Trend Micro™

Virtual Analyzer Image Preparation Tool

7.0

User's Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the tool described herein without notice. Before installing and using the tool, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

https://docs.trendmicro.com

Document Part No.: APTM79813/230816

Release Date: August 2023

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

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

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

Chapter 4: Linux OVA File Preparation

Chapter 5: Virtual Analyzer Image Preparation Tool

Index

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 navigation 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:

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 2-8*.

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 2-43*.

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.

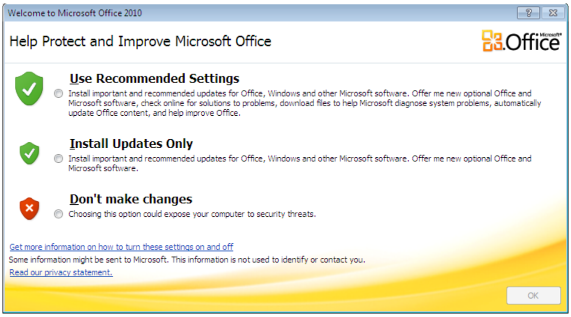
Note

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 21H2 and before, Windows 11 Version 21H2, 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.

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.  Welcome to Microsoft Office 2010 Help Protect and Improve Microsoft Office ○ **Use Recommended Settings** Install important and recommended updates for Office, Windows and other Microsoft software. Offer me new optional Office and Microsoft software, check online for solutions to problems, download files to help Microsoft diagnose system problems, automatically update Office content, and help improve Office. ○ **Install Updates Only** Install important and recommended updates for Office, Windows and other Microsoft software. Offer me new optional Office and Microsoft software. ○ **Don't make changes** Choosing this option could expose your computer to security threats. Get more information on how to turn these settings on and off Some information might be sent to Microsoft. This information is not used to identify or contact you. Read our privacy statement. **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.

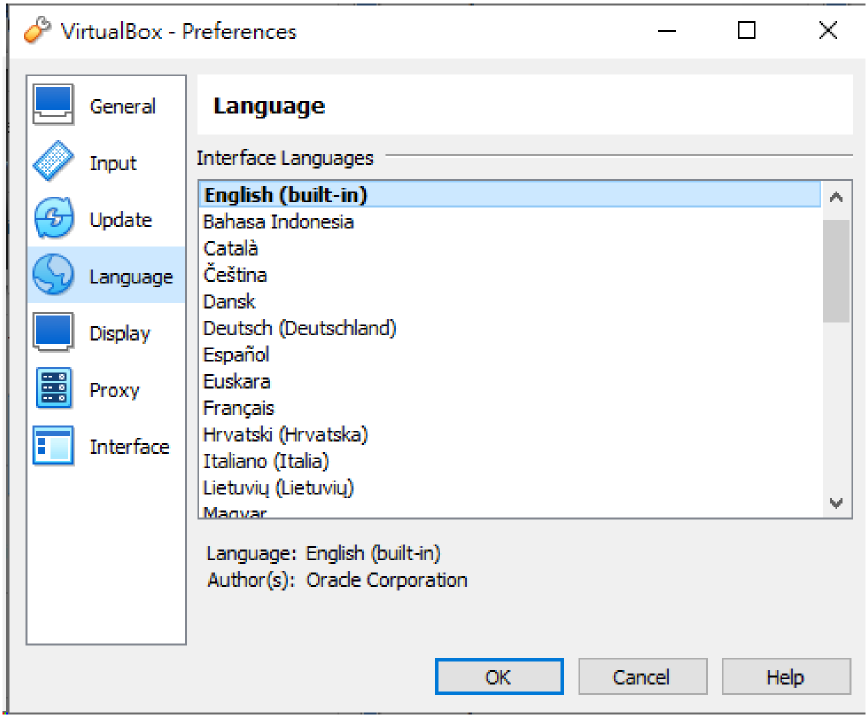
   Trend Micro recommends using VirtualBox version 7.0 and later.

   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**.



Language: English (built-in)
Author(s): Oracle Corporation

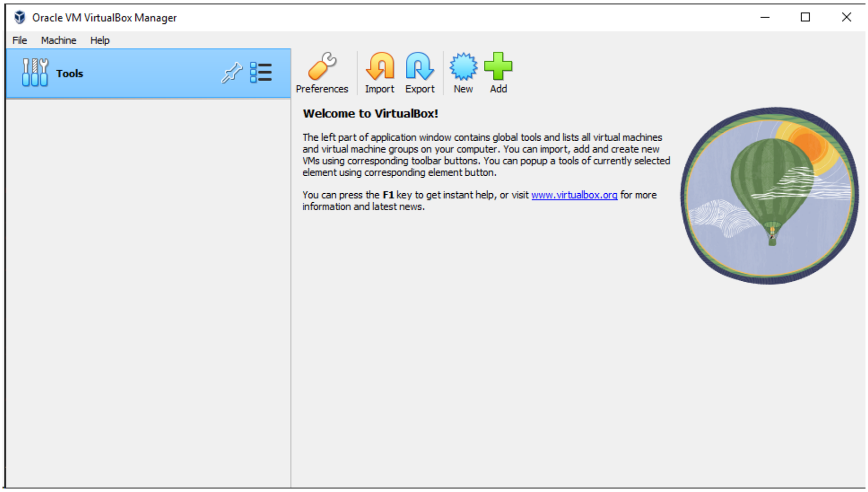
FIGURE 2-2. Language Settings

Creating Windows Virtual Machine Images

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

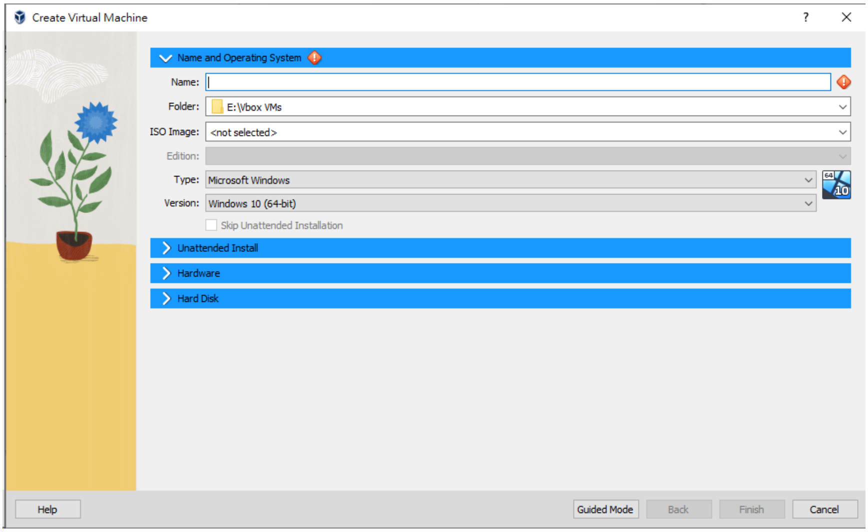
FIGURE 2-3. VirtualBox Manager

2. Click **New**.

   The **Create Virtual Machine** window opens.

3. Click **Expert Mode**.

The Create Virtual Machine wizard enters Expert Mode.



Create Virtual Machine

Name:

Folder: E:\Vbox VMs

ISO Image: <not selected>

Edition:

Type: Microsoft Windows

Version: Windows 10 (64-bit)

☐ Skip Unattended Installation

FIGURE 2-4. Create Virtual Machine - Expert Mode

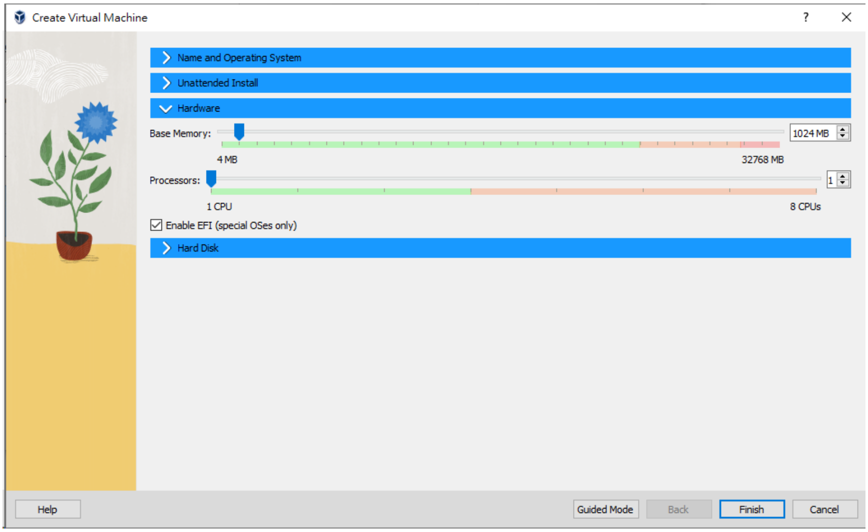
4. Configure the **Name and Operating System** settings.

   - 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.



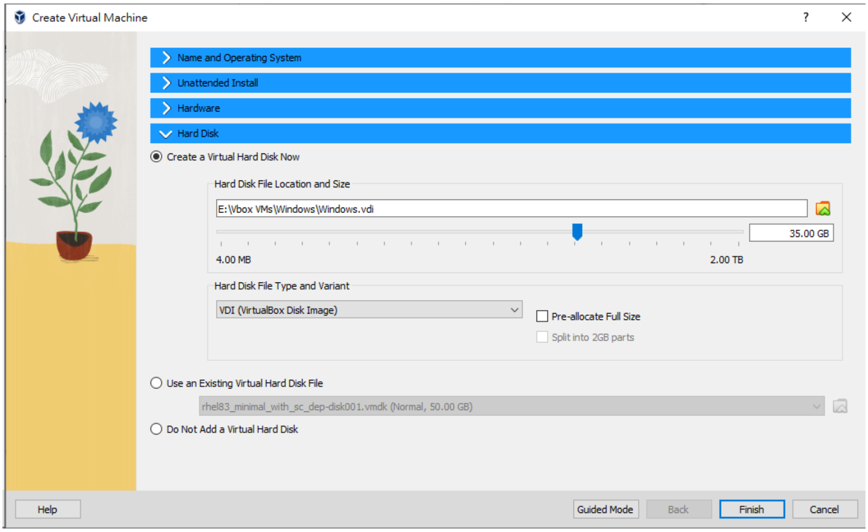
Base Memory: 1024 MB

Processors: 1

☑ Enable EFI (special OSes only)

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.



Create Virtual Machine

- Name and Operating System
- Unattended Install
- Hardware
- Hard Disk

● Create a Virtual Hard Disk Now

Hard Disk File Location and Size

E:\Vbox VMs\Windows\Windows.vdi

35.00 GB

4.00 MB — 2.00 TB

Hard Disk File Type and Variant

VDI (VirtualBox Disk Image)

□ Pre-allocate Full Size

□ Split into 2GB parts

○ Use an Existing Virtual Hard Disk File

rhel83_minimal_with_sc_dep-disk001.vmdk (Normal, 50.00 GB)

○ Do Not Add a Virtual Hard Disk

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.

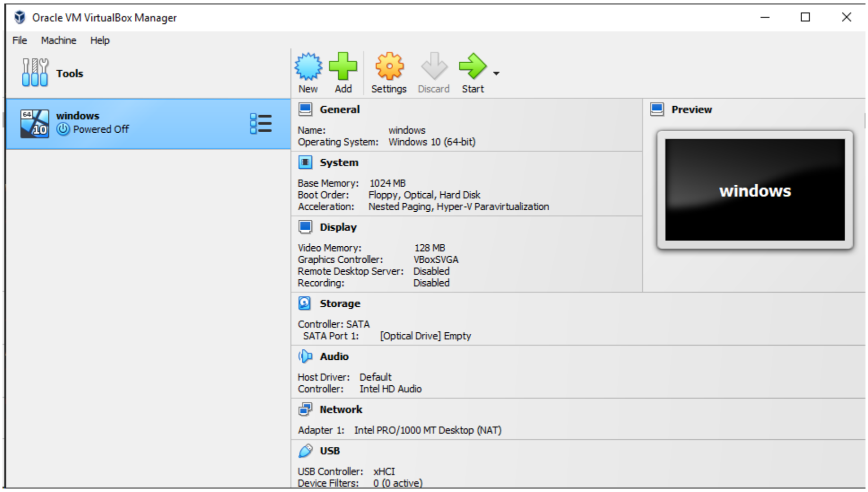
For best results, Trend Micro recommends selecting **VDI (VirtualBox Disk Image)**.

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.



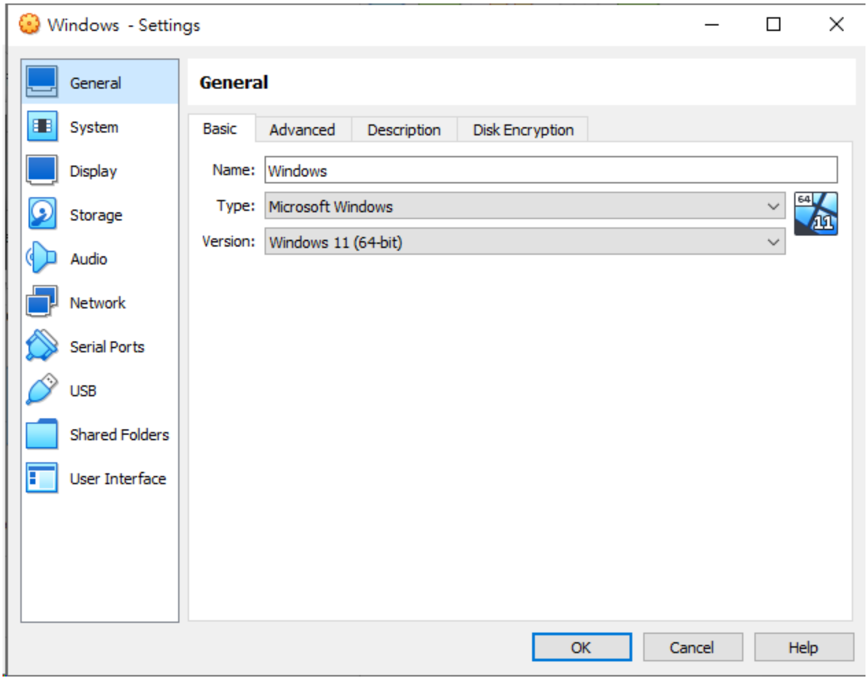
```
General
Name:               windows
Operating System:   Windows 10 (64-bit)

System
Base Memory:   1024 MB
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  Nested Paging, Hyper-V Paravirtualization

Display
Video Memory:            128 MB
Graphics Controller:     VBoxSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage
Controller: SATA
 SATA Port 1:      [Optical Drive] Empty

Audio
Host Driver:   Default
Controller:    Intel HD Audio

Network
Adapter 1:   Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller:   xHCI
Device Filters:   0 (0 active)
```

FIGURE 2-7. Newly-created Virtual Machine

Ensure that the virtual machine is not in any group.

12. Click **Settings**.

The **Settings** window opens.



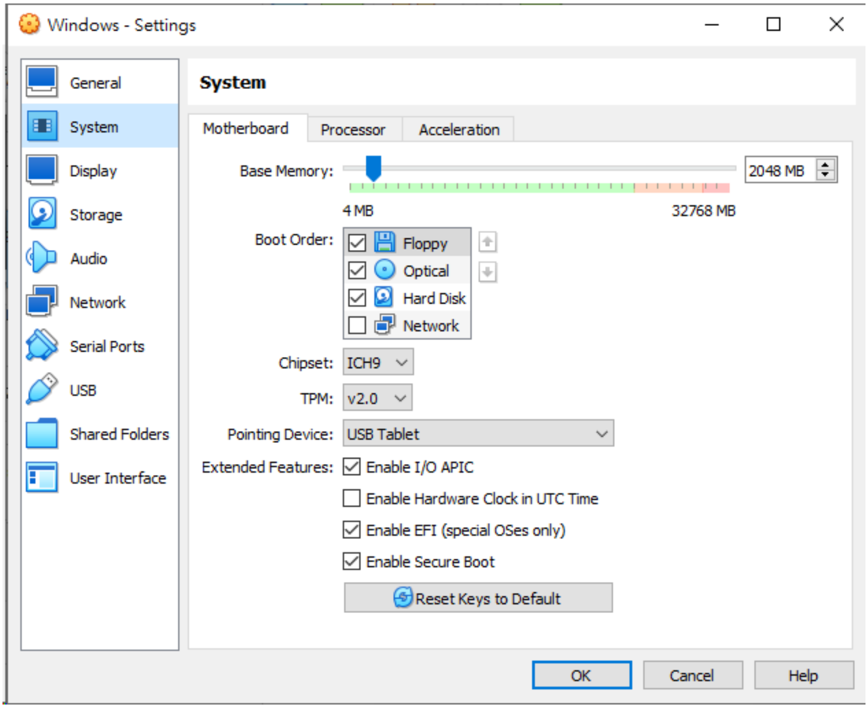
Name: Windows

Type: Microsoft Windows

Version: Windows 11 (64-bit)

FIGURE 2-8. VirtualBox Settings

13. Go to **System**.



Base Memory: 2048 MB (4 MB – 32768 MB)

Boot Order:
☑ Floppy
☑ Optical
☑ Hard Disk
☐ Network

Chipset: ICH9

TPM: v2.0

Pointing Device: USB Tablet

Extended Features:
☑ Enable I/O APIC
☐ Enable Hardware Clock in UTC Time
☑ Enable EFI (special OSes only)
☑ Enable Secure Boot

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**.

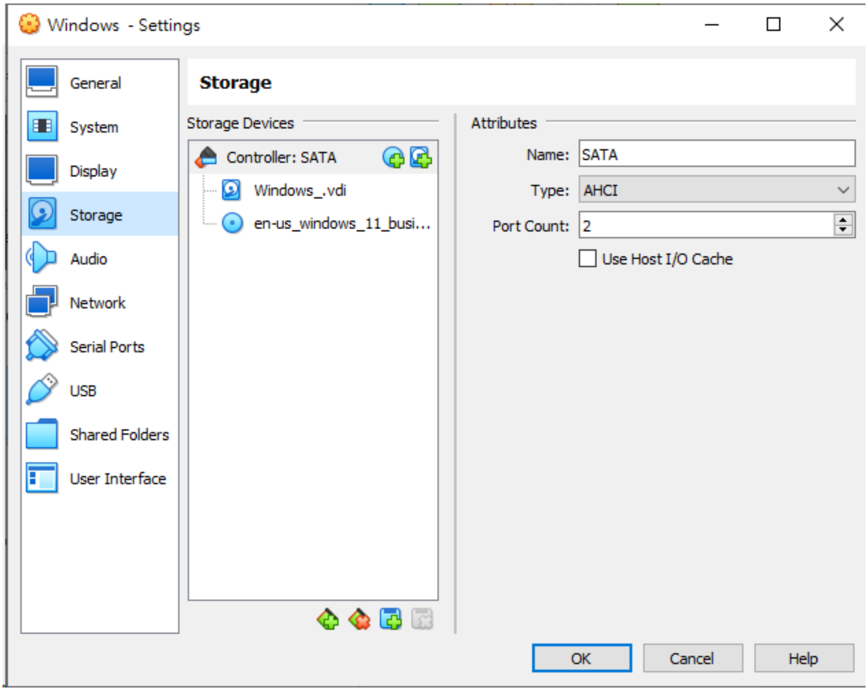
16. On the **Acceleration** tab, select **Enable Nested Paging**.

    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**.



Windows - Settings

Storage

Storage Devices

- Controller: SATA
  - Windows_.vdi
  - en-us_windows_11_busi...

Attributes

Name: SATA

Type: AHCI

Port Count: 2

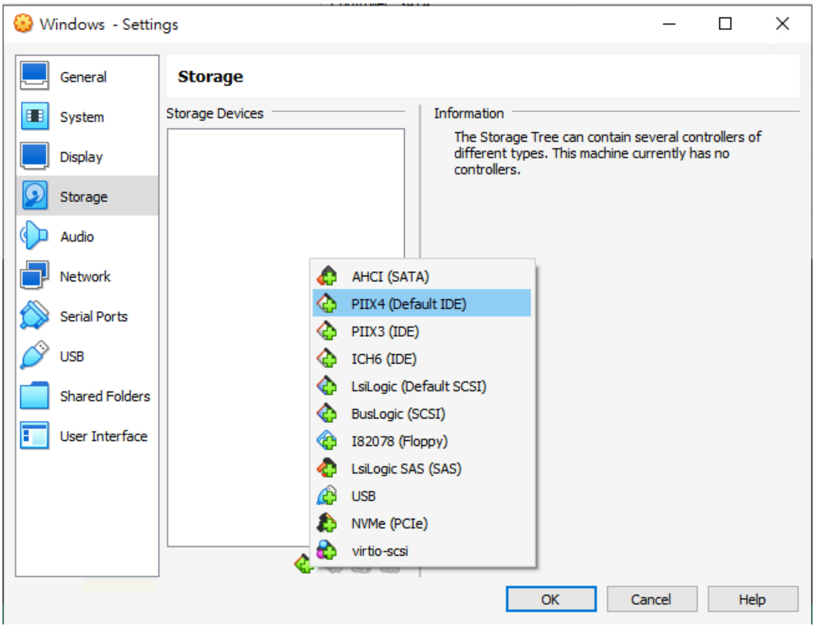
□ Use Host I/O Cache

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)**.

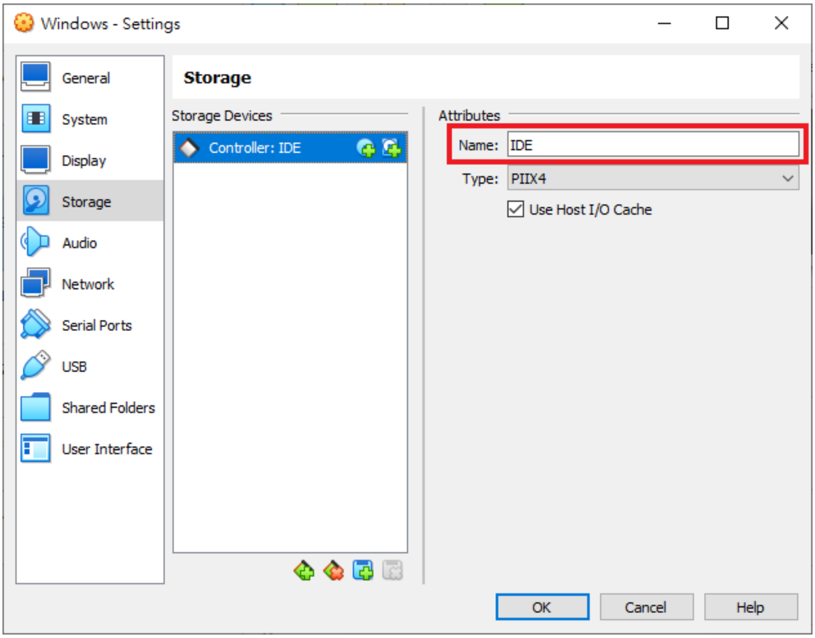


The Storage Tree can contain several controllers of different types. This machine currently has no controllers.

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`**.



Name: IDE

Type: PIIX4

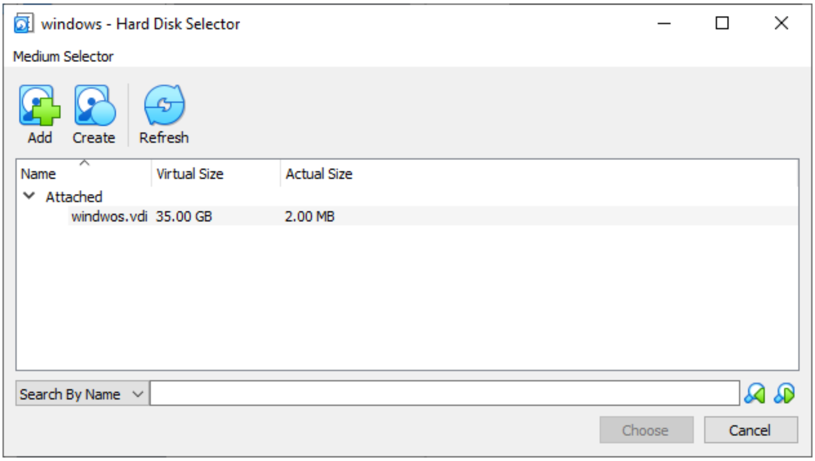
☑ Use Host I/O Cache

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.



windows - Hard Disk Selector

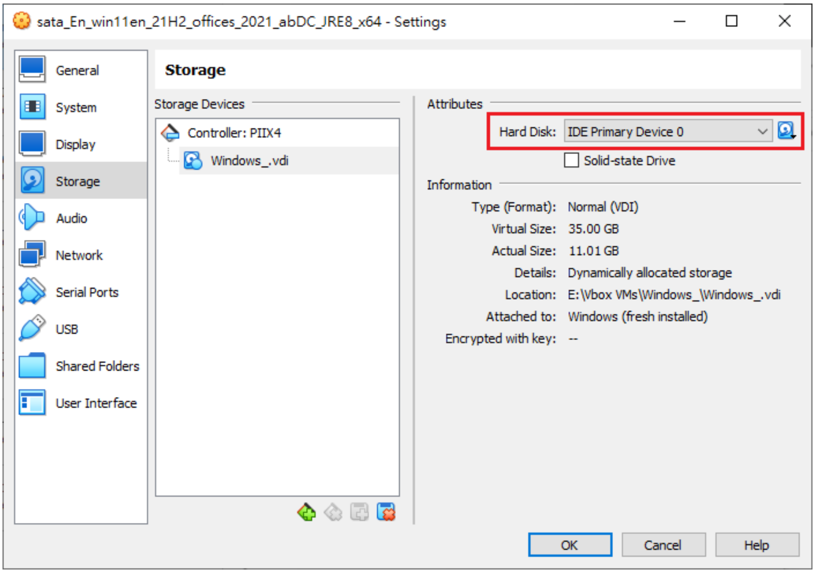
Medium Selector

Name	Virtual Size	Actual Size
Attached		
windwos.vdi	35.00 GB	2.00 MB

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**.



sata_En_win11en_21H2_offices_2021_abDC_JRE8_x64 - Settings

Storage

Storage Devices

- Controller: PIIX4
  - Windows_.vdi

Attributes

Hard Disk: IDE Primary Device 0

□ Solid-state Drive

Information

Type (Format):	Normal (VDI)
Virtual Size:	35.00 GB
Actual Size:	11.01 GB
Details:	Dynamically allocated storage
Location:	E:\Vbox VMs\Windows_\Windows_.vdi
Attached to:	Windows (fresh installed)
Encrypted with key:	--

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**.

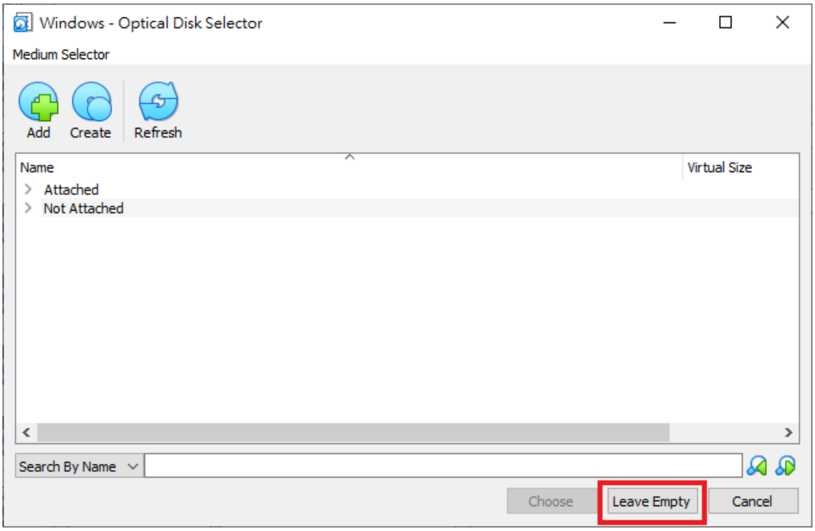
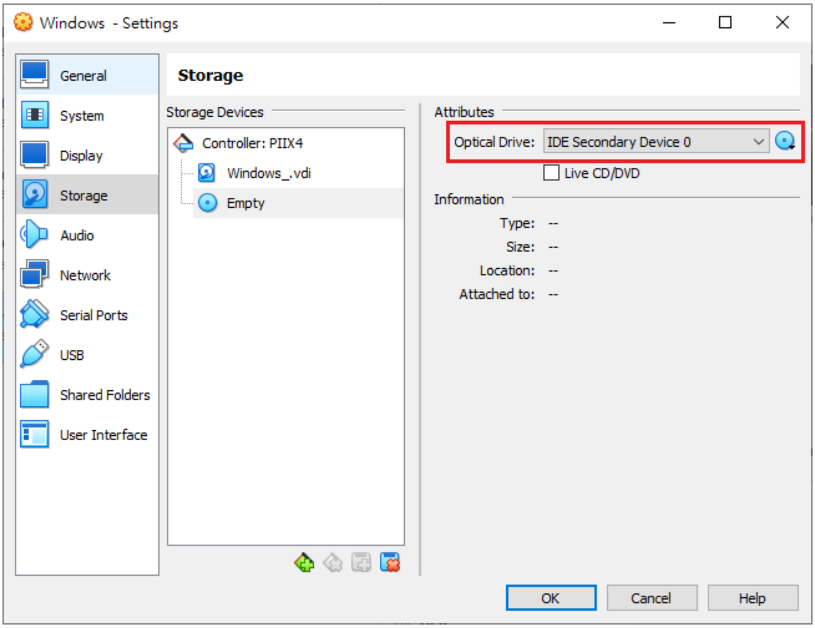


FIGURE 2-15. Optical Disk Selector

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



Optical Drive: IDE Secondary Device 0

□ Live CD/DVD

Type: --

Size: --

Location: --

Attached to: --

FIGURE 2-16. IDE Secondary Device 0

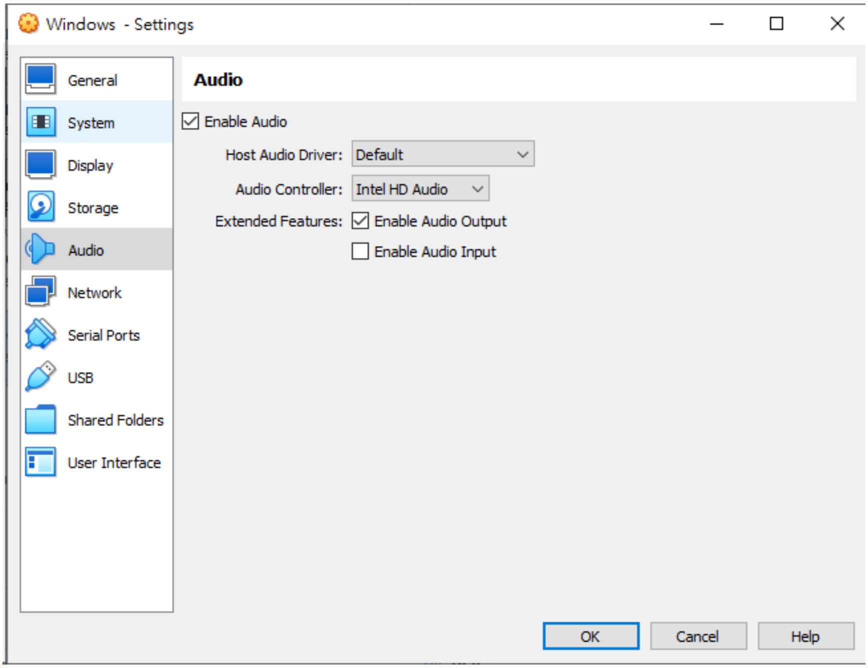
j. Click 💿 and select **Choose/Create a Virtual Optical Disk...**

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.



Audio

☑ Enable Audio

Host Audio Driver: Default

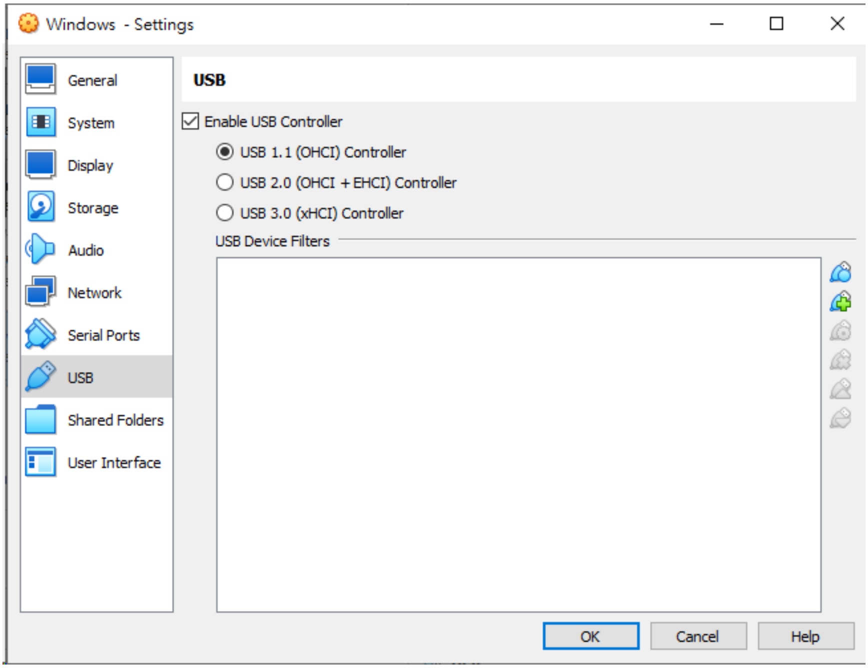
Audio Controller: Intel HD Audio

Extended Features: ☑ Enable Audio Output

☐ Enable Audio Input

FIGURE 2-17. Audio Options Settings

21. Go to **USB**.



Windows - Settings

USB

☑ Enable USB Controller

● USB 1.1 (OHCI) Controller

○ USB 2.0 (OHCI + EHCI) Controller

○ USB 3.0 (xHCI) Controller

USB Device Filters

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.

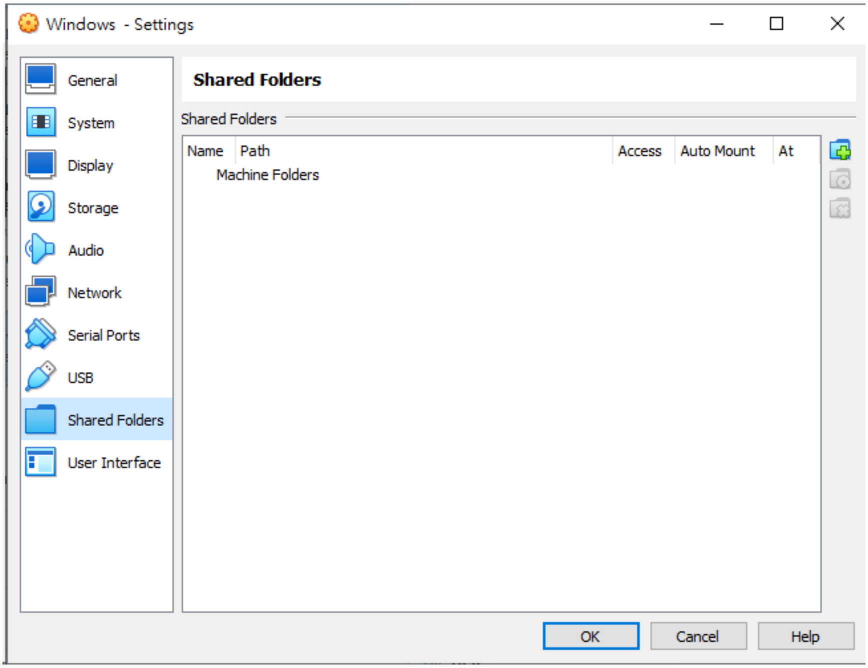
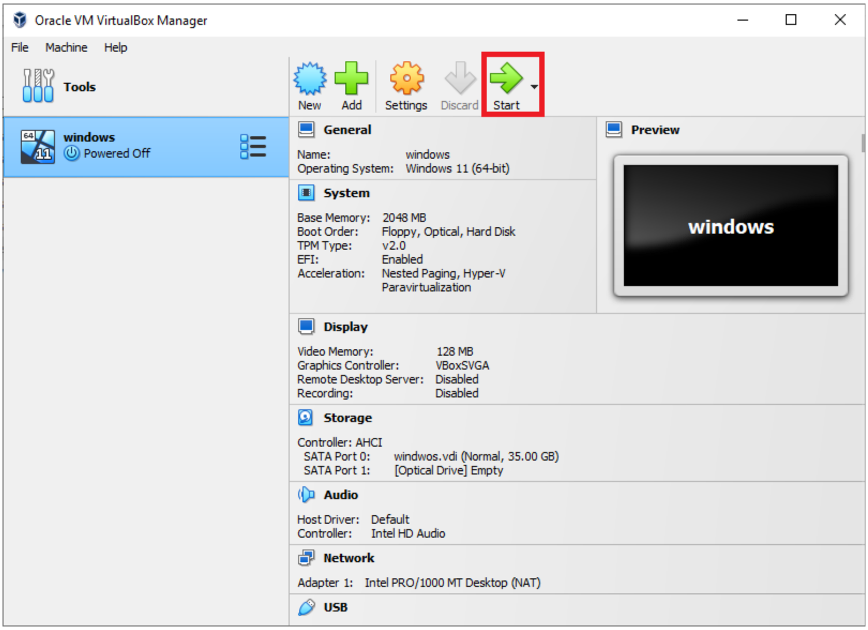


FIGURE 2-19. Shared Folders Settings

25. Click **OK**.

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



windows
Powered Off

General

Name: windows
Operating System: Windows 11 (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
TPM Type: v2.0
EFI: Enabled
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: AHCI
SATA Port 0: windwos.vdi (Normal, 35.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Default
Controller: Intel HD Audio

Network

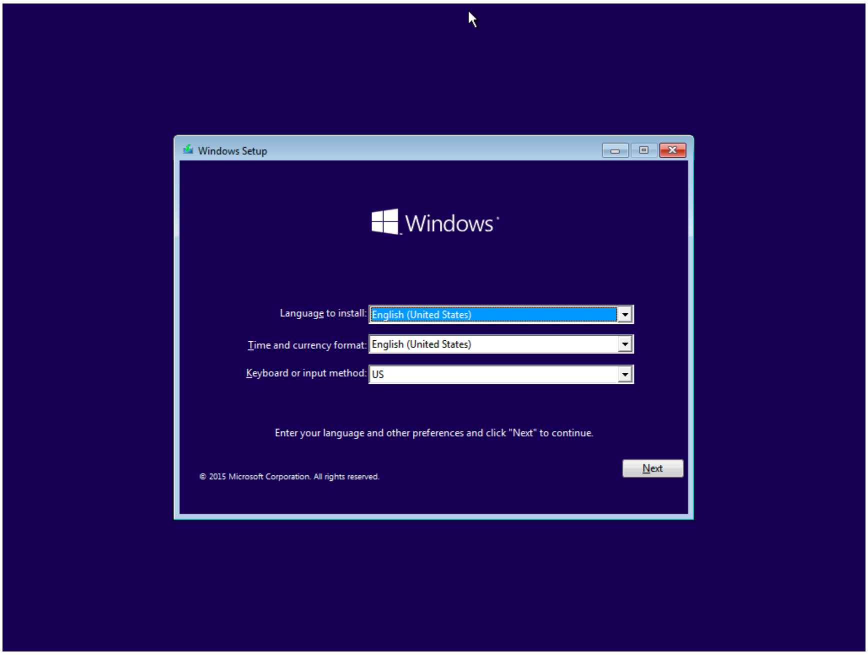
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

FIGURE 2-20. VirtualBox Manager

The installation process starts.

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



Language to install: English (United States)

Time and currency format: English (United States)

Keyboard or input method: US

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

© 2015 Microsoft Corporation. All rights reserved.

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.

<table>
<tr><th>TASK</th><th>STEPS</th></tr>
<tr><td></td><td>

Note

No logon prompt is displayed and the “Administrator” account is automatically used to log on.

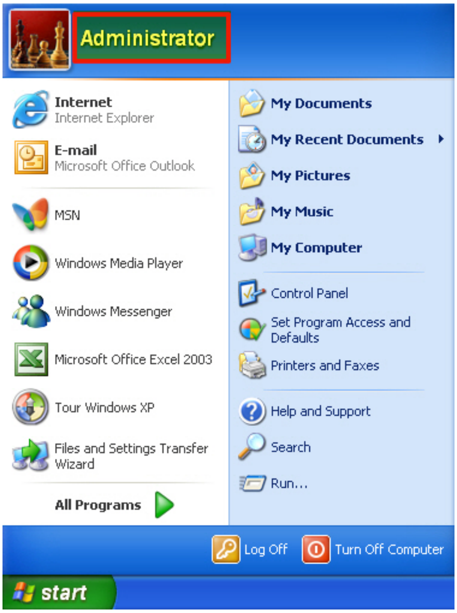


FIGURE 2-22. Windows XP Administrator Account

</td></tr>
<tr><td>View all user accounts.</td><td>Type <code>net user</code>.</td></tr>
<tr><td>Delete non-built-in user accounts one at a time.</td><td>Type <code>net user “<username>” /delete</code>.
Example: <code>net user “test” /delete</code></td></tr>
<tr><td>View all network adapters with an active link</td><td>Type <code>wmic nic where "netconnectionstatus=2" get netconnectionid /value</code>.</td></tr>
</table>

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:

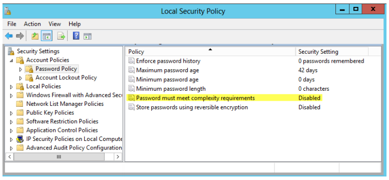
TASK	STEPS
Enable the “Administrator” account	Type **`net user “Administrator” /active:yes`**.

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`**

<table>
<tr><th>TASK</th><th>STEPS</th></tr>
<tr><td></td><td>

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.



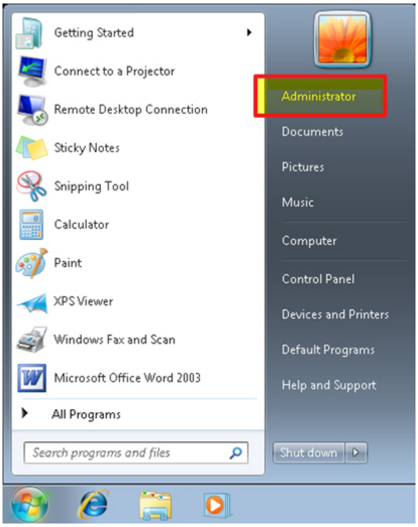
- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

<table>
<tr><th>Policy</th><th>Security Setting</th></tr>
<tr><td>Enforce password history</td><td>0 passwords remembered</td></tr>
<tr><td>Maximum password age</td><td>42 days</td></tr>
<tr><td>Minimum password age</td><td>0 days</td></tr>
<tr><td>Minimum password length</td><td>0 characters</td></tr>
<tr><td>Password must meet complexity requirements</td><td>Disabled</td></tr>
<tr><td>Store passwords using reversible encryption</td><td>Disabled</td></tr>
</table>

FIGURE 2-23. Disable Password must meet complexity requirements

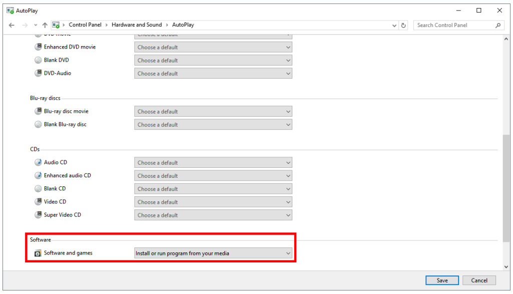
- Restart the image.

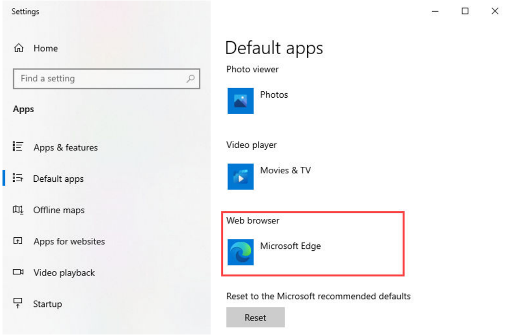
</td></tr>
</table>

Task	Steps
	No logon prompt is displayed and the "Administrator" account is automatically used to log on.  Getting Started Connect to a Projector Remote Desktop Connection Sticky Notes Snipping Tool Calculator Paint XPS Viewer Windows Fax and Scan Microsoft Office Word 2003 All Programs Search programs and files Administrator Documents Pictures Music Computer Control Panel Devices and Printers Default Programs Help and Support Shut down **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"`**

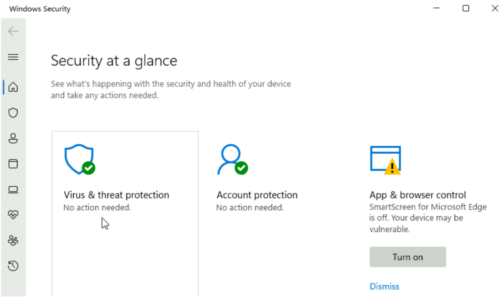
3. Perform the following tasks using the Windows graphical user interface:

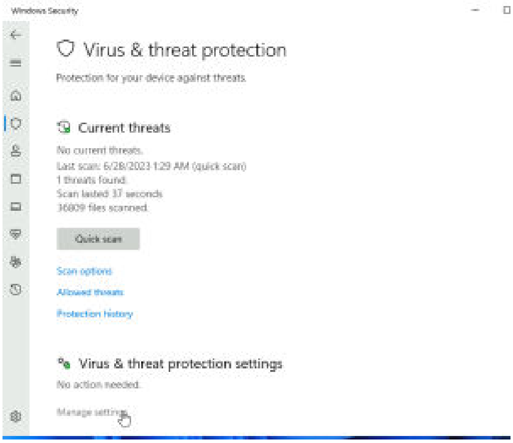
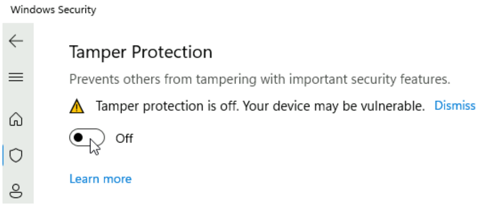
Task	Steps
Configure AutoPlay	a. Open the Windows **Start** menu, type `Control Panel` into the search box and press ENTER. b. In the **Control Panel**, go to **Hardware and Sound** > **AutoPlay**. AutoPlay Control Panel > Hardware and Sound > AutoPlay Enhanced DVD movie: Choose a default Blank DVD: Choose a default DVD-Audio: Choose a default Blu-ray discs Blu-ray disc movie: Choose a default Blank Blu-ray disc: Choose a default CDs Audio CD: Choose a default Enhanced audio CD: Choose a default Blank CD: Choose a default Video CD: Choose a default Super Video CD: Choose a default Software Software and games: Install or run program from your media **Figure 2-25. AutoPlay** c. For **Software and games**, select **Install or run program from your media**. d. Click **Save**.

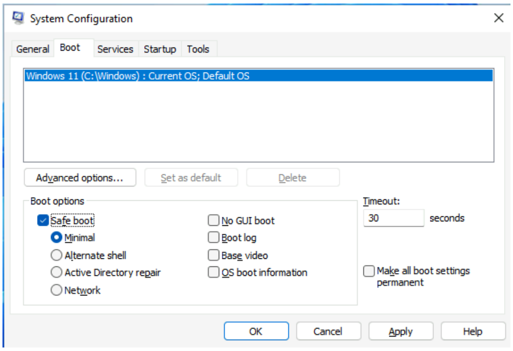
Task	Steps
Configure default web browser on Windows 10/11	The Virtual Analyzer supports both Microsoft Edge (Chromium) and Internet Explorer. One of these browsers must be manually set as the default web browser in Windows 10/11 before running the Virtual Analyzer. To configure the default web browser, 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.  Settings Home Find a setting Apps Apps & features Default apps Offline maps Apps for websites Video playback Startup Default apps Photo viewer Photos Video player Movies & TV Web browser Microsoft Edge Reset to the Microsoft recommended defaults Reset **Figure 2-26. Default apps** c. In the **Choose an app** context menu, select **Internet Explorer** or **Microsoft Edge**.

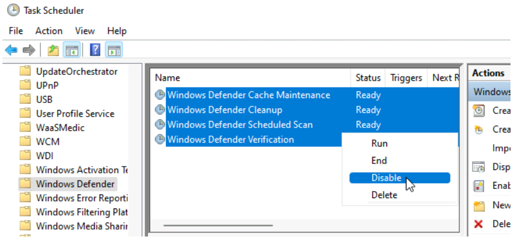
Task	Steps
	d. If the **Before you switch** dialog appears, select **Switch anyway**.
(Optional) Change the display resolution	Trend Micro recommends settings the screen resolution to at least **`1152 x 864`** to avoid triggering the anti-virtual machine functions of some malware. a. Open the Windows **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**.

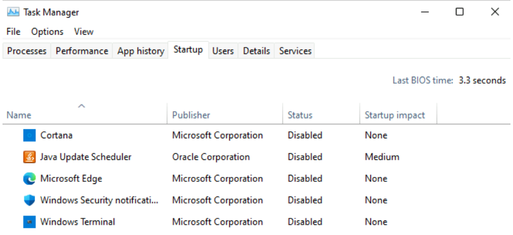
4. For Windows 11 21H2, perform the following tasks using the Windows graphical user interface:

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**.  Windows Security Security at a glance See what's happening with the security and health of your device and take any actions needed. Virus & threat protection No action needed. Account protection No action needed. App & browser control SmartScreen for Microsoft Edge is off. Your device may be vulnerable. **Figure 2-27. Windows Security**

Task	Steps
	c. Under **Virus & threat protection**, click **Manage settings**.  Windows Security Virus & threat protection Protection for your device against threats. Current threats No current threats. Last scan: 6/28/2023 1:29 AM (quick scan) 1 threats found. Scan lasted 37 seconds 36809 files scanned. Quick scan Scan options Allowed threats Protection history Virus & threat protection settings No action needed. Manage settings **FIGURE 2-28. Virus & Threat Protection** d. Turn **Tamper Protection** off.  Windows Security Tamper Protection Prevents others from tampering with important security features. ⚠ Tamper protection is off. Your device may be vulnerable. Dismiss ● Off Learn more **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**. System Configuration General Boot Services Startup Tools Windows 11 (C:\Windows) : Current OS; Default OS Advanced options... Set as default Delete Boot options ☑ Safe boot ● Minimal ○ Alternate shell ○ Active Directory repair ○ Network □ No GUI boot □ Boot log □ Base video □ OS boot information Timeout: 30 seconds □ Make all boot settings permanent OK Cancel Apply Help **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\CurrentControlSet\Services\WdFilter" /v Start /t REG_DWORD /d 4 /f`**

Task	Steps
	- `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**. k. Disable all Windows Defender tasks.  Name / Status Windows Defender Cache Maintenance / Ready Windows Defender Cleanup / Ready Windows Defender Scheduled Scan / Ready Windows Defender Verification Task Scheduler File Action View Help UpdateOrchestrator UPnP USB User Profile Service WaaSMedic WCM WDI Windows Activation Te Windows Defender Windows Error Reporti Windows Filtering Plat Windows Media Sharir Triggers Next R Run End Disable Delete Actions Windows Crea Crea Impo Disp Enab New Dele **FIGURE 2-31. Task Scheduler**

<table>
<tr><th>TASK</th><th>STEPS</th></tr>
<tr>
<td>(Optional) Disable startup applications</td>
<td>
a. Open the Windows <b>Start</b> menu, type <code><b>Task Manager</b></code> and press ENTER.
b. In <b>Task Manager</b>, go to the <b>Startup</b> tab.
c. Disable the following applications. To disable, right-click the name of the application and select <b>Disable</b>.
<ul>
<li>Cortana</li>
<li>Java Update Scheduler</li>
<li>Microsoft Edge</li>
<li>Windows Security notification icon</li>
<li>Windows Terminal</li>
</ul>


Last BIOS time: 3.3 seconds
<table>
<tr><th>Name</th><th>Publisher</th><th>Status</th><th>Startup impact</th></tr>
<tr><td>Cortana</td><td>Microsoft Corporation</td><td>Disabled</td><td>None</td></tr>
<tr><td>Java Update Scheduler</td><td>Oracle Corporation</td><td>Disabled</td><td>Medium</td></tr>
<tr><td>Microsoft Edge</td><td>Microsoft Corporation</td><td>Disabled</td><td>None</td></tr>
<tr><td>Windows Security notificati...</td><td>Microsoft Corporation</td><td>Disabled</td><td>None</td></tr>
<tr><td>Windows Terminal</td><td>Microsoft Corporation</td><td>Disabled</td><td>None</td></tr>
</table>
<b>FIGURE 2-32. Task Manager</b>
</td>
</tr>
</table>

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 3-24*
- *Converting VMware ESXi Virtual Hard Disk Drives on page 3-31*
- *Creating Virtual Machine Images Using Converted Virtual Hard Disk Drives on page 3-38*
- *Configuring Virtual Machine Images on page 3-57*
- *Exporting Virtual Machine Images to OVA Files on page 3-62*

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 3-24*.

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 3-31*.

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 3-38*.

6. Configure the new virtual machine image.

   For details, see *Configuring Virtual Machine Images on page 3-57*.

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

   For details, see *Exporting Virtual Machine Images to OVA Files on page 3-62*.

Required Software

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

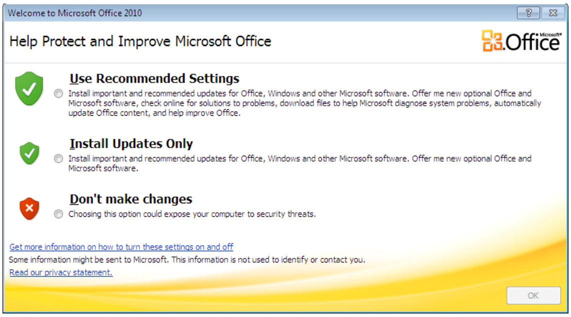
Note

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 21H2 and before, Windows 11 Version 21H2, 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.

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.  Welcome to Microsoft Office 2010 Help Protect and Improve Microsoft Office ○ **Use Recommended Settings** Install important and recommended updates for Office, Windows and other Microsoft software. Offer me new optional Office and Microsoft software, check online for solutions to problems, download files to help Microsoft diagnose system problems, automatically update Office content, and help improve Office. ○ **Install Updates Only** Install important and recommended updates for Office, Windows and other Microsoft software. Offer me new optional Office and Microsoft software. ○ **Don't make changes** Choosing this option could expose your computer to security threats. Get more information on how to turn these settings on and off Some information might be sent to Microsoft. This information is not used to identify or contact you. Read our privacy statement. **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.

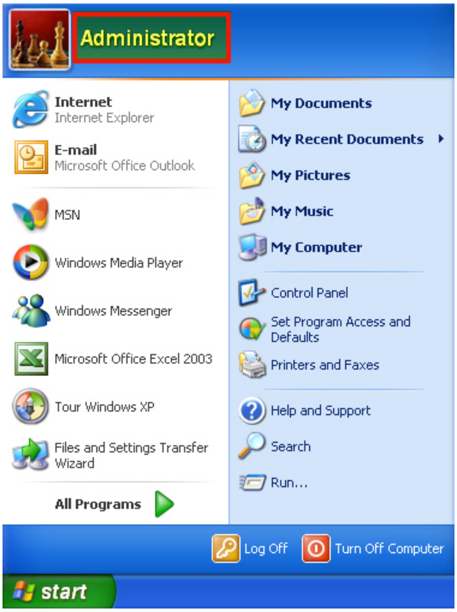
- *Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003) on page 3-8*
- *Modifying the Virtual Machine Environment (All Other Supported Windows Versions) on page 3-10*
- *Uninstalling VMware Tools on page 3-22*

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`** • **`REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows NT\CurrentVersion`**

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.	`\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. **Note** No logon prompt is displayed and the “Administrator” account is automatically used to log on.  Administrator Internet Internet Explorer E-mail Microsoft Office Outlook MSN Windows Media Player Windows Messenger Microsoft Office Excel 2003 Tour Windows XP Files and Settings Transfer Wizard All Programs My Documents My Recent Documents My Pictures My Music My Computer Control Panel Set Program Access and Defaults Printers and Faxes Help and Support Search Run... Log Off Turn Off Computer start **Figure 3-2. Windows XP Administrator Account**

Task	Steps
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`.
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 3-22*.

3. Restart the virtual machine.

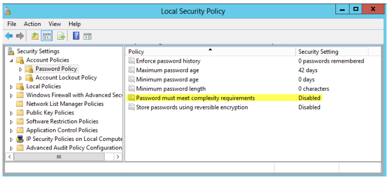
Modifying the Virtual Machine Environment (All Other Supported Windows Versions)

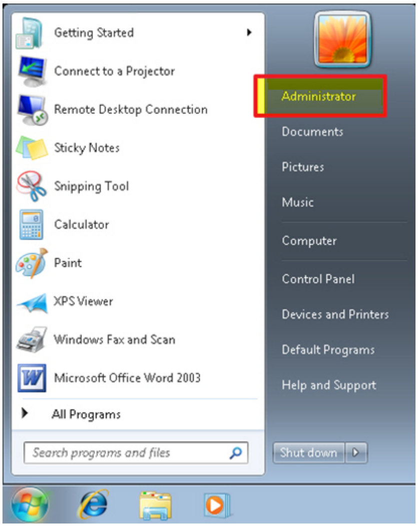
Procedure

1. Open a Command Prompt window (`cmd.exe`) using an account with administrator privileges.

2. Perform the following tasks:

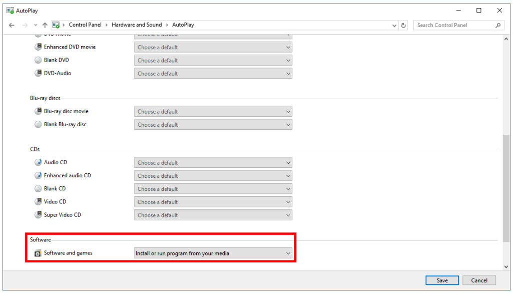
TASK	STEPS
Enable the “Administrator” account.	Type **`net user “Administrator” /active:yes`**.
Set the logon password for the “Administrator” account to “1111”.	Type **`net user "Administrator" 1111`**.
Configure automatic logon from the administrator account. **Note** Each time the image starts, the 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`**

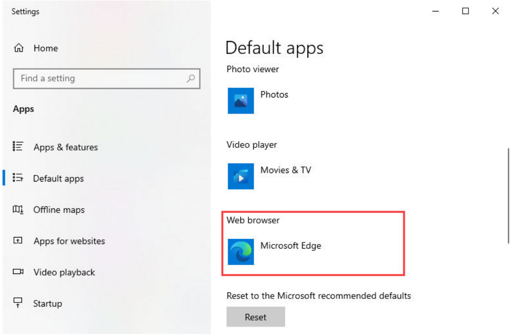
<table>
<tr><th>TASK</th><th>STEPS</th></tr>
<tr><td></td><td>
<b>Note</b>
In Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022, launch the <b>Local Security Policy</b> snap-in (<code>secpol.msc</code>) to disable the <b>Password must meet complexity requirements</b> Local Security Setting.

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
<table>
<tr><th>Policy</th><th>Security Setting</th></tr>
<tr><td>Enforce password history</td><td>0 passwords remembered</td></tr>
<tr><td>Maximum password age</td><td>42 days</td></tr>
<tr><td>Minimum password age</td><td>0 days</td></tr>
<tr><td>Minimum password length</td><td>0 characters</td></tr>
<tr><td>Password must meet complexity requirements</td><td>Disabled</td></tr>
<tr><td>Store passwords using reversible encryption</td><td>Disabled</td></tr>
</table>
<b>FIGURE 3-3. Disable Password must meet complexity requirements</b>
• Restart the image.
</td></tr>
</table>

TASK	STEPS
	No logon prompt is displayed and the “Administrator” account is automatically used to log on.  Getting Started Connect to a Projector Remote Desktop Connection Sticky Notes Snipping Tool Calculator Paint XPS Viewer Windows Fax and Scan Microsoft Office Word 2003 All Programs Search programs and files Administrator Documents Pictures Music Computer Control Panel Devices and Printers Default Programs Help and Support Shut down **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"`**

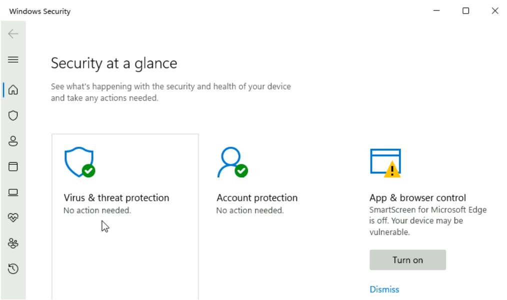
3. Perform the following tasks using the Windows graphical user interface:

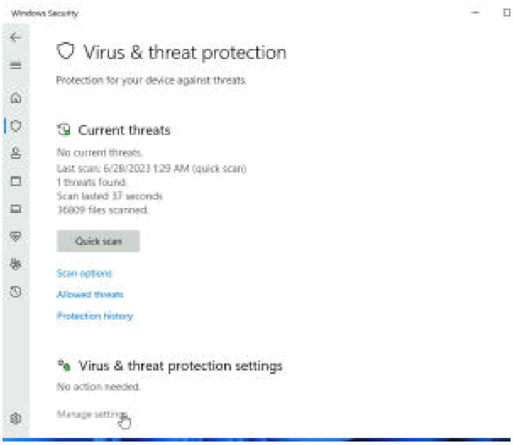
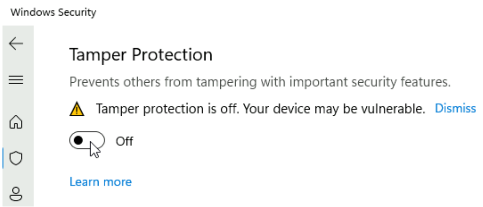
Task	Steps
Configure AutoPlay	a. Open the Windows **Start** menu, type **`Control Panel`** into the search box and press ENTER. b. In the **Control Panel**, go to **Hardware and Sound** > **AutoPlay**.  AutoPlay Control Panel > Hardware and Sound > AutoPlay Search Control Panel Save Cancel Enhanced DVD movie: Choose a default Blank DVD: Choose a default DVD-Audio: Choose a default Blu-ray discs Blu-ray disc movie: Choose a default Blank Blu-ray disc: Choose a default CDs Audio CD: Choose a default Enhanced audio CD: Choose a default Blank CD: Choose a default Video CD: Choose a default Super Video CD: Choose a default Software Software and games: Install or run program from your media **FIGURE 3-5. AutoPlay** c. For **Software and games**, select **Install or run program from your media**. d. Click **Save**.

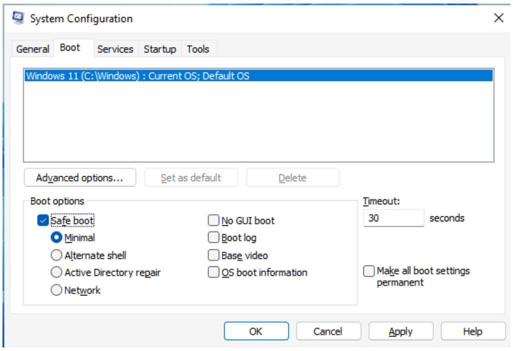
Task	**Steps**
Configure default web browser on Windows 10/11	The Virtual Analyzer supports both Microsoft Edge (Chromium) and Internet Explorer. One of these browsers must be manually set as the default web browser in Windows 10/11 before running the Virtual Analyzer. To configure the default web browser, 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.  Default apps Photo viewer: Photos Video player: Movies & TV Web browser: Microsoft Edge Reset to the Microsoft recommended defaults Settings Home Find a setting Apps Apps & features Default apps Offline maps Apps for websites Video playback Startup Reset **Figure 3-6. Default apps** c. In the **Choose an app** context menu, select **Internet Explorer** or **Microsoft Edge**.

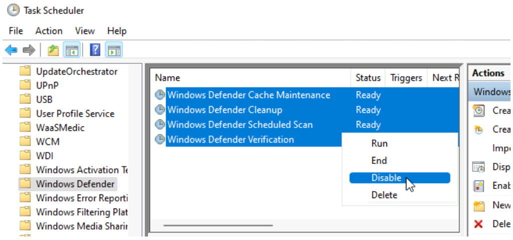
Task	Steps
	d. If the **Before you switch** dialog appears, select **Switch anyway**.
(Optional) Change the display resolution	Trend Micro recommends settings the screen resolution to at least **`1152 x 864`** to avoid triggering the anti-virtual machine functions of some malware. a. Open the Windows **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 3-22*.

4. For Windows 11 21H2, 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**.  Windows Security Security at a glance See what's happening with the security and health of your device and take any actions needed. Virus & threat protection No action needed. Account protection No action needed. App & browser control SmartScreen for Microsoft Edge is off. Your device may be vulnerable. **FIGURE 3-7. Windows Security**

TASK	STEPS
	c. Under **Virus & threat protection**, click **Manage settings**.  Windows Security Virus & threat protection Protection for your device against threats. Current threats No current threats. Last scan: 6/28/2023 1:29 AM (quick scan) 1 threats found. Scan lasted 37 seconds 36809 files scanned. Quick scan Scan options Allowed threats Protection history Virus & threat protection settings No action needed. **FIGURE 3-8. Virus & Threat Protection** d. Turn **Tamper Protection** off.  Windows Security Tamper Protection Prevents others from tampering with important security features. ⚠ Tamper protection is off. Your device may be vulnerable. 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**. System Configuration General | Boot | Services | Startup | Tools Windows 11 (C:\Windows) : Current OS; Default OS Advanced options... | Set as default | Delete Boot options ☑ Safe boot ● Minimal ○ Alternate shell ○ Active Directory repair ○ Network ☐ No GUI boot ☐ Boot log ☐ Base video ☐ OS boot information Timeout: 30 seconds ☐ Make all boot settings permanent OK | Cancel | Apply | Help **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\CurrentControlSet\Services\WdFilter" /v Start /t REG_DWORD /d 4 /f`**

Task	Steps
	- `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**. k. Disable all Windows Defender tasks.  Name / Status Windows Defender Cache Maintenance / Ready Windows Defender Cleanup / Ready Windows Defender Scheduled Scan / Ready Windows Defender Verification Task Scheduler File Action View Help UpdateOrchestrator UPnP USB User Profile Service WaaSMedic WCM WDI Windows Activation Te Windows Defender Windows Error Reporti Windows Filtering Plat Windows Media Sharir Triggers Next R Run End Disable Delete Actions Windows Crea Crea Impo Disp Enab New Dele **FIGURE 3-11. Task Scheduler**

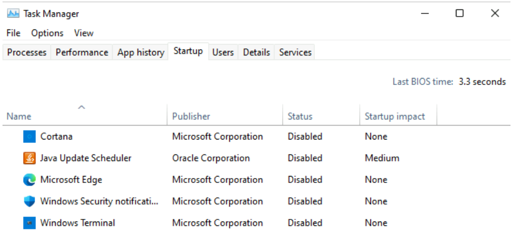
<table>
<tr><th>TASK</th><th>STEPS</th></tr>
<tr><td>(Optional) Disable startup applications</td><td>

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



Last BIOS time: 3.3 seconds

<table>
<tr><th>Name</th><th>Publisher</th><th>Status</th><th>Startup impact</th></tr>
<tr><td>Cortana</td><td>Microsoft Corporation</td><td>Disabled</td><td>None</td></tr>
<tr><td>Java Update Scheduler</td><td>Oracle Corporation</td><td>Disabled</td><td>Medium</td></tr>
<tr><td>Microsoft Edge</td><td>Microsoft Corporation</td><td>Disabled</td><td>None</td></tr>
<tr><td>Windows Security notificati...</td><td>Microsoft Corporation</td><td>Disabled</td><td>None</td></tr>
<tr><td>Windows Terminal</td><td>Microsoft Corporation</td><td>Disabled</td><td>None</td></tr>
</table>

FIGURE 3-12. Task Manager

</td></tr>
</table>

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

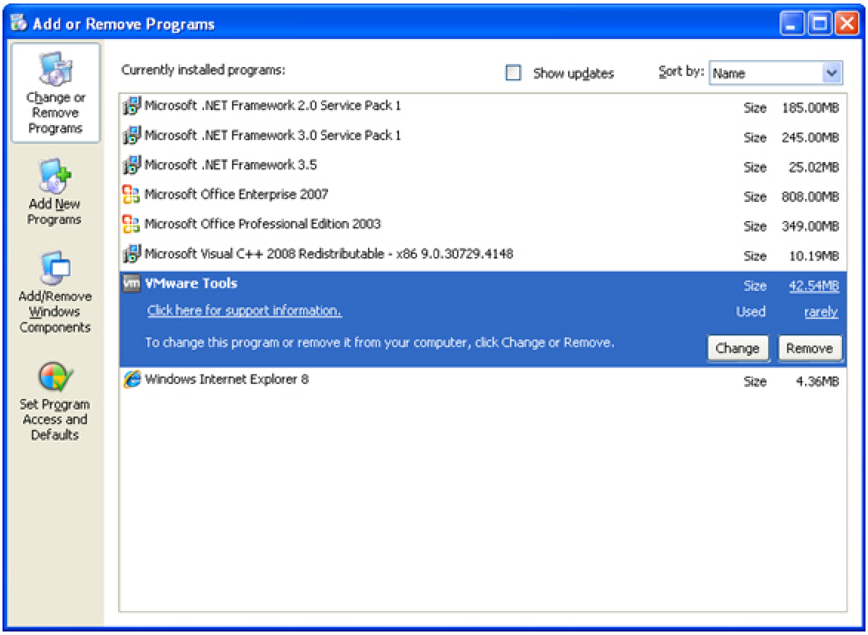
1. Go to **Start** > **Control Panel**.

   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** .

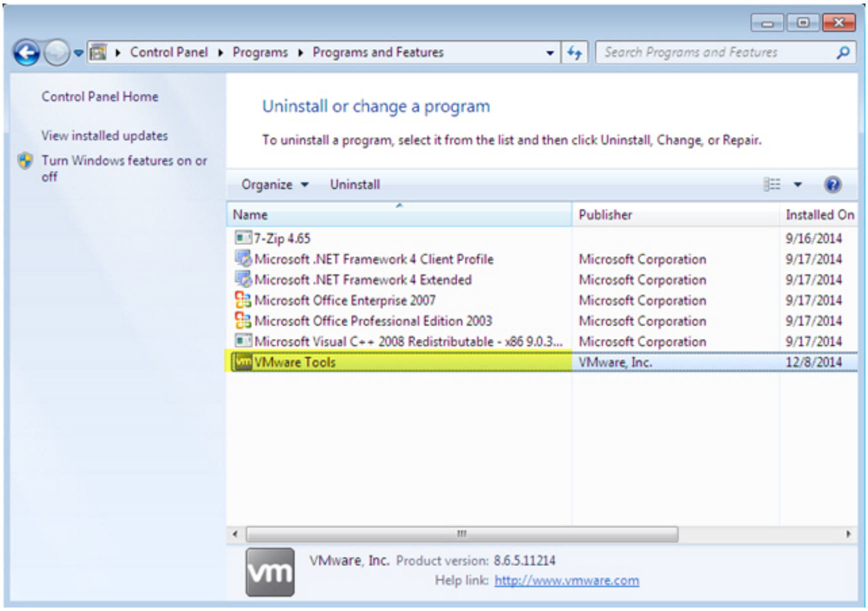
    A list of installed programs appears.



Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Currently installed programs:
□ Show updates
Sort by: Name
Change
Remove

Microsoft .NET Framework 2.0 Service Pack 1	Size	185.00MB
Microsoft .NET Framework 3.0 Service Pack 1	Size	245.00MB
Microsoft .NET Framework 3.5	Size	25.02MB
Microsoft Office Enterprise 2007	Size	808.00MB
Microsoft Office Professional Edition 2003	Size	349.00MB
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	Size	10.19MB
VMware Tools	Size	42.54MB
Click here for support information.	Used	rarely
To change this program or remove it from your computer, click Change or Remove.		
Windows Internet Explorer 8	Size	4.36MB

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


Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Uninstall

Uninstall or change a program

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

Name	Publisher	Installed On
7-Zip 4.65		9/16/2014
Microsoft .NET Framework 4 Client Profile	Microsoft Corporation	9/17/2014
Microsoft .NET Framework 4 Extended	Microsoft Corporation	9/17/2014
Microsoft Office Enterprise 2007	Microsoft Corporation	9/17/2014
Microsoft Office Professional Edition 2003	Microsoft Corporation	9/17/2014
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...	Microsoft Corporation	9/17/2014
VMware Tools	VMware, Inc.	12/8/2014

VMware, Inc. Product version: 8.6.5.11214
Help link: http://www.vmware.com

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 3-25*
- *Exporting Virtual Machine Images on VMware ESXi on page 3-27*

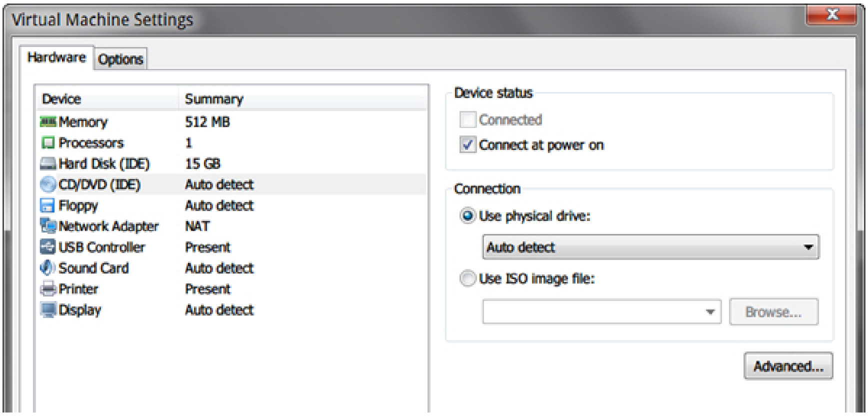
- *Converting VMware ESXi Virtual Hard Disk Drives on page 3-31*

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.



Device	Summary
Memory	512 MB
Processors	1
Hard Disk (IDE)	15 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Connection

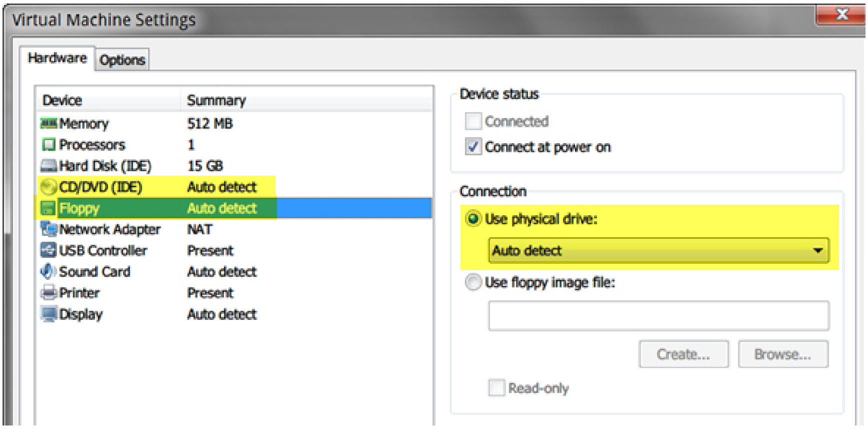
● Use physical drive:

Auto detect

○ Use ISO image file:

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**.



Device	Summary
Memory	512 MB
Processors	1
Hard Disk (IDE)	15 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☐ Connected

☑ Connect at power on

Connection

● Use physical drive:

Auto detect

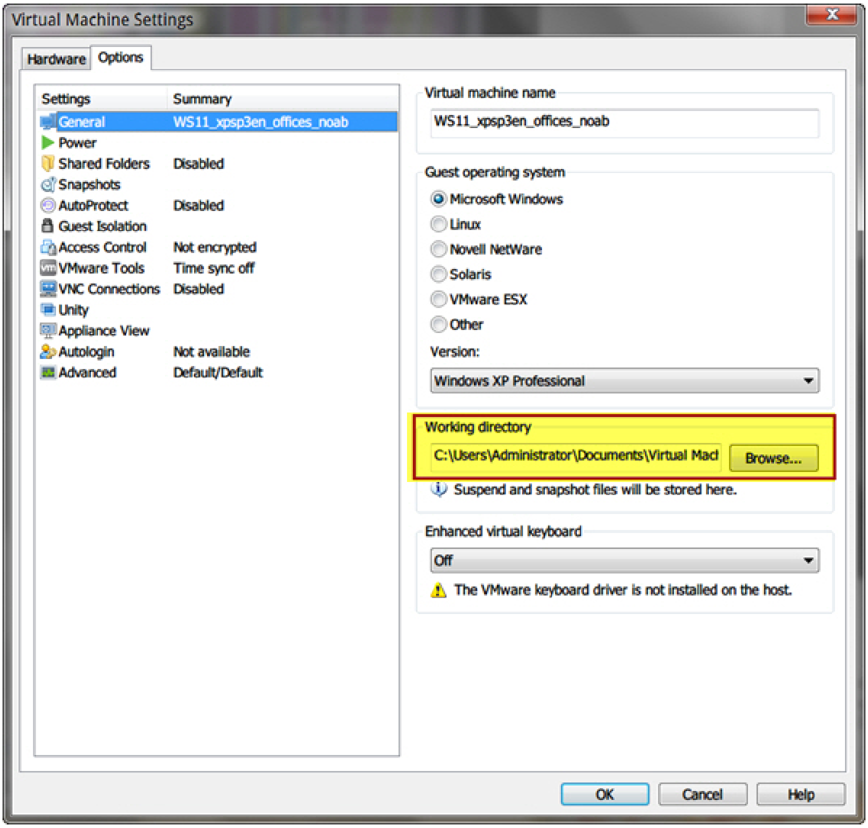
○ Use floppy image file:

☐ Read-only

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`).



Settings	Summary
General	WS11_xpsp3en_offices_noab
Power	
Shared Folders	Disabled
Snapshots	
AutoProtect	Disabled
Guest Isolation	
Access Control	Not encrypted
VMware Tools	Time sync off
VNC Connections	Disabled
Unity	
Appliance View	
Autologin	Not available
Advanced	Default/Default

Virtual machine name: WS11_xpsp3en_offices_noab

Guest operating system

● Microsoft Windows
○ Linux
○ Novell NetWare
○ Solaris
○ VMware ESX
○ Other

Version: Windows XP Professional

Working directory: C:\Users\Administrator\Documents\Virtual Macl

Suspend and snapshot files will be stored here.

Enhanced virtual keyboard: Off

The VMware keyboard driver is not installed on the host.

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**.

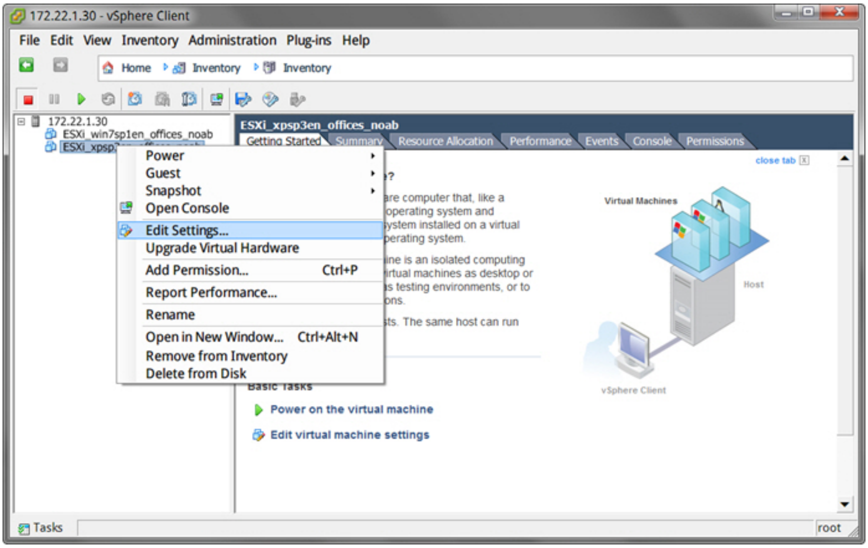
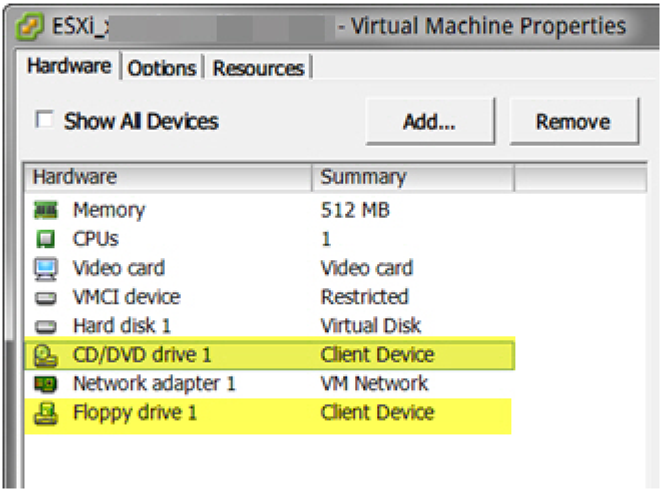


FIGURE 3-18. Edit Settings

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**

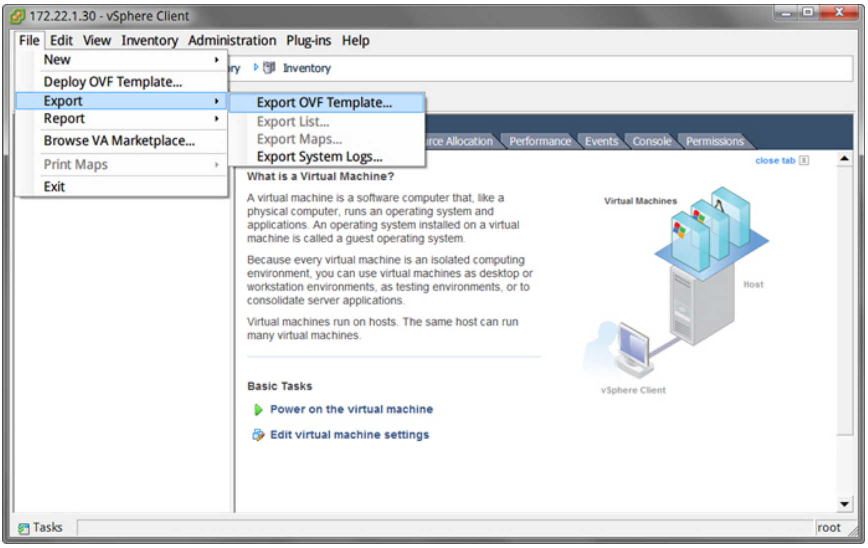


ESXi_[redacted] - Virtual Machine Properties

Hardware	Summary
Memory	512 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk
CD/DVD drive 1	Client Device
Network adapter 1	VM Network
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**.



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

Power on the virtual machine

Edit virtual machine settings

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 3-31*
- *Using QEMU on page 3-37*

Using VMware vCenter Converter Standalone

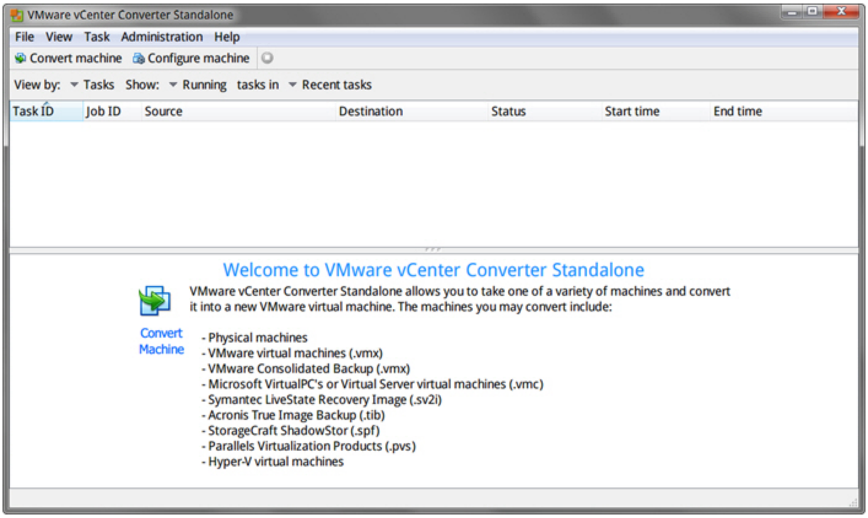
Procedure

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**.


VMware vCenter Converter Standalone
File View Task Administration Help
Convert machine
Configure machine
View by: Tasks Show: Running tasks in Recent tasks
Task ID
Job ID
Source
Destination
Status
Start time
End time
Convert Machine

Welcome to VMware vCenter Converter Standalone

VMware vCenter Converter Standalone allows you to take one of a variety of machines and convert it into a new VMware virtual machine. The machines you may convert include:

- Physical machines
- VMware virtual machines (.vmx)
- VMware Consolidated Backup (.vmx)
- Microsoft VirtualPC's or Virtual Server virtual machines (.vmc)
- Symantec LiveState Recovery Image (.sv2i)
- Acronis True Image Backup (.tib)
- StorageCraft ShadowStor (.spf)
- Parallels Virtualization Products (.pvs)
- Hyper-V virtual machines

FIGURE 3-21. VMware vCenter Converter Standalone

The **Conversion** window opens.

3. On the **Source System** screen, configure the following:

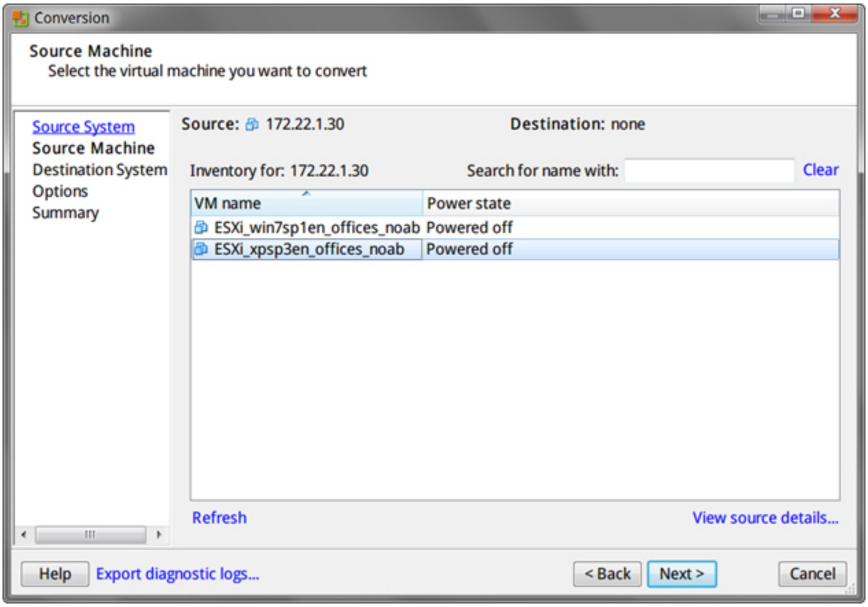
   a. **Select source type**: Select **VMware Infrastructure virtual machine**.

   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.



Conversion

Source Machine

Select the virtual machine you want to convert

Source: 172.22.1.30

Destination: none

Inventory for: 172.22.1.30

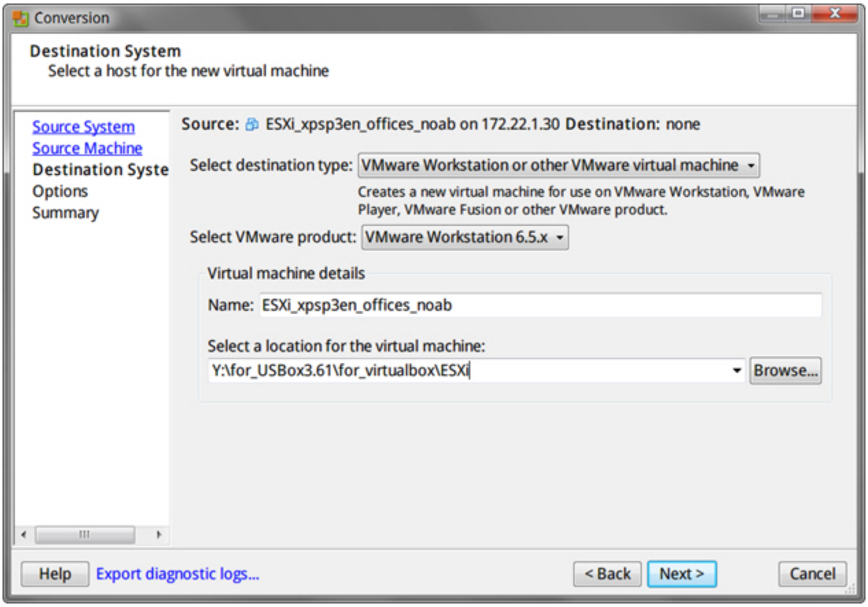
Search for name with:

VM name	Power state
ESXi_win7sp1en_offices_noab	Powered off
ESXi_xpsp3en_offices_noab	Powered off

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.


Conversion

Destination System
Select a host for the new virtual machine

Source: ESXi_xpsp3en_offices_noab on 172.22.1.30 Destination: none

Select destination type: VMware Workstation or other VMware virtual machine

Creates a new virtual machine for use on VMware Workstation, VMware Player, VMware Fusion or other VMware product.

Select VMware product: VMware Workstation 6.5.x

Virtual machine details

Name: ESXi_xpsp3en_offices_noab

Select a location for the virtual machine:
Y:\for_USBox3.61\for_virtualbox\ESXi

FIGURE 3-23. Conversion > Destination System

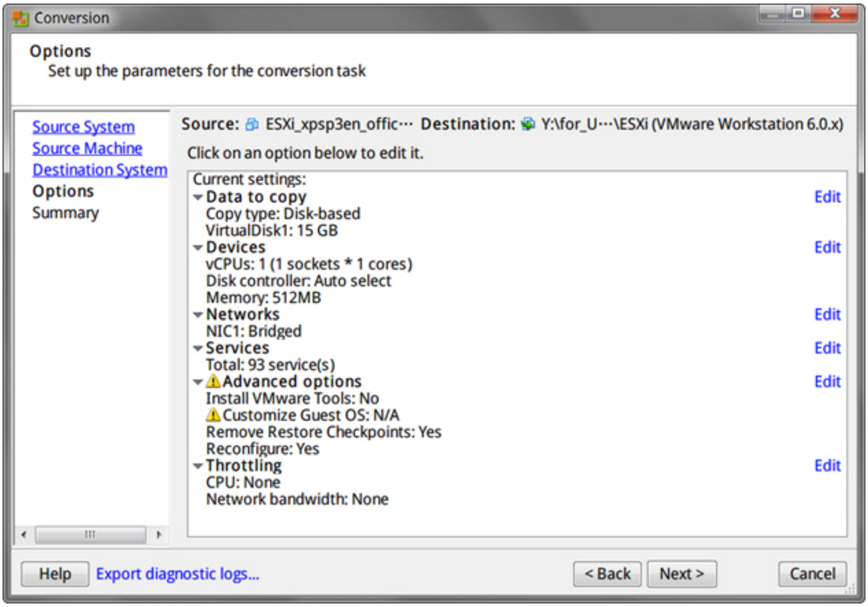
6. Configure the following and then click **Next**.

   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.



Conversion

Options

Set up the parameters for the conversion task

Source: ESXi_xpsp3en_offic··· Destination: Y:\for_U···\ESXi (VMware Workstation 6.0.x)

Click on an option below to edit it.

Current settings:

- Data to copy — Edit
  - Copy type: Disk-based
  - VirtualDisk1: 15 GB
- Devices — Edit
  - vCPUs: 1 (1 sockets * 1 cores)
  - Disk controller: Auto select
  - Memory: 512MB
- Networks — Edit
  - NIC1: Bridged
- Services — Edit
  - Total: 93 service(s)
- ⚠Advanced options — Edit
  - Install VMware Tools: No
  - ⚠Customize Guest OS: N/A
  - Remove Restore Checkpoints: Yes
  - Reconfigure: Yes
- Throttling — Edit
  - CPU: None
  - Network bandwidth: None

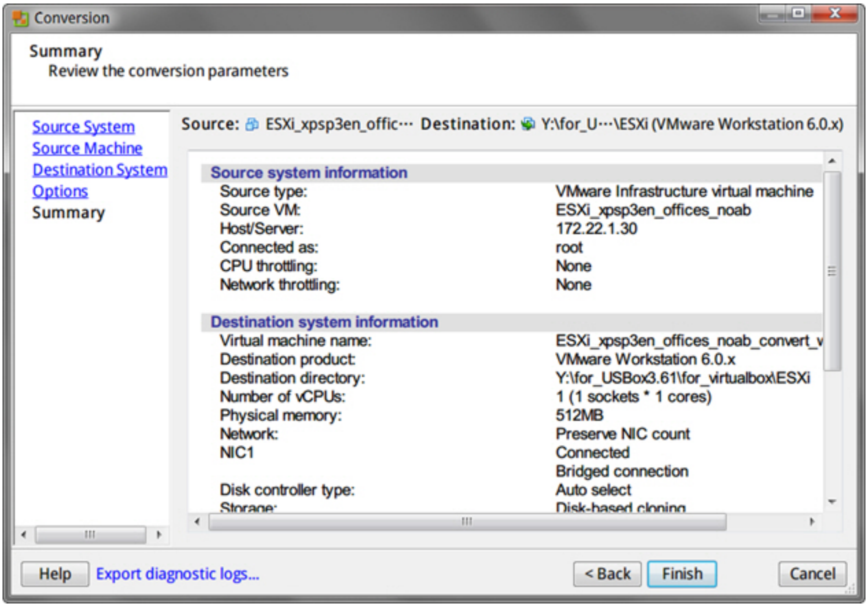
FIGURE 3-24. Conversion > Options

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

Important

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

The **Summary** screen appears.



Summary

Review the conversion parameters

Source: ESXi_xpsp3en_offic··· **Destination:** Y:\for_U···\ESXi (VMware Workstation 6.0.x)

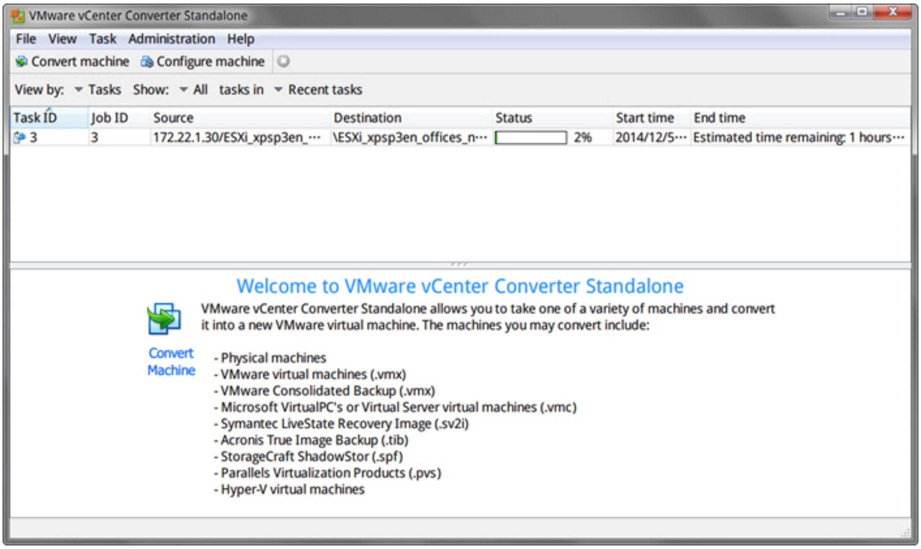
Source system information	
Source type:	VMware Infrastructure virtual machine
Source VM:	ESXi_xpsp3en_offices_noab
Host/Server:	172.22.1.30
Connected as:	root
CPU throttling:	None
Network throttling:	None

Destination system information	
Virtual machine name:	ESXi_xpsp3en_offices_noab_convert_v
Destination product:	VMware Workstation 6.0.x
Destination directory:	Y:\for_USBox3.61\for_virtualbox\ESXi
Number of vCPUs:	1 (1 sockets * 1 cores)
Physical memory:	512MB
Network:	Preserve NIC count
NIC1	Connected Bridged connection
Disk controller type:	Auto select
Storage:	Disk-based cloning

FIGURE 3-25. Conversion > Summary

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

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


VMware vCenter Converter Standalone
File View Task Administration Help
Convert machine
Configure machine
View by: Tasks Show: All tasks in Recent tasks
Convert Machine

Task ID	Job ID	Source	Destination	Status	Start time	End time
3	3	172.22.1.30/ESXi_xpsp3en_···	\ESXi_xpsp3en_offices_n···	2%	2014/12/5···	Estimated time remaining: 1 hours···

Welcome to VMware vCenter Converter Standalone

VMware vCenter Converter Standalone allows you to take one of a variety of machines and convert it into a new VMware virtual machine. The machines you may convert include:

- Physical machines
- VMware virtual machines (.vmx)
- VMware Consolidated Backup (.vmx)
- Microsoft VirtualPC's or Virtual Server virtual machines (.vmc)
- Symantec LiveState Recovery Image (.sv2i)
- Acronis True Image Backup (.tib)
- StorageCraft ShadowStor (.spf)
- Parallels Virtualization Products (.pvs)
- Hyper-V virtual machines

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 3-39*

Downloading and Installing VirtualBox

Procedure

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

Note

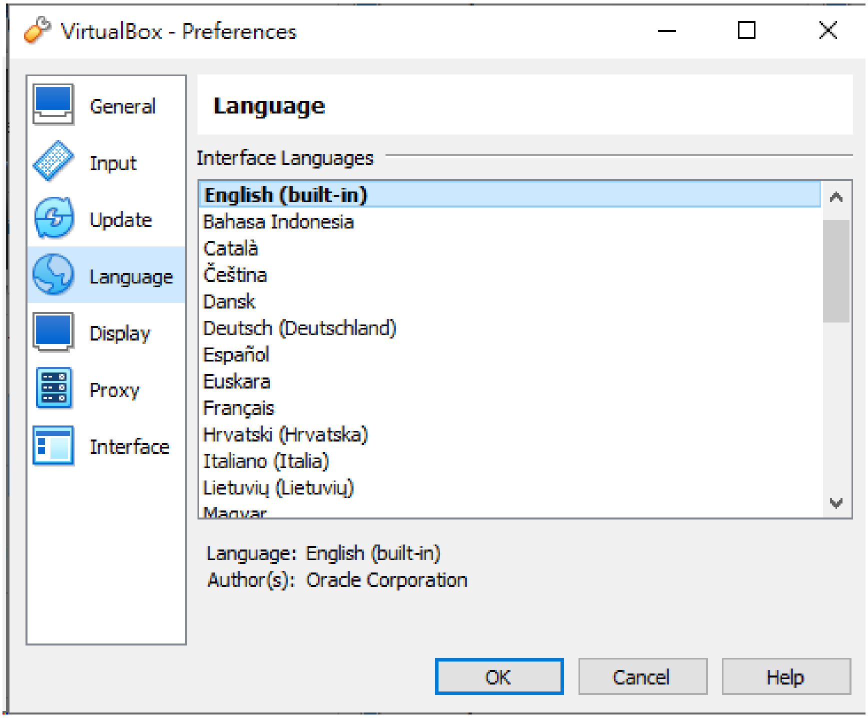
The VirtualBox Open Source Edition is licensed under the GPL V2. The full text of the license is available at http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.

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**.



Language: English (built-in)
Author(s): Oracle Corporation

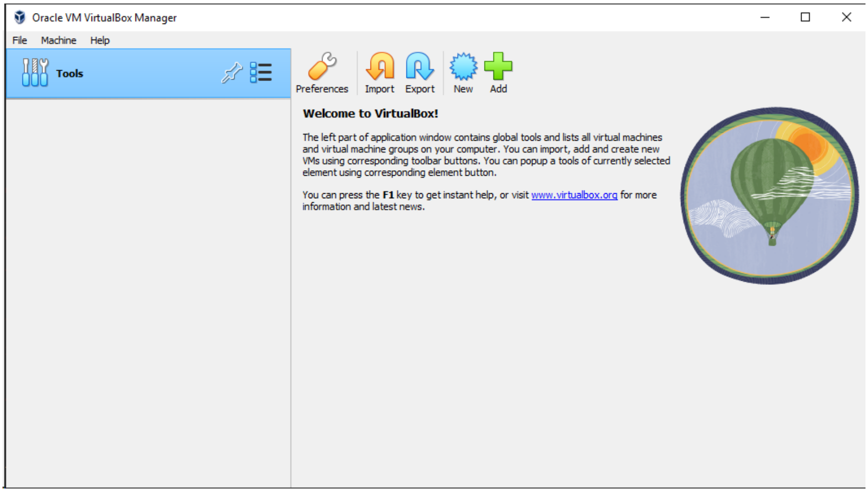
FIGURE 3-27. Language Settings

Creating Virtual Machine Images Using VirtualBox

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

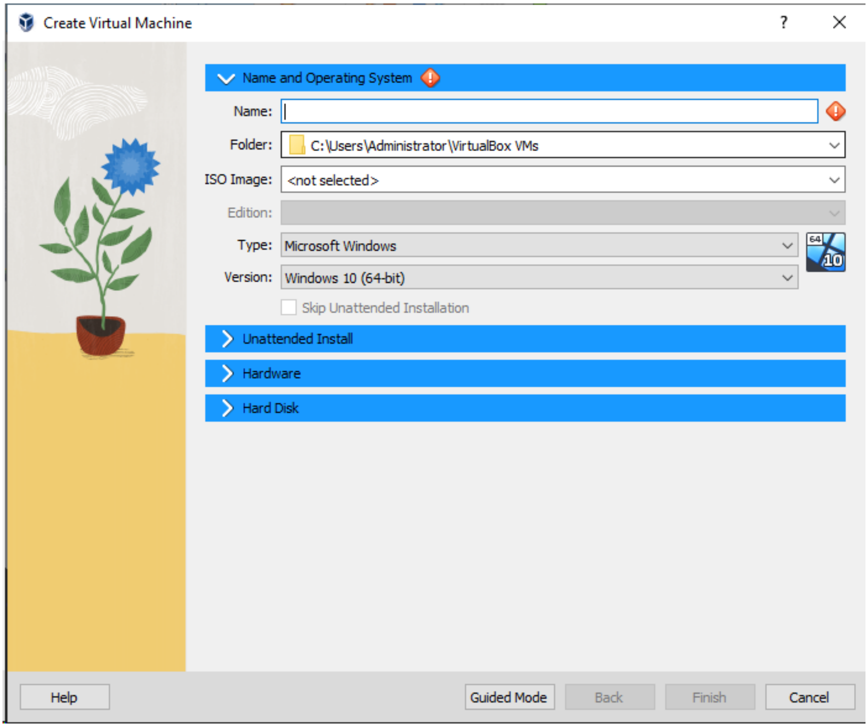
FIGURE 3-28. VirtualBox Manager

2. Click **New**.

   The **Create Virtual Machine** window opens.

3. Click **Expert Mode**.

The Create Virtual Machine wizard enters Expert Mode.


Create Virtual Machine

Name and Operating System

Name:

Folder: C:\Users\Administrator\VirtualBox VMs

ISO Image: <not selected>

Edition:

Type: Microsoft Windows

Version: Windows 10 (64-bit)

□ Skip Unattended Installation

Unattended Install

Hardware

Hard Disk

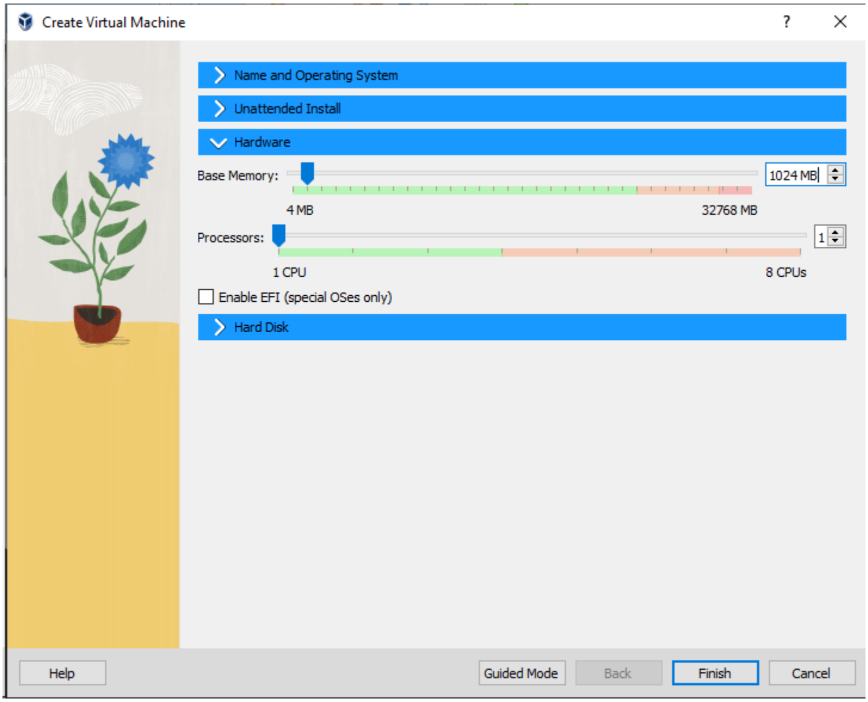
FIGURE 3-29. Create Virtual Machine - Expert Mode

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.



Create Virtual Machine

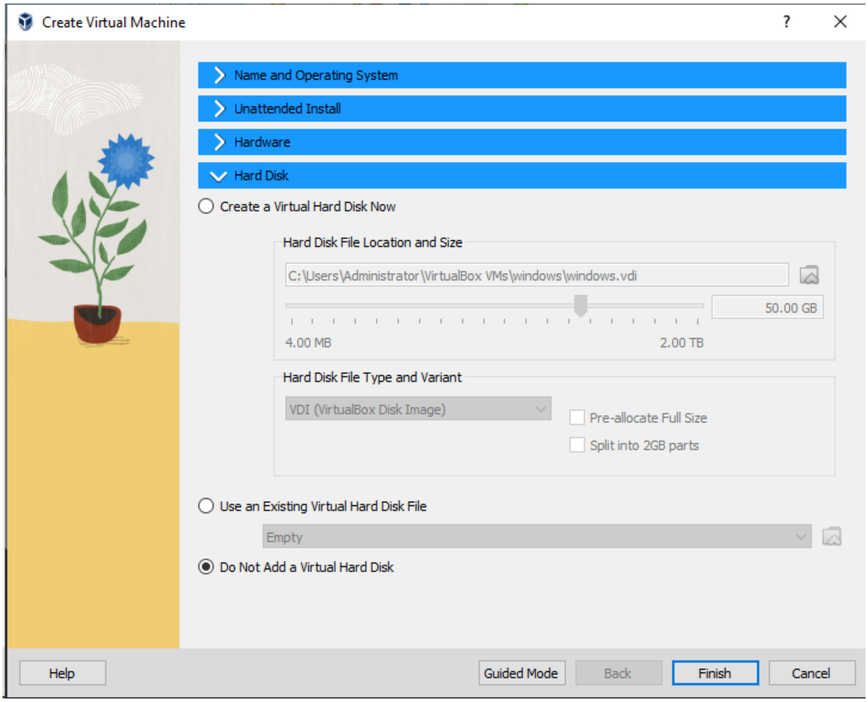
Base Memory: 1024 MB

Processors: 1

□ Enable EFI (special OSes only)

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.



Create Virtual Machine

Name and Operating System

Unattended Install

Hardware

Hard Disk

○ Create a Virtual Hard Disk Now

Hard Disk File Location and Size

C:\Users\Administrator\VirtualBox VMs\windows\windows.vdi

50.00 GB

4.00 MB

2.00 TB

Hard Disk File Type and Variant

VDI (VirtualBox Disk Image)

□ Pre-allocate Full Size

□ Split into 2GB parts

○ Use an Existing Virtual Hard Disk File

Empty

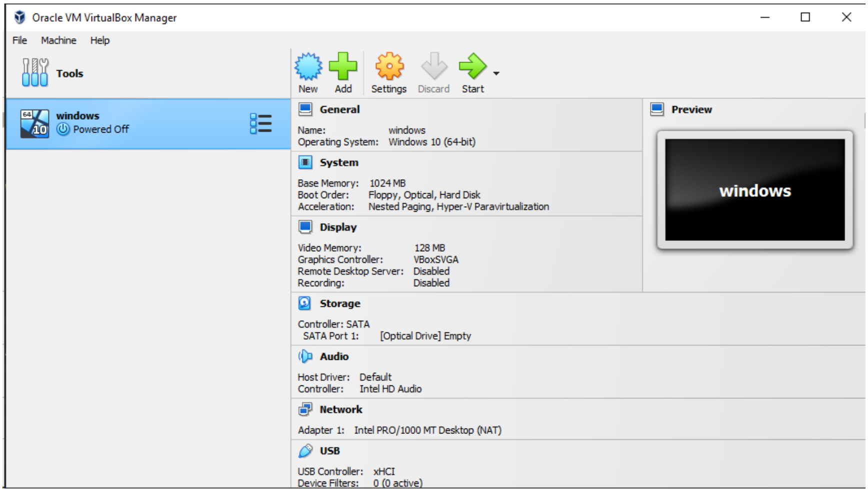
● Do Not Add a Virtual Hard Disk

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.



windows
Powered Off

General
Name: windows
Operating System: Windows 10 (64-bit)

System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage
Controller: SATA
SATA Port 1: [Optical Drive] Empty

Audio
Host Driver: Default
Controller: Intel HD Audio

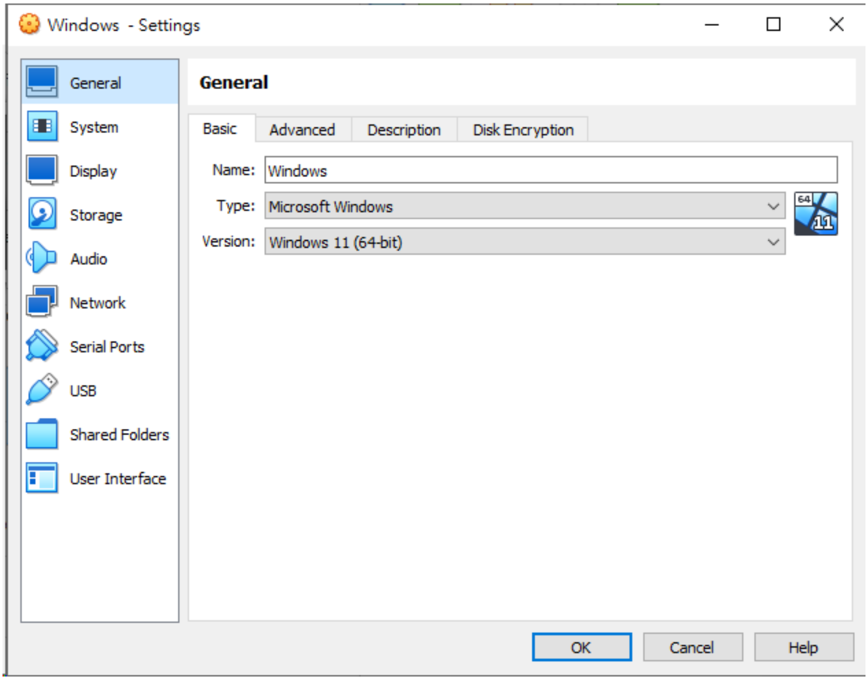
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller: xHCI
Device Filters: 0 (0 active)

FIGURE 3-32. Newly-created Virtual Machine

11. Click **Settings**.

The **Settings** window opens.



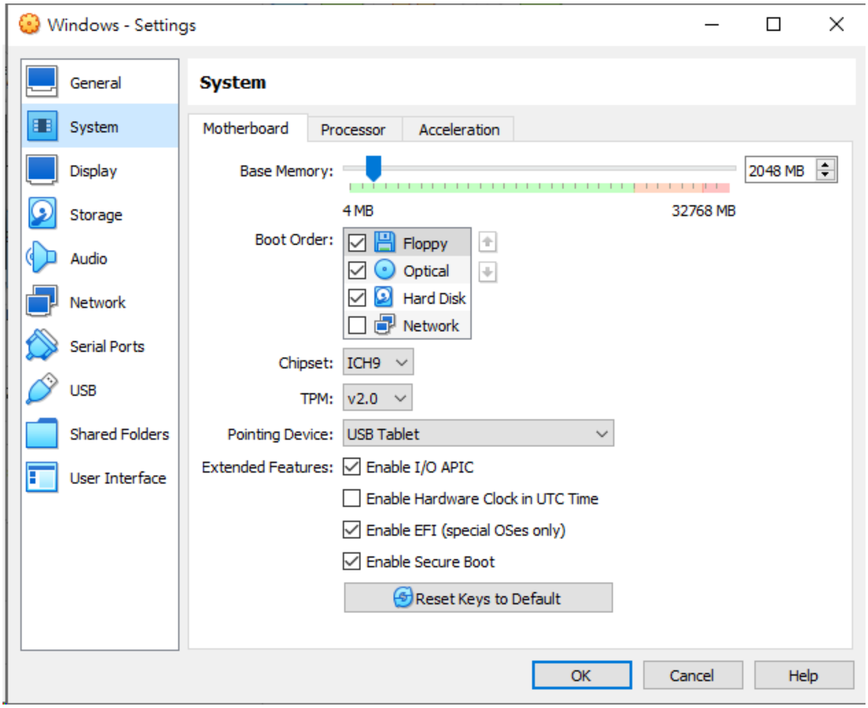
Name: Windows

Type: Microsoft Windows

Version: Windows 11 (64-bit)

FIGURE 3-33. VirtualBox Settings

12. Go to **System**.



System

Base Memory: 2048 MB (4 MB – 32768 MB)

Boot Order:

- ☑ Floppy
- ☑ Optical
- ☑ Hard Disk
- ☐ Network

Chipset: ICH9

TPM: v2.0

Pointing Device: USB Tablet

Extended Features:

- ☑ Enable I/O APIC
- ☐ Enable Hardware Clock in UTC Time
- ☑ Enable EFI (special OSes only)
- ☑ Enable Secure Boot

Reset Keys to Default

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

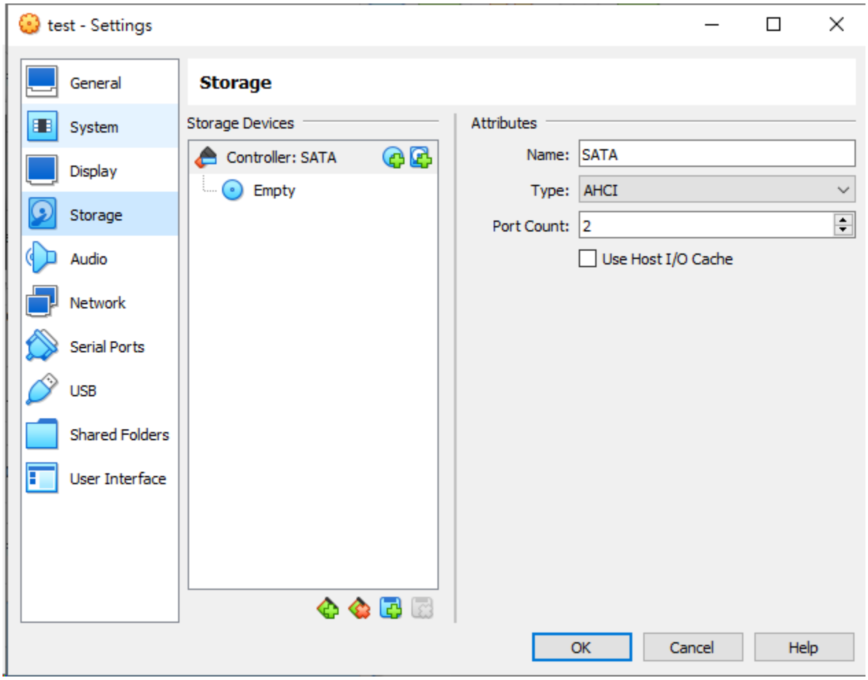
14. On the **Processor** tab, select **Enable PAE/NX**.
15. On the **Acceleration** tab, select **Enable Nested Paging**.

    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**.



Storage

Storage Devices

- Controller: SATA
  - Empty

Attributes

Name: SATA

Type: AHCI

Port Count: 2

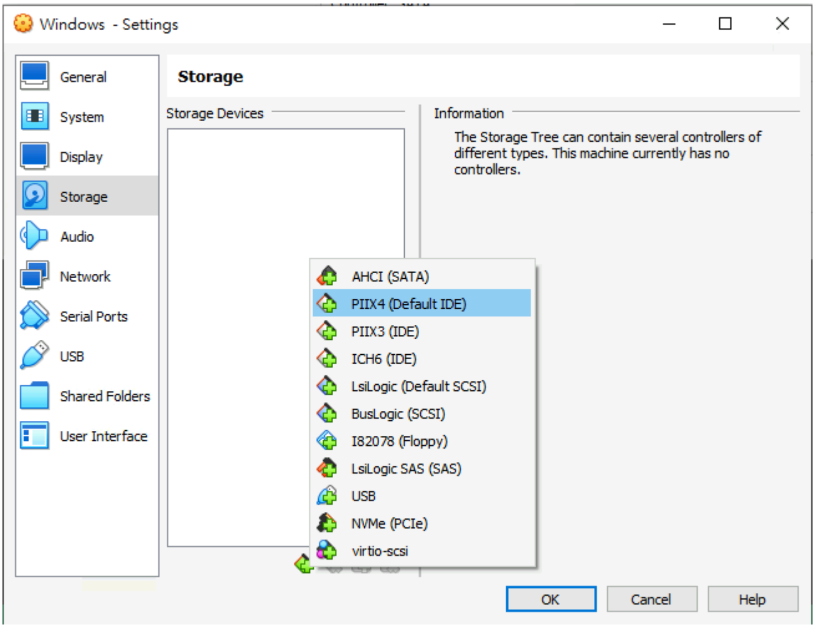
□ Use Host I/O Cache

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)**.

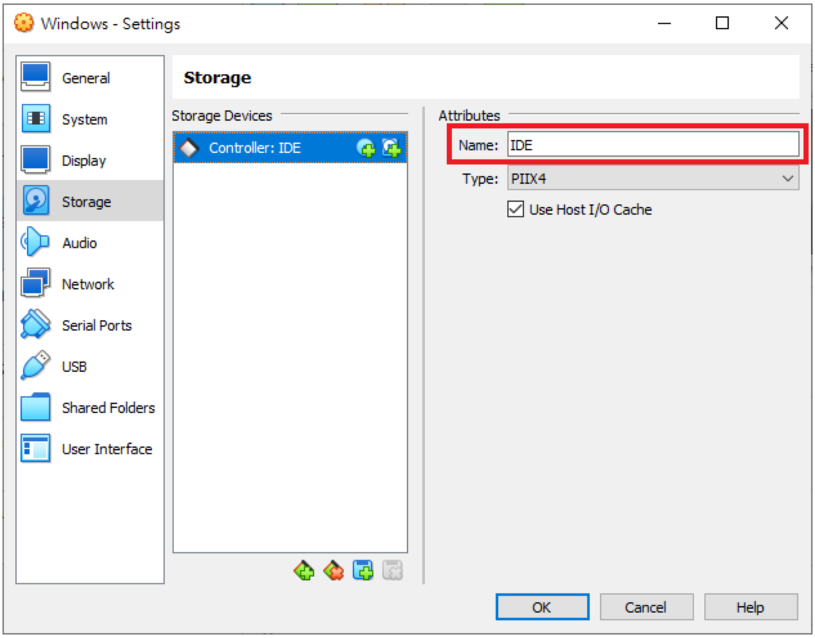


The Storage Tree can contain several controllers of different types. This machine currently has no controllers.

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`**.



Name: IDE

Type: PIIX4

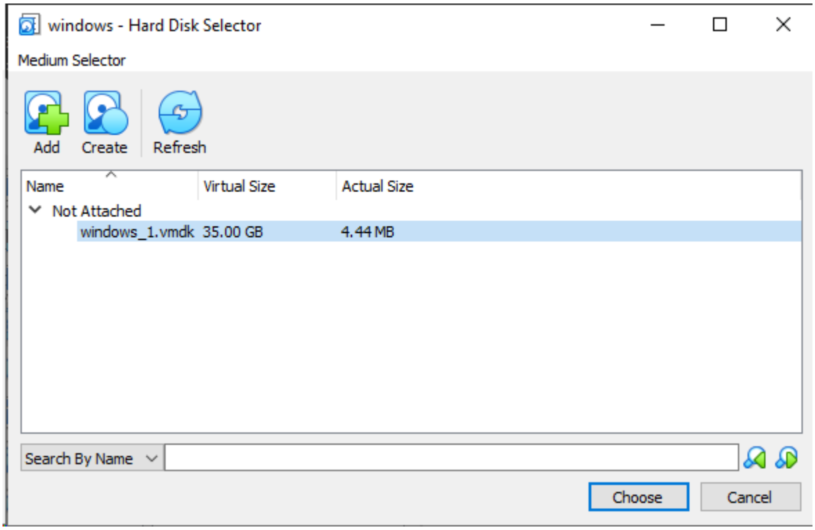
☑ Use Host I/O Cache

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.



Name	Virtual Size	Actual Size
Not Attached		
windows_1.vmdk	35.00 GB	4.44 MB

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**.

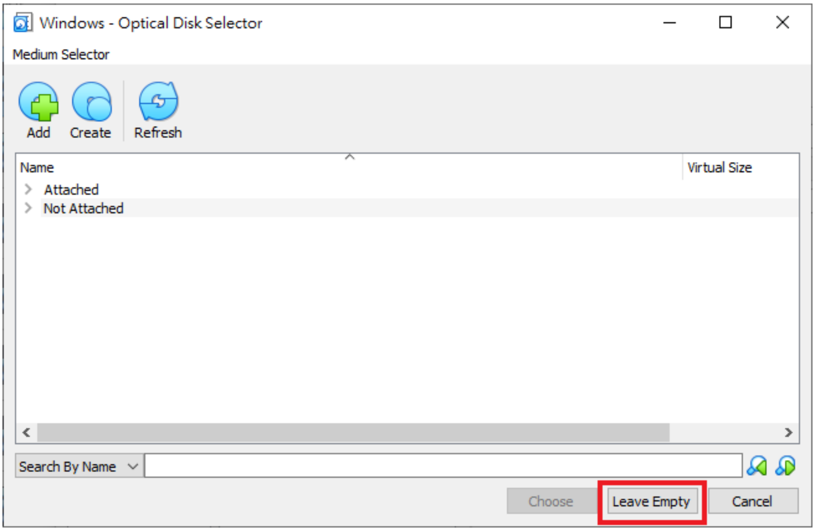
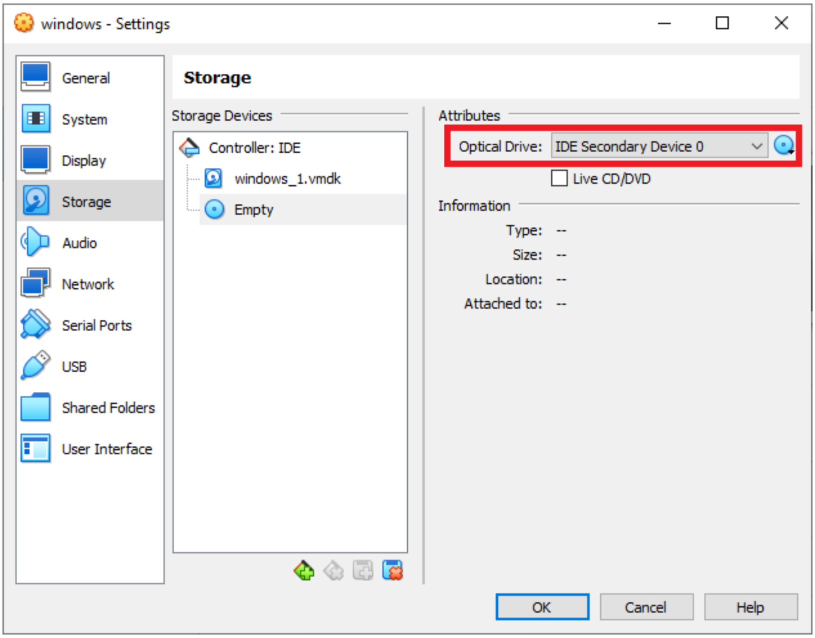


FIGURE 3-39. Optical Disk Selector

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



Storage

Storage Devices

Controller: IDE
windows_1.vmdk
Empty

Attributes

Optical Drive: IDE Secondary Device 0

□ Live CD/DVD

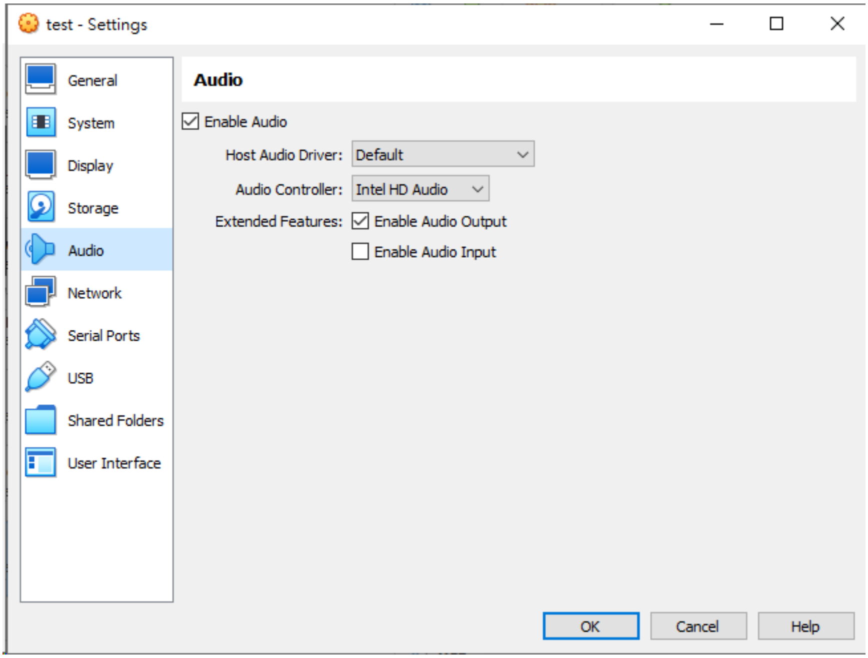
Information

Type: --
Size: --
Location: --
Attached to: --

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.



Audio

☑ Enable Audio

Host Audio Driver: Default

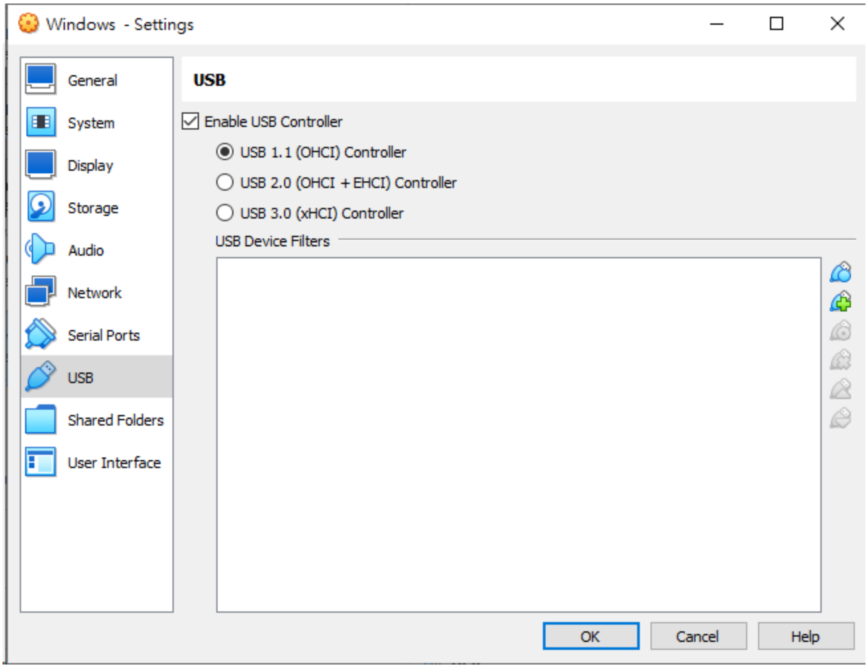
Audio Controller: Intel HD Audio

Extended Features: ☑ Enable Audio Output

□ Enable Audio Input

FIGURE 3-41. Audio Options Settings

20. Go to **USB**.



USB

☑ Enable USB Controller

● USB 1.1 (OHCI) Controller

○ USB 2.0 (OHCI + EHCI) Controller

○ USB 3.0 (xHCI) Controller

USB Device Filters

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.

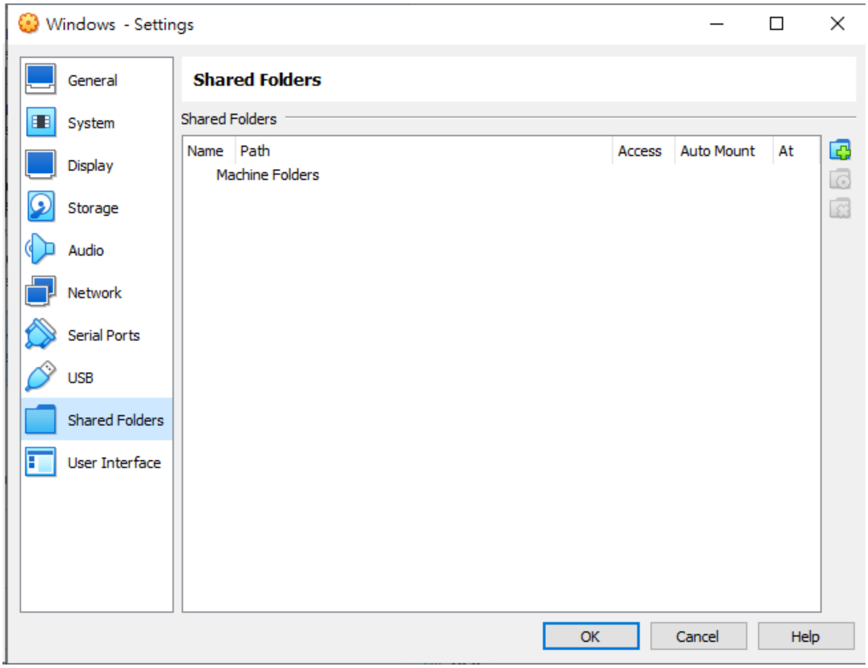
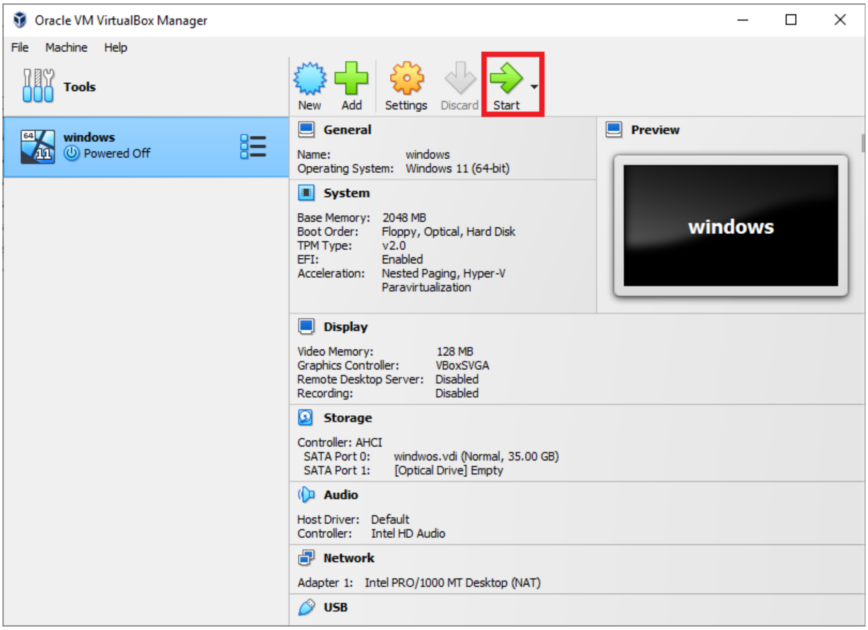


FIGURE 3-43. Shared Folders Settings

24. Click **OK**.

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



windows
Powered Off

General

Name: windows
Operating System: Windows 11 (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
TPM Type: v2.0
EFI: Enabled
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: AHCI
SATA Port 0: windwos.vdi (Normal, 35.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Default
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

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 3-58*
- *Configuring Virtual Machine Images (All Other Supported Windows Versions) on page 3-60*

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.

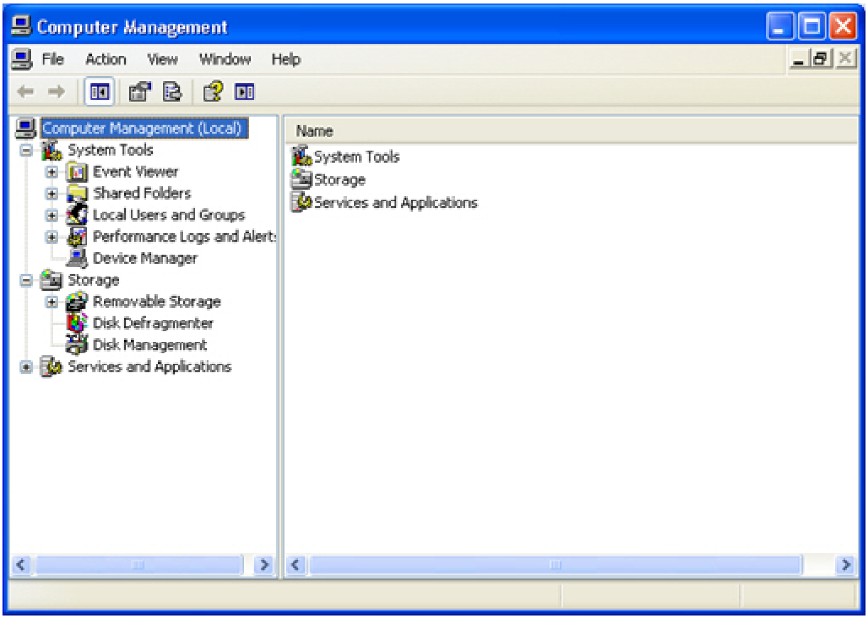
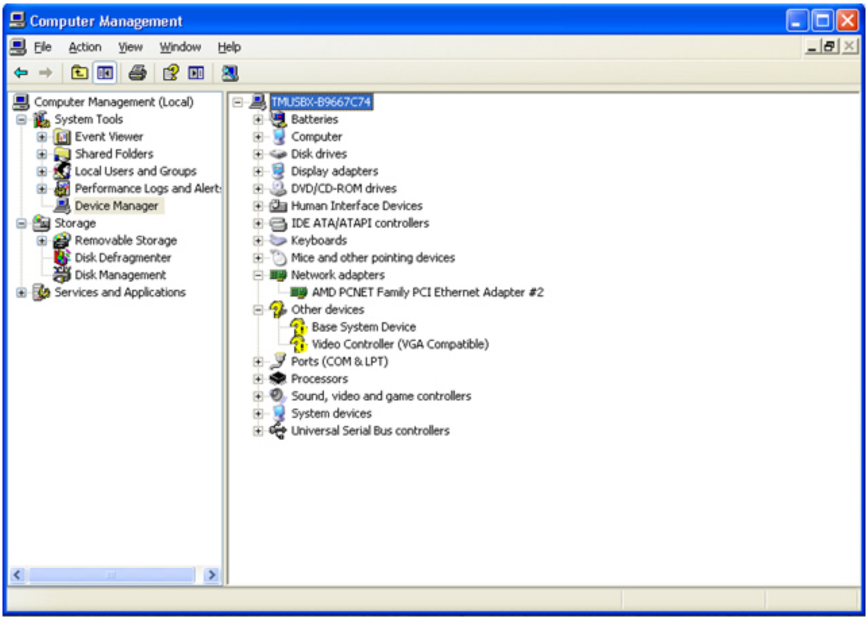


FIGURE 3-45. Computer Management

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

A list of devices appears.



- Computer Management (Local)
  - System Tools
    - Event Viewer
    - Shared Folders
    - Local Users and Groups
    - Performance Logs and Alert:
    - Device Manager
  - Storage
    - Removable Storage
    - Disk Defragmenter
    - Disk Management
  - Services and Applications

- TMUSBX-B9667C74
  - Batteries
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Network adapters
    - AMD PCNET Family PCI Ethernet Adapter #2
  - Other devices
    - Base System Device
    - Video Controller (VGA Compatible)
  - Ports (COM & LPT)
  - Processors
  - Sound, video and game controllers
  - System devices
  - Universal Serial Bus controllers

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.

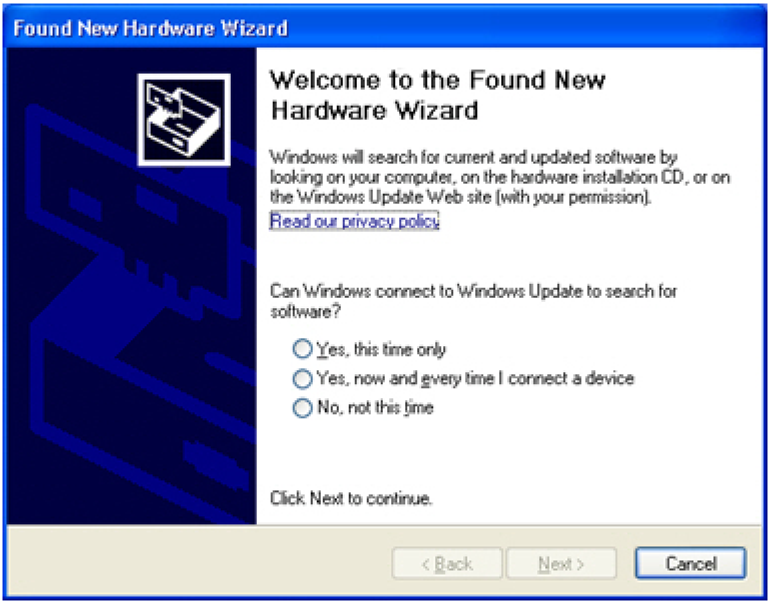
5. Disable the **Found New Hardware Wizard** by typing the following commands:

   - 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\PlugPlay\Parameters" /v SuppressUI /t
REG_DWORD /d 1 /f
```



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Read our privacy policy

Can Windows connect to Windows Update to search for software?

○ Yes, this time only

○ Yes, now and every time I connect a device

○ No, not this time

Click Next to continue.

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.

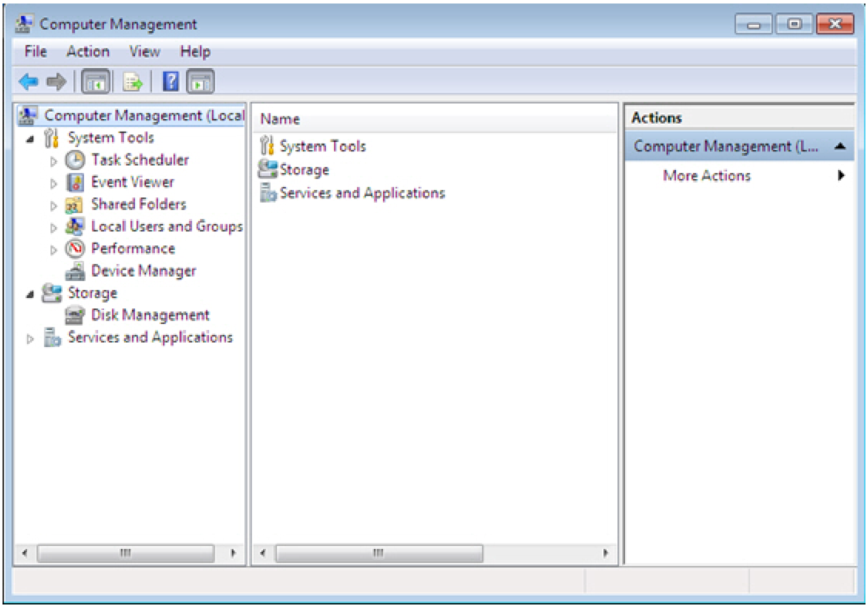


FIGURE 3-48. Computer Management

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

A list of devices appears.

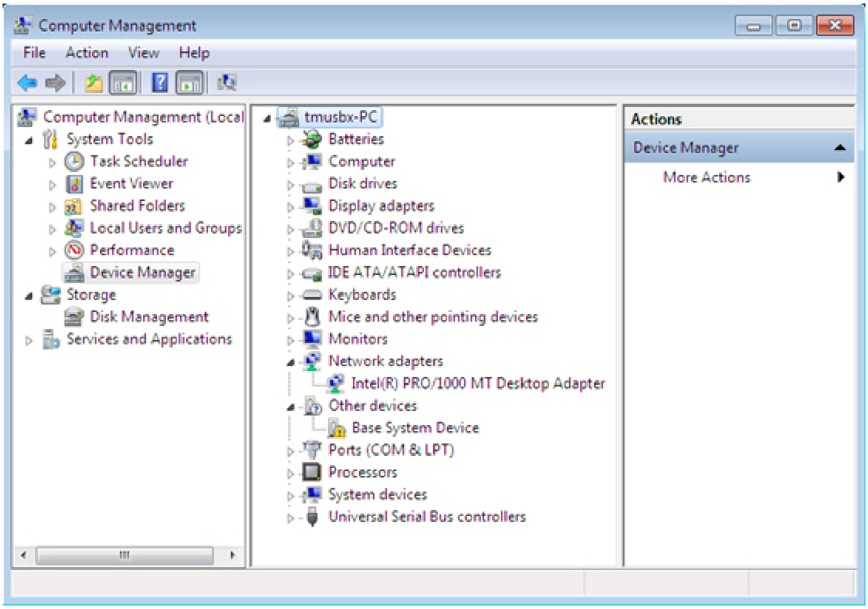


FIGURE 3-49. Device Management - Network Adapter

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.

  The **Predefined Linux Virtual Analyzer Image** is based on CentOS 7.8, comes with all required packages installed and optimized system settings.

  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 only available for CentOS 7.8. To use RHEL 7.9 or RHEL 8.3, you must create your own image.

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

  - *Required Software on page 4-3*
  - *Downloading and Installing VirtualBox on page 4-8*

- *Creating Linux Virtual Machine Images on page 4-9*
- *Modifying the Virtual Machine Environment on page 4-35*
- *Reducing the Size of VirtualBox Disk Images on page 2-43*
- *Exporting Virtual Machine Images to OVA Files on page 4-36*

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 4-8*.

3. Create a virtual machine image.

   For details, see *Creating Linux Virtual Machine Images on page 4-9*.

4. Modify the environment of the virtual machine image.

   For details, see *Modifying the Virtual Machine Environment on page 4-35*.

5. Reduce the size of the VirtualBox Disk Image.

   For details, see *Reducing the Size of VirtualBox Disk Images on page 2-43*.

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

   For details, see *Exporting Virtual Machine Images to OVA Files on page 4-36*.

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

SOFTWARE	DESCRIPTION
Operating system	Virtual Analyzer supports the following operating systems: CentOS 7.8.2003, RHEL 7.9, RHEL 8.3 **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 following packages must be installed on the virtual machine to achieve satisfactory detection results.

TABLE 4-2. Required Packages

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 • 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	• 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 • 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	• 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 • 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

Repository	CentOS 7.8	RHEL 7.9	RHEL 8.3
yum	• 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 • 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	• 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 • 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	• 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 • tcsh • yum-utils • zlib-1.2.11-16.el8_2.x86_64

Repository	CentOS 7.8	RHEL 7.9	RHEL 8.3
yum	• 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	• 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	
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

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

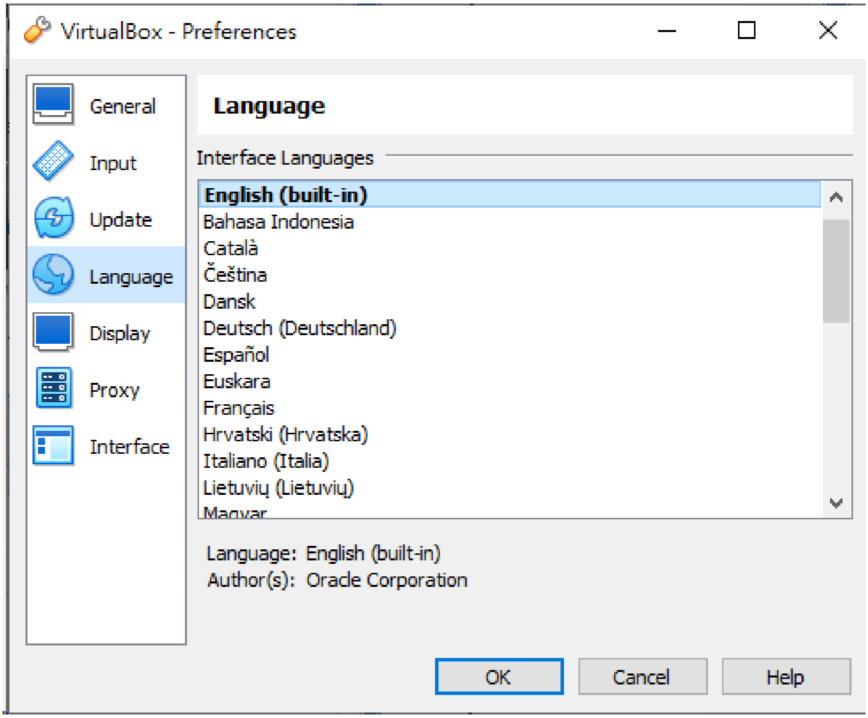
Procedure

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.

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**.



Language

Interface Languages

English (built-in)
Bahasa Indonesia
Català
Čeština
Dansk
Deutsch (Deutschland)
Español
Euskara
Français
Hrvatski (Hrvatska)
Italiano (Italia)
Lietuvių (Lietuvių)
Magyar

Language: English (built-in)
Author(s): Oracle Corporation

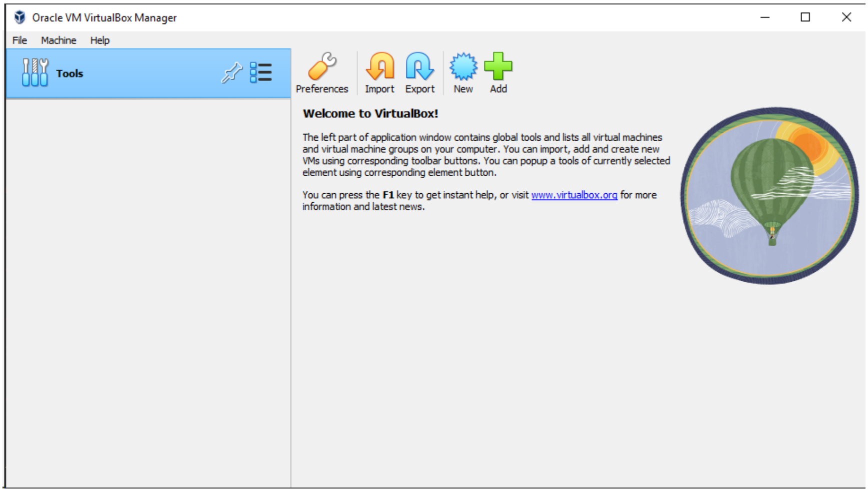
FIGURE 4-1. Language Settings

Creating Linux Virtual Machine Images

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

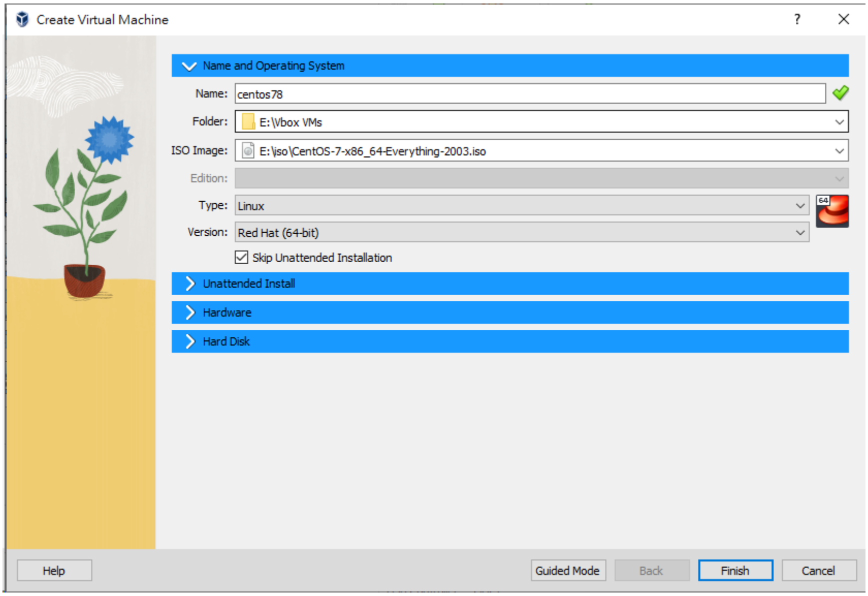
FIGURE 4-2. VirtualBox Manager

2. Click **New**.

   The **Create Virtual Machine** window opens.

3. Click **Expert Mode**.

The Create Virtual Machine wizard enters Expert Mode.



Create Virtual Machine

Name and Operating System

Name: centos78

Folder: E:\Vbox VMs

ISO Image: E:\iso\CentOS-7-x86_64-Everything-2003.iso

Edition:

Type: Linux

Version: Red Hat (64-bit)

☑ Skip Unattended Installation

Unattended Install

Hardware

Hard Disk

FIGURE 4-3. Create Virtual Machine - Expert Mode

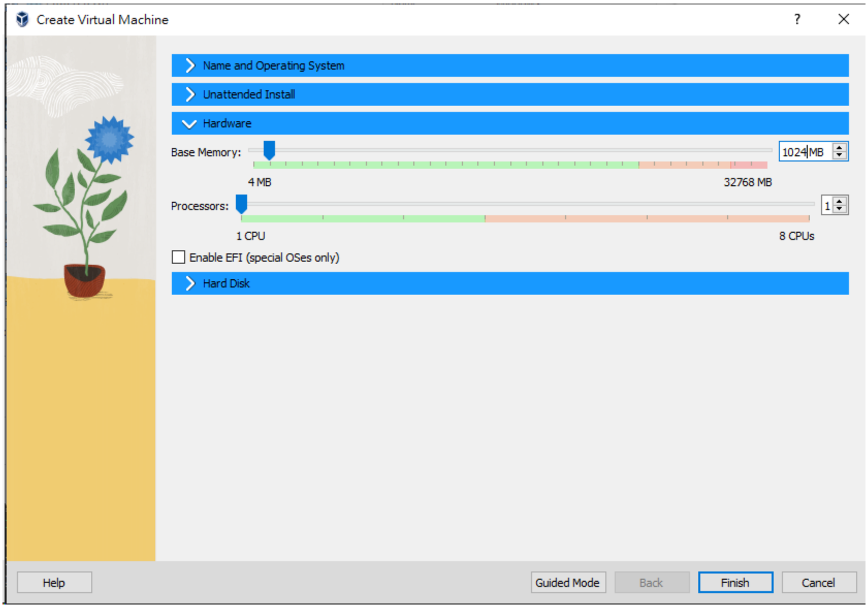
4. Configure the **Name and Operating System** settings.

    - 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**.
    - For the **Version**, select **Red Hat (64-bit)**.
    - Select **Skip Unattended Installation**.

Note

Select **Linux** and **Red Hat (64-bit)** when using CentOS 7.8, RHEL 7.9, or RHEL 8.3.

5. Open the **Hardware** section.



Base Memory: 1024 MB (4 MB – 32768 MB)

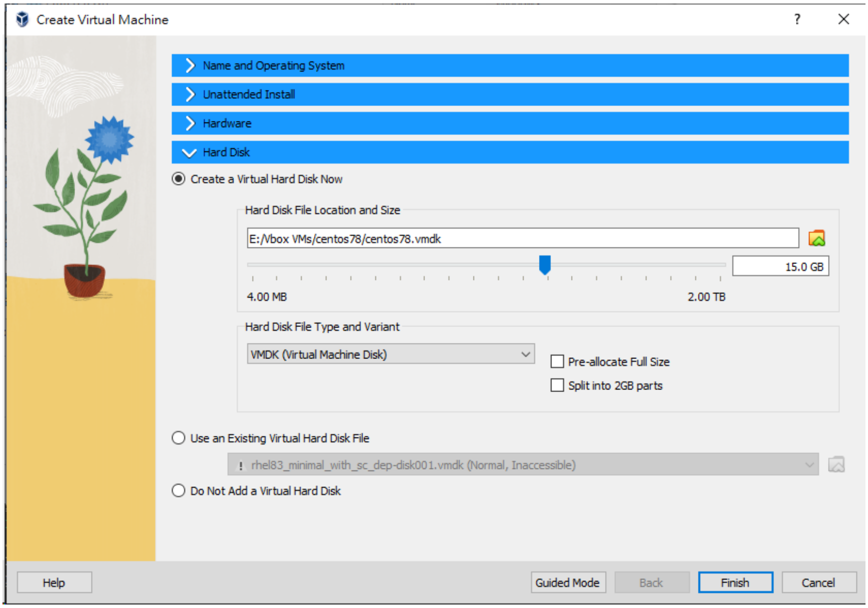
Processors: 1 (1 CPU – 8 CPUs)

□ Enable EFI (special OSes only)

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

7. Open the **Hard Disk** section.



● Create a Virtual Hard Disk Now

Hard Disk File Location and Size

E:/Vbox VMs/centos78/centos78.vmdk

15.0 GB

4.00 MB

2.00 TB

Hard Disk File Type and Variant

VMDK (Virtual Machine Disk)

□ Pre-allocate Full Size

□ Split into 2GB parts

○ Use an Existing Virtual Hard Disk File

! rhel83_minimal_with_sc_dep-disk001.vmdk (Normal, Inaccessible)

○ Do Not Add a Virtual Hard Disk

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 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.

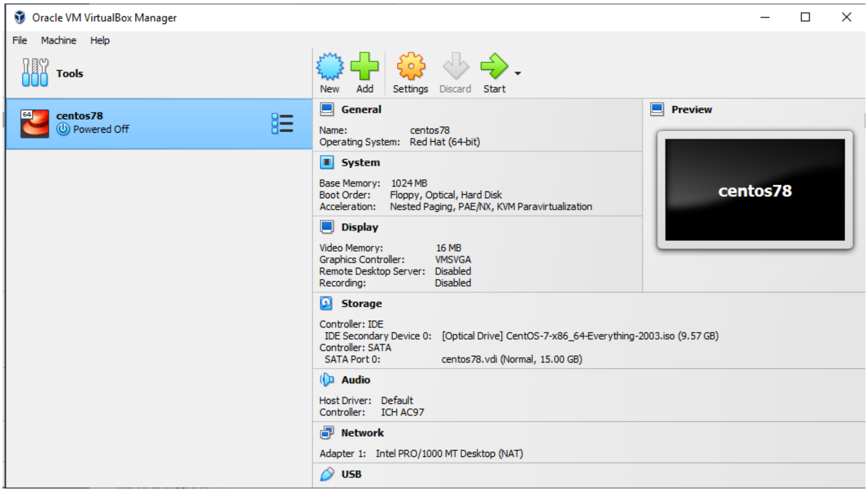
For best results, Trend Micro recommends selecting **VDI (VirtualBox Disk Image)**.

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.



centos78
Powered Off

General

Name: centos78
Operating System: Red Hat (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] CentOS-7-x86_64-Everything-2003.iso (9.57 GB)
Controller: SATA
SATA Port 0: centos78.vdi (Normal, 15.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

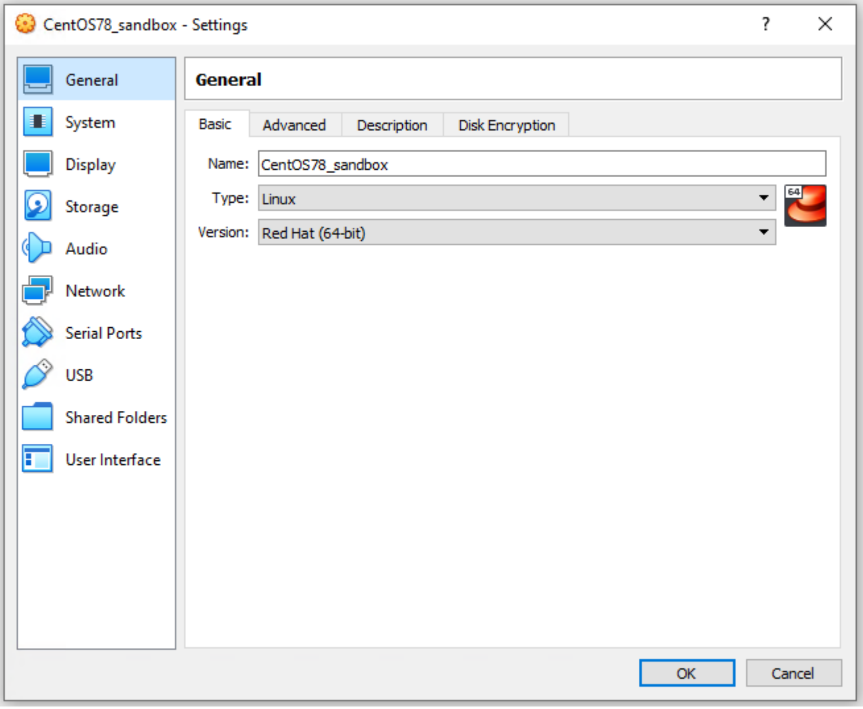
USB

FIGURE 4-6. Newly-created Virtual Machine

Ensure that the virtual machine is not in any group.

11. Click **Settings**.

The **Settings** window opens.



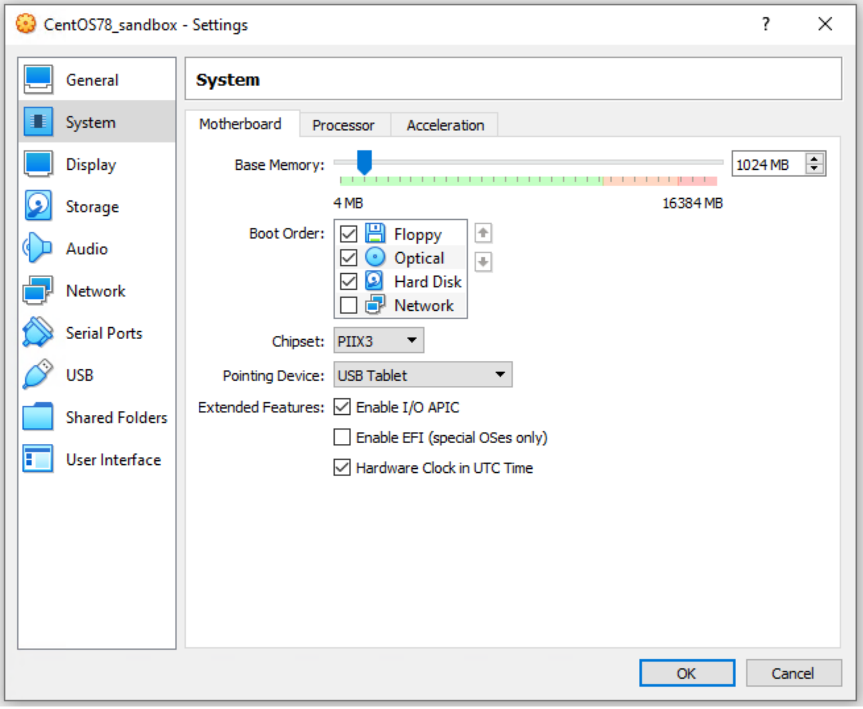
Name: CentOS78_sandbox

Type: Linux

Version: Red Hat (64-bit)

FIGURE 4-7. VirtualBox Settings

12. Go to **System**.



System

Base Memory: 1024 MB (4 MB – 16384 MB)

Boot Order:
☑ Floppy
☑ Optical
☑ Hard Disk
□ Network

Chipset: PIIX3

Pointing Device: USB Tablet

Extended Features:
☑ Enable I/O APIC
□ Enable EFI (special OSes only)
☑ Hardware Clock in UTC Time

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

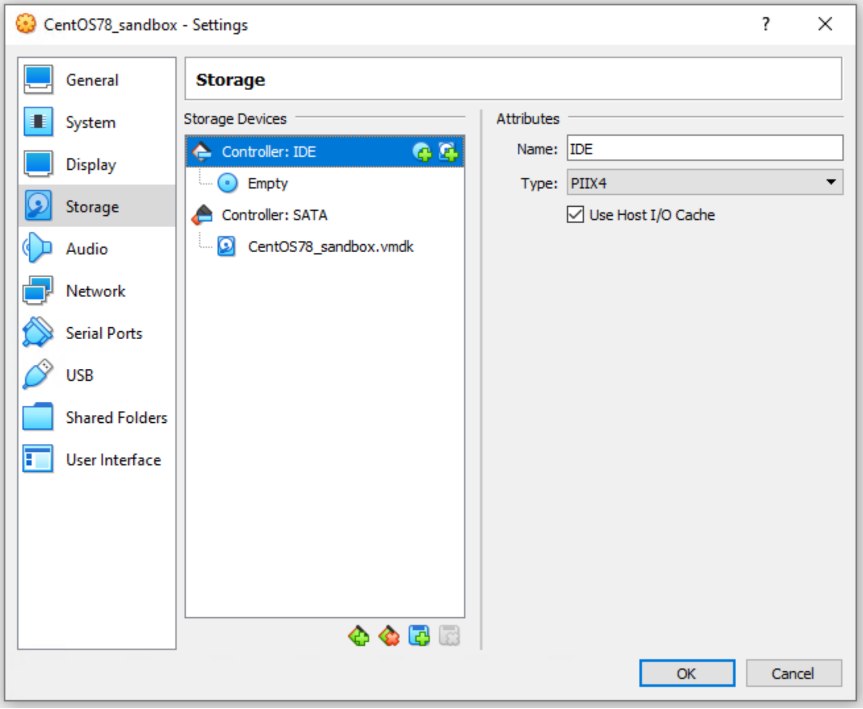
14. On the **Processor** tab, select **Enable PAE/NX**.
15. On the **Acceleration** tab, select **Enable Nested Paging**.

    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**.



CentOS78_sandbox - Settings

Storage

Storage Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - CentOS78_sandbox.vmdk

Attributes

Name: IDE

Type: PIIX4

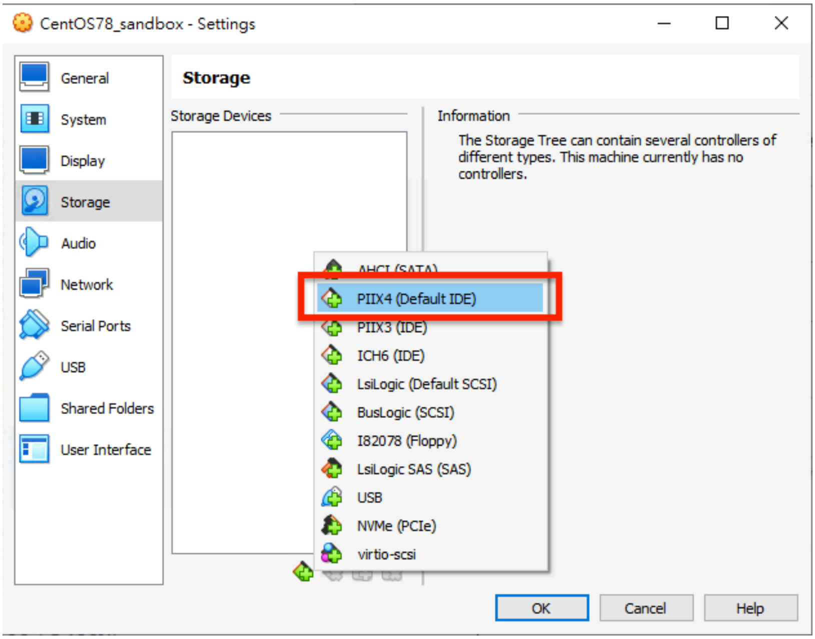
☑ Use Host I/O Cache

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.

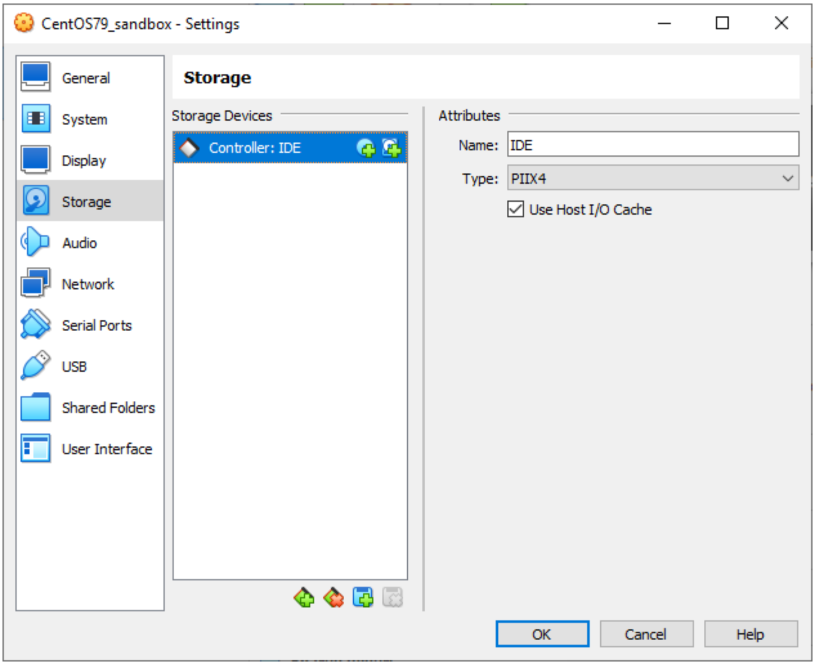
    a. Click and then select **PIIX4 (Default IDE)**.



The Storage Tree can contain several controllers of different types. This machine currently has no controllers.

FIGURE 4-10. Add Storage Controller

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



Name: IDE

Type: PIIX4

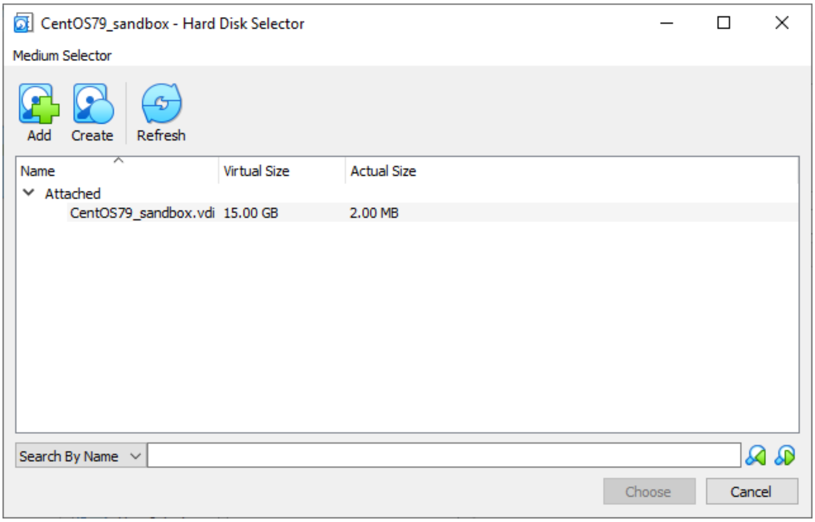
☑ Use Host I/O Cache

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.



CentOS79_sandbox - Hard Disk Selector

Medium Selector

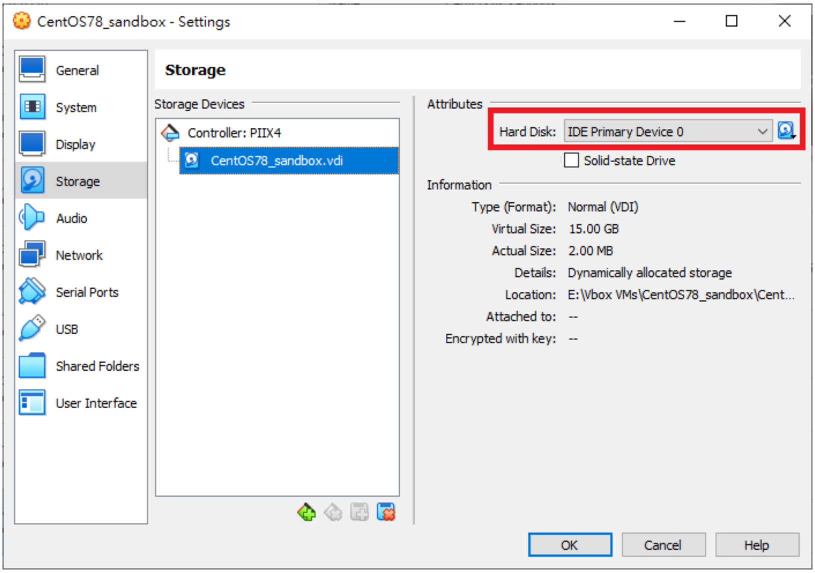
Name	Virtual Size	Actual Size
Attached		
CentOS79_sandbox.vdi	15.00 GB	2.00 MB

Search By Name

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**.



Storage

Storage Devices

Controller: PIIX4

CentOS78_sandbox.vdi

Attributes

Hard Disk: IDE Primary Device 0

□ Solid-state Drive

Information

Type (Format): Normal (VDI)

Virtual Size: 15.00 GB

Actual Size: 2.00 MB

Details: Dynamically allocated storage

Location: E:\Vbox VMs\CentOS78_sandbox\Cent...

Attached to: --

Encrypted with key: --

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**.

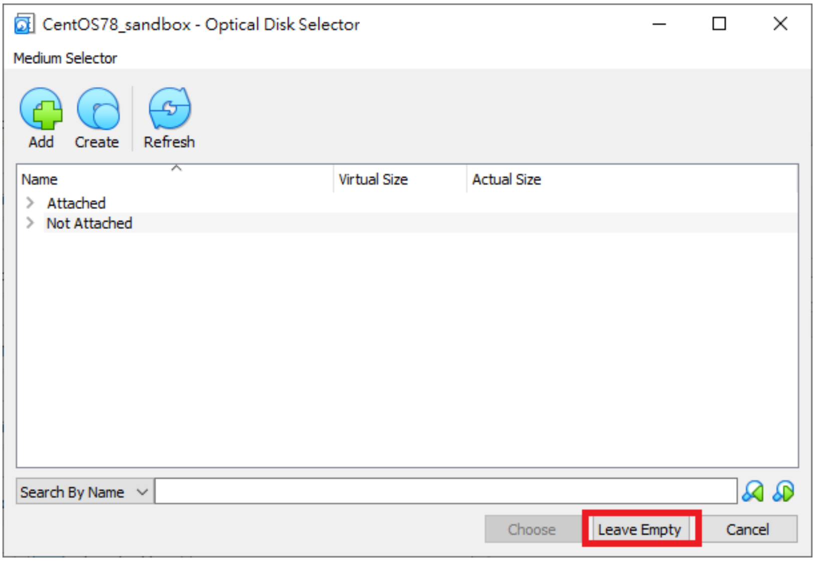
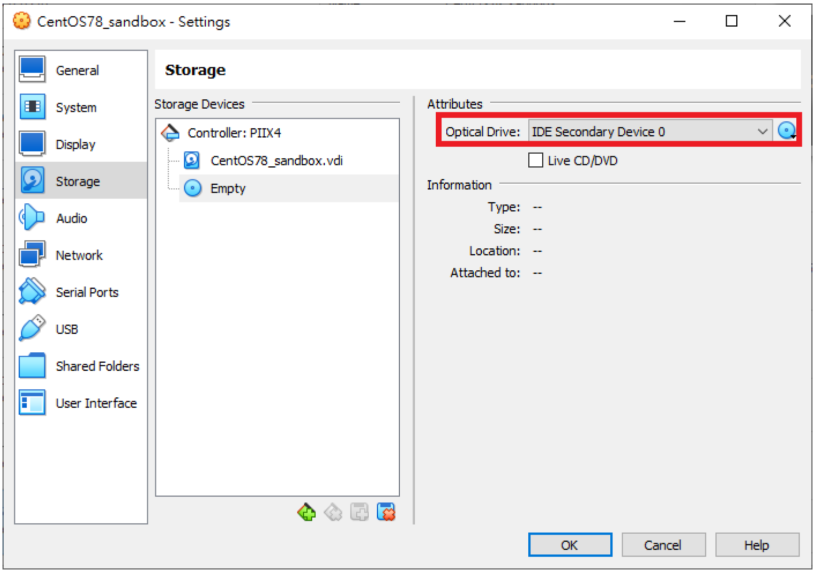


FIGURE 4-14. Optical Disk Selector

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



CentOS78_sandbox - Settings

Storage

Storage Devices

- Controller: PIIX4
  - CentOS78_sandbox.vdi
  - Empty

Attributes

Optical Drive: IDE Secondary Device 0

□ Live CD/DVD

Information

Type: --

Size: --

Location: --

Attached to: --

FIGURE 4-15. IDE Secondary Device 0

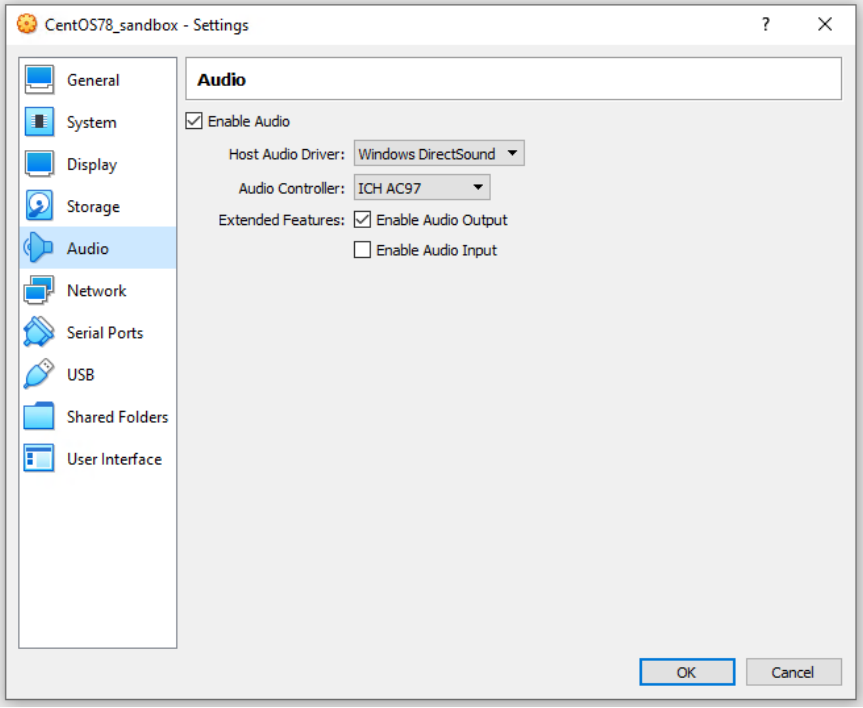
j. Click 💿 and select **Choose/Create a Virtual Optical Disk...**

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.



CentOS78_sandbox - Settings

Audio

☑ Enable Audio

Host Audio Driver: Windows DirectSound

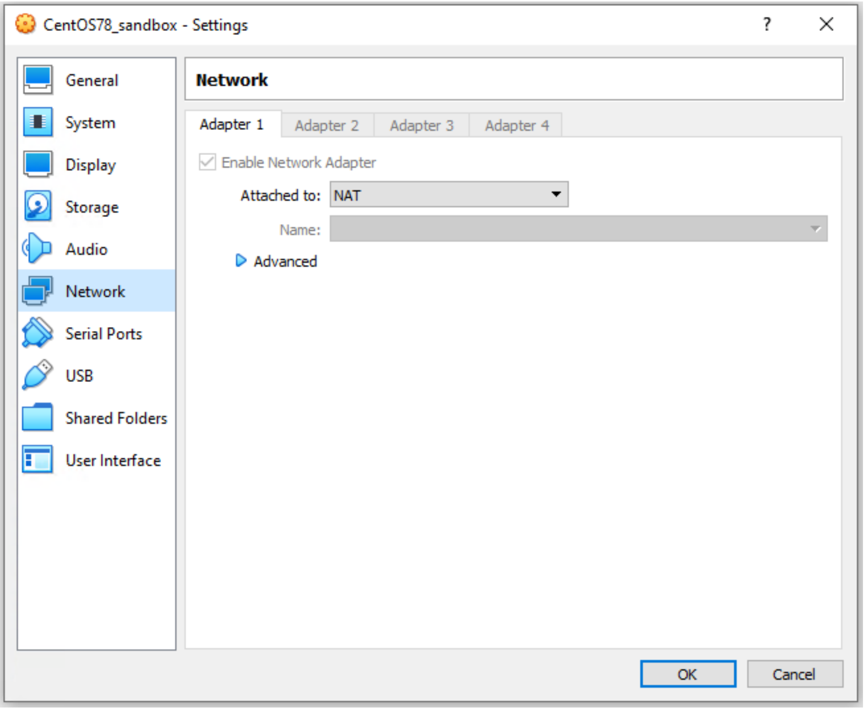
Audio Controller: ICH AC97

Extended Features: ☑ Enable Audio Output

□ Enable Audio Input

FIGURE 4-16. Audio Options Settings

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



☑ Enable Network Adapter

Attached to: NAT

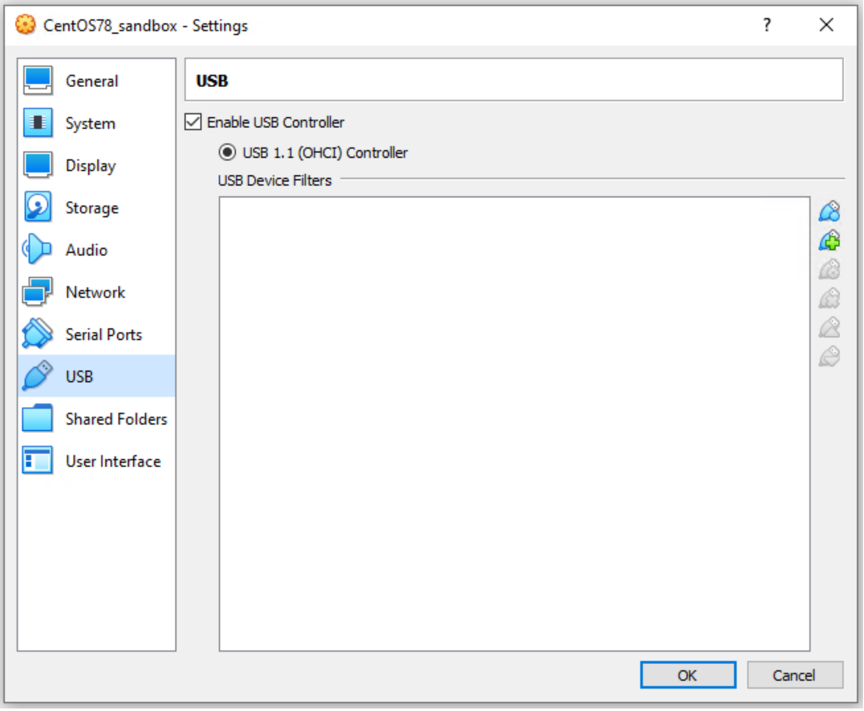
Name:

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**.



CentOS78_sandbox - Settings

USB

☑ Enable USB Controller

● USB 1.1 (OHCI) Controller

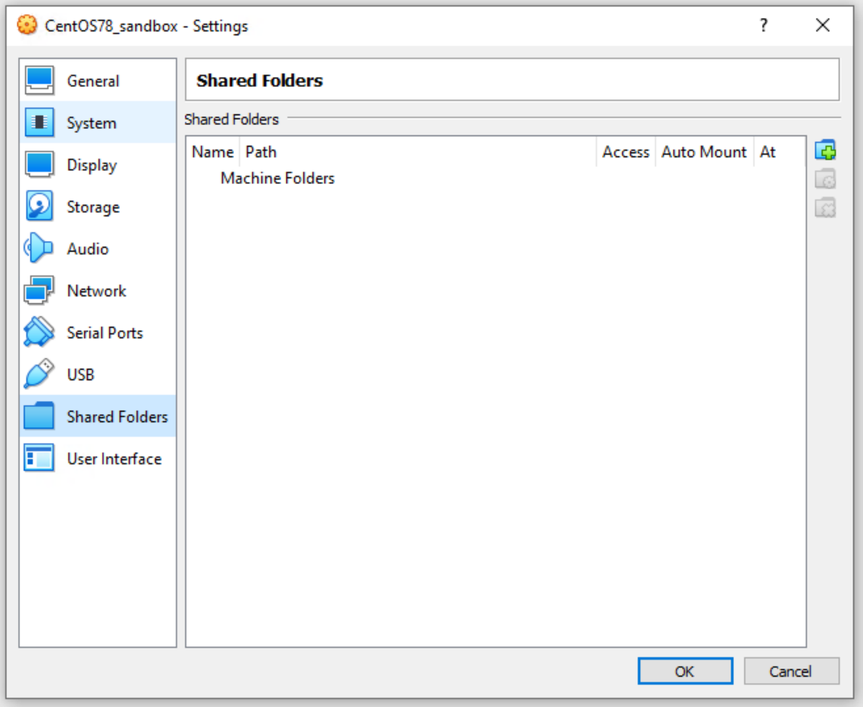
USB Device Filters

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.

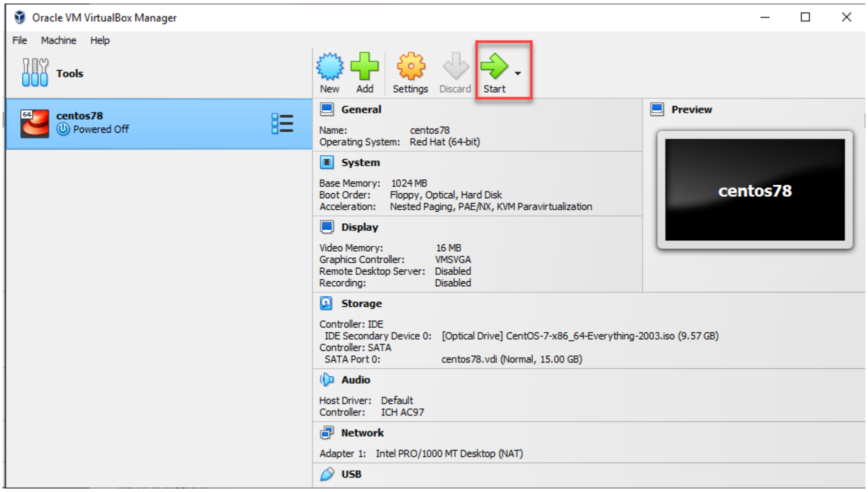


Name	Path	Access	Auto Mount	At
	Machine Folders			

Figure 4-19. Shared Folders Settings

25. Click **OK**.

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



centos78
Powered Off

General

Name: centos78
Operating System: Red Hat (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] CentOS-7-x86_64-Everything-2003.iso (9.57 GB)
Controller: SATA
SATA Port 0: centos78.vdi (Normal, 15.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

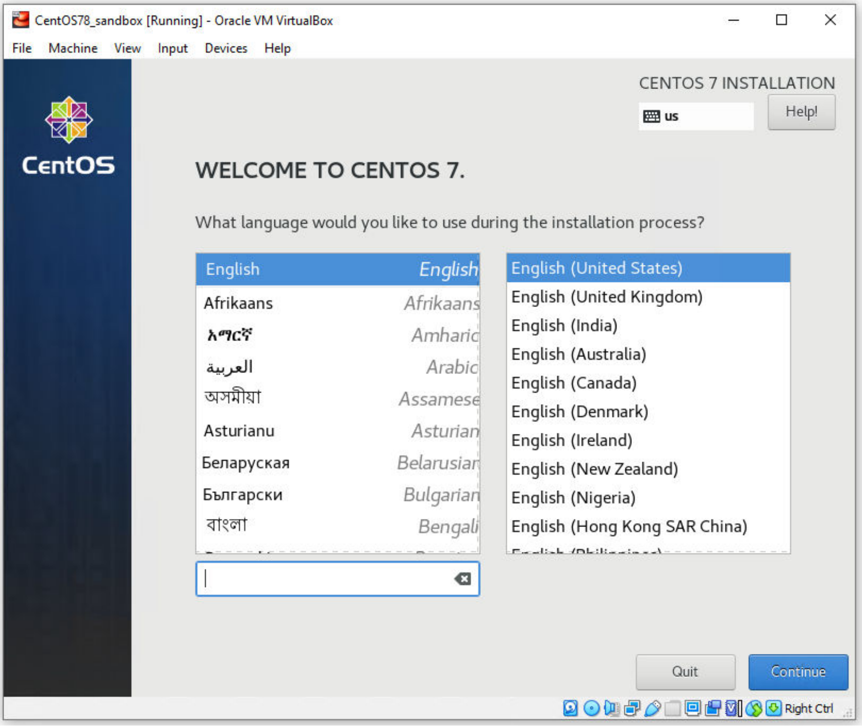
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

FIGURE 4-20. VirtualBox Manager

The installation process starts.

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



WELCOME TO CENTOS 7.

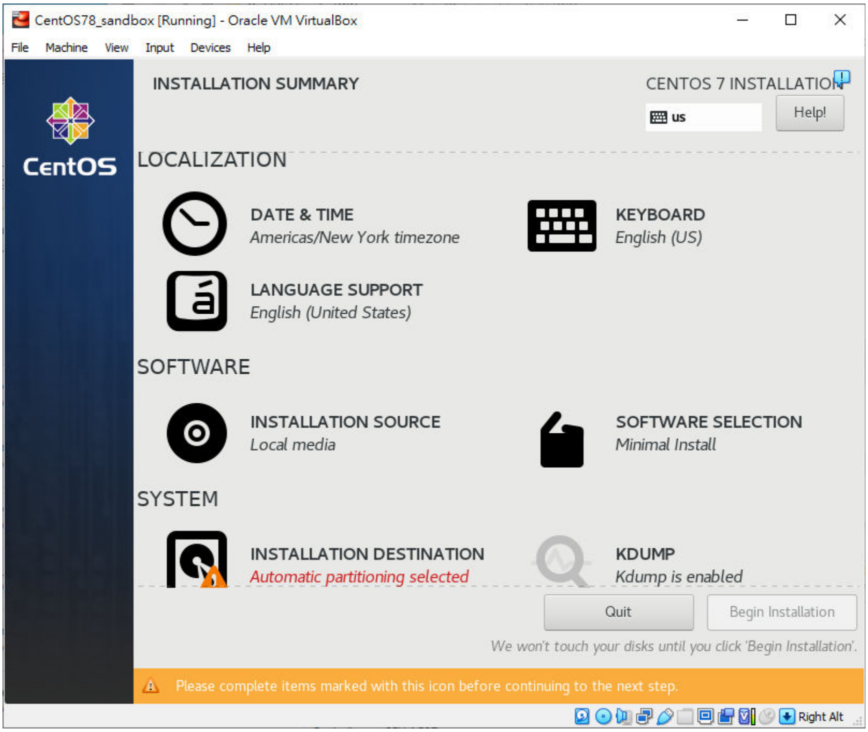
What language would you like to use during the installation process?

English	English
Afrikaans	Afrikaans
አማርኛ	Amharic
العربية	Arabic
অসমীয়া	Assamese
Asturianu	Asturian
Беларуская	Belarusian
Български	Bulgarian
বাংলা	Bengali

English (United States)
English (United Kingdom)
English (India)
English (Australia)
English (Canada)
English (Denmark)
English (Ireland)
English (New Zealand)
English (Nigeria)
English (Hong Kong SAR China)

FIGURE 4-21. Operating System Installation Process

28. Select **English** and click **Continue**.



INSTALLATION SUMMARY

CENTOS 7 INSTALLATION

LOCALIZATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Minimal Install

SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

KDUMP
Kdump is enabled

We won't touch your disks until you click 'Begin Installation'.

⚠ Please complete items marked with this icon before continuing to the next step.

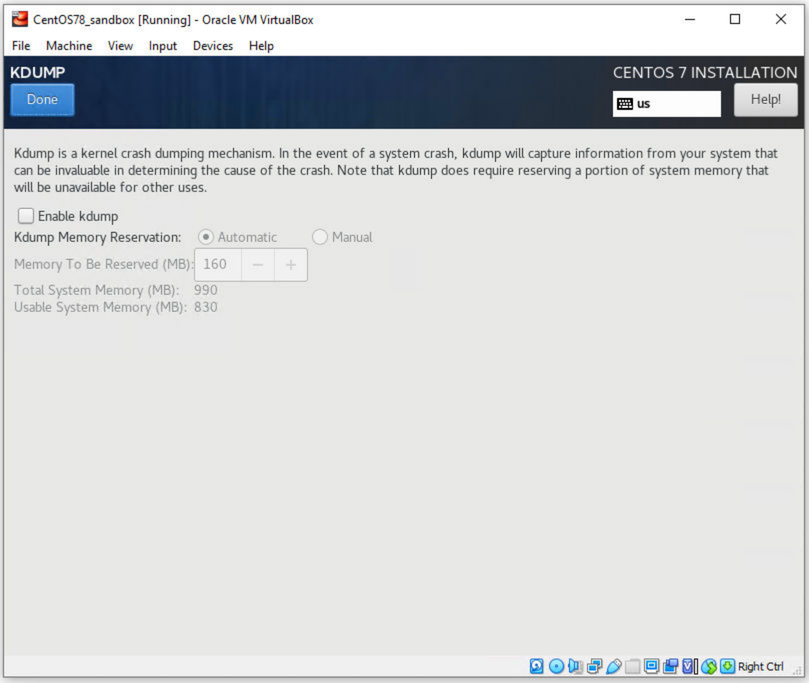
FIGURE 4-22. Installation Summary

29. Configure kdump settings.

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

    b. Disable **Enable kdump**.

    c. Click **Done**.


CentOS78_sandbox [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KDUMP
Done
CENTOS 7 INSTALLATION
us
Help!
Right Ctrl

Kdump is a kernel crash dumping mechanism. In the event of a system crash, kdump will capture information from your system that can be invaluable in determining the cause of the crash. Note that kdump does require reserving a portion of system memory that will be unavailable for other uses.

□ Enable kdump

Kdump Memory Reservation: ● Automatic ○ Manual

Memory To Be Reserved (MB): 160 − +

Total System Memory (MB): 990

Usable System Memory (MB): 830

Figure 4-23. Installation Summary kdump

30. Configure network settings.

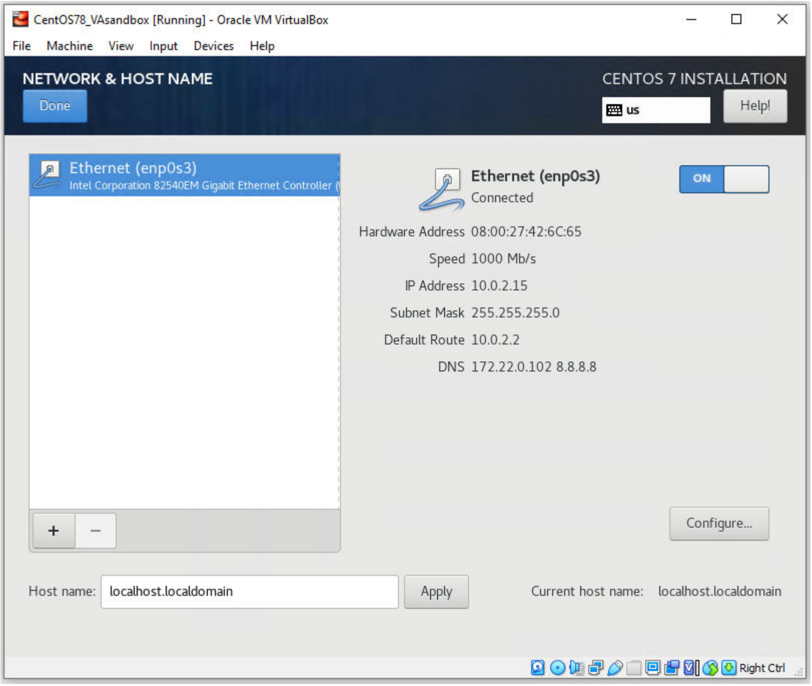
    a. On the **Installation Summary** screen, click **NETWORK & HOST NAME**.

    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**.



Ethernet (enp0s3)
Intel Corporation 82540EM Gigabit Ethernet Controller (

Ethernet (enp0s3)
Connected

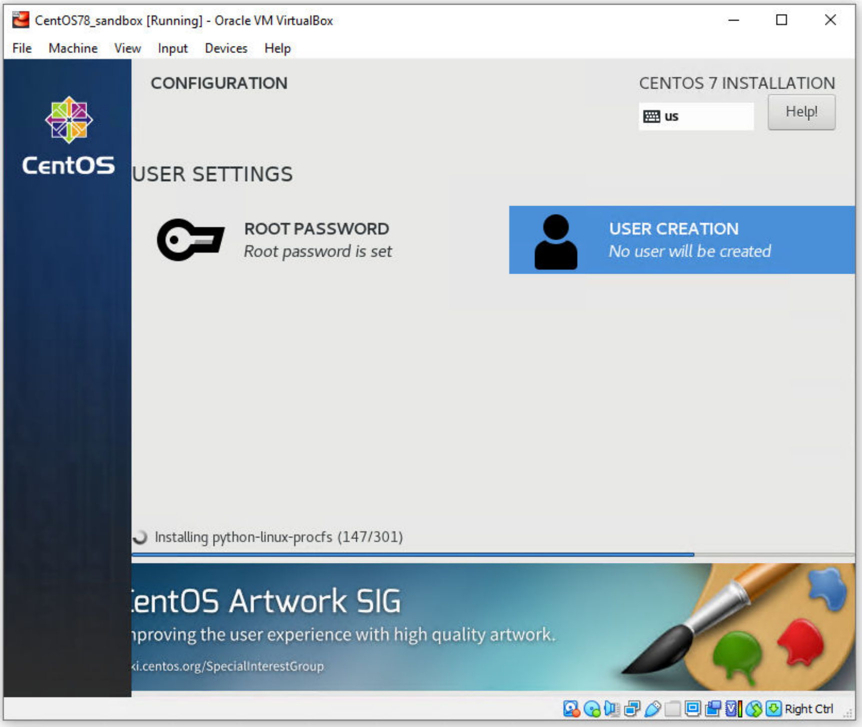
Hardware Address 08:00:27:42:6C:65
Speed 1000 Mb/s
IP Address 10.0.2.15
Subnet Mask 255.255.255.0
Default Route 10.0.2.2
DNS 172.22.0.102 8.8.8.8

Host name: localhost.localdomain

Current host name: localhost.localdomain

FIGURE 4-24. Installation Summary Network & Host Name

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



CentOS78_sandbox [Running] - Oracle VM VirtualBox

Installing python-linux-procfs (147/301)

entOS Artwork SIG
nproving the user experience with high quality artwork.
ki.centos.org/SpecialInterestGroup
Right Ctrl

FIGURE 4-25. Password Configuration

Important

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

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 4-35*

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	Type **`nmcli`** to check the network interface status. **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	Edit the network interface configuration file `/etc/sysconfig/network-scripts/ifcfg-<network interface name>`, and modify the following line: `ONBOOT=yes`
Enable and verify that sshd is running	Type the following commands: a. **`systemctl enable sshd`** b. **`systemctl start sshd`** c. **`systemctl status sshd`** Verify that the ssh status is `active (running)`
Disable SELinux	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*.

TASK	STEPS
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.

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

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 **Important** Microsoft .NET Framework 4.0 or later must be installed on the host operating system.
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.

Requirement	Specification
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
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

Setting	Correct Configuration
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	1024 MB
PAE/NX	Enabled
Hardware virtualization	VT-x/AMD-V and nested paging enabled
Audio driver	Enabled
Root password	1111
SELinux	Disabled
kdump	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.

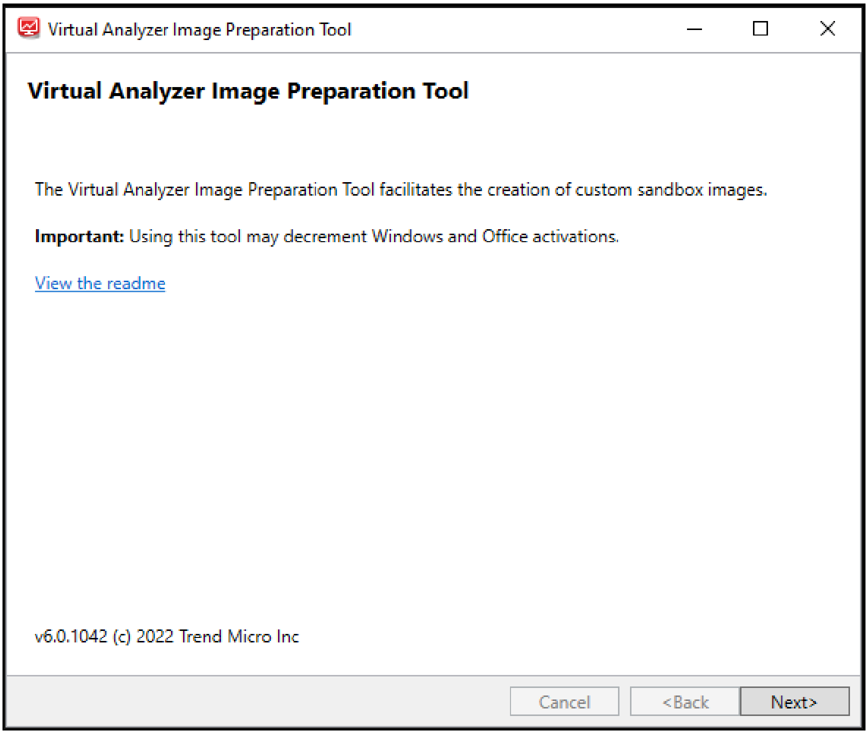
For RHEL 8.3, the RHEL 8.3 Installation ISO `rhel-8.3-x86_64-dvd.iso` is required.

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.



Virtual Analyzer Image Preparation Tool

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

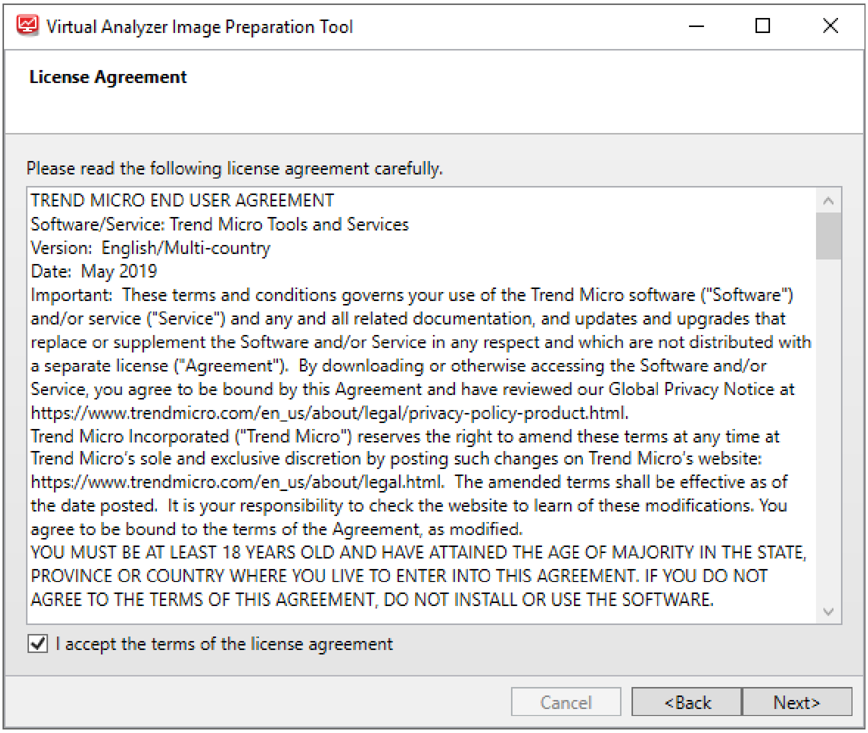
Important: Using this tool may decrement Windows and Office activations.

View the readme

v6.0.1042 (c) 2022 Trend Micro Inc

FIGURE 5-1. Introduction screen

4. Click **Next**.



License Agreement

Please read the following license agreement carefully.

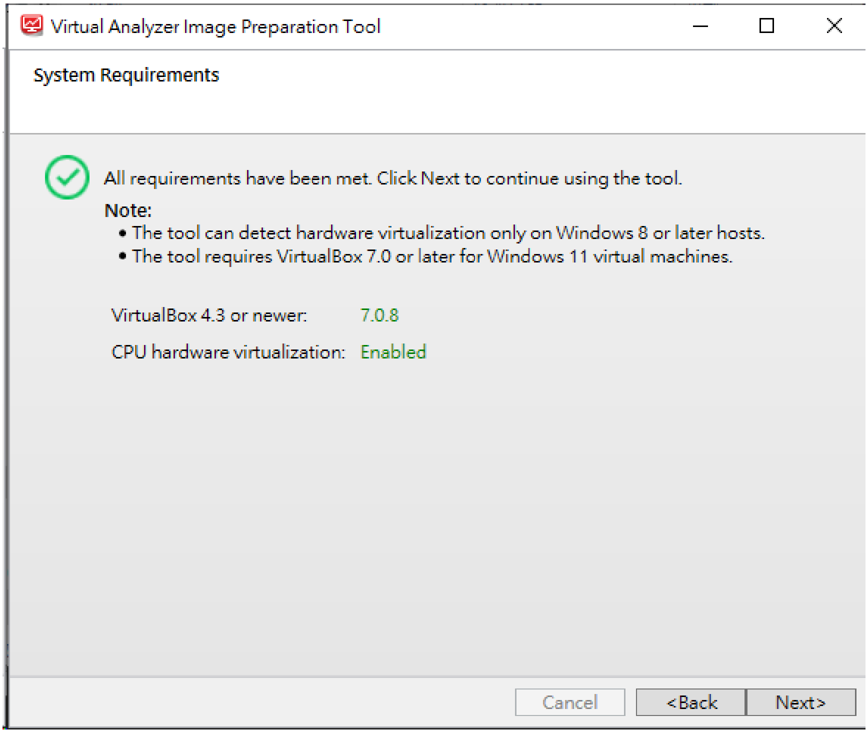
TRENDMICRO END USER AGREEMENT
Software/Service: Trend Micro Tools and Services
Version: English/Multi-country
Date: May 2019
Important: These terms and conditions governs your use of the Trend Micro software ("Software") and/or service ("Service") and any and all related documentation, and updates and upgrades that replace or supplement the Software and/or Service in any respect and which are not distributed with a separate license ("Agreement"). By downloading or otherwise accessing the Software and/or Service, you agree to be bound by this Agreement and have reviewed our Global Privacy Notice at https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html.
Trend Micro Incorporated ("Trend Micro") reserves the right to amend these terms at any time at Trend Micro's sole and exclusive discretion by posting such changes on Trend Micro's website: https://www.trendmicro.com/en_us/about/legal.html. The amended terms shall be effective as of the date posted. It is your responsibility to check the website to learn of these modifications. You agree to be bound to the terms of the Agreement, as modified.
YOU MUST BE AT LEAST 18 YEARS OLD AND HAVE ATTAINED THE AGE OF MAJORITY IN THE STATE, PROVINCE OR COUNTRY WHERE YOU LIVE TO ENTER INTO THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE SOFTWARE.

☑ I accept the terms of the license agreement

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.



System Requirements

All requirements have been met. Click Next to continue using the tool.

Note:

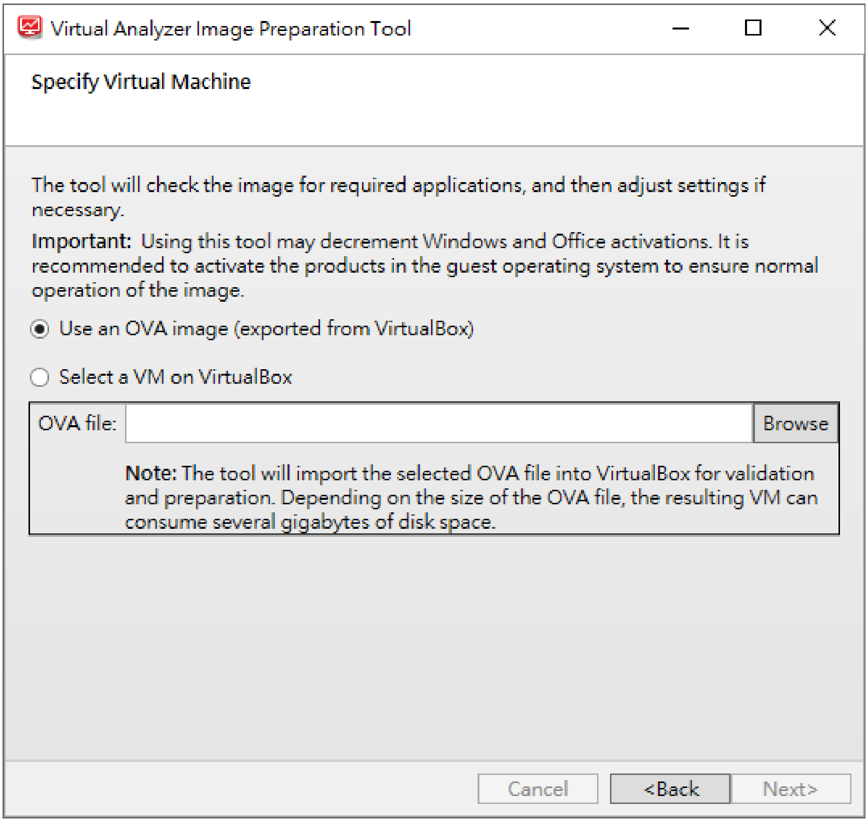
- The tool can detect hardware virtualization only on Windows 8 or later hosts.
- The tool requires VirtualBox 7.0 or later for Windows 11 virtual machines.

VirtualBox 4.3 or newer: 7.0.8

CPU hardware virtualization: Enabled

FIGURE 5-3. System Requirements screen

6. Click **Next**.



Virtual Analyzer Image Preparation Tool

Specify Virtual Machine

The tool will check the image for required applications, and then adjust settings if necessary.

Important: Using this tool may decrement Windows and Office activations. It is recommended to activate the products in the guest operating system to ensure normal operation of the image.

● Use an OVA image (exported from VirtualBox)

○ Select a VM on VirtualBox

OVA file:

Note: The tool will import the selected OVA file into VirtualBox for validation and preparation. Depending on the size of the OVA file, the resulting VM can consume several gigabytes of disk space.

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*.

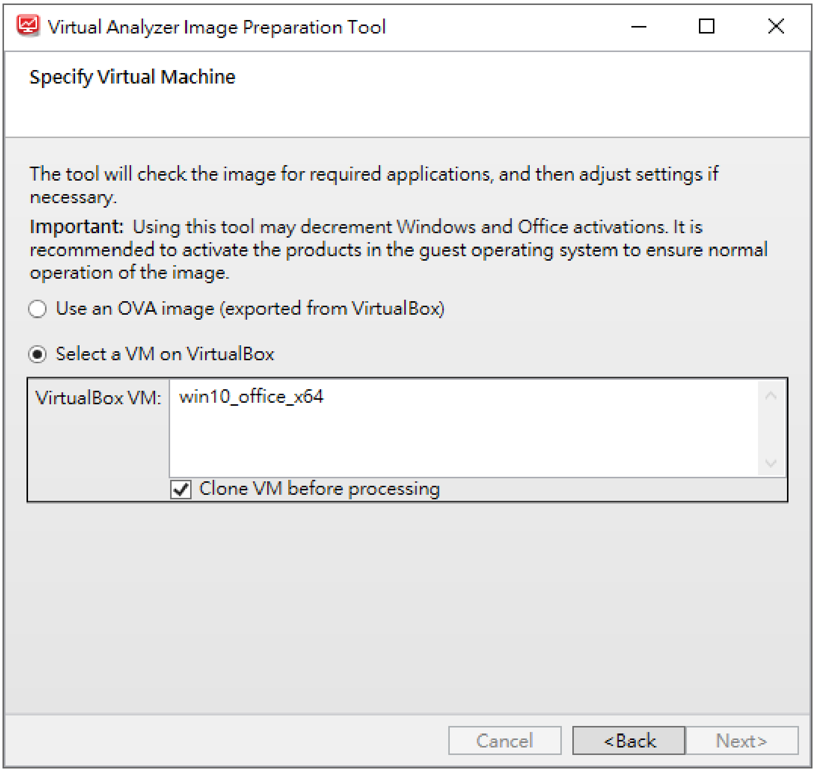
Important

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**.



Virtual Analyzer Image Preparation Tool

Specify Virtual Machine

The tool will check the image for required applications, and then adjust settings if necessary.

Important: Using this tool may decrement Windows and Office activations. It is recommended to activate the products in the guest operating system to ensure normal operation of the image.

○ Use an OVA image (exported from VirtualBox)

● Select a VM on VirtualBox

VirtualBox VM: win10_office_x64

☑ Clone VM before processing

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..

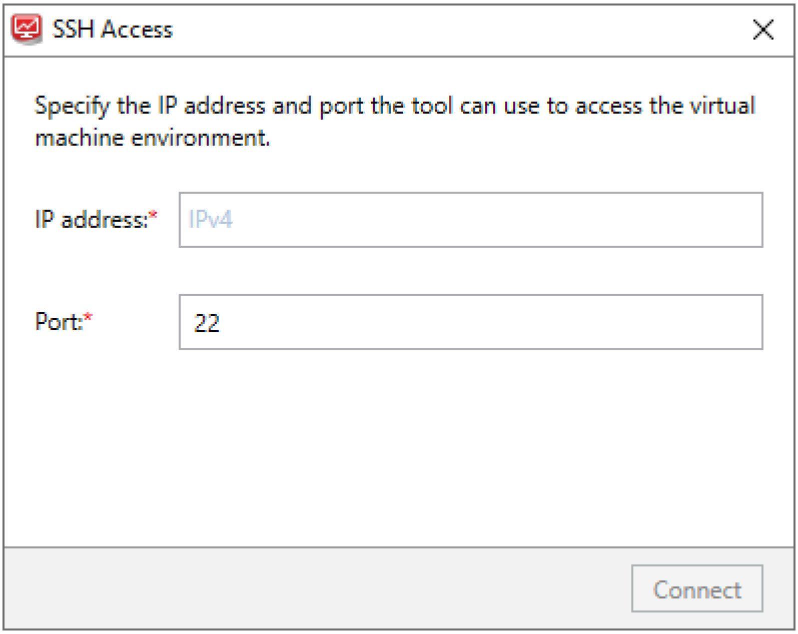
   Cloning allows quick creation of duplicate environments for testing. You can run as many clones as the memory and processors on the system allow.

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**.



Specify the IP address and port the tool can use to access the virtual machine environment.

IP address:* IPv4

Port:* 22

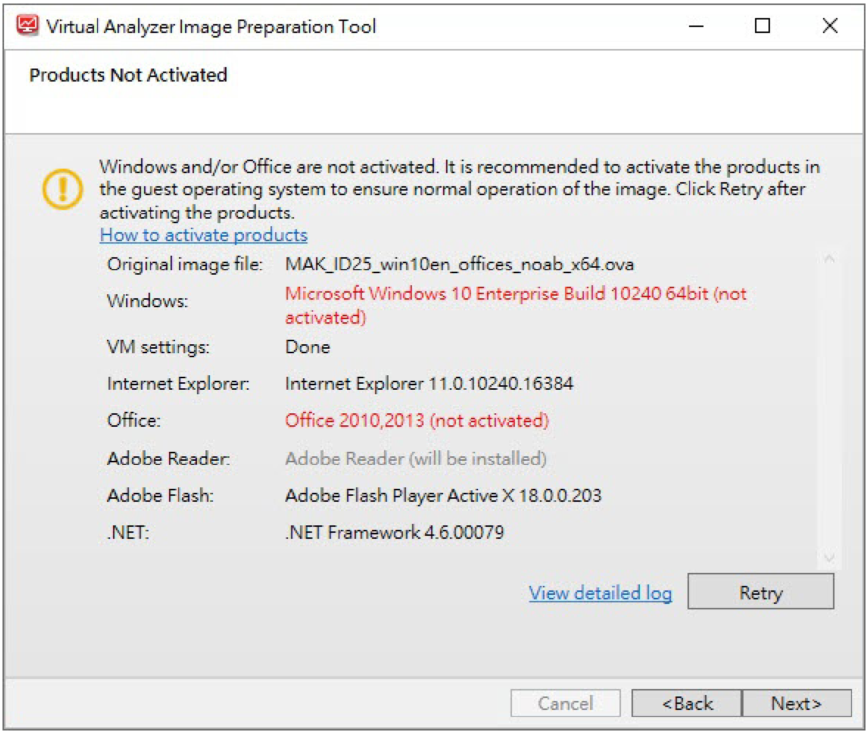
FIGURE 5-6. SSH Access screen for Linux images

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**.



Virtual Analyzer Image Preparation Tool

Products Not Activated

Windows and/or Office are not activated. It is recommended to activate the products in the guest operating system to ensure normal operation of the image. Click Retry after activating the products.

How to activate products

Original image file: MAK_ID25_win10en_offices_noab_x64.ova

Windows: Microsoft Windows 10 Enterprise Build 10240 64bit (not activated)

VM settings: Done

Internet Explorer: Internet Explorer 11.0.10240.16384

Office: Office 2010,2013 (not activated)

Adobe Reader: Adobe Reader (will be installed)

Adobe Flash: Adobe Flash Player Active X 18.0.0.203

.NET: .NET Framework 4.6.00079

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

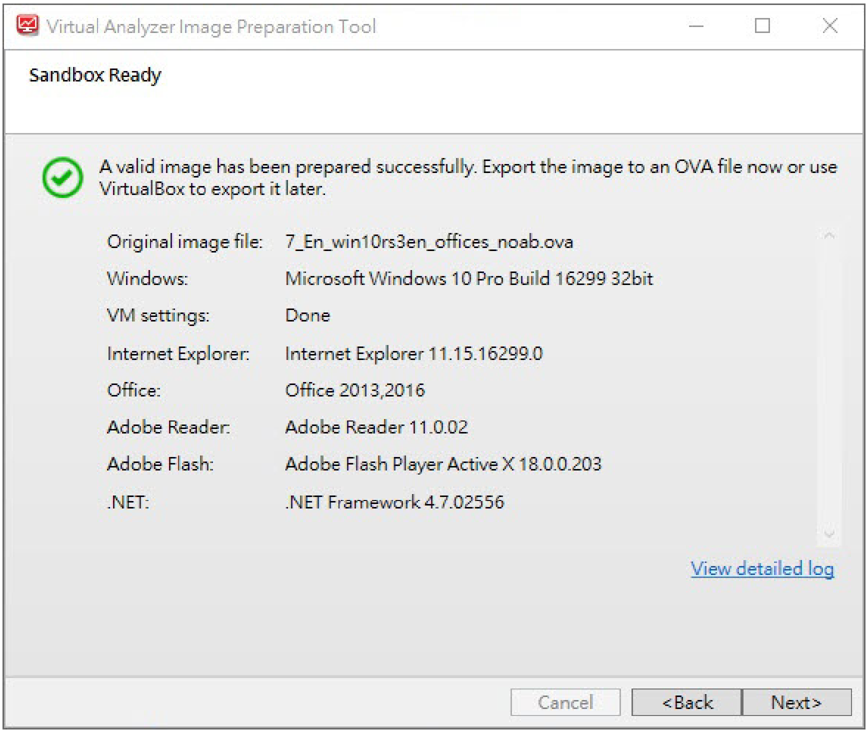
To resolve the issue, see *Products Not Activated - Windows on page 5-20*.

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.

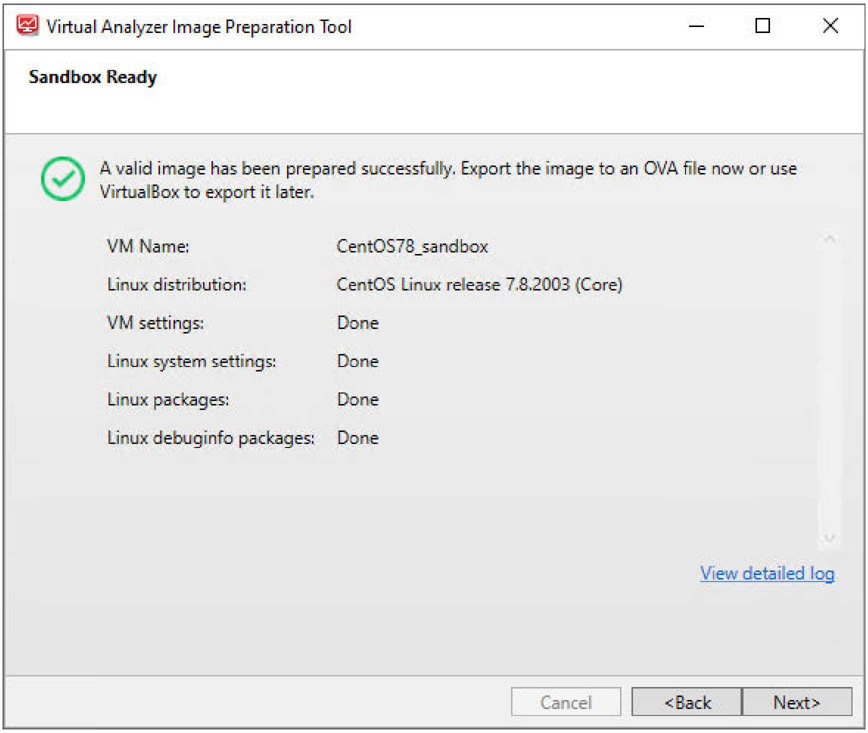


Sandbox Ready

A valid image has been prepared successfully. Export the image to an OVA file now or use VirtualBox to export it later.

Original image file:	7_En_win10rs3en_offices_noab.ova
Windows:	Microsoft Windows 10 Pro Build 16299 32bit
VM settings:	Done
Internet Explorer:	Internet Explorer 11.15.16299.0
Office:	Office 2013,2016
Adobe Reader:	Adobe Reader 11.0.02
Adobe Flash:	Adobe Flash Player Active X 18.0.0.203
.NET:	.NET Framework 4.7.02556

FIGURE 5-8. Sandbox Ready screen for Windows images



Sandbox Ready

A valid image has been prepared successfully. Export the image to an OVA file now or use VirtualBox to export it later.

VM Name:	CentOS78_sandbox
Linux distribution:	CentOS Linux release 7.8.2003 (Core)
VM settings:	Done
Linux system settings:	Done
Linux packages:	Done
Linux debuginfo packages:	Done

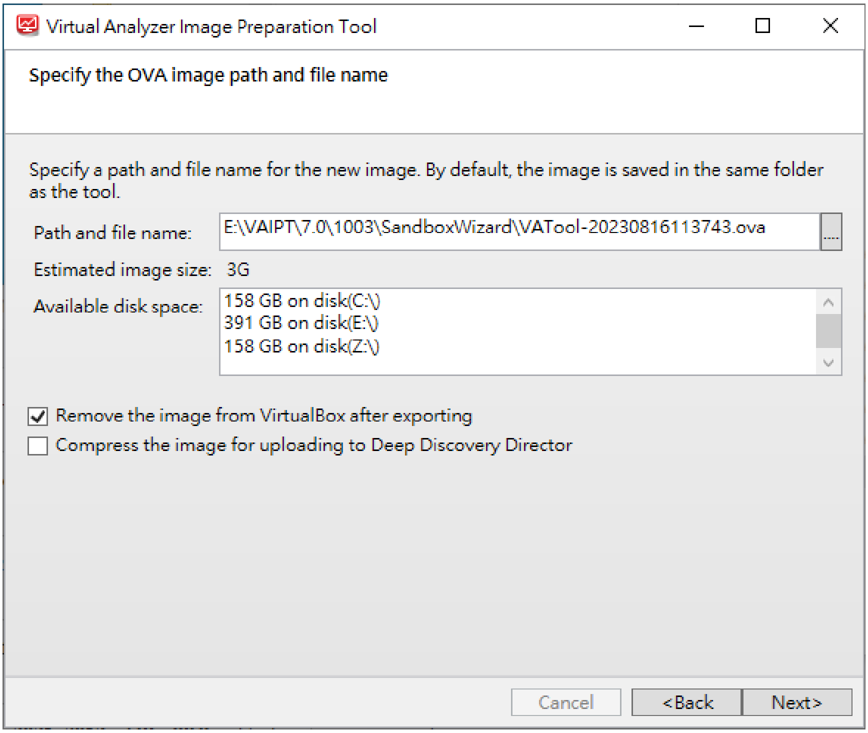
View detailed log

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_output.txt`

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



Specify the OVA image path and file name

Specify a path and file name for the new image. By default, the image is saved in the same folder as the tool.

Path and file name: E:\VAIPT\7.0\1003\SandboxWizard\VATool-20230816113743.ova

Estimated image size: 3G

Available disk space:
158 GB on disk(C:\)
391 GB on disk(E:\)
158 GB on disk(Z:\)

☑ Remove the image from VirtualBox after exporting

□ Compress the image for uploading to Deep Discovery Director

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**.

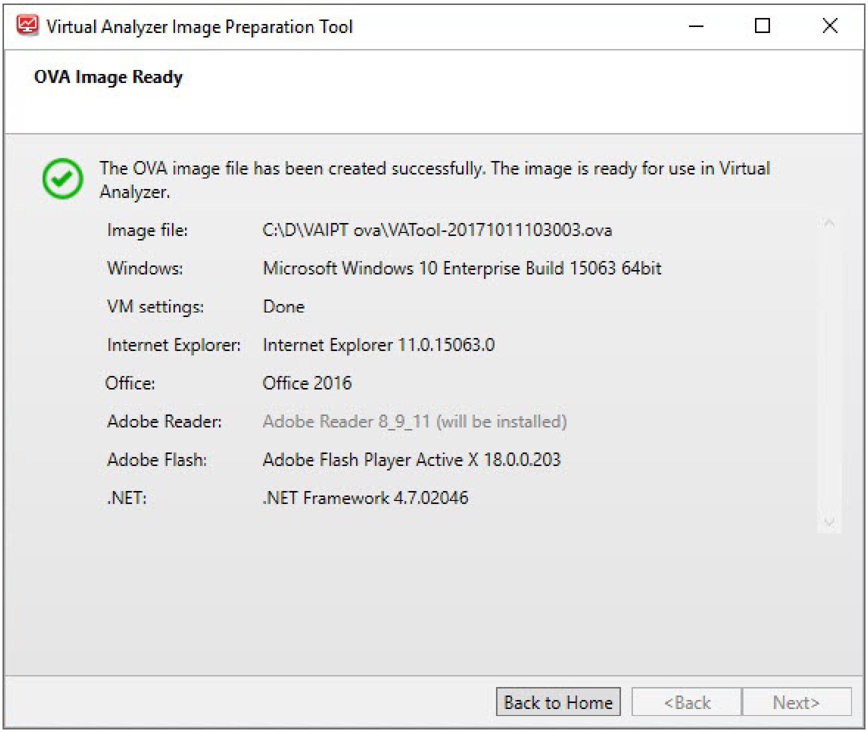
Important

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.

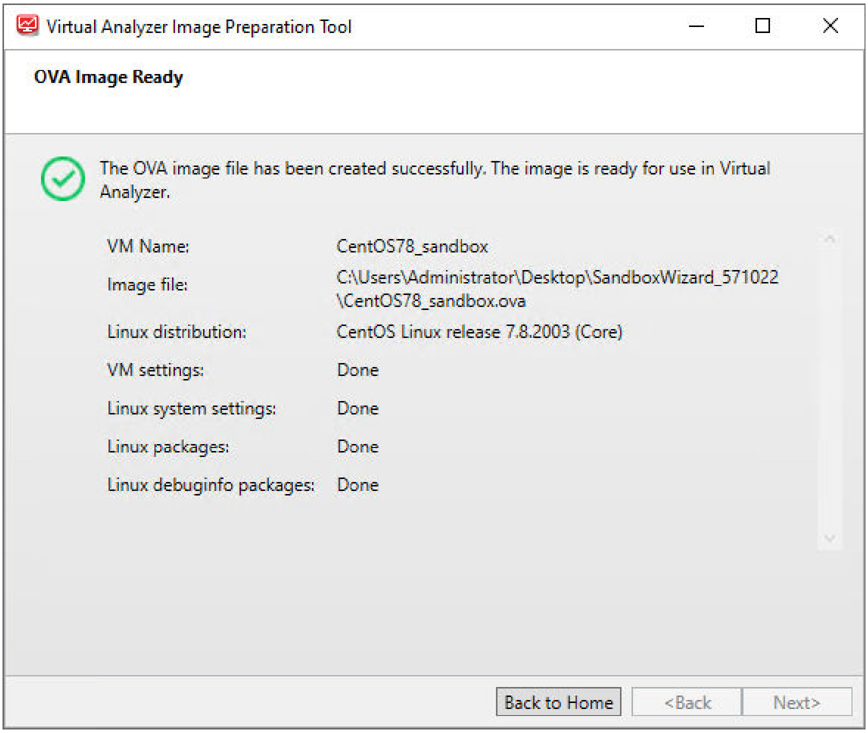


OVA Image Ready

The OVA image file has been created successfully. The image is ready for use in Virtual Analyzer.

Image file:	C:\D\VAIPT ova\VATool-20171011103003.ova
Windows:	Microsoft Windows 10 Enterprise Build 15063 64bit
VM settings:	Done
Internet Explorer:	Internet Explorer 11.0.15063.0
Office:	Office 2016
Adobe Reader:	Adobe Reader 8_9_11 (will be installed)
Adobe Flash:	Adobe Flash Player Active X 18.0.0.203
.NET:	.NET Framework 4.7.02046

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



OVA Image Ready

The OVA image file has been created successfully. The image is ready for use in Virtual Analyzer.

VM Name:	CentOS78_sandbox
Image file:	C:\Users\Administrator\Desktop\SandboxWizard_571022 \CentOS78_sandbox.ova
Linux distribution:	CentOS Linux release 7.8.2003 (Core)
VM settings:	Done
Linux system settings:	Done
Linux packages:	Done
Linux debuginfo packages:	Done

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

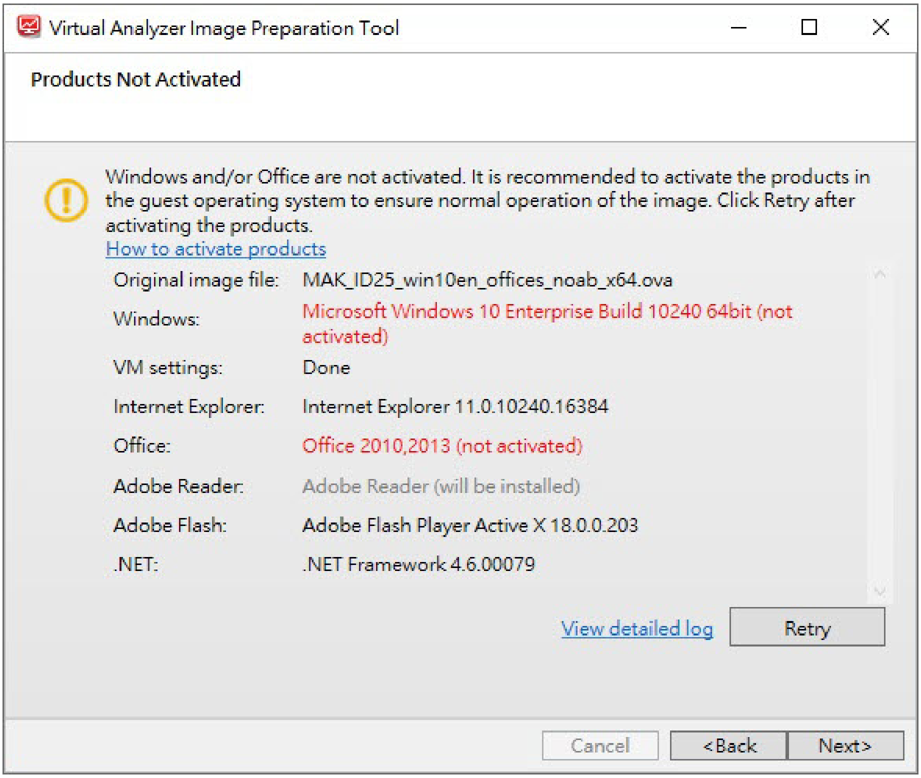
15. Click the **Close** button in the upper right corner to exit the tool or click **Back to Home** to prepare another image.

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.



Virtual Analyzer Image Preparation Tool

Products Not Activated

Windows and/or Office are not activated. It is recommended to activate the products in the guest operating system to ensure normal operation of the image. Click Retry after activating the products.

How to activate products

Original image file:	MAK_ID25_win10en_offices_noab_x64.ova
Windows:	Microsoft Windows 10 Enterprise Build 10240 64bit (not activated)
VM settings:	Done
Internet Explorer:	Internet Explorer 11.0.10240.16384
Office:	Office 2010,2013 (not activated)
Adobe Reader:	Adobe Reader (will be installed)
Adobe Flash:	Adobe Flash Player Active X 18.0.0.203
.NET:	.NET Framework 4.6.00079

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

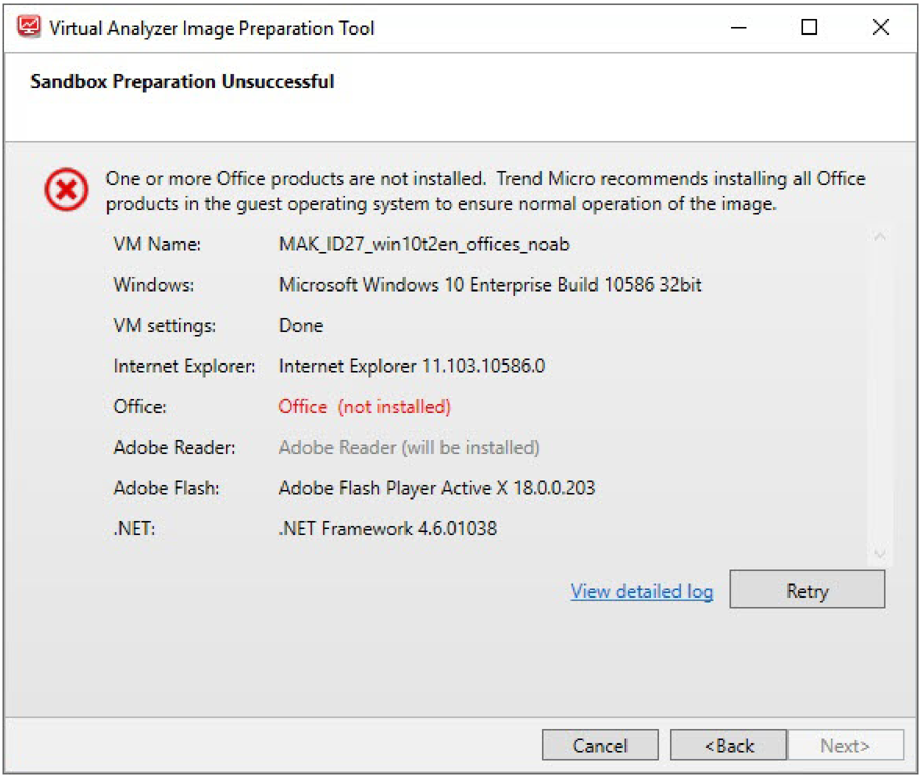
To activate Windows and/or Microsoft Office, perform the following steps.

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.


Virtual Analyzer Image Preparation Tool
Sandbox Preparation Unsuccessful

One or more Office products are not installed. Trend Micro recommends installing all Office products in the guest operating system to ensure normal operation of the image.

VM Name: MAK_ID27_win10t2en_offices_noab

Windows: Microsoft Windows 10 Enterprise Build 10586 32bit

VM settings: Done

Internet Explorer: Internet Explorer 11.103.10586.0

Office: Office (not installed)

Adobe Reader: Adobe Reader (will be installed)

Adobe Flash: Adobe Flash Player Active X 18.0.0.203

.NET: .NET Framework 4.6.01038

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*.

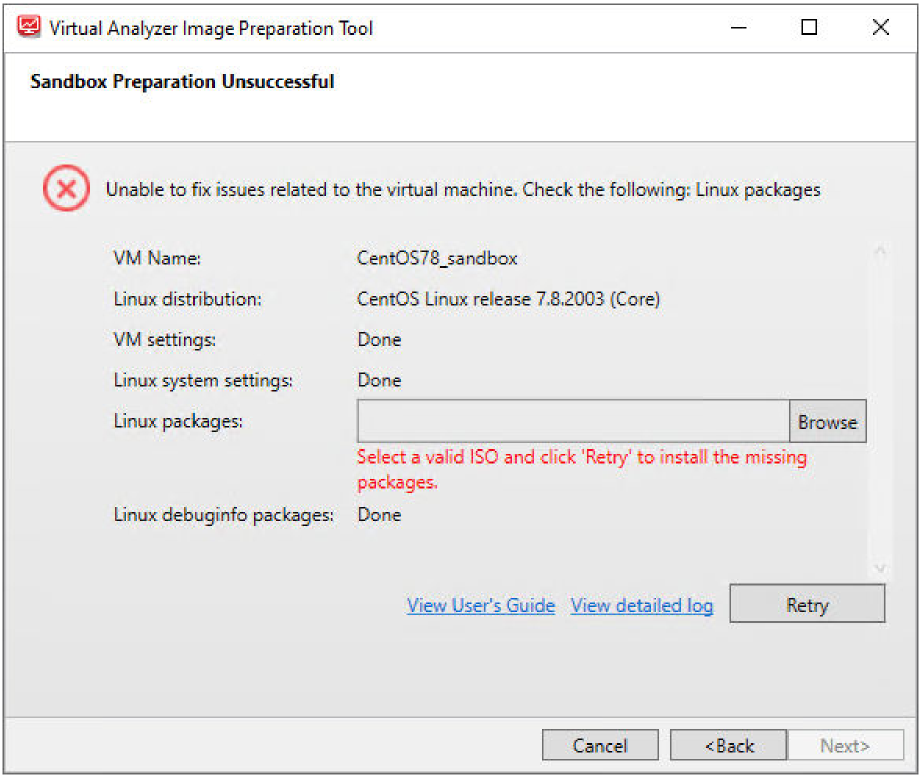
   Note

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

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

Sandbox Preparation Unsuccessful - Missing Linux Packages

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



Virtual Analyzer Image Preparation Tool

Sandbox Preparation Unsuccessful

Unable to fix issues related to the virtual machine. Check the following: Linux packages

VM Name:	CentOS78_sandbox
Linux distribution:	CentOS Linux release 7.8.2003 (Core)
VM settings:	Done
Linux system settings:	Done
Linux packages:	Select a valid ISO and click 'Retry' to install the missing packages.
Linux debuginfo packages:	Done

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_output.txt`

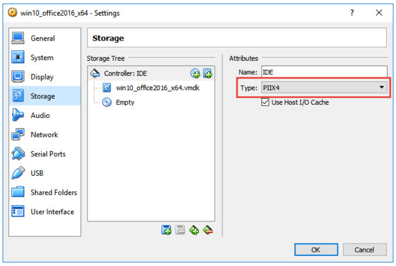
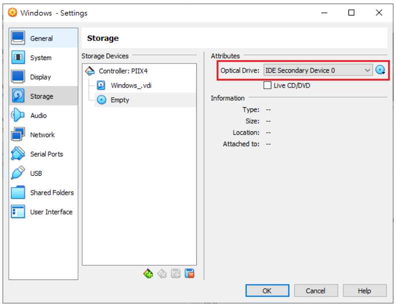
For example: `d:\SandboxWizard\log\VATool-20170925025520_output.txt`

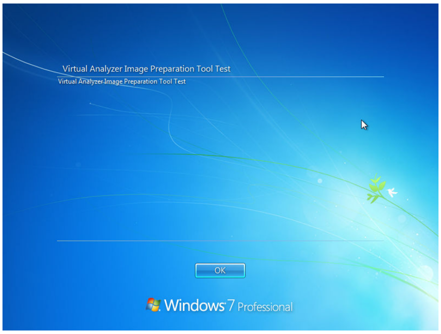
Troubleshooting Common Issues

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**.  win10_office2016_x64 - Settings Storage Storage Tree: Controller: IDE; win10_office2016_x64.vmdk; Empty Attributes Name: IDE Type: PIIX4 ☑ Use Host I/O Cache General System Display Storage Audio Network Serial Ports USB Shared Folders User Interface OK Cancel **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**.  Windows - Settings Storage Storage Devices: Controller: PIIX4; Windows_.vdi; Empty Attributes Optical Drive: IDE Secondary Device 0 ☐ Live CD/DVD Information Type: -- Size: -- Location: -- Attached to: -- General System Display Storage Audio Network Serial Ports USB Shared Folders User Interface OK Cancel Help **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.  Virtual Analyzer Image Preparation Tool Test Virtual Analyzer Image Preparation Tool Test

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 Start 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 Start 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.

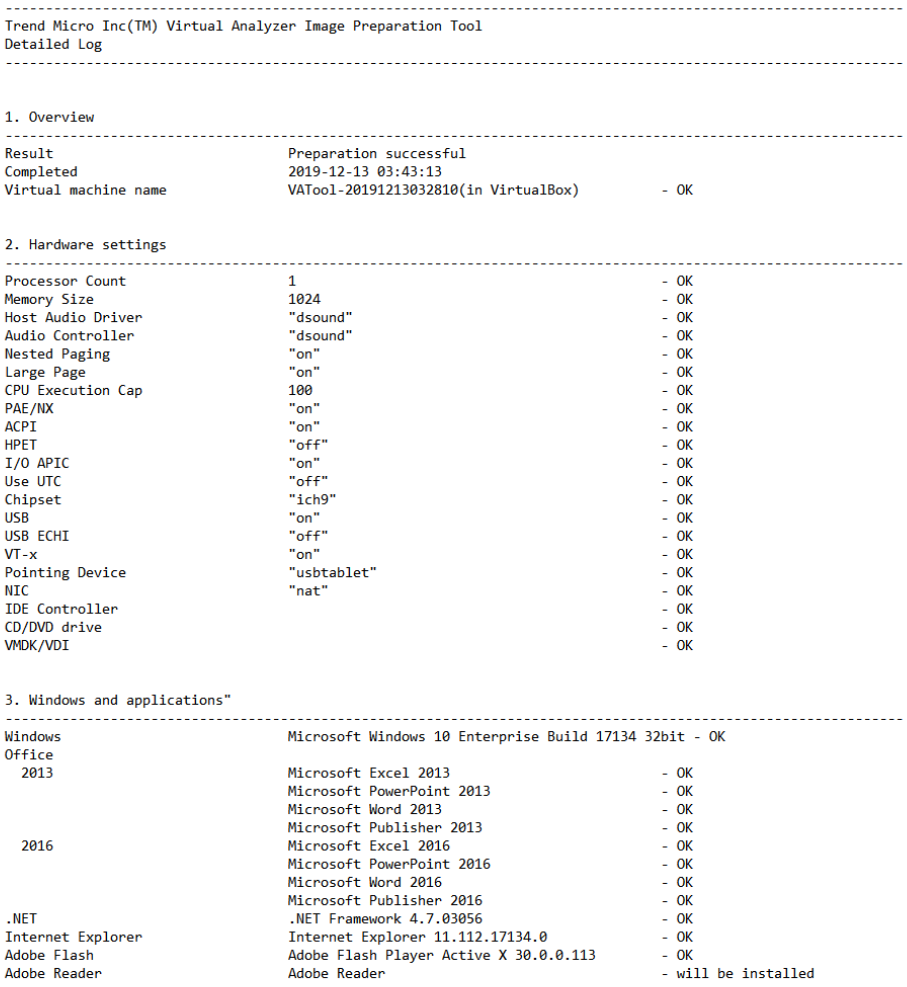
Table 5-6. Common Issues When Using the Tool to Validate Linux Images

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: Red Hat (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.

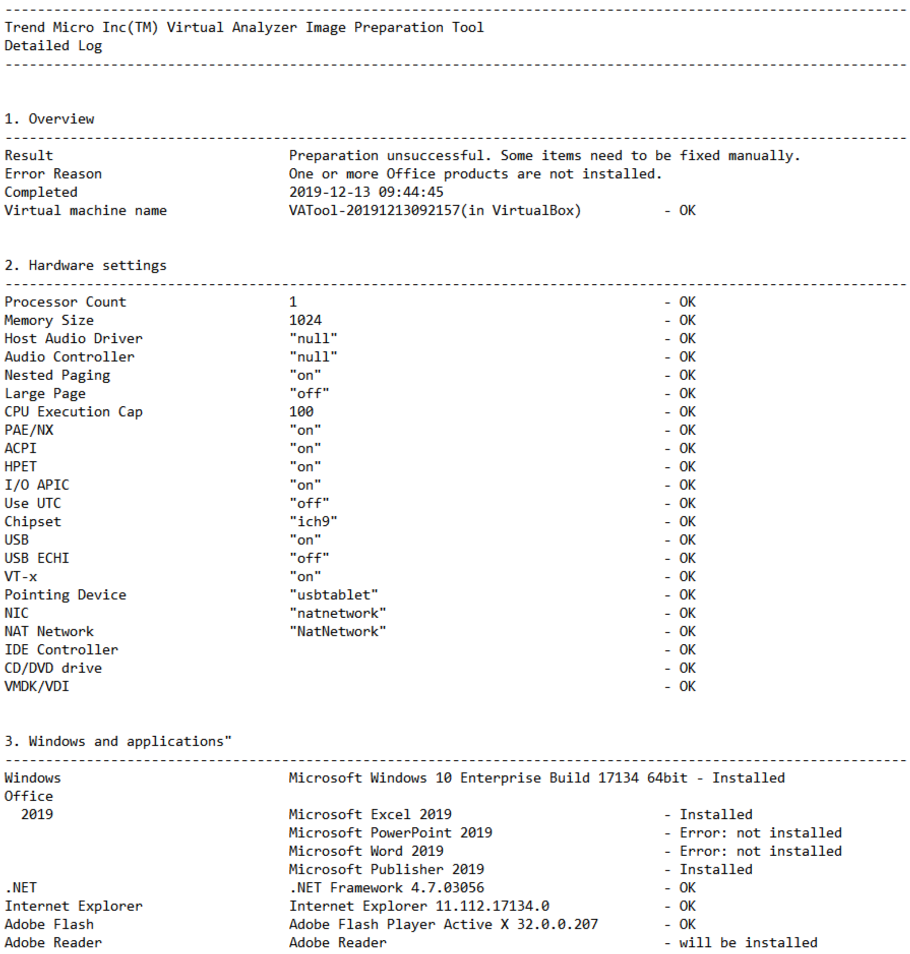
Sample Logs

Windows image preparation successful. Missing app detected.



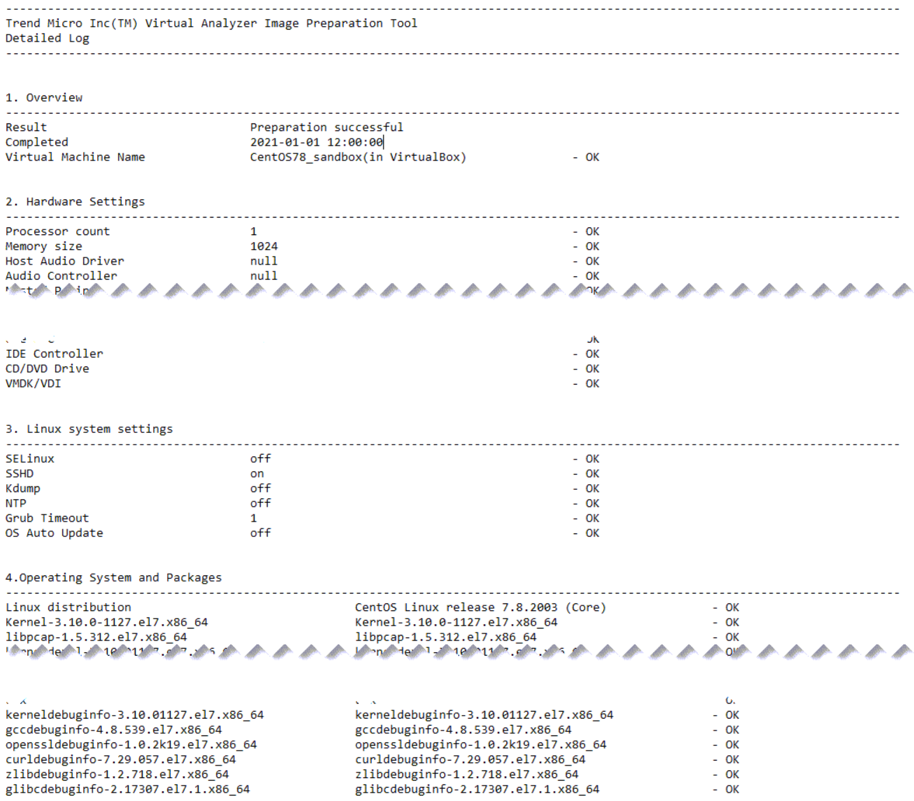
```
---------------------------------------------------------------------------------------------------------------
Trend Micro Inc(TM) Virtual Analyzer Image Preparation Tool
Detailed Log
---------------------------------------------------------------------------------------------------------------


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.



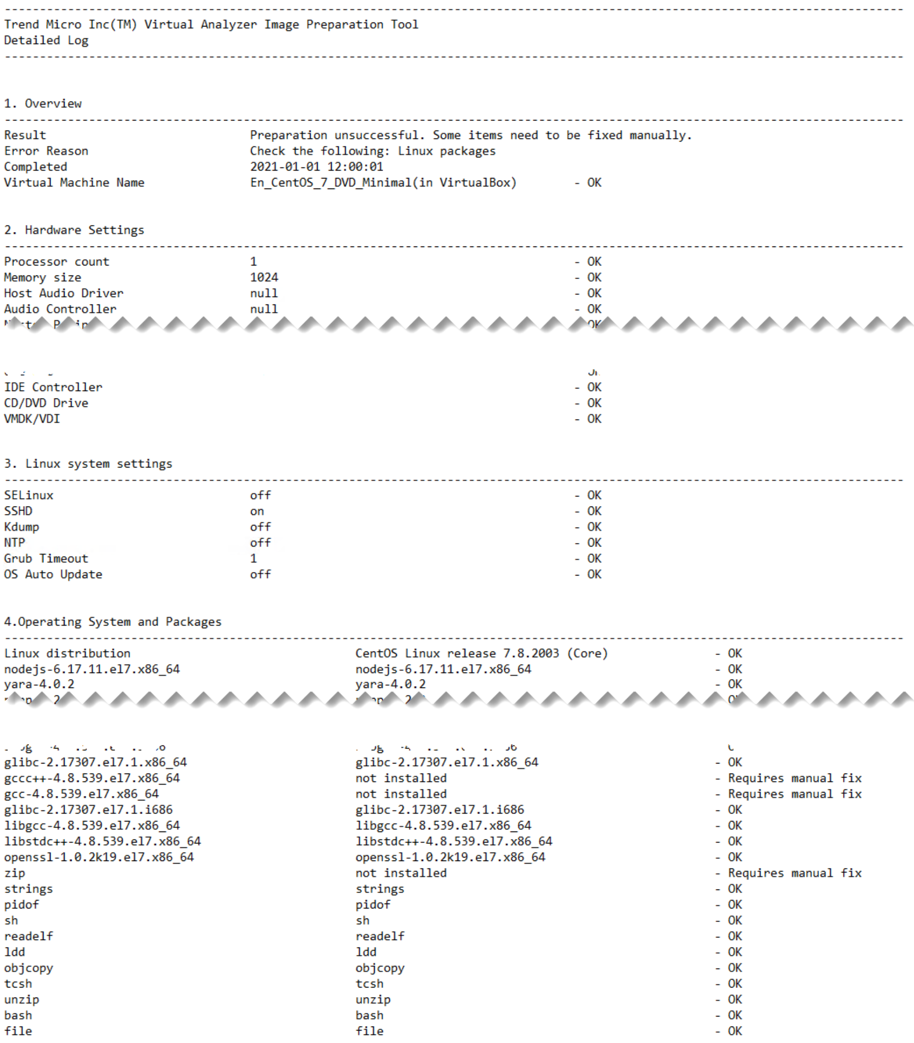
```
----------------------------------------------------------------------------------------------------------------
Trend Micro Inc(TM) Virtual Analyzer Image Preparation Tool
Detailed Log
----------------------------------------------------------------------------------------------------------------


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

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

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: APTM79813/230816