TREND MICRO™

Virtual Analyzer Image Preparation

User's Guide

Document Part No.: APEM16860/150128

Release Date: January 2016

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:

http://docs.trendmicro.com/en-us/survey.aspx

Table of Contents

Chapter 1

About this Guide

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

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

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

OVA File Creation Using New Virtual Machine Images

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

Creating 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 2-4*.

3. Create a virtual machine image.

   For details, see *Creating Virtual Machine Images on page 2-5*.

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

   For details, see *Exporting Virtual Machine Images to OVA Files on page 2-20*.

Required Software

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

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 Server 2003/2003 R2 • Windows Server 2008/2008 R2 **Important** • Package the installer as an ISO file. • Disable automatic updates. • Trend Micro recommends using the English version of the listed operating systems.
Microsoft Office	Virtual Analyzer supports the following versions: • 2003 (32-bit) • 2007 (32-bit) • 2010 (32-bit) • 2013 (32-bit) **Important** • Verify that your license allows you to virtualize the applications. For details, see https://support.office.com. • Disable automatic updates. • Enable macros.

SOFTWARE	DESCRIPTION
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 images during importing. • Uses all three versions during analysis. **WARNING!** This consumes additional computing resources. • Installs .NET Framework 3.5 or later if the operating system is Windows XP or Windows Server 2003. Configure Adobe Reader to manually check for and install updates. For details, see https://helpx.adobe.com/acrobat/kb/reader-acrobat-updater-settings.html.

Important

Do not install VMware tools to avoid triggering the anti-virtual machine functions of some malware.

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**.

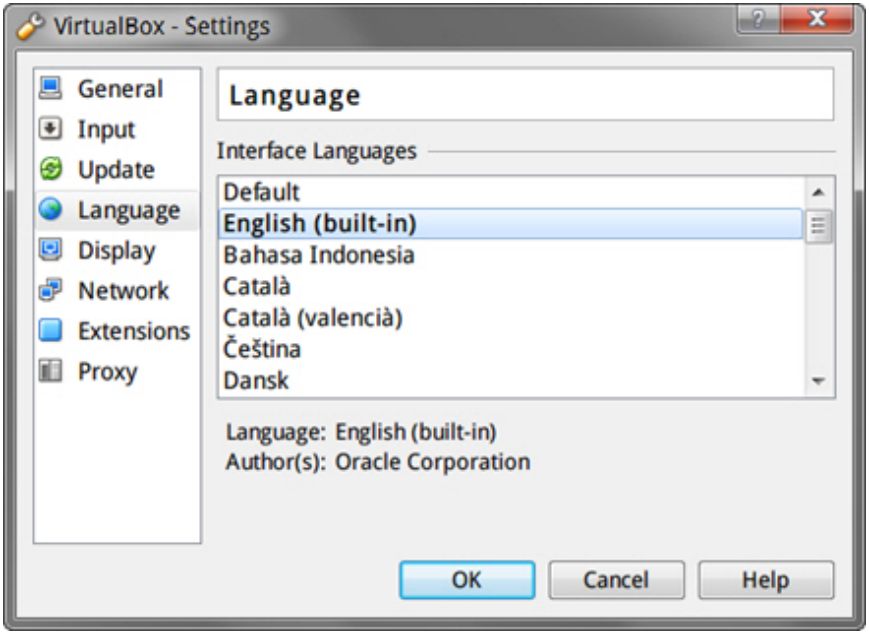


FIGURE 2-1. Language Settings

Creating Virtual Machine Images

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.

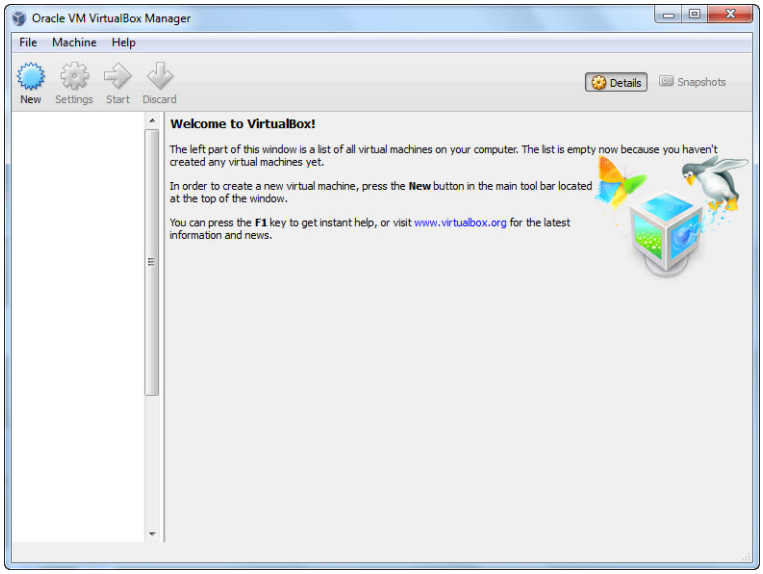


FIGURE 2-2. VirtualBox Manager

2. Click **New**.

The **Create Virtual Machine** window opens.

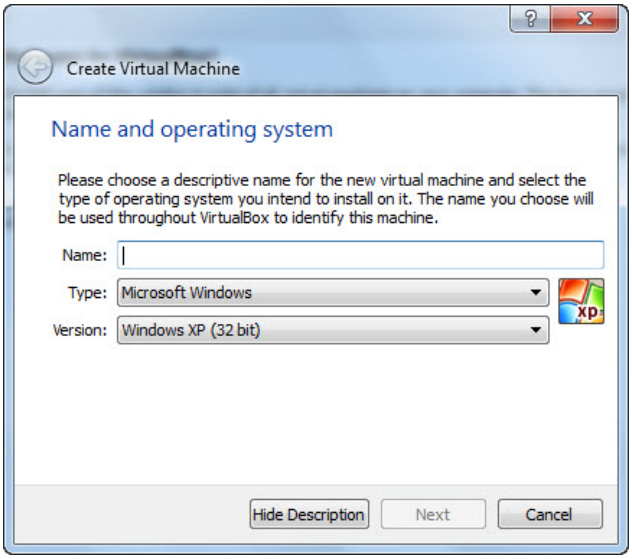


FIGURE 2-3. Create Virtual Machine

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

The **Memory size** screen appears.

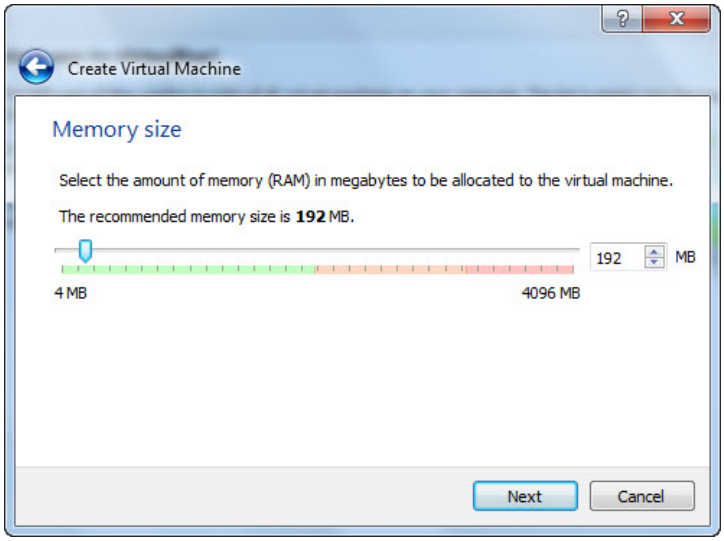


FIGURE 2-4. Memory Size

5. Specify the recommended memory size for your operating system.
   - Windows XP and Windows Server 2003: 512 MB
   - Windows 7/8/8.1 and Windows Server 2008/2008 R2: 1024 MB
6. Click **Next**.

The **Hard drive** screen appears.

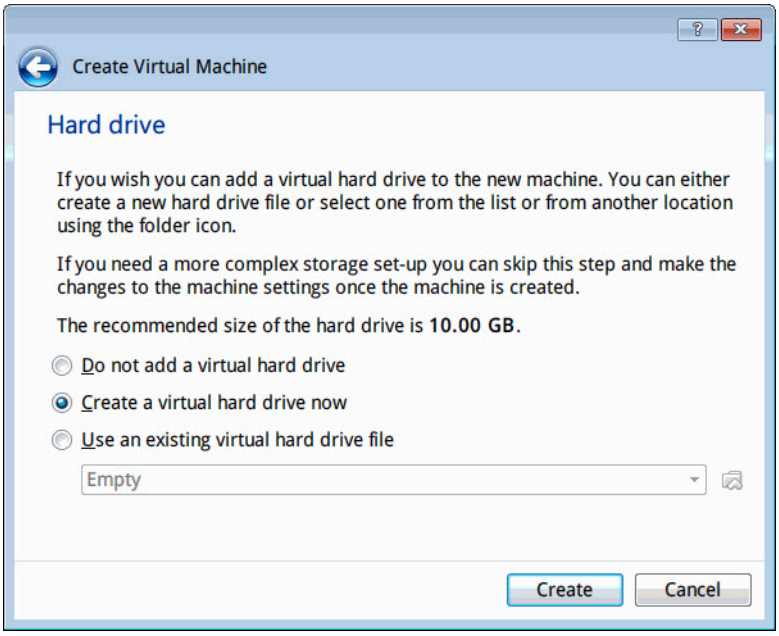
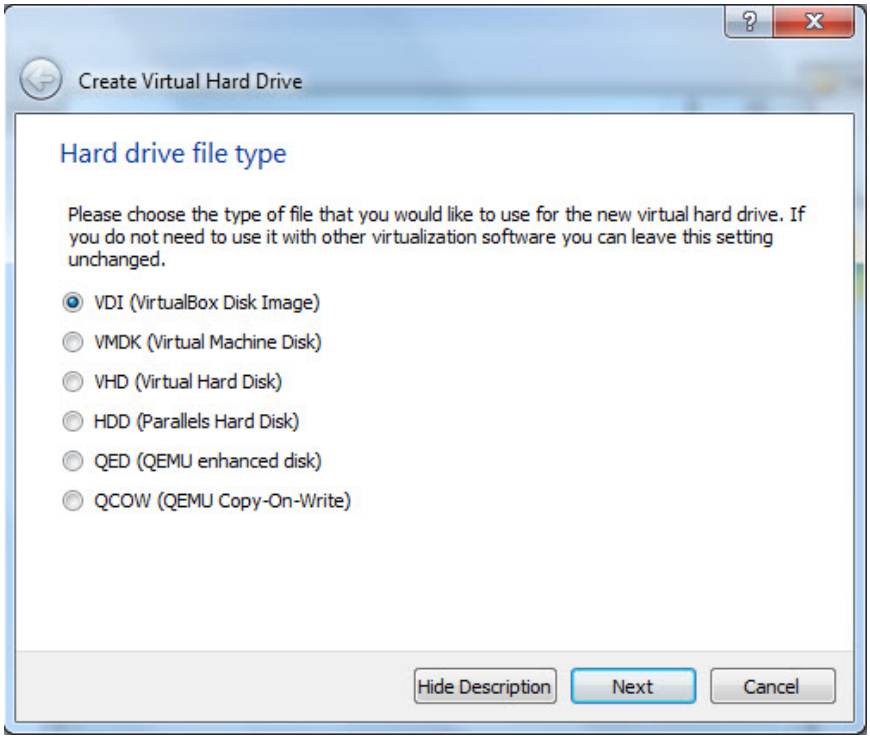


FIGURE 2-5. Create Virtual Hard Drive

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

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



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

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

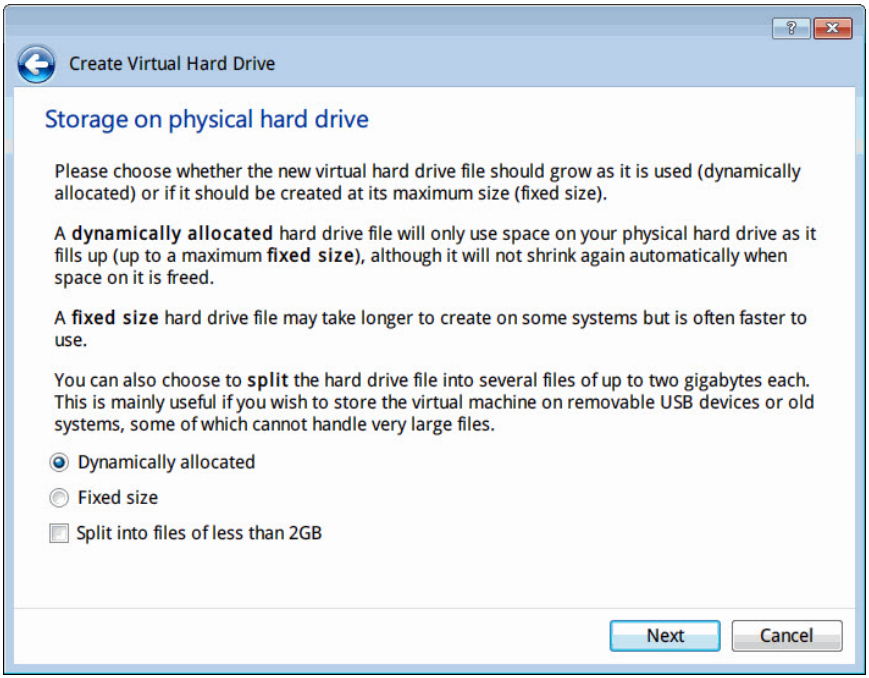


FIGURE 2-6. Storage on Physical Hard Drive

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

Note

If you selected **VMDK (Virtual Machine Disk)** as the hard drive file type, do not enable **Split into files of less than 2GB**.

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

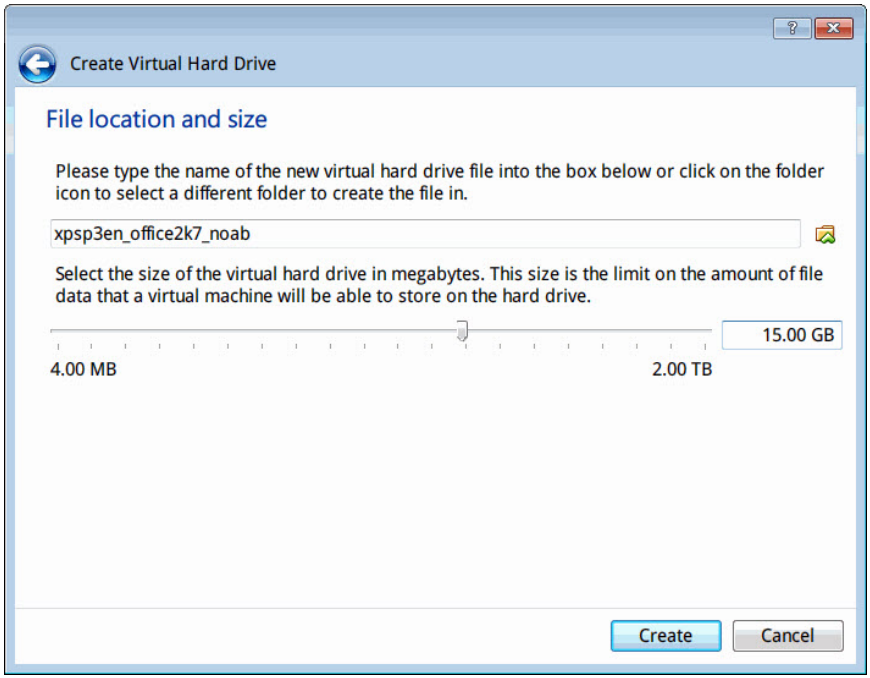


FIGURE 2-7. File Location and Size

10. (Optional) Click the folder icon to change the path of the virtual disk file.
11. Specify the recommended virtual disk size for your operating system.
    - Windows XP and Windows Server 2003: 15 GB
    - Windows 7/8/8.1 and Windows Server 2008/2008 R2: 25 GB
12. Click **Create**.

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

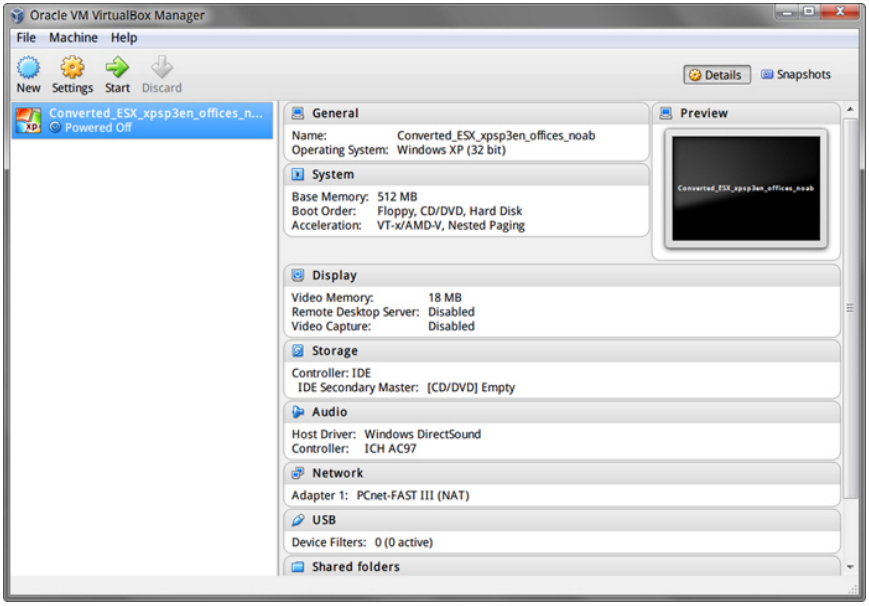


FIGURE 2-8. Newly-created Virtual Machine

13. Click **Settings**.

The **Settings** window opens.

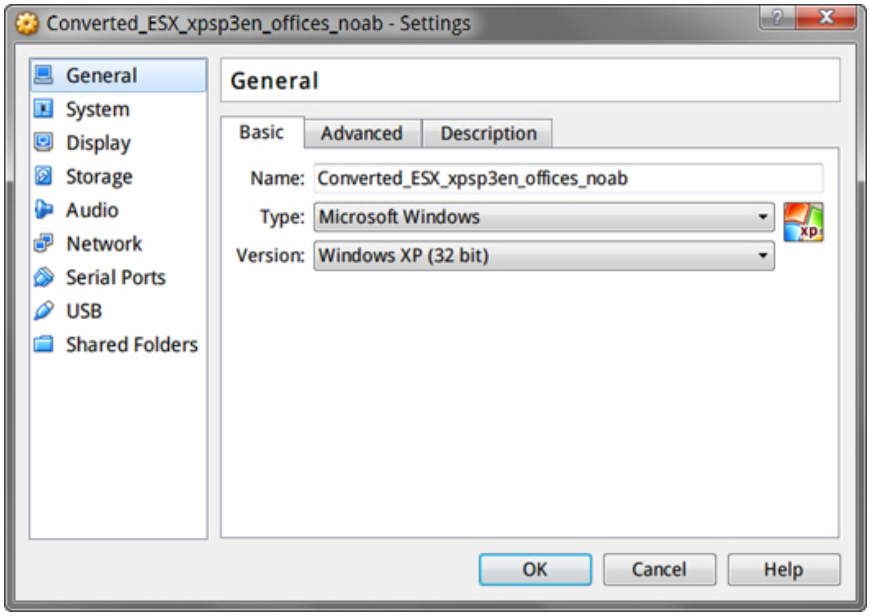


FIGURE 2-9. VirtualBox Settings

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

The **System** screen appears.

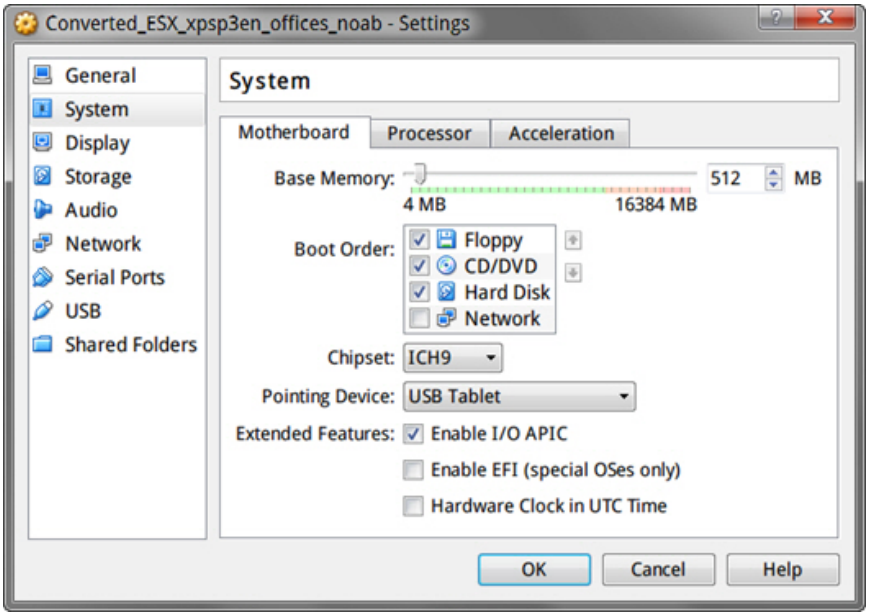
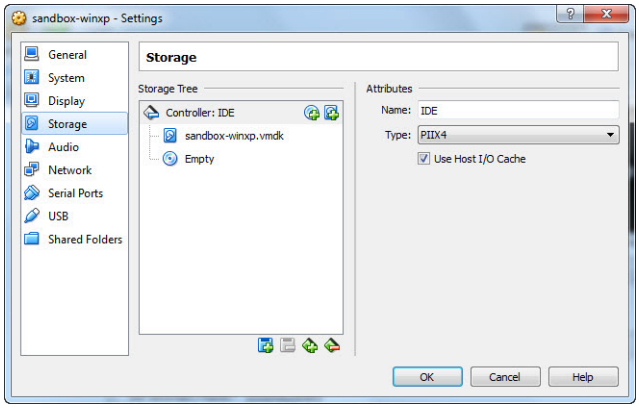


FIGURE 2-10. System Screen

15. On the **Motherboard** tab, configure the following:
    - **Chipset**: Select **ICH9**
    - **Pointing Device**: Select **USB Tablet**
    - **Extended Features**: Select **Enable IO APIC**
16. Go to the **Processor** tab and then select **Enable PAE/NX**.
17. Go to the **Acceleration** tab and then select **Enable VT-x/AMD-V** and **Enable Nested Paging**.
18. In the left pane, click **Storage**.

The **Storage** screen appears.



19. (Optional) If **Controller: SATA** appears under **Storage Tree**, remove the SATA controller and then add the virtual hard drive to the IDE controller.

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

    b. Click **Controller: IDE** and then click  .

    The following message appears:

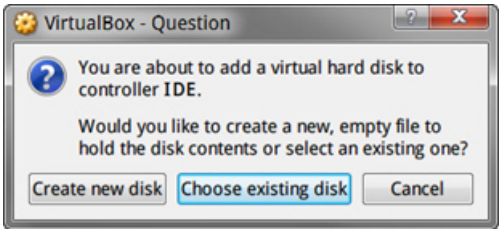


FIGURE 2-11. Choose Existing Disk

    c. Click **Choose existing disk** and then select the virtual hard disk file (*.vdi or *.vmdk) that you previously created.

    d. Under **Attributes**, retain all default settings.

e. Under **Storage Tree**, click **Controller: IDE** and then click the optical drive icon. Verify that **CD/DVD Drive** is **IDE Secondary Master**.

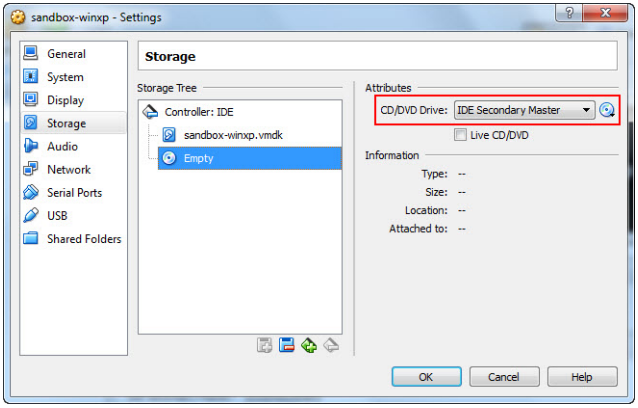


FIGURE 2-12. IDE SECONDARY MASTER

20. Under **Storage Tree**, click **Controller: IDE** and then click the optical drive icon.

21. Under **Attributes**, click the optical drive icon.

    A file menu appears.

22. Select **Choose a virtual CD/DVD disk file…** and then select the ISO file containing the operating system installer.

    The ISO file is available as a device.

23. In the left pane, click **Audio** and deselect **Enable Audio**.

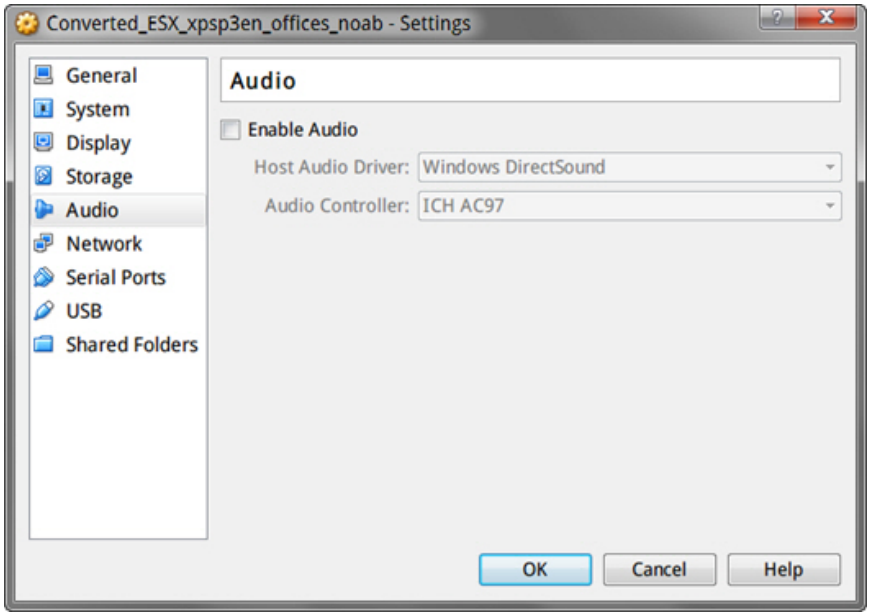


FIGURE 2-13. Audio Options Settings

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

Important

Verify that **Enable USB 2.0 (EHCI) Controller** is not selected.

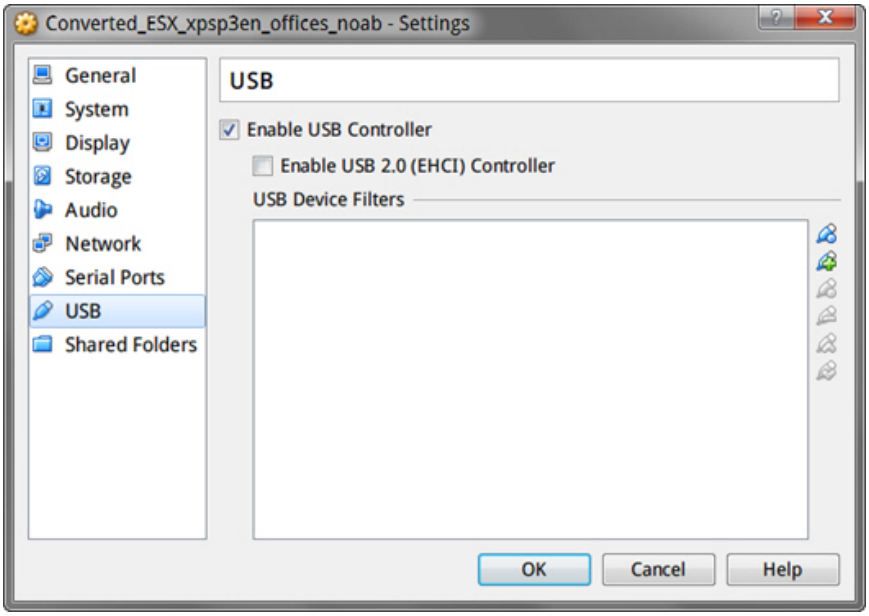


FIGURE 2-14. Enable USB Controller

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

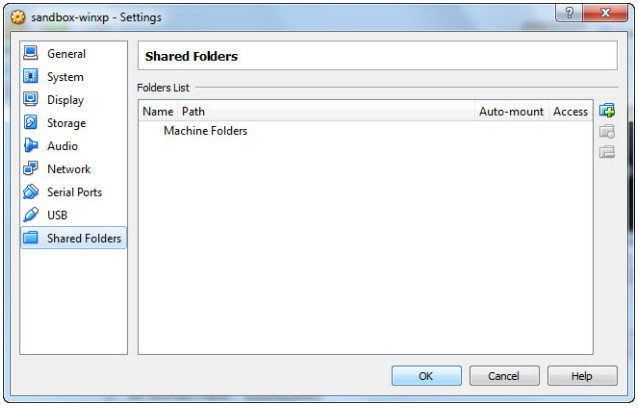


FIGURE 2-15. Shared Folders Settings

26. Click **OK**.

    The **Settings** window closes.

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

to power on the image.

    The installation process starts.

28. Follow the on-screen instructions to complete the installation.

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.

TABLE 2-2. Maximum OVA File Size

PRODUCT	VERSION	MAXIMUM FILE SIZE
Deep Discovery Inspector	3.8 and earlier	10 GB
	3.8 Service Pack 1 and later	20 GB
Deep Discovery Analyzer	5.1 and earlier	10 GB
	5.5	20 GB
Deep Discovery Email Inspector	2.1 and earlier	10 GB
	2.5	20 GB
Trend Micro TippingPoint Advanced Threat Protection for Networks	3.8 Service Pack 2	20 GB
Trend Micro TippingPoint Advanced Threat Protection for Email	2.5	20 GB
Trend Micro TippingPoint Advanced Threat Protection Analyzer	5.5	20 GB

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.

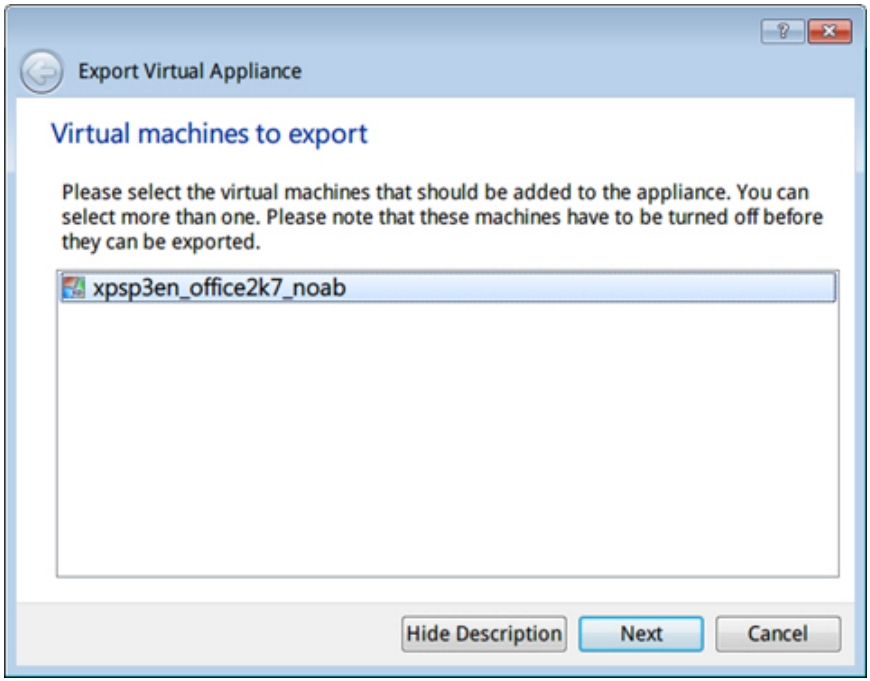


FIGURE 2-16. Export Virtual Appliance

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

The **Storage settings** screen appears.

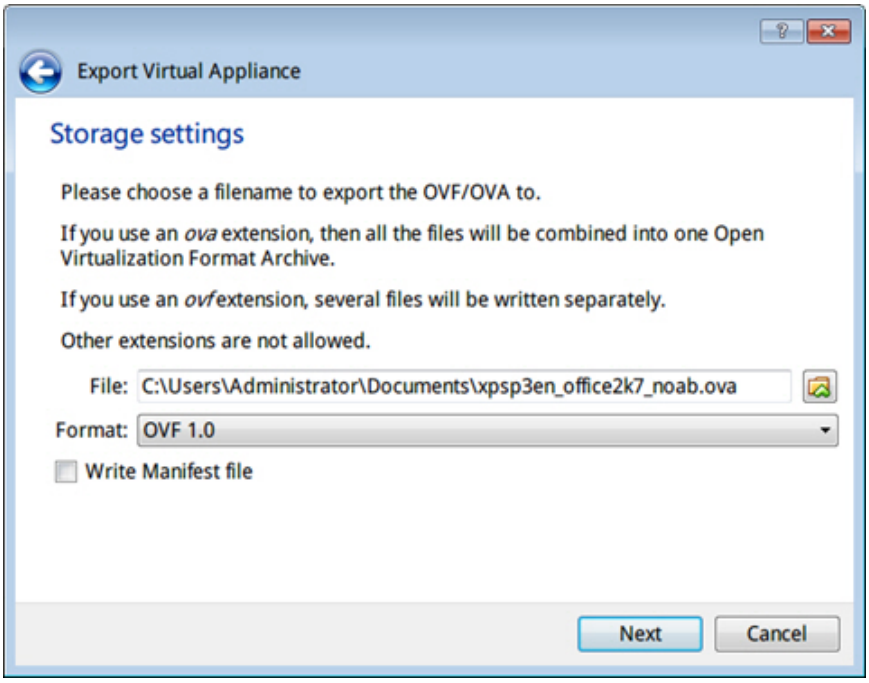


FIGURE 2-17. Storage Settings

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.

5. Click **Next**.

The **Appliance settings** screen appears.

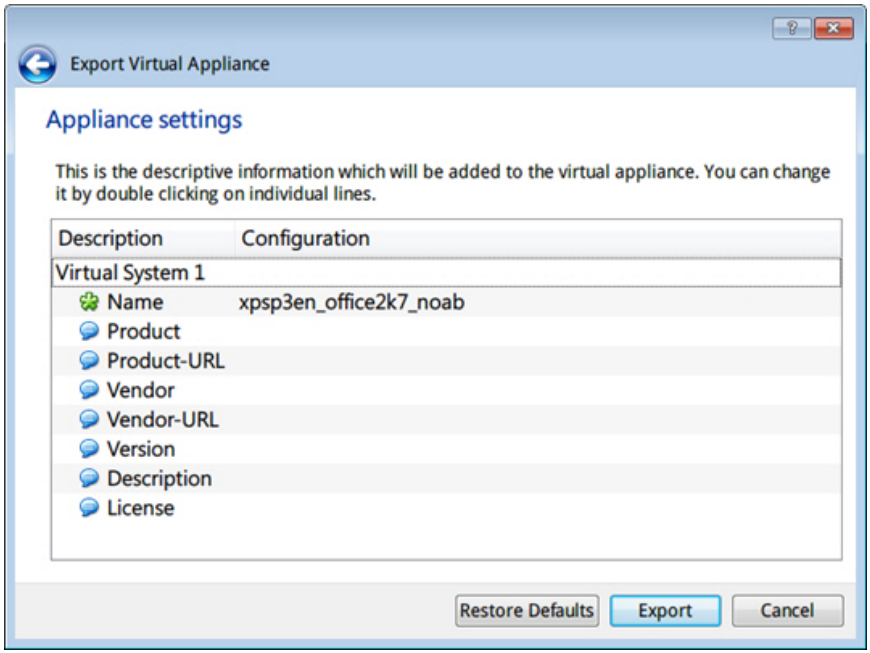


FIGURE 2-18. Export Virtual Appliance - Appliance Settings

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

VirtualBox creates the OVA file.

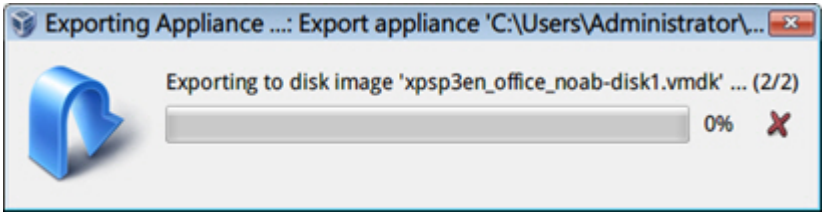


FIGURE 2-19. Disk Image Export Progress Bar

Chapter 3

OVA File Creation Using Converted Virtual Hard Disk Drives

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

Creating OVA Files Using Converted Virtual Hard Disk Drives

Procedure

1. Prepare Adobe Reader.

   For details, see *Preparing Adobe Reader on page 3-5*

2. Modify the environment of the virtual machine image.

   For details, see *Modifying the Virtual Machine Environment on page 3-5*.

3. Reduce the size of the virtual hard disk drive.

   For details, see *Reducing the Size of Virtual Hard Disk Drives on page 3-14*.

4. Export the virtual machine image.

   For details, see *Exporting Virtual Machine Images on page 3-15*.

5. 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 3-22*.

6. 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 3-29*.

7. Configure the new virtual machine image.

   For details, see *Configuring Virtual Machine Images on page 3-41*.

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

   For details, see *Exporting Virtual Machine Images to OVA Files on page 2-20*.

Required Software

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

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 Server 2003/2003 R2 • Windows Server 2008/2008 R2 **Important** • Package the installer as an ISO file. • Disable automatic updates. • Trend Micro recommends using the English version of the listed operating systems.

SOFTWARE	DESCRIPTION
Microsoft Office	Virtual Analyzer supports the following versions: • 2003 (32-bit) • 2007 (32-bit) • 2010 (32-bit) • 2013 (32-bit) **Important** • Verify that your license allows you to virtualize the applications. For details, see https://support.office.com. • Disable automatic updates. • Enable macros.
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 images during importing. • Uses all three versions during analysis. **WARNING!** This consumes additional computing resources. • Installs .NET Framework 3.5 or later if the operating system is Windows XP or Windows Server 2003. Configure Adobe Reader to manually check for and install updates. For details, see https://helpx.adobe.com/acrobat/kb/reader-acrobat-updater-settings.html.

Important

Do not install VMware tools to avoid triggering the anti-virtual machine functions of some malware.

Preparing Adobe Reader

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

Procedure

1. Disable automatic updates.

   For details, see http://helpx.adobe.com/acrobat/kb/disable-automaticupdates-acrobat-reader.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.

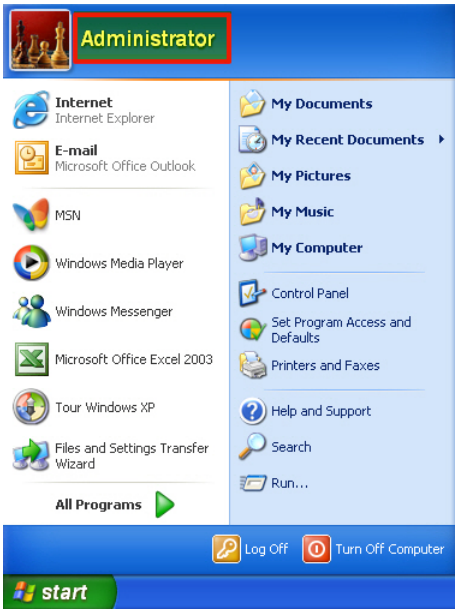
- *Modifying the Virtual Machine Environment (Windows XP and Windows Server 2003) on page 3-6*

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 3-1. 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`
Disable Windows Firewall.	Type `netsh firewall set opmode mode=DISABLE`.

TASK	STEPS
	Note Windows Firewall slows down the installation of Virtual Analyzer Sensors.
Uninstall VMware Tools.	For details, see *Uninstalling VMware Tools on page 3-12*.

3. Restart the virtual machine.

Modifying the Virtual Machine Environment (Windows 7/8/8.1 and Windows Server 2008/2008 R2)

Procedure

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

TASK	STEPS
Enable the "Administrator" account.	Type `net user "Administrator" /active:yes`.
Set the logon password for the "Administrator" account to "1111".	Type `net user "Administrator" 1111`.
Configure automatic logon from the administrator account.	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`

<table>
<tr><th>TASK</th><th>STEPS</th></tr>
<tr><td>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>
\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, launch the Local Security Policy snap-in (<code>secpol.msc</code>) to disable the Password must meet complexity requirements Local Security Setting.

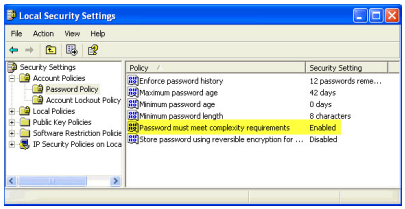
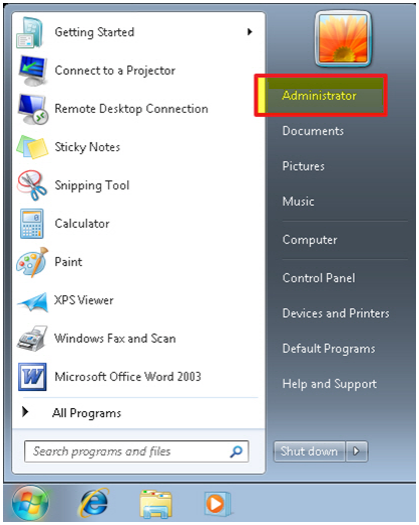
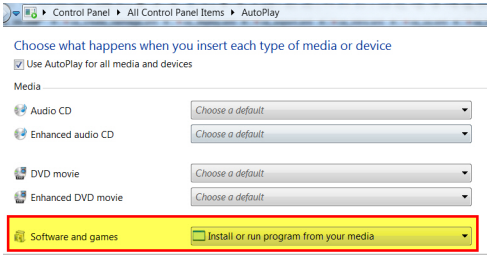


FIGURE 3-2. Disable Password must meet complexity requirements

• Restart the image.
</td></tr>
</table>

TASK	STEPS
	No logon prompt is displayed and the "Administrator" account is automatically used to log on.  **FIGURE 3-3. 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`

TASK	STEPS
	a. Go to **Control Panel** > **AutoPlay**.  **FIGURE 3-4. AutoPlay** b. For **Software and games**, select **Install or run program from your media**. c. Click **Save**.
Disable Windows Firewall.	• Windows 8/8.1: a. Go to **Control Panel**. b. In the search box, type `Windows Firewall`. c. Click **Turn Windows Firewall on or off**. • Windows 7 and Windows Server 2008/2008 R2: a. Open a Command Prompt window. b. 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 3-12*.

3. 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 and Windows Server 2008/2008 R2: Click **Programs and Features**.

A list of installed programs appears.

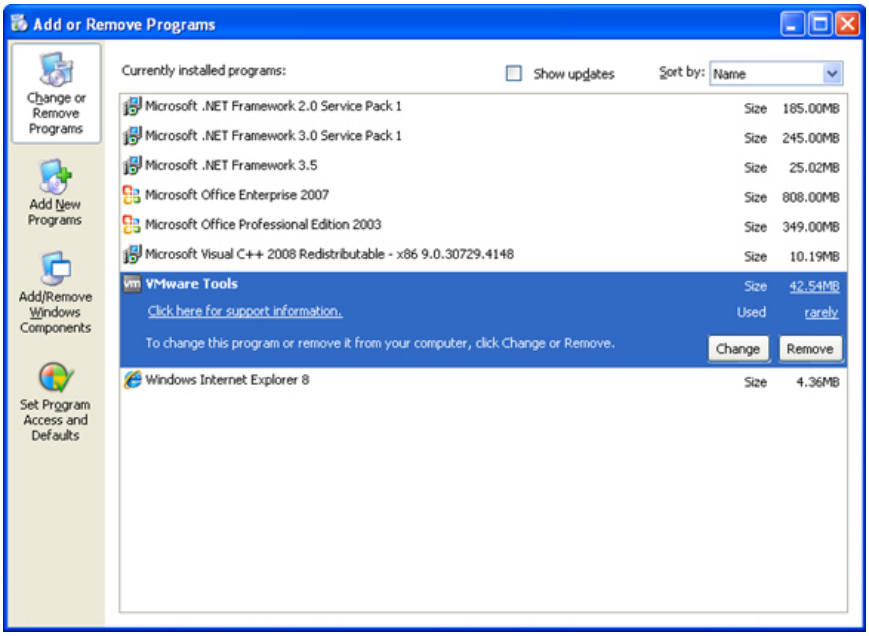


FIGURE 3-5. Add or Remove Programs (Windows XP)

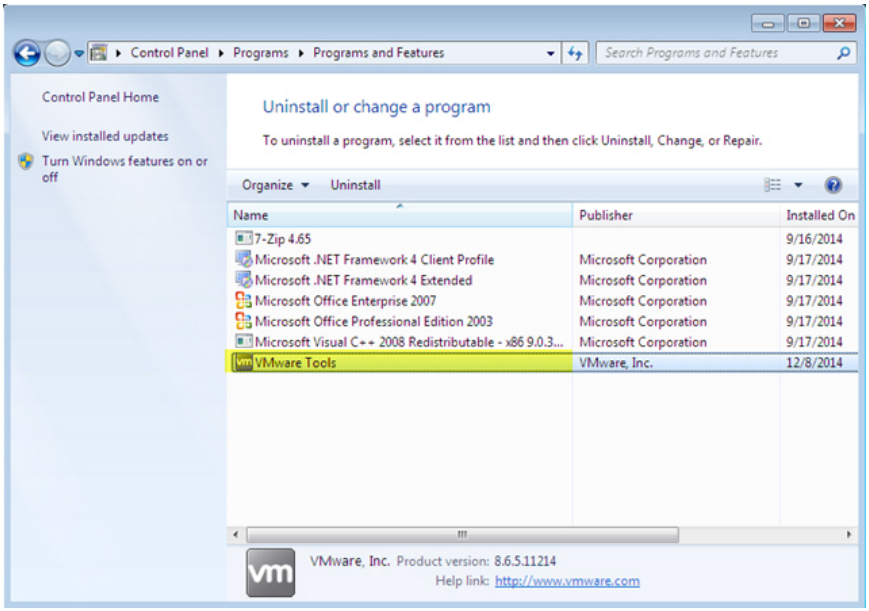


FIGURE 3-6. Add or Remove Programs (Windows 7)

3. Select **VMware Tools** and then click **Remove** (Windows XP or Windows Server 2003) or **Uninstall** (Windows 7/8/8.1 or Windows Server 2008/2008 R2).
4. Click **Yes** to uninstall VMware Tools.
5. Click **Yes** to restart Windows.

VMware Tools is uninstalled.

Reducing the Size of Virtual Hard Disk Drives

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. Download SDelete and then zero out the free space on the virtual 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 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]`**.

Exporting Virtual Machine Images

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

- *Verifying Virtual Machine Settings on VMware Workstation on page 3-16*
- *Exporting Virtual Machine Images on VMware ESXi on page 3-18*
- *Converting VMware ESXi Virtual Hard Disk Drives on page 3-22*

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.

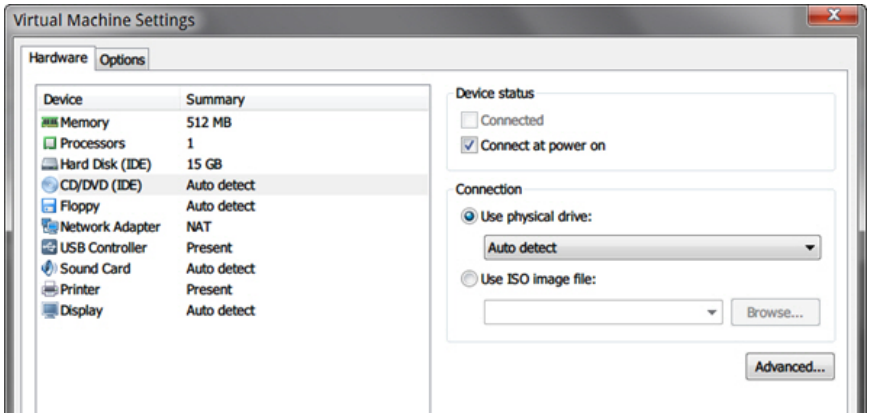


FIGURE 3-7. Virtual Machine Settings

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

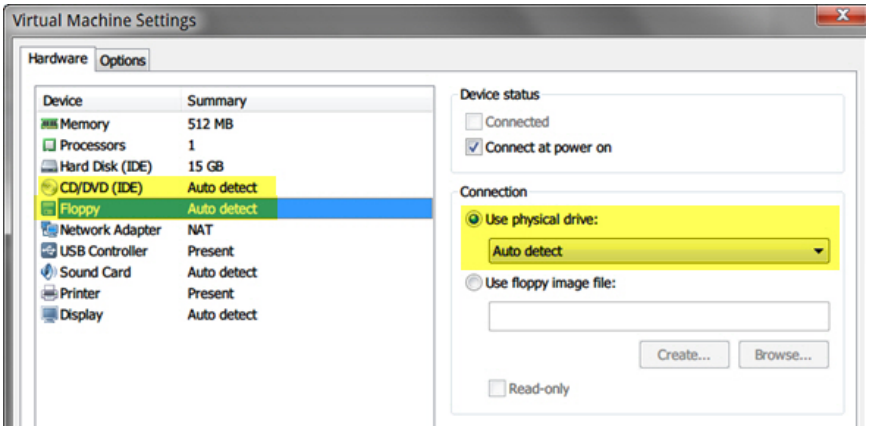


FIGURE 3-8. Virtual Machine Settings - Hardware

4. Go to the **Options** tab and then click **General**.

5. In the right pane, under **Working directory**, locate the Virtual Machine Disk (`*.vmdk`).

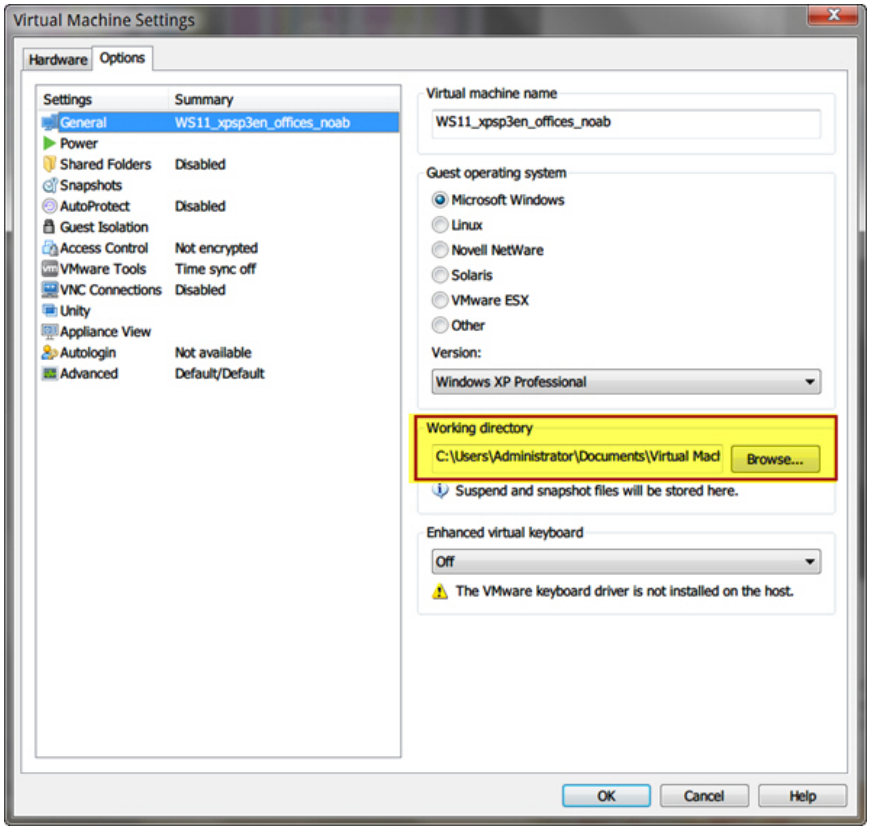


FIGURE 3-9. Working Directory

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**.

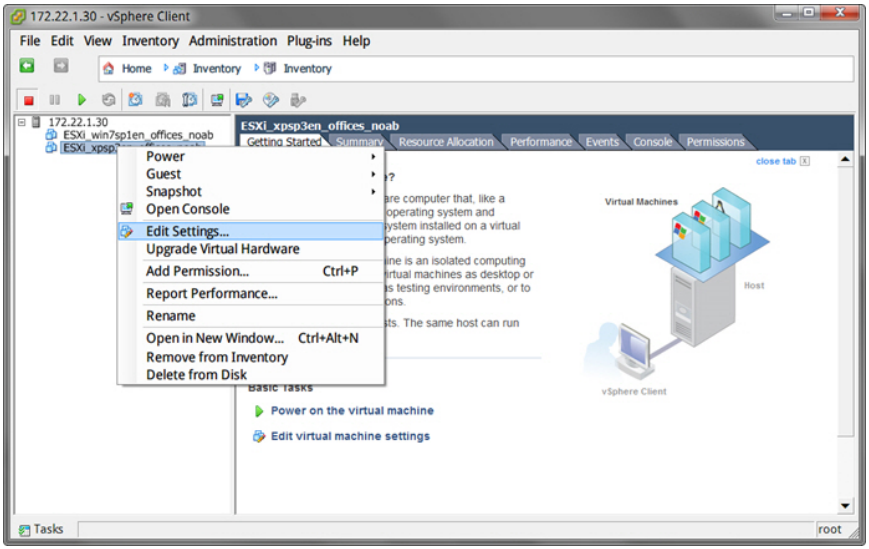


FIGURE 3-10. Edit Settings

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**

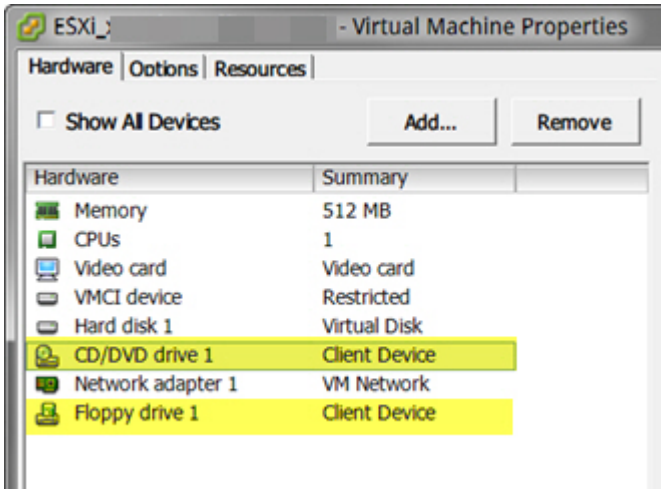


FIGURE 3-11. Virtual Machine Properties - Hardware

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

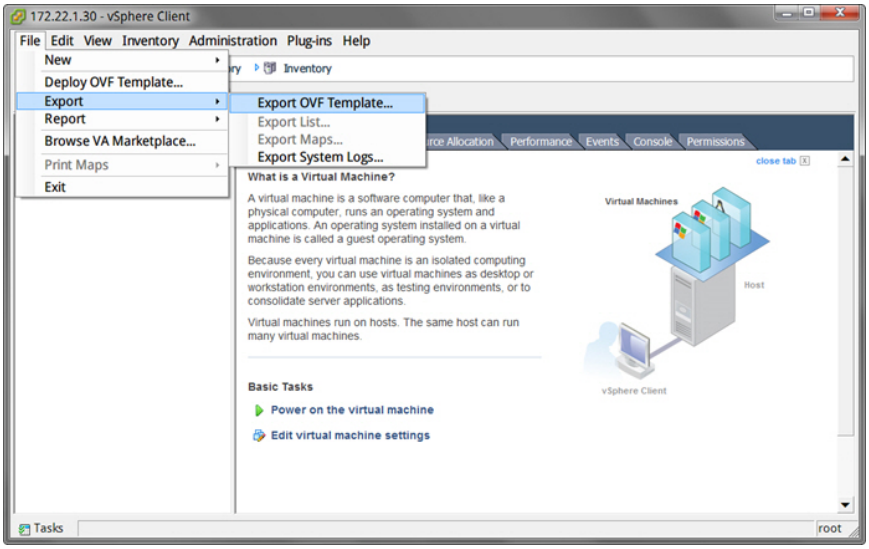


FIGURE 3-12. OVF Template

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 3-22*
- *Using QEMU on page 3-28*

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**.

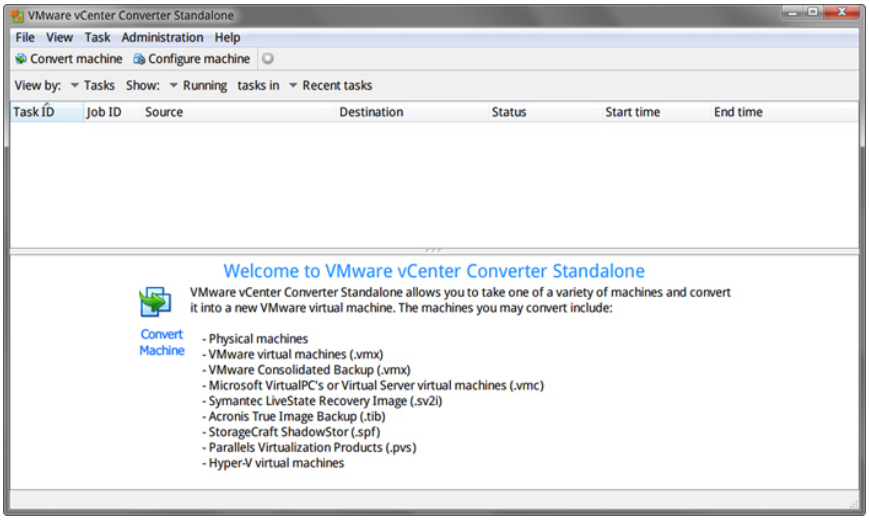


FIGURE 3-13. VMware vCenter Converter Standalone

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.

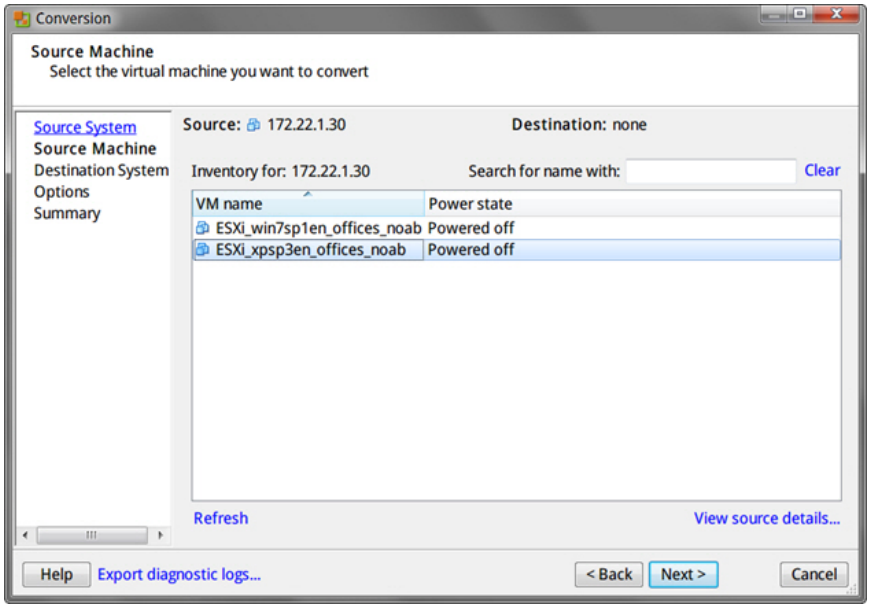


FIGURE 3-14. Conversion > Source Machine

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

The **Destination System** section appears.

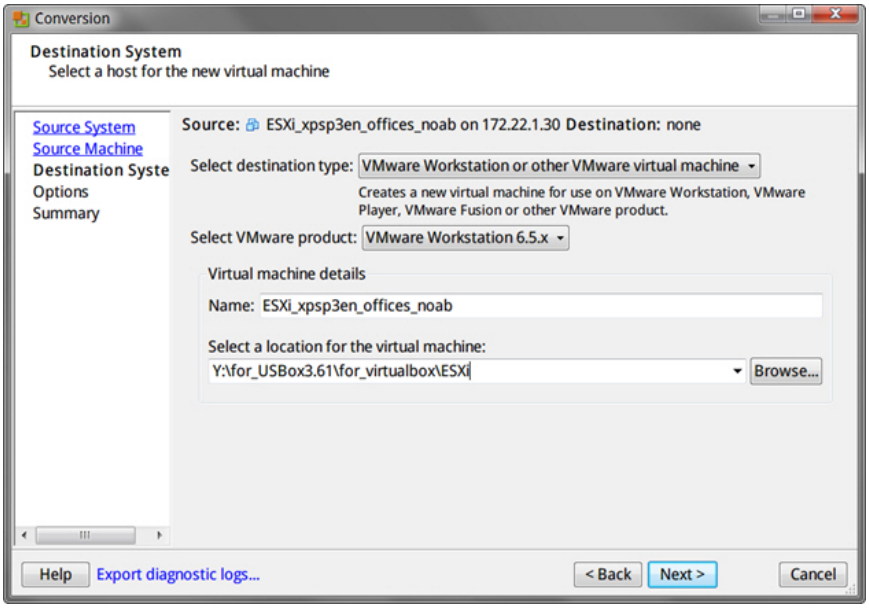


FIGURE 3-15. Conversion > Destination System

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.

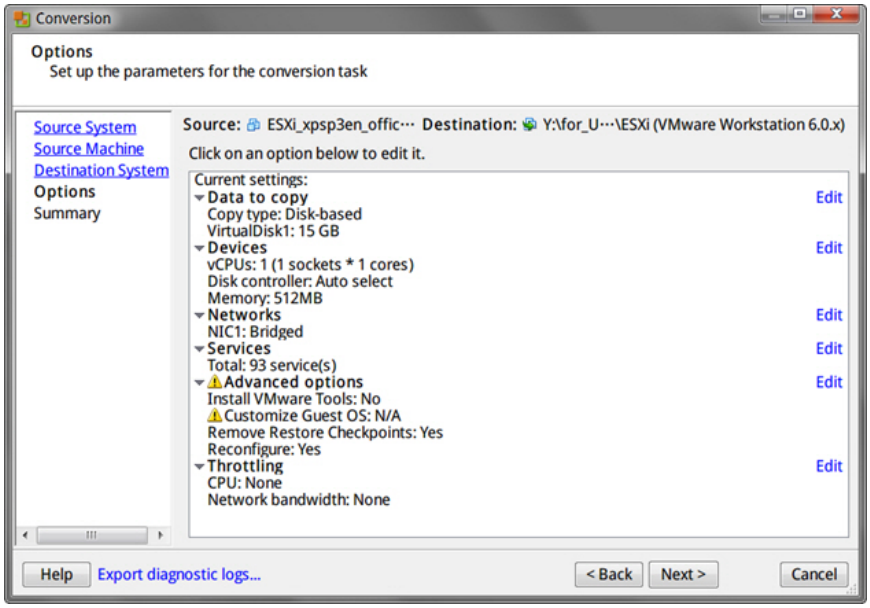


FIGURE 3-16. Conversion > Options

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

Important

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

The **Summary** screen appears.

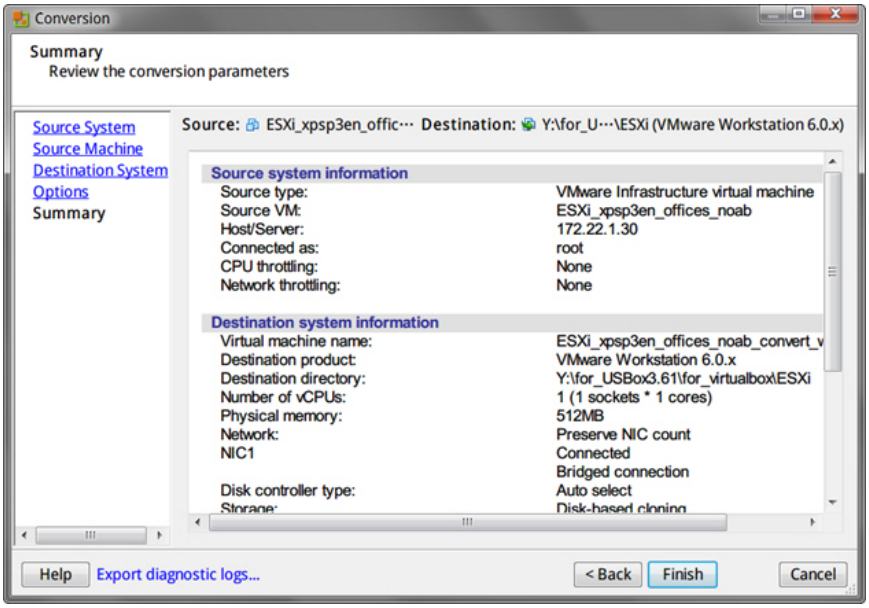


FIGURE 3-17. Conversion > Summary

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

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

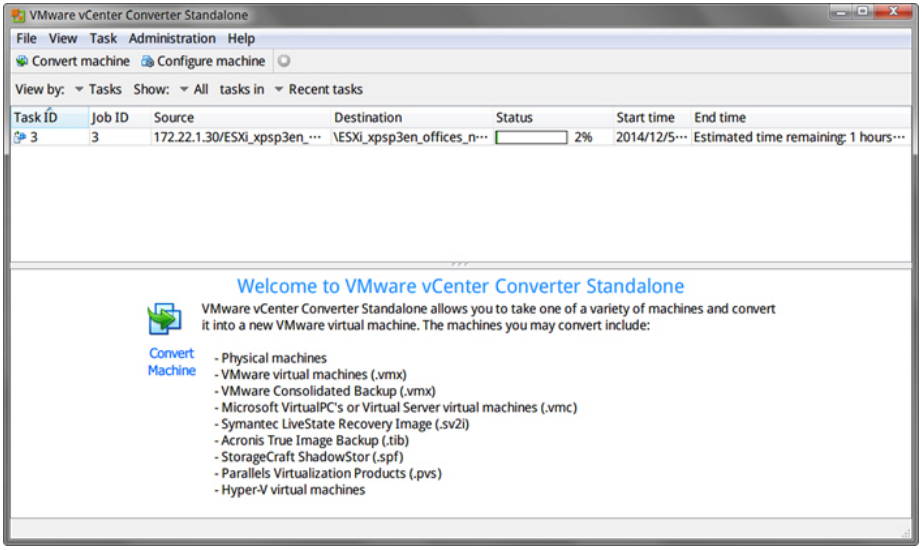


FIGURE 3-18. Image Conversion Progress

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 2-4*
- *Creating Virtual Machine Images Using VirtualBox on page 3-30*

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**.

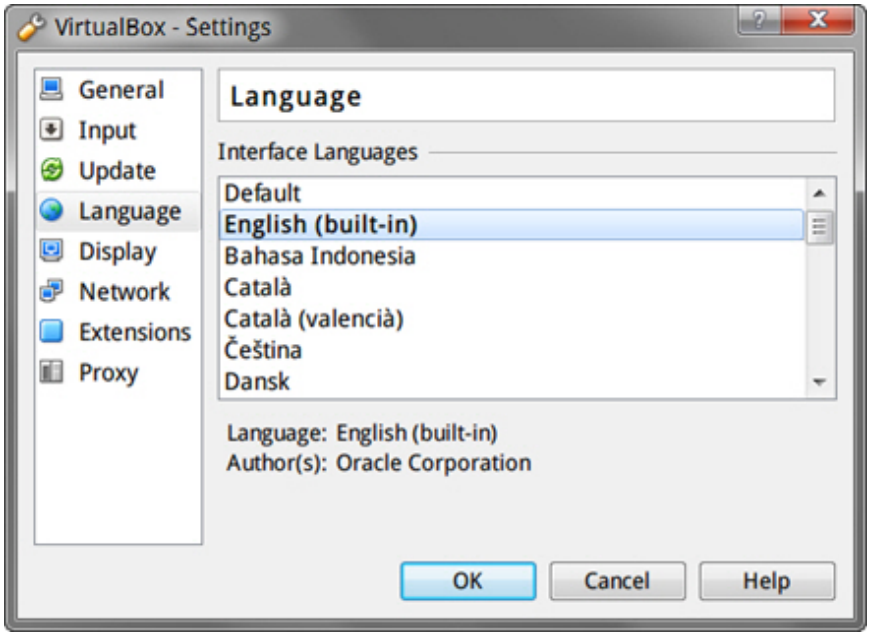


FIGURE 3-19. Language Settings

Creating Virtual Machine Images Using VirtualBox

Procedure

1. Open VirtualBox.

The **VirtualBox Manager** window opens.

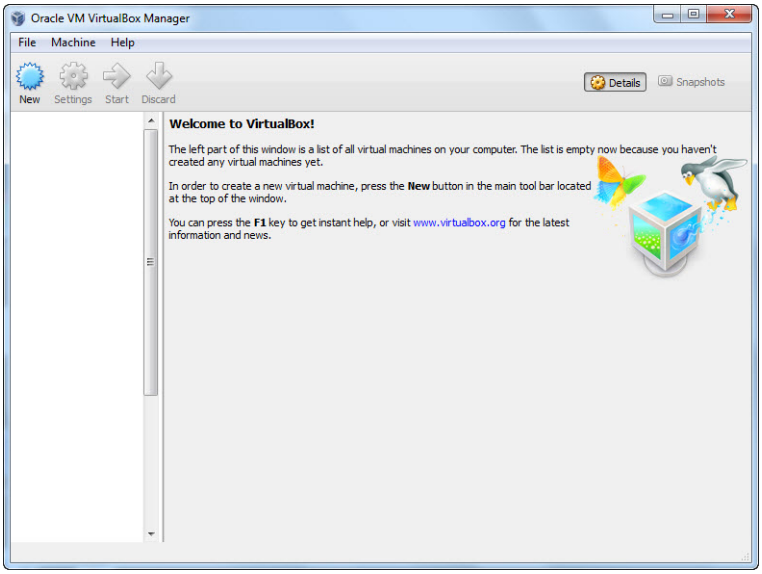


FIGURE 3-20. VirtualBox Manager

2. Click **New**.

The **Create Virtual Machine** window opens.

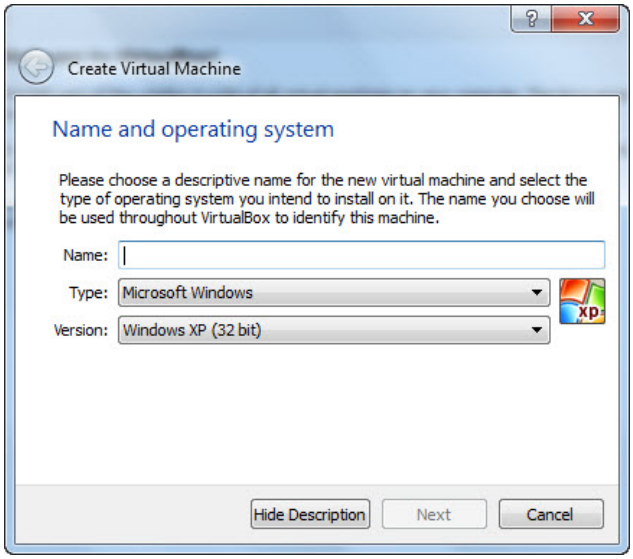


FIGURE 3-21. Create Virtual Machine

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 2008**, or **Windows 2008 R2**.
4. Click **Next**.

The **Memory size** screen appears.

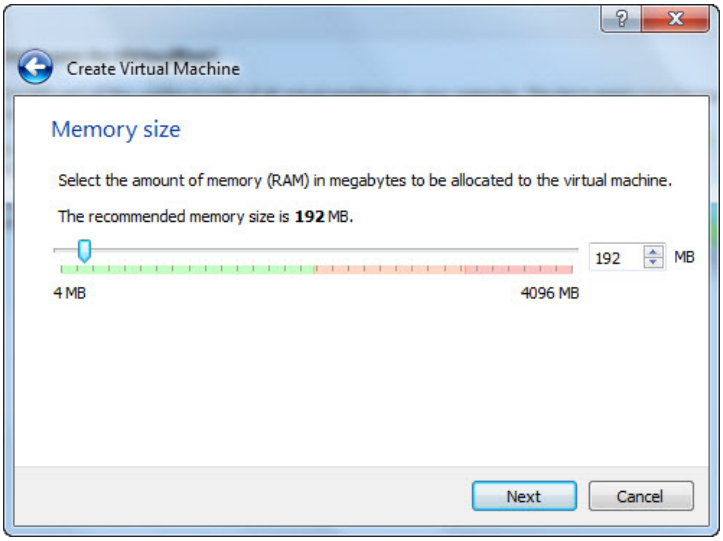


FIGURE 3-22. Memory Size

5. Specify the recommended memory size for your operating system.
   - Windows XP and Windows Server 2003: 512 MB
   - Windows 7/8/8.1 and Windows Server 2008/2008 R2: 1024 MB
6. Click **Next**.

The **Hard drive** screen appears.

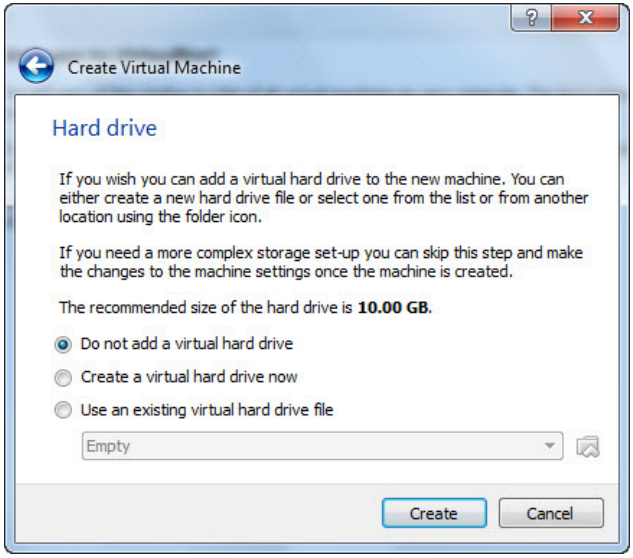
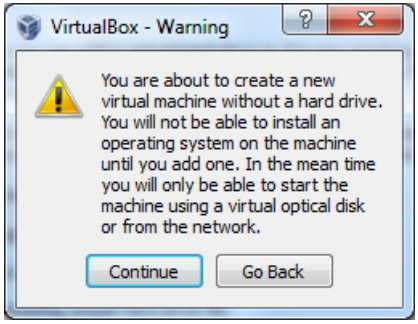


FIGURE 3-23. Hard Drive

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

   The following message appears:



8. Click **Continue**.

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

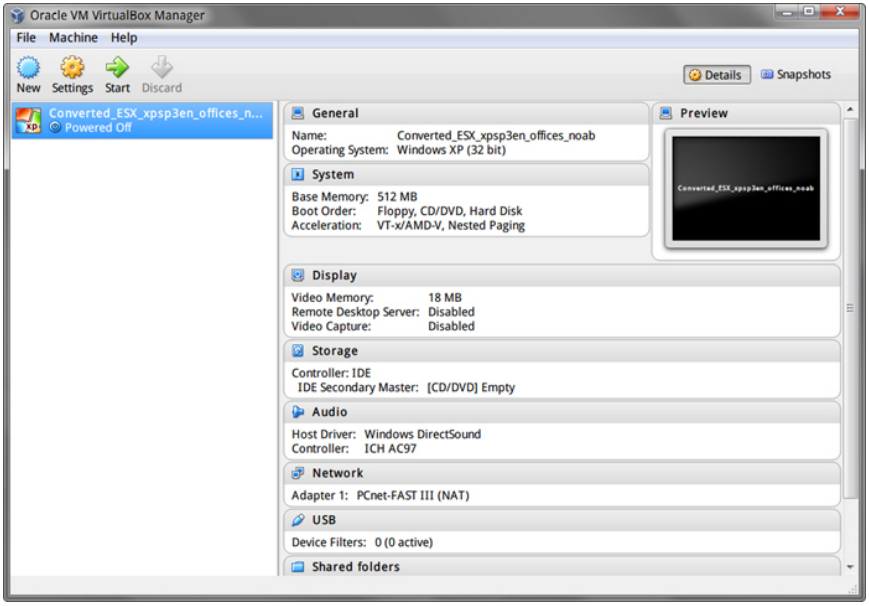


FIGURE 3-24. Newly-created Virtual Machine

9. Click **Settings**.

The **Settings** window opens.

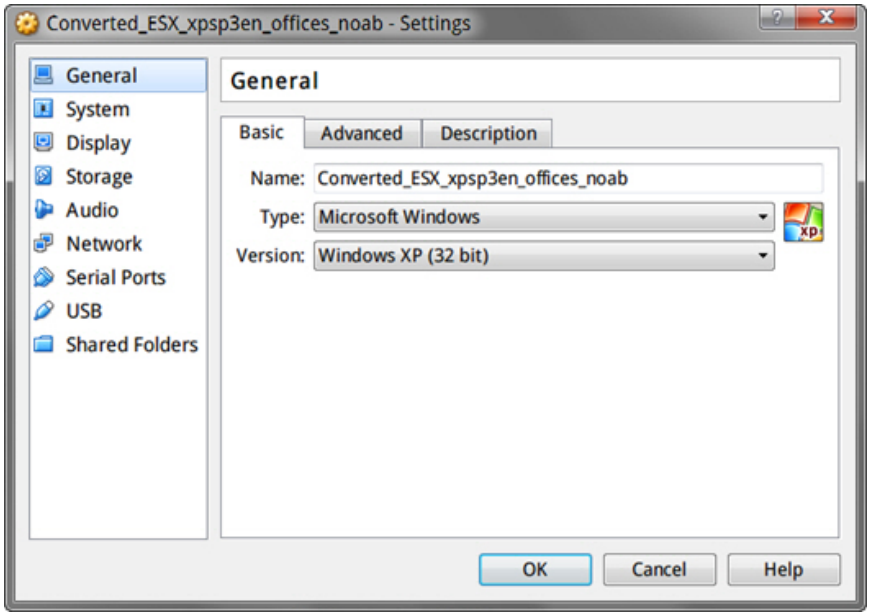


FIGURE 3-25. VirtualBox Settings

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

The **System** screen appears.

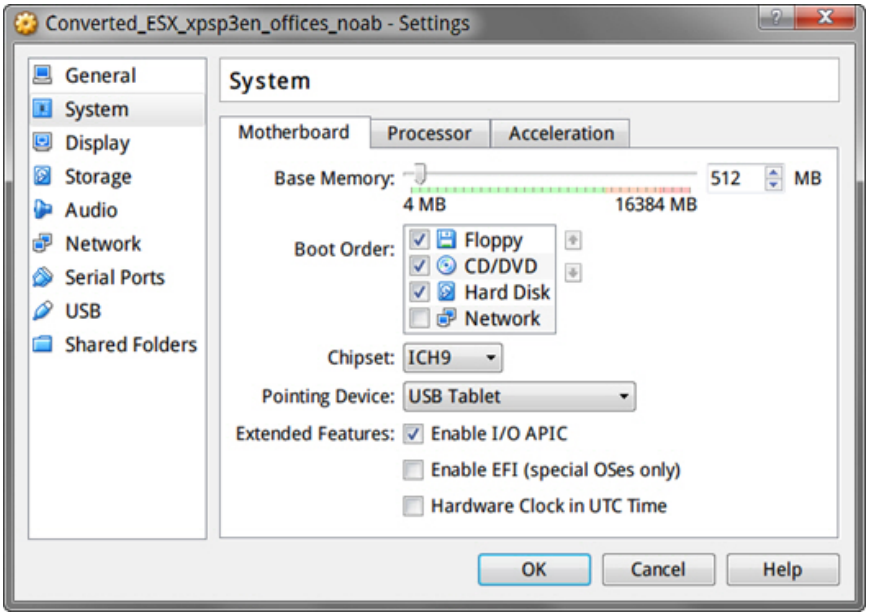
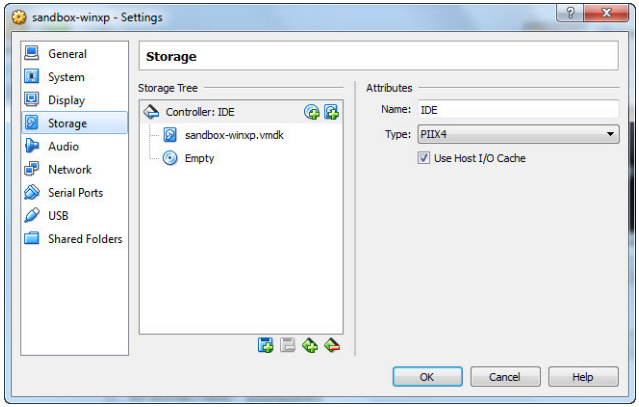


FIGURE 3-26. System Options

11. On the **Motherboard** tab, configure the following:
    - **Chipset**: Select **ICH9**.
    - **Pointing Device**: Select **USB Tablet**.
    - **Extended Features**: Select **Enable IO APIC**.
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**.
14. In the left pane, click **Storage**.

The **Storage** screen appears.



15. (Optional) If **Controller: SATA** appears under **Storage Tree**, remove the SATA controller and then add the virtual hard drive to the IDE controller.

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

    b. Click **Controller: IDE** and then click  .

    The following message appears:

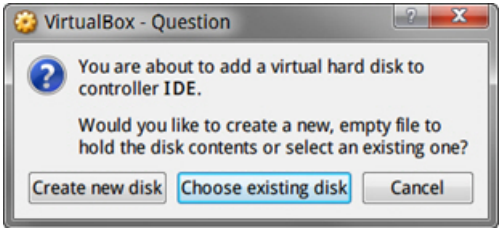


FIGURE 3-27. Choose Existing Disk

    c. Click **Choose existing disk** and then select the converted `*.vmdk` file.

    d. Under **Attributes**, keep all default settings.

    e. Under **Storage Tree**, select **Controller: IDE** and then click the optical drive icon. Verify that **CD/DVD Drive** is **IDE Secondary Master**.

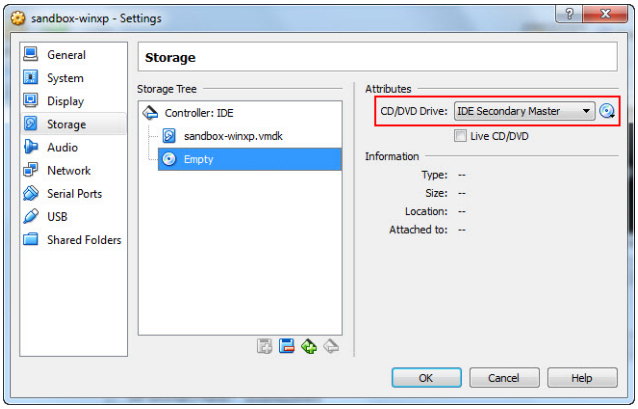


FIGURE 3-28. IDE SECONDARY MASTER

16. In the left pane, click **Audio** and then deselect **Enable Audio**.

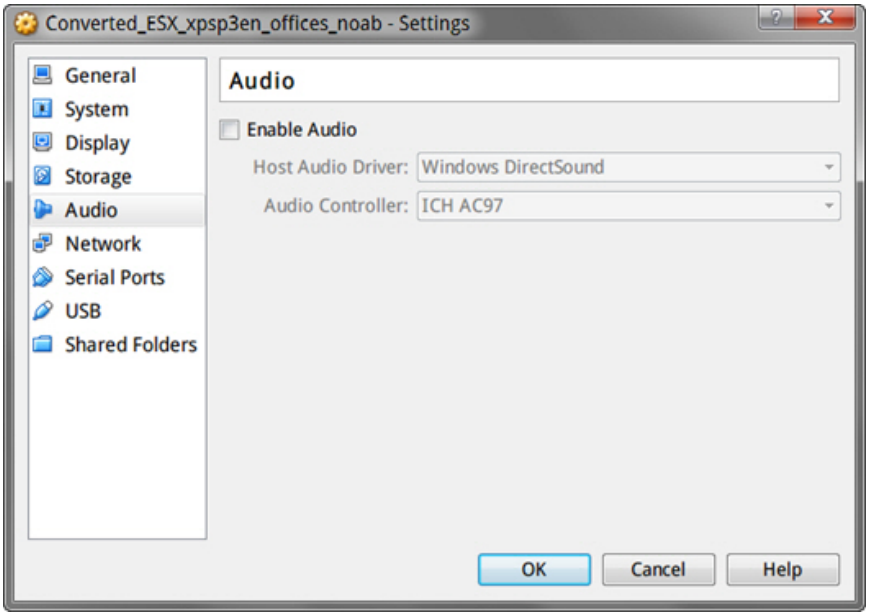


FIGURE 3-29. AUDIO OPTIONS SETTINGS

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

Important

Verify that **Enable USB 2.0 (EHCI) Controller** is not selected.

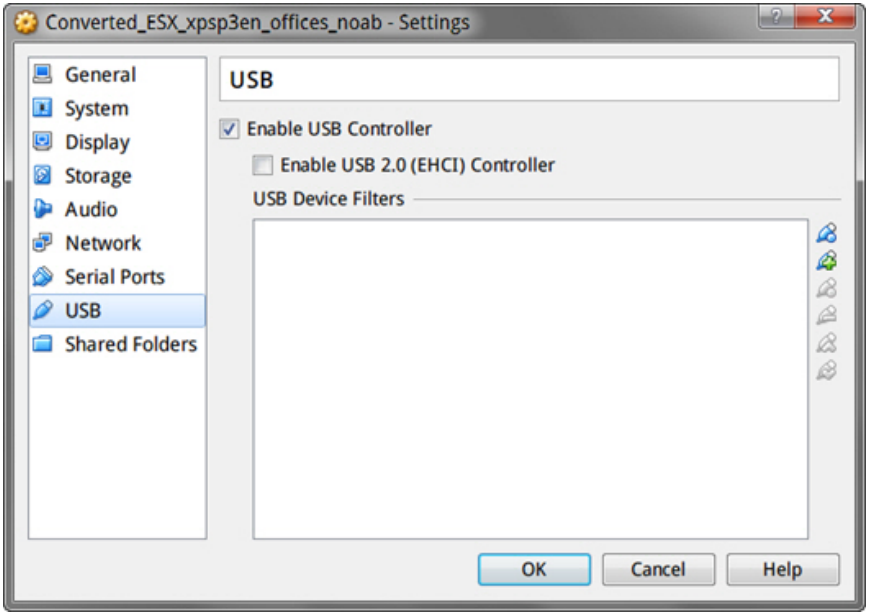


FIGURE 3-30. Enable USB Controller

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

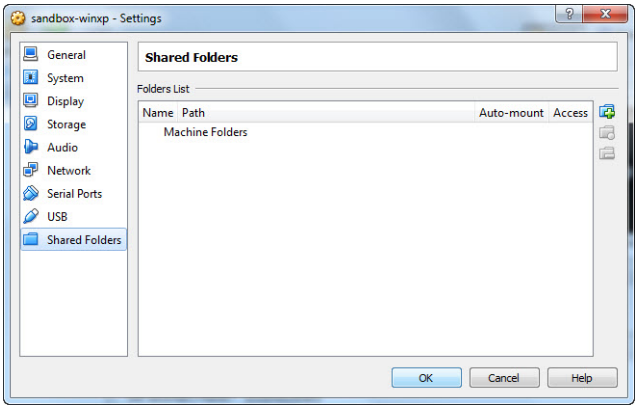


FIGURE 3-31. Shared Folders Settings

19. Click **OK**.

    The **Settings** window closes.

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

to power on the image.

    The installation process starts.

21. Follow the on-screen instructions to complete the installation.

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 3-42*
- *Configuring Virtual Machine Images (Windows 7/8/8.1 and Windows Server 2008/2008 R2) on page 3-44*

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.

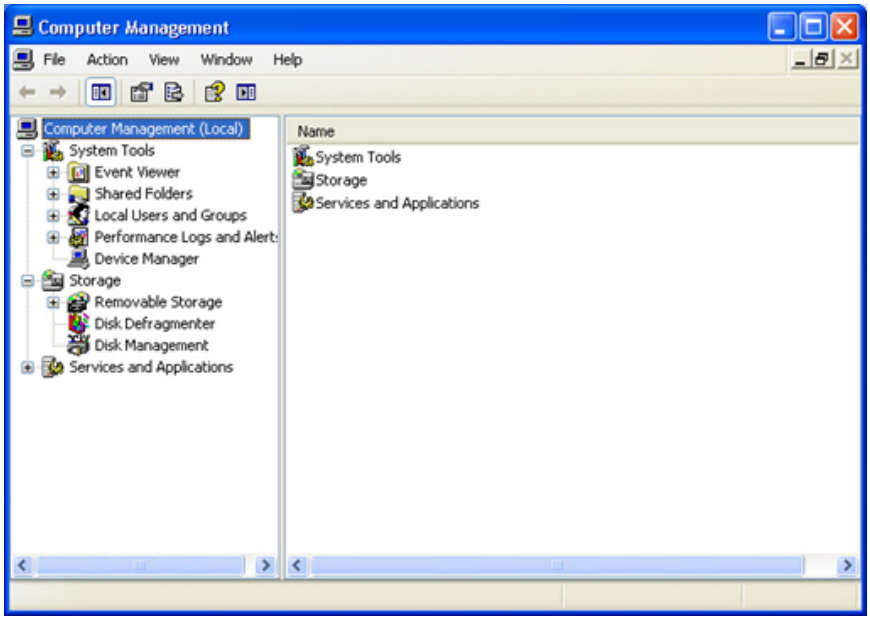


FIGURE 3-32. Computer Management

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

A list of devices appears.

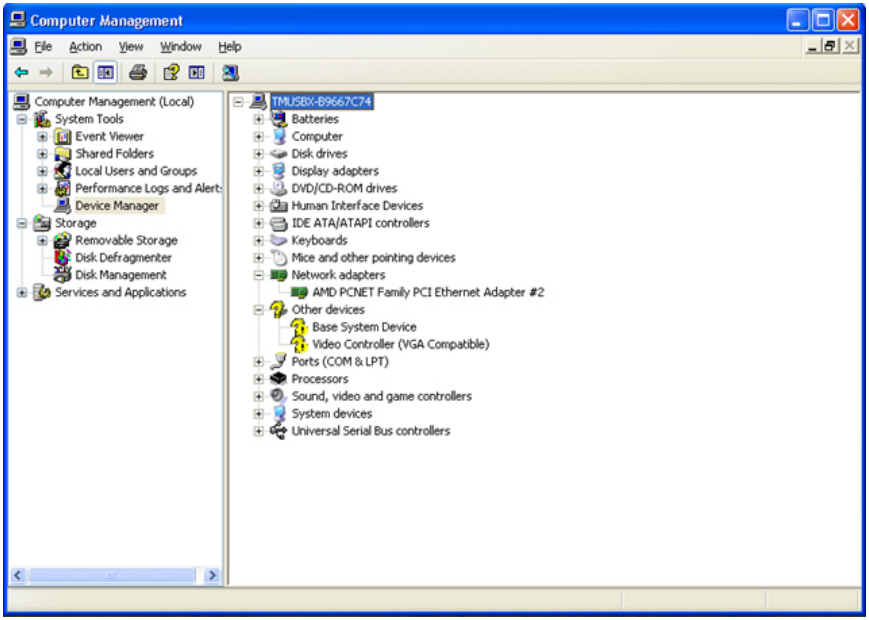


FIGURE 3-33. Device Management - Network Adapter Window

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 3-34. 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 and Windows Server 2008/2008 R2)

Procedure

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

The **Computer Management** screen appears.

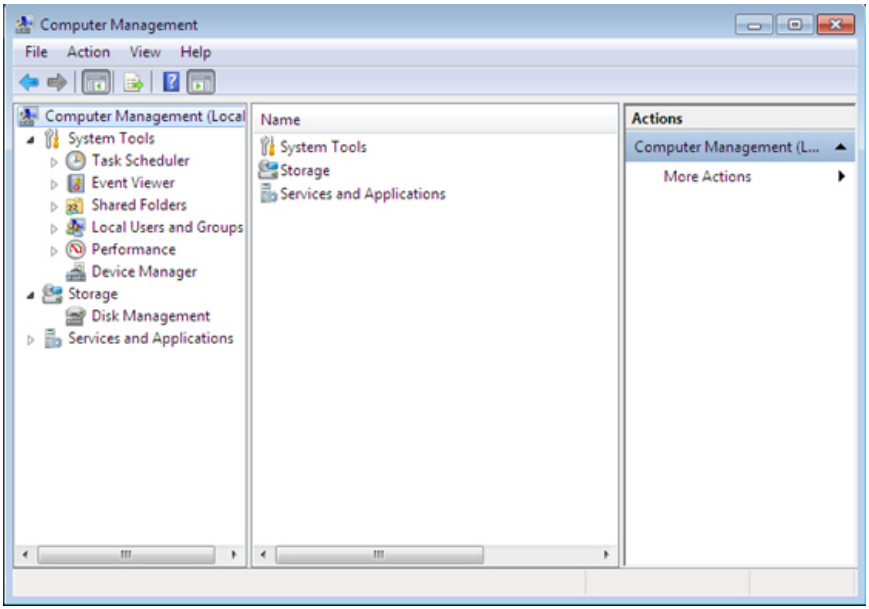


FIGURE 3-35. Computer Management

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

A list of devices appears.

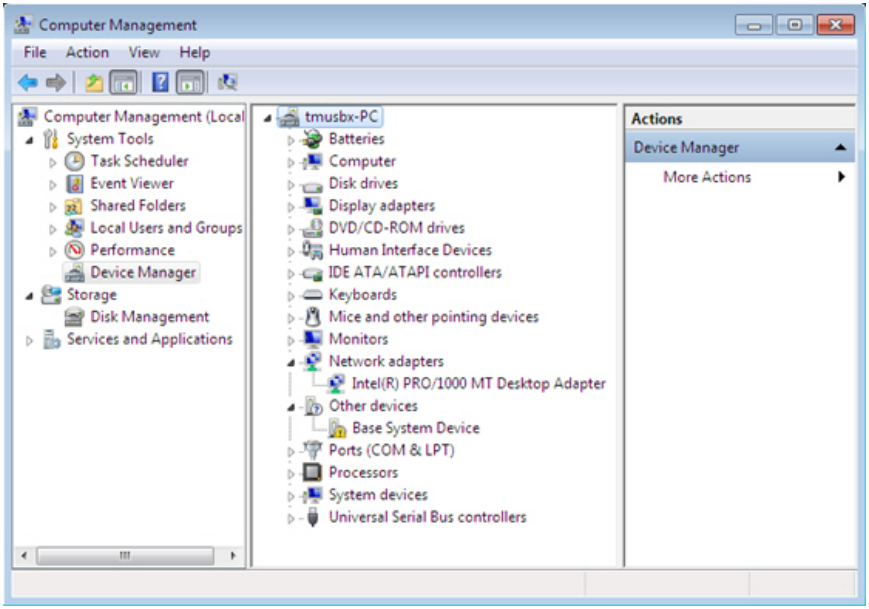


FIGURE 3-36. Device Management - Network Adapter

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.

TABLE 3-2. Maximum OVA File Size

PRODUCT	VERSION	MAXIMUM FILE SIZE
Deep Discovery Inspector	3.8 and earlier	10 GB
	3.8 Service Pack 1 and later	20 GB
Deep Discovery Analyzer	5.1 and earlier	10 GB
	5.5	20 GB
Deep Discovery Email Inspector	2.1 and earlier	10 GB
	2.5	20 GB
Trend Micro TippingPoint Advanced Threat Protection for Networks	3.8 Service Pack 2	20 GB
Trend Micro TippingPoint Advanced Threat Protection for Email	2.5	20 GB
Trend Micro TippingPoint Advanced Threat Protection Analyzer	5.5	20 GB

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.

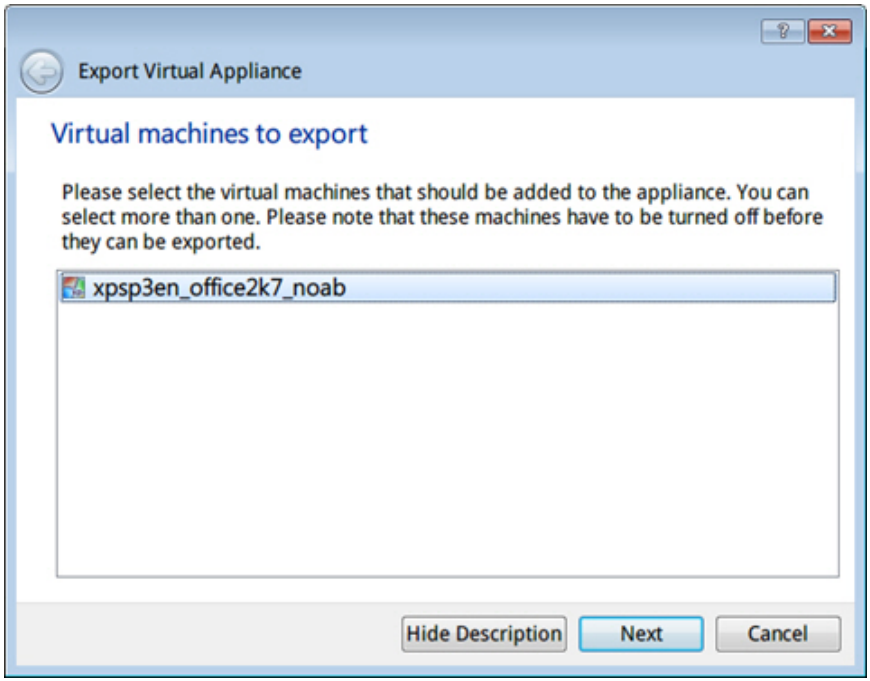


FIGURE 3-37. Export Virtual Appliance

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

The **Storage settings** screen appears.

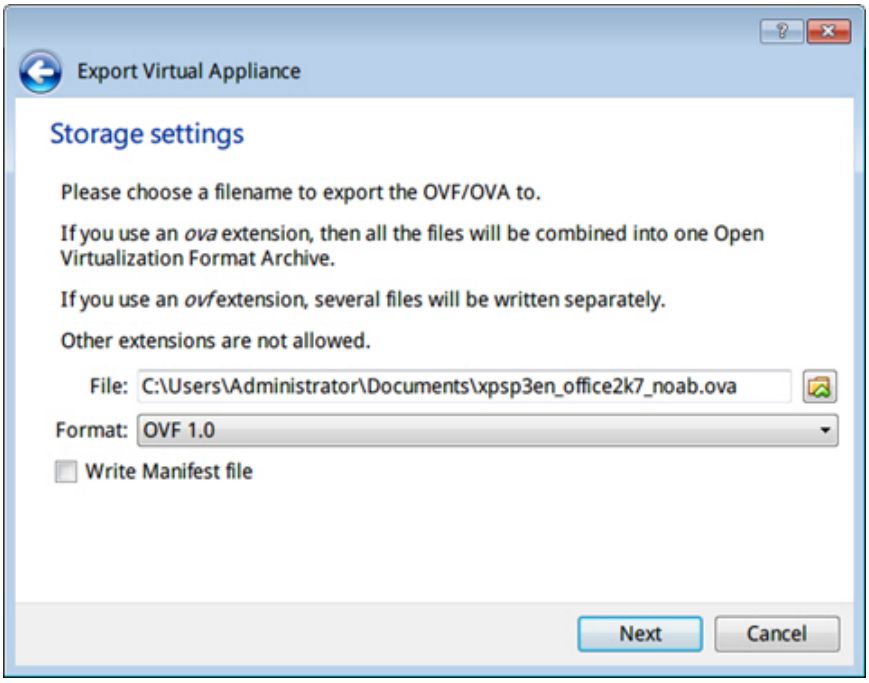


FIGURE 3-38. Storage Settings

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.

5. Click **Next**.

The **Appliance settings** screen appears.

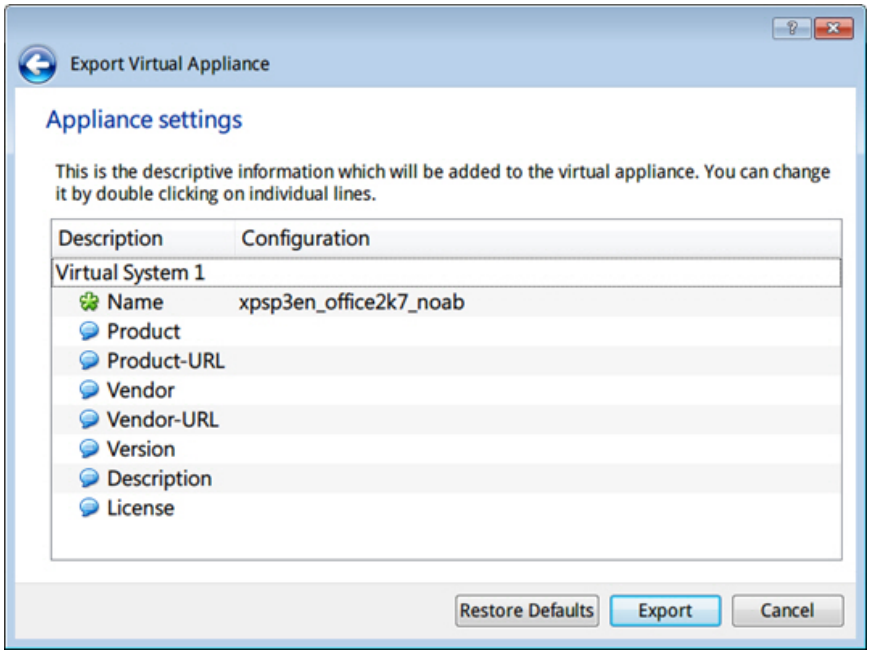


FIGURE 3-39. Export Virtual Appliance - Appliance Settings

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

VirtualBox creates the OVA file.

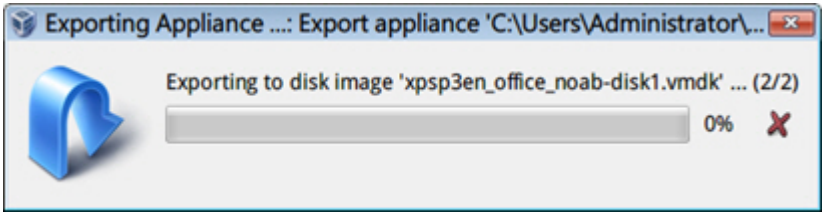


FIGURE 3-40. Disk Image Export Progress Bar

Chapter 4

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 4-1. Features

FEATURE	DESCRIPTION
Image creation	Create custom sandbox images for the following products: • Deep Discovery Inspector 3.8, 3.8 Service Pack 1, and 3.8 Service Pack 2 • Deep Discovery Email Inspector 2.1 and 2.5 • Deep Discovery Analyzer 5.1 and 5.5 • TippingPoint Advanced Threat Protection for Networks 3.8 SP2 • TippingPoint Advanced Threat Protection for Email 2.5 • TippingPoint Advanced Threat Protection Analyzer 5.5
Image validation and configuration	The tool validates and configures OVA files created using VirtualBox. **Note** For images created using VMware, see *OVA File Creation Using Converted Virtual Hard Disk Drives on page 3-1*.
Support for Windows 7 and Windows 8/8.1	Use the tool on computers running Windows 7 or Windows 8/8.1, and with Microsoft .NET Framework 4.0 or later.
Enhanced hardware identifier configuration	Enhanced configuration of universally unique identifiers (UUIDs) eliminates the need to reactivate Microsoft Windows and Microsoft Office.

System Requirements

TABLE 4-2. 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) Build 3.8.1240 and later: • Windows Server 2003/2003 R2 • Windows Server 2008/2008 R2 **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. For virtual machine images created in VMware, see *Creating OVA Files Using Converted Virtual Hard Disk Drives on page 3-2*.

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 or any 64-bit guest operating systems. **Note** The tool can detect hardware virtualization only on Windows 8/8.1 hosts.

Image Validation and Configuration

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

TABLE 4-3. Validating and configuring 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 8 and 8.1
Microsoft Office macros	Enabled

Important

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

Using the Tool

Procedure

1. Obtain a copy of `SandboxWizard.zip` 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.

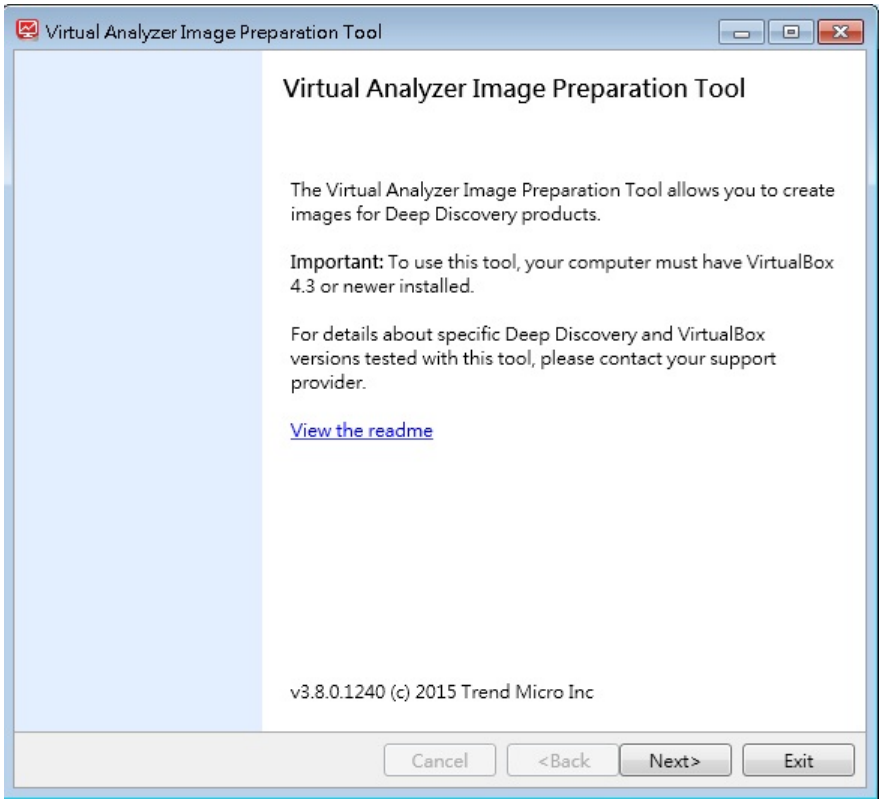


FIGURE 4-1. Introduction screen

3. Click **Next**.

   The tool checks if the computer meets the system requirements, and then the **System Requirements** screen appears.

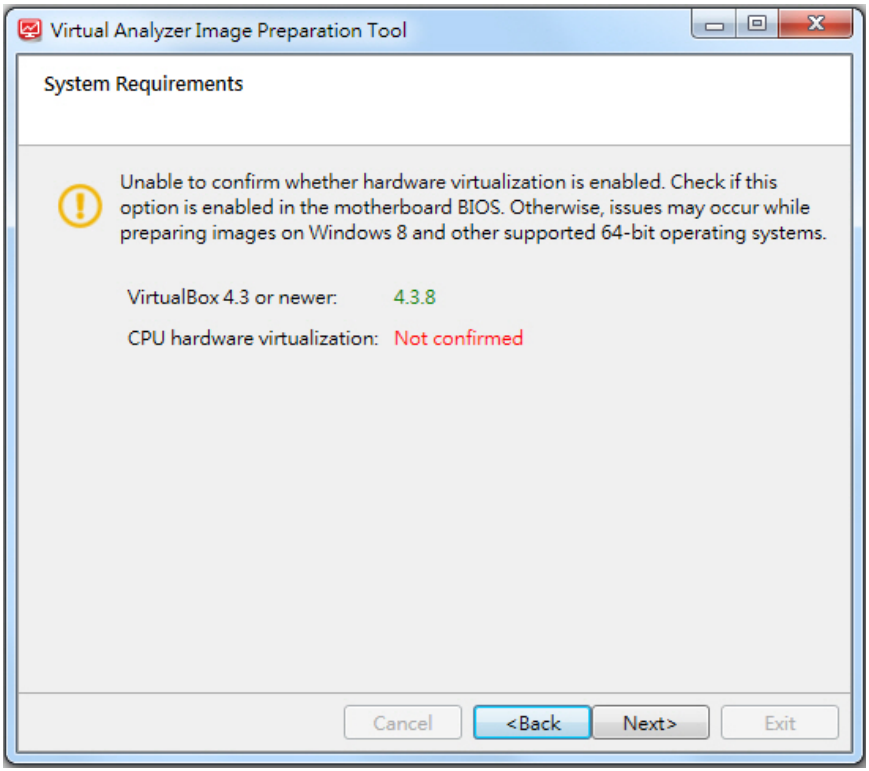


FIGURE 4-2. System Requirements screen

4. Click **Next**.

The **Specify Virtual Machine** screen appears.

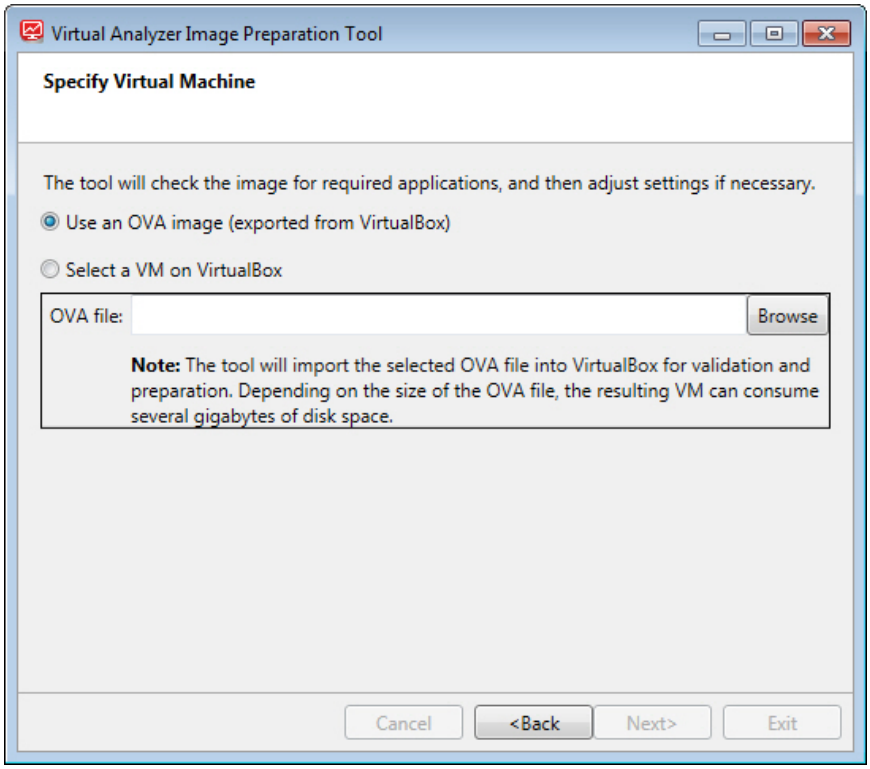


FIGURE 4-3. Specify Virtual Machine screen

5. 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 VMware image and then packaged it as an OVA file. For details, see *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.

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

For example:

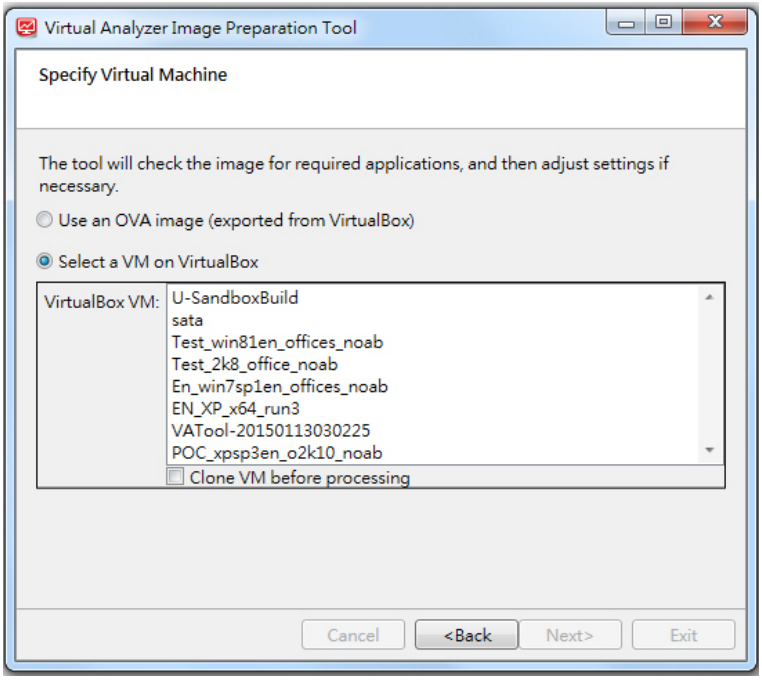


FIGURE 4-4. Specify Virtual Machine screen - select a VM on VirtualBox

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.

6. Click **Next**.

The **Sandbox Preparation** screen appears.

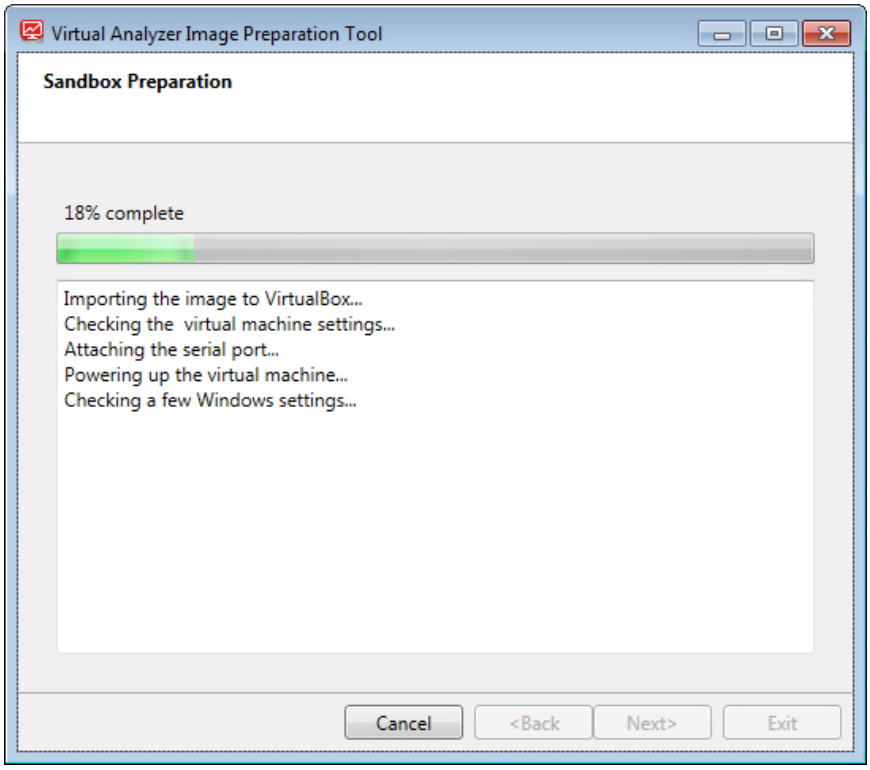


FIGURE 4-5. Sandbox Preparation screen

The tool modifies incorrectly configured settings. For a list of settings that the tool validates, see *Image Validation and Configuration on page 4-4*. For solutions to

issues that occur during this phase, see *Troubleshooting Common Issues on page 4-16*.

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

SCREEN	USER ACTION
Ready for Export: The screen appears when all settings are validated.	Click **Export to OVA** to generate a custom sandbox image in OVA format. **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-20160101091011_output.txt`
Preparation Unsuccessful: The screen appears when the tool is unable to fix issues encountered during preparation.	Click **Back to Home** or **Exit**. Check the logs and perform any recommended actions before running the tool again.

If no issues arise, the tool:

- Restarts the virtual machine.
- Performs the necessary system clean-up.
- Exports the OVA file.

- Displays the the **Sandbox Ready** screen.

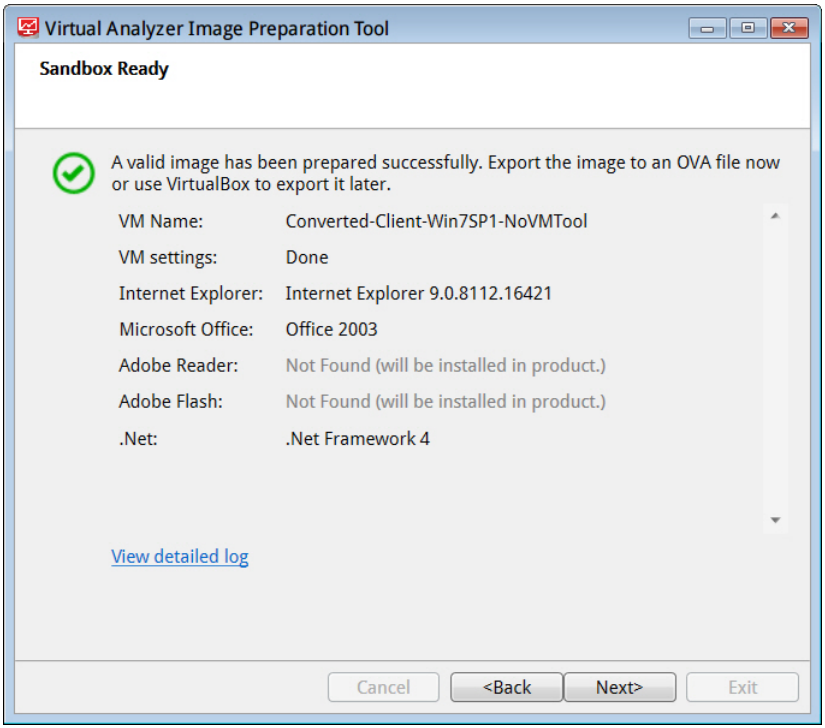


FIGURE 4-6. Sandbox Ready screen

If issues arise and are not resolved, see *Troubleshooting Common Issues on page 4-16*.

8. Click **Next**.

The **Specify the OVA image path and file name** screen appears.

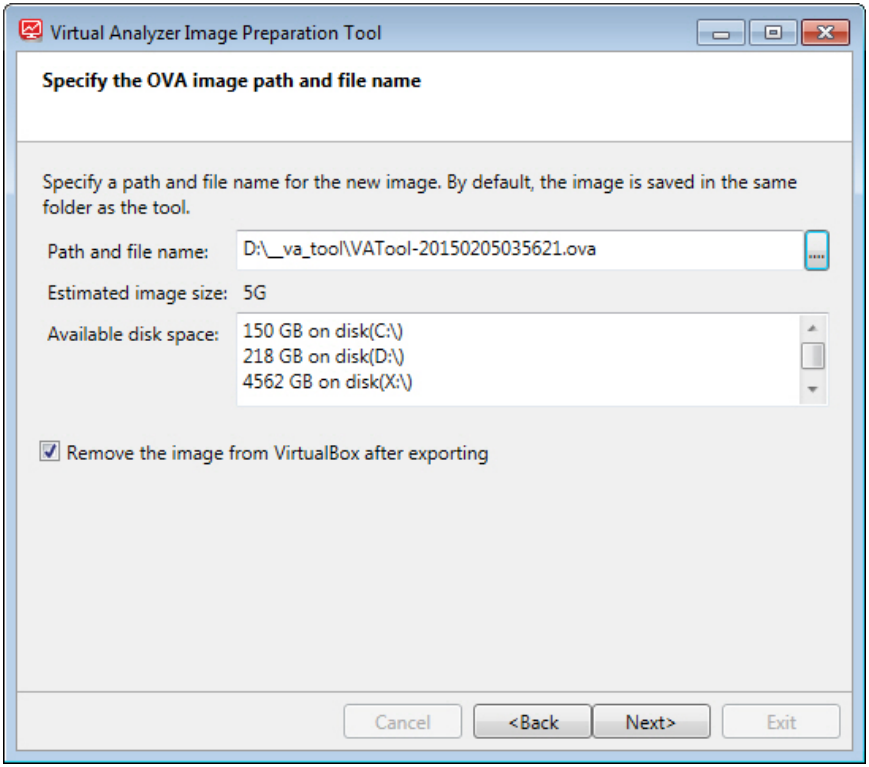


FIGURE 4-7. Specify OVA image path and file name screen

9. Configure the following settings:

   - Specify the location 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-20150205035621.ova`

   - Select **Remove the image from VirtualBox after exporting**.

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

Important

Unused images consume valuable disk space may impact performance.

10. Click **Next**.

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

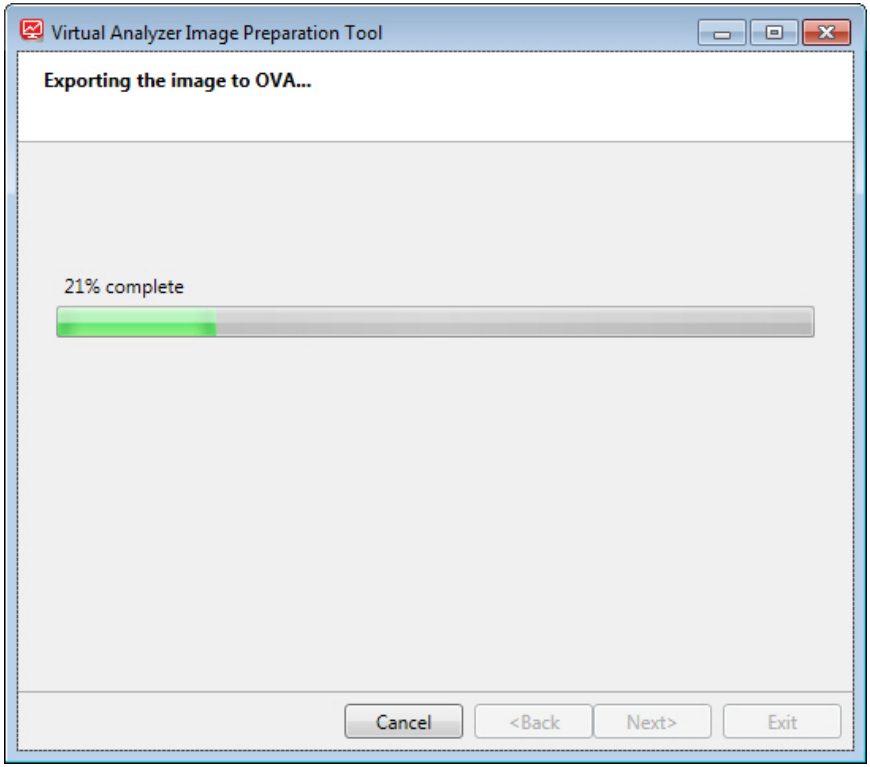


FIGURE 4-8. Export the image to OVA screen

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

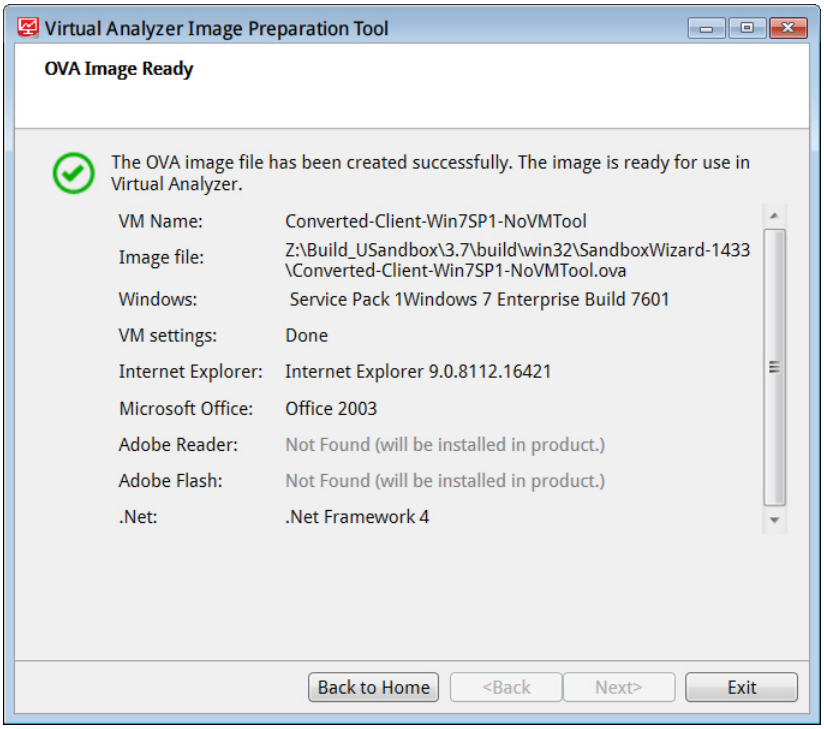


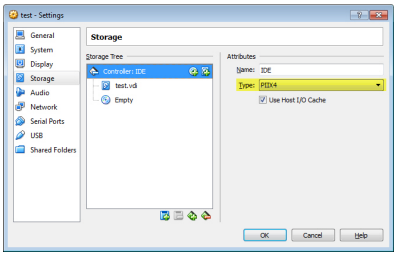
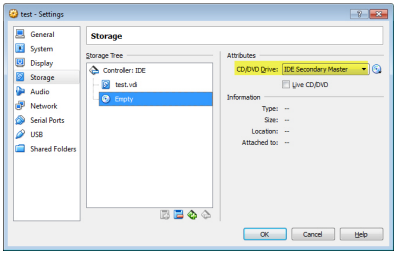
FIGURE 4-9. OVA Image Ready screen

11. Click **Exit** to close the window or click **Back to Home** to create another image.

Troubleshooting Common Issues

TABLE 4-4. Common Issues When Using the Tool

ISSUE	CAUSE	RECOMMENDED ACTION
Unable to upload an OVA file.	The image does not meet the minimum or maximum size requirements.	Verify that the OVA image is between 1 GB and 20 GB in size.
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 4-3*. For virtual machine images created in VMware, see *Creating OVA Files Using Converted Virtual Hard Disk Drives on page 3-2*.
	VirtualBox is not installed on the computer.	
	The image uses an unsupported operating system.	Use a supported operating system. For details, see *System Requirements on page 4-3*.
	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 4-10. Controller: IDE must be set to PIIX4** • Select the optical disc icon and verify that the specified **CD/DVD drive** is **IDE Secondary Master**.  **Figure 4-11. CD/DVD drive is set to IDE Secondary Master**

Sample Logs

Preparation successful. Missing app detected.

```
------------------------------------------------------------
Trend Micro(TM) Virtual Analyzer Image Preparation Tool 2.0
Detailed Log
------------------------------------------------------------

1. Overview
-------------------------------------------------------------------------------
Result: Preparation successful, missing apps to be installed in product
Completed: 2014-10-01 16:02:23
Original image: d:\userimage.ova
Virtual machine name: VATool-20140901133402 (in VirtualBox)

2. Hardware settings
-------------------------------------------------------------------------------
Processor count:                          1                       - OK
Memory size:                              512 MB                  - OK
PAE/NX:                                   Enabled                 - OK
VT-x / AMD-V and nested paging:           Enabled                 - OK
IDE settings:                IDE 0, port 1 emtpy, CD-ROM          - OK
Pointing device:                          USB tablet              - OK
Hard disk format:                         VMDK                    - OK
Chipset:                                  ICH9                    - OK
I/O APIC:                                 Enabled                 - OK
USB controller:                           Enabled                 - OK
Storage controller:                       IDE                     - OK

3. Accounts
-------------------------------------------------------------------------------
Admin password:                           1111                    - OK
Non-default accounts:                     None                    - OK
Automatic logon:                          Enabled                 - OK

4. Windows and applications
-------------------------------------------------------------------------------
Windows:                                  Windows 7               - OK
Microsoft Office:             Office 2012 (1111.12.12)            - OK
.NET Framework:                           Version 4.5.2           - OK
Internet Explorer:               Version 11.09600.17420           - OK
Java SE Runtime Environment:              Version 7               - OK
Adobe Reader:                           Not found                 - To be installed in product
Adobe Flash:                              Version 10.2.1          - OK
```

Preparation unsuccessful. Some items must be fixed manually.

```
------------------------------------------------------------
Trend Micro(TM) Virtual Analyzer Image Preparation Tool 2.0
Detailed Log
------------------------------------------------------------
```

```
1. Overview
--------------------------------------------------------------------------------
Result: Preparation unsuccessful. Some items need to be fixed manually.
Completed: 2014-12-01 18:12:33
Original image: d:\userimage.ova
Virtual machine name: VATool-20140901133402 (in VirtualBox)

2. Hardware settings
--------------------------------------------------------------------------------
Processor count:                        1                       - OK
Memory size:                            512 MB                  - OK
PAE/NX:                                 Enabled                 - OK
VT-x / AMD-V and nested paging:         Enabled                 - OK
IDE settings:               IDE 0, port 1 emtpy, CD-ROM         - OK
Pointing device:                        USB tablet              - OK
Hard disk format:                       VMDK                    - OK
Chipset:                                ICH9                    - OK
I/O APIC:                               Enabled                 - OK
USB controller:                         Enabled                 - OK
Storage controller:                     IDE                     - OK

3. Accounts
--------------------------------------------------------------------------------
Admin password:                         1111                    - OK
Non-default accounts:                   None                    - OK
Automatic logon:                        Enabled                 - OK

4. Windows and applications
--------------------------------------------------------------------------------
Windows:                                Windows 98              - Requires manual fix
Microsoft Office:                       (not checked)
.NET Framework:                         (not checked)
Internet Explorer:                      (not checked)
Java SE Runtime Environment:            (not checked)
Adobe Reader:                           (not checked)
Adobe Flash:                            (not checked)
```

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: APEM06860/150128