



VFC Frequently Asked Questions

Contents

What does VFC do? Why is it special?	3
Where can I find VFC pricing, offers, renewals and expiry dates?	3
How do I get technical support for VFC?	3
What platforms does VFC support and what does it require?	4
How do I use VFC?	4
Do I need a forensic write blocker?	4
What limitations does VFC have?	4
Will booting an image using VFC alter the original evidence?	4
Does VFC support 'partition only' images?.....	5
Does VFC support multi-boot systems?.....	5
How can I download the latest VFC?	5
I'm using VFC v4 and cannot download updates (404 error). How do I download new software?	6
How do I update my VFC license/dongle?	6
VFC License Manager reports "No license available". How can I fix it?	7
My dongle doesn't work. What are the troubleshooting steps?.....	8
Can VFC be used in a Virtualised / Terminal environment?	11
What is VFC Mount? Which other mount tools does VFC support?	11
What guest operating systems does VFC work with?.....	12
How do I fix VM fails to start and reports "Physical drive already in use" (PDIU) error?.....	13
Which virtualisation platforms is VFC compatible with?	14
What disk image formats does VFC support?	14
Can VFC virus check the VM?.....	15
How can I copy file(s) from the VM to my host machine?	15
Does VFC create a log that can be used for case/audit purposes?	15
Does VFC record screenshots from the VM?.....	15
How can I bypass a Windows password with VFC?	16
What is the PWB5.BIN file and how do I update it?	17
Which guest operating systems does VFC currently support?	17
Can VFC be used with BitLocker / encrypted forensic images?.....	18
The Generic Password Reset (GPR) user interface does not appear. How can I fix it?	19
How do I fix "Could not find VMware installation"?.....	20
How do I fix "Unable to load VMWare VDDK library"?	20
How do I fix "Unable to validate VFC v5 License"?.....	21



How do I fix “License system reports no license available?” 21

How do I fix License Manager hangs or reports “Internal date error”? 21

How do I fix “No license found”? 22

How do I fix License Manager error “Unexpected license data” or “Failed to download license information”? 22

How do I fix “Unable to start: VMware unsupported”? 22

The guest OS fails to boot (BSOD). What can I do? 23

The guest OS reports that new hardware has been found. Do I need to install drivers and reboot? . 23

How can I improve the performance of a new virtual machine? 23

Can I access the Internet from the virtual machine? 23

Can I transfer data between the New Virtual Machine and my own System? 24

Why does the New Virtual Machine need to be activated? 24

Is VFC compatible with Windows 10 “Creators” Update? 24

How can I fix Windows compatibility assistant prevents VMware from running? 25

Windows NT5 SP0-SP5 fail to boot after virtualisation. How can I fix it? 26

How do I fix error “Could not load/unload registry” 26

How can I fix “Operating System not found” error? 27

How I fix “Unable to open kernel device” error? 28

How do I fix the guest operating system " is not supported error? 29

 system “ is not supported 29

How do I resolve VMware asks to Take Ownership of the VM? 30

What is the Generic Password Reset (GPR) feature and how do I use it? 30

© MD5 Ltd 2007-2020. VFC and the VFC logo are registered trademarks of MD5 Ltd. All other product names, trademarks and registered trademarks are the property of their respective owners.



What does VFC do? Why is it special?

VFC is used by digital forensic investigators to create a virtual copy of a suspect computer. The process is forensically safe and does not modify any original evidential data. This procedure allows the investigator to experience the original desktop environment just like the original user. This puts the investigator “in the room” with the suspect, providing invaluable access to software and data that cannot be easily found with a typical “dead box” examination.

In some cases, an experienced investigator could manually perform some of the processes performed by VFC. However, this would be time-consuming and error-prone. VFC automates the process and applies almost 15 years of acquired knowledge to fix numerous known issues and quickly produce a compatible and stable virtual machine in seconds. VFC removes the guesswork from virtualisation and allows the investigator to concentrate on the investigation.

Where can I find VFC pricing, offers, renewals and expiry dates?

Please contact your VFC account manager or authorised reseller for this information. If you cannot find the information required, please contact VFC Technical Support (see below).

How do I get technical support for VFC?

A variety of resources are available to support VFC. Please see the following:

1. The VFC FAQ (this document)
2. The VFC Installation Guide
3. The VFC User Guide
4. The VFC support website: <https://vfc.uk.com/support>

If you cannot find an answer to your question from the above, please use the support website to request assistance.

When contacting technical support, please provide as much information as possible. This will allow us to offer the best advice:

1. Your name/organisation
2. Dongle ID (printed on the side of the dongle)
3. Preferred contact phone number or email address
4. Product revision: VFC v3, v4, v5 or other
5. Brief description of problem/question
6. If applicable, a copy of the VFC log file

What platforms does VFC support and what does it require?

VFC is supported on Windows 7 SP1 and later. It is available as both a 32-bit and a 64-bit application. The 64-bit version is recommended. VFC also requires VMware Player/Workstation v12 or later and a compatible forensic image “mount” tool. VFC is provided with the VFC Mount tool and is also compatible with several common third-party imaging mounting utilities.

How do I use VFC?

VFC supports a variety of different workflows and configurations. The basic process is very quick and simple:

- Mount the evidence file (or attach the [write-blocked] physical disk)
- Select the disk and then the relevant partition
- Generate the machine and launch it with VMware

Do I need a forensic write blocker?

VFC is typically used with a forensic “image” that has been previously created from a real disk. The use of images is a standard industry practice that ensures the continuity of evidence and avoids the possibility of damaging or contaminating original evidence. VFC can also be used with a physical disk drive. However, in this case, we would strongly recommend that it is connected via a forensic “write blocker” to ensure that no changes are made to the original material.

What limitations does VFC have?

VFC is expected to successfully boot over 95% of Windows-based disks / images that it is presented with. VFC cannot dynamically fix machines that are 'broken' and unable to be booted in the original machine. Similarly, VFC cannot bypass software protection that is linked/licensed to the original hardware, or workaround full disk encryption without the encryption key.

Will booting an image using VFC alter the original evidence?

VFC creates a temporary disk cache and directs all subsequent reads and writes ‘through’ this cache. This emulates normal read/write behaviour and allows the guest operating system and installed software to function as normal. This process is forensically safe and no changes are made to the original image files. We recommend using a forensic “write blocker” when using physical disk drives to avoid making inadvertent changes to the disk whilst it is connected to the forensic workstation.



Does VFC support 'partition only' images?

No. VFC requires a full disk image. A variation of this feature was available in previous versions of VFC but was removed because it had several limitations.

Does VFC support multi-boot systems?

Yes, multi-boot systems will generally work. In some cases, for instance, if one OS requires legacy BIOS start-up and another uses EFI based start-up it may be necessary to create two distinct virtual machines using VFC. This is necessary because VMware can emulate either BIOS or EFI but not both at the same time. This is a minor limitation of VMware and not VFC.

How can I download the latest VFC?

The VFC website has a download page here: <https://vfc.uk.com/downloads>

Some downloads are publically available. However, the majority of downloads require an active license (dongle). There are three ways to access these restricted downloads:

Accessing downloads directly from within VFC

VFC provides direct access to the software downloads page. If VFC is already installed, proceed as follows:

1. Ensure your dongle is connected
2. Start VFC
3. Click the About Tab
4. Click Download VFC
5. Scroll to the bottom of the page and select the desired download

Accessing downloads from VFC License Manager

If VFC is not already installed, you can access the downloads page using VFC License Manager. This software is installed alongside VFC and is also available as a public download from the website. To use VFC License Manager proceed as follows:

1. Open the VFC download page in your browser: <https://vfc.uk.com/downloads>
2. Scroll to the bottom
3. Select VFC License Manager and download
4. Ensure your dongle is connected
5. Start VFC License Manager
6. Click Query Dongle and allow your dongle to be detected (if this fails, see FAQ)
7. Click Download VFC
8. Scroll to the bottom of the page and click the desired download

Offline access to VFC downloads

In some cases, it may not be possible to download VFC from the computer that has the VFC dongle connected. In this case, please contact VFC Technical support for a time-limited offline download link.

I'm using VFC v4 and cannot download updates (404 error). How do I download new software?

To improve the user experience, the VFC license system was re-designed when VFC v5 was released. To access the downloads, please visit the following web page: <https://vfc.uk.com/downloads> and download the latest VFC License Manager tool. This can be used to upgrade your dongle and access restricted downloads including older versions of VFC.

How do I update my VFC license/dongle?

An active license is required to use VFC. The license is stored in a hardware "dongle". This connects to your computer via the USB port. Two types of dongle have been released:

1. Green dongle – This requires a software driver to function. Please see the FAQ for instructions on how to install the driver.
2. White/Blue dongles – These do not require a software driver to function.



The dongle is typically supplied pre-programmed with your VFC license. To update the license please use the VFC License Manager tool. This software is supplied with VFC and is also available from the VFC website. There are two ways to update the dongle:

Online dongle update with VFC License Manager

On a computer with internet access, the VFC License Manager tool can automatically download your current license and program the dongle. To update the dongle using this method proceed as follows:

1. Ensure your dongle is connected
2. Start VFC License Manager
3. Click Query Dongle and allow your dongle to be detected (if this fails, see FAQ)
4. Click Check Online
5. Confirm the license details are as expected
6. Click Update Dongle
7. Restart VFC

Offline dongle update with VFC License Manager / PID key

In some cases, it may not be possible to access the internet from the computer that has the VFC dongle connected. In this case, please contact Technical Support for an offline PID key. Each PID key is unique and can only be used with a specific dongle. To update the dongle using this method proceed as follows:

1. Acquire a VFC PID key
2. Ensure your dongle is connected
3. Start VFC License Manager
4. Click Query Dongle and allow your dongle to be detected (if this fails, see FAQ)
5. Click ...
6. Enter the PID key and click OK
7. Confirm the license details are as expected
8. Click Update Dongle
9. Restart VFC

VFC License Manager reports “No license available”. How can I fix it?

There are two reasons why VFC License Manager may report that no license is available:

1. The computer does not have online access. Try visiting the website <https://www.vfc.uk.com>. If this website is not accessible then VFC License Manager cannot be used in online mode. Recent versions of VFC License Manager have been updated to support proxy servers. If you use a proxy server, please manually download the latest VFC License Manager and try again.
2. The dongle was programmed before the release of VFC v5 and has not subsequently been updated with a v5 license. In this case, the VFC License Manager tool will report “VFC4 [Legacy]” when you click the Query Dongle button. Please contact your Sales Manager / authorised reseller to arrange a new license and then try again.



My dongle doesn't work. What are the troubleshooting steps?

The VFC license is stored in a hardware “dongle”. This connects to your computer via the USB port. Two types of dongle have been released:

1. Green dongle – This requires a software driver to function. Please see the FAQ for instructions on how to install the driver.
2. White/Blue dongles – These do not require a software driver to function.

Installing the dongle driver (green dongle only)

The dongle driver is included in the VFC software distribution. To install the driver proceed as follows:

1. Install VFC in the usual way
2. Ensure the dongle is **not** connected
3. Open the folder containing VFC. This is typically one of the following:

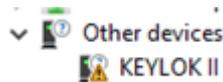
c:\Program Files\MD5 Ltd\VFC5
c:\Program Files (x86)\MD5 Ltd\VFC5

4. Double click on “VFC Dongle Driver Install.exe”
5. Select “KEYLOK2 (USB w/Driver)”
6. Select Standalone
7. Click Begin Install
8. Click Next
9. If prompted, click Install to confirm the driver installation
10. Click Finish
11. Insert the dongle
12. Start VFC License Manager
13. Click Query Dongle to confirm the dongle is now detected

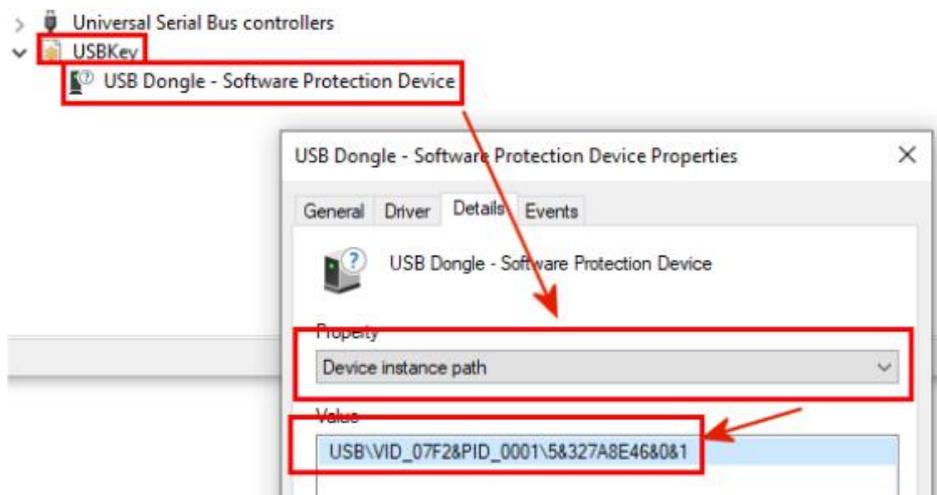
Troubleshooting green dongle

The following steps describe how to troubleshoot a green dongle that is not detected by VFC License Manager:

1. Confirm that the USB port is functional by inserting another USB device (e.g. memory stick)
2. Confirm the dongle is not damaged and is firmly connected to the USB port
3. Remove and then re-insert the dongle
4. Open Windows Device Manager
5. If the driver is not installed, the device is reported in the “Other devices” category as shown below. In this case, please see above for driver installation instructions:



6. If the driver is installed, try removing and then re-inserting the dongle
7. Check Windows Device Manager again
8. The dongle should be listed under the USBKey category as similar to below:

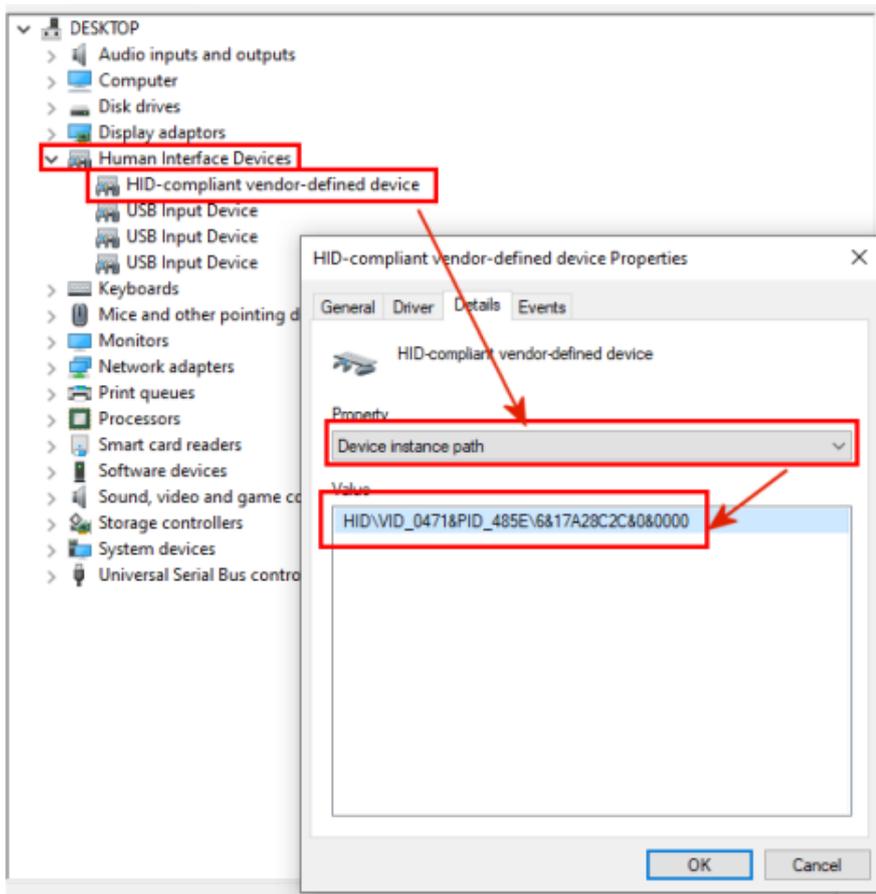


9. If the dongle still fails to work, this may be due to a problem with either with the PC or the dongle. Please try the dongle on another PC
10. Finally, please contact VFC Technical Support to arrange a replacement dongle

Troubleshooting white/blue dongle

The following steps describe how to troubleshoot a white/blue dongle that is not detected by VFC License Manager:

1. Confirm that the USB port is functional by inserting another USB device (e.g. memory stick)
2. Confirm the dongle is not damaged and is firmly connected to the USB port
3. Remove the dongle
4. Opening Device Manager and expand the HID category
5. Re-insert the dongle
6. Wait a few seconds and see if additional “HID-complaint” device appears (there may already be others present for keyboard, mice and other dongles). The result should be similar to the screenshot below:



11. If the dongle still fails to work, this may be due to a problem with either with the PC or the dongle. Please try the dongle on another PC
12. Finally, please contact VFC Technical Support to arrange a replacement dongle

Can VFC be used in a Virtualised / Terminal environment?

Subject to the limitations below, VFC itself can run in a virtualised or terminal (remote desktop) environment. There are two limitations to be aware of:

- a. VFC requires a hardware dongle to function. It must be possible to “connect” the hardware dongle to VFC. We do not currently support this scenario but are aware that it has been successfully used with some environments that support such USB device redirection. It is more likely to work with the white/blue (non-driver) VFC dongle.
- b. VMware is a hypervisor and requires direct access to the hardware. It cannot typically be used alongside other hypervisors (such as Hyper-V). This may mean that whilst you can create a VM using VFC in such an environment, it may not be possible to launch that VM.

What is VFC Mount? Which other mount tools does VFC support?

VFC requires a data source to create a virtual machine from. This is typically provided by a forensic disk image (.e01 file or similar) or a physical disk connected by a forensic “write blocker”. The forensic disk image must be “mounted” to make it visible to both VFC and later VMware. VFC v5 is supplied with the VFC Mount tool. This has been designed specifically for use with VFC and optimised to avoid common compatibility problems with VMware. The tool supports read-only mount of the following disk image formats:

- .e01
- .ex01
- .aff4
- .vmdk
- Raw / spanned image e.g. .dd, .img, .bin, .raw, .001 etc

VFC is also compatible with other third-party mount tools. These may be used to mount other image formats not supported by VFC Mount. The following have been used successfully:

- Mount Image Pro v5/6
- FTK Imager v4.x
- OSF Mount v3
- Guidance Software Encase PDE (Physical Disk Emulator)
- Arsenal Imager Mount (AIM) v3.x

We recommend you use VFC Mount in the first instance as this contains a specific feature to improve compatibility with VMware and to avoid the common “Physical drive already in use” that may be encountered with other tools.

VFC provides easy access to common mount tools using the icons that are located at the bottom left of the VFC application. Depending on the installed mount tools, the following items may be displayed:





To launch VFC Mount and mount a forensic image proceed as follows:

- a. Click the VFC Mount icon (left-most icon)
- b. Confirm “Disable automatic file system mounting” is checked
- c. Click Mount
- d. Select the desired forensic disk image
- e. Wait for the image to mount (this may take a few seconds)
- f. Click the Disk icon in VFC and select the desired drive

Tips:

1. Larger emulated disks can take a few seconds to mount. If the drive is not yet visible in VFC, close the mount dialog, wait a few seconds and then re-open it
2. VFC Mount continues to run even when VFC has been closed. This behaviour is essential because the emulated physical drive created by VFC Mount must remain available whilst the associated virtual machine is open in VMware. To access VFC Mount again click the disk item in the notification area (system tray)

What guest operating systems does VFC work with?

VFC has been used to successfully virtualise the following:

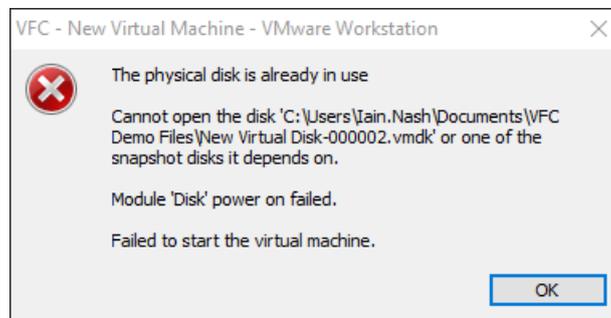
- Windows 3.1
- Windows 95/98/ME
- Windows NT 4
- Windows 2000
- Windows XP (x86 & x64)
- Windows Vista (x86 & x64)
- Windows 7 (x86 & x64)
- Windows 8 (x86 & x64)
- Windows 8.1 (x86 & x64)
- Windows 10 (x86 & x64)
- Windows Server (x86 & x64)
- Windows Server 2008 (x86 & x64)
- Windows Server 2012 x64
- Windows Server 2012 R2 x64
- Windows Server 2016 x64
- Windows Server 2019 x64
- Linux (experimental)
- MAC OS X (10.5 and above) (experimental)
- Sun Solaris (experimental)

How do I fix VM fails to start and reports “Physical drive already in use” (PDIU) error?

VFC can be used in a variety of ways. The typical scenario is:

1. Mount forensic image using compatible mount tool. This creates an emulated physical disk
2. Select desired settings and build VM
3. Launch VM with VMware

In some cases, the host Windows operating system can attempt to mount the emulated physical disk and then lock it. This prevents VMware from acquiring exclusive access to the disk and can result in the VMware error message “Physical drive already in use” when the VM is started:



Tip: We recommend using VFC Mount as the preferred mount tool because it contains features which have been specifically designed to minimise this problem and improve compatibility with VMware. This feature may not be available in third-party mount tools.

To resolve this problem please proceed as follows:

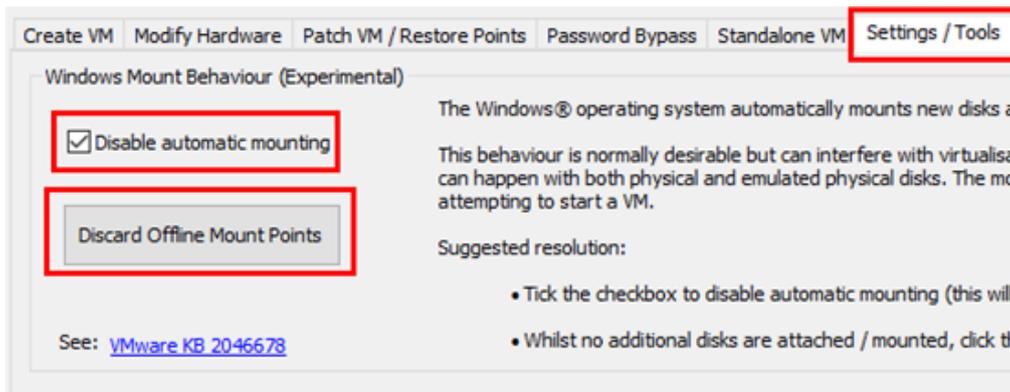
1. Unmount any existing images, close your mount tool and close VFC

NB: You can quit VFC Mount by right-clicking on the notification area icon and selecting “Exit”. Alternatively, reboot your machine.

2. Re-start VFC and navigate to the Settings/Tools tab
3. Tick the “Disable automatic mounting” checkbox. This disables the default Windows behaviour.

NB: It will also mean that future drives mounted on your system are not automatically assigned drive letters. You can assign them manually via the Windows Disk Manager tool

4. Click the “Discard Offline Mount Points” button and follow the on-screen instructions. This discards the Windows history of previously mounted disk/drive letter assignments. It ensures that any images previously mounted on the system are forgotten and will not auto-mount again in the future.



5. Start VFC Mount. This has the same checkbox and it should already be ticked:



Tip: Occasionally, Windows can lock a disk and refuse to release it. If this happens (including with VFC Mount) try rebooting the host system. This will resolve the problem in most cases. The following article from VMware provides more technical information on the issue:

<https://kb.vmware.com/s/article/2046678>

Which virtualisation platforms is VFC compatible with?

VFC supports the VMware platform. Extensive testing has found this to be the most capable, flexible and reliable tool. VFC can be used with either VMware Workstation or VMware Player v12 or later.

What disk image formats does VFC support?

VFC requires a full disk image. The following image formats are currently supported by the built-in VFC Mount tool:

- .e01
- .ex01
- .aff4
- .vmdk
- .vhd (from v5.1)
- Raw / spanned "dd" image

In addition, VFC can also be used with third-party mount tools and physical disks connected via a forensic write blocker. VFC does not currently support single volume (e.g. file system) images. This is because they do not contain the necessary boot loader (MBR) or system partition (GPT) to start the operating system.

Can VFC virus check the VM?

VFC does not have a built-in AV capability. However, you can virus check a mounted forensic image as follows:

1. Mount the forensic image using VFC Mount (or similar)
2. If necessary, use Windows Disk Manager to allocate the target partition a drive letter
3. Perform an AV scan in the usual way

Warning: Making a mounted image accessible to the host OS in this way may potentially expose that host computer to malware present in the disk image. Please take care not to execute any software (or directly open documents) from the forensic image without taking appropriate security precautions.

How can I copy file(s) from the VM to my host machine?

To copy files from the guest to the host computer, please proceed as follows:

1. Mount the forensic image using VFC Mount (or similar)
2. If necessary, use Windows Disk Manager to allocate the target partition a drive letter
3. Browse the drive and copy files as normal

Warning: Making a mounted image accessible to the host OS in this way may potentially expose that host computer to malware present in the disk image. Please take care not to execute any software (or directly open documents) from the forensic image without taking appropriate security precautions.

Does VFC create a log that can be used for case/audit purposes?

Yes, the VFC log file is located in the same folder as the VFC software. You can open the log directly from within VFC by clicking the View Log button and optionally save a copy of the log to an alternative location.

Does VFC record screenshots from the VM?

No, this feature is not currently available. VFC is principally designed to create a working and stable virtual machine. A variety of third-party software is available that can take screenshots/video from the VM.



How can I bypass a Windows password with VFC?

VFC includes two different mechanisms to bypass words on Windows-based systems:

Generic Password Reset Tool (GPR)

The GPR feature injects a VFC component directly into the VM. This feature is enabled by default for Windows guest systems and may be configured via the VFC Options dialog (the “cog” icon). When the VM starts, the GPR tool will display a user interface allowing specific account passwords to be reset. Password changes using GPR remain for the lifecycle of the VM.

Password Bypass (PWB) feature

The PWB feature may be used to temporarily disable the password feature of supported Windows guest systems. This may be beneficial in some circumstances because it does not make a permanent change to the VM and the password bypass is removed the next time the VM is rebooted. To use the PWB feature proceed as follows:

1. Boot the Windows-based VM
2. Enter (any) password into the password dialog
3. Suspend the VM
4. Open VFC
5. Open the Password Bypass tab
6. Click Select VM and locate the VM folder
7. Click Apply PWB
8. Click Resume VM
9. Log in using any password

In some cases, the PWB feature may fail to recognise the specific edition/revision of the guest operating system. In this case, please try the “Use fuzzy search logic” option available in the PWB tab. If this fails, please follow the on-screen prompts to generate a support file to send to VFC Technical Support. This contains relevant system files from the guest operating system which can be analysed to generate a new PWB procedure. No user identifiable information is exported by this process.

What is the PWB5.BIN file and how do I update it?

The PWB5.BIN file contains the password bypass definitions used by VFC v4.50 and later. This is periodically updated to support new editions/revisions of Microsoft Windows. A definition file is supplied with VFC and the latest definition file can be downloaded from the VFC website (active license required). To install a new definition file proceed as follows:

1. Extract the PWB5.ZIP file from the website. This will contain a PWB5.BIN file
2. Close VFC
3. Navigate to the VFC installation folder
4. Rename the PWB5.BIN file to PWB5.OLD
5. Copy the new file to the folder and restart VFC

The status of the current PWB definition file is shown at the bottom of the VFC PWB tab. For instance:

```
Using PWB definition file 'C:\Program Files\MD5 Ltd\VFC5\PWB5.BIN' created 20200123 095257 [315]
```

Which guest operating systems does VFC currently support?

VFC v5 can be used with the following guest operating systems:

- Windows NT4 and later (both 32-bit and 64-bit)
- Linux v2 and later (both 32-bit and 64-bit)
- Sun Solaris v6 and later
- Other PC / UEFI based operating systems

Please note that in all cases the user of VFC is responsible for confirming that they are correctly licensed or have other legal authority to use the guest operating system, associated software and VMware platform.



Can VFC be used with BitLocker / encrypted forensic images?

VFC uses full disk images. Such images can easily be created from encrypted drives (such as those produced by BitLocker). However, encrypted images can be a challenge for tools such as VFC because the encryption prevents the software from manipulating the image to create a compatible and stable virtual machine. There are two ways to work around this. Both methods require the recovery key. Please try one of the following:

1. Use the recovery key to create a decrypted image. Use this image with VFC. Under this approach, all VFC features are available from the start.
2. Use the encrypted image directly with VFC and select the appropriate mass storage type from the Options (cog) dialog. The selected storage type should match that present on the original hardware. For most desktop/laptop systems, this will currently be the SATA option. When prompted, enter the recovery key.

Tip: This technique is analogous to the original hard disk being moved to different PC hardware. Once the VM has started, consider decrypting the image to remove the prompt on subsequent start-ups. When the image is decrypted, consider running the VFC/RPF tab to patch the VM for known issues. This will increase VM compatibility with VMware and should result in a more stable and faster user experience. The downside of this approach is that until the VFC/RPF feature has been used, the VM may be slower and sometimes less stable than a standard VM conversion using VFC.



The Generic Password Reset (GPR) user interface does not appear. How can I fix it?

The VFC Generic Password Reset (GPR) tool provides a convenient means to reset Windows user passwords, convert Windows “Live” accounts to local accounts and start a system-level (root) command prompt. The tool is a small VFC component that is injected into Windows-based virtual machines when they are created. If necessary, this feature can be disabled using the Options dialog.

Typically, the GPR user interface should appear a few seconds after the operating system has completed loading. In some cases, the user interface may not be displayed if components installed in the guest operating system prevent this or the GPR tool is otherwise incompatible with the operating environment. In this case, please remember that you can still use the VFC PWB feature to disable password authentication.

If GPR is still required, please follow the steps below to troubleshoot the problem:

1. Browse the VM file system and check for `\Windows\GPRSERVICE32.EXE`. This file contains the GPR tool and must be present on the guest file system for GPR to function.
2. Mount the guest OS “System” hive using the Windows RegEdit tool. This hive file is normally located at `\Windows\System32\Config\System`. Open the hive file and confirm that, as a minimum, the registry entries below are present. If these are missing, GPR cannot function:

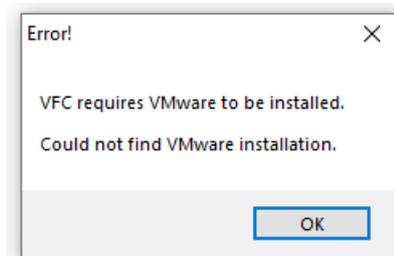
```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSetXXX\Services\VFCGPRSERVICE]
"Type"=dword:00000010
"Start"=dword:00000002
"DisplayName"="VFCGPRSERVICE"
"Description"="VFC GPR Service"
```

3. Reboot the VM and after the OS has loaded, try pressing Alt-Tab a few times. This may reveal the GPR user interface if it is hiding behind other user interface components
4. If VFC v5.0.17 or later is installed, you can also try the following additional steps:
 - a. Listen to the VM at start-up. The GPR tool in v5.0.17 and later emits a beep when it starts (requires sound to be enabled in the VM)
 - b. Try pressing shift five times (Windows XP) or clicking the Windows Ease of Access icon (Windows Vista and later) on the login screen. This should display the GPR user interface. If you hear the beep but the user interface does not appear, this may indicate that another software component is suppressing the GPR tool
 - c. Browse the VM file system and locate the GPR log file. Please use the form on the support website (<https://vfc.uk.com/support>) to send this to technical support. The file is located here:

```
\Windows\VFCGPRService32.log
```

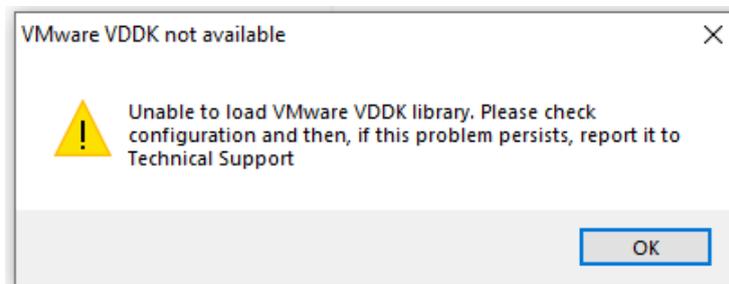
How do I fix “Could not find VMware installation”?

VFC requires VMware Workstation/Player v12 or later to function. If one of these products is not installed the following message will be displayed on start-up. To resolve the problem, please install a supported VMware product:



How do I fix “Unable to load VMWare VDDK library”?

VFC is designed to be used with the VMware Workstation/Player virtualisation products. It requires a component called the VMWare VDDK to function. If this component is missing, the following error is displayed:



VFC is currently supplied with v5.1.4 of the VDDK. This is located in the VFC ZIP file. To install the VDDK, please proceed as follows:

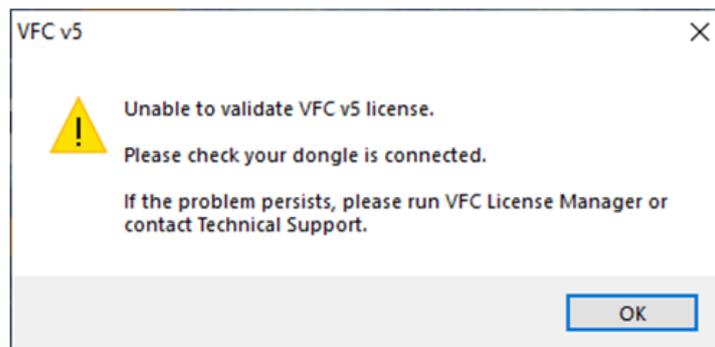
1. Open the VFC distribution ZIP file
2. Locate the **VMWare-vix-disklib-xxxxx** file and double click on it:



3. Follow the on-screen prompts to install the software with default settings

How do I fix “Unable to validate VFC v5 License”?

VFC requires a current license (dongle) to function. If the dongle is not connected or is not functioning, VFC will report “Unable to validate VFC v5 license”. Please check the dongle driver is installed (green dongle only) and then use VFC License Manager to troubleshoot this. This is described elsewhere in the FAQ.



How do I fix “License system reports no license available?”

The message “License system reports no license available” typically indicates that no VFC v5 license has been assigned to your dongle. Please contact Technical Support to resolve this.

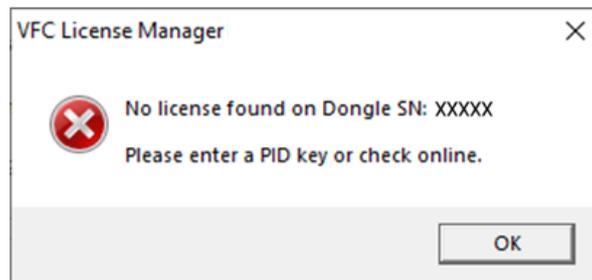


How do I fix License Manager hangs or reports “Internal date error”?

This problem has been reported with older versions of License Manager. Please download the latest License Manager from the VFC website.

How do I fix “No license found”?

The message “No license found” indicates that no VFC v5 license is present on the dongle. Please contact Technical Support to confirm this and arrange for a VFC v5 license.

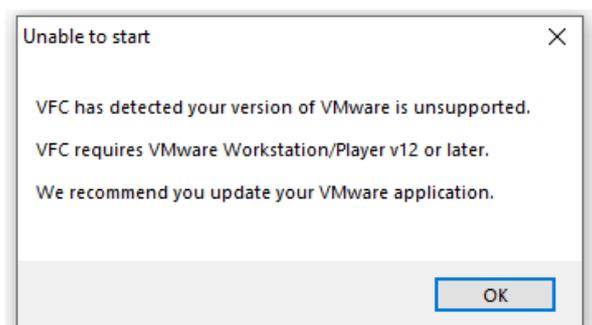


How do I fix License Manager error “Unexpected license data” or “Failed to download license information”?

These error messages occur when License Manager is unable to successfully contact the VFC license system. This can be due to a network blockage or a proxy/firewall issue. Please try running License Manager on a different PC or if that fails or is not available, please contact Technical Support for an offline product activation key.

How do I fix “Unable to start: VMware unsupported”?

The message “Unable to start: VMWare is unsupported” indicates that VMWare is either not installed or is before VMWare v12. To resolve this problem, please update your VMWare installation:



The guest OS fails to boot (BSOD). What can I do?

The virtual hardware provided by VMware may be significantly different from the original hardware. VFC supports a wide range of hardware and, in most cases, can successfully modify an image so that it will boot successfully. However, in some cases, VFC may not be successful. In this case, we recommend approaching the problem in the same way as on a physical computer.

- Disk encryption – Identify if disk encryption is present and obtain a recovery key
- Mass storage driver – Identify the original mass storage drive type (SCSI, SATA or IDE) and change the default option in the VFC Options dialog to match
- Safe mode – Try booting the system in safe mode and remove drivers which are not relevant to VMware or the investigation (typically high-end graphics/audio drivers and OEM utilities)

The guest OS reports that new hardware has been found. Do I need to install drivers and reboot?

The virtual hardware provided by VMware may be significantly different from the original hardware. It is therefore very likely that new hardware devices will be detected and the guest OS may prompt you to reboot. This is rarely absolutely necessary but, if you have the time, it will typically lead to a more stable and better-performing guest OS. We recommend taking a moment to do this if you will be using the guest OS for a prolonged period.

How can I improve the performance of a new virtual machine?

VMware Workstation Pro and VMware Workstation Player 12 and above include a suite of tools known as the VMware Tools Package. Installing this will usually improve the performance of the virtual machine.

Can I access the Internet from the virtual machine?

VFC is primarily designed to be a forensic application. For this reason, it does not enable network access in newly created virtual machines. This ensures that such guest systems remain isolated from the network. If appropriate and safe, network support may be added to the virtual machine by using the VFC Modify Hardware tab. We recommend that this is done cautiously and only after assessing the risks of connecting the guest environment to the network/internet.

Can I transfer data between the New Virtual Machine and my own System?

Yes. The virtual machine is just like any other computer and you can transfer data using one or more of the following techniques:

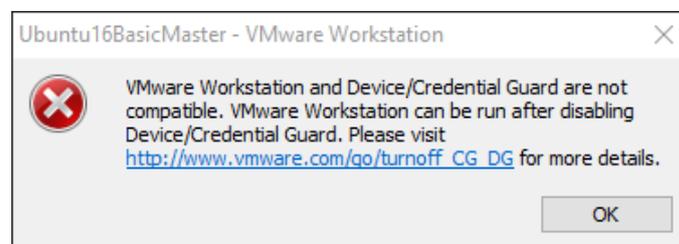
- Real/virtual floppy disk
- USB device
- External physical/virtual disk
- External optical drive / ISO image file
- Copy/paste (requires VMware Tools)

Why does the New Virtual Machine need to be activated?

The virtual machine is just like any other computer and the conversion from the original hardware environment to the new virtual hardware environment may trigger a software activation procedure. VFC includes a variety of features that may be used to work around this for legitimate investigatory purposes.

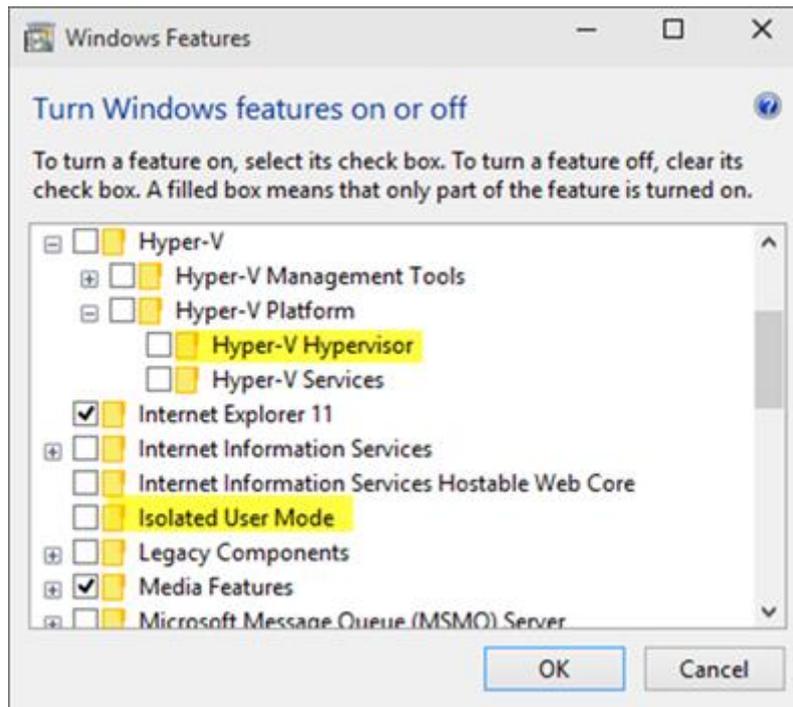
Is VFC compatible with Windows 10 “Creators” Update?

Microsoft has enabled the Hyper-V feature in the Windows 10 “Creators” Update (Build 15063). This alternative virtualisation (hypervisor) platform similar to VMware. Hyper-V is not compatible with previous versions of VMware and will typically need to be disabled:



To resolve this problem, disable Hyper-V on the host computer. Please proceed as follows:

1. Open **Control Panel / Programs and Features** (appwiz.cpl)
2. Click **Turn Windows feature on or off**
3. Expand the tree and locate Hyper-V
4. Disable **Hyper-V Hypervisor** and **Isolated User Mode**



Note: This is a VMware/Microsoft and User compatibility issue, and not a limitation of VFC.

How can I fix Windows compatibility assistant prevents VMware from running?

Windows 10 (OS Build 18362.387 or later, released September 2019) updates the Windows Compatibility Assistant and to prevent older versions of VMWare Workstation/Player from running.

To remove this block on standalone computers and permit older versions of VMware to run, apply the Registry file provided in the [VFC install path]\VMware folder. This is available in VFC v5.0.13 and later.

NOTE: This technique is not suitable for computers that are members of a domain and where the Compatibility Assistant is managed by Group Policy. If this is the case, please contact Technical Support for further advice.

Windows NT5 SP0-SP5 fail to boot after virtualisation. How can I fix it?

Virtual machines running Windows NT4 SP0-SP5 (but not SP6) may fail to boot after virtualisation. This problem is due to a change in the on-disk NTFS format introduced in SP6 / Windows 2000. Later operating systems automatically update the on-disk format and this is unsupported by NT4 SP5 and earlier. The problem can be avoided by using one of the following techniques:

1. Install NT4 SP6 before virtualisation

OR

2. Convert the image to FAT

Note: This is a limitation of Windows NT4 SP5 and earlier and not a limitation of VFC.

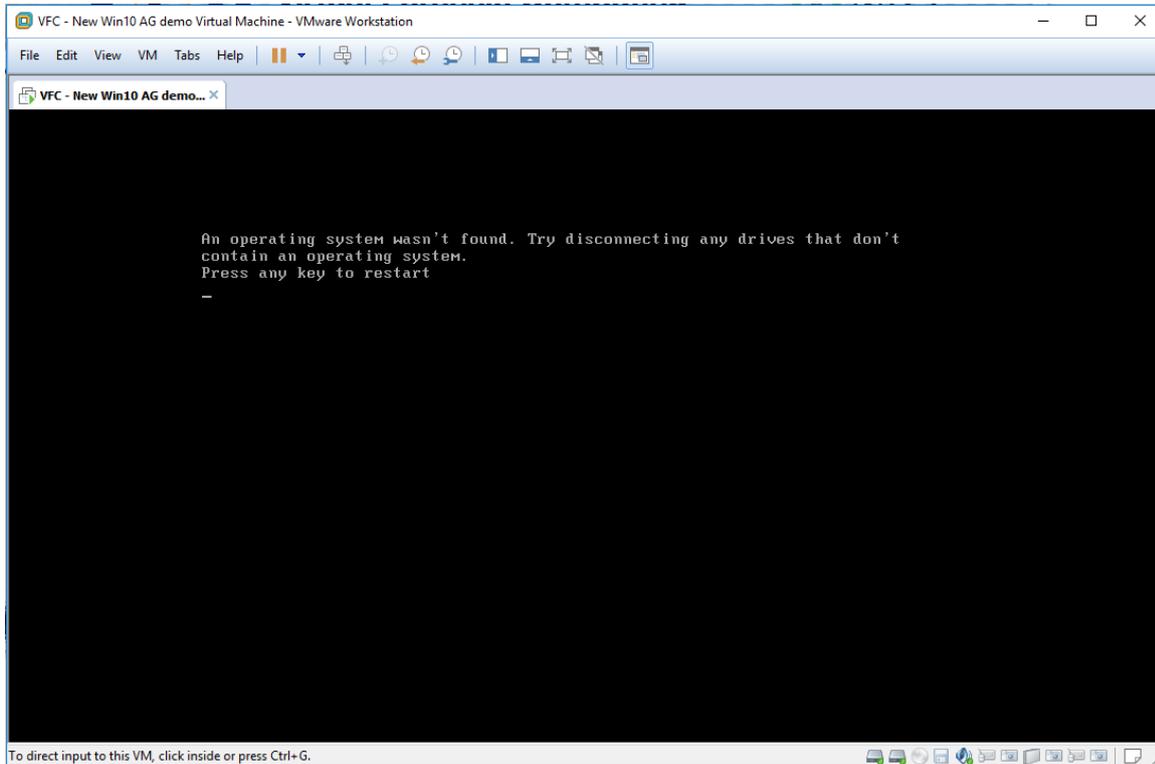
How do I fix error “Could not load/unload registry”

This error can occasionally occur if the VM generation process is interrupted. Please reboot your forensic workstation and try again to resolve this error.



How can I fix “Operating System not found” error?

The error “An Operating system wasn’t found” indicates that the OS loader code was unable to find a bootable partition. This can occur if there is no bootable partition or if the system has multiple virtual hard disks and has booted in the incorrect sequence:



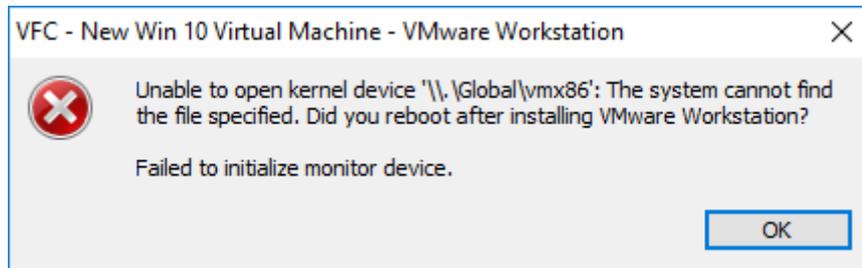
To resolve this, we suggest:

1. Close virtual machine
2. Check virtual machine configuration and remove any unnecessary virtual disks
3. Start the VM, press F2 to enter the VMware BIOS and change the boot order to the desired disk

Note: The default VFC configuration is to use a SCSI virtual disk. This offers the widest range of compatibility with different operating systems and reduces the chance of error.

How I fix “Unable to open kernel device” error?

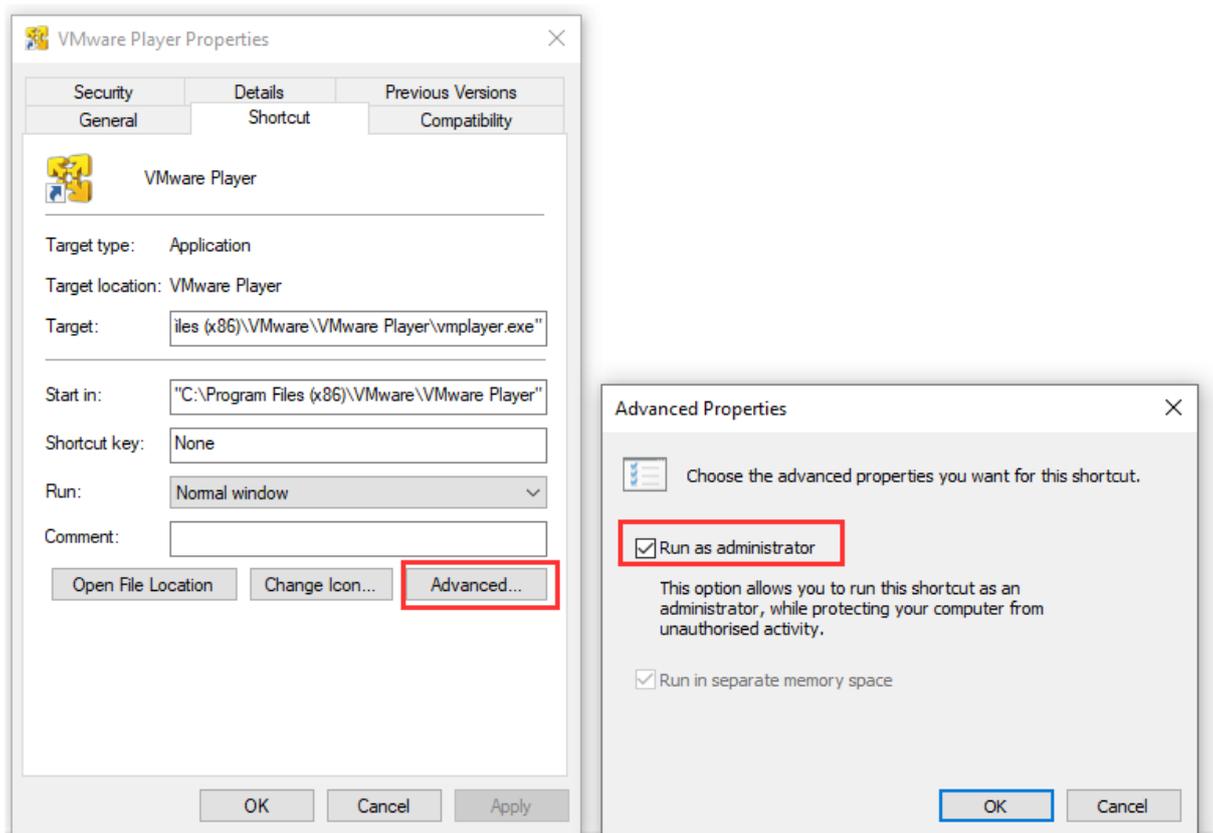
The VMware error “Unable to open kernel device” can occur when VMware is not launched with elevated (administrator) privileges:



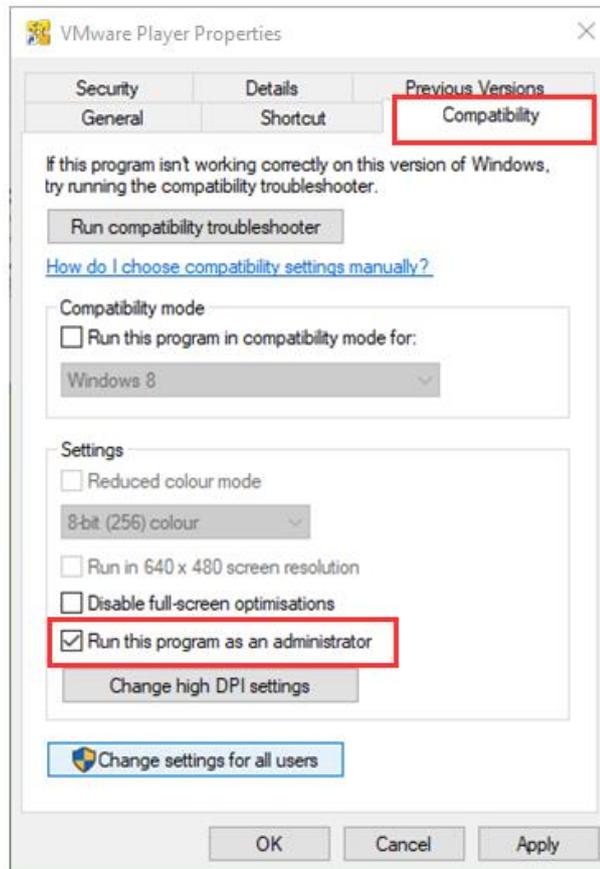
VFC requires forensic image files to be “mounted” as an emulated physical disk. This scenario requires that VMware operate with elevated (or “administrator” privileges). This allows VMware to access the emulated physical disk used by VFC.

To run VMware with administrator privileges, please proceed as follows:

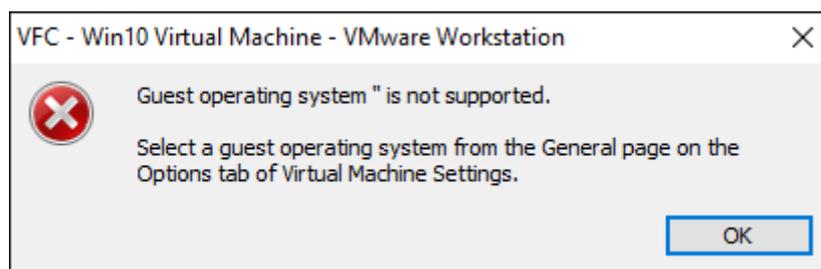
1. Locate the VMware application shortcut
2. Right-click on it and select **Properties**
3. On Windows 10, click **Advanced**, select **Run as administrator** and then **OK**



- On older systems, click **Compatibility**, select **Run as administrator** and then **OK**



How do I fix the guest operating system " is not supported error?



This error can occur when VFC fails to correctly identify the guest OS. To work around this, please manually select the target OS from the drop-down list. If this happens, please send a copy of your log file and an explanation of the issue to our Support team for further investigation.

How do I resolve VMware asks to Take Ownership of the VM?

This problem is known to occur in the following situations:

1. VM created by VFC but then attempt to open directly in VMware (without Administrator privileges)
2. VMware fails to exit correctly (or PC crashes) leaving VM in the locked state

To resolve this problem, please try running VMware with Administrator rights, check the VMware log files and, if this fails, reboot and try re-creating the virtual machine again.

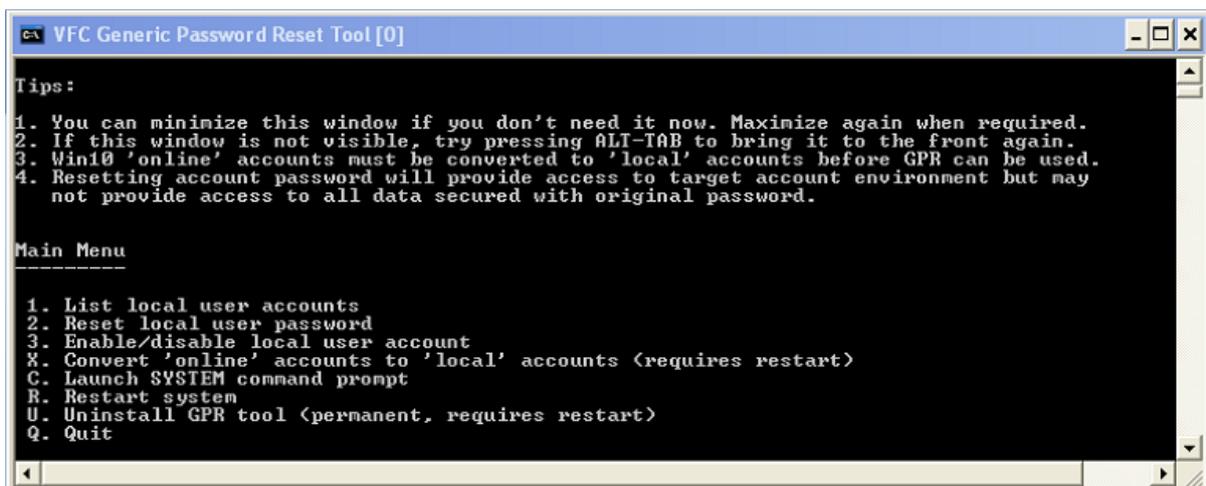
What is the Generic Password Reset (GPR) feature and how do I use it?

The Generic Password Reset (GPR) feature provides a powerful alternative to the original VFC PWB feature. It uses a completely different technique that can be used to make permanent account and password changes:

- Change Windows online “live” user accounts to “local” user accounts
- Reset password for local accounts to a known value
- Launch a Command Prompt with system-level privileges

GPR operates by injecting a VFC software component directly into a Windows-based virtual machine. This feature is enabled by default and may be disabled using the VFC Options dialog. GPR displays a console (text) application on the login screen which can be used to list and manipulate user accounts and launch a system (root) command-prompt.

Please see the VFC User Guide for a detailed description of how to use the GPR feature.



```

ca VFC Generic Password Reset Tool [0]
Tips:
1. You can minimize this window if you don't need it now. Maximize again when required.
2. If this window is not visible, try pressing ALT-TAB to bring it to the front again.
3. Win10 'online' accounts must be converted to 'local' accounts before GPR can be used.
4. Resetting account password will provide access to target account environment but may
   not provide access to all data secured with original password.

Main Menu
-----
1. List local user accounts
2. Reset local user password
3. Enable/disable local user account
X. Convert 'online' accounts to 'local' accounts (requires restart)
C. Launch SYSTEM command prompt
R. Restart system
U. Uninstall GPR tool (permanent, requires restart)
Q. Quit
  
```