TREND MICRO™

6.2 TREND MICRO™ Virtual Analyzer Image Preparation Tool

User's Guide

Document Part No.: APEM629665/221221

Release Date: January 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 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 2-6*.

3. Create a virtual machine image.

   For details, see *Creating Windows Virtual Machine Images on page 2-7*.

4. Modify the environment of the virtual machine image.

   For details, see *Modifying the Virtual Machine Environment on page 2-27*.

5. Reduce the size of the VirtualBox Disk Image.

   For details, see *Reducing the Size of VirtualBox Disk Images on page 2-36*.

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

   For details, see *Exporting Virtual Machine Images to OVA Files on page 2-38*.

Required Software

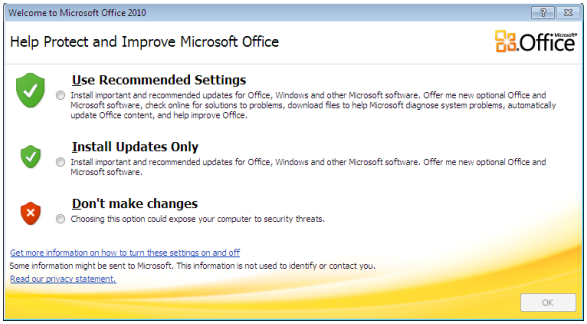
The following software must be installed on the virtual machine to achieve satisfactory detection results.

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 Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019. **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) **Important** • For Office 2007 and after, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and Microsoft Publisher must be installed. • Activate Microsoft Office with a valid product key after the tool has validated and modified virtual machine settings. Do not activate Microsoft Office before that. • After installation, open all Microsoft Office applications and verify that the main editing screen is displayed. If any confirmation dialog or welcome screen displays, make any selection to close the screen and display the main editing screen.  **FIGURE 2-1. Help Protect and Improve Microsoft Office** • Verify that your license allows you to virtualize the applications. For details, see https://support.office.com. • Disable automatic updates. • Enable macros. For details, see Enable or disable macros in Office files

SOFTWARE	DESCRIPTION
Internet Browser	Virtual Analyzer supports the following internet browsers: Microsoft Edge (Chromium-based version), Internet Explorer **Important** • The default browser must be set to a supported internet browser. • For Windows 8.1 and before, the tool will automatically configure Internet Explorer as the default browser. • For Windows 10, 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.

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

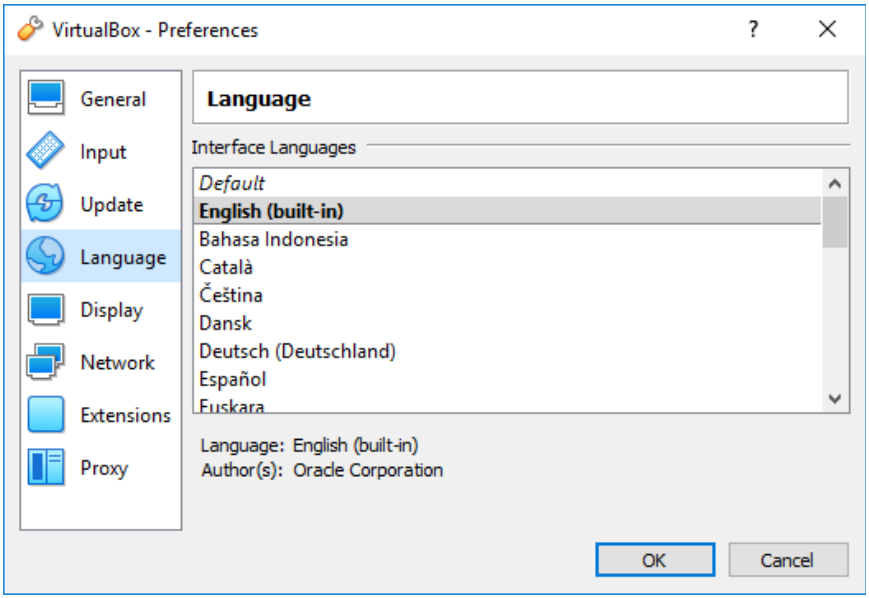


FIGURE 2-2. Language Settings

Creating Windows Virtual Machine Images

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.

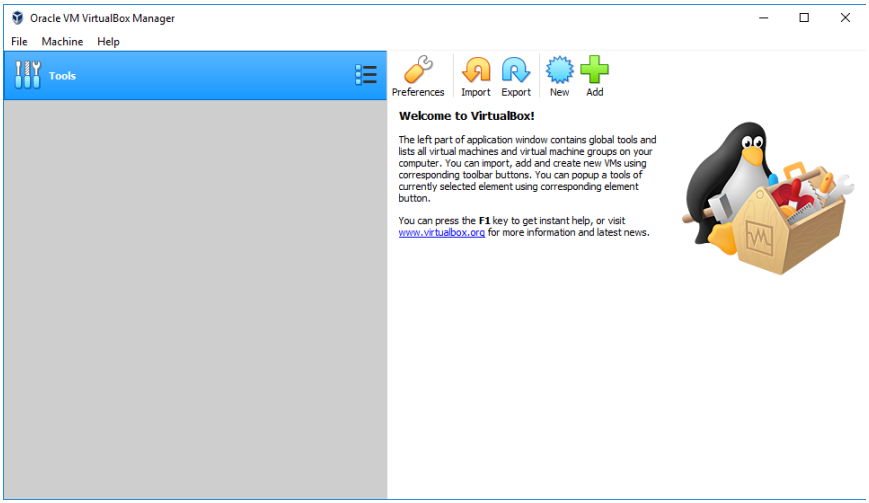


FIGURE 2-3. VirtualBox Manager

2. Click **New**.

The **Create Virtual Machine** window opens.

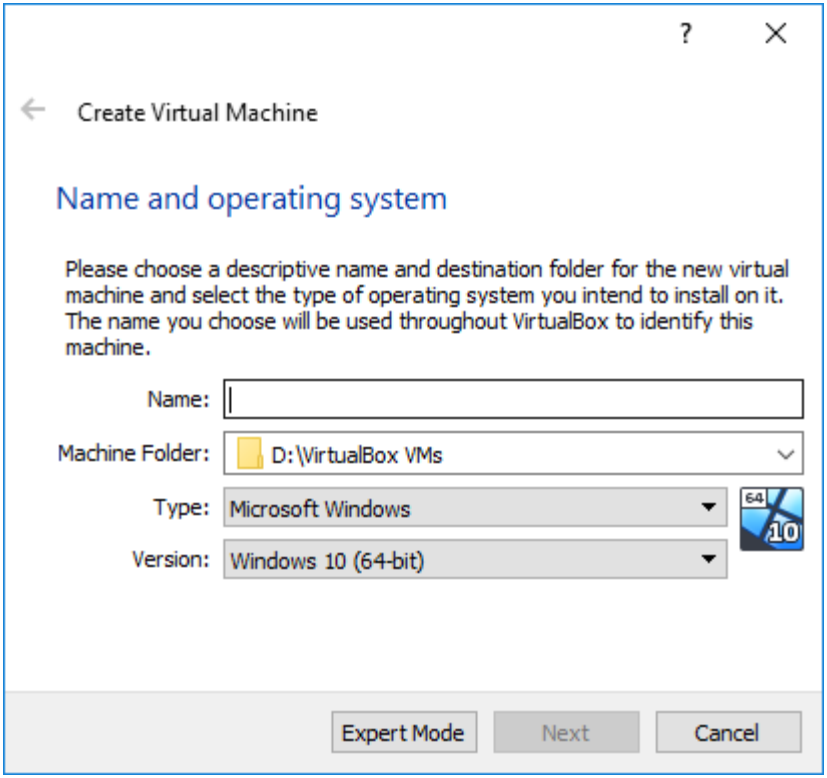


FIGURE 2-4. Create Virtual Machine

3. On the **Name and operating system** screen, configure the following:

   - **Name**: Type a permanent name for the virtual machine.
   - **Type**: Select **Microsoft Windows**.
   - **Version**: Select **Windows XP**, **Windows 2003**, **Windows 7**, **Windows 8**, **Windows 8.1**, **Windows 10**, **Windows 2008/2008 R2**, **Windows 2012/2012 R2**, **Windows 2016**, or **Windows 2019**.

4. Click **Next**.

   The **Memory size** screen appears.

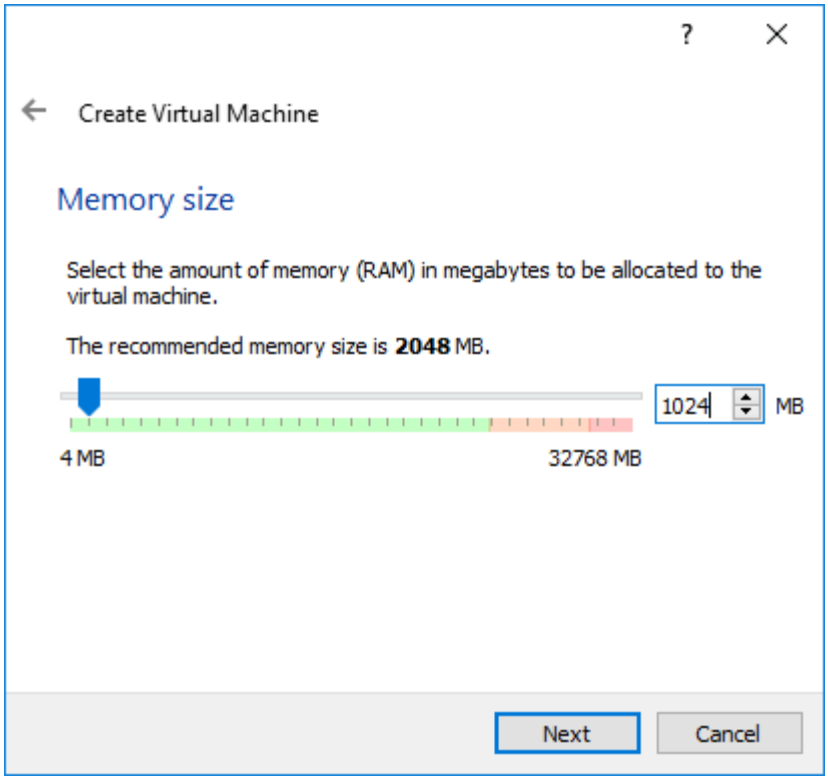


FIGURE 2-5. Memory Size

5. Specify the recommended memory size for your operating system.

   - Windows XP and Windows Server 2003: 512 MB
   - Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019: 1024 MB

6. Click **Next**.

   The **Hard disk** screen appears.

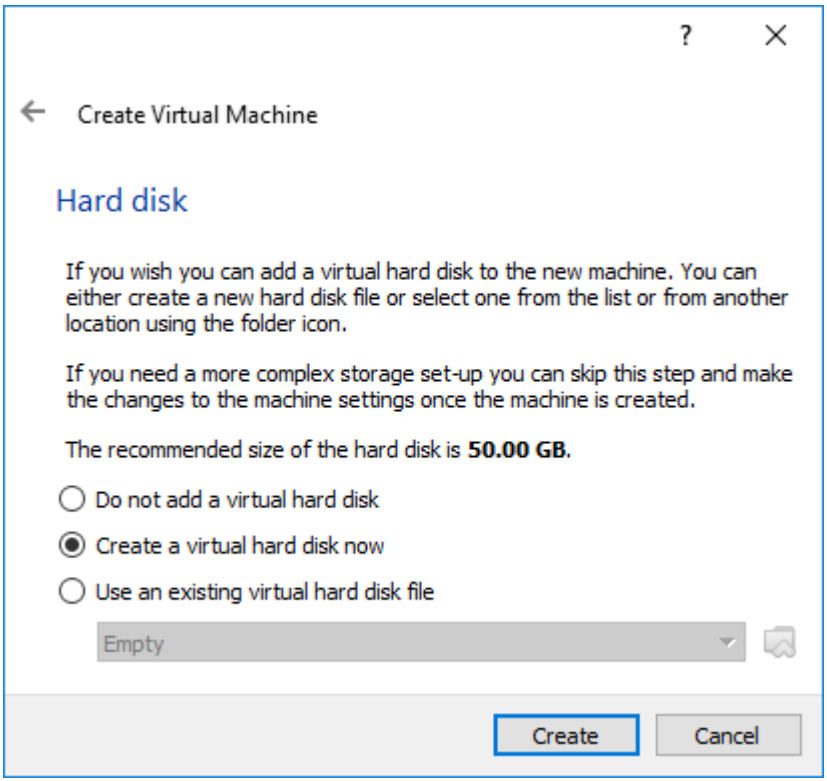


FIGURE 2-6. Hard Disk

7. Select **Create a virtual hard disk now** and then click **Create**.

The **Hard disk file type** screen appears.

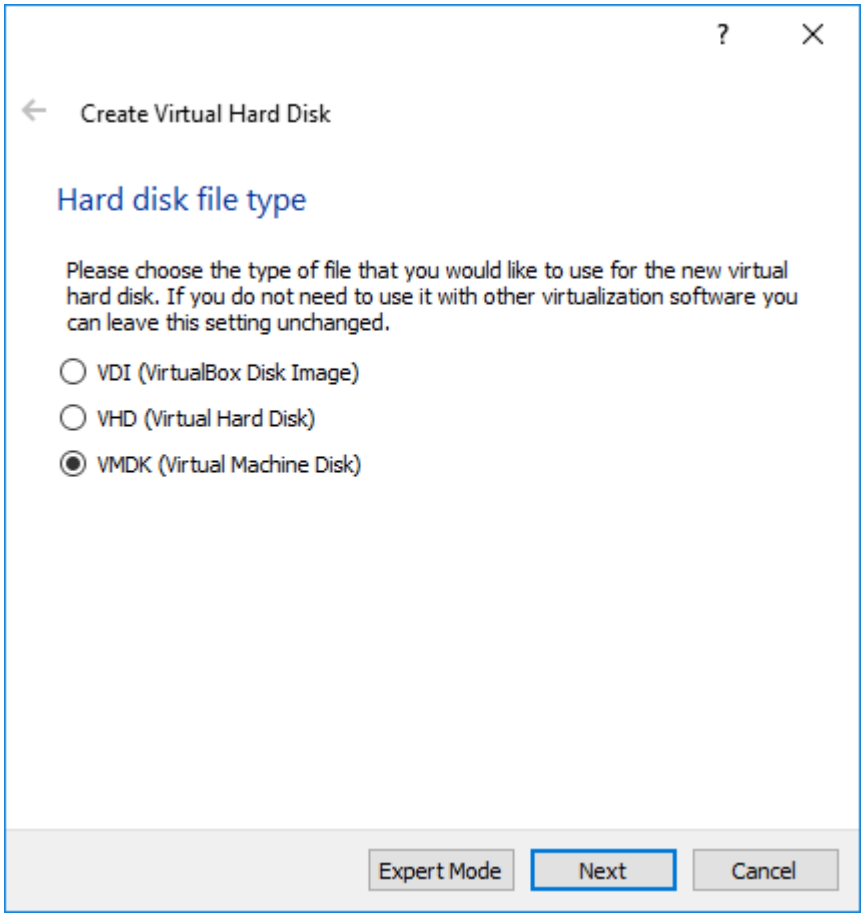


FIGURE 2-7. Hard Disk File Type

8. Select **VDI (VirtualBox Disk Image)** or **VMDK (Virtual Machine Disk)** and then click **Next**.

The **Storage on physical hard disk** screen appears.

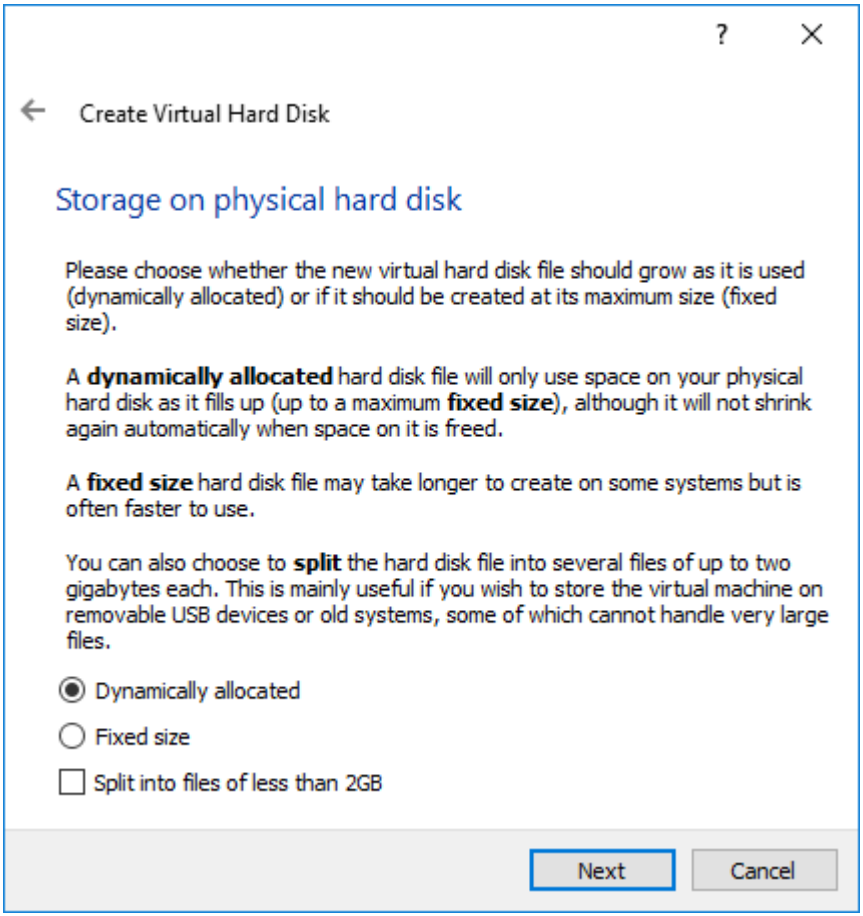


FIGURE 2-8. Storage on Physical Hard Disk

9. Select **Dynamically allocated** and then click **Next**.

Important

Do not select **Fixed size** or **Split into files of less than 2GB**.

The **File location and size** screen appears.

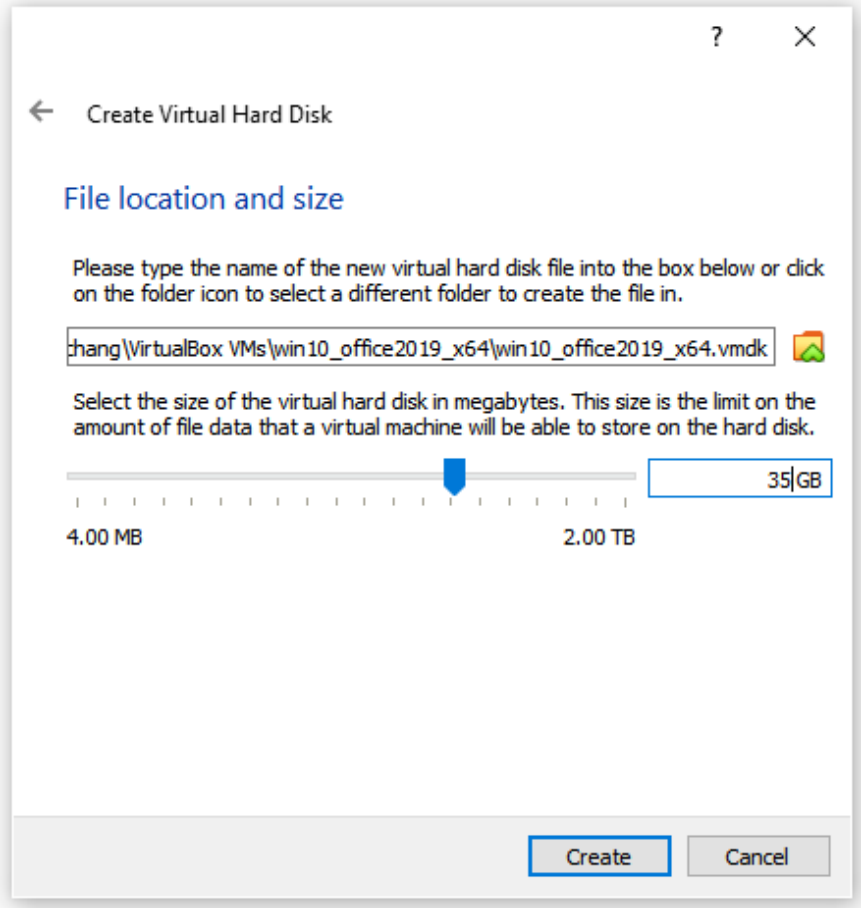


FIGURE 2-9. File Location and Size

10. (Optional) Click the folder icon to change the path of the virtual disk file.
11. Specify the virtual disk size for your operating system.
    - Windows XP and Windows Server 2003: 15 GB

- Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019: 35 GB

Note

Trend Micro recommends specifying a larger virtual disk size if you intend to install additional software.

12. Click **Create**.

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

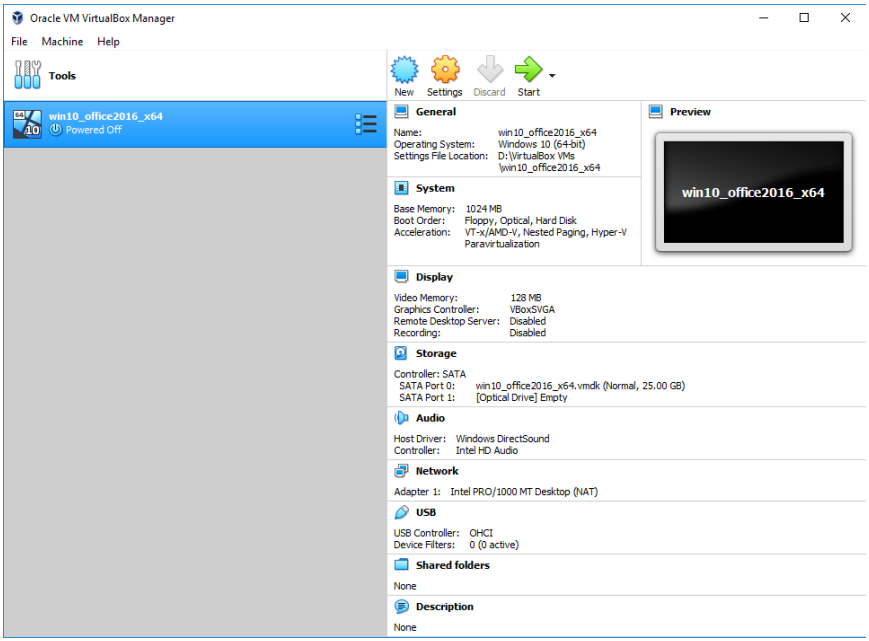


FIGURE 2-10. Newly-created Virtual Machine

Ensure that the virtual machine is not in any group.

13. Click **Settings**.

    The **Settings** window opens.

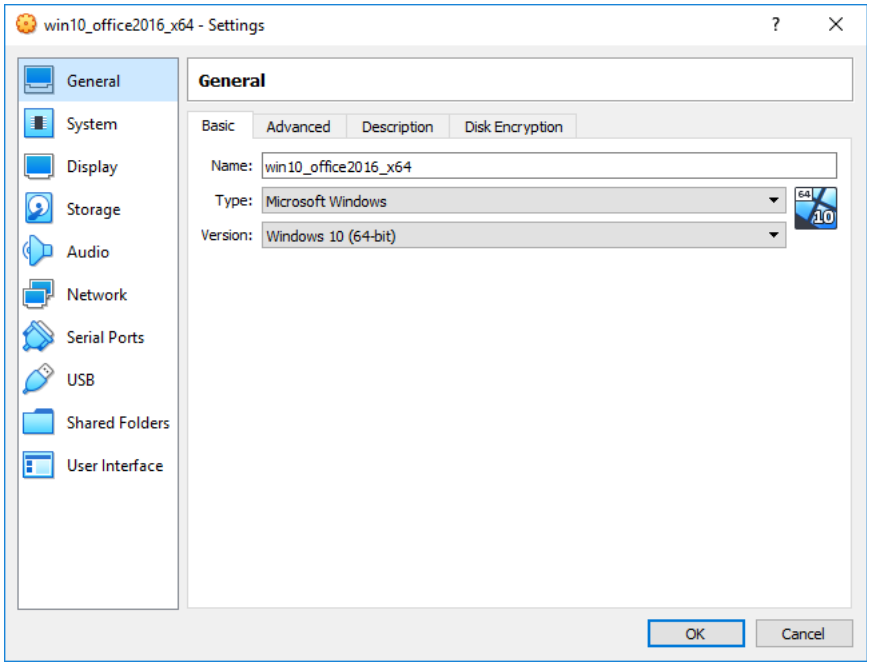


FIGURE 2-11. VirtualBox Settings

14. In the left pane, click **System**.

The **System** screen appears.

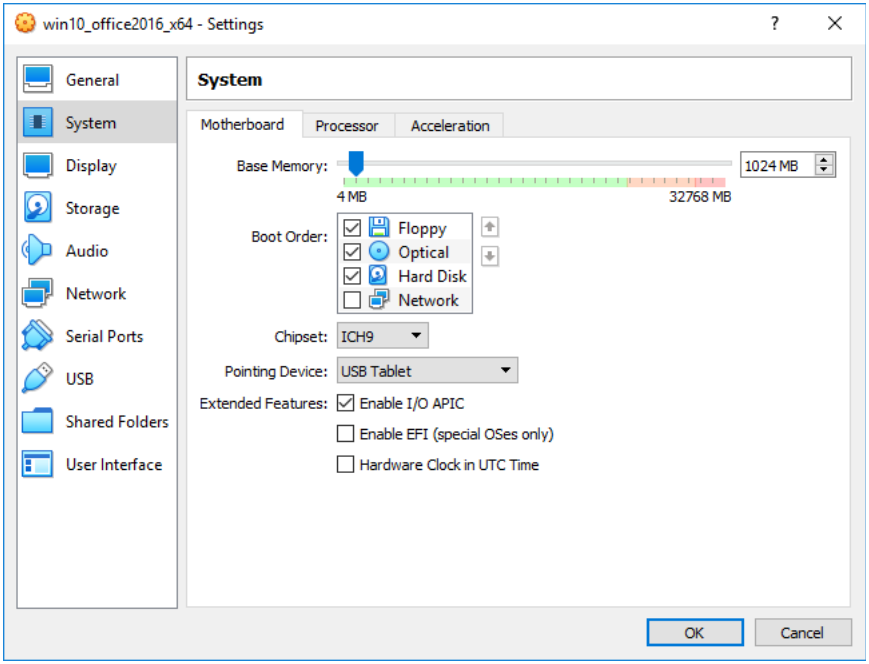


FIGURE 2-12. System Screen

15. On the **Motherboard** tab, configure the following:
    - **Chipset**: Select **ICH9**
    - **Pointing Device**: Select **USB Tablet**
    - **Extended Features**:
        - Select **Enable I/O APIC**
        - (Optional) Select **Enable EFI (special OSes only)** if you want to create an EFI-compatible image. EFI-compatible images are only supported by the following 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

16. Go to the **Processor** tab and then select **Enable PAE/NX**.

17. Go to the **Acceleration** tab and then select **Enable Nested Paging**. If you are using VirtualBox 5.2 and before, select **Enable VT-x/AMD-V** as well.

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.

18. In the left pane, click **Storage**.

The **Storage** screen appears.

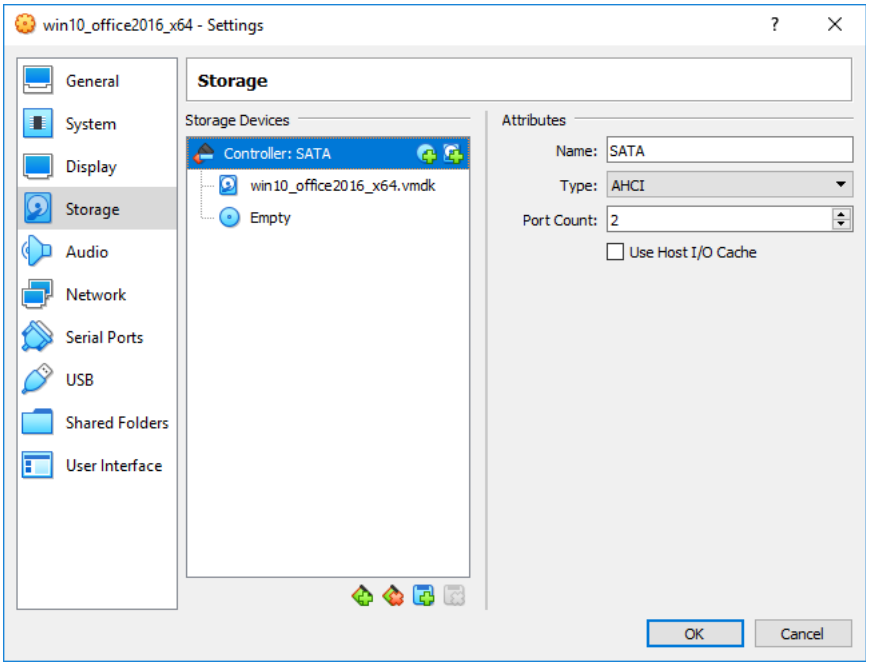


FIGURE 2-13. Storage Screen

19. If **Controller: SATA** appears under **Storage Tree**, remove the SATA controller and then add an IDE controller.

    a. Click **Controller: SATA** and then click to remove the default controller.

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

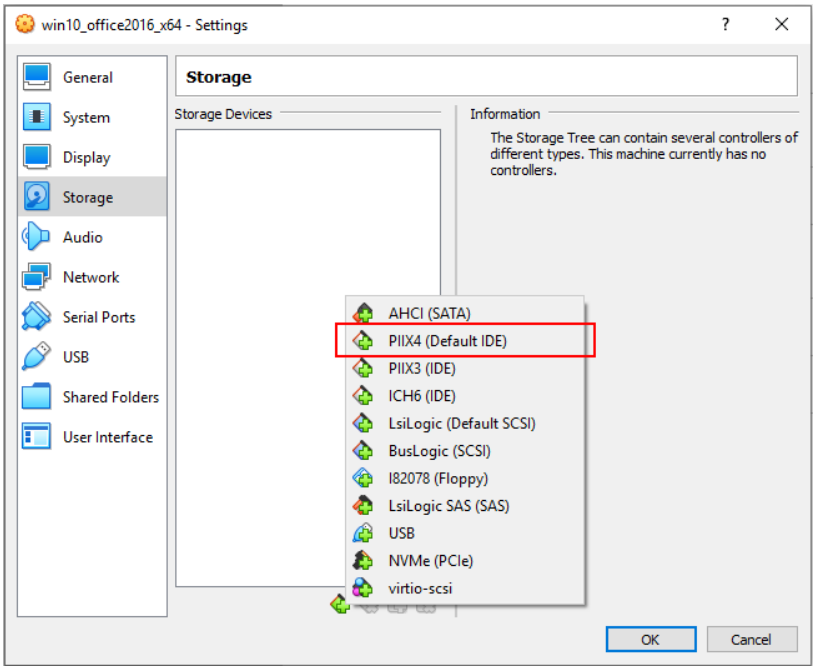


FIGURE 2-14. Add Storage Controller

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

The following window appears:

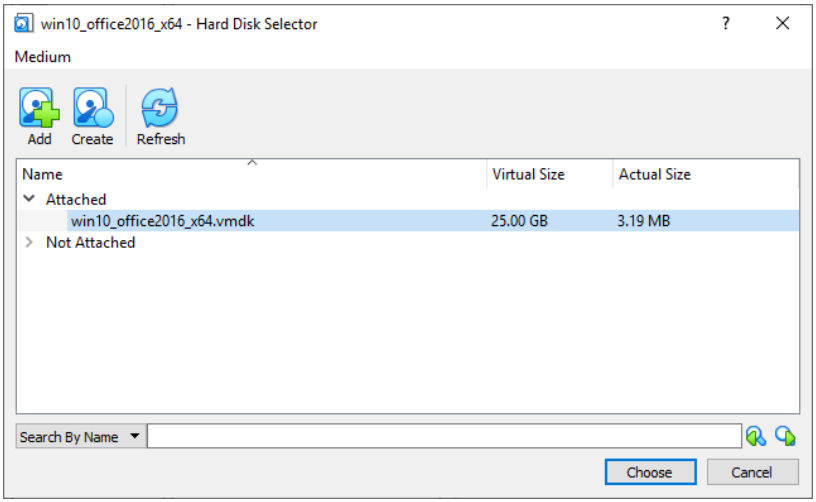


FIGURE 2-15. Hard Disk Selector

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

e. Under **Attributes**, verify that **Hard Disk** is **IDE Primary Device 0**.

f. Under **Storage Tree**, click **Controller: IDE** and then click .

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

h. Under **Attributes**, verify that **CD/DVD Drive** is **IDE Secondary Device 0**.

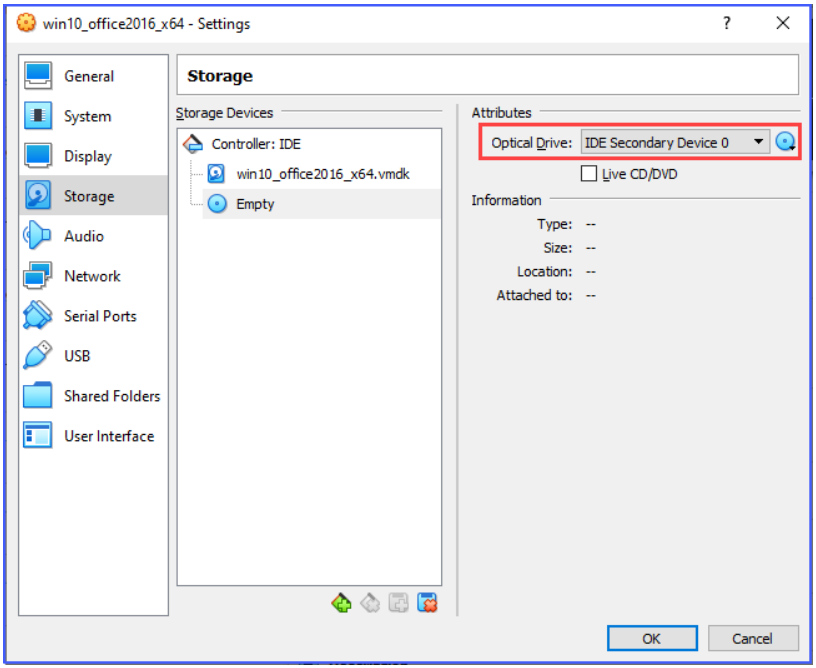


FIGURE 2-16. IDE Secondary Device 0

20. Under **Attributes**, click , and then select **Choose a virtual CD/DVD disk file...**.

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

    The ISO file is available as a device.

22. Verify that there is only one **Controller: IDE** controller. Remove any other controllers by clicking on the controller and then clicking .

23. (Optional) In the left pane, click **Audio** and verify that **Enable Audio** is enabled.

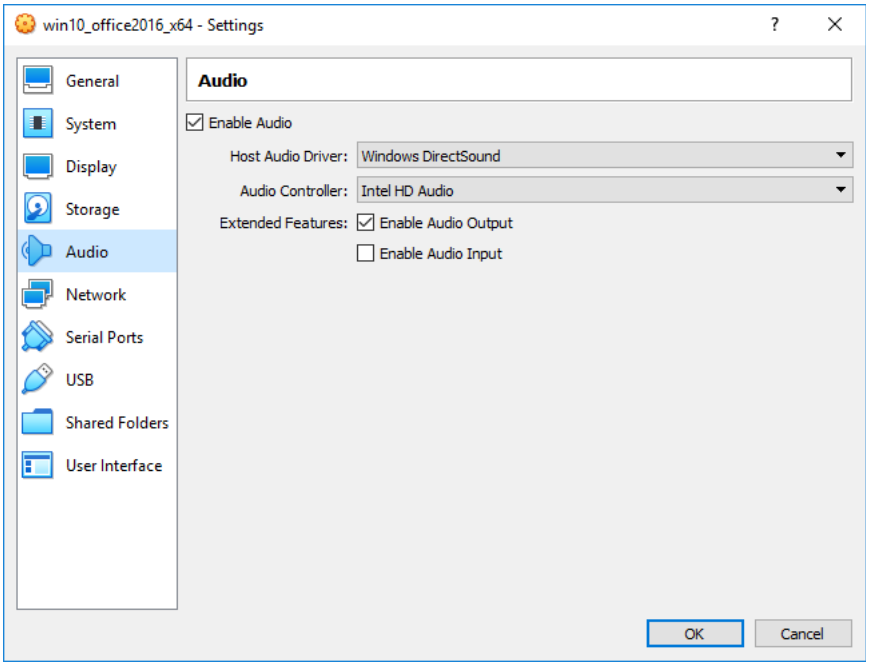


FIGURE 2-17. Audio Options Settings

24. In the left pane, click **USB** and then select **Enable USB Controller**.

Important

Verify that **USB 1.1 (OHCI) Controller** is selected.

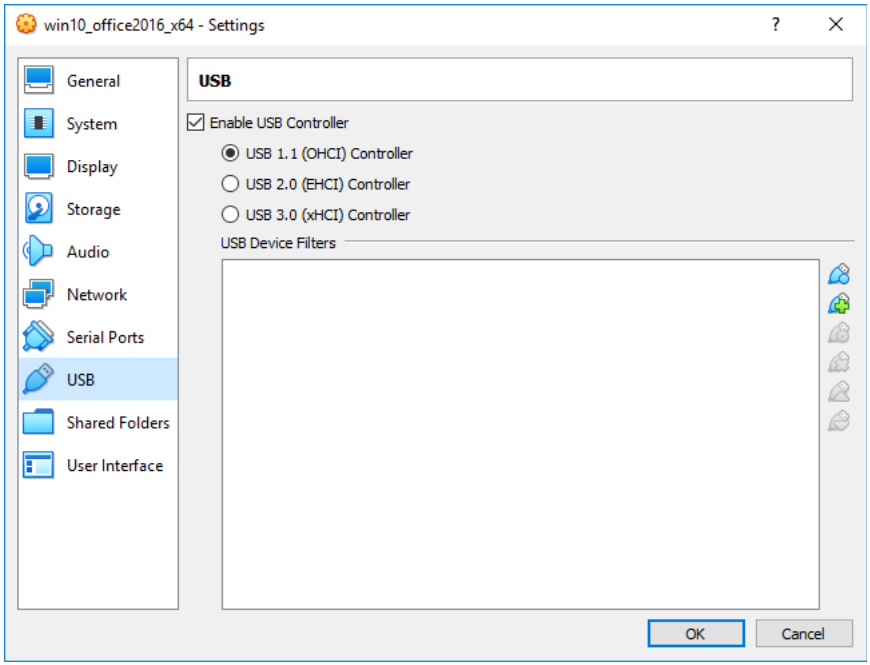


FIGURE 2-18. Enable USB Controller

25. In the left pane, click **Shared Folders** and then verify that no folders are shared.

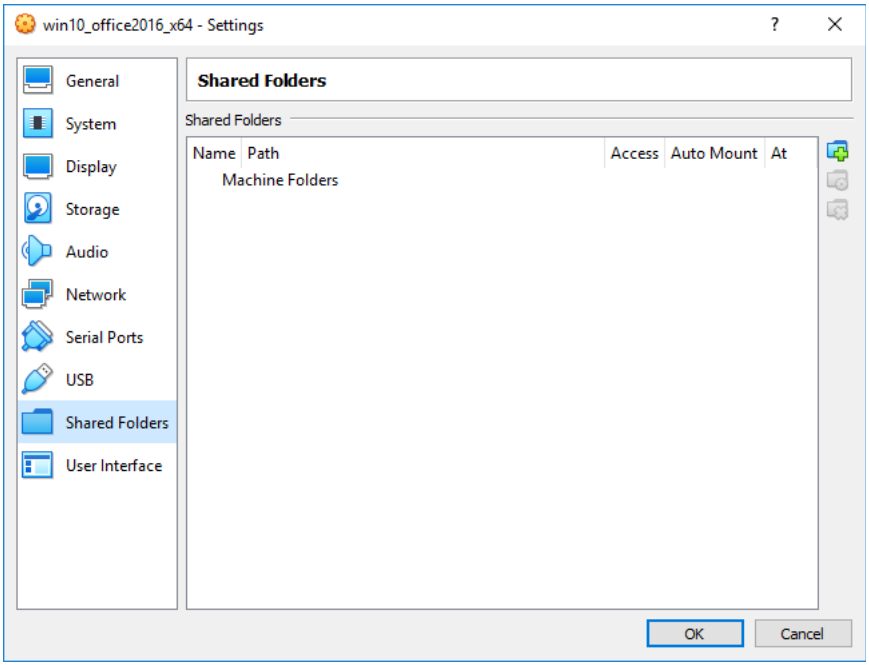


FIGURE 2-19. Shared Folders Settings

26. Click **OK**.

    The **Settings** window closes.

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

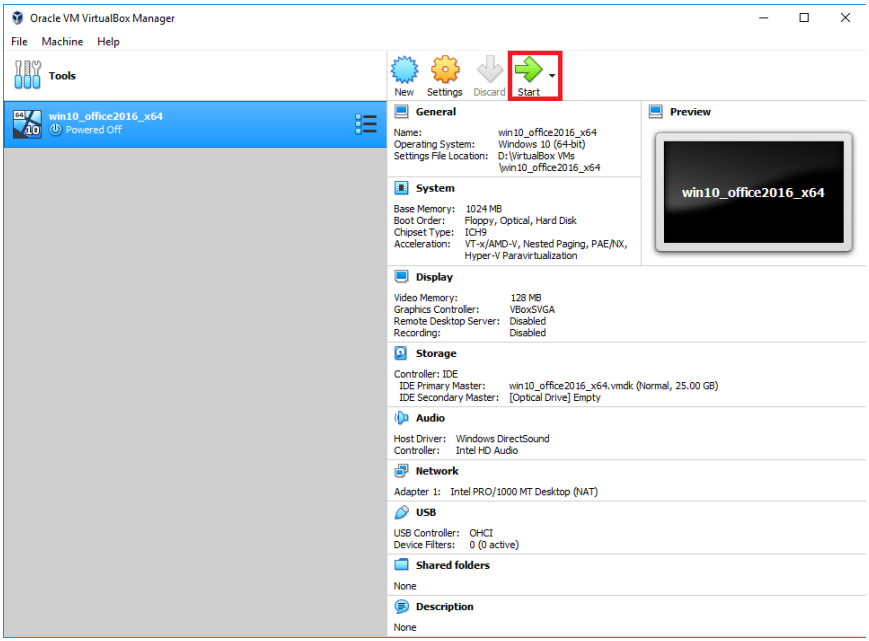


FIGURE 2-20. VirtualBox Manager

The installation process starts.

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

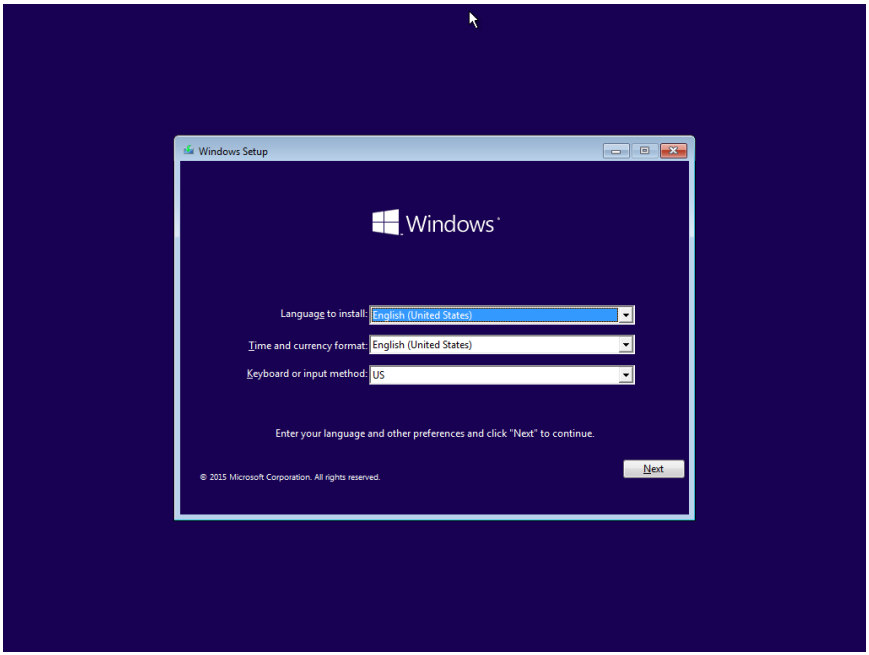


FIGURE 2-21. Operating System Installation Process

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

Important

Ensure that you have at least 3072 MB free virtual disk space on the virtual machine to ensure normal operation of Virtual Analyzer.

Modifying the Virtual Machine Environment

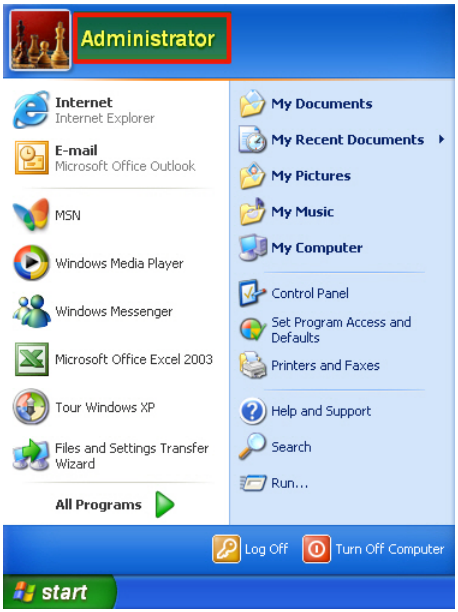
Modify the virtual machine environment to run Virtual Analyzer Sensors, a collection of utilities that execute and detect malware, and record all behavior in Virtual Analyzer.

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

Procedure

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

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

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

TASK	STEPS
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.

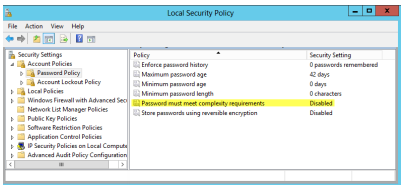
3. Restart the virtual machine.

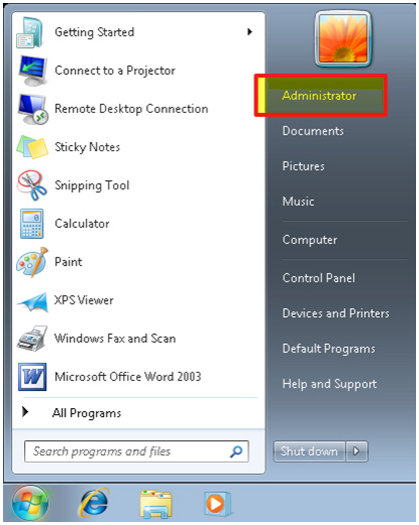
Modifying the Virtual Machine Environment (Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019)

Procedure

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

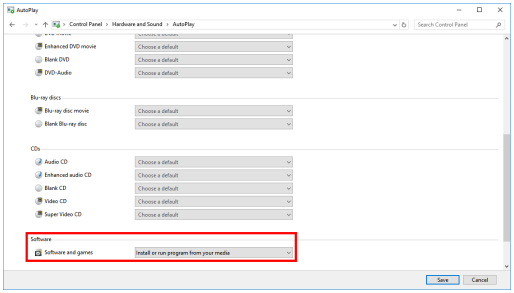
TASK	STEPS
Enable the "Administrator" account	Type **`net user "Administrator" /active:yes`**.

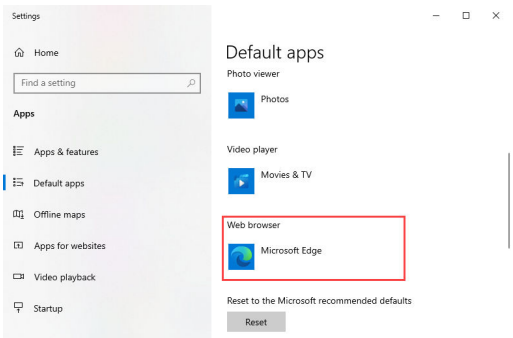
TASK	STEPS
Set the logon password for the “Administrator” account to “1111”	Type **`net user "Administrator" 1111`**.
Configure automatic logon from the administrator account **Note** Each time the image starts, the logon prompt is bypassed and the “Administrator” account is automatically used to log 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`** **Note** In Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019, launch the **Local Security Policy** snap-in (`secpol.msc`) to disable the **Password must meet complexity requirements** Local Security Setting.  **FIGURE 2-23. Disable Password must meet complexity requirements** • Restart the image.

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

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

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

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

Task	Steps
Configure default web browser on Windows 10	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 before running the Virtual Analyzer. To configure the default web browser, perform the following: **Note** The Virtual Analyzer does not support Microsoft Edge Legacy. You can quickly check which version of Microsoft Edge is installed by comparing the icon: • Microsoft Edge (Chromium): • Microsoft Edge Legacy: a. Open the Windows **Start** menu, type **`Default apps`** and press ENTER. b. Under **Web browser**, select the current web browser.  **Figure 2-26. Default apps** c. In the **Choose an app** context menu, select **Internet Explorer** or **Microsoft Edge**. d. If the **Before you switch** dialog appears, select **Switch anyway**.

TASK	STEPS
(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. 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:

Creating Windows OVA Files Using Converted Virtual Hard Disk Drives

Procedure

1. Prepare Adobe Reader.

   For details, see *Preparing Adobe Reader on page 3-6*

2. Modify the environment of the virtual machine image.

   For details, see *Modifying the Virtual Machine Environment on page 3-7*.

3. Export the virtual machine image.

   For details, see *Exporting Virtual Machine Images on page 3-18*.

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 3-25*.

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 3-32*.

6. Configure the new virtual machine image.

   For details, see *Configuring Virtual Machine Images on page 3-49*.

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

   For details, see *Exporting Virtual Machine Images to OVA Files on page 3-54*.

Required Software

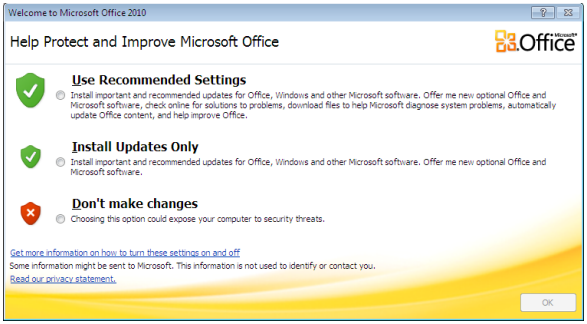
The following software must be installed on the virtual machine to achieve satisfactory detection results.

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 Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019. **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) **Important** • For Office 2007 and after, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and Microsoft Publisher must be installed. • Activate Microsoft Office with a valid product key after the tool has validated and modified virtual machine settings. Do not activate Microsoft Office before that. • After installation, open all Microsoft Office applications and verify that the main editing screen is displayed. If any confirmation dialog or welcome screen displays, make any selection to close the screen and display the main editing screen.  **FIGURE 3-1. Help Protect and Improve Microsoft Office** • Verify that your license allows you to virtualize the applications. For details, see https://support.office.com. • Disable automatic updates. • Enable macros. For details, see Enable or disable macros in Office files

SOFTWARE	DESCRIPTION
Internet Browser	Virtual Analyzer supports the following internet browsers: Microsoft Edge (Chromium-based version), Internet Explorer **Important** • The default browser must be set to a supported internet browser. • For Windows 8.1 and before, the tool will automatically configure Internet Explorer as the default browser. • For Windows 10, 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 3-7*
- *Modifying the Virtual Machine Environment (Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019) on page 3-10*
- *Uninstalling VMware Tools on page 3-16*

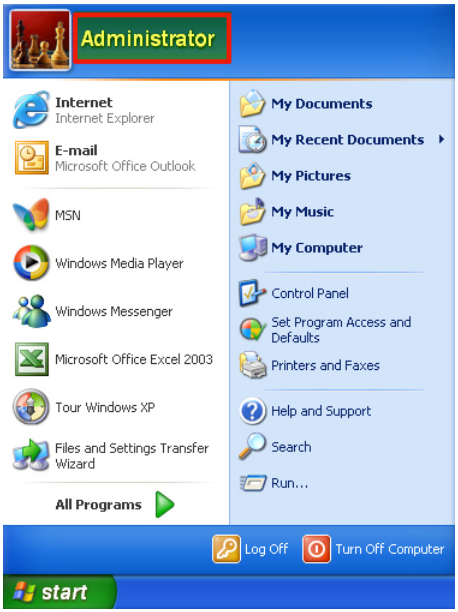
Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003)

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`**

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 DefaultUserName /t REG_SZ /d Administrator /f` • `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f` • `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f` b. Restart the image.

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

TASK	STEPS
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 3-16*.

3. Restart the virtual machine.

Modifying the Virtual Machine Environment (Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019)

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`**.

<table>
<tr><th>TASK</th><th>STEPS</th></tr>
<tr><td>Set the logon password for the “Administrator” account to “1111”.</td><td>Type <code>net user "Administrator" 1111</code>.</td></tr>
<tr><td>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.</td><td>a. Type the following commands:
• <code>REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f</code>
• <code>REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f</code>
• <code>REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f</code>

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

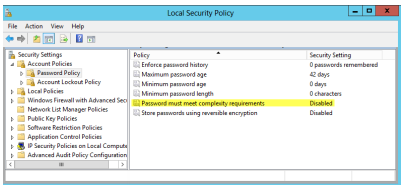
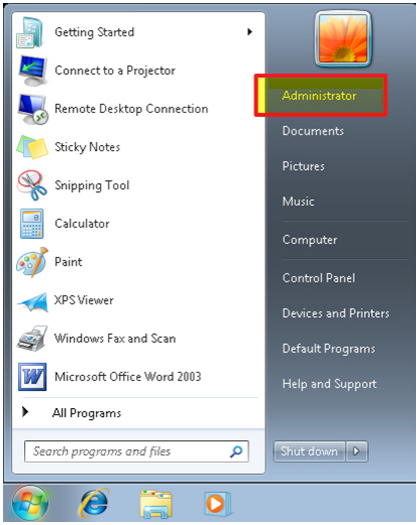
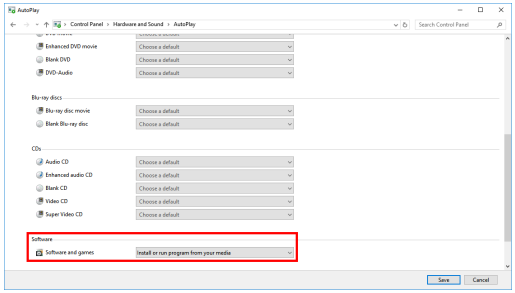
 

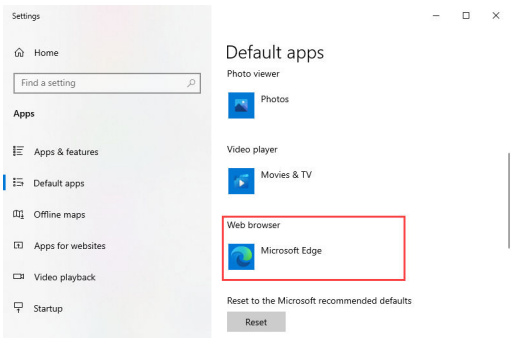
FIGURE 3-3. Disable Password must meet complexity requirements
• Restart the image.</td></tr>
</table>

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

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

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

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

Task	Steps
Configure default web browser on Windows 10	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 before running the Virtual Analyzer. To configure the default web browser, perform the following: **Note** The Virtual Analyzer does not support Microsoft Edge Legacy. You can quickly check which version of Microsoft Edge is installed by comparing the icon: • Microsoft Edge (Chromium): • Microsoft Edge Legacy: a. Open the Windows **Start** menu, type **`Default apps`** and press ENTER. b. Under **Web browser**, select the current web browser.  **Figure 3-6. Default apps** c. In the **Choose an app** context menu, select **Internet Explorer** or **Microsoft Edge**. d. If the **Before you switch** dialog appears, select **Switch anyway**.

TASK	STEPS
(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 3-16*.

4. 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.

   - Windows XP and Windows Server 2003: Click **Add or Remove Programs**.
   - Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019: Click **Programs and Features**.

A list of installed programs appears.

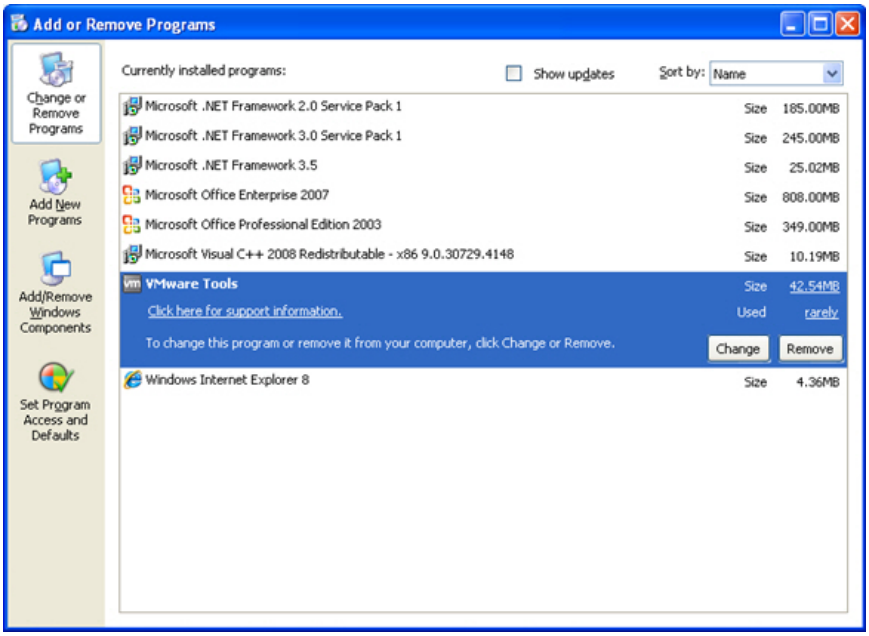


FIGURE 3-7. Add or Remove Programs (Windows XP)

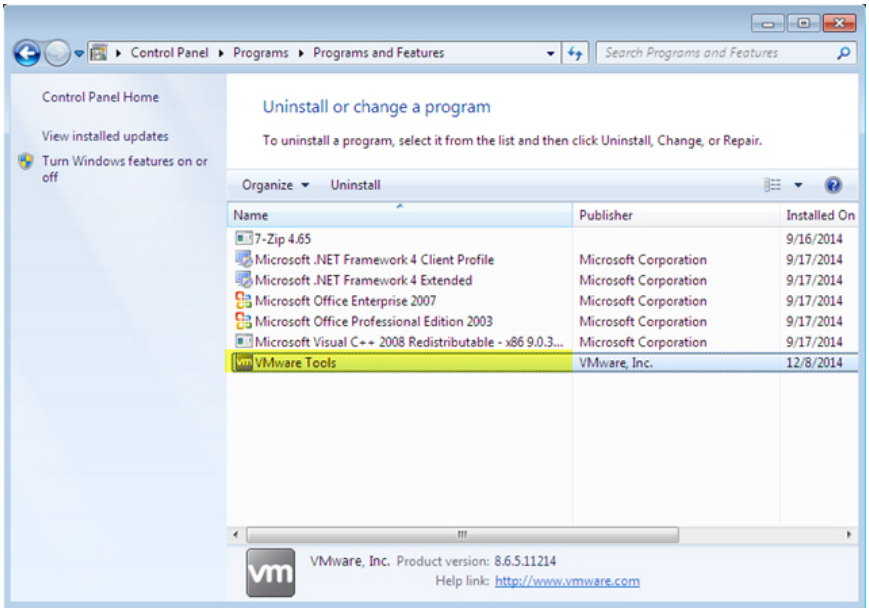


FIGURE 3-8. Add or Remove Programs (Windows 7)

3. Select **VMware Tools** and then click **Remove** (Windows XP or Windows Server 2003) or **Uninstall** (Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, or Windows Server 2019).
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

Procedure

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

   The **Virtual Machine Settings** screen appears.

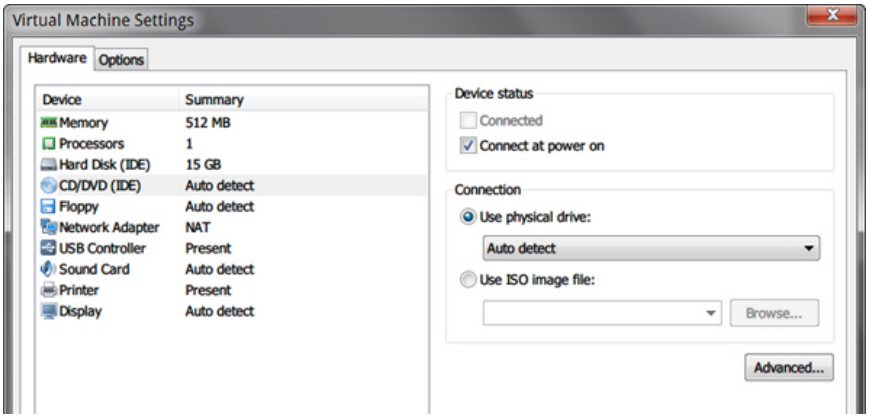


FIGURE 3-9. Virtual Machine Settings

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

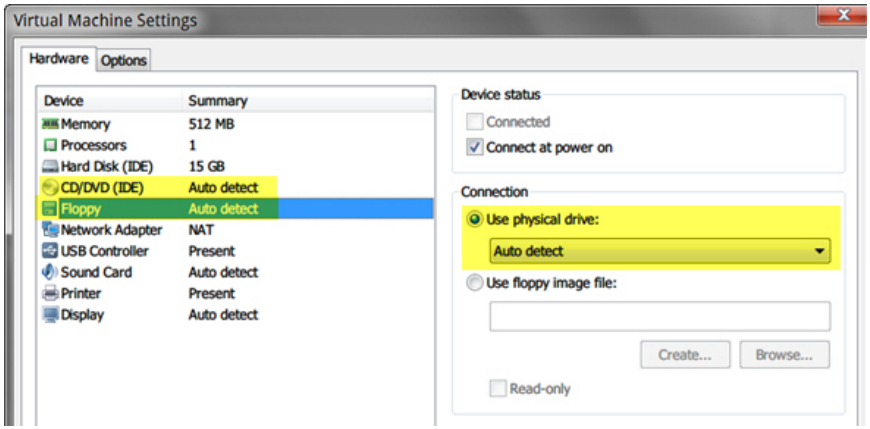


FIGURE 3-10. Virtual Machine Settings - Hardware

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

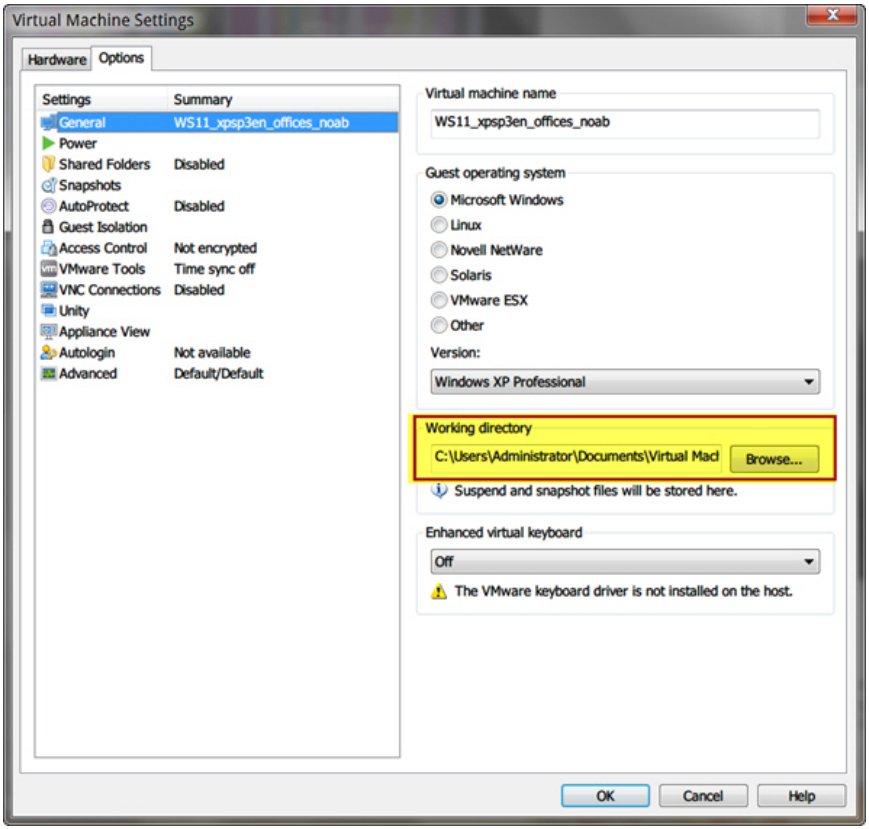


FIGURE 3-11. Working Directory

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**.

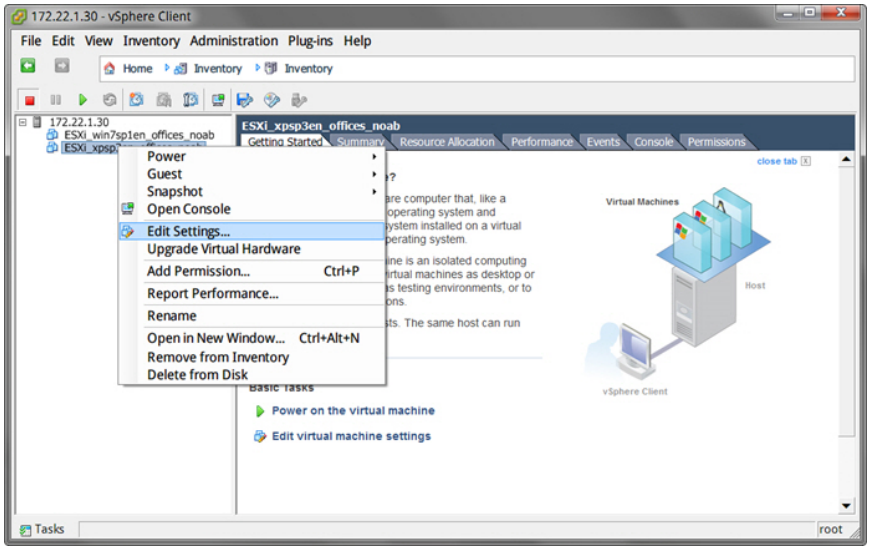


FIGURE 3-12. Edit Settings

The **Virtual Machine Properties** screen appears.

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

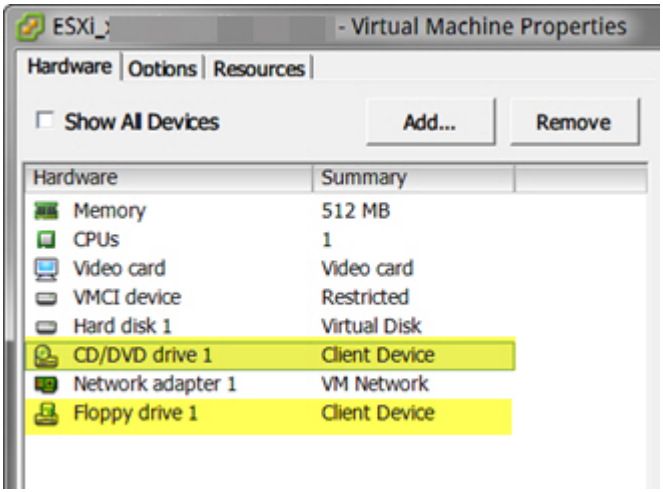


FIGURE 3-13. Virtual Machine Properties - Hardware

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

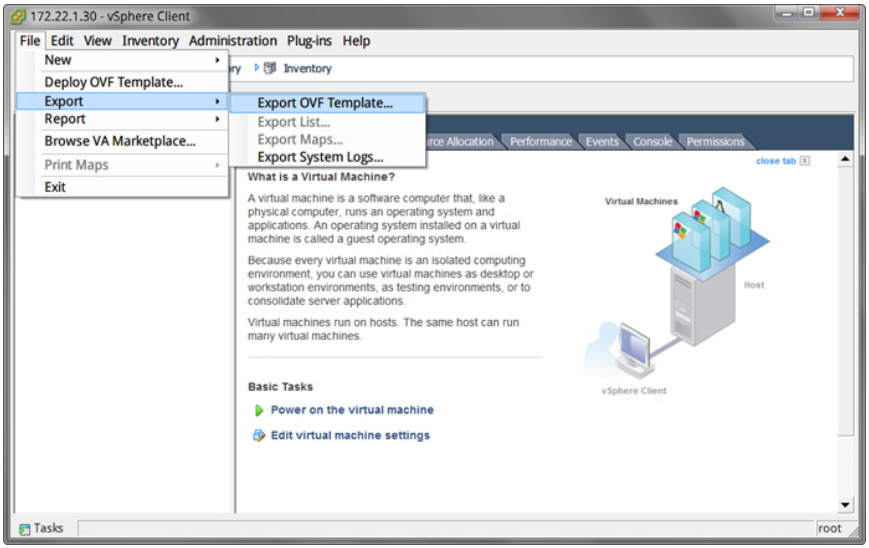


FIGURE 3-14. OVF Template

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 3-25*
- *Using QEMU on page 3-31*

Using VMware vCenter Converter Standalone

Procedure

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

   Note

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

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

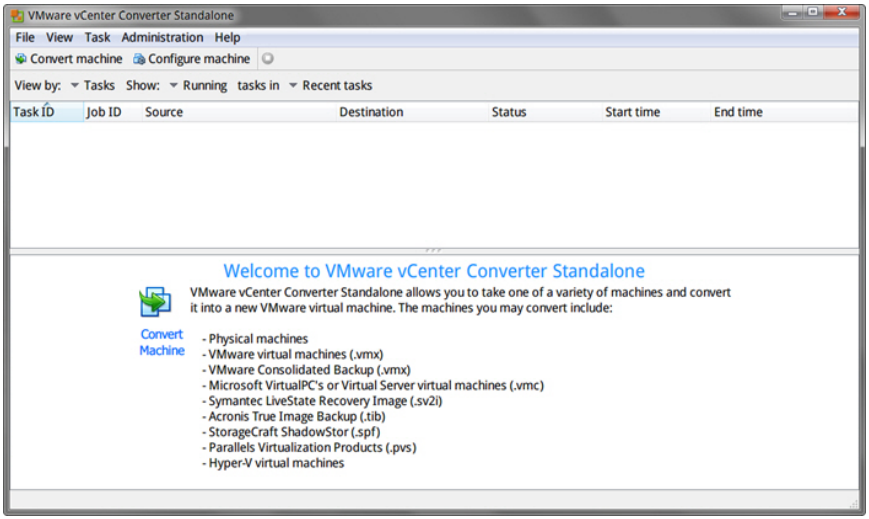


FIGURE 3-15. VMware vCenter Converter Standalone

The **Conversion** window opens.

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

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

   b. **Server**: Type the ESXi server IP address.

   c. **User name**, **Password**: Type the credentials that provide administrator access to the VMware server.

4. Click **Next**.

The **Source Machine** screen appears.

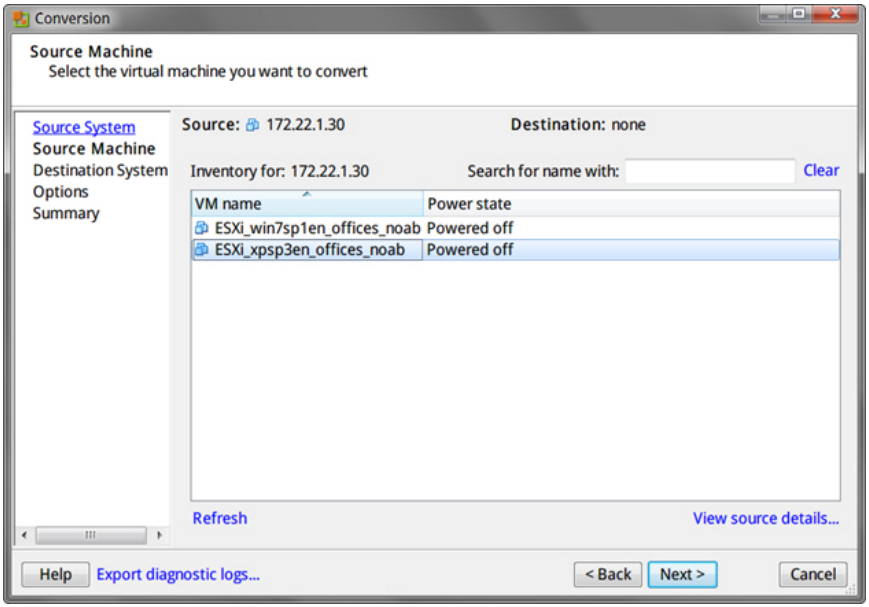


FIGURE 3-16. Conversion > Source Machine

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

The **Destination System** section appears.

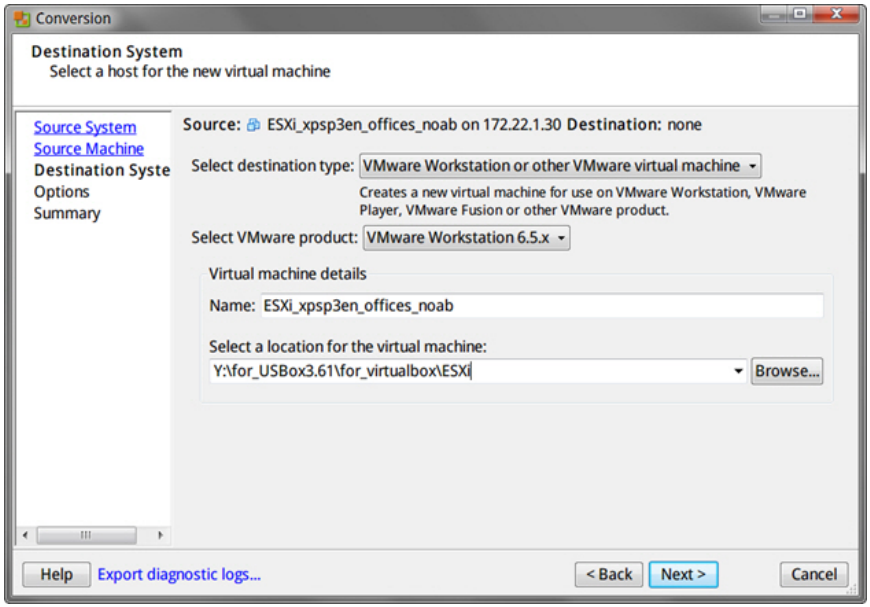


FIGURE 3-17. Conversion > Destination System

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

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

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

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

The **Options** screen appears.

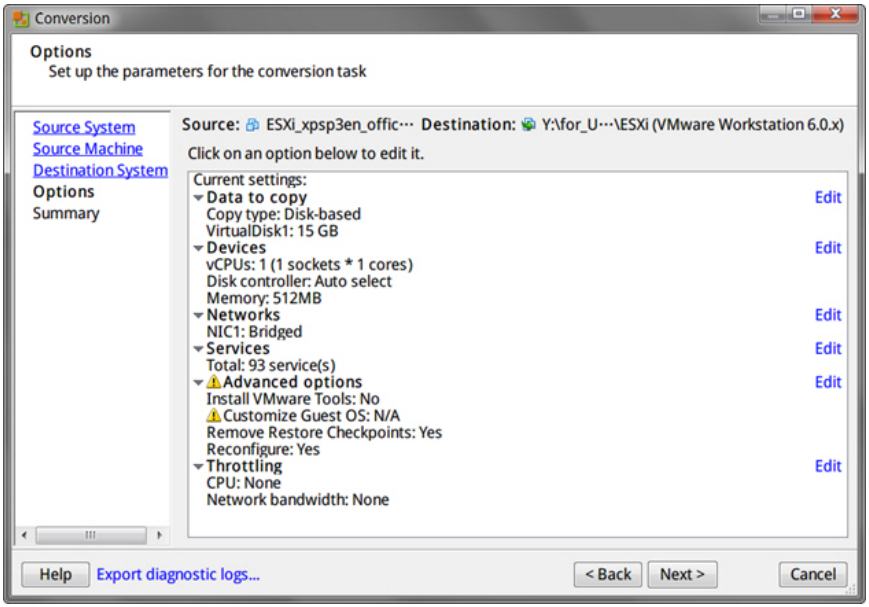


FIGURE 3-18. Conversion > Options

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

Important

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

The **Summary** screen appears.

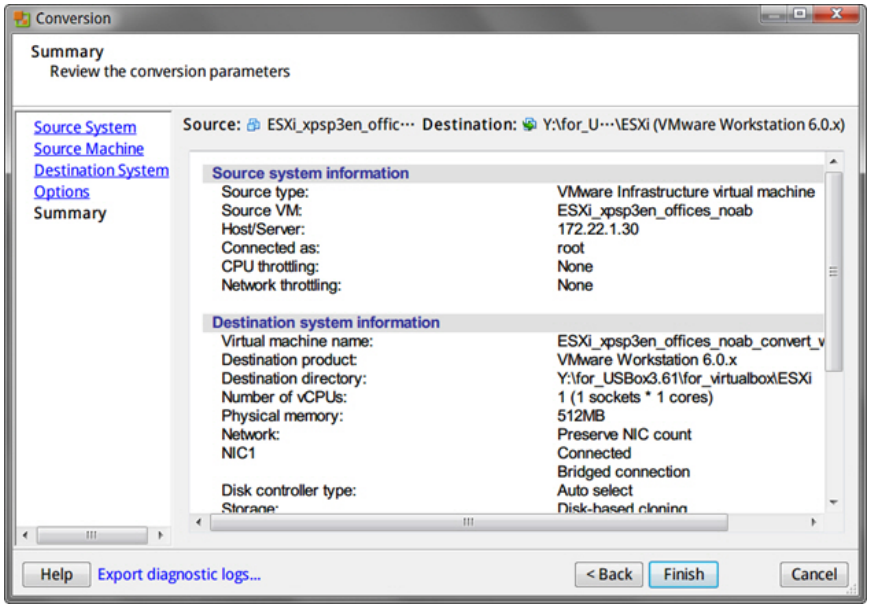


FIGURE 3-19. Conversion > Summary

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

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

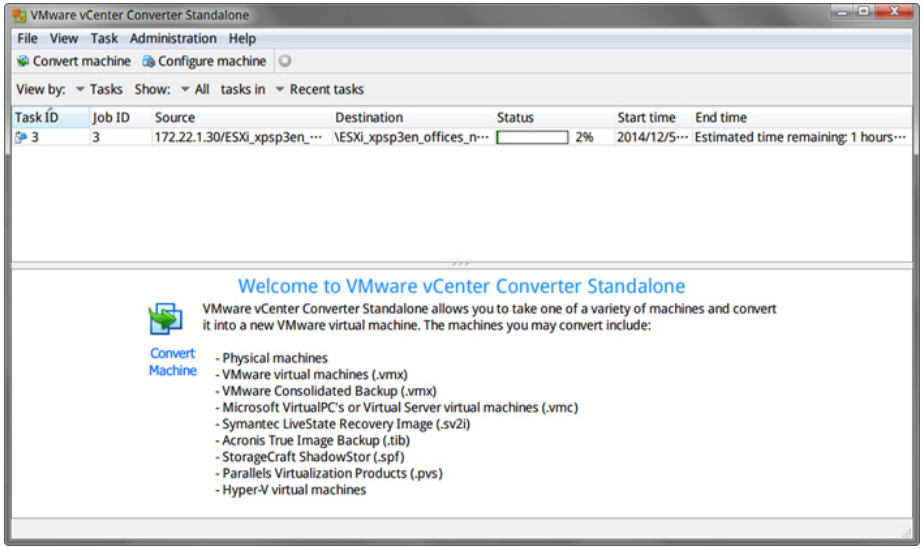


FIGURE 3-20. Image Conversion Progress

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 2-6*
- *Creating Virtual Machine Images Using VirtualBox on page 3-33*

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**.

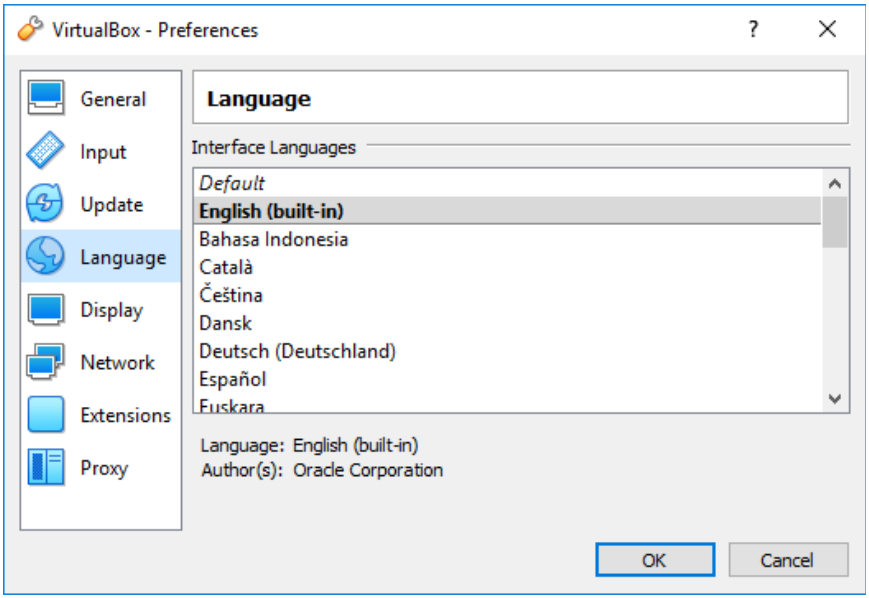


FIGURE 3-21. Language Settings

Creating Virtual Machine Images Using VirtualBox

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.

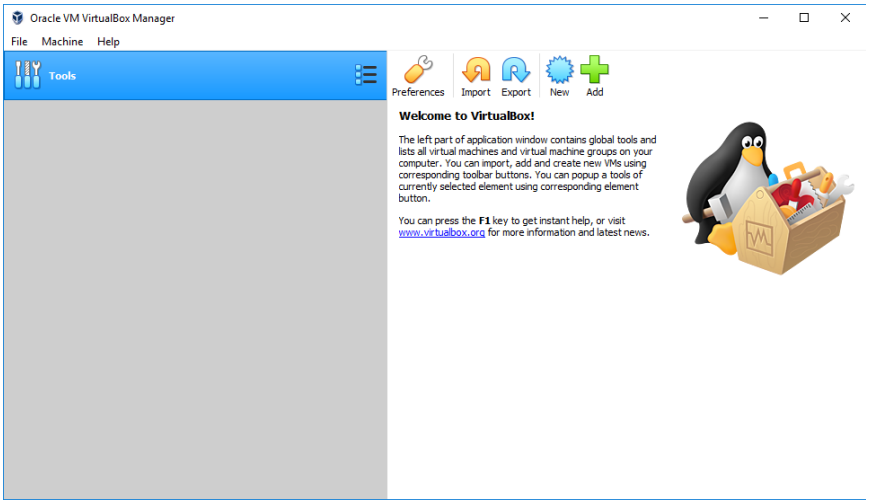


FIGURE 3-22. VirtualBox Manager

2. Click **New**.

The **Create Virtual Machine** window opens.

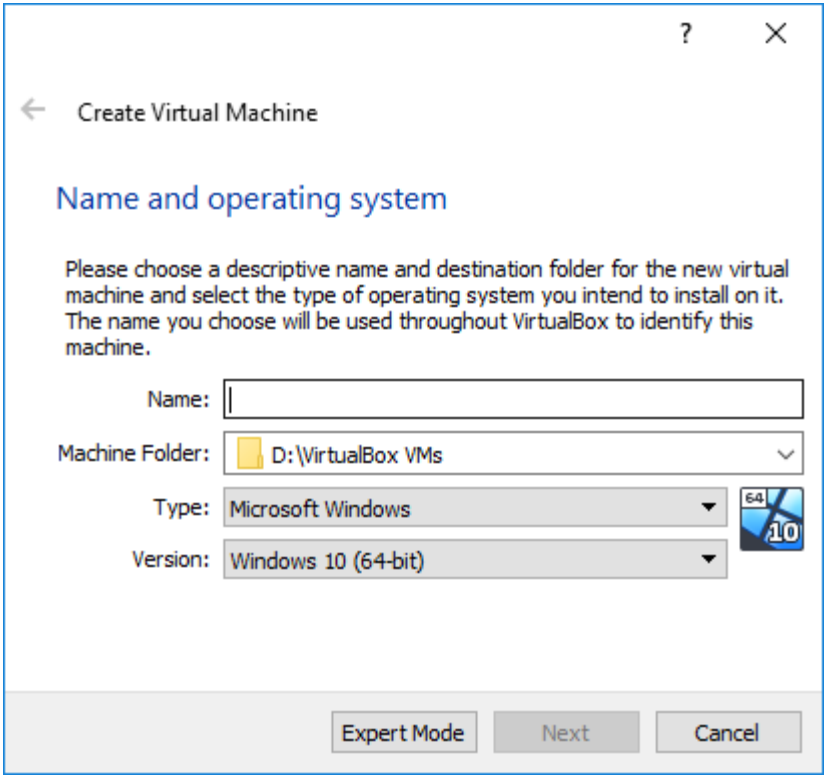


FIGURE 3-23. Create Virtual Machine

3. On the **Name and operating system** screen, configure the following:
   - **Name**: Type a permanent name for the virtual machine.
   - **Type**: Select **Microsoft Windows**.
   - **Version**: Select **Windows XP**, **Windows 2003**, **Windows 7**, **Windows 8**, **Windows 8.1**, **Windows 10**, **Windows 2008/2008 R2**, **Windows 2012/2012 R2**, **Windows 2016**, or **Windows 2019**.

4. Click **Next**.

   The **Memory size** screen appears.

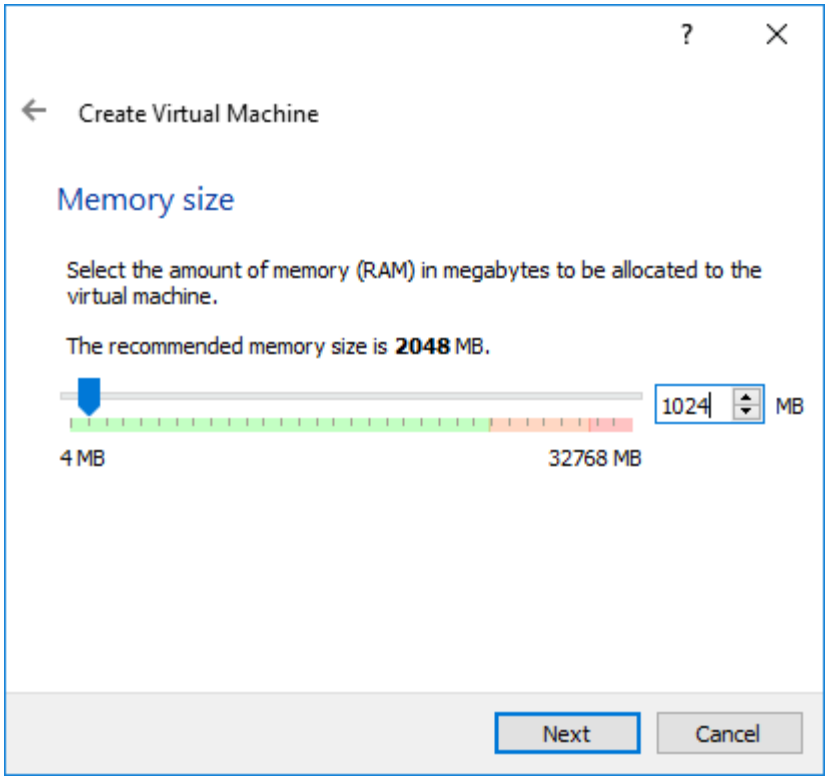


FIGURE 3-24. Memory Size

5. Specify the recommended memory size for your operating system.

   - Windows XP and Windows Server 2003: 512 MB
   - Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019: 1024 MB

6. Click **Next**.

   The **Hard disk** screen appears.

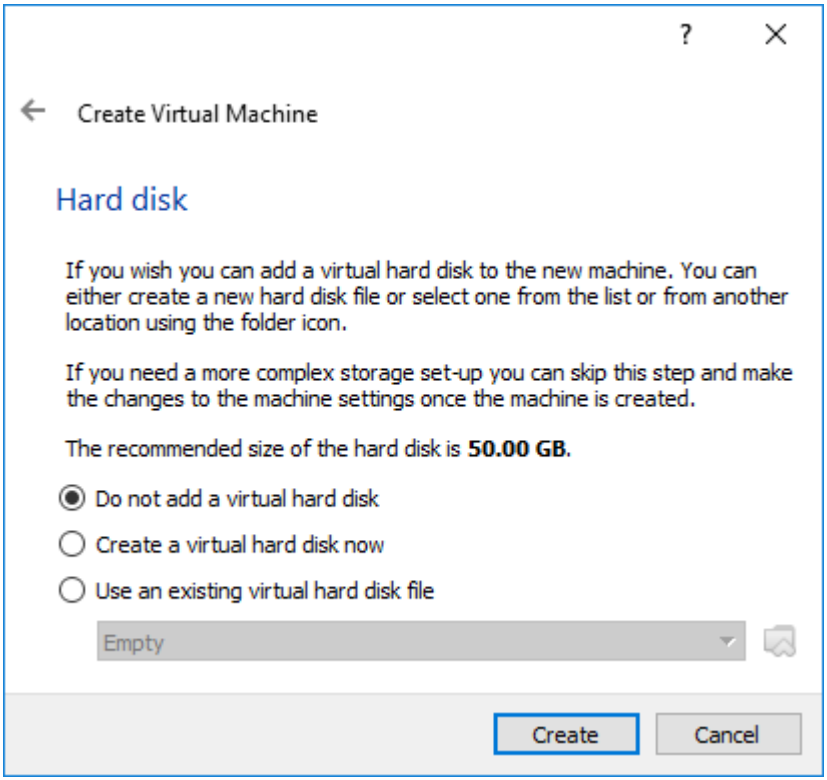


FIGURE 3-25. Hard Disk

7. Select **Do not add a virtual hard disk** and then click **Create**.

The following message appears:

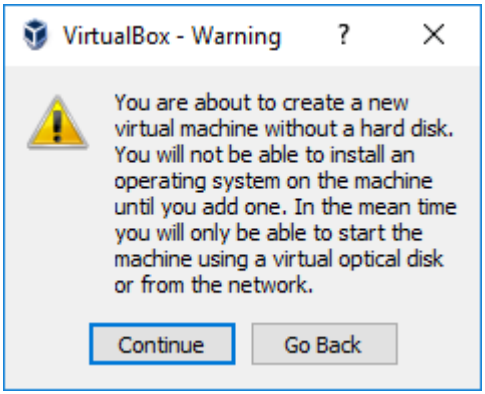


FIGURE 3-26. Warning

8. Click **Continue**.

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

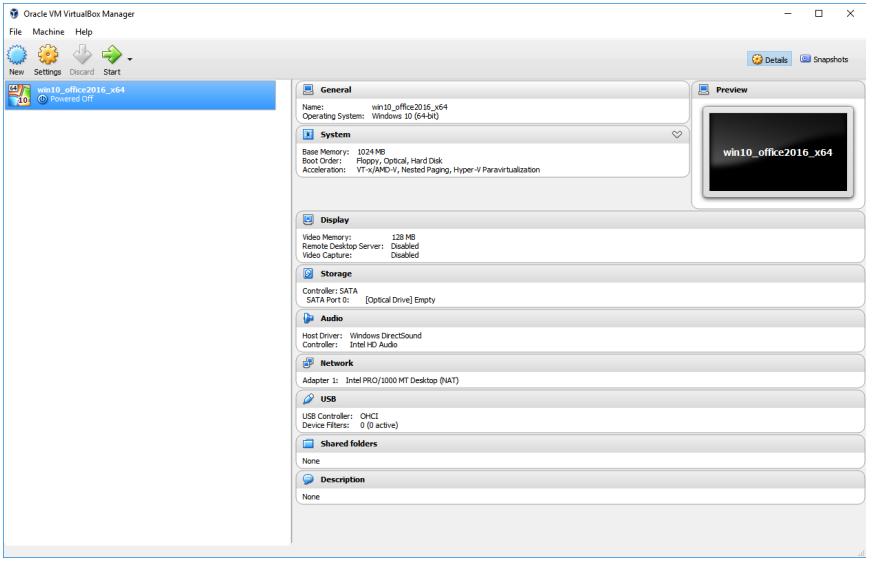


FIGURE 3-27. Newly-created Virtual Machine

9. Click **Settings**.

The **Settings** window opens.

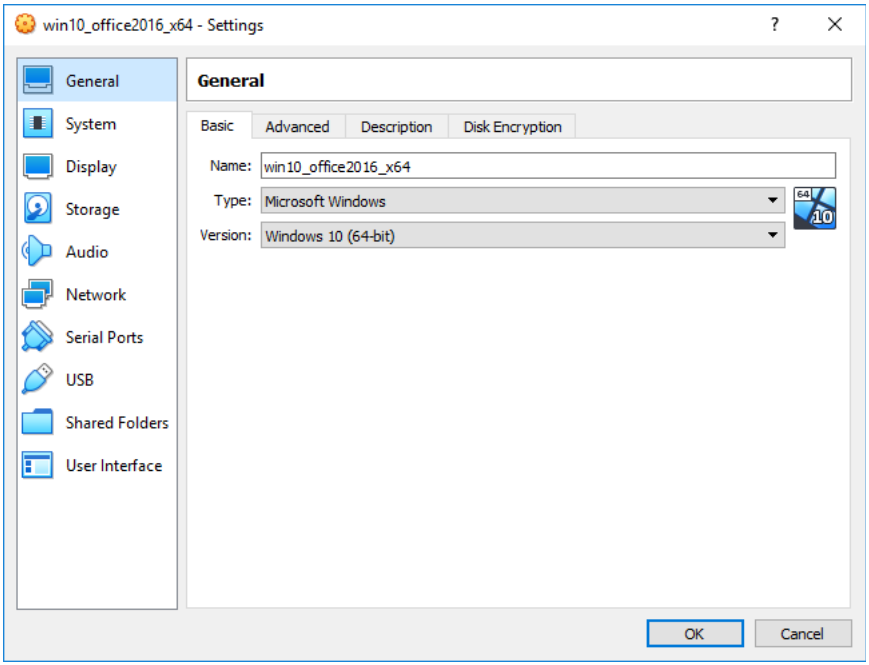


FIGURE 3-28. VirtualBox Settings

10. In the left pane, click **System**.

The **System** screen appears.

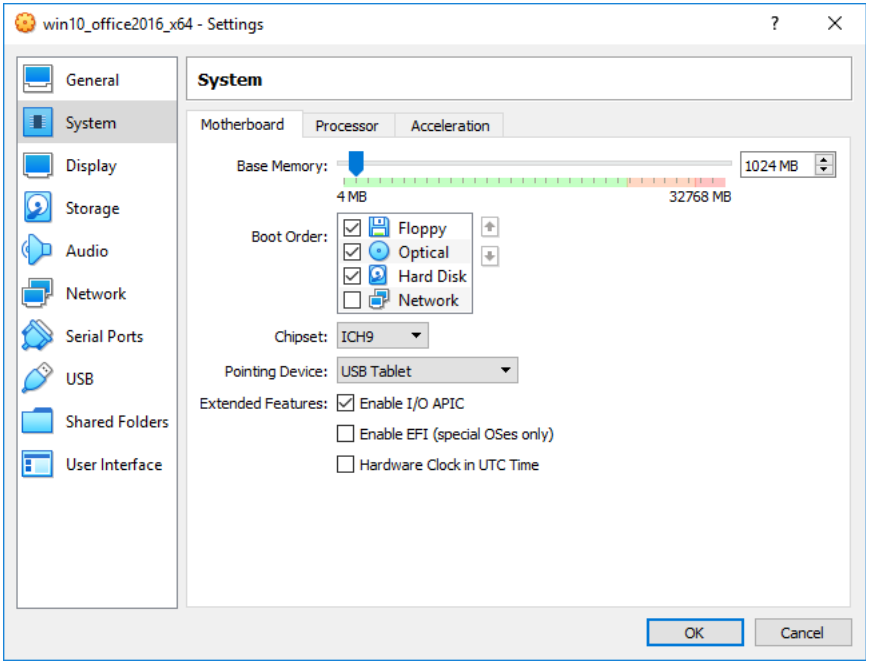


FIGURE 3-29. System Screen

11. On the **Motherboard** tab, configure the following:
    - **Chipset**: Select **ICH9**.
    - **Pointing Device**: Select **USB Tablet**.
    - **Extended Features**:
        - Select **Enable I/O APIC**
        - (Optional) Select **Enable EFI (special OSes only)** if you want to create an EFI-compatible image. EFI-compatible images are only supported by the following 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

12. Go to the **Processor** tab and then select **Enable PAE/NX**.

13. Go to the **Acceleration** tab and then select **Enable VT-x/AMD-V** and **Enable Nested Paging**.

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.

14. In the left pane, click **Storage**.

The **Storage** screen appears.

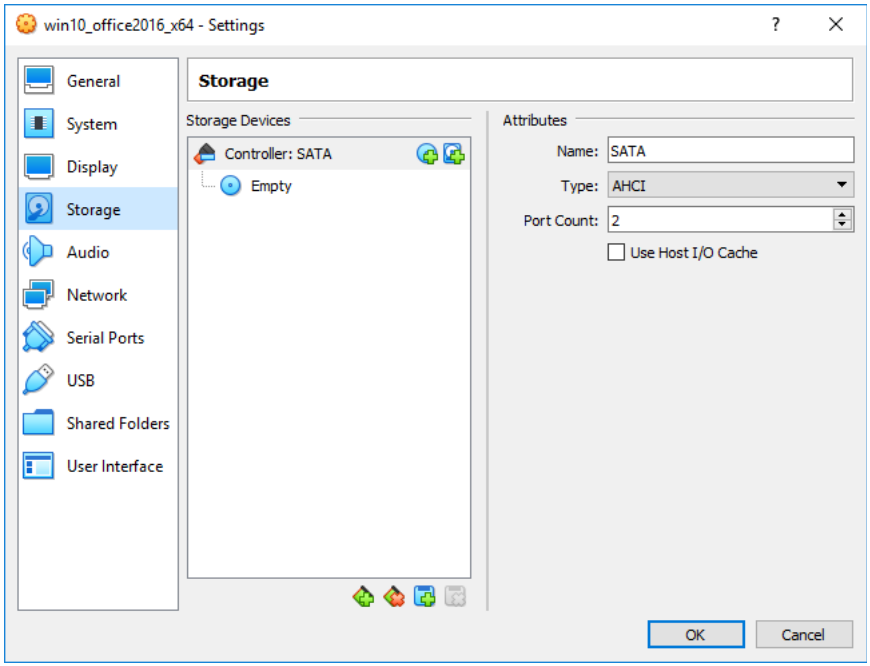


FIGURE 3-30. Storage Screen

15. If **Controller: SATA** appears under **Storage Tree**, remove the SATA controller and then add an IDE controller.

    a. Click **Controller: SATA** and then click to remove the default controller.

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

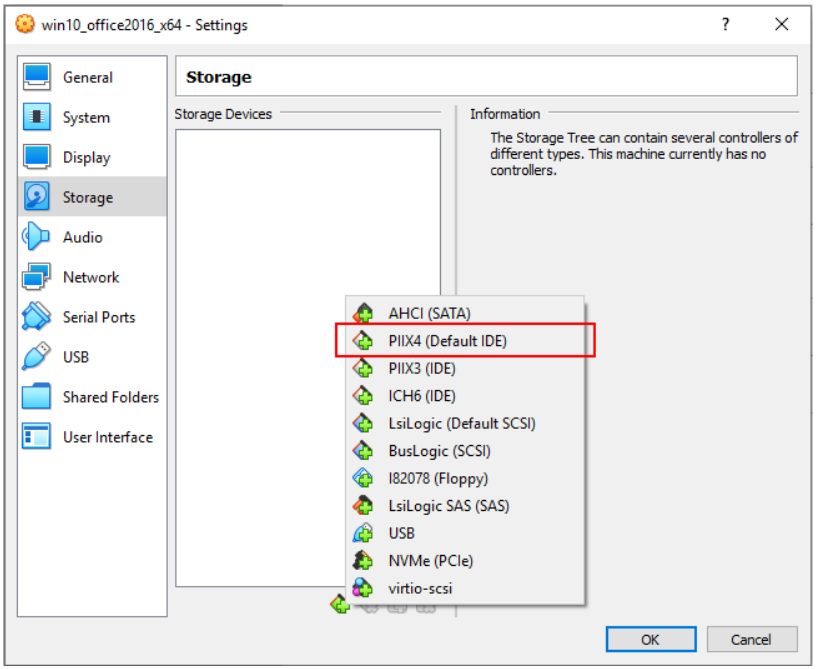


FIGURE 3-31. Add Storage Controller

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

The following window appears:

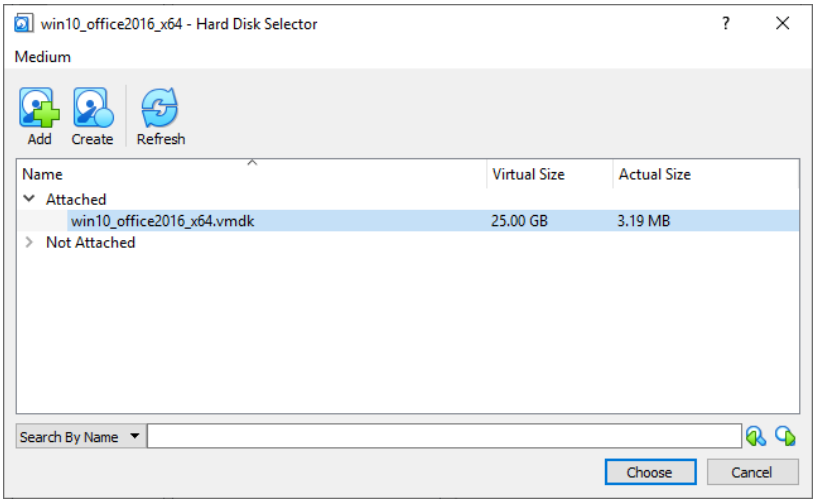


FIGURE 3-32. Hard Disk Selector

d. Select the converted `*.vmdk` file and then click **Choose**.

e. Under **Attributes**, change the name to `IDE`.

f. Under **Storage Tree**, click **Controller: IDE** and then click .

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

h. Under **Attributes**, verify that **CD/DVD Drive** is **IDE Secondary Device 0**.

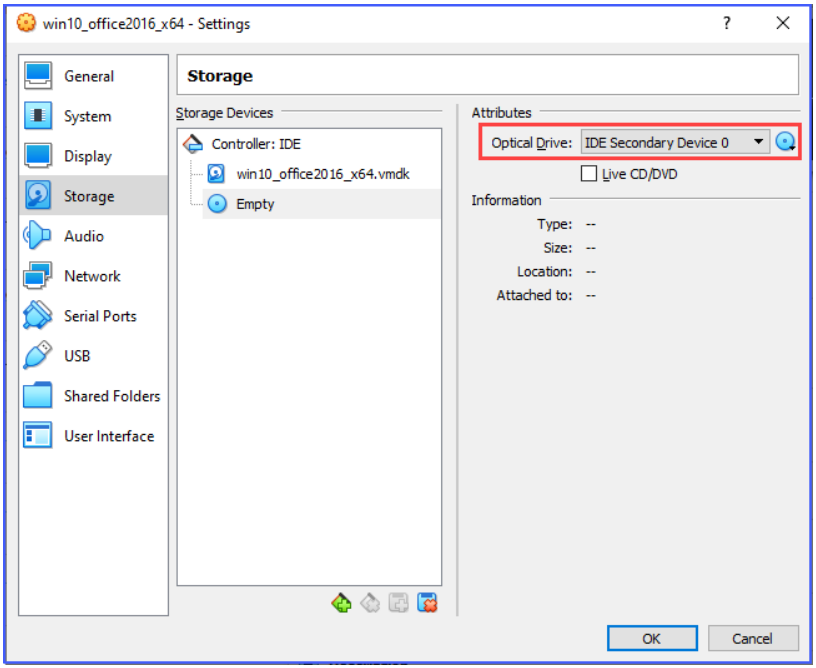


FIGURE 3-33. IDE Secondary Device 0

16. (Optional) In the left pane, click **Audio** and verify that **Enable Audio** is enabled.

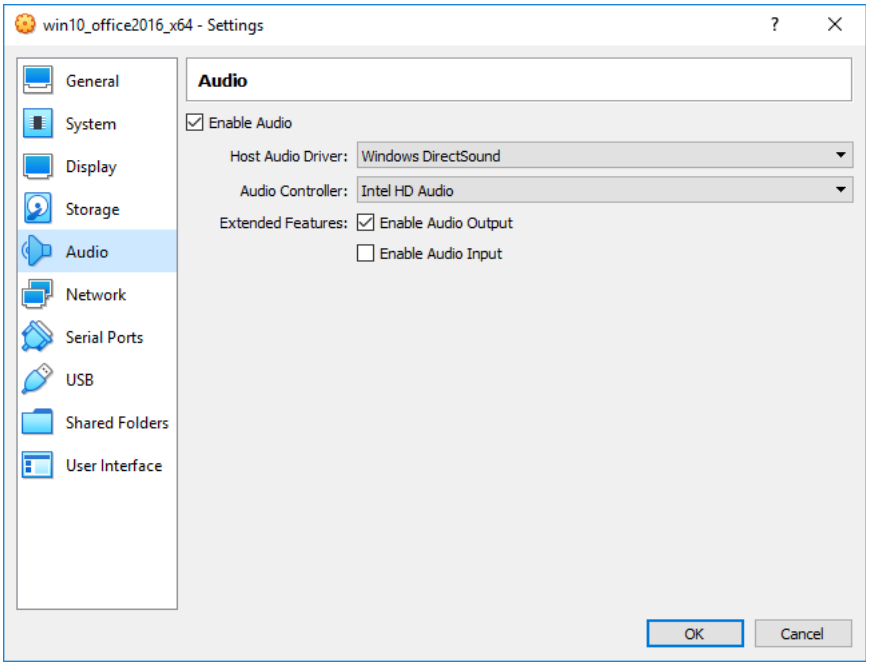


FIGURE 3-34. Audio Options Settings

17. In the left pane, click **USB** and then select **Enable USB Controller**.

Important

Verify that **USB 1.1 (OHCI) Controller** is selected.

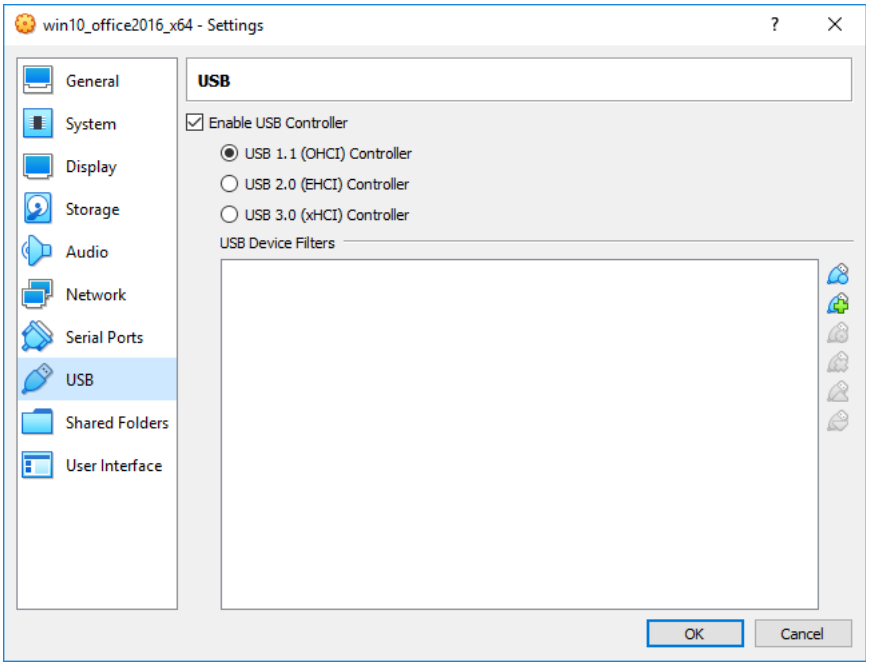


FIGURE 3-35. Enable USB Controller

18. In the left pane, click **Shared Folders** and then verify that no folders are shared.

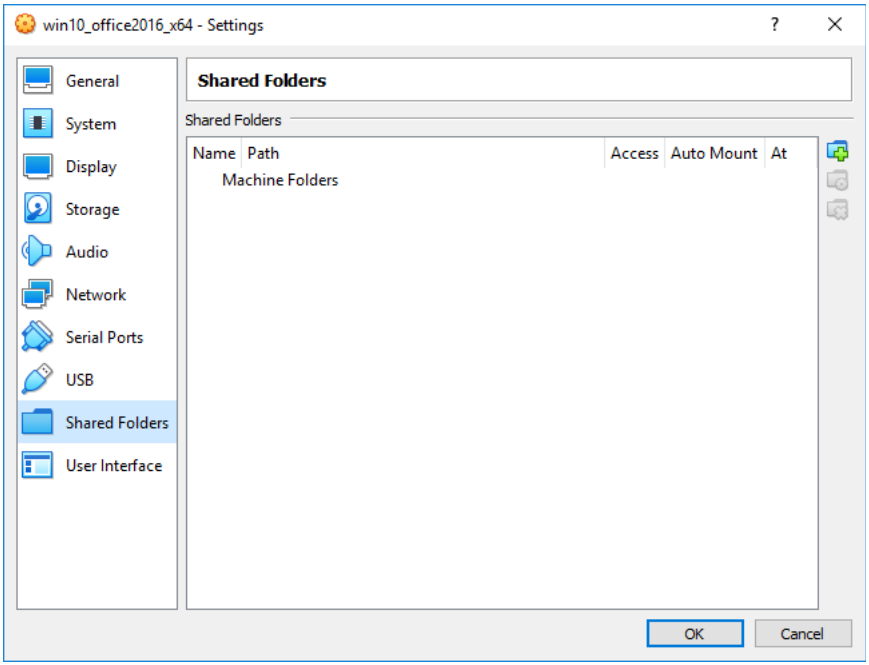


FIGURE 3-36. Shared Folders Settings

19. Click **OK**.

    The **Settings** window closes.

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

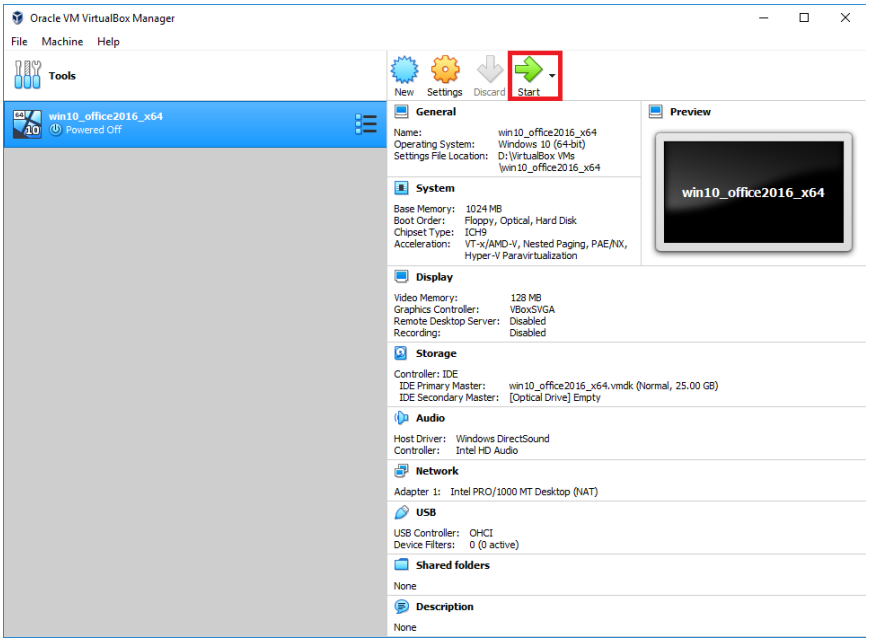


FIGURE 3-37. VirtualBox Manager

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

Important

Ensure that you have 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 3-50*

- *Configuring Virtual Machine Images (Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019) on page 3-53*

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.

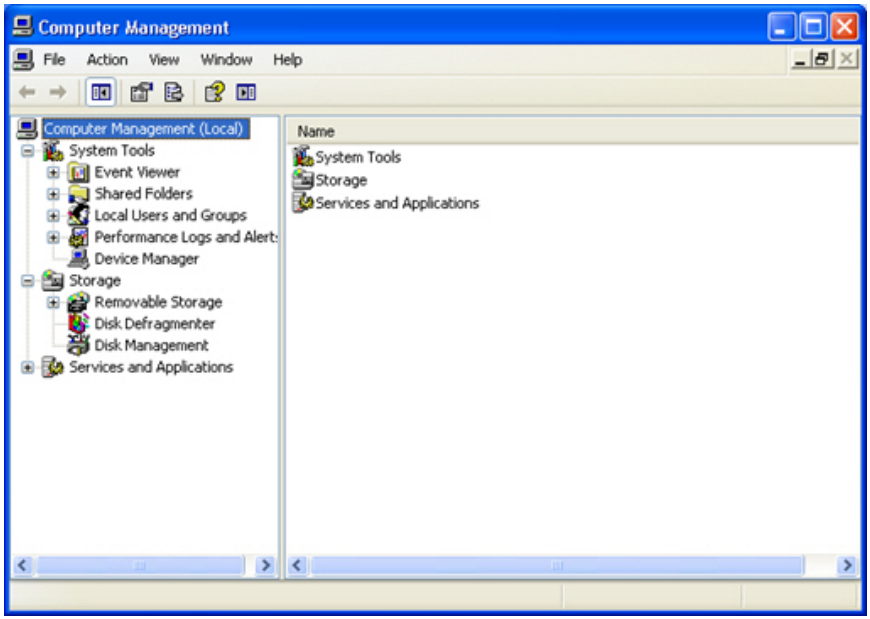


FIGURE 3-38. Computer Management

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

A list of devices appears.

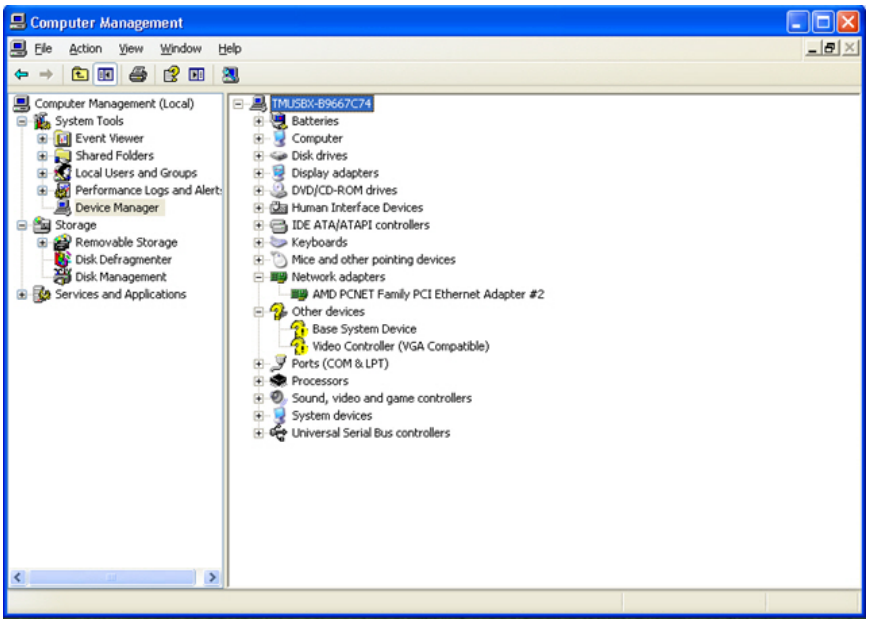


FIGURE 3-39. Device Management - Network Adapter Window

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
```

FIGURE 3-40. 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 (Windows 7/8/8.1/10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019)

Procedure

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

   The **Computer Management** screen appears.

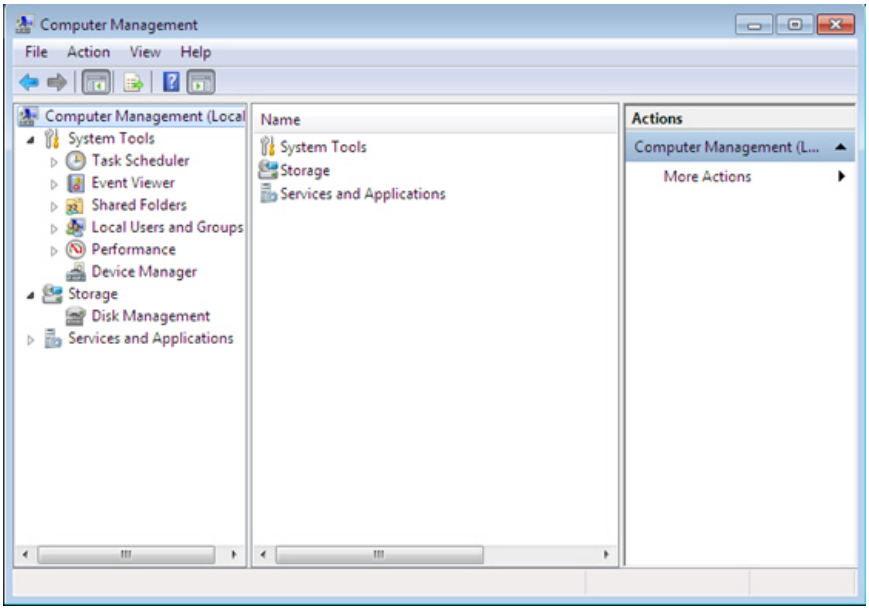


FIGURE 3-41. Computer Management

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

A list of devices appears.

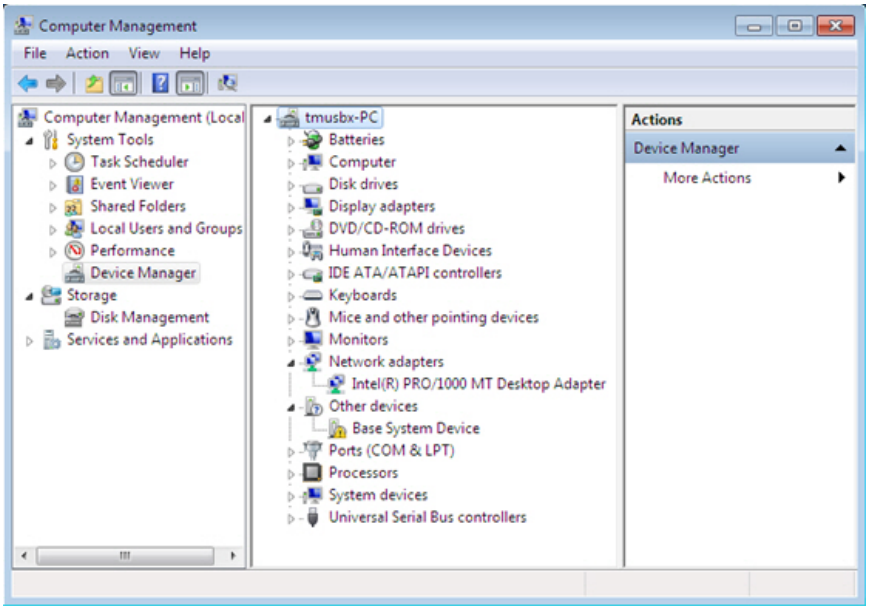


FIGURE 3-42. Device Management - Network Adapter

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, 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 4-7*

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 4-7*.

3. Create a virtual machine image.

   For details, see *Creating Linux Virtual Machine Images on page 4-8*.

4. Modify the environment of the virtual machine image.

   For details, see *Modifying the Virtual Machine Environment on page 4-30*.

5. Reduce the size of the VirtualBox Disk Image.

   For details, see *Reducing the Size of VirtualBox Disk Images on page 2-36*.

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

   For details, see *Exporting Virtual Machine Images to OVA Files on page 4-31*.

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 7.9.2009 **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, the RHEL 7.9.2009 Installation ISO `rhel-server-7.9-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
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 • 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	• 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-2.17-325.el7_9 • glibc-common-2.17-307.el7.1 • glibc-devel-2.17-325.el7_9 • glog • glog-devel • kernel-devel-3.10.0-1160.el7.x86_64 • libcurl-7.29.0-59.el7 • libcurl-devel-7.29.0-59.el7 • libgcc-4.8.5-44.el7 • libpcap-1.5.3-12.el7 • libpcap-devel-1.5.3-12.el7 • libstdc++-4.8.5-44.el7 • libstdc++-devel-4.8.5-44.el7 • net-tools-2.0-0.25.20131004git.el

Repository	CentOS 7.8	RHEL 7.9
yum	• 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 • 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	• 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 • 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

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**.

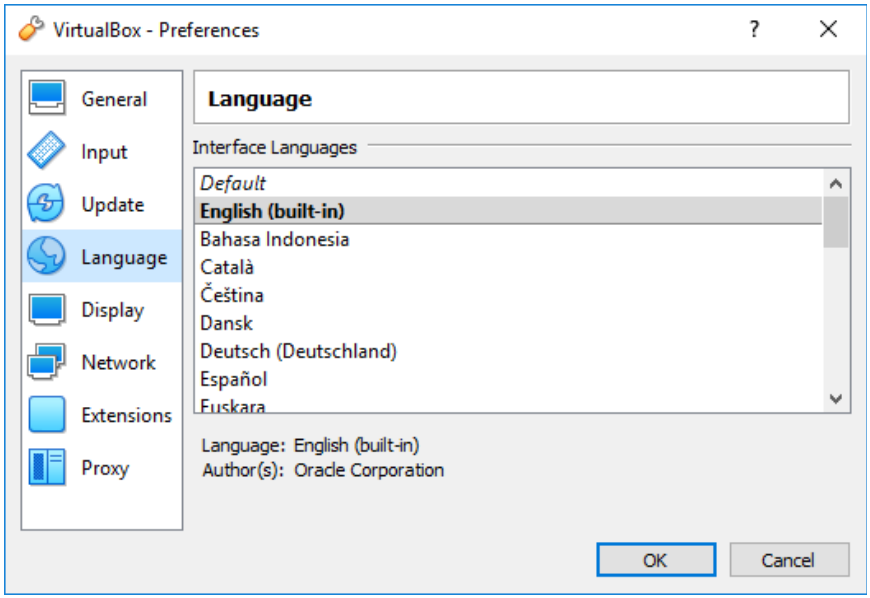


FIGURE 4-1. Language Settings

Creating Linux Virtual Machine Images

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.

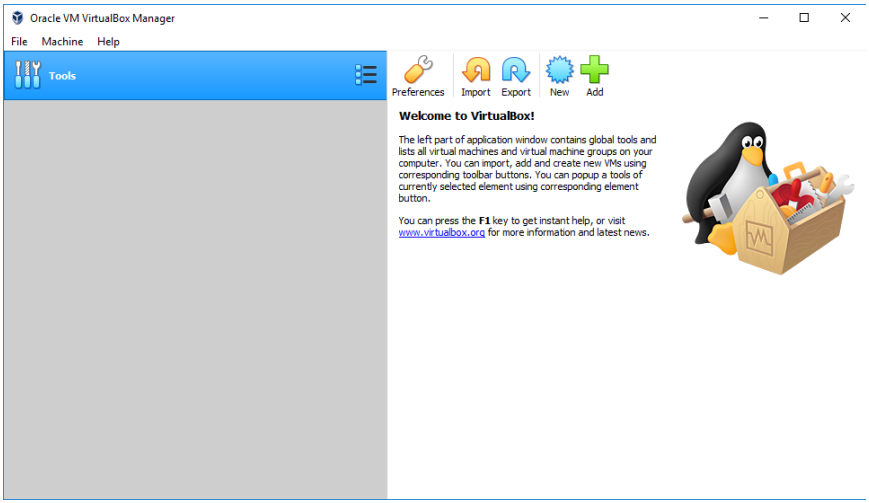


FIGURE 4-2. VirtualBox Manager

2. Click **New**.

The **Create Virtual Machine** window opens.

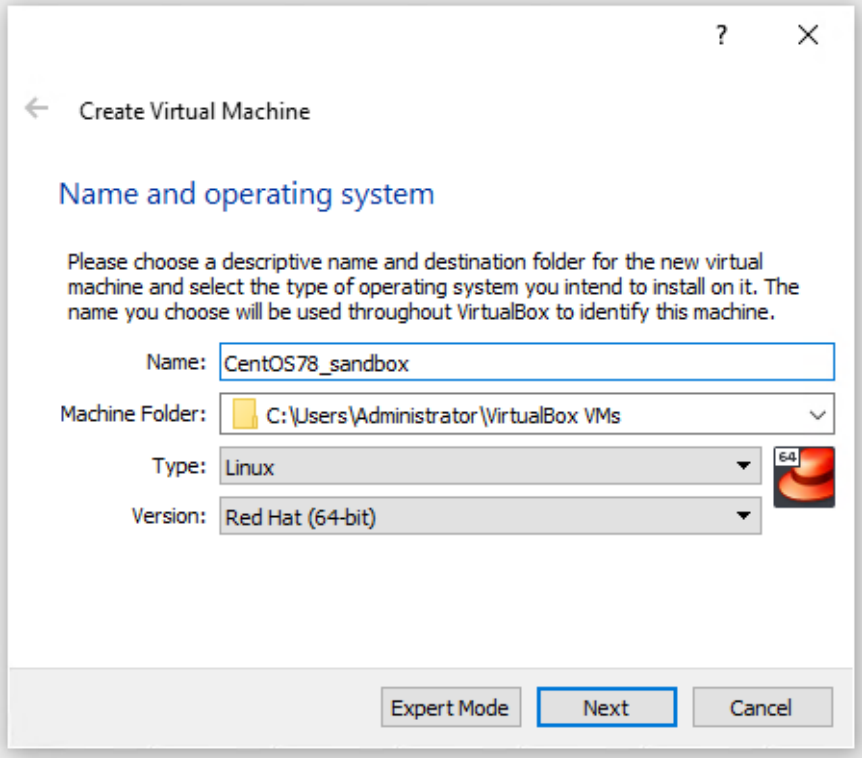


FIGURE 4-3. Create Virtual Machine

3. On the **Name and operating system** screen, configure the following:
   - **Name**: Type a permanent name for the virtual machine.
   - **Type**: Select **Linux**.
   - **Version**: Select **Red Hat (64-bit)**.

Note

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

4. Click **Next**.

   The **Memory size** screen appears.

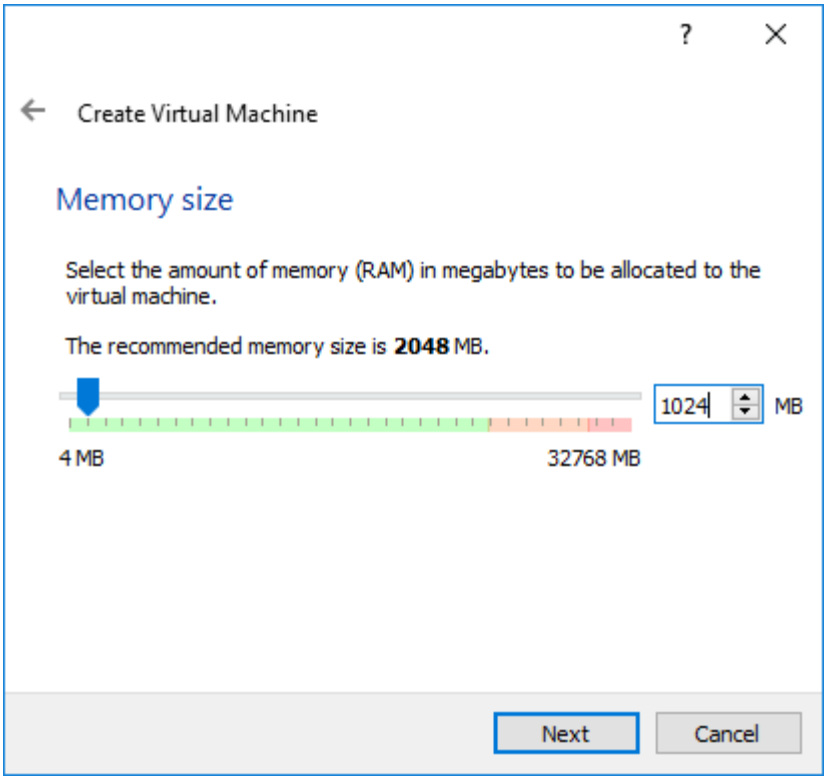


FIGURE 4-4. Memory Size

5. Specify the recommended memory size for your operating system.
   - CentOS 7.8: 1024 MB
   - RHEL 7.9: 1024 MB
6. Click **Next**.

The **Hard disk** screen appears.

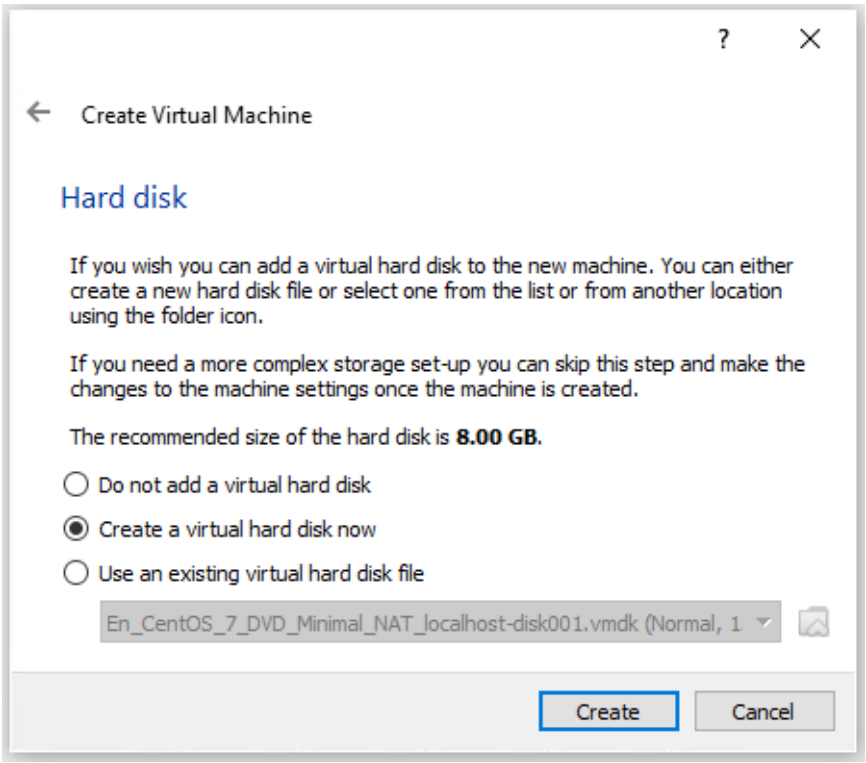


FIGURE 4-5. Hard Disk

7. Select **Create a virtual hard disk now** and then click **Create**.

The **Hard disk file type** screen appears.

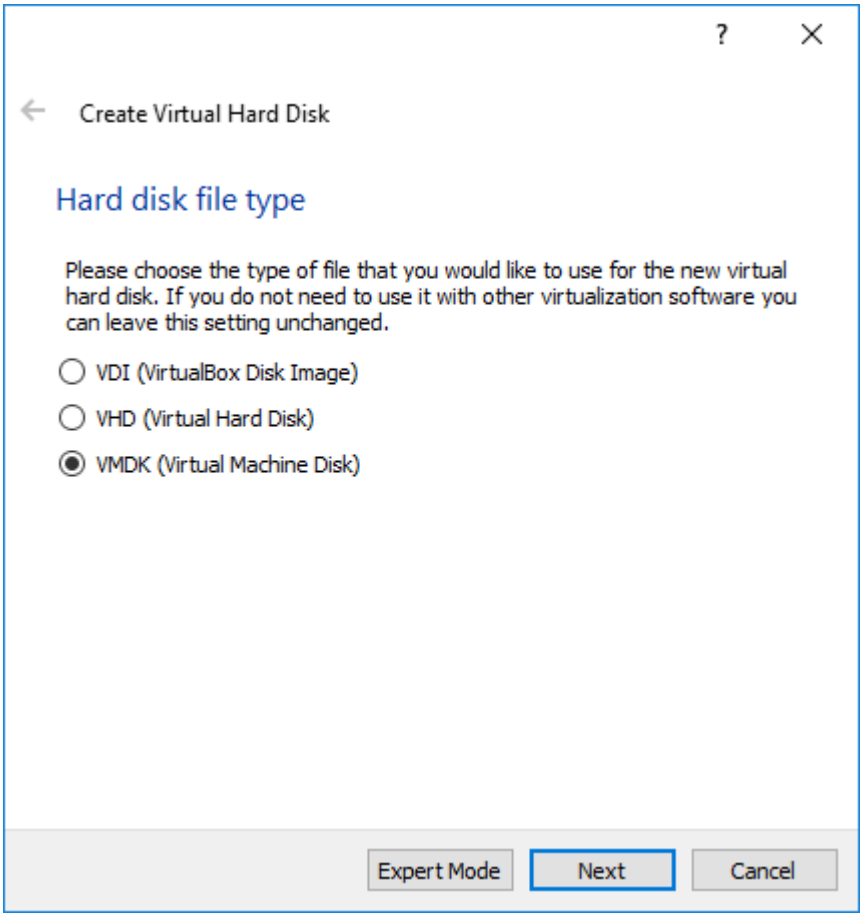


FIGURE 4-6. Hard Disk File Type

8. Select **VDI (VirtualBox Disk Image)** or **VMDK (Virtual Machine Disk)** and then click **Next**.

The **Storage on physical hard disk** screen appears.

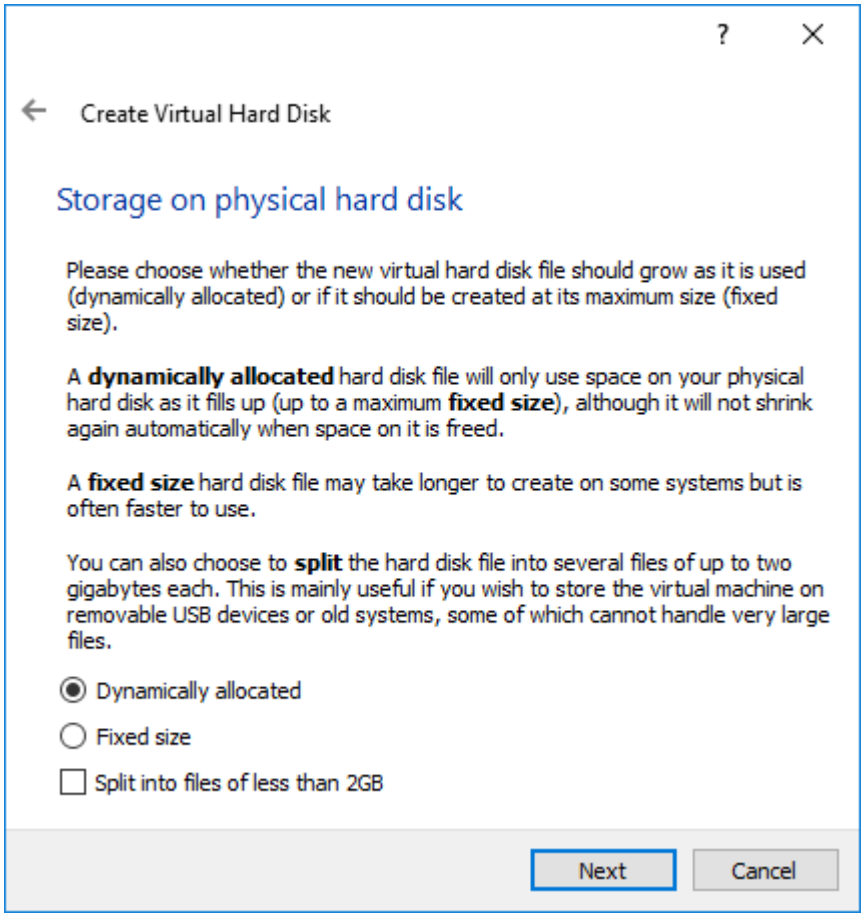


FIGURE 4-7. Storage on Physical Hard Disk

9. Select **Dynamically allocated** and then click **Next**.

Important

Do not select **Fixed size** or **Split into files of less than 2GB**.

The **File location and size** screen appears.

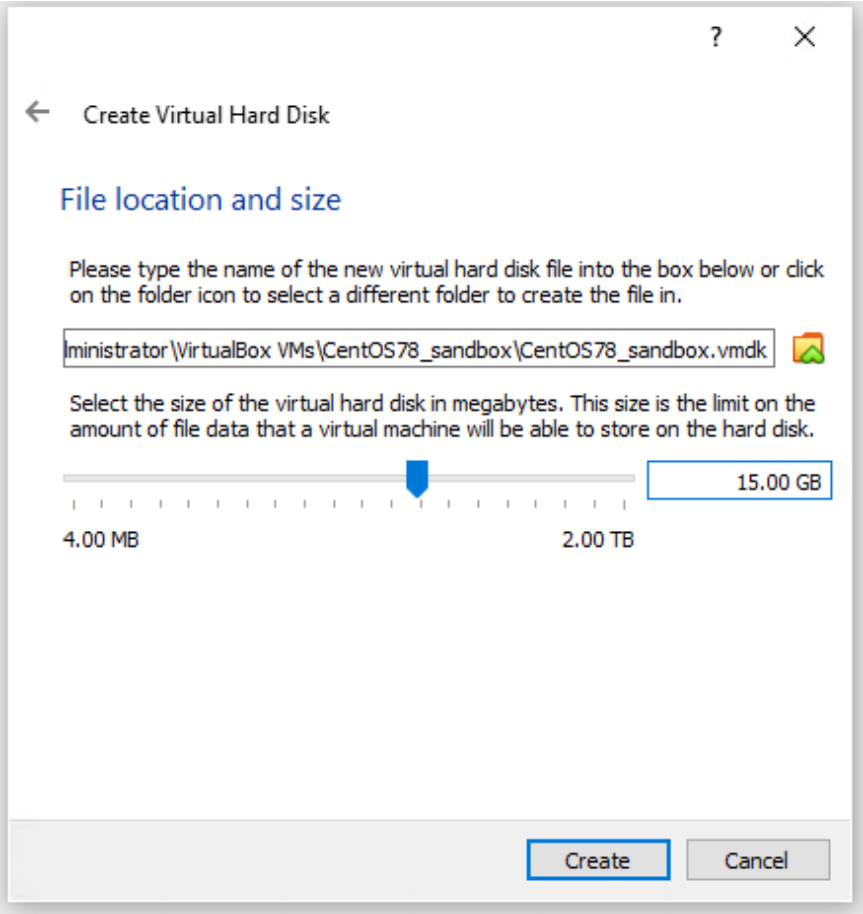


FIGURE 4-8. File Location and Size

10. (Optional) Click the folder icon to change the path of the virtual disk file.
11. Specify the virtual disk size for your operating system.
    - CentOS 7.8: 15 GB

- RHEL 7.9: 15 GB

12. Click **Create**.

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

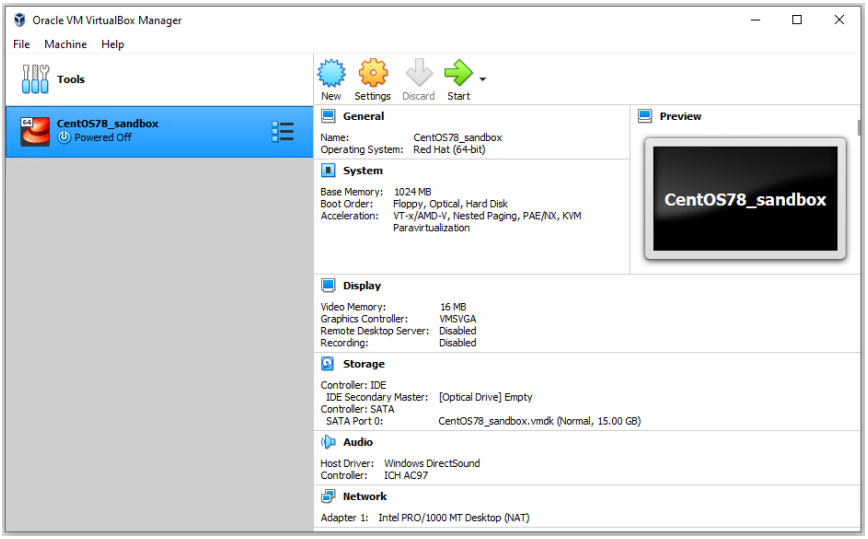


FIGURE 4-9. Newly-created Virtual Machine

Ensure that the virtual machine is not in any group.

13. Click **Settings**.

The **Settings** window opens.

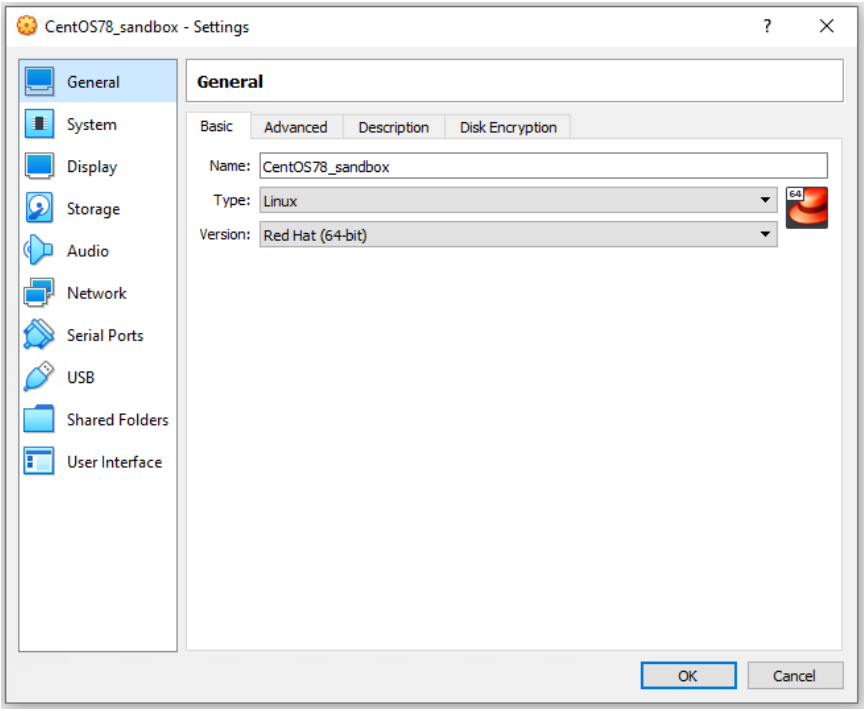


FIGURE 4-10. VirtualBox Settings

14. In the left pane, click **System**.

The **System** screen appears.

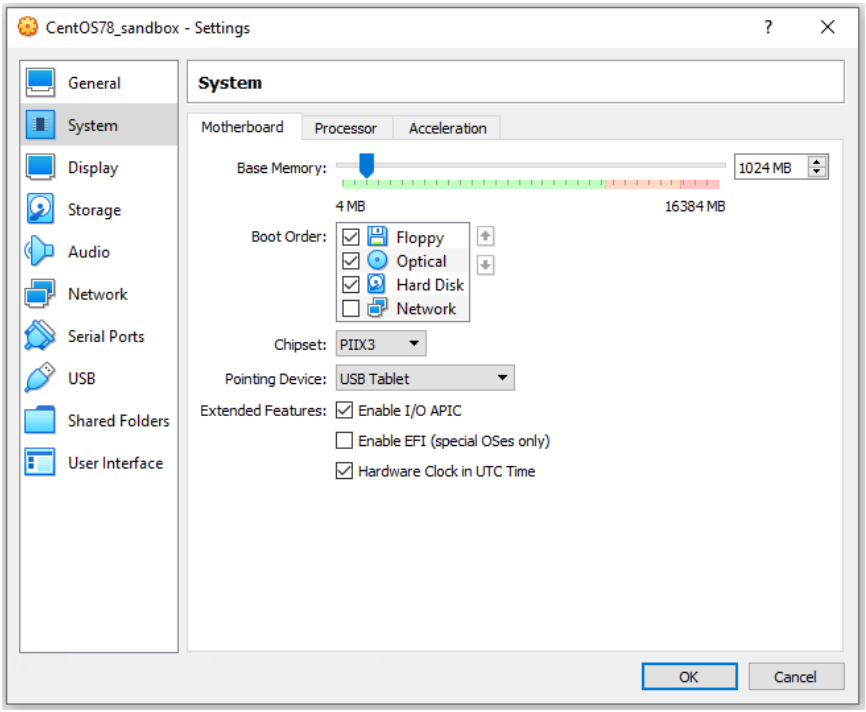


FIGURE 4-11. System Screen

15. On the **Motherboard** tab, configure the following:
    - **Chipset**: Select **PIIX3**
    - **Pointing Device**: Select **USB Tablet**
    - **Extended Features**:
        - Select **Enable I/O APIC**
        - (Optional) Select **Enable EFI (special OSes only)** if you want to create an EFI-compatible image. EFI-compatible images are only supported by the following 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

16. Go to the **Processor** tab and then select **Enable PAE/NX**.

17. Go to the **Acceleration** tab and then select **Enable Nested Paging**. If you are using VirtualBox 5.2 and before, select **Enable VT-x/AMD-V** as well.

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.

18. In the left pane, click **Storage**.

The **Storage** screen appears.

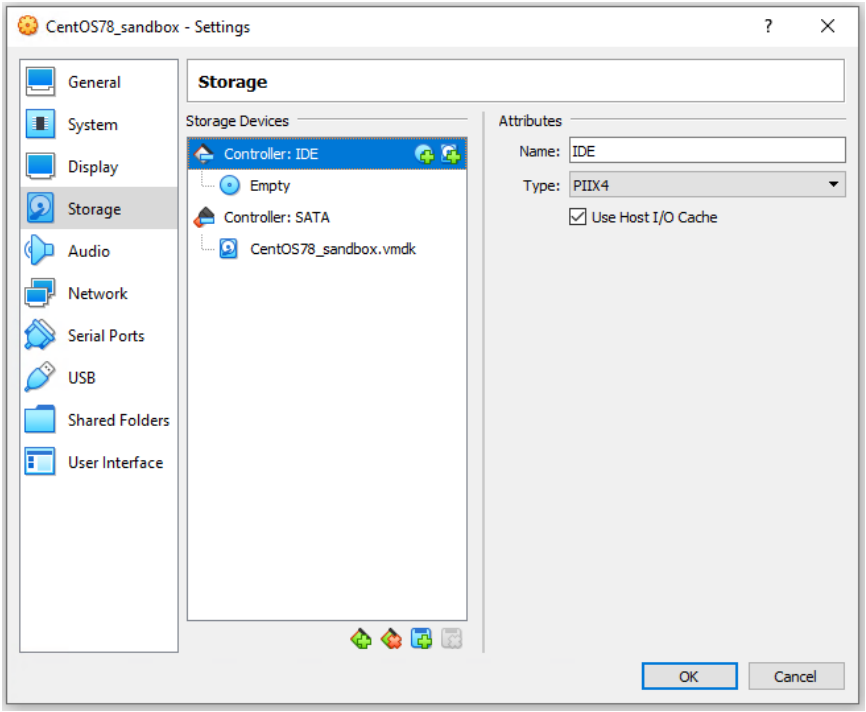


FIGURE 4-12. Storage Screen

19. If **Controller: SATA** appears under **Storage Tree**, remove the SATA controller and then add an IDE controller.

    a. Click **Controller: SATA** and then click to remove the default controller.

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

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

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

e. Under **Attributes**, verify that **Hard Disk** is **IDE Primary Device 0**.

f. Under **Storage Tree**, click **Controller: IDE** and then click  .

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

h. Under **Attributes**, verify that **Optical Drive** is **IDE Secondary Device 0**.

20. Under **Attributes**, click  , and then select **Choose a virtual CD/DVD disk file...**.

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

The ISO file is available as a device.

22. Verify that there is only one **Controller: IDE** controller. Remove any other controllers by clicking on the controller and then clicking  .

23. (Optional) In the left pane, click **Audio** and verify that **Enable Audio** is enabled.

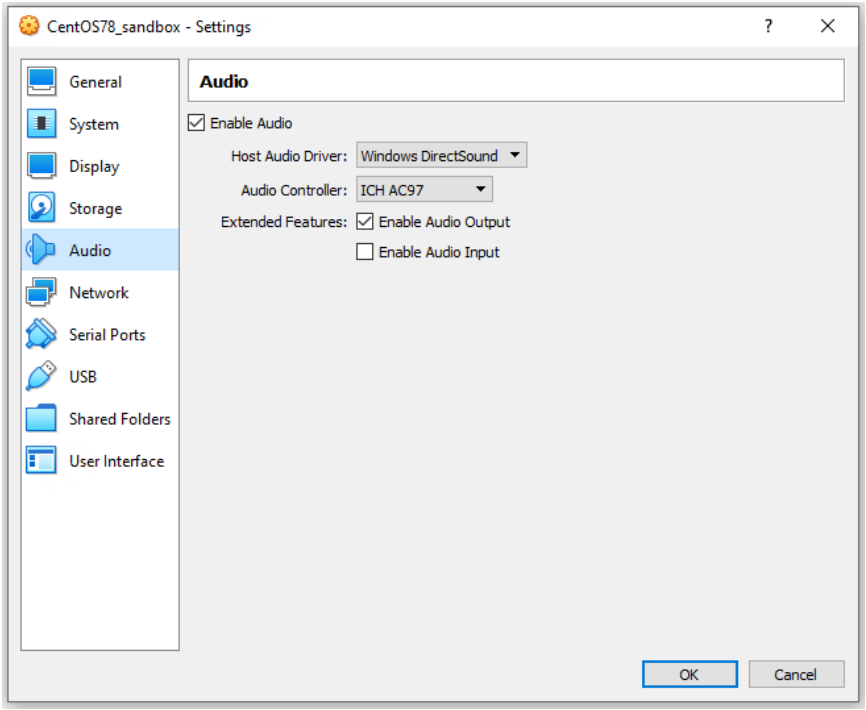


FIGURE 4-13. Audio Options Settings

24. In the left pane, click **Network**, go to the **Adapter 1** tab, and verify that **Enable Network Adapter** is enabled and that **Attached to** is **NAT** or **Bridged Adapter**.

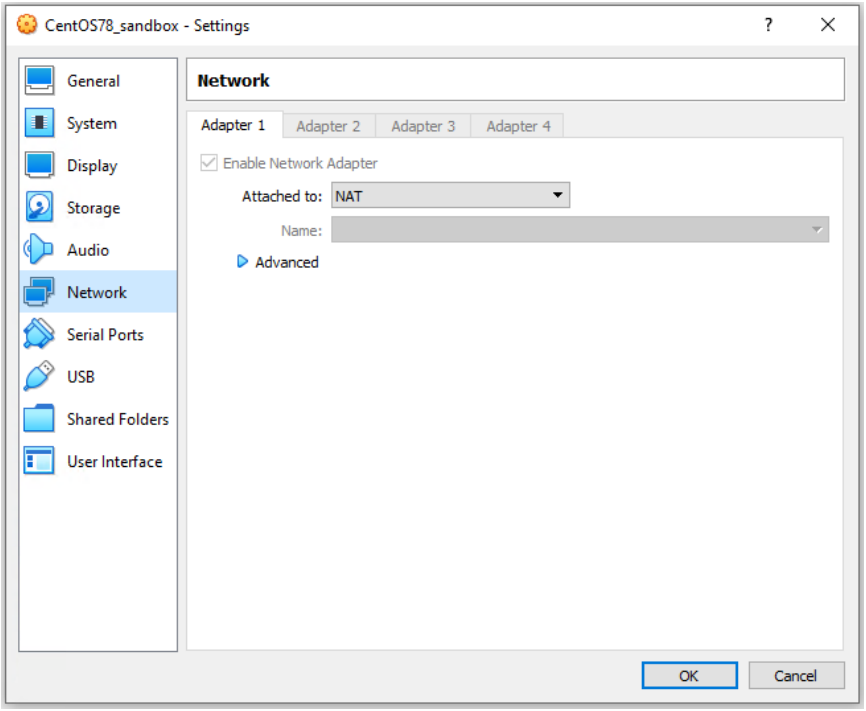


FIGURE 4-14. Network Settings

25. In the left pane, click **USB** and then select **Enable USB Controller**.

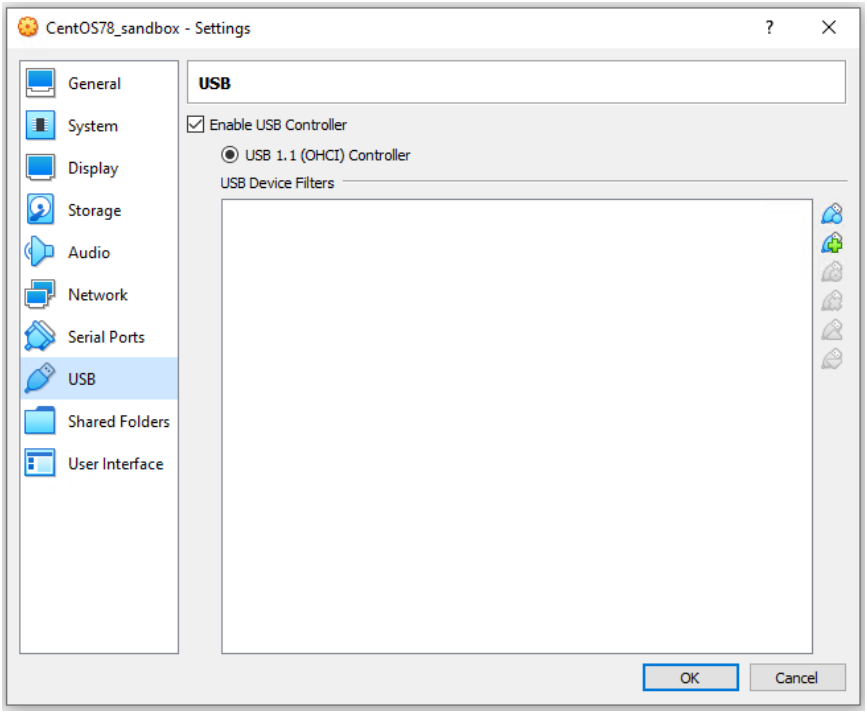


FIGURE 4-15. Enable USB Controller

26. In the left pane, click **Shared Folders** and then verify that no folders are shared.

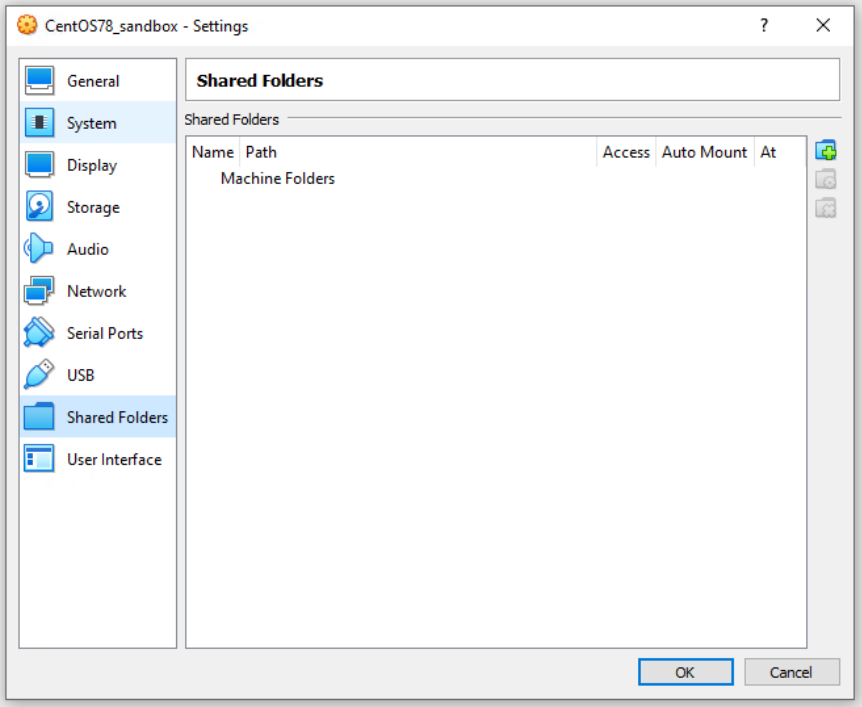


FIGURE 4-16. Shared Folders Settings

27. Click **OK**.

    The **Settings** window closes.

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

    The installation process starts.

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

FIGURE 4-17. Operating System Installation Process

30. On the **Installation Summary** screen, perform the following:

    a. Click **KDUMP**, disable **Enable kdump**, and then click **Done**.

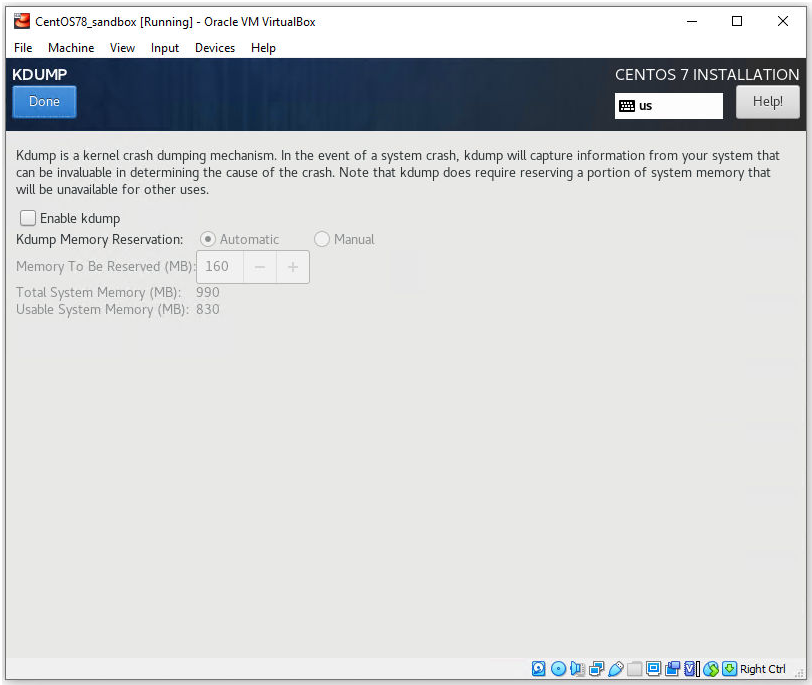


FIGURE 4-18. Installation Summary kdump

a. Click **NETWORK & HOST NAME**, click the toggle to enable the network interface, configure the network settings, verify that the network interface is able to get an IP address and connect to the network, and then click **Done**.

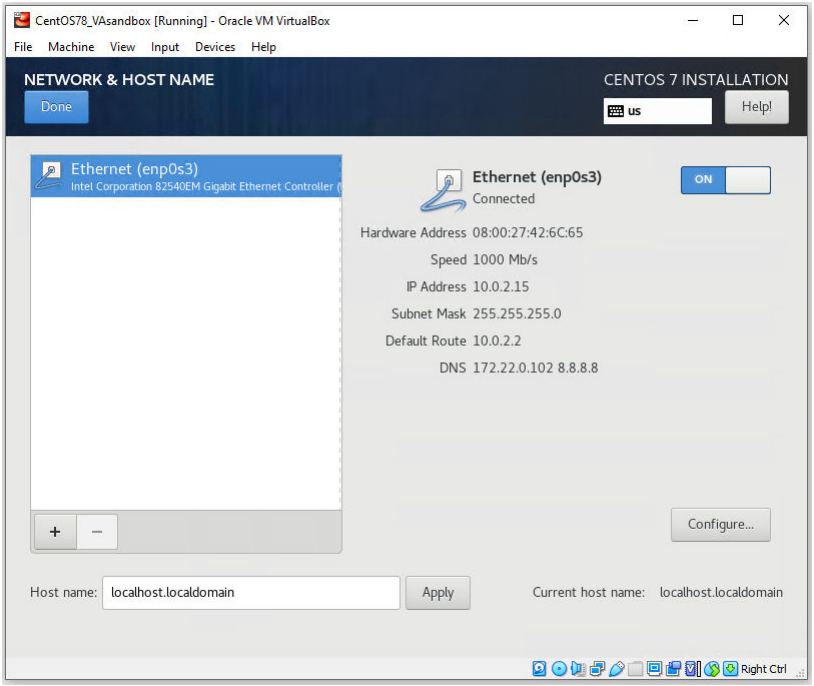


FIGURE 4-19. Installation Summary Network & Host Name

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

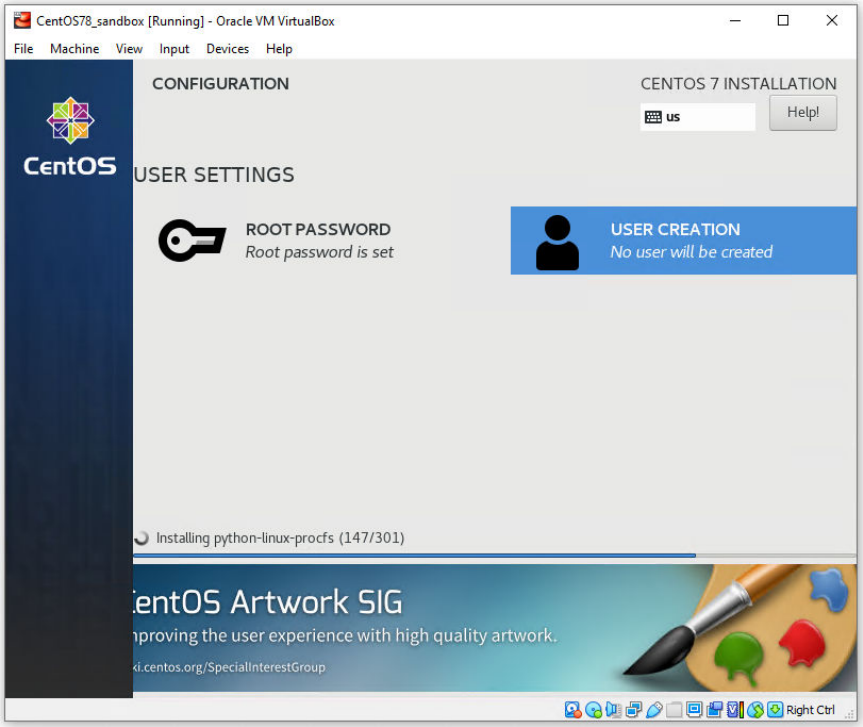


FIGURE 4-20. Password Configuration

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 4-30*

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/sysconf ig/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
(Optional) For RHEL 7.9, 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) **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.

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 • 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
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, the RHEL 7.9.2009 Installation ISO `rhel-server-7.9-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. Go to the folder and then open `SandboxWizard.exe`.

The introduction screen appears.

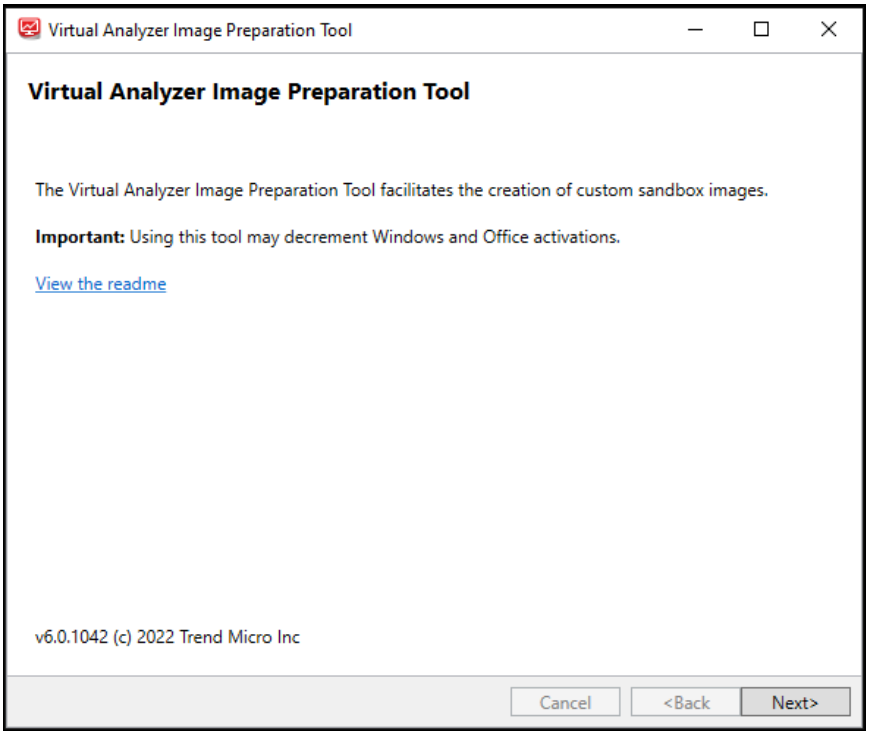


FIGURE 5-1. Introduction screen

3. Click **Next**.

The **License Agreement** screen appears.

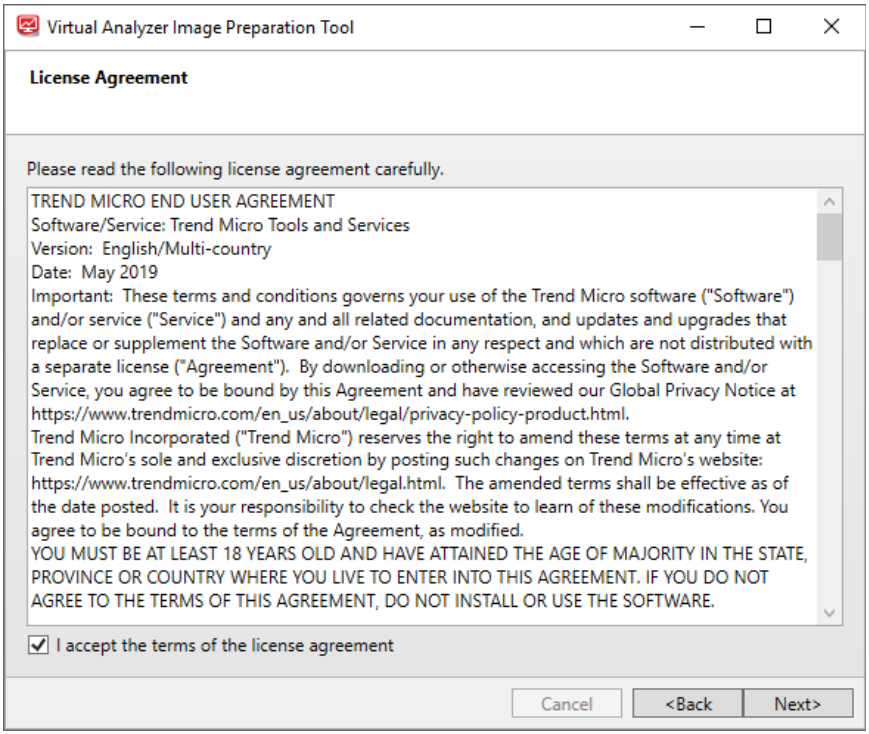


FIGURE 5-2. License Agreement screen

4. 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, and then the **System Requirements** screen appears.

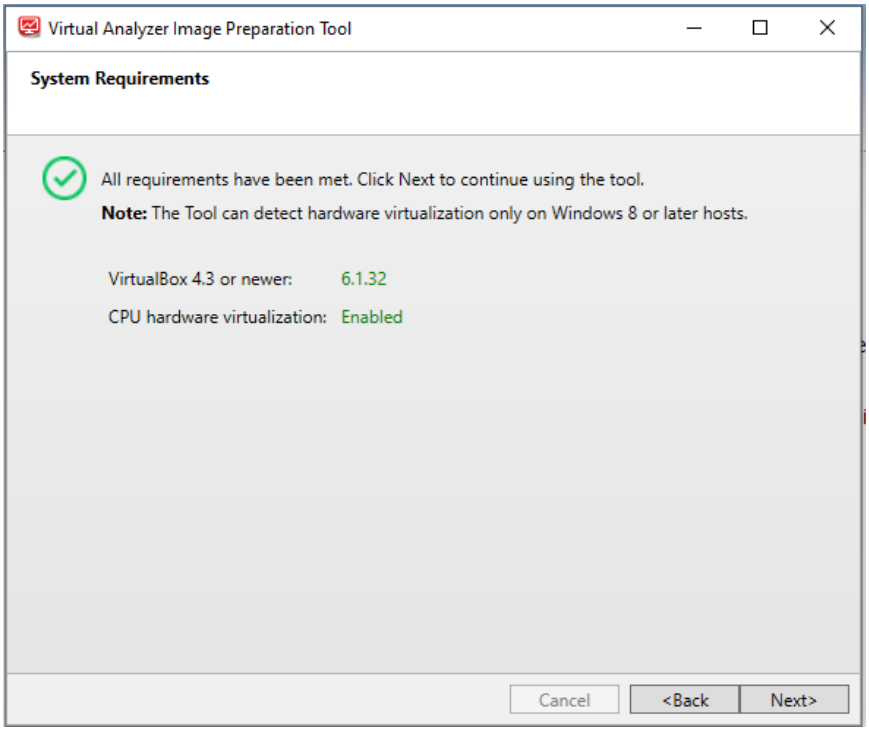


FIGURE 5-3. System Requirements screen

5. Click **Next**.

The **Specify Virtual Machine** screen appears.

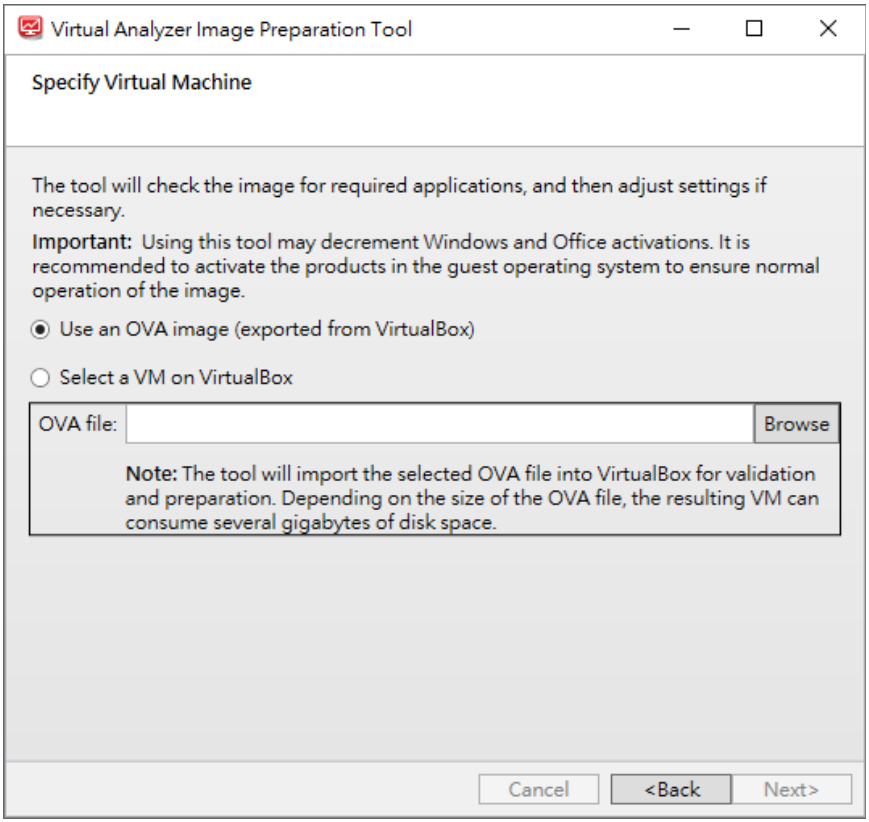


FIGURE 5-4. Specify Virtual Machine screen

6. Specify an OVA file or a virtual machine instance running on VirtualBox.

   a. Select one of the following:

      - **Use an OVA image (exported from VirtualBox)**: Select this option if you converted a Windows VMware image and then packaged it as an OVA file. For details, 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.

- **Select a VM on VirtualBox**: Select this option if you want to create an image based on an existing virtual machine on VirtualBox.

For example:

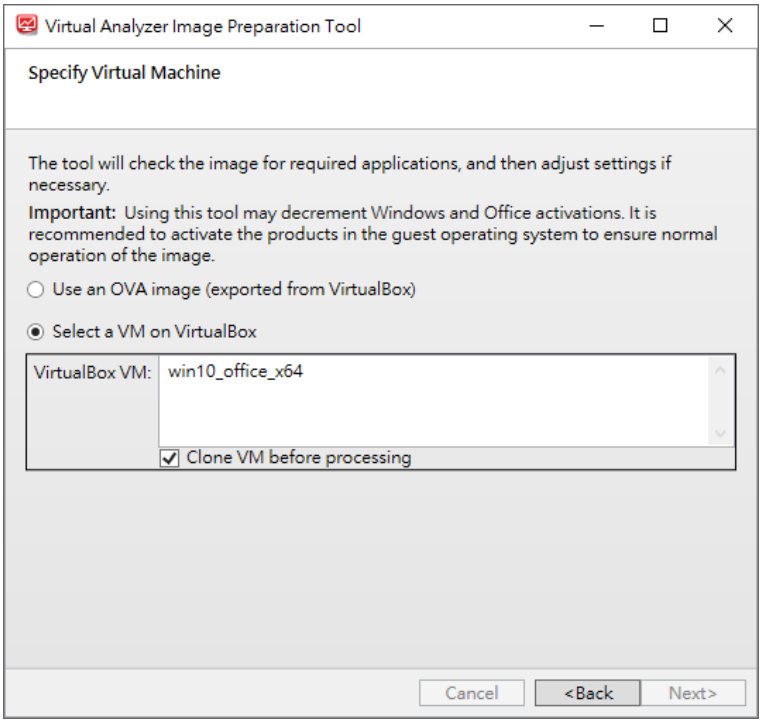


FIGURE 5-5. Specify Virtual Machine screen - Select a VM on VirtualBox

b. 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.

7. Click **Next**.

   The **Sandbox Preparation** screen appears.

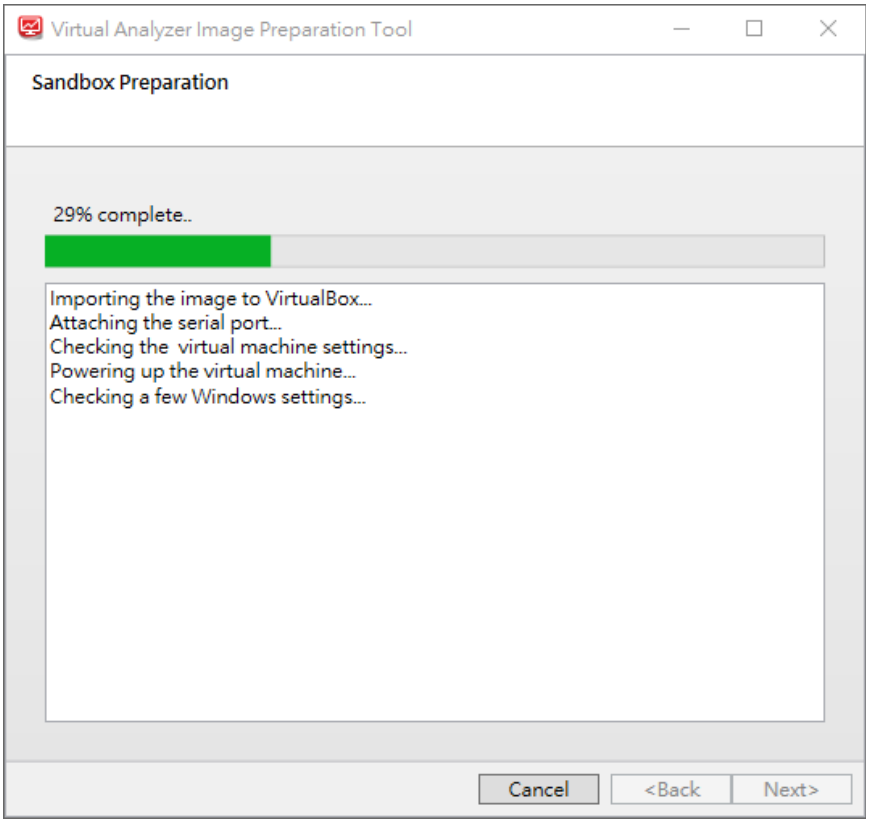


FIGURE 5-6. Sandbox Preparation screen for Windows images

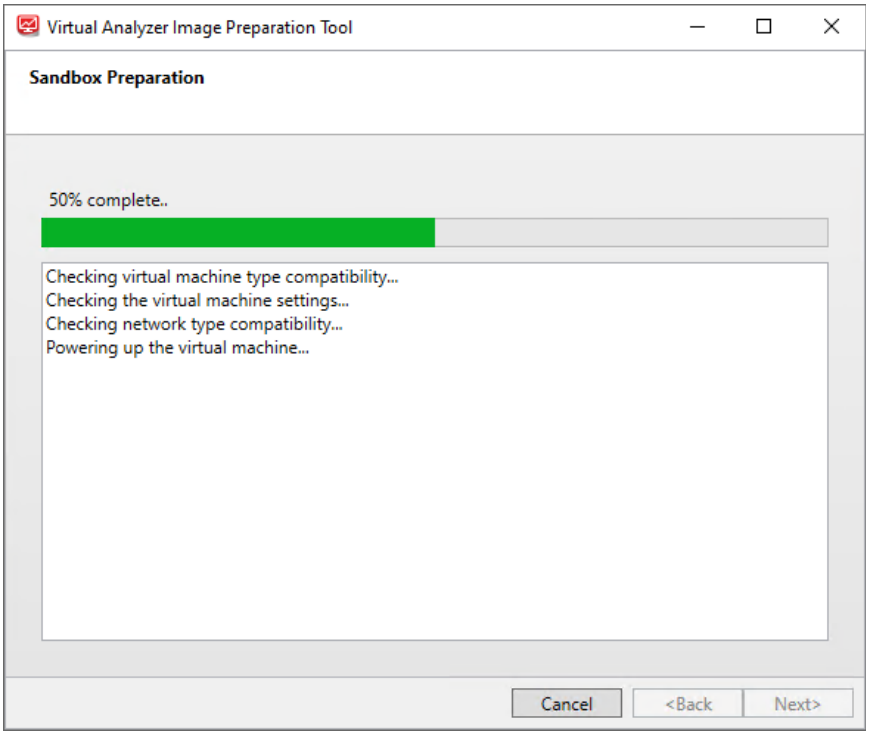


FIGURE 5-7. Sandbox Preparation screen for Linux images

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

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

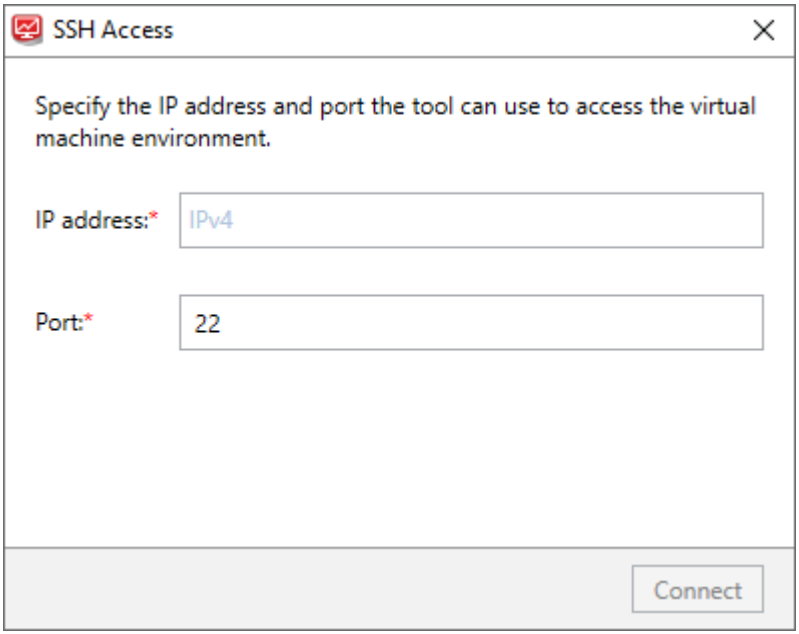


FIGURE 5-8. SSH Access screen for Linux images

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 5-26*.

8. Perform one of the following actions depending on the screen that appears:

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

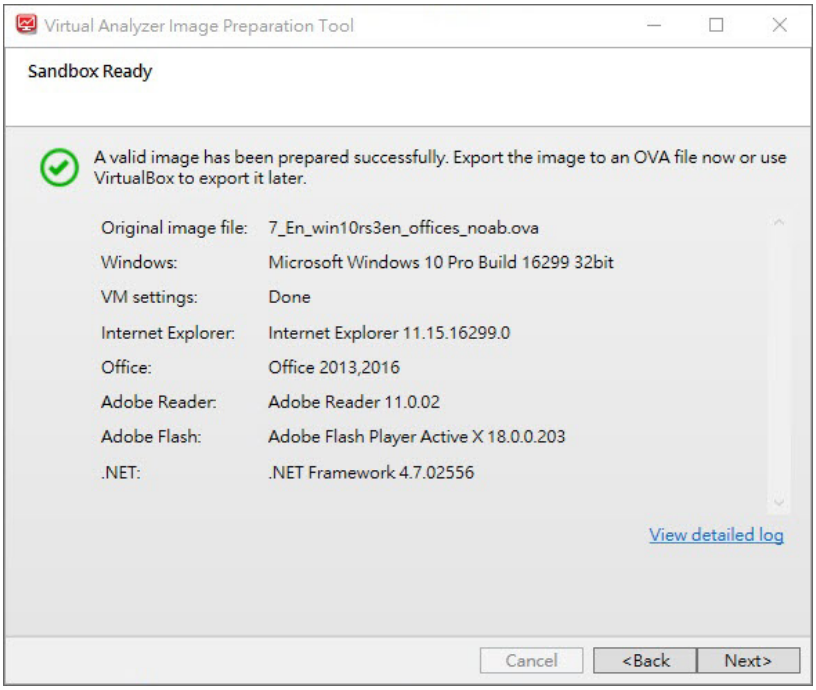


FIGURE 5-9. Sandbox Ready screen for Windows images

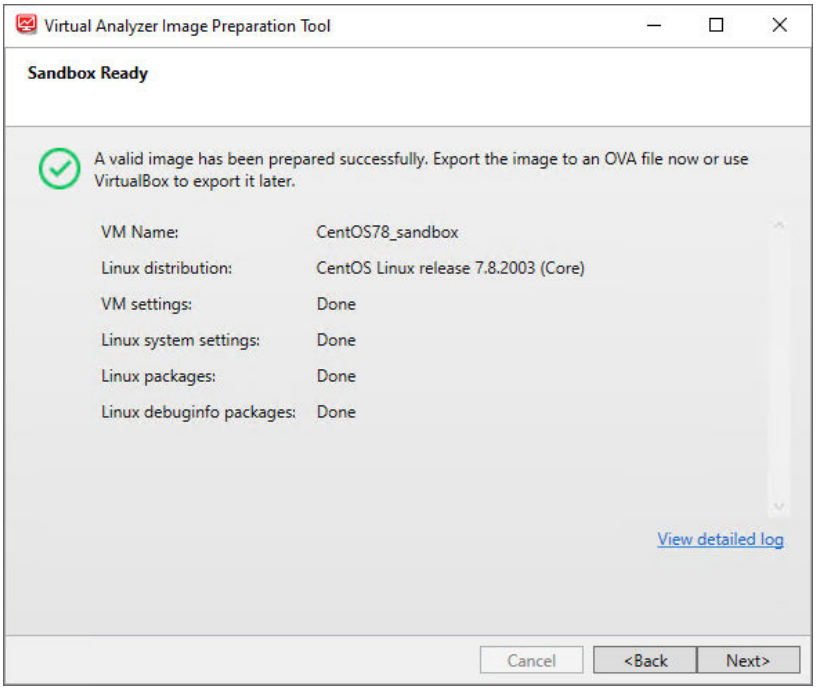


FIGURE 5-10. Sandbox Ready screen for Linux images

Click **Next** to continue.

- The **Products Not Activated** screen appears when the tool detects that Windows and/or Office are installed but not activated.

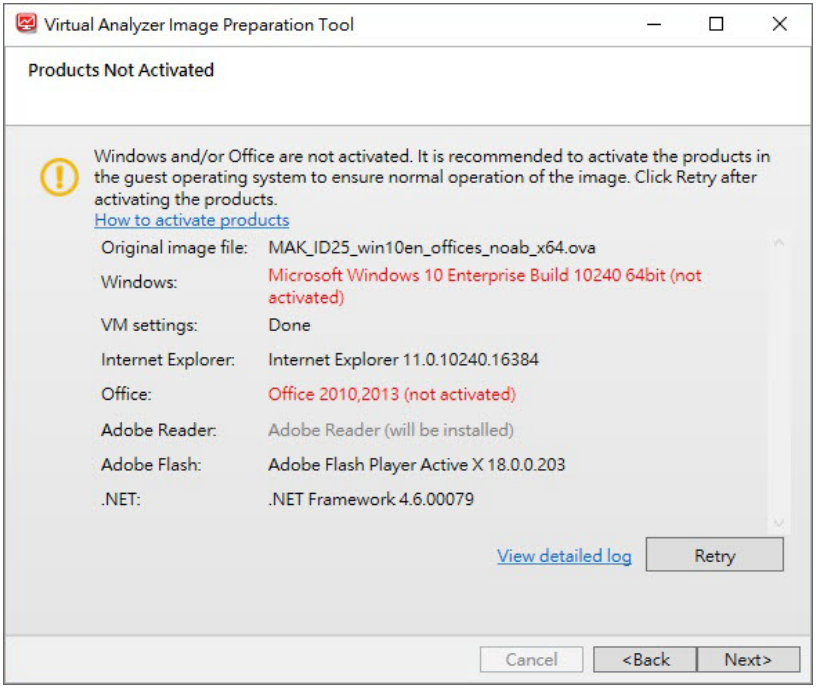


FIGURE 5-11. Products Not Activated screen for Windows images

Click **How to activate products** to learn to how to activate Windows and/or Office in the guest operating system.

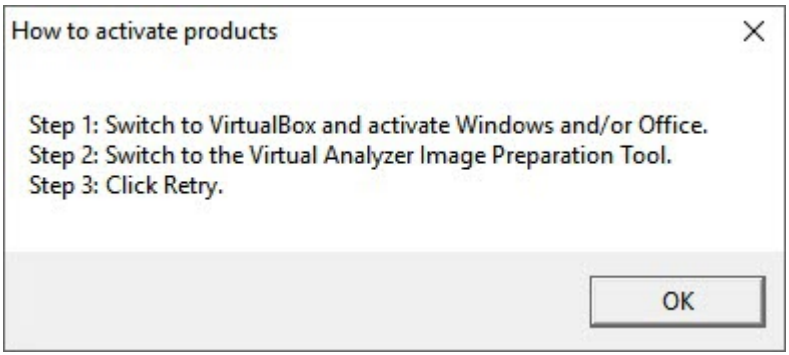


FIGURE 5-12. How to activate products dialog

Click **Retry** after activating the products, or click **Next** to continue without activating the products. It is recommended to activate the products in the guest operating system to ensure normal operation of the image.

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

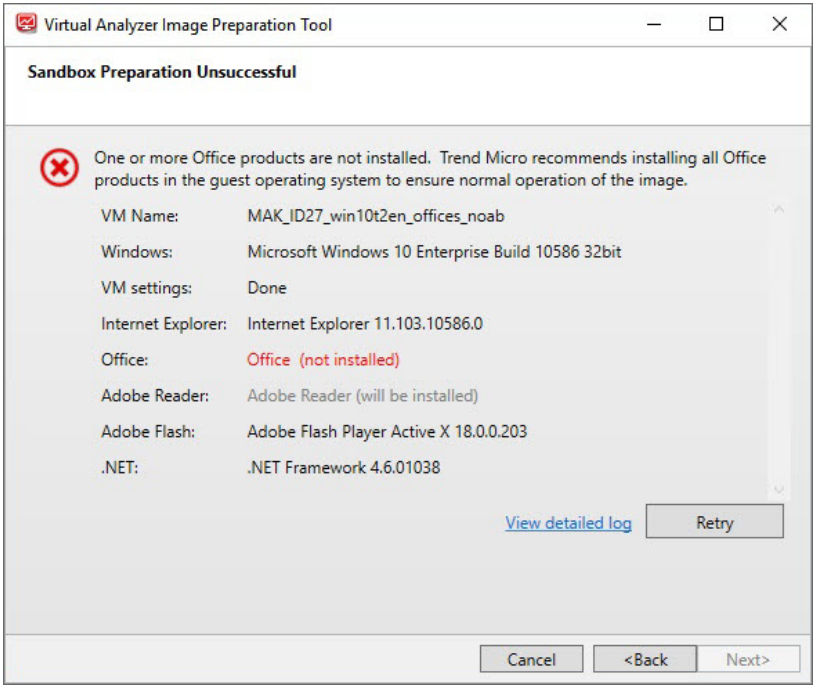


FIGURE 5-13. Sandbox Preparation Unsuccessful screen for Windows images

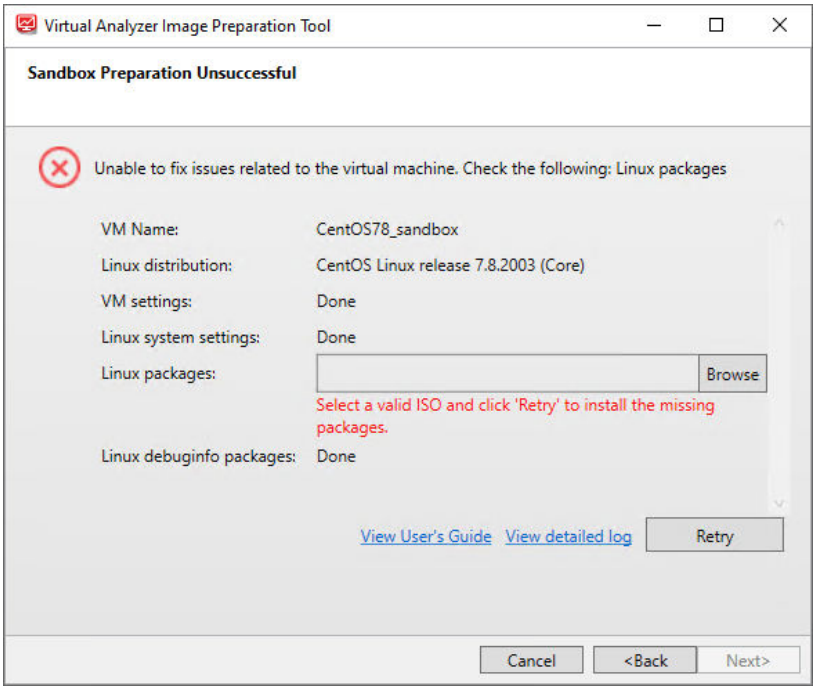


FIGURE 5-14. Sandbox Preparation Unsuccessful screen for Linux images

- If required packages are missing, perform one of the following actions to install the missing packages:
  - Manually install missing packages and then click **Retry**.
  - Install the missing packages automatically with the tool:
    - Click **Browse**.
    - Locate and select the installation ISO file for the Linux distribution used.
    - Click **Retry**.

Click **View detailed log** and perform any recommended actions before running the tool again.

Click **Retry** to try preparing the sandbox again, or **Cancel** to exit the tool.

If no issues arise, the **Specify the OVA image path and file name** screen appears.

If issues arise and are not resolved, see *Troubleshooting Common Issues on page 5-26*.

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`

9. Configure the following settings:

   - 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**.

     Disable this option if you want to keep the image in VirtualBox even after exporting.

     Important

     Unused images consume valuable disk space which may impact performance.

   - (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.

10. Click **Next**.

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

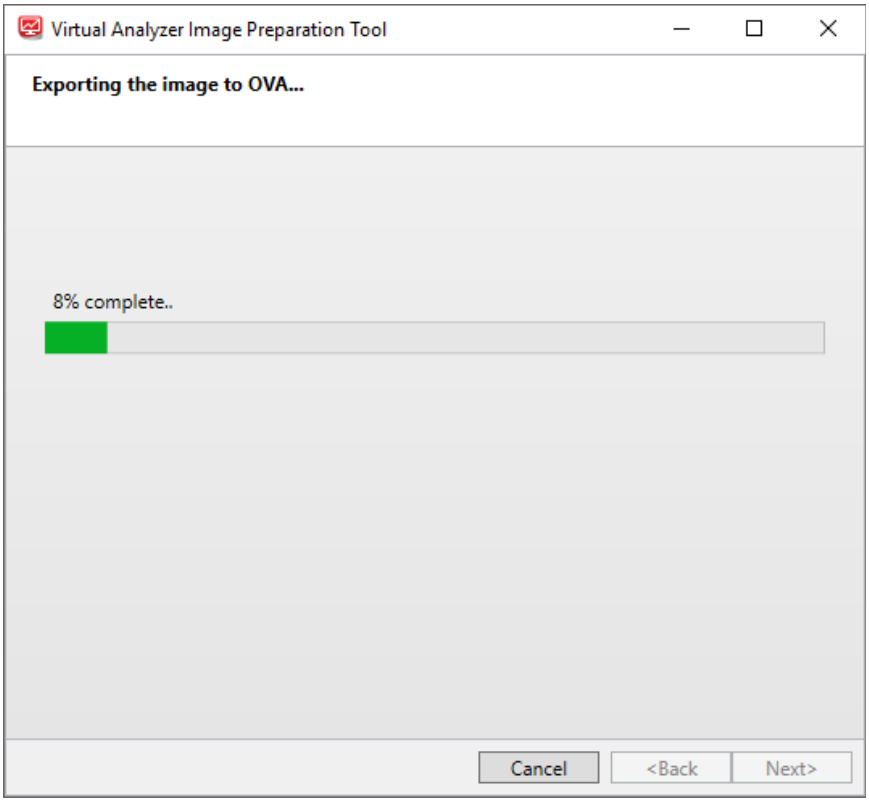


FIGURE 5-15. Export the image to OVA screen

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

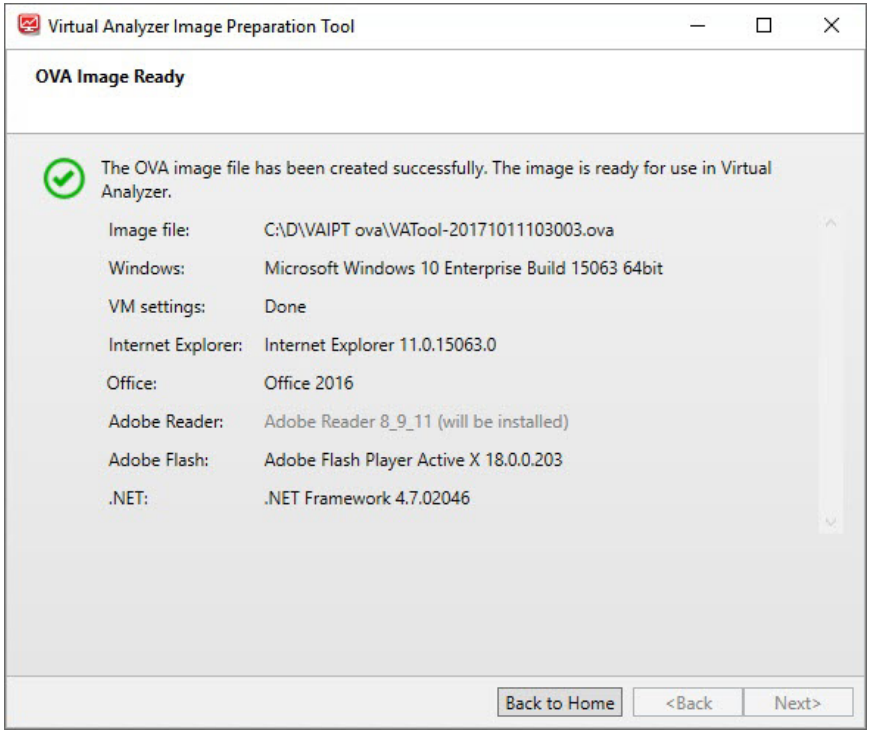


FIGURE 5-16. OVA Image Ready screen for Windows images

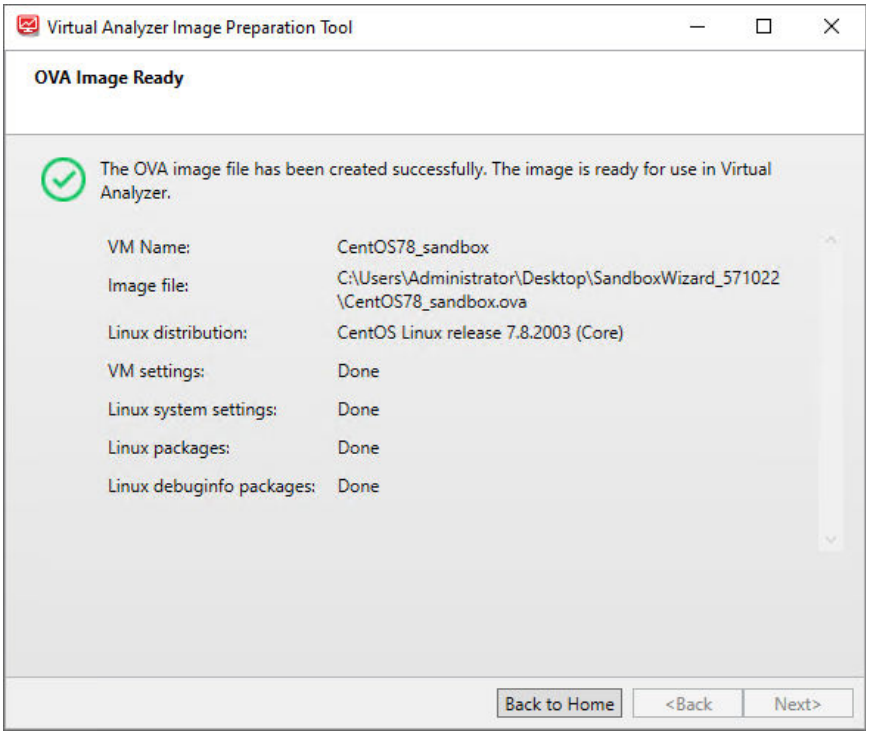


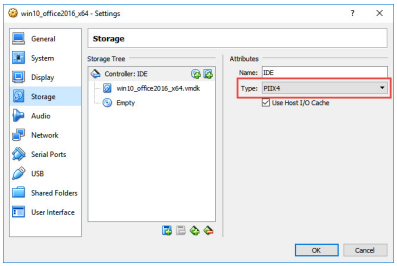
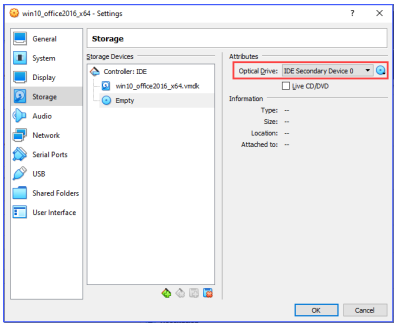
FIGURE 5-17. OVA Image Ready screen for Linux images

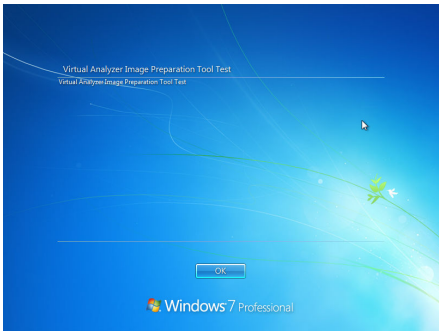
11. Click the **Close** button in the upper right corner to exit the tool or click **Back to Home** to create another image.

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.
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.	
	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 **PIIX4**.  **Figure 5-18. Controller: IDE must be set to PIIX4** • Select the optical disc icon and verify that the specified **CD/DVD drive** is **IDE Secondary Device 0**.  **Figure 5-19. CD/DVD drive is set to IDE Secondary Device 0**

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

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

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

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

Issue	Cause	Recommended Action
Unable to prepare a virtual machine image.	The VirtualBox virtual machine type is not supported.	Use the correct virtual machine type. • Type: Linux • Version: 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 7.9.2009 distribution ISO `rhel-server-7.9-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]                                     G
kerneldebuginfo-3.10.01127.el7.x86_64       kerneldebuginfo-3.10.01127.el7.x86_64           - OK
gccdebuginfo-4.8.539.el7.x86_64             gccdebuginfo-4.8.539.el7.x86_64                 - OK
openssldebuginfo-1.0.2k19.el7.x86_64        openssldebuginfo-1.0.2k19.el7.x86_64            - OK
curldebuginfo-7.29.057.el7.x86_64           curldebuginfo-7.29.057.el7.x86_64               - OK
zlibdebuginfo-1.2.718.el7.x86_64            zlibdebuginfo-1.2.718.el7.x86_64                - OK
glibcdebuginfo-2.17307.el7.1.x86_64         glibcdebuginfo-2.17307.el7.1.x86_64             - OK
```

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

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


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


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


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


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


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


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

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: APEM629665/221221