# Using VMware Workstation

VMware Workstation 10

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001200-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

**VMware, Inc.**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

# Contents

Using VMware Workstation 5

**1** Creating Virtual Machines 7
- Understanding Virtual Machines 7
- Preparing to Create a New Virtual Machine 8
- Create a New Virtual Machine on the Local Host 18
- Cloning Virtual Machines 22
- Virtualize a Physical Machine 25
- Importing Virtual Machines 27
- Installing and Upgrading VMware Tools 29
- Virtual Machine Files 40

**2** Using Virtual Machines 43
- Starting Virtual Machines 43
- Stopping Virtual Machines 47
- Transferring Files and Text 51
- Add a Host Printer to a Virtual Machine 60
- Using Removable Devices in Virtual Machines 61
- Changing the Virtual Machine Display 68
- Using Folders to Manage Virtual Machines 74
- Taking Snapshots of Virtual Machines 77
- Install New Software in a Virtual Machine 84
- Share Tablet Sensor Data with Windows 8 Guests 84
- Take a Screenshot of a Virtual Machine 85
- Delete a Virtual Machine 85

**3** Configuring and Managing Virtual Machines 87
- Configure Power Options and Power Control Settings 87
- Set Workstation Display Preferences 89
- Configure Display Settings for a Virtual Machine 90
- Set Preferences for Unity Mode 92
- Setting Screen Color Depth 92
- Using Advanced Linux Sound Architecture 93
- Encrypting and Restricting Virtual Machines 94
- Moving Virtual Machines 98
- Configure a Virtual Machine as a VNC Server 103
- Change the Hardware Compatibility of a Virtual Machine 106
- Clean Up a Virtual Hard Disk on Windows Hosts 107
- Export a Virtual Machine to OVF Format 108
- Writing and Debugging Applications That Run In Virtual Machines 109

**4** Configuring and Managing Devices 111
Configuring DVD, CD-ROM, and Floppy Drives 111
Configuring a USB Controller 113
Configuring and Maintaining Virtual Hard Disks 116
Adding a Physical Disk to a Virtual Machine 122
Configuring Virtual Ports 125
Configuring Generic SCSI Devices 129
Configuring Eight-Way Virtual Symmetric Multiprocessing 133
Configuring Keyboard Features 134
Modify Hardware Settings for a Virtual Machine 143

**5** Configuring Network Connections 145
Understanding Virtual Networking Components 145
Understanding Common Networking Configurations 146
Changing the Default Networking Configuration 147
Configuring Bridged Networking 151
Configuring Network Address Translation 154
Configuring Host-Only Networking 163
Assigning IP Addresses in Host-Only Networks and NAT Configurations 169
Configuring LAN Segments 172
Configuring Samba for Workstation 174
Using Virtual Network Adapters in Promiscuous Mode on Linux Hosts 175
Maintaining and Changing MAC Addresses for Virtual Machines 175
Sample Custom Networking Configuration 176

**6** Using Remote Connections and Sharing Virtual Machines 179
Understanding VMware Workstation Server 179
Connect to a Remote Server 182
Disconnect from a Remote Server 184
Creating and Managing Shared Virtual Machines 184
Upload a Virtual Machine to a Remote Server 188
Download a Virtual Machine from a Remote Server 188
Create a Virtual Machine on a Remote Host 189
Configure Shared and Remote Virtual Machines to Start with the Host 190
Using Roles to Assign Privileges 191
Using Permissions to Restrict Users 195

**7** Using the vmware Command 199
Run the vmware Command 199
Incorporate Workstation Startup Options in a Windows Shortcut 200

Index 201

# Using VMware Workstation

*Using VMware Workstation* describes how to use VMware® Workstation and create, configure, and manage virtual machines.

## Intended Audience

This information is intended for anyone who wants to use Workstation and create and manage virtual machines.

## Where to Find Additional Information

See the following documents for more information about using Workstation. All of the documents are available from the VMware Web site.

- *Getting Started with VMware Workstation* describes how to install and upgrade Workstation, create a typical virtual machine, and perform common virtual machine operations.
- *Installing and Configuring VMware Tools* contains complete information on using VMware Tools.
- The *VMware Guest Operating System Installation Guide* contains information about installing specific guest operating systems.
- The online VMware Compatibility Guide lists the supported host and guest operating systems for Workstation.

The Workstation online help provides quick reference information about Workstation settings and common tasks. It is available from the Workstation **Help** menu and when you click **Help** on a Workstation dialog box.

# 1 Creating Virtual Machines

You can create a new virtual machine in Workstation by using the New Virtual Machine wizard, clone an existing Workstation virtual machine or virtual machine template, import third-party and Open Virtualization Format (OVF) virtual machines, and create a virtual machine from a physical machine.

You can also create shared virtual machines, which can be used by remote users, and virtual machines that run on remote hosts. See Chapter 6, "Using Remote Connections and Sharing Virtual Machines," on page 179.

This chapter includes the following topics:


- "Understanding Virtual Machines," on page 7
- "Preparing to Create a New Virtual Machine," on page 8
- "Create a New Virtual Machine on the Local Host," on page 18
- "Cloning Virtual Machines," on page 22
- "Virtualize a Physical Machine," on page 25
- "Importing Virtual Machines," on page 27
- "Installing and Upgrading VMware Tools," on page 29
- "Virtual Machine Files," on page 40


## Understanding Virtual Machines

A virtual machine is a software computer that, like a physical machine, runs an operating system and applications. A virtual machine uses the physical resources of the physical machine on which it runs, which is called the host system. Virtual machines have virtual devices that provide the same functionality as physical hardware, but with the additional benefits of portability, manageability, and security.

A virtual machine has an operating system and virtual resources that you manage in much the same way that you manage a physical computer. For example, you install an operating system in a virtual machine in the same way that you install an operating system on a physical computer. You must have a CD-ROM, DVD, or ISO image that contains the installation files from an operating system vendor.

# Preparing to Create a New Virtual Machine

You use the New Virtual Machine wizard to create a new virtual machine in Workstation. The wizard prompts you to make decisions about many aspects of the virtual machine. You should make these decisions before you start the New Virtual Machine wizard.

## Selecting a Virtual Machine Configuration

When you start the New Virtual Machine wizard, the wizard prompts you to select a typical or custom configuration.

### Typical Configuration

If you select a typical configuration, you must specify or accept defaults for a few basic virtual machine settings.

- How you want to install the guest operating system.
- A name for the virtual machine and a location for the virtual machine files.
- The size of the virtual disk and whether to split the disk into multiple virtual disk files.
- Whether to customize specific hardware settings, including memory allocation, number of virtual processors, and network connection type.

### Custom Configuration

You must select a custom configuration if you need to perform any of the following hardware customizations.

- Create a virtual machine that has a different Workstation version than the default hardware compatibility setting.
- Select the I/O controller type for the SCSI controller.
- Select the virtual disk device type.
- Configure a physical disk or an existing virtual disk instead of create a new virtual disk.
- Allocate all virtual disk space rather than let disk space gradually grow to the maximum disk size.

## Selecting the Virtual Machine Hardware Compatibility Setting

All virtual machines have a hardware version. The hardware version indicates which virtual hardware features that the virtual machine supports, such as BIOS or EFI, number of virtual slots, maximum number of CPUs, maximum memory configuration, and other hardware characteristics. The virtual machine hardware compatibility setting determines the hardware features of the virtual machine.

If you select a typical configuration, the wizard uses the default hardware compatibility setting configured in the Workstation preferences. By default, the default hardware compatibility setting is the installed Workstation version.

If you select a custom configuration, the New Virtual Machine wizard prompts you to select a hardware compatibility setting for the virtual machine. When you select a hardware compatibility setting, a list of the VMware products and versions that are compatible with your selection appears. Limitations and features that are not available for your selection are also listed. If a feature compatibility check box is available for your selection, you can select that check box to see a list of the additional limitations.

To deploy virtual machines to run on a different VMware product, you might need to select a hardware compatibility setting that is compatible with that product.

## Selecting a Guest Operating System

The New Virtual Machine prompts you to select the source media for the operating system that will run inside the virtual machine. You can specify an installer disc inserted in a physical drive, an ISO image file, or you can instruct the New Virtual Machine wizard to create a virtual machine that has a blank hard disk.

If you select an installer disc or an ISO image file and the operating system supports Easy Install, the guest operating system installation is automated and VMware Tools is installed. If the installer disc or ISO image file contains a product key number and is already set up to perform an unattended installation, the only benefit of using Easy Install is the automatic installation of VMware Tools.

**NOTE** For remote virtual machines, you must specify whether the physical drive or ISO image file is located on the local host or remote host before you select the installer disc or ISO image file.

If you instruct the New Virtual Machine wizard to create a virtual machine that has a blank hard disk, the wizard prompts you to specify an operating system and version and you must install the guest operating system manually after the virtual machine is created. Workstation uses this information to set the appropriate default values, name files associated with the virtual machine, adjust performance settings, and work around special behaviors and bugs in the guest operating system. If the operating system you plan to install is not listed in the wizard, select **Other** for both the operating system and version.

If you are installing an operating system that supports Easy Install but you do not want to use Easy Install, you can instruct the wizard to create a virtual machine that has a blank disk and install the guest operating system manually.

### Providing Easy Install Information

When the New Virtual Wizard detects an operating system that supports Easy Install, the wizard prompts you for information about the guest operating system. After the virtual machine is created, the guest operating system installation is automated and VMware Tools is installed.

For Windows guest operating systems, you must provide the following Easy Install information.

**Table 1-1.** Easy Install Information for Windows Guests

| Easy Install Prompt | Description |
|---|---|
| **Windows product key** | (Optional) Type a product key unless the installation media contains a volume license product key. If you provide a product key here, you are not prompted to provide a product key when you install the guest operating system. |
| **Version of Windows to install** | For Windows Vista, Windows 7, and Windows Server 2008 guest operating systems, select the operating system edition. |
| **Full name** | The name to use to register the guest operating system. Do not use the name Administrator or Guest. If you use one of these names, you must enter a different name when you install the guest operating system. |
| **Password** | (Optional) The password to use for an account with Administrator permissions on Windows operating systems other than Windows 2000. On Windows 2000, this is the password for the Administrator account. On Windows XP Home, an Administrator account without a password is created and you are automatically logged in to the guest operating system. |
| **Log on automatically (requires a password)** | (Optional) Save your login credentials and bypass the login dialog box when you power on the virtual machine. You must enter a name and password to use this feature. |

For Linux guest operating systems, you must provide the following Easy Install information.

**Table 1-2.** Easy Install Information for Linux Guests

| Prompt | Description |
|---|---|
| **Full name** | The name to use to register the guest operating system, if registration is required. Workstation uses the first name to create the host name for the virtual machine. |
| **User name** | Your user name. You can use lowercase letters, numbers, and dashes, but avoid using user names that begin with a dash. Do not use the name root. Some operating systems set up sudo access for this user and other operating systems require this user to use `su` to obtain root privileges. |
| **Password** | The password for the **User name** and the root user. |

## Specifying the Virtual Machine Name and File Location

The New Virtual Machine wizard prompts you for a virtual machine name and a directory for the virtual machine files.

The name of the default directory for virtual machine files is derived from the name of the guest operating system, for example, `Microsoft Windows 7 (32-bit)`.

For standard virtual machines, the default directory for virtual machine files is located in the virtual machine directory. For best performance, do not place the virtual machines directory on a network drive. If other users need to access the virtual machine, consider placing the virtual machine files in a location that is accessible to those users.

For shared virtual machines, the default directory for virtual machine files is located in the shared virtual machines directory. Shared virtual machine files must reside in the shared virtual machines directory.

### Virtual Machines Directory

Workstation stores standard virtual machines in the virtual machines directory.

The default location of the virtual machines directory depends on the host operating system.

**Table 1-3.** Default Virtual Machines Directory

| Host Operating System | Default Location |
|---|---|
| Windows XP<br>Windows Server 2003<br>Windows Server 2008 | `C:\Documents and Settings\`*username*`\My Documents\My Virtual Machines`<br>*username* is the name of the currently logged in user. |
| Windows Vista<br>Windows 7<br>Windows 8 | `C:\Users\` *username* `\Documents\Virtual Machines`<br>*username* is the name of the currently logged in user. |
| Linux | *homedir*`/vmware`<br>*homedir* is the home directory of the currently logged in user. |

### Shared Virtual Machines Directory

Workstation stores shared virtual machines in the shared virtual machines directory, where VMware Workstation Server manages them.

The default location of the shared virtual machines directory depends on the host operating system.

**Table 1-4.** Default Shared Virtual Machines Directory

| Host Operating System | Default Shared Virtual Machines Directory |
|---|---|
| Windows XP<br>Windows Server 2003<br>Windows Server 2008 | `C:\Documents and Settings\All Users\Documents\Shared Virtual Machines` |
| Windows Vista<br>Windows 7<br>Windows 8 | `C:\Users\Public\Documents\Shared Virtual Machines` |
| Linux | `/var/lib/vmware/Shared VMs` |

## Select the Number of Processors for a Virtual Machine

When you select a custom configuration, the New Virtual Machine wizard prompts you to specify the number of processors for the virtual machine.

Specifying multiple virtual processors is supported only on host machines that have at least two logical processors. Single-processor hosts that have hyperthreading enabled or dual-core CPUs are considered to have two logical processors. Multiprocessor hosts that have two CPUs are considered to have at least two logical processors, regardless of whether they are dual-core or have hyperthreading enabled.

For Windows virtual machines running mostly office and Internet productivity applications, using multiple virtual processors is not beneficial, so the default single virtual processor is ideal. For server workloads and data-intensive computing applications, adding extra virtual processors may provide an increase in application performance.

| Application | Recommended number of processors |
|---|---|
| Desktop applications | 1 processor |
| Server operating systems | 2 processors |
| Video encoding, modeling, and scientific | 4 processors |

In some circumstances, adding additional processors can decrease the overall perfomance of the virtual machine and your computer. This can occur if the operating system or application is not using the processors efficiently. In this case, reducing the number of processors is recommended.

Assigning all processors on your computer to the virtual machine results in extremely poor performance. The host operating system must continue to perform background tasks even if no applications are running. If you assign all processors to a virtual machine, this prevents important tasks from being completed.

## Allocating Memory for a Virtual Machine

When you select a custom configuration, the New Virtual Machine wizard prompts you to specify the default settings for memory allocation.

Color-coded icons correspond to the maximum recommended memory, recommended memory, and guest operating system recommended minimum memory values. To adjust the memory allocated to the virtual machine, move the slider along the range of values. The high end of the range is determined by the amount of memory allocated to all running virtual machines. If you allow virtual machine memory to be swapped, this value changes to reflect the specified amount of swapping.

On 64-bit hosts, the maximum amount of memory for each virtual machine is 64GB. On 32-bit hosts, the maximum amount of memory for each virtual machine is 8GB. You cannot power on virtual machines that are configured to use more than 8GB of memory on 32-bit hosts. Memory management limitations on 32-bit operating systems cause virtual machine memory to overcommit, which severely affects system performance.

The total amount of memory that you can assign to all virtual machines running on a single host machine is limited only by the amount of RAM on the host machine.

You can change the amount of memory available to all virtual machines by modifying Workstation memory settings.

## Selecting the Network Connection Type for a Virtual Machine

When you select a custom configuration, the New Virtual Machine wizard prompts you to configure the network connection type for the virtual machine.

If you are creating a remote virtual machine, you must select either a custom network or no network connection.

**Table 1-5.** Network Connection Settings

| Setting | Description |
|---|---|
| **Use bridged networking** | Configure a bridged network connection for the virtual machine. With bridged networking, the virtual machine has direct access to an external Ethernet network. The virtual machine must have its own IP address on the external network.<br>If your host system is on a network and you have a separate IP address for your virtual machine (or can get an IP address from a DHCP server), select this setting. Other computers on the network can then communicate directly with the virtual machine. |
| **Use network address translation (NAT)** | Configure a NAT connection for the virtual machine. With NAT, the virtual machine and the host system share a single network identity that is not visible outside the network.<br>Select NAT if you do not have a separate IP address for the virtual machine, but you want to be able to connect to the Internet. |
| **Use host-only networking** | Configure a host-only network connection for the virtual machine. Host-only networking provides a network connection between the virtual machine and the host system, using a virtual network adapter that is visible to the host operating system.<br>With host-only networking, the virtual machine can communicate only with the host system and other virtual machines in the host-only network. Select host-only networking to set up an isolated virtual network. |
| **Do not use a network connection** | Do not configure a network connection for the virtual machine. |
| **Custom** (Windows host) or **Named Network** (Linux host) | (Remote virtual machine only) Select a specific virtual network. |

See Chapter 5, "Configuring Network Connections," on page 145 for information about virtual switches, virtual network adapters, the virtual DHCP server, and the NAT device.

## Selecting the I/O Controller Type for a Virtual Machine

When you select a custom configuration, the New Virtual Machine wizard prompts you to select the I/O controller type for the virtual machine.

Workstation installs an IDE controller and a SCSI controller in the virtual machine. SATA controllers are supported for some guest operating systems. The IDE controller is always ATAPI. For the SCSI controller, you can choose BusLogic, LSI Logic, or LSI Logic SAS. If you are creating a remote virtual machine on an ESX host, you can also select a VMware Paravirtual SCSI (PVSCSI) adapter.

BusLogic and LSI Logic adapters have parallel interfaces. The LSI Logic SAS adapter has a serial interface. The LSI Logic adapter has improved performance and works better with generic SCSI devices. The LSI Logic adapter is also supported by ESX Server 2.0 and later.

PVSCSI adapters are high-performance storage adapters that can provide greater throughput and lower CPU utilization. They are best suited for environments where hardware or applications drive a very high amount of I/O throughput, such as SAN environments. PVSCSI adapters are not suited for DAS environments.

**NOTE** The choice of SCSI controller does not affect whether the virtual disk can be an IDE, SCSI, or SATA disk.

Some guest operating systems, such as Windows XP, do not include a driver for the LSI Logic or LSI Logic SAS adapter. You must download the driver from the LSI Logic Web site. Drivers for a Mylex (BusLogic) compatible host bus adapter are not obvious on the LSI Logic Web site. Search the support area for the numeric string in the model number, for example, search for 958 for BT/KT-958 drivers.

See the *VMware Guest Operating System Installation Guide* for driver support information. For guest operating system support information and known issues, as well as SATA support, see the online Compatibility Guide on the VMware Web site.

## Selecting a Hard Disk for a Virtual Machine

When you select a custom configuration, the New Virtual Machine wizard prompts you to configure a hard disk for the virtual machine.

Virtual hard disks are the best choice for most virtual machines because they are easy to set up and can be moved to new locations on the same host system or to different host systems. In a typical configuration, Workstation creates a new virtual hard disk for the virtual machine.

In some cases, you might want to select an existing virtual hard disk or give the virtual machine access to a physical hard disk or unused partition on the host system.

- Selecting the Virtual Hard Disk Type for a Virtual Machine on page 14

  If you instruct the New Virtual Machine wizard to create a new virtual disk during a custom configuration, the wizard prompts you to select the virtual hard disk type for the virtual machine.

- Selecting the Disk Mode on page 14

  When you select a custom configuration on a Linux host, you can use the New Virtual Machine wizard to configure normal or independent mode for a disk.

- Prepare to Use a Physical Disk or Unused Partition on page 14

  You must perform certain tasks before you configure a virtual machine to use a physical disk or unused partition on the host system.

- Specifying Disk Capacity for a Virtual Machine on page 15

  If you instruct the New Virtual Machine wizard to create a new virtual disk during a custom configuration, the wizard prompts you to set the size of the virtual disk and specify whether to split the disk into multiple virtual disk (`.vmdk`) files.

- Specifying the Name and Location of Virtual Disk Files on page 17

  During a custom configuration, if you instruct the New Virtual Machine wizard to create a new virtual disk, use an existing virtual disk, or use a physical disk, the wizard prompts you for the name and location of a virtual disk (`.vmdk`) file.

## Selecting the Virtual Hard Disk Type for a Virtual Machine

If you instruct the New Virtual Machine wizard to create a new virtual disk during a custom configuration, the wizard prompts you to select the virtual hard disk type for the virtual machine.

You can set up a virtual disk as an IDE disk for any guest operating system. You can set up a virtual disk as a SCSI disk for any guest operating system that has a driver for the LSI Logic or BusLogic SCSI controller available in the virtual machine. You can set up a virtual disk as SATA for some guest operating systems.

You can change virtual disk node and mode settings after a virtual machine is created.

## Selecting the Disk Mode

When you select a custom configuration on a Linux host, you can use the New Virtual Machine wizard to configure normal or independent mode for a disk.

In normal mode, disks are included in snapshots that you take of the virtual machine. If you do not want data on the disk to be recorded when you take a snapshot of the virtual machine, configure the disk to be independent.

If you configure a disk to be independent, you can further specify whether changes you make to the disk are to persist or be discarded when you power off the virtual machine or restore a snapshot.

You can also exclude virtual disks from snapshots by modifying virtual machine settings.

## Prepare to Use a Physical Disk or Unused Partition

You must perform certain tasks before you configure a virtual machine to use a physical disk or unused partition on the host system.

You must perform these tasks before you run the New Virtual Machine wizard to add a physical disk to a new virtual machine, and before you add a physical disk to an existing virtual machine.

### Procedure

1 If a partition is mounted by the host or in use by another virtual machine, unmount it.

The virtual machine and guest operating system access a physical disk partition while the host continues to run its operating system. Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted on the host operating system.

| Option | Description |
|---|---|
| **The partition is mapped to a Windows Server 2003, Windows Server 2008, or Windows XP host** | a Select **Start > Settings > Control Panel > Administrative Tools > Computer Management > Storage > Disk Management**.<br>b Select a partition and select **Action > All Tasks > Change Drive Letter and Paths**.<br>c Click **Remove**. |
| **The partition is mapped to a Windows 7 or Windows 8 host** | a Select **Start > Control Panel**.<br>b In the menu bar, click the arrow next to **Control Panel**.<br>c From the drop-down menu, select **All Control Panel Items > Administrative Tools > Computer Management > Storage > Disk Management (Local)**.<br>d Right-click a partition and choose **Change Drive Letter and Paths**.<br>e Click **Remove** and **OK**. |
| **The partition is mapped to a Windows Vista host** | a Select **Start > Control Panel (Classic View) > Administrative Tools > Computer Management > Storage > Disk Management**.<br>b Right-click a partition and choose **Change Drive Letter and Paths**.<br>c Click **Remove** and **OK**. |

2 Check the guest operating system documentation regarding the type of partition on which the guest operating system can be installed.

   On Windows Vista and Windows 7 hosts, you cannot use the system partition, or the physical disk that contains it, in a virtual machine. DOS, Windows 95, and Windows 98 operating systems must be installed on the first primary partition. Other operating systems, such as Linux, can be installed on a primary or an extended partition on any part of the drive.

3 If the physical partition or disk contains data that you need in the future, back up the data.

4 If you use a Windows host IDE disk in a physical disk configuration, verify that it is not configured as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.

5 On a Windows XP or Windows Server 2003 host, if the host is using a dynamic disk, use the disk management tool to change the dynamic disk to a basic disk.

   You cannot use a dynamic disk as a physical disk in a virtual machine.

   a On the host, select **Start > Settings > Control Panel > Administrative Tools > Computer Management > Disk Management**.

   b Delete all logical volumes on the disk.

      This action destroys all data on the disk.

   c Right-click the disk icon and select **Revert to Basic Disk**.

   d Partition the disk.

6 On a Linux host, set the device group membership or device ownership appropriately.

   a Verify that the master physical disk device or devices are readable and writable by the user who runs Workstation.

      Physical devices, such as `/dev/hda` (IDE physical disk) and `/dev/sdb` (SCSI physical disk), belong to group-id `disk` on most distributions. If this is the case, you can add VMware Workstation users to the `disk` group. Another option is to change the owner of the device. Consider all the security issues involved in this option.

   b Grant VMware Workstation users access to all `/dev/hd[abcd]` physical devices that contain operating systems or boot managers.

      When permissions are set correctly, the physical disk configuration files in Workstation control access. This reliability provides boot managers access to configuration files and other files they might need to boot operating systems. For example, LILO needs to read `/boot` on a Linux partition to boot a non-Linux operating system that might be on another drive.

## Specifying Disk Capacity for a Virtual Machine

If you instruct the New Virtual Machine wizard to create a new virtual disk during a custom configuration, the wizard prompts you to set the size of the virtual disk and specify whether to split the disk into multiple virtual disk (`.vmdk`) files.

A virtual disk is made up of one or more virtual disk files. Virtual disk files store the contents of the virtual machine hard disk drive. Almost all of the file content is virtual machine data. A small portion of the file is allotted to virtual machine overhead. If the virtual machine is connected directly to a physical disk, the virtual disk file stores information about the partitions that the virtual machine is allowed to access.

You can set a size between 0.001GB and 8TB for a virtual disk file. You can also select whether to store a virtual disk as a single file or split it into multiple files.

Select **Split virtual disk into multiple files** if the virtual disk is stored on a file system that has a file size limitation. When you split a virtual disk less than 950GB, a series of 2GB virtual disk files are created. When you split a virtual disk greater than 950GB, two virtual disk files are created. The maximum size of the first virtual disk file is 1.9TB and the second virtual disk file stores the rest of the data.

For custom configurations, you can select **Allocate all disk space now** to allocate all disk space immediately rather than allow the disk space to gradually grow to the maximum amount. Allocating all the disk space immediately might provide better performance, but it is a time-consuming operation that requires as much physical disk space as you specify for the virtual disk. If you allocate all the disk space immediately, you cannot use the shrink disk feature.

After you create a virtual machine, you can edit virtual disk settings and add additional virtual disks.

### Disk Size Compatibility

The size of a virtual disk is limited to 8TBs. However, your hardware version, bus type, and controller type also impact the size of your virtual disks.

| Workstation Hardware Version | Bus Type | Controller Type | Maximum Disk Size |
|---|---|---|---|
| 10 | IDE | ATAPI | 8192GB (8TB) |
| 10 | SCSI | BusLogic | 2040GB (2TB) |
| 10 | SCSI | LSI Logic | 8192GB (8TB) |
| 10 | SCSI | LSI Logic SAS | 8192GB (8TB) |
| 10 | SATA | AHCI | 8192GB (8TB) |
| 9, 8, 7, 6.5 | All | All | 2040GB (2TB) |
| 6.0, 5 | All | All | 950 GB |

To discover your controller type, open the virtual machine .vmx file. The value of the setting `scsi0.virtualDev` determines your controller type.

| Value | Controller Type |
|---|---|
| Blank or not present | BusLogic |
| lsilogic | LSI Logic |
| lsisas1068 | LSI Logic SAS |

### Specifying the Name and Location of Virtual Disk Files

During a custom configuration, if you instruct the New Virtual Machine wizard to create a new virtual disk, use an existing virtual disk, or use a physical disk, the wizard prompts you for the name and location of a virtual disk (`.vmdk`) file.

**Table 1-6.** Required Information for Each Disk Type

| Type of Disk | Description |
|---|---|
| New virtual disk | If you specified that all disk space should be stored in a single file, Workstation uses the filename that you provide to create one 40GB disk file. If you specified that disk space should be stored in multiple files, Workstation generates subsequent filenames by using the filename that you provide. If you specified that files can increase in size, subsequent filenames include an `s` in the file number, for example, `Windows 7-s001.vmdk`. If you specified that all disk space should be allocated when the virtual disk is created, subsequent filenames include an `f` in the file number, for example, `Windows 7-f001.vmdk`. |
| Existing virtual disk | You select the name and location of an existing virtual disk file. |
| Physical disk | After the wizard prompts you to select a physical device and specify whether to use the entire disk or individual partitions, you must specify a virtual disk file. Workstation uses this virtual disk file to store partition access configuration information for the physical disk. |

**NOTE** Earlier VMware products use the `.dsk` extension for virtual disk files.

## Customizing Virtual Machine Hardware

You can click **Customize Hardware** on the last page of the New Virtual Machine wizard to customize the virtual machine hardware.

You can change the default hardware settings, including memory allocation, number of virtual CPUs, CD/DVD and floppy drive settings, and the network connection type.

## Worksheet for Creating a Virtual Machine

You can print this worksheet and write down the values to specify when you run the New Virtual Machine wizard.

**Table 1-7.** Worksheet: Creating a Virtual Machine

| Option | Fill In Your Value Here |
|---|---|
| Hardware compatibility setting | |
| Guest operating system source | |
| Guest operating system type (for manual installation) | |
| Easy Install information for Windows guests<br>■ Product key<br>■ Operating system version<br>■ Full name<br>■ Password<br>■ Credentials for automatic login | |

**Table 1-7.** Worksheet: Creating a Virtual Machine (Continued)

| Option | Fill In Your Value Here |
|---|---|
| Easy Install information for Linux guests<br>■ Full name<br>■ User name<br>■ Password | |
| Virtual machine name | |
| Virtual machine location | |
| Number of processors | |
| Memory allocation | |
| Network connection type | |
| I/O controller type | |
| Hard disk | |
| Virtual hard disk type | |
| Disk capacity | |
| Virtual disk file name and location | |

# Create a New Virtual Machine on the Local Host

You create a new virtual machine on the local host system by running the New Virtual Machine wizard.

You can also use the New Virtual Machine wizard to create shared virtual machines, which can be used by remote users, and remote virtual machines, which run on remote hosts. See Chapter 6, "Using Remote Connections and Sharing Virtual Machines," on page 179.

### Prerequisites

- Verify that you have the information the New Virtual Machine wizard requires to create a virtual machine. See "Preparing to Create a New Virtual Machine," on page 8.
- Verify that the guest operating system you plan to install is supported. See the online VMware Compatibility Guide on the VMware Web site.
- See the *VMware Guest Operating System Installation Guide* for information about the guest operating system that you plan to install.
- If you are installing the guest operating system from an installer disc, insert the installer disc in the CD-ROM drive in the host system.
- If you are installing the guest operating system from an ISO image file, verify that the ISO image file is in a directory that is accessible to the host system.
- If the virtual machine will use a physical disk or unused partition on the host system, perform the appropriate preparation tasks. See "Prepare to Use a Physical Disk or Unused Partition," on page 14.

### Procedure

1 Start the New Virtual Machine wizard.

| Option | Description |
|---|---|
| **Windows host** | ■ If the host is not connected to a remote server, select **File > New Virtual Machine**.<br>■ If the host is connected to a remote server, select **File > New Virtual Machine > On this Computer**. |
| **Linux host** | Select **File > New Virtual Machine**. |

2 Select the configuration type.

| Option | Description |
|---|---|
| **Typical** | The wizard prompts you to specify or accept defaults for basic virtual machine settings. The typical configuration type is appropriate in most instances. |
| **Custom** | You must select the custom configuration type to make a different virtual machine version than the default hardware compatibility setting, specify the I/O adapter type for SCSI adapters, specify whether to create an IDE, SCSI, or SATA virtual disk, use a physical disk instead of a virtual disk, use an existing virtual disk, or allocate all virtual disk space rather than let disk space gradually grow to the maximum disk size. |

3 If you selected the **Custom** option, select a hardware compatibility setting.

The hardware compatibility setting determines the hardware features of the virtual machine.

4 Select the source of the guest operating system.

| Option | Description |
|---|---|
| **Use a physical disc** | Select the physical drive where you inserted the installation disc. |
| **Use an ISO image** | Type or browse to the location of the ISO image file for the guest operating system. |
| **Install the guest operating system later** | Create a virtual machine that has a blank disk. You must install the guest operating system manually after you create the virtual machine. |

5 Specify information about the guest operating system.

| Option | Description |
|---|---|
| **You are using Easy Install** | Type the Easy Install information for the guest operating system. |
| **You are not using Easy Install** | Select the guest operating system type and version. If the guest operating system is not listed, select **Other**. |

6 Type a virtual machine name and type or browse to the directory for the virtual machine files.

7 Follow the prompts to configure the virtual machine.

If you selected a typical configuration, the wizard prompts you to configure the virtual disk size and specify whether the disk should be split into multiple files. If you selected a custom configuration, the wizard prompts you to configure the virtual machine processors, memory allocation, networking configuration, I/O controller types, virtual disk type and mode, and virtual disk.

8 (Optional) Click **Customize Hardware** to customize the hardware configuration.

You can also modify virtual hardware settings after you create the virtual machine.

9 (Optional) Select **Power on this virtual machine after creation** to power on the virtual machine after you create it.

This option is not available if you are installing the guest operating system manually.

10 Click **Finish** to create the virtual machine.

If you are using Easy Install, guest operating system installation begins when the virtual machine powers on. The guest operating system installation is automated and typically runs without requiring any input from you. After the guest operating system is installed, Easy Install installs VMware Tools.

If you are not using Easy Install, the virtual machine appears in the library.

### What to do next

If you used Easy Install and the virtual machine did not power on when you finished the New Virtual Machine wizard, power on the virtual machine to start the guest operating system installation. See "Use Easy Install to Install a Guest Operating System," on page 20.

If you did not use Easy Install, install the guest operating system manually. See "Install a Guest Operating System Manually," on page 21.

## Use Easy Install to Install a Guest Operating System

When you use Easy Install, you usually do not need to provide information during guest operating system installation.

If you did not provide all of the Easy Install information in the New Virtual Machine wizard, you might be prompted for a product key, username, or password.

Also, if the guest operating system installation consists of multiple discs or ISO image files, the installer might prompt you for the next disk.

### Procedure

- If the installer prompts you for a product key, username, or password, click in the virtual machine window and type the required information.

  Mouse and keyboard input are captured by the virtual machine.

- If you are using physical discs and the installer prompts you for the next disk, use the CD-ROM or DVD drive on the host system.

- If you are using multiple ISO image files and the installer prompts you for the next disk, select the next ISO image file.

| Option | Description |
|---|---|
| **Windows host** | Click **Change Disk** and browse to the next ISO image file. |
| **Linux host** | a Select **VM > Removable Devices > CD/DVD > Settings** and browse to the next ISO image file.<br>b Select **Connected**.<br>c Click **Save**. |

## Install a Guest Operating System Manually

Installing a guest operating system in a virtual machine is similar to installing an operating system on a physical computer. If you do not use Easy Install when you create a virtual machine in the New Virtual Machine wizard, you must install the guest operating system manually.

You can install a guest operating system from an installer disc or ISO image file. You can also use a PXE server to install the guest operating system over a network connection. If the host configuration does not permit the virtual machine to boot from an installer disc, you can create an ISO image file from the installer disc.

### Prerequisites

- Verify that the operating system is supported. See the online VMware Compatibility Guide on the VMware Web site.
- See the *VMware Guest Operating System Installation Guide* for information on the guest operating system that you are installing.

### Procedure

1. If you are installing the guest operating system from an installer disc, configure the virtual machine to use a physical CD-ROM or DVD drive and configure the drive to connect at power on.
   a. Select the virtual machine and select **VM > Settings**.
   b. On the **Hardware** tab, select **CD/DVD drive**.
   c. Select **Connect at power on**.
   d. (Remote virtual machine only) Select the location of the CD-ROM or DVD drive.
   e. Select **Use physical drive** and select a the drive.
   f. Click **OK** to save your changes.
2. If you are installing the guest operating system from an ISO image file, configure the CD/DVD drive in the virtual machine to point to the ISO image file and configure the drive to connect at power on.
   a. Select the virtual machine and select **VM > Settings**.
   b. On the **Hardware** tab, select **CD/DVD drive**.
   c. Select **Connect at power on**.
   d. (Remote virtual machine only) Select the location of the ISO image file.
   e. Select **Use ISO image file** and browse to the location of the ISO image file.
   f. Click **OK** to save your changes.
3. If you are installing the guest operating system from an installer disc, insert the disc in the CD-ROM or DVD drive.
4. Power on the virtual machine.
5. Follow the installation instructions provided by the operating system vendor.
6. If the operating system consists of multiple installer discs and you are prompted to insert the next disc, insert the next disc in the physical drive.

7 If the operating system consists of multiple ISO image files, select the image file for the next CD.

   a Select **VM > Removable Devices > CD/DVD > Disconnect** and disconnect from the current ISO image file.

   b Select **VM > Removable Devices > CD/DVD > Settings** and select the next ISO image file.

   c Select **Connected** and click **OK**.

8 Use the standard tools in the operating system to configure its settings.

#### What to do next

Install VMware Tools. You should install VMware Tools before you activate the license for the operating system. See "Installing VMware Tools," on page 30.

### Installing a Guest Operating System on a Physical Disk or Unused Partition

You can install a guest operating system directly on a physical disk or unused partition on the host system.

A physical disk directly accesses an existing local disk or partition. You can use physical disks to run one or more guest operating systems from existing disk partitions.

Workstation supports physical disks up to 2TB capacity. Booting from an operating system already set up on an existing SCSI disk or partition is not supported.

Running an operating system natively on the host system and switching to running it inside a virtual machine is similar to pulling the hard drive out of one computer and installing it in a second computer that has a different motherboard and hardware. The steps you take depend on the guest operating system in the virtual machine. In most cases, a guest operating system that is installed on a physical disk or unused partition cannot boot outside of the virtual machine, even though the data is available to the host system. See the *Dual-Boot Computers and Virtual Machines* technical note on the VMware Web site for information about using an operating system that can also boot outside of a virtual machine.

After you configure a virtual machine to use one or more partitions on a physical disk, do not modify the partition tables by running `fdisk` or a similar utility in the guest operating system. If you use `fdisk` or a similar utility on the host operating system to modify the partition table of the physical disk, you must recreate the virtual machine physical disk. All files that were on the physical disk are lost when you modify the partition table.

---

**IMPORTANT** You cannot use a physical disk to share files between the host system and a guest operating system. Making the same partition visible to both the host system and a guest operating system can cause data corruption. Instead, use shared folder to share files between the host system and a guest operating system.

---

## Cloning Virtual Machines

Installing a guest operating system and applications can be time consuming. With clones, you can make many copies of a virtual machine from a single installation and configuration process. Cloning a virtual machine is faster and easier than copying it.

Clones are useful when you must deploy many identical virtual machines to a group. For example, an MIS department can clone a virtual machine that has a suite of preconfigured office applications for each employee. You can also configure a virtual machine that has a complete development environment and then clone it repeatedly as a baseline configuration for software testing.

The existing virtual machine is called the parent virtual machine. When the cloning operation is complete, the clone becomes a separate virtual machine.

Changes made to a clone do not affect the parent virtual machine, and changes made to the parent virtual machine do not appear in a clone. The MAC address and UUID for a clone are different from the parent virtual machine.

- Using Linked Clones on page 23

  A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner.

- Using Full Clones on page 24

  A full clone is a complete and independent copy of a virtual machine. It shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is entirely separate from the parent virtual machine.

- Enable Template Mode for a Parent Virtual Machine of Linked Clones on page 24

  To prevent the parent virtual machine for a linked clone from being deleted, you can designate the parent as a template. When template mode is enabled, the virtual machine, and snapshots of the virtual machine, cannot be deleted.

- Clone a Virtual Machine on page 24

  The Clone Virtual Machine wizard guides you through the process of cloning a virtual machine. You do not need to locate and manually copy the parent virtual machine files.

## Using Linked Clones

A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner.

Because a linked clone is made from a snapshot of the parent, disk space is conserved and multiple virtual machines can use the same software installation. All files available on the parent at the moment you take the snapshot continue to remain available to the linked clone.

Ongoing changes to the virtual disk of the parent do not affect the linked clone, and changes to the disk of the linked clone do not affect the parent. A linked clone must have access to the parent. Without access to the parent, you cannot use a linked clone.

Because linked clones are created swiftly, you can create a unique virtual machine for each task. You can also share a virtual machine with other users by storing the virtual machine on your local network where other users can quickly make a linked clone. For example, a support team can reproduce a bug in a virtual machine, and an engineer can quickly make a linked clone of that virtual machine to work on the bug.

You can make a linked clone from a linked clone, but the performance of the linked clone degrades. If you make a full clone from a linked clone, the full clone is an independent virtual machine that does not require access to the linked clone or its parent. You should make a linked clone of the parent virtual machine, if possible.

**IMPORTANT** You cannot delete a linked clone snapshot without destroying the linked clone. You can safely delete the snapshot only if you also delete the clone that depends on it.

## Using Full Clones

A full clone is a complete and independent copy of a virtual machine. It shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is entirely separate from the parent virtual machine.

Because a full clone does not share virtual disks with the parent virtual machine, full clones generally perform better than linked clones. Full clones take longer to create than linked clones. Creating a full clone can take several minutes if the files involved are large.

Because a full clone duplicates only the state of the virtual machine at the instant of the cloning operation, it does not have access to snapshots of the parent virtual machine.

## Enable Template Mode for a Parent Virtual Machine of Linked Clones

To prevent the parent virtual machine for a linked clone from being deleted, you can designate the parent as a template. When template mode is enabled, the virtual machine, and snapshots of the virtual machine, cannot be deleted.

**NOTE** You cannot enable template mode for a shared or remote virtual machine.

### Prerequisites

If the parent does not have at least one snapshot, create a snapshot. See "Taking Snapshots of Virtual Machines," on page 77.

### Procedure

1 Select the virtual machine to use as a parent of the linked clone and select **VM > Settings**.

2 On the **Options** tab, select **Advanced**.

3 Select **Enable Template mode (to be used for cloning)** and click **OK**.

## Clone a Virtual Machine

The Clone Virtual Machine wizard guides you through the process of cloning a virtual machine. You do not need to locate and manually copy the parent virtual machine files.

### Prerequisites

- Familiarize yourself with the different types of clones. See "Using Full Clones," on page 24 and "Using Linked Clones," on page 23.
- Run a defragmentation utility in the guest operating system to defragment the drives on the parent virtual machine.
- If the parent virtual machine is a Workstation 4.x and Workstation 4.x-compatible virtual machine, upgrade it to Workstation 5.x or later.
- If you are creating a linked clone, enable template mode for the parent virtual machine. See "Enable Template Mode for a Parent Virtual Machine of Linked Clones," on page 24.
- Power off the parent virtual machine.

### Procedure

1 Select the parent virtual machine and select **VM > Manage > Clone**.

2 Select the state of the parent from which you want to create a clone.

You can create a clone from the current state of the parent virtual machine or from an existing snapshot. If you select the current state, Workstation creates a snapshot of the parent virtual machine before cloning it.

**NOTE** You cannot clone from the current state if template mode is enabled for the parent virtual machine.

3 Specify whether to create a linked clone or a full clone.

4 Type a name and a location for the cloned virtual machine.

5 Click **Finish** to create the clone and **Close** to exit the wizard.

A full clone can take several minutes to create, depending on the size of the virtual disk that is being duplicated.

6 If the parent virtual machine uses a static IP address, change the static IP address of the clone before the clone connects to the network to prevent IP address conflicts.

Although the wizard creates a new MAC address and UUID for the clone, other configuration information, such as the virtual machine name and static IP address configuration, is identical to that of the parent virtual machine.

The summary view for a linked clone shows the path to the virtual machine configuration (`.vmx`) file of the parent virtual machine.

## Virtualize a Physical Machine

You can create a virtual machine from a Windows physical machine in Workstation. When you virtualize a physical machine, you capture all of the applications, documents, and settings on the physical machine in a new virtual machine. Workstation must be running on a Windows host system to use this feature.

### Prerequisites

- Verify that the physical machine that you want to virtualize is running Windows. You cannot create a virtual machine from a non-Windows physical machine in Workstation.
- Verify that you have administrative access on the physical machine that you want to virtualize and on the Workstation host system.
- Verify that the Workstation host system has network access to the physical machine that you want to virtualize.
- Verify that on the Workstation host system you have disabled User Account Control (UAC). For instructions, see "Prepare a Windows Physical Machine for Virtualization," on page 26.
- Turn off firewall applications running on the physical machine that you want to virtualize.
- Prepare the physical machine for virtualization. See "Prepare a Windows Physical Machine for Virtualization," on page 26.

### Procedure

1 Power on the physical machine that you want to virtualize.

2 On the Windows host system, in Workstation, select **File > Virtualize a Physical Machine**.

If you have never virtualized a physical machine or imported a third-party virtual machine in Workstation, Workstation installs VMware vCenter Converter Standalone. After the installation is finished, you must restart the virtualization wizard.

3 Type the hostname or IP address, user name, and password for the physical machine that you want to virtualize.

   You must use the Administrator account or a user account that is a member of the local Administrators group.

4 Type a name for the new virtual machine and specify a location on the host system in which to store the virtual machine files.

5 Type the user name and password for your user account on the host system.

6 Click **Finish** to create a virtual machine from the physical machine.

   The amount of time required to create the virtual machine depends on the size of the hard disk on the physical machine.

VMware Tools installation begins the first time you power on the new virtual machine.

## Prepare a Windows Physical Machine for Virtualization

To avoid problems related to permissions and network access, you must perform certain steps to prepare a Windows physical machine before you run the Virtualize a Physical Machine wizard.

### Procedure

1 If the physical machine is running Windows XP, turn off simple file sharing on the physical machine.

   Turning off simple file sharing does not turn off the Shared Documents feature. You can use the simple file sharing interface, which is located in folder properties, to configure share and file permissions.

   **NOTE** On Windows XP systems that are part of a workgroup, the simple file sharing interface is turned on by default. Windows XP systems that are part of a domain use only the classic file sharing and security interface.

   a Open the **Folder Options** control panel.

   b On the **View** tab, deselect **Use Simple File Sharing (Recommended)**.

2 If the physical machine is running Windows Vista or Windows 7, disable User Account Control (UAC).

   - On Windows Vista, open the **User Accounts** control panel, select **Turn User Account Control On or Off**, and deselect **Use User Account Control (UAC) to help protect your computer**.
   - On Windows 7, open the **Change User Account Control Settings** control panel and drag the slider to **Never notify**.

## Troubleshoot Windows Authentication Problems During Physical Machine Virtualization

User authentication fails when the Virtualize a Physical Machine wizard attempts to connect a Windows physical machine.

### Problem

After you provide user credentials for the physical machine, the Virtualize a Physical Machine wizard reports that your user credentials are incorrect or you have insufficient permissions to connect to the physical machine.

### Cause

Simple file sharing or User Account Control (UAC) is enabled on the physical machine.

#### Solution

Perform the steps in "Prepare a Windows Physical Machine for Virtualization," on page 26 and rerun the Virtualize a Physical Machine wizard.

### Troubleshoot Windows Activation Problems

A virtual machine that you create from a physical machine prompts you to activate Windows when you use it in Workstation.

#### Problem

After you create a virtual machine from a Windows Vista or Windows 7 physical machine, or from a physical PC that came with Windows preinstalled, you were required to reactivate Windows in the virtual machine.

#### Cause

When you create a virtual machine from a Windows Vista or Windows 7 physical machine, the operating system detects that the computer hardware has changed. When you make a significant hardware change, Microsoft requires you to activate Windows again.

The OEM versions of Windows that are preinstalled on some new computers are customized for those computers. OEM licenses of Windows are not transferrable.

#### Solution

Any virtual machine that was created from a physical machine that had its Windows license key successfully activated needs to be reactivated when you run it in Workstation.

The activation process in Windows Vista and Windows 7 is different from the Windows XP activation process. In Windows Vista and Windows 7, retail activation keys are good for only one use. If you enter the same activation key in Workstation that you used previously, you cannot successfully activate the virtual machine.

The activation wizard tells you that the activation key was already used and prompts you to call the Microsoft activation hotline to get a second key. If you did not previously call the hotline for the same license key, you should receive a new activation key. Your call is not transferred to an operator unless you call repeatedly for the same key.

See the Microsoft Web site for more information about why reactivation is necessary.

## Importing Virtual Machines

You can import Windows XP Mode, Open Virtualization Format (OVF), and Windows Virtual PC virtual machines in Workstation.

### Import a Windows XP Mode Virtual Machine

You can import a Windows XP Mode virtual machine and run it in Workstation. When you import a Windows XP Mode virtual machine, Workstation creates a new virtual machine in VMware runtime (`.vmx`) format.

You can power on only one Windows XP Mode virtual machine at a time in Workstation. If you move a Windows XP Mode virtual machine to another host system, it becomes a new virtual machine and you must activate it.

**NOTE** Changes made to the original Windows XP Mode virtual machine through Virtual PC do not affect the virtual machine imported in Workstation.

### Prerequisites

- Verify that the Windows 7 Professional, Enterprise, or Ultimate edition operating system is running on the host system. Importing Windows XP Mode virtual machines is not supported on Linux host systems or on host systems that are running other versions of Windows.
- Download and install the Windows XP Mode virtual machine on the host system.

### Procedure

1 Select **File > Import Windows XP Mode VM**, or select **File > Open** and browse to the virtual machine configuration (`.vmc`) file.

   If you have never imported a third-party virtual machine or virtualized a physical machine in Workstation, Workstation installs VMware vCenter Converter Standalone. After the installation is finished, you must restart the import.

2 Type a name for the new virtual machine, type or browse to the directory for the virtual machine files, and click **Import**.

   Workstation begins importing the Windows XP Mode virtual machine.

After Workstation successfully imports the Windows XP Mode virtual machine, a new virtual machine appears in the virtual machine library.

## Import an Open Virtualization Format Virtual Machine

You can import an Open Virtualization Format (OVF) virtual machine and run it in Workstation. Workstation converts the virtual machine from OVF format to VMware runtime (`.vmx`) format. You can import both `.ovf` and `.ova` files.

OVF is a platform-independent, efficient, extensible, and open packaging and distribution format for virtual machines. For example, you can import OVF virtual machines exported from VMware Fusion™ or Oracle VM VirtualBox into Workstation. You can import OVF 1.0 and later files only.

You can also use the standalone OVF Tool to convert an OVF virtual machine to VMware runtime format. The standalone version of the OVF Tool is installed in the Workstation installation directory under `OVFTool`. See the *OVF Tool User Guide* on the VMware Web site for information on using the OVF Tool.

### Procedure

1 In Workstation, select **File > Open**.

2 Browse to the `.ovf` or `.ova` file and click **Open**.

3 Type a name for the virtual machine, type or browse to the directory for the virtual machine files, and click **Import**.

   Workstation performs OVF specification conformance and virtual hardware compliance checks. A status bar indicates the progress of the import process.

4 If the import fails, click **Retry** to try again, or click **Cancel** to cancel the import.

   If you retry the import, Workstation relaxes the OVF specification conformance and virtual hardware compliance checks and you might not be able to use the virtual machine in Workstation.

After Workstation successfully imports the OVF virtual machine, the virtual machine appears in the virtual machine library.

## Import a Windows Virtual PC Virtual Machine

You can import a Windows Virtual PC virtual machine and run it in Workstation. Workstation converts the virtual machine from Virtual PC (`.vmc`) format to VMware runtime (`.vmx`) format. This feature is supported only on Windows host systems.

### Prerequisites

Download and install the Virtual PC virtual machine on the Windows host system.

### Procedure

1 In Workstation, select **File > Open**.

If you have never imported a third-party virtual machine or virtualized a physical machine in Workstation, Workstation installs VMware vCenter Converter Standalone. After the installation is finished, you must restart the import.

2 Browse to the `.vmc` file and click **Open**.

3 Type a name for the virtual machine, type or browse to the directory for the virtual machine files, and click **Import**.

After Workstation successfully imports the Virtual PC virtual machine, the virtual machine appears in the virtual machine library.

# Installing and Upgrading VMware Tools

Installing VMware Tools is part of the process of creating a new virtual machine. Upgrading VMware Tools is part of the process of keeping virtual machines up to current standards.

For the best performance and latest updates, install or upgrade VMware Tools to match the version of Workstation that you are using. Other compatibility options are also available.

- Installing VMware Tools on page 30

  VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.

- Upgrading VMware Tools on page 30

  You can upgrade VMware Tools manually, or you can configure virtual machines to check for and install newer versions of VMware Tools.

- Configure Automatic Software Updates on page 31

  You can configure Workstation to automatically download software updates, including new versions of VMware Tools. When automatic software updates are enabled, Workstation always includes the latest support for guest operating systems and virtual machines always have the latest version of VMware Tools.

- Configure VMware Tools Updates for a Specific Virtual Machine on page 32

  You can configure virtual machines that have Windows or Linux guest operating systems to update VMware Tools automatically. For other guest operating systems, you must manually update VMware Tools.

- Manually Installing and Upgrading VMware Tools on page 33

  You can manually install or upgrade VMware Tools on Windows, Linux, NetWare, Solaris, and FreeBSD virtual machines.

- Start the VMware User Process Manually If You Do Not Use a Session Manager on page 39

  VMware Tools in Linux, Solaris, and FreeBSD guest operating systems uses the VMware User process executable file. This  program implements the fit-guest-to-window feature and Unity mode, among other features.

- Uninstall VMware Tools on page 39

  Occasionally, an upgrade of VMware Tools is incomplete. You can usually solve the problem by uninstalling VMware Tools and then reinstalling.

## Installing VMware Tools

VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.

Although the guest operating system can run without VMware Tools, many VMware features are not available until you install VMware Tools. For example, if you do not have VMware Tools installed in your virtual machine, you cannot use the shutdown or restart options from the toolbar. You can use only the power options.

You can use the Windows Easy Install or Linux Easy Install feature to install VMware Tools as soon as the operating system is finished installing.

The installers for VMware Tools are ISO image files. An ISO image file looks like a CD-ROM to your guest operating system. Each type of guest operating system, including Windows, Linux, Solaris, FreeBSD, and NetWare, has an ISO image file. When you select the command to install or upgrade VMware Tools, the virtual machine's first virtual CD-ROM disk drive temporarily connects to the VMware Tools ISO file for your guest operating system.

The most recent versions of the ISO files are stored on a VMware Web site. When you select the command to install or upgrade VMware Tools, the VMware product determines whether it has downloaded the most recent version of the ISO file for the specific operating system. If the latest version has not been downloaded or if no VMware Tools ISO file for that operating system has ever been downloaded, you are prompted to download the file.

The installation procedure varies, depending on the operating system.

## Upgrading VMware Tools

You can upgrade VMware Tools manually, or you can configure virtual machines to check for and install newer versions of VMware Tools.

The guest operating system checks the version of VMware Tools when you power on a virtual machine. The status bar of the virtual machine displays a message when a new version is available.

In Windows virtual machines, you can set VMware Tools to notify you when an upgrade is available. If this notification option is enabled, the VMware Tools icon in the Windows taskbar includes a yellow caution icon when a VMware Tools upgrade is available.

To install a VMware Tools upgrade, you can use the same procedure that you used for installing VMware Tools the first time. Upgrading VMware Tools means installing a new version.

For Windows and Linux guest operating systems, you can configure the virtual machine to automatically upgrade VMware Tools. Although the version check is performed when you power on the virtual machine, on Windows guest operating systems, the automatic upgrade occurs when you power off or restart the virtual machine. The status bar displays the message `Installing VMware Tools ...` when an upgrade is in progress.

**IMPORTANT** When you upgrade VMware Tools on Linux guest operating systems, new network modules are available but are not used until you either restart the guest operating system or stop networking, unload and reload the VMware networking kernel modules, and restart networking. This behavior means that even if VMware Tools is set to automatically upgrade, you must restart or reload network modules to make new features available.

This strategy avoids network interruptions and allows you to install VMware Tools over SSH.

## Configure Automatic Software Updates

You can configure Workstation to automatically download software updates, including new versions of VMware Tools. When automatic software updates are enabled, Workstation always includes the latest support for guest operating systems and virtual machines always have the latest version of VMware Tools.

### Prerequisites

- On a Linux host, become root. On Linux systems, non-root users are not allowed to modify the preference setting for VMware Tools updates.
- Verify that the host system is connected to the Internet.

### Procedure

1 Select **Edit > Preferences** and select **Updates**.

2 Select a software update download option.

If you deselect all of the software update options, automatic software updates are disabled.

| Option | Description |
|---|---|
| **Check for product updates on startup** | When Workstation starts, it checks for new versions of the application and installed software components. |
| **Check for software components as needed** | When a software component is needed, for example, when you install or upgrade VMware Tools on a virtual machine, Workstation checks for a new version of the component. |
| **Download All Components Now** | Click this button to download all software updates immediately. This option is useful if you are planning to use a virtual machine at a later time when you do not have access to the Internet. |

3 If you use a proxy server to connect to the Internet, click **Connection Settings** and select a proxy setting.

| Option | Description |
|---|---|
| **No proxy** | Select this option if you do not use a proxy server. This is the default setting. |
| **Windows proxy settings** | (Windows hosts only) Workstation uses the host proxy settings from the Connections tab in the Internet Options control panel to access the VMware Update Server. Click **Internet Options** to set the guest connection options. Type a username and password to use for proxy server authentication. If you leave either the **Username** or **Password** text box blank, Workstation does not use either value. |
| **Manual proxy settings** | Select an HTTP or SOCKS proxy, specify the proxy server address and designate a port number to access the VMware Update Server. Type a username and password to use for proxy server authentication. If you leave either the **Username** or **Password** text box blank, Workstation does not use either value (Windows hosts) or it uses the username and password set in the gnome settings (Linux hosts). |

4 To update VMware Tools when you power on a virtual machine or shut down the guest operating system, select **Automatically update VMware Tools on a virtual machine**.

You can override this setting for a specific virtual machine by modifying virtual machine settings.

When you power on a virtual machine, you are prompted to download VMware Tools if a new version is available.

5 Click **OK** to save your changes.

### What to do next

To override the VMware Tools update setting for a specific virtual machine, edit the virtual machine settings. See "Configure VMware Tools Updates for a Specific Virtual Machine," on page 32.

## Configure VMware Tools Updates for a Specific Virtual Machine

You can configure virtual machines that have Windows or Linux guest operating systems to update VMware Tools automatically. For other guest operating systems, you must manually update VMware Tools.

Automatic VMware Tools updates are supported for versions of VMware Tools included in Workstation 5.5 and later virtual machines only. Automatic updates are not supported for versions of VMware Tools included in virtual machines created with VMware Server 1.x.

IMPORTANT If you update VMware Tools in a Windows virtual machine that was created with Workstation 4 or 5.x, some new components are not installed. To install the new components, you must uninstall the old version of VMware Tools and install the new version of VMware Tools.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **VMware Tools**.

3 Select a VMware Tools update setting.

| Option | Description |
|---|---|
| **Update manually (do nothing)** | You must update VMware Tools manually. The virtual machine status bar indicates when a new version of VMware Tools is available. |
| **Update automatically** | VMware Tools is updated automatically. The virtual machine status bar indicates when an update is in progress. If you are logged in to a Windows guest, a restart prompt appears after the update is complete. If you are not logged in, the operating system restarts without prompting. An auto-update check is performed as part of the boot sequence when you power on the virtual machine. If the virtual machine was suspended and you resume it or restore it to a snapshot during the boot sequence before this check, the automatic update occurs as planned. If you resume the virtual machine or restore it to a snapshot after the check, the automatic update does not occur. |
| **Use application default (currently update manually)** | Use the default VMware Tools update behavior. The default behavior is set in Workstation preferences.<br>NOTE You cannot configure this option for a shared or remote virtual machine. |

4 Click **OK** to save your changes.

## Manually Installing and Upgrading VMware Tools

You can manually install or upgrade VMware Tools on Windows, Linux, NetWare, Solaris, and FreeBSD virtual machines.

If you are installing VMware Tools in a number of Windows virtual machines, you can automate its installation by using the VMware Tools `setup.exe` at a command prompt in the guest operating system. See *Installing and Configuring VMware Tools* for more information.

- Manually Install or Upgrade VMware Tools in a Windows Virtual Machine on page 33

  All supported Windows guest operating systems support VMware Tools.

- Manually Install or Upgrade VMware Tools in a Linux Virtual Machine on page 34

  For Linux virtual machines, you manually install or upgrade VMware Tools by using the command line.

- Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine on page 36

  For NetWare virtual machines, you manually install or upgrade VMware Tools by using the command line.

- Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine on page 37

  For Solaris virtual machines, you manually install or upgrade VMware Tools by using the command line.

- Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine on page 38

  For FreeBSD virtual machines, you manually install or upgrade VMware Tools by using the command line.

### Manually Install or Upgrade VMware Tools in a Windows Virtual Machine

All supported Windows guest operating systems support VMware Tools.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility in your environment.

For Windows 2000 and later, VMware Tools installs a virtual machine upgrade helper tool. This tool restores the network configuration if you upgrade the virtual machine compatibility from ESX/ESXi 3.5 to ESX/ESXi 4.0 and later or from Workstation 5.5 to Workstation 6.0 and later.

#### Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- If you connected the virtual machine's virtual CD/DVD drive to an ISO image file when you installed the operating system, change the setting so that the virtual CD/DVD drive is configured to autodetect a physical drive.

  The autodetect setting enables the virtual machine's first virtual CD/DVD drive to detect and connect to the VMware Tools ISO file for a VMware Tools installation. This ISO file looks like a physical CD to your guest operating system. Use the virtual machine settings editor to set the CD/DVD drive to autodetect a physical drive.
- Log in as an administrator unless you are using an older Windows operating system. Any user can install VMware Tools in a Windows 95, Windows 98, or Windows ME guest operating system. For operating systems newer than these, you must log in as an administrator.

#### Procedure

1. On the host, from the Workstation menu bar, select **VM > Install VMware Tools**.

   If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.
2. If you are installing VMware Tools for the first time, click **OK** on the Install VMware Tools information page.

   If autorun is enabled for the CD-ROM drive in the guest operating system, the VMware Tools installation wizard starts.
3. If autorun is not enabled, to manually launch the wizard, click **Start > Run** and enter **`D:\setup.exe`**, where **`D:`** is your first virtual CD-ROM drive.
4. Follow the on-screen instructions.
5. If the New Hardware wizard appears, follow the prompts and accept the defaults.
6. If you are installing a beta or RC version of VMware Tools and you see a warning that a package or driver is not signed, click **Install Anyway** to complete the installation.
7. When prompted, reboot the virtual machine.

#### What to do next

If a new virtual hardware version is available for the virtual machine, upgrade the virtual hardware.

## Manually Install or Upgrade VMware Tools in a Linux Virtual Machine

For Linux virtual machines, you manually install or upgrade VMware Tools by using the command line.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility in your environment.

#### Prerequisites

- Power on the virtual machine.

- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.

### Procedure

1 On the host, from the Workstation menu bar, select **VM > Install VMware Tools**.

If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

2 In the virtual machine, log in to the guest operating system as root and open a terminal window.

3 Run the `mount` command with no arguments to determine whether your Linux distribution automatically mounted the VMware Tools virtual CD-ROM image.

If the CD-ROM device is mounted, the CD-ROM device and its mount point are listed as something like this:

```
/dev/cdrom on /mnt/cdrom type iso9660 (ro,nosuid,nodev)
```

4 If the VMware Tools virtual CD-ROM image is not mounted, mount the CD-ROM drive.

a If a mount point directory does not already exist, create it.

```
mkdir /mnt/cdrom
```

Some Linux distributions use different mount point names. For example, on some distributions the mount point is `/media/VMware Tools` rather than `/mnt/cdrom`. Modify the command to reflect the conventions that your distribution uses.

b Mount the CD-ROM drive.

```
mount /dev/cdrom /mnt/cdrom
```

Some Linux distributions use different device names or organize the `/dev` directory differently. If your CD-ROM drive is not `/dev/cdrom` or if the mount point for a CD-ROM is not `/mnt/cdrom`, modify the command to reflect the conventions that your distribution uses.

5 Change to a working directory, for example, `/tmp`.

```
cd /tmp
```

6 Delete any previous `vmware-tools-distrib` directory before you install VMware Tools.

The location of this directory depends on where you placed it during the previous installation. Often this directory is placed in `/tmp/vmware-tools-distrib`.

7 List the contents of the mount point directory and note the filename of the VMware Tools tar installer.

```
ls mount-point
```

8 Uncompress the installer.

```
tar zxpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
```

The value *x.x.x* is the product version number, and *yyyy* is the build number of the product release.

If you attempt to install a tar installation over an RPM installation, or the reverse, the installer detects the previous installation and must convert the installer database format before continuing.

9 If necessary, unmount the CD-ROM image.

```
umount /dev/cdrom
```

If your Linux distribution automatically mounted the CD-ROM, you do not need to unmount the image.

10 Run the installer and configure VMware Tools.

```
cd vmware-tools-distrib
./vmware-install.pl
```

Usually, the `vmware-config-tools.pl` configuration file runs after the installer file finishes running.

11 Follow the prompts to accept the default values, if appropriate for your configuration.

12 Follow the instructions at the end of the script.

Depending on the features you use, these instructions can include restarting the X session, restarting networking, logging in again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

### What to do next

If a new virtual hardware version is available for the virtual machine, upgrade the virtual hardware.

## Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine

For NetWare virtual machines, you manually install or upgrade VMware Tools by using the command line.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility in your environment.

### Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.

### Procedure

1 On the host, from the Workstation menu bar, select **VM > Install VMware Tools**.

If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

2 Load the CD-ROM driver so that the virtual CD-ROM device mounts the ISO image as a volume.

| Operating System | Command |
|---|---|
| **NetWare 6.5** | `LOAD CDDVD` |
| **NetWare 6.0 or NetWare 5.1** | `LOAD CD9660.NSS` |
| **NetWare 4.2 (not available in vSphere)** | `load cdrom` |

When the installation finishes, the message `VMware Tools for NetWare are now running` appears in the Logger Screen for NetWare 6.5 and NetWare 6.0 guest operating systems and in the Console Screen for NetWare 4.2 and 5.1 operating systems.

3 If the VMware Tools virtual disc (`netware.iso`) is attached to the virtual machine, right-click the CD-ROM icon in the status bar of the console window and select **Disconnect** to disconnect it.

### What to do next

If a new virtual hardware version is available for the virtual machine, upgrade the virtual hardware.

## Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine

For Solaris virtual machines, you manually install or upgrade VMware Tools by using the command line.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility in your environment.

### Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.

### Procedure

1 On the host, from the Workstation menu bar, select **VM > Install VMware Tools**.

If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

2 In the virtual machine, log in to the guest operating system as root and open a terminal window.

3 If the Solaris volume manager does not mount the CD-ROM under `/cdrom/vmwaretools`, restart the volume manager.

```
/etc/init.d/volmgt stop
/etc/init.d/volmgt start
```

4 Change to a working directory, for example, `/tmp`.

```
cd /tmp
```

5 Extract VMware Tools.

```
gunzip -c /cdrom/vmwaretools/vmware-solaris-tools.tar.gz | tar xf -
```

6 Run the installer and configure VMware Tools.

```
cd vmware-tools-distrib
./vmware-install.pl
```

Usually, the `vmware-config-tools.pl` configuration file runs after the installer file finishes running.

7 Follow the prompts to accept the default values, if appropriate for your configuration.

8 Follow the instructions at the end of the script.

Depending on the features you use, these instructions can include restarting the X session, restarting networking, logging in again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

### What to do next

If a new virtual hardware version is available for the virtual machine, upgrade the virtual hardware.

## Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine

For FreeBSD virtual machines, you manually install or upgrade VMware Tools by using the command line.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility in your environment.

### Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.

### Procedure

1 On the host, from the Workstation menu bar, select **VM > Install VMware Tools**.

If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

2 In the virtual machine, log in to the guest operating system as root and open a terminal window.

3 If the distribution does not automatically mount CD-ROMs, mount the VMware Tools virtual CD-ROM image.

For example, type **`mount /cdrom`**.

4 Change to a working directory, for example, `/tmp`.

```
cd /tmp
```

5 Untar the VMware Tools tar file.

```
tar zxpf /cdrom/vmware-freebsd-tools.tar.gz
```

6 If the distribution does not use automounting, unmount the VMware Tools virtual CD-ROM image.

```
umount /cdrom
```

7 Run the installer and configure VMware Tools.

```
cd vmware-tools-distrib
./vmware-install.pl
```

Usually, the `vmware-config-tools.pl` configuration file runs after the installer file finishes running.

8 Follow the prompts to accept the default values, if appropriate for your configuration.

9 Follow the instructions at the end of the script.

Depending on the features you use, these instructions can include restarting the X session, restarting networking, logging in again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

### What to do next

If a new virtual hardware version is available for the virtual machine, upgrade the virtual hardware.

## Start the VMware User Process Manually If You Do Not Use a Session Manager

VMware Tools in Linux, Solaris, and FreeBSD guest operating systems uses the VMware User process executable file. This program implements the fit-guest-to-window feature and Unity mode, among other features.

Normally, this process starts after you configure VMware Tools, log out of the desktop environment, and log back in. The `vmware-user` program is located in the directory in which you selected to install binary programs, which defaults to `/usr/bin`. The startup script that you need to modify depends on your system. You must start the process manually in the following environments:

- If you run an X session without a session manager. For example, if you use `startx` to start a desktop session and do not use `xdm`, `kdm`, or `gdm`.
- If you are using an older version of GNOME without `gdm` or `xdm`.
- If you are using a session manager or environment that does not support the Desktop Application Autostart Specification, available from http://standards.freedesktop.org.
- If you upgrade VMware Tools.

### Procedure

- Start the VMware User process.

| Option | Action |
|---|---|
| **Start the VMware User process when you start an X session.** | Add `vmware-user` to the appropriate X startup script, such as the `.xsession` or `.xinitrc` file. |
| **Start the process after a VMware Tools software upgrade, or if certain features are not working.** | Open a terminal window and type the **`vmware-user`** command. |

## Uninstall VMware Tools

Occasionally, an upgrade of VMware Tools is incomplete. You can usually solve the problem by uninstalling VMware Tools and then reinstalling.

### Prerequisites

- Power on the virtual machine.
- Log in to the guest operating system.

### Procedure

- Select a method to uninstall VMware Tools.

| Operating System | Action |
|---|---|
| **Windows 7, 8** | In the guest operating system, select **Programs > Uninstall a program**. |
| **Windows Vista and Windows Server 2008** | In the guest operating system, select **Programs and Features > Uninstall a program**. |
| **Windows XP and earlier** | In the guest operating system, select **Add/Remove Programs**. |
| **Linux** | On a Linux guest operating system that has VMware Tools installed by using an RPM installer, enter **`rpm -e VMwareTools`** in a terminal window. |
| **Linux, Solaris, FreeBSD, NetWare** | Log in as root and enter **`vmware-uninstall-tools.pl`** in a terminal window. |
| **Mac OS X Server** | Use the **Uninstall VMware Tools** application, found in `/Library/Application Support/VMware Tools`. |

### What to do next

Reinstall VMware Tools.

# Virtual Machine Files

When you create a virtual machine, Workstation creates a set of files for that specific virtual machine. Virtual machine files are stored in either the virtual machines directory or the working directory. Both directories are typically on the host system.

**Table 1-8.** Virtual Machine Files

| Extension | File Name | Description |
|---|---|---|
| .vmx | *vmname*.vmx | The primary configuration file, which stores virtual machine settings. If you created the virtual machine with an earlier version of Workstation on a Linux host, this file might have a .cfg extension. |
| .log | *vmname*.log<br>or<br>vmware.log | The main log file. If you need to troubleshoot a problem, refer to this file. This file is stored in the same directory as the .vmx file. |
| .nvram | *vmname*.nvram<br>or<br>nvram | The NVRAM file, which stores the state of the virtual machine BIOS. This file is stored in the same directory as the .vmx file. |
| .vmdk | *vmname*.vmdk | Virtual disk files, which store the contents of the virtual machine hard disk drive. These files are stored in the same directory as the .vmx file.<br>A virtual disk is made up of one or more virtual disk files. The virtual machine settings show the name of the first file in the set. This file contains pointers to the other files in the set.<br>If you specify that all disk space should be allocated when the virtual disk is created, these files start at the maximum size and do not grow. Almost all of the file content is virtual machine data. A small portion of the file is allotted to virtual machine overhead.<br>If the virtual machine is connected directly to a physical disk, the virtual disk file stores information about the partitions that the virtual machine is allowed to access.<br>NOTE Earlier VMware products use the .dsk extension for virtual disk files. |
| | *vmname*–s###.vmdk | If you specified that the files can increase, filenames include an s in the file number, for example, Windows 7–s001.vmdk.<br>If you specified that the virtual disk is divided into 2GB sections, the number of files depends on the size of the virtual disk. As data is added to a virtual disk, the files increase to a maximum of 2GB each. |
| | *vmname*–f###.vmdk | If all disk space was allocated when the disk was created, filenames include an f, for example, Windows 7–f001.vmdk. |
| | *vmname*–*disk*–###.vmdk | If the virtual machine has one or more snapshots, some files are redo log files. These files store changes made to a virtual disk while the virtual machine is running. The ### indicates a unique suffix that Workstation adds to avoid duplicate file names. |
| .vmem | *uuid*.vmem | The virtual machine paging file, which backs up the guest main memory on the host file system. This file exists only when the virtual machine is running or if the virtual machine fails. It is stored in the working directory. |
| | *snapshot_name_number*.vmem | Each snapshot of a virtual machine that is powered on has an associated .vmem file, which contains the guest operating system main memory, saved as part of the snapshot. |
| .vmsd | *vmname*.vmsd | A centralized file for storing information and metadata about snapshots. It is stored in the working directory. |

**Table 1-8.** Virtual Machine Files (Continued)

| Extension | File Name | Description |
|---|---|---|
| .vmsn | *vmname*.Snapshot.vmsn | The snapshot state file, which stores the running state of a virtual machine at the time you take that snapshot. It is stored in the working directory. |
| | *vmname*.Snapshot###.vmsn | The file that stores the state of a snapshot. |
| .vmss | *vmname*.vmss | The suspended state file, which stores the state of a suspended virtual machine. It is stored in the working directory.<br>Some earlier VMware products used the .std extension for suspended state files. |

Other files, such as lock files, might also be present in the virtual machines directory. Some files are present only while a virtual machine is running.

# Using Virtual Machines 2

When you use virtual machines in Workstation, you can transfer files and text between virtual machines and the host system, print to host printers, connect removable devices, and change display settings. You can use folders to manage multiple virtual machines, take snapshots to preserve virtual machine states, and create screenshots and movies of virtual machines.

You can also use Workstation to interact with remote virtual machines. See Chapter 6, "Using Remote Connections and Sharing Virtual Machines," on page 179 for more information.

This chapter includes the following topics:


- "Starting Virtual Machines," on page 43
- "Stopping Virtual Machines," on page 47
- "Transferring Files and Text," on page 51
- "Add a Host Printer to a Virtual Machine," on page 60
- "Using Removable Devices in Virtual Machines," on page 61
- "Changing the Virtual Machine Display," on page 68
- "Using Folders to Manage Virtual Machines," on page 74
- "Taking Snapshots of Virtual Machines," on page 77
- "Install New Software in a Virtual Machine," on page 84
- "Share Tablet Sensor Data with Windows 8 Guests," on page 84
- "Take a Screenshot of a Virtual Machine," on page 85
- "Delete a Virtual Machine," on page 85


## Starting Virtual Machines

When you start a virtual machine, the guest operating system starts and you can interact with the virtual machine. You can use Workstation to start virtual machines on the host system and on remote servers. You can also stream virtual machines from a Web server.

To start a virtual machine from the command line, use the `vmware` command. See Chapter 7, "Using the vmware Command," on page 199.


- Start a Virtual Machine on page 44

  You can start a virtual machine from the **VM** menu or from the toolbar. When you use the **VM** menu, you can select a soft or hard power option or start the virtual machine in BIOS setup mode.

- Start a Virtual Machine That Is Running in the Background on page 45

  You can start a virtual machine that is running in the background when Workstation is not started.

- Stream a Virtual Machine from a Web Server on page 45

  When you stream a virtual machine, you can start the virtual machine as soon as the download process begins. When you power off a streamed virtual machine, you are prompted to save or discard changes. If you discard changes, the directory that was created on the local computer and all the virtual machine data are deleted.

- Enable Autologon in a Windows Virtual Machine on page 46

  With Autologon, you can save your login credentials and bypass the login dialog box when you power on a Windows virtual machine. The guest operating system securely stores the password.

## Start a Virtual Machine

You can start a virtual machine from the **VM** menu or from the toolbar. When you use the **VM** menu, you can select a soft or hard power option or start the virtual machine in BIOS setup mode.

When virtual machines are in a folder, you can perform batch power operations. See "Using Folders to Manage Virtual Machines," on page 74.

You can use the AutoStart feature to configure shared and remote virtual machines to start when the host system starts. See "Configure Shared and Remote Virtual Machines to Start with the Host," on page 190.

### Prerequisites

- If the virtual machine is on the local host, select **File > Open** and browse to the virtual machine configuration (`.vmx`) file.
- If the virtual machine is on a remote host, connect to the remote server. See "Connect to a Remote Server," on page 182.

### Procedure

- To select a power option when you start the virtual machine, select the virtual machine and select **VM > Power**.

| Option | Description |
|---|---|
| **Power On** | (Hard option) Workstation starts the virtual machine. |
| **Start Up Guest** | (Soft option) Workstation starts the virtual machine and VMware Tools runs a script in the guest operating system. On Windows guests, if the virtual machine is configured to use DHCP, the script renews the IP address of the virtual machine. On a Linux, FreeBSD, or Solaris guest, the script starts networking for the virtual machine. |
| **Power On to BIOS** | Workstation starts the virtual machine in BIOS setup mode. |

- To start the virtual machine from the toolbar, select the virtual machine and click the start button.

  The start power control setting that is configured for the virtual machine determines whether Workstation performs a hard or soft power on operation. The configured behavior appears in a tooltip when you mouse over the button.

### What to do next

Click anywhere inside the virtual machine console to give the virtual machine control of the mouse and keyboard on the host system.

## Start a Virtual Machine That Is Running in the Background

You can start a virtual machine that is running in the background when Workstation is not started.

### Prerequisites

Set the virtual machine to run in the background. See "Closing Virtual Machines and Exiting Workstation," on page 48.

### Procedure

1 On the host system, click the virtual machine status icon that is located in the notification area of the taskbar.

A list of the virtual machines that are running in the background appears in a tooltip. The list contains the virtual machines that belong to the currently logged in user.

2 Select a virtual machine from the list in the tooltip.

Workstation starts and displays the console view of the virtual machine.

## Stream a Virtual Machine from a Web Server

When you stream a virtual machine, you can start the virtual machine as soon as the download process begins. When you power off a streamed virtual machine, you are prompted to save or discard changes. If you discard changes, the directory that was created on the local computer and all the virtual machine data are deleted.

NOTE You cannot stream a remote virtual machine.

### Prerequisites

- Make the virtual machine available for streaming. See "Make a Virtual Machine Available for Streaming," on page 46.
- Determine the URL of the virtual machine.

### Procedure

1 Run the `vmware` command and specify the URL of the virtual machine.

Both HTTP and HTTPS are supported.

| Option | Description |
|---|---|
| **Windows host** | `vmware.exe http://path_to_vm.vmx` |
| **Linux host** | `vmware http://path_to_vm.vmx` |

A tab for the virtual machine opens in the Workstation window.

2 Select the virtual machine and select **VM > Power > Power On**.

Workstation fetches virtual disk data on demand so that you can start using the virtual machine before it finishes downloading. The status bar indicates the progress of the download. When you point to the VM streaming icon on the status bar, a tooltip indicates whether streaming is active and provides the URL of the Web server.

3 (Optional) To save the virtual machine so that you can use it when you do not have access to the Web server, select **VM > Save for Offline Use**.

Using this setting also allows you to pause downloading by powering off the virtual machine before streaming is finished, restart it later by powering on the virtual machine, and open the virtual machine in Workstation after you close it.

### Make a Virtual Machine Available for Streaming

You can make a virtual machine available for streaming from a Web server.

#### Prerequisites

- (Optional) To improve streaming performance, use Virtual Disk Manager (`vmware-diskmanager`) to compress the virtual disk (`.vmdk`) files for the virtual machine. See the *Virtual Disk Manager User's Guide* for more information. This guide is available on the VMware Web site.
- If the virtual machine has any snapshots, delete them.

#### Procedure

1 Configure the Web server to support HTTP keep-alive connections.

| Option | Description |
|---|---|
| **Apache HTTP Server 1.2 and later** | Turn the **KeepAlive** option on, set **MaxKeepAliveRequest** to 2000 to 5000, and set **KeepAliveTimeout** to 2000 to 5000 seconds, depending on server load. |
| **Microsoft Internet Information Services (IIS) 6.0 or later** | Set the connection timeout to a value above 300 seconds and load **HTTP Keep-Alives**. |

2 If you use a proxy server, set the proxy connection to **Keep-alive**.

3 Upload the virtual machines directory to the Web server.

Do not compress the directory. Depending on the size of the virtual machine, downloading a virtual machine in a `.zip` or `.tar` file from a Web server can take a considerable amount of time.

After it is uploaded to the Web server, users can use a URL to stream the virtual machine and start it in Workstation.

## Enable Autologon in a Windows Virtual Machine

With Autologon, you can save your login credentials and bypass the login dialog box when you power on a Windows virtual machine. The guest operating system securely stores the password.

Use the Autologon feature if you restart the guest operating system frequently and want to avoid entering your login credentials. You can also use the Autologon feature to grant users access to the guest operating system without sharing your password.

#### Prerequisites

- Verify that the guest operating system is Windows 2000 or later.
- Verify that you have an existing user account to enable Autologon. The account must be a local machine account, not a domain account.
- Verify that the latest version of VMware Tools is running in the guest operating system.
- Power on the virtual machine.

#### Procedure

1 Select the virtual machine, select **VM > Settings**.

2 On the **Options** tab, select **Autologon**.

3 Click **Enable**, type your login credentials, and click **OK**.

If you type an incorrect or expired password, you must type your login credentials when you power on the virtual machine.

4 Click **OK** to save your changes.

When you enable Autologon or change your login credentials, the Autologon settings are saved immediately. Clicking **Cancel** in the Virtual Machine Settings dialog box does not affect the changes applied to the Autologon settings.

# Stopping Virtual Machines

You can use Workstation to stop virtual machines on the host system and on remote servers. You can shut down, pause, and suspend virtual machines. You can also close virtual machines and continue running them in the background.

- Shut Down a Virtual Machine on page 47

  You can shut down a virtual machine from the **VM** menu or from the toolbar. When you use the **VM** menu, you can select a hard or soft power option.

- Closing Virtual Machines and Exiting Workstation on page 48

  You can close a virtual machine that is running on the local host system without powering it off. By default, Workstation prompts you to select an action when you close a powered-on virtual machine and when you exit Workstation while virtual machines are running on the local host system.

- Pause and Unpause a Virtual Machine on page 48

  You can pause a virtual machine multiple times for a few seconds, or up to several minutes. The pause feature is useful when a virtual machine is engaged in an lengthy, processor-intensive activity that prevents you from using the host system to do a more immediate task.

- Suspend and Resume a Virtual Machine on page 49

  You suspend a virtual machine when you want to save its current state. When you resume the virtual machine, applications that were running before the virtual machine was suspended resume in their running state and their content is unchanged.

## Shut Down a Virtual Machine

You can shut down a virtual machine from the **VM** menu or from the toolbar. When you use the **VM** menu, you can select a hard or soft power option.

You are not required to power off a virtual machine that is running on the local host system before you exit Workstation. You can exit Workstation and leave the virtual machine running in the background. See "Closing Virtual Machines and Exiting Workstation," on page 48.

When virtual machines are in a folder, you can perform batch power operations. See "Using Folders to Manage Virtual Machines," on page 74.

### Procedure

- To select a power option when you shut down the virtual machine, select the virtual machine and select **VM > Power**.

| Option | Description |
|---|---|
| **Power Off** | (Hard option) Workstation powers off the virtual machine abruptly with no consideration for work in progress. |
| **Shut Down Guest** | (Soft option) Workstation sends a shut down signal to the guest operating system. An operating system that recognizes the signal shuts down gracefully. Not all guest operating systems respond to a shutdown signal from Workstation. If the guest operating system does not respond to the signal, shut down from the guest operating system as you would a physical machine. |

- To shut down the virtual machine from the toolbar, select the virtual machine and click the stop button.

  The stop power control setting that is configured for the virtual machine determines whether Workstation performs a hard or soft power off operation. The configured behavior appears in a tooltip when you mouse over the button.

- To shut down a virtual machine that is suspended, select the virtual machine and click **VM > Power > Power Off**.

## Closing Virtual Machines and Exiting Workstation

You can close a virtual machine that is running on the local host system without powering it off. By default, Workstation prompts you to select an action when you close a powered-on virtual machine and when you exit Workstation while virtual machines are running on the local host system.

**NOTE** When you close a remote virtual machine, the virtual machine tab closes. If the virtual machine is powered on, it continues to run on the remote host.

**Table 2-1.** Close and Exit Actions

| Action | Description |
|---|---|
| **Run in Background** | Continue to run the virtual machine in the background. You can interact with the virtual machine through VNC or some other service.<br>By default, a virtual machine status icon appears in the notification area of the taskbar on the host system. When you mouse over this icon, a tooltip shows the number of virtual machines running in the background that belong to the currently logged in user. |
| **Suspend** | Suspend the virtual machine and save its current state. |
| **Power Off** | Power off the virtual machine. By default, Workstation powers off the virtual machine abruptly. The effect is the same as using the power button on a physical machine. |

You can configure Workstation preference settings so that virtual machines always run in the background and you are not prompted to select an action. You can also configure virtual machine option settings to control power off behavior.

### Configure Virtual Machines to Always Run in the Background

You can configure Workstation preference settings so that virtual machines always run in the background and you are not prompted to select an action when you close powered-on virtual machines.

#### Procedure

1 Select **Edit > Preferences**.

2 Select **Workspace** and select **Keep VMs running after Workstation closes**.

3 Click **OK** to save your changes.

## Pause and Unpause a Virtual Machine

You can pause a virtual machine multiple times for a few seconds, or up to several minutes. The pause feature is useful when a virtual machine is engaged in an lengthy, processor-intensive activity that prevents you from using the host system to do a more immediate task.

**NOTE** You cannot pause a remote virtual machine.

### Prerequisites

Familiarize yourself with the restrictions and limitations of the pause feature. See "Pause Feature Restrictions and Limitations," on page 49.

### Procedure

- To pause a virtual machine, select the virtual machine and select **VM > Pause**.

  The virtual machine display dims and a play button appears over the display. Paused virtual machines that are configured to display on more than one monitor have a play button on each monitor.

- To pause all of the powered-on virtual machines without interacting with the Workstation user interface, right-click the virtual machine status icon located in the notification area on the task bar of the host computer and select **Pause All Virtual Machines**.

- To unpause a virtual machine, click the play button on the virtual machine display or deselect **VM > Pause**.

## Pause Feature Restrictions and Limitations

The pause feature has certain restrictions and limitations.

- You cannot switch to Unity mode when a virtual machine is paused.
- When paused, a virtual machine does not send or receive network packets. If a virtual machine is paused for more than a few minutes, some network connections might be interrupted.
- If you take a snapshot when the virtual machine is paused, the virtual machine is not paused when you restore that snapshot. Similarly, if you suspend a virtual machine while it is paused, it is not paused when you resume the virtual machine.
- If you initiate soft power operations when a virtual machine is paused, those operations do not take effect until the virtual machine is unpaused.
- While a virtual machine is paused, LEDs and devices remain enabled, but device connection changes do not take effect until the virtual machine is unpaused.
- You cannot pause a remote virtual machine.

# Suspend and Resume a Virtual Machine

You suspend a virtual machine when you want to save its current state. When you resume the virtual machine, applications that were running before the virtual machine was suspended resume in their running state and their content is unchanged.

How quickly the suspend and resume operations perform depends on the how much data changed after you started the virtual machine. The first suspend operation typically takes longer than subsequent suspend operations. When you suspend a virtual machine, Workstation creates a virtual machine suspended state (`.vmss`) file in the working directory.

After you resume a virtual machine and do more work, you cannot return to the state that the virtual machine was in when you suspended it. To return to the same state repeatedly, you must take a snapshot.

When virtual machines are in a folder, you can perform batch power operations. See "Using Folders to Manage Virtual Machines," on page 74.

### Procedure

- To select a suspend option when you suspend a virtual machine, select the virtual machine and select **VM > Power**.

| Option | Description |
|---|---|
| **Suspend** | (Hard option) Workstation suspends the virtual machine and leaves it connected to the network. |
| **Suspend Guest** | (Soft option) Workstation suspends the virtual machine and disconnects it from the network. VMware Tools runs a script in the guest operating system. On Windows guests, if the virtual machine is configured to use DHCP, the script releases the IP address of the virtual machine. On Linux, FreeBSD, and Solaris guests, the script stops networking for the virtual machine. |

- To suspend a virtual machine from the toolbar, select the virtual machine and click the suspend button.

  The suspend power control setting that is configured for the virtual machine determines whether Workstation performs a hard or soft suspend operation. The configured behavior appears in a tooltip when you mouse over the button.

- To select a resume option when you resume a suspended virtual machine, select the virtual machine and select **VM > Power**.

| Option | Description |
|---|---|
| **Resume** | (Hard option) Workstation resumes the virtual machine from the suspended state. |
| **Resume Guest** | (Soft option) Workstation resumes the virtual machine from the suspended state and reconnects it to the network. |

- To resume a virtual machine from the toolbar, select the virtual machine and click the resume button.

  The suspend power control setting that is configured for the virtual machine determines whether Workstation performs a hard or soft resume operation. The configured behavior appears in a tooltip when you mouse over the button.

- To power off a suspended virtual machine, select the virtual machine and click **VM > Power > Power Off**.

## Using the Guest ACPI S1 Sleep Feature on Windows Hosts

On Windows hosts, Workstation provides experimental support for guest operating system ACPI S1 sleep. Not all guest operating systems support this feature. Common guest operating system interfaces for entering standby mode are supported.

By default, ACPI S1 sleep is implemented in Workstation as suspend. You can use the Workstation **Resume** button to wake the guest operating system.

You can implement ACPI S1 sleep as power-on suspend. The guest operating system is not fully powered down. This feature can be useful for test and development scenarios. You can wake the virtual machine through keyboard input, mouse input, or by programming the CMOS external timer.

# Transferring Files and Text

You can use the drag-and-drop feature, the copy and paste feature, shared folders, and mapped drives to transfer files and text between the host system and virtual machines and between virtual machines.

- Using the Drag-and-Drop Feature on page 51

  You can use the drag-and-drop feature to move files and directories, email attachments, plain text, formatted text, and images between the host system and virtual machines. Dragging email attachments is especially useful in Unity mode.

- Using the Copy and Paste Feature on page 52

  You can cut, copy, and paste text between virtual machines and between applications running in virtual machines.

- Using Shared Folders on page 53

  You can use shared folders to share files among virtual machines and between virtual machines and the host system. The directories that you add as shared folders can be on the host system, or they can be network directories that are accessible from the host computer.

- Mapping a Virtual Disk to the Host System on page 59

  Instead of using shared folders or copying data between a virtual machine and the host system, you can map a virtual disk to the host system. In this case, you map a virtual disk in the host file system as a separate mapped drive. Using a mapped drive lets you connect to the virtual disk without going into a virtual machine.

## Using the Drag-and-Drop Feature

You can use the drag-and-drop feature to move files and directories, email attachments, plain text, formatted text, and images between the host system and virtual machines. Dragging email attachments is especially useful in Unity mode.

You can drag files or directories between the following locations.

- File managers, such as Windows Explorer, on the host system and virtual machines.
- A file manager to an application that supports drag-and-drop.
- Applications, such as zip file managers, which support drag-and-drop extraction of individual files.
- Different virtual machines.

When you drag a file or folder between the host and a virtual machine, Workstation copies the file or folder to the location where you drop it. For example, if you drop a file on the desktop icon of a word processor, the word processor opens a copy of the original file. The original file does not include changes that you make to the copy.

Initially, the application opens a copy of the file that is stored in the temp directory. On Windows, the temp directory is specified in the `%TEMP%` environment variable. On Linux and Solaris, the temp directory is `/tmp/VMwareDnD`. Save the file in a different directory to protect changes that you make.

### Drag-and-Drop Requirements and Restrictions

The drag-and-drop feature has certain requirements and restrictions.

- You must install VMware Tools in a virtual machine to use the drag-and-drop feature.
- The drag-and-drop feature requires Linux hosts and guests to run X Windows and Solaris 10 guests to run an Xorg X server and JDS/Gnome.
- You can drag images between applications on Windows hosts and applications on Windows guests only. Dragging images is not supported for Linux hosts or guests.

- You can drag files and directories, email attachments, plain text, and formatted text between Linux and Windows hosts and Linux, Windows, and Solaris 10 guests only.
- Dragging email attachments is restricted to images or files smaller than 4MB.
- Dragging plain text and formatted text (including the formatting) is restricted to amounts less than 4MB.
- Dragging text is restricted to text in languages that can be represented by Unicode characters.
- Workstation uses the PNG format to encode images that are dragged. Dragging images is restricted to images smaller than 4MB after conversion to PNG format.
- On Windows 95 and Windows 98 guests, the drag-and-drop feature is supported only for files and directories.

### Disable the Drag-and-Drop Feature

The drag-and-drop feature is enabled by default when you create a virtual machine in Workstation. To prevent dragging and dropping between a virtual machine and the host system, disable the drag-and-drop feature.

**NOTE** You cannot enable or disable the drag-and-drop feature for a shared or remote virtual machine.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Guest Isolation**.

3 Deselect **Enable drag and drop**.

4 Click **OK** to save your changes.

## Using the Copy and Paste Feature

You can cut, copy, and paste text between virtual machines and between applications running in virtual machines.

You can also cut, copy, and paste images, plain text, formatted text, and email attachments between applications running on the host system and applications running in virtual machines.

Copying and pasting email attachments is especially useful in Unity mode. Use the normal hot keys or menu choices to cut or copy and paste.

### Copy and Paste Requirements and Restrictions

The copy and paste feature has certain requirements and restrictions.

- You must install VMware Tools in a virtual machine to use the copy and paste feature.
- The copy and paste feature works with Linux and Windows hosts and Linux, Windows, and Solaris 10 guests only.
- The copy and paste feature requires Linux hosts and guests to run X Windows and Solaris 10 guests to run an Xorg X server and JDS/Gnome.
- Copying and pasting email attachments is restricted to images or files smaller than 4MB.
- Copying and pasting plain text and formatted text (including the formatting) is restricted to amounts less than 4MB.
- Copying and pasting text is restricted to text in languages that can be represented by Unicode characters.

- Workstation uses the PNG format to encode images that are copied and pasted. Copying and pasting images is restricted to images smaller than 4MB after conversion to PNG format.
- You cannot copy and paste files between virtual machines.
- On Windows 95 and Windows 98 guests, copying and pasting is restricted to plain text in amounts less than 64KB.

### Disable the Copy and Paste Feature

The copy and paste feature is enabled by default when you create a virtual machine in Workstation. To prevent copying and pasting between a virtual machine and the host system, disable the copy and paste feature.

**NOTE** You cannot enable or disable the copy and paste feature for a shared or remote virtual machine.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Guest Isolation**.

3 Deselect **Enable copy and paste**.

4 Click **OK** to save your changes.

## Using Shared Folders

You can use shared folders to share files among virtual machines and between virtual machines and the host system. The directories that you add as shared folders can be on the host system, or they can be network directories that are accessible from the host computer.

**IMPORTANT** You cannot open a file in a shared folder from more than one application at a time. For example, do not open the same file in an application on the host operating system and in another application in the guest operating system. If one of the applications writes to the file, data might be corrupted.

- Guest Operating Systems that Support Shared Folders on page 54

  To use shared folders, a virtual machine must have a supported guest operating system.
- Enable a Shared Folder for a Virtual Machine on page 54

  You can enable folder sharing for a specific virtual machine. To set up a folder for sharing between virtual machines, you must configure each virtual machine to use the same directory on the host system or network share.
- Enable Shared Folders for Virtual Machines Created By Other Users on page 55

  If a shared folder is not created by the user who powers on the virtual machine, it is disabled by default. This is a security precaution.
- View Shared Folders in a Windows Guest on page 56

  In a Windows guest operating system, you can view shared folders by using desktop icons.
- Mounting Shared Folders in a Linux Guest on page 56

  After you have enabled a shared folder, you can mount one or more directories or subdirectories in the shared folder to any location in the file system in addition to the default location of `/mnt/hgfs`.
- Change Shared Folder Properties on page 57

  After you create a shared folder, you can change the folder name, the host path, and other attributes.
- Change the Folders That a Virtual Machine Can Share on page 58

  You can change the folders that a specific virtual machine is allowed to share.

- Disable Folder Sharing for a Virtual Machine on page 58
  You can disable folder sharing for a specific virtual machine.

## Guest Operating Systems that Support Shared Folders

To use shared folders, a virtual machine must have a supported guest operating system.

The following guest operating systems support shared folders.

- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT 4.0
- Windows Vista
- Windows 7
- Linux with a kernel version of 2.6 or later
- Solaris x86 10
- Solaris x86 10 Update 1 and later

## Enable a Shared Folder for a Virtual Machine

You can enable folder sharing for a specific virtual machine. To set up a folder for sharing between virtual machines, you must configure each virtual machine to use the same directory on the host system or network share.

**NOTE** You cannot enable a shared folder for a shared or remote virtual machine.

### Prerequisites

- Verify that the virtual machines use a guest operating system that supports shared folders. See "Guest Operating Systems that Support Shared Folders," on page 54.
- Verify that the latest version of VMware Tools is installed in the guest operating system.
- Verify that permission settings on the host system allow access to files in the shared folders. For example, if you are running Workstation as a user named User, the virtual machine can read and write files in the shared folder only if User has permission to read and write them.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Shared Folders**.

3 Select a folder sharing option.

| Option | Description |
|---|---|
| **Always enabled** | Keep folder sharing enabled, even when the virtual machine is shut down, suspended, or powered off. |
| **Enabled until next power off or suspend** | Enable folder sharing temporarily, until you power off, suspend, or shut down the virtual machine. If you restart the virtual machine, shared folders remain enabled. This setting is available only when the virtual machine is powered on. |

4 (Optional) To map a drive to the `Shared Folders` directory, select **Map as a network drive in Windows guests**.

This directory contains all of the shared folders that you enable. Workstation selects the drive letter.

5 Click **Add** to add a shared folder.

On Windows hosts, the Add Shared Folder wizard starts. On Linux hosts, the Shared Folder Properties dialog box opens.

6 Type the path on the host system to the directory to share.

If you specify a directory on a network share, such as `D:\share`, Workstation always attempts to use that path. If the directory is later connected to the host on a different drive letter, Workstation cannot locate the shared folder.

7 Specify the name of the shared folder as it should appear inside the virtual machine.

Characters that the guest operating system considers illegal in a share name appear differently when viewed inside the guest. For example, if you use an asterisk in a share name, you see %002A instead of * in the share name on the guest. Illegal characters are converted to their ASCII hexadecimal value.

8 Select shared folder attributes.

| Option | Description |
|---|---|
| **Enable this share** | Enable the shared folder. Deselect this option to disable a shared folder without deleting it from the virtual machine configuration. |
| **Read-only** | Make the shared folder read-only. When this property is selected, the virtual machine can view and copy files from the shared folder, but it cannot add, change, or remove files. Access to files in the shared folder is also governed by permission settings on the host computer. |

9 Click **Finish** to add the shared folder.

The shared folder appears in the Folders list. The check box next to folder name indicates that the folder is being shared. You can deselect this check box to disable sharing for the folder.

10 Click **OK** to save your changes.

### What to do next

View the shared folder. On Linux guests, shared folders appear under `/mnt/hgfs`. On Solaris guests, shared folders appear under `/hgfs`. To view shared folders on a Windows guest, see "View Shared Folders in a Windows Guest," on page 56.

## Enable Shared Folders for Virtual Machines Created By Other Users

If a shared folder is not created by the user who powers on the virtual machine, it is disabled by default. This is a security precaution.

Folder sharing is also disabled by default for Workstation 4 and 5.x virtual machines, regardless of who creates the folder.

**IMPORTANT** Enabling shared folders on all virtual machines can pose a security risk because a shared folder might enable existing programs inside the virtual machine to access the host file system without your knowledge.

### Procedure

1 Select **Edit > Preferences**.

2 Select **Workspace** and select **Enable all shared folders by default**.

This setting applies to shared folders on all virtual machines that are created by other users.

## View Shared Folders in a Windows Guest

In a Windows guest operating system, you can view shared folders by using desktop icons.

NOTE If the guest operating system has VMware Tools from Workstation 4.0, shared folders appear as folders on a designated drive letter.

### Procedure

- Depending on the Windows operating system version, look for **VMware Shared Folders** in **My Network Places**, **Network Neighborhood**, or **Network**.
- If you mapped the shared folder as a network drive, open **My Computer** and look for **Shared Folders on 'vmware-host'** under **Network Drives**.
- To view a specific shared folder, go directly to the folder by using the UNC path `\\vmware-host\Shared Folders\`*`shared_folder_name`*.

## Mounting Shared Folders in a Linux Guest

After you have enabled a shared folder, you can mount one or more directories or subdirectories in the shared folder to any location in the file system in addition to the default location of `/mnt/hgfs`.

Use the `mount` command to mount all shares, one share, or a subdirectory within a share to any location in the file system.

**Table 2-2.** Mount Command Syntax

| Command | Description |
|---|---|
| `mount -t vmhgfs .host:/ /home/user1/shares` | Mounts all shares to `/home/user1/shares` |
| `mount -t vmhgfs .host:/foo /tmp/foo` | Mounts the share named `foo` to `/tmp/foo` |
| `mount -t vmhgfs .host:/foo/bar /var/lib/bar` | Mounts the subdirectory `bar` within the share `foo` to `/var/lib/bar` |

You can use VMware-specific options in addition to the standard `mount` syntax. For usage information for the host-guest file system options, type the command **`/sbin/mount.vmhgfs -h`**.

When you install VMware Tools, an entry is made to `etc/fstab` to specify the location of shared folders. You can edit this file to change or add entries. For example, to auto-mount at startup, edit `/etc/fstab` and add the line:

```
.host:/ /mnt/hgfs vmhgfs defaults 0 0
```

The VMware Tools services script loads a driver that performs the mount. If the mount fails, a message appears regarding mounting HGFS shares.

NOTE The mount can fail if shared folders are disabled or if the share does not exist. You are not prompted to run the VMware Tools `vmware-config-tools.pl` configuration program again.

### Optimizing Read and Write Access to Shared Files on Linux

Host-guest file sharing is integrated with the guest page cache. Files in shared folders are cached for reading and can be written to asynchronously.

Files that are being actively written to from the guest do not experience read caching benefits. To improve performance, you can use the `mount` command time-to-live (`ttl`) option to specify the interval that the host-guest file system (`hgfs`) driver uses for validating file attributes.

For example, to validate attributes every 3 seconds instead of every 1 second, which is the default, use the following command.

```
mount –o ttl=3 –t vmhgfs .host:/sharemountpoint
```

NOTE Lengthening the interval involves some risk. If a process in the host modifies file attributes, the guest operating system might not get the modifications as quickly and the file can become corrupted.

#### Using Permissions to Restrict Access to Shared Files in a Linux Guest

You can use permissions to restrict access to the files in a shared folder on a Linux guest operating system.

On a Linux host, if you create files that you want to share with a Linux guest operating system, the file permissions shown on the guest operating system are the same as the permissions on the host system. You can use the `fmask` and `dmask` commands to mask permissions bits for files and directories.

If you create files on a Windows host system that you want to share with a Linux guest operating system, read-only files are displayed as having read and execute permission for everyone and other files are shown as fully writable by everyone.

If you use a Linux guest operating system to create files for which you want to restrict permissions, use the `mount` program with the following options in the guest operating system.

- `uid`
- `gid`
- `fmask`
- `dmask`
- `ro` (read only)
- `rw` (read-write)

`rw` is the default.

If you are using a virtual machine that was created with the Windows version of Workstation, or a previous release of the Linux version of Workstation, you can change the owner permissions only.

## Change Shared Folder Properties

After you create a shared folder, you can change the folder name, the host path, and other attributes.

#### Prerequisites

Create a shared folder. See "Enable a Shared Folder for a Virtual Machine," on page 54.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Shared Folders**.

3 Select the shared folder in the folders list and click **Properties**.

4 To change the name of the shared folder as it appears inside the virtual machine, type the new name in the **Name** text box.

Characters that the guest operating system considers illegal in a share name appear differently when viewed inside the guest. For example, if you use an asterisk in a share name, you see %002A instead of * in the share name on the guest. Illegal characters are converted to their ASCII hexadecimal value.

5 To change the host path for the shared folder, browse to or type the new path in the **Host path** text box.

If you specify a directory on a network share, such as `D:\share`, Workstation always attempts to use that path. If the directory is later connected to the host on a different drive letter, Workstation cannot locate the shared folder.

6 To change an attribute for the shared folder, select or deselect the attribute.

| Option | Description |
|---|---|
| **Enabled** | Enable the shared folder. Deselect this option to disable a shared folder without deleting it from the virtual machine configuration. |
| **Read-only** | Make the shared folder read-only. When this property is selected, the virtual machine can view and copy files from the shared folder, but it cannot add, change, or remove files. Access to files in the shared folder is also governed by permission settings on the host computer. |

7 Click **OK** to save your changes.

## Change the Folders That a Virtual Machine Can Share

You can change the folders that a specific virtual machine is allowed to share.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Shared Folders**.

3 In the folders list, select the check boxes next to the folders to share and deselect the check boxes next to the folders to disable.

4 Click **OK** to save your changes.

## Disable Folder Sharing for a Virtual Machine

You can disable folder sharing for a specific virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Shared Folders**.

3 Select **Disabled** to disable folder sharing.

4 Click **OK** to save your changes.

# Mapping a Virtual Disk to the Host System

Instead of using shared folders or copying data between a virtual machine and the host system, you can map a virtual disk to the host system. In this case, you map a virtual disk in the host file system as a separate mapped drive. Using a mapped drive lets you connect to the virtual disk without going into a virtual machine.

## Map or Mount a Virtual Disk to a Drive on the Host System

When you map a virtual disk and its associated volume to a drive on the host system, you can connect to the virtual disk without opening a virtual machine.

After you map the virtual disk to a drive on the host system, you cannot power on any virtual machine that uses the disk until you disconnect the disk from the host system.

**NOTE** You cannot map a virtual hard disk for a shared or remote virtual machine.

**IMPORTANT** If you mount a virtual disk that has a snapshot and then write to the disk, you can irreparably damage a snapshot or linked clone created from the virtual machine.

### Prerequisites

- Power off all virtual machines that use the virtual disk.
- Verify that the virtual disk (`.vmdk`) files on the virtual disk are not compressed and do not have read-only permissions.
- On a Windows host, verify that the volume is formatted with FAT (12/16/32) or NTFS. Only FAT (12/16/32) and NTFS formatting is supported. If the virtual disk has mixed partitions, for example, one partition is formatted with a Linux operating system and another partition is formatted with a Windows operating system, you can map the Windows partition only.
- Verify that the virtual disk is unencrypted. You cannot map or mount encrypted disks.

### Procedure

1 Mount the virtual disk to a drive on the host system.

| Option | Description |
|---|---|
| **Windows host** | Select **File > Map Virtual Disks**. |
| **Linux host** | Select **File > Mount Virtual Disks**. |

2 Map or mount the virtual disk.

| Option | Description |
|---|---|
| **Windows host** | In the Map or Disconnect Virtual Disks dialog box, click **Map**. |
| **Linux host** | In the Mount or Unmount Virtual Disks dialog box, click **Mount Disk**. |

3 (Optional) You can also map a virtual disk from Windows Explorer.

   a Open Explorer and browse to the `.vmdk` file you want to map.

   b Right-click the `.vmdk` file and select **Map Virtual Disk**.

   The menu also allows you to map the first volume of the `.vmdk` file to a drive immediately. If you select that option, no further configurations are needed.

4 On a Windows host, leave the check box **Open file in read-only mode** selected in the Map Virtual Disk dialog box.

   This setting prevents you from accidentally writing data to a virtual disk that might be the parent of a snapshot or linked clone. Writing to such a disk might make the snapshot or linked clone unusable.

5 On a Linux host, select the **Mount in read-only mode** check box in the Mount Disk dialog box.

   This setting prevents you from accidentally writing data to a virtual disk that might be the parent of a snapshot or linked clone. Writing to such a disk might make the snapshot or linked clone unusable.

6 Browse to a virtual disk (`.vmdk`) file, select it, and click **Open**.

7 Select the volume to map or mount and select an unused drive letter on the host system.

8 (Optional) On a Windows host, if you do not want the drive to open in Windows Explorer after it is mapped, deselect the **Open drive in Windows Explorer after mapping** check box.

9 Click **OK** or **Mount**.

   The drive appears on the host system. You can read from or write to files on the mapped virtual disk on the host system.

10 (Optional) View the mapped or mounted drive.

| Option | Description |
|---|---|
| **Windows host** | Select **File > Map Virtual Disks**. A list of mapped drives displays. |
| **Linux host** | Select **File > Mount Virtual Disks**. A list of mounted drives displays. |

### Disconnect a Virtual Disk from the Host System

To use a virtual disk from a virtual machine after it has been mapped or mounted on the host system, you must disconnect it from the host system.

On Windows hosts, you must use Workstation to disconnect the drive from the host system. The mapped drive letter does not appear in the list of network drives when you use the Windows **Disconnect Network Drive** command.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Hard Disk**, click **Utilities**, and select **Disconnect**.

You can now power on any virtual machine that uses this disk.

## Add a Host Printer to a Virtual Machine

You can print from a virtual machine to any printer available to the host computer without having to install additional drivers in the virtual machine.

The Workstation printer feature uses ThinPrint technology to replicate the host system printer mapping in the virtual machine. When you enable the virtual machine printer, Workstation configures a virtual serial port to communicate with the host printers.

**NOTE** You cannot add a printer to a shared or remote virtual machine.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Add**.

3 In the Add Hardware wizard, select **Printer** and **Finish**.

The default device setting is to connect the virtual machine printer when the virtual machine is powered on.

#### What to do next

In a Print window, when you attempt to select a printer in Windows 7 virtual machines, you might see only the default printer, even though other printers are available. To see the other printers, right-click the default printer and point to **Printer properties**.

# Using Removable Devices in Virtual Machines

You can use removable devices such as floppy drives, DVD and CD-ROM drives, USB devices, and smart card readers in virtual machines.

Some devices cannot be used by the host system and a guest operating system, or by multiple guest operating systems, simultaneously.

For example, if the host system is using a floppy drive, you must connect the floppy drive to the virtual machine before you can use it in the virtual machine. To use the floppy drive on the host again, you must disconnect it from the virtual machine. By default, a floppy drive is not connected when a virtual machine powers on.

## Use a Removable Device in a Virtual Machine

You can connect and disconnect removable devices in a virtual machine. You can also change the settings for a removable device by modifying virtual machine settings.

#### Prerequisites

- Power on the virtual machine.
- If you are connecting or disconnecting a USB device, familiarize yourself with the way Workstation handles USB devices. See "Connecting USB Devices to Virtual Machines," on page 62.
- If you are connecting or disconnecting a USB device on a Linux host and the USB device file system is not located in `/proc/bus/usb`, mount the USB file system to that location. See "Mount the USB File System on a Linux Host," on page 63.

#### Procedure

- To connect a removable device, select the virtual machine, select **VM > Removable Devices**, select the device, and select **Connect**.

  If the device is connected to the host system through a USB hub, the virtual machine sees only the USB device, not the hub.

  A check mark appears next to the name of the device when the device is connected to the virtual machine and a device icon appears on the virtual machine taskbar.
- To change the settings for a removable device, select **VM > Removable Devices**, select the device, and select **Settings**.
- To disconnect a removable device, select the virtual machine, select **VM > Removable Devices**, select the device, and select **Disconnect**.

  You can also disconnect the device by clicking or right-clicking the device icon on the virtual machine taskbar. Using the taskbar icon is especially useful if you run the virtual machine in full screen mode.

## Connecting USB Devices to Virtual Machines

When a virtual machine is running, its window is the active window. If you plug a USB device into the host system, the device connects to the virtual machine instead of the host by default. If a USB device connected to the host system does not connect to a virtual machine at power on, you must manually connect the device to the virtual machine.

When you connect a USB device to a virtual machine, Workstation retains the connection to the affected port on the host system. You can suspend or power off the virtual machine, or unplug the device. When you plug in the device again or resume the virtual machine, Workstation reconnects the device. Workstation retains the connection by writing an autoconnect entry to the virtual machine configuration (`.vmx`) file.

If Workstation cannot reconnect to the device, for example, because you disconnected the device, the device is removed and Workstation displays a message to indicate that it cannot connect to the device. You can connect to the device manually if it is still available.

Follow the device manufacturer's procedures for unplugging the device from the host computer when you physically unplug the device, move the device from host system to a virtual machine, move the device between virtual machines, or move the device from a virtual machine to the host computer. Following these procedures is especially important for data storage devices, such as zip drives. If you move a data storage device too soon after saving a file and the operating system did not actually write the data to the disk, you can lose data.

- Installing USB Drivers on Windows Hosts on page 62

  When a particular USB device is connected to a virtual machine for the first time, the host detects it as a new device named VMware USB Device and installs the appropriate VMware driver.

- Disable Automatic Connection of USB Devices on page 63

  You can disable the autoconnect feature if you do not want USB devices to connect to a virtual machine when you power it on.

- Mount the USB File System on a Linux Host on page 63

  On Linux hosts, Workstation uses the USB device file system to connect to USB devices. If the USB device file system is not located in `/proc/bus/usb`, you must mount the USB file system to that location.

- Connect USB HIDs to a Virtual Machine on page 63

  To connect USB human interface devices (HIDs) to a virtual machine, you must configure the virtual machine to show all USB input devices in the **Removable Devices** menu.

- Install a PDA Driver and Synchronize With a Virtual Machine on page 64

  To install a PDA driver in a virtual machine, you must synchronize the PDA with the virtual machine.

### Installing USB Drivers on Windows Hosts

When a particular USB device is connected to a virtual machine for the first time, the host detects it as a new device named VMware USB Device and installs the appropriate VMware driver.

The Windows operating system prompts you to run the Microsoft Windows Found New Hardware wizard. Select the default action to install the software automatically. After the software is installed, the guest operating system detects the USB device and searches for a suitable driver.

## Disable Automatic Connection of USB Devices

You can disable the autoconnect feature if you do not want USB devices to connect to a virtual machine when you power it on.

### Prerequisites

Power off the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **USB Controller**.

3 Deselect **Automatically connect new USB devices** to disable automatic connection of USB devices.

4 Click **OK** to save your changes.

## Mount the USB File System on a Linux Host

On Linux hosts, Workstation uses the USB device file system to connect to USB devices. If the USB device file system is not located in `/proc/bus/usb`, you must mount the USB file system to that location.

**IMPORTANT** Do not attempt to add a USB drive device node directory, for example, `/dev/sda`, to the virtual machine as a hard disk.

### Prerequisites

Verify that you have root access to the host system.

### Procedure

1 As root, mount the USB file system.

```
mount –t usbfs none /proc/bus/usb
```

2 Connect the USB device to the host system.

## Connect USB HIDs to a Virtual Machine

To connect USB human interface devices (HIDs) to a virtual machine, you must configure the virtual machine to show all USB input devices in the **Removable Devices** menu.

By default, USB HIDs, such as USB 1.1 and 2.0 mouse and keyboard devices, do not appear in the **Removable Devices** menu in a virtual machine, even though they are plugged in to USB ports on the host system.

An HID that is connected to a virtual machine is not available to the host system.

**NOTE** You cannot configure a shared or remote virtual machine to show all USB input devices.

### Prerequisites

- Power off the virtual machine.
- If you are using a KVM switch for a mouse or keyboard, disable automatic connection of USB devices. See "Disable Automatic Connection of USB Devices," on page 63.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **USB Controller**.

3 Select **Show all USB input devices**.

This option allows users to use special USB HIDs inside the virtual machine.

4 Click **OK** to save your changes.

5 Power on the virtual machine.

HIDs appear in the **Removable Devices** menu.

### Install a PDA Driver and Synchronize With a Virtual Machine

To install a PDA driver in a virtual machine, you must synchronize the PDA with the virtual machine.

#### Procedure

1 Connect the PDA to the host system and synchronize it with the host system.

The PDA driver should begin installing in the virtual machine.

2 Allow the virtual machine to install the PDA driver.

3 If connection warning messages appear, dismiss them.

4 If the PDA disconnects from the host system before the virtual machine can synchronize with it, synchronize the PDA with the host system again.

The total time required to load the VMware USB device driver in the host system and install the PDA driver in the virtual machine might exceed the device connection timeout value. A second synchronization attempt usually succeeds.

## Troubleshooting USB Device Control Sharing

Only the host system or the virtual machine can have control of a particular USB device at any one time. Device control operates differently, depending on whether the host system is a Linux or a Windows computer.

When you connect a device to a virtual machine, it is disconnected from the host system or from the virtual machine that previously had control of the device. When you disconnect a device from a virtual machine, it is returned to the host system.

Under some circumstances, if a USB storage device is in use on the host system, for example, one or more files stored on the device are open on the host, an error appears in the virtual machine when you try to connect to the device. You must let the host system complete its operation or close any application connected to the device on the host system and connect to the device in the virtual machine again.

On Windows XP and Windows Server 2003 host systems, a message might appear that says the device can be removed safely when you connect a USB network or storage device to a virtual machine. This is normal behavior and you can dismiss the dialog box, but do not remove the device from the physical computer. If the network or storage device does not disconnect from the host system, use the appropriate system tray icon to disconnect it. On Windows XP and Windows Server 2003, the system tray icon is called **Safely Remove Hardware**.

### Troubleshoot USB Device Control Issues on a Linux Host

You have problems connecting or disconnecting USB devices on a Linux host system.

#### Problem

You are prompted to disconnect the driver on the host system when you connect a USB device to the virtual machine or disconnecting the device fails.

### Cause

On Linux host systems, guest operating systems can use devices that are not claimed by a host operating system driver. A related issue sometimes affects devices that rely on automatic connection, such as PDAs. Occasionally, even if you successfully use autoconnection to connect the device to the virtual machine, you might experience problems with the connection to the device.

### Solution

1 If you have problems with autoconnection, perform these steps.

   a Select the virtual machine and select **VM > Removable Devices** to disconnect and reconnect the device.

   b If the problem persists, unplug the device and plug it in again.

   c If a warning message indicates that the device is in use, disable the device in the `hotplug` configuration files in the `/etc/hotplug` directory.

   The documentation for the Linux distribution contains information on editing these configuration files.

2 If disconnection fails, either disable the driver or unload the driver manually.

| Option | Description |
|---|---|
| **Disable the driver** | If the driver was automatically loaded by hotplug, disable it in the hotplug configuration files in the `/etc/hotplug` directory. See the documentation for your Linux distribution for information on editing these configuration files. |
| **Unload the driver manually** | Become root (`su –`) and use the `rmmod` command. |

## Using Smart Cards in Virtual Machines

Virtual machines can connect to smart card readers that interface to serial ports, parallel ports, USB ports, PCMCIA slots, and PCI slots. A virtual machine considers a smart card reader to be a type of USB device.

A smart card is a plastic card that has an embedded computer chip. Many government agencies and large enterprises use smart cards to send secure communication, digitally sign documents, and authenticate users who access their computer networks. Users plug a smart card reader into their computer and insert their smart card in the reader. They are then prompted for their PIN to log in.

You can select a smart card reader from the **Removable Devices** menu in a virtual machine. A smart card can be shared between virtual machines, or between the host system and one or more virtual machines. Sharing is enabled by default.

When you plug a smart card reader into the host system, the reader appears as two separate USB devices in Workstation. This is because you can use smart cards in one of two mutually exclusive modes.

**Shared mode** (Recommended) The smart card reader device is available as **Shared** *smart_card_reader_model* in the **Removable Devices** menu. In Windows XP guest operating systems, the shared reader appears as **USB Smart Card Reader** after it is connected to the virtual machine. In Windows Vista and

Windows 7 guest operating systems, the generic smart card reader device name appears under the Windows Device Manager list. The smart card reader can be shared among applications on the host system and among applications in different guest operating systems.

**USB passthrough mode** The smart card reader device is available as *smart_card_reader_model* in the **Removable Devices** menu. In USB passthrough mode, a single virtual machine directly controls the physical smart card reader. A USB passthrough smart card reader cannot be used by applications on the host system or by applications in other virtual machines. You should use USB passthrough mode only if connection in shared mode does not work well for your scenario. You might need to install the driver provided by the manufacturer to use USB passthrough mode.

You can use smart cards with Windows operating systems and most Linux distributions. VMware provides full smart card support for Windows virtual machines running on Linux hosts. Using smart cards in Linux typically requires third-party software to effectively authenticate to a domain or enable secure communications.

**NOTE** Although smart cards should work with common Linux browsers, email applications, and directory services, these products have not been tested or certified by VMware.

## Use a Smart Card in a Virtual Machine

You can configure a virtual machine to use the smart card reader on the host system.

### Prerequisites

- On a Windows host, start the `SCardSvr.exe` service.
- On a Linux host, verify that the `libpcsclite` library is installed and that the `pcscd` daemon is running.
- Verify that the virtual machine has a USB controller. A USB controller is required, regardless of whether the smart card reader is a USB device. A USB controller is added by default when you create a virtual machine.
- Connect the smart card reader to the host system.
- Start the virtual machine

### Procedure

- To connect the smart card reader to the virtual machine, select the virtual machine and select **VM > Removable Devices > Shared <smart_card_reader_model> > Connect**.

  If the smart card reader is a USB device, two items appear for it in the menu. Both items use the model name of the reader, but one item name begins with Shared.

- To disconnect the smart card reader from the virtual machine, select **VM > Removable Devices > Shared <smart_card_reader_model> > Disconnect**.
- To remove the smart card from the virtual machine, select **VM > Removable Devices > Shared <smart_card_reader_model> > Remove Smart Card**.

  The smart card is removed from the virtual machine, but it remains connected on the host system. If the smart card is physically removed from the smart card reader, this option is disabled.

- To insert the smart card to the virtual machine, select **VM > Removable Devices > Shared <smart_card_reader_model> > Insert Smart Card**.

  If the smart card is physically inserted in the smart card reader, the smart card is also inserted in the virtual machine.

## Disable Smart Card Sharing

By default, you can share a smart card between virtual machines or between the host system and one or more virtual machines. You might want to disable smart card sharing if you are using a PCMCIA smart card reader, deploying virtual machines for enterprise use and do not want to support drivers for various smart card readers, or the host system has drivers but the virtual machines do not.

The setting that controls smart card sharing is located in the Workstation global configuration file.

### Procedure

1 Find the global configuration file on the host system.

| Operating System | Location |
|---|---|
| **Most Windows hosts** | `C:\Documents and Settings\All Users\Application Data\VMware\VMware Workstation\config.ini` |
| **Windows Vista and Windows 7 hosts** | `C:\ProgramData\VMware\VMware Workstation\config.ini` |
| **Linux hosts** | `/etc/vmware/config` |

2 If the global configuration file does not yet exist on the host system, select **Edit > Preferences** and change at least one Workstation preference settings.

Workstation creates the global configuration file when you change Workstation preference settings.

3 Open the global configuration file in a text editor and set the `usb.ccid.useSharedMode` property to `FALSE`.

For example: **`usb.ccid.useSharedMode = "FALSE"`**

4 Save and close the global configuration file.

5 Set permissions on the global configuration file so that other users cannot change it.

## Switch to a Virtual Smart Card Reader on a Linux Host

Because of the way smart card reader functionality is implemented on Linux hosts, you must exit Workstation and restart the `pcscd` daemon on the host system before you can switch from the non-virtual smart card reader to the virtual smart card reader.

### Procedure

1 Select the virtual machine, select **VM > Removable Devices**, select the smart card reader, and select **Disconnect**.

2 Power off the virtual machine and exit Workstation.

3 Physically disconnect the smart card reader from the host system.

4 Restart the `pcscd` daemon on the host system.

5 Physically connect the smart card reader to the host system.

6 Start Workstation and start the virtual machine.

7 Select the virtual machine, select **VM > Removable Devices**, select the smart card reader, and select **Connect**.

# Changing the Virtual Machine Display

You can change the way Workstation displays virtual machines and virtual machine applications. You can use full screen mode to make the virtual machine display fill the screen and use multiple monitors, and you can use Unity mode to display applications directly on the host system desktop.

You can also match the Workstation console with the guest operating system display size.

- Use Full Screen Mode on page 68

  In full screen mode, the virtual machine display fills the screen and you cannot see the borders of the Workstation window.

- Use Exclusive Mode on page 69

  Like full screen mode, exclusive mode causes the Workstation virtual machine display to fill the screen. You might want to use exclusive mode to run graphics-intensive applications, such as games, in full screen mode.

- Use Unity Mode on page 70

  You can switch virtual machines that have Linux or Windows 2000 or later guest operating systems to Unity mode to display applications directly on the host system desktop.

- Use Multiple Monitors for One Virtual Machine on page 71

  If the host system has multiple monitors, you can configure a virtual machine to use multiple monitors. You can use the multiple-monitor feature when the virtual machine is in full screen mode.

- Use Multiple Monitors for Multiple Virtual Machines on page 72

  If the host system has multiple monitors, you can run a different virtual machine on each monitor.

- Fit the Workstation Console to the Guest Operating System Display on page 73

  You can control the size of the virtual machine display and match the Workstation console with the display size of the guest operating system for an active virtual machine.

## Use Full Screen Mode

In full screen mode, the virtual machine display fills the screen and you cannot see the borders of the Workstation window.

You can configure the guest operating system to report battery information. This feature is useful when you run a virtual machine in full screen mode on a laptop. See "Report Battery Information in the Guest," on page 69.

### Prerequisites

- Verify that the latest version of VMware Tools is installed in the guest operating system.
- Verify that the guest operating system display mode is larger than the host system display mode. If the guest operating system display mode is smaller than the host system display mode, you might not be able to enter full screen mode. If you cannot enter full screen mode, add the line `mks.maxRefreshRate=1000` to the virtual machine configuration (`.vmx`) file.
- Power on the virtual machine.
- If you have multiple monitors, move the Workstation window onto the monitor to use for full screen mode.

### Procedure

- To enter full screen mode, select the virtual machine and select **View > Full Screen**.

- Press Ctrl+Alt+right arrow to switch to the next powered-on virtual machine and Ctrl+Alt+left arrow to switch to the previous powered-on virtual machine.
- When in full screen mode, you can also use the tabs on the full screen toolbar to switch between powered-on virtual machines.
- To hide the full screen toolbar while you are using full screen mode, click the push pin icon on the full screen toolbar and move the mouse pointer off of the toolbar.

  The toolbar is unpinned and slides up to the top of the monitor and disappears.
- To show the full screen toolbar after it has been hidden, point to the top of the screen until the toolbar appears and click the push pin icon.
- To exit full screen mode, on the full screen toolbar select **View > Full Screen**, and deselect **Full Screen**.

### Report Battery Information in the Guest

If you run a virtual machine on a laptop in full screen mode, configure the option to report battery information in the guest so that you can determine when the battery is running low.

#### Prerequisites

Power off the virtual machine.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Power**.

3 Select **Report battery information to guest**.

4 Click **OK** to save your changes.

## Use Exclusive Mode

Like full screen mode, exclusive mode causes the Workstation virtual machine display to fill the screen. You might want to use exclusive mode to run graphics-intensive applications, such as games, in full screen mode.

Exclusive mode has certain advantages and limitations.

- The full screen toolbar is not engaged when you move the mouse to the top of the screen. To configure virtual machine settings, you must exit exclusive mode.
- When input is grabbed by the virtual machine, only the ungrab shortcut is respected. You can change the ungrab shortcut to reduce the chance of unintentionally pressing it.
- On a Windows host, exclusive mode does not use multiple monitors.

#### Prerequisites

- Verify that the latest version of VMware Tools is installed in the guest operating system.
- Power on the virtual machine.
- If you have multiple monitors, move the Workstation window onto the monitor to use for exclusive mode.
- Enter full screen mode. See "Use Full Screen Mode," on page 68.

#### Procedure

1 Enter full screen mode.

2 Select **View > Exclusive Mode** from the full screen toolbar.

### What to do next

To exit exclusive mode, press Ctrl+Alt.

On a Windows or Linux host, pressing Ctrl+Alt returns you to full screen mode.

## Use Unity Mode

You can switch virtual machines that have Linux or Windows 2000 or later guest operating systems to Unity mode to display applications directly on the host system desktop.

In Unity mode, virtual machine applications appear on the host system desktop, you can use the virtual machine **Start** or **Applications** menu from the host system, and the virtual machine console view is hidden. Items for open virtual machine applications appear on the host system taskbar in the same way as open host applications.

On host system and virtual machine applications that are displayed in Unity mode, you can use keyboard shortcuts to copy, cut, and paste images, plain text, formatted text, and email attachments between applications. You can also drag and drop and copy and paste files between the host system and the guest operating system.

If you save a file or attempt to open a file from an application in Unity mode, the file system you see is the file system inside the virtual machine. You cannot open a file from the host operating system or save a file to the host operating system.

For some guest operating systems, application windows in Unity mode can appear only on the monitor that is set as the primary display when you have multiple monitors. If the host and guest operating systems are Windows XP or later, the application windows can appear on additional monitors.

Unity mode is not available in full screen mode on Windows.

---

**NOTE** You cannot use Unity mode with a remote virtual machine.

---

### Prerequisites

- Verify that the virtual machine is a Workstation 6.x or later virtual machine.
- Verify that the latest version of VMware Tools is installed in the guest operating system.
- Verify that the guest operating system is Linux or Windows 2000 or later.
- For Linux guests and hosts, verify that a modern version of Metacity or KDE is installed. Performance on Linux depends on a combination of variables such as the system, the applications that are running, and the amount of RAM.
- Power on the virtual machine.
- If you are entering Unity mode, open applications in the virtual machine to use in Unity mode.

### Procedure

- To enter Unity mode, select the virtual machine and select **View > Unity**.

  The console view in the Workstation window is hidden, and open applications appear in application windows on the host system desktop. A check mark appears next to **Unity** in the **View** menu.
- To display the virtual machine **Start** menu on a Windows host system, point to the **Start** menu on a Windows host system.
- To display the virtual machine **Applications** menu on a Linux host system, point to the upper-left corner of the primary monitor on the Linux host system.
- To navigate between multiple **Start** or **Applications** menus when multiple virtual machines are in Unity mode, press the arrow keys, Tab, or Shift+Tab to cycle through the virtual machine menus and press Enter and the spacebar to select a virtual machine.

- To exit Unity mode, select **View > Unity** and deselect **Unity**.

### Create Virtual Machine Application Shortcuts on the Host in Unity Mode

You can create a shortcut for a virtual machine application on the host system in Unity mode.

You open the application in the same way that you open an application on the host system. You can open a virtual machine application shortcut from the host system even when the virtual machine is powered off or suspended.

#### Prerequisites

- Verify that the virtual machine is configured to display the virtual machine **Start** or **Application** menu on the host system desktop. See "Set Preferences for Unity Mode," on page 92.
- Verify that the latest version of VMware Tools is running in the guest operating system.
- Power on the virtual machine.

#### Procedure

1 Select the virtual machine and select **View > Unity**.

2 Select a virtual machine application.

| Option | Action |
|---|---|
| **Windows host** | Point to the **Start** button to display the virtual machine **Start** menu on the host system desktop, click the **Start** menu, and select the application. |
| **Linux host** | Point to the upper-left corner of the primary monitor to display the virtual machine **Applications** menu on the host system desktop, click **Applications** menu, and select the application. |

3 Create a shortcut to the application on the host system.

| Option | Action |
|---|---|
| **Windows host** | Right-click the application and select **Create Shortcut on Desktop**, or drag the application to the host system. |
| **Linux host** | Drag the application to the host system. |

## Use Multiple Monitors for One Virtual Machine

If the host system has multiple monitors, you can configure a virtual machine to use multiple monitors. You can use the multiple-monitor feature when the virtual machine is in full screen mode.

NOTE You do not need to use the Windows display properties settings in a Windows guest operating system to configure multiple monitors.

#### Prerequisites

- Verify that the virtual machine is a Workstation 6.x or later virtual machine.
- Verify that the latest version of VMware Tools is installed in the guest operating system.
- Verify that the guest operating system is Windows XP or higher, or Linux.
- Power off the virtual machine.

#### Procedure

1 Select **Edit > Preferences**.

2 Select **Display**, select **Autofit guest**, and click **OK**.

This setting causes the virtual machine display settings to match the application window when the application window is resized.

3 If the virtual machine is set to be restored from a snapshot and background snapshots are enabled, select **Edit > Preferences > Priority**. Deselect **Take snapshots in the background when possible** and **Restore snapshots in the background when possible**and click **OK**.

Displaying the virtual machine on two monitors might not work correctly if these setting are enabled.

4 Power on the virtual machine and select **View > Full Screen**.

5 On the full screen toolbar, click the **Choose a Monitor Layout** button.

If the host system has more than two monitors, the **Choose a Monitor Layout** button provides a drop-down menu of monitor layouts. The monitors that are part of each layout are marked with a Workstation icon.

The **Choose a Monitor Layout** button is available when the guest is Linux, or Windows Vista or later. For other guests, or if the host has two monitors, use the **Cycle Multiple Monitors** button to change the monitor layout.

On a Windows host, you can mouse over a button on the toolbar to see its name.

The guest operating system desktop extends to the additional monitor or monitors.

6 (Optional) If the virtual machine display does not resize correctly, select **View > Autosize > Autofit Guest**.

### Limitations for Mutiple Monitors

The use of more than two monitors with a virtual machine has certain limitations.

- If you attempt to use more than two monitors with a virtual machine, your virtual machine must support more than two monitors for this feature to function.
- More than two monitors is supported on Windows and Linux host and guest operating systems.
- Windows XP guests support more than three monitors. However, only three monitors can be in use by a Windows XP guest at one time. If more than three monitors are connected to a Windows XP guest, use the **Cycle multiple monitors** button to cycle through the monitors to the configuration you want to use.

## Use Multiple Monitors for Multiple Virtual Machines

If the host system has multiple monitors, you can run a different virtual machine on each monitor.

#### Prerequisites

Verify that the latest version of VMware Tools is installed in the guest operating system.

#### Procedure

1 Open a second Workstation window.

| Option | Description |
|---|---|
| **Open a new Workstation window from Workstation** | Select **File > New Window**. On Linux hosts, the windows operate in a single Workstation process. |
| **(Linux hosts only) Run a separate Workstation process in a different X server** | Use the `vmware` command with the `–W` flag, for example, `vmware –W &`. |

2 Start one or more virtual machines in each Workstation window.

3 Drag each Workstation window to the monitor on which you want to use it.

If a virtual machine is running in one Workstation window and you want to run that virtual machine in another Workstation window, you must close the virtual machine in the first window before you attempt to open it in the other window.

4 To switch mouse and keyboard input from the virtual machine on the first monitor to the virtual machine on the second monitor, move the mouse pointer from one screen to the other screen and click inside the second monitor.

## Fit the Workstation Console to the Guest Operating System Display

You can control the size of the virtual machine display and match the Workstation console with the display size of the guest operating system for an active virtual machine.

The fit options are redundant if the corresponding Autofit option is active because the console and the guest operating system display are the same size.

### Prerequisites

- For a Linux virtual machine, familiarize yourself with the considerations for resizing displays. See "Considerations for Resizing Displays in Linux Virtual Machines," on page 73.
- For a Solaris virtual machine, familiarize yourself with the considerations for resizing displays. See "Considerations for Resizing Displays in Solaris Virtual Machines," on page 74.

### Procedure

- To configure a display size option, select **View > Autosize** and select an Autofit option.

| Option | Description |
|---|---|
| **Autofit Guest** | The virtual machine resizes the guest display resolution to match the size of the Workstation console. |
| **Stretch Guest** | The virtual machine changes the guest display to fit the full screen. The guest display resolution is not changed. |
| **Center Guest** | The virtual machine centers the guest display in the full screen. The guest display resolution is not changed. |
| **Autofit Window** | The Workstation console maintains the size of the virtual machine display resolution. If the guest operating system changes its resolution, the Workstation console resizes to match the new resolution. |

- To configure a fit option, select **View** and select a fit option.

| Option | Description |
|---|---|
| **Fit Window Now** | The Workstation console changes to match the current display size of the guest operating system. |
| **Fit Guest Now** | The guest operating system display size changes to match the current Workstation console. |

## Considerations for Resizing Displays in Linux Virtual Machines

Certain considerations apply to resizing displays in Linux virtual machines.

- If you have virtual machines that were suspended under a version of VMware Tools earlier than version 5.5, display resizing does not work until the virtual machines are powered off and powered on again. Rebooting the guest operating system is not sufficient.
- To use the resizing options, you must update VMware Tools to the latest version in the guest operating system.

- You cannot use the **Autofit Guest** and **Fit Guest Now** options unless VMware Tools is running in the guest operating system.
- The resizing restrictions that the X11 Windows system imposes on physical host systems also apply to guest operating systems.
  - You cannot resize to a mode that is not defined. The VMware Tools configuration script can add a large number of mode lines, but you cannot resize in 1-pixel increments as you can in Windows. VMware Tools adds modelines in 100-pixel increments. This means that you cannot resize a guest larger than the largest mode defined in the X11 configuration file. If you attempt to resize larger than that mode, a black border appears and the guest operating system size stops increasing.
  - The X server always starts up in the largest defined resolution. The XDM/KDM/GDM login screen always appears at the largest size. Because Gnome and KDE allow you to specify your preferred resolution, you can reduce the guest display size after you log in.

### Considerations for Resizing Displays in Solaris Virtual Machines

Certain considerations apply to resizing displays in Solaris virtual machines.

- To use the display resizing options, you must update VMware Tools to the latest version in the guest operating system.
- You cannot use the **Autofit Guest** and **Fit Guest Now** options unless VMware Tools is running in the guest operating system.
- Solaris 10 guests must be running an Xorg X server and JDS/Gnome.

### Working with Nonstandard Resolutions

A guest operating system and its applications might react unexpectedly when the Workstation console size is not a standard VESA resolution.

For example, you can use **Autofit Guest** and **Fit Guest Now** to set the guest operating system screen resolution smaller than 640×480, but some installers do not run at resolutions smaller than 640×480. Programs might refuse to run. Error messages might include phrases such as `VGA Required to Install` or `You must have VGA to install`.

If the host computer screen resolution is high enough, you can enlarge the window and select **Fit Guest Now**. If the host computer screen resolution does not allow you to enlarge the Workstation console sufficiently, you can manually set the guest operating system's screen resolution to 640×480 or larger.

## Using Folders to Manage Virtual Machines

You can use folders to organize and manage multiple virtual machines in the library. When virtual machines are in a folder, you can manage them on the folder tab and perform batch power operations.

- Add a Virtual Machine to a Folder on page 75

  When you add a virtual machine to a folder, it remains an independent entity, but you can also perform batch power operations. For example you can power on, suspend, and resume each virtual machine in a folder separately, or you can power on, suspend, and resume all of the virtual machines in a folder at the same time.

- Remove a Virtual Machine from a Folder on page 75

  You can remove a virtual machine from a folder or move it to a different folder or subfolder.

- Manage Virtual Machines in a Folder on page 75

  When virtual machines are in a folder, you can manage them as a unit. For example, you can select multiple virtual machines on the folder tab and perform power operations on several virtual machines at the same time.

- Change the Power On Delay on page 76

  By default, when you power on several virtual machines in a folder, Workstation delays 10 seconds before powering on the next virtual machine. The power on delay avoids overloading the CPU on the host system when you power on multiple virtual machines. You can change the default power on delay setting by modifying a Workstation preference.

- Convert a Team on page 76

  If you created a team in an earlier version of Workstation, you must convert the team before you can use the virtual machines in the current version of Workstation.

## Add a Virtual Machine to a Folder

When you add a virtual machine to a folder, it remains an independent entity, but you can also perform batch power operations. For example you can power on, suspend, and resume each virtual machine in a folder separately, or you can power on, suspend, and resume all of the virtual machines in a folder at the same time.

### Procedure

1 If the folder does not already exist, create it.

| Option | Description |
|---|---|
| **Create a folder at the top level of the library** | Right-click **My Computer**, select **New Folder**, and type a name for the folder. The folder appears under **My Computer** in the library. |
| **Create a subfolder** | Right-click the folder, select **New Folder**, and type a name for the folder. The new folder appears under the folder in the library. |

You can create an unlimited number of folders or subfolders.

2 To add a virtual machine to a folder, select the virtual machine in the library and drag it to the folder.

The virtual machine appears under the folder in the library. You can add an unlimited number of virtual machines to a folder.

## Remove a Virtual Machine from a Folder

You can remove a virtual machine from a folder or move it to a different folder or subfolder.

### Procedure

- To remove a virtual machine from a folder, select the virtual machine in the library and drag it to **My Computer**.

  The virtual machine appears under **My Computer** in the library.

- To move a virtual machine to a different folder or subfolder, select the virtual machine in the library and drag it to the folder or subfolder.

  The virtual machine appears under the folder or subfolder in the library.

## Manage Virtual Machines in a Folder

When virtual machines are in a folder, you can manage them as a unit. For example, you can select multiple virtual machines on the folder tab and perform power operations on several virtual machines at the same time.

When you power on several virtual machines at the same time, Workstation delays 10 seconds before powering on the next virtual machine by default. Workstation performs power operations on virtual machines in the order in which they appear on the folder tab.

You can change the default power on delay setting by modifying a Workstation preference. See "Change the Power On Delay," on page 76.

### Procedure

- To perform a power operation on several virtual machines at the same time, use Ctrl-Click to select the virtual machines on the folder tab and select the power operation from the toolbar or from the **VM** menu.

  All of the virtual machines that you select must be in the same power state.

- To perform a power operation on all of the virtual machines at the same time, select the folder in the library and select the power operation from the toolbar or from the **VM** menu.

  All of the virtual machines in the folder must be in the same power state.

- To display thumbnails for virtual machines on the folder tab, select a thumbnail size from the drop-down menu on the folder tab.

  When a virtual machine is powered on, Workstation updates the thumbnail in real time to show the actual content of the virtual machine. When a virtual machine is suspended, the thumbnail shows a screenshot of the virtual machine at the time that it was suspended.

- To display virtual machine names on the folder tab, select **Details** from the drop-down menu on the folder tab.

- To open the tab for a virtual machine, double-click the virtual machine on the folder tab.

## Change the Power On Delay

By default, when you power on several virtual machines in a folder, Workstation delays 10 seconds before powering on the next virtual machine. The power on delay avoids overloading the CPU on the host system when you power on multiple virtual machines. You can change the default power on delay setting by modifying a Workstation preference.

### Procedure

1. Select **Edit > Preferences** and select **Workspace**.
2. Select the number of seconds for the delay from the **Seconds between powering on multiple VMs** drop-down menu.
3. Click **OK** to save your changes.

## Convert a Team

If you created a team in an earlier version of Workstation, you must convert the team before you can use the virtual machines in the current version of Workstation.

### Procedure

1. Open the team in Workstation or browse to the location of the virtual machine team configuration (`.vmtm`) file and drag it to the library.

   A dialog box appears that prompts you to convert the team.

2. Click **Convert Team** to convert the team.

After the team is converted, the `.vmtm` file is deleted and the virtual machines are added to a new folder in the library.

After you convert a team, the virtual machines keep their packet loss and bandwidth settings. LAN segment information appears in the network adapter settings for each virtual machine, where you can modify it.

# Taking Snapshots of Virtual Machines

Taking a snapshot of a virtual machine saves its current state and enables you to return to the same state repeatedly. When you take a snapshot, Workstation captures the entire state of the virtual machine. You can use the snapshot manager to review and act on the snapshots for an active virtual machine.


- Using Snapshots to Preserve Virtual Machine States on page 78

  A snapshot includes the contents of the virtual machine memory, virtual machine settings, and the state of all the virtual disks. When you revert to a snapshot, you return the memory, settings, and virtual disks of the virtual machine to the state they were in when you took the snapshot.

- Using the Snapshot Manager on page 78

  You can review all snapshots for a virtual machine and act on them directly in the snapshot manager.

- Take a Snapshot of a Virtual Machine on page 79

  When you take a snapshot, you preserve the state of a virtual machine at a specific moment in time and the virtual machine continues to run. Taking a snapshot enables you to return to the same state repeatedly. You can take a snapshot while a virtual machine is powered on, powered off, or suspended.

- Revert to a Snapshot on page 80

  You can restore a virtual machine to a previous state by reverting to a snapshot.

- Take or Revert to a Snapshot at Power Off on page 80

  You can configure a virtual machine to revert to a snapshot or take a new snapshot when you power off the virtual machine. This feature is useful if you need to discard changes when a virtual machine is powered off.

- Enable AutoProtect Snapshots on page 80

  The AutoProtect feature preserves the state of a virtual machine by taking snapshots at regular intervals that you specify. This process is in addition to manual snapshots, which you can take at any time.

- Enable Background Snapshots on page 81

  When you enable background snapshots, you can continue working while Workstation preserves the state of a virtual machine. A progress indicator for the background snapshot appears in a corner of the Workstation window.

- Exclude a Virtual Disk from Snapshots on page 82

  You can configure snapshots so that Workstation preserves states only for certain virtual disks.

- Delete a Snapshot on page 82

  When you delete a snapshot, you delete the state of the virtual machine that you preserved and you can never return to that state again. Deleting a snapshot does not affect the current state of the virtual machine.

- Troubleshooting Snapshot Problems on page 83

  You can use a variety of procedures for diagnosing and fixing problems with snapshots.

## Using Snapshots to Preserve Virtual Machine States

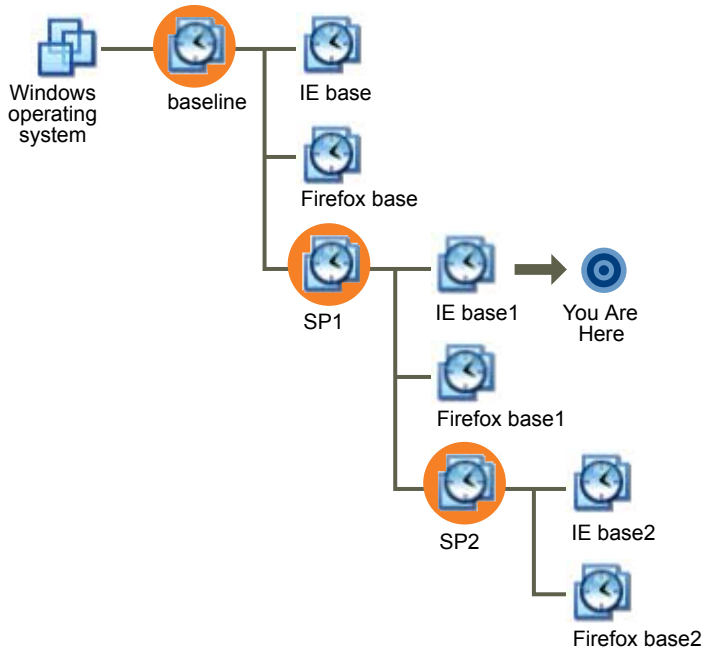
A snapshot includes the contents of the virtual machine memory, virtual machine settings, and the state of all the virtual disks. When you revert to a snapshot, you return the memory, settings, and virtual disks of the virtual machine to the state they were in when you took the snapshot.

You might want to take snapshots in a linear process if you plan to make changes in a virtual machine. For example, you can take a snapshot, continue to use the virtual machine from that point, take another snapshot at a later point, and so on. You can revert to the snapshot of a previous known working state of the project if the changes do not work as expected.

For local virtual machines, you can take more than 100 snapshots for each linear process. For shared and remote virtual machines, you can take a maximum of 31 snapshots for each linear process.

If you are testing software, you might want to save multiple snapshots as branches from a single baseline in a process tree. For example, you can take a snapshot before installing different versions of an application to make sure that each installation begins from an identical baseline.

**Figure 2-1.** Snapshots as Restoration Points in a Process Tree




Multiple snapshots have a parent-child relationship. The parent snapshot of a virtual machine is the snapshot on which the current state is based. After you take a snapshot, that stored state is the parent snapshot of the virtual machine. If you revert to an earlier snapshot, the earlier snapshot becomes the parent snapshot of the virtual machine.

In a linear process, each snapshot has one parent and one child, except for the last snapshot, which has no children. In a process tree, each snapshot has one parent, one snapshot can have more than one child, and many snapshots have no children.

## Using the Snapshot Manager

You can review all snapshots for a virtual machine and act on them directly in the snapshot manager.

You must use the snapshot manager to perform the following tasks.

- Show AutoProtect snapshots in the **Snapshot** menu.
- Prevent an AutoProtect snapshot from being deleted.

- Rename a snapshot or change its description.
- Delete a snapshot.

All other snapshot actions are available as menu items in the **Snapshot** menu under the **VM** menu.

When you open the snapshot manager for a virtual machine, the snapshot tree appears. The snapshot tree shows all of the snapshots for the virtual machine and the relationships between the snapshots.

The **You Are Here** icon in the snapshot tree shows the current state of the virtual machine. The other icons that appear in the snapshot tree represent AutoProtect snapshots, snapshots of powered-on virtual machines, snapshots of powered-off virtual machines, and snapshots that are used to create linked clones.

The snapshot manager is available as a menu item in the **Snapshot** menu under the **VM** menu.

## Take a Snapshot of a Virtual Machine

When you take a snapshot, you preserve the state of a virtual machine at a specific moment in time and the virtual machine continues to run. Taking a snapshot enables you to return to the same state repeatedly. You can take a snapshot while a virtual machine is powered on, powered off, or suspended.

Avoid taking snapshots when applications in the virtual machine are communicating with other computers, especially in production environments. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file after you take the snapshot. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

---

**NOTE** Workstation 4 virtual machines do not support multiple snapshots. You must upgrade the virtual machine to Workstation 7.x or later to take multiple snapshots.

---

### Prerequisites

- Verify that the virtual is not configured to use a physical disk. You cannot take a snapshot of a virtual machine that uses a physical disk.
- To have the virtual machine revert to suspend, power on, or power off when you start it, be sure it is in that state before you take the snapshot. When you revert to a snapshot, you return the memory, settings, and virtual disks of the virtual machine to the state they were in when you took the snapshot.
- Complete any suspend operations.
- Verify that the virtual machine is not communicating with another computer.
- For better performance, defragment the guest operating system drives.
- If the virtual machine has multiple disks in different disk modes, power off the virtual machine. For example, if a configuration requires you to use an independent disk, you must power off the virtual machine before you take a snapshot.
- If the virtual machine was created with Workstation 4, delete any existing snapshots or upgrade the virtual machine to Workstation 5.x or later.

### Procedure

1 Select the virtual machine and select **VM > Snapshot > Take Snapshot**.

2 Type a unique name for the snapshot.

3 (Optional) Type a description for the snapshot.

The description is useful for recording notes about the virtual machine state captured in the snapshot.

4 Click **OK** to take the snapshot.

## Revert to a Snapshot

You can restore a virtual machine to a previous state by reverting to a snapshot.

If you take a snapshot of a virtual machine and add any kind of disk, reverting to the snapshot removes the disk from the virtual machine. If associated disk (`.vmdk`) files are not used by another snapshot, the disk files are deleted.

**IMPORTANT** If you add an independent disk to a virtual machine and take a snapshot, reverting to the snapshot does not affect the state of the independent disk.

### Procedure

- To revert to the parent snapshot, select the virtual machine and select **VM > Snapshot > Revert to Snapshot**.
- To revert to any snapshot, select the virtual machine, select **VM > Snapshot**, select the snapshot, and click **Go To**.

## Take or Revert to a Snapshot at Power Off

You can configure a virtual machine to revert to a snapshot or take a new snapshot when you power off the virtual machine. This feature is useful if you need to discard changes when a virtual machine is powered off.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Snapshots**.

3 Select a power off option.

| Option | Description |
|---|---|
| **Just power off** | Powers off the virtual machine without making any changes to snapshots. |
| **Revert to snapshot** | Reverts to the parent snapshot of the current state of the virtual machine. |
| **Take a new snapshot** | Takes a snapshot of the virtual machine state after it is powered off. The snapshot appears in the Snapshot Manager. The name of the snapshot is the date and time that the virtual machine was powered off and the description is Automatic snapshot created when powering off.<br>**NOTE** You cannot configure this option for a shared or remote virtual machine. |
| **Ask me** | Prompts you to power off, revert, or take a snapshot when the virtual machine is powered off. |

4 Click **OK** to save your changes.

## Enable AutoProtect Snapshots

The AutoProtect feature preserves the state of a virtual machine by taking snapshots at regular intervals that you specify. This process is in addition to manual snapshots, which you can take at any time.

When AutoProtect snapshots are enabled for a virtual machine, Workstation shows an estimate of the minimum amount of disk space taken by AutoProtect snapshots on the Virtual Machine Settings window. This minimum is affected by the memory settings for the virtual machine. The more virtual machine memory a virtual machine has, the more disk space is available for AutoProtect snapshots.

The AutoProtect feature has certain restrictions.

- Because AutoProtect takes snapshots only while a virtual machine is powered on, AutoProtect snapshots cannot be cloned. You can clone a virtual machine only if it is powered off.
- AutoProtect snapshots are not taken in VMware Player, even if AutoProtect is enabled for the virtual machine in Workstation.
- You cannot configure the AutoProtect feature for a shared or remote virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **AutoProtect** and select **Enable AutoProtect**.

3 Select the interval between snapshots.

| Option | Description |
|---|---|
| **Half-Hourly** | Snapshots are taken every half hour. |
| **Hourly** | Snapshots are taken every hour. |
| **Daily** | Snapshots are taken daily. |

The interval is measured only when the virtual machine is powered on. For example, if you set AutoProtect to take snapshots hourly and then power off the virtual machine five minutes later, the next AutoProtect snapshot takes place 55 minutes after you power on the virtual machine again, regardless of the length of time the virtual machine was powered off.

Workstation saves only one snapshot per tier, even if a snapshot matches more than one tier.

4 Select the maximum number of AutoProtect snapshots to retain.

After the maximum number of AutoProtect snapshots is reached, Workstation deletes the oldest AutoProtect snapshot each time a new AutoProtect snapshot is taken. This setting does not affect the number of manual snapshots that you can take and keep.

5 Select **OK** to save your changes.

## Enable Background Snapshots

When you enable background snapshots, you can continue working while Workstation preserves the state of a virtual machine. A progress indicator for the background snapshot appears in a corner of the Workstation window.

**IMPORTANT** Enabling background snapshots for a host with slow hard disks can adversely affect performance. If you experience significant performance problems when taking or restoring snapshots, disable background snapshots.

### Prerequisites

On a Linux host, run Workstation as the root user. Only root users are allowed to change background snapshot settings.

### Procedure

1 Select **Edit > Preferences**.

2 On the **Priority** tab, select **Take snapshots in the background**.

3 Click **OK** to save your changes.

4 Restart the virtual machines.

Virtual machines must be powered off and then powered on, rather than restarted, for background snapshot changes to take effect.

## Exclude a Virtual Disk from Snapshots

You can configure snapshots so that Workstation preserves states only for certain virtual disks.

In certain configurations, you might want to revert some disks to a snapshot while other disks retain all changes. For example, you might want a snapshot to preserve a disk with the operating system and applications, but always keep the changes to a disk with documents.

### Prerequisites

- Power off the virtual machine.
- Delete existing snapshots.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select the drive to exclude and click **Advanced**.

3 Select **Independent** and select the disk mode.

| Option | Description |
|---|---|
| **Persistent** | Changes are immediately and permanently written to the disk. Disks in persistent mode behave like conventional disks on a physical computer. |
| **Nonpersistent** | Changes to the disk are discarded when you power off or restore a snapshot. In nonpersistent mode, a virtual disk is in the same state every time you restart the virtual machine. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset the virtual machine. |

## Delete a Snapshot

When you delete a snapshot, you delete the state of the virtual machine that you preserved and you can never return to that state again. Deleting a snapshot does not affect the current state of the virtual machine.

If a snapshot is used to create a clone, the snapshot becomes locked. If you delete a locked snapshot, the clones created from the snapshot no longer operate.

You cannot delete a snapshot if the associated virtual machine is designated as a template for cloning.

### Procedure

1 Select the virtual machine and select **VM > Snapshot > Snapshot Manager**.

2 If you are deleting an AutoProtect snapshot, select **Show AutoProtect snapshots**.

3 Select the snapshot.

4 Select an option to delete the snapshot.

| Option | Action |
|---|---|
| **Delete a single snapshot** | Click **Delete**. |
| **Delete the snapshot and all of its children** | Right-click and select **Delete Snapshot and Children**. |
| **Delete all snapshots** | Right-click, select **Select All**, and click **Delete**. |

5 Click **Close** to close the snapshot manager.

## Troubleshooting Snapshot Problems

You can use a variety of procedures for diagnosing and fixing problems with snapshots.

### Guest Operating System Has Startup Problems

The guest operating system experiences problems during startup.

#### Problem

The guest operating system does not start up properly.

#### Cause

Keeping more than 99 snapshots for each branch in a process tree can cause startup problems.

#### Solution

Delete some snapshots or create a full clone of the virtual machine.

### Take Snapshot Option Is Disabled

The Snapshot Manager **Take Snapshot** option is disabled.

#### Problem

You cannot select the **Take Snapshot** option in the Snapshot Manager.

#### Cause

The virtual machine might have multiple disks in different disk modes.

#### Solution

If your configuration requires an independent disk, you must power off the virtual machine before you take a snapshot.

### Performance Is Slow When You Take a Snapshot

Significant performance problems occur when you take or restore snapshots.

#### Problem

Performance is slow when you take or restore snapshots.

#### Cause

The host operating system has a slow hard disk.

#### Solution

Upgrade the hard disk or disable background snapshots to improve performance. See "Enable Background Snapshots," on page 81 for information on background snapshots.

# Install New Software in a Virtual Machine

Installing new software in a virtual machine is similar to installing new software on a physical computer. Only a few additional steps are required.

### Prerequisites

- Verify that VMware Tools is installed in the guest operating system. Installing VMware Tools before installing the software minimizes the likelihood that you will have to reactivate the software if the virtual machine configuration changes.
- Verify that the virtual machine has access to the CD-ROM drive, ISO image file, or floppy drive where the installation software is located.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Memory**, set the final memory size for the virtual machine, and click **OK**.

Some applications use a product activation feature that creates a key based on the virtual hardware in the virtual machine where it is installed. Changes in the configuration of the virtual machine might require you to reactivate the software. Setting the memory size minimizes the number of significant changes.

3 Install the new software according to the manufacturer's instructions.

## Disable Acceleration if a Program Does Not Run

When you install or run software inside a virtual machine, Workstation might appear to stop responding. This problem typically occurs early in the program's execution. In many cases, you can get past the problem by temporarily disabling acceleration in the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Processors**.

3 Select **Disable acceleration for binary translation** to disable acceleration.

4 Click **OK** to save your changes.

### What to do next

After you pass the point where the program encountered problems, re-enable acceleration. Because disabling acceleration slows down virtual machine performance, you should use it only for getting past the problem with running the program

# Share Tablet Sensor Data with Windows 8 Guests

You can configure a Windows 8 guest operating system to pass tablet sensor data to your host Windows 8 tablet. This allows you to use applications designed for tablets inside your virtual machine.

### Prerequisites

- Workstation 10 or higher.
- Power off a Windows 8 virtual machine.

**NOTE** Tablet data is only available on guest operating systems and hosts running Windows 8 or higher.

### Procedure

1 Select the Windows 8 virtual machine and click **VM > Settings > Options > Guest Isolation**

2 Select the tablet sensor data to be shared with the Windows 8 host from the **Share sensor input** section.

| Option | Description |
|---|---|
| **Location** | Location information. |
| **Orientation** | Detects the orientation of the device. For example in landscape or portrait mode. |
| **Motion** | Detects changes in physical speed. |
| **Ambient light** | Checks the available light. |

3 Click **OK**.

## Take a Screenshot of a Virtual Machine

You can take a screenshot of a virtual machine and save it to the clipboard, to a file, or to both a file and the clipboard.

When a take a screenshot of a virtual machine, the image is saved as a portable network graphics (`.png`) file by default. On Windows hosts, you can also save the screenshot as a bitmap (`.bmp`) file.

On Linux hosts, saving a screenshot to the clipboard is supported only on systems running Gnome 2.12 or later.

### Procedure

1 Select **Edit > Preferences**.

2 Select **Workspace** and select a save screenshots option.

You can select both options to save screenshots to both a file and the clipboard.

| Option | Description |
|---|---|
| **Clipboard** | Save the screenshot to the clipboard. |
| **File** | Save screenshots to a file. You can select:<br>■ Always ask for location<br>■ Save to Desktop<br>■ Browse for custom location<br>■<br>By default, Workstation saves screenshots to `.png` files on the Desktop of the host computer. If you save the file to the desktop, the filename is generated from the virtual machine name and the time at which the screenshot is taken.<br>To save screenshots to `.bmp` files on Windows hosts, select **Always ask for location** and specify the file type when you save the screenshot. |

3 Click **OK** to save your changes.

4 To take the screenshot, select the virtual machine, select **VM > Capture Screen**.

## Delete a Virtual Machine

You can delete a virtual machine and all of its files from the host file system.

**IMPORTANT** Do not delete a virtual machine if it was used to make a linked clone and you want to continue to use the linked clone. A linked clone stops working if it cannot find the virtual disk files for the parent virtual machine.

### Prerequisites

Power off the virtual machine.

### Procedure

- Select the virtual machine and select **VM > Manage > Delete from Disk**.

# Configuring and Managing Virtual Machines

3

You can configure virtual machine power, display, video, and sound card settings, encrypt a virtual machine to secure it from unauthorized use, and restrict the Workstation user interface to limit virtual machine operations.

You can also move a virtual machine to another host system or to a different location on the same host system, configure a virtual machine as a VNC server, change the hardware compatibility of a virtual machine, and export a virtual machine to Open Virtualization Format (OVF).

This chapter includes the following topics:


- "Configure Power Options and Power Control Settings," on page 87
- "Set Workstation Display Preferences," on page 89
- "Configure Display Settings for a Virtual Machine," on page 90
- "Set Preferences for Unity Mode," on page 92
- "Setting Screen Color Depth," on page 92
- "Using Advanced Linux Sound Architecture," on page 93
- "Encrypting and Restricting Virtual Machines," on page 94
- "Moving Virtual Machines," on page 98
- "Configure a Virtual Machine as a VNC Server," on page 103
- "Change the Hardware Compatibility of a Virtual Machine," on page 106
- "Clean Up a Virtual Hard Disk on Windows Hosts," on page 107
- "Export a Virtual Machine to OVF Format," on page 108
- "Writing and Debugging Applications That Run In Virtual Machines," on page 109


## Configure Power Options and Power Control Settings

You can configure how a virtual machine behaves when it is powered on, powered off, and closed. You can also configure the behavior of the power controls and specify which power options appear in the context menu when you right-click the virtual machine in the library.

You can configure a soft or hard setting for each power control. A soft setting sends a request to the guest operating system, which the guest operating system can ignore or, in the case of a deadlocked guest, it might not be able to handle. A guest operating system cannot ignore a hard power control. Hard power control settings are configured by default.

Power control settings affect the behavior of the stop, suspend, start, and reset buttons. The behavior you select for a power control appears in a tooltip when you mouse over the button. Power control settings also determine which power options appear in the context menu. For example, if you select the hard setting for the start control, **Power On** appears in the context menu when you right-click the virtual machine in the library. If you select the soft setting, **Start Up Guest** appears instead.

Not all guest operating systems respond to a shutdown or restart signal. If the guest operating system does not respond to the signal, shut down or restart from within the guest operating system.

You can pass X toolkit options when you power on a virtual machine for a Linux guest operating system. See Chapter 7, "Using the vmware Command," on page 199 for more information.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Power**.

3 Select a power option.

NOTE You cannot configure these options for a shared or remote virtual machine.

| Option | Description |
|---|---|
| **Enter full screen mode after powering on** | The virtual machine enters full screen mode after it is powered on. |
| **Close after powering off or suspending** | The virtual machine closes after it is powered off or suspended. |
| **Report battery information to guest** | Battery information is reported to the guest operating system. If you run the virtual machine on a laptop in full screen mode, this option enables you to determine when the battery is running low. This option is available only for Workstation 6.x and later virtual machines. |

4 Select a setting for the power off control.

| Option | Description |
|---|---|
| **Power Off** | (Hard option) Workstation powers off the virtual machine abruptly with no consideration for work in progress. |
| **Shut Down Guest** | (Soft option) Workstation sends a shut down signal to the guest operating system. An operating system that recognizes the signal shuts down gracefully. Not all guest operating systems respond to a shutdown signal from Workstation. If the guest operating system does not respond to the signal, shut down from the guest operating system as you would a physical machine. |

5 Select a setting for the suspend control.

| Option | Description |
|---|---|
| **Suspend** | (Hard option) Workstation suspends the virtual machine and leaves it connected to the network. |
| **Suspend Guest** | (Soft option) Workstation suspends the virtual machine and disconnects it from the network. VMware Tools runs a script in the guest operating system. On Windows guests, if the virtual machine is configured to use DHCP, the script releases the IP address of the virtual machine. On Linux, FreeBSD, and Solaris guests, the script stops networking for the virtual machine. |

6 Select a setting for the start control.

NOTE You cannot configure start control settings for a shared or remote virtual machine.

| Option | Description |
|---|---|
| **Power On** | (Hard option) Workstation starts the virtual machine. |
| **Start Up Guest** | (Soft option) Workstation starts the virtual machine and VMware Tools runs a script in the guest operating system. On Windows guests, if the virtual machine is configured to use DHCP, the script renews the IP address of the virtual machine. On a Linux, FreeBSD, or Solaris guest, the script starts networking for the virtual machine. |

7 Select a setting for the reset control.

| Option | Description |
|---|---|
| **Reset** | (Hard option) Workstation resets the virtual machine abruptly with no consideration for work in progress. |
| **Restart Guest** | (Soft option) Workstation shuts down and restarts the guest operating system gracefully. VMware Tools runs scripts before the virtual machine shuts down and when the virtual machine starts up. |

8 Click **OK** to save your changes.

## Set Workstation Display Preferences

You can configure Workstation display preferences to control how the display settings of all virtual machines adjust to fit the Workstation window. These adjustments occur when you resize the Workstation window or when you change the display settings in the guest operating system.

### Prerequisites

Verify that the latest version of VMware Tools is installed in all guest operating systems.

### Procedure

1 Select **Edit > Preferences** and select **Display**.

2 Configure the Autofit options.

You can select one option, both options, or no options.

| Option | Description |
|---|---|
| **Autofit window** | Resize the application window to match the virtual machine display settings when the virtual machine display settings are changed. |
| **Autofit guest** | Change the virtual machine settings to match the application window when the application window is resized. |

3 Select a full screen option.

| Option | Description |
|---|---|
| **Autofit guest (change guest resolution)** | Virtual machine resolution settings change to match the display settings of the host system when you are in full screen mode. |
| **Stretch guest (no resolution change)** | Virtual machine resolution settings are retained, but the display still changes to fill the full screen. Select this setting if you need to retain low-resolution settings, for example, when playing older computer games that run only at low resolutions. |
| **Center guest (no resolution change)** | The host system and virtual machines retain their own display settings when you are in full screen mode. |

4 Select menu and toolbar options.

You can select one or more options, or no options.

| Option | Description |
|---|---|
| **Use a single button for power controls** | (Windows hosts only) When this setting is selected, the start, stop, suspend, and reset power controls appear on the toolbar as a single button with a drop-down menu. When this setting is deselected, each power control has a separate button on the toolbar. |
| **Combine toolbar with menu bar in windowed mode** | Show the Workstation menus and toolbar on a single bar when Workstation is in windowed mode. |
| **Show toolbar edge when unpinned** | Show the edge of the full screen toolbar. When this setting is deselected, the edge of the full screen toolbar is not visible. The full screen toolbar appears for a few seconds when you place your cursor near the top of the screen. |

5 Click **OK** to save your changes.

# Configure Display Settings for a Virtual Machine

You can specify monitor resolution settings, configure multiple monitors, and select accelerated graphics capabilities for a virtual machine. You can use the multiple-monitor feature when the virtual machine is in full screen mode.

To use DirectX 9 accelerated graphics, the guest operating system must be Windows XP, Windows Vista, or Windows 7.

Only Workstation 6.x and later virtual machines support specifying resolution settings and setting the number of monitors that the guest operating system can use.

### Prerequisites

- Verify that the latest version of VMware Tools is installed in the guest operating system.
- Verify that the guest operating system in the virtual machine is Windows XP, Windows Vista, Windows 7, or Linux.
- If you plan to use DirectX 9 accelerated graphics, prepare the host system. See "Prepare the Host System to Use DirectX 9 Accelerated Graphics," on page 91.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Display**.

3 Specify whether host settings determine the number of monitors.

| Option | Description |
|---|---|
| **Use host setting for monitors** | When you select this setting, the SVGA driver uses two monitors, a maximum bounding box width of 3840, and a maximum bounding box height of 1920. The virtual machine is configured to have a minimum of two 1920x1200 monitors, in a side-by-side topology, in both normal and rotated orientations. If the host system has more than two monitors, the virtual machine uses the number of monitors on the host system instead. If the host system's bounding box is wider or taller than the defaults, the virtual machine uses the larger size. You should select this setting in most cases. |
| **Specify monitor settings** | Set the number of monitors that the virtual machine will see, regardless of the number of monitors on the host system. This setting is useful if you use a multimonitor host system and you need to test in a virtual machine that has only one monitor. It is also useful if you are developing a multimonitor application in a virtual machine and the host system has only one monitor. After you power on the virtual machine, the guest operating system sees the number of monitors that you specified. Select a resolution from the list or type a setting that has the format *width* x *height*, where *width* and *height* are the number of pixels.<br>NOTE You cannot configure the resolution setting for a remote virtual machine. |

4 (Optional) To run applications that use DirectX 9 accelerated graphics, select **Accelerate 3D graphics**.

5 Click **OK** to save your changes.

## Prepare the Host System to Use DirectX 9 Accelerated Graphics

You must perform certain preparation tasks on the host system to use DirectX 9 accelerated graphics in a virtual machine.

### Prerequisites

- Verify that the host operating system is Windows XP, Windows Vista, Windows 7, or Linux.
- On a Windows host, verify that the host has a video card that supports DirectX 9 and the latest DirectX Runtime.
- On a Linux host, verify that the host has a video card that can run accelerated OpenGL 2.0.

### Procedure

1 Upgrade the video drivers on the host system to the latest versions.

ATI Graphics drivers are available from the AMD Web site. NVIDIA drivers are available from the NVIDIA Web site.

2 If you have a Windows host system, move the **Hardware Acceleration** slider to the **Full** position.

| Option | Description |
|---|---|
| **Windows XP** | Right-click the desktop and select **Properties > Settings > Advanced > Troubleshoot**. |
| **Windows Vista** | Right-click the desktop and select **Personalize > Display Settings > Advanced Settings > Troubleshoot > Change settings**. |
| **Windows 7** | Right-click the desktop and select **Personalize > Screen resolution > Advanced Settings > Troubleshoot > Change settings**. |

3 If you have a Linux host system, run commands to test the host for compatibility.

   a Verify that direct rendering is enabled.

   ```
   glxinfo | grep direct
   ```

   b Verify that 3-D applications work.

   ```
   glxgears
   ```

# Set Preferences for Unity Mode

You can set preferences for Unity mode to control whether that the virtual machine **Start** or **Applications** menu is available from the host system desktop. You can also select the border color that appears around applications that run in Unity mode when they appear on the host system desktop.

When you use the virtual machine **Start** or **Applications** menu from the host system desktop, you can start applications in the virtual machine that are not open in Unity mode. If you do not enable this feature, you must exit Unity mode to display the virtual machine **Start** or **Applications** menu in the console view.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options**, select **Unity**.

3 Select a Unity window decoration option.

| Option | Description |
|---|---|
| **Show borders** | Set a window border that identifies the application as belonging to the virtual machine rather than to the host computer. |
| **Show badges** | Display a logo in the title bar. |
| **Use a custom color in window borders** | Use a custom color in window borders to help distinguish between the application windows that belong to various virtual machines. For example, you can set the applications for one virtual machine to have a blue border and set the applications for another virtual machine to have a yellow border. On Linux hosts, click the colored rectangle to use the color chooser. On Windows hosts, click **Choose color** to use the color chooser. |

4 To control whether the virtual machine **Start** or **Application** menu available on the host system desktop, select or deselect **Enable applications menu**.

5 Click **OK** to save your changes.

6 (Optional) To minimize the Workstation window when you enter Unity mode, edit the Workstation Unity preference setting.

   Workstation preference settings apply to all virtual machines.

   a Select **Edit > Preferences** and select **Unity**.

   b Select **Minimize Workstation when entering Unity** .

   c Click **OK** to save your changes.

# Setting Screen Color Depth

The number of screen colors available in the guest operating system depends on the screen color setting of the host operating system.

Virtual machines support the following screen colors.

- 16-color (VGA) mode

- 8-bit pseudocolor
- 16 bits per pixel (16 significant bits per pixel)
- 32 bits per pixel (24 significant bits per pixel)

If the host operating system is in 15-bit color mode, the guest operating system color setting controls offer 15-bit mode in place of 16-bit mode. If the host operating system is in 24-bit color mode, the guest operating system color setting controls offer 24-bit mode in place of 32-bit mode.

If you run a guest operating system set for a greater number of colors than the host operating system, the colors in the guest operating system might not be correct or the guest operating system might not be able to use a graphical interface. If these problems occur, you can either increase the number of colors in the host operating system or decrease the number of colors in the guest operating system.

To change color settings on the host operating system, power off all virtual machines and close Workstation and then follow standard procedures for changing color settings.

How you change color settings in a guest operating system depends on the type of guest operating system. In a Windows guest, the Display Properties control panel offers only those settings that are supported. In a Linux or FreeBSD guest, you must change the color depth before you start the X server, or you must restart the X server after making the changes.

For best performance, use the same number of colors in the host and guest operating systems.

# Using Advanced Linux Sound Architecture

Workstation 7.x and later versions support Advanced Linux Sound Architecture (ALSA). You might need to perform certain preparation tasks before you can use ALSA in a virtual machine.

To use ALSA, the host system must meet certain requirements.

- The ALSA library version on the host system must be version 1.0.16 or later.
- The sound card on the host system must support ALSA. The ALSA project Web site maintains a current listing of sound cards and chipsets that support ALSA.
- The ALSA sound card on the host system must not be muted.
- The current user must have the appropriate permissions to use the ALSA sound card.

## Override the ALSA Library Version Requirement for a Virtual Machine

If the host system has an earlier version of the ALSA library, you can override the requirement for version 1.0.16.

If the host system does not meet ALSA requirements, or for some other reason cannot use ALSA, Workstation uses the OSS API for sound playback and recording. Depending on the sound card in the host system, the sound quality might not be as good when an older version of the ALSA library is used.

You should upgrade the host system to use the latest sound drivers and libraries.

### Procedure

1 Open the virtual machine configuration (`.vmx`) file in a text editor.

2 Add the `sound.skipAlsaVersionCheck` property and set it to `TRUE`.

For example: `sound.skipAlsaVersionCheck = "TRUE"`

## Obtain ALSA Sound Card Information

You can type commands at the command prompt on a Linux host system to obtain information about the ALSA sound card and determine whether the current user has the appropriate permissions to access it.

### Prerequisites

Obtain the documentation for the `alsamixer` program. The documentation is available on the Internet.

### Procedure

- Use the `alsamixer` program to determine whether the current user has the appropriate permissions to access the ALSA sound card.

  If the user does not have the appropriate permissions, an error similar to `alsamixer: function snd_ctl_open failed for default: No such device.` appears.

- If a user does not have the appropriate permissions to access the ALSA sound card, give the user read, write, and execute permissions to the directory that contains the ALSA sound card.

  The ALSA sound card is usually located in `/dev/snd/`. This location can vary depending on the Linux distribution.

- To list the name and type of sound chipset on the host system, type the command `lspci | grep –I audio`.
- To list the sound cards on the host system, type the command `cat /proc/asound/cards`.
- If the ALSA sound card is muted, use the `alsamixer` program to unmute it.

## Configure a Virtual Machine to Use an ALSA Sound Card

You can configure a virtual machine to use an ALSA sound card by modifying virtual machine settings.

### Procedure

1. Select the virtual machine and select **VM > Settings**.
2. On the **Hardware** tab, select **Sound Card**.
3. Select **Connected** and **Connect at power on**.
4. Select **Specify host sound card** and select the ALSA sound card.
5. If the ALSA sound card does not appear in the list, use the `alsa–utils` package to list the ALSA sound cards on the host system and select **Specify host sound card** again.

   For example: **`aplay –L`**
6. Click **OK** to save your changes.

# Encrypting and Restricting Virtual Machines

Encrypting a virtual machine secures it from unauthorized use. To decrypt a virtual machine, users must enter the correct encryption password. Restricting a virtual machine prevents users from changing configuration settings unless they first enter the correct restrictions password. You can also set other restriction policies.

When you encrypt a virtual machine, Workstation prompts you for a password. After the virtual machine is encrypted, you must enter this password to open the virtual machine or to remove encryption from it. Workstation displays the encrypted virtual machine with a lock icon until you enter the password to open the virtual machine.

If you also enable restrictions, users are prevented from modifying the virtual machine. For example, you can enable restrictions to prevent users from removing virtual devices, changing the memory allocation, modifying removable devices, changing the network connection type, and changing the virtual hardware compatibility. A password prompt appears whenever anyone performs any of the following actions on the virtual machine:

- Clicks **Edit virtual machine settings** or **Upgrade Virtual Machine** on the virtual machine summary tab
- Double-clicks a virtual device in the **Devices** list on the virtual machine summary tab
- Selects the virtual machine and selects **VM > Settings** or **VM > Manage > Change Hardware Compatibility** from the menu bar
- Clicks or right-clicks on a removable device icon to edit its settings
- Uses a **Removable Devices >** ***device_name*** menu to edit the settings for a device

Besides restricting users from changing USB device settings, you can also optionally set a policy that prevents users from connecting USB devices to the guest operating system. If you set the policy to allow connecting USB devices, users are not prompted to enter the restrictions password to use the devices.

An optional policy includes a setting that forces users to change the encryption password if they move or copy the virtual machine. For example, a teacher might provide a copy of the virtual machine to all students in the class and set this restriction so that all students must create their own encryption password.

Another optional policy includes setting an expiration date for a virtual machine. For example, an administrator can create a virtual machine for a temporary employee and set the virtual machine to expire when the temporary employee leaves the company.

---

**IMPORTANT** Make sure you record the encryption password and the restrictions password. Workstation does not provide a way to retrieve these passwords if you lose them.

---

Encryption applies to all snapshots in a virtual machine. If you restore a snapshot in an encrypted virtual machine, the virtual machine remains encrypted whether or not it was encrypted when the snapshot was taken. If you change the password for an encrypted virtual machine, the new password applies to any snapshot you restore, regardless of the password in effect when the snapshot was taken.

- Virtual Machine Encryption Limitations on page 95

  The encryption feature has certain limitations.

- Encrypt and Restrict a Virtual Machine on page 96

  You can encrypt a virtual machine to secure it from unauthorized use. You can also enable restrictions to prevent users from changing configuration settings.

- Remove Encryption from a Virtual Machine on page 97

  You can remove encryption from a virtual machine.

- Change the Password for an Encrypted Virtual Machine on page 98

  You can change the password for an encrypted virtual machine. Changing the password does not re-encrypt the virtual machine.

## Virtual Machine Encryption Limitations

The encryption feature has certain limitations.

- You must power off a virtual machine before you add or remove encryption or change the encryption password.
- The encryption feature supports virtual machines that have virtual hardware version 5.x or later only.
- You cannot create a linked clone from an encrypted virtual machine.

- If more than one unencrypted virtual machine shares the same virtual disk and you encrypt one of the virtual machines, the virtual disk becomes unusable for the unencrypted virtual machine.
- You cannot encrypt a shared or remote virtual machine.
- You cannot upload an encrypted virtual machine to a remote server.
- You cannot share an encrypted virtual machine.

## Encrypt and Restrict a Virtual Machine

You can encrypt a virtual machine to secure it from unauthorized use. You can also enable restrictions to prevent users from changing configuration settings.

Depending on the size of the virtual machine, the encryption process can take several minutes or several hours.

### Prerequisites

- Power off the virtual machine.
- Familiarize yourself with the encryption feature limitations. See "Virtual Machine Encryption Limitations," on page 95.
- Familiarize yourself with restricted virtual machine expirations. See "Restricted Virtual Machine Expiration," on page 97.

### Procedure

1. Select the virtual machine and select **VM > Settings**.
2. On the **Options** tab, select **Access Control**.
3. Click **Encrypt**.
4. Click **Encrypt**, enter an encryption password, and click **Encrypt**.

   The encryption password is required to gain access to the virtual machine. It does not prevent the user from changing the virtual machine configuration. Turn on restrictions and enter a password to prevent the user from changing the virtual machine configuration.

   **IMPORTANT** Record the encryption password you use. If you forget the password, Workstation does not provide a way to retrieve it.

   Workstation begins encrypting the virtual machine. After the encryption process is complete, you can optionally set a restrictions password.

5. (Optional) Select the **Enable Restrictions** check box to turn on restrictions.

| Option | Description |
|---|---|
| **Restrictions password** | You can set a password that prevents the user of the virtual machine from changing the virtual machine configuration. |
| **Require the user to change the encryption password** | Requires the user to change the encrypted password for the virtual machine if the virtual machine is moved or copied. |

| Option | Description |
|---|---|
| **Allow USB devices to be connected** | USB device connections are allowed. |
| **Expire the virtual machine** | Set a date and time for the virtual machine to expire by clicking the down arrow and selecting an expiration date. Click into the time field and enter the expiration time.<br>To enter an alert message:<br>a Click **Advanced**.<br>b Enter text to be displayed when the virtual machine expires.<br>c (Optional) Select the check box to show a message when the virtual machine is about to expire and enter message text.<br>d (Optional) Set the number of days before expiration that the message is displayed.<br>e Click **OK**. |

**IMPORTANT** Record the restrictions password you use. If you forget the password, Workstation does not provide a way to retrieve it.

6 Click **OK** in the Virtual Machine Settings dialog box.

### Restricted Virtual Machine Expiration

You can set an expiration date and time for an encrypted virtual machine.

When you set an expiration for an encrypted virtual machine, the local date and time are used. For example, December 12, 2012 11:00am in local time, with the time and date in Universal Time Coordinated (UTC) displayed below.

When an encrypted virtual machine with an expiration date is powered on, the virtual machine verifies the time and compares it to the expiration date. While running, the virtual machine periodically checks the time and stores all successful timestamps as the last trusted timestamp.

If the last trusted timestamp exceeds the date set for the virtual machine expiration, a warning message displays and the virtual machine is suspended.

Once a virtual machine has expired, the administrator of the virtual machine can delete or extend the expiration date. This requires the restrictions password.

## Remove Encryption from a Virtual Machine

You can remove encryption from a virtual machine.

#### Prerequisites

- Power off the virtual machine.
- Remove any sensitive information from the virtual machine.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Encryption**.

3 Click **Remove Encryption**.

4 Type the encryption password.

5 Click **Remove Encryption**.

### Change the Password for an Encrypted Virtual Machine

You can change the password for an encrypted virtual machine. Changing the password does not re-encrypt the virtual machine.

When you use this feature to change the password, the master key used to decrypt the virtual machine is not changed, and the virtual machine is not re-encrypted. For security reasons, instead of changing the password by using this procedure, you might choose to remove encryption and then encrypt the virtual machine again with a different password.

#### Prerequisites

Power off the virtual machine.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **Encryption**.

3 Select **Change Password**.

4 Type the current password and the new password.

IMPORTANT Make sure that you record the password. If you forget the password, Workstation does not provide a way to retrieve it.

## Moving Virtual Machines

You can move a virtual machine that was created in Workstation to a different host system or to a different location on the same host system. You can also use a virtual machine that was created in Workstation in VMware Player.

- Move a Virtual Machine to a New Location or Host on page 99

  You can move a virtual machine that was created in Workstation to a different host system or to a different location on the same host system. You can also move a virtual machine to a host system that has a different operating system.

- Use a Virtual Machine in VMware Player on page 100

  VMware® Player opens and plays virtual machines created in other VMware products. On Windows hosts, Player can also open and play Microsoft Virtual PC and Virtual Server virtual machines and Symantec LiveState Recovery and system images.

- Configure a Virtual Machine for Compatibility on page 101

  When you create a virtual machine that you intend to distribute to other users, you should configure the virtual machine for maximum compatibility with all expected host systems. Users might be limited in their ability to make changes in a virtual machine so that it is compatible with their host systems.

- Using the Virtual Machine UUID on page 101

  Each virtual machine has a universal unique identifier (UUID). The UUID is generated when you initially power on the virtual machine.

## Move a Virtual Machine to a New Location or Host

You can move a virtual machine that was created in Workstation to a different host system or to a different location on the same host system. You can also move a virtual machine to a host system that has a different operating system.

Moving a virtual machine typically involves moving the files that make up the virtual machine. The path names for all files associated with a Workstation virtual machine are relative to the virtual machine directory.

When you move a virtual machine to a different host system or to a different location on the same host system, Workstation generates a new MAC address for the virtual network adapter. Workstation also generates a new MAC address when you rename a directory in the path to the virtual machine configuration file.

### Prerequisites

- Familiarize yourself with how Workstation generates UUIDs for moved virtual machines. See "Using the Virtual Machine UUID," on page 101.
- If you are moving the virtual machine to a different host system, familiarize yourself with the limitations of moving a virtual machine to a new host. see "Limitations of Moving a Virtual Machine to a Different Host," on page 99.
- If you are moving a linked clone or a parent virtual machine, verify that the clone can access the parent virtual machine. See "Moving Linked Clones," on page 100 for more information.
- Make backup copies of the files in the virtual machine directory for the virtual machine that you are moving.

### Procedure

1 Verify that all virtual machine files are stored in the virtual machines directory.

  Some files might reside outside of the virtual machines directory.

2 Shut down the guest operating system and power off the virtual machine.

3 Copy the virtual machine files to the new location.

4 If you moved the virtual machine to a different location on the same host system, remove the virtual machine from the library, select **File > Open**, and browse to the virtual machine configuration (`.vmx`) file in its new location.

5 If you moved the virtual machine to a different host system, start Workstation on the new host system, select **File > Open** and browse to the virtual machine configuration (`.vmx`) file.

6 When you are certain that the virtual machine works correctly in its new location, delete the virtual machine files from its original location.

7 If the virtual machine does not work correctly, verify that you copied all of the virtual machine files to the new location.

  You can examine virtual machine device settings to determine whether any associated files point to locations that cannot be accessed from the new location.

## Limitations of Moving a Virtual Machine to a Different Host

You should be aware of certain limitations before you move a virtual machine to a different host system.

- The guest operating system might not work correctly if you move a virtual machine to a host system that has significantly different hardware, for example, if you move a virtual machine from a 64-bit host to a 32-bit host or from a multiprocessor host to a uniprocessor host.

- Workstation 7.x and later virtual machines support up to eight-way virtual symmetric multiprocessing (SMP) on multiprocessor host systems. You can assign up to eight virtual processors to virtual machines running on host systems that have at least two logical processors. If you attempt to assign two processors to a virtual machine that is running on a uniprocessor host system, a warning message appears. You can disregard this message and assign two processors to the virtual machine, but you must move it to a host that has at least two logical processors before you can power it on.
- You can move a virtual machine from a 32-bit host to a 64-bit host. You cannot move a virtual machine from a 64-bit host to a 32-bit host unless the 32-bit host has a supported 64-bit processor.

### Moving Linked Clones

If you move a linked clone, or if you move its parent virtual machine, make sure that the clone can access the parent virtual machine.

You cannot power on a linked clone if Workstation cannot locate the original virtual machine.

For example, if you put a linked clone on a laptop and the parent remains on another machine, you can use the clone only when the laptop connects to the network or drive where the parent is stored.

To use a cloned virtual machine on a disconnected laptop, you must use a full clone, or you must move the parent virtual machine to the laptop.

## Use a Virtual Machine in VMware Player

VMware® Player opens and plays virtual machines created in other VMware products. On Windows hosts, Player can also open and play Microsoft Virtual PC and Virtual Server virtual machines and Symantec LiveState Recovery and system images.

Player is included with Workstation. When you install Workstation, the Player application file is stored with the Workstation program files. On Windows hosts, the file is called `vmplayer.exe`. On Linux hosts, the file is called `vmplayer`.

NOTE You can download the standalone version of Player for free from the VMware Web site.

#### Prerequisites

Verify that the virtual machine compatible with Player. See "Configure a Virtual Machine for Compatibility," on page 101.

#### Procedure

1 Start Player.

| Option | Action |
|---|---|
| **From the GUI on a Windows host** | Select **Start > Programs > VMware > VMware Player**. |
| **From the command line on a Windows host** | Type ***path*\vmplayer.exe**, where *path* is the path to the application file. |
| **From a Linux X session** | Select **VMware Player** from the corresponding program menu, such as the **System Tools** menu. |
| **From the command line on a Linux host** | Type **vmplayer &**. |

2 Select **File > Open a Virtual Machine** and browse to the virtual machine configuration (`.vmx`) file.

3 Select the virtual machine and select **Virtual Machine > Power > Play Virtual Machine** to start the virtual machine in Player.

## Configure a Virtual Machine for Compatibility

When you create a virtual machine that you intend to distribute to other users, you should configure the virtual machine for maximum compatibility with all expected host systems. Users might be limited in their ability to make changes in a virtual machine so that it is compatible with their host systems.

### Procedure

- Install VMware Tools in the virtual machine.

  VMware Tools significantly improves the user's experience working with the virtual machine.

- Determine which virtual devices are actually required, and do not include any that are not needed or useful for the software you are distributing with the virtual machine.

  Generic SCSI devices are typically not appropriate.

- To connect a physical device to a virtual device, use the **Auto detect** options when you configure the virtual machine.

  The **Auto detect** options allow the virtual machine to adapt to the user's system, and they work whether the host operating system is Windows or Linux. Users who have no physical device receive a warning message.

- To connect a CD-ROM or floppy to an image file that you ship with the virtual machine, make sure the image file is in the same directory as the virtual machine.

  A relative path, rather than an absolute path, is used.

- For both a physical CD-ROM and an image, provide two virtual CD-ROM devices in the virtual machine.

  For example, Player does not provide an option to switch a single CD-ROM device between a physical CD-ROM and an image, and the user cannot switch between them if you plan to ship multiple images.

- Choose a reasonable amount of memory to allocate to the virtual machine.

  For example, if the host system does not have enough physical memory to support the memory allocation, the user cannot power on the virtual machine.

- Choose a reasonable screen resolution for the guest.

  A user is likely to find it easier to increase the resolution manually than to deal with a display that exceeds the user's physical screen size.

- To ensure that CD-ROMs work properly in virtual machines that you intend to distribute and play on Player, configure CD-ROM devices in legacy mode.

  Some host operating systems do not support CD-ROMs in non-legacy mode.

- When you configure a snapshot option for the virtual machine, select **Just power off** or **Revert to snapshot**.

  The **Revert to snapshot** option is useful if you want to distribute a demo virtual machine that resets itself to a clean state when it is powered off. Player does not allow taking snapshots.

## Using the Virtual Machine UUID

Each virtual machine has a universal unique identifier (UUID). The UUID is generated when you initially power on the virtual machine.

You can use the UUID of a virtual machine for system management in the same way that you use the UUID of a physical computer. The UUID is stored in the SMBIOS system information descriptor, and you can access it by using standard SMBIOS scanning software, including SiSoftware Sandra or IBM smbios2.

If you do not move or copy the virtual machine to another location, the UUID remains constant. When you power on a virtual machine that was moved or copied to a new location, you are prompted to specify whether you moved or copied the virtual machine. If you indicate that you copied the virtual machine, the virtual machine receives a new UUID.

Suspending and resuming a virtual machine does not trigger the process that generates a UUID. The UUID in use at the time the virtual machine was suspended remains in use when the virtual machine is resumed, even if it was copied or moved. You are not prompted to specify whether you moved or copied the virtual machine until the next time you reboot the virtual machine.

## Configure a Virtual Machine to Always Receive a New UUID

You can configure a virtual machine to always receive a new UUID when it is copied or moved so that you are not prompted when you move or copy the virtual machine.

### Prerequisites

Power off the virtual machine.

### Procedure

1 Open the virtual machine configuration (`.vmx`) file in a text editor.

2 Add the **`uuid.action`** property to the `.vmx` file and set it to `create`.

For example: **`uuid.action = "create"`**

## Configure a Virtual Machine to Keep the Same UUID

You can configure a virtual machine to always keep the same UUID, even when it is moved or copied. When a virtual machine is set to always keep the same UUID, you are not prompted when a virtual machine is moved or copied.

### Prerequisites

Power off the virtual machine.

### Procedure

1 Open the virtual machine configuration (`.vmx`) file in a text editor.

2 Add the `uuid.action` property and set it to **`keep`**.

For example: **`uuid.action = "keep"`**

## Override the Generated UUID for a Virtual Machine

You can override the generated UUID and assign a specific UUID to a virtual machine.

### Prerequisites

Power off the virtual machine.

### Procedure

1 Open the virtual machine configuration (`.vmx`) file in a text editor.

2 Search for the line that contains `uuid.bios`.

The format of the line is `uuid.bios = "`*`uuid_value`*`"`. The UUID is a 128-bit integer. The 16 bytes are separated by spaces, except for a dash between the eighth and ninth hexadecimal pairs.

For example: `uuid.bios = "00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff"`

3 Replace the existing UUID value with the specific UUID value.

4 Power on the virtual machine.

The virtual machine uses new UUID is used when it reboots.

# Configure a Virtual Machine as a VNC Server

You can use Workstation to configure a virtual machine to act as a VNC server so that users on other computers can use a VNC client to connect to the virtual machine. You do not need to install specialized VNC software in a virtual machine to set it up as a VNC server.

**NOTE** You cannot configure a shared or remote virtual machine as a VNC server.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **VNC Connections** and select **Enable VNC**.

3 (Optional) To allow VNC clients to connect to multiple virtual machines on the same host system, specify a unique port number for each virtual machine.

Use should use a port number in the range from 5901 to 6001. Other applications use certain port numbers, and some port numbers are privileged. For example, the VMware Management Interface uses ports 8333 and 8222 and VMware Workstation Server uses port 443. On Linux, only the root user can listen to ports up to port number 1024.

4 (Optional) Set a password for connecting to the virtual machine from a VNC client.

The password can be up to eight characters long. Because it is not encrypted when the VNC client sends it, do not use a password that you use for other systems.

5 (Optional) Click **View VNC Connections** to see a list of the VNC clients that are remotely connected to the virtual machine and find out how long they have been connected.

6 Click **OK** to save your changes.

### What to do next

If you do not VNC clients use to use the US101 keyboard map (U.S. English) when they connect to the virtual machine, specify a different language. See "Specify a Language Keyboard Map for VNC Clients," on page 103.

## Specify a Language Keyboard Map for VNC Clients

If you set a virtual machine to act as a VNC server, you can specify which language to use for the keyboard that VNC clients use. By default, the US101 keyboard map (U.S. English) is used.

### Prerequisites

- Verify that the virtual machine is set to act as a VNC server.
- Determine the language code to use. See "Language Codes," on page 104.

### Procedure

1 In a text editor, open the virtual machine configuration file (`.vmx`) file for the virtual machine and add the `RemoteDisplay.vnc.enabled` and `RemoteDisplay.vnc.port` properties.

   a Set `RemoteDisplay.vnc.enabled` to TRUE.

   b Set `RemoteDisplay.vnc.port` to the port number to use.

   For example:

```
RemoteDisplay.vnc.enabled = "TRUE"
RemoteDisplay.vnc.port = "portnumber"
```

2 Determine the location of the keymap file to use.

   Default keymap files are included in the Workstation installation directory.

| Host System | Keymap File Location |
|---|---|
| **Windows XP host** | `C:\Documents and Settings\All Users\Application Data\VMware\vnckeymap` |
| **Windows Vista and Windows 7 hosts** | `C:\ProgramData\VMware\vnckeymap` |
| **Linux host** | `C:\ProgramData\VMware\vnckeymap` |

3 In the virtual machine configuration (`.vmx`) file, add a property to specify the location of the keymap file.

| Option | Description |
|---|---|
| **To use the default keymap file included in the Workstation installation directory** | Add **`RemoteDisplay.vnc.keyMap = "xx"`**, where *xx* is the code for the language to use, such as **`jp`** for Japanese. |
| **To use a keyboard map file in another location** | Add **`RemoteDisplay.vnc.keyMapFile = "filepath"`**, where *filepath* is the absolute file path. |

4 Start the virtual machine and connect to it from a VNC client.

## Language Codes

When you specify a language keyboard map for VNC clients, you must specify a language code.

**Table 3-1.** Language Codes

| Code | Language |
|---|---|
| `de` | German |
| `de-ch` | German (Switzerland) |
| `es` | Spanish |
| `fi` | Finnish |
| `fr` | French |
| `fr-be` | French (Belgium) |
| `fr-ch` | French (Switzerland) |
| `is` | Icelandic |
| `it` | Italian |
| `jp` | Japanese |
| `nl-be` | Dutch (Belgium) |

**Table 3-1.** Language Codes (Continued)

| Code | Language |
|---|---|
| no | Norwegian |
| pt | Polish |
| uk | UK English |
| us | US English |

## Use a VNC Client to Connect to a Virtual Machine

You can use a VNC client to connect to a running virtual machine. Because VNC software is cross-platform, you can use virtual machines running on different types of computers.

Workstation does not need to be running to use VNC to connect to a virtual machine. Only the virtual machine needs to be running, and it can be running in the background.

When you use a VNC client to connect to a virtual machine, some features do not work or are not available.

- You cannot take or revert to snapshots.
- You cannot power on, power off, suspend, or resume the virtual machine. You can shut down the guest operating system. Shutting down might power off the virtual machine.
- You cannot copy and paste text between the host system and the guest operating system.
- You cannot change virtual machine settings.
- Remote display does not work well if you are also using the 3D feature.

### Prerequisites

- Configure the virtual machine as a VNC server. See "Configure a Virtual Machine as a VNC Server," on page 103.
- Determine the machine name or IP address of the host system on which the virtual machine is running and, if required, the VNC port number and password.

### Procedure

1 Install a VNC client on your computer.

   Open-source versions of VNC are freely and publicly available. You can use any VNC client, but not a Java viewer in a browser.

2 Start the VNC client on your computer.

3 Verify that the client is set for hextile encoding.

   For example, if you use RealVNC Viewer, select **Hextile** under the **Preferred Encoding** option.

4 Set the VNC client to use all colors.

   For example, if you use RealVNC Viewer, select **Full (all available colours)** under the **Colour Level** option.

5 When prompted for the VNC server name, type the name or IP address and the port number of the host system where the virtual machine is running.

   For example: ***machine_name:port_number***

6 Type a password if one is required.

## View VNC Connections for a Virtual Machine

When a virtual is configured to act as a VNC server, you can view a list of the VNC clients that are remotely connected to the virtual machine and find out how long they have been connected.

### Prerequisites

Configure the virtual machine to act as a VNC server. See "Configure a Virtual Machine as a VNC Server," on page 103.

### Procedure

- Select the virtual machine and select **VM > Manage > VNC Connections**.

# Change the Hardware Compatibility of a Virtual Machine

You can change the hardware compatibility of a virtual machine. All virtual machines have a hardware version. The hardware version indicates which virtual hardware features that the virtual machine supports, such as BIOS or EFI, number of virtual slots, maximum number of CPUs, maximum memory configuration, and other hardware characteristics.

When you upgrade Workstation, you must change the hardware compatibility of virtual machines that were created in previous versions of Workstation so that they can use the new features in the new version of Workstation. You can run older versions of virtual machines in the new version of Workstation, but you will not have the benefits of the new features.

If you want a virtual machine to remain compatible with other VMware products that you are using, you might not want to change the hardware compatibility to the latest Workstation version.

**NOTE** If you decide not to change the hardware compatibility of a virtual machine, you should consider upgrading to the latest version of VMware Tools to obtain the latest VMware Tools features.

### Prerequisites

Familiarize yourself with the considerations and limitations of changing the hardware compatibility of a virtual machine. See "Considerations for Changing the Hardware Compatibility of a Virtual Machine," on page 107.

### Procedure

1. Make backup copies of the virtual disk (`.vmdk`) files.
2. If you are upgrading from a Workstation 4 or 5.x virtual machine, or downgrading to a Workstation 4 or 5.x virtual machine, make a note of the NIC settings in the guest operating system.

   If you specified a static IP address for the virtual machine, that setting might be changed to automatic assignment by DHCP after the upgrade.
3. Shut down the guest operating system and power off the virtual machine.
4. Select the virtual machine and select **VM > Manage > Change Hardware Compatibility**.
5. Follow the prompts in the wizard to change the hardware compatibility of the virtual machine.

   When you select a hardware compatibility setting, a list of the VMware products that are compatible with that setting appears. For example, if you select Workstation 4, 5, or 6, a list of Workstation 6.5 and later features that are not supported for that Workstation version also appears.

   **NOTE** Using Workstation 10, you can change the hardware compatibility of a shared or remote virtual machine. However, you cannot down grade a previously created virtual machine.

6 Power on the virtual machine.

If you upgrade a virtual machine that contains a Windows 98 operating system to a Workstation 6.5 or later virtual machine, you must install a PCI-PCI bridge driver when you power on the virtual machine.

**NOTE** Because Workstation 6.5 and later versions have 32 more PCI-PCI bridges than Workstation 6, you might need to respond to the prompt 32 or 33 times.

7 If the NIC settings in the guest operating system have changed, use the NIC settings that you recorded to change them back to their original settings.

8 If the virtual machine does not have the latest version of VMware Tools installed, update VMware Tools.

You should update VMware Tools to the version included with the latest version of Workstation, even if you upgraded the virtual machine to an earlier version of Workstation. Do not remove the older version of VMware Tools before installing the new version.

**NOTE** If you are upgrading a virtual machine that runs from a physical disk, you can safely ignore this message: `Unable to upgrade drive_name. One of the supplied parameters is invalid.`

### Considerations for Changing the Hardware Compatibility of a Virtual Machine

Before you change the hardware compatibility of a virtual machine, you should be aware of certain considerations and limitations.

- For Workstation 5.x, 6, 6.5, 7.x, and later virtual machines, you can change the version of the original virtual machine or create a full clone so that the original virtual machine remains unaltered. For Workstation 4 virtual machines, Workstation changes the original virtual machine.
- If you upgrade a Workstation 4 or 5.x virtual machine that is compatible with ESX Server to Workstation 6, 6.5, 7.x, or later, you cannot use the Change Hardware Compatibility wizard to later downgrade the virtual machine to an ESX-compatible virtual machine.
- When you upgrade a Windows XP, Windows Server 2003, Windows Vista, or Windows 7 virtual machine, the Microsoft product activation feature might require you to reactivate the guest operating system.
- Using Workstation 9 or earlier, you cannot change the hardware compatibility of a shared or remote virtual machine.
- Using Workstation 10 and later, you can change the hardware compatibility of a shared or remote virtual machine. However, you cannot down grade a previously created virtual machine.

## Clean Up a Virtual Hard Disk on Windows Hosts

When you delete files from your virtual machine, the disk space occupied by those files is not immediately returned to your host system. If a virtual disk has such empty space, you can use the **Clean up disks** command to return that space to the hard drive on a Microsoft Windows host.

The **Clean up disks** command is similar to the **Compact** command in the Workstation virtual machine settings and the **shrink** command provided by VMware Tools. The **Clean up disks** command has these advantages:

- You can use the **Clean up disks** command with virtual machines that have snapshots or are linked clones or parents of a linked clone.
- The **Clean up disks** command reclaims more disk space than the **Compact** command.

The **Clean up disks** command reclaims disk space from the current state of the virtual machine, from any powered-off snapshots, and from any powered-on snapshots where the guest operating system is Windows XP or later and you have installed a version of VMware Tools that is compatible with Workstation 8 or later.

- Unlike the **Defragment** command and the **shrink** command provided by VMware Tools, the **Clean up disks** command does not require any extra disk space on the host. The **Clean up disks** command operates directly on the virtual disk (`.vmdk`) files.

**NOTE** This command is not available for shared or remote virtual machines.

### Prerequisites

- Verify that you are using a Windows host and that the guest operating system uses NTFS. (NTFS is standard in Windows XP or later operating systems.) This feature works on all NTFS hard disks but reclaims more disk space if the operating system is Windows XP or later.
- Shut down or power off the virtual machine. You cannot use this command while the virtual machine is powered on or suspended.

### Procedure

1 Select the virtual machine in the library.

2 From the menu bar, select **VM > Manage > Clean Up Disks**.

Workstation calculates how much space can be reclaimed, and either the **Clean Up Now** button becomes available or a message appears, explaining why the command is unavailable.

3 Click **Clean Up Now** to start the process.

A dialog box reports the progress of the clean-up process.

## Export a Virtual Machine to OVF Format

You can export a virtual machine from Workstation to OVF format.

OVF is a platform-independent, efficient, extensible, and open packaging and distribution format for virtual machines. OVF format provides a complete specification of the virtual machine, including the full list of required virtual disks and the required virtual hardware configuration, including CPU, memory, networking, and storage. An administrator can quickly provision an OVF-formatted virtual machine with little or no intervention.

You can also use the standalone OVF Tool to convert a virtual machine that is in VMware runtime format to an OVF virtual machine. The standalone version of the OVF Tool is installed in the Workstation installation directory under `OVFTool`. See the *OVF Tool User Guide* on the VMware Web site for information about using the OVF Tool.

### Prerequisites

- Verify that the virtual machine is not encrypted. You cannot export an encrypted virtual machine to OVF format.
- Verify that the virtual machine is powered off.

### Procedure

1 Select the virtual machine and select **File > Export to OVF**.

2 Type a name for the OVF file and specify a directory in which to save it.

3 Click **Save** to start the OVF export process.

The export process can take several minutes. A status bar indicates the progress of the export process.

# Writing and Debugging Applications That Run In Virtual Machines

Application developers can use APIs, SDKs, and IDEs to write and debug applications that run in virtual machines.

**VIX API**

You can use the VIX API to write programs that automate virtual machine operations. The API is easy to use and useful for both script writers and application programmers. Functions enable you to power virtual machines on and off, register them, and run programs to manipulate files in the guest operating systems. Additional language bindings are available for Perl, COM, and shell scripts (for example, `vmrun`).

**VProbes Tool**

You can use the VProbes tool to investigate guest behavior. You can write VProbes scripts that inspect and record activities in the guest, VMX, and virtual devices, without interfering with run-state. For example, VProbes can track which applications are running or indicate which processes are causing page faults. See the *VProbes Programming Reference*.

**VMCI Sockets Interface**

VMCI Sockets is a network sockets API for the Virtual Machine Communication Interface. It provides a fast means of communication between a host and its guest virtual machines. This API is well-suited for client-server applications. See the *VMCI Sockets Programming Guide*.

**Integrated Virtual Debuggers for Visual Studio and Eclipse**

The integrated development environment (IDE) plug-ins provide a configurable interface between virtual machines and Visual Studio or Eclipse. They let you test, run, and debug programs in virtual machines. See the *Integrated Virtual Debugger for Eclipse Developer's Guide* and the *Integrated Virtual Debugger for Visual Studio Developer's Guide*.

## Debugging Over a Virtual Serial Port

You can use virtual machines to debug kernel code on one system without the need for two physical computers, a modem, or a serial cable. You can use Debugging Tools for Windows (WinDbg) or Kernel Debugger (KD) to debug kernel code in a virtual machine over a virtual serial port.

You can Download Debugging Tools for Windows from the Windows Hardware Developer Central (WHDC) Web site.

### Debug an Application in a Virtual Machine from a Windows Host

You can debug an application in a virtual machine from a Windows host system over a virtual serial port.

#### Prerequisites

- Verify that Debugging Tools for Windows is installed on the host system and that it supports debugging over a pipe. It must be version 5.0.18.0 or later.
- Verify that a serial port is configured for the virtual machine. See "Configuring Virtual Ports," on page 125.

#### Procedure

1. Configure the named pipe on the target virtual machine and select **This end is the server**.
2. Power on the virtual machine.
3. Select the virtual machine, select **VM > Removable Devices**, and verify that the serial port is connected.
4. If the serial port is not reported as `\\.\pipe\`*`namedpipe`*, select the virtual serial port and click **Connect**.

5 On the host system, type the debugger command.

For example: ***debugger*** **-k com:port=\\.\pipe*** ***namedpipe*** **,pipe**

The *debugger* value is `WinDbg` or `KD`.

6 Press Enter to start debugging.

## Debug an Application in a Virtual Machine from Another Virtual Machine

You can use the WinDbg or KD debugger to debug an application in a virtual machine from another virtual machine over a serial port.

### Prerequisites

- Download and install WinDbg or KD in the Windows guest operating system that you plan to use as the debugger virtual machine.
- Verify that a serial port is configured for the virtual machine. See "Configuring Virtual Ports," on page 125.

### Procedure

1 Power on both virtual machines.

2 Select the virtual machine and select **VM > Removable Devices** to verify that the serial port is connected.

3 If the serial port is not connected, select the virtual serial port and click **Connect**.

4 In the debugger virtual machine, start debugging by using WinDbg or KD.

# Configuring and Managing Devices 4

You can use Workstation to add devices to virtual machines, including DVD and CD-ROM drives, floppy drives, USB controllers, virtual and physical hard disks, parallel and serial ports, generic SCSI devices, and processors. You can also modify settings for existing devices.

This chapter includes the following topics:


- "Configuring DVD, CD-ROM, and Floppy Drives," on page 111
- "Configuring a USB Controller," on page 113
- "Configuring and Maintaining Virtual Hard Disks," on page 116
- "Adding a Physical Disk to a Virtual Machine," on page 122
- "Configuring Virtual Ports," on page 125
- "Configuring Generic SCSI Devices," on page 129
- "Configuring Eight-Way Virtual Symmetric Multiprocessing," on page 133
- "Configuring Keyboard Features," on page 134
- "Modify Hardware Settings for a Virtual Machine," on page 143


## Configuring DVD, CD-ROM, and Floppy Drives

You can add up to 4 IDE devices, up to 60 SCSI devices, and up to 120 SATA devices (4 controllers with 30 devices per controller) to a virtual machine. Any of these devices can be a virtual or physical hard disk or DVD or CD-ROM drive. By default, a floppy drive is not connected when a virtual machine powers on.

A virtual machine can read data from a DVD disc. Workstation does not support playing DVD movies in a virtual machine. You might be able to play a movie if you use a DVD player application that does not require video overlay support in the video card.

### Add a DVD or CD-ROM Drive to a Virtual Machine

You can add one or more DVD or CD-ROM drives to a virtual machine. You can connect the virtual DVD or CD-ROM drive to a physical drive or an ISO image file.

You can configure the virtual DVD or CD-ROM drive as an IDE or a SCSI device, regardless of the type of physical drive that you connect it to. For example, if the host has an IDE CD-ROM drive, you can set up the virtual machine drive as either SCSI or IDE and connect it to the host drive.

Do not configure legacy emulation mode unless you experience problems with normal mode. See "Configure Legacy Emulation Mode for a DVD or CD-ROM Drive," on page 113 for more information.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 In the Add Hardware wizard, select **DVD/CD Drive**.

4 Select a physical drive or ISO image file to connect to the drive.

| Option | Description |
|---|---|
| **Use physical drive** | The virtual machine uses a physical drive. |
| **Use ISO image** | The drive connects to an ISO image file. |

5 Configure the physical drive or ISO image file.

| Option | Description |
|---|---|
| **Physical drive** | Select a specific drive, or select **Auto detect** to allow Workstation to auto-detect the drive to use. |
| **ISO image file** | Type the path or browse to the location of the ISO image file. |

6 To connect the drive or ISO image file to the virtual machine when the virtual machine powers on, select **Connect at power on**.

7 Click **Finish** to add the drive to the virtual machine.

The drive initially appears as an IDE drive to the guest operating system.

8 (Optional) To change which SCSI or IDE device identifier to use for the drive, select the drive and click **Advanced**.

9 Click **OK** to save your changes.

## Add a Floppy Drive to a Virtual Machine

You can configure a virtual floppy drive to connect to a physical floppy drive or an existing or blank floppy image file. You can add up to two floppy drives to a virtual machine.

### Prerequisites

Power off the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 In the Add Hardware wizard, select **Floppy Drive**.

4 Select the floppy media type.

| Option | Description |
|---|---|
| **Use a physical floppy drive** | The virtual machine uses a physical floppy drive. |
| **Use a floppy image** | The drive connects to an floppy image (`.flp`) file. |
| **Create a blank floppy image** | The drive connects to a blank floppy image (`.flp`) file that you create. |

5 If you selected the physical floppy drive media type, select a specific floppy drive or select **Auto detect** to allow Workstation to auto-detect the drive to use.

6 If you selected the floppy image or blank floppy image media type, type the name or browse to the location of a floppy image (`.flp`) file.

7 To connect the drive or floppy image file to the virtual machine when the virtual machine powers on, select **Connect at power on**.

8 Click **Finish** to add the drive to the virtual machine.

9 Click **OK** to save your changes.

10 If you added a second floppy drive to the virtual machine, enable the drive in the virtual machine BIOS.

   a Select the virtual machine and select **VM > Power > Power On to BIOS**.

   b Select **Legacy Diskette B:** and use the plus (+) and minus (-) keys on the numerical keypad to select the type of floppy drive to use.

   c Press F10 to save the settings.

### Configure Legacy Emulation Mode for a DVD or CD-ROM Drive

Use legacy emulation mode to work around direct communication problems between a guest operating system and a DVD or CD-ROM drive.

In legacy emulation mode, you can read only from data discs in the DVD or CD-ROM drive. Legacy emulation mode does not provide the other capabilities of normal mode. In normal mode, the guest operating system communicates directly with the CD-ROM or DVD drive. This direct communication enables you to read multisession CDs, perform digital audio extraction, view videos, and use CD and DVD writers to burn discs.

If you run more than one virtual machine at a time, and if their CD-ROM drives are in legacy emulation mode, you must start the virtual machines with their CD-ROM drives disconnected. By disconnecting the CD-ROM drives in the virtual machines, you prevent multiple virtual machines from being connected to the CD-ROM drive at the same time.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select the drive and click **Advanced**.

3 Select **Legacy emulation** and click **OK**.

   On Windows hosts, this option is deselected by default. On Linux hosts that have IDE drives, the default setting depends on whether the `ide-scsi` module is loaded in the kernel. The `ide-scsi` module must be loaded, or you must use a physical SCSI drive, to connect directly to the DVD or CD-ROM drive.

4 Click **OK** to save your changes.

## Configuring a USB Controller

A virtual machine must have a USB controller to use USB devices and smart card readers. To use a smart card reader, a virtual machine must have a USB controller regardless of whether the smart card reader is actually a USB device.

Workstation provides a USB controller to support the following types of USB devices.

- USB 1.1 UHCI (Universal Host Controller Interface) is supported for all virtual machine hardware versions.
- USB 2.0 EHCI (Enhanced Host Controller Interface) controllers are supported if the virtual machine hardware is compatible with Workstation 6 and later virtual machines.

- USB 3.0 xHCI (Extensible Host Controller Interface) support is available for Linux guests running kernel version 2.6.35 or later and for Windows 8 guests. The virtual machine hardware must be compatible with Workstation 8 or later virtual machines.

For USB 2.0 or 3.0 support, you must select USB 2.0 or 3.0 compatibility by configuring virtual machine settings for the USB controller. USB 2.0 and 3.0 devices are high-speed devices that include the latest models of USB flash drives, USB hard drives, iPods, and iPhone.

If you select USB 2.0 compatibility, when a USB 2.0 device connects to a USB port on the host system, the device connects to the EHCI controller and operates in USB 2.0 mode. A USB 1.1 device connects to the UHCI controller and operates in USB 1.1 mode. If you enable USB 3.0, the xHCI controller can support all USB devices, including USB 1.1, 2.0, and 3.0 devices.

Although the host operating system must support USB, you do not need to install device-specific drivers for USB devices in the host operating system to use those devices only in the virtual machine. Windows NT and Linux kernels earlier than 2.2.17 do not support USB.

VMware has tested a variety of USB devices. If the guest operating system has the appropriate drivers, you can use many different USB devices, including PDAs, Smart phones, printers, storage devices, scanners, MP3 players, digital cameras, memory card readers, and isochronous transfer devices, such as webcams, speakers, and microphones.

You can connect USB human interface devices (HIDs), such as the keyboard and mouse, to a virtual machine by enabling the **Show all USB input devices** option. If you do not select this option, these devices do not appear in the **Removable Devices** menu and are not available to connect to the virtual machine, even though they are plugged in to USB ports on the host system.

See "Connect USB HIDs to a Virtual Machine," on page 63 for information on connecting HIDs.

## Add a USB Controller to a Virtual Machine

A USB controller is required to use a smart card in a virtual machine, regardless of whether the smart card reader is a USB device. You can add one USB controller to a virtual machine.

When you create a virtual machine in Workstation, a USB controller is added by default. If you remove the USB controller, you can add it back.

**NOTE** Shared and remote virtual machines are created without a USB controller by default. You can add a USB controller manually after you finish creating a shared or remote virtual machine.

### Prerequisites

Power off the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 In the New Hardware wizard, select **USB Controller**.

4 Configure the USB connection settings.

You can select multiple settings.

NOTE You typically cannot configure USB connection settings for a shared or remote virtual machine.

| Option | Description |
|---|---|
| **USB Compatibility** | Selecting USB 2.0 or 3.0 enables support for isochronous USB devices, including Web cams, speakers, and microphones. |
| **Automatically connect new USB devices** | Connect new USB devices to the virtual machine. If this setting is not selected, new USB devices are connected only to the host system. |
| **Show all USB input devices** | Human interface devices (HIDs), such as USB 1.1 and 2.0 mouse and keyboard devices, appear in the **Removable Devices** menu. Icons for HIDs appear in the status bar. An HID that is connected to the guest operating system is not available to the host system. The virtual machine must be powered off when you change this setting. |
| **Share Bluetooth devices with the virtual machine** | Enable support for Bluetooth devices. |

5 Click **Finish** to add the USB controller.

## Enable Support for Isochronous USB Devices

Modems and certain streaming data devices, such as speakers and webcams, do not work properly in a virtual machine unless you enable support for isochronous USB devices.

### Prerequisites

- Verify that the virtual machine is a Workstation 6.x or later virtual machine. Isochronous USB devices are supported in Workstation 6.x and later virtual machines only.
- Verify that the guest operating system supports USB 2.0 devices or 3.0 devices.
- On a Windows XP guest operating system, verify that the latest service pack is installed. If you use Windows XP with no service packs, the driver for the EHCI controller cannot be loaded.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **USB Controller**.

3 From the **USB Compatibility** list, select **USB 2.0** or **USB 3.0**.

| Option | Description |
|---|---|
| **USB 2.0** | Available if the virtual machine hardware is compatible with Workstation 6 and later virtual machines. |
| **USB 3.0** | Available for Linux guests running kernel version 2.6.35 or later and for Windows 8 guests. The virtual machine hardware must be compatible with Workstation 8 and later virtual machines. |

4 Click **OK** to save your changes.

# Configuring and Maintaining Virtual Hard Disks

You can use Workstation to configure virtual hard disk storage for virtual machines.

A virtual disk is a file or set of files that appears as a physical disk drive to a guest operating system. The files can be on the host system or on a remote computer. When you configure a virtual machine to use a virtual disk, you can install a new operating system onto the virtual disk without repartitioning a physical disk or rebooting the host.

The New Virtual Machine wizard creates a virtual machine that has one disk drive. You can modify virtual machine settings to add more disk drives to a virtual machine, remove disk drives from a virtual machine, and change certain settings for the existing disk drives.

- Configuring a Virtual Hard Disk on page 117

  You can configure virtual hard disks as IDE or SATA disks for any guest operating system. You can also set up a virtual hard disk as a SCSI disk for any guest operating system that has a driver for the LSI Logic or BusLogic SCSI adapter. You determine which SCSI adapter to use when you create a virtual machine.

- Compact a Virtual Hard Disk on page 119

  Compacting a virtual hard disk reclaims unused space in the virtual disk. If a disk has empty space, this process reduces the amount of space the virtual disk occupies on the host drive.

- Expand a Virtual Hard Disk on page 119

  You can add storage space to a virtual machine by expanding its virtual hard disk.

- Defragment a Virtual Hard Disk on page 120

  Like physical disk drives, virtual hard disks can become fragmented. Defragmenting disks rearranges files, programs, and unused space on the virtual hard disk so that programs run faster and files open more quickly. Defragmenting does not reclaim unused space on a virtual hard disk.

- Remove a Virtual Hard Disk from a Virtual Machine on page 121

  Removing a virtual hard disk disconnects it from a virtual machine. It does not delete files from the host file system.

- Using Virtual Disk Manager on page 121

  Virtual Disk Manager (`vmware-diskmanager`) is a Workstation utility that you can use to create, manage, and modify virtual disk files from the command line or in scripts.

- Using Legacy Virtual Disks on page 121

  You can use the current version of Workstation in a mixed environment with virtual machines that were created with earlier versions of Workstation or with other VMware products.

- Using Lock Files to Prevent Consistency Problems on Virtual Hard Disks on page 122

  A running virtual machine creates lock files to prevent consistency problems on virtual hard disks. Without locks, multiple virtual machines might read and write to the disk, causing data corruption.

- Moving a Virtual Hard Disk to a New Location on page 122

  A key advantage of virtual hard disks is their portability. Because the virtual hard disks are stored as files on the host system or a remote computer, you can move them easily to a new location on the same computer or to a different computer.

# Configuring a Virtual Hard Disk

You can configure virtual hard disks as IDE or SATA disks for any guest operating system. You can also set up a virtual hard disk as a SCSI disk for any guest operating system that has a driver for the LSI Logic or BusLogic SCSI adapter. You determine which SCSI adapter to use when you create a virtual machine.

The files that make up an IDE, SATA, or SCSI virtual hard disk can be stored on an IDE hard disk, SATA hard disk, or on a SCSI hard disk. They can also be stored on other types of fast-access storage media.

To use SCSI hard disks in a 32-bit Windows XP virtual machine, you must download a special SCSI driver from the VMware Web site. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP.

## Growing and Allocating Virtual Disk Storage Space

IDE and SCSI virtual hard disks can be up to 8TB. Depending on the size of the virtual hard disk and the host operating system, Workstation creates one or more files to hold each virtual disk.

Virtual hard disk files include information such as the operating system, program files, and data files. Virtual disk files have a `.vmdk` extension.

By default, the actual files that the virtual hard disk uses start small and grow to their maximum size as needed. The main advantage of this approach is the smaller file size. Smaller files require less storage space and are easier to move to a new location, but it takes longer to write data to a disk configured in this way.

You can also configure virtual hard disks so that all of the disk space is allocated when the virtual disk is created. This approach provides enhanced performance and is useful if you are running performance-sensitive applications in the virtual machine.

Regardless of whether you allocate all disk space in advance, you can configure the virtual hard disk to use a set of files limited to 2GB per file. Use this option if you plan to move the virtual hard disk to a file system that does not support files larger than 2GB.

## Add a New Virtual Hard Disk to a Virtual Machine

To increase storage space, you can add a new virtual hard disk to a virtual machine. You can add up to four IDE devices and up to 60 SCSI devices. Any of these devices can be a virtual or physical hard disk or DVD or CD-ROM drive.

Virtual hard disks are stored as files on the host computer or on a network file server. A virtual IDE drive or SCSI drive can be stored on a physical IDE drive or on a physical SCSI drive.

If you have a Windows NT 4.0 virtual machine that has a SCSI virtual hard disk, you cannot add both an additional SCSI disk and an IDE disk to the configuration.

As an alternative to adding a new virtual hard disk, you can expand the existing virtual hard disk. See "Expand a Virtual Hard Disk," on page 119.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 In the New Hardware wizard, select **Hard Disk**.

4 Select **Create a new virtual disk**.

5 Select the disk type.

| Option | Description |
|---|---|
| **IDE** | Create an IDE device. You can add up to four IDE devices to a virtual machine. |
| **SCSI** | Create a SCSI device. You can add up to 60 SCSI devices to a virtual machine. |
| **SATA** | Create a SATA device. You can add up to 120 SATA devices: four controllers and 30 devices per controller. |

6 (Optional) To exclude the disk from snapshots, select **Independent** for the mode and select a persistence option.

| Option | Description |
|---|---|
| **Persistent** | Disks in persistent mode behave like conventional disks on a physical computer. All data written to a disk in persistent mode is written permanently to the disk. |
| **Nonpersistent** | Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you always restart the virtual machine with a virtual disk in the same state. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset the virtual machine. |

7 Set the capacity for the new virtual hard disk.

You can set a size between 0.001GB and 8TB for a virtual disk.

8 Specify how to allocate the disk space.

| Option | Description |
|---|---|
| **Allocate all disk space now** | Allocating all of the disk space when you create the virtual hard disk can enhance performance, but it requires all of the physical disk space to be available now. If you do not select this setting, the virtual disk starts small and grows as you add data to it. |
| **Store virtual disk as a single file** | Select this option if the virtual disk is stored on a file system that does not have a file size limitation. |
| **Split virtual disk into multiple files** | Select this option if the virtual disk is stored on a file system that has a file size limitation. When you split a virtual disk less than 950GB, a series of 2GB virtual disk files are created. When you split a virtual disk greater than 950GB, two virtual disk files are created. The maximum size of the first virtual disk file is 1.9TB and the second virtual disk file stores the rest of the data. |

9 Accept the default filename and location, or browse to and select a different location.

10 Click **Finish** to add the new virtual hard disk.

The wizard creates the new virtual hard disk. The disk appears to the guest operating system as a new, blank hard disk.

11 Click **OK** to save your changes.

12 Use the guest operating system tools to partition and format the new drive.

### Add an Existing Virtual Hard Disk to a Virtual Machine

You can reconnect an existing virtual hard disk that was removed from a virtual machine.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 In the Add Hardware wizard, select **Hard Disk**.

4 Select **Use an existing virtual disk**.

5 Specify the path name and filename for the existing disk file.

6 Click **Finish** to add the existing virtual hard disk.

7 Click **OK** to save your changes.

## Compact a Virtual Hard Disk

Compacting a virtual hard disk reclaims unused space in the virtual disk. If a disk has empty space, this process reduces the amount of space the virtual disk occupies on the host drive.

#### Prerequisites

- Power off the virtual machine.
- Verify that the virtual disk is not mapped or mounted. You cannot compact a virtual disk while it is mapped or mounted.
- Verify that the disk space is not preallocated for the virtual hard disk. If the disk space was preallocated, you cannot compact the disk.
- If the virtual hard disk is an independent disk, verify that it is in persistent mode.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select the virtual hard disk to compact.

3 Select **Utilities > Compact**.

4 Click **OK** after the disk compacting process is complete.

## Expand a Virtual Hard Disk

You can add storage space to a virtual machine by expanding its virtual hard disk.

When you expand a virtual hard disk, the added space is not immediately available to the virtual machine. To make the added space available, you must use a disk management tool to increase the size of the existing partition on the virtual hard disk to match the expanded size.

The disk management tool that you use depends on the virtual machine guest operating system. Many operating systems, including Windows Vista, Windows 7, and Windows 8 and some versions of Linux, provide built-in disk management tools that can resize partitions. Third-party disk management tools are also available, such as EASEUS Partition Master, Acronis Disk Director, and the open-source tool GParted.

When you expand the size of a virtual hard disk, the sizes of partitions and file systems are not affected.

As an alternative to expanding a virtual hard disk, you can add a new virtual hard disk to the virtual machine. See "Add a New Virtual Hard Disk to a Virtual Machine," on page 117.

### Prerequisites

- Power off the virtual machine.
- Verify that the virtual disk is not mapped or mounted. You cannot expand a virtual disk while it is mapped or mounted.
- Verify that the virtual machine has no snapshots.
- Verify that the virtual machine is not a linked clone or the parent of a linked clone.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select the virtual hard disk to expand.

3 Select **Utilities > Expand**.

4 Set the new maximum size for the virtual disk.

You can set a size between 0.001GB and 2TB for a virtual disk.

5 Select **Expand**.

6 Click **OK** after the disk expansion process is complete.

### What to do next

Use a disk management tool to increase the disk partition size to match the expanded virtual disk size.

## Defragment a Virtual Hard Disk

Like physical disk drives, virtual hard disks can become fragmented. Defragmenting disks rearranges files, programs, and unused space on the virtual hard disk so that programs run faster and files open more quickly. Defragmenting does not reclaim unused space on a virtual hard disk.

Defragmenting disks can take considerable time.

### Prerequisites

- Verify that there is adequate free working space on the host system. For example, if the virtual hard disk is contained in a single file, there must be free space equal to the size of the virtual disk file. Other virtual hard disk configurations require less free space.
- Verify that the virtual disk is not mapped or mounted. You cannot defragment a virtual disk while it is mapped or mounted.

### Procedure

1 Run a disk defragmentation utility in the guest operating system.

2 If disk space is not preallocated for the virtual hard disk, use the Workstation defragmentation tool to defragment it.

   a Power off the virtual machine.

   b Select the virtual machine and select **VM > Settings**.

   c On the **Hardware** tab, select **Hard Disk**.

   d Select **Utilities > Defragment**.

   e When the defragmentation process is finished, click **OK**.

3 Run a disk defragmentation utility on the host system.

## Remove a Virtual Hard Disk from a Virtual Machine

Removing a virtual hard disk disconnects it from a virtual machine. It does not delete files from the host file system.

After you remove a virtual hard disk from a virtual machine, you can map or mount the disk to the host system and copy data from the guest operating system to the host without powering on the virtual machine or starting Workstation. You can also add the disk to another virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select the virtual hard disk and click **Remove**.

3 Click **OK** to save your changes.

## Using Virtual Disk Manager

Virtual Disk Manager (`vmware-diskmanager`) is a Workstation utility that you can use to create, manage, and modify virtual disk files from the command line or in scripts.

With Virtual Disk Manager, you can enlarge a virtual disk so that its maximum capacity is larger than it was when you created it. This feature is useful if you need more disk space in a given virtual machine, but do not want to add another virtual disk or use ghosting software to transfer the data on a virtual disk to a larger virtual disk.

You can also use Virtual Disk Manager to change how disk space is allocated for a virtual hard disk. You can preallocate all the disk space in advance or configure the disk to grow as more disk space is needed. If you allocate all the disk space but later need to reclaim some hard disk space on the host system, you can convert the preallocated virtual disk into a growable disk. The new virtual disk is still large enough to contain all the data in the original virtual hard disk. You can also change whether the virtual hard disk is stored in a single file or split into 2GB files.

See the *Virtual Disk Manager User's Guide* for information on using Virtual Disk Manager. This guide is available on the VMware Web site.

## Using Legacy Virtual Disks

You can use the current version of Workstation in a mixed environment with virtual machines that were created with earlier versions of Workstation or with other VMware products.

Although you can use the current version of Workstation to power on virtual machines that were created with older versions of Workstation or other VMware products, many new features of Workstation are not available in older virtual machines.

If you decide not to upgrade a virtual machine, you should still upgrade VMware Tools to the latest version in the guest operating system. Do not remove the older version of VMware Tools before installing the new version.

You can also use the current version of Workstation to create a version 4, 5.x, 6.x, and 7.x virtual machine.

If you have a Workstation 2, 3, or 4 virtual machine that you want to use with the current version of Workstation, upgrade the virtual machine to at least Workstation version 5 before you attempt to power it on.

### Using Lock Files to Prevent Consistency Problems on Virtual Hard Disks

A running virtual machine creates lock files to prevent consistency problems on virtual hard disks. Without locks, multiple virtual machines might read and write to the disk, causing data corruption.

Lock files have a `.lck` suffix and are created in subdirectories in the same directory as the virtual disk (`.vmdk`) files. A locking subdirectory and lock file are created for .vmdk files, `.vmx` files, and `.vmem` files.

A unified locking method is used on all host operating systems so that files shared between them are fully protected. For example, if one user on a Linux host tries to power on a virtual machine that is already powered on by another user with a Windows host, the lock files prevent the second user from powering on the virtual machine.

When a virtual machine powers off, it removes the locking subdirectories and the lock files. If the virtual machine cannot remove these locking controls, one or more stale lock files might remain. For example, if the host system fails before the virtual machine removes its locking controls, stale lock files remain.

When the virtual machine restarts, it scans any locking subdirectories for stale lock files and, when possible, removes them. A lock file is considered stale if the lock file was created on the same host system that is now running the virtual machine and the process that created the lock is no longer running. If either of these conditions is not true, a dialog box warns you that the virtual machine cannot be powered on. You can delete the locking directories and their lock files manually.

Locks also protect physical disk partitions. Because the host operating system is not aware of this locking convention, it does not recognize the lock. For this reason, you should install the physical disk for a virtual machine on the same physical disk as the host operating system.

### Moving a Virtual Hard Disk to a New Location

A key advantage of virtual hard disks is their portability. Because the virtual hard disks are stored as files on the host system or a remote computer, you can move them easily to a new location on the same computer or to a different computer.

For example, you can use Workstation on a Windows host system to create virtual hard disks, move the disks to a Linux computer, and use the disks with Workstation on a Linux host system.

## Adding a Physical Disk to a Virtual Machine

In some circumstances, you might need to give a virtual machine direct access to a physical disk or unused partition on the host computer.

A physical disk directly accesses an existing local disk or partition. You can use physical disks to run one or more guest operating systems from existing disk partitions.

Workstation supports physical disks up to 2TB capacity. Booting from an operating system already set up on an existing SCSI disk or partition is not supported.

Running an operating system natively on the host computer and switching to running it inside a virtual machine is similar to pulling the hard drive out of one computer and installing it in a second computer that has a different motherboard and hardware. The steps you take depend on the guest operating system in the virtual machine. In most cases, a guest operating system that is installed on a physical disk or unused partition cannot boot outside of the virtual machine, even though the data is available to the host system. See the *Dual-Boot Computers and Virtual Machines* technical note on the VMware Web site for information about using an operating system that can also boot outside of a virtual machine.

After you configure a virtual machine to use one or more partitions on a physical disk, do not modify the partition tables by running `fdisk` or a similar utility in the guest operating system. If you use `fdisk` or a similar utility on the host operating system to modify the partition table of the physical disk, you must recreate the virtual machine physical disk. All files that were on the physical disk are lost when you modify the partition table.

**IMPORTANT** You cannot use a physical disk to share files between the host computer and a guest operating system. Making the same partition visible to both the host computer and a guest operating system can cause data corruption. Instead, use shared folder to share files between the host computer and a guest operating system.

## Prepare to Use a Physical Disk or Unused Partition

You must perform certain tasks before you configure a virtual machine to use a physical disk or unused partition on the host system.

You must perform these tasks before you run the New Virtual Machine wizard to add a physical disk to a new virtual machine, and before you add a physical disk to an existing virtual machine.

### Procedure

1 If a partition is mounted by the host or in use by another virtual machine, unmount it.

The virtual machine and guest operating system access a physical disk partition while the host continues to run its operating system. Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted on the host operating system.

| Option | Description |
|---|---|
| **The partition is mapped to a Windows Server 2003, Windows Server 2008, or Windows XP host** | a Select **Start > Settings > Control Panel > Administrative Tools > Computer Management > Storage > Disk Management**.<br>b Select a partition and select **Action > All Tasks > Change Drive Letter and Paths**.<br>c Click **Remove**. |
| **The partition is mapped to a Windows 7 or Windows 8 host** | a Select **Start > Control Panel**.<br>b In the menu bar, click the arrow next to **Control Panel**.<br>c From the drop-down menu, select **All Control Panel Items > Administrative Tools > Computer Management > Storage > Disk Management (Local)**.<br>d Right-click a partition and choose **Change Drive Letter and Paths**.<br>e Click **Remove** and **OK**. |
| **The partition is mapped to a Windows Vista host** | a Select **Start > Control Panel (Classic View) > Administrative Tools > Computer Management > Storage > Disk Management**.<br>b Right-click a partition and choose **Change Drive Letter and Paths**.<br>c Click **Remove** and **OK**. |

2 Check the guest operating system documentation regarding the type of partition on which the guest operating system can be installed.

On Windows Vista and Windows 7 hosts, you cannot use the system partition, or the physical disk that contains it, in a virtual machine. DOS, Windows 95, and Windows 98 operating systems must be installed on the first primary partition. Other operating systems, such as Linux, can be installed on a primary or an extended partition on any part of the drive.

3 If the physical partition or disk contains data that you need in the future, back up the data.

4 If you use a Windows host IDE disk in a physical disk configuration, verify that it is not configured as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.

5 On a Windows XP or Windows Server 2003 host, if the host is using a dynamic disk, use the disk management tool to change the dynamic disk to a basic disk.

   You cannot use a dynamic disk as a physical disk in a virtual machine.

   a On the host, select **Start > Settings > Control Panel > Administrative Tools > Computer Management > Disk Management**.

   b Delete all logical volumes on the disk.

   This action destroys all data on the disk.

   c Right-click the disk icon and select **Revert to Basic Disk**.

   d Partition the disk.

6 On a Linux host, set the device group membership or device ownership appropriately.

   a Verify that the master physical disk device or devices are readable and writable by the user who runs Workstation.

   Physical devices, such as `/dev/hda` (IDE physical disk) and `/dev/sdb` (SCSI physical disk), belong to group-id `disk` on most distributions. If this is the case, you can add VMware Workstation users to the `disk` group. Another option is to change the owner of the device. Consider all the security issues involved in this option.

   b Grant VMware Workstation users access to all `/dev/hd[abcd]` physical devices that contain operating systems or boot managers.

   When permissions are set correctly, the physical disk configuration files in Workstation control access. This reliability provides boot managers access to configuration files and other files they might need to boot operating systems. For example, LILO needs to read `/boot` on a Linux partition to boot a non-Linux operating system that might be on another drive.

## Add a Physical Disk to an Existing Virtual Machine

You can add a physical disk to an existing virtual machine by modifying virtual machine hardware settings.

To add a physical disk to a new virtual machine, run the New Virtual Machine wizard and select the **Custom** option. See "Create a New Virtual Machine on the Local Host," on page 18.

**NOTE** You cannot add a physical disk to a shared or remote virtual machine.

### Prerequisites

- Perform the appropriate preparation tasks. See "Prepare to Use a Physical Disk or Unused Partition," on page 14.
- Power off the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 Select **Hard Disk**.

4 Select **Use a physical disk**.

5 If a warning message appears, click **OK**.

6 Select the physical hard disk to use from the drop-down menu.

7 Select whether to use the entire disk or individual partitions.

8 If you selected individual partitions, select the partitions.

The virtual machine can access only the partitions that you select. The guest operating system might be able to detect other partitions, but you cannot mount, access, or format those partitions.

9 Accept the default filename and location for the virtual disk (`.vmdk`) file, or browse to a different location.

10 Click **Finish** to add the physical disk to the virtual machine.

11 Use the tools in the guest operating system to format any partitions on the physical disk that are not formatted for the guest operating system.

# Configuring Virtual Ports

You can add virtual parallel (LPT) ports and virtual serial (COM) ports to a virtual machine. A Workstation virtual machine can use up to three parallel ports and up to four virtual serial ports.

- Add a Virtual Parallel Port to a Virtual Machine on page 125

  You can attach up to three bidirectional parallel (LPT) ports to a virtual machine. Virtual parallel ports can output to parallel ports or to files on the host system.

- Configure a Virtual Parallel Port on a Linux 2.6.x Kernel Host on page 126

  Linux 2.6.x kernels that support parallel ports use the `modprobe` *`modulename`* and `modprobe parport_pc` modules. Workstation requires that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) is built and loaded as a kernel module.

- Configure Permissions for a Parallel Port Device on a Linux Host on page 127

  Some Linux distributions do not grant a virtual machine access to the `lp` and `parport` devices by default. If this is the case on your Linux host system, you must add the VMware user to the group that has permission to access those devices.

- Troubleshoot ECR Errors for Parallel Ports on page 127

  A parallel port on the host system does not have an Extended Control Register (ECR).

- Add a Virtual Serial Port to a Virtual Machine on page 128

  You can add up to four serial (COM) ports to a virtual machine. Virtual serial ports can output to physical serial ports, files, or named pipes.

- Change the Input Speed of a Serial Connection on page 129

  You can increase the speed of a serial connection over a pipe to a virtual machine.

## Add a Virtual Parallel Port to a Virtual Machine

You can attach up to three bidirectional parallel (LPT) ports to a virtual machine. Virtual parallel ports can output to parallel ports or to files on the host system.

Parallel ports are used for a variety of devices, including printers, scanners, dongles, and disk drives. Although these devices can connect to the host system, only printers can reliably connect to virtual machines by using parallel ports.

Workstation provides only partial emulation of PS/2 hardware. Interrupts that a device connected to a physical port requests are not passed to the virtual machine. The guest operating system cannot use direct memory access (DMA) to move data to or from the port. For this reason, not all devices that attach to a parallel port work correctly. Do not use virtual parallel ports to connect parallel port storage devices or other types of parallel port devices to a virtual machine.

### Prerequisites

- If you are using a Linux host system that has a 2.6.x kernel, verify that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) is built and loaded as a kernel module. See "Configure a Virtual Parallel Port on a Linux 2.6.x Kernel Host," on page 126.
- If you are using a Linux host system that does not grant virtual machines access to the `lp` and `parport` devices by default, add the VMware user to the group that has permission to access those devices. See "Configure Permissions for a Parallel Port Device on a Linux Host," on page 127.
- Power off the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 In the New Hardware wizard, select **Parallel Port**.

4 Select where the virtual parallel port sends output.

| Option | Description |
|---|---|
| **Use a physical parallel port** | Select a parallel port on the host system. |
| **Use output file** | Send output from the virtual parallel port to a file on the host system. Either locate an existing output file or browse to a directory and type a filename to create a new output file. |

5 To connect the virtual parallel port to the virtual machine when the virtual machine powers on, select **Connect at power on**.

6 Click **Finish** to add the virtual parallel port to the virtual machine.

When a parallel port is configured for a virtual machine, most guest operating systems detect the port at installation time and install the required drivers. Some operating systems, including Linux, Windows NT, and Windows 2000, detect the ports at boot time.

### What to do next

If the guest operating system is Windows 95 or Windows 98, run the Add New Hardware wizard to detect and add the parallel port.

## Configure a Virtual Parallel Port on a Linux 2.6.x Kernel Host

Linux 2.6.x kernels that support parallel ports use the `modprobe` *`modulename`* and `modprobe parport_pc` modules. Workstation requires that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) is built and loaded as a kernel module.

Linux kernels in the 2.6.x series use a special arbitrator for access to the parallel port hardware. If the host system is using the parallel port, the virtual machine cannot use it. If a virtual machine is using the parallel port, the host and any users accessing the host are denied access to the device. You must use the **Removable Devices** menu to disconnect the parallel port from the virtual machine to access the device from the host system.

### Procedure

1 To determine whether the `modprobe` *`modulename`* and `modprobe parport_pc` modules are installed and loaded on the host system, run the `lsmod` command as the root user.

You can also see a list of modules in the `/proc/modules` file.

**NOTE** In Linux 2.6.x, loading `parport_pc` does not load all modules.

2 If necessary, load the parallel port modules.

For example: `modprobe parport_pc && modprobe ppdev`

This command inserts the modules that are required for a parallel port.

3 If the `lp` module is loaded, run the `rmmod` command as root to remove it.

For example: `rmmod lp`

The virtual machine cannot use the parallel port correctly if the `lp` module is loaded.

4 Comment out the line that refers to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file.

The name of the configuration file depends on the Linux distribution.

When the line is commented out, the configuration file no longer starts the lp module when you reboot the host system.

5 To make sure that the proper modules for the parallel port are loaded at boot time, add the following line to the `/etc/modules.conf` or `/etc/conf.modules` file.

```
alias parport_lowlevel parport_pc
```

## Configure Permissions for a Parallel Port Device on a Linux Host

Some Linux distributions do not grant a virtual machine access to the `lp` and `parport` devices by default. If this is the case on your Linux host system, you must add the VMware user to the group that has permission to access those devices.

### Procedure

1 On the Linux host system, use the `ls` command to determine the owner and group for the device.

For example: **`ls -la /dev/parport0`**

The third and fourth columns of the output show the owner and group, respectively. In most cases, the owner of the device is root and the associated group is `lp`.

2 To add the user to the device group, become root and open the `/etc/group` file in a text editor.

3 On the line that defines the `lp` group, add the Workstation username.

For example: **`lp::7:daemon,lp,`*`workstation_username`***

The changes take effect the next time the user logs in to the host system.

## Troubleshoot ECR Errors for Parallel Ports

A parallel port on the host system does not have an Extended Control Register (ECR).

### Problem

When you power on a virtual machine after adding a parallel port, an error messages states that the parallel port on the host system does not have an ECR.

### Cause

This problem can occur when the hardware supports ECR, but ECR has been disabled in the BIOS.

### Solution

1 Reboot the host system.

2 Early in the boot process, press and hold down the Delete key to enter the BIOS configuration editor.

3 Find the parallel port field and enable Extended Capability Port (ECP) mode or a combination of modes that includes ECP.

Most modern computers support ECP mode.

## Add a Virtual Serial Port to a Virtual Machine

You can add up to four serial (COM) ports to a virtual machine. Virtual serial ports can output to physical serial ports, files, or named pipes.

You might want to add a virtual serial port to a virtual machine to make devices such as modems and printers available to the virtual machine. You can also use virtual ports to send debugging data from a virtual machine to the host system or to another virtual machine.

**NOTE** The virtual printer feature configures a serial port to make host printers available to the guest. You do not need to install additional drivers in the virtual machine.

### Prerequisites

Power off the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 In the Add Hardware wizard, select **Serial Port**.

4 Select where the virtual serial port sends output.

| Option | Description |
|---|---|
| **Use a physical parallel port** | Send output to a physical serial port on the host system. |
| **Use output file** | Send output to a file on the host system. Either locate an existing output file or browse to a directory and type a filename to create a new output file. |
| **Output to named pipe** | Set up a direct connection between two virtual machines, or a connection between a virtual machine and an application on the host system. |

5 If you selected **Output to named pipe**, configure the named pipe.

a (Windows host) Use the default pipe name, or type another pipe name.

The pipe name must begin with **\\.\pipe** and must be the same on both the server and the client.

For example: **\\.\pipe*namedpipe***

b (Linux host) Type **/tmp/socket** or another UNIX socket name in the first text box.

The pipe name must be the same on both the server and the client.

c To send debugging information to an application on the host system, select **This end is the server** from the first drop-down menu and select **The other end is an application** from the second drop-down menu.

d To send debugging information to another virtual machine, select **This end is the server** from the first drop-down menu and **The other end is a virtual machine** from the second drop-down menu.

6 To connect the port to the virtual machine when the virtual machine powers on, select **Connect at power on**.

7 Click **Finish** to add the virtual serial port to the virtual machine.

8 (Optional) On the **Hardware** tab, select the new serial port, select **Yield CPU on poll**, and click **OK**.

This option is useful if you are using debugging tools that communicate over a serial connection. If the serial port in the guest operating system is being used in polled mode rather than interrupt mode, you might notice performance issues. This option forces the virtual machine to yield processor time if the only task it is trying to do is poll the virtual serial port.

#### What to do next

If you set up a connection between two virtual machines, the first virtual machine is set up as the server. Repeat this procedure for the second virtual machine, but set it up as the client by selecting **This end is the client** when you configure the named pipe.

### Change the Input Speed of a Serial Connection

You can increase the speed of a serial connection over a pipe to a virtual machine.

In principle, the output speed, which is the speed at which the virtual machine sends data through the virtual serial port, is unlimited. In practice, the output speed depends on how fast the application at the other end of the pipe reads inbound data.

#### Prerequisites

- Use the guest operating system to configure the serial port for the highest setting supported by the application that you are running in the virtual machine.
- Power off the virtual machine and exit Workstation.

#### Procedure

1 In a text editor, add the following line to the virtual machine configuration (`.vmx`) file.

```
serialport_number.pipe.charTimePercent = "time"
```

*port_number* is the number of the serial port, starting from 0. The first serial port is serial0. *time* is a positive integer that specifies the time taken to transmit a character, expressed as a percentage of the default speed set for the serial port in the guest operating system. For example, a setting of 200 forces the port to take twice as long for each character, or send data at half the default speed. A setting of 50 forces the port to take only half as long for each character, or send data at twice the default speed.

2 Assuming that the serial port speed is set appropriately in the guest operating system, experiment with this setting by starting with a value of 100 and gradually decreasing it until you find the highest speed at which the connection works reliably.

## Configuring Generic SCSI Devices

The generic SCSI feature gives the guest operating system direct access to SCSI devices that are connected to the host system, including scanners, tape drives, and other data storage devices. A virtual machine can use the generic SCSI driver to run any SCSI device that is supported by the guest operating system.

To use SCSI devices in a virtual machine running on a Windows host system, you must run Workstation as a user who has administrator access.

On Linux host systems, you must have read and write permissions on a given generic SCSI device to use that device in a virtual machine, even if the device is a read-only device, such as a CD-ROM drive. These devices typically default to root-only permissions. A Linux administrator can create a group that has read and write access to these devices and add the appropriate users to that group.

Although generic SCSI is device independent, it can be sensitive to the guest operating system, device class, and specific SCSI hardware.

- Add a Generic SCSI Device to a Virtual Machine on page 130

  You must add a generic SCSI device to the virtual machine to map virtual SCSI devices on a virtual machine to physical generic SCSI devices on the host system. You can add up to 60 generic SCSI devices to a virtual machine.

- Install the BusLogic Driver in a Windows NT 4.0 Guest on page 131

  Generic SCSI devices use the virtual Mylex (BusLogic) BT/KT-958 compatible host bus adapter provided by the virtual machine. On Windows NT 4.0, you might need to install the driver manually if it is not already installed for a virtual SCSI disk. Install the driver before you add a generic SCSI device.

- Avoiding Concurrent Access Problems for SCSI Devices on Linux Hosts on page 131

  Workstation makes sure that multiple programs do not use the same `/dev/sg` entry at the same time, but it cannot always ensure that multiple programs do not use the `/dev/sg` entry and the traditional `/dev` entry at the same time.

- Troubleshoot Problems Detecting Generic SCSI Devices on page 131

  When you add a generic SCSI device to a virtual machine, the device does not appear in the list of available SCSI devices.

## Add a Generic SCSI Device to a Virtual Machine

You must add a generic SCSI device to the virtual machine to map virtual SCSI devices on a virtual machine to physical generic SCSI devices on the host system. You can add up to 60 generic SCSI devices to a virtual machine.

NOTE You cannot add a generic SCSI device to a shared or remote virtual machine.

### Prerequisites

- On a Windows host system, run Workstation as a user who has administrator access.
- On a Linux host system, log in as a user who has read and write permissions for the SCSI device. Also, verify that version 2.1.36 or later of the SCSI Generic driver (`sg.o`) is installed. This version of the SCSI Generic driver is included with Linux kernel 2.2.14 and later.
- On a Windows 95, Windows 98, or Windows Me virtual machine, install the latest Mylex (BusLogic) BT/KT-958 compatible host bus adapter. This driver overrides the driver that Windows chooses as the best driver, but it corrects known problems. You can download the driver from the LSI Web site.
- On a 32-bit Windows XP virtual machine, install the special SCSI driver that VMware provides. You can download the driver from the VMware Web site.
- On a Windows NT 4.0 virtual machine, install the BusLogic MultiMaster PCI SCSI Host Adapters driver. See "Install the BusLogic Driver in a Windows NT 4.0 Guest," on page 131.

### Procedure

1. Select the virtual machine and select **VM > Settings**.
2. On the **Hardware** tab, click **Add**.
3. In the Add Hardware wizard, select **Generic SCSI Device**.
4. Select the physical SCSI device to map to the virtual SCSI device.

   When you type the path to the SCSI device on a Linux host, do not enter `/dev/st0` or `/dev/sr0`.
5. To connect the device when the virtual machine powers on, select **Connect at power on**.
6. Click **Finish** to add the device.

7 On the **Hardware** tab, select the SCSI device identifier to use for the device from the **Virtual device node** drop-down menu and click **OK**.

For example, if you select **SCSI 0:2**, the guest operating system sees the drive as ID 2 on controller 0.

## Install the BusLogic Driver in a Windows NT 4.0 Guest

Generic SCSI devices use the virtual Mylex (BusLogic) BT/KT-958 compatible host bus adapter provided by the virtual machine. On Windows NT 4.0, you might need to install the driver manually if it is not already installed for a virtual SCSI disk. Install the driver before you add a generic SCSI device.

### Prerequisites

Verify that the Windows NT installation CD is available.

### Procedure

1 Select **Start > Settings > Control Panel > SCSI Adapters** to open the SCSI Adapters control panel.

2 On the **Drivers** tab, click **Add**.

3 From the list of vendors, select **BusLogic**.

4 From the list of drivers, select **BusLogic MultiMaster PCI SCSI Host Adapters** and click **OK**.

5 Insert the Windows NT CD and click **OK**.

6 Reboot the virtual machine.

## Avoiding Concurrent Access Problems for SCSI Devices on Linux Hosts

Workstation makes sure that multiple programs do not use the same `/dev/sg` entry at the same time, but it cannot always ensure that multiple programs do not use the `/dev/sg` entry and the traditional `/dev` entry at the same time.

The SCSI generic driver sets up a mapping in `/dev` for each SCSI device. Each entry starts with `sg`, for the SCSI generic driver, followed by a number. For example, `/dev/sg0` is the first generic SCSI device. Each entry corresponds to a SCSI device in the order specified in `/proc/scsi/scsi`, from the lowest device ID on the lowest adapter to the highest device ID on the lowest adapter, and so on to the highest device ID on the highest adapter.

Some Linux devices, such as tape drives, disk drives, and CD-ROM drives, already have a designated `/dev` entry (`st`, `sd`, and `sr`, respectively). When the SCSI generic driver is installed, Linux identifies these devices with corresponding `sg` entries in `/dev`, in addition to their traditional entries.

To avoid concurrent access problems, do not specify `/dev/st0` or `/dev/sr0` when you specify which SCSI device to use in a virtual machine.

**IMPORTANT** Do not attempt to use the same generic SCSI device in both the host system and guest operating system. Unexpected behavior and data loss or corruption might occur.

## Troubleshoot Problems Detecting Generic SCSI Devices

When you add a generic SCSI device to a virtual machine, the device does not appear in the list of available SCSI devices.

### Problem

The SCSI device does not appear in the list of available SCSI devices after you add it to a virtual machine.

### Cause

A driver for that device is not installed on the host system, a driver on the host system prevents the device from being detected, or the virtual machine uses a device for which there are no drivers available to the host operating system.

### Solution

1 Determine the SCSI bus number that the device uses on the host system.

The SCSI bus is assigned a number by the host operating system after all IDE buses are assigned numbers. For example, if you have two IDE buses, they are numbered 0 and 1. The first SCSI bus is assigned bus number 2. You can use a third-party tool, such as `winobj`, to determine the SCSI bus number.

2 Determine the target ID that the device uses in the virtual machine and on the host system.

This ID is usually set by some jumpers or switches on the device.

3 Determine whether the device driver for the device is installed on the host system.

If the device driver is not installed, install it and see if the device appears. To avoid a device-in-use conflict between the host and guest, you might not want to install the driver on the host system.

4 If an original SCSI device driver is already installed on the host system, disable it.

Some Windows operating systems do not process the send command from the adapter if the device driver owns the device.

5 Power off the virtual machine and open the virtual machine configuration (`.vmx`) file in a text editor.

6 Add or change the following line in the virtual machine configuration (`.vmx`) file.

**`scsiZ:Y.fileName = "`*`deviceName`*`"`**

**`Z`** is the SCSI bus number the device uses in the virtual machine. For *deviceName*, use **`scsiX:Y`**, where **`X`** is the SCSI bus number that the device uses on the host system and **`Y`** is the target ID that the device uses in both the virtual machine and on the host system.

For example, if the problematic device is a CD-ROM drive, the existing entry is **`scsi0:4.fileName = "CdRom0"`** and the device on the host system is located on bus 2 with target ID 4, change the line to **`scsi0:4.fileName = "scsi2:4"`**.

7 If the virtual machine does not contain any SCSI devices, to add a generic SCSI device to a new virtual SCSI adapter, or to use an existing SCSI device as a generic SCSI device, add the following line to the virtual machine configuration (`.vmx`) file.

**`scsiZ:Y.deviceType = "scsi-passthru"`**

8 If the virtual machine does not contain any SCSI devices, or to add a generic SCSI device to a new virtual SCSI adapter, add the following lines to the virtual machine configuration (`.vmx`) file.

```
scsiZ:Y.present = "true"
scsiZ.present = "true"
```

# Configuring Eight-Way Virtual Symmetric Multiprocessing

With virtual symmetric multiprocessing (SMP), you can assign processors and cores per processor to a virtual machine on any host system that has at least two logical processors.

Workstation considers multiprocessor hosts that have two or more physical CPUs, single-processor hosts that have a multicore CPU, and single-processor hosts that have hyperthreading enabled, to have two logical processors.

**NOTE** On hyperthreaded uniprocessor hosts, performance of virtual machines that have virtual SMP might be below normal. Even on multiprocessor hosts, performance is affected if you overcommit by running multiple workloads that require more total CPU resources than are physically available.

You can power on and run multiple dual-processor virtual machines concurrently. The number of processors for a given virtual machine appears in the summary view of the virtual machine.

## Configure Eight-Way Virtual Symmetric Multiprocessing

You can configure eight-way virtual symmetric multiprocessing (SMP) for an existing virtual machines.

**NOTE** For a new virtual machine, you can specify the number of processors when you select the custom configuration option in the New Virtual Machine wizard.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Processors**.

3 Change the **Number of processors** setting to 8.

4 Click **OK** to save your changes.

## Use a Virtual Machine That Has More Than Eight Virtual Processors

If Workstation is running on a multiprocessor host system, you can open a virtual machine that has more than eight virtual processors assigned to it. You must change the number of processors before powering on the virtual machine.

You can see the number of processors in the virtual machine summary view or by viewing the virtual machine hardware settings.

### Prerequisites

Power off the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Processors**.

Note that **Number of processors** is set to **Other (x)**, where **x** is the number of processors originally assigned to it. Workstation preserves this original configuration setting for the number of processors, even though eight is the maximum number of processors supported.

3 Change the **Number of processors** setting to 1, 2, 4, 8, or 16.

After you commit a change to this setting, the original setting for the number of processors is discarded and no longer appears as an option.

4 Click **OK** to save your changes.

# Configuring Keyboard Features

You can change key combinations for hot-key sequences in Workstation and the language for the keyboard that VNC clients use. You can also configure platform-specific keyboard features for Windows and Linux host systems.

- Use the Enhanced Virtual Keyboard Feature in a Virtual Machine on page 134

  The enhanced virtual keyboard feature provides better handling of international keyboards and keyboards that have extra keys. This feature is available only on Windows host systems.

- Change Hot-Key Combinations for Common Operations on page 136

  You can change the hot-key combinations that you use to perform common virtual machine operations.

- Change Hot-Key Combinations for Unity Mode on page 137

  You can change the hot-key combination that you use to access the **Start** and **Applications** menus in Unity mode.

- Configure Keyboard Mapping for a Remote X Server on page 137

  Although the keyboard works correctly with a local X server, it might not work correctly when you run the same virtual machine with a remote X server.

- Change How a Specific Key Is Mapped on page 138

  If some keys on the keyboard do not work correctly in a virtual machine, you can set a property that makes a modification to the map. To change how a specific key is mapped, you add the appropriate property to the virtual machine configuration (`.vmx`) file or to `~/.vmware/config`.

- Configure How Keysyms Are Mapped on page 139

  When key code mapping cannot be used or is disabled, Workstation maps keysyms to v-scan codes. If a language-specific keyboard does not appear to be supported by Workstation, you might need to set a property that tells Workstation which keysym table to use.

- V-Scan Code Table on page 140

  You specify v-scan codes when you change how keys or keysyms are mapped.

## Use the Enhanced Virtual Keyboard Feature in a Virtual Machine

The enhanced virtual keyboard feature provides better handling of international keyboards and keyboards that have extra keys. This feature is available only on Windows host systems.

Because it processes raw keyboard input as soon as possible, the enhanced virtual keyboard feature also offers security improvements by bypassing Windows keystroke processing and any malware that is not already at a lower layer. When you use the enhanced virtual keyboard feature, only the guest operating system acts when you press Ctrl+Alt+Delete.

**NOTE** You cannot configure the enhanced virtual keyboard setting for a shared or remote virtual machine.

### Prerequisites

- Power off the virtual machine.
- If you did not install the Enhanced Keyboard Utility feature when you initially installed or upgraded Workstation, install it by running the Workstation installer in program maintenance mode. See "Install the Enhanced Keyboard Driver on a Windows Host," on page 135.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Options** tab, select **General**.

3 Select an option from the **Enhanced virtual keyboard** drop-down menu.

| Option | Description |
|---|---|
| **Off** | The virtual machine does not use the enhanced virtual keyboard feature. This is the default value. |
| **Use if available (recommended)** | The virtual machine uses the enhanced virtual keyboard feature, but only if the enhanced virtual keyboard driver is installed on the host system. |
| **Required** | The virtual machine must use the enhanced the virtual keyboard feature. If you select this option and the enhanced keyboard driver is not installed on the host system, Workstation returns an error message. |

4 Click **OK** to save your changes.

## Install the Enhanced Keyboard Driver on a Windows Host

To use the enhanced virtual keyboard feature in a virtual machine, you must install the enhanced keyboard driver on the Windows host system. If you did not install the enhanced keyboard driver when you initially installed or upgraded Workstation, you can install it by running the Workstation installer in program maintenance mode.

### Prerequisites

Verify that you have administrative privileges on the host system.

### Procedure

1 Log in to the Windows host system as the Administrator user or as a user who is a member of the local Administrators group.

If you log in to a domain, the domain account must also be a local administrator.

2 If you installed Workstation from a CD, insert the CD in the CD-ROM drive on the host system.

If autorun is enabled, the installation program begins.

3 If autorun is not enabled, or if you downloaded the installation software, double-click the setup file.

| Option | Description |
|---|---|
| **Workstation installed from a CD** | The setup file is called `setup.exe`. |
| **Workstation installed from a download** | The setup filename is similar to `VMware-workstation-xxxx-xxxx.exe`, where *xxxx-xxxx* is the version and build numbers. |

4 Select **Modify/Change**.

5 Select **Enhanced Keyboard Utility**.

6 Follow the prompts to finish the installation.

### What to do next

Enable the enhanced virtual keyboard feature for the virtual machine. See "Use the Enhanced Virtual Keyboard Feature in a Virtual Machine," on page 134.

## Change Hot-Key Combinations for Common Operations

You can change the hot-key combinations that you use to perform common virtual machine operations.

Configuring hot keys is useful to prevent key combinations such as Ctrl+Alt+Del from being intercepted by Workstation instead of being sent to the guest operating system. You can use hot-key sequences to switch between virtual machines, enter or exit from full screen mode, release input, send Ctrl+Alt+Del only to virtual machines, and send commands only to virtual machines.

### Prerequisites

Familiarize yourself with the default hot-key combinations. See "Default Hot-Key Combinations," on page 136.

### Procedure

1 Select **Edit > Preferences > Hot Keys**.

2 To change the hot-key combinations for common virtual machine operations, click one or more hot key buttons on the dialog box.

For example, to use Ctrl+Shift to release control from the current virtual machine, click the **Ctrl** and **Shift** buttons.

The text under the hot key buttons describes the new hot key combinations.

3 Click **OK** to save your changes.

## Default Hot-Key Combinations

You can use keyboard shortcuts to interact with Workstation and with virtual machines. Most of the available keyboard shortcuts for Workstation are listed next to their associated commands in Workstation menus.

**Table 4-1.** Default Hot-Key Combinations

| Shortcut | Action |
|---|---|
| Ctrl+G | Grab input from the keyboard and mouse. |
| Ctrl+Alt | Release the mouse cursor. |
| Ctrl+Alt+Insert | Shut down or, depending on the guest operating system, log out of the guest operating system. This command is received solely by the virtual machine. |
| Ctrl+Alt+Delete | Shut down or, depending on the operating system, log out of the guest operating system.<br>On a Windows host, if you do not use the enhanced virtual keyboard feature, both the host operating system and the virtual machine receive this command, even when Workstation has control of input. Cancel the ending of the host operating system session and return to the virtual machine to log out or shut down or perform administrative tasks. |
| Ctrl+Alt+Enter | Enter full screen mode. |
| Ctrl+Alt+spacebar | Send any command to the virtual machine so that Workstation does not process it. Hold down Ctrl+Alt as you press and release the spacebar, and continue to hold the Ctrl+Alt keys down as you press the next key in the combination. |
| Ctrl+Tab<br>Ctrl+Shift+Tab | (Windows hosts only) Switch among tabs. |
| Ctrl+Alt+right arrow | In full screen mode, switch to the next powered-on virtual machine. |
| Ctrl+Alt+left arrow | In full screen mode, switch to the previous powered-on virtual machine. |
| Ctrl+Shift+U | In Unity mode, give access to the virtual machine **Start** or **Applications** menu.<br>You can change the Unity hot-key combination by modifying Unity preference settings. |

You can change the default hot-key combinations by modifying Workstation preference settings. If you change the hot-key settings, substitute your new hot-key combination for Ctrl+Alt. For example, if you change the hot-key combination for common virtual machine operations to Ctrl+Shift, you press Ctrl+Shift instead of Ctrl+Alt to release control from the current virtual machine.

### Use Ctrl+Alt in a Key Combination

Because Ctrl+Alt tells Workstation to release mouse and keyboard input, hot-key combinations that include Ctrl+Alt are not passed to the guest operating system. You must use the Space key if the key combination includes Ctrl+Alt.

#### Procedure

1 Press Ctrl+Alt+spacebar.

2 Release the spacebar without releasing Ctrl and Alt.

3 Press the third key of the key combination to send to the guest operating system.

## Change Hot-Key Combinations for Unity Mode

You can change the hot-key combination that you use to access the **Start** and **Applications** menus in Unity mode.

#### Procedure

1 Select **Edit > Preferences > Unity**.

2 Type a new hot-key combination in the **Hot Key** text box.

3 To minimize the Workstation when you enter Unity mode, select **Minimize Workstation when entering Unity**.

Do not select this setting if you plan to run virtual machines in Unity mode and simultaneously run other virtual machines that are accessible only in the Workstation window.

4 Click **OK** to save your changes.

## Configure Keyboard Mapping for a Remote X Server

Although the keyboard works correctly with a local X server, it might not work correctly when you run the same virtual machine with a remote X server.

For local X servers, Workstation maps X key codes to PC scan codes to correctly identify a key. Because it cannot tell whether a remote X server is running on a PC or on some other kind of computer, Workstation uses this key code map only for local X servers. You can set a property to tell Workstation to use key code mapping. See "Understanding X-Key Codes and Keysyms," on page 138 for more information.

To configure a keyboard mapping for a remote X server, you add the appropriate property to the virtual machine configuration (`.vmx`) file or to `~/.vmware/config`.

#### Prerequisites

- Verify that the remote X server is an XFree86 server running on a PC.
- Power off the virtual machine and exit Workstation.

**NOTE** If the keyboard does not work correctly on an XFree86 server running locally, report the problem to VMware technical support.

### Procedure

- If you use an XFree86-based server that Workstation does not recognize as an XFree86 server, add the `xkeymap.usekeycodeMap` property and set it to **`TRUE`**.

  This property tells Workstation to always use key code mapping regardless of server type.

  For example: **`xkeymap.usekeycodeMap = "TRUE"`**

- If Workstation does not recognize the remote server as an XFree86 server, add the `xkeymap.usekeycodeMapIfXFree86` property and set it to **`TRUE`**.

  This property tells Workstation to use key code mapping if you are using an XFree86 server, even if it is remote.

  For example: **`usekeycodeMapIfXFree86 = "TRUE"`**

## Understanding X-Key Codes and Keysyms

Pressing a key on a PC keyboard generates a PC scan code based roughly on the position of the key. For example, the Z key on a German keyboard generates the same code as the Y key on an English keyboard because they are in the same position on the keyboard. Most keys have one-byte scan codes, but some keys have two-byte scan codes with prefix 0xe0.

Internally, Workstation uses a simplified version of the PC scan code that is a single nine-bit numeric value, called a v-scan code. A v-scan code is written as a three-digit hexadecimal number. The first digit is 0 or 1. For example, the Ctrl key on the left side of the keyboard has a one-byte scan code (0x1d) and its v-scan code is 0x01d. The Ctrl key scan code on the right side of the keyboard is two bytes (0xe0, 0x1d) and its v-scan code is 0x11d.

An XFree86 server on a PC has a one-to-one mapping from X key codes to PC scan codes, or v-scan codes, which is what Workstation uses. When Workstation is hosted on an XFree86 server and runs a local virtual machine, it uses the built-in mapping from X key codes to v-scan codes. This mapping is keyboard independent and should be correct for most languages. In other cases (not an XFree86 server or not a local server), Workstation must map keysyms to v-scan codes by using a set of keyboard-specific tables.

An X server uses a two-level encoding of keys, which includes the X key code and the keysym. An X key code is a one-byte value. The assignment of key codes to keys depends on the X server implementation and the physical keyboard. As a result, an X application normally cannot use key codes directly. Instead, the key codes are mapped into keysyms that have names like space, escape, x and 2. You can use an X application to control the mapping by using the function `XChangeKeyboardMapping()` or by the program xmodmap. To explore keyboard mappings, you can use the `xev` command, which shows the key codes and keysyms for keys typed into its window.

A key code corresponds roughly to a physical key, while a keysym corresponds to the symbol on the key top. For example, with an XFree86 server running on a PC, the Z key on the German keyboard has the same key code as the Y key on an English keyboard. The German Z keysym, however, is the same as the English Z keysym, and different from the English Y keysym.

# Change How a Specific Key Is Mapped

If some keys on the keyboard do not work correctly in a virtual machine, you can set a property that makes a modification to the map. To change how a specific key is mapped, you add the appropriate property to the virtual machine configuration (`.vmx`) file or to `~/.vmware/config`.

### Prerequisites

- Verify that the X server is an XFree86 server running on a PC. If the X server is remote, configure it to use key code mapping. See "Configure Keyboard Mapping for a Remote X Server," on page 137.
- Determine the X key code and the corresponding v-scan code for the key. To find the X key code for a key, run `xev` or `xmodmap -pk`. See "V-Scan Code Table," on page 140 for most v-scan codes.

- Power off the virtual machine and exit Workstation.

### Procedure

1 Open `.vmx` or `~/.vmware/config` in a text editor.

2 Add the `xkeymap.keycode.`*code* property and set it to the v-scan code.

*code* must be a decimal number and the v-scan code must be a C-syntax hexadecimal number, such as 0x001.

In this example, the properties swap left Ctrl and Caps Lock.

```
xkeymap.keycode.64 = "0x01d # X Caps_Lock -> VM left ctrl"
xkeymap.keycode.37 = "0x03a # X Control_L -> VM caps lock"
```

## Configure How Keysyms Are Mapped

When key code mapping cannot be used or is disabled, Workstation maps keysyms to v-scan codes. If a language-specific keyboard does not appear to be supported by Workstation, you might need to set a property that tells Workstation which keysym table to use.

Workstation determines which table to use by examining the current X keymap. However, its decision-making process can sometimes fail. In addition, each mapping is fixed and might not be completely correct for any given keyboard and X key code-to-keysym mapping. For example, if a user uses `xmodmap` to swap Ctrl and Caps Lock by, the keys are swapped in the virtual machine when using a remote server (keysym mapping), but are unswapped when using a local server (key code mapping). To correct this situation, you must remap the keys in Workstation.

To configure how keysyms are mapped, you add one or more properties to the virtual machine configuration (`.vmx`) file or to `~/.vmware/config`.

### Prerequisites

- To change the mapping of a few keys, determine the keysym name for each key. To find a keysym name, use the `xev` or `xmodmap -pk` command. The X header file `/usr/include/X11/keysymdef.h` also has a complete list of keysyms. The name of a keysym is the same as its C constant, but without the XK_ prefix.
- To use a different keysym table, determine which mapping table to use. The tables are located in the `xkeymap` directory in the Workstation installation directory, which is usually `/usr/lib/vmware`. The table you must use depends on the keyboard layout. The normal distribution includes tables for PC keyboards for the United States and a number of European countries and languages. For most of these, both the 101-key (or 102-key) and the 104-key (or 105-key) variants are available.

  If none of the mapping tables is completely correct, find one that works best, copy it to a new location, and change the individual keysym mappings.
- Familiarize yourself with the v-scan codes. See "V-Scan Code Table," on page 140.
- Power off the virtual machine and exit Workstation.

### Procedure

- To disable X key code mapping to map keysyms rather than key codes to v-scan codes, add the `xkeymap.nokeycodeMap` property and set it to TRUE.

  For example: **`xkeymap.nokeycodeMap = "TRUE"`**

- If Workstation has a table in the `xkeymap` directory for your keyboard but cannot detect it, add the `xkeymap.language` property and set it to one of the tables in the `xkeymap` directory.

  For example: **`xkeymap.language = "keyboard_type"`**

  If the failure to detect the keyboard means that the table is not completely correct for you, you might need to create a modified table and use the `xkeymap.fileName` property instead.

- To use a different keysym mapping table that is not in the `xkeymap` directory, add the `xkeymap.fileName` property and set it to the path to the table.

  For example: **`xkeymap.fileName = "file_path"`**

  The table must list a keysym for each key by using the form *sym*="*v-scan_code*", where the *sym* value is an X keysym name and *v-scan_code* is a C-syntax hexadecimal number, for example, 0x001. Use a new line for each keysym.

  **NOTE** Because compiling a complete keysym mapping is difficult, you should usually edit an existing table and make small changes.

- To change the keysym mapping of a few keys, type the `xkeymap.keysym` property for each key, on separate lines.

  For example: **`xkeymap.keysym.sym = "v-scan_code"`**

  The value of *sym* must be an X keysym name and *v-scan_code* is a C-syntax hexadecimal number, for example, 0x001.

## V-Scan Code Table

You specify v-scan codes when you change how keys or keysyms are mapped.

Following are the v-scan codes for the 104-key U.S. keyboard.

**Table 4-2.** V-Scan Codes for the 104-Key U.S. Keyboard

| Symbol | Shifted Symbol | Location | V-Scan Code |
|---|---|---|---|
| Esc | | | 0x001 |
| 1 | ! | | 0x002 |
| 2 | @ | | 0x003 |
| 3 | # | | 0x004 |
| 4 | $ | | 0x005 |
| 5 | % | | 0x006 |
| 6 | ^ | | 0x007 |
| 7 | & | | 0x008 |
| 8 | * | | 0x009 |
| 9 | ( | | 0x00a |
| 0 | ) | | 0x00b |
| - | _ | | 0x00c |
| = | + | | 0x00d |
| Backspace | | | 0x00e |
| Tab | | | 0x00f |
| Q | | | 0x010 |
| W | | | 0x011 |

**Table 4-2.** V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

| Symbol | Shifted Symbol | Location | V-Scan Code |
|---|---|---|---|
| E | | | 0x012 |
| R | | | 0x013 |
| T | | | 0x014 |
| Y | | | 0x015 |
| U | | | 0x016 |
| I | | | 0x017 |
| O | | | 0x018 |
| P | | | 0x019 |
| [ | { | | 0x01a |
| ] | } | | 0x01b |
| Enter | | | 0x01c |
| Ctrl | | left | 0x01d |
| A | | | 0x01e |
| S | | | 0x01f |
| D | | | 0x020 |
| F | | | 0x021 |
| G | | | 0x022 |
| H | | | 0x023 |
| J | | | 0x024 |
| K | | | 0x025 |
| L | | | 0x026 |
| ; | | | 0x027 |
| ' | | | 0x028 |
| ` | | | 0x029 |
| Shift | | left | 0x02a |
| \ | \| | | 0x02b |
| Z | | | 0x02c |
| X | | | 0x02d |
| C | | | 0x02e |
| V | | | 0x02f |
| B | | | 0x030 |
| N | | | 0x031 |
| M | | | 0x032 |
| , | < | | 0x033 |
| . | > | | 0x034 |
| / | ? | | 0x035 |
| Shift | | right | 0x036 |
| * | | numeric pad | 0x037 |
| Alt | | left | 0x038 |

**Table 4-2.** V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

| Symbol | Shifted Symbol | Location | V-Scan Code |
|---|---|---|---|
| Space bar | | | 0x039 |
| Caps Lock | | | 0x03a |
| F1 | | | 0x03b |
| F2 | | | 0x03c |
| F3 | | | 0x03d |
| F4 | | | 0x03e |
| F5 | | | 0x03f |
| F6 | | | 0x040 |
| F7 | | | 0x041 |
| F8 | | | 0x042 |
| F9 | | | 0x043 |
| F10 | | | 0x044 |
| Num Lock | | numeric pad | 0x045 |
| Scroll Lock | | | 0x046 |
| Home | 7 | numeric pad | 0x047 |
| Up arrow | 8 | numeric pad | 0x048 |
| PgUp | 9 | numeric pad | 0x049 |
| - | | numeric pad | 0x04a |
| Left arrow | 4 | numeric pad | 0x04b |
| 5 | | numeric pad | 0x04c |
| Right arrow | 6 | numeric pad | 0x04d |
| + | | numeric pad | 0x04e |
| End | 1 | numeric pad | 0x04f |
| Down arrow | 2 | numeric pad | 0x050 |
| PgDn | 3 | numeric pad | 0x051 |
| Ins | 0 | numeric pad | 0x052 |
| Del | | numeric pad | 0x053 |
| F11 | | | 0x057 |
| F12 | | | 0x058 |
| Break | Pause | | 0x100 |
| Enter | | numeric pad | 0x11c |
| Ctrl | | right | 0x11d |
| / | | numeric pad | 0x135 |
| SysRq | Print Scrn | | 0x137 |
| Alt | | right | 0x138 |
| Home | | function pad | 0x147 |
| Up arrow | | function pad | 0x148 |
| Page Up | | function pad | 0x149 |
| Left arrow | | function pad | 0x14b |

**Table 4-2.** V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

| Symbol | Shifted Symbol | Location | V-Scan Code |
|---|---|---|---|
| Right arrow | | function pad | 0x14d |
| End | | function pad | 0x14f |
| Down arrow | | function pad | 0x150 |
| Page Down | | function pad | 0x151 |
| Insert | | function pad | 0x152 |
| Delete | | function pad | 0x153 |
| Windows | | left | 0x15b |
| Windows | | right | 0x15c |
| Menu | | | 0x15d |

The 84-key keyboard has a Sys Req key on the numeric pad. Its v-scan code is 0x054.

Keyboards outside the U.S. usually have an extra key (often < > or < > |) next to the left Shift key. The v-scan code for this key is 0x056.

# Modify Hardware Settings for a Virtual Machine

You can modify memory, processor, virtual and physical hard disk, CD-ROM and DVD drive, floppy drive, virtual network adapter, USB controller, sound card, serial port, generic SCSI device, printer, and display settings for a virtual machine.

### Procedure

1 Select the virtual machine, select **VM > Settings**.

2 Click the **Hardware** tab.

3 Select the hardware setting to modify.

4 Click **Help** for information about how to modify the hardware setting.

You must power off a virtual machine before you change certain hardware settings.

# Configuring Network Connections 5

Workstation provides bridged networking, network address translation (NAT), host-only networking, and custom networking options to configure a virtual machine for virtual networking. The software needed for all networking configurations is installed on the host system when you install Workstation.

This chapter includes the following topics:


- "Understanding Virtual Networking Components," on page 145
- "Understanding Common Networking Configurations," on page 146
- "Changing the Default Networking Configuration," on page 147
- "Configuring Bridged Networking," on page 151
- "Configuring Network Address Translation," on page 154
- "Configuring Host-Only Networking," on page 163
- "Assigning IP Addresses in Host-Only Networks and NAT Configurations," on page 169
- "Configuring LAN Segments," on page 172
- "Configuring Samba for Workstation," on page 174
- "Using Virtual Network Adapters in Promiscuous Mode on Linux Hosts," on page 175
- "Maintaining and Changing MAC Addresses for Virtual Machines," on page 175
- "Sample Custom Networking Configuration," on page 176


## Understanding Virtual Networking Components

The virtual networking components in Workstation include virtual switches, virtual network adapters, the virtual DHCP server, and the NAT device.

### Virtual Switches

Like a physical switch, a virtual switch connects networking components together. Virtual switches, which are also referred to as virtual networks, are named VMnet0, VMnet1, VMnet2, and so on. A few virtual switches are mapped to specific networks by default.

**Table 5-1.** Default Virtual Network Switches

| Network Type | Switch Name |
|---|---|
| Bridged | VMnet0 |
| NAT | VMnet8 |
| Host-only | VMnet1 |

Workstation creates virtual switches as needed, up to 20 virtual switches on a Windows host system and up to 255 virtual switches on a Linux host system. You can connect an unlimited number of virtual network devices to a virtual switch on a Windows host system and up to 32 virtual network devices to a virtual switch on a Linux host system.

**NOTE** On Linux host systems, the virtual switch names are in all lowercase letters, for example, vmnet0.

### Virtual Network Adapters

When you use the New Virtual Machine wizard to create a new virtual machine, the wizard creates a virtual network adapter for the virtual machine. The virtual network adapter appears in the guest operating system as an AMD PCNET PCI adapter or Intel Pro/1000 MT Server Adapter. In Windows Vista, Windows 7, and Windows 8 guest operating systems, it is an Intel Pro/1000 MT Server Adapter.

Workstation 6.0 and later virtual machines can have up to 10 virtual network adapters. Workstation 4 or 5.x virtual machines are limited to three virtual network adapters.

### Virtual DHCP Server

The virtual Dynamic Host Configuration Protocol (DHCP) server provides IP addresses to virtual machines in configurations that are not bridged to an external network. For example, the virtual DHCP server assigns IP addresses to virtual machines in host-only and NAT configurations.

### NAT Device

In a NAT configuration, the NAT device passes network data between one or more virtual machines and the external network, identifies incoming data packets intended for each virtual machine, and sends them to the correct destination.

## Understanding Common Networking Configurations

You can configure bridged networking, NAT, and host-only networking for virtual machines. You can also use the virtual networking components to create sophisticated custom virtual networks.

### Bridged Networking

Bridged networking connects a virtual machine to a network by using the network adapter on the host system. If the host system is on a network, bridged networking is often the easiest way to give the virtual machine access to that network.

When you install Workstation on a Windows or Linux host system, a bridged network (VMnet0) is set up for you.

### NAT Networking

With NAT, a virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host system. In the default configuration, a virtual machine gets an address on this private network from the virtual DHCP server. The virtual machine and the host system share a single network identity that is not visible on the external network.

When you install Workstation on a Windows or Linux host system, a NAT network (VMnet8) is set up for you. When you use the New Virtual Machine wizard to create a new virtual machine and select the typical configuration type, the wizard configures the virtual machine to use the default NAT network.

You can have only one NAT network.

### Host-Only Networking

Host-only networking creates a network that is completely contained within the host computer. Host-only networking provides a network connection between the virtual machine and the host system by using a virtual network adapter that is visible on the host operating system.

When you install Workstation on a Windows or Linux host system, a host-only network (VMnet1) is set up for you.

### Custom Networking Configurations

With the Workstation virtual networking components, you can create sophisticated virtual networks. The virtual networks can be connected to one or more external networks, or they can run entirely on the host system. You can use the virtual network editor to configure multiple network cards in the host system and create multiple virtual networks.

## Changing the Default Networking Configuration

When you choose the standard network options in the New Virtual Machine wizard, the wizard sets up the networking configuration for the virtual machine.

In a typical configuration, the New Virtual Machine wizard sets up NAT for the virtual machine. You must select the custom configuration option to configure bridged networking or host-only networking. The wizard connects the virtual machine to the appropriate virtual network.

You can change the networking configuration for a virtual machine by modifying virtual machine settings. For example, you can use virtual machine settings to add virtual network adapters and change existing virtual network adapters for a particular virtual machine.

You use the virtual network editor to change key networking settings, add and remove virtual networks, and create custom virtual networking configurations. The changes you make in the virtual network editor affect all virtual machines running on the host system.

---

**IMPORTANT** If you click **Restore Default** in the virtual network editor to restore network settings, all changes that you made to network settings after you installed Workstation are permanently lost. Do not restore the default network settings when a virtual machine is powered on as this might cause serious damage to bridged networking.

---

- Add a Virtual Network Adapter to a Virtual Machine on page 148

  You can add up to 10 virtual network adapters to a virtual machine.

- Modify an Existing Virtual Network Adapter for a Virtual Machine on page 148

  You can change the settings of a virtual network adapter that is currently used by a virtual machine.

- Disconnect a Host Virtual Network Adapter on page 149

  When you install Workstation, two virtual network adapters, VMware Network Adapter VMnet1 and VMware Network Adapter VMnet8, are added to the configuration of the host operating system. You might want to disconnect one or both of these virtual network adapters to improve performance on the host system.

- Configure Bandwidth and Packet Loss Settings for a Virtual Machine on page 150

  You can use advanced virtual network adapter settings to limit the bandwidth and specify the acceptable packet loss percentage for incoming and outgoing data transfers for a virtual machine.

## Add a Virtual Network Adapter to a Virtual Machine

You can add up to 10 virtual network adapters to a virtual machine.

NOTE Workstation 4 or 5.x virtual machines are limited to three virtual network adapters.

### Prerequisites

Familiarize yourself with the network configuration types. See "Understanding Common Networking Configurations," on page 146.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, click **Add**.

3 Select **Network Adapter**.

4 Select the virtual network adapter type.

You cannot select a custom network or LAN segment for a shared virtual machine. For a remote virtual machine, you must select a custom network.

| Option | Description |
|---|---|
| **Bridged** | The virtual machine is connected to the network by using the network adapter on the host system. The virtual machine has a unique identity on the network, separate from and unrelated to the host system. |
| **NAT** | The virtual machine and the host system share a single network identity that is not visible on the external network. When the virtual machine sends a request to access a network resource, it appears to the network resource as if the request is coming from the host system. |
| **Host-only** | The virtual machine and the host virtual network adapter are connected to a private Ethernet network. The network is completely contained within the host system. |
| **Custom** | Select a custom network from the drop-down menu. Although VMnet0, VMnet1, and VMnet8 might be available in the list, these networks are usually used for bridged, host-only, and NAT networks. |
| **LAN segment** | Select a LAN segment from the drop-down menu. A LAN segment is a private network that is shared by other virtual machines. |

5 Click **Finish** to add the virtual network adapter to the virtual machine.

6 Click **OK** to save your changes.

7 Verify that the guest operating system is configured to use an appropriate IP address on the new network.

a If the virtual machine is using DHCP, release and renew the lease.

b If the IP address is set statically, verify that the guest operating system has an address on the correct virtual network.

## Modify an Existing Virtual Network Adapter for a Virtual Machine

You can change the settings of a virtual network adapter that is currently used by a virtual machine.

### Prerequisites

Familiarize yourself with the network configuration types. See "Understanding Common Networking Configurations," on page 146.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select the virtual network adapter.

3 Select the virtual network adapter type.

You cannot select a custom network or LAN segment for a shared virtual machine. For a remote virtual machine, you must select a custom network.

| Option | Description |
|---|---|
| **Bridged** | The virtual machine is connected to the network by using the network adapter on the host system. The virtual machine has a unique identity on the network, separate from and unrelated to the host system. |
| **NAT** | The virtual machine and the host system share a single network identity that is not visible on the external network. When the virtual machine sends a request to access a network resource, it appears to the network resource as if the request is coming from the host system. |
| **Host-only** | The virtual machine and the host virtual network adapter are connected to a private Ethernet network. The network is completely contained within the host system. |
| **Custom** | Select a custom network from the drop-down menu. Although VMnet0, VMnet1, and VMnet8 might be available in this list, these networks are usually used for bridged, host-only, and NAT networks. |
| **LAN segment** | Select a LAN segment from the drop-down menu. A LAN segment is a private network that is shared by other virtual machines. |

4 Click **OK** to save your changes.

5 Verify that the guest operating system is configured to use an appropriate IP address on the new network.

a If the virtual machine is using DHCP, release and renew the lease.

b If the IP address is set statically, verify that the guest operating system has an address on the correct virtual network.

## Disconnect a Host Virtual Network Adapter

When you install Workstation, two virtual network adapters, VMware Network Adapter VMnet1 and VMware Network Adapter VMnet8, are added to the configuration of the host operating system. You might want to disconnect one or both of these virtual network adapters to improve performance on the host system.

Because broadcast packets must go to these adapters, the presence of virtual network adapters has a slight performance cost. On Windows networks, browsing the network might be slower than usual. In some cases, these adapters interact with the host computer networking configuration in undesirable ways.

You can reconnect a host virtual network adapter after you disconnect it.

### Prerequisites

- Determine whether you are going to use the host virtual network adapter. The host system uses VMware Network Adapter VMnet1 to connect to the host-only network and it uses VMware Network Adapter VMnet8 to connect to the NAT network.
- On a Windows host, log in as an Administrator user. Only an Administrator user can change network settings in the virtual network editor.
- On a Linux host, log in as root. You must enter the root password to use the virtual network editor.

### Procedure

1 Start the virtual network editor on the host system.

| Option | Description |
|---|---|
| **Windows host** | Select **Edit > Virtual Network Editor**. |
| **Linux host** | Select **Applications > System Tools > Virtual Network Editor**. The menu path might be different for your version of Linux. You can also start the network editor from the command line by using the `vmware-netcfg` command. |

2 Select the virtual network.

3 Deselect **Connect a host virtual adapter to this network** to disconnect the host virtual network adapter from the virtual network.

4 Click **OK** to save your changes.

## Configure Bandwidth and Packet Loss Settings for a Virtual Machine

You can use advanced virtual network adapter settings to limit the bandwidth and specify the acceptable packet loss percentage for incoming and outgoing data transfers for a virtual machine.

**NOTE** You cannot configure advanced virtual network adapter settings for a shared or remote virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select the virtual network adapter and click **Advanced**.

3 Select a bandwidth setting.

| Option | Description |
|---|---|
| **Limit incoming or outgoing data transfers to the data transfer rate for a specific network connection type** | Select the network connection type from the **Bandwidth** drop-down menu. The value in the **Kbps** text box changes to the data transfer rate, in kilobits per second, of the network connection type that you select. For example, if you select **Leased Line T1 (1.544 Mbps)**, the value in the **Kbps** text box changes to 1544. |
| **Limit incoming or outgoing data transfers to a specific data transfer rate** | Select **Custom** and type the data transfer rate, in kilobits per second, in the **Kbps** text box. |

4 Type the acceptable packet loss percentage for incoming and outgoing data transfers in the **Packet Loss (%)** text box.

The default setting is 0.0%.

5 Click **OK** to save your changes.

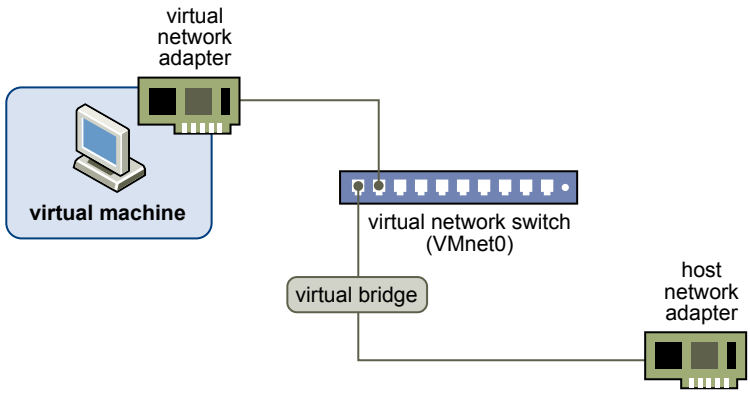
# Configuring Bridged Networking

When you install Workstation on a Windows or Linux host system, a bridged network (VMnet0) is set up for you. Bridged networking connects a virtual machine to a network by using the network adapter on the host system. If the host system is on a network, bridged networking is often the easiest way to give the virtual machine access to that network.

With bridged networking, the virtual network adapter in the virtual machine connects to a physical network adapter in the host system. The host network adapter enables the virtual machine to connect to the LAN that the host system uses. Bridged networking works with both wired and wireless host network adapters.

Bridged networking configures the virtual machine as a unique identity on the network, separate from and unrelated to the host system. The virtual machine is a full participant in the network. It has access to other machines on the network, and other machines on the network can contact it as if it were a physical computer on the network.

**Figure 5-1.** Bridged Networking Configuration




You can view and change the settings for bridged networking on the host system, determine which network adapters to use for bridged networking, and map specific host network adapters to specific virtual switches.

- Assigning IP Addresses in a Bridged Networking Environment on page 152

  A virtual machine must have its own identity on a bridged network. For example, on a TCP/IP network, the virtual machine needs its own IP address. Your network administrator can tell you whether IP addresses are available for virtual machines and which networking settings to use in the guest operating system.

- Add a Bridged Network on page 152

  When you install Workstation on a Windows or Linux host system, a bridged network (VMnet0) is set up for you. If you install Workstation on a host system that has multiple network adapters, you can configure multiple bridged networks.

- Configure Bridged Networking for an Existing Virtual Machine on page 152

  You can configure bridged networking for an existing virtual machine.

- Change VMnet0 Bridged Networking Settings on page 153

  By default, VMnet0 is set to use auto-bridging mode and is configured to bridge to all active network adapters on the host system. You can use the virtual network editor to change VMnet0 to bridge to one specific host network adapter, or restrict the host network adapters that VMnet0 auto-bridges to. The changes you make affect all virtual machines that use bridged networking on the host system.

## Assigning IP Addresses in a Bridged Networking Environment

A virtual machine must have its own identity on a bridged network. For example, on a TCP/IP network, the virtual machine needs its own IP address. Your network administrator can tell you whether IP addresses are available for virtual machines and which networking settings to use in the guest operating system.

Typically, the guest operating system can acquire an IP address and other network details from a DHCP server, but you might need to set the IP address and other details manually in the guest operating system.

Users who boot multiple operating systems often assign the same address to all systems because they assume that only one operating system will be running at a time. If the host system is set up to boot multiple operating systems, and you run one or more operating systems in virtual machines, you must configure each operating system to have a unique network address.

## Add a Bridged Network

When you install Workstation on a Windows or Linux host system, a bridged network (VMnet0) is set up for you. If you install Workstation on a host system that has multiple network adapters, you can configure multiple bridged networks.

For example, if the host system has two network adapters connected to two different networks, you might want virtual machines on the host system to bridge to both network adapters so that they can access either or both physical networks.

### Prerequisites

- Verify that a network adapter is available on the host system to bridge to. If VMnet0 is bridging to all of the available host network adapters (the default setting), you can modify it to make an adapter available. See "Change VMnet0 Bridged Networking Settings," on page 153.
- On a Windows host, log in as an Administrator user. Only an Administrator user can change network settings in the virtual network editor.
- On a Linux host, log in as root. You must enter the root password to access the virtual network editor.

### Procedure

1 Select **Edit > Virtual Network Editor**.

2 Click **Add Network** and select a network to add.

You can create a custom bridged network on VMnet2 to VMnet7. On Windows hosts, you can also use VMnet9. On Linux hosts, you can also use vmnet10 through vmnet255.

3 Select the new network and select **Bridged (connect VMs directly to the external network)**.

4 Select a host network adapter to bridge to from the **Bridged to** drop-down menu.

5 Click **OK** to save your changes.

## Configure Bridged Networking for an Existing Virtual Machine

You can configure bridged networking for an existing virtual machine.

To configure bridged networking for a new virtual machine, select **Customize Hardware** when you run the New Virtual Machine wizard.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Network Adapter**.

3 Select **Bridged: Connected directly to the physical network**.

4 If you use the virtual machine on a laptop or other mobile device, select **Replicate physical network connection state**.

This setting causes the IP address to be renewed when you move from one wired or wireless network to another.

5 Click **OK** to save your changes.

## Change VMnet0 Bridged Networking Settings

By default, VMnet0 is set to use auto-bridging mode and is configured to bridge to all active network adapters on the host system. You can use the virtual network editor to change VMnet0 to bridge to one specific host network adapter, or restrict the host network adapters that VMnet0 auto-bridges to. The changes you make affect all virtual machines that use bridged networking on the host system.

For example, you might want to change VMnet0 to bridge to a specific host network adapter, or to auto-bridge to as subset of the available host network adapters, to make a host network adapter available to create a second bridged network.

**IMPORTANT** If you reassign a host network adapter to a different virtual network, any virtual machine that is using the original network loses its network connectivity through that network and you must change the setting for each affected virtual machine network adapter individually. This restriction can be especially problematic if the host system has only one physical network adapter and you reassign it to a virtual network other than VMnet0. Even though the virtual network appears to be bridged to an automatically chosen adapter, the only adapter it can use was assigned to a different virtual network.

### Prerequisites

- On a Windows host, log in as an Administrator user. Only an Administrator user can change network settings in the virtual network editor.
- On a Linux host, log in as root. You must enter the root password to use the virtual network editor.

### Procedure

1 Select **Edit > Virtual Network Editor**.

2 Select **VMnet0**.

3 Change the host network adapters that VMnet0 bridges to.

| Option | Description |
|---|---|
| **Prevent VMnet0 from automatically bridging to a particular host network adapter** | a Click **Automatic Settings**.<br>b Deselect the check box for the host network adapter.<br>c Click **OK**. |
| **Disable automatic bridging and bridge VMnet0 to a specific host network adapter** | Select the host network adapter from the **Bridge to** drop-down menu. |

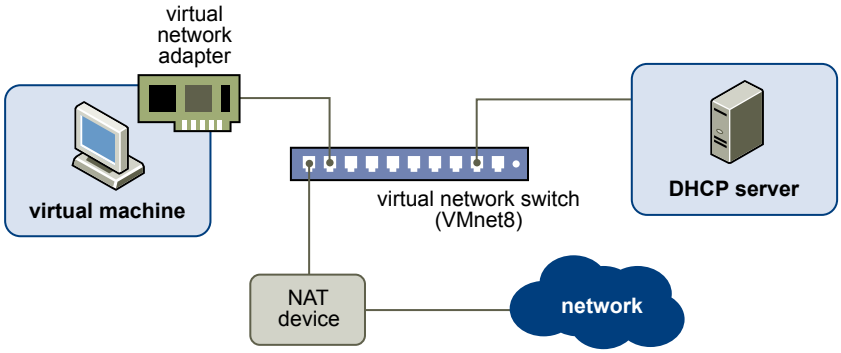
4 Click **OK** to save your changes.

# Configuring Network Address Translation

When you install Workstation on a Windows or Linux host system, a NAT network (VMnet8) is set up for you. When you use the New Virtual Machine wizard to create a typical virtual machine, the wizard configures the virtual machine to use the default NAT network.

With NAT, a virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host system. In the default configuration, virtual machines get an address on this private network from the virtual DHCP server.

**Figure 5-2.** NAT Configuration




The virtual machine and the host system share a single network identity that is not visible on the external network. NAT works by translating the IP addresses of virtual machines in the private network to the IP address of the host system. When a virtual machine sends a request to access a network resource, it appears to the network resource as if the request is coming from the host system.

The host system has a virtual network adapter on the NAT network. This adapter enables the host system and virtual machines to communicate with each other. The NAT device passes network data between one or more virtual machines and the external network, identifies incoming data packets intended for each virtual machine, and sends them to the correct destination.

- Features and Limitations of NAT Configurations on page 155

  NAT is useful when the number of IP addresses is limited or the host system is connected to the network through a non-Ethernet adapter.

- Change NAT Settings on a Windows Host on page 156

  You can use the virtual network editor to change NAT settings. For example, you can change the gateway IP address, add a port for forwarding, and change DNS and NetBIOS settings.

- Editing the NAT Configuration File on page 158

  If you are an advanced user, you can edit the NAT configuration file to modify NAT settings.

- Using NAT with NetLogon on page 161

  If you use NAT networking in a Windows virtual machine running on a Windows host system, you can use NetLogon to log in to a Windows domain from the virtual machine and access file shares that the WINS server knows.

- Specifying Connections from Source Ports Below 1024 on page 162

  If a virtual machine that uses NAT attempts to connect to a server that requires the client to use a source port below 1024, the NAT device must forward the request from a port below 1024. For security reasons, some servers accept connections only from source ports below 1024.

## Features and Limitations of NAT Configurations

NAT is useful when the number of IP addresses is limited or the host system is connected to the network through a non-Ethernet adapter.

With NAT, a virtual machine can use many standard TCP/IP protocols to connect to other machines on the external network. For example, you can use HTTP to browse Web sites, FTP to transfer files, and Telnet to log in to other computers. You also can connect to a TCP/IP network by using a Token Ring adapter on the host system. NAT works with Ethernet, DSL, and phone modems.

In the default NAT configuration, computers on the external network cannot initiate connections to the virtual machine. For example, you cannot use the virtual machine as a Web server to send Web pages to computers on the external network. This feature protects the guest operating system from being compromised before you have a chance to install security software.

NAT configurations have the following additional features and limitations.

- NAT causes some performance loss. Because NAT requires that every packet sent to and received from a virtual machine must be in the NAT network, an unavoidable performance penalty occurs.
- NAT is not perfectly transparent. NAT does not usually allow connections to be initiated from outside the network, although you can manually configure the NAT device to set up server connections. The practical result is that some TCP and UDP protocols that require a connection be initiated from the server machine do not work automatically and some might not work at all.
- NAT provides some firewall protection. A standard NAT configuration provides basic-level firewall protection because the NAT device can initiate connections from the private NAT network, but devices on the external network usually cannot initiate connections to the private NAT network.

### Understanding DHCP in a NAT Configuration

In a NAT configuration, virtual machines running on the network with the NAT device can send DHCP requests to dynamically obtain their IP addresses.

In the default configuration, the virtual DHCP server dynamically allocates IP addresses in the range of *net*.128 through *net*.254, where *net* is the network number assigned to the NAT network. Workstation always uses a Class C address for NAT networks. IP addresses *net*.3 through *net*.127 can be used for static IP addresses. IP address net.1 is reserved for the host virtual network adapter and *net*.2 is reserved for the NAT device.

In addition to the IP address, the virtual DHCP server on the NAT network sends out configuration information that enables the virtual machine to operate. This information includes the default gateway and the DNS server. In the DHCP response, the NAT device instructs the virtual machine to use the IP address *net*.2 as the default gateway and DNS server. This routing causes all IP packets destined for the external network and DNS requests to be forwarded to the NAT device.

### Understanding the NAT Device

The NAT device is connected to the VMnet8 virtual switch. Virtual machines connected to the NAT network also use the VMnet8 virtual switch.

The NAT device waits for packets coming from virtual machines on the VMnet8 virtual network. When a packet arrives, the NAT device translates the address of the virtual machine to the address of the host system before forwarding the packet to the external network.

When data arrives from the external network for the virtual machine on the private network, the NAT device receives the data, replaces the network address with the address of the virtual machine, and forwards the data to the virtual machine on the virtual network. This translation occurs automatically and requires minimal configuration on the guest operating system and the host system.

The NAT device is a DNS proxy and forwards DNS requests from the virtual machines to a DNS server that the host system knows. Responses return to the NAT device, which then forwards them to the virtual machines.

If they get their configuration information from the virtual DHCP server, the virtual machines on the NAT network use the NAT device as the DNS server. The virtual machines in the private NAT network are not accessible through DNS. To have the virtual machines running on the NAT network access each other by DNS names, you must set up a private DNS server connected to the NAT network and configure the virtual machines to use the DNS server.

### Accessing External Networks from a NAT Network

For most client applications, including Web browsers, Telnet, passive-mode FTP, and downloaded streaming video, a virtual machine on a NAT network can use any protocol using TCP or UDP if the virtual machine initiates the network connection. Additional protocol support is built into the NAT device to allow FTP and ICMP echo (ping) to work transparently through the NAT device.

On the external network, a virtual machine on the NAT network appears to be the host system because its network traffic uses the host system IP address. The virtual machine can send and receive data by using TCP/IP to any machine that is accessible from the host system.

Before any communication can occur, the NAT device must set up a map between the virtual machine address on the private NAT network and the host network address on the external network. When a virtual machine initiates a network connection with another network resource, this map is created automatically. The operation is transparent to the user of the virtual machine on the NAT network.

Network connections that are initiated from outside the NAT network to a virtual machine on the NAT network are not transparent. When a machine on the external network attempts to initiate a connection with a virtual machine on the NAT network, it cannot reach the virtual machine because the NAT device does not forward the request. You can configure port forwarding manually on the NAT device so that network traffic destined for a certain port can still be forwarded automatically to a virtual machine on the NAT network.

File sharing of the type used by Windows operating systems and Samba is possible among computers on the NAT network, including virtual machines and the host system. If you use WINS servers on your network, a virtual machine that uses NAT networking can access shared files and folders on the host system that the WINS server knows if those shared files and folders are in the same workgroup or domain.

## Change NAT Settings on a Windows Host

You can use the virtual network editor to change NAT settings. For example, you can change the gateway IP address, add a port for forwarding, and change DNS and NetBIOS settings.

To change NAT settings on a Linux host, you must edit the NAT configuration file. See "Editing the NAT Configuration File," on page 158.

#### Prerequisites

- Familiarize yourself with the NAT settings. See "NAT Settings," on page 157.
- Log in as an Administrator user. Only an Administrator user can change network settings in the virtual network editor.

#### Procedure

1. On the Windows host system, select **Edit > Virtual Network Editor**.
2. Select the NAT network and click **NAT Settings** and change the NAT settings.
3. Click **OK** to save your changes.

## NAT Settings

On a Windows host, you can use the virtual network editor to change the gateway IP address, configure port forwarding, and configure advanced networking settings for a NAT network.

**Table 5-2.** NAT Settings

| Setting | Description | |
|---|---|---|
| **Gateway IP** | Specifies the gateway IP address for the selected network. | |
| **Port Forwarding** | Add a port for port forwarding. With port forwarding, incoming TCP or UDP requests are sent to a specific virtual machine on the virtual network that is served by the NAT device. | |
| | **Host port** | The number of the incoming TCP or UDP port. For example, incoming HTTP requests are usually on port 80. |
| | **Virtual machine IP address** | The IP address of the virtual machine to which you want to forward the incoming requests. |
| | **Virtual machine port** | The port number to use for requests on the specified virtual machine. It may be the standard port, such as 80 for HTTP, or a nonstandard port if software running in the virtual machine is configured to accept requests on a nonstandard port. |
| | **Description** | (Optional) You can use this text box to identify the forwarded service, for example, HTTP. |
| | To change settings for an existing port, select its name and click **Properties**. | |
| **Allow active FTP** | Specifies whether to allow only passive mode FTP over the NAT device. | |
| **Allow any Organizationally Unique Identifier** | Select this setting if you change the organizationally unique identifier (OUI) portion of the MAC address for the virtual machine and subsequently cannot use NAT with the virtual machine. | |
| **UDP timeout (in seconds)** | Select the number of minutes to keep the UDP mapping for the NAT. | |
| **Config port** | Select the port to use to access status information about NAT.<br>IMPORTANT Change this value only under the direction of VMware technical support. | |
| **DNS Settings** | Configure the DNS servers for the virtual NAT device to use. | |
| | **Auto detect available DNS servers** | Select this option to detect the available DNS servers. To add a DNS server to the list, deselect this check box and enter the IP address of the preferred and alternate DNS servers in the **Preferred DNS server** text boxes. |
| | **Policy** | If you have multiple DNS servers, select the strategy for choosing which server to send a request to. **Order** sends one DNS request at a time in order of the name. **Rotate** sends one DNS request at a time and rotates through the DNS servers. **Burst** sends to three servers and waits for the first server to respond. |
| | **Timeout (sec)** | Select the number of seconds to keep trying if the NAT device cannot connect to the DNS server. |
| | **Retries** | Select the number of retries. |
| **NetBios Settings** | Select NBNS (NetBIOS Name Service) and NBDS (NetBIOS Datagram Service) timeouts and retry settings. | |

## Editing the NAT Configuration File

If you are an advanced user, you can edit the NAT configuration file to modify NAT settings.

The location of the NAT configuration file depends on the host operating system.

**Table 5-3.** NAT Configuration File Location

| Host Operating System | NAT Configuration File Location |
|---|---|
| Windows XP | `C:\Documents and Settings\All Users\Application Data\VMware\vmnetnat.conf` |
| Windows Vista or Windows 7 | `C:\ProgramData\VMware\vmnetnat.conf` |
| Linux | `/etc/vmware/vmnet8/nat/nat.conf` |

The NAT configuration file is divided into sections, and each section configures a part of the NAT device. Text surrounded by square brackets, such as **`[dns]`**, marks the beginning of a section. Each section contains one or more configuration parameters. The configuration parameters take the form **`ip = 192.168.27.1/24`**.

On a Windows host system, you can change the NAT configuration by using the virtual network editor. You do not need to edit the NAT configuration file. On a Linux host system, you must edit the NAT configuration file to modify the NAT configuration.

**IMPORTANT** Make a backup copy of the NAT configuration file. If you edit the NAT configuration file and then use the virtual network editor, your edits might be lost.

### NAT Configuration File Sections

The NAT configuration file is divided into sections. The parameters in each section configure a part of the NAT device.

#### [host] Section

The [host] section includes parameters to configure the NAT connection.

**Table 5-4.** [host] Section Parameters

| Parameter | Description |
|---|---|
| `ip` | The IP address that the NAT device should use. It can be followed by a slash and the number of bits in the subnet. |
| `netmask` | The subnet mask to use for the NAT network. DHCP addresses are allocated from this range of addresses. |
| `configport` | A port that can be used to access status information about the NAT device. |
| `device` | The VMnet device to use. Windows devices are of the form `vmnetx` where *x* is the number of the VMnet. Linux devices are of the form `/dev/vmnetx`. |
| `activeFTP` | Flag to indicate if active FTP is to be allowed. Active FTP allows incoming connections to be opened by the remote FTP server. Turning this off means that only passive mode FTP works. Set this flag to `0` to turn it off. |

#### [udp] Section

The [udp] section contains the `timeout` parameter, which specifies the number of seconds to keep the UDP mapping for the NAT network.

#### [dns] Section

The [dns] section is for Windows hosts only. Linux hosts do not use this section.

**Table 5-5.** [dns] Section Parameters

| Parameter | Description |
|---|---|
| `policy` | Policy to use for DNS forwarding.<br>■ `order` sends one DNS request at a time in the order of the name servers.<br>■ `rotate` sends one DNS request at a time and rotate through the DNS servers.<br>■ `burst` sends to three servers and wait for the first one to respond. |
| `timeout` | Time in seconds before retrying a DNS request. |
| `retries` | Number of retries before the NAT device stops trying to respond to a DNS request. |
| `autodetect` | Flag to indicate whether the NAT device should detect the DNS servers available to the host. |
| `nameserver1` | IP address of a DNS server to use. |
| `nameserver2` | IP address of a DNS server to use. |
| `nameserver3` | IP address of a DNS server to use. |

If autodetect is on and some name servers are specified, the DNS servers specified in `nameserver1`, `nameserver2`, and `nameserver3` are added before the list of detected DNS servers.

### [netbios] Section

The [netbios] section applies to Windows hosts only. Linux hosts do not use this section.

**Table 5-6.** [netbios] Section Parameters

| Parameter | Description |
|---|---|
| `nbnsTimeout = 2` | Timeout, in seconds, for NBNS queries. |
| `nbnsRetries = 3` | Number of retries for each NBNS query. |
| `nbdsTimeout = 3` | Timeout, in seconds, for NBDS queries. |

### [incomingtcp] Section

The [incomingtcp] section configures TCP port forwarding for NAT. You can assign a port number to an IP address and port number on a virtual machine.

This example creates a map from port 8887 on the host to the IP address 192.168.27.128 and port 21.

```
8887 = 192.168.27.128:21
```

When this map is set and an external machine connects to the host at port 8887, the network packets are forwarded to port 21 (the standard port for FTP) on the virtual machine that has IP address 192.168.27.128.

### [incomingudp] Section

The [incomingudp] section configures UDP port forwarding for NAT. You can assign a port number to an IP address and port number on a virtual machine.

This example creates a map from port 6000 on the host to the IP address 192.168.27.128 and port 6001.

```
6000 = 192.168.27.128:6001
```

When this map is set and an external machine connects to the host at port 6000, the network packets are forwarded to port 6001 on the virtual machine that has IP address 192.168.27.128.

## Sample Linux nat.conf File

This is an example of a NAT configuration file on a Linux host system.

```
# Linux NAT configuration file
[host]
# NAT gateway address
ip = 192.168.237.2/24
hostMAC = 00:50:56:C0:00:08
# enable configuration; disabled by default for security reasons
#configport = 33445
# vmnet device if not specified on command line
device = vmnet8
# Allow PORT/EPRT FTP commands (they need incoming TCP stream...)
activeFTP = 1
# Allows the source to have any OUI. Turn this one if you change the OUI
# in the MAC address of your virtual machines.
#allowAnyOUI = 1
[udp]
# Timeout in seconds, 0 = no timeout, default = 60; real value might
# be up to 100% longer
timeout = 30
[dns]
# This section applies only to Windows.
#
# Policy to use for DNS forwarding. Accepted values include order,
# rotate, burst.
#
# order: send one DNS request at a time in order of the name servers
# rotate: send one DNS request at a time, rotate through the DNS servers
# burst: send to three servers and wait for the first one to respond
policy = order;
# Timeout in seconds before retrying DNS request.
timeout = 2
# Retries before giving up on DNS request
retries = 3
# Automatically detect the DNS servers (not supported in Windows NT)
autodetect = 1
# List of DNS servers to use. Up to three may be specified
#nameserver1 = 208.23.14.2
#nameserver2 = 63.93.12.3
#nameserver3 = 208.23.14.4
[netbios]
# This section applies only to Windows.
# Timeout for NBNS queries.
nbnsTimeout = 2
# Number of retries for each NBNS query.
nbnsRetries = 3
# Timeout for NBDS queries.
nbdsTimeout = 3
[incomingtcp]
# Use these with care - anyone can enter into your virtual machine through
# these...
# FTP (both active and passive FTP is always enabled)
#   ftp localhost 8887
```

```
#8887 = 192.168.27.128:21
# WEB (make sure that if you are using named webhosting, names point to
#   your host, not to guest... And if you are forwarding port other
#   than 80 make sure that your server copes with mismatched port
#   number in Host: header)
#   lynx http://localhost:8888
#8888 = 192.168.27.128:80
# SSH
#   ssh -p 8889 root@localhost
#8889 = 192.168.27.128:22
[incomingudp]
# UDP port forwarding example
#6000 = 192.168.27.128:6001
```

## Using NAT with NetLogon

If you use NAT networking in a Windows virtual machine running on a Windows host system, you can use NetLogon to log in to a Windows domain from the virtual machine and access file shares that the WINS server knows.

To use NetLogon, you need to set up the virtual machine to use NetLogon. The setup process is similar to the way you set up a physical computer on one LAN that is using a domain controller on another LAN.

To log in to a Windows domain outside the virtual NAT network, the virtual machine needs access to a WINS server for that domain. If the WINS server that the DHCP server uses on the NAT network is already set up on the host system, you can connect the virtual machine to it. To connect from the virtual machine to a WINS server that is not set up on the host system, you must manually configure the IP address of the WINS server.

After the virtual machine has an IP address for a WINS server, you can use NetLogon in the virtual machine to log in to a domain and access shares in that domain. Your access is limited to shares of virtual machines that are on the same NAT network or are bridged on the same domain.

For example, if the WINS server covers a domain with a domain controller, you can access that domain controller from the virtual machine and add the virtual machine to the domain. You need the Administrator user ID and password for the domain controller.

### Use NAT to Connect to an Existing WINS Server on the Host

If the WINS server that the DHCP server uses on the NAT network is already set up on the host system, you can connect the virtual machine to it.

You can use this procedure for Windows 2000, XP, 2003 Server, NT, Me, and 9x guest operating systems. The steps might be different, depending on the Windows operating system type.

#### Procedure

1 In the Windows virtual machine, right-click **My Network Places** and select **Properties**.

2 Right-click the virtual network adapter and click **Properties**.

3 In the Properties dialog box, select **Internet Protocol (TCP/IPv4)** and click **Properties**.

4 In the TCP/IP Properties dialog box, click **Advanced**.

5 On the **WINS** tab, under the **NetBIOS** setting, select **Default: Use NetBIOS setting from DHCP Server**.

6 Click **OK** twice and click **Close**.

### Configure the IP Address of a WINS Server Manually

To connect from a virtual machine to a WINS server that is not set up on the host system, you must manually configure the IP address of the WINS server.

You can use this procedure for Windows 2000, XP, 2003 Server, NT, Me, and 9x guest operating systems. The steps might be different, depending on the Windows operating system type. Repeat this procedure for each WINS server that you want to connect to from the virtual machine.

#### Procedure

1 In the Windows virtual machine, right-click **My Network Places** and select **Properties**.

2 In the Network Connections window, right-click the virtual network adapter and choose **Properties**.

3 In the Properties dialog box, select **Internet Protocol (TCP/IPv4)** and click **Properties**.

4 In the TCP/IP Properties dialog box, click **Advanced**.

5 On the **WINS** tab, click **Add**.

6 In the TCP/IP WINS Server dialog box, type the IP address for the WINS server in the **WINS server** text box and click **Add**.

The IP address of the WINS server appears in the WINS addresses list on the WINS tab.

7 Click **OK** twice and click **Close**.

## Specifying Connections from Source Ports Below 1024

If a virtual machine that uses NAT attempts to connect to a server that requires the client to use a source port below 1024, the NAT device must forward the request from a port below 1024. For security reasons, some servers accept connections only from source ports below 1024.

The parameters that control virtual machine source and destination ports are in the `[privilegedUDP]` and `[privilegedTCP]` sections in the NAT configuration file. You might need to add settings or modify settings in either or both of these sections, depending on the kind of connection you need to make. You can set two parameters, each of which appears on a separate line.

**Table 5-7.** Parameters that Map Virtual Machine Source and Destination Ports

| Parameter | Description |
|---|---|
| `autodetect = n` | Determines whether the NAT device attempts to map virtual machine source ports below 1024 to NAT source ports below 1024. A setting of `1` means true. A setting of `0` means false. On a Windows host, the default is `1` (true). On a Linux host, the default is `0` (false). |
| `port = n` | Specifies a destination port, where *n* is the port on the server that accepts the connection from the client. When a virtual machine connects to the specified port on any server, the NAT device attempts to make the connection from a source port below 1024. You can include one or more port settings in the `[privilegedUDP]` or `[privilegedTCP]` section or in both sections, as required for the connections you need to make. Enter each port setting on a separate line. |

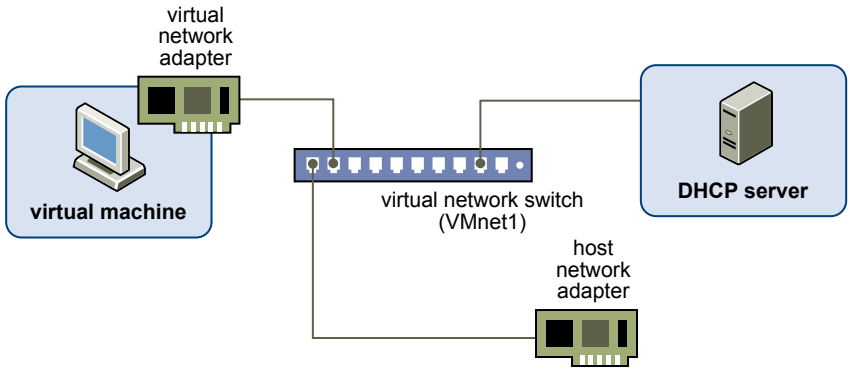
See "Editing the NAT Configuration File," on page 158 for more information.

# Configuring Host-Only Networking

When you install Workstation on a Windows or Linux host system, a host-only network (VMnet1) is set up for you. Host-only networking is useful if you need to set up an isolated virtual network. In a host-only network, the virtual machine and the host virtual network adapter are connected to a private Ethernet network. The network is completely contained within the host system.

The network connection between the virtual machine and the host system is provided by a virtual network adapter that is visible on the host operating system. The virtual DHCP server provides IP addresses on the host-only network.

**Figure 5-3.** Host-Only Networking Configuration




In the default configuration, a virtual machine in a host-only network cannot connect to the Internet. If you install the proper routing or proxy software on the host system, you can establish a connection between the host virtual network adapter and a physical network adapter on the host system to connect the virtual machine to a Token Ring or other non-Ethernet network.

On a Windows XP or Windows Server 2003 host computer, you can use host-only networking in combination with the Internet connection sharing feature in Windows to allow a virtual machine to use the dial-up networking adapter or other connection to the Internet on the host system. See Microsoft documentation for information on configuring Internet connection sharing.

- Add a Host-Only Network on page 164

  When you install Workstation on a Windows or Linux host system, a host-only network (VMnet1) is set up for you. You might want to configure multiple host-only networks to manage network traffic between virtual machines in specific ways.

- Configure Host-Only Networking for an Existing Virtual Machine on page 164

  You can configure host-only networking for an existing virtual machine. You can connect a virtual network adapter to the default host-only network (VMnet1) or to a custom host-only network. If a virtual machine has two virtual network adapters, you can connect it to two host-only networks.

- Set Up Routing Between Two Host-Only Networks on page 165

  If you are setting up a complex test network that uses virtual machines, you might want to have two independent host-only networks with a router between them.

- Avoiding IP Packet Leakage in Host-Only Networks on page 166

  Each host-only network should be confined to the host system on which it is set up. Packets that virtual machines send on this network should not leak out to a physical network attached to the host system. Packet leakage can occur only if a machine actively forwards packets.

- Controlling Routing Information for Host-Only Networks on Linux on page 167

  A host-only network has a network interface associated with it (vmnet1) that is marked up when the host operating system is booted. Routing server processes that operate on the host operating system automatically discover the host-only network and propagate information on how to reach the network, unless you explicitly configure them not to do so.

- Using DHCP and DDNS with Host-Only Networking on Linux on page 168

  The virtual DHCP server in Workstation cannot update a DNS server by using a Dynamic Domain Name Service (DDNS). For this reason, you should use DHCP to supply IP addresses as well as other information, such as the identity of a host running a name server and the nearest router or gateway.

## Add a Host-Only Network

When you install Workstation on a Windows or Linux host system, a host-only network (VMnet1) is set up for you. You might want to configure multiple host-only networks to manage network traffic between virtual machines in specific ways.

For example, you can set up multiple host-only networks on the same host system to test routing between two virtual networks or test a virtual machine that has multiple network interface cards without using any physical network adapters. You might also want to have two virtual machines connected to one host-only network and other virtual machines connected to another host-only network to isolate the network traffic on each network.

### Prerequisites

- On a Windows host, log in as an Administrator user. Only an Administrator user can change network settings in the virtual network editor.
- On a Linux host, log in as root. You must enter the root password to use the virtual network editor.

### Procedure

1 Select **Edit > Virtual Network Editor**.

2 Click **Add Network** and select a network to add, for example, **VMnet2**.

  You can create a custom host-only network on VMnet2 to VMnet7. On Windows hosts, you can also use VMnet9. On Linux hosts, you can also use vmnet10 through vmnet255.

  The new network is configured as a host-only network by default.

3 Click **OK** to save your changes.

After the host-only networks are set up on a Linux host system, at least four network interfaces appear: eth0, lo, vmnet1, and vmnet2. These four interfaces should have different IP addresses on separate subnets.

## Configure Host-Only Networking for an Existing Virtual Machine

You can configure host-only networking for an existing virtual machine. You can connect a virtual network adapter to the default host-only network (VMnet1) or to a custom host-only network. If a virtual machine has two virtual network adapters, you can connect it to two host-only networks.

To configure host-only networking for a new virtual machine, select **Customize Hardware** when you run the New Virtual Machine wizard.

### Prerequisites

To connect the virtual machine to two host-only networks, add a second virtual network adapter to the virtual machine. See "Add a Virtual Network Adapter to a Virtual Machine," on page 148.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab select a virtual network adapter.

3 Select the host-only network.

| Option | Action |
|---|---|
| **Use the default host-only network (VMnet1)** | Select **Host-only: A private network shared with the host**. |
| **Use a custom host-only network** | Select **Custom** and select the custom host-only network from the drop-down menu. |

4 To connect the virtual machine to a second host-only network, select another virtual network adapter and select the second host-only network.

5 Click **OK** to save your changes.

### What to do next

Assign IP addresses to the virtual network adapters. To see the IP address that a host-only network is using, use the `ipconfig /all` command on a Windows host or the `ipconfig` command on a Linux host.

## Set Up Routing Between Two Host-Only Networks

If you are setting up a complex test network that uses virtual machines, you might want to have two independent host-only networks with a router between them.

You can run the router software on the host system or on its own virtual machine. In both cases, you need two host-only networks.

In a simple configuration, you configure one virtual machine on each of the host-only networks. For more complex configurations, you can add more virtual machines and host-only networks.

### Prerequisites

Create a second host-only network. On Windows and Linux host systems, the first host-only network (VMnet1) is set up for you when you install Workstation. See "Add a Host-Only Network," on page 164.

### Procedure

1 Set up the connection to the first host-only network.

   a Select the virtual machine and select **VM > Settings**.

   b On the **Hardware** tab, select **Network Adapter**.

   c Select **Host-only** to connect to the default host-only network (VMnet1).

2 Set up the connection to the second host-only network.

   a Select the virtual machine and select **VM > Settings**.

   b On the **Hardware** tab, select **Network Adapter**.

   c Select **Custom** and select the custom host-only network from the drop-down menu.

3 (Optional) To run the router software on a virtual machine, set up a third virtual machine that has connections to the two host-only networks.

   a Select the virtual machine and select **VM > Settings**.

   b On the **Hardware** tab, select **Network Adapter**.

c Select **Host-only**.

The adapter is connected to the default host-only interface (VMnet1).

d Select the second network adapter, select **Custom**, and select the custom host-only network from the drop-down menu.

4 Stop the VMware DHCP Server service.

| Option | Description |
|---|---|
| **Windows host** | Use the `services.msc` command to open the Services Console and stop the VMware DHCP Service. |
| **Linux host** | Use the `killall –TERM vmnet–dhcpd` command to stop the `vmnet–dhcpd` service. |

5 Install the router software on the host system or in the third virtual machine, depending on the approach you are using.

6 Configure networking in the first two virtual machines to use addresses on the appropriate host-only network.

| Option | Description |
|---|---|
| **Windows host** | Use the `ipconfig /all` command to determine which IP addresses each host-only network is using. |
| **Linux host** | Use the `ifconfig` command to determine which IP addresses each host-only network is using. |

7 Assign IP addresses.

| Option | Description |
|---|---|
| **The router software is on the host system** | Assign default router addresses based on the addresses of the host-only adapters on the host computer. In the first virtual machine, the default router address should be the IP address for the host-only adapter connected to VMnet1. In the second virtual machine, the default router address should be the IP address for the host-only adapter connected to VMnet2. |
| **The router software is in a third virtual machine** | Set the default router addresses in the first two virtual machines based on the addresses that the third virtual machine. In the first virtual machine, the default router address should be the IP address for the network adapter connected to VMnet1 in third virtual machine. In the second virtual machine, the default router address should be the IP address for the network adapter connected to VMnet2 in third virtual machine. |

8 Ping the router machine from the first and second virtual machines.

If the router software is set up correctly, you can communicate between the first and second virtual machines.

## Avoiding IP Packet Leakage in Host-Only Networks

Each host-only network should be confined to the host system on which it is set up. Packets that virtual machines send on this network should not leak out to a physical network attached to the host system. Packet leakage can occur only if a machine actively forwards packets.

If you use dial-up networking support in a virtual machine and packet forwarding is enabled, host-only network traffic might leak out through the dial-up connection. To prevent the leakage, disable packet forwarding in the guest operating system.

If the host system has multiple network adapters, it might be intentionally configured to use IP forwarding. If that is the case, you do not want to disable forwarding. To avoid packet leakage, you must enable a packet filtering facility and specify that packets from the host-only network should not be sent outside the host system. See the operating system documentation for information on configuring packet filtering.

### Disable Packet Forwarding on a Windows Host

Systems that use server versions of Windows operating systems can forward IP packets that are not addressed to them. These systems, and Windows Vista and Windows 7 systems, have IP packet forwarding disabled by default.

If packets are leaking from a host-only network on a Windows host system, check whether packet forwarding is enabled on the host system. If packet forwarding is enabled, you must disable it.

---

**NOTE** IP forwarding is not a problem on Windows XP Professional or Windows XP Home Edition host systems.

---

#### Procedure

- On a Windows Vista or Windows 7 host, stop the Routing and Remote Access service.
  a. Type **`services.msc`** to open the Services Console.
  b. Select **Routing and Remote Access** and click **Stop**.
- On a Windows 2003 Server host, use Windows Administrative Tools to disable routing and remote access.
  a. Select **Start > Programs > Administrative Tools > Routing and Remote Access**.

     An icon on the left is labeled with the host name. If a green dot appears over the icon, IP forwarding is turned on.
  b. To turn off IP forwarding, right-click the icon and disable **Routing and Remote Access**.

     A red dot appears, indicating that IP forwarding is disabled.

### Disable Packet Forwarding on a Linux Host

If packets are leaking from a host-only network on a Linux host system, packet forwarding might be mistakenly enabled on the host system. If packet forwarding is enabled, you must disable it.

How you disable packet forwarding depends on your Linux distribution. For example, you might be able to use a control panel, specify a setting at the time you compile your kernel, or enter a specification when you boot your system. See the operating system documentation for more information.

#### Procedure

- As root, write a 0 (zero) to the special file `/proc/sys/net/ipv4/ip_forward`.

```
echo "0" > /proc/sys/net/ipv4/ip_forward
```

## Controlling Routing Information for Host-Only Networks on Linux

A host-only network has a network interface associated with it (vmnet1) that is marked up when the host operating system is booted. Routing server processes that operate on the host operating system automatically discover the host-only network and propagate information on how to reach the network, unless you explicitly configure them not to do so.

If you are running the routed or gated daemon only to receive routing information, the simplest solution is to run the routing configuration with the `–q` option so that the host-only network receives, but does not supply, routing information.

If you are running routing services to supply routing information, configure the services so that they do not advertise routes to the host-only network. The routed daemon version that is included with many Linux distributions does not support specifying that an interface should not be advertised. See the *routed(8)* manual page for your system for more information.

If you are using the gated daemon, you must explicitly exclude the vmnet1 interface from any protocol activity. If you need to run virtual machines on a host-only network on a multihomed system where gated is used and you experience problems, contact VMware technical support.

## Using DHCP and DDNS with Host-Only Networking on Linux

The virtual DHCP server in Workstation cannot update a DNS server by using a Dynamic Domain Name Service (DDNS). For this reason, you should use DHCP to supply IP addresses as well as other information, such as the identity of a host running a name server and the nearest router or gateway.

To use names to communicate with other virtual machines, you must either edit the DHCP configuration file for vmnet1 (`/etc/vmware/vmnet1/dhcpd/dhcpd.conf`), or use IP addresses that are statically bound to a host name. Editing the DHCP server configuration file requires information that is best obtained directly from the DHCP server documentation. See the *dhcpd(8)* and *dhcpd.conf(8)* manual pages.

---

**NOTE** The edits made inside the read-only section of the DHCP configuration file are lost the next time you run the virtual network editor.

---

### Troubleshooting DHCPD Problems on a Linux Host

If a DHCP server (`dhcpd`) utility was running on the Linux host system before you installed Workstation, it might have noticed that an additional network interface, vmnet1, was marked up and available for use when host-only networking was configured.

Some `dhcpd` implementations abort if their configuration files do not include a subnet specification for the interface. This can happen even if `dhcpd` is not supposed to respond to messages that arrive through the interface.

The best solution is to add a line to the `dhcpd` configuration file in the format **`subnet net.0 netmask 255.255.255.0 {}`**. The *net* value is the network number assigned to the host-only network, for example, **`192.168.0`**. This line in the configuration file informs `dhcpd` about the host-only network and tells it explicitly not to respond to any `dhcpd` requests arriving from that network.

An alternative solution is to explicitly state the set of network interfaces for `dhcpd` to monitor each time you start the program. For example, if the host system has one Ethernet interface (`eth0`), list the interface on the command line each time you start `dhcpd`.

```
dhcpd eth0
```

This solution prevents `dhcpd` from searching for all available network interfaces.

If these solutions do not work for your DHCP server program, it might be an older version of the program and you can try upgrading to more current version. DHCP server programs are available from the Internet Systems Consortium (ISC) Web site.

# Assigning IP Addresses in Host-Only Networks and NAT Configurations

The host system and all virtual machines configured for host-only networking are connected to the network through a virtual switch. Typically, all the parties on this network use the TCP/IP protocol suite, although other communication protocols can be used.

A NAT configuration also sets up a private network, which must be a TCP/IP network. The virtual machines configured for NAT are connected to that network through a virtual switch. A host virtual network adapter connects the host system to the private network used for NAT. Each virtual machine and the host system must be assigned addresses on the private network.

When host-only networking is enabled at the time Workstation is installed, the subnet IP address for the virtual network is automatically selected as an unused private subnet IP address. A NAT configuration also uses an unused private network automatically selected when you install Workstation. The subnet number associated with a virtual network is shown in the virtual network editor.

IP addresses are typically assigned by using the virtual DHCP server included with Workstation. IP addresses can also be assigned statically from a pool of addresses that the virtual DHCP server does not assign. Using DHCP to assign IP addresses is simpler and more automatic than statically assigning them. Most Windows operating systems are preconfigured to use DHCP at boot time, so Windows virtual machines can connect to the network the first time they are booted, without additional configuration.

If you want virtual machines to communicate with each other by using names instead of IP addresses, you must set up a naming convention, a name server on the private network, or both. In this case, it might be simpler to use static IP addresses.

In general, if you have virtual machines that you intend to use frequently or for extended periods of time, it is more convenient to assign static IP addresses or configure the virtual DHCP server to always assign the same IP address to each of these virtual machines. For temporary virtual machines, let the virtual DHCP allocate IP addresses.

**NOTE** The virtual DHCP server does not service virtual or physical machines residing on bridged networks.

- Change DHCP Settings for a Host-Only or NAT Network on a Windows Host on page 169

  You can use the virtual network editor to change DHCP settings for a host-only or NAT network on a Windows host system.

- Change the Subnet Settings for a Host-Only or NAT Network on a Windows Host on page 170

  You can use the virtual network editor to change the subnet IP address and subnet mask for a host-only or NAT network on a Windows host system.

- Change the Subnet IP Address for a Host-Only or NAT Network on a Linux Host on page 171

  You can use the virtual network editor to change the subnet IP address for a host-only or NAT network on a Linux host system.

- DHCP Conventions for Assigning IP Addresses in Host-Only and NAT Networks on page 172

  For each host-only or NAT network, the virtual DHCP server allocates available IP addresses by using certain conventions. Workstation always uses a Class C address for host-only and NAT networks.

## Change DHCP Settings for a Host-Only or NAT Network on a Windows Host

You can use the virtual network editor to change DHCP settings for a host-only or NAT network on a Windows host system.

### Prerequisites

- Verify that you have administrative privileges on the host system.

- Familiarize yourself with the DHCP conventions for assigning IP addresses. See "DHCP Conventions for Assigning IP Addresses in Host-Only and NAT Networks," on page 172.

### Procedure

1. Log in to the host system as an Administrator user.

   Only an Administrator user can change network settings in the virtual network editor.

2. Select **Edit > Virtual Network Editor**.
3. Select the host-only or NAT network.
4. To use the virtual DHCP server to assign IP addresses to virtual machines on the network, select **Use local DHCP service to distribute IP addresses to VMs**.
5. To change additional DHCP settings, click **DHCP Settings**.

   You can change the range of IP addresses that the virtual DHCP server provides on the selected network and the duration of DHCP licenses that the DHCP server provides to clients on the virtual network.

6. Click **OK** to save your changes.

## Change the Subnet Settings for a Host-Only or NAT Network on a Windows Host

You can use the virtual network editor to change the subnet IP address and subnet mask for a host-only or NAT network on a Windows host system.

The default subnet mask is 255.255.255.0, which is a Class C address. Typically, you should modify only the third number in the IP address, for example, x in 192.168.x.0 or 198.16.x.0. In general, do not change the subnet mask. Certain virtual network services might not work as well with a customized subnet mask.

When you modify the subnet mask, Workstation updates the IP address settings for other components, including DHCP, NAT, and the host virtual network adapter, if the default settings were never changed. Settings that are automatically updated include the DHCP lease range and DHCP server address, the NAT gateway address, and the host network adapter IP address.

If you change any of these settings from their default values, Workstation does not update that setting automatically if the value is within the valid range. If the value exceeds the valid range, Workstation resets the settings based on the subnet range. Workstation presumes that a custom setting should not be modified, even if you later change the setting back to its default value.

### Prerequisites

- Verify that you have administrative privileges on the host system.
- Familiarize yourself with the DHCP conventions for assigning IP addresses. See "DHCP Conventions for Assigning IP Addresses in Host-Only and NAT Networks," on page 172.

### Procedure

1. Log in to the host system as an Administrator user.

   Only an Administrator user can change network settings in the virtual network editor on a Windows host system.

2. Select **Edit > Virtual Network Editor**.
3. Select the host-only or NAT network.
4. To change the subnet IP address, type a new value in the **Subnet IP** text box.

   The address should specify a valid network address that is suitable for use with the subnet mask.

5 To change the subnet mask, type a new value in the **Subnet mask** text box.

6 Click **OK** to save your changes.

## Change the Subnet IP Address for a Host-Only or NAT Network on a Linux Host

You can use the virtual network editor to change the subnet IP address for a host-only or NAT network on a Linux host system.

You can also use the virtual network editor to specify that a local DHCP service distributes IP addresses to virtual machines. To change DHCP settings further, you must edit the DHCP server configuration file (`dhcp.conf`). See "Editing the DHCP Server Configuration File," on page 171.

### Prerequisites

- Verify that you have root access on the host system.
- Familiarize yourself with the DHCP conventions for assigning IP addresses. See "DHCP Conventions for Assigning IP Addresses in Host-Only and NAT Networks," on page 172.

### Procedure

1 Log in to the Linux host system as root.

You must enter the root password to use the virtual network editor on a Linux host system.

2 Select **Applications > System Tools > Virtual Network Editor** to start the virtual network editor.

The menu path might be different for your version of Linux. You can also start the network editor from the command line by using the `vmware-netcfg` command.

3 Select the virtual network.

4 Change the subnet IP address.

| Option | Description |
|---|---|
| **Select an unused subnet IP address** | Leave the **Subnet IP** text box empty. |
| **Configure a specific subnet IP address** | Type the subnet IP address that you want to use in the **Subnet IP** text box. |

5 To have the virtual DHCP server distribute IP addresses to virtual machines on the network, select **Use local DHCP service to distribute IP addresses to VMs**.

6 Click **Save** to save your changes.

## Editing the DHCP Server Configuration File

If you are an advanced user, you can edit the DHCP server configuration file to modify DHCP settings.

The location of the DHCP server configuration file depends on the operating system type.

**Table 5-8.** DHCP Configuration File Location

| Host Operating System | DHCP Server Configuration File Location |
|---|---|
| Windows XP | `C:\Documents and Settings\All Users\Application Data\VMware\vmnetdhcp.conf` |
| Windows Vista or Windows 7 | `C:\ProgramData\VMware\vmnetdhcp.conf` |
| Linux | For the default host-only network: `/etc/vmware/vmnet1/dhcp/dhcp.conf`<br>For the NAT network: `/etc/vmware/vmnet8/dhcp/dhcp.conf` |

On a Windows host system, you can change DHCP settings by using the virtual network editor. You do not need to edit the DHCP server configuration file.

On a Linux host system, you can use the virtual network editor to specify that a local DHCP service distributes IP addresses to virtual machines on the network. To change DHCP settings further, you must edit the DHCP server configuration file. Editing the DHCP server configuration file requires information that is best obtained directly from the DHCP server documentation. See the *dhcpd(8)* and *dhcpd.conf(8)* manual pages.

**NOTE** Changes made to the read-only section of the DHCP configuration file are lost the next time you run the virtual network editor.

### DHCP Conventions for Assigning IP Addresses in Host-Only and NAT Networks

For each host-only or NAT network, the virtual DHCP server allocates available IP addresses by using certain conventions. Workstation always uses a Class C address for host-only and NAT networks.

The *net* value is the network number assigned to the host-only or NAT network.

**Table 5-9.** IP Address Use on a Host-Only Network

| Range | Address Use | Example |
|---|---|---|
| *net*.1 | Host machine | 192.168.0.1 |
| *net*.2–*net*.127 | Static addresses | 192.168.0.2–192.168.0.127 |
| *net*.128–*net*.253 | DHCP-assigned | 192.168.0.128–192.168.0.253 |
| *net*.254 | DHCP server | 192.168.0.254 |
| *net*.255 | Broadcasting | 192.168.0.255 |

**Table 5-10.** IP Address Use on a NAT Network

| Range | Address Use | Example |
|---|---|---|
| *net*.1 | Host machine | 192.168.0.1 |
| *net*.2 | NAT device | 192.168.0.2 |
| *net*.3–*net*.127 | Static addresses | 192.168.0.3–192.168.0.127 |
| *net*.128–*net*.253 | DHCP-assigned | 192.168.0.128–192.168.0.253 |
| *net*.254 | DHCP server | 192.168.0.254 |
| *net*.255 | Broadcasting | 192.168.0.255 |

## Configuring LAN Segments

A LAN segment is a private network that is shared by other virtual machines. A LAN segment can be useful for multitier testing, network performance analysis, and situations where virtual machine isolation are important.

### Create a LAN Segment for a Virtual Machine

You create a LAN segment by configuring virtual machine network settings. When you convert a team that was created in an earlier version of Workstation, the LAN segment configuration is retained for each virtual machine. You do not need to recreate the LAN segment.

#### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Network Adapter**.

3 Click **LAN Segments**.

4 Click **Add**, type a name for the LAN segment, and click **OK**.

5 Click **OK** to save your changes.

### What to do next

Configure the virtual machine to use the LAN segment. See "Configure a Virtual Machine to Use a LAN Segment," on page 173.

## Configure a Virtual Machine to Use a LAN Segment

You can configure an existing virtual machine to use a LAN segment, and you can change the LAN segment that a virtual machine is currently using.

In this release of Workstation, bandwidth and packet loss settings are associated with individual virtual machines rather than LAN segments. See "Configure Bandwidth and Packet Loss Settings for a Virtual Machine," on page 150.

### Prerequisites

- If the LAN segment does not already exist, create it. See "Create a LAN Segment for a Virtual Machine," on page 172.
- To configure a virtual machine to use multiple LAN segments, you must configure the virtual machine to have multiple network adapters. See "Add a Virtual Network Adapter to a Virtual Machine," on page 148.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Network Adapter**.

3 Select **LAN segment** and select the LAN segment from the drop-down menu.

4 Click **OK** to save your changes.

### What to do next

When you add an existing virtual machine to a LAN segment, the virtual machine might be configured to expect an IP address from a DHCP server. Unlike host-only and NAT networking, Workstation does not provide a DHCP server for LAN segments. You must manually configure IP addressing for virtual machines on a LAN segment. You can either configure a DHCP server on the LAN segment to allocate IP addresses, or you can configure a fixed IP address for each virtual machine on the LAN segment.

## Delete a LAN Segment

Deleting a LAN segment disconnects all virtual network adapters that are configured for that LAN segment. When you delete a LAN segment, you must manually configure its disconnected virtual network adapter to reconnect the virtual machine to a network.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select **Network Adapter**.

3 Click **LAN Segments**, select the LAN segment, click **Remove**, and click **OK**.

4 Either select another LAN segment or change the network connection type for the virtual machine.

5 Click **OK** to save your changes.

### What to do next

If you deleted a LAN segment that is being used by other virtual machines, select another LAN segment or change the network connection type for those virtual machines. See "Modify an Existing Virtual Network Adapter for a Virtual Machine," on page 148.

# Configuring Samba for Workstation

If you have Samba on a Linux host system, you can configure it so that it works with Workstation.

You must modify the Samba configuration so that it includes the IP subnet that the vmnet1 virtual network adapter uses. You can determine which subnet vmnet1 uses by using the command `/sbin/ifconfig vmnet1`.

You must also make sure the Samba password file includes entries for all users of the virtual machine who will access the host file system. The user names and passwords in the Samba password file must match those used for logging on to the guest operating system.

## Add Users to the Samba Password File

You can add user names and passwords to the Samba password file at any time from a terminal window on the Linux host system. The Samba password file must include entries for all users of the virtual machine who will access the host file system.

### Procedure

1 Log in to the root account.

2 Run the Samba password command with the user name to add to the password file.

For example: `smbpasswd –a` *user_name*

3 Follow the instructions on the screen.

4 Log out of the root account.

## Use a Samba Server for Bridged or Host-Only Networking

You can use a Samba server for bridged or host-only networking.

### Procedure

1 Open the Samba configuration file (`/etc/samba/smb.conf`) in a text editor.

2 Add the `interfaces` parameter and set it to VMnet interface.

You can define the `interface` parameter so that the Samba server serves multiple interfaces. This example tells the Samba server to monitor and use both the eth0 and vmnet1 interfaces, which are the networks that bridged and host-only networking use

For example: **`interface = eth0 vmnet1`**

3 Restart Samba.

## Use Samba Without Network Access

You can make Samba inaccessible from the physical network interface.

### Procedure

1 Open the Samba configuration file (`/etc/samba/smb.conf`) in a text editor.

2 Add the `interfaces` parameter and set it to **`vmnet*`**.

For example: `interfaces = vmnet*`

3 Restart Samba.

## Using Virtual Network Adapters in Promiscuous Mode on Linux Hosts

Workstation does not allow the virtual network adapter to go into promiscuous mode unless the user running Workstation has permission to make that setting. This restriction follows the standard Linux practice that only the root user can put a network interface into promiscuous mode.

When you install and configure Workstation, you must run the installation as the root user. Because Workstation creates the vmnet devices with root ownership and root group ownership, only the root user has read and write permissions to the devices.

To set a virtual machine network adapter to promiscuous mode, you must launch Workstation as the root user because you must have read and write access to the vmnet device. For example, if you use bridged networking, you must have access to `/dev/vmnet0`.

To grant selected users read and write access to the vmnet device, you can create a new group, add the appropriate users to the group, and grant that group read and write access to the appropriate device. You must make these changes on the host operating system as the root user.

In this example, *newgroup* is the group that should be able to set vmnet0 to promiscuous mode.

```
chgrp newgroup /dev/vmnet0
chmod g+rw /dev/vmnet0
```

In the next example, all users are able to set vmnet0 to promiscuous mode.

```
chmod a+rw /dev/vmnet0
```

## Maintaining and Changing MAC Addresses for Virtual Machines

When a virtual machine is powered on, Workstation assigns each of its virtual network adapters an Ethernet media access control (MAC) address. A MAC address is the unique address assigned to each Ethernet network device.

A virtual machine is assigned the same MAC address every time it is powered unless the virtual machine configuration (`.vmx`) file is moved or changes are made to certain settings in the configuration file.

Moving the file to a different host system, or even moving it to a different location on the same host system, changes the MAC address.

The MAC address changes if you remove or change any of these options in the virtual machine configuration (`.vmx`) file.

- `ethernet[n].generatedAddress`
- `ethernet[n].addressType`
- `ethernet[n].generatedAddressOffset`
- `uuid.location uuid.bios`
- `ethernet[n].present`

In these options, `[n]` is the number of the virtual network adapter. If you never edit the configuration file by hand and do not remove the virtual network adapter, these settings remain unchanged.

Workstation cannot guarantee to automatically assign unique MAC addresses for virtual machines that run on multiple host systems.

**NOTE** To preserve the MAC address for a virtual network adapter, you must be careful not to remove the adapter. If you remove the adapter but later recreate it, the adapter might receive a different MAC address.

## Change the MAC Address for a Virtual Machine

You can use advanced virtual network adapter settings to assign a new MAC address to a virtual machine.

**NOTE** You cannot configure advanced virtual network adapter settings for a shared or remote virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Settings**.

2 On the **Hardware** tab, select the virtual network adapter and click **Advanced**.

3 Type a new MAC address in the **MAC Address** text box, or click **Generate** to have Workstation generate a new address.

4 Click **OK** to save your changes.

## Manually Assign a MAC Address to a Virtual Machine

You can manually assign a MAC address to a virtual machine.

You might want to assign a MAC address to guarantee that the same address is assigned to a virtual machine every time it powers on, even it is moved, or to be sure that a unique MAC address is provided for each virtual machine in a networked environment.

### Procedure

1 Use a text editor to remove the following options from the virtual machine configuration (`.vmx`) file.

```
ethernet[n].generatedAddress
ethernet[n].addressType
ethernet[n].generatedAddressOffset
```

In these options, *[n]* is the number of the virtual network adapter.

2 Add the **`ethernet[n].address`** option to the `.vmx` file above the UUID lines in the file and set it to the MAC address.

For example: **`ethernet[n].address = 00:50:56:`*`XX:YY:ZZ`***

In this line, the fourth pair of numbers, *XX*, must be a valid hexadecimal number between 00h and 3Fh, and *YY* and *ZZ* must be valid hexadecimal numbers between 00h and FFh. You must use this format. Workstation virtual machines do not support arbitrary MAC addresses.

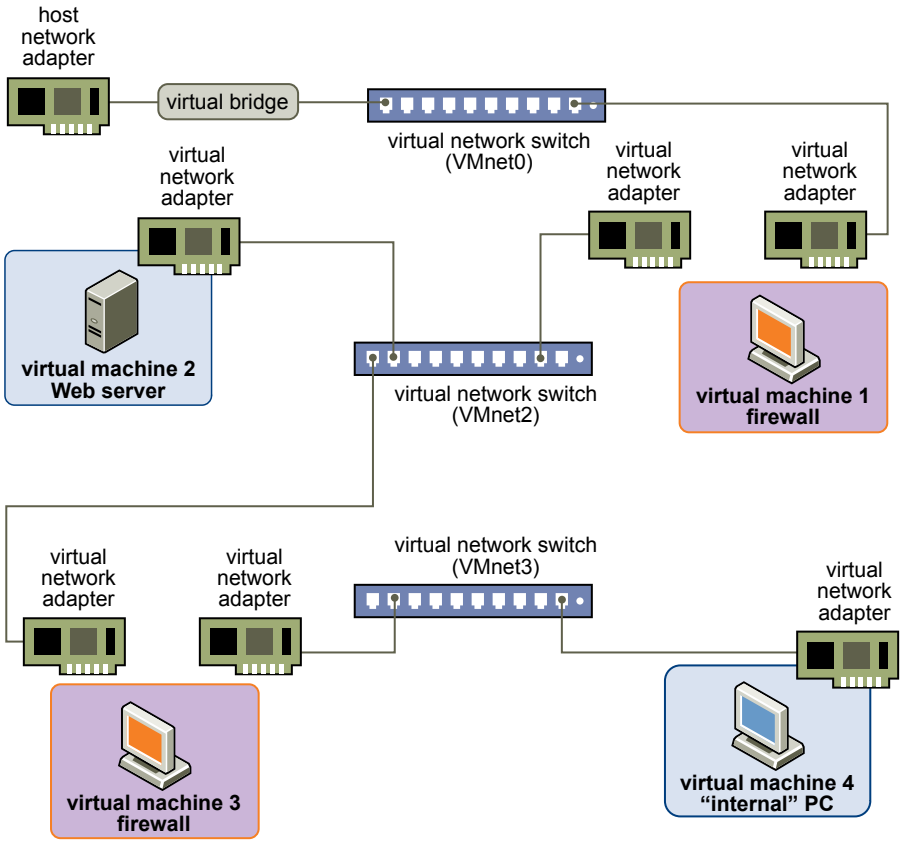
A value for *XX:YY:ZZ* that is unique among your hard-coded addresses avoids conflicts between the automatically assigned MAC addresses and the manually assigned addresses.

# Sample Custom Networking Configuration

There are many ways to combine devices on a virtual network. This example shows server connections through multiple firewalls.

You can combine devices on a virtual network in many ways. In this example, a Web server connects through a firewall to an external network and an administrator's computer connects to the Web server through a second firewall.

**Figure 5-4.** Custom Configuration with Two Firewalls




## Create the Sample Custom Networking Configuration

You can create the sample custom networking configuration.

### Prerequisites

- Familiarize yourself with how to create virtual machines and configure network devices in the host and guest operating systems.
- Familiarize yourself with the diagram of the sample networking configuration. See Figure 5-4.

### Procedure

1 Use the New Virtual Machine wizard to create four virtual machines.

   a Create the first virtual machine with bridged networking so that it can connect to an external network by using the host network adapter.

   b Create the other three virtual machines without networking.

2 Configure network settings for the first virtual machine.

   a Open the first virtual machine, but do not power it on.

   b Edit the virtual machine settings to add a second virtual network adapter.

   c Connect the second network adapter to VMnet2.

3 Configure network settings for the second virtual machine.

   a Open the virtual machine, but do not power it on.

   b Edit the virtual machine settings to add a virtual network adapter.

   c Connect the network adapter to VMnet2.

4 Configure network settings for the third virtual machine.

   a Open the virtual machine, but do not power it on.

   b Edit the virtual machine settings to add a virtual network adapter.

   c Connect the network adapter to VMnet2.

   d Edit the virtual machine settings to add a second virtual network adapter.

   e Connect the second network adapter to VMnet3.

5 Configure network settings for the fourth virtual machine.

   a Open the virtual machine, but do not power it on.

   b Edit the virtual machine settings to add a virtual network adapter.

   c Connect the network adapter to VMnet3.

6 Determine the network addresses that are used for VMnet2 and VMnet3.

| Option | Description |
|---|---|
| **Windows host** | Use the `ipconfig /all` command. |
| **Linux host** | Use the `ifconfig` command. |

7 Power on each virtual machine and install the appropriate guest operating system.

8 Use the virtual network editor to configure VMnet2 to use the virtual DHCP service to distribute IP address to virtual machines.

9 Configure the networking in each guest operating system.

| Option | Description |
|---|---|
| **Virtual machine 1** | For the bridged network adapter in virtual machine 1, use the networking settings needed for a connection to the external network. If the virtual machine receives its IP address from a DHCP server on the external network, the default settings should work. For the second network adapter in virtual machine 1, manually assign an IP address in the range you are using with VMnet2. |
| **Virtual machine 2** | Assign an IP address in the range you are using with VMnet2. |
| **Virtual machine 3** | Network adapters are connected to VMnet2 and VMnet3. Assign an IP address in the virtual network's range it is connected to. |
| **Virtual machine 4** | Assign an IP address in the range you are using with VMnet3. |

10 Install the necessary application software in each virtual machine.

# Using Remote Connections and Sharing Virtual Machines

# 6

A shared virtual machine is a virtual machine on the host system that remote Workstation users can access as a remote virtual machine. Up to 100 remote users can connect to a single shared virtual machine at the same time.

You can configure Workstation so that users on remote Workstation hosts can interact with your local host and use the shared virtual machines that are running on it. You can also connect to remote hosts and run remote virtual machines. You control who can access host systems and shared virtual machines by setting permissions.

This chapter includes the following topics:


- "Understanding VMware Workstation Server," on page 179
- "Connect to a Remote Server," on page 182
- "Disconnect from a Remote Server," on page 184
- "Creating and Managing Shared Virtual Machines," on page 184
- "Upload a Virtual Machine to a Remote Server," on page 188
- "Download a Virtual Machine from a Remote Server," on page 188
- "Create a Virtual Machine on a Remote Host," on page 189
- "Configure Shared and Remote Virtual Machines to Start with the Host," on page 190
- "Using Roles to Assign Privileges," on page 191
- "Using Permissions to Restrict Users," on page 195


## Understanding VMware Workstation Server

VMware Workstation Server is a service that runs on the Workstation host system. Remote Workstation users connect to VMware Workstation Server when they run shared virtual machines on the host system.

On a Windows host, VMware Workstation Server is the VMware Workstation Server service. On a Linux host, it is `vmware-workstation-server`.

When you install Workstation, virtual machine sharing and remote access are enabled by default and VMware Workstation Server starts when the host system starts. When Workstation starts, it connects to VMware Workstation Server by using the credentials of the currently logged in user.

Remote Workstation users connect to VMware Workstation Server through HTTPS port 443 on the host system. You can change the VMware Workstation Server port when you install Workstation and after Workstation is installed by modifying the Shared VMs Workstation preference.

Shared virtual machines appear under the **Shared VMs** item in the virtual machine library. If virtual machine sharing is disabled, or if the current user does not have permissions to connect to VMware Workstation Server, the **Shared VMs** item is inactive.

If you click the **Shared VMs** item when virtual machine sharing is disabled, Workstation returns a message that explains how to enable virtual machine sharing. If the **Shared VMs** item is inactive because the current user does not have the proper permissions, a login dialog box appears and you can log in as a user who can connect to VMware Workstation Server.

## Configure Virtual Machine Sharing and Remote Access

You can enable or disable virtual machine sharing and remote access, change the HTTPS port that VMware Workstation Server uses on the host system, and change the shared virtual machines directory.

When you enable virtual machine sharing and remote access, Workstation starts VMware Workstation Server and configures the service to start with the host system.

When you disable virtual machine sharing and remote access, Workstation disables virtual machine sharing and stops VMware Workstation Server. You cannot create shared virtual machines and remote users cannot connect to the host system.

You must disable virtual machine sharing and remote access before you can change the HTTPS port that VMware Workstation Server uses.

### Prerequisites

- On a Linux host, verify that you have root access.
- On a Windows host, verify that you have administrative privileges.
- If you plan to change the shared virtual machines directory, stop sharing virtual machines on the host system. You cannot change the shared virtual machines directory if there are shared virtual machines on the host system. See "Stop Sharing a Virtual Machine," on page 187.

### Procedure

1. Select **Edit > Preferences > Shared VMs**.
2. To enable or disable virtual machine sharing and remote access, click **Enable Sharing** or **Disable Sharing** (Windows host), or select or deselect **Enable virtual machine sharing and remote access** (Linux host).
3. To change the HTTPS port that VMware Workstation Server uses on the host system, select a different port from the drop-down menu.

   **NOTE** If you change the port to a non-default value, remote users must specify the port number when they connect to the host system, for example, *host*:*port*.

4. To change the shared virtual machines directory, type or browse to the location of the new shared virtual machines directory (Windows host), or type the new directory in the text box and click **Apply** (Linux host).
5. Click **OK** to save your changes.

## Replace the Default Certificate for VMware Workstation Server

VMware Workstation Server generates a self-signed certificate. This certificate is sufficient for encryption, but it does not provide identity verification. For increased security, you should replace the default certificate with a certificate that is signed by a commercial Certificate Authority (CA).

### Prerequisites

Obtain a signed certificate. Obtaining a signed certificate involves creating a certificate signing request (CSR) and sending it to a CA in accordance with the CA's enrollment process. After conducting some checks on your company, the CA signs your request, encrypts it with a private key, and sends you a validated certificate. See the instructions provided by the CA for more information.

### Procedure

1 On the host system, replace the default certificate text in the VMware SSL certificate file with the certificate text that you obtained from the CA.

The location of the certificate file depends on the host operating system.

| Option | Certificate File |
|---|---|
| **Windows XP and Windows Server 2003 hosts** | `C:\Documents and Settings\All Users\Application Data\VMware\SSL\rui.crt` |
| **Windows Vista and Windows 7 hosts** | `C:\ProgramData\VMware\SSL\rui.crt`<br>NOTE You can access the SSL directory only from an elevated command prompt. |
| **Linux hosts** | `/etc/vmware/ssl/rui.crt` |

2 On the host system, replace the default private key text in the VMware SSL key file with the private key text that you obtained from the CA.

The location of the key file depends on the host operating system.

| Option | Certificate File |
|---|---|
| **Windows XP and Windows Server 2003 hosts** | `C:\Documents and Settings\All Users\Application Data\VMware\SSL\rui.key` |
| **Windows Vista and Windows 7 hosts** | `C:\ProgramData\VMware\SSL\rui.key`<br>NOTE You can access the SSL directory only from an elevated command prompt. |
| **Linux hosts** | `/etc/vmware/ssl/rui.key` |

3 Restart the host system.

The VMware Workstation Server service restarts and begins using the new certificate.

## Shared Virtual Machines Directory

Workstation stores shared virtual machines in the shared virtual machines directory, where VMware Workstation Server manages them.

The default location of the shared virtual machines directory depends on the host operating system.

**Table 6-1.** Default Shared Virtual Machines Directory

| Host Operating System | Default Shared Virtual Machines Directory |
|---|---|
| Windows XP<br>Windows Server 2003<br>Windows Server 2008 | `C:\Documents and Settings\All Users\Documents\Shared Virtual Machines` |
| Windows Vista<br>Windows 7<br>Windows 8 | `C:\Users\Public\Documents\Shared Virtual Machines` |
| Linux | `/var/lib/vmware/Shared VMs` |

### VMware Workstation Server Log Files

VMware Workstation Server saves messages in log files. Refer to these log files if you need to audit or troubleshoot a problem with remote access or remote authorization.

**Table 6-2.** Workstation Server Log Files

| Host System | Location |
|---|---|
| Most Windows hosts | `C:\Documents and Settings\All Users\Application Data\VMware\hostd\hostd-`*`n`*`.log` |
| Windows Vista and Windows 7 hosts | `C:\ProgramData\VMware\hostd\hostd-`*`n`*`.log` |
| Linux hosts | `/var/log/vmware/hostd-`*`n`*`.log` |

On Linux hosts, security-related information, such as authorization attempts, is sent to the system messages log.

## Connect to a Remote Server

You can use Workstation to connect to a remote server that is running Workstation, ESX, ESXi, or vCenter Server.

When you connect to a remote server for the first time, Workstation asks you whether to save your login information. You can configure Workstation to never ask you to save login information for a remote server. See "Disable the Prompt to Save Remote Login Information," on page 183.

#### Prerequisites

Verify that the remote server is running Workstation 8.x or later, or ESX, ESXi, or vCenter Server 4.1 or later.

#### Procedure

1 Select **File > Connect to Server**.

2 Type the host name or IP address, your user name and password, and click **Connect**.

If the VMware Workstation Server service running on the remote server is not using the default port, you must specify the port number, for example, **`remotehost:444`**.

3 (Optional) If Workstation asks you whether to save your login information, select an option.

| Option | Description |
|---|---|
| **Remember** | Workstation saves your login information so that you do not need to provide it the next time you log in to the server. |
| **Never for this Host** | Workstation saves the server name to an exceptions list and does not prompt you to save your login information for this server again. |
| **Not Now** | Workstation does not save your login information, but it prompts you to save your login information the next time you connect to this server. |

After you are connected to the remote server, the remote host and remote virtual machines appear in the library.

#### What to do next

Interact with the remote host and remote virtual machines.

## Interacting with Remote Hosts and Virtual Machines

After you connect to a remote server, the remote host and remote virtual machines appear in the library. If the remote server is running vCenter Server, datacenters and folders appear in the library.

To interact with a remote host, you select it in the library. The tasks that you can perform on a remote host appear on the tab for the remote host. For example, you might be able to restart, shut down, or suspend the remote host and create virtual machines.

To interact with a remote virtual machine, you select it in the library. You interact with remote virtual machines in the same way that you interact with local virtual machines, but some features and devices are not supported. Features that you cannot use with remote virtual machines include Unity mode, shared folders, AutoProtect snapshots, drag-and-drop, and copy and paste.

Your permissions determine the actions that you can perform on remote hosts and remote virtual machines. When a feature is not supported, or when you do not have permission to use it, the associated menu item is unavailable.

## Disable the Prompt to Save Remote Login Information

You can disable the prompt to save remote login information for a specific remote server or for all remote servers.

#### Procedure

- Disable the prompt to save login information for a specific remote server.
  a Log in to the remote server for the first time.
  b Select **Never for this Host**.
  Workstation saves the name of the remote server to an exceptions list. You must type login information the next time you connect to the remote server.
- Disable the prompt to save login information for all remote servers.
  a Select **Edit > Preference > Workspace**.
  b Deselect **Offer to save login information for remote servers**.
  c Click **OK** to save your changes.
  You must type login information every time you connect to a remote server.

### Remove Saved Login and Exception Information for Remote Servers

You can remove the login information that Workstation saves for a remote server. You might need to remove saved login information if the user name or password changes for a remote sever. You can also remove a remote server from the exceptions list.

Workstation adds a remote server to the exceptions list when you select **Never for this Host** the first time you log in to the remote server. If you subsequently want Workstation to prompt you to save login information for that remote server, you must remove the remote server from the exceptions list.

#### Procedure

1 Select **Edit > Preferences**, select **Workspace**, and click **Show Saved Login Information**.

The **Saved Passwords** tab shows the saved user names. The remote servers for which Workstation does not prompt you to save login information appear on the **Exceptions** tab.

| Option | Description |
|---|---|
| **Remove saved login information for a specific remote server** | On the **Saved Passwords** tab, select the remote server and click **Remove**. You must type login information the next time you connect to that remote server. |
| **Remove all saved login information** | On the **Saved Passwords** tab, click **Remove All**. You must type login information the next time you connect to any remote server. |
| **Remove a remote server from the exceptions list** | On the **Exceptions** tab, select the remote server and click **Remove**. Workstation prompts you to save login information the next time you connect to the remote server. |
| **Remove all remote servers from the exceptions list** | On the **Exceptions** tab, click **Remove All** (Windows host) or **Clear** (Linux host). Workstation prompts you to save login information the next time you connect to any remote server. |

2 Click **Close** to close the dialog box and click **OK** to save your changes.

## Disconnect from a Remote Server

When you disconnect from a remote server, the remote virtual machines no longer appear in the library.

#### Procedure

- On a Windows host, right-click the remote host in the library and select **Disconnect**.
- On a Linux host, select the remote host in the library and click **Disconnect From This Server** on the tab for the remote host.

## Creating and Managing Shared Virtual Machines

A shared virtual machine is a virtual machine on the host system that remote Workstation users can access as a remote virtual machine. You can create a new shared virtual machine, convert a standard virtual machine to a shared virtual machine, or create a shared virtual machine clone of a standard virtual machine.

You can configure specific shared virtual machines to start when the host system starts, and you can view status and task information for shared virtual machines.

Workstation stores shared virtual machines in the shared virtual machines directory, where VMware Workstation Server manages them. Shared virtual machines appear in the virtual machine library under the **Shared VMs** item.

- Convert or Clone a Standard Virtual Machine to a Shared Virtual Machine on page 185

  You can convert a standard virtual machine to a shared virtual machine or create a shared virtual machine by creating a clone of a standard virtual machine. Workstation stores shared virtual machines in the shared virtual machines directory.

- Create a New Shared Virtual Machine on page 186

  You can create a new shared virtual machine in Workstation by using the New Virtual Machine wizard. Creating a shared virtual machine is similar to creating a standard virtual machine.

- Stop Sharing a Virtual Machine on page 187

  When you stop sharing a virtual machine, Workstation changes the shared virtual machine to a standard virtual machine.

- View the Status of Shared and Remote Virtual Machines on page 187

  You can view power status and task information for shared virtual machines, and you can view the power status of remote virtual machines. Tasks are operations that can affect the use of a virtual machine, such as power state changes and changes to virtual machine settings.

## Convert or Clone a Standard Virtual Machine to a Shared Virtual Machine

You can convert a standard virtual machine to a shared virtual machine or create a shared virtual machine by creating a clone of a standard virtual machine. Workstation stores shared virtual machines in the shared virtual machines directory.

### Prerequisites

- Verify that the virtual machine is not encrypted.
- Verify that the virtual machine is not configured to use a physical disk.
- Power off the virtual machine.

### Procedure

1 Select the virtual machine and select **VM > Manage > Share**, or drag the virtual machine to the **Shared VMs** item.

2 Type a name for the shared virtual machine.

3 Select how to create the shared virtual machine.

| Option | Description |
|---|---|
| **Move the virtual machine** | Convert the standard virtual machine to a shared virtual machine. Workstation moves the virtual machine files to the shared virtual machines directory. If you decide to prevent remote access to virtual machine at a later time, you can change the virtual machine back to a standard virtual machine. |
| **Make a full clone of the virtual machine** | Create a shared virtual machine by cloning the virtual machine. Workstation creates the clone in the shared virtual machines directory. The clone is a complete and independent copy of the virtual machine and additional disk space is required to store it. |

4 Click **Finish** to share the virtual machine and click **Close** to exit the wizard.

A clone can take several minutes to create, depending on the size of the virtual disk that is being duplicated.

If you converted a standard virtual machine to a shared virtual machine, the virtual machine appears under the **Shared VMs** item in the library. If you cloned a standard virtual machine, the clone appears under the **Shared VMs** item and the original virtual machine remains under **My Computer**.

### What to do next

If the virtual machine uses a static IP address, change it after cloning a standard virtual machine to a shared virtual machine.

## Create a New Shared Virtual Machine

You can create a new shared virtual machine in Workstation by using the New Virtual Machine wizard. Creating a shared virtual machine is similar to creating a standard virtual machine.

### Prerequisites

- Verify that you have the information the New Virtual Machine wizard requires to create a virtual machine. See "Preparing to Create a New Virtual Machine," on page 8.
- Verify that the guest operating system you plan to install is supported. See the VMware Compatibility Guide on the VMware Web site for a list of the supported guest operating systems.
- See the *VMware Guest Operating System Installation Guide* for information about the guest operating system that you plan to install.
- If you are installing the guest operating system from an installer disc, insert the installer disc in the CD-ROM drive in the host system.
- If you are installing the guest operating system from an ISO image file, verify that the ISO image file is in a directory that is accessible to the host system.

### Procedure

1 In the library, select **Shared VMs**.

2 On the **Shared VMs** tab, click **Create a New Virtual Machine**.

3 On the Welcome screen, select the configuration type.

| Option | Description |
|---|---|
| **Typical** | The wizard prompts you to specify or accept defaults for basic virtual machine settings. The typical configuration type is appropriate in most instances.<br>After specifying an operating system version and virtual machine name and location, the wizard prompts you to configure only the virtual disk size and whether the disk should be split into multiple files. If you choose a custom setup, the wizard includes additional prompts for such things as processors, memory, and networking. |
| **Custom** | You must select the custom configuration type to make a different virtual machine version than the default hardware compatibility setting, specify the I/O adapter type for SCSI adapters, specify whether to create an IDE, SCSI, or SATA virtual disk, use an existing virtual disk, or allocate all virtual disk space rather than let disk space gradually grow to the maximum disk size. |

4 If you selected a custom configuration, select the hardware compatibility setting for the virtual machine.

The hardware compatibility setting determines the hardware features of the virtual machine.

5 Follow the prompts to select a guest operating system and name and configure the virtual machine.

Use the following guidelines:

- The Easy Install feature is not available for installing operating systems in shared or remote virtual machines.
- If you choose to install the operating system later, the virtual machine is created with a blank disk.

6 (Optional) Click **Customize Hardware** to customize the hardware configuration.

You can also modify virtual hardware settings after you create the virtual machine.

7 (Optional) Select **Power on this virtual machine after creation** to power on the virtual machine after you create it.

This option is not available if you are installing the guest operating system manually.

8 Click **Finish** to create the virtual machine.

If you are using Easy Install, guest operating system installation begins when the virtual machine powers on. The guest operating system installation is automated and typically runs without requiring any input from you. After the guest operating system is installed, Easy Install installs VMware Tools.

Newly created shared virtual machines appear in the library under the **Shared VMs** item.

#### What to do next

If you used Easy Install and the virtual machine did not power on when you finished the New Virtual Machine wizard, power on the virtual machine to start the guest operating system installation. See "Use Easy Install to Install a Guest Operating System," on page 20.

If you did not use Easy Install, install the guest operating system manually. See "Install a Guest Operating System Manually," on page 21.

## Stop Sharing a Virtual Machine

When you stop sharing a virtual machine, Workstation changes the shared virtual machine to a standard virtual machine.

#### Prerequisites

Power off the virtual machine.

#### Procedure

1 Select the shared virtual machine and select **VM > Manage > Stop Sharing**, or drag the virtual machine from under the **Shared VMs** item and drop it on **My Computer**.

2 Type or browse to the new location for the virtual machine.

3 Click **Finish** to stop sharing the virtual machine and click **Close** to exit the wizard.

The virtual machine no longer appears on the **Shared VMs** tab.

## View the Status of Shared and Remote Virtual Machines

You can view power status and task information for shared virtual machines, and you can view the power status of remote virtual machines. Tasks are operations that can affect the use of a virtual machine, such as power state changes and changes to virtual machine settings.

#### Prerequisites

To view the power status of remote virtual machines, connect to the remote server. See "Connect to a Remote Server," on page 182.

#### Procedure

- To view power status and task information for shared virtual machines, select **Shared VMs** and select the list view on the **Shared VMs** tab.

  Power status and task information appears on the **Shared VMs** tab for each shared virtual machine.

- To view the power status of remote virtual machines, select the remote host and select the list view on the tab for the remote host.

  The power status of each virtual machine on the remote host appears on the tab.

# Upload a Virtual Machine to a Remote Server

When you upload a virtual machine to a remote server, Workstation copies the virtual machine to the remote host and datastore that you select. The original virtual machine remains on the host system.

### Prerequisites

- Verify that the remote server is running ESX, ESXi, or vCenter Server 4.1 or later.
- Verify that the virtual machine is not encrypted. You cannot upload an encrypted virtual machine.
- Verify that the remote host supports the hardware version of the virtual machine. If the remote host does not support the hardware version, the upload wizard returns an error message.
- Open the virtual machine in Workstation.
- If the virtual machine is powered on or suspended, power it off.

### Procedure

1 Select the virtual machine and select **VM > Manage > Upload**.

**NOTE** You can also start the upload process by dragging and dropping the virtual machine to the remote host in the library.

2 Select the destination remote server.

| Option | Action |
|---|---|
| **The remote server appears in the list** | Select the remote server in the list. |
| **The remote server does not appear in the list** | Select **New Server Connection** and log in to the remote server. |

Workstation verifies the connection to the remote server.

3 If the remote server is running vCenter Server, select a destination location.

4 (Optional) Type a new name for the virtual machine on the remote host.

5 Select a remote host and datastore to store the uploaded virtual machine.

If the remote server is running vCenter Server, multiple hosts and datastores might be available.

6 Click **Finish** to upload the virtual machine to the remote server.

A status bar indicates the progress of the upload process. How long it takes to upload a virtual machine depends on the size of the virtual disk and the network connection speed.

After the virtual machine is uploaded to the remote server, it appears in the inventory for the remote host in the library.

# Download a Virtual Machine from a Remote Server

When you download a virtual machine from a remote server, Workstation copies the virtual machine from the remote host and datastore. The original virtual machine remains on the host system, and a copy is created on the Workstation host in the location you specify.

This feature is available for virtual machines on remote servers. It is not available for shared virtual machines or standard virtual machines on Workstation hosts.

### Prerequisites

- Connect to the remote server that hosts the virtual machine you want to download. See "Connect to a Remote Server," on page 182.
- Verify that the remote server is running ESX, ESXi, or vCenter Server 4.1 or later.
- If the virtual machine is powered on or suspended, power it off.

### Procedure

1 Select the virtual machine on the remote server and select **VM > Manage > Download**.

**NOTE** You can also start the download process by dragging the virtual machine from the remote host into the **My Computer** portion of the Workstation library or into any sub-folder of **My Computer** in the library.

2 In the Download Virtual Machine dialog box that appears, type a name for the virtual machine, type or browse to the directory for the virtual machine files, and click **Download**.

## Create a Virtual Machine on a Remote Host

When you are connected to a remote server, you can create a remote virtual machine. Creating a remote virtual machine is similar to creating a virtual machine on the local host, but Easy install is not supported and you must install the guest operating system manually.

When you select a typical configuration, the New Virtual Machine wizard uses the default hardware version configured in the Workstation preferences, unless the remote host does not support that version. If the remote host does not support the default hardware version, the wizard uses the latest hardware version that is supported on the remote host.

### Prerequisites

- Connect to the remote server. See "Connect to a Remote Server," on page 182.
- Verify that you have permission to create a virtual machine on the remote host.
- Verify that you have the information the New Virtual Machine wizard requires to create a virtual machine. See "Preparing to Create a New Virtual Machine," on page 8.

### Procedure

1 Start the New Virtual Machine wizard.

| Option | Description |
|---|---|
| **Windows host** | Select **File > New Virtual Machine** and select the remote host from the menu, or click **New Virtual Machine** on the tab for the remote host. |
| **Linux host** | Click **Create a New Virtual Machine** on the tab for the remote host. |

2 On the Welcome screen, select the configuration type.

| Option | Description |
|---|---|
| **Typical** | The wizard prompts you to specify or accept defaults for basic virtual machine settings. The typical configuration type is appropriate in most instances.<br>After specifying an operating system version and virtual machine name and location, the wizard prompts you to configure only the virtual disk size and whether the disk should be split into multiple files. If you choose a custom setup, the wizard includes additional prompts for such things as processors, memory, and networking. |
| **Custom** | You must select the custom configuration type to make a different virtual machine version than the default hardware compatibility setting, specify the I/O adapter type for SCSI adapters, specify whether to create an IDE, SCSI, or SATA virtual disk, use an existing virtual disk, or allocate all virtual disk space rather than let disk space gradually grow to the maximum disk size. |

3 If the remote server running is ESX or ESXi and it has multiple datastores, select a datastore to store the virtual machine.

4 If the remote server is running vCenter Server, select an inventory location, a remote host, and a datastore to store the virtual machine.

The inventory location can be a datacenter or a folder within a datacenter. You must select a datastore only if the remote host has multiple datastores.

5 If you selected a custom configuration, select the hardware compatibility setting for the virtual machine.

The hardware compatibility setting determines the hardware features of the virtual machine.

6 Select the guest operating system type and version, or select **Other** if the guest operating system is not listed.

7 Type a name for the virtual machine.

8 Follow the prompts to select a guest operating system and name and configure the virtual machine.

Use the following guidelines:

- The Easy Install feature is not available for installing operating systems in shared or remote virtual machines.
- If you choose to install the operating system later, the virtual machine is created with a blank disk.

9 Click **Finish** to create the virtual machine.

The virtual machine appears in the library under the remote host.

### What to do next

Install the guest operating system manually. See "Install a Guest Operating System Manually," on page 21.

## Configure Shared and Remote Virtual Machines to Start with the Host

You can use the AutoStart feature to configure shared virtual machines to start when the local host system starts. You can also configure remote virtual machines to start when the remote host system starts.

You cannot configure AutoStart if the remote server is running vCenter Server. You cannot use the AutoStart feature to configure virtual machines to start in a preferred sequence. You can use the VMware vSphere Client to configure more advanced features, including startup order. See the vSphere virtual machine administration documentation.

### Prerequisites

- If you are configuring AutoStart for remote virtual machines, connect to the remote server. See "Connect to a Remote Server," on page 182.
- Verify that you have the Administrator role or a custom role that contains the **Host.Configuration.Virtual machine autostart configuration** privilege.

### Procedure

1 Select the location of the virtual machines.

| Option | Description |
|---|---|
| **The virtual machines are on the local host** | a In the library, select **Shared VMs**.<br>b On the **Shared VMs** tab, click **Manage Autostart VMs**. |
| **The virtual machines are on a remote host** | a In the library, select the remote host.<br>b On the tab for the remote host, **Manage Autostart VMs**. |

2 Select the virtual machines to start with the host system.

3 If you selected multiple virtual machines, select the number of seconds to delay between starting the virtual machines.

4 Click **Save** to save your changes.

# Using Roles to Assign Privileges

A role is a predefined set of privileges. Privileges define individual rights that a user requires to perform actions and read properties. Workstation includes a default set of system roles. You can also create your own roles.

A single user might have different roles for different objects. For example, if you have two shared virtual machines, virtual machine A and virtual machine B, you might assign a particular user the Administrator role on virtual machine A and the Read Only permission on virtual machine B.

- Default System Roles on page 191

  Workstation provides a set of default system roles. You can use the default system roles to assign permissions, or you can use them as a model to create your own roles.

- Create a Role on page 192

  If the default system roles do not meet your needs, you can combine selected privileges to create your own roles.

- Edit a Role on page 193

  You can change the name of a role. You can add or remove the privileges in a role. You cannot edit the default system roles.

- Clone a Role on page 193

  You can make a copy of an existing role by cloning it. When you clone a role, the new role is not applied to users, groups, or objects. You must assign the role to users or groups and objects.

- Remove a Role on page 194

  When you remove a role, Workstation removes the definition from the list of roles.

## Default System Roles

Workstation provides a set of default system roles. You can use the default system roles to assign permissions, or you can use them as a model to create your own roles.

The default system roles are permanent. You cannot edit the privileges associated with these roles.

**Table 6-3.** Default System Roles

| Role | User Capabilities |
|---|---|
| Administrator | ■ Has all privileges for all objects.<br>■ Can add, remove, and set access rights and privileges on all objects.<br>Default role for members of the Administrators group on Windows hosts and the root user on Linux hosts. |
| No Access | ■ Cannot view or change the associated object.<br>■ Tabs associated with the object appear without content.<br>Except for users in the Administrators group on Windows hosts and the root user on Linux hosts, this is the default role for all users. |
| Read Only | ■ Can view the object state and details about the object.<br>■ Cannot perform any actions through the menus and toolbars. |
| VM Creator | Can create, use, configure, and delete virtual machines. |
| VM User | Can configure and use existing virtual machines. |

## Create a Role

If the default system roles do not meet your needs, you can combine selected privileges to create your own roles.

Privileges define individual rights that a user requires to perform actions and read properties. The privileges that you can select when you create a role depend on whether the server is running Workstation, ESX, ESXi, or vCenter Server.

See *Defined Privileges* in the Workstation documentation center for descriptions of the available privileges. The Workstation documentation center is available on the VMware Web site at https://www.vmware.com/support/pubs/ws_pubs.html.

### Prerequisites

If you are creating a role on a remote host, connect to the remote server. See "Connect to a Remote Server," on page 182.

### Procedure

1 Open the Edit Roles dialog box.

| Option | Description |
|---|---|
| **Create a role on the local host** | ■ (Windows host) Right-click **Shared VMs** and select **Roles**.<br>■ (Linux host) Right-click **Shared VMs** and select **Edit Roles**. |
| **Create a role on a remote host** | ■ (Windows host) Right-click the remote host and select **Roles**.<br>■ (Linux host) Right-click the remote host and select **Edit Roles**. |

2 Click **Add**.

3 Type a name for the new role.

| Option | Description |
|---|---|
| **Windows host** | Replace the name of the role in the Roles list. |
| **Linux host** | Type a new name in the **Name** text box. |

4 From the privileges tree, select the privileges to include in the new role.

You can expand the tree to view the privileges in each category.

5 Click **OK** (Windows host) or **Save** (Linux host) to create the new role.

## Edit a Role

You can change the name of a role. You can add or remove the privileges in a role. You cannot edit the default system roles.

When you change the privileges in a role, the changes are applied to any user or group that is assigned that role. When you change the name of a role, no changes occur to the role's assignments.

See *Defined Privileges* in the Workstation documentation center for descriptions of the available privileges. The Workstation documentation center is available on the VMware Web site at https://www.vmware.com/support/pubs/ws_pubs.html.

### Prerequisites

If you are editing a role on a remote host, connect to the remote server. See "Connect to a Remote Server," on page 182.

### Procedure

1 Open the Edit Roles dialog box.

| Option | Description |
|---|---|
| **Edit a role on the local host** | ■ (Windows host) Right-click **Shared VMs** and select **Roles**.<br>■ (Linux host) Right-click **Shared VMs** and select **Edit Roles**. |
| **Edit a role on a remote host** | ■ (Windows host) Right-click the remote host and select **Roles**.<br>■ (Linux host) Right-click the remote host and select **Edit Roles**. |

2 Select the role to edit.

| Option | Description |
|---|---|
| **Change the role name** | ■ (Windows host) Double-click the role in the Roles list and type a new name.<br>■ (Linux host) Type a new name in the **Name** text box. |
| **Change the privileges in the role** | Select or deselect privileges from the privileges tree. You can expand the tree to view the privileges in each category. |

3 Click **OK** (Windows host) or **Save** (Linux host) to save your changes.

## Clone a Role

You can make a copy of an existing role by cloning it. When you clone a role, the new role is not applied to users, groups, or objects. You must assign the role to users or groups and objects.

You can change the privileges in a cloned role during the cloning process. See *Defined Privileges* in the Workstation documentation center for descriptions of the available privileges. The Workstation documentation center is available on the VMware Web site at https://www.vmware.com/support/pubs/ws_pubs.html.

### Prerequisites

If you are cloning a role on a remote host, connect to the remote server. See "Connect to a Remote Server," on page 182.

### Procedure

1 Open the Edit Roles dialog box.

| Option | Description |
|---|---|
| **Clone a role on the local host** | ■ (Windows host) Right-click **Shared VMs** and select **Roles**.<br>■ (Linux host) Right-click **Shared VMs** and select **Edit Roles**. |
| **Clone a role on a remote host** | ■ (Windows host) Right-click the remote host and select **Roles**.<br>■ (Linux host) Right-click the remote host and select **Edit Roles**. |

2 Select the role to clone and click **Clone**.

Workstation adds a copy of the role to the list of roles.

3 Type a new name for the cloned role.

| Option | Description |
|---|---|
| **Windows host** | Replace the name of the role in the Roles list. |
| **Linux host** | Type a new name in the **Name** text box. |

4 (Optional) To change the privileges in the cloned role, select or deselect privileges from the privileges tree.

You can expand the tree to view the privileges in each category.

5 Click **OK** (Windows host) or **Save** (Linux host) to create the new role.

## Remove a Role

When you remove a role, Workstation removes the definition from the list of roles.

IMPORTANT Make sure that you understand how users will be affected before you remove or replace role assignments.

### Prerequisites

If you are removing a role on a remote host, connect to the remote server. See "Connect to a Remote Server," on page 182.

### Procedure

1 Open the Edit Roles dialog box.

| Option | Description |
|---|---|
| **Remove a role on the local host** | ■ (Windows host) Right-click **Shared VMs** and select **Roles**.<br>■ (Linux host) Right-click **Shared VMs** and select **Edit Roles**. |
| **Remove a role on a remote host** | ■ (Windows host) Right-click the remote host and select **Roles**.<br>■ (Linux host) Right-click the remote host and select **Edit Roles**. |

2 Select the role to remove and click **Remove**.

On a Windows host, Workstation removes configured user or group and role pairings on the host. Users or groups that do not have other permissions assigned lose all privileges.

3 If the role is assigned to a user or group, select a reassignment option and click **OK**.

| Option | Description |
|---|---|
| **Remove the role from all affected users and groups** | ■ (Windows host) Select **Remove role assignments**.<br>■ (Linux host) Select **Remove affected permissions**.<br>Users or groups that do not have other permissions assigned lose all privileges. |
| **Remove the role and assign another role to all affected users and groups** | ■ (Windows host) Select **Reassign affected users to** and select a role.<br>■ (Linux host) Select **Reassign affected permissions to** and select a role. |

# Using Permissions to Restrict Users

You can control which users can access remote hosts and shared virtual machines by creating permissions. To create a permission, you pair a user or group with a role and associate that pairing with an object. The role defines the actions that a user or group can perform, the user or group indicates who can perform the actions, and the object is the target of the actions.

A role is a predefined set of privileges. Privileges define individual rights that a user requires to perform actions and read properties. A single user can have different roles for different objects.

Users can inherit permissions through group membership and through the object hierarchy. When you assign permissions to a group, all of the users in the group inherit those permissions. If you define multiple group permissions on the same object and a user belongs to two or more of those groups, the user inherits all of the privileges assigned to the groups. If you define a permission for the user on the object, that permission takes precedence over all group permissions.

## Add a Permission

To create a permission, you assign a user or group and a role to an object.

The available users and groups include local users and groups on the host system. For Workstation, users and groups in the Windows domain that the host system belongs to are also included. For remote hosts that vCenter Server manages, users and groups in the Windows domain list that vCenter Server references are also included.

The object of a permission can be a shared or remote virtual machine, the **Shared VMs** item, or a remote host. For remote hosts that vCenter Server manages, you can also set permissions on datacenters and folders within datacenters.

When you add a permission, you can indicate whether the permission propagates down the object hierarchy. Propagation is not universally applied. Permissions that you define for a child object always override the permissions that propagate from parent objects.

**NOTE** You cannot use Workstation to create, remove, or modify users and groups. To manage users and groups, use the mechanisms that the host operating system provides.

### Prerequisites

- Verify that you know the default roles. See "Default System Roles," on page 191.
- If you are setting a permission on a remote object, connect to the remote server. See "Connect to a Remote Server," on page 182.

### Procedure

1 Open the Permissions dialog box.

| Option | Description |
|---|---|
| **If the object is a shared or remote virtual machine** | Right-click the object and select **Manage > Permissions**. |
| **If the object is a remote host, datacenter, or folder** | Right-click the object and select **Permissions**. |

2 Click **Add**.

3 Select the location of the user or group from the **Domain** drop-down menu.

If you select **(server)**, only local users and groups appear in the list.

4 Select the name of the user or group from the list.

You can type a name in the search box to filter the users and groups in the list.

5 Add the permission.

| Option | Description |
|---|---|
| **Windows host** | Click **Add**, select the user or group, select a role from the drop-down menu under Assigned Role, and click **OK**. |
| **Linux host** | Select a role from the **Role** drop-down menu and click **Add**. |

On a Linux host, the permission is added immediately. On a Windows host, the permission is not added until you click **OK**.

6 (Optional) If you do not want to propagate the permission to child objects, deselect the **Propagate** check box next to the new permission.

If the object is a shared or remote virtual machine and you deselect the **Propagate** check box, you must confirm that the user can have read-only access to the host. Users must have read-only access to the host on which a virtual machine is running to access the virtual machine through Workstation.

The propagation setting takes effect immediately.

7 (Windows host only) Click **OK** to add the permission.

## Edit a Permission

You can change the role that is paired with a user or group. You can also change the propagation setting.

### Prerequisites

- Verify that you know the default roles. See "Default System Roles," on page 191.
- If you are editing a permission on a remote object, connect to the remote server. See "Connect to a Remote Server," on page 182.

### Procedure

1 Open the Permissions dialog box.

| Option | Description |
|---|---|
| **If the object is a shared or remote virtual machine** | Right-click the object and select **Manage > Permissions**. |
| **If the object is a remote host, datacenter, or folder** | Right-click the object and select **Permissions**. |

2 Select the permission.

3 Select a new role from the drop-down menu.

On a Windows host, the drop-down menu is under Assigned Role.

On a Linux host, the role is changed immediately. On a Windows host, the role is not changed until you click **OK**.

4 To change the propagation setting, select or deselect the **Propagate** check box.

The propagation setting change takes effect immediately.

5 (Windows host only) Click **OK** to save your changes.

## Remove a Permission

You can remove the user or group and role pair for a selected object. You cannot remove an inherited permission.

Removing a permission does not remove the user or group from the list of available users and groups, nor does it remove the role from the list of available roles.

### Prerequisites

If you are removing a permission on a remote object, connect to the remote server. See "Connect to a Remote Server," on page 182.

### Procedure

1 Open the Permissions dialog box.

| Option | Description |
|---|---|
| **If the object is a shared or remote virtual machine** | Right-click the object and select **Manage > Permissions**. |
| **If the object is a remote host, datacenter, or folder** | Right-click the object and select **Permissions**. |

2 Select the permission and click **Remove**.

On a Linux host, the permission is removed immediately. On a Windows host, the permission is not removed until you click **OK**.

3 (Windows host only) Click **OK** to remove the permission.

# Using the vmware Command 7

You can use the vmware command to run Workstation from the command line on a Linux or Windows host system.

This chapter includes the following topics:


- "Run the vmware Command," on page 199
- "Incorporate Workstation Startup Options in a Windows Shortcut," on page 200


## Run the vmware Command

You can run the vmware command on a Linux or Windows host system. You can type the command in a Linux terminal window or at the Windows command prompt. You can also create scripts to run multiple commands.

### Prerequisites

Familiarize yourself with the vmware command options. See "vmware Command Options," on page 199.

### Procedure

- To run the vmware command on a Linux host system, use the following syntax.

  `/usr/bin/vmware [-n] [-x] [-X] [-t] [-q] [-s` *variable_name* `=` *value* `] [-v] [` *path_to_vm* `.vmx] [http[s]://` *path_to_vm* `.vmx] [X toolkit options]`

- To run the vmware command on a Windows host system, use the following syntax.

  `C:\Program Files\VMware\VMware Workstation\vmware.exe [-n] [-x] [-X] [-t] [-q] [-s` *variable_name* `=` *value* `] [-v] [` *path_to_vm* `.vmx] [http[s]://` *path_to_vm* `.vmx]`

## vmware Command Options

When you run the vmware command, you can specify certain options.

**Table 7-1.** vmware Command Options

| Option | Description |
|---|---|
| -n | Opens a new Workstation window. |
| -t | Opens a virtual machine in a new tab in the existing Workstation window. |
| -x | Powers on the virtual machine when Workstation starts. This option is equivalent to clicking **Power On** in the Workstation toolbar. |
| -X | Powers on the virtual machine and switches the Workstation window to full screen mode. |

**Table 7-1.** vmware Command Options (Continued)

| Option | Description |
|---|---|
| `-q` | Closes the virtual machine tab when the virtual machine powers off. If no other virtual machine is open, it also exits Workstation. This option is useful when the guest operating system can power off the virtual machine. |
| `-s` | Sets the specified variable to the specified value. You can specify at the command line any variable names and values that are valid in the configuration file. |
| `-v` | Displays the product name, version, and build number. |
| *`path_to_vm`*`.vmx` | Launches a virtual machine by using the specified virtual machine configuration (.vmx) file. |
| `http[s]://` *`path_to_vm`* `.vmx` | Stream a virtual machine from a Web server. The virtual machine must be made available for streaming. |

On Linux hosts, you can pass X toolkit options as arguments, such as `--display` and `--geometry`. Some options, such as the size and title of the Workstation window, cannot be overridden.

# Incorporate Workstation Startup Options in a Windows Shortcut

The most convenient way to use `vmware` command options is to incorporate them into the command that a Windows shortcut generates.

### Prerequisites

Familiarize yourself with the `vmware` command options. See "vmware Command Options," on page 199.

### Procedure

1 Right-click the Workstation shortcut and select **Properties**.

2 In the **Target** text box, add any options to use after the `vmware.exe` and enclose the entire command string in quotation marks.

For example:

```
"C:\Program Files\VMware\VMware Workstation\vmware.exe -X
C:\Documents and Settings\username\My Documents\My Virtual Machines\Windows Me\Windows
Me.vmx"
```

# Index


## A

accelerated 3D graphics, preparing the host system **91**
acceleration, disabling **84**
ACPI S1 sleep feature **50**
Administrator default role **191**
ALSA
  configuring virtual machines **94**
  giving a user permission **94**
  overriding the library version **93**
  using **93**
application shortcuts, creating in Unity mode **71**
audience information **5**
Autologon, configuring **46**
AutoProtect snapshots, enabling **80**

## B

background settings, configuring **48**
bandwidth, configuring **150**
batch power operations **75**
battery information **69**
bridged networking
  assigning IP addresses **152**
  configuring **151–153**
BusLogic driver, installing **131**

## C

CD-ROM drives
  adding **111**
  configuring **111**
  configuring legacy emulation mode **113**
cleaning up virtual disks **107**
clones
  creating **22, 24**
  full **24**
  linked **23**
closing virtual machines **48**
converting teams **76**
copy and paste feature
  disabling **53**
  restrictions **52**
  using **52**
creating virtual machines **7**
Ctrl+Alt, using in a key combination **137**
custom configuration, virtual machine **8**

## D

DDNS **168**
debugging, using serial connection **109**
deleting, virtual machines **85**
devices, configuring and managing **111**
DHCP
  changing settings **169**
  DHCPD **168**
  editing the configuration file **171**
DHCP server, NAT **155**
disk drives, cleaning up **107**
disk modes, configuring **14**
disk types **14**
display settings, configuring **90**
displays
  changing **68**
  configuring preference settings **89**
  resizing **73**
download components **31**
downloading virtual machines **188**
drag-and-drop feature
  disabling **52**
  restrictions **51**
  using **51**
DVD drives
  adding **111**
  configuring **111**
  configuring legacy emulation mode **113**

## E

Easy Install, responding to prompts **9, 20**
ECR errors, troubleshooting **127**
encryption
  changing the password **98**
  limitations **95**
  removing **97**
  virtual machine **94, 96**
enhanced virtual keyboard, installing the driver **135**
exclusive mode **69**
experiation date **97**
expiration date, timestamp **97**
exporting OVF files **108**

## F

files, virtual machine **40**
floppy drives
  adding **112**
  configuring **111**
folders
  creating **75**
  managing virtual machines **74**
  removing virtual machines **75**
FreeBSD guest operating system, VMware Tools installation or upgrade (tar installer) **38**
full screen mode **68**

## G

generic SCSI devices
  adding **130**
  avoiding concurrent access problems on Linux **131**
  configuring **129**
  troubleshooting detection problems **131**
guest operating systems
  installing manually **21**
  selecting **9**

## H

hard disk, cleanup **107**
hard power controls **87**
hardware, customizing **17**
hardware compatibility, changing **107**
hardware compatibility setting, selecting in the New Virtual Machine wizard **8**
hardware settings, modifying **143**
host-only networks
  adding **152, 164**
  avoiding packet leakage **166**
  configuring **163, 164**
hot keys
  changing combinations **136**
  changing for Unity mode **137**
  default combinations **136**
human interface devices, connecting **63**

## I

I/O controller types **12**
IDE **12**
importing virtual machines **27**
install components **31**
installing VMware Tools
  FreeBSD (tar installer) **38**
  Linux (tar installer) **34**
  Microsoft Windows **33**
  NetWare (tar installer) **36**
  process overview **30**
  Solaris (tar installer) **37**
IP addresses, assigning **169, 172**

## K

key code mappings, configuring **139**
key mappings, changing **138**
keyboard features, configuring **134**
keyboard shortcuts **136**
keysyms
  defined **138**
  mapping **139**

## L

LAN segments
  configuring **172**
  configuring virtual machines to use **173**
  creating **172**
  deleting **173**
language codes **104**
linked clones, moving **100**
Linux guest, VMware Tools installation or upgrade (tar installer) **34**
lock files **122**

## M

MAC addresses
  assigning manually **176**
  changing **175, 176**
mapped drives **59**
maximum virtual disk size **16**
memory allocation **11**
Microsoft Windows guest operating system, VMware Tools installation or upgrade **33**
monitors, using multiple **71, 72**
moving virtual machines
  considerations **99**
  new location or host **99**

## N

NAT
  changing settings **156, 157**
  configuration file sections **158**
  configuring **154**
  editing the configuration file **158**
  external access **156**
  features and limitations **155**
  sample Linux configuration file **160**
  specifying connections from ports below 1024 **162**
  using NetLogon **161, 162**
NAT device, understanding **155**
NetLogon **161**
NetWare guest operating system, VMware Tools installation or upgrade (tar installer) **36**
network
  changing the configuration **147**
  virtual network editor **149**

network configuration example **176, 177**
network connection types **12**
networking components, understanding **145**
networking configurations, common **146**
New Virtual Machine wizard **18, 84**
No Access default role **191**

## O

OVA format virtual machines **28**
OVF files, exporting virtual machines **108**
OVF format virtual machines **28**

## P

packet forwarding, disabling **167**
packet leakage, host-only networks **166**
packet loss percentage, configuring **150**
parallel ports
  configuring **125**
  configuring device permissions **127**
  configuring on Linux 2.6.x kernels hosts **126**
passwords for encrypting and restricting virtual machines **94, 96**
pause feature restrictions **49**
pausing virtual machines **48, 49**
PDAs, installing drivers **64**
permissions
  adding **195**
  changing **196**
  removing **197**
  understanding **195**
physical machines
  preparing for virtualization **26**
  virtualizing **25**
physical disks
  adding to an existing virtual machine **124**
  preparing to use **14, 123**
  using in a virtual machine **122**
power off behavior, configuring **87**
power on delay **76**
powering off virtual machines **47**
printers, using host printers in a virtual machine **60**
processors
  specifying number **11**
  using a virtual machine that has more than eight **133**
promiscuous mode **175**

## R

Read Only default role **191**
remote access, configuring **179, 180**
remote hosts **183**
remote servers
  connecting **182**
  disabling the prompt to save login information **183**
  disconnecting **184**
  downloading virtual machines from **188**
  removing saved login information **184**
removable devices, using in virtual machines **61**
repairing VMware Tools installations **39**
resizing
  Linux guests **73**
  Solaris guests **74**
restricted virtual machine, espiration date **97**
restriction password **97**
restrictions password **94, 96**
resuming virtual machines **49**
roles
  changing **193**
  cloning **193**
  creating **192**
  default **191**
  removing **194**
  using to assign privileges **191**
routing
  between host-only networks **165**
  controlling on host-only networks **167**

## S

Samba
  adding user passwords **174**
  configuring **174**
  on both bridged and host-only networks **174**
SATA **12**
screen colors, setting for virtual machines **92**
screen resolutions, working with nonstandard **74**
screenshots, creating for virtual machines **85**
SCSI **12**
serial ports
  changing the input speed **129**
  configuring **125, 128**
  using to debug applications **109, 110**
shared files, optimizing read and write access **56**
shared folders
  changing **58**
  changing properties **57**
  configuring **54**
  created by other users **55**
  disabling **58**
  mounting **56**
  supported guest operating systems **54**
  using **53**
  using permissions to restrict access **57**
  viewing in Windows **56**
shared virtual machines
  configuring **184**

configuring autostart **190**
converting to standard virtual machines **187**
creating **185, 186**
creating on remote hosts **189**
directory **10, 181**
viewing status **187**
shared virtual machines directory, default location **179**
smart card readers, switching on Linux hosts **67**
smart cards
disabling sharing **67**
using in virtual machines **65, 66**
snapshot manager, using **78**
snapshots
deleting **82**
enabling AutoProtect **80**
enabling background **81**
excluding virtual disks **82**
power-off options **80**
reverting **80**
taking **77, 79**
troubleshooting **83**
using **78**
soft power controls **87**
Solaris, resizing guests **74**
Solaris guest operating system, VMware Tools installation or upgrade (tar installer) **37**
SSL certificates, replacing **181**
starting background virtual machines **45**
starting virtual machines, streaming **45**
stopping virtual machines **47**
streaming virtual machines **45, 46**
subnet IP addresses, changing **170, 171**
suspending virtual machines **49**


## T


tar installer **34**
teams **76**
template mode, enabling **24**
thumbnails
managing virtual machines **74**
using **75**
transferring files and text **51**
typical configuration, virtual machine **8**


## U


uninstalling VMware Tools **39**
Unity mode, setting preferences **92**
Unity mode features **70**
upgrading VMware Tools
FreeBSD (tar installer) **38**
Linux (tar installer) **34**
Microsoft Windows **33**
NetWare (tar installer) **36**
process overview **30**
Solaris (tar installer) **37**
uploading virtual machines **188**
USB controller
adding **114**
configuring **113**
USB devices
connecting **62**
disabling autoconnect **63**
enabling high-speed support for USB 2.0 or 3.0 **115**
installing drivers **62**
mounting on a Linux host **63**
troubleshooting connection issues **64**
understanding device control sharing **64**
UUIDs
clones **22**
configuring **102**
using **101**


## V


v-scan codes **140**
vCPU
best use **11**
specifying number **11**
virtual machine, expiration date **97**
virtual disk
bus type **16**
controller type **16**
maximum size **16**
virtual disk capacity **16**
virtual disk files **17**
Virtual Disk Manager **121**
virtual disks
allocating disk space **15**
cleaning up **107**
configuring in the New Virtual Machine wizard **13**
disconnecting from the host **60**
mapping and mounting **59**
virtual hard disks
adding **117, 119**
cleaning up **107**
compacting **119**
configuring **116**
defragmenting **120**
expanding **119**
growing and allocating storage space **117**
moving **122**
removing **121**
setting up as IDE or SCSI **117**
using legacy **121**

virtual machine files, specifying in the New Virtual Machine wizard **10**
virtual machines
changing hardware compatibility **106**
configuring **87**
configuring for compatibility **101**
configuring power off behavior **87**
deleting **85**
downloading from a remote server **188**
installing software **84**
managing **87**
moving **98**
understanding **7**
uploading to remote servers **188**
using **43**
using the New Virtual Machine Wizard **8**
virtual machines directory **10**
virtual network adapter, changing **148**
virtual network adapters, adding **148**
virtual networking, configuring **145**
virtual symmetric multiprocessing, configuring **133**
virtualizing physical machines **25**
VIX API **109**
VM, expiration date **97**
VM Creator default role **191**
VM User default role **191**
VMCI Sockets interface **109**
VMnet
virtual network **145**
virtual switch **145**
VMware Tools
installing **33**
updating on a specific virtual machine **32**
using **29**
vmware command
incorporating into a Windows shortcut **200**
options **199**
running **199**
using **199**
VMware Player, using virtual machines **100**
VMware Tools installation
FreeBSD (tar installer) **38**
Linux (tar installer) **34**
Microsoft Windows **33**
NetWare (tar installer) **36**
process **30**
Solaris (tar installer) **37**
VMware Tools upgrade
FreeBSD (tar installer) **38**
Linux (tar installer) **34**
Microsoft Windows **33**
NetWare (tar installer) **36**
process **30**
Solaris (tar installer) **37**
VMware Workstation Server, understanding **179**
vmware-user, starting manually **39**
VNC client, connecting to a virtual machine **105**
VNC connections, viewing **106**
VNC server
configuring a virtual machine **103**
specifying a language keyboard map **103**
VProbes **109**

## W

Windows activation problems **27**
Windows authentication problems **26**
Windows Virtual PC virtual machines **29**
Windows XP Mode virtual machine, importing **27**
worksheet, typical virtual machine **17**
Workstation Server, log files **182**

## X

X server and keyboard mapping **137**
x-key codes, defined **138**
xFree86 and keyboard mapping **137**