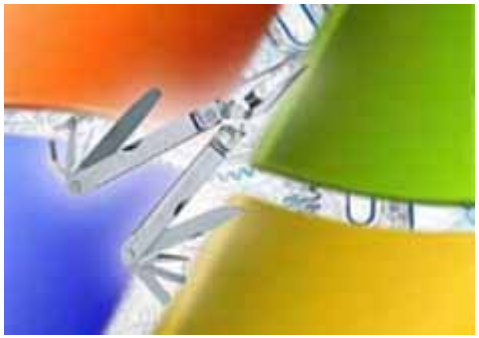


CIA Commander

for Windows NT 4 / Windows 2000 / Windows XP

Administration Manual

CIA Commander

Confidential Internal Administration

1. Common

Problems with a defective driver, files or anything else are easy to solve on operating systems that are based on FAT! You boot with a DOS floppy and you have access to nearly everything. On NTFS things are quite different. If you locked for example your account or a driver causes a blue screen, you have no way to access the secured system. CIA Commander is a perfect utility to access these computers anyway! There is absolutely no need to install anything on the PC before the problem occurs. All you need to fix it is the one single CIA Commander floppy. Even recovery console that ships with Windows 2000 can't solve a lost password or a smart-card protected system. CIA Commander does it all!

CIA Commander

Confidential Internal Administration

- ***Accesses any NTFS partition***
- ***Gives you chance change any passwords***
- ***Gives you full access to NTFS from CIA Commander-DOS***
- ***With registry-editor included***
- ***Easy to use - all features offered through GUI***

1.1. Introduction

Thank you for choosing CIA Commander!

Congratultaions! Choosing CIA Commander was a good choice. You got the most effective tool to recover and repair inaccessible Windows NT and Windows 2000 installations without losing important data. The way CIA Commander works is quite different from what is known up to now. CIA Commander is a single floppy that can access your NTFS-partitions and handle the file system, the user database and the registry.

Regaining Access if you don't have a password

CIA Commander gives you the possibility of changing the passwords for all accounts on your WinNT-installations! You can save the old password on floppy and you can restore it back! Sometimes, passwords are used in other applications too - so a change in NT doesn't solve the complete problem.

Handling GINA, Services, Drivers

A GINA that needs a smart-card reader can cause a lot of problems if the reader is defect or you lost your (only) card. CIA Commander makes it easy to change GINA back to the original version.

Drivers that are buggy can cause a blue screen. With CIA Commander you simply remove these drivers or change their starting behavior

Editing Registry

CIA Commander allows you to edit the complete registry. You will even see the entries that Microsoft has hidden, even in regedit32.

All registry keys can be edited. A graphical user interface allows you to navigate very comfortably.

The File Manager - Explorer from CIA Commander-DOS

Very often, incorrect DLLs are replaced or are in use when they should be replaced. This can cause various problems.

CIA Commander file manager explores all NTFS drives. You have the chance to copy,

rename and delete files. If a file can't be accessed because of wrong NTFS rights, you can correct this too.

Handling of Compressed Files

CIA Commander has a built-in support for compressed files and folders. You can access them like normal files.

Worst-case Support

In some rare cases, even with CIA Commander you can't repair your installation. (I. e. a virus changed all your EXEs). In this case, you can at least copy your important data to a safe location (other partition) or floppy for later usage.

1.2. Supported systems

All you need to install CIA Commander is a PC running any DOS or Windows 95/98 or Millennium to create the CIA Commander-floppy. On systems running with Windows NT/2000 you can't create the CIA Commander-floppy because direct access to the hardware is required!

CIA Commander will work with Windows NT (tested up to service pack 6a) and Windows 2000 (tested up to service pack 1).

Systems that are not based on NTFS can currently not be repaired with CIA Commander. We intend to add support for FAT and FAT32 in the next release.

Because CIA Commander-DOS doesn't offer support for special SCSI-adapters you can only access partitions, that are accessible by BIOS. If you use special drivers to access your NTFS partitions please contact support for assistance.

2. Installation

Installing CIA Commander is easy!

All you have to do is to start CIAINST.EXE. The installation program will ask you for a blank floppy. Be careful - all data on the floppy that you insert can be destroyed! The installation program will further install this Help File and a PDF documentation.

Don't use an old and damaged floppy to copy CIA Commander. The CIA Commander-floppy is copy-protected and the only way to duplicate it is to run CIAINST.EXE again.

After the installation is finished, you can use the CIA Commander-floppy to boot any PC and access it with the power of CIA Commander.

3. Program usage

To use CIA Commander you must boot the target-PC with the CIA Commander-floppy. If the PC doesn't boot with the floppy, change the settings in your BIOS. CIA Commander will boot on most PCs in less than 10 seconds. If your PC doesn't have a floppy drive, you can create a bootable CD-ROM with nearly every CDRW-software supporting bootable CDs.

Because CIA Commander fits on one floppy, there are no special settings to be adjusted.

After starting CIA Commander, you will see the CIA Commander's welcome-screen.

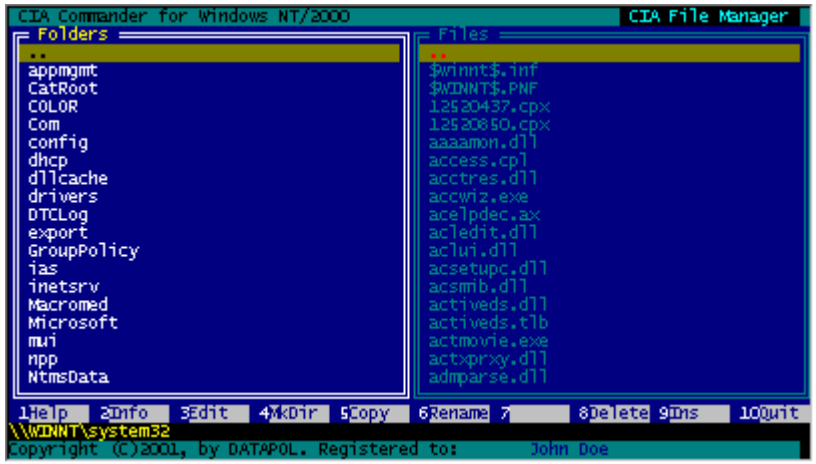
After pressing any key, you must select the partition you want to work with. Use the cursor keys to navigate to the correct partition and press the enter-key. Please remember, that at the moment only NTFS partitions are supported.

After making your choice, you will see CIA Commander's main menu. Select here the tool you want to use.

3.1. The file manager

On the left side, you will see the directory structure of the chosen partition. To navigate to a folder, you can use the cursor-up and cursor-down keys, or the page-up and page-down keys to scroll one page. To select a directory, press the Enter-key. To select a subdirectory, do exactly the same.

With the TAB-key, you can toggle between directories and files. On the right side of the screen, you see the files in the chosen directory. To navigate here, you can use the cursor-up and cursor-down keys, or the page-up and page-down keys to scroll one page. You can navigate very fast by pressing the first character of an entry.



Use the Function Keys to:

F1 - Display a Help Screen

F2 - Show information about the currently selected file or folder

F3 - Edit the currently selected file with the text/hex editor (see text/hex editor)

F4 - Make a new directory

F5 - Copy the currently selected file

F6 - Rename the currently selected file or directory

F8 - Delete the currently selected directory or file

F9 - Copy a file from the floppy to the current folder

F10 - Return to the main menu

3.2. The user manager

To work with a SAM, CIA Commander must know where it is located. First, navigate to your WinNT directory and press the space-key. The SAM will be initialized after pressing the space-key. After initialization, you will see on the left side all users which are present in the SAM. To navigate to a user, you can use the cursor-up and cursor-down keys, or the page-up and page-down keys to scroll one page. To select a key, please press the Enter-key.

On the right side of the screen, you will see your NT installation's build number and how SYSKEY is used. SYSKEY is a special feature to better protect passwords in Windows NT and Windows 2000. On the green window at the bottom, you will see detailed information about the selected user.

Use the Function keys to:

F1 - Display a Help -Screen

F2 - Save the password data to floppy. You can crack the password later on with CIA CommanderPWD.EXE

F3 - Change the selected user's password

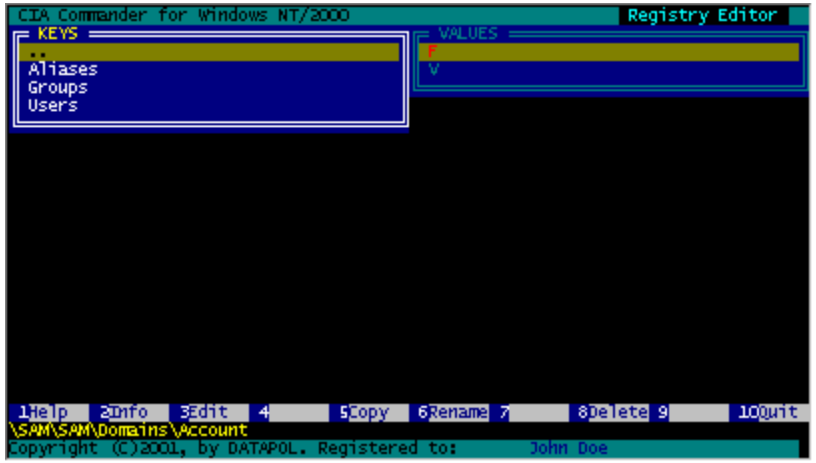
F6 - Restore a saved password from floppy

F10 Return to the main menu

3.3. The registry editor

To work with a registry, CIA Commander must know where it is located. First, navigate to your WinNT directory and press the space-key. The registry will be initialized after pressing the space-key. After initialization, you will see on the left side the registry's directory structure. To navigate to a key, you can use the cursor-up and cursor-down keys, or the page-up and page-down keys to scroll one page. To select a key press the enter-key. You do exactly the same to select a subkey.

With the TAB-key, you can toggle between keys and values. On the right side of the screen, you will see the values in the chosen key. To navigate here, you can use the cursor-up and cursor-down keys, or the page-up / page-down keys to scroll one page.



Use the Function Keys you to:

F1 - Display a Help Screen

F2 - Show information about the currently selected value

F3 - Edit the currently selected value in with the text/hex editor (see text/ hex editor)

F5 - Copy the currently selected key or value

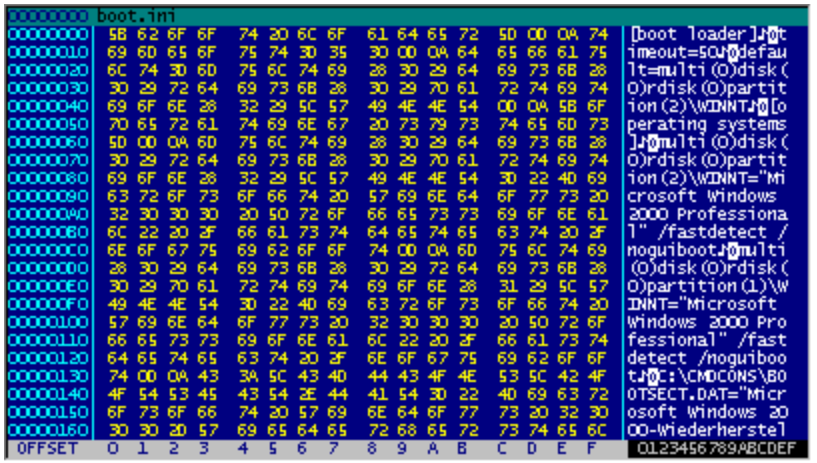
F6 - Rename the currently selected key or value

F8 - Delete the currently selected key or value

F10 - Return to the main menu

3.4. The text/hex editor

In the text/hex-editor you can view and edit files. To change between textmode and hexmode use the TAB-key. When you finished to work, press F10 to return to the main menu. A dialog will appear asking you if you want to save the changes.



We plan in the future to add support search and replace functions!

4. Common scenarios

Here are some scenarios where CIA Commander can help you to solve a problem:

1. The Boot.ini file was modified so that NT doesn't boot any more.

A wrong boot.ini file can exist after installing an additional hard disk or working with partitioning tools! To correct the problem, use the file manager within CIA Commander and edit the boot.ini with the text/hex-editor. Try to modify the disk and partition numbers until the boot-partition will be found again.

2. A service causes a blue-screen.

To disable a buggy service use the registry editor. Be carefulll, the subkey "Current Controlset" is not present. Use "Controlset001" instead. In the subkey services, change the start values of the service to disabled (3) or to manual (2).

At the next boot, the service will not start any more.

3. Accidentally deleted System File.

To recover a system file that was deleted, or perhaps infected by a virus, copy the needed file to a floppy. In the file manager you can copy the file to the hard disk.

4. A wrong GINA.DLL prevents you from logon to Windows.

Biometric devices or smartcard solutions might change the GINA.DLL settings in the registry. If the device doesn't work any more you can't logon any more. Use the registry editor in CIA Commander and navigate to software/Microsoft/WindowsNT/Winlogon, edit the entry GINA.DLL and change it to MSGINA.DLL. After reboot, you will find the original Windows logon dialog.

5. You forgot the Password of the administrator account.

Use the User Manager in CIA Commander and change the password. In any case, it is a good idea to store first of all the password to a file. Perhaps it is used for the start of services too! To save the original password use the F2 Function Key.

5. List of FAQ

Does CIA Commander support Windows 2000?

Yes. CIA Commander supports Windows NT4 and Windows 2000.

I lost the Administrator's Password. Will CIA Commander show me the Password?

No. With CIA Commander you can replace passwords for any user. If you need to know the password because it is also used in another application, an additional tool (availible soon) can show you the password in plain text.

Why should I buy CIA Commander instead of reinstalling the OS?

That question depends upon what is worth more. The time for reinstalling depends upon the system and the number of applications and services installed. However, in some situations, you can't reinstall everything because the backup might be to old. If your exchange server crashes for example, you could lose an important email! However, the biggest advantage of CIA Commander is, that you can still buy and use it, exactly when you really need it!.

Does CIA Commander support drives larger then 8GB?

Yes. CIA Commander supports large drives. Only the drives that are not supported by the BIOS (some SCSI-adapters) and partitions on stripe sets are not supported by CIA Commander.

CIA Commander might be a Security Risk for my Windows NT and Windows 2000 Computer. Is there any Protection against CIA Commander?

You are right. CIA Commander is a very dangerous set of tools if in wrong hands. With the features of the OS you can't protect against CIA Commander if physical access to PC exists! However, to protect your passwords from being changed or overwritten, you can visit http://www.datapol.net. You will find good security solutions for any requirement. Anyway, the usage of CIA Commander is strictly forbidden by law and License Agreement, if you are not the owner of the PC you want to use it or if you are not authorized to use it.

I get an Error Message while accessing my partition. What does this mean?

In most cases, the error message is caused by a not supported SCSI adapter or a damaged partition.

Try to start Windows NT in safe mode. This will cause a chkdsk. If the partition is still not accessible, try to mount the hard disk in a different computer. If chkdsk is still not working... you really have a problem.

I have a Read-Only-Version of CIA Commander. Where can I buy the full version and what does it cost?

You can buy CIA Commander in our online shop or at the resellers listet on our website. The CIA Commander's list price is US$249. Visit our website at http://www.datapol.net to see more details.

How many CIA Commander Licenses do I need?

CIA Commander is licensed per user. For each administrator in your company you need a separate CIA Commander license.

6. Conditions of Use / License Agreement

END USER LICENSE AGREEMENT FOR CIA Commander SOFTWARE

IMPORTANT - PLEASE READ CAREFULLY: this end user license agreement from Datapol is a legal contract between you (either as a natural or legal person) and the authors for the aforementioned SOFTWARE PRODUCT. By installing the SOFTWARE PRODUCT, you are accepting to be bound by the terms of this license agreement. If you do not accept the provisions of this license agreement, you are not authorized to install or use the SOFTWARE PRODUCT. If you have purchased the SOFTWARE PRODUCT, you may return it to the point of sale and obtain a full refund.

The SOFTWARE PRODUCT is protected both by copyright laws and international copyright agreements and by other laws and agreements on intellectual property. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANTING a license

The SOFTWARE PRODUCT is licensed as follows:
This SOFTWARE PRODUCT is licensed to be used by a single user at any point in time. A valid license must be purchased for each user of the SOFTWARE PRODUCT. This means if you have 5 administrators in your company and 2000 personal computer and each administrator will use the SOFTWARE PRODUCT you will need 5 licenses of the SOFTWARE PRODUCT even if they are not using the SOFTWARE PRODUCT at the same time.

* Installation and use: authors gives you the right to install and use copies of the SOFTWARE PRODUCT on your computers, on which validly licensed copies of the operating system for which the SOFTWARE PRODUCT was developed (e.g. Windows(r) NT, Windows 2000, Macintosh, etc.) are running. If several operating systems are running on the same computer, the licensee requires only one license.

* Backup copies: you are also entitled to produce copies of the SOFTWARE PRODUCT required for backup and archiving purposes.

2. DESCRIPTION OF FURTHER RIGHTS AND RESTRICTIONS

Retention of copyright statements: you are not entitled to remove or amend the copyright statements on copies of the SOFTWARE PRODUCT.

Sale: you are not entitled to sell copies of the SOFTWARE PRODUCT to third parties.

Ban in relation to reverse engineering, decompilation and disassembly: you are not entitled to reverse engineer, decompile or disassemble the SOFTWARE PRODUCT, unless and only insofar as the applicable law allows this, notwithstanding this restriction.

Hire: you are not entitled to hire, lease or lend the SOFTWARE PRODUCT.

Transfer: you are entitled to transfer all your rights arising from this license agreement, provided the recipient accepts the provisions of this license agreement.

Support services: authors may offer you support services in connection with the SOFTWARE PRODUCT ("support services"). The support services may be used in accordance with the provisions and programs of sellers, which are described in the user's guide, the online documentation and/or other material provided by Datapol

website. Any additional software code which you are given as part of these support services shall be seen as part of the SOFTWARE PRODUCT and be subject to the provisions of this license agreement. Authors entitled to use the technical data which you provide them with as part of the support services for commercial ends, including product support and development. Authors undertake to use such technical data on a purely anonymous basis within the meaning of the data protection act.

Observance of all applicable laws: you are obliged to use the SOFTWARE PRODUCT only in compliance with all applicable laws.

Usage of CIA Commander for hacking foreign computers is strictly forbidden! These license conditions allow usage of CIA Commander only on systems where you are the owner or you explicit got permission from owner to use CIA Commander on the computer.

3. TERMINATION

Irrespective of other rights authors are entitled to terminate this license agreement if you are found to be in breach of the provisions of this license agreement. In this case, you are obliged to destroy all copies of the SOFTWARE PRODUCT.

4. OWNERSHIP

Any ownership rights, including but not limited to copyright, in respect of and in relation to the SOFTWARE PRODUCT and any copy thereof, shall lie with the authors or its suppliers. Ownership rights and intellectual ownership in respect of and in relation to the content which is accessed through the SOFTWARE PRODUCT, shall lie with the relevant owner and may be protected by appropriate copyright or other laws relating to intellectual property. This license agreement does not give you any rights to such content. All rights not explicitly granted shall remain with the authors.

5. GUARANTEE EXCLUSION

Authors explicitly exclude any guarantee for the SOFTWARE PRODUCT. THE SOFTWARE PRODUCT AND ANY RELATED DOCUMENTATION ARE GIVEN TO YOU "AS IS", WITHOUT ANY FORM OF GUARANTEE, EITHER EXPLICIT OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED GUARANTEES OF SUITABILITY, APPROPRIATENESS FOR A SPECIFIC PURPOSE OR THE NON-EXISTENCE OF A VIOLATION OF THE LAW. THE TOTAL RISK ARISING FROM

USE OR PERFORMANCE OF THE SOFTWARE PRODUCT LIES WITH YOU.

6. LIMITED LIABILITY

Except for what is at most permitted by the applicable law, neither authors nor its suppliers can be held liable for any damage or subsequent damage, specific, accidental or indirect (including but not limited to lost profits, interruptions to operations, loss of commercial information or any other damage to property) which arises from the use of or inability to use the SOFTWARE PRODUCT or through the performance or non-performance of support services, including if authors have been notified in advance of the possibility of such damage. In any case the entire liability of authors remains limited to the amount which you have paid for the SOFTWARE PRODUCT, or to DM 10.-, whichever is the higher amount. If however you have entered into a support services agreement with authors, the entire liability of authors in relation to these support services shall be governed by the provisions of this agreement. As some states/ jurisdictions do not allow exclusion from or limitation of liability for subsequent or accidental damage, the above restriction may not apply there.