For the sake of simplicity, we sometimes refer to **_viruses_** as a collective description of unwanted code.

When NVC detects and/or removes malicious code, you are informed about the incident. NVC provides the file name and location of the infection, as well as the **_type_** of malware detected. The most common types of unwanted code are:

- viruses
- trojans
- worms

More:

Improving protection

There are several ways of getting infected. To further improve your protection, you should:

1. Run Internet Update to ensure that your installation is always up-to-date.

2. Make sure that you configure NVC to **Remove** infected files. NVC will always try repair before removal anyway.

3. It is also a good idea to quarantine infected files that cannot be repaired.

4. If you are notified about a virus that is moved to quarantine, we recommend that you check what kind of malware you have received. On Norman's web site you can look up the virus/worm/trojan etc.:

   www.norman.com/virus_info/

5. Unless you have very good reasons for doing so, do *not* stop the On-access scanner.

6. When you have received a message that confirms that detected viruses have been removed, deleted, or quarantined, we recommend that you run a manual scan (with the On-demand scanner) to make sure your system is clean.

Please refer to Norman's *Reference* Guide for details on configuring NVC.

In some situations NVC cannot remove a detected virus. When this happens, you will receive a warning like this.

Note that your system is probably not infected, but the file still is. Nevertheless, we recommend that you run an on-demand scan of your system to verify that everything is OK. You will never be granted access to an infected file, and it is therefore safe to proceed.

See Definitions and tips for information on how to further improve virus protection.

A virus cannot be removed if the infected file resides on a:

1   Write-protected diskette

2   CD-ROM

3   Network drive and the file is write-protected, or if

4   The file is in use (i.e., you do not have write
         access), or:

5   A cleaning script is not defined in the scanner
         engine for this virus.

NVC detected a virus and removed it because automatic cleaning is on. If possible, NVC removes viruses, trojans, worms etc. automatically when this option is selected.

To select automatic cleaning, use the NVC configuration tool:

In the module On-access scanner under *Norman Virus Control*, select **Remove** in the tab **Cleaning**.
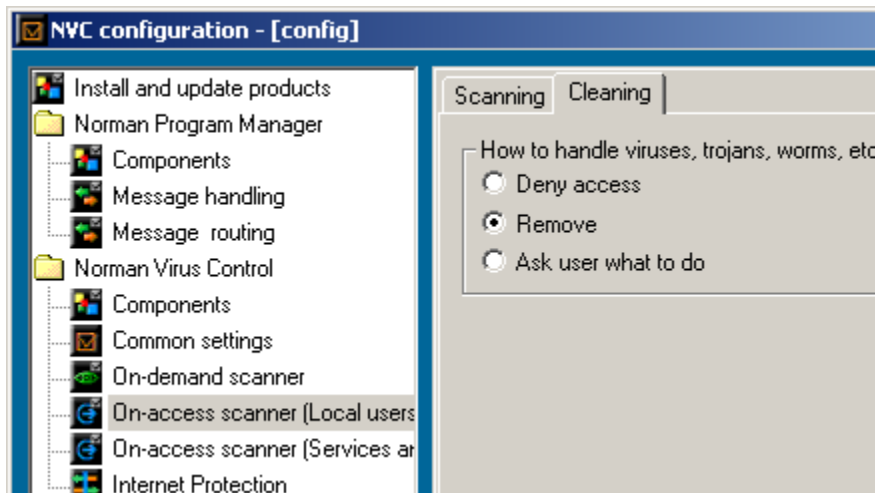
Select the option **Don't show this message again** if you don't want NVC to notify you about further virus removals today.

See <u>Definitions and tips</u> for information on how to further improve virus protection.

In some situations NVC cannot remove a detected virus. When this happens, you will receive a warning like this.

Note that your system is probably not infected, but the file still is. Nevertheless, we recommend that you run an on-demand scan of your system to verify that everything is OK. You will never be granted access to an infected file, and it is therefore safe to proceed.

See Definitions and tips for information on how to further improve virus protection.

A virus cannot be removed if the infected file resides on a:

1   Write-protected diskette

2   CD-ROM

3   Network drive and the file is write-protected, or if

4   The file is in use (i.e., you do not have write
         access), or:

5   A cleaning script is not defined in the scanner
         engine for this virus.

NVC detected a virus, but the virus was not removed because automatic cleaning is off.

Click on **Remove** to clean the file.

To select automatic cleaning, use the NVC configuration tool:

In the module On-access scanner under *Norman Virus Control*, select **Remove** in the tab **Cleaning**.
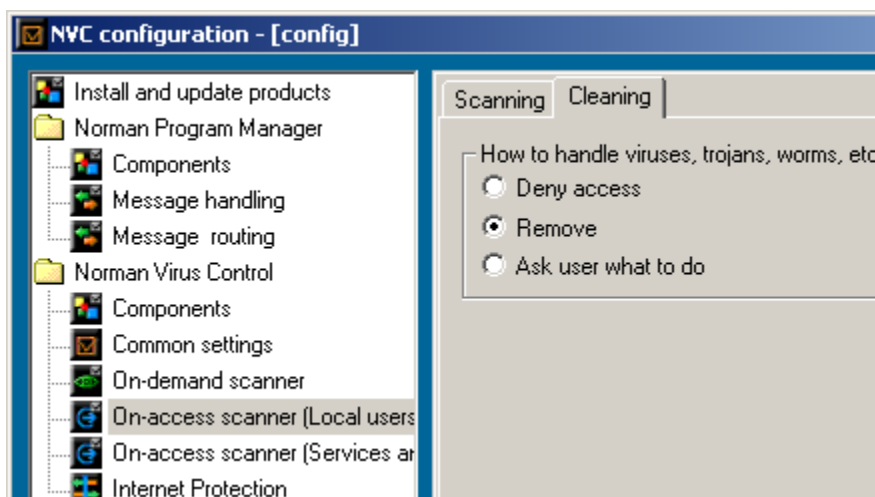
See Definitions and tips for information on how to further improve virus protection.

NVC could not remove the detected virus because you have selected **Deny access** in the On-access scanner module's **Cleaning** tab.
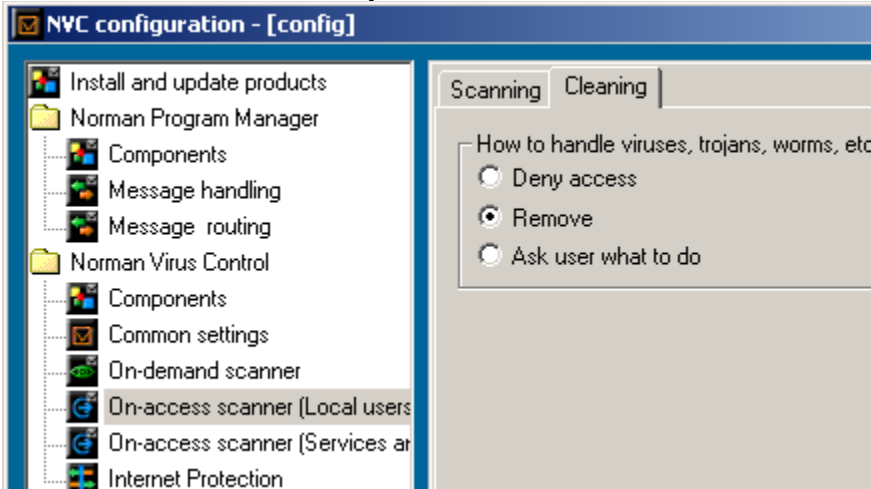
To remove viruses automatically, select **Remove** from the same tab:
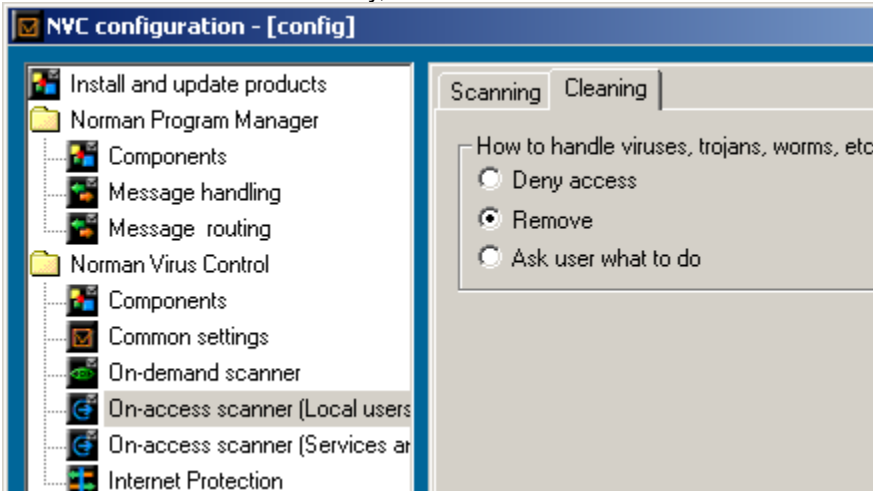
See Definitions and tips for information on how to further improve virus protection.

NVC detected a virus, but in the NVC configuration tool you have selected **Deny access** in the On-access scanner module, **Cleaning** tab.

To remove viruses automatically, select **Remove** from the same tab:

NVC cannot remove this particular boot sector virus.

The most likely reason is that there is currently no repair script for this virus.

Other situations where NVC cannot remove detected viruses are that the file is in use so you don't have write-access to it,   the virus resides on a write-protected floppy or a CD-ROM, or on a network drive where you don't have the necessary privileges to remove it.

NVC detected and removed a boot sector virus. This message appears if NVC detects a boot sector virus on a removable media and automatic cleaning is **ON**. It also appears if the virus is located on a hard drive, and you selected to remove the virus ***without*** backing up the boot sector to a floppy before cleaning.

NVC detected a boot sector virus on a removable media or on a hard drive, but NVC cannot remove this particular virus. Select the backup option before you try to remove the virus again.

NVC detected a virus, but in the NVC configuration tool you have selected **Ask user what to do** in the module On-access scanner's **Cleaning** tab.

To remove viruses automatically, select **Remove** from the same tab:
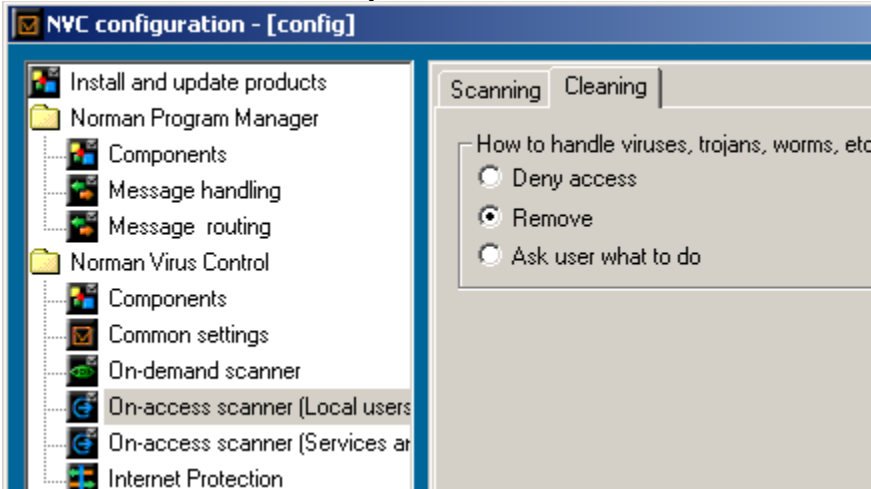
A boot sector virus was detected on a hard drive, but NVC does not allow automatic removal in this situation. Therefore, we recommend that you insert a formatted, blank, and write-enabled floppy in drive A: for backing up the boot sector area. Make sure that you label the floppy properly. When you have selected this option, click on **Remove**.

NVC will back up your boot sector to a "Rollback Disk" **before** it attempts to remove the virus.

If anything goes wrong and the boot sector on your machine is damaged, you can boot from the rollback floppy and thereby restore your boot sector. Note that if this incident occurs, your system is still infected.

It is important that you label the restore diskette properly and keep it in a safe place. If repair fails, you will most likely discover it on next reboot. If this happens, boot from the restore diskette. Note that in such a situation, your system is still infected.

The boot virus was removed from the hard drive, but no restore diskette was created. The reason for failing to create a restore diskette is most likely a damaged diskette.

However, the virus is removed.

Virus removal as well as restore diskette creation failed, but your boot sector is most likely intact. This rare situation could have been caused by a write-protected medium, for example a Jaz disk.

When virus removal fails, a restore diskette will never be created.

Note that your hard drive is still infected.

You are infected by a memory virus. NVC cannot repair this particular virus.

Follow the instructions in the dialog to remove the virus.

NVC detected a virus in memory and removed it because automatic cleaning is on. If possible, NVC removes viruses, trojans, worms etc. automatically when this option is selected.

Note well: You **must** find the offending file/source for the infection. Use the on-demand scanner to check the entire system.

You are infected by a memory virus. NVC cannot repair this particular virus.

Follow the instructions in the dialog to remove the virus.

One or more infected files were detected, but could not be removed. Reboot your machine and try to remove the infected file(s) again.

You have selected **Move unrepairable files to quarantine** in the Norman product folder ***Norman Quarantine***, and the file specified in the dialog box is malware that NVC has no cleaning script for.

Certain types of malware, like backdoors and trojans, cannot be repaired because such files have no useful purpose and *only* contains harmful code. In such instances, removing (i.e. deleting) the file equals cleaning.