Using VMware Workstation Pro

VMware Workstation Pro 17

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

https://docs.vmware.com/

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

Contents

Using VMware Workstation Pro 14

1 Introduction and System Requirements 15

Host System Requirements for Workstation Pro 15

Processor Requirements for Host Systems 15

Supported Host Operating Systems 16

Memory Requirements for Host Systems 16

Display Requirements for Host Systems 16

Disk Drive Requirements for Host Systems 16

Local Area Networking Requirements for Host Systems 18

ALSA Requirements 18

Virtual Machine Features and Specifications 18

Supported Guest Operating Systems 18

Virtual Machine Processor Support 18

Virtual Machine Chipset and BIOS Support 19

Virtual Machine Memory Allocation 19

Virtual Machine Graphics and Keyboard Support 19

Virtual Machine IDE Drive Support 19

Virtual Machine SCSI Device Support 20

Virtual Machine Floppy Drive Support 20

Virtual Machine Serial and Parallel Port Support 20

Virtual Machine USB Port Support 20

Virtual Machine Mouse and Drawing Tablet Support 21

Virtual Machine Ethernet Card Support 21

Virtual Machine Networking Support 21

Virtual Machine Sound Support 21

2 Installing and Using Workstation Pro 23

Obtaining the Workstation Pro Software and License Key 23

Trial Version Expiration Date Warnings 24

Installing Workstation Pro with Other VMware Products 24

Reinstalling Workstation Pro When Upgrading a Windows Host Operating System 24

Installing the Integrated Virtual Debuggers for Eclipse 25

Installing Workstation Pro 25

Install Workstation Pro on a Windows Host 25

Run an Unattended Workstation Pro Installation on a Windows Host 26

Install Workstation Pro on a Linux Host 28

Upgrading Workstation Pro 31

Prepare for an Upgrade 31
Upgrade Workstation Pro on a Windows Host 33
Upgrade Workstation Pro on a Linux Host 34
Change the Hardware Compatibility of a Virtual Machine 35
Uninstalling Workstation Pro 37
Uninstall Workstation Pro from a Windows Host 37
Uninstall Workstation Pro from a Linux Host 37
Start Workstation Pro 38
Using the Workstation Pro Window 38
Use Virtual Machines in the Workstation Pro Window 39
Use the Virtual Machine Library 40
Use the Thumbnail Bar 41
Use the Status Bar 42
Use Workstation Pro Tabs 42
Customize the Workstation Pro Window 43
Default Hot-Key Combinations 43
Using the Workstation Pro Online Help 44

3 Creating Virtual Machines 45
Understanding Virtual Machines 45
Preparing to Create a New Virtual Machine 46
Worksheet for Creating a Virtual Machine 46
Selecting a Virtual Machine Configuration 47
Selecting the Virtual Machine Hardware Compatibility Setting 47
Selecting a Guest Operating System 48
Specifying the Virtual Machine Name and File Location 49
Selecting the Firmware Type 50
Selecting the Number of Processors for a Virtual Machine 50
Allocating Memory for a Virtual Machine 51
Selecting the Network Connection Type for a Virtual Machine 51
Selecting the I/O Controller Type for a Virtual Machine 52
Selecting a Hard Disk for a Virtual Machine 53
Customizing Virtual Machine Hardware 58
Create a New Virtual Machine on the Local Host 58
Use Easy Install to Install a Guest Operating System 61
Install a Guest Operating System Manually 61
Install Windows 11 on a Virtual Machine in Workstation 63
Installing a Guest Operating System on a Physical Disk or Unused Partition 65
Create a Virtual Machine Shortcut 66
Cloning Virtual Machines 66
Using Linked Clones 67

Using Full Clones 68
Enable Template Mode for a Parent Virtual Machine of Linked Clones 68
Clone a Virtual Machine 68
Importing Virtual Machines 69
Import an Open Virtualization Format Virtual Machine 70
Import a VMware vCenter Server Appliance 71
Installing and Upgrading VMware Tools 71
Installing VMware Tools 72
Upgrading VMware Tools 73
Configure Automatic Software Updates 74
Configure VMware Tools Updates for a Specific Virtual Machine 76
Manually Installing and Upgrading VMware Tools 76
Starting the VMware User Process Manually If You Do Not Use a Session Manager 84
Uninstalling VMware Tools 85
Virtual Machine Files 85

4 Using Virtual Machines 88
Scan for Virtual Machines to Add to the Virtual Machine Library 88
Starting Virtual Machines 90
Start a Virtual Machine 91
Start a Virtual Machine That Is Running in the Background 92
Enable Autologon in a Windows Virtual Machine 92
Configure a Firmware Type 93
Enable Auto Start for Local Virtual Machine on Windows Host 94
Stopping Virtual Machines 95
Shut Down a Virtual Machine 96
Closing Virtual Machines and Exiting Workstation Pro 97
Pause and Unpause a Virtual Machine 98
Suspend and Resume a Virtual Machine 99
Transferring Files and Text 100
Using the Drag-and-Drop Feature 101
Using the Copy and Paste Feature 102
Using Shared Folders 103
Using Removable Devices in Virtual Machines 110
Use a Removable Device in a Virtual Machine 110
Connecting USB Devices to Virtual Machines 111
Troubleshooting USB Device Control Sharing 116
Using Smart Cards in Virtual Machines 117
Changing the Virtual Machine Display 120
Use Full Screen Mode 121
Use Exclusive Mode 122

Use Unity Mode 123
Use Multiple Monitors for One Virtual Machine 124
Use Multiple Monitors for Multiple Virtual Machines 125
Fit the Workstation Pro Console to the Guest Operating System Display 125
Using Folders to Manage Virtual Machines 128
Add a Virtual Machine to a Folder 128
Remove a Virtual Machine from a Folder 129
Manage Virtual Machines in a Folder 129
Change the Power On Delay 130
Convert a Team 130
Taking Snapshots of Virtual Machines 130
Using Snapshots to Preserve Virtual Machine States 132
Using the Snapshot Manager 133
Take a Snapshot of a Virtual Machine 133
Revert to a Snapshot 134
Take or Revert to a Snapshot at Power Off 135
Enable AutoProtect Snapshots 135
Enable Background Snapshots 136
Exclude a Virtual Disk from Snapshots 137
Delete a Snapshot 137
Troubleshooting Snapshot Problems 138
Install New Software in a Virtual Machine 139
Deactivate Acceleration if a Program Does Not Run 139
Take a Screenshot of a Virtual Machine 140
Delete a Virtual Machine 141

5 Running Workstation on a Hyper-V Enabled Host 142
Host VBS Mode on Workstation 142
Host VBS Mode Compatibility with Windows Version 143
Limitations of Host VBS Mode 143
Limitations in the VMs Suspend/Resume Operation 143

6 Configuring and Managing Virtual Machines 145
Configure Power Options and Power Control Settings 146
Configure SSH Login on a Linux Virtual Machine 148
Edit or Delete the SSH Login Configuration for a Linux Virtual Machine 149
Set Workstation Pro Display Preferences 149
Configure Display Settings for a Virtual Machine 151
Prepare the Host System to Use 3D Accelerated Graphics 153
Prepare a Virtual Machine to Use Accelerated 3D Graphics 154
Set Preferences for Unity Mode 155

Setting Screen Color Depth 156
Using Advanced Linux Sound Architecture 157
Override the ALSA Library Version Requirement for a Virtual Machine 157
Obtain ALSA Sound Card Information 158
Configure a Virtual Machine to Use an ALSA Sound Card 158
Encrypting Virtual Machines 159
Virtual Machine Encryption Limitations 160
Encrypt a Virtual Machine 160
Remove Encryption From a Virtual Machine 161
Change the Password for an Encrypted Virtual Machine 161
Moving Virtual Machines 162
Move a Virtual Machine to a New Location or Host 162
Open a Virtual Machine in VMware Workstation Player 164
Configure a Virtual Machine for Compatibility 165
Using the Virtual Machine UUID 166
Configure a Virtual Machine as a VNC Server 168
Specify a Language Keyboard Map for VNC Clients 168
Use a VNC Client to Connect to a Virtual Machine 170
View VNC Connections for a Virtual Machine 171
Change the Hardware Compatibility of a Virtual Machine 171
Considerations for Changing the Hardware Compatibility of a Virtual Machine 173
Clean Up a Virtual Hard Disk on Windows Hosts 173
Export a Virtual Machine to OVF Format 174
Export a Virtual Machine with vTPM to OVF Format on Intel-based Mac 175
Writing and Debugging Applications That Run In Virtual Machines 177
Debugging Over a Virtual Serial Port 177

7 Configuring and Managing Devices 179
Configuring DVD, CD-ROM, and Floppy Drives 179
Add a DVD or CD-ROM Drive to a Virtual Machine 179
Add a Floppy Drive to a Virtual Machine 180
Configure Legacy Emulation Mode for a DVD or CD-ROM Drive 181
Configuring a USB Controller 182
Add a USB Controller to a Virtual Machine 182
Enable Support for Isochronous USB Devices 183
Configuring and Maintaining Virtual Hard Disks 184
Configuring a Virtual Hard Disk 185
Compact a Virtual Hard Disk 188
Expand a Virtual Hard Disk 188
Defragment a Virtual Hard Disk 190
Remove a Virtual Hard Disk from a Virtual Machine 190

Using Virtual Disk Manager 191
Using Legacy Virtual Disks 191
Using Lock Files to Prevent Consistency Problems on Virtual Hard Disks 191
Moving a Virtual Hard Disk to a New Location 192
Adding a Physical Disk to a Virtual Machine 192
Prepare to Use a Physical Disk or Unused Partition 193
Add a Physical Disk to an Existing Virtual Machine 194
Configuring Virtual Ports 195
Add a Virtual Parallel Port to a Virtual Machine 196
Configure a Virtual Parallel Port on a Linux 2.6.x Kernel Host 197
Configure Permissions for a Parallel Port Device on a Linux Host 197
Troubleshoot ECR Errors for Parallel Ports 198
Add a Virtual Serial Port to a Virtual Machine 198
Change the Input Speed of a Serial Connection 200
Configuring Generic SCSI Devices 200
Add a Generic SCSI Device to a Virtual Machine 201
Avoiding Concurrent Access Problems for SCSI Devices on Linux Hosts 202
Troubleshoot Problems Detecting Generic SCSI Devices 202
Configuring Virtual Trusted Platform Module Devices 204
Add a Virtual Trusted Platform Module Device 204
Remove a Virtual Trusted Platform Module Device 204
Configuring Sixteen-Way Virtual Symmetric Multiprocessing 205
Configure Sixteen-Way Virtual Symmetric Multiprocessing 205
Use a Virtual Machine That Has More Than Sixteen Virtual Processors 206
Configuring Keyboard Features 206
Use the Enhanced Virtual Keyboard Feature in a Virtual Machine 207
Change Hot-Key Combinations for Common Operations 208
Change Hot-Key Combinations for Unity Mode 209
Configure Keyboard Mapping for a Remote X Server 210
Change How a Specific Key Is Mapped 211
Configure How Keysyms Are Mapped 212
V-Scan Code Table 213
Modify Hardware Settings for a Virtual Machine 217

8 Configuring Network Connections 218
Understanding Virtual Networking Components 218
Understanding Common Networking Configurations 219
Changing the Default Networking Configuration 220
Add a Virtual Network Adapter to a Virtual Machine 221
Modify an Existing Virtual Network Adapter for a Virtual Machine 222
Disconnect a Host Virtual Network Adapter 223

Configure Bandwidth, Packet Loss, and Latency Settings for a Virtual Machine 224
Configuring Bridged Networking 225
Assigning IP Addresses in a Bridged Networking Environment 226
Add a Bridged Network 227
Configure Bridged Networking for an Existing Virtual Machine 228
Change VMnet0 Bridged Networking Settings 228
Configuring Network Address Translation 229
Features and Limitations of NAT Configurations 230
Change NAT Settings 233
Editing the NAT Configuration File 235
Using NAT with NetLogon 239
Specifying Connections from Source Ports Below 1024 240
Configuring Host-Only Networking 241
Add a Host-Only Network 243
Configure Host-Only Networking for an Existing Virtual Machine 243
Set Up Routing Between Two Host-Only Networks 244
Avoiding IP Packet Leakage in Host-Only Networks 246
Controlling Routing Information for Host-Only Networks on Linux 247
Using DHCP and DDNS with Host-Only Networking on Linux 247
Assigning IP Addresses in Host-Only Networks and NAT Configurations 248
Change DHCP Settings for a Host-Only or NAT Network on a Windows Host 250
Change the Subnet Settings for a Host-Only or NAT Network on a Windows Host 250
Change the Subnet IP Address for a Host-Only or NAT Network on a Linux Host 251
DHCP Conventions for Assigning IP Addresses in Host-Only and NAT Networks 253
Enable Jumbo Frames 253
Enable Jumbo Frames on Linux Host 253
Enable Jumbo Frames on Windows Host 254
Configuring LAN Segments 254
Create a LAN Segment for a Virtual Machine 254
Configure a Virtual Machine to Use a LAN Segment 255
Delete a LAN Segment 255
Configuring Samba for Workstation Pro 256
Add Users to the Samba Password File 256
Use a Samba Server for Bridged or Host-Only Networking 256
Use Samba Without Network Access 257
Using Virtual Network Adapters in Promiscuous Mode on Linux Hosts 257
Maintaining and Changing MAC Addresses for Virtual Machines 258
Change the MAC Address for a Virtual Machine 259
Manually Assign a MAC Address to a Virtual Machine 259
Sample Custom Networking Configuration 260
Create the Sample Custom Networking Configuration 260

9 Using Remote Connections to Manage Remote Virtual Machines 263

Connect to a Remote Server 263

Interacting with Remote Hosts and Virtual Machines 264

Turn Off the Prompt to Save Remote Login Information 265

Remove Saved Login and Exception Information for Remote Servers 265

Disconnect from a Remote Server 266

Uploading Virtual Machines to Remote Servers 266

Upload a Virtual Machine to a Remote Server 267

Download a Virtual Machine from a Remote Server 268

Create a Virtual Machine on a Remote Host 268

Manage Virtual Machine Power Actions on Remote Hosts 270

Using Roles to Assign Privileges 271

Default System Roles 272

Create a Role 272

Edit a Role 273

Clone a Role 274

Remove a Role 275

10 Changing Workstation Pro Preference Settings 276

Configuring Workspace Preference Settings 276

Configuring the Default Locations for Virtual Machine Files and Screenshots 277

Configuring Virtual Machine Exit Behavior 278

Enabling Shared Folders Created By Other Users 279

Changing the Default Hardware Compatibility Setting 280

Configuring Power On Delay and Aero Peek Thumbnail Settings 280

Changing the Remote Server Login Privacy Setting 281

Configuring Input Preference Settings 281

Configuring Keyboard and Mouse Settings 281

Configuring Cursor Settings 282

Changing Hot-Key Combinations 283

Configuring Workstation Pro Display Preference Settings 284

Configuring Autofit Settings 284

Configuring Full Screen Settings 285

Configuring Menu and Toolbar Settings 285

Configuring Workstation Pro Color Theme Settings 286

Configuring USB Device Connection Behavior 286

Configuring Software Update Preference Settings 286

Configuring Software Updates Settings 287

Configuring Connection Settings for a Proxy Server 288

Join or Leave the Customer Experience Improvement Program 288

Configuring Workstation Pro Memory Preference Settings 289

Configuring Reserved Memory 289
Configuring Additional Memory Settings 290
Configuring Workstation Pro Priority Preference Settings 290
Configuring Process Priorities on Windows Hosts 291
Configuring Background Snapshots 291
Configuring Device Settings for Windows Hosts 291
Configuring the Autorun Feature on Windows Hosts 292

11 Configuring Virtual Machine Option Settings 293
Configuring General Option Settings for a Virtual Machine 293
Changing a Virtual Machine Name 294
Changing the Guest Operating System 294
Changing the Virtual Machine Working Directory 295
Configuring Power Settings for a Virtual Machine 295
Configuring Power Options for a Virtual Machine 296
Configuring Power Controls for a Virtual Machine 296
Configuring Snapshot Options for a Virtual Machine 297
Configuring AutoProtect Options for a Virtual Machine 298
Configuring Guest Isolation Options for a Virtual Machine 299
Configuring Tablet Sensor Input Options for a Virtual Machine 300
Configuring VMware Tools Options for a Virtual Machine 301
Configuring a Virtual Machine as a VNC Server 302
Configuring Unity Mode for a Virtual Machine 302
Configuring Appliance Details for a Virtual Machine 303
Configuring Autologin for a Virtual Machine 304
Configuring Advanced Options for a Virtual Machine 304
Configuring Process Priorities for a Virtual Machine 305
Gathering Debugging Information 305
Configuring Advanced Settings for a Virtual Machine 306
Configuring the Firmware Type for a Virtual Machine 308
Configuring Access Control for a Virtual Machine 308

12 Configuring Virtual Machine Hardware Settings 309
Adding Hardware to a Virtual Machine 309
Removing Hardware from a Virtual Machine 311
Adjusting Virtual Machine Memory 311
Configuring Virtual Machine Processor Settings 312
Configuring and Maintaining Virtual Hard Disks 313
Defragmenting Virtual Hard Disks 314
Expanding Virtual Hard Disks 314
Compacting Virtual Hard Disks 314

Changing Virtual Hard Disk Node and Mode Settings 315
Configuring CD-ROM and DVD Drive Settings 315
Configuring CD-ROM and DVD Drive Status and Connection Settings 316
Changing Virtual Device Node and Legacy Emulation Settings 317
Configuring Floppy Drive Settings 317
Configuring Virtual Network Adapter Settings 318
Configuring Virtual Network Adapter Device Status Settings 319
Configuring a Network Connection 319
Configuring Virtual Network Adapter Advanced Settings 322
Configuring USB Controller Settings 323
Configuring Sound Card Settings 324
Configuring Parallel Port Settings 324
Configuring Serial Port Settings 325
Configuring Generic SCSI Device Settings 326
Configuring Display Settings 326
Installing a Guest Operating System on a Physical Disk or Unused Partition 327

13 Using the Virtual Network Editor 329
Add a Bridged Virtual Network 330
Add a Host-Only Virtual Network 331
Rename a Virtual Network 332
Change Automatic Bridging Settings 332
Change NAT Settings 333
Change DHCP Settings on a Windows Host 335
Importing and Exporting Network Settings on Windows Host 336
Exporting Network Settings 336
Importing Network Settings 336

14 Running the Support Script 337
Register and Create a Support Request 337
Run the Support Script from Workstation Pro 338
Run the Support Script from a Windows Command Prompt 338
Run the Support Script from a Linux Terminal Window 339

15 Using vctl Command to Manage Containers and Run Kubernetes Cluster 340
Using the vctl Utility 341
Enabling KIND to Use vctl Container as Nodes to Run Kubernetes Clusters 341
Running vctl Commands 342
Syntax of vctl Commands 342
Examples of vctl Commands 345
Cleaning Up Residual Environment Data 347

16 Using the vmrun Command to Control Virtual Machines 349
Use the vmrun Utility 351
Syntax of the vmrun Command 351
Using Authentication Flags in vmrun Commands 351
Running vmrun Commands 352
Path to VMX File 352
Deactivate Dialog Boxes 352
Syntax of vmrun Commands 353
Examples of vmrun Commands 359

17 Using the vmware Command 364
Run the vmware Command 364
vmware Command Options 364
Incorporate Workstation Pro Startup Options in a Windows Shortcut 365

18 Using VMware Workstation Pro REST API 366
Use the VMware Workstation Pro REST API Service 366
Using Workstation REST API Service to Manage Power Options of Encrypted Virtual Machines 368

Using VMware Workstation Pro

Using VMware Workstation Pro describes how to use VMware Workstation Pro™ to create, configure, and manage virtual machines.

Intended Audience

This information is intended for anyone who wants to install, upgrade, or use Workstation Pro. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Introduction and System Requirements

1

Host computers that run Workstation Pro must meet specific hardware and software requirements. Virtual machines that run in Workstation Pro support specific devices and provide certain features.

Read the following topics next:

- Host System Requirements for Workstation Pro
- Virtual Machine Features and Specifications

Host System Requirements for Workstation Pro

The physical computer on which you install Workstation Pro is called the host system and its operating system is called the host operating system. To run Workstation Pro, the host system and the host operating system must meet specific hardware and software requirements.

Processor Requirements for Host Systems

You must install Workstation Pro on a host system that meets certain processor requirements.

Supported Processors

The following host systems are supported:

- A compatible 64-bit x86/AMD64 CPU launched in 2011 or later.
- For specific Host Operating Systems (HOS), refer to the vendor's recommended processor requirements:
  - For Microsoft-specific HOS, refer to the Microsoft documentation
  - For Linux-specific HOS, refer to the Linux Vendor-specific documentation

Processor Requirements for 64-Bit Guest Operating Systems

For supported processors to run 64-bit guest operating systems, the host system must use one of the following processors.

- An AMD CPU with AMD-V support
- An Intel CPU with VT-x support

If you have an Intel CPU that has VT-x support, you must verify that VT-x support is enabled in the host system BIOS. The BIOS settings that must be enabled for VT-x support vary depending on the system vendor. See the VMware knowledge base article at http://kb.vmware.com/kb/1003944 for information about how to determine if VT-x support is enabled.

When you install a 64-bit operating system, Workstation Pro performs checks to make sure the host system has a supported processor. You cannot install a 64-bit operating system if the host system does not meet the processor requirements.

Supported Host Operating Systems

You can install Workstation Pro on Windows and Linux host operating systems.

To see a list of the supported host operating systems, refer to the following KB article: KB80807

Memory Requirements for Host Systems

The host system must have enough memory to run the host operating system, the guest operating systems that run inside the virtual machines on the host system, and the applications that run in the host and guest operating systems.

The minimum memory required on the host system is 2 GB of RAM. 4 GB and above is recommended.

See your guest operating system and application documentation for more information on memory requirements.

Display Requirements for Host Systems

The host system must have a 16-bit or 32-bit display adapter. Use the latest graphics driver recommended for the host system.

To support Windows 7 Aero graphics, the host system should have either an NVIDIA GeForce 8800GT or later or an ATI Radeon HD 2600 or later graphics processor.

Important 3D benchmarks, such as 3DMark '06, might not render correctly or at all when running Windows Vista or Windows 7 virtual machines on some graphics hardware.

Guest 3D Support for Host Systems

The Windows host system must have GPUs that support DX 11.1 or later.

Disk Drive Requirements for Host Systems

Host systems must meet certain disk drive requirements. Guest operating systems can reside on physical disk partitions or in virtual disk files.

Table 1-1. Disk Drive Requirements for Host Systems

Drive Type	Requirements
Hard disk	■ IDE, SATA, SCSI and NVMe hard drives are supported. ■ At least 1 GB free disk space is recommended for each guest operating system and the application software used with it. If you use a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer. Refer to the vendor's recommended disk space for a specific guest operating system. ■ For basic installation, ~2.5 GB of free disk space is required on Windows and Linux. You can delete the installer after the installation is complete to reclaim disk space.
Optical CD-ROM and DVD	■ IDE, SATA, and SCSI optical drives are supported. ■ CD-ROM and DVD drives are supported. ■ ISO disk image files are supported.
Floppy	Virtual machines can connect to disk drives on the host computer. Floppy disk image files are also supported.

Solid-State Drives

If your host machine has a physical solid-state drive (SSD), the host informs guest operating systems they are running on an SSD.

This allows the guest operating systems to optimize behavior. How the virtual machines recognize SSD and use this information depends on the guest operating system and the disk type of the virtual disk (SCSI, SATA, IDE, or NVMe).

- On Windows 8, Windows 10, Ubuntu, and Red Hat Enterprise Linux virtual machines, all drive types can report their virtual disks as SSD drives.

  Note

  - NVMe virtual hard disks are natively supported for Windows 8.1 and later.
  - To create a new a virtual machine with a Windows 7 or Windows 2008 R2 guest operating system using NVMe as the virtual hard disk, apply the appropriate Windows hot fix. See https://support.microsoft.com/en-us/kb/2990941.
  - Several Linux operating systems support NVMe while others do not. Check with the operating system vendor.

- On Windows 7 virtual machines, only IDE and SATA virtual disks can report their virtual disks as SSD. SCSI virtual disks only report as SSD when used as a system drive in a virtual machine, or as a mechanical drive when used as a data drive inside a virtual machine.

Use the virtual machine operating system to verify your virtual machine is using SSD as its virtual disk.

Local Area Networking Requirements for Host Systems

You can use any Ethernet controller that the host operating system supports.

Non-Ethernet networks are supported by using built-in network address translation (NAT) or by using a combination of host-only networking and routing software on the host operating system.

ALSA Requirements

To use ALSA in a virtual machine, 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 sound device on the host system must not be muted.
- The current user must have the appropriate permissions to use the sound device.

Virtual Machine Features and Specifications

Workstation Pro virtual machines support specific devices and provide certain features.

Supported Guest Operating Systems

A guest operating system can be Windows, Linux, and other commonly used operating systems.

For the most recent list of guest operating systems that VMware products support, see the VMware Compatibility Guide site: http://www.vmware.com/resources/compatibility/search.php.

For instructions about how to install the most common guest operating systems, see the *VMware Guest Operating System Installation Guide*: http://partnerweb.vmware.com/GOSIG/home.html.

Virtual Machine Processor Support

Virtual machines support certain processor features.

- The same as the processor on the host computer.
- One virtual processor on a host system that has one or more logical processors.
- Up to 16 virtual processors (sixteen-way virtual symmetric multiprocessing, or Virtual SMP) on a host system that has at least 2 logical processors.

  Note Workstation Pro considers multiprocessor hosts that have 2 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.

Virtual Machine Chipset and BIOS Support

Virtual machines support certain virtual machine chipsets and BIOS features.

- Intel 440BX-based motherboard
- NS338 SIO chipset
- 82093AA I/O Advanced Programmable Controller (I/O APIC)
- Phoenix BIOS 4.0 Release 6 with VESA BIOS

Virtual Machine Memory Allocation

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

The maximum amount of memory for each virtual machine is 64GB.

Virtual Machine Graphics and Keyboard Support

Virtual machines support certain graphics features.

- VGA and SVGA are supported.
- 104-key Windows 95/98 enhanced keyboards are supported.
- To use the `GL_EXT_texture_compression_s3tc` and `GL_S3_s3tc` Open Graphics Library (OpenGL) extensions in a Windows XP or Windows 7 or later guest operating system, you must install Microsoft DirectX End-User Runtime in the guest operating system. OpenGL is an API that is used to define 2D and 3D computer graphics. You can download Microsoft DirectX End-User Runtime from the Microsoft Download Center Web site.

  The VMware guest operating system OpenGL driver for Windows and Linux supports the OpenGL 4.3 compatibility profile.

Virtual Machine IDE Drive Support

Virtual machines support certain IDE drives and features.

- Up to four devices, including disk, CD-ROM, and DVD drives, are supported.
- DVD drives can be used to read data DVD discs only.
- DVD video is not supported.
- Hard disks can be virtual disks or physical disks.
- IDE virtual disks can be up to 8TB.
- CD-ROM drives can be physical devices or ISO image files.

Virtual Machine SCSI Device Support

Virtual machines support certain SCSI devices and features.

- Up to 60 devices are supported.
- SCSI virtual disks can be up to 8TB.
- Hard disks can be virtual disks or physical disks.
- With Generic SCSI support, you can use devices in a virtual machine without installing drivers in the host operating system. Generic SCSI support works with scanners, CD-ROM drives, DVD drives, tape drives, and other SCSI devices.
- The LSI Logic LSI53C10xx Ultra320 SCSI I/O controller is supported.

Virtual Machine Floppy Drive Support

Virtual machines can have floppy drives.

- Up to two 2.88MB floppy devices are supported.
- Floppy drives can be physical drives or floppy image files.

Virtual Machine Serial and Parallel Port Support

Virtual machines support serial (COM) and parallel (LPT) ports.

- Up to four serial (COM) ports are supported. Output can be sent to serial ports, Windows or Linux files, or named pipes.
- Up to three bidirectional parallel (LPT) ports. Output can be sent to parallel ports or host operating system files.

Virtual Machine USB Port Support

Virtual machines can have USB ports and can support certain 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 and later virtual machines.
- Support for USB 2.0 and 3.0 requires that you configure virtual machine settings to enable USB 2.0 and 3.0 support and that you have compatible guest operating systems and virtual machine hardware versions.
- Most USB devices are supported, including USB printers, scanners, PDAs, hard disk drives, memory card readers, and digital cameras. Streaming devices, such as webcams, speakers, and microphones, are also supported.

Virtual Machine Mouse and Drawing Tablet Support

Virtual machines support certain types of mice and drawing tablets.

- PS/2 and USB mouse types are supported.
- Serial tablets are supported.
- USB tablets are supported.

Virtual Machine Ethernet Card Support

Virtual machines support certain types of Ethernet cards.

- Up to 10 virtual Ethernet cards are supported.
- The AMD PCnet-PCI II Ethernet Adapter is supported. For 64-bit guests, the Intel Pro/1000 MT Server Adapter is also supported.

Virtual Machine Networking Support

Virtual machines support certain Ethernet switches and networking protocols.

- Up to 10 virtual Ethernet switches are supported on Windows host operating systems. Up to 255 virtual Ethernet switches are supported on Linux host operating systems.
- Three switches are configured by default for bridged, host-only, and NAT networking.
- Most Ethernet-based protocols are supported, including TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell NetWare, and Network File System (NFS).
- Built-in NAT networking supports client software that uses TCP/IP, FTP, DNS, HTTP, and Telnet. VPN is supported for PPTP over NAT.

Virtual Machine Sound Support

Workstation Pro provides a sound device that is compatible with the Sound Blaster AudioPCI and Intel High-Definition Audio Specification. The Workstation Pro sound device is enabled by default.

Workstation Pro supports sound in all supported Windows and Linux guest operating systems.

Sound support includes pulse code modulation (PCM) output and input. You can play `.wav` files, MP3 audio, and Real Media audio. MIDI output from Windows guest operating systems is supported by the Windows software synthesizer. MIDI input is not supported, and no MIDI support is available for Linux guest operating systems.

Windows XP, Windows Vista, Windows 7 and most recent Linux distributions detect the sound device and install appropriate drivers for it.

For Workstation 7.x and earlier virtual machines, the vmaudio driver in VMware Tools is installed in 64-bit Windows XP, Windows 2003, Windows Vista, Windows 2008, and Windows 7 guest operating systems and in 32-bit Windows 2003, Windows Vista, Windows 2008, and Windows 7 guest operating systems.

For Workstation 8.x and later virtual machines, the High-Definition Audio (HD Audio) device is presented by default for both 64-bit and 32-bit Windows Vista and Windows 7 guest operating systems and their server counterparts. Windows provides a driver for HD Audio that is not part of VMware Tools.

On Linux host systems, Workstation 7.x and later supports Advanced Linux Sound Architecture (ALSA). Earlier versions of Workstation use the Open Sound System (OSS) interface for sound playback and recording in virtual machines running on Linux host systems. Unlike OSS, ALSA does not require exclusive access to the sound device. The host system and multiple virtual machines can play sound at the same time.

Installing and Using Workstation Pro

2

You can install Workstation Pro on a Linux or Windows host system. Installing or upgrading Workstation Pro typically involves running a standard GUI wizard.

Read the following topics next:

- Obtaining the Workstation Pro Software and License Key
- Installing Workstation Pro with Other VMware Products
- Reinstalling Workstation Pro When Upgrading a Windows Host Operating System
- Installing the Integrated Virtual Debuggers for Eclipse
- Installing Workstation Pro
- Upgrading Workstation Pro
- Uninstalling Workstation Pro
- Start Workstation Pro
- Using the Workstation Pro Window
- Using the Workstation Pro Online Help

Obtaining the Workstation Pro Software and License Key

The Workstation Pro installation software is in the file that you downloaded and the license key is sent to you in email.

The installation files for both host platforms are included in the packaged distribution. You can use the license key on both the Windows and Linux versions of Workstation Pro. You need one license for each host system.

If you do not enter the Workstation Pro license key during installation, you can specify the license key later, in Workstation Pro, select **Help > Enter License Key** and enter the license key on the Workstation Activation dialog box. You can also purchase a license key and view the status of an evaluation license from the Workstation Activation dialog box.

See the VMware Web site for information on obtaining an evaluation license.

Note If you have an invalid license, Workstation Pro prompts you to enter a license key each time you attempt to power on a virtual machine.

Once you have installed Workstation Pro, you can find your license key in the **About VMware Workstation Pro** window. Click **Help > About VMware Workstation Pro**.

- If you have an individual license for Workstation Pro, the key is displayed in the License Information section under Type. It is labeled *Individual* and followed by your license key.
- If you have a version of Workstation Pro licensed for multiple users, the Type field displays *Volume* and your license key is not displayed.
- If you did not enter a license for Workstation Pro, the Type field displays *Not applicable* and a license key is not displayed.
- If you have an evaluation license key for Workstation Pro, the Type field displays *Not applicable*. The date the evaluation license key expires is also displayed.

Trial Version Expiration Date Warnings

When you use the trial version of VMware Workstation Pro, a notice appears on the home page advising you of the trial license expiration date.

To purchase a license key click, click **Get a license key**. If you have a license key, click **Enter a license key**. You can also go to the **Help** menu and click **Enter a license key**.

Installing Workstation Pro with Other VMware Products

The only VMware products that can share a host system with Workstation Pro are VMware vSphere Client and VMware vCenter Converter Standalone. You cannot install Workstation Pro on a host system that has any other VMware virtualization products installed.

If the host system has another VMware virtualization product installed, you must uninstall that product before you install Workstation Pro.

Reinstalling Workstation Pro When Upgrading a Windows Host Operating System

Before you upgrade the operating system on a Microsoft Windows host, VMware recommends that you uninstall VMware Workstation Pro.

The way Workstation Pro is installed and configured depends partly on the version of Windows used. As a best practice, to ensure that Workstation Pro is properly configured for a new operating system, you must remove the Workstation Pro application before you perform the operating system upgrade. Uninstalling Workstation Pro guarantees that legacy components that apply only to older versions of Windows are not left behind .

For example, if you do not uninstall Workstation Pro before upgrading the Windows operating system, some virtual network adapters might not function properly after the operating system upgrade. Before you uninstall Workstation Pro, open the virtual network editor and note the settings used. You must configure these settings again after you reinstall Workstation Pro.

When you uninstall Workstation Pro, you need only uninstall the Workstation Pro application, not the virtual machines that you have created. When the operating system upgrade is complete, reinstall Workstation Pro or, if you are also upgrading Workstation Pro, install the new version of Workstation Pro.

Installing the Integrated Virtual Debuggers for Eclipse

If you plan to use the Integrated Virtual Debugger for Eclipse, you should install it on the host system before you install Workstation Pro.

If you must install the Integrated Virtual Debugger for Eclipse after you install Workstation Pro, run the Workstation Pro installer again and select **Modify/Change** to install the associated Workstation Pro plug-ins.

See the *Integrated Virtual Debugger for Eclipse Developer's Guide* for host system requirements and supported operating systems. This guide is available on the VMware Web site.

Installing Workstation Pro

You can install Workstation Pro on a Windows host system by running the installation wizard or by using the unattended installation feature of the Microsoft Windows Installer (MSI). The MSI unattended installation feature is useful if you are installing Workstation Pro on several Windows hosts and do not want to respond to wizard prompts. You install Workstation Pro on a Linux host system by running the Workstation Pro bundle installer.

- Install Workstation Pro on a Windows Host

  You run the Windows setup program and installation wizard to install Workstation Pro on a Windows host system.

- Run an Unattended Workstation Pro Installation on a Windows Host

  You can use the unattended installation feature of the Microsoft Windows Installer (MSI) to install Workstation Pro on Windows host systems without having to respond to wizard prompts. This feature is convenient in a large enterprise.

- Install Workstation Pro on a Linux Host

  You run the Linux bundle installer to install Workstation Pro on a Linux host system. By default, Workstation Pro is installed silently, and the installation progress is displayed in the terminal. When Workstation Pro is launched for the first time, a dialog box asks you to accept the EULAs and configure necessary settings. At the same time, pure console installation is also supported. You can run the installer with the `--console` option to install and configure Workstation Pro in the terminal, without the first-time dialog box appearing during the first launch.

Install Workstation Pro on a Windows Host

You run the Windows setup program and installation wizard to install Workstation Pro on a Windows host system.

Remote connections and virtual machine sharing are enabled by default when you install Workstation Pro. With remote connections, you can connect to remote hosts and run remote virtual machines. With virtual machine sharing, you can create virtual machines that other instances of Workstation Pro can access remotely.

Prerequisites

- Verify that the host system meets the host system requirements. See Host System Requirements for Workstation Pro.
- Verify that you have administrative privileges on the host system.
- Verify that no incompatible VMware products are installed on the host system. See Installing Workstation Pro with Other VMware Products.
- Obtain the Workstation Pro software and license key. See Obtaining the Workstation Pro Software and License Key.
- If you plan to use the Integrated Virtual Debugger for Eclipse, install it on the host system. See Installing the Integrated Virtual Debuggers for Eclipse .

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. Double-click the `VMware-workstation-xxxx-xxxxxxx.exe` file, where *xxxx-xxxxxxx* is the version and build numbers.
3. Follow the prompts to finish the installation.

   Depending on your configuration, you might need to restart the host system to finish the installation.

Results

After Workstation Pro is installed, the VMware Workstation Server service starts on the host system. The VMware Workstation Server service starts whenever you restart the host system.

Run an Unattended Workstation Pro Installation on a Windows Host

You can use the unattended installation feature of the Microsoft Windows Installer (MSI) to install Workstation Pro on Windows host systems without having to respond to wizard prompts. This feature is convenient in a large enterprise.

Prerequisites

- Verify that the host system meets the host system requirements. See Host System Requirements for Workstation Pro.
- Verify that no incompatible VMware products are installed on the host system. See Installing Workstation Pro with Other VMware Products.

- Obtain the Workstation Pro software and license key. See Obtaining the Workstation Pro Software and License Key.
- If you plan to use the Integrated Virtual Debugger for Eclipse, install it on the host system. See Installing the Integrated Virtual Debuggers for Eclipse .
- Verify that the host computer has version 2.0 or later of the MSI runtime engine. This version of the installer is available in versions of Windows beginning with Windows XP and is available from Microsoft. For more information, see the Microsoft Web site.
- Familiarize yourself with the installation properties. See Installation Properties.

Procedure

1. Log in to the host system as the Administrator user or as a user who is a member of the local Administrators group.

   If you log in to the domain, the domain account must also be a local administrator.
2. Open a command-line console as Administrator.
3. Enter the installation command on one line.

   The following example installs Workstation Pro:

   ```
   VMware-workstation-full-x.x.x-xxxxxx.exe /s /v"/qn EULAS_AGREED=1 SERIALNUMBER="xxxxx-
   xxxxx-xxxxx-xxxxx-xxxxx" AUTOSOFTWAREUPDATE=1"
   ```

   You can use the optional `INSTALLDIR` property to specify a file path for the installation that is different from the default location.

   ```
   VMware-workstation-full-x.x.x-xxxxxx.exe /s /v"/qn EULAS_AGREED=1
   INSTALLDIR=C:\tests\test_install SERIALNUMBER=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
   AUTOSOFTWAREUPDATE=1"
   ```

   Note The double quotes around the file path are important. All the MSI arguments are passed with the `/v` option. The outer quotes group the MSI arguments and the double quotes put a quote in that argument.

   You can also run an unattended uninstallation of Workstation Pro on a Windows host. The following example uninstalls Workstation Pro and removes the license from the host.

   ```
   VMware-workstation-full-x.x.x-xxxxxx.exe /s /v"/qn REMOVE=ALL"
   ```

Installation Properties

When you perform an unattended installation of Workstation Pro, you can customize the installation by specifying installation properties in the installation command.

To specify an installation property in the installation command, use the format *property*="*value*". A value of 1 means true and a value of 0 means false.

Table 2-1. Installation Properties

Property	Description	Default Value
AUTOSOFTWAREUPDATE	Enables automatic upgrades for Workstation Pro when a new build becomes available.	1
DATACOLLECTION	Sends user experience information to VMware.	1
DESKTOP_SHORTCUT	Adds a shortcut on the desktop when Workstation Pro is installed.	1
EULAS_AGREED	Allows you to silently accept the product EULAs. Set to 1 to complete the installation or upgrade.	0
INSTALLDIR	Install Workstation Pro in a directory that is different from the default Workstation Pro location.	C:\Program Files (86)\VMware\VMware Workstation
KEEP_LICENSE	Specifies whether to keep or remove license keys when Workstation Pro is uninstalled.	1
KEEP_SETTINGFILES	Specifies whether to keep or remove settings files when Workstation Prois uninstalled	1
SERIALNUMBER	Lets you enter the license key when Workstation Pro is installed. Enter the license key with hyphens, for example, "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx".	
SOFTWAREUPDATEURL	Specifies a custom URL for managing software updates (separate from vmware.com).	
STARTMENU_SHORTCUT	Adds a **Start** menu item when Workstation Pro is installed.	1
SUPPORTURL	Set a support URL or email alias specifically for your users to contact with product issues through the Workstation Pro **Help** menu.	

Install Workstation Pro on a Linux Host

You run the Linux bundle installer to install Workstation Pro on a Linux host system. By default, Workstation Pro is installed silently, and the installation progress is displayed in the terminal. When Workstation Pro is launched for the first time, a dialog box asks you to accept the EULAs and configure necessary settings. At the same time, pure console installation is also supported. You can run the installer with the `--console` option to install and configure Workstation Pro in the terminal, without the first-time dialog box appearing during the first launch.

Remote connections and virtual machine sharing are enabled by default when you install Workstation Pro. With remote connections, you can connect to remote hosts and run remote virtual machines. With virtual machine sharing, you can create virtual machines that other instances of Workstation Pro can access remotely.

Prerequisites

- Verify that the host system meets the host system requirements. See Host System Requirements for Workstation Pro.

- Verify that no incompatible VMware products are installed on the host system. See Installing Workstation Pro with Other VMware Products.
- Obtain the Workstation Pro software and license key. See Obtaining the Workstation Pro Software and License Key.
- If you plan to use the Integrated Virtual Debugger for Eclipse, install it on the host system. See Installing the Integrated Virtual Debuggers for Eclipse .
- Compile the real-time clock function into the Linux kernel.
- Verify that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) is built and loaded as a kernel module and that it is set to `m` when the kernel is compiled.
- Familiarize yourself with the Linux command-line installation options. You must use the `--custom` option to specify certain configuration settings. See Linux Command Line Installation Options .
- Verify that you have root access on the host system.

Procedure

1. Log in to the host system with the user name that you plan to use when you run Workstation Pro.
2. Become root.

   For example: `su root`

   The command that you use depends on your Linux distribution and configuration.
3. Change directories to the directory that contains the Workstation Pro installer file.
4. Run the appropriate Workstation Pro installer for the host system.

   For example: `sh VMware-Workstation-`*`xxxx-xxxxxxx`*`.`*`architecture`*`.bundle [--`*`option`*`]`

   xxxx-xxxxxxx is the version and build numbers, *architecture* is x86_64, and *option* is a command-line option.
5. Accept the Open Virtualization Format (OVF) Tool license agreement.

   If you are using the `--console` option or installing Workstation Pro on a host system that does not support the GUI wizard, press Enter to scroll through and read the license agreement or type **q** to skip to the **[yes/no]** prompt.
6. Follow the prompts to finish the installation.

Results

After Workstation Pro is installed, `vmware-workstation-server` starts on the host system. When Workstation Pro starts, log in using your regular user name, not root. `vmware-workstation-server` starts whenever you restart the host system.

Linux Command Line Installation Options

You can use command line installation options to install Workstation Pro on a Linux host system.

To use the installation options, you must be logged in as root. Exit from the root account after the installation is finished.

Table 2-2. Linux Command Line Installation Options

Option	Description
`--console`	Enables you to use the terminal for installation.
`--custom`	Use this option to customize the following installation settings. ■ The locations of the installation directories. ■ The user who will initially connect to VMware Workstation Server. ■ The HTTPS port that VMware Workstation Server uses on the host system.
`--deferred-gtk`	Installs the product silently and configures the product on first launch.
`--ignore-errors` or `-I`	Allows the installation to continue even if there is an error in one of the installer scripts. Because the section that has an error does not complete, the component might not be properly configured
`--regular`	Shows installation questions that have not been answered before or are required. This is the default option.
`--required`	Shows the license agreement only and then proceeds to install Workstation Pro.
`--set-setting vmware-installer installShortcuts yes | no`	Adds shortcuts when Workstation Pro is installed. The default is `yes`.
`--set-setting vmware-installer libdir lib_path`	The `libdir` parameter instructs the installer where to place product-specific data files, such as libraries and internal icons. The installer places product files in `$libdir/vmware` and `$libdirvmware-installer`. The default is `/usr/lib`.
`--set-setting vmware-installer prefix /usr/local`	Installs executable files you run directly (ex: vmware, vmplayer, vmware-networks, etc.) here. Remainder of the product distributed under `libdir`-derived paths. The default is `/usr` .
`--set-setting vmware-workstation serialNumber xxxxx-xxxxx-xxxxx-xxxxx-xxxxx` `--set-setting vmware-player serialNumber xxxxx-xxxxx-xxxxx-xxxxx-xxxxx`	Lets you enter the license key when Workstation Pro or Workstation Player is installed. Enter the license key with hyphens, for example, xxxxx-xxxxx-xxxxx-xxxxx-xxxxx.
`--set-setting vmware-player-app simplifiedUI yes|no`	Turn on or off certain UI features of Workstation Player. The default is `no`.
`--set-setting vmware-player-app softwareUpdateEnabled yes|no`	Enables automatic upgrades for Workstation Pro or Workstation Player when a new build becomes available.

Table 2-2. Linux Command Line Installation Options (continued)

Option	Description
`--set-setting vmware-player-app softwareUpdateURL https://url/`	Specifies a custom URL for managing software updates (separate from vmware.com).
`--set-setting vmware-player-app supportURL https://url/`	Set a support URL or email alias specifically for your users to contact with product issues through the **Help** menu.

Upgrading Workstation Pro

You can upgrade from a previous version of Workstation to the current version of Workstation Pro by running the Workstation Pro installation program.

When you upgrade Workstation Pro, the installation program removes the previous version of Workstation Pro before it installs the new version.

To use the latest features, virtual machines that were created in the previous versions of Workstation must be upgraded to the current version of Workstation Pro.

What to read next

- Prepare for an Upgrade

  You must perform certain steps before you upgrade Workstation Pro.
- Upgrade Workstation Pro on a Windows Host

  You can upgrade to the current version of Workstation Pro on a Windows host system by running the Workstation Pro setup program and installation wizard for Windows.
- Upgrade Workstation Pro on a Linux Host

  You can upgrade to the current version of Workstation Pro on a Linux host system by running the Linux bundle installer for Workstation Pro. On most Linux distributions, the Linux bundle installer launches a GUI wizard. On some Linux distributions, including Red Hat Enterprise Linux 5.1, the bundle installer launches a command-line wizard instead of a GUI wizard. You can run the installer with the `--console` option to upgrade Workstation Pro in a terminal window.
- 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 UEFI, number of virtual slots, maximum number of CPUs, maximum memory configuration, and other hardware characteristics.

Prepare for an Upgrade

You must perform certain steps before you upgrade Workstation Pro.

Procedure

- Verify that all virtual machines are Workstation 7.x, 8, 9, 10 or 11 virtual machines.

  Direct upgrades from Workstation 2 and 3 virtual machines are not supported .
- Review the system requirements for the new version of Workstation Pro.
- If a virtual machine was created with a version of Workstation earlier than Workstation 5.5 and it has a snapshot, delete the snapshot.
- If you are upgrading from Workstation 4, 5.x, 6.x, or 7.x, and the previous version of Workstation used bridged settings to map virtual networks to specific physical or virtual adapters, record those settings.

  You must recreate these mappings after you upgrade Workstation Pro.
- Power off all running virtual machines in Workstation Pro.
- If any virtual machines are suspended, resume them and power them off in Workstation Pro.
- If any virtual machines are running in the background, start them in Workstation Pro and power them off.
- Back up all virtual machines by making backup copies of the files in the virtual machine directories and storing them in different directories.

  The files that you back up should include `.vmdk` or `.dsk` files, `.vmx` or `.cfg` files, and `.nvram` files. Depending on the upgrade path, you might not be able to run virtual machines under both the current version of Workstation Pro and the previous version.
- If you are upgrading Workstation 6.x on Windows XP to the current version of Workstation Pro on Windows Vista or Windows 7, verify that Service Pack 2 is installed and then upgrade the host operating system to Windows Vista or Windows 7.
- If you are upgrading Workstation 5.x on Windows Vista to the current version of Workstation Pro on Windows Vista, select **Programs > Programs and Features > Uninstall a program** in the Windows control panel to manually uninstall Workstation 5.x.
- If you are upgrading Workstation 5.x on Windows XP to the current version of Workstation Pro on Windows Vista or Windows 7, select **Add or Remove Programs** in the Windows control panel to manually uninstall Workstation 5.x.

Results

During an upgrade from Windows XP to Windows Vista or Windows 7, the location of virtual machines might change. The Windows Vista and Windows 7 upgrade use the registry to map the virtual machines to a new location. Before the upgrade, the default virtual machine location on Windows XP is `C:\Documents and Settings\`*`username`*`\My Documents\My Virtual Machines`. After the upgrade, the default virtual machine location on Windows Vista and Windows 7 is `C:\Users\`*`username`*`\Documents\Virtual Machines\`*`guestOSname`*.

Upgrade Workstation Pro on a Windows Host

You can upgrade to the current version of Workstation Pro on a Windows host system by running the Workstation Pro setup program and installation wizard for Windows.

Remote connections and virtual machine sharing are enabled by default when you upgrade Workstation Pro. With remote connections, you can connect to remote hosts and run remote virtual machines. With virtual machine sharing, you can create virtual machines that other instances of Workstation Pro can access remotely.

Prerequisites

- Verify that the host system meets the host system requirements. See Host System Requirements for Workstation Pro.
- Verify that you have a license key.
- Verify that you have administrative privileges on the host system.
- Prepare for the upgrade. See Prepare for an Upgrade.

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. Double-click the `VMware-workstation-xxxx-xxxxxxx.exe` file, where *xxxx-xxxxxxx* is the version and build numbers.
3. Click **Uninstall** to uninstall the previous version of Workstation Pro.
4. After the host system restarts, log in 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.
5. Follow the prompts to finish the upgrade.

   Depending on your configuration, you might need to restart the host system to finish the installation.

Results

After Workstation Pro is upgraded and you restart the host system, the VMware Workstation Server service starts. The VMware Workstation Server service starts whenever you restart the host system.

What to do next

To use the latest features, upgrade existing virtual machines to the new version of Workstation Pro. See Change the Hardware Compatibility of a Virtual Machine.

If you used bridged settings to map virtual networks to specific physical or virtual adapters in the previous version of Workstation Pro, recreate the mappings. If you created teams in the previous version of Workstation, convert the teams to use them in the new version of Workstation Pro.

Upgrade Workstation Pro on a Linux Host

You can upgrade to the current version of Workstation Pro on a Linux host system by running the Linux bundle installer for Workstation Pro. On most Linux distributions, the Linux bundle installer launches a GUI wizard. On some Linux distributions, including Red Hat Enterprise Linux 5.1, the bundle installer launches a command-line wizard instead of a GUI wizard. You can run the installer with the `--console` option to upgrade Workstation Pro in a terminal window.

Remote connection is enabled by default when you upgrade Workstation Pro. With remote connections, you can connect to remote hosts and run remote virtual machines.

Prerequisites

- Verify that the host system meets the host system requirements. See Host System Requirements for Workstation Pro.
- Verify that you have a license key.
- Prepare for the upgrade. See Prepare for an Upgrade.
- Familiarize yourself with the Linux command-line installation options. You must use the `--custom` option to specify certain configuration settings. See Linux Command Line Installation Options .
- Verify that you have root access to the host system.

Procedure

1. Log in to the host system with the user name that you plan to use when you run Workstation Pro.
2. Become root.

   For example: `su root`

   The command that you use depends on your Linux distribution and configuration.
3. Change directories to the directory that contains the Workstation Pro installer file.
4. Run the appropriate Workstation Pro installer for the host system.

   For example: `sh VMware-Workstation-xxxx-xxxxxxx.architecture.bundle [--option]`

   xxxx-xxxxxxx is the version and build numbers, *architecture* is x86_64, and *option* is a command-line option.

5 Accept the Open Virtualization Format (OVF) Tool license agreement.

   If you are using the `--console` option or installing Workstation Pro on a host system that does not support the GUI wizard, press Enter to scroll through and read the license agreement or type **q** to skip to the **[yes/no]** prompt.

6 Follow the prompts to finish the installation.

Results

After Workstation Pro is upgraded, `vmware-workstation-server` starts on the host system. `vmware-workstation-server` starts whenever you restart the host system.

What to do next

To use the latest features, upgrade existing virtual machines to the new version of Workstation Pro. See Change the Hardware Compatibility of a Virtual Machine.

If you used bridged settings to map virtual networks to specific physical or virtual adapters in the previous version of Workstation Pro, recreate the mappings. If you created teams in the previous version of Workstation, convert the teams to use them in the new version of Workstation Pro.

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 UEFI, number of virtual slots, maximum number of CPUs, maximum memory configuration, and other hardware characteristics.

When you upgrade Workstation Pro, you must change the hardware compatibility of virtual machines that were created in previous versions of Workstation Pro so that they can use the new features in the new version of Workstation Pro. You can run older versions of virtual machines in the new version of Workstation Pro, 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 Pro 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.

Procedure

1 Make backup copies of the virtual disk (`.vmdk`) files.

2 If you are upgrading from a Workstation 5.x virtual machine, or downgrading to a Workstation 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 or later, you can change the hardware compatibility of a remote virtual machine. However, you cannot downgrade 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.

   Update VMware Tools to the version included with the latest version of Workstation Pro, even if you upgraded the virtual machine to an earlier version of Workstation Pro. 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.

- If you upgrade a Workstation 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, Windows 7, or Windows 8 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 remote virtual machine.
- Using Workstation 10 and later, you can change the hardware compatibility of a remote virtual machine. However, you cannot down grade a previously created virtual machine.

Uninstalling Workstation Pro

You uninstall Workstation Pro on a Windows host by using the Windows setup program. On a Linux host, you uninstall Workstation Pro by running the bundle installer.

You can save the configuration before you uninstall the Workstation Pro Pro. This retains the configuration in Workstation Pro if you choose to reinstall Workstation Pro later.

Uninstall Workstation Pro from a Windows Host

You can run the Windows setup program to uninstall Workstation Pro from a Windows 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 the domain, the domain account must also be a local administrator.
2. Double-click the `VMware-workstation-xxxx-xxxxxxx.exe` file, where *xxxx-xxxxxxx* is the version and build numbers.
3. Click **Next** on the Welcome screen and then click **Remove**.
4. (Optional) To save product license and Workstation Pro configuration information, select the appropriate check boxes.
5. Click **Next** to begin uninstalling Workstation Pro.

Uninstall Workstation Pro from a Linux Host

You must run a command to uninstall Workstation Pro from a Linux host.

Prerequisites

Verify that you have root access to the host system.

Procedure

1 Log in to the Linux host system with the user name that you use when you run Workstation Pro.

2 Become root.

For example: `su root`

The command that you use depends on your Linux distribution and configuration.

3 In a terminal window, type **`vmware-installer -u vmware-workstation`**

4 Click **Next** to begin uninstalling Workstation Pro.

Start Workstation Pro

How you start Workstation Pro depends on the host system platform and the options that you selected during Workstation Pro installation.

On Windows host systems, you might have a desktop shortcut, a quick launch shortcut, or a combination of these options in addition to a **Start** menu item.

On Linux host systems, you start Workstation Pro from the command line. On some Linux distributions, including Red Hat Enterprise Linux 5.1, you can also start Workstation Pro from the **System Tools** menu under **Applications**.

Procedure

- To start Workstation Pro on a Windows host system, select **Start > Programs > VMware > VMware Workstation**.
- To start Workstation Pro on a Linux host system, type the `vmware` command in a terminal window.

Option	Command
/usr/bin is in your default path	`vmware &`
/usr/bin is not in your default path	`/usr/bin/vmware &`

Results

The first time you start Workstation Pro, Workstation Pro prompts you to accept the End User License Agreement. After you start Workstation Pro, the Workstation Pro window opens.

Using the Workstation Pro Window

A virtual machine is like a separate computer that runs in a window on the host system. Workstation Pro displays more than the screen of another computer. From the Workstation Pro window, you can interact with and run virtual machines. You can also switch easily from one virtual machine to another.

The best way to learn how to use Workstation Pro is to use it. The Workstation Pro window is designed to be intuitive and easy to use.

What to read next

- Use Virtual Machines in the Workstation Pro Window

  You interact with virtual machines through the Workstation Pro window.
- Use the Virtual Machine Library

  The virtual machine library appears on the left side of the Workstation Pro window. You use the library to view and select virtual machines, folders, and remote hosts in Workstation Pro. The library appears by default.
- Use the Thumbnail Bar

  The thumbnail bar appears along the bottom of the Workstation Pro window.
- Use the Status Bar

  The status bar appears at the bottom of the Workstation Pro window. You can use the icons on the status bar to see Workstation Pro messages and perform actions on devices such as hard disks, CD/DVD drives, floppy drives, and network adapters. The status bar appears by default.
- Use Workstation Pro Tabs

  Workstation Pro creates a tab in the right pane of the Workstation Pro window when you select an item in the library. Tabs appear by default.
- Customize the Workstation Pro Window

  You can customize the appearance of the Workstation Pro window by selecting items from the **View** menu.
- Default Hot-Key Combinations

  You can use keyboard shortcuts to interact with Workstation Pro and with virtual machines. Most of the available keyboard shortcuts for Workstation Pro are listed next to their associated commands in Workstation Pro menus.

Use Virtual Machines in the Workstation Pro Window

You interact with virtual machines through the Workstation Pro window.

Procedure

- Use the icons on the **Home** tab to create a new virtual machine, open an existing virtual machine, connect to a remote server, or view the Workstation Pro help system.
- Select a powered-off virtual machine in the library or click its tab to see the summary view for that virtual machine.

  The summary view shows a summary of configuration information and the virtual machine state. You can power on the virtual machine and edit virtual machine settings from the summary view.

- Select an active virtual machine in the library or click its tab to see the console view.

  The console view is like the monitor display of a physical computer. You can click the console view button on the toolbar to switch between the console and summary views.

- Select a virtual machine in the library and use the **VM** menu on the menu bar at the top of the Workstation Pro window to perform all virtual machine operations for the selected virtual machine.

  You can use the **VM** menu when a virtual machine is powered on or off. If an operation is not supported for the virtual machine in its current state, the menu item is not available.

- Select a virtual machine in the library and use the buttons on the toolbar at the top of the Workstation Pro window to perform common virtual machine operations and change the display for the selected virtual machine.

  You can use the buttons on the toolbar to take and manage snapshots, enter full screen and Unity mode, cycle multiple monitors, switch between the console and summary views, set the stretch ratio of the virtual machine.

- When a virtual machine is powered on, use the icons on the status bar at the bottom of the Workstation Pro window to see Workstation Pro messages and perform actions on virtual devices such as hard disks, CD/DVD drives, floppy drives, and network adapters.

  You can click or right-click on a removable device icon to connect or disconnect the device or edit its settings, and you can click the **Message log** icon to view the message log. Messages include warning information about the virtual machine. If the icon is dimmed, all messages have already been read.

- Select items in the library or use tabs to quickly switch between virtual machines, folders, and remote hosts.

Use the Virtual Machine Library

The virtual machine library appears on the left side of the Workstation Pro window. You use the library to view and select virtual machines, folders, and remote hosts in Workstation Pro. The library appears by default.

Prerequisites

If the library is not visible, select **View > Customize > Library**.

Procedure

- Right-click a virtual machine, folder, or remote host in the library to view the item's context menu and perform common operations.

- To find a specific virtual machine in the library, type its name, part of its description, or the name of the guest operating system in the search box.

  For example, to find all the virtual machines that have a Windows 8 guest operating system, type **`Windows 8`**. You can also search for folders and remote hosts.

- To view information about a virtual machine, select the virtual machine name in the library and, if powered on, click the **Show or hide console view** icon and **View All**.

Option	Description
A Powered Off Virtual Machine	The virtual machine details appear at the bottom of the page.
A Powered On Virtual Machine	In the menu bar, select the **Show or hide console view** for the virtual machine details to appear at the bottom of the page. Click **View All** to see network connection information.

  Virtual machines in either a powered off or powered on state provide information about the virtual machine, such as the hardware compatibility information. The information provided for a powered on virtual machine with VMware Tools installed is more detailed. For example, only a powered on virtual machine with VMware Tools installed lists the primary IP address.

- To mark a virtual machine or folder as a favorite in the library, right-click it and select **Mark as Favorite** or click the star icon.
- Use the library drop-down menu to show only powered on virtual machines or favorite items.

  By default, the library shows all items.
- To remove an item from the library, right-click it and select **Remove**.
- To remove non-existent virtual machines from the library, right-click **My Computer** and select **Remove Non-existent Virtual Machines**.

  Non-existent virtual machines are virtual machines that are no longer available from the library. For example, virtual machines on a removable storage device that is no longer connected to your host system.

  Workstation Pro removes all non-existent virtual machines from the library.

Use the Thumbnail Bar

The thumbnail bar appears along the bottom of the Workstation Pro window.

For active virtual machines, Workstation Pro updates the thumbnail in real time to show the actual content of the virtual machine. When a virtual machine is suspended, the thumbnail is a screenshot of the virtual machine at the time that it was suspended.

Prerequisites

If the thumbnail bar is not visible, select **View > Customize > Thumbnail Bar**.

Procedure

- Click a thumbnail to show the summary or console view for a virtual machine.
- Click thumbnails to quickly switch between virtual machines.

- To change the order of the thumbnails, change the order of the virtual machine tabs.

  Thumbnails appear in the same order as the virtual machine tabs. To move a virtual machine tab, drag and drop it to a new location.

- To change the virtual machines that appear in the thumbnail bar, select **Open Virtual Machines** or **Folder View Virtual Machines** from the thumbnail bar drop-down menu.

  The drop-down menu is a down-arrow on the thumbnail bar.

Use the Status Bar

The status bar appears at the bottom of the Workstation Pro window. You can use the icons on the status bar to see Workstation Pro messages and perform actions on devices such as hard disks, CD/DVD drives, floppy drives, and network adapters. The status bar appears by default.

Procedure

- Mouse over an icon on the status bar to see its name.
- Click or right-click on a removable device icon to connect or disconnect the device or edit its settings.
- Click the message log icon to view the message log.

  Messages include warning information about the virtual machine. If the icon is dimmed, all messages have already been read.

Use Workstation Pro Tabs

Workstation Pro creates a tab in the right pane of the Workstation Pro window when you select an item in the library. Tabs appear by default.

Procedure

- Use the links on the **Home** tab to create a virtual machine, open a virtual machine, connect to a remote server, virtualize a physical machine, use the virtual network editor, customize Workstation Pro preferences, download software updates, and view the help system.
- Use the virtual machine tabs to view virtual machine configuration information, modify virtual machine hardware and option settings, and create or modify the virtual machine description.
- Use the tab for a remote host to browse information about the remote host, including CPU, memory, and disk usage, and the virtual machines, and virtual machine tasks running on the remote host.

  If you are using Workstation Pro on a Windows host and the remote server is running vCenter Server, other objects can appear in the library. In this situation, when vCenter Server appears in the library, you can toggle between the Hosts and Clusters view and the VMs view. The Hosts and Clusters view displays datacenters, clusters, ESXi hosts, resource pools, vApps, and virtual machines.

- Select **File > Close Tab** to close a tab.

Customize the Workstation Pro Window

You can customize the appearance of the Workstation Pro window by selecting items from the **View** menu.

Procedure

1 Select **View > Customize** and select a Workstation Pro window view.

Option	Description
Library	The virtual machine library appears in the left side of the window. You can use the library to view and select virtual machines, folders, and remote hosts in Workstation Pro. The library appears by default.
Thumbnail Bar	A thumbnail bar appears at the bottom of the window. Depending on the thumbnail bar option that is selected, the thumbnail bar shows all open virtual machines or the virtual machines in the selected folder.
Toolbar	A toolbar appears at the top of the window. You can use the icons on the toolbar to start and stop virtual machines, take snapshots, change the display, and perform other common tasks. The toolbar appears by default.
Status Bar	A status bar appears at the bottom of the window when a virtual machine is selected. You can use the icons on the status bar to see Workstation Pro messages and perform actions on virtual machine devices such as hard disks, CD/DVD drives, floppy drives, and network adapters. The status bar appears by default.
Tabs	Workstation Pro creates a tab in the right pane when you select an item in the library. Tabs appear by default.

2 To specify which virtual machines appear in the thumbnail bar, select **View > Customize > Thumbnail Bar Options**.

Option	Description
Open Virtual Machines	The thumbnail bar shows thumbnails for all open virtual machines.
Folder View Virtual Machines	The thumbnail bar shows thumbnails for virtual machines in the selected folder.

Default Hot-Key Combinations

You can use keyboard shortcuts to interact with Workstation Pro and with virtual machines. Most of the available keyboard shortcuts for Workstation Pro are listed next to their associated commands in Workstation Pro menus.

Table 2-3. Default Hot-Key Combinations

Shortcut	Action
Ctrl+G	Grab input from the keyboard and mouse.
Ctrl+Alt	Release the mouse cursor.

Table 2-3. Default Hot-Key Combinations (continued)

Shortcut	Action
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. 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 Pro 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 Pro 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 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. You can change the Unity hot-key combination by modifying Unity preference settings.
Ctrl+Alt+M	In full screen mode, brings up the monitor layout menu. You can change the hot-key combination by modifying preference settings.

You can change the default hot-key combinations by modifying Workstation Pro for common virtual machine operations to Ctrl+Shift, you press Ctrl+Shift instead of Ctrl+Alt to release control from the current virtual machine.

Using the Workstation Pro Online Help

The Workstation Pro online help contains information about Workstation Pro settings and common tasks. Use the online help when you need to quickly find information about Workstation Pro preferences, virtual hardware settings, and virtual machine options.

For example, if you are configuring a virtual machine and you need information about a specific hardware setting, click **Help** on the dialog box that contains the setting. The Help window opens and a context-sensitive help topic appears in the right pane. To see the entire help system, select **Help > Help Topics** (Windows host) or **Help > Contents** (Linux host).

Creating Virtual Machines

3

You can create virtual machines on a host operating system that Workstation Pro supports.

You can create a new virtual machine in Workstation Pro by using the **New Virtual Machine** wizard, clone an existing Workstation Pro 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.

Read the following topics next:

- Understanding Virtual Machines
- Preparing to Create a New Virtual Machine
- Create a New Virtual Machine on the Local Host
- Cloning Virtual Machines
- Importing Virtual Machines
- Installing and Upgrading VMware Tools
- Virtual Machine Files

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 Pro. 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.

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 3-1. 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 ■ Product key ■ Operating system version ■ Full name ■ Password ■ Credentials for automatic login	
Easy Install information for Linux guests ■ Full name ■ User name ■ 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	

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 Pro 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 UEFI, 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 Pro preferences. By default, the default hardware compatibility setting is the installed Workstation Pro 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 Pro 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 3-2. 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	Select the Windows operating system edition to install.
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 3-3. 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 Pro 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.

See Use Easy Install to Install a Guest Operating System.

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 10 x64`.

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.

Virtual Machines Directory

Workstation Pro stores standard virtual machines in the virtual machines directory.

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

Table 3-4. Default Virtual Machines Directory

Host Operating System	Default Location
Windows Server 2008 R2 Windows Server 2012 R2	`C:\Documents and Settings\`*username*`\My Documents\My Virtual Machines` *username* is the name of the currently logged-in user.
Windows 7 Windows 8 Windows 10	`C:\Users\` *username* `\Documents\Virtual Machines` *username* is the name of the currently logged in user.
Linux	*homedir*`/vmware` *homedir* is the home directory of the currently logged in logged in user.

Selecting the Firmware Type

Depending on the guest operating system, when you use a custom configuration, the New Virtual Machine wizard prompts you to select the firmware type the virtual machine uses when it boots.

This option appears in the **New Virtual Machine Wizard** when the guest operating system is supported with the UEFI firmware type. Otherwise, the BIOS firmware type is selected by default.

Table 3-5. Firmware Type Options

Option	Description
BIOS	The virtual machine firmware uses BIOS when booting.
UEFI	The virtual machine uses UEFI when booting. If you select UEFI, depending on the guest operating system, you might have the option of enabling UEFI Secure Boot.

See Configure a Firmware Type.

Selecting 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 performance 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.

For more information about virtual processors, see Virtual Machine Processor Support.

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.

The maximum amount of memory for each virtual machine is 64GB.

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 Pro 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 3-6. 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. 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. 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. 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 8 Configuring Network Connections 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 Pro automatically configures your virtual machine with the SCSI controller best suited for the guest operating system, but you can change the controller.

Workstation Pro 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, LSI Logic SAS, or VMware Paravirtual (PVSCSI) adapter. If you are creating a remote virtual machine on an ESX host, you can also select a VMware Paravirtual SCSI 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 compatible with 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 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 website. Drivers for a Mylex (BusLogic) compatible host bus adapter are not obvious on the LSI Logic website. Search the support area for the numeric string in the model number, for example, search for 958 for BT/KT-958 drivers.

Selecting the VMware Paravirtual SCSI (PVSCSI) Adapter

In a Windows virtual machine:

Since the Windows ISO does not include a driver for the VMware Paravirtual SCSI (PVSCSI) adapter.

1 Add a Floppy Drive and select the driver file from the `C:\Program Files (x86)\VMware\VMware Workstation\Resources\*.flp` folder on the Windows host.

   If you are running a Windows virtual machine on a Linux host, the driver is saved in the `/usr/lib/vmware/resources` folder by default.

2 During the Windows setup, select **Load Driver > Browse** and select the PVSCSI adapter driver file.

In a Linux virtual machine:

The Linux distribution already includes the PVSCSI driver.

For more information about driver support, see the *VMware Guest Operating System Installation Guide*. For guest operating system support information, known issues, and SATA support, see the *VMware Compatibility Guide* available on the VMware website.

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 Pro 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.

What to read next

- 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.

- 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.

- 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.

- 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.

- 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.

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 a SATA disk for some guest operating systems. You can set up a virtual disk as an NVMe disk for guest operating systems that support the NVMe disk type.

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 2008 R2 or Windows Server 2012 R2 host	a Select **Start > Settings > Control Panel > Administrative Tools > Computer Management > Storage > Disk Management**. b Select a partition and select **Action > All Tasks > Change Drive Letter and Paths**. c Click **Remove**.
The partition is mapped to a Windows 7, Windows 8, or Windows 10 host	a Select **Start > Control Panel**. b In the menu bar, click the arrow next to **Control Panel**. c From the drop-down menu, select **All Control Panel Items > Administrative Tools > Computer Management > Storage > Disk Management (Local)**. d Right-click a partition and choose **Change Drive Letter and Paths**. e 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 7 hosts, you cannot use the system partition, or the physical disk that contains it, in a virtual machine. 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, ensure that it is configured as the primary on the IDE channel.

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

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

   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 Workstation Pro 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 Workstation Pro 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 Pro 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 0.001 GB and 8 TB 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 950 GB, a series of 2-GB virtual disk files are created. When you split a virtual disk greater than 950 GB, two virtual disk files are created. The maximum size of the first virtual disk file is 1.9 TB 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 8 TB. 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, 11, 12, 14	IDE	ATAPI	8192 GB (8TB)
10, 11, 12, 14	SCSI	BusLogic	2040 GB (2TB)
10, 11, 12, 14	SCSI	LSI Logic	8192 GB (8TB)
10, 11, 12, 14	SCSI	LSI Logic SAS	8192 GB (8TB)
10, 11, 12, 14	SATA	AHCI	8192 GB (8TB)
14	NVMe	NVMe	8192 GB (8TB)
9, 8, 7, 6.5	All	All	2040 GB (2TB)
6.0, 5	All	All	950 GB

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

Value	SCSI 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 3-7. 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 Pro 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 Pro 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 Pro 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.

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.

While creating a new virtual machine, you can follow the Easy Install option to create the virtual machine easily.

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.
- 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.

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**. ■ 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, SATA, or NVMe 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 firmware type, virtual machine processors, memory allocation, networking configuration, I/O controller types, virtual disk type and mode, and virtual disk.

Note For the firmware type, if you select UEFI and if the guest operating system supports UEFI Secure Boot, you can select the option to enable UEFI Secure Boot.

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.

Results

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.

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

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, user name, 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, user name, 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. b Select **Connected**. 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.

Install Windows 11 on a Virtual Machine in Workstation

Installing Windows 11 on a virtual machine is similar to installing Windows 11 on a physical computer. When you create a virtual machine with Windows 11 as the guest operating system, Workstation Pro adds vTPM (virtual Trusted Platform Module) to the virtual machine.

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

Note After you complete the installation of the Windows 11 operating system, we recommend that you do not remove the encryption or the vTPM device from the virtual machine for a seamless experience of using Windows 11.

Note Workstation does not support creating a Windows 11 guest operating system on a remote virtual machine.

Prerequisites

- Verify that you have the information the **New Virtual Machine** wizard requires to create a virtual machine.
- 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.

Procedure

1 Start the **New Virtual Machine** wizard.

Option	Description
Windows host	Select **File > New Virtual Machine**.
Linux host	Select **File > New Virtual Machine**.

2 Select the configuration type and click **Next**.

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, SATA, or NVMe 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
Installer disc	Select the physical drive where you inserted the installation disc.
Installer disc image file (iso)	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 Select the guest operating system as **Windows 11 x64**, and then click **Next**.

6 Type a name for the virtual machine, specify the location of the directory for the virtual machine files, and then click **Next**.

7 Select an encryption type, enter a password for the encryption, and then click **Next**.

You can choose to encrypt all the files, or only the minimum needed files to support the vTPM device.

Note You can specify a password of your choice or select the **Generate** option to automatically generate a password. To copy the password to the clipboard, click **Copy**. You can also select the option to remember the encryption password. For a Windows host operating system, Microsoft Credential Manager stores the password. For a Linux host operating system, GNOME libsecret library stores the password.

8 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 firmware type, virtual machine processors, memory allocation, networking configuration, I/O controller types, virtual disk type and mode, and virtual disk.

Note For the firmware type, if you select UEFI and if the guest operating system supports UEFI Secure Boot, you can select the option to enable UEFI Secure Boot.

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

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

10 (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.

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

Results

The virtual machine appears in the library.

What to do next

Workstation Pro creates the new virtual machine and user can install the operating system by following the installation instructions.

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 Pro supports physical disks up to 2 TB 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.

Create a Virtual Machine Shortcut

You can use a shortcut to select a virtual machine from your desktop.

Prerequisites

A virtual machine must be present in the Workstation Pro Virtual Machine Library.

This feature is available on Windows host systems only.

Procedure

1. Select a virtual machine from the virtual machine library.
2. Drag the virtual machine to the host desktop or to a folder.

   A shortcut is created for the virtual machine.

Results

You can select the virtual machine by double-clicking the shortcut.

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.

What to read next

- 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.

- 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.

- 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.

- 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.

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 remote virtual machine.

Prerequisites

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

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 and Using Linked Clones.

- 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.
- 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 Pro 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.

Results

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

Importing Virtual Machines

You can import virtual machines in other formats into Workstation Pro.

Import an Open Virtualization Format Virtual Machine

You can import an Open Virtualization Format (OVF) virtual machine and run it in Workstation Pro. Workstation Pro 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 Pro. You can import OVF 1.x 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 Pro 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 Pro, 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 Pro performs OVF specification conformance and virtual hardware compliance checks. A status bar indicates the progress of the import process.

   Note You must use the graphical user interface to import an OVF virtual machine file with vTPM placeholder. You cannot import such OVF files using the OVF tool command line. If the OVF file contains a vTPM device placeholder, the option **Choose Encryption Type** appears.
4. If the **Choose Encryption Type** option appears, choose an encryption option, enter a password, and then click **Continue**.
5. If the import fails, click **Retry** to try again, or click **Cancel** to cancel the import.

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

Results

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

Note If the OVF file contains a vTPM placeholder, Workstation Pro adds the vTPM device to the virtual machine after it is encrypted.

Import a VMware vCenter Server Appliance

You can import a VMware vCenter® Server Appliance™ and run it in Workstation Pro. You can import both `.ovf` and `.ova` files.

Procedure

1. In Workstation Pro, select **File > Open**.
2. Browse to the vCenter Server Appliance `.ovf` or `.ova` file and click **Open**.
3. Select the license agreement check box and click **Next**.
4. Continue through the wizard, responding to prompts and clicking through to the next dialog box.
5. If the import fails, click **Retry** to try again, or click **Cancel** to cancel the import.

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

Results

After Workstation Pro successfully imports the vCenter Server Appliance as a virtual machine, the virtual machine appears in the virtual machine library. Workstation Pro then powers on the virtual machine and applies the vCenter Server Appliance configuration.

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 Pro that you are using. Other compatibility options are also available.

For more information about using VMware Tools, see *Installing and Configuring VMware Tools* at http://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf.

What to read next

- Installing VMware Tools

  Installing VMware Tools is part of the process of creating a new virtual machine, and upgrading VMware Tools is part of the process of keeping your virtual machine up to current standards. Although your guest operating systems can run without VMware Tools, many VMware features are not available until you install VMware Tools. When you install VMware Tools, the utilities in the suite enhance the performance of the guest operating system in your virtual machine and improve the management of your virtual machines.

- 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.

- Configure Automatic Software Updates

  You can configure Workstation Pro to automatically download software updates, including new versions of VMware Tools. When automatic software updates are enabled, Workstation Pro 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

  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

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

- Starting 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. This program implements the fit-guest-to-window and other features.

- Uninstalling VMware Tools

  If the upgrade process of VMware Tools is incomplete, you can uninstall and then reinstall the VMware Tools.

Installing VMware Tools

Installing VMware Tools is part of the process of creating a new virtual machine, and upgrading VMware Tools is part of the process of keeping your virtual machine up to current standards. Although your guest operating systems can run without VMware Tools, many VMware features are not available until you install VMware Tools. When you install VMware Tools, the utilities in the suite enhance the performance of the guest operating system in your virtual machine and improve the management of your virtual machines.

For information about creating virtual machines, see the documentation for the applicable VMware product.

The installers for VMware Tools are ISO image files. The CD-ROM in your guest operating system detects the ISO image file. Each type of guest operating system, including Windows, Linux, and Mac OS X, 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.

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 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.

- VMware Tools installer from `windows.iso` automatically detects the windows version. It does not proceed with the installation on guest operating systems earlier than Windows Vista.
- VMware Tools installer from `winPreVista.iso` does not proceed with the installation on Windows Vista and later.
- VMware Tools installer from `linux.iso` does not proceed with installation on Linux guest operating system versions earlier than RHEL5, SLES 11, Ubuntu 10.04, and other Linux distributions with `glibc` version earlier than 2.5.
- VMware Tools installer from `darwinPre15.iso` does not proceed with installation on MAC OS X guest operating systems versions 10.11 or later.
- VMware Tools installer from `darwin.iso` does not proceed with installation on MAC OS X guest operating systems versions earlier than 10.11.

The installation procedure varies, depending on the operating system. For information about installing or upgrading VMware Tools on your guest operating systems, see the topic about upgrading virtual machines in the *Virtual Machine Administration Guide*. For general instructions about installing VMware Tools, see the VMware Knowledge base article http://kb.vmware.com/kb/1014294.

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 your virtual machine displays a message when a new version is available.

For vSphere virtual machines,

```
A newer version of Tools is available for this VM
```

is displayed when the installed version of VMware Tools is out of date.

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. The procedure is mentioned below.

Note Upgrading VMware Tools on Windows guest operation systems automatically installs the WDDM graphics drivers. The WDDM graphics driver allows the sleep mode available in guest OS power settings to adjust the sleep options. For example, you can use the sleep mode setting **Change when the computer sleeps** to configure your guest OS to automatically go to sleep mode after a certain time or prevent your guest OS from automatically switching to sleep mode after being idle for some time.

Some features in a particular release of a VMware product might depend on installing or upgrading to the version of VMware Tools included in that release. Upgrading to the latest version of VMware Tools is not always necessary. Newer versions of VMware Tools are compatible with several host versions. To avoid unnecessary upgrades, evaluate whether the added features and capabilities are necessary for your environment.

Configure Automatic Software Updates

You can configure Workstation Pro to automatically download software updates, including new versions of VMware Tools. When automatic software updates are enabled, Workstation Pro 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 deactivated.

Option	Description
Check for product updates on startup	When Workstation Pro 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 Pro 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 Pro 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 user name and password to use for proxy server authentication. If you leave either the **Username** or **Password** text box blank, Workstation Pro 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 user name and password to use for proxy server authentication. If you leave either the **Username** or **Password** text box blank, Workstation Pro does not use either value (Windows hosts) or it uses the user name 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.

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 Pro preferences. **Note** You cannot configure this option for a 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* at http://www.vmware.com/pdf/vmware-tools-installation-configuration.pdfor more information.

What to read next

- Manually Install VMware Tools on Windows

  You can manually install VMware Tools on a windows virtual machine. The Guest operating systems that support VMware Tools are Windows 2000 and earlier, Windows XP, Windows Server 2003, Windows Vista and later versions.

- Manually Install VMware Tools on Linux

  You can manually install VMware Tools on a Linux virtual machine using the command line. For later Linux distributions, use the integrated open-vm-tools version.

- Manually Installing VMware Tools on a NetWare Virtual Machine

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

- Manually Installing VMware Tools on a Solaris Virtual Machine

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

- Manually Installing VMware Tools on a FreeBSD Virtual Machine

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

Manually Install VMware Tools on Windows

You can manually install VMware Tools on a windows virtual machine. The Guest operating systems that support VMware Tools are Windows 2000 and earlier, Windows XP, Windows Server 2003, Windows Vista and later versions.

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 is detected as a physical CD by 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 later than these, you must log in as an administrator.
- The AppDefense component is not installed by default. You must perform a custom installation and include that component.

Procedure

1. On the host, from the Workstation Pro 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 on the guest operating system, the VMware Tools installation wizard starts.

   To launch the wizard manually if autorun is not enabled, click **Start > Run** and enter **`D:\setup.exe`**, where **`D:`** is your first virtual CD-ROM drive. Use **`D:\setup64.exe`** for 64-bit Windows guest operating system.

3. Follow the on-screen prompts.

4. If the New Hardware wizard appears, follow the prompts and accept the defaults.

   Note 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.

5. When prompted, reboot the virtual machine.

Results

What to do next

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

Manually Install VMware Tools on Linux

You can manually install VMware Tools on a Linux virtual machine using the command line. For later Linux distributions, use the integrated open-vm-tools version.

For more information about Linux distributions supported by Open VM Tools, see Open VM Tools (README) and the VMware Compatibility Guide at https://www.vmware.com/resources/compatibility/search.php.

VMware Tar Tool for Linux virtual machine is feature-frozen at version 10.3.10, so the tar tools (linux.iso) included in Workstation Pro is 10.3.10 and will not be updated. Due to this change, the **Install/Update/Reinstall VMware Tools** menu is not available for the following Linux virtual machines:

- Modern Linux distributions not officially supported by tar tools.
  - Red Hat Enterprise Linux 8 and later releases.
  - CentOS 8 and later releases.
  - Oracle Linux 8 and later releases.
  - SUSE Linux Enterprise 15 and later releases.
- Linux kernel version is 4.0 or later, and the version of the installed Open VM Tools is 10.0.0 or later.
- Linux kernel version is 3.10 or later, and the version of the installed Open VM Tools is 10.3.0 or later.

For the Linux virtual machines that have Open VM Tools installed but are not in the scope mentioned in the preceding bullet, **Install/Update/Reinstall VMware Tools** menu is enabled, so that you can install bundled tar tools on top of Open VM Tools to get Shared Folder (HGFS) feature support.

For old Linux virtual machines not supported by Open VM Tools, perform the following steps to install tar tools.

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 Pro 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, open a terminal window. 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 in a manner similar to the following output:

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

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.

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

```
cd /tmp
```

4 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`.

List the contents of the mount point directory and note the file name of the VMware Tools tar installer.

```
ls mount-point
```

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.

5 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.

6 Run the installer and configure VMware Tools as a root user

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

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

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.

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

Note For newer Linux distributions, users are prompted to choose the integrated open-vm-tools.

What to do next

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

Manually Installing VMware Tools on a NetWare Virtual Machine

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

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.

Note VMware Tools 10.1.0 does not support the NetWare operating system.

Procedure

1 On the host, from the Workstation Pro 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**.

What to do next

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

Manually Installing VMware Tools on a Solaris Virtual Machine

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

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 Pro 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.

Results

What to do next

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

Manually Installing VMware Tools on a FreeBSD Virtual Machine

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

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 Pro 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.gz` 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.

Results

What to do next

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

Starting 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. This program implements the fit-guest-to-window and other features.

Normally, this process starts after you configure VMware Tools, log out of the desktop environment, and log back in. You can invoke the VMware user process by running the `vmtoolsd -n vmusr` command. 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 `vmtoolsd -n vmusr` 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 `vmtoolsd -n vmusr` command.

Uninstalling VMware Tools

If the upgrade process of VMware Tools is incomplete, you can uninstall and then reinstall the VMware Tools.

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, 8.1, or Windows 10	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	Log in as root and enter **`vmware-uninstall-tools.pl`** in a terminal window.
Mac OS X, OS X, or macOS	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 Pro 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 3-8. 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 Pro on a Linux host, this file might have a .cfg extension.
.log	*vmname*.log or 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 or 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. 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. 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. 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. **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. 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 Pro 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.

Table 3-8. Virtual Machine Files (continued)

Extension	File Name	Description
.vmsd	*vmname*.vmsd	A centralized file for storing information and metadata about snapshots. It is stored in the working directory.
.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. 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

4

When you use virtual machines in Workstation Pro, you can transfer files and text between virtual machines and the host system, 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 Pro to interact with remote virtual machines. See Chapter 9 Using Remote Connections to Manage Remote Virtual Machines for more information.

Read the following topics next:

- Scan for Virtual Machines to Add to the Virtual Machine Library
- Starting Virtual Machines
- Stopping Virtual Machines
- Transferring Files and Text
- Using Removable Devices in Virtual Machines
- Changing the Virtual Machine Display
- Using Folders to Manage Virtual Machines
- Taking Snapshots of Virtual Machines
- Install New Software in a Virtual Machine
- Take a Screenshot of a Virtual Machine
- Delete a Virtual Machine

Scan for Virtual Machines to Add to the Virtual Machine Library

You can quickly add multiple virtual machines to the virtual machine library by initiating a scan.

You can manually select and add virtual machines to the virtual machine library. Alternatively, you can initiate a scan that locates virtual machines in a folder, removable storage device, or hard disk of your choice. In the context of a scan, files with the `.vmx` extension are considered virtual machines.

Procedure

1 Select **File > Scan for Virtual Machines**.

2 In the **Select a location to scan** text box, enter or browse for a location, such as a folder, removable storage device, or hard disk.

3 Click **Next**.

4 (Optional) If Workstation Pro is scanning the location for virtual machines, but the scan is taking too long, click **Stop Scan**.

5 Select the virtual machines to add and the library node in which to add them.

a Select the virtual machines.

Option	Description
To select individual virtual machines	Click **Unselect All** and select the check boxes next to the virtual machines that you want to add to the library.
To select all virtual machines	If not selected, click **Select All**.

b (Optional) To use the same folder hierarchy in the library, click **Match the file system folder hierarchy in the library**.

c To continue, click the appropriate option, depending on which option is available.

Option	Description
Finish	If the scan location is on the local machine, the **Finish** option is available.
Next	If the scan location is on a remote server or removable storage device, the **Next** option is available.

d If the location of the virtual machines you are adding to the library is on a remote server or a removable storage device, select the options in the **Copy to local disk options** dialog box that meet your needs and click **Finish**.

Option	Description
Copy all selected virtual machines to	Select this option to copy the selected virtual machines to your local machine. If you do not select this option, the virtual machines remain on the remote server or removable storage device.
Browse	If you select the copy virtual machine option and you do not want to accept the default virtual machine location, you can browse to a location in which to copy the virtual machines.
Keep the hierarchy of the folder in target location	If you select the copy virtual machine option, you can select this option to use the same folder hierarchy used in the remote server or removable storage device in the target location on your local machine.

e Review the progress and results of the operation on the **Result** dialog box and click the appropriate options.

Option	Description
Stop	If the process is taking too long, click **Stop** to cancel the operation.
Close	Click **Close** to close the **Result** dialog box.

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 Pro to start virtual machines on the host system and on remote servers.

To start a virtual machine from the command line, use the `vmware` command. See Chapter 17 Using the vmware Command.

What to read next

- 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.

- Start a Virtual Machine That Is Running in the Background

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

- 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.

- Configure a Firmware Type

  You can select the firmware type for a virtual machine.

- Enable Auto Start for Local Virtual Machine on Windows Host

  You can use the Auto Start feature available in VMware Workstation Pro to automatically power on the local virtual machines when the Windows host machine boots up.

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.

You can use the AutoStart feature to configure remote virtual machines to start when the host system starts. See Manage Virtual Machine Power Actions on Remote Hosts.

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.

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 Pro starts the virtual machine.
Start Up Guest	(Soft option) Workstation Pro 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 firmware	Workstation Pro 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 Pro 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 Pro is not started.

Prerequisites

Set the virtual machine to run in the background. See Closing Virtual Machines and Exiting Workstation Pro.

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

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.

Configure a Firmware Type

You can select the firmware type for a virtual machine.

You can change your firmware type of a virtual machine after you create the virtual machine.

Prerequisites

- To change the firmware type of an existing virtual machine, the guest operating system is powered off.
- The software to boot the system is installed.
- If you want to select Unified Extensible Firmware Interface (UEFI) as the firmware type, verify that the following conditions are met:
  - The guest operating system to be installed on the virtual machine supports UEFI firmware.
  - The virtual machine does not have virtualization-based security (VBS) enabled.
  - The virtual machine uses hardware version 8 or later.
  - The virtual machine has a Windows 8, Windows 10, Windows 2012, or Windows 2016 guest operating system.
- If you want to select UEFI Secure Boot, verify that the following conditions are met.
  - The virtual machine uses the UEFI firmware type.
  - The virtual machine uses hardware version 14 or later.

Procedure

1 In the Workstation Pro interface, select **VM > Settings**.

2 Click the **Options** tab and click **Advanced**.

3 In the Firmware type section, make your firmware selections.

If the guest operating system is supported and the prerequisites are met, the following firmware types are selectable.

Option	Description
UEFI	UEFI is an interface between the operating system and the platform firmware. UEFI has architectural advantages over Basic Input/Output System (BIOS) firmware.
Legacy BIOS	Standard BIOS firmware.

Note

- Once a guest operating system is installed, changing the firmware type might cause the virtual machine boot process to fail.
- If you select UEFI, depending on the guest operating system, you might have the option of enabling UEFI Secure Boot. UEFI Secure Boot secures the boot process by preventing the loading of drivers and operating system loaders that are not signed with an acceptable digital signature.
- If VBS is enabled, the firmware type is set to UEFI and the UEFI Secure Boot option is selected.
- You cannot edit the firmware type or the UEFI Secure Boot setting when VBS is enabled.

4 Click **OK**.

Results

When you start the virtual machine, it boots with the selected firmware configuration.

Enable Auto Start for Local Virtual Machine on Windows Host

You can use the Auto Start feature available in VMware Workstation Pro to automatically power on the local virtual machines when the Windows host machine boots up.

VMware Workstation Pro installs a new Windows service named **VMware Autostart Service** for the Auto Start feature. You must configure this service to start automatically if you want to use the feature.

You can choose the virtual machines for Auto Start from the Workstation UI.

Prerequisites

- Ensure that you have installed VMware Workstation Pro 17.0 or later.

Procedure

1 To configure **VMware Autostart Service** to **Automatic** start type, perform the following steps:

   a Click **Start** > **Run**.

   b Type **services.msc**, and then press **Enter**.

   c From the service list, right click **VMware Autostart Service**, and then click **Properties**.

   d On the **General** tab of the **VMware Autostart Service Properties** dialog box, select the **Startup type** as **Automatic**, and then click **OK**.

   Note You can configure the user account with which you want to run the **VMware Autostart Service**. To change the login information, on the **Log On** tab of the **VMware Autostart Service Properties** dialog box, select **This account**, and specify the required credentials. By default, the service is configured to run with **LocalSystem** account, so changing the account information is recommended.

   The user you specify must have the following rights:

   - Write access to the `vmAutoStart.xml` file located in `%ALLUSERSPROFILE%\VMware\VMware Workstation\vmAutoStart.xml`.
   - Ownership to the `VMX` files specified in the `vmAutoStart.xml` file.

2 Launch VMware Workstation Pro.

3 On the VMware Workstation Pro user interface, right-click **My Computer**, and then select **Configure Auto Start VMs**.

4 On the **Configure VM Power Actions** dialog box, select the **Auto Start** check boxes and modify the **Start Order** fields for the virtual machines you want to autostart.

   The virtual machines are started in the sequence as per the **Start Order**.

   Note Same value of the **Start Order** for more than one VM still starts the VMs sequentially but the power-on sequence for those VMs is undefined.

5 Click **OK**.

   Note You cannot configure Auto Start for an encrypted VM.

Stopping Virtual Machines

You can use Workstation Pro 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

  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 Pro

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

- 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.

- Suspend and Resume a Virtual Machine

  Use the suspend and resume feature to save the current state of a virtual machine. When you resume the virtual machine, the applications that were running before the suspension will resume their running state with their content 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 Pro. You can exit Workstation Pro and leave the virtual machine running in the background. See Closing Virtual Machines and Exiting Workstation Pro.

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

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 Pro powers off the virtual machine abruptly with no consideration for work in progress.
Shut Down Guest	(Soft option) Workstation Pro 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 shut-down signal from Workstation Pro. 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 Pro 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 Pro

You can close a virtual machine that is running on the local host system without powering it off. By default, Workstation Pro prompts you to select an action when you close a powered-on virtual machine and when you exit Workstation Pro 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 4-1. 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. 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 Pro powers off the virtual machine abruptly. The effect is the same as using the power button on a physical machine.

You can configure Workstation Pro 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 Pro 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.

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 Pro 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

Use the suspend and resume feature to save the current state of a virtual machine. When you resume the virtual machine, the applications that were running before the suspension will resume their running state with their content unchanged.

How quickly the suspend operation performs depends on the how much data changed after you started the virtual machine. The first suspend operation usually takes longer than subsequent suspend operations. When you suspend a virtual machine, Workstation Pro creates a virtual machine suspended state (.vmss or .vmem) file set in the working directory. How quickly the resume operation performs depends on how active the virtual machine is. The more active the virtual machine is, the longer it will take to resume. It also depends on whether the virtual machine suspended state (.vmss or .vmem) file set is already in the physical memory of the host system. If it is, the virtual machine will resume much faster.

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.

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 Pro suspends the virtual machine and leaves it connected to the network.
Suspend Guest	(Soft option) Workstation Pro 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 Pro 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 Pro resumes the virtual machine from the suspended state.
Resume Guest	(Soft option) Workstation Pro 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 Pro 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 Pro 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 Pro as suspend. You can use the Workstation Pro **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

  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.

- Using the Copy and Paste Feature

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

- 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.

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.

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 Pro 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 4 MB.
- Dragging plain text and formatted text (including the formatting) is restricted to amounts less than 4 MB.
- Dragging text is restricted to text in languages that can be represented by Unicode characters.

- Workstation Pro uses the PNG format to encode images that are dragged. Dragging images is restricted to images smaller than 4 MB after conversion to PNG format.

Turn Off the Drag-and-Drop Feature

The drag-and-drop feature is turned on by default when you create a virtual machine in Workstation Pro. To prevent dragging and dropping between a virtual machine and the host system, turn off the drag-and-drop feature.

Note You cannot enable or turn off the drag-and-drop feature for a 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.

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 4 MB.
- 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 Pro uses the PNG format to encode images that are copied and pasted. Copying and pasting images is restricted to images smaller than 4 MB after conversion to PNG format.
- You cannot copy and paste files between virtual machines.

Turn Off the Copy and Paste Feature

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

Note You cannot turn on or off the copy and paste feature for a 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.

What to read next

- Guest Operating Systems That Support Shared Folders

  To use shared folders, a virtual machine must have a supported guest operating system.
- 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.
- 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 deactivated by default. This is a security precaution.
- View Shared Folders in a Windows Guest

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

  After you enable 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

  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

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

- Turn Off Folder Sharing for a Virtual Machine

  You can turn off 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 R2
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Vista
- Windows 7
- Windows 8
- Windows 10
- 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 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.
- 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 Pro 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 Pro 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 Browse to, or 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 Pro always attempts to use that path. If the directory is later connected to the host on a different drive letter, Workstation Pro cannot locate the shared folder.

7 Specify the name of the shared folder as it should appear inside the virtual machine and click **Next**.

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 turn off the shared folder option 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 turn off 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.

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 deactivated by default. This is a security precaution.

Folder sharing is also deactivated by default for Workstation 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 enable 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`.

Depending on the kernel version of the Linux guest operating system, VMware Tools uses different components to provide shared-folder functionality. In Linux kernels prior to version 4.0, the VMware Tools services script loads a driver that performs the mount. Linux kernels 4.0 and later use a FUSE file system component.

You can use different mount commands to mount all shares, one share, or a subdirectory within a share to any location in the file system. The commands also vary depending on the Linux-kernel version of the guest.

Table 4-2. Mount Command Syntax

Linux Kernel Prior to 4.0	Linux Kernel 4.0 and Later	Description
`mount -t vmhgfs .host:/ /home/user1/shares`	`/usr/bin/vmhgfs-fuse .host:/ /home/user1/shares -o subtype=vmhgfs-fuse,allow_other`	Mounts all shares to `/home/user1/shares`
`mount -t vmhgfs .host:/foo /tmp/foo`	`/usr/bin/vmhgfs-fuse .host:/foo /tmp/foo -o subtype=vmhgfs-fuse,allow_other`	Mounts the share named `foo` to `/tmp/foo`
`mount -t vmhgfs .host:/foo/bar /var/lib/bar`	`/usr/bin/vmhgfs-fuse .host:/foo/bar /var/lib/bar -o subtype=vmhgfs-fuse,allow_other`	Mounts the subdirectory `bar` within the share `foo` to `/var/lib/bar`

For Linux kernel prior to version 4.0, you can use VMware-specific options in addition to the standard `mount` syntax. Enter the command `/sbin/mount.vmhgfs -h` to list the options.

For Linux kernel version 4.0 or later, enter the command `/usr/bin/vmhgfs-fuse -h` to list the available options.

Note The mount can fail if shared folders are not enabled 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 Pro, or a previous release of the Linux version of Workstation Pro, 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.

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 Pro always attempts to use that path. If the directory is later connected to the host on a different drive letter, Workstation Pro 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 deactivate 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 deactivate share.

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

Turn Off Folder Sharing for a Virtual Machine

You can turn off 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 turn off folder sharing.

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

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 Pro handles USB devices. See Connecting USB Devices to Virtual Machines.

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

Workstation Pro responds differently when you plug a USB device into a Windows host or a Linux host.

On a Windows host, by default, unless Workstation Pro is currently configured to remember a connection rule for a specific USB device, when you plug the USB device into the host system, Workstation Pro prompts you to select a machine to connect the device to. Workstation Pro connects the device to the machine you select, but a remember option is also available, which creates a USB device connection rule that, in the future, directs Workstation Pro to either automatically connect that device to the host or to a virtual machine, depending on the machine you selected.

On a Linux host, 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.

Also, on a Linux host, when you connect a USB device to a virtual machine, Workstation Pro 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 Pro reconnects the device. Workstation Pro retains the connection by writing an autoconnect entry to the virtual machine configuration (`.vmx`) file. If Workstation Pro cannot reconnect to the device, for example, because you disconnected the device, the device is removed and Workstation Pro displays a message to indicate that it cannot connect to the device. If the device is still available, you can connect to it manually. To connect a USB device to the virtual machine manually, select **VM > Removable Devices > *Device Name* > Connect (Disconnect from host)**

Follow the device manufacturer's procedures for unplugging the device from the host computer when you physically unplug the device, move the device from the host system to a virtual machine, 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.

What to read next

- 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.
- Configure USB Device Connection Behavior
- Select the Machine a USB Device Connects To
- Delete the Connection Rule for a Specific USB Device
- Turn Off Automatic Connection of USB Devices
- 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.
- 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.

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.

Configure USB Device Connection Behavior

This feature is only available for Workstation Pro on a Windows host. When you plug a new USB device into your Windows host machine, Workstation Pro responds according to the USB Connections setting, which you can configure.

The default setting for the USB Connections setting is **Ask me what to do**. You can change the setting to suit your needs.

Procedure

1 Select **Edit > Preferences > USB**.

2 Select one of the options and click **OK**.

- **Ask me what to do**
- **Connect the device to the host**
- **Connect the device to the foreground virtual machine**

Results

Selected Option	Result When You Plug a New USB Device into the Host
Ask me what to do	If Workstation Pro is open and one or more virtual machines is powered on, a dialog box appears that prompts you to choose which machine to connect the device to. You can choose the host or one of the powered-on virtual machines.
Connect the device to the host	Workstation Pro always connects new USB devices to the host machine regardless of whether a virtual machine is running.
Connect the device to the foreground virtual machine	If Workstation Pro is open and one or more virtual machines is powered on, Workstation Pro connects the device to the powered-on virtual machine in the foreground.

What to do next

Plug a USB device into the Windows host machine. If the **Ask me what to do** option is configured, when you plug in a device, you must respond to the New USB Device Detected dialog box. See Select the Machine a USB Device Connects To. Access the USB device from the machine you selected.

You can manually connect a USB device to the virtual machine by selecting **VM > Removable Devices > *Device Name* > Connect (Disconnect from host)**

Select the Machine a USB Device Connects To

This feature is only available for Workstation Pro on a Windows host. If the USB Connections setting is set to **Ask me what to do**, when you plug a new USB device into the Windows host, the New USB Device Detected dialog box appears. You can connect the USB device to the host or one of the powered-on virtual machines.

A USB device is treated as new when Workstation Pro does not have a remembered connection rule for the USB device. A connection rule is remembered when you select **Remember my choice and do not ask again**, and stays remembered until you configure Workstation Pro to forget the rule.

Prerequisites

1 Set the USB Connections setting to **Ask me what to do**. See Configure USB Device Connection Behavior.

2 Plug a new USB device into the Windows host machine.

Procedure

1 Select the machine to connect the USB device to.

Option	Description
Connect to host	The device connects to the Windows host machine.
Connect to a virtual machine	The device connects to the powered-on virtual machine of your choice. Select a virtual machine in the list.

2 (Optional) If you want Workstation Pro to remember your machine selection, select **Remember my choice and do not ask again**.

This option creates a connection rule between the specific USB device and the specific machine.

3 Click **OK**.

Results

Workstation Pro connects the USB device to the machine you selected. If you selected **Remember my choice and do not ask again**, in the future, when you connect the USB device to the Windows host machine, Workstation Pro implements the connection rule and connects the device to the machine you configured without prompting. However, if the target virtual machine of the connection rule is powered off or deleted at the time the device is plugged into the host, the USB device automatically connects to the host. Anytime in the future, you can delete the connection rule. After which, Workstation Pro treats the USB device as new again. See Delete the Connection Rule for a Specific USB Device.

What to do next

Access the USB device from the machine you configured.

Delete the Connection Rule for a Specific USB Device

This feature is only available for Workstation Pro on a Windows host. If you created a connection rule for a USB device to a specific virtual machine or to the host machine, you can delete the connection rule.

Selecting **Remember my choice and do not ask again** in the New USB Device Detected dialog box creates a connection rule. See Select the Machine a USB Device Connects To. If you no longer want a specified USB device to connect to a specified machine, delete the connection rule by configuring Workstation Pro to forget the rule.

Procedure

- Use one of the following methods to delete the connection rule.
  - Select the virtual machine and select **VM > Removable Devices > *Device Name* > Forget Connection Rule**.

- Right-click the icon of the USB device in the Workstation Pro status bar and select **Forget Connection Rule**.

Results

Workstation Pro is no longer configured to remember the rule. When you plug a USB device into the Windows host, the device no longer automatically connects to the virtual machine. Instead, the New USB Device Detected dialog box appears.

Turn Off Automatic Connection of USB Devices

This feature is only available for Workstation Pro on a Linux host. You can turn off the autoconnect feature if you do not want USB devices to connect to a virtual machine when you plug the devices into the host machine.

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 turn off automatic connection of USB devices.
4. Click **OK** to save your changes.

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 remote virtual machine to show all USB input devices.

Prerequisites

- Power off the virtual machine.
- This prerequisite only applies to Workstation Pro on a Linux host. If you are using a KVM switch for a mouse or keyboard, turn off automatic connection of USB devices. See Turn Off Automatic Connection of USB Devices.

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.

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, deactivate 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 deactivate the driver or unload the driver manually.

Option	Description
Disable the driver	If the driver was automatically loaded by hotplug, deactivate 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 Pro. 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

- 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 not available.
- 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.

Turn Off 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 turn off 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 Pro global configuration file.

Procedure

1 Find the global configuration file on the host system.

Operating System	Location
Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows 7, Windows 8, Windows 10 hosts	`%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 Pro preference setting.

  Workstation Pro creates the global configuration file when you change Workstation Pro 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 Pro 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 Pro.

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 Pro 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 Pro 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.

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

What to read next

- Use Full Screen Mode

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

- Use Exclusive Mode

  Like full screen mode, exclusive mode causes the Workstation Pro 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

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

- 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.

- Use Multiple Monitors for Multiple Virtual Machines

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

- Fit the Workstation Pro Console to the Guest Operating System Display

  You can control the size of the virtual machine display and match the Workstation Pro 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 Pro 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.

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 Pro 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 Pro 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 Pro window onto the monitor to use for exclusive mode.
- Enter full screen mode. See Use Full Screen Mode .

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 Windows XP 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 latest version of VMware Tools is installed in the guest operating system.
- Verify that the guest operating system is Windows XP or later.
- 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 Pro 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 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**.

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 Windows or Linux guest operating system is supported.

Procedure

1. Select the virtual machine and select **View > Autosize > Autofit Guest** to verify that the virtual machine can resize correctly.
2. Power on the virtual machine and select **View > Full Screen**.
3. On the full screen toolbar, click the **Cycle Multiple Monitors** button.

   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.
4. (Optional) Click the **Cycle Multiple Monitors** button again if the host system has more than two monitors and you want the virtual machine to use all of the monitors.

   The order in which the virtual machine uses the monitors depends on the order in which the monitors were added to the host operating system. If you continue to click the button, you return to fewer monitors.

Limitations for Multiple 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 Pro window.

Option	Description
Open a new window from Workstation Pro	Select **File > New Window**. On Linux hosts, the windows operate in a single Workstation Pro process.
(Linux hosts only) Run a separate Workstation Pro 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 Pro window.

3 Drag each Workstation Pro window to the monitor on which you want to use it.

If a virtual machine is running in one Workstation Pro window and you want to run that virtual machine in another Workstation Pro 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 pointer from one screen to the other screen and click inside the second monitor.

Fit the Workstation Pro Console to the Guest Operating System Display

You can control the size of the virtual machine display and match the Workstation Pro 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.
- For a Solaris virtual machine, familiarize yourself with the considerations for resizing displays. See Considerations for Resizing Displays in Solaris Virtual Machines.

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 Pro console.
Center Guest	The virtual machine centers the guest display in the full screen. The guest display resolution is not changed.
Autofit Window	The Workstation Pro console maintains the size of the virtual machine display resolution. If the guest operating system changes its resolution, the Workstation Pro 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 Pro 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 Pro console.
Stretch Guest	This option is available on Linux host only. The virtual machine changes the guest display to fit the full screen. The guest display resolution is not changed.

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 Pro 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 Pro 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

  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

  You can remove a virtual machine from a folder or move it to a different folder or subfolder.

- 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.

- Change the Power On Delay

  By default, when you power on several virtual machines in a folder, Workstation Pro 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 Pro preference.

- Convert a Team

  If you created a team in an earlier version, you must convert the team before you can use the virtual machines in the current version of Workstation Pro.

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 Pro delays 10 seconds before powering on the next virtual machine by default. Workstation Pro 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 Pro preference. See Change the Power On Delay.

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 Pro 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 Pro 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 Pro 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, you must convert the team before you can use the virtual machines in the current version of Workstation Pro.

Procedure

1. Open the team in Workstation Pro 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.

Results

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 Pro 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

  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

  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

  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

  You can restore a virtual machine to a previous state by reverting to a snapshot.

- 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.

- 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.

- Enable Background Snapshots

  When you enable background snapshots, you can continue working while Workstation Pro preserves the state of a virtual machine. A progress indicator for the background snapshot appears in a corner of the Workstation Pro window.

- Exclude a Virtual Disk from Snapshots

  You can configure snapshots so that Workstation Pro preserves states only for certain virtual disks.

- 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.

- Troubleshooting Snapshot Problems

  You can use a variety of procedures for diagnosing and fixing problems with snapshots.

Using Snapshots to Preserve Virtual Machine States

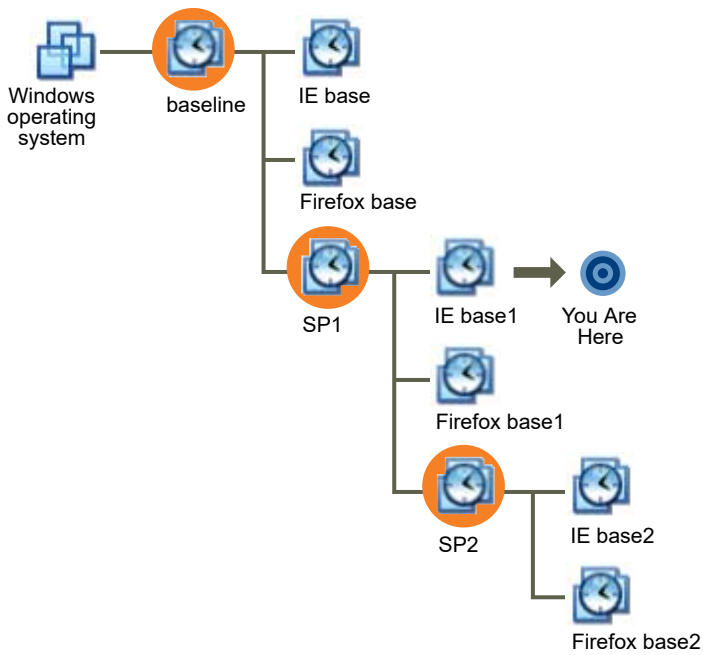
A snapshot includes the contents of the virtual machine memory, virtual machine settings, and the state of all the virtual disks. When you revert to a snapshot, you return the memory, settings, and virtual disks of the virtual machine to the state they were in when you took the snapshot.

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 4-1. 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.
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 Pro 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 Workstation Player, even if AutoProtect is enabled for the virtual machine in Workstation Pro.
- You cannot configure the AutoProtect feature for a 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 Pro 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 Pro 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 Pro preserves the state of a virtual machine. A progress indicator for the background snapshot appears in a corner of the Workstation Pro 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, turn off background snapshots.

Prerequisites

On a Linux host, run Workstation Pro 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 Pro 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 Turned Off

The Snapshot Manager **Take Snapshot** option is turned off.

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 turn off background snapshots to improve performance. See Enable Background Snapshots 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.

Deactivate Acceleration if a Program Does Not Run

When you install or run software inside a virtual machine, Workstation Pro 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 deactivate 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

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: ■ Always ask for location ■ Save to Desktop ■ Browse for custom location By default, Workstation Pro 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. 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**.

Running Workstation on a Hyper-V Enabled Host

5

The traditional implementation of Workstation Pro relies on direct access to specific hardware features of the x86 microprocessor.

These features, generally called Intel VT or AMD-V, are also used by recent versions of Windows that support Hyper-V. Also, it is not possible to run traditional Workstation Pro on a Windows host with the Hyper-V capability enabled because some Windows features like the virtualization-based security (or VBS), are built on top of Hyper-V. Therefore, a VBS-enabled Windows host is also incompatible with traditional Workstation Pro.

Note This feature is only available in 15.5.5 version of Workstation Pro.

System Requirements

Processor Requirements for Host System

- Intel Sandy Bridge or newer CPU
- AMD Bulldozer or newer CPU

Supported Host Operating Systems

- Windows 10 20H1 build 19041.264 or newer

Note For all other Windows host versions, Hyper-V must be deactivated for Workstation Pro to power on VMs.

Read the following topics next:

- Host VBS Mode on Workstation
- Host VBS Mode Compatibility with Windows Version
- Limitations of Host VBS Mode
- Limitations in the VMs Suspend/Resume Operation

Host VBS Mode on Workstation

A special mode of operation called Host VBS Mode is introduced so Workstation Pro can work with Windows.

In the Host VBS Mode, Workstation Pro uses a set of newly introduced Windows 10 features (Windows Hypervisor Platform) that permits the use of VT/AMD-V features, which enables Workstation Pro and Hyper-V to coexist. And because VBS is built on Hyper-V, Windows hosts with VBS enabled can now power on VM in Workstation Pro successfully.

Host VBS Mode Compatibility with Windows Version

Host VBS Mode is automatically enabled whenever Workstation Pro is launched on a suitably capable Windows 10 (or later) host with Hyper-V enabled.

If Hyper-V is deactivated, Workstation Pro operates in its traditional mode. And if Hyper-V is enabled, but the WHP feature is not sufficiently recent or not installed, Workstation Pro fails to start.

Note WHP is not supported on the Windows Server editions. Therefore, Workstation Pro host VBS mode is not available on these editions.

Limitations of Host VBS Mode

A Workstation Pro VM running in Host VBS Mode has functional limitations when compared to the VM running in traditional mode.

Depending on the workload, a Host VBS Mode VM can run slower when compared to a VM in traditional mode. The limitations and use overhead introduced by the WHP feature set causes these issues.

Here is a list of functional limitations of a Workstation Pro VM running in Host VBS Mode:

- Nested VMs are not supported:

  x86 virtualization features (Intel VT / AMD-V) are unavailable to a guest running on a Host VBS Mode VM. Therefore such VMs cannot themselves run Windows with Hyper-V or VBS enabled.

- PMCs are not supported:

  x86 performance monitoring counters (PMCs) are unavailable.

- RTM and HLE are not supported:

  Restricted transactional memory and hardware lock elision capabilities are not available.

- PKU is not supported:

  User-mode protection keys capability is not available.

Limitations in the VMs Suspend/Resume Operation

When Resuming a suspended VM or reverting to a snapshot created in power-on or suspend states, Workstation Pro compares the CPU features with which the VM was created against the features actually available to the host environment running Workstation Pro.

If features requested during the VM creation are unavailable on the host environment, the VM resume operation fails. This ensures that a guest does not attempt to use unimplemented features. Because some CPU features are not supported in Host VBS Mode, attempting to resume suspended VMs or snapshots that were initially created on previous versions of Workstation Pro may fail.

For example, consider a physical PC that supports the RTM feature. A VM created with RTM enabled, will power on with RTM available to it, when Workstation Pro is running in traditional mode. However, the same VM running on the same PC will power on with RTM deactivated, if Workstation Pro is in Host VBS Mode. This is because, as previously listed in the functional limitations list, Host VBS Mode does not support RTM.

Now consider a suspended VM which has a particular feature enabled is resumed some time later. If the particular feature is not available on the host environment of the resumed VM, the expected behavior is that the resume operation fails.

Note The resume operation can fail on the same physical hardware, when the VM is suspended while operating in traditional mode and the resumed while in Host VBS Mode.

For example:

1 Create a VM with RTM enabled.

2 Start Workstation Pro with Hyper-V deactivated and power on the VM on a physical hardware that supports RTM.

3 Suspend the VM at some point after it is powered on.

4 Enable Hyper-V. (The physical machine must be rebooted and Workstation Pro must be relaunched.)

5 Resume the suspended VM.

6 The resume operation fails.

Even though the physical hardware is the same, the resume operation fails because RTM is no longer supported in Host VBS Mode.

Note If the VM is launched with Hyper-V enabled, the VM will not have the RTM capability, and so the suspended image created will also be RTM-free. Regardless of whether Hyper-V is deactivated or not, the resume VM operation will succeed.

Configuring and Managing Virtual Machines

6

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 Pro 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).

Read the following topics next:

- Configure Power Options and Power Control Settings
- Configure SSH Login on a Linux Virtual Machine
- Set Workstation Pro Display Preferences
- Configure Display Settings for a Virtual Machine
- Set Preferences for Unity Mode
- Setting Screen Color Depth
- Using Advanced Linux Sound Architecture
- Encrypting Virtual Machines
- Moving Virtual Machines
- Configure a Virtual Machine as a VNC Server
- Change the Hardware Compatibility of a Virtual Machine
- Clean Up a Virtual Hard Disk on Windows Hosts
- Export a Virtual Machine to OVF Format
- Export a Virtual Machine with vTPM to OVF Format on Intel-based Mac
- Writing and Debugging Applications That Run In Virtual Machines

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 17 Using the vmware Command 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 remote virtual machine.

Option	Description
Enter full screen mode after powering on	The virtual machine window enters full screen mode after it is powered on.
Close after powering off or suspending	The virtual machine tab 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 Pro powers off the virtual machine abruptly with no consideration for work in progress.
Shut Down Guest	(Soft option) Workstation Pro 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 shut-down signal from Workstation Pro. 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 Pro suspends the virtual machine and leaves it connected to the network.
Suspend Guest	(Soft option) Workstation Pro 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 remote virtual machine.

Option	Description
Power On	(Hard option) Workstation Pro starts the virtual machine.
Start Up Guest	(Soft option) Workstation Pro 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 Pro resets the virtual machine abruptly with no consideration for work in progress.
Restart Guest	(Soft option) Workstation Pro 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.

Configure SSH Login on a Linux Virtual Machine

With Workstation Pro on a Windows 10, version 1803 or later host, when a Linux virtual machine has an SSH service enabled, you can configure quick SSH login to the virtual machine. The configuration enables SSH login from the host to a Linux virtual machine in the virtual machine library. The virtual machine can be running on the host or on a remote server running Workstation Pro, VMware ESXi, or VMware vCenter Server.

By configuring SSH login, you provide yourself with easy and secure SSH access to the Linux virtual machine now and at anytime in the future. You can then use a terminal window to access the Linux virtual machine, where you can view files, transfer data, and run the commands available on the Linux operating system.

Prerequisites

- Enable SSH on the Linux virtual machine, if not already enabled. See instructions for the specific Linux operating system.
- Add the Linux virtual machine to the virtual machine library, if not already added.

  You can add virtual machines that reside on the host or on a supported remote server.
- Start the Linux virtual machine, if not already started.

Procedure

1. Select the Linux virtual machine and select **VM > SSH > Connect to SSH**.
2. Complete the form and click **Connect**.

Option	Description
Username	Enter the user name of the virtual machine.
Port	If 22, the default SSH service port number, is not correct for the Linux virtual machine you are configuring, enter the correct port number.
Options	You can use this text box to specify additional parameters to pass to the SSH client. For example, if you created an SSH key pair to log in to the virtual machine without a password, you can enter it here.

   A terminal window opens on the host desktop.
3. Enter the password of the virtual machine.

   SSH connects to the virtual machine. During the first connection, Workstation Pro automatically saves the connection information for future connections.

Results

You now have command-line access to the Linux virtual machine.

What to do next

In the future, to open an SSH connection from the host to the Linux virtual machine, in the Workstation Pro virtual machine library, select the Linux virtual machine and select **VM > SSH > Connect to SSH**.

Edit or Delete the SSH Login Configuration for a Linux Virtual Machine

After you configure SSH login on a Linux virtual machine, you can change or delete the configuration.

If any of the following items change, you must change the SSH login configuration.

- Port number for the SSH service
- Your Linux virtual machine user name

You can also delete the SSH login configuration.

Procedure

1. Select the Linux virtual machine and select **VM > SSH > Configure SSH**.
2. Either edit updated options and click **Save** or remove the configuration.

Option	Description
Username	Edit this option if your virtual machine user name changed.
Port	Edit this option if the port number for the SSH service changed.
Options	You can use this text box to specify additional parameters to pass to the SSH client. For example, if you created an SSH key pair to log in to the virtual machine without a password, you can enter it here.
Remove	To delete the SSH login configuration, click this option.

Set Workstation Pro Display Preferences

You can configure Workstation Pro display preferences to control how the display settings of all virtual machines adjust to fit the Workstation Pro window. These adjustments occur when you resize the Workstation Pro 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**.

   If you are using Windows 8.1 (Update 2) or Windows 10, Workstation Pro detects the DPI on each monitor and scales the virtual machine to match the DPI on the host.

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)	This option is available on Linux hosts only. 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.
Use a single button for stretch controls	When this setting is selected, the **Keep Aspect Ratio Stretch** and **Free Stretch** display controls appear on the toolbar as a single button with a drop-down menu. When this setting is deselected, each stretch control appears as a separate button on the toolbar.
Combine toolbar with menu bar in windowed mode	Show the Workstation Pro menus and toolbar on a single bar when Workstation Pro is in windowed mode.
Combine tabs with toolbar in full screen	Show the tabs and toolbar in a single bar when Workstation Pro is in full screen mode.
Show toolbar edge when unpinned in full screen	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.

For Windows guests, to use DirectX 9 accelerated graphics, the guest operating system must be Windows XP or later. To use DirectX 10 accelerated graphics, the guest operating system must be Windows Vista or later. To use DirectX 10.1 or DirectX 11 accelerated graphics, the guest operating system must be Windows 7 or later.

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 or later, or Linux.
- If you plan to use DirectX 9, DirectX 10, DirectX 10.1, or DirectX 11 accelerated graphics, prepare the host system. See Prepare the Host System to Use 3D Accelerated Graphics.
- If the guest operating system is Windows 7 or later and you want Workstation Pro to automatically adjust the virtual machine user interface size, update VMware Tools in the guest to the newest version.
- If you are using Windows 8.1 (Update 2) or Windows 10, Workstation Pro detects the DPI on each monitor and scales the virtual machine to match the DPI on the host.

Procedure

1. Select the virtual machine and select **VM > Settings**.
2. On the **Hardware** tab, select **Display**.
3. (Optional) To run applications that use DirectX 9, DirectX 10, DirectX 10.1 or DirectX 11 accelerated graphics, select **Accelerate 3D graphics**.

4 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 a maximum bounding box width of 7680 and a maximum bounding box height of 4320. The virtual machine uses the number of monitors on the host system. The guest monitors cannot exceed the maximum bounding box that the SVGA driver uses, 7680x4320. 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. **Note** You cannot configure the resolution setting for a remote virtual machine.

5 (Optional) Select the maximum amount of guest memory that can be used for graphics memory using the drop-down menu. The default value of video memory varies by guest OS.

Guest OS	Default	HW Version
Windows 7 and later	1 GB	HW-v18 earlier
Windows XP and earlier	512 MB	HW-v18 earlier
Linux	768 MB	HW-v18 earlier
All OS types	8 GB	HW-v18 and later

Note If you manually edited the `.vmx` file to change the memory size for the virtual machine, the value you entered in the `.vmx` file is displayed, labeled **Custom**.

6 (Optional) Either enable display scaling or set the display stretch ratio for a virtual machine, depending on the option available to you.

Workstation Pro presents the option that the selected guest operating system supports.

Option	Guest Support	Description
Display scaling	Windows 7 or later	To enable the DPI synchronization, select **Automatically adjust user interface size in the virtual machine**.
Display scaling, Stretch mode	All	To allow the virtual machine display to stretch when the virtual machine is in full screen mode or windowed mode, select **Stretch mode** and select one of the stretch options. ■ **Keep aspect ratio stretch** When you adjust the Workstation Pro window, the virtual machine display maintains the user interface aspect ratio. ■ **Free stretch** When you adjust the Workstation Pro window, the virtual machine display stretches to fill the user interface, without maintaining the user interface aspect ratio.

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

Prepare the Host System to Use 3D Accelerated Graphics

You must perform certain preparation tasks on the Windows or Linux host system to use 3D accelerated graphics in a virtual machine.

Prerequisites

- On a Windows host, verify that the host has a video card that supports DirectX 9, DirectX 10, DirectX 10.1, or DirectX 11 and the latest DirectX Runtime required for the DirectX version being used.
- On a Linux host, verify that the host has a video card that supports accelerated OpenGL 2.0 if you are using DirectX 9, or OpenGL 3.3 if you are using DirectX 10 or DirectX 10.1, or OpenGL 4.5 if you are using DirectX 11.

The VMware guest operating system OpenGL driver for Windows and Linux supports the OpenGL 3.3, OpenGL 4.1, and OpenGL 4.3 compatibility profile.

Note You can use Vulkan renderer on a Linux host with Intel, Nvidia, or AMD GPUs. Vulkan renderer provides support for Direct3D 11 (and earlier) and OpenGL 4.3 (and earlier) in the guest.

The Vulkan renderer support is limited to the following GPUs:

- Intel Skylake and later GPUs (for example, Kaby Lake and Ice Lake)
- AMD RDNA/NAVI14 and later GPUs (for example, the Radeon RX/Pro 5300 and 5500 series)

  Note Presently, for AMD GPUs, use the AMDVLK driver. You can download the AMDVLK driver from here: https://github.com/GPUOpen-Drivers/AMDVLK/releases

- Nvidia Turing and later GPUs (for example, the RTX series)

  Note For pre-Turing GPUs, Workstation uses the legacy OpenGL renderer.

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. Intel drivers are available from the Intel Web site.

2 If you have a Windows host system, move the **Hardware Acceleration** slider to the **Full** position.

Option	Description
Windows 7, Windows 8, and Windows 10	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 3D applications work.

  ```
  glxgears
  ```

Prepare a Virtual Machine to Use Accelerated 3D Graphics

You must perform certain preliminary tasks to use accelerated 3D graphics on a virtual machine.

The accelerated 3D graphics feature is enabled by default on Workstation 6.x and later virtual machines.

Prerequisites

- Prepare the host system to use accelerated 3D graphics. See Prepare the Host System to Use 3D Accelerated Graphics.
- If using DirectX 9, verify that the guest operating system is Windows XP or later. DirectX 9 is supported on virtual machines running hardware version 11 or earlier.
- If using DirectX 10, verify that the guest operating system is Windows 7 or later. DirectX 10 is supported on virtual machines running hardware version 12 or later.
- If using DirectX 10.1, verify that the guest operating system is Windows 7 or later. DirectX 10.1 is supported on virtual machines running hardware version 16 or later.
- If using DirectX 11, verify that the guest operating system is Windows 7 or later. DirectX 11 is supported on virtual machines running hardware version 18 or later.
- Verify that the latest version of VMware Tools is installed in the guest operating system.
- Power off the virtual machine. The virtual machine must not be suspended.

Procedure

1. Select the virtual machine and select **VM > Settings**.
2. On the **Hardware** tab, select **Display**.
3. Select **Accelerate 3D graphics**.
4. Configure the virtual machine to use only one monitor.
5. Click **OK** to save your changes.
6. Power on the virtual machine and install the required DirectX EndRuntime version.

   This download is available from the Microsoft Download Center.
7. Install and run your 3D applications.

Set Preferences for Unity Mode

You can set preferences for Unity mode to control whether 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** tab, 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	To help distinguish between the application windows that belong to various virtual machines, use a custom color in window borders. 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 Windows hosts, click **Choose color** to use the color chooser.

4 To control whether the virtual machine **Start** or **Applications** menu is 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 Pro window when you enter Unity mode, edit the Workstation Pro Unity preference setting.

Workstation Pro 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 Pro 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 Virtual Machines

Encrypting a virtual machine secures it from unauthorized use. To decrypt a virtual machine, users must enter the correct encryption password.

When you encrypt a virtual machine, Workstation Pro 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 Pro displays the encrypted virtual machine with a lock icon until you enter the password to open the virtual machine.

You can choose **Remember password** to save the password on local password vault which is Windows Credential Manager for Windows and GNOME libsecret library for Linux. Make sure you record the encryption password. Workstation Pro does not provide a way to retrieve the passwords if you lose them.

Important Make sure you record the encryption password and the restrictions password. Workstation Pro 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.

There are two types of encryptions available. You can choose from the following two types of encryptions:

Fast VM Encryption

Fast encryption refers to the encryption of a minimal set of VM files as follows:

- Ancillary data files such as snapshot/screenshot/NVRAM files. These are encrypted with the key in the configuration file. List of files encrypted- .nvram, .vmsn, .vmss, .vmem
- Partially encrypted VM configuration file.

Full VM Encryption

Full encryption refers to encryption of all VM files as follows:

- Disk file headers. These are encrypted with the key in the configuration file.
- Disk file data. These are encrypted with the key in the configuration file.
- Ancillary data files such as the snapshot/screenshot/NVRAM files. These are encrypted with the key in the configuration file.
- VM configuration file is encrypted with authentication keys.

What to read next

- Virtual Machine Encryption Limitations

  The encryption feature has certain limitations.

- Encrypt a Virtual Machine

  You can encrypt a virtual machine to secure it from unauthorized use.
- Remove Encryption From a Virtual Machine

  You can remove encryption from a virtual machine.
- 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.

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 remote virtual machine.
- You cannot upload an encrypted virtual machine to a remote server.
- You cannot change the encryption state (encrypted/ decrypted) when snapshots exist.

Encrypt a Virtual Machine

You can encrypt a virtual machine to secure it from unauthorized use.

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.

Procedure

1. Select the virtual machine and select **VM > Settings**.
2. On the **Options** tab, select **Access Control**.
3. Click **Encrypt**.
4. Choose the appropriate encryption type.

5 Click **Encrypt**, type 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.

Important Record the encryption password you use. If you forget the password, Workstation Pro does not provide a way to retrieve it. You can select **Remember password** option to save the password to the local password vault.

Workstation Pro begins encrypting the virtual machine.

6 Click **OK** in the Virtual Machine Settings dialog box.

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 Deselect the **Enable restrictions** check box, if it is selected.

You cannot remove encryption from a virtual machine while restrictions are enabled.

4 Click **Remove Encryption**.

5 Type the encryption password.

6 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 primary 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 Pro does not provide a way to retrieve it.

Moving Virtual Machines

You can move a virtual machine that was created in Workstation Pro 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 Pro in Workstation Player.

- Move a Virtual Machine to a New Location or Host

  You can move a virtual machine that was created in Workstation Pro 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.

- Open a Virtual Machine in VMware Workstation Player

  VMware® Workstation Player opens and plays virtual machines created in other VMware products.

- 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.

- 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.

Move a Virtual Machine to a New Location or Host

You can move a virtual machine that was created in Workstation Pro 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 all of the files that make up the virtual machine. All files in the virtual machine's original directory when the virtual machine was created must be moved. The path names for all files associated with a Workstation Pro virtual machine are relative to the virtual machine directory. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine.

When you move a virtual machine to a different host system or to a different location on the same host system, Workstation Pro generates a new MAC address for the virtual network adapter. Workstation Pro 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 Pro generates UUIDs for moved virtual machines. See Using the Virtual Machine UUID.
- 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.
- 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 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 Pro 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 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. Workstation 10.x and later virtual machines support up to sixteen-way multiprocessing on multiprocessor host systems. You can assign up to 8 or 16 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.

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 Pro 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.

Open a Virtual Machine in VMware Workstation Player

VMware® Workstation Player opens and plays virtual machines created in other VMware products.

Workstation Player is included with VMware Workstation Pro. When you install Workstation Pro, the Workstation Player application file is stored with the Workstation Pro 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 Workstation Player for free from the VMware Web site.

Prerequisites

Verify that the virtual machine is compatible with Workstation Player. See Configure a Virtual Machine for Compatibility.

Procedure

1 Start Workstation 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 Workstation 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, Workstation Pro 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 Workstation Pro, 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. Workstation Pro 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.

Results

The virtual machine uses new UUID is used when it reboots.

Configure a Virtual Machine as a VNC Server

You can use Workstation Pro to configure a virtual machine to act as a Virtual Network Computing (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 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.

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.

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 Pro installation directory.

Host System	Keymap File Location
Windows 7, Windows 8, and Windows 10 hosts	`C:\ProgramData\VMware\vnckeymap`
Linux host	`/usr/lib/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 Pro 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 6-1. Language Codes

Code	Language
`de`	German
`de-ch`	German (Switzerland)
`es`	Spanish
`fi`	Finnish
`fr`	French
`fr-be`	French (Belgium)

Table 6-1. Language Codes (continued)

Code	Language
fr-ch	French (Switzerland)
is	Icelandic
it	Italian
jp	Japanese
nl-be	Dutch (Belgium)
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 Pro 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.
- 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.

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 UEFI, number of virtual slots, maximum number of CPUs, maximum memory configuration, and other hardware characteristics.

When you upgrade Workstation Pro, you must change the hardware compatibility of virtual machines that were created in previous versions of Workstation Pro so that they can use the new features in the new version of Workstation Pro. You can run older versions of virtual machines in the new version of Workstation Pro, 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 Pro 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.

Procedure

1. Make backup copies of the virtual disk (`.vmdk`) files.
2. If you are upgrading from a Workstation 5.x virtual machine, or downgrading to a Workstation 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 or later, you can change the hardware compatibility of a remote virtual machine. However, you cannot downgrade 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.

Update VMware Tools to the version included with the latest version of Workstation Pro, even if you upgraded the virtual machine to an earlier version of Workstation Pro. 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.
- If you upgrade a Workstation 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, Windows 7, or Windows 8 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 remote virtual machine.
- Using Workstation 10 and later, you can change the hardware compatibility of a 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 Pro 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 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 Pro 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 Pro 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 Pro 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.

Export a Virtual Machine with vTPM to OVF Format on Intel-based Mac

You can manually export a virtual machine with vTPM device from Workstation Pro to Open Virtualization Format (OVF) using the command line of OVF Tool 4.5 or later. The OVF Tool is bundled with Workstation Pro. You can export to both .ovf and .ova files.

A virtual machine with vTPM is always encrypted. You cannot directly convert a virtual machine with vTPM device in Workstation Pro from VMware runtime (.vmx) format to OVF format because the OVF Tool does not support export of an encrypted virtual machine. Before you proceed with the manual export, you must manually remove the vTPM device and decrypt the virtual machine. After you decrypt the virtual machine, export the virtual machine to OVF with a vTPM placeholder.

The following steps guide you through the process of manually removing the vTPM, decrypting the virtual machine, and then exporting to OVF using command line.

Prerequisites

- Remove any application in the virtual machine that uses the vTPM device.

  Note If you do not remove an application in the virtual machine that uses the vTPM, the application might not function properly when you later import the virtual machine with the vTPM device.

- Verify that the virtual machine is powered off.

Procedure

1 To remove the vTPM, perform the following steps:

   a Select the required virtual machine, and then go to **VM > Settings**.

   b On the **Hardware** tab, select **Trusted Platform Module**.

   c Click **Remove**.

   Workstation Pro removes the vTPM successfully.

2 To remove the virtual machine encryption, perform the following steps:

   a Select the required virtual machine, and then go to **VM > Settings**.

   b On the **Options** tab, select **Access Control**.

   c On the right panel, click **Remove Encryption...**.

   d Enter the encryption password of the virtual machine, and then click **Remove Encryption**.

   Workstation Pro removes the encryption successfully.

3 To export the virtual machine to OVF with an added vTPM placeholder, use the following command in the OVF Tool bundled with Workstation Pro:

```
main % "C:\Program Files (x86)\VMware\VMware Workstation\OVFTool\ovftool.exe" --
X:logLevel=verbose --exportFlags=extraconfig --allowExtraConfig --addDevice:vtpm '<path of
the virtual machine vmx file with the file name>' '<path to export the ovf file with the
file name>'
```

   The following is an example command to export a virtual machine named *vm*:

```
main % "C:\Program Files (x86)\VMware\VMware Workstation\OVFTool\ovftool.exe"
--X:logLevel=verbose --exportFlags=extraconfig --allowExtraConfig --addDevice:vtpm
"C:\Users\abc\Documents\Virtual Machines\vm\vm.vmx" "C:\Users\abc\Documents\Virtual
Machines\vm\vm.vmx"
```

   Note Workstation Pro does not provide a graphical user interface to export a virtual machine with a vTPM placeholder. A user must use the command line to export a virtual machine with a vTPM placeholder.

   After you export the virtual machine, the OVF file shows the added vTPM placeholder in the following format:

```
<Item ovf:required="false">
 <rasd:AutomaticAllocation>false</rasd:AutomaticAllocation>
 <rasd:ElementName>Virtual TPM</rasd:ElementName>
 <rasd:InstanceID>14</rasd:InstanceID>
 <rasd:ResourceSubType>vmware.vtpm</rasd:ResourceSubType>
 <rasd:ResourceType>1</rasd:ResourceType>
</Item>
```

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`).

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 Eclipse

The integrated development environment (IDE) plug-ins provide a configurable interface between virtual machines and Eclipse. They let you test, run, and debug programs in virtual machines. See the *Integrated Virtual Debugger for Eclipse 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.

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.

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

7

You can use Workstation Pro 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.

Read the following topics next:

- Configuring DVD, CD-ROM, and Floppy Drives
- Configuring a USB Controller
- Configuring and Maintaining Virtual Hard Disks
- Adding a Physical Disk to a Virtual Machine
- Configuring Virtual Ports
- Configuring Generic SCSI Devices
- Configuring Virtual Trusted Platform Module Devices
- Configuring Sixteen-Way Virtual Symmetric Multiprocessing
- Configuring Keyboard Features
- Modify Hardware Settings for a Virtual Machine

Configuring DVD, CD-ROM, and Floppy Drives

You can add up to four IDE devices, up to 60 SCSI devices, and up to 120 SATA devices (four controllers with 30 devices per controller) to a virtual machine. Any of these devices can be connected to a physical or virtual CD-ROM or DVD device. CD-ROM and DVD devices cannot be connected to an NVMe controller.

A virtual machine can read data from a DVD disc. Workstation Pro does not support playing DVD movies in a virtual machine. If you use a DVD player application that does not require video overlay support in the video card, you might be able to play a movie.

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, SCSI, or SATA 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 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. Click **Finish** to add the drive to the virtual machine.
5. (Optional) To change which SCSI, IDE, or SATA device identifier to use for the drive, select the drive and click **Advanced**.
6. 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. Click **Finish** to add the drive to the virtual machine.
5. 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.

6. If you selected the physical floppy drive media type, select a specific floppy drive or select **Auto detect** to allow Workstation Pro to auto-detect the drive to use.

7 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.

8 To connect the drive or floppy image file to the virtual machine when the virtual machine powers on, select **Connect at power on**.

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 Pro 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. 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 for information on connecting HIDs.

Add a USB Controller to a Virtual Machine

A USB controller is required to use a USB device in a virtual machine. You can add one USB controller to a virtual machine.

When you create a virtual machine in Workstation Pro, a USB controller is added by default. If you remove the USB controller, you can add it back.

Note Remote virtual machines are created without a USB controller by default. You can add a USB controller manually after you finish creating a 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. Click **Finish** to add the USB controller.
5. Configure the USB connection settings.

   You can select multiple settings.

   Note You typically cannot configure USB connection settings for a 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 This feature only appears when you use Workstation Pro on a Linux host.	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.

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 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 Pro 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.

What to read next

- Configuring a Virtual Hard Disk

  You can configure virtual hard disks as IDE or SATA disks for any guest operating system. You can 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 can also set up a virtual hard disk as an NVMe disk for any guest system that includes NVMe drivers. You determine which SCSI adapter to use when you create a virtual machine.

- Compact a Virtual Hard Disk

  Compacting a virtual hard disk can reclaim unused space in the virtual disk. Modern disks and operating systems are much more efficient at managing disk space than in the recent past. Therefore, do not expect the compacting procedure to return large amounts of disk space to the host drive.

- Expand a Virtual Hard Disk

  You can add storage space to a virtual machine by expanding its virtual hard disk.

- 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.

- 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.

- Using Virtual Disk Manager

  Virtual Disk Manager (`vmware-vdiskmanager.exe`) is a Workstation Pro utility that you can use to create, manage, and modify virtual disk files from the command line or in scripts.

- Using Legacy Virtual Disks

  You can use the current version of Workstation Pro in a mixed environment with virtual machines that were created with earlier versions or with other VMware products.

- 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.

- 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.

Configuring a Virtual Hard Disk

You can configure virtual hard disks as IDE or SATA disks for any guest operating system. You can 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 can also set up a virtual hard disk as an NVMe disk for any guest system that includes NVMe drivers. You determine which SCSI adapter to use when you create a virtual machine.

The files that make up an IDE, SATA, SCSI, or NVMe virtual hard disk can be stored on a hard disk of any type. 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

Most virtual hard disks can be up to 8TB. SCSI disks on the BusLogic controller are limited to 2TB. Depending on the size of the virtual hard disk and the host operating system, Workstation Pro 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 slightly 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 split into multiple files on the host disk. The split is not visible to the virtual machine, but is necessary if you move the virtual machine or its disks to a file system that does not support files larger than 4GB, such as a USB thumb drive formatted with the FAT32 file system.

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. Workstation Pro supports up to four IDE devices, 60 SCSI devices, 120 SATA devices, and 256 NVMe virtual disks.

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.

As an alternative to adding a new virtual hard disk, you can expand the existing virtual hard disk. See Expand a Virtual Hard Disk.

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 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.

Option	Description
SATA	Create a SATA device. You can add up to 120 SATA devices, four controllers, and 30 devices per controller.
NVMe	Create an NVMe device. You can add up to 256 NVMe devices, four controllers, and 64 devices per controller.

5 Select **Create a new virtual disk**.

6 Set the capacity for the new virtual hard disk.

You can set a size between 0.001 GB and 8 TB for a virtual disk.

7 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 in a file system that has a file size limitation. Split extent size is decided based on the disk capacity. If the capacity is less than or equal to 127 GB, it creates a series of 32 virtual disk files, each with a size of 4064 MB. If the capacity is between 127 GB and 2032 GB, the virtual disk is divided into 32 extents. If the capacity is greater than or equal to 2032 GB, it utilizes 2032 GB extents to maximize efficiency and minimize the number of files.

8 Accept the default filename and location, or browse to and select a different location.

9 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.

10 (Optional) To exclude the disk from snapshots, select **Advanced > 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.

11 Click **OK or Save** to save your changes.

12 Use the guest operating system tools (such as the Windows Disk Management tool or the `fdisk` command in Linux) 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 can reclaim unused space in the virtual disk. Modern disks and operating systems are much more efficient at managing disk space than in the recent past. Therefore, do not expect the compacting procedure to return large amounts of disk space to 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.

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.

  You can determine whether a virtual machine is a linked clone by the virtual machine name string on the summary page. If the string includes "Clone of: *virtual machine name*", the virtual machine is a linked clone. If the string includes "Snapshot: Snapshot for *virtual machine name*", the virtual machine is a 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 0.001 GB and 8192 GB 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 Pro 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 Pro. 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-vdiskmanager.exe`) is a Workstation Pro utility that you can use to create, manage, and modify virtual disk files from the command line or in scripts.

Virtual Disk Manager is included in the VMware Workstation program files directory when Workstation Pro is installed. 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.

Using Legacy Virtual Disks

You can use the current version of Workstation Pro in a mixed environment with virtual machines that were created with earlier versions or with other VMware products.

Although you can use the current version of Workstation Pro to power on virtual machines that were created with older versions or other VMware products, many new features of Workstation Pro 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 5.x and later 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 Pro on a Windows host system to create virtual hard disks, move the disks to a Linux computer, and use the disks with Workstation Pro 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 Pro supports physical disks up to 2TB capacity. Booting from an operating system already set up on an existing 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 2008 R2 or Windows Server 2012 R2 host	a Select **Start > Settings > Control Panel > Administrative Tools > Computer Management > Storage > Disk Management**. b Select a partition and select **Action > All Tasks > Change Drive Letter and Paths**. c Click **Remove**.
The partition is mapped to a Windows 7, Windows 8, or Windows 10 host	a Select **Start > Control Panel**. b In the menu bar, click the arrow next to **Control Panel**. c From the drop-down menu, select **All Control Panel Items > Administrative Tools > Computer Management > Storage > Disk Management (Local)**. d Right-click a partition and choose **Change Drive Letter and Paths**. e 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 7 hosts, you cannot use the system partition, or the physical disk that contains it, in a virtual machine. 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, ensure that it is configured as the primary on the IDE channel.

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

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

      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 Workstation Pro 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 Workstation Pro 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 Pro 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.

Note You cannot add a physical disk to a remote virtual machine.

Prerequisites

- Perform the appropriate preparation tasks. See Prepare to Use a Physical Disk or Unused Partition.
- 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 Pro 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

  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

  Linux 2.6.x kernels that support parallel ports use the `modprobe` *`modulename`* and `modprobe parport_pc` modules. Workstation Pro 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

  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

  A parallel port on the host system does not have an Extended Control Register (ECR).

- 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.

- Change the Input Speed of a Serial Connection

  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 scanners, dongles, and disk drives.

Workstation Pro 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

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. Click **Finish** to add the virtual parallel port to the virtual machine.
5. 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.

6. To connect the virtual parallel port to the virtual machine when the virtual machine powers on, select **Connect at power on**.

Results

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, detect the ports at boot time.

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 Pro 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 Pro username.

   For example: **`lp::7:daemon,lp,`*`workstation_username`***

Results

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 deactivated 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 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.

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 Click **Finish** to add the virtual serial port to the virtual machine.

5 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.

6 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.

7 To connect the port to the virtual machine when the virtual machine powers on, select **Connect at power on**.

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 Pro.

Procedure

1 In a text editor, add the following line to the virtual machine configuration (`.vmx`) file.

serial*port_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 Pro as a user who has administrator access.

Although generic SCSI is device independent, it can be sensitive to the guest operating system, device class, and specific SCSI hardware.

What to read next

- 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.

- Avoiding Concurrent Access Problems for SCSI Devices on Linux Hosts

  Workstation Pro 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

  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 remote virtual machine.

Prerequisites

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. Click **Finish** to add the device.
5. 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`.
6. To connect the device when the virtual machine powers on, select **Connect at power on**.

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.

Avoiding Concurrent Access Problems for SCSI Devices on Linux Hosts

Workstation Pro 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, deactivate 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.

   scsi*Z*:*Y*.fileName = "*deviceName*"

   Z is the SCSI bus number the device uses in the virtual machine. For *deviceName*, use **scsi*X*:*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.

   scsi*Z*:*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 Virtual Trusted Platform Module Devices

You can add a virtual cryptoprocessor that uses Trusted Platform Module (TPM) technology to an encrypted virtual machine. Afterward, you can remove the cryptoprocessor from the virtual machine.

TPM technology provides hardware-based, security-related functions. A TPM cryptoprocessor carries out cryptographic operations. Workstation Pro supports TPM version 2.0.

You can add TPM device on an encrypted virtual machine with a minimum hardware version of 14 that uses the UEFI firmware type.

Add a Virtual Trusted Platform Module Device

For increased security, you can add a virtual cryptoprocessor that is equipped with Trusted Platform Module (TPM) technology to an encrypted virtual machine.

Prerequisites

- Create a virtual machine with a minimum hardware version of 14 that uses the UEFI firmware type.
- Encrypt the virtual machine. See Encrypting Virtual Machines.

Procedure

1. Select the virtual machine and select **VM > Settings**.
2. Click **Add**.
3. Click **Trusted Platform Module**.

   If the option is not available, the Trusted Platform Module device is not supported on the guest.
4. Click **Finish**.
5. Click **OK**.

Results

The virtual machine uses the virtual TPM device.

Note When a TPM device is present on a virtual machine, you cannot perform the following actions.

- Decrypt the virtual machine.
- Change the firmware type to BIOS.

Remove a Virtual Trusted Platform Module Device

You can remove a Trusted Platform Module device from a virtual machine.

After you add a virtual cryptoprocessor equipped with Trusted Platform Module (TPM) technology to an encrypted virtual machine, you can then remove the TPM device.

Procedure

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

2 Select **Trusted Platform Module** and click **Remove**.

3 Click **OK**.

Results

Workstation Pro removes the TPM device from the virtual machine.

Configuring Sixteen-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 Pro 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 Sixteen-Way Virtual Symmetric Multiprocessing

You can configure sixteen-way virtual symmetric multiprocessing (SMP) for an existing virtual machine.

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 16.

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

Use a Virtual Machine That Has More Than Sixteen Virtual Processors

If Workstation Pro is running on a multiprocessor host system, you can open a virtual machine that has more than 16 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 Pro 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 Pro 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

  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

  You can change the hot-key combinations that you use to perform common virtual machine operations.
- 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.
- 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.

- 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`.

- Configure How Keysyms Are Mapped

  When key code mapping cannot be used or is turned off, Workstation Pro maps keysyms to v-scan codes. If a language-specific keyboard does not appear to be supported by Workstation Pro, you might need to set a property that tells Workstation Pro which keysym table to use.

- V-Scan Code Table

  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 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 Pro, install it by running the Workstation Pro installer in program maintenance mode. See Install the Enhanced Keyboard Driver on a Windows Host.

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 Pro 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 Pro, you can install it by running the Workstation Pro 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 Double-click the `VMware-workstation-xxxx-xxxxxxx.exe` file, where *xxxx-xxxxxxx* is the version and build numbers.

3 Select **Modify/Change**.

4 Select **Enhanced Keyboard Utility**.

5 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.

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 Pro 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.

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.

Use Ctrl+Alt in a Key Combination

Because Ctrl+Alt tells Workstation Pro 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 Pro 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 Pro 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 Pro 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 Pro uses this key code map only for local X servers. You can set a property to tell Workstation Pro to use key code mapping. See Understanding X-Key Codes and Keysyms 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 Pro.

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 Pro does not recognize as an XFree86 server, add the `xkeymap.usekeycodeMap` property and set it to **`TRUE`**.

  This property tells Workstation Pro to always use key code mapping regardless of server type.

  For example: **`xkeymap.usekeycodeMap = "TRUE"`**

- If Workstation Pro does not recognize the remote server as an XFree86 server, add the `xkeymap.usekeycodeMapIfXFree86` property and set it to **`TRUE`**.

  This property tells Workstation Pro 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 Pro 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 Pro uses. When Workstation Pro 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 Pro 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.
- 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 for most v-scan codes.
- Power off the virtual machine and exit Workstation Pro.

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 turned off, Workstation Pro maps keysyms to v-scan codes. If a language-specific keyboard does not appear to be supported by Workstation Pro, you might need to set a property that tells Workstation Pro which keysym table to use.

Workstation Pro 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 Pro.

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 Pro 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.
- Power off the virtual machine and exit Workstation Pro.

Procedure

- To turn off 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 Pro 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 7-1. 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

Table 7-1. V-Scan Codes for the 104-Key U.S. Keyboard (continued)

Symbol	Shifted Symbol	Location	V-Scan Code
5	%		0x006
6	^		0x007
7	&		0x008
8	*		0x009
9	(		0x00a
0	)		0x00b
-	_		0x00c
=	+		0x00d
Backspace			0x00e
Tab			0x00f
Q			0x010
W			0x011
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

Table 7-1. V-Scan Codes for the 104-Key U.S. Keyboard (continued)

Symbol	Shifted Symbol	Location	V-Scan Code
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
Space bar			0x039
Caps Lock			0x03a
F1			0x03b
F2			0x03c
F3			0x03d

Table 7-1. V-Scan Codes for the 104-Key U.S. Keyboard (continued)

Symbol	Shifted Symbol	Location	V-Scan Code
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

Table 7-1. V-Scan Codes for the 104-Key U.S. Keyboard (continued)

Symbol	Shifted Symbol	Location	V-Scan Code
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
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, 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

8

Workstation Pro 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 Pro.

Read the following topics next:

- Understanding Virtual Networking Components
- Understanding Common Networking Configurations
- Changing the Default Networking Configuration
- Configuring Bridged Networking
- Configuring Network Address Translation
- Configuring Host-Only Networking
- Assigning IP Addresses in Host-Only Networks and NAT Configurations
- Enable Jumbo Frames
- Configuring LAN Segments
- Configuring Samba for Workstation Pro
- Using Virtual Network Adapters in Promiscuous Mode on Linux Hosts
- Maintaining and Changing MAC Addresses for Virtual Machines
- Sample Custom Networking Configuration

Understanding Virtual Networking Components

The virtual networking components in Workstation Pro 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 8-1. Default Virtual Network Switches

Network Type	Switch Name
Bridged	VMnet0
NAT	VMnet8
Host-only	VMnet1

Workstation Pro 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, Intel Pro/1000 MT Server Adapter, or Intel 82574L Gigabit Network Connection. In Windows Vista, Windows 7, and Windows 8 guest operating systems, the adapter is an Intel Pro/1000 MT Server Adapter. In Windows 8.1 and Windows10 guest operation systems, the adapter is an Intel 82574L Gigabit Network Connection.

Workstation 6.0 and later virtual machines can have up to 10 virtual network adapters. Workstation 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 Pro on a Windows or Linux host system, a bridged network (VMnet0) is set up for you. See Configuring Bridged Networking.

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 Pro 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. See Configuring Network Address Translation.

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 Pro on a Windows or Linux host system, a host-only network (VMnet1) is set up for you. See Configuring Host-Only Networking.

Custom Networking Configurations

With the Workstation Pro 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. Sample Custom Networking Configuration.

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 Pro 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.

What to read next

- Add a Virtual Network Adapter to a Virtual Machine

  You can add up to 10 virtual network adapters to a virtual machine.
- 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.
- Disconnect a Host Virtual Network Adapter

  When you install Workstation Pro, 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, Packet Loss, and Latency Settings for a Virtual Machine

  You can use advanced virtual network adapter settings to limit the bandwidth, specify the acceptable packet loss percentage, and create network latency 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 5.x virtual machines are limited to three virtual network adapters.

Prerequisites

Familiarize yourself with the network configuration types. See Understanding Common Networking Configurations.

Procedure

1. Select the virtual machine and select **VM > Settings**.
2. On the **Hardware** tab, click **Add**.

3 To add the virtual network adapter to the virtual machine, select **Network Adapter** and click **Finish**.

4 Select the virtual network adapter type.

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.

5 (Optional) Select the **Connect at power on** checkbox.

6 Click **Finish** to add the virtual network adapter to the virtual machine.

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

8 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.

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.

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 Pro, 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, Packet Loss, and Latency Settings for a Virtual Machine

You can use advanced virtual network adapter settings to limit the bandwidth, specify the acceptable packet loss percentage, and create network latency for incoming and outgoing data transfers for a virtual machine.

Note You cannot configure advanced virtual network adapter settings for a 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 Enter the acceptable packet loss percentage for incoming and outgoing data transfers in the **Packet Loss (%)** text box.

The default setting is 0.0%.

5 Enter the number of milliseconds (ms) for network latency of incoming and outgoing data transfers.

The latency setting allows you to simulate the latency in a network environment that differs from your own. The latency range is 0 to 2,000 ms.

Note Expect actual network latency to be up to 10 ms above the number you set. For example, if you set latency at 200 ms, expect the actual latency to be between 200 to 210 ms.

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

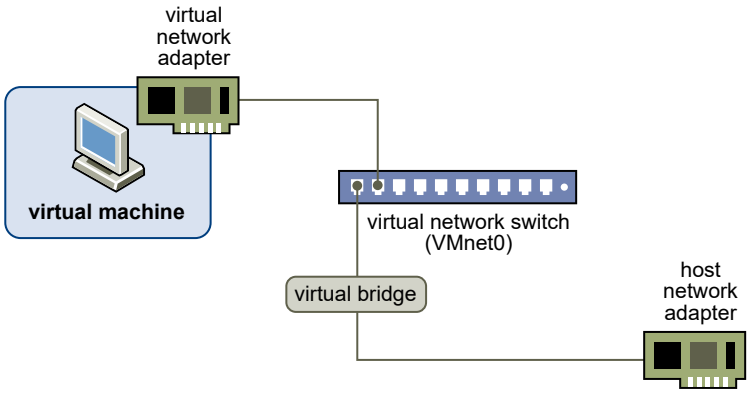
Configuring Bridged Networking

When you install Workstation Pro 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 8-1. 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.

What to read next

- 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.

- Add a Bridged Network

  When you install Workstation Pro on a Windows or Linux host system, a bridged network (VMnet0) is set up for you. If you install Workstation Pro on a host system that has multiple network adapters, you can configure multiple bridged networks.

- Configure Bridged Networking for an Existing Virtual Machine

  You can configure bridged networking for an existing virtual machine.

- 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.

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 Pro on a Windows or Linux host system, a bridged network (VMnet0) is set up for you. If you install Workstation Pro 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 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 to VMnet19. 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.

What to do next

If you want to rename the new network to a name that is meaningful to you, see Rename a Virtual Network.

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**.

The location of the **VMnet0** option can vary.

Status	Description
VMnet0 option listed	If listed, select **VMnet0**.
VMnet0 option not listed	If not listed, click **Change Settings** and 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**. b Deselect the check box for the host network adapter. 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.

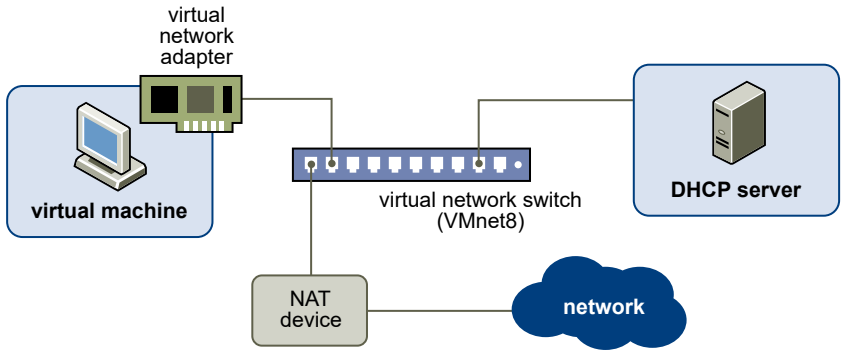
4 Click **OK** to save your changes.

Configuring Network Address Translation

When you install Workstation Pro 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 8-2. 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.

What to read next

- 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.

- Change NAT Settings

  You can change the gateway IP address, configure port forwarding, and configure advanced networking settings for NAT networks.

- Editing the NAT Configuration File

  If you are an advanced user, you can edit the NAT configuration file to modify NAT settings.

- 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.

- 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.

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 Pro 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

You can change the gateway IP address, configure port forwarding, and configure advanced networking settings for NAT networks.

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 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 NAT network, and click **NAT Settings**.

By default, the NAT device is connected to the VMnet8 virtual switch. You can have only one NAT virtual network.

Table 8-2. NAT Settings

Setting	Description
Gateway IP	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	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. **Important** Change this value only under the direction of VMware technical support.
Enable IPv6	Enable NAT to use an IPv6 address.
IPv6 Prefix	If IPv6 is enabled, enter the IPv6 prefix that the NAT device uses.

Table 8-2. NAT Settings (continued)

Setting	Description
DNS Settings	(Windows hosts only) 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	(Windows hosts only) 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 8-3. NAT Configuration File Location

Host Operating System	NAT Configuration File Location
Windows Server 2008 R2, Windows Server 2012 R2, Windows 7, Windows 8 or Windows 10	`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`**.

You can change the NAT configuration by using the virtual network editor. You do not need to edit the NAT configuration file.

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 8-4. [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 8-5. [dns] Section Parameters

Parameter	Description
`policy`	Policy to use for DNS forwarding. ■ `order` sends one DNS request at a time in the order of the name servers. ■ `rotate` sends one DNS request at a time and rotate through the DNS servers. ■ `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.

Table 8-5. [dns] Section Parameters (continued)

Parameter	Description
`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 8-6. [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
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 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, 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 8-7. 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.

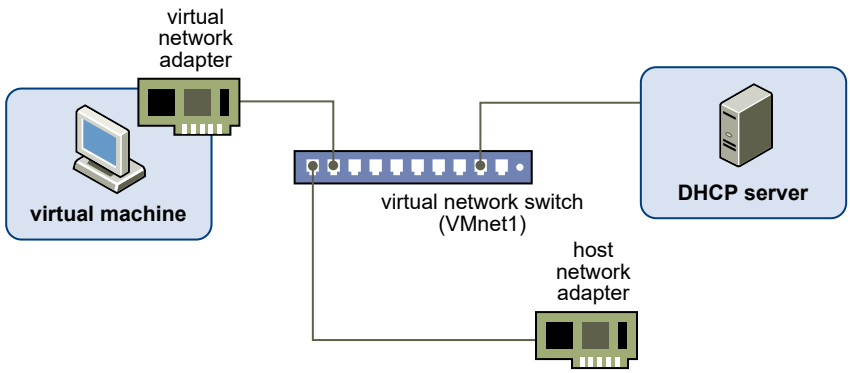
See Editing the NAT Configuration File for more information.

Configuring Host-Only Networking

When you install Workstation Pro 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 8-3. 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 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.

What to read next

- Add a Host-Only Network

  When you install Workstation Pro 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

  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

  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

  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

  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

  The virtual DHCP server in Workstation Pro 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 Pro 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 to VMnet19. 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.

Results

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.

What to do next

If you want to rename the new network to a name that is meaningful to you, see Rename a Virtual Network.

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.

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 Pro. See Add a Host-Only Network.

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 turned on, host-only network traffic might leak out through the dial-up connection. To prevent the leakage, turn off 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 turn off forwarding. To avoid packet leakage, you must turn on 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.

Turn Off 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 and later systems, have IP packet forwarding turned off by default.

If packets are leaking from a host-only network on a Windows host system, check whether packet forwarding is turned off on the host system. If packet forwarding is turned on, you must turn it off.

Procedure

- On a Windows Vista or Windows 7 or later 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**.

Turn Off 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 turned on, you must turn it off.

How you turn off 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 Pro 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 Pro, 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 Pro 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 Pro. 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 Pro. 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.

What to read next

- 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.

- 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.

- 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.

- 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 Pro 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.

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 Pro 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 Pro does not update that setting automatically if the value is within the valid range. If the value exceeds the valid range, Workstation Pro resets the settings based on the subnet range. Workstation Pro 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.

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.

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.

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 8-8. DHCP Configuration File Location

Host Operating System	DHCP Server Configuration File Location
Windows Server 2008 R2, Windows Server 2012 R2, Windows 7, Windows 8, or Windows 10	`C:\ProgramData\VMware\vmnetdhcp.conf`
Linux	For the default host-only network: `/etc/vmware/vmnet1/dhcp/dhcp.conf` 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 Pro 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 8-9. 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 8-10. 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

Enable Jumbo Frames

With Workstation Pro, you can enable jumbo frames for VMware virtual networks.

Jumbo frames let you send larger frames out onto the physical network or between virtual machines on the same host.

Enable Jumbo Frames on Linux Host

With Workstation Pro, you can enable jumbo frames for VMware virtual networks using the Virtual Network Editor on Linux.

Procedure

1 To launch the **Virtual Network Editor**, run the `vmware-netcfg` command in the terminal or click **Edit > Virtual Network Editor** from the UI.

Note The **Edit > Virtual Network Editor** option is only available in Workstation Pro.

2 Enter the super user password, and click **Authenticate**.

3 To configure jumbo frames, enter a value between 68 bytes and 9194 bytes in the **MTU** text box and click **Save**.

Results

Jumbo frame is enabled.

Enable Jumbo Frames on Windows Host

With Workstation Pro, you can enable jumbo frames for VMware virtual networks in the VMware Virtual Ethernet Adapter on Windows.

Procedure

1 Navigate to **Control Panel > Network and Internet > Network Connections**.

2 In the Network Connections window, right-click a VMware network adapter and select **Properties**. Click **Configure** on the **Networking** tab.

3 In the new window that appears, select the **Advanced** tab and select **Jumbo Packet**.

4 In the **Value** drop-down menu, select the packet size and click **Ok**.

Results

Jumbo frame is enabled.

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 Pro, 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.

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 Pro, bandwidth and packet loss settings are associated with individual virtual machines rather than LAN segments. See Configure Bandwidth, Packet Loss, and Latency Settings for a Virtual Machine.

Prerequisites

- If the LAN segment does not already exist, create it. See Create a LAN Segment for a Virtual Machine.
- 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.

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 Pro 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.

Configuring Samba for Workstation Pro

If you have Samba on a Linux host system, you can configure it so that it works with Workstation Pro.

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 Pro does not allow the virtual network adapter to go into promiscuous mode unless the user running Workstation Pro 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 Pro, you must run the installation as the root user. Because Workstation Pro 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 Pro 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 Pro 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 Pro 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 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 Pro 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 Pro virtual machines do not support arbitrary MAC addresses.

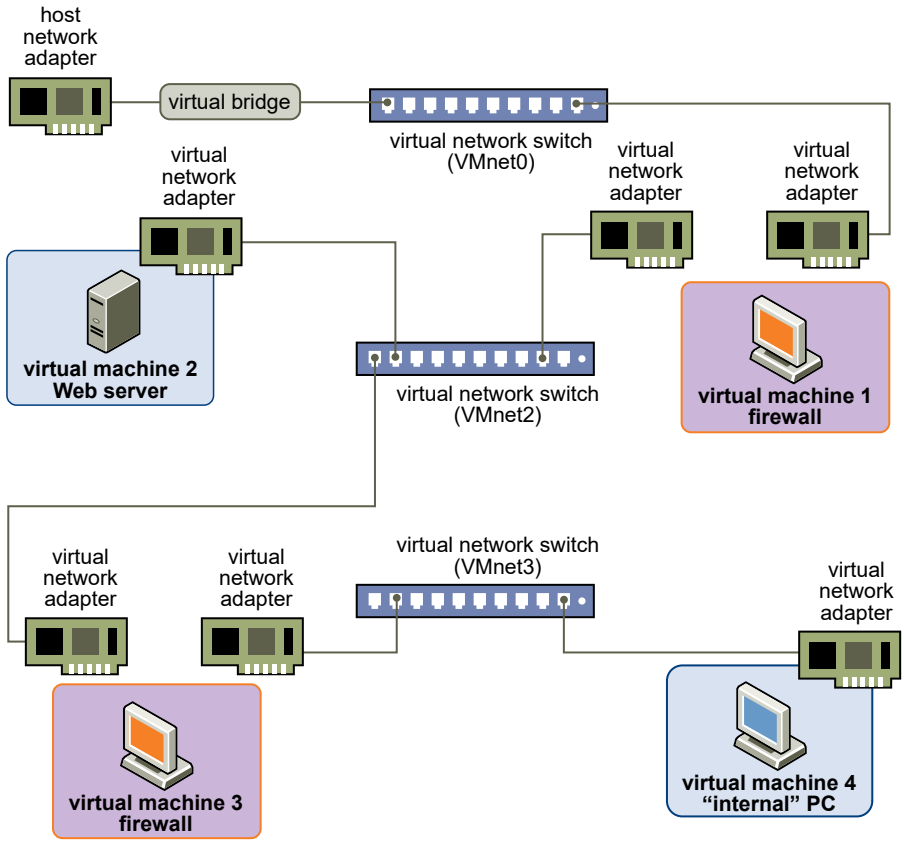
   A value for *XX:YY:ZZ* that is unique among your hard-coded addresses avoids conflicts between the automatically assigned MAC addresses and the manually assigned addresses.

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 8-4. 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 8-4. Custom Configuration with Two Firewalls.

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 to Manage Remote Virtual Machines

9

The following sections describe howremote virtual machines can be managed using remote connections.

Read the following topics next:

- Connect to a Remote Server
- Disconnect from a Remote Server
- Uploading Virtual Machines to Remote Servers
- Download a Virtual Machine from a Remote Server
- Create a Virtual Machine on a Remote Host
- Manage Virtual Machine Power Actions on Remote Hosts
- Using Roles to Assign Privileges

Connect to a Remote Server

You can use Workstation Pro to connect to a remote server that is running ESXi, or vCenter Server.

When you connect to a remote server for the first time, Workstation Pro asks you whether to save your login information. You can configure Workstation Pro to never ask you to save login information for a remote server. See Turn Off the Prompt to Save Remote Login Information.

Prerequisites

Verify that the remote server is running or 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**.

3 (Optional) If Workstation Pro asks you whether to save your login information, select an option.

Option	Description
Remember	Workstation Pro 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 Pro 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 Pro does not save your login information, but it prompts you to save your login information the next time you connect to this server.

Results

After you connect to the remote server, the remote host appears in the library. At a minimum, remote virtual machines also appear in the library.

If you are using Workstation Pro on a Windows host and the remote server is running vCenter Server, other objects can appear in the library. In this situation, when vCenter Server appears in the library, you can toggle between the Hosts and Clusters view and the VMs view. The Hosts and Clusters view displays datacenters, clusters, ESXi hosts, resource pools, vApps, and virtual machines. The VMs view lists datacenters, folders, and virtual machines.

What to do next

Interact with the remote host and remote virtual machines. See Interacting with Remote Hosts and 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 you are using Workstation Pro on a Windows host and the remote server is running vCenter Server, you can toggle between the Hosts and Clusters view and the VMs view. The Hosts and Clusters view displays datacenters, clusters, ESXi hosts, resource pools, vApps, and virtual machines. The VMs view lists datacenter, folders, and virtual machines.

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 perform the following actions on the remote host.

- Restart
- Shut down
- Enter maintenance mode
- 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.

Turn Off the Prompt to Save Remote Login Information

You can turn off the prompt to save remote login information for a specific remote server or for all remote servers.

Procedure

- Turn off 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 Pro 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.
- Turn off the prompt to save login information for all remote servers.
  a Select **Edit > Preference > Workspace**.
  b Deselect **Offer to save login information for remote hosts**.
  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 Pro 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 Pro 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 Pro 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 Pro 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 Pro 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 Pro 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.

Uploading Virtual Machines to Remote Servers

You can upload virtual machines created with Workstation Pro to remote servers running VMware ESXi or VMware vCenter Server.

What to read next

- Upload a Virtual Machine to a Remote Server

  When you upload a virtual machine to a remote server, Workstation Pro copies the virtual machine to the remote host and datastore that you select. The original virtual machine remains on the host system.

Upload a Virtual Machine to a Remote Server

When you upload a virtual machine to a remote server, Workstation Pro 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 VMware Workstation Pro, VMware ESXi or VMware vCenter Server..
- 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 Pro.
- 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 Pro 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.

Results

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 Pro 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 Pro host in the location you specify.

This feature is available for virtual machines on remote servers. It is not available for standard virtual machines on Workstation Pro hosts.

Prerequisites

- Connect to the remote server that hosts the virtual machine you want to download. See Connect to a Remote Server.
- 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 Pro 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 Pro 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.
- 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.

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. 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, SATA, or NVMe 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 virtual machine 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 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.

Results

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 .

Manage Virtual Machine Power Actions on Remote Hosts

You can manage power actions, such as start and stop actions, on remote virtual machines.

The available power options differ for Windows and Linux hosts.

Table 9-1. Virtual Machine Power Options on Windows host for Remote virtual machines

Power Actions	Description
Auto Start	When you select **Auto Start**, the virtual machines start when the host starts.
Auto Suspend	When you select **Auto Suspend**, the virtual machines suspend when the host shuts down.

Table 9-2. Virtual Machine Power Options on Linux host for Remote virtual machines

Power Actions	Description
Auto Start	When you select **Auto Start**, the virtual machines start when the host starts.
Suspend	When you select **Suspend**, the virtual machines suspend when the host shuts down.
Shut Down Guest	When you select **Shut Down Guest**, the virtual machines shut down when the host shuts down.
Power Off	When you select **Power Off**, the virtual machines power off when the host shuts down.
None	When you select **None**, the stop actions of the host do not affect the virtual machines.

If the remote server is running vCenter Server, you cannot configure power actions . You cannot use the power actions to configure virtual machines to start or stop 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 power actions for remote virtual machines, connect to the remote server. See Connect to a Remote Server.
- 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 a remote host	a In the library, select the remote host. b On the tab for the remote host, click **Manage VM Power Actions**.

2 Select the virtual machines to start or stop with the host system.

3 If you selected multiple virtual machines, select the number of seconds to delay between starting or stopping the virtual machines.

4 To save your changes, click **Save**.

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 Pro 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 remote 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.

What to read next

- Default System Roles

  Workstation Pro 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

  If the default system roles do not meet your needs, you can combine selected privileges to create your own roles.

- 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.

- 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.

- Remove a Role

  When you remove a role, Workstation Pro removes the definition from the list of roles.

Default System Roles

Workstation Pro 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 9-3. Default System Roles

Role	User Capabilities
Administrator	■ Has all privileges for all objects. ■ Can add, remove, and set access rights and privileges on all objects. 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. ■ Tabs associated with the object appear without content. 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. ■ 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 ESX, ESXi, or vCenter Server.

See *Defined Privileges* in the Workstation Pro documentation center for descriptions of the available privileges. The Workstation Pro 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.

Procedure

1 Open the Edit Roles dialog box.

Option	Description
Create a role on a remote host	■ (Windows host) Right-click the remote host and select **Roles**. ■ (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 Pro documentation center for descriptions of the available privileges. The Workstation Pro 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.

Procedure

1 Open the Edit Roles dialog box.

Option	Description
Edit a role on a remote host	■ (Windows host) Right-click the remote host and select **Roles**. ■ (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. ■ (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 Pro documentation center for descriptions of the available privileges. The Workstation Pro 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.

Procedure

1 Open the Edit Roles dialog box.

Option	Description
Clone a role on a remote host	■ (Windows host) Right-click the remote host and select **Roles**. ■ (Linux host) Right-click the remote host and select **Edit Roles**.

2 Select the role to clone and click **Clone**.

Workstation Pro 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 Pro 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.

Procedure

1 Open the Edit Roles dialog box.

Option	Description
Remove a role on a remote host	■ (Windows host) Right-click the remote host and select **Roles**. ■ (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 Pro 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**. ■ (Linux host) Select **Remove affected permissions**. 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. ■ (Linux host) Select **Reassign affected permissions to** and select a role.

Changing Workstation Pro Preference Settings

10

Workstation Pro preference settings are global configuration settings that apply to Workstation Pro and the virtual machines that you run in Workstation Pro. You can override certain Workstation Pro preference settings for specific virtual machines.

To change Workstation Pro preference settings, select **Edit > Preferences**.

Important The default settings for Workstation Pro preferences are correct for most cases. Do not change Workstation Pro preference settings unless you are an experienced user.

Read the following topics next:

- Configuring Workspace Preference Settings
- Configuring Input Preference Settings
- Changing Hot-Key Combinations
- Configuring Workstation Pro Display Preference Settings
- Configuring USB Device Connection Behavior
- Configuring Software Update Preference Settings
- Join or Leave the Customer Experience Improvement Program
- Configuring Workstation Pro Memory Preference Settings
- Configuring Workstation Pro Priority Preference Settings
- Configuring Device Settings for Windows Hosts

Configuring Workspace Preference Settings

You can use workspace preference settings to change the default hardware compatibility setting for newly created virtual machines, control how virtual machines behave when you exit Workstation Pro, and configure general workspace settings.

To configure workspace preference settings, select **Edit > Preferences > Workspace**.

What to read next

- Configuring the Default Locations for Virtual Machine Files and Screenshots

  You can configure the default locations for virtual machine files and captured screenshots.
- Configuring Virtual Machine Exit Behavior

  You can configure how virtual machines behave when you exit Workstation Pro.
- Enabling Shared Folders Created By Other Users

  As a security precaution, a shared folder is turned off by default if it was not created by the user who powers on the virtual machine. Folder sharing is also turned off by default for Workstation 5.x virtual machines, regardless of who created the virtual machine.
- Changing the Default Hardware Compatibility Setting

  You can change the hardware compatibility setting that the **New Virtual Machine** wizard uses when it creates a typical virtual machine. The hardware compatibility setting determines the hardware features that are supported in the virtual machine.
- Configuring Power On Delay and Aero Peek Thumbnail Settings

  You can configure the number of seconds that Workstation Pro delays between powering on virtual machines when you perform a batch power operation. You can also specify whether to show Aero Peek thumbnails on open virtual machine tabs.
- Changing the Remote Server Login Privacy Setting

  You can change the setting to turn on or off a prompt to save your login information when connecting to a remote server.

Configuring the Default Locations for Virtual Machine Files and Screenshots

You can configure the default locations for virtual machine files and captured screenshots.

To configure the default locations for virtual machine files and screenshots, select **Edit > Preferences > Workspace**.

Table 10-1. Virtual Machine File and Screenshot Location Settings

Setting	Description
Default location for virtual machines	The default location for storing virtual machine files. This path appears in the **Location** text box in the **New Virtual Machine** wizard and the **Clone Virtual Machine** wizard. It applies to virtual machines that the currently logged in user creates.
Save screenshots to	Select whether to save virtual machine screenshots to the clipboard, to a file, or to both. When saving a screenshot to a file, you can have Workstation Pro: ■ Aways ask for location ■ Save to desktop ■ Browse for custom location By default, Workstation Pro saves screenshots to `.png` files on the Desktop of the host computer. To save screenshots to `.bmp` files on Windows hosts, select **Always ask for location** and specify the file type when you create the screenshot.

Configuring Virtual Machine Exit Behavior

You can configure how virtual machines behave when you exit Workstation Pro.

To configure virtual machine exit behavior, select **Edit > Preferences > Workspace**.

Table 10-2. Virtual Machine Exit Behavior Settings

Setting	Description
Remember opened tabs between sessions	The virtual machine tabs that appear when you exit Workstation Pro appear the next time you start Workstation Pro. If a tab for a virtual machine appears in the Workstation Pro window, the virtual machine is considered open even if it is not powered on.
Keep VMs running after Workstation closes	Powered-on virtual machines remain running in the background when you close them or exit Workstation Pro. If you deselect this setting, Workstation Pro prompts you for the action to take each time you close a powered-on virtual machine or exit Workstation Pro. If a powered-on virtual machine continues running after you close it or exit Workstation Pro, you can interact with it through VNC or another service.
Show tray icon	If you run virtual machines in the background, use this setting to select how the tray icon appears. The tray icon is represented by three overlapping squares in the notification area in the taskbar on the host system. **Always** The tray icon appears in the taskbar when no virtual machines are running, even if Workstation Pro is not running. **When a virtual machine is powered on** The tray icon appears in the taskbar only when a virtual machine is powered on. **Never** The tray icon does not appear in the taskbar when a virtual machine is running, even if you restart Workstation Pro.

Enabling Shared Folders Created By Other Users

As a security precaution, a shared folder is turned off by default if it was not created by the user who powers on the virtual machine. Folder sharing is also turned off by default for Workstation 5.x virtual machines, regardless of who created the virtual machine.

To enable shared folders that were created by other users, select **Edit > Preferences > Workstation** and select **Enable all shared folders by default**.

After this setting is enabled, you can specify which virtual machines can share folders and which folders can be shared.

Important Enabling all shared folders 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.

Changing the Default Hardware Compatibility Setting

You can change the hardware compatibility setting that the **New Virtual Machine** wizard uses when it creates a typical virtual machine. The hardware compatibility setting determines the hardware features that are supported in the virtual machine.

To change the default hardware compatibility setting, select **Edit > Preferences > Workspace**. The default hardware compatibility setting appears in the **Default hardware compatibility** menu.

By default, the default hardware compatibility setting is the Workstation Pro version that is installed on the host system.

If you plan to create virtual machines and deploy them in environments that use other VMware products, you might need to change the default hardware compatibility setting to an earlier Workstation version. Some products do not support all of the hardware features in the installed Workstation Pro version. If the virtual machine must be ESX server compatible, you can select the check box for ESX server compatibility on the Workspace preferences dialog box.

Note The check box for ESX server compatibility is not available when you create a virtual machine on a remote ESX host. Virtual machines created on remote ESX hosts are always ESX compatible.

See the *Virtual Machine Mobility Planning Guide* for information about virtual hardware versions. This guide lists compatibility problems to consider when you move virtual machines into different environments.

Note If you create a custom virtual machine in the **New Virtual Machine** wizard, you can override the default hardware compatibility setting.

Configuring Power On Delay and Aero Peek Thumbnail Settings

You can configure the number of seconds that Workstation Pro delays between powering on virtual machines when you perform a batch power operation. You can also specify whether to show Aero Peek thumbnails on open virtual machine tabs.

To configure power on delay and thumbnail settings, select **Edit > Preferences > Workspace**.

Table 10-3. Power On Delay and Thumbnail Settings

Setting	Description
Seconds between powering on multiple VMs	Select the number of seconds that Workstation Pro delays between starting virtual machines when you perform a batch power operation. You can perform a batch power operation on virtual machines in a folder by selecting the folder or by selecting thumbnails on the folder tab.
Show Aero Peek thumbnails for open tabs	Select whether to show Aero Peek thumbnails on open virtual machine tabs. This check box is available on Windows 7 version 6.1 and later host operating systems only.

Changing the Remote Server Login Privacy Setting

You can change the setting to turn on or off a prompt to save your login information when connecting to a remote server.

By default, when you connect to a remote server you are prompted whether you want Workstation Pro to save your login and password information. You can turn off this prompt from displaying by deselecting the **Offer to Save Login Information for Remote Hosts** checkbox. For more information, see Connect to a Remote Server.

Configuring Input Preference Settings

To direct input to a virtual machine, Workstation Pro captures input from the host system so that all keystrokes, mouse moves, and button clicks go to the virtual machine. You can use input preference settings to configure how Workstation Pro captures input from the host system.

To configure input preference settings, select **Edit > Preferences > Input**.

What to read next

- Configuring Keyboard and Mouse Settings

  Keyboard and mouse settings control how virtual machines that run in Workstation Pro capture input from the keyboard and mouse.
- Configuring Cursor Settings

  Cursor settings control cursor behavior for the virtual machines that you run in Workstation Pro.

Configuring Keyboard and Mouse Settings

Keyboard and mouse settings control how virtual machines that run in Workstation Pro capture input from the keyboard and mouse.

To configure keyboard and mouse settings, select **Edit > Preferences > Input**.

Table 10-4. Keyboard and Mouse Settings

Setting	Description
Grab keyboard and mouse input on mouse click	Virtual machines grab input the first time you click in the virtual machine window.
Grab keyboard and mouse input on key press	Virtual machines grab keyboard and mouse input the first time you press a key when the cursor is in the virtual machine window. When this setting is selected, you cannot use the normal application and system accelerator key sequences when the virtual machine display is active.

Troubleshooting Input Problems

You might occasionally encounter problems when virtual machines capture input from the keyboard and mouse on the host system.

Table 10-5. Common Input Problems and Solutions

Problem	Solution
Pressing Ctrl+Alt to release the mouse and keyboard causes a laptop to suspend.	By default, Workstation Pro uses Ctrl+Alt to release the mouse and keyboard. Some laptops use this same key combination to suspend the host machine. In these cases, try using Ctrl and Alt on the right side of the keyboard. Workstation Pro recognizes both sets of Ctrl and Alt keys, but laptops usually recognize only the keys on the left side of the keyboard for the suspend function.
After you press Ctrl+Alt to release the mouse and keyboard, the keyboard does not function properly within the host operating system.	Occasionally, Workstation Pro causes the host operating system to lose keyboard events, which in turn causes the host operating system to detect that keys are being pressed when they are not. If keys do not respond as expected after you exit Workstation Pro, they might be stuck in the host operating system. Press and release each of the modifier keys individually, including Ctrl, Shift, and Alt. If the keys still do not respond, press and release more special keys, including the Windows, Esc, and Caps Lock keys.
On Linux hosts, pressing Ctrl+Alt does not release the cursor.	The modifier keys might be mapped under X (in Linux) in unexpected ways. For example, the left Ctrl key might be mapped to Caps Lock, or an Alt key is generating special keystrokes. Run `xmodmap -- kim -- kp` and submit a support request to VMware technical support that includes the output.

Configuring Cursor Settings

Cursor settings control cursor behavior for the virtual machines that you run in Workstation Pro.

To configure cursor settings, select **Edit > Preferences > Input**.

Table 10-6. Cursor Settings

Setting	Description
Automatically grab and ungrab the mouse	Virtual machines release the cursor when you point outside of the virtual machine window. When this setting is selected, you can use the host system without first pressing a key combination. You might need to deselect this setting if you play computer games that pan or scroll when you move the pointer to the edge of the screen. VMware Tools must be installed in the virtual machine to use this feature.
Hide cursor on ungrab	The cursor does not appear in the virtual machine display after input is transferred back to the host system. If you have multiple virtual machines open at the same time, selecting this setting helps you track the active cursor. VMware Tools must be installed in the virtual machine to use this feature.
Optimize mouse for games	Select mouse behavior for computer games. In some computer games, you move the pointer to the edge of the screen to pan the scene or scroll. By optimizing the virtual mouse for games, you can achieve this effect in a virtual machine. **Automatic** Workstation Pro determines when to optimize mouse motion. This is the default setting. **Always** Mouse motion is always optimized for games. **Never** Mouse motion is never optimized. When you play computer games in a virtual machine, the optimized mouse is usually not released from the virtual machine. Some applications, such as AutoCAD, are incorrectly identified as games. Select this setting if you use AutoCAD and find that the mouse cannot pass freely from the virtual machine to the host system or if pointer speed is different when you use AutoCAD.

Changing Hot-Key Combinations

Hot-keys, which are also called keyboard shortcuts, provide a quick way to perform common virtual machine operations. Hot-key settings are usually a combination of the Ctrl, Shift, Alt, and Windows keys.

- You can change the hot-key combinations that you use to perform common virtual machine operations. See Change Hot-Key Combinations for Common Operations.
- You can change the hot-key combination that you use to access the **Start** and **Applications** menus in Unity mode. See Change Hot-Key Combinations for Unity Mode.

Configuring Workstation Pro Display Preference Settings

Display adjustments occur when you resize the Workstation Pro window and when you change the display settings inside the guest operating system. You can use display preference settings to configure how Workstation Pro makes display adjustments.

To configure display preference settings, select **Edit > Preferences > Display**.

If you are using Windows 8.1 (Update 2) or Windows 10, Workstation Pro detects the DPI on each monitor and scales the virtual machine to match the DPI on the host.

What to read next

- Configuring Autofit Settings

  Autofit settings control how the display of virtual machines adjusts to fit the Workstation Pro window.

- Configuring Full Screen Settings

  Full screen settings control how the host system and guest operating system display settings interact when you enter full screen mode. In full screen mode, the virtual machine display fills the screen and you cannot see the borders of the Workstation Pro window.

- Configuring Menu and Toolbar Settings

  Menu and toolbar settings control how the menus and toolbars appear when Workstation Pro is in full screen and windowed mode.

- Configuring Workstation Pro Color Theme Settings

  The Color Theme setting controls how the Workstation Pro main window appears on a Windows 10 host system.

Configuring Autofit Settings

Autofit settings control how the display of virtual machines adjusts to fit the Workstation Pro window.

To configure autofit settings, select **Edit > Preferences > Display**.

Table 10-7. Autofit Settings

Setting	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.

Configuring Full Screen Settings

Full screen settings control how the host system and guest operating system display settings interact when you enter full screen mode. In full screen mode, the virtual machine display fills the screen and you cannot see the borders of the Workstation Pro window.

To configure full screen settings, select **Edit > Preferences > Display**.

Table 10-8. Full Screen Settings

Setting	Description
Autofit guest	Change the virtual machine settings to match the application window when the application window is resized.
Center guest (no resolution change)	The host system and virtual machines retain their own display settings when you are in full screen mode.

Configuring Menu and Toolbar Settings

Menu and toolbar settings control how the menus and toolbars appear when Workstation Pro is in full screen and windowed mode.

To configure menu and toolbar settings, select **Edit > Preferences > Display**.

Table 10-9. Menu and Toolbar Settings

Setting	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.
Use a single button for stretch controls	When this setting is selected, the **Keep Aspect Ratio Stretch** and **Free Stretch** display controls appear on the toolbar as a single button with a drop-down menu. When this setting is deselected, each stretch control appears as a separate button on the toolbar.
Combine toolbar with menu bar in windowed mode	Show the Workstation Pro menus and toolbar on a single bar when Workstation Pro is in windowed mode.
Combine tabs with toolbar in full screen	Show the tabs and toolbar in a single bar when Workstation Pro is in full screen mode.
Show toolbar edge when unpinned in full screen	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.

Configuring Workstation Pro Color Theme Settings

The Color Theme setting controls how the Workstation Pro main window appears on a Windows 10 host system.

Note The Color Theme setting is only available on Windows 10 1809 or later host systems.

Setting	Description
System (use app mode of HOS)	The Workstation Pro window appears consistent with Windows 10 host's app mode color settings. This is the default setting.
Light	The Workstation Pro window is set to the light mode theme.
Dark	The Workstation Pro window is set to the dark mode theme.

Configuring USB Device Connection Behavior

This feature is only available for Workstation Pro on a Windows host. You can configure Workstation Pro to behave in one of the following ways when you connect a new USB device to the Windows host machine.

- Ask you which machine you want to connect the device to.
- Automatically connect the device to the host.
- Automatically connect the device to the foreground virtual machine.

To configure USB device connection settings, select **Edit > Preferences > USB**. For an overview of connecting USB devices to virtual machines, see Connecting USB Devices to Virtual Machines. For specific information about configuring the USB device connection settings, see Configure USB Device Connection Behavior.

Configuring Software Update Preference Settings

You can use software update preference settings to configure when Workstation Pro checks for the availability of new versions of software components and VMware Tools updates. You can also configure a proxy server to connect to the VMware Update Server.

To configure software update preference settings, select **Edit > Preferences > Updates**.

What to read next

- Configuring Software Updates Settings

  Software updates settings control when Workstation Pro downloads software updates to the host system and whether it uses a proxy server to connect to the VMware Update Server.

- Configuring Connection Settings for a Proxy Server

  You can configure connection settings to use a proxy server to connect to the VMware Update Server.

Configuring Software Updates Settings

Software updates settings control when Workstation Pro downloads software updates to the host system and whether it uses a proxy server to connect to the VMware Update Server.

Table 10-10. Software Update Preference Settings

Setting	Description
Check for product updates on startup	Check for new versions of the application and installed components when you start Workstation Pro. This setting is selected by default.
Check for new software components as needed	Check for a new version of a component when a component, such as VMware Tools, is required. When this setting is selected, Workstation Pro verifies if a new version is available to download and install.
Download All Components Now	Manually download all of the available software components to the host system. Click this button if you are planning to use a virtual machine at a later time when you do not have access to the Internet.
Connection Settings	Click this button to configure a proxy server to connect to the VMware Update Server.
Automatically update VMware Tools on virtual machine	Install the latest version of VMware Tools when you power on a virtual machine or shut down the guest operating system. You can override this setting for specific virtual machines.

Understanding the Automatic Software Update Process

When you turn on automatic software updates, you are always aware of the latest releases from VMware.

By keeping your software up-to-date, you can take advantage of new product features and performance improvements, ensure that your system includes the latest patches, and obtain timely support for new guest operating systems. You can turn on the automatic software update feature when you install Workstation Pro or by configuring Workstation Pro preference settings. You can turn off the feature at any time.

To determine if software updates are available, the VMware software updates feature securely sends the following anonymous information to VMware.

- A universal unique identifier (UUID), which it uses to identify each individual system
- The product name, the product version, and the build number
- Your host operating system name, version, and the locale setting

The VMware software updates feature does not collect any personal data, such as your name, address, telephone number, or mail address. Your product license key and MAC address are not sent to VMware, and VMware does not store your IP address with the data that it receives from you.

VMware might use the information it receives from the software update feature for product planning purposes. VMware limits access to your data and uses industry-standard controls to protect your information, including physical access controls, Internet firewalls, intrusion detection, and network monitoring.

The information collected by the VMware software updates feature is handled in accordance with VMware Privacy Policy.

Configuring Connection Settings for a Proxy Server

You can configure connection settings to use a proxy server to connect to the VMware Update Server.

To configure proxy connection settings, select **Edit > Preferences > Updates** and click **Connection Settings**.

Table 10-11. Connection Settings

Setting	Description
No proxy	Do not use a proxy server.
Windows proxy settings	(Windows hosts only) Workstation Pro 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.
System proxy settings	(Linux hosts only) Workstation Pro uses the host proxy settings to access the VMware Update Server.
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.
Username and **Password**	The username and password to use for proxy server authentication. On Windows hosts, if either the **Username** or **Password** text box is blank, Workstation Pro does not use either value. On Linux hosts, if either the **Username** or **Password** text box is blank, Workstation Pro uses the username and password set in the gnome settings.

You must restart Workstation Pro for proxy setting changes to take effect.

Join or Leave the Customer Experience Improvement Program

The VMware Customer Experience Improvement Program (CEIP) provides information to VMware. VMware uses the information to improve its products and services, to fix problems, and to advise you on how best to deploy and use VMware products.

Workstation Pro participates in the VMware CEIP. Information about the data collected through CEIP and how VMware uses it are in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

The CEIP appears the first time you start Workstation Pro after you install the product. You must then make a selection. You can change your selection any time afterwards.

Procedure

1 Start Workstation Pro.

2 Select **Edit > Preferences**.

3 Click **Feedback**.

4 Join or leave the CEIP depending on the participation preference currently selected.

Option	Description
Join	Select **Join the VMware Customer Experience Improvement Program.**
Leave	Unselect **Join the VMware Customer Experience Improvement Program.**

Configuring Workstation Pro Memory Preference Settings

You can use memory preference settings to configure the amount of memory that Workstation Pro is allowed to reserve for all running virtual machines. You can also configure settings to control memory swapping.

To configure memory preference settings, select **Edit > Preferences > Memory**.

What to read next

- Configuring Reserved Memory

  The reserved memory setting specifies the maximum amount of host RAM that Workstation Pro is allowed to reserve for all running virtual machines. Reserved memory is not allocated in advance.

- Configuring Additional Memory Settings

  The additional memory settings control how the memory manager on the host system swaps virtual machines out of physical RAM.

Configuring Reserved Memory

The reserved memory setting specifies the maximum amount of host RAM that Workstation Pro is allowed to reserve for all running virtual machines. Reserved memory is not allocated in advance.

To configure the reserved memory setting, select **Edit > Preferences > Memory** and move the **Reserved memory** slider to select the reserved memory amount.

If you set the reserved memory value too high, the CPU might thrash if you run other applications on the host. If you set the value too low, virtual machines might perform poorly, and you cannot run as many virtual machines at the same time.

The maximum amount of memory for each virtual machine is 64GB.

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

Configuring Additional Memory Settings

The additional memory settings control how the memory manager on the host system swaps virtual machines out of physical RAM.

To configure additional memory settings, select **Edit > Preferences > Memory**.

Table 10-12. Additional Memory Settings

Setting	Description
Fit all virtual machine memory into reserved host RAM	Select this option to impose the tightest restrictions on the number and memory size of virtual machines that can run at a given time. Because the virtual machines are running entirely in RAM, they have the best possible performance.
Allow some virtual machine memory to be swapped	The host operating system can swap a moderate amount of virtual machine memory to disk. Select this setting to allow the number or memory size of virtual machines to be increased so that they can run on the host system at a given time. This setting might result in reduced performance if virtual machine memory must be shifted between RAM and disk.
Allow most virtual machine memory to be swapped	The host operating system can swap as much virtual machine memory to disk as necessary. When this setting is selected, you can run more virtual machines with more memory than when the **Allow some virtual machine memory to be swapped** setting is selected. This setting might result in reduced performance if virtual machine memory must be shifted between RAM and disk.

Configuring Workstation Pro Priority Preference Settings

You can use priority preference settings to turn on or off the background snapshots. On Windows hosts, you can also use priority preference settings to configure process priorities.

To configure priority preference settings, select **Edit > Preferences > Priority**.

What to read next

- Configuring Process Priorities on Windows Hosts

  The default process priority settings control the priority that the Windows process scheduler gives to the virtual machines that run on the host system. These settings affect the performance of both the host system and the virtual machines running on it.

- Configuring Background Snapshots

  Background snapshots settings control how Workstation Pro handles background snapshots.

Configuring Process Priorities on Windows Hosts

The default process priority settings control the priority that the Windows process scheduler gives to the virtual machines that run on the host system. These settings affect the performance of both the host system and the virtual machines running on it.

To configure default process priority settings, select **Edit > Preferences > Priority**.

Process priority settings apply to Windows hosts only. You can override these settings for specific virtual machines.

Table 10-13. Default Process Priority Settings

Setting	Description
Input grabbed	Select the priority for virtual machines when their keyboard and mouse input is grabbed.
Input ungrabbed	Select the priority for virtual machines when their keyboard and mouse input is not grabbed.

The **Normal** setting means that the processes within virtual machines contend equally for resources with all other processes running on the host.

Configuring Background Snapshots

Background snapshots settings control how Workstation Pro handles background snapshots.

To configure background snapshot settings, select **Edit > Preferences > Priority**.

Taking a snapshot is not an instantaneous process. When background snapshots are enabled, you can continue to work while Workstation Pro completes the snapshot process in the background.

Table 10-14. Snapshot Setting Options

Option	Description
Take snapshots in the background when possible	Enable background snapshots.
Restore snapshots in the background when possible	Enable the restoration of background snapshots.

Virtual machines must be powered off and then powered on, rather than restarted, for background snapshot changes to take effect.

Configuring Device Settings for Windows Hosts

You can use device settings to configure removable media settings for Windows hosts.

To configure device settings for Windows hosts, select **Edit > Preferences > Devices**.

Configuring the Autorun Feature on Windows Hosts

On Windows hosts, the Autorun feature causes CDs and DVDs to run automatically when you insert them in to the CD-ROM or DVD drive on the host system.

To turn on or off the Autorun feature on a Windows host system, select **Edit > Preferences > Devices**. You must be logged in as a member of the Administrators group to change this setting.

To run Autorun programs, some operating systems poll the CD-ROM drive every second or so to determine whether a disk is present. Polling can cause Workstation Pro to connect to the host CD-ROM or DVD drive, which can make the drive spin up while the virtual machine appears to pause. Because this behavior is undesirable, the Autorun feature is turned off by default in Workstation Pro.

Note You can use Windows Explorer to open a disk on the host system when the Autorun feature is turned off.

Configuring Virtual Machine Option Settings

11

Virtual machine options settings control characteristics of individual virtual machines, such as how files are transferred between the host and guest operating system and what happens to a guest operating system when you exit Workstation Pro. Some virtual machine options override similar Workstation Pro preference settings.

To configure virtual machine option settings for a selected virtual machine, select **VM > Settings** and click the **Options** tab.

Read the following topics next:

- Configuring General Option Settings for a Virtual Machine
- Configuring Power Settings for a Virtual Machine
- Configuring Snapshot Options for a Virtual Machine
- Configuring AutoProtect Options for a Virtual Machine
- Configuring Guest Isolation Options for a Virtual Machine
- Configuring Tablet Sensor Input Options for a Virtual Machine
- Configuring VMware Tools Options for a Virtual Machine
- Configuring a Virtual Machine as a VNC Server
- Configuring Unity Mode for a Virtual Machine
- Configuring Appliance Details for a Virtual Machine
- Configuring Autologin for a Virtual Machine
- Configuring Advanced Options for a Virtual Machine
- Configuring Access Control for a Virtual Machine

Configuring General Option Settings for a Virtual Machine

General option settings include the virtual machine name, the guest operating system type and version, and the location of the directory where virtual machine files are stored.

To configure general option settings for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **General**.

What to read next

- Changing a Virtual Machine Name

  You can change the name of a virtual machine. Changing the name of the virtual machine does not change the name of this directory, nor does it rename the virtual machine files on the host. Workstation Pro uses the original name of the virtual machine to create the directory where virtual machine files are stored.

- Changing the Guest Operating System

  You can change the guest operating system or operating system version for a virtual machine. You might want to change the guest operating system for a virtual machine when you upgrade the guest operating system or if you specified the wrong operating system version when you created the virtual machine.

- Changing the Virtual Machine Working Directory

  You can change the working directory for a virtual machine. The working directory is where Workstation Pro stores suspended state (`.vmss`), snapshot (`.vmsn`), and virtual machine paging (`.vmem`) files. By default, the working directory is where the virtual machine files are stored.

Changing a Virtual Machine Name

You can change the name of a virtual machine. Changing the name of the virtual machine does not change the name of this directory, nor does it rename the virtual machine files on the host. Workstation Pro uses the original name of the virtual machine to create the directory where virtual machine files are stored.

To specify a new name for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **General**.

Changing the Guest Operating System

You can change the guest operating system or operating system version for a virtual machine. You might want to change the guest operating system for a virtual machine when you upgrade the guest operating system or if you specified the wrong operating system version when you created the virtual machine.

To select a new guest operating system or operating system version for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **General**.

When you change the operating system type, the virtual machine configuration file is changed but the guest operating system is not changed. To change the guest operating system, you must obtain the operating system software and upgrade the guest operating system.

The virtual machine must be powered off when you change these settings.

Changing the Virtual Machine Working Directory

You can change the working directory for a virtual machine. The working directory is where Workstation Pro stores suspended state (`.vmss`), snapshot (`.vmsn`), and virtual machine paging (`.vmem`) files. By default, the working directory is where the virtual machine files are stored.

Note You cannot change the working directory for a remote virtual machine.

To specify a new working directory for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **General**.

You might want to change the working directory in the following situations.

- To organize all of your snapshots in a separate directory, you can create a directory in another location. If you plan to take many snapshots and use a large amount of disk space, place the working directory on a disk with a lot of space.
- To run a virtual machine that is stored on a network share or iPod, which might slow performance, you can change the working directory to your local hard disk. Then you can take a snapshot, power on the virtual machine, use it, and discard the snapshot when you are finished. The virtual machine then reverts to its original state.
- To create a paging file on a fast disk with a lot of disk space but leave the virtual disk and configuration file on a different disk, you can change the working directory so that it is located on the fast disk.

Changing the working directory does not change the directory where Workstation Pro stores the virtual machine configuration (`.vmx`) file and log files.

The virtual machine must be powered off when you change this setting.

Configuring Power Settings for a Virtual Machine

You can configure power options and power control settings for a virtual machine.

To change power options and settings for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Power**.

What to read next

- Configuring Power Options for a Virtual Machine

  Power options control how a virtual machine behaves after it is powered off, closed, or suspended.

- Configuring Power Controls for a Virtual Machine

  Power control settings affect the behavior of the stop, suspend, start, and reset buttons for a virtual machine. The behavior that you select appears in a tooltip when you mouse over the associated button. Power control settings also determine which power options appear in the context menu when you right-click the virtual machine in the library.

Configuring Power Options for a Virtual Machine

Power options control how a virtual machine behaves after it is powered off, closed, or suspended.

To configure power options for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Power**.

Note You cannot configure power options for a remote virtual machine.

Table 11-1. Power Options

Option	Description
Enter full screen mode after powering on	The virtual machine window enters full screen mode after it is powered on.
Close after powering off or suspending	The virtual machine tab 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.

Configuring Power Controls for a Virtual Machine

Power control settings affect the behavior of the stop, suspend, start, and reset buttons for a virtual machine. The behavior that you select appears in a tooltip when you mouse over the associated button. Power control settings also determine 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 it 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.

To change power controls for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Power**.

Table 11-2. Power Controls

Control	Description
Stop	**Power Off** (Hard option) Workstation Pro powers off the virtual machine abruptly with no consideration for work in progress. **Shut Down Guest** (Soft option) Workstation Pro 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 shut-down signal from Workstation Pro. If the guest operating system does not respond to the signal, shut down from the guest operating system as you would a physical machine.
Suspend	**Suspend** (Hard option) Workstation Pro suspends the virtual machine and leaves it connected to the network. **Suspend Guest** (Soft option) Workstation Pro 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.
Start	**Power On** (Hard option) Workstation Pro starts the virtual machine. **Start Up Guest** (Soft option) Workstation Pro 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. **Note** You cannot configure this setting for a remote virtual machine.
Reset	**Reset** (Hard option) Workstation Pro resets the virtual machine abruptly with no consideration for work in progress. **Restart Guest** (Soft option) Workstation Pro 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.

Configuring Snapshot Options for a Virtual Machine

When you take a snapshot, Workstation Pro preserves the state of a virtual machine so that you can return to the same state repeatedly. A snapshot captures the entire state of the

virtual machine at the time you take the snapshot, including the contents of the virtual machine memory, the virtual machine settings, and the state of all virtual disks.

To configure snapshot options for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Snapshots**.

Table 11-3. Snapshot Options

Option	Description
Just power off	Power off the virtual machine without making any changes to snapshots.
Revert to snapshot	Revert to the parent snapshot of the current state of the virtual machine. When you revert to a snapshot, you return the memory, settings, and virtual disks of the virtual machine to the state that they were in when you took the snapshot.
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. **Note** You cannot configure this option for a remote virtual machine.
Ask me	Prompts you to power off or take a snapshot when the virtual machine is powered off.

Configuring AutoProtect Options for a Virtual Machine

The AutoProtect feature preserves the state of a virtual machine by taking snapshots at regular intervals. You can also take manual snapshots at any time.

The AutoProtect feature has certain restrictions.

- Because AutoProtect takes snapshots only while a virtual machine is powered on, you cannot clone AutoProtect snapshots. You can clone a virtual machine only if it is powered off.
- AutoProtect snapshots are not taken in Workstation Player, even if AutoProtect is enabled for the virtual machine in Workstation Pro.
- You cannot configure the AutoProtect feature for a remote virtual machine.

To configure AutoProtect options for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **AutoProtect**.

Table 11-4. AutoProtect Options

Option	Description
Enable AutoProtect	When you enable the AutoProtect feature, an estimate of the minimum of amount of disk space used appears in the **Virtual Machine Settings** window. The Memory setting for the virtual machine affects this minimum. The more virtual memory that a virtual machine has, the more disk space is available for AutoProtect snapshots.
AutoProtect interval	Select the interval of time between AutoProtect snapshots. **Half-Hourly** Snapshots are taken every half hour. **Hourly** Snapshots are taken every hour. **Daily** Snapshots are taken daily. The interval between AutoProtect snapshots is measured only when the virtual machine is powered on. For example, if you set AutoProtect to take snapshots hourly and 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 that the virtual machine was powered off. Workstation Pro saves only one snapshot per tier, even if a snapshot matches more than one tier.
Maximum AutoProtect snapshots	Select the maximum number of snapshots to be retained. After the maximum number of AutoProtect snapshots is reached, Workstation Pro deletes the oldest AutoProtect snapshot each time a new AutoProtect snapshot is taken. Based on the settings that you enter, Workstation Pro retains a selection of AutoProtect snapshots over a range of time.

Configuring Guest Isolation Options for a Virtual Machine

With the guest isolation option, you can restrict file operations between the virtual machine and the host system, and between the virtual machine and other virtual machines.

To configure guest isolation options for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Guest Isolation**.

These restrictions apply:

- VMware Tools must be installed in the guest operating system to use guest isolation features.
- You cannot configure these options for a remote virtual machine.

Note The drag-and-drop and copy-and-paste operations are turned on by default. You might want to turn off these operations to prevent files from being accidentally transferred between the virtual machine and the host system.

Table 11-5. Guest Isolation Options

Option	Description
Enable drag and drop	When this check box is deselected, these operations are restricted. ■ Drag and drop files from the host system to a Linux, Windows, or Solaris guest operating system. ■ Drag and drop files from the guest operating system to the host system. ■ Drag files from a file manager to an application that supports drag and drop, or from applications such as zip file managers that support drag-and-drop extraction of individual files.
Enable copy and paste	When this check box is deselected, these operations are restricted. ■ Copy and paste text and files from the host system to a Linux, Windows, or Solaris 10 guest operating system. ■ Copy and paste from the guest operating system to the host system. ■ Copy and paste text and files from one virtual machine to another.

For virtual machines running Windows 8 or later guest operating systems, you can configure the guest operating system to pass tablet sensor data to a tablet. See Configuring Tablet Sensor Input Options for a Virtual Machine

Configuring Tablet Sensor Input Options for a Virtual Machine

You can configure a Windows 8 or later guest operating system to pass tablet sensor data to your host Windows 8 or later tablet. With this setting, you can use tablet applications inside your virtual machine.

Prerequisites

- Power off a Windows 8 or later virtual machine.

Note Tablet data is available only on guest operating systems and hosts running Windows 8 or later.

Procedure

1 Select the Windows 8 or later virtual machine and select **VM > Settings > Options > Guest Isolation**

2 Select the tablet sensor data to be shared with the Windows 8 or later host from the **Share sensor input** section.

Option	Description
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**.

Configuring VMware Tools Options for a Virtual Machine

You can configure how VMware Tools is updated on a virtual machine. You can also configure whether the clock on the guest operating system is synchronized with the clock on the host.

VMware Tools Update Options

The virtual machine VMware Tools update options override the Workstation Pro preferences for automatically updating VMware Tools on Linux and Windows guest operating systems.

To configure VMware Tools updates for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **VMware Tools**.

Note Automatic updates are not supported for versions of VMware Tools included in virtual machines created with older versions of VMware products, such as Workstation 5.5 and earlier or VMware Server 1.x.

Table 11-6. VMware Tools Update Options

Option	Description
Update manually (do nothing)	You must update VMware Tools manually. A message appears on the status bar of the guest operating system when a new version of VMware Tools is available.
Update automatically	VMware Tools is updated automatically when a new version is available. The status bar indicates when an update is in progress.
Use application default (currently update automatically)	Use the default VMware Tools update behavior. **Note** You cannot configure this option for a remote virtual machine.

To install a VMware Tools update, use the same procedure that you used for installing VMware Tools the first time.

Time Synchronization

If you turn on the VMware Tools time synchronization feature, VMware Tools checks once every minute to determine whether the clocks on the guest and host operating systems still match. If not, the clock on the guest operating system is synchronized to match the clock on the host.

Native time synchronization software, such as Network Time Protocol (NTP) for Linux and the Mac OS X, or Microsoft Windows Time Service (Win32Time) for Windows, is typically more accurate than VMware Tools periodic time synchronization and is therefore preferred.

Configuring a Virtual Machine as a VNC Server

You can configure a virtual machine so that VNC clients can access it remotely. You do not need to install specialized VNC software in the virtual machine.

To configure Virtual Network Computing (VNC) client access for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **VNC Connections**.

Note You cannot configure VNC client access for a remote virtual machine.

Table 11-7. Remote Display Options

Option	Description
Enable VNC	VNC clients can access the virtual machine.
Port	Select a unique port number for the virtual machine. A unique port number is required to connect to multiple virtual machines on the same host. Use a port number in the range 5901 to 6001. The default port is 5900. **Important** Make sure that you specify an available port number. The VMware Management Interface uses ports 8333 and 8222. The VMware Workstation Server service uses port 443 by default. On Linux, only the root user can listen to ports up to port number 1024.
Password	The password to use to connect to the virtual machine from a VNC client. It can be up to eight characters long. Because the password is not encrypted when the VNC client sends it, do not use a password that you use for other systems.
View VNC Connections	Click this button to see a list of the VNC clients that are connected to the virtual machine.

Configuring Unity Mode for a Virtual Machine

In virtual machines that have Windows XP or later guest operating systems, you can switch to Unity mode to display applications directly on the host system desktop. Open applications in Unity mode appear on the taskbar in the same way as open host system applications.

To configure Unity mode settings for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Unity**.

Note You cannot configure Unity mode settings for a remote virtual machine.

Table 11-8. Unity Mode Options

Setting	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	To help distinguish between the application windows that belong to various virtual machines, use a custom color in window borders. 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 Windows hosts, click **Choose color** to use the color chooser.
Enable applications menu	The virtual machine **Start** or **Applications** menu appears on the host system desktop. When you can access the virtual machine **Start** or **Applications** menu from the host machine desktop, you can start applications in the virtual machine that are not open in Unity mode. If you do not enable this setting, you must exit Unity mode to display the virtual machine **Start** or **Applications** menu in the console view.

Configuring Appliance Details for a Virtual Machine

You can configure version and author information and enable an HTTP access port inside a virtual machine.

To configure appliance details for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Appliance Details**.

The virtual machine must be a Workstation 6.x or later virtual machine.

Note You cannot configure appliance details for a remote virtual machine.

Table 11-9. Application Details Options

Setting	Description
Version	(Optional) The virtual machine version, which appears in the upper right corner of the summary page.
Author	(Optional) The virtual machine author, which appears in the upper right corner of the summary page.
Access port inside virtual machine	The HTTP access port. When this check box is selected, the HTTP access port is enabled inside the virtual machine. You can also change the port number. The default HTTP port is 80.

Configuring Autologin for a Virtual Machine

You can configure the Autologin feature for virtual machines that have a Windows 2000 or later guest operating system. To use Autologin, the virtual machine must be powered on, you must have an existing user account on the local machine, and the latest version of VMware Tools must be installed.

To configure Autologin for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Autologin**.

Note You cannot configure the Autologin feature for a remote virtual machine.

When you enable Autologin, you must type your login credentials. If you type an incorrect or expired password, you must type your login credentials when you power on the virtual machine. To change your login credentials, select **Change User**.

Note When you enable Autologin or change your login credentials, Autologin settings are saved immediately. If you click **Cancel** in the Virtual Machine Settings dialog box, the changes applied to the Autologin settings are not affected.

Configuring Advanced Options for a Virtual Machine

Advanced options include process-priority settings, debugging settings, memory settings, an automated disk-cleanup setting, a virtualization-based security setting, firmware-type settings, and virtual-machine-file locations.

To configure advanced options for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Advanced**.

What to read next

- Configuring Process Priorities for a Virtual Machine

  Process priority settings control the priority that the Windows process scheduler gives to the virtual machine. Process priority settings apply to Windows hosts only. The default settings are specified in Workstation Pro priority preference settings.

- Gathering Debugging Information

  When it runs in debugging mode, a virtual machine collects information that helps VMware technical support resolve problems.

- Configuring Advanced Settings for a Virtual Machine

  You can configure advanced settings for the selected virtual machine to turn off memory page trimming, turn on Template mode, turn on automated disk cleanup, and turn on virtualization-based security (VBS).

- Configuring the Firmware Type for a Virtual Machine

  You can select the firmware-type options that the guest operating system supports.

Configuring Process Priorities for a Virtual Machine

Process priority settings control the priority that the Windows process scheduler gives to the virtual machine. Process priority settings apply to Windows hosts only. The default settings are specified in Workstation Pro priority preference settings.

To configure process priority settings for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Advanced**.

Note You cannot configure process priority settings for a remote virtual machine.

Table 11-10. Process Priority Options

Option	Description
Input grabbed	Select the priority for the virtual machine when its keyboard and mouse input is grabbed. The default setting is specified in Workstation Pro priority preference settings.
Input ungrabbed	Select the priority for the virtual machine when its keyboard and mouse input is not grabbed.

The **Normal** setting specifies that processes in the virtual machine contend equally for resources with all other processes running on the host.

Gathering Debugging Information

When it runs in debugging mode, a virtual machine collects information that helps VMware technical support resolve problems.

To configure debugging mode for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Advanced**. The debugging level is set in the **Gather debugging information** drop-down menu.

Table 11-11. Debugging Levels

Option	Description
None	Normal mode. No debugging information is gathered. When this mode is selected, the virtual machine runs faster than it does in the other modes. When the cause and remedy for the problem are found, return to normal mode by selecting **None**.
Full	Select this mode if the virtual machine crashes and you want to send the debugging logs to VMware technical support.
Statistics	Select this mode if the virtual machine runs very slowly under certain workloads. You can send the statistics file to VMware technical support.

If you select the **Full** option, you can select the **Gather verbose USB debugging information** check box for USB debugging purposes.

For local virtual machines, you can select **Log virtual machine progress periodically** to increase logging information for debugging and troubleshooting purposes. You cannot use this feature for remote virtual machines. When this setting is selected, you do not need to edit a configuration file or restart the virtual machine to extract more detailed logging for VMware technical support.

Configuring Advanced Settings for a Virtual Machine

You can configure advanced settings for the selected virtual machine to turn off memory page trimming, turn on Template mode, turn on automated disk cleanup, and turn on virtualization-based security (VBS).

To configure additional advanced options for a selected virtual machine, select **VM > Settings**, click the **Options** tab, and select **Advanced**.

Note You cannot configure these options for a remote virtual machine.

Table 11-12. Additional Advanced Options

Option	Description
Disable memory page trimming	Workstation Pro uses a memory trimming technique to return unused virtual machine memory to the host machine for other uses. While trimming usually has little effect on performance and might be needed in low-memory situations, the I/O caused by memory trimming can sometimes interfere with disk-oriented workload performance in a guest.
Log virtual machine progress periodically	When turned on, Workstation Pro includes information about your virtual machine's virtual CPU state, instruction pointer, and code segment registers in the log file. This is useful for troubleshooting or optimizing the performance of your virtual machine.
Enable Template mode (to be used for cloning)	When you create a linked clone of a virtual machine, the clone depends on the parent virtual machine to function. If a linked clone cannot access the parent virtual machine or the snapshot on which the clone is based, the clone no longer operates. You can avoid this problem by designating the parent virtual machine of a linked clone as a template. You typically must have write access to a virtual machine to clone it. A virtual machine that is designated as a clone template can be cloned by users who do not have write access to the template virtual machine. To protect linked clones, you cannot delete a template virtual machine. You cannot delete snapshots of the template.

Table 11-12. Additional Advanced Options (continued)

Option	Description
Clean up disks after shutting down this virtual machine	Instead of performing a manual disk cleanup of a virtual machine, by selecting **VM > Manage > Clean Up Disks**, you can configure the automated disk cleanup option. When selected, this option shrinks and defragments the virtual machine each time you shut down the virtual machine. Other power-off related operations, such as power off, suspend, restart, and reset do not trigger the automated disk cleanup. The automated disk cleanup option is only selectable on Workstation Pro on Windows host systems and for Windows guest operating systems. Also, the option is only selectable when VMware Tools is installed on the virtual machine and when the virtual machine is powered on. **Note** This option is not available for remote virtual machines. With this option selected, when you shut down the virtual machine the first time, Workstation Pro prompts you to accept the cleanup of the disks on the virtual machine. If you select **Do not show this message again** and click **Clean Up**, Workstation Pro performs the cleanup this time and in the future without issuing the prompt again. After the cleanup starts, the progress of the cleanup appears on the left side of the Workstation Pro status bar. You can terminate the cleanup task by closing the virtual machine tab and clicking **Yes**. After the cleanup finishes, a note appears in the message log and on the right side of the Workstation Pro status bar that reports the amount of disk space reclaimed.
Enable VBS (Virtualization Based Security) support	This option is only available for virtual machines that use hardware version 14 or later. With this option, Workstation Pro provides the technical support for Microsoft VBS feature in the virtual machine. You can then turn on and configure the Microsoft VBS feature in one of the following supported Windows guest operating systems. ■ Windows 10, version 1703 and later, Enterprise, 64-bit ■ Windows Sever 2016, version 1607 and later To use Windows 2016, version 1607 as the guest operating system, apply all Microsoft updates to the guest. VBS might not function in a Windows 2016 guest without the most current updates. VBS reinforces the security of Microsoft Hyper-V. When you turn on VBS, Workstation Pro configures the virtual machine with the following settings.

Option	Required Setting	Workstation Pro Virtual Machine Settings
Firmware type	UEFI	**Options > Advanced**
Enable secure boot	Enabled	**Options > Advanced**
Virtualize Intel VT-x/EPTor AMD-V/RVI	Enabled	**Hardware > Processors**
Virtualize IOMMU (IO memory management unit)	Enabled	**Hardware > Processors**

Table 11-12. Additional Advanced Options (continued)

Option	Description
	For VBS to run in the guest operating system, you must also perform configurations in the guest. See Microsoft documentation related to virtualization-based security.

Configuring the Firmware Type for a Virtual Machine

You can select the firmware-type options that the guest operating system supports.

If selectable, you can choose the BIOS or UEFI firmware type. If you select UEFI, depending on the guest operating system, you might be able to select **Enable secure boot** . See Configure a Firmware Type.

Configuring Access Control for a Virtual Machine

You can encrypt a virtual machine to protect the virtual machine and its configurations. Any user without encryption password can't use or configure the encrypted virtual machine.

- Encryption - Enter and confirm the new password, the VM will be encrypted. Remember this encryption password.
- Change password - For an encrypted VM, users with old password can change it to the new encryption password.
- Remove Encryption - For an encrypted VM, users with encryption password can remove the encryption and turn the VM into a normal VM.

Configuring Virtual Machine Hardware Settings

12

You can use virtual machine hardware settings to add, remove, and modify virtual devices for a virtual machine.

To configure hardware settings for a selected virtual machine, select **VM > Settings** and click the **Hardware** tab. When you select a device in the left pane, the configuration options for that device appear in the right pane.

Read the following topics next:

- Adding Hardware to a Virtual Machine
- Removing Hardware from a Virtual Machine
- Adjusting Virtual Machine Memory
- Configuring Virtual Machine Processor Settings
- Configuring and Maintaining Virtual Hard Disks
- Configuring CD-ROM and DVD Drive Settings
- Configuring Floppy Drive Settings
- Configuring Virtual Network Adapter Settings
- Configuring USB Controller Settings
- Configuring Sound Card Settings
- Configuring Parallel Port Settings
- Configuring Serial Port Settings
- Configuring Generic SCSI Device Settings
- Configuring Display Settings
- Installing a Guest Operating System on a Physical Disk or Unused Partition

Adding Hardware to a Virtual Machine

You can use virtual machine hardware settings to add hardware to an existing virtual machine.

To add hardware to a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and click **Add**.

Note You cannot add hardware to a virtual machine while it is in a suspended state.

The **Add Hardware** wizard prompts you to select the type of device that you want to add and to specify device-specific configuration settings. You can modify many of the configuration settings after the device is created by changing virtual machine hardware settings.

You can add the following types of devices to a virtual machine.

Virtual hard disks

A virtual hard disk is a set of files that appears as a physical disk drive to the guest operating system. You can configure a virtual hard disk as an IDE, SCSI, SATA, or NVMe device. You can add up to 4 IDE devices, up to 60 SCSI devices, up to 120 SATA devices (4 controllers and 30 devices per controller), and up to 256 NVMe devices (4 controllers and 64 devices per controller) to a virtual machine. You can also give a virtual machine direct access to a physical disk.

CD-ROM and DVD drives

You can configure a virtual CD-ROM or DVD drive as an IDE, SCSI, or SATA device. You can add up to 4 IDE devices, up to 60 SCSI devices, and up to 120 SATA devices (4 controllers and 30 devices per controller). You can connect virtual CD-ROM and DVD drives to a physical drive on the host system or to an ISO image file.

Floppy drives

You can add up to two floppy drives. A virtual floppy drive can connect to a physical drive on the host system, to an existing floppy image file, or to a blank floppy image file.

Network adapters

You can add up to 10 virtual network adapters to a virtual machine.

USB controller

You can add one USB controller to a virtual machine. A virtual machine must have a USB controller to use USB devices or smart card readers. For smart card readers, a virtual machine must have a USB controller regardless of whether the smart card reader is actually a USB device.

Sound card

If the host system is configured for sound and has a sound card installed, you can enable sound for virtual machines.

Parallel (LPT) ports

You can attach up to three bidirectional parallel ports to a virtual machine. Virtual parallel ports can output to parallel ports or to files on the host operating system.

Serial (COM) ports

You can add up to four serials ports to a virtual machine. Virtual serial ports can output to physical serial ports, files on the host operating system, or named pipes.

Generic SCSI devices

You can add up to 60 SCSI devices to a virtual machine. A generic SCSI device gives the guest operating system direct access to a SCSI device connected to the host system. Generic SCSI devices can include scanners, tape drives, CD-ROM drives, and DVD drives.

Removing Hardware from a Virtual Machine

You can remove certain types of hardware from a virtual machine.

To remove hardware from a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, select the device, and click **Remove**.

Note You cannot remove hardware from a virtual machine while it is in suspended state.

You can remove the following types of devices from a virtual machine.

- Virtual hard disks
- CD-ROM and DVD drives
- Floppy drives
- Virtual network adapters
- USB controllers
- Sound cards
- Generic SCSI devices

You cannot remove the Memory, Processors, and Display device types.

You must power off a virtual machine before you remove a virtual network adapter, sound card, parallel port, serial port, or generic SCSI device. You must also power off Workstation 5 virtual machines before you remove a USB controller.

Adjusting Virtual Machine Memory

You can adjust the amount of memory that is allocated to a virtual machine. You must power off a virtual machine before you change its memory allocation setting.

To adjust the memory allocation for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and click **Memory**.

The Memory panel includes information to help you select the appropriate amount of memory for the virtual machine. The high end of the range is determined by the amount of memory that is 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.

The color-coded icons on the Memory panel indicate the maximum recommended memory, the recommended memory, and the guest operating system recommended minimum memory amounts. To adjust the memory, move the slider along the range of values, or type a value in the **Memory for this virtual machine** text box.

Note Allocating more than the maximum memory to a virtual machine might cause memory swapping. It can also negatively affect host system performance, including the ability to run Workstation Pro.

Configuring Virtual Machine Processor Settings

You can configure processor settings for a virtual machine, including the number of processors, the number of cores per processor, and the preferred execution mode for the virtualization engine.

To configure processor settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select **Processors**.

Table 12-1. Processor Settings

Setting	Description
Number of processors and **Number of cores per processor**	Select the number of processors and the number of cores per processor. Workstation Pro supports up to 16-way virtual Symmetric Multiprocessing (SMP) for guest operating systems running on multiprocessor host machines. You can assign processors and cores per processor to a virtual machine on any host machine that has at least two logical processors.
Virtualize Intel VT-x/EPT or AMD-V/RVI	Workstation Pro forces the virtual machine execution mode to VT-x/EPT or AMD-RVI. Physical Address Extension (PAE) mode must be enabled to use virtualized AMD-V/RVI. If the execution mode is not supported by the host system, virtualized VT-x/EPT or AMD/RVI is not available. If you migrate the virtual machine to another VMware product, virtualized VT-x/EPT or AMD-V/RVI might not be available. **Note** You cannot configure this setting for a remote virtual machine.

Table 12-1. Processor Settings (continued)

Setting	Description
Virtualize CPU performance counters	Turn on this feature if you plan to use performance monitoring applications such as VTune or OProfile to optimize or debug software that runs inside the virtual machine. This feature is available only if the virtual machine compatibility is Workstation 9 or later.
Virtualize IOMMU (IO memory management unit)	Select this feature to provide the Intel Virtualization Technology for Directed I/O for virtual machines. **Note** You cannot configure this setting for a remote virtual machine. When you enable virtualization-based security (VBS) for a virtual machine, Workstation Pro automatically selects the **Virtual IOMMU** feature for you.

Configuring and Maintaining Virtual Hard Disks

You can configure virtual hard disk node and mode settings. You can also use command in the **Utilities** menu to perform common disk maintenance tasks, such as defragmenting, compacting, and expanding a disk.

To perform actions on a virtual hard disk for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the virtual hard disk.

What to read next

- Defragmenting Virtual Hard Disks

  Like physical disk drives, virtual hard disks can become fragmented. Defragmenting disks rearranges files, programs, and unused space on the virtual disk so that programs run faster and files open more quickly. Defragmenting does not reclaim unused space on a virtual disk.

- Expanding Virtual Hard Disks

  Expanding a virtual hard disk adds storage space to the virtual machine.

- Compacting Virtual Hard Disks

  Compacting a virtual hard disk can reclaim unused space in the virtual disk. Modern disks and operating systems are much more efficient at managing disk space than in the recent past. Therefore, do not expect the compacting procedure to return large amounts of disk space to the host drive.

- Changing Virtual Hard Disk Node and Mode Settings

  You can change virtual hard disk node and mode settings.

Defragmenting Virtual Hard Disks

Like physical disk drives, virtual hard disks can become fragmented. Defragmenting disks rearranges files, programs, and unused space on the virtual disk so that programs run faster and files open more quickly. Defragmenting does not reclaim unused space on a virtual disk.

There must be adequate free working space on the host system to defragment a virtual hard disk. If the disk is contained in a single file, for example, you need free space equal to the size of the disk file. Other virtual hard disk configurations require less free space. You cannot defragment a virtual hard disk while it is mapped or mounted.

To defragment a virtual hard disk for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, select the virtual hard disk, and select **Defragment** from the **Utilities** menu.

Note Defragmenting a virtual hard disk can take several minutes.

Expanding Virtual Hard Disks

Expanding a virtual hard disk adds storage space to the virtual machine.

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 7 and later, and many versions of Linux, provide built-in disk management tools that can resize partitions. Third-party disk management tools are also available, such as Symantec/Norton PartitionMagic, EASEUS Partition Master, Acronis Disk Director, and the open-source tool GParted.

When you expand the size of a virtual hard disk, partition and file-system size are not affected.

To expand a virtual hard disk for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, select the virtual hard disk, and select **Expand** from the **Utilities** menu.

Note As an alternative to expanding a virtual hard disk, you can add a new virtual hard disk to the virtual machine.

Compacting Virtual Hard Disks

Compacting a virtual hard disk can reclaim unused space in the virtual disk. Modern disks and operating systems are much more efficient at managing disk space than in the recent past. Therefore, do not expect the compacting procedure to return large amounts of disk space to the host drive.

You cannot compact a virtual hard disk if disk space is preallocated or if the virtual hard disk is mapped or mounted.

To compact a virtual hard disk for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, select the virtual hard disk, and select **Compact** from the **Utilities** menu.

Changing Virtual Hard Disk Node and Mode Settings

You can change virtual hard disk node and mode settings.

To change the node and mode settings for a virtual hard disk on a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, select the virtual hard disk, and click **Advanced**. By default, changes are immediately written to the disk. The data on the disk is saved when you take a snapshot of the virtual machine.

Table 12-2. Virtual Hard Disk Node and Mode Settings

Setting	Description
Virtual device node	Select the SCSI, IDE, SATA, or NVMe device identifier to use for the drive. For example, if you select SCSI 0:2, the guest operating system detects the drive as ID 2 on controller 0. You determine whether the virtual disk is seen as a SCSI, IDE, SATA, or NVMe device at the time that you create it.
Independent	If the **Independent** check box is unavailable, the virtual machine might have snapshots. After you delete the snapshots, the check box becomes available. **Caution** Independent disks do not participate in snapshots. Only select **Independent** mode for a disk in a virtual machine if you are prepared to give up the ability to take snapshots of the virtual machine when powered on. Although independent disks are not commonly used, they are useful in specific situations. For example, you have a virtual machine with two virtual disks. The second disk is configured to hold the Linux swap file or the Windows page file. The data on this disk has no value once the virtual machine is powered off. Therefore, you have no need to save the data from the second disk in a snapshot of the virtual machine. You can economize host disk space by not storing that data when a snapshot is taken. Accomplish this economy of host disk space by making the second disk independent. Specify independent disks as **Persistent** or **Nonpersistent**. While the virtual machine is running, a non-persistent disk stores all of the changes made to a disk in a separate file. When the virtual machine is shut down, the changes are discarded. Discarding the changes is useful in certain situations. For example, you have a virtual machine configured for a school setting or kiosk. The virtual machine has all the necessary software loaded, such as browsers, programming tools, computer-aided learning software, and so on. Students can use the virtual machine normally during the day. When the virtual machine is powered off at the end of the day, all changes made are discarded. When the virtual machine is powered on the following day, the non-persistent disk is exactly as it was at the beginning of the previous day. The disk contains no new malware or misconfigured software. Students can save their work to a USB thumb drive or network location as needed.

Configuring CD-ROM and DVD Drive Settings

You can configure CD-ROM and DVD drive settings, including the virtual device node and legacy emulation modes.

To configure CD-ROM and DVD drive settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the drive.

What to read next

- Configuring CD-ROM and DVD Drive Status and Connection Settings

  Device status and connection settings control when a CD-ROM or DVD drive is connected to a virtual machine, whether to use a specific drive or allow Workstation Pro to detect a drive, and whether to use an ISO image file instead of a physical drive.

- Changing Virtual Device Node and Legacy Emulation Settings

  You can use the advanced settings to change the virtual device node and legacy emulation settings for a CD-ROM or DVD drive. You must power off the virtual machine before you change these settings.

Configuring CD-ROM and DVD Drive Status and Connection Settings

Device status and connection settings control when a CD-ROM or DVD drive is connected to a virtual machine, whether to use a specific drive or allow Workstation Pro to detect a drive, and whether to use an ISO image file instead of a physical drive.

To configure device status and connection settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the drive.

Table 12-3. Device Status and Connection Settings

Setting	Description
Connected	Connect the drive or ISO image file while the virtual machine is running.
Connect at power on	Connect the drive or ISO image path when you power on the virtual machine.
Connection	Select the location of the physical drive or ISO image file. **Remote Server** (Remote virtual machine only) The physical drive or ISO image file is located on the remote host. **Local Client** (Remote virtual machine only) The physical drive or ISO image file is located on the local host. **Local (Across Sessions)** (Shared virtual machine only) The physical drive or ISO image file can be used across multiple sessions. **Local (Single Session)** (Shared virtual machine only) The physical drive or ISO image file can be used only in this session.

Table 12-3. Device Status and Connection Settings (continued)

Setting	Description
Use physical drive	Select a specific drive or select **Auto detect** to allow Workstation Pro to detect a drive to use.
Use ISO image file	Specify or select an ISO image file for the virtual machine to use.

To turn on or off the access to a CD-ROM or DVD drive while a virtual machine is running, select the virtual machine, select **VM > Removable Devices > CD/DVD**, and select **Disconnect** or **Connect**.

Changing Virtual Device Node and Legacy Emulation Settings

You can use the advanced settings to change the virtual device node and legacy emulation settings for a CD-ROM or DVD drive. You must power off the virtual machine before you change these settings.

To configure virtual device and legacy emulation settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, select the drive, and click **Advanced**.

Use the settings to select which SCSI, IDE, SATA, or NVMe device identifier to use for the drive. For example, if you select SCSI 0:2, the guest operating system detects the drive as ID 2 on controller 0. You can select the IDE, SCSI, SATA, or NVMe node options regardless of the physical device type. For example, if the physical drive is an IDE device, you can select a SCSI node. In this case, the virtual machine detects the drive as a SCSI device.

If you select the **Legacy emulation** setting, the virtual hardware works as it did in an earlier release of Workstation Pro. By default, Workstation Pro attempts to make the advanced features of your drive available, but sometimes this setting might cause the drive to not work with the virtual machine. Selecting the **Legacy emulation** setting reverts Workstation Pro to the previous emulation mode for the drive. Legacy emulation is helpful for troubleshooting purposes.

Configuring Floppy Drive Settings

You can configure when a floppy drive is connected to a virtual machine, whether to use a specific drive or allow Workstation Pro to detect a drive, and whether to use an disk drive image file instead of a physical drive.

To configure floppy drive settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the floppy drive.

Table 12-4. Floppy Drive Settings

Setting	Description
Connected	Connect the drive or floppy image file while the virtual machine is running.
Connect at power on	Connect the floppy drive when you power on the virtual machine.

Table 12-4. Floppy Drive Settings (continued)

Setting	Description
Location	Select the location of the physical drive or floppy image file. **Remote Server** (Remote virtual machine only) The physical drive or floppy image file is located on the remote host. **Local Client** (Remote virtual machine only) The physical drive or floppy image file is located on the local host. **Local (Across Sessions)** (Shared virtual machine only) The physical drive or floppy image file can be used across multiple sessions. **Local (Single Session)** (Shared virtual machine only) The physical drive or floppy image file can be used only in this session.
Use a physical drive	Select a specific floppy drive or select **Auto detect** to allow Workstation Pro to detect a drive to use.
Use a floppy image file	Create or browse to a floppy image (`.img` or `.flp`) file. Select **Read only** to prevent changes from being made to the file.

To turn on or off the access to a floppy drive while a virtual machine is running, select the virtual machine, select **VM > Removable Devices > Floppy**, and select **Disconnect** or **Connect**.

Configuring Virtual Network Adapter Settings

You can configure when a virtual network adapter is connected to a virtual machine and the type of network connection that the adapter provides.

The type of network configuration that you can select depends on whether the virtual machine is a local, shared, or remote virtual machine.

To configure virtual network adapter settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the virtual network adapter.

What to read next

- Configuring Virtual Network Adapter Device Status Settings

  Device status settings control when a virtual network adapter is connected to a virtual machine.
- Configuring a Network Connection

  You can configure the type of network connection that a virtual network adapter provides.

- Configuring Virtual Network Adapter Advanced Settings

  You can use the advanced virtual network adapter settings to limit the bandwidth, specify the acceptable packet loss percentage, and create network latency for incoming and outgoing data transfers for a virtual machine.

Configuring Virtual Network Adapter Device Status Settings

Device status settings control when a virtual network adapter is connected to a virtual machine.

To configure virtual network adapter device status settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the virtual network adapter.

Table 12-5. Device Status Settings

Setting	Description
Connected	Connect the virtual network adapter while the virtual machine is running.
Connect at power on	Connect the virtual network adapter when you power on the virtual machine.

Configuring a Network Connection

You can configure the type of network connection that a virtual network adapter provides.

For a local virtual machine, you can configure bridged, NAT, or host-only networking, or you can select a custom network or LAN segment. For a remote virtual machine, you must select a custom network.

To configure a network connection for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the virtual network adapter.

What to read next

- Configuring Bridged Networking

  When you configure bridged networking, the virtual machine uses physical network adapters on the host system to connect a network.

- Configuring Network Address Translation

  When you configure Network Address Translation (NAT), the virtual machine shares the IP address and MAC address of the host system.

- Configuring Host-Only Networking

  When you configure host-only networking, Workstation Pro creates a virtual private network (VPN) connection between the virtual machine and the host system.

- Configuring a Custom Network Configuration

  A custom network is a network that you create by using the virtual network editor. You can select a custom network when you modify the network connection setting for a local virtual machine. For a remote virtual machine, you must select a custom network.

- Configuring LAN Segments

  When you select a LAN segment, the virtual machine uses a private network that can be shared with other virtual machines. LAN segments are useful for multitier testing, network performance analysis, and situations where virtual machine isolation are important.

Configuring Bridged Networking

When you configure bridged networking, the virtual machine uses physical network adapters on the host system to connect a network.

If the host system is on a network, bridged networking is often the easiest way to give a virtual machine access to that network.

With bridged networking, the virtual machine appears as an additional computer on the same physical Ethernet network as the host system. The virtual machine can transparently use the services available on the network, including file servers, printers, and gateways. Physical hosts and other virtual machines configured with bridged networking can also use the resources of the virtual machine.

When you use bridged networking, the virtual machine must have its own identity on the network. For example, on a TCP/IP network, the virtual machine must have its own IP address. Virtual machines typically acquire an IP address and other network details from a DHCP server. In some configurations, you might need to set the IP address and other details manually.

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 the same time. If the host system is set up to boot multiple operating systems and you run one or more of them in virtual machines, configure each operating system with a unique network address.

When the **Replicate physical connection state** option is selected, the IP address is automatically renewed when you move from one wired or wireless network to another. This setting is useful for virtual machines than run on laptops or other mobile devices.

Configuring Network Address Translation

When you configure Network Address Translation (NAT), the virtual machine shares the IP address and MAC address of the host system.

The virtual machine and the host system share the a single identity that is not visible outside the network. The virtual machine does not have its own IP address. Instead, a separate private network is set up on the host system and the virtual machine obtains an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. The VMware NAT device identifies incoming data packets that are intended for each virtual machine and sends them to the correct destination.

With NAT, a virtual machine can use many standard 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 systems. You can also connect to a TCP/IP network by using a Token Ring adapter on the host system.

In the default configuration, systems on the external network cannot initiate connections to the virtual machine. For example, the default configuration does not let you use the virtual machine as a Web server to send Web pages to systems on the external network. This limitation protects the guest operating system from being compromised before you can install security software.

By default, NAT is used when you use the **New Virtual Machine** wizard to create a virtual machine.

The virtual machine uses NAT to connect to the Internet or other TCP/IP network by using the networking connection on the host system. NAT works with Ethernet, DSL, and phone modems. A separate private network is set up on the host system. The virtual machine obtains an address on that network from the VMware virtual DHCP server.

Configuring Host-Only Networking

When you configure host-only networking, Workstation Pro creates a virtual private network (VPN) connection between the virtual machine and the host system.

A VPN is typically not visible outside the host system. Multiple virtual machines configured with host-only networking on the same host system are on the same network. The VMware DHCP server provides addresses on the network.

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. With this configuration, you can connect the virtual machine to a Token Ring or other non-Ethernet network.

Configuring a Custom Network Configuration

A custom network is a network that you create by using the virtual network editor. You can select a custom network when you modify the network connection setting for a local virtual machine. For a remote virtual machine, you must select a custom network.

A custom network can be connected to one or more external networks, or it can run entirely on the host system. You can use the virtual network editor to access multiple network cards in the host system and create multiple virtual networks.

For more information, see Chapter 13 Using the Virtual Network Editor.

Configuring LAN Segments

When you select a LAN segment, the virtual machine uses a private network that can be shared with other virtual machines. LAN segments are useful for multitier testing, network performance analysis, and situations where virtual machine isolation are important.

You cannot configure a LAN segment for a remote virtual machine.

If 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 Pro 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.

If you convert a team that was created in an earlier version of Workstation Pro, the LAN segment that was configured for the team appears in the **LAN segment** drop-down menu for each virtual machine.

You can click **LAN Segments** to create new LAN segments or delete and rename existing LAN segments. 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 the network.

Configuring Virtual Network Adapter Advanced Settings

You can use the advanced virtual network adapter settings to limit the bandwidth, specify the acceptable packet loss percentage, and create network latency for incoming and outgoing data transfers for a virtual machine.

The advanced virtual network adapter settings allow you to simulate a network environment that differs from your own.

To configure advanced virtual network adapter settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, select the virtual network adapter, and click **Advanced**.

Note You cannot configure advanced virtual network adapter settings for a remote virtual machine.

Table 12-6. Virtual Network Adapter Advanced Settings

Setting	Description
Bandwidth and **Kbps**	To 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. To 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. The default bandwidth setting for both incoming and outgoing data transfers is **Unlimited**.
Packet Loss (%)	The acceptable packet loss percentage for incoming or outgoing data transfers. The default setting is 0.0%.

Table 12-6. Virtual Network Adapter Advanced Settings (continued)

Setting	Description
Latency (ms)	To simulate network latency for incoming and outgoing data transfers, set the number of milliseconds (ms) of latency. The latency range is 0 to 2,000 ms. **Note** Expect actual network latency to be up to 10 ms above the number you set. For example, if you set latency at 200 ms, expect the actual latency to be between 200 to 210 ms.
MAC Address	To assign a new MAC address to the network adapter, either type a new address in this text box or click **Generate** to have Workstation Pro generate a new address.

Configuring USB Controller Settings

You can configure whether a USB controller supports isochronous USB and Bluetooth devices and whether human interface devices (HIDs) appear in the **Removable Devices** menu. On Linux host machines only, you can also configure whether a new USB device can be automatically connected to a virtual machine.

Note You typically cannot configure USB controller settings for a remote virtual machine.

To configure USB controller settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and click **USB Controller**.

Table 12-7. USB Controller Settings

Setting	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 This feature only appears when you use Workstation Pro on a Linux host.	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.

To connect or disconnect USB devices while a virtual machine is running, select the virtual machine and select **VM > Removable Devices**. With the two-port USB controller, you can connect to both USB 1.1 and USB 2.0 devices.

Important Before you unplug a USB device or select a removable device to disconnect a USB device from a virtual machine, follow the device manufacturer's procedures for safely unplugging the device from a physical computer.

Configuring Sound Card Settings

You can configure when a sound card is connected to a virtual machine. You can also configure whether a virtual machine uses a specific sound card or the default sound card in the host system.

To configure sound card settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and click **Sound Card**.

Note You cannot change sound card settings for a remote virtual machine.

Table 12-8. Sound Card Settings

Setting	Description
Connected	Connect the sound device while the virtual machine is running.
Connect at power on	Connect the sound device when you power on the virtual machine.
Use default host sound card	Make the virtual machine use the default sound card in the host system.
Specify host sound card	(Windows hosts only) Select a specific host sound card for the virtual machine to use.
Use physical sound card	(Linux hosts only) Select a specific host sound card to for the virtual machine to use.
Enable Echo Cancellation	Enable echo cancellation for the sound card.

Configuring Parallel Port Settings

You can configure when a parallel port is connected to a virtual machine and whether to send output to a physical port or to a file on the host system.

To configure parallel port settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the parallel port.

Table 12-9. Parallel Port Settings

Setting	Description
Connected	Connect the port while the virtual machine is running.
Connect at power on	Connect the port when you power on the virtual machine. If the guest operating system cannot access the parallel port device when you power on the virtual machine, deselect this setting. You can use the **Removable Devices** menu to enable access to the parallel port after the virtual machine is powered on.
Use a physical parallel port	Select a host parallel port for the virtual machine to use.
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.

Configuring Serial Port Settings

You can configure when a serial port is connected to a virtual machine. You can also configure whether to send output to a physical port or to a file on the host system, set up a direct connection between two virtual machines, and specify whether the guest operating system uses the port in polled mode.

To configure serial port settings for a selected virtual machine, select the virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the serial port.

Table 12-10. Serial Port Settings

Setting	Description
Connected	Connect the port while the virtual machine is running.
Connect at power on	Connect the port when you power on the virtual machine.
Use a physical serial port	Select a host serial port.
Use output file	Send output from the virtual serial port to a file on the host system. Either locate an existing output file or navigate to the desired directory and type a filename for the file to create.
Use named pipe or **Use socket (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.
Yield CPU on poll	The guest operating system uses the port in polled mode rather than interrupt mode. It yields processor time if its only task is to poll the virtual serial port. If the guest operating system uses the serial port in interrupt mode, do not select this setting. **Note** This setting is useful for developers who are using debugging tools that communicate over a serial connection. Selecting this setting can improve performance when the guest operating system uses the serial port in polled mode.

Configuring Generic SCSI Device Settings

You can configure when a generic SCSI device is connected to a virtual machine, specify the physical SCSI device to connect to on the host system, and select the SCSI identifier to use for the drive.

To configure generic SCSI device settings for a selected virtual machine, select **VM > Settings**, click the **Hardware** tab, and select the generic SCSI device.

Note You cannot configure a generic SCSI device for a remote virtual machine.

Table 12-11. Generic SCSI Device Settings

Setting	Description
Connected	Connect the device while the virtual machine is running.
Connect at power on	Connect the device when you power on the virtual machine.
Specify the physical SCSI device to connect to	Select a host SCSI device. (Windows hosts) Select a device. The menu shows the SCSI devices that are available on the host system. (Linux hosts) Type the name of the `/dev/sg` entry for the device to install in the virtual machine. For example, if the device is named `sga`, type `/dev/sga`.
Virtual device node	Select the SCSI device identifier to use for the drive. For example, if you select SCSI 0:2, the guest operating system sees the drive as ID 2 on controller 0. The virtual machine must be powered off when you change this setting.

Note For specific Windows guest operating systems, you might need to perform additional configuration steps to use a generic SCSI device.

Configuring Display Settings

You can specify monitor resolution settings, configure multiple monitors, and select accelerated graphics capabilities for a virtual machine.

To configure display settings for a virtual machine, select the virtual machine, select **VM > Settings**, click the **Hardware** tab, and select **Display** (local virtual machine) or **Video card** (remote virtual machine).

Note 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.

Table 12-12. Display Settings

Setting	Description
Accelerate 3D graphics	Select this setting if you run applications that use DirectX 9 or DirectX 10 accelerated graphics. Accelerated graphics capabilities apply to Windows XP or later guests on hosts running Windows or Linux. The virtual machine must be a Workstation 6.x or later virtual machine and must have VMware Tools installed from Workstation 7.x or later.
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. **Note** You cannot configure the resolution setting for a remote virtual machine.
Graphics memory	Select the maximum amount of guest memory that can be used for graphics memory using the drop down menu. The default value of video memory varies by guest OS.
Display scaling or **Display scaling, Stretch mode**	Workstation Pro presents the option that the selected guest operating system supports. ■ The Display scaling option turns on or off the display scaling. Windows 7 or later guests support this feature. ■ The Display scaling, Stretch mode option allows you to set the display stretch ratio for a virtual machine.

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 Pro supports physical disks up to 2 TB 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.

Using the Virtual Network Editor

13

You can use the virtual network editor to view and change key networking settings, add and remove virtual networks, and create custom virtual networking configurations. The changes that you make in the virtual network editor affect all virtual machines running on the host system.

On a Windows host, any user can view network settings, but only Administrator users can change them. On a Linux host, you must enter the root password to access the virtual network editor.

On Windows hosts, select **Edit > Virtual Network Editor** to start the virtual network editor in Workstation Pro. You can also select **Start > Programs > VMware > Virtual Network Editor** to start the virtual network editor from the host operating system.

Note **Import** and **Export** buttons are added to the **Virtual Network Editor** to import and export network configurations.

On Linux hosts, 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.

Important When you click **Restore Default** to restore the default network settings, all changes that you made to network settings after you installed Workstation Pro are permanently lost. Do not restore the default network settings when a virtual machine is powered on as this might cause damage to the bridged network.

Read the following topics next:

- Add a Bridged Virtual Network
- Add a Host-Only Virtual Network
- Rename a Virtual Network
- Change Automatic Bridging Settings
- Change NAT Settings
- Change DHCP Settings on a Windows Host
- Importing and Exporting Network Settings on Windows Host

Add a Bridged Virtual Network

If you installed Workstation Pro on a host system that has multiple network adapters, you can configure multiple bridged networks.

By default, virtual switch VMnet0 is mapped to a bridged network. You can create a custom bridged network on virtual switches VMnet2 to VMnet7. On Windows, you can also use VMnet19. On Linux, you can also use vmnet10 through vmnet255.

Important If you reassign a physical network adapter to a different virtual network, any virtual machine that used the original network is no longer bridged to the external network through that virtual 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 bridge to an automatically chosen adapter, the only adapter it can use was assigned to a different virtual network.

Prerequisites

- Familiarize yourself with bridged networking. See Configuring Bridged Networking for more information.
- Verify that a physical network adapter is available on the host system. By default, the VMnet0 virtual switch is set to use automatic bridging mode and bridges to all active physical network adapters on the host system. You can make a physical network adapter available by restricting the physical network adapters that are bridged to VMnet0. See Change Automatic Bridging Settings for more information.

Procedure

1. Select **Edit > Virtual Network Editor**.
2. Click **Add Network**.
3. Select a virtual switch.

   Workstation Pro assigns a subnet IP address to the virtual network adapter.
4. Select the new virtual network from the list and select **Bridged (connect VMs directly to the external network)**.
5. From the **Bridged to** menu, select a physical adapter on the host system to bridge to.

Option	Description
Automatic	Workstation Pro automatically bridges the virtual network to all active physical network adapters on the host system. The choice of which adapter to use is arbitrary.
physical_adapter	Bridge to a specific physical network adapter on the host system.

6 (Optional) If you selected automatic bridging mode and you want to place restrictions on the physical adapters that the virtual network adapter bridges to, click **Automatic Settings** and deselect one or more physical adapters.

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

What to do next

If you want to rename the new network to a name that is meaningful to you, see Rename a Virtual Network.

Add a Host-Only Virtual Network

You can use the virtual network editor to set up multiple host-only virtual networks.

On Windows and Linux host systems, the first host-only network is set up automatically when you install Workstation Pro. You might want to set up multiple host-only networks on the same computer in the following situations.

- 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.
- To test routing between two virtual networks.
- To test a virtual machine that has multiple network interface cards, without using any physical network adapters.

Prerequisites

Familiarize yourself with host-only networking. See Configuring Host-Only Networking for more information.

Procedure

1 Select **Edit > Virtual Network Editor**.

2 Click **Add Network**.

3 Select a virtual switch.

On Windows and Linux hosts, the VMnet1 virtual switch is mapped to a host-only network by default.

Workstation Pro assigns a subnet IP address to the virtual network.

4 Select the new virtual network from the list and select **Host-only (connect VMs internally on a private network)**.

5 (Optional) To connect a physical network on the host system to the network, select **Connect a host virtual adapter to this network**.

6 (Optional) To use a local DHCP service to distribute IP addresses to virtual machines on the network, select **Use local DHCP service to distribute IP addresses to VMs**.

7 (Optional) (Windows hosts only) To customize DHCP settings if the network uses a local DHCP service, click **DHCP Settings**.

8 (Optional) To change the subnet IP address or subnet mask, modify the addresses in the **Subnet IP** and **Subnet mask** text boxes.

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

What to do next

If you want to rename the new network to a name that is meaningful to you, see Rename a Virtual Network.

Rename a Virtual Network

With Workstation Pro on a Windows host system, you can rename a network you previously added to a name that is meaningful to you.

You cannot change the name of a network in the following situations.

- On a Linux host
- On a network Workstation Pro created automatically, such as VMnet0. VMnet1, or VMnet8.
- On a remote virtual machine.

Prerequisites

Add a virtual network. See Add a Bridged Virtual Network or Add a Host-Only Virtual Network

Procedure

1 Select **Edit > Virtual Network Editor**.

2 Select an added network.

The network must be one you added, not VMnet0. VMnet1, or VMnet8.

3 Click **Rename Network**.

4 Enter a new name and click **OK**.

Results

The network is renamed.

Change Automatic Bridging Settings

When automatic bridging mode is configured, you can restrict the physical network adapters that a virtual switch bridges to.

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 bridged network, and click **Automatic Settings**.

By default, a virtual switch bridges to all active network adapters on the host system when it is configured for automatic bridging. The choice of which adapter to use is arbitrary.

To prevent a virtual switch from bridging to a particular physical network adapter, deselect the check box for that host network adapter.

Change NAT Settings

You can change the gateway IP address, configure port forwarding, and configure advanced networking settings for NAT networks.

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 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 NAT network, and click **NAT Settings**.

By default, the NAT device is connected to the VMnet8 virtual switch. You can have only one NAT virtual network.

Table 13-1. NAT Settings

Setting	Description
Gateway IP	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	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. **Important** Change this value only under the direction of VMware technical support.
Enable IPv6	Enable NAT to use an IPv6 address.
IPv6 Prefix	If IPv6 is enabled, enter the IPv6 prefix that the NAT device uses.

Table 13-1. NAT Settings (continued)

Setting	Description
DNS Settings	(Windows hosts only) 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	(Windows hosts only) Select NBNS (NetBIOS Name Service) and NBDS (NetBIOS Datagram Service) timeouts and retry settings.

Change DHCP Settings on a Windows Host

On a Windows host, you can change the range of IP addresses and the duration of DHCP licenses for NAT and host-only networks that use a DHCP service to distribute IP addresses.

Procedure

1 Select **Edit > Virtual Network Editor**.

2 Select the NAT or host-only network, and click **DHCP Settings**

Table 13-2. DHCP Settings

Setting	Description
Start IP address and **End IP address**	The range of IP addresses that the virtual DHCP service provides on the selected virtual network.
Default lease time and **Max lease time**	Select the duration of the DHCP leases that the DHCP service provides to clients on the virtual network.

Importing and Exporting Network Settings on Windows Host

With Workstation Pro on a Windows host system, you can export network settings to a backup file, and later restore the network settings from this file.

Note You cannot import or export network settings across different hosts.

Exporting Network Settings

You can use the virtual network editor to export virtual network settings into a backup file, which can later be used to restore these settings.

Procedure

1. Select **Edit > Virtual Network Editor** to start the virtual network editor on the Windows host system.
2. Click the **Export** button. In the **Save As** window, select the save folder and enter a filename in the **File Name** field.
3. Click **Save**.

Results

The network settings are saved for future use.

Importing Network Settings

You can use the virtual network editor to import virtual network settings from a backup file and restore network settings.

Procedure

1. Select **Edit > Virtual Network Editor** to start the virtual network editor on the Windows host system.
2. Click the **Import** button. In the **Open** window, select a previously exported network settings backup file.
3. Click **Open**.

Results

The network settings are restored from the backup file.

Running the Support Script

14

VMware technical support might ask you to run the support script to gather information from the host system or virtual machines running on the host system. For example, if a virtual machine exits abnormally or fails, you can run the support script to collect the appropriate log files and system information. You can run the support script from Workstation Pro, from a Windows command prompt, or from a Linux terminal window.

Note The support script collects local data only. It does not collect data for remote hosts or for virtual machines running on remote hosts.

To collect diagnostic information for VMware Tools, you must edit the `tools.conf` file. See the VMware knowledge base article at http://kb.vmware.com/kb/1010744 for more information.

Read the following topics next:

- Register and Create a Support Request
- Run the Support Script from Workstation Pro
- Run the Support Script from a Windows Command Prompt
- Run the Support Script from a Linux Terminal Window

Register and Create a Support Request

To report problems to VMware support, you create a support request.

Prerequisites

Locate your Workstation Pro license key. The license key is sent to you in an email message when you register.

Procedure

1. If you do not have a VMware account, select **Help > Enter License Key > Register** and follow the instructions on the Web site.
2. Select **Help > Support > Submit Support Request** to create a support request.

Run the Support Script from Workstation Pro

You can run the support script from Workstation Pro to collect support data from the local host system or from the local host system and selected virtual machines running on the local host system.

On a Linux host, the script displays messages that indicate that it cannot collect some information because you are not logged in as root. If VMware technical support needs this information, a support representative will ask you to run the script from a terminal window as root. See Run the Support Script from a Linux Terminal Window.

Prerequisites

- Create a support request. See Register and Create a Support Request.
- Increase the level of logging. See Gathering Debugging Information.
- If you plan to collect support data from specific virtual machines, verify that the latest version of VMware Tools is installed and power on the virtual machines.

Procedure

1 On the host system, select **Help > Support > Collect Support Data** in Workstation Pro.

Option	Description
To collect data from the host system and a virtual machine	Select the virtual machine and click **Collect**. You can select multiple virtual machines.
To collect data only from the host system	Deselect all virtual machines and click **Collect**.

On a Windows host, the support script creates a `.ZIP` file of the collected data and displays the file in an open Windows Explorer window. Choose a directory location for the `.ZIP` file. On a Linux host, the support script creates a compressed `.TGZ` file in your home directory.

2 Add the `.ZIP` or `.TGZ` file to your support request.

Run the Support Script from a Windows Command Prompt

On a Windows host system, you can run the support script from the Windows command prompt to collect support data from the local host system.

Prerequisites

- Create a support request. See Register and Create a Support Request
- Increase the level of logging. See Gathering Debugging Information.

Procedure

1. Open a command prompt on the Windows host system and change to the `VMware Workstation` directory.

   For example: **`cd C:\Program Files\VMware\VMware Workstation`**

2. Run the support script.

   `cscript vm-support.vbs`

   The script displays the name of the directory where it stores its output.

3. Use a file compression utility to compress the script output directory.
4. Include the zip file of the script output directory with your support request.
5. If you are reporting a problem that occurred during Workstation Pro installation, include the installation log file (`VMInst.log`) with your support request.

   The installation log file is located in the `Temp` directory. On a Windows host, the default location is `C:\Documents and Settings\`*username*`\Local Settings\temp`.

Run the Support Script from a Linux Terminal Window

On a Linux host system, you can run the support script from a Linux terminal window to collect support data from the local host system.

If you do not run the support script as root, the script displays messages that indicate that it cannot collect some information. If the VMware support team needs this information, a support representative will ask you to run the script as root.

Prerequisites

- Create a support request. See Register and Create a Support Request
- Increase the level of logging. See Gathering Debugging Information.

Procedure

1. On the Linux host system, open a terminal window and run the support script as root or as the user who is running the virtual machine.

   `vm-support`

   The script creates a compressed `.TGZ` file in the user's home directory.

2. Include the `.TGZ` file with your support request.
3. If you are reporting a problem that occurred during Workstation Pro installation, include the installation log file with your support request.

Using vctl Command to Manage Containers and Run Kubernetes Cluster

15

You can use the `vctl` command-line utility in Workstation Pro to manage containers. In addition, vctl provides support for KIND so that KIND can use vctl container as "nodes" to run local Kubernetes clusters.

The `vctl` is a command-line utility bundled inside the Workstation Pro application, it is supported only on Windows 10 1809 or later. Workstation Pro on hosts with Linux OS or Windows OS earlier than Windows 10 1809 don't support the `vctl` CLI.

Related executables come bundled in the Workstation Pro application and are available in `C:\Program Files (x86)\VMware\VMware Workstation` folder by default.

The three executables of the vctl command-line utility are summarized in the following section.

containerd.exe

This is a runtime daemon that runs in the background. The containerd daemon must be started first before you can run any container related operation. To start it, use the `vctl system start` command and to stop it use the `vctl system stop` command.

containerd-shim-crx-v2.exe

When a new container is started, a new **containerd-shim-crx-v2** process is launched and works as an adapter between the container in CRX VM and the containerd daemon.

bin/vctl.exe

It is a command-line utility that runs in the foreground and relays the user input to the containerd daemon.

Note The vctl CLI runs every container inside a lightweight virtual machine, called CRX VM. By default, a CRX VM is created and starts up when a container starts. It shuts down and is removed when the container stops. The name of the CRX VM is same as the container.

Read the following topics next:

- Using the vctl Utility

- Enabling KIND to Use vctl Container as Nodes to Run Kubernetes Clusters
- Running vctl Commands
- Cleaning Up Residual Environment Data

Using the vctl Utility

The vctl utility is included with Workstation Pro and is ready to run in the Command Prompt or Windows PowerShell window.

Prerequisites

- VMware recommends the use of modern solid-state drive (SSD) as system disk.
- The host operating system must be Window 10 1809 or later.
- Before using `vctl` to run any operation on a container image or container, the container runtime must be started first. The container runtime doesn't start automatically when Workstation Pro application launches, and does not stop automatically when Workstation Pro application quits. You must manually run the `vctl system start` command to start it and run `vctl system stop` command to stop it.

Procedure

1. Open a Command Prompt or Windows PowerShell window.
2. Run the `vctl system info` command to check the status of the container runtime.

   If the command output displays **Container runtime is stopped**, run `vctl system start` command to start the container runtime.

   If the command output shows **Container runtime is running**, you can start using `vctl` to manage containers and container images.
3. Run the `vctl` command to list the command-line options.

Enabling KIND to Use vctl Container as Nodes to Run Kubernetes Clusters

In Workstation Pro, `vctl` utility supports KIND. It enables KIND to use vctl container instead of Docker container as nodes to run local Kubernetes clusters.

Prerequisites

By default, `vctl` assigns 2 GB memory for every CRX VM that hosts the `vctl` container node. Ensure that your physical machine has 2 GB free memory when running single-node cluster, 4 GB free memory when running two-node cluster. The more nodes configured in your cluster, the more free memory is needed.

Procedure

1 Open a Command Prompt or Windows PowerShell window.

2 Run the `vctl system start` command to start the `vctl` container runtime.

3 Run `vctl kind` command.

This command performs the following four tasks:

a Creates a **bin** folder in the `<Home_Folder_of_Your_Account>\.vctl` folder.

b Downloads **kubectl.exe**, **kind.exe** and **crx.vmdk** files, and saves them to the **bin** folder.

c Creates a docker shortcut that points to `C:\Program Files (x86)\VMware\VMware Workstation\bin\vctl.exe` by default.

d Opens a Command Prompt or Windows PowerShell window and creates a vctl-based KIND context by adding `<Home_Folder_of_Your_Account>/.vctl/bin` to the PATH environment variable and makes it the first searchable path.

So in this window, the three executables under `<Home_Folder_of_Your_Account>\.vctl\bin` folder will take precedence over other existing versions of `kubectl/kind/docker.exe` executables that were installed before.

4 The vctl-based KIND context will be lost if you close the window.

Next time you want to interact with the Kubernetes clusters, run the `vctl kind` command.

This time only Step 3.d will be repeated.

Note

- vctl does not support `kind build` and `kind export logs` kind subcommands.
- By default, vctl assigns 2 GB memory and 2 CPU cores for the CRX VM that hosts the node container, you can use the `--k8s-cpus` and `--k8s-mem` options of `vctl system config` command to customize the configurations.

Running vctl Commands

The `vctl` commands have syntax and other requirements that you must follow.

Syntax of vctl Commands

The `vctl` commands are divided into function categories.

The following tables list `vctl` commands and their function. Options enclosed in square brackets are optional. The vertical bar indicates a keyword choice.

Note Use `--help` to review all the available command options.

`vctl` Commands to Manage the Container Runtime Resource

Command	Description
`vctl system config [OPTIONS]`	Configures and initializes the host OS environment for the container engine. The command performs the following tasks: ■ Creates a `<Home_Folder_of_Your_Account>\.vctl` folder if it doesn't exist. ■ Updates the `config.yaml` file in the `.vctl` folder with the customized configurations specified by the command options. ■ Prepares the storage. **Note** The `vctl system config` command doesn't start containerd daemon.
`vctl system info [OPTIONS]`	Displays the container runtime information.
`vctl system start [OPTIONS]`	Starts the container engine. The command performs the following tasks: ■ Creates a `<Home_Folder_of_Your_Account>\.vctl` folder if it doesn't exist. ■ Updates the `config.yaml` file in the `.vctl` folder with the customized configurations specified by the command options. ■ Prepares the storage. ■ Starts the containerd daemon.
`vctl system stop [OPTIONS]`	Stops the container runtime.

`vctl` Commands to Manage the Image Resource

Command	Description
`vctl build [OPTIONS] PATH`	Builds a container image using a Dockerfile. **Note** If the RUN instructions in the Dockerfile run network-related commands, add ENV instruction into the Dockerfile to set network proxy, for example: **ENV https_proxy <Proxy_Server>:Proxy_Port** for the network operations to succeed.
`vctl images [OPTIONS] [IMAGE...]`	Lists container images and displays basic information about the container images.
`vctl push [OPTIONS] IMAGE [REMOTE_URL]`	Pushes the container image to the registry.
`vctl rmi [OPTIONS] ([IMAGE...]|--all)`	Deletes one or more container images.
`vctl tag [OPTIONS] SOURCE_IMAGE TARGET_IMAGE [TARGET_IMAGE...]`	Tags container images. It creates an image alias with the `TARGET_IMAGE`.
`vctl pull [OPTIONS] IMAGE`	Pulls a container image from the registry.

`vctl` Commands to Manage the Container Resource

Command	Description
`vctl create [OPTIONS] IMAGE [COMMAND] [ARGUMENTS...]`	Creates a new container from a container image. **Note** Ensure the following when you use the `--volume` option: ■ Specify paths to the folder. The `--volume` doesn't support path to files. ■ Use absolute path. Relative paths are not supported. ■ Only anonymous volumes can be mounted, mounting named volumes is not supported. **Note** Ensure the following when you use the `--publish` option: ■ The vctl utility doesn't have a subnet or a link feature to connect multiple containers to a subnet. To enable communication between multiple containers, start the container with the `--publish` option. This binds the container port to the host port so that the service provided by the container is accessible from the outside.
`vctl describe [OPTIONS] CONTAINER`	Displays details about the container.
`vctl exec [OPTIONS] CONTAINER COMMAND [ARGUMENTS...]`	Runs a command inside a running container.
`vctl ps [OPTIONS][CONTAINER...]`	Lists the containers and displays basic information about the container.
`vctl rm [OPTIONS] ([CONTAINER...]|--all)`	Deletes one or more containers.
`vctl run [OPTIONS] IMAGE [COMMAND] [ARGUMENTS...]`	Runs a new container from a container image. **Note** Ensure the following when you use the `--volume` option: ■ Specify paths to the folder. The `--volume` doesn't support path to files. ■ Use absolute path. Relative paths are not supported. ■ Only anonymous volumes can be mounted, mounting named volumes is not supported. **Note** Ensure the following when you use the `--publish` option: ■ The vctl utility doesn't have a subnet or a link feature to connect multiple containers to a subnet. To enable communication between multiple containers, start the container with the `--publish` option. This binds the container port to the host port so that the service provided by the container is accessible from the outside.
`vctl start [OPTIONS] CONTAINER`	Starts a created or stopped container.

Command	Description
`vctl stop [OPTIONS] CONTAINER`	Stops the container.
`vctl inspect [OPTIONS] NAME`	Displays detailed container information.

`vctl` Commands to Manage the CRX VM Resource

Command	Description
`vctl execvm [OPTIONS] (vmx|-c=CONTAINER) COMMAND [ARGUMENTS...]`	Runs commands from inside a running virtual machine that hosts the container.

`vctl` Commands to Manage Volumes

Command	Description
`vctl volume prune [flags]`	Removes all unused local volumes.

`vctl` Commands to Manage Container Images Registry Authentication

Command	Description
`vctl login [OPTION] [SERVER]`	Logs in to a remote registry.
`vctl logout [SERVER]`	Logs out from a remote registry.

Note

- On macOS, the credentials are saved in the Keychain. On Windows, the credentials are saved in the Credential Manager.
- Once the login is successful, future Pull, Push and Build requests will leverage the saved credential.
- Logout request deletes the corresponding credential from the Keychain or the Credential Manager.

`vctl` Commands to Get System Environment Ready for vctl-Based KIND

Command	Description
`vctl kind`	Prepares the system environment for vctl-based KIND. KIND uses vctl containers as nodes for running Kubernetes clusters.

Examples of vctl Commands

The command-line examples that follow work on Workstation Pro.

Commands Related to Image

- When you build a new image, to pull the base image from a private Docker registry successfully, either use the `vctl login` command to log in to the private Docker registry first or use the `--credential` option to pass a JSON file that stores credentials to `vctl build` command for registry authentication. For example:

  a Encode your Docker registry username and password in base64 with the following command:

  ```
  echo -n USER:PASSWORD | base64
  ```

  b Create a `config.json` file with your Docker registry URL and the base64 encoded string generated in step 1.

  ```
  {
                              "auths": {
                                           "https://index.docker.io/v2/": {
                                                          "auth": "xxxxxxxxxxxxxxx"
                                           }
                               }
  }
  ```

  c Build the new image whose base image is in a private Docker registry, by passing the JSON file to `vctl build` command:

  ```
  vctl build --file Dockerfile --tag docker.io/mynamespace/myrepo:1.0 --
  credential config.json .
  ```

Commands Related to Container

- List running containers.

  ```
  vctl ps
  ```

- List all containers, including the running containers and stopped containers.

  ```
  vctl ps --all
  ```

- Run a container in detached mode using the `nginx` image, which is the same as `docker.io/library/nginx:latest`.

  ```
  vctl run --name myContainer -d nginx
  ```

- Run a container using the `--publish` option and the `fluentd` image, here `fluentd` is equivalent to `docker.io/library/fluentd:latest`.

  ```
  vctl run --name myContainer --publish 24224:24224/udp --publish
  24224:24224 fluentd
  ```

- Run multiple containers and enable discovery and communication with each other.
  - The vctl utility doesn't have a subnet or a link feature to connect multiple containers to a subnet.

To enable communication between multiple containers, start the container with the `--publish` option. This binds the container port to the host port so that the service provided by the container is accessible from the outside.

```
vctl run --name mydb -m 2048 -e MYSQL_ROOT_PASSWORD=password -p 3306:3306
mysql

vctl run --name mymatomo -m 4096 -p 8080:80 -e
MATOMO_DATABASE_HOST=<Host_IP>:3306 matomo
```

- Run a container using the `--volume` option and the `bonita` image, here `bonita` is equivalent to `docker.io/library/bonita:latest`.

  ```
  vctl run --name myContainer -p 8080:8080 --volume %userprofile%
  \Documents\container:/opt/bonita bonita
  ```

Commands Related to CRX VM

- Get shell access to a CRX VM.
  - By specifying the container hosted by the CRX VM.

    ```
    vctl execvm --sh -c myContainer
    ```

  - By specifying the vmx path of the CRX VM.

    Note To get the vmx path, run the `vctl describe myContainer` command and refer to the **Host virtual machine** value in the output.

    ```
    vctl execvm --sh %userprofile%\.vctl\.r\vms\myContainer\myContainer.vmx
    ```

- Execute a command within a CRX VM.
  - By specifying the container hosted by the CRX VM.

    ```
    vctl execvm -c myContainer /bin/ls
    ```

  - By specifying the vmx path of the CRX VM.

    Note To get the vmx path, run the `vctl describe myContainer` command and refer to the **Host virtual machine** value in the output.

    ```
    vctl execvm %userprofile%
    \.vctl\.r\vms\myContainer\myContainer.vmx /bin/ls
    ```

Cleaning Up Residual Environment Data

By default, the vctl utility stores all its data in the `.vctl` folder under the home folder of your user account.

Perform the following to clean up the environment data:

Procedure

1. Run the `vctl system stop -f` command to stop all running containers and stop container runtime.
2. Run the `vctl system info` command to check if container runtime has stopped.
3. Remove the `<Home_Folder_of_Your_Account>/.vctl` folder.

Using the vmrun Command to Control Virtual Machines

16

You can use the `vmrun` command-line utility in `Workstation Pro` to control virtual machines and automate guest operations on VMware virtual machines. The `vmrun` utility is associated with the VIX API libraries.

The capabilities of the `vmrun` utility are summarized in the following sections.

Power Commands

Power commands control virtual machine operations. You can use power commands to start (power on), stop (power off), reset (reboot), suspend, pause, and unpause a virtual machine.

Snapshot Commands

A snapshot captures the state of a virtual machine at the time of the snapshot, including all data on virtual disks. You can then use the snapshot to revert the virtual machine to its previous state. Snapshots are useful for data backup and as a placeholder for development and testing. You can use snapshot commands to list existing snapshots of a virtual machine, create a snapshot, delete a snapshot, and revert a virtual machine to its state at the time of a snapshot. Revert to snapshot does not resume running a virtual machine, even if it was running at the time of a snapshot.

Network Adapter Commands

Network adapter commands allow you to control the virtual network adapters associated with a virtual machine. You can use network adapter commands to list, add, update, and remove a network adapter.

Host Network Commands

Host network commands allow you to list the host virtual networks and to list, update, or remove a port forwarding configuration.

Guest Operating System Commands

Guest operating system commands enable you to interact with a guest operating system in the following ways.

- Run an executable program in the guest operating system or run an interpreted script that you provide.
- Check if a file or directory exists in the guest, delete a file or directory, rename a file, list files, or create a new directory.
- Copy a file from the host to the guest or from the guest to the host.
- Create a temporary file in the guest operating system.
- Add a shared folder from the host, make a shared folder writable in the guest, or remove a shared folder.
- Capture a screen image from the guest.
- List the processes running in the guest operating system or end a process.
- Read or write a variable in the guest operating system's environment or virtual machine state.
- Obtain the IP address of the guest operating system.

The timeout, which is the wait period for VMware Tools, is five minutes for all guest-related commands.

General Commands

General commands include commands that list all running virtual machines, upgrade the virtual machine hardware version, install VMware Tools in the guest operating system, check the current status of VMware Tools, and delete virtual machines. Also, you can clone a virtual machine to create a copy of the virtual machine.

Template Virtual Machine Command

The name of the template virtual machine command is `downloadPhotonVM`. The command allows you to download the VMware Project Photon operating system virtual machine.

Read the following topics next:

- Use the vmrun Utility
- Syntax of the vmrun Command
- Using Authentication Flags in vmrun Commands
- Running vmrun Commands

Use the vmrun Utility

No configuration is needed to use the `vmrun` utility on a Windows or Linux host.

The `vmrun` utility is included with Workstation Pro and ready to run in a command prompt window.

Procedure

1. Open the command prompt.
2. If you use a Windows operating system, go the folder where `vmrun` is installed.

   For example,

   ```
   cd C:\Program Files (x86)\VMware\VMware Workstation
   ```

3. Run the `vmrun` command to list the command-line options.

Syntax of the vmrun Command

The `vmrun` command syntax can contain authentication flags, commands, and parameters.

The following syntax applies to the `vmrun` command.

```
vmrun [AUTHENTICATION-FLAGS] COMMAND [PARAMETERS]
```

Using Authentication Flags in vmrun Commands

You can use authentication flags in `vmrun` commands to provide information required to access a system.

For example, you can use an authentication flag to specify the local host type because `vmrun` commands apply to both VMware Workstation and VMware Fusion host types. You can also use authentication flags to provide the credentials required to access encrypted virtual machines or a guest operating system.

Authentication flags must appear before the command and command parameters.

The `vmrun` command supports the following authentication flags.

`-T` *`hostType`*

`-vp` *`encryptedVirtualMachinePassword`*

`-gu` *`guestUser`*

`-gp` *`guestPassword`*

Product Type

The `-T` flag is optional. When you run `vmrun` commands with Workstation Pro, `workstation` is the default. Use the `-T` flag for Workstation Pro as follows.

```
vmrun -T workstation
```

Encrypted Virtual Machines

Encrypted virtual machines require a password for most operations.

`-vp` *`encryptedVirtualMachinePassword`*

Guest Operations

Guest operations require authentication by the guest operating system.

Use the following flags to specify the user name and password of the user in the guest operating system.

`-gu` *`guestUser`*

`-gp` *`guestPassword`*

Running vmrun Commands

The `vmrun` commands have syntax and other requirements that you must follow.

Path to VMX File

VMware stores virtual machines as a package that includes the virtual machine settings file, *`filename`*`.vmx`, and the virtual disks.

When required, you must provide the path to the `.vmx` file. The examples that follow are of default paths to Windows and Linux virtual machine for Mac OS X, OS X, or macOS.

Unless you specify a file location for a virtual machine when you create it, Workstation saves the virtual machine package to a default location, which might vary.

Examples of the `vmrun` command include the relative path to the `.vmx` file instead of the absolute paths that follow.

- `C:\Users\<username>\Documents\Virtual Machines`
- `C:\Users\<username>\Documents\Virtual Machines\Ubuntu\Ubuntu.vmx`

Important For `vmrun` commands that require VMware Tools, install the latest VMware Tools package and, especially after operating system updates, keep VMware Tools up-to-date.

Deactivate Dialog Boxes

To prevent the `vmrun` utility from failing when you provide user input through a dialog box, you can deactivate dialog boxes.

The `vmrun` utility might time out and fail when you use the utility on a virtual machine that requires user input through a dialog box.

To deactivate dialog boxes, insert the following line in the virtual machine configuration file, the `.vmx` file.

```
msg.autoAnswer = TRUE
```

Syntax of vmrun Commands

The `vmrun` commands are divided into function categories.

The following tables list `vmrun` commands and parameters for Workstation Pro according to their function. Parameters are listed one per line. Parameters enclosed in square brackets are optional. The vertical bar indicates a keyword choice.

The `vmrun` Power Commands and Parameters

Option	Parameters	Description
`start`	*path to .vmx file* `[ gui | nogui ]`	Starts a virtual machine. The default `gui` option starts the machine interactively, which is required to display the Workstation Pro interface. The `nogui` option suppresses the Workstation Pro interface, including the startup dialog box, to allow noninteractive scripting.
`stop`	*path to .vmx file* `[ hard | soft ]`	Stops a virtual machine. Use the `soft` option to power off the guest after running shutdown scripts. Use the `hard` option to power off the guest without running scripts, as if you pressed the power button. The default is to use the `powerType` value specified in the `.vmx` file, if present.
`reset`	*path to .vmx file* `[ hard | soft ]`	Resets a virtual machine. Use the `soft` option to run shutdown scripts before rebooting the guest. Use the `hard` option to reboot the guest without running scripts, as if you pressed the reset button. The default is to use the `powerType` value specified in the `.vmx` file, if present.
`suspend`	*path to .vmx file* `[ hard | soft ]`	Suspends a virtual machine without shutting down the virtual machine, so local work can resume later. The `soft` option suspends the guest after running system scripts. On Windows guests, these scripts release the IP address. On Linux guests, the scripts suspend networking. The `hard` option suspends the guest without running the scripts. The default is to use the `powerType` value specified in the `.vmx` file, if present. To resume virtual machine operations after the `suspend` command finishes, use the `start` command. On Windows, the IP address is retrieved. On Linux, networking is restarted.
`pause`	*path to .vmx file*	Pauses a virtual machine.
`unpause`	*path to .vmx file*	Resumes operations of a virtual machine from where you paused normal operations.

The `vmrun` Snapshot Commands and Parameters

Option	Parameters	Description
`listSnapshots`	*path to .vmx file* `[ showtree ]`	Lists all snapshots in a virtual machine. The `showtree` option displays snapshots in tree format, with children indented under their parent.
`snapshot`	*path to .vmx file* *snapshot name*	Creates a snapshot of a virtual machine. Because Workstation Pro supports multiple snapshots, you must provide the snapshot name.

Option	Parameters	Description
deleteSnapshot	*path to .vmx file* *snapshot name* [andDeleteChildren]	Removes a snapshot from a virtual machine. Because Workstation Pro supports multiple snapshots, you must provide the snapshot name. The virtual machine must be powered off or suspended. If the snapshot has children, they become children of the deleted snapshot's parent, and subsequent snapshots continue as before from the end of the chain. The andDeleteChildren option deletes the specified snapshot and its children recursively. See revertToSnapshot for solutions to name conflicts.
revertToSnapshot	*path to .vmx file* *snapshot name* or *path to .vmx file* *Snapshot/"Snapshot 2"/"Snapshot N"*	Sets the virtual machine to its state at snapshot time. However if the virtual machine was powered on at the time of the snapshot, vmrun reverts it to a suspended state, but does not resume running the virtual machine. If a snapshot has a unique name within a virtual machine, revert to that snapshot by specifying the path to the virtual machine's configuration file and the unique snapshot name. If several snapshots have the same name, specify the snapshot by including a full pathname for the snapshot. A pathname is a series of snapshot names, separated by forward slash characters (/). Each name specifies a new snapshot in the tree. For example, the pathname Snap1/Snap2 identifies a snapshot named Snap2 that was taken from the state of a snapshot named Snap1.

The vmrun Host Network Commands and Parameters

Only Workstation Pro with Windows supports the host network commands. Workstation Pro with Linux does not support the host network commands.

Option	Parameters	Description
listHostNetworks		Lists all networks on the host.
listPortForwardings	*host network name*	Lists all available port forwardings on a host network.
setPortForwarding	*host network name* *protocol* *host port* *guest ip* *guest port* [Description]	Sets a port forwarding on a host network. **Note** To prevent the command from returning an error, use the sudo utility with this option. For example, sudo vmrun setPortForwarding.
deletePortForwarding	*host network name* *protocol* *host port*	Deletes a port forwarding on a host network. **Note** To prevent the command from returning an error, use the sudo utility with this option. For example, sudo vmrun deletePortForwarding.

The vmrun Guest Operating System Commands and Parameters

The timeout, which is the wait for VMware Tools, is five minutes for all guest-related commands.

Option	Parameters	Description
runProgramInGuest	*path to .vmx file* [-noWait | -activeWindow | -interactive] *program name* [*program arguments*]	Runs a specified program in the guest operating system. The -noWait option returns a prompt immediately after the program starts in the guest, rather than waiting for it to finish. This option is useful for interactive programs. The -activeWindow option ensures that the Windows GUI is visible, not minimized. It has no effect on Linux. The -interactive option forces interactive guest login. The option is useful for Windows Vista and Windows 7 or later guests to make the program visible in the console window. You must provide the full pathname of a program accessible to the guest. Also provide fully accessible path names for any files specified in the program arguments, according to the requirements of the program. VMware Tools and a valid guest login are required.
fileExistsInGuest	*path to .vmx file*	Checks whether the specified file exists in the guest operating system. VMware Tools and a valid guest login are required.
directoryExistsInGuest	*path to .vmx file* *directory path on guest*	Checks whether the specified directory exists in the guest operating system. VMware Tools and a valid guest login are required.
setSharedFolderState	*path to .vmx file* *share name* *path to folder on host* writable | readonly	Modifies the writability state of a specified folder shared between the host and a guest virtual machine. The value for the *share name* parameter is a mount point in the guest file system. The value for the *path to folder on host* parameter is the exported directory on the host. To make a shared folder writable or read-only, include the writable or readonly parameter.
addSharedFolder	*path to .vmx file* *share name* *path to folder on host*	Adds a folder to be shared between the host and guest. The virtual machine must be running for the addSharedFolder option to take effect. The value for the *share name* parameter is a mount point in the guest file system. The value for the *path to folder on host* parameter is the exported directory on the host. On Windows guests, a delay might occur before shared folders are visible to the runProgramInGuest, fileExistsInGuest, and directoryExistsInGuest options.
removeSharedFolder	*path to .vmx file* *share name*	Removes the guest virtual machine's access to a shared folder on the host. The virtual machine must be running for the removeSharedFolder option to take effect. The value for the *share name* parameter is a mount point in the guest file system.
enableSharedFolders	*path to .vmx file* [runtime]	Allows the guest virtual machine, specified by the .vmx file, to share folders with its host. After enabling, run the addSharedFolder option to specify each host folder to share. The optional [runtime] argument limits the sharing of folders until the virtual machine is powered off. Otherwise, the setting persists at the next power-on. **Note** The enableSharedFolders option takes effect after the shut-down and restart of the guest. No error message appears.

Option	Parameters	Description
disableSharedFolders	*path to .vmx file* [runtime]	Prevents the guest virtual machine, specified by the .vmx file, from sharing folders with its host. The optional [runtime] argument limits the stop applied to the sharing of folders until the virtual machine is powered off. Otherwise, the setting persists at next power on. **Note** The disableSharedFolders option takes effect after the shut-down and restart of the guest. No error message appears.
listProcessesInGuest	*path to .vmx file*	Lists all processes running in the guest operating system. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest.
killProcessInGuest	*path to .vmx file process ID*	Stops a specified process in the guest operating system. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest. The process ID can be any number listed after pid= in the output of the listProcessesInGuest option.
runScriptInGuest	*path to .vmx file* [-noWait | -activeWindow | -interactive] *interpreter path script text*	Runs the specified command script in the guest operating system. See the runProgramInGuest entry for an explanation of options. The *interpreter path* option runs the script. Provide the complete text of the script, not a filename. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest.
deleteFileInGuest	*path to .vmx file path to file on guest*	Deletes the given file from the guest operating system. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest.
createDirectoryInGuest	*path to .vmx file directory path on guest*	Creates the specified directory in the guest operating system. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest.
deleteDirectoryInGuest	*path to .vmx file directory path on guest*	Deletes the specified directory from the guest operating system. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest
createTempfileInGuest	*path to .vmx file*	Creates a temporary file in the guest operating system, and returns the path name of the temporary file created. The path name varies according to the operating system. You can run the deleteFileInGuest option to remove the file. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest.
listDirectoryInGuest	*path to .vmx file directory path on guest*	Lists contents of the specified directory in the guest operating system. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest.
CopyFileFromHostToGuest	*path to .vmx file file path on host file path in guest*	Copies a file from the host to the guest operating system. VMware Tools and a valid guest login are required. For example, you can use the -gu and -gp options to log in to the guest. Specify the source filename, or host filename, before the destination filename, or guest filename.

Option	Parameters	Description
`CopyFileFromGuestToHost`	*path to .vmx file file path in guest file path on host*	Copies a file from the guest operating system to the host. VMware Tools and a valid guest login are required. For example, you can use the `-gu` and `-gp` options to log in to the guest. Specify the source filename, or guest filename, before the destination filename, or host filename.
`renameFileInGuest`	*path to .vmx file original filename new filename*	Renames or moves a file in the guest operating system. VMware Tools and a valid guest login are required. For example, you can use the `-gu` and `-gp` options to log in to the guest. Specify the source filename, or original filename, before the destination filename.
`connectNamedDevice`	*path to .vmx file device name*	Connects the device named in the command to the guest operating system. You can only run this command when the virtual machine is powered on. You can use device names, such as `sound`, `serial0`, `Ethernet0`, `sata0:1`, etc. **Note** After you use the `vmrun connectNamedDevice` command to connect a disconnected sound device to a running virtual machine, powering off the virtual machine might disconnect the sound device from the virtual machine, even though the virtual machine settings list the sound device as connected.
`disconnectNamedDevice`	*path to .vmx file device name*	Disconnects the device named in the command from the guest operating system. You can only run this command when the virtual machine is powered on. You can use device names, such as `sound`, `serial0`, `Ethernet0`, `sata0:1`, etc. **Note** After you use the `vmrun disconnectNamedDevice` command to disconnect a connected sound device from a running virtual machine, powering off the virtual machine might reconnect the sound device to the virtual machine, even though the virtual machine settings list the sound device as disconnected.
`captureScreen`	*path to .vmx file output path on host*	Captures the screen of the virtual machine to a local file. The specified output file on the host is in PNG format. A valid guest login is required. For example, you can use the `-gu` and `-gp` options to log in to the guest.
`writeVariable`	*path to .vmx file* `[ guestVar | runtimeConfig | guestEnv ]` *variable name variable value*	Writes a variable to the virtual machine state or guest. You can set a non-persistent guest variable, `guestVar`, a runtime configuration variable,`runtimeConfig`, as stored in the `.vmx` file, or an environment variable, `guestEnv`, in the guest operating system. A guest variable is a runtime-only value that provides a simple way to pass runtime values in and out of the guest. Environment variables require VMware Tools and a valid guest login. For example, you can use the `-gu` and `-gp` options to log in to the guest. With Linux, setting the guest environment also requires root login.

Option	Parameters	Description
readVariable	*path to .vmx file* [guestVar | runtimeConfig | guestEnv] *variable name*	Reads a variable from the virtual machine state or guest. You can get a guest variable, a runtime configuration as stored in the .vmx file, or environment variables in the guest operating system. Reading the guestEnv variable requires a valid guest login. For example, you can use the -gu and -gp options to log in to the guest. See the writeVariable entry for a description of variable types.
getGuestIPAddress	*path to .vmx file* [-wait]	Retrieves the IP address of the guest. When you use the [-wait] option, the command waits until the IP address is available. For example, the IP address is not available until the virtual machine powers on. If the network is not ready, the command returns to the command-line prompt immediately.

The vmrun General Commands and Parameters

Option	Parameters	Description
list		Lists all running virtual machines.
upgradevm	*path to .vmx file*	Upgrades a virtual machine to the current virtual hardware version. Has no effect if the virtual hardware version is the most recent supported. Power off the virtual machine, such as with the vmrun stop command. Wait a short period of time for the command to finish. Then run the vmrun upgradevm command.
installTools	*path to .vmx file*	Prepares to install VMware Tools in the guest operating system. In Windows guests with autorun enabled, the VMware Tools installer starts by itself. In Linux guests without autorun, the command connects the virtual CD-ROM drive to the VMware Tools ISO image suitable for the guest, but the installer does not start. You must complete the installation with additional manual steps, as described in the product documentation.
checkToolsState	*path to .vmx file*	Checks the status of VMware Tools in the guest. The possible states are unknown, installed, and running.
deleteVM	*path to .vmx file*	Deletes a virtual machine.
clone	*path to .vmx file* *destination .vmx file path* full|linked [-snapshot=Snapshot Name] [-cloneName=Name]	Creates a copy of the virtual machine. Only Workstation Pro supports the clone option.

The vmrun Template Virtual Machine Commands and Parameters

Option	Parameters	Description
downloadPhotonVM	*path to save the downloaded VM*	Downloads a VMware Project Photon operating system virtual machine.

Examples of vmrun Commands

The command-line examples that follow work on VMware Fusion. Ubuntu16 is the virtual machine example for Linux and Win10 is the virtual machine example for Windows.

Reboot Commands

- Reboot a virtual machine.

  ```
  vmrun reset Win10.vmwarevm/Win10.vmx soft
  ```

Snapshot Commands

- Create a snapshot of a virtual machine

  ```
  vmrun snapshot Ubuntu16.vmwarevm/Ubuntu16.vmx mySnapshot
  ```

- List snapshots on the virtual machine, showing the snapshot created in the previous command.

  ```
  vmrun listSnapshots Ubuntu16.vmwarevm/Ubuntu16.vmx
  ```

- Revert to the snapshot you made, which suspends the virtual machine, and restart to resume operation.

  ```
  vmrun revertToSnapshot Ubuntu16.vmwarevm/Ubuntu16.vmx mySnapshot
  ```

  ```
  vmrun start Ubuntu16.vmwarevm/Ubuntu16.vmx
  ```

- Delete the snapshot by specifying its name.

  ```
  vmrun deleteSnapshot Ubuntu16.vmwarevm/Ubuntu16.vmx mySnapshot
  ```

Network Adapter Commands

- List all network adapters on a virtual machine.

  ```
  vmrun listNetworkAdapters Win10.vmwarevm/Win10.vmx
  ```

- Add a NAT network adapter to a virtual machine.

  ```
  vmrun addNetworkAdapter Win10.vmwarevm/Win10.vmx nat
  ```

Host Network Commands

- List all networks on the host.

  ```
  vmrun listHostNetworks
  ```

- Add a port forwarding on a host network with examples provided of the host network name, protocol, host port, guest IP address, guest port, and description.

  ```
  sudo vmrun setPortForwarding vmnet2 tcp 8082 1.1.1.2 88 portforwarding-description
  ```

Running Guest Applications

Most `vmrun` guest operations require VMware Tools to be installed on the guest operating system.

- Start the command tool, minimized, on a Windows guest.

  ```
  vmrun -gu guestUser -gp guestPassword runProgramInGuest Win10.vmwarevm/Win10.vmx
  -interactive cmd.exe
  ```

- Start the command tool on a Windows guest as an active window on the desktop.

  ```
  vmrun -gu guestUser -gp guestPassword runProgramInGuest Win10.vmwarevm/Win10.vmx
  -activeWindow -interactive cmd.exe
  ```

- Run a script on a Windows guest, with Perl as the script interpreter. Two separate examples follow.

  ```
  vmrun -gu guestUser -gp guestPassword runScriptInGuest Win10.vmwarevm/Win10.vmx
  -interactive "C:\perl\bin\perl.exe" "system('notepad.exe');"
  ```

  ```
  vmrun -gu guestUser -gp guestPassword runScriptInGuest Win10.vmwarevm/Win10.vmx
  -interactive "" "C:\perl\perl.exe C:\script.pl"
  ```

- Run a batch script and keep running afterwards. To use `cmd.exe` on Windows, you must specify the script interpreter as null.

  ```
  vmrun -gu guestUser -gp guestPassword runScriptInGuest Win10.vmwarevm/Win10.vmx ""
  "cmd.exe /k \"C:\\Program Files\\Microsoft Visual Studio\\VC\\vcvarsall.bat\" x86"
  ```

- Run a Bash shell script file or Perl script on a Linux guest.

  ```
  vmrun -gu guestUser -gp guestPassword runScriptInGuest Ubuntu16.vmwarevm/
  Ubuntu16.vmx -interactive "" "/bin/bash myscript"
  ```

  ```
  vmrun -gu guestUser -gp guestPassword runScriptInGuest Ubuntu16.vmwarevm/
  Ubuntu16.vmx -interactive "/usr/bin/perl" "system('firefox');"
  ```

- Start an X clock on a Linux guest, which requires the `-display` option to appear on the console.

  ```
  vmrun -gu guestUser -gp guestPassword runProgramInGuest Ubuntu16.vmwarevm/
  Ubuntu16.vmx /usr/bin/xclock -display :0
  ```

- Run the same X clock command, but return control back to the console immediately.

  ```
  vmrun -gu guestUser -gp guestPassword runProgramInGuest Ubuntu16.vmwarevm/
  Ubuntu16.vmx -noWait /usr/bin/xclock -display :0
  ```

- Run Firefox.

  ```
  vmrun -gu guestUser -gp guestPassword runProgramInGuest Ubuntu16.vmwarevm/
  Ubuntu16.vmx /usr/bin/firefox --display=:0
  ```

- Setting the guest environment with the `guestEnv` parameter requires root permission on Linux because the change affects subsequent commands issued by other users.

  ```
  vmrun -gu guestUser -gp guestPassword writeVariable Ubuntu16.vmwarevm/Ubuntu16.vmx
  guestEnv SRC tmp.example.com:1666
  ```

- List processes in a Linux guest and end the process numbered 8192.

  ```
  vmrun -gu guestUser -gp guestPassword listProcessesInGuest Ubuntu16.vmwarevm/
  Ubuntu16.vmx
  ```

  ```
  vmrun -gu guestUser -gp guestPassword killProcessInGuest UUbuntu16.vmwarevm/
  Ubuntu16.vmx 8192
  ```

- Run a Perl script on a Linux guest to remove DOS-style carriage returns from a file.

  ```
  vmrun -gu guestUser -gp guestPassword runProgramInGuest Ubuntu16.vmwarevm/
  Ubuntu16.vmx /usr/bin/perl -e "open(FILE, '>/tmp/unix.txt'); while (<>) { s/
  \r\n/\n/ ; print FILE}" /tmp/dos.txt
  ```

- Run a Perl script on a Windows guest to insert DOS-style carriage returns in a file.

  ```
  vmrun -gu guestUser -gp guestPassword runProgramInGuest Win10.vmwarevm/Win10.vmx
  C:\cygwin\bin\perl.exe -e "open(FILE, '>C:\Users\user\dos.txt'); while (<>) { s/\n/
  \r\n/ ; print FILE}" C:\Users\guestUser\unix.txt
  ```

Guest to Host File Operations

- To copy a file from the host to a guest, the user must have write permission on the destination.

  ```
  vmrun -gu guestUser -gp guestPassword copyFileFromHostToGuest Ubuntu16.vmwarevm/
  Ubuntu16.vmx ~/img.db /tmp/img.db
  ```

- To copy a file from a guest to the host, the user must have read permission on the source file.

  ```
  vmrun -gu guestUser -gp guestPassword copyFileFromGuestToHost Ubuntu16.vmwarevm/
  Ubuntu16.vmx /home/username/addr addr.txt
  ```

- To enable shared folders.

  ```
  vmrun enableSharedFolders Ubuntu16.vmwarevm/Ubuntu16.vmx
  ```

- To share a folder on a Mac host with a particular Linux guest.

  Note Before sharing folders, you must enable them with the `enabledSharedFolders` option, or by selecting **Enable Shared Folders** in the **Sharing Settings** panel of the virtual machine. On Linux guests, the `/mnt/hgfs` directory is available for sharing, but you can use a different directory for shared folders.

  ```
  vmrun addSharedFolder Ubuntu16.vmwarevm/Ubuntu16.vmx sharedFolderName ~/Share
  ```

- To make a shared folder read-only or to delete the shared folder.

  Note Shared folders are writable by default.

  ```
  vmrun setSharedFolderState Ubuntu16.vmwarevm/Ubuntu16.vmx sharedFolderName ~/Share
  readonly
  ```

  ```
  vmrun removeSharedFolder Ubuntu16.vmwarevm/Ubuntu16.vmx sharedFolderName
  ```

  Note On Windows Vista and Windows 7 or later guests, only the Administrator account can use `copyFileFromHostToGuest` and `deleteFileInGuest` options to write and delete files in the `C:\` and system folders, or use the `createDirectoryInGuest` and `deleteDirectoryInGuest` options to modify system directories. Regular users, even those with administrator privilege, cannot perform these operations.

Guest Variables and Environment

- From the host, set a guest variable on the virtual machines.

  ```
  vmrun writeVariable Win10.vmwarevm/Win10.vmx guestVar vmstartdate 21April2017
  ```

- On the guest operating systems, read the guest variable that you just set.

  ```
  > rpctool.exe "info-get guestinfo.vmstartdate"
  ```

  ```
  $ vmware-rpctool "info-get guestinfo.vmstartdate"
  ```

- From the host, set a guest environment variable on a Linux virtual machine and verify by writing the environment variables into a temporary file.

  ```
  vmrun writeVariable Ubuntu16.vmwarevm/Ubuntu16.vmx guestEnv LD_LIBRARY_PATH /usr/local/lib
  Guest user: root
  Guest password:
  ```

  ```
  vmrun runScriptInGuest Ubuntu16.vmwarevm/Ubuntu16.vmx /bin/bash "/usr/bin/env > /tmp/
  env.out"
  Guest user: root
  Guest password:
  ```

  Note No output is sent to the host when you use the `runScriptInGuest` option with the `vmrun` command. Find the output of the command in the `/tmp/env.out` file on the guest.

- On a Linux guest, determine the IP address and set it in a guest variable.

  ```
  $ ipaddr=`ifconfig eth0 | grep inet.addr`
  $ vmware-rpctool "info-set guestinfo.theip $ipaddr"
  ```

- From the host, retrieve the IP address that was just set to the guest.

  ```
  vmrun readVariable Ubuntu10/Ubuntu10.vmx guestVar theip
  ```

General Commands

- List running virtual machines.

```
vmrun list
Total running VMs: 2
Absolute-path-to-virtual-machine.vmx

Absolute-path-to-virtual-machine.vmx
```

- Prepare to install VMware Tools.

```
vmrun installTools Ubuntu16.vmwarevm/Ubuntu16.vmx
```

The Template Virtual Machine Commands

- Download a VMware Project Photon operating system virtual machine.

```
vmrun downloadPhotonVM ~
```

Using the vmware Command

17

You can use the `vmware` command to run Workstation Pro from the command line on a Linux or Windows host system.

Read the following topics next:

- Run the vmware Command
- Incorporate Workstation Pro Startup Options in a Windows Shortcut

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.

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(x86)\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 17-1. vmware Command Options

Option	Description
`-n`	Opens a new Workstation Pro window.
`-t`	Opens a virtual machine in a new tab in the existing Workstation Pro window.
`-x`	Powers on the virtual machine when Workstation Pro starts. This option is equivalent to clicking **Power On** in the Workstation Pro toolbar.
`-X`	Powers on the virtual machine and switches the Workstation Pro window to full screen mode.
`-q`	Closes the virtual machine tab when the virtual machine powers off. If no other virtual machine is open, it also exits Workstation Pro. 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.

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 Pro window, cannot be overridden.

Incorporate Workstation Pro 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.

Procedure

1. Right-click the Workstation Pro shortcut and select **Properties**.
2. In the **Target** text box, add any options to use after the `vmware.exe` command and enclose the entire command string in quotation marks.

   For example:

   ```
   "C:\Program Files(x86)\VMware\VMware Workstation\vmware.exe -X
   C:\Documents and Settings\username\My Documents\My Virtual Machines\Windows Me\Windows
   Me.vmx"
   ```

Using VMware Workstation Pro REST API

18

VMware Workstation Pro REST API allow you to interact programmatically with the core VMware hypervisor and virtual machines.

Overview of Workstation Pro REST API

You can send standard `GET`, `PUT`, `POST`, and `DELETE` requests through HTTP and HTTPS to control configuration and deployment options. For example, you can use VMware Workstation Pro REST API to perform clone and power operations. You can perform network-related operations, such as to create and update virtual NIC configurations and to retrieve IP addresses from the virtual machine. You can also configure shared folders. Response payloads are delivered in JSON format.

Workstation Pro REST API Considerations

Keep the following considerations in mind when using the Workstation Pro REST API.

- VMware Workstation Pro REST API are available only for Workstation Pro.
- The Workstation Pro REST API service depends on the `vmrest` process.
- The `vmrest` service runs as the user who starts it. For example, on Windows hosts, as administrator, you can use a terminal window to start the `vmrest` service. On Linux hosts, as the root user, you can use the `sudo vmrest` command.

Read the following topics next:

- Use the VMware Workstation Pro REST API Service
- Using Workstation REST API Service to Manage Power Options of Encrypted Virtual Machines

Use the VMware Workstation Pro REST API Service

You can access the VMware Workstation Pro REST API from a local machine.

Note To view the Workstation Pro API online, search VMware API Explorer for the appropriate version of the Workstation Pro API.

Procedure

1 Install Workstation Pro on your Windows or Linux host.

2 Before you start the REST API service the first time, set up your credentials.

a In a terminal window, run the appropriate command, depending on the operating system of the host machine.

- On Windows, change directories to the Workstation Pro installation folder, and run the `vmrest.exe -C` command.
- On Linux, run the `vmrest -C` command.

b Enter a user name and password as prompted.

You do not need to set up credentials when you start the REST API on subsequent occasions.

The user name and password are saved to the appropriate file.

Operating System	File
Windows	`%USERPROFILE%\vmrest.cfg`
Linux	`~/.vmrestcfg`

3 Configure the REST API service for HTTP and HTTPS access.

You can configure the REST API service to provide HTTP access locally and HTTPS access locally.

- Provide HTTP service.

a In a terminal window, run the `vmrest` command.

The command returns the IP address and port number from which you can access the HTTP service. The default IP address is 127.0.0.1:8697.

b Open a web browser and go to http://*address-returned-by-vmrest-command*.

c Click **Authorize** in the top-right corner of the Workstation Pro API Explorer page.

d Enter the user name and password you configured in Step 2.

- Provide HTTPS service.

You can configure the REST API service to provide HTTPS service. In this situation, when you use the `vmrest` command to start the REST API service, you must use the `-c` and `-k` options together to specify the certificate and private key.

a In a terminal window, run a command to generate a certificate and a private key.

The example command that follows, generates a self-signed OpenSSL-based certificate and a private key.

```
openssl req -x509 -newkey rsa:4096 -keyout workstationapi-key.pem -out
workstationapi-cert.pem -days 365 -nodes
```

b To start the Workstation Pro REST API service, run the command that follows. Replace the placeholders with the full path to the certificate file and the full path to the private key file.

```
vmrest -c certificate-file -k private-key-file
```

The command returns the IP address and port number from which you can access the HTTPS service.

c Open a web browser and go to https://*address-returned-by-vmrest-command*.

d Click **Authorize** in the top-right corner of the Workstation Pro API Explorer page.

e Enter the user name and password you configured in Step 2.

Using Workstation REST API Service to Manage Power Options of Encrypted Virtual Machines

You can power on, power off, suspend, pause, unpause, or retrieve the state of an encrypted virtual machine using the Workstation Pro REST API service.

Note To view the Workstation Pro API online, search VMware API Explorer for the appropriate version of the Workstation Pro API.

Prerequisites

You must perform the following steps before using the Workstation Pro REST API services:

- Connect to the IP address from which you can access the HTTP/HTTPS services of Workstation Pro REST API. The default IP address is 127.0.0.1:8697.
- Authenticate using the credentials you configured for the API service.

For more information on how to set the credentials for the Workstation Pro REST API service, see #unique_490

Procedure

1 After you log in to the Workstation Pro API service page, click **VM Power Management** from the list of API services.

2 To retrieve the power state of the encrypted virtual machine, click the **GET** operation, and then perform the following steps:

a Under the **Parameters** section, enter the ID and the encryption password of the virtual machine.

b Click **Try it Out!**

The Workstation Pro REST API service returns the power state of the encrypted virtual machine.

3 To manage the power options of the encrypted virtual machine, click the **PUT** operation, and then perform the following steps:

   a Under the **Parameters** section, enter the ID and the encryption password of the virtual machine.

   b Enter one of the following options in the **operation** field:

      - on
      - off
      - shutdown
      - suspend
      - pause
      - unpause

   a Click **Try it Out!**

      The Workstation Pro REST API service performs the operation you choose for the encrypted virtual machine.