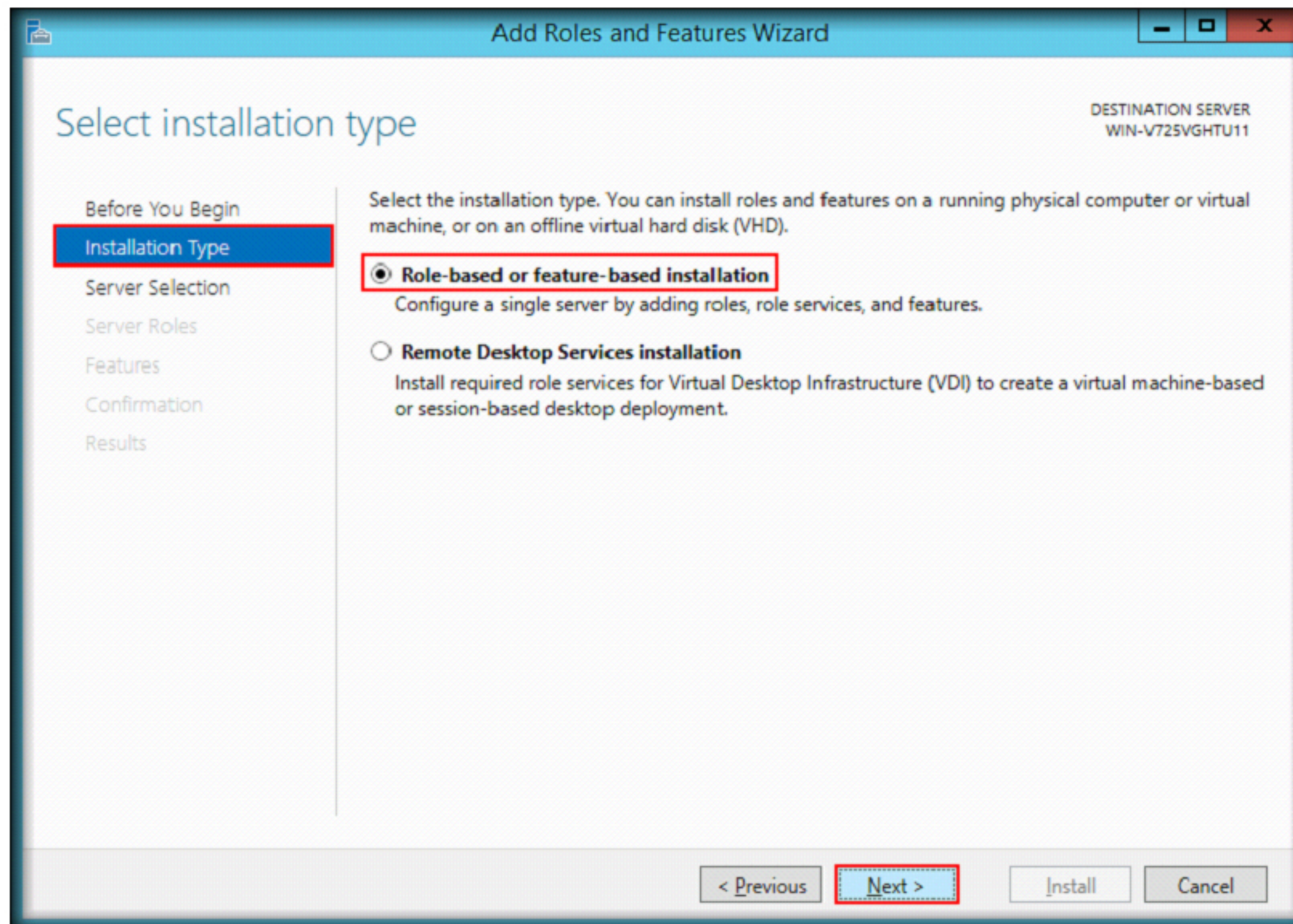
1. To open Server Manager, click **Start → Server Manager App**
2. In Server Manager **Dashboard**, click **Add Roles and Features**



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



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



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

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. In the top right corner, it says 'DESTINATION SERVER WIN-V725VGHTU11'. On the left, a navigation pane lists the steps: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted with a red box), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the instruction 'Select a server or a virtual hard disk on which to install roles and features.' with two radio buttons: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Below this is a 'Server Pool' section with a 'Filter:' text box and a table. The table has three columns: 'Name', 'IP Address', and 'Operating System'. It contains one row: 'WIN-V725VGHTU11', '192.168.0.114', and 'Microsoft Windows Server 2012 R2 Standard'. Below the table, it says '1 Computer(s) found'. A note at the bottom states: '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.' At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'.

DESTINATION SERVER
WIN-V725VGHTU11

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

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:

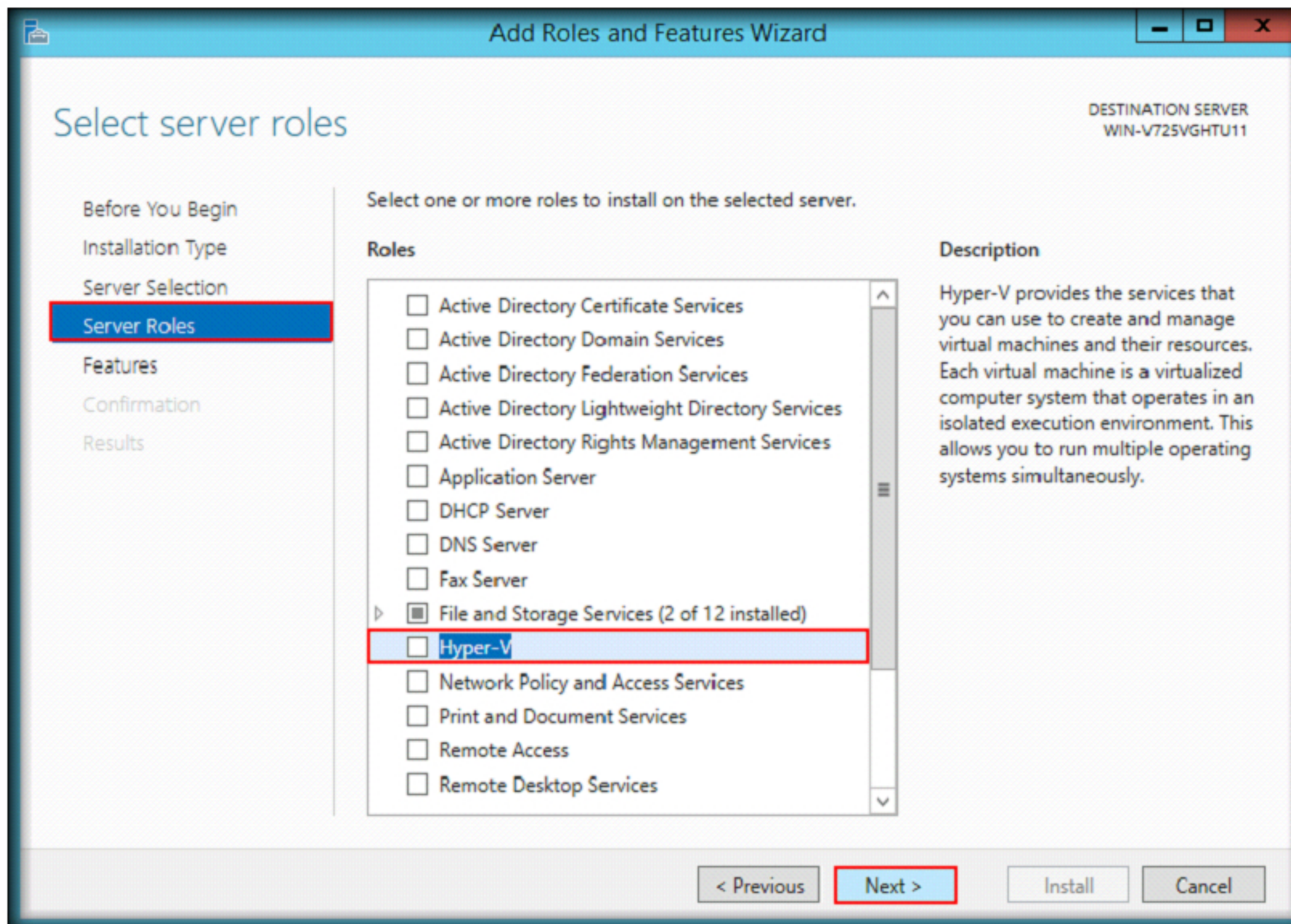
Name	IP Address	Operating System
WIN-V725VGHTU11	192.168.0.114	Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

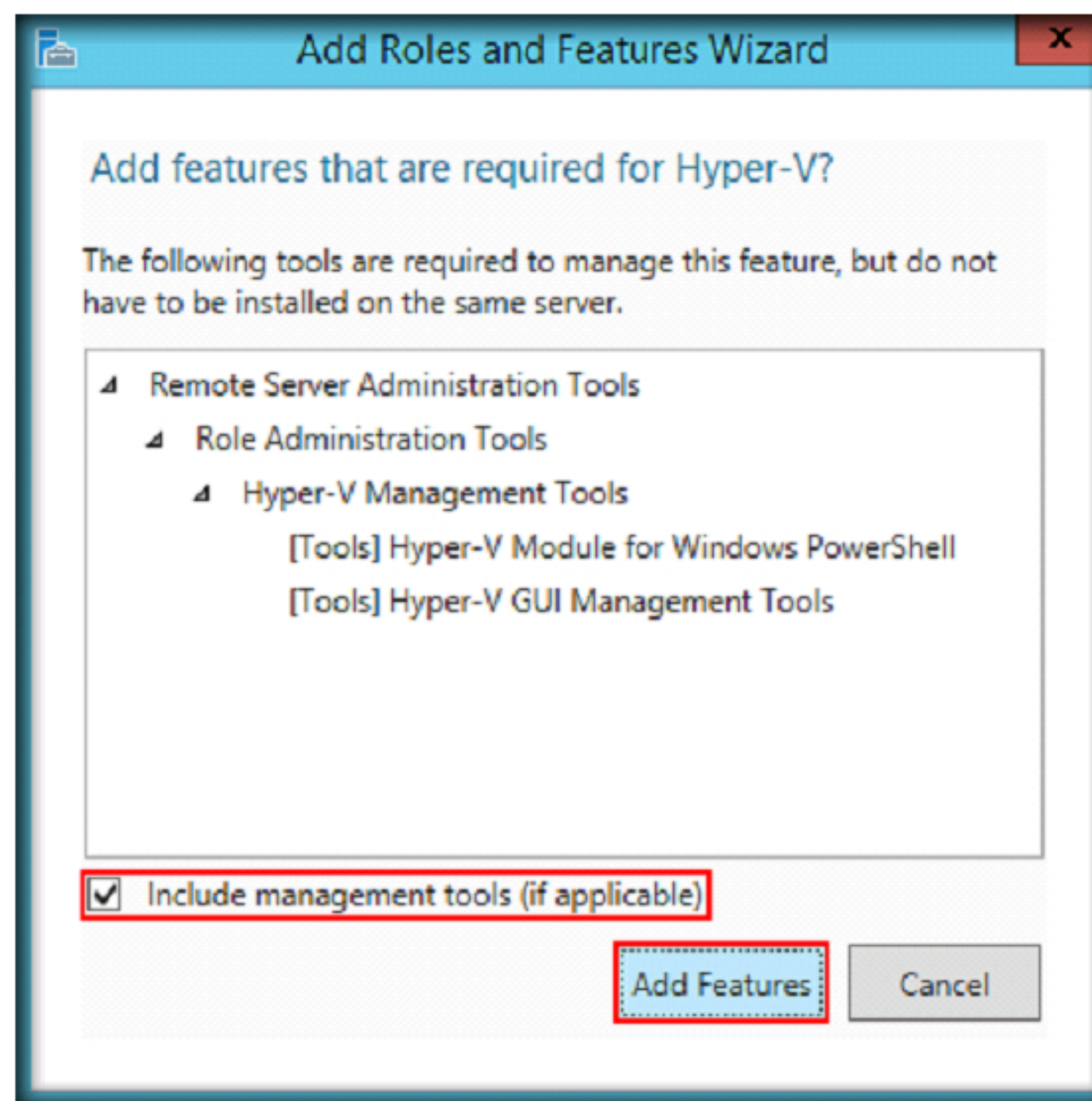
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous **Next >** Install Cancel

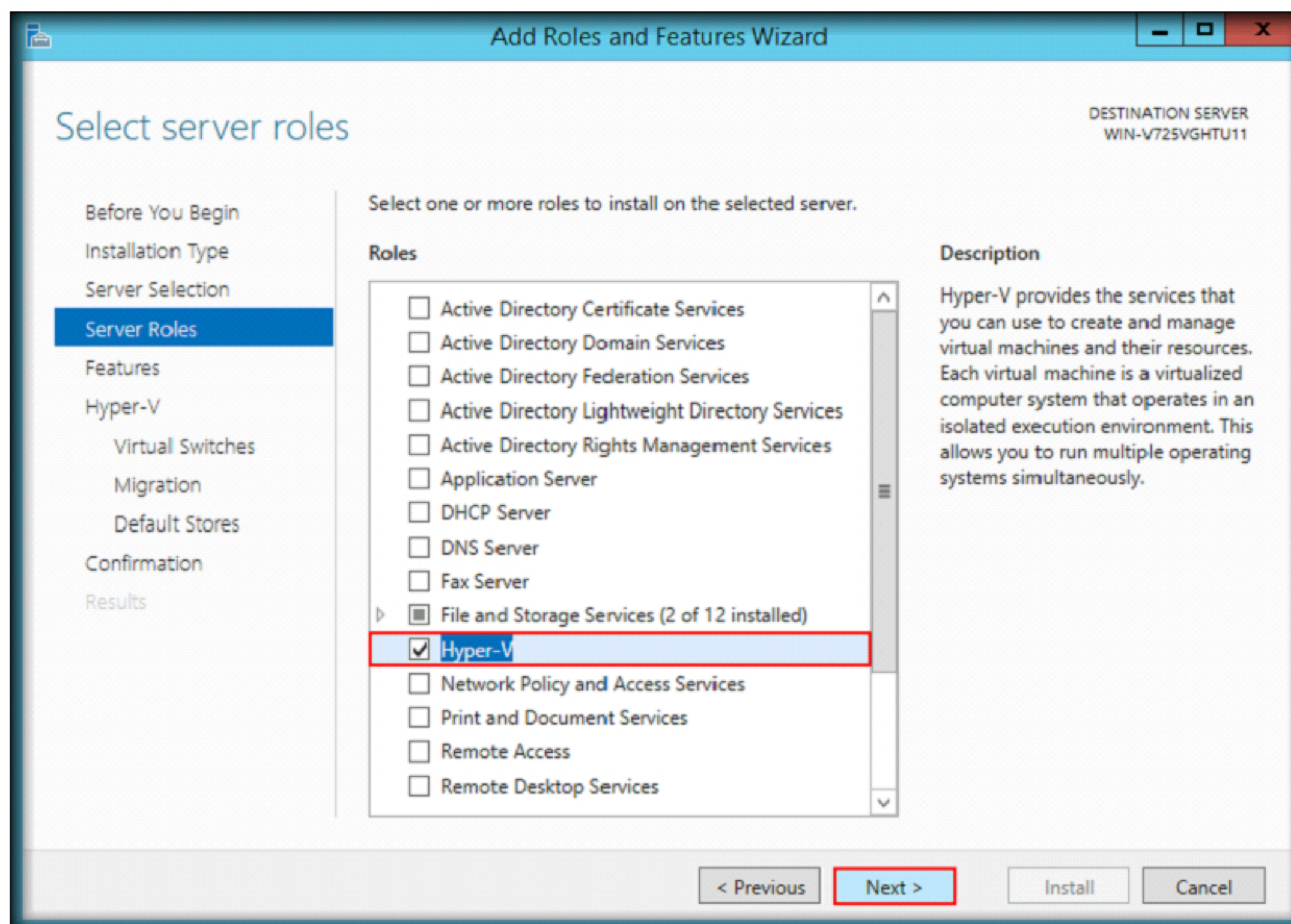
6. Check the **Hyper-V** role in **Server Roles** section



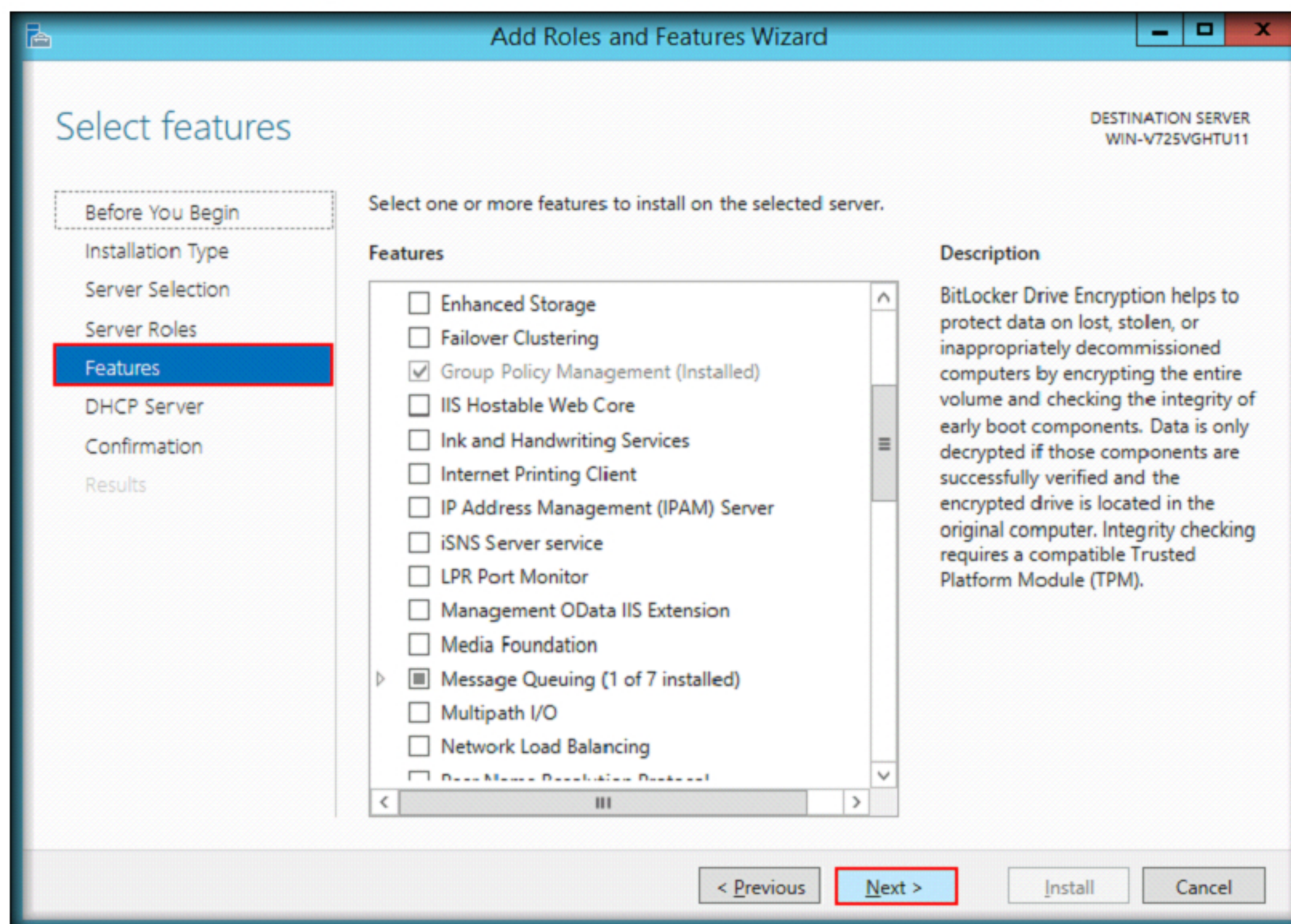
7. **Add Roles and Features wizard** for Hyper-V will appear. Click **Add Features**



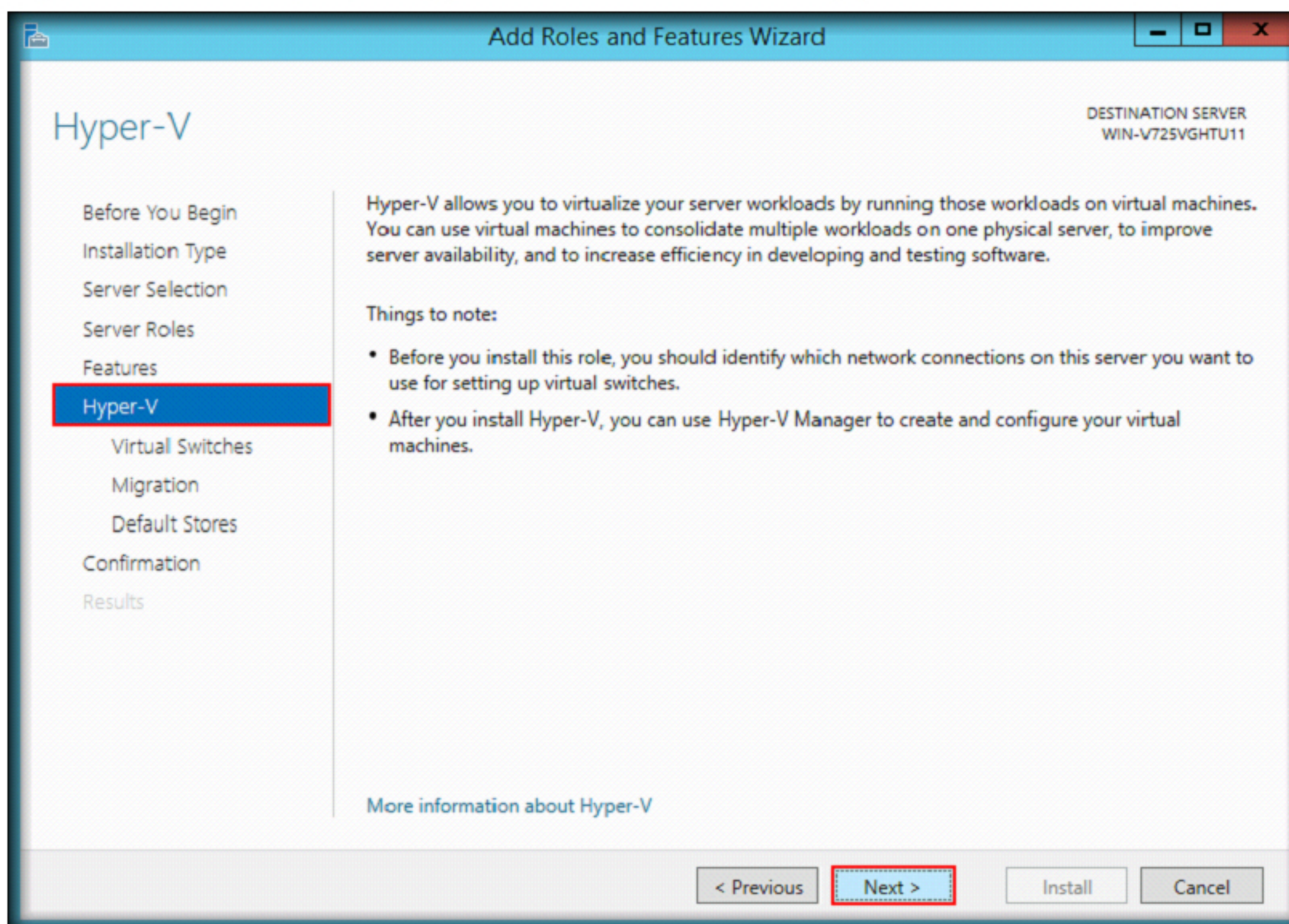
8. You will observe that the Hyper-V server role option is checked. Click **Next**



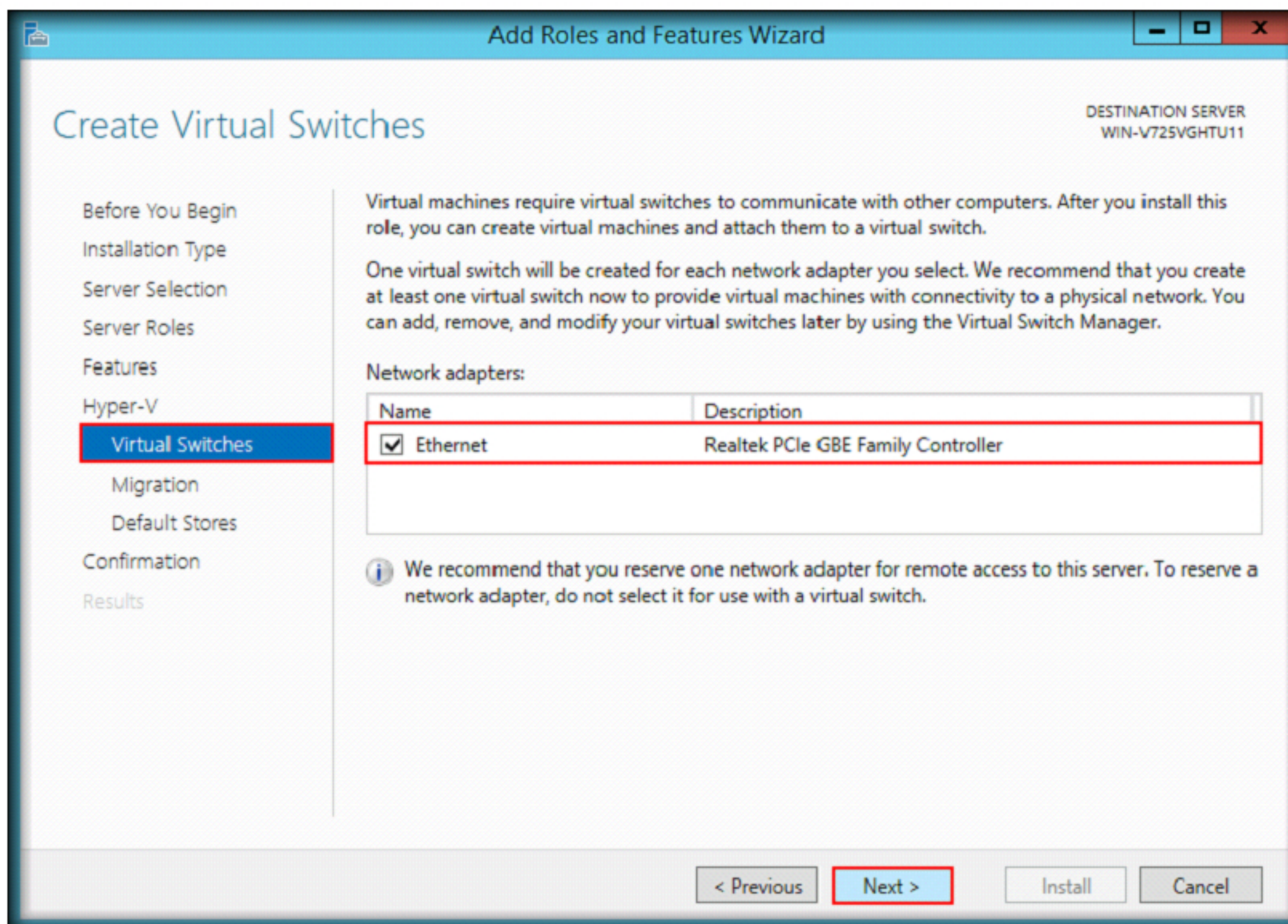
9. **Add Roles and Features Wizard** will appear for **Features** selection; click Next without selecting any role



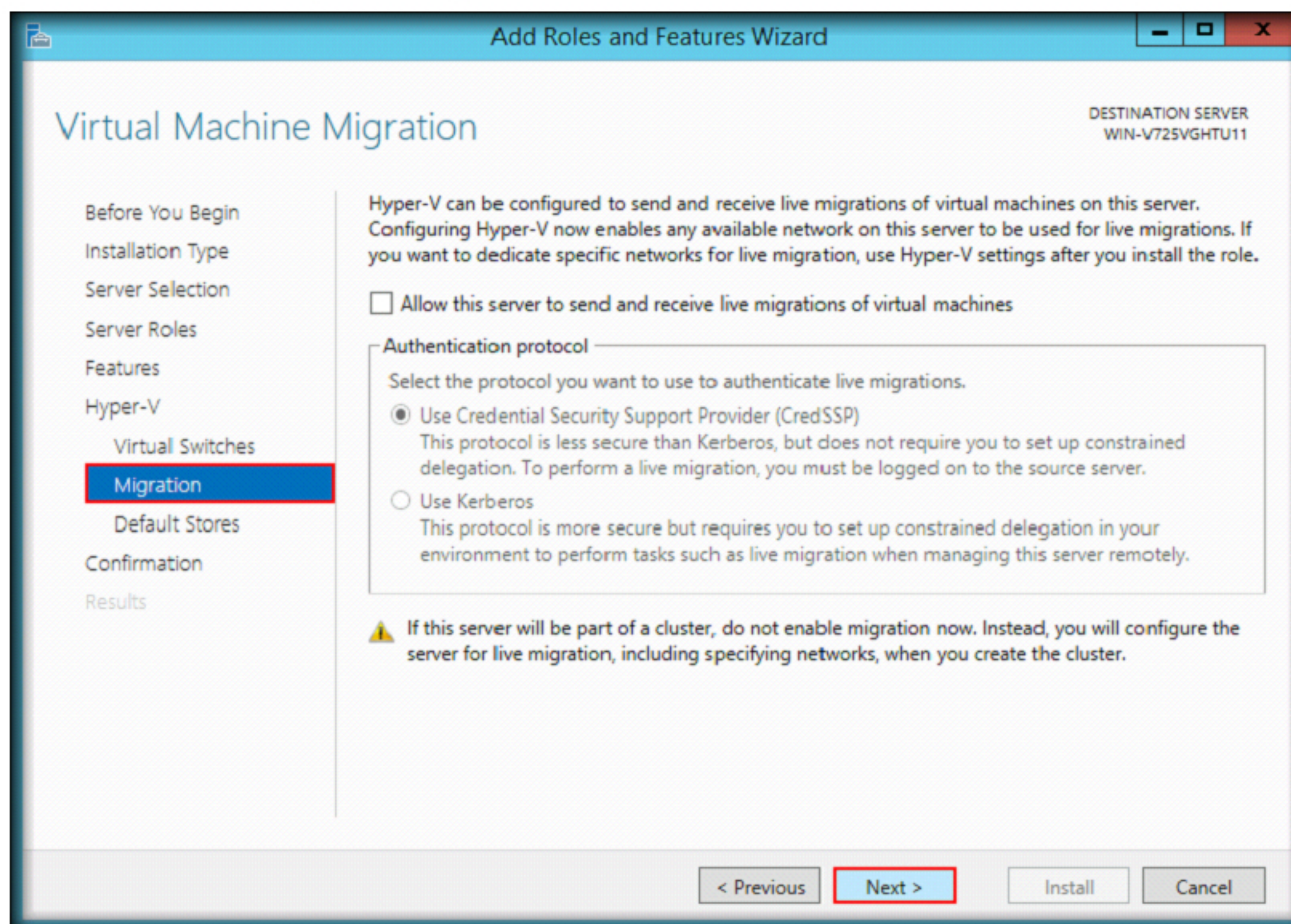
10. **Hyper-V** section appears in the wizard, explaining the detailed information for **Hyper-V**. Click **Next**



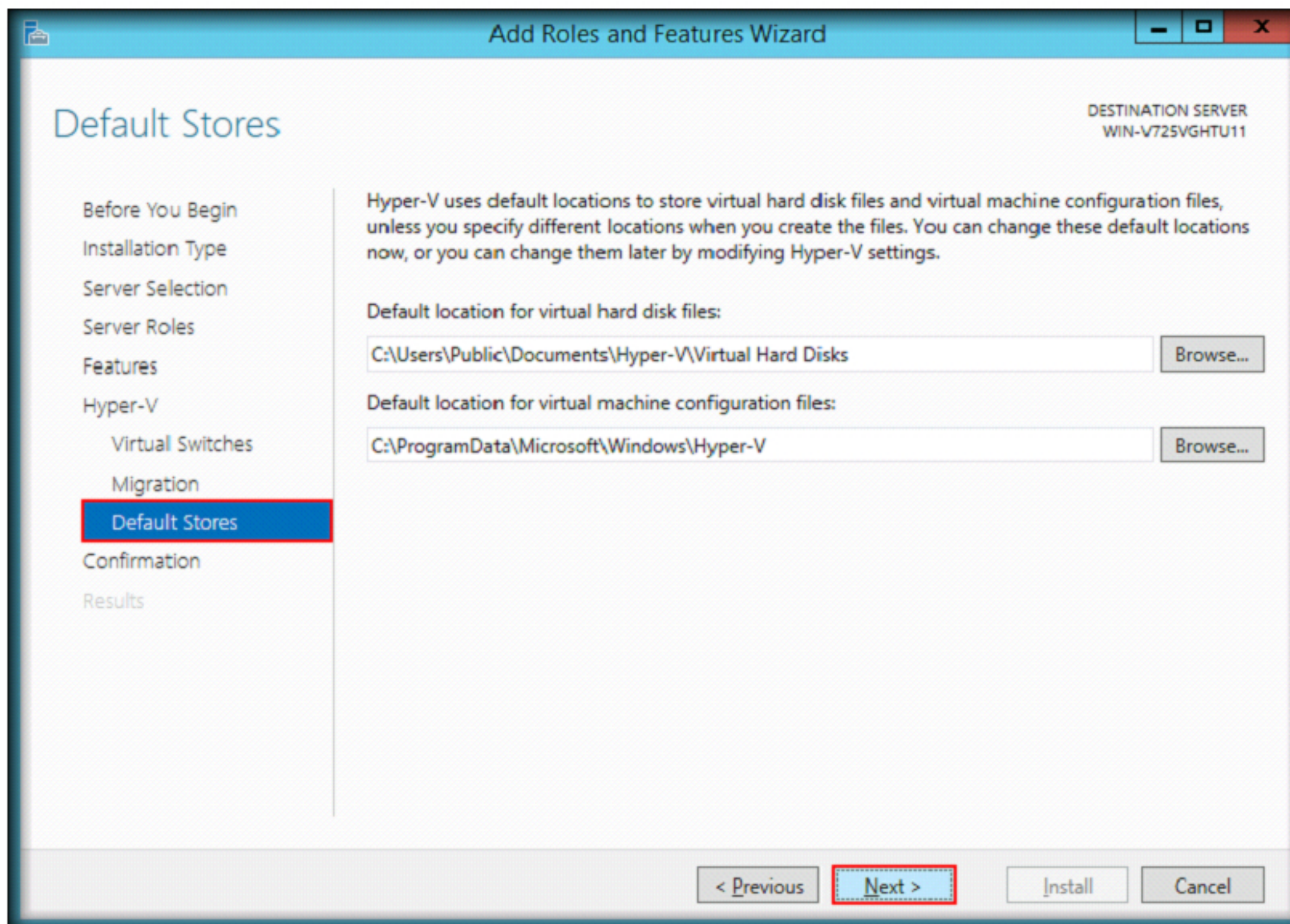
11. **Virtual Switches** section appears in the wizard. Under the **Network adapters** field, select the available network connection (here **Ethernet**) and click **Next**



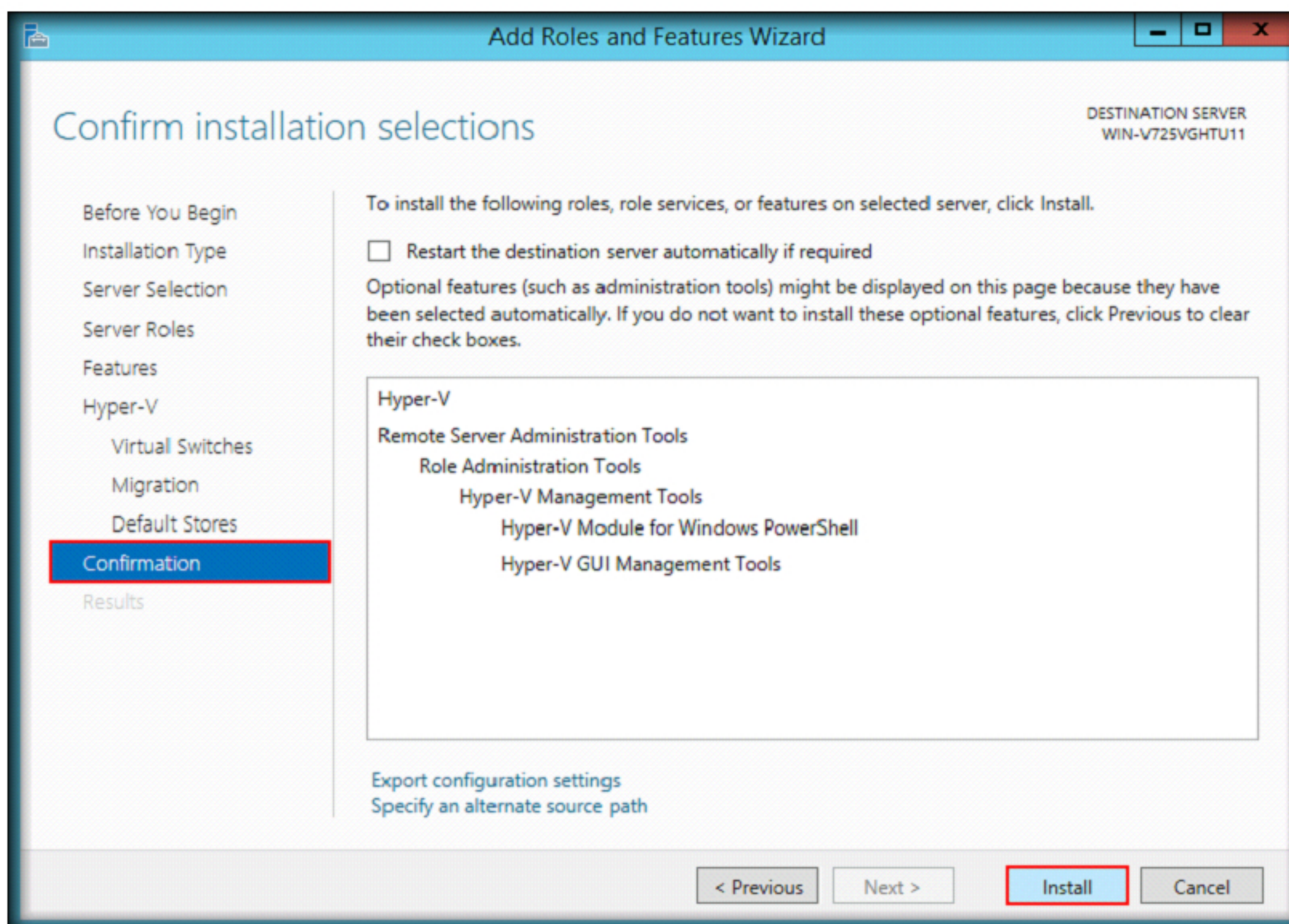
12. In the **Migration** section of the wizard, leave the options set to default and click **Next**



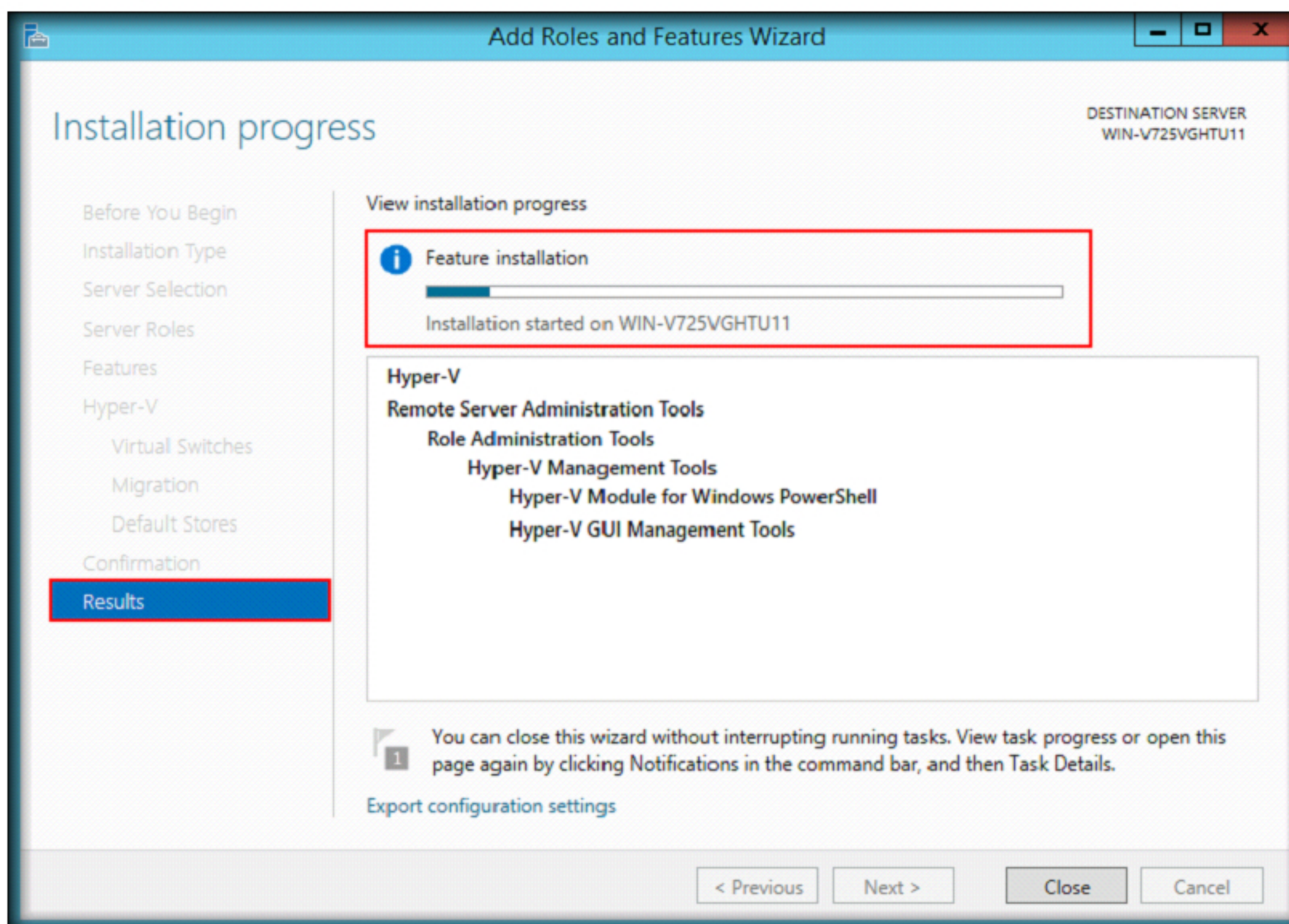
13. In **Default Stores** section, Hyper-V uses default location to store the disk and configuration files. Leaving the options set to default, click **Next**.



14. Click **Install** button to confirm installation for the selected Roles and Features



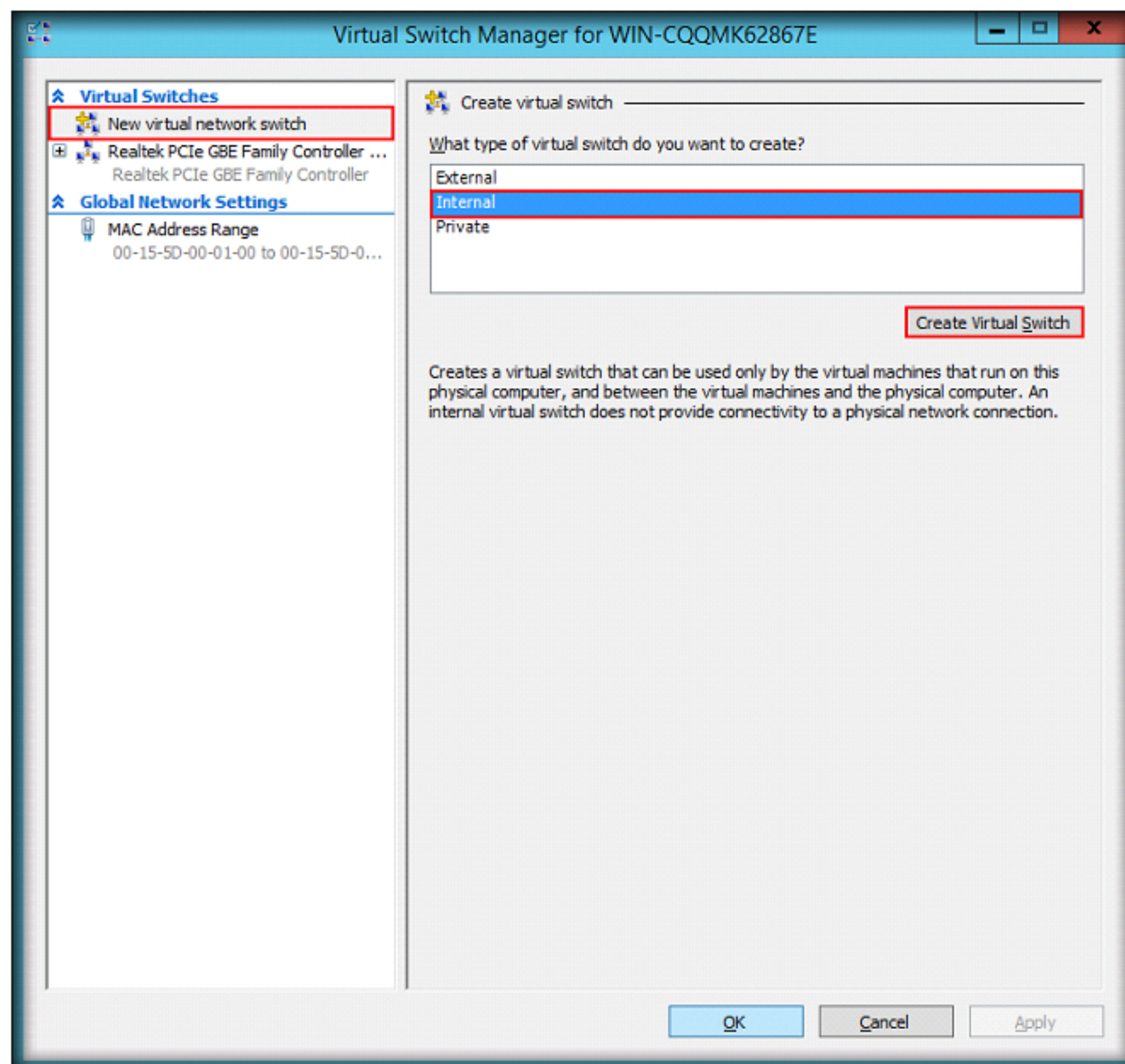
15. It will take a while to **complete** installation of selected roles and features



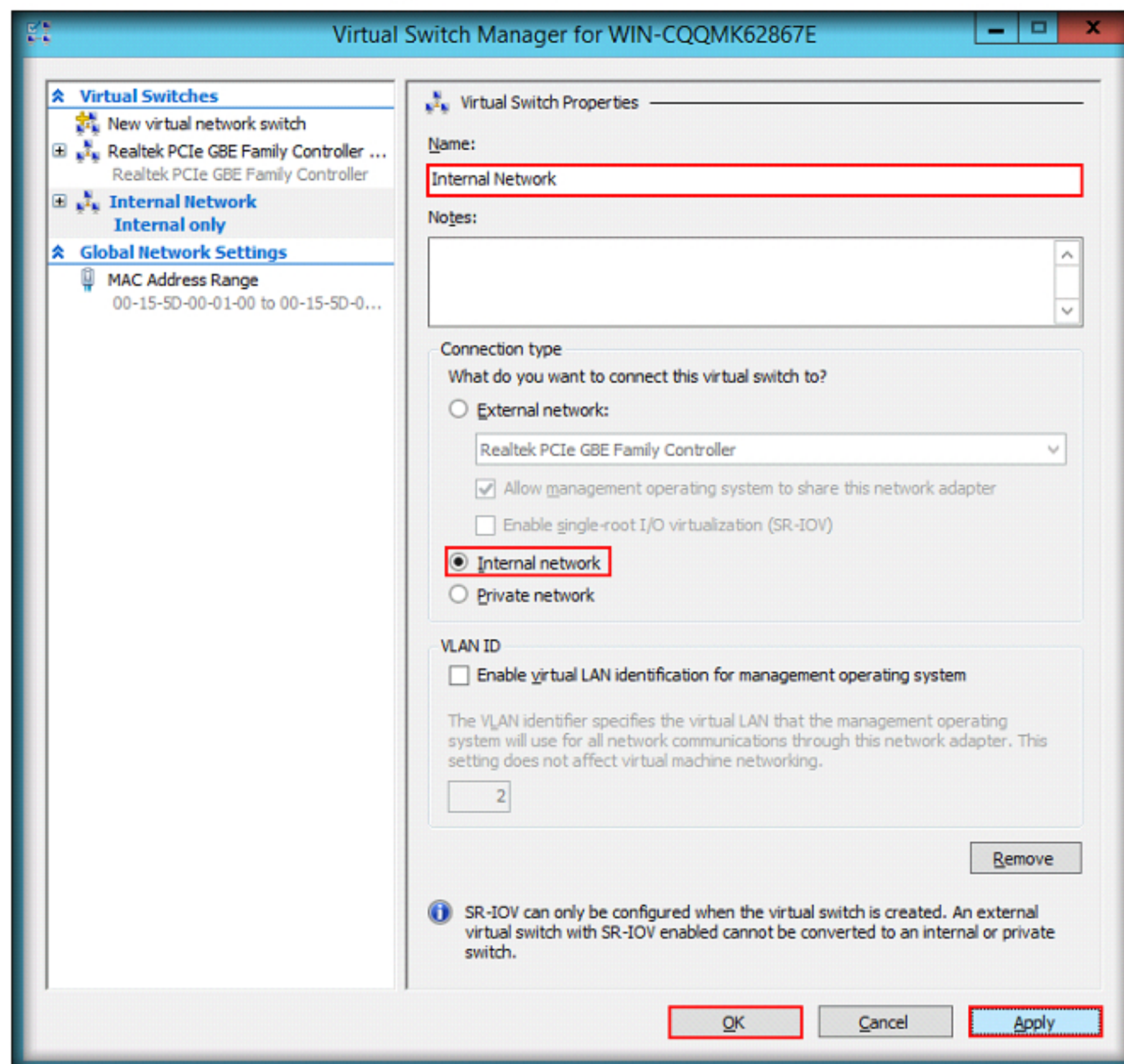
16. After the completion of installation, click **Close** and restart the machine.

CT#3: Configure Internal Network for Hyper-V

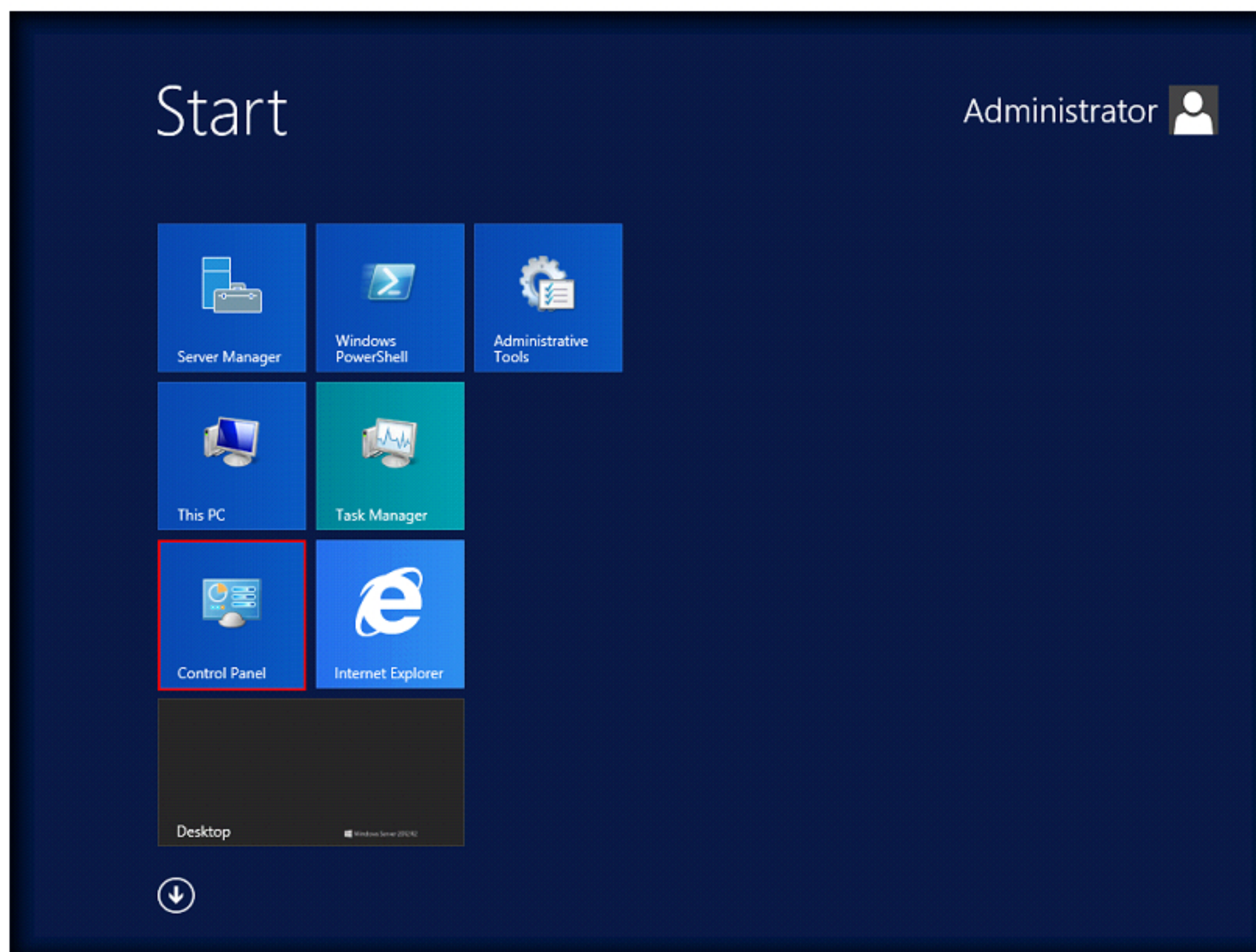
1. Launch Hyper-V Manager, Click **Start** → **Administrative Tools** → **Hyper-V Manager**
2. Click **Virtual Switch Manager** in the right pane of **Hyper-V Manager**. The **Virtual Switch Manager** window appears
3. Select **New Virtual network** from left pane, and select **Internal** as the network type
4. Click the **Create Virtual Switch** button



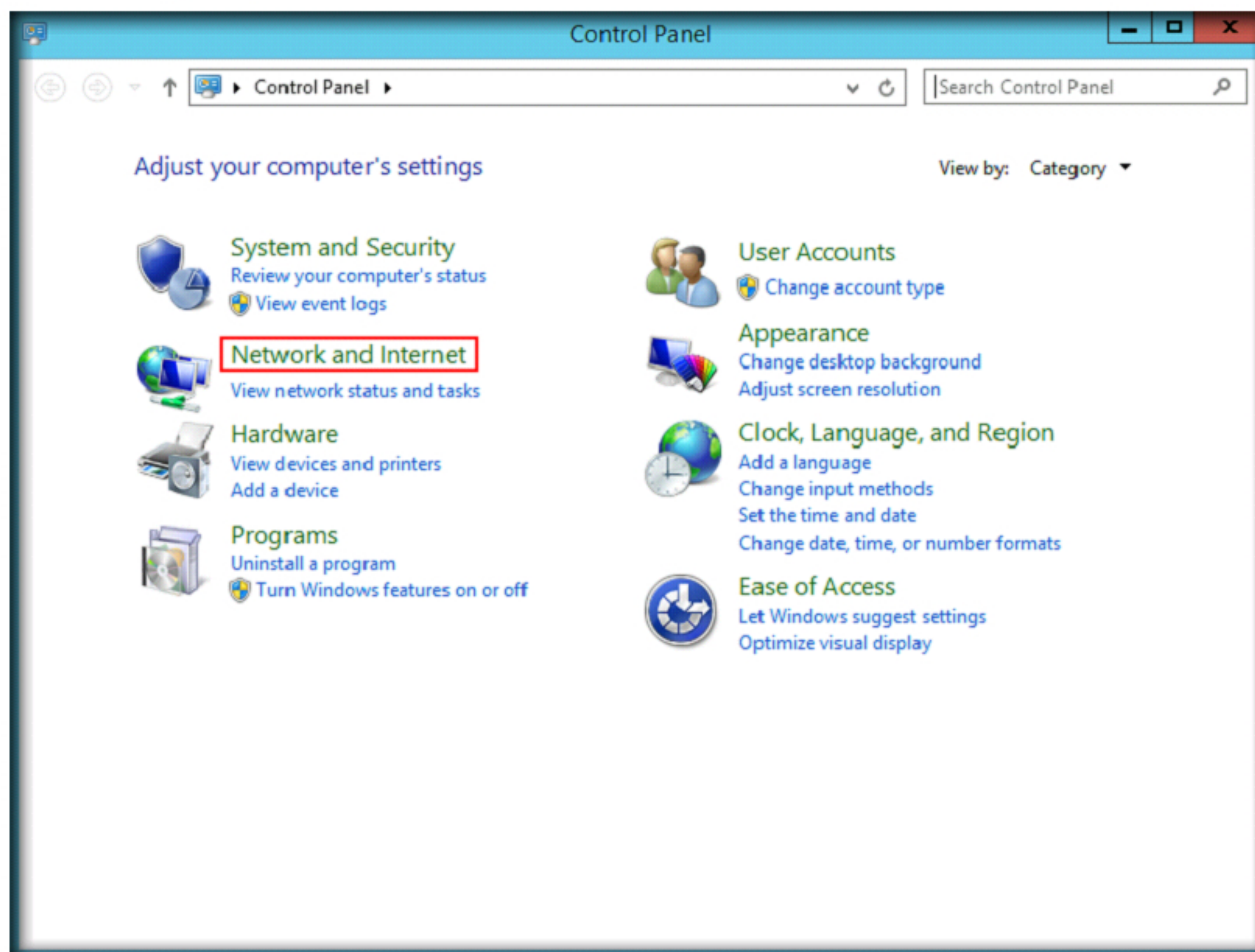
5. The newly created virtual switch appears in the left pane. Enter the name of the virtual switch as **Internal Network** under the **Name** field, select **Internal network** radio button, click **Apply** and then click **OK**



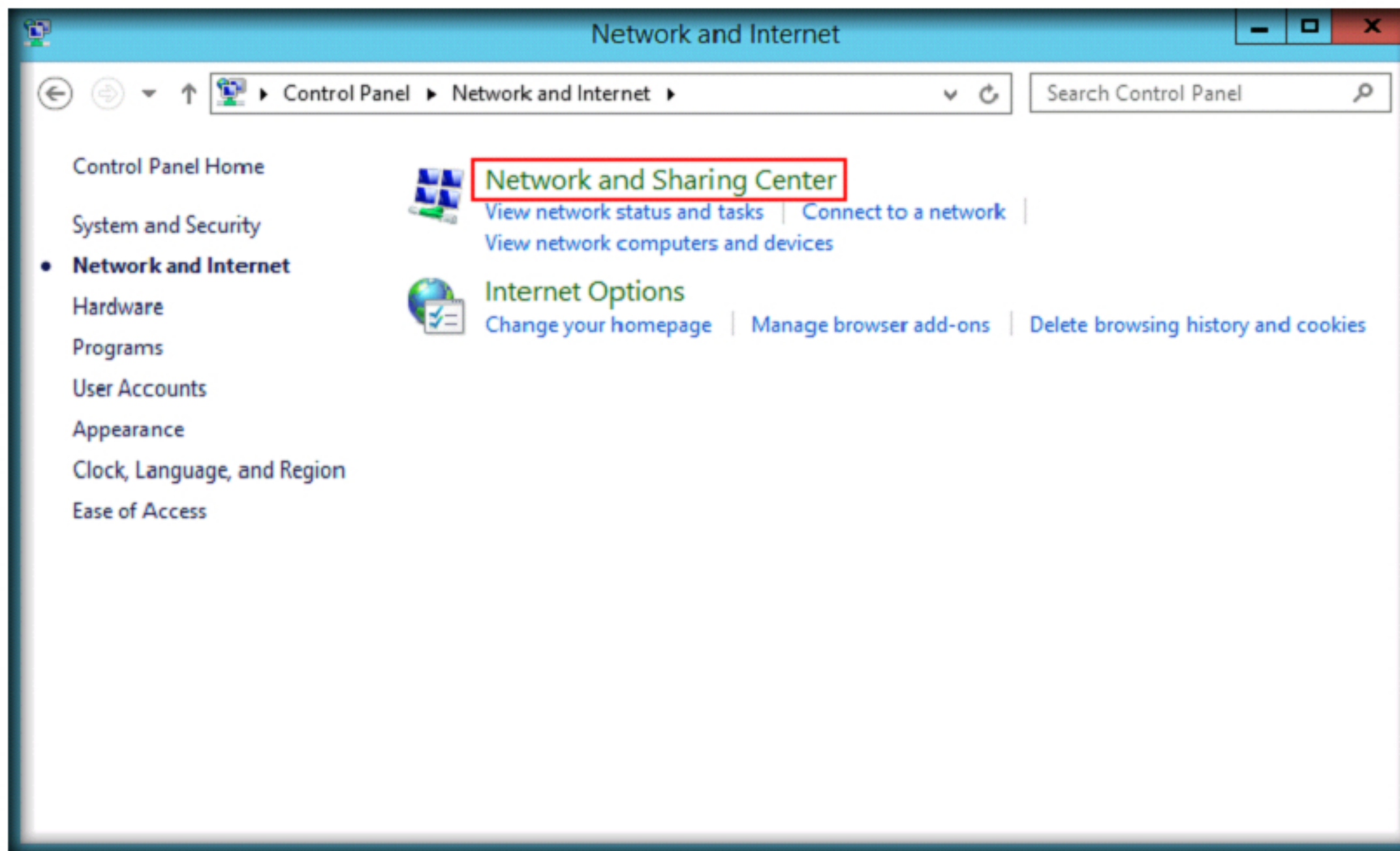
6. Now, go to **Start** screen and click **Control Panel**



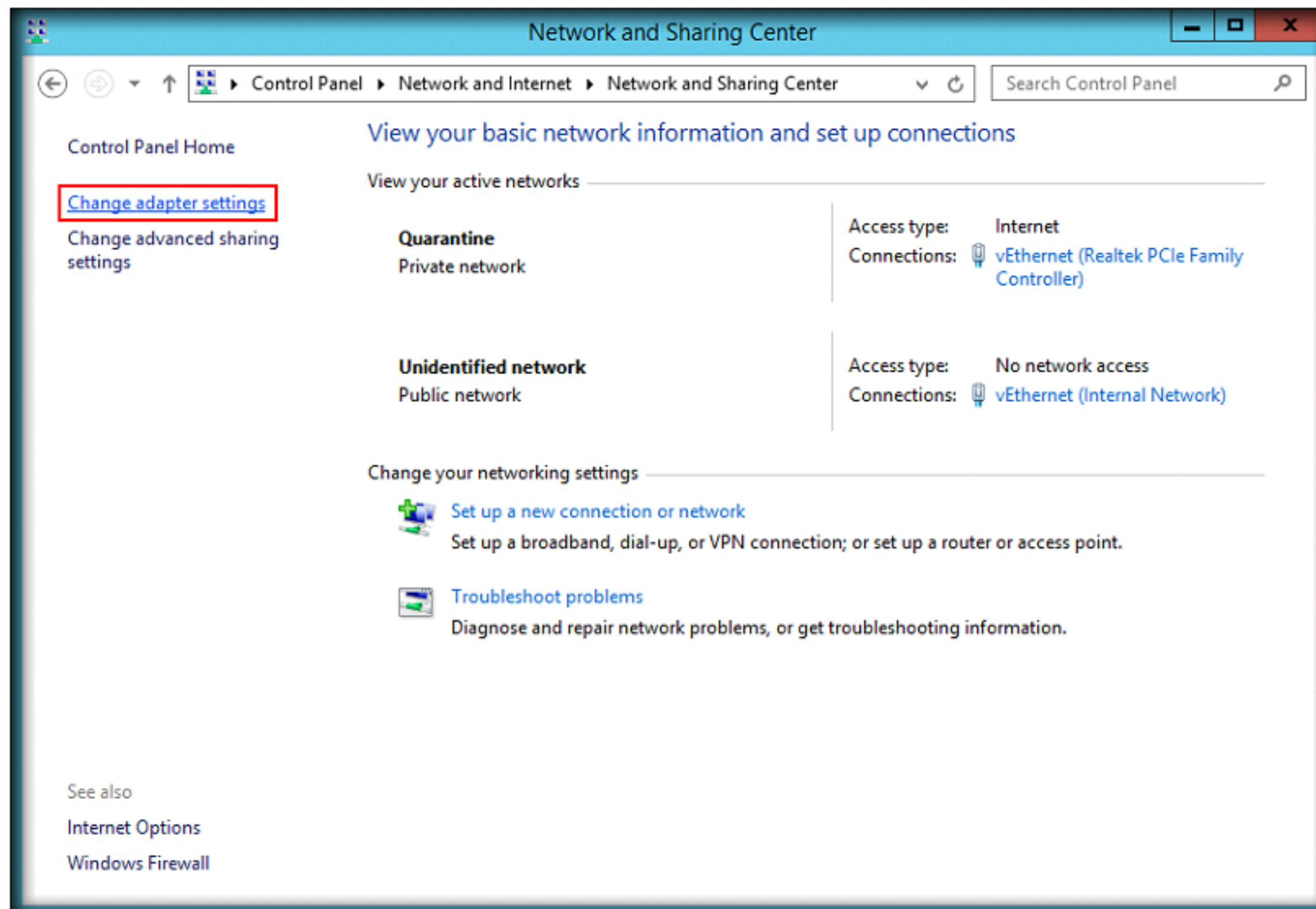
7. **Control Panel** window appears, click **Network and Internet** link



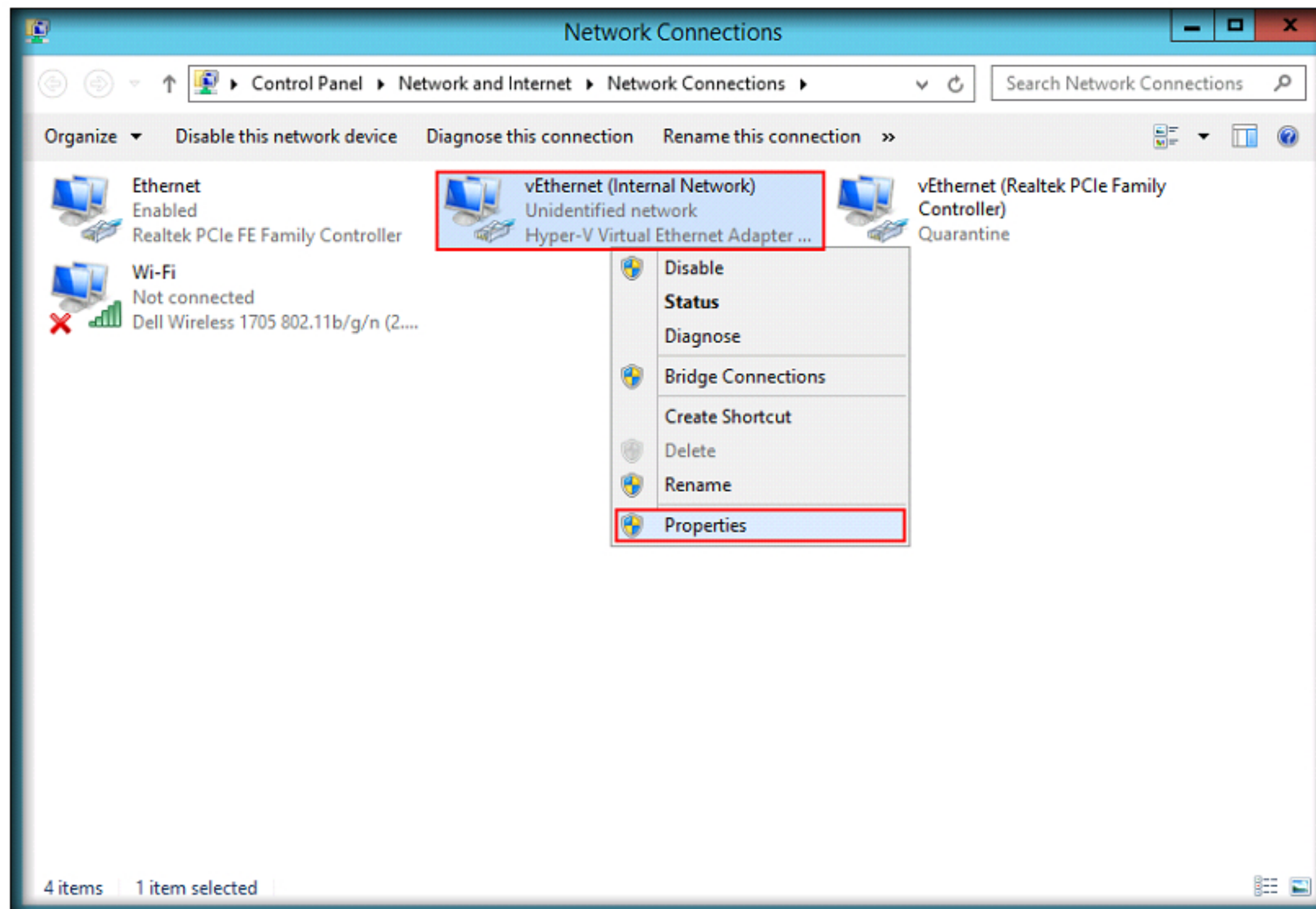
8. Network and Internet window appears, click **Network and Sharing Center** link



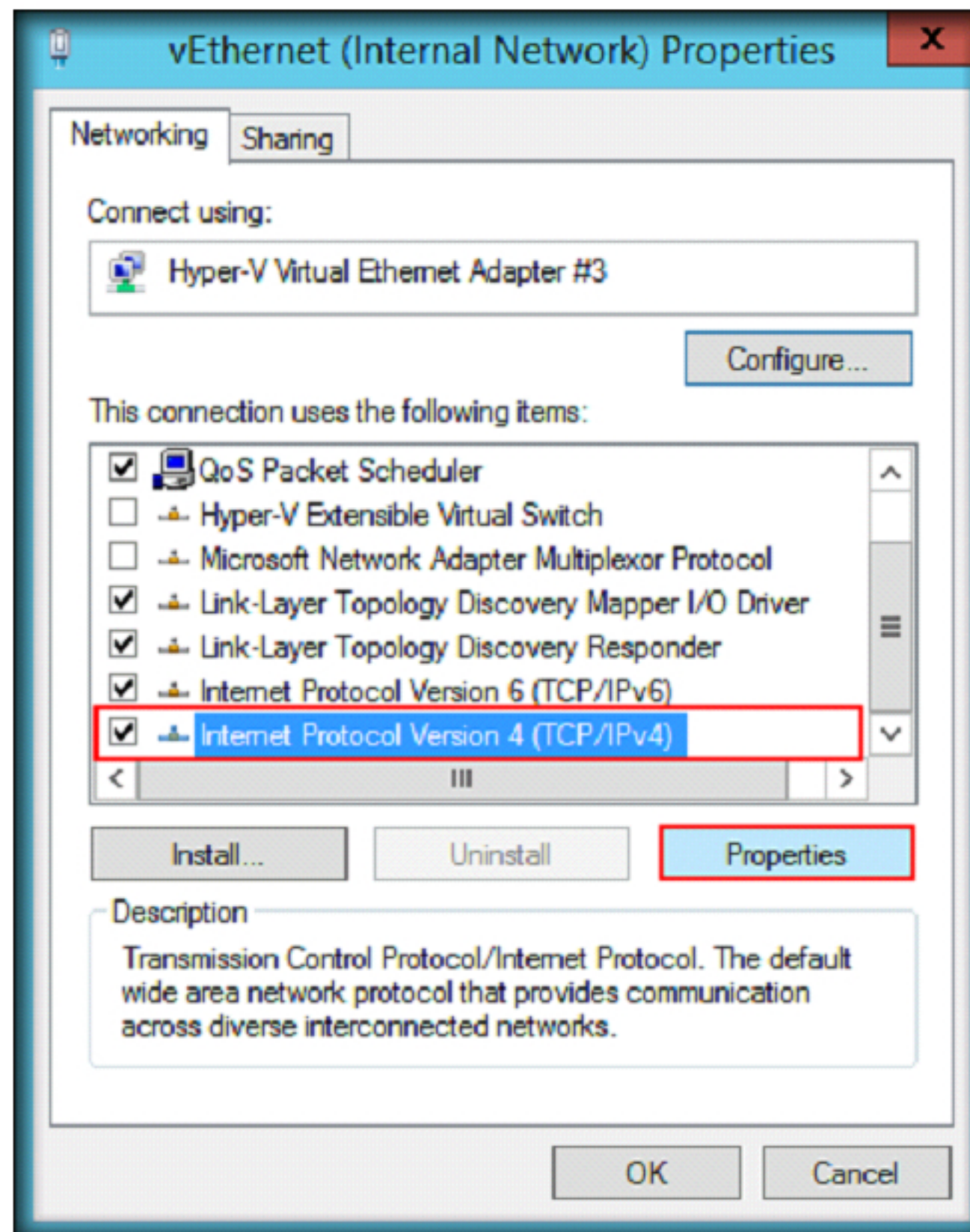
9. **Network and Sharing Centre** window appears, click **Change adapter settings** link from the left pane



10. Right-click the **Internal Network** adapter and click **Properties**



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



12. Select **Use the following IP address** radio button, assign **10.0.0.1** as **IP address**, **255.0.0.0** as **Subnet mask** and click **OK**

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 . 0 . 0 . 1

Subnet mask: 255 . 0 . 0 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

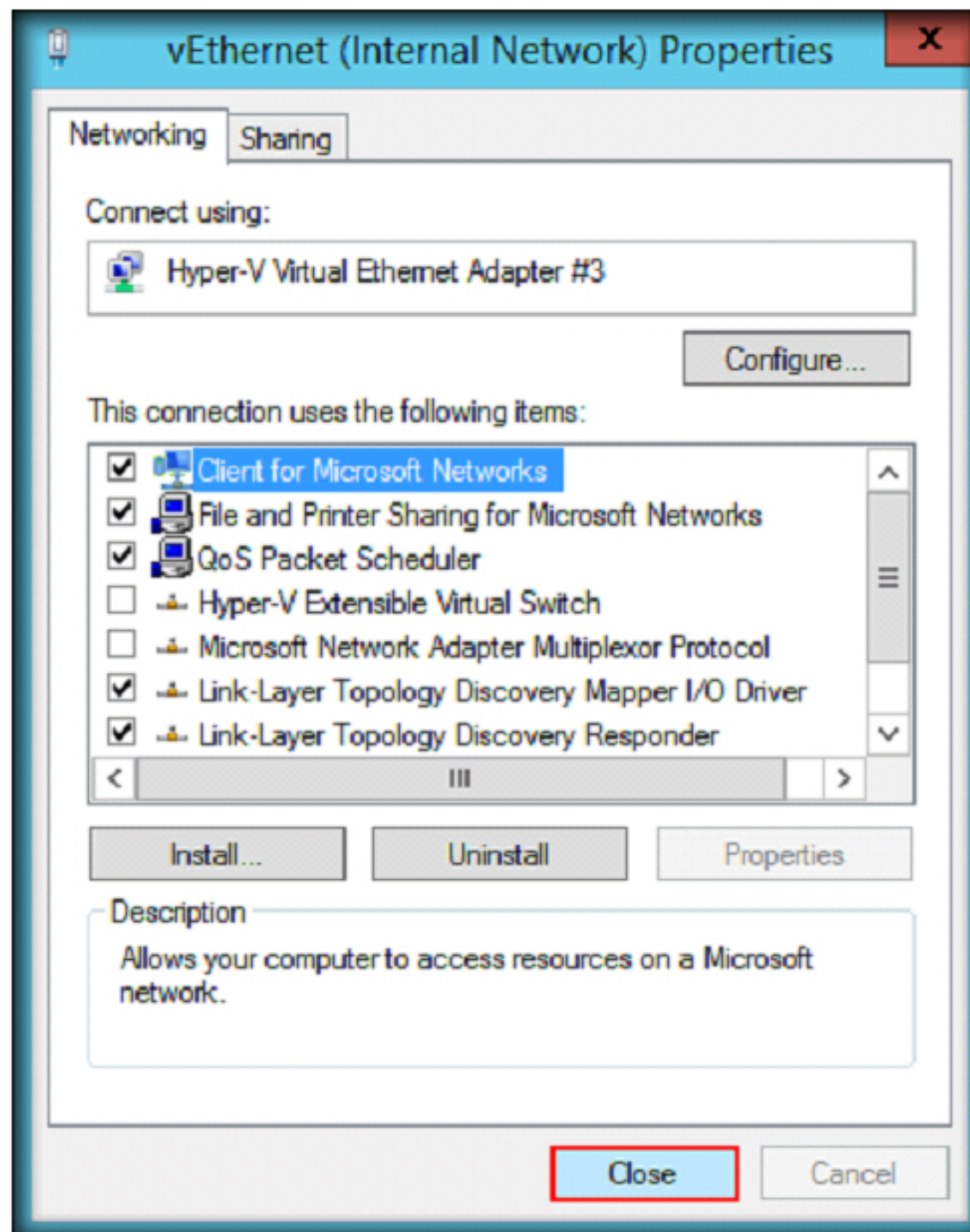
Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

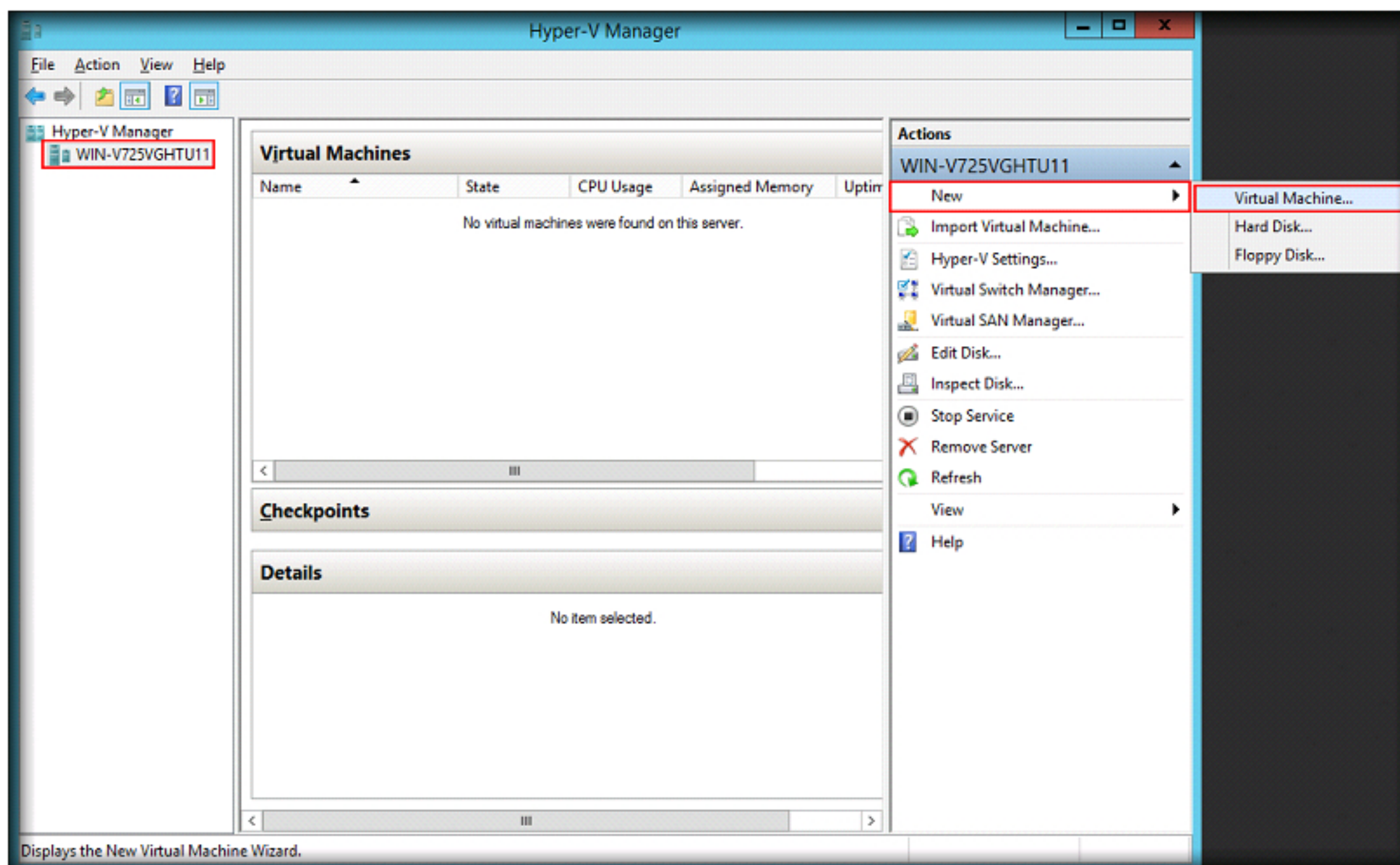
OK Cancel

13. **Close** the **Properties** window



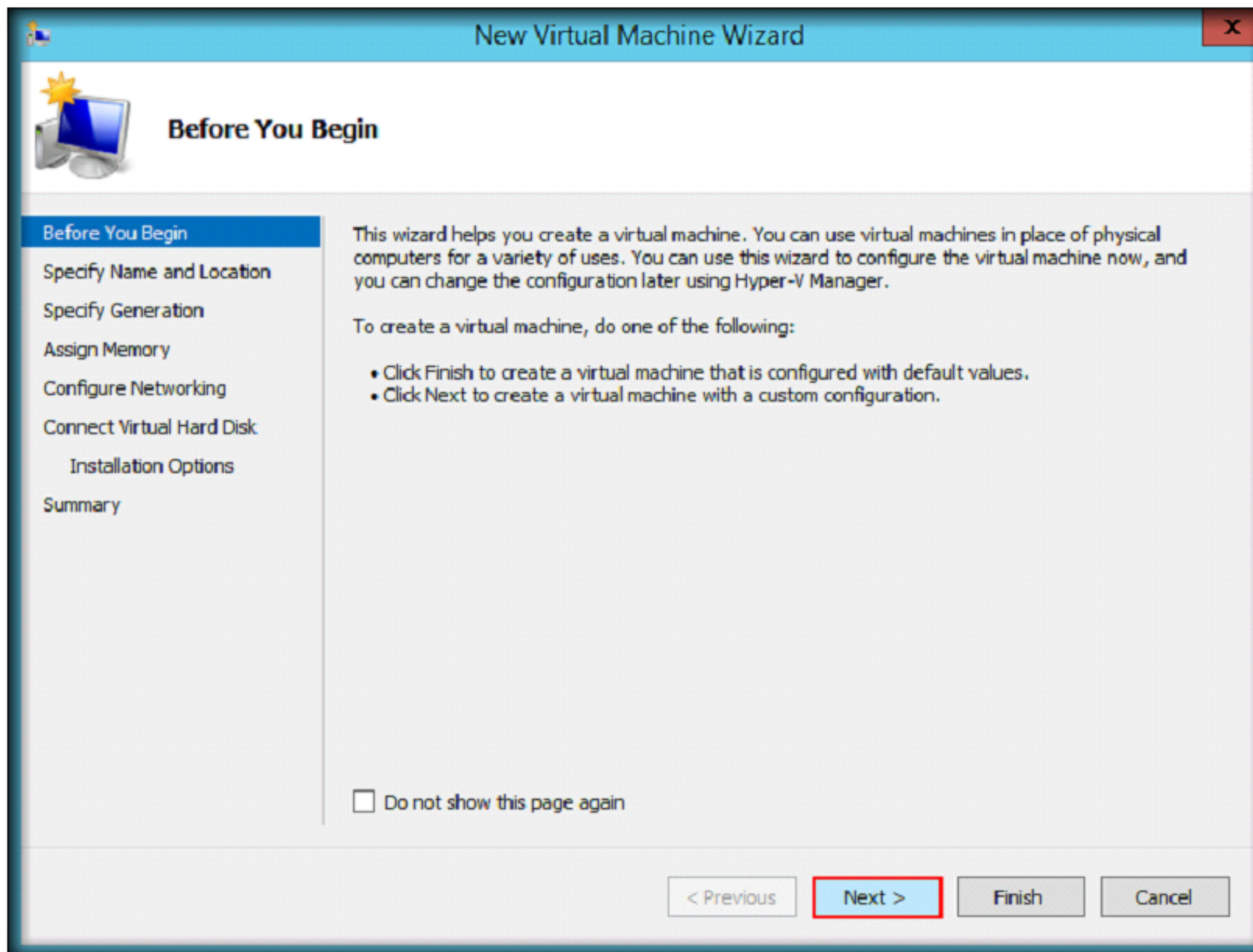
CT#4: Create a New Virtual Machine in Hyper-V

1. Click **Start → Administrative Tools → Hyper-V Manager**
1. Select your **machine's name** in the left pane of the window, and click **New → Virtual Machine...** option located at the right pane of window



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

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



3. Specify **Name** and **location** of new virtual machine. Assign the name of the virtual machine as **Windows Server 2012**.
4. The default location for storing the virtual machine is **C:\ProgramData\Microsoft\Windows\Hyper-V**. Choose **E:** drive to store the virtual machine in a different location.
5. 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

The screenshot shows the 'New Virtual Machine Wizard' window with the 'Specify Name and Location' step selected in the left-hand navigation pane. The main area contains instructions and input fields for naming and locating the virtual machine. The 'Name' field is set to 'Windows Server 2012'. The checkbox 'Store the virtual machine in a different location' is checked, and the 'Location' field is set to 'E:\'. A warning icon and text advise selecting a location with enough free space for checkpoints. The 'Next >' button is highlighted in blue.

New Virtual Machine Wizard

Specify Name and Location

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

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:

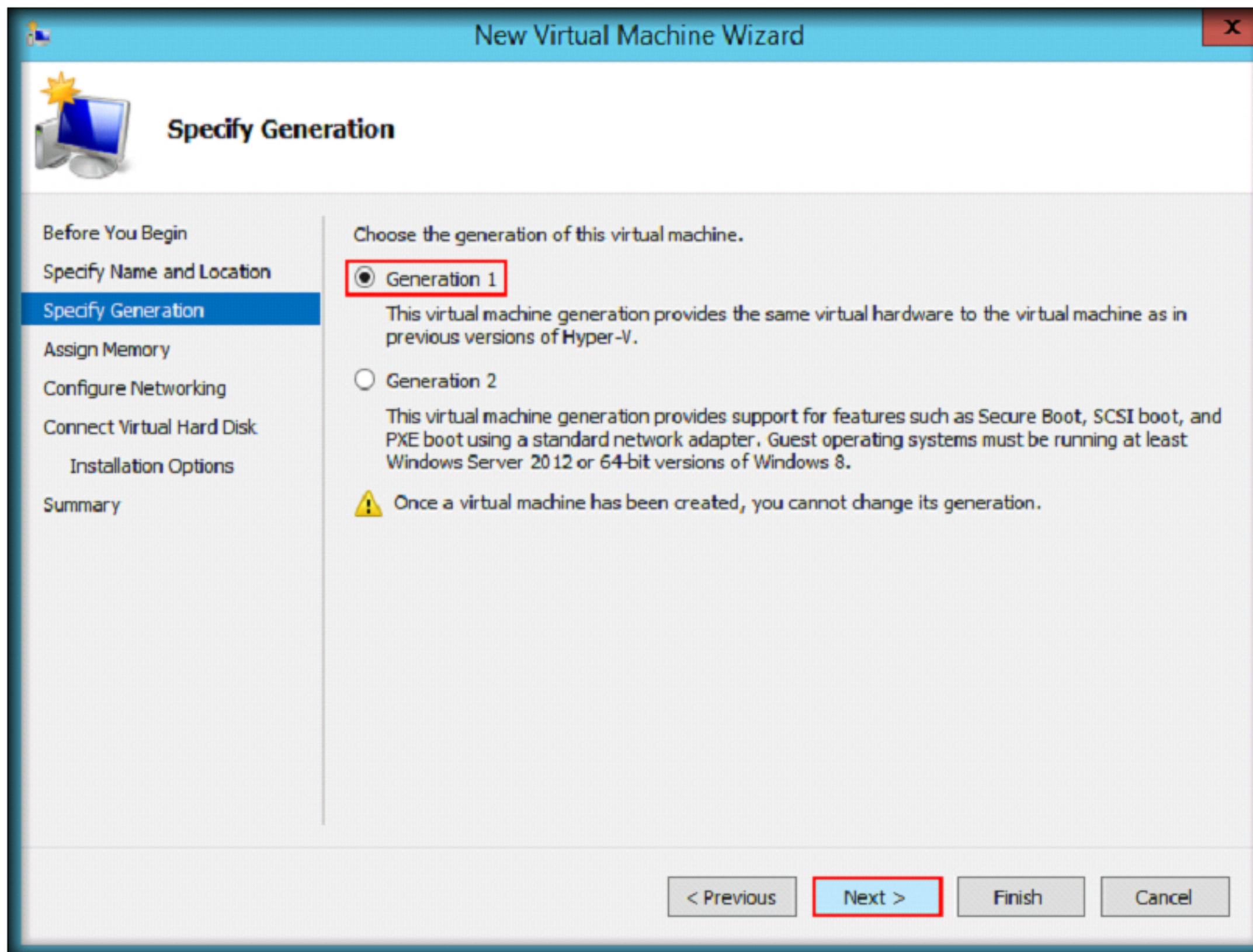
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☒ Store the virtual machine in a different location

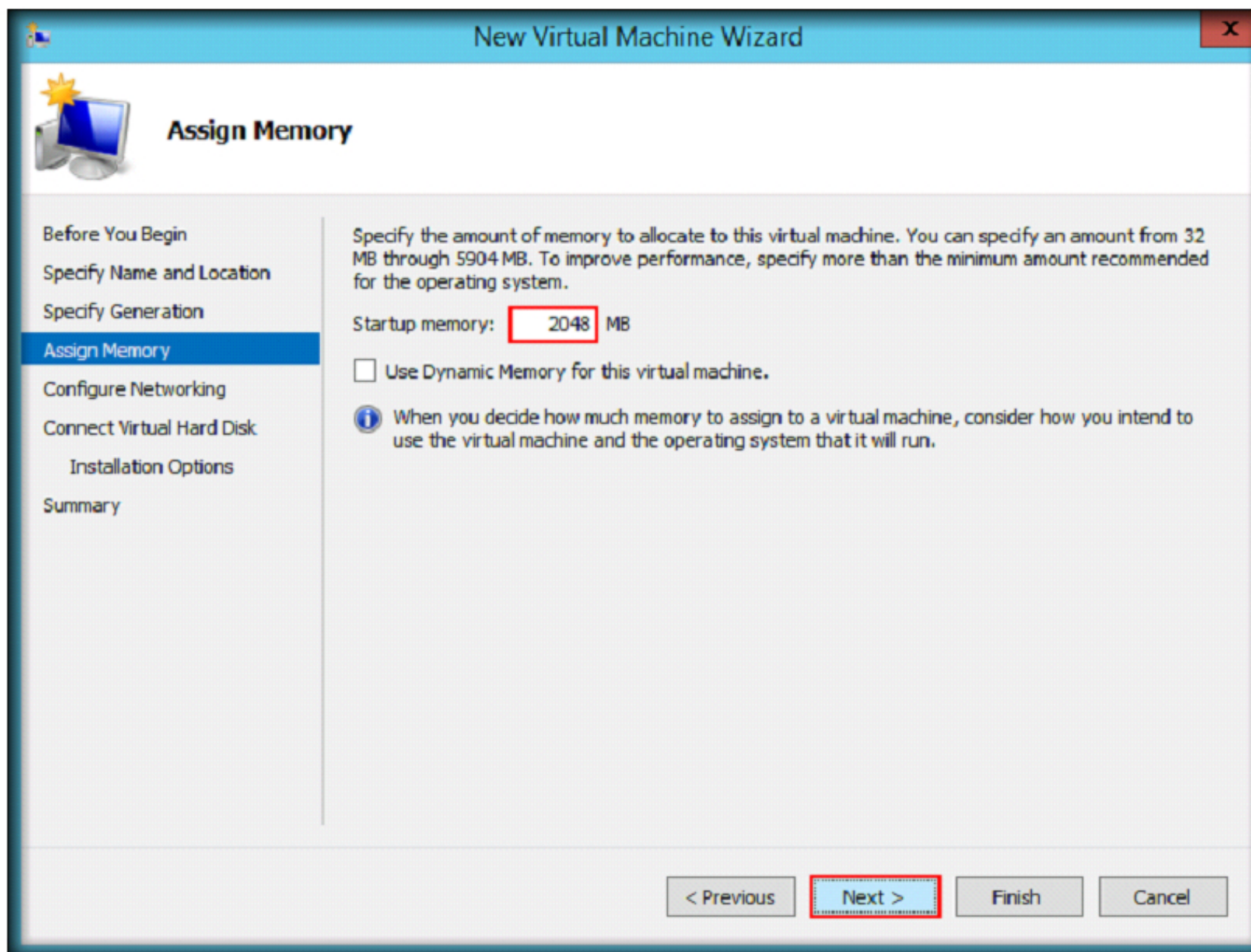
Location:

 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.

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

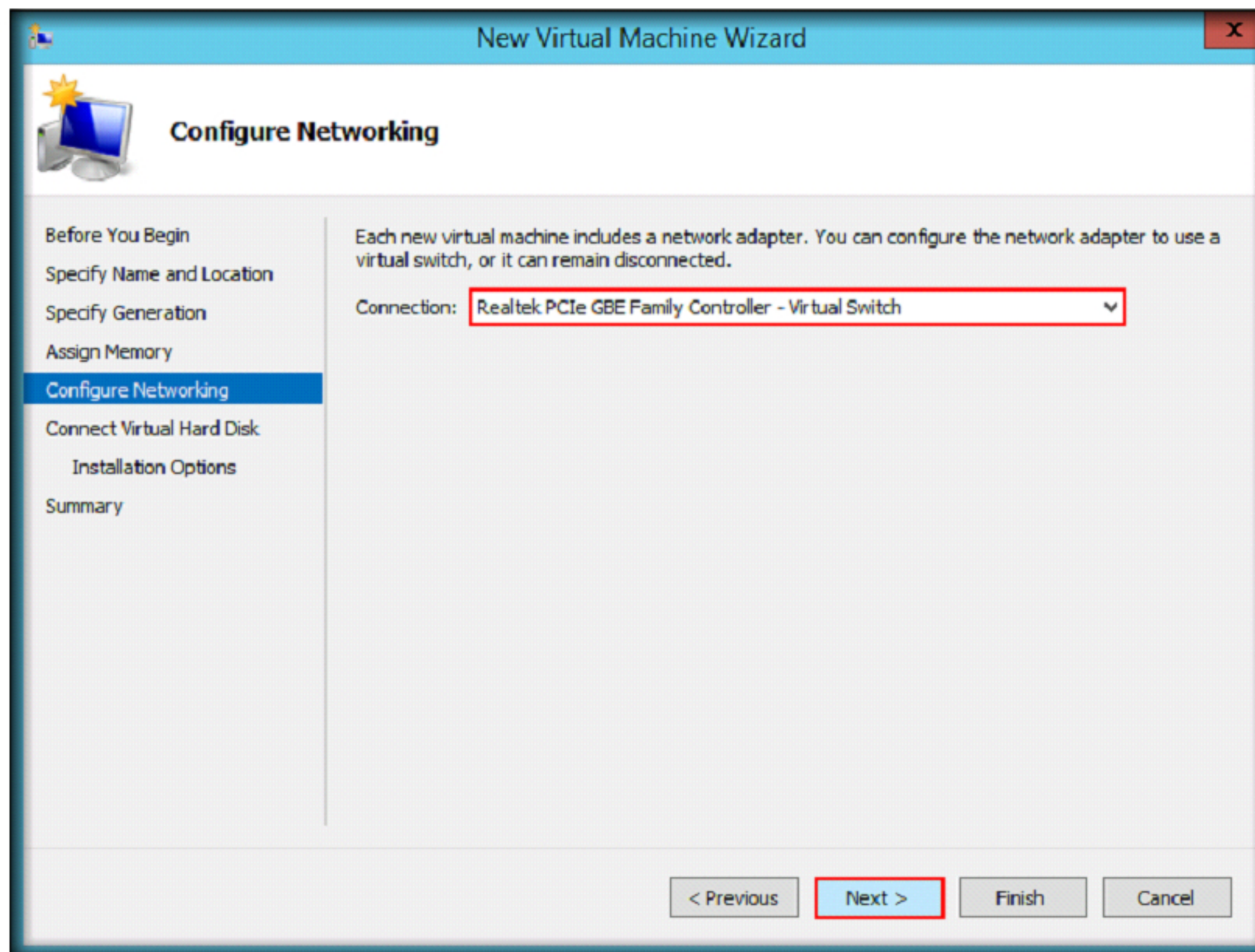


7. Assign the amount of **memory** to allocate to this virtual machine in MB (here, **2048**)
8. Click **Next**



9. In the next step, select **network adapter** as **Realtek PCIe GBE Family Controller - Virtual Switch** from connection drop-down list and click **Next**

Note: The network adapter shown in the above screenshot might vary in your lab environment.



10. Connect Virtual Hard Disk section appears, Allocate **80 GB** space for hard disk and click **Next**

The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Connect Virtual Hard Disk' step. The window has a blue title bar with the text 'New Virtual Machine Wizard' and a close button. On the left, there is a navigation pane with the following steps: 'Before You Begin', 'Specify Name and Location', 'Specify Generation', 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk' (which is highlighted in blue), 'Installation Options', and 'Summary'. The main area of the window contains the following text: '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.' There are three radio button options: 1. 'Create a virtual hard disk' (selected): 'Use this option to create a VHDX dynamically expanding virtual hard disk.' Below this, there are three input fields: 'Name:' with the value 'Windows Server 2012.vhdx', 'Location:' with the value 'E:\Windows Server 2012\Virtual Hard Disks\' and a 'Browse...' button, and 'Size:' with the value '80' GB (Maximum: 64 TB). The '80' is highlighted with a red box. 2. 'Use an existing virtual hard disk': 'Use this option to attach an existing virtual hard disk, either VHD or VHDX format.' Below this, there is a 'Location:' input field with the value 'C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\' and a 'Browse...' button. 3. 'Attach a virtual hard disk later': 'Use this option to skip this step now and attach an existing virtual hard disk later.' At the bottom of the window, there are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Finish', and 'Cancel'.

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: Windows Server 2012.vhdx
Location: E:\Windows Server 2012\Virtual Hard Disks\ Browse...
Size: **80** GB (Maximum: 64 TB)

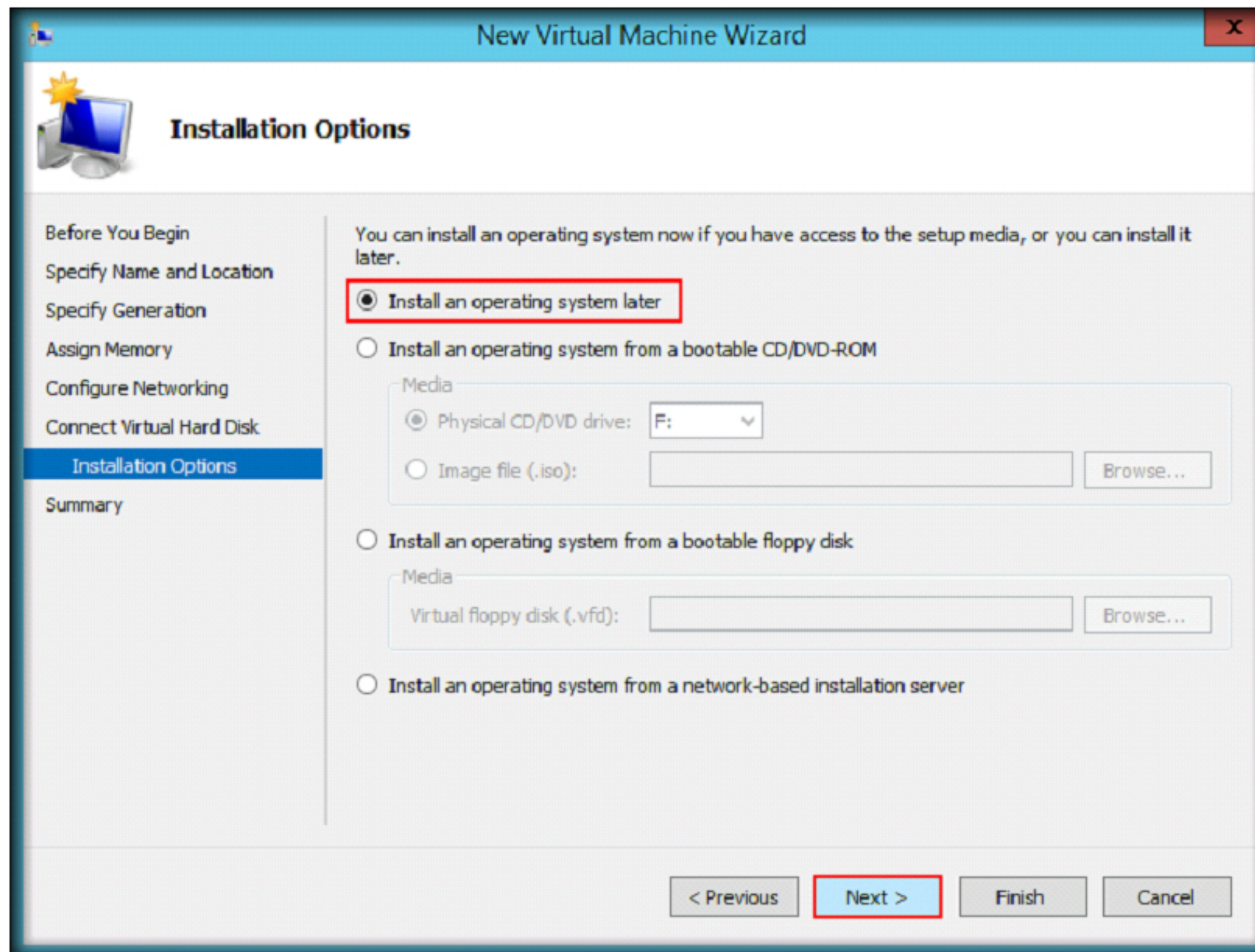
☐ Use an existing virtual hard disk
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

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.

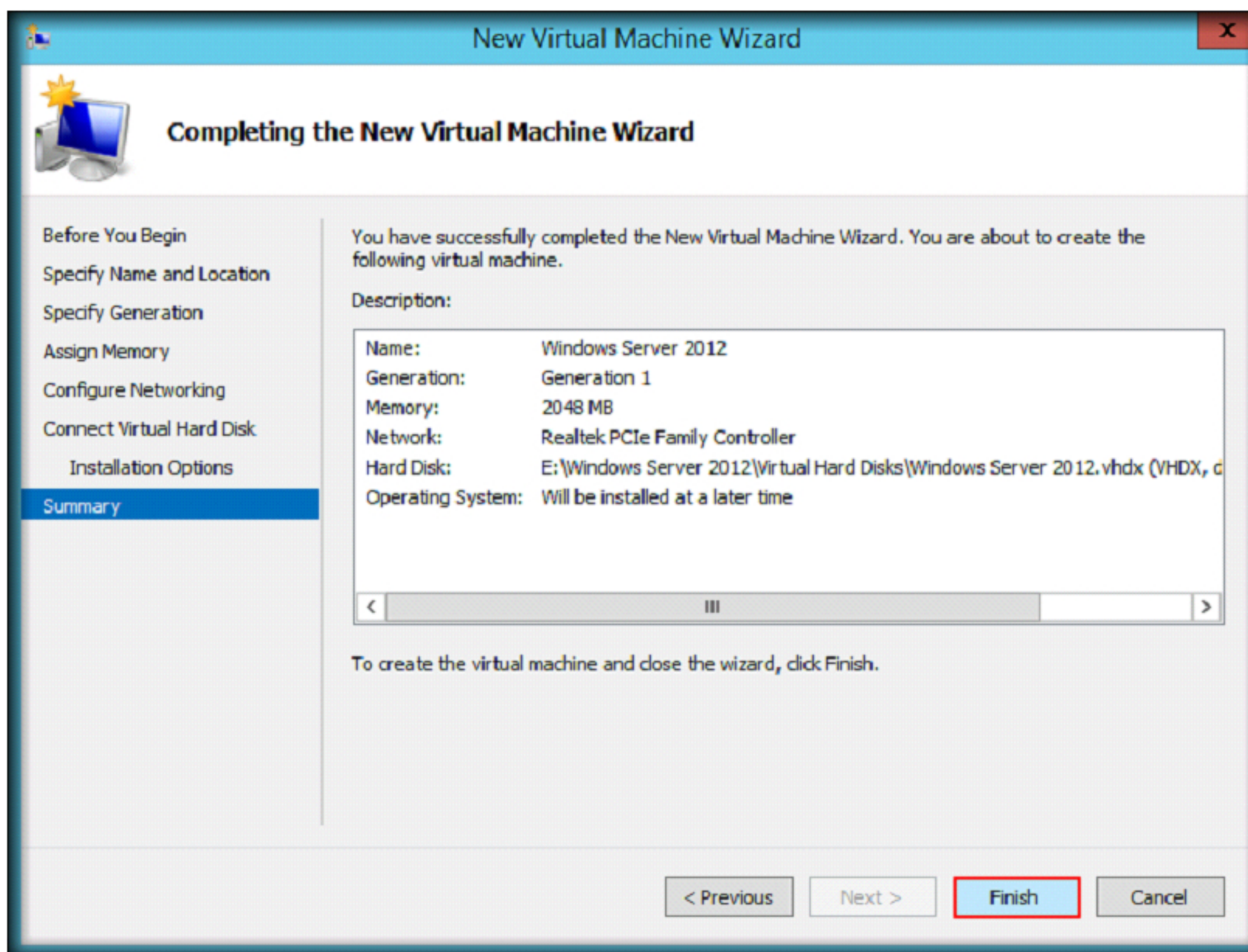
< Previous **Next >** Finish Cancel

11. The **installation options** section appears, select **Install an operating system later** radio button and click **Next**

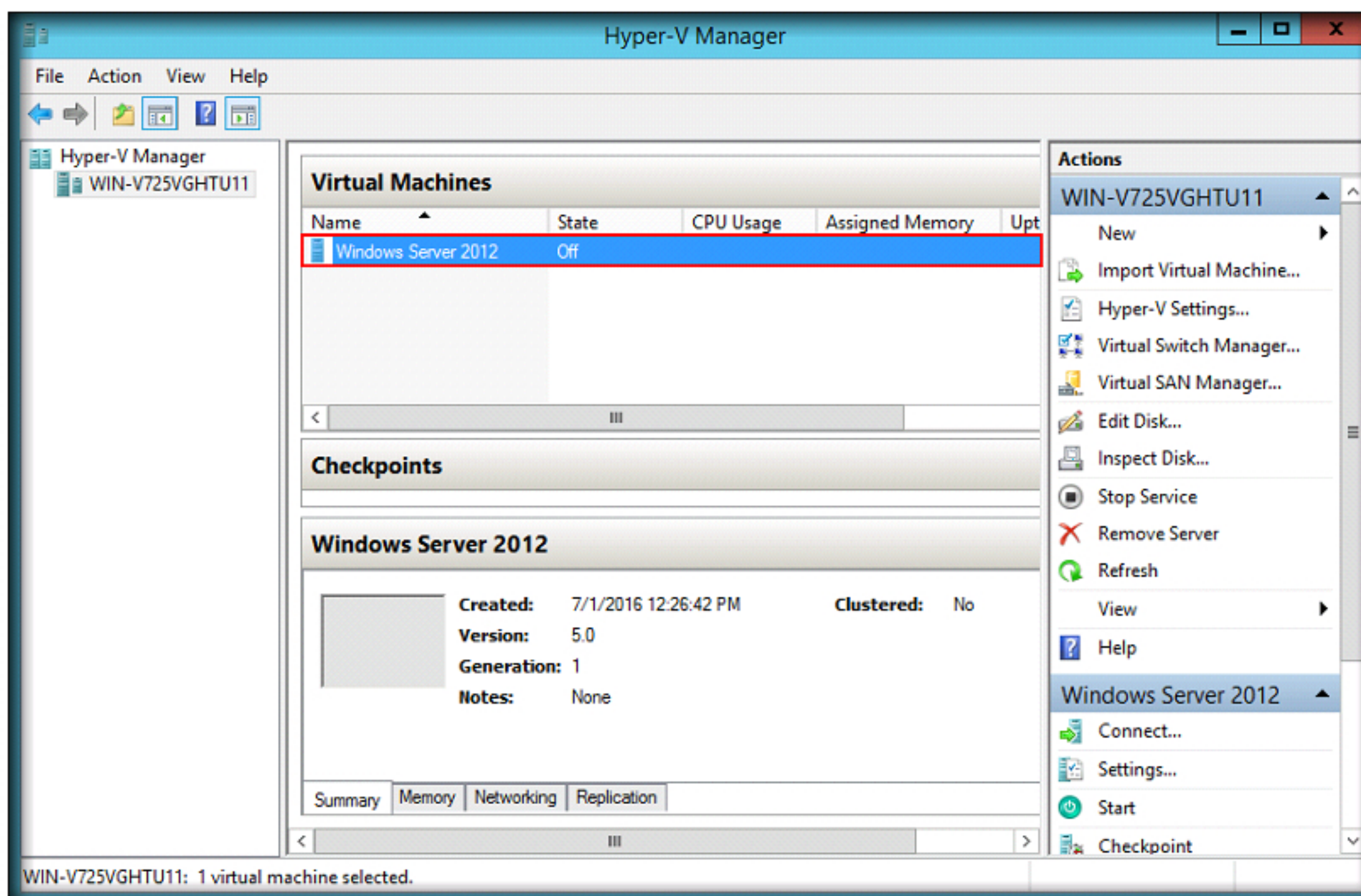


12. Virtual machine wizard appears with summary information

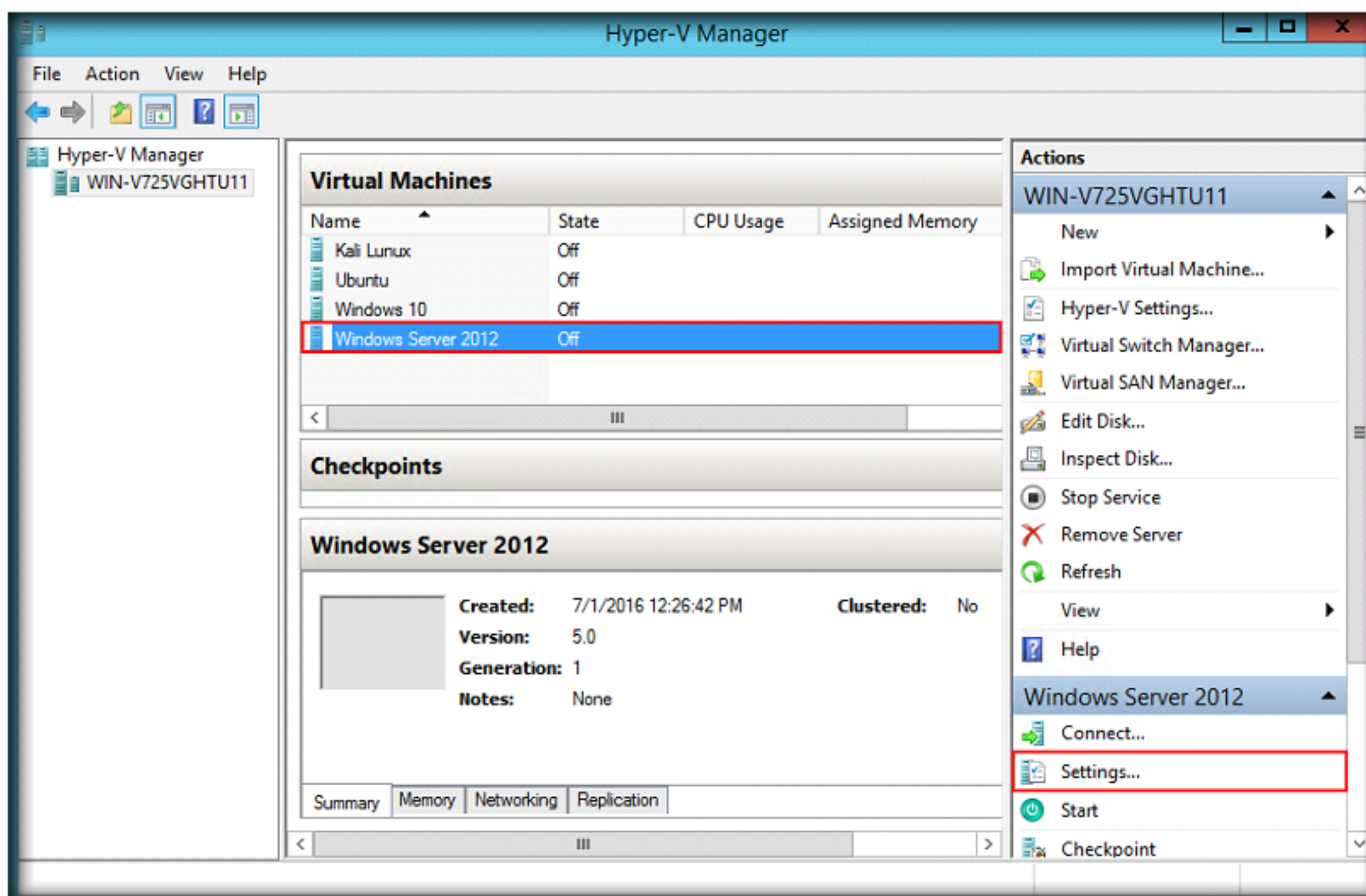
13. Click **Finish**



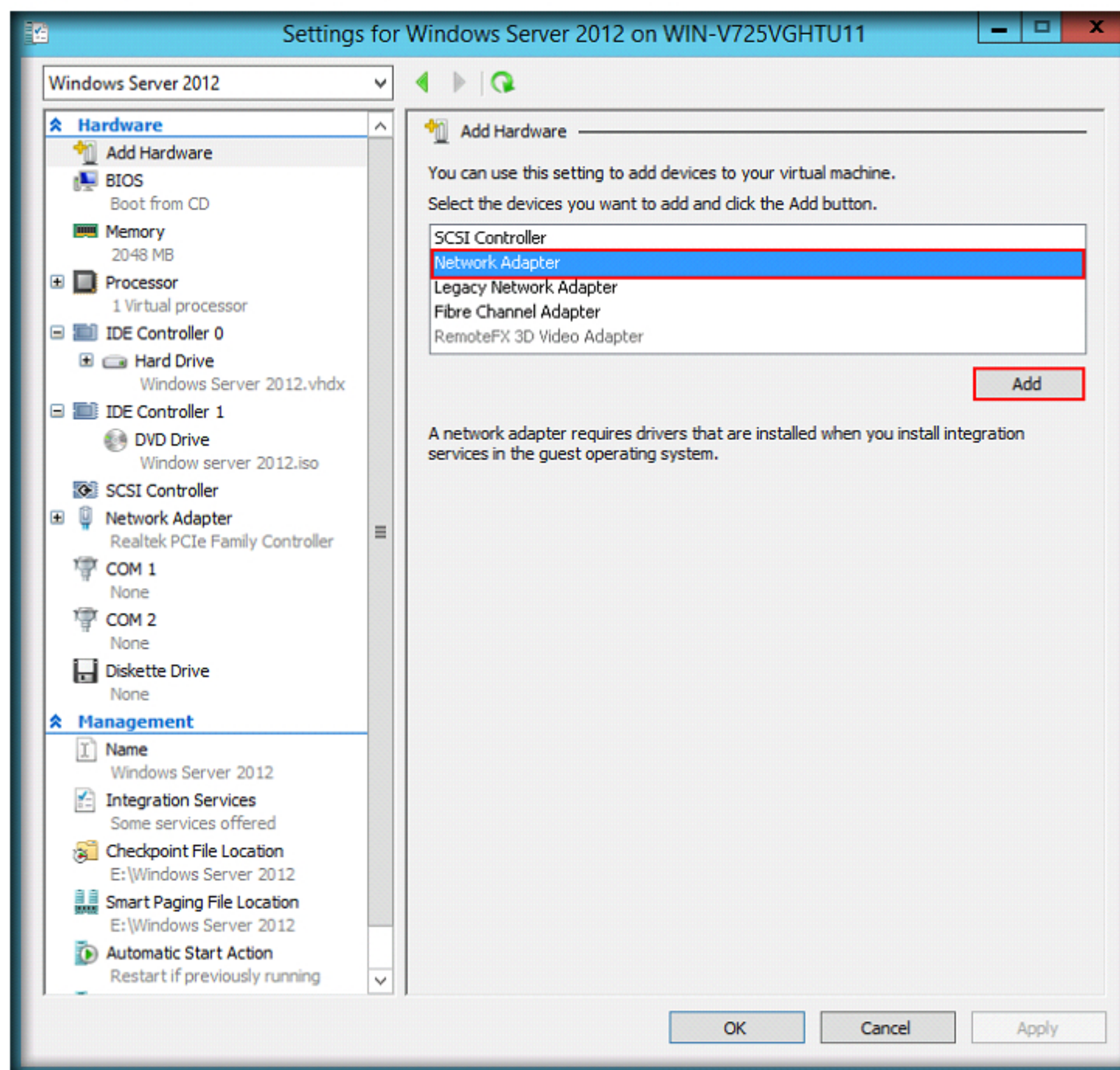
14. Hyper-V Manager creates **Windows Server 2012** virtual machine profile
15. In **Hyper-V Manager** main window, you see a new virtual machine named **Windows Server 2012**



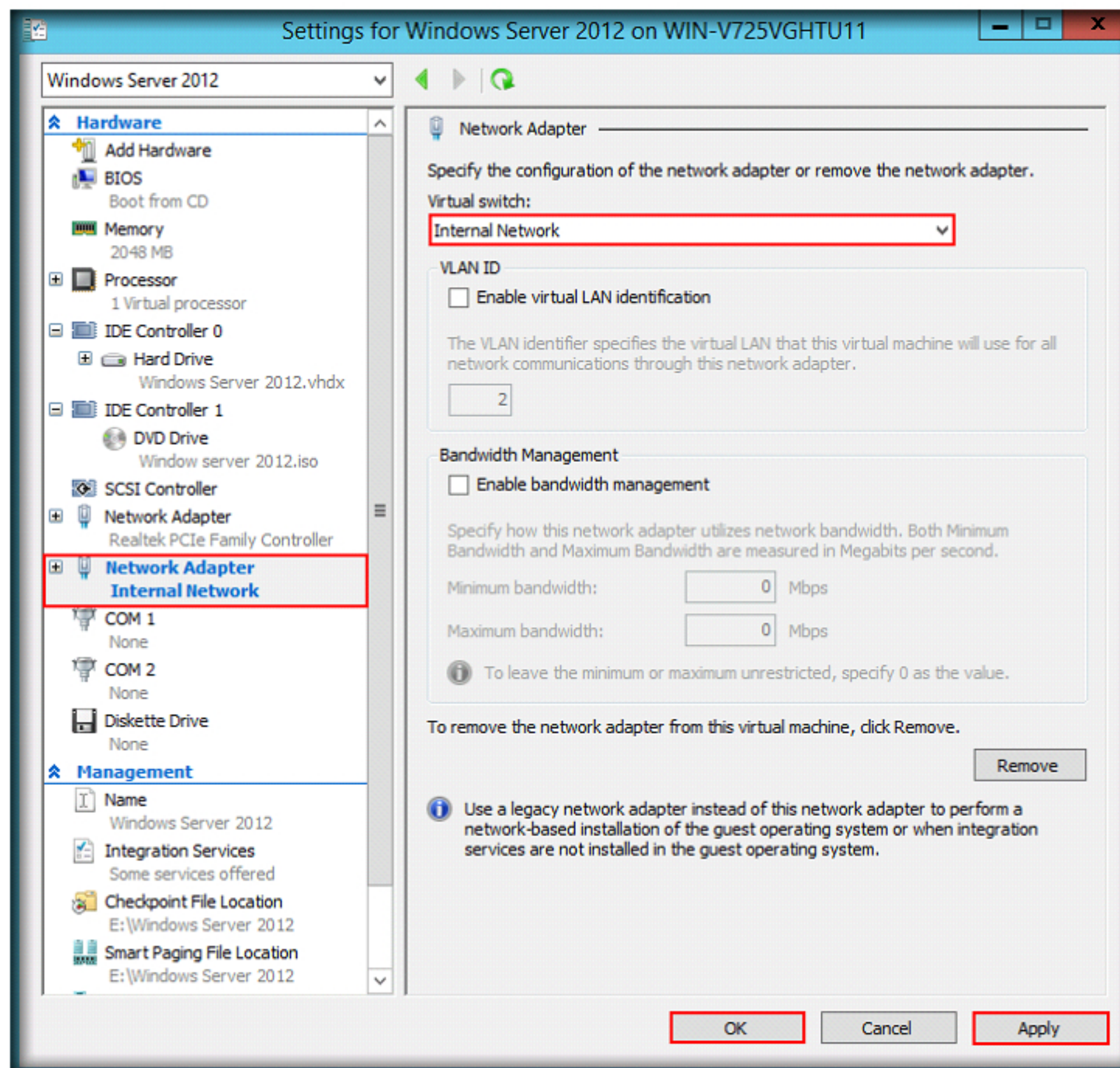
16. Select the virtual machine and click **Settings...** in the right pane



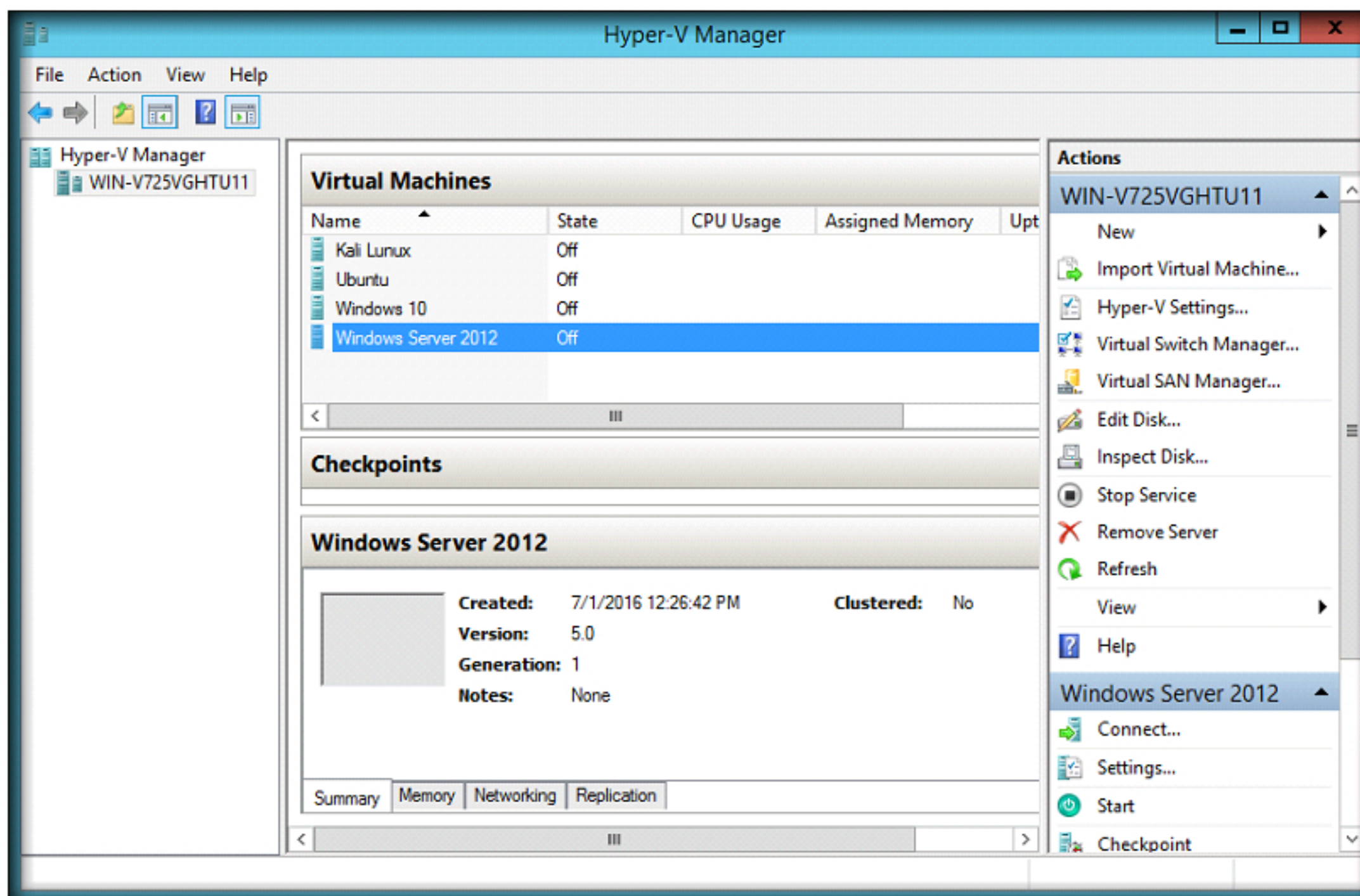
17. **Settings** window appears, select **Network Adapter** in the **Add Hardware** section and click **Add**



18. The newly added **Network Adapter** appears in the left pane. Select **Internal Network** from the **Virtual switch** drop-down list, click **Apply** and then click **OK**.

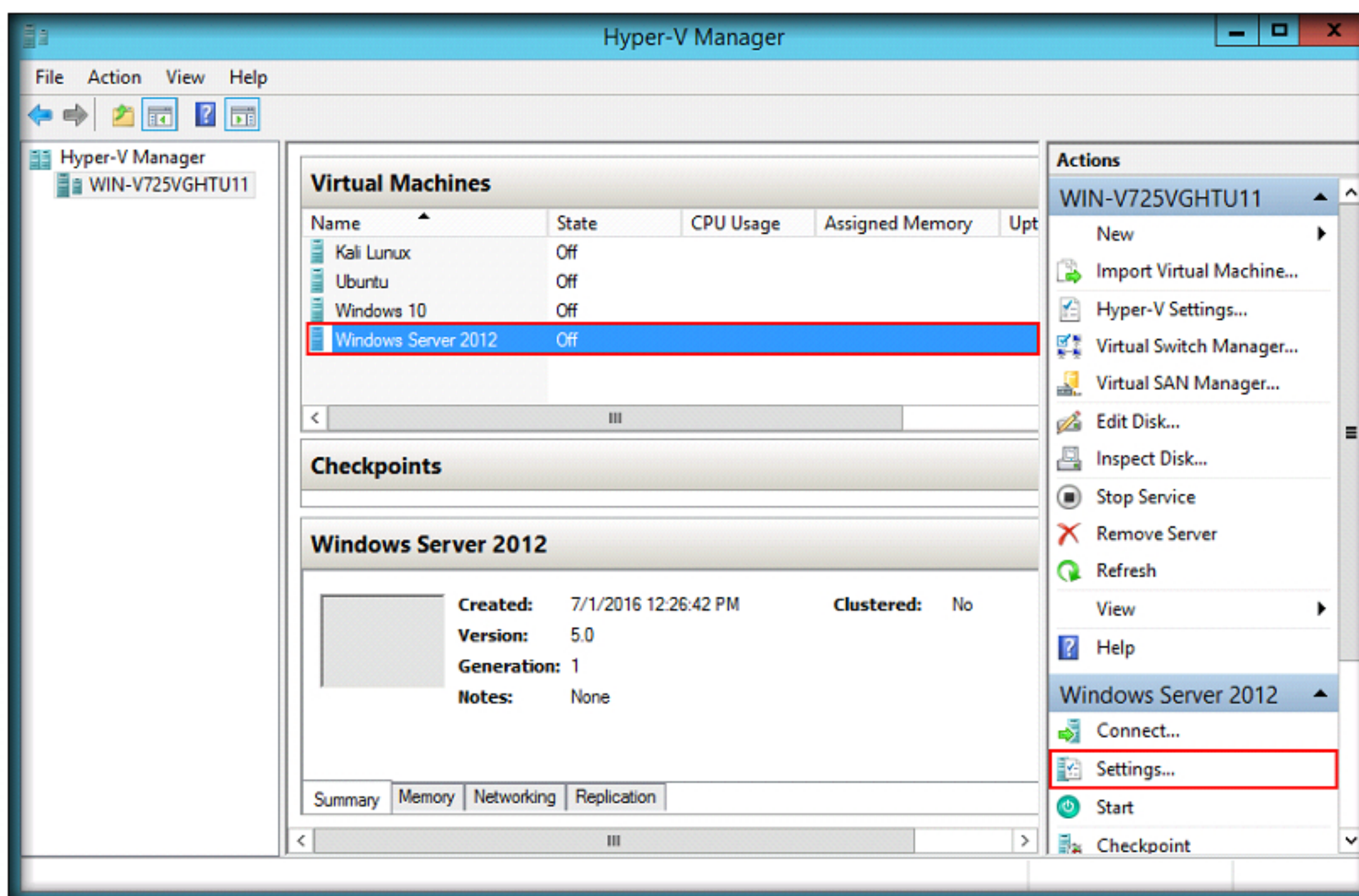


19. Similarly, create **Windows 10**, **Kali Linux** and **Ubuntu** Virtual Machines each with **25GB** of Hard disk space and **1500MB** of RAM memory, and add Internal Network adapter to the virtual machines



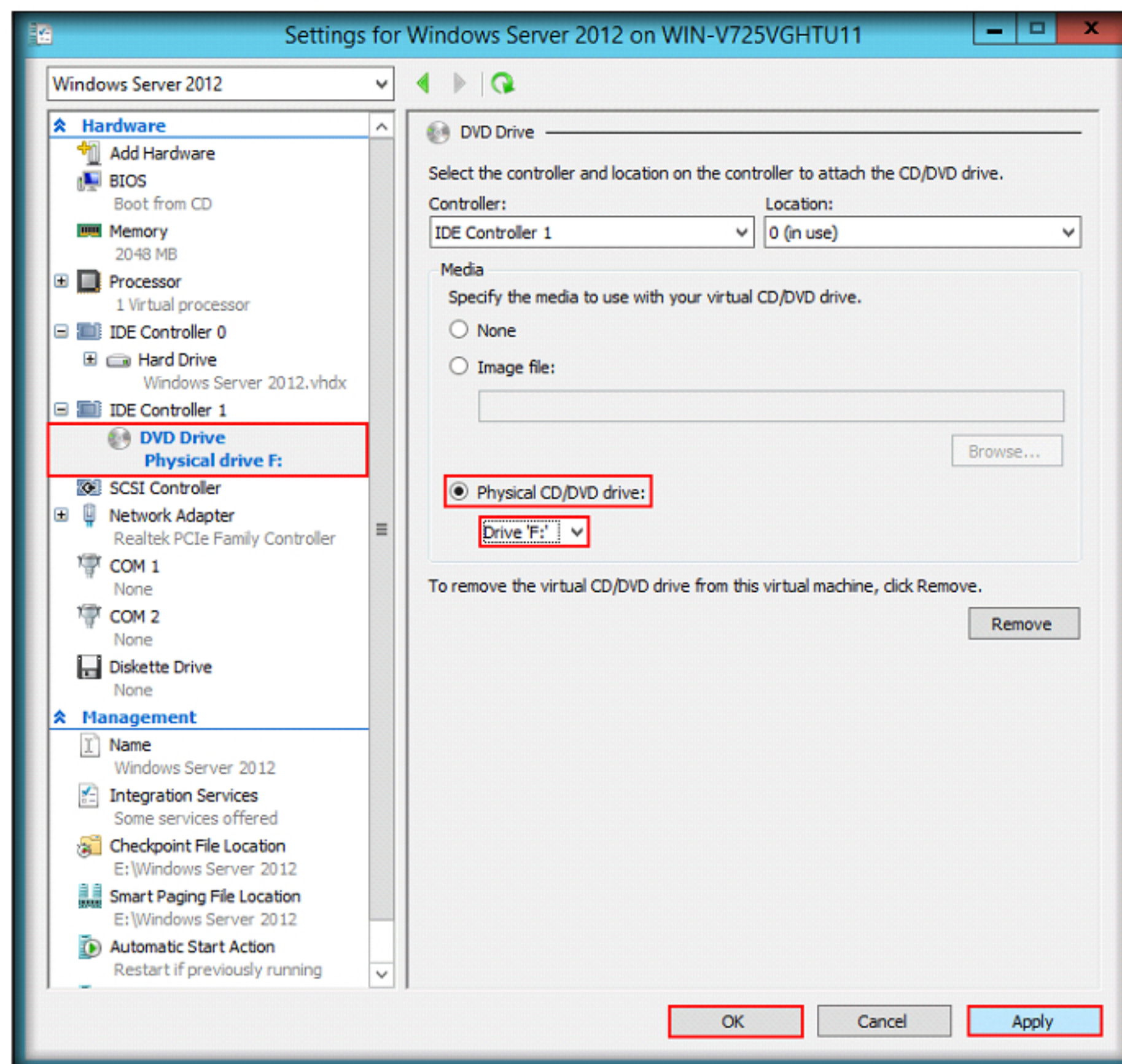
CT#5: Install Windows Server 2012 Operating System in Hyper-V

1. Before beginning this task, you need to insert a **Windows Server 2012** operating system bootable DVD in the **Physical CD/DVD drive**
2. Launch Hyper-V manager and select **Windows Server 2012** virtual machine and click **settings...**

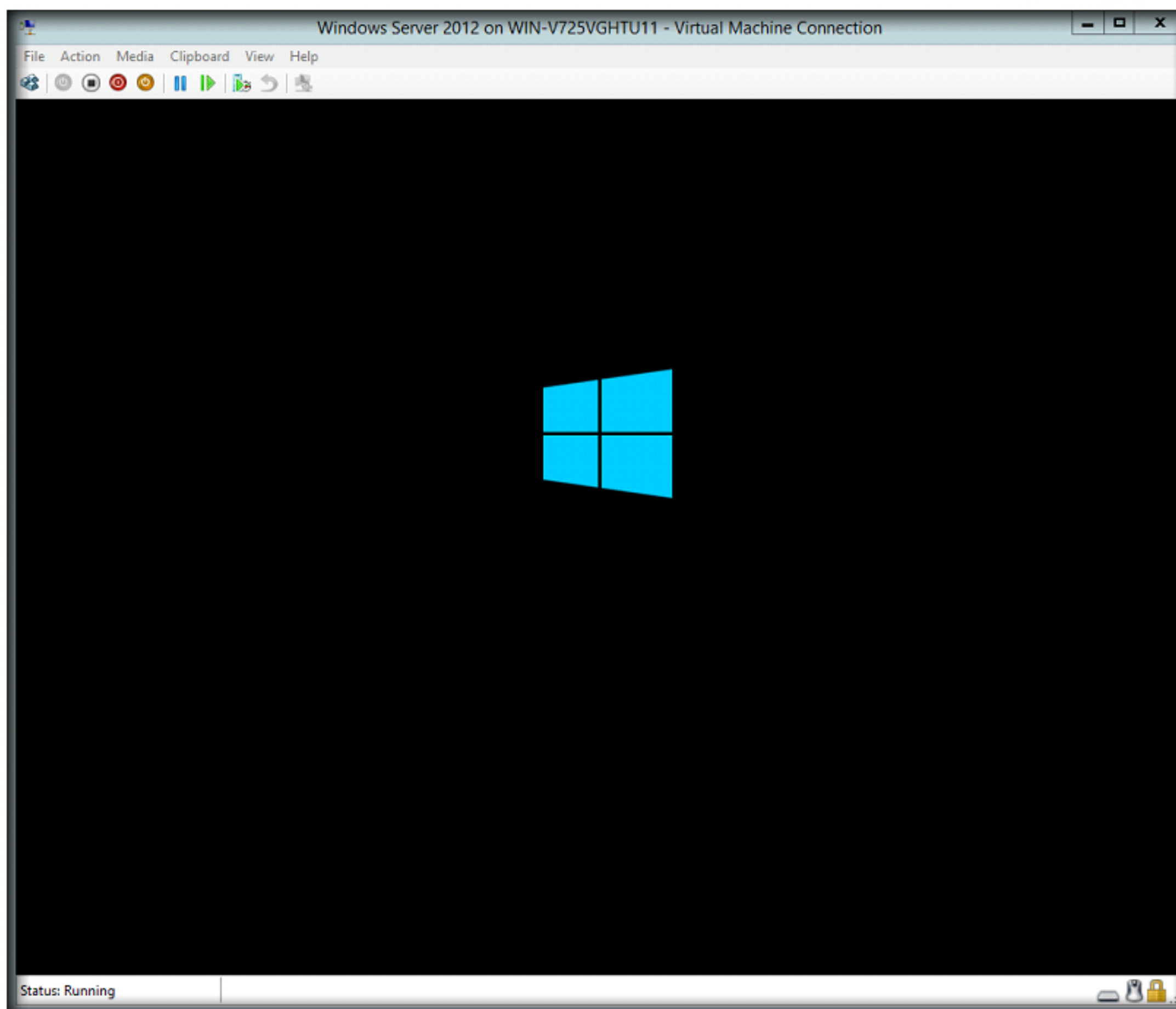


3. Select **DVD Drive** option and click **Physical CD/DVD drive** radio button
4. Click **Apply** and then click **OK**

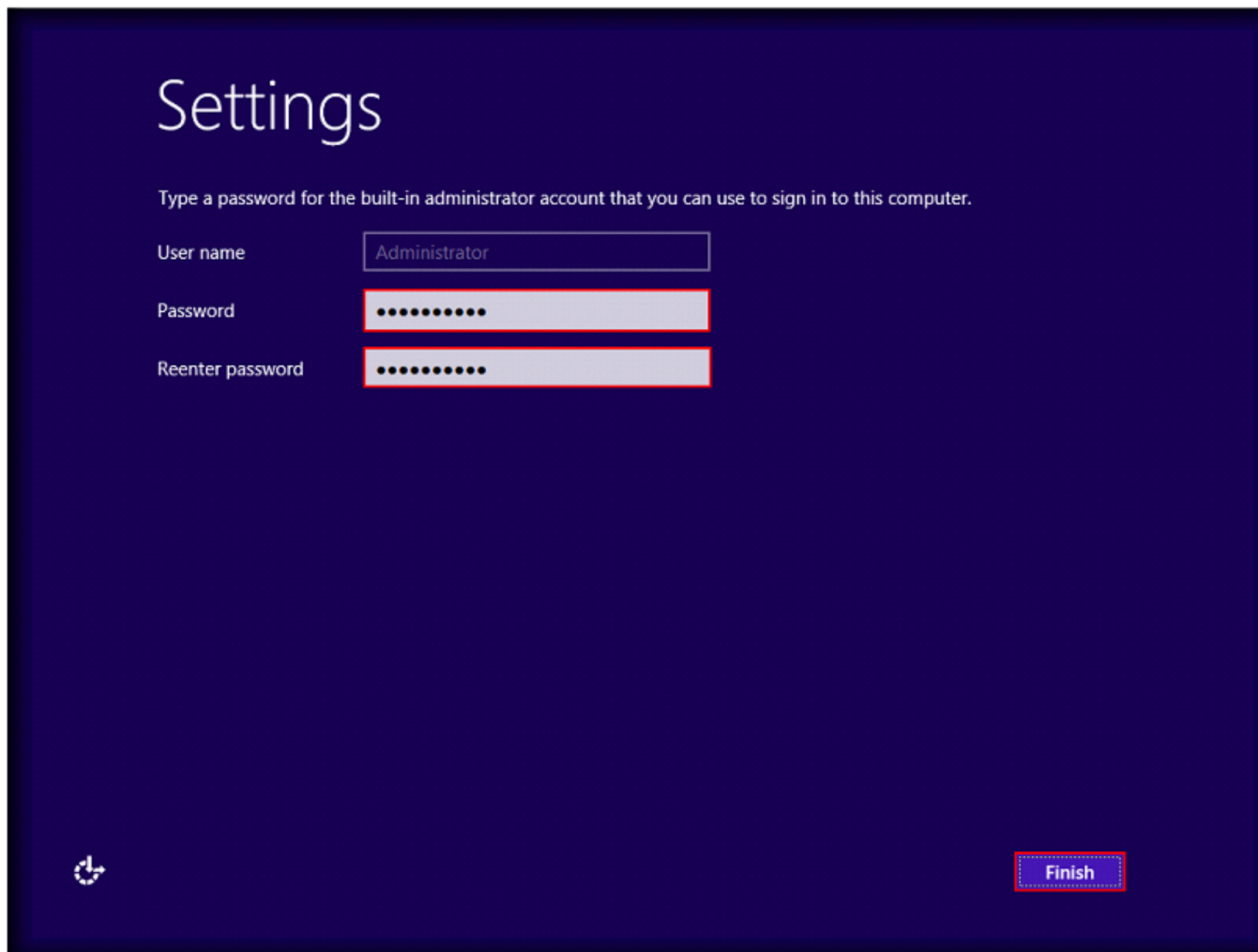
Note: The Physical CD/DVD drive letter may differ in your lab environment.



5. Right-click **Windows Server 2012** in Hyper-V manager and click **Start**
6. Again right-click **Windows Server 2012** and click **Connect**
7. **Boot** Windows Server 2012 virtual machine with DVD-ROM and **Install** Windows Server 2012 operating system



8. Follow the **instructions** during the installation and **install** Windows Server 2012 operating system
9. On installation, **Settings** window appears, where the username is set by default as **Administrator**. Enter the password as **qwerty@123** in **Password** and **Reenter Password** fields, and click **Finish**

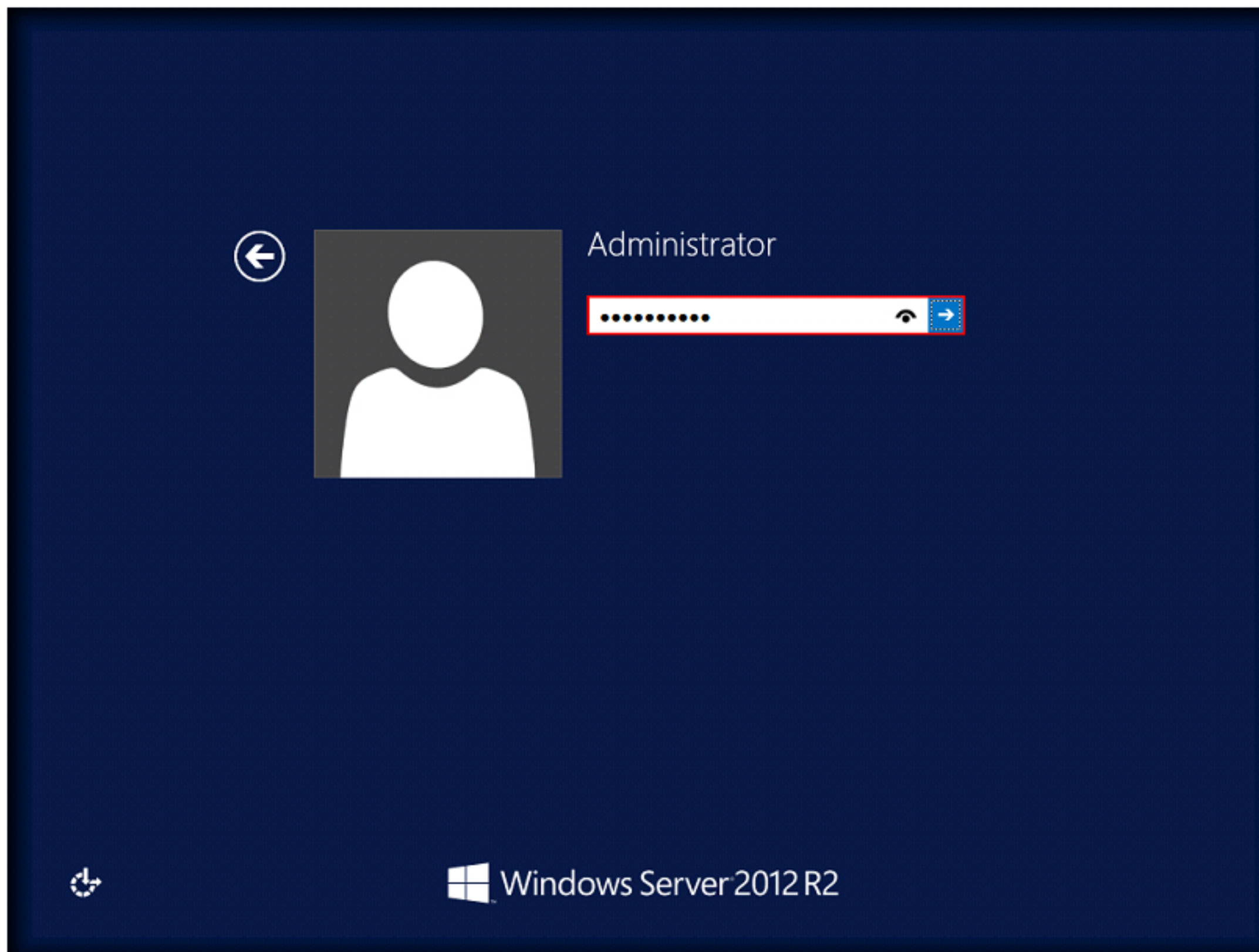


The screenshot shows the 'Settings' window for creating a new user. The title 'Settings' is at the top. Below it, a message says 'Type a password for the built-in administrator account that you can use to sign in to this computer.' There are three input fields: 'User name' with 'Administrator' entered, 'Password' with 'qwerty@123' entered, and 'Reenter password' with 'qwerty@123' entered. A 'Finish' button is at the bottom right. A small icon is at the bottom left.

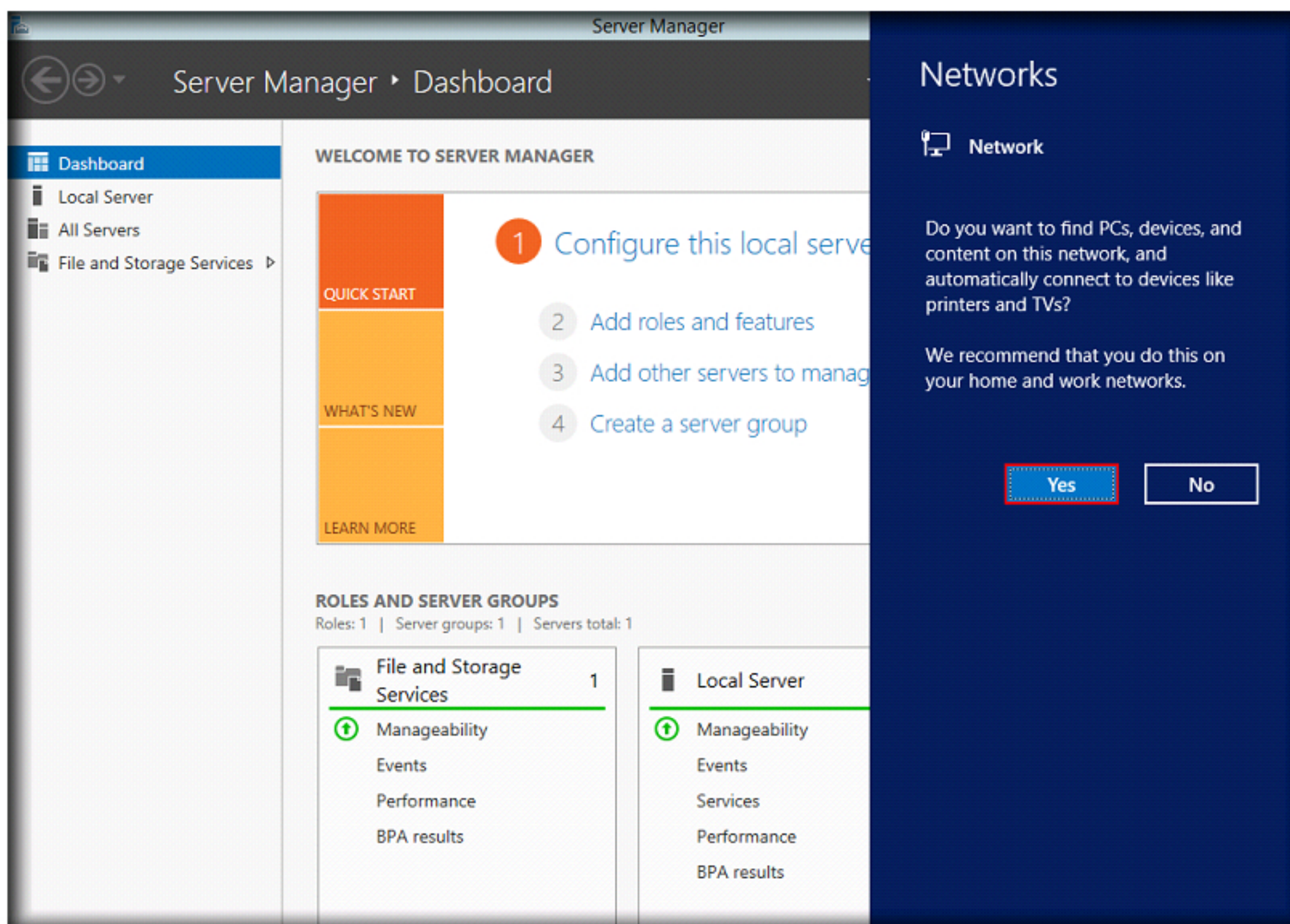
Field	Value
User name	Administrator
Password	qwerty@123
Reenter password	qwerty@123

Finish

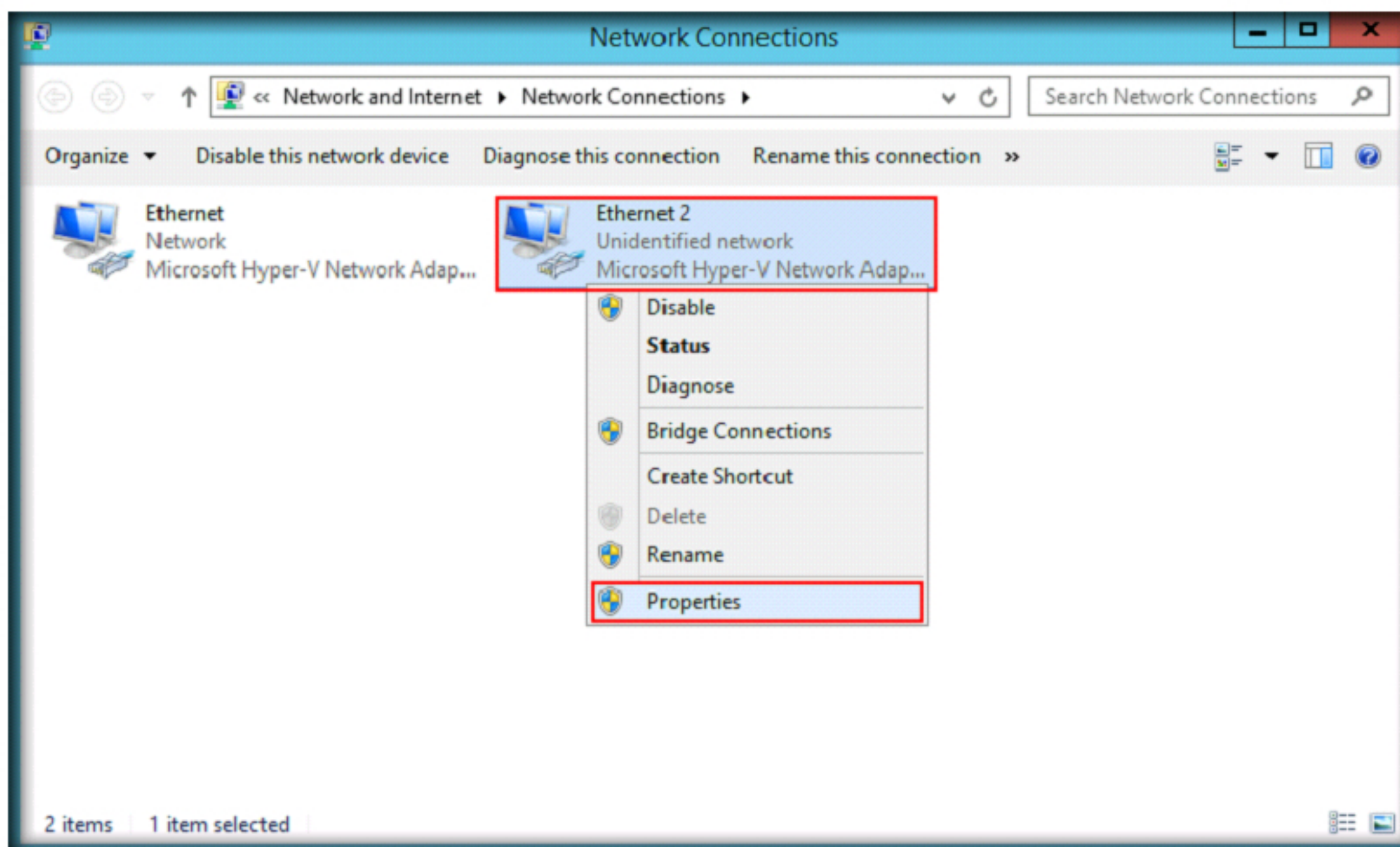
10. Now, the operating system restarts, and the login section appears. Type the password (**qwerty@123**) and press **Enter**.



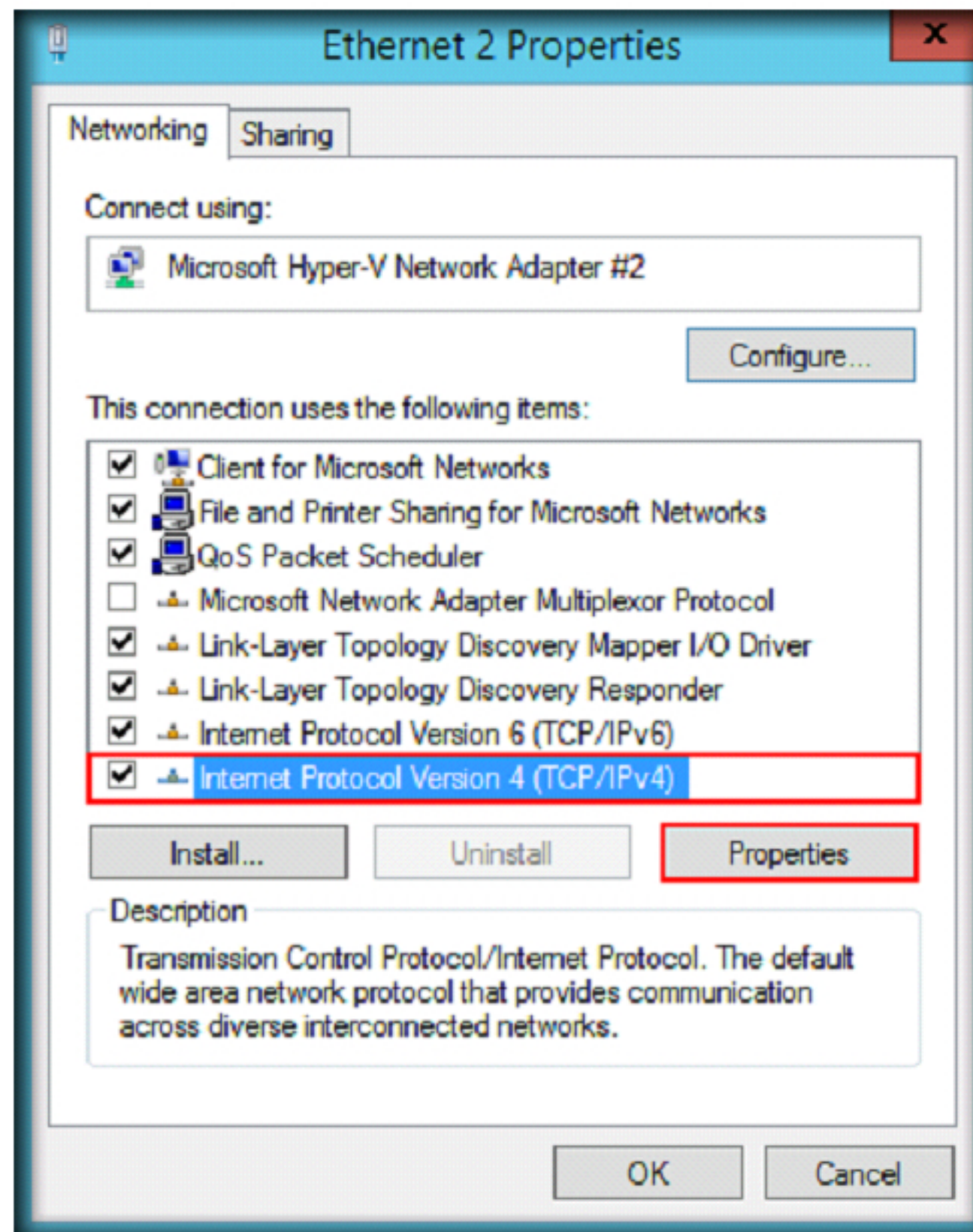
11. Once the machine is logged on, a Networks section appears in the right-pane of the window. Click **Yes** to close the section.
12. Then, close the **Server Manager** window



13. Launch **Control Panel** and go to **Network Connections** window. In the **Network Connections** window, right-click on the adapter associated with **Internal Network (Ethernet 2)** and click **Properties**.



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



15. Select **Use the following IP address** radio button, assign **10.0.0.12** as **IP address**, **255.0.0.0** as **Subnet mask**, **10.0.0.1** as **Default gateway**, and click **OK**

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 . 0 . 0 . 12

Subnet mask: 255 . 0 . 0 . 0

Default gateway: 10 . 0 . 0 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

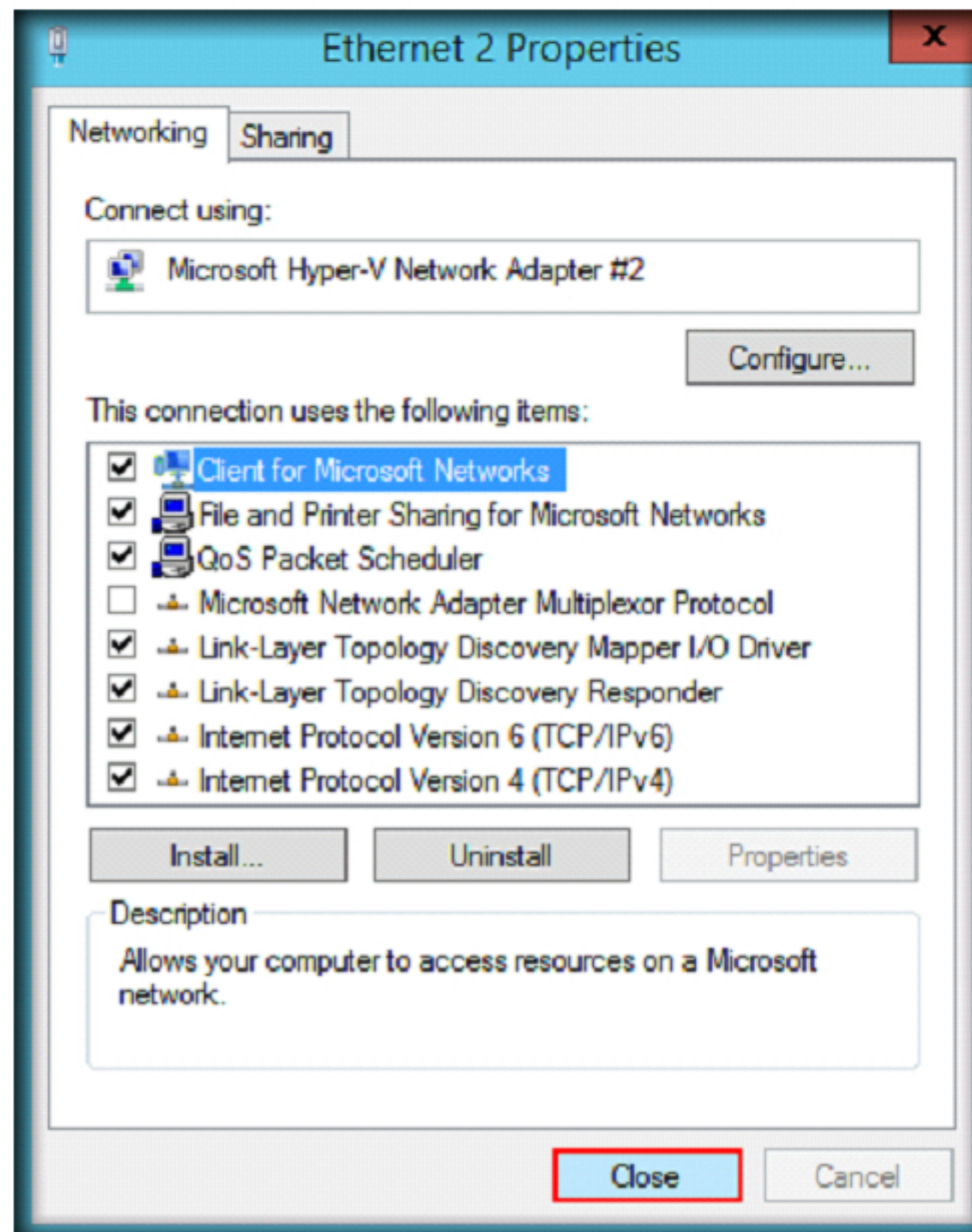
Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

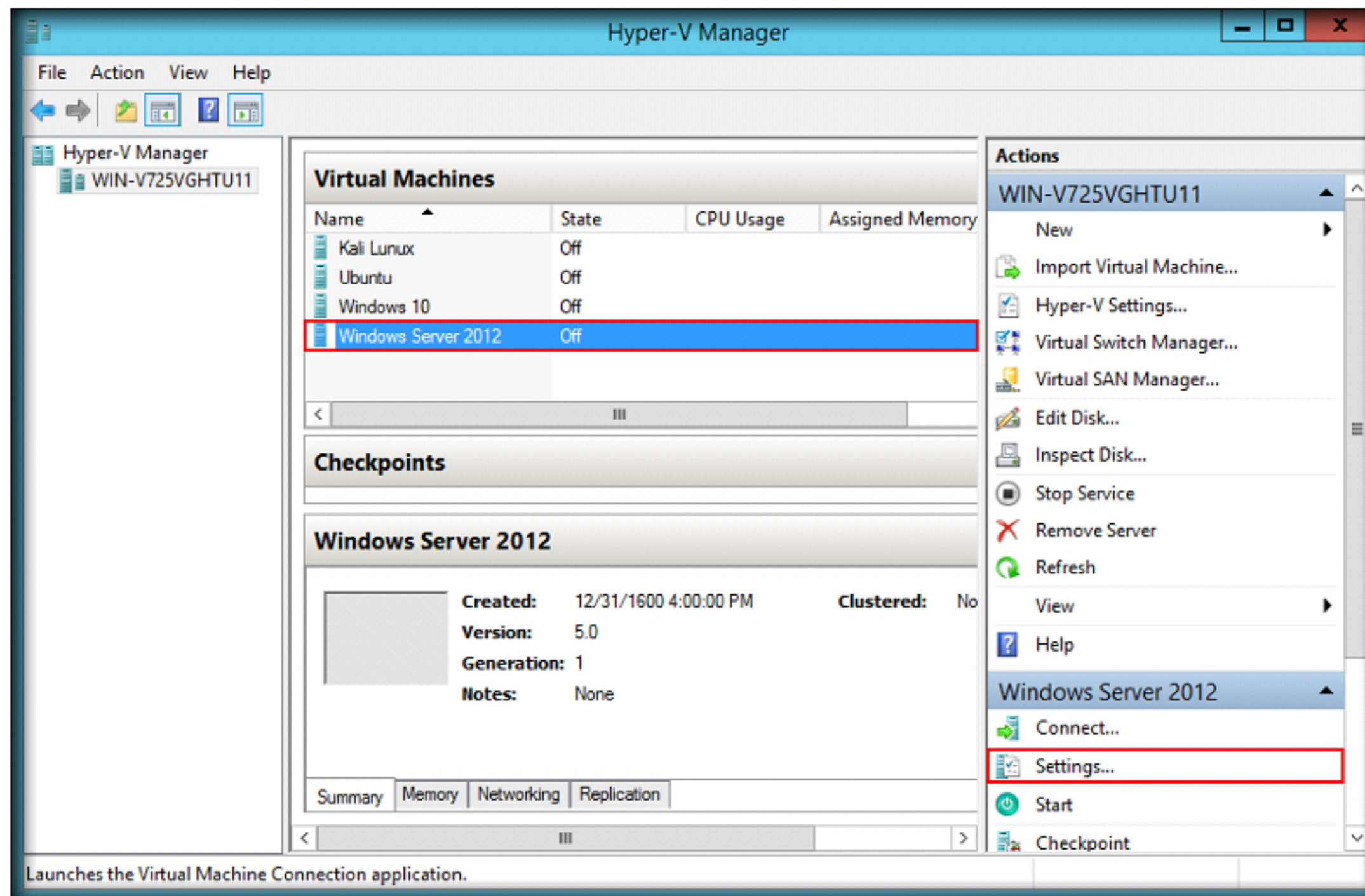
OK Cancel

16. **Close** the **Properties** window

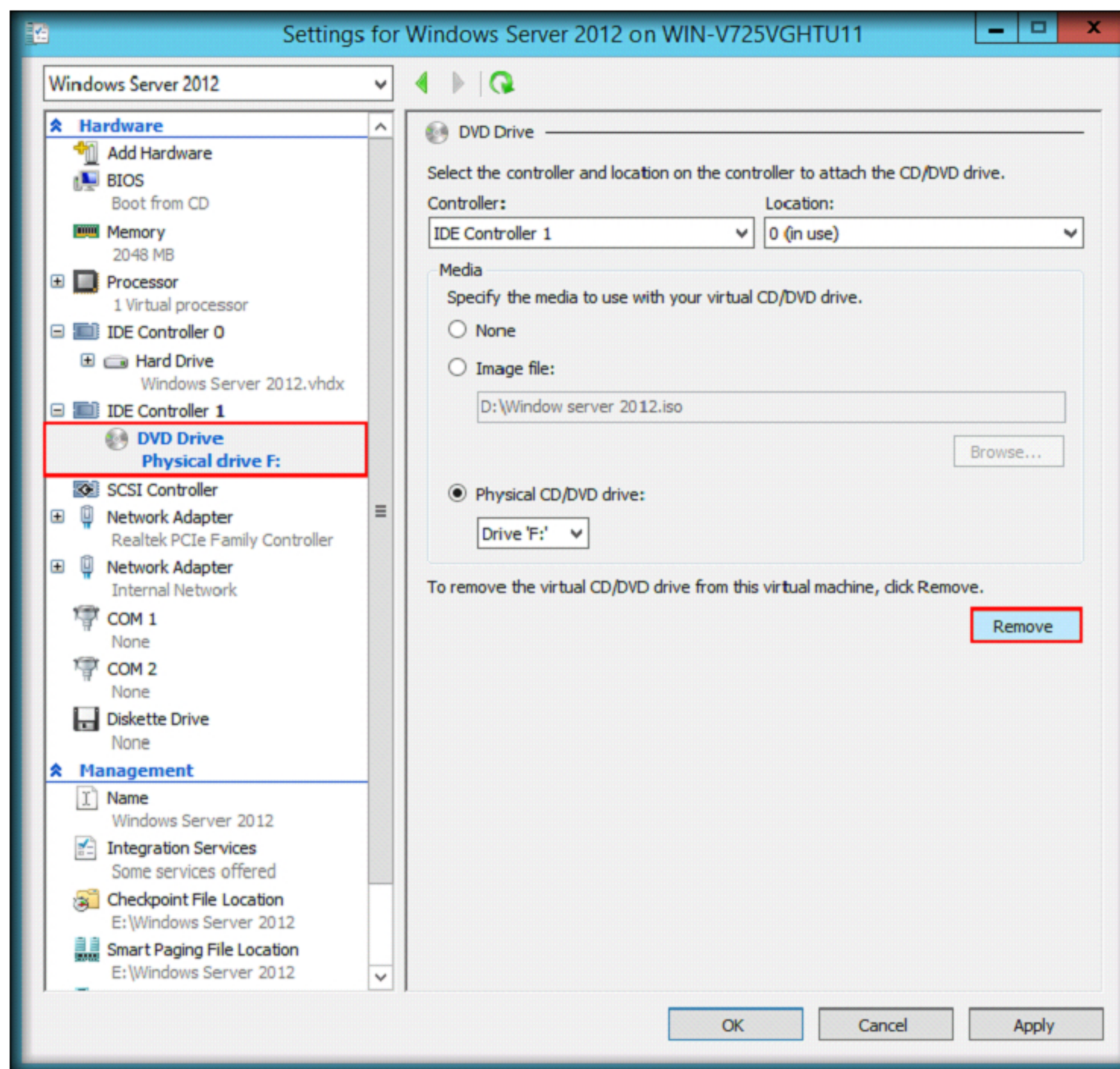


17. Now, check whether **Windows Server 2012** is installed and **working properly** and also check whether **Internet** is accessible
18. Once verified, **shutdown Window Server 2012** virtual machine
19. Similarly install **Windows 10 (64-bit)** OS in respective Virtual Machine with **25GB** of Hard Disk space and **1500MB** of RAM memory. While installing the operating system, you need to create an additional partition of **4GB**.
20. Assign **10.0.0.10** as **IP address**, **255.0.0.0** as **Subnet mask** and **10.0.0.1** as **Default gateway** for the internal network adapter of **Windows 10**
21. Once the above guest OS is installed, go to Hyper-V Manager, select **Windows Server 2012** and click on **Settings...** located at the right pane of the Hyper-V control window
22. Remember, you **CANNOT** change virtual machine **settings** while it is running
23. Make sure that you **shutdown** virtual machine **properly** before making changes in virtual machine **settings**

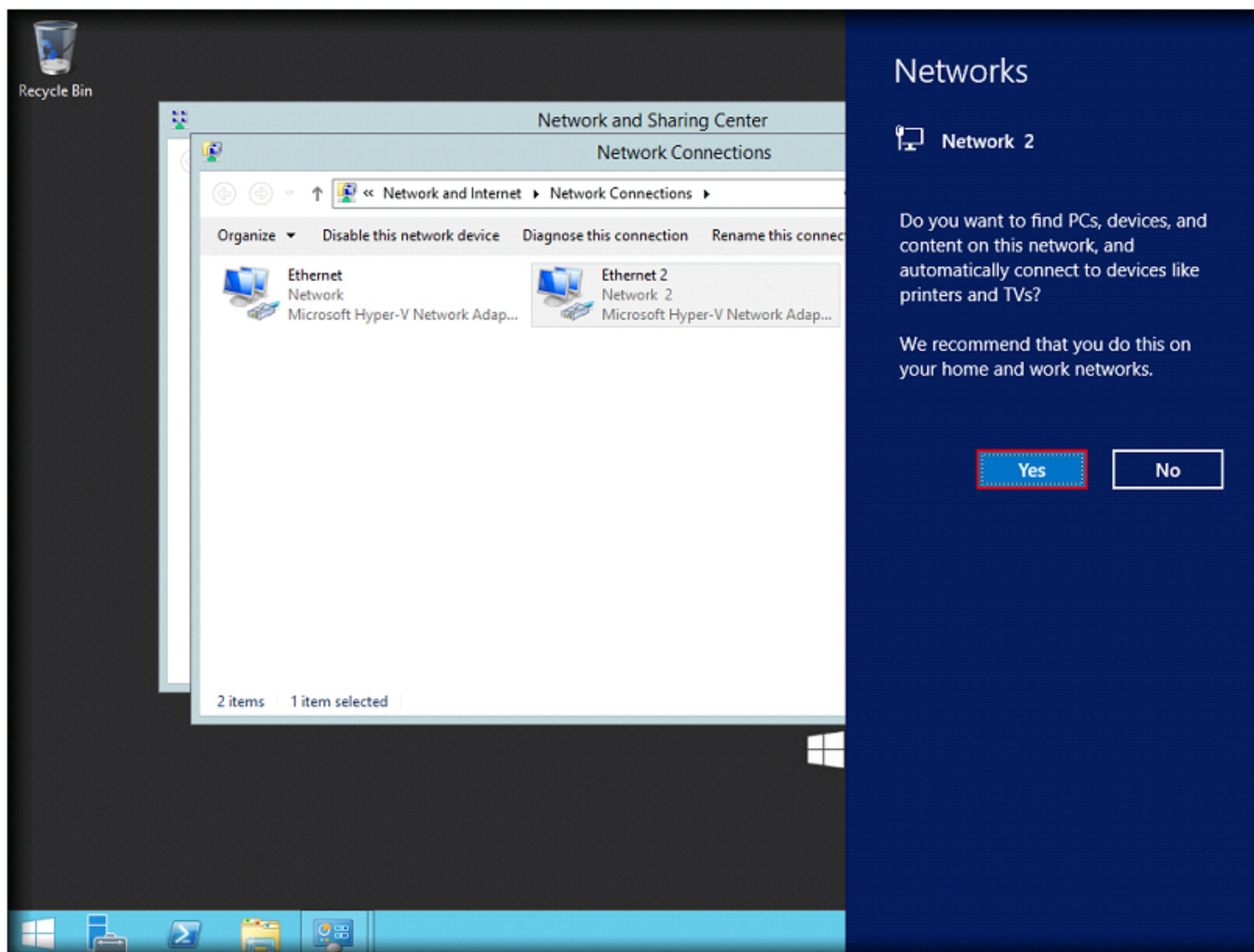
24. Select **Windows Server 2012** virtual machine, and then click **Settings** in the right-pane



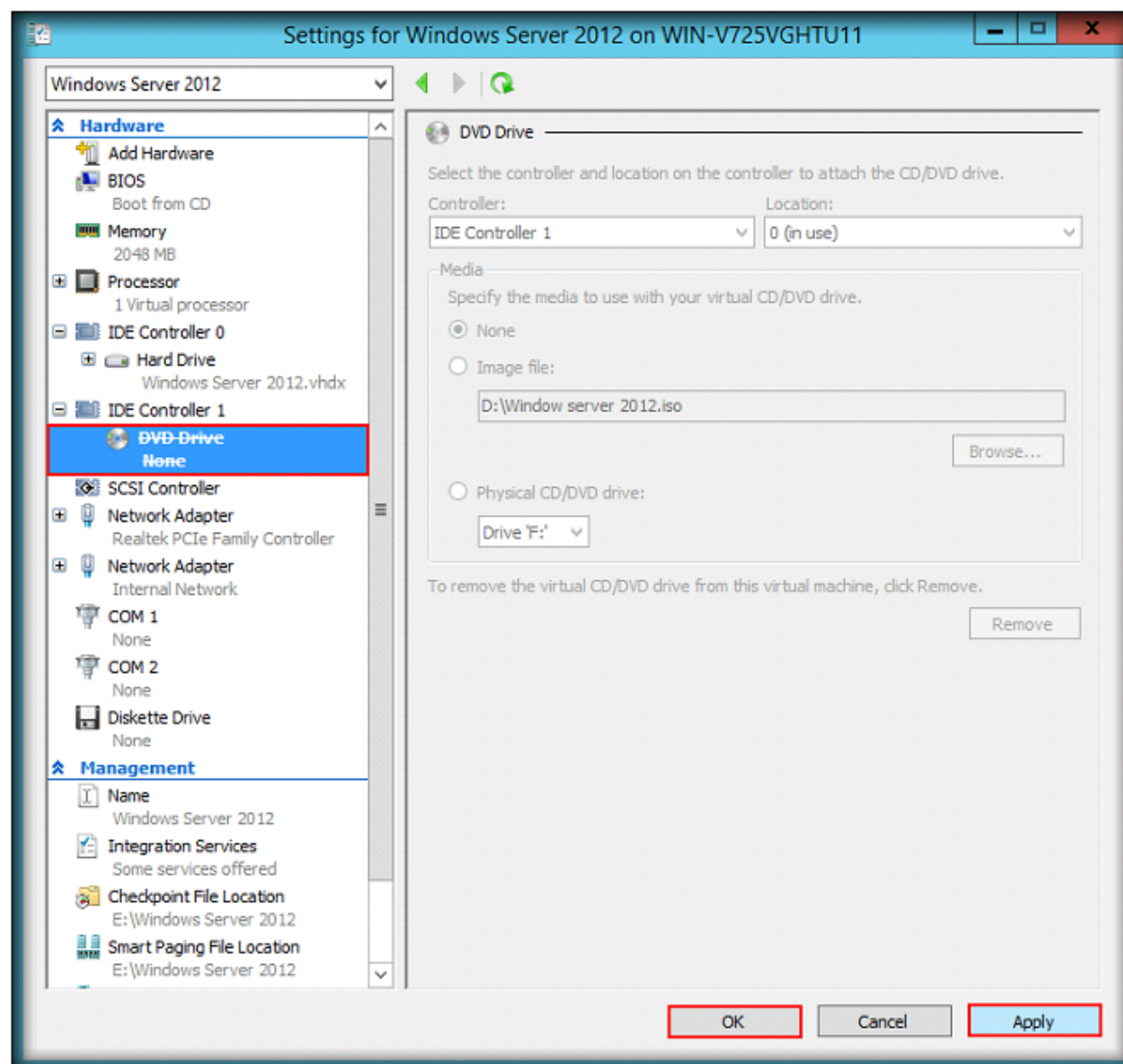
25. **Setting** for **Window Server 2012** window appears, click **DVD Drive** option in the left pane of the Hyper-V Manager window
26. Click **Remove** button located at the right pane of the window



27. If a **Networks** notification appears in the right pane, click **Yes**

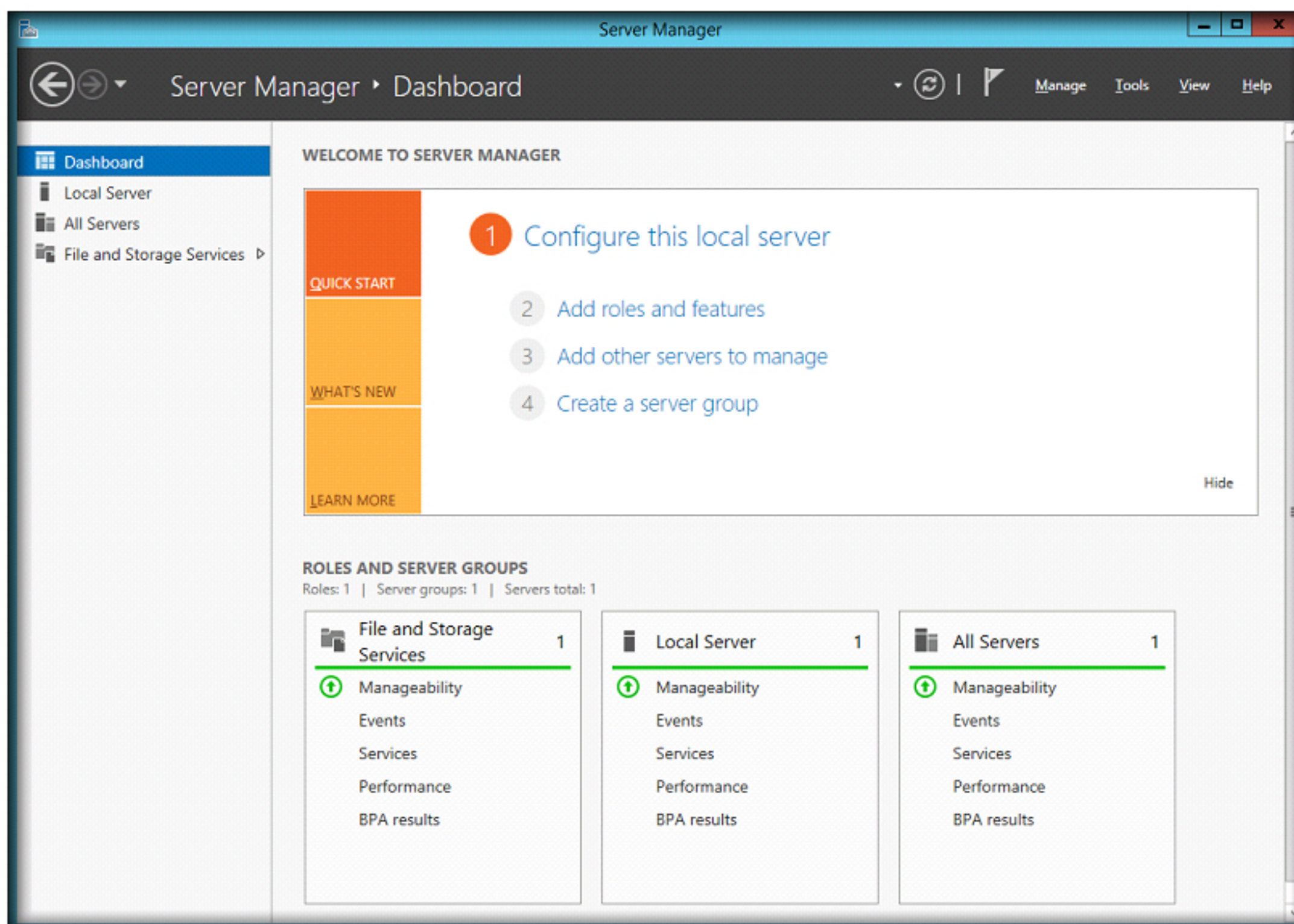


28. After clicking Remove, click **Apply** and then click **OK**
29. Perform the **steps 24-28** for the **Windows 10** virtual machines to remove DVD Drive
30. The purpose of removing DVD Drive is to **enable multiple** virtual machines to **start** simultaneously
31. If this DVD Drive is not removed, you **CANNOT** start multiple virtual machines **simultaneously**

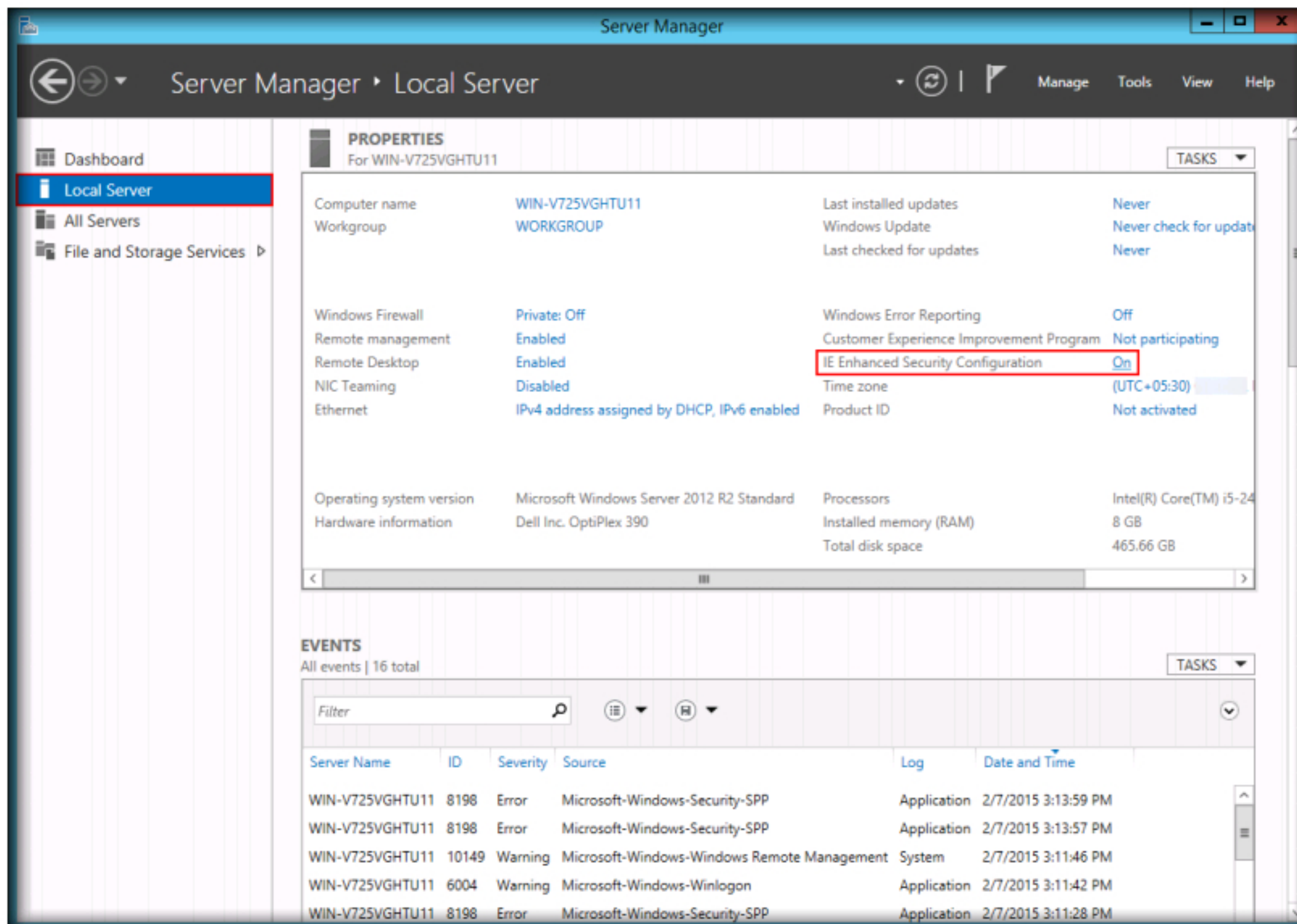


CT#6: Configure Internet Explorer (IE) Enhanced Security Configuration in Windows Server 2012 Virtual Machine

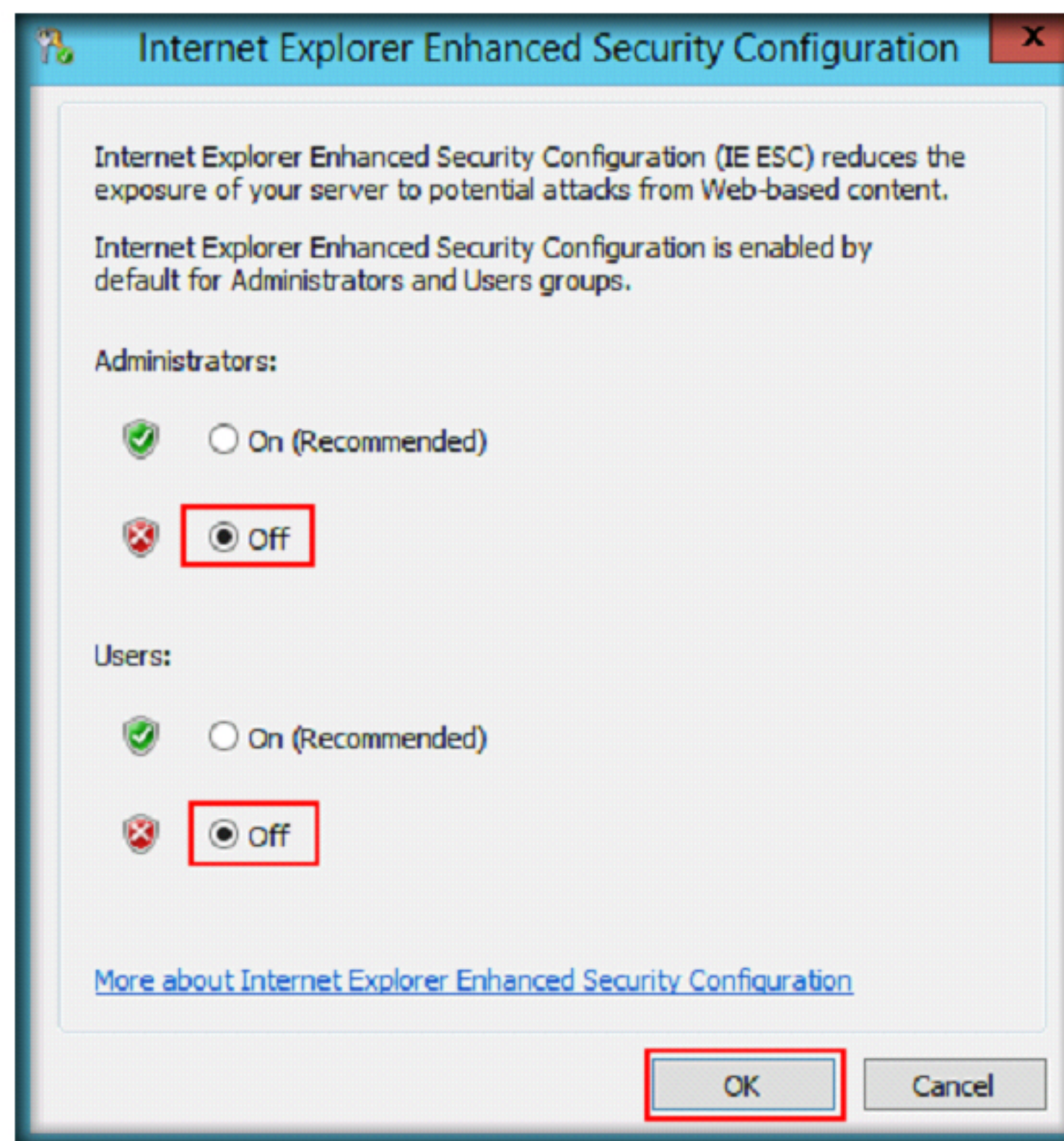
1. To configure Internet Explorer Enhanced Security Configuration, go to **Start** → **Server Manager** App
2. **Server Manager** main window appears. By default Dashboard will be selected



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



4. **Internet Explorer Enhanced Security Configuration** window appears
5. Select **Off** radio button for both **Administrators** and **Users** sections and click **OK**

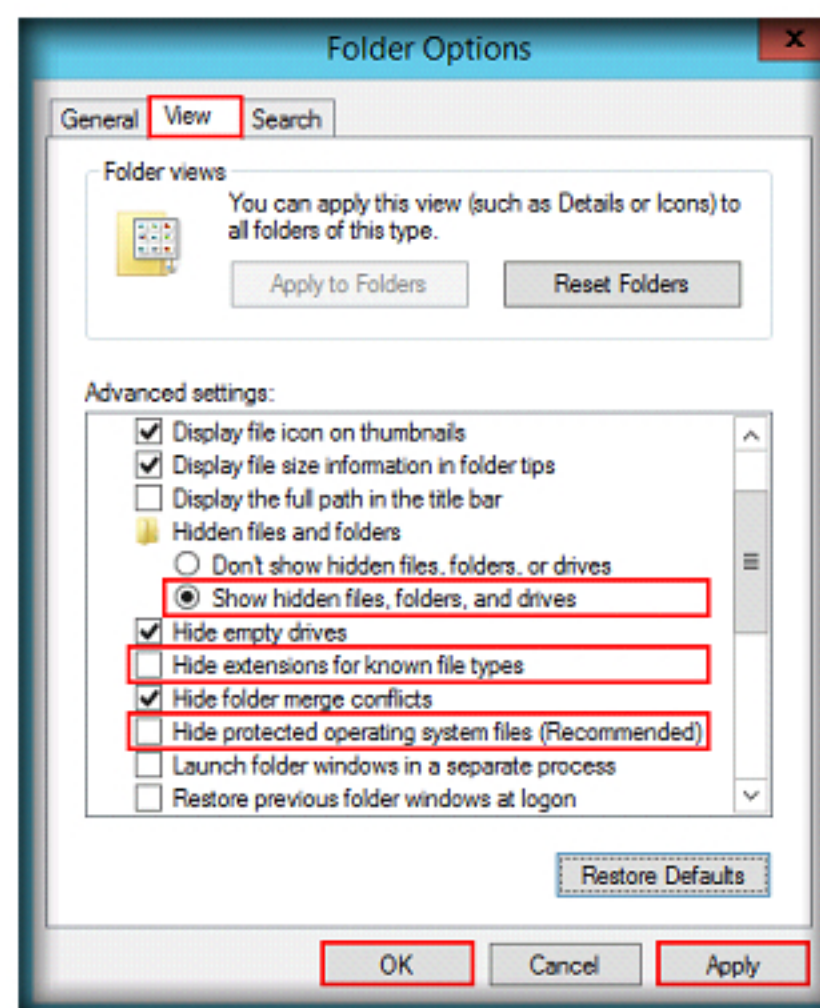


CT#7: Disable DEP in Windows Server 2012 Virtual Machine

1. Click **Start → Control Panel → System and Security**
2. In **System and Security** window click **System**
3. Click **Advanced system settings** on the left pane of the Control Panel window
4. **System Properties** window appears
5. Click **Advanced** tab and click **settings** button of **Performance** section
6. **Performance Options** window appears. Click **Data Execution Prevention** tab
7. Select the radio button for **Turn on DEP for essential Windows programs and Services only**
8. Click **Apply** and then click **OK**
9. Click **OK** to close the System Properties Window and close **System** window
10. It might prompt to **reboot** the system for the changes to take effect, so reboot the machine

CT#8: Configure Windows Explorer in Windows Server 2012 Virtual Machine

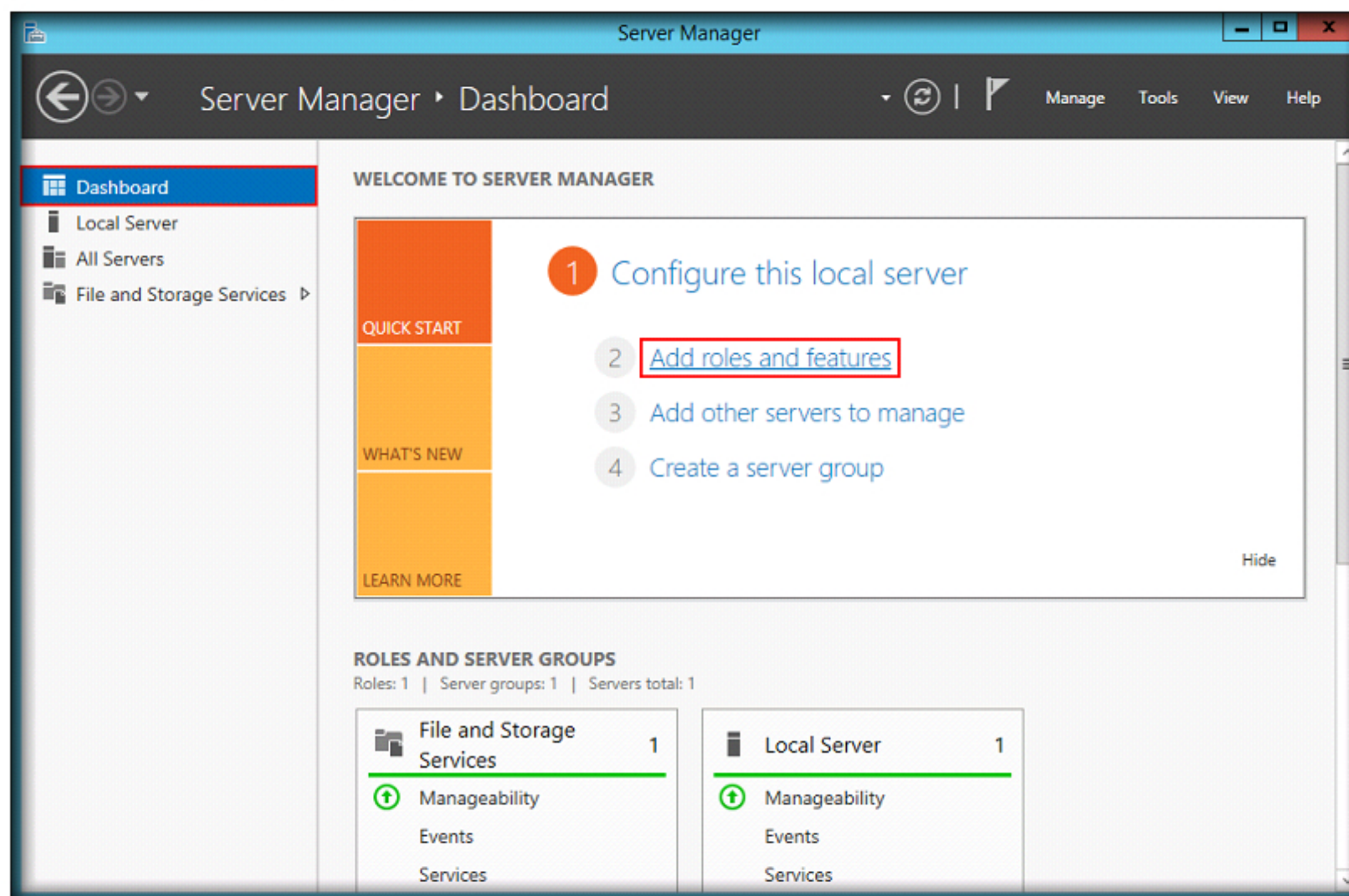
1. Click **Start** → **Control Panel**
2. Control Panel appears on the screen, select **Small icons** from the **Category** drop down list to see all the control panel options.
3. Double-click **Folder Options**
4. The **Folder Options** window appears
5. In the **Folder Options** window, click the **View** tab
6. In the **Advanced Settings** section, under **Hidden files and folders**, check **Show hidden files and folders**, uncheck **Hide extensions for known file types** and uncheck **Hide protected operating system files (Recommended)**. Click **Apply**, and then click **OK**.



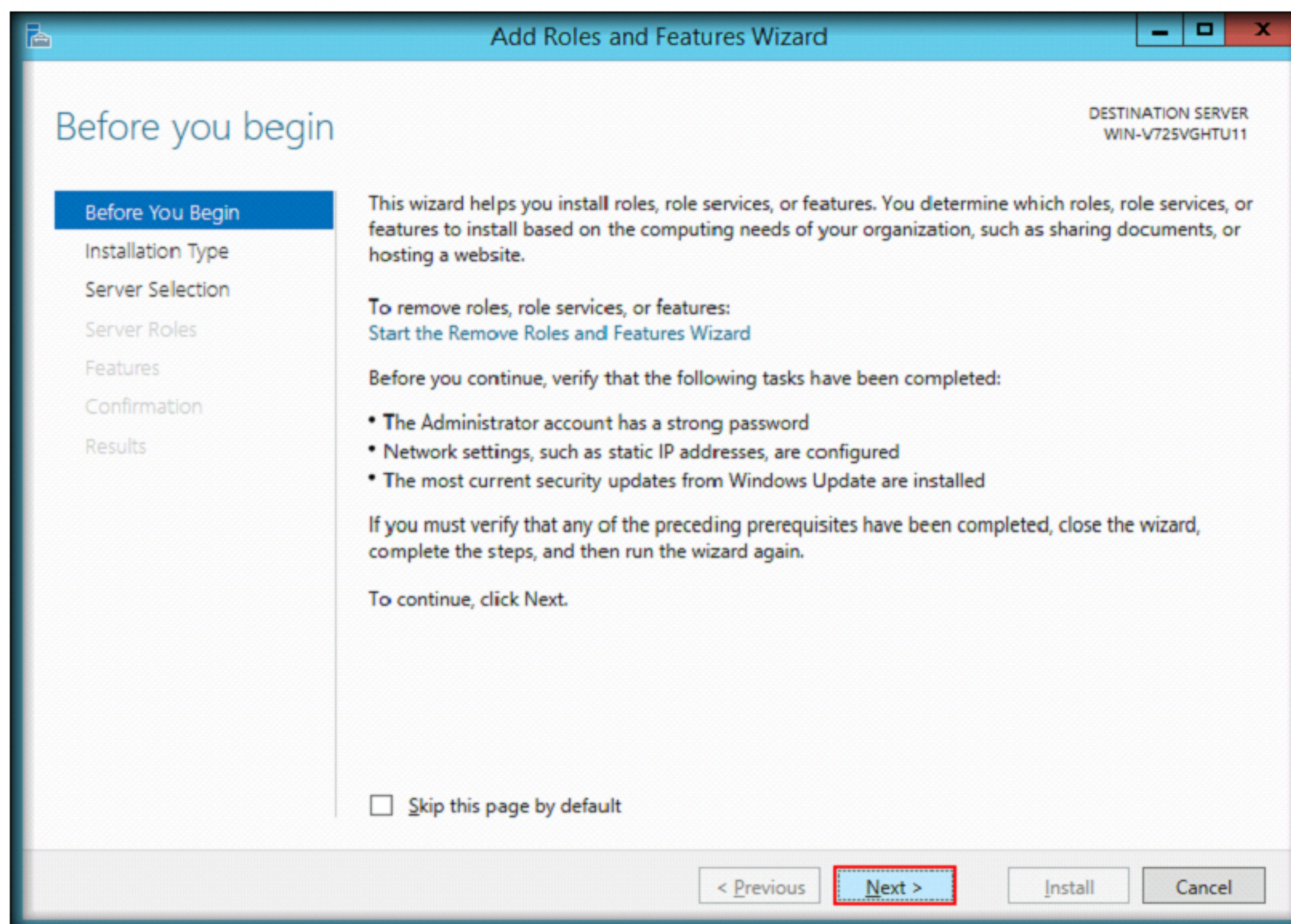
7. In the same way, configure these settings in Windows 10 virtual machine

CT#9: Adding .NET Framework and Telnet Roles in Windows Server 2012 Virtual Machine

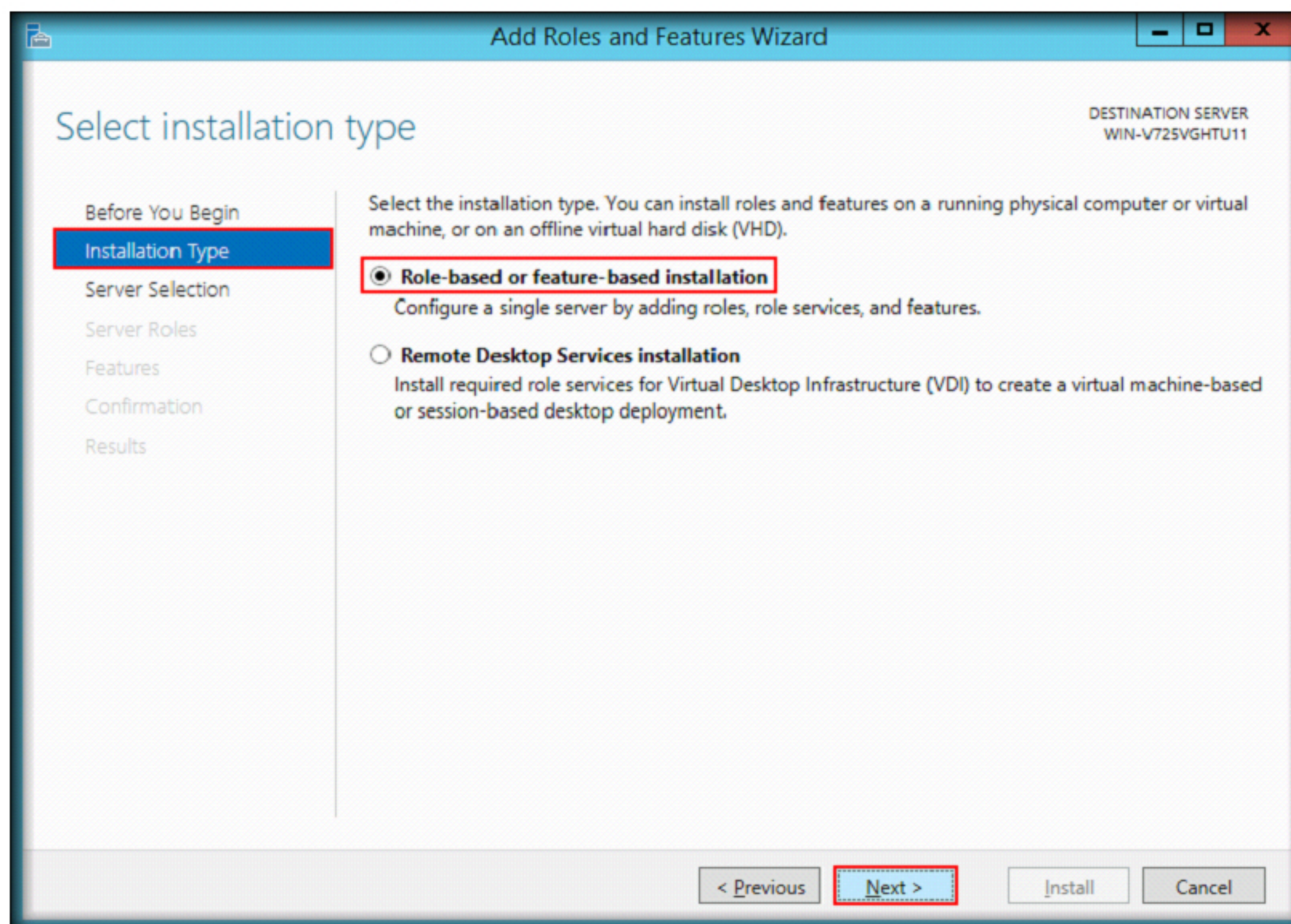
1. Launch Windows Server 2012 virtual machine from Hyper-V
2. Select **Server Manager** from the **Apps** screen



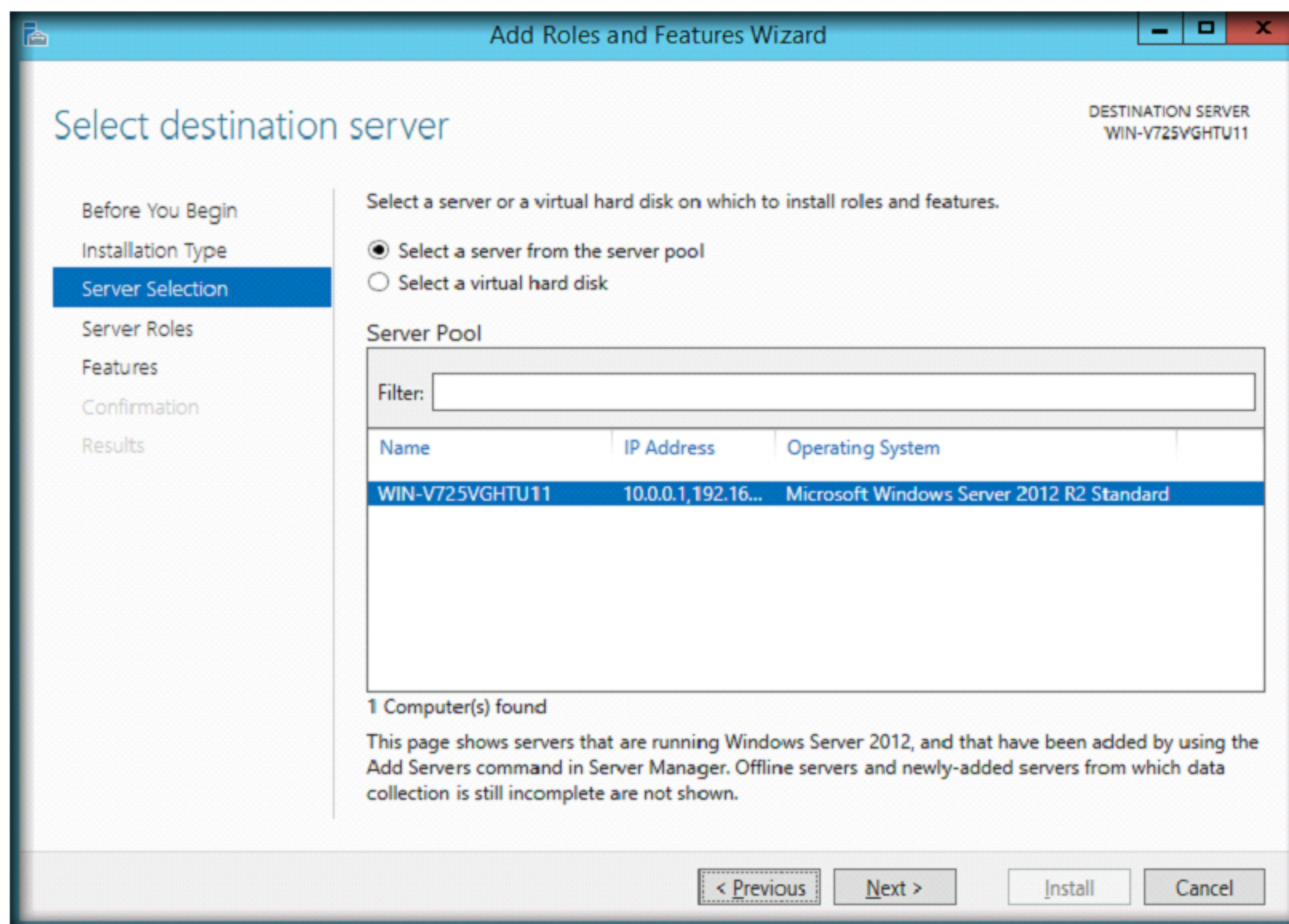
3. **Add Roles and Features** Wizard appears, click **Next**



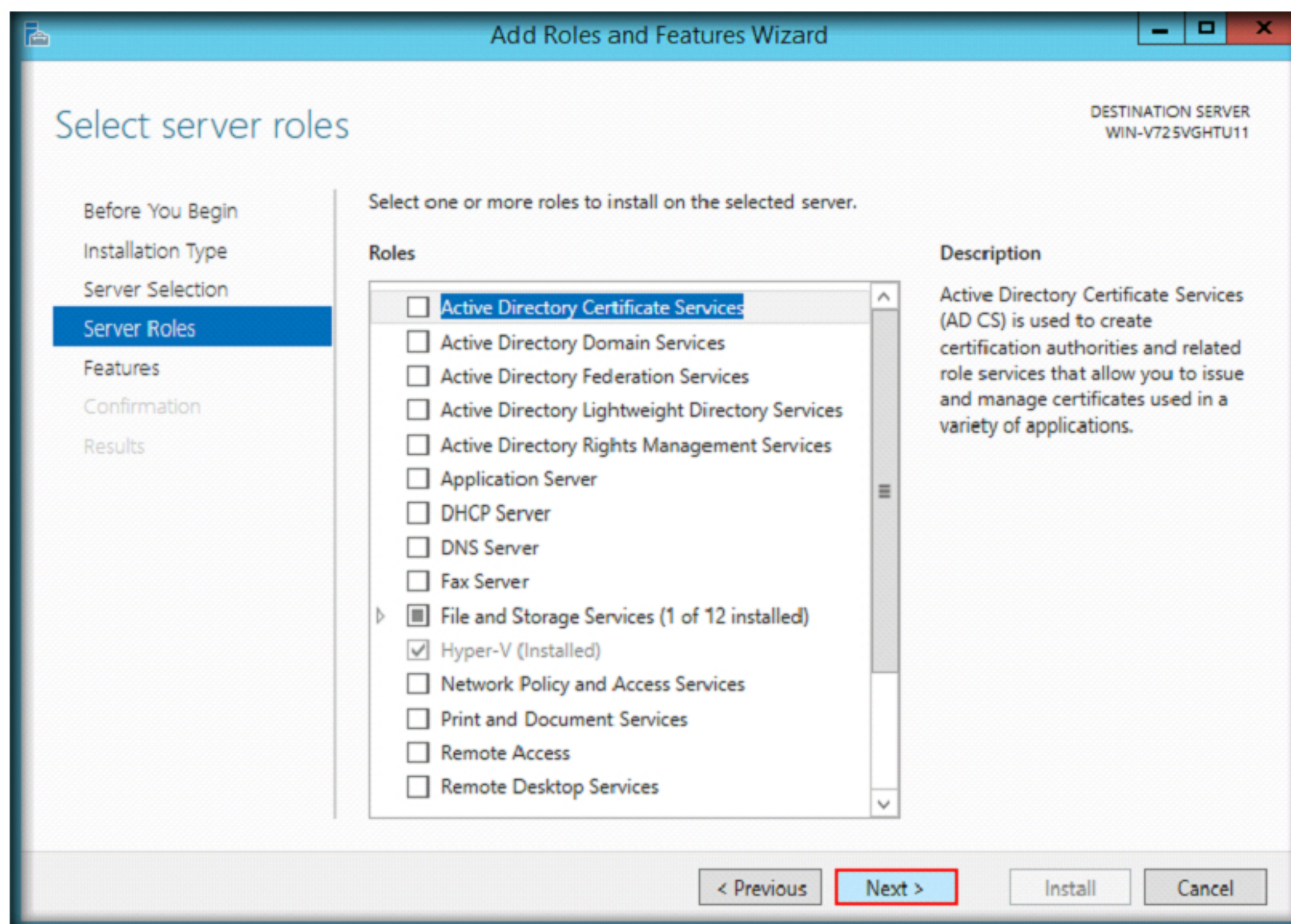
4. In **Installation Type** section of the wizard, select **Role-based or feature-based installation** radio button and click **Next**



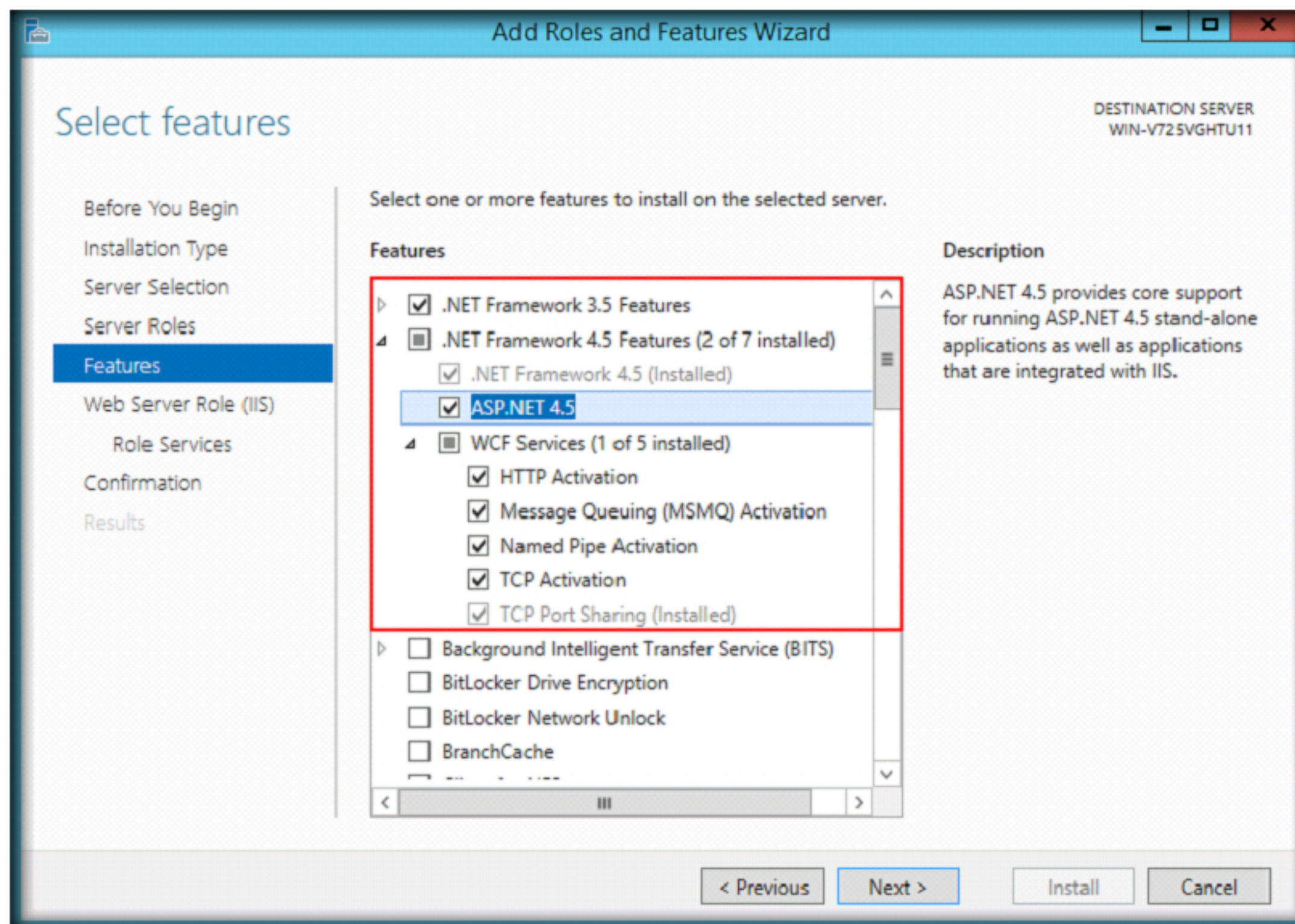
5. In **Server Selection** section, leave the selections to default and click **Next**



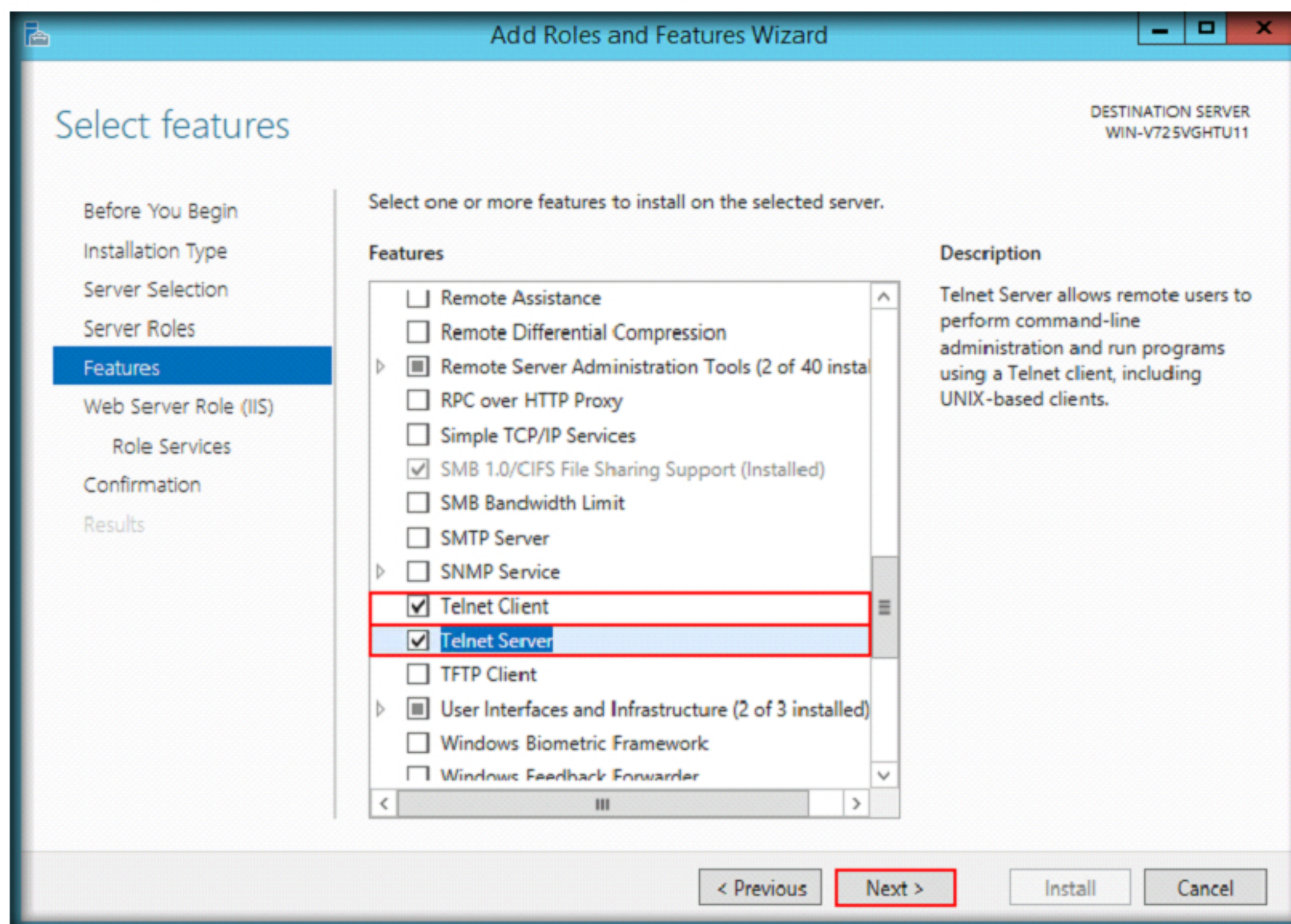
6. **Server Roles** section appears, click **Next**



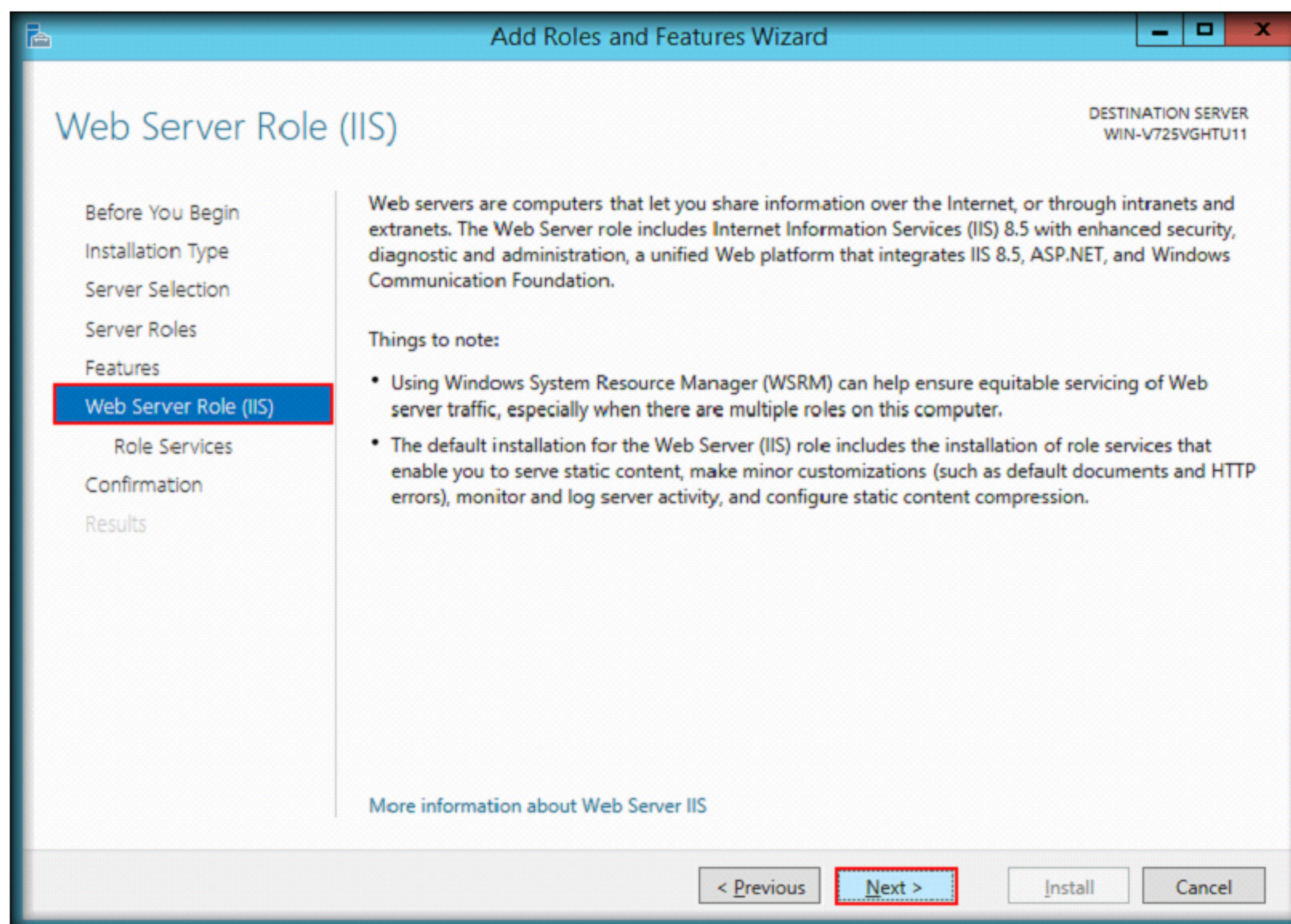
7. **Features** section appears, select the checkbox for **.NET Framework 3.5** Feature and select all the checkboxes under **.NET Framework 4.5** Features



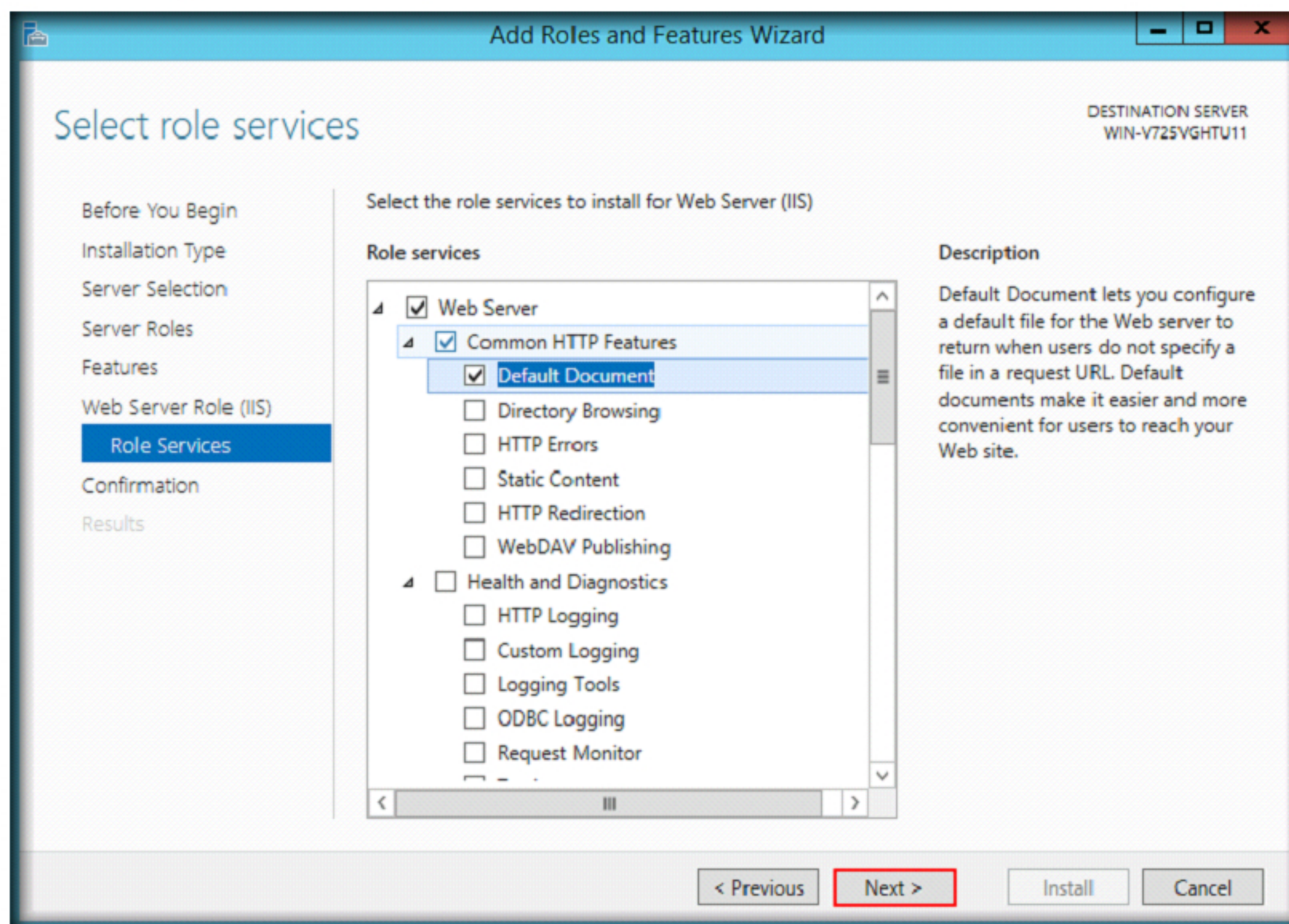
8. Scroll down the section, check **Telnet Client** and **Telnet Server**, and click **Next**



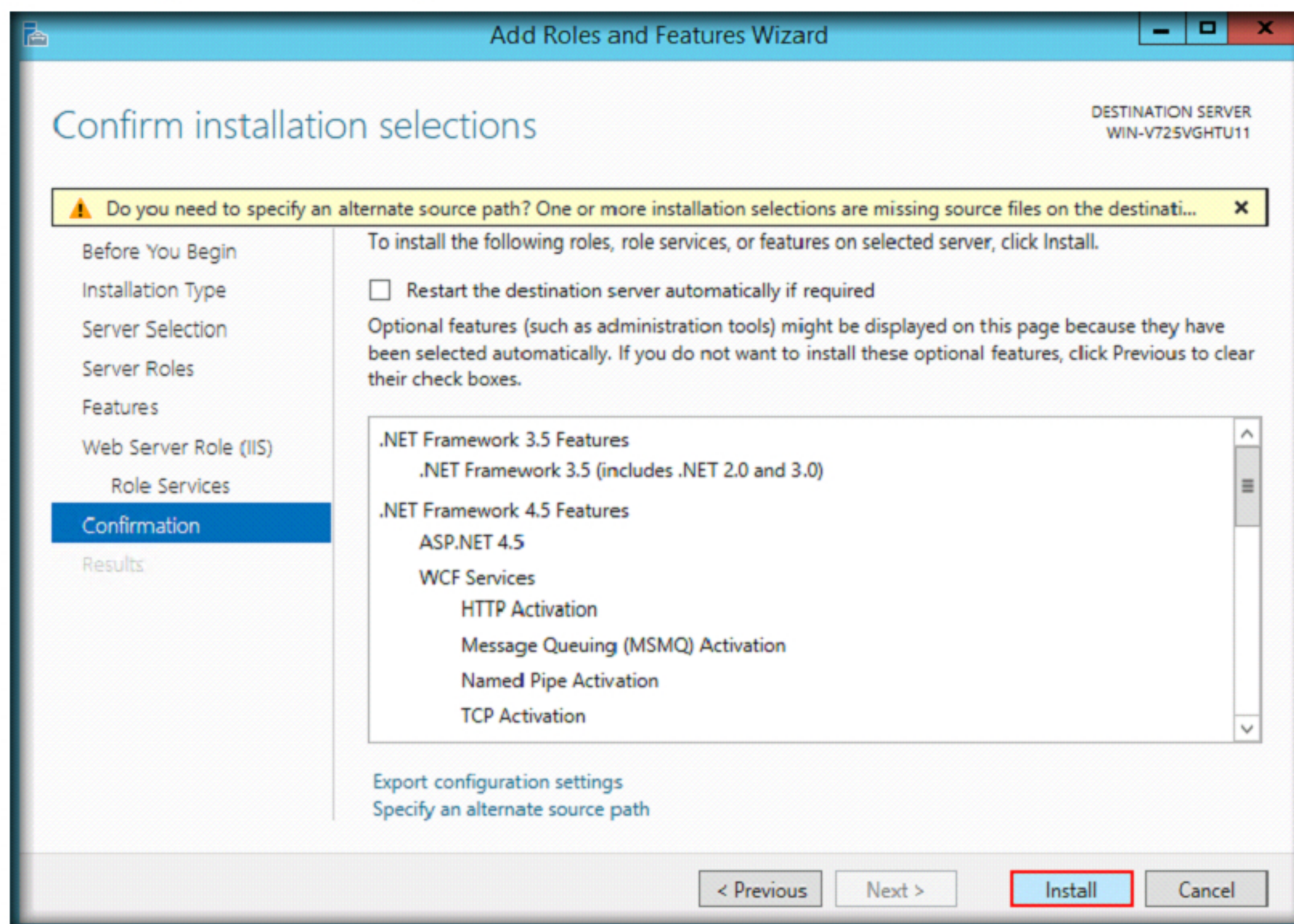
9. **Web Server Role (IIS)** section appears in the wizard, click **Next**



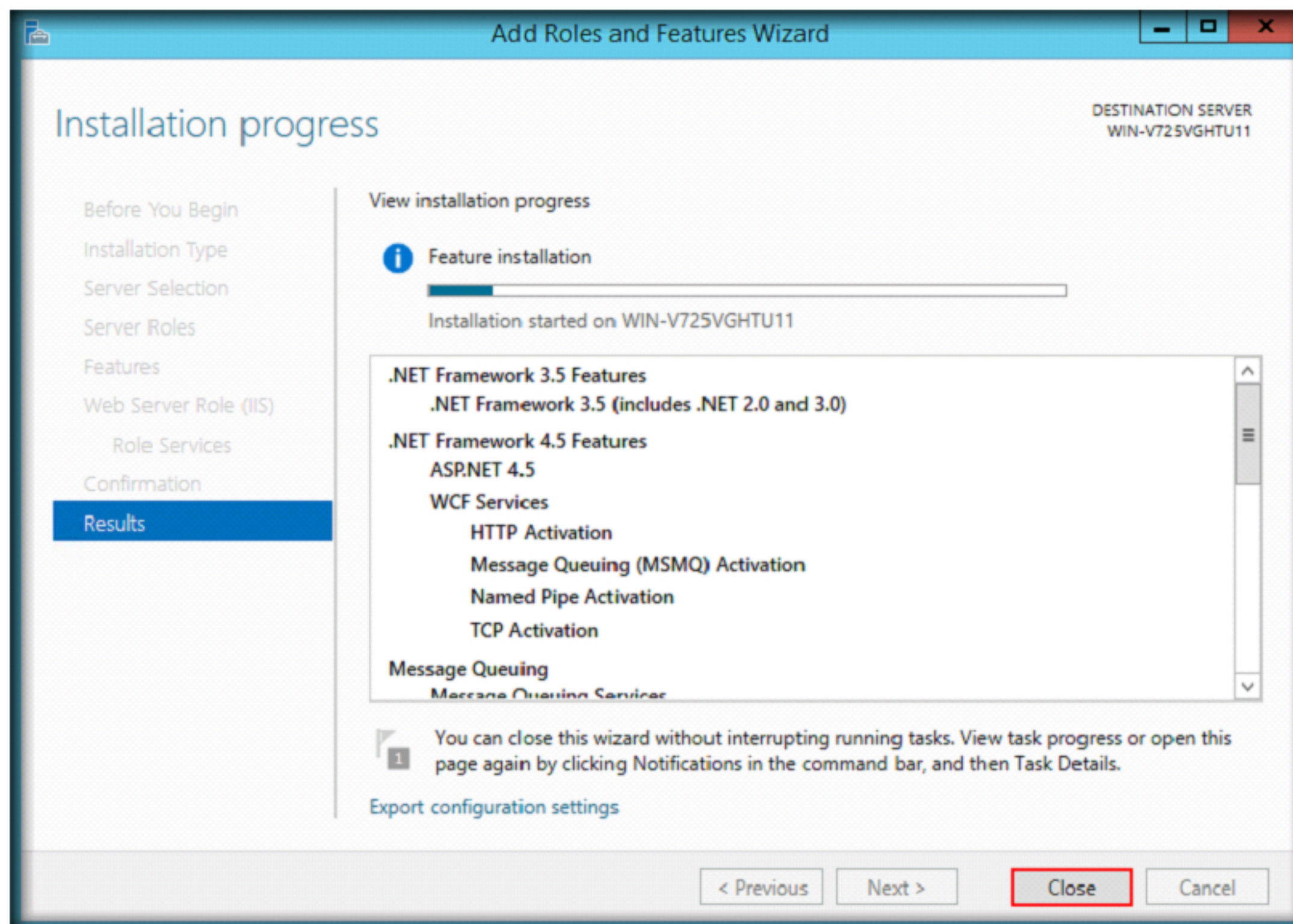
10. **Role Services** section appears in the wizard, click **Next**



11. **Confirmation** section appears in the wizard, click **Install**



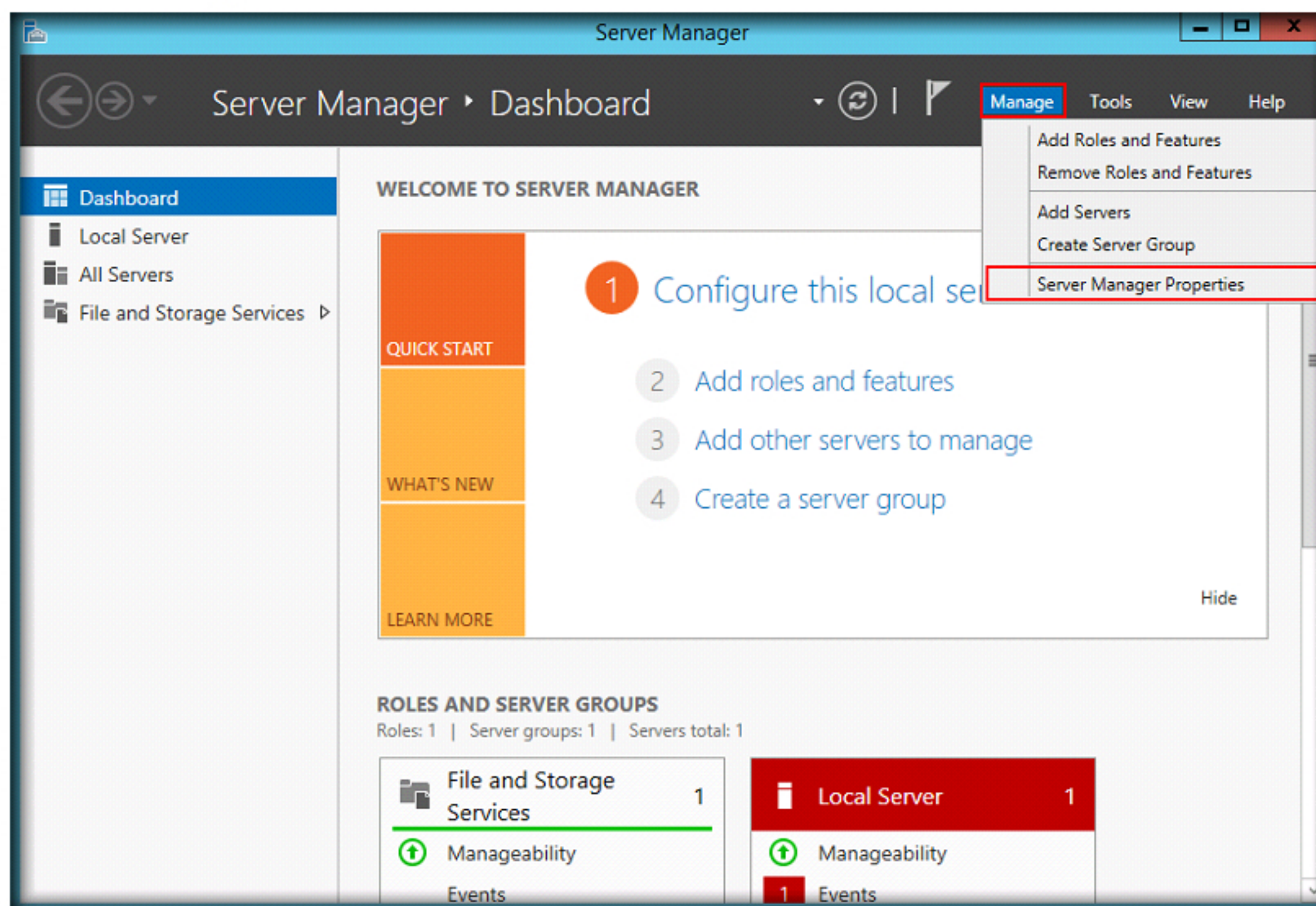
12. Add Roles and Features Wizard for **Installation progress** will show the installation progress of the features. It will take a while to **complete** the installation of selected roles



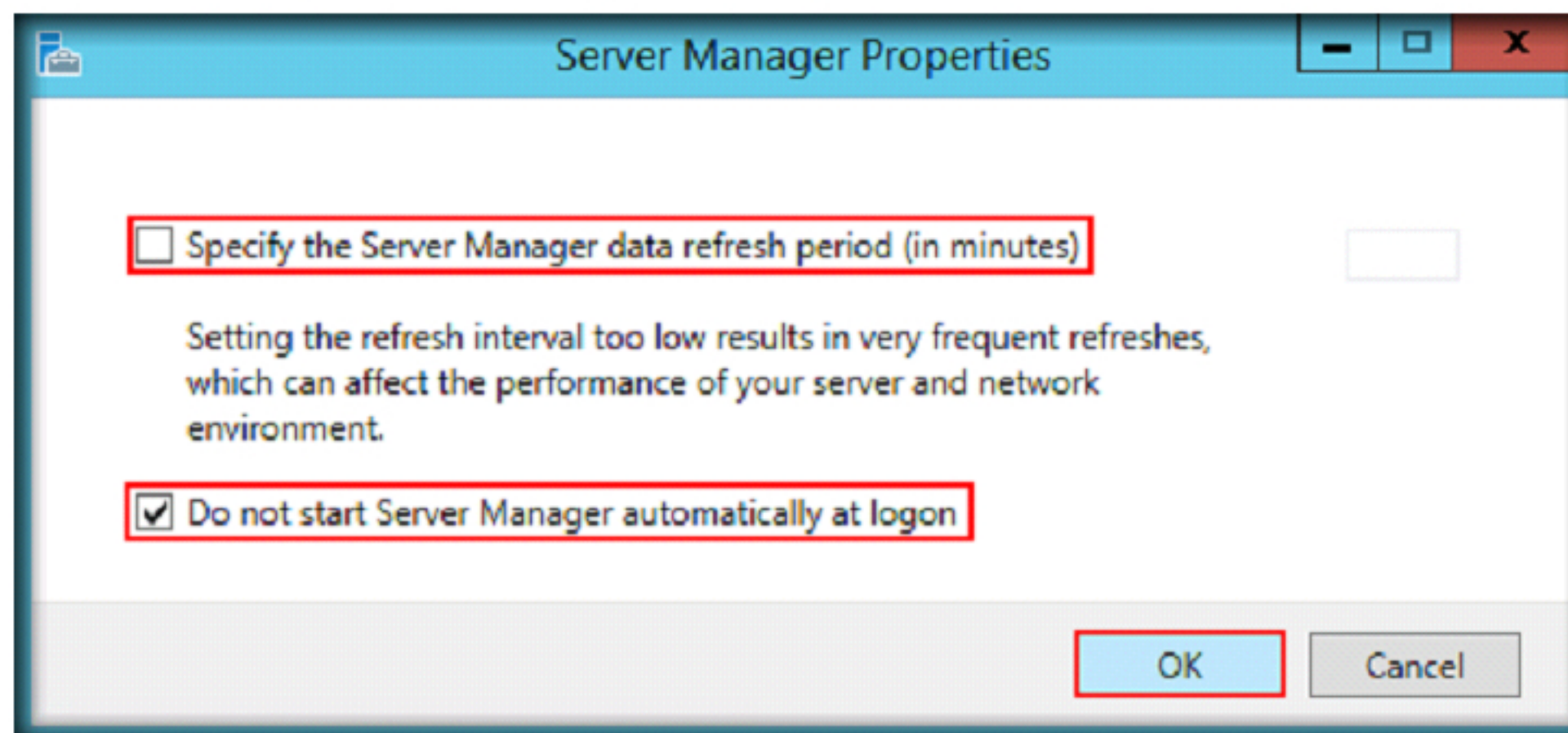
13. After the completion of installation, click **Close** button

CT#10: Disable Server Manager in Windows Server 2012 Virtual Machine

1. Logon to Windows Server 2012 virtual machine
2. Click **Server Manager** icon located in the taskbar
3. **Server Manager** window appears, click **Manage** from the menu and select **Server Manager Properties**



4. **Server Manager Properties** window appears, uncheck **Specify the Server Manager data refresh period (in minutes)** option, check **Do not start Server Manager automatically at logon** option and click **OK**



5. Close the **Server Manager** window

CT#11: Install a Web Browser in Windows Server 2012 Virtual Machine

1. Download a web browser such as Chrome, Firefox or Safari from its respective developer site
2. Double-click the installer and follow the wizard-driven installation steps to install the web browser

Note: You may install a single web browser or multiple web browsers

CT#12: Install WinRAR in Windows Server 2012 Virtual Machine

1. Download the latest version of WinRAR from <http://www.rarlab.com/download.htm>
2. Double-click installer to begin the installation
3. Complete the installation by choosing **defaults** throughout the installation process
4. After the installation is completed, a window opens automatically showing the location of the installed WinRAR files
5. Close the **window**

CT#13: Download CHFI Tools in Windows Server 2012 Virtual Machine

1. Logon to Windows Server 2012 virtual machine
2. Create a folder in the drive **C:** named **CHFI-Tools**
3. Login to your Aspen account → click **Academia** icon under the **Learning Resources** section → enter the **Access Code** (check with Training center or EC-Council support) (if not already used) → click **Submit** → select **CHFIv9 Courseware** from the **Select Courseware** drop-down list in the **Download PDF Courseware** section → scroll down to the **Tools** section
4. Click the module names and download all the **Essential Tools** files to the **C:\CHFI-Tools** folder
5. Right-click the .zip files in the **C:\CHFI-Tools** folder and select **Extract Here** option
6. Download **Kali Linux 2016 Rolling Release (x64)** from the URL <http://cdimage.kali.org/kali-2016.1/kali-linux-2016.1-amd64.iso>) and save the file to **C:\CHFI-Tools\Lab Prerequisites\Kali Linux**
7. Download **Ubuntu Linux 16.04 LTS (x64)** from the URL <http://ubuntu.excellmedia.net/releases/16.04.1/ubuntu-16.04.1-desktop-amd64.iso> and save the file to **C:\CHFI-Tools\Lab Prerequisites\Ubuntu**

Note: If you want to download and experiment with additional tools,

1. Create a folder named **Additional Tools** in the **C:\CHFI-Tools**

2. Expand the **Additional Tools** node in the **Tools** section
3. Click the module names and download the required Additional Tools files to the **C:\CHFI-Tools\Additional Tools** folder
4. Right-click the .zip files in the **C:\CHFI-Tools\Additional Tools** folder and select **Extract Here** option

CT#14: Install Adobe Reader v11.0.10

1. Navigate to **C:\CHFI-Tools\CHFIv9 Lab Prerequisites\Adobe Reader**, or download from **Aspen Portal**
2. Double-click **AdbeRdr11010_en_US.exe** to begin the installation
3. Follow the wizard-driven installation steps and complete the installation by choosing **defaults** throughout the installation process
4. Alternatively, you can install the latest Adobe Reader from the **Adobe website**

CT#15: Install WinPcap 4.1.3 in Windows Server 2012 Virtual Machine

1. Navigate to **C:\CHFI-Tools\CHFIv9 Lab Prerequisites\WinPcap**, or download from **Aspen Portal**
2. Double-click **WinPcap_4_1_3.exe** to begin the installation
3. The **WinPcap setup** window appears
4. Follow the wizard-driven installation steps and complete the installation by choosing **defaults** throughout the installation process

CT#16: Install Java SE Development Kit in Windows Server 2012 Virtual Machine

1. Navigate to **C:\CHFI-Tools\CHFIv9 Lab Prerequisites\Java SE Development Kit**, or download from **Aspen Portal**
2. Double-click **jdk-8u91-windows-x64.exe** to begin the installation
3. The **Java SE Development Kit setup** window appears
4. Follow the wizard-driven installation steps and complete the installation by choosing defaults throughout the installation process

CT#17: Install Java SE Run Time Environment in Windows Server 2012 Virtual Machine

1. Navigate to **C:\CHFI-Tools\CHFIv9 Lab Prerequisites\Java SE Runtime Environment**, or download from **Aspen Portal**

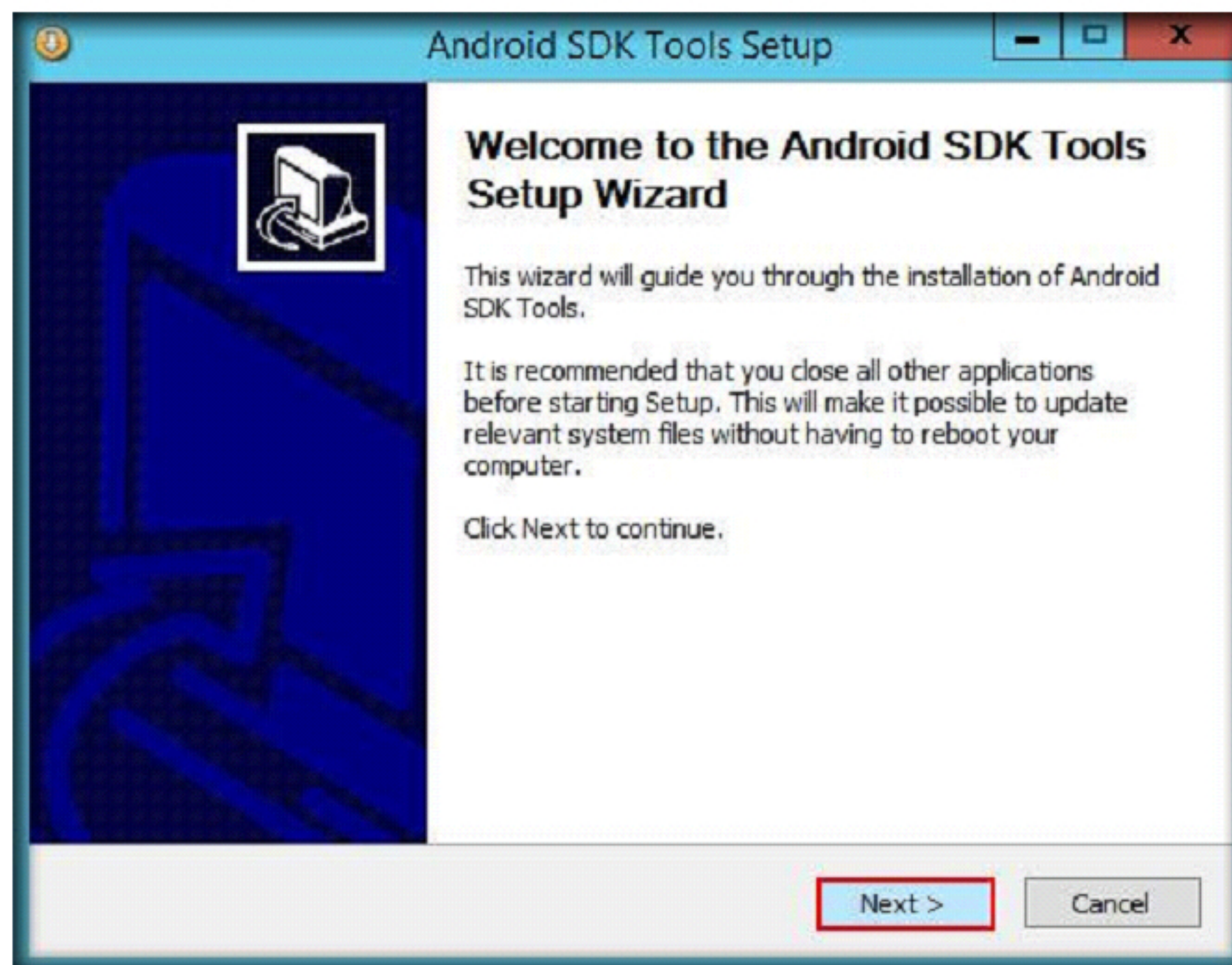
2. Double-click **jre-6u23-windows-i586.exe** to begin the installation
3. The **Java SE Run Time Environment setup** window appears
4. Follow the wizard-driven installation steps and complete the installation by choosing **defaults** throughout the installation process

CT#18: Install and configure Android SDK Tools on Windows Server 2012 Virtual Machine

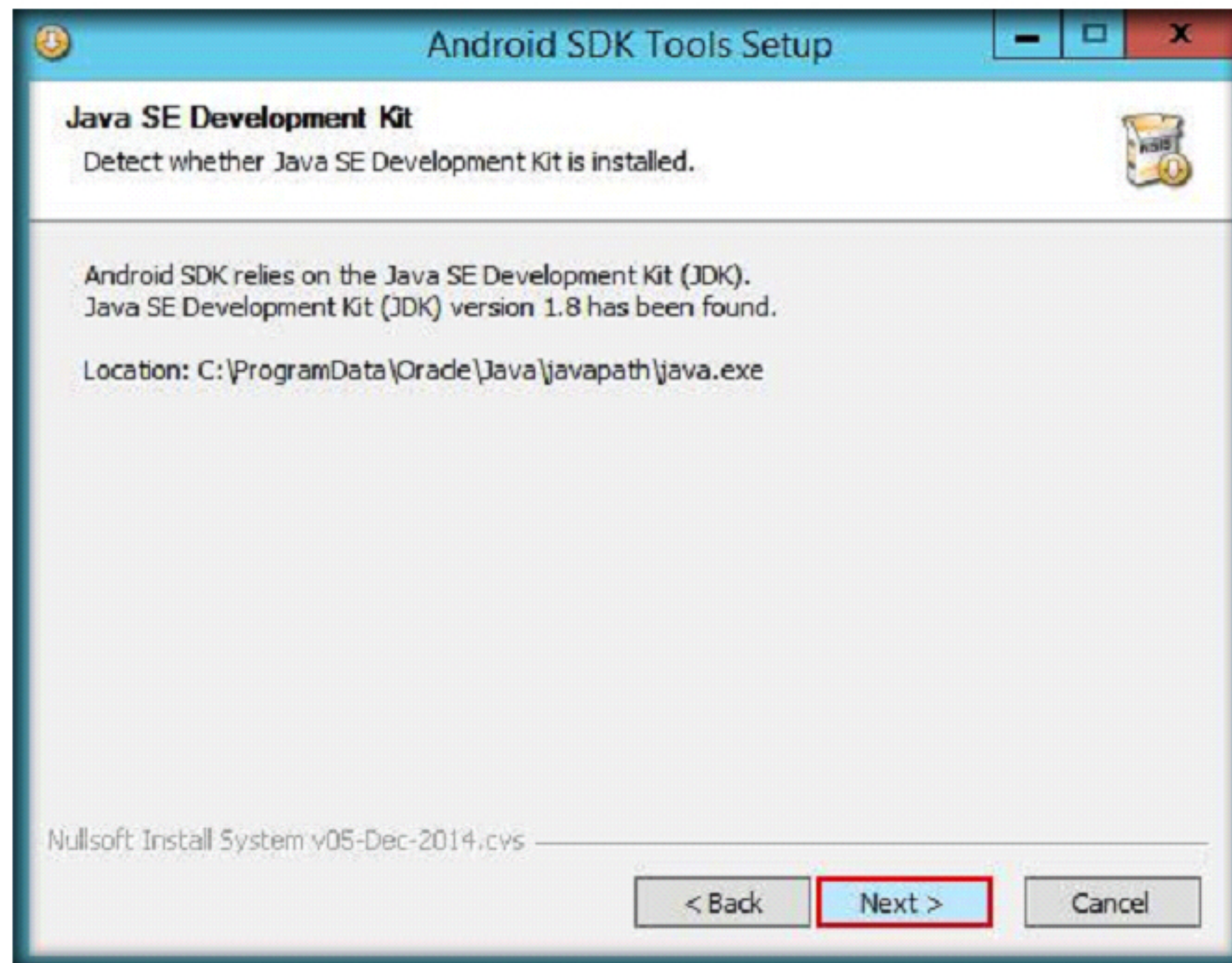
1. Navigate to **C:\CHFI-Tools\CHFIv9 Lab Prerequisites\Android SDK Tools** and double-click **SDK Installer.exe**

Note: If an **Open File - Security Warning** pop-up appears, click **Run**

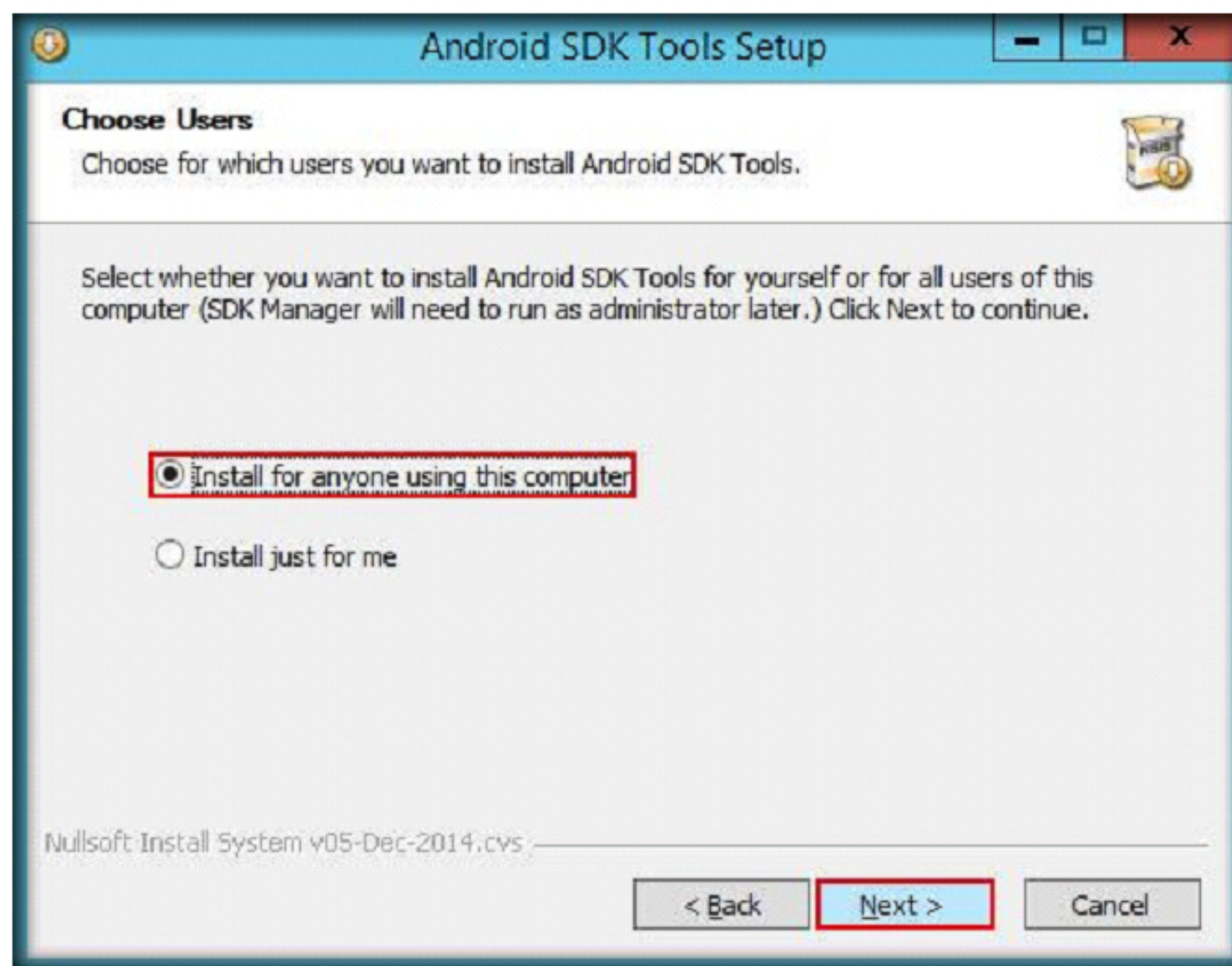
2. **Android SDK Tools Setup** wizard appears, click **Next**



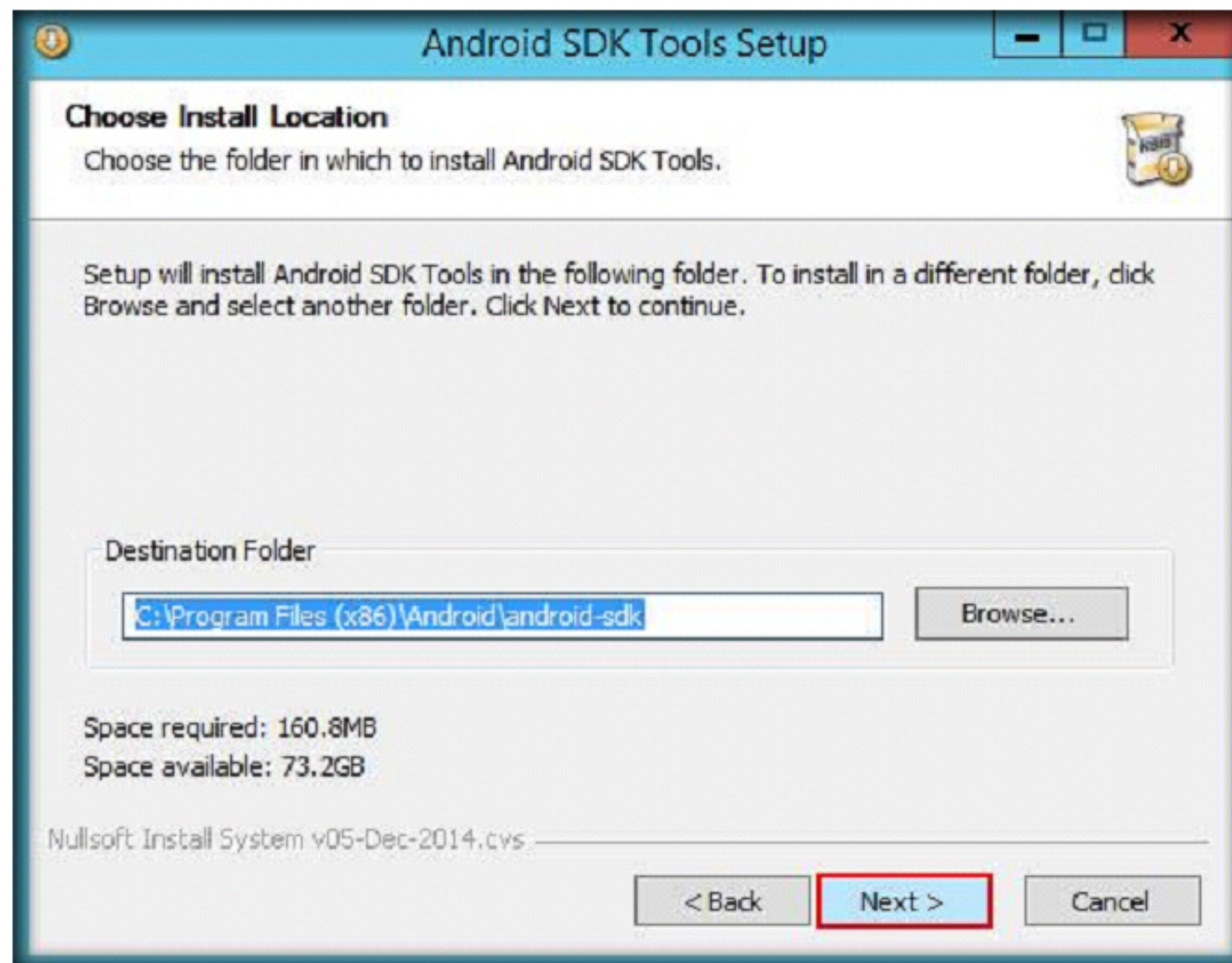
3. **Java SE Development Kit** section appears, click **Next**



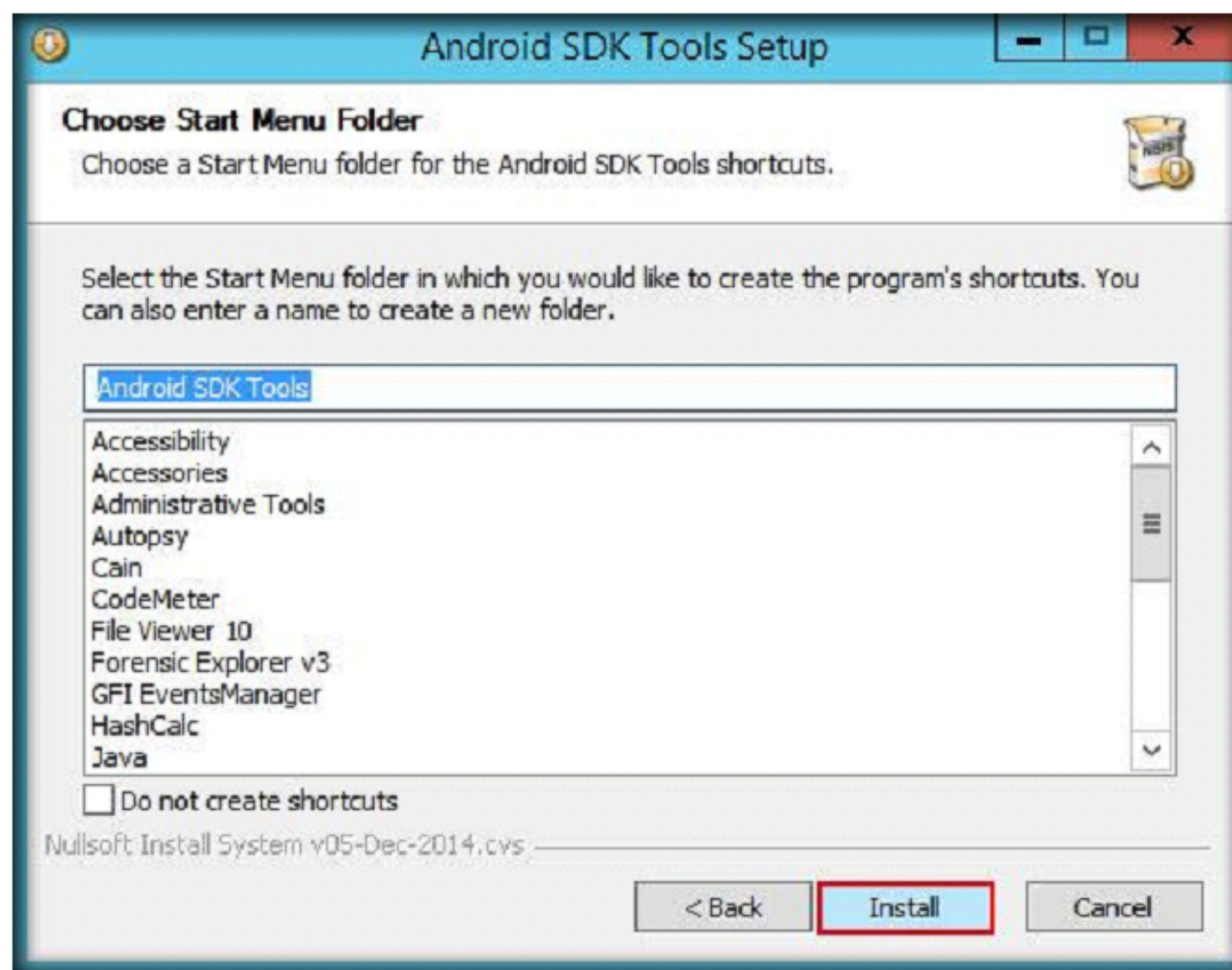
4. **Choose Users** section appears, select **Install for anyone using this computer** radio button and click **Next**



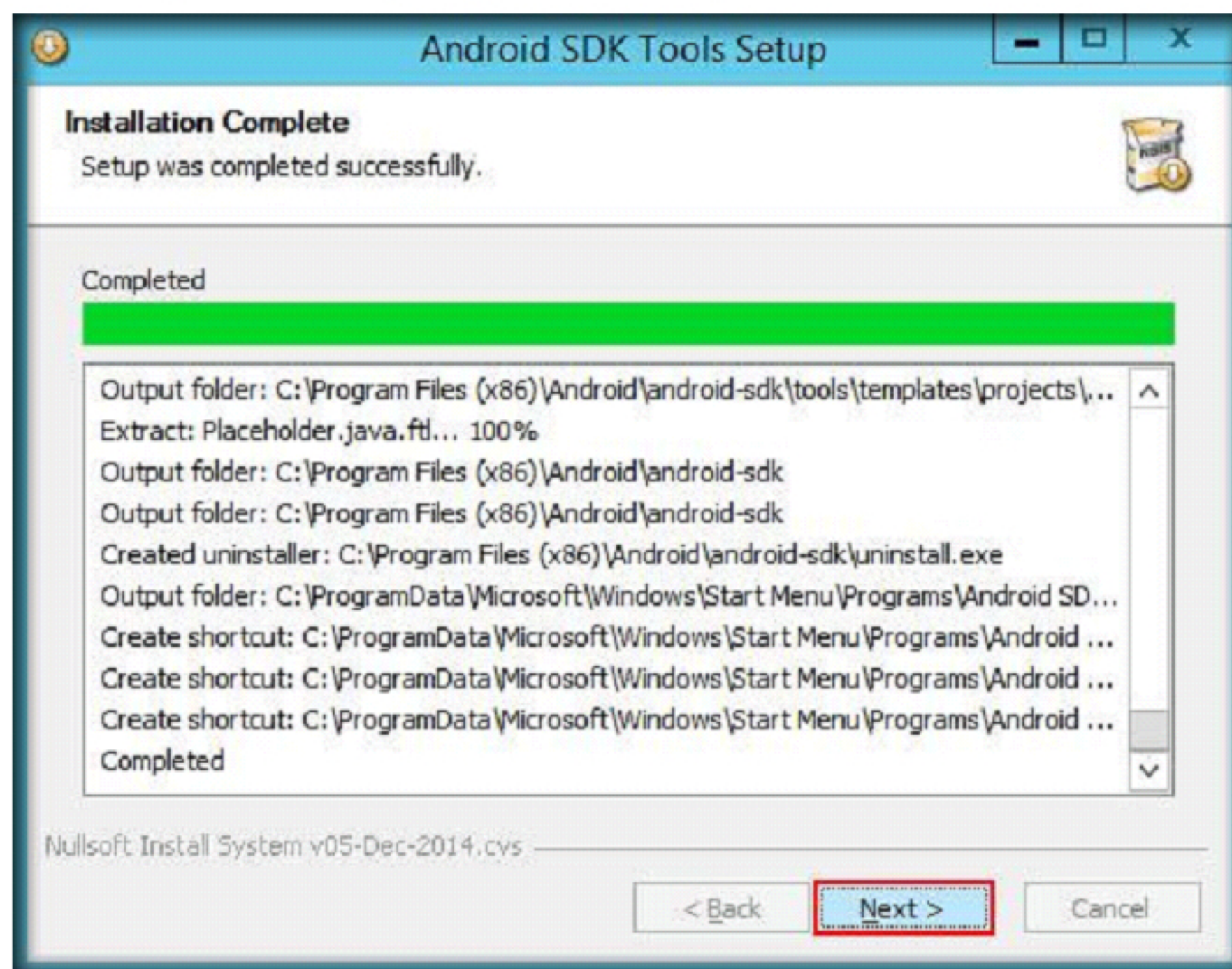
5. **Choose Install Location** section appears, select **Destination Folder** and click **Next**. In the lab setup, default destination folder location is chosen.



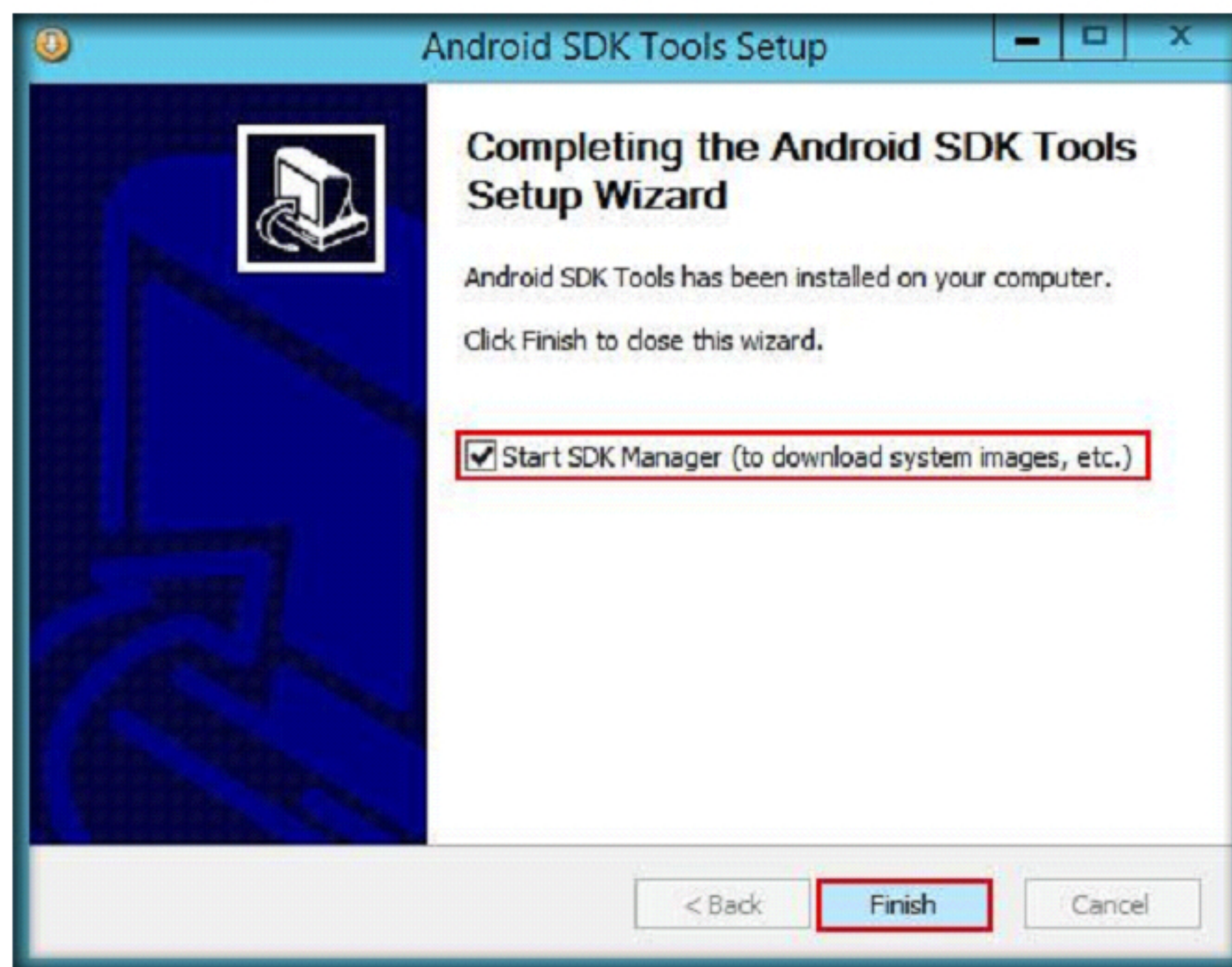
6. Choose Start Menu Folder section appears, click **Install**



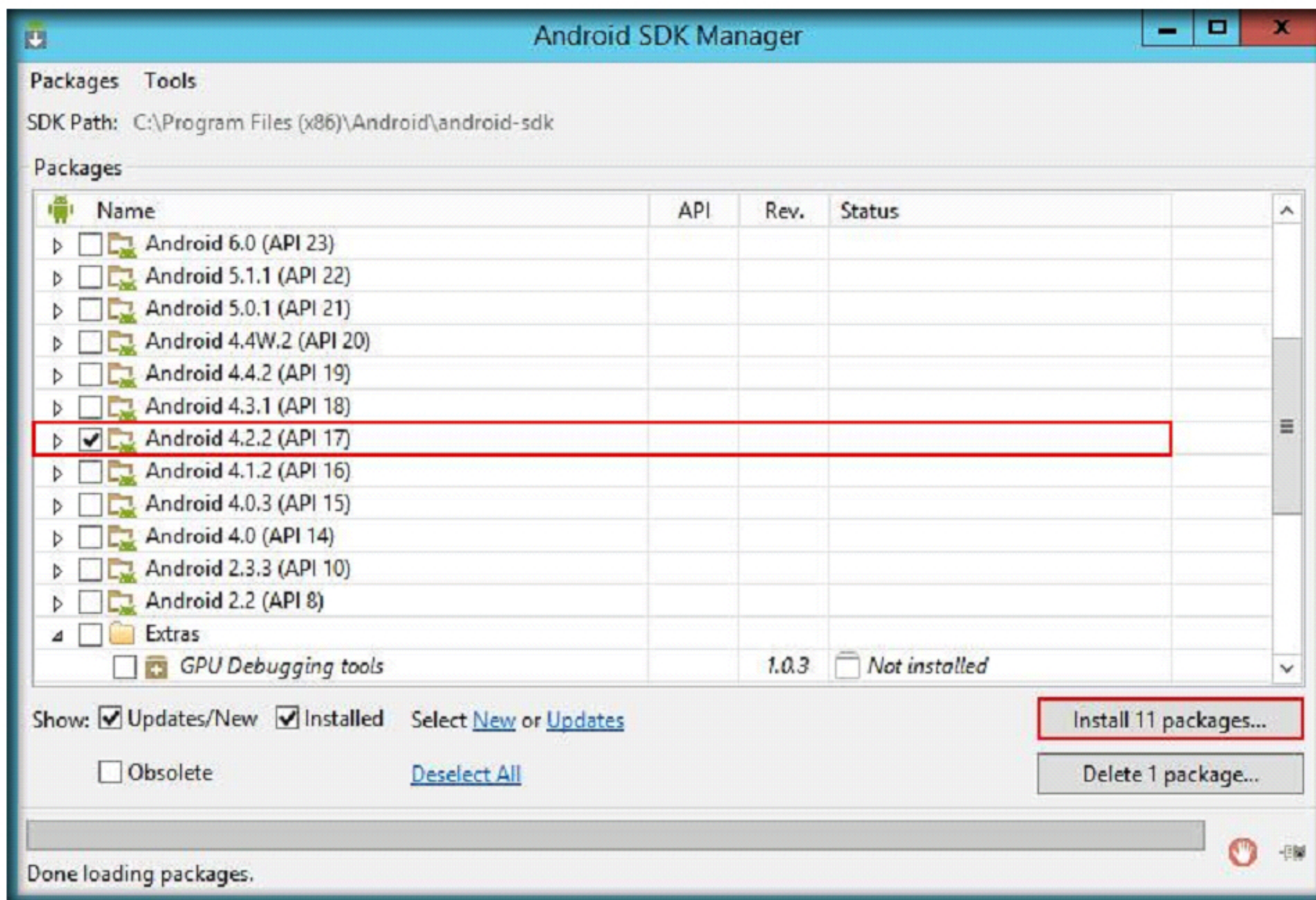
7. Wait for the installation to complete. On completing the installation, click **Next**



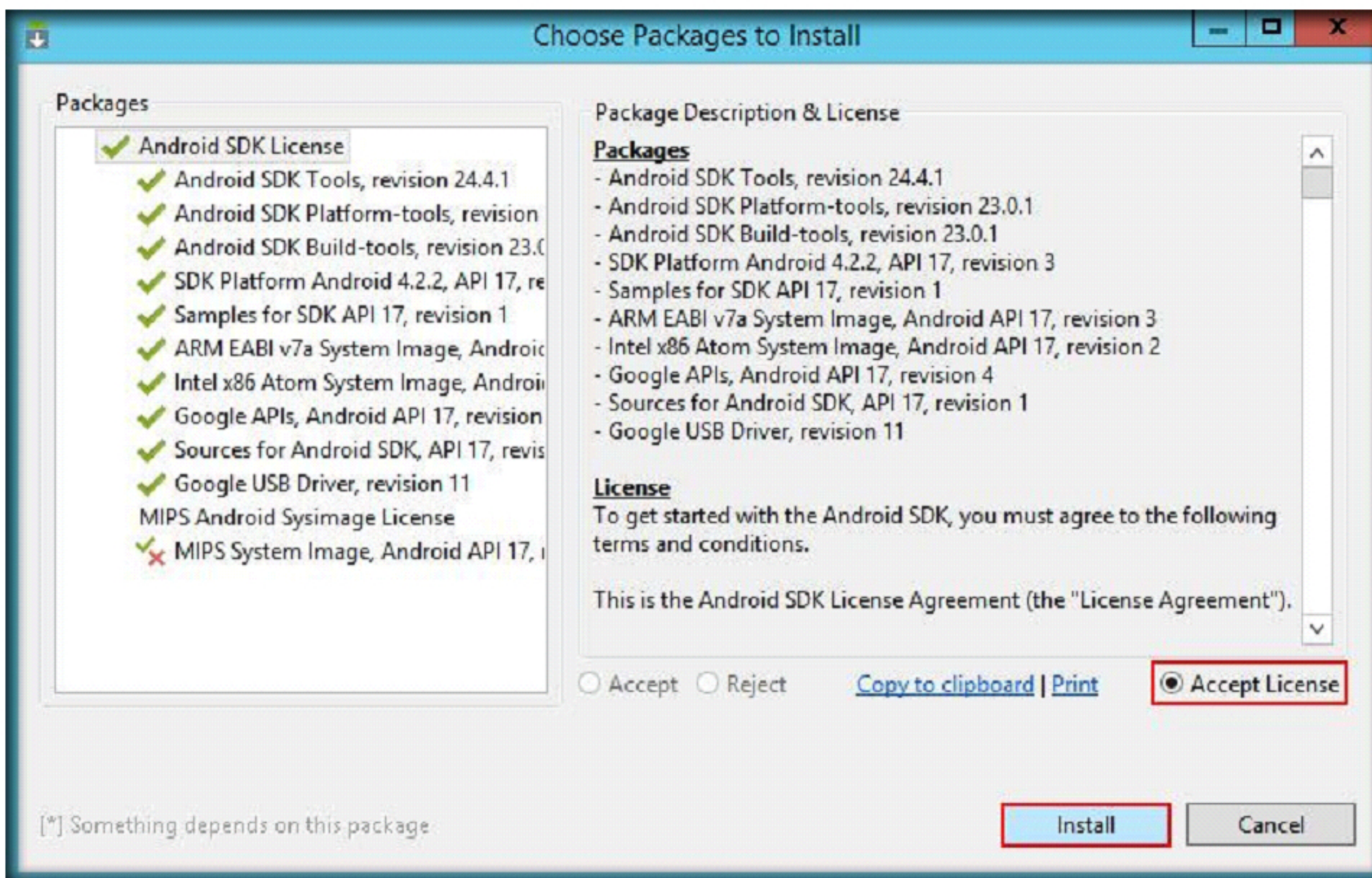
8. In the final step of installation wizard, check **Start SDK Manager (to download system images, etc.)** and click **Finish**



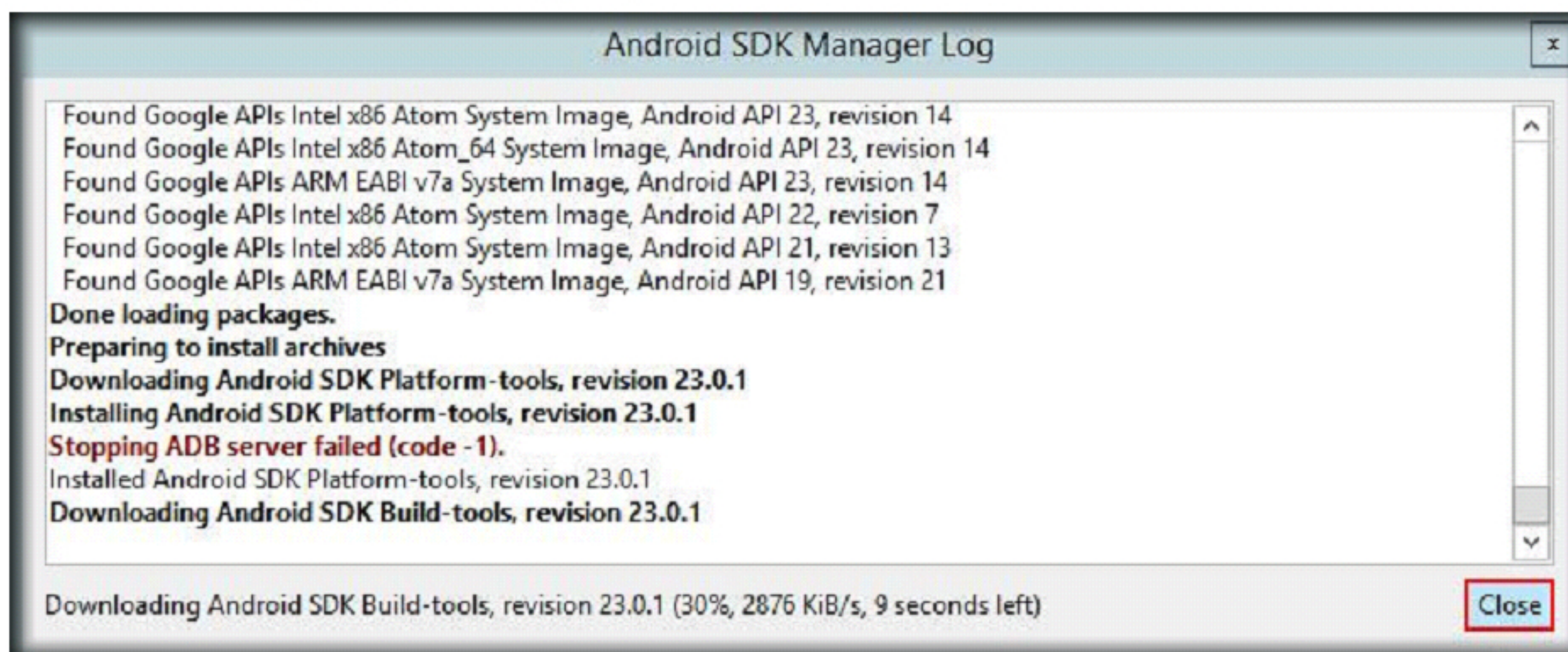
9. Android SDK Manager window appears, check **Android SDK Tools**, **Android SDK Platform-tools**, **Android SDK Build-tools** under **Tools** Package, **Android 4.2.2 (API 17)**, and uncheck the remaining Packages that were checked by default
10. Click **Install Packages...**



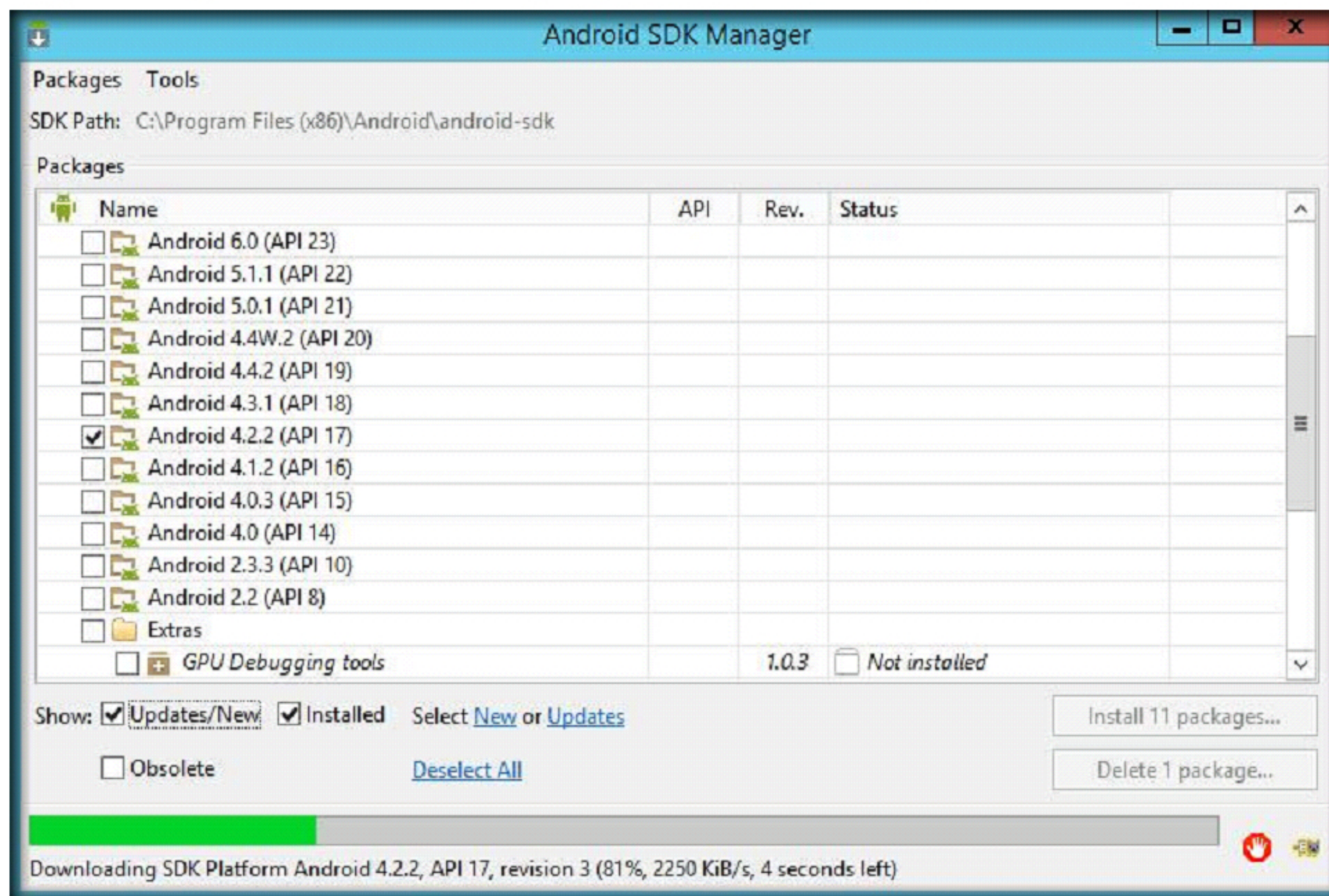
11. **Choose Packages to Install** window appears; select **Android SDK License** and click **Accept License** radio button.
12. Later, select **MIPS Android Sysimage License** and click **Accept License** radio button, and then, click **Install**



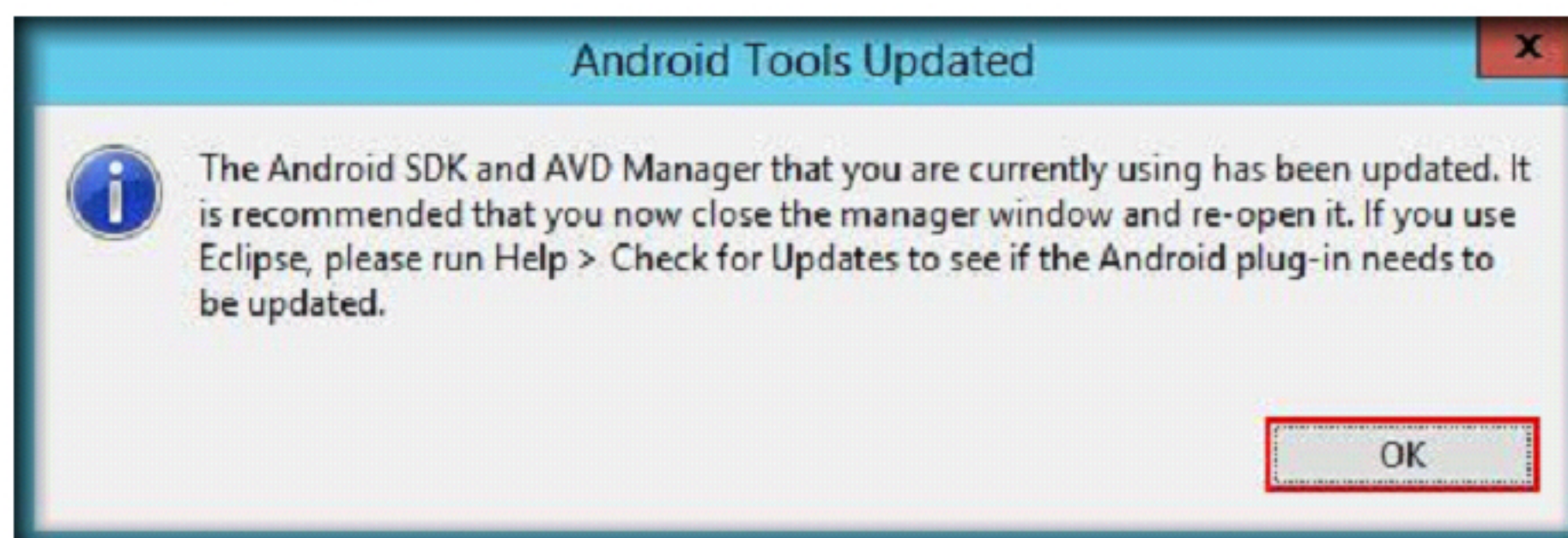
13. If an **Android SDK Manager Log** window appears, click **Close**



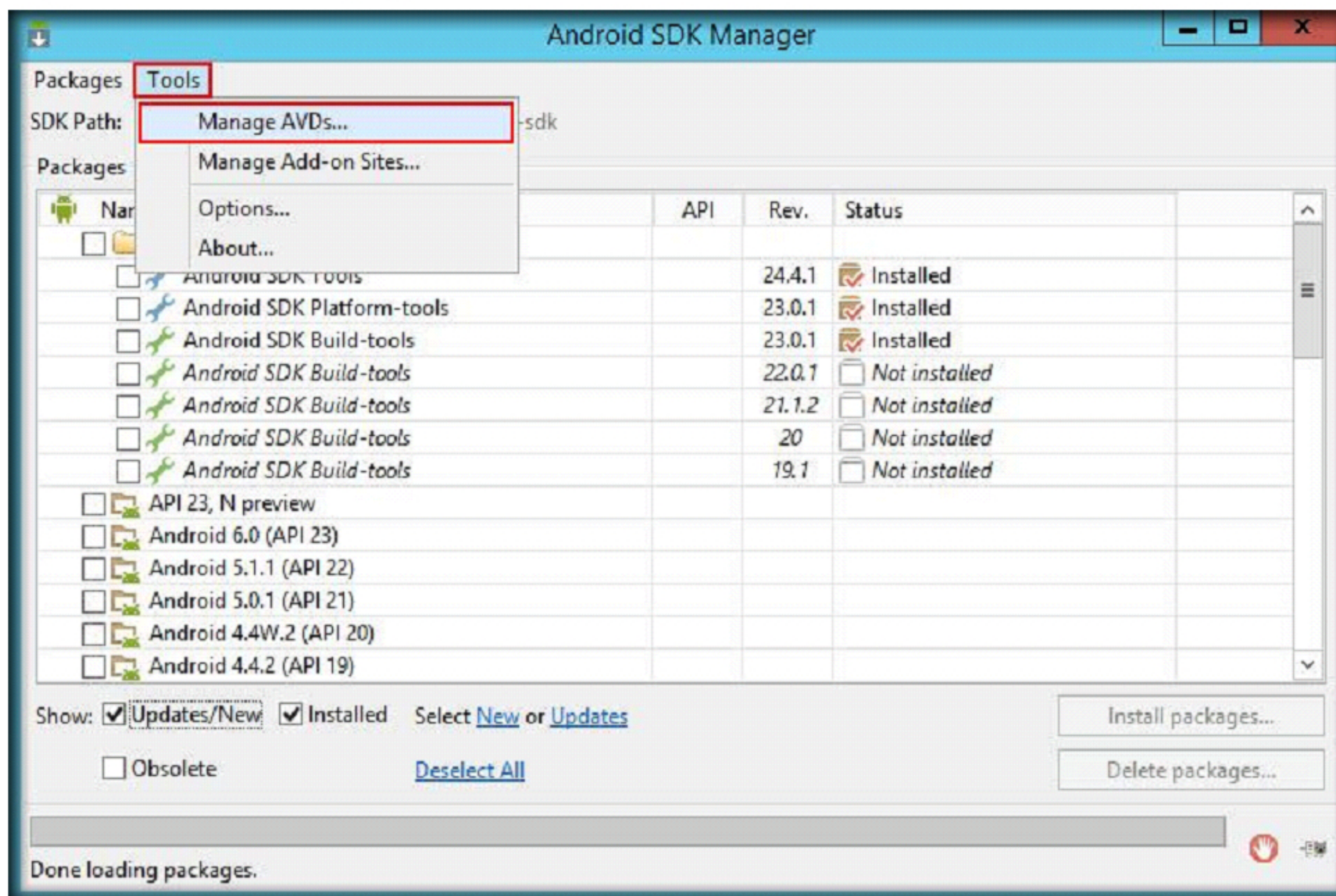
14. The application begins to download the required packages as shown in the following screenshot:



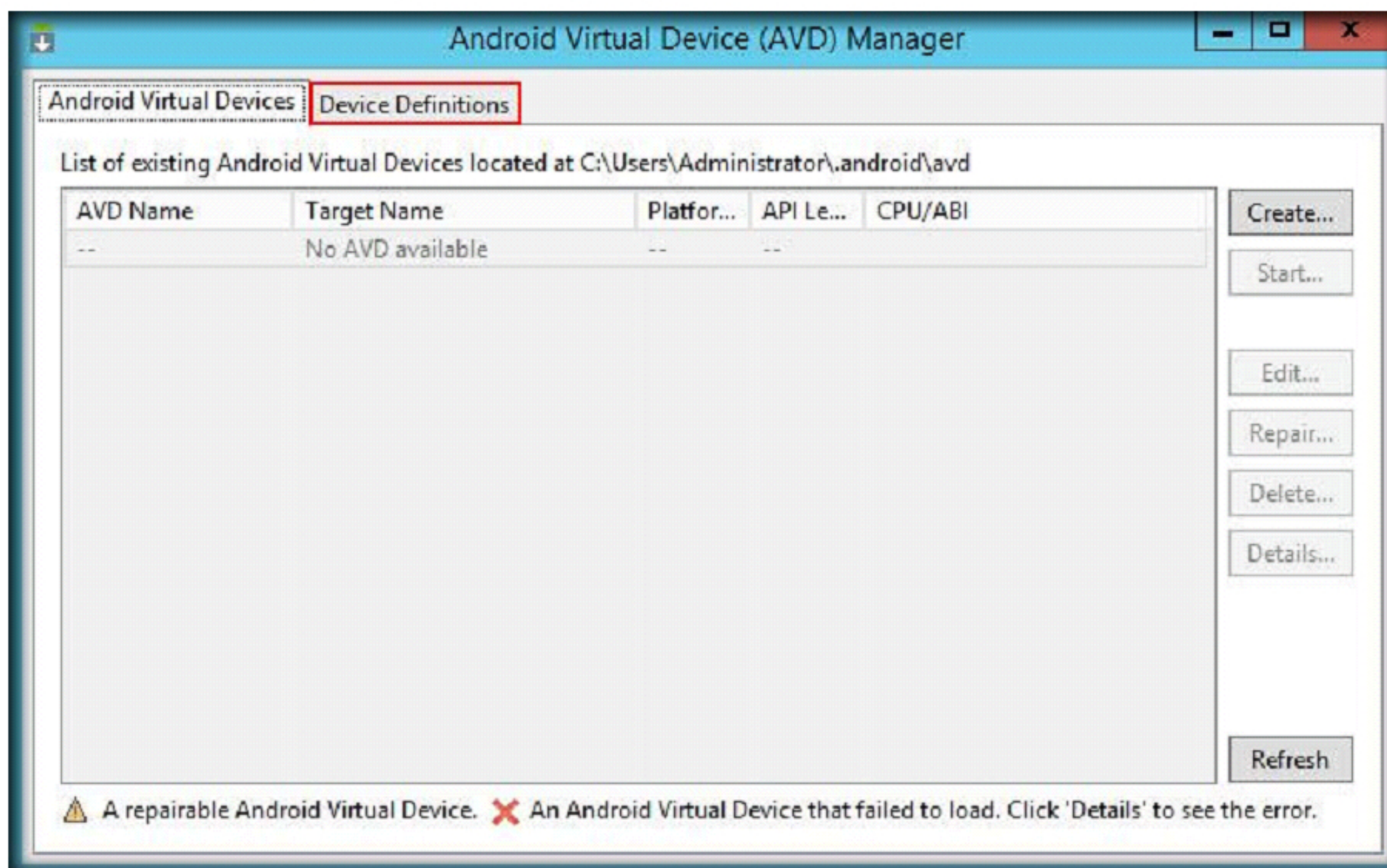
15. **Android Tools Updated** dialog-box appears, click **OK**



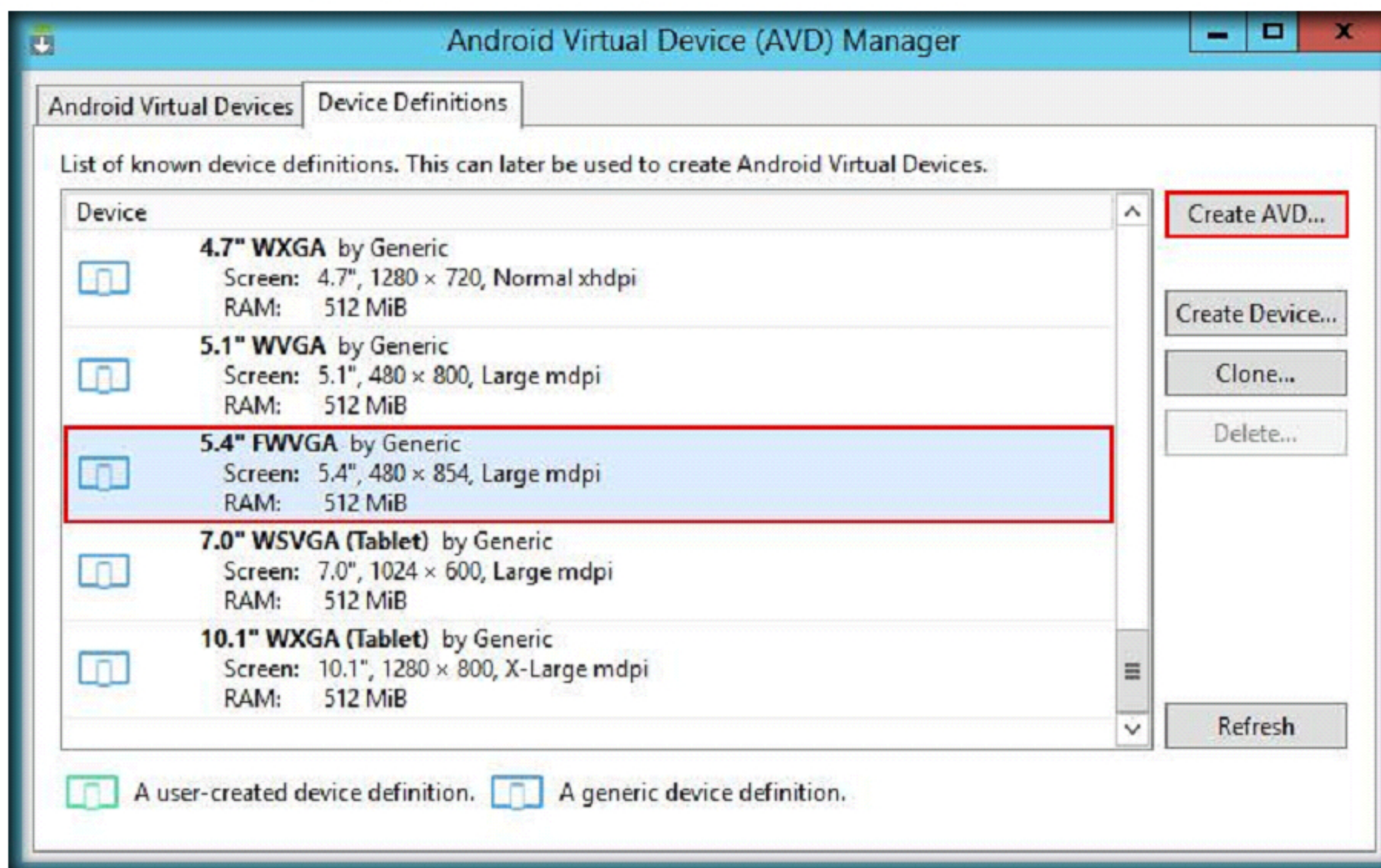
16. Now, in the **Android SDK Manager**, go to **Tools** and click **Manage AVDs...**



17. **Android Virtual Device (AVD) Manager** window appears, click **Device Definitions** tab

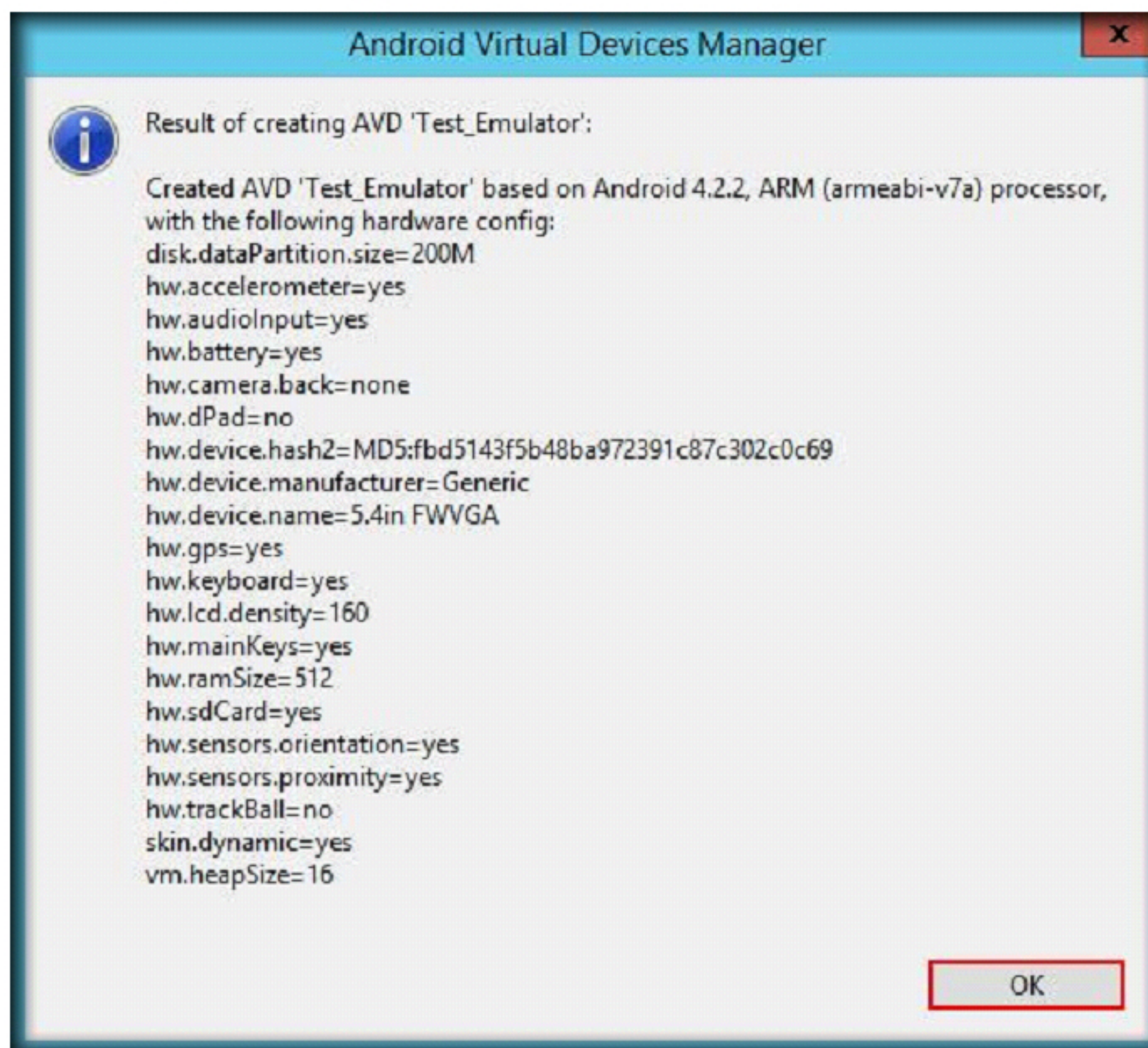


18. A list of **Device Definitions** appears, scroll down the list, select **5.4" FWVGA** and click **Create AVD...**

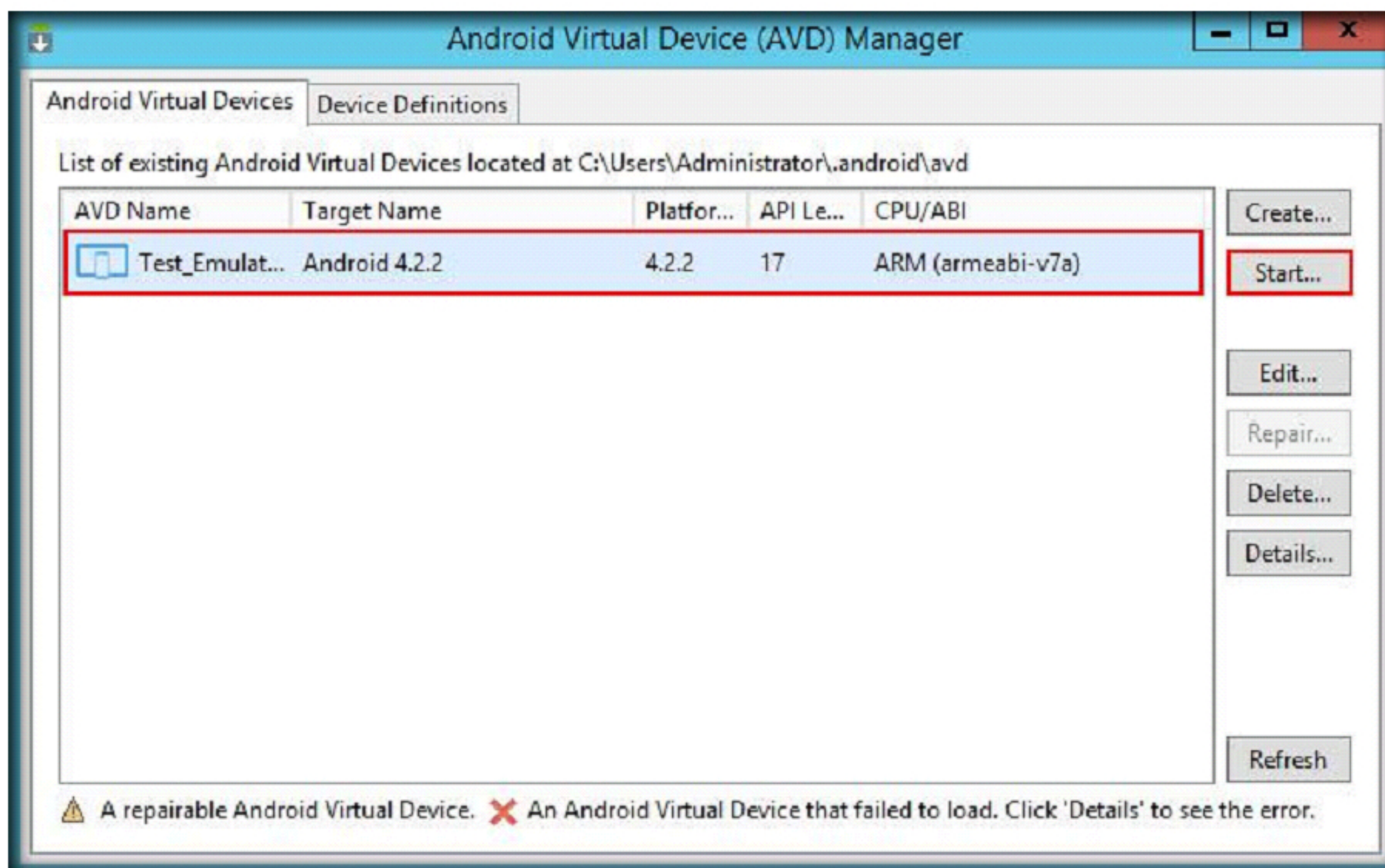


19. **Create new Android Virtual Device (AVD)** window appears, specify **AVD Name** as **Test_Emulator**, select **ARM (armeabi-v71)** from the **CPU/ABI** drop-down list, check **Hardware keyboard** present option for the **Keyboard** section, select **Skin with dynamic hardware controls** from **Skin** drop-down list, set the **Size of SD Card** as **100 MiB**, and click **OK**

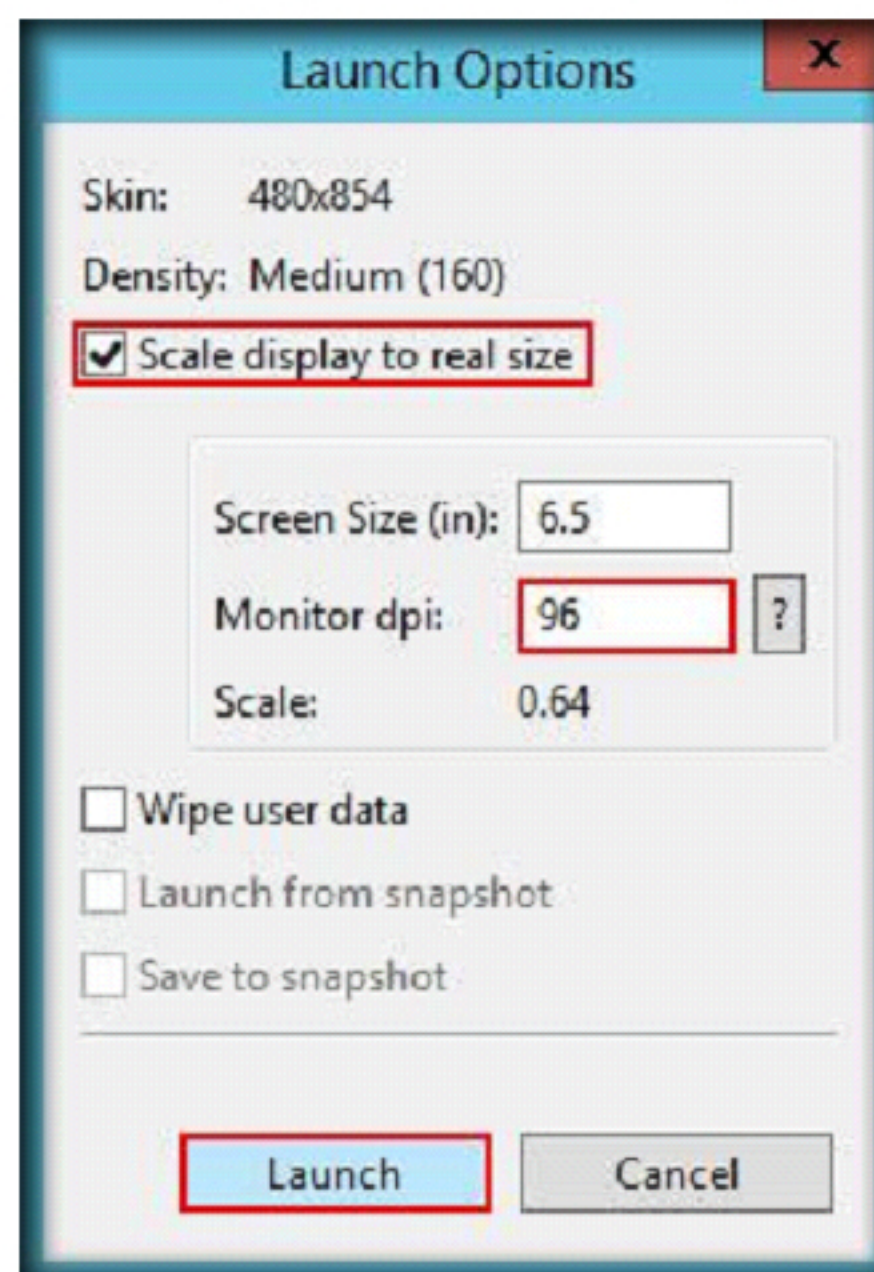
20. **Android Virtual Devices Manager** window appears, click **OK**



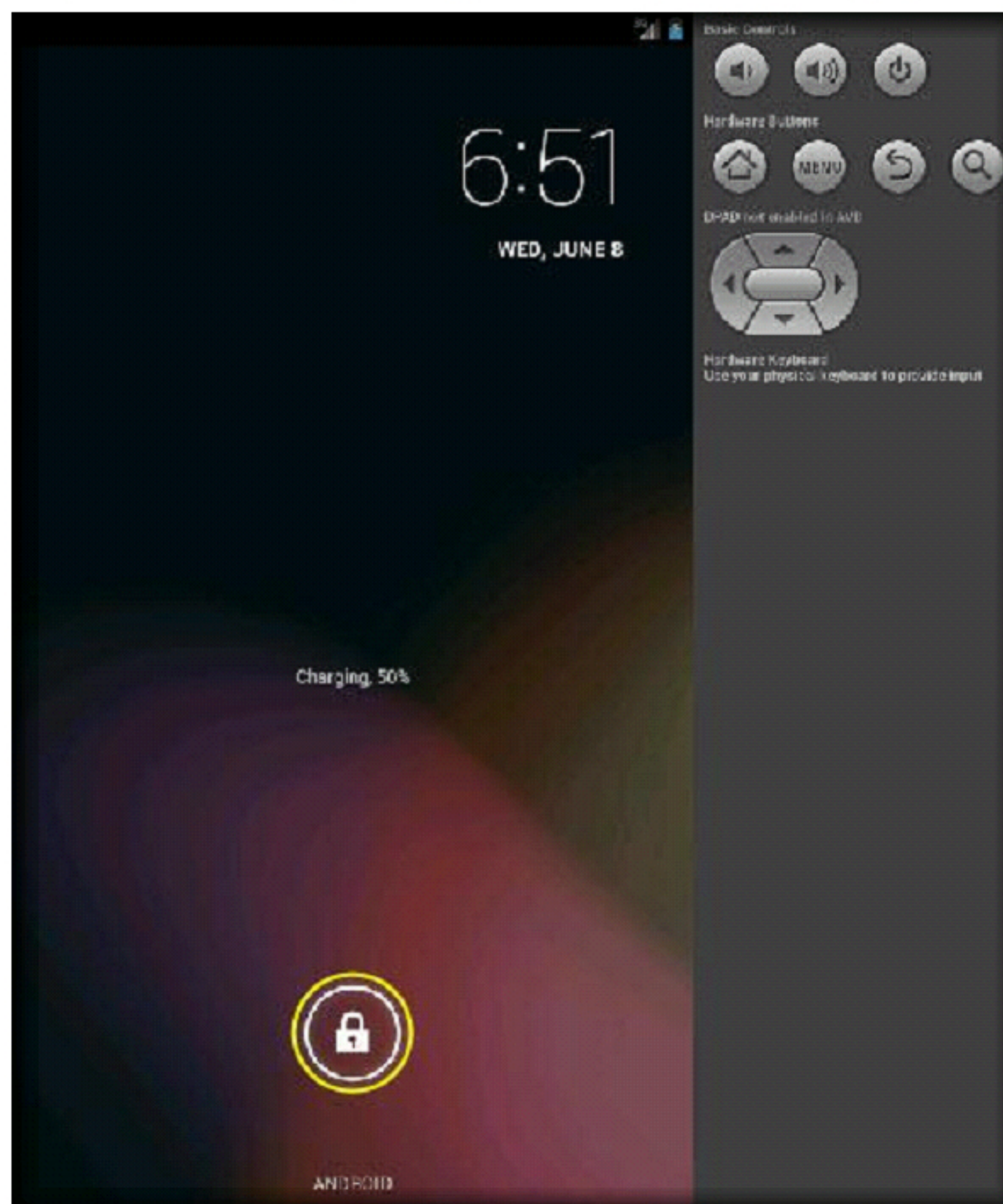
21. The newly created virtual device can be found under the **Android Virtual Devices** tab. Select the device and click **Start....**



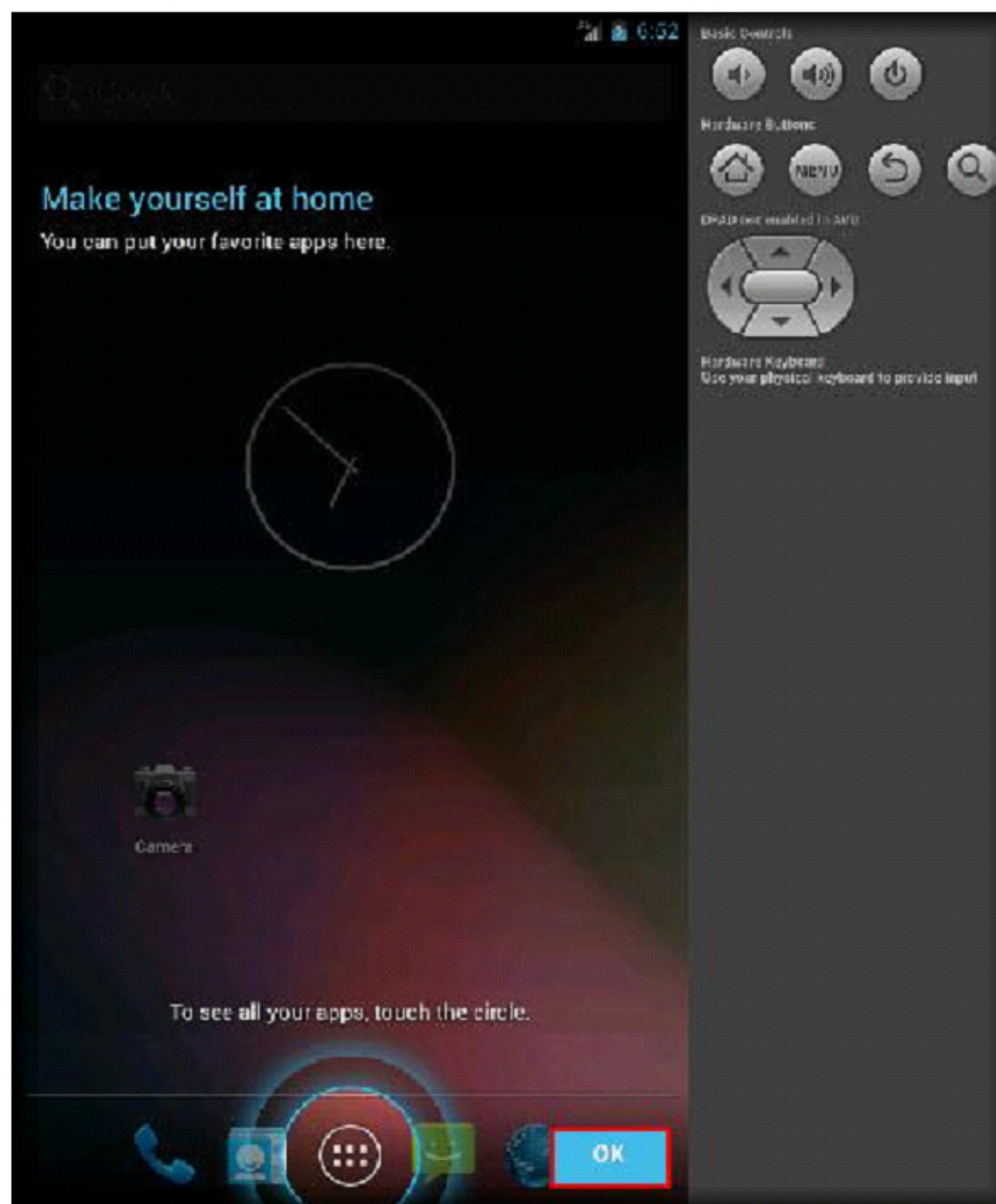
22. **Launch Options** window appears, check **Scale display to real size** option, specify the **Monitor dpi** value as **96** and click **Launch**



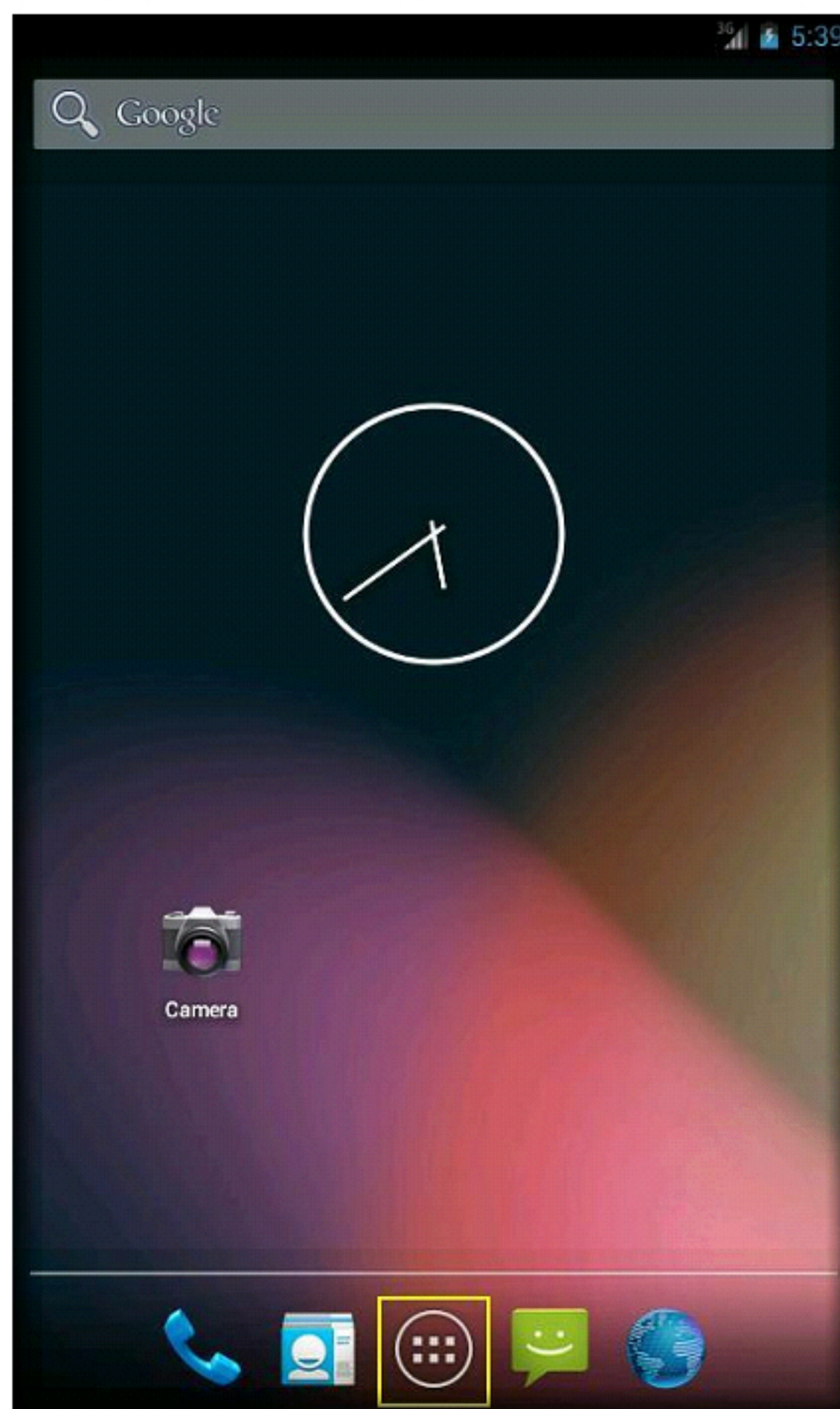
23. If the device is found locked, unlock the device by clicking on the lock symbol and dragging it towards right or left



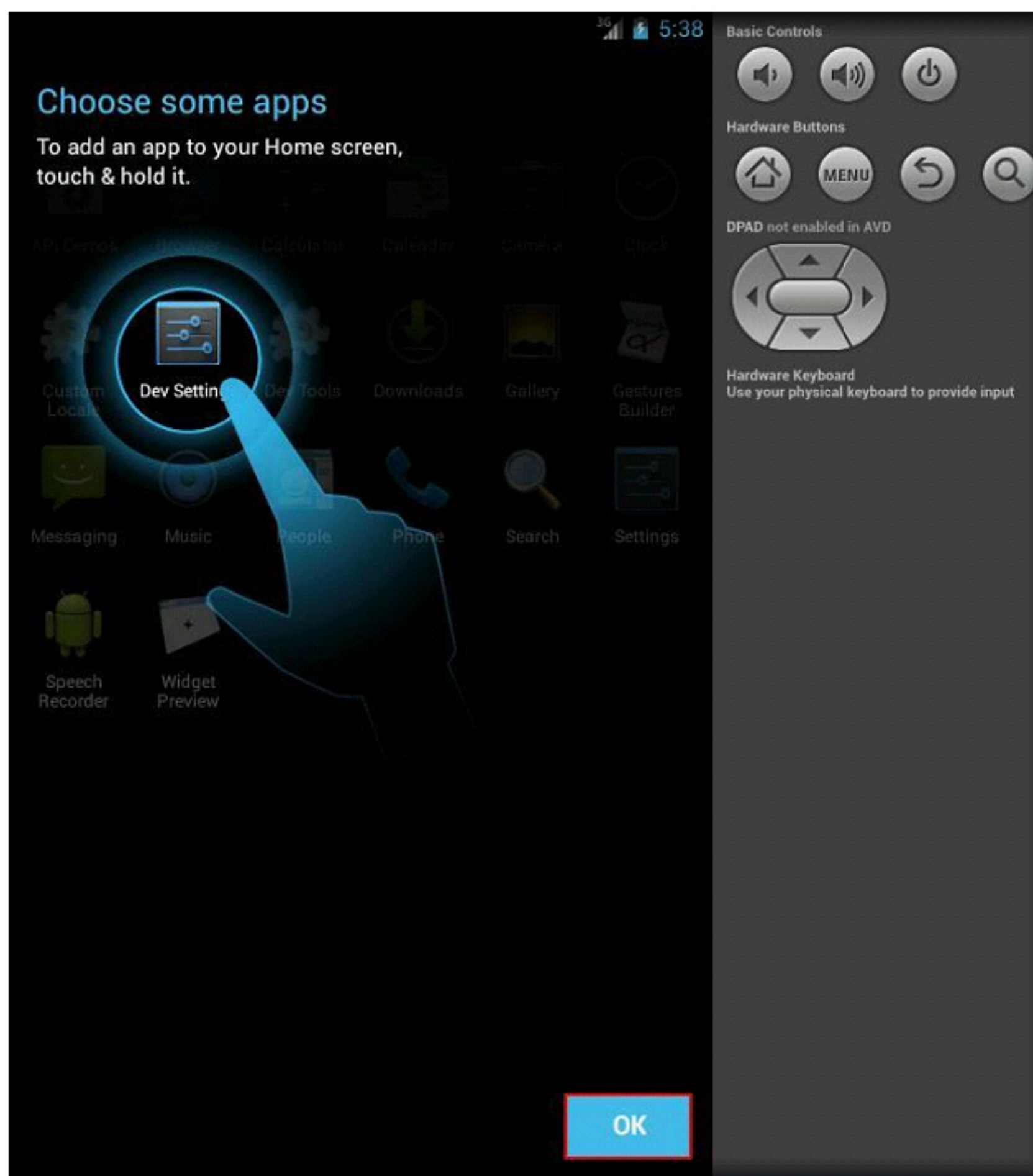
24. A **Make yourself at home** screen appears over the **Android** home screen, click **OK**




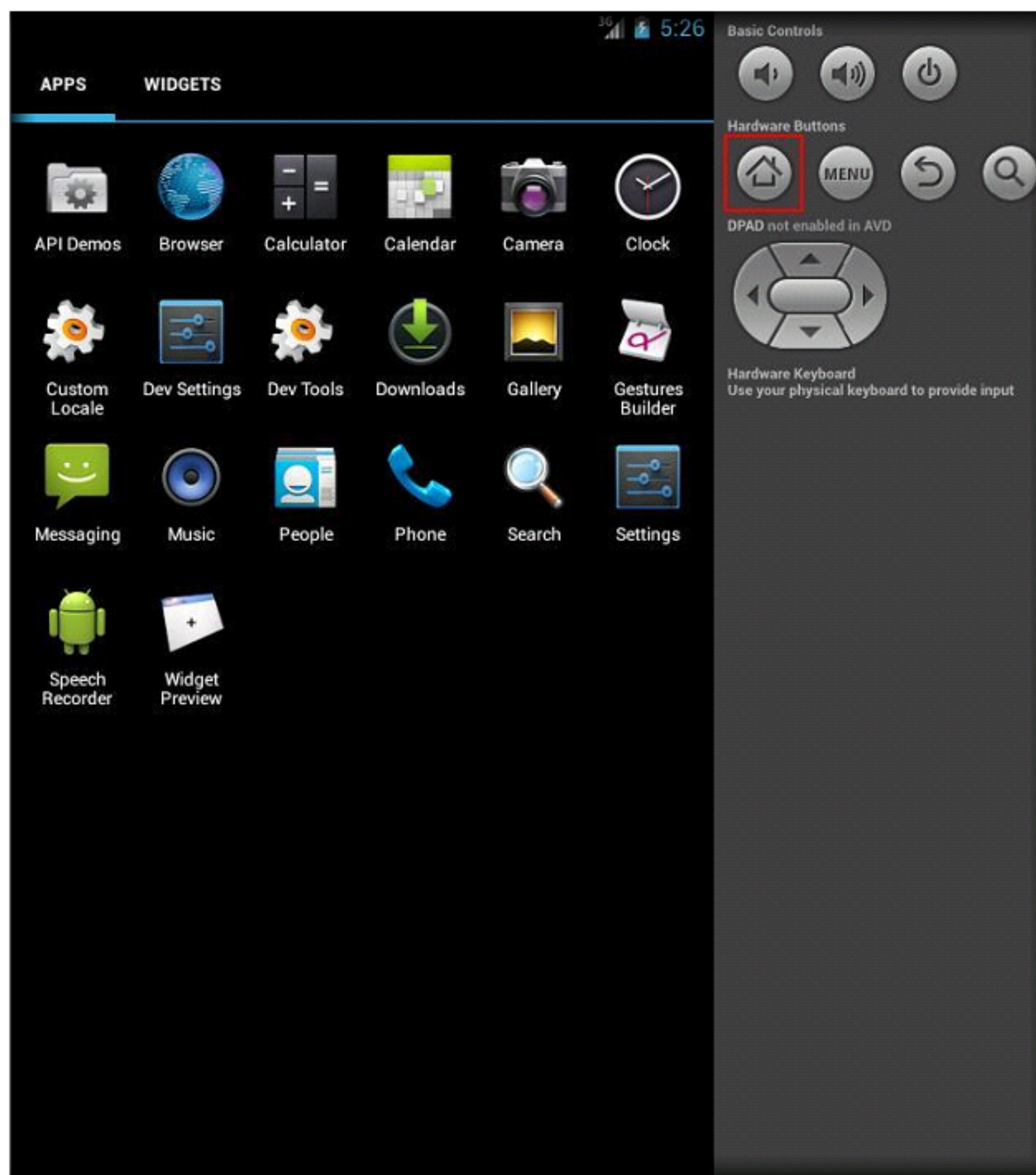
25. After clicking **OK**, Android home screen appears, tap the **App Drawer** icon on the home screen to launch the android menu



26. A **Choose some apps** screen appears over the **Android** menu screen, click **OK** to close it

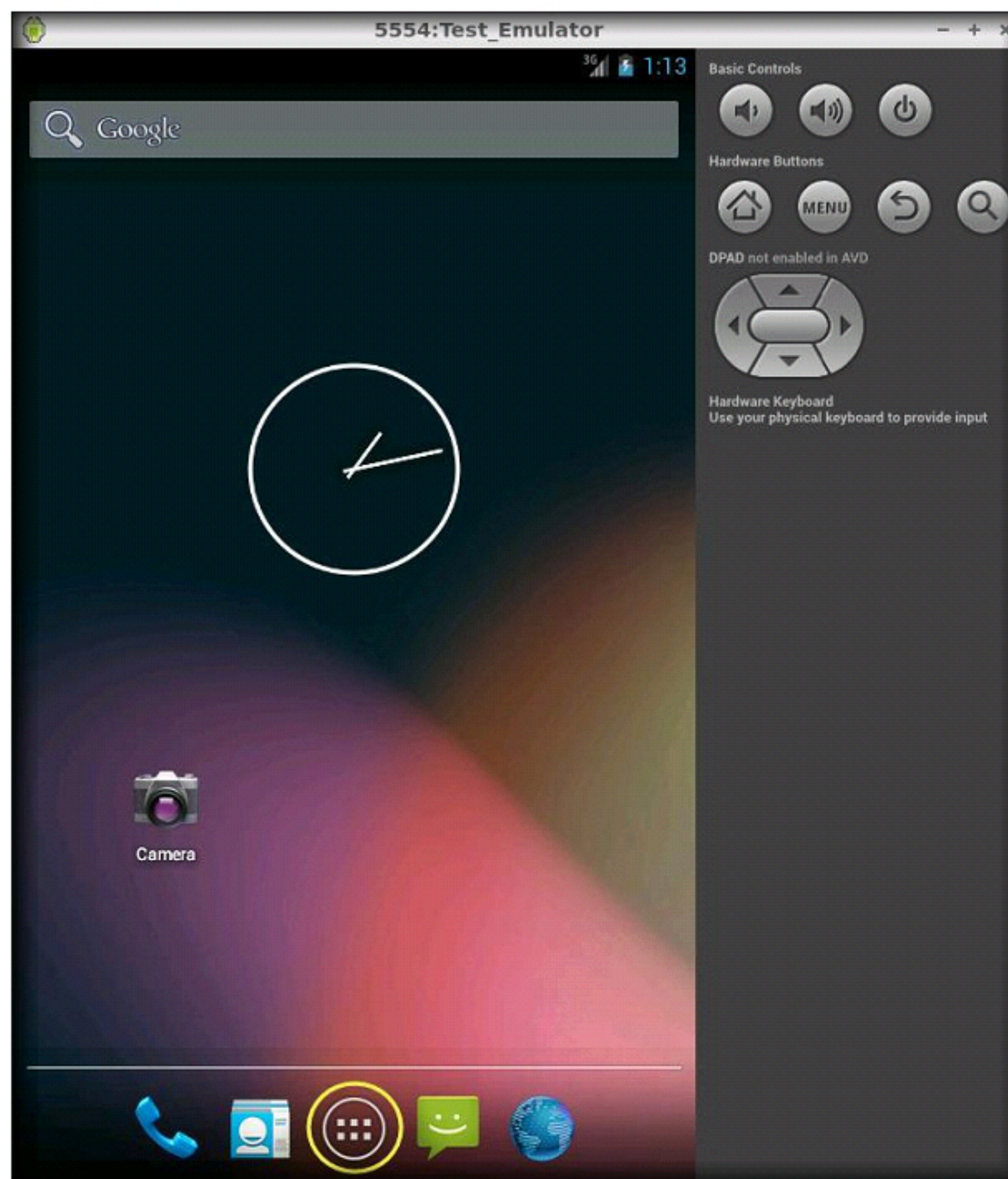


27. Android menu appears, now click **Home** button  on the android emulator, in order to go back to the home screen and then minimize the emulator

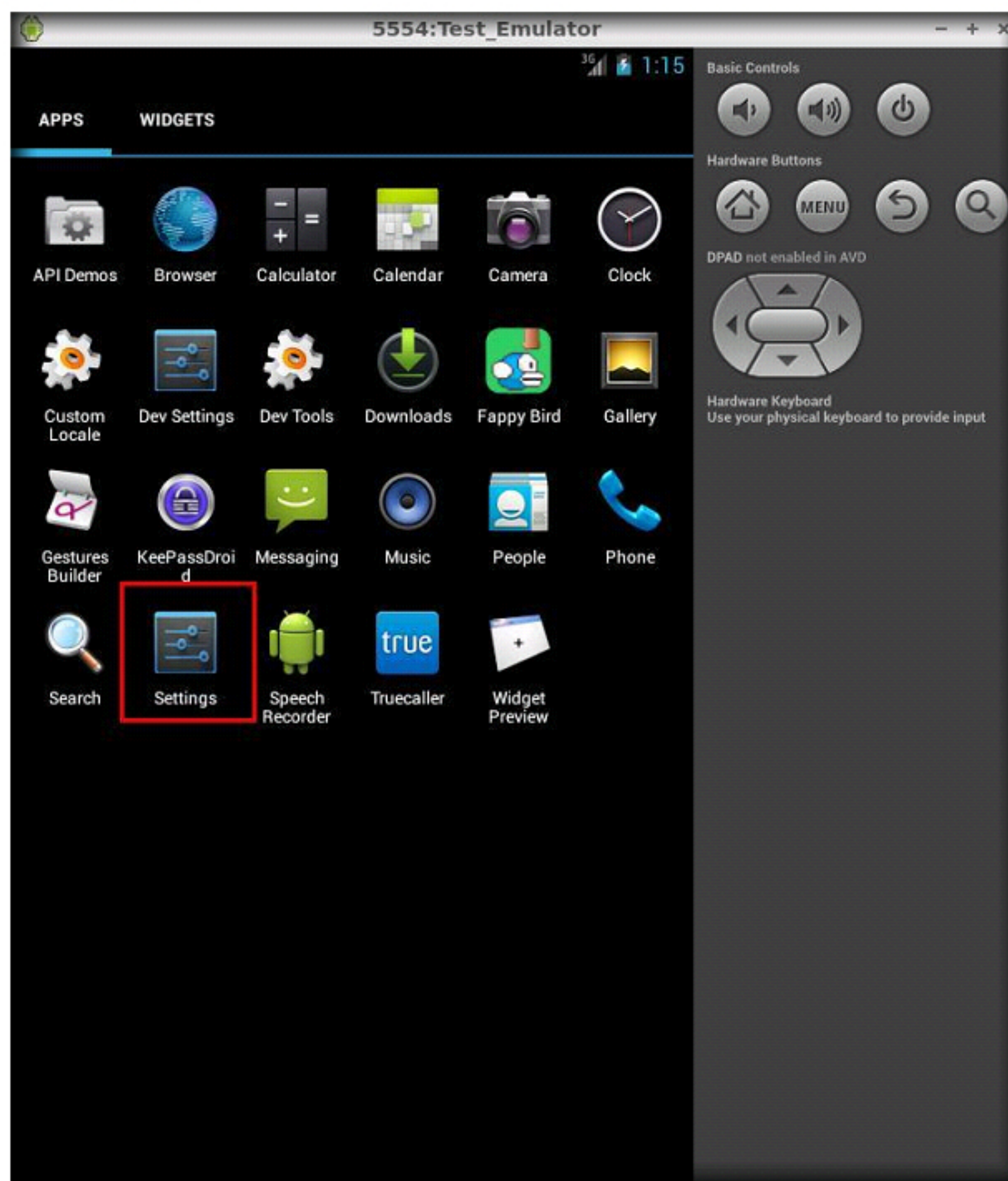


Setting Screen Lock Pattern

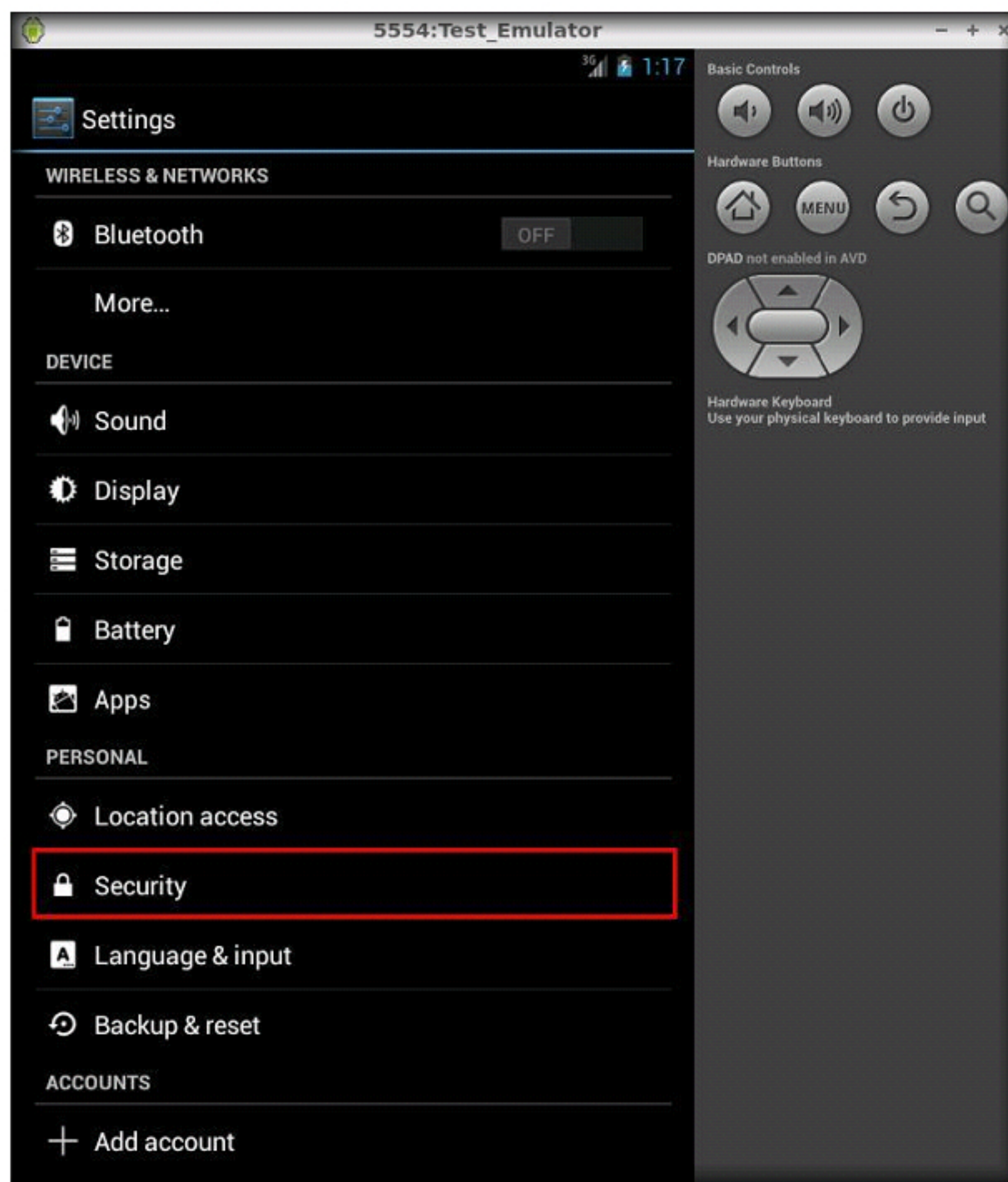
28. To set Screen Lock Pattern, tap **App Drawer** icon as shown in the following screenshot



29. **Apps** screen appears, tap **Settings** application

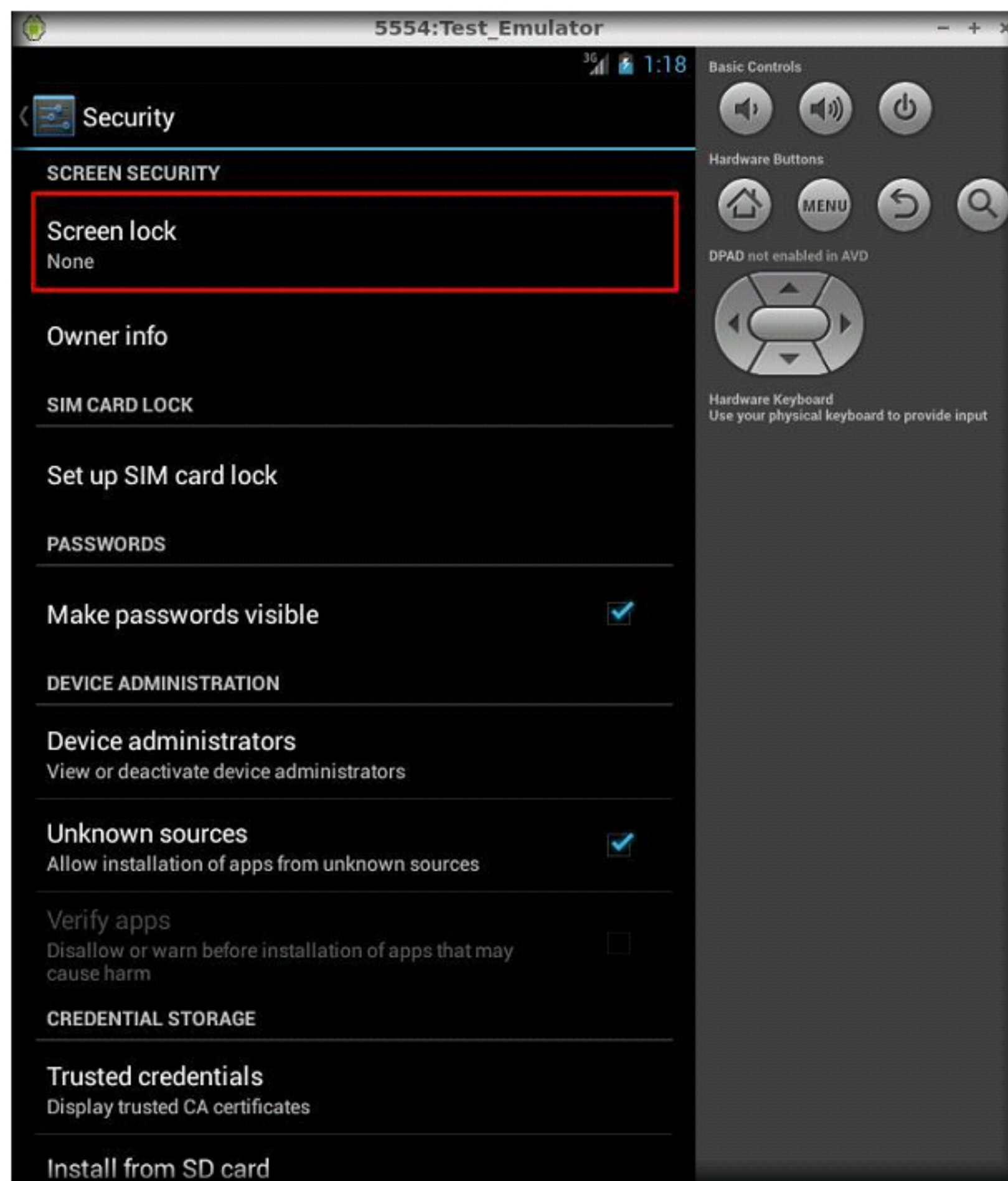


30. Scroll down the **Settings** screen and tap **Security**

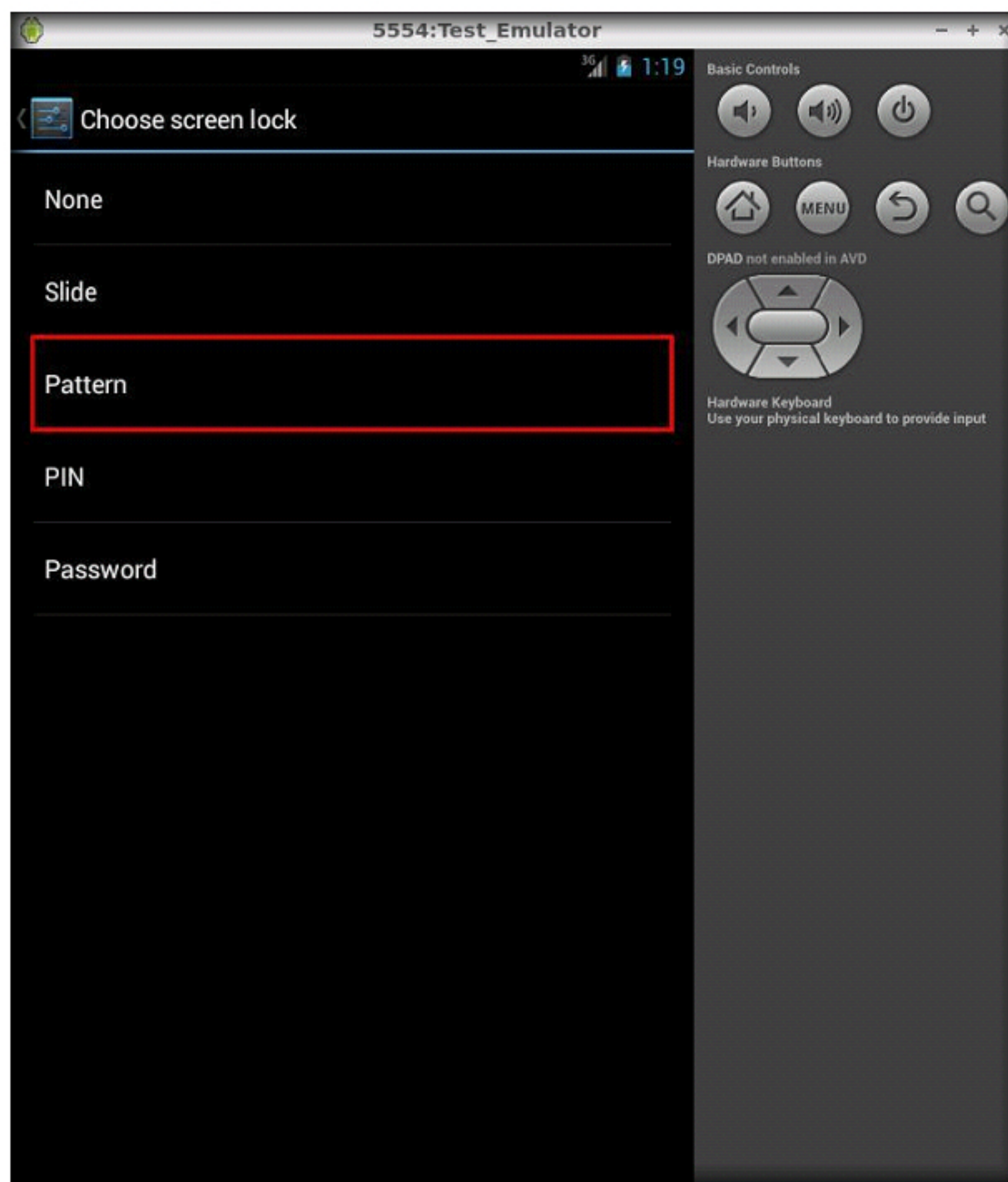


31. Tap **Screen lock** option in the **Security** screen

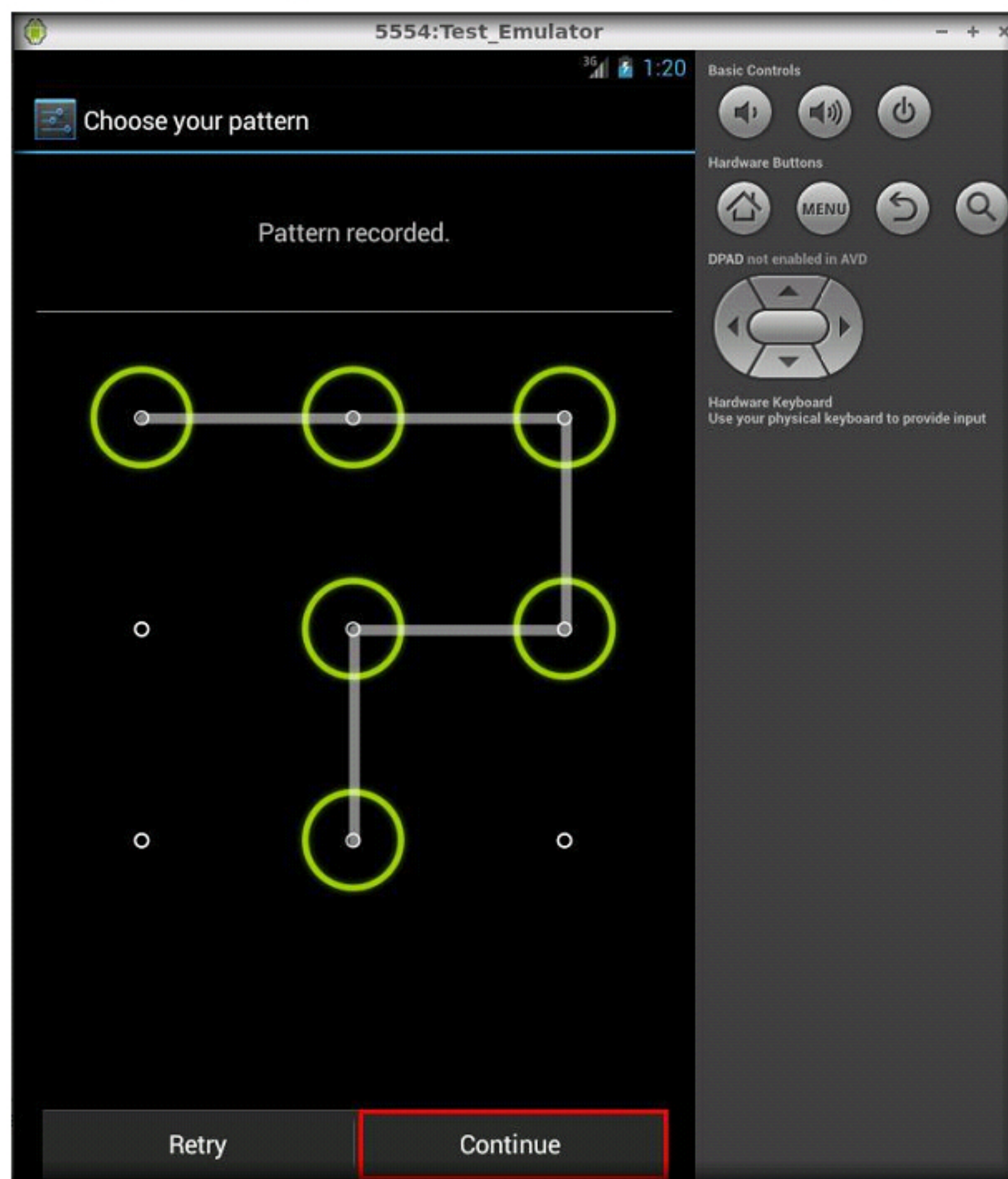
Note: By default, Screen lock is set to **None**



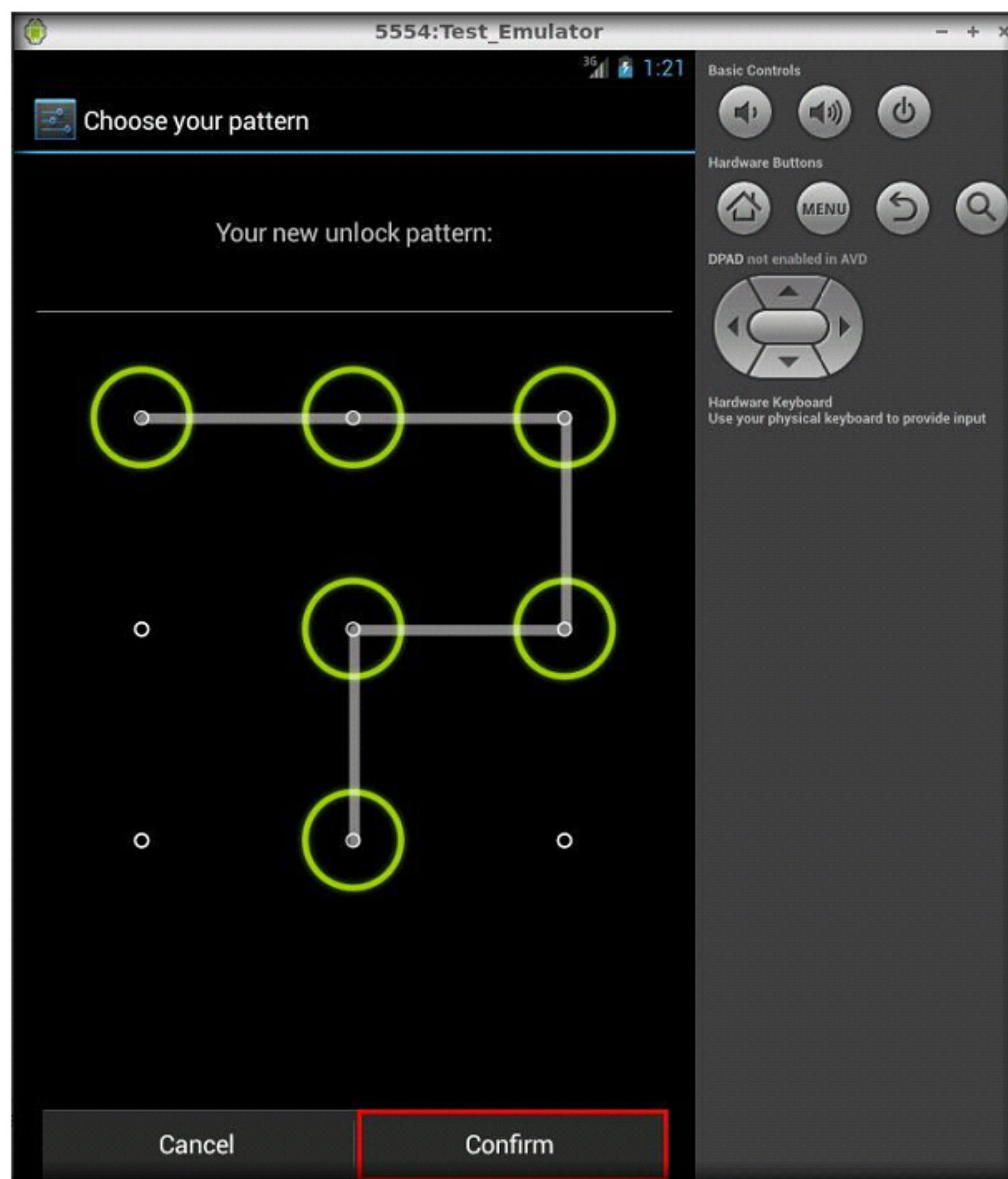
32. **Choose screen lock** screen appears, tap **Pattern** option



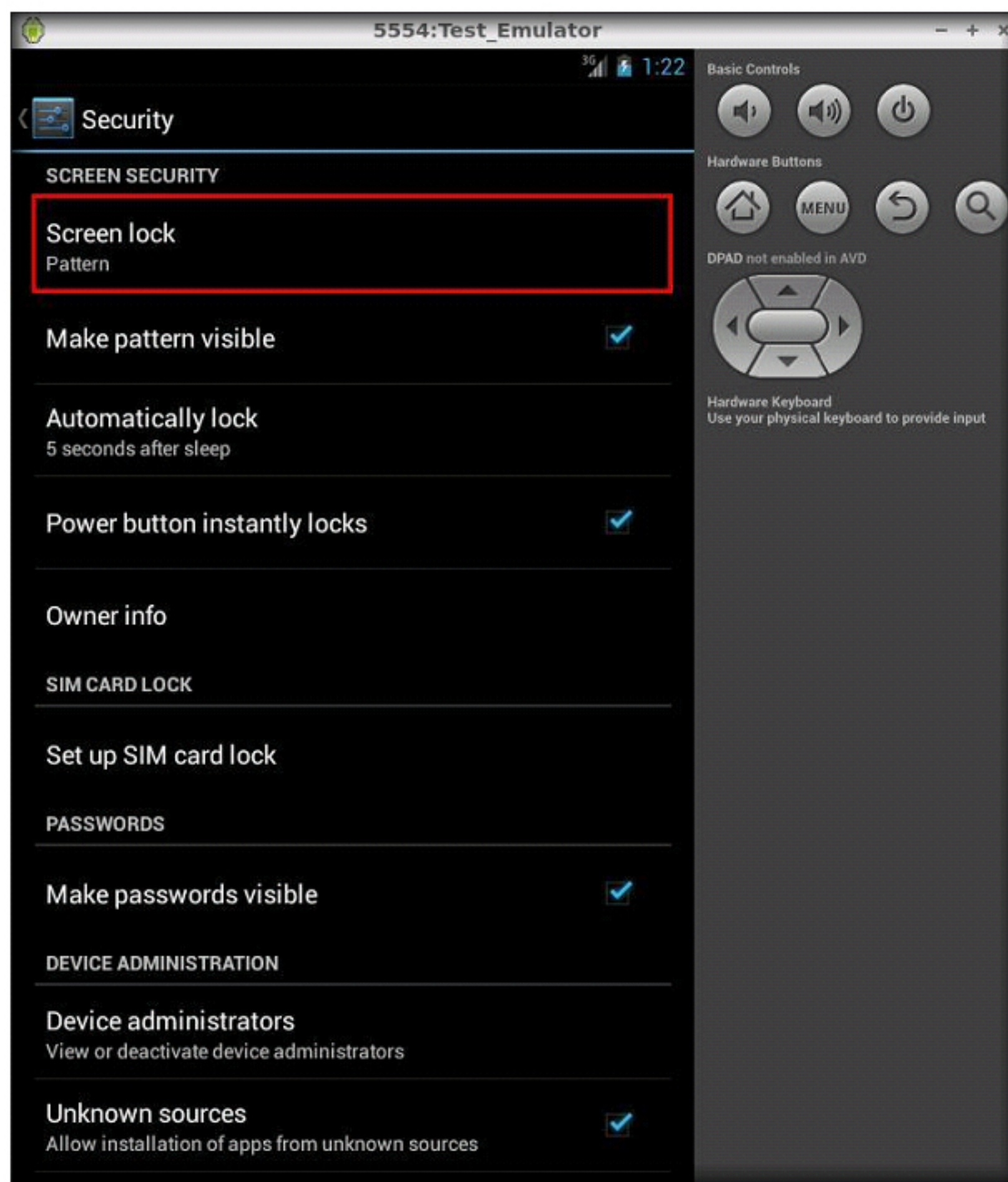
33. **Choose your pattern** screen appears, draw a pattern as shown in the screenshot and tap **Continue**



34. Now **redraw** the same pattern and tap **Confirm**

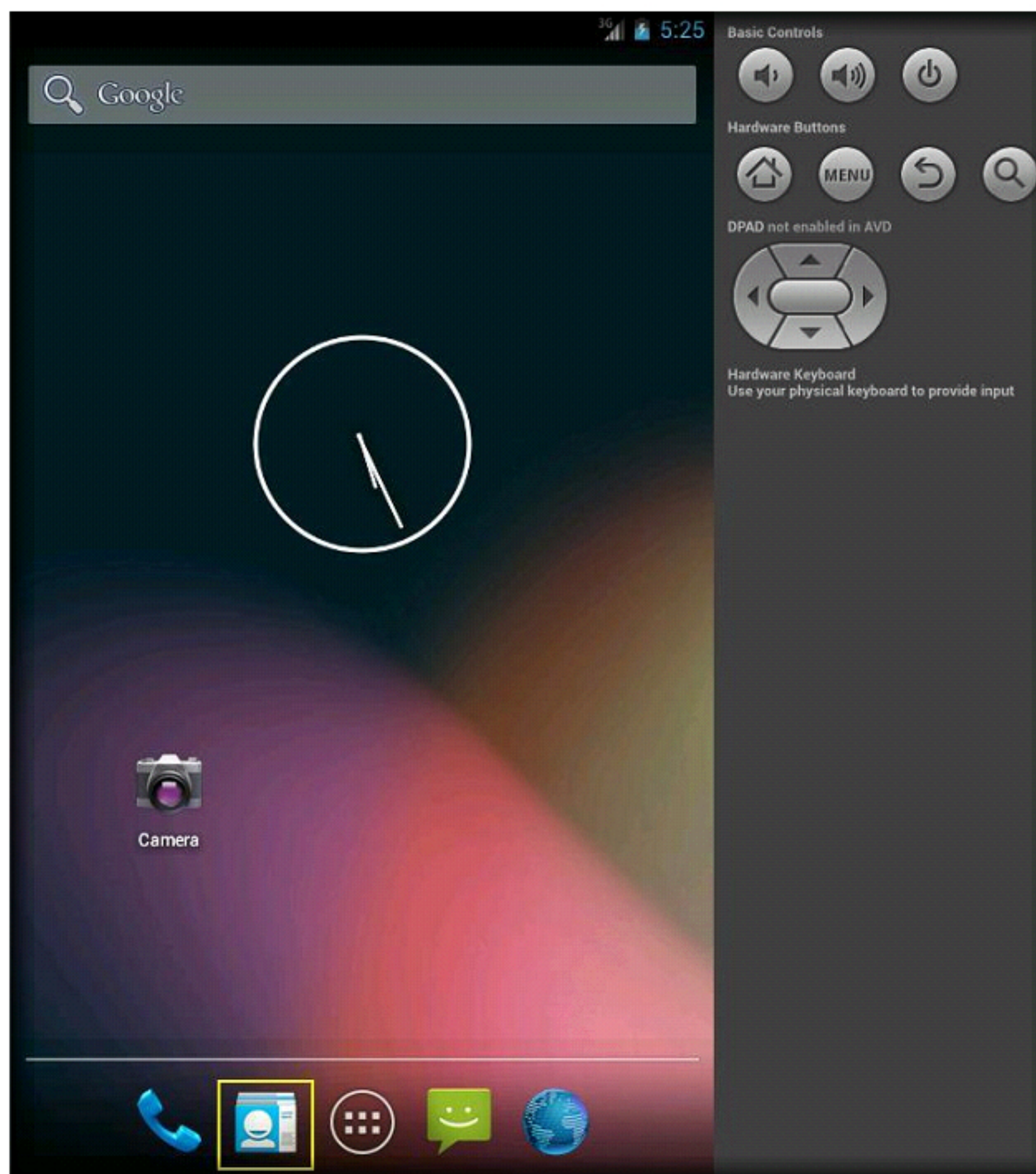


35. Now in **Security** wizard, you can see that **Screen lock** is enabled with a **Pattern**

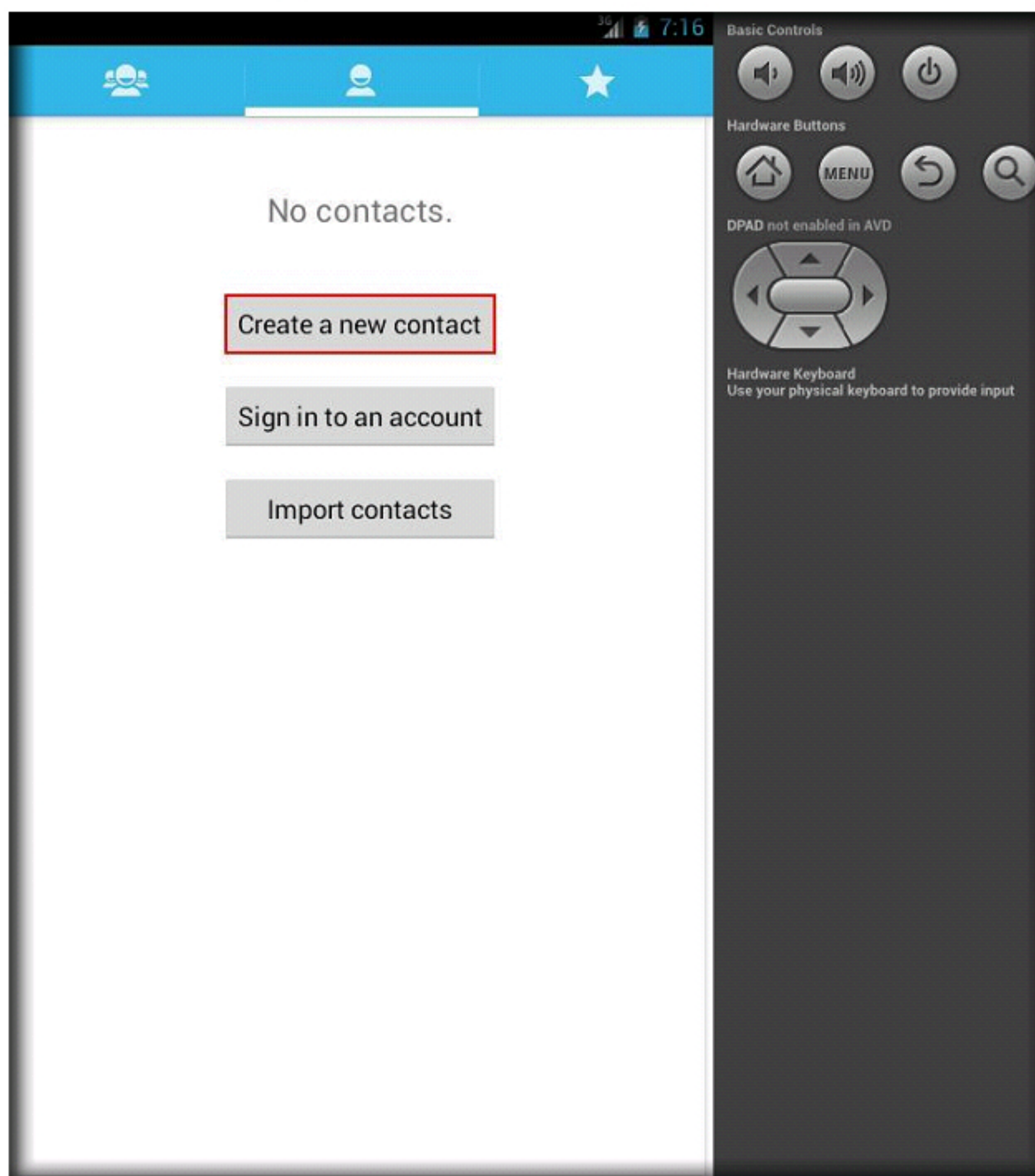


Add contacts, make calls and send text messages

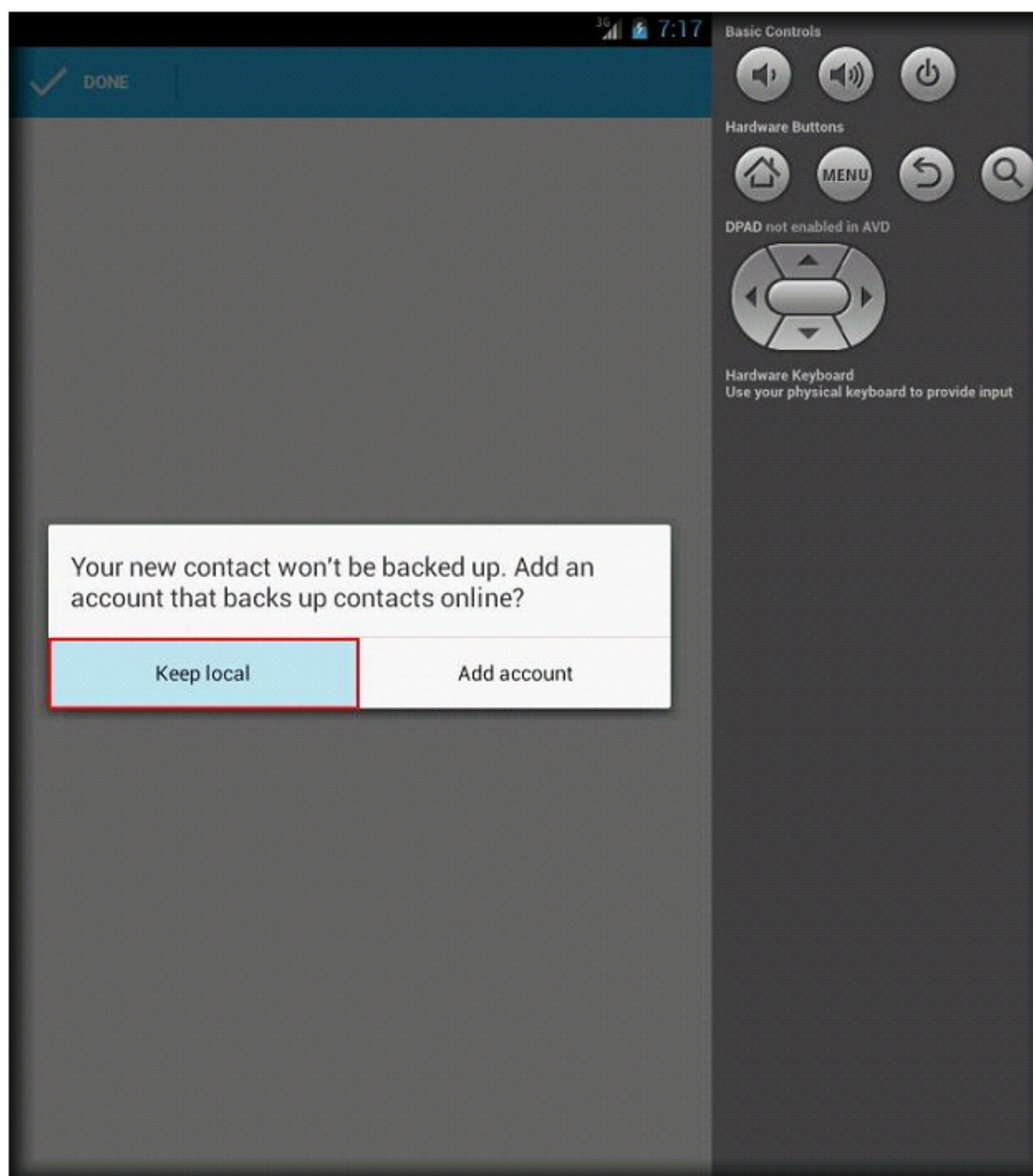
36. Tap **Contacts** icon on the home screen in order to view the contacts stored on the device



37. You will observe that the contact list is empty in the device. Click **Create a new contact** button in order to add a contact.



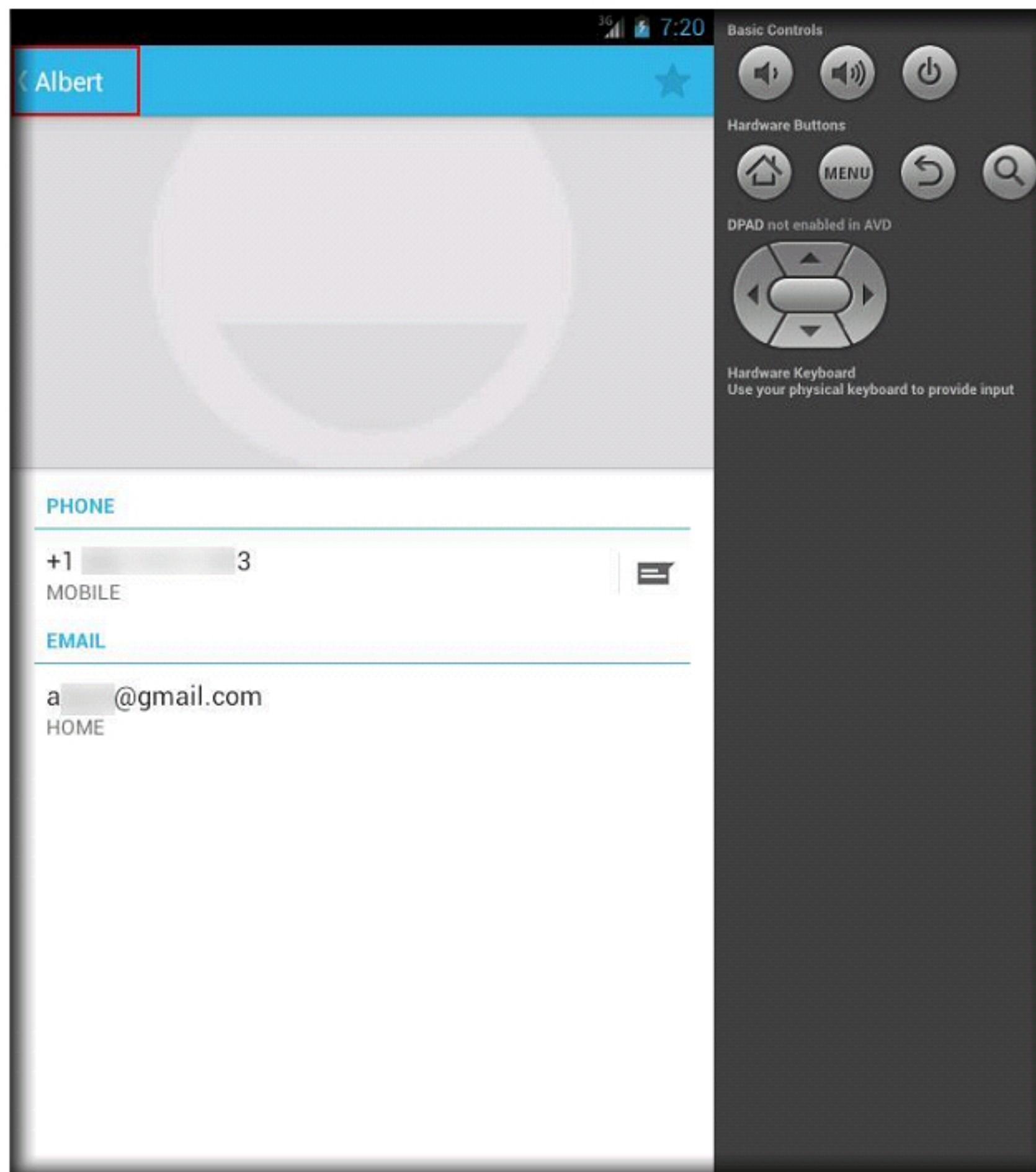
38. In order to avoid the contacts from being backed up, tap **Keep local** icon on the pop-up




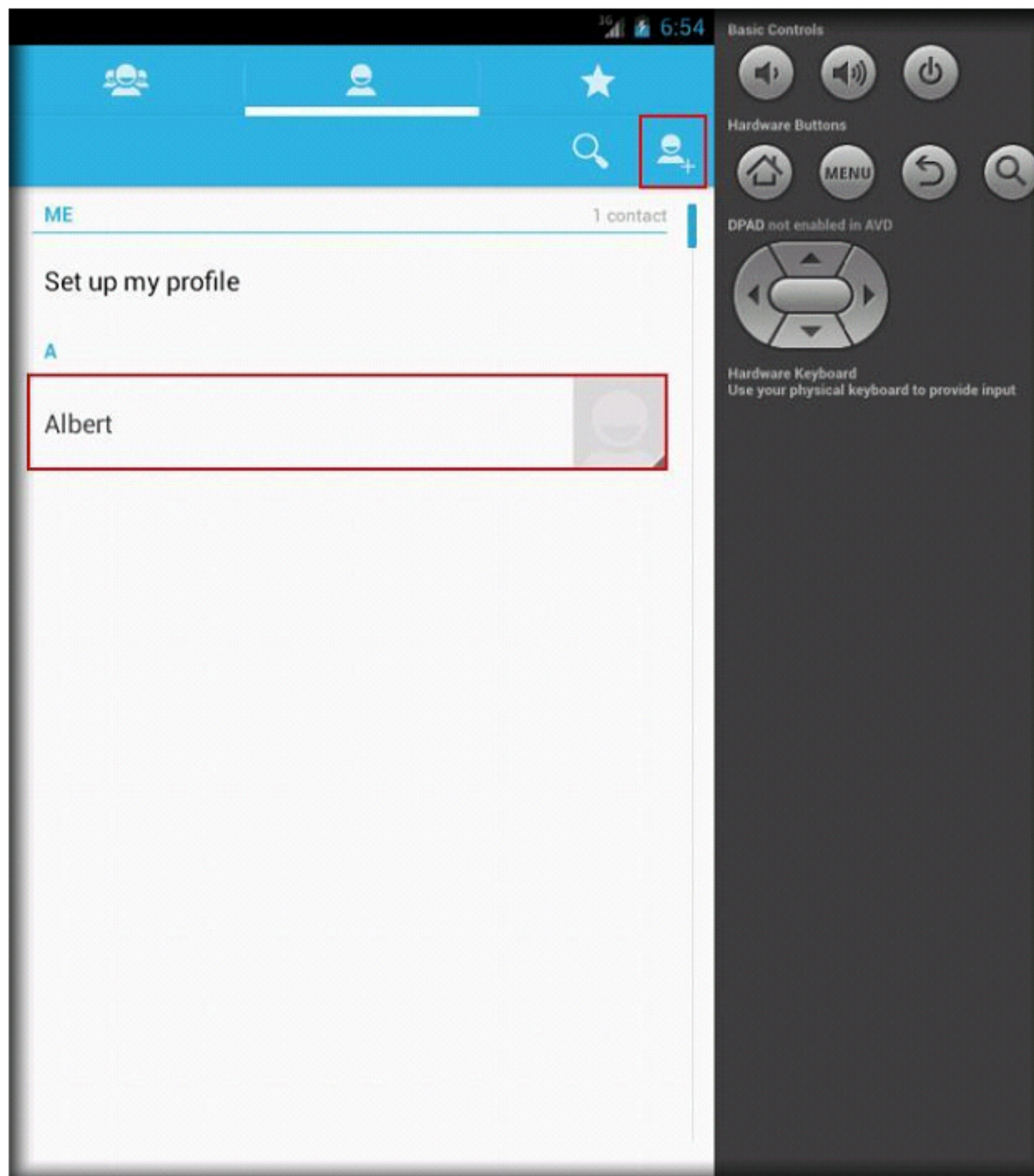
39. A **Contact** screen appears, fill in the details and tap **Done** in order to save the contact to the device

The screenshot shows an Android contact creation interface. At the top, a blue bar contains a checkmark icon and the word "DONE". Below this, the text "Phone-only, unsynced contact" is displayed. The name field contains "Albert". Below the name field is the "Add organization" section. The "PHONE" section has a field with "+1" and ".3", and a "MOBILE" label with a close button. Below the phone field is the "Add new" section. The "EMAIL" section has a field with "a" and "@gmail.com", and a "HOME" label with a close button. Below the email field is the "Add new" section. The "ADDRESS" section has a field with "Address" and a "HOME" label. At the bottom, there is a button labeled "Add another field". On the right side of the screen, there is a virtual control panel with the following elements: "Basic Controls" (volume, power), "Hardware Buttons" (home, menu, back, search), "DPAD not enabled in AVD" (a directional pad icon), and "Hardware Keyboard" (a message to use the physical keyboard).

40. The created contact appears on the screen with the contact name displayed on the top-left corner of the screen. Tap the contact name in order to go back to the **Contacts** screen.



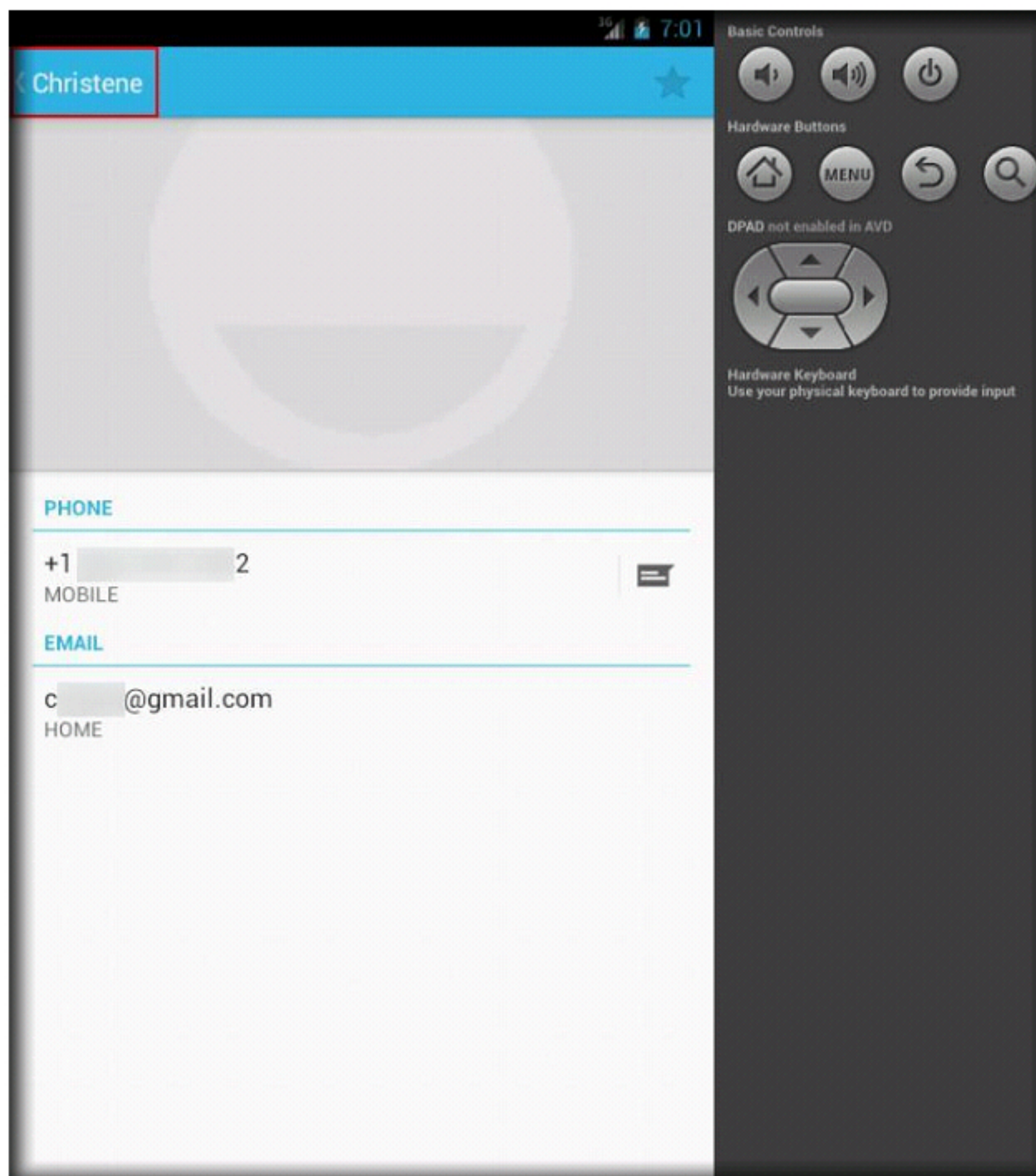
41. The added contact appears in the **Contacts** screen, tap  icon in order to add a new contact



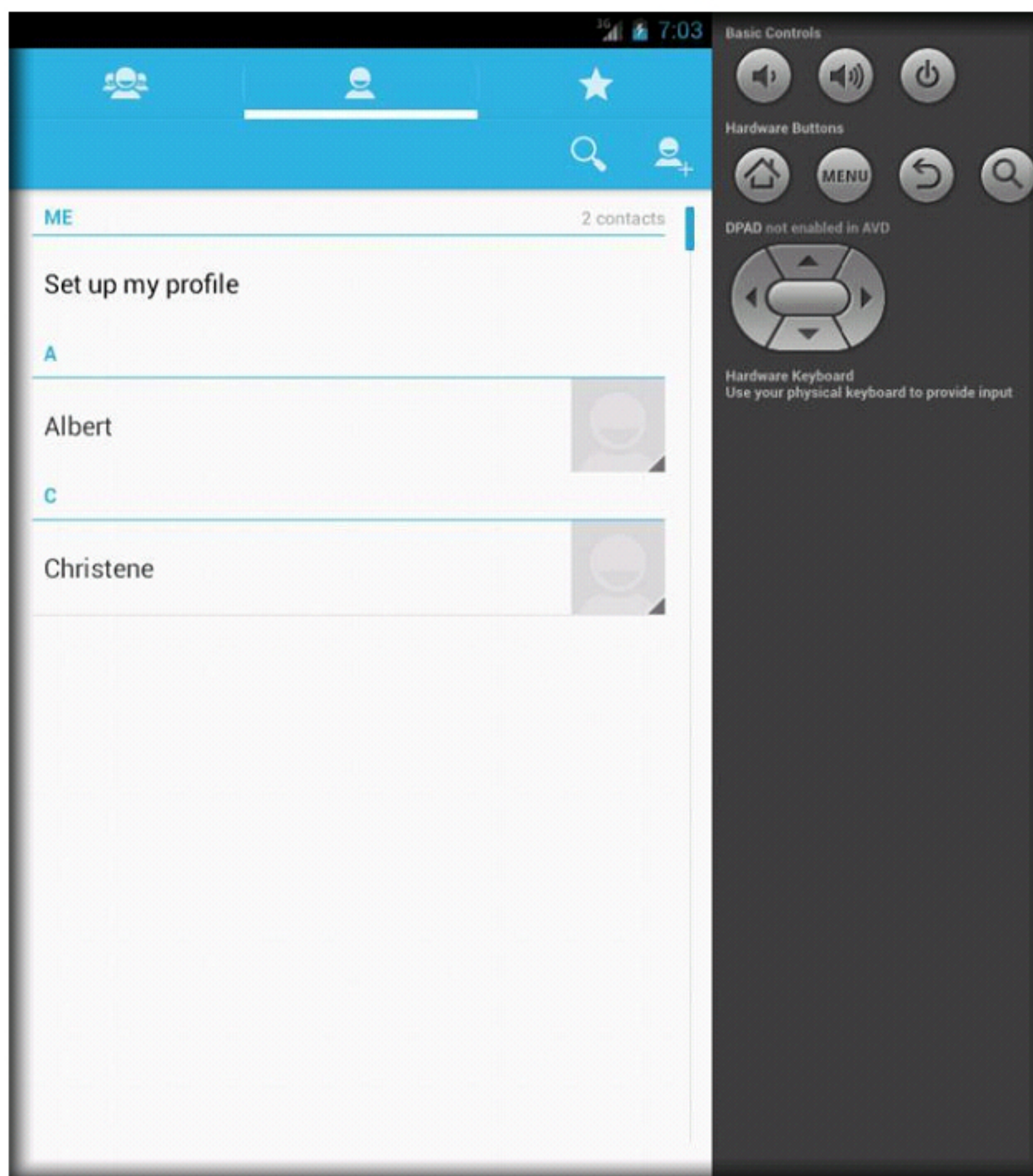
42. A **Contact** screen appears, fill in the details and tap **Done** in order to save the contact to the device

The screenshot shows an Android contact creation interface. At the top, a blue bar contains a checkmark icon and the word "DONE". Below this, the text "Phone-only, unsynced contact" is displayed. The name field contains "Christene". Below the name field is the "Add organization" section. The "PHONE" section has a field with "+1" and "2", and a "MOBILE" label with a close button. Below the phone field is the "Add new" section. The "EMAIL" section has a field with "c" and "@gmail.com", and a "HOME" label with a close button. Below the email field is the "Add new" section. The "ADDRESS" section has a field with "Address" and a "HOME" label with a close button. At the bottom, there is a button labeled "Add another field". On the right side of the screen, there is a virtual control panel with the following elements: "Basic Controls" (volume up/down, power), "Hardware Buttons" (home, menu, back, search), "DPAD not enabled in AVD" (a directional pad icon), and "Hardware Keyboard" (a message: "Use your physical keyboard to provide input").

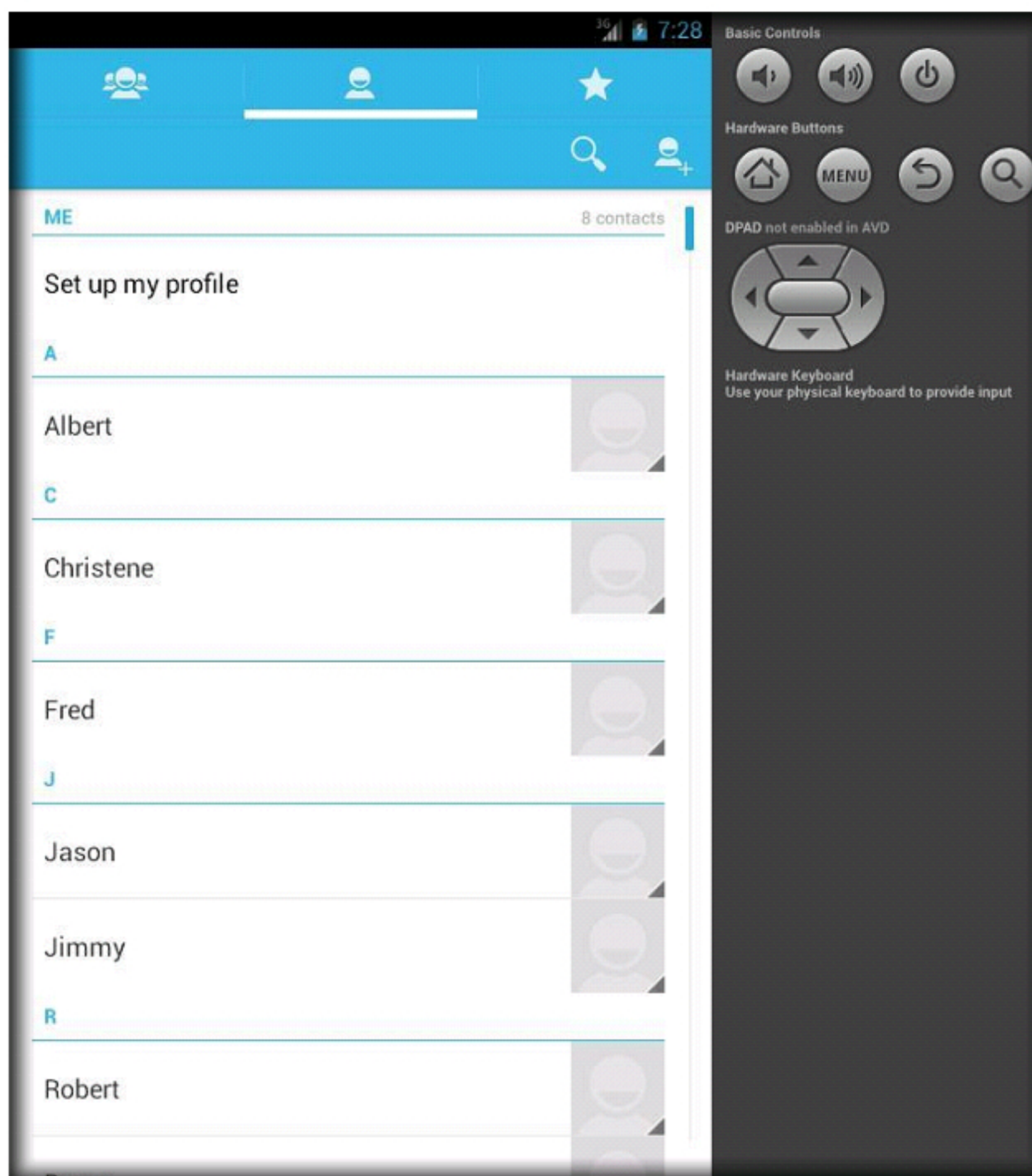
43. The created contact appears on the screen with the contact name displayed on the top-left corner of the screen. Tap the contact name in order to go back to the **Contacts** screen.




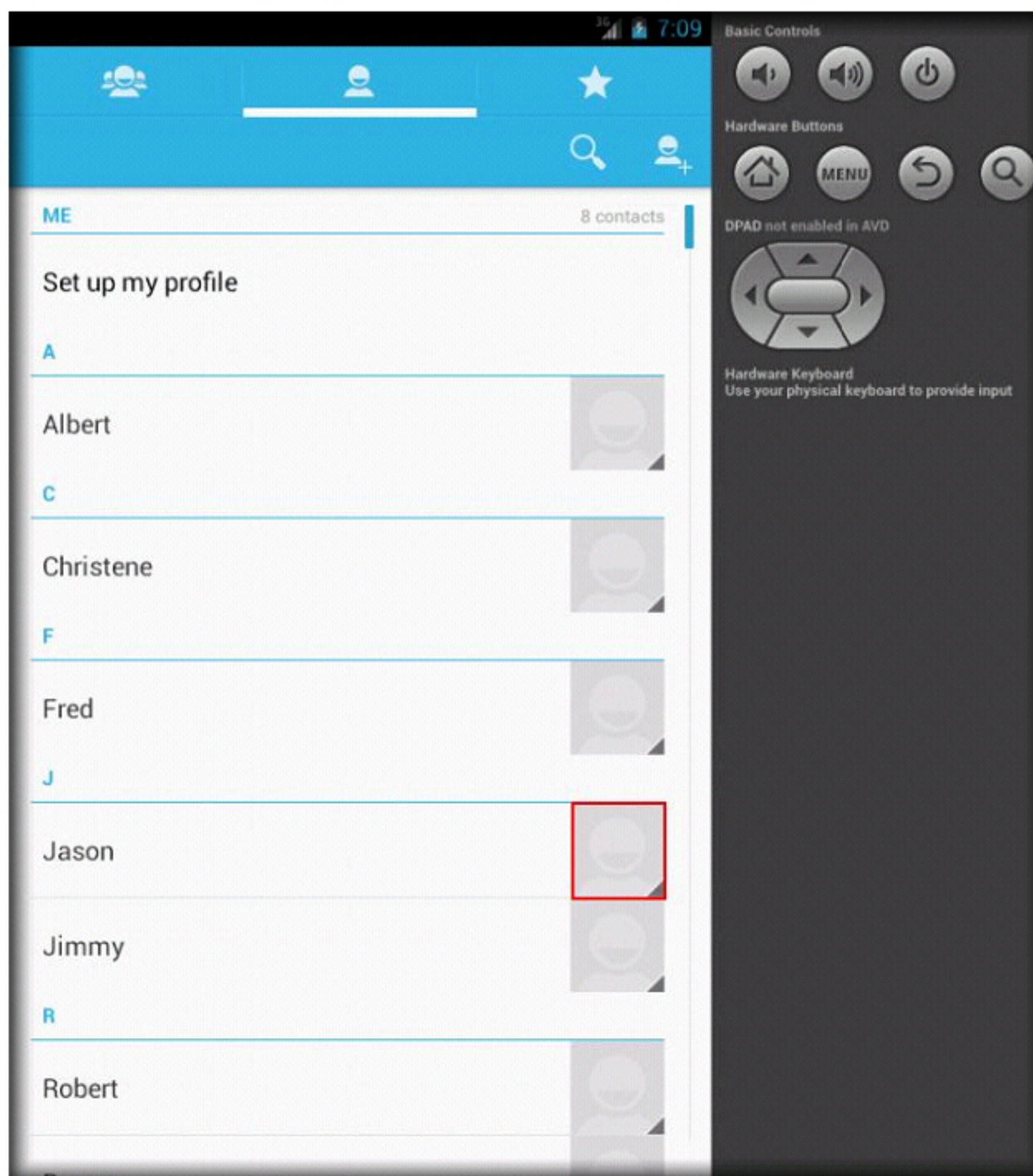
44. The added contact appears in the Contacts screen as shown in the following screenshot:



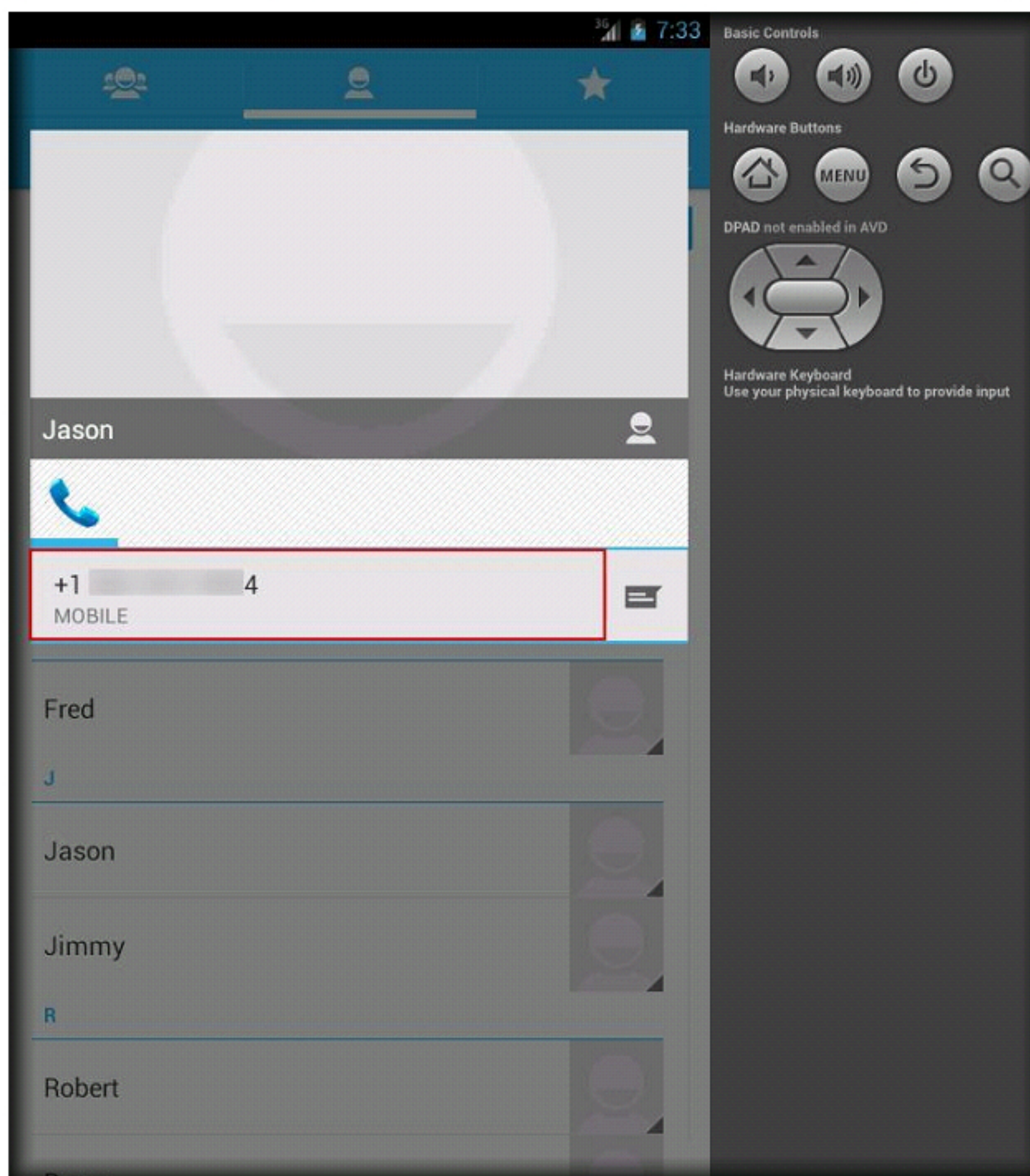
45. This way, follow the steps **41** and **42** in order to add a few more contacts:



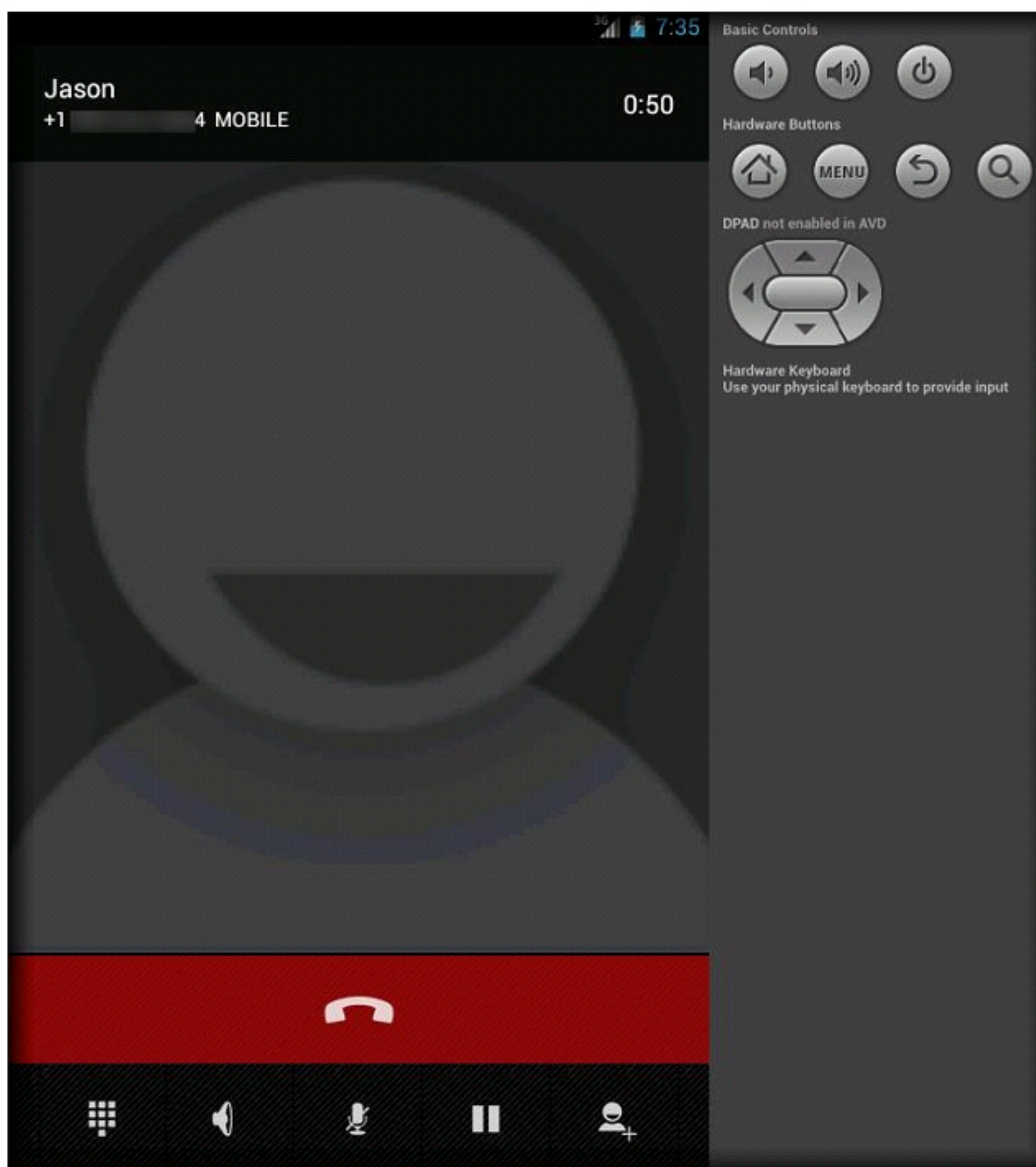
46. Tap on  icon of a particular contact (here, **Jason**) in order to call or text that particular contact




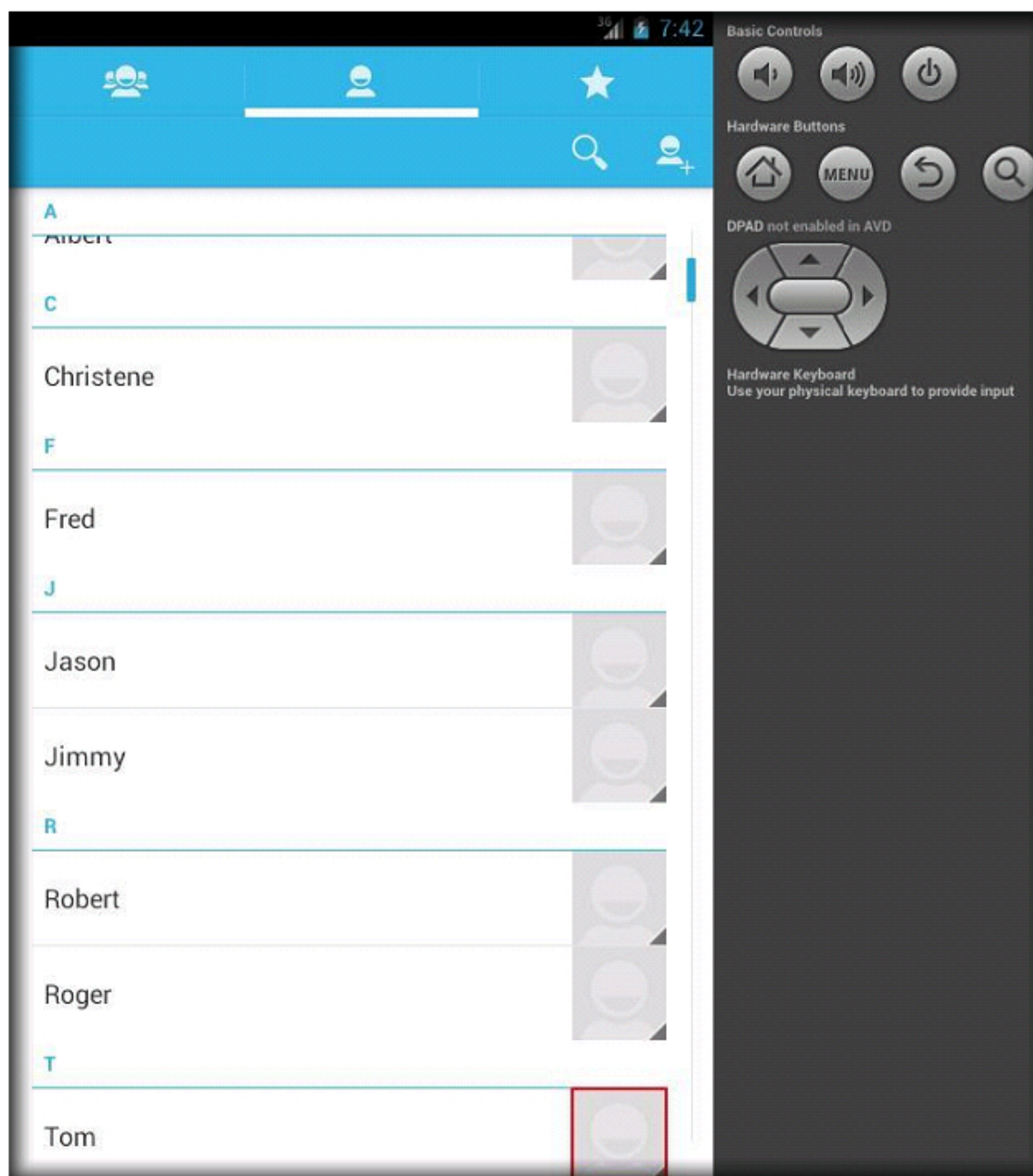
47. The selected contact appears on the screen, tap on the mobile number in order to make a (dummy) call




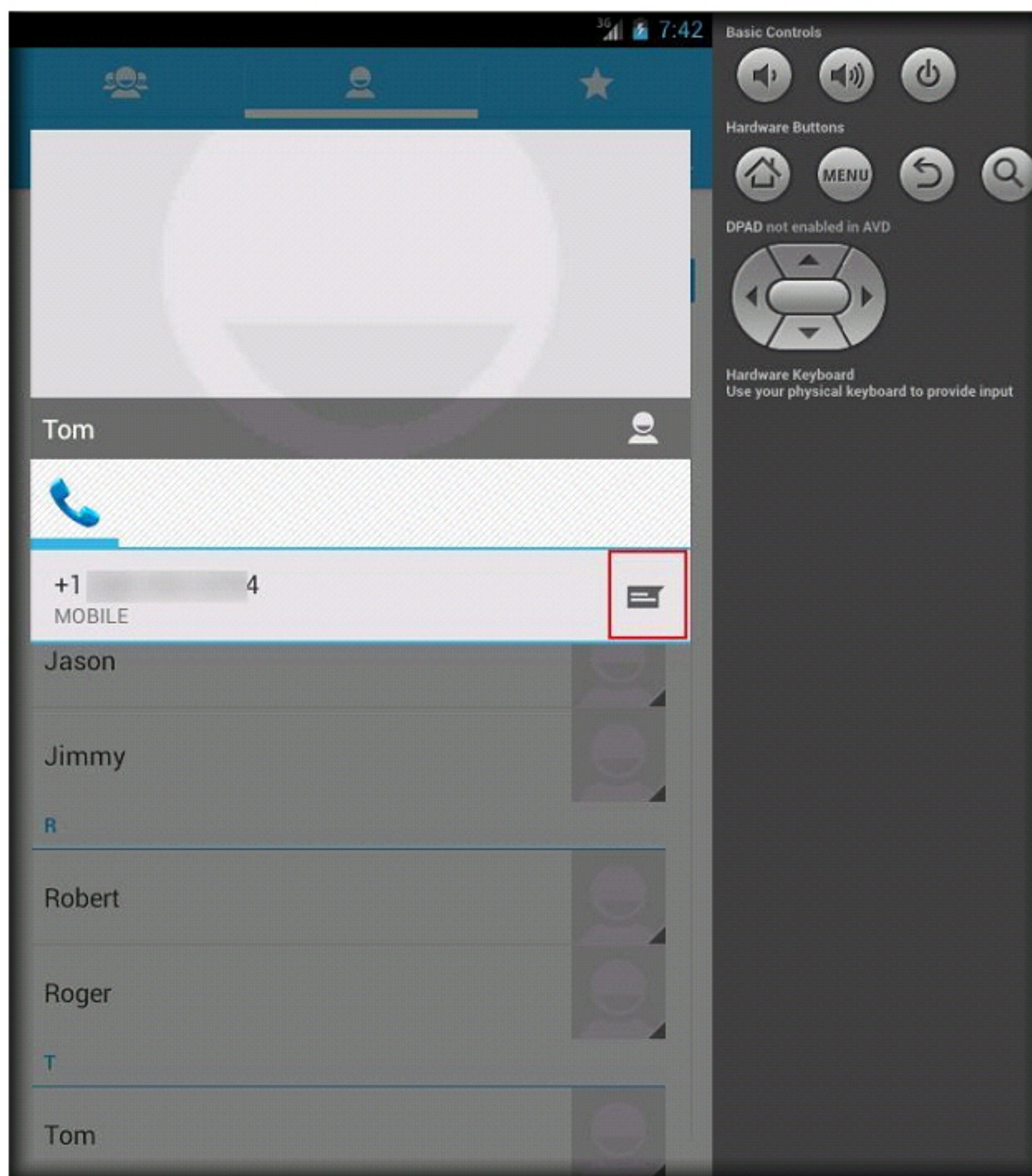
48. The emulator device makes a call to the selected contact as shown in the following screenshot:




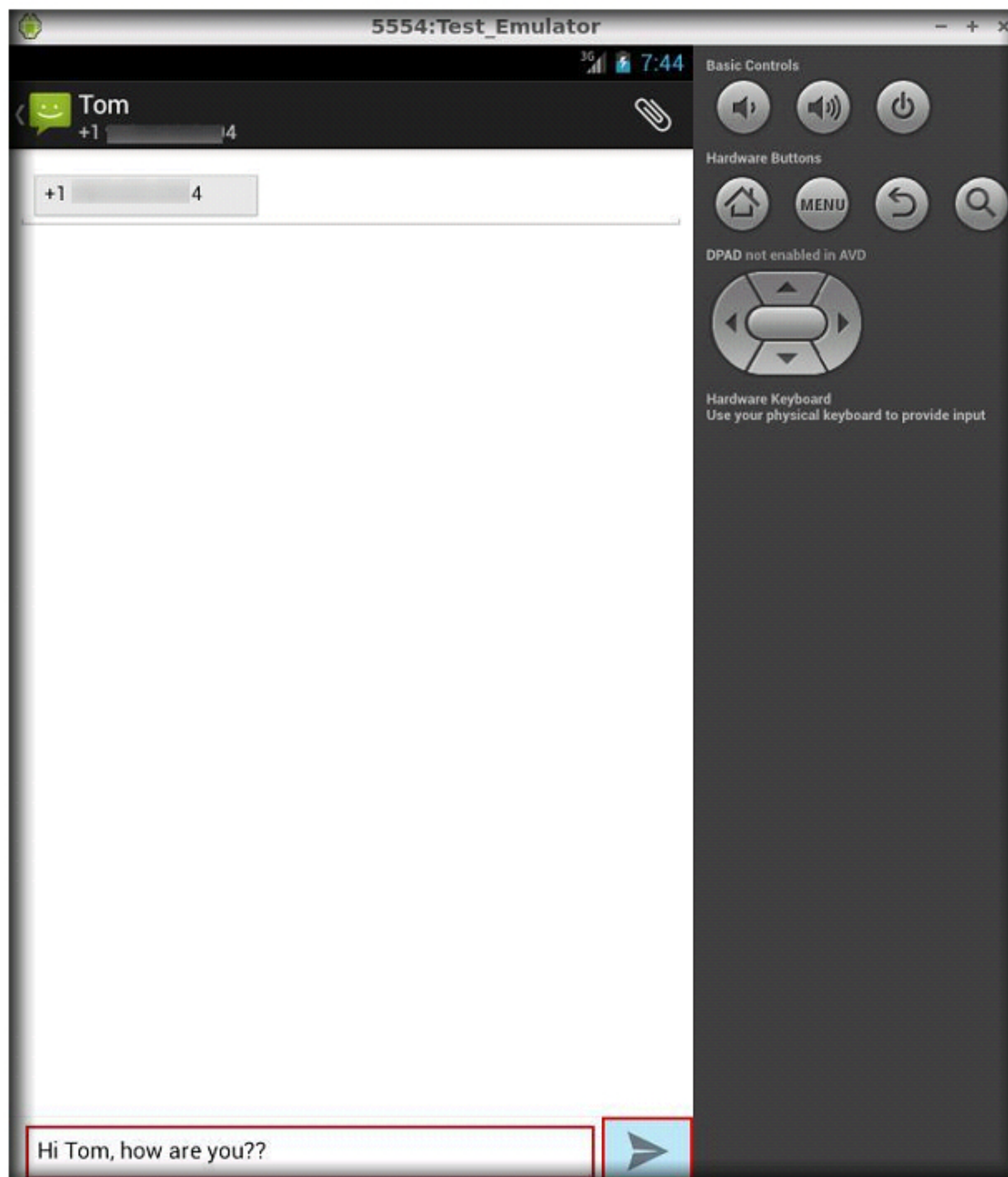
49. Tap on  icon of a particular contact (here, **Tom**) in order to call or text that particular contact



50. The selected contact appears on the screen, tap on  icon in order to put a (dummy) text message to that contact



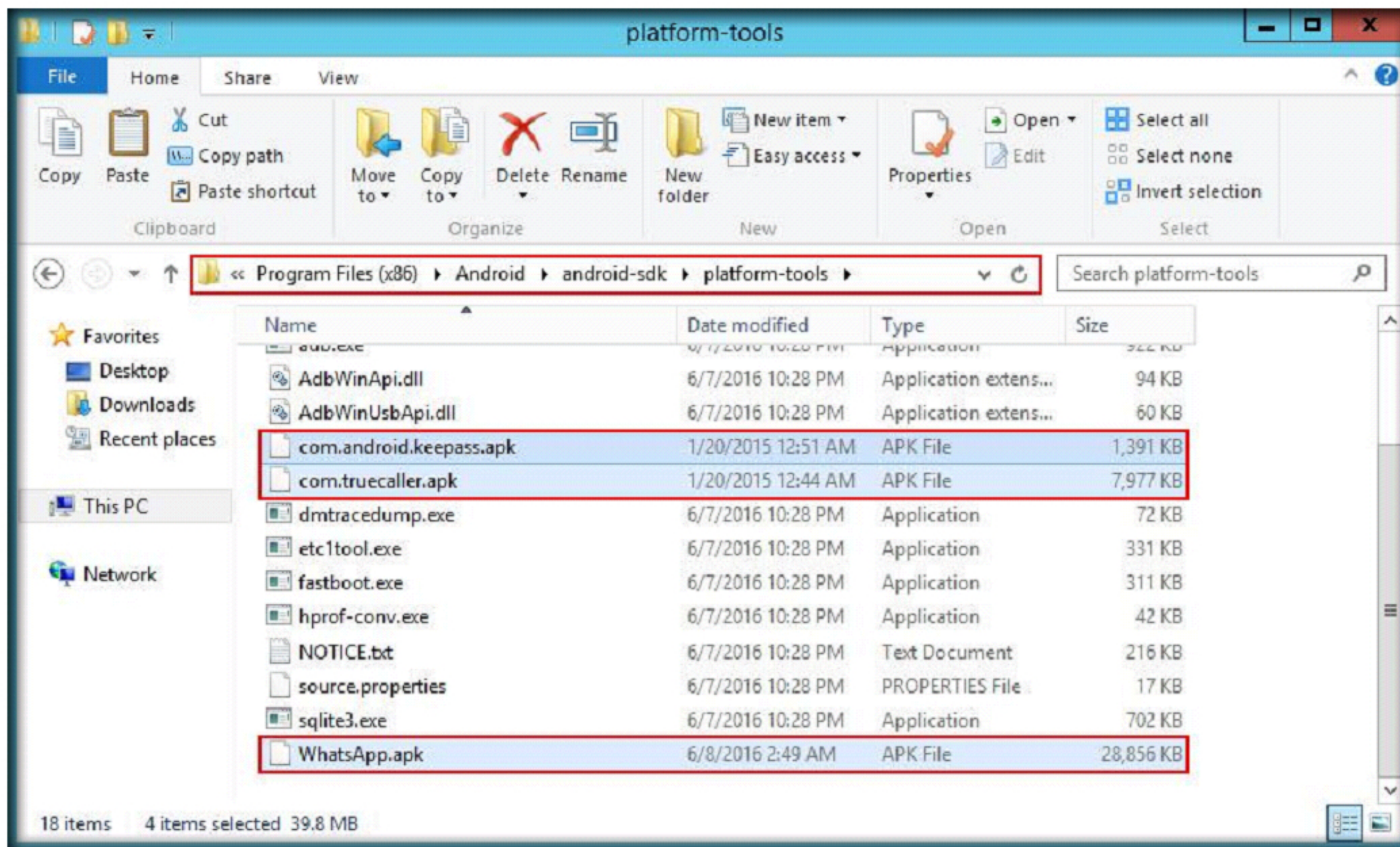
51. Text screen appears for the selected contact, type-in some text and tap  icon in order to send the text message



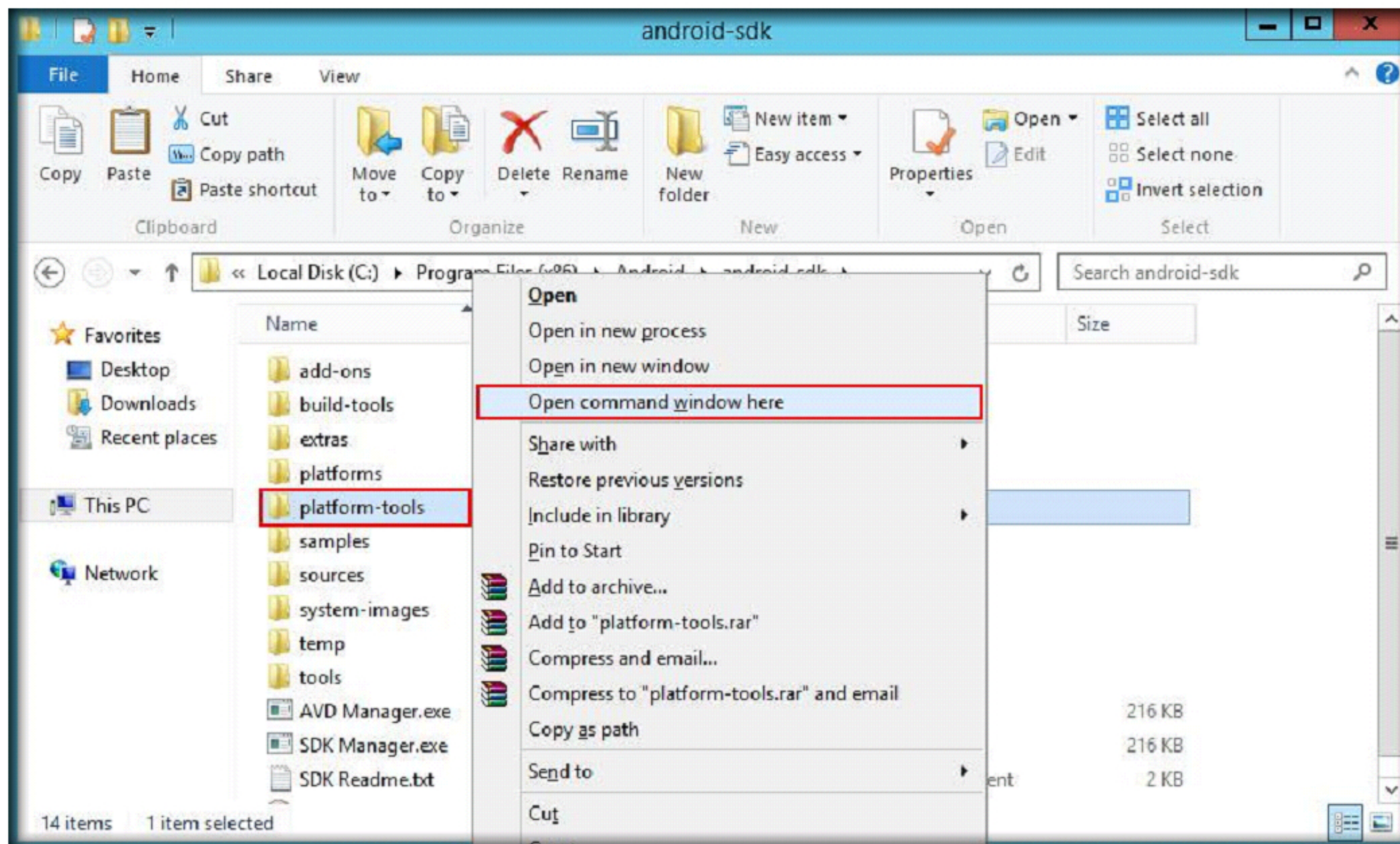
52. This way, you need to make a few calls and messages from the device

Install apks

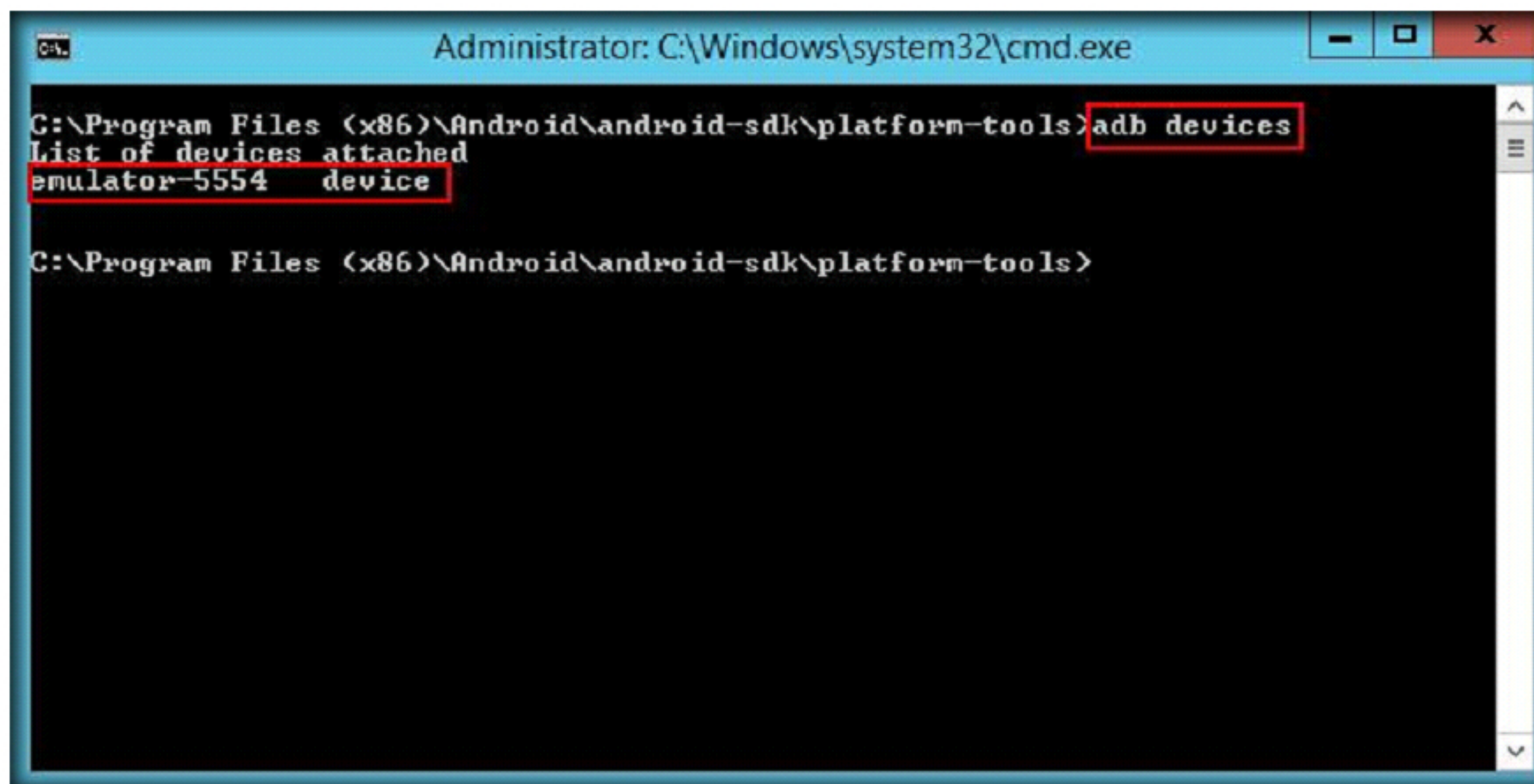
53. Navigate to **C:\CHFI-Tools\CHFIv9 Module 13 Mobile Forensics\apks**, copy **com.android.keeppass.apk**, **com.truecaller.apk** and **WhatsApp.apk**, and paste them in **C:\Program Files (x86)\Android\android-sdk\platform-tools**



54. Now, navigate to **C:\Program Files (x86)\Android\android-sdk**, select **platform-tools** folder, hold left or right **Shift** key on the keyboard, right-click **platform-tools** folder and select **Open command window here** from the context menu



55. Command prompt appears, pointing to the location to **C:\Program Files (x86)\Android\android-sdk\platform-tools**. Type **adb devices** command in the terminal and press **Enter**. This displays a the android emulated device as shown in the following screenshot:

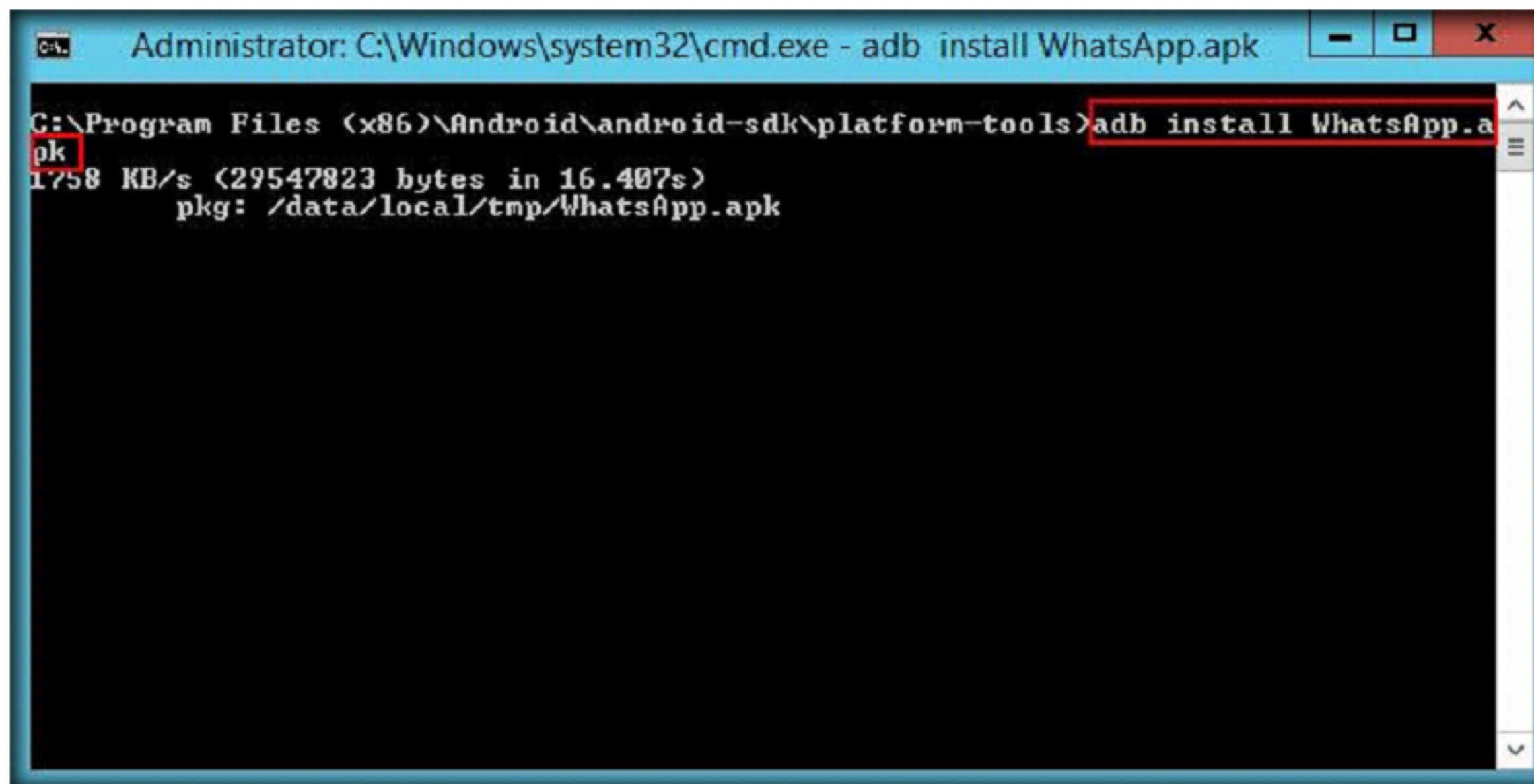


```
Administrator: C:\Windows\system32\cmd.exe

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb devices
List of devices attached
emulator-5554    device

C:\Program Files (x86)\Android\android-sdk\platform-tools>
```

56. In order to install **keePassDroid** application, type the command **adb install WhatsApp.apk** and press **Enter**. This installs the **Whatsapp** application in the emulator.

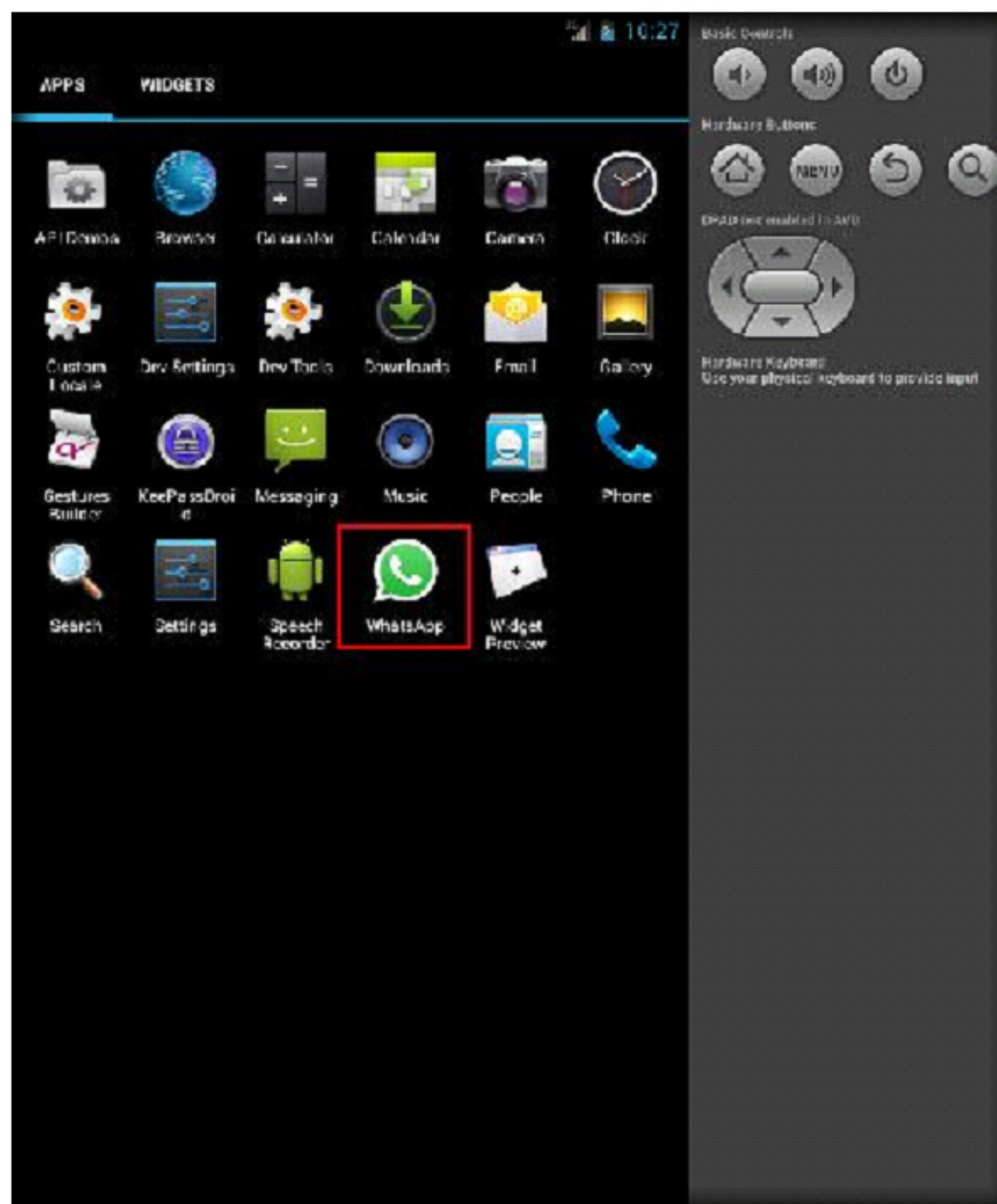


The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe - adb install WhatsApp.apk". The command prompt displays the following text:

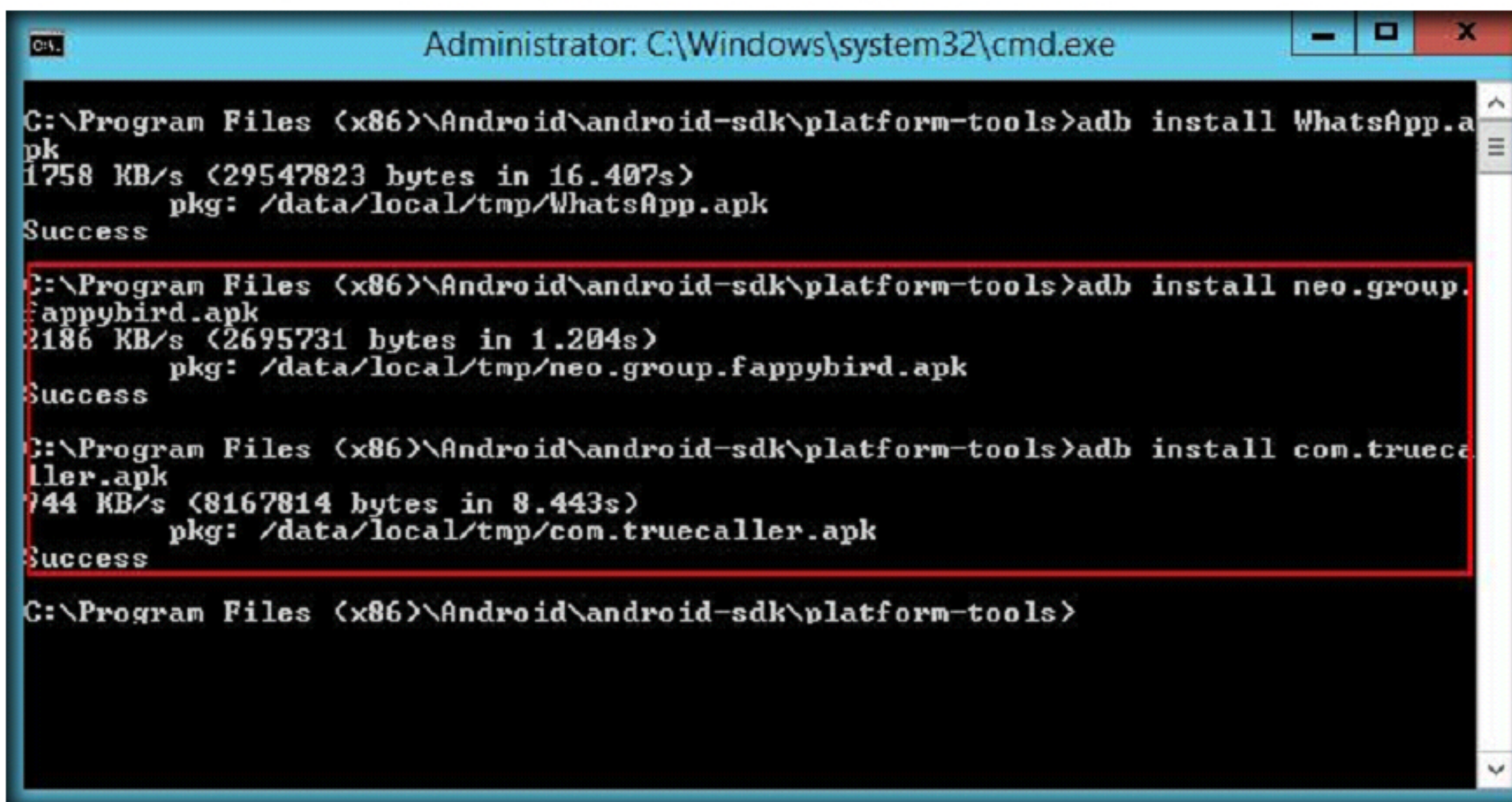
```
C:\Program Files (x86)\Android\android-sdk\platform-tools>adb install WhatsApp.apk
1758 KB/s (29547823 bytes in 16.407s)
pkg: /data/local/tmp/WhatsApp.apk
```

The command `adb install WhatsApp.apk` is highlighted with a red box, and the output `pkg: /data/local/tmp/WhatsApp.apk` is also highlighted with a red box.

57. You should be able to view the installed **WhatsApp** application in the **Apps** screen as shown in the following screenshot:



58. In the same way, follow step **56** and install flappybird and truecaller applications on the emulator



```
Administrator: C:\Windows\system32\cmd.exe

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb install WhatsApp.apk
1758 KB/s (29547823 bytes in 16.407s)
  pkg: /data/local/tmp/WhatsApp.apk
Success

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb install neo.group.flappybird.apk
2186 KB/s (2695731 bytes in 1.204s)
  pkg: /data/local/tmp/neo.group.flappybird.apk
Success

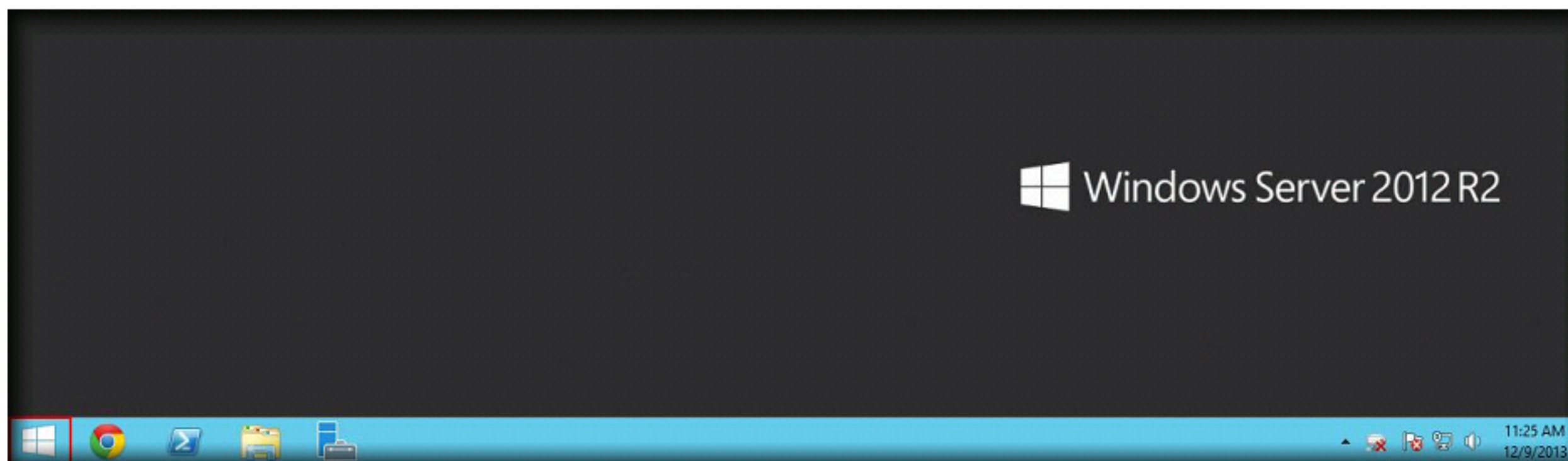
C:\Program Files (x86)\Android\android-sdk\platform-tools>adb install com.truecaller.apk
744 KB/s (8167814 bytes in 8.443s)
  pkg: /data/local/tmp/com.truecaller.apk
Success

C:\Program Files (x86)\Android\android-sdk\platform-tools>
```

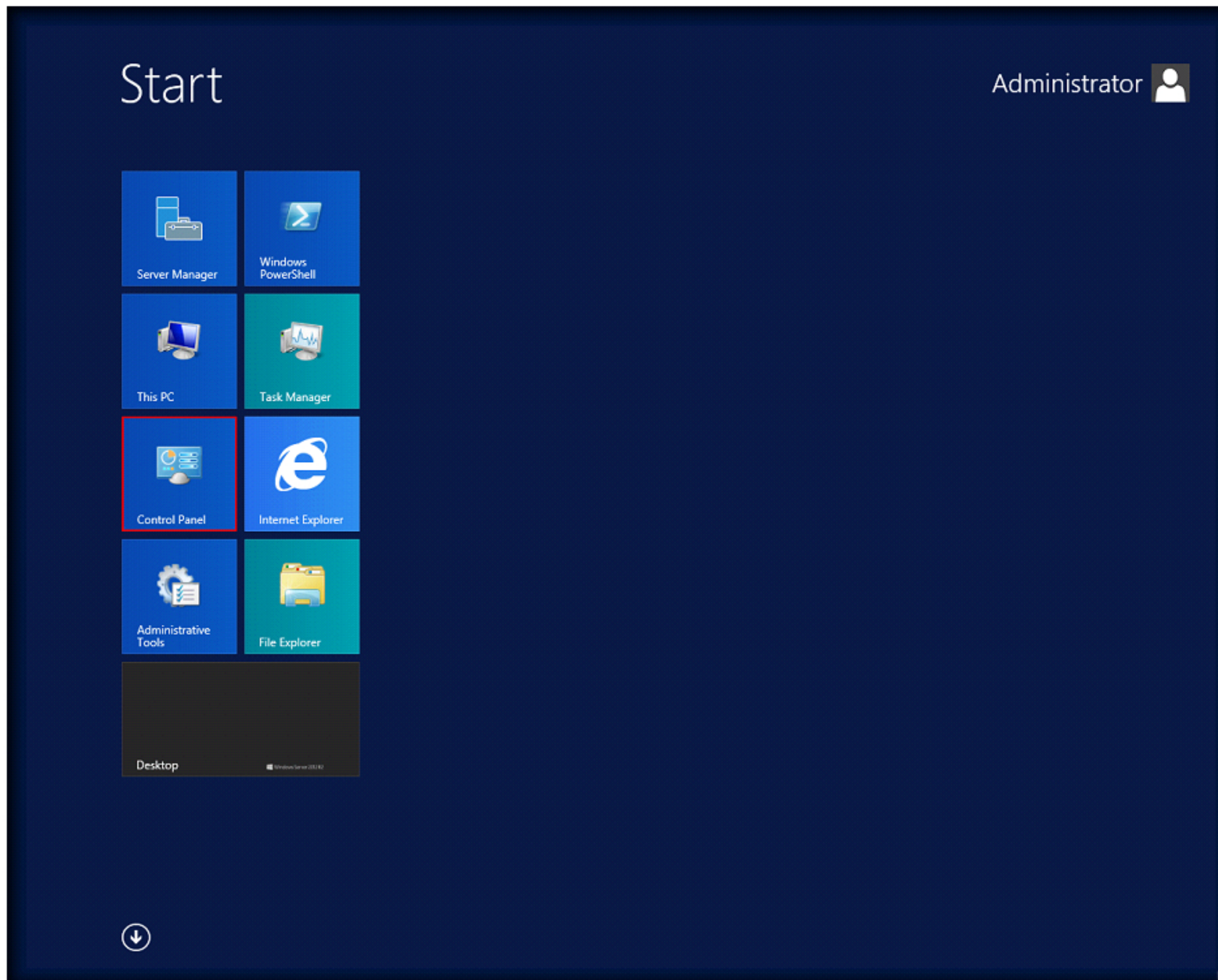

CT#19: Turn off Firewall in Windows Server 2012 and Windows 10 Virtual Machines

Windows Server 2012 Virtual Machine:

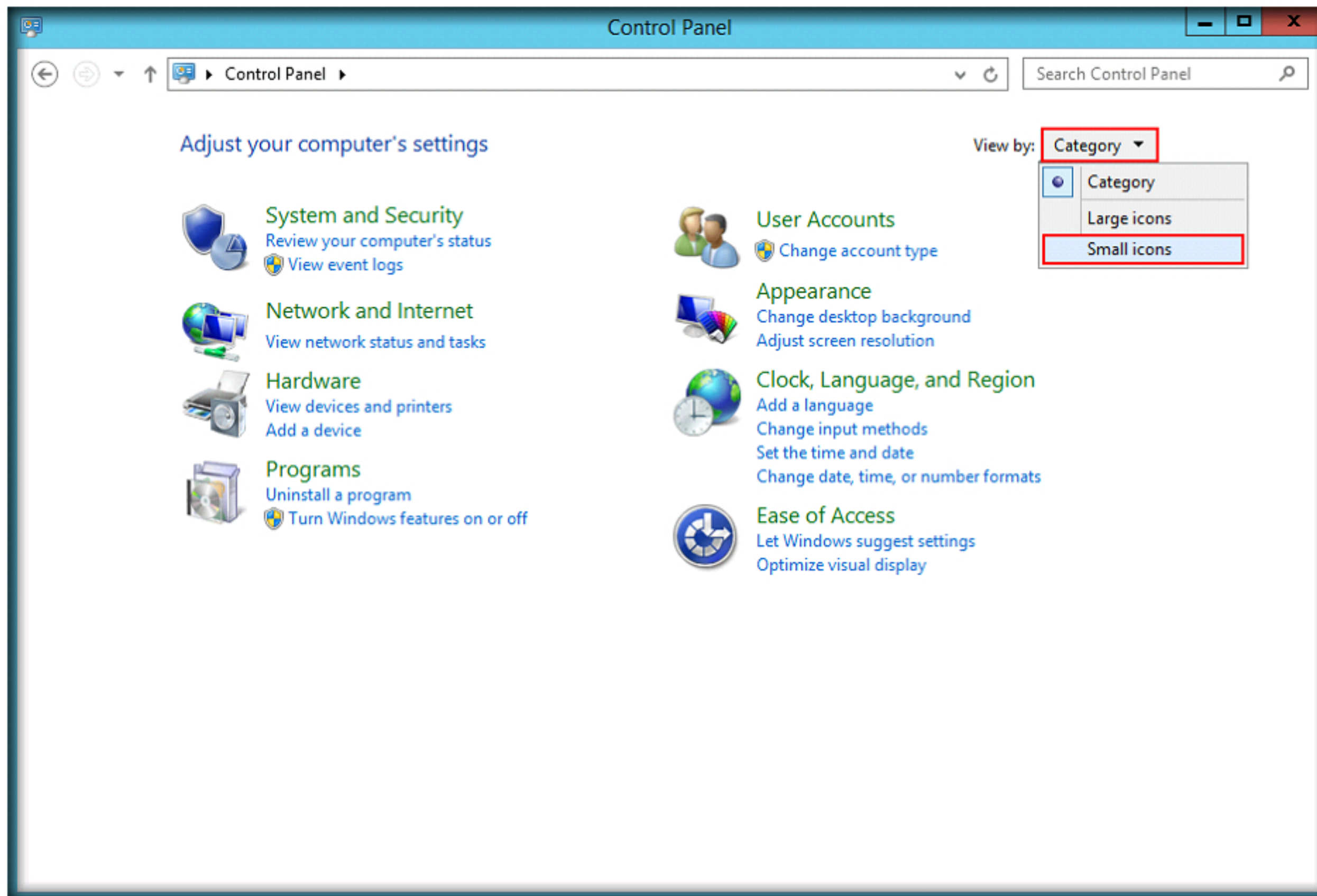
1. Logon to Windows Server 2012 virtual machine
2. Click **Windows** icon at the lower left corner of the screen



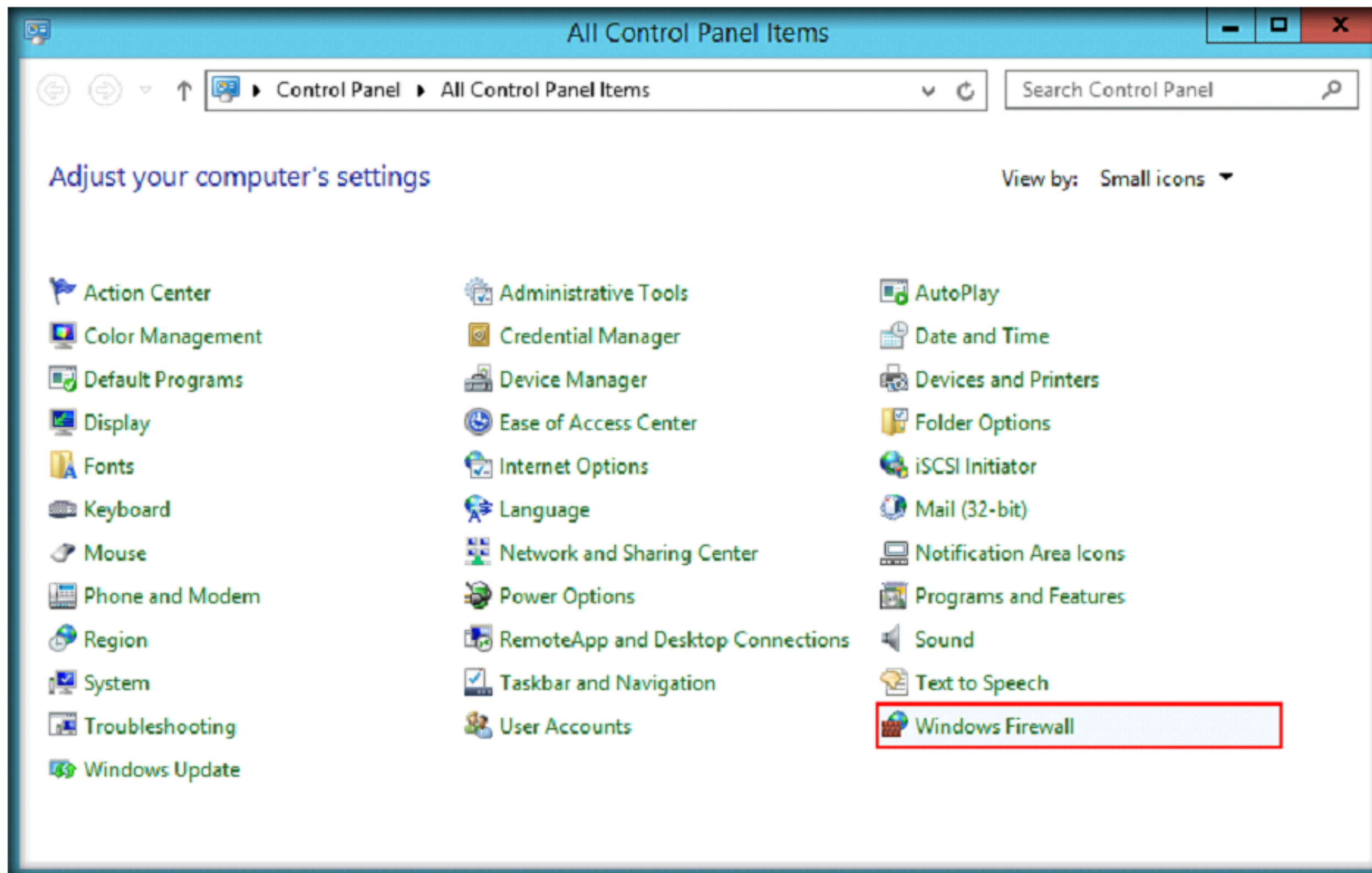
3. **Start** screen appears, click **Control Panel** icon



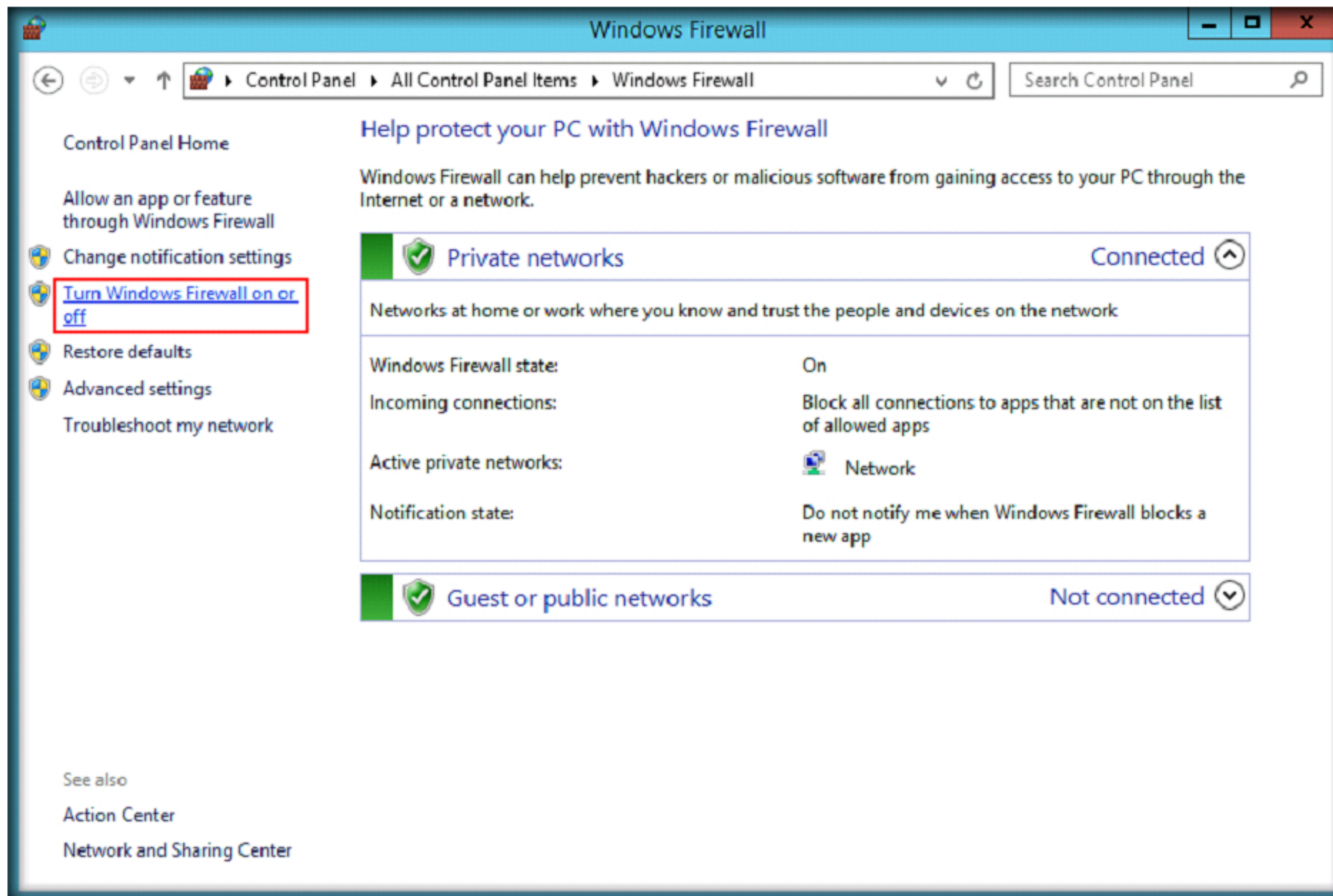
4. Control Panel appears on the screen, select **Small icons** from the **Category** drop down list to see all the control panel options



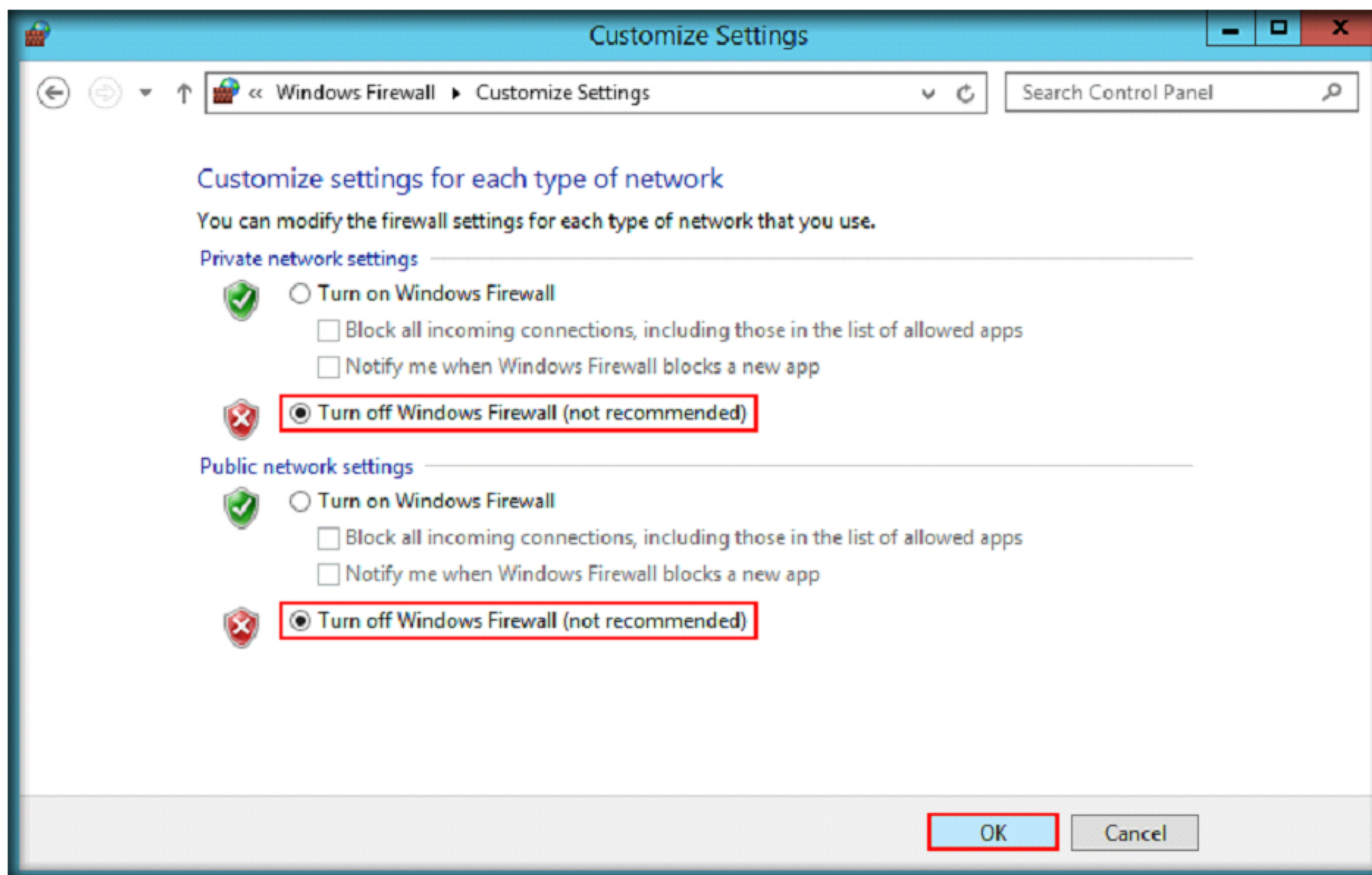
5. **All Control Panel Items** Window, click **Windows Firewall**



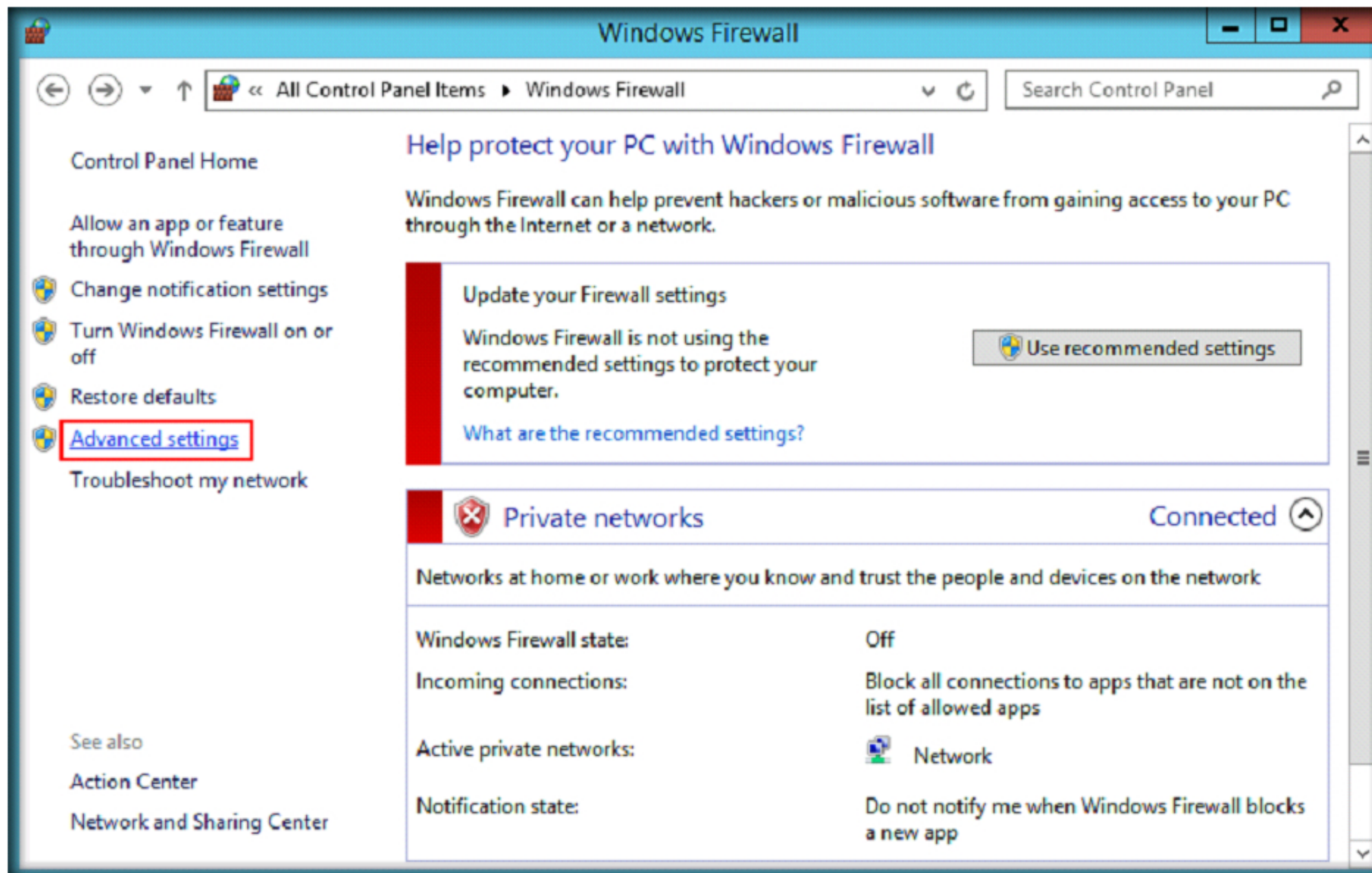
6. **Windows Firewall** control panel appears on the screen, click **Turn Windows Firewall on or off** link in the left pane of the window



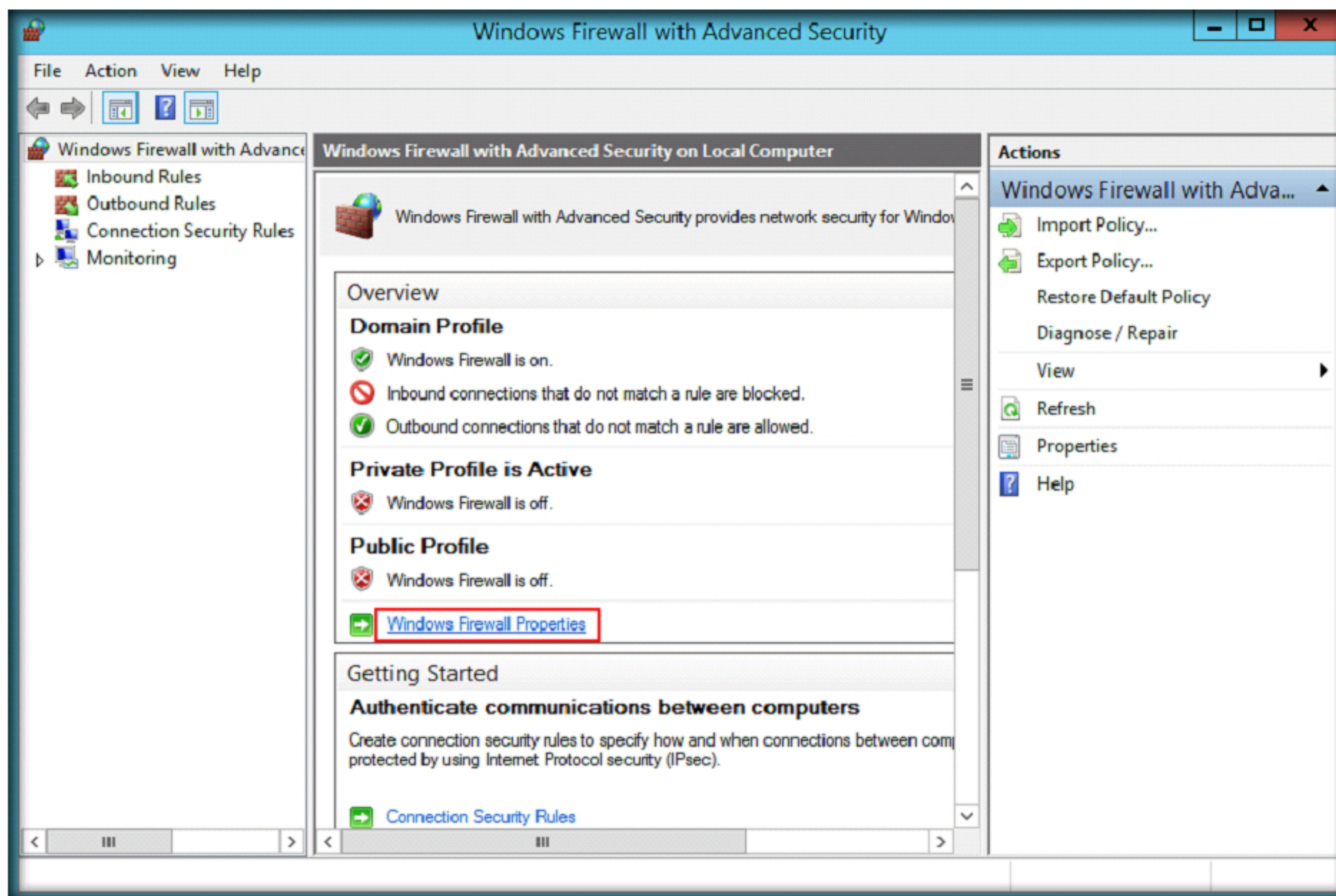
7. In **Customize Settings** window, select the radio button **Turn off Windows Firewall (not recommended)** for both Private and Public network settings and click **OK**



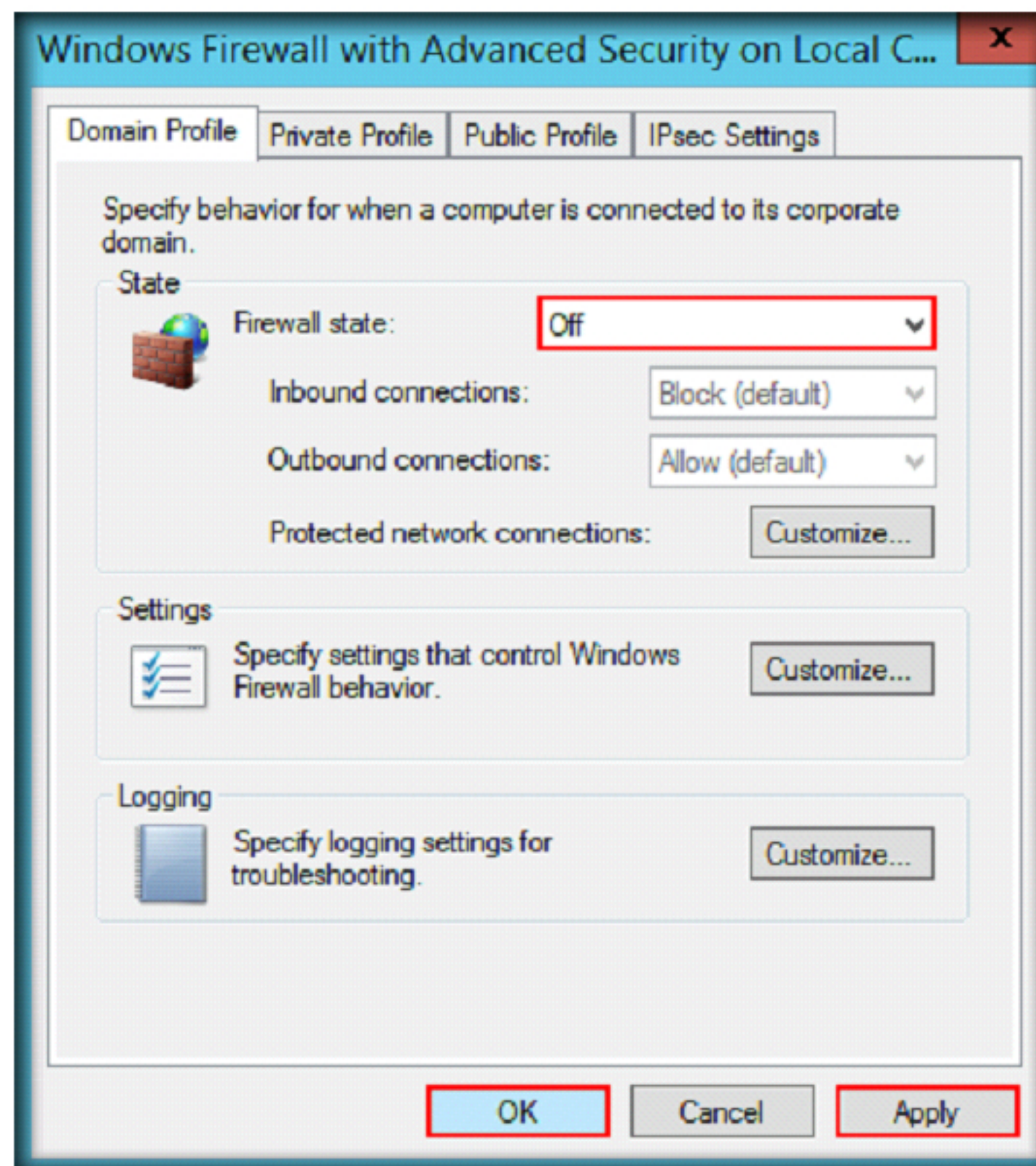
8. In the Windows Firewall control panel, click **Advanced settings** link in the left pane.



9. A window named **Windows Firewall with Advanced Security** appears on the screen, click **Windows Firewall Properties** link in the Overview section



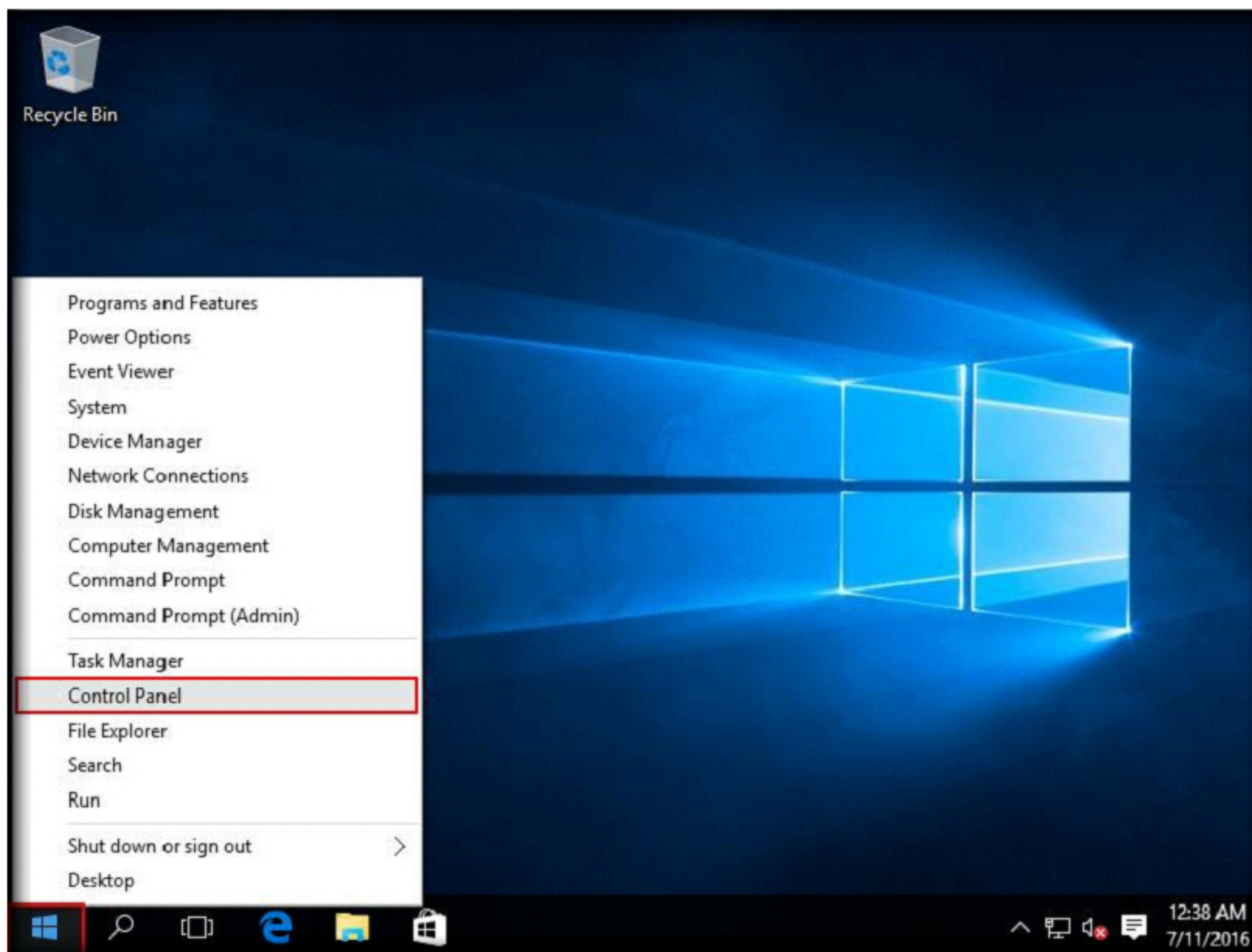
10. **Windows Firewall with Advanced Security on Local Computer** window appears, choose **Off** from the **Firewall state** drop-down list, click **Apply** and then click **OK**



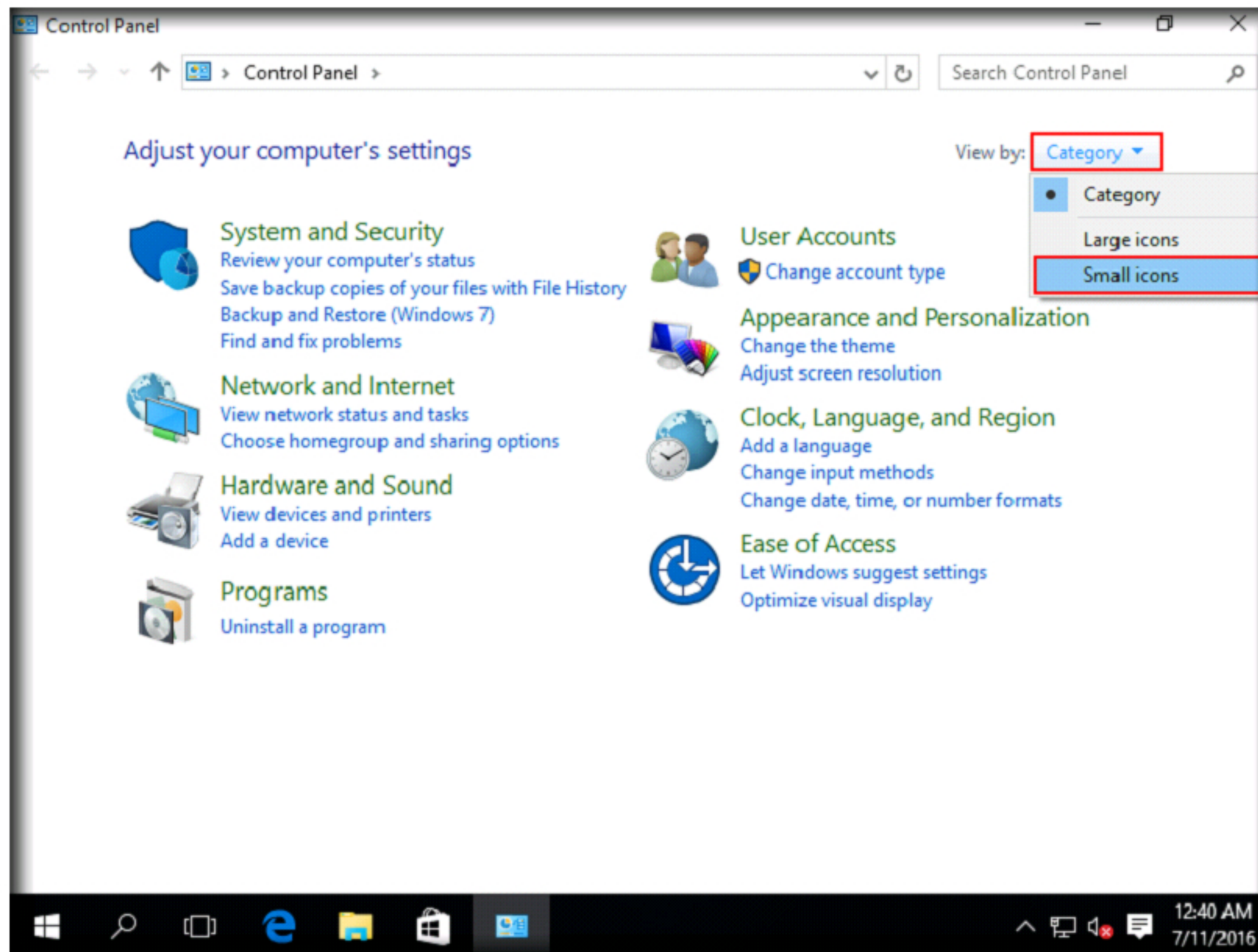
11. Ensure that Firewall state under **Private Profile** tab is also turned off.
12. **Close** all the windows

Windows 10 Virtual Machine

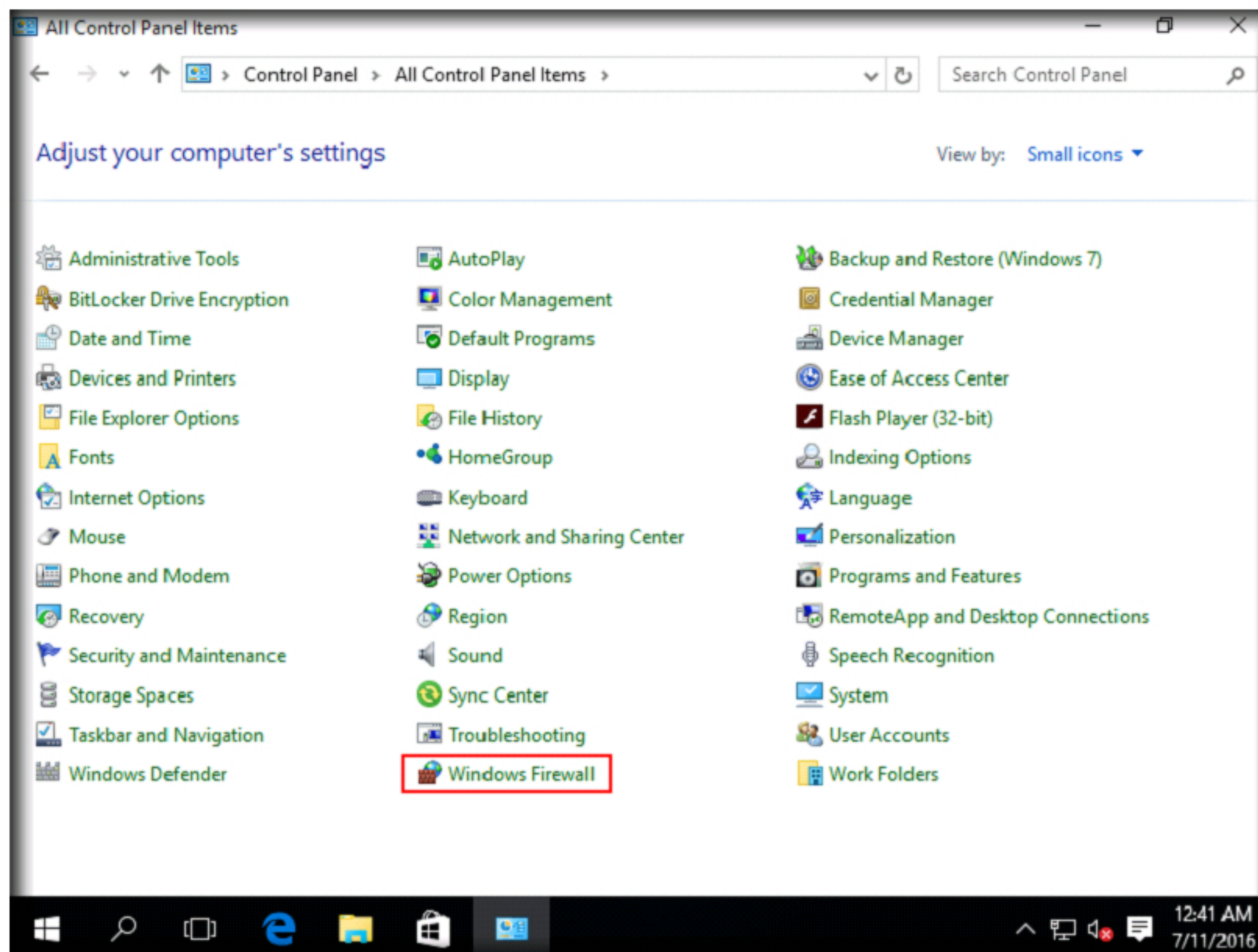
1. Logon to Windows 10 virtual machine
2. Right-click **Start** menu icon at the lower left corner of the screen and click **Control Panel**



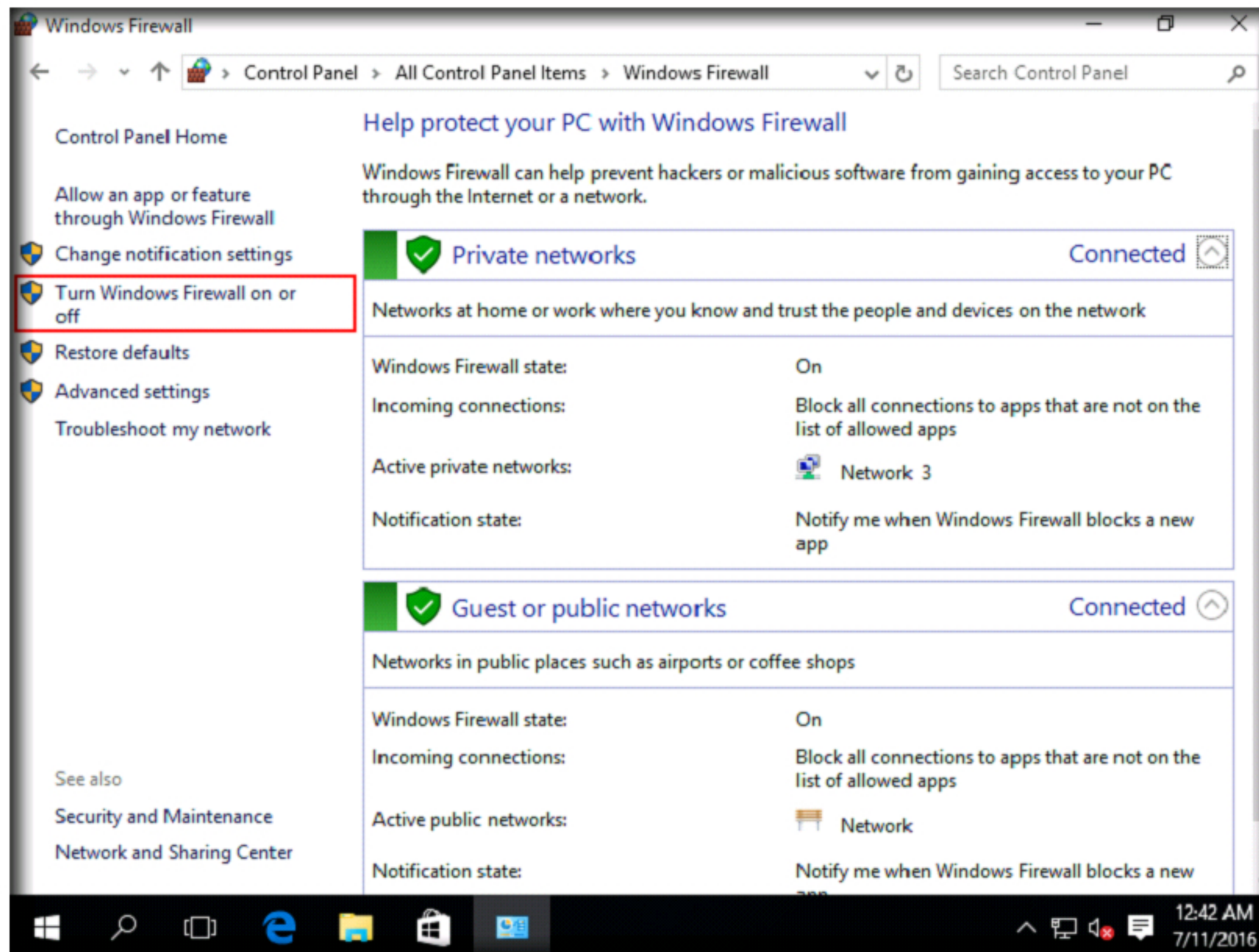
3. Control Panel appears on the screen, select **Small icons** from the **Category** drop down list to see all the control panel options



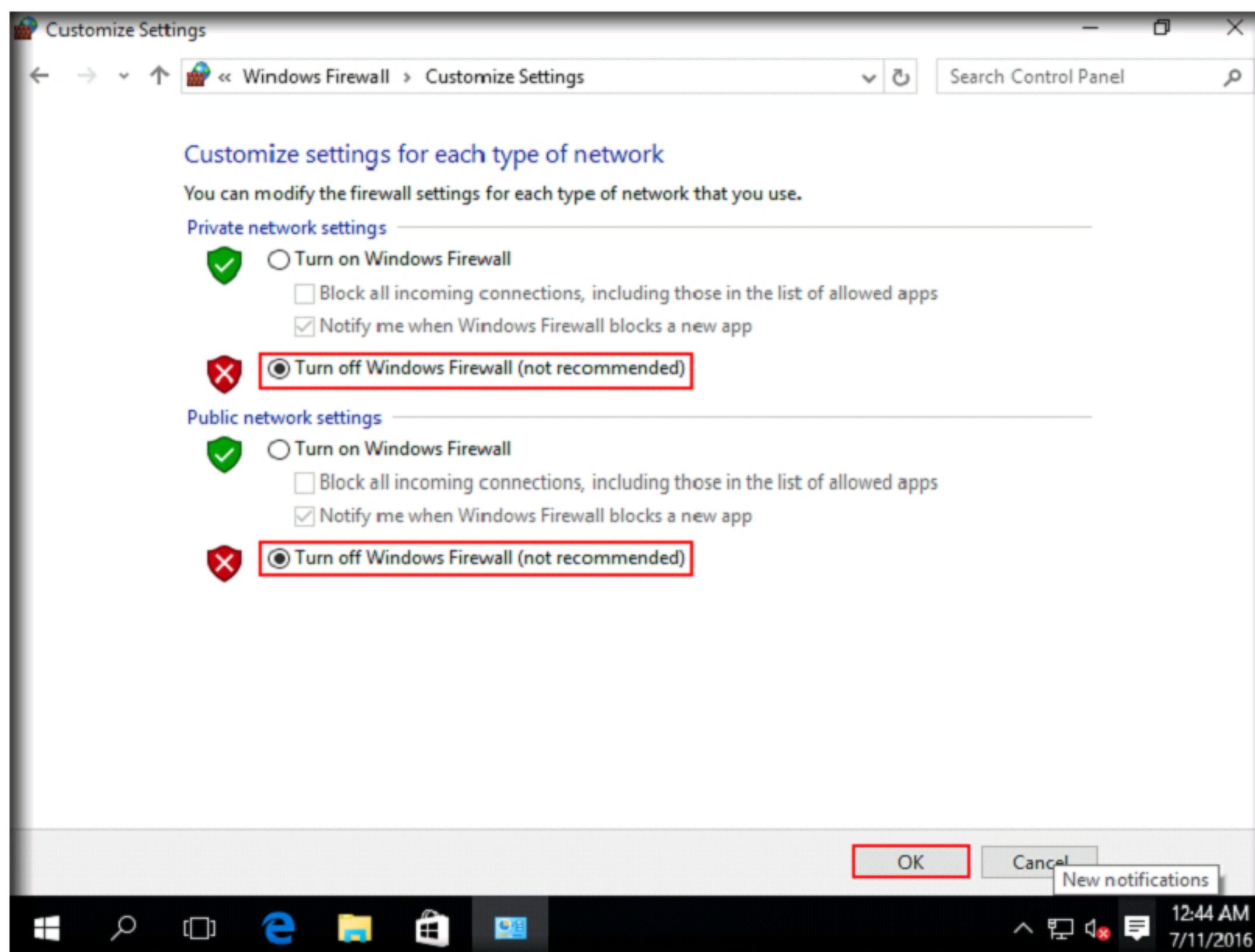
4. **All Control Panel Items** window appears, click **Windows Firewall**



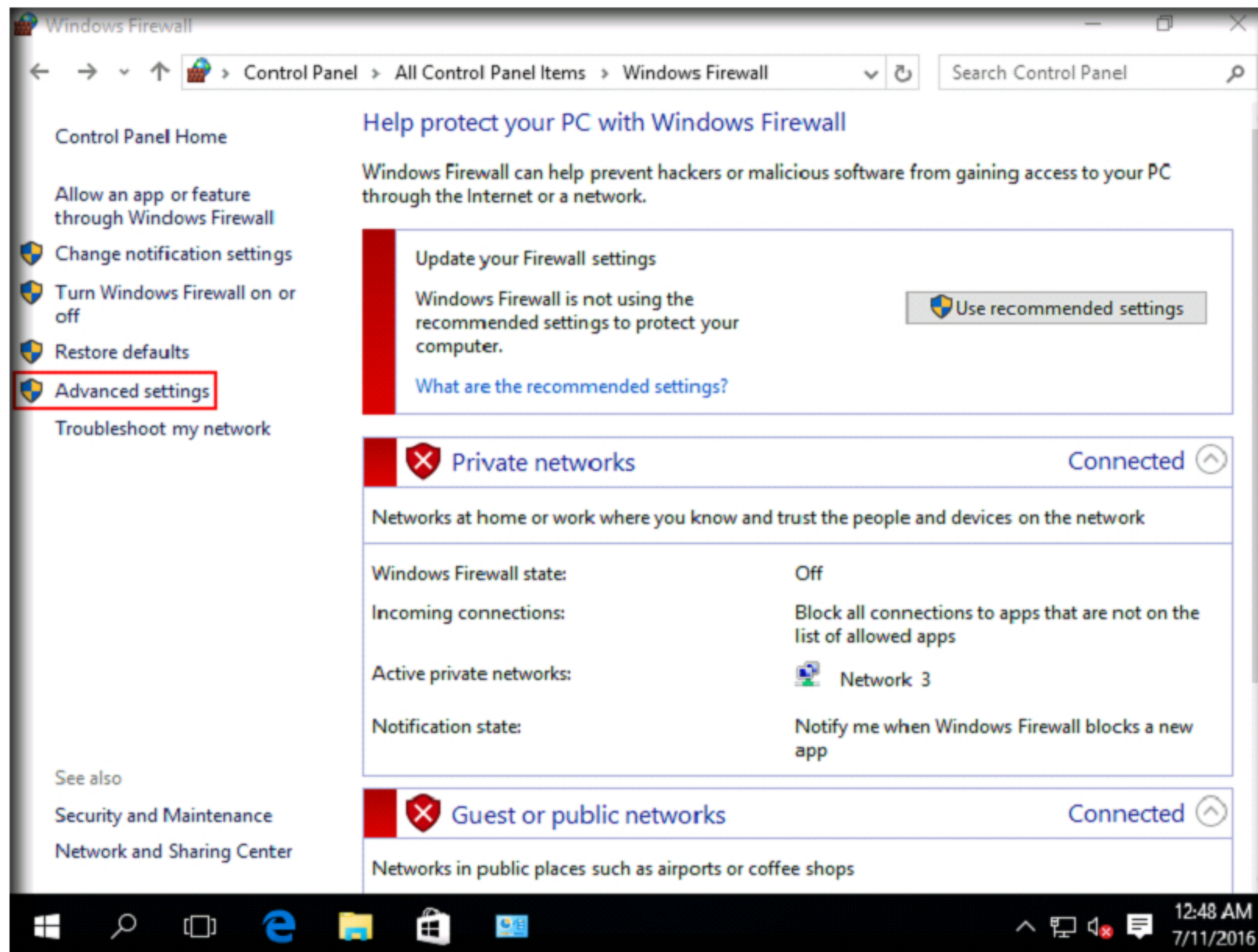
5. In **Windows Firewall** window, click **Turn Windows Firewall on or off** in the left pane of the window



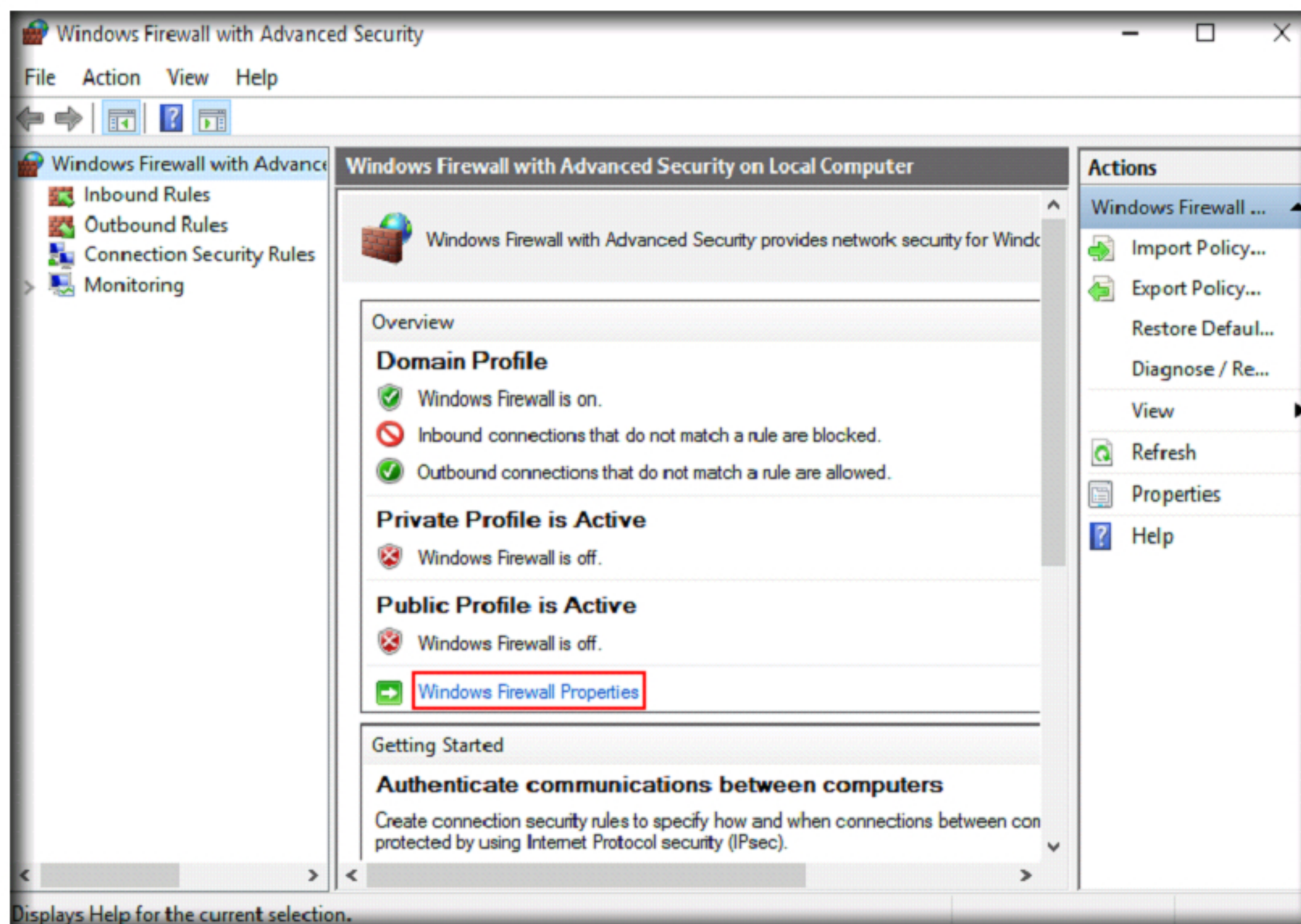
6. In **Customize Settings** window, select **Turn off Windows Firewall (not recommended)** radio button for both Private and Public network settings and click **OK**



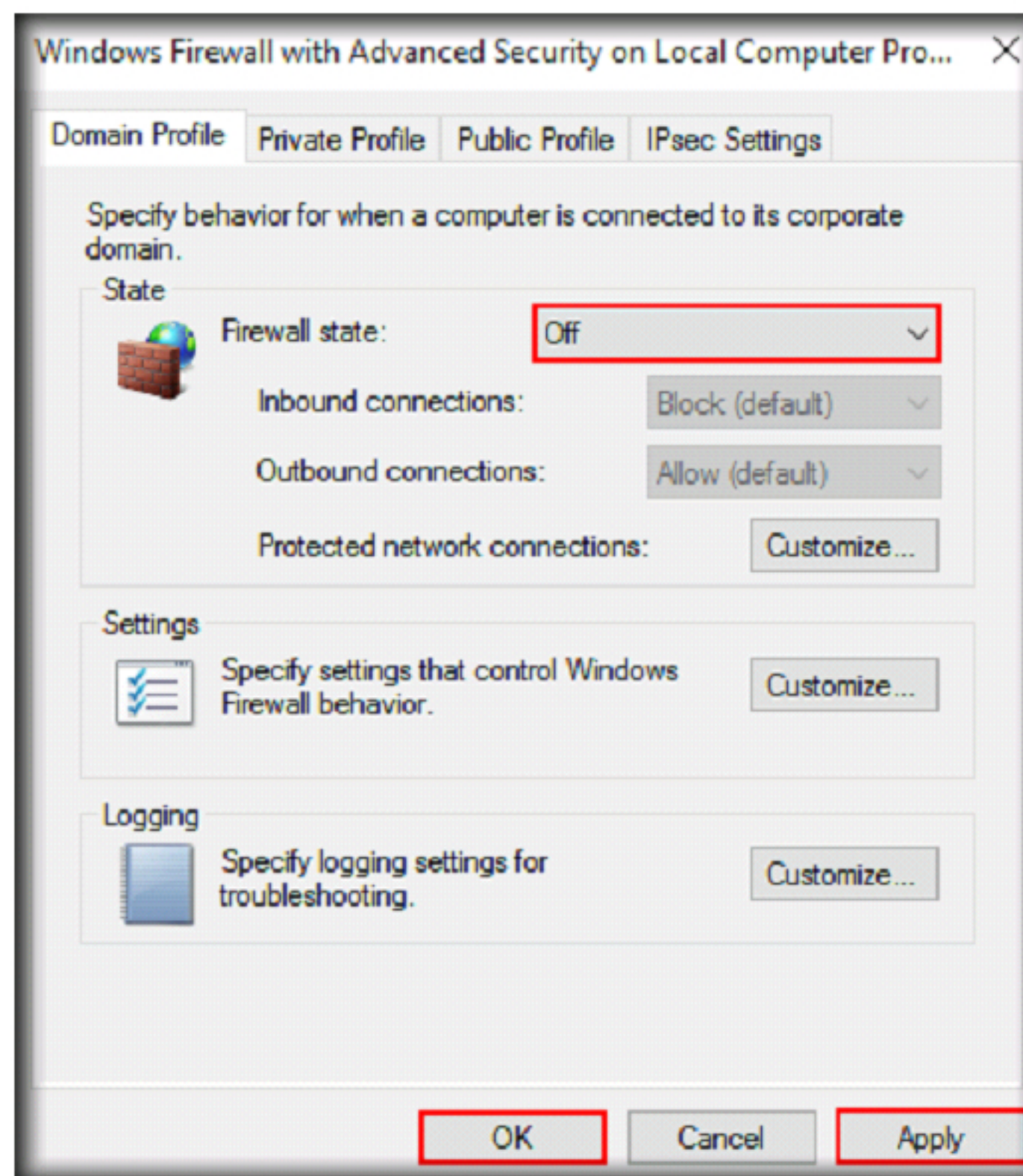
7. In the Windows Firewall control panel, click **Advanced settings** link in the left pane.



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



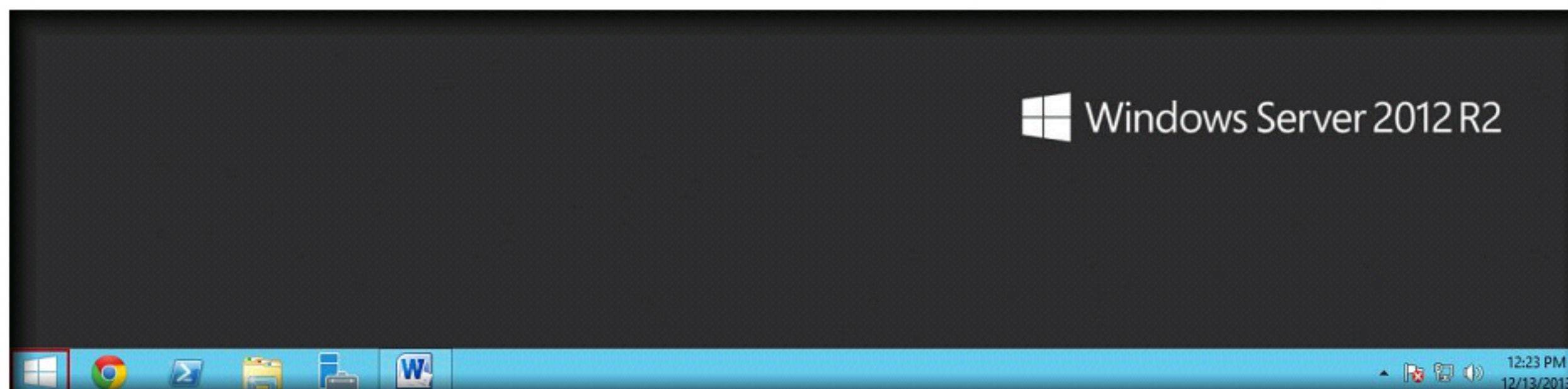
9. **Windows Firewall with Advanced Security on Local Computer** window appears, choose **Off** from the **Firewall state** drop-down list, click **Apply** and then click **OK**



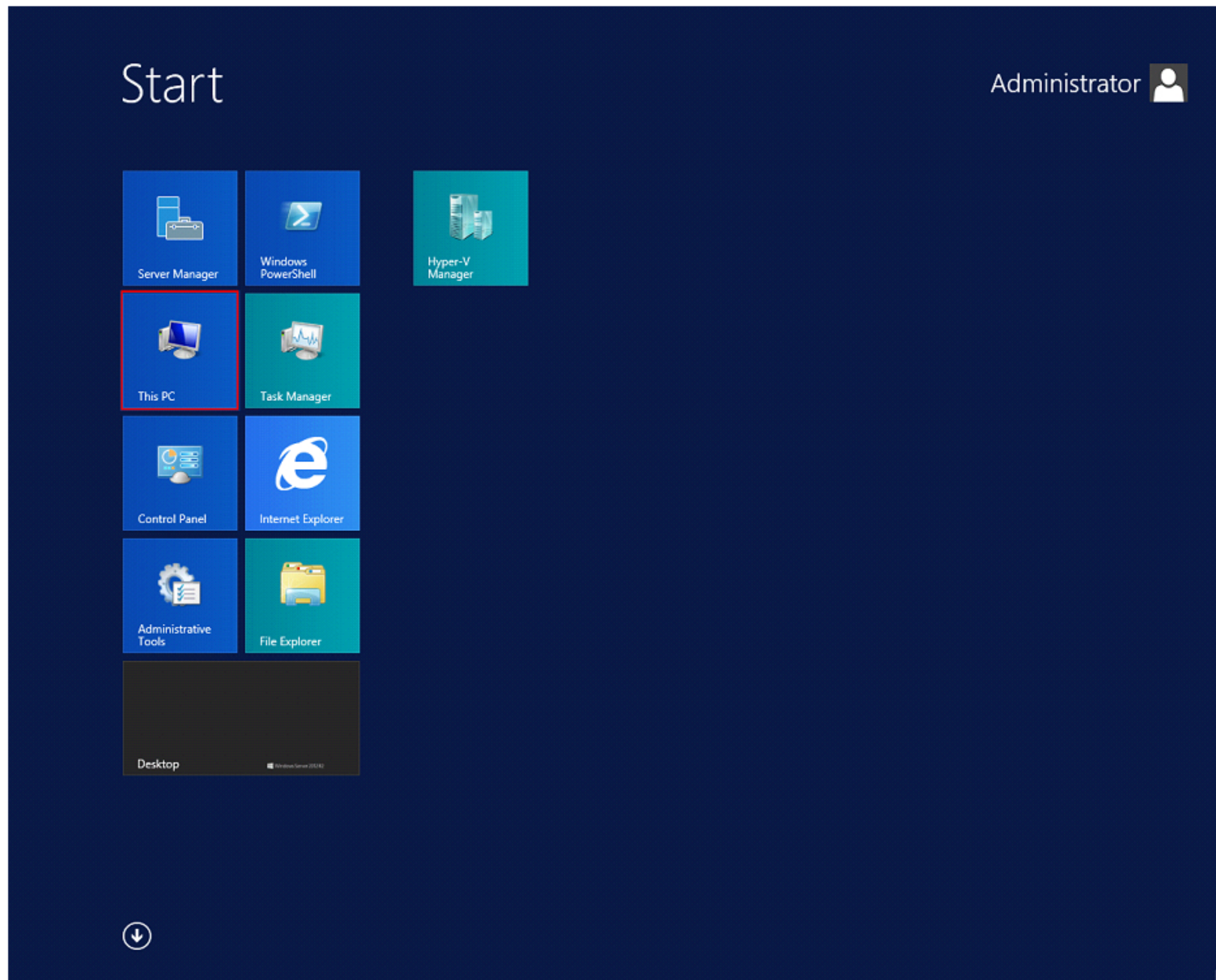
10. Ensure that Firewall state under **Private Profile** tab is also turned off
11. **Close** all the windows

CT#20: Share CHFI-Tools folder as 'Z:\' drive (Mapping Z:\ drive)

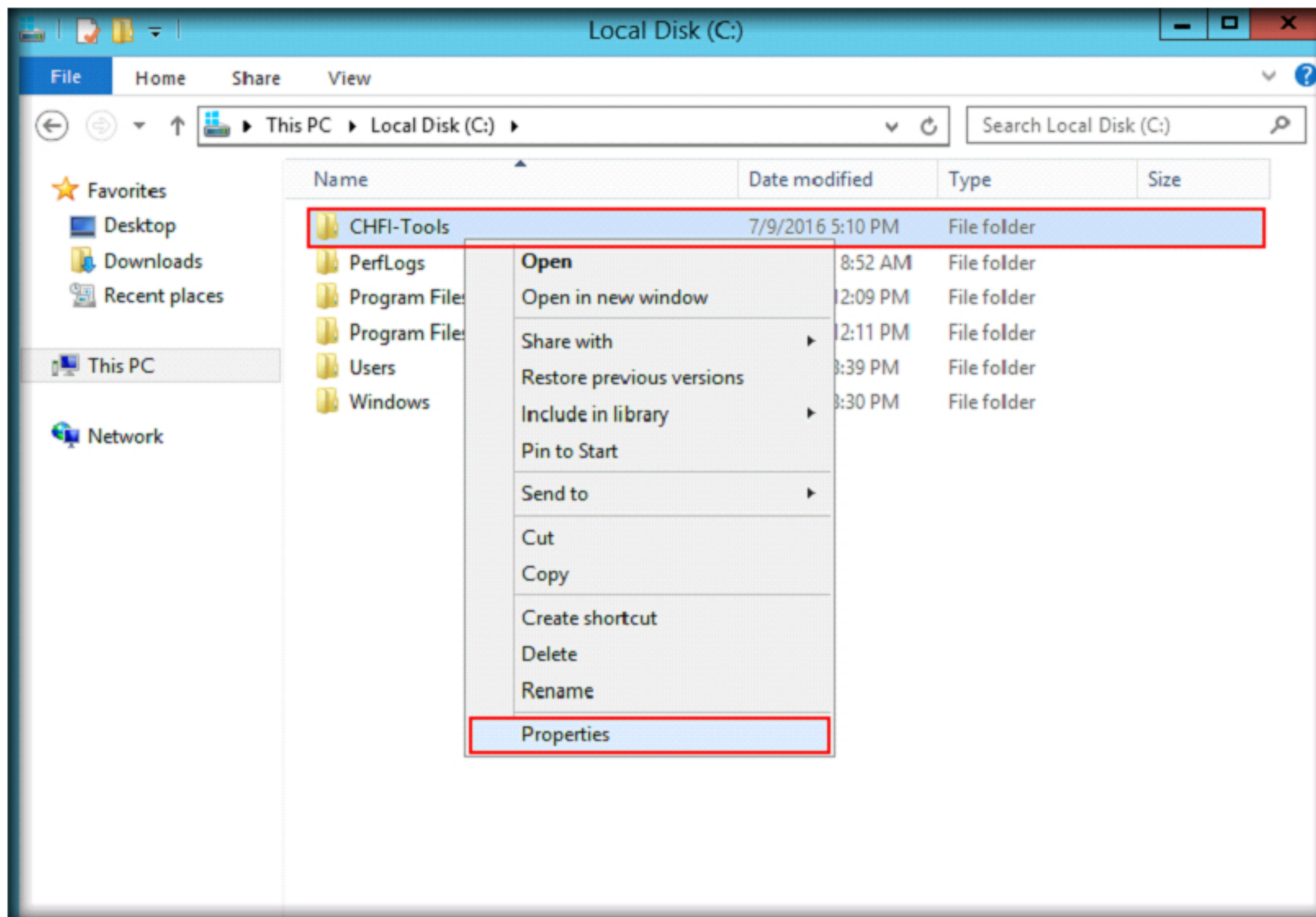
1. Click **Windows** icon at the lower left corner of the screen



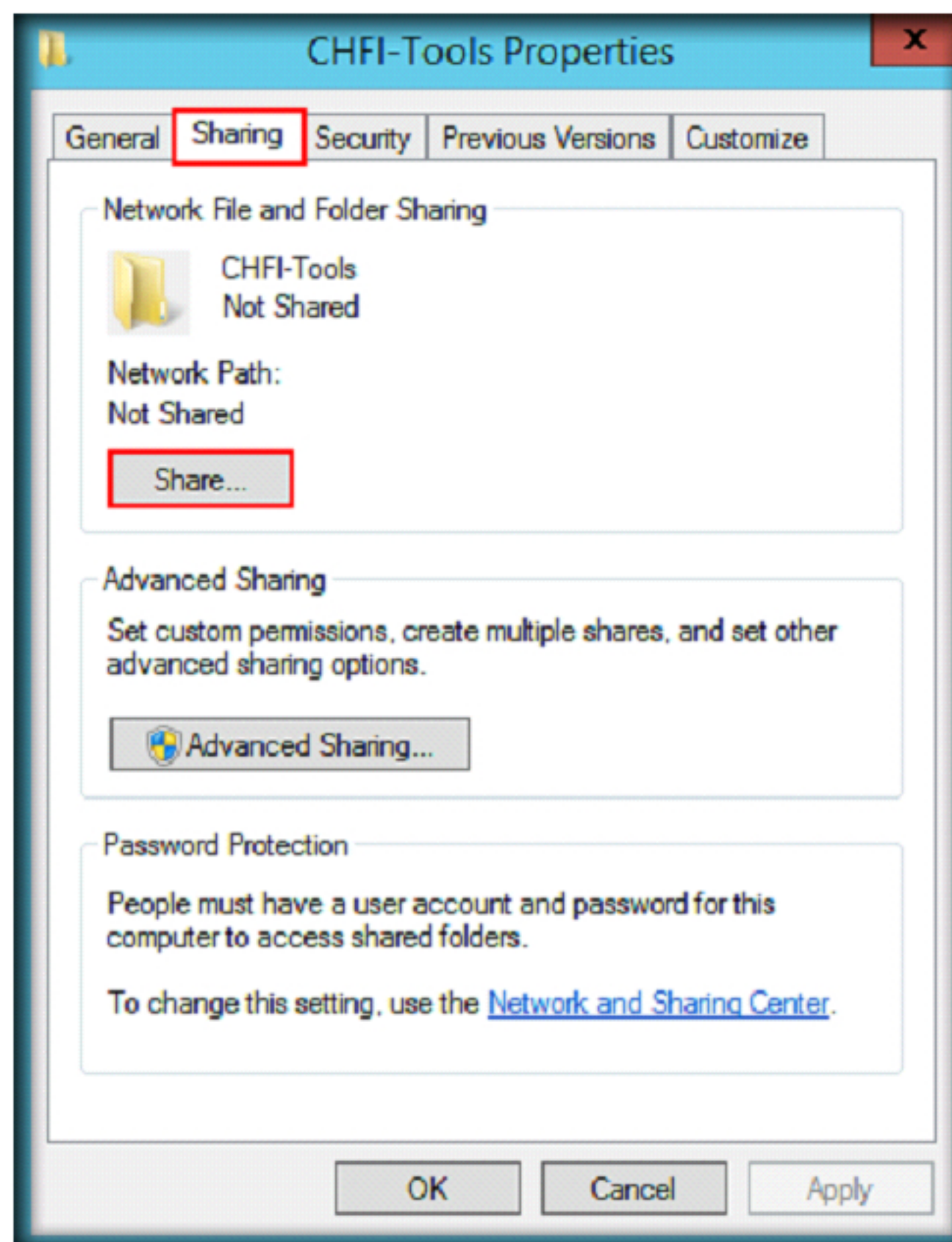
2. Click **This PC** icon in **Start** screen



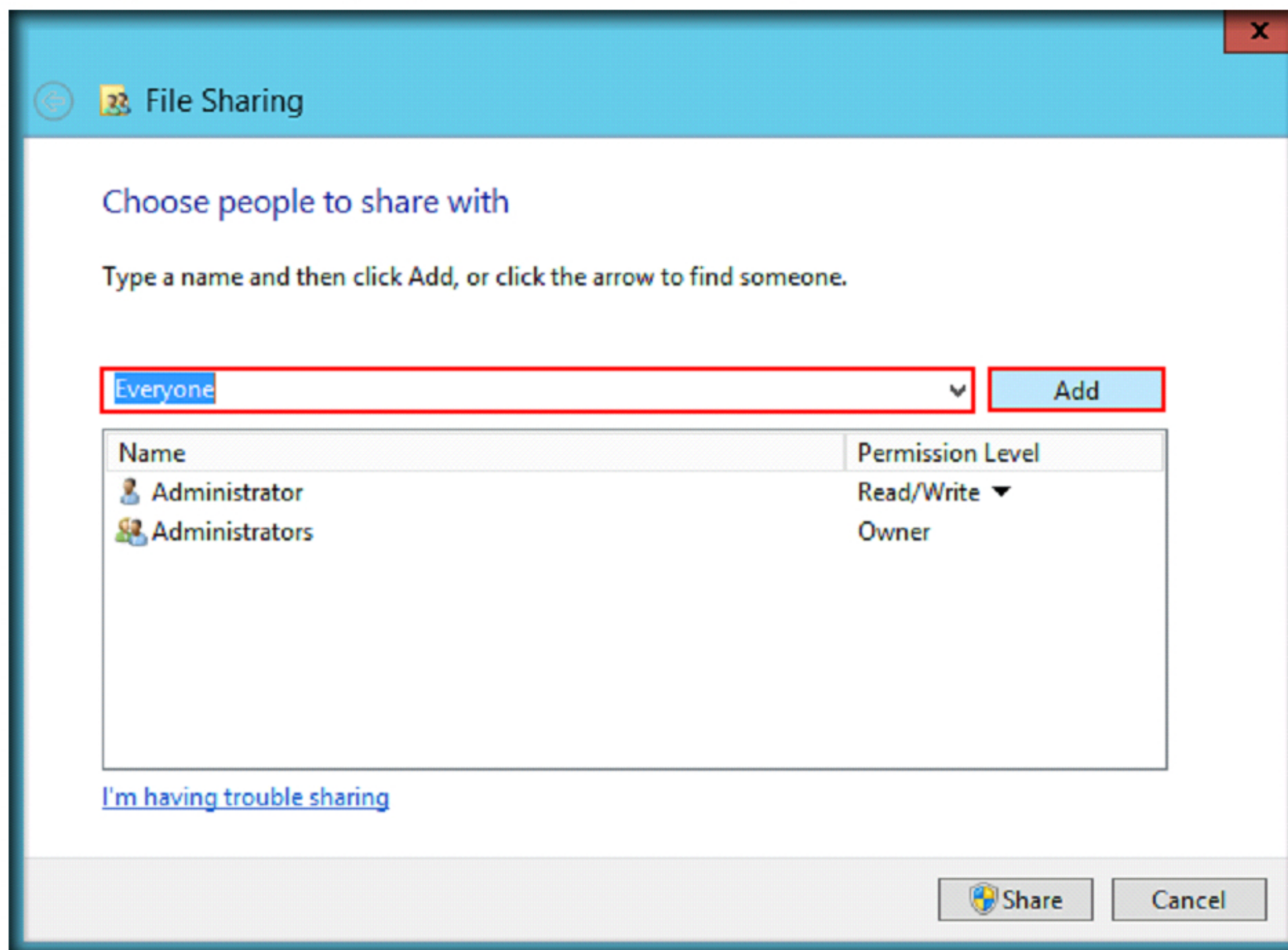
3. **This PC** screen appears, navigate to **C:**, right-click on **CHFI-Tools** folder and select **Properties** from the context menu



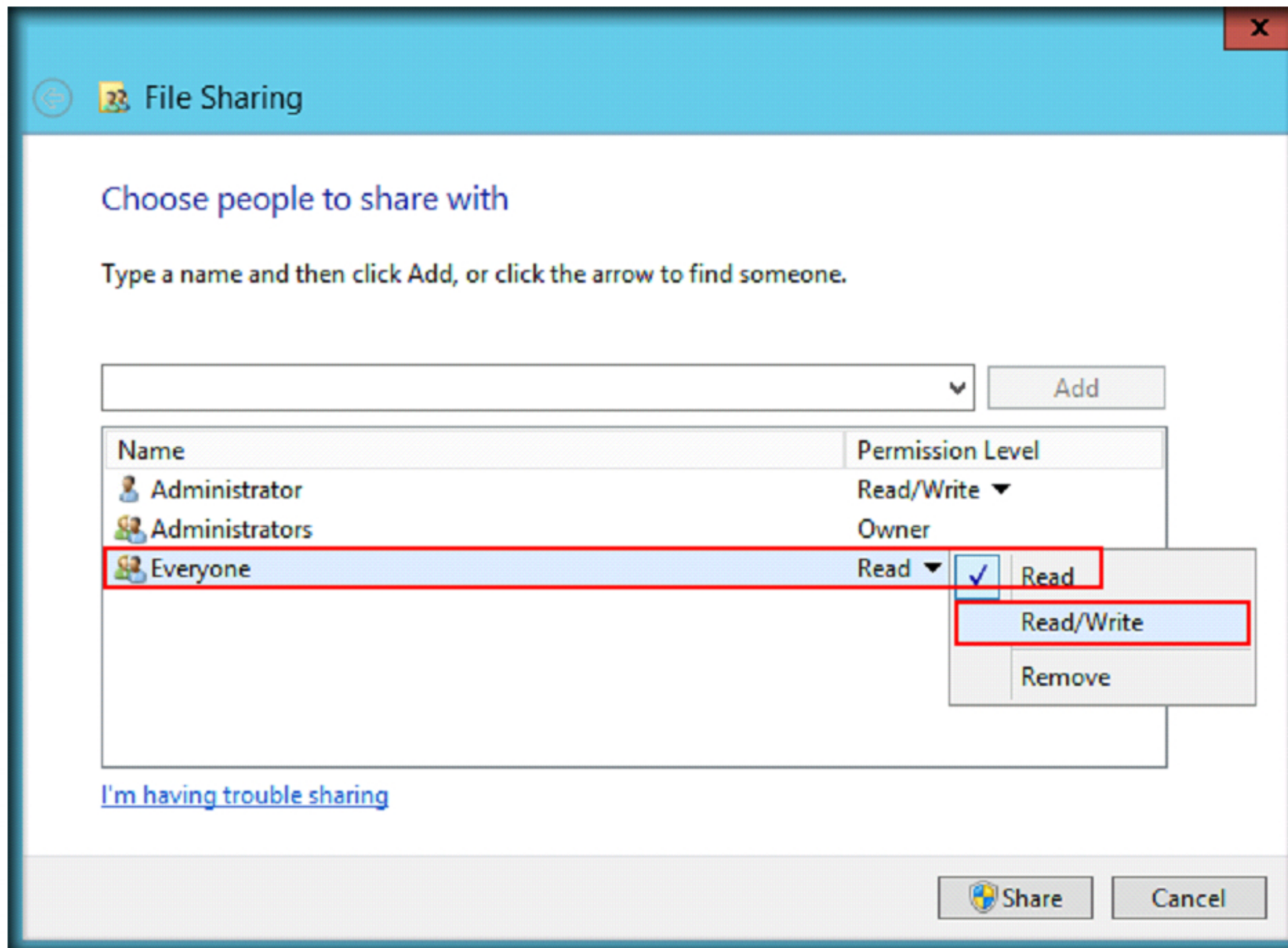
4. Select **Sharing** tab from the **CHFI-Tools Properties** window to modify and display current **shared folder settings**
5. Click **Share** button to access the File Sharing option



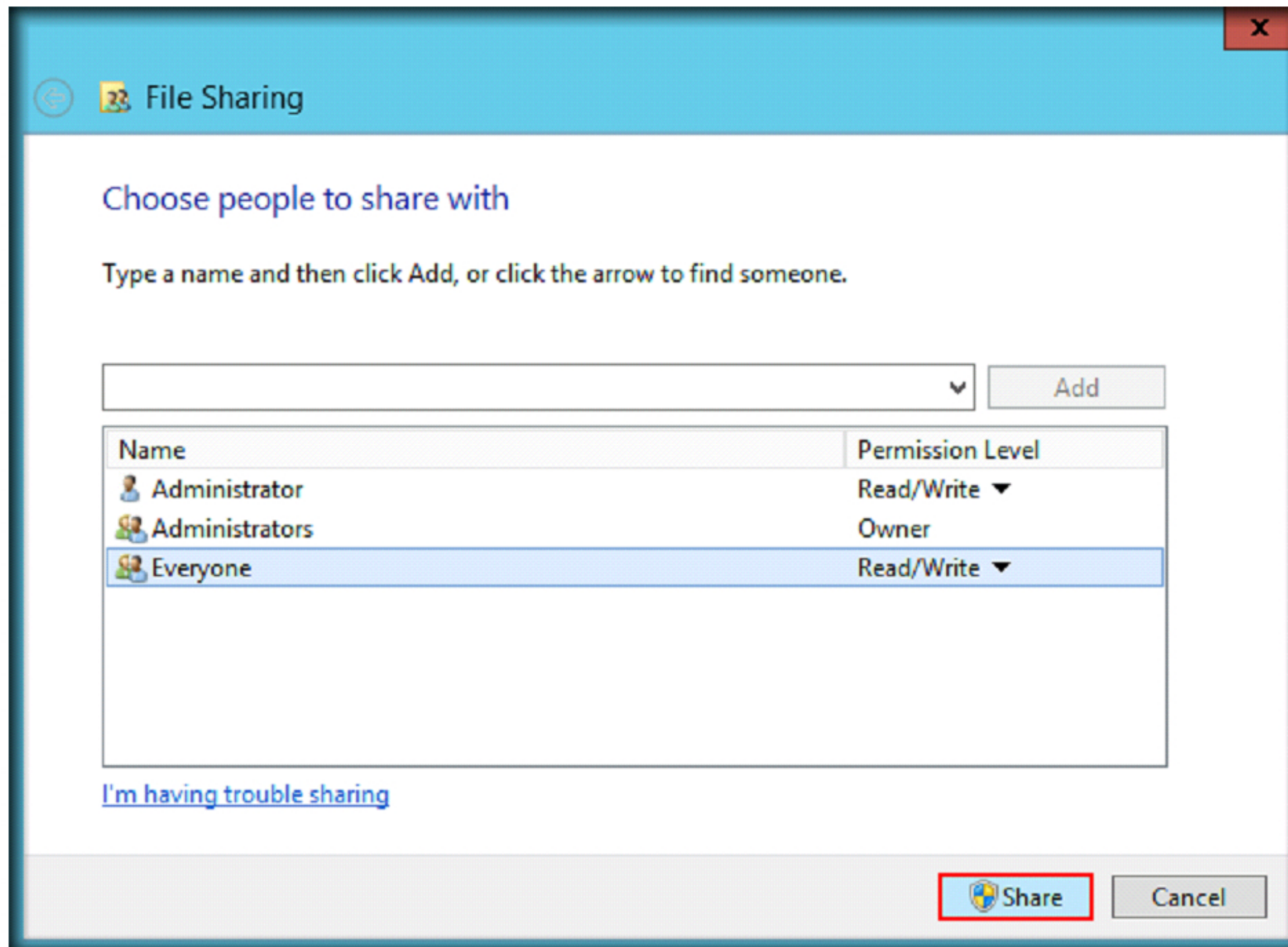
6. In File Sharing wizard, select **Everyone** (All Users in the list) from the drop down list and click **Add**



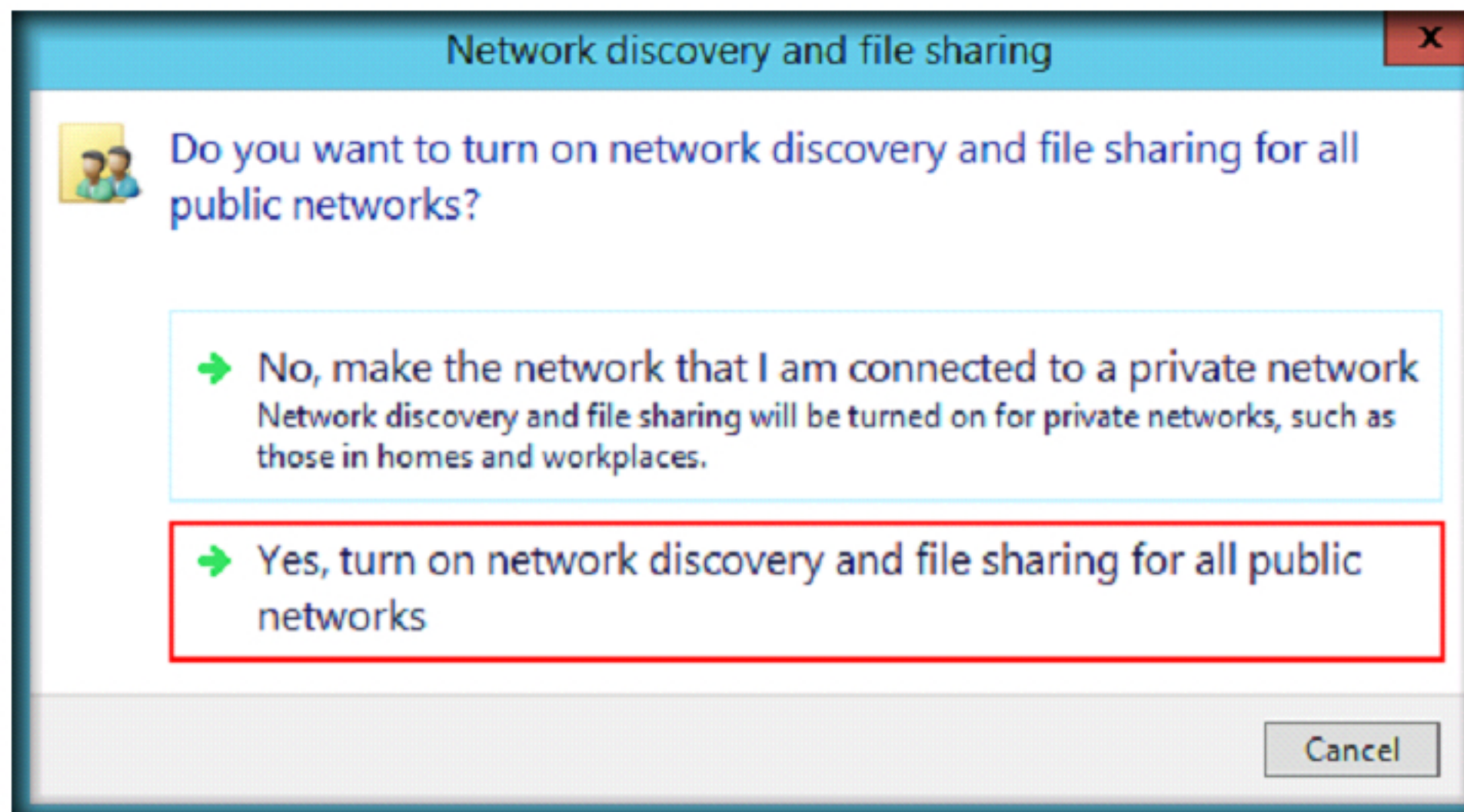
- In the newly added users (**Everyone**), click Read drop-down menu and click **Read/Write**



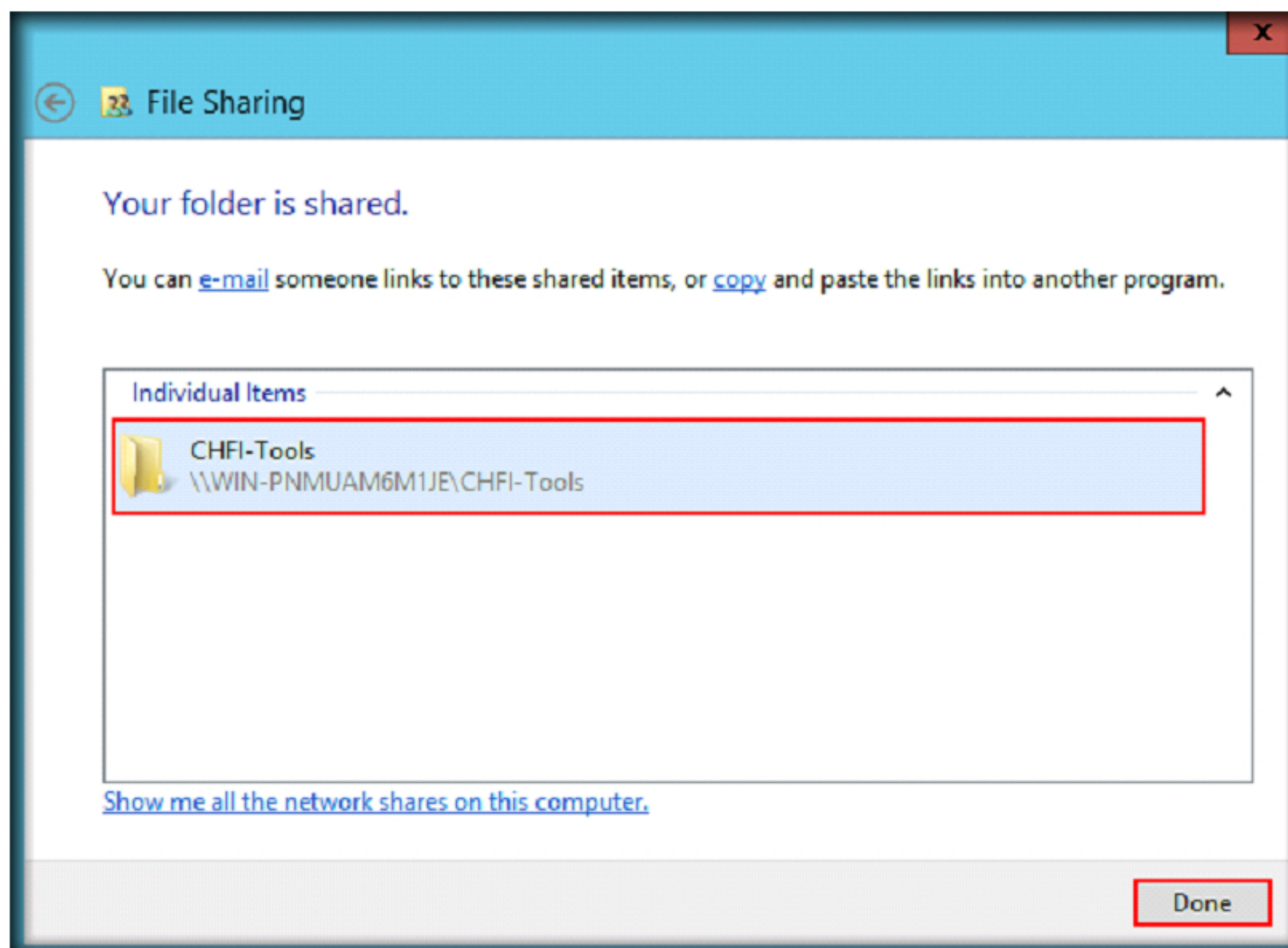
8. Click **Share** in order to begin sharing with the added users



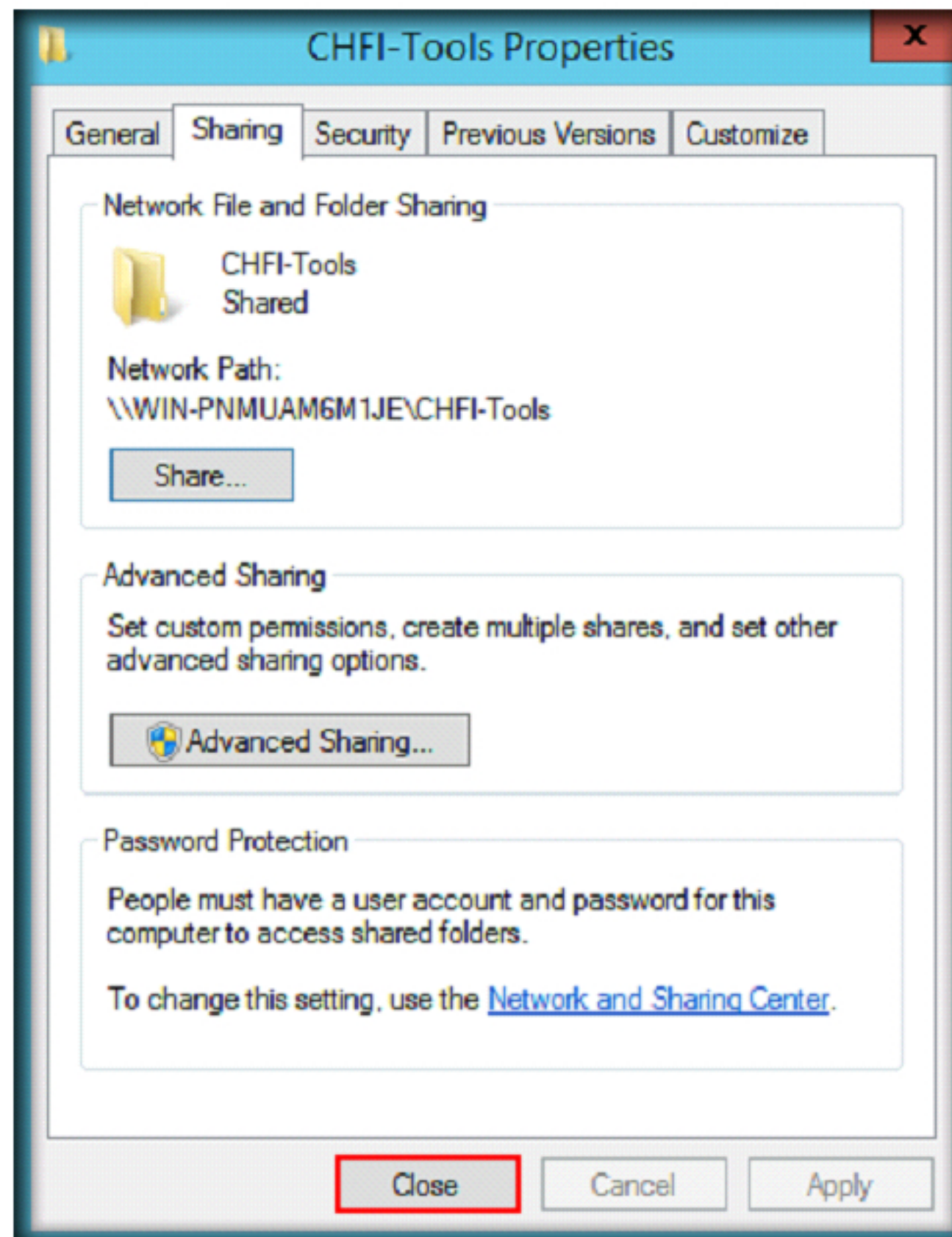
9. If a Network discovery and file sharing window appears, select **Yes, turn on network discovery and file sharing for all public networks**



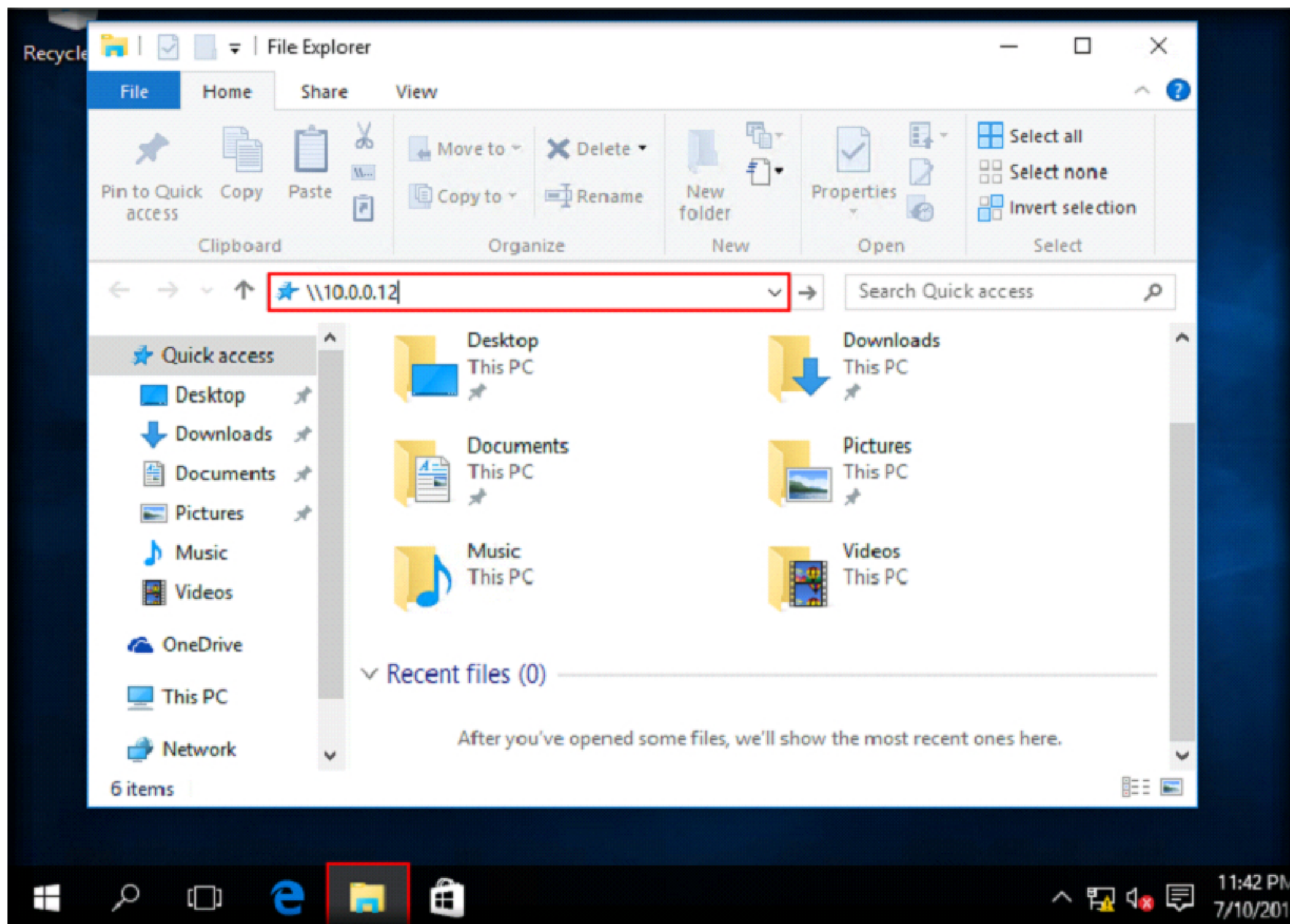
10. The shared **CHFI-Tools** folder appears under **Individual Items** section. Click **Done** to confirm the file sharing.



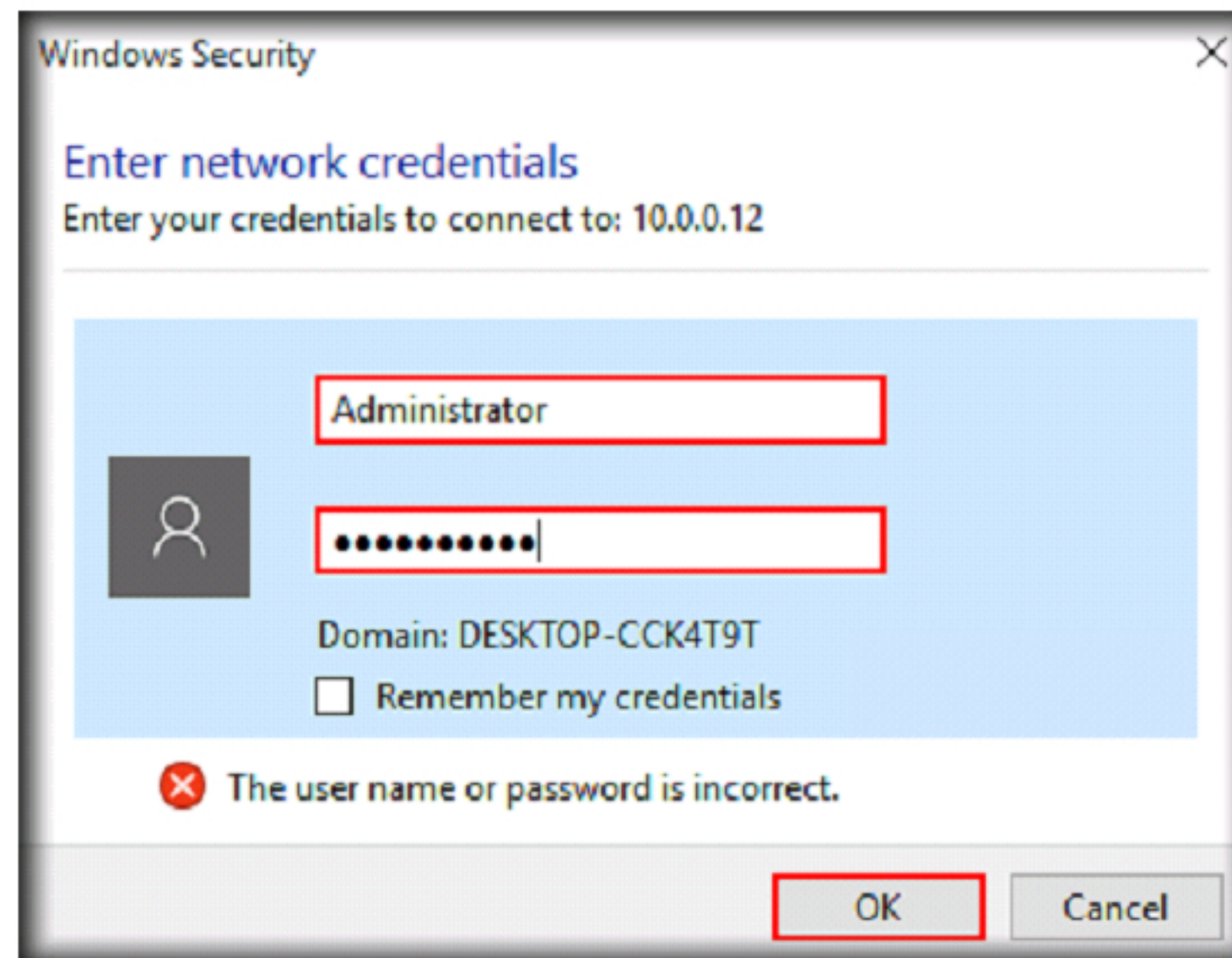
11. Close the **CHFI-Tools Properties** window



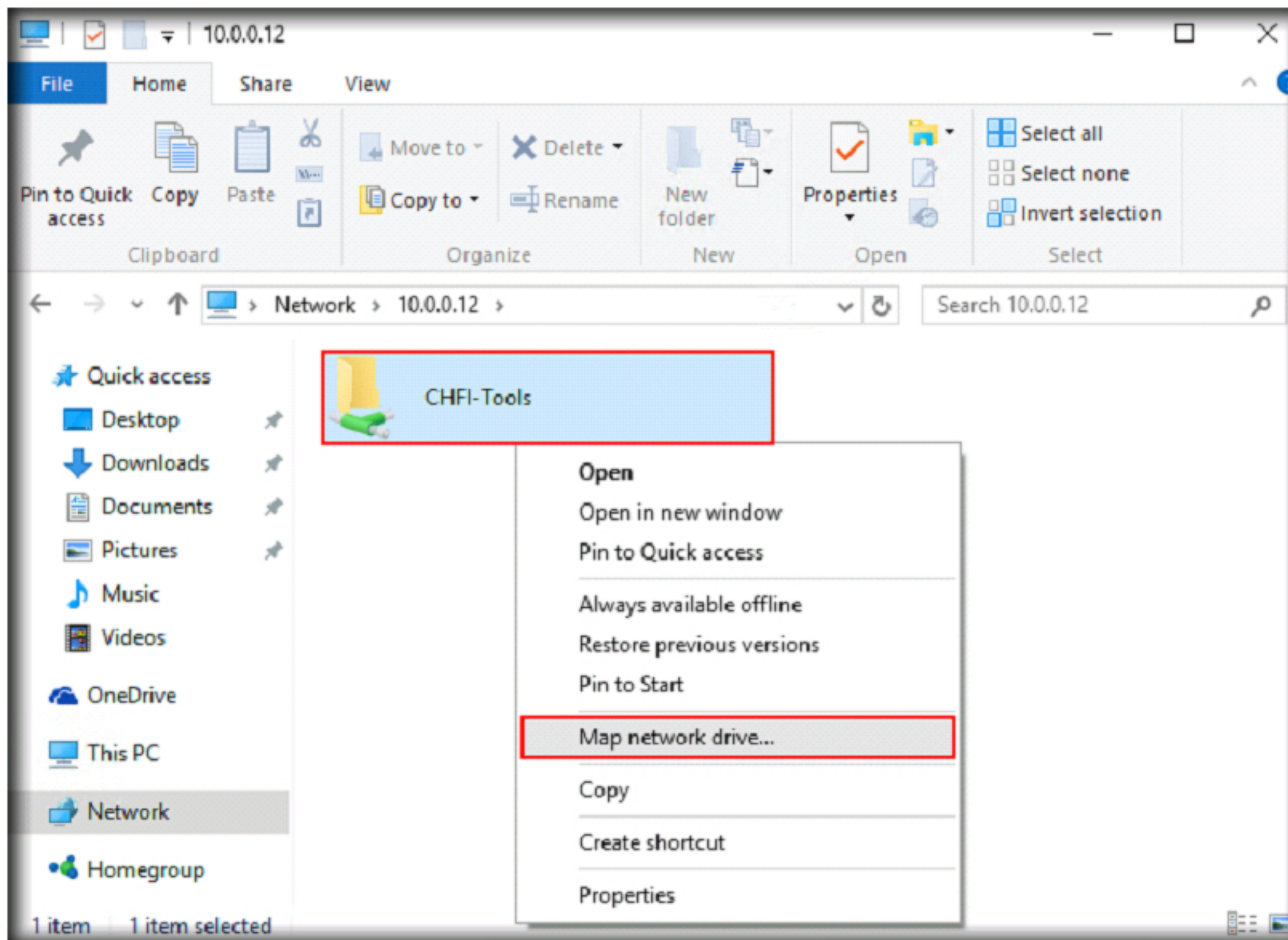
12. Now Login into **Windows 10** virtual machine from Hyper-V Manager
13. Click **File Explorer** from the Task bar
14. File explorer appears, type **//10.0.0.12** in the address bar and press **Enter**



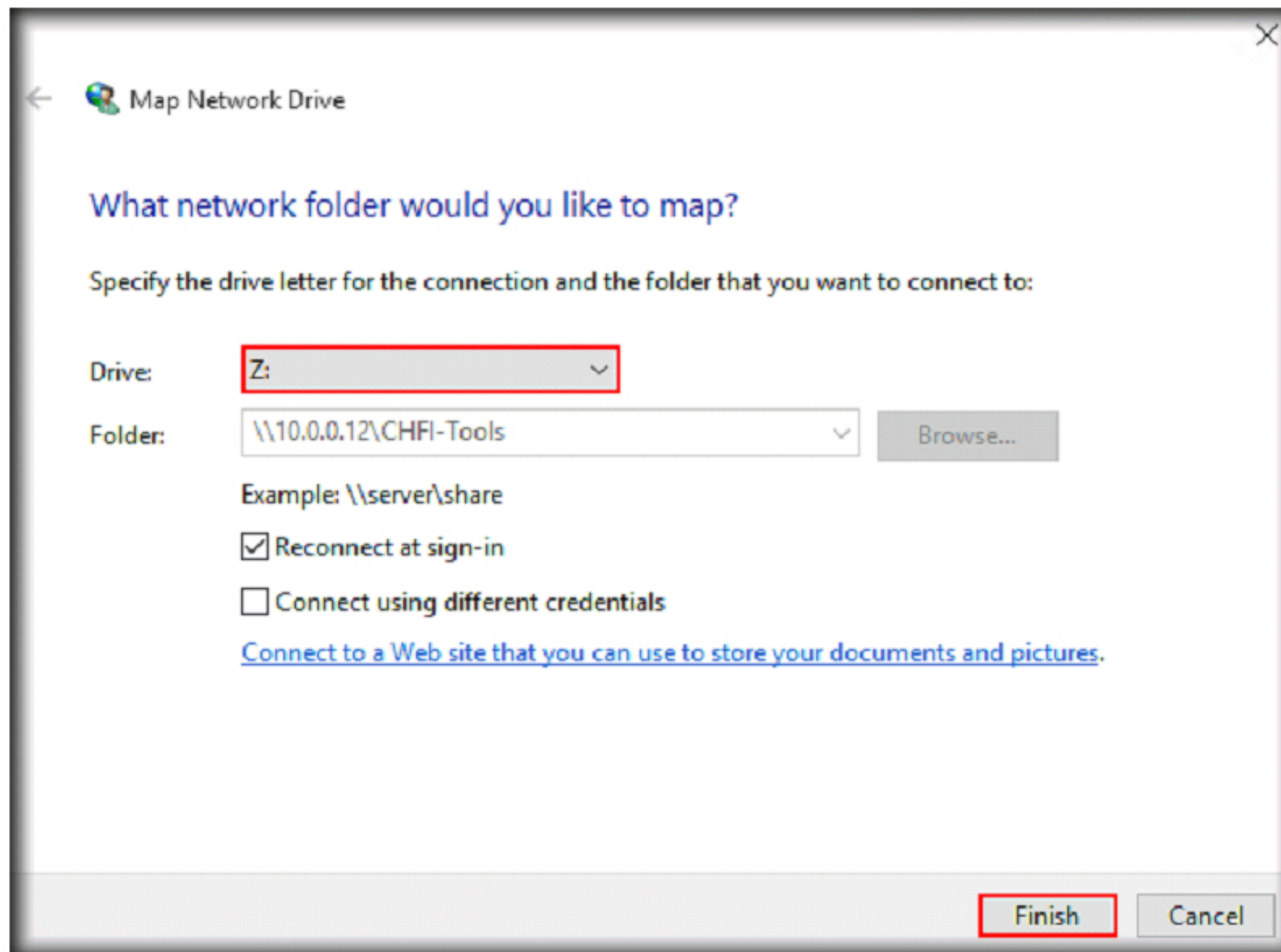
15. If a **Windows Security** dialog-box appears, enter the credentials of Windows Server 2012 virtual machine and click **OK**



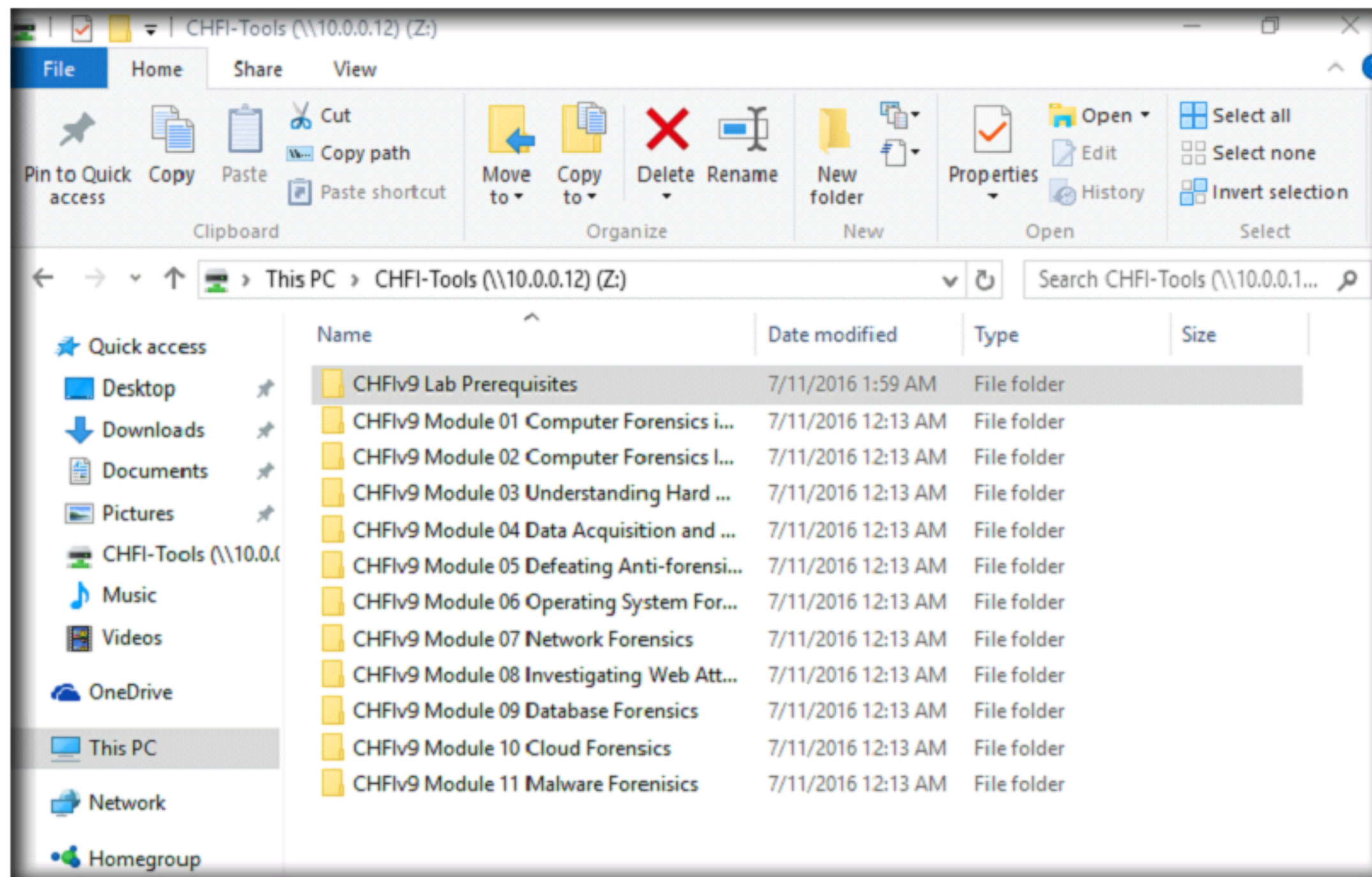
16. Now, the shared folder appears in the window. Right-click on the folder and select **Map network drive...** from the context menu.



17. Click **Finish** button to complete the Mapping of the **Z:** drive in **Map Network Drive** window

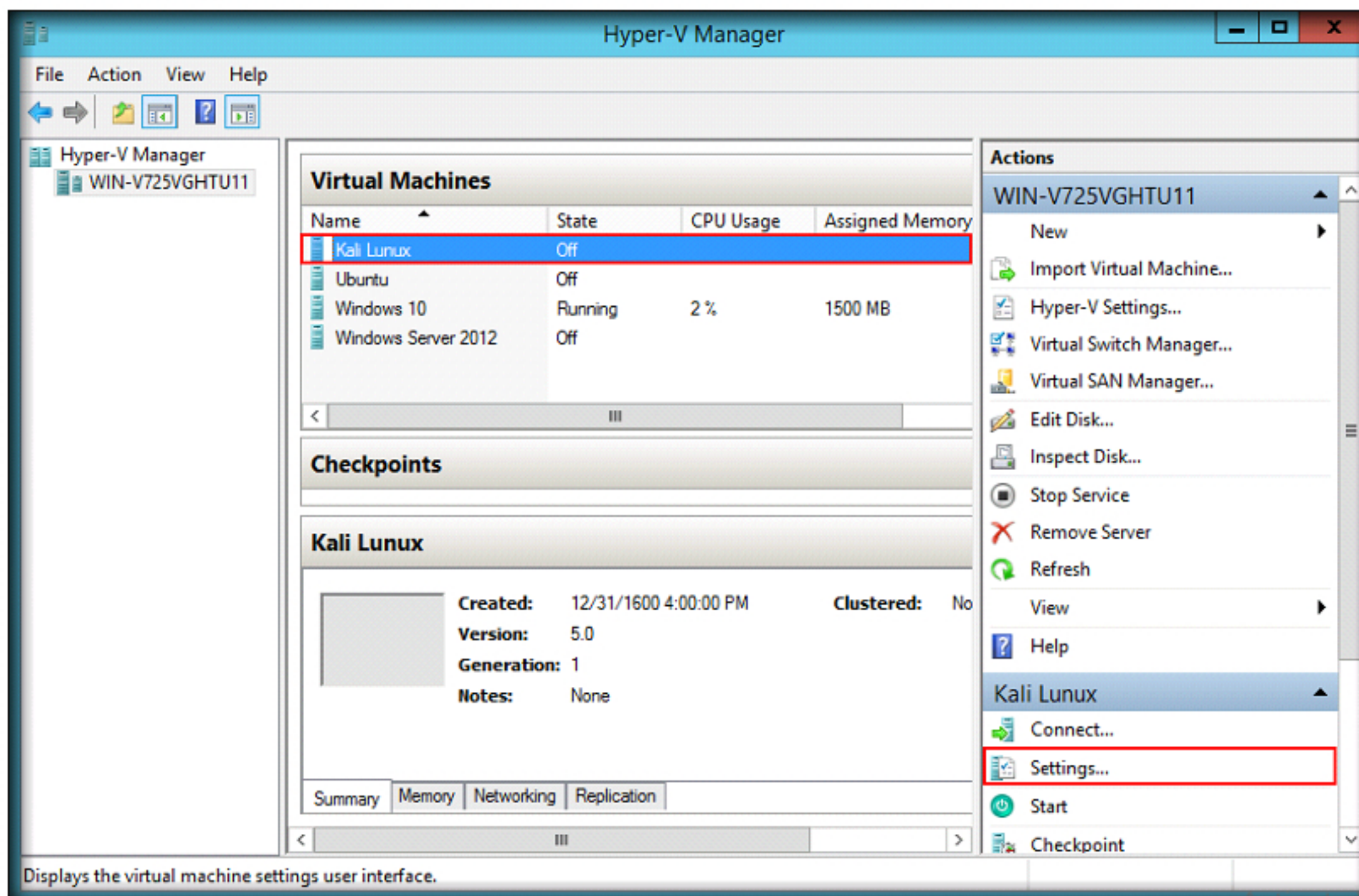


18. Once you click **Finish**, you will be redirected to the mapped network drive folder or shared folder

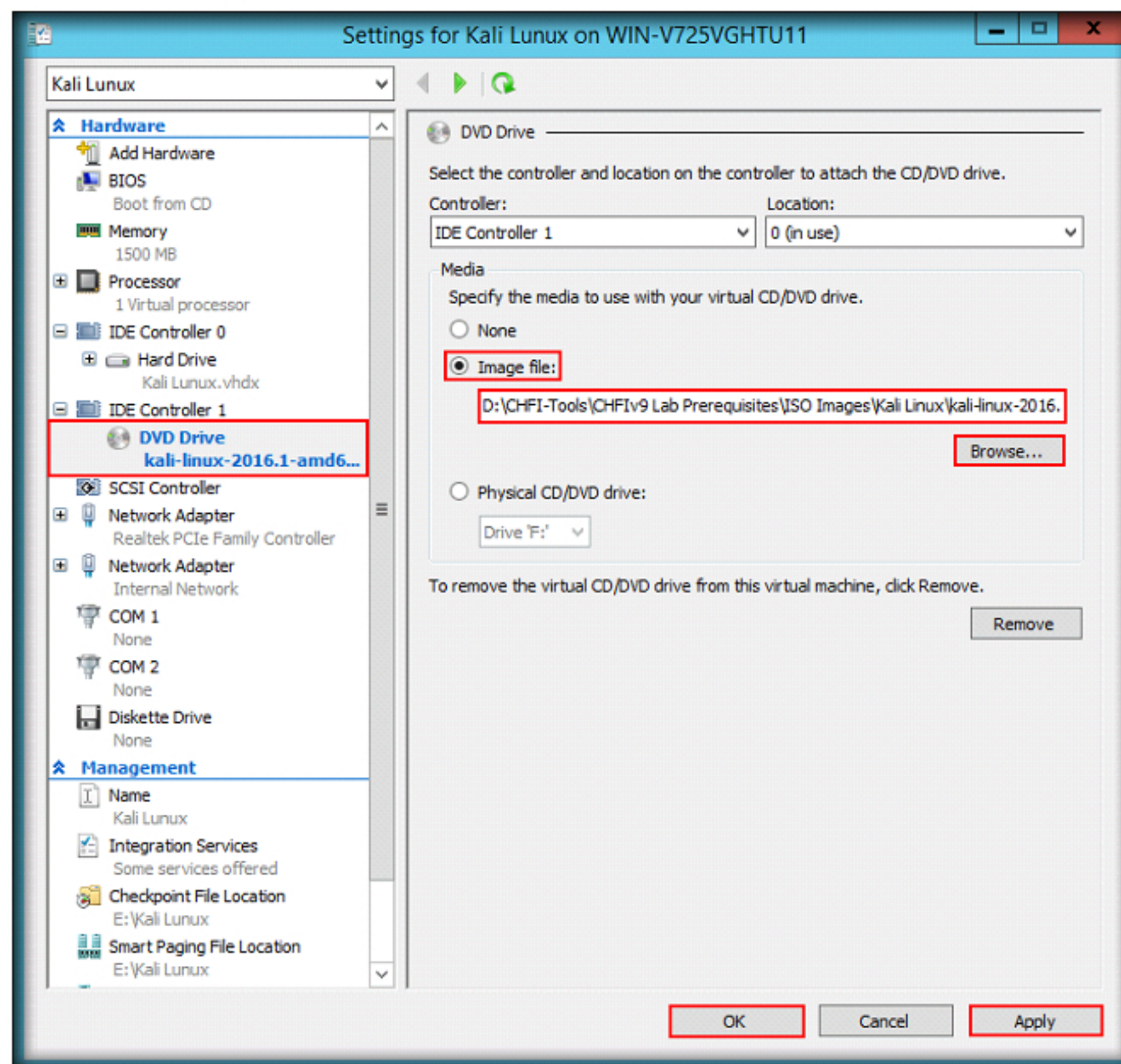


CT#21: Install Kali Linux in Hyper-V

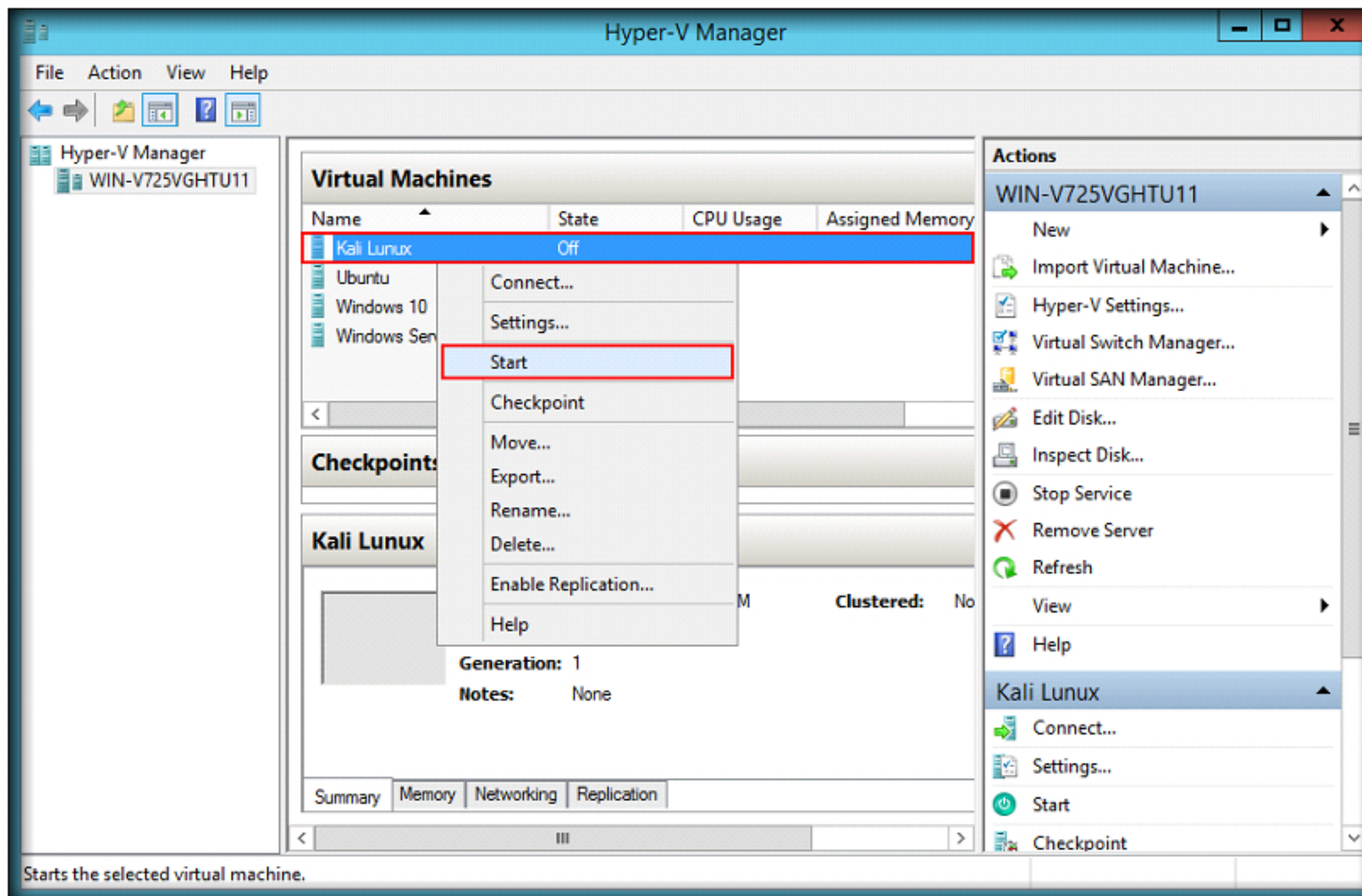
1. Launch Hyper-V Manager, select **Kali Linux** virtual machine and click **settings**



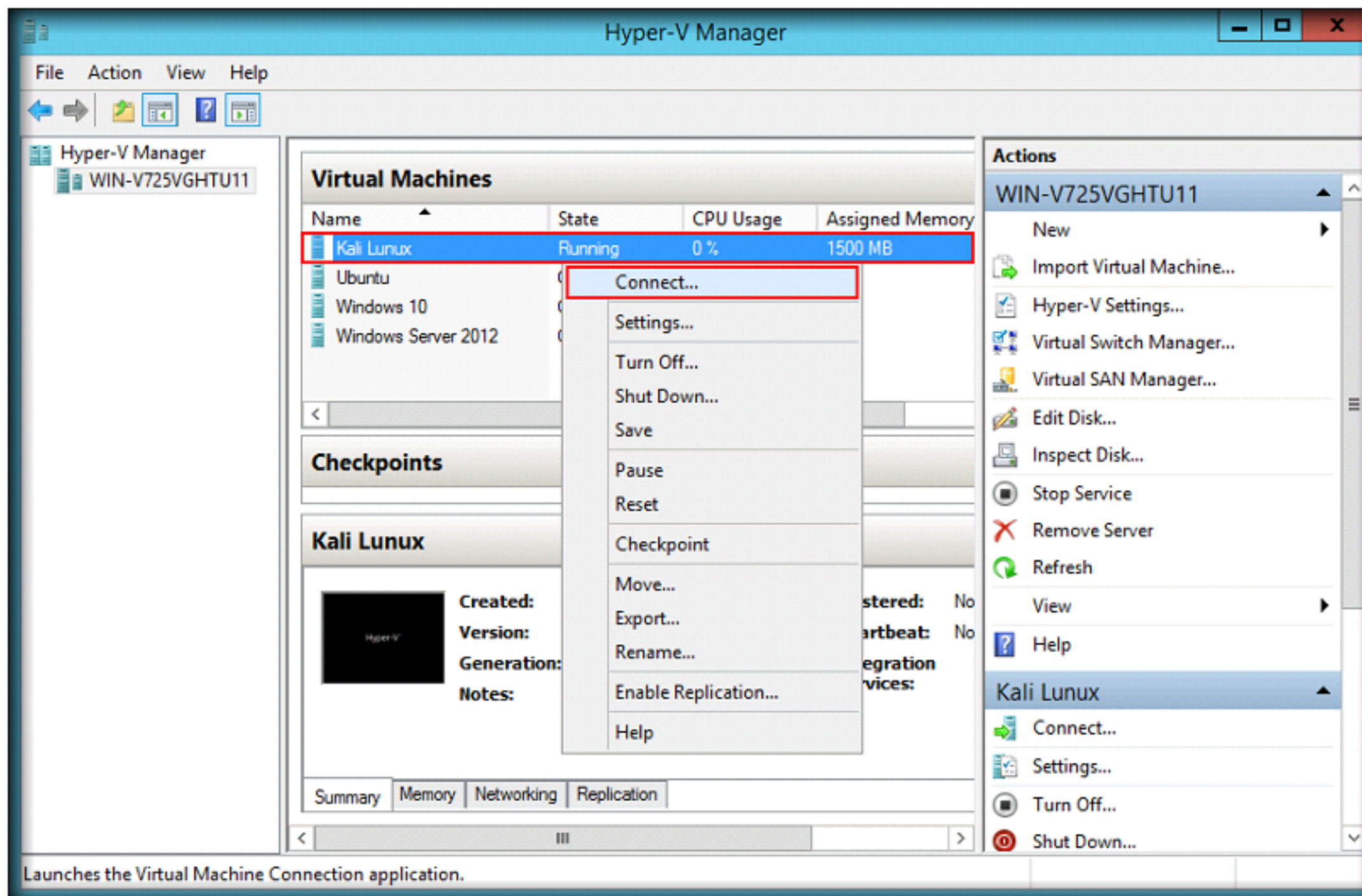
2. **Settings for Kali Linux** window appears
3. Click **DVD drive** option in the left pane and click **Image file** radio button in the right pane
4. Click **Browse** button, navigate to **C:\CHFI-Tools\CHFIv9 Lab Prerequisites\ISO Images\Kali Linux** and select **kali-linux-2016.1-amd64.iso**
5. Click **Apply** and then click **OK**. Settings for Kali Linux window **exits**



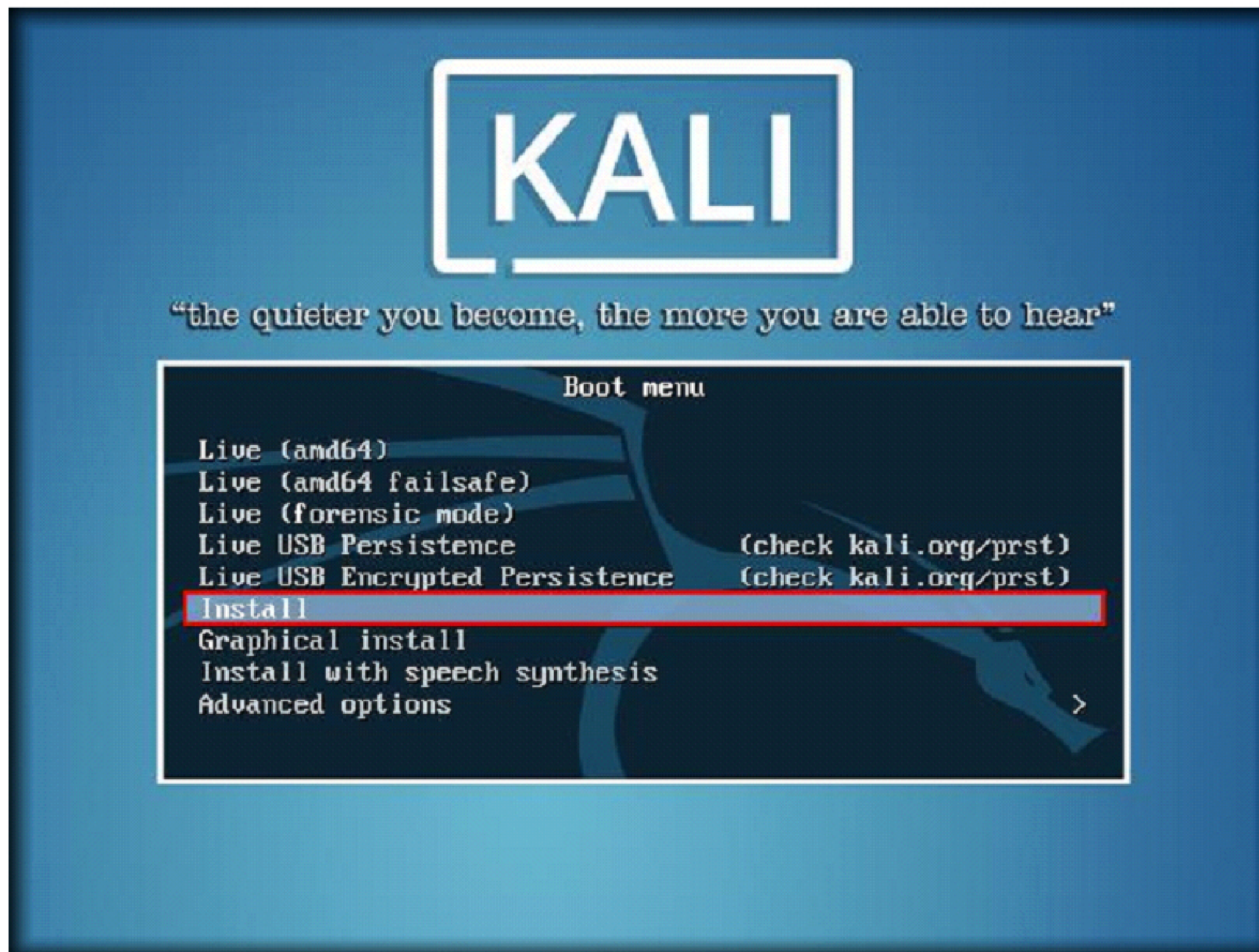
6. In the Hyper-V manager, **right-click** Kali Linux virtual machine, and select **Start**



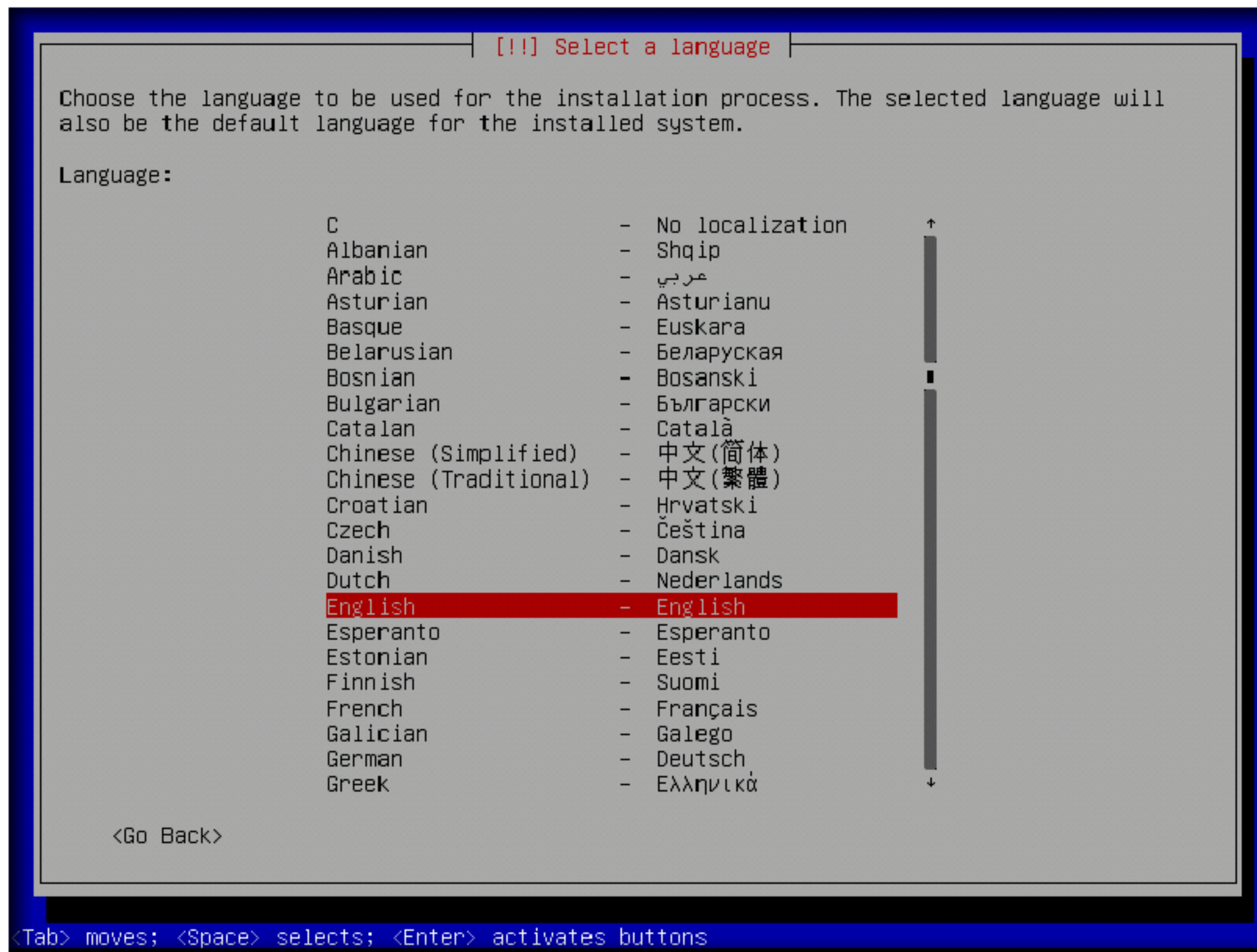
7. Go to Hyper-V manager, **right-click** Kali Linux virtual machine, and select **Connect...**



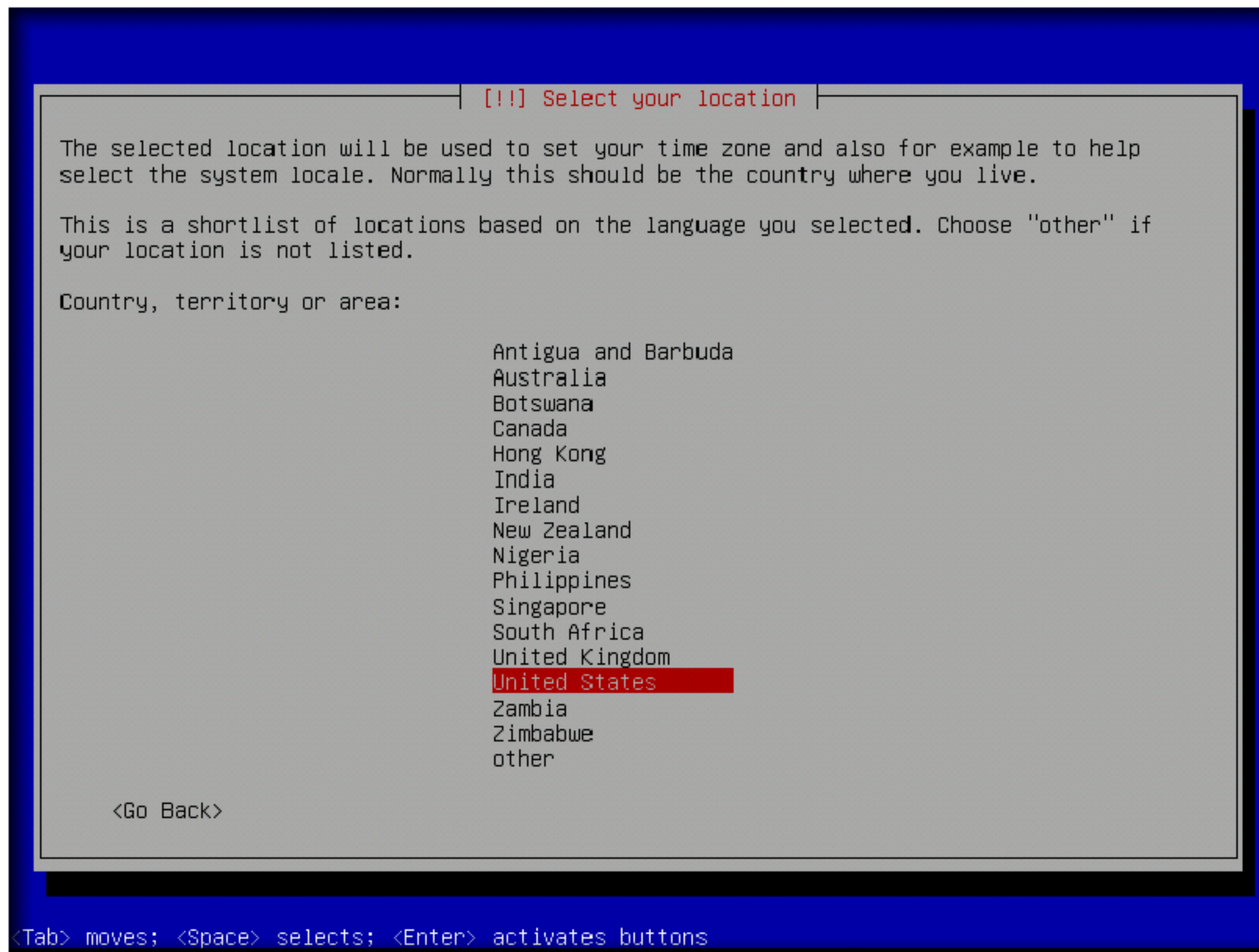
8. Kali Linux **Boot menu** appears, select **Install** and press **Enter**



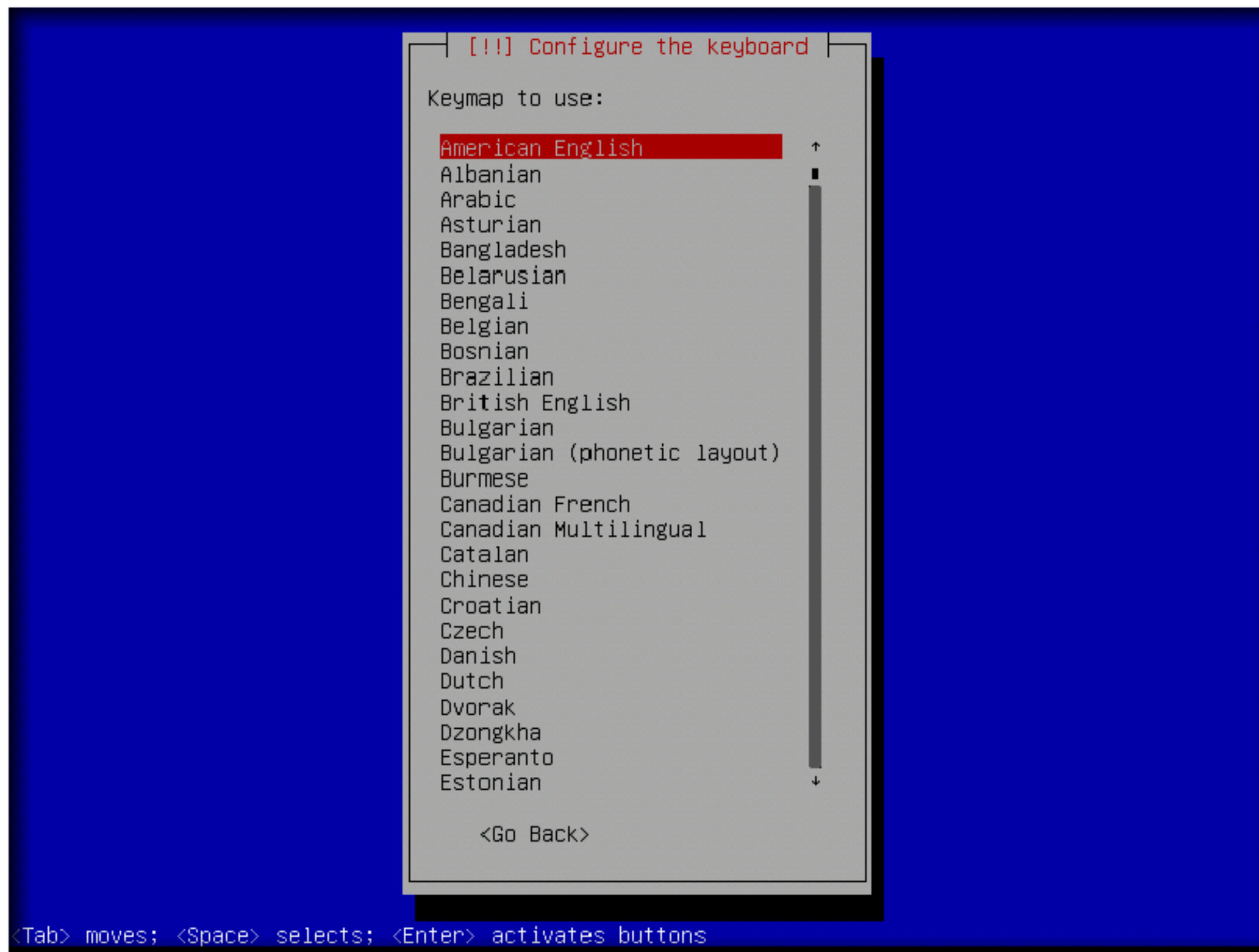
9. **Select a language** window appears, choose a language (here, **English**) and press **Enter**



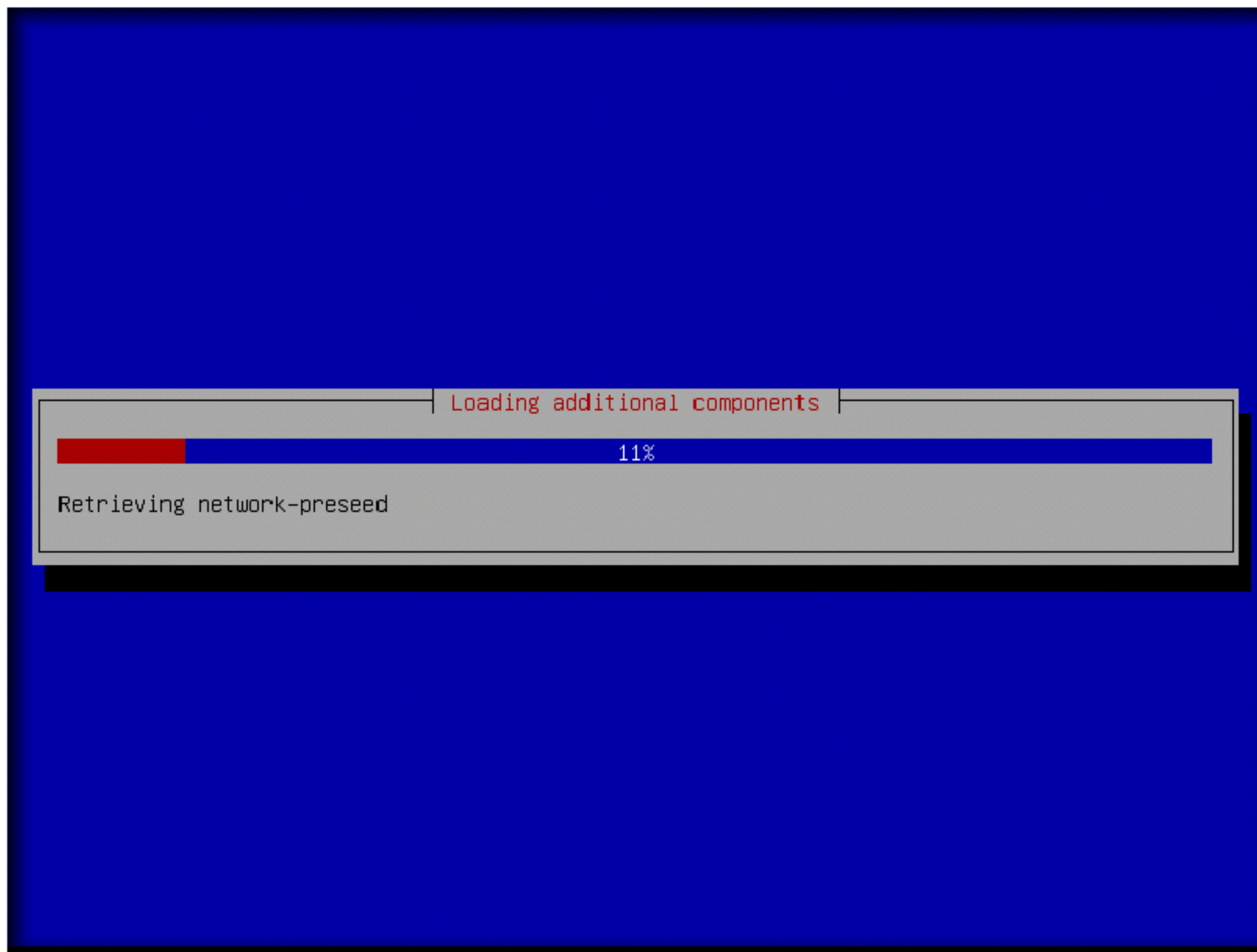
10. In the **Select your location** window, choose a location (here, **United States**) and press **Enter**



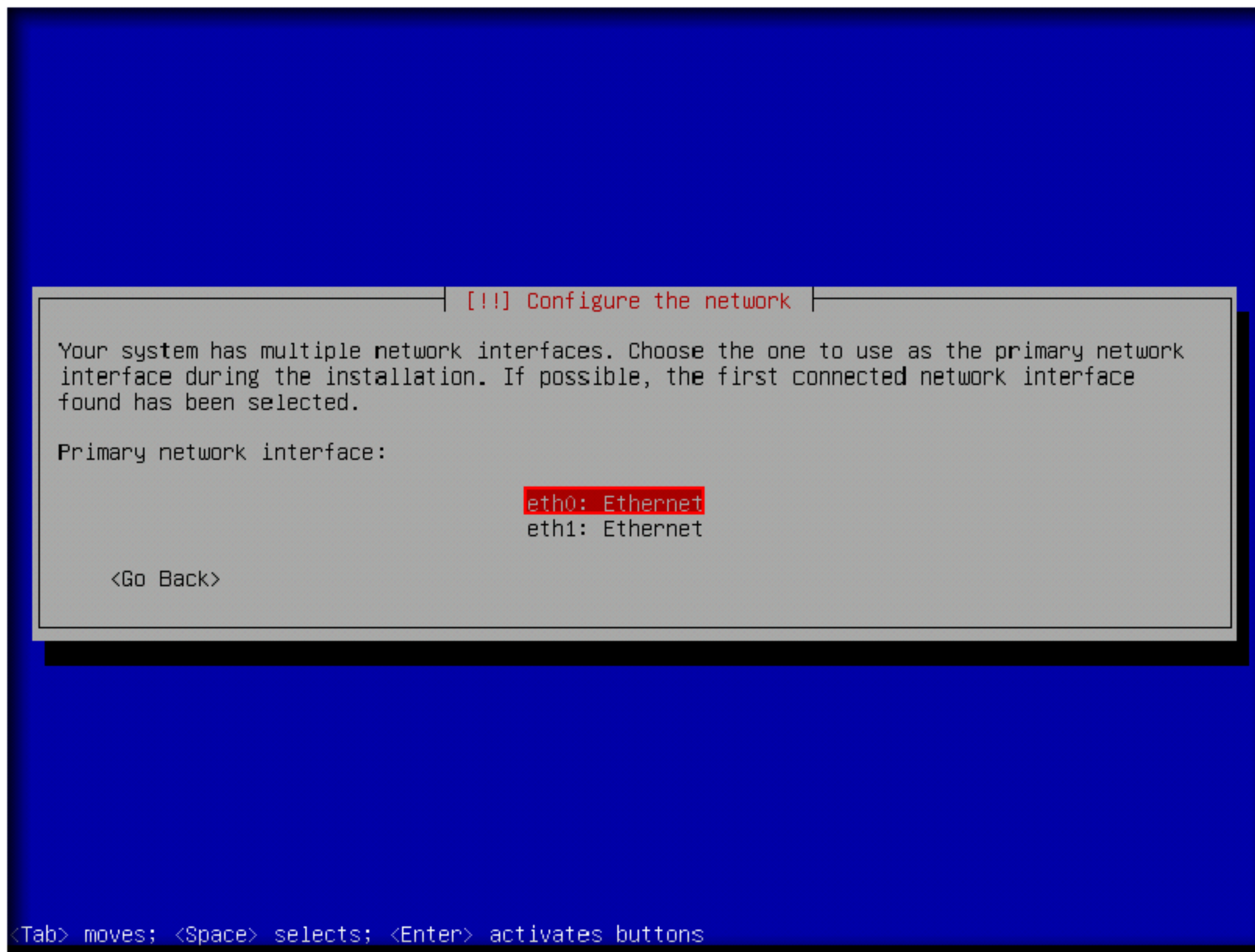
11. **Configure the keyboard** window appears, choose a language (here, **American English**) and press **Enter**



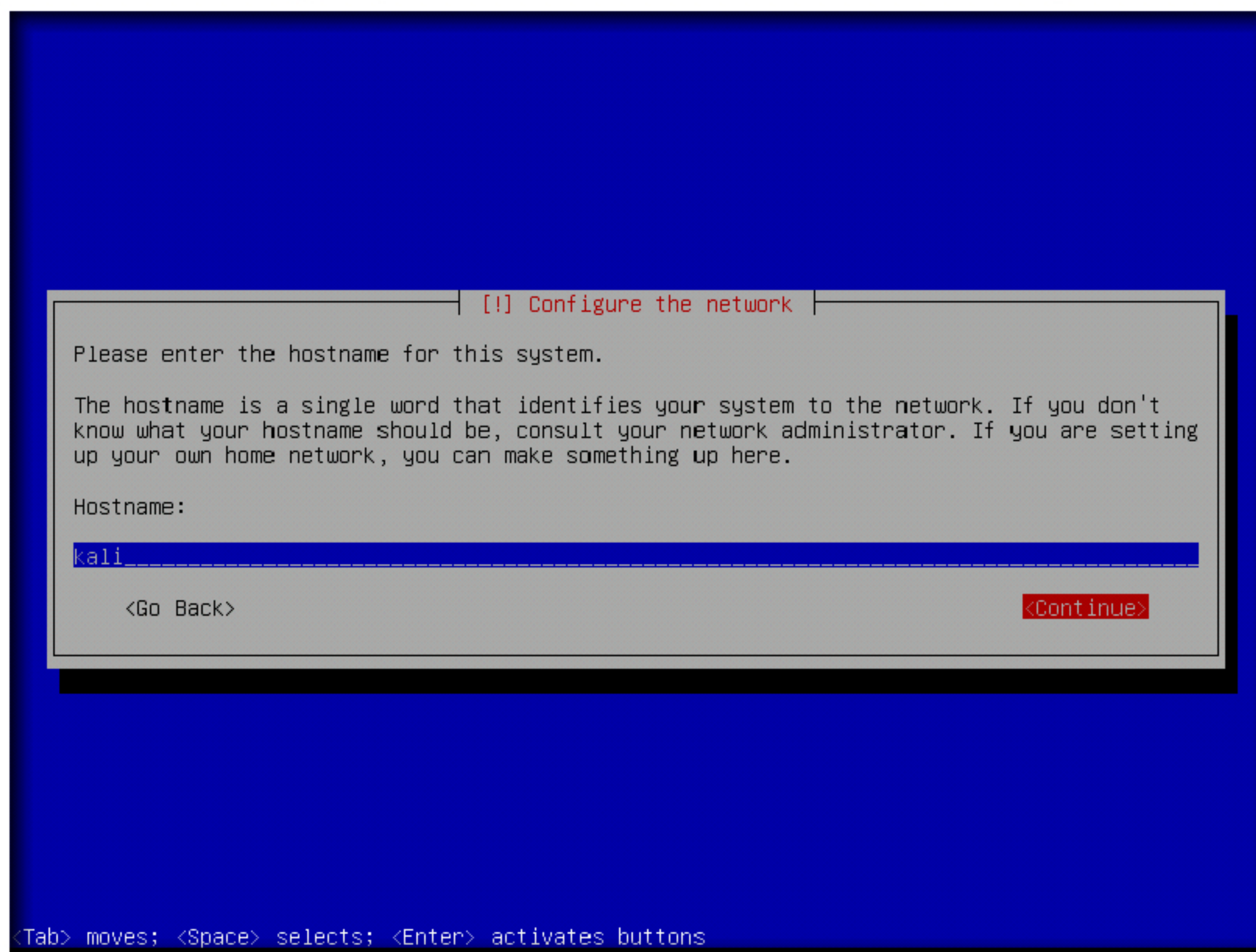
12. Wait until the additional components are loaded



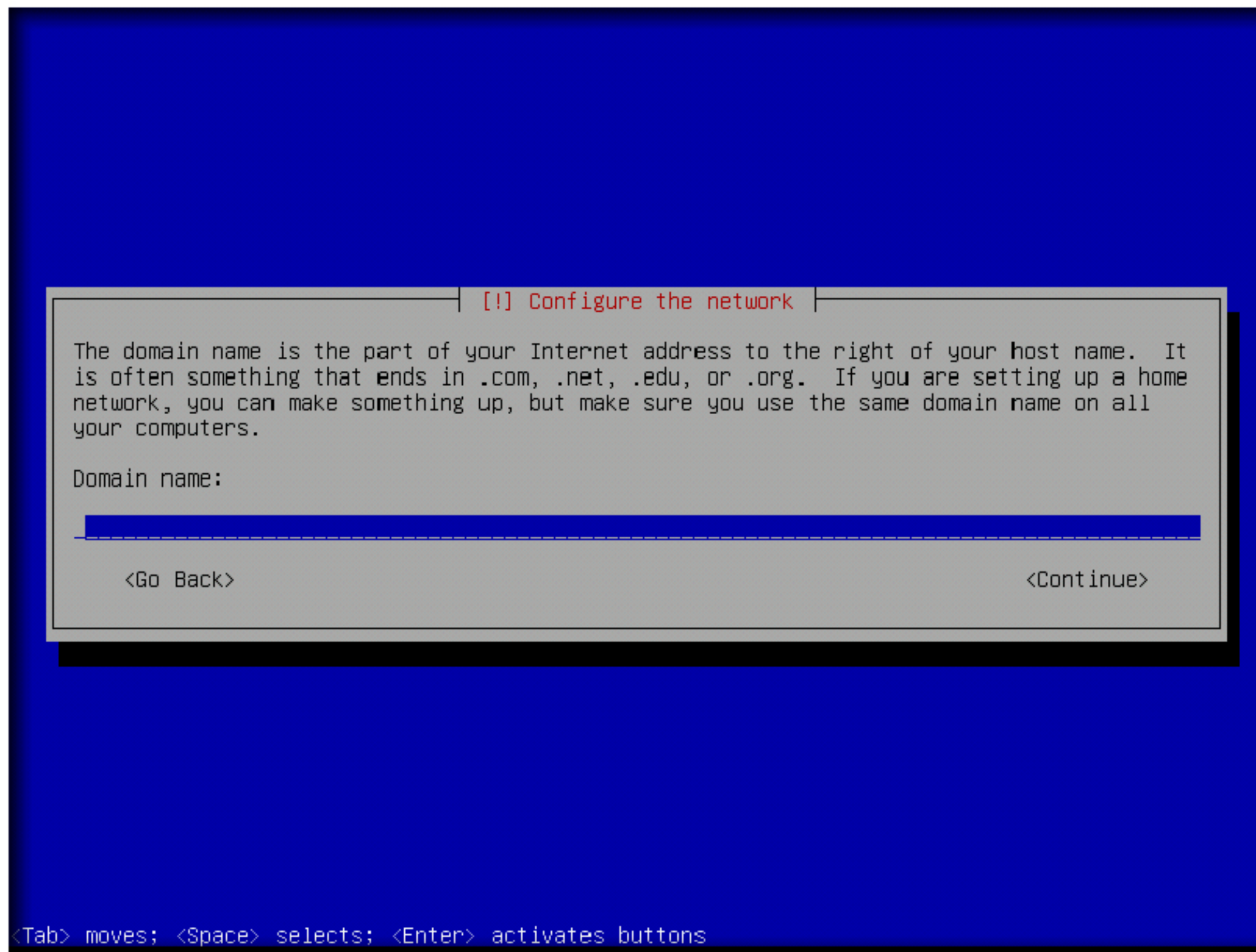
13. **Configure the network** window appears, select the **Primary network interface** as **eth0** and press **Enter**



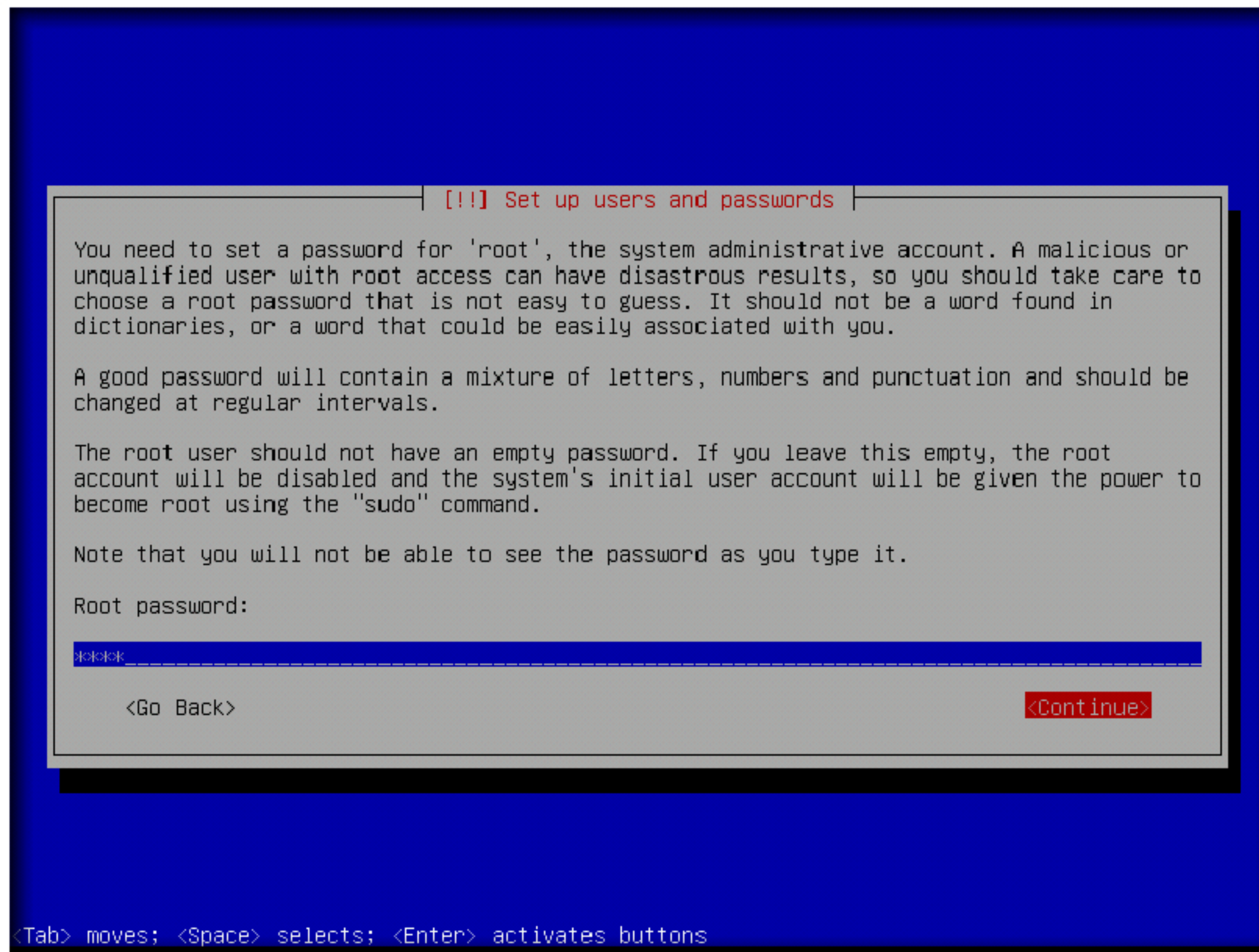
14. **Configure the network** window appears, leave the **Hostname** as **Kali** and select **Continue** and press **Enter**



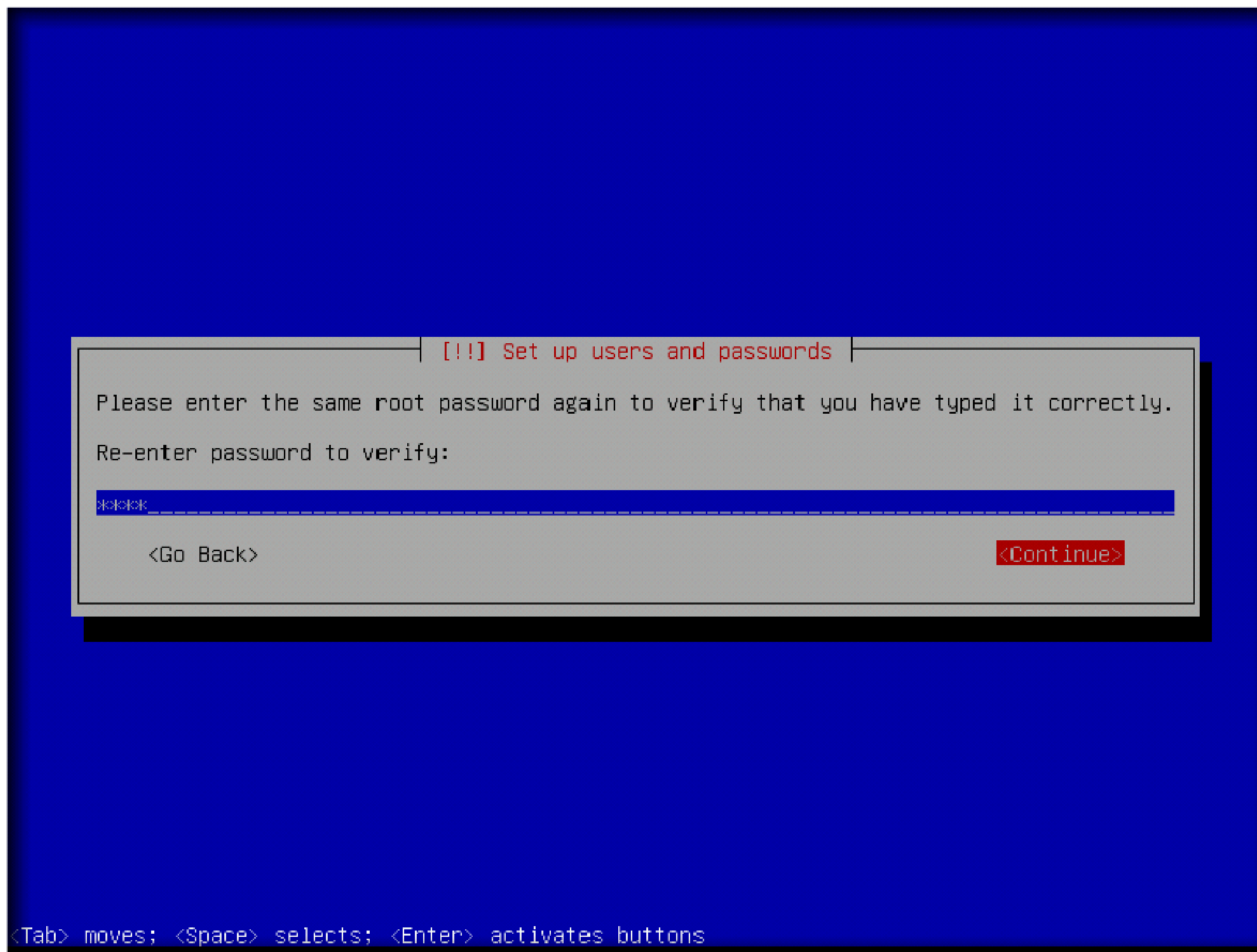
15. In **Configure the network** window, leave the **Domain name** field empty and select **Continue** and press **Enter**



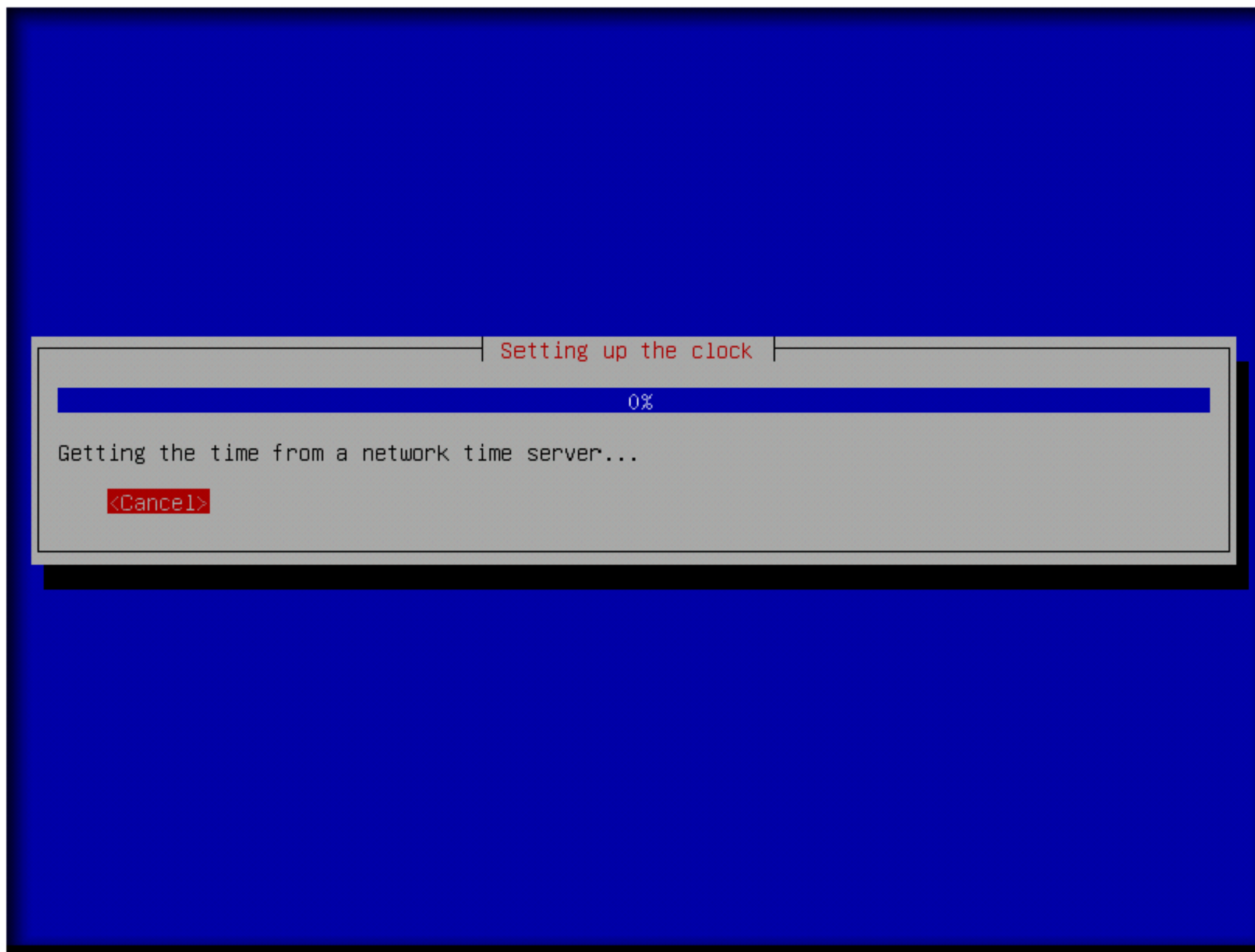
16. **Set up users and passwords** window appears, enter the **Root password** as **toor** and select **Continue** and press **Enter**



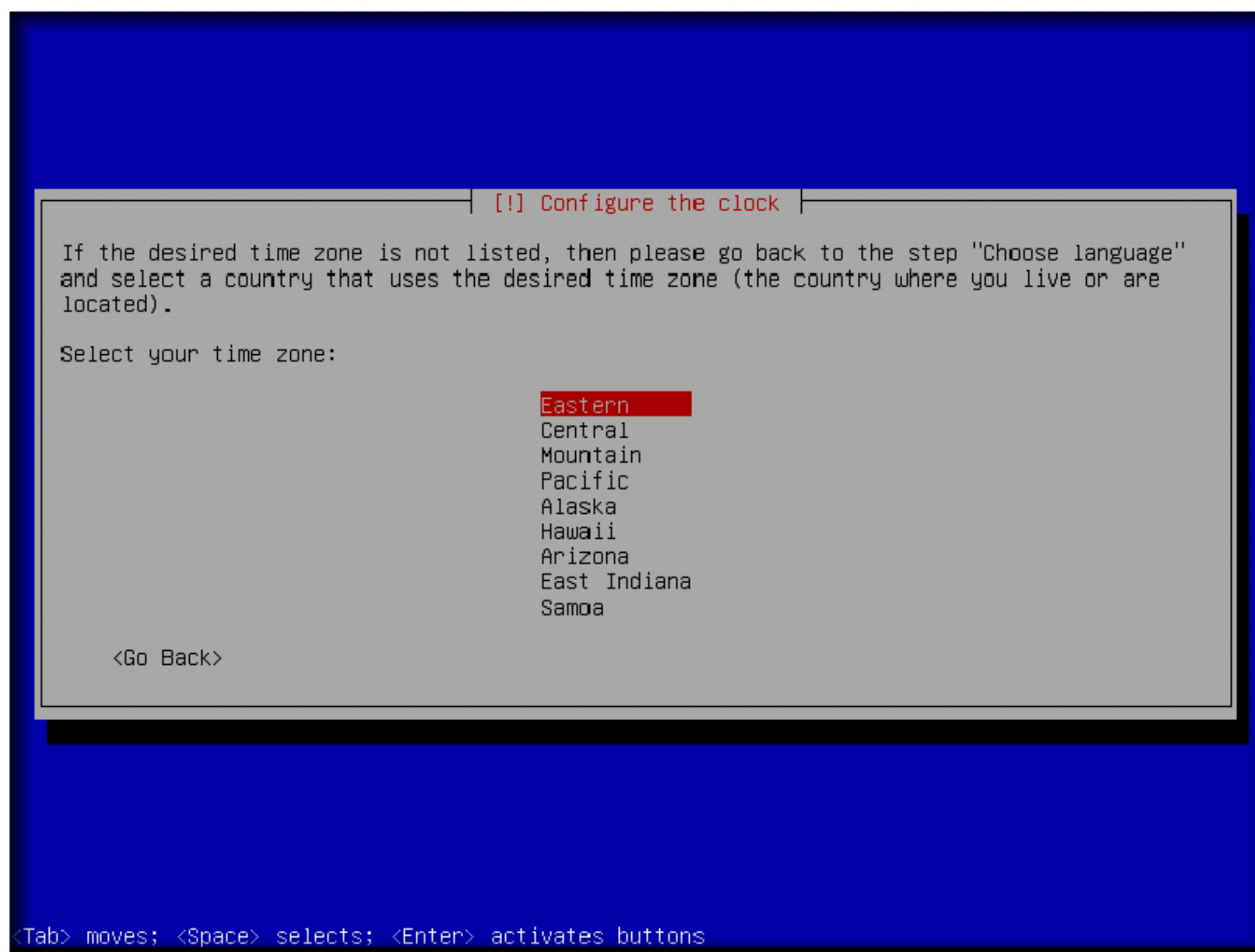
17. **Set up users and passwords** window appears, re-enter the password **toor** and select **Continue** and press **Enter**



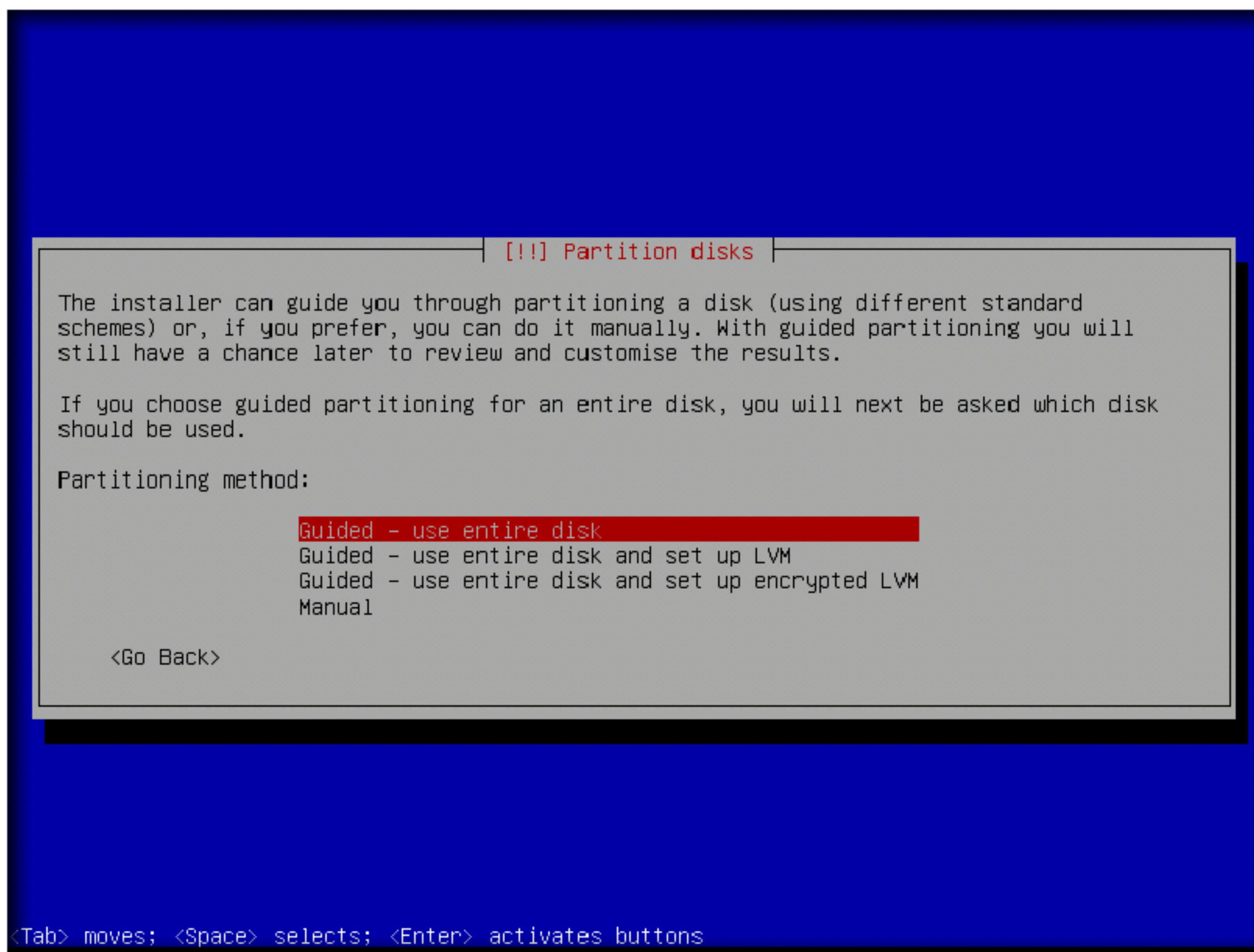
18. Wait until the installer fetches time from the network time server



19. In **Configure the clock** window, choose the time zone (here, **Eastern**) and press **Enter**

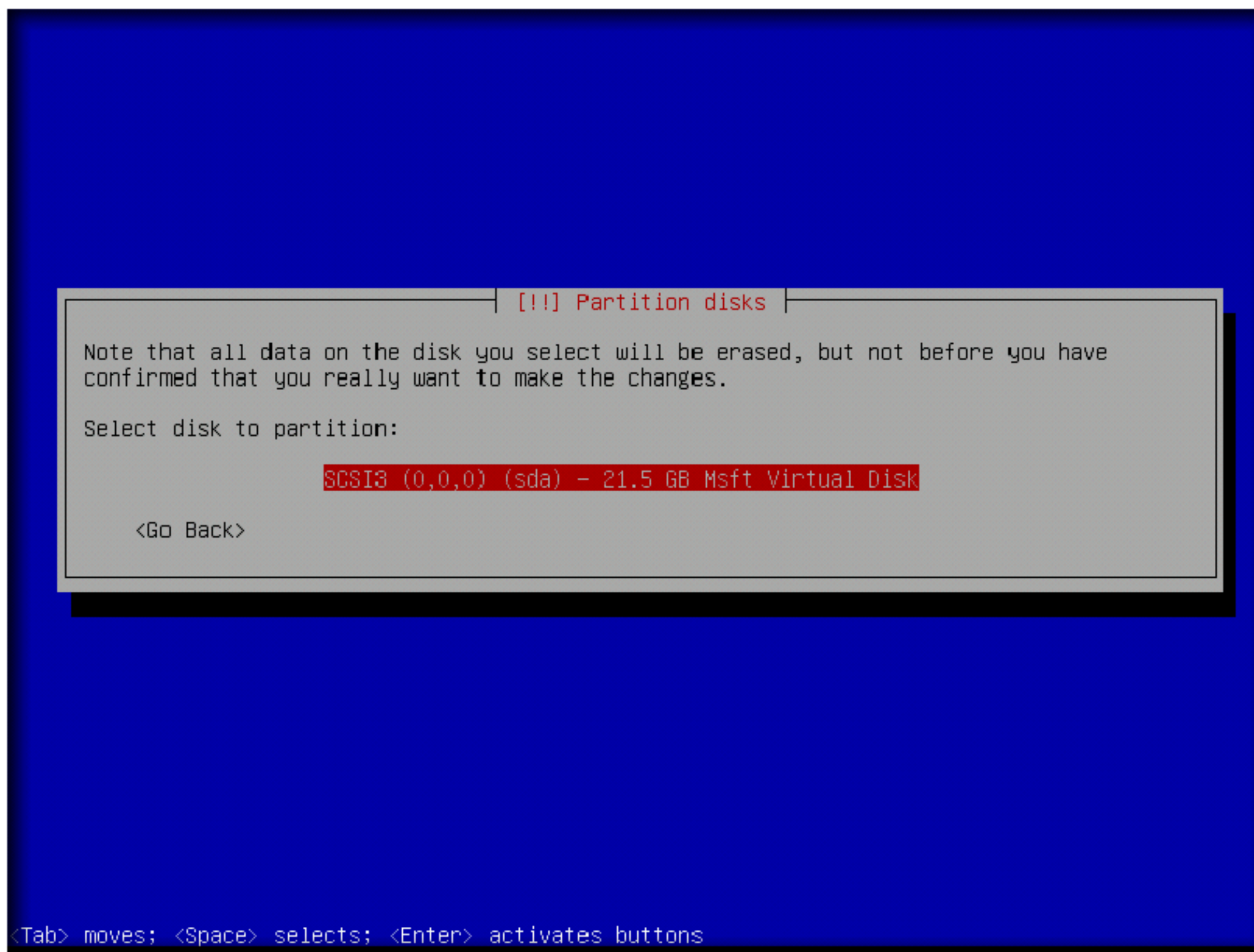


20. **Partition disks** window appears, choose the partition method: **Guided – use entire disk** and press **Enter**

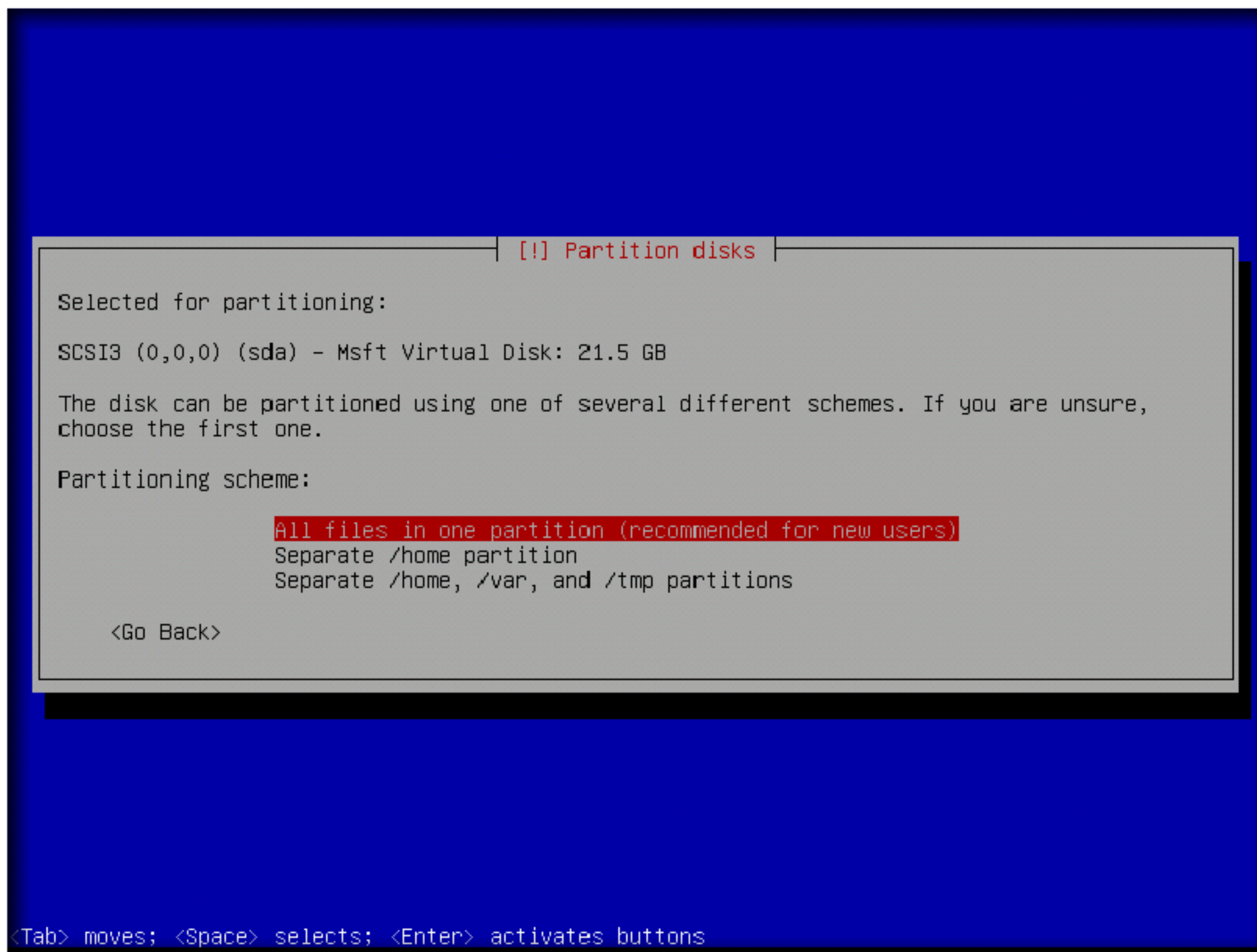


21. Another **Partition disks** window appears, select the disk **SCSI3 (0,0,0) (sda) – 21.5 GB Msft Virtual Disk** and press **Enter**

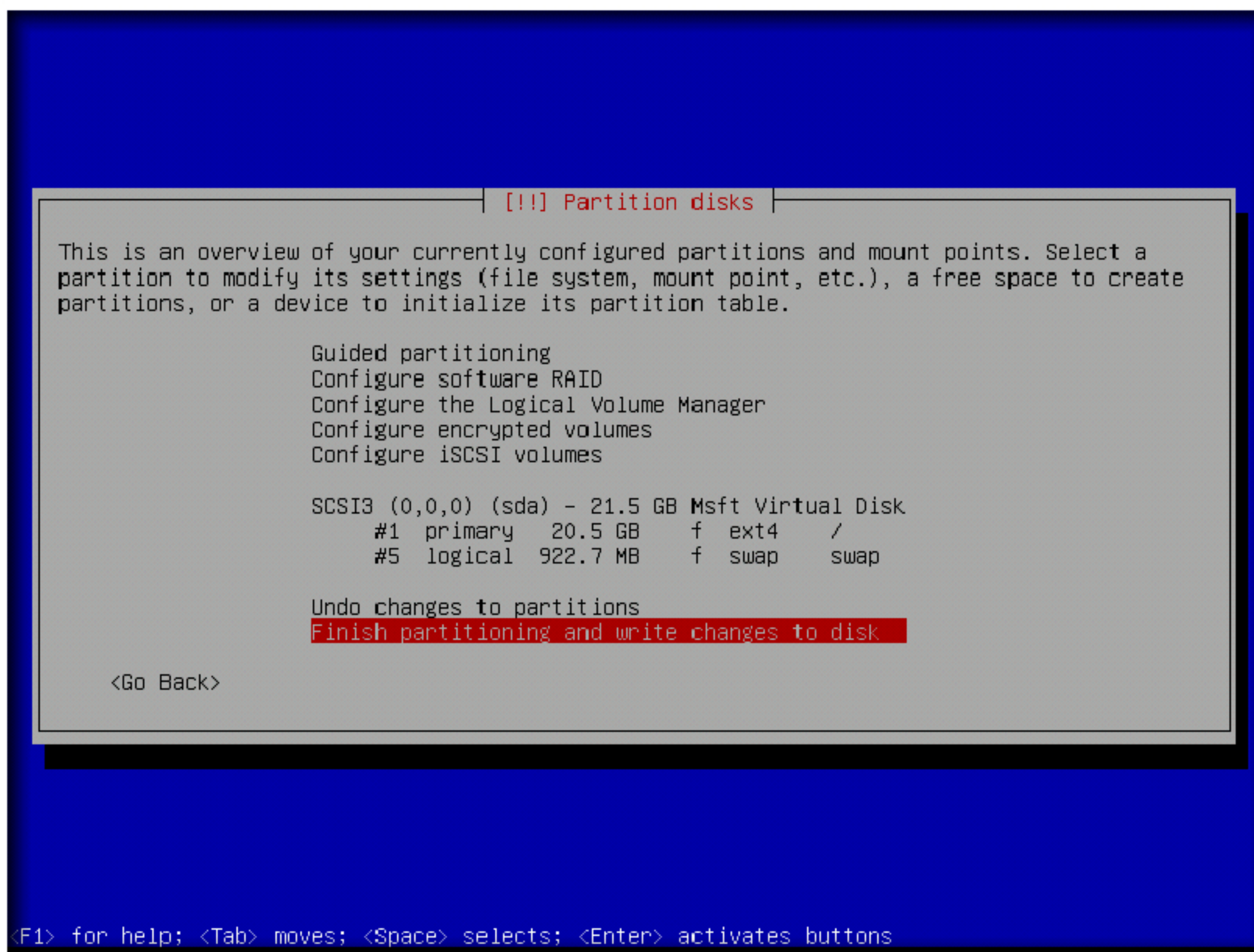
Note: The size of the disk (**21.5 GB**) may vary in your lab environment



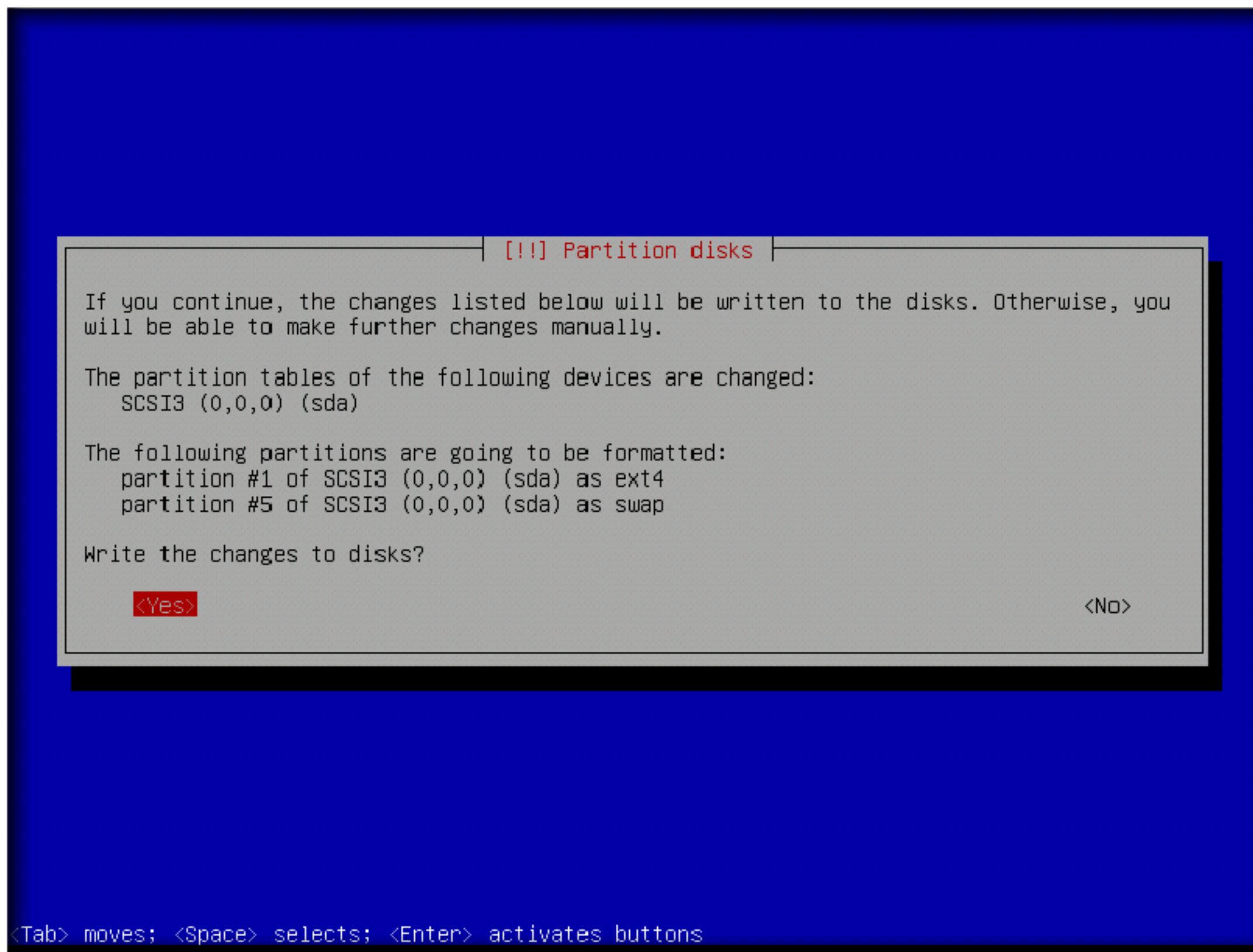
22. In the **Partition disks** window, choose the Partitioning scheme: **All files in one partition (recommended for new users)** and press **Enter**



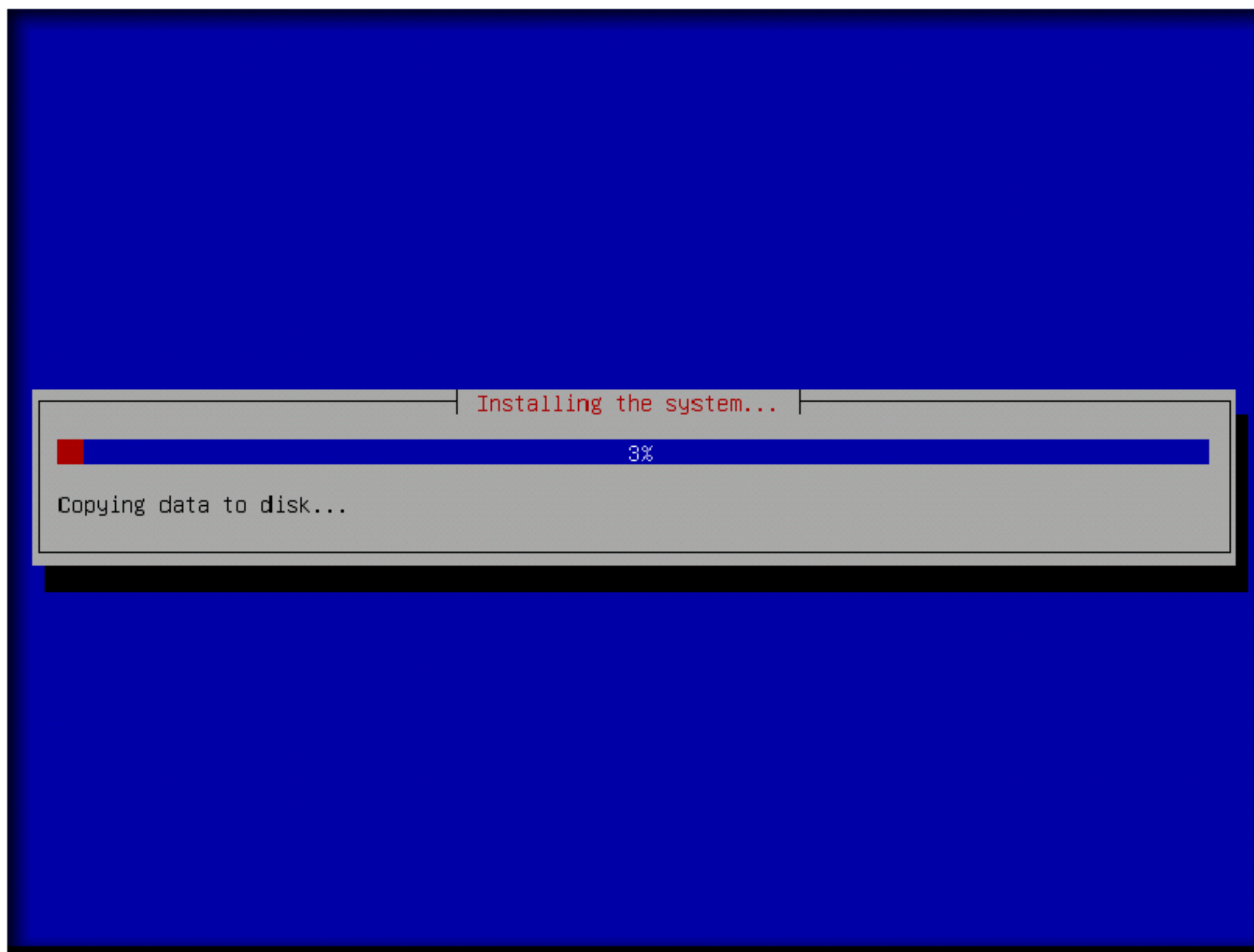
23. **Partition disks** window appears displaying the overview of your currently configured partitions, choose **Finish partitioning and write changes to disk** and press **Enter**



24. A **Partition disks** window appears stating that the changes will be written to the disk, select **Yes** and press **Enter**.

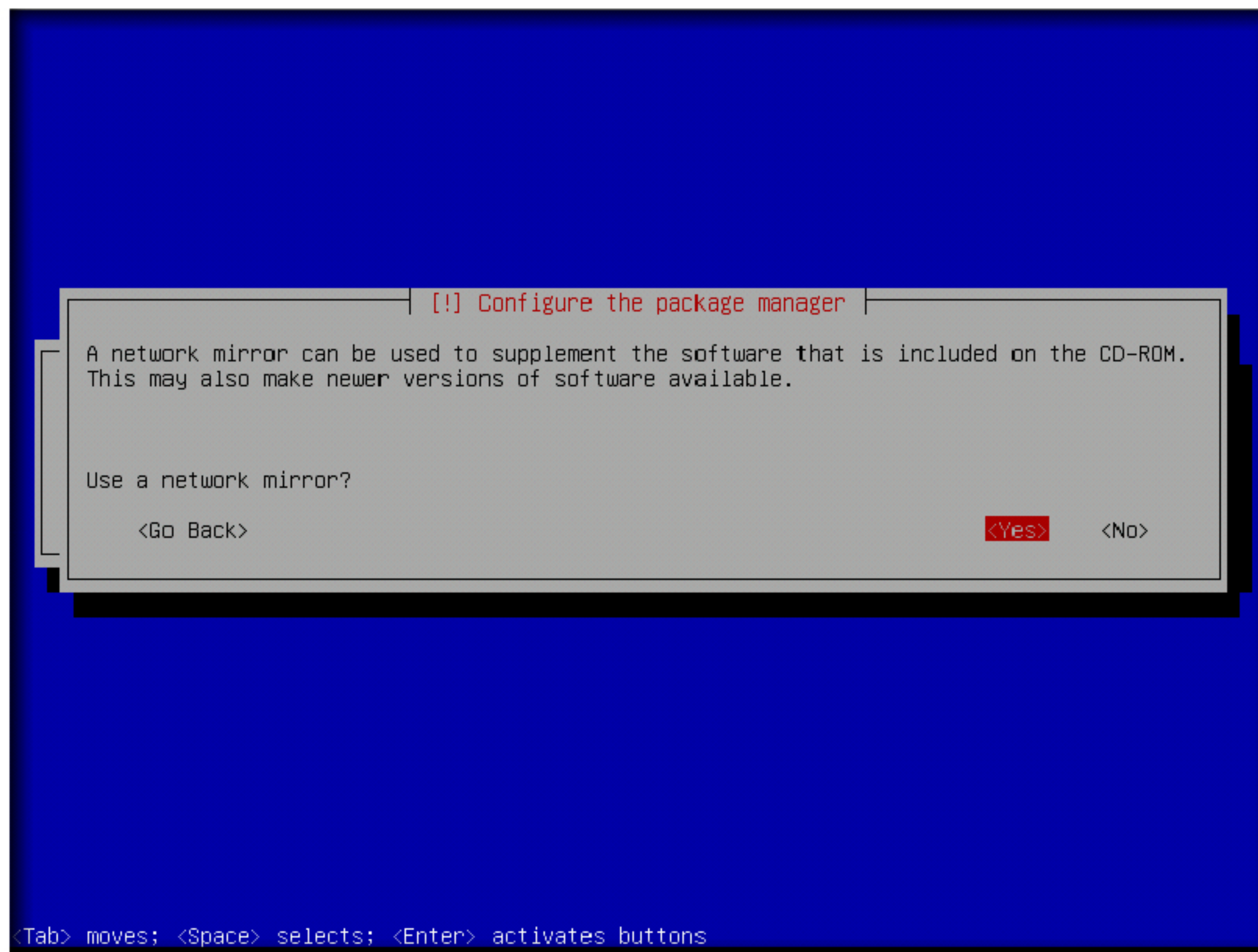


25. Wait until the partitions are formatted and the operating system is installed
26. It takes some time for the installation to complete



27. On completion of installation, **Configure the package manager** window appears, select **Yes** in order to use a network mirror and press **Enter**

Note: If you get any Bad Archive error continue without using a Network Mirror



28. **Configure the package manager** window appears, leave the HTTP proxy information field empty and select **Continue** and press **Enter**

[!] Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

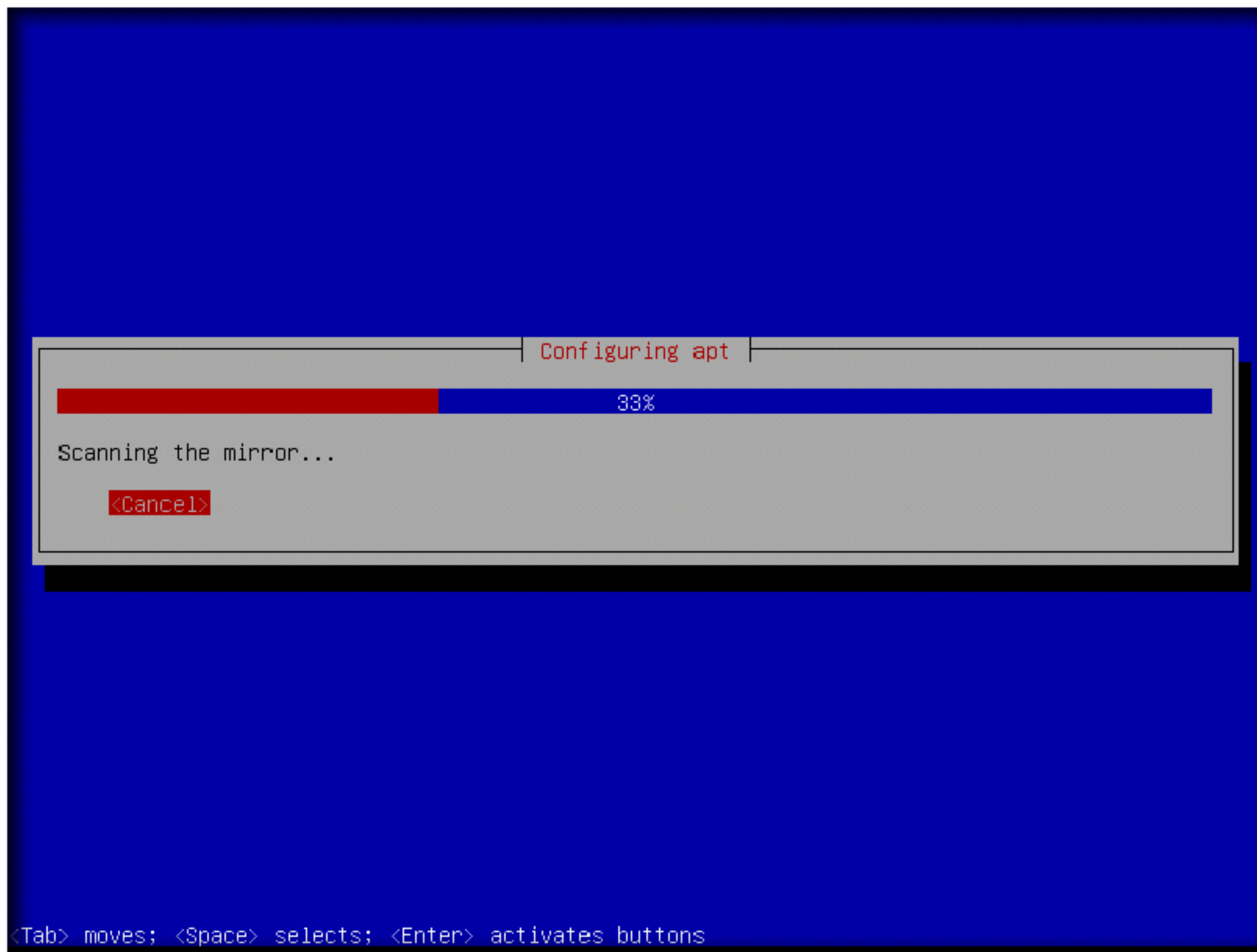
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):

<Go Back> <Continue>

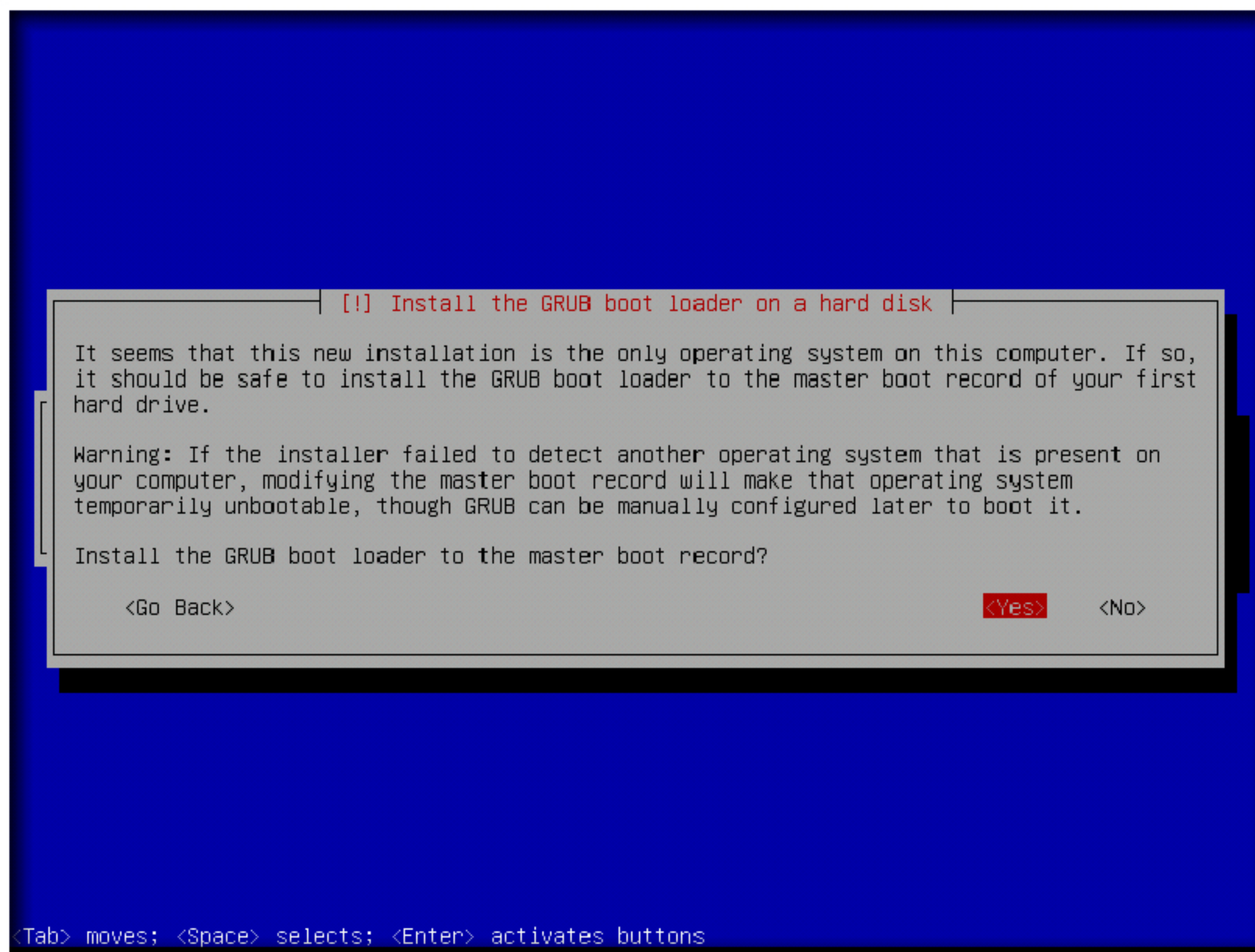
<Tab> moves; <Space> selects; <Enter> activates buttons

29. Wait until the **apt** is configured

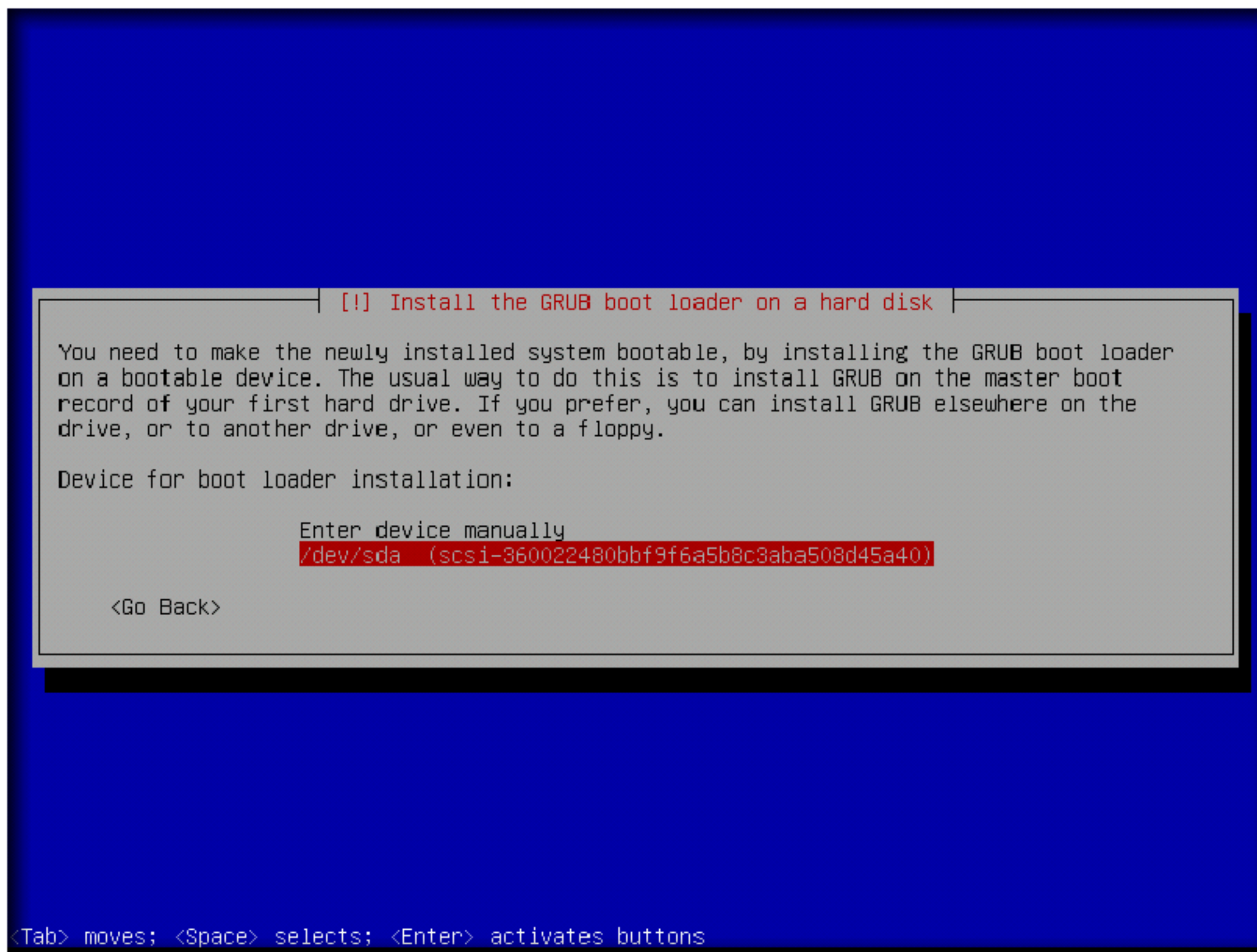


Note: A blank screen may appear for a considerable amount of time. Do not perform any actions on the keyboard until you are redirected to the next window (**Install the GRUB boot loader on a hard disk**)

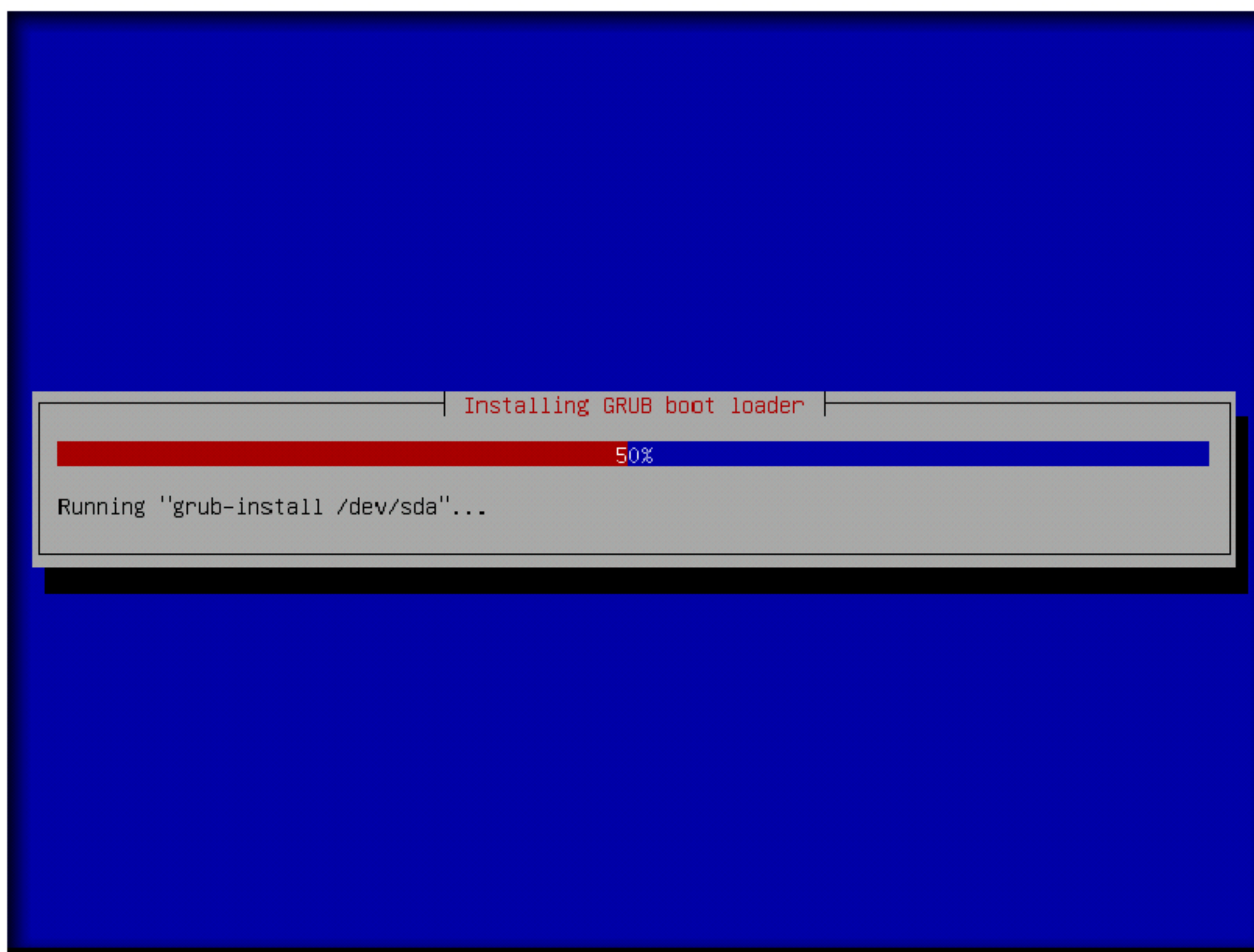
30. **Install the GRUB boot loader on a hard disk** window appears, select **Yes** in order to install the GRUB boot loader to the master boot record and press **Enter**



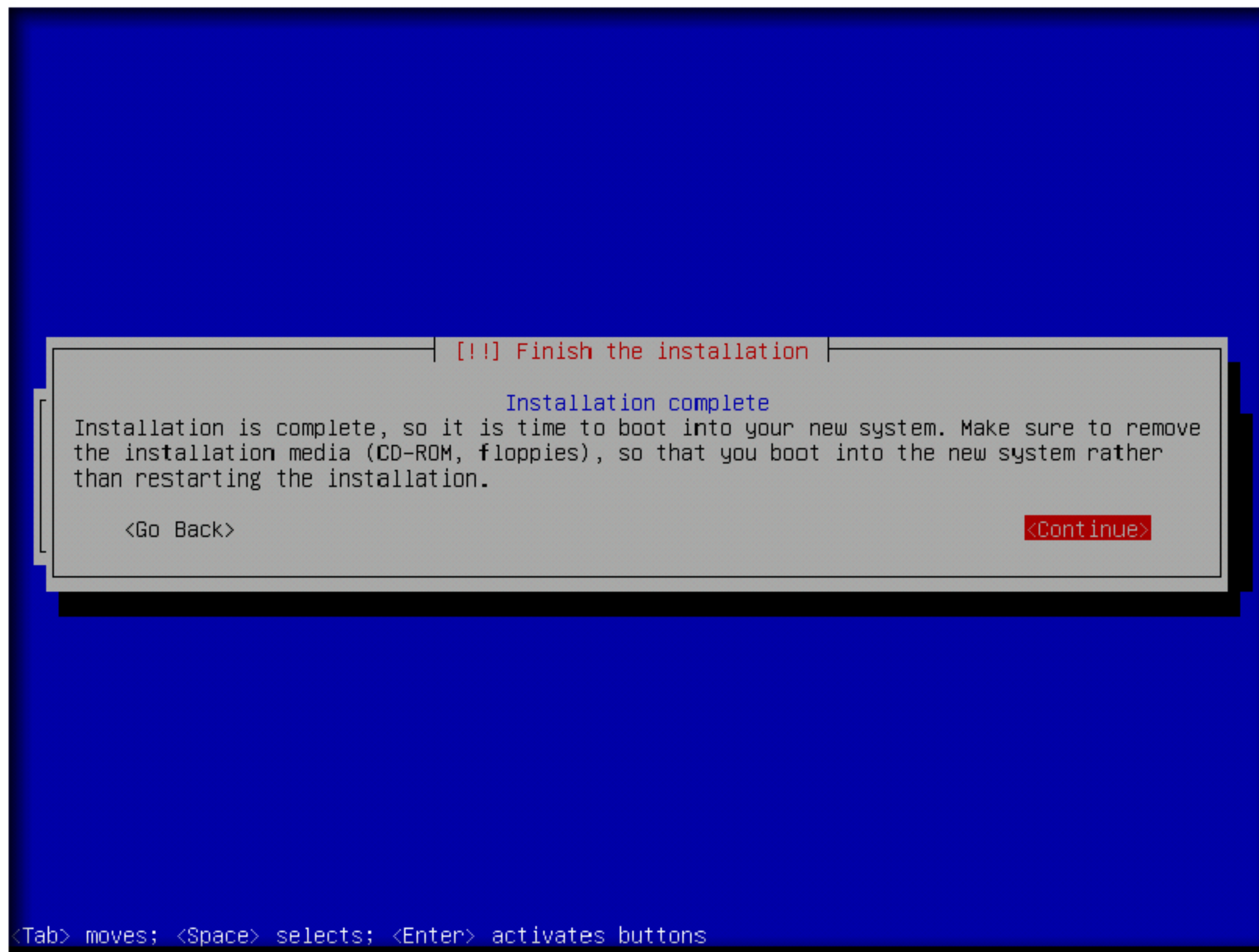
31. If **Install the GRUB boot loader on a hard disk** window appears, select **/dev/sda** device for boot loader installation and press **Enter**



32. Wait until the GRUB boot loader is installed



33. Finish the installation window appears, select **Continue** and press **Enter**

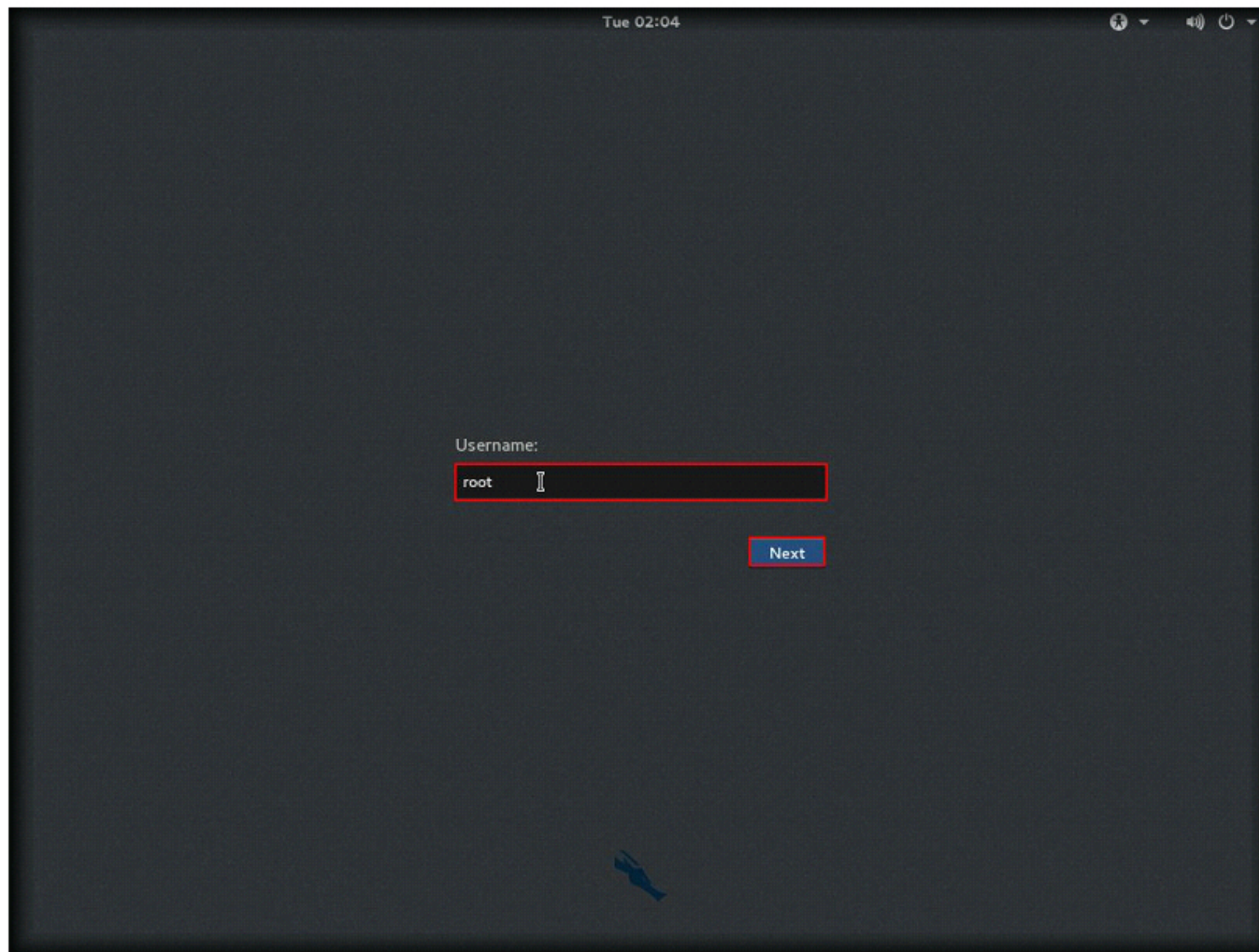


34. Finishing the installation takes considerable amount of time. Wait until the installation is completed.

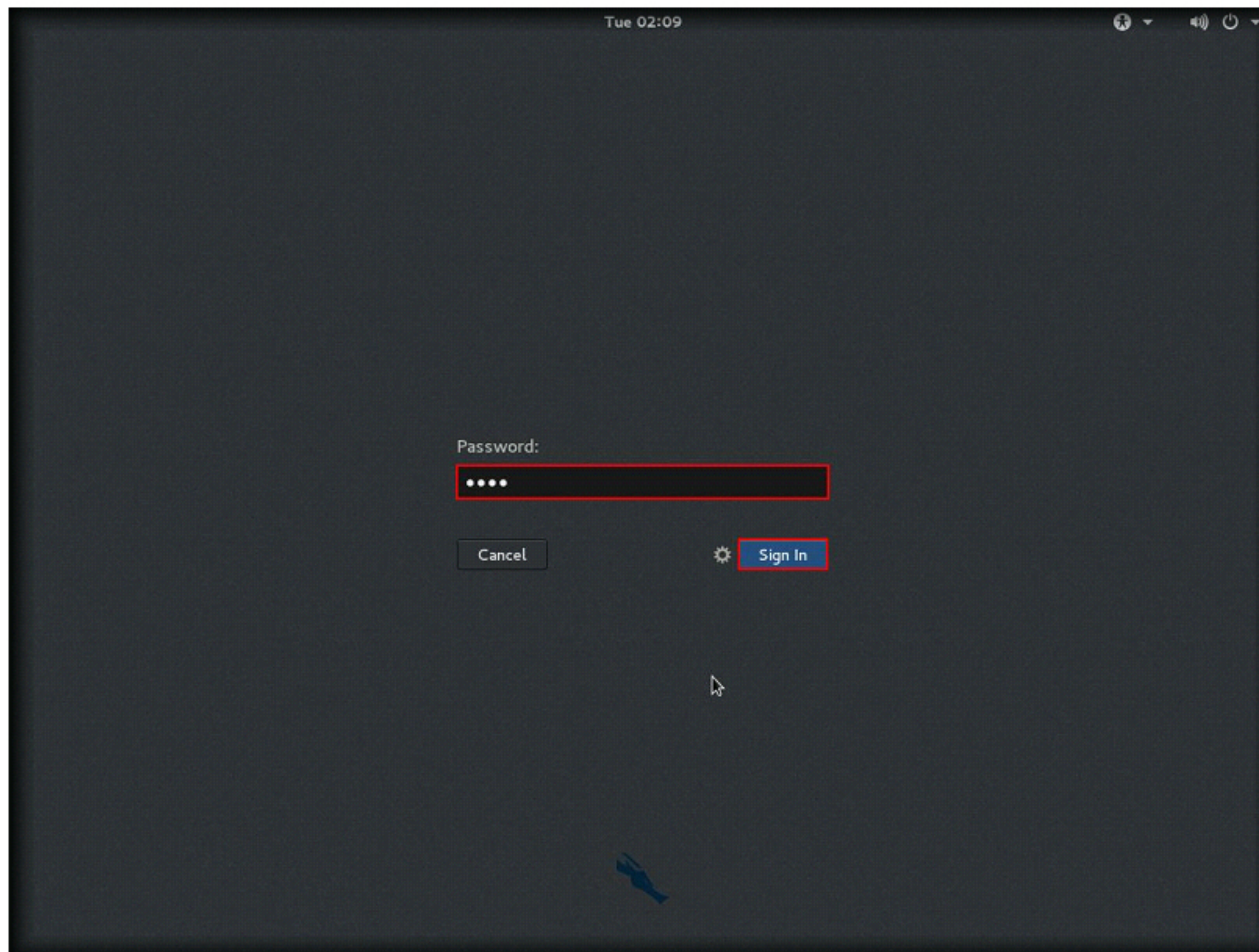
Note: Make sure that after installation remove ISO file from the Kali Linux Settings.



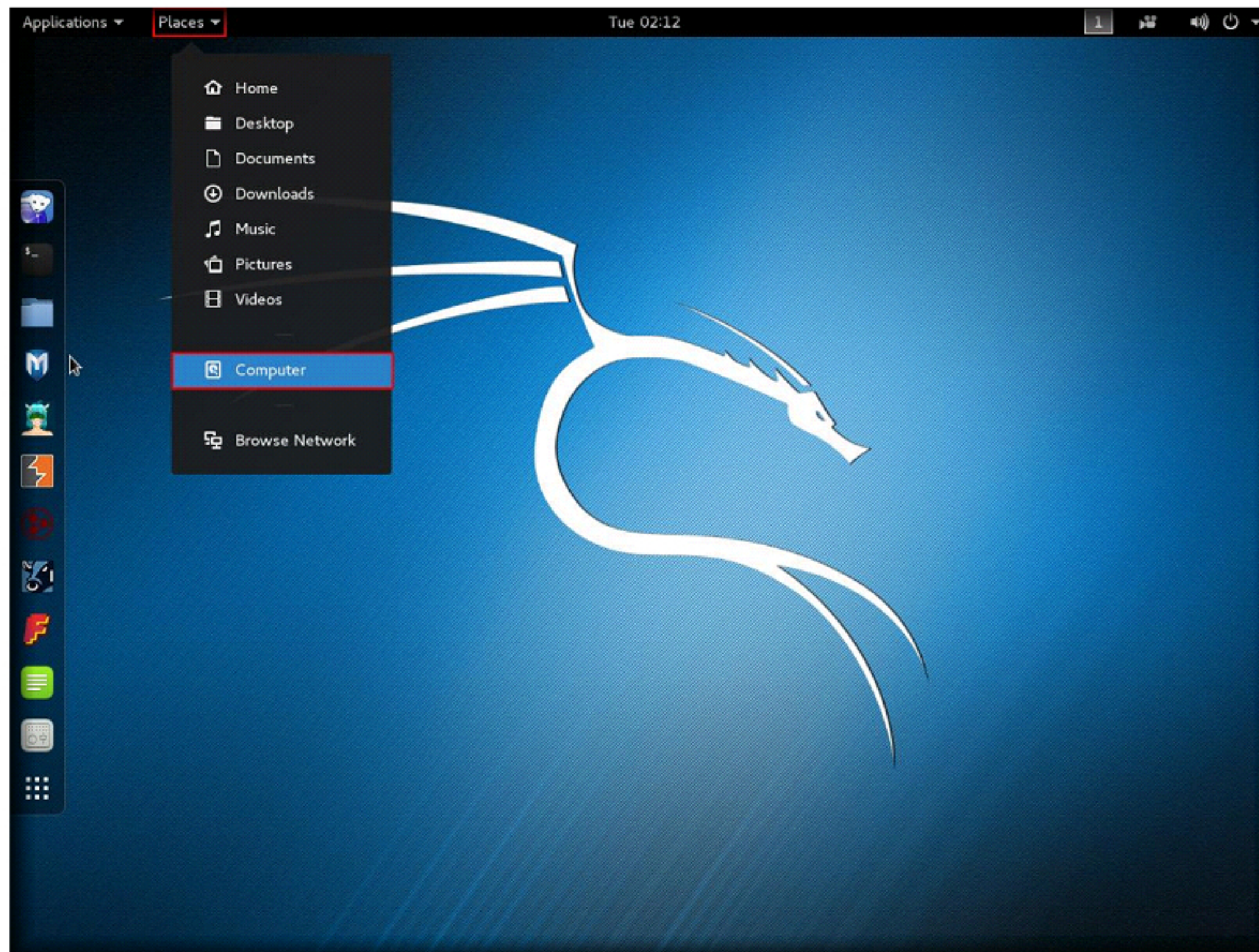
35. On completion of installation, wait until **Kali Linux** login screen appears. Type **root** in the **Username** text field and click **Next**.



36. Type **toor** in the **Password** text field and click **Sign In**



37. Kali Linux Desktop appears, go to Places → Computer



38. Now, go to **Computer** → **etc** → **network** and double-click **interfaces** file. The interfaces file appears in **leafpad** text editor.

39. Now, add the following lines in the file and save it:

a. auto eth0

b. iface eth0 inet static

c. address [IP Address of External Network]

d. netmask 255.255.255.0

e. gateway 192.168.0.1

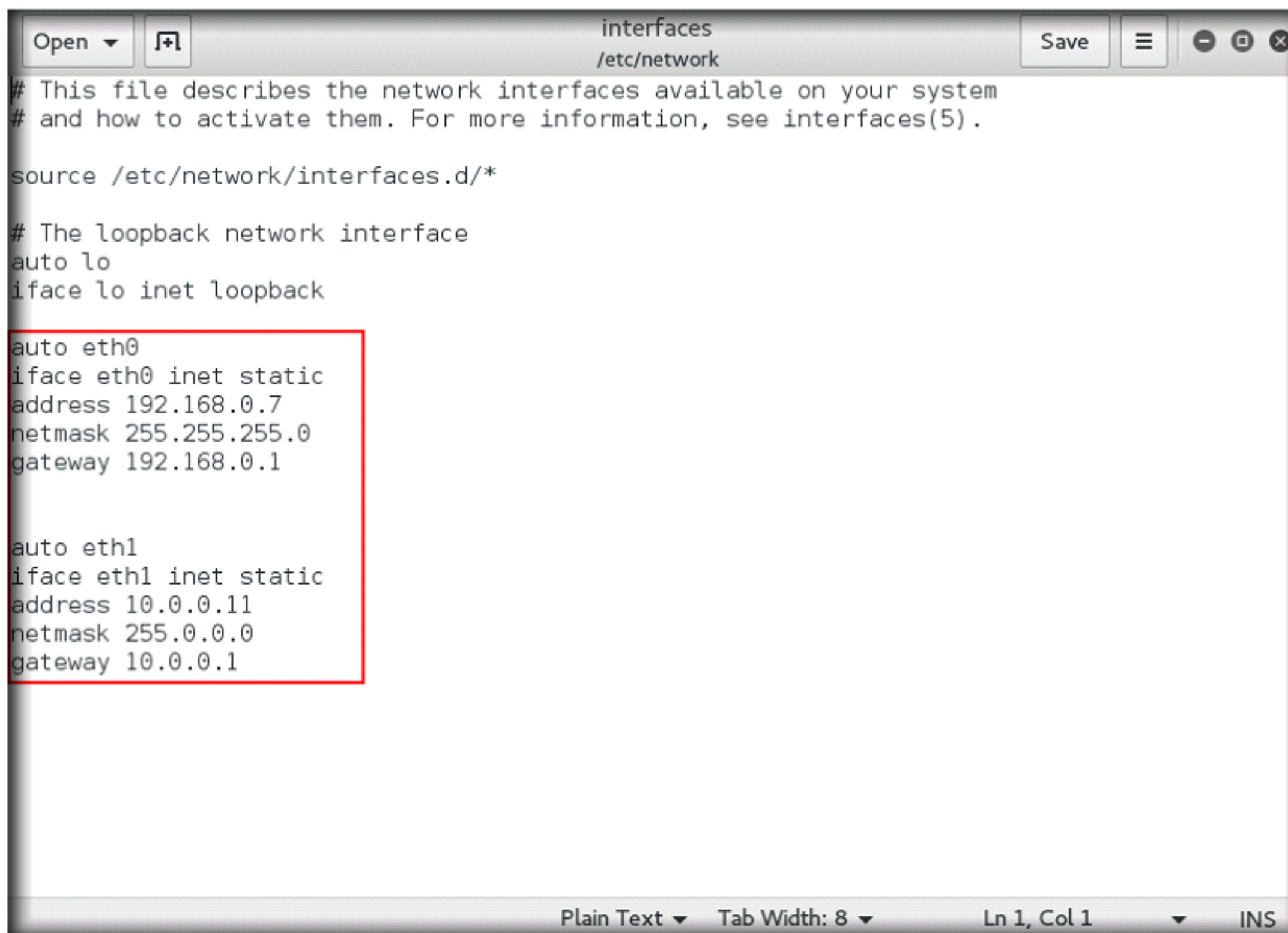
f. auto eth1

g. iface eth1 inet static

h. address 10.0.0.11

i. netmask 255.0.0.0

j. gateway 10.0.0.1



```
Open [icon] interfaces /etc/network Save [icon] [icon] [icon] [icon]
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

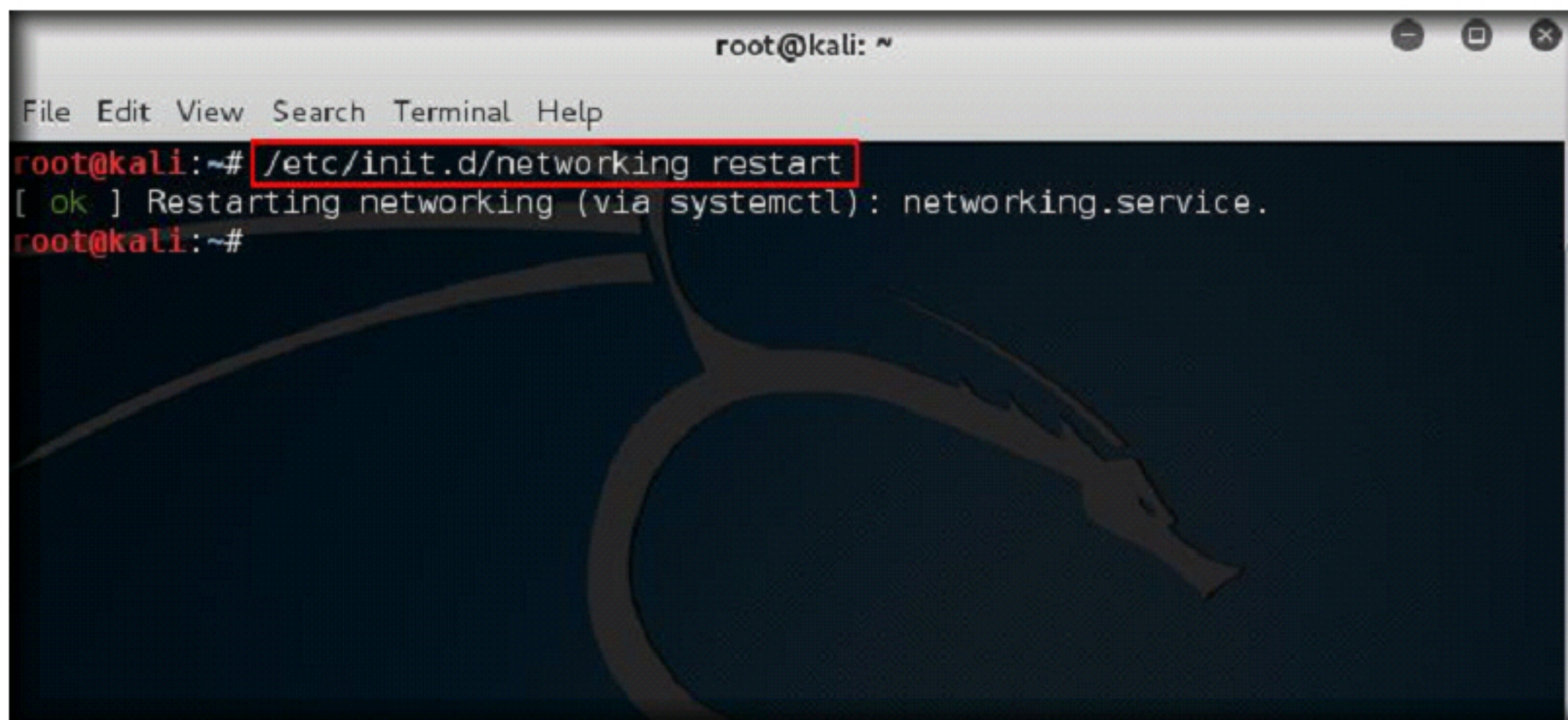
auto eth0
iface eth0 inet static
address 192.168.0.7
netmask 255.255.255.0
gateway 192.168.0.1

auto eth1
iface eth1 inet static
address 10.0.0.11
netmask 255.0.0.0
gateway 10.0.0.1

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS
```


40. Once done, close the file and restart the interfaces by issuing the command **/etc/init.d/networking restart** in command line terminal

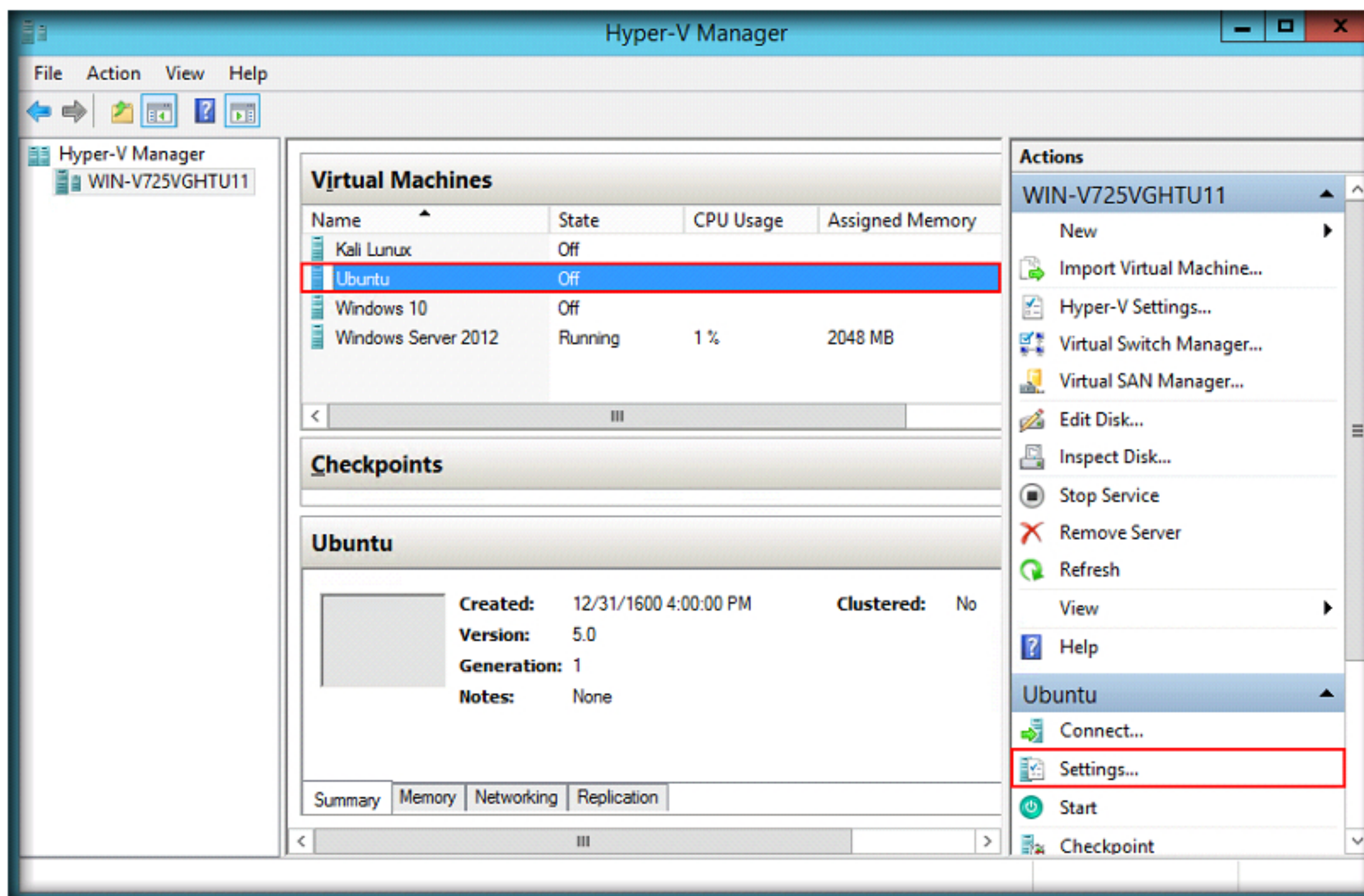
Note: If an error occurs while the restarting the network interfaces, restart the Kali Linux virtual machine



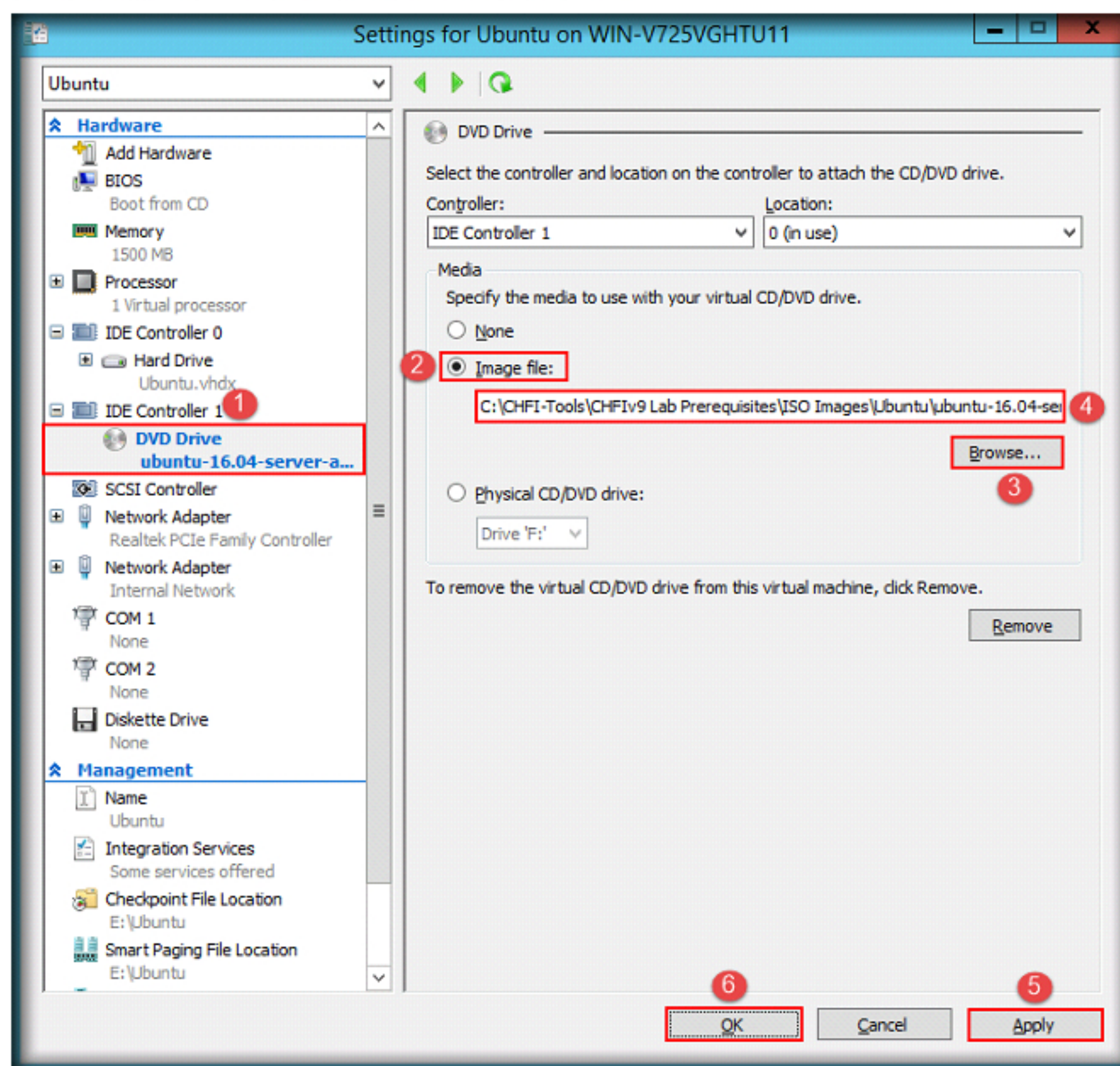
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# /etc/init.d/networking restart  
[ ok ] Restarting networking (via systemctl): networking.service.  
root@kali:~#
```

CT#22: Install Ubuntu in Hyper-V

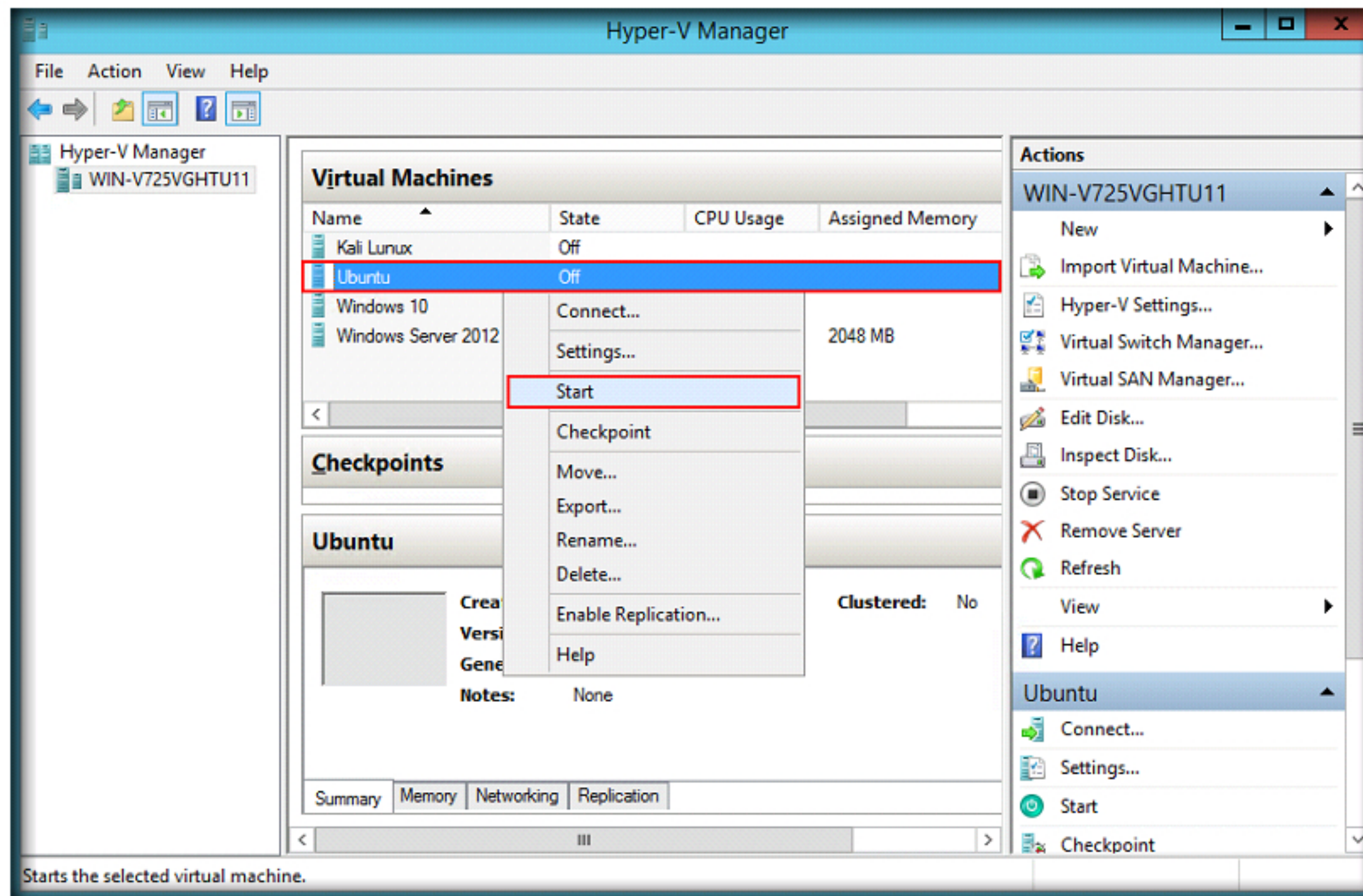
1. Launch Hyper-V Manager, select **Ubuntu** virtual machine and click **settings**



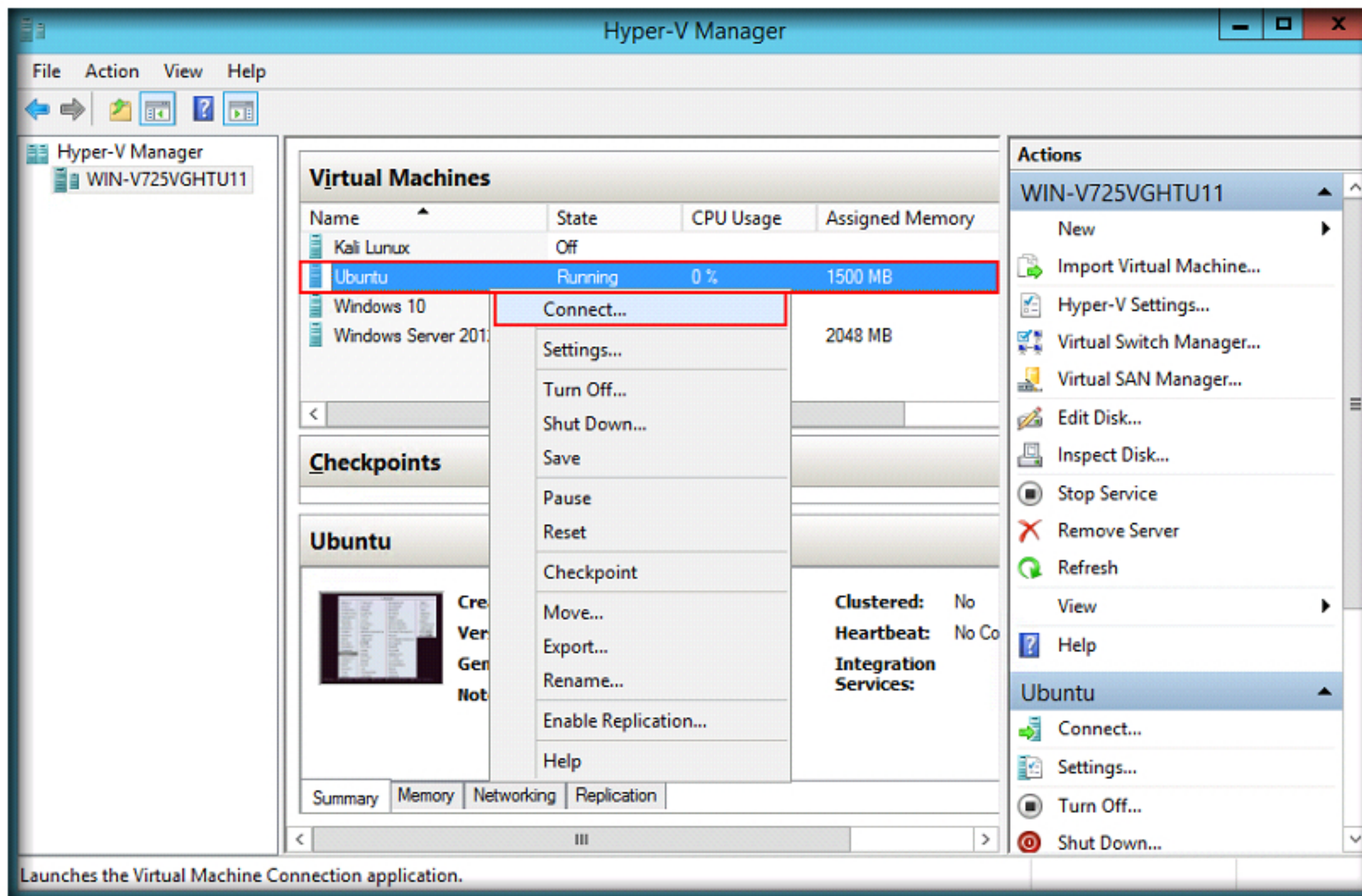
2. **Settings for Ubuntu** window appears
3. Click **DVD drive** option in the left pane and click **Image file** radio button in the right pane
4. Click **Browse** button, navigate to **C:\CHFI-Tools\CHFIv9 Lab Prerequisites\ISO Images\Ubuntu** and select **ubuntu-16.04-server-amd64.iso**
5. Click **Apply** and then click **OK**. Settings for Ubuntu window **exits**.



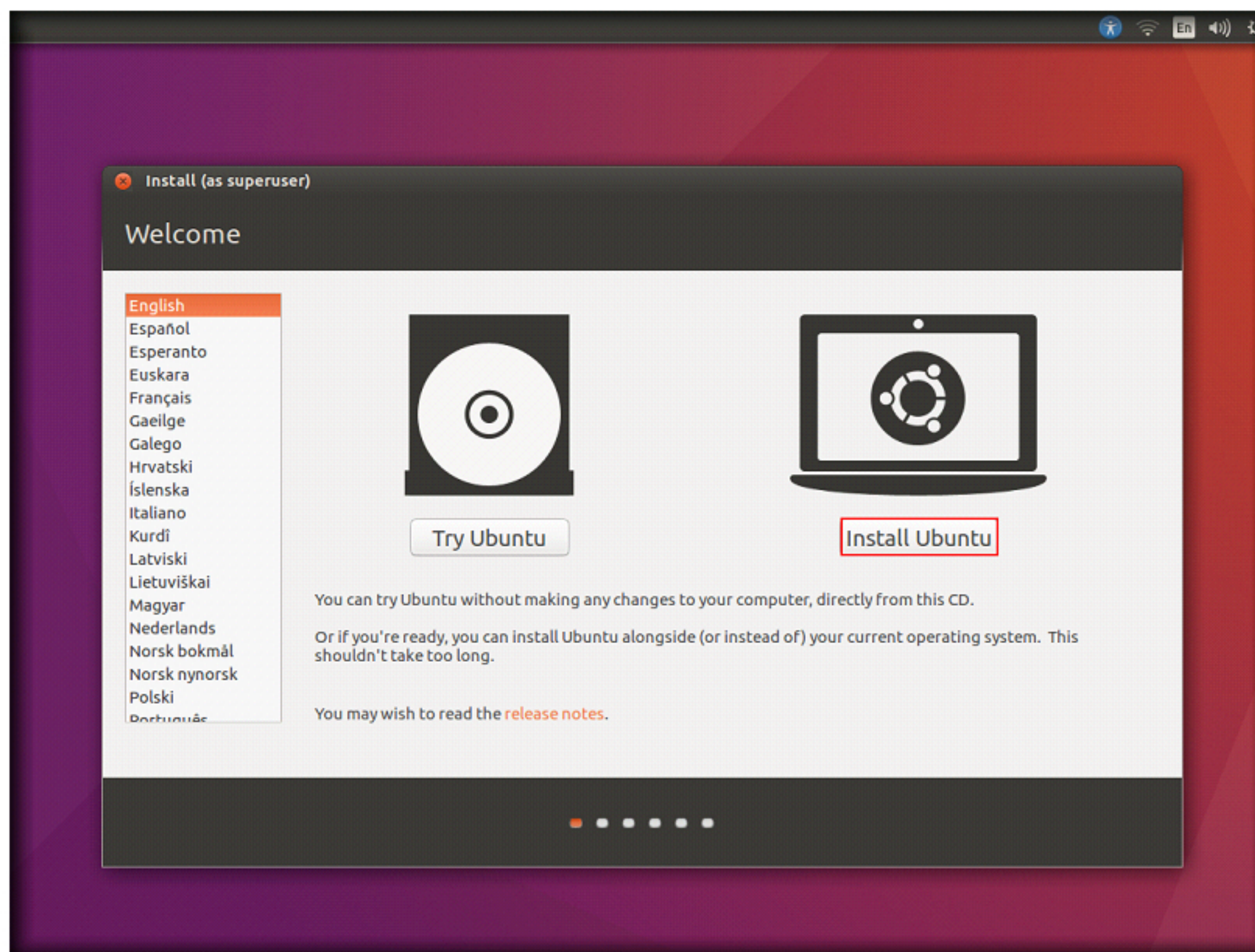
6. Right-click the **Ubuntu** virtual machine and click **Start**



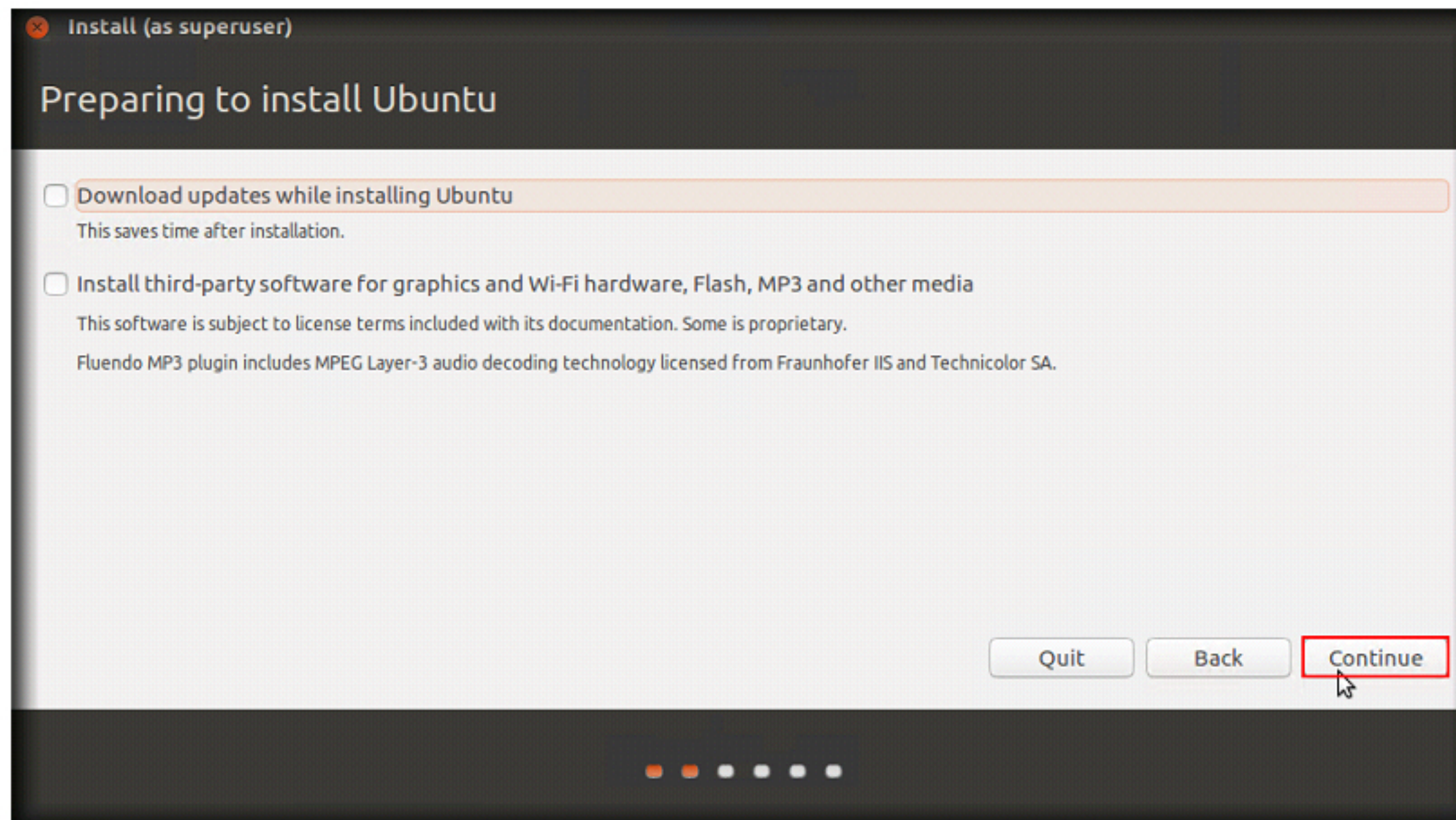
7. Again right-click the **Ubuntu** virtual machine and click **Connect...**



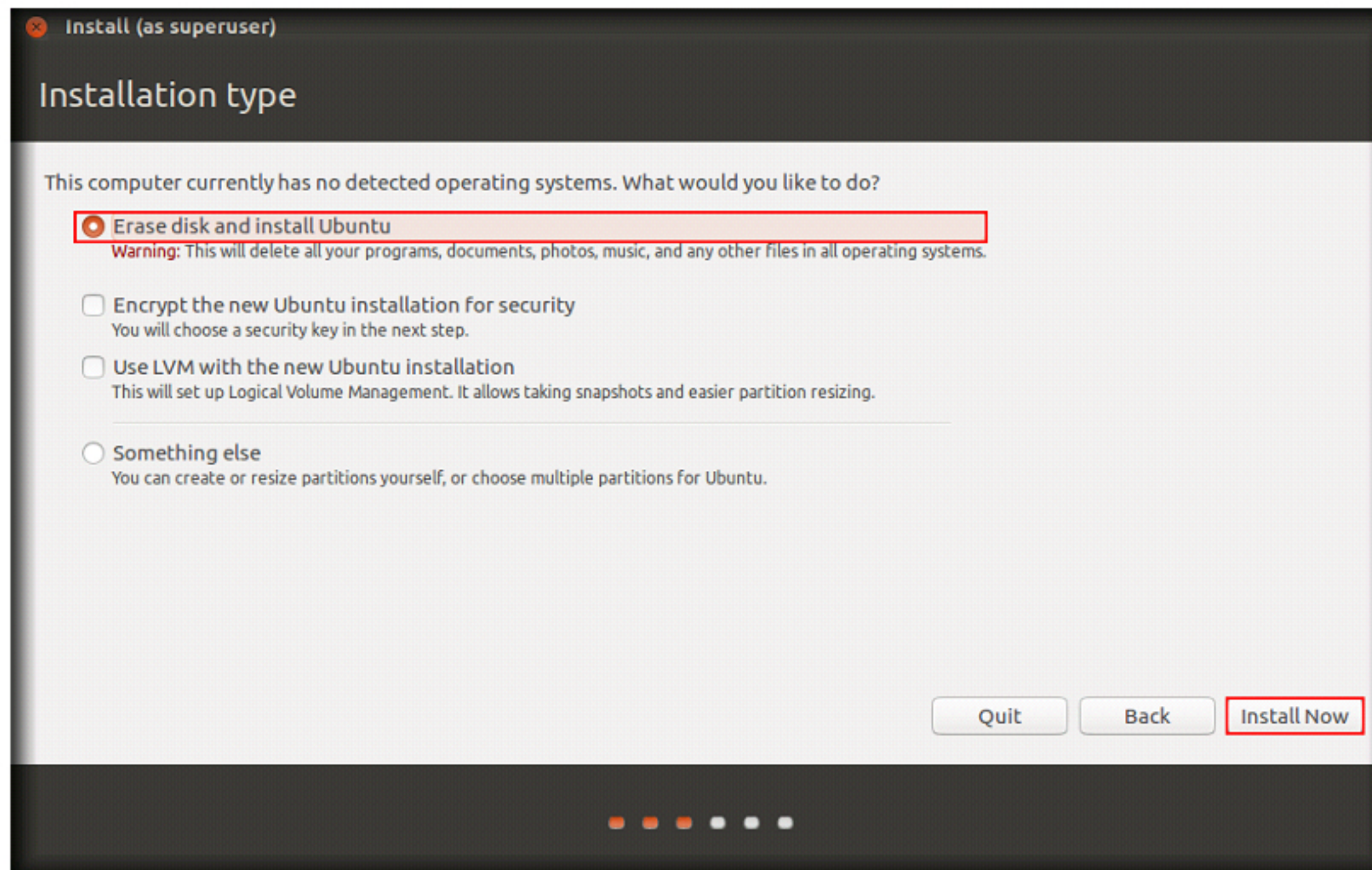
8. Ubuntu virtual machine installation GUI appears on the screen
9. Click **Install Ubuntu** button



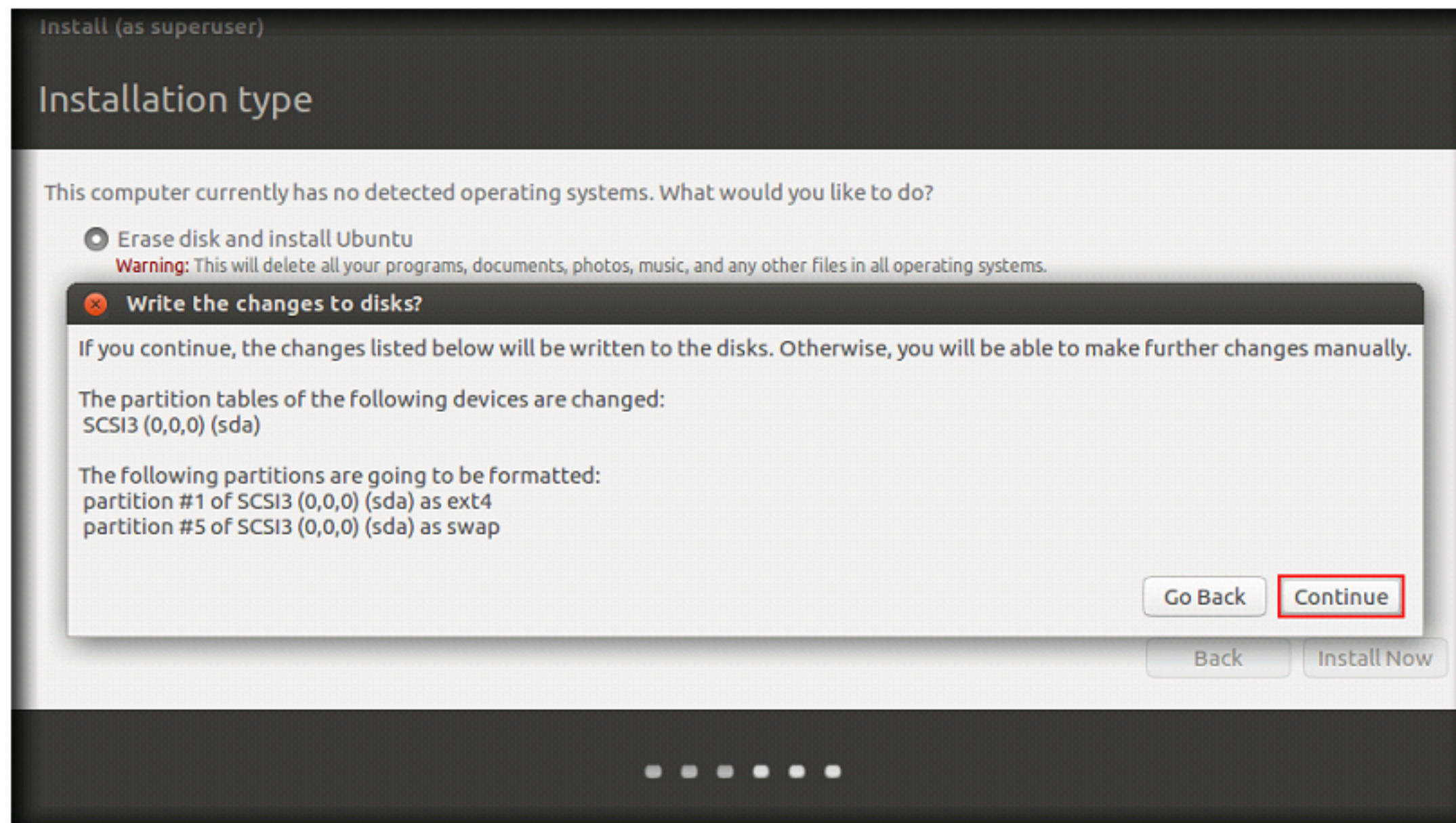
10. **Preparing to install Ubuntu** window appears. Leaving the options set to default, click **Continue**



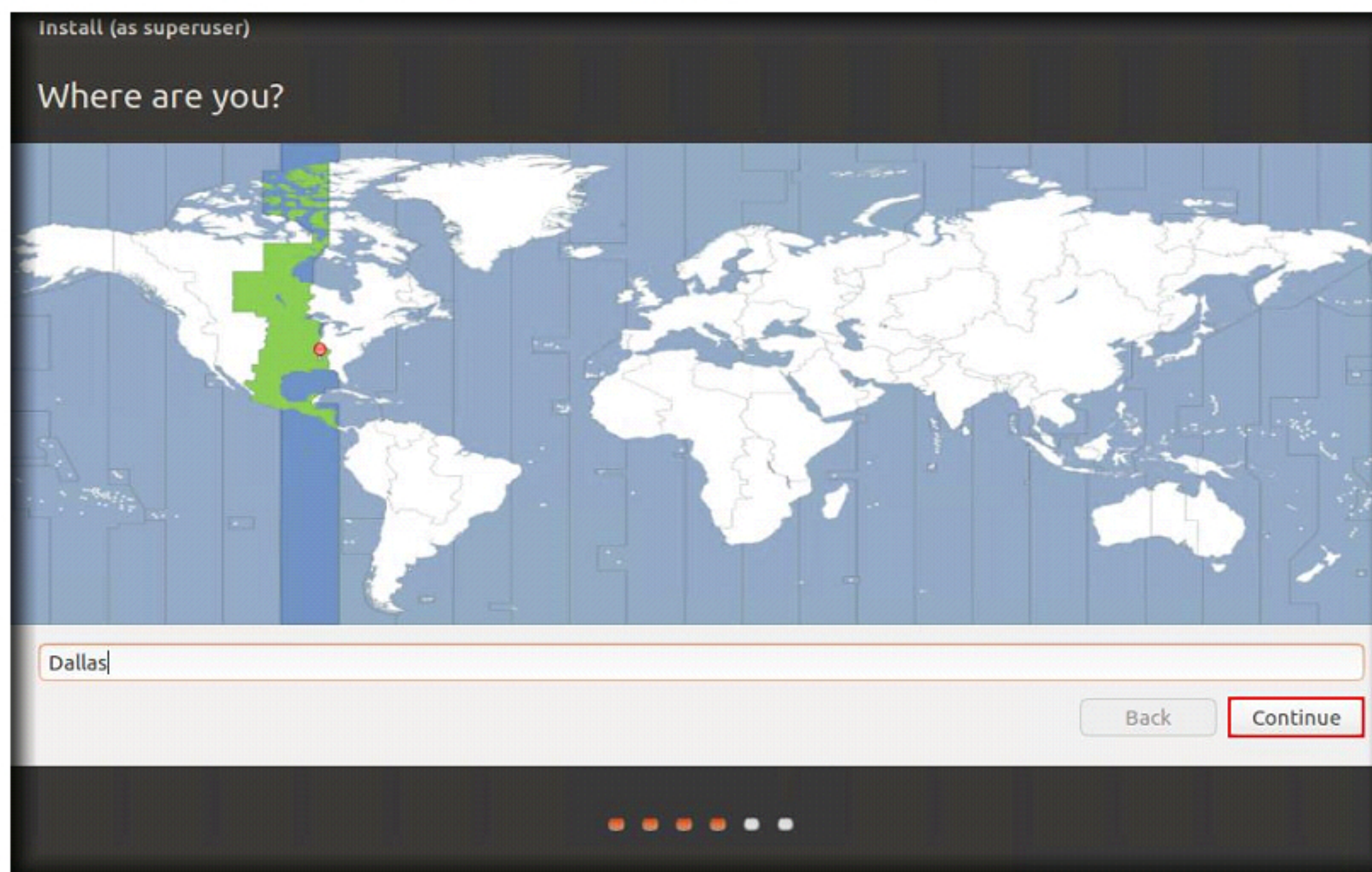
11. **Installation type** window appears, select **Erase disk and install Ubuntu** radio button and click **Install Now**



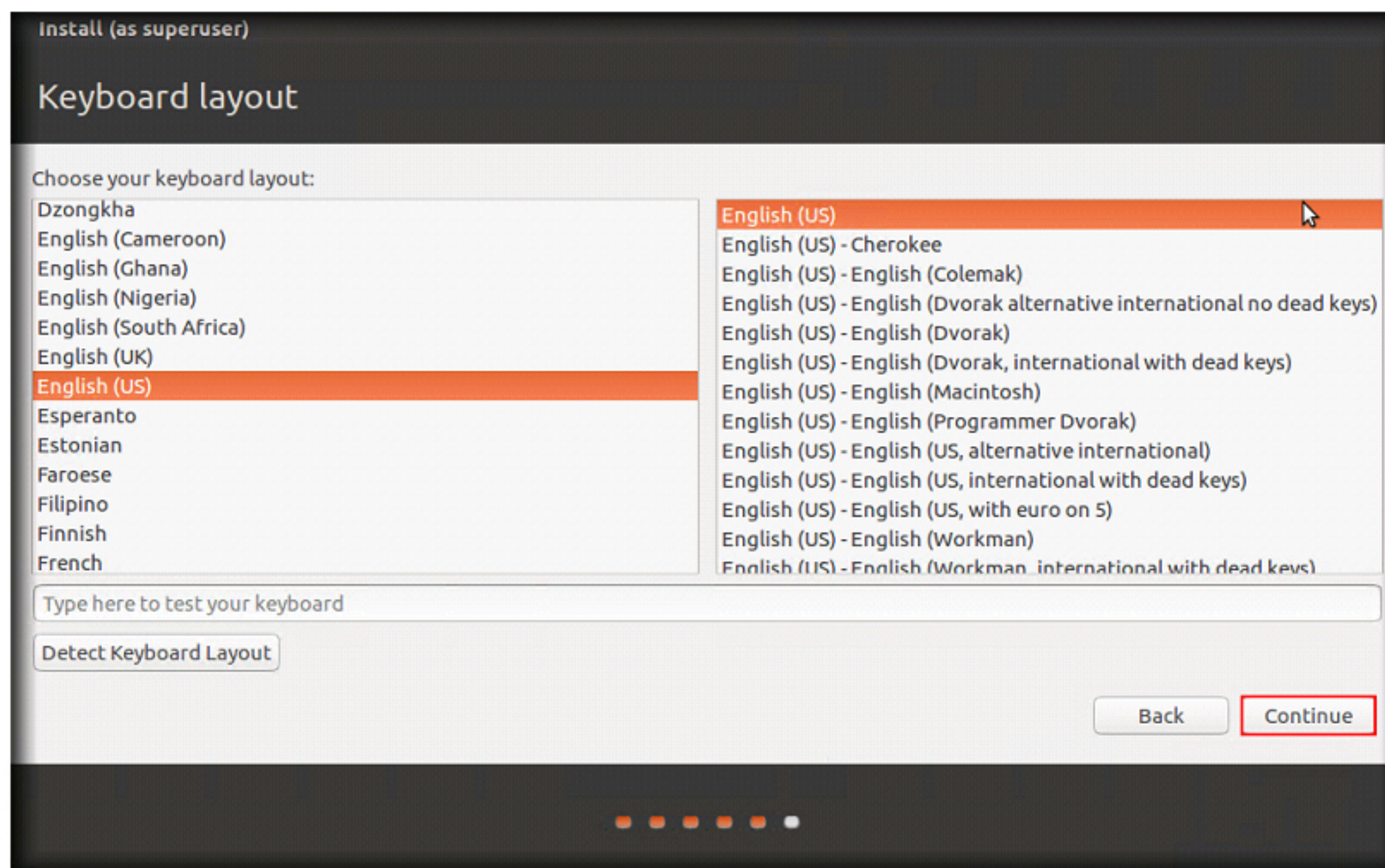
12. If a **Write the changes to disks?** dialog-box appears, click **Continue**



13. **Where are you?** window appears displaying your current geographical location/time zone. Click **Continue**.



14. **Keyboard layout** window appears, select the keyboard layout from the left pane and choose language from the right-pane and click **Continue**



15. **Who are you?** window appears; enter your name in **Your name** field, enter username as jason in **Pick a username** field, enter the password as **toor** in both **Choose a password** and **Confirm your password** fields, select **Require my password to log in** radio button and click **Continue**.

The screenshot shows the 'Who are you?' window from the Ubuntu installer. The window has a dark header with the text 'Install (as superuser)' and 'Who are you?'. The main area is light gray and contains several input fields and options. The 'Your name' field is filled with 'Jason' and has a green checkmark. The 'Your computer's name' field is filled with 'jason-Virtual-Machine' and has a green checkmark. Below it, a small text says 'The name it uses when it talks to other computers.' The 'Pick a username' field is filled with 'jason' and has a green checkmark. The 'Choose a password' field is filled with four black dots and has a red 'Short password' warning. The 'Confirm your password' field is also filled with four black dots and has a green checkmark. Below the password fields, there are three radio button options: 'Log in automatically' (unselected), 'Require my password to log in' (selected), and 'Encrypt my home folder' (unselected). At the bottom right, there are two buttons: 'Back' and 'Continue'. The 'Continue' button is highlighted with a red border. At the very bottom of the window, there are six small orange squares.

Install (as superuser)

Who are you?

Your name: Jason ✓

Your computer's name: jason-Virtual-Machine ✓
The name it uses when it talks to other computers.

Pick a username: jason ✓

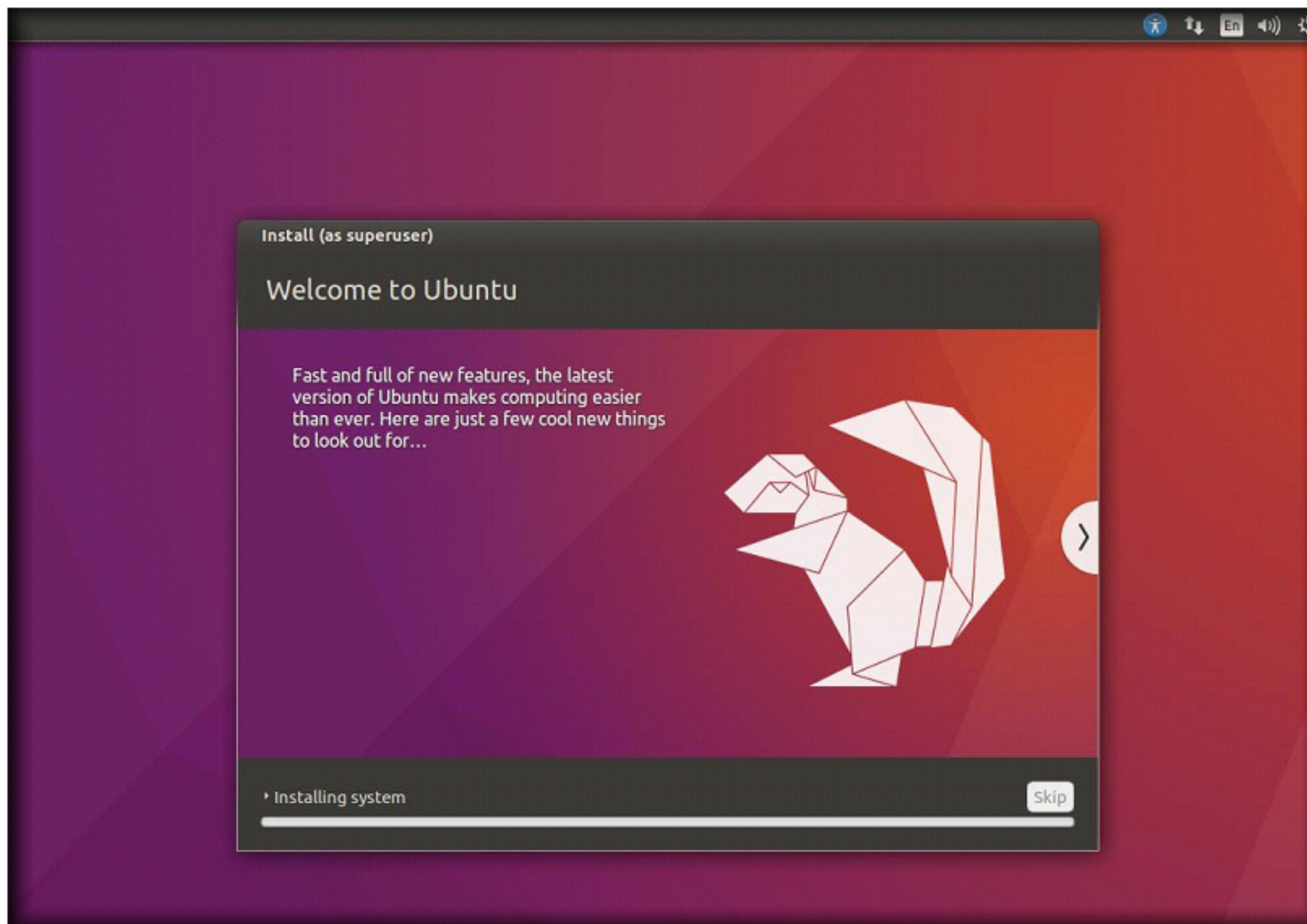
Choose a password: ●●●● Short password

Confirm your password: ●●●● ✓

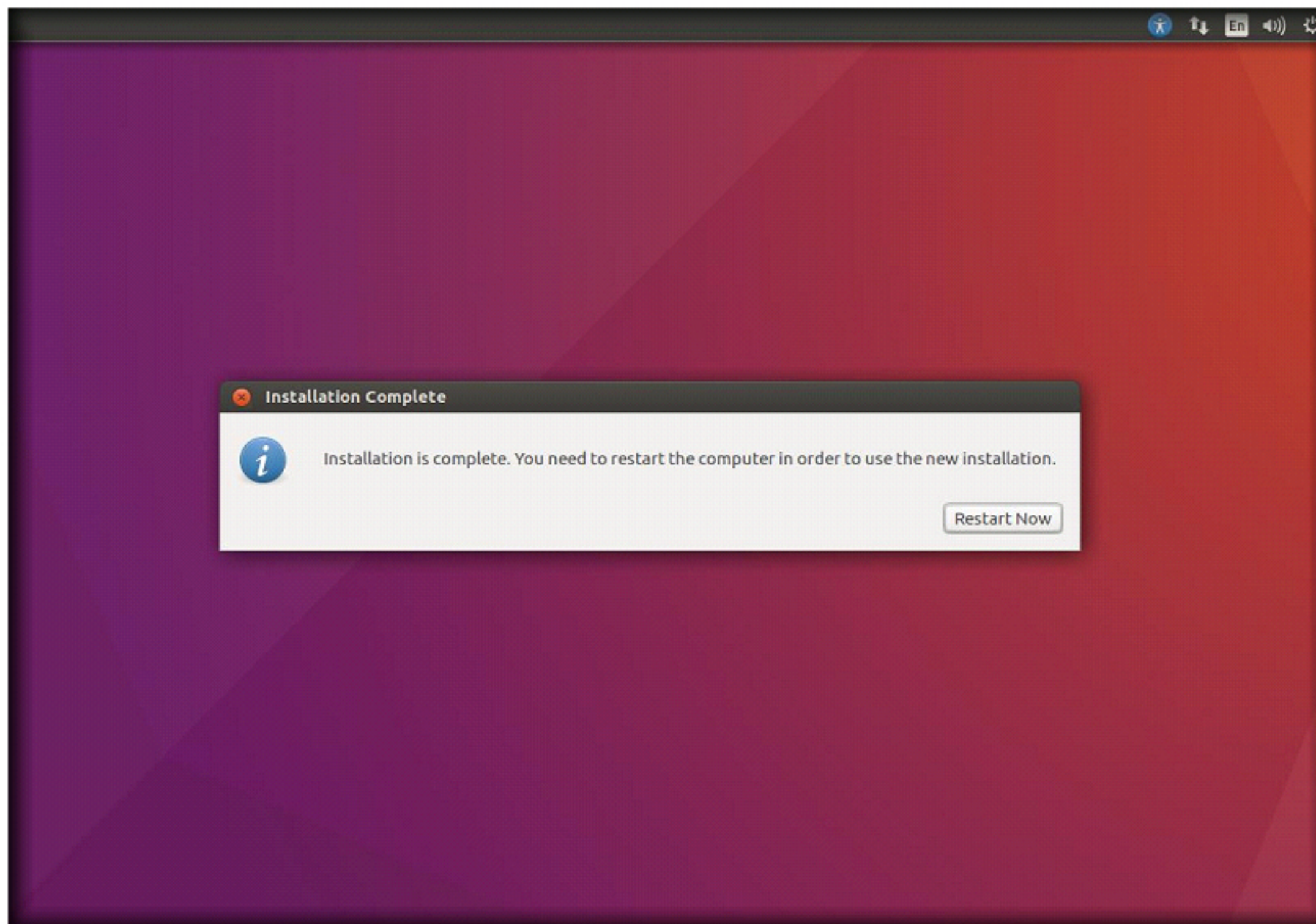
☐ Log in automatically
☒ Require my password to log in
☐ Encrypt my home folder

Back Continue

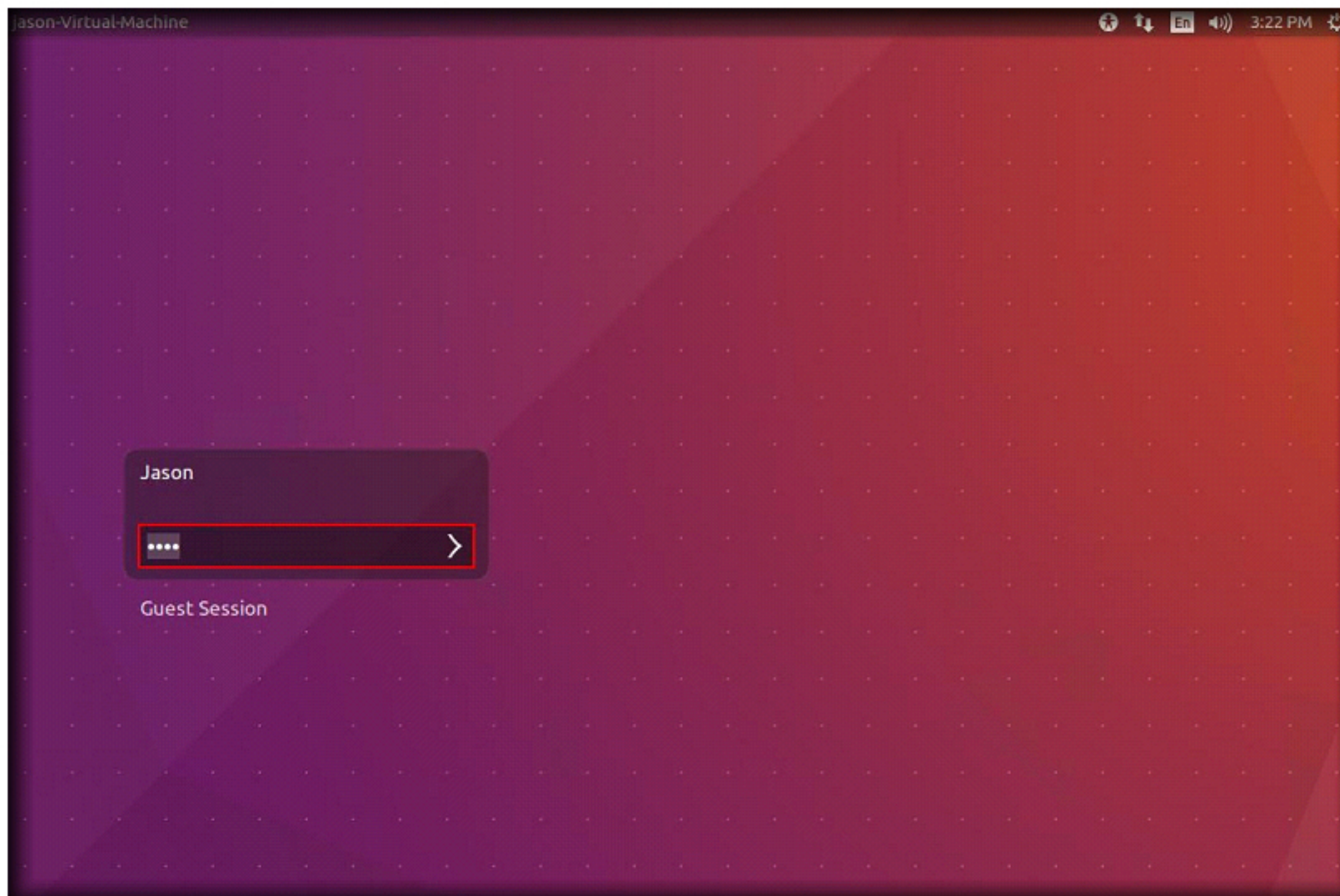
16. **Welcome to Ubuntu** window appears, wait until the installation is completed



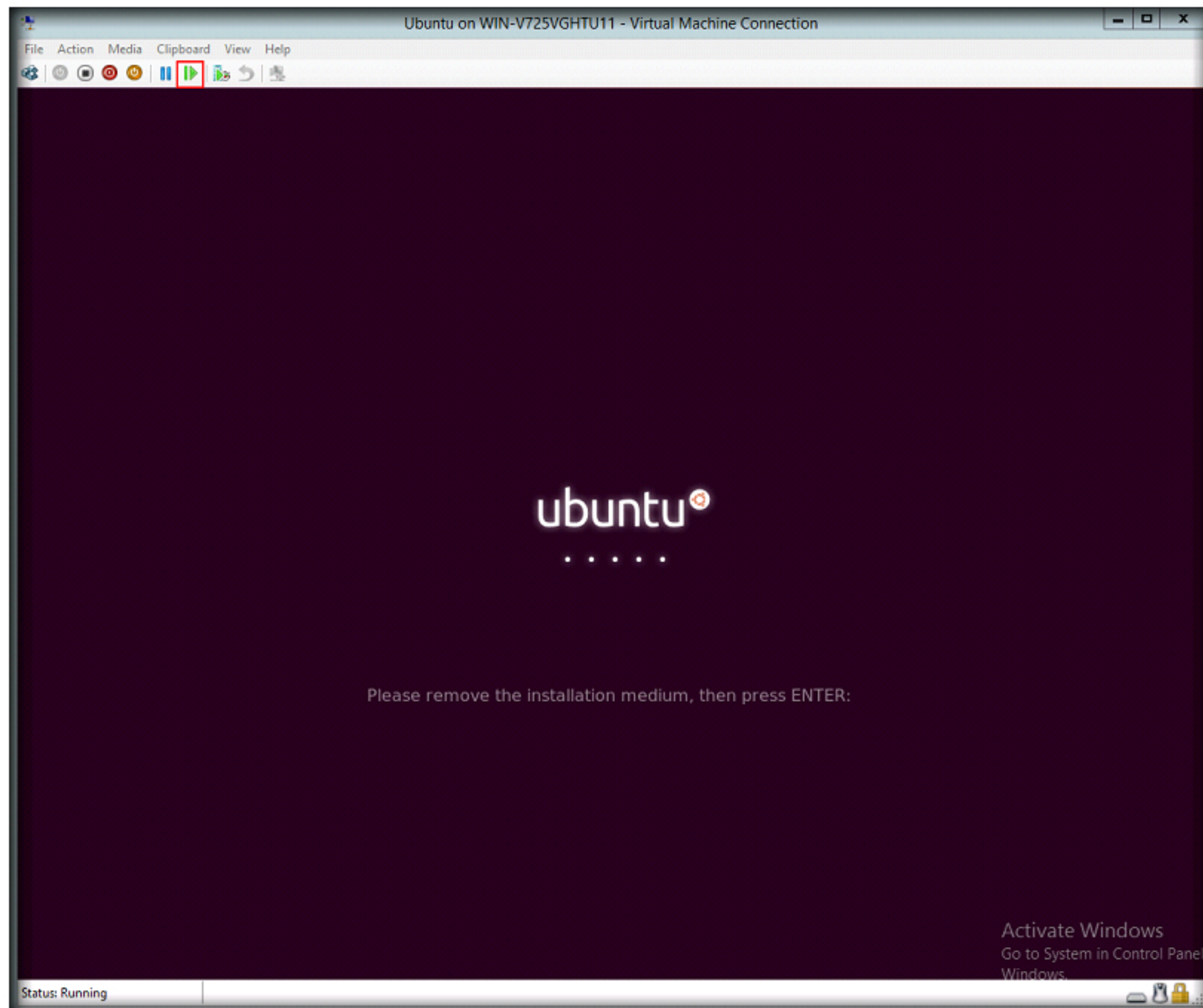
17. On completing the installation, click **Restart Now** button.



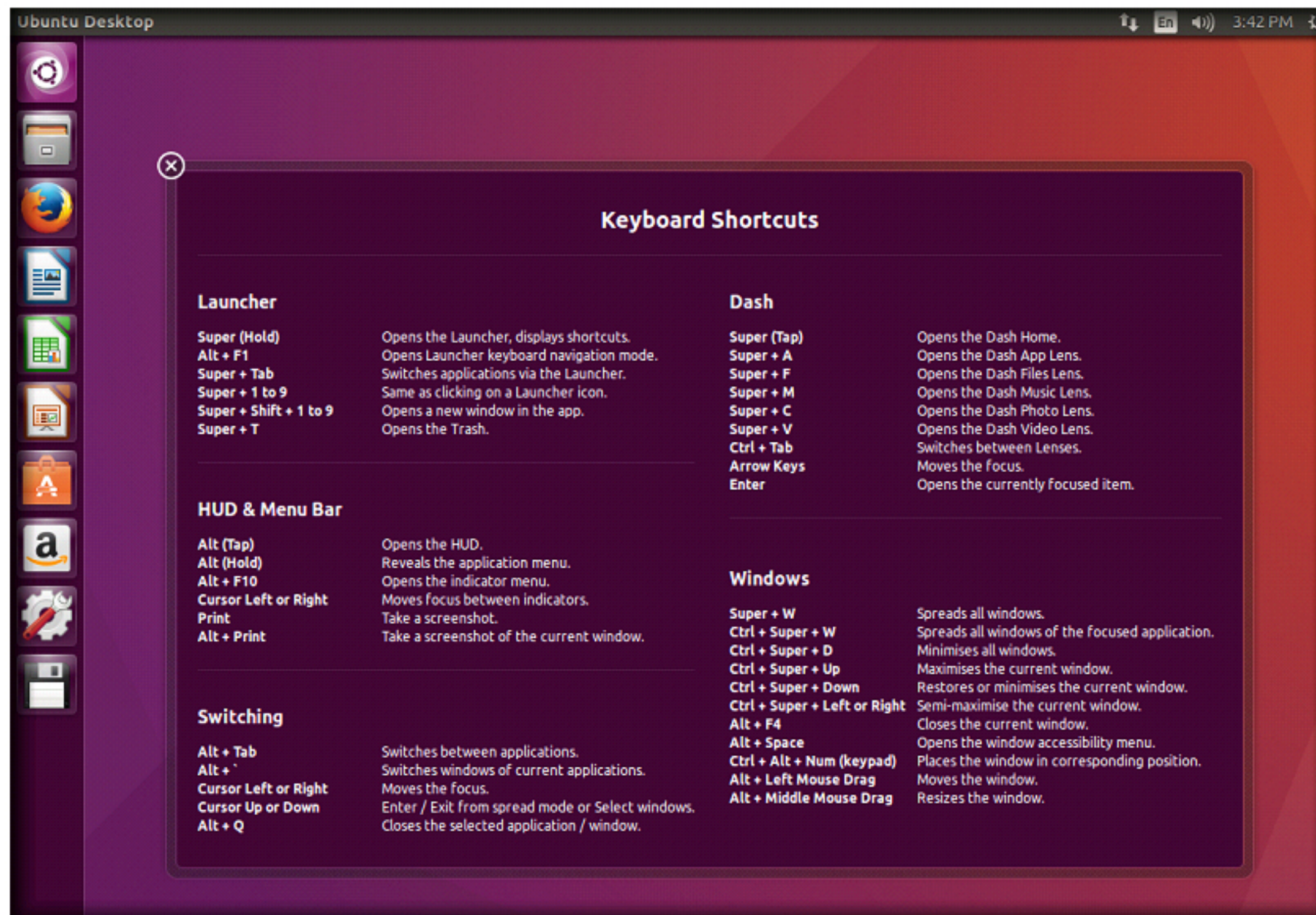
18. Once the machine is restarted, type the password (**toor**) and press **Enter**



Note: If a screen appears asking you to remove the installation medium, go to **Hyper-v** toolbar and click the **Reset** icon

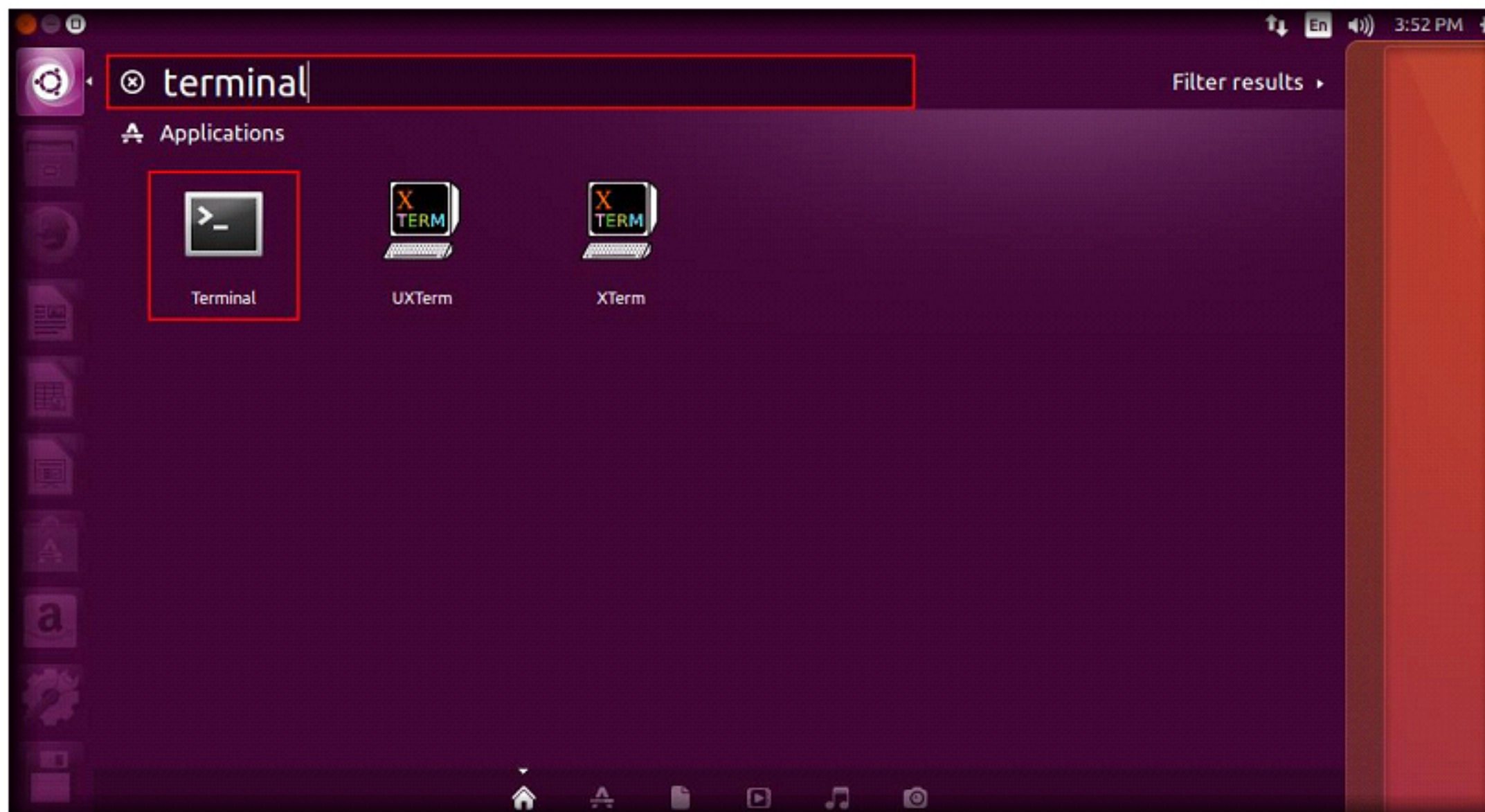


21. Ubuntu Desktop screen appears, displaying the **Keyboard Shortcuts** window. Close the window.



Note: While configuring the machine, an Upgrade pop-up may appear on the screen, asking you to upgrade the operating system. If that pop-up appears, click **Don't Upgrade** button.

22. Click **Search your computer** icon in the left pane, type **terminal** in the **Search** field and press **Enter**

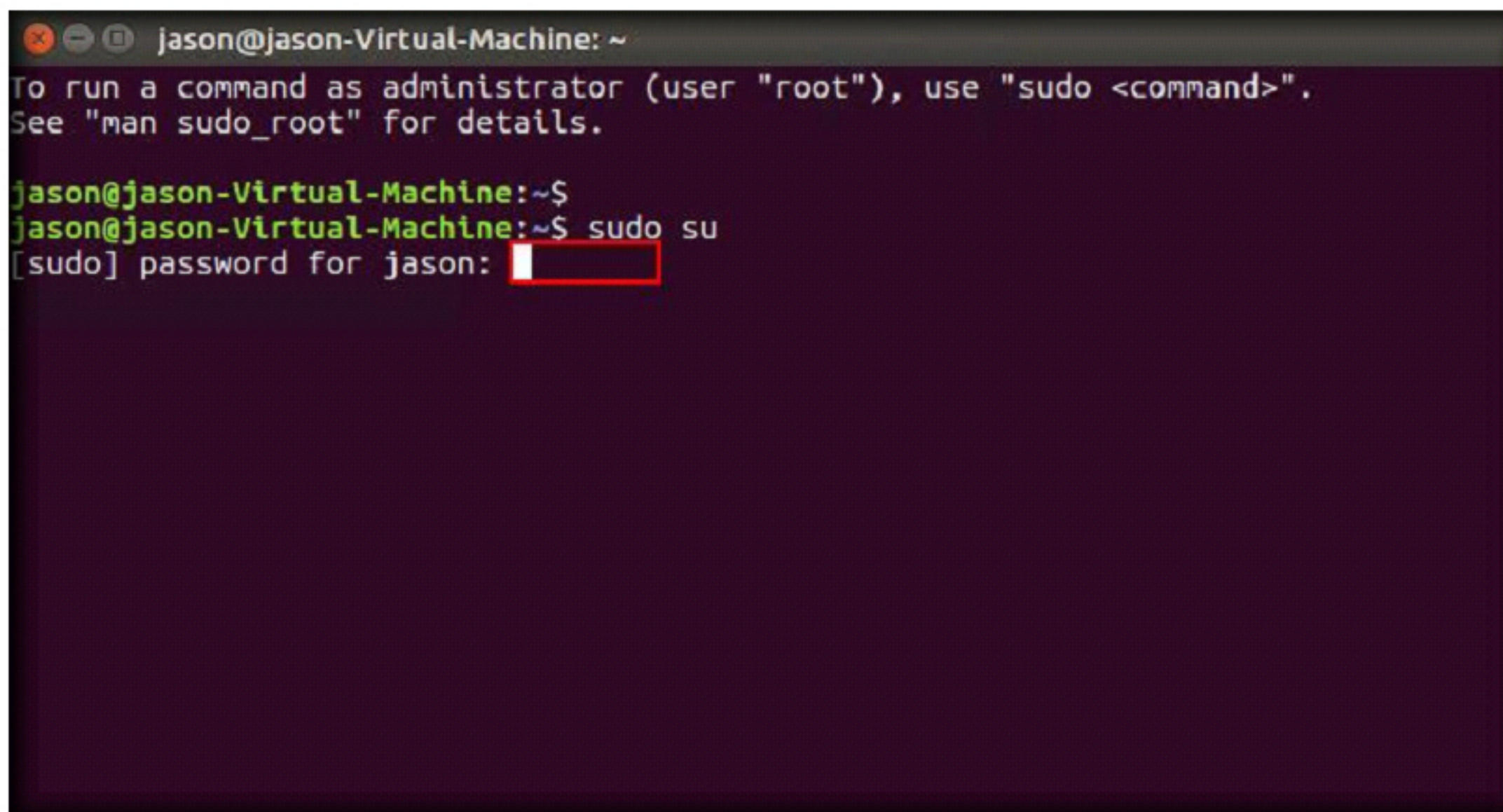


23. Terminal appears on the screen, type **sudo su** and press **Enter**

A terminal window titled 'jason@jason-Virtual-Machine: ~' with standard window controls. It displays a message: 'To run a command as administrator (user "root"), use "sudo <command>". See "man sudo_root" for details.' Below this, the prompt 'jason@jason-Virtual-Machine:~\$' is followed by the command 'sudo su' which is highlighted with a yellow box.

```
jason@jason-Virtual-Machine: ~  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
jason@jason-Virtual-Machine:~$ sudo su
```

24. You will be prompted to enter a password. Type the password as **toor** and press **Enter**. The password which you type will not be visible.

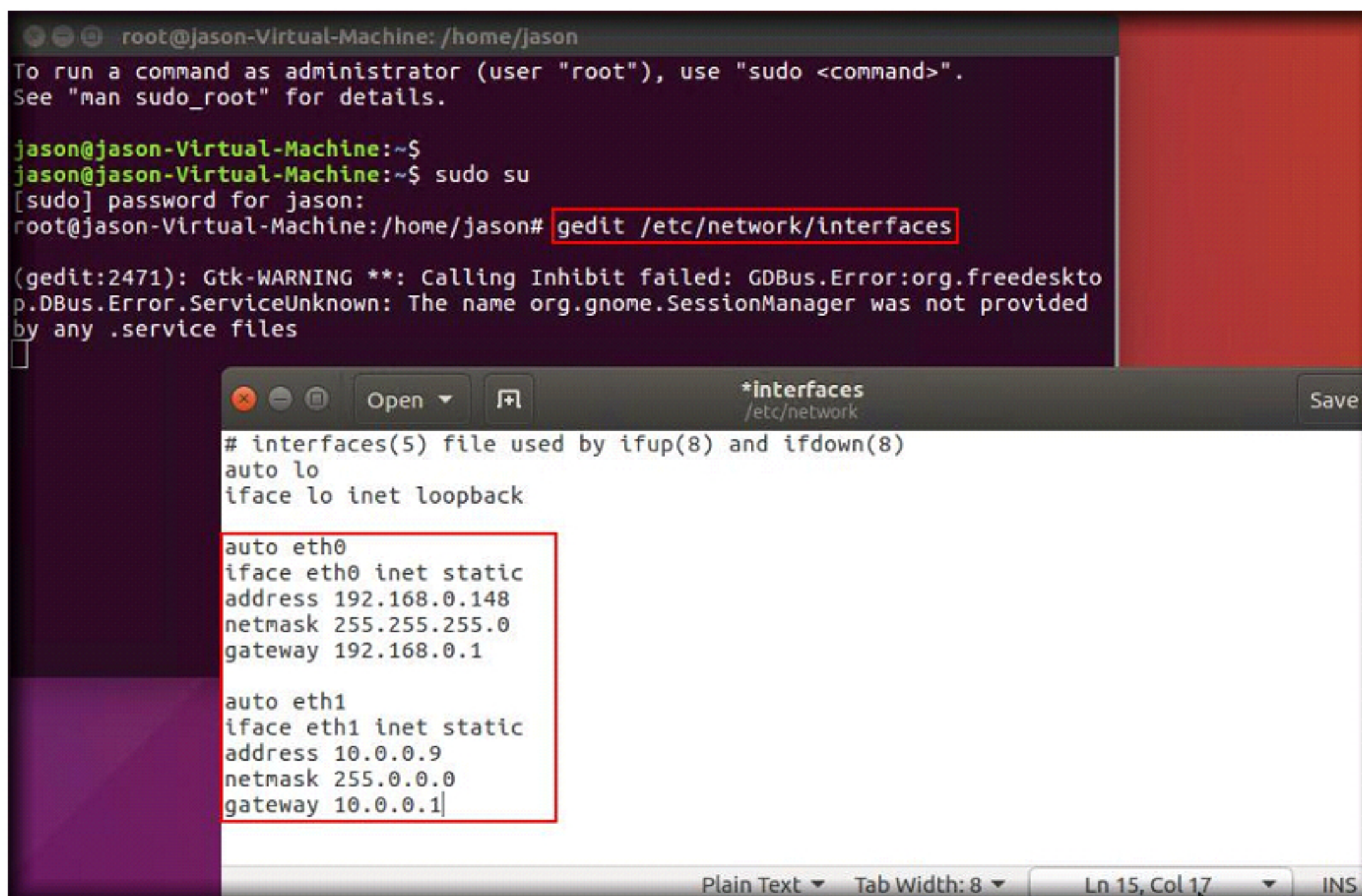


```

x  ←  □  jason@jason-Virtual-Machine: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jason@jason-Virtual-Machine:~$
jason@jason-Virtual-Machine:~$ sudo su
[sudo] password for jason: 
```


25. Type the command **gedit /etc/network/interfaces** and press **Enter**
26. Interfaces file appears in gedit text editor window. Now, add the following lines in the file and **save** it:
- | | |
|--|----------------------------------|
| a. auto eth0 | f. auto eth1 |
| b. iface eth0 inet static | g. iface eth1 inet static |
| c. address [IP Address of External Network] | h. address 10.0.0.9 |
| d. netmask 255.255.255.0 | i. netmask 255.0.0.0 |
| e. gateway 192.168.0.1 | j. gateway 10.0.0.1 |



```
root@jason-Virtual-Machine: /home/jason
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jason@jason-Virtual-Machine:~$
jason@jason-Virtual-Machine:~$ sudo su
[sudo] password for jason:
root@jason-Virtual-Machine:/home/jason# gedit /etc/network/interfaces

(gedit:2471): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.0.148
netmask 255.255.255.0
gateway 192.168.0.1

auto eth1
iface eth1 inet static
address 10.0.0.9
netmask 255.0.0.0
gateway 10.0.0.1
```

27. Close the file

28. Now, we need to restart the network interfaces, so that the machine takes the assigned external and internal IP addresses. To do this, we shall disable the interfaces and then, enable them.
29. Type the command **ifdown -a** to disable all the interfaces

```
root@jason-Virtual-Machine: /home/jason
root@jason-Virtual-Machine:/home/jason# /etc/init.d/networking restart
* Running /etc/init.d/networking restart is deprecated because it may not enable
e again some interfaces
* Reconfiguring network interfaces... [ OK ]
root@jason-Virtual-Machine:/home/jason#
```

30. Type the command **ifup -a** to enable all the interfaces

```
root@jason-Virtual-Machine: /home/jason
root@jason-Virtual-Machine:/home/jason# gedit /etc/network/interfaces
(gedit:2370): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided
by any .service files
** (gedit:2370): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2370): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2370): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
root@jason-Virtual-Machine:/home/jason# ifdown -a
root@jason-Virtual-Machine:/home/jason# ifup -a
RTNETLINK answers: File exists
Failed to bring up eth0.
root@jason-Virtual-Machine:/home/jason#
```


31. If you are facing any network related issues, or if the IP addresses are not properly bound to the interfaces, you need to reboot the machine
32. Now, type **ifconfig** and press **Enter** to ensure that the IP addresses are assigned to the interfaces

```
root@jason-Virtual-Machine: /home/jason
root@jason-Virtual-Machine:/home/jason# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:27:0a
          inet addr:192.168.0.148  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe00:270a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:136831 errors:0 dropped:165 overruns:0 frame:0
          TX packets:1396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19235982 (19.2 MB)  TX bytes:125288 (125.2 KB)

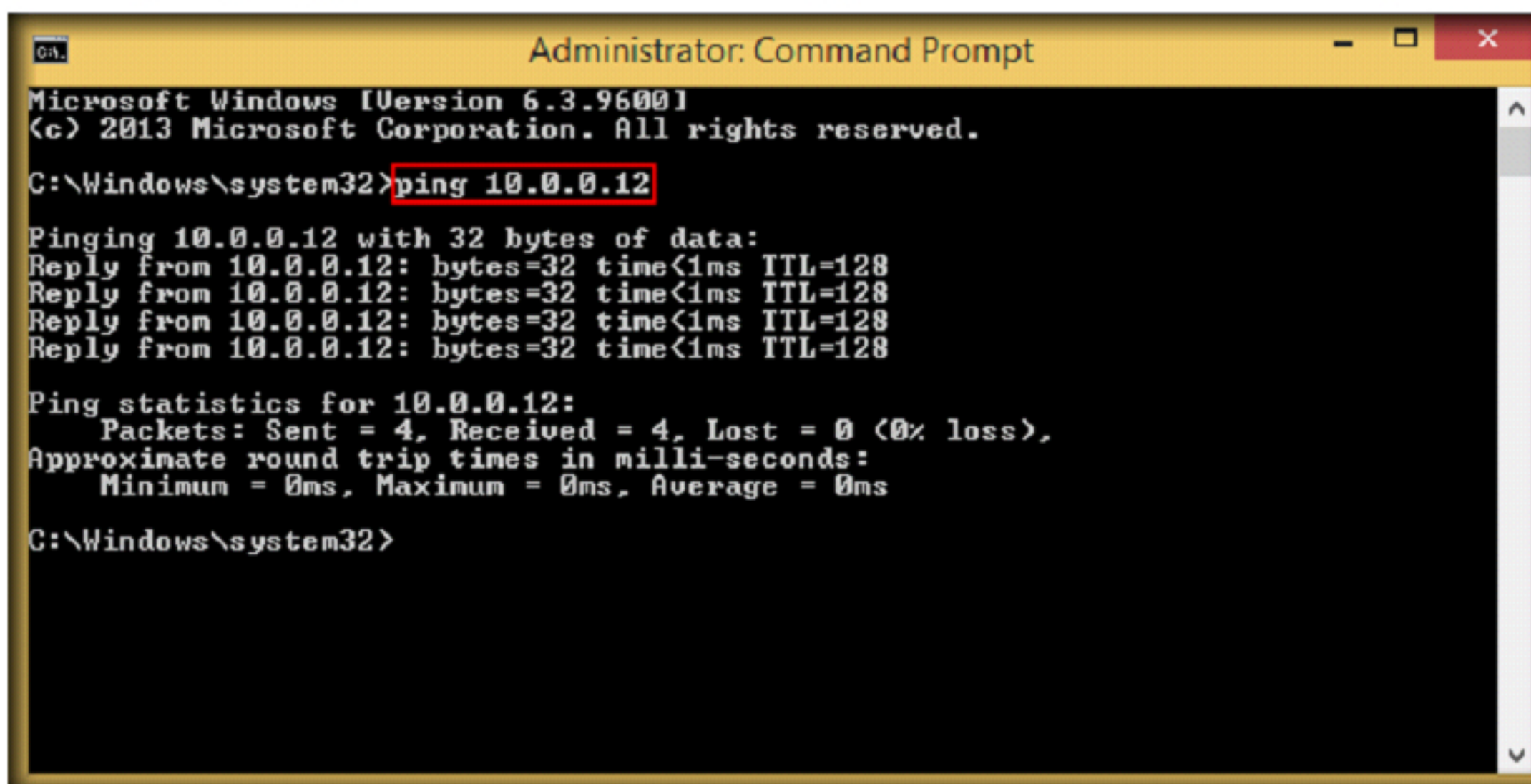
eth1      Link encap:Ethernet  HWaddr 00:15:5d:00:27:0b
          inet addr:10.0.0.9  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::215:5dff:fe00:270b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:181 errors:0 dropped:0 overruns:0 frame:0
          TX packets:173 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24859 (24.8 KB)  TX bytes:20206 (20.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:18368 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1359496 (1.3 MB)  TX bytes:1359496 (1.3 MB)

root@jason-Virtual-Machine:/home/jason#
```


CT#23: Test for Pinging Each Other

1. Before pinging the virtual machines, make sure that the **Virtual Machine are up and running**
2. Check for the reply from the Virtual Machines. Here as an example, we are using **Windows 10** Virtual Machine with the IP address **10.0.0.8**
3. Launch command prompt in one of the **Virtual Machines**. Here as an example, we are using **Windows 10** virtual machine.
4. Now, type in command line **Ping 10.0.0.12** (IP Address of Windows Server 2012), and check for the **Reply**
5. Ensure that you are getting a reply from the machine without any packet loss as shown in the following screenshot:



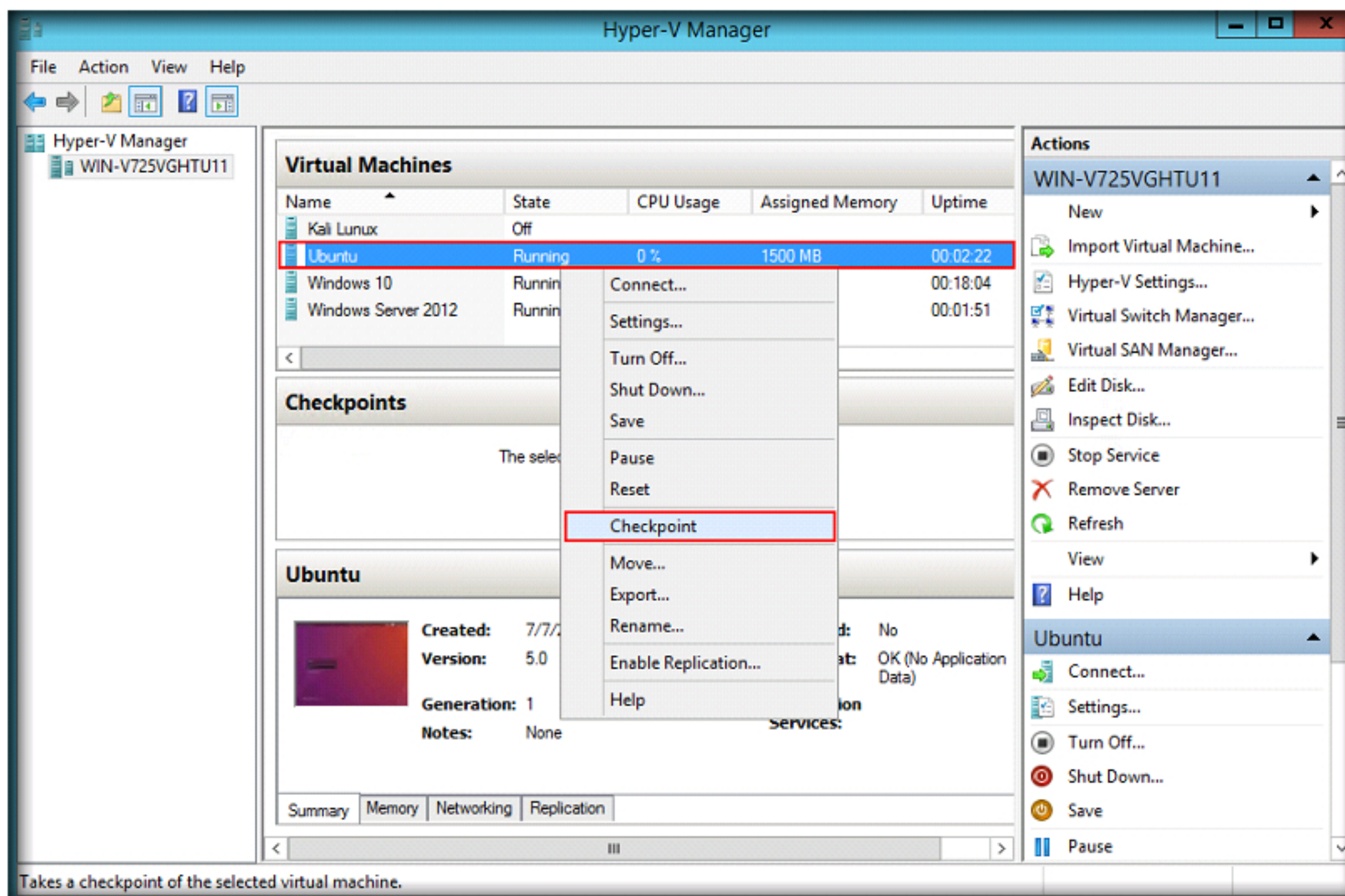
```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>ping 10.0.0.12
Pinging 10.0.0.12 with 32 bytes of data:
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Windows\system32>
```

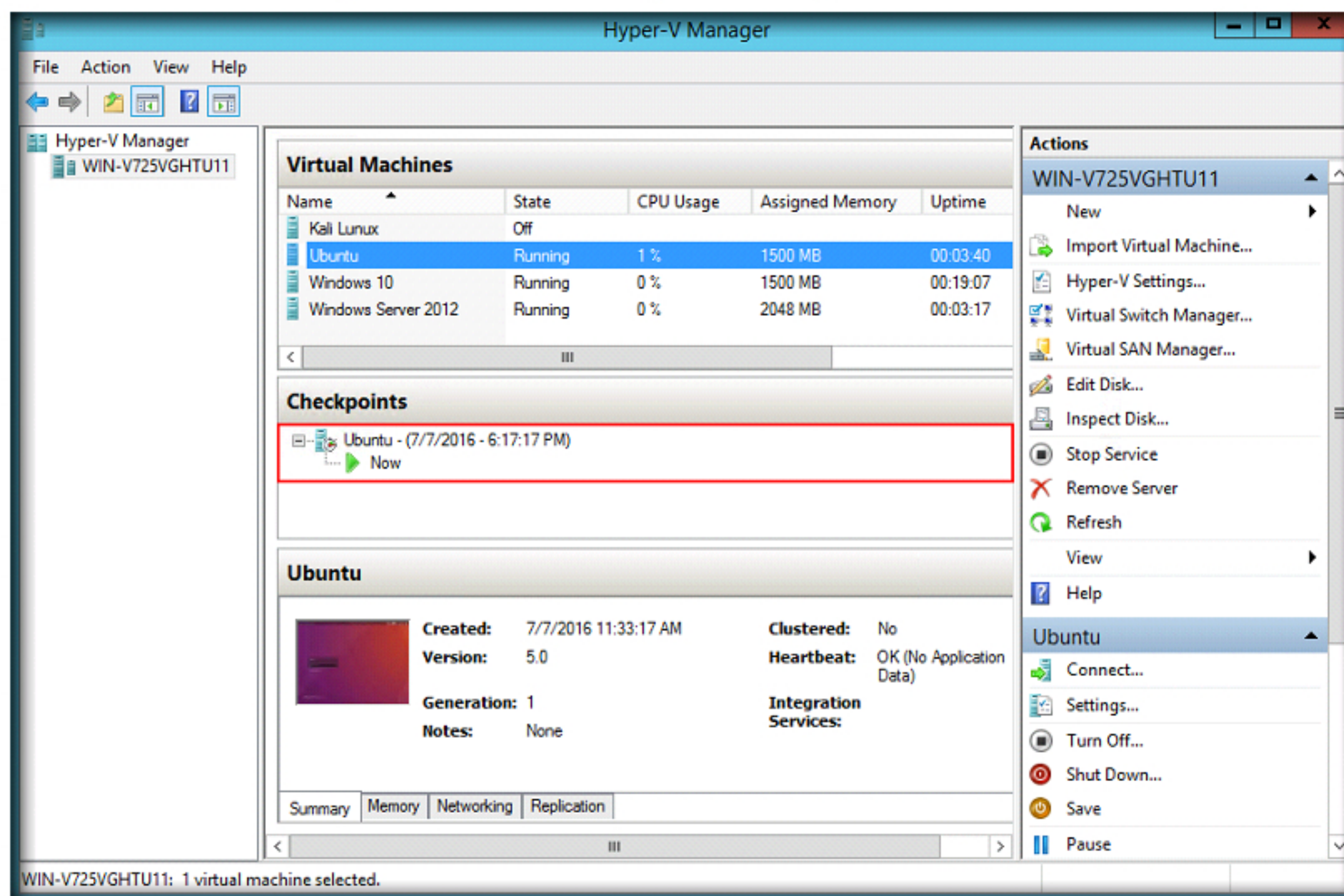
6. **Repeat** the above steps to ping all the Virtual Machines

CT#24: Create Checkpoints for all Virtual Machines

1. After installing all the guest operating systems on virtual machines, set Checkpoints of these virtual machines. Checkpoints can be used to **restore** virtual machines in case of **any problem** in the virtual machines
2. Open Hyper-V Manager, **right-click** on a virtual machine and click **Checkpoint**



3. Checkpoints will be **listed** in **Checkpoint** section of the Hyper-V Manager



4. Perform this action for **all** the virtual machines. Ensure that the machines are in **ON** state while taking checkpoints.

End of the Document