Trend Micro™

Virtual Analyzer Image Preparation Tool

7.0 September 2024 Update

User's Guide

Virtual Analyzer Image Preparation Tool User's Guide

Document Part No.: APEM79916/240722

Release Date: September 2024

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the tool and/or provides installation instructions for a production environment. Read through the documentation before installing or using the tool.

Detailed information about how to use specific features within the tool may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

https://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

Chapter 1: About this Guide

Document Conventions 1-2

Audience 1-3

Terminology 1-3

Chapter 2: Windows OVA File Creation Using New Virtual Machine Images

Creating Windows OVA Files Using New Virtual Machine Images 2-2

- Required Software 2-2
- Downloading and Installing VirtualBox 2-7
- Creating Windows Virtual Machine Images 2-9
- Modifying the Virtual Machine Environment 2-28
  - Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003) 2-29
  - Modifying the Virtual Machine Environment (All Other Supported Windows Versions) 2-31
- Reducing the Size of VirtualBox Disk Images 2-44
- Exporting Virtual Machine Images to OVA Files 2-45

Chapter 3: Windows OVA File Creation Using Converted Virtual Hard Disk Drives

Creating Windows OVA Files Using Converted Virtual Hard Disk Drives 3-2

- Required Software 3-2
  - Preparing Adobe Reader 3-7
- Modifying the Virtual Machine Environment 3-8
  - Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003) 3-8
  - Modifying the Virtual Machine Environment (All Other Supported Windows Versions) 3-11

Uninstalling VMware Tools 3-24
Exporting Virtual Machine Images 3-26
Verifying Virtual Machine Settings on VMware Workstation 3-27
Exporting Virtual Machine Images on VMware ESXi 3-29
Converting VMware ESXi Virtual Hard Disk Drives .. 3-33
Using VMware vCenter Converter Standalone ... 3-33
Using QEMU 3-39
Creating Virtual Machine Images Using Converted Virtual Hard Disk Drives 3-40
Downloading and Installing VirtualBox 3-40
Creating Virtual Machine Images Using VirtualBox . 3-41
Configuring Virtual Machine Images 3-59
Configuring Virtual Machine Images (Windows XP and Windows Server 2003) 3-60
Configuring Virtual Machine Images (All Other Supported Windows Versions) 3-63
Exporting Virtual Machine Images to OVA Files 3-64

Chapter 4: Linux OVA File Preparation

Creating Linux OVA Files From Scratch 4-3
Required Software 4-3
Downloading and Installing VirtualBox 4-12
Creating Linux Virtual Machine Images 4-13
CentOS and RHEL Installation 4-33
Ubuntu Installation 4-38
Modifying the Virtual Machine Environment 4-43
Modifying the Virtual Machine Environment 4-44
Exporting Virtual Machine Images to OVA Files 4-45

Chapter 5: Virtual Analyzer Image Preparation Tool

Overview 5-2
System Requirements 5-3
Image Validation and Configuration 5-4

Using the Tool 5-6
Products Not Activated - Windows 5-20
Sandbox Preparation Unsuccessful - Missing Windows Software 5-22
Sandbox Preparation Unsuccessful - Missing Linux Packages 5-24
Troubleshooting Common Issues 5-25
Sample Logs 5-32

Index

Index IN-1

Chapter 1

About this Guide

This User's Guide provides information on how to prepare custom Virtual Analyzer images in the following topics:

- *Windows OVA File Creation Using New Virtual Machine Images on page 2-1*
- *Windows OVA File Creation Using Converted Virtual Hard Disk Drives on page 3-1*
- *Linux OVA File Preparation on page 4-1*
- *Virtual Analyzer Image Preparation Tool on page 5-1*

Document Conventions

The documentation uses the following conventions:

TABLE 1-1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

Audience

This User Guide is intended for administrators who need to create custom sandbox images for Virtual Analyzer. The document assumes a working knowledge of networks and information security, including the following topics:

- Deploying and administering Deep Discovery or TippingPoint products
- Using Oracle VM VirtualBox™ or VMware™ products

Terminology

Terminology	Description
Open Virtual Appliance (OVA)	A ready-to-use software package (operating system with applications) that does not require additional configuration or installation. Virtual Analyzer supports only image files in the Open Virtual Appliance (OVA) format.
Sandbox image	A template used to deploy sandbox instances in Virtual Analyzer. A sandbox image includes an operating system, installed software, and other settings necessary for that specific computing environment.
Sandbox instance	A single virtual machine based on a sandbox image.
Virtual Analyzer	A secure virtual environment that manages and analyzes objects submitted by integrated products and administrators. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings.
Virtual Analyzer Sensors	A collection of utilities that execute and detect malware, and record all behavior in Virtual Analyzer.
Virtual Machine Disk (`*.vmdk`)	A file format used in virtual machines like VMware Workstation or Oracle VM VirtualBox.

Chapter 2

Windows OVA File Creation Using New Virtual Machine Images

Learn how to create a Virtual Analyzer-supported OVA file in the following topics:

- *Required Software on page 2-2*
- *Downloading and Installing VirtualBox on page 2-7*
- *Creating Windows Virtual Machine Images on page 2-9*
- *Modifying the Virtual Machine Environment on page 2-28*
- *Reducing the Size of VirtualBox Disk Images on page 2-44*
- *Exporting Virtual Machine Images to OVA Files on page 2-45*

Creating Windows OVA Files Using New Virtual Machine Images

Procedure

1. Prepare the operating system and required applications.

   For details, see *Required Software on page 2-2*.

2. Download and install VirtualBox.

   For details, see *Downloading and Installing VirtualBox on page 2-7*.

3. Create a virtual machine image.

   For details, see *Creating Windows Virtual Machine Images on page 2-9*.

4. Modify the environment of the virtual machine image.

   For details, see *Modifying the Virtual Machine Environment on page 2-28*.

5. Reduce the size of the VirtualBox Disk Image.

   For details, see *Reducing the Size of VirtualBox Disk Images on page 2-44*.

6. Export the virtual machine image to an OVA file.

   For details, see *Exporting Virtual Machine Images to OVA Files on page 2-45*.

Required Software

The following software must be installed on the virtual machine to achieve satisfactory detection results.

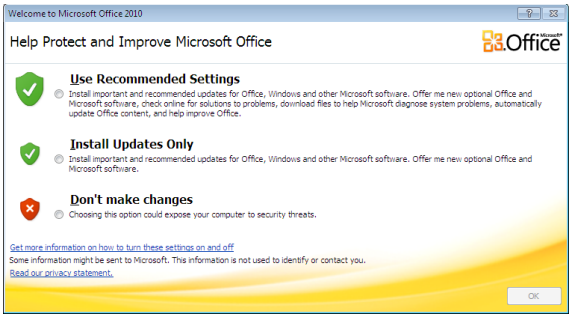
Note

Operating system, Office suite, and third-party software support may change or end without prior notice from Trend Micro due to specification, license model, and lifecycle changes.

TABLE 2-1. Required Applications

SOFTWARE	DESCRIPTION
Operating system	Virtual Analyzer supports the following operating systems: Windows XP, Windows 7, Windows 8/8.1, Windows 10 Version 22H2 and before, Windows 11 Version 21H2 and 23H2, Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022. **Important** • Package the installer as an ISO file. • Activate Windows with a valid product key after the tool has validated and modified virtual machine settings. Do not activate Windows before that. • Use a computer name that reflects your organizations' naming scheme. • Disable automatic updates. • Trend Micro recommends using the English version of the listed operating systems. • For Windows 7 and Windows Server 2008 R2, updates KB4474419 and KB4490628 must be installed. • Virtual Analyzer does not support Windows 11 Version 22H2

Software	Description
Office suite	Virtual Analyzer supports the following office suites: Office 2003 (32-bit), Office 2007 (32-bit), Office 2010 (32-bit and 64-bit), Office 2013 (32-bit and 64-bit), Office 2016 (32-bit and 64-bit), Office 2019 (32-bit and 64-bit), and Office 2021 (32-bit and 64-bit)

SOFTWARE	DESCRIPTION
	Important • For Office 2007 and after, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and Microsoft Publisher must be installed. • Activate Microsoft Office with a valid product key after the tool has validated and modified virtual machine settings. Do not activate Microsoft Office before that. • After installation, open all Microsoft Office applications and verify that the main editing screen is displayed. If any confirmation dialog or welcome screen displays, make any selection to close the screen and display the main editing screen.  **FIGURE 2-1. Help Protect and Improve Microsoft Office** • Verify that your license allows you to virtualize the applications. For details, see https://support.office.com. • Disable automatic updates. • Enable macros. For details, see Enable or disable macros in Office files

SOFTWARE	DESCRIPTION
Internet Browser	Virtual Analyzer supports the following internet browsers: Microsoft Edge (Chromium-based version), Internet Explorer **Important** • The default browser must be set to a supported internet browser. • For Windows 8.1 and before, the tool will automatically configure Internet Explorer as the default browser. • For Windows 10 and after, the default browser must be configured manually before the tool is used to validate the image. • Virtual Analyzer does not support Microsoft Edge Legacy (EdgeHTML version).
Adobe Reader	Install the version of Adobe Reader that is most widely used in your organization. To download the most current version of Adobe Reader, go to http://www.adobe.com/downloads/. If you do not install Adobe Reader, Virtual Analyzer: • Installs Adobe Reader 8, 9, and 11 on all Windows XP and Windows Server 2003/2003 R2 images during importing. • Installs Adobe Reader 9, 11, and DC on all Windows 7 and newer images during import. • Uses all versions during analysis. **WARNING!** This consumes additional computing resources. Configure Adobe Reader to manually check for and install updates. For details, see https://helpx.adobe.com/acrobat/kb/reader-acrobat-updater-settings.html.
.NET Framework	Install .NET Framework 3.5 or later if the operating system is Windows XP or Windows Server 2003.

Note

Trend Micro recommends installing the following software on the virtual machine to improve detection results.

- .NET Framework 4.0 in addition to .NET Framework 3.5
- Java SE Runtime Environment 8
- LibreOffice 6.4.7 or later, with macro security level set to low

Important

- Do not install VMware tools to avoid triggering the anti-virtual machine functions of some malware.
- Do not install any anti-malware software on the virtual machine to ensure normal operation of Virtual Analyzer.

Downloading and Installing VirtualBox

Procedure

1. Download the latest version of VirtualBox from https://www.virtualbox.org/wiki/Downloads.

   Note

   The VirtualBox Open Source Edition is licensed under the GPL V2. The full text of the license is available at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

   Trend Micro recommends using VirtualBox version 7.0 and later. The procedures outlined in this user guide have been tested with Virtual Box version 7.0.14.

Important

VirtualBox version 7.0 and later is required for Windows 11 virtual machines.

2. Configure the language settings using one of the following methods:
   - Install VirtualBox with English as the default language.
   - After installation, go to **File** > **Preferences** > **Language** and then select **English**.

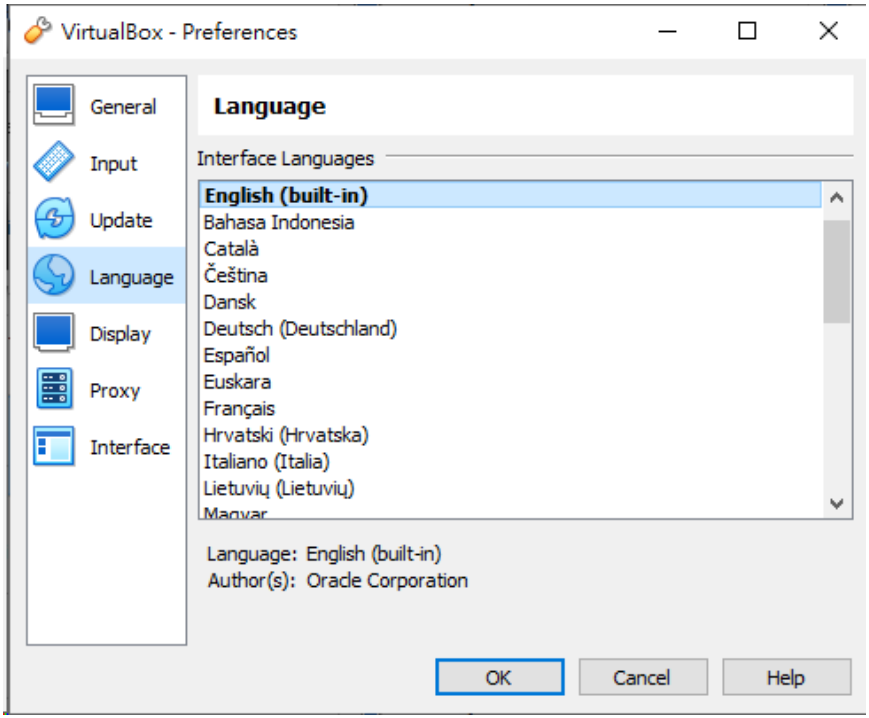


FIGURE 2-2. Language Settings

Creating Windows Virtual Machine Images

Procedure

1. Open VirtualBox.

   The **VirtualBox Manager** window opens.

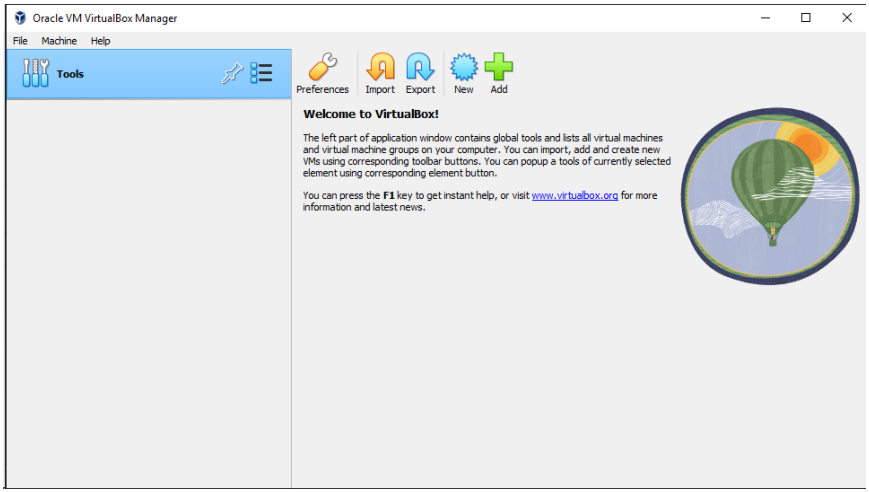


FIGURE 2-3. VirtualBox Manager

2. Click **New**.

   The **Create Virtual Machine** window opens.

3. Click **Expert Mode**.

The Create Virtual Machine wizard enters Expert Mode.

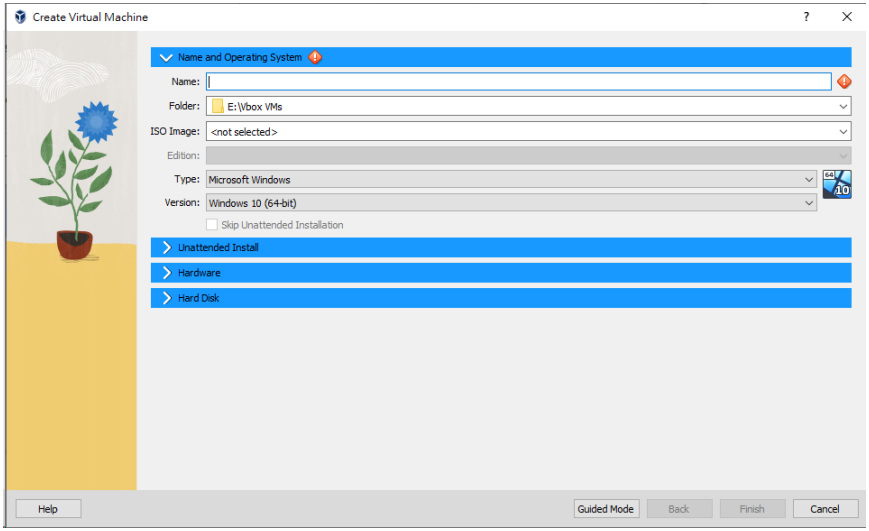


FIGURE 2-4. Create Virtual Machine - Expert Mode

4. Configure the **Name and Operating System** settings.
   - Type a permanent and unique **Name** for the virtual machine.
   - Specify the **Folder** to store the completed virtual machine.
   - Specify the **ISO Image** for the virtual machine.
   - For the **Type**, select **Microsoft Windows**.
   - For the **Version**, select the version of Windows you want to use for the virtual machine.

     For a list of supported Windows OS versions, see *Required Software on page 2-2*.
   - Select **Skip Unattended Installation**.
5. Open the **Hardware** section.

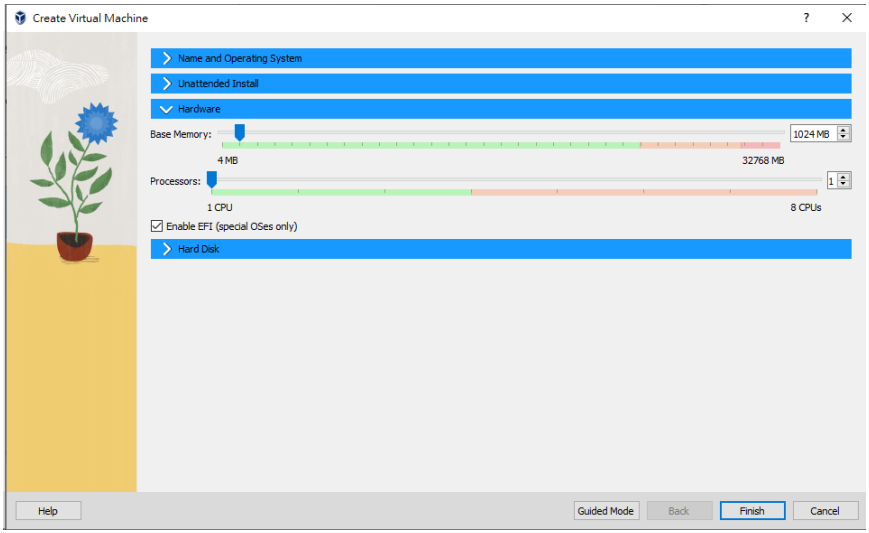


FIGURE 2-5. Hardware

6. Specify the recommended memory size for your operating system.
   - For Windows XP and Windows Server 2003, specify at least 512 MB
   - For Windows 11, specify at least 2048 MB
   - For all other supported versions of Windows and Windows Server, specify at least 1024 MB.
7. For Windows 11, select **Enable EFI (special OSes only)**.
8. Open the **Hard Disk** section.

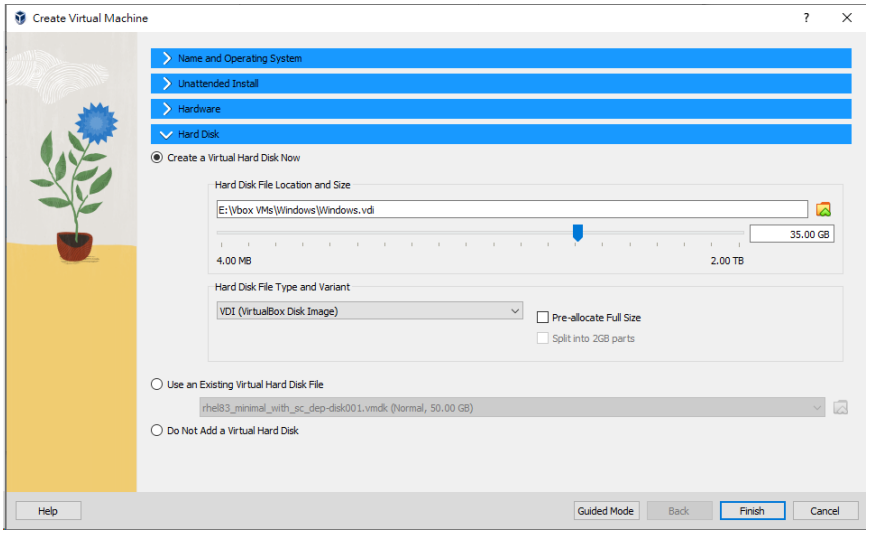


FIGURE 2-6. Hard Disk

9. Select **Create a Virtual Hard Disk Now**.
10. Specify the hard disk settings.
    - Specify the location of the virtual hard disk on the host machine.
    - Specify the size of the virtual hard disk according to your chosen operating system:
        - For Windows XP and Windows Server 2003, specify at least 15 GB.
        - For all other supported versions of Windows and Windows Server, specify at least 35 GB.
    - For the **Hard Disk File Type and Variant**, select **VDI (VirtualBox Disk Image)** or **VMDK (Virtual Machine Disk)**

Note

Specify additional virtual hard drive space if you plan to install additional software.

For best results, Trend Micro recommends selecting **VDI (VirtualBox Disk Image)**.

Important

Do not select "Pre-allocate Full Size" or "Split into 2GB parts." The options may cause the tool to fail.

11. Click **Finish**.

VirtualBox creates the virtual machine. The new virtual machine appears in the left pane of the VirtualBox Manager screen.

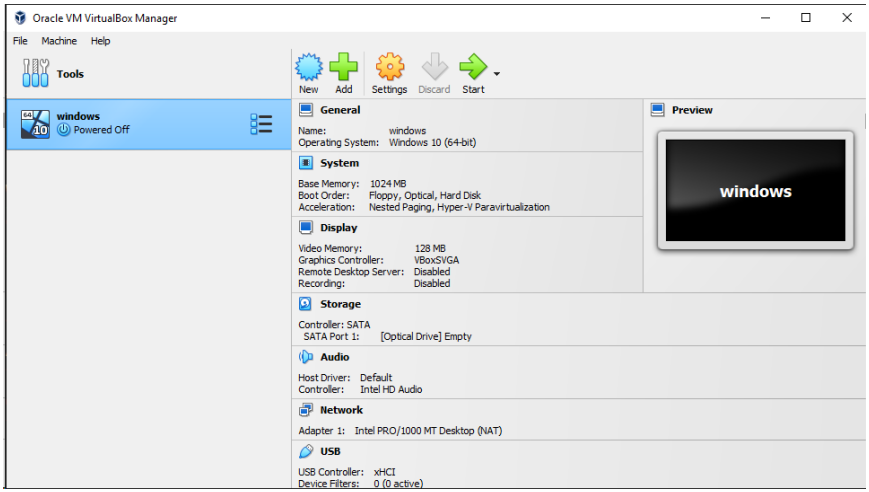


FIGURE 2-7. Newly-created Virtual Machine

Ensure that the virtual machine is not in any group.

12. Click **Settings**.

The **Settings** window opens.

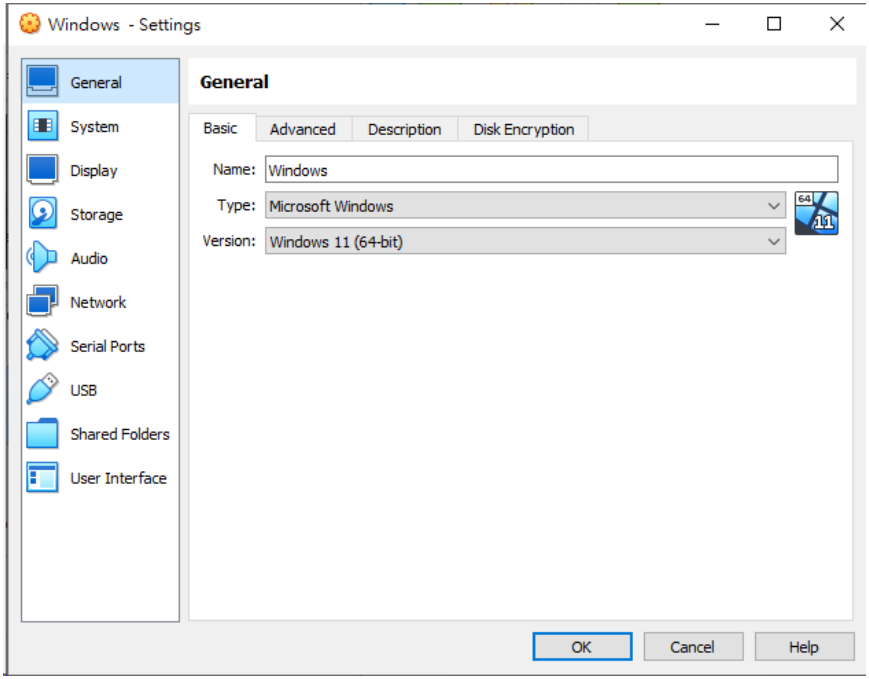


FIGURE 2-8. VirtualBox Settings

13. Go to **System**.

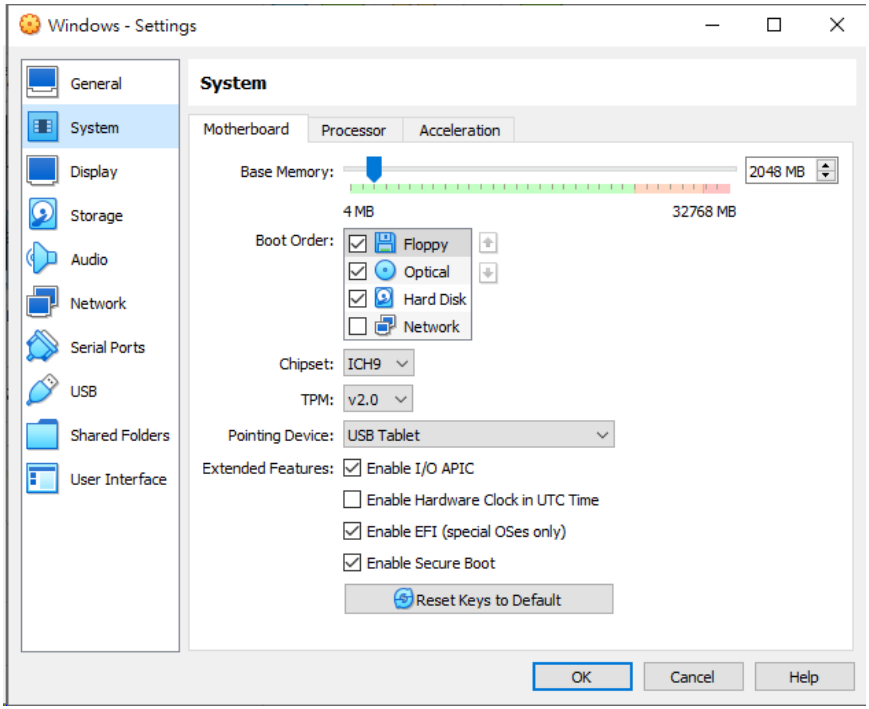


FIGURE 2-9. System Screen

14. Configure the settings on the **Motherboard** tab.
    - For **Chipset**, select **ICH9**.
    - For **TPM**, select **v2.0**.

      Note

      TPM v2.0 is required for Windows 11. The setting is optional for all other Windows versions.

    - For **Pointing Device**, select **USB Tablet**
    - Select the following **Extended Features**:
      - **Enable I/O APIC**

- **Enable EFI (special OSes only)** (Required for Windows 11, Optional for all other supported versions)
- **Enable Secure Boot** (Required for Windows 11)

Note

For Windows 11 virtual machines, **Enable EFI (special OSes only)** and **Enable Secure Boot** are required settings. The settings are optional for all other versions of Windows.

Use **Enable EFI (special OSes only)** if you want to create EFI-compatible images. EFI-compatible images are only supported by the following Trend Micro products:

- Deep Discovery Inspector 5.6 and later
- Deep Discovery Email Inspector 3.6 and later
- Deep Discovery Analyzer 6.8 and later
- Deep Discovery Director 5.1 and later
- Deep Discovery Web Inspector 2.5 and later

15. On the **Processor** tab, select **Enable PAE/NX**.
16. On the **Acceleration** tab, select **Enable Nested Paging**.

    If you are using VirtualBox 5.2 and before, also select **Enable VT-x/AMD-V**.

Note

- The **Acceleration** tab is only available if the processor of the host system supports virtualization technology and the virtualization setting is enabled in the BIOS of the host system.
- VirtualBox 6.0 and later automatically enables VT-x/AMD-V if the processor of the host system supports virtualization technology and the virtualization setting is enabled in the BIOS of the host system.

17. Go to **Storage**.

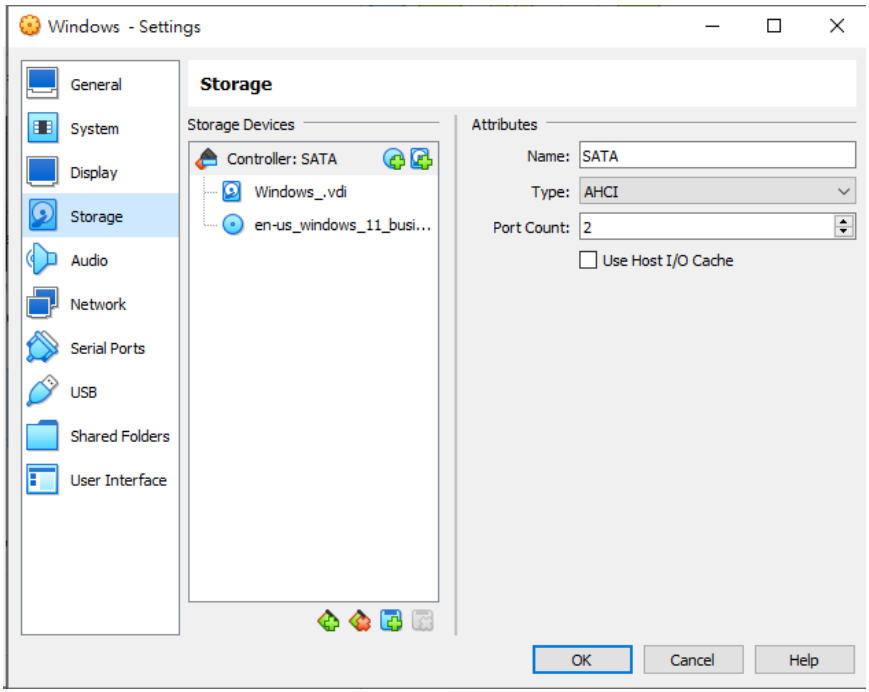


FIGURE 2-10. Storage Screen

18. If **Controller: SATA** appears under **Storage Devices**, select the controller and click to remove the SATA controller.

19. Add an IDE controller.

    a. Click and select **PIIX4 (Default IDE)**.

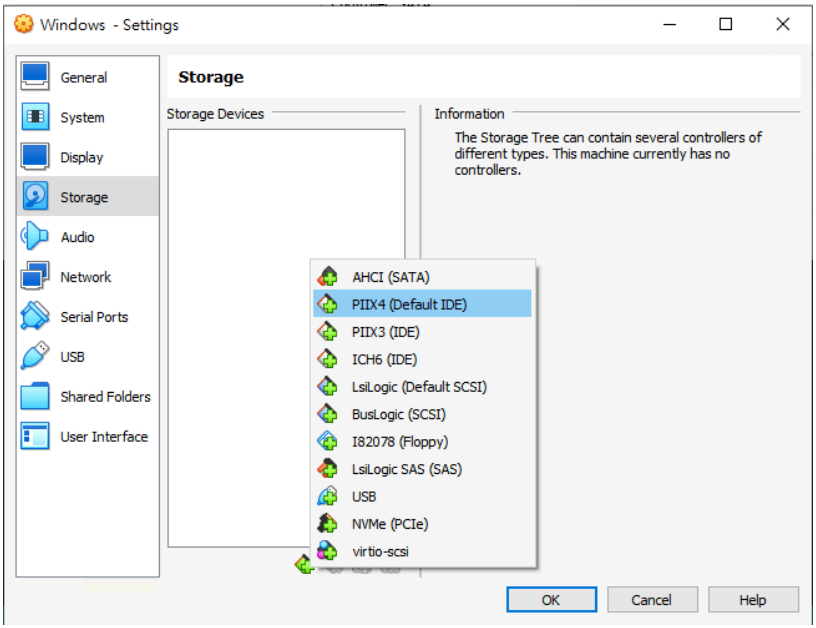


FIGURE 2-11. Add Storage Controller

Controller: PIIX4 appears on the Storage Devices list.

b. Click the controller and change the **Name** attribute to **`IDE`**.

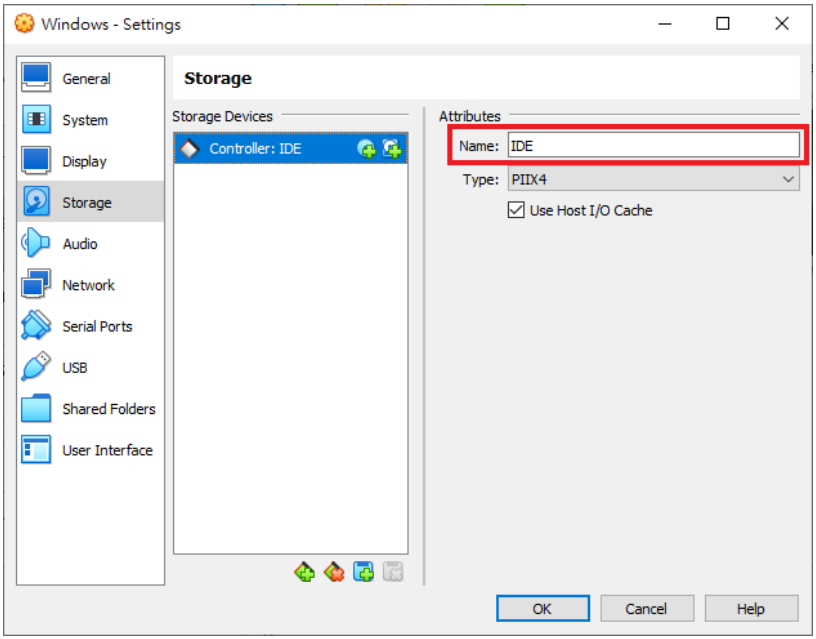


FIGURE 2-12. Controller IDE

c. Select **Use Host I/O Cache**.

d. Next to **Controller: PIIX4**, click to create a virtual hard disk.

The **Hard Disk Selector** window appears.

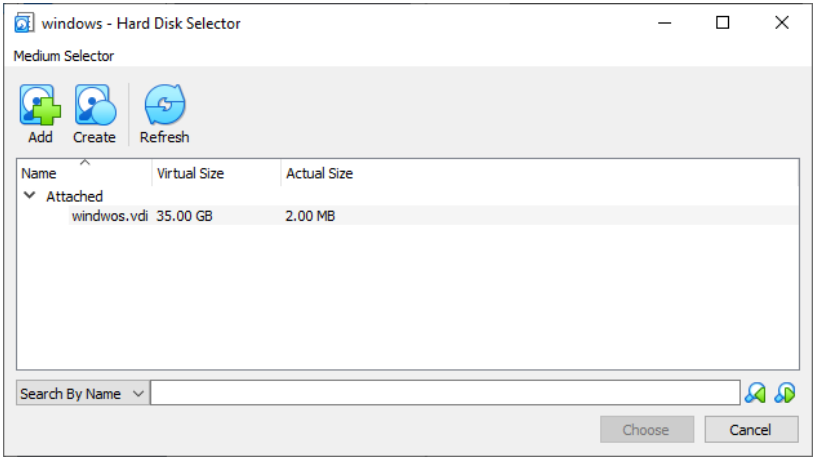


FIGURE 2-13. Hard Disk Selector

e. Select the virtual hard disk file that you previously created and click **Choose**.

f. Click the hard drive you created and verify the **Hard Disk** attribute is set to **IDE Primary Device 0**.

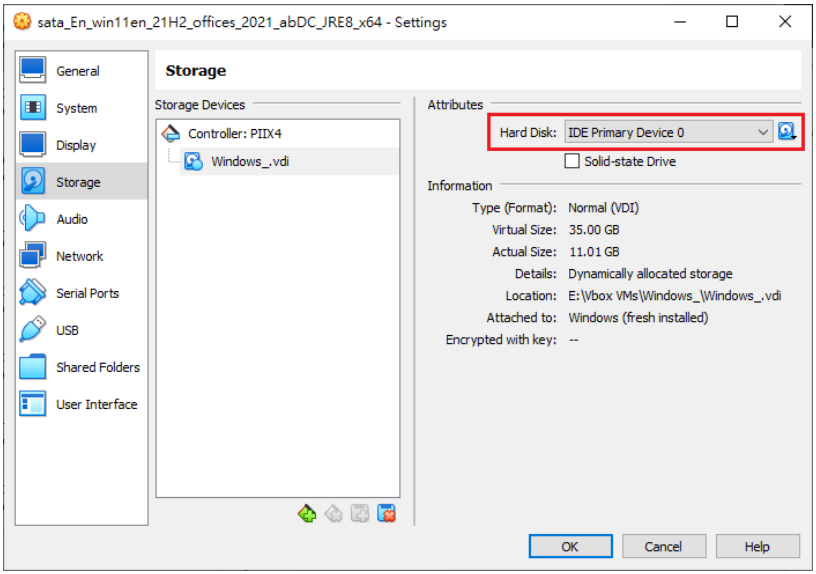


FIGURE 2-14. IDE Primary Device 0

g. Click **Controller: PIIX4** and then click to create an optical drive.

h. In the **Optical Disk Selector** window, click **Leave Empty**.

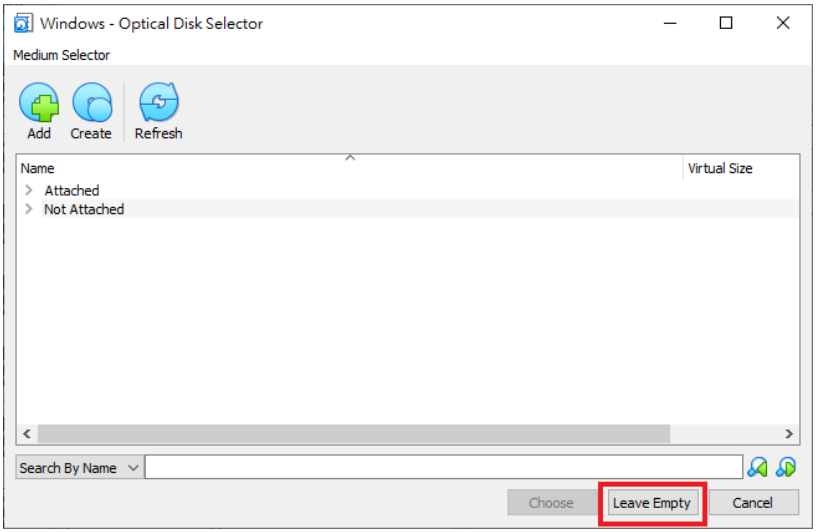


FIGURE 2-15. Optical Disk Selector

i. Click the optical drive you created and verify the **Optical Drive** attribute is set to **IDE Secondary Device 0**.

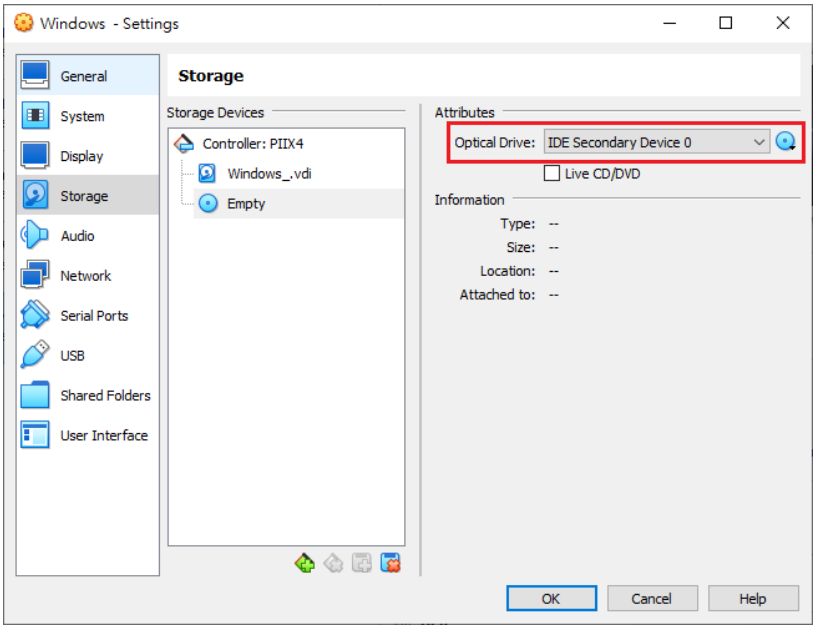


FIGURE 2-16. IDE Secondary Device 0

j. Click and select **Choose/Create a Virtual Optical Disk...**

k. Select the ISO file containing the operating system installer.

The ISO file appears as an available device.

You should only have one **Controller: PIIX4** listed under Storage Devices. If there are any other controllers listed, remove the extra controllers.

20. (Optional) Go to **Audio** and verify that **Enable Audio** is selected.

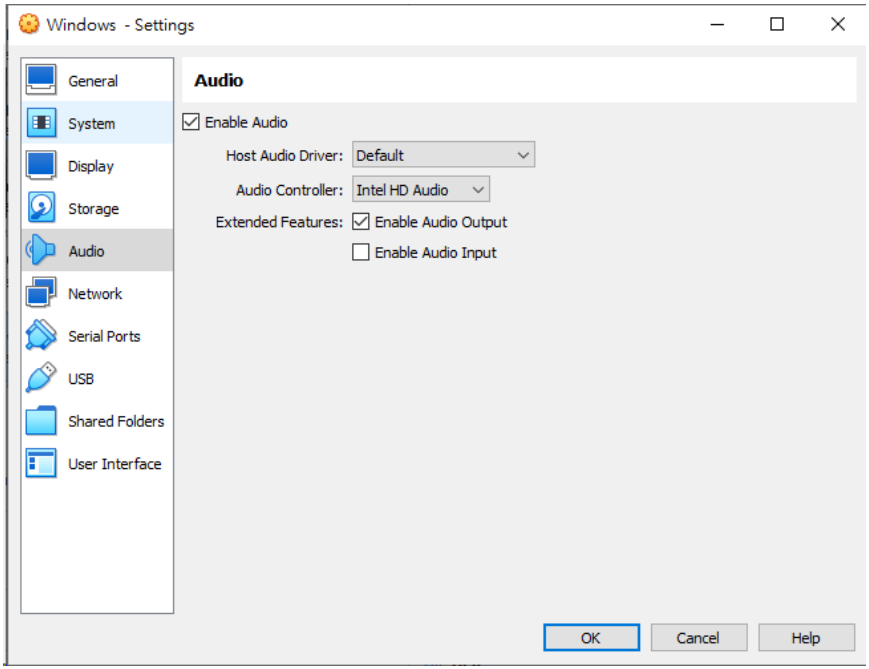


FIGURE 2-17. Audio Options Settings

21. Go to **USB**.

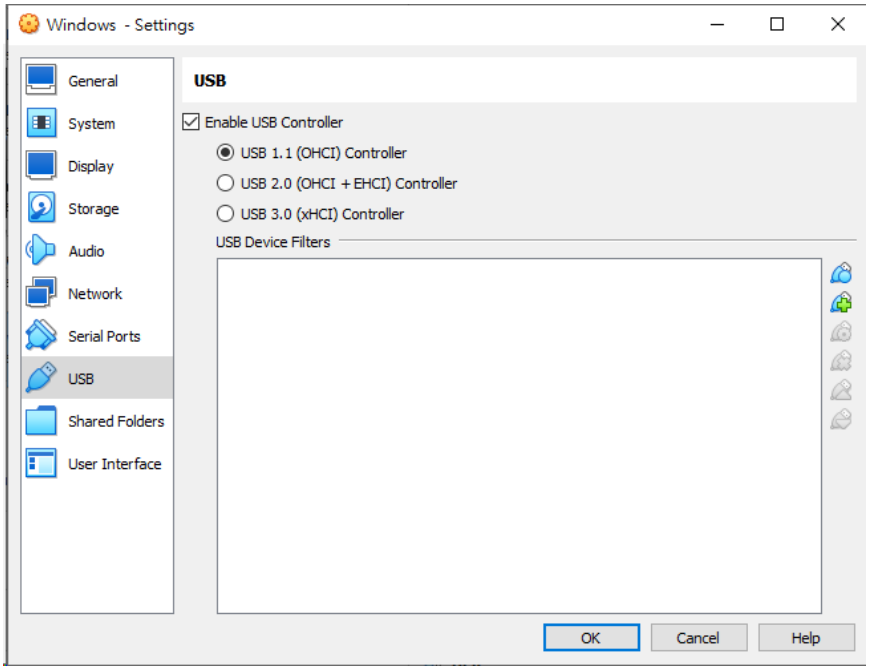


FIGURE 2-18. USB Settings

22. Select **Enable USB Controller**.
23. Select **USB 1.1 (OHCI) Controller**.
24. Go to **Shared Folders** and verify that no folders are shared.

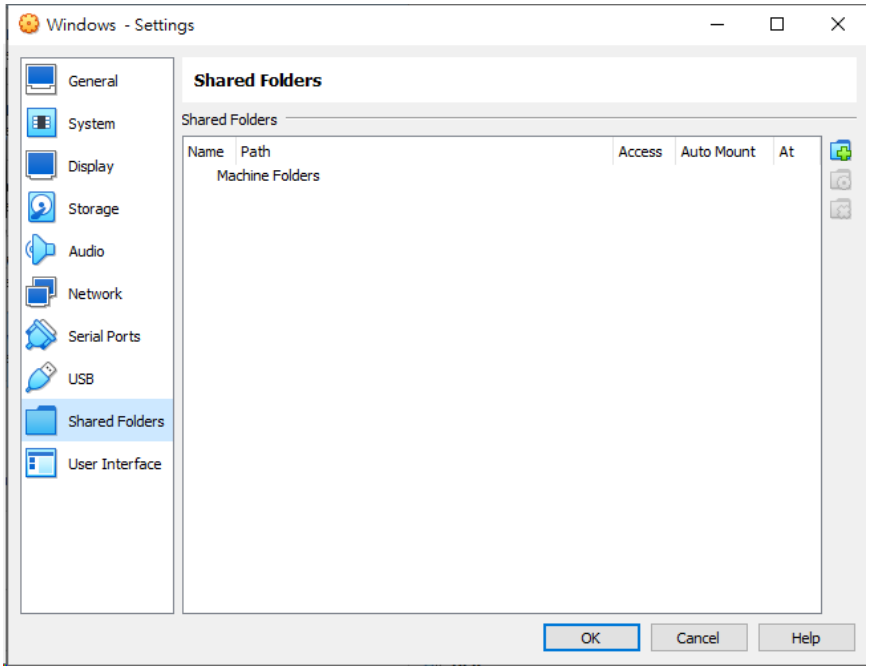


FIGURE 2-19. Shared Folders Settings

25. Click **OK**.

26. On the **VirtualBox Manager** screen, click 

to power on the image.

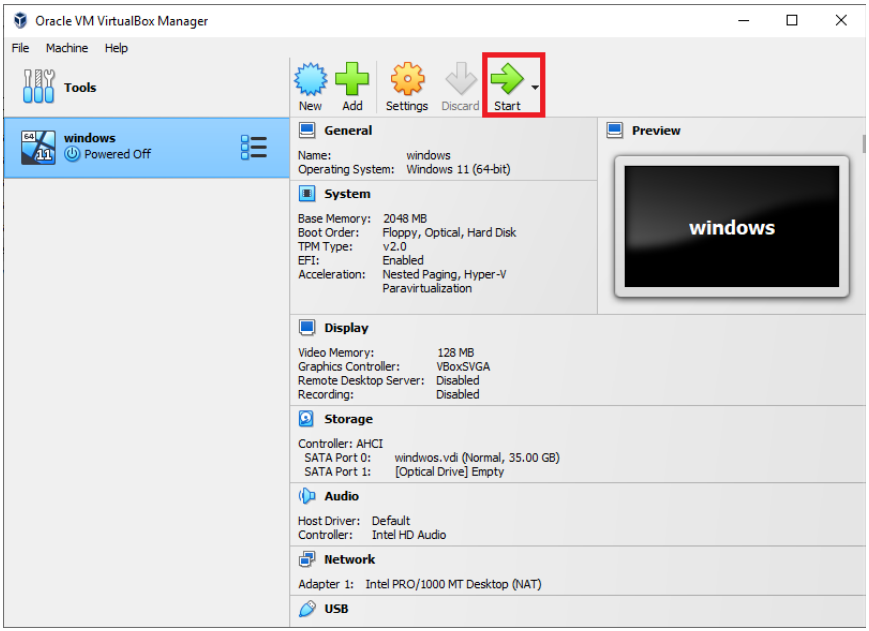


FIGURE 2-20. VirtualBox Manager

The installation process starts.

27. Follow the on-screen instructions to install the guest operating system.

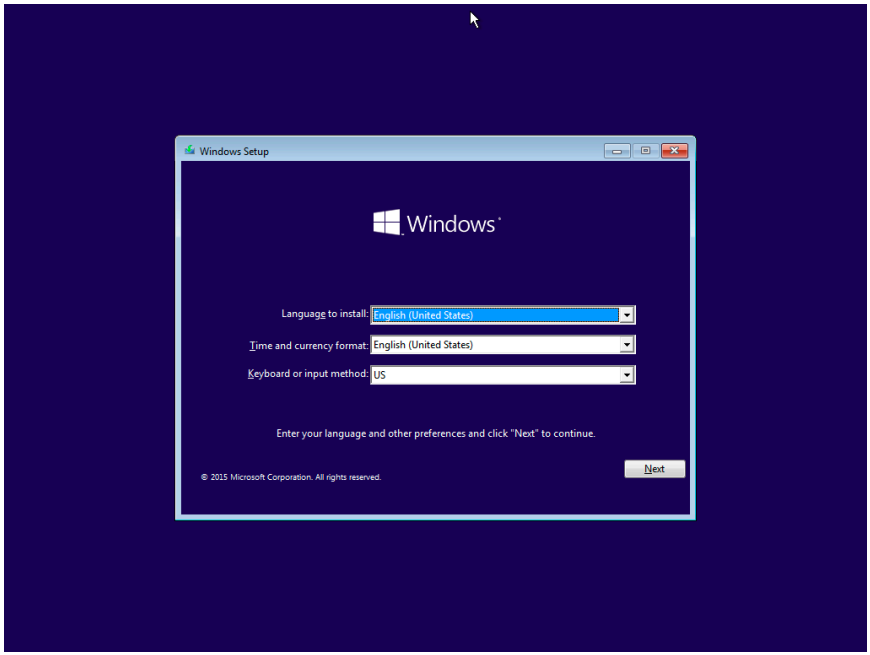


FIGURE 2-21. Operating System Installation Process

28. Install Microsoft Office and other required software to achieve satisfactory detection results.

Important

Verify there is at least 3072 MB free virtual disk space on the virtual machine to ensure normal operation of Virtual Analyzer.

Modifying the Virtual Machine Environment

Modify the virtual machine environment to run Virtual Analyzer Sensors, a collection of utilities that execute and detect malware, and record all behavior in Virtual Analyzer.

- *Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003) on page 2-29*

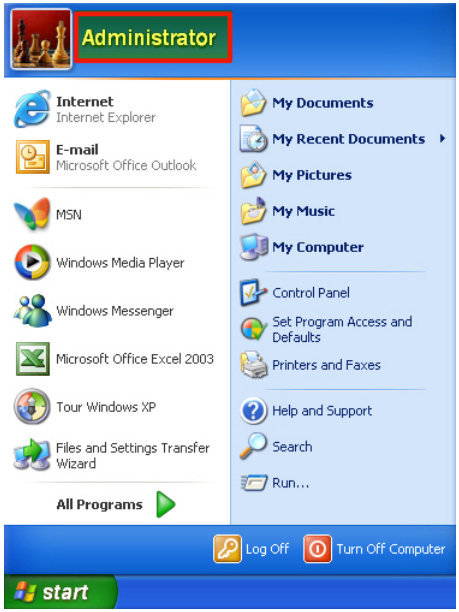
- *Modifying the Virtual Machine Environment (All Other Supported Windows Versions) on page 2-31*

Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003)

Procedure

1. Open a Command Prompt window (`cmd.exe`) using an account with administrator privileges.
2. Perform the following tasks:

Task	Steps
Set the "Administrator" logon password to "1111".	Type **`net user "Administrator" 1111`**.
Configure automatic logon from the “Administrator” account. **Note** The logon prompt is bypassed and the “Administrator” account is automatically used to log on to the system every time the virtual machine starts.	a. Type the following commands: • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f`** b. Restart the image.

Task	Steps
	Note No logon prompt is displayed and the "Administrator" account is automatically used to log on.  **FIGURE 2-22. Windows XP Administrator Account**
View all user accounts.	Type **`net user`**.
Delete non-built-in user accounts one at a time.	Type **`net user "<username>" /delete`**. Example: **`net user "test" /delete`**
View all network adapters with an active link	Type **`wmic nic where "netconnectionstatus=2" get netconnectionid /value`**.

TASK	STEPS
	Example output: **NetConnctionID=Local Area Connection**
Verify the DHCP status of all installed network adapters	Type **netsh interface ip show config**. The configuration of all installed network adapters displays. Verify that the value for **DHCP enabled:** is **Yes**.
Configure a network adapter to use DHCP	Type **netsh interface ip set address name="<network adapter>" dhcp**. Example: **netsh interface ip set address name="Local Area Connection" dhcp**
Disable Windows Firewall.	Type **netsh firewall set opmode mode=DISABLE**. **Note** Windows Firewall slows down the installation of Virtual Analyzer Sensors.

3. Restart the virtual machine.

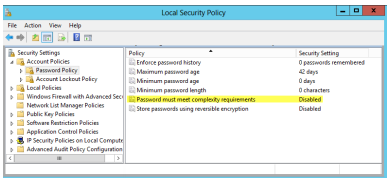
Modifying the Virtual Machine Environment (All Other Supported Windows Versions)

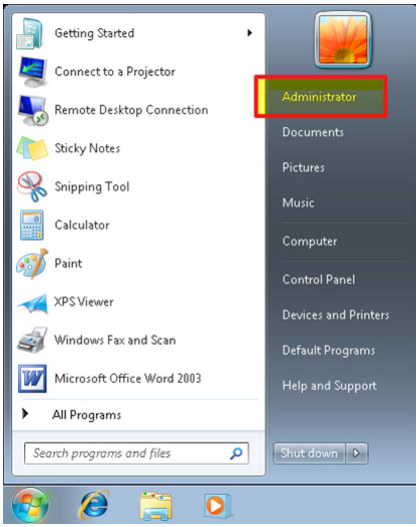
Procedure

1. Open a Command Prompt window (`cmd.exe`) using an account with administrator privileges.
2. Perform the following tasks:

TASK	STEPS
Enable the "Administrator" account	Type **net user "Administrator" /active:yes**.

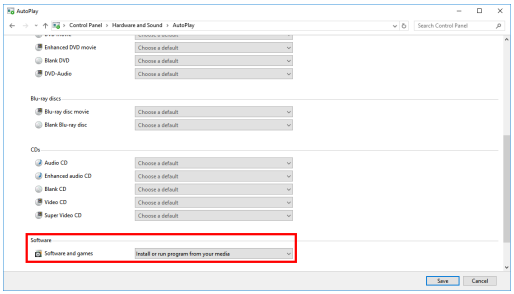
TASK	STEPS
Set the logon password for the “Administrator” account to “1111”	Type **`net user "Administrator" 1111`**.
Configure automatic logon from the administrator account **Note** Each time the image starts, the logon prompt is bypassed and the “Administrator” account is automatically used to log on to the system.	a. Type the following commands: • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f`**

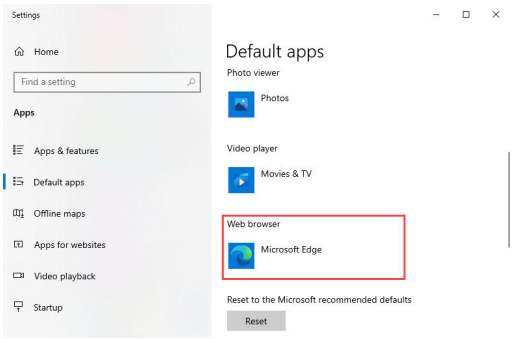
Task	Steps
	Note In Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022, launch the **Local Security Policy** snap-in (`secpol.msc`) to disable the **Password must meet complexity requirements** Local Security Setting.  **Figure 2-23. Disable Password must meet complexity requirements** • Restart the image.

TASK	STEPS
	No logon prompt is displayed and the "Administrator" account is automatically used to log on.  **FIGURE 2-24. Windows 7 Administrator Account**
View all user accounts	Type **`net user`**.
Delete non-built-in user accounts one at a time	Type **`net user "<username>" /delete`**. Example: **`net user "test" /delete`**
View all network adapters with an active link	Type **`wmic nic where "netconnectionstatus=2" get netconnectionid /value`**. Example output: **`NetConnctionID=Local Area Connection`**
Verify the DHCP status of all installed network adapters	Type **`netsh interface ip show config`**. The configuration of all installed network adapters displays. Verify that the value for **`DHCP enabled:`** is **`Yes`**.

TASK	STEPS
Configure a network adapter to use DHCP	Type **`netsh interface ip set address name="<network adapter>" dhcp`**. Example: **`netsh interface ip set address name="Local Area Connection" dhcp`**
Disable Windows Firewall	Type **`netsh advfirewall set allprofiles state off`**. **Note** Windows Firewall slows down the installation of Virtual Analyzer Sensors.
(Optional) Install Adobe Flash in Windows Server 2016 and Windows Server 2019	For Windows Server 2016: Type **`C:\> dism /online /add-package /packagepath:"C:\Windows\servicing\Packages\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~10.0.14393.0.mum`**" For Windows Server 2019: Type **`C:\> dism /online /add-package /packagepath:"C:\Windows\servicing\Packages\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~10.0.17763.1.mum"`**

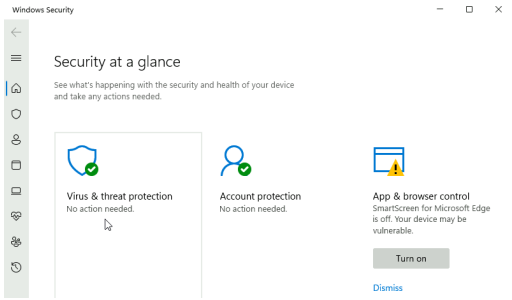
3. Perform the following tasks using the Windows graphical user interface:

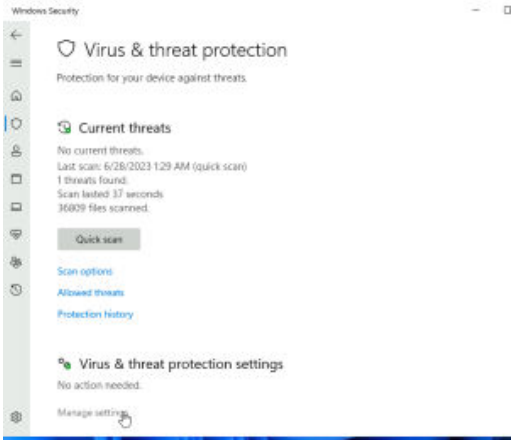
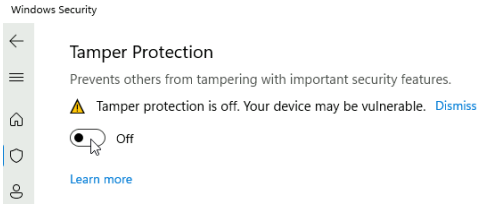
Task	Steps
Configure AutoPlay	a. Open the Windows **Start** menu, type **`Control Panel`** into the search box and press ENTER. b. In the **Control Panel**, go to **Hardware and Sound** > **AutoPlay**.  **Figure 2-25. AutoPlay** c. For **Software and games**, select **Install or run program from your media**. d. Click **Save**.

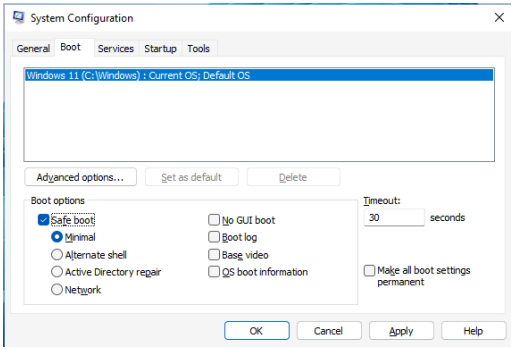
Task	Steps
Configure default web browser on Windows 10/11	The Virtual Analyzer supports both Microsoft Edge (Chromium) and Internet Explorer. One of these browsers must be manually set as the default web browser in Windows 10/11 before running the Virtual Analyzer. To configure the default web browser, perform the following: **Note** The Virtual Analyzer does not support Microsoft Edge Legacy. You can quickly check which version of Microsoft Edge is installed by comparing the icon: • Microsoft Edge (Chromium): • Microsoft Edge Legacy: a. Open the Windows **Start** menu, type **`Default apps`** and press ENTER. b. Under **Web browser**, select the current web browser.  **FIGURE 2-26. Default apps** c. In the **Choose an app** context menu, select **Internet Explorer** or **Microsoft Edge**.

TASK	STEPS
	d. If the **Before you switch** dialog appears, select **Switch anyway**.
(Optional) Change the display resolution	Trend Micro recommends settings the screen resolution to at least **`1152 x 864`** to avoid triggering the anti-virtual machine functions of some malware. a. Open the Windows **Start** menu, type **`Display settings`** and press ENTER. b. Under **Resolution**, select **`1152 x 864`** or any higher resolution. c. In the prompt that appears, click **Keep changes**.

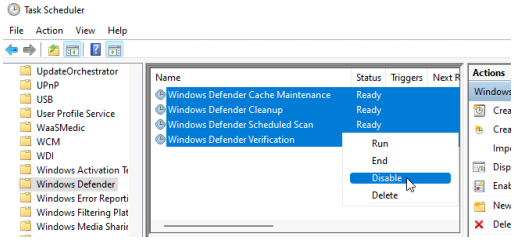
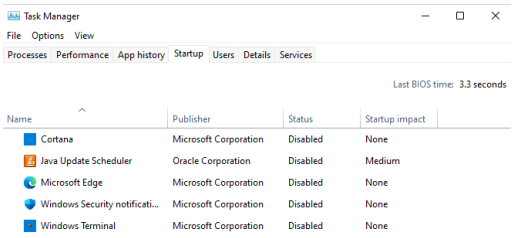
4. For Windows 11 21H2 and 23H2, perform the following tasks using the Windows graphical user interface:

Task	Steps
Disable Tamper Protection	**Important** Tamper Protection must be disabled to ensure normal operation and performance of Virtual Analyzer. a. Open the Windows **Start** menu, type **`Windows Security`** into the search box and press ENTER. b. In Windows Security, go to **Virus & threat protection**.  **FIGURE 2-27. Windows Security**

Task	Steps
	c. Under **Virus & threat protection**, click **Manage settings**.  **Figure 2-28. Virus & Threat Protection** d. Turn **Tamper Protection** off.  **Figure 2-29. Tamper Protection**

Task	Steps
(Optional) Disable Windows Defender Antivirus	a. Open the Windows **Start** menu, type **`msconfig`** into the search box and press ENTER. b. In the **System Configuration** window, go to the **Boot** tab. c. Under **Boot options**, enable **Safe boot** and select **Minimal**.  **Figure 2-30. System Configuration - Boot** d. Click **OK**. Windows 11 prompts to restart now. Click **Restart**. e. After the Windows 11 virtual machine restarts, run Command Prompt (cmd.exe) with administrator privileges and run the following commands. • **`REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sense" /v Start /t REG_DWORD /d 4 /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdBoot" /v Start /t REG_DWORD /d 4 /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentCon`**

Task	Steps
	`trolSet\Services\WdFilter" /v Start /t REG_DWORD /d 4 /f` • `REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisDrv" /v Start /t REG_DWORD /d 4 /f` • `REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisSvc" /v Start /t REG_DWORD /d 4 /f` • `REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinDefend" /v Start /t REG_DWORD /d 4 /f` f. Open the Windows **Start** menu, type **`msconfig`** into the search box and press ENTER. g. In the **System Configuration** window, go to the **Boot** tab. h. Under **Boot options**, disable **Safe boot** and click **OK**. Windows 11 prompts to restart now. Click **Restart**. i. After the Windows 11 virtual machine restarts, open the Windows **Start** menu, type **`Task Scheduler`** into the search box and press ENTER. j. In the **Task Scheduler** window, go to **Microsoft** > **Windows** > **Windows Defender**.

Task	Steps
	k. Disable all Windows Defender tasks.  **FIGURE 2-31. Task Scheduler**
(Optional) Disable startup applications	a. Open the Windows **Start** menu, type **`Task Manager`** and press ENTER. b. In **Task Manager**, go to the **Startup** tab. c. Disable the following applications. To disable, right-click the name of the application and select **Disable**. • Cortana • Java Update Scheduler • Microsoft Edge • Windows Security notification icon • Windows Terminal  **FIGURE 2-32. Task Manager**

5. Restart the virtual machine.

Reducing the Size of VirtualBox Disk Images

Procedure

1. Uninstall unnecessary applications and optional Windows components.
2. Run **Disk Cleanup** to free up space on the hard disk.

   The utility searches for files and data that you can safely delete, including:

   - Temporary Windows and Internet files
   - ActiveX controls, Java applets, and other downloaded program files
   - Files in the Recycle Bin

   For details, see the Microsoft Help: http://windows.microsoft.com/en-us/windows/delete-files-using-disk-cleanup#delete-files-using-disk-cleanup=windows-7.
3. Use **Deployment Image Servicing and Management (DISM)** to free up space on the hard disk.

   DISM is a command-line utility that can be used to free up disk space by managing the Windows Component Store (WinSxS directory).

   For details, see the Microsoft Developer resource website: https://msdn.microsoft.com/en-us/windows/hardware/commercialize/manufacture/desktop/clean-up-the-winsxs-folder

   a. Open a Command Prompt window.

   Note

   Depending on the Windows version, not all of the following commands may be supported.

   b. Type `dism /Online /Cleanup-Image /SPSuperseded`.

   c. Type `dism /Online /Cleanup-Image /StartComponentCleanup /ResetBase`.

4. Download **SDelete** and then zero out the free space on the hard disk.

   SDelete is a free command-line utility that securely deletes existing files and permanently erases file data in unallocated clusters of a disk. The utility can also ensures that even encrypted files cannot be recovered by overwriting all addressable locations with new and random characters.

   a. Download `sdelete.zip` from the Windows Sysinternals website: https://technet.microsoft.com/en-us/sysinternals/sdelete.aspx

   b. Extract `sdelete.exe`.

   c. Open a Command Prompt window.

   d. Go to the folder that contains `sdelete.exe`.

   e. Type **`sdelete -z [drive letter]`**.

      SDelete zeroes the free space on the hard disk.

5. Shut down the virtual machine.

6. Open a Command Prompt window on the host system.

7. Type **`"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" modifyhd [path\[vm_name.vdi] --compact`**.

   The virtual hard disk drive size is reduced.

Exporting Virtual Machine Images to OVA Files

A virtual machine image comprises many uncompressed files. The files must be combined into a single OVA file to avoid issues when importing.

Important

Verify that the size of the created OVA file is supported by your product.

For details, go to https://docs.trendmicro.com/en-us/home.aspx#Enterprise.

Procedure

1. On the VirtualBox Manager screen, power off the virtual machine.

   Note
   Verify that the CD/DVD drive is empty before powering off and exporting.

2. Go to **File** > **Export Appliance**.

   The **Export Virtual Appliance** window appears.

3. Select the virtual machine image to export and click **Next**.

   The **Appliance settings** screen appears.

4. Configure the following:

   - **File**: Accept the default name and path or click  to select a different file.
   - **Format**: Select **OVF 1.0**.

     Important
     Format options include OVF 0.9, 1.0 and 2.0. Virtual Analyzer does not support OVF 2.0.

   - **MAC Address Policy**: Select **Include only NAT network adapter MAC addresses**.

5. Click **Next**.

   The **Virtual system settings** screen appears.

6. Verify that the **License** field is empty and then click **Export**.

VirtualBox creates the OVA file.

Chapter 3

Windows OVA File Creation Using Converted Virtual Hard Disk Drives

Learn how to prepare and import an Windows OVA file in the following topics:

- *Modifying the Virtual Machine Environment on page 3-8*
- *Exporting Virtual Machine Images on page 3-26*
- *Converting VMware ESXi Virtual Hard Disk Drives on page 3-33*
- *Creating Virtual Machine Images Using Converted Virtual Hard Disk Drives on page 3-40*
- *Configuring Virtual Machine Images on page 3-59*
- *Exporting Virtual Machine Images to OVA Files on page 3-64*

Creating Windows OVA Files Using Converted Virtual Hard Disk Drives

Procedure

1. Prepare Adobe Reader.

   For details, see *Preparing Adobe Reader on page 3-7*

2. Modify the environment of the virtual machine image.

   For details, see *Modifying the Virtual Machine Environment on page 3-8*.

3. Export the virtual machine image.

   For details, see *Exporting Virtual Machine Images on page 3-26*.

4. Convert the virtual hard disk drive of the exported image to the VirtualBox format.

   For details, see *Converting VMware ESXi Virtual Hard Disk Drives on page 3-33*.

5. Create a new virtual machine image using the converted virtual hard disk drive.

   For details, see *Creating Virtual Machine Images Using Converted Virtual Hard Disk Drives on page 3-40*.

6. Configure the new virtual machine image.

   For details, see *Configuring Virtual Machine Images on page 3-59*.

7. Export the virtual machine image to an OVA file.

   For details, see *Exporting Virtual Machine Images to OVA Files on page 3-64*.

Required Software

The following software must be installed on the virtual machine to achieve satisfactory detection results.

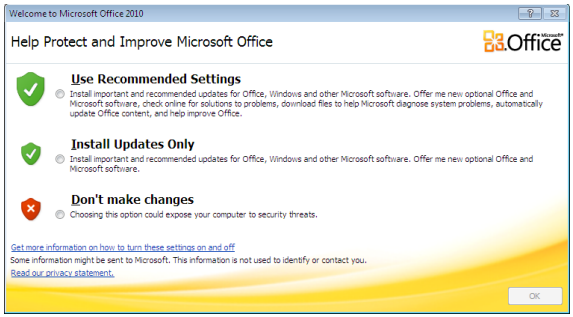
Note

Operating system, Office suite, and third-party software support may change or end without prior notice from Trend Micro due to specification, license model, and lifecycle changes.

TABLE 3-1. Required Applications

SOFTWARE	DESCRIPTION
Operating system	Virtual Analyzer supports the following operating systems: Windows XP, Windows 7, Windows 8/8.1, Windows 10 Version 22H2 and before, Windows 11 Version 21H2 and 23H2, Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022. **Important** • Package the installer as an ISO file. • Activate Windows with a valid product key after the tool has validated and modified virtual machine settings. Do not activate Windows before that. • Use a computer name that reflects your organizations' naming scheme. • Disable automatic updates. • Trend Micro recommends using the English version of the listed operating systems. • For Windows 7 and Windows Server 2008 R2, updates KB4474419 and KB4490628 must be installed. • Virtual Analyzer does not support Windows 11 Version 22H2

Software	Description
Office suite	Virtual Analyzer supports the following office suites: Office 2003 (32-bit), Office 2007 (32-bit), Office 2010 (32-bit and 64-bit), Office 2013 (32-bit and 64-bit), Office 2016 (32-bit and 64-bit), Office 2019 (32-bit and 64-bit), and Office 2021 (32-bit and 64-bit)

SOFTWARE	DESCRIPTION
	Important • For Office 2007 and after, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and Microsoft Publisher must be installed. • Activate Microsoft Office with a valid product key after the tool has validated and modified virtual machine settings. Do not activate Microsoft Office before that. • After installation, open all Microsoft Office applications and verify that the main editing screen is displayed. If any confirmation dialog or welcome screen displays, make any selection to close the screen and display the main editing screen.  **FIGURE 3-1. Help Protect and Improve Microsoft Office** • Verify that your license allows you to virtualize the applications. For details, see https://support.office.com. • Disable automatic updates. • Enable macros. For details, see Enable or disable macros in Office files

SOFTWARE	DESCRIPTION
Internet Browser	Virtual Analyzer supports the following internet browsers: Microsoft Edge (Chromium-based version), Internet Explorer **Important** • The default browser must be set to a supported internet browser. • For Windows 8.1 and before, the tool will automatically configure Internet Explorer as the default browser. • For Windows 10 and after, the default browser must be configured manually before the tool is used to validate the image. • Virtual Analyzer does not support Microsoft Edge Legacy (EdgeHTML version).
Adobe Reader	Install the version of Adobe Reader that is most widely used in your organization. To download the most current version of Adobe Reader, go to http://www.adobe.com/downloads/. If you do not install Adobe Reader, Virtual Analyzer: • Installs Adobe Reader 8, 9, and 11 on all Windows XP and Windows Server 2003/2003 R2 images during importing. • Installs Adobe Reader 9, 11, and DC on all Windows 7 and newer images during import. • Uses all versions during analysis. **WARNING!** This consumes additional computing resources. Configure Adobe Reader to manually check for and install updates. For details, see https://helpx.adobe.com/acrobat/kb/reader-acrobat-updater-settings.html.
.NET Framework	Install .NET Framework 3.5 or later if the operating system is Windows XP or Windows Server 2003.

Note

Trend Micro recommends installing the following software on the virtual machine to improve detection results.

- .NET Framework 4.0 in addition to .NET Framework 3.5
- Java SE Runtime Environment 8
- LibreOffice 6.4.7 or later, with macro security level set to low

Important

- Do not install VMware tools to avoid triggering the anti-virtual machine functions of some malware.
- Do not install any anti-malware software on the virtual machine to ensure normal operation of Virtual Analyzer.

Preparing Adobe Reader

Perform the following steps if Adobe Reader is installed on the virtual machine.

Procedure

1. Disable automatic updates.

   For details, see https://helpx.adobe.com/enterprise/kb/disable-auto-updates-application-manager.html.

2. Install the necessary Adobe Reader language packs so that Virtual Analyzer can process files authored in languages other than those supported in your native Adobe Reader.

   For example, if you use the English version of Adobe Reader and you expect to analyze files authored in East Asian languages, install the Asian and Extended Language Pack.

3. Start Adobe Reader.

Important

Perform this step before exporting the virtual machine.

Modifying the Virtual Machine Environment

Modify the virtual machine environment to run Virtual Analyzer Sensors, a collection of utilities that execute and detect malware, and record all behavior in Virtual Analyzer.

- *Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003) on page 3-8*
- *Modifying the Virtual Machine Environment (All Other Supported Windows Versions) on page 3-11*
- *Uninstalling VMware Tools on page 3-24*

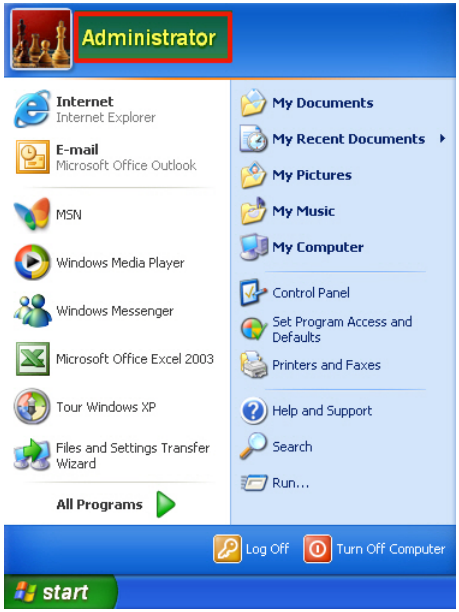
Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003)

Procedure

1. Open a Command Prompt window (`cmd.exe`) using an account with administrator privileges.
2. Perform the following tasks:

TASK	STEPS
Set the "Administrator" logon password to "1111".	Type **`net user "Administrator" 1111`**.
Configure automatic logon from the “Administrator” account.	a. Type the following commands: • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f`**

Task	Steps
Note The logon prompt is bypassed and the “Administrator” account is automatically used to log on to the system every time the virtual machine starts.	• `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f` • `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f` b. Restart the image.

TASK	STEPS
	Note No logon prompt is displayed and the "Administrator" account is automatically used to log on.  **FIGURE 3-2. Windows XP Administrator Account**
View all user accounts.	Type **`net user`**.
Delete non-built-in user accounts one at a time.	Type **`net user "<username>" /delete`**. Example: **`net user "test" /delete`**
View all network adapters with an active link	Type **`wmic nic where "netconnectionstatus=2" get netconnectionid /value`**.

TASK	STEPS
	Example output: **NetConnctionID=Local Area Connection**
Verify the DHCP status of all installed network adapters	Type **netsh interface ip show config**. The configuration of all installed network adapters displays. Verify that the value for **DHCP enabled:** is **Yes**.
Configure a network adapter to use DHCP	Type **netsh interface ip set address name="<network adapter>" dhcp**. Example: **netsh interface ip set address name="Local Area Connection" dhcp**
Disable Windows Firewall.	Type **netsh firewall set opmode mode=DISABLE**. **Note** Windows Firewall slows down the installation of Virtual Analyzer Sensors.
Uninstall VMware Tools.	For details, see *Uninstalling VMware Tools on page 3-24*.

3. Restart the virtual machine.

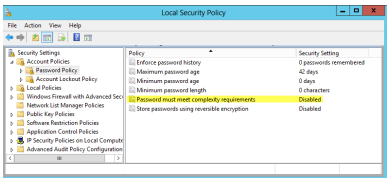
Modifying the Virtual Machine Environment (All Other Supported Windows Versions)

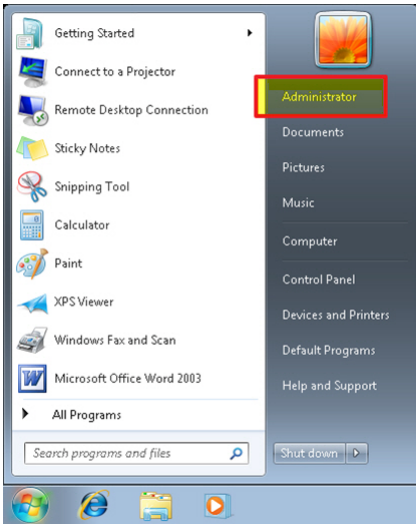
Procedure

1. Open a Command Prompt window (`cmd.exe`) using an account with administrator privileges.
2. Perform the following tasks:

TASK	STEPS
Enable the "Administrator" account.	Type **net user "Administrator" /active:yes**.

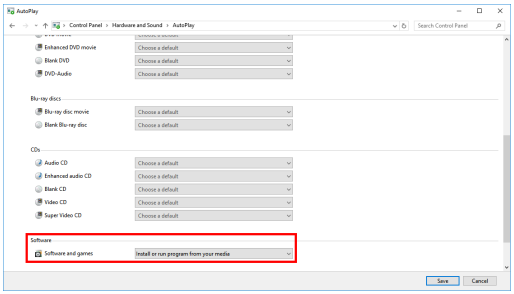
TASK	STEPS
Set the logon password for the “Administrator” account to “1111”.	Type **`net user "Administrator" 1111`**.
Configure automatic logon from the administrator account. **Note** Each time the image starts, the logon prompt is bypassed and the “Administrator” account is automatically used to log on to the system.	a. Type the following commands: • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f`**

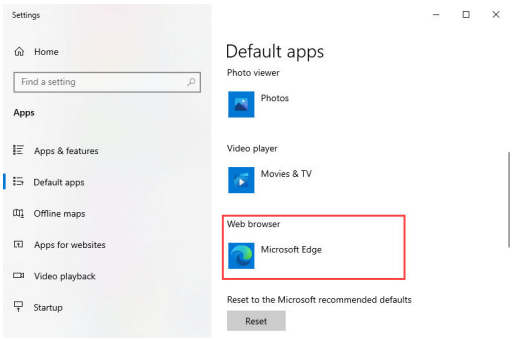
Task	Steps
	Note In Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022, launch the **Local Security Policy** snap-in (`secpol.msc`) to disable the **Password must meet complexity requirements** Local Security Setting.  **Figure 3-3. Disable Password must meet complexity requirements** • Restart the image.

TASK	STEPS
	No logon prompt is displayed and the "Administrator" account is automatically used to log on.  **FIGURE 3-4. Windows 7 Administrator Account**
View all user accounts.	Type **`net user`**.
Delete non-built-in user accounts one at a time.	Type **`net user "<username>" /delete`**. Example: **`net user "test" /delete`**
View all network adapters with an active link	Type **`wmic nic where "netconnectionstatus=2" get netconnectionid /value`**. Example output: **`NetConnctionID=Local Area Connection`**
Verify the DHCP status of all installed network adapters	Type **`netsh interface ip show config`**. The configuration of all installed network adapters displays. Verify that the value for **`DHCP enabled:`** is **`Yes`**.

TASK	STEPS
Configure a network adapter to use DHCP	Type **`netsh interface ip set address name="<network adapter>" dhcp`**. Example: **`netsh interface ip set address name="Local Area Connection" dhcp`**
Disable Windows Firewall.	Type **`netsh advfirewall set allprofiles state off`**. **Note** Windows Firewall slows down the installation of Virtual Analyzer Sensors.
(Optional) Install Adobe Flash in Windows Server 2016 and Windows Server 2019	For Windows Server 2016: Type **`C:\> dism /online /add-package /packagepath:"C:\Windows\servicing\Packages\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~10.0.14393.0.mum`**" For Windows Server 2019: Type **`C:\> dism /online /add-package /packagepath:"C:\Windows\servicing\Packages\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~10.0.17763.1.mum"`**

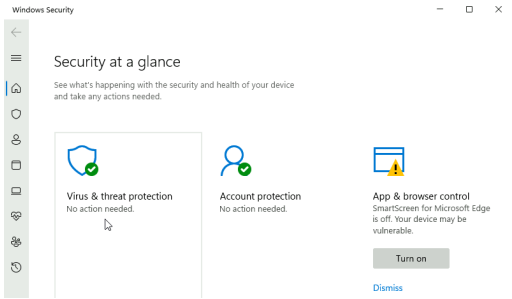
3. Perform the following tasks using the Windows graphical user interface:

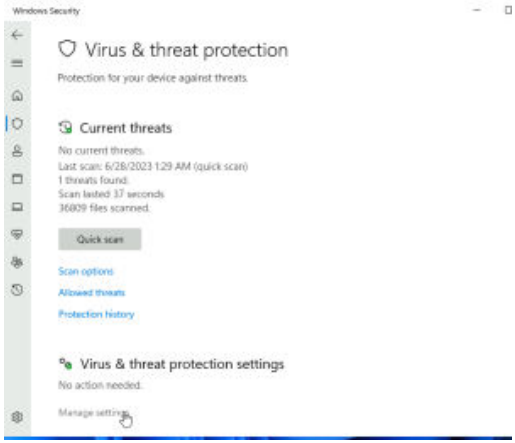
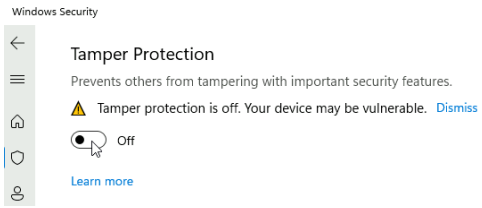
Task	Steps
Configure AutoPlay	a. Open the Windows **Start** menu, type **`Control Panel`** into the search box and press ENTER. b. In the **Control Panel**, go to **Hardware and Sound** > **AutoPlay**.  **Figure 3-5. AutoPlay** c. For **Software and games**, select **Install or run program from your media**. d. Click **Save**.

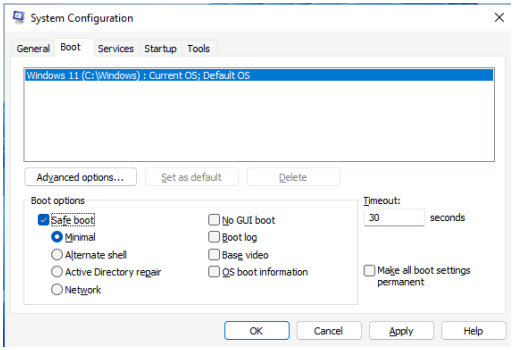
Task	Steps
Configure default web browser on Windows 10/11	The Virtual Analyzer supports both Microsoft Edge (Chromium) and Internet Explorer. One of these browsers must be manually set as the default web browser in Windows 10/11 before running the Virtual Analyzer. To configure the default web browser, perform the following: **Note** The Virtual Analyzer does not support Microsoft Edge Legacy. You can quickly check which version of Microsoft Edge is installed by comparing the icon: • Microsoft Edge (Chromium): • Microsoft Edge Legacy: a. Open the Windows **Start** menu, type **`Default apps`** and press ENTER. b. Under **Web browser**, select the current web browser.  **FIGURE 3-6. Default apps** c. In the **Choose an app** context menu, select **Internet Explorer** or **Microsoft Edge**.

TASK	STEPS
	d. If the **Before you switch** dialog appears, select **Switch anyway**.
(Optional) Change the display resolution	Trend Micro recommends settings the screen resolution to at least **`1152 x 864`** to avoid triggering the anti-virtual machine functions of some malware. a. Open the Windows **Start** menu, type **`Display settings`** and press ENTER. b. Under **Resolution**, select **`1152 x 864`** or any higher resolution. c. In the prompt that appears, click **Keep changes**.
Uninstall VMware Tools.	For details, see *Uninstalling VMware Tools on page 3-24*.

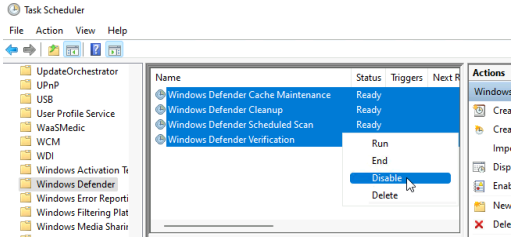
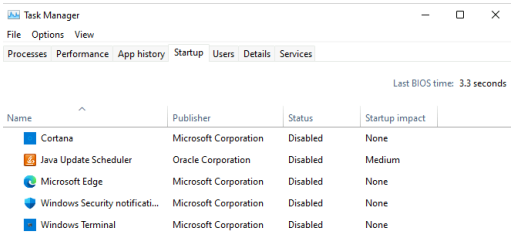
4. For Windows 11 21H2 and 23H2, perform the following tasks using the Windows graphical user interface:

Task	Steps
Disable Tamper Protection	**Important** Tamper Protection must be disabled to ensure normal operation and performance of Virtual Analyzer. a. Open the Windows **Start** menu, type **`Windows Security`** into the search box and press ENTER. b. In Windows Security, go to **Virus & threat protection**.  **FIGURE 3-7. Windows Security**

Task	Steps
	c. Under **Virus & threat protection**, click **Manage settings**.  **FIGURE 3-8. Virus & Threat Protection** d. Turn **Tamper Protection** off.  **FIGURE 3-9. Tamper Protection**

Task	Steps
(Optional) Disable Windows Defender Antivirus	a. Open the Windows **Start** menu, type **`msconfig`** into the search box and press ENTER. b. In the **System Configuration** window, go to the **Boot** tab. c. Under **Boot options**, enable **Safe boot** and select **Minimal**.  **FIGURE 3-10. System Configuration - Boot** d. Click **OK**. Windows 11 prompts to restart now. Click **Restart**. e. After the Windows 11 virtual machine restarts, run Command Prompt (cmd.exe) with administrator privileges and run the following commands. • **`REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sense" /v Start /t REG_DWORD /d 4 /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdBoot" /v Start /t REG_DWORD /d 4 /f`** • **`REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentCon`**

Task	Steps
	`trolSet\Services\WdFilter" /v Start /t REG_DWORD /d 4 /f` • `REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisDrv" /v Start /t REG_DWORD /d 4 /f` • `REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdNisSvc" /v Start /t REG_DWORD /d 4 /f` • `REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinDefend" /v Start /t REG_DWORD /d 4 /f` f. Open the Windows **Start** menu, type `msconfig` into the search box and press ENTER. g. In the **System Configuration** window, go to the **Boot** tab. h. Under **Boot options**, disable **Safe boot** and click **OK**. Windows 11 prompts to restart now. Click **Restart**. i. After the Windows 11 virtual machine restarts, open the Windows **Start** menu, type `Task Scheduler` into the search box and press ENTER. j. In the **Task Scheduler** window, go to **Microsoft** > **Windows** > **Windows Defender**.

Task	Steps
	k. Disable all Windows Defender tasks.  **Figure 3-11. Task Scheduler**
(Optional) Disable startup applications	a. Open the Windows **Start** menu, type **`Task Manager`** and press ENTER. b. In **Task Manager**, go to the **Startup** tab. c. Disable the following applications. To disable, right-click the name of the application and select **Disable**. • Cortana • Java Update Scheduler • Microsoft Edge • Windows Security notification icon • Windows Terminal  **Figure 3-12. Task Manager**

5. Restart the virtual machine.

Uninstalling VMware Tools

VMware Tools will attempt to connect to a VMware ESXi host, which might prevent VirtualBox from importing the virtual machine image.

Procedure

1. Go to **Start** > **Control Panel**.

   The **Control Panel** screen appears.

2. Check the list of installed programs.

   - For Windows XP and Windows Server 2003, click **Add or Remove Programs**.
   - For other supported Windows and Windows Server versions, go to **Programs** > **Programs and Features** .

A list of installed programs appears.

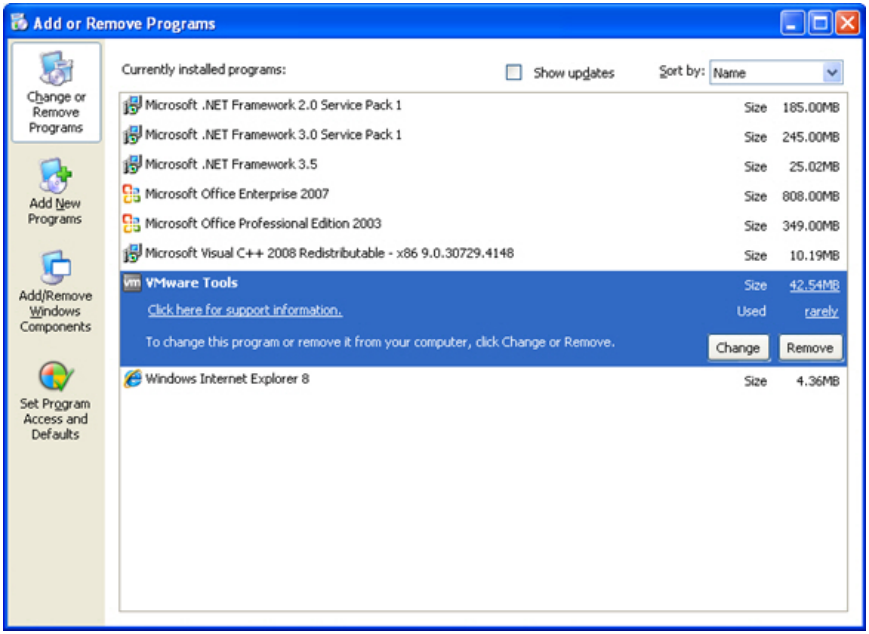


FIGURE 3-13. Add or Remove Programs (Windows XP)

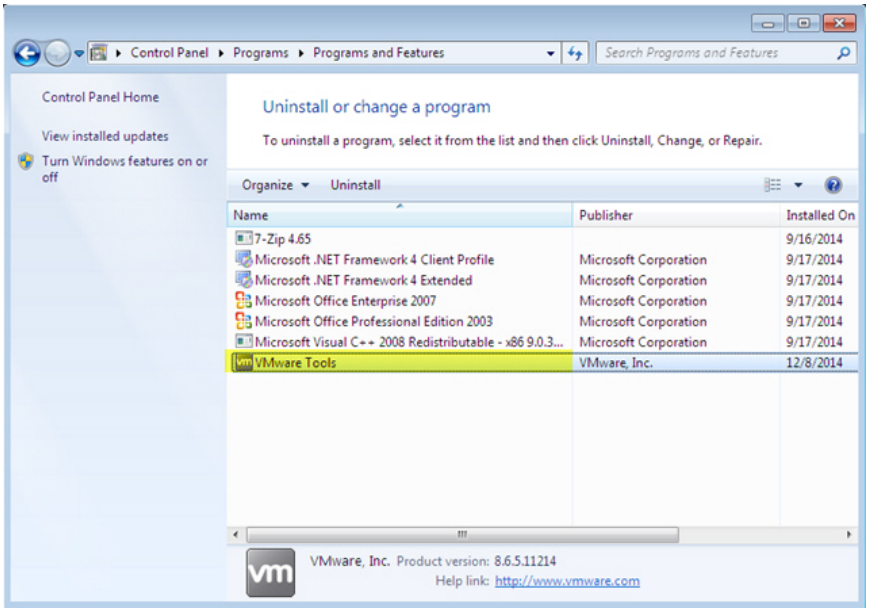


FIGURE 3-14. Add or Remove Programs (Windows 7)

3. Select **VMware Tools** and then click **Remove** (Windows XP or Windows Server 2003) or **Uninstall** (Other supported Windows and Windows Server versions).
4. Click **Yes** to uninstall VMware Tools.
5. Click **Yes** to restart Windows.

VMware Tools is uninstalled.

Exporting Virtual Machine Images

You must verify and modify some settings before exporting a virtual machine image from VMware ESXi or Workstation.

- *Verifying Virtual Machine Settings on VMware Workstation on page 3-27*
- *Exporting Virtual Machine Images on VMware ESXi on page 3-29*

- *Converting VMware ESXi Virtual Hard Disk Drives on page 3-33*

Verifying Virtual Machine Settings on VMware Workstation

Procedure

1. Shut down the virtual machine.
2. In the left pane, right-click the virtual machine and then select **Settings**.

   The **Virtual Machine Settings** screen appears.

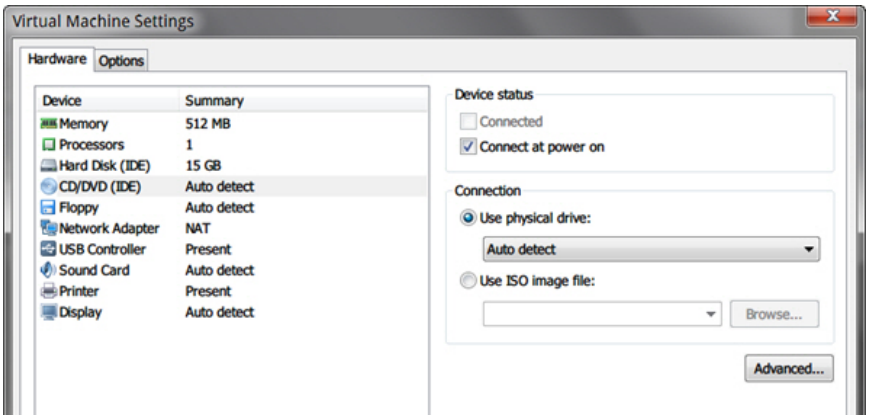


FIGURE 3-15. Virtual Machine Settings

3. On the **Hardware** tab, verify the following:
   - **CD/DVD (IDE)**: **Connection** is **Use physical drive**.
   - **Floppy**: **Connection** is **Use physical drive**.

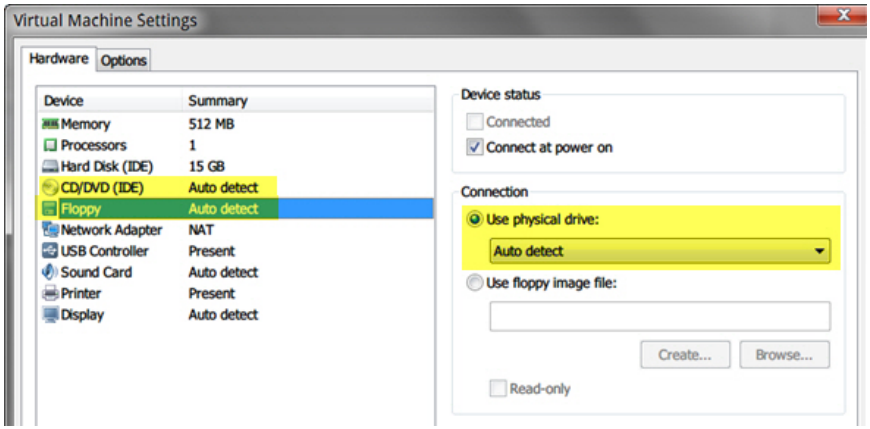


FIGURE 3-16. Virtual Machine Settings - Hardware

4. Go to the **Options** tab and then click **General**.
5. In the right pane, under **Working directory**, locate the Virtual Machine Disk (`*.vmdk`).

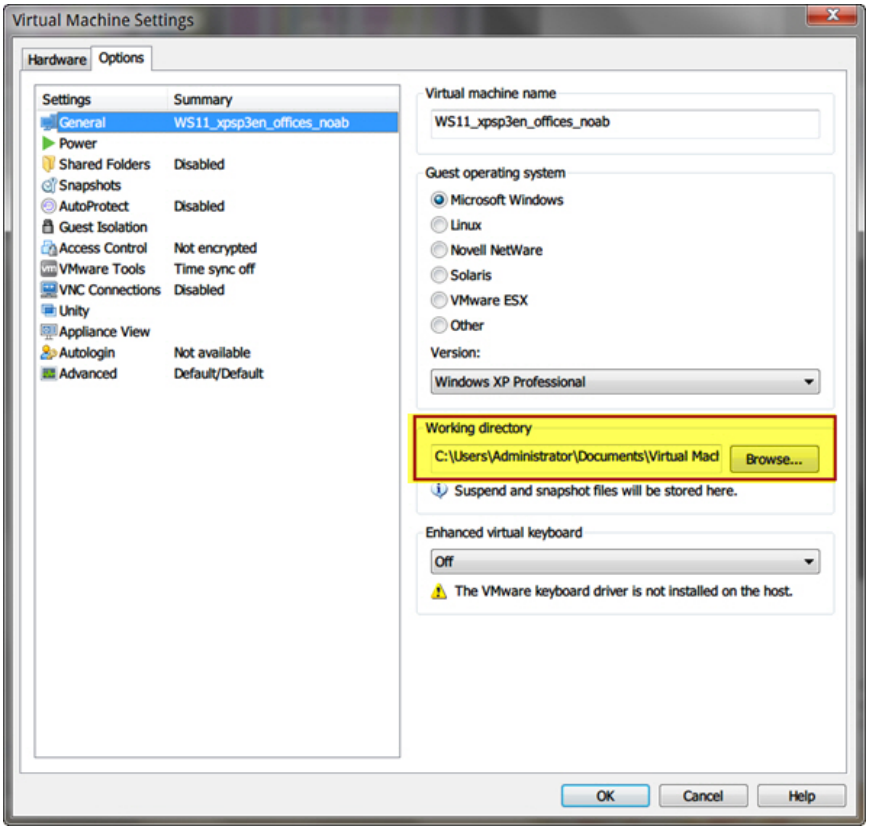


FIGURE 3-17. Working Directory

Exporting Virtual Machine Images on VMware ESXi

Procedure

1. Shut down the virtual machine.
2. In the left pane, right-click the virtual machine and then select **Edit Settings**.

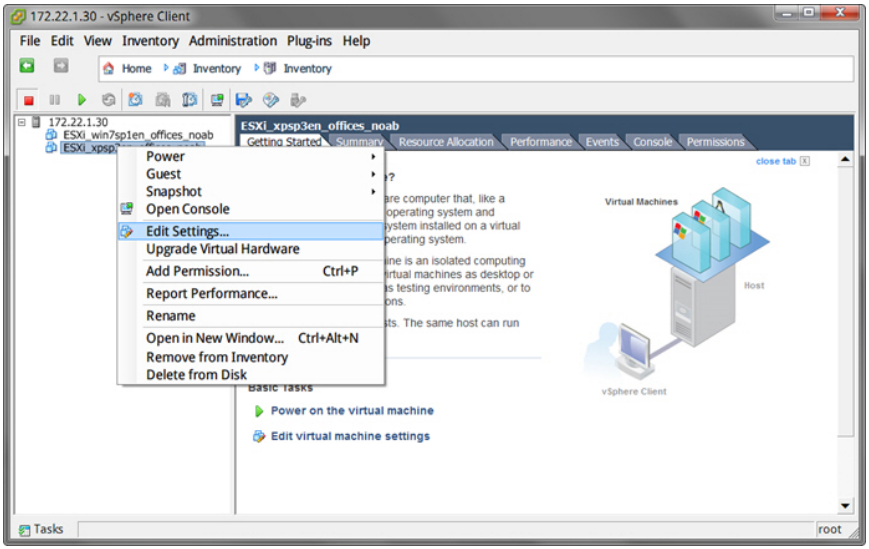


FIGURE 3-18. Edit Settings

The **Virtual Machine Properties** screen appears.

3. On the **Hardware** tab, verify the following settings:
   - **CD/DVD drive 1**: **Client Device**
   - **Floppy drive 1**: **Client Device**

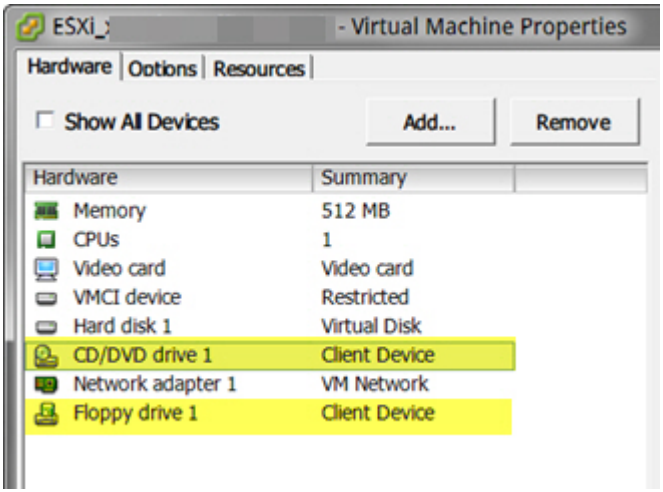


FIGURE 3-19. Virtual Machine Properties - Hardware

4. In the left pane, select the virtual machine and then go to **File** > **Export** > **Export OVF Template**.

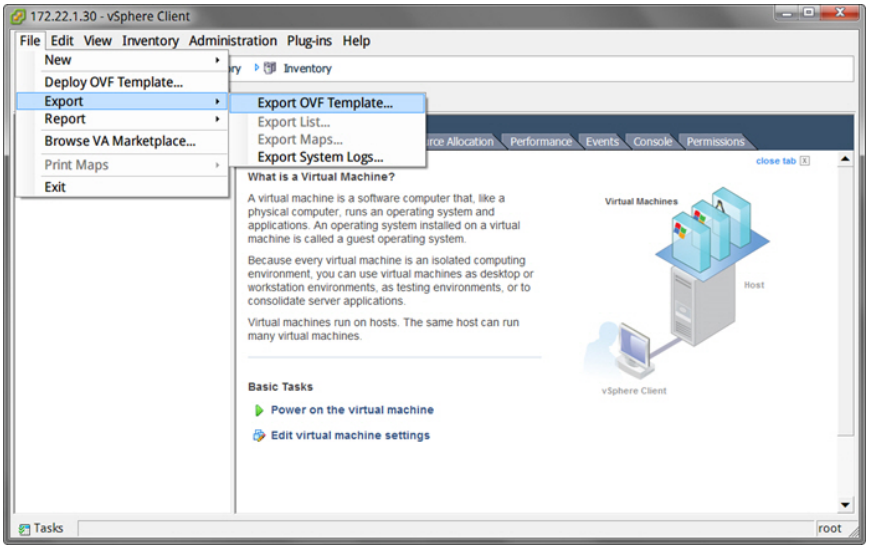


FIGURE 3-20. OVF Template

The **Export OVF Template** screen appears.

5. Configure the following settings:

   - **Name**: Type a name for the virtual machine image.

   Note

   (Optional) Click the **folder** icon to change the path of the OVF template files.

   - **Format**: Select **Folder of files (OVF)**.

   Important

   Verify that **Include image files attached to floppy and CD/DVD devices in the OVF package** is not selected.

6. Click **OK**.

Converting VMware ESXi Virtual Hard Disk Drives

VirtualBox does not support the virtual hard disk drive format (`*.vmdk`) of VMware ESXi images. Use one of the following tools to convert the disks:

- *Using VMware vCenter Converter Standalone on page 3-33*
- *Using QEMU on page 3-39*

Using VMware vCenter Converter Standalone

Procedure

1. Download VMware vCenter Converter Standalone from https://my.vmware.com/web/vmware/info/slug/infrastructure_operations_management/vmware_vcenter_converter_standalone/5_5#product_downloads.

   Note

   VMware vCenter Converter Standalone 5.0 does not support vCenter Server and ESXi versions later than 5.0. Download and install a version later than 5.0.1.

2. Open VMware vCenter Converter Standalone and then click **Convert machine**.

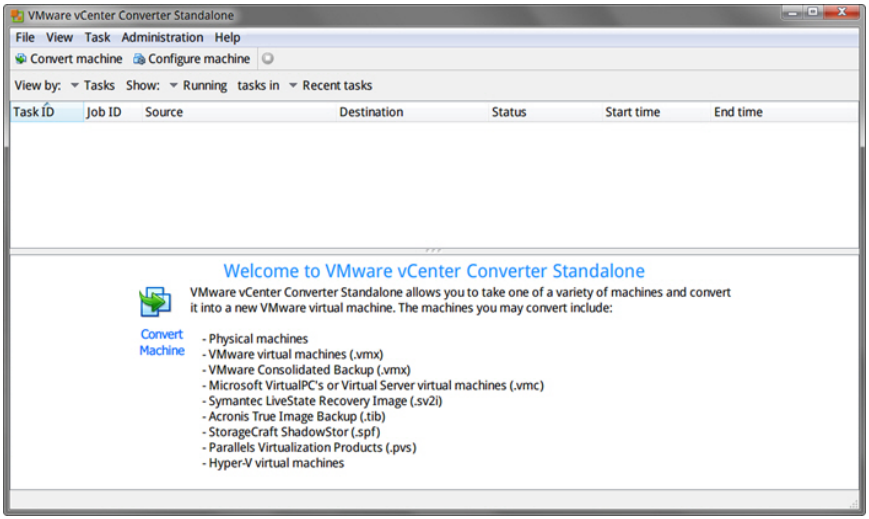


FIGURE 3-21. VMware vCenter Converter Standalone

The **Conversion** window opens.

3. On the **Source System** screen, configure the following:
   a. **Select source type**: Select **VMware Infrastructure virtual machine**.
   b. **Server**: Type the ESXi server IP address.
   c. **User name**, **Password**: Type the credentials that provide administrator access to the VMware server.
4. Click **Next**.

The **Source Machine** screen appears.

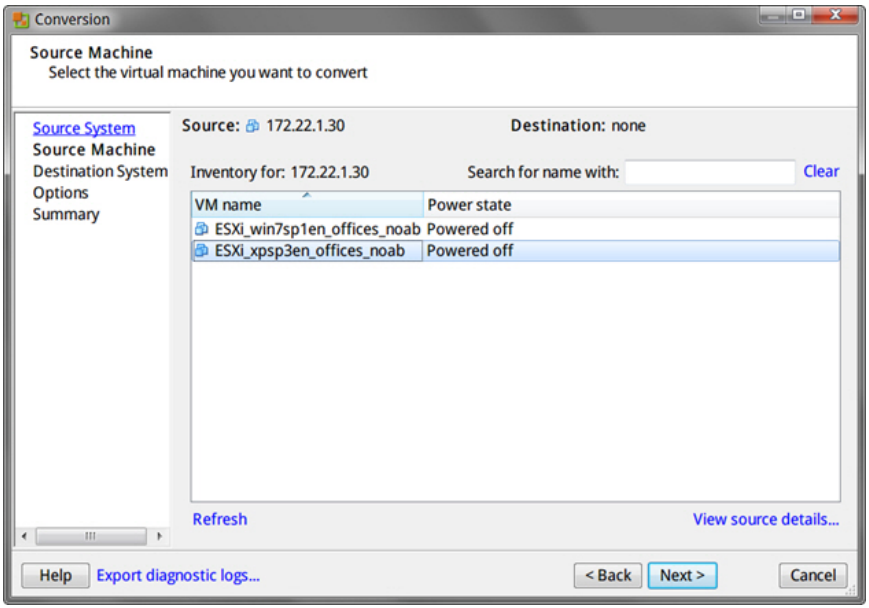


FIGURE 3-22. Conversion > Source Machine

5. Select the virtual machine that you want to convert and then click **Next**.

The **Destination System** section appears.

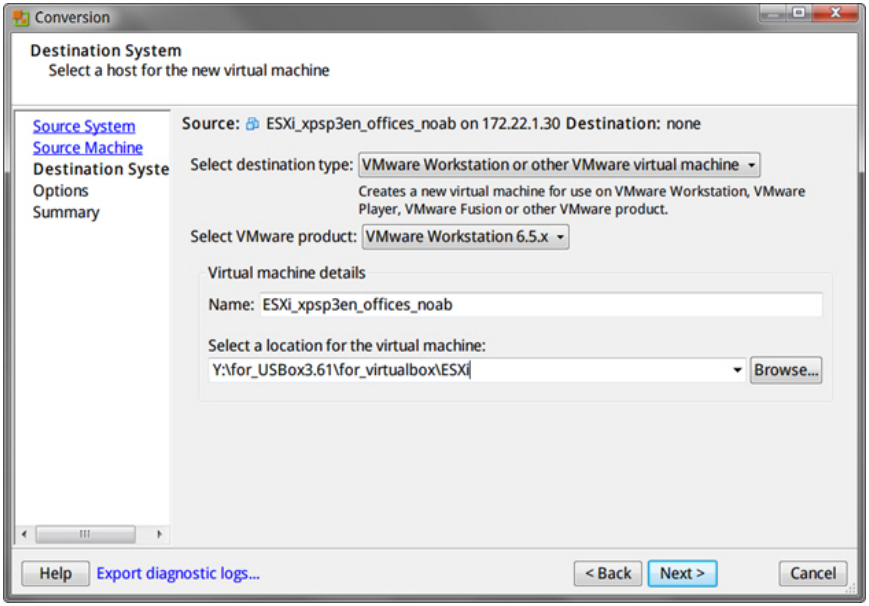


FIGURE 3-23. Conversion > Destination System

6. Configure the following and then click **Next**.

   a. **Select destination type**: Select **VMware Workstation or other VMware virtual machine**.

   b. **Select VMware product**: Select **VMware Workstation 6.5.x**.

   c. **Virtual machine details**: Accept the default name and location or click **Browse** to select a different file.

The **Options** screen appears.

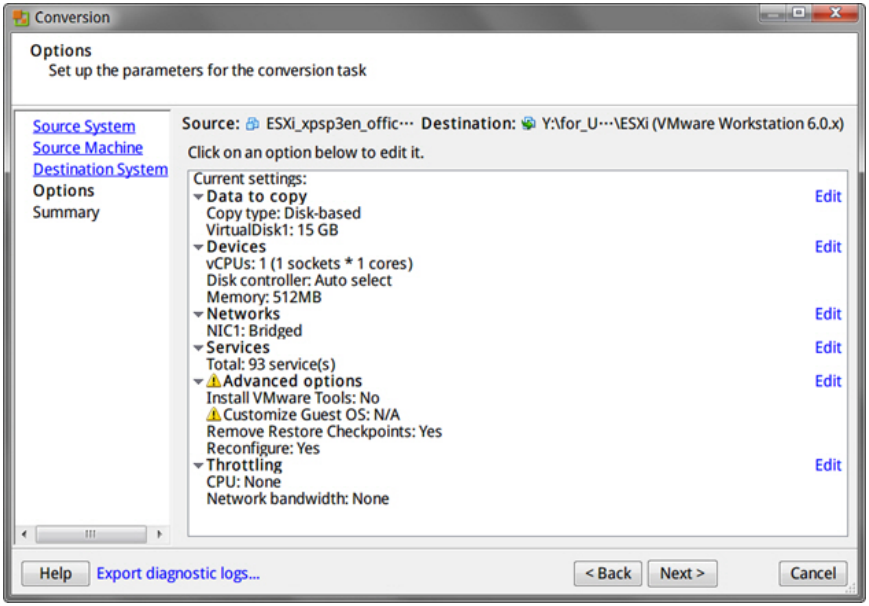


FIGURE 3-24. Conversion > Options

7. Verify the settings and then click **Next**.

Important

Verify that **Install VMware Tools** is set to **No**.

The **Summary** screen appears.

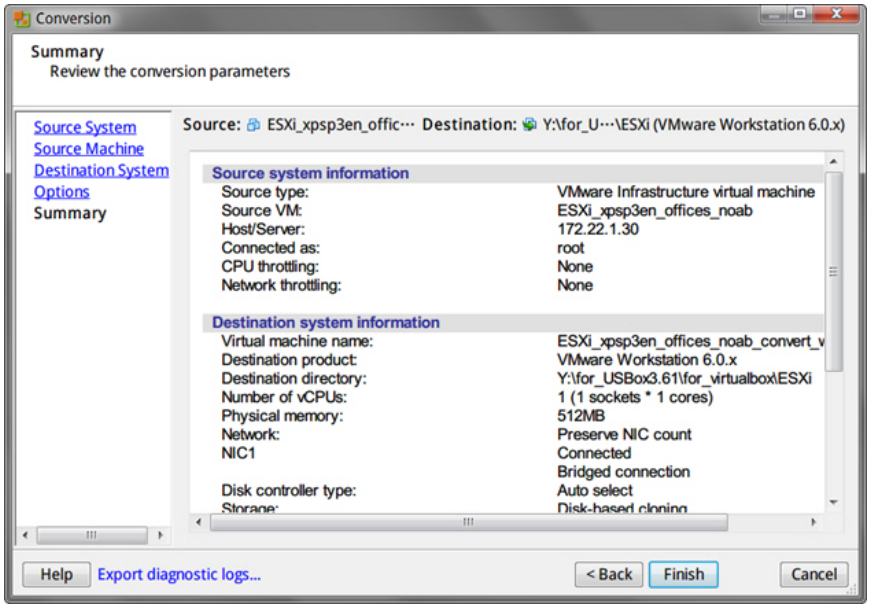


FIGURE 3-25. Conversion > Summary

8. Verify the information and then click **Finish**.

VMware vCenter Converter Standalone converts the Virtual Machine Disk (`*.vmdk`).

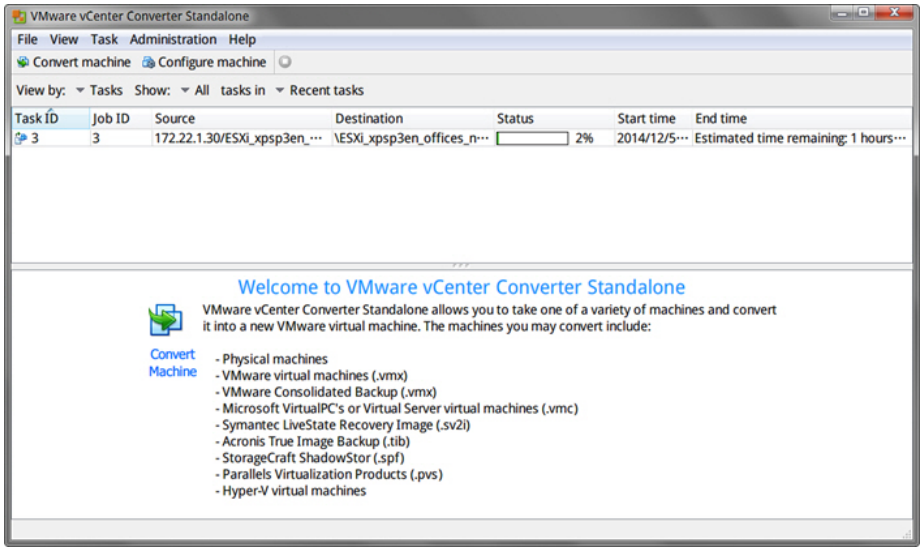


FIGURE 3-26. Image Conversion Progress

Using QEMU

For details on QEMU, see http://wiki.qemu.org/Main_Page.

Procedure

1. Download the latest version of QEMU from http://qemu.weilnetz.de/w64/.
2. Install QEMU with the default settings.
3. Open a Command Prompt window (`cmd.exe`) using an account with administrator privileges.
4. Convert the Virtual Machine Disk (`*.vmdk`) by typing the following command:

`qemu-img.exe convert [-f fmt] [-O output_fmt] filename output_filename`.

For example:

```
"C:\Program Files\qemu\qemu-img.exe" convert -f vmdk -O vmdk
C:\ESX_xpsp3en_offices_noab.vmdk C:\ESX_xpsp3en_offices_noab_converted.vmdk
```

The `*.vmdk` file can be used to create an OVA file using VirtualBox.

Creating Virtual Machine Images Using Converted Virtual Hard Disk Drives

Use VirtualBox to create a new virtual machine image.

- *Downloading and Installing VirtualBox on page 2-7*
- *Creating Virtual Machine Images Using VirtualBox on page 3-41*

Downloading and Installing VirtualBox

Procedure

1. Download the latest version of VirtualBox from https://www.virtualbox.org/wiki/Downloads.

   Note

   The VirtualBox Open Source Edition is licensed under the GPL V2. The full text of the license is available at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

   Trend Micro recommends using VirtualBox version 7.0 and later.

   Important

   VirtualBox version 7.0 and later is required for Windows 11 virtual machines.

2. Configure the language settings using one of the following methods:
   - Install VirtualBox with English as the default language.
   - After installation, go to **File** > **Preferences** > **Language** and then select **English**.

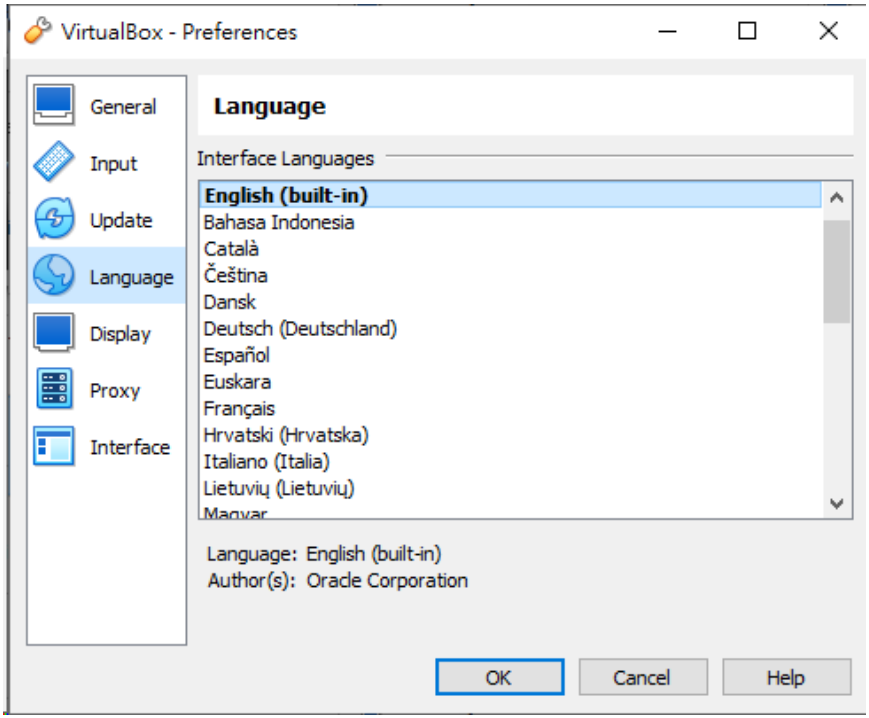


FIGURE 3-27. Language Settings

Creating Virtual Machine Images Using VirtualBox

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.

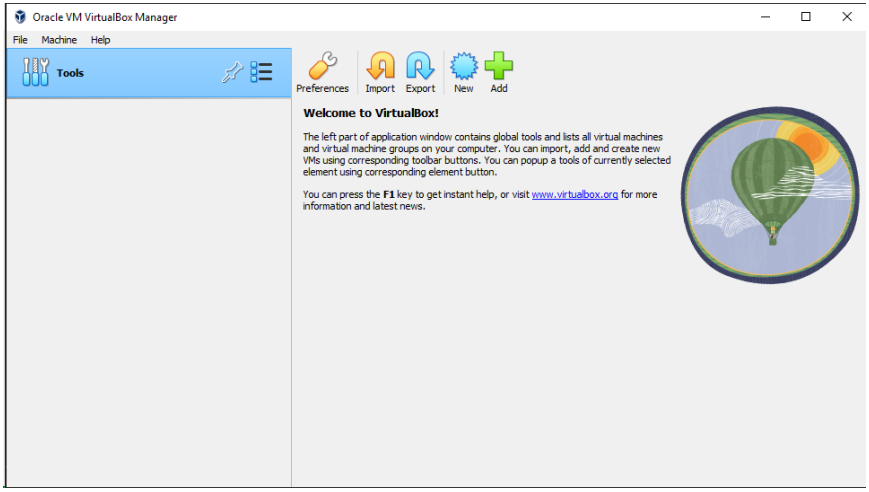


FIGURE 3-28. VirtualBox Manager

2. Click **New**.

   The **Create Virtual Machine** window opens.

3. Click **Expert Mode**.

The Create Virtual Machine wizard enters Expert Mode.

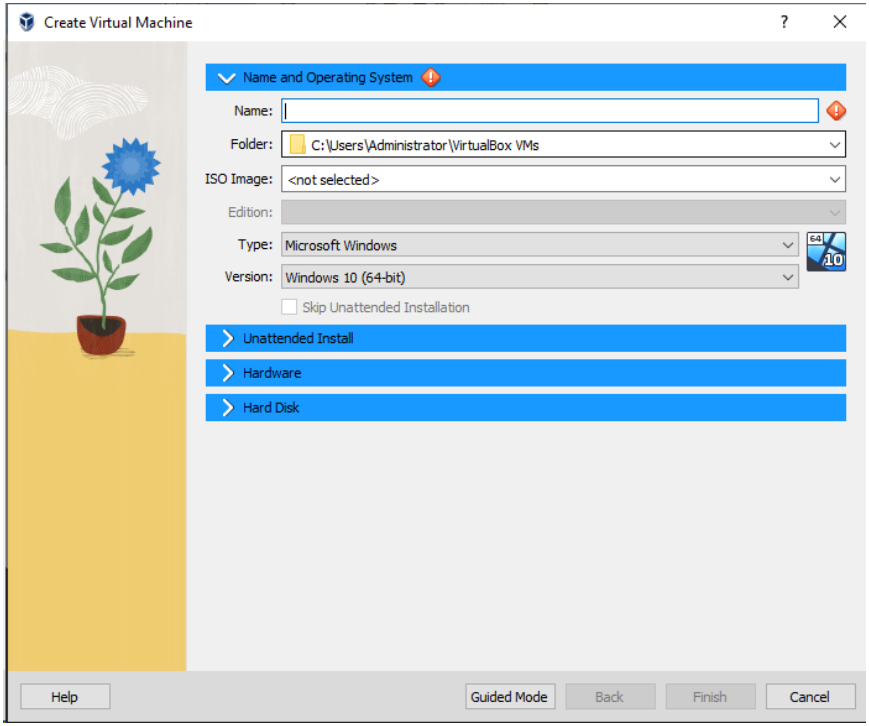


FIGURE 3-29. Create Virtual Machine - Expert Mode

4. Configure the **Name and Operating System** settings.
   - Type a permanent and unique **Name** for the virtual machine.
   - Specify the **Folder** to store the completed virtual machine.
   - For the **Type**, select **Microsoft Windows**.
   - For the **Version**, select the version of Windows you want to use for the virtual machine.

     For a list of supported Windows OS versions, see *Required Software on page 2-2*.

5. Open the **Hardware** section.

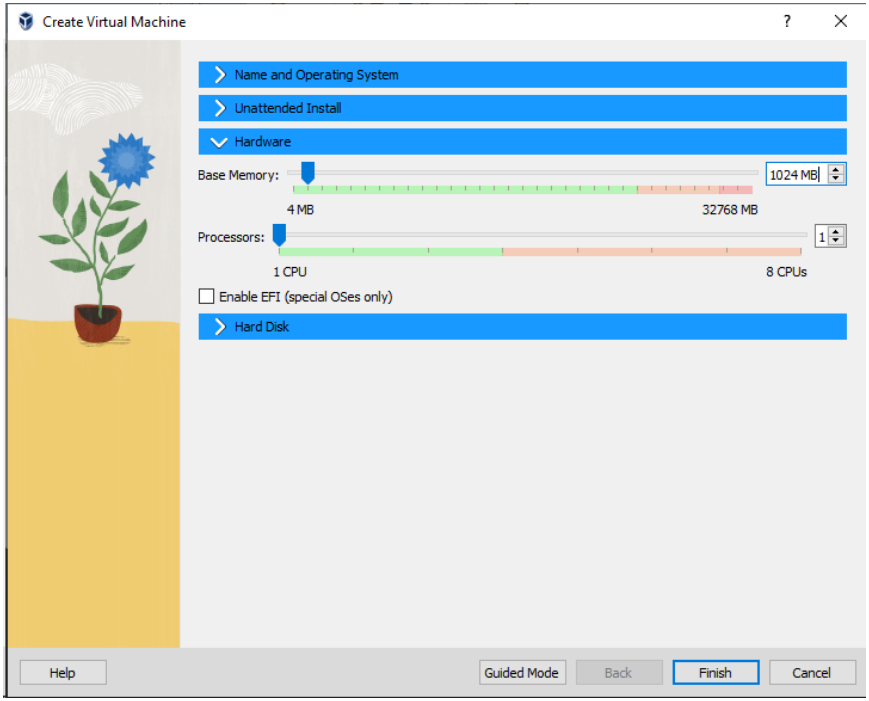


FIGURE 3-30. Hardware

6. Specify the recommended memory size for your operating system.
   - For Windows XP and Windows Server 2003, specify at least 512 MB
   - For Windows 11, specify at least 2048 MB
   - For all other supported versions of Windows and Windows Server, specify at least 1024 MB.
7. For Windows 11, select **Enable EFI (special OSes only)**.
8. Open the **Hard Disk** section.

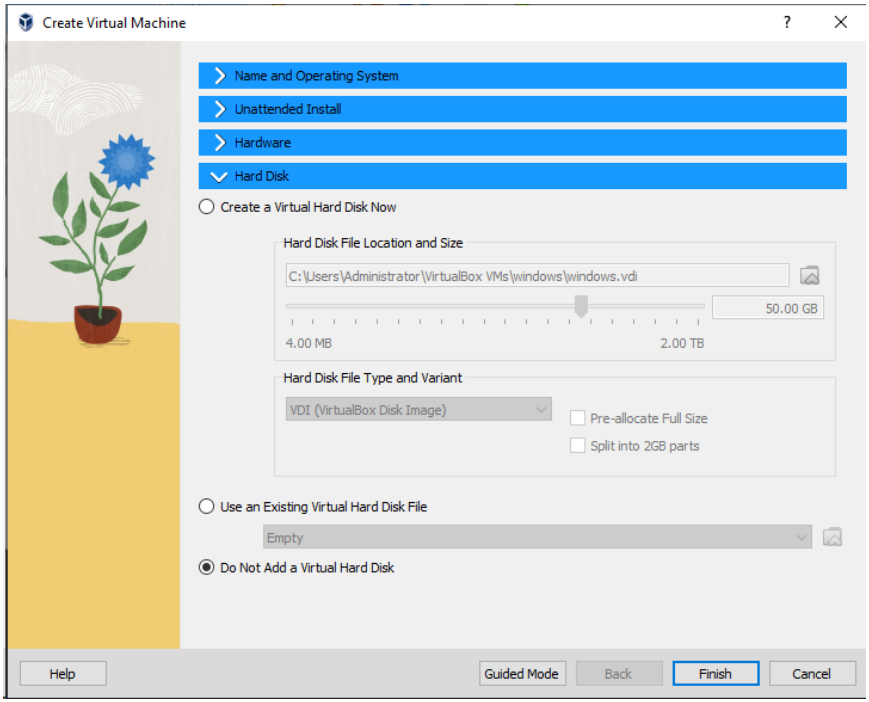


FIGURE 3-31. Hard Disk

9. Select **Do Not Add a Virtual Hard Disk**.
10. Click **Finish**.

VirtualBox creates the virtual machine. The new virtual machine appears in the left pane.

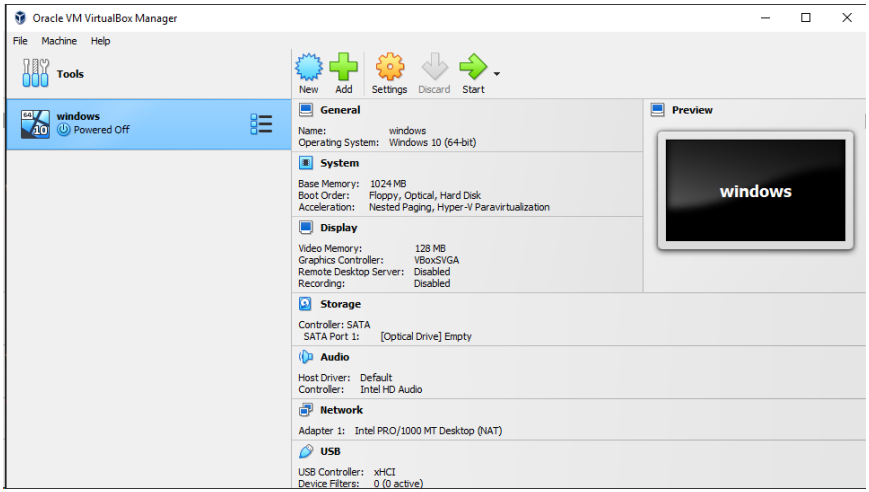


FIGURE 3-32. Newly-created Virtual Machine

11. Click **Settings**.

The **Settings** window opens.

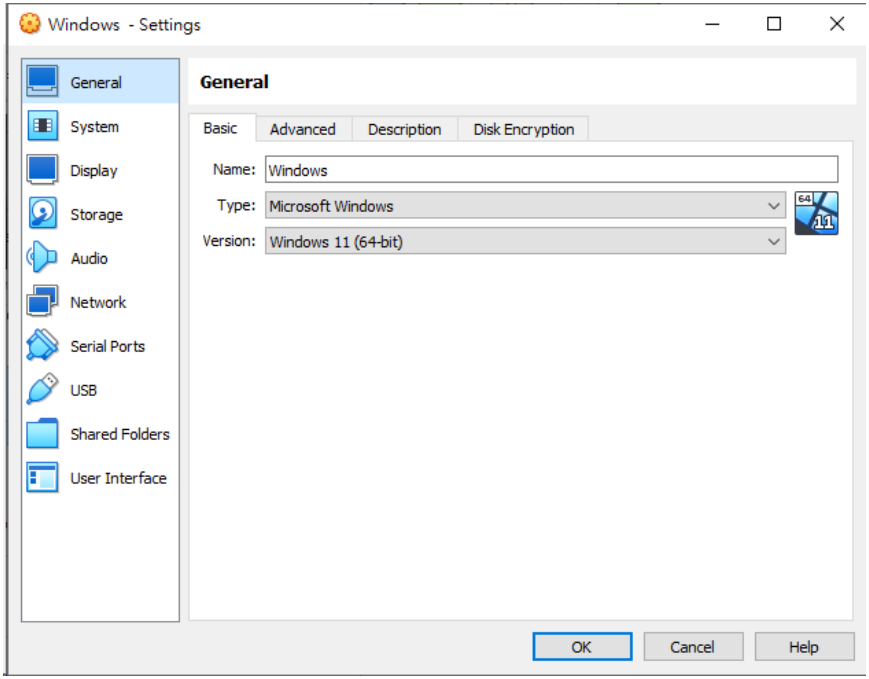


FIGURE 3-33. VirtualBox Settings

12. Go to **System**.

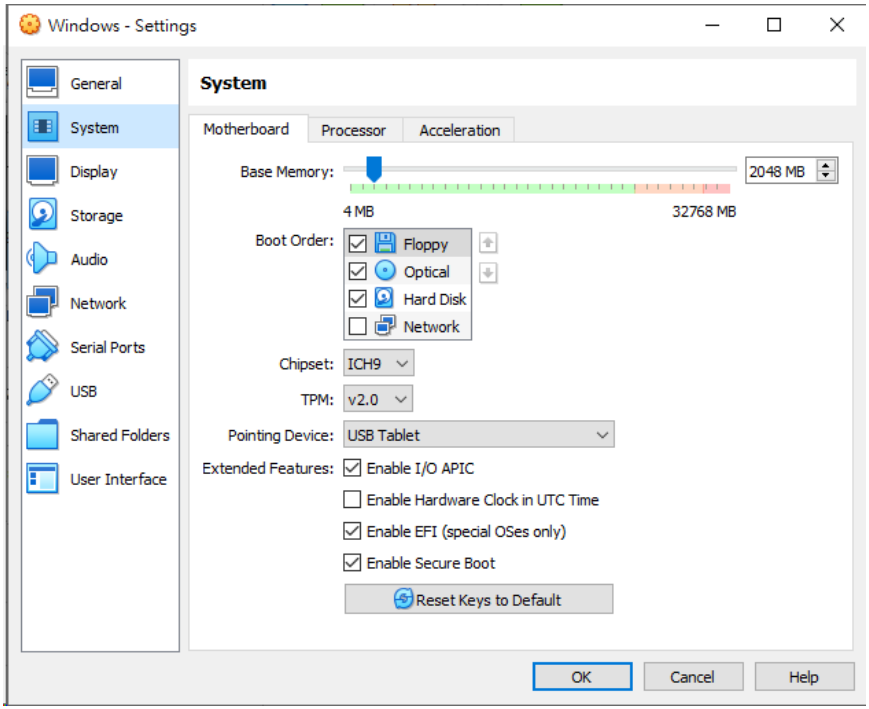


FIGURE 3-34. System Screen

13. Configure the settings on the **Motherboard** tab.
    - For **Chipset**, select **ICH9**.
    - For **TPM**, select **v2.0**.

      Important

      TPM v2.0 is required for Windows 11. The setting is optional for all other supported Windows versions.

    - For **Pointing Device**, select **USB Tablet**
    - Select the following **Extended Features**:
      - **Enable I/O APIC**

- **Enable EFI (special OSes only)**
- **Enable Secure Boot**

Important

For Windows 11 virtual machines, **Enable EFI (special OSes only)** and **Enable Secure Boot** are required settings. The settings are optional for all other versions of Windows.

Use **Enable EFI (special OSes only)** if you want to create EFI-compatible images. EFI-compatible images are only supported by the following Trend Micro products:

- Deep Discovery Inspector 5.6 and later
- Deep Discovery Email Inspector 3.6 and later
- Deep Discovery Analyzer 6.8 and later
- Deep Discovery Director 5.1 and later
- Deep Discovery Web Inspector 2.5 and later

14. On the **Processor** tab, select **Enable PAE/NX**.
15. On the **Acceleration** tab, select **Enable Nested Paging**.

    If you are using VirtualBox 5.2 and before, also select **Enable VT-x/AMD-V**.

Note

- The **Acceleration** tab is only available if the processor of the host system supports virtualization technology and the virtualization setting is enabled in the BIOS of the host system.
- VirtualBox 6.0 and later automatically enables VT-x/AMD-V if the processor of the host system supports virtualization technology and the virtualization setting is enabled in the BIOS of the host system.

16. Go to **Storage**.

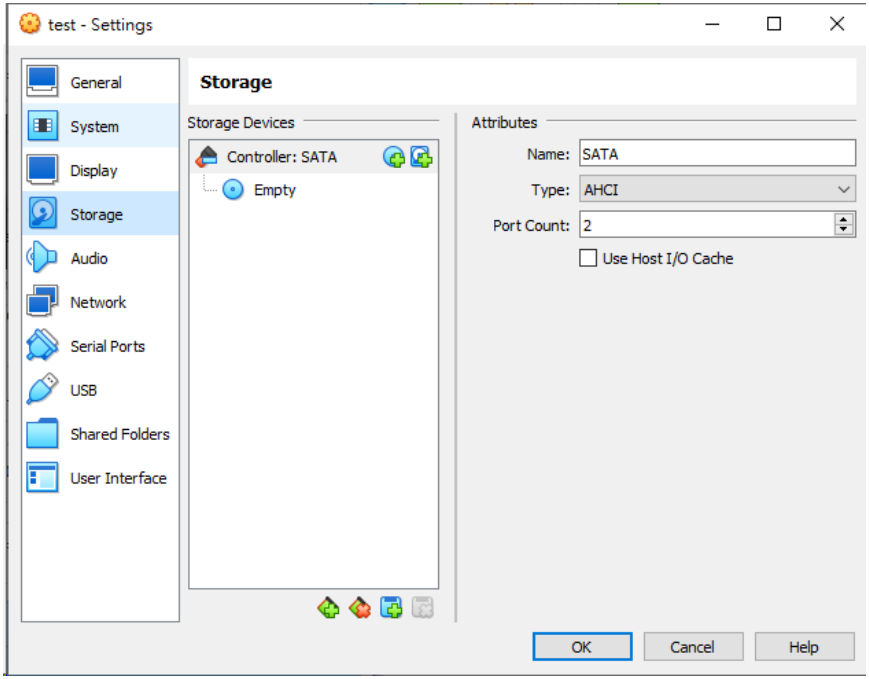


FIGURE 3-35. Storage Screen

17. If **Controller: SATA** appears under **Storage Devices**, select the controller and click to remove the SATA controller.

18. Add an IDE controller.

    a. Click and select **PIIX4 (Default IDE)**.

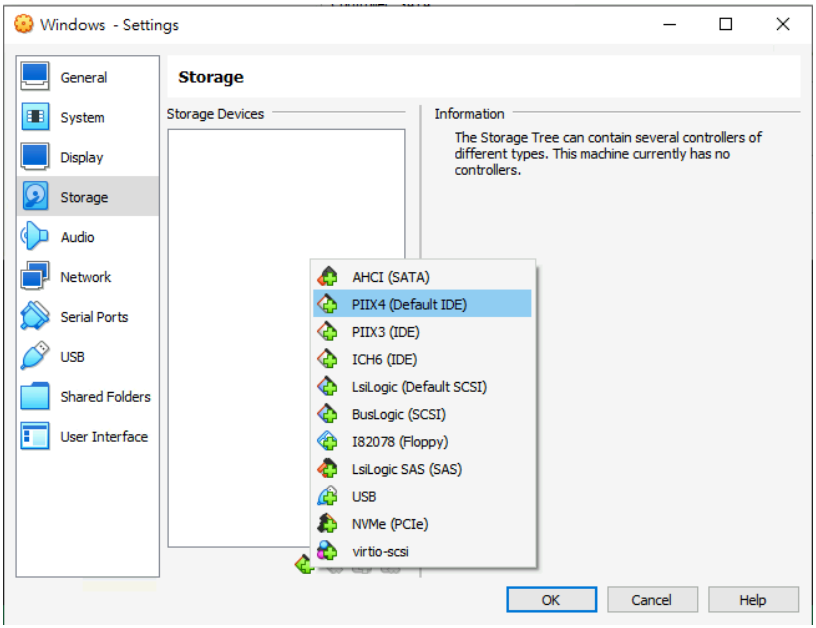


FIGURE 3-36. Add Storage Controller

Controller: PIIX4 appears on the Storage Devices list.

b. Click the controller and change the **Name** attribute to **`IDE`**.

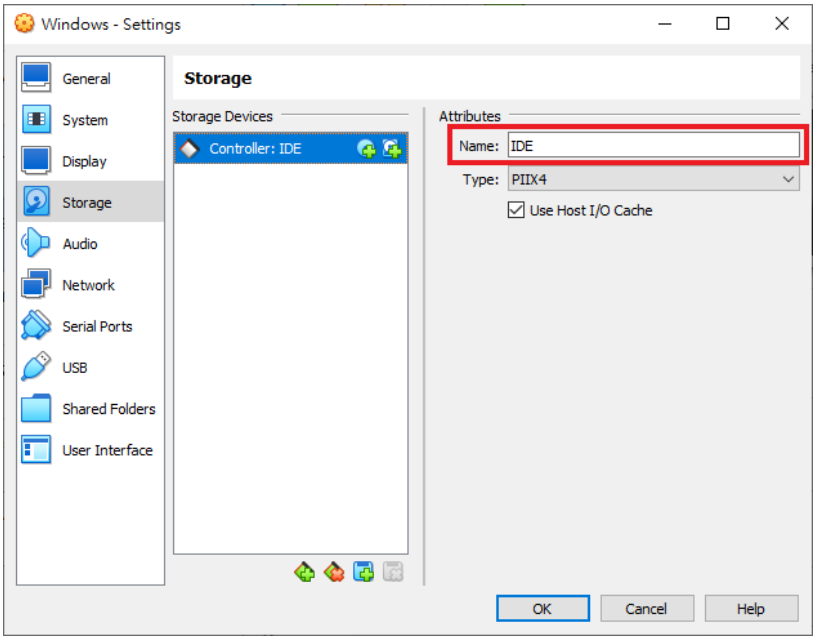


FIGURE 3-37. Controller IDE

c. Select **Use Host I/O Cache**.

d. Click **Controller: PIIX4** and then click .

The **Hard Disk Selector** window appears.

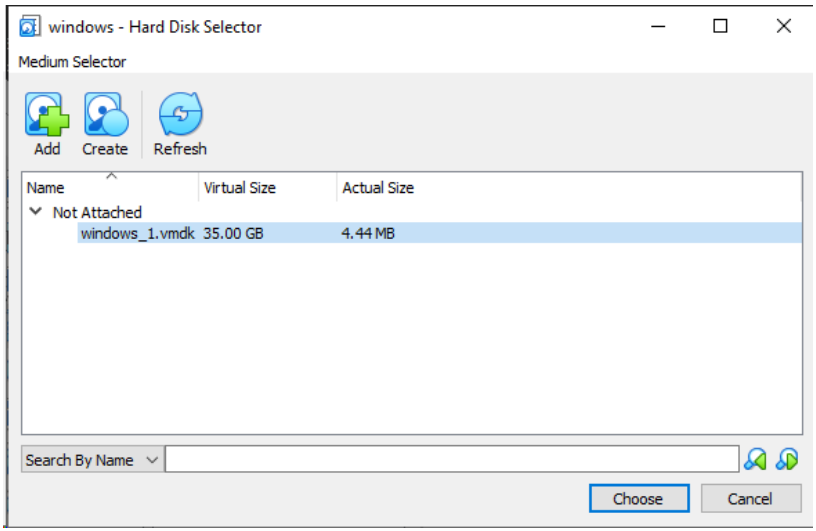


FIGURE 3-38. Hard Disk Selector

e. Select the converted VMDK file you want to use and click **Choose**.

f. Click **Controller: IDE** and then click to create an optical drive.

g. In the **Optical Disk Selector** window, click **Leave Empty**.

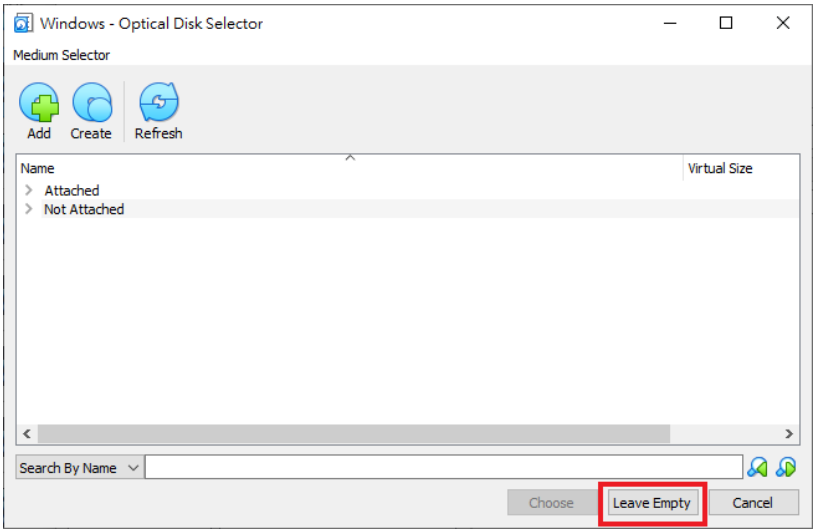


FIGURE 3-39. Optical Disk Selector

h. Click the optical drive you created and verify the **Optical Drive** attribute is set to **IDE Secondary Device 0**.

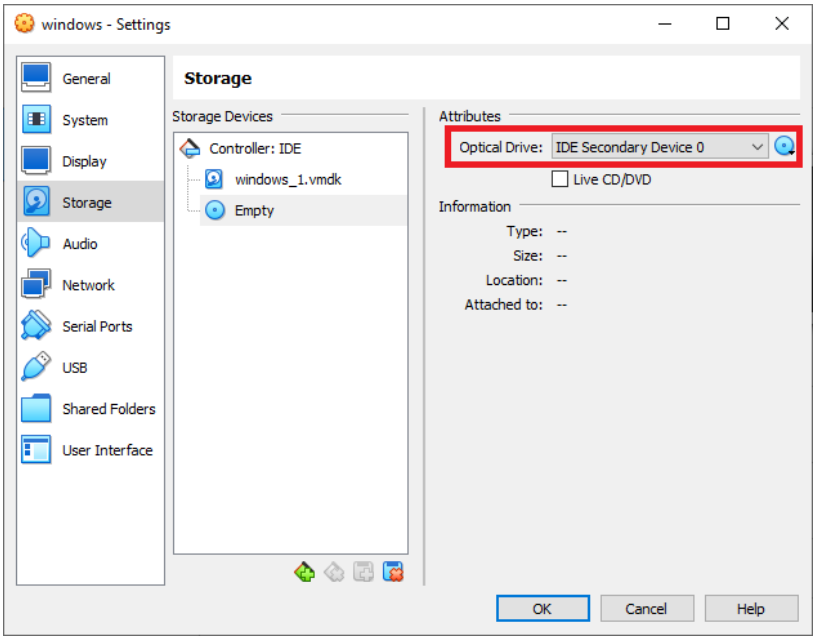


FIGURE 3-40. IDE Secondary Device 0

You should only have one **Controller: IDE** listed under Storage Devices. If there are any other controllers listed, remove the extra controllers.

19. (Optional) Go to **Audio** and verify that **Enable Audio** is selected.

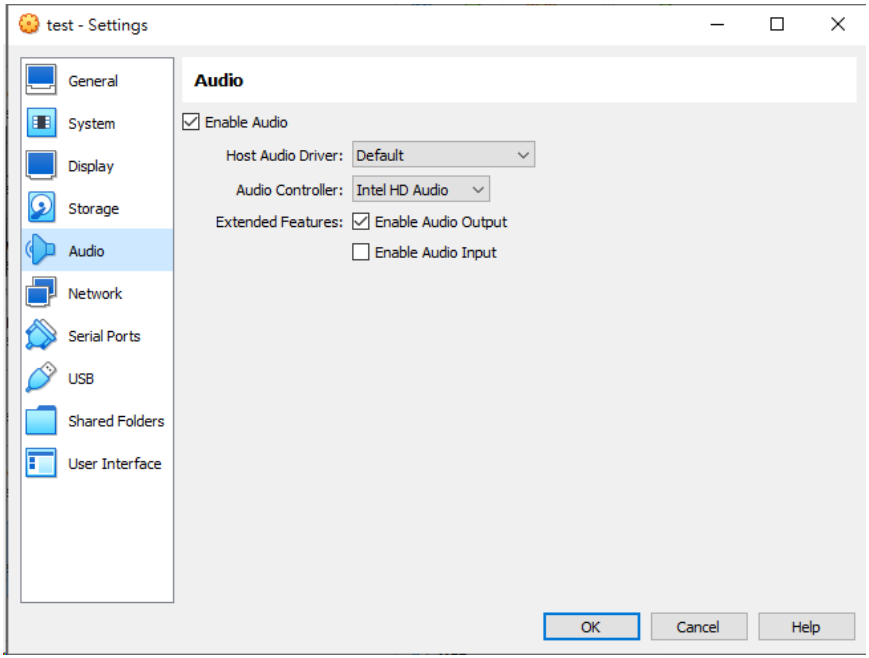


FIGURE 3-41. Audio Options Settings

20. Go to **USB**.

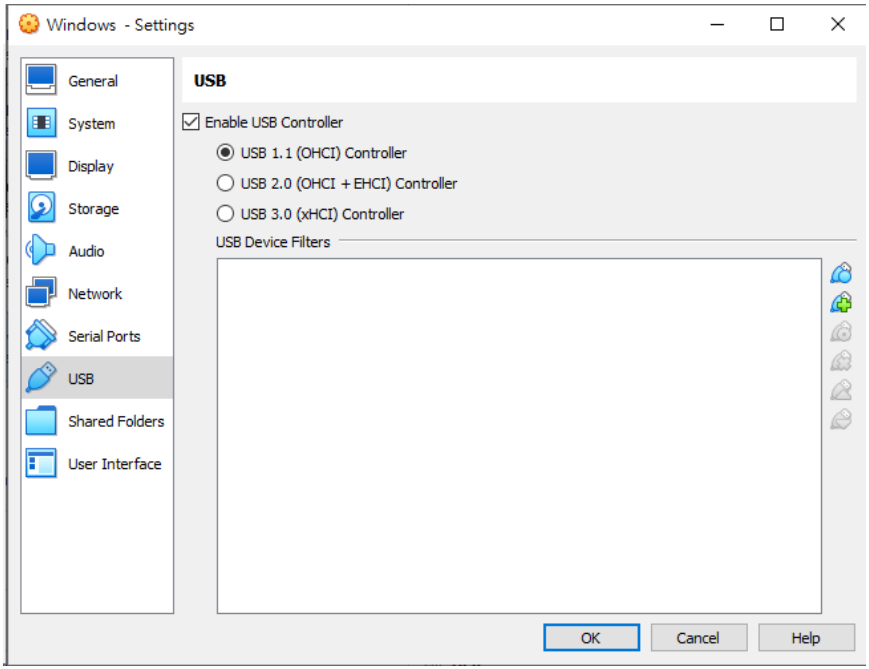


FIGURE 3-42. USB Settings

21. Select **Enable USB Controller**.
22. Select **USB 1.1 (OHCI) Controller**.
23. Go to **Shared Folders** and verify that no folders are shared.

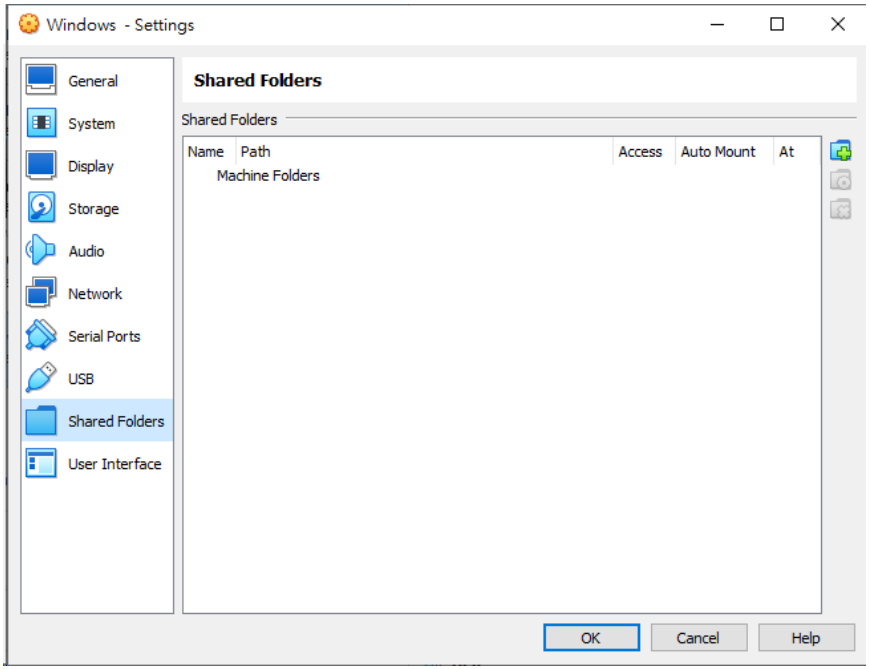


FIGURE 3-43. Shared Folders Settings

24. Click **OK**.

25. On the **VirtualBox Manager** screen, click 

to power on the image.

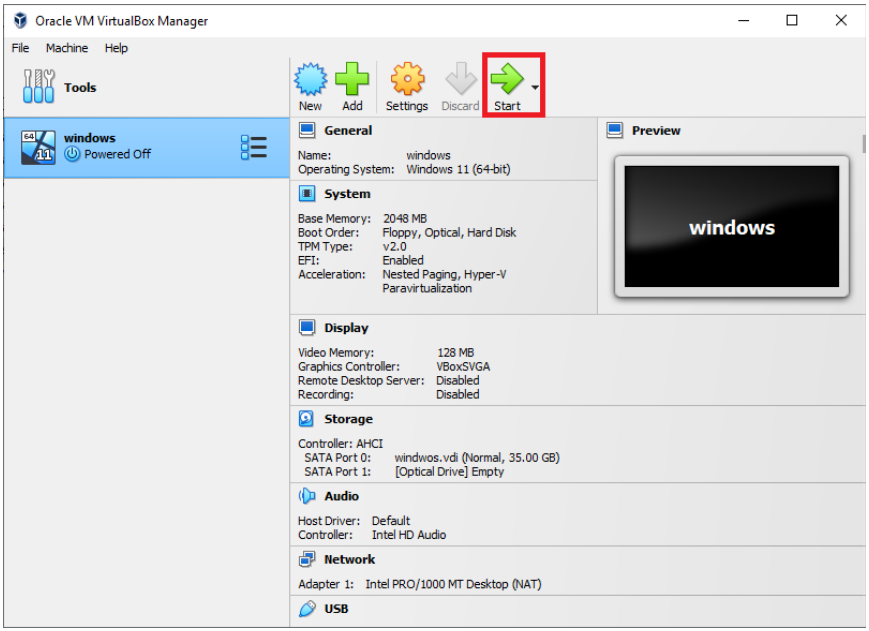


FIGURE 3-44. VirtualBox Manager

The installation process starts.

26. Install Microsoft Office and other required software to achieve satisfactory detection results.

Important

Verify there is at least 3072 MB free virtual disk space on the virtual machine to ensure normal operation of Virtual Analyzer.

Configuring Virtual Machine Images

Configure virtual machine images that were created using converted virtual hard disk drives to avoid importing issues.

- *Configuring Virtual Machine Images (Windows XP and Windows Server 2003) on page 3-60*
- *Configuring Virtual Machine Images (All Other Supported Windows Versions) on page 3-63*

Configuring Virtual Machine Images (Windows XP and Windows Server 2003)

Procedure

1. On the guest operating system, click **Start**, right-click **My Computer**, and then click **Manage**.

   The **Computer Management** screen appears.

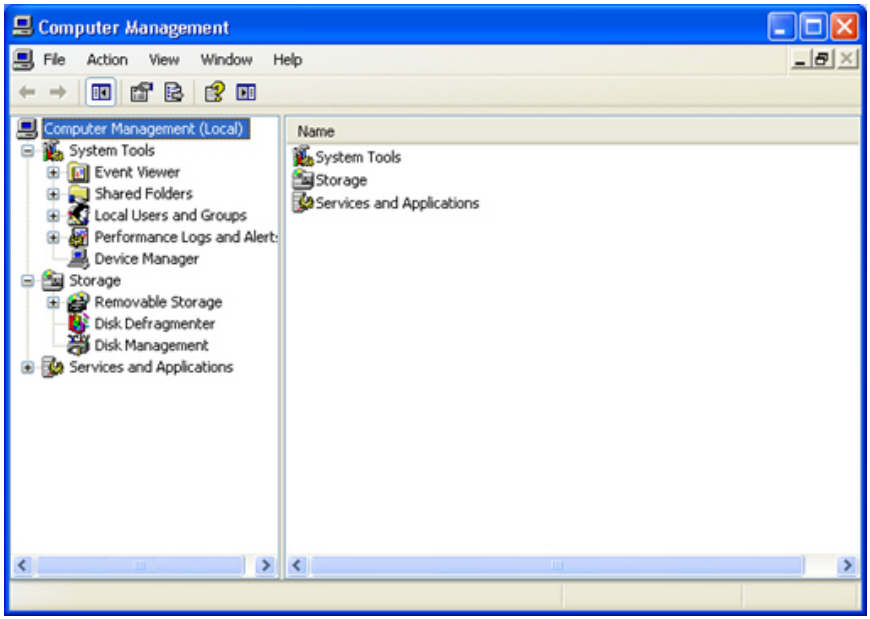


FIGURE 3-45. Computer Management

2. In the left pane, click **Device Manager**.

A list of devices appears.

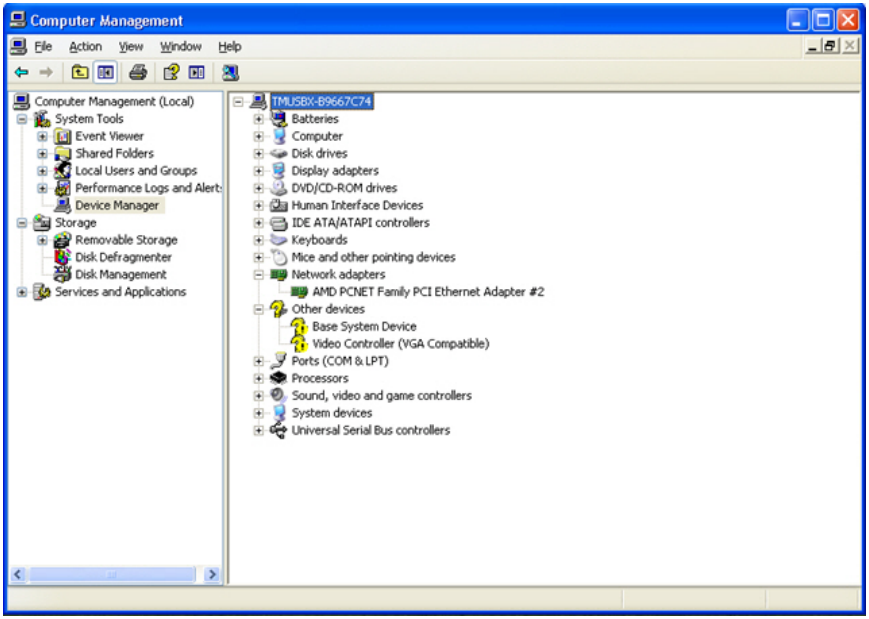


FIGURE 3-46. Device Management - Network Adapter Window

3. In the right pane, click **Network adapters** and then verify that the network adapter driver is ready.
4. Open a Command Prompt window (`cmd.exe`) using an account with administrator privileges.
5. Disable the **Found New Hardware Wizard** by typing the following commands:
   - Windows XP 32-bit:

     ```
     reg add
     "HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\
     DeviceInstall\Settings" /v SuppressNewHWUI /t
     REG_DWORD /d 1 /f
     ```

- Windows XP 64-bit or Windows Server 2003:

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Pl
ugPlay\Parameters" /v SuppressUI /t REG_DWORD /d 1 /f
```

FIGURE 3-47. Found New Hardware Wizard

6. Restart the image and then verify that the **Found New Hardware Wizard** does not appear.
7. Power off the image.

Configuring Virtual Machine Images (All Other Supported Windows Versions)

Procedure

1. On the guest operating system, click **Start**, right-click **Computer**, and then click **Manage**.

   The **Computer Management** screen appears.

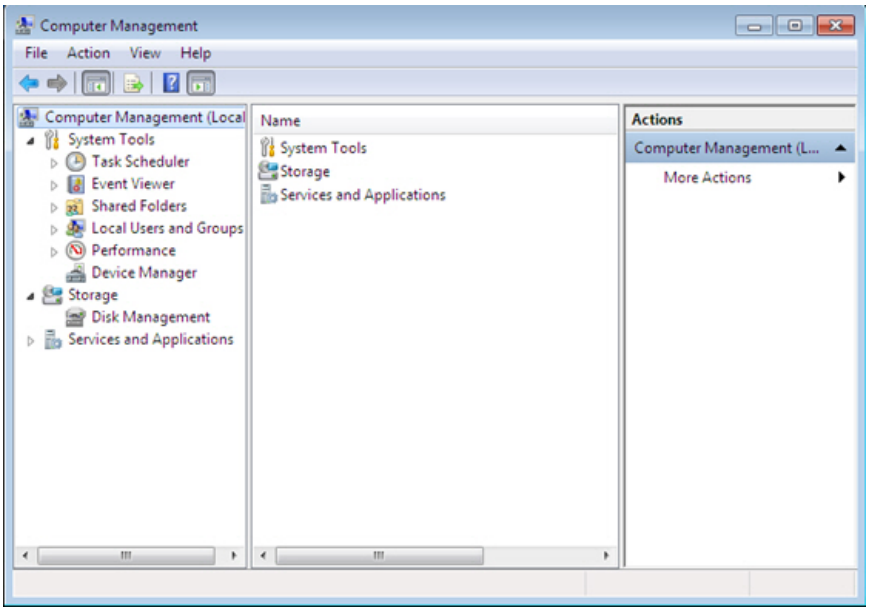


FIGURE 3-48. Computer Management

2. In the left pane, click **Device Manager**.

A list of devices appears.

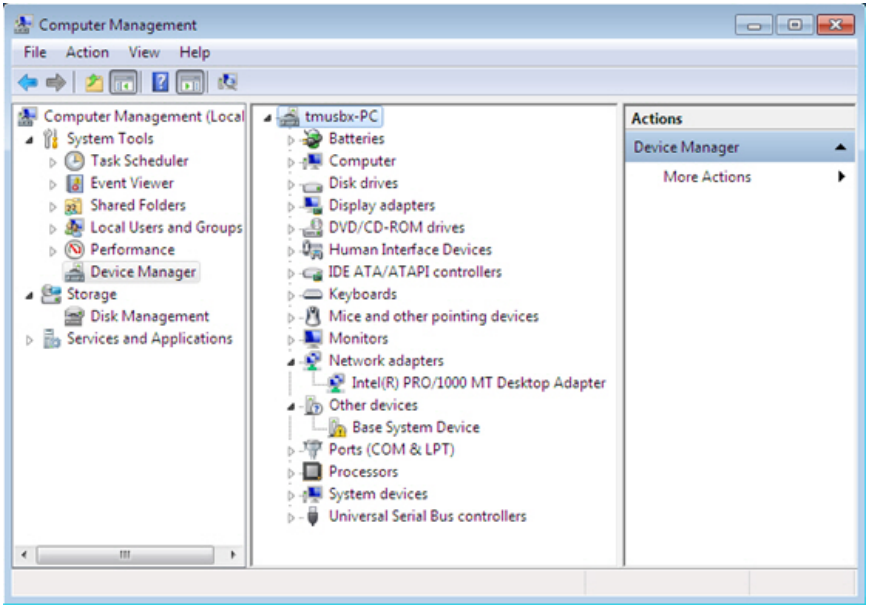


FIGURE 3-49. Device Management - Network Adapter

3. In the right pane, click **Network adapters** and then verify that the network adapter driver is ready.
4. Power off the image.

Exporting Virtual Machine Images to OVA Files

A virtual machine image comprises many uncompressed files. The files must be combined into a single OVA file to avoid issues when importing.

Important

Verify that the size of the created OVA file is supported by your product.

For details, go to https://docs.trendmicro.com/en-us/home.aspx#Enterprise.

Procedure

1. On the VirtualBox Manager screen, power off the virtual machine.

   Note
   Verify that the CD/DVD drive is empty before powering off and exporting.

2. Go to **File** > **Export Appliance**.

   The **Export Virtual Appliance** window appears.

3. Select the virtual machine image to export and click **Next**.

   The **Appliance settings** screen appears.

4. Configure the following:

   - **File**: Accept the default name and path or click  to select a different file.
   - **Format**: Select **OVF 1.0**.

     Important
     Format options include OVF 0.9, 1.0 and 2.0. Virtual Analyzer does not support OVF 2.0.

   - **MAC Address Policy**: Select **Include only NAT network adapter MAC addresses**.

5. Click **Next**.

   The **Virtual system settings** screen appears.

6. Verify that the **License** field is empty and then click **Export**.

VirtualBox creates the OVA file.

Chapter 4

Linux OVA File Preparation

There are two methods to prepare a Virtual Analyzer-supported Linux OVA file.

- Use the **Predefined Linux Virtual Analyzer Image** from Trend Micro.

  Trend Micro provides pre-configured images with all required packages installed and optimized system settings for the following operating systems:

  - CentOS 7.8
  - Ubuntu 20.04.6

  Download the **Predefined Linux Virtual Analyzer Image** from the Trend Micro Download Center, or obtain a copy from your support provider.

  After customization, use the tool to validate the image.

  Note

  The **Predefined Linux Virtual Analyzer Image** is not available for RHEL 7.9 or RHEL 8.3.

- Create your own Virtual Analyzer-supported Linux OVA file from scratch.

- *Required Software on page 4-3*
- *Downloading and Installing VirtualBox on page 4-12*
- *Creating Linux Virtual Machine Images on page 4-13*
- *Modifying the Virtual Machine Environment on page 4-44*
- *Reducing the Size of VirtualBox Disk Images on page 2-44*
- *Exporting Virtual Machine Images to OVA Files on page 4-45*

Creating Linux OVA Files From Scratch

Procedure

1. Prepare the operating system and required applications.

   For details, see *Required Software on page 4-3*.

2. Download and install VirtualBox.

   For details, see *Downloading and Installing VirtualBox on page 4-12*.

3. Create a virtual machine image.

   For details, see *Creating Linux Virtual Machine Images on page 4-13*.

4. Modify the environment of the virtual machine image.

   For details, see *Modifying the Virtual Machine Environment on page 4-44*.

5. Reduce the size of the VirtualBox Disk Image.

   For details, see *Reducing the Size of VirtualBox Disk Images on page 2-44*.

6. Export the virtual machine image to an OVA file.

   For details, see *Exporting Virtual Machine Images to OVA Files on page 4-45*.

Required Software

The following software must be installed on the virtual machine to achieve satisfactory detection results.

Note

Operating system, Office suite, and third-party software support may change or end without prior notice from Trend Micro due to specification, license model, and lifecycle changes.

TABLE 4-1. Required Software

OPERATING SYSTEM	KERNEL VERSION	NOTES
CentOS 7.8	3.10.0-1127.el7.x86_64	**Note** Image validation requires the installation ISO to enable automatic installation of missing Linux packages. For CentOS, the CentOS 7.8.2003 Installation ISO `CentOS-7-x86_64-Everything-2003.iso` is required. For RHEL 7.9, the RHEL 7.9 Installation ISO `rhel-server-7.9-x86_64-dvd.iso` is required. For RHEL 8.3, the RHEL 8.3 Installation ISO `rhel-8.3-x86_64-dvd.iso` is required. **Important** • Use a host name that reflects your organizations' naming scheme. • Trend Micro recommends using the English version of the operating system. • The Virtual Analyzer Image Preparation Tool only supports the specific kernel versions listed. Make sure you are using the exact kernel version specified in this table.
RHEL 7.9	3.10.0-1160.el7.x86_64	
RHEL 8.3	4.18.0-240.el8.x86_64	
Ubuntu 20.04.6	5.15.0-76-generic	

The following packages must be installed on the virtual machine to achieve satisfactory detection results.

Important

- Do not install newer or older versions of the packages.
- Do not install any VMware and VirtualBox tools to avoid triggering the anti-virtual machine functions of some malware.
- Do not install any anti-malware software on the virtual machine to ensure normal operation of Virtual Analyzer.

TABLE 4-2. Required Packages for CentOS and RHEL

REPOSITORY	CENTOS 7.8	RHEL 7.9	RHEL 8.3
yum	• bash-4.2.46-34.el7.x86_64 • binutils-2.27-43.base.el7 • dos2unix-6.0.3-7.el7 • file-5.11-36.el7 • gcc-4.8.5-39.el7 • gcc-c++-4.8.5-39.el7 • glibc-2.17-307.el7.1 • glibc-2.17-307.el7.1.i686 • glibc-common-2.17-307.el7.1 • glibc-devel-2.17-307.el7.1	• at-3.1.13-24.el7 • bash-4.2.46-34.el7.x86_64 • bind-utils-9.11.4-26.P2.el7_9.2 • binutils-2.27-43.base.el7 • dos2unix-6.0.3-7.el7 • epel-release • file-5.11-36.el7 • gcc-4.8.5-44.el7 • gcc-c++-4.8.5-44.el7 • glibc-2.17-326.el7_9	• elfutils-devel • gcc-8.5.0-15.el8.x86_64 • gcc-c++-8.5.0-15.el8.x86_64 • gettext • git • glibc-2.28-211.el8.x86_64 • glibc-devel-2.28-211.el8.x86_64 • glog • kernel-devel-4.18.0-240.el8.x86_64 • libcurl-7.61.1-14.el8.x86_64

Repository	CentOS 7.8	RHEL 7.9	RHEL 8.3
yum	• glibc-devel-2.17-307.el7.1.i686 • kernel-devel-3.10.0-1127.el7.x86_64 • libcurl-7.29.0-57.el7 • libcurl-devel-7.29.0-57.el7 • libgcc-4.8.5-39.el7 • libpcap-1.5.3-12.el7 • libpcap-devel-1.5.3-12.el7 • libstdc++-4.8.5-39.el7 • libstdc++-4.8.5-39.el7.i686 • libstdc++-devel-4.8.5-39.el7 • libstdc++-devel-4.8.5-39.el7.i686 • net-tools-2.0-0.25.20131004git.el7 • openssl-1.0.2k-19.el7 • python-devel • samba-4.10.4-10.el7	• glibc-common-2.17-326.el7_9 • glibc-devel-2.17-326.el7_9 • glog • glog-devel • kernel-devel-3.10.0-1160.el7.x86_64 • libcurl-7.29.0-59.el7 • libcurl-devel-7.29.0-59.el7 • libgcc-4.8.5-44.el7 • libpcap-1.5.3-12.el7 • libpcap-devel-1.5.3-12.el7 • libstdc++-4.8.5-44.el7 • libstdc++-devel-4.8.5-44.el7 • net-tools-2.0-0.25.20131004git.el • nmap-6.40-19.el7 • nmap-ncat-6.40-19.el7	• libgcc-8.5.0-15.el8.x86_64 • libpcap-1.9.1-5.el8.x86_64 • libpcap-devel-1.9.1-5.el8.x86_64 • libstdc++-8.5.0-15.el8.x86_64 • openssl-1.1.1g-11.el8.x86_64 • procps-ng-3.3.15-9.el8.x86_64 • python2 • python2-devel • rkhunter • samba-4.16.4-2.el8.x86_64 • samba-client-4.16.4-2.el8.x86_64 • samba-common-4.16.4-2.el8.noarch • systemtap-4.7-1.el8.x86_64 • systemtap-devel-4.7-1.el8.x86_64 • systemtap-runtime-4.7-1.el8.x86_64

Repository	CentOS 7.8	RHEL 7.9	RHEL 8.3
yum	• samba-client-4.10.4-10.el7 • samba-common-4.10.4-10.el7 • systemtap-4.0-11.el7 • systemtap-devel-4.0-11.el7 • systemtap-runtime-4.0-11.el7 • sysvinit-tools-2.88-14.dsf.el7 • tcsh-6.18.01-16.el7 • unzip-6.0-21.el7 • zip-3.0-11.el7 • zlib-1.2.7-18.el7	• openssl-1.0.2k-19.el7 • python-devel • rsync-3.1.2-10.el7 • samba-4.10.16-15.el7_9 • samba-client-4.10.16-15.el7_9 • samba-common-4.10.16-15.el7_9 • systemtap-4.0-13.el7 • systemtap-devel-4.0-13.el7 • systemtap-runtime-4.0-13.el7 • sysvinit-tools-2.88-14.dsf.el7 • tcsh-6.18.01 • unzip-6.0-21.el7 • zip-3.0-11.el7 • zlib-1.2.7-18.el7.x86_64	• tcsh • yum-utils • zlib-1.2.11-16.el8_2.x86_64

Repository	CentOS 7.8	RHEL 7.9	RHEL 8.3
debuginfo	• glibc-devel • kernel-3.10.0-1127.el7.x86_64 • libcurl • libgcc • libstdc++ • openssl • zlib	• bash • glibc • kernel-3.10.0-1160.el7.x86_64 • libcurl • libgcc • libstdc++ • openssl • zlib	• bash • glibc • kernel-debuginfo-4.18.0-240.el8.x86_64 • kernel-debuginfo-common-x86_64-4.18.0-240.el8.x86_64 • libcurl • libgcc • libstdc++ • openssl • zlib

TABLE 4-3. Required Packages for Ubuntu

REPOSITORY	UBUNTU 20.04.6
apt	• bash-builtins=5.0-6ubuntu1.2 • bind9-utils • curl=7.68.0-1ubuntu2 • gcc=4:9.3.0-1ubuntu2 • g++=4:9.3.0-1ubuntu2 • ipcalc • kernel-package=13.018+nmu2 • libc6=2.31-0ubuntu9.14 • libc6-dev=2.31-0ubuntu9.14 • libcurl4=7.68.0-1ubuntu2 • libcurl4-openssl-dev=7.68.0-1ubuntu2 • libdw1=0.176-1.1build1 • libdw-dev=0.176-1.1build1 • libelf1=0.176-1.1build1 • libelf-dev=0.176-1.1build1 • libgcc1=1:10.5.0-1ubuntu1~20.04 • libgoogle-glog-dev=0.4.0-1build1 • libpcap0.8=1.9.1-3 • libpcap0.8-dev=1.9.1-3 • libprocps-dev=2:3.3.16-1ubuntu2.3 • libstdc++6=10.5.0-1ubuntu1~20.04 • libstdc++-9-dev=9.4.0-1ubuntu1~20.04.1 • linux-headers-5.15.0-76-generic • net-tools • network-manager • openssl=1.1.1f-1ubuntu2.20

Repository	Ubuntu 20.04.6
apt	• python-dev-is-python2=2.7.17-4 • python2=2.7.17-2ubuntu4 • python2-dev=2.7.17-2ubuntu4 • rsync • samba • samba-common • tcsh • zlib1g=1:1.2.11.dfsg-2ubuntu1.5 • libucl1_1.03+repack-5_amd64.deb • node-v8.15.0-linux-x64.tar.xz • upx-ucl_3.95-2build1_amd64.deb
Python library	• configobj-5.0.8.tar.gz • dpkt-1.9.3.tar.gz • psutil-5.7.2.tar.gz • pypcap-1.2.2.tar.gz • setuptools-44.1.1.zip • yara-python-4.0.2.tar.gz

Repository	Ubuntu 20.04.6
debuginfo	• bash-builtins-dbgsym_5.0-6ubuntu1.2_amd64.ddeb • bash-dbgsym_5.0-6ubuntu1.2_amd64.ddeb • coreutils-dbgsym_8.30-3ubuntu2_amd64.ddeb • libc6-dbg_2.31-0ubuntu9.14_amd64.deb • libcurl3-gnutls-dbgsym_7.68.0-1ubuntu2.16_amd64.ddeb • libcurl4-dbgsym_7.68.0-1ubuntu2_amd64.ddeb • libgcc-s1-dbgsym_10.5.0-1ubuntu1~20.04_amd64.ddeb • libpcap0.8-dbg_1.9.1-3_amd64.deb • libstdc++6-9-dbg_9.4.0-1ubuntu1~20.04.2_amd64.deb • linux-image-5.15.0-76-generic-dbgsym • openssl-dbgsym_1.1.1f-1ubuntu2.20_amd64.ddeb • zlib1g-dbgsym_1.2.11.dfsg-2ubuntu1.5_amd64.ddeb

Important

- Do not install newer or older versions of the packages.
- Do not install any VMware and VirtualBox tools to avoid triggering the anti-virtual machine functions of some malware.
- Do not install any anti-malware software on the virtual machine to ensure normal operation of Virtual Analyzer.

Downloading and Installing VirtualBox

Procedure

1. Download the latest version of VirtualBox from https://www.virtualbox.org/wiki/Downloads.

   Note

   The VirtualBox Open Source Edition is licensed under the GPL V2. The full text of the license is available at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

   Trend Micro recommends using VirtualBox version 7.0 and later. The procedures outlined in this user guide have been tested with Virtual Box version 7.0.14.

2. Configure the language settings using one of the following methods:

   - Install VirtualBox with English as the default language.
   - After installation, go to **File** > **Preferences** > **Language** and then select **English**.

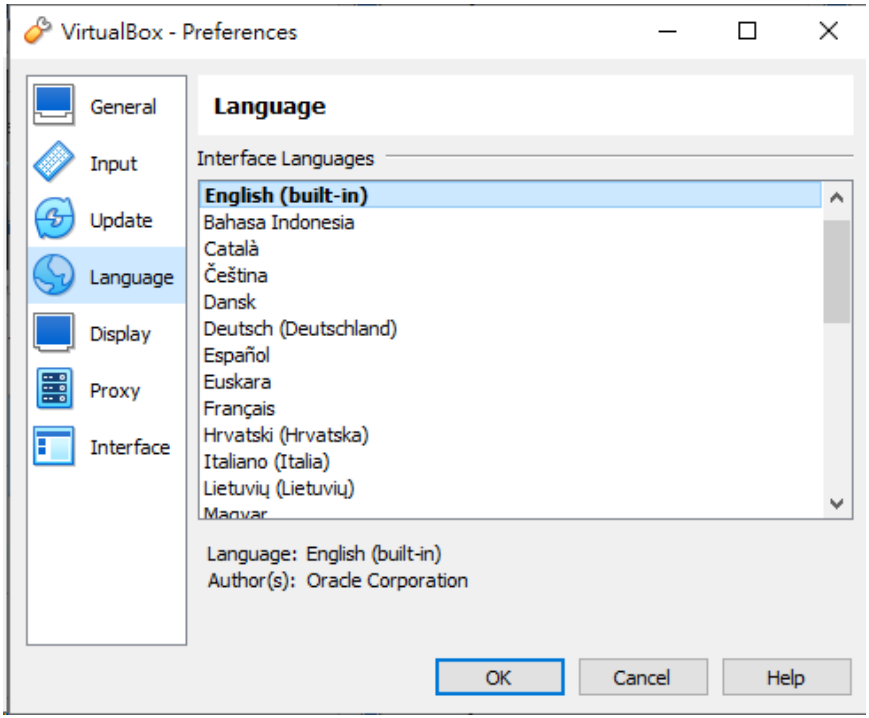


FIGURE 4-1. Language Settings

Creating Linux Virtual Machine Images

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.

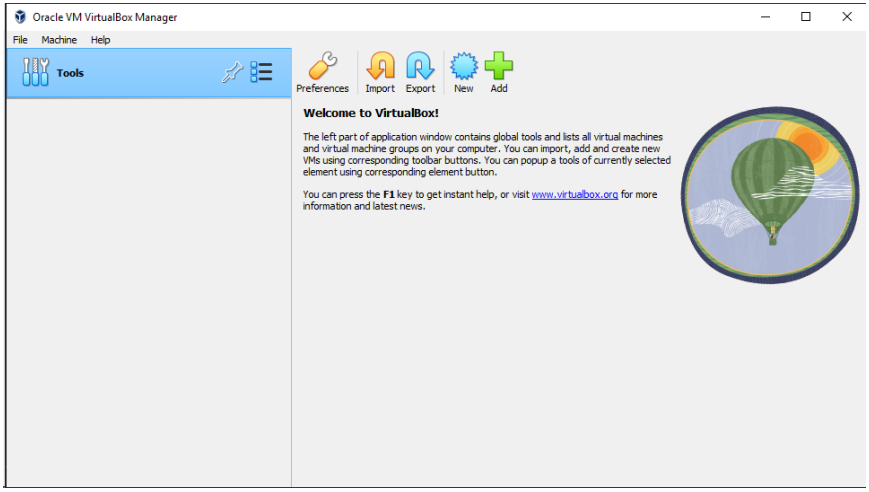


FIGURE 4-2. VirtualBox Manager

2. Click **New**.

   The **Create Virtual Machine** window opens.

3. Click **Expert Mode**.

The Create Virtual Machine wizard enters Expert Mode.

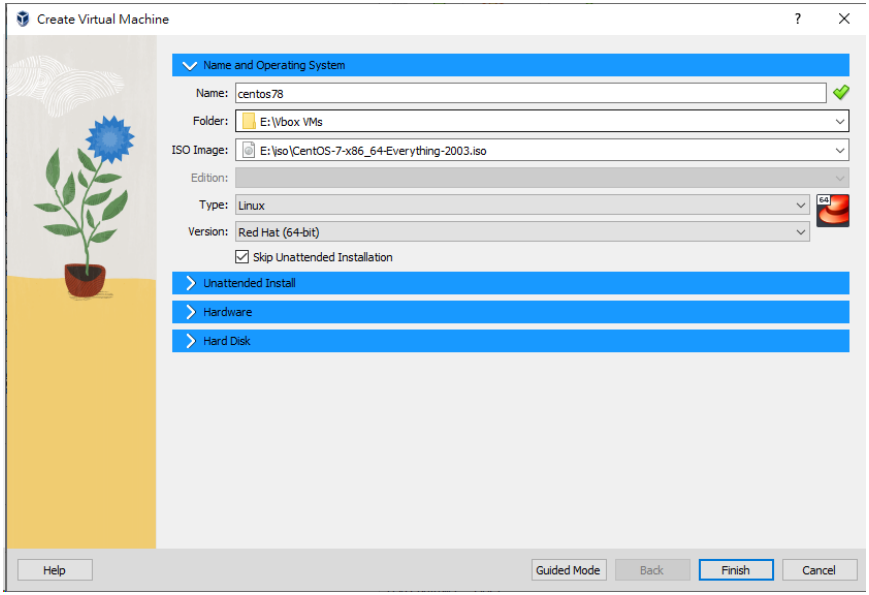


FIGURE 4-3. Create Virtual Machine - Expert Mode

4. Configure the **Name and Operating System** settings.
   - Type a permanent and unique **Name** for the virtual machine.
   - Specify the **Folder** to store the completed virtual machine.
   - Specify the **ISO Image** for the virtual machine.
   - For the **Type**, select **Linux**.
   - Select the **Version** based on your Linux OS:
     - For CentOS 7.8, RHEL 7.9, and RHEL 8.3, select **Red Hat (64-bit)**
     - For Ubuntu 20.04.6, select **Ubuntu (64-bit)**
   - Select **Skip Unattended Installation**.

5. Open the **Hardware** section.

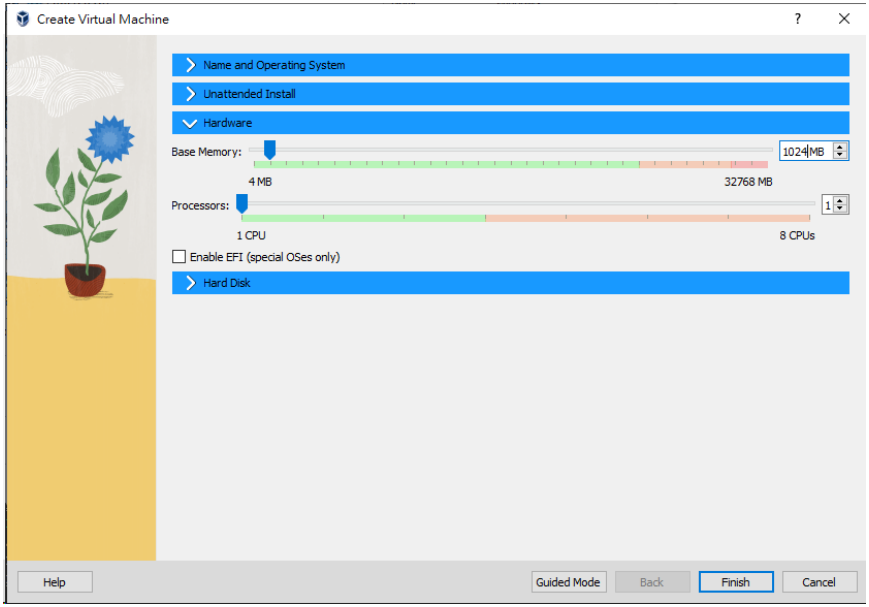


FIGURE 4-4. Hardware

6. Specify the recommended memory size for your operating system.
   - CentOS 7.8: 1024 MB
   - RHEL 7.9: 1024 MB
   - RHEL 8.3: 1024 MB
   - Ubuntu 20.04.6: 2048 MB
7. Open the **Hard Disk** section.

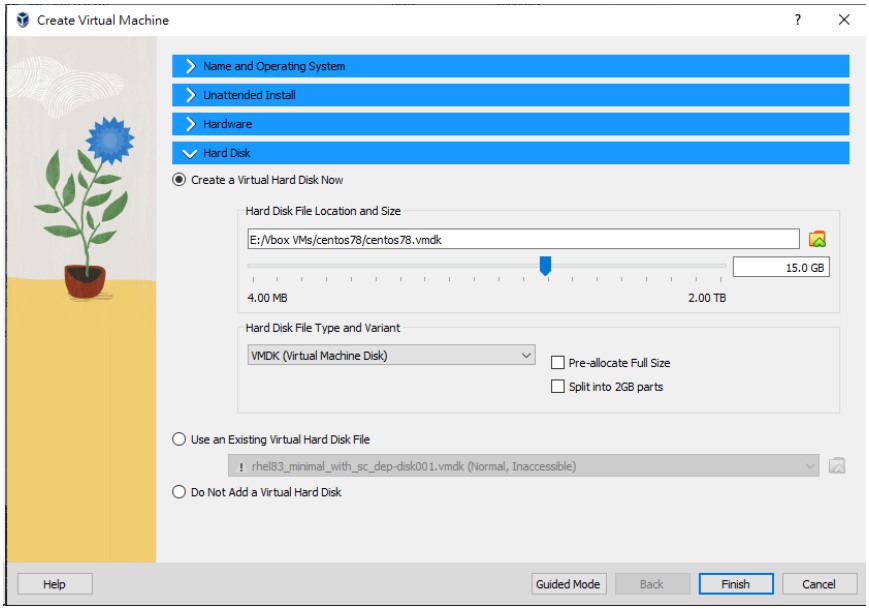


FIGURE 4-5. Hard Disk

8. Select **Create a Virtual Hard Disk Now**.
9. Specify the hard disk settings.
    - Specify the location of the virtual hard disk on the host machine.
    - Specify the size of the virtual hard disk according to your chosen operating system:
        - For CentOS 7.8, RHEL 7.9, and RHEL 8.3, specify at least 15 GB.
        - For Ubuntu 20.04.6, specify at least 25 GB.
    - For the **Hard Disk File Type and Variant**, select **VDI (VirtualBox Disk Image)** or **VMDK (Virtual Machine Disk)**

Note

Specify additional virtual hard drive space if you plan to install additional software.

For best results, Trend Micro recommends selecting **VDI (VirtualBox Disk Image)**.

Important

Do not select "Pre-allocate Full Size" or "Split into 2GB parts." The options may cause the tool to fail.

10. Click **Create**.

VirtualBox creates the virtual machine. The new virtual machine appears in the left pane of the VirtualBox Manager screen.

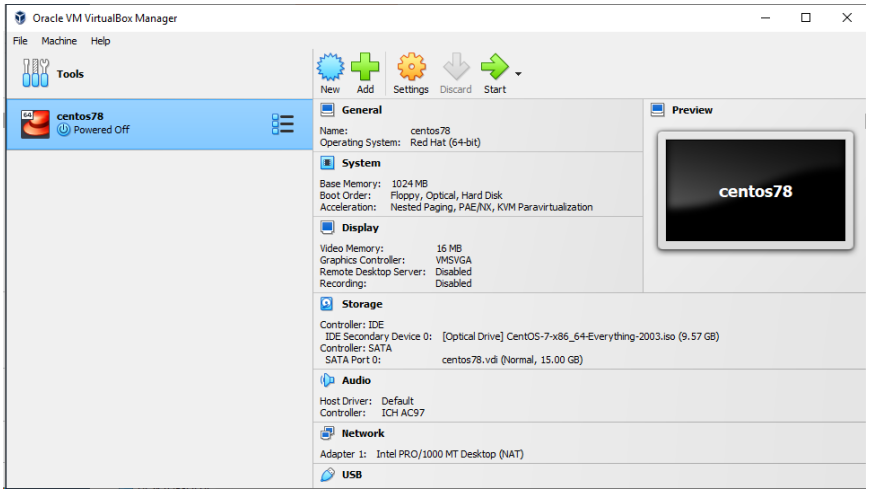


FIGURE 4-6. Newly-created Virtual Machine

Ensure that the virtual machine is not in any group.

11. Click **Settings**.

The **Settings** window opens.

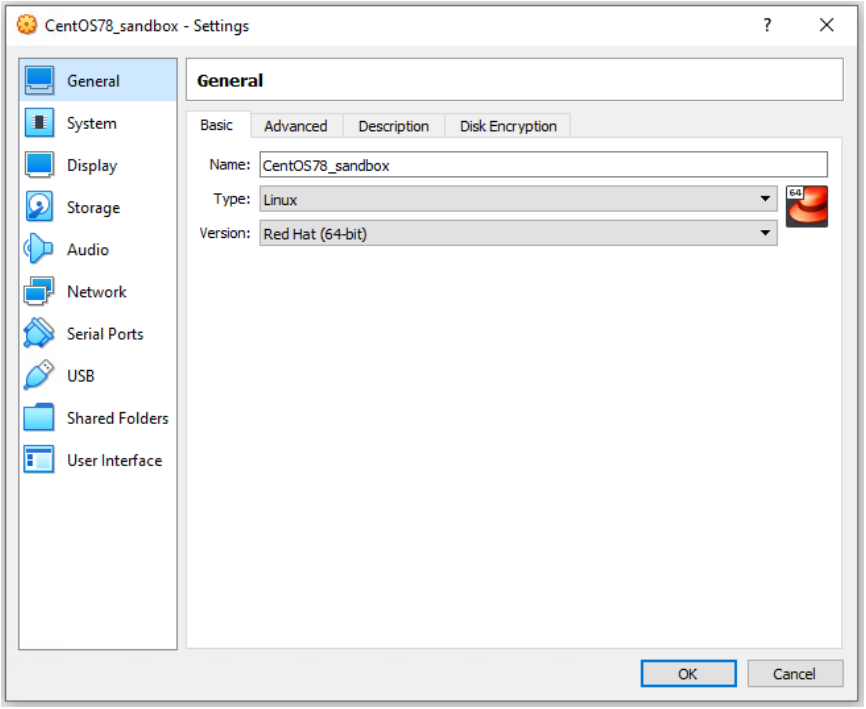


FIGURE 4-7. VirtualBox Settings

12. Go to **System**.

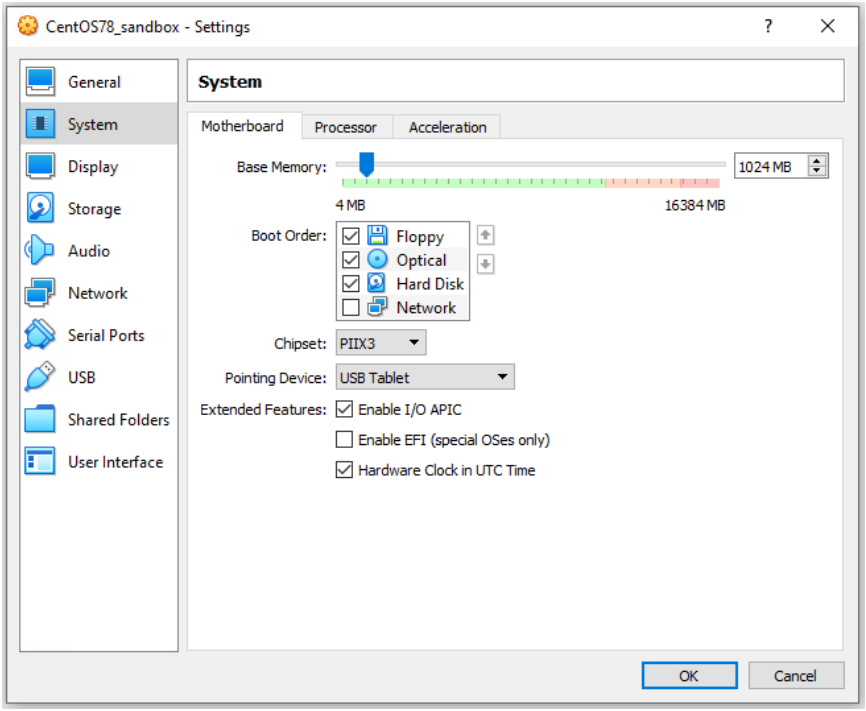


FIGURE 4-8. System Screen

13. Configure the settings on the **Motherboard** tab.
    - For **Chipset**, select **PIIX3**.
    - For **Pointing Device**, select **USB Tablet**
    - Select the following **Extended Features**:
        - **Enable I/O APIC**
        - **Enable EFI (special OSes only)** (Optional)

Note

Use **Enable EFI (special OSes only)** if you want to create EFI-compatible images. EFI-compatible images are only supported by the following Trend Micro products:

- Deep Discovery Inspector 5.6 and later
- Deep Discovery Email Inspector 3.6 and later
- Deep Discovery Analyzer 6.8 and later
- Deep Discovery Director 5.1 and later
- Deep Discovery Web Inspector 2.5 and later

14. On the **Processor** tab, select **Enable PAE/NX**.
15. On the **Acceleration** tab, select **Enable Nested Paging**.

    If you are using VirtualBox 5.2 and before, also select **Enable VT-x/AMD-V**.

Note

- The **Acceleration** tab is only available if the processor of the host system supports virtualization technology and the virtualization setting is enabled in the BIOS of the host system.
- VirtualBox 6.0 and later automatically enables VT-x/AMD-V if the processor of the host system supports virtualization technology and the virtualization setting is enabled in the BIOS of the host system.

16. Go to **Storage**.

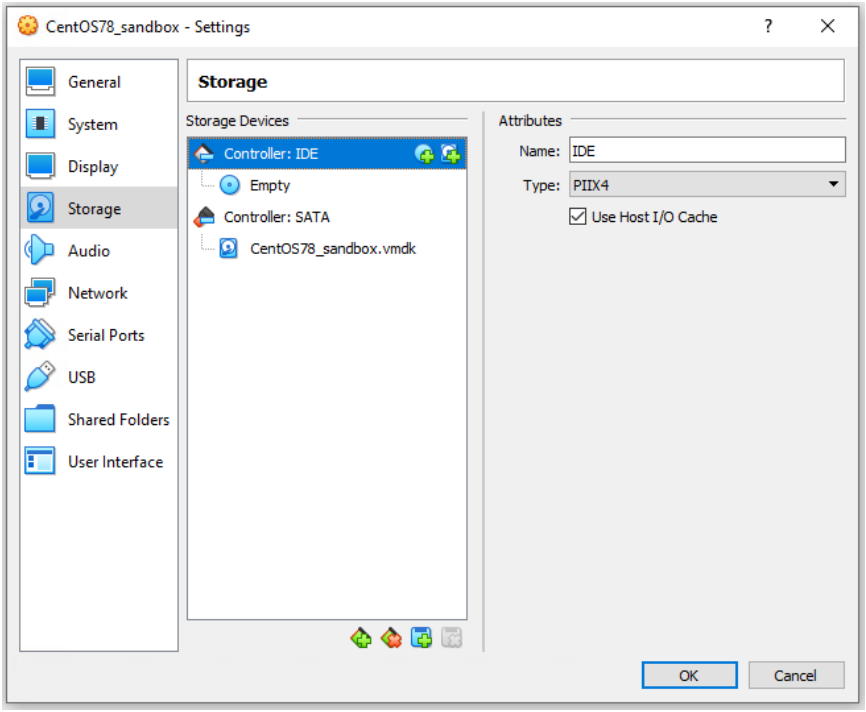


FIGURE 4-9. Storage Screen

17. If **Controller: SATA** appears under **Storage Devices**, select the controller and click to remove the SATA controller.

18. Add an IDE controller.

    a. Click and then select **PIIX4 (Default IDE)**.

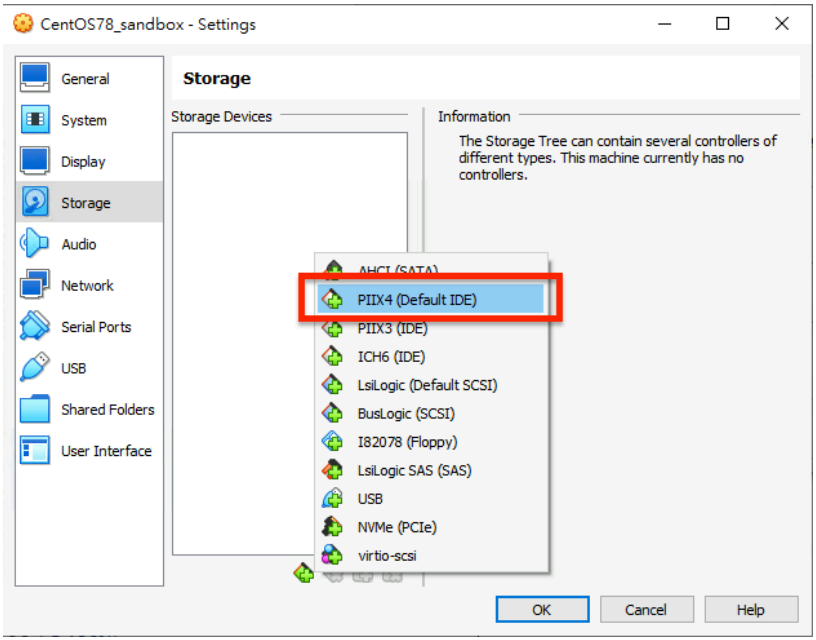


FIGURE 4-10. Add Storage Controller

b. Click the controller and change the **Name** attribute to **`IDE`**.

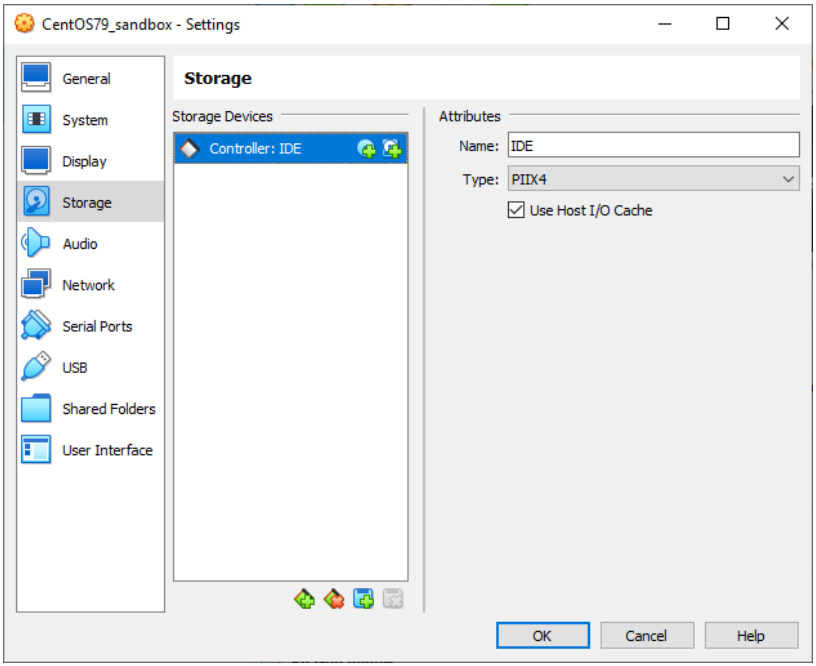


FIGURE 4-11. Controller IDE

c. Select **Use Host I/O Cache**.

d. Next to **Controller: PIIX4**, click to create a virtual hard disk.

The **Hard Disk Selector** window appears.

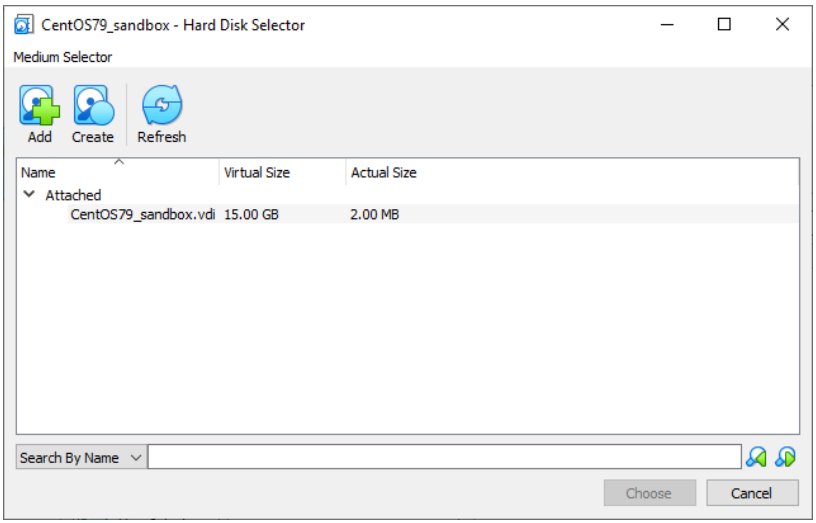


FIGURE 4-12. Hard Disk Selector

e. Select the virtual hard disk file that you previously created and then click **Choose**.

f. Click the hard drive you created and verify the **Hard Disk** attribute is set to **IDE Primary Device 0**.

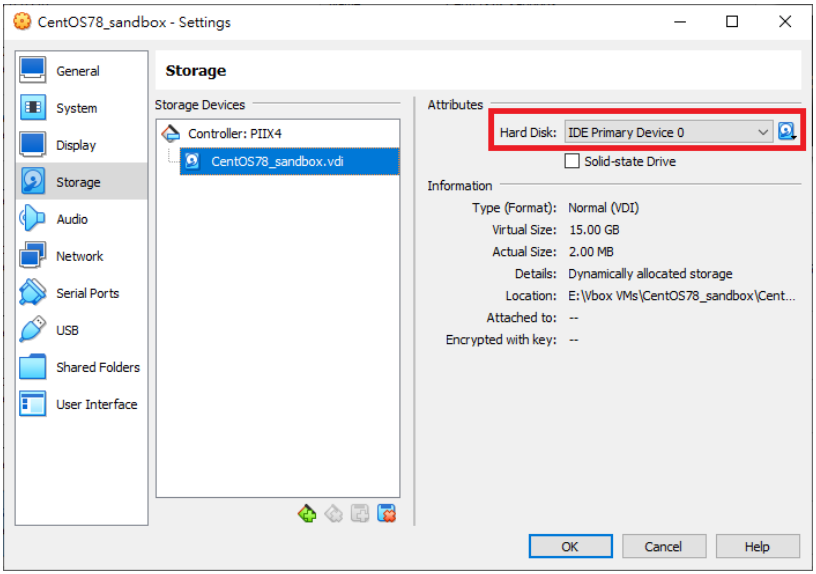


FIGURE 4-13. IDE Primary Device 0

g. Click **Controller: PIIX4** and then click to create an optical drive.

h. In the **Optical Disk Selector** window, click **Leave Empty**.

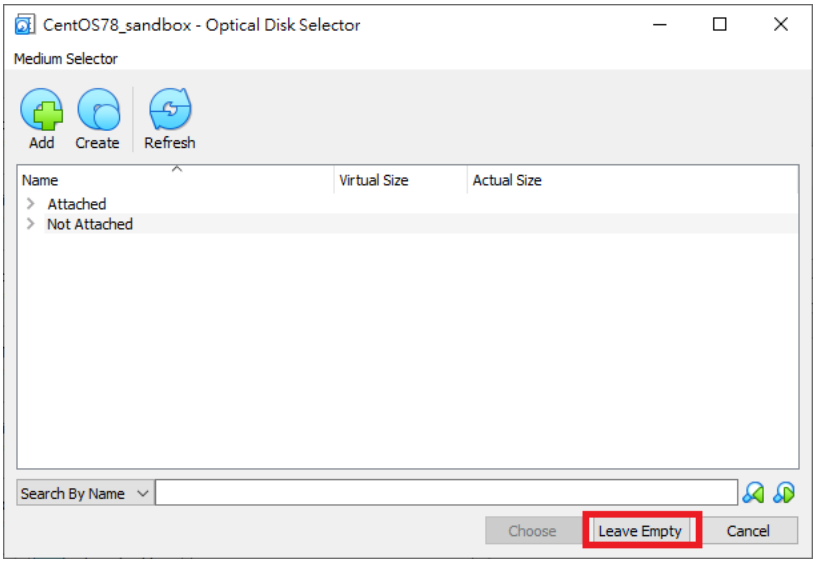


FIGURE 4-14. Optical Disk Selector

i. Click the optical drive you created and verify the **Optical Drive** attribute is set to **IDE Secondary Device 0**.

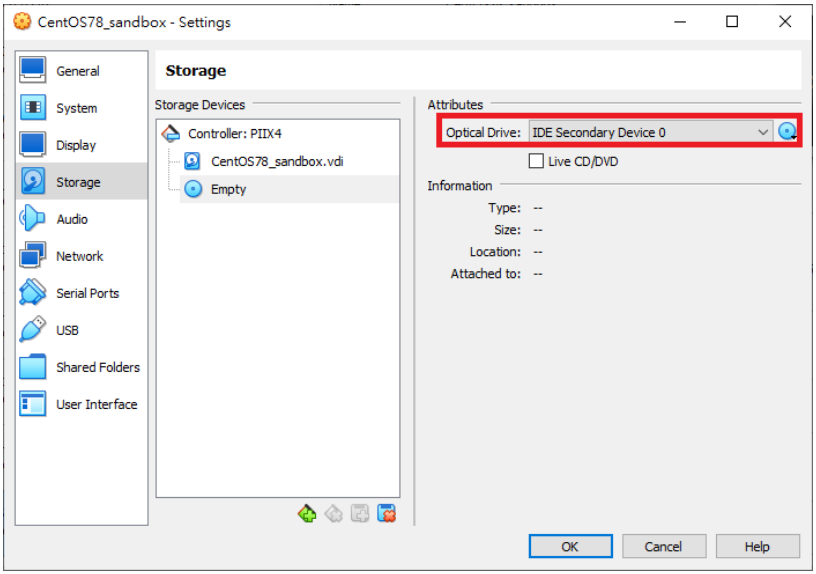


FIGURE 4-15. IDE Secondary Device 0

j. Click and select **Choose/Create a Virtual Optical Disk...**

k. Select the ISO file containing the operating system installer.

The ISO file appears as an available device.

You should only have one **Controller: PIIX4** listed under Storage Devices. If there are any other controllers listed, remove the extra controllers.

19. (Optional) Go to **Audio** and verify that **Enable Audio** is selected.

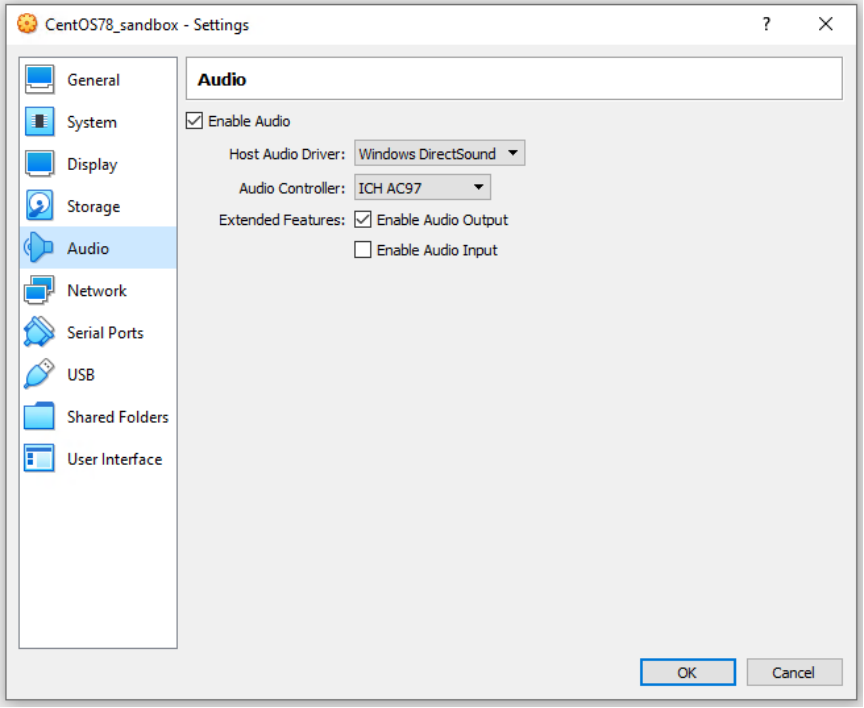


FIGURE 4-16. Audio Options Settings

20. Go to **Network** and click the **Adapter 1** tab.

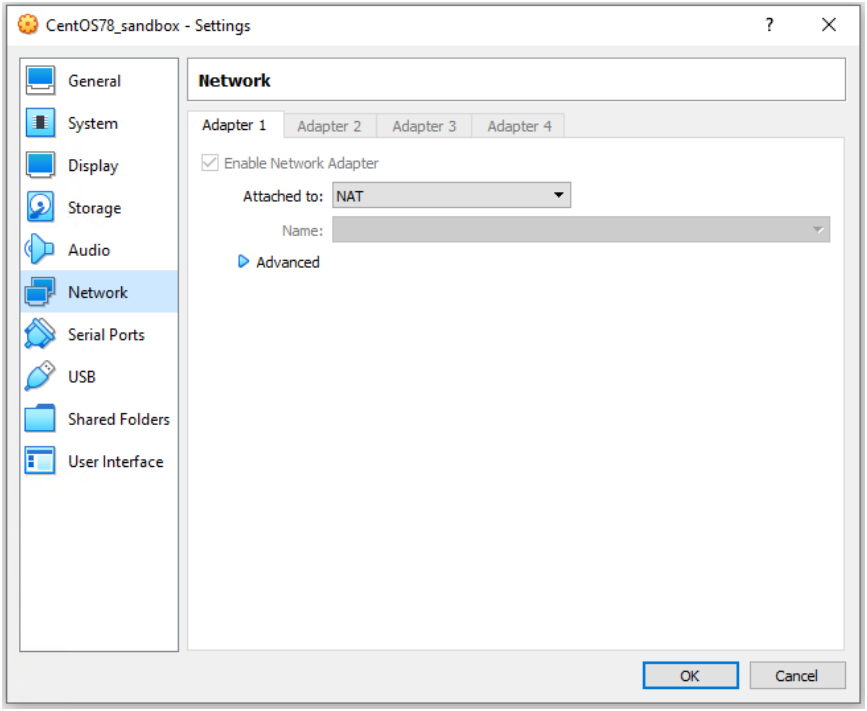


FIGURE 4-17. Network Settings

a. Verify **Enable Network Adapter** is selected.

b. For **Attached to**, select **NAT** or **Bridged Adapter**.

21. Go to **USB**.

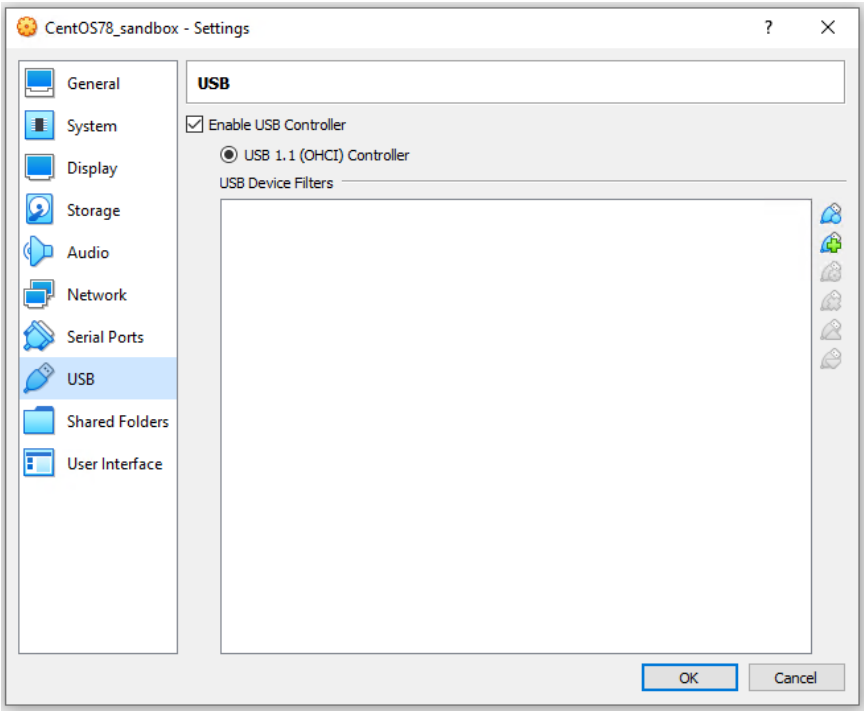


FIGURE 4-18. Enable USB Controller

22. Select **Enable USB Controller**.
23. Select **USB 1.1 (OHCI) Controller**.
24. Go to **Shared Folders** and verify that no folders are shared.

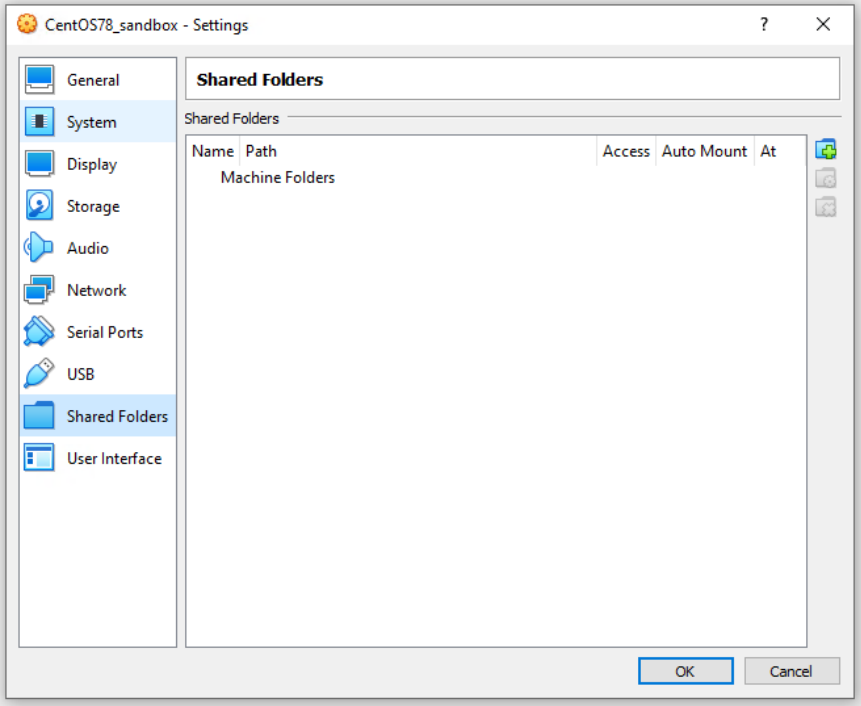


FIGURE 4-19. Shared Folders Settings

25. Click **OK**.

26. On the **VirtualBox Manager** screen, click Start to power on the image.

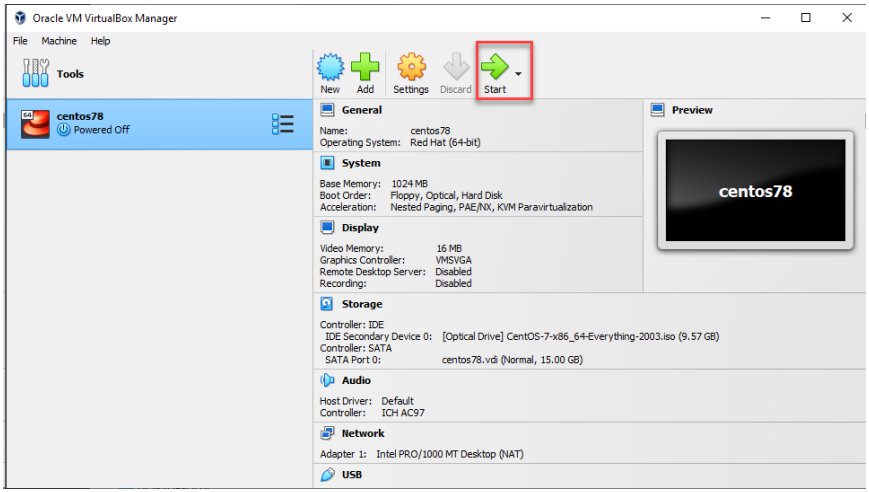


FIGURE 4-20. VirtualBox Manager

The installation process starts.

To install CentOS and RHEL, see *CentOS and RHEL Installation on page 4-33*.

To install Ubuntu, see *Ubuntu Installation on page 4-38*.

CentOS and RHEL Installation

Note

The screenshots in this section use CentOS as the example. However, the steps and settings also apply to RHEL.

Procedure

1. Follow the on-screen instructions to install the guest operating system.

FIGURE 4-21. Operating System Installation Process

2. Select **English** and click **Continue**.

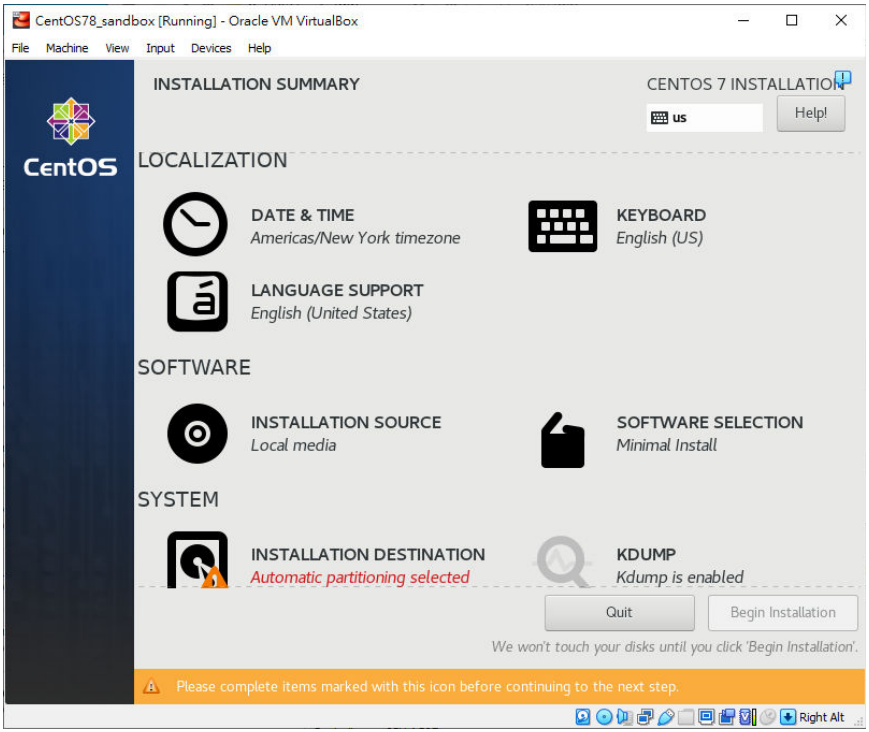


FIGURE 4-22. Installation Summary

3. Configure kdump settings.

   a. On the **Installation Summary** screen, click **KDUMP**

   b. Disable **Enable kdump**.

   c. Click **Done**.

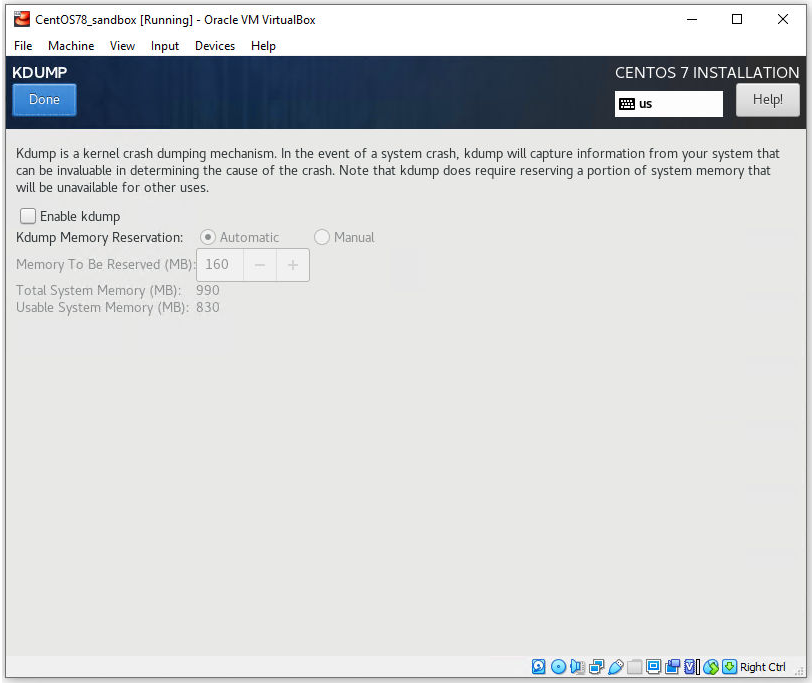


FIGURE 4-23. Installation Summary kdump

4. Configure network settings.

   a. On the **Installation Summary** screen, click **NETWORK & HOST NAME**.

   b. Enable/turn on the network interface.

   c. Configure the network settings.

   d. Verify that the network interface is able to get an IP address and connect to the network.

   e. Click **Done**.

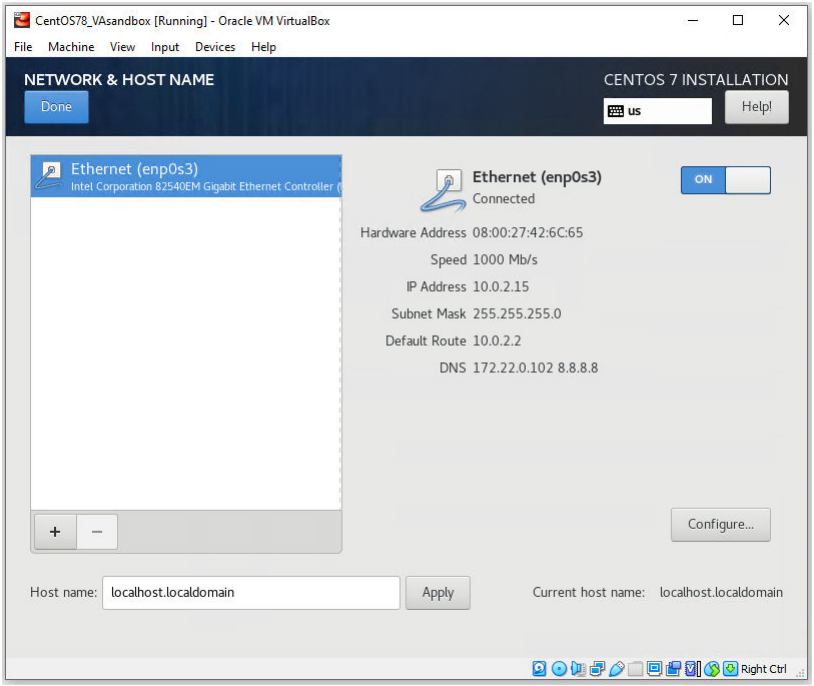


FIGURE 4-24. Installation Summary Network & Host Name

5. After the **Begin Installation** screen, on the **CONFIGURATION** screen, set the **ROOT PASSWORD** to `1111`.

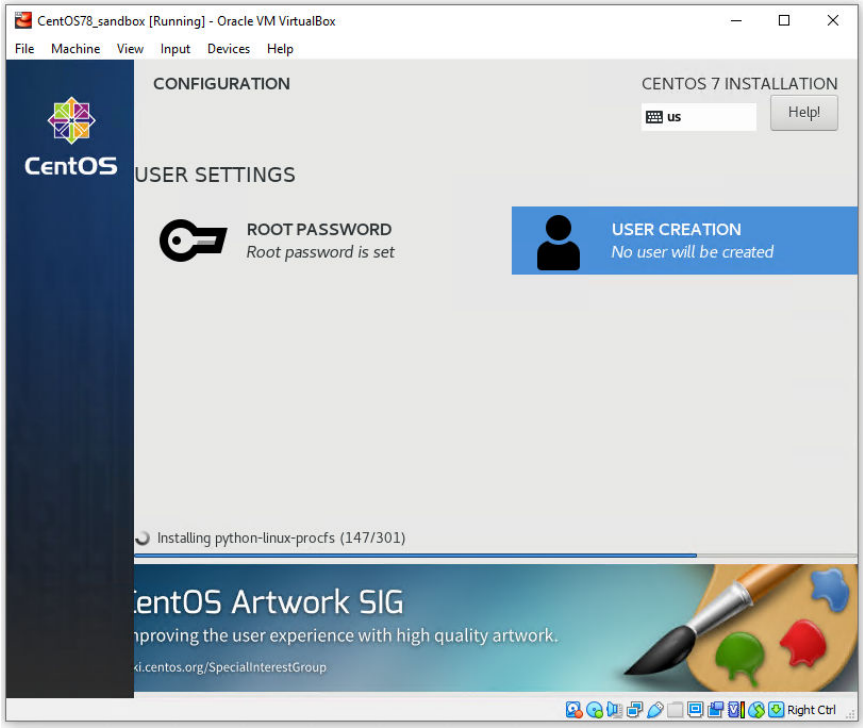


FIGURE 4-25. Password Configuration

Important

The Linux Operating System root password must be set to `1111`.

Ubuntu Installation

Procedure

1. Follow the on-screen instructions to install the guest operating system.

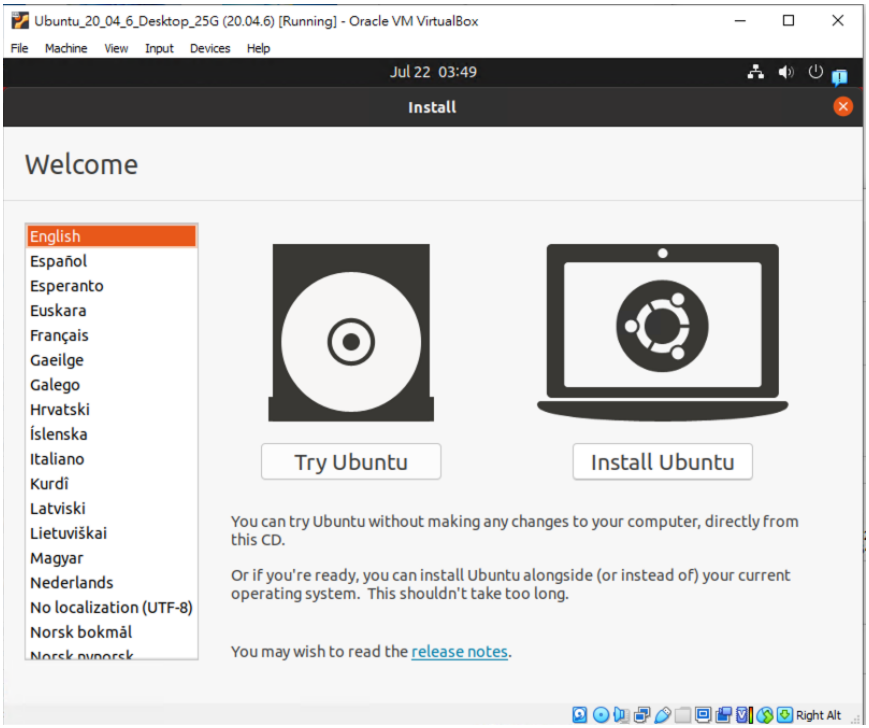


FIGURE 4-26. Ubuntu Installation Process

2. Select **English** and click **Install Ubuntu**.

   The **Keyboard layout** screen appears.

3. Select **English (US)** in both columns and click **Continue**.

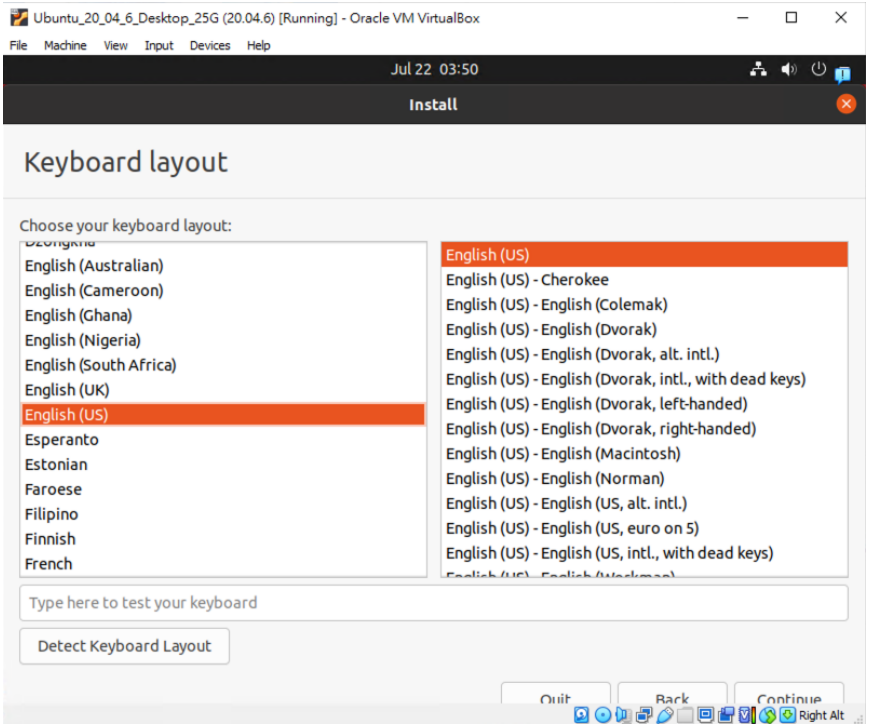


FIGURE 4-27. Keyboard Layout

4. Configure the **Updates and other software** settings to prevent updating required packages.

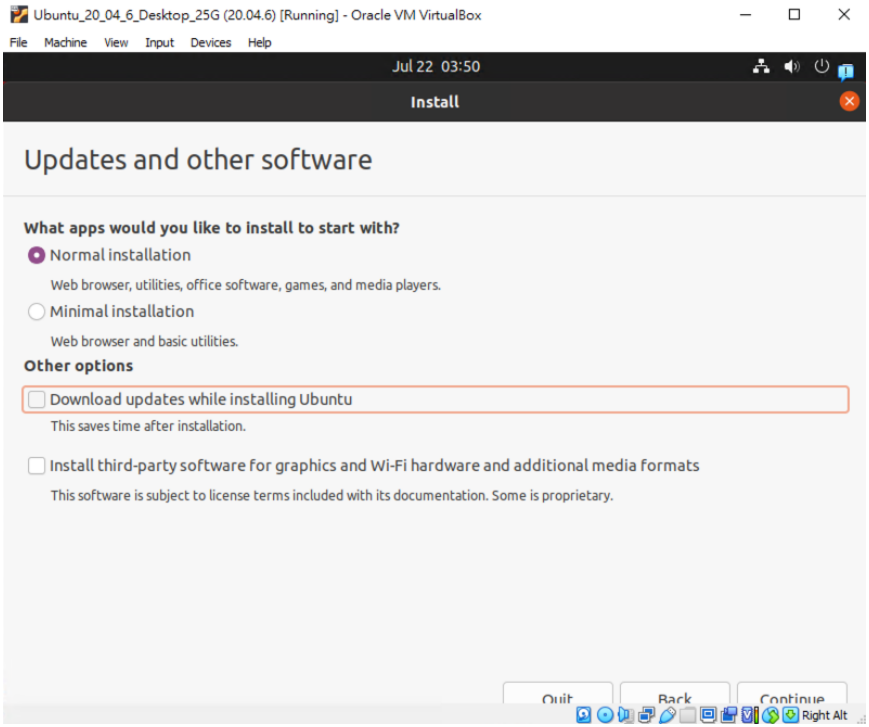


FIGURE 4-28. Updates and Other Software

a. Select **Normal installation**.

b. Under **Other options**, clear all selections.

Important

Download updates while installing Ubuntu must be disabled to prevent updating packages to versions not supported by the Virtual Analyzer.

Trend Micro recommends turning off network connections to prevent auto-upgrade during installation.

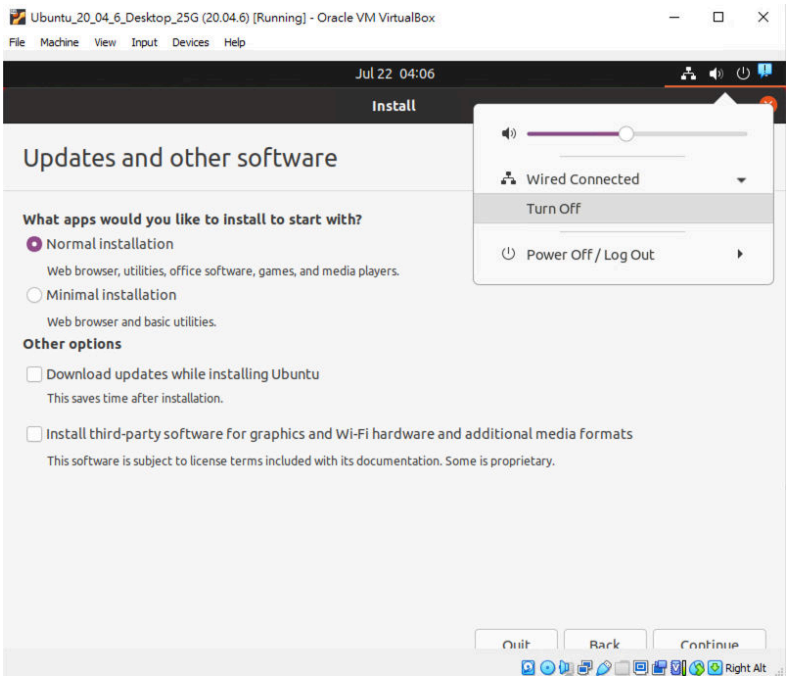


FIGURE 4-29. Turn off Network

5. Click **Continue**.
6. On the **Installation type** screen, select **Erase disk and install Ubuntu**.

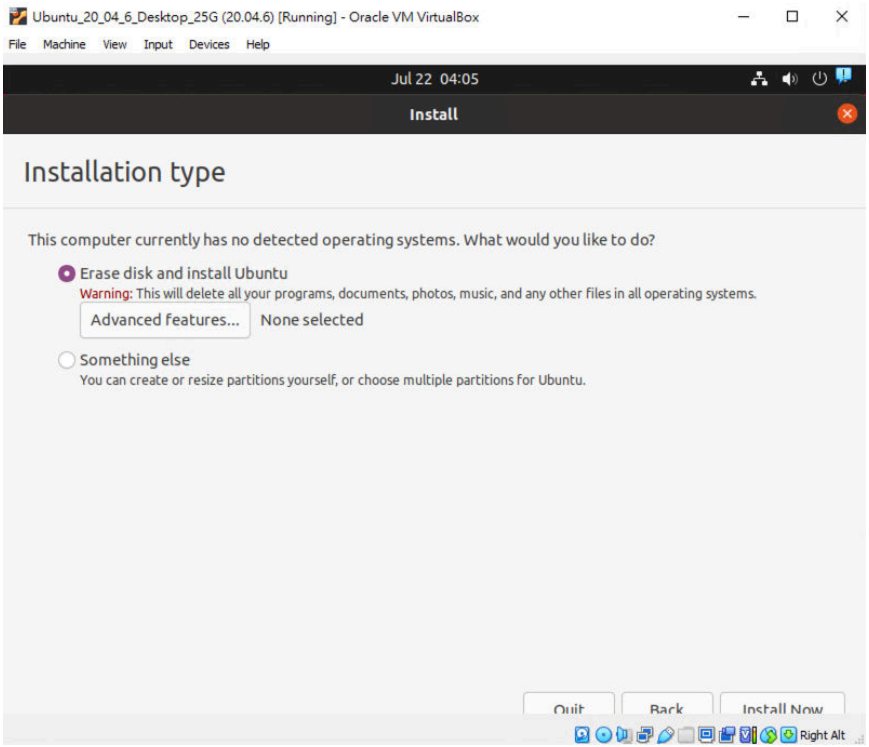


FIGURE 4-30. Installation Type

7. Click **Install Now**.

Note

The root password for Ubuntu is set in a later step.

Modifying the Virtual Machine Environment

Modify the virtual machine environment to run Virtual Analyzer Sensors, a collection of utilities that execute and detect malware, and record all behavior in Virtual Analyzer.

• *Modifying the Virtual Machine Environment on page 4-44*

Modifying the Virtual Machine Environment

Procedure

1. Open a Terminal window and perform the following tasks:

Task	Steps
Verify that the network interface is able to get an IP address and connect to the network	• For CentOS and RHEL, type **`nmcli`** to check the network interface status. • For Ubunut, type **`ip addr`** to check if the network interface is able to get an IP address. **Note** If the network interface is disconnected, type **`ifup "<network interface name>"`** to connect the network interface.
Verify that the network interface is enabled on boot	For CentOS, edit the network interface configuration file `/etc/sysconf ig/network-scripts/ifcfg-<network interface name>`, and modify the following line: `ONBOOT=yes`
Verfiy that the sshd is installed and running with configured settings	Type the following commands: a. For Ubuntu 20.04.6, type **`sudo apt install -y openssh-server`** to install OpenSSH. b. Enable the SSH: **`systemctl enable sshd`** c. Start the SSH: **`systemctl start sshd`** d. Verify the SSH status: **`systemctl status sshd`** e. Open the SSH config file: **`sudo vi /etc/ssh/shhd_config`** f. Set `PermitRootLogin` to `yes`.

Task	Steps
	g. Verify `Port` is configured to `22`. h. Save changes and restart SSH with the command: **`systemctl restart sshd`** Verify that the ssh status is `active (running)`
Disable SELinux on CentOS and RHEL	Edit the SELinux configuration file `/etc/selinux/config`, and modify the following line: `SELINUX=disabled`
Verify that all required packages are installed	Use Virtual Analyzer Image Preparation Tool to automatically install missing packages or manually install them. For details, see *Required Software on page 4-3*.
For RHEL 7.9 and RHEL 8.3, register system	Registration is required to enable automatic installation of missing packages. Refer to documentation provided by Red Hat to complete registration.
For Unbuntu 20.04.6, set the root account password	Use the following commands to set the root password: a. Type `sudo passwd root`. b. Type `1111` to set the root password to `1111`. c. Type the password again if prompted.

2. Restart the virtual machine.

Exporting Virtual Machine Images to OVA Files

A virtual machine image comprises many uncompressed files. The files must be combined into a single OVA file to avoid issues when importing.

Important

Verify that the size of the created OVA file is supported by your product.

For details, go to https://docs.trendmicro.com/en-us/home.aspx#Enterprise.

Procedure

1. On the VirtualBox Manager screen, power off the virtual machine.

   Note
   Verify that the CD/DVD drive is empty before powering off and exporting.

2. Go to **File** > **Export Appliance**.

   The **Export Virtual Appliance** window appears.

3. Select the virtual machine image to export and click **Next**.

   The **Appliance settings** screen appears.

4. Configure the following:

   - **File**: Accept the default name and path or click  to select a different file.
   - **Format**: Select **OVF 1.0**.

     Important
     Format options include OVF 0.9, 1.0 and 2.0. Virtual Analyzer does not support OVF 2.0.

   - **MAC Address Policy**: Select **Include all network adapter MAC addresses**.

5. Click **Next**.

   The **Virtual system settings** screen appears.

6. Verify that the **License** field is empty and then click **Export**.

VirtualBox creates the OVA file.

Chapter 5

Virtual Analyzer Image Preparation Tool

Learn how to use the Virtual Analyzer Image Preparation Tool in the following topics:

- *Overview on page 5-2*
- *Image Validation and Configuration on page 5-4*
- *System Requirements on page 5-3*
- *Using the Tool on page 5-6*
- *Troubleshooting Common Issues on page 5-25*

Overview

The Virtual Analyzer Image Preparation Tool facilitates the creation of custom sandbox images.

TABLE 5-1. Features

FEATURE	DESCRIPTION
Image creation	Create custom sandbox images for the following products: • Deep Discovery Inspector 3.8 and later • Deep Discovery Email Inspector 2.1 and later • Deep Discovery Analyzer 5.1 and later • TippingPoint Advanced Threat Protection for Networks 3.8 SP2 and later • TippingPoint Advanced Threat Protection for Email 2.5 and later • TippingPoint Advanced Threat Protection Analyzer 5.5 and later • Deep Discovery Director 1.1 and later • Deep Discovery Web Inspector 2.0 and later
Image validation and configuration	The tool validates and configures OVA files created using VirtualBox.

System Requirements

TABLE 5-2. Virtual Analyzer Image Preparation Tool System requirements

REQUIREMENT	SPECIFICATION
Host operating system	Build 3.8.1009 and later: • Windows 7 (32-bit and 64-bit) • Windows 8 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows 10 (32-bit and 64-bit) Build 3.8.1240 and later: • Windows Server 2003/2003 R2 • Windows Server 2008/2008 R2 • Windows Server 2012/2012 R2 • Windows Server 2016 • Windows Server 2019 Build 7.0.1007 and later: • Windows 11 **Important** Microsoft .NET Framework 4.0 or later must be installed on the host operating system.

Requirement	Specification
Virtualization application	• Oracle™ VM VirtualBox 4.3 or later (except 5.0.6) • Oracle™ VM VirtualBox 7.0 or later for Windows 11 images **Important** The tool does not support VirtualBox 5.0.6 because a defect prevents the first serial port from functioning properly. Trend Micro recommends using VirtualBox 5.0.7 or later. The tool only supports VirtualBox 7.0 or later for Windows 11 virtual machines.
Hardware virtualization	The hardware virtualization in the motherboard BIOS of the host operating system must be enabled to support Windows 8/8.1/10 or any 64-bit guest operating systems. **Note** The tool can detect hardware virtualization only on Windows 8/8.1/10 hosts.

Image Validation and Configuration

The tool automatically validates and configures the following VirtualBox image settings.

Table 5-3. Validating and configuring Windows image settings

Setting	Correct Configuration
Admin password	1111
Keyboard layout	Enhanced keyboard layout: 101
Found New Hardware Wizard	Disabled
Disk defragmentation	Disabled
.NET Optimization	Disabled

Setting	Correct Configuration
CPU count	1
Memory size	• Windows XP or Windows Server 2003: 512 MB • Windows 11: 2048 MB • Other operating systems: 1024 MB
PAE/NX	Enabled
Hardware virtualization	VT-x/AMD-V and nested paging enabled
Audio driver	Enabled
Windows SMB service (TCP port 445)	Enabled
File and Printer Sharing for Microsoft Networks	Enabled
AutoPlay	Enabled in Windows 7/8/8.1/10/11
Default web browser	Internet Explorer or Microsoft Edge (Chromium-based version)
Microsoft Office macros	Enabled
Network adapter settings	Obtain an IP address automatically

Important

The tool checks but does not modify the Windows and Office versions. Verify that the image meets the requirements before running the tool.

Table 5-4. Validating and configuring Linux image settings

Setting	Correct Configuration
CPU count	1
Memory size	• CentOS and RHEL: 1024 MB • Ubuntu: 2048 MB

Setting	Correct Configuration
PAE/NX	Enabled
Hardware virtualization	VT-x/AMD-V and nested paging enabled
Audio driver	Enabled
Root password	1111
SELinux (CentOS and RHEL)	Disabled
kdump (CentOS and RHEL)	Disabled
sshd	Enabled
Kernel update	Disabled

Important

Image validation requires the installation ISO to enable automatic installation of missing Linux packages.

For CentOS, the CentOS 7.8.2003 Installation ISO `CentOS-7-x86_64-Everything-2003.iso` is required.

For RHEL 7.9, the RHEL 7.9 Installation ISO `rhel-server-7.9-x86_64-dvd.iso` is required.

For RHEL 8.3, the RHEL 8.3 Installation ISO `rhel-8.3-x86_64-dvd.iso` is required.

Using the Tool

Procedure

1. Download `SandboxWizard.zip` from the Trend Micro Download Center, or obtain a copy from your support provider.
2. Extract the package content to a local folder.

3. Go to the folder you extracted the package to and run `SandboxWizard.exe`.

   The introduction screen appears.

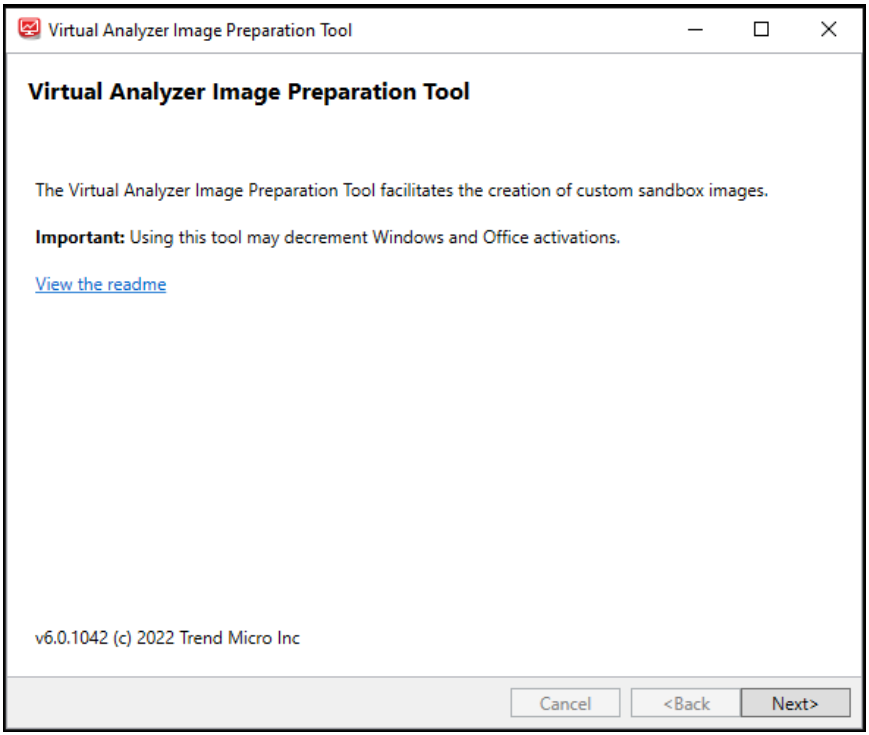


FIGURE 5-1. Introduction screen

4. Click **Next**.

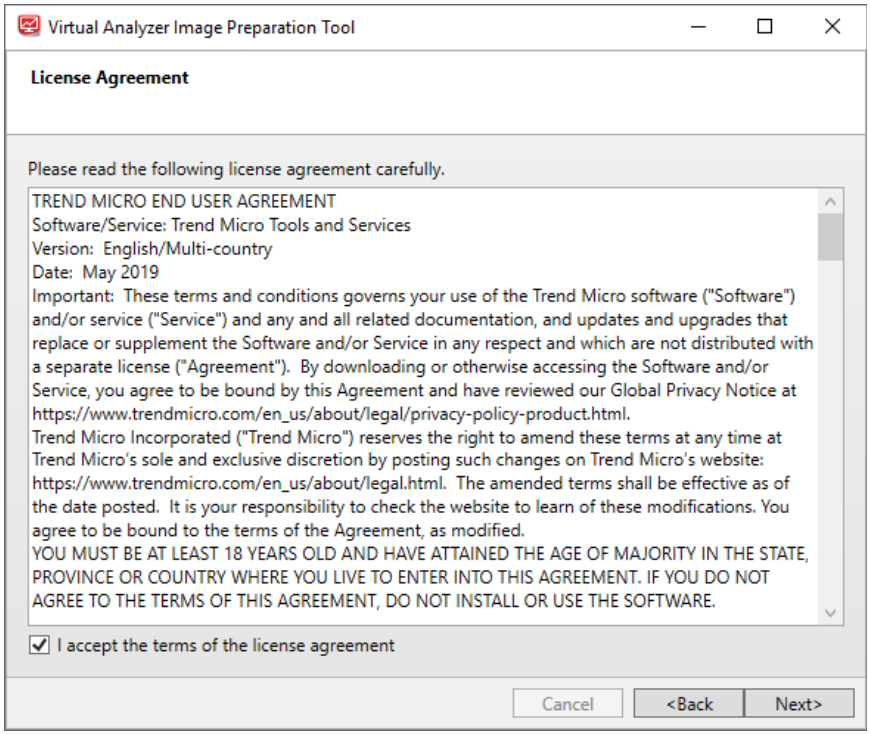


FIGURE 5-2. License Agreement screen

5. Read the license agreement. If you agree with the terms, select **I accept the terms of the license agreement** and then click **Next**.

   The tool checks if the computer meets the system requirements. After the check is complete, the **System Requirements** screen appears.

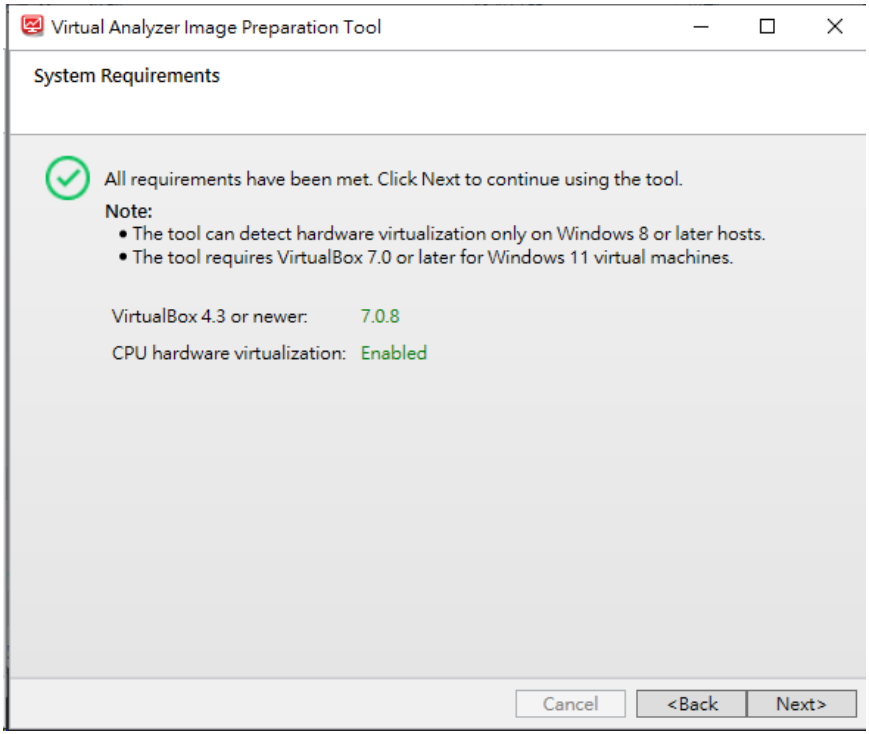


FIGURE 5-3. System Requirements screen

6. Click **Next**.

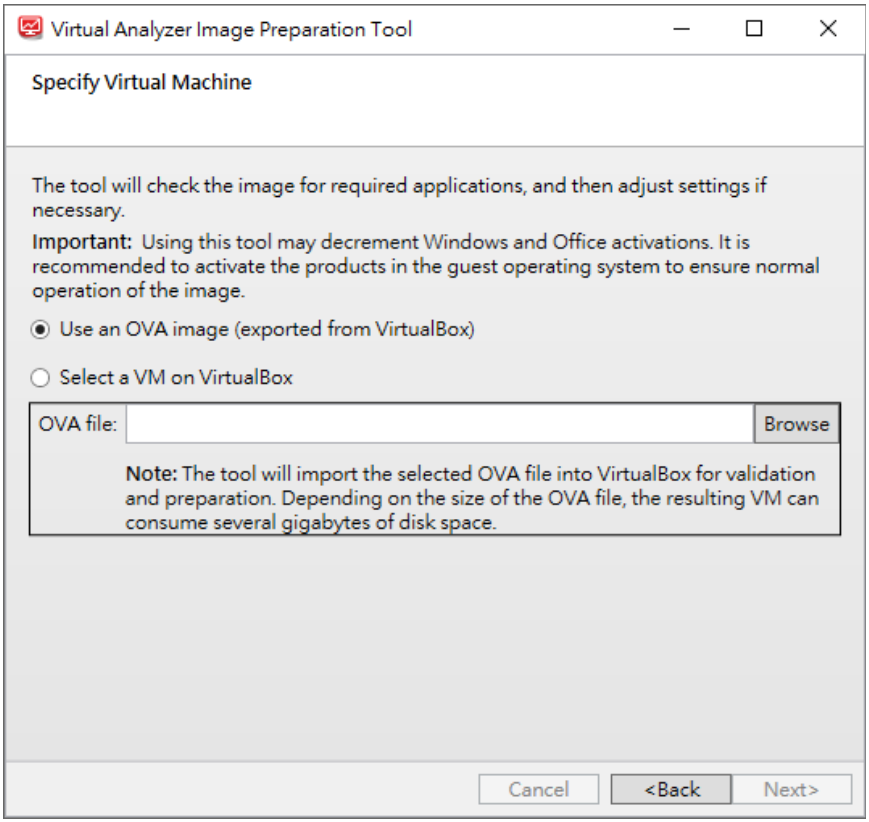


FIGURE 5-4. Specify Virtual Machine screen

7. If you converted a Windows VMware image to an OVA file, perform the following steps:

   a. Select **Use an OVA image (exported from VirtualBox)**.

   b. Click **Browse** and select the OVA file you exported.

   For more details about this option, see *Windows OVA File Creation Using Converted Virtual Hard Disk Drives on page 3-1*.

Important

Open Virtualization Format (OVF) is a cross-platform standard for packaging and distributing software to be run in virtual machines. OVF enables the creation of ready-to-use software packages (operating systems with applications) that require no configuration or installation.

An OVF package consists of several files that can be packed into a single archive file with the extension `.ova`. Virtual Analyzer supports only image files in the OVA format.

8. If you created a virtual machine on VirtualBox, perform the following steps:

   a. Select **Select a VM on VirtualBox**.

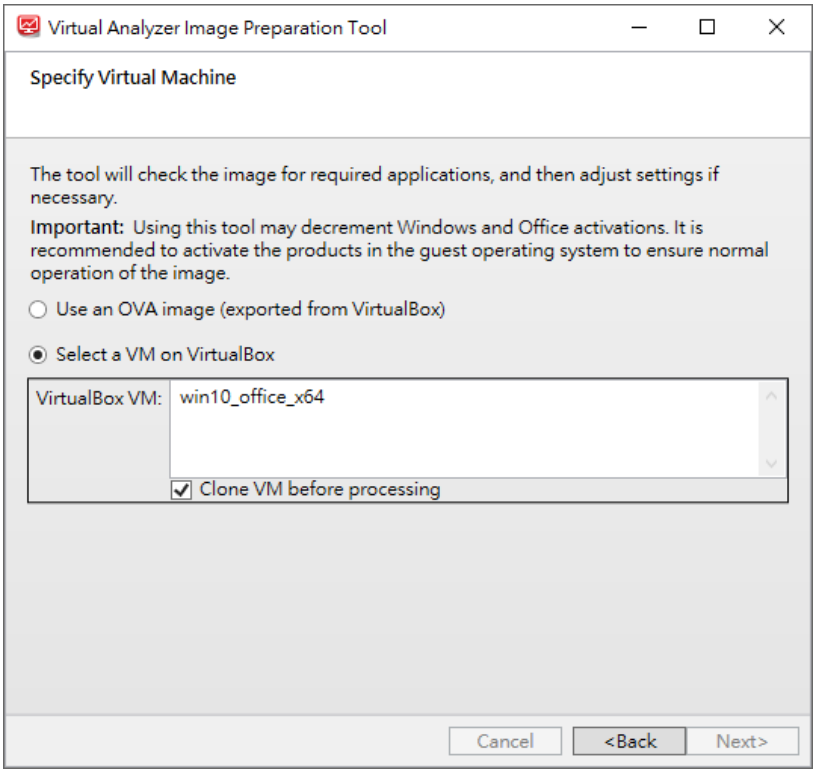


FIGURE 5-5. Specify Virtual Machine screen - Select a VM on VirtualBox

b. Select the virtual machine you want to use from the **VirtualBox VM** list.

c. Select **Clone VM before processing** to create a new copy of the virtual machine with its own set of individual snapshots..

Cloning allows quick creation of duplicate environments for testing. You can run as many clones as the memory and processors on the system allow.

9. Click **Next**.

The **Sandbox Preparation** screen appears and the tool begins preparing the image.

If the Linux virtual machine network adapter is attached to **NAT**, the tool automatically modifies settings using SSH.

If the Linux virtual machine network adapter is attached to **Bridged Adapter**, the **SSH Access** dialog appears. Specify the IP address and port the tool can use to access the virtual machine environment and then click **Connect**.

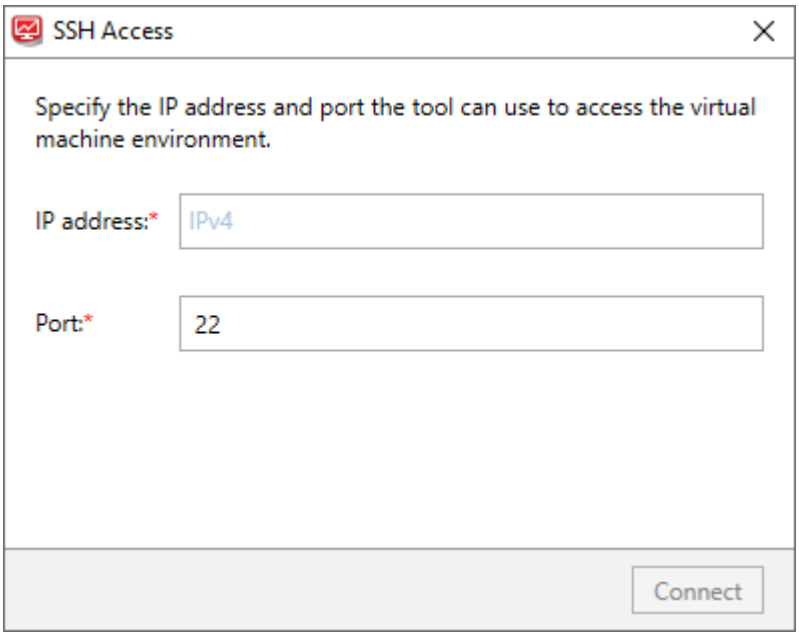


FIGURE 5-6. SSH Access screen for Linux images

The tool modifies incorrectly configured settings. For a list of settings that the tool validates, see *Image Validation and Configuration on page 5-4*. For solutions to issues that occur during this phase, see *Troubleshooting Common Issues on page 5-25*.

10. If the **Sandbox Preparation Unsuccessful** screen appears, click **View detailed log** to see recommended actions.

- For missing software on Windows images, see *Sandbox Preparation Unsuccessful - Missing Windows Software on page 5-22*.
- For missing packages on Linux images, see *Sandbox Preparation Unsuccessful - Missing Linux Packages on page 5-24*.
- For all other issues, see *Troubleshooting Common Issues on page 5-25*.

11. If the **Products Not Activated** screen appears, resolve the issue or click **Next**.

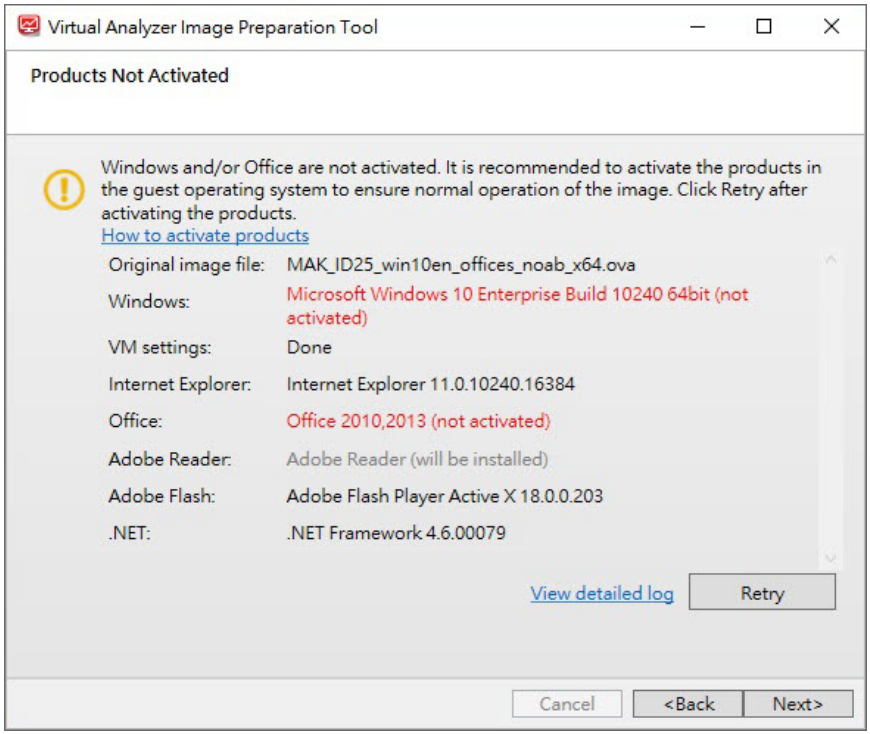


FIGURE 5-7. Products Not Activated screen for Windows images

To resolve the issue, see *Products Not Activated - Windows on page 5-20*.

Note

Trend Micro recommends activating Windows and Microsoft Office to ensure normal operation of the image.

12. Once the **Sandbox Ready** screen appears, click **Next**.

    The **Sandbox Ready** screen appears when the tool has successfully validated and configured all settings.

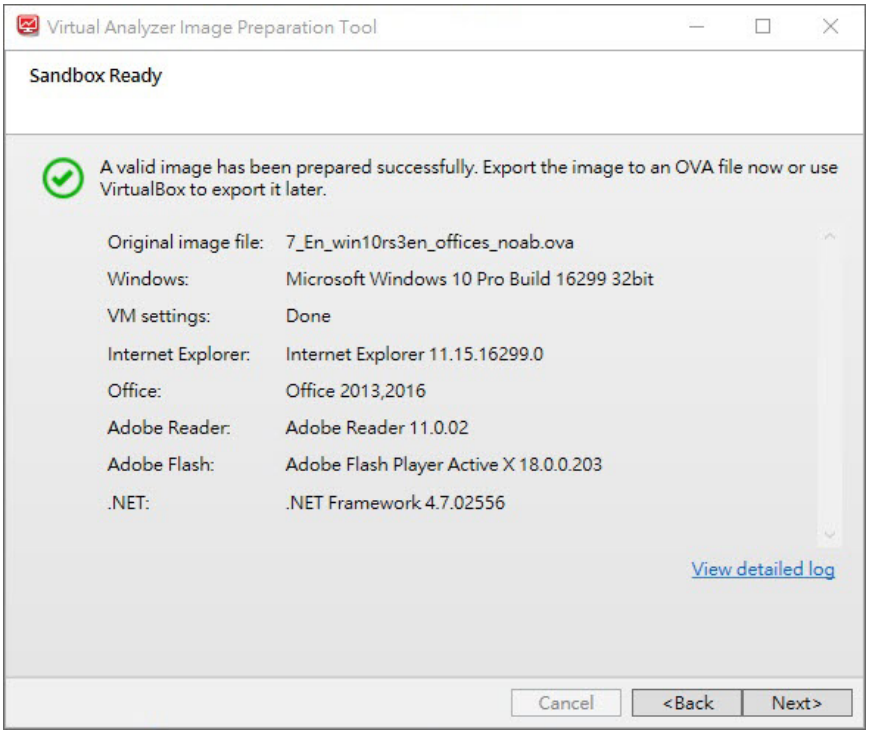


FIGURE 5-8. Sandbox Ready screen for Windows images

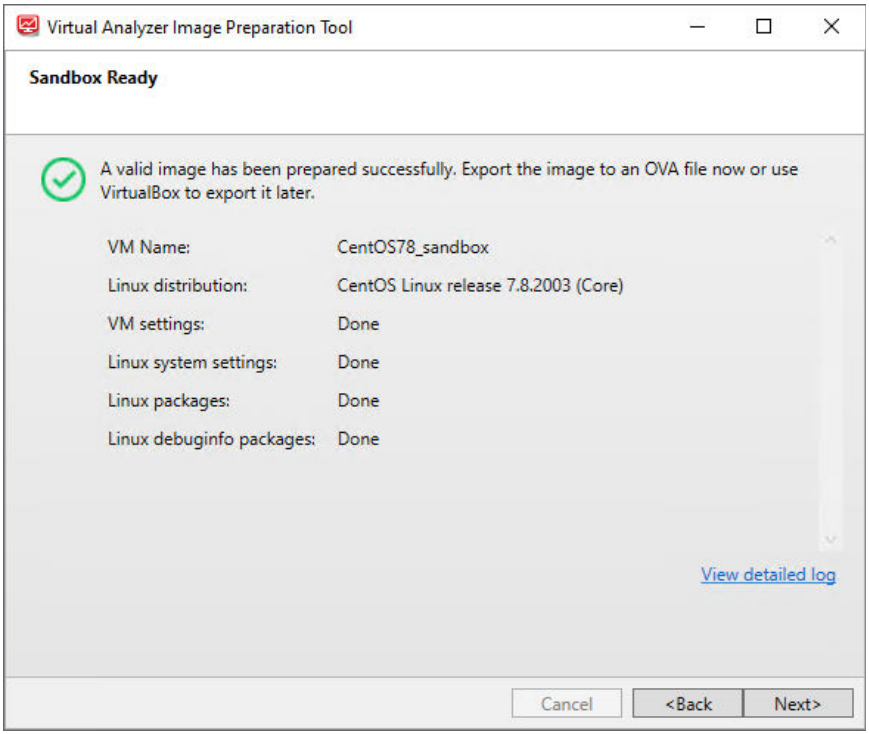


FIGURE 5-9. Sandbox Ready screen for Linux images

Note

`SandboxWizard.exe` saves logs in the `\log` folder where you run the tool. Logs use the following naming convention: `d:\SandboxWizard\log\VATool-yyyymmddhhmmss.txt`

For example: `d:\SandboxWizard\log\VATool-20170925025520.txt`

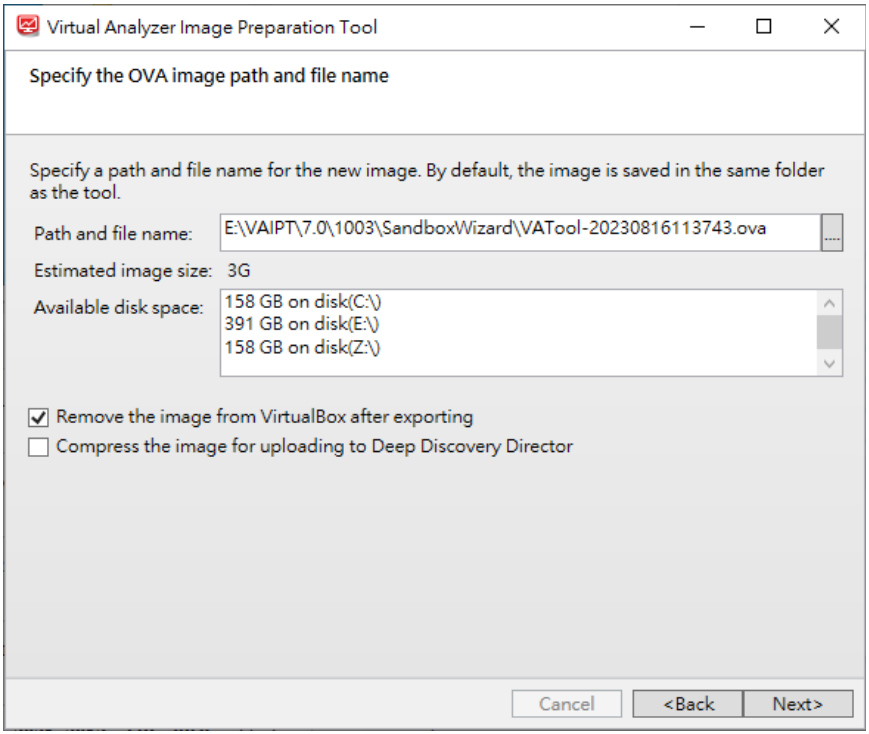


FIGURE 5-10. Specify the OVA image path and file name

13. Configure the settings on the **Specify the OVA image path and file name** screen.

    - Specify the path and file name that the tool uses when saving the OVA file.

      Note

      The tool uses the following naming convention when saving an OVA file: `VATool-20170925025520.ova`

    - (Optional) Enable **Remove the image from VirtualBox after exporting**.

Trend Micro recommends removing unused images from VirtualBox to help reduce storage usage and minimize performance impact on the host system.

- (Optional) Enable **Compress the image for uploading to Deep Discovery Director**.

Important

Only Virtual Analyzer images compressed in TAR format by the Virtual Analyzer Image Preparation Tool can be uploaded to and deployed from Deep Discovery Director.

14. Click **Next**.

    The **Export the image to OVA** screen appears and the tool exports the OVA file.

The **OVA Image Ready** screen appears when the export process completes.

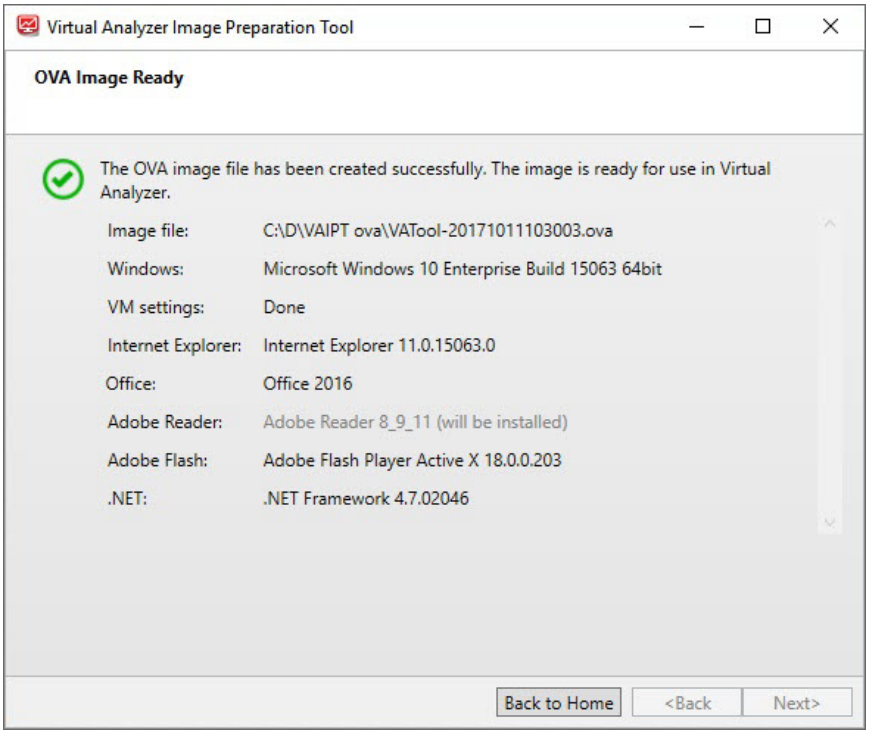


FIGURE 5-11. OVA Image Ready screen for Windows images

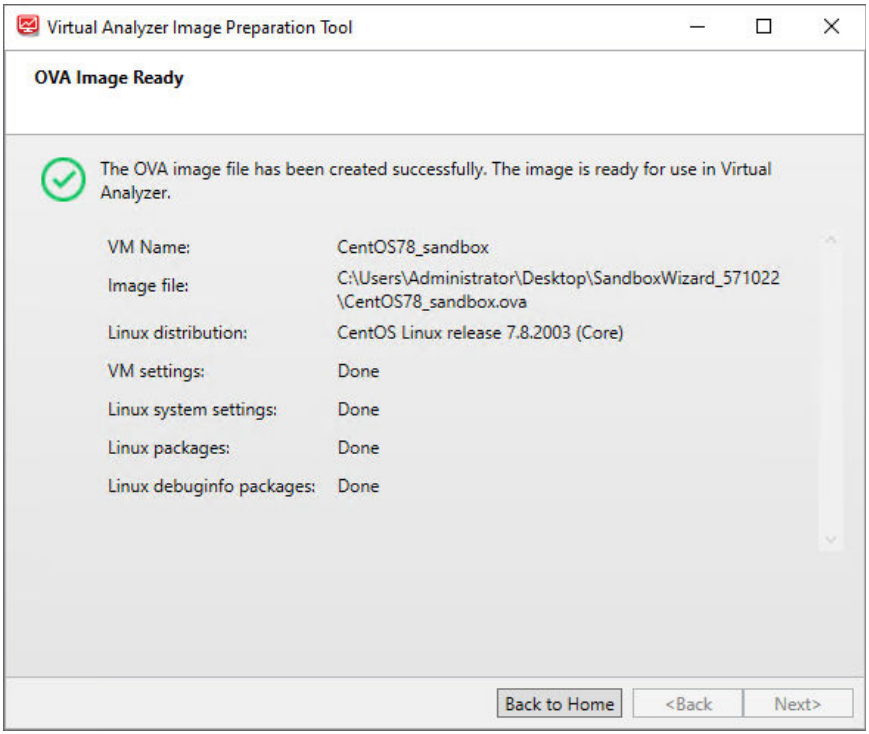


FIGURE 5-12. OVA Image Ready screen for Linux images

15. Click the **Close** button in the upper right corner to exit the tool or click **Back to Home** to prepare another image.

Products Not Activated - Windows

The **Products Not Activated** screen appears when the tool detects that Windows and/or Microsoft Office are installed but not activated. You can choose to activate the products or continue with image preparation.

Note

Trend Micro recommends activating Windows and Microsoft Office to ensure normal operation of the image.

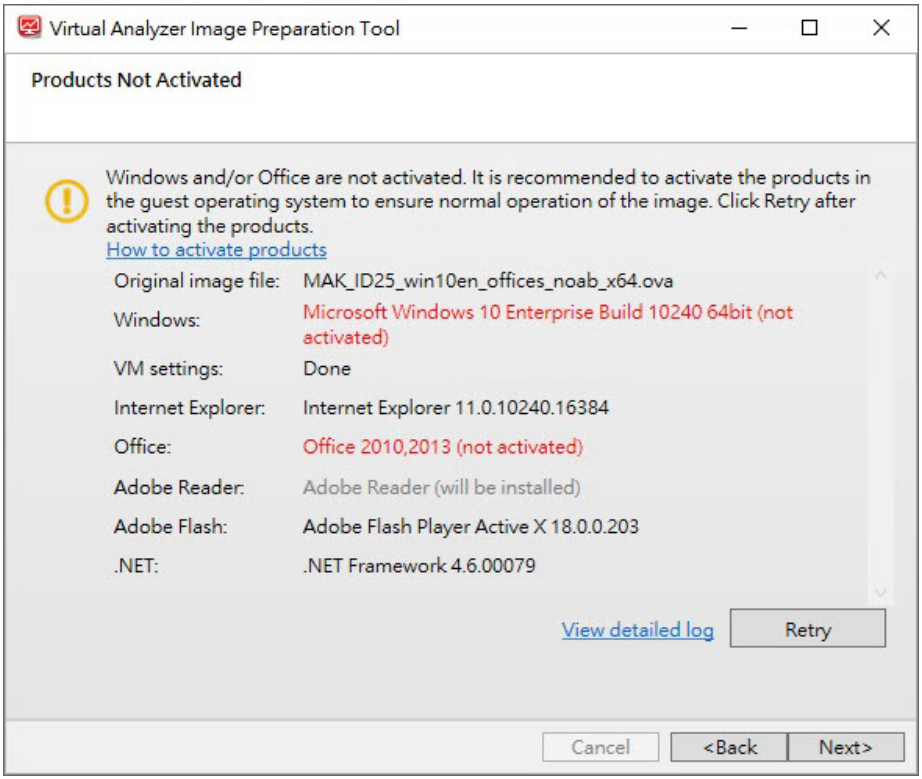


FIGURE 5-13. Products Not Activated screen for Windows images

To activate Windows and/or Microsoft Office, perform the following steps.

Procedure

1. Open VirtualBox and run the virtual machine.
2. Activate Windows and/or Microsoft Office.
3. After the software activates, go back to the tool and click **Retry**.

Sandbox Preparation Unsuccessful - Missing Windows Software

The **Sandbox Preparation Unsuccessful** screen appears when the tool is unable to fix issues during preparation.

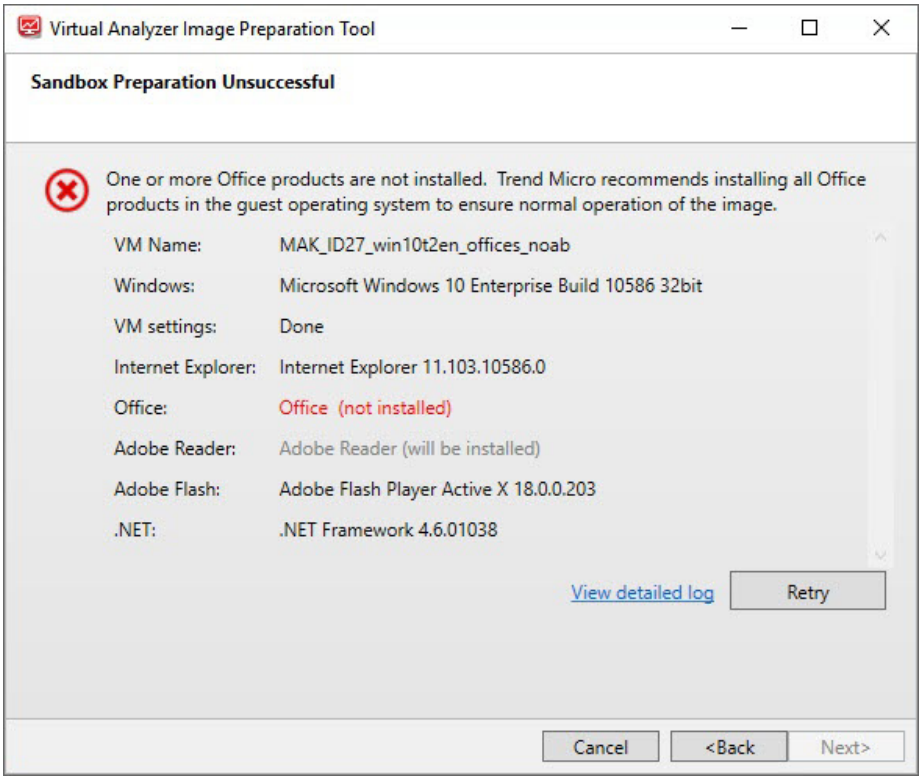


FIGURE 5-14. Sandbox Preparation Unsuccessful screen for Windows images

The most common reason for Windows preparation to fail is missing software. To fix the issue, perform the following steps:

Procedure

1. Open VirtualBox and run the virtual machine.
2. Install the missing software.
3. Go back to the tool and click **View detailed log**.
4. Perform any recommended actions in the log.
5. Click **Retry**.

   If any issues persist or continue to be unresolved, see *Troubleshooting Common Issues on page 5-25*.

Note

`SandboxWizard.exe` saves logs in the `\log` folder where you run the tool. Logs use the following naming convention: `d:\SandboxWizard\log\VATool-yyyymmddhhmmss.txt`

For example: `d:\SandboxWizard\log\VATool-20170925025520.txt`

Sandbox Preparation Unsuccessful - Missing Linux Packages

The **Sandbox Preparation Unsuccessful** screen appears when the tool is unable to fix issues during preparation.

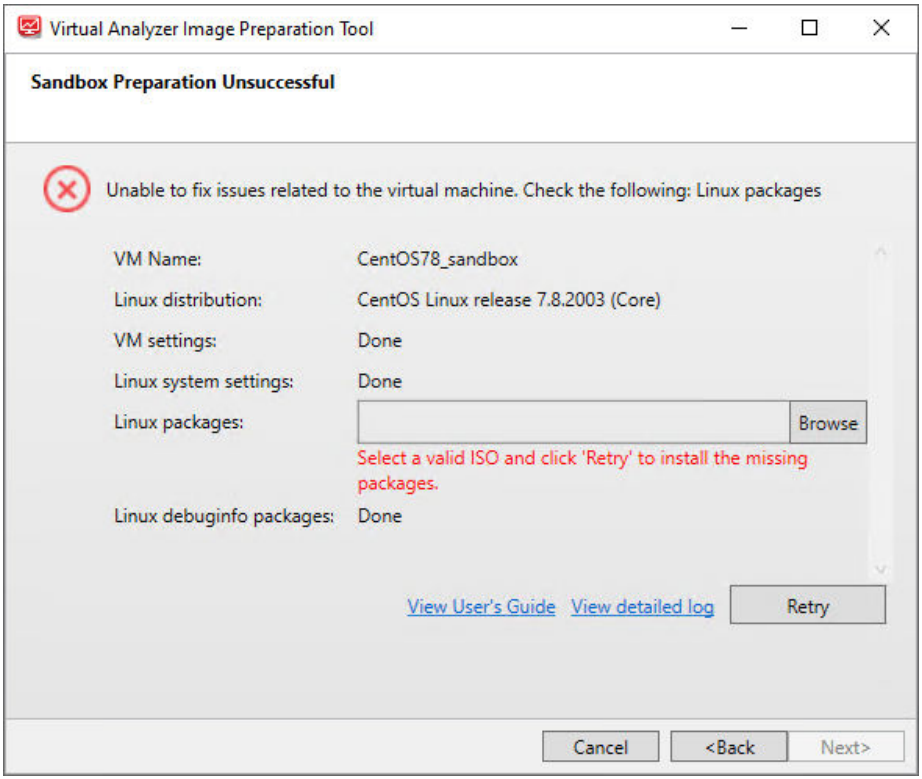


FIGURE 5-15. Sandbox Preparation Unsuccessful screen for Linux images

The most common reason for Linux preparation to fail is missing packages. To fix the issue, perform the following steps:

Procedure

1. To manually install the missing packages:

a. Open VirtualBox and run the virtual machine.

b. Install the missing packages.

2. To install missing packages automatically with the tool:

   a. For Red Hat Enterprise Linux, sign into the virtual machine register a valid subscription account.

   b. On the Sandbox Preparation Unsuccessful screen, click **Browse**.

   c. Locate and select the installation ISO file for the Linux distribution used.

3. Click **View detailed log** and perform any recommended actions.

4. Click **Retry**.

   If any issues persist or continue to be unresolved, see *Troubleshooting Common Issues on page 5-25*.

Note

`SandboxWizard.exe` saves logs in the `\log` folder where you run the tool. Logs use the following naming convention:

`d:\SandboxWizard\log\VATool-yyyymmddhhmmss.txt`

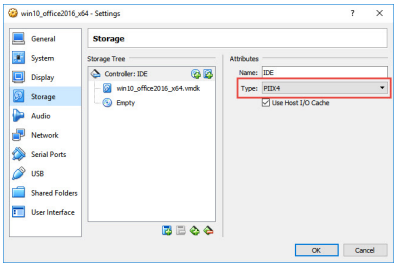
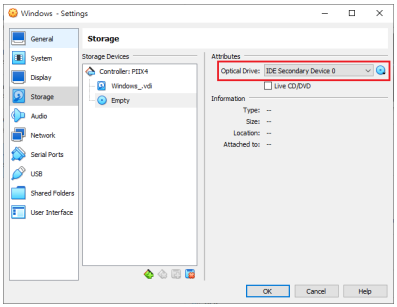
For example: `d:\SandboxWizard\log\VATool-20170925025520.txt`

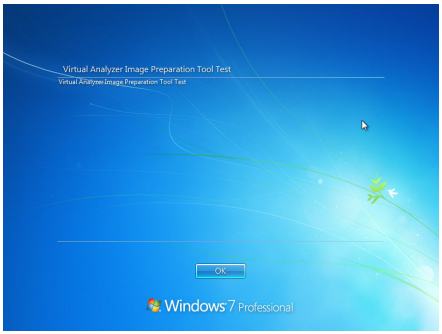
Troubleshooting Common Issues

TABLE 5-5. Common Issues When Using the Tool to Validate Windows Images

ISSUE	CAUSE	RECOMMENDED ACTION
Unable to upload an OVA file.	The image does not meet the minimum or maximum size requirements.	Verify that the size of the OVA file is supported by your product.

Issue	Cause	Recommended Action
Unable to prepare a virtual machine image.	The image was not created using VirtualBox.	Install a supported VirtualBox version. For details, see *System Requirements on page 5-3*.
	VirtualBox is not installed on the computer.	
	VirtualBox version is not supported for the selected guest OS	
	The image uses an unsupported operating system.	Use a supported operating system. For details, see *Required Software on page 2-2*.
	VirtualBox is unresponsive.	Refer to the VirtualBox documentation. https://www.virtualbox.org/manual/ch12.html#idp54271008

Issue	Cause	Recommended Action
Unable to start the VirtualBox installation CD/DVD.	Settings are incorrectly configured.	Open the imported image using VirtualBox and verify the following **Storage** settings. • Select **Controller: IDE** and verify that the specified type is set to **PIIX4**.  **Figure 5-16. Controller: IDE must be set to PIIX4** • Select the optical disc icon and verify that the specified **Optical Drive** is set to **IDE Secondary Device 0**.  **Figure 5-17. Optical drive is set to IDE Secondary Device 0**

Issue	Cause	Recommended Action
Unable to enter the desktop of the guest operating system.	Group policy settings are incorrectly configured.	Click **OK** on the **Virtual Analyzer Image Preparation Tool Test** screen to enter the desktop of the guest operating system. 

Issue	Cause	Recommended Action
Unable to start SandboxWizard.exe in the guest image.	AutoPlay settings are incorrectly configured.	1. Open VirtualBox. 2. On the **VirtualBox Manager** screen, click  to power on the image. 3. On the guest operating system, perform the following: a. Go to **Control Panel** > **Hardware and Sound** > **AutoPlay**. b. Select **Install or run program from your media** from the **Software and games** drop-down menu. c. Click **Save**. d. Open the **Local Group Policy Editor**. e. Go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **AutoPlay Policies**. f. Select **Not configured** to disable AutoPlay.

Issue	Cause	Recommended Action
Unable to prepare a Windows 7 or Windows Server 2008 R2 virtual machine image.	Updates KB4474419 and KB4490628 are not installed.	Manually install the updates. 1. Open VirtualBox. 2. On the **VirtualBox Manager** screen, click  to power on the image. 3. On the guest operating system, perform the following: a. Open a web browser and go to the **Microsoft Update Catalog** site. b. Search for `KB4474419` and `KB4490628` and download the correct update files for the guest operating system. c. Install the updates.

Table 5-6. Common Issues When Using the Tool to Validate Linux Images

Issue	Cause	Recommended Action

Unable to prepare a virtual machine image.	The VirtualBox virtual machine type is not supported.	Use the correct virtual machine type.
		• Type: Linux
		• Version:
		  • CentOS and RHEL: Red Hat (64-bit)
		  • Ubuntu: Ubuntu (64-bit)

Unable to connect to the virtual machine environment.	sshd is not running in virtual machine environment.	Start sshd in virtual machine environment.
	The virtual machine environment's network interface is not connected.	Verify network interface is connected on boot.

Issue	Cause	Recommended Action
Unable to install required packages with specified ISO.	The specified ISO is not the correct installation ISO.	Download the installation ISO from the official website. • For CentOS 7.8, download the CentOS 7.8.2003 Installation ISO `CentOS-7-x86_64-Everything-2003.iso` • For RHEL 7.9, download the RHEL 7.9 distribution ISO `rhel-server-7.9-x86_64-dvd.iso` • For RHEL 8.3, download the RHEL 8.3 distribution ISO `rhel-8.3-x86_64-dvd.iso` The ISO file can be verified by checking the hash value. If the issue persists, contact your support provider for assistance.

Sample Logs

Windows image preparation successful. Missing app detected.

```
--------------------------------------------------------------------------------------------------------------
Trend Micro Inc(TM) Virtual Analyzer Image Preparation Tool
Detailed Log
--------------------------------------------------------------------------------------------------------------


1. Overview
--------------------------------------------------------------------------------------------------------------
Result                          Preparation successful
Completed                       2019-12-13 03:43:13
Virtual machine name            VATool-20191213032810(in VirtualBox)          - OK


2. Hardware settings
--------------------------------------------------------------------------------------------------------------
Processor Count                 1                                             - OK
Memory Size                     1024                                          - OK
Host Audio Driver               "dsound"                                      - OK
Audio Controller                "dsound"                                      - OK
Nested Paging                   "on"                                          - OK
Large Page                      "on"                                          - OK
CPU Execution Cap               100                                           - OK
PAE/NX                          "on"                                          - OK
ACPI                            "on"                                          - OK
HPET                            "off"                                         - OK
I/O APIC                        "on"                                          - OK
Use UTC                         "off"                                         - OK
Chipset                         "ich9"                                        - OK
USB                             "on"                                          - OK
USB ECHI                        "off"                                         - OK
VT-x                            "on"                                          - OK
Pointing Device                 "usbtablet"                                   - OK
NIC                             "nat"                                         - OK
IDE Controller                                                                - OK
CD/DVD drive                                                                  - OK
VMDK/VDI                                                                      - OK


3. Windows and applications"
--------------------------------------------------------------------------------------------------------------
Windows                         Microsoft Windows 10 Enterprise Build 17134 32bit - OK
Office
  2013                          Microsoft Excel 2013                          - OK
                                Microsoft PowerPoint 2013                     - OK
                                Microsoft Word 2013                           - OK
                                Microsoft Publisher 2013                      - OK
  2016                          Microsoft Excel 2016                          - OK
                                Microsoft PowerPoint 2016                     - OK
                                Microsoft Word 2016                           - OK
                                Microsoft Publisher 2016                      - OK
.NET                            .NET Framework 4.7.03056                      - OK
Internet Explorer               Internet Explorer 11.112.17134.0              - OK
Adobe Flash                     Adobe Flash Player Active X 30.0.0.113        - OK
Adobe Reader                    Adobe Reader                                  - will be installed
```

Windows image preparation unsuccessful. Some items must be fixed manually.

```
-------------------------------------------------------------------------------------------------------------
Trend Micro Inc(TM) Virtual Analyzer Image Preparation Tool
Detailed Log
-------------------------------------------------------------------------------------------------------------


1. Overview
-------------------------------------------------------------------------------------------------------------
Result                          Preparation unsuccessful. Some items need to be fixed manually.
Error Reason                    One or more Office products are not installed.
Completed                       2019-12-13 09:44:45
Virtual machine name            VATool-20191213092157(in VirtualBox)          - OK


2. Hardware settings
-------------------------------------------------------------------------------------------------------------
Processor Count                 1                                             - OK
Memory Size                     1024                                          - OK
Host Audio Driver               "null"                                        - OK
Audio Controller                "null"                                        - OK
Nested Paging                   "on"                                          - OK
Large Page                      "off"                                         - OK
CPU Execution Cap               100                                           - OK
PAE/NX                          "on"                                          - OK
ACPI                            "on"                                          - OK
HPET                            "on"                                          - OK
I/O APIC                        "on"                                          - OK
Use UTC                         "off"                                         - OK
Chipset                         "ich9"                                        - OK
USB                             "on"                                          - OK
USB ECHI                        "off"                                         - OK
VT-x                            "on"                                          - OK
Pointing Device                 "usbtablet"                                   - OK
NIC                             "natnetwork"                                  - OK
NAT Network                     "NatNetwork"                                  - OK
IDE Controller                                                                - OK
CD/DVD drive                                                                  - OK
VMDK/VDI                                                                      - OK


3. Windows and applications"
-------------------------------------------------------------------------------------------------------------
Windows                         Microsoft Windows 10 Enterprise Build 17134 64bit - Installed
Office
  2019                          Microsoft Excel 2019                          - Installed
                                Microsoft PowerPoint 2019                     - Error: not installed
                                Microsoft Word 2019                           - Error: not installed
                                Microsoft Publisher 2019                      - Installed
.NET                            .NET Framework 4.7.03056                      - OK
Internet Explorer               Internet Explorer 11.112.17134.0              - OK
Adobe Flash                     Adobe Flash Player Active X 32.0.0.207        - OK
Adobe Reader                    Adobe Reader                                  - will be installed
```

Linux image preparation successful.

```
--------------------------------------------------------------------------------------------------------------------------
Trend Micro Inc(TM) Virtual Analyzer Image Preparation Tool
Detailed Log
--------------------------------------------------------------------------------------------------------------------------


1. Overview
--------------------------------------------------------------------------------------------------------------------------
Result                          Preparation successful
Completed                       2021-01-01 12:00:00
Virtual Machine Name            CentOS78_sandbox(in VirtualBox)             - OK


2. Hardware Settings
--------------------------------------------------------------------------------------------------------------------------
Processor count                 1                                           - OK
Memory size                     1024                                        - OK
Host Audio Driver               null                                        - OK
Audio Controller                null                                        - OK
[illegible]                                                                 - OK


[illegible]                                                                 - OK
IDE Controller                                                              - OK
CD/DVD Drive                                                                - OK
VMDK/VDI                                                                    - OK


3. Linux system settings
--------------------------------------------------------------------------------------------------------------------------
SELinux                         off                                         - OK
SSHD                            on                                          - OK
Kdump                           off                                         - OK
NTP                             off                                         - OK
Grub Timeout                    1                                           - OK
OS Auto Update                  off                                         - OK


4.Operating System and Packages
--------------------------------------------------------------------------------------------------------------------------
Linux distribution                          CentOS Linux release 7.8.2003 (Core)            - OK
Kernel-3.10.0-1127.el7.x86_64               Kernel-3.10.0-1127.el7.x86_64                   - OK
libpcap-1.5.312.el7.x86_64                  libpcap-1.5.312.el7.x86_64                      - OK
[illegible]                                 [illegible]                                     - OK


[illegible]                                 [illegible]                                     - OK
kerneldebuginfo-3.10.01127.el7.x86_64       kerneldebuginfo-3.10.01127.el7.x86_64           - OK
gccdebuginfo-4.8.539.el7.x86_64             gccdebuginfo-4.8.539.el7.x86_64                 - OK
openssldebuginfo-1.0.2k19.el7.x86_64        openssldebuginfo-1.0.2k19.el7.x86_64            - OK
curldebuginfo-7.29.057.el7.x86_64           curldebuginfo-7.29.057.el7.x86_64               - OK
zlibdebuginfo-1.2.718.el7.x86_64            zlibdebuginfo-1.2.718.el7.x86_64                - OK
glibcdebuginfo-2.17307.el7.1.x86_64         glibcdebuginfo-2.17307.el7.1.x86_64             - OK
```

Linux image preparation unsuccessful. Missing packages detected. Manual fix required.

```
--------------------------------------------------------------------------------------------------------------------------------
Trend Micro Inc(TM) Virtual Analyzer Image Preparation Tool
Detailed Log
--------------------------------------------------------------------------------------------------------------------------------


1. Overview
--------------------------------------------------------------------------------------------------------------------------------
Result                          Preparation unsuccessful. Some items need to be fixed manually.
Error Reason                    Check the following: Linux packages
Completed                       2021-01-01 12:00:01
Virtual Machine Name            En_CentOS_7_DVD_Minimal(in VirtualBox)        - OK


2. Hardware Settings
--------------------------------------------------------------------------------------------------------------------------------
Processor count                 1                                             - OK
Memory size                     1024                                          - OK
Host Audio Driver               null                                          - OK
Audio Controller                null                                          - OK
[illegible]                                                                   - OK


[illegible]                                                                   - OK
IDE Controller                                                                - OK
CD/DVD Drive                                                                  - OK
VMDK/VDI                                                                      - OK


3. Linux system settings
--------------------------------------------------------------------------------------------------------------------------------
SELinux                         off                                           - OK
SSHD                            on                                            - OK
Kdump                           off                                           - OK
NTP                             off                                           - OK
Grub Timeout                    1                                             - OK
OS Auto Update                  off                                           - OK


4.Operating System and Packages
--------------------------------------------------------------------------------------------------------------------------------
Linux distribution              CentOS Linux release 7.8.2003 (Core)          - OK
nodejs-6.17.11.el7.x86_64       nodejs-6.17.11.el7.x86_64                     - OK
yara-4.0.2                      yara-4.0.2                                    - OK
[illegible]                     [illegible]                                   - OK


[illegible]                     [illegible]                                   [illegible]
glibc-2.17307.el7.1.x86_64      glibc-2.17307.el7.1.x86_64                    - OK
gccc++-4.8.539.el7.x86_64       not installed                                 - Requires manual fix
gcc-4.8.539.el7.x86_64          not installed                                 - Requires manual fix
glibc-2.17307.el7.1.i686        glibc-2.17307.el7.1.i686                      - OK
libgcc-4.8.539.el7.x86_64       libgcc-4.8.539.el7.x86_64                     - OK
libstdc++-4.8.539.el7.x86_64    libstdc++-4.8.539.el7.x86_64                  - OK
openssl-1.0.2k19.el7.x86_64     openssl-1.0.2k19.el7.x86_64                   - OK
zip                             not installed                                 - Requires manual fix
strings                         strings                                       - OK
pidof                           pidof                                         - OK
sh                              sh                                            - OK
readelf                         readelf                                       - OK
ldd                             ldd                                           - OK
objcopy                         objcopy                                       - OK
tcsh                            tcsh                                          - OK
unzip                           unzip                                         - OK
bash                            bash                                          - OK
file                            file                                          - OK
```

Index

TREND MICRO INCORPORATED
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com
Item Code: APEM79955/240827