PASSWORD RECOVERY TOOLKIT

VERSION 5

USER GUIDE

ACCESSDATA™

Password Recovery Toolkit 5.0
User Guide

Password Recovery Toolkit by AccessData Corporation

Manual Version 1

Printed in the U.S.A.

The entire risk of the use or the result of the use of this software and documentation remains with the user. No part of this documentation may be reproduced in any means, electronic or mechanical, for any purpose, except as expressed in the Software License Agreement.

AccessData Corporation
2500 North University Avenue, Suite 200 • Provo, Utah 84604 • USA

Sales

(801) 377-5410
(800) 574-5199 (USA only)
Home page: www.accessdata.com
E-mail: info@accessdata.com

AccessData End User License Agreement

IMPORTANT: Read this before using your copy of AccessData ® Password Recovery Toolkit™.

CAREFULLY READ THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE ("LICENSE") TO USE THE PASSWORD RECOVERY SOFTWARE COMPACT DISC ("COMPACT DISC") AND DISKETTE ("DISKETTE") AND ACCOMPANYING PASSWORD RECOVERY USER DOCUMENTATION ("DOCUMENTATION") CONTAINED IN THIS PACKAGE (COLLECTIVELY REFERRED TO AS "YOU OR YOUR") AND ACCESSDATA, INCLUDING ITS SUCCESSORS OR ASSIGNS, (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES. IF YOU DO NOT WISH TO ENTER INTO THIS LICENSE, RETURN TO THE PLACE OF PURCHASE, UNUSED AND UNINSTALLED, FOR A REFUND OF THE PURCHASE PRICE LESS ANY APPLICABLE RETAILER HANDLING, RESTOCKING OR SERVICE CHARGES.

License Grant

Licensor hereby grants to You, and You accept, a non-exclusive license to use the Diskettes, including the password recovery software contained therein in object-code-only from ("Software"), and Documentation, only as authorized in this License. The Software may be used only on a single computer or local area network ("System") owned, leased, or otherwise controlled by You; or, in the event of the in operability of that system, on a backup system selected by You. Concurrent use of the program on two or more systems in not authorized without the advance written consent of Licensor and the payment of additional license fees. You agree that You will not assign, sublicense, transfer, pledge, lease, rent, or share Your rights under this License. You will not use this software for any form of services.

Upon loading the Software into Your system, You may retain the Diskettes for backup purposes. In addition, You may make one copy of the Software on a second set of diskettes for the purpose of backup in the event that the Diskettes are damaged or destroyed. Any such copies of the Software shall include Licensor's copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Program or any portions thereof may be made by You or any person under your authority or control.

Licensor's Rights

You acknowledge and agree that the Program consists of proprietary, published and unpublished property of Licensor, protected under United States copyright law and trade secret laws of general applicability. You further acknowledge and agree that all right, title, and interest in and to the Program are and shall remain with Licensor. This License does not convey to you an interest in or to the Program, but only a limited right of use revocable in accordance with the terms of this License.

License Fees

The license fees paid by you are paid in consideration of the licenses granted under this License.
Software Installation
It shall be your sole responsibility to install and make operational the Software on Your system. In the event you need installation assistance, such services may be available from Licensor at an additional cost to you.

Term

This License is effective upon your breaking of any of the seals on the package containing the Program, and shall continue until terminated. You may terminate this License at any time by returning the entire Program, including the Diskettes, Software and Documentation, and all copies thereof and extracts therefrom, to Licensor and by erasing all copies of the software that may be located on any systems owned or controlled by You; or upon which You know a copy of the Software has been placed. Licensor may terminate this License upon the breach by you of any term hereof. Upon such termination by Licensor, You agree to immediately return to Licensor the entire Program, including the Diskettes, Software and Documentation, and all copies thereof and extracts therefrom, and to erase all copies of the Software that may be located on any systems owned or controlled by You or upon which You know a copy of the Software has been placed.

Limited Warranty
Licensor warrants, for Your benefit alone, that the Diskettes in which the Software is embedded shall, for a period of ninety (90) days from the date of Your purchase of the Program (referred to as the "Warranty Period"), be free from defects in material and workmanship. Licensor further warrants, for your benefit alone, that during the Warranty Period the software shall operate substantially in accordance with the Documentation. If, during the Warranty Period, a defect in the Program diskettes or Software appears, You may return the Program to Licensor personally or by mail to AccessData, 560 South State Street Suite J-1, Orem, Utah 84058, with written instructions for replacement.

YOU AGREE THAT THE FOREGOING CONSTITUTES YOUR SOLE AND EXCLUSIVE REMEDY FOR BREACH BY LICENSOR OF ANY WARRANTIES MADE UNDER THIS LICENSE. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE PROGRAM, DISKETTES, SOFTWARE AND DOCUMENTATION ARE LICENSED "AS IS," AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
Limitation of Liability

LICENSOR'S CUMULATIVE LIABILITY TO YOU OR ANY OTHER PARTY FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS, OR ACTIONS ARISING OUT OF OR RELATING TO THIS LICENSE OR THE USE OF THE PROGRAM SHALL BE LIMITED TO REPLACEMENT OF THE PROGRAM AND, IN ANY EVENT, SHALL NOT EXCEED THE LICENSE FEE PAID TO LICENSOR FOR THE USE OF THE PROGRAM. IN NO EVENT SHALL LICENSOR BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS OR ANY SIMILAR CLAIMS, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Indemnification
You accept full legal responsibility for all password recovery performed through your use of the Program. You agree to hold harmless and indemnify Licensor for any and all demands, claims, legal action and damages, including all attorney's fees and costs, against Licensor which arise out of Your use of the Program. In any legal action regarding the indemnification contained in the paragraph 7, the prevailing party shall be entitled to recover from the non-prevailing party all of its attorney's fees and costs. Password recovery and the subsequencial data decryption of unauthorized or otherwise illegally obtained files may constitute theft and may result in your civil and criminal prosecution.

Governing Law
This License shall be construed and governed in accordance with the laws of the State of Utah. The competent Federal or State court situated in Salt Lake City, Utah shall solely adjudicate any dispute arising out of or with respect to this License between You and Licensor. You and Licensor consent to the venue and jurisdiction of such court for purposes of any such dispute.

Severability
Should any court of competent jurisdiction declare any term of this License void or unenforceable, such declaration shall have no effect on the remaining terms hereof.

No Waiver
The failure of either You or Licensor to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breach.

Commercial Use
The software may be used for non-commercial purposes only, wherein commercial purposes include but are not limited to use of the Software for the benefit of another whether or not compensation is received for such use. For business users, the Software may be used for any non-commercial purpose within a single corporation, institution, government agency, business, or other single entity for the benefit of that corporation, institution, government agency, business, or entity only.

Table of Contents

Introducing Password Recovery Toolkit

General Information

Thank you for purchasing AccessData's Password Recovery Toolkit. This software allows an organization or individual to use passwords, confident in the knowledge that passwords which are lost can be retrieved. AccessData can recovery passwords in a variety of applications including the following:

Microsoft Word
QuickBooks
DataPerfect
Quicken
Schedule
PGP

Ami Pro
ACT
Paradox
Organizer
Word Pro
PkZip
Windows NT

Approach
PFS Write
Microsoft Access
Ascend
Q&A
Novell NetWare

WordPerfect
Lotus 1-2-3
Quattro Pro
Microsoft Excel
Microsoft Money

With the ability to recover passwords in most of the major spreadsheet, word processors, and database programs, the Password Recovery Toolkit allows you to avoid a crisis before it happens.

What's new for investigators?

With the forensic investigator in mind AccessData has added some additional features to the toolkit. All of these options are explained in detail in other sections of the help file.
Bio Profile
Expanded Personal Dictionary
Auto Scans of Drives
Multiple Hash Options
Expanded Report Options
Increased number of file types identified

AccessData's research and development department is constantly working on new products. If you have any need for a file recovery that is not in the toolkit please feel free to contact AccessData.

Registration

Enclosed with your toolkit is an AccessData product registration card. It is very important that you fill out this card completely, and return it to AccessData. This card is AccessData's only way of identifying you as a legitimate user. This is for your protection as the end user. AccessData will not administer technical support and upgrade eligibility until after the registration card for the product has been returned. If you would like AccessData to keep a record of your access code please write it in the PIN area on your registration card.

Registration can be sent in via the mail system, fax at (801) 377-5426, or go online to http://www.accessdata.com

Guarantees for Recovery Rate

AccessData stands behind every product that it sells. If one of the modules does not recover your password, then please call AccessData, and as stated in the return policy AccessData will exhaust its resources in order to recover your data. However, with the difficulties in some of the better encryption techniques, AccessData can only guarantee certain module versions 100%. None of AccessData's brute force modules are 100% guaranteed due to the nature of the attack used to recover the password. If you have any questions regarding this policy please contact AccessData.

Product Returns

AccessData has a strict return policy due to the nature of the products. The return policy of AccessData follows directly along with the license agreement stated at the begining of this manual. If the Password Recovery Toolkit is unable to recover a password, the following will apply. If this incidence does occur, a copy of the unrecoverable file MUST be sent to AccessData, and the file will be worked on directly by AccessData's engineers. At this time, if a password is recovered, the owner of the Utility will be both able to keep the module, and receive the password to the file or a return can be made and the end user will need to pay for the in-house recovery in order to receive the password. If AccessData is unable to recover the password, a return in full will be made on the Utility minus the shipping charges. If the Utility is unopened and there is no online transfer done of the program, it can be returned at any time within 60 days of purchase.

Upgrades & Subscriptions

Upgrades

If you have purchased a utility in the past 45 days, and AccessData upgrades the product that you purchased, then you are eligible for an upgrade of that product free of charge. In order for a free upgrade to be acquired your product must be registered, and the date of purchase must be called into AccessData within the first 45 days after purchase.

Subscriptions

A yearly subscription is now offered on all of AccessData's password Recovery Modules and toolkits. The subscription price is 50% off the retail price of the module or toolkit for an entire year's worth of upgrades. A subscription is good for one year's time from the date of purchase. The password recovery subscription allows you the ability to download updates from AccessData's Web site at any time, and quarterly CD-ROM updates will also be sent out. All users can go and take a look at the general features of the subscription site by going to http://www.accessdata.com.

Contact Information

AccessData Corporation can be reached at the following address, phone, fax and e-mail from 8 A.M. to 5:00 P.M. MST.

AccessData Corporation
2500 North University Ave. Suite 200
Provo, UT 84604-3864

Phone: (801) 377-5410 or call us toll free at (800) 574-5199
Fax: (801) 377-5426

E-mail: info@accessdata.com

Web site: http://www.accessdata.com

Getting Started

System Requirements

Password Recovery Toolkit requires Windows 95 or later to run including Windows NT. Therefore, systems that can run those operating systems will run Password Recovery Toolkit. Here are some guidelines.

Hardware/Software	Minimum
Processor	Intel 486 33Mhz
RAM	32 MB
Hard-Disk Space	15 MB
Operating systems	Windows 95, Windows 98, Windows NT 4.0
3.5-inch diskette drive	High-Density
CD-ROM drive	4x speed
Monitor	VGA compatible

Processor speed is the component that most effects the password recovery time. For best results use a machine with the fastest processor available.

Installing Password Recovery Toolkit

Installation of the Password Recovery Toolkit is very simple. To install the toolkit on your Windows 95, Windows NT, or Windows 98 machine please follow one of the following options.

Installation Option 1

1. Insert the Password Recovery Toolkit CD-ROM into your CD-ROM drive.

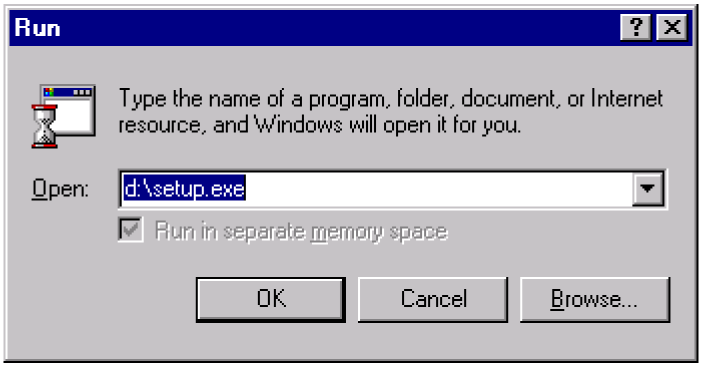
   When you insert the CD-ROM into your CD-ROM drive, the installation program automatically starts.

2. Follow the on-screen installation instructions.

Installation Option 2

If your computer does not have auto play enabled or setup fails to start automatically follow these steps:

1. Insert the Password Recovery Toolkit CD-ROM into your CD-ROM drive.
2. Click on the Windows Start button, and then choose the Run… from the Start menu.
3. Once the Run dialog has appeared, type "D:\setup.exe" on the open dialog line.



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: d:\setup.exe

☑ Run in separate memory space

Now click the OK button to continue in the installation process. Make sure that the drive letter used above reflects the drive path for your CD-ROM drive.

4. Follow the on-screen installation instructions.

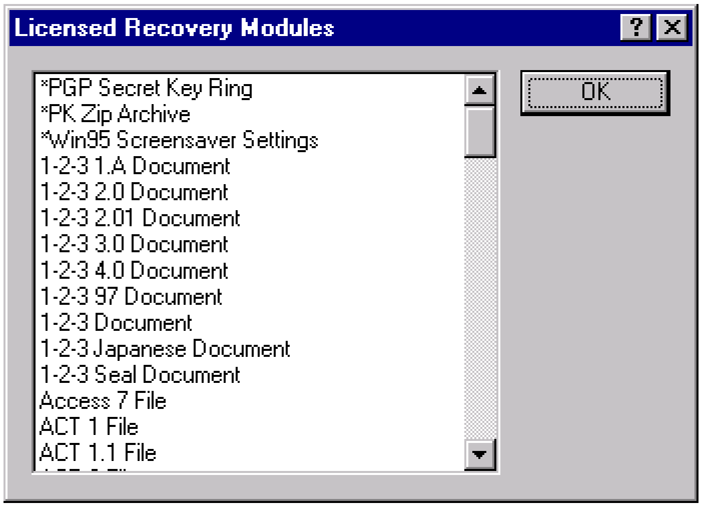
Using Password Recovery Toolkit

Using the License Diskette

The license diskette is created in-house by AccessData and is the green diskette located in your product packaging. This license diskette cannot be copied so no backup copy can be made. If a problem arises with the license diskette, a temporary copy of the program can be rushed to you via e-mail or ftp until the problem is resolved.

The license diskette is the key to your Password Recovery Toolkit and must be present in the 3.5-inch floppy drive whenever the toolkit is executed. Each time the license diskette is used, the license information is loaded into your toolkit. Please be patient as this can take a few minutes.

To view which modules you have active go to the Help menu option and choose Licensed Recovery Modules. All modules listed with an asterisk character are free modules offered with AccessData's compliments.


Licensed Recovery Modules

*PGP Secret Key Ring
*PK Zip Archive
*Win95 Screensaver Settings
1-2-3 1.A Document
1-2-3 2.0 Document
1-2-3 2.01 Document
1-2-3 3.0 Document
1-2-3 4.0 Document
1-2-3 97 Document
1-2-3 Document
1-2-3 Japanese Document
1-2-3 Seal Document
Access 7 File
ACT 1 File
ACT 1.1 File

Starting Out

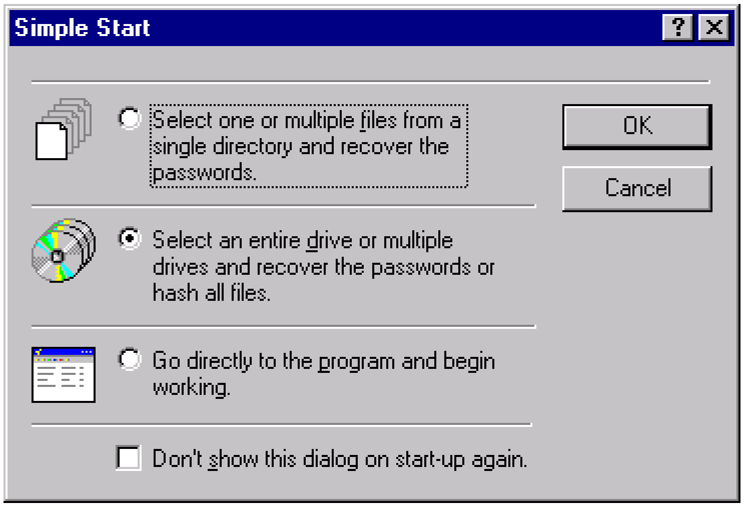
Setup Options
There are general features in your Password Recovery Toolkit that are set in your Options dialog. There are numerous items that can be changed including: Startup, Language, Simultaneous recoveries, recovery dialog preference and backup time. AccessData has set the defaults for these options for the optimal performance of an average user of the Password Recovery Toolkit.

Columns
The PRTK Main window appears and is automatically set to display all columns. To add or remove columns, click the View menu option and then chose Columns.

You can sort the columns using the column headings at the top of the windows. The toolkit default is set to sort by file name. Clicking on another column heading will sort on that column. If you would like to sort by a secondary column, click on another column. All columns being used for sorting are marked with a 1 for primary sort column or a 2 for secondary sort column and an up or down arrow (representing ascending or descending sort). The most recent column you clicked will be the primary sort column for the toolkit.

Toolkit Recovery Features

Simple Start



Simple Start

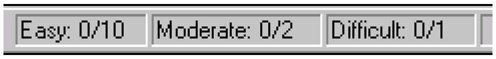
○ Select one or multiple files from a single directory and recover the passwords.

● Select an entire drive or multiple drives and recover the passwords or hash all files.

○ Go directly to the program and begin working.

☐ Don't show this dialog on start-up again.

There are three options for starting the recovery of your files. The first time you launch Password Recovery Toolkit, a window appears that allows you to choose different ways to add your file or files for recovery. All of these options that are available in the simple start are also available through shortcut buttons on the top of the toolkit's main screen.
With all of the simple start options a general feature of the toolkit is to make a classification on the file of Easy, Medium, and Complex. These classifications are determined by the potential recovery time. Most files are classified as Easy and take anywhere from a few seconds to a couple hours to recover. Medium files are files that will take between 24–48 hours to recover, and complex files take potentially 48 hours or more for recovery time. These classifications will determine the ratios in which the files are analyzed. The number of files in each classification will appear on the bottom of the main program screen as well as the default ratios.



Easy: 0/10 | Moderate: 0/2 | Difficult: 0/1

Option 1 "Select one or multiple files from a single directory and recover the passwords."

This option should be used when you only want to recover one file's password or are dealing with any number of files that exist in a single directory.

To select a single file for recovery, highlight the file and then chose Add.

To select multiple files for recovery you can chose one of the following options:

1. Highlight a single file, then press Ctrl-A on your keyboard. The rest of the files in that directory will also then be highlighted. Click Add.

2. Hold the Ctrl key and drag your mouse over the files in the directory that you would like to recover. Then click Add.

Once the files are chosen, there are multiple actions that can be done on the files. Before adding the files to the main recovery screen, a variety of options appear on the bottom of the Select Files screen. Those options include Recover Passwords (the default), Determine File Types, or the Hash Files. For an explanation on the Profile option please refer to Dictionary Profiles. (Page 12)

Option 2 "Select an entire drive or multiple drives and recover the passwords."

This option should be used when you want to analyze an entire drive, multiple drives, or portions of a drive or drives.

To select an entire drive for recovery, click on the drive letter that you would like to analyze. You will know that the check mark and plus sign select the drive (☑▭) that appear next to the drive. If the check mark is grayed (☑▭) then the drive is selected, but you have only some of the sub directories on that drive are selected.

Once the files are chosen there are multiple actions that can be done on the files. Before adding the files to the PRTK Main window, a variety of options appear on the bottom of the Select Files screen. Those options include Recover Passwords (the program default), Determine File Types, or Hash Files. For an explanation on the Profile option please refer to Brute Force Attacks.

Option 3 "Go directly to the program and begin working."

This option is available when you want to drag-and-drop files using your desktop or your Windows Explorer. Simply highlight and drag the files to the PRTK Main Recovery window. Once the files are chosen, there are multiple actions that can be performed on the files. Before adding the files to the Main Recovery window, a variety of options appear on the bottom of the Select Files screen. Those options include Recover Passwords (the program default), Determine File Types, or Hash Files. For an explanation on the Profile option please refer to Brute Force Attacks.

If don't wish to see the simple start screen during each startup check the box in the lower left-hand corner that says "Don't show this dialog at start-up again." The simple start option can also be disabled in the View menu item under Options.

Hashing Files

The hashing file option available in the file actions is mainly for use by the computer investigator to verify that the contents of the file were not changed during the recovery of the password. The toolkit allows the use of two different hash methods: the Secure Hash Algorithm (SHA) or Message Digest 5 (MD5) . Both of these hashes are automatically performed when any recovery is done on a file unless the hash feature is disabled. Once the hash of a file is complete, a verification of the hash can be done. If the hash verifies as identical, then a message appears next to the key graphic, stating that the hash has not changed. If the hash is not the same, a report is generated, showing the two hashes, the date, and time the report was generated, and the path name to the file.

Security Features

AccessData recognizes the sensitive nature of the Password Recovery Toolkit. For this reason, AccessData has incorporated several security measures into all of the Password Recovery Modules.

Access Codes

The assigning of an access code to your license diskette gives you the ability to control the use of the Password Recovery Toolkit. If you forget your access code, there is no way of retrieving that information. Please contact AccessData at (801) 377-5410 if you have forgotten your access code. Your access code should be written in the PIN section of your registration card so that AccessData has a record of the code.

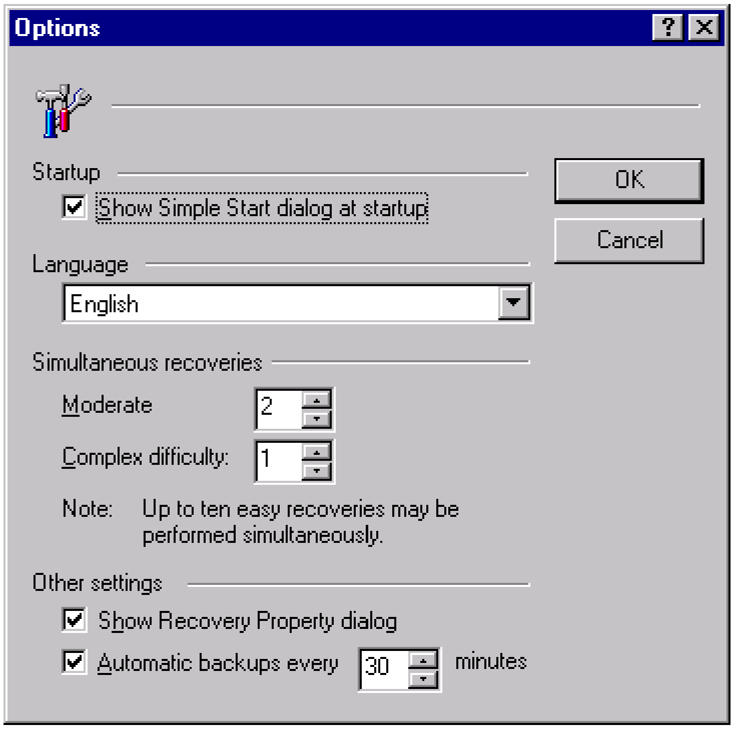
Security Characters

AccessData realizes that unauthorized use of Password Recovery Toolkit may be a concern for some. For this reason, AccessData has designated certain characters as security characters. If a security character is included in the password, the Password Recovery Toolkit will not reveal the password. For most applications (i.e. WordPerfect, Microsoft Word, Lotus 1-2-3, Quattro Pro, etc.) the security character is the underscore character "_". Using a security character gives you the ability to completely secure certain documents against unauthorized access. AccessData can only retrieve passwords that contain security characters, in-house. If you are interested in additional security measures, please contact AccessData and ask what they recommend for your data.

Changing your License Diskette Password

AccessData has added the ability for the end user to change the password that is stored on the license diskette. This password should be changed in the event that the password was released to unauthorized personnel. The only way to change the password that is recorded on the license diskette is to know the current password. If the current password is known, the user can click the Edit menu, then choose the Change Password Option.

Options



Startup

☑ Show Simple Start dialog at startup

Language

English

Simultaneous recoveries

Moderate 2

Complex difficulty: 1

Note: Up to ten easy recoveries may be performed simultaneously.

Other settings

☑ Show Recovery Property dialog

☑ Automatic backups every 30 minutes

The Options dialog box is located under the View menu item under Options.

Startup Options

When the Password Recovery Toolkit begins, you have two options that can be chosen for beginning recoveries. The default for the toolkit is for the Simple Start dialog to be active. If the Simple Start dialog is not active whenever the toolkit is launched, the program automatically goes to the PRTK Main Recovery window.

Language Options

The Password Recovery Toolkit automatically defaults to display all functions and text of the toolkit in English (U.S.). If you would like to change the language option, click the arrow key and highlight the language you want to use.

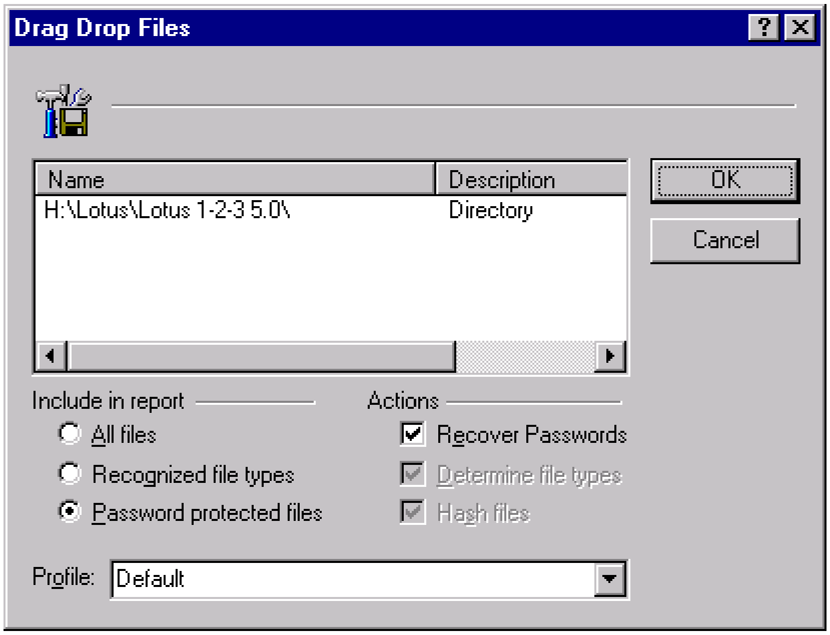
Simultaneous Recoveries

All of the passwords recovered by the Password Recovery Toolkit are automatically categorized as Easy, Medium, and Complex. An unlimited number of Easy files can be run at any given time. However, a default number is set for the medium to complex recoveries. A maximum of two complex recoveries and three medium recoveries can be chosen to run at one time. AccessData recommends that if more then one complex recovery is chosen then only one medium should be chosen at the same time. All recoveries in progress can be paused at once by clicking on the Pause All Recoveries button located on the main toolkit screen the pause button is highlighted in red. To resume the recoveries click on the pause button on the main recovery screen highlighted in green.

General Settings

Two main options are located under the general setting section: Show recovery dialog and automatic backup options. The first option of showing the recovery dialog is chosen if you want to have the individual recovery screen appear automatically when a file is recovering. The second option of automatic backups is set to 30 minutes. The PRTK Main Recovery screen will be saved every 30 minutes showing all of the files that were recovered at that time. It will not save the status of any file not recovered.

Actions



Name	Description
H:\Lotus\Lotus 1-2-3 5.0\	Directory

Include in report

○ All files
○ Recognized file types
● Password protected files

Actions

☑ Recover Passwords
☑ Determine file types
☑ Hash files

Profile: Default

Recover Passwords Action

This action allows you to recover the passwords on any file that you have selected for recovery. The toolkit automatically defaults to having the Determine File Types and hash Files action used when using the Recover Passwords Action is chosen. This action can be used with any of the options in the Include in report options.

Determine File Types Action

This action tells you how the Password Recovery Toolkit best identifies your file or files. The only way to use this option is the have the All files selected in the Include in report options.

Hashes

Hash Files Action

This action performs a simple hash on the files that are chosen. A hash is mainly a function used for authentication. Since changing a single bit in a file with result in a completely different hash. The hash features are mainly used for investigations to prove the file was not altered. The Hash Files option can be used when any of the Include in report options are selected, and can be used with the Determine File Types action without using the Recover Passwords action.

Secure Hash Algorithm (SHA)

The National Institute of Standards and Technology designed the Secure Hash Algorithm. SHA takes as input an arbitrary-length file and output a fixed-length number referred to as a "hash" or "digest." The number is derived from the input in such a way as to make it computationally infeasible to derive any information about the input from the hash. It is also computationally infeasible to "generate a collision," or find another file that will produce the same output.

Message Digest 5 (MD5)

Ron Rivest of RSA designed the Message Digest 5. MD5 takes as input an arbitrary-length file and outputs a fixed-length number referred to as a "hash" or "digest." The number is derived from the input in such a way as to make it computationally infeasible to derive any information about the input from the hash. It is also computationally infeasible to "generate a collision," or find another file that will produce the same output.

General Information

Brute Force Attacks

There are a few of AccessData's modules that use a recovery process known as a brute force attack. These modules will go through series of different passwords. The brute force attacks can go through thousands of passwords every minute until the correct password is determined. Because of the special nature of the brute force attacks, AccessData recommends a minimum running time of 72 hours before contacting AccessData.

Microsoft Word & Excel version 8.0 (Office '97)

When the 8.0 versions of Word and Excel were released, they were found to use an encryption algorithm called RC4. The use of the more difficult encryption caused AccessData to develop a brute force attack to recover the passwords. Brute force attacks are not as reliable as the previous analytical methods used to recover the passwords so some added features have been included in the toolkit. The ability to create biographical dictionaries or the option to create profiles of multiple dictionaries can now be used in the attack.

Ami Pro

Ami Pro uses a brute force attack to recover the password because of the method that was used in the storing of the password. Most Ami Pro recoveries can take between one hour and four days. Ami Pro can also use dictionaries to aid in the retrieval of the password. The more specific information that can be chosen for use in the attack, the better the chances for recovery.

PkZip & PGP

Both program attacks are offered free with the purchase of any of AccessData's software. Both use brute force attacks to recover the passwords, and can take a substantial amount of time to do the recovery.

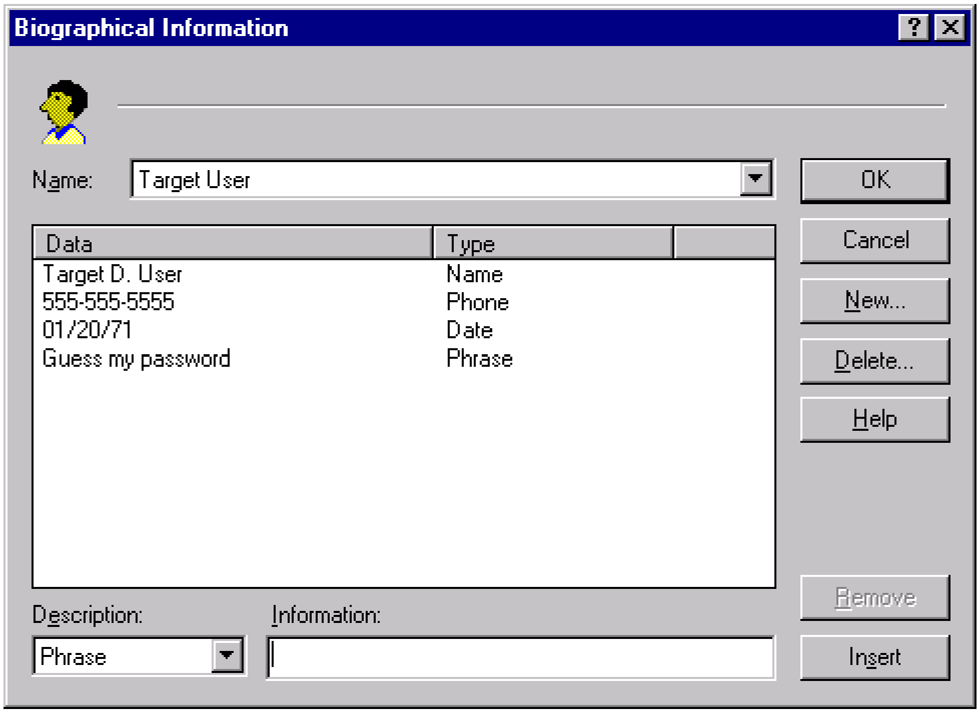
PkZip must have at **minimum of five files** in the archive in order for the PRTK to identify and begin recovery of the file. If there are less than five files in the archive an error message of "Not Enough Data" will appear on the screen.

PGP is very time intensive to recover the password and can take up to 254 days or more depending on the machine that is running the toolkit to completely go through the default dictionary included in the PRTK. We do recommend that you limit the dictionaries to very relevant information when using the PGP engine.

Biographical Dictionaries

Most typical passwords used with general applications usually contain some information on the individual who locked the file. All of the dictionary options available with the toolkit can be accessed through the short cut buttons at the top of the main screen or through the Tools menu option. With this in mind the ability to store this information and use it to break the password is invaluable. The Password Recovery Toolkit allows each user to take this information and create a special dictionary attack that contains all of this personal data.

To "Setup Biographical Information" click on the short-cut button with the profile of a person on it. There are multiple approaches that can be taken when setting up a biographical profile on an individual. The toolkit gives you the most general suggestions in the Description area of the Biographical Information screen. However, it is entirely up to you as the end user as to how specific the information can be. To set up a bio profile, put the name of the profile in the Name box at the top of the screen. Once the profile is named you may begin to add information. To add information to the profile, choose the general item that you would like to use in the description box and then type the appropriate specific information in the information box. Then click the Insert command. Multiple biographical profiles can be made and used together by setting up and then adding them in the dictionary profiles section of the toolkit. All biographical dictionaries are saved in the AccessData directory that is set up during installation under the Dictionaries sub folder.



Biographical Information

Name: Target User

Data	Type
Target D. User	Name
555-555-5555	Phone
01/20/71	Date
Guess my password	Phrase

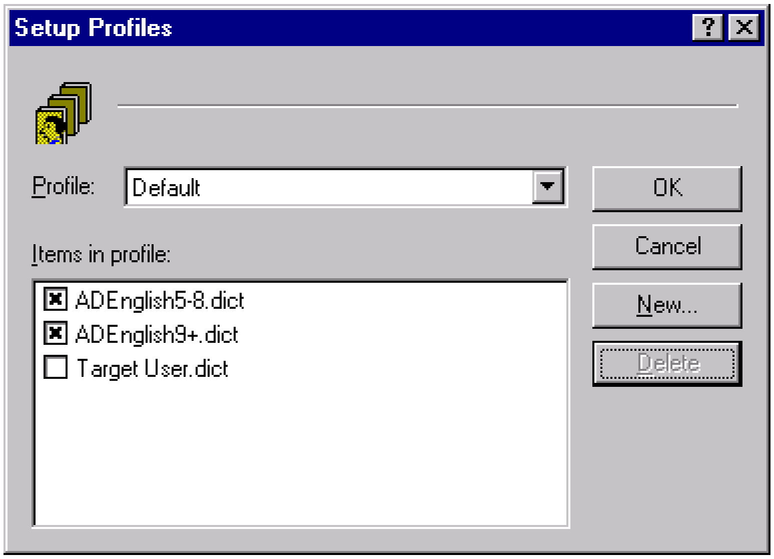
Description: Phrase

Information:

Dictionary Profiles

The Password Recovery Toolkit accepts dictionary files in a text format and can be added into the recovery mechanism. You can format any dictionary file in a word processor as long as it is saved as a text file separated by a hard return.

To "Select Dictionary Profile," the user must go to the short cut button with the picture of the books profile on it. The dictionary profile is automatically set to Default, which only uses the English dictionary file that is included with the installation of the toolkit. All dictionaries that are being used by the toolkit must be in the AccessData directory that is set up during installation under the Dictionaries sub-folder. Once the dictionaries are in the appropriate sub-folder, they can be added to any dictionary profile. To add a new profile, click on the New button located at the right of the Setup Profiles screen. Type a name for the profile, and then click in the box on the left of the dictionary to select it. To add a profile to a file, click on the area at the bottom of the select file or select drive screens and chose the profile desired from the list.



Profile: Default

Items in profile:

- ☒ ADEnglish5-8.dict
- ☒ ADEnglish9+.dict
- ☐ Target User.dict

Use of the Dictionaries

After the information is entered, the program scrambles that information into different possible passwords. Every dictionary attack goes through at least 40 different scrambles for the recovery of the password. Each dictionary stage is also permutated within the stage in increase the number of passwords being tried against the file password. Please note that the default dictionaries used by the toolkit are broken into two files: one will test passwords up to eight characters and the other file will test nine-character passwords and above.

AccessData has multiple dictionaries available on line at
http://www.accessdata.com/dictionaries.html

Personal Dictionary Description Suggestions

Names: first names, last names, middle names, nicknames, family names, pets names
Numbers: Driver's license number, employee ID number, license plates, bank accounts
Words: religion, cars, hobbies, birth place, company, favorite colors, music groups
Date: birthdays, anniversaries, commencements

RC4

RC4 is a variable-key-length stream cipher designed by Ron Rivest of RSA. Stream ciphers are key-dependent pseudo-random number generators whose output is XORed with the data: <plaintext> XOR <random-looking stream> = <random-looking ciphertext>. Since XOR is symmetric (i.e. [AXOR B] XOR B = A), XORing the ciphertext with the stream again will get back the plaintext. Microsoft Word and Excel use RC4 and a 40-bit key to encrypt their files.

Passwords

Multiple Passwords

The Password Recovery Toolkit was designed to recover all types of passwords that can be assigned in any application with a few exceptions. The exceptions are with Microsoft Access is limited too only recovering the main database password and not the user passwords or permissions.

With Lotus Approach module will recover multiple passwords for each file in most cases. Because of the method that the encryption is stored the Approach module recovers a list of passwords that have been used on any particular file. The list of passwords that the module recovers is the history of passwords used on this particular file. One of these passwords will open the file, but you will need to attempt to open the file to determine which is the correct password.

Unique Passwords

Some of the password recovery modules do not recover the original password that was used to lock the file. The Paradox module is a good example of this because it returns a password that is a string of numbers. This string of numbers acts just like a spare key to your car or home; it unlocks the document even though it is not the original password. Other modules also recover passwords that are a combination of alphanumeric characters. These passwords act as spare keys, so before calling technical support, please be sure to try the password that was recovered by the module. If, after trying the password, it does not unlock the document, please contact AccessData.

International Passwords

In today's marketplace, it is not uncommon for even some of the smallest companies to do business in the international arena. Since most programs are used extensively both in North America and internationally, the password recovery modules are capable of recovering documents locked with international characters such as ë and ñ. AccessData has been used successfully to recover documents created in French, German, Italian, Spanish, and Portuguese. All of the Password Recovery Modules are able to recover passwords written in other languages, but there is no guarantee as to the accuracy of this recovery in languages other than English. The Utilities are able to recover foreign passwords due to the frequency of the characters in the English language compared to the frequency of the characters in the foreign language. Passwords that have been locked with an international character are returned in the form of a mapping code.

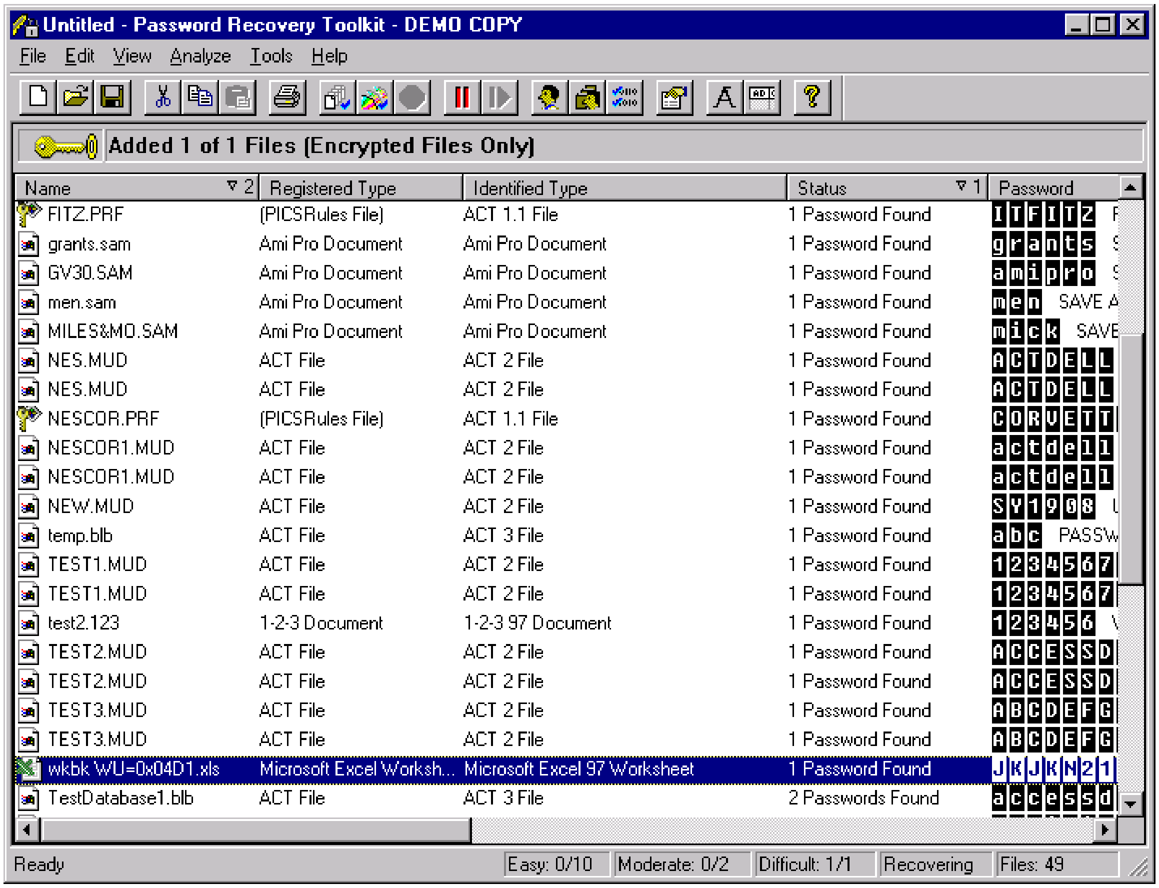
If a password recovered has a character that is not found on a standard keyboard, the module returns a mapping code. For example if the password: "dêrek" was used to lock a WordPerfect document, the WordPerfect Module would return

[D[Map-42]REK]

To retrieve this password, at the password prompt enter "d [ctrl]2 1,42 [Enter] rek". In most cases, if a map character is returned in the password you will need to contact AccessData for the best method of entering your password. If you still have problems gaining access please contact AccessData.

Password Recovery Toolkit Interface

PRTK Main Recovery window



Added 1 of 1 Files (Encrypted Files Only)

Name ▽ 2	Registered Type	Identified Type	Status ▽ 1	Password
FITZ.PRF	(PICSRules File)	ACT 1.1 File	1 Password Found	ITFITZ F
grants.sam	Ami Pro Document	Ami Pro Document	1 Password Found	grants S
GV30.SAM	Ami Pro Document	Ami Pro Document	1 Password Found	amipro S
men.sam	Ami Pro Document	Ami Pro Document	1 Password Found	men SAVE A
MILES&MO.SAM	Ami Pro Document	Ami Pro Document	1 Password Found	mick SAVE
NES.MUD	ACT File	ACT 2 File	1 Password Found	ACTDELL
NES.MUD	ACT File	ACT 2 File	1 Password Found	ACTDELL
NESCOR.PRF	(PICSRules File)	ACT 1.1 File	1 Password Found	CORVETT
NESCOR1.MUD	ACT File	ACT 2 File	1 Password Found	actdell
NESCOR1.MUD	ACT File	ACT 2 File	1 Password Found	actdell
NEW.MUD	ACT File	ACT 2 File	1 Password Found	SY1908 U
temp.blb	ACT File	ACT 3 File	1 Password Found	abc PASSW
TEST1.MUD	ACT File	ACT 2 File	1 Password Found	1234567
TEST1.MUD	ACT File	ACT 2 File	1 Password Found	1234567
test2.123	1-2-3 Document	1-2-3 97 Document	1 Password Found	123456 V
TEST2.MUD	ACT File	ACT 2 File	1 Password Found	ACCESSD
TEST2.MUD	ACT File	ACT 2 File	1 Password Found	ACCESSD
TEST3.MUD	ACT File	ACT 2 File	1 Password Found	ABCDEFG
TEST3.MUD	ACT File	ACT 2 File	1 Password Found	ABCDEFG
wkbk WU=0x04D1.xls	Microsoft Excel Worksh...	Microsoft Excel 97 Worksheet	1 Password Found	JKJKN21
TestDatabase1.blb	ACT File	ACT 3 File	2 Passwords Found	accessd

Ready | Easy: 0/10 | Moderate: 0/2 | Difficult: 1/1 | Recovering | Files: 49

The PRTK Main Recovery window allows you to view all the files that have been analyzed by the Password Recovery Toolkit at one time. Each screen can be saved or printed, or you can start a new document depending on your preference. The status of all of the toolkit actions that can be preformed from the PRTK Main Recovery window appears below the shortcut buttons on the Main window. Main window.

Saving the PRTK Main Recovery window

To save the PRTK Main Recovery window, go to the File menu and chose Save or Save As, and type the name of the file in the field. The information on the PRTK Main Recovery window will be saved to this file and can be opened by any word processor. The short cut Save option located at the top of the Main Recovery window will also save it to a file.

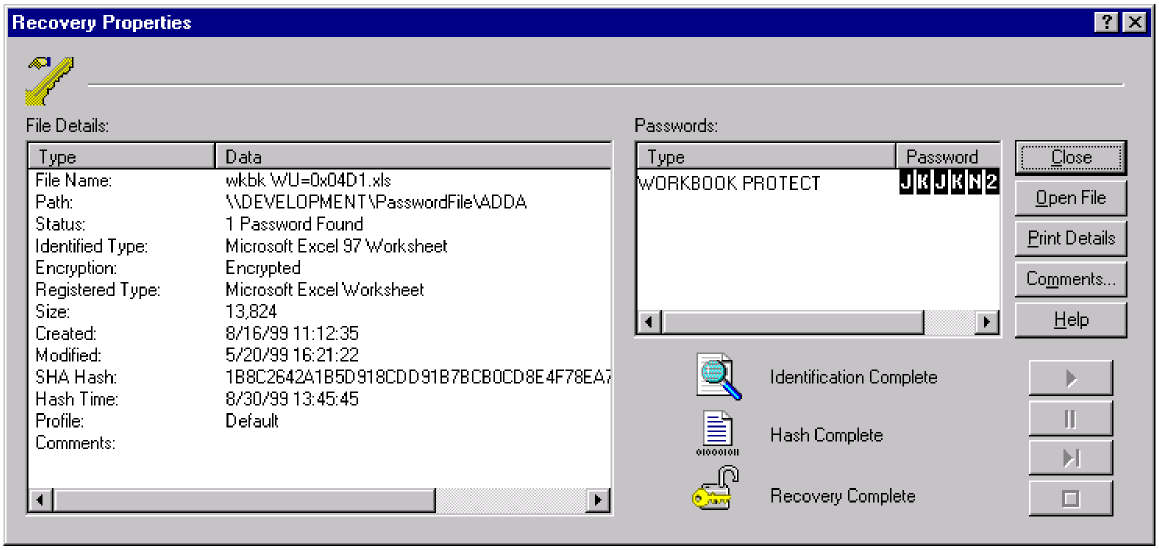
Printing the PRTK Main Recovery window

To print the PRTK Main Recovery window, go to the File menu command select Print. If you would like to preview the document then chose the Print Preview command instead. All of the column information that is active on the window is printed. The short-cut print option located at the top of the Main Recovery window will also print the main recovery screen.

New Document

To have a new document appear for the main recovery screen go to the File menu command select New. The short cut New option located at the top of the main screen will also open a new document.

Recovery Properties



Recovery Properties

File Details:

Type	Data
File Name:	wkbk WU=0x04D1.xls
Path:	\\DEVELOPMENT\PasswordFile\ADDA
Status:	1 Password Found
Identified Type:	Microsoft Excel 97 Worksheet
Encryption:	Encrypted
Registered Type:	Microsoft Excel Worksheet
Size:	13,824
Created:	8/16/99 11:12:35
Modified:	5/20/99 16:21:22
SHA Hash:	1B8C2642A1B5D918CDD91B7BCB0CD8E4F78EA7
Hash Time:	8/30/99 13:45:45
Profile:	Default
Comments:	

Passwords:

Type	Password
WORKBOOK PROTECT	JKJKN2

Identification Complete

Hash Complete

Recovery Complete

The Recovery Properties dialog was designed to show all of the information that can be viewed on a single file on one screen. In the Type column of the Recovery Property screen, a list of all the columns that were activated appears with the coordinating information next to it in the Data section. The additional option of Comments can be found on the right side of the screen for any special information that needs to be stated on the file. If comments are entered on the file, that information is also printed with the Print Details option.

When the recovery is in progress and you need to see the Recovery Properties, highlight the file and double-click its name. In the bottom right box, a graphic appears, showing that the recovery is in progress. In the lower left box, the password type and password are listed. Please note that all passwords recovered by the password recovery toolkit are case sensitive.

NWACCESS

Introduction to NWAccess

The NetWare Access Utility is a password modification utility for use with Novell NetWare versions 3.x through 4.x file servers. The intent of this utility is not to bypass file server security, but to allow continued access to file server services in the event of an unknown Supervisor/System Administrator password.

In order for NetWare to maintain a secure operating environment, the operating system requires that any user who wishes to change his/her password first type in his/her old password. End Users that are logged into a server as SUPERVISOR or with a user name that is supervisor equivalent are allowed to change the password for any user without knowing the previous password. In some cases however, it is not possible to login as SUPERVISOR or as a SUPERVISOR equivalent user. At these times, the NetWare Access Utility can be of assistance because it requires only that you have physical access to the file server in order to change the password of any user, including that of the SUPERVISOR.

Registration

It is very important that you register your copy of NWACCESS as soon as possible to make you eligible for technical support, and to give you access to the Utility. In order to register, the enclosed release form/registration card must be filled out completely and returned before an access code can be given.

Please note that there are spaces for TWO signatures on the release form. Due to the sensitive nature of NWACCESS, AccessData requires TWO signatures on the registration form. (One of the user and one of management) Both signatures must be present before an access code will be given.

As soon as the information on the registration card is complete, return the card to AccessData at the address listed below. If there is an urgent need for the program, you may fax the registration card to AccessData and send the original through the mail.

AccessData Corporation
2500 North University Avenue Suite 200
Provo, Utah 84604-3864
TEL (801) 377-5410   FAX (801) 377-5426

AccessData will record your registration information in their database, at which time you may call and obtain the access code that allows you to modify user passwords with NWACCESS. This access code will not be given until registration is complete, and you must call in for your access code.

Loading NWAccess

NWACCESS runs on top of NetWare 3.x or 4.x as a Network Loadable Module (NLM). In order to load any NLM, you must be at the file server, or you must be able to view and control the server remotely through RCONSOLE. Some utilities, such as NetWare Monitor’s “Lock File Server Console” option, can restrict access to the file server’s keyboard by requiring a password before letting you access the console’s prompt. If you cannot access the console because of such a utility, you may have to reboot the file server and bring it back up to remove the restriction.

If the console restriction is loaded at boot up from the AUTOEXEC.NCF file, you must reboot the file server again but this time restart the server by typing

```
<SERVER-na
```

at the DOS prompt. The "na" switch will allow the server to come up without running the AUTOEXEC.NCF file that loads NLM's at boot up. You will be prompted to supply information such as file server name and network number, etc. Once you get to the colon (:) prompt, you can either load NWACCESS or you can load NetWare's Install NLM and edit the autoexec.ncf file to remove the line that loads the utility that is restricting console access. Then you will be able to "DOWN" the server properly and restart it, allowing you then to load NWACCESS. Either method is acceptable.

Changing Server Passwords

NWACCESS now prompts you for the User name whose password you will change. By default, this field is set to "SUPERVISOR." You must type in the exact login name of any user whose password you wish to change.

For NetWare 4.x file servers running directory services, we recommended that you enter a fully distinguished name. A distinguished name includes the directory context where the user object exists, along with the user name separated by ".", for example:

Supervisor.myworkgroup.mycompany

If the context is not included, NWACCESS will only look for the user object in the current bindery context.

If the user object cannot be found in the context, you will be prompted to reenter the distinguished name. You may need to login to the directory as any user and use NetWare's NLIST Utility to verify the existence of the user in a given context. You can also use NetWare's CX Utility without being logged in to verify a context name, but you can't get user names with this method.

You will then be prompted to type in a new password for this user. The normal restrictions that may apply when changing the password in SYSCON or with SETPASS do not apply to NWACCESS. For example, there is no required password, minimum password length, or required unique password. After entering the password, you will be asked if the information is correct.

If the password you type in is the original user's password, NWACCESS will warn you that the password is currently in use and ask you to press a key. You will then be able to enter a new password or hit ESC to exit the program. At any time, you can hit ESC to exit the program except when viewing an error or warning message at the bottom of the screen. In this case you are prompted to "Press a key." After doing so, ESC will exit you out of the program.

When NWACCESS has successfully completed the password modification, a message similar to the following will be displayed:

"Password for user SUPERVISOR has been changed to NEWPASS."

Again, to discourage the unauthorized use of this product, NWACCESS will broadcast a 25th line message to the users attached to this server stating:

"Password for SUPERVISOR changed at server!"

The password change takes effect right away so you can login to the file server as the User name and new password anytime after the change has been made.

Technical Questions about NWAccess

Following is a list of NetWare Error codes that might be returned in an error message while modifying a password. The description next to each error number will assist you in resolving problems you might encounter while running NWACCESS.

215 Password Not Unique

This error indicates that unique passwords are required on this file server and that you have tried to modify a password with a new password that is not unique.

216 Password Too Short

This error indicates that there is a minimum length required for passwords on this file server and that the new password you have entered is too short.

252 No Such Object

This error is returned when the User name that has been entered is not a valid user on this file server. Check the spelling or enter a different User name.

254 Bindery Locked

This error is returned when NWACCESS is unable to access the server’s bindery because another user or NLM has locked it. This error is rare since many file server functions rely on access to the bindery. Try running NWACCESS again. If the bindery is still locked, you will have to down restart your file server. You may need to reload the server with the -na switch.

255 Bindery Failure

This error indicates that NWACCESS was unable to read the server’s bindery because of a hardware error or a corrupted file. In either case you will have to correct the error before running NWACCESS. Novell Technical Support may be of some assistance.

Following is a list of possible error messages that can occur within NWACCESS, along with their explanations.

Error: Access code is invalid. Press a key.

This error occurs if you have typed in an access code that is not correct. You must obtain a correct access code by calling AccessData and giving them the serial number to your copy of NetWare Access Utility.

Error: (NUMBER) accessing bindery for (USER NAME).

Explanations for possible meanings of this error are found above based on what error number is printed.

Error: Unable to remove password for (USER NAME). Error Code (NUMBER).

If you receive this error, NWACCESS is not operating properly. You will need to call AccessData for an explanation.

Error: Unable to change (USER NAME’s) password to (PASSWORD). Error Code (NUMBER).

If you receive this error, NWACCESS is not operating properly. You will need to call AccessData.

Password for (USER NAME) is already (PASSWORD). Press a key.

This is an information message. After you press a key, you will be prompted to enter a new password. If you are content knowing that you just guessed the user password, you can then hit ESC to exit the program.

If the above information did not solve the problem you were having with NWACCESS please feel free to contact Technical Support.

Executing the Utility

To run NWACCESS, place the NWACCESS disk in the A: drive and type:

```
:load A:NWACCS
```

at the file server system prompt.

You will be prompted for an access code after you load the NLM. If you still have NetWare 386 version 3.0 or 3.0a, we encourage you to upgrade soon! Until then, you may see an error message like the one below when you try to load NWACCS.NLM.

Auto loading feature not yet implemented.

Modules required to run NWACCS.NLM have not yet been loaded.

If you see this message, you will need to load the STREAMS.NLM and the CLIB.NLM before attempting to load NWACCS.NLM.

Note: To help preserve security on your file server, it is not recommended that NWACCESS be copied to a network drive.

If you have NetWare 4.x, you will need to load DSAPI.NLM first. NWACCESS will not run and will prompt you to load it if it is not loaded. Once loaded, the NWACCESS screen will appear on the server monitor as shown below:

NWACCESS displays the serial number for your version of NetWare as well as the serial number for your copy of NWACCESS. It then prompts you for an access code. A help line is always available at the bottom of the screen prompting you for the information you must type in next.

Access Code for NWAccess

You can obtain your access code by calling AccessData at (801) 377-5410. An operator will ask you for the NWACCESS serial number and verify registration. He/she will then give you your access code. You should keep this code in a safe place, as it will allow anyone who runs NWACCESS to change anyone's password on the file server.

NOTE: Be patient after entering the access code since the validation process can take several seconds.

Technical Support

If after reviewing Technical Questions, you are unable to get the password recovery software to function, contact AccessData's customer support service by calling:

(800) 574-5199 or (801) 377-5410

NTACCESS

Introduction to NTAccess

NTAccess will get you into the administrator account on a Windows NT server when you don't know the password. Unlike other programs, it does not require that you reinstall Windows NT, and it doesn't have you disassemble your server. NTAccess Utility requires that you shut down the server and boot to DOS from a floppy disk for a few minutes. NTAccess will then scan your hard drive for the administrator account information, analyze the information, and alter the appropriate bytes. Reboot the server and, you're in!

NT Access will not work on RAID or mirrored systems. AccessData is currently working on improvements to the program to combat these problems. If you have any questions please let us know at info@accessdata.com.

Registration

You must register this program with AccessData Corporation before using the utility. Once the registration card is sent in, please call during regular business hours Mountain Time at (801) 377-5410 and your access code will be released to you. NTAccess will not run without the program specific access code.

Notice that there is space for two signatures on the release form. Due to the sensitive nature of NTAccess Utility, AccessData requires two signatures for registration. (One of the user, and one of the manager.) BOTH signatures must be present before the password can be released.

When you have completed the registration card, return it to the address listed below. If there is an urgent need for the program, you may fax the registration card to AccessData and send the original through the mail.

AccessData Corporation
2500 N. University Suite 200
Provo, UT 84604-3864
TEL (801) 377-5410   FAX (801) 377-5426

Running NTAccess

Booting to DOS

NT passwords are stored in the Security Account Manager (SAM) file. This file is constantly in use by the NT File System. When you boot to DOS, however, nothing uses the SAM file and the NTAccess Utility is free to modify it.

To make the NTAccess disk bootable:

1. Go to a computer other than the server and pull up a DOS prompt. On Windows 95 machines, you can find it under Start|Programs; on Windows 3.11, it will be in the Main program group.

2. Once you have a DOS prompt, make sure the NTAccess program disk is not write protected (the hole should be covered, not open), and put it in the A: drive.

   Now type: `SYS A:`

   This will install the system files on the NTAccess program disk.

*If you get the response: Bad command or file name, then you'll have to search for `SYS.COM` on your hard drive. It should either be in the `\DOS` directory or `\WINDOWS\COMMAND` directory. If all else fails, type:

```
cd \
```

```
dir sys.com /s
```

This will search your hard drive for SYS.COM.

3. If your server does not boot from the floppy drive, you'll have to change the CMOS settings on the server. See the Trouble Shooting section for more information on how to do this.
4. Shut down the server, following whatever procedures are necessary for your system.
5. Turn off the server; put the NTAccess disk in the floppy drive, and turn the server back on. The computer should boot up and present you with a DOS prompt.
6. Once you are at the DOS prompt, you will be prompted for different command lines for NT 3.x or 4 .

NT version 3.x	NT version 4
Please type: `ntaccess -root winnt 35`	Please type: `Ntaccess`

Before replacing the administrator password, NTAccess will prompt you for the password you received over the phone from AccessData when you registered. If you have not registered, you must do so before receiving your password. If you have forgotten your password, call AccessData at (801) 377-5410.

After you enter the correct password, NTAccess will display a list of all the NTFS partitions, as well as the FAT partitions with SAM files. If there is only one NT partition, NTAccess will select that one automatically and wait for you to press a key. Otherwise it will ask you which one to use.

NTAccess will then present you with a list of all the accounts with administrator privileges. Choose one.

Finally, you will be asked to enter a replacement password for the account you chose. **Do not use spaces, tabs, or commas.** The password will be truncated at fourteen characters. We suggest that you change the password again using user manager for domains once you have access to the administrator account, as it allows a much wider range of passwords to be entered.

Remove the NTAccess diskette from the drive and reboot the server. Login under the account you chose, and type in the new password.

Emergency Repair Disk

On NT 4.0 systems you can create an Emergency Repair Disk. The Emergency Repair Disk contains all of NT's most vital files, and will allow you to recover any data from anything that may go wrong while using NTAccess Utility. NTAccess is designed to be able to undo all the changes it makes, but should a power failure occur while writing the undo file, it may not be possible. If you can log in under any name, do so now and create an Emergency Repair Disk before executing the NTAccess Utility.

Creating an Emergency Repair Disk:

1. Click on the Start menu and select Help.
2. The Help dialog will appear. Choose the Index tab.
3. Type the first few letters of 'emergency' until Emergency Repair Disk is highlighted in the box below. Press <enter>.
4. The Help information will appear. Under the heading To start Repair Disk, press the Create Repair Disk button and follow the instructions.

Technical Questions about NTAccess

File not Found
This error means that the partition you selected either does not contain the SAM file or the SAM file is in a directory other than the default. The usual directory for the SAM file on an NT 4.0 system is `WINNT\SYSTEM32\CONFIG\SAM`, and NTAccess will look there by default if you installed NT 4.0 in a directory other than `\WINNT`, you must use the -root option.

To use the -root option, type the following at the DOS prompt:
`ntaccess -root` <the name of your %SystemRoot% directory>

For example, if you had installed NT 4.0 to the `\WINNT40` directory, you would type:

```
ntaccess -root winnt40
```

Changing the CMOS Settings
These steps to change the CMOS settings so that the server will boot off of the floppy drive replace steps 3, 4, and 5 under the Booting to DOS heading above

First, shut down the server. Follow whatever procedures are necessary for your particular system. Turn off the server, then turn it back on again. To get into the CMOS setup menu, you must hold down a key. On most PC's, you have to hold down the DEL key to get into the setup menu, but some are different; the computer will say what to push as soon as you turn it on. Once you're in the CMOS setup menu, find the section that lets you specify the boot order of the drives and set it to check the floppy drive first.

Put the NTAccess program disk in the floppy drive and exit the CMOS setup. Be sure you save your settings. The computer should reset and boot up off of the NTAccess program disk.

Returning the server to Original State
The undo file's name is MMDDhhmm.nta, where MM is the month, DD is the date, hh is the hour (out of 24), and mm is the minute that the password was changed. To reverse the change, type:

`ntaccess -undo` <filename.nta>

If after reviewing the above problems and solutions and NTACCESS is still unable to change the password contact AccessData at (800) 574-5199 or (801) 377-5410.