

NORMAN Contents

Cat's Claw

[About Cat's Claw](#)

[Limitations in This Version](#)

[Configuration Concepts](#)

[Cat's Claw Factory Settings](#)

Configuration Dialogs

[General](#)

[Certified Macros](#)

[Behavior](#)

[Warnings from Cat's Claw](#)

[Logging](#)

NORMAN About Cat's Claw

Cat's Claw is an on-access (real-time) scanner that detects viruses in files as well as boot sectors. One of its unique features is the Certify Macro function. This function allows you block Word and Excel files with unknown and possibly infected macros from your system.

Cat's Claw will scan for viruses in files as they are being opened. Whenever possible, an infected file is repaired before the file is handed over to the application.

If repair is not possible, you will receive a message and access to the infected file is blocked.

If repair is not possible, you will receive a message and the application is not allowed to open the infected file.

The present version of Cat's Claw *detects and removes* binary file and boot sector viruses as well as all macro viruses in MS-Word and MS-Excel known to NVC.

NORMAN Limitations in This Version

In a Novell network with Novell 32 bits client in Windows 95, Cat's Claw can not check files from the server.

In an environment like this, Cat's Claw should not reside on the server, but on the workstation.

We recommend that you copy the file from the server to the workstation and access the file locally or use Norman FireBreak on the server.

NORMAN Configuration Concepts

Users are not a homogenous group, and we therefore provide you with the option of configuring Cat's Claw to best suit your needs. If you run Cat's Claw with the default settings, the following options apply:

- Cat's Claw will be loaded into memory at startup
- you will be prompted for action when a virus is found
- you will receive a warning if Cat's Claw is unable to scan a file
- uncertified macros will not be removed

The following discussion covers the different dialogs and their options. Cat's Claw is not equipped with default options that we believe provide the optimal protection for you. One reason is that users have very different needs, another is that regulations in some countries do not allow a program to remove files without the user's explicit consent. This legal restraint is blocking our wish to set automatic removal of viruses as default option.

NORMAN Cat's Claw Factory Settings

The factory settings in the Cat's Claw configuration program should therefore not be considered as recommended options.

From a security point of view, we strongly recommend that you check the option **Load Cat's Claw on startup** in the tabbed dialog General.

However, you should use the configuration options to make Cat's Claw work smoothly and efficiently on your PC anyway.

NORMAN General

Start Cat's Claw automatically

If you want Cat's Claw to be active on your system at all times, then run the application with this default option on to ensure that Cat's Claw is loaded into memory when you start your machine.

Show icon on desktop

For a visible confirmation that Cat's Claw is active, you can check this option to display an icon like this on your desktop:



Cat's Claw

User can disable scanning

If you're an administrator and don't want to allow the users to turn off scanning, you should not check this option. The user will then be prevented from disabling Cat's Claw by clicking on the Cat's Claw icon on the desktop.

Display warning after automatic repair

If you select **Remove virus from file** (see [Handling of Viruses](#)), you will be informed when Cat's Claw has removed a virus from an infected file.

Automatic repair of boot sector viruses on hard disks is not possible. With the **Remove virus from file** option ON, boot sector viruses will automatically be removed from diskettes.

If Cat's Claw is already loaded, the **Start** button will appear as **Stop**.

NORMAN Certified Macros

From this dialog box you can certify the macros that Cat's Claw shall allow in your files. Deciding whether to certify macros or not is a critical decision. Using this function will protect you against new macro viruses not yet identified. We consider this extremely important because new macro viruses pop up every day. On the other hand, 'healthy' but unknown macros can be removed and inflict damage on files. The decision on whether to use the certify macro function is consequently a matter of balancing security versus convenience.

If you certify macros, only these macros will be accepted. See [Handling of Uncertified Macros](#) for more considerations on certified and uncertified macros.

Follow these steps to certify a macro:

- 1 Click on the **Add** button and choose a file from the Open file dialog.
- 2 If the selected file doesn't contain any macros, the list box will be empty. Possible macros appear in the Certify Macros list box.
- 3 Highlight the macros you wish to include and click on **Certify**. You are returned to the Certified Macros dialog.
- 4 When you highlight a macro in the Certified Macros dialog, the **Delete** and **Comment** buttons become available.
- 5 Click on **Add** and repeat step 1 through 4 to certify more macros.

Note: If you check the **No action** option in the "Handling of uncertified macros", you will disable the certified macro function.

More:

[Fields in the Dialogs for Certifying Macros](#)

NORMAN Fields in the Dialogs for Certifying Macros

There are six fields in the two dialog boxes (“Certified Macros” and “Certify Macros”). Except for the Comments field in the Certify Macros dialog, the information is provided by Cat’s Claw:

Status:

There are three types of status that can appear in this field:

- 1 **Empty:** if the status field is empty, you can certify the macro.
- 2 **Certified:** since this macro is already certified, you cannot certify it again.
- 3 **Viral:** macro viruses are made up of multiple macros. This macro is/has been part of a virus and cannot be certified.

Name:

Cat’s Claw will use the macro’s actual name, or as many characters as possible if it’s a long name, to make it possible to recognize for a user.

Cat’s Claw will use the following three fields to identify a certified macro. This is internal read-only information.

Type:

Three different types can appear in this field:

- 1 **WB:** denoting a Word 6/7 macro.
- 2 **VBA3:** denoting an Excel 5 macro.
- 3 **VBA5:** denoting an Office 97 macro.

CRC32:

A checksum established as one of the three distinguishing marks for a macro. If the macro is changed after being certified, the changed macro must be certified.

Length:

Like any other file, a macro has a certain length. This field displays the macro length used by Cat’s Claw to check that a certified macro hasn’t been changed after certification.

Comment:

Whatever information you add to a certified macro. This is the only field available for user input.

NORMAN Behavior

This tabbed dialog box is divided into three sections. This is where you instruct the application how to handle viruses, uncertified macros, and files that cannot be scanned.

More:

[Handling of Viruses](#)

[Handling of Uncertified Macros](#)

[Handling of Files That Cannot Be Scanned](#)

NORMAN Handling of Viruses

Ask user what to do

If you don't want automatic removal of viruses when you access infected files, you must check this option. When you try to open an infected file, you'll receive information about the incident.

Remove virus from file

Checking this option will automatically remove possible viruses from infected files. You will, however, receive a message about the infection.

NORMAN Handling of Uncertified Macros

An uncertified macro does not necessarily contain a virus. However, all unknown macros are possible virus carriers, and you can therefore decide how to handle these. If you have certified certain macros, then these are the only macros that Cat's Claw will accept.

[] Do nothing

Cat's Claw will not touch the macro, nor inform you about it. Remember that if the macro contains a known virus, Cat's Claw will take action anyway.

Note: The certify macro function is disabled if you choose this option.

[] Ask user what to do

With this options checked, Cat's Claw will warn when an uncertified macro is found.

Note: If you run with this option on, ALL macros will be removed except for previously certified macros.

[] Remove macros from document

When you open a file with an uncertified macro, you will receive a warning. Click on Help for assistance.

Note: If you run with this option on, ALL macros will be removed except for previously certified macros.

NORMAN Handling of Files That Cannot Be Scanned

In some situations Cat's Claw is unable to scan a file. Examples are Word 8 files with password protection, damaged files, or when internal system errors occur. The following options decide how Cat's Claw should react under such circumstances.

Display warning

When you receive a warning when you access a file, you know that this file has not been checked for viruses. You can, however, proceed at your own risk.

Display warning and deny access

Checking this option involves that you are warned about an unscanned file, and access is denied.

NORMAN Warnings from Cat's Claw

The following is a list of the warnings that you may encounter in certain situations. When a warning is displayed, click on Help for assistance.

More:

[Manual Virus Removal](#)

[Virus Removed](#)

[Virus Not Removed](#)

[Uncertified Macro Not Removed](#)

[Uncertified Macro Removed](#)

[Cannot Remove Uncertified Macro](#)

[Password Protected File](#)

[Damaged File](#)

[Internal Error](#)

[Password Protected File Blocked](#)

[Damaged File Blocked](#)

[Internal Error Denied Access](#)

[Cannot Repair File](#)

[Boot Virus On Medium Detected](#)

[Boot Virus On Medium Not Removed](#)

[Boot Virus On Medium Not Repaired](#)

[Boot Virus On Hard Drive Detected](#)

[Boot Virus Removed And Restore Diskette Created](#)

[Boot Virus Removed But Restore Diskette Was Not Created](#)

[Boot Virus Repair And Restore Diskette Creation Failed](#)

NORMAN Manual Virus Removal

You have specified **Ask user what to do** in the tabbed dialog Behavior, and access to this file is therefore denied. Try to remove the virus manually by clicking on the **Remove** button. Then try to access the file again. For automatic removal of viruses, change your configuration to **Remove virus from file**. See Handling of viruses.

NORMAN Virus Removed

If you check the box **Don't show this message again today** in this dialog, you will not be informed about other possible cleaning operations until you reboot your machine. However, you can keep track of removed viruses by checking **Viruses removed** in the tabbed dialog [Logging](#).

NORMAN Virus Not Removed

In some situations Cat's Claw cannot remove a detected virus. When this happens, you will receive a warning like this.

Note that your system has not been infected, but the file still is. You will never be granted access to an infected file, and it is therefore safe to proceed.

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).

NORMAN Uncertified Macro Not Removed

The detected macro is not a virus, but it does not appear on your list of certified macros. Your choices are:

- 1 Click on **Remove** to clean the file.
- 2 If you want to access the file without removing the macro, check the option **Do nothing** (Handling of Uncertified Macros) and try to open the file again.

NORMAN Uncertified Macro Removed

Cat's Claw removed macros from this file because:

- 1 They did not appear on the list of certified macros.
- 2 You checked the option **Remove macros from document** in the tabbed dialog Behavior.

With this option checked, Cat's Claw will remove all macros not specified in the tabbed dialog Certified Macros.

NORMAN Cannot Remove Uncertified Macro

The macro(s) cannot be removed if they reside 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).

See [Handling of Uncertified Macros](#).

NORMAN Password Protected File

Cat's Claw will not deny access to this file because you selected the option **Display warning** in the tabbed dialog Behavior. You can enter the password and open the file at your own risk. Cat's Claw cannot guarantee it's free for viruses or uncertified macros.

Note: This situation will occur only when a password protected Word 8 file is detected. Cat's Claw can detect and remove macro viruses from password protected files in Word 6 and Word 7.

NORMAN Damaged File

Cat's Claw will not deny access to this file because you selected the option **Display warning** in the tabbed dialog Behavior. The file is damaged and has not been scanned. You can open the file at your own risk. Cat's Claw can not guarantee it's free for viruses or uncertified macros.

NORMAN Internal Error

Cat's Claw will not deny access to this file because you selected the option **Display warning** in the tabbed dialog Behavior. Due to an internal error in Cat's Claw or Windows, the file has not been scanned. You can open the file at your own risk. Cat's Claw can not guarantee it's free for viruses or uncertified macros.

NORMAN Password Protected File Blocked

You checked the option **Display warning and deny access** in the tabbed dialog Behavior. Password protection stopped Cat's Claw from scanning the file, and you cannot access it. Possible solution is changing your configuration to **Display warning** only and access the file at your own risk.

Note: This situation will occur only when a password protected Word 8 file is detected. Cat's Claw can detect and remove macro viruses from password protected files in Word 6 and Word 7.

NORMAN Damaged File Blocked

You checked the option **Display warning and deny access** in the tabbed dialog Behavior. Cat's Claw could not scan the file because it's damaged, and you cannot access it. Possible solution is changing your configuration to **Display warning** only and access the file at your own risk.

NORMAN Internal Error Denied Access

You checked the option **Display warning and deny access** in the tabbed dialog Behavior. Due to an internal error in Cat's Claw or Windows, the file has not been scanned. Possible solution is changing your configuration to **Display warning** only and access the file at your own risk, or reboot your machine and try again.

NORMAN Cannot Repair File

A virus is detected, but Cat's Claw does not know how to remove it.

We recommend that you move the infected file to a removable medium (for example a diskette) and contact Norman.

NORMAN Boot Virus On Medium Detected

A boot sector virus was detected on the medium, but Cat's Claw does not know how to remove it.

Possible reasons that prevent removal are:

- 1 A write-protected diskette
- 2 The virus resides on a CD-ROM

Note: If the virus resides on a diskette, remember to remove it from the diskette drive before you reboot.

NORMAN Boot Virus On Medium Not Removed

Automatic removal of boot sector viruses is possible from media like diskettes and zip-disks, for example, but not from hard drives. Try to remove it manually by clicking the **Remove** button.

Note: If removal fails, make sure that you don't boot from the infected medium.

NORMAN Boot Virus On Medium Not Repaired

A boot virus on the medium (for example diskette, zip-disk) was detected, but not removed. A repair script for this particular virus is not established yet.

Please feel free to report the incident to Norman.

NORMAN Boot Virus On Hard Drive Detected

A boot sector virus was detected on the hard drive. Cat's Claw is not allowed to remove a boot virus automatically. Repairing a boot sector virus is not risky, but in case something goes wrong, we recommend that you back up the replaced sectors.

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.

NORMAN Boot Virus Removed And Restore Diskette Created

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.

NORMAN Boot Virus Removed But Restore Diskette Was Not Created

The boot virus was removed from the hard drive, but no restore diskette was created. The reason for not succeeding in creating a restore diskette is most likely a damaged diskette.

However, the virus is removed.

NORMAN Boot Virus Repair And Restore Diskette Creation Failed

Repair failed, but your boot sector is most likely intact. This is a rare situation, which could have been caused by a write-protected medium, for example a Jaz disk.

When repair fails, a restore diskette will never be created.

Note that your hard drive is still infected.

NORMAN Logging

Cat's Claw will register vital activity in a log file. In this dialog you can decide what kind of information the log file should hold.

As for the other configuration dialogs, you should decide for yourself what kind of information that is important to you.

[] Viruses removed

Logs path, file name and name of removed viruses.

[] Viruses not removed

Logs path, file name and name of viruses detected but not removed.

[] Uncertified macros removed

Logs path and file name of removed uncertified macros.

[] Uncertified macros not removed

Logs path and file name of uncertified macros not removed.

[] Files that could not be scanned

Logs path and file name of files that Cat's Claw could not scan. Cat's Claw cannot scan files which are:

- password protected, possibly containing macros
- corrupted

[] Lost alarms (overflow)

Due to limitations of system's resources assigned to Cat's Claw, a maximum of, for example, 20 alarms can accumulate waiting for user response. If the unlikely situation should occur that you run into e.g. 25 infected files without responding to any of the waiting messages, then you will not be warned from infection number 21 and upwards. This option will give you the *number of infections* that Cat's Claw was unable to handle. If this happens, Cat's Claw will block access to the files rather than ask user what to do.

Loosing alarms does therefore not represent a security risk.

[] Log file

Enter a valid path and file name for the log file, for example `c:\norman\win95\claw95.log`.

