

## **VMware Tools 13.0.0.0**

# Table of Contents

<b>Release Notes.....</b>	<b>4</b>
<b>VMware Tools 13.0.5.0 Release Notes.....</b>	<b>4</b>
<b>VMware Tools 13.0.1.0 Release Notes.....</b>	<b>9</b>
<b>VMware Tools 13.0.0.0 Release Notes.....</b>	<b>15</b>
<b>VMware Tools Administration.....</b>	<b>22</b>
<b>Introduction to VMware Tools.....</b>	<b>22</b>
VMware Tools Services.....	22
VMware Tools Lifecycle Management.....	23
VMware Tools Device Drivers.....	25
VMware User Process.....	27
Open VM Tools.....	27
Operating System Specific Packages for Linux Guest Operating Systems.....	29
<b>Installing VMware Tools.....</b>	<b>29</b>
Disable Access Protection from McAfee Antivirus Virus Scan Console.....	30
Enable Carbon Black Sensor using VMware Tools for Windows.....	31
Enable Salt Minion Using VMware Tools.....	32
Manually Install VMware Tools on Windows.....	36
Manually Install VMware Tools on Windows Arm.....	37
Automatically Install VMware Tools on Multiple Windows Virtual Machines.....	38
Specify VMware Tools Components in Silent Installation.....	38
Manually Install VMware Tools on Linux.....	41
Manually Install VMware Tools on macOS.....	43
Manually Install VMware Tools on Solaris.....	44
Install Open VM Tools.....	45
<b>Upgrading VMware Tools.....</b>	<b>46</b>
Configure Virtual Machines to Automatically Upgrade VMware Tools.....	47
Manually Upgrade VMware Tools in Virtual Machines.....	47
Automatically Upgrade VMware Tools in Virtual Machines.....	48
VMware Tools Installer Logging to Host.....	48
<b>Installing and Automatically Upgrading VMware Tools Component.....</b>	<b>50</b>
<b>Configuring VMware Tools Components.....</b>	<b>50</b>
Using VMware Tools Configuration File.....	51
Configure Network Interface Information.....	51
Exclude Specific File Systems from Quiesced Snapshots.....	52
Security Considerations to Configure VMware Tools.....	53
Using Custom VMware Tools Scripts.....	55

Default VMware Tools Scripts.....	55
Custom VMware Tools Scripts for Windows.....	56
Custom VMware Tools Scripts for Multiple OSs Except Windows.....	57
Disable VMware Tools Script.....	58
Using VMware Tools Configuration Utility.....	58
Enable Periodic Time Synchronization.....	59
Disable Periodic Time Synchronization.....	60
Connect or Disconnect a Virtual Device.....	60
View Virtual Machine Status Information.....	61
Configure appInfo.....	65
Configure ContainerInfo for Linux.....	66
Configure Service Discovery.....	67
Configure VMware Time Provider for Windows.....	68
Using GuestStore.....	68
<b>Uninstalling VMware Tools.....</b>	<b>71</b>
<b>Configuring Customer Experience Improvement Program.....</b>	<b>72</b>
VMware Customer Experience Improvement Program.....	72
Join or Leave Customer Experience Improvement Program in vSphere Client.....	72
<b>VMware Tools Install and Upgrade Issues.....</b>	<b>72</b>
Install or Upgrade to VMware Tools 10.3.0.....	73
<b>Troubleshooting VMware Tools Components.....</b>	<b>74</b>
Repair VMware Tools Components in Windows Virtual Machine.....	74
Start VMware User Process Manually.....	74
<b>VMware Tools FAQs.....</b>	<b>74</b>
<b>Published Windows Drivers.....</b>	<b>76</b>
VMware Tools Drivers Published to Windows Update.....	76
<b>Documentation Legal Notice.....</b>	<b>78</b>

# Release Notes

---

Release notes include product enhancements and notices, bug fixes, and resolved issues.

## VMware Tools 13.0.5.0 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Before You Begin](#)
- [Internationalization](#)
- [Product Support Notice](#)
- [End of Feature Support Notice](#)
- [Compatibility Notes](#)
- [Guest Operating System Customization Support](#)
- [Interoperability Matrix](#)
- [Installation and Upgrades for This Release](#)
- [Windows Guest Drivers Installed by VMware Tools](#)
- [Useful Links](#)
- [Known Issues from Previous Releases](#)

### Introduction

VMware Tools 13.0.5.0 | 29 SEP 2025 | Build No 24915695  
Check for additions and updates to these release notes.

### What's New

- This release resolves CVE-2025-41244 and CVE-2025-41246. For more information on these vulnerabilities and their impact on Broadcom products, see [VMSA-2025-0015](#).
- Updated OpenSSL version to 3.0.17.
- Updated libxml2 version to 2.14.4.
- Updated xmlsec version to 1.3.7.

### Before You Begin

- **VMware Tools 13.0.5.0 supports the following guest operating systems:**
  - windows.iso supports the following 64-bit Windows versions - Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
    - The Microsoft Visual C++ Redistributable package is a prerequisite for installing VMware Tools 13.0.5.0 for Windows and ships with the VMware Tools 13.0.5.0 download package. While preparing a Windows guest for

installation, VMware Tools runs the Microsoft Visual C++ Redistributable Package installer, which checks for a more recent version in the guest. If the guest already has a more recent version, the package does not install.

For a 64-bit Windows guest, the prerequisite versions are Microsoft Visual C++ 2015-2022 Redistributable (x86) version 14.40.33816 and Microsoft Visual C++ 2015-2022 Redistributable (x64) version 14.40.33816.

Refer to Microsoft's update [KB2977003](#) for the latest supported Visual C++ downloads.

- Installing or upgrading to VMware Tools 13.0.5.0 is not supported for Windows versions that do not meet the prerequisite. Customers should use or upgrade to VMware Tools 11.3.5 until they can update their Windows OS to meet the prerequisites for VMware Tools 13.0.5.0.
- Windows OS level prerequisites
  - Windows Server 2025
  - Windows Server 2022
  - Windows 11
  - Windows Server 2019
  - Windows Server 2016
  - Windows 10
  - Windows Server 2012 R2 with Microsoft's update [KB2919355](#)
  - Windows 8.1 with Microsoft's update [KB2919355](#)
  - Windows Server 2012
  - Windows 8
  - Windows Server 2008 R2 Service Pack 1 (SP1) with Microsoft's update [KB4474419](#)
  - Windows 7 Service Pack 1 (SP1) with Microsoft's update [KB4474419](#)
- For windows.iso support for 32-bit Windows versions - Windows 7 SP1 or Windows Server 2008 R2 SP1 and later, refer to [VMware Tools 12.5.4 Release Notes](#).
- windows.iso for Windows Arm supports Windows 11 Arm 64-bit and later.
  - The prerequisite version for a Windows Arm guest is Microsoft Visual C++ 2015-2022 Redistributable (Arm64) version 14.40.33816. Refer to Microsoft's update [KB2977003](#) for the latest supported Visual C++ downloads.
  - For Windows Arm versions that do not meet the prerequisite, installing or upgrading to VMware Tools 13.0.5.0 is not supported.
  - Windows OS level prerequisites
    - Windows 11 Arm
- For details on darwin.iso version, refer to [VMware Tools 12.1.0 Release Notes](#).
- For details on linux.iso, refer to [VMware Tools 10.3.26 Release Notes](#).
- For details on solaris.iso, refer to [VMware Tools 10.3.10 Release Notes](#).
- VMware Tools ISO images are frozen for some end-of-life guest operating systems. Some ISO images are not included with ESX in the tools-light VIB. For more details, see the VMware Tools [Documentation](#) page. All VMware Tools ISO images are available for download from <https://support.broadcom.com>.
- **VMware Tools for Windows:** A 64-bit installer executable (.exe) file is available for download. This file is provided for easier access and installation of VMware Tools in Windows guest operating systems.
- **VMware Tools for Windows Arm:** Installer executable (.exe) files are available for download.

## **Internationalization**

VMware Tools 13.0.5.0 is available in the following languages:

- English
- French
- Japanese
- Spanish

## **Product Support Notice**

- Starting with VMware Tools 12.5.0, VMware Tools ISO image releases only support 64-bit Windows versions.
- VMware Tools 12.4.9 was the last regular release for 32-bit Windows versions. For more information, see the [VMware Tools 12.5.4 Release Notes](#).
- VMware Tools 12.1.1 was the last regular release for Mac OS. Refer to [KB 88698](#) for details.
- The Windows pre-Vista ISO image for VMware Tools is no longer packaged with ESX and is available for download only. For download information, see the [Product Download](#) page.

## **End of Feature Support Notice**

- VMware Tools 12.4.0 and later do not provide new driver versions for virtual machines running Windows 7 and Windows Server 2008 R2 guest operating systems. For more information, see the "Windows Guest Drivers Installed by VMware Tools" section below.
- VMware Tools 13.0.5.0 does not support virtual machines running 32-bit versions of Windows 7 SP1, Windows Server 2008 R2 SP1 and later guest operating systems.
- The Unity mode has been deprecated with VMware Tools 12.4.0 and later.
- VMware Tools ships PVSCSI floppy images and PVSCSI drivers in Tools ISO for OS installation on a PVSCSI disk controller. The PVSCSI floppy images to support OS versions Vista, Server 2008, and Windows 7 are removed from VMware Tools 12.1.0 and later releases.
- The Tar Tools (linux.iso) and OSPs shipped with VMware Tools 10.3.x release will continue to be supported. However, releases after VMware Tools 10.3.5 only include critical and security fixes. No new features are provided in these types of VMware Tools (Tar Tools and OSPs). Using open-vm-tools is recommended for the Linux distributions that provide open-vm-tools packages. For more information about open-vm-tools, see [KB 2073803](#). For information on VMware Tools compatibility with guest operating systems, see [KB 90203](#).

### **Note:**

For more information about the end of technical guidance, see the [Broadcom Support Portal](#).

You must have a profile at the Broadcom Support Portal to access the **Product Lifecycle** page.

## **Compatibility Notes**

- Starting with VMware Tools version 10.2.0, Perl script-based VMware Tools installation for FreeBSD has been discontinued. FreeBSD systems are supported only through the open-vm-tools packages directly available from FreeBSD package repositories. FreeBSD packages for open-vm-tools 10.1.0 and later are available from FreeBSD package repositories.

## **Guest Operating System Customization Support**

The [Guest OS Customization Support Matrix](#) provides details about the guest operating systems that are supported for customization.

## **Interoperability Matrix**

- The [Broadcom Product Interoperability Matrix](#) provides details about the compatibility of current and earlier versions of VMware Products.

## **Installation and Upgrades for This Release**

VMware Tools can be downloaded from the [Product Download](#) page.

The steps to install VMware Tools vary depending on your VMware product and the guest operating system you have installed. For general steps to install VMware Tools in most VMware products, see [General VMware Tools installation instructions \(1014294\)](#).

To set up productLocker to point to the shared datastore, see [KB 2004018](#).

This release provides packages to upgrade VMware Tools 11.2.5 or later deployments using [GuestStore](#).

Install or upgrade to VMware Tools 13.0.5.0 and later that includes `vmmouse`, `vmhgfs`, or `pvscsi` drivers when the VM's system disk resides on a paravirtual SCSI controller will require a system restart. Depending on the system state, other guest drivers might also require a system restart.

For specific instructions to install, upgrade, and configure VMware Tools, see the [VMware Tools Documentation](#).

## Windows Guest Drivers Installed by VMware Tools

VMware Tools 13.0.5.0 provides the following driver versions for Windows 8 (64-bit), Windows Server 2012 and later:

Drivers	VMware Tools 13.0.5.0
<b>Hardware Drivers</b>	
efifwfromhost.bin	1.0.0.2
pvscsi.sys	1.3.29.0
vmci.sys	9.8.30.0
vmmouse.sys	12.5.15.0
vmusbmouse.sys	12.5.15.0
vmxnet3.sys	1.9.20.0
vm3dmp.sys	9.17.09.0004
<b>Software Drivers</b>	
vmhgfs.sys	11.0.49.0
vmmemctl.sys	7.5.10.0
vmrawdsk.sys	1.1.9.0
vnetWFP.sys	13.0.0.0
vsepfilt.sys	13.0.0.0
vsock.sys	9.8.24.0
<b>Security DLL</b>	
vmwsu.dll	2.5.2.0

VMware Tools 13.0.5.0 provides the following driver versions for Windows Arm:

Hardware Drivers	VMware Tools 13.0.5.0
vmusbmouse.sys	12.5.15.0
vmxnet3.sys	1.9.20.0
vm3dmp.sys	9.17.09.0004

## Useful Links

- For more information about previous versions of VMware Tools, see [KB 86165](#).
- For more information about VMware Tools compatibility with guest operating systems, see [KB 90203](#).
- For more information about the guest operating systems support levels, see [KB 2015161](#).

## Known Issues from Previous Releases

## **VMware Tools Issues**

### **The Unity mode does not work with VMware Tools 12.4.0 and later**

For VMs running on VMware Workstation 17.6 and earlier and VMware Fusion 13.6 and earlier, the Unity mode stops working if the VMs run VMware Tools 12.4.0 and later versions.

The Unity mode has been deprecated, starting with VMware Workstation 17.6 and VMware Fusion 13.6. These product versions include VMware Tools 12.4.5 or later. For more information about the features supported by VMware Workstation and VMware Fusion, refer to product release notes.

**Workaround:** To use the Unity mode on earlier VMware Workstation and VMware Fusion versions, use VMware Tools 12.3.5 and earlier.

### **Provide tools.conf settings to deactivate one-time and periodic time synchronization**

The new tools.conf settings `disable-all` and `disable-periodic` allow the guest OS administrator to deactivate one-time and periodic time synchronization without rebooting the VM or restarting the guest OS.

### **Memory leak when running the Ortec application**

When you run the Ortec application, you might experience an increase in memory usage and see a memory error.

**Workaround:** To avoid this issue, set the system environment variable to zero - `SVGA_ALLOW_LLVMPIPE=0`

### **Shared Folders mount is unavailable on Linux VM**

If the **Shared Folders** feature is enabled on a Linux VM while it is powered off, the shared folders mount is not available on restart.

Note: This issue applies to VMware Tools running on Workstation and Fusion.

If the VM is powered on, disable and enable the **Shared Folders** feature from the interface. To resolve the issue permanently, edit `/etc/fstab` and add an entry to mount the Shared Folders automatically on boot.

For example, add the line:

```
vmhgfs-fuse /mnt/hgfs fuse defaults,allow_other 0 0
```

For more information on how to configure VMware Tools Shared Folders, see [KB 60262](#).

### **VMware Tools upgrade fails on Windows 7 SP1 and Windows Server 2008 R2 SP1 without SHA-2 code signing support**

Microsoft has changed Windows driver signing to use the SHA-2 algorithm exclusively starting December 3, 2019. Legacy Windows systems without SHA-2 code signing support fail driver signature verification.

Refer to [KB 78708](#).

### **Installation of Windows Vista, Server 2008, or Windows 7 fails in a virtual machine**

Installing a Windows OS Vista, Server 2008, or Windows 7 in a virtual machine with a boot disk on a PVSCSI controller, fails to install the required PVSCSI driver.

Download the VMware Tools package version 11.1.5 from the [Broadcom Support Portal](#), extract the contents, and use the VMware Tools windows.iso or the floppies for Windows OS Vista or Server 2008.

#### **Note:**

Users managing ESX hosts or having a requirement to perform multiple installations of the same Windows OS version on a PVSCSI controller, can see the steps outlined in [KB 84200](#).

### **VMware Tools upgrade failed with error code 1072 (The specified service has been marked for deletion.)**

When upgrading VMware Tools to a new version, if the previous version's VMware Tools service is not deleted completely, this incomplete service removal causes installing the new VMware Tools version service to fail and leads to a fatal error for the upgrade.

When detecting an incomplete service removal to prevent VMware Tools upgrade from failing catastrophically every time, the new service creation will pause and retry to see if the condition clears. The VMware Tools installer will pause for up to 2 1/2 minutes. After this, a fatal error will occur. If the condition clears, the upgrade creates the new service and continues.

For more information, see [KB 84269](#).

**Workaround:** Reboot the Windows system and restart VMware Tools install.

**After upgrading to a new version of VMware Tools with an installer parameter to remove the NetworkIntrospection feature, the old version of the vnetflt or vnetWFP driver service continues to run**

After the upgrade, the NetworkIntrospection feature is not present in the system's VMware Tools MSI database, but the feature's vnetflt or vnetWFP driver service still exists.

Refer to [KB 78016](#).

Note: This issue applies to VMware Tools upgrades from versions older than 11.1.0 only.

**Installing or upgrading versions earlier than VMware Tools 10.3.0 to VMware Tools 11.1.x might take longer and Windows OS might need a restart**

The installation process might appear to be in progress and display a message similar to the following: "Preparing 'VMware Tools' for installation..."

During this process, the user might be prompted to restart the operating system.

For more information, see [KB 55798](#).

**VMware Tools Issues on Windows Arm**

**Windows Arm VMs encounter either BSOD with DPC\_WATCHDOG\_VIOLATION or hang**

Typically, with 3D games or resizing a remote desktop on VMware Tools 12.3.0, Windows Arm VMs encounter either BSOD with DPC\_WATCHDOG\_VIOLATION or hang.

You can disable 3D acceleration in VM settings. For more information, see [KB 95283](#).

## VMware Tools 13.0.1.0 Release Notes

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Before You Begin](#)
- [Internationalization](#)
- [Product Support Notice](#)
- [End of Feature Support Notice](#)
- [Compatibility Notes](#)
- [Guest Operating System Customization Support](#)
- [Interoperability Matrix](#)
- [Installation and Upgrades for This Release](#)
- [Windows Guest Drivers Installed by VMware Tools](#)
- [Useful Links](#)
- [Known Issues from Previous Releases](#)

## Introduction

VMware Tools 13.0.1.0 | 15 JUL 2025 | Build No 24843032  
Check for additions and updates to these release notes.

## What's New

- This release resolves CVE-2025-41239. For more information on this vulnerability and its impact on Broadcom products, see [VMSA-2025-0013](#).

## Before You Begin

- VMware Tools 13.0.1.0 supports the following guest operating systems:**
  - windows.iso supports the following 64-bit Windows versions - Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
    - The Microsoft Visual C++ Redistributable package is a prerequisite for installing VMware Tools 13.0.1.0 for Windows and ships with the VMware Tools 13.0.1.0 download package. While preparing a Windows guest for installation, VMware Tools runs the Microsoft Visual C++ Redistributable Package installer, which checks for a more recent version in the guest. If the guest already has a more recent version, the package does not install. For a 64-bit Windows guest, the prerequisite versions are Microsoft Visual C++ 2015-2022 Redistributable (x86) version 14.40.33816 and Microsoft Visual C++ 2015-2022 Redistributable (x64) version 14.40.33816. Refer to Microsoft's update [KB2977003](#) for the latest supported Visual C++ downloads.
  - Installing or upgrading to VMware Tools 13.0.1.0 is not supported for Windows versions that do not meet the prerequisite. Customers should use or upgrade to VMware Tools 11.3.5 until they can update their Windows OS to meet the prerequisites for VMware Tools 13.0.1.0.
  - Windows OS level prerequisites
    - Windows Server 2025
    - Windows Server 2022
    - Windows 11
    - Windows Server 2019
    - Windows Server 2016
    - Windows 10
    - Windows Server 2012 R2 with Microsoft's update [KB2919355](#)
    - Windows 8.1 with Microsoft's update [KB2919355](#)
    - Windows Server 2012
    - Windows 8
    - Windows Server 2008 R2 Service Pack 1 (SP1) with Microsoft's update [KB4474419](#)
    - Windows 7 Service Pack 1 (SP1) with Microsoft's update [KB4474419](#)
  - For windows.iso support for 32-bit Windows versions - Windows 7 SP1 or Windows Server 2008 R2 SP1 and later, refer to [VMware Tools 12.5.3 Release Notes](#).
  - windows.iso for Windows Arm supports Windows 11 Arm 64-bit and later.
    - The prerequisite version for a Windows Arm guest is Microsoft Visual C++ 2015-2022 Redistributable (Arm64) version 14.40.33816. Refer to Microsoft's update [KB2977003](#) for the latest supported Visual C++ downloads.
    - For Windows Arm versions that do not meet the prerequisite, installing or upgrading to VMware Tools 13.0.1.0 is not supported.
    - Windows OS level prerequisites

- Windows 11 Arm
  - For details on darwin.iso version, refer to [VMware Tools 12.1.0 Release Notes](#).
  - For details on linux.iso, refer to [VMware Tools 10.3.26 Release Notes](#).
  - For details on solaris.iso, refer to [VMware Tools 10.3.10 Release Notes](#).
- VMware Tools ISO images are frozen for some end-of-life guest operating systems. Some ISO images are not included with ESX in the tools-light VIB. For more details, see the VMware Tools [Documentation](#) page. All VMware Tools ISO images are available for download from <https://support.broadcom.com>.
- **VMware Tools for Windows:** A 64-bit installer executable (.exe) file is available for download. This file is provided for easier access and installation of VMware Tools in Windows guest operating systems.
- **VMware Tools for Windows Arm:** Installer executable (.exe) files are available for download.

### **Internationalization**

VMware Tools 13.0.1.0 is available in the following languages:

- English
- French
- Japanese
- Spanish

### **Product Support Notice**

- Starting with VMware Tools 12.5.0, VMware Tools ISO image releases only support 64-bit Windows versions.
- VMware Tools 12.4.8 was the last regular release for 32-bit Windows versions. For more information, see the [VMware Tools 12.5.3.0 Release Notes](#).
- VMware Tools 12.1.1 was the last regular release for Mac OS. Refer to [KB 88698](#) for details.
- The Windows pre-Vista ISO image for VMware Tools is no longer packaged with ESX and is available for download only. For download information, see the [Product Download](#) page.

### **End of Feature Support Notice**

- VMware Tools 12.4.0 and later do not provide new driver versions for virtual machines running Windows 7 and Windows Server 2008 R2 guest operating systems. For more information, see the "Windows Guest Drivers Installed by VMware Tools" section below.
- VMware Tools 13.0.1.0 does not support virtual machines running 32-bit versions of Windows 7 SP1, Windows Server 2008 R2 SP1 and later guest operating systems.
- The Unity mode has been deprecated with VMware Tools 12.4.0 and later.
- VMware Tools ships PVSCSI floppy images and PVSCSI drivers in Tools ISO for OS installation on a PVSCSI disk controller. The PVSCSI floppy images to support OS versions Vista, Server 2008, and Windows 7 are removed from VMware Tools 12.1.0 and later releases.
- The Tar Tools (linux.iso) and OSPs shipped with VMware Tools 10.3.x release will continue to be supported. However, releases after VMware Tools 10.3.5 only include critical and security fixes. No new features are provided in these types of VMware Tools (Tar Tools and OSPs). Using open-vm-tools is recommended for the Linux distributions that provide open-vm-tools packages. For more information about open-vm-tools, see [KB 2073803](#). For information on VMware Tools compatibility with guest operating systems, see [KB 90203](#).

### **Note:**

For more information about the end of technical guidance, see <https://support.broadcom.com>.

You must have a profile at the Broadcom Support Portal to access the **Product Lifecycle** page.

## Compatibility Notes

- VMware Tools 13.0.1.0 provides the same compatibility as VMware Tools 13.0.0.0. For VMware Tools 13.0.1.0 compatibility details, refer to the VMware Tools 13.0.0.0 compatibility in the [Broadcom Product Interoperability Matrix](#).
- Starting with VMware Tools version 10.2.0, Perl script-based VMware Tools installation for FreeBSD has been discontinued. FreeBSD systems are supported only through the open-vm-tools packages directly available from FreeBSD package repositories. FreeBSD packages for open-vm-tools 10.1.0 and later are available from FreeBSD package repositories.

## Guest Operating System Customization Support

The [Guest OS Customization Support Matrix](#) provides details about the guest operating systems that are supported for customization.

## Interoperability Matrix

- The [Broadcom Product Interoperability Matrix](#) provides details about the compatibility of current and earlier versions of VMware Products.
- The VMware Tools 13.0.1.0 express patch release follows the interoperability of the VMware Tools 13.0.0.0 major release.

## Installation and Upgrades for This Release

VMware Tools can be downloaded from the [Product Download](#) page.

The steps to install VMware Tools vary depending on your VMware product and the guest operating system you have installed. For general steps to install VMware Tools in most VMware products, see [General VMware Tools installation instructions \(1014294\)](#).

To set up productLocker to point to the shared datastore, see [KB 2004018](#).

This release provides packages to upgrade VMware Tools 11.2.5 or later deployments using [GuestStore](#).

Install or upgrade to VMware Tools 13.0.1.0 and later that includes `vmmouse`, `vmhgfs`, or `pvscsi` drivers when the VM's system disk resides on a paravirtual SCSI controller will require a system restart. Depending on the system state, other guest drivers might also require a system restart.

For specific instructions to install, upgrade, and configure VMware Tools, see the [VMware Tools Documentation](#).

## Windows Guest Drivers Installed by VMware Tools

VMware Tools 13.0.1.0 provides the following driver versions for Windows 8 (64-bit), Windows Server 2012 and later:

Drivers	VMware Tools 13.0.1.0
<b>Hardware Drivers</b>	
efifwfromhost.bin	1.0.0.2
pvscsi.sys	1.3.29.0
vmci.sys	9.8.30.0
vmmouse.sys	12.5.15.0
vmusbmouse.sys	12.5.15.0
vmxnet3.sys	1.9.20.0
vm3dmp.sys	9.17.09.0004
<b>Software Drivers</b>	

vmhgfs.sys	11.0.49.0
vmmemctl.sys	7.5.10.0
vmrawdsk.sys	1.1.9.0
vnetWFP.sys	13.0.0.0
vsepflt.sys	13.0.0.0
vsock.sys	9.8.24.0
<b>Security DLL</b>	
vmwsu.dll	2.5.2.0

VMware Tools 13.0.1.0 provides the following driver versions for Windows Arm:

Hardware Drivers	VMware Tools 13.0.1.0
vmusbmouse.sys	12.5.15.0
vmxnet3.sys	1.9.20.0
vm3dmp.sys	9.17.09.0004

### Useful Links

- For more information about previous versions of VMware Tools, see [KB 86165](#).
- For more information about VMware Tools compatibility with guest operating systems, see [KB 90203](#).
- For more information about the guest operating systems support levels, see [KB 2015161](#).

### Known Issues from Previous Releases

#### VMware Tools Issues

##### The Unity mode does not work with VMware Tools 12.4.0 and later

For VMs running on VMware Workstation 17.6 and earlier and VMware Fusion 13.6 and earlier, the Unity mode stops working if the VMs run VMware Tools 12.4.0 and later versions.

The Unity mode has been deprecated, starting with VMware Workstation 17.6 and VMware Fusion 13.6. These product versions include VMware Tools 12.4.5 or later. For more information about the features supported by VMware Workstation and VMware Fusion, refer to product release notes.

**Workaround:** To use the Unity mode on earlier VMware Workstation and VMware Fusion versions, use VMware Tools 12.3.5 and earlier.

##### Provide tools.conf settings to deactivate one-time and periodic time synchronization

The new tools.conf settings `disable-all` and `disable-periodic` allow the guest OS administrator to deactivate one-time and periodic time synchronization without rebooting the VM or restarting the guest OS.

##### Memory leak when running the Ortec application

When you run the Ortec application, you might experience an increase in memory usage and see a memory error.

**Workaround:** To avoid this issue, set the system environment variable to zero - `SVGA_ALLOW_LLVMPIPE=0`

##### Shared Folders mount is unavailable on Linux VM

If the **Shared Folders** feature is enabled on a Linux VM while it is powered off, the shared folders mount is not available on restart.

Note: This issue applies to VMware Tools running on Workstation and Fusion.

If the VM is powered on, disable and enable the **Shared Folders** feature from the interface. To resolve the issue permanently, edit **/etc/fstab** and add an entry to mount the Shared Folders automatically on boot.

For example, add the line:

```
vmhgfs-fuse    /mnt/hgfs    fuse    defaults,allow_other    0    0
```

For more information on how to configure VMware Tools Shared Folders, see [KB 60262](#).

### **VMware Tools upgrade fails on Windows 7 SP1 and Windows Server 2008 R2 SP1 without SHA-2 code signing support**

Microsoft has changed Windows driver signing to use the SHA-2 algorithm exclusively starting December 3, 2019. Legacy Windows systems without SHA-2 code signing support fail driver signature verification.

Refer to [KB 78708](#).

### **Installation of Windows Vista, Server 2008, or Windows 7 fails in a virtual machine**

Installing a Windows OS Vista, Server 2008, or Windows 7 in a virtual machine with a boot disk on a PVSCSI controller, fails to install the required PVSCSI driver.

Download the VMware Tools package version 11.1.5 from <https://support.broadcom.com/>, extract the contents, and use the VMware Tools windows.iso or the floppies for Windows OS Vista or Server 2008.

#### **Note:**

Users managing ESX hosts or having a requirement to perform multiple installations of the same Windows OS version on a PVSCSI controller, can see the steps outlined in [KB 84200](#).

### **VMware Tools upgrade failed with error code 1072 (The specified service has been marked for deletion.)**

When upgrading VMware Tools to a new version, if the previous version's VMware Tools service is not deleted completely, this incomplete service removal causes installing the new VMware Tools version service to fail and leads to a fatal error for the upgrade.

When detecting an incomplete service removal to prevent VMware Tools upgrade from failing catastrophically every time, the new service creation will pause and retry to see if the condition clears. The VMware Tools installer will pause for up to 2 1/2 minutes. After this, a fatal error will occur. If the condition clears, the upgrade creates the new service and continues.

For more information, see [KB 84269](#).

**Workaround:** Reboot the Windows system and restart VMware Tools install.

### **After upgrading to a new version of VMware Tools with an installer parameter to remove the NetworkIntrospection feature, the old version of the vnetflt or vnetWFP driver service continues to run**

After the upgrade, the NetworkIntrospection feature is not present in the system's VMware Tools MSI database, but the feature's vnetflt or vnetWFP driver service still exists.

Refer to [KB 78016](#).

Note: This issue applies to VMware Tools upgrades from versions older than 11.1.0 only.

### **Installing or upgrading versions earlier than VMware Tools 10.3.0 to VMware Tools 11.1.x might take longer and Windows OS might need a restart**

The installation process might appear to be in progress and display a message similar to the following: "Preparing 'VMware Tools' for installation..."

During this process, the user might be prompted to restart the operating system.

For more information, see [KB 55798](#).

## **VMware Tools Issues on Windows Arm**

### **Windows Arm VMs encounter either BSOD with DPC\_WATCHDOG\_VIOLATION or hang**

Typically, with 3D games or resizing a remote desktop on VMware Tools 12.3.0, Windows Arm VMs encounter either BSOD with DPC\_WATCHDOG\_VIOLATION or hang.

You can disable 3D acceleration in VM settings. For more information, see [KB 95283](#).

## **VMware Tools 13.0.0.0 Release Notes**

This document contains the following sections

- [Introduction](#)
- [What's New](#)
- [Before You Begin](#)
- [Internationalization](#)
- [Product Support Notice](#)
- [End of Feature Support Notice](#)
- [Compatibility Notes](#)
- [Guest Operating System Customization Support](#)
- [Interoperability Matrix](#)
- [Installation and Upgrades for This Release](#)
- [Windows Guest Drivers Installed by VMware Tools](#)
- [Useful Links](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Known Issues from Previous Releases](#)

### **Introduction**

VMware Tools 13.0.0.0   17 JUN 2025   Build No 24696409 Check for additions and updates to these release notes.
--

### **What's New**

- Updated OpenSSL to version 3.0.15.
- Updated 7zip version to 24.09.
- Updated uriparser to version 0.9.7.

### **Before You Begin**

- **VMware Tools 13.0.0.0 supports the following guest operating systems:**
  - windows.iso supports the following 64-bit Windows versions - Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
    - The Microsoft Visual C++ Redistributable package is a prerequisite for installing VMware Tools 13.0.0.0 for Windows and ships with the VMware Tools 13.0.0.0 download package. While preparing a Windows guest for

installation, VMware Tools runs the Microsoft Visual C++ Redistributable Package installer, which checks for a more recent version in the guest. If the guest already has a more recent version, the package does not install.

For a 64-bit Windows guest, the prerequisite versions are Microsoft Visual C++ 2015-2022 Redistributable (x86) version 14.40.33816 and Microsoft Visual C++ 2015-2022 Redistributable (x64) version 14.40.33816.

Refer to Microsoft's update [KB2977003](#) for the latest supported Visual C++ downloads.

- Installing or upgrading to VMware Tools 13.0.0.0 is not supported for Windows versions that do not meet the prerequisite. Customers should use or upgrade to VMware Tools 11.3.5 until they can update their Windows OS to meet the prerequisites for VMware Tools 13.0.0.0.
- Windows OS level prerequisites
  - Windows Server 2025
  - Windows Server 2022
  - Windows 11
  - Windows Server 2019
  - Windows Server 2016
  - Windows 10
  - Windows Server 2012 R2 with Microsoft's update [KB2919355](#)
  - Windows 8.1 with Microsoft's update [KB2919355](#)
  - Windows Server 2012
  - Windows 8
  - Windows Server 2008 R2 Service Pack 1 (SP1) with Microsoft's update [KB4474419](#)
  - Windows 7 Service Pack 1 (SP1) with Microsoft's update [KB4474419](#)
- For windows.iso support for 32-bit Windows versions - Windows 7 SP1 or Windows Server 2008 R2 SP1 and later, refer to [VMware Tools 12.5.2 Release Notes](#).
- windows.iso for Windows Arm supports Windows 11 Arm 64-bit and later.
  - The prerequisite version for a Windows Arm guest is Microsoft Visual C++ 2015-2022 Redistributable (Arm64) version 14.40.33816. Refer to Microsoft's update [KB2977003](#) for the latest supported Visual C++ downloads.
  - For Windows Arm versions that do not meet the prerequisite, installing or upgrading to VMware Tools 13.0.0.0 is not supported.
  - Windows OS level prerequisites
    - Windows 11 Arm
- For details on darwin.iso version, refer to [VMware Tools 12.1.0 Release Notes](#).
- For details on linux.iso, refer to [VMware Tools 10.3.26 Release Notes](#).
- For details on solaris.iso, refer to [VMware Tools 10.3.10 Release Notes](#).
- VMware Tools ISO images are frozen for some end-of-life guest operating systems. Some ISO images are not included with ESX in the tools-light VIB. For more details, see the VMware Tools [Documentation](#) page. All VMware Tools ISO images are available for download from <https://support.broadcom.com>.
- **VMware Tools for Windows:** A 64-bit installer executable (.exe) file is available for download. This file is provided for easier access and installation of VMware Tools in Windows guest operating systems.
- **VMware Tools for Windows Arm:** Installer executable (.exe) files are available for download.

## **Internationalization**

VMware Tools 13.0.0.0 is available in the following languages:

- English
- French
- Japanese
- Spanish

## **Product Support Notice**

- The following languages will no longer be supported:
  - Italian, German, Brazilian Portuguese, Traditional Chinese, Korean, Simplified Chinese
- Impact:
  - Users who have been using the deprecated languages will no longer receive updates or support in these languages.
  - All user interfaces, help documentation, and customer support will be available only in English or in the three supported languages mentioned above.
- Starting with VMware Tools 12.5.0, VMware Tools ISO image releases only support 64-bit Windows versions.
- VMware Tools 12.4.7 was the last regular release for 32-bit Windows versions. For more information, see the [VMware Tools 12.5.2 Release Notes](#).
- VMware Tools 12.1.1 was the last regular release for Mac OS. Refer to [KB 88698](#) for details.
- The Windows pre-Vista ISO image for VMware Tools is no longer packaged with ESX and is available for download only. For download information, see the [Product Download](#) page.

## **End of Feature Support Notice**

- VMware Tools 12.4.0 and later do not provide new driver versions for virtual machines running Windows 7 and Windows Server 2008 R2 guest operating systems. For more information, see the "Windows Guest Drivers Installed by VMware Tools" section below.
- VMware Tools 13.0.0.0 does not support virtual machines running 32-bit versions of Windows 7 SP1, Windows Server 2008 R2 SP1 and later guest operating systems.
- The Unity mode has been deprecated with VMware Tools 12.4.0 and later.
- VMware Tools ships PVSCSI floppy images and PVSCSI drivers in Tools ISO for OS installation on a PVSCSI disk controller. The PVSCSI floppy images to support OS versions Vista, Server 2008, and Windows 7 are removed from VMware Tools 12.1.0 and later releases.
- The Tar Tools (linux.iso) and OSPs shipped with VMware Tools 10.3.x release will continue to be supported. However, releases after VMware Tools 10.3.5 only include critical and security fixes. No new features are provided in these types of VMware Tools (Tar Tools and OSPs). Using open-vm-tools is recommended for the Linux distributions that provide open-vm-tools packages. For more information about open-vm-tools, see [KB 2073803](#). For information on VMware Tools compatibility with guest operating systems, see [KB 90203](#).

### **Note:**

For more information about the end of technical guidance, see <https://support.broadcom.com>.

You must have a profile at the Broadcom Support Portal to access the **Product Lifecycle** page.

## **Compatibility Notes**

- Starting with VMware Tools version 10.2.0, Perl script-based VMware Tools installation for FreeBSD has been discontinued. FreeBSD systems are supported only through the open-vm-tools packages directly available from FreeBSD package repositories. FreeBSD packages for open-vm-tools 10.1.0 and later are available from FreeBSD package repositories.

## **Guest Operating System Customization Support**

The [Guest OS Customization Support Matrix](#) provides details about the guest operating systems that are supported for customization.

## Interoperability Matrix

The [Broadcom Product Interoperability Matrix](#) provides details about the compatibility of current and earlier versions of VMware Products.

## Installation and Upgrades for This Release

VMware Tools can be downloaded from the [Product Download](#) page.

The steps to install VMware Tools vary depending on your VMware product and the guest operating system you have installed. For general steps to install VMware Tools in most VMware products, see [General VMware Tools installation instructions \(1014294\)](#).

To set up productLocker to point to the shared datastore, see [KB 2004018](#).

This release provides packages to upgrade VMware Tools 11.2.5 or later deployments using [GuestStore](#).

Install or upgrade to VMware Tools 13.0.0.0 and later that includes `vmmouse`, `vmhgfs`, or `pvscsi` drivers when the VM's system disk resides on a paravirtual SCSI controller will require a system restart. Depending on the system state, other guest drivers might also require a system restart.

For specific instructions to install, upgrade, and configure VMware Tools, see the [VMware Tools Documentation](#).

## Windows Guest Drivers Installed by VMware Tools

VMware Tools 13.0.0.0 provides the following driver versions for Windows 8 (64-bit), Windows Server 2012 and later:

Drivers	VMware Tools 13.0.0.0
<b>Hardware Drivers</b>	
efifwfromhost.bin	1.0.0.2
pvscsi.sys	1.3.29.0
vmci.sys	9.8.30.0
vmmouse.sys	12.5.15.0
vmusbmouse.sys	12.5.15.0
vmxnet3.sys	1.9.20.0
vm3dmp.sys	9.17.09.0004
<b>Software Drivers</b>	
vmhgfs.sys	11.0.49.0
vmmemctl.sys	7.5.10.0
vmrawdsk.sys	1.1.9.0
vnetWFP.sys	13.0.0.0
vsepflt.sys	13.0.0.0
vsock.sys	9.8.23.0
<b>Security DLL</b>	
vmwsu.dll	2.5.2.0

VMware Tools 13.0.0.0 provides the following driver versions for Windows Arm:

Hardware Drivers	VMware Tools 13.0.0.0
vmusbmouse.sys	12.5.15.0
vmxnet3.sys	1.9.20.0

vm3dmp.sys	9.17.09.0004
------------	--------------

## Useful Links

- For more information about previous versions of VMware Tools, see [KB 86165](#).
- For more information about VMware Tools compatibility with guest operating systems, see [KB 90203](#).
- For more information about the guest operating systems support levels, see [KB 2015161](#).

## Resolved Issues

**After October 25, 2024, with VMware Tools or open-vm-tools earlier than 13.0.0, the salt-minion component is not installed or fails to install in a guest operating system through the VMware Component Manager**

When you configure the salt-minion component in the `present` state, its last status is set to 102 (not installed) or 103 (installation failed), never reaching the installed state 100 .

- The VM advanced setting with the key "`guestinfo./vmware.components.salt_minion.desiredstate`" has a value `present` .
- The VM advanced setting with the key "`guestinfo.vmware.components.salt_minion.laststatus`" has a value 102 or 103 .

The salt-minion component installs a log file as traces indicating failure to access the online salt repository on <https://repo.saltproject.io>.

## On Linux

The "`vmware-svtminion.sh-install-*.log`" file for the failed install shows a trace similar to:

```
<date+time> INFO: /usr/lib64/open-vm-tools/componentMgr/saltMinion/svtminion.sh:_curl_download attempting
download of file 'repo.json' <date+time> WARNING: /usr/lib64/open-vm-tools/componentMgr/saltMinion/svtmin-
ion.sh:_curl_download failed to download file 'repo.json' from 'https://repo.saltproject.io/salt/py3/onedir/
repo.json' on '0' attempt, retcode '6'
<date+time> WARNING: /usr/lib64/open-vm-tools/componentMgr/saltMinion/svtminion.sh:_curl_download failed to
download file 'repo.json' from 'https://repo.saltproject.io/salt/py3/onedir/repo.json' on '1' attempt, ret-
code '6'
<date+time> WARNING: /usr/lib64/open-vm-tools/componentMgr/saltMinion/svtminion.sh:_curl_download failed to
download file 'repo.json' from 'https://repo.saltproject.io/salt/py3/onedir/repo.json' on '2' attempt, ret-
code '6'
<date+time> WARNING: /usr/lib64/open-vm-tools/componentMgr/saltMinion/svtminion.sh:_curl_download failed to
download file 'repo.json' from 'https://repo.saltproject.io/salt/py3/onedir/repo.json' on '3' attempt, ret-
code '6'
<date+time> WARNING: /usr/lib64/open-vm-tools/componentMgr/saltMinion/svtminion.sh:_curl_download failed to
download file 'repo.json' from 'https://repo.saltproject.io/salt/py3/onedir/repo.json' on '4' attempt, ret-
code '6'
<date+time> ERROR: /usr/lib64/open-vm-tools/componentMgr/saltMinion/svtminion.sh:_curl_download failed to
download file 'repo.json' from 'https://repo.saltproject.io/salt/py3/onedir/repo.json' after '5' attempts
```

## On Windows

The "`vmware-svtminion-install-*.log`" file for the failed install shows a trace similar to:

```
[<date+time>] [#] [DEBUG ] repo.json not found at: https://repo.saltproject.io/salt/py3/onedir
[<date+time>] [#] [DEBUG ] Looking for version in web directory: https://repo.saltproject.io/salt/py3/onedir/
latest
[<date+time>] [#] [DEBUG ] Directory not found: https://repo.saltproject.io/salt/py3/onedir/latest
[<date+time>] [#] [ERROR ] Failed to get Package Info for Version: latest
[<date+time>] [#] [INFO ] Setting status: installFailed
```

```
[<date+time>] [#] [DEBUG ] Set status to installFailed
```

This issue is resolved in this release.

The new versions of the salt-minion integration scripts supporting the new Salt Project repository locations are available.

- <https://packages.broadcom.com/artifactory/saltproject-generic/onedir/>

## **Known Issues**

### **VMware Tools Issues**

The issues described in this section are not applicable to Windows Arm.

#### **Provide tools.conf settings to deactivate one-time and periodic time synchronization**

The new tools.conf settings `disable-all` and `disable-periodic` allow the guest OS administrator to deactivate one-time and periodic time synchronization without rebooting the VM or restarting the guest OS.

### **Known Issues from Previous Releases**

### **VMware Tools Issues**

#### **The Unity mode does not work with VMware Tools 12.4.0 and later**

For VMs running on VMware Workstation 17.6 and earlier and VMware Fusion 13.6 and earlier, the Unity mode stops working if the VMs run VMware Tools 12.4.0 and later versions.

The Unity mode has been deprecated, starting with VMware Workstation 17.6 and VMware Fusion 13.6. These product versions include VMware Tools 12.4.5 or later. For more information about the features supported by VMware Workstation and VMware Fusion, refer to product release notes.

**Workaround:** To use the Unity mode on earlier VMware Workstation and VMware Fusion versions, use VMware Tools 12.3.5 and earlier.

#### **Memory leak when running the Ortec application**

When you run the Ortec application, you might experience an increase in memory usage and see a memory error.

**Workaround:** To avoid this issue, set the system environment variable to zero - `SVGA_ALLOW_LLVMPIPE=0`

#### **Shared Folders mount is unavailable on Linux VM**

If the **Shared Folders** feature is enabled on a Linux VM while it is powered off, the shared folders mount is not available on restart.

Note: This issue applies to VMware Tools running on Workstation and Fusion.

If the VM is powered on, disable and enable the **Shared Folders** feature from the interface. To resolve the issue permanently, edit `/etc/fstab` and add an entry to mount the Shared Folders automatically on boot.

For example, add the line:

```
vmhgfs-fuse    /mnt/hgfs    fuse    defaults,allow_other    0    0
```

For more information on how to configure VMware Tools Shared Folders, see [KB 60262](#).

#### **VMware Tools upgrade fails on Windows 7 SP1 and Windows Server 2008 R2 SP1 without SHA-2 code signing support**

Microsoft has changed Windows driver signing to use the SHA-2 algorithm exclusively starting December 3, 2019. Legacy Windows systems without SHA-2 code signing support fail driver signature verification.

Refer to [KB 78708](#).

### **Installation of Windows Vista, Server 2008, or Windows 7 fails in a virtual machine**

Installing a Windows OS Vista, Server 2008, or Windows 7 in a virtual machine with a boot disk on a PVSCSI controller, fails to install the required PVSCSI driver.

Download the VMware Tools package version 11.1.5 from <https://support.broadcom.com/>, extract the contents, and use the VMware Tools windows.iso or the floppies for Windows OS Vista or Server 2008.

#### **Note:**

Users managing ESX hosts or having a requirement to perform multiple installations of the same Windows OS version on a PVSCSI controller, can see the steps outlined in [KB 84200](#).

### **VMware Tools upgrade failed with error code 1072 (The specified service has been marked for deletion.)**

When upgrading VMware Tools to a new version, if the previous version's VMware Tools service is not deleted completely, this incomplete service removal causes installing the new VMware Tools version service to fail and leads to a fatal error for the upgrade.

When detecting an incomplete service removal to prevent VMware Tools upgrade from failing catastrophically every time, the new service creation will pause and retry to see if the condition clears. The VMware Tools installer will pause for up to 2 1/2 minutes. After this, a fatal error will occur. If the condition clears, the upgrade creates the new service and continues.

For more information, see [KB 84269](#).

**Workaround:** Reboot the Windows system and restart VMware Tools install.

### **After upgrading to a new version of VMware Tools with an installer parameter to remove the NetworkIntrospection feature, the old version of the vnetflt or vnetWFP driver service continues to run**

After the upgrade, the NetworkIntrospection feature is not present in the system's VMware Tools MSI database, but the feature's vnetflt or vnetWFP driver service still exists.

Refer to [KB 78016](#).

Note: This issue applies to VMware Tools upgrades from versions older than 11.1.0 only.

### **Installing or upgrading versions earlier than VMware Tools 10.3.0 to VMware Tools 11.1.x might take longer and Windows OS might need a restart**

The installation process might appear to be in progress and display a message similar to the following: "Preparing 'VMware Tools' for installation..."

During this process, the user might be prompted to restart the operating system.

For more information, see [KB 55798](#).

### **VMware Tools Issues on Windows Arm**

#### **Windows Arm VMs encounter either BSOD with DPC\_WATCHDOG\_VIOLATION or hang**

Typically, with 3D games or resizing a remote desktop on VMware Tools 12.3.0, Windows Arm VMs encounter either BSOD with DPC\_WATCHDOG\_VIOLATION or hang.

You can disable 3D acceleration in VM settings. For more information, see [KB 95283](#).

# VMware Tools Administration

---

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.

## Introduction to VMware Tools

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

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 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.

You must 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, you must 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 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*.

## 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.SAMLSAMLTokenAuthentication](#) 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 plug-in.
- `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 plug-in.
- `appInfo` - Collects the information about running applications inside the guest and publishes the information to a guest variable.
- `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 plug-in 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 plug-in.
- `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 a simplified and scalable approach for the installation 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 13.0.0 brings in several improvements to lifecycle management.

- Offline bundles with VMware Tools VIB are available for installation on supported vSphere releases using vSphere Lifecycle Manager (formerly vSphere Update Manager). These bundles are intended for vSphere 6.7 and later versions, including vSphere 7.x, 8.x, and 9.0.
- Microsoft System Center Configuration Manager (SCCM) manages the deployment of Windows applications across an enterprise and can also deploy VMware Tools. For more information, see [Deploying VMware Tools using SCCM](#).

VMware Tools 13.0.0 depends on and ships Microsoft Visual C++ 2015-2022 Redistributable version 14.x. As a prerequisite for VMware Tools 13.0.0 installation, Microsoft Visual C++ 2015-2022 Redistributable is installed on the system.

## Mapping of VMware Tools and Guest Operating System

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

**Table 1: VMware Tools support for Guest Operating Systems**

ISO Images	Supported Guest Operating System	Available Version
<code>windows.iso</code>	Windows 7 Service Pack 1 (SP1) or Windows Server 2008 R2 Service Pack 1 (SP1) and later <ul style="list-style-type: none"> <li>Windows OS level prerequisites               <ul style="list-style-type: none"> <li>Windows Server 2025</li> <li>Windows Server 2022</li> <li>Windows 11</li> <li>Windows Server 2019</li> <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> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>For Windows Server 2025, use VMware Tools 11.3.0 or later. For best performance, use VMware Tools 12.5.0 or later.</li> <li>For Windows Server 2022 or Windows 11, use VMware Tools 10.3.5 or later. For best performance, use VMware Tools 12.0.0 or later.</li> <li>For the other guest operating system versions, use VMware Tools 10.1.0 or later.</li> </ul>
<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 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  <b>Note:</b> The Windows pre-Vista iso image for VMWare Tools is no longer packaged with ESX. The Windows pre-Vista iso image is available for download by users who require it.	10.0.12
<code>linuxPreGLibc25.iso</code>	Linux guest operating systems earlier than RHEL 5, SLES 11, and other distributions with glibc version earlier than 2.5	10.0.12
<code>darwinPre15.iso</code>	MAC OS versions earlier than 10.10.x	10.0.12

## VMware Tools Device Drivers

Device drivers improve sound, graphics, networking, and storage performance. You can select the drivers to be installed while performing a custom VMware Tools installation or reinstallation.

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 of these drivers, including configuration requirements, best practices, and performance, see the documentation for your VMware product. The following device drivers can be included with VMware Tools.

### VMCI Driver

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.

VMCI driver is installed by default as part of VMware Tools installation. If the user had disabled this VMCI driver in the setup settings during a previous installation, VMware Tools automatically re-installs VMCI driver during the upgrade.

**Note:** VMCI driver cannot be disabled as the VMware Tools System service functionality is dependent on this driver.

### 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.

- **NSX 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.
- **NSX Network Introspection Driver:** The Network Introspection driver supports NSX for vSphere Activity Monitoring.

### 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.

### VMXNet NIC Driver

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.

### 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.

	<p>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.</p> <p>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.</p> <p>The driver is included as part of the VMware Tools package or comes bundled with VMware ESX. It is available on the host as a floppy image at <code>/vmimages/floppies/vm SCSI.flp</code>. The driver can be used in Windows XP, Windows Server 2003, or Windows 2000.</p>
<b>Mouse Driver</b>	<p>The virtual mouse driver improves mouse performance. This driver is required if you use third-party tools such as Microsoft Terminal Services.</p>
<b>Audio Driver</b>	<p>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.</p>
<b>Audio driver</b>	<p>This sound driver is required for all 64-bit Windows guest operating systems and 32-bit Windows Server 2003, Windows Server 2008, and Windows Vista guest operating systems if you use the virtual machine with Workstation or Fusion.</p>
<b>Kernel module for sharing folders</b>	<p>The host-guest file system module, called <code>hgfs.sys</code> on Windows guest operating systems and <code>vmhgfs</code> on Linux and Solaris, is required to use the virtual machine with Workstation or Fusion and share folders between hosts and guests.</p>
<b>vmblock Module</b>	<p>Used in Workstation and Fusion, this module is essential for drag-and-drop copy operations between hosts and guests.</p>
<b>ThinPrint driver</b>	<p>This driver enables the Virtual Printing feature on Microsoft Windows virtual machines. With Virtual Printing, printers added to the operating system on the client or host appear in the list of available printers in the guest operating system. No additional printer drivers must be installed in the virtual machine.</p>
<b>Memory controller driver</b>	<p>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.</p>
<b>Modules and drivers that support making automatic backups of virtual machines</b>	<p>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</p>
<b>VMware drivers for Linux</b>	<p>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.</p>

**VMHGFS driver**

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.

For more information about availability, maintenance, and support policy for inbox drivers for Linux, see the KB article [2073804](#).

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.

## VMware User Process

VMware user process allow you to use certain features (such as copy, paste, drag, drop and so on) with VMware product supporting them.

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.

## Open VM Tools

Open VM Tools (open-vm-tools) is the open source implementation of VMware Tools for Linux and FreeBSD 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 [Broadcom Compatibility Guide](#).

**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 website 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.

**Note:** For support on open-vm-tools, you must contact the Linux 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 operating systems. 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 operating systems, 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 website at <https://github.com/vmware/open-vm-tools>.
- The Vendor-provided optional packages (availability varies by distribution). Some Linux versions may include additional `open-vm-tools` packages tailored for specific use cases.
  - `open-vm-tools-sdmp` contains a plug-in for Service Discovery.
  - `open-vm-tools-containerinfo` contains the `containerInfo` plug-in, which requires additional build and runtime dependencies.
  - `open-vm-tools-salt-minion` embeds Salt Minion for configuration management.

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, and later releases
- 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 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 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 KB article [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, 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 system to manage VMware Tools and you cannot use vSphere Update Manager to upgrade VMware Tools.

For more information, go to the [Broadcom Operating System Specific Packages](#) Web site. For more information on installing OSPs, see the VMware Tools Installation Guide for [Operating System Specific Packages for ESX](#) version 4.1 and later, and ESX versions 5.x and 6.x.

## Installing VMware Tools

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

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

The installers for VMware Tools are ISO image files. The CD-ROM in your guest operating system detects the ISO image file. Each type of guest operating system, including Windows, Linux, and Mac OS X, has an ISO image file. When you select the command to install or upgrade VMware Tools, the virtual machine's first virtual CD-ROM disk drive temporarily connects to the VMware Tools ISO file for your guest operating system.

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.

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.

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

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

#### Note:

On ESX 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 a missing ISO error. For more information, see [KB 2129825](#).

**Note:** AppDefense is not supported for VMware Tools 12.0.0 and later versions.

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 KB article [1014294](#).

**Note:** If the VMware Tools ISO file for the guest operating system is not available with the product, you are prompted to download the file from <https://packages-prod.broadcom.com/tools/frozen/>. Alternatively, on the host, from the VMware Workstation Pro/VMware Fusion menu bar, select **Virtual Machine > Install VMware Tools**. You will get a link to download the specific VMware Tools ISO file.

## Disable Access Protection from McAfee Antivirus Virus Scan Console

You must disable the Access Protection in the McAfee Antivirus Scan Console before installing VMware Tools in a Windows guest operating system.

- Power on the virtual machine
- Use McAfee Antivirus in 'Standard' mode

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

**Note:** McAfee Antivirus prevents VMware Tools upgrade, if it is 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.
- Install VMware Tools.
- Re-activate **Access Protection** when your VMware Tools upgrade or installation is complete.
- For more information, see the KB article [1009965](#).

## Enable Carbon Black Sensor using VMware Tools for Windows

VMware Tools enables Carbon Black Sensor feature to provide intrinsic security in the virtual machine. VMware Tools Carbon Black feature comprises of a lightweight VMware Tools system service Carbon Black Helper (CBHelper) plug-in and a Carbon Black launcher (CBLauncher) application. The CBHelper plug-in runs as part of VMware Tools service. When the administrator enables security in a virtual machine, this CBHelper plug-in triggers the CBLauncher, which downloads the Carbon Black Sensor install package, performs installation, and exits.

Ensure the following before using this feature:

- vCenter version: 6.7U1 and higher
- VMTools version: 11.2
- Only 64 bit platforms are supported. List of supported platforms:
  - Desktop Platforms: Windows 7-SP1, Windows 8, Windows 8.1, Windows 10
  - Server Platforms: Windows Server 2008R2, 2012, 2012R2, 2016, 2019

VMware Tools enables only the new installation, upgrade, or uninstallation of the CBHelper plug-in and CBLauncher application. For any following VMware Tools uninstall or upgrade, it only upgrades or removes the VMware Tools system service CBHelper plug-in and CBLauncher. It does not uninstall the Carbon Black installer or Sensor.

**Note:** Carbon Black Sensor is a separate product installation from VMware Tools. VMware Tools does not install the Carbon Black Sensor, but provides support to enable this feature by installing the CBHelper plug-in and CBLauncher application.

### 1. Installing VMware Carbon Black Sensor on a virtual machine

- Enable the CBHelper plug-in
  - VMware Tools Installer:  
The VMware CBHelper plug-in is present as as part of the default installation setup of VMware Tools. By default, this plug-in is enabled.
  - Silent installation:  
To add the CBHelper plug-in after installation is complete, run the following command:  
`setup.exe /S /v "/qn REBOOT=R ADDLOCAL=CBHelper"`
- Disable the CBHelper plug-in:
  - VMware Tools Installer:  
To disable the CBHelper plug-in, select **CUSTOM** option in the VMware Tools Installer Setup and remove the the Carbon Black Helper feature from the default settings list.
  - Silent installation:  
To install of VMware Tools without the CBHelper plug-in using silent installation, run the following command:  
`setup.exe /S /v "/qn REBOOT=R ADDLOCAL=ALL REMOVE=CBHelper"`

## 2. Overriding the installation of VMware Carbon Black Sensor on a virtual machine

There are two ways to turn off installation of Carbon Black Sensors:

- **VMware Tools Configuration File:**  
The VI administrator can set the CBHelper plug-in poll interval to 0 by updating the `tools.conf`. By default, the poll interval value is 180 seconds.
- **Registry Setting:**  
When a VM administrator (other than the VI administrator) wants to block the Carbon Black Sensor installation, even if the VMware Tools is installed with the Carbon Black feature, the CBLauncher provides a configuration to override this feature. When this configuration is set, CBLauncher skips the installation of the Carbon Black Sensor. This override mechanism provides an 'opt-out' for VM administrators.

For Windows, this registry setting is as follows,

**Registry Path:** HKLM\SOFTWARE\VMware Inc.\CbLauncher

- Value Name: DisableCBInstall
- Value Name: DisableCBInstall
- Value Type: REG\_DWORD
- Value Data: 1

### Operation Result

- 1 – Disable installation: The Carbon Black Sensor will not be installed.
- Any other value/no value/error: Ignored. The Carbon Black Sensor will be installed.

### Note:

A Carbon Black Cloud Workload Plug-in is provided for vCenter to secure your workloads. For more information on how to install, configure, and use this plug-in, see the *VMware Carbon Black Cloud Workload* guide.

## Enable Salt Minion Using VMware Tools

Salt Project is Python-based open-source software for event-driven IT automation, remote task execution, and configuration management.

- Supports only 64-bit operating systems.
- Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022 are supported.  
**Note:** Windows Server 2008 R2 is not supported.
- VMware Tools must be installed with the Salt Minion feature. By default, this feature is enabled.
- There are dependencies on installed packages in Linux (like curl and wget)

For more information on Salt, see the [Salt User Guide](#).

Salt requires a salt-minion to be deployed on the guest. Salt-specific guest variables are set on the host side per VM basis and subsequently read by VMware Tools inside the guest. VMware Tools then downloads the salt bundle and spins up a salt-minion instance inside the guest.

- **Host side configuration per VM using guest variables**

The host admin manages all the guest variable settings on the host side for a particular VM using the VIM API or vSphere/VC UI.

- Windows:

The VMware Tools Salt Minion feature is installed by default and can be modified in a custom installation.

For VMware Tools to create a salt-minion instance on a particular VM and connect the salt-minion with the salt-master, the host admin must configure and set the guest variable for that VM.

In the vSphere Client, navigate to, right-click a VM, and select **Edit Settings**. In the VM Options tab, select **Advanced > Edit Configuration > Add/Delete parameter**, and set

- `guestinfo./vmware.components.salt_minion.desiredstate` to **present**
- `guestinfo./vmware.components.salt_minion.args` to <custom arguments to VMware Tools salt-minion setup script>

For example:

```
guestinfo./vmware.components.salt_minion.desiredstate → present
guestinfo./vmware.components.salt_minion.args → master=1.2.3.4
```

- Linux:

The host admin must install open-vm-tools and open-vm-tools-salt-minion, and then set the guest variable for a particular VM as:

- `guestinfo./vmware.components.salt_minion.desiredstate` to **present**
- `guestinfo./vmware.components.salt_minion.args` to <custom arguments to VMware Tools salt-minion setup script>

For example:

```
guestinfo./vmware.components.salt_minion.desiredstate → present
guestinfo./vmware.components.salt_minion.args → master=1.2.3.4 id=12345
```

- **Removing salt-minion**

In Windows or Linux, if the host admin sets the guest variable `guestinfo./vmware.components.salt_minion.desiredstate` to **absent**, then VMware Tools removes the salt-minion instance in the guest VM.

For example:

```
guestinfo./vmware.components.salt_minion.desiredstate → absent
```

- **Checking the latest status of salt-minion inside the guest**

To check the latest status of the salt-minion inside the guest in the vSphere Client, use the guest variable:

```
guestinfo.vmware.components.salt_minion.laststatus
```

- **Guest side configuration using tools.conf**

The `tools.conf` file contains the configurations for VMware Tools in an `.ini` format. This tool looks for the `salt_minion` section and uses the configurations defined under that section. This file is stored at:

Windows - `C:\ProgramData\VMware\VMware Tools\tools.conf`

Linux - `/etc/vmware-tools/tools.conf`

Here is an example of the `salt_minion` section as defined in `tools.conf`:

```
[salt_minion]
master=1.2.3.4
conf_file=/etc/salt/minion
```

```
id=dev_minion
```

**Note:** Only minion config options are available in `tools.conf`. The desired script action cannot be obtained from `tools.conf`.

- **Configuring the interval to monitor state change in the guest variables:**

VMware Tools periodically polls guest variables for state changes. The default poll-interval is 180 seconds and can be configured in the `tools.conf` settings.

```
[componentmgr]
```

```
poll-interval=180 (Default value: 180 seconds)
```

- **Enabling and disabling component (salt\_minion):**

- The guest admin can enable salt\_minion by configuring the `tools.conf` settings.

```
[componentmgr]
```

```
included=salt_minion
```

- Guest admin can enable all the components by configuring the `tools.conf` settings.

```
[componentmgr]
```

```
included=all (Default configuration)
```

- Guest admin can deactivate all components by configuring the `tools.conf` settings.

```
[componentmgr]
```

```
included=none
```

- **Installing salt-minion using an install script**

- **Linux environment**

On Linux systems, the install script `svtminion.sh` is a bash script with the following prerequisites:

```
-systemctl
```

```
-curl
```

```
-sha256sum
```

```
-vmtoolsd
```

```
-grep
```

```
-awk
```

```
-sed
```

```
-cut
```

```
-wget
```

`svtminion.sh --help` shows the command line options.

**Usage:**

```
bora-vmsoft/install/Source/services/plugins/componentMgr/svtminion.sh
```

```
[-c|--clear] [-d|--depend] [-h|--help] [-i|--install]
```

```
[-j|--source] [-l|--loglevel] [-m|--minionversion]
```

```
[-n|--reconfig] [-q|--stop] [-p|--start]
```

```
[-r|--remove] [-s|--status] [-u|--upgrade]
```

```
[-v|--version]
```

Script	Description
<code>-c, --clear</code>	Clears the previous Salt Minion identifier and keys, and sets the specified identifier if it is present.
<code>-d, --depend</code>	Checks the dependencies required to run the existing script.
<code>-h, --help</code>	Shows the help message and exit.
<code>-c, --clear</code>	Clears the previous Salt Minion identifier and keys, and sets the specified identifier if present.

Script	Description
<code>-i, --install</code>	Install and activate Salt Minion configuration parameters. The key=value can also be passed on to the CLI.
<code>-j, --source</code>	Specifies location to install Salt Minion from. The default is <a href="https://packages.broadcom.com/artifactory/saltproject-generic/onedir/">https://packages.broadcom.com/artifactory/saltproject-generic/onedir/</a> For example: URL location <code>http://my_web_server.com/my_salt_onedir</code> <code>https://my_web_server.com/my_salt_onedir</code> file: <code>file://my_path/my_salt_onedir</code> <code>//my_path/my_salt_onedir</code> If a specific Salt Minion version is specified with <code>-m</code> , it will be appended to the source path. The default is the latest version.
<code>-l, --loglevel</code>	Sets the log level for logging: silent error, warning, debug, info. The default loglevel is warning.
<code>-m, --minionversion</code>	Installs a Salt Minion version. The default Salt Minion version is latest.
<code>-n, --reconfig</code>	Restarts the Salt Minion after reading the updated config.
<code>-q, --stop</code>	Stops Salt Minion.
<code>-p, --start</code>	Starts or restarts Salt Minion.
<code>-r, --remove</code>	Deactivates and removes Salt Minion.
<code>-s, --status</code>	Returns the status for this script.
<code>-u, --upgrade</code>	Upgrades when installing. Used with <code>--install</code> .
<code>-v, --version</code>	Displays the script version.

For example, the Salt Minion VMware Tools integrations script is `svtminion.sh --status`.

Here is an example of the installing `salt_minion` as defined in `tools.conf`:

```
[salt_minion]
master=1.2.3.4
conf_file=/etc/salt/minion
id=dev_minion
source=https://my_web_server.com/my_salt_onedir
```

#### Note:

If installing from your private replica of the standard repository location for salt, use `source=https://packages.broadcom.com/artifactory/saltproject-generic/onedir/`.

- Windows environment

On Windows systems, the install script `svtminion.ps1` is a powershell script. The only prerequisite for Windows is the 'vmtoolsd.exe' binary, which is used to query the guest variables data.

To get help for this script, run the command `svtminion.ps1 -h` or `Get-Help svtminion.ps1`.

VMware Tools script for managing the Salt minion on a Windows guest is:

```
.\svtminion.ps1 [-Install] [-MinionVersion <String>] [-Source <String>] [[-ConfigOptions] <String[]>] [-LogLevel <String>] [-Help] [-Version] [<CommonParameters>]
```

where `-Source <String>` is the URL or path to the repo containing the installers.

This would contain a directory structure similar to that found at the default location: <https://packages.broadcom.com/artifactory/saltproject-generic/onedir/>. This can handle most common protocols like http, https, ftp, unc, local.

For example:

```
PS>svtminion.ps1 -Install
```

```
PS>svtminion.ps1 -Install -MinionVersion 3004-1 master=192.168.10.10 id=dev_box
PS>svtminion.ps1 -Install -Source https://my.domain.com/vmtools/salt
```

**Note:**

To see the examples, type `get-help .\svtminion.ps1 -examples`

For more information, type `get-help .\svtminion.ps1 -detailed`

For technical information, type `get-help .\svtminion.ps1 -full`

- **Fetching log information**

Guest admin can fetch log information related to salt-minion from the following path:

#### Windows

Log File	Location
Log file for checking salt-minion status	C:\Windows\Temp\vmware-svtminion-status-{Timestamp}.log
Log file for installing a salt-minion instance inside the guest	C:\Windows\Temp\vmware-svtminion-install-{Timestamp}.log
Log file for removing a salt-minion instance inside the guest:	C:\Windows\Temp\vmware-svtminion-remove-{Timestamp}.log
Log file for checking runtime information after installing or removing a salt-minion instance inside the guest	C:\salt\var\log\minion log files

#### Linux

Log File	Location
Log file for checking salt-minion status	/var/log/vmware-svtminion.sh-status-{Timestamp}.log
Log file for installing a salt-minion instance inside the guest	/var/log/vmware-svtminion.sh-install-{Timestamp}.log
Log file for removing a salt-minion instance inside the guest:	/var/log/vmware-svtminion.sh-remove-{Timestamp}.log
Log file for checking runtime information after installing or removing a salt-minion instance inside the guest	/var/log/salt/minion

## Manually Install VMware Tools on Windows

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

- 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.

Perform the following steps to manually install VMware Tools on Windows.

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

VMware Product	Action
vSphere Client	Right-click the virtual machine and select <b>Guest OS &gt; Install VMware Tools...or Guest OS &gt; 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>

- If you are using vCenter 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.  
To launch the wizard manually if autorun is not enabled, click **Start > Run** and enter `D:\setup.exe`, where `D:` is your first virtual CD-ROM drive.
- 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.  
**Note:** If NSX Guest Introspection (GI) drivers are installed and you are using 'Custom' installation option in the Tools installer for upgrade, ensure that all installed GI drivers are upgraded during upgrade.
- When prompted, reboot the virtual machine.  
If you use vCenter, the **VMware Tools** label on the **Summary** tab changes to **OK**.  
If you upgraded VMware Tools as part of a vSphere upgrade, 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 Install VMware Tools on Windows Arm

You can manually install VMware Tools for Windows Arm on a virtual machine running Windows 10 1709 Arm and later versions. VMware only supports Windows Arm VMs running on VMware Fusion on Apple silicon.

This VMware Tools Arm functionality is limited to:

- Installer with interactive GUI and command line support

- 3D Graphics
- Multiple monitor
- Resizing fit to window
- Guest clock time synchronization
- Soft power operations
- Desktop events for user switching
- Drag and drop of files between the host and guest
- Copy and paste of files and text between host and guest
- `vmrun` support for running guest operations

For example, transferring files to and from guest, running programs and scripts in the guest.

For the prerequisites and install steps, refer to the [Manually Install VMware Tools on Windows](#) section for the VMware Fusion product.

## Automatically Install VMware Tools on Multiple Windows Virtual Machines

You can install VMware Tools on multiple virtual machines with Windows guest operating systems. You can automate this installation and specify the VMware Tools components that you want to include or exclude in the options.

- 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 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 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 [Specify VMware Tools Components for Silent Installations](#).

1. In vSphere Client, select the host, cluster, or datacenter and click the **Virtual Machine** inventory object.
2. Right-click the virtual machine and select **Guest OS > Install VMware Tools**.
3. Provide the install or upgrade configuration information.

## Specify VMware Tools Components in Silent Installation

You can specify the VMware Tools Components that you want during VMware Tools installation using the command line options and properties, or during the automatic installation process.

VMware Tools provides various VMware Tools Components. You can install these components either during a new installation or an upgrade of VMware Tools.

### Silent Install - New Install or Upgrade

The command format for a new install or upgrade is:

```
setup.exe /S /v "/qn msi_args"
```

The command format to include all customizable features except those specified, using ADDLOCAL and REMOVE MSI properties is:

```
setup.exe /S /v "/qn msi_args ADDLOCAL=ALL REMOVE=component"
```

**Note:** Component name is feature name and is case-sensitive. If you want to remove more than one component, the feature names must be comma separated.

For example:

- To install all customizable features except the 'Shared Folders' feature, run the command:  

```
setup.exe /S /v "/qn REBOOT=R ADDLOCAL=ALL REMOVE=Hgfs"
```
- To install all customizable features except the 'Shared Folders', 'File Introspection', 'Network Introspection', and 'Salt Minion' features, run the command:  

```
setup.exe /S /v "/qn REBOOT=R ADDLOCAL=ALL  
REMOVE=Hgfs,FileIntrospection,NetworkIntrospection,SaltMinion"
```
- The following command shows MSI options and properties to perform a silent installation with a logging file specified that suppresses rebooting when installation is complete. This command also installs all components except the shared folders component.  

```
setup.exe /S /v "/qn /l*v ""%TEMP%\vmmsi.log"" REBOOT=R ADDLOCAL=ALL  
REMOVE=Hgfs"
```

### Silent Install - Modify Install

After a new install or upgrade, to modify the installed customizable features, you can add or remove a component using the ADDLOCAL and/or REMOVE MSI properties:

```
setup.exe /S /v "/qn msi_args ADDLOCAL=component REMOVE=component"
```

msi\_args can be specified as mentioned above for logging and suppressing of reboot. For more extensive list of msi\_args arguments, see *Microsoft documentation*.

**Table 3: VMware Tools Visible Core Components (Not customizable)**

Feature Name	Description
VMCI	<p>Virtual Machine Communication Interface (VMCI) 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>VMCI driver is installed by default as part of VMware Tools installation. If the user had disabled this VMCI driver in the setup settings during a previous installation, VMware Tools automatically re-installs VMCI driver during the upgrade.</p> <p><b>Note:</b> From this release onwards, VMCI driver cannot be disabled as the VMware Tools System service functionality is dependent on this driver.</p>

Other core components installed by default are not visible.

**Table 4: VMware Tools Customizable Components (Using ADDLOCAL and/or REMOVE MSI properties) Note: Features available on Windows Arm are noted in the description.**

Feature Name	Description
CBHelper	Helper to install of Carbon black Sensor on a virtual machine.

Feature Name	Description
Perfmon	Utility for WMI performance logging. Enables performance monitoring between the Guest SDK and the WMI environment.
VmwTimeProvider	Time provider for VMware virtual precision clock device.
FileIntrospection	The NSX File Introspection driver, <code>vsepflt.sys</code> is the first of the two guest introspection drivers. You can install it separately, without installing the NSX Network Introspection driver. <b>Note:</b> This component is dependent on the VMCI driver.
NetworkIntrospection	The NSX Network Introspection driver, <code>vnetflt.sys</code> is the second of the two guest introspection drivers. <b>Note:</b> This component is dependent on the VMCI driver. VMware Tools 10.2.5 supports <code>vnetWFP</code> driver for Windows 7 and later.
ServiceDiscovery	The Service Discovery component enables the discovery of various services running inside a virtual machine. <b>Note:</b> This user-mode component is dependent on the VMCI driver.
DeviceHelper	The VMware Device Helper component helps to perform a device check and swap in your virtual machine. <b>Note:</b> This user-mode component is dependent on the VMCI driver.
Hgfs	Hgfs is a VMware shared folders driver that allows files to be shared between your virtual machine and the host computer. You can use this driver, if you plan to use this virtual machine with VMware Workstation, Player, or Fusion. <b>Note:</b> <ul style="list-style-type: none"> <li>If you exclude this feature, you cannot share a folder between your virtual machine and the host system.</li> <li>This component is dependent on the VMCI driver.</li> </ul>
SVGA	The VMware SVGA driver enhances the performance of your virtual video card. <b>Note:</b> If you exclude this feature, it limits the display capabilities of your virtual machine. <b>Note:</b> This feature is also available for Windows Arm.
VMXNet	The VMware VMXNet networking driver enhances the performance of your virtual network card.
VMXNet3	The VMware VMXNet3 networking driver enhances the performance of your virtual network card (ndis5/ndis6). This is the Next-generation VMware VMXnet networking driver for virtual machines that use virtual hardware version 7 and higher. For more information, see the KB article <a href="#">1001805</a> . VMXNET3 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 the Windows VMXNET3 driver. Virtual hardware version 7 corresponds to ESX 4.x compatibility. <b>Note:</b> This feature is also available for Windows Arm.
PVSCSI	The VMware Paravirtual SCSI adapters enhances the performance of your paravirtual SCSI devices.
EFIFW	The EFIFW driver is used for EFI Firmware update.

Feature Name	Description
MemCtl	The Memory Control Driver provides enhanced memory management of the virtual machine. You can use this driver, if you plan to use a virtual machine in the vSphere environment. <b>Note:</b> If you exclude this feature, it hinders the memory management capabilities of the virtual machine running in a vSphere environment.
Mouse	The VMware PS2 Mouse driver enhances the performance of your virtual PS2 mouse. <b>Note:</b> If you exclude this feature, the mouse performance of your virtual machine will decrease.
MouseUsb	The VMware USB Mouse Driver enhances performance of your USB mouse. <b>Note:</b> This feature is also available for Windows Arm.
Audio	The Audio driver provides audio for your virtual sound card. <b>Note:</b> This Audio driver is for 64-bit Windows Vista and later operating systems.
VSS	The VSS driver is used for creating automatic backups. This driver is used, if the guest operating system is Windows Vista, Windows Server 2003, or other newer operating systems. Linux and older Windows operating systems use the Filesystem Sync driver.
BootCamp	The BootCamp driver provides Mac BootCamp support.
SaltMinion	Scripts required to set up Salt Minion on a virtual machine.

## Manually Install VMware Tools on Linux

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

- 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.

For more information about Linux distributions supported by Open VM Tools, see [Open VM Tools \(README\)](#) and the [Broadcom Compatibility Guide](#).

VMware Tar Tool for Linux virtual machine is feature-frozen at version 10.3.26, which includes important security features. Therefore, the linux.iso included in Workstation Player is 10.3.26 and will not be updated. Due to this change, the **Install/Update/Reinstall VMware Tools** menu is not available for the following Linux virtual machines:

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

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

For old Linux virtual machines that are not supported by Open VM Tools, follow these steps to install tar tools.

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

VMware Product	Action
vSphere Client	Right-click the virtual machine and select <b>Guest OS &gt; Install VMware Tools...or Guest OS &gt; 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. Run the `mount` command with no arguments to determine whether your Linux distribution automatically mounted the VMware Tools virtual CD-ROM image.

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

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

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

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

```
mkdir /mnt/cdrom
```

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

- b) Mount the CD-ROM drive.

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

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

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

```
cd /tmp
```

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

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

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

```
ls mount-point
```

Uncompress the installer.

```
tar xzpf /mnt/cdrom/VMwareTools-x.x.x-yyy.tar.gz
```

The value `x.x.x` is the product version number, and `yyy` is the build number of the product release.

5. If necessary, unmount the CD-ROM image.

```
umount /dev/cdrom
```

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

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

```
cd vmware-tools-distrib
```

```
sudo ./vmware-install.pl
```

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

Follow the instructions at the end of the script.

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

Usually, the `vmware-config-tools.pl` configuration file runs after the installer file finishes running. If you attempt to install a tar installation over an RPM installation, or the reverse, the installer detects the previous installation and must convert the installer database format before continuing.

#### Note:

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

If you upgraded VMware Tools as part of a vSphere upgrade, determine whether to upgrade the virtual machines in your environment. For more information about the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

## Manually Install VMware Tools on macOS

You can install or upgrade VMware Tools on a macOS virtual machine using an installer assistant.

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

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

For macOS VMs, the VMware Tools contains the following two kernel extension modules that are vital for certain features when running on Fusion:

- `com.vmware.kext.vmhgfs`: For hgfs or shared folder support
- `com.vmware.kext.VMwareGfx`: For VMware video driver

**Note:** macOS Big Sur onwards, Apple has deprecated support for KEXT kernel extension modules. The KEXT modules are not loaded automatically when you install the VMware tools. If you want to use the features associated with the kernel extension modules, ensure that you manually allow the loading of VMware kernel extension modules when prompted with an option.

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	Right-click the virtual machine and select <b>Guest OS &gt; Install VMware Tools...</b> or <b>Guest OS &gt; Upgrade VMware Tools...</b> and select <b>Interactive Tools Installation</b> or <b>Interactive Tools Upgrade</b>
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>

2. In the vSphere Client inventory, right-click the virtual machine and select **Guest > Install/Upgrade VMware Tools**.
3. Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
4. Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware Tools</b>

VMware Product	Action
vSphere Web Client	<p>Right-click the virtual machine and select <b>Guest OS &gt; Install/Upgrade VMware Tools</b>.</p> <ol style="list-style-type: none"> <li>1. To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp.</li> <li>2. Click the <b>Virtual Machines</b> tab.</li> </ol>

5. If you 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.

6. On the host, from the VMware Fusion menu bar, select **Virtual Machine > Install VMware Tools**.

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

If the VMware Tools ISO file for the guest operating system is not available with the product, you get a pop-up with a link to download the VMware Tools ISO file.

7. On the **Connect VMware Tools installer CD** pop-up, click **Install**

8. On the **VMware Tools** dialog box, click **Install VMware Tools**.

a) On the **Welcome to the VMware Tools Installer** page, click **Continue**.

b) Select **Standard Install on 'Macintosh HD'**, and then click **Install**.

If this is a first-time installation on macOS Big Sur or later, a System Extension Blocked pop-up will appear for each .kext in the VMware Tools release.

9. If you do not want to load the kernel extension modules, click **OK**.

**Note:** If you do not load the kernel extension modules, the features associated with the kernel extension modules will not work.

10. If you want to load the kernel extension modules, perform the following steps.

a) Click **Open Security Preference**.

b) Unlock the **Security & Privacy** user interface.

c) For the **System software from developer 'VMware, Inc.' was blocked from loading** option, click **Allow**.

d) For the restart prompt, click **Not now**.

e) Re-lock the **Security & Privacy** user interface.

f) Close the **Security & Privacy** window.

The VMware Tools installation completes successfully.

11. Click **Restart** to reboot the system with the KEXT modules loaded.

12. Optionally, to verify that the VMware KEXT modules are loaded, log in and run the following command:

```
sudo kextstat --list-only | grep -i vmware
```

## Manually Install VMware Tools on Solaris

You can manually install or upgrade VMware Tools on a Solaris virtual machine using the command line.

- 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.

1. VMware Product	Action
vSphere Client	Right-click the virtual machine and select <b>Guest OS &gt; Install 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>

- 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 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 again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

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

If you upgraded VMware Tools as part of a vSphere upgrade, determine whether to upgrade the virtual machines in your environment. For more information about the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

## Install Open VM Tools

Most Linux distributions include `open-vm-tools` and some distributions install `open-vm-tools` by default.

Like installing any other software on the guest, set up the package repository properly for the guest.

The `open-vm-tools` provided by Linux distributions meet the need of many users.

**Note:** Different Linux distributions update their version of `open-vm-tools` at different times.

Users can update their `open-vm-tools` from the package repository provided by a Linux distribution. The install instructions vary depending on the package management system used by a Linux distribution. Sometimes another package repository can be configured to install a newer version from the OS vendor. For detailed instructions, refer to the documentation of the OS vendor.

In general, `open-vm-tools` is supported for OSs that use three different package management systems:

- Ubuntu, Debian and Related OSes from this family use `apt` to install Debian (`*.deb`) packages

- Red Hat, Fedora and CentOS use dnf or yum to install RPM (\*.rpm) packages
- SUSE Linux Enterprise (SLE) and openSUSE use zypper to install RPM (\*.rpm) packages

All distributions split the package into a system and a desktop component. The desktop component is useful on systems that have a graphical UI (X11, Wayland, and so on). The package names are 'open-vm-tools' and 'open-vm-tools-desktop'. SLE and openSUSE ship another package 'libvmtools' as a dependency. The package management system automatically installs this dependency when 'open-vm-tools' or 'open-vm-tools-desktop' are installed.

## 1. Ubuntu, Debian, and Related OSes

1. Ensure that the package index is updated:

```
sudo apt-get update
```

2. If the VM has a GUI (X11, and so on), install or upgrade open-vm-tools-desktop:

```
sudo apt-get install open-vm-tools-desktop
```

3. Otherwise, use the command to install open-vm-tools:

```
sudo apt-get install open-vm-tools
```

## 2. RHEL, Fedora and CentOS

1. If the VM has a GUI (X11, and so on), install or upgrade open-vm-tools-desktop:

```
sudo yum install open-vm-tools-desktop
```

2. Otherwise, install open-vm-tools:

```
sudo yum install open-vm-tools
```

## 3. SLE and openSUSE

1. If the VM has a GUI (X11, and so on), install or upgrade open-vm-tools-desktop:

```
zypper install open-vm-tools-desktop
```

2. Otherwise, install open-vm-tools:

```
zypper install open-vm-tools
```

# Upgrading VMware Tools

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

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

For vSphere virtual machines,

A newer version of Tools is available for this VM

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

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

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

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

### Note:

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

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

## Configure Virtual Machines to Automatically Upgrade VMware Tools

You can configure virtual machines to automatically update VMware Tools.

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

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

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.

The next time the virtual machine is powered on, it checks the ESX 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 Upgrade VMware Tools in Virtual Machines

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

1. Start the vSphere Client and log in to the vCenter.
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:

1. This upgrade procedure is not applicable for operating systems that are installed with OSPs or Open VM Tools
2. If NSX Guest Introspection (GI) drivers are installed and you are using 'Custom' installation option in the Tools installer for upgrade, ensure that all installed GI drivers are upgraded during upgrade.

Virtual machine has upgraded version of VMware Tools.

## Automatically Upgrade VMware Tools in Virtual Machines

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 ESX host.

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

- Power on the virtual machine.
- Verify that the guest operating system is running.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.

1. Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
2. Select **Automatic Tools Upgrade**.
3. Optional: In the **Advanced Options** text box, enter advanced options for the Windows or Linux guest operating systems.

| Option                                           | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Microsoft Windows Guest Operating Systems</b> | <p>For the Windows guest operating system:</p> <ul style="list-style-type: none"> <li>• Enter <code>/s /v "/qn" /l "Microsoft_Windows_location\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.</li> </ul>                                                                                                                                                                                                                                                                  |
| <b>Linux Guest Operating Systems</b>             | <p>For the Linux guest operating system:</p> <ul style="list-style-type: none"> <li>• Enter <code>--default</code> to perform a silent upgrade of VMware Tools and install the <code>bin</code>, <code>lib</code>, and <code>doc</code> files in the default <code>/usr</code> directory. This is the default behavior.</li> <li>• Enter <code>--prefix=binary_location,lib_location,doc_location</code> to perform a silent upgrade of VMware Tools and install the <code>bin</code>, <code>lib</code>, and <code>doc</code> files in the specified locations.</li> </ul> |

4. Click **OK**.

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

## VMware Tools Installer Logging to Host

When GSS support team collects the `vm-support` bundle from customers, the installer log files are also included in it. The installer logs reside in the virtual machine as well as the host. These log files are critical for diagnosis and triaging of installation issues.

Install the VMware Tools version 11.0.0 and vSphere 7.0 (and later).

The Windows installer log files are all guest only and go to the `%Temp%` folder of the user account which launches the bootstrapper setup application.

The log files generated are:

Install log (`vminst.log`): Contains VMware controlled components log output.

MSI log (`vmmsi.log`): Contains Microsoft MSI controlled log output. To enable or disable MSI logging output, see the Microsoft knowledge base article [KB 22330](#).

1. For new installation or uninstallation or upgrade, `vmx.log.guest.level` option is used to enable or disable the installer logging to the host.

The allowed values to be set for this option are listed below:

| Value                                        | Description                                                                                                                                            |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>vmx.log.guest.level = "off"</code>     | Logging to host is disabled.<br>This is the default value.                                                                                             |
| <code>vmx.log.guest.level = "error"</code>   | The installer logs <code>vminst.log</code> and <code>vmmsi.log</code> are not sent to the host. Both the installer logs remain in the virtual machine. |
| <code>vmx.log.guest.level = "warning"</code> | The installer logs <code>vminst.log</code> and <code>vmmsi.log</code> are not sent to the host. Both the installer logs remain in the virtual machine. |
| <code>vmx.log.guest.level = "notice"</code>  | The installer logs <code>vminst.log</code> and <code>vmmsi.log</code> are not sent to the host. Both the installer logs remain in the virtual machine. |
| <code>vmx.log.guest.level = "info"</code>    | The installer log <code>vminst.log</code> is sent to the host but <code>vmmsi.log</code> remains in the virtual machine.                               |
| <code>vmx.log.guest.level = "verbose"</code> | Both the installer logs <code>vminst.log</code> and <code>vmmsi.log</code> are sent to the host.                                                       |
| <code>vmx.log.guest.level = "trivia"</code>  | Both the installer logs <code>vminst.log</code> and <code>vmmsi.log</code> are sent to the host.                                                       |

**Note:** Guest admin can use `"/mg"` or `"LOGMODE=G"` command line options to control and suppress logging to the host.

For example:

```
setup.exe /mg
setup.exe /v "LOGMODE=G"
setup.exe /S /v "/qn LOGMODE=G"
setup.exe /S /mg /v "/qn LOGMODE=G"
```

2. For auto upgrade, `install-vmxGuestLogDisabled` is read and parsed instead of `vmxGuestLogDisabled` in `tools.conf` file.

The allowed values to be set for this setting are listed as below:

| Value                                            | Description                                                                                    |
|--------------------------------------------------|------------------------------------------------------------------------------------------------|
| <code>install-vmxGuestLogDisabled = true</code>  | The installer logs are not sent to the host during auto upgrade.<br>This is the default value. |
| <code>install-vmxGuestLogDisabled = false</code> | The installer logs are sent to the host during auto upgrade.                                   |

**Note:** These settings go into the logging section. For example:

Under the [logging] group,

```
[logging]
install-vmxGuestLogDisabled = false
```

3. vMotion Impact:

- a) New Host to Old Host:

For VMware Tools 11.0.0 and later versions, before vMotion, logs went to host guest log. After vMotion, logs stopped going to the host.

For versions earlier to VMware Tools 11.0.0, before vMotion, logs went to guest %TEMP% folder only. After vMotion, logs go to guest %TEMP% folder only.

b) Old Host to New Host:

For VMware Tools 11.0.0 and later versions, before vMotion, logs went to guest %TEMP% folder only. After vMotion, logs go to guest %TEMP% folder only.

For versions earlier to VMware Tools 11.0.0, before vMotion, logs went to guest %TEMP% folder only. After vMotion, logs go to guest %TEMP% folder only.

**Note:** vSphere administrator can set the VM option to redirect to host guest log after vMotion.

## Installing and Automatically Upgrading VMware Tools Component

Guest administrator can control the automatic upgrade, installation or removal of a component using the configuration options provided in VMware Tools Configuration file (`tools.conf`).

1. **Automatic Upgrade:** The guest admin can control automatic upgrade using the `allow-upgrade` option.

The `allow-upgrade` option controls whether automatic upgrades (or re-installations) are allowed or not. This option has the values:

- `allow-upgrade=true`: Enables automatic upgrade of VMware Tools.  
This is the default value.
- `allow-upgrade=false`: Disables automatic upgrade of VMware Tools.

**Note:** The `allow-upgrade` option affects all the auto upgradable tools.

2. **Add or Remove a Feature:** The guest admin can control adding or removing a feature from VMware Tools using the following options:

- `allow-add-feature`: This option controls whether adding a feature from VMware Tools is allowed or not. This option has the values:
  - `allow-add-feature=true`: Enables adding a feature from VMware Tools.  
This is the default value.
  - `allow-add-feature=false`: Disables adding a feature from VMware Tools.
- `allow-remove-feature`: This option controls whether removing a feature from VMware Tools is allowed or not. This option has the values:
  - `allow-remove-feature=true`: Enables removing a feature from VMware Tools.  
This is the default value.
  - `allow-remove-feature=false`: Disables removing a feature from VMware Tools.

**Note:**

1. The `allow-add-feature` and `allow-remove-feature` options affect Windows tools only.
2. If the guest admin disables the automatic upgrade option (`allow-upgrade=false`), the feature modification options (`allow-add-feature` and `allow-remove-feature`) get disabled as well.

## Configuring VMware Tools Components

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.
- By editing the configuration file `tools.conf`

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 the KB article [2004018](#).

## Using VMware Tools Configuration File

VMware Tools uses a configuration file called `tools.conf` to configure different operations such as logging, upgrade, guest info, and so on.

### Configuration File Location

Administrators can configure VMware Tools by editing this `tools.conf` file.

For example: Right click **Start > All Programs > Accessories > Notepad** and select **Run as administrator**.

#### Note:

- If the configuration file does not exist, you can create it.
- The **Application Data** folder is hidden.
- The **Program Data** folder is hidden.
- There is no need to restart the tools service when the file is edited. The tools service will check this file every 5 seconds (by default) for changes and apply them.

The table provides the location of configuration file for various Guest OSs:

| Guest OS                                                 | Path                                                                                        |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Windows XP, Windows Server 2000, and Windows Server 2003 | C:\Documents and Settings\All Users<br>\Application Data\VMware\VMware Tools<br>\tools.conf |
| Windows Vista, Windows 7, and Windows Server 2008        | C:\ProgramData\VMware\VMware Tools<br>\tools.conf                                           |
| Linux, Solaris, and FreeBSD                              | /etc/vmware-tools/tools.conf                                                                |
| FreeBSD with open-vm-tools 10.1.x or later               | /usr/local/share/vmware-tools/tools.conf                                                    |
| Mac OS X                                                 | /Library/Application Support/VMware Tools/<br>tools.conf                                    |

### Example Configuration File

VMware Tools installs an example configuration file in the same directory as the location for `tools.conf`. This file lists the available options with possible values but commented out (with a leading '#' character), together with a description. If you want to change the options, uncomment them and copy this file to `tools.conf`, or copy parts of it into the `tools.conf` file.

## Configure Network Interface Information

You can configure Network Interface information using the `tools.conf` configuration option.

## 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

You can exclude specific file systems from a quiesced snapshot operation.

In Linux guest operating systems, the configuration setting `excludedFileSystems` allows file systems to be excluded from a quiesced snapshot. 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 `/`

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>
```

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 to Configure VMware Tools

You must ensure certain data security considerations while configuring VMware Tools as VMware Tools configuration settings might expose some security threats or risks.

There are many kind of possible security threats while configuring VMware Tools components or features.

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.

**Note:** 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: Unprivileged User Account Access

#### 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: 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: 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 Custom VMware Tools Scripts

You can associate custom VMware Tools 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 partially depends on the guest operating system.

#### Microsoft Windows Guest Operating Systems

For most of the Microsoft's Windows guest operating systems, the default script for suspending a virtual machine releases the IP address of the virtual machine. The default script for resuming a virtual machine renews the IP address of the virtual machine. This behavior affects only the 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 5: Default VMware Tools Scripts**

| Script Name                      | Description                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>poweroff-vm-default</code> | Runs when the virtual machine is being powered off or reset.<br>Has no effect on networking for the virtual machine.                                                                                                                                                                                                                            |
| <code>poweron-vm-default</code>  | Runs when the virtual machine is being powered on rather than resumed.<br>Also runs after virtual machine restarts.<br>Has no effect on networking for the virtual machine.                                                                                                                                                                     |
| <code>resume-vm-default</code>   | Runs when the virtual machine is resumed after it was suspended.<br>On Windows guest operating systems, if the virtual machine is configured to use DHCP, this script renews the IP address of the virtual machine.<br>On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, this script starts networking for the virtual machine. |
| <code>suspend-vm-default</code>  | Runs when the virtual machine is being suspended.<br>On Windows guest operating systems, if the virtual machine is configured to use DHCP, this script releases the IP address of the virtual machine.<br>On Linux, Mac OS X, Solaris, and FreeBSD, this script stops networking for the virtual machine.                                       |

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

## Custom VMware Tools Scripts for Windows

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

- Familiarize yourself with the default VMware Tools scripts. For more information, see [Default VMware Tools Scripts](#).
- If you plan to script commands and need to know the exit codes, see [Common Exit Codes](#).

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.

- 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                              |
|----------------------|-------------------------------------------------------|
| <code>suspend</code> | <code>@%SYSTEMROOT%\system32\ipconfig /release</code> |
| <code>resume</code>  | <code>@%SYSTEMROOT%\system32\ipconfig /renew</code>   |

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
```

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

## Custom VMware Tools Scripts for Multiple OSs Except Windows

For 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.

- Familiarize yourself with the default VMware Tools scripts. For more information, 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 [Common Exit Codes](#).

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.

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.

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

## Disable VMware Tools Script

The default scripts for suspending and resuming a virtual machine are interdependent. If you disable the script for one of these actions, you must also disable the script for the other action.

Log in as root on Linux, Solaris, and FreeBSD guest operating systems, to test, edit, or disable a script.

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

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-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.

## Using 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, 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 6: VMware Tools Configuration Utilities for Guest Operating Systems**

| Guest Operating System  | Utility                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows                 | VMwareToolboxCmd.exe                                                                                                                                                                   |
| Mac OS X                | vmware-tools-cli<br>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 vSphere 4.1 and later.

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

## Enable Periodic Time Synchronization

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

- 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 [Common Exit Codes](#).

**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.

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`.

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**.

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.

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.

## Disable Periodic 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.

Power off the virtual machine.

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.

Power on the virtual machine.

## Connect or Disconnect a Virtual Device

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

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

- 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.

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-namedevice statusdevice-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-namedevicedevice-namesubcommand
```

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

The device is connected or disconnected, as you specified.

## View Virtual Machine Status Information

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.

- Determine the status information to display. For more information, see [Display Status Information](#).

- If you plan to script commands and need to know the exit codes, see [Common Exit Codes](#).

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 <i>hosttime</i> or, <i>speed</i> , one of the subcommands available for virtual machines hosted in a vSphere environment. |

## Display Status Information

When a virtual machine is running on an ESX host, 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 7: Subcommands for the stat Command**

| Subcommand Name        | Description                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| <code>hosttime</code>  | Displays the date and time on the host.                                                                              |
| <code>speed</code>     | Displays the CPU speed, in MHz.                                                                                      |
| <code>balloon</code>   | Displays the amount of memory that is currently reclaimed from the virtual machine through ballooning, in megabytes. |
| <code>swap</code>      | Displays the current amount of memory swapped out to the virtual machine's swap file, in megabytes.                  |
| <code>memlimit</code>  | Displays memory limit information, in megabytes.                                                                     |
| <code>memres</code>    | Displays memory reservation information, in megabytes.                                                               |
| <code>cpures</code>    | Displays CPU reservation information, in MHz.                                                                        |
| <code>cpulimit</code>  | Displays CPU limit information, in MHz.                                                                              |
| <code>sessionid</code> | Displays the current session ID.                                                                                     |

**Table 8: Subcommands for the stat Command**

| Subcommand Name       | Description                             |
|-----------------------|-----------------------------------------|
| <code>hosttime</code> | Displays the date and time on the host. |
| <code>speed</code>    | Displays the CPU speed, in MHz.         |

## Common Exit Codes

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

The following table lists the common error codes defined in `toolbox-cmd`. Each subcommand may return other Windows or Linux error codes.

**Table 9: Exit Codes**

| Code Number | Applicable Command                                                               | Description                                                                                                                                                                                                                                                                                   |
|-------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0           | All commands                                                                     | The command was successful.                                                                                                                                                                                                                                                                   |
| 1           | All commands                                                                     | A error occurred.<br>For the <code>shrink</code> command, 1 indicates that although shrinking is enabled, the shrink command cannot be carried out.                                                                                                                                           |
| 64          | All commands                                                                     | The command-line argument is not valid (EX_USAGE).                                                                                                                                                                                                                                            |
| 69          | upgrade<br>timesync<br>config<br>device<br>stat<br>shrink                        | 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.<br>For the <code>stat</code> command, 69 indicates that the program could not communicate with the host (EX_UNAVAILABLE). |
| 70          | globalconf<br>gueststore                                                         | There is an internal software error (EX_SOFTWARE).                                                                                                                                                                                                                                            |
| 71          | Not used                                                                         | There is a system error (EX_OSERR).                                                                                                                                                                                                                                                           |
| 72          | device<br>shrink<br>script                                                       | A critical OS file is missing (EX_OSFILE).                                                                                                                                                                                                                                                    |
| 75          | upgrade<br>stat<br>shrink<br>script<br>config<br>globalconf<br>logging<br>device | The host does not support the query, perhaps because the host is not an ESX host (EX_TEMPFAIL).                                                                                                                                                                                               |
| 77          | script<br>disk<br>upgrade<br>globalconf<br>logging<br>info<br>config             | Permission error occurred (EX_NOPERM).                                                                                                                                                                                                                                                        |
| 130         | Shrink                                                                           | SIGINT received (VM_EX_INTERRUPT).                                                                                                                                                                                                                                                            |

## Query Information using GuestInfo Variable

You can use the 'guestinfo' variable to query information such as version description, version string, build number, and so on.

The following table list down the 'guestinfo' variables to query information:

Table 10: VMware Tools 'guestinfo' Variables

| Command                                                                                                                                                                                                                                                                                                                                                                       | Description                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Windows Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.vmtools.description"</code><br><code>rpctool.exe "info-get guestinfo.vmtools.description"</code><br><b>Linux Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.vmtools.description"</code><br><code>vmware-rpctool "info-get guestinfo.vmtools.description"</code>                                     | Reports the version description.                                                                                                                                                                                                                                                                                                          |
| <b>Windows Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.vmtools.versionString"</code><br><code>rpctool.exe "info-get guestinfo.vmtools.versionString"</code><br><b>Linux Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.vmtools.versionString"</code><br><code>vmware-rpctool "info-get guestinfo.vmtools.versionString"</code>                             | Reports the version string.                                                                                                                                                                                                                                                                                                               |
| <b>Windows Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.vmtools.versionNumber"</code><br><code>rpctool.exe "info-get guestinfo.vmtools.versionNumber"</code><br><b>Linux Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.vmtools.versionNumber"</code><br><code>vmware-rpctool "info-get guestinfo.vmtools.versionNumber"</code>                             | Reports the version number.                                                                                                                                                                                                                                                                                                               |
| <b>Windows Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.vmtools.buildNumber"</code><br><code>rpctool.exe "info-get guestinfo.vmtools.buildNumber"</code><br><b>Linux Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.vmtools.buildNumber"</code><br><code>vmware-rpctool "info-get guestinfo.vmtools.buildNumber"</code>                                     | Reports the build number.                                                                                                                                                                                                                                                                                                                 |
| <b>Windows Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.toolsInstallErrCode"</code><br><code>rpctool.exe "info-get guestinfo.toolsInstallErrCode"</code><br><b>Linux Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.toolsInstallErrCode"</code><br><code>vmware-rpctool "info-get guestinfo.toolsInstallErrCode"</code>                                     | Reports the error code of last VMware Tools installation.<br><br><b>Note:</b> VMware Tools installation and upgrade on Windows often require a reboot of the guest operating system for the changes to take effect. If a reboot is required but has not occurred, the <code>guestinfo.toolsInstallErrCode</code> variable is set to 3010. |
| <b>Windows Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.driver.[driver name].version"</code><br><code>rpctool.exe "info-get guestinfo.driver.[driver name].version"</code><br><b>Linux Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.driver.[driver name].version"</code><br><code>vmware-rpctool "info-get guestinfo.driver.[driver name].version"</code> | Reports the running version of the driver.<br>For example:<br><code>vmtoolsd --cmd "info-get guestinfo.driver.pvscsi.version"</code> returns 1.3.10.0                                                                                                                                                                                     |
| <b>Windows Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.ip"</code><br><code>rpctool.exe "info-get guestinfo.ip"</code><br><b>Linux Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.ip"</code>                                                                                                                                                                | Reports the IP address of Guest OS.                                                                                                                                                                                                                                                                                                       |

| Command                                                                                                                                                                                                                                                                                   | Description                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <code>vmware-rpctool "info-get guestinfo.ip"</code>                                                                                                                                                                                                                                       |                                                                           |
| <b>Windows Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.appInfo"</code><br><code>rpctool.exe "info-get guestinfo.appInfo"</code><br><b>Linux Guest:</b><br><code>vmtoolsd --cmd "info-get guestinfo.appInfo"</code><br><code>vmware-rpctool "info-get guestinfo.appInfo"</code> | Reports information about applications that are running inside the guest. |

For customized variables, you can use the command:

```
vmtoolsd --cmd "info-set guestinfo.foo bar"
```

## Configure appInfo

The appInfo plug-in collects information about applications running inside the guest and publishes that information to the management layers. appInfo is installed by default as a part of VMware Tools installation in a virtual machine (VM).

appInfo can be managed (enabled or disabled) at both VM and Host levels.

## Using the VMware Tools Configuration File at VM Level

The appInfo plug-in collects the information about running applications inside the guest and publishes the information to a guest variable. For each application running inside the guest, the name and version information is captured and published by the plug-in. This application information is collected by default.

1. **Retrieving the data:** The data collected by appInfo plug-in is retrieved as follows:

- From inside the guest

Linux guest

- `vmtoolsd --cmd "info-get guestinfo.appInfo"`
- `vmware-rpctool "info-get guestinfo.appInfo"`

Windows guest

- `rpctool.exe "info-get guestinfo.appInfo"`

2. **Changing the poll-interval:** The appInfo plug-in captures the information in every 30 minutes by default.

**Note:** The default value is changed to '6 hours' in VMware Tools 11.1.0.

Guest admin can configure this poll-interval at anytime as follows:

- Linux

```
vmware-toolbox-cmd config set appinfo poll-interval <new value in seconds>
```

- Windows

```
VMwareToolboxCmd.exe config set appinfo poll-interval <new value in seconds>
```

### 3. Disabling the appInfo plug-in: Guest admin can disable the appInfo plug-in as follows:

- Linux guest  

```
vmware-toolbox-cmd config set appinfo disabled true or
vmware-toolbox-cmd config set appinfo poll-interval 0
```
- Windows guest  

```
VMwareToolboxCmd.exe config set appinfo disabled true or
VMwareToolboxCmd.exe config set appinfo poll-interval 0
```

## Using the ESXCLI plug-in at the Host Level

In the ESXCLI, a plug-in is added under 'vm' namespace to enable or disable appinfo feature at the host level. By default, this feature is enabled at the ESX host.

Install ESX version 7.0 Update 1 or later.

This plug-in provides two command options at the host level:

- **get option:** Queries the configstore and returns the current state of the appinfo feature.  

```
esxcli vm appinfo get
```
- **set option:** Updates the configstore and instantly notifies all the running virtual machines that the feature state is modified.
  - Enabling the appinfo feature at host:  

```
esxcli vm appinfo set --enabled true
```

--enabled is a mandatory option for set command.  
Valid values for enabling the appinfo feature are: "1", "yes", "y", "true", "True", "t", "T"
  - Disabling the appinfo feature at host:  

```
esxcli vm appinfo set --enabled false
```

--enabled is a mandatory option for set command.  
Valid values for enabling the appinfo feature are: "0", "no", "n", "false", "False", "f", "F"

**Note:** This plug-in can also be invoked by:

1. Using a PowerCLI script to enable or disable the appinfo feature at the host, cluster, and datacenter levels. For details on its usage with examples, see the KB article [81033](#).
2. Using /bin/localcli utility on ESX host. However, /bin/localcli can only be invoked locally and cannot be invoked remotely.

## Configure ContainerInfo for Linux

The containerinfo plug-in gathers the list of running containers inside the Linux guest.

1. **Retrieving data:** For Linux guest, the data collected by containerinfo plug-in is retrieved as follows:

```
vmtoolsd --cmd "info-get guestinfo.vmttools.containerinfo"
```

2. **Changing poll-interval:** For Linux guest, the containerinfo plug-in captures information in every 6 hours by default. Guest admin can configure this poll-interval at anytime as follows:

```
vmware-toolbox-cmd config set containerinfo poll-interval <new value in seconds>
```

To revert the containerinfo poll-interval to default value, run the following command:

```
vmware-toolbox-cmd config remove containerinfo poll-interval
```

3. **Querying container information:** For Linux guest, the number of containers queried per namespace can be limited to a value as follows:

```
vmware-toolbox-cmd config set containerinfo max-containers <value>
```

The default value for max-containers is 100. The containerinfo plug-in will stop collecting information after it collects information from 100 containers.

4. **Communicate with docker daemon (docker-unix-socket):** The docker unix socket is used to communicate with the docker daemon. Default is `/var/run/docker.sock`

**Note:**

- This key is specific to docker users.
- The default value can be overridden using `vmware-toolbox-cmd`:  

```
vmware-toolbox-cmd config set docker-unix-socket <path of the socket>
```

5. **Communicate with containerd gRPC server (containerd-unix-socket):** The containerd unix socket is used to communicate with the containerd gRPC server. Default is `/run/containerd/containerd.sock`

- The default value can be overridden using `vmware-toolbox-cmd`:  

```
vmware-toolbox-cmd config set containerd-unix-socket <path of the socket>
```

6. **Disabling the containerinfo plug-in:**

To disable the containerinfo gather loop set the `poll-interval=0`

```
vmware-toolbox-cmd config set containerinfo poll-interval 0
```

## Configure Service Discovery

The Service Discovery plug-in connects with the vRealize Operations Manager product. This plug-in provides fabric admins with more information to better manage VMs at large scale. VMware Tools already collects some data from VMs, but it is not sufficient. This plug-in collects additional data and relays it to vRealize Operations Manager if the management feature is enabled. The plug-in is enabled by default and can be disabled at any time by the guest administrator inside the guest.

Ensure that 'vsock' driver is present or installed in windows guest successfully.

1. **Disabling the Service Discovery plug-in:** This plug-in can be disabled using one of the following approaches:

- Using the toolbox command utility, execute the following commands:
  - For Linux  

```
vmware-toolbox-cmd config set servicediscovery disabled true
```
  - For Windows  

```
VMwareToolboxCmd.exe config set servicediscovery disabled true
```
- Open `tools.conf` file and manually add the following section:  

```
[servicediscovery]
disabled = true
```

2. **Enabling the Service Discovery plug-in:** This plug-in can be enabled using one of the following approaches:

- Using the toolbox command utility, execute the following commands:
  - For Linux
 

```
vmware-toolbox-cmd config set servicediscovery disabled false
```
  - For Windows
 

```
VMwareToolboxCmd.exe config set servicediscovery disabled false
```
- Open tools.conf file and manually add the following section:
 

```
[servicediscovery]
disabled = false
```

## Configure VMware Time Provider for Windows

A new time provider plug-in vmwTimeProvider is provided for Microsoft Windows native time synchronization service 'W32Time' running inside vSphere VMs. The plug-in interacts with the precision clock virtual device to provide the underlying ESX host time, as an alternative to NTP and Active Directory-based time sources.

Ensure to add a precision clock virtual device to the VM before using the vmwTimeProvider plug-in.

**Note:** For information on how to add a precision clock virtual device to a VM, see the *vSphere Virtual Machine Administration*.

- Enable vmwTimeProvider plug-in:  
To add this plug-in, explicitly select the **VMware Time Provider** component in the VMware Tools installer setup during installation. By default, this component is deselected.
- Disable vmwTimeProvider plug-in:  
To remove this plug-in, modify the installation and deselect the **VMware Time Provider** component in the VMware Tools installer.

You can check the status of the plug-in post installation by running the following w32time command:

```
w32tm /query /status
```

## Using GuestStore

The GuestStore feature provides a simple and flexible mechanism to distribute VMware specific or custom content from a GuestStore repository to multiple guests simultaneously.

To use the GuestStore feature, virtual machines must meet the following requirements:

- Virtual machines must have Windows guest operating systems.
- Virtual machines must be running on vSphere 7.0 Update 2 and later versions.
- Virtual machines must be running VMware Tools 11.2.5 and later.
- The file that is distributed through GuestStore must be 512 MB or smaller.

For more information about configuring ESXi hosts for the GuestStore feature, see the [Distributing Content with GuestStore](#) section in the *vSphere Virtual Machine Administration* documentation.

## Get Resource Content

When the GuestStore repository has been configured on ESX host, resources from the GuestStore repository can be easily accessed using VMware Tools command line utility.

You can fetch a resource content from the GuestStore repository using the VMware Tools Toolbox command line utility.

```
"C:\Program Files\VMware\VMwareTools\VMwareToolboxCmd.exe" gueststore getcontent <resource path>
<output file>
```

```
/usr/bin/vmware-toolbox-cmd gueststore getcontent <resource path> <output file>
```

where, <resource path> is the path under the GuestStore repository datastore root URL.

For example:

```
"C:\Program Files\VMware\VMware Tools\VMwareToolboxCmd.exe" gueststore getcontent /vmware/apps/
vmtools/windows64/metadata.json C:\Temp\metadata.json
```

```
"C:\Program Files\VMware\VMware Tools\VMwareToolboxCmd.exe" gueststore getcontent /vmware/
configurations/vmtools/windows/tools.conf C:\Temp\tools.conf
```

Guest admin can use the following `tools.conf` settings to control access to the GuestStore repository.

```
[guestStore]
```

`disabled = false` (By default, access to the GuestStore repository is enabled when configured on the ESX host side)

`adminOnly = false` (By default, admin privilege is not required to access the GuestStore repository)

If `disabled = true`, then all guest access to the GuestStore repository is disabled including [VMware Tools GuestStore based upgrade](#) and [GlobalConf](#) features.

When GuestStore access is enabled (`disabled = false`), setting `adminOnly = true` restricts that only administrators or root users can get content from the GuestStore repository by running the following command:

- Windows

```
"C:\Program Files\VMware\VMwareTools\VMwareToolboxCmd.exe" gueststore getcontent <resource path>
<output file>
```

- Linux

```
/usr/bin/vmware-toolbox-cmd gueststore getcontent <resource path> <output file>
```

## Distribute VMware Tools Upgrade on Windows

You can perform VMware Tools upgrade for virtual machines from the GuestStore repository.

VMware provides VMware Tools content for download with each new release of VMware Tools. Starting with VMware Tools releases after 11.2.5, you can download the VMware Tools content from VMware website and extract it under the GuestStore repository path. Among all VMware Tools versions extracted in GuestStore repository, the latest version is selected by default for subsequent upgrades unless overridden by a setting in the VMware Tools configuration file.

By importing the VMware Tools content in the GuestStore repository, you can schedule an automated VMware Tools upgrade at the next reboot of the virtual machines. You can also trigger VMware Tools upgrade from GuestStore repository for particular virtual machines through vSphere UI or API.

**Note:** Triggering VMware Tools upgrade from GuestStore repository using VMware Tools Toolbox command line is not supported in this release.

GuestStore based VMware Tools upgrade is installed as part of VMware Tools installation. This feature generates notification to the logged-on user, if GuestStore repository has newer version of VMware Tools and if VMware Tools upgrade needs a system restart to complete the upgrade process.

There are multiple policies supported for GuestStore based VMware Tools upgrade. In `tools.conf` following setting can be used to configure the policy:

```
[guestStoreUpgrade]
```

```
policy>manual
```

where, "policy" can have one of the following values:

- `off`
  - Disables the GuestStore based VMware Tools upgrade in the guest.
- `manual`
  - This is the default policy. This policy allows vSphere administrators to trigger VMware Tools upgrade from GuestStore repository using vSphere UI or API.
  - If the virtual machine has VMware Tools upgrade policy configured to upgrade at powercycle (VMX setting `tools.upgrade.policy = "upgradeAtPowerCycle"`), the setting is applied when the GuestStore based VMware Tools upgrade feature is enabled. On first VMware Tools system service start after virtual machine powers on, VMware Tools system service queries the host side VMware Tools upgrade policy setting for the virtual machine. If the policy is set to upgrade at powercycle, a check for an upgrade of VMware Tools from the GuestStore repository is triggered automatically.

**Note:**

When GuestStore based VMware Tools upgrade is enabled, the VMware Tools bundled with VMware ESX host is not used including the VMware Tools images added to VMware ESX host through vSphere Update Manager (VUM).

- `powercycle`
  - Triggers VMware Tools upgrade from GuestStore repository right after guest OS boots up.
  - This policy also allows vSphere administrators to trigger VMware Tools upgrade from GuestStore repository using vSphere UI or API.

By default, GuestStore based VMware Tools upgrade picks the latest version of VMware Tools from GuestStore repository. This behavior can be overridden by specifying a VMware Tools version for "vmtools-version-key" setting. This setting defaults to "vmtools" which refers to the latest VMware Tools version in the GuestStore repository.

For example, following setting restricts VMware Tools upgrades from the GuestStore repository to version 11.2.5.

```
vmtools-version-key=vmtools-11.2.5
```

## Distribute VMware Tools Configuration at Scale

You can distribute VMware Tools configuration file across multiple virtual machines from the GuestStore repository.

The GlobalConf feature automatically updates VMware Tools configuration with the configuration available in the GuestStore repository. The GlobalConf feature is disabled by default. When enabled, it allows vSphere administrators to distribute global VMware Tools configuration across multiple virtual machines in the vSphere environment.

The GlobalConf feature relies on VMware Tools configuration being present in GuestStore repository. By default, VMware Tools configuration is fetched from GuestStore repository `"/vmware/configurations/vmtools/windows/tools.conf"` for Windows GOSes and `"/vmware/configurations/vmtools/linux/tools.conf"` for Linux GOSes, unless overridden by a setting in local VMware Tools configuration inside the guest. Before using this feature, the desired VMware Tools configuration should be added to GuestStore repository as the resource GlobalConf feature expects.

When the GlobalConf feature is enabled, VMware Tools system service periodically checks for `tools.conf` file in the GuestStore repository.

- If a `tools.conf` file is present, it is downloaded and applied locally at runtime. During this process, only the settings that are not specified in the local `tools.conf` file inside the guest are applied.
- If the `tools.conf` file is not available in the GuestStore repository, any previously downloaded configuration file will be deleted from the local file system in the guest.

The GlobalConf module in VMware Tools checks the GuestStore repository every 60 mins by default. Inside the virtual machine, the guest administrator can manually edit the `tools.conf` file to configure various settings related to the GlobalConf module.

GlobalConf feature has the following configuration settings:

[globalconf]

- `enabled=true`: Enables the module.
- `poll-interval=3600`: Interval value should be specified in seconds. Default value: 3600 seconds. Minimum Value: 1800 seconds.
- `resource=/path/to/tools/conf/in/gueststore`: Default value is `"/vmware/configurations/vmtools/windows/tools.conf"` for Windows GOSes and `"/vmware/configurations/vmtools/linux/tools.conf"` for Linux GOSes.

#### Note:

- The VMware Tools system service (vmsvc) must be restarted, if any of the above settings are updated in the local `tools.conf` file.
- Starting from VMware Tools 11.3.0 release, when GlobalConf related settings are modified in the `tools.conf` file, VMware Tools system service (vmsvc) does not need a restart.

You can use VMware Tools Toolbox command line utility to perform the following operations:

- Query the state of GlobalConf module.
  - Windows
 

```
VMwareToolboxCmd.exe globalconf status
```
  - Linux
 

```
vmware-toolbox-cmd globalconf status
```
- Enable the GlobalConf module.
  - Windows
 

```
VMwareToolboxCmd.exe globalconf enable
```
  - Linux
 

```
vmware-toolbox-cmd globalconf enable
```
- Disable the GlobalConf module.
  - Windows
 

```
VMwareToolboxCmd.exe globalconf disable
```
  - Linux
 

```
vmware-toolbox-cmd globalconf disable
```
- Trigger an immediate update of VMware Tools configuration from the GuestStore repository without waiting for polling interval.
  - Windows
 

```
VMwareToolboxCmd.exe globalconf refresh
```
  - Linux
 

```
vmware-toolbox-cmd globalconf refresh
```

**Note:** You can use the `globalconf enable` or `globalconf disable` commands instead of editing `tools.conf` for enabling or disabling GlobalConf feature.

## Uninstalling VMware Tools

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

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

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 have 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](#).

1. Select a method to uninstall VMware Tools.

| Operating System                                | Action                                                                                                                                                    |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows 7, 8, 8.1, or Windows 10, or Windows 11 | In the guest operating system, start the Control Panel applet, and select <b>Programs and Features</b> . Select VMware Tools and click <b>Uninstall</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 <code>vmware-uninstall-tools.pl</code> 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> .                                      |
| Windows on ARM                                  | In the guest operating system, start the Control Panel applet, and select <b>Programs and Features</b> . Select VMware Tools and click <b>Uninstall</b> . |
| Windows Server 2008 R2 and later                | In the guest operating system, start the Control Panel applet, and select <b>Programs and Features</b> . Select VMware Tools and click <b>Uninstall</b> . |

2. Restart the guest operation system.

Reinstall VMware Tools.

## Configuring Customer Experience Improvement Program

You can participate in the Customer Experience Improvement Program (CEIP) to provide anonymous feedback or information to VMware for quality, reliability, and functionality improvements of VMware products and services.

### VMware Customer Experience Improvement Program

VMware Tools 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 <https://www.broadcom.com/company/legal/privacy/data-usage-programs/ceip-products>.

### Join or Leave Customer Experience Improvement Program in vSphere Client

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

Obtain the user name and password of the administrator account.

1. From the vSphere Client login page, log in to vCenter by using the credentials of the administrator account.
2. On the vSphere Client home page, click **Administration**.
3. Under Deployment, click **Customer Experience Improvement Program**
4. Click **Join** to join the CEIP or **Leave CEIP** to leave the Program.

## VMware Tools Install and Upgrade Issues

This topic covers issues related to VMware Tools install and upgrade process.

## Install or Upgrade 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.

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.

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 require 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.
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.toolsInstallErrCode=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

When you perform a VMware Tools upgrade, the VMware Tools components are upgraded and new features are added. If some features do not work correctly after an upgrade, you must change or repair the components. For operating systems other than Windows and Linux, you must manually start the VMware User process after an upgrade.

### Repair VMware Tools Components in Windows Virtual Machine

You need to repair or modify the installed VMware Tools Components, if you have problems with enhanced graphics display, mouse actions, or with features that depend on VMware Tools.

Some new VMware Tools Components are not installed during a VMware Tools upgrade by default. You can manually install these by modifying the installed VMware Tools Components.

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

### Start VMware User Process Manually

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 re-login. You can start the VMware user process by running the `vmtoolsd -n vmusr` command. The startup command can be modified based 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.
- 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.                                                               |

## VMware Tools FAQs

This topic provides frequently asked questions about VMware Tools.

- **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 [Broadcom Tools Operating System Specific Packages \(OSPs\)](#). For a list of supported guest operating systems, see the [Broadcom 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 the KB article [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, and later releases
- 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.

## Published Windows Drivers

VMware Tools drivers published to Windows Update.

### VMware Tools Drivers Published to Windows Update

This article provides information about the VMware Tools Windows drivers published to Windows Update. The information provided includes the latest driver version that is available for each supported Windows Operating System version. For supported Windows Operating System versions, running Windows Update will install or upgrade to the latest versions of these drivers, regardless of the VMware Tools version installed.

VMware Tools ships the newest versions of these drivers with each release. To determine the drivers' version shipped with the most recent, or a particular release of VMware Tools, please check the release notes in the *VMware Tools Documentation*.

#### Drivers on Windows Update

The Windows drivers below are available through Windows Update.

##### Note:

✓ The driver for the specified OS is published to Windows Update.

✗ The driver for the specified OS is not published to Windows Update.

#### In Windows Server

| Driver  | Version     | Windows Server 2025 | Windows Server 2022 | Windows Server 2019 | Windows Server 2016 | Windows Server 2012 R2 | Windows Server 2012 |
|---------|-------------|---------------------|---------------------|---------------------|---------------------|------------------------|---------------------|
| WDDM    | 9.17.09.004 | ✗                   | ✗                   | ✗                   | ✗                   | ✗                      | ✗                   |
| vmci    | 9.8.30.0    | ✓                   | ✓                   | ✓                   | ✓                   | ✓                      | ✓                   |
| vmxnet3 | 1.9.20.0    | ✓                   | ✓                   | ✓                   | ✓                   | ✓                      | ✓                   |
| pvscsi  | 1.3.29.0    | ✓                   | ✓                   | ✓                   | ✓                   | ✓                      | ✓                   |

#### In Windows Client

| Driver  | Version     | Windows 11 (64-bit) | Windows 10 (64-bit) |
|---------|-------------|---------------------|---------------------|
| WDDM    | 9.17.09.004 | ✓                   | ✓                   |
| vmci    | 9.8.30.0    | ✓                   | ✓                   |
| vmxnet3 | 1.9.20.0    | ✓                   | ✓                   |

| Driver | Version  | Windows 11 (64-bit) | Windows 10 (64-bit) |
|--------|----------|---------------------|---------------------|
| pvscsi | 1.3.29.0 | ✓                   | ✓                   |

### Discontinued-Publish OS

| Driver  | Version  | Windows Server 2008 R2 | Windows 7 |        | Windows 8 |        | Windows 8.1 |        |
|---------|----------|------------------------|-----------|--------|-----------|--------|-------------|--------|
|         |          |                        | 32-bit    | 64-bit | 32-bit    | 64-bit | 32-bit      | 64-bit |
| vmci    | 9.8.16.0 | ✓                      | ✓         | ✓      | ✗         | ✗      | ✗           | ✗      |
|         | 9.8.18.0 | ✗                      | ✗         | ✗      | ✓         | ✓      | ✓           | ✓      |
| vmxnet3 | 1.9.2.0  | ✓                      | ✓         | ✓      | ✗         | ✗      | ✗           | ✗      |
|         | 1.9.5.0  | ✗                      | ✗         | ✗      | ✓         | ✓      | ✓           | ✓      |
| pvscsi  | 1.3.15.0 | ✓                      | ✓         | ✓      | ✗         | ✗      | ✗           | ✗      |
|         | 1.3.17.0 | ✗                      | ✗         | ✗      | ✓         | ✓      | ✓           | ✓      |

### Known Issues

1. Broadcom removes previous drivers from Windows Update, but due to a Microsoft Portal issue, a search of the [Microsoft Update Catalog](#) for VMware Drivers will list those drivers. However, they are not available for download. This is expected.
2. Broadcom will publish the latest driver to Windows Update with each release, but due to the [Microsoft Gradual Rollout](#), the driver will not appear in search results until the gradual rollout is complete. Due to the limited release period, a Windows VM may have a delay before receiving the driver update.

**Disclaimer:** Broadcom is not responsible for the reliability of any data, opinions, advice, or statements made on third-party websites. Inclusion of such links does not imply that Broadcom endorses, recommends, or accepts any responsibility for the content of such sites.

## Documentation Legal Notice

---

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2025 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

