

# VMware Tools User Guide

VMware Tools 10.3.0

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](http://www.vmware.com)

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

About This Book	5
Updated Information	6
<b>1 Introduction to VMware Tools</b>	<b>7</b>
VMware Tools Services	8
VMware Tools Lifecycle Management	9
VMware Tools Device Drivers	11
VMware User Process	13
Using Open VM Tools	14
Operating System Specific Packages for Linux Guest Operating Systems	16
<b>2 Installing VMware Tools</b>	<b>18</b>
Disable Access Protection from the McAfee Antivirus Virus Scan Console	19
Integration of VMware AppDefense with VMware Tools	20
Exclude AppDefense Component During Installation	21
Automating VMware Tools Installation for Multiple Windows Virtual Machines	22
Suppress Prompts About Unsigned Drivers on Windows Operating Systems Before Vista	22
Add VMware as a Trusted Publisher to Suppress Driver Prompts	23
Names of VMware Tools Features Used in Silent Installations	24
Manually Installing VMware Tools on a Windows Virtual Machine	27
Manually Installing VMware Tools on a Linux Virtual Machine	28
Manually Installing VMware Tools in a macOS Virtual Machine	31
Manually Installing VMware Tools on a Solaris Virtual Machine	32
<b>3 Upgrading VMware Tools</b>	<b>34</b>
Configure Virtual Machines to Automatically Upgrade VMware Tools	36
Manually upgrading VMware Tools in virtual machines	36
Performing an Automatic Upgrade of VMware Tools	37
<b>4 Configuring VMware Tools Components</b>	<b>39</b>
Configuring Network Interface Information	39
Exclude Specific File Systems from Quiesced Snapshots	40
Security Considerations for Configuring VMware Tools	41
Using the VMware Tools Configuration Utility	44
Configuring Time Synchronization Between Guest and Host Operating Systems	45
Disabling Time Synchronization	46

- [Use Device Connect or Disconnect](#) 47
  - [Using Custom VMware Tools Scripts](#) 48
  - [Retrieving Status Information About the Virtual Machine](#) 53
  
- 5** [Configuring Customer Experience Improvement Program](#) 56
  - [Categories of Information That VMware Receives](#) 56
  - [Join the Customer Experience Improvement Program in the vSphere Web Client](#) 56
  
- 6** [Troubleshooting VMware Tools Installation and Upgrade Issues](#) 57
  - [Installing or Upgrading to VMware Tools 10.3.0](#) 57
  
- 7** [Troubleshooting VMware Tools Components](#) 59
  - [Repair or Change Modules in Windows Virtual Machines](#) 59
  - [Starting the VMware User Process Manually If You Do Not Use a Session Manager](#) 59
  
- 8** [Uninstalling VMware Tools](#) 61
  
- 9** [FAQs about VMware Tools](#) 62

# About This Book

The *VMware Tools Guide* describes how to install, upgrade, and configure VMware Tools.

## Intended Audience

This information is intended for anyone who wants to install, upgrade, and configure VMware Tools. The information is written for system administrators who are familiar with virtualization.

## VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

# Updated Information

This *VMware Tools User Guide* is updated with each release of the product or when necessary.

This table provides the update history of the *VMware Tools User Guide*.

<b>Revision</b>	<b>Description</b>
12 JUL 2018	Initial release.

# Introduction to VMware Tools

# 1

VMware Tools is a set of services and modules that enable several features in VMware products for better management of, and seamless user interactions with, guests operating systems.

For example, VMware Tools has the ability to:

- Pass messages from the host operating system to the guest operating system.
- Customize guest operating systems as a part of the vCenter Server and other VMware products.
- Run scripts that help automate guest operating system operations. The scripts run when the power state of the virtual machine changes.
- Synchronize the time in the guest operating system with the time on the host operating system

VMware Tools Lifecycle Management provides a simplified and scalable approach for installation and upgrade of VMware Tools. It includes a number of feature enhancements, driver-related enhancements, and support for new guest operating systems. Run the latest version of VMware Tools or use open-vm-tools distributed with the Linux OS distribution. Although a guest operating system can run without VMware Tools, always run the latest version of VMware Tools in your guest operating systems to access the latest features and updates. You can configure your virtual machine to automatically check for and apply VMware Tools upgrades each time you power on your virtual machines. For information about enabling automatic upgrade of VMware Tools on your virtual machines, see *vSphere Virtual Machine Administration Guide*

This chapter includes the following topics:

- [VMware Tools Services](#)
- [VMware Tools Lifecycle Management](#)
- [VMware Tools Device Drivers](#)
- [VMware User Process](#)
- [Using Open VM Tools](#)
- [Operating System Specific Packages for Linux Guest Operating Systems](#)

## VMware Tools Services

The VMware Tools services start when the guest operating system starts. The service passes information between host and guest operating systems.

- **VMware Alias Manager and Ticket Service or VGAuthService:** VGAuthService in taskmgr provides support for SAML based authentication for vSphere Guest Operations, see [guest.SAMLTokenAuthentication](#) and [vim.vm.guest.GuestOperationsManager](#).
- **VMware Snapshot Provider Service:** VMware Snapshot Provider Service provides support for freezing or thawing file systems for VSS (Volume Shadow Copy Service).

---

**Note** This is applicable for Windows guest operating systems only.

---

- **VMware Tools Daemon Service:** This application runs in the background. It is called `vmtoolsd.exe` on Windows guest operating systems, `vmware-tools-daemon` on Mac OS X guest operating systems, and `vmtoolsd` on Linux, FreeBSD, and Solaris guest operating systems. The VMware Tools service performs the following tasks using the plug-ins:
  - `autohidpi` - Set guest screen resolution for Mac OS X guest operating systems.
  - `autoLogon` - Bypasses the guest operating system login when powering on a VM.
  - `autoUpgrade` - Handles VMware Tools upgrade operations.
  - `bitMapper` - Creates a bit map of disk blocks used by the guest operating system, used in vMotion.
  - `deployPkg` - Handles guest customization operations.
  - `desktopEvents` - Starting or stopping VMware Tools user service based on screen/X11 changes.

---

**Note** This is a VMware Tools user service plugin.

---

- `disableGuestHibernate` - Disables option for hibernation in guest operating system.
- `diskWiper` - Releases unused guest disk blocks so they can be reclaimed by the hypervisor.
- `dndcp` - Drag and drop, copy and paste operations. Enables copying and pasting of text, graphics, and files between guest operating systems and hosts or client desktops. This is a VMware Tools user service plugin.
- `guestInfo` - Collects and reports guest information and statistics to hypervisor.
- `hgfsServer` - HGFS server for transferring files, drag and drop and VMware Tools upgrade operations.
- `hgfsUsability` - Handles mapping HGFS folders to special user folders, adds HGFS links to the desktop.
- `hwUpgradeHelper` - Handles changes due to virtual hardware upgrade.

- `powerOps` - Handles graceful shutdown and reboot of the guest, and execution of scripts for a power operation.
- `resolutionKMS` - Handles communicating guest user interface topology to the `vmwgfx drm` (direct rendering manager) driver.

---

**Note** This plugin is for Linux only.

---

- `resolutionSet` - Handles guest screen re-sizing when `vmwgfx drm` (direct rendering manager) driver is not available.
- `timeSync` - Synchronizes guest clock with host clock at power on or resume.
- `vmbackup` - Handles freezing and thawing file systems during a quiesced snapshot operation.
- `vmtray` - Provides VMware Tools tray icon and pop-up menu.

---

**Note** This is a VMware Tools user service plugin.

---

- `vsep` - Manages NSX file and network introspection.
- `vix` - Handles guest operations related to files, processes and registry.

## VMware Tools Lifecycle Management

Starting with a major version 10.1.0, VMware tools added simplified and scalable approach for install and upgrade of VMware Tools, reboot less upgrade for newer Linux Tools, support for OSP upgrades, enhanced version reporting using UI and status reporting using API and UI. This version was released with a number of feature enhancements, driver related enhancements and support for new guest operating systems. With offline bundles and the integration with SCCM to distribute and upgrade VMware Tools, VMware Tools 10.2.0 brings in several improvements to lifecycle management.

- Offline bundles with VMware Tools VIB that can be installed on vSphere 5.5.x, 6.0.x and 6.5.x releases using vSphere Update Manager.
- Microsoft System Center Configuration Manager (SCCM) is used to manage the deployment of Windows applications across an enterprise and can be used to deploy VMware Tools. For more information, see [Deploying VMware Tools using SCCM](#).

VMware Tools 10.3.0 depends on and ships Microsoft Visual C++ 2017 Redistributable version 14.x. While preparing the system for VMware Tools 10.3.0 installation, Microsoft Visual C++ 2017 Redistributable is installed on the system as a prerequisite. For more information, see [Installing or Upgrading to VMware Tools 10.3.0](#).

## Mapping of VMware Tools and Guest Operating System

In earlier versions, VMware Tools ISO images were shipped with the ESXi image. These ISO images are deployed on ProductLocker partition of the ESXi. However, this approach poses a challenge due to limited space in ProductLocker. In order to address this space limitation, only `windows.iso`, `linux.iso` and `winPreVista.iso` are bundled with ESXi. Other ISO images are available for download from <https://myvmware.com> and will not be shipped with ESXi in the `tools-light vib`. ISO images for few end of life guest operating systems are frozen.

Table 1-1. VMware Tools support for Guest Operating Systems

ISO Images	Supported Guest Operating System	Available Version
<code>windows.iso</code>	Windows Vista SP2 and later <ul style="list-style-type: none"> <li>■ Windows OS level prerequisites               <ul style="list-style-type: none"> <li>■ Windows Server 2016</li> <li>■ Windows 10</li> <li>■ Windows Server 2012 R2 with <a href="#">Microsoft update KB2919355</a></li> <li>■ Windows 8.1 with <a href="#">Microsoft update KB2919355</a></li> <li>■ Windows Server 2012</li> <li>■ Windows 8</li> <li>■ Windows Server 2008 R2 Service Pack 1 (SP1)</li> <li>■ Windows 7 SP1</li> <li>■ Windows Server 2008 Service Pack 2 (SP2)</li> <li>■ Windows Vista SP2</li> </ul> </li> </ul>	10.3.0
<code>linux.iso</code>	Linux guest operating systems with glibc version 2.5 and later	10.3.0
<code>darwin.iso</code>	MAC OS versions 10.11 and later	10.3.0
<code>solaris.iso</code>	Solaris operating systems	10.3.0

Table 1-2. VMware Tools support for frozen Guest Operating Systems

ISO images	Supported Guest Operating System	Version of VMware Tools
<code>winPre2k.iso</code>	Versions earlier than Windows 2000	7.7.0
<code>netware.iso</code>	Netware operating systems	8.1.0
<code>winPreVista.iso</code>	Windows 2000, Windows XP, and Windows Server 2003 <p><b>Note</b> The Windows pre-Vista iso image for VMWare Tools is no longer packaged with ESXi. The Windows pre-Vista iso image is available for download by users who require it.</p>	10.0.12

Table 1-2. VMware Tools support for frozen Guest Operating Systems (continued)

ISO images	Supported Guest Operating System	Version of VMware Tools
linuxPreGLibc25.iso	Linux guest operating systems earlier than RHEL 5, SLES 11, and other distributions with glibc version earlier than 2.5	10.0.12
darwinPre15.iso	MAC OS versions earlier than 10.10.x	10.0.12

## VMware Tools Device Drivers

Device drivers improve sound, graphics, networking, and storage performance. If you perform a custom VMware Tools installation or reinstallation, you can choose which drivers to install.

The set of drivers that are installed when you install VMware Tools depends on the guest operating system and the VMware product. For detailed information about the features or functionality that these drivers enable, including configuration requirements, best practices, and performance, see the documentation for your VMware product. The following device drivers can be included with VMware Tools.

### SVGA driver

This virtual driver enables 32-bit displays, high display resolution, and faster graphics performance. When you install VMware Tools, a virtual SVGA driver replaces the default VGA driver, which allows for only 640 X 480 resolution and 16-color graphics.

On Windows guest operating systems whose operating system is Windows Vista or later, the VMware SVGA 3D (Microsoft - WDDM) driver is installed. This driver provides the same base functionality as the SVGA driver, and it adds Windows Aero support.

### Paravirtual SCSI driver

When you create a virtual machine, if you specify that you want the virtual machine to use a BusLogic adapter, the guest operating system uses the SCSI driver that VMware Tools provides. A VMware Paravirtual SCSI driver is included for use with Paravirtual SCSI devices. This driver for VMware Paravirtual SCSI adapters enhances the performance of some virtualized applications. Drivers for other storage adapters are either bundled with the operating system, or they are available from third-party vendors.

For example, Windows Server 2008 defaults to LSI Logic SAS, which provides the best performance for that operating system. In this case, the LSI Logic SAS driver provided by the operating system is used.

VMware supplies a special SCSI driver for virtual machines that are configured to use the BusLogic virtual SCSI adapter. Virtual machines do not need this driver if they do not need to access any SCSI devices or if they are configured to use the LSI Logic virtual SCSI adapter.

The driver is included as part of the VMware Tools package or comes bundled with VMware ESX/ ESXi. It is available on the host as a floppy image at `/vmimages/floppies/vmcsis.flp`. The driver can be used in Windows XP, Windows Server 2003, or Windows 2000.

## VMXNet NIC drivers

The VMXNET and VMXNET3 networking drivers improve network performance. The set of drivers that are used depends on how you configure device settings for the virtual machine. Search the VMware Knowledge Base for information on which guest operating systems support these drivers.

When you install VMware Tools, a VMXNET NIC driver replaces the default vance driver.

## Mouse driver

The virtual mouse driver improves mouse performance. This driver is required if you use third-party tools such as Microsoft Terminal Services.

## Audio driver

This sound driver is required for 64-bit Windows XP, 32-bit Windows Server 2003, 64-bit Windows Server 2003, Windows Server 2008, Windows 7, and Windows Vista guest operating systems.

## Guest Introspection Driver

The two Guest Introspection drivers are the File Introspection driver and the Network Introspection driver. You can install the two drivers separately. When you install VMware Tools, by default, the Guest Introspection drivers are not installed.

- File Introspection Driver: The File Introspection driver uses the hypervisor to perform antivirus scans without a bulky agent. This strategy avoids resource bottlenecks and optimizes memory use.
- Network Introspection Driver: The Network Introspection driver supports NSX for vSphere Activity Monitoring.

## Memory control driver

This driver is required for memory ballooning and is recommended if you use VMware vSphere. Excluding this driver hinders the memory management capabilities of the virtual machine in a vSphere deployment.

## Modules and drivers that support making automatic backups of virtual machines

If the guest operating system is Windows Vista, Windows Server 2003, or other newer Windows operating systems, a Volume Shadow Copy Services (VSS) module is installed. For other, earlier Windows operating systems, the Filesystem Sync driver is installed. These modules allow external third-party back up software that is integrated with vSphere to create application-consistent snapshots. During the snapshot process, certain processes are paused and virtual machine disks are quiesced. The modules also support quiescing snapshot on Linux OS

## VMCI and VMCI Sockets drivers

The Virtual Machine Communication Interface driver supports fast and efficient communication between virtual machines and the hosts they run on. Developers can write client-server applications to the VMCI Sock (vsock) interface to make use of the VMCI virtual device.

### **VMware drivers for Linux**

The drivers for Linux are automatically installed during your operating system installation, eliminating the need to separately install drivers after OS installation. VMware actively maintains the source code for VMware Paravirtual drivers, VMXNET, VMXNET3 and kernel modules, and any Linux distributions creating new OS releases automatically include the latest VMware drivers.

Do not delete or replace existing inbox drivers for Linux that are distributed by your OS vendors. Deleting or replacing these drivers might cause conflict with future updates to the drivers. Contact your OS vendor or OS community for availability of specific updates to drivers.

See <http://kb.vmware.com/kb/2073804> for information about availability, maintenance, and support policy for inbox drivers for Linux.

### **VMHGFS driver**

If you use Workstation or Fusion, you can install the Shared Folders component. With Shared Folders, you can easily share files among virtual machines and the host computer. The VMHGFS driver is a file system redirector that allows file system redirection from the guest operating system to the host file system. This driver is the client component of the Shared Folders feature and provides an easy to use alternative to NFS and CIFS file sharing that does not rely on the network. For Linux distributions with kernel version 3.10 and later, a new FUSE based Shared Folders client is used as a replacement for the kernel mode client.

### **Appdefense**

VMware Tools installation include the VMware AppDefense, a security management and monitoring solution. AppDefense agent can be installed on the guest virtual machine using the VMware Tools installer. However, VMware Tools cannot install the AppDefense component automatically. You need to install the component manually.

## **VMware User Process**

With the VMware user process, you can use such features as copy and paste, drag and drop with VMware products that support these features.

In Linux, Solaris, Windows and FreeBSD guest operating systems, VMware Tools uses the VMware User process executable file that implements fit-guest-to-window feature.

The user process starts automatically when you log in to a Windows guest operating system. On Linux, the user process starts when you start a Desktop Environment session. The user process can also be started manually.

The program file for this process is called `vmtoolsd.exe` on Windows guest operating systems and `vmtoolsd` on Linux, Solaris, and FreeBSD guest operating systems. In POSIX, it is `vmtoolsd` with `-n vmusr` on command line interface. The user process supports the following tasks:

- Enables copy and paste of text between guest operating system and the vSphere Web Client or the Workstation, Fusion, or Player host operating system. For virtual machines that are used with Workstation or Fusion, you can copy and paste files between the host operating system and Windows, Linux, Solaris, and FreeBSD guest operating systems.
- On Linux, Solaris, Windows, and FreeBSD guest operating systems, grabs and releases the pointer if the SVGA driver is not installed.
- On Linux, Solaris, and FreeBSD guest operating systems, fits the screen display resolution of the guest to the screen resolution of the vSphere Web Client or the Workstation, Fusion, or Player host operating system, if running in full screen mode. If running in normal (windowed) mode, fits the screen resolution of the guest to the size of the window on the client or host.
- For virtual machines used with Workstation or Fusion, allows you to drag files between the host operating system and Windows, Linux, Solaris, and FreeBSD guest operating systems.

## Using Open VM Tools

Open VM Tools (`open-vm-tools`) is the open source implementation of VMware Tools for Linux guest operating systems.

The `open-vm-tools` suite is bundled with some Linux operating systems and is installed as a part of the OS, eliminating the need to separately install the suite on guest operating systems. All leading Linux vendors support the `open-vm-tools` suite on vSphere, Workstation, and Fusion, and bundle `open-vm-tools` with their product releases. For information about OS compatibility check for the `open-vm-tools` suite, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

---

**Note** Use of `open-vm-tools` with a OS distribution which is not listed under *VMware Compatibility Guide* must be certified by VMware.

---

Bundling `open-vm-tools` with Linux OS releases reduces virtual machine downtime because all updates to the `open-vm-tools` suite are included with the OS maintenance patches and updates. You do not have to maintain separate maintenance cycles for `open-vm-tools` suite updates. This is also applicable for VMware guest operating system drivers.

In some cases, `open-vm-tools` is installed by default when you install your guest operating systems. In other cases, the `open-vm-tools` suite is not installed by default, unless specifically selected during installation.

Follow the installation instructions provided by your OS vendor for your specific release or check the partner Web site at <http://partnerweb.vmware.com/GOSIG/home.html>.

VMware fully supports open-vm-tools that are developed in collaboration with OS vendors and open source communities and recommends using open-vm-tools that are redistributed by your OS vendors.

## Open VM Tools Packages

For better managing guest operating systems, the open-vm-tools suite includes the following packages:

- The core open-vm-tools package contains the core open-vm-tools user space utilities, application programs, and libraries, including `vmtoolsd`, to help effectively manage communication between your host and guest OSs. This package includes features as, synchronizing guest OS clocks with the virtualization platform, transferring files between hosts and guests, sending heartbeat information from guest OSs to the virtualization infrastructure to support vSphere High Availability (HA), publishing resource utilization and networking information of the guest OSs to the virtualization platform, and so on.
- The `open-vm-tools-desktop` package is optional and includes additional user programs and libraries to improve the interactive functionality of desktop operations of your virtual machines. The package enables you to resize a guest display to match its host console window or the VMware Remote Console Window for vSphere. The package also allows you to copy and paste between host and guest OSs, as well as to drag and drop between guests and a host for the VMware Workstation and VMware Fusion products.
- The `open-vm-tools-devel` package contains libraries and additional documentation for developing `vmtoolsd` plug-ins and applications.
- The `open-vm-tools-debuginfo` package contains the source code for open-vm-tools and binary files. For the latest copy of the Open VM Tools source code, see the GitHub Web site at <https://github.com/vmware/open-vm-tools>.

List of operating systems with open-vm-tools

- Red Hat Enterprise Linux 7.0 and later releases
- SUSE Linux Enterprise 12 and later releases
- Ubuntu 14.04 and later releases
- CentOS 7 and later releases
- FreeBSD 10.3, 10.4 & 11.1
- Debian 7.x and later releases
- Oracle Linux 7 and later
- Fedora 19 and later releases
- openSUSE 11.x and later releases

---

**Note** To manually install open-vm-tools on a FreeBSD virtual machine, see [FreeBSD 10.x](#) and [FreeBSD 11.x](#)

---

---

**Important** If you use an open-vm-tools, the VMware Tools status is Guest Managed on the virtual machine **Summary** tab. The status Guest Managed means that you cannot use the vCenter Server to manage VMware Tools and you cannot use vSphere Update Manager to upgrade VMware Tools.

---

For information about the open-vm-tools support policy and availability, see the VMware knowledge base article at <http://kb.vmware.com/kb/2073803>.

## Operating System Specific Packages for Linux Guest Operating Systems

For vSphere deployments, VMware provides operating system specific packages (OSPs) as a packaging and distribution mechanism for VMware Tools. These VMware Tools OSPs are packaged using native package formats and standards such as rpm and deb.

---

**Note** Operating System Specific Packages are not provided for new Linux operating systems that have open-vm-tools. For information about compatibility support for guest operating system, see the *VMware Compatibility Guide*.

---

Using OSPs provides the following benefits:

- You can use the native update mechanisms of the guest operating system to download, install, and manage VMware Tools.
- You can upgrade to the latest version of VMware Tools without having to upgrade to the latest version of vSphere.
- Because VMware Tools OSPs follow the best practices and standards of the specific Linux operating system, OSPs use standard mechanisms for determining dependencies among packages. These mechanisms allow you to audit the packages on virtual machines with or without graphics components.
- You can use standard operating system tools to examine OSPs during VMware Tools installation. This process allows you to easily determine which components to install and to verify the validity of the packaging.

---

**Important** Use OSPs if you want to use native update mechanisms, rather than vCenter Server, to manage updates for VMware Tools. If you use an OSP, the VMware Tools status is Guest Managed on the virtual machine **Summary** tab. The status Guest Managed means that you cannot use the vCenter Server to manage VMware Tools and you cannot use vSphere Update Manager to upgrade VMware Tools.

---

For more information, go to the VMware Operating System Specific Packages Web site, at <https://www.vmware.com/download/packages.html>. For more information on installing OSPs, see the VMware Tools Installation Guide for Operating System Specific Packages for ESX/ESXi version 4.1 and later at <https://packages.vmware.com/tools/docs/manuals/osp-esx-41-install-guide.pdf> and ESXi versions 5.x and 6.x at <https://packages.vmware.com/tools/docs/manuals/osp-esxi-51-install-guide.pdf>

# Installing VMware Tools

# 2

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.

If you are using VMware Fusion, Workstation Player, or Workstation Pro, 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.

If you are using VMware Fusion, Workstation Player, or Workstation Pro, 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 was not downloaded or if no VMware Tools ISO file for that operating system was ever 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.

---

**Note** On ESXi hosts, for guest operating systems that do not have the necessary VMware Tools ISOs bundled, users must set up the `ProductLockerLocation` variable on all the VMware Tools ISO images to manage VMware Tools on these guests. Attempts to upgrade or install without setting up the `ProductLockerLocation` variable fails with missing ISO error. For more information, see the VMware Knowledge base article at <http://kb.vmware.com/kb/2129825>.

---

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>.

This chapter includes the following topics:

- [Disable Access Protection from the McAfee Antivirus Virus Scan Console](#)
- [Integration of VMware AppDefense with VMware Tools](#)
- [Automating VMware Tools Installation for Multiple Windows Virtual Machines](#)
- [Manually Installing VMware Tools on a Windows Virtual Machine](#)
- [Manually Installing VMware Tools on a Linux Virtual Machine](#)
- [Manually Installing VMware Tools in a macOS Virtual Machine](#)
- [Manually Installing VMware Tools on a Solaris Virtual Machine](#)

## Disable Access Protection from the McAfee Antivirus Virus Scan Console

Access Protection has to be disabled in the McAfee Antivirus Scan Console before installing VMware Tools in a Windows guest operating system. For more information, see the VMware Knowledge Base article <https://kb.vmware.com/kb/1009965>

### Prerequisites

- Power on the virtual machine
- Use McAfee Antivirus in Standard Mode

## Procedure

- 1 Install VMware Tools before installing McAfee Antivirus on the Windows guest operating system.

---

**Note** McAfee Antivirus will, however, prevent VMware Tools upgrade if run in Maximum Protection mode.

---

- 2 Disable **Access Protection** from the McAfee Antivirus Virus Scan Console when either installing or upgrading VMware Tools.
  - a Select **Start > Programs > McAfee > Virus Scan Console**.
  - b Right-click the **Access Protection** icon in the **Tasks** window and select **Disable** from the pop-up menu.

## What to do next

- Install VMware Tools.
- Re-activate **Access Protection** when your VMware Tools upgrade or installation is complete.

# Integration of VMware AppDefense with VMware Tools

VMware Tools installation includes the VMware AppDefense, a security management, and monitoring solution. This data center security solution is based on application control, detection, and response. AppDefense agent can be installed on the guest virtual machine using the VMware Tools installer. Virtual machines with VMware Tools installed are monitored and managed whenever they are started up on an ESXi host that has the solution installed. However, VMware Tools cannot install the AppDefense component automatically. The component must be installed manually.

## Prerequisites

- If you have installed VMware AppDefense version older than 1.2.1.0 using VMware AppDefense installer, uninstall the older version.
- Ensure that the guest virtual machine is hosted on ESXi 6.5 or later.
- This feature is available on a fresh installation or custom installation of VMware Tools. It is not available by default.
- Ensure that the guest virtual machine has a supported version of Windows installed. AppDefense component supports the following Windows 64-bit guest operating systems running on a ESXi server.
  - Windows 2008 R2
  - Windows 2012
  - Windows 2012 R2
  - Windows 2016

**Procedure**

- 1 Follow the procedure [Manually Installing VMware Tools on a Windows Virtual Machine](#).
- 2 After you select the **Custom** setup in step 4, choose **Appdefense** from the list.
- 3 Follow the remaining steps in the procedure.

**Results**

VMware AppDefense component is installed in your guest operating system.

**Exclude AppDefense Component During Installation**

Installing VMware Tools without the AppDefense driver.

**Procedure**

- 1 For a silent installation, run the command.
 

```
setup64.exe /s /v"/qn ADDLOCAL=All REMOVE=AppDefense
```

 or
 

```
setup64.exe /s /v"/qn ADDLOCAL=All REMOVE=AppDefense,<other unwanted feature list>
```
- 2 In a manual installation,
  - AppDefense is not part of the typical install option.
  - AppDefense is unselected by default in the custom install option.
- 3 Using the Full Install option, AppDefense is installed during installation,
  - AppDefense must be removed manually using the **Programs and Features** option in your operating system.
    - a Select **VMware Tools**.
    - b Right click and select **Change**. VMware Tools installer is launched.
    - c Select **Modify**.
    - d Click **Next**.
    - e Navigate to **AppDefense** node in the tree.
    - f Right click and select **Entire feature will be unavailable**.
    - g Click **Next**.
    - h Click **Change**.
    - i Click **Finish**.

**Results**

AppDefense driver is not installed while installing VMware Tools.

# Automating VMware Tools Installation for Multiple Windows Virtual Machines

If you are installing VMware Tools in multiple virtual machines with Windows guest operating systems, you can automate its installation and specify options for the components to include or exclude.

## Prerequisites

- Power on the virtual machine.
- Log in to the guest operating system as an administrator.
- If you plan to use the `setup.exe` command at the command line to run the VMware Tools installation, edit the virtual machine settings to connect the virtual CD/DVD drive to the VMware Tools ISO image. In VMware Workstation Pro and Workstation Player, the `windows.iso` file is on the host in the directory where you installed Workstation Pro or Workstation Player.
- If you plan to use MSI arguments to specify options regarding the silent installation, go to the Windows Installer page on the MSDN Web site to familiarize yourself with the syntax. You can use these arguments with the `setup.exe` command or place them in the vCenter Server dialog box for automatic installations and upgrades.
- To prevent some VMware Tools components from being installed, familiarize yourself with the VMware Tools component names so that you can specify which components to exclude. See [Names of VMware Tools Components Used in Silent Installations](#).
- If you are installing VMware Tools from a beta or release candidate of a VMware product, suppress prompts about unsigned drivers. See [Suppress Prompts About Unsigned Drivers on Windows Operating Systems Before...](#) and [Add VMware as a Trusted Publisher to Suppress Driver Prompts...](#)

## Procedure

- 1 In the vSphere Web Client inventory, select the host, cluster, or datacenter and click the **Virtual Machines** tab.
- 2 Select the virtual machines, right-click and select **Guest OS > Install VMware Tools**.
- 3 Provide the installation or upgrade configuration information.

## Suppress Prompts About Unsigned Drivers on Windows Operating Systems Before Vista

If you are installing a beta or RC version of VMware Tools in a Windows Server 2003 or earlier guest operating system, you can use a computer properties setting to suppress prompts that interfere with automatic installation of VMware Tools.

The version of VMware Tools included in a beta or release candidate version of a VMware product usually has some drivers that are signed only by VMware. If you are installing one of these versions in many virtual machines that run Windows Server 2003 or earlier guest operating systems, or if you plan to install VMware Tools from the command line, you can suppress prompts about unsigned drivers. If you do not suppress the prompts, during a VMware Tools installation, a message box appears several times and requires you to click **Continue Anyway** to complete the installation.

#### Prerequisites

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

#### Procedure

- 1 In the Windows Server 2003 or earlier guest operating system, in the **Start** menu, right-click **My Computer** and select **Properties**.
- 2 In the **System Properties** dialog box, click the **Hardware** tab and click **Driver Signing**.
- 3 In the **Driver Signing Options** dialog box, click **Ignore**, click **OK**, and click **OK** again.

#### Results

When you run the VMware Tools installer, no prompts appear in the guest operating system.

#### What to do next

Install VMware Tools.

## Add VMware as a Trusted Publisher to Suppress Driver Prompts

If you are installing a beta or RC version of VMware Tools in a Windows Vista or later guest operating system, you can add a VMware certificate to suppress prompts that interfere with automatic installation of VMware Tools.

The version of VMware Tools included in a beta or release candidate version of a VMware product usually has some drivers that are signed only by VMware. If you are installing one of these versions in many virtual machines that run Windows Vista or later guest operating systems, or if you plan to install VMware Tools from the command line, add a VMware security certificate to the trusted publishers group. If you do not add the VMware certificate, during a VMware Tools installation, a message box appears several times and prompts you to install device software from VMware.

#### Prerequisites

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

- Obtain a copy of the `certmgr.exe` application and copy it to the guest operating system on which you plan to install VMware Tools. The `certmgr.exe` application is included in the Windows SDK

---

**Note** This is applicable only for Beta or RC version of VMware Tools.

---

### Procedure

- 1 Use the certificate export wizard to create a VMware certificate file.
  - a Locate a signed VMware file, such as a VMware `.exe` or `.sys` file.
  - b Right-click the file and select **Properties**.
  - c Click the **Digital Signatures** tab and select **View Certificate**.
  - d Click the **Details** tab and click **Copy to File**.
  - e Follow the prompts and name the exported certificate `vmware.cer`.
- 2 Copy the exported VMware certificate to the guest operating system on which you plan to install VMware Tools.
- 3 In the guest operating system, run the `certmgr.exe` command to add the VMware certificate to the trusted publishers group.

```
certmgr.exe -add vmware.cer -c -s -r localMachine TrustedPublisher
```

### Results

When you run the VMware Tools installer, no prompts appear in the guest operating system.

### What to do next

Install VMware Tools.

## Names of VMware Tools Features Used in Silent Installations

In Windows virtual machines, when running an automatic installation or running an installation of VMware Tools using the command line, you can specify which VMware Tools components to install.

Because VMware Tools contains so many components, if you do not want to install particular components, you specify which ones to exclude rather than which ones to include. The syntax is `ADDLOCAL=ALL REMOVE=component`. The valid values for VMware Tools components are listed in the following table.

Component names are case-sensitive. Not all components are installed on all operating systems.

Table 2-1. VMware Tools Component Values

Valid Component Values	Description
Drivers	<p data-bbox="472 285 536 310"><b>Audio</b></p> <p data-bbox="507 327 1337 352">Audio driver for 64-bit operating systems and Windows Vista and later systems.</p> <p data-bbox="472 390 568 415"><b>BootCamp</b></p> <p data-bbox="507 432 863 457">Driver for Mac BootCamp support.</p> <p data-bbox="472 495 544 520"><b>MemCtl</b></p> <p data-bbox="507 537 1423 625">VMware memory control driver. Use this driver if you plan to use this virtual machine in a vSphere environment. Excluding this feature hinders the memory management capabilities of the virtual machine running in a vSphere environment.</p> <p data-bbox="472 663 536 688"><b>Mouse</b></p> <p data-bbox="507 705 1374 760">VMware mouse driver. Excluding this feature decreases mouse performance in your virtual machine.</p> <p data-bbox="472 798 544 823"><b>PVSCSI</b></p> <p data-bbox="507 840 1401 894">Driver for VMware Paravirtual SCSI adapters, which enhance the performance of some virtualized applications.</p> <p data-bbox="472 932 520 957"><b>SVGA</b></p> <p data-bbox="507 974 1414 1029">VMware SVGA driver. Excluding this feature limits the display capabilities of your virtual machine.</p> <p data-bbox="472 1066 520 1092"><b>Sync</b></p> <p data-bbox="507 1108 1422 1230">Filesystem Sync driver, which enables backup applications to create application-consistent snapshots. This driver ensures that no I/O is written during snapshot creation. This driver is used if the guest operating system is earlier than Windows Server 2003. Newer operating systems use the VSS driver.</p> <p data-bbox="472 1268 584 1293"><b>ThinPrint</b></p> <p data-bbox="507 1310 1422 1398">Driver that enables printers added to the host operating system to appear in the list of available printers in the virtual machine. This virtual printing feature does not require any additional printer drivers to be installed in the virtual machine.</p> <hr/> <p data-bbox="507 1423 1362 1449"><b>Note</b> VMware Tools does not support ThinPrint features for vSphere 5.5 and later</p> <hr/> <p data-bbox="472 1486 520 1512"><b>VMCI</b></p> <p data-bbox="507 1528 1394 1650">Virtual Machine Communication Interface driver. This driver allows virtual machines to communicate with the hosts on which they run without using the network. Developers can write client-server applications to the VMCI Sock (vsock) interface to make use of the VMCI virtual device.</p> <p data-bbox="472 1688 520 1713"><b>Hgfs</b></p> <p data-bbox="507 1730 1426 1818">VMware shared folders driver. Use this driver if you plan to use this virtual machine with VMware Workstation, Player, or Fusion. Excluding this feature prevents you from sharing a folder between your virtual machine and the host system.</p> <p data-bbox="472 1856 544 1881"><b>VMXNet</b></p> <p data-bbox="507 1898 879 1923">VMware VMXnet networking driver.</p>

Table 2-1. VMware Tools Component Values (continued)

Valid Component Values	Description
	<p><b>VMXNet3</b></p> <p>Next-generation VMware VMXnet networking driver for virtual machines that use virtual hardware version 7 and higher. For more information, see the VMware Knowledge Base article <a href="#">1001805</a>. VMXNET 3 adds several new features, such as multiqueue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery. VMXNET 3 is not related to VMXNET or VMXNET 2. Receive Side Scaling is enabled by default. VMware Tools 10.3.0 adds receive data ring support for Windows VMXNET3 driver.</p> <p>Virtual hardware version 7 corresponds to ESX/ESXi 4.x compatibility.</p> <p><b>FileIntrospection</b></p> <p>NSX File Introspection driver, <code>vsepflt.sys</code>. The first of the two guest introspection drivers. You can install it separately, without installing the NSX Network Introspection driver.</p> <p><b>NetworkIntrospection</b></p> <p>NSX Network Introspection driver, <code>vnetflt.sys</code>. The second of the two guest introspection drivers. VMware Tools 10.2.5 supports <code>vnetWFP</code> driver for Windows 7 and later.</p> <p><b>VSS</b></p> <p>Driver for creating automatic backups. This driver is used if the guest operating system is Windows Vista, Windows Server 2003, or other newer operating system. Linux and older Windows operating systems use the Filesystem Sync driver.</p> <p><b>AppDefense</b></p> <p>VMware AppDefense component. The AppDefense components consists of <code>glxgi.sys</code> kernel mode driver and <code>gisvc.exe</code> user mode service.</p>
Toolbox	<p><b>Perfmon</b></p> <p>Driver for WMI performance logging.</p>

**Important** One way to determine the component values to use is to run the interactive VMware Tools installer with full logging turned on, select the components that you want installed, and then search the log files for the ADDLOCAL and REMOVE properties. The log files show the names used by the program. The following command runs the interactive installer with full logging turned on:

```
Setup.exe /s /v"/qn /l*v ""%TEMP%\vmmsi.log""
```

# Manually Installing VMware Tools on a Windows Virtual Machine

Guest operating system Windows 2000 and earlier, Windows XP, Windows Server 2003, Windows Vista, and later support VMware Tools.

## Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- For vSphere virtual machines, determine whether you have the latest version of VMware Tools. In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.
- For Workstation Player, Fusion, and Workstation Pro virtual machines, if you connected the virtual machine's virtual CD/DVD drive to an ISO image file when you installed the operating system, change the setting so that the virtual CD/DVD drive is configured to autodetect a physical drive.

The autodetect setting enables the virtual machine's first virtual CD/DVD drive to detect and connect to the VMware Tools ISO file for a VMware Tools installation. This ISO file looks like a physical CD to your guest operating system. Use the virtual machine settings editor to set the CD/DVD drive to autodetect a physical drive.

- Log in as an administrator unless you are using an older Windows operating system. Any user can install VMware Tools in a Windows 95, Windows 98, or Windows ME guest operating system. For operating systems later than these, you must log in as an administrator.
- If you use vSphere and plan to install the Guest Introspection Thin Agent driver, see the system requirements listed in the *vShield Quick Start Guide*. The vShield component is not installed by default. You must perform a custom installation and include that component.
- The AppDefense component is not installed by default. You must perform a custom installation and include that component.

## Procedure

- 1 Select the menu command to mount the VMware Tools virtual disk on the guest operating system.

VMware Product	Action
vSphere Client (HTML5)	Right-click the virtual machine and select <b>Guest OS &gt; Install (or Upgrade) Tools</b>
vSphere Client	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware</b>
vSphere Web Client	Right-click the virtual machine and select <b>Guest OS &gt; Install (or Upgrade) VMware Tools</b>
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>

VMware Product	Action
Workstation Pro	VM > Install (or Upgrade) VMware Tools
Workstation Player	Player > Manage > Install (or Upgrade) VMware Tools

- If you are using vCenter Server and are performing an upgrade or reinstallation, in the **Install/Upgrade VMware Tools** dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

- 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.

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

- Follow the on-screen prompts.

If you use vSphere, to install nondefault components, such as the Guest Introspection Thin Agent driver, select the **Custom** setup.

- 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.

---

- When prompted, reboot the virtual machine.

### Results

If you are using vCenter Server, the **VMware Tools** label on the **Summary** tab changes to **OK**.

### What to do next

If you upgraded VMware Tools as part of a vSphere upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

## Manually Installing VMware Tools on a Linux Virtual Machine

For Linux virtual machines, you manually install VMware Tools from the command line. For later Linux distributions, use the integrated open-vm-tools version.

## Prerequisites

For more information on OS compatibility for open-vm-tools, see the *VMware Compatibility Guide* at <https://www.vmware.com/resources/compatibility/search.php>.

- 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.
- For vSphere virtual machines, determine whether you have the latest version of VMware Tools. In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.

## Procedure

- 1 Select the menu command to mount the VMware Tools virtual disk on the guest operating system.

VMware Product	Action
vSphere Client (HTML5)	Right-click the virtual machine and select <b>Guest OS &gt; Install (or Upgrade) Tools</b>
vSphere Client	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware</b>
vSphere Web Client	Right-click the virtual machine and select <b>Guest OS &gt; Install (or Upgrade) VMware Tools</b>
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>
Workstation Pro	<b>VM &gt; Install (or Upgrade) VMware Tools</b>
Workstation Player	<b>Player &gt; Manage &gt; Install (or Upgrade) VMware Tools</b>

- 2 In the virtual machine, open a terminal window.
- 3 Run the `mount` command with no arguments to determine whether your Linux distribution automatically mounted the VMware Tools virtual CD-ROM image.

If the CD-ROM device is mounted, the CD-ROM device and its mount point are listed in a manner similar to the following output:

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

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

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

```
mkdir /mnt/cdrom
```

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

- b Mount the CD-ROM drive.

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

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

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

```
cd /tmp
```

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

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

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

```
ls mount-point
```

- 8** Uncompress the installer.

```
tar xzpf /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.

- 9** If necessary, unmount the CD-ROM image.

```
umount /dev/cdrom
```

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

- 10** Run the installer and configure VMware Tools as a root user

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

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.

---

- 11 Follow the prompts to accept the default values, if appropriate for your configuration.
- 12 Follow the instructions at the end of the script.

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

### Results

If you are using vCenter Server, the **VMware Tools** label on the **Summary** tab changes to **OK**.

### What to do next

If you upgraded VMware Tools as part of a vSphere upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

## Manually Installing VMware Tools in a macOS Virtual Machine

For macOS virtual machines you install or upgrade VMware Tools using an installer assistant.

If you use VMware Fusion or ESXi on a computer with an Apple label, you can create Mac OS X Server (10.5 or later) virtual machines and install VMware Tools.

### Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.

## Procedure

- 1 Select the menu command to mount and open the VMware Tools virtual disc on the guest operating system.

VMware Product	Menu Command
vSphere Client	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware Tools</b> and select <b>Interactive Tools Installation</b> or <b>Interactive Tools Upgrade</b>
vSphere Web Client	Right-click the virtual machine in the vCenter inventory and select <b>All vCenter Actions &gt; Guest OS &gt; Install/Upgrade VMware Tools</b>
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>

- 2 Open **Install VMware Tools** on the VMware Tools virtual disc, follow the prompts in the installer assistant, and click **OK**.

## Results

The virtual machine restarts to have VMware Tools take effect.

# 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.
- For vSphere virtual machines, determine whether you have the latest version of VMware Tools. In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.

## Procedure

- 1 Select the menu command to mount the VMware Tools virtual disk on the guest operating system.

VMware Product	Action
vSphere Client (HTML5)	Right-click the virtual machine and select <b>Guest OS &gt; Install (or Upgrade) Tools</b>
vSphere Client	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware</b>
vSphere Web Client	Right-click the virtual machine and select <b>Guest OS &gt; Install (or Upgrade) VMware Tools</b>

VMware Product	Action
Fusion	Virtual Machine > Install (or Upgrade) VMware Tools
Workstation Pro	VM > Install (or Upgrade) VMware Tools
Workstation Player	Player > Manage > Install (or Upgrade) VMware Tools

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

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

```
cd /tmp
```

- Extract VMware Tools.

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

- 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.

- 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.

## Results

If you are using vCenter Server, the **VMware Tools** label on the **Summary** tab changes to **OK**.

## What to do next

If you upgraded VMware Tools as part of a vSphere upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

# Upgrading VMware Tools

# 3

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.

---

For vSphere virtual machines, you can use one of the following processes to upgrade multiple virtual machines at the same time.

- Log in to vCenter Server, select a host or cluster, and on the **Virtual Machines** tab specify the virtual machines on which to perform a VMware Tools upgrade.
- Use Update Manager to perform an orchestrated upgrade of virtual machines at the folder or datacenter level.

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.

**Table 3-1. Virtual Machine Compatibility Options**

Compatibility	Description
ESXi 6.7 Update 2 and later	This virtual machine (hardware version 15) is compatible with ESXi 6.7 Update 2 and later.
ESXi 6.7 and later	This virtual machine (hardware version 14) is compatible with ESXi 6.7 and ESXi 6.7 Update 2.
ESXi 6.5 and later	This virtual machine (hardware version 13) is compatible with ESXi 6.5, ESXi 6.7, and ESXi 6.7 Update 2.
ESXi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0, ESXi 6.5, ESXi 6.7, and ESXi 6.7 Update 2.
ESXi 5.5 and later	This virtual machine (hardware version 10) is compatible with ESXi 5.5, ESXi 6.0, ESXi 6.5, ESXi 6.7, and ESXi 6.7 Update 2.
ESXi 5.1 and later	This virtual machine (hardware version 9) is compatible with ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, ESXi 6.7, and ESXi 6.7 Update 2.
ESXi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXi 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, ESXi 6.7, and ESXi 6.7 Update 2.
ESX/ESXi 4.x and later	This virtual machine (hardware version 7) is compatible with ESX/ESXi 4.x, ESXi 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, ESXi 6.7, and ESXi 6.7 Update 2.
ESX/ESXi 3.5 and later	This virtual machine (hardware version 4) is compatible with ESX/ESXi 3.5, ESX/ESXi 4.x, ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, ESXi 6.7, and ESXi 6.7 Update 2. It is also compatible with VMware Server 1.0 and later. ESXi 5.0 does not allow creation of virtual machines with ESX/ESXi 3.5 and later compatibility, but you can run such virtual machines if they were created on a host with different compatibility.

For more information, see the documentation for your specific VMware product.

This chapter includes the following topics:

- [Configure Virtual Machines to Automatically Upgrade VMware Tools](#)
- [Manually upgrading VMware Tools in virtual machines](#)
- [Performing an Automatic Upgrade of VMware Tools](#)

# Configure Virtual Machines to Automatically Upgrade VMware Tools

You can configure virtual machines to automatically update VMware Tools.

---

**Note** Automatic VMware Tools upgrade is not supported for virtual machines with Solaris or NetWare guest operating systems.

---

## Prerequisites

- Verify that the virtual machines have a version of VMware Tools shipped with ESX/ESXi 3.5 or later installed.
- Verify that the virtual machines are hosted on ESX/ESXi 3.5 or later and vCenter Server 3.5 or later.
- Verify that the virtual machines are running a Linux or Windows guest OS that ESX/ESXi 3.5 or later and vCenter Server 3.5 or later support.

## Procedure

- 1 Right-click the virtual machine and click **Edit Settings**.
- 2 Click the **VM Options** tab and select **VMware Tools**.
- 3 Select **Check and upgrade VMware Tools before each power on**.
- 4 Click **OK** to save your changes and close the dialog box.

## Results

The next time the virtual machine is powered on, it checks the ESX/ESXi host for a newer version of VMware Tools. If one is available, it is installed and the guest operating system is restarted (if required).

# Manually upgrading VMware Tools in virtual machines

You can upgrade VMware Tools in one or more virtual machines by using the vSphere Web Client.

## Procedure

- 1 Start the vSphere Web Client and log in to the vCenter Server.
- 2 Select the virtual machines.
  - a Select a datacenter, folder, cluster, resource pool, or host.
  - b Click the **VMs** tab.
- 3 Power on the virtual machines to upgrade.
- 4 Right-click your selections.

- 5 Select **Guest OS > Install/Upgrade VMware Tools** and click **OK**.
- 6 Select **Interactive Upgrade** or **Automatic Upgrade** and click **Upgrade**.
- 7 If you chose the interactive upgrade for a virtual machine with a Linux guest operating system, reboot the operating system by running the `reboot` command from a command-line prompt so that you can use the new network modules.

---

**Note** This upgrade procedure is not applicable for operating systems that are installed with OSPs or Open VM Tools

---

## Results

VMware Tools are upgraded.

## Performing an Automatic Upgrade of VMware Tools

When you start an automatic upgrade of VMware Tools, you do not need to perform any operations in the guest operating system that is running on the virtual machine. The automatic upgrade uninstalls the previous version of VMware Tools, installs the latest version that is available for your ESXi host.

Automatic VMware Tools upgrade is supported only for virtual machines with Windows guest operating system.

### Prerequisites

The following requirements are for each virtual machine in the upgrade:

- Power on the virtual machine.
- Verify that the guest operating system is running.

### Procedure

- 1 Select **Automatic Tools Upgrade**.
- 2 (Optional) In the **Advanced Options** text box, enter advanced options for the guest operating system.

Option	Action
<b>Microsoft Windows Guest Operating Systems</b>	Enter <code>/s /v "/qn" /l "<i>Microsoft_Windows_location</i>\filename.log"</code> to perform a silent upgrade of VMware Tools and create a log file in the specified location on the guest operating system.
<b>Linux Guest Operating Systems</b>	<ul style="list-style-type: none"> <li>■ Enter <code>--default</code> to perform the default behavior. Perform a silent upgrade of VMware Tools. Install tools bin, lib and doc files in the default /usr directory.</li> <li>■ Enter <code>--prefix=<i>binary_location, lib_location, doc_location</i></code> to perform a silent upgrade of VMware Tools and install the binary, library, and document files in the specified locations.</li> </ul>

3 Click **OK**.

#### Results

The **VMware Tools** label on the **Summary** tab changes to **OK**.

# Configuring VMware Tools Components

# 4

VMware Tools provides drivers and services that enhance the performance of virtual machines and make several vSphere features easy to use. When VMware Tools is installed, you can configure many of these utilities and change their characteristics.

You can use one of the following methods to configure VMware Tools.

- The command-line configuration utility in the guest operating system. You can modify VMware Tools settings, shrink virtual disks, and connect and disconnect virtual devices.
- Custom scripts.
- Menu commands and dialog boxes.

For information about installing and configuring VMware Tools in other VMware products, see the documentation for your product. For information about VMware Tools in hosts that are provisioned with vSphere Auto Deploy, see VMware Knowledge Base article <http://kb.vmware.com/kb/2004018>.

This chapter includes the following topics:

- [Configuring Network Interface Information](#)
- [Exclude Specific File Systems from Quiesced Snapshots](#)
- [Security Considerations for Configuring VMware Tools](#)
- [Using the VMware Tools Configuration Utility](#)

## Configuring Network Interface Information

You can exclude network interfaces from GuestInfo and set primary and low priority network interfaces. The configuration option is added to the `tools.conf` file.

### Exclude specific interfaces from GuestInfo

To exclude specific interfaces from GuestInfo, set the option `exclude-nics` to a comma separated list of network interfaces.

## Example

```
[guestinfo]
exclude-nics=docker*,veth*
```

The configuration will exclude all interfaces with the names matching the patterns `docker*` and `veth*` from GuestInfo.

## Set primary and low priority interfaces

The options `primary-nics` and `low-priority-nics` accept a list of comma separated patterns for interface names which are considered as primary or low priority network interfaces. This will cause the interface information to be put on top of the list for primary interfaces, and to the bottom for low priority interfaces.

### Example

```
[guestinfo]
primary-nics=eth1
```

The configuration ensures that the IP address for `eth1` will be sorted on top of the list of IP addresses.

### Example

```
[guestinfo]
primary-nics=eth*
```

This configuration ensures that any address in the interfaces matching `eth*` is sorted on top of the list of IP addresses.

### Example

```
[guestinfo]
low-priority-nics=eth*
```

This configuration ensures that any address in the interfaces matching `eth*` is sorted at the bottom of the list of IP addresses.

---

**Note** After the limit of the number of interfaces to be reported is reached, low priority interfaces are the first to be skipped.

---

## Exclude Specific File Systems from Quiesced Snapshots

On the Linux guest operating systems, the configuration setting `excludedFileSystems` allows file systems to be excluded from a quiesced snapshot operation. This setting, if specified, is listed in the section of `vmbackup` of the `tools.conf` file.

The value of `excludedFileSystems` is a comma-separated list of glob-style patterns specifying the file systems to be excluded from quiesced snapshots. The patterns may use `*` (wildcard) to represent any string of characters and `?` (joker) to represent any single character. Note that the characters represented by these patterns, `*` and `?` may include any characters, including `/`

### Procedure

- 1 Open the `tools.conf` file from `/etc/vmware-tools/tools.conf` in your Linux guest operating system.
- 2 Add a `vmbackup` section in the file, if it does not exist.

```
[vmbackup]
```

- 3 In the `vmbackup` section, set `excludedFileSystems` to the preferred list of patterns.

```
excludedFileSystems = <list of patterns>
```

### Example

For example, this setting excludes the file system mounted at `/fs1` from a quiesced snapshot operation.

```
[vmbackup]
excludedFileSystems = /fs1
```

As another example, this setting excludes all the file systems whose mount points start with `/fs` or `/dev` from a quiesced snapshot operation.

```
[vmbackup]
excludedFileSystems = /fs*,/dev/*
```

## Security Considerations for Configuring VMware Tools

Some VMware Tools settings might expose security risks. For example, VMware Tools enables you to connect virtual devices such as serial and parallel ports to virtual machines. A connected device might be a potential channel of attack. To harden a virtual machine and reduce security risks as much as possible, disable the VMware Tools features that might be vulnerable to security threats.

For complete information about securely deploying VMware vSphere in a production environment, including security recommendations for hosts, virtual machines, management components, and a networking infrastructure, see the *vSphere Hardening Guide*. VMware Tools settings relate only to the virtual machine aspect of a deployment.

Virtual machines are encapsulated in a small number of files. Of these, the configuration file (.vmx file) governs the performance of the virtual hardware and other settings. You can use several methods to see and modify the configuration settings:

- Use the vSphere Web Client to edit virtual machine settings. In the vSphere Web Client, editing these configuration parameters is an advanced option in the virtual machine **Edit Settings** dialog box.
- Use the vSphere Host Client to edit virtual machine settings. In the vSphere Host Client, editing these configuration parameters is an advanced option in the virtual machine **Edit Settings** dialog box.
- Use a vSphere API-based tool, such as Power CLI, to view and modify .vmx parameters.

After you edit a setting, the change does not take effect until you restart the virtual machine.

You can eliminate several potential threats by setting parameters appropriately in the corresponding VMware Tools parameters to set in the virtual machine's .vmx file. The defaults for many of these parameters are already set to protect virtual machines from these threats.

## Threats Associated with Unprivileged User Accounts

### Copy and paste

By default, the ability to copy and paste text, graphics, and files is disabled, as is the ability to drag and drop files. When this option is enabled, you can copy and paste rich text, and depending on the VMware product, graphics and files from your clipboard to the guest operating system in a virtual machine. That is, when the console window of a virtual machine gains focus, nonprivileged users and processes running in the virtual machine can access the clipboard on the computer where the console window is running. To avoid risks associated with this feature, retain the following .vmx settings, which disable copying and pasting:

```
isolation.tools.copy.disable = "TRUE"  
isolation.tools.paste.disable = "TRUE"
```

## Threats Associated with Virtual Devices

### Connecting and modifying devices

By default, the ability to connect and disconnect devices is disabled. When this feature is enabled, users and processes without root or administrator privileges can connect devices such as network adapters and CD-ROM drives, and they can modify device settings. That is, a user can connect a disconnected CD-ROM drive and access sensitive information on the media that is in the drive. A user can also disconnect a network adapter to isolate the virtual machine from its network, which is a denial of service. To avoid risks associated with this

feature, retain the following `.vmx` settings, which disable the ability to connect and disconnect devices or to modify device settings:

```
isolation.device.connectable.disable = "TRUE"
isolation.device.edit.disable = "TRUE"
```

## Threats Associated with Virtual Machine Information Flow

### VMX file size

By default the configuration file is limited to a size of 1 MB because uncontrolled size for the file can lead to a denial of service if the datastore runs out of disk space. Informational messages are sometimes sent from the virtual machine to the `.vmx` file. These `setInfo` messages define virtual machine characteristics or identifiers by writing name-value pairs to the file. You might need to increase the size of the file if large amounts of custom information must be stored in the file. The property name is `tools.setInfo.sizeLimit`, and you specify the value in kilobytes. Retain the following `.vmx` setting:

```
tools.setInfo.sizeLimit = "1048576"
```

### Sending performance counters into PerfMon

You can integrate virtual machine performance counters for CPU and memory into PerfMon for Linux and Microsoft Windows guest operating systems. This provides detailed information about the physical host available to the guest operating system. A malicious user could potentially use this information to perform further attacks on the host. By default this feature is disabled. Retain the following `.vmx` setting to prevent host information from being sent to the virtual machine:

```
tools.guestlib.enableHostInfo = "FALSE"
```

This setting blocks some but not all metrics. If you set this property to `FALSE`, the following metrics are blocked:

- GUESTLIB\_HOST\_CPU\_NUM\_CORES
- GUESTLIB\_HOST\_CPU\_USED\_MS
- GUESTLIB\_HOST\_MEM\_SWAPPED\_MB
- GUESTLIB\_HOST\_MEM\_SHARED\_MB
- GUESTLIB\_HOST\_MEM\_USED\_MB
- GUESTLIB\_HOST\_MEM\_PHYS\_MB
- GUESTLIB\_HOST\_MEM\_PHYS\_FREE\_MB
- GUESTLIB\_HOST\_MEM\_KERN\_OVHD\_MB
- GUESTLIB\_HOST\_MEM\_MAPPED\_MB

- GUESTLIB\_HOST\_MEM\_UNMAPPED\_MB

### Features not exposed in vSphere that could cause vulnerabilities

Because VMware virtual machines run in many VMware products in addition to vSphere, some virtual machine parameters do not apply in a vSphere environment. Although these features do not appear in vSphere user interfaces, disabling them reduces the number of vectors through which a guest operating system could access a host. Use the following `.vmx` setting to disable these features:

```
isolation.tools.unity.push.update.disable = "TRUE"
isolation.tools.ghi.launchmenu.change = "TRUE"
isolation.tools.ghi.autologon.disable = "TRUE"
isolation.tools.hgfsServerSet.disable = "TRUE"
isolation.tools.memSchedFakeSampleStats.disable = "TRUE"
isolation.tools.getCreds.disable = "TRUE"
```

## Using the VMware Tools Configuration Utility

The VMware Tools configuration utility is a command-line interface that you can use in the guest operating system to modify VMware Tools settings, shrink virtual disks, and connect and disconnect virtual devices.

The VMware Tools configuration utility provides a command-line interface for functionality that was previously available only in the VMware Tools control panel. The name of this program depends on the guest operating system.

**Table 4-1. VMware Tools Configuration Utilities for Guest Operating Systems**

Guest Operating System	Utility
Windows	VMwareToolboxCmd.exe
Mac OS X	vmware-tools-cli Because the VMware Tools installer does not modify any PATH environment variables on Mac OS X operating systems, you must type <code>./</code> before the command.
Linux, FreeBSD, Solaris	vmware-toolbox-cmd

Use the utility's `help` command to display complete usage information and syntax.

The VMware Tools configuration utility is included in the following VMware products:

- VMware vSphere 4.1 and later
- VMware Workstation 7.0 and later
- VMware Fusion 3.0 and later
- VMware Player 3.0 and later
- VMware ACE 2.6 and later

## Configuring Time Synchronization Between Guest and Host Operating Systems

When you enable periodic time synchronization, VMware Tools sets the time of the guest operating system to be the same as the time of the host.

After time synchronization occurs, 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.

If the clock on the guest operating system falls behind the clock on the host, VMware Tools moves the clock on the guest forward to match the clock on the host. If the clock on the guest operating system is ahead of the clock on the host, VMware Tools causes the clock on the guest to run more slowly until the clocks are synchronized.

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. Use only one form of periodic time synchronization in your guests. If you are using native time synchronization software, disable VMware Tools periodic time synchronization.

Regardless of whether you turn on VMware Tools periodic time synchronization, time synchronization occurs after certain operations:

- When you start the VMware Tools daemon, such as during a reboot or power on operation
- When you resume a virtual machine from a suspend operation
- After you revert to a snapshot
- After you shrink a disk

When the operating system starts or restarts, and when you first turn on periodic time synchronization, if the `time.synchronize.tools.startup.backward` parameter is not enabled in the `.vmx` file, the guest clock is set to forward. For other events, synchronization is forward in time.

To disable time synchronization completely, you must edit the configuration file (`.vmx` file) of the virtual machine and set several synchronization properties to `FALSE`.

### Prerequisites

- Disable other periodic time synchronization mechanisms. For example, some guests might have NTP or Win32Time clock synchronization turned on by default.
- If you plan to script the commands used in this procedure and need to know what the exit codes are, see [Exit Codes for the VMware Tools Configuration Utility](#).

---

**Note** Mac OS X guest operating systems use NTP and do not become out of sync with the host. For Mac OS X guest operating systems, there is no need to turn on VMware Tools time synchronization.

---

**Procedure**

- 1 Open a command prompt or terminal in the guest operating system.
- 2 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	C:\Program Files\VMware\VMware Tools
Linux and Solaris	/usr/sbin
FreeBSD	/usr/local/sbin
Mac OS X	/Library/Application Support/VMware Tools

- 3 Type the command to determine whether time synchronization is enabled.

```
utility-name timesync status
```

For *utility-name* use the guest-specific program name.

Operating System	Program Name
Windows	VMwareToolboxCmd.exe
Linux, Solaris, and FreeBSD	vmware-toolbox-cmd
MAC OS X	vmware-tools-cli

- 4 Type the command to enable or disable periodic time synchronization.

```
utility-name timesync subcommand
```

For *subcommand*, use `enable` or `disable`.

**Results**

The VMware Tools service enables or disables periodic time synchronization, as you specified. Disabling periodic time synchronization does not disable all VMware Tools time synchronization.

**What to do next**

If you need to keep a fictitious time in a virtual machine, such that the clock in the guest operating system is never synchronized with that on the host, disable time synchronization completely for the guest operating system.

## Disabling Time Synchronization

A virtual machine occasionally synchronizes time with the host even if you do not turn on periodic time synchronization. To completely disable time synchronization, you must set some properties in the virtual machine configuration file.

**Prerequisites**

Power off the virtual machine.

**Procedure**

- 1 Open the configuration (.vmx) file of the virtual machine in a text editor.
- 2 Add lines for the time synchronization properties and set the properties to FALSE.

```
tools.syncTime = "FALSE"
time.synchronize.continue = "FALSE"
time.synchronize.restore = "FALSE"
time.synchronize.resume.disk = "FALSE"
time.synchronize.shrink = "FALSE"
time.synchronize.tools.startup = "FALSE"
```

- 3 Save and close the file.

**What to do next**

Power on the virtual machine.

**Use Device Connect or Disconnect**

You can connect and disconnect removable devices such as floppy drives, DVD/CD-ROM drives, ISO images, USB devices, sound adapters, and network adapters.

- Some devices cannot be shared between the host and guest operating systems or between two guest operating systems. For example, only one virtual machine or the host can access the physical CD-ROM drive at any one time.
- The controls for connecting and disconnecting devices might not be available, depending on whether your system administrator has enabled them.

You can run the configuration utility to connect and disconnect virtual devices. For security reasons, this ability is disabled by default. To connect or disconnect devices, you must first change the settings in the configuration file.

**Prerequisites**

If you plan to script commands to connect or disconnect a virtual device, and for the exit codes are, see [Exit Codes for the VMware Tools Configuration Utility](#).

**Procedure**

- 1 Configure the virtual machine to allow devices to connect or disconnect.
  - a Edit the configuration (.vmx) file of the virtual machine with a text editor.
  - b If the following properties are not listed in the file, add them and set them to FALSE.

```
isolation.device.connectable.disable = "FALSE"
isolation.device.edit.disable = "FALSE"
```

- c Save and close the file.
- 2 Open a command prompt or terminal in the guest operating system.

- 3 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	C:\Program Files\VMware\VMware Tools
Linux and Solaris	/usr/sbin
FreeBSD	/usr/local/sbin
Mac OS X	/Library/Application Support/VMware Tools

- 4 Type ***utility-name device list*** to list available devices.

For *utility-name*, use the guest-specific application name.

Operating System	Utility Name
Windows	VMwareToolboxCmd.exe
Linux, Solaris, and FreeBSD	vmware-toolbox-cmd
Mac OS X	vmware-tools-cli

- 5 (Optional) Type the command to determine whether a device is connected.

```
utility-name device status device-name
```

For *device-name*, use one of the names displayed when you used the `list` subcommand.

- 6 Type the command to connect or disconnect the device.

```
utility-name device device-name subcommand
```

Option	Action
<b><i>device-name</i></b>	Use one of the names displayed when you used the <code>list</code> subcommand.
<b><i>subcommand</i></b>	Use <code>enable</code> or <code>disable</code> .

## Results

The device is connected or disconnected, as you specified.

## Using Custom VMware Tools Scripts

You can associate custom scripts with power operations.

When VMware Tools is installed, one or more default scripts run on the guest whenever you change the power state of the virtual machine. You change the power state by using menu commands or by clicking the **Suspend**, **Resume**, **Power On**, and **Power Off** buttons. For example, when you power off a virtual machine, by default the `poweroff-vm-default` script runs.

## Default VMware Tools Scripts

VMware Tools includes one or more default scripts for each power state. The default script behavior depends in part on the guest operating system.

### Microsoft Windows Guest Operating Systems

On most Microsoft Windows guest operating systems, the default script that runs when you suspend a virtual machine releases the IP address of the virtual machine. The default script that runs when you resume a virtual machine renews the IP address of the virtual machine. This behavior affects only virtual machines configured to use DHCP.

On Windows guest operating systems, the default scripts are located in the Program Files \VMware\VMware Tools folder.

---

**Note** You cannot run scripts on NetWare, Windows NT, Me, Windows 98, and Windows 95 guest operating systems.

---

### Linux, Mac OS X, Solaris, and Free BSD Guest Operating Systems

On most Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, the default script that runs when you suspend a virtual machine stops networking for the virtual machine. The default script that runs when you resume a virtual machine starts networking for the virtual machine.

On Linux, Solaris, and FreeBSD guest operating systems, the default scripts are located in the /etc/vmware-tools directory. On Mac OS X operating systems the default scripts are located in the /Library/Application Support/VMware Tools directory.

**Table 4-2. Default VMware Tools Scripts**

Script Name	Description
poweroff-vm-default	Runs when the virtual machine is being powered off or reset. Has no effect on networking for the virtual machine.
poweron-vm-default	Runs when the virtual machine is being powered on rather than resumed. Also runs after virtual machine restarts. Has no effect on networking for the virtual machine.

Table 4-2. Default VMware Tools Scripts (continued)

Script Name	Description
resume-vm-default	<p>Runs when the virtual machine is resumed after it was suspended.</p> <p>On Windows guest operating systems, if the virtual machine is configured to use DHCP, this script renews the IP address of the virtual machine.</p> <p>On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, this script starts networking for the virtual machine.</p>
suspend-vm-default	<p>Runs when the virtual machine is being suspended.</p> <p>On Windows guest operating systems, if the virtual machine is configured to use DHCP, this script releases the IP address of the virtual machine.</p> <p>On Linux, Mac OS X, Solaris, and FreeBSD, this script stops networking for the virtual machine.</p>

For information about how to configure power operations, see the documentation for the VMware product you are using.

## Use Custom VMware Tools Scripts in Windows Guests

On Windows guest operating systems, you can write scripts to automate guest operating system operations when you change the power state of a virtual machine.

For Windows guest operating systems, you can write new scripts or modify default scripts, save them with new names, and configure VMware Tools to use your custom script instead of the default script.

Scripts are run by the VMware Tools service, or daemon (`vmtoolsd`). Because `vmtoolsd` is run as System on Windows, the scripts are run in a separate session from the session of the logged-in user. The VMware Tools daemon does not detect desktop sessions, which means that it cannot display graphical applications. Do not attempt to use custom scripts to display graphical applications.

**Note** You cannot run scripts on NetWare, Windows NT, Me, Windows 98, and Windows 95 guest operating systems.

### Prerequisites

- Familiarize yourself with the default VMware Tools scripts. See [Default VMware Tools Scripts](#).
- If you plan to script commands and need to know what the exit codes are, see [Exit Codes for the VMware Tools Configuration Utility](#).

## Procedure

- 1 Write a new script or modify default scripts and save them as .bat files with new names.

The default scripts for power-on and power-off operations are placeholders only. These scripts are located in the Program Files\VMware\VMware Tools directory.

The scripts for suspend and resume operations contain a line that releases or renews the IP address for the virtual machine. You must add this line first when you write custom scripts for these operations.

Default Script	Required IP Address Line
suspend	@%SYSTEMROOT%\system32\ipconfig /release
resume	@%SYSTEMROOT%\system32\ipconfig /renew

- 2 Open a command prompt in the guest operating system.
- 3 Change directories to the VMware Tools installation directory.  
The default installation directory is C:\Program Files\VMware\VMware Tools.
- 4 Type the command to enable the script.

```
VMwareToolboxCmd.exe script script-name enable
```

- 5 Type the command to use the custom script that you created.

```
VMwareToolboxCmd.exe script script-name set script-path
```

For *script-path*, use the full path to the file, such as C:\Temp\poweron-my-vm.bat.

- 6 Type the command to verify that the custom script that you specified is now being used.

```
VMwareToolboxCmd.exe script script-name current
```

## Results

The VMware Tools service runs the script whenever the specified power operation occurs.

## Using Custom Scripts in Operating Systems Other Than Windows

On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, you can write scripts to automate guest operating system operations when you change the power state of a virtual machine.

For Linux, Mac OS X, Solaris, and FreeBSD guests, you can write scripts and place them in a certain directory, and then VMware Tools runs your scripts in addition to the default scripts. For power-on and resume operations, the default scripts run before the custom scripts. For suspend and power-off, the default scripts run after the custom scripts. This way, VMware Tools stops services only after the custom scripts finish their work, and restores the same services before the custom scripts attempt to use the services.)

Scripts are run by the VMware Tools service, or daemon (`vmtoolsd`). Because `vmtoolsd` is run as root on Linux, Solaris, and FreeBSD, the scripts are run in a separate session from the session of the logged-in user. The VMware Tools daemon does not detect desktop sessions, which means that it cannot display graphical applications. Do not attempt to use custom scripts to display graphical applications.

### Prerequisites

- Familiarize yourself with the default VMware Tools scripts. See [Default VMware Tools Scripts](#).
- On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, if you plan to test, edit, or disable the running of a script, log in as root.
- If you plan to script commands and need to know what the exit codes are, see [Exit Codes for the VMware Tools Configuration Utility](#).

### Procedure

- 1 Log in to the guest operating system as root.
- 2 Write the custom scripts and place them in the correct directory, as instructed by the comments in the default script files for each power operation.

Guest Operating System	Directory
Linux, Solaris, FreeBSD	<code>/etc/vmware-tools</code>
Mac OS X	<code>/Library/Application Support/VMware Tools</code>

Do not make changes to the default scripts.

### Results

The VMware Tools service runs the script whenever the specified power operation occurs.

## Disable a VMware Tools Script

Default scripts for suspending and resuming a virtual machine are written to work together. If you disable the script for one of these actions, you must also disable the script for the other action.

---

**Note** You cannot run scripts on NetWare, Windows NT, Me, Windows 98, and Windows 95 guest operating systems.

---

## Prerequisites

On Linux, Solaris, and FreeBSD guest operating systems, to test, edit, or disable the running of a script, log in as root.

## Procedure

- 1 Open a command prompt or terminal in the guest operating system.
- 2 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	C:\Program Files\VMware\VMware Tools
Linux and Solaris	/usr/sbin
FreeBSD	/usr/local/sbin
Mac OS X	/Library/Application Support/VMware Tools

- 3 Type the command to disable the script.

```
utility-name script script-name disable
```

Option	Action
<i>utility-name</i> On Windows	Use VMwareToolboxCmd.exe.
<i>utility-name</i> On Linux, Solaris, and FreeBSD	Use vmware-toolbox-cmd.
<i>utility-name</i> On MAC OS	Use vmware-tools-cli.
<i>script-name</i>	Use power, resume, suspend, or shutdown.

- 4 (Optional) If you disabled the script for suspending a virtual machine, repeat this procedure for resuming the virtual machine.
- 5 (Optional) If you disabled the script for resuming a virtual machine, also disable the script for suspending the virtual machine.

## Retrieving Status Information About the Virtual Machine

You can view information about host time and CPU speed. For virtual machines hosted in a vSphere environment, you can view additional information about memory and CPU reservations and limits.

### Prerequisites

- Determine the status information to display. See [Subcommands for the stat Command](#).
- If you plan to script commands and need to know what the exit codes are, see [Exit Codes for the VMware Tools Configuration Utility](#).

## Procedure

- 1 Open a command prompt or terminal in the guest operating system.
- 2 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	C:\Program Files\VMware\VMware Tools
Linux and Solaris	/usr/sbin
FreeBSD	/usr/local/sbin
Mac OS X	/Library/Application Support/VMware Tools

- 3 Type the command to display the status information.

```
utility-name stat subcommand
```

Option	Action
<i>utility-name</i> (On Windows)	Use VMwareToolboxCmd.exe.
<i>utility-name</i> (On Linux, Solaris, and FreeBSD)	Use vmware-toolbox-cmd.
<i>utility-name</i> (On Mac OS X)	Use vmware-tools-cli.
<i>subcommand</i>	Use hosttime or, speed, one of the subcommands available for virtual machines hosted in a vSphere environment.

## Subcommands for the stat Command

You can use the `vmware-toolbox-cmd help stat` command to display information such as host time and CPU speed. Additional subcommands are available for virtual machines in a vSphere environment.

Table 4-3. Subcommands for the stat Command

Subcommand Name	Description
hosttime	Displays the date and time on the host.
speed	Displays the CPU speed, in MHz.

## Exit Codes for the VMware Tools Configuration Utility

You can use exit codes to integrate the VMware Tools configuration utility commands with a scripting tool.

Table 4-4. Exit Codes

Code Number	Applicable Command	Description
0	All commands	The command was successful.
1	All commands	A error occurred. For the <code>shrink</code> command, 1 indicates that although shrinking is enabled, the <code>shrink</code> command cannot be carried out.
64	All commands	The command-line argument is not valid.
66	<code>script</code>	The file name does not exist.
69	<code>device</code> and <code>stat</code>	For the <code>device</code> command, 69 indicates that the specified device does not exist. Use the <code>list</code> subcommand to display valid names of devices. For the <code>stat</code> command, 69 indicates that the program could not communicate with the host (EX_UNAVAILABLE).
75	<code>stat</code>	The host does not support the query, perhaps because the host is not an ESX/ESXi host (EX_TEMPFAIL).
77	All commands	Permission error occurred

## guestinfo Variables

You can use the `guestinfo` variables to query information such as version and build information.

For `guestinfo` samples-related PowerCLI scripts, see [PowerCLI-Example-Scripts](#)

Table 4-5. `guestinfo` Variables for VMware Tools

Variable Name	Description
<code>guestinfo.vmtools.description</code>	Reports the version description.
<code>guestinfo.vmtools.versionString</code>	Reports the version string.
<code>guestinfo.vmtools.versionNumber</code>	Reports the version number.
<code>guestinfo.vmtools.buildNumber</code>	Reports the build number.
<code>guestinfo.toolsInstallErrCode</code>	Reports the error code of last VMware Tools installation.  <b>Note</b> VMware Tools installation and upgrade on Windows often requires a reboot the guest operating system for the changes to take effect. If a reboot has not occurred, the <code>guestinfo</code> variable <code>guestinfo.toolsInstallErrCode</code> is set 3010.
<code>guestinfo.driver.[driver name].version</code> For example,	Reports the running version of the driver.
<code>guestinfo.driver.pvscsi.version</code>	1.3.10.0
<code>guestinfo.driver.vmhgfs.version</code>	11.0.34.0
<code>guestinfo.driver.vmxnet3.version</code>	1.8.3.0

# Configuring Customer Experience Improvement Program

# 5

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

This chapter includes the following topics:

- [Categories of Information That VMware Receives](#)
- [Join the Customer Experience Improvement Program in the vSphere Web Client](#)

## Categories of Information That VMware Receives

This product participates in VMware's Customer Experience Improvement Program ("CEIP").

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>. To join or leave the CEIP for this product, see .

## Join the Customer Experience Improvement Program in the vSphere Web Client

You can choose to join your vCenter Server to the Customer Experience Improvement Program (CEIP), or leave the CEIP at any time. To leave and rejoin your host to the CEIP, see the vSphere Single Host Management - VMware Host Client documentation.

### Prerequisites

Verify that you are a member of the Administrators@vsphere.local group.

### Procedure

- 1 Log in to the vCenter Server instance as a member of Administrators@vsphere.local group by using the vSphere Web Client.
- 2 On the vSphere Web Client Home page, under Administration, click **Customer Experience Improvement Program**.
- 3 Click **Join** to enable the CEIP or **Leave** to disable the Program.

# Troubleshooting VMware Tools Installation and Upgrade Issues

# 6

VMware Tools installation and Upgrade issues.

This chapter includes the following topics:

- [Installing or Upgrading to VMware Tools 10.3.0](#)

## Installing or Upgrading to VMware Tools 10.3.0

VMware Tools 10.3.0 depends on and ships Microsoft Visual C++ 2017 Redistributable version 14.0. While preparing the system for VMware Tools 10.3.0 installation, Microsoft Visual C++ 2017 Redistributable is installed on the system as a prerequisite.

### Problem

When installing or upgrading to VMware Tools 10.3.0, different symptoms might be encountered as described:

- Installing or upgrading to VMware Tools 10.3.0 on Windows versions before Windows 10 might fail with an error message if Windows OS level pre-requisites are not met.
- Installing or upgrading to VMware Tools 10.3.0 on Windows versions before Windows 10 may appear stuck with "VMware Product Installation" dialog box carrying "Preparing 'VMware Tools' for installation..." message.
- Installing or upgrading to VMware Tools 10.3.0 on Windows versions before Windows 10 asks for restarting the system without completing the install or upgrade.
- Installing or upgrading to VMware Tools 10.3.0 on Windows versions after Windows 10 asks for restarting the system without completing the install or upgrade.

### Cause

Since VMware Tools 10.3.0 depends on and ships Microsoft Visual C++ 2017 Redistributable version 14.0, it requires the Windows operating system to be at a certain service pack level. Microsoft Visual C++ 2017 Redistributable also includes Windows Update KB2999226.

Installing Windows Update KB2999226 on the system may take a while and may also need a system restart depending on the state of the system as mentioned in the article [Update for Universal C Runtime in Windows](#)

The installation might take a long time as described in the article [Stuck while installing Visual Studio 2015 \(Update for Microsoft Windows KB2999226\)](#)

---

**Note** VMware tries to ensure that all external links provided are correct at the time of inclusion on the website but does not guarantee the accuracy of such information. VMware provides these links merely as a convenience. Third-party URLs might change. If you find a URL in VMware documentation that is out of date, provide feedback on the VMware Docs website. You might be able to locate a third-party document by searching from the third-party home page.

---

NOTE: This issue applies to only Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

Windows operating system might need a restart for different reasons

- For pre-Windows 10 versions it might be either due to KB2999226 or due to the presence of an existing older version of Microsoft Visual C++ 2017 Redistributable DLL on the system that is already loaded by other applications.
- For Windows 10 and later, the latter reason is a common cause of system restart.

#### Solution

- 1 Keep your Windows operating system up-to-date with latest updates.
- 2 Install the Microsoft Visual C++ 2017 Redistributable manually before installing or upgrading VMware Tools to version 10.3.0.
- 3 Alternatively, install Windows Update KB2999226 manually before installing or upgrading VMware Tools, as it reduces some of the issues for Windows versions before Windows 10.
- 4 Update the Windows operating system, Microsoft Visual C++ 2017 Redistributable and other Microsoft applications before installing or upgrading to VMware Tools 10.3.0.
- 5 When the VMware Tools installation or upgrade is invoked with "REBOOT=ReallySuppress" argument, system might require a manual restart for completing Microsoft Visual C++ 2017 Redistributable installation. Reattempt the VMware Tools installation or upgrade after restarting the Windows system. vSphere Client can detect this situation by noticing no change in VMware Tools version and "guestinfo.toolsInstallErrorCode=3010" in the guest variables or in the advanced configuration of the VM.
- 6 When the VMware Tools installation or upgrade is invoked without any arguments, a system restart may occur automatically to complete Microsoft Visual C++ 2017 Redistributable install. After Windows system restarts, reattempt the VMware Tools installation or upgrade.

# Troubleshooting VMware Tools Components

# 7

Usually when you upgrade VMware Tools, the modules are upgraded and new features are added. If some features do not work correctly after an upgrade, you must change or repair modules. On operating systems other than Windows and Linux, you must manually start the VMware User process after an upgrade.

This chapter includes the following topics:

- [Repair or Change Modules in Windows Virtual Machines](#)
- [Starting the VMware User Process Manually If You Do Not Use a Session Manager](#)

## Repair or Change Modules in Windows Virtual Machines

If you have problems with enhanced graphics display or mouse actions or with features that depend on VMware Tools, you might need to repair or modify installed modules.

Occasionally, some new modules are not installed during a VMware Tools upgrade. You can manually install new modules by modifying installed modules.

Use the guest operating system's **Programs and Features** item in the Windows Control Panel to repair or modify VMware Tools.

## 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
<b>Start the VMware User process when you start an X session.</b>	Add <code>vmtoolsd -n vmusr</code> to the appropriate X startup script, such as the <code>.xsession</code> or <code>.xinitrc</code> file.
<b>Start the process after a VMware Tools software upgrade, or if certain features are not working.</b>	Open a terminal window and type the <code>vmtoolsd -n vmusr</code> command.

# Uninstalling VMware Tools



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

In a vSphere and open-vm-tools deployment, if you decide to use packages specific to Linux operating systems to manage VMware Tools, and if you already used vSphere to install VMware Tools, you must uninstall the existing VMware Tools. For more information about Linux OSPs for VMware Tools, see [Operating System Specific Packages for Linux Guest Operating Systems](#).

## 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 <b>Programs &gt; Uninstall a program</b> .
Windows Vista and Windows Server 2008	In the guest operating system, select <b>Programs and Features &gt; Uninstall a program</b> .
Windows XP and earlier	In the guest operating system, select <b>Add/Remove Programs</b> .
Linux	Log in as root and enter <b>vmware-uninstall-tools.pl</b> in a terminal window.
Mac OS X, OS X, or macOS	Use the <b>Uninstall VMware Tools</b> application, found in <code>/Library/Application Support/VMware Tools</code> .

## What to do next

Reinstall VMware Tools.

# FAQs about VMware Tools

## 9

- Can my OS run without VMware Tools?

Although a guest operating system can run without VMware Tools, always run the latest version of VMware Tools in your guest operating systems to access the latest features and updates. You can configure your virtual machine to automatically check for and apply VMware Tools upgrades each time you power on your virtual machines.

- How is VMware Tools released?

ISOs (containing installers): These are packaged with the product and are installed in a number of ways, depending upon the VMware product and the guest operating system installed in the virtual machine. For more information, see the [Installing VMware Tools](#) section. VMware Tools provides a different ISO file for each type of supported guest operating system: Mac OS X, Windows, Linux, NetWare, Solaris, and FreeBSD.

Operating System Specific Packages (OSPs): Downloadable binary packages that are built and provided by VMware for particular versions of Linux distributions. OSPs are typically available for older releases, such as RHEL 6. Most current versions of Linux include Open VM Tools, eliminating the need to separately install OSPs. To download OSPs and to find important information and instructions, see [VMware Tools Operating System Specific Packages \(OSPs\)](#). For a list of supported guest operating systems, see [VMware Compatibility Guide](#).

open-vm-tools (OVT): This is the open source implementation of VMware Tools intended for Linux distribution maintainors and virtual appliance vendors. OVTs are generally included in the current versions of popular Linux distributions, allowing administrators to effortlessly install and update VMware Tools alongside other Linux packages. For more information, see KB [VMware support for Open VM Tools \(2073803\)](#)

- Which operating systems are supported by open-vm-tools?

- Red Hat Enterprise Linux 7.0 and later releases
- SUSE Linux Enterprise 12 and later releases
- Ubuntu 14.04 and later releases
- CentOS 7 and later releases

- FreeBSD 10.3, 10.4 & 11.1
- Debian 7.x and later releases
- Oracle Linux 7 and later
- Fedora 19 and later releases
- openSUSE 11.x and later releases
- Are there VMware Tools VIB available?

Offline bundles with VMware Tools VIB can be installed on vSphere 5.5.x, 6.0.x and 6.5.x versions using vSphere Update Manager. Offline bundles are supported from 10.2.0 and later.