

Reset Windows Password

USER MANUAL

Copyright (c) 2021 Passcape Software. All rights reserved.
Passcape Software

1.	Introduction	5
1.1	About the program	6
1.2	Features and benefits	6
1.3	System Requirements	7
2.	Creating bootable environment	8
2.1	3 simple steps to launching the application from a boot disk	9
2.2	Creating RWP boot disk	9
2.3	Changing BIOS/UEFI settings	12
2.4	Running the program from the bootable CD/DVD/USB	16
2.5	Running the program using UEFI's boot media selection option	19
3.	Working with the program	21
3.1	Main window	22
3.2	Reset user passwords	25
3.3	Reset DSRM passwords	28
3.4	Reset domain cached password	29
3.5	Add new user account	33
3.6	Edit user account properties	35
3.7	Logon policy options	38
3.8	Interface and system restriction policy	45
3.9	Password policy editor	57
3.10	Search for logon passwords	60
3.10.1	Custom recovery	63
3.11	Search for domain cached passwords	66
3.11.1	Custom recovery	69
3.12	Extract BitLocker recovery passwords	72
3.13	Dump password hashes	74
3.14	Dump domain cached passwords	77
3.15	Restoring previous modified password	78
3.16	PASSWORD RECOVERY TOOLS	81
3.16.1	Decrypt Windows Hello credentials	81
3.16.2	Lookup PIN	82
3.16.2.1	Custom recovery	86
3.16.3	Search for SYSKEY startup password	88
3.16.3.1	Custom recovery	94

3.16.4	Search for virtual machine passwords	97
3.16.5	Search passwords for encrypted documents	100
3.16.6	Search for Internet/mail/network passwords	104
3.16.6.1	Search for Web passwords stored by Internet browsers	105
3.16.6.2	Search for mail passwords saved by email clients	107
3.16.6.3	Search LAN/WAN/RAS/DSL/VPN/WiFi and other network passwords	108
3.17	FORENSICS	109
3.17.1	View logon history and statistics	109
3.17.2	View hardware history	113
3.17.3	View software history	116
3.17.4	View network history	119
3.17.5	View recent user activity	122
3.17.6	Search for recently opened documents	126
3.17.7	View program execution timeline	127
3.17.8	View system events	129
3.17.9	View web history	132
3.17.10	View last modified files	139
3.17.11	View last modified directories	141
3.18	UTILS	141
3.18.1	Search for lost product/CD keys	141
3.18.2	Search for password-protected documents	143
3.18.3	Search for recently opened files	146
3.18.4	Backup passwords and sensitive information	148
3.18.5	Removing user's private information	151
3.18.5.1	Removing password history of SAM or Active Directory users	153
3.18.5.2	Removing domain cached passwords	155
3.18.5.3	Removing cached logon password	158
3.18.5.4	Removing password reset disk information	160
3.18.5.5	Removing password hints	163
3.18.5.6	Resetting SYSKEY	166
3.18.6	Loading additional hard disk drivers	169
3.18.7	Unlock Bitlocker encrypted drives	170
3.18.8	Mounting virtual drives	171
3.18.9	Create disk image	171
4.	License and registration	174
4.1	License Agreement	175
4.2	Registration	176
4.3	Limitation of unregistered version	176
4.4	Program editions	177
5.	Technical support	181

- 5.1 Reporting problems 182
- 5.2 Suggesting features 182
- 5.3 Contacts 182

Introduction

1 Introduction

1.1 About the program

Reset Windows Password was developed for resetting, changing and recovering Windows logon passwords. For example, when the computer Administrator's password is lost or forgotten. Reset Windows Password is the most optimal and functionally richest solution in its class. The application supports all versions of Windows (based on NT), works with Active Directory and domain cached credentials, possesses artificial intelligence skills for recovering passwords instantly to certain accounts and demonstrates a number of additional unique features.

The interface of the application is traditionally carried out in the form of a step-by-step wizard. Therefore, the operation process does not seem complicated to even an inexperienced user. For example, resetting an administrator password takes just three simple steps:

1. Select the SAM and SYSTEM files (the application automatically searches all hard drives for the registry files.)
2. Select the user account.
3. Reset or modify the password.

Using a built-in utility, you can easily create a bootable CD, DVD or USB disk (including devices like Compact Flash, SmartMedia, SONY Memory Stick, Secure Digital, ZIP drives, USB Hard Disk drives, etc.) within a few minutes, from an existing ISO image with the program. Reset Windows Password has a graphic user interface, supports loading IDE, SATA, SCSI, RAID volumes on the fly, is compatible with FAT, FAT32, NTFS, NTFS5 file systems, goes with a large collection of hard disk drivers from Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware.

1.2 Features and benefits

Application's advantages:

- Support for all versions of NT-based Windows.
- Support for 32/64-bit Windows.
- Large collection of hard disk drivers. Loads additional drivers from the application.
- Reset and modify passwords of local and domain users, local administrator, domain administrator, other Active Directory accounts.
- Enable and unlock user accounts, both local and domain administrators.
- Disable password expiry options.
- Detect several operating systems.
- Support for non-English versions of Windows and passwords in national encoding.
- Dump user password hashes from SAM for further analysis.
- Dump password hashes from Active Directory.
- Dump domain cached passwords.
- Several modules to extract and decrypt Active Directory plain-text passwords.
- Allow undoing changes made to the system.
- Delete passwords and other sensitive data from PC.
- Advanced password search and recovery algorithms.
- Reset SYSKEY security.
- SYSKEY startup password recovery.
- Search for lost serial keys.

- Search for network passwords.
- Search for virtual machine passwords.
- Backup registry/Active Directory and other sensitive information.
- Unlock Bitlocker drives.
- View user activity, different forensic information.
- Password search and recovery for MS Office, OpenOffice, LibreOffice, MyOffice, and PDF documents.
- Edit local or domain password policy, as well as system and interface restrictions.

The software is available in three editions: **Light**, **Standard** and **Advanced**. The detailed list of features for each edition is available [here](#).

1.3 System Requirements

Requirements

x64-based microprocessor, a minimum of 1 GB of RAM, CD-ROM or USB drive. The size of the bootable USB drive should be 512 Mb or bigger (it is recommended 2-32 Gb USB stick for better compatibility). Computer BIOS must support booting from CD, DVD or USB device.

Compatibility

Windows NT or newer OS, Windows Server 2000 or newer. File systems: FAT, FAT32, NTFS, NTFS5. The program is compatible with the majority of CD/DVD recorders and USB devices, including Memory Stick, Compact Flash, SmartMedia, Secure Digital, USB flash drives, USB ZIP drives, USB Hard Disk drives, etc.

Restrictions

Once your system uses a non-standard mass storage device, you may need to specify a 3d-party driver compatible with Windows 10. Please refer to your motherboard manual for the details.

Known issues or bugs

- If you have 2 or more logical disks in your system, the disks letters may be reassigned/reordered.
- If you are resetting a password of the built-in Administrator account in some editions of Windows, please keep in mind that in order to activate the built-in Administrator account and log on the system, you will need to load the system in the safe mode.
- The program supports all types of SYSKEY encryption. In some cases you may need to provide the SYSKEY startup password or startup diskette. However the program also allows to reset/lookup SYSKEY password. So even if you forgot your SYSKEY, it's not a problem.
- After you reset the password of a local account, you may lose access to your Web page passwords, wireless network and file share credentials, EFS-encrypted files, e-mail messages encrypted with private keys. Please refer to [Microsoft Knowledgebase](#) for further details.
- Resetting Active Directory passwords for certain accounts may have no effect. For example, on a RODC.
- Password reset (as well as other features that imply disk-write operations) on a virtual OS will have no effect.
- When resetting a password for Microsoft Account, you should provide a non-empty password. Otherwise you will not be able to log on the system.

Creating bootable environment

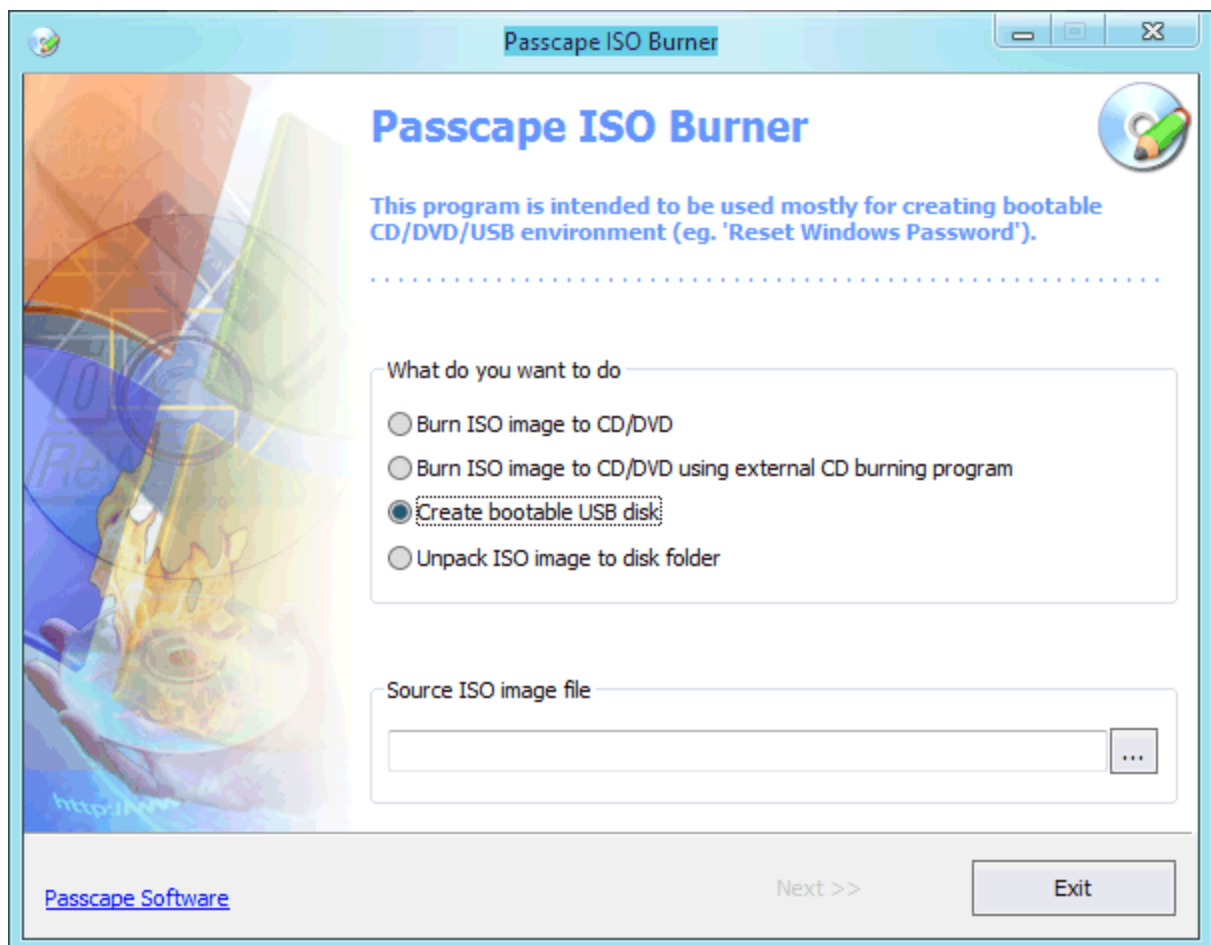
2 Creating bootable environment

2.1 3 simple steps to launching the application from a boot disk

1. Download Reset Windows Password package at <https://www.passcape.com/download/rwp.zip> (or using the link that was sent to you in the registration e-mail)
2. [Create RWP boot disk](#): unpack the RWP.ZIP file, run IsoBurner.exe, select an item for creating bootable CD/DVD/USB, specify the path to the unpacked ISO image and write it to the disk.
3. Start the target computer and [change its BIOS/UEFI settings](#) to make the boot device (CD-ROM, DVD-ROM or USB disk) first on the list. Save the settings, reboot once again to start the program off your bootable CD, DVD or USB disk. You can use fast boot option if your BIOS/UEFI supports fast boot media selection during startup.

2.2 Creating RWP boot disk

Passcape ISO Burner



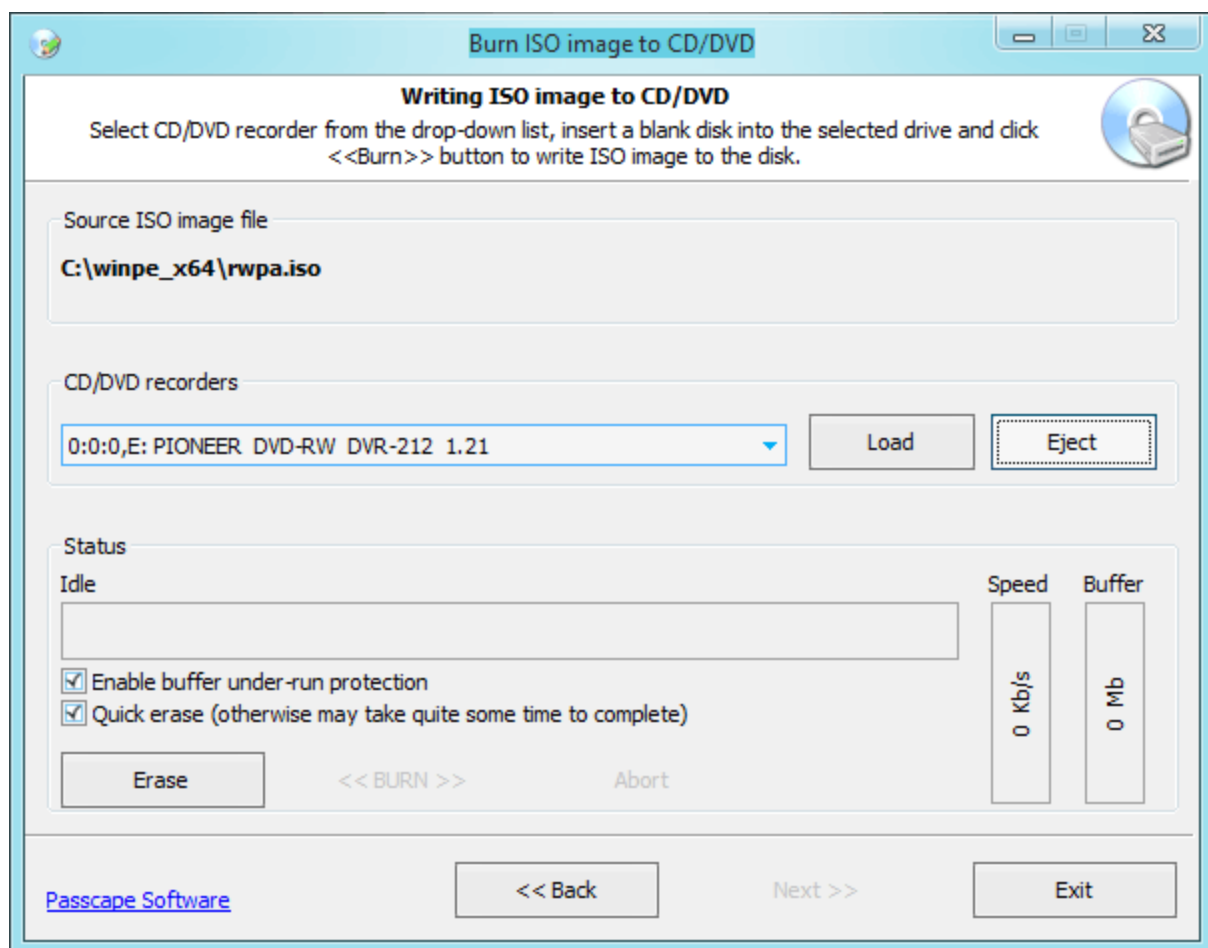
Passcape ISO Burner is a program for creating bootable CD, DVD or USB disks from ISO-9660 images. The program is free and comes with RWP. it is also available for downloading and using at our

website: <https://www.passcape.com/download/pib.zip>

The application's interface is ultimate-simple. When started, the application asks you to select what you would like to do:

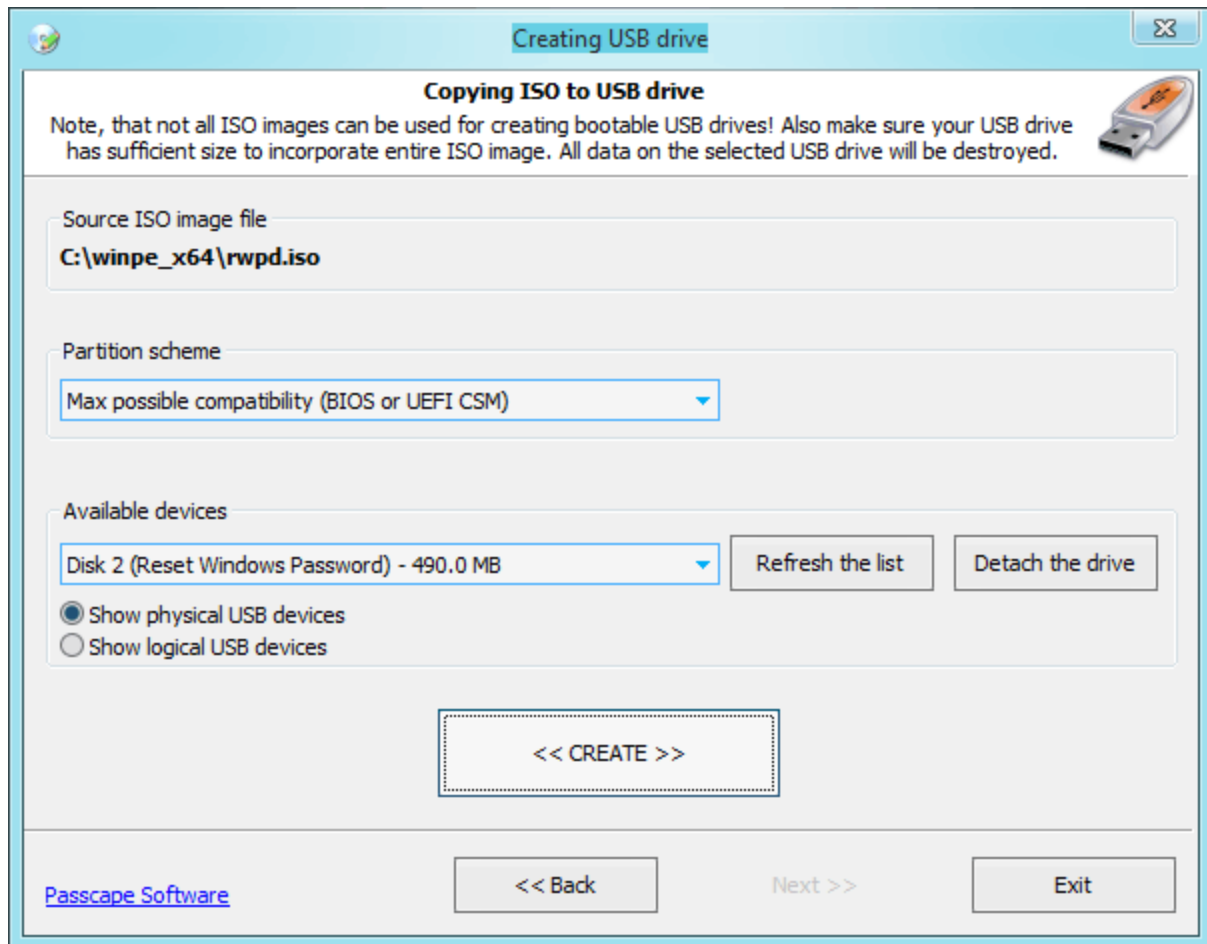
- Record ISO image to CD/DVD using this application
- Record ISO image to CD/DVD using an external burning application installed on your computer. For example, Nero or its free analog ImgBurn.
- Use ISO image to create a USB boot disk
- Extract ISO image to disk (keep in mind that this action causes the loss of boot data).

Creating Reset Windows Password bootable CD



Select the first menu item: 'Burn ISO image to CD/DVD'. At the bottom of the screen, enter path to the file with the ISO image. That enables the 'Next' button, and you can move on to actually creating the disk. All we need to do here is select the recorder we are going to use, insert a blank CD/DVD in it and click on the <<BURN>> button to create a boot disk from the ISO image selected on the previous step.

Creating Reset Windows Password bootable USB



Select the existing bootable ISO image with the program and set the 'Create bootable USB disk' option on. Enter the product serial number if you have one. When the next window appears, plug the USB device to your computer; it should automatically appear on the list of found USB devices. Click on the 'Create' button to format and create the boot USB. In some cases (for example, if the USB device is installed as a hard disk drive, and an extended partition entry is found on that disk) the application will require restarting for reassigning drive letters.

The program offers several partition schemes (formatting modes) to supply better compatibility when booting from USB devices. If you feel uncertain about what partition scheme to select, consider using the following simple algorithm:

- If the target PC is based on [UEFI](#) (graphical) interface, select 'Max compatibility with new PCs (FAT32 MBR for UEFI)' mode. This scheme will create a USB to be run on UEFI-based PCs where secure boot mode is turned on.
- If your target PC is based on [BIOS](#) (textual) interface, select 'Max compatibility with old PCs (FAT32 MBR for BIOS)' mode. This mode will create a USB that is fully compatible with BIOS firmware.
- If you know nothing about target PC, switch to 'Max possible compatibility' scheme. This mode creates bootable USBs that can run on both BIOS- and UEFI-based computers (with **Compatibility Support Mode** is turned on). On some PCs or laptops the Compatibility Support Mode is also known as **Legacy Boot Mode**.

If you bought your PC after 2010, most likely, it comes with UEFI. New computers use UEFI firmware instead of the traditional BIOS. Both are low-level software that starts when you boot your PC and are used to 'communicate' with hardware. Unlike BIOS, UEFI is a more modern solution with graphic interface, supporting larger hard drives, faster boot times and more security features.

Be careful! All data on the target drive will be overwritten. If the application is unable to detect boot files in the source ISO image, it will show the respective warning.

Some AntiVirus/AntiMalware software block creating bootable disks or copying some boot files to media even without onscreen warnings!

2.3 Changing BIOS/UEFI settings

General information

In order to load Reset Windows Password, you may need to adjust your computer's BIOS/UEFI settings to make the boot device (CD, DVD, or USB) first on the list of devices. This is the routine to follow for that:

1. When booting the computer, press the **Del** key to enter the BIOS menu. Some versions of BIOS use other hotkeys; those could be **F2**, **F10**, **F11**, **ESC**, etc. The hint is normally displayed at the bottom of the boot screen.
2. Enter the BIOS/UEFI, then on the menu find the item that's in charge of the initial boot devices. Edit it to make the CD or USB with the Reset Windows Password first on the list.
3. Make sure to have saved the changes and then reboot the computer.

If your PC uses UEFI firmware, you can use fast boot selection switch without altering any settings. For more information, please refer to your computer's motherboard user manual.

Setting up BIOS, questions and answers

Q: My computer's BIOS has several items for booting from USB devices: USB FDD, USB ZIP, USB HDD, USB CDRM. Which one should be selected?

A: Different BIOS manufacturers set up the initial boot different ways. In the majority of cases, to boot from a regular flash: on old motherboards you would need to select the USB ZIP option; on some other ones - USB HDD.

Q: The application takes too long (sometimes up to 10 minutes) to boot from USB media.

A: That indicates that the device runs over the slow USB protocol, 1.1. First, the storage device must support the 2.0+ specification. Second, the USB port in the motherboard where you plug the storage device must support the 2.0+ specification. And third, you must enable the USB 2.0 (or higher) support in the BIOS.

Q: The computer wouldn't boot from USB devices at all. When attempting to boot – either black screen or the 'no operating system' error message.

A: Try finding the 'Legacy USB storage detect' option and make it 'Enabled'. In the boot options, you should have only one USB device. If you have two or more USB devices plugged to the computer (eg. UPS, printer, scanner, modem, etc.), leave only one bootable USB disk. Unplug the USB device from the computer, turn the computer off, plug the USB device to a different USB port, turn your computer on and attempt to boot again. If that didn't help – update your BIOS. Also there is a chance that your motherboard doesn't support booting from USB devices or doesn't support the file system used on this USB storage device.

Q: Blue or black screen, all kinds of driver, registry load, etc. errors occur when booting from CD or USB.

A: Maybe your computer does not have sufficient memory. The minimum required by the application is 1

GB RAM. To run it with comfort, you would need 2 GB or more.

Q: Can't get into my BIOS. A password is required.

A: An unpleasant surprise can watch for you when you try to modify the boot device settings in BIOS. The matter is that some hardware manufacturers, sellers or previous owners of the PC may have set their own passwords for accessing BIOS. In other words, in order to modify BIOS settings, you would need to enter that password, which usually is not possible to find out.

Some versions of BIOS allow resetting their settings by pressing a certain key on the keyboard; normally that's **Ins**. For some type of AMI BIOS it is a **Ctrl+Alt+Del+Ins** combination. On AWARD BIOS, the key is to be pressed and held down until the computer is turned on. That will load the default settings. However, this option is to be used extremely carefully, as it resets all other settings of the BIOS.

Also, there are universal back-door passwords. They are provided below for many popular old versions of BIOS. If you don't know it, BIOS type and version is normally displayed for a few seconds during the initial boot of the computer at the bottom of the screen.

If none of the universal passwords has worked out, you can take advantage of the method described in many motherboard user manuals: simply reset BIOS settings by shorting the respective jumper. It is normally located near the large CMOS battery. If the motherboard doesn't have a CMOS battery, find the microchip with the Dallas or Odin marking; the jumper must be somewhere nearby. Simply removing the CMOS battery doesn't always help, as the BIOS microchip can live for several hours without the power. Also, you are highly discouraged from shorting the CMOS itself for resetting BIOS settings, as that may cut the battery life essentially.

On the Net, you can find a number of software solutions for recovering passwords and resetting BIOS. For example, cmospwd and killcmos. You are highly discouraged from resetting all BIOS settings in laptops. That may lead to the complete halt of the system.

Q: A error pops up which states that the CPU does not support 64-bit mode or running 64-bit applications.

A: Reset Windows Password does not support 32-bit CPUs any longer (but has support for 32-bit OSes though). Contact tech. support to get a link for the latest 32-bit compatible version.

Q: Can I boot a BIOS compatible CD/USB drive in UEFI?

A: Yes. Enter your UEFI settings (press ESC, F2 or DEL). Open 'Boot' menu and enable 'Launch CSM' option. Now locate 'Security' tab and disable 'Secure Boot Control'. Save changes and reset your PC. Enter the UEFI setup once again and make sure your DVD/USB drive is available under the 'Boot' tab. Some UEFIs also have a boot device menu (it is usually launch by hitting F8) where you can select your boot device and mode.

Q: Can I create a USB drive that will be able to boot in both BIOS and UEFI?

A: Yes. Run the IsoBurner tool and select 'Max possible compatibility' partition scheme when creating a bootable USB. This mode creates bootable USBs that can run on both BIOS- and UEFI-based computers (with Compatibility Support Mode is turned on). On some PCs or laptops the Compatibility Support Mode is also known as Legacy Boot Mode.

Q: USB is not listed as a boot option in my UEFI. How can I enable booting for a USB stick?

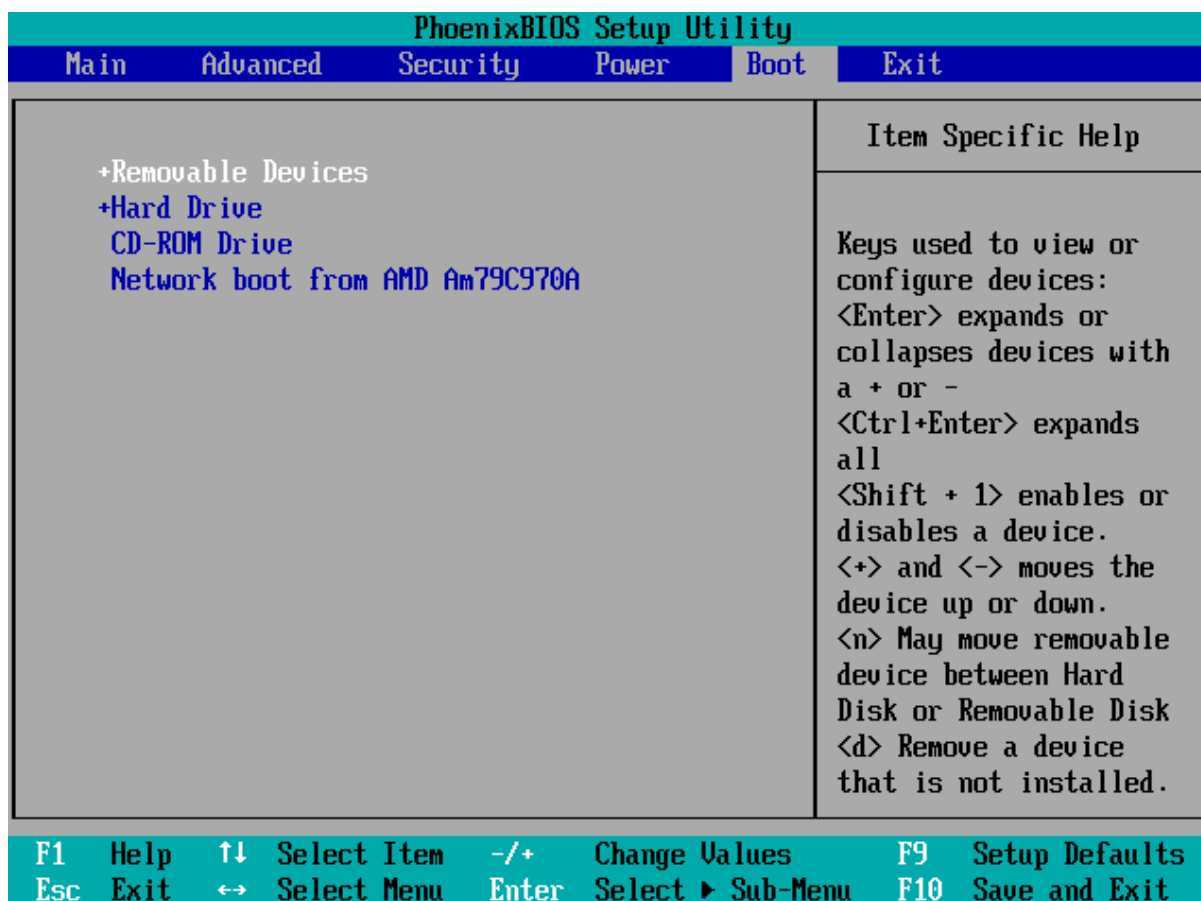
A: Seems that the USB was formatted either to BIOS or UEFI CSM mode but your UEFI allows booting in Secure Boot mode only. You will have to allow booting in legacy mode. In your UEFI settings disable both 'Boot - Fast Boot' and 'Security - Secure Boot' and enable 'Compatibility Support Mode (CSM)' or similarly worded options. Another workaround would be just creating a bootable USB using 'Max compatibility with new PCs (FAT32 MBR for UEFI)' scheme. This scheme is fully compatible with UEFI Secure Boot mode.

Back-door BIOS passwords

BIOS manufacture	Universal password
AWARD BIOS 2.50	AWARD_SW, 01322222, j262, TTPTHA, KDD, ZBAAACA, aPAf, lkwpeter, t0ch88, t0ch20x, h6BB
AWARD BIOS 2.51	AWARD_WG, HLT, BIOSTAR, SWITCHES_SW, 256256, j256, ZAAADA, Syxz, ?award, alfarome, Sxyz, SZXY
AWARD BIOS 2.51G	HEWITRAND, HLT, biostar, HELGA-S, bios*, g6PG, j322, ZJAAADC, Wodj, h6BB, t0ch88, zjaaadc
AWARD BIOS 2.51U	condo, biostar, CONDO, CONCAT, 1EAAh, djonet, efmukl, g6PG, j09F, j64, zbaaaca
AWARD BIOS 4.5	AWARD_SW, AWARD_PW, PASSWORD, SKYFOX, award.sw, AWARD?SW, award_?, award_pc, ZAAADA, 589589
AWARD BIOS 6.0	AWARD_SW, HLT, KDD, ?award, lkwpeter, Wodj, aPAf, j262, Syxz, ZJAAADC, j322, TTPTHA, six spaces, nine spaces, 01355555, ZAAADA
AMI BIOS	AMI, SER, A.M.I., AMI!SW, AMIPSWD, BIOSPASS, aammii, AMI.KEY, amipswd, CMOSPWD, ami.kez, AMI?SW, helga s, HEWITT RAND, ami', AMISETUP, bios310, KILLCMOS, amiami, AMI~, amidecod
AMPTON BIOS	Polrty
AST BIOS	SnuFG5
BIOSTAR BIOS	Biostar, Q54arwms
COMPAQ BIOS	Compaq
CONCORD BIOS	last
CTX International BIOS	CTX_123
CyberMax BIOS	Congress
Daewoo BIOS	Daewuu, Daewoo
Daytec BIOS	Daytec
DELL BIOS	Dell
Digital Equipment BIOS	komprrie
Enox BIOS	xo11nE
EpoX BIOS	Central
Fretech BIOS	Posterie
HP Vectra BIOS	hewlpack

IMB BIOS	IBM, MBIUO, sertaFu
Iwill BIOS	iwill
JetWay BIOS	spooml
Joss Technology BIOS	57gbz6, technology
M Technology BIOS	mMmM
MachSpeed BIOS	sp99dd
Magic-Pro BIOS	prost
Megastar BIOS	star, sldkj754, xyzall
Micronics BIOS	dn_04rjc
Nimble BIOS	xdfk9874t3
Packard Bell BIOS	bell9
QDI BIOS	QDI
Quantex BIOS	teX1, xljbj
Research BIOS	Col2ogro2
Shuttle BIOS	Col2ogro2
Siemens Nixdorf BIOS	SKY_FOX
SpeedEasy BIOS	lesarot1
SuperMicro BIOS	ksdjfg934t
Tinys BIOS	tiny, tinys
TMC BIOS	BIGO
Toshiba BIOS	Toshiba, 24Banc81, toshy99
Vextrec Technology BIOS	Vextrex
Vobis BIOS	merlin
WIMBIOS v.2.10 BIOS	Compleri
Zenith BIOS	3098z, Zenith
ZEOS BIOS	zeosx

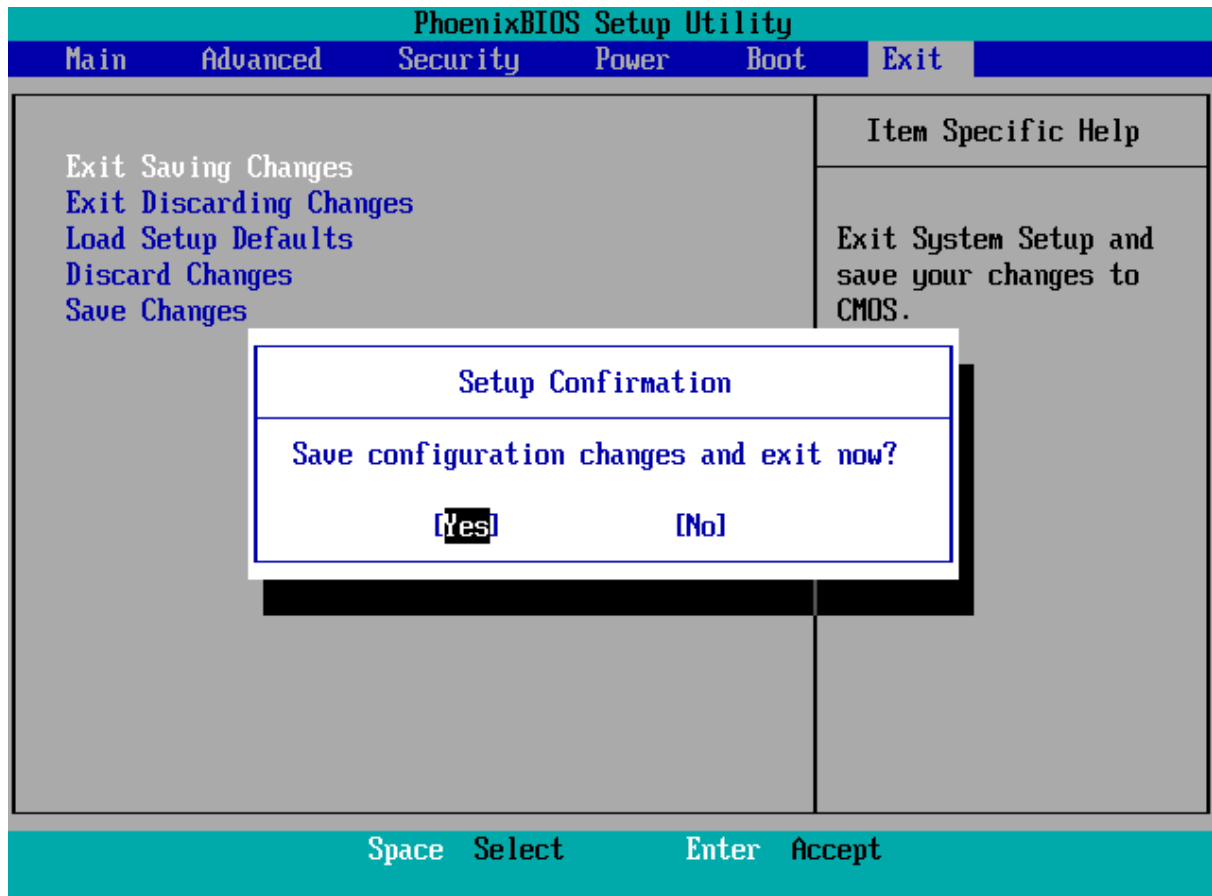
2.4 Running the program from the bootable CD/DVD/USB



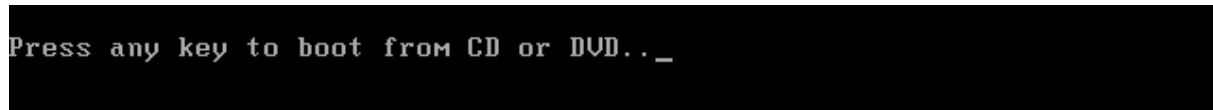
Turn on your computer. Press the Del key to enter the BIOS menu. Some versions of BIOS use other hotkeys; those could be F2, F10, F11, ESC, etc. The hint is normally displayed at the bottom of the boot screen.

PhoenixBIOS Setup Utility											
Main		Advanced		Security		Power		Boot		Exit	
CD-ROM Drive +Removable Devices +Hard Drive Network boot from AMD Am79C970A										Item Specific Help	
										Keys used to view or configure devices: <Enter> expands or collapses devices with a + or - <Ctrl+Enter> expands all <Shift + 1> enables or disables a device. <+> and <-> moves the device up or down. <n> May move removable device between Hard Disk or Removable Disk <d> Remove a device that is not installed.	
F1	Help	↑↓	Select Item	-/+	Change Values	F9	Setup Defaults				
Esc	Exit	↔	Select Menu	Enter	Select ► Sub-Menu	F10	Save and Exit				

Edit Boot menu the way to make the CD or USB disk with the Reset Windows Password first on the list of boot devices.



Make sure to have saved the changes and then reboot the computer.



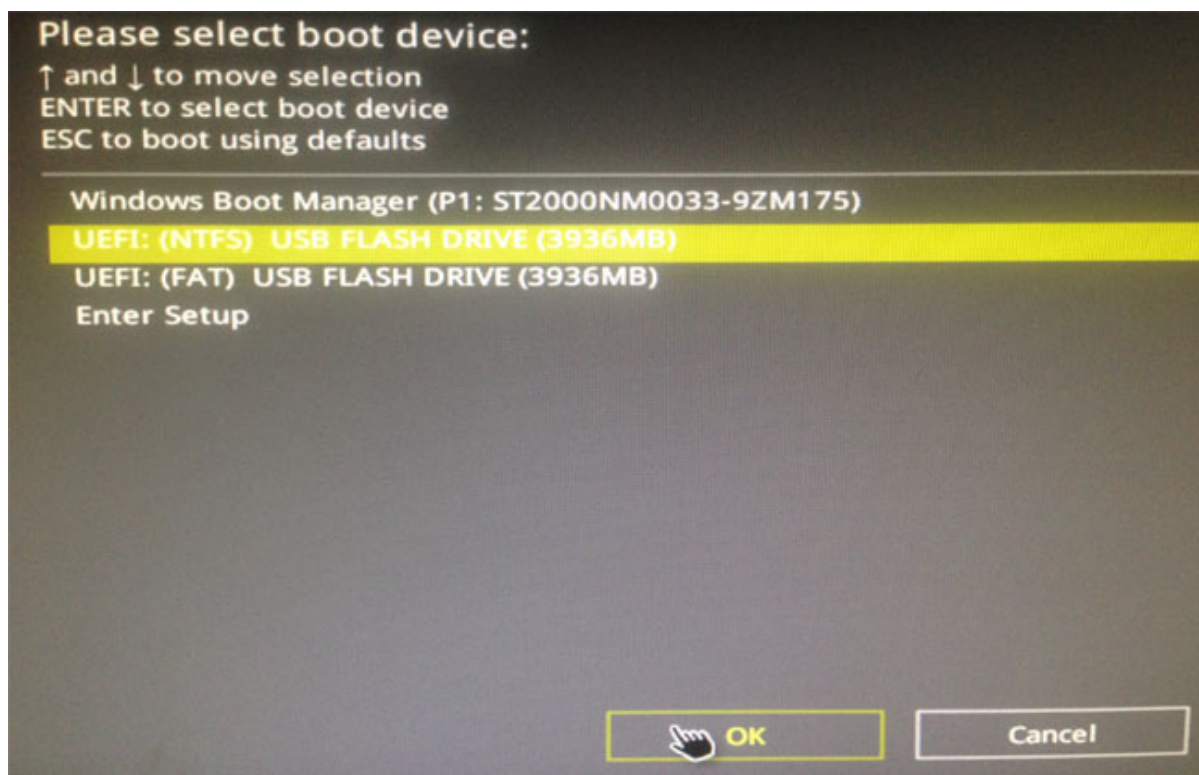
If everything's gone smoothly, you'll see the following textual message. Hit any key to load from Reset Windows Password bootable disk. Otherwise your old OS will started.



RWP has been successfully loaded and ready to use.

2.5 Running the program using UEFI's boot media selection option

If your UEFI supports boot media selection, you can use it to start the program easily off the boot disk. The option is invoked by hitting a hot key (usually, F8) on PC startup. In most versions of UEFI this option is also available from the main menu.



Working with the program

3 Working with the program

3.1 Main window



First, the program suggests to select one of the recovery modes: **SAM** – regular user accounts, **AD** – Active Directory accounts, **DCC** - domain cached passwords, **PASSWORDS** - password recovery tools, **FORENSICS** - system investigation and forensic tools, **UTILS** - other utilities. As you make the selection, the list of available operations should be available for the mode.

SAM - regular user accounts

- [Reset user account password](#)
- [Add new user account](#)
- [Edit account properties](#)
- [Logon policy options](#)
- [Password policy editor](#)
- [Interface and system restriction policy editor](#)
- [Lookup user passwords](#)
- [Dump password hashes](#)

- [Restore previously modified passwords, rollback changes](#)

AD - Active Directory domain accounts

- [Reset user account password](#)
- [Reset or change DSRM \(Directory Services Restore Mode\) password](#)
- [Edit account properties](#)
- [Password policy editor](#)
- [Lookup user passwords](#)
- [Extract BitLocker recovery passwords](#)
- [Dump password hashes](#)
- [Restore previously modified passwords, rollback changes](#)

DCC - domain cached credentials

- [Reset domain cached password](#)
- [Lookup DCC passwords](#)
- [Dump domain cached credentials to text file](#)
- [Restore previously modified passwords, rollback changes](#)

PASSWORDS - password recovery tools

- [Decrypt Windows Hello credentials](#)
- [Lookup PIN](#)
- [Lookup SYSKEY startup password](#)
- [Lookup passwords for virtual machines](#)
- [Lookup passwords for encrypted documents](#)
- [Search for Internet/mail/network passwords](#)

FORENSICS - system investigation tools

- [View logon history and statistics](#)
- [View hardware history](#)
- [View software history](#)
- [View network history](#)
- [View recent user activity](#)
- [Search for recently opened documents](#)
- [View program execution timeline](#)
- [View system events](#)
- [View Web history](#)
- [View last modified files](#)
- [View last modified directories](#)

UTILS - miscellaneous tools

- [Lookup lost product keys and serial numbers](#)
- [Search for protected documents](#)

- [Search for recently opened documents](#)
- [Backup Passwords and sensitive information](#)
- [Remove user sensitive information](#)
- [Load IDE/SATA/SCSI/RAID driver](#)
- [Unlock Bitlocker-encrypted drives](#)
- [Mounting virtual drives](#)
- [Create disk image](#)

Schematic description of logon types

SAM

A regular user account of any home PC. Password hashes are stored in SAM registry file on the same computer.



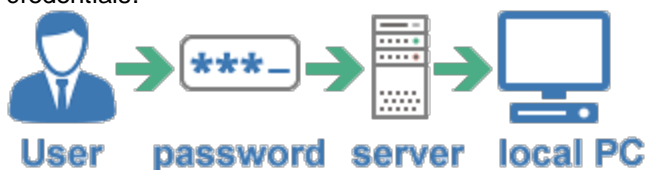
Active Directory

A domain user account. Password hashes are stored in NTDS.DIT database on domain PC.



DCC

Cached credentials of domain accounts. Password hashes can be stored (depending on domain security policy) on the local PC. The account login is performed either through the domain or using the cached credentials.



3.2 Reset user passwords

Selecting data source

Reset or change user account password

Resetting SAM user account password (step 2 of 4)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

Path to SAM and SYSTEM files

SAM registry file
D:\Windows\System32\Config\SAM

SYSTEM registry file
D:\Windows\System32\Config\SYSTEM

OS info

OS version	Windows 10 Enterprise 17134.1.amd64fre.rs4_release.180410-1804
OS owner and org	John
OS install date	2018-05-03
Windows product key	
Last logon user	John (Last logon 2018-10-13 12:44:54)

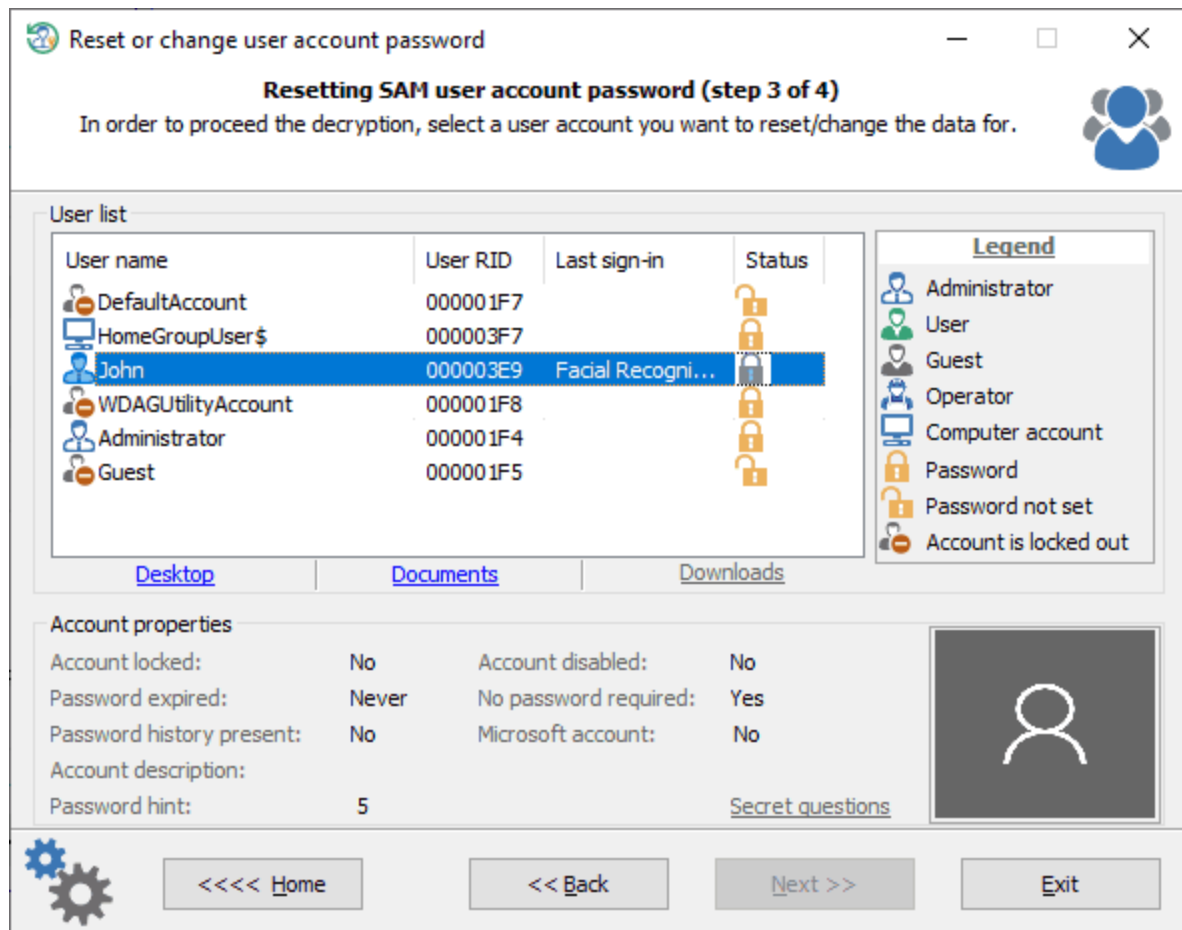
<<<< Home << Back Next >> Exit

To reset a regular account password, you should select two registry files: **SAM** and **SYSTEM**. The application automatically searches all files and suggests the first ones it finds. The registry files are located in the **%WINDIR%\system32\config** folder. Where **%WINDIR%** is your windows directory.

If you select Active Directory mode during the previous step, you should set the location of the Active Directory database instead of the SAM registry file. By default, that's the **%WINDIR%\NTDS** folder. So the full path to the AD database may look like this: **C:\Windows\NTDS\ntds.dit**

The *OS Info* shows a version of the found Operating System, its owner and installation date, the last logged-in user, and the Windows product key if found.

Choosing a Windows account



The top of the dialog displays the list of user accounts found, their status, and the date of the last logon. By clicking on one of the items, you can view additional information about the account; namely: whether it is locked or disabled, whether the password is required, whether the password history is available, its password hint, etc.

You can also display the selected account's desktop, documents, or download folder.

All Windows 10 versions starting from v17063 have a new security feature, called [secret questions](#). The secret questions is an additional security layer aimed to protect the local accounts against an unauthorized password change. Reset Windows Password can successfully extract and display the secret questions.

Resetting password

Reset or change user account password

Resetting SAM user account password (step 4 of 4)

Enter new password for the user account you selected or set blank password to reset it. Pay special attention to additional options. Windows will decline the password if the account is locked or disabled.

User account information

SAM path	D:\Windows\System32\Config\SAM
Account name	John
Account RID	1001
Account description	

Reset

Account locked	No	Password policy set (ADMIN-PC): No
Account disabled	No	New password conforms to the policy: Yes
Password expired	No	Account lockout policy set: No

➔ New password: 123

<< RESET/CHANGE >>

Home <<<< << Back Next >> Exit

To reset the password, leave the 'New password' field blank and click on the 'Reset/Change' button. Take a note of the additional options. The account must be not locked, disabled or expired.

Besides that, if local or domain password policies are set, make sure that the new password complies with the length and complexity requirements and does not match any of the passwords used earlier (if password history exists.) Otherwise, you will be unable to logon to the system even if you reset the password successfully.

If you are resetting a password of the built-in Administrator, keep in mind that in order to activate this account and logon to the system, you would need to load the system in Safe mode. To do that, before Windows starts loading, keep pressing the F8 key until the textual system boot selection dialog appears. In that dialog, select the safe mode item. After that, the built-in Administrator account will become active, and you will be able to use it.

On Windows 8 and later operating systems, click the *Power* button, press and hold the SHIFT key on your keyboard and select *Restart*.

Note that you will have to enter a non-empty password in order to be able to log on LiveID or Microsoft account.

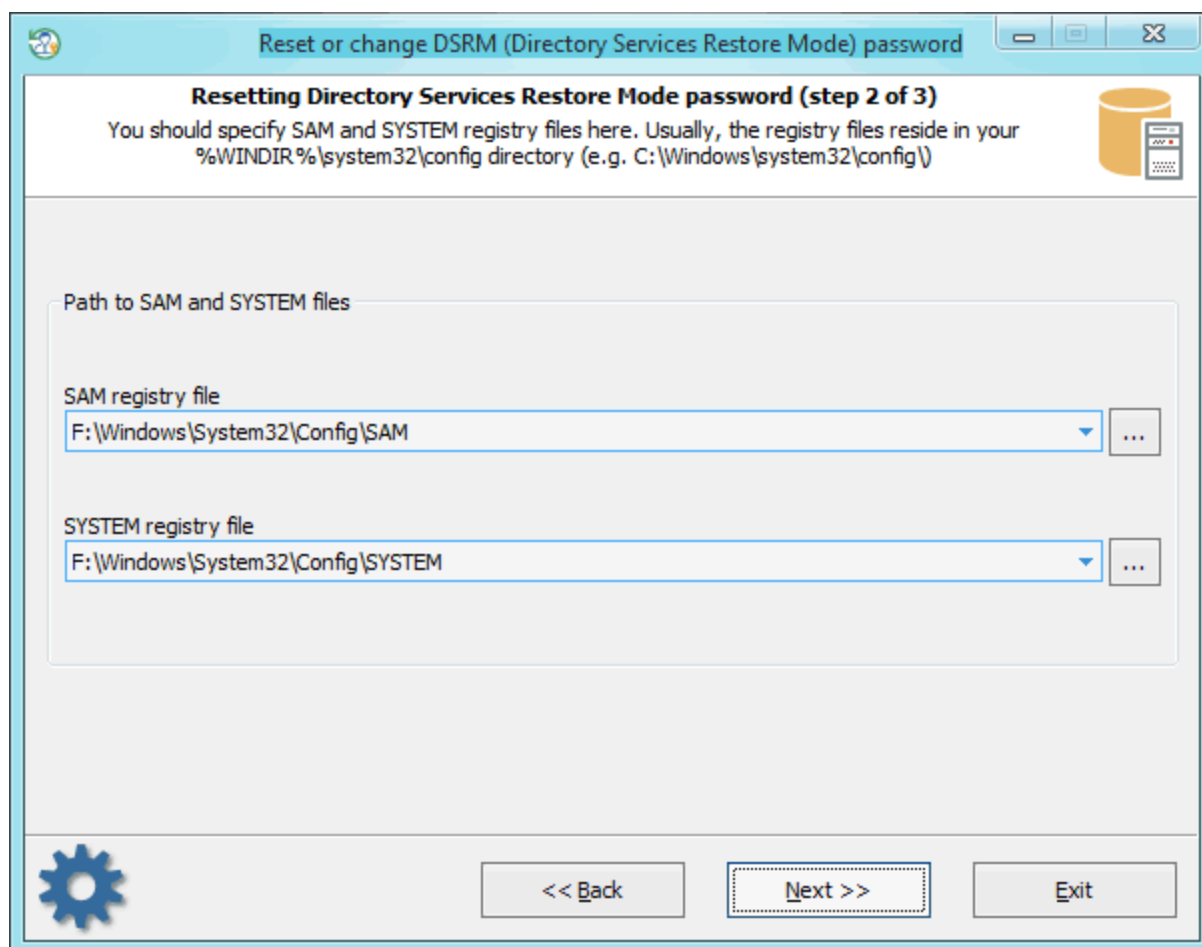
3.3 Reset DSRM passwords

What is DSRM

DSRM (known as **Directory Services Repair Mode** or **Directory Services Restore Mode** in versions prior to Windows Server 2012) is a special boot mode of a Windows Server domain controller that is something similar to Safe Mode with Networking, but without Active Directory running. DSRM is used to restore Active Directory from a backup. It is also helpful in different situations and problems with the AD.

To get into DSRM one needs to press the F8 key immediately after BIOS/UEFI POST screen, but before the Windows logo appears. In Windows Server 2012 and later OSes there's **Advanced Boot Options** menu or **Windows Recovery Environment** for that.

Selecting data source



Password recovery process for DSRM account is almost the same as for regular user account. First you'll have to specify the location for **SAM** and **SYSTEM** registry files.

Resetting password

The screenshot shows a Windows-style dialog box titled "Reset or change DSRM (Directory Services Restore Mode) password". The main heading is "Resetting Directory Services Restore Mode password (step 3 of 3)". Below this, it says "Enter new password for DSRM account you selected or set blank to reset it." There is a user icon in the top right corner. The dialog is divided into two sections: "General information" and "Reset DSRM password".

General information

SAM path	F:\Windows\System32\Config\SAM
SYSTEM path	F:\Windows\System32\Config\SYSTEM
System role	Domain controller
Password present	Yes

Reset DSRM password

→ New password: Secret!@#&\$

<< RESET/CHANGE >>

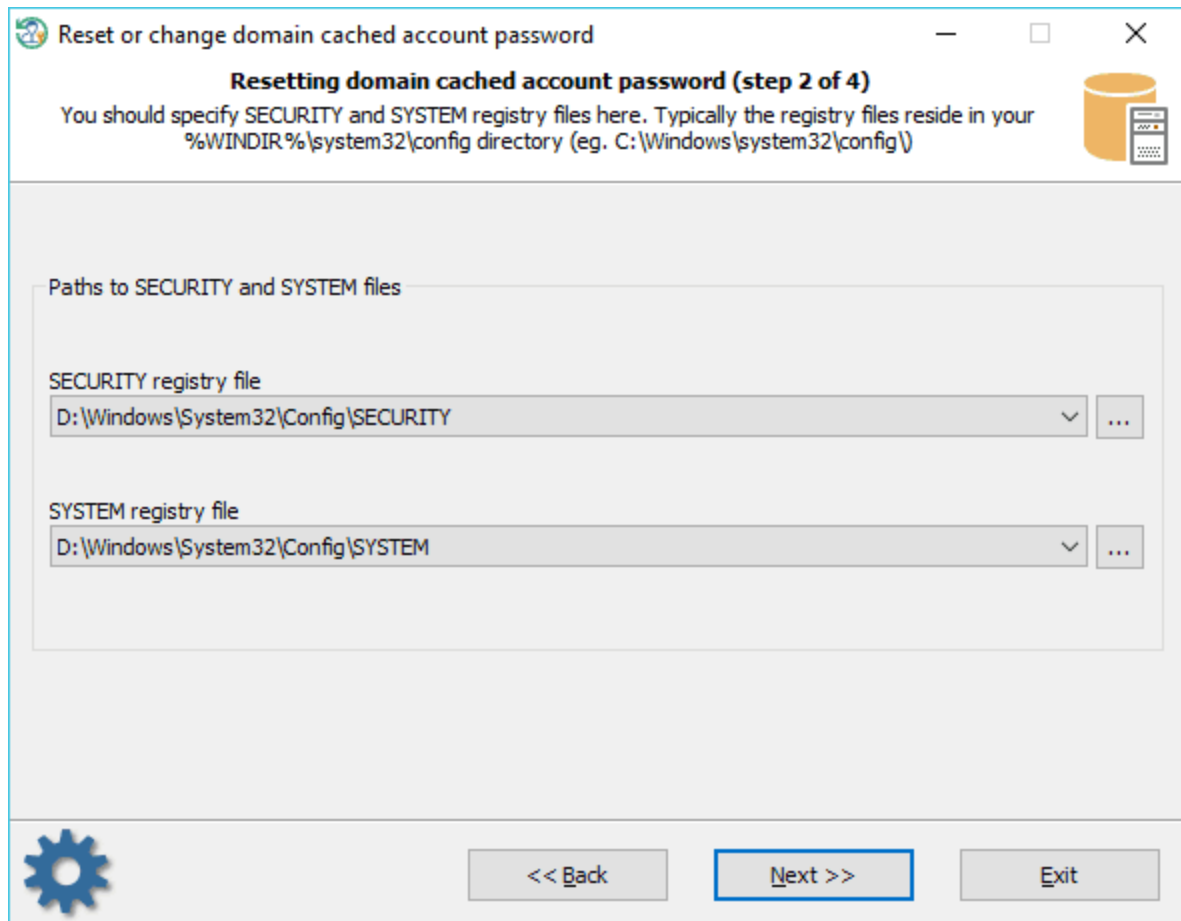
At the bottom, there is a gear icon, a "<< Back" button, a "Next >>" button, and an "Exit" button.

Type in a new password or just set the input field blank if you want to reset it. Then confirm the changes by clicking the 'RESET/CHANGE' button. The program may ask you to create a backup file. You can use the backup file later to roll-back the changes.

3.4 Reset domain cached password

When a user logs on to a Windows domain, the user's domain credentials are securely cached and saved to his/her PC. This feature allows users logging on to the domain when the local workstation is disconnected from the network or even if no domain controller is available. To get around the problem of lost or forgotten password for the domain account, you can simply reset your domain cached credentials using Reset Windows Password. The process consists of 3 simple steps.

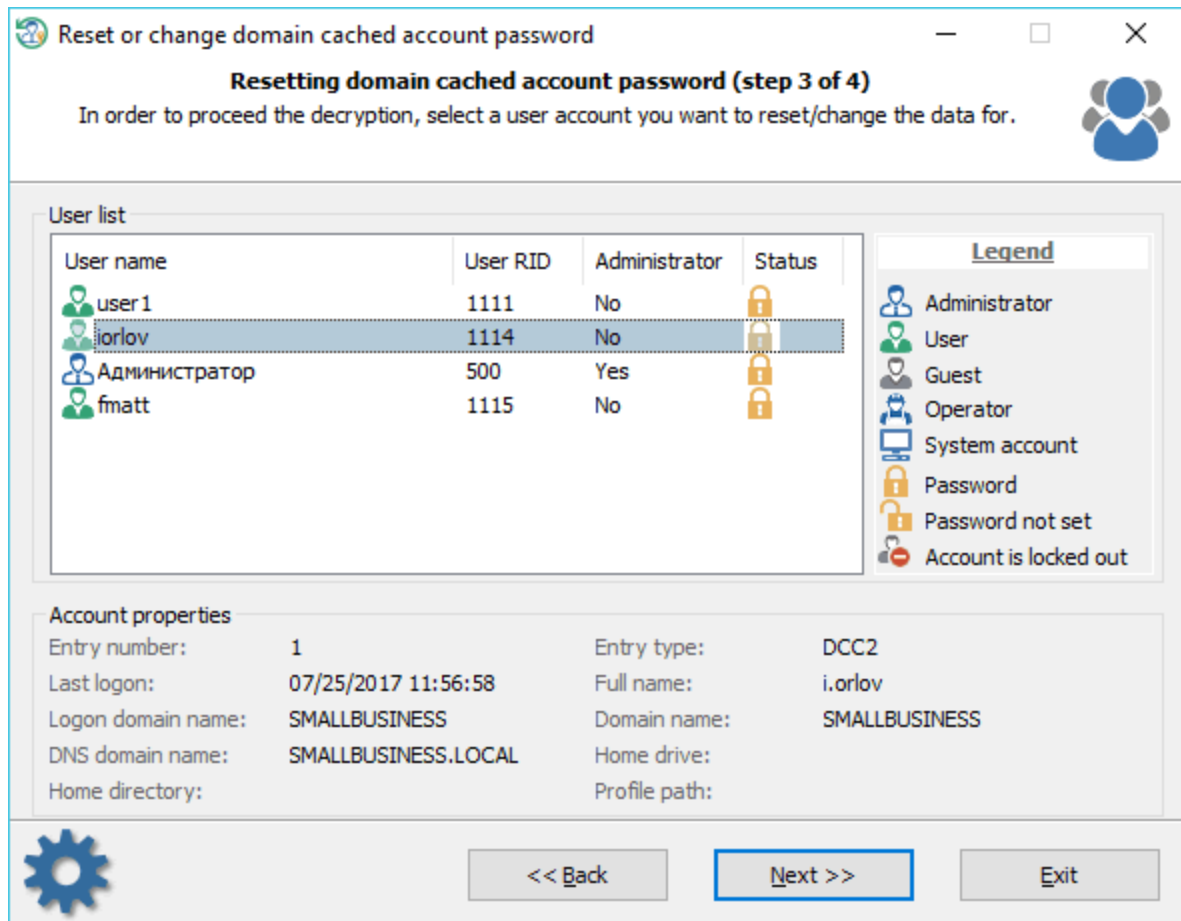
Selecting registry files



To reset a domain cached password, you should provide two registry files: **SECURITY** and **SYSTEM**. Both files are located in the **%WINDIR%\system32\config** folder. Where %WINDIR% is your windows directory. Usually, the program takes care of that and suggests the files it found.

Before proceeding to the next recovery step, make sure you selected exactly the files you need.

Selecting domain account



The upper part of the dialog displays a list of found cached entries with the names of the user accounts. Select one of the entries to view its properties: the full name of the user account, last login date, logon domain, home directory, etc.

Resetting password

Reset or change domain cached account password

Resetting domain cached account password (step 4 of 4)

Enter new password for selected domain cached account or set input box to blank to reset it.

General information

SECURITY registry: D:\WinW\System32\Config\SECURITY

Account name: iorlov

Account RID: 1114

Full name: i.orlov

Reset DCC password

→ New password: Test123

☒ Change passwords for all cached entries of this user account

<< RESET/CHANGE >>

<< Back Next >> Exit

To reset the password, leave the 'New password' input box empty and click the 'RESET/CHANGE'. Do pay special attention to the additional option. Domain cache is arranged in such a manner that it can contain multiple entries of the same user. If the 'Change password for all cached entries for this user account' option is set, then the program will try to change/reset passwords of all found entries of the selected account (with the specified RID). Otherwise it will reset the password for the selected entry only. It is recommended to set this option on unless you know what you do.

Make sure that your new password meets the domain length and complexity requirements and does not match any of the previously entered passwords (if security policy and password history are used.) Otherwise, Windows may deny access even if the password is successfully modified.

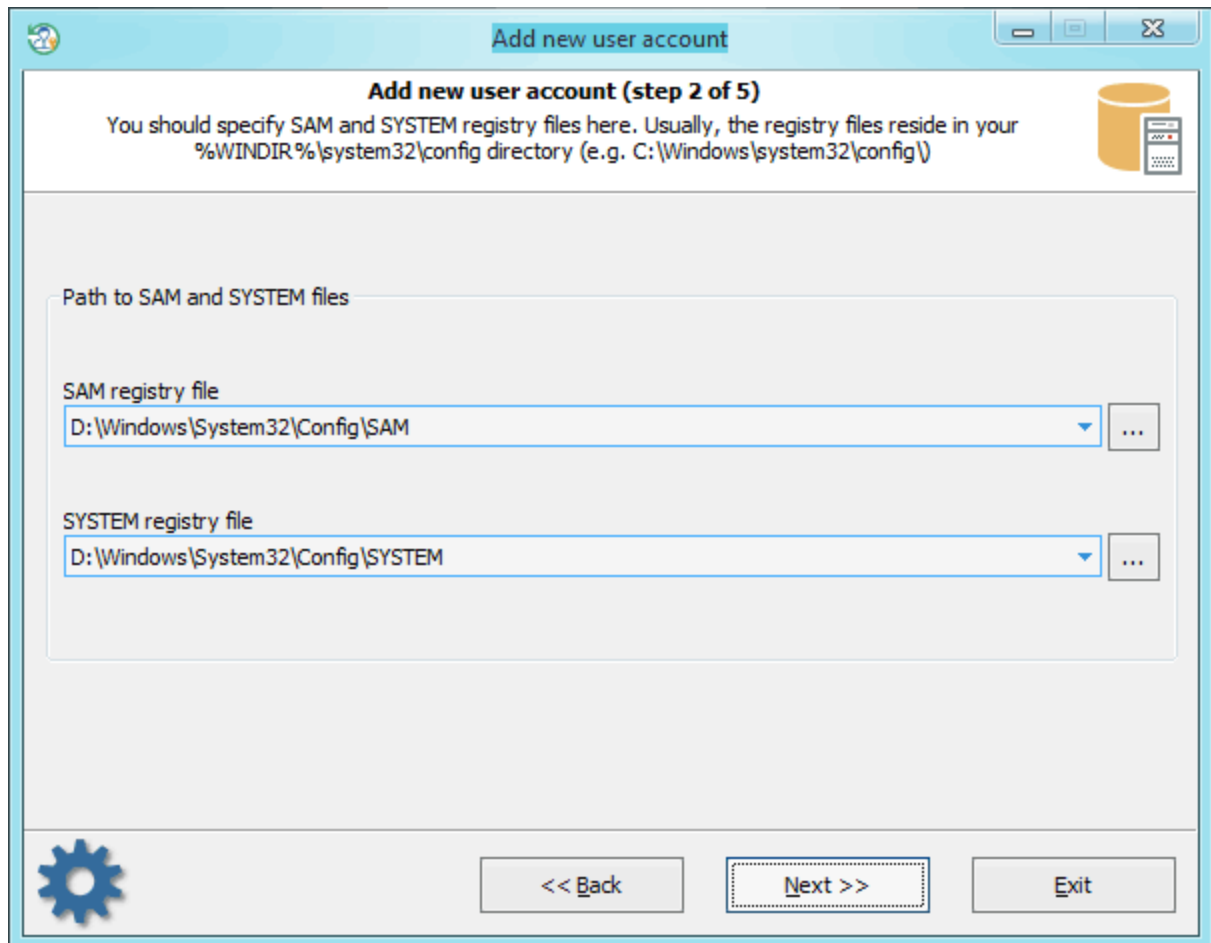
Please note, to log in to your domain account successfully after the cached password is reset, you must temporarily **disable connection to the domain!** Otherwise, Windows will not use the local cached entry but the regular domain credentials instead.

Keep in mind, logging on to the domain with cached credentials gives you access to local resources only.

3.5 Add new user account

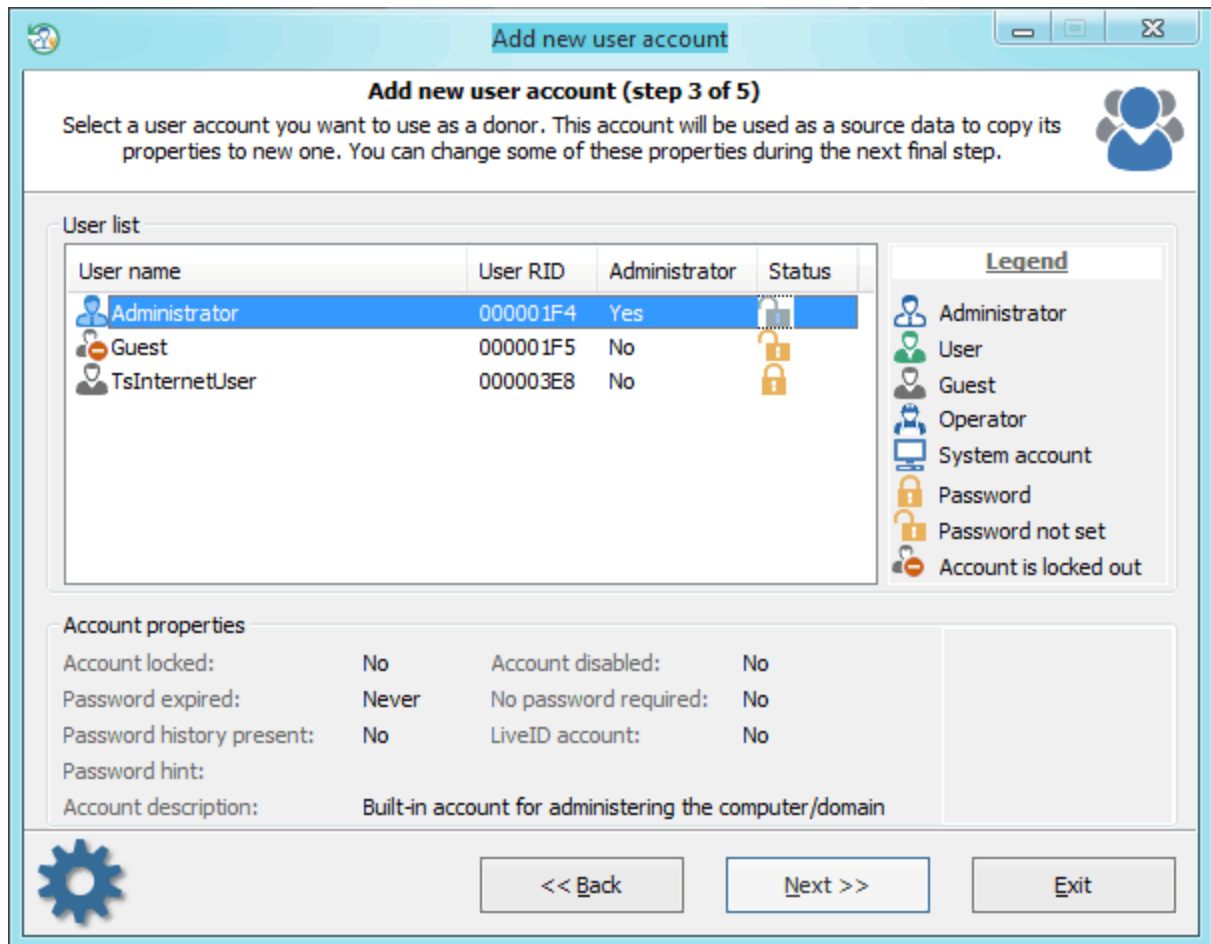
Adding new local account is simple as it is. We tried to arrange it into 3 common steps.

1. Selecting data source



You should select **SAM** and **SYSTEM** files first. The program usually searches for and suggests the files automatically. In case you need to set the files manually for some reason, do know that the registry files are located in the **%WINDIR%\system32\config** directory.

2. Choosing a donor account



Select a user you want to use as a donor account. All properties of the source account will be copied to the newly created one. No problem if the source account is locked or disabled, the program should fix some of its critical properties and set up default flags. For example, if the source account is set to allow logging on to system in certain hours, the program will zero out the restriction.

3. Adding new account

Add new user account (step 4 of 5)

Type in a name and a password for the new user account. You will have to set a non-empty password that conform password policy, if one is set! Click <<Create>> button to add new account to SAM file.

Account properties

Account RID: 000003E9

Account name: new

Account description: my new account

Password: 123

Member of

- Administrators
- Power Users
- Replicator
- Users

Not member of

- Backup Operators
- Guests

<< Create >>

<< Back Next >> Exit

Now all you need is to set a name, description and a password for the new account. Leave the password field blank to set empty password. Note that if the target OS has password policy set, your new password should conform the policy.

You should pay a special attention setting group membership of the new account. Usually, you should make it a member of 'Administrators' and/or 'Users' group in order to be able to log on locally, if otherwise is not specified by your security policy. Setting an incorrect membership may cause troubles, for example, deleting the account.

After the account is created successfully, you can step back to the main dialog, select '[Edit account properties](#)' mode and set/unset some extended flags, if needed.

3.6 Edit user account properties

New version of the program allows you manipulating with extended properties of the target user account, as well as changing Microsoft Live ID account to local account or vice versa. This is an extremely helpful when you need to unlock/enable locked/disabled account, unset the 'password expired' flag, disable the

"Smart card logon" if your smart card has lost occasionally, etc. Modifying properties of the problem account is easy pretty much. First you should select the target Operating System's files.

Selecting data source

The screenshot shows a Windows-style dialog box titled "Edit user account properties". The main heading is "Modify account flags and properties (step 2 of 4)". Below the heading, there is a text instruction: "You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)".

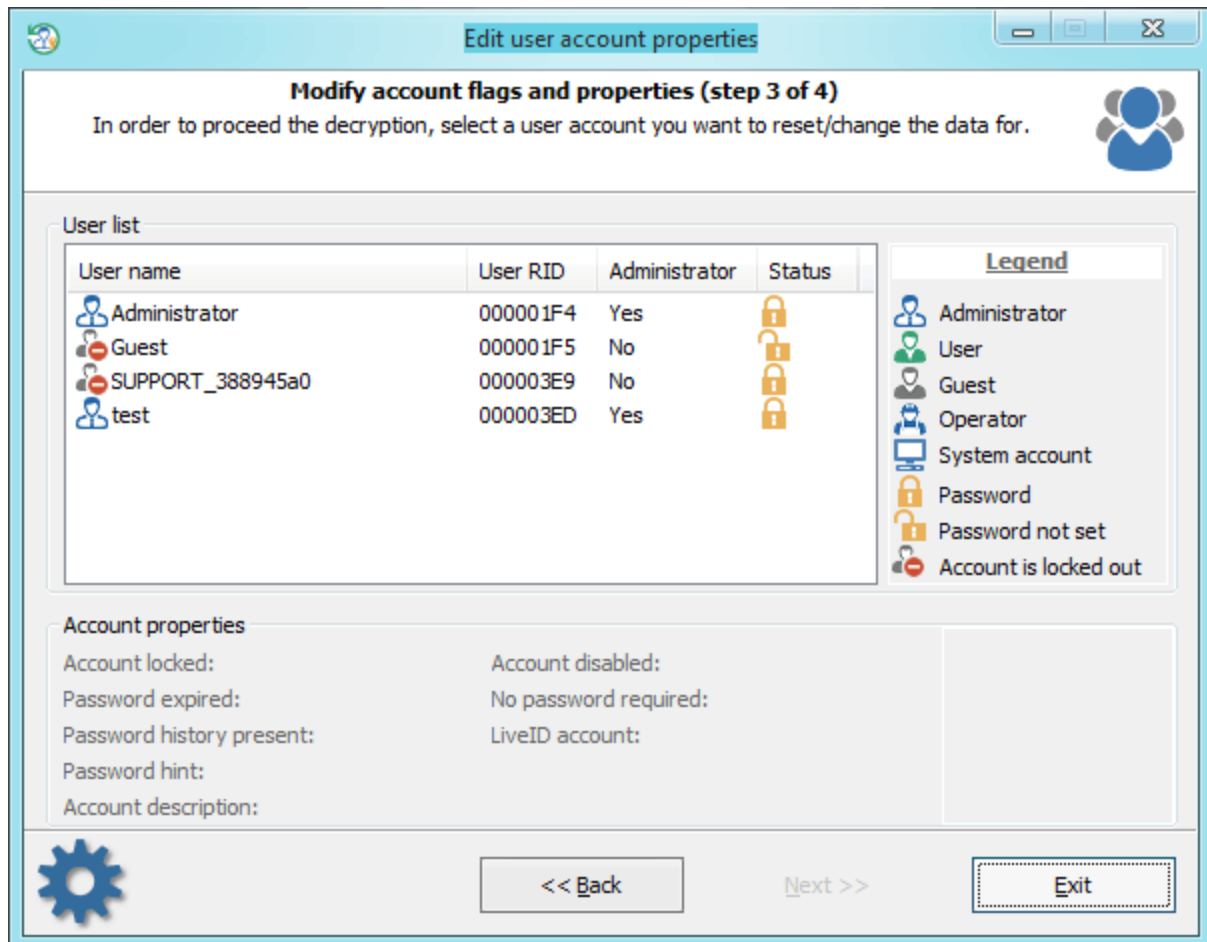
Under the heading "Path to SAM and SYSTEM files", there are two input fields:

- "SAM registry file" with the value "F:\WINDOWS\System32\Config\SAM" and a browse button (three dots).
- "SYSTEM registry file" with the value "F:\WINDOWS\System32\Config\SYSTEM" and a browse button (three dots).

At the bottom of the dialog, there is a gear icon on the left and three buttons: "<< Back", "Next >>" (which is highlighted with a dashed border), and "Exit".

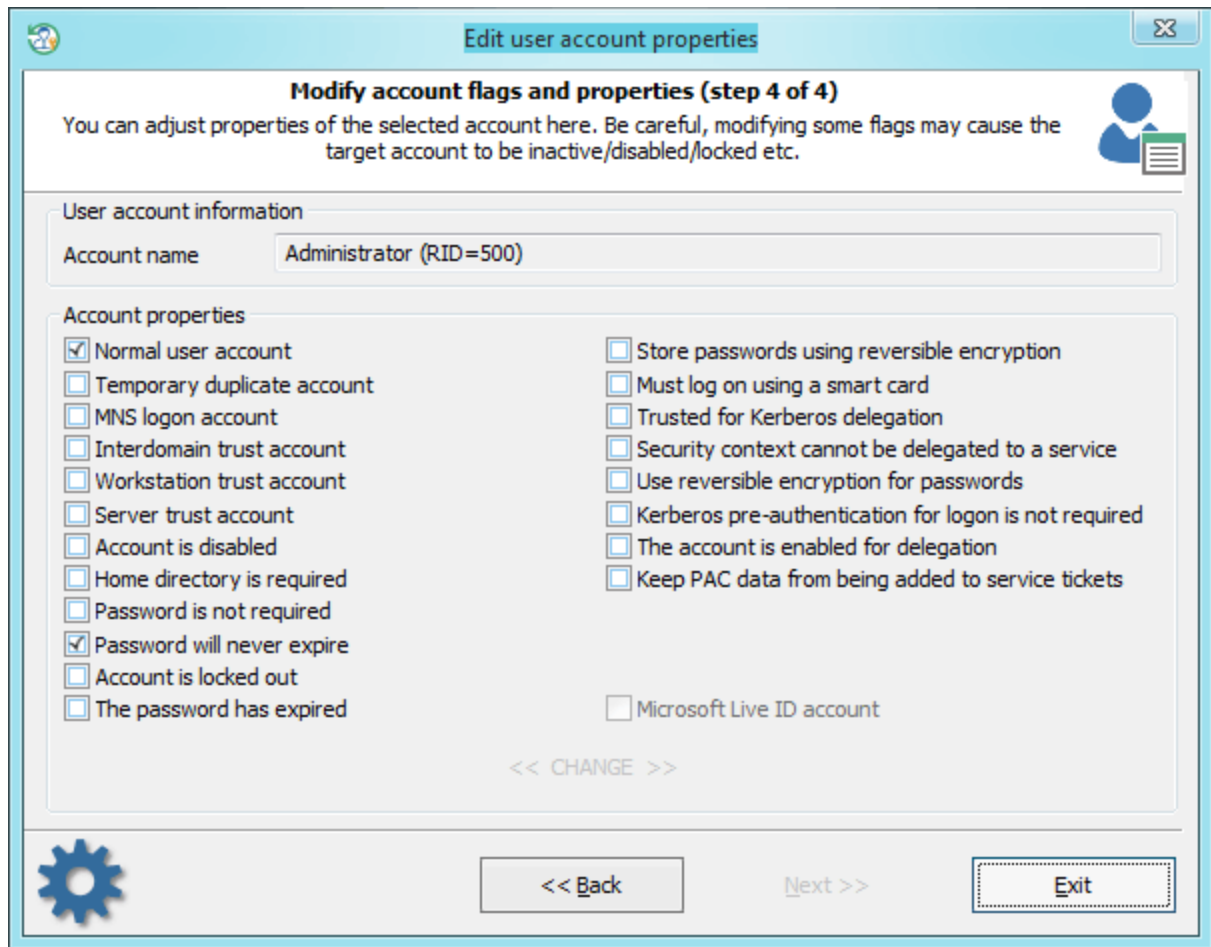
Two files are needed. These are either **SAM** and **SYSTEM** (in case you're modifying a local account) or **NTDS.DIT** and **SYSTEM** (when you need to change the properties of a domain user). The program automatically searches for these files and suggests the first ones it finds. You can also specify paths to these files manually. They are located in the **%WINDIR%\system32\config** and **%WINDIR%\NTDS** folders. Where %WINDIR% is your windows directory. So the full path to the Active Directory database may look like this: C:\Windows\NTDS\ntds.dit

Choosing a Windows account



Once the source files are selected, the program enumerates and displays the list of all found user accounts. Select one you need and click 'Next' button to open the final dialog with the user's properties.

Changing account properties



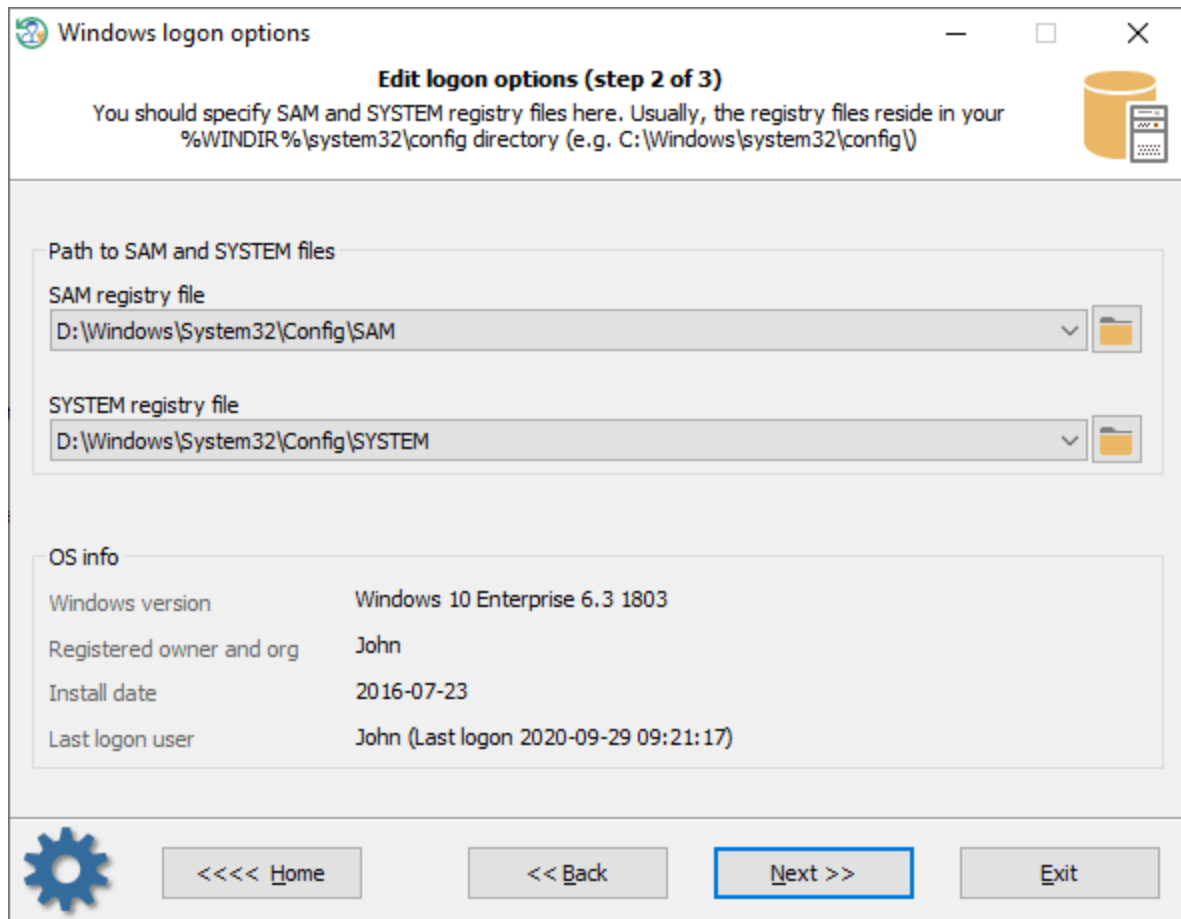
You can set/unset here different flags that control the behavior of the user account.

Be careful, changing some flags may cause the target account to be locked/disabled etc.

3.7 Logon policy options

You can use the settings to change the way users log on to Windows. For example, display last logged on user name, assign a default domain for logon, turn on/off passwordless sign-in, etc.

Selecting data source



Windows logon options

Edit logon options (step 2 of 3)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

Path to SAM and SYSTEM files

SAM registry file
D:\Windows\System32\Config\SAM

SYSTEM registry file
D:\Windows\System32\Config\SYSTEM

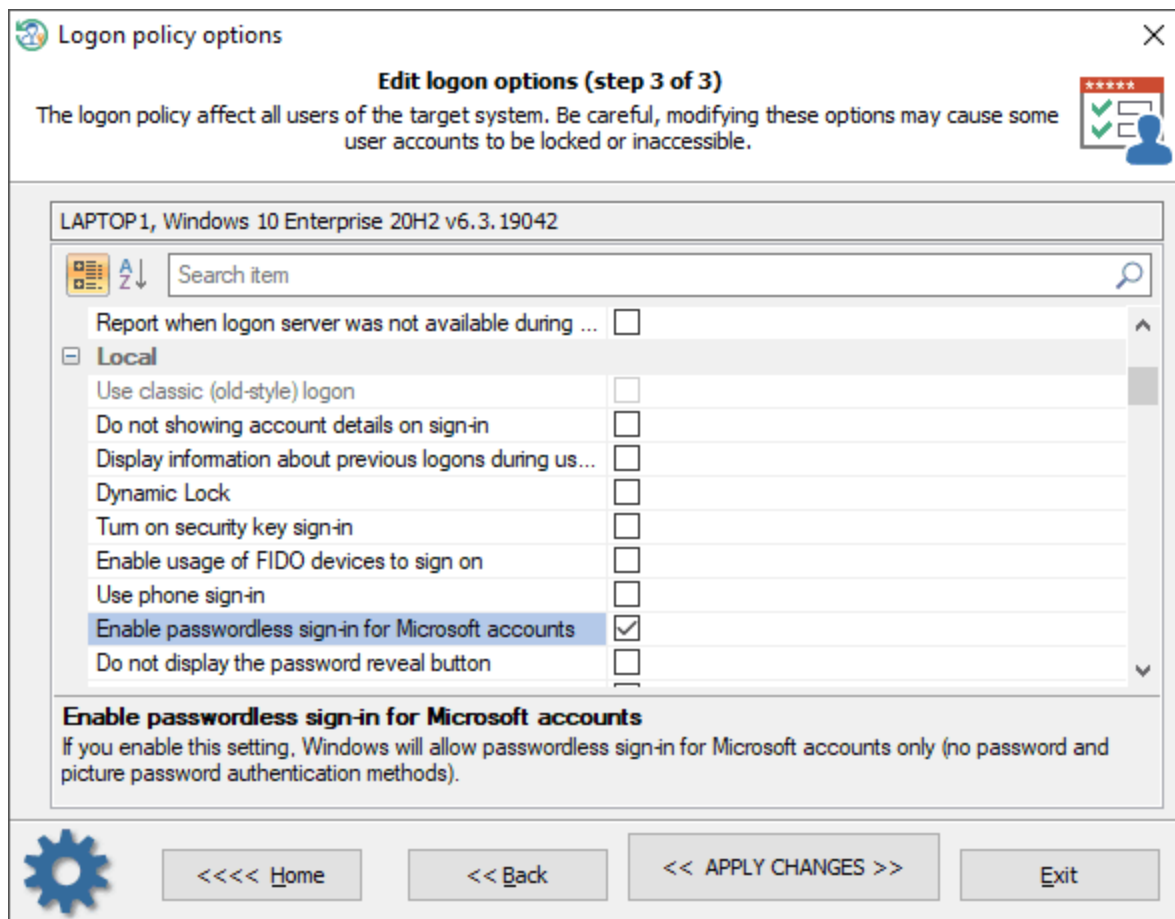
OS info

Windows version	Windows 10 Enterprise 6.3 1803
Registered owner and org	John
Install date	2016-07-23
Last logon user	John (Last logon 2020-09-29 09:21:17)

Settings icon: <<<< Home << Back Next >> Exit

First, choose SAM and SYSTEM registry files that were found by the program or specify paths to them manually if RWP failed to find ones.

Changing logon policy options



Once the files are selected, you can alter any available logon options. Click the << APPLY CHANGES >> button to apply and save the changes. The options affect all local users of the target system.

Be careful, modifying these options may cause some accounts to be inaccessible or locked.

The setting of the **Domain** group:

Name	Description
Allow users to select when a password is required when resuming from connected standby	If you enable this setting, a user on a Connected Standby device can change the amount of time after the device's screen turns off before a password is required when waking the device. If you disable this setting, a user cannot change the amount of time after the device's screen turns off before a password is required when waking the device. Instead, a password is required immediately after the screen turns off.
Default domain for logon	Specifies a default logon domain, which might be a different domain than the domain to which the computer is joined.
Do not enumerate connected users on domain-joined computers	If you enable this setting, the Logon UI will not enumerate any connected users on domain-joined computers.
Enumerate local users on domain-joined computers	If you enable this setting, Logon UI will enumerate all local users on domain-joined computers.

Turn off picture password sign-in for domain users	This setting allows you to control whether a domain user can sign in using a picture password.
Turn on convenience PIN sign-in for domain users	If you enable this setting, a domain user can set up and sign in with a convenience PIN. Note: The user's domain password will be cached in the system vault when using this feature.
Report when logon server was not available during user logon	This setting controls whether the logged on user should be notified if the logon server could not be contacted during logon and he has been logged on using previously stored account information.

The setting of the **Local** group:

Name	Description
Use classic (old-style) logon	Always use classic logon interface scheme
Do not showing account details on sign-in	If set, prevents the user from showing account details (email address or user name) on the sign-in screen.
Display information about previous logons during user logon	If you enable this setting, a message appears after the user logs on that displays the date and time of the last successful logon by that user, the date and time of the last unsuccessful logon attempted with that user name, and the number of unsuccessful logons since the last successful logon by that user.
Dynamic Lock	If you enable this setting, Windows will enable dynamic lock for all users on managed devices and users will not be allowed to disable dynamic lock on their accounts.
Turn on security key sign-in	If you enable this setting, users can sign in with external security keys.
Enable usage of FIDO devices to sign on	This setting allows users to use a FIDO device, such as a phone, NFC card, to sign on to a desktop computer running Windows 10.
Use phone sign-in	If you enable this setting, phone sign-in will be enabled, allowing the use of a phone as a companion device for desktop authentication.
Enable passwordless sign-in for Microsoft accounts	If you enable this setting, Windows will allow passwordless sign-in only: both password and picture password authentication methods will be turned off. This option affects Microsoft accounts only.
Do not display the password reveal button	If you enable this setting, the password reveal button will not be displayed after a user types a password in the password entry text box.
Prevent the use of security questions for local accounts	If you turn this setting on, local users won't be able to set up and use security questions to reset their passwords.
Allow companion device for secondary authentication	If you enable or do not configure this setting, users can authenticate to Windows Hello using a companion device. Such as a phone, fitness band, or IoT device.
Software Secure Attention Sequence	This setting controls whether or not software can simulate the Secure Attention Sequence (SAS).
The mode of automatically signing in and locking last interactive user after a restart or cold boot	This setting controls the configuration under which an automatic restart and sign on and lock occurs after a restart or cold boot.
Sign-in and lock last interactive user	This setting controls whether a device will automatically sign in and lock the last interactive user after the system restarts or after a shutdown and cold

automatically after a restart	boot. This only occurs if the last interactive user didn't sign out before the restart or shutdown.?
-------------------------------	--

The setting of the **Misc** group:

Name	Description
Always use custom logon background	If you enable this policy setting, the logon screen always attempts to load a custom background instead of the Windows-branded logon background.
Show clear logon background	This setting disables the acrylic blur effect on logon background image.
Do not display the Getting Started welcome screen at logon	If you enable this setting, the welcome screen is hidden from the user logging on to the system.
Turn off app notifications on the lock screen	This setting allows you to prevent app notifications from appearing on the lock screen.
Show first sign-in animation	This setting allows you to control whether users see the first sign-in animation when signing in to the computer for the first time.
Turn off Windows Startup sound	Turn off Windows sounds during authentication
Do not process the legacy run list	This setting ignores the customized run list (programs and services that the system starts).
Do not process the run once list	If you enable this setting, the system ignores the list of additional programs and documents that are started automatically the next time the system starts. The customized run-once lists are stored in the registry in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\runOnce.
Hide entry points for Fast User Switching	This setting allows you to hide the Switch User interface in the Logon UI, the Start menu and the Task Manager.
Block all consumer Microsoft account user authentication	If this setting is enabled, all applications and services on the device are prevented from using Microsoft accounts for authentication.
Default credential provider	Assign a specified credential provider as the default credential provider.
Exclude credential providers	This setting allows the administrator to exclude the specified credential providers from use during authentication.

The setting of the **Network** group:

Name	Description
Always wait for the network at computer startup and logon	Determines whether computers wait for the network to be fully initialized during startup and user logon. By default, computers do not wait for the network to be fully initialized at startup and logon.
Do not display network selection UI	If you enable this setting, the PC's network connectivity state cannot be changed without signing into Windows.

The setting of the **Biometrics** group:

Name	Description
Allow domain users to log on using biometrics	If you enable or do not configure this setting, Windows allows domain users to log on to a domain-joined computer using biometrics.

Allow users to log on using biometrics	If you enable or do not configure this setting, all users can log on to a local Windows-based computer and can elevate permissions with UAC using biometrics.
Allow the use of biometrics	If you enable or do not configure this setting, the Windows Biometric Service is available, and users can run applications that use biometrics on Windows.
Configure enhanced anti-spoofing	If you enable this setting, Windows requires all users on managed devices to use enhanced anti-spoofing for Windows Hello face authentication. This disables Windows Hello face authentication on devices that do not support enhanced anti-spoofing.
Specify timeout for fast user switching events	This setting specifies the number of seconds a pending fast user switch event will remain active before the switch is initiated. By default, a fast user switch event is active for 10 seconds before becoming inactive.

The setting of the **PIN** group:

Name	Description
PIN expiration	This setting specifies the period of time in days (between 1 and 730) that a PIN can be used before the system requires the user to change it.
PIN history	This setting specifies the number of past PINs that can be associated to a user account that can't be reused. The value must be between 0 to 50 PINs.
Maximum PIN length	Maximum PIN length configures the maximum number of characters allowed for the PIN. The largest number you can configure for this policy setting is 127.
Minimum PIN length	Minimum PIN length configures the minimum number of characters required for the PIN. The lowest number you can configure for this policy setting is 4.
Require digits	If you enable or do not configure this setting, Windows requires users to include at least one digit in their PIN.
Require lowercase letters	If you enable this setting, Windows requires users to include at least one lowercase letter in their PIN.
Require special characters	If you enable this policy setting, Windows requires users to include at least one special character in their PIN.
Require uppercase letters	If you enable this policy setting, Windows requires users to include at least one uppercase letter in their PIN.

The setting of the **Windows Hello** group:

Name	Description
Allow enumeration of emulated smart card for all users	Windows prevents users on the same computer from enumerating provisioned Windows Hello for Business credentials for other users. If you enable this setting, Windows allows all users of the computer to enumerate all Windows Hello for Business credentials, but still require each user to provide their own factors for authentication.
Device unlock factors A	First unlock factor credential providers
Device unlock factors B	Second unlock factor credential providers
Device unlock rules	Signal rules for device unlock
Dynamic lock factors	If you enable this setting, these signal rules will be evaluated to detect user absence and automatically lock the device.
Dynamic lock rules	Signal rules for dynamic lock
Turn off smart card emulation	If you enable this setting, Windows Hello for Business provisions Windows Hello for Business credentials that are not compatible with smart card applications.

Use a hardware security device	If you enable this setting, Windows Hello for Business provisioning only occurs on devices with usable 1.2 or 2.0 TPMs. You can optionally exclude security devices, which prevents Windows Hello for Business provisioning from using those devices.
Do not use the tpm 1.2 security devices	Exclude TPM 1.2 security devices.]
Use biometrics	If you enable or do not configure this setting, Windows Hello for Business allows the use biometric gestures.
Use certificate for on-premises authentication	If you enable this setting, Windows Hello for Business enrolls a sign-in certificate that is used for on-premises authentication.
Use PIN Recovery	If you enable this setting, Windows Hello for Business uses the PIN recovery service.
Use Windows Hello for Business certificates as smart card certificates	If you enable this setting, applications use Windows Hello for Business certificates as smart card certificates. Biometric factors are unavailable when a user is asked to authorize the use of the certificate's private key.
Use Windows Hello for Business	If you enable this setting, the device provisions Windows Hello for Business using keys or certificates for all users.
Do not start Windows Hello provisioning after sign-in	If you enable this setting, Windows Hello for Business does not automatically start provisioning after the user has signed in.

The setting of the **TPM** group:

Name	Description
The level of TPM owner authorization information available to the operating system	This policy setting configures how much of the TPM owner authorization information is stored in the registry of the local computer. Depending on the amount of TPM owner authorization information stored locally, the operating system and TPM-based applications can perform certain TPM actions which require TPM owner authorization without requiring the user to enter the TPM owner password. You can choose to have the operating system store either the full TPM owner authorization value, the TPM administrative delegation blob plus the TPM user delegation blob, or none. If you enable this policy setting, Windows will store the TPM owner authorization in the registry of the local computer according to the operating system managed TPM authentication setting you choose.
Configure the system to clear the TPM if it is not in a ready state.	This policy setting configures the system to prompt the user to clear the TPM if the TPM is detected to be in any state other than Ready. This policy will take effect only if the system's TPM is in a state other than Ready, including if the TPM is "Ready, with reduced functionality". The prompt to clear the TPM will start occurring after the next reboot, upon user login only if the logged in user is part of the Administrators group for the system. The prompt can be dismissed, but will reappear after every reboot and login until the policy is disabled or until the TPM is in a Ready state.
Configure the system to use legacy Dictionary Attack Prevention Parameters setting for TPM 2.0	This policy setting configures the TPM to use the Dictionary Attack Prevention Parameters (lockout threshold and recovery time) to the values that were used for Windows 10 Version 1607 and below. Setting this policy will take effect only if a) the TPM was originally prepared using a version of Windows after Windows 10 Version 1607 and b) the System has a TPM 2.0. Note that enabling this policy will only take effect after the TPM maintenance task runs (which typically happens after a system restart). Once this policy has been enabled on a system and has taken effect (after a system restart), disabling it will have no impact and the system's TPM will remain configured using the

	legacy Dictionary Attack Prevention parameters, regardless of the value of this group policy. The only way for the disabled setting of this policy to take effect on a system where it was once enabled is to a) disable it from group policy and b)clear the TPM on the system.
Ignore the default list of blocked TPM commands	If you enable this policy setting, Windows will ignore the computer's default list of blocked TPM commands and will only block those TPM commands specified by Group Policy or the local list.
Ignore the local list of blocked TPM commands	If you enable this policy setting, Windows will ignore the computer's local list of blocked TPM commands and will only block those TPM commands specified by Group Policy or the default list.
Standard User Individual Lockout Threshold	This policy setting allows you to manage the maximum number of authorization failures for each standard user for the Trusted Platform Module (TPM). If the number of authorization failures for the user within the duration for Standard User Lockout Duration equals this value, the standard user is prevented from sending commands to the Trusted Platform Module (TPM) that require authorization. This setting helps administrators prevent the TPM hardware from entering a lockout mode because it slows the speed standard users can send commands requiring authorization to the TPM. If this value is not configured, a default value of 4 is used.
Standard User Lockout Duration	This policy setting allows you to manage the duration in minutes for counting standard user authorization failures for Trusted Platform Module (TPM) commands requiring authorization. If the number of TPM commands with an authorization failure within the duration equals a threshold, a standard user is prevented from sending commands requiring authorization to the TPM. If this value is not configured, a default value of 480 minutes (8 hours) is used.
Standard User Total Lockout Threshold	This policy setting allows you to manage the maximum number of authorization failures for all standard users for the Trusted Platform Module (TPM). If the total number of authorization failures for all standard users within the duration for Standard User Lockout Duration equals this value, all standard users are prevented from sending commands to the Trusted Platform Module (TPM) that require authorization. This setting helps administrators prevent the TPM hardware from entering a lockout mode because it slows the speed standard users can send commands requiring authorization to the TPM. If this value is not configured, a default value of 9 is used.
Turn on TPM backup to Active Directory Domain Services (1 of 2)	If you enable this option along with one below, TPM owner information will be automatically and silently backed up to AD DS when you use Windows to set or change a TPM owner password.
Turn on TPM backup to Active Directory Domain Services (2 of 2)	If you enable this option along with one above, TPM owner information will be automatically and silently backed up to AD DS when you use Windows to set or change a TPM owner password.

3.8 Interface and system restriction policy

You can use this feature to change or reset different interface and system restrictions for the selected user. For example, allow/disallow access to specific Windows applications, lock/unlock the Run Dialog box, enable/disable certain control panel settings, allow/prevent access to the command prompt or the Windows registry, allow/prohibit access to CD-ROM or removable disks, etc.

Choosing Windows registry files

Interface and system restriction policy

Edit interface and system restrictions (step 2 of 4)

You should specify SAM and SYSTEM registry files here. Usually, the registry files reside in your %WINDIR%\system32\config directory (e.g. C:\Windows\system32\config\)

Path to SAM and SYSTEM files

SAM registry file
D:\Windows\System32\Config\SAM

SYSTEM registry file
D:\Windows\System32\Config\SYSTEM

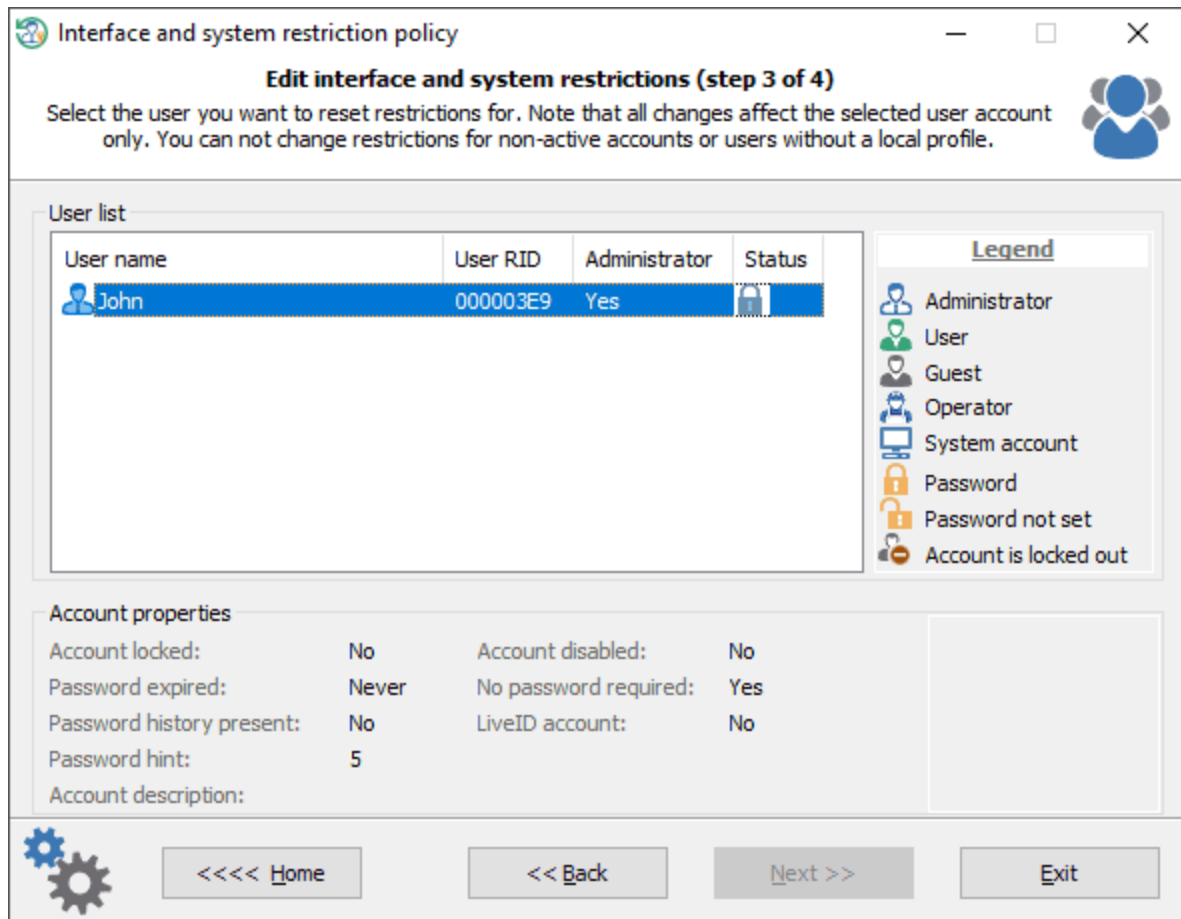
OS info

OS version	Windows 10 Enterprise 6.3 1803
OS owner and org	John
OS install date	2018-05-03
Last logon user	John (Last logon 2018-10-13 12:44:54)

Navigation buttons: <<<< Home, << Back, **Next >>**, Exit

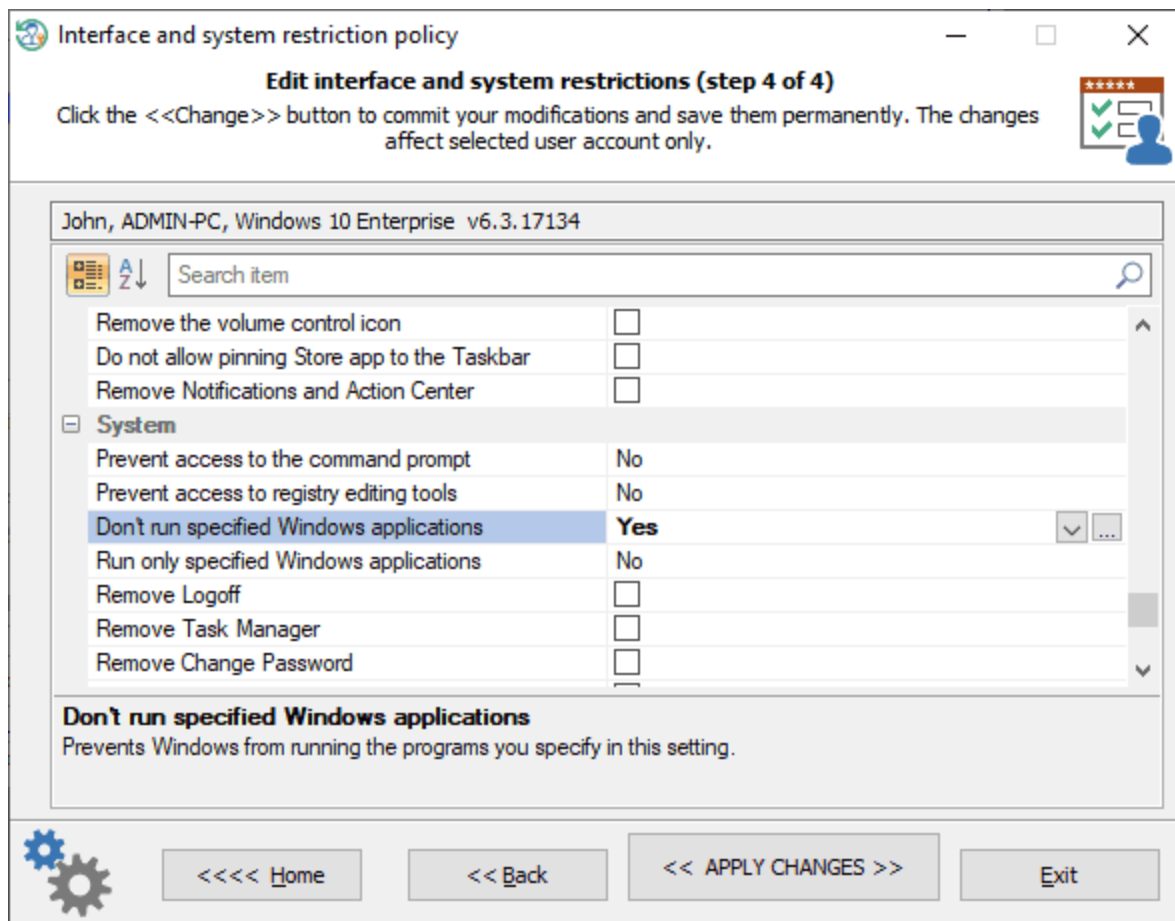
Choose the SAM and SYSTEM registry files found by the program, or specify the path to them manually.

Selecting user account



Select the user you want to change or reset the restrictions for. The program displays only active accounts that have a local profile.

Changing interface and system restrictions for selected user



Once the user is selected, you can alter the interface and system options available for the user account. Click the << APPLY CHANGES >> button to commit the changes.

The options affect selected user account only.

Short description of the interface and system options.

Control panel restrictions:

Name	Description
Hide specified Control Panel items	This option allows you to display or hide specified Control Panel items, such as Mouse, System, or Personalization, from the Control Panel window and the Start screen. The option affects the Start screen and Control Panel window, as well as other ways to access Control Panel items, such as shortcuts in Help and Support or command lines that use control.exe. This policy has no effect on items displayed in PC settings. If you enable this setting, you can select specific items not to display on the Control Panel window and the Start screen.
Show only specified Control Panel items	This option controls which Control Panel items such as Mouse, System, or Personalization, are displayed on the Control Panel window and the Start screen. The only items displayed in Control Panel are those you specify in this setting. This option affects the Start screen and Control Panel, as well as other ways to access Control Panel items such as shortcuts in Help and Support or command lines that use control.exe. This policy has no effect on items

	displayed in PC settings. For example, enter Microsoft.Mouse, Microsoft.System, or Microsoft.Personalization.
Prohibit access to Control Panel and PC settings	Disables all Control Panel programs and the PC settings app. This option prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
Settings Page Visibility	Specifies the list of pages to show or hide from the System Settings app. This policy allows an administrator to block a given set of pages from the System Settings app. Blocked pages will not be visible in the app, and if all pages in a category are blocked the category will be hidden as well. Example: showonly:about,bluetooth hide:bluetooth
Disable the Display Control Panel	If you enable this setting, the Display Control Panel does not run. When users try to start Display, a message appears explaining that a setting prevents the action.
Hide Settings tab	Removes the Settings tab from Display in Control Panel
Prevent changing theme	This option disables the theme gallery in the Personalization Control Panel.
Prevent changing visual style for windows and buttons	Prevents users or applications from changing the visual style of the windows and buttons displayed on their screens.
Enable screen saver	If you disable this setting, screen savers do not run. Also, this option disables the Screen Saver section of the Screen Saver dialog in the Personalization or Display Control Panel. As a result, users cannot change the screen saver options.
Prevent changing color and appearance	Disables the Color (or Window Color) page in the Personalization Control Panel, or the Color Scheme dialog in the Display Control Panel on systems where the Personalization feature is not available. This option prevents users from using Control Panel to change the window border and taskbar color (on Windows 8), glass color (on Windows Vista and Windows 7), system colors, or color scheme of the desktop and windows.
Prevent changing desktop background	Prevents users from adding or changing the background design of the desktop. If you enable this setting, none of the Desktop Background settings can be changed by the user.
Prevent changing desktop icons	Prevents users from changing the desktop icons. If you enable this setting, none of the desktop icons can be changed by the user.
Prevent changing mouse pointers	If you enable this setting, none of the mouse pointer scheme settings can be changed by the user.
Prevent changing screen saver	This option prevents users from using Control Panel to add, configure, or change the screen saver on the computer. It does not prevent a screen saver from running.
Prevent changing sounds	If you enable this setting, none of the Sound Scheme settings can be changed by the user.
Password protect the screen saver	If you enable this setting, all screen savers are password protected. If you disable this setting, password protection cannot be set on any screen saver.
Browse the network to find printers	Allows users to use the Add Printer Wizard to search the network for shared printers.
Browse a common web site to find printers	Adds a link to an Internet or intranet Web page to the Add Printer Wizard.
Turn off Windows default printer management	This preference allows you to change default printer management. If you enable this setting, Windows will not manage the default printer.

Prevent addition of printers	Prevents users from using familiar methods to add local and network printers. If this option is enabled, it removes the Add Printer option from the Start menu. (To find the Add Printer option, click Start, click Printers, and then click Add Printer.) This option also removes Add Printer from the Printers folder in Control Panel.
Prevent deletion of printers	If this option is enabled, it prevents users from deleting local and network printers. If a user tries to delete a printer, such as by using the Delete option in Printers in Control Panel, a message appears explaining that a setting prevents the action.
Hide "Set Program Access and Computer Defaults" page	This option removes the Set Program Access and Defaults page from the Programs Control Panel. As a result, users cannot view or change the associated page.
Hide "Get Programs" page	Prevents users from viewing or installing published programs from the network. If this option is enabled, users cannot view the programs that have been published by the system administrator, and they cannot use the "Get Programs" page to install published programs. Enabling this feature does not prevent users from installing programs by using other methods. Users will still be able to view and installed assigned (partially installed) programs that are offered on the desktop or on the Start menu.
Hide "Installed Updates" page	This option prevents users from accessing "Installed Updates" page from the "View installed updates" task.
Hide "Programs and Features" page	This option prevents users from accessing "Programs and Features" to view, uninstall, change, or repair programs that are currently installed on the computer.
Hide the Programs Control Panel	This option prevents users from using the Programs Control Panel in Category View and Programs and Features in Classic View.
Hide "Windows Features"	This option prevents users from accessing the "Turn Windows features on or off" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs. As a result, users cannot view, enable, or disable various Windows features and services.
Hide "Windows Marketplace"	This option prevents users from access the "Get new programs from Windows Marketplace" task from the Programs Control Panel in Category View, Programs and Features in Classic View, and Get Programs.
Hide Regional and Language Options administrative options	This option removes the Administrative options from the Region settings control panel. Administrative options include interfaces for setting system locale and copying settings to the default user. This option does not, however, prevent an administrator or another application from changing these values programmatically.
Hide the geographic location option	This option removes the option to change the user's geographical location (GeoID) from the Region settings control panel.
Hide the select language group options	This option removes the option to change the user's menus and dialogs (UI) language from the Language and Regional Options control panel.
Hide user locale selection and customization options	This option removes the regional formats interface from the Region settings control panel.

Desktop restrictions:

Name	Description
Hide Network Locations icon on desktop	Removes the Network Locations icon from the desktop.

Remove the Desktop Cleanup Wizard	Prevents users from using the Desktop Cleanup Wizard.
Remove Computer icon on the desktop	This option hides Computer from the desktop and from the new Start menu. It also hides links to Computer in the Web view of all Explorer windows, and it hides Computer in the Explorer folder tree pane. If the user navigates into Computer via the "Up" button while this option is enabled, they view an empty Computer folder. This option allows administrators to restrict their users from seeing Computer in the shell namespace, allowing them to present their users with a simpler desktop environment.
Remove Properties from the Documents icon context menu	This option hides the Properties menu command on the shortcut menu for the My Documents icon.
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Prevents users from manipulating desktop toolbars. If you enable this setting, users cannot add or remove toolbars from the desktop. Also, users cannot drag toolbars on to or off of docked toolbars.
Remove Recycle Bin icon from desktop	Removes most occurrences of the Recycle Bin icon.
Hide Internet Explorer icon on desktop	Removes the Internet Explorer icon from the desktop and from the Quick Launch bar on the taskbar.
Hide and disable all items on the desktop	Removes icons, shortcuts, and other default and user-defined items from the desktop, including Briefcase, Recycle Bin, Computer, and Network Locations.
Remove Properties from the Recycle Bin context menu	Removes the Properties option from the Recycle Bin context menu.
Remove Properties from the Computer icon context menu	This option hides Properties on the context menu for Computer.
Hide Active Directory folder	Hides the Active Directory folder in Network Locations.
Prohibit adjusting desktop toolbars	Prevents users from adjusting the length of desktop toolbars. Also, users cannot reposition items or toolbars on docked toolbars.
Remove My Documents icon on the desktop	Removes most occurrences of the My Documents icon.
Enable Active Desktop	Enables Active Desktop and prevents users from disabling it.
Disable Active Desktop	Disables Active Desktop and prevents users from enabling it.
Prohibit changes	Prevents the user from enabling or disabling Active Desktop or changing the Active Desktop configuration.
Prohibit adding items	Prevents users from adding Web content to their Active Desktop.
Prohibit closing items	Prevents users from removing Web content from their Active Desktop.
Prohibit editing items	Prevents users from changing the properties of Web content items on their Active Desktop.
Prohibit deleting items	Prevents users from deleting Web content from their Active Desktop.
Disable all items	Removes Active Desktop content and prevents users from adding Active Desktop content.
Add/delete items	Adds and deletes specified Web content items.

Network restrictions:

Name	Description
------	-------------

Prohibit connecting and disconnecting a remote access connection	Determines whether users can connect and disconnect remote access connections.
Prohibit deletion of remote access connections	Determines whether users can delete remote access connections.
Prohibit renaming private remote access connections	Determines whether users can rename their private remote access connections.
Ability to rename all user remote access connections	Determines whether non-administrators can rename all-user remote access connections.
Prohibit access to the Remote Access Preferences item on the Advanced menu	Determines whether the Remote Access Preferences item on the Advanced menu in Network Connections folder is enabled.
Prohibit access to properties of a LAN connection	Determines whether users can change the properties of a LAN connection.
Prohibit TCP/IP advanced configuration	Determines whether users can configure advanced TCP/IP settings.
Prohibit access to the Advanced Settings item on the Advanced menu	Determines whether the Advanced Settings item on the Advanced menu in Network Connections is enabled for administrators.
Ability to rename LAN connections	Determines whether non-administrators can rename a LAN connection.
Prohibit adding and removing components for a LAN or remote access connection	Determines whether administrators can add and remove network components for a LAN or remote access connection. This option has no effect on non-administrators.
Ability to delete all user remote access connections	Determines whether users can delete all user remote access connections.
Prohibit changing properties of a private remote access connection	Determines whether users can view and change the properties of their private remote access connections.
Ability to change properties of an all user remote access connection	Determines whether a user can view and change the properties of remote access connections that are available to all users of the computer.
Prohibit access to properties of components of a remote access connection	Determines whether users can view and change the properties of components used by a private or all-user remote access connection.
Enable Windows 2000 Network Connections settings for Administrators	Determines whether settings that existed in Windows 2000 Server family will apply to Administrators.
Prohibit access to properties of components of a LAN connection	Determines whether Administrators and Network Configuration Operators can change the properties of components used by a LAN connection.
Ability to Enable/Disable a LAN connection	Determines whether users can enable/disable LAN connections.

Prohibit viewing of status for an active connection	Determines whether users can view the status for an active connection.
Ability to rename LAN connections or remote access connections available to all users	Determines whether users can rename LAN or all user remote access connections.
Prohibit Enabling/Disabling components of a LAN connection	Determines whether administrators can enable and disable the components used by LAN connections.
Prohibit access to the New Connection Wizard	Determines whether users can use the New Connection Wizard, which creates new network connections.
Prohibit user configuration of Offline Files	Prevents users from enabling, disabling, or changing the configuration of Offline Files.
Remove "Work offline" command	This option removes the "Work offline" command from Explorer, preventing users from manually changing whether Offline Files is in online mode or offline mode.
Remove "Make Available Offline" command	This option prevents users from making network files and folders available offline.
Prohibit access of the Windows Connect Now wizards	This option prohibits access to Windows Connect Now (WCN) wizards.

Start menu and taskbar restrictions:

Name	Description
Remove the "Undock PC" button from the Start Menu	If you enable this setting, the "Undock PC" button is removed from the simple Start Menu, and your PC cannot be undocked.
Remove user folder link from Start Menu	If you enable this option the start menu will not show a link to the user's storage folder.
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	This option prevents users from performing the following commands from the Start menu or Windows Security screen: Shut Down, Restart, Sleep, and Hibernate. This option does not prevent users from running Windows-based programs that perform these functions.
Remove user's folders from the Start Menu	Hides all folders on the user-specific (top) section of the Start menu. Other items appear, but folders are hidden.
Remove programs on Settings menu	This option allows you to remove programs on Settings menu. If you enable this setting, the Control Panel, Printers, and Network and Connection folders are removed from Settings on the Start menu, and from Computer and File Explorer. It also prevents the programs represented by these folders (such as Control.exe) from running.
Remove See More Results / Search Everywhere link	If you enable this policy, a "See more results" / "Search Everywhere" link will not be shown when the user performs a search in the start menu search box.
Remove Favorites menu from Start Menu	Prevents users from adding the Favorites menu to the Start menu or classic Start menu. If you enable this setting, the Display Favorites item does not appear in the Advanced Start menu options box.
Show QuickLaunch on Taskbar	This option controls whether the QuickLaunch bar is displayed in the Taskbar.

Add the Run command to the Start Menu	If you enable this setting, the Run command is added to the Start menu.
Remove Recorded TV link from Start Menu	This option allows you to remove the Recorded TV link from the Start Menu.
Disable context menus in the Start Menu	This allows you to prevent users from being able to open context menus in the Start Menu.
Remove All Programs list from the Start menu	If you enable this setting, the Start Menu will either collapse or remove the all apps list from the Start menu.
Lock the Taskbar	This option affects the taskbar, which is used to switch between running applications.
Hide the notification area	This option affects the notification area (previously called the "system tray") on the taskbar.
Remove Clock from the system notification area	Prevents the clock in the system notification area from being displayed.
Show "Run as different user" command on Start	This option shows or hides the "Run as different user" command on the Start application bar.
Remove access to the context menus for the taskbar	This option allows you to remove access to the context menus for the taskbar.
Remove Run menu from Start Menu	Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager.
Remove Documents icon from Start Menu	This option allows you to remove the Documents icon from the Start menu and its submenus.
Remove the People Bar from the taskbar	This allows you to remove the People Bar from the taskbar and disables the My People experience.
Remove Help menu from Start Menu	This option allows you to remove the Help command from the Start menu.
Prevent changes to Taskbar and Start Menu Settings	This option allows you to prevent changes to Taskbar and Start Menu Settings.
Remove Downloads link from Start Menu	This option allows you to remove the Downloads link from the Start Menu.
Remove Videos link from Start Menu	This option allows you to remove the Videos link from the Start Menu.
Remove frequent programs list from the Start Menu	If you enable this setting, the frequently used programs list is removed from the Start menu.
Remove Games link from Start Menu	If you enable this option the start menu will not show a link to the Games folder.
Remove Search link from Start Menu	This option allows you to remove the Search link from the Start menu, and disables some File Explorer search elements. Note that this does not remove the search box from the new style Start menu.
Prevent users from customizing their Start Screen	This option allows you to prevent users from changing their Start screen layout.
Remove common program groups from Start Menu	Removes items in the All Users profile from the Programs menu on the Start menu.
Prevent users from uninstalling applications from Start	If you enable this setting, users cannot uninstall apps from Start.

Remove Network Connections from Start Menu	This option allows you to remove Network Connections from the Start Menu.
Remove pinned programs list from the Start Menu	If you enable this setting, the "Pinned Programs" list is removed from the Start menu. Users cannot pin programs to the Start menu.
Add Logoff to the Start Menu	This option only applies to the classic version of the start menu and does not affect the new style start menu.
Remove Default Programs link from the Start menu	This option allows you to remove the Default Programs link from the Start menu.
Remove Recent Items menu from Start Menu	Removes the Recent Items menu from the Start menu. Removes the Documents menu from the classic Start menu.
Remove Music icon from Start Menu	This option allows you to remove the Music icon from Start Menu.
Remove "Recently added" list from Start Menu	This option allows you to prevent the Start Menu from displaying a list of recently installed applications.
Remove Logoff on the Start Menu	This option allows you to removes the "Log Off <username>" item from the Start menu and prevents users from restoring it.
Remove Homegroup link from Start Menu	If you enable this option the Start menu will not show a link to Homegroup. It also removes the homegroup item from the Start Menu options. As a result, users cannot add the homegroup link to the Start Menu.
Remove Search Computer link	If you enable this policy, the "See all results" link will not be shown when the user performs a search in the start menu search box.
Add Search Internet link to Start Menu	If you enable this policy, a "Search the Internet" link is shown when the user performs a search in the start menu search box. This button launches the default browser with the search terms.
Remove Network icon from Start Menu	This option allows you to remove the Network icon from Start Menu.
Remove links and access to Windows Update	This option allows you to remove links and access to Windows Update.
Show additional calendar	By default, the calendar is set according to the locale of the operating system, and users can show an additional calendar. For zh-CN and zh-SG locales, an additional calendar shows the lunar month and date and holiday names in Simplified Chinese (Lunar) by default. For zh-TW, zh-HK, and zh-MO locales, an additional calendar shows the lunar month and date and holiday names in Traditional Chinese (Lunar) by default.
Prevent users from rearranging toolbars	This option allows you to prevent users from rearranging toolbars.
Lock all taskbar settings	This option allows you to lock all taskbar settings.
Remove the battery meter	This option allows you to remove the battery meter from the system control area.
Remove pinned programs from the Taskbar	This option allows you to remove pinned programs from the taskbar.
Remove the Security and Maintenance icon	This option allows you to remove Security and Maintenance from the system control area.
Do not allow pinning programs to the Taskbar	This option allows you to control pinning programs to the Taskbar.

Prevent users from adding or removing toolbars	This option allows you to prevent users from adding or removing toolbars.
Prevent users from moving taskbar to another screen dock location	This option allows you to prevent users from moving taskbar to another screen dock location.
Remove the networking icon	This option allows you to remove the networking icon from the system control area.
Prevent users from resizing the taskbar	This option allows you to prevent users from resizing the taskbar.
Show Windows Store apps on the taskbar	This option allows users to see Windows Store apps on the taskbar.
Remove the volume control icon	This option allows you to remove the volume control icon from the system control area.
Do not allow pinning Store app to the Taskbar	This option allows you to control pinning the Store app to the Taskbar.
Remove Notifications and Action Center	This option removes Notifications and Action Center from the notification area on the taskbar.

System restrictions:

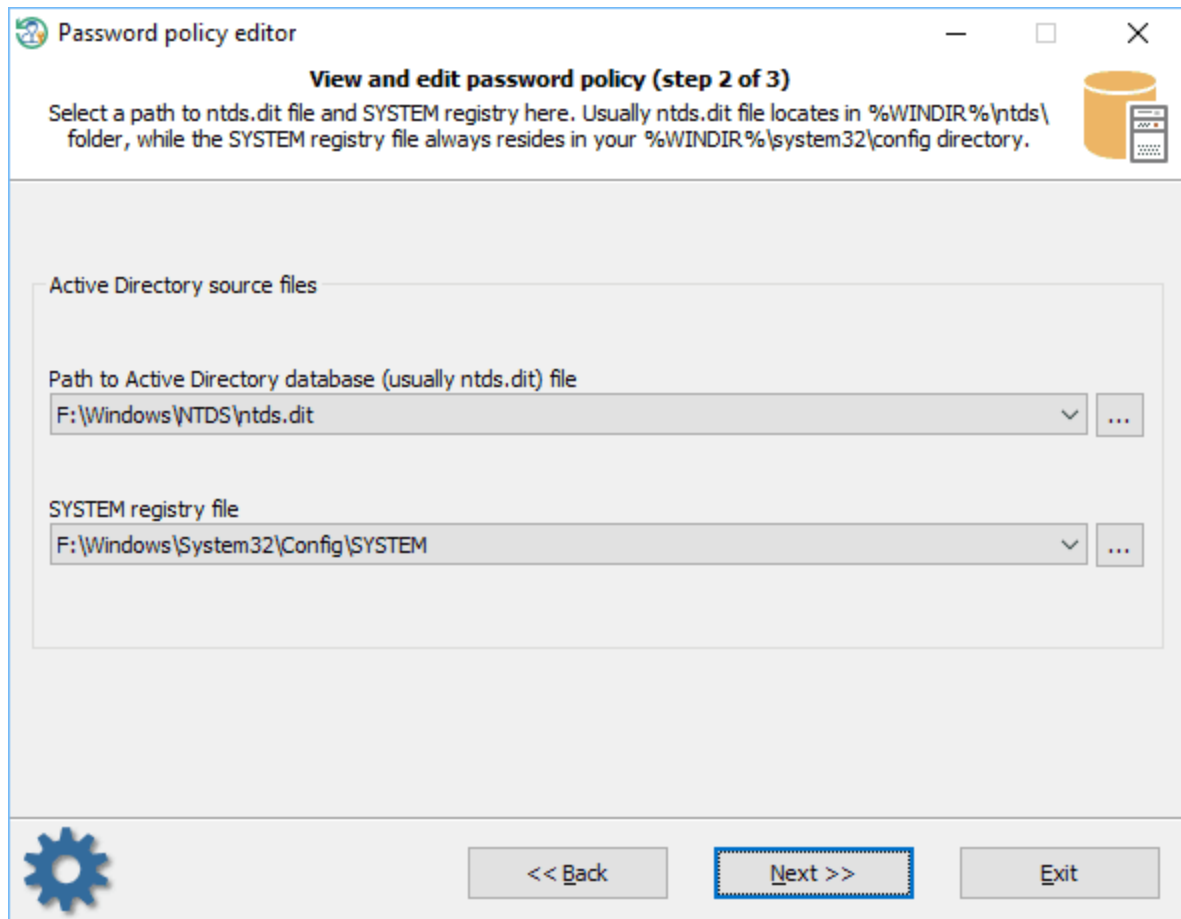
Name	Description
Prevent access to the command prompt	This option prevents users from running the interactive command prompt, Cmd.exe. This option also determines whether batch files (.cmd and .bat) can run on the computer. If you enable this option and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.
Prevent access to registry editing tools	Disables the Windows registry editor Regedit.exe. If you enable this option and the user tries to start Regedit.exe, a message appears explaining that a setting prevents the action.
Don't run specified Windows applications	Prevents Windows from running the programs you specify in this setting.
Run only specified Windows applications	Limits the Windows programs that users have permission to run on the computer.
Remove Logoff	This option disables or removes all menu items and buttons that log the user off the system. If you enable this setting, users will not see the Log off menu item when they press Ctrl+Alt+Del. This will prevent them from logging off unless they restart or shutdown the computer, or clicking Log off from the Start menu.
Remove Task Manager	This option prevents users from starting Task Manager. If you enable this setting, users will not be able to access Task Manager. If users try to start Task Manager, a message appears explaining that a policy prevents the action.
Remove Change Password	This option prevents users from changing their Windows password on demand. If you enable this setting, the 'Change Password' button on the Windows Security dialog box will not appear when you press Ctrl+Alt+Del.
Remove Lock Computer	This option prevents users from locking the system. If you enable this setting, users cannot lock the computer from the keyboard using Ctrl+Alt+Del.
All Removable Storage classes: Deny all access	Configure access to all removable storage classes.

Removable Disks: Deny read access	This option denies read access to removable disks.
Removable Disks: Deny write access	This option denies write access to removable disks.
CD and DVD: Deny read access	This option denies read access to the CD and DVD removable storage class.
CD and DVD: Deny write access	This option denies write access to the CD and DVD removable storage class.
WPD Devices: Deny read access	This option denies read access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices.
WPD Devices: Deny write access	This option denies write access to removable disks, which may include media players, cellular phones, auxiliary displays, and CE devices.
Floppy Drives: Deny read access	This option denies read access to the Floppy Drives removable storage class, including USB Floppy Drives.
Floppy Drives: Deny write access	This option denies write access to the Floppy Drives removable storage class, including USB Floppy Drives.
Tape Drives: Deny read access	This option denies read access to the Tape Drive removable storage class.
Tape Drives: Deny write access	This option denies write access to the Tape Drive removable storage class.

3.9 Password policy editor

Sometimes to functioning security settings properly, it is vitally required to set up workstation's or domain's password policy. For example, if you want to deny domain users to log on to a system without supplying strong passwords, you should restrict it through the domain password policy. However that would be quite a problem if you cannot log on to the workstation or to the domain as an administrator. The new RWP's password policy editor can get around the problem and allows changing various password policy's properties on any Windows system without logging on to the system.

Selecting data source



First of all, you will need to feed the program with two system files:

- either **SAM** and **SYSTEM**, in case you' want to modify password policy of a workstation or a standalone PC;
 - or **NTDS.DIT** and **SYSTEM**, when you need to change the password policy properties of a domain.
- The program should try to find the files automatically. You can however provide the paths manually.

Changing password policy

Password policy editor

View and edit password policy (step 3 of 3)

Password policy affect all system security. Be careful, modifying some flags may cause target accounts be inactive/disabled/locked etc. Setting zero value should disable appropriate attribute.

PC name: WIN-K4HA0SF2R91

Password policy

Minimum password length	<input type="text" value="7"/>	Maximum password age (days)	<input type="text" value="42"/>
Password history length	<input type="text" value="24"/>	Minimum password age (days)	<input type="text" value="1"/>

- ☒ Password must meet complexity requirements
- ☐ The password cannot be changed without logging on
- ☐ Force to use a protocol that does not allow DC to get the plaintext password
- ☐ Allows the built-in administrator account to be locked out from network logons
- ☐ Store passwords using reversible encryption
- ☐ Refuse weekly password change for machine accounts
- ☒ Prevent Windows from storing LM hashes
- ☒ Limit local accounts use of blank passwords to console logon only

<< APPLY CHANGES >>

Navigation buttons: <<<< Home, << Back, Next >>, Exit

Here's the short description of what you can modify in password policy of the target system:

- Minimum password length - minimum length of a valid password, in characters.
- Password history length - number of previous passwords saved in the history list. A user is not allowed to reuse a password from the list.
- Maximum password age - maximum length (in days) that a password can remain the same. Passwords older than this must be changed.
- Minimum password age - minimum length of time before a password can be changed.
- Password must meet complexity requirements - passwords must meet the following minimum requirements: contain no user's account name or a part of it, be at least six characters in length (if otherwise is not set), contain characters from at least three charsets, do not be one used previously (if password history is set).
- The password cannot be changed without logging on - password cannot be changed without logging on. Otherwise, if it has expired, you can change it and then log on.
- Force to use a protocol that does not allow DC to get the plaintext password - forces the client to use a protocol that does not allow the domain controller to get plaintext passwords.
- Allows the built-in administrator account to be locked out from network logons
- Store passwords using reversible encryption - force to store plaintext passwords for all users instead of hashing the passwords.
- Refuse weekly password change for machine accounts - removes the requirement for any machine account to automatically change its password every week.
- Prevent Windows from storing LM hashes. The LAN Manager hash uses an extremely weak encryption algorithm. This setting controls whether a LM hash of the password can be stored in Active

Directory and the local SAM database (the next time a new user is created or the password is changed). This setting is on by default on Windows Vista and later OSes.

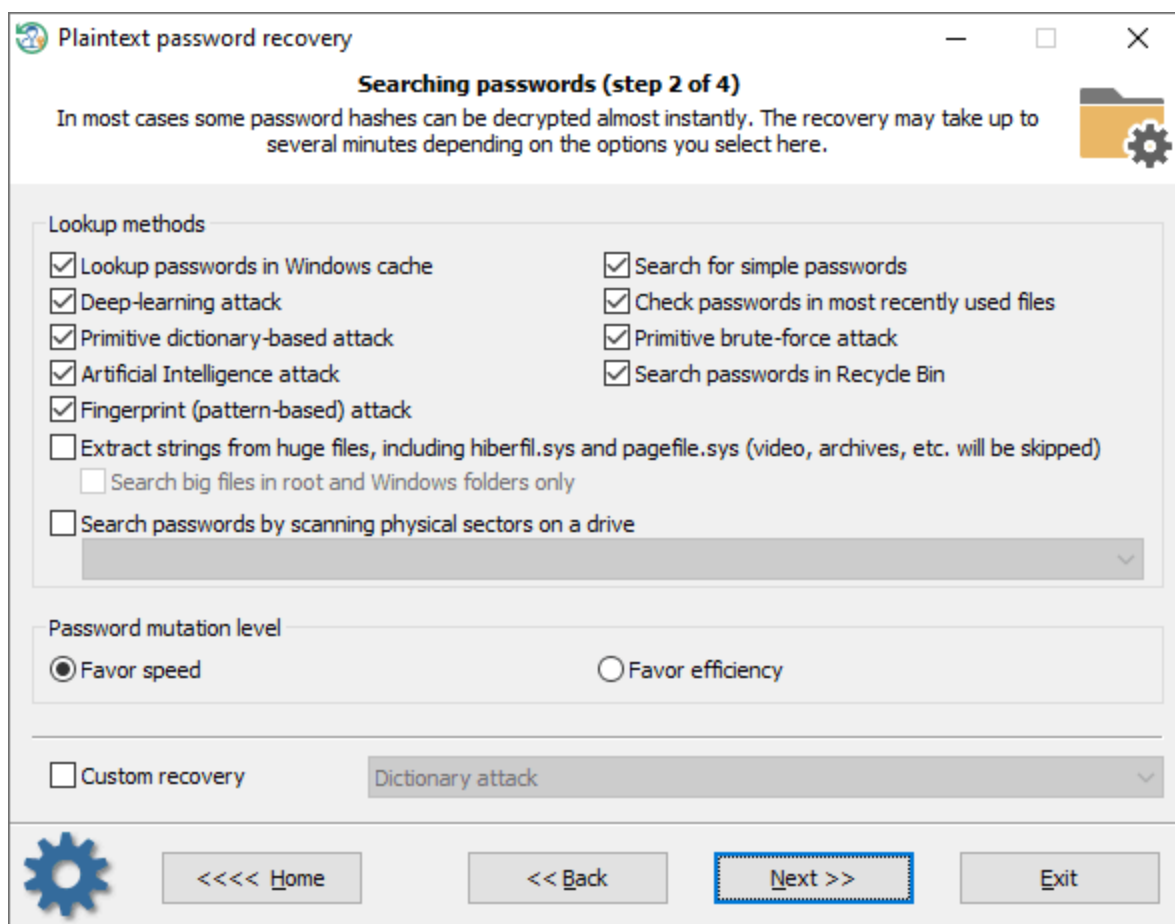
- Limit local accounts to use blank passwords to console logon only. Prevent accounts with blank passwords from existing on a system. However, if a local account with a blank password did exist, enabling this setting will prevent network access, limiting the account to local console logon only.

To disable an editable attribute, just set zero value into its edit box.

Be careful, altering any value of the password policy will affect on all security of the Windows system!

3.10 Search for logon passwords

Setting search and recovery methods



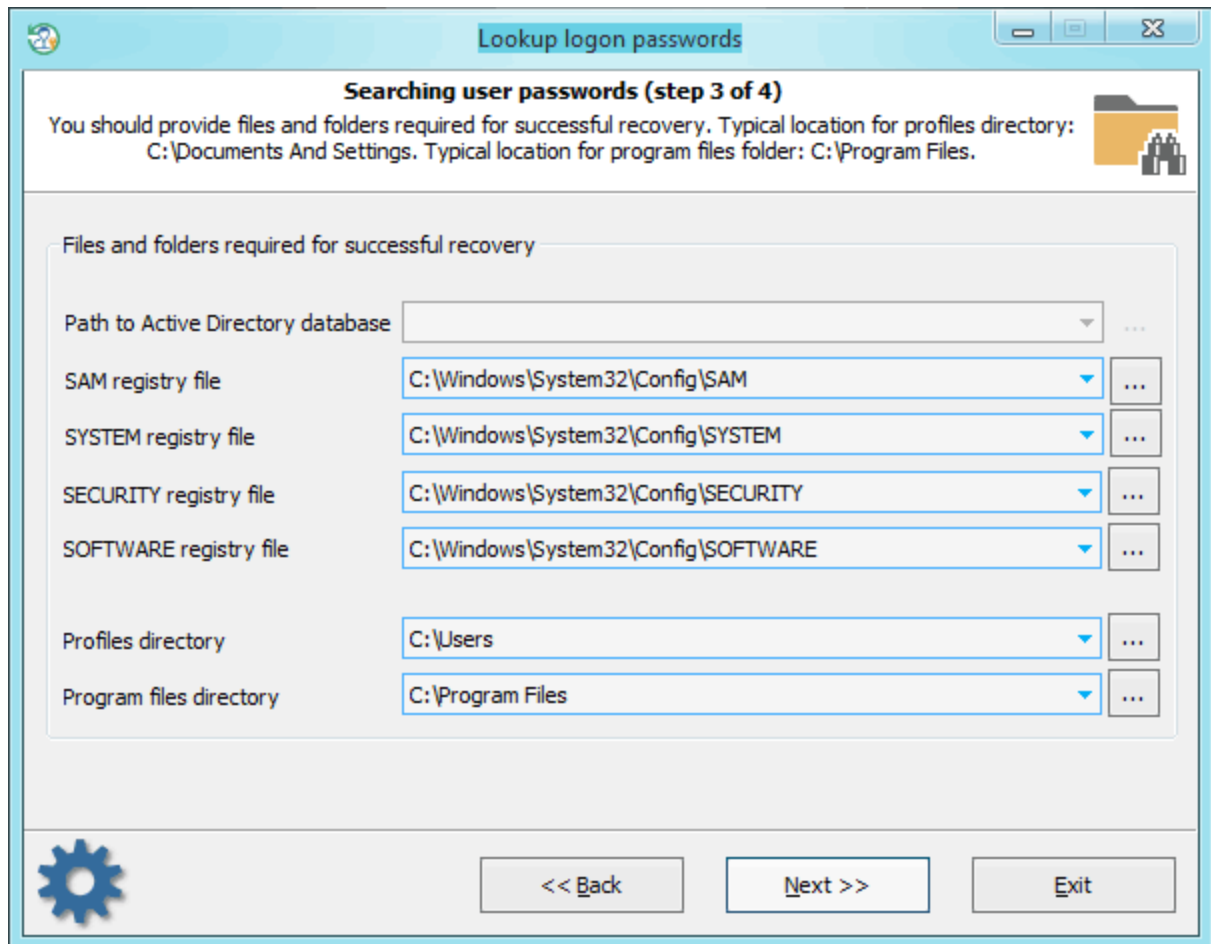
Finding user's passwords takes 11 steps:

1. Finding information in Windows system cache. This method, in its turn, consists of over a dozen of mini-attacks, during which the program analyzes all kinds of personal data like LSA secrets, VPN, WiFi, DSL, FTP, IM, etc, passwords, e-mail correspondence, sticky notes, browser passwords, auto-completion and search phrases, etc.
2. Analyzing simple, short passwords, keyboard shortcuts, etc.

3. Password search using deep learning algorithms. Even though these algorithms are cut significantly to meet CPU requirements, they work much better compared to previous ones.
4. Scan, parse and analyze most recently used files of the target system.
5. Primitive dictionary attack. The application checks all passwords from the built-in dictionary for the Light and Standard editions or from several dictionaries (Arabic, Chinese, English, French, German, Portuguese, Russian, Spanish) for the Advanced Edition. If the deep search option is on, simple word mutations will also be taken into account during the search.
6. Primitive brute-force attack.
7. Artificial Intelligence attack. This is our little 'know-how'. The attack analyzes network activity of a user on the computer. Over thirty mini-modules take care of that. Upon the results of the analysis, the application generates user preferences and generates a semantic dictionary for the attack, which it later uses it for finding the password.
8. Look for passwords in deleted files.
9. Primitive Fingerprint attack on some complicated English passwords.
10. Extract strings from huge files: RAM images, hiberfil.sys, pagefile.sys and so on. When this option is set, the program will try to skip files useless in password analysis like video, archives, audio files, etc.
11. Search passwords by reading and analyzing raw sectors of the selected drive. This feature works for both LM and NTLM hashes, looking for both ASCII and UNICODE passwords. If the '*Password mutation level*' is set to '*Favor efficiency*', the program additionally tries to mutate all found passwords, thus walking through all sectors of the target drive may take quite a time. Note that the sector-based scanning algorithm is not effective against drives which have a full-disk encryption set on. Like Bitlocker or TrueCrypt, for example.

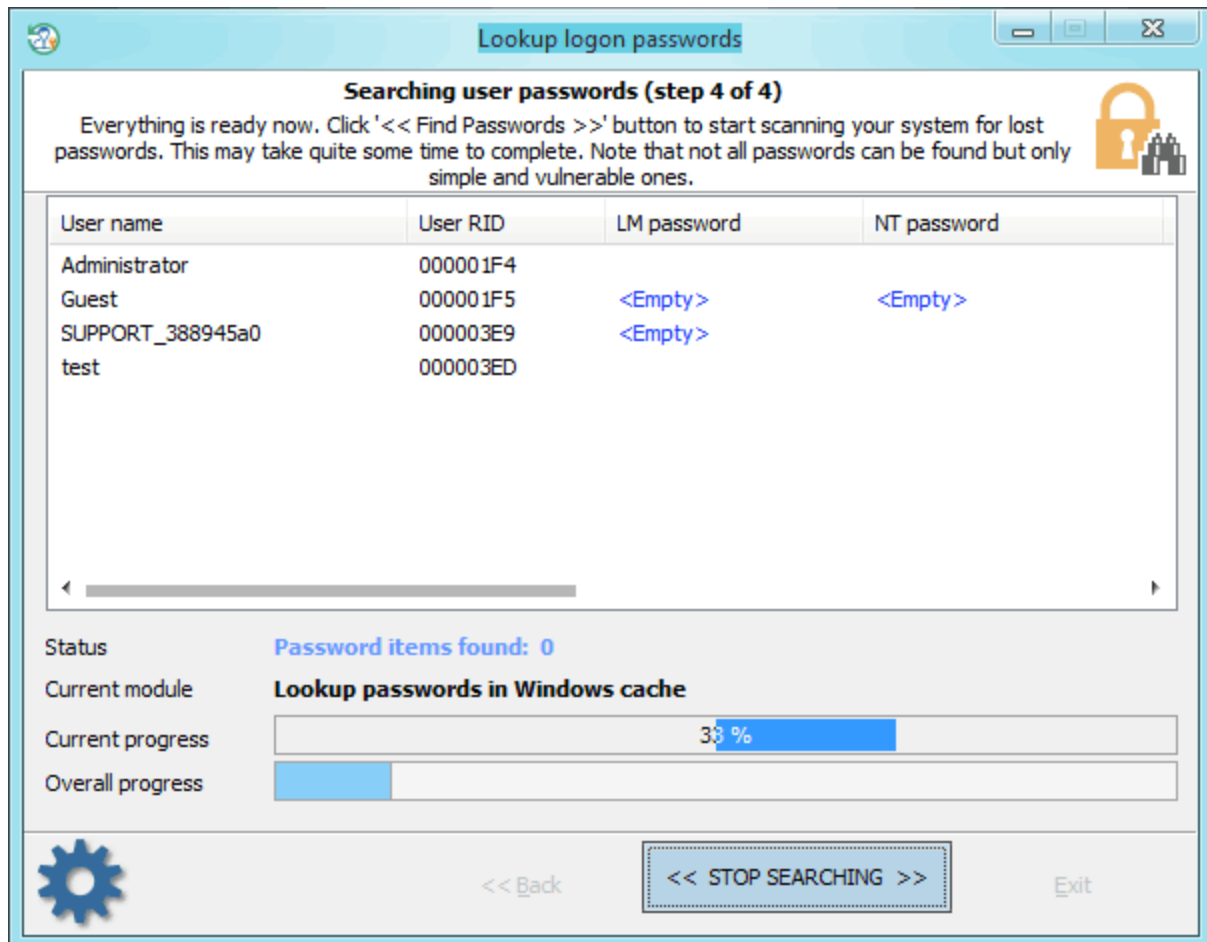
To apply a [custom recovery method](#), turn on the 'Custom recovery' option and select one of the available attacks. On the next step you will be prompted to set up various options related to the selected attack.

Selecting data source



When searching for passwords, special attention is to be paid to entering files and folders required for the analysis process. Without those, password search will be inefficient. The application finds the files automatically, but sometimes, e.g., when the computer has several operating systems installed, you may need to use the 'manual control'. Please also keep in mind that if the computer has 2 or more hard disk drives, the sequence of the letters for these disks can be set totally different than in the original system.

Searching and decrypting passwords



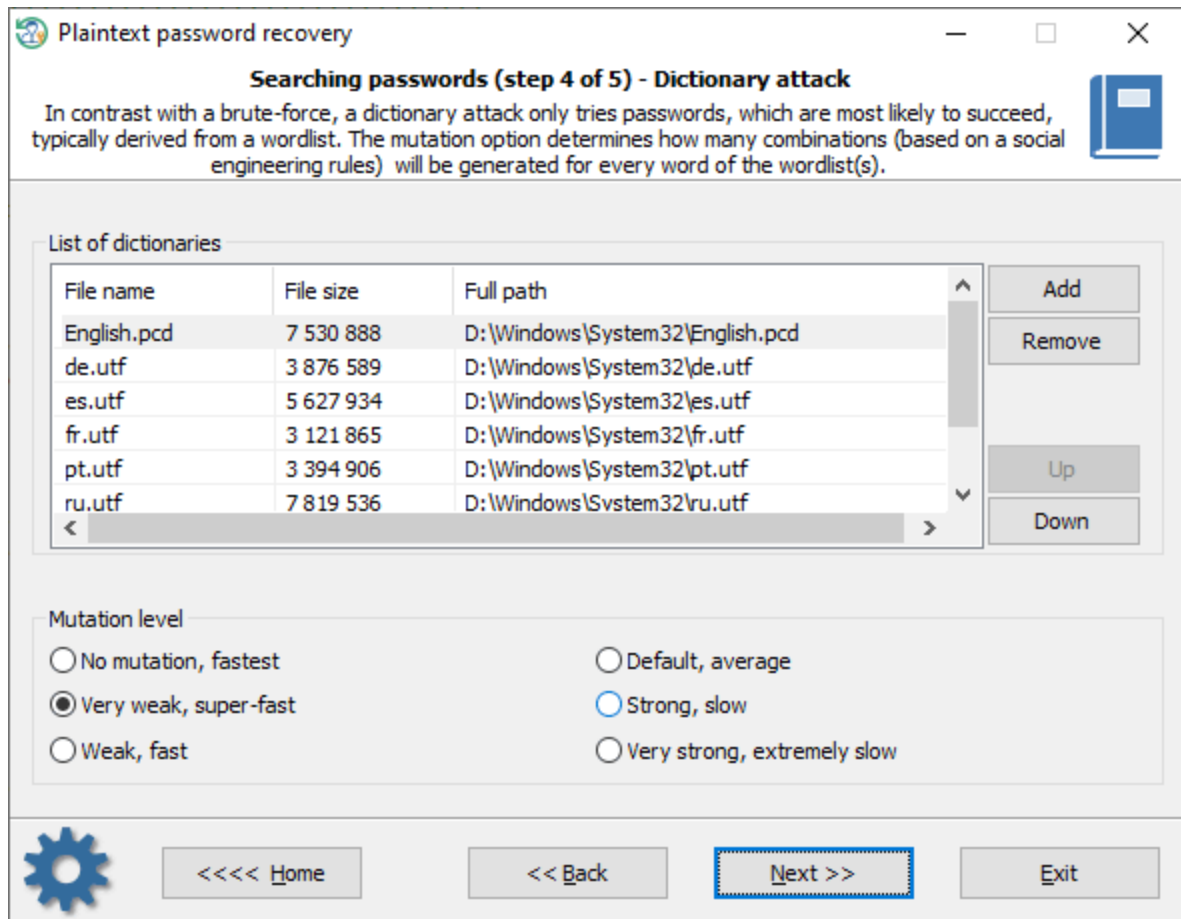
Finding/analyzing passwords can take some time, which depends on attack settings and peculiarities of your system. Completing the search normally takes approximately 10-15 minutes without Passcape table and disk search attacks. The Passcape table attack takes much longer and depends on your CPU and the number of hashes to recover. For example, on a 2-core CPU it takes usually up to 3 minutes for a single hash.

3.10.1 Custom recovery

Once the custom recovery option is set, the program can additionally run 3 different attacks to guess the passwords:

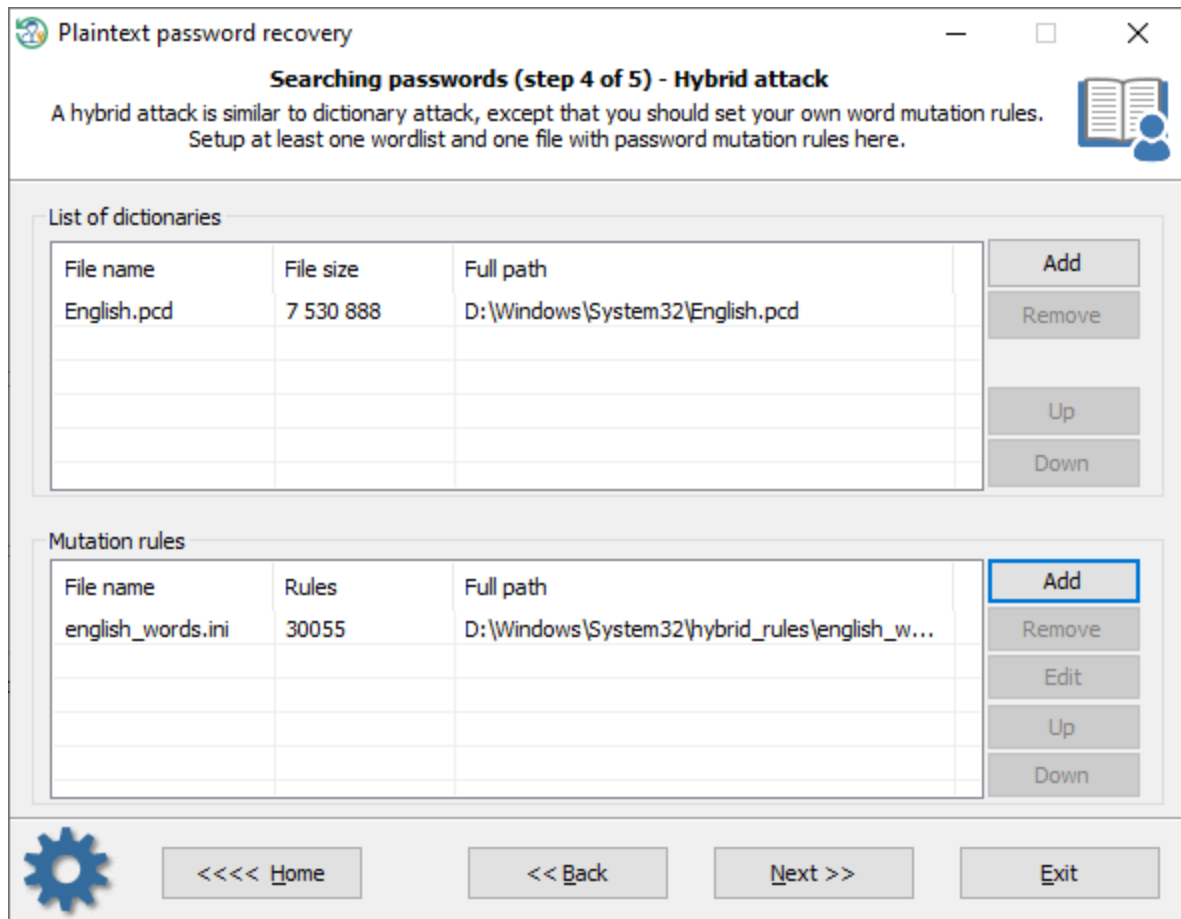
- Dictionary attack
- Hybrid attack
- Mask attack

Dictionary attack



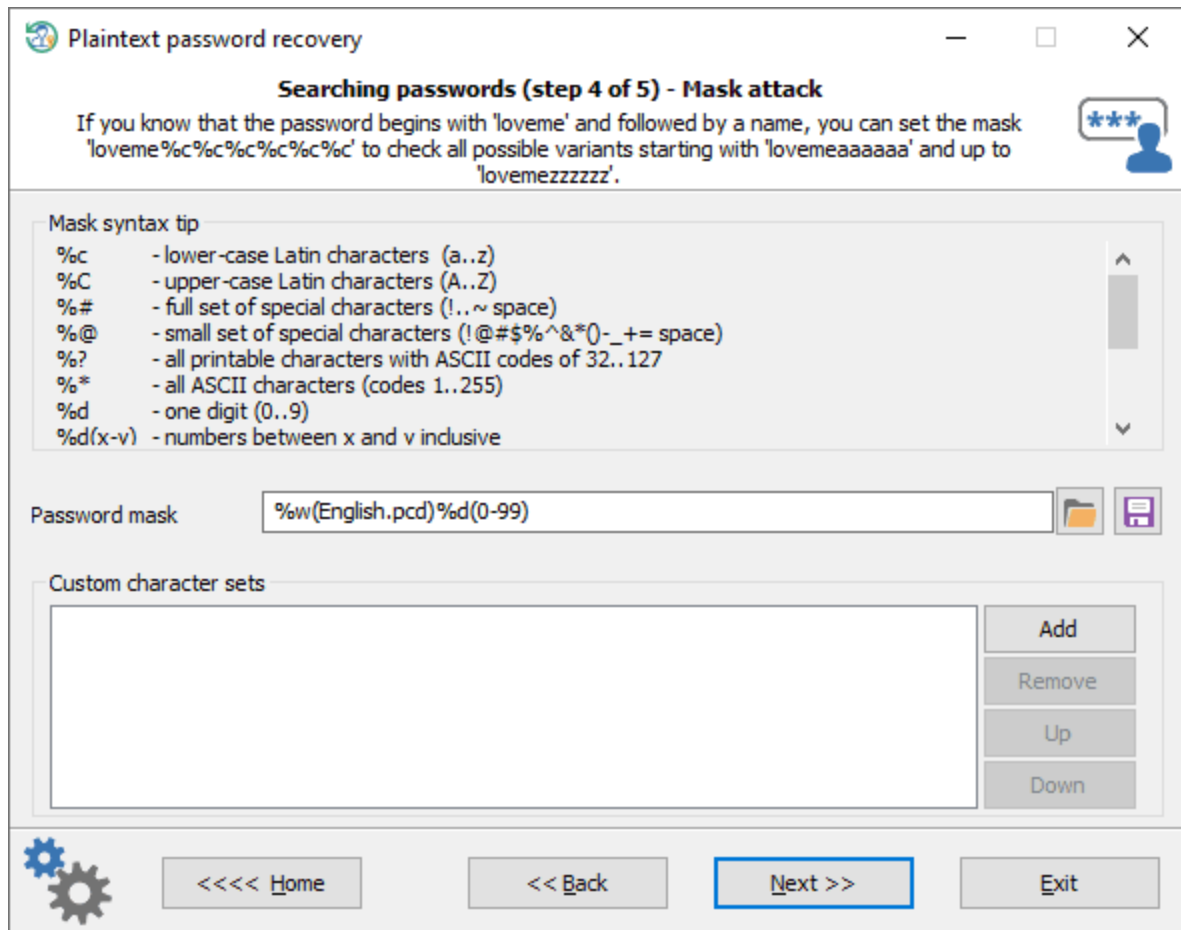
A [dictionary attack](#) tries passwords, which are most likely to succeed, typically derived from a wordlist. RWP supports for different types of dictionaries: ASCII, UNICODE, UTF8, as well as encrypted/compressed dictionaries in the native PCD format. You can use both predefined and custom dictionaries. To add your own wordlist, copy one to a USB drive and attach the drive to the target PC. The mutation level determines how many combinations (based on social engineering rules) will be generated for every word of the wordlist(s).

Hybrid attack



A [hybrid attack](#) is similar to a dictionary one, except that you can set your own word mutation rules. The program comes with a huge set of rule-files. Just use one that is best for your task. The good thing in a Hybrid attack is that you can additionally create, edit and modify password mutation rules according to your needs.

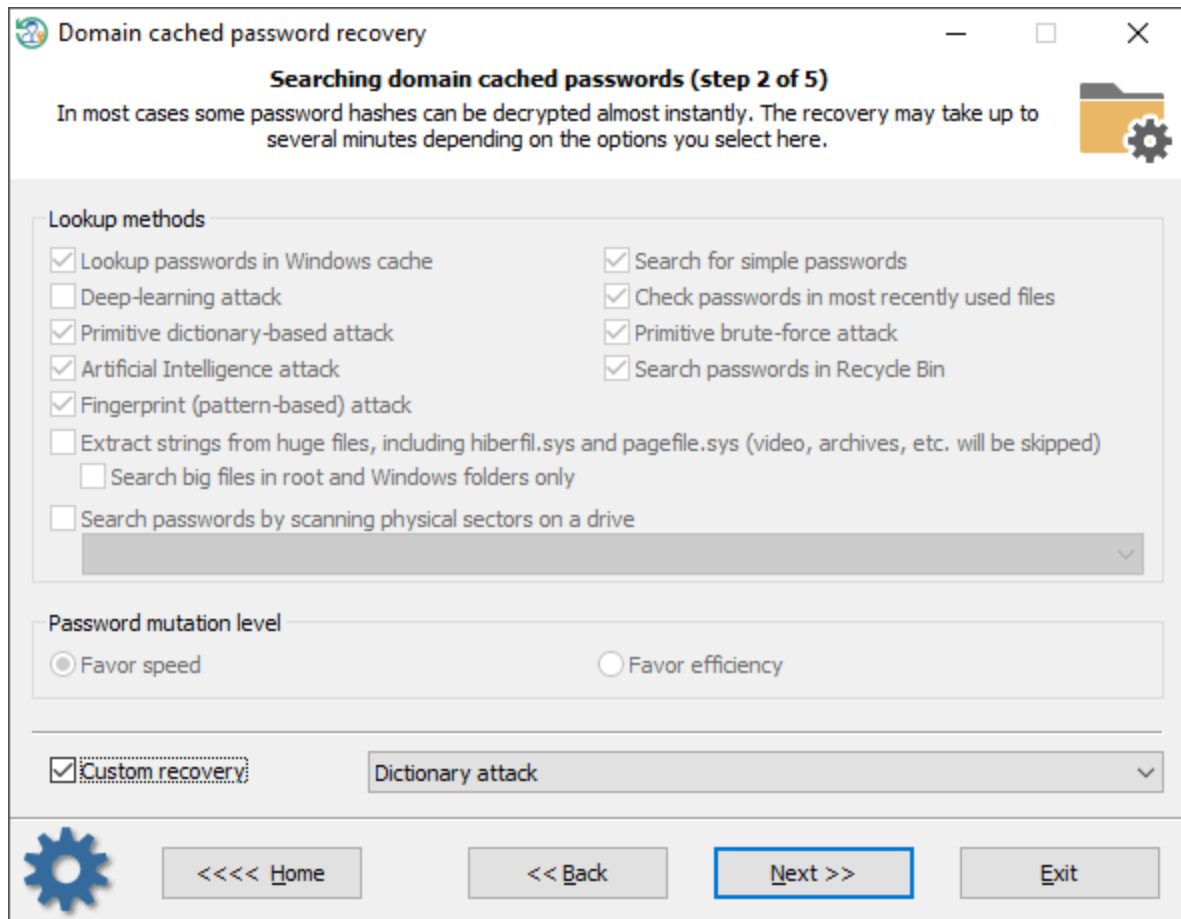
[Mask attack](#)



A [Mask attack](#) is an irreplaceable tool when you know a part of the password or have any specific details about it. For example, if you know that the password consists of 12 characters and starts with 'loveme', obviously it's just enough to guess the last 6 characters of the password. That is what the mask attack is for. In our example, you can set the following mask: loveme%c%c%c%c%c%c%c To get more information about how the mask works, please refer to our [online documentation](#).

3.11 Search for domain cached passwords

[Setting search and recovery options](#)



Domain cached password recovery consists of several modules. Each one can be turned on/off separately:

1. Finding information in Windows system cache. This module consists of over a dozen of mini-attacks, during which the program analyzes all kinds of system passwords: LSA secrets, DSL, FTP, LAN, WAN passwords, Internet and email credentials, etc. Later the found passwords are used by the program to check other passwords by generating more complex variations.
2. Analyzing simple, short and numeric passwords, keyboard combinations, etc. Over 20 mini-modules in total.
3. Scanning, reading and analyzing most recently used files of the target system. The program parses the files and creates a list of words (by generating various mutations) to be checked as passwords.
4. Primitive dictionary attack. The application checks all passwords from the built-in dictionary for the Light and Standard editions or from several dictionaries (Arabic, Chinese, English, French, German, Portuguese, Russian, Spanish) for the Advanced Edition. If the deep search option is on, simple word mutations will also be taken into account during the search.
5. Primitive brute-force module that consists of several simple attacks to search for short passwords.
6. Artificial Intelligence module analyzes network activity of users on the target computer. Over thirty mini-modules take care of that. Upon the results of the analysis, the application generates user preferences and creates a semantic dictionary for the attack. Then the dictionary is used for guessing passwords.
7. Looking for passwords in deleted files.
8. Primitive Fingerprint attack on English passwords. This module may take a lot of time to complete.
9. Extract strings from huge files: RAM images, hiberfil.sys, pagefile.sys and so on. The program can skip files useless in password analysis like video, archives, audio files, etc.

10. Searching for passwords by reading and analyzing raw sectors of the selected drive. If the Password mutation level is set to '*Favor efficiency*', the program additionally tries to mutate all found passwords as well, thus walking through all sectors of the target drive may take quite a time. This module is not effective for drives which have a full-disk encryption set on. Like Bitlocker or TrueCrypt, for example.

To apply a [custom recovery method](#), turn on the 'Custom recovery' option and select one of the available attacks. On the next step you will be prompted to set up various options related to the selected attack.

Selecting data source

Domain cached password recovery

Searching domain cached passwords (step 3 of 4)

You should provide files and folders required for successful recovery. Typical location for profiles directory: C:\Users. Typical location for program files folder: C:\Program Files.

Files and folders required for successful recovery

Path to Active Directory database

SAM registry file

SYSTEM registry file: C:\Windows\System32\Config\SYSTEM

SECURITY registry file: C:\Windows\System32\Config\SECURITY

SOFTWARE registry file: C:\Windows\System32\Config\SOFTWARE

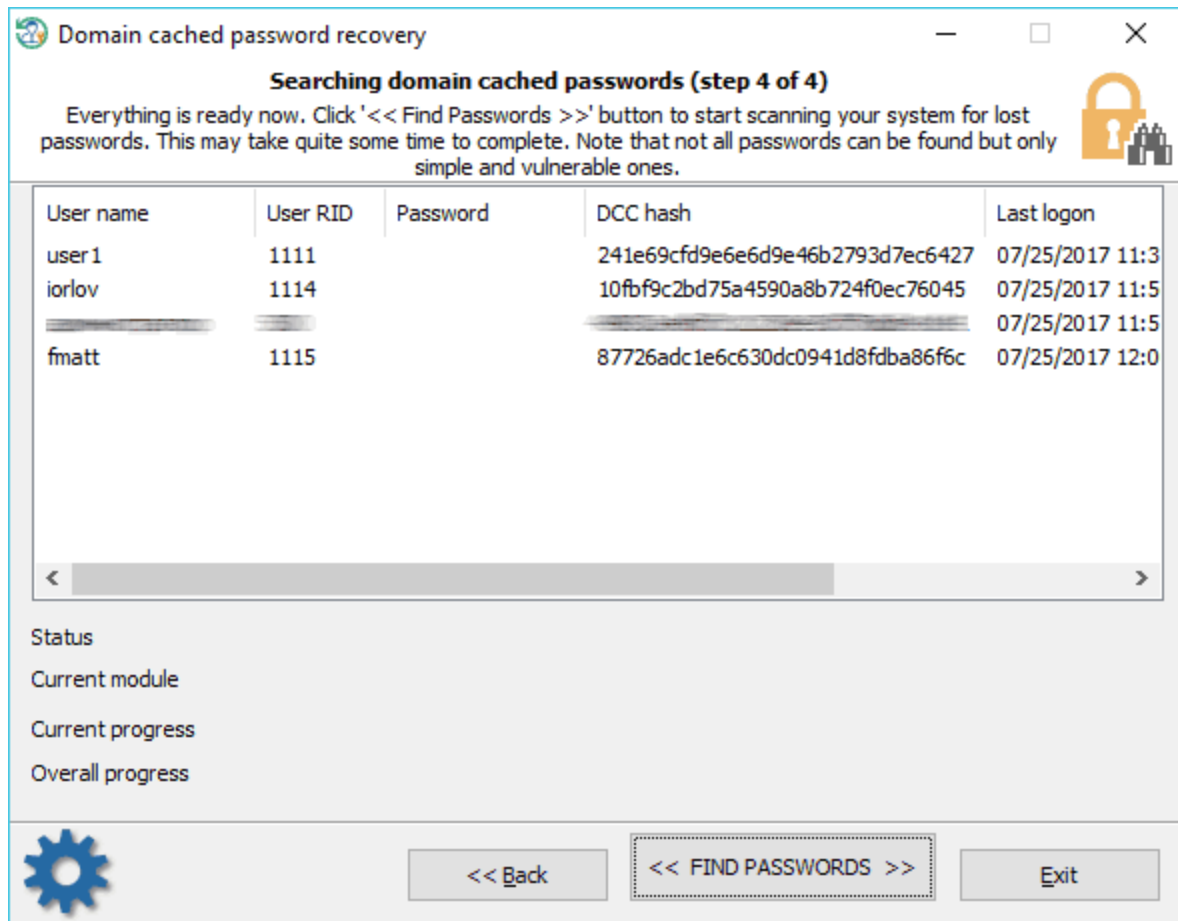
Profiles directory: C:\Users

Program files directory: C:\Program Files

<< Back Next >> Exit

When searching for domain cached passwords, special attention is to be paid to proper setting files and folders required for the process. RWP finds the files automatically, but sometimes, e.g., when the computer has several operating systems installed, you may need to adjust it manually. Also keep in mind that if the target PC has 2 or more hard disk drives, the sequence of the letters for these disks can be set totally different than in the original system.

Searching for domain cached passwords



Domain cached credentials are of two types. DCC type 1 has very weak encryption and was used in Windows 2000, Windows XP and Windows 2003 OSes. Recovery rate can exceed millions or even billions passwords per second. DCC type 2 is used in Windows Vista and later operating systems. Its encryption is much much stronger and quite resistant to cracking. The brute-force speed is only hundreds/thousands passwords per second. Just imagine, guessing an 8 character long password consisting of upper and lower case letters using brute-force attack might take over 1000 years!

Do take into account the following considerations:

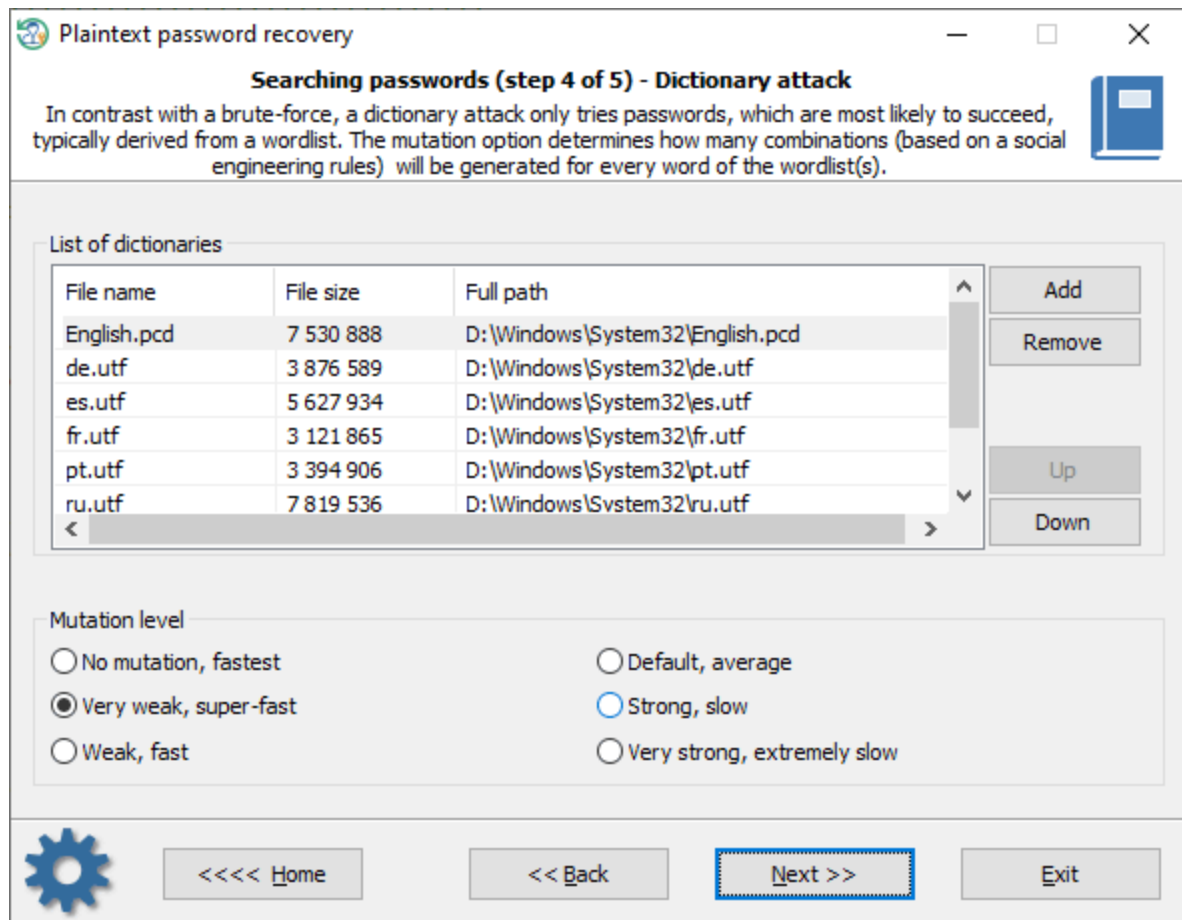
- Process of searching for DCC type 2 is extremely slow. Completing some modules (for example, Fingerprint attack) may take hours or even days.
- To speed up the search, select only account you need the password for. Just right-click the cached entry and select '*Exclude from search all entries except selected*'. Otherwise, the speed of the password recovery will decrease by a multiple of the number of accounts.

3.11.1 Custom recovery

Once the custom recovery option is set, the program can additionally run 3 different attacks to guess the passwords:

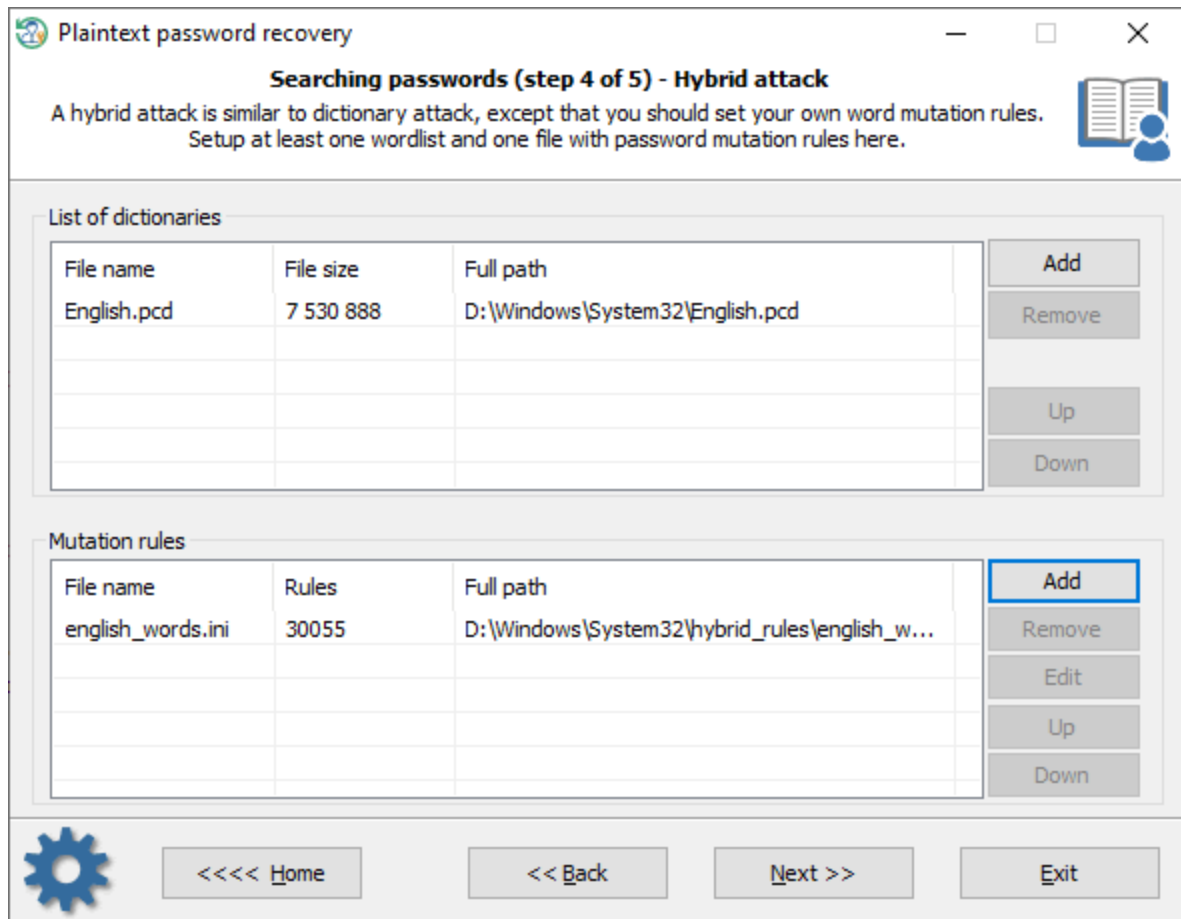
- Dictionary attack
- Hybrid attack
- Mask attack

Dictionary attack



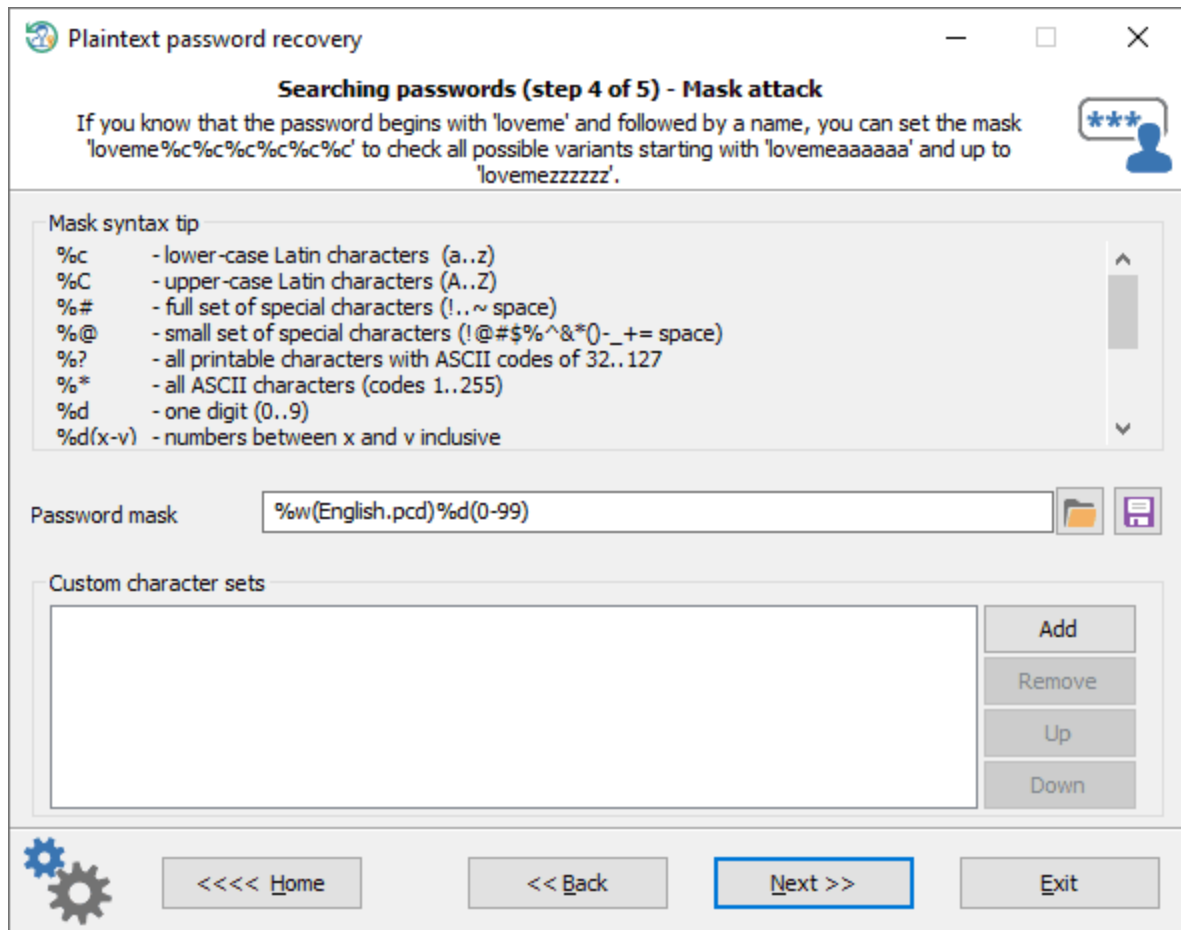
A [dictionary attack](#) tries passwords, which are most likely to succeed, typically derived from a wordlist. RWP supports for different types of dictionaries: ASCII, UNICODE, UTF8, as well as encrypted/compressed dictionaries in the native PCD format. You can use both predefined and custom dictionaries. To add your own wordlist, copy one to a USB drive and attach the drive to the target PC. The mutation level determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

Hybrid attack



A [hybrid attack](#) is similar to a dictionary one, except that you can set your own word mutation rules. The program comes with a huge set of rule-files. Just use one that is best for your task. The good thing in a Hybrid attack is that you can additionally create, edit and modify password mutation rules according to your needs.

[Mask attack](#)



A [Mask attack](#) is an irreplaceable tool when you know a part of the password or have any specific details about it. For example, if you know that the password consists of 12 characters and starts with 'loveme', obviously it's just enough to guess the last 6 characters of the password. That is what the mask attack is for. In our example, you can set the following mask: `loveme%c%c%c%c%c%c%c`. To get more information about how the mask works, please refer to our [online documentation](#).

3.12 Extract BitLocker recovery passwords

Often, BitLocker recovery passwords are backed-up in an Active Directory database. This function of the program is designed to extract BitLocker passwords even out of a non-bootable or a non-working domain.

[Selecting Active Directory database](#)

Extract BitLocker recovery passwords (step 2 of 3)

Select a path to ntds.dit file and SYSTEM registry here. Usually ntds.dit file locates in %WINDIR%\ntds\ folder, while the SYSTEM registry file always resides in your %WINDIR%\system32\config directory.

Active Directory source files

Path to Active Directory database (usually ntds.dit) file
F:\Windows\NTDS\ntds.dit

SYSTEM registry file
F:\Windows\System32\config\SYSTEM

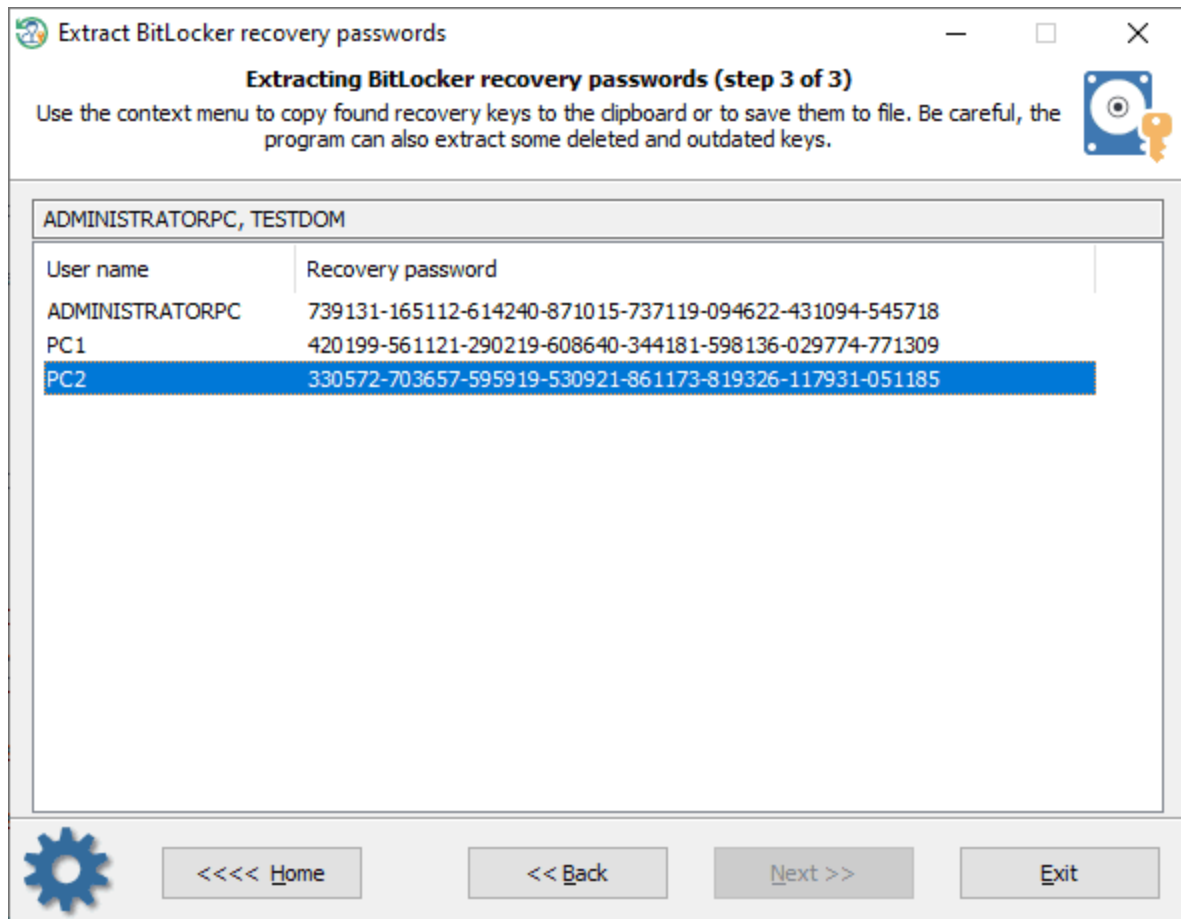
OS info

Windows version	Windows Server 2012 Standard 6.2 9200.win8_rtm.120725-1247
Registered owner and org	Windows User
Install date	2018-02-15
Last logon user	John

Navigation buttons: <<<< Home, << Back, Next >>, Exit

In the beginning, you have to set up paths for the **SYSTEM** registry and for the **NTDS.DIT** database. The program should locate the paths automatically but you can select them on your own.

Extracting BitLocker recovery passwords

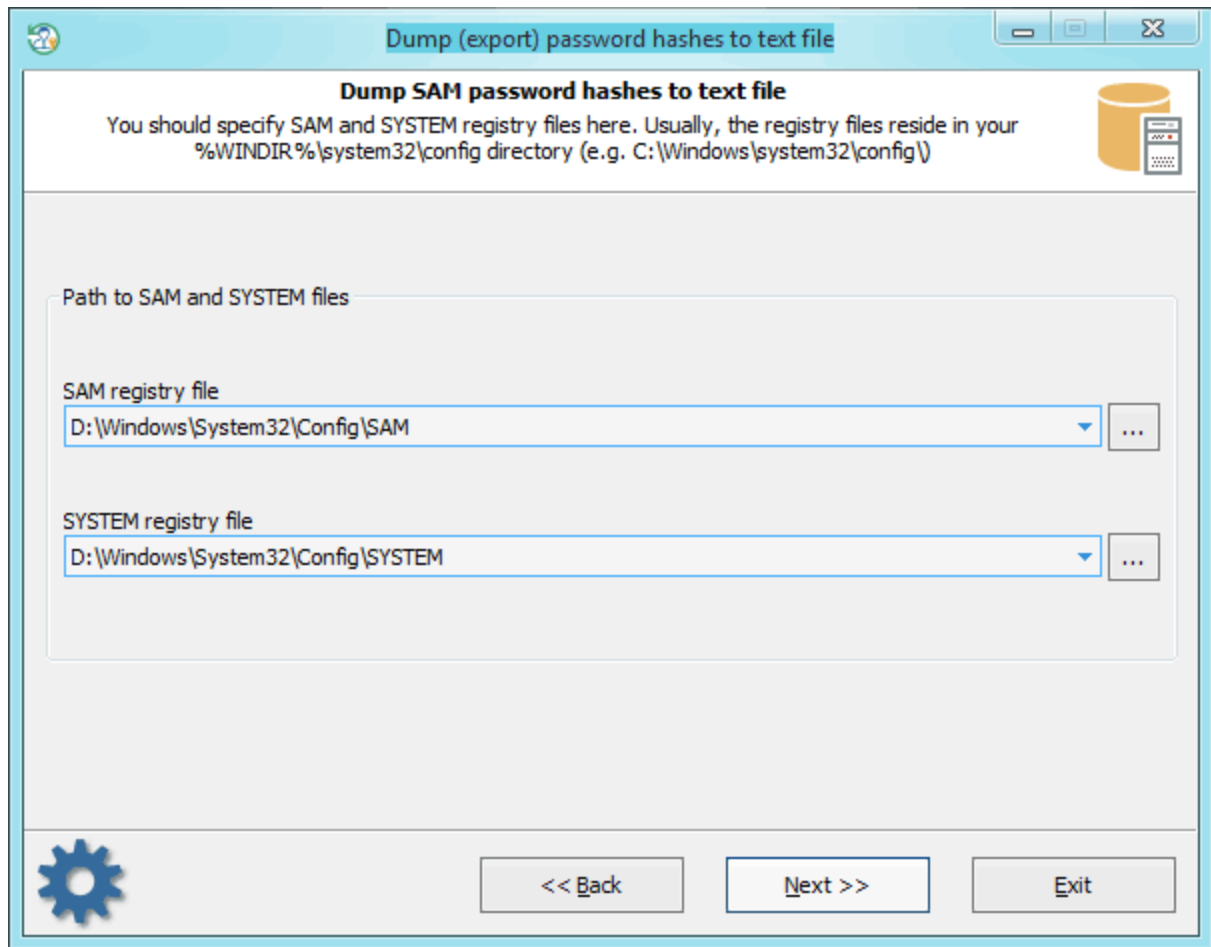


Be careful, the program can additionally retrieve expired and deleted BitLocker keys, and often there's no way to get the real names of the key owners.

You can copy the required key to the clipboard or save it to a file.

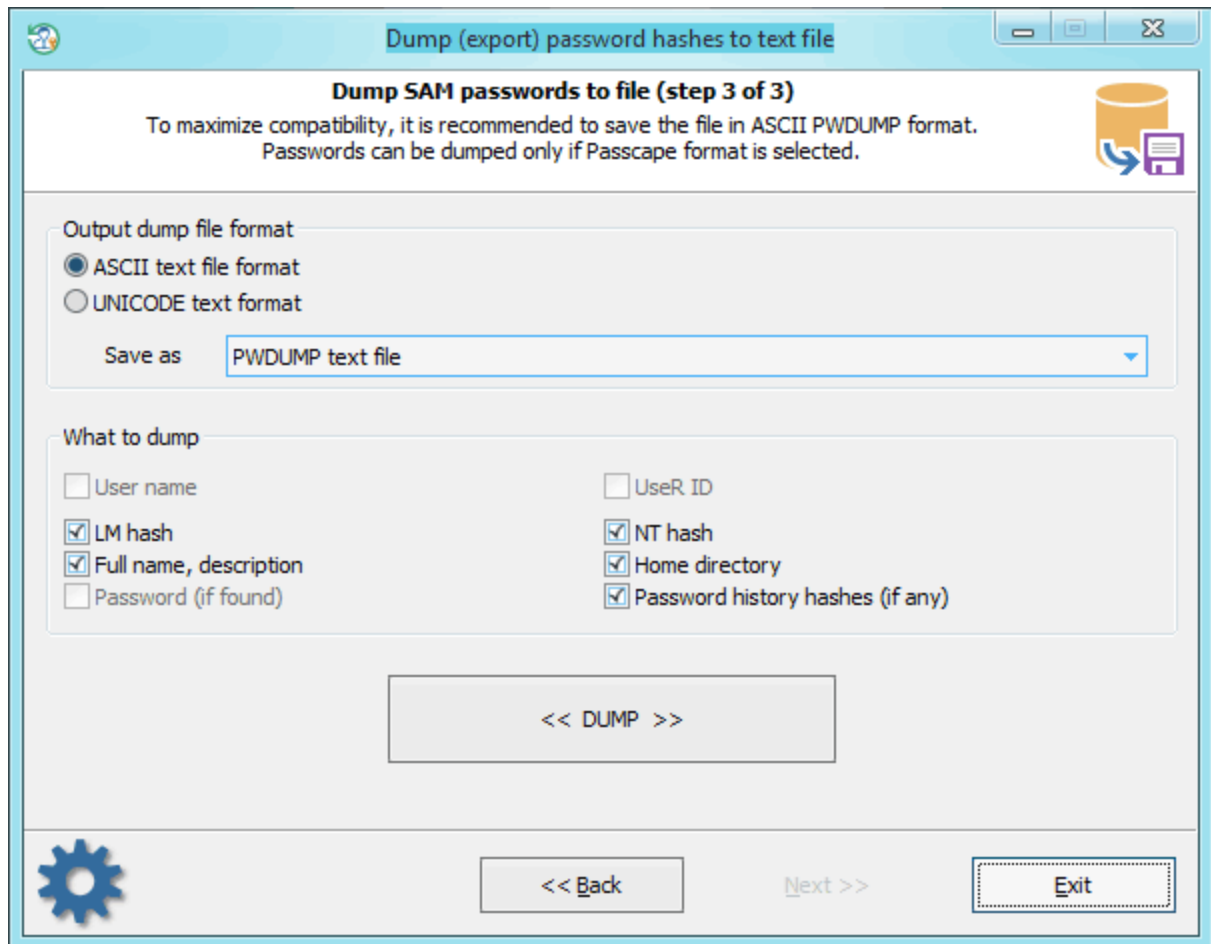
3.13 Dump password hashes

Selecting data source



On this step, specify the location of SAM and SYSTEM files. Or, in the case with domain users, – ntds.dit and SYSTEM.

Export password hashes



Select the format and type of the dump file. While generating the dump, you can also delete, if that's no value to you, individual unnecessary attributes of the account. If the Passcape format is selected, you can also dump plaintext passwords (if ones were found). The application scans your computer for the availability of such and, if such are available, maps them to the accounts while saving to the dump file.

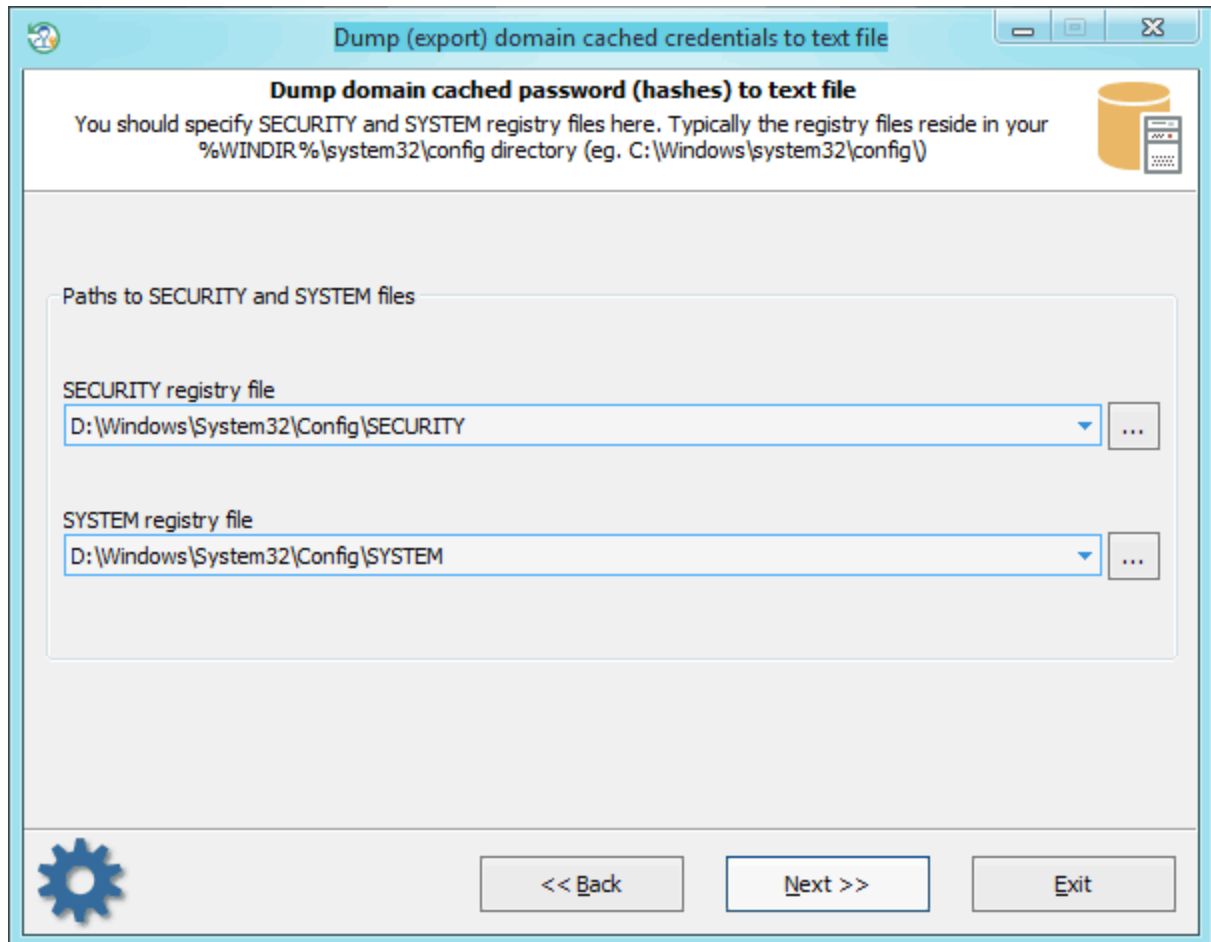
Plaintext passwords are stored in domain when the option '*Store passwords using reversible encryption for all users in the domain*' is set; you can find it in the groups policy console.

Further on, you can use the dump file with different password audit and recovery applications.

Please note also that Reset Windows Password, thanks to the AI attack technology developed by Passcape Software, can decrypt passwords to certain accounts literally instantly, without searching. For details, please refer to the [Lookup user passwords](#) section.

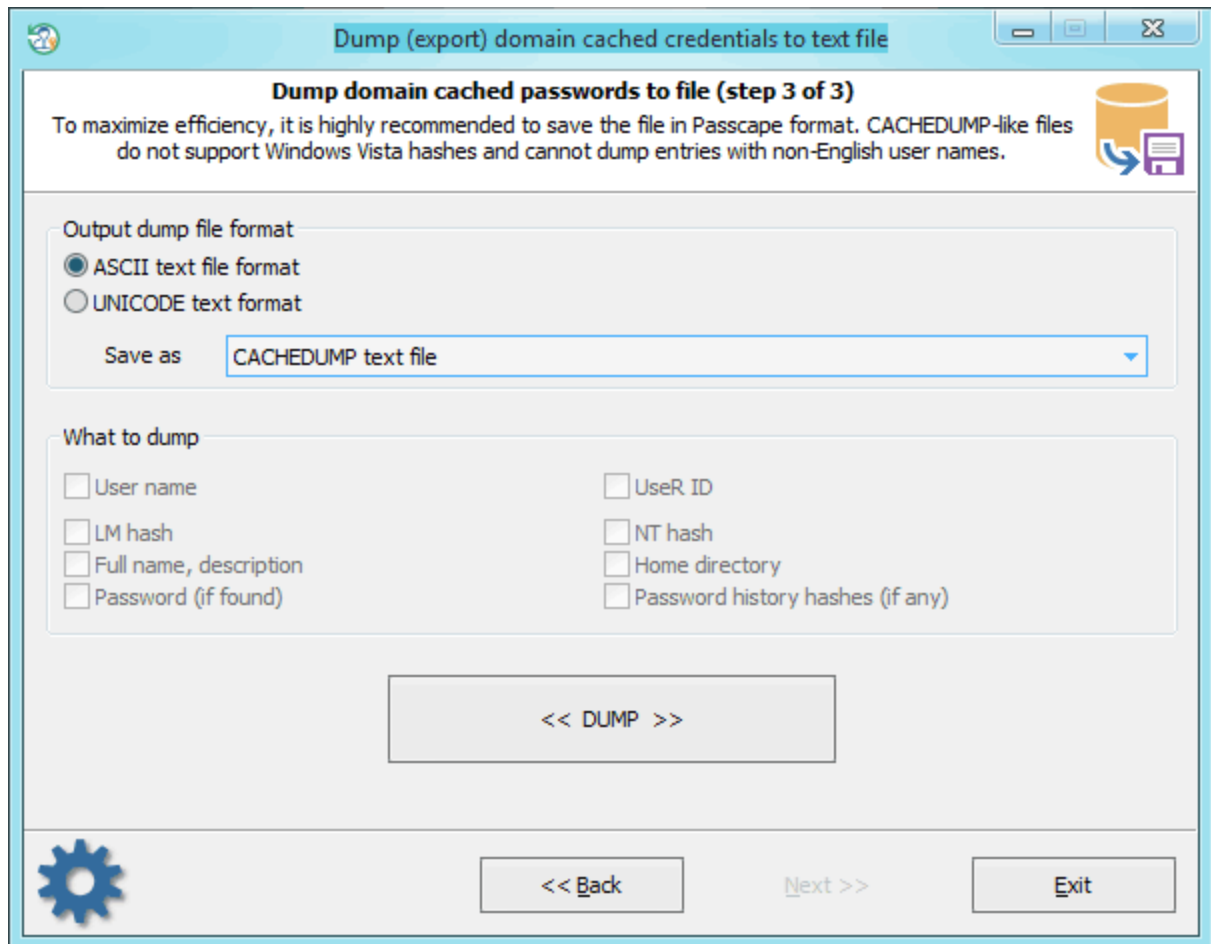
3.14 Dump domain cached passwords

Selecting data source



For decrypting [domain cached credentials](#), the program needs to 'know' the location of two system registry files: SECURITY and SYSTEM. Select them from the list or, if the application was unable to locate them, provide the path to them manually.

Dumping domain cached credentials

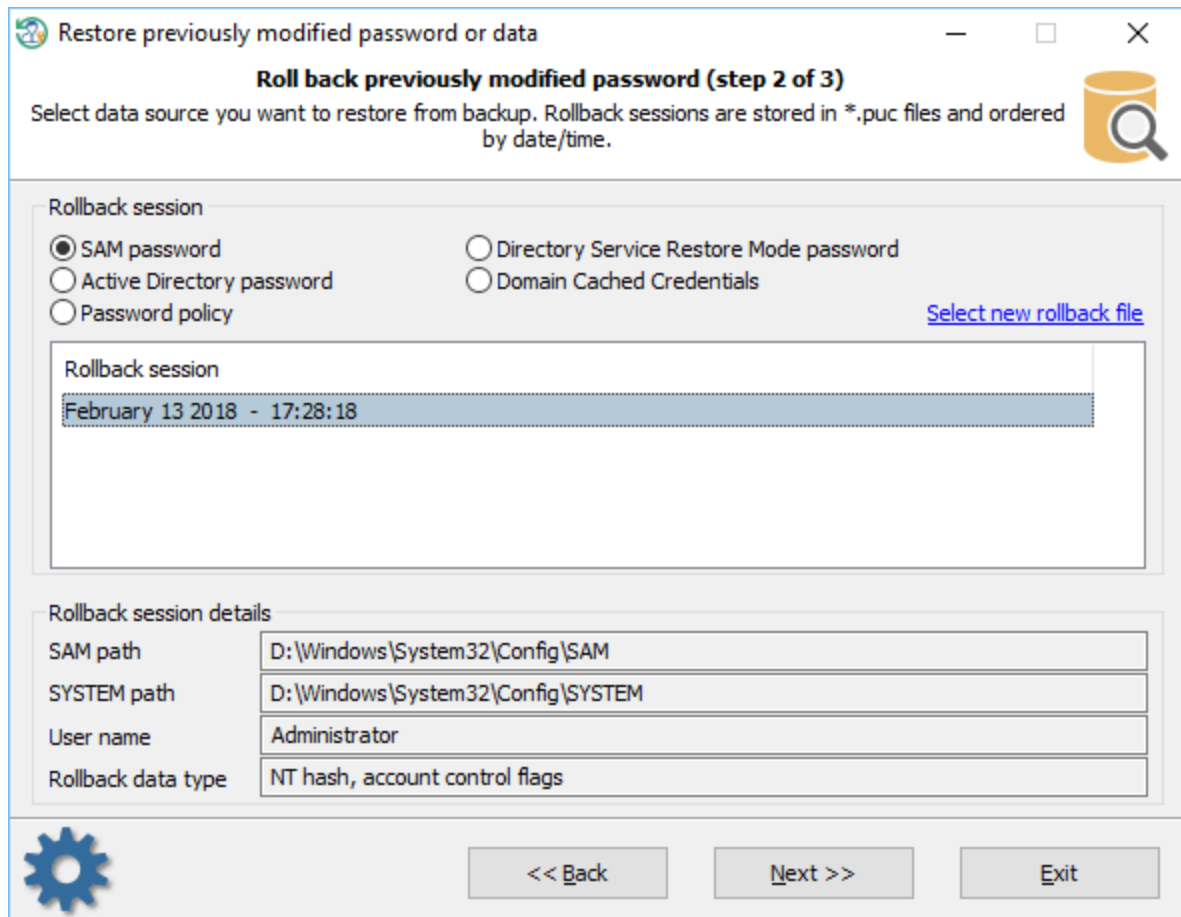


The final dialog provides just two options:

- **Dump file format.** ASCII is good for all cases, but problems may occur with non-English user names and, respectively, with further analysis and decryption of those hashes. UNICODE supports all languages, but compatibility problems may occur when reading this format in different applications.
 - **Dump file type** can be either CACHEDUMP – a simple but widespread format. No compatibility problems will occur. However, this format imposes a number of restrictions. First, it does not support non-English user names. Respectively, further on, you will be unable to decrypt the account password, as it is bound to the name. Second, the current version of the CACHEDUMP format does not support operating systems Windows Vista and higher.
- Passcape format – free from these disadvantages and can be successfully used in password audit and recovery applications like, for example, [Network Password Recovery](#).

3.15 Restoring previous modified password

Choosing a roll-back file



Restore previously modified password or data

Roll back previously modified password (step 2 of 3)

Select data source you want to restore from backup. Rollback sessions are stored in *.puc files and ordered by date/time.

Rollback session

☒ SAM password ☐ Directory Service Restore Mode password
☐ Active Directory password ☐ Domain Cached Credentials
☐ Password policy [Select new rollback file](#)

Rollback session

February 13 2018 - 17:28:18

Rollback session details

SAM path D:\Windows\System32\Config\SAM

SYSTEM path D:\Windows\System32\Config\SYSTEM

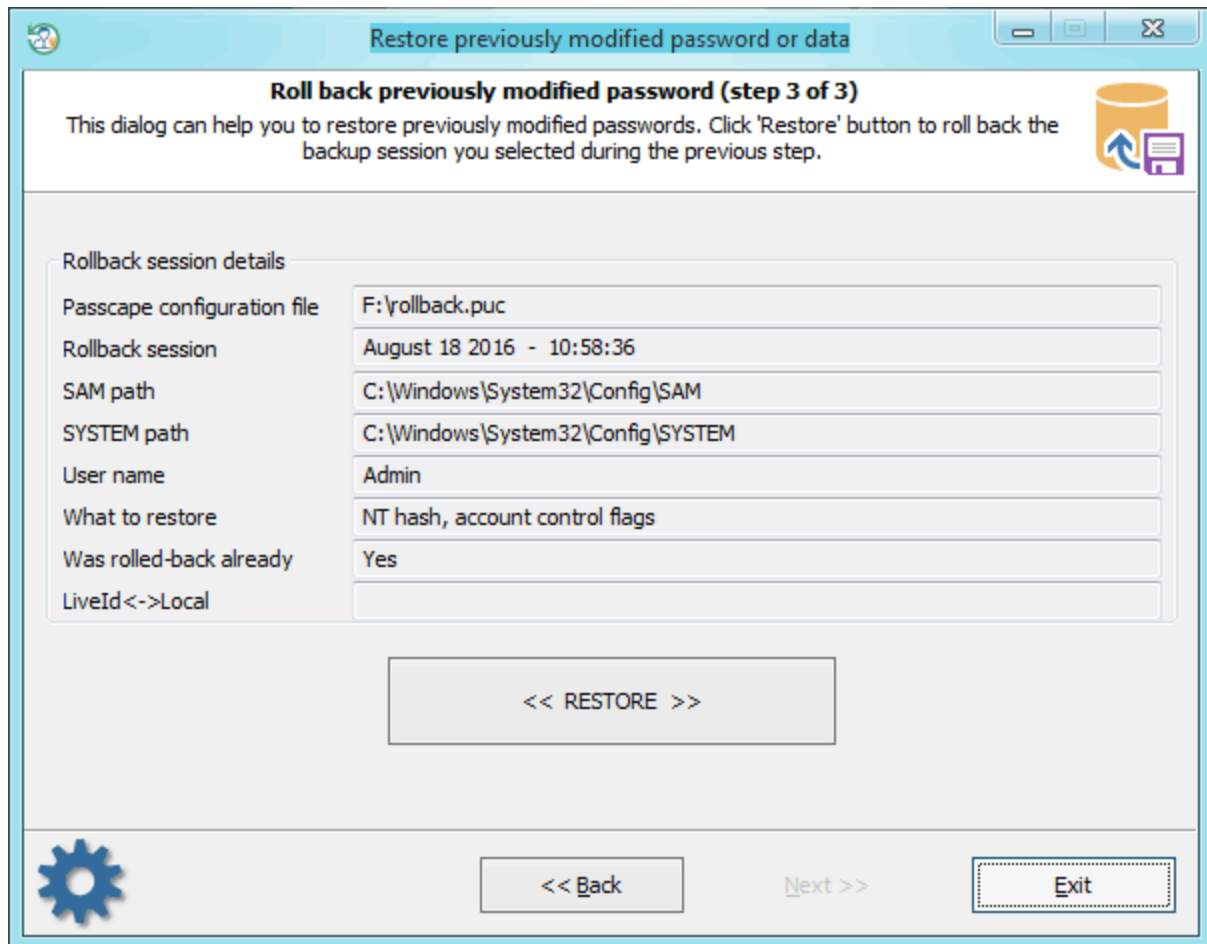
User name Administrator

Rollback data type NT hash, account control flags

<< Back Next >> Exit

If for whatsoever reason you need to undo (i.e. restore) the password that was reset or modified earlier, on the second step of the Wizard, provide the application with the *.puc file with the roll-back (undo) sessions. Activate the type of the password to be restored: regular SAM account password, Active Directory, DSRM password or domain cached credentials, password policy flags. After that, select the date when the change was made.

Restoring previously modified password



On the last step, the application will offer you to review the details of the undo session; please pay close attention to the last three items:

- Account to be managed.
- Data to be restored. That's the data you have modified at some point.
- Whether or not this undo session has been used already

Let's review this situation for an example:

A computer security expert needs to logon to Windows under a certain account. The password for that account is unknown. At the same time, the account password must remain unmodified.

Here is the routine:

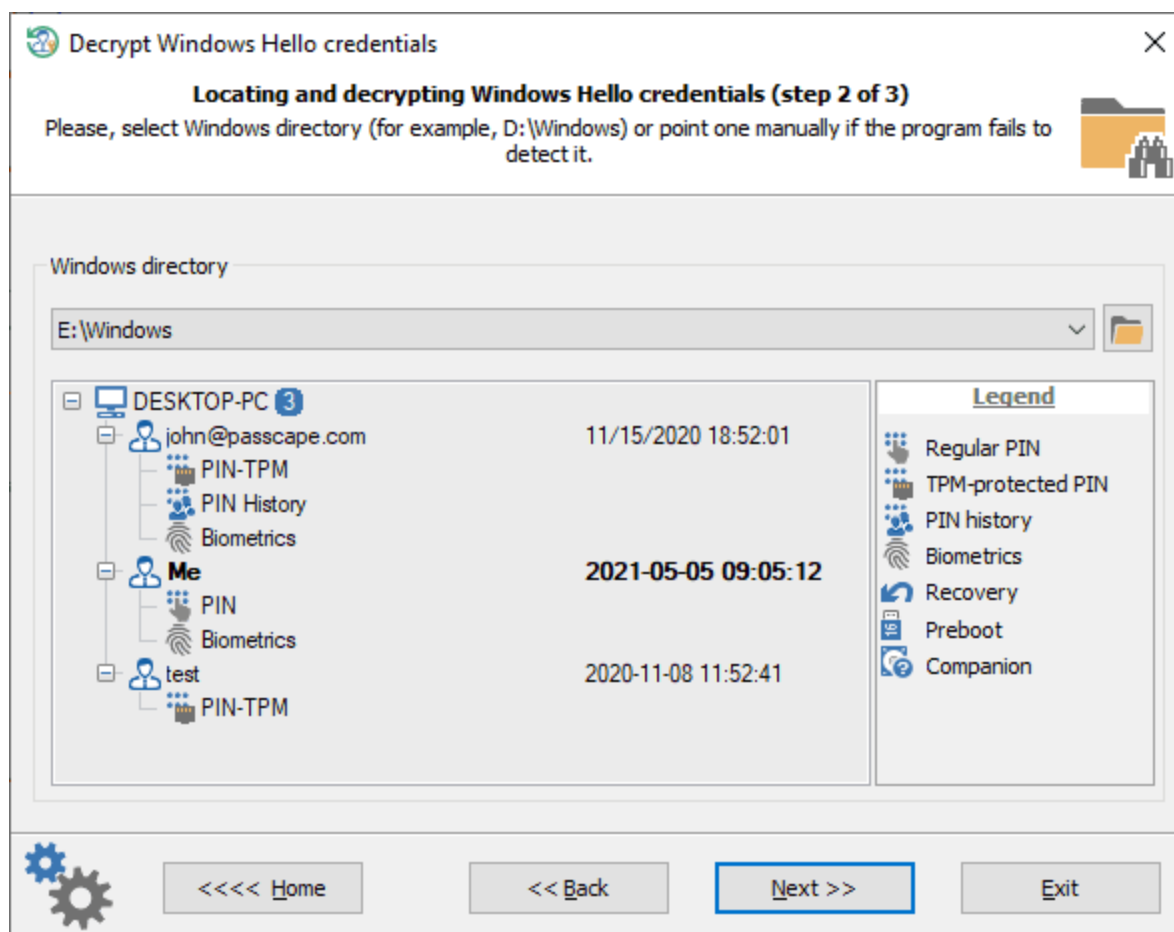
- Run Reset Windows Password, select the corresponding account and reset its password. At the same time, save the undo session to a *.puc file (the application will prompt you to do that when you modify the password).
- Close Reset Windows Password and start Windows. Logon under the modified account with the blank password. Do what you need under that account.
- Now you need to restore the old account password. For that purpose, reboot once again and launch Reset Windows Password. On the main menu, select 'Restore previously modified password or data', enter path to the undo file where you have saved the changes you had made. Move on to the third step and make sure that this is the account you need. Click on the <<Restore>> button, and the old password will be restored.

3.16 PASSWORD RECOVERY TOOLS

3.16.1 Decrypt Windows Hello credentials

Windows Hello is a biometric security system that allows Windows users to log into OS, applications and their devices without passwords but using a fingerprint, iris scan, facial or voice recognition. Windows Hello stores different types of users personal information: digital identities, PINs, plaintext logon passwords, etc.

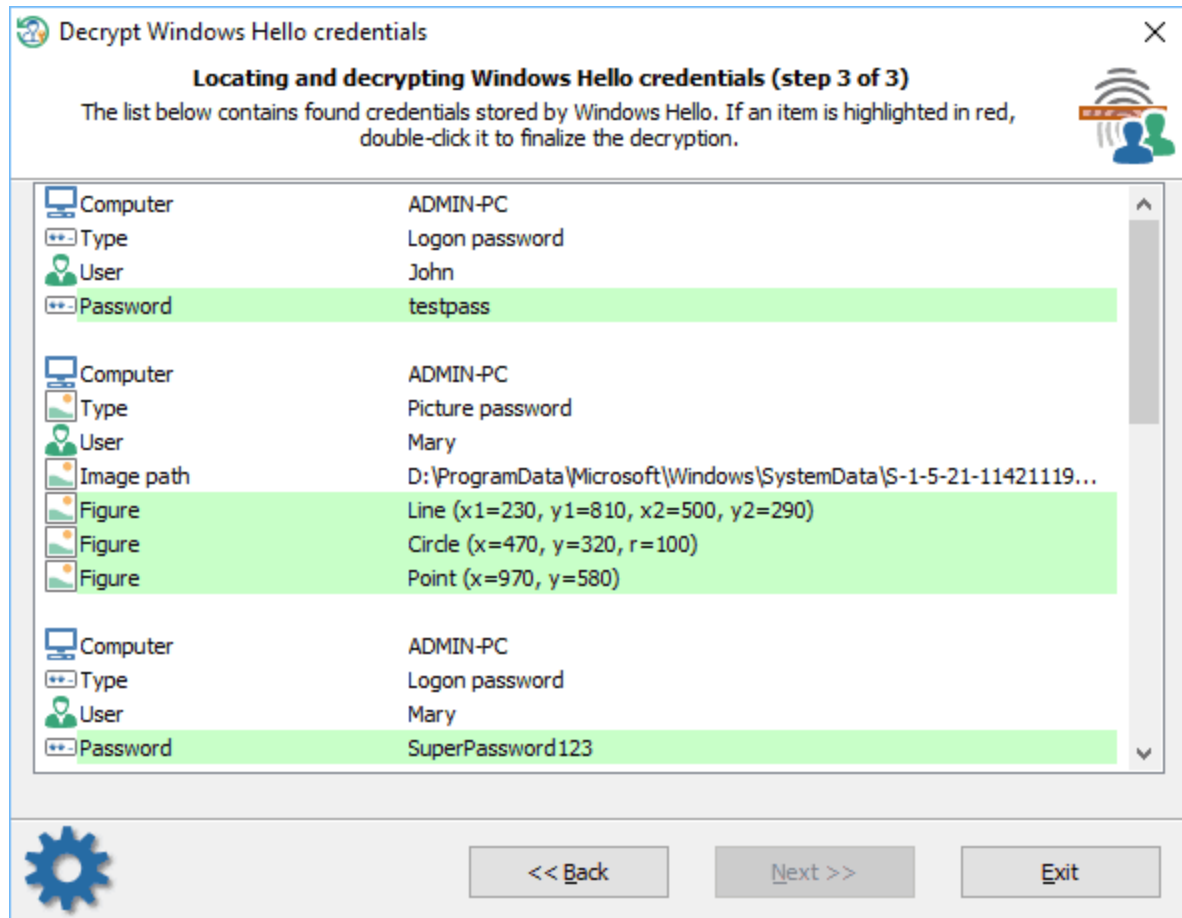
Selecting Windows directory



Reset Windows Password recovers all kinds of personal data saved in Windows Hello except some protected with TPM. First of all, you will need to specify Windows directory of the target Windows 10 system. After the Windows directory is selected, the program analyzes the installed OS and displays a list of all available Windows Hello accounts, as well as the authentication methods they use. The last user logged in using Windows Hello is highlighted in bold. Here are the common Windows Hello authentication types:

- PIN - regular PIN authentication is available
- PIN-TPM - a TPM protection is set for PIN authentication
- PIN History - PIN history is present and can be decrypted
- Biometrics - a fingerprint authentication is used by the user

Decrypting passwords



The program should then scan the target Windows directory for any personal data and output found information to the screen. Reset Windows Password automatically decrypts logon passwords if the user accounts was set up to logon using biometrics, for example, fingerprint or face recognition.

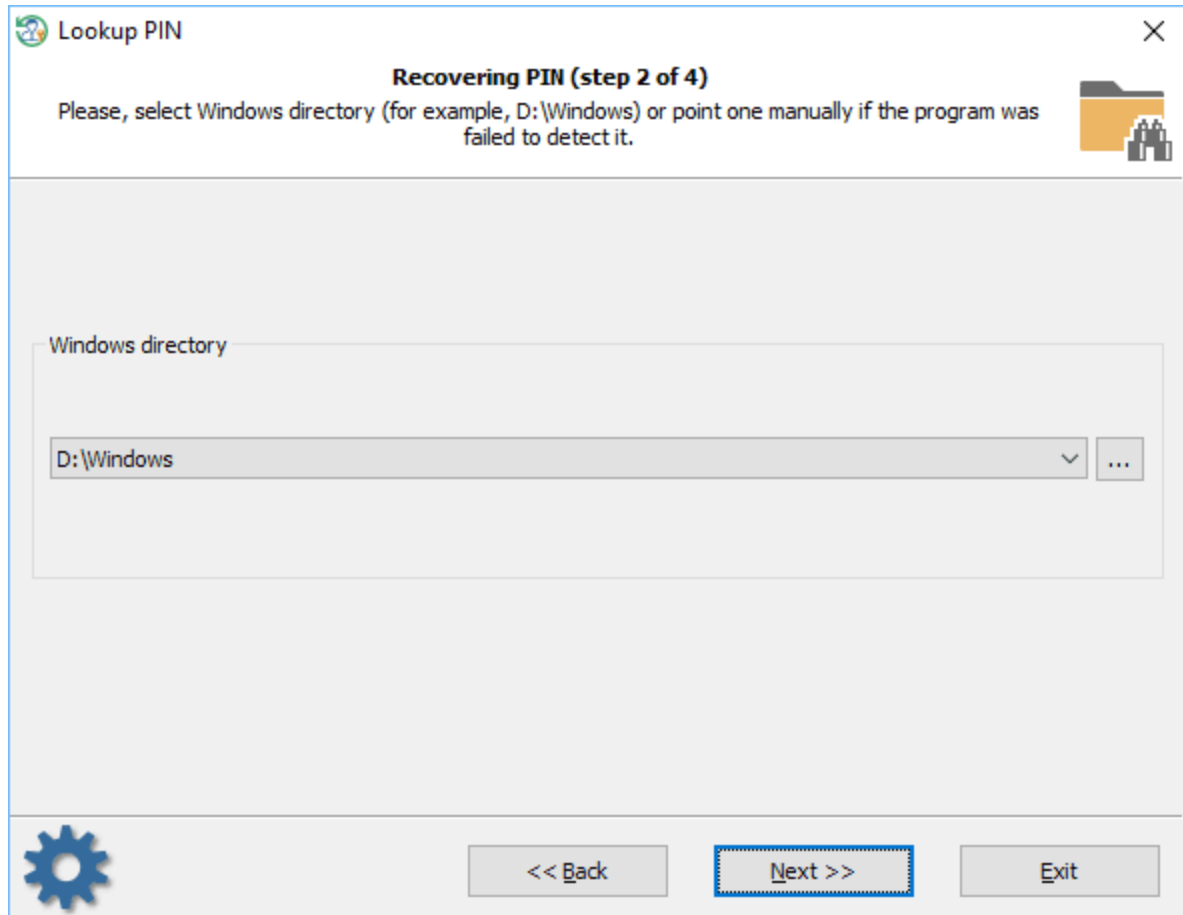
Some items in the table may be marked in red. It means that to finalize the decryption the program needs to know the PIN code of the user account. Double-click the item and type in the PIN that corresponds to the user account.

3.16.2 Lookup PIN

When you set up Windows Hello first, you're asked to create a PIN. The PIN is used as an alternative to biometric logon, when the biometric sensor is unavailable or not working properly. Unlike Windows 8,

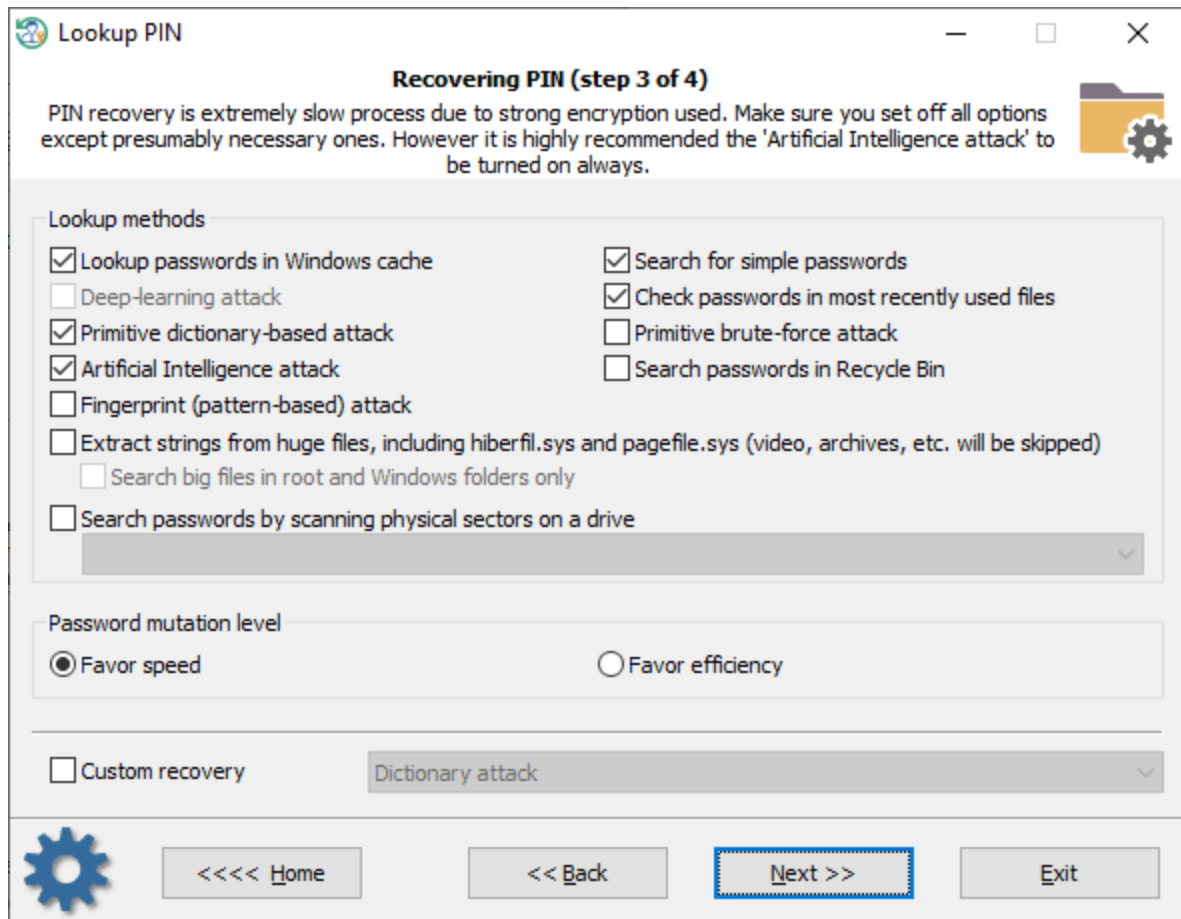
Windows 10 ensures very strong encryption (using even undocumented features and APIs) to protect PINs. Therefore, the problem of forgotten PIN's recovery is extremely vital and faces every user.

Selecting Windows directory



First of all, you should select the Windows directory or browse for it manually.

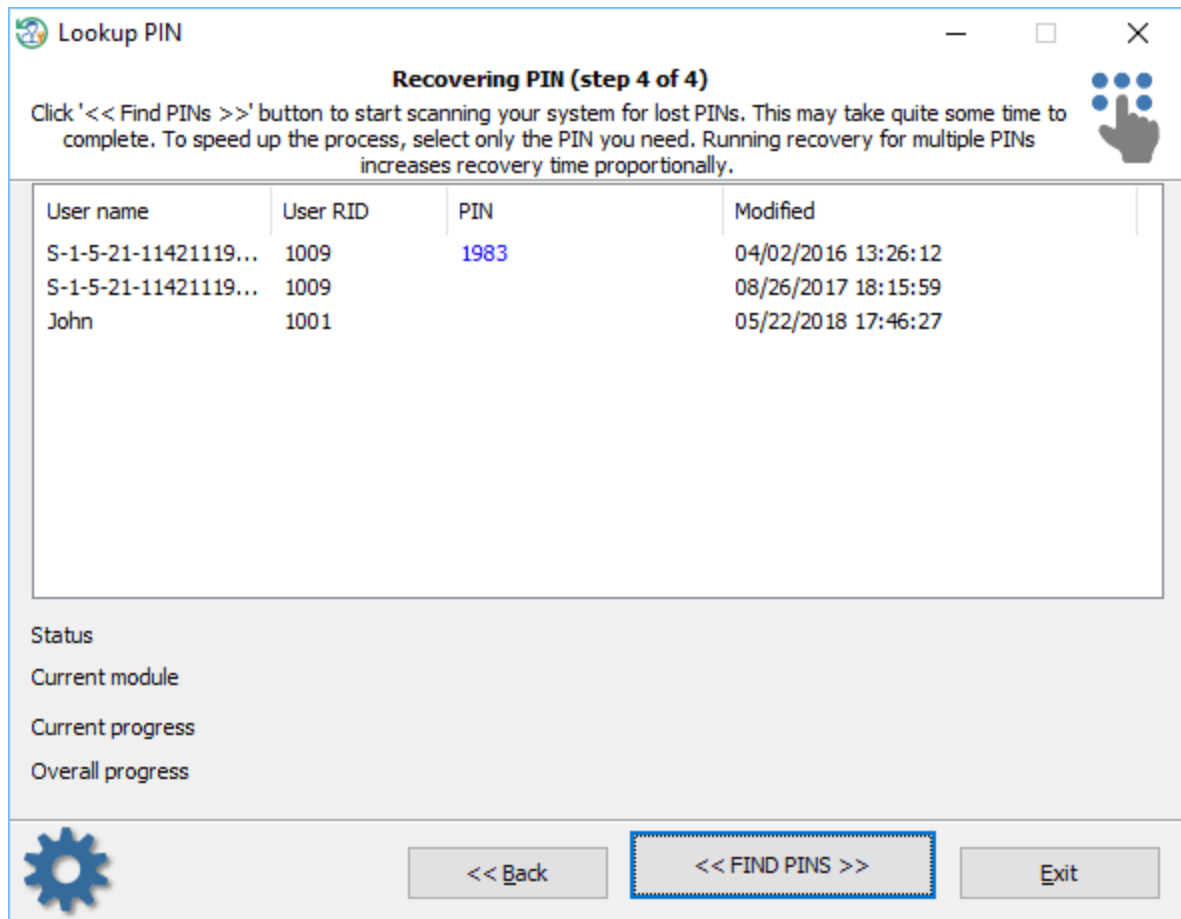
Setting up search and recovery options



On the next step, the program offers available recovery methods used to search for PINs. The program's code is highly optimized for speed. But in spite of this, the process of searching for a PIN is extremely slow. For this reason, it is highly recommended to turn off most time-expensive attacks, for example, like on the picture above.

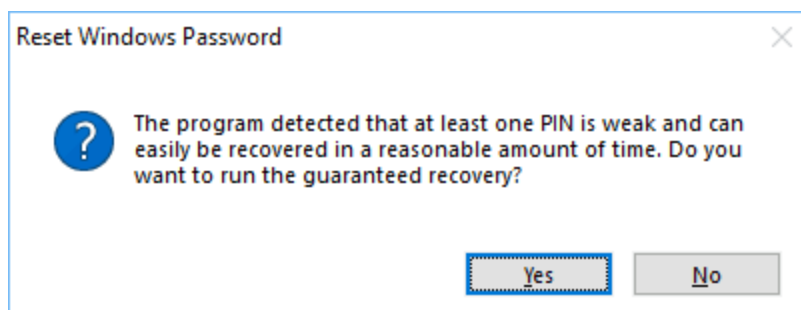
To apply a [custom recovery method](#), turn on the 'Custom recovery' option and select one of the available attacks. On the next step you will be prompted to set up various options related to the selected attack.

Searching for PIN



The search speed is inversely proportional to the number of pins sought. That is, the more PIN codes are searched simultaneously, the lower the search speed. Therefore, it is recommended to exclude all unnecessary PINs from the search, and leave only necessary one. You can do it simply right-clicking on the PIN you need to recover and selecting 'Exclude all except selected'. To start the process, hit the << FIND PINS >> button.

Do know that some PINs can be guaranteed to be decrypted in a reasonable amount of time. If the program can detect such a vulnerable PIN, it offers to launch the guaranteed recovery, just like on the screenshot below.



The latest version of the program implements so-called *Intelligent PIN recovery*. Every time a user tries to decrypt a Windows PIN, the program analyzes found PINs and, if some weak ones are found, offers

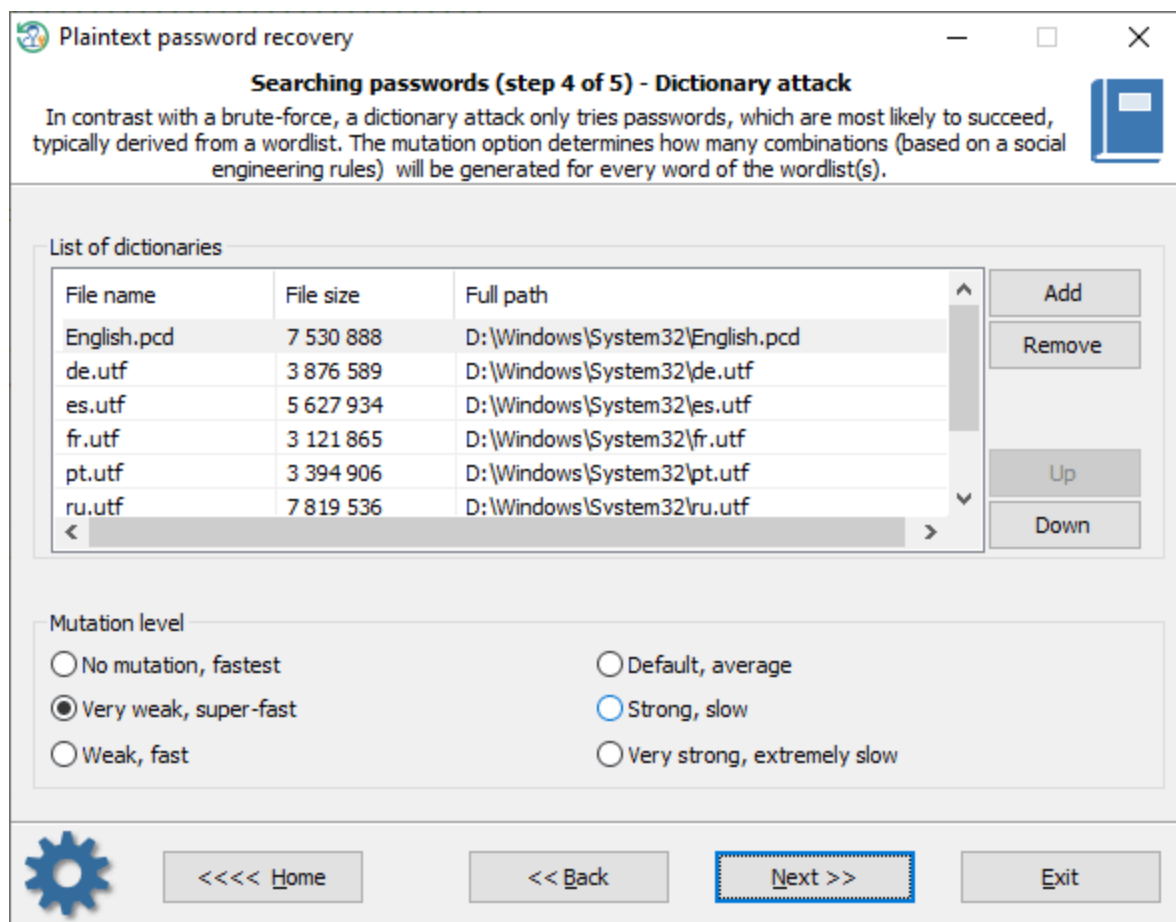
an intelligent recovery. Initially, it launches the guaranteed recovery for the PINs that can be found in the fastest possible way, then goes time-consuming ones, and at last, those with no guaranteed decryption but with a pattern-based search instead. A user can bypass the Intelligent recovery and launch the attack that was chosen during previous steps.

3.16.2.1 Custom recovery

Once the custom recovery option is set, the program can additionally run 3 different attacks to guess the passwords:

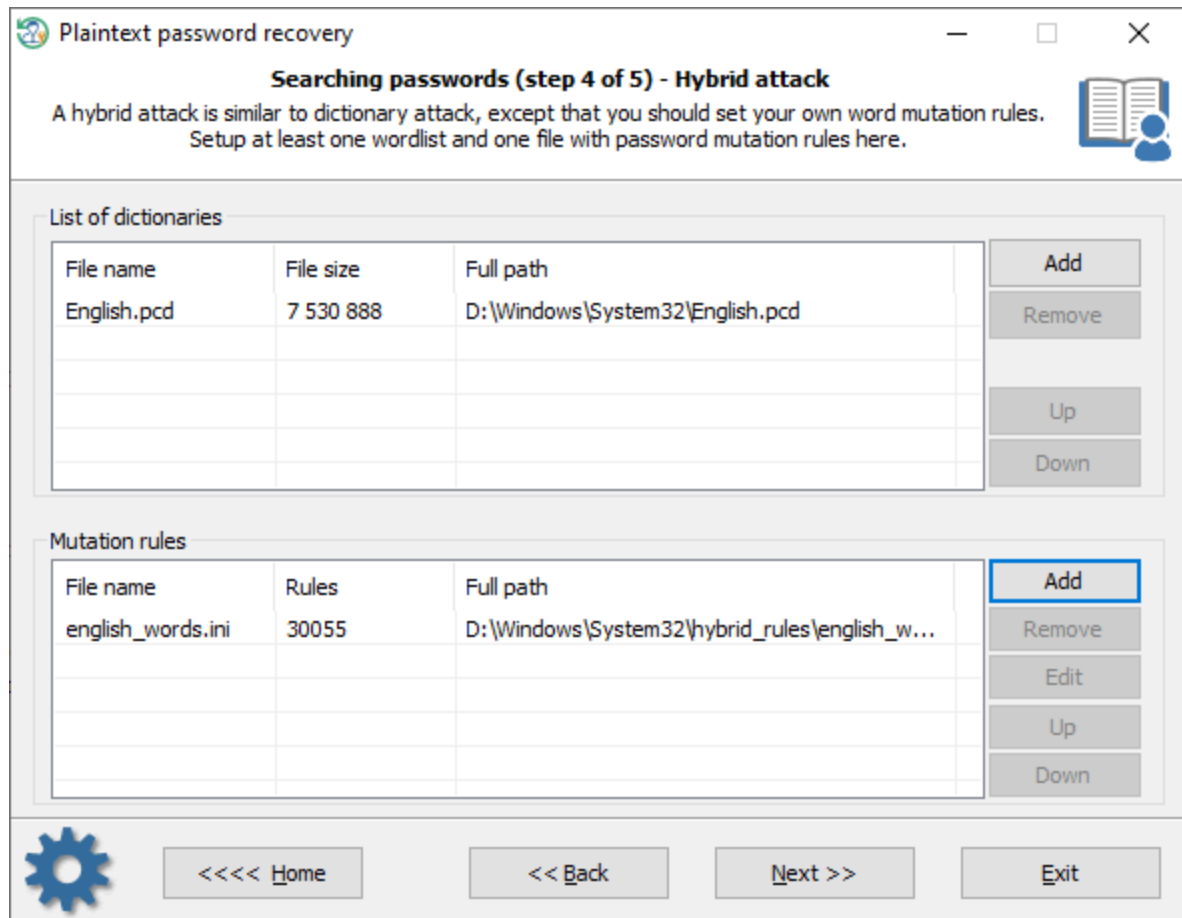
- Dictionary attack
- Hybrid attack
- Mask attack

Dictionary attack



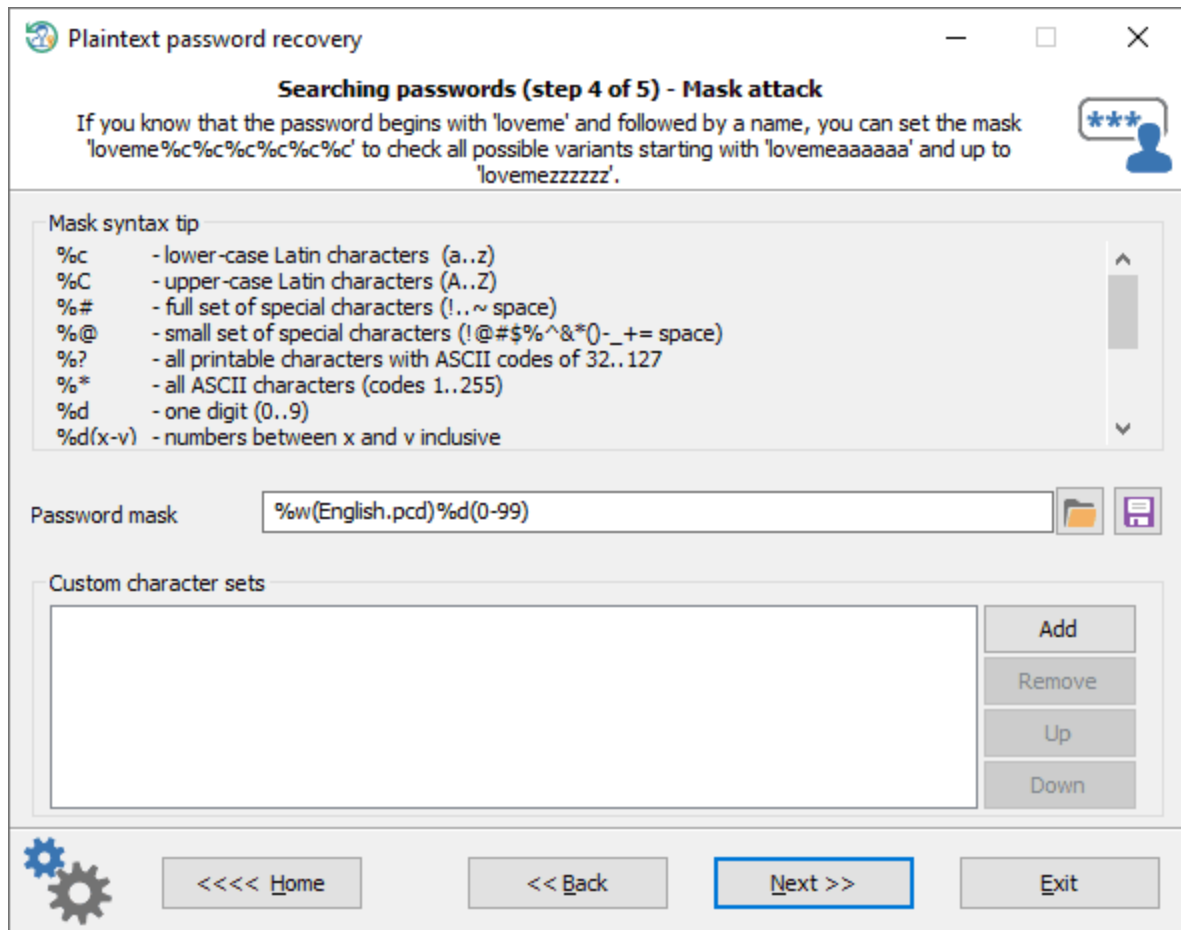
A [dictionary attack](#) tries passwords, which are most likely to succeed, typically derived from a wordlist. RWP supports for different types of dictionaries: ASCII, UNICODE, UTF8, as well as encrypted/compressed dictionaries in the native PCD format. You can use both predefined and custom dictionaries. To add your own wordlist, copy one to a USB drive and attach the drive to the target PC. The mutation level determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

Hybrid attack



A [hybrid attack](#) is similar to a dictionary one, except that you can set your own word mutation rules. The program comes with a huge set of rule-files. Just use one that is best for your task. The good thing in a Hybrid attack is that you can additionally create, edit and modify password mutation rules according to your needs.

Mask attack



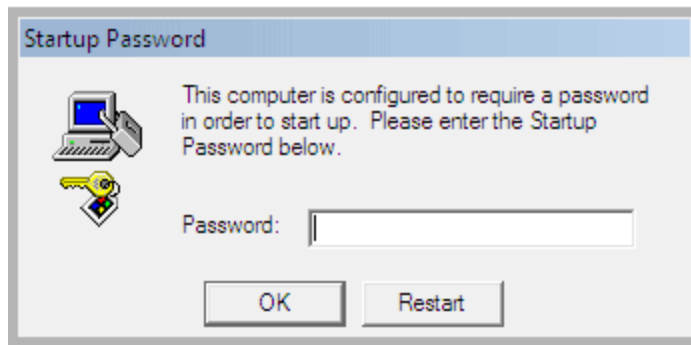
A [Mask attack](#) is an irreplaceable tool when you know a part of the password or have any specific details about it. For example, if you know that the password consists of 12 characters and starts with 'loveme', obviously it's just enough to guess the last 6 characters of the password. That is what the mask attack is for. In our example, you can set the following mask: `loveme%c%c%c%c%c%c%c`. To get more information about how the mask works, please refer to our [online documentation](#).

3.16.3 Search for SYSKEY startup password

Syskey is the additional layer of security, was introduced first in Windows 2000. It is used by default and offers 3 types of protection:

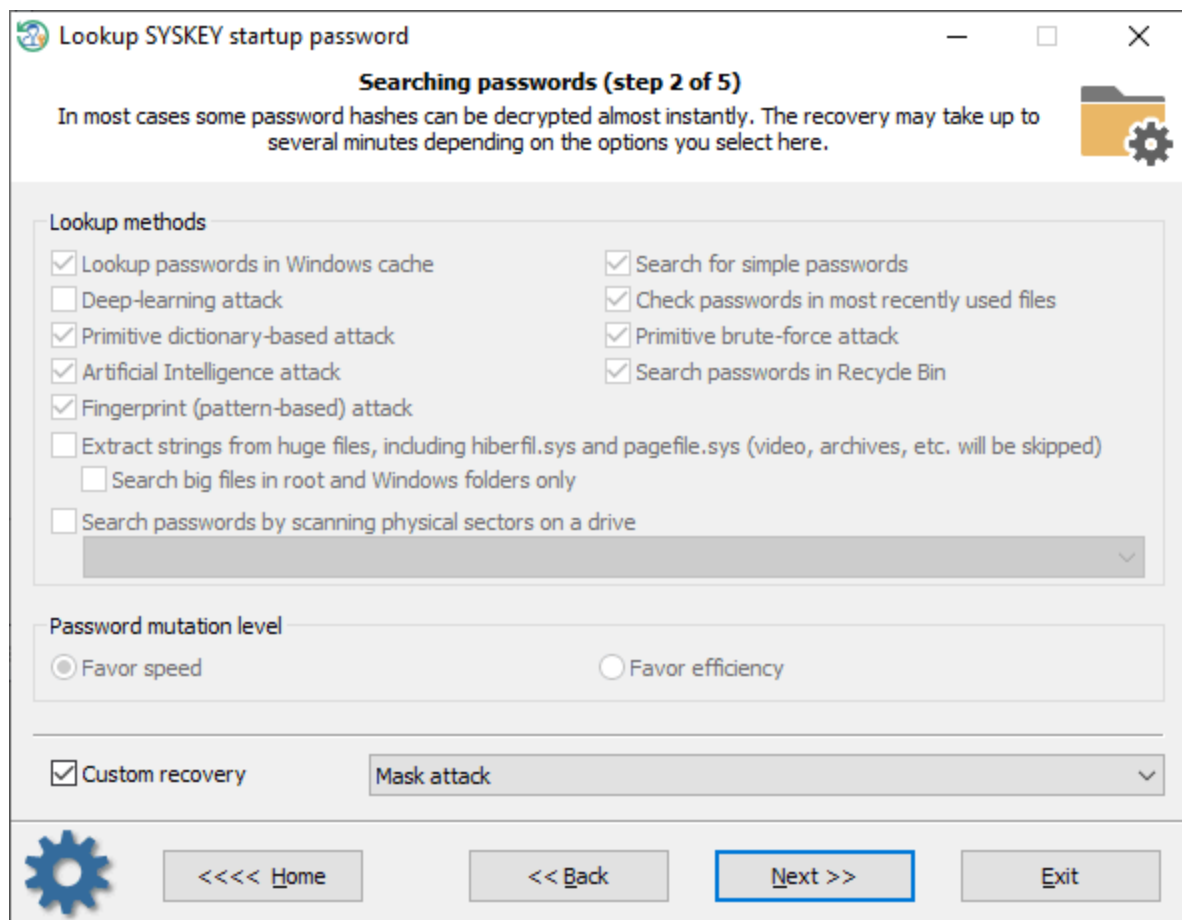
1. **Default** - when the syskey encryption key is stored in Windows registry.
2. **Startup disk** - syskey encryption key is stored on a diskette.
3. **Startup password** - syskey encryption key is generated from a user pass-phrase.

Scammers take advantage of the SYSKEY power and often set a syskey startup password on a victim's PC. Usually they contact you with a thick Indian accent identifying themselves as a member of Microsoft support and tells that your PC need to be fixed immediately because it has a critical problem. They will try convincing you to allow them to connect your system remotely and fix the issues. If you do make the mistake, they will set a SYSKEY startup password. Since you do not know the password, after reloading the system you will get the screen like that (see below) and will not be able to logon unless you pay for fix.



Fortunately, in most cases the passwords they use are pretty trivial and can be decrypted using our SYSKEY password lookup feature. You will have to go through the 3 simple steps to start searching the password.

Setting SYSKEY recovery methods

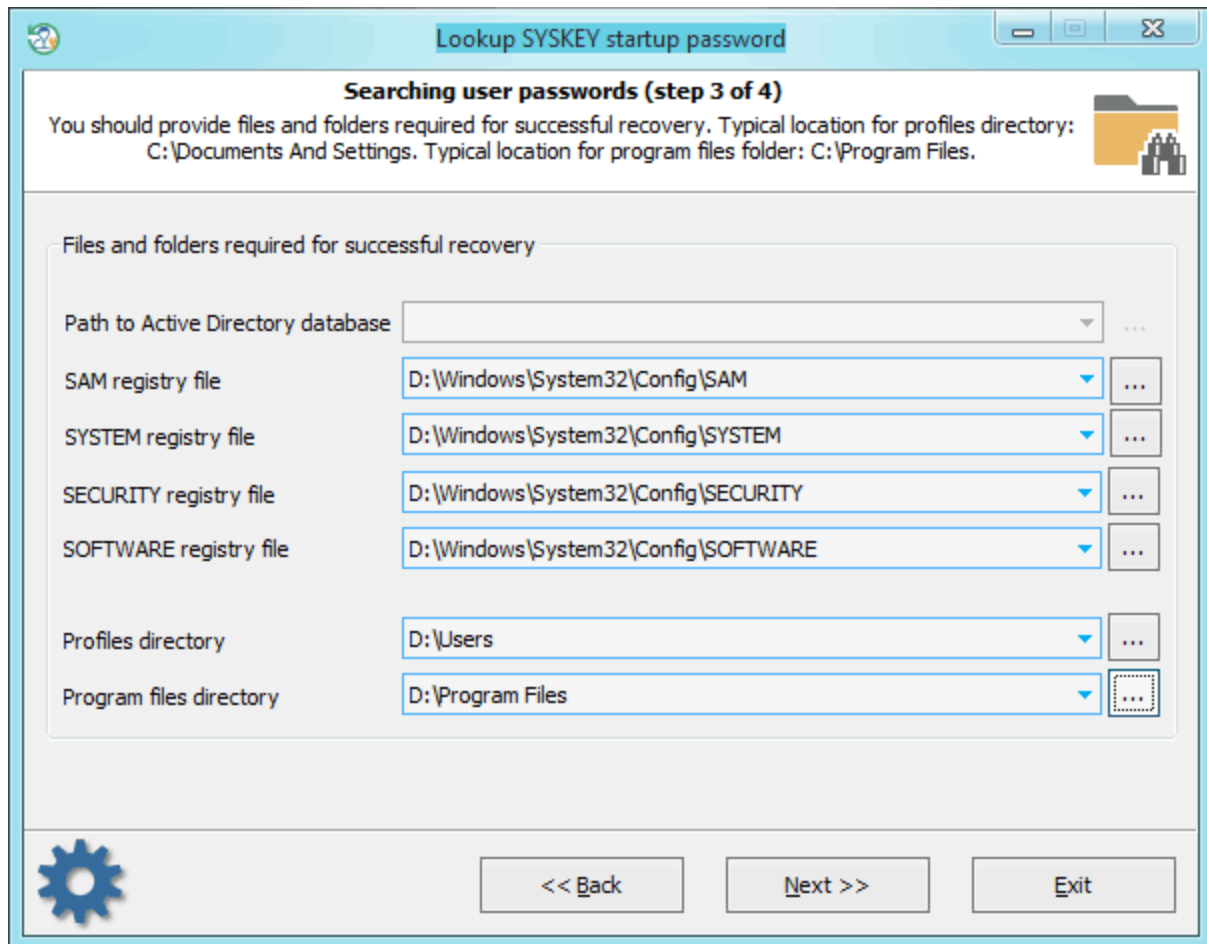


SYSKEY password lookup may take quite some time and consists of the following steps:

1. Searching information in Windows system cache. This method consists of over a dozen of mini sub-attacks, during which the program analyzes all kinds of user passwords: LSA secrets, DSL, VPN, WIFI, FTP, IM, browser passwords, etc.
2. Analyzing simple, short passwords, keyboard combinations, etc.
3. Scan, parse and analyze most recently used files of the target system.
4. Primitive dictionary attack. The application checks all passwords from the built-in dictionary for the Light and Standard editions or from several dictionaries (Arabic, Chinese, English, French, German, Portuguese, Russian, Spanish) for the Advanced Edition. If the deep search option is on, simple word mutations will also be taken into account during the search.
5. Primitive brute-force recovery will try to reveal short passwords. The brute-force options are also depend on the mutation level.
6. Artificial Intelligence attack analyzes network activity of a user on the computer. Upon the results of the analysis, the application generates user preferences and generates a semantic dictionary for the attack, which it later uses it for finding and guessing the password.
7. Look for passwords in deleted files.
8. Searching for complicated English passwords (Fingerprint attack).
9. Extract strings and words from huge files: RAM images, hiberfil.sys, pagefile.sys and so on. When this option is set, the program will try to skip files useless in password analysis like video, archives, audio files, etc.
10. Search passwords by reading and analyzing raw sectors of the selected drive. If the '*Password mutation level*' is set to '*Deep search*', the program additionally tries to generate different combinations and 'mutate' found passwords, thus walking through all sectors of the target drive may take quite a time. Note that the sector-based scanning algorithm is not effective against drives which have a full-disk encryption set on.

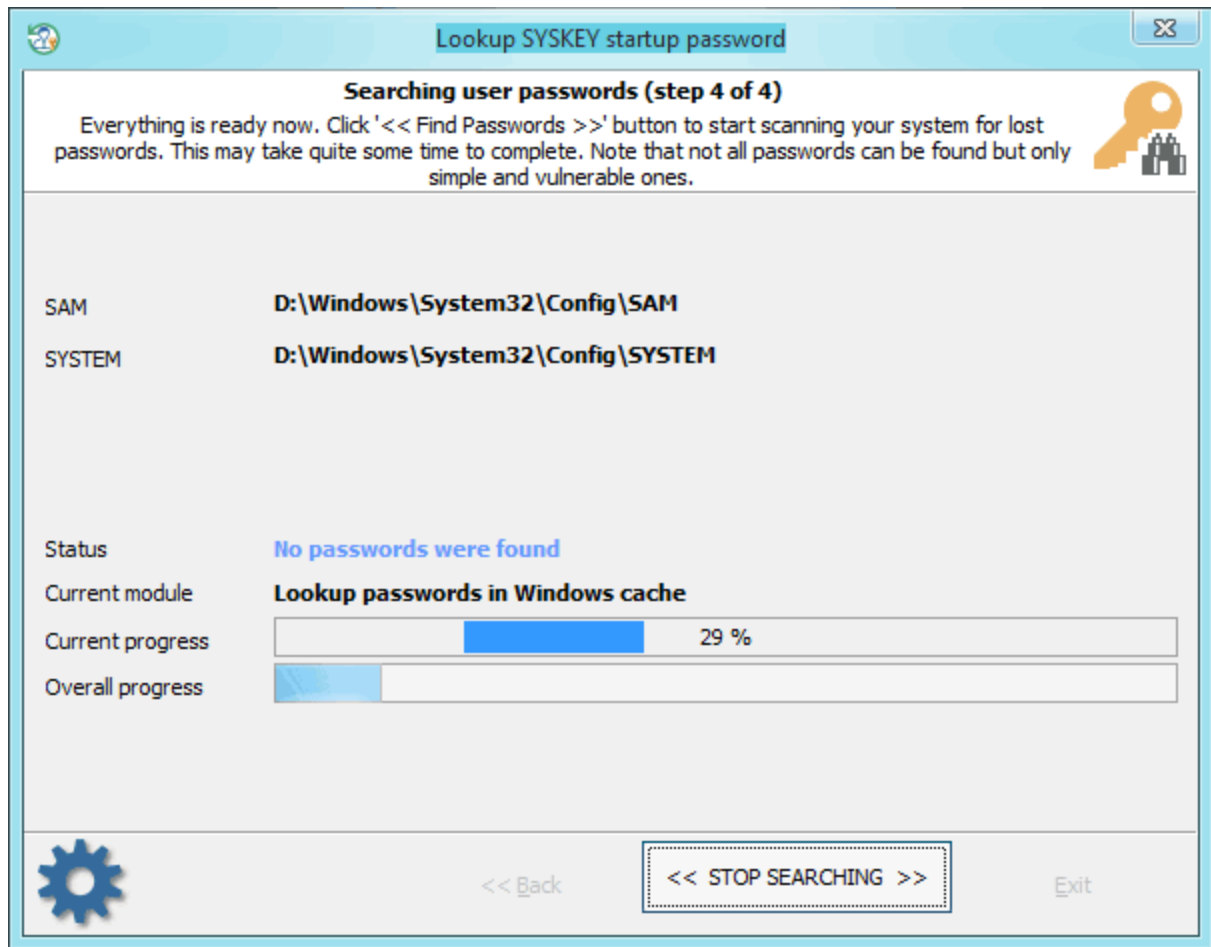
To apply a [custom recovery method](#), turn on the 'Custom recovery' option and select one of the available attacks. On the next step you will be prompted to set up various options related to the selected attack.

Selecting data source



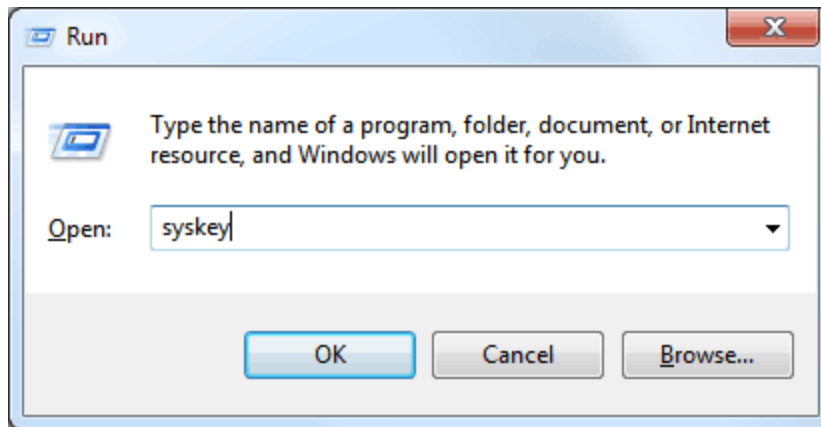
When searching for the SYSKEY startup password, special attention is to be paid to supplying correct files and folders required for the analysis process. Otherwise, password search will be inefficient or even not available. The application tries to locate the files automatically, but sometimes, e.g., when the computer has several operating systems installed, you may need to use the 'manual control' over it. Please also keep in mind that if the problem PC has 2 or more logical drives, the sequence of the letters for these disks may be set totally different than in the original system.

Searching for SYSKEY password

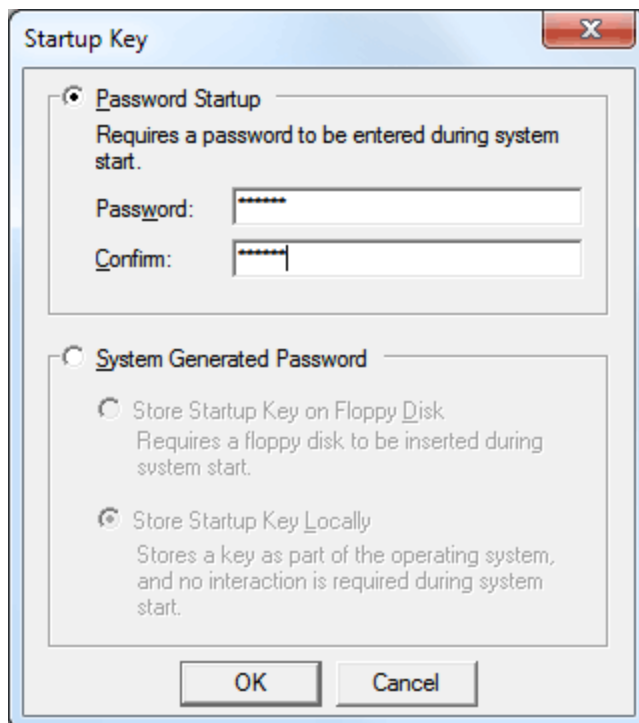


Finding/guessing the password may take some time, which depends on attack settings and peculiarities of your system. Note that only simple and vulnerable passwords can be recovered!

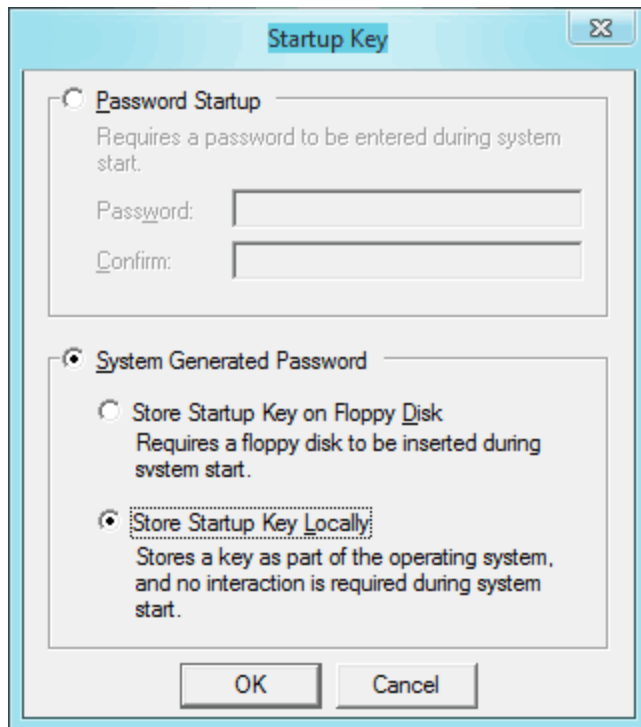
Once you retrieve the SYSKEY plaintext password, all you need is to turn off the SYSKEY startup prompt and set your system back to its original state. Turn on your problem PC and use the found password to bypass the SYSKEY startup dialog. Then logon into your Windows account, hit '**Win+R**' keys, type in '**SYSKEY**' and click '**OK**' button.



This should bring up the SYSKEY options dialog. All you need here is to click the '**Update**' button and switch the '**Password Startup**' option back to '**System Generated Password**' by supplying the found plaintext.



So, after all changes, you should have it look like this:

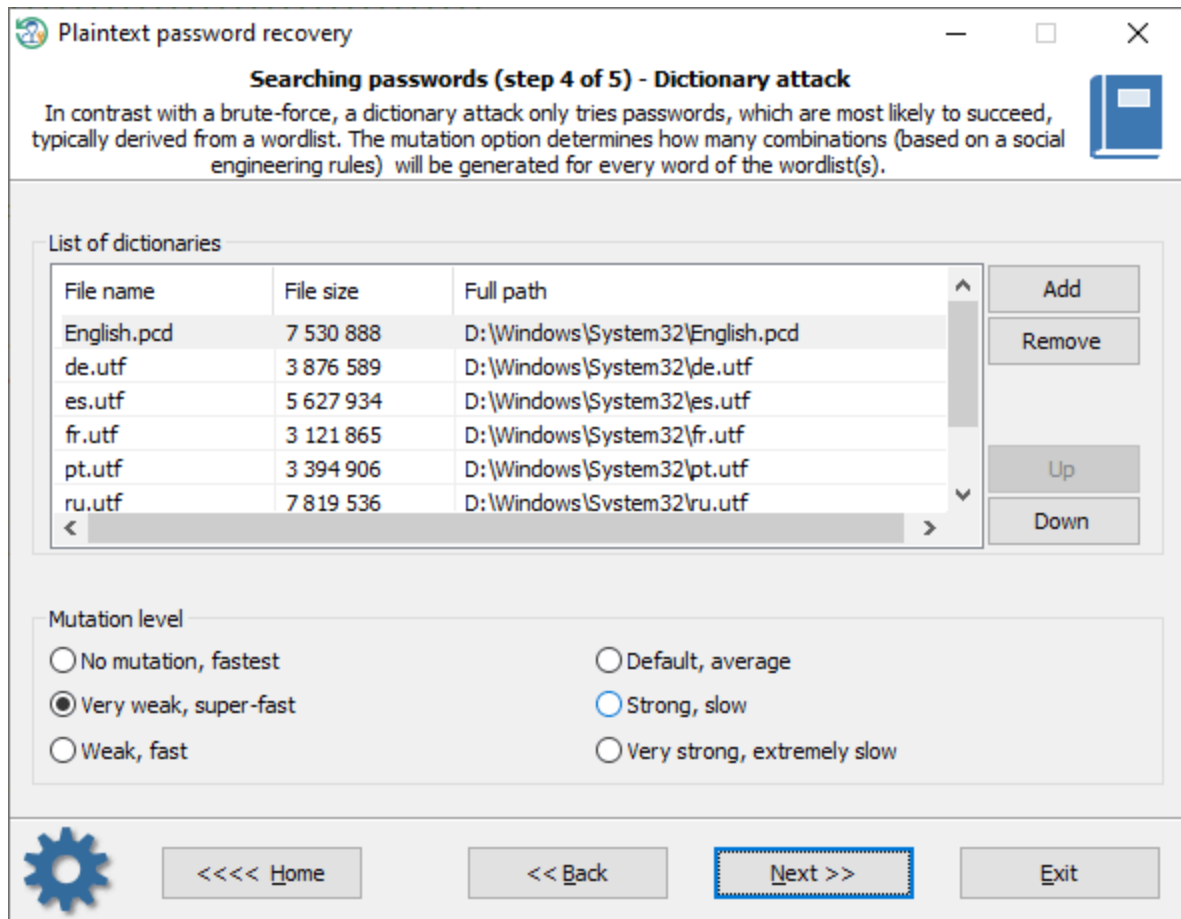


3.16.3.1 Custom recovery

Once the custom recovery option is set, the program can additionally run 3 different attacks to guess the passwords:

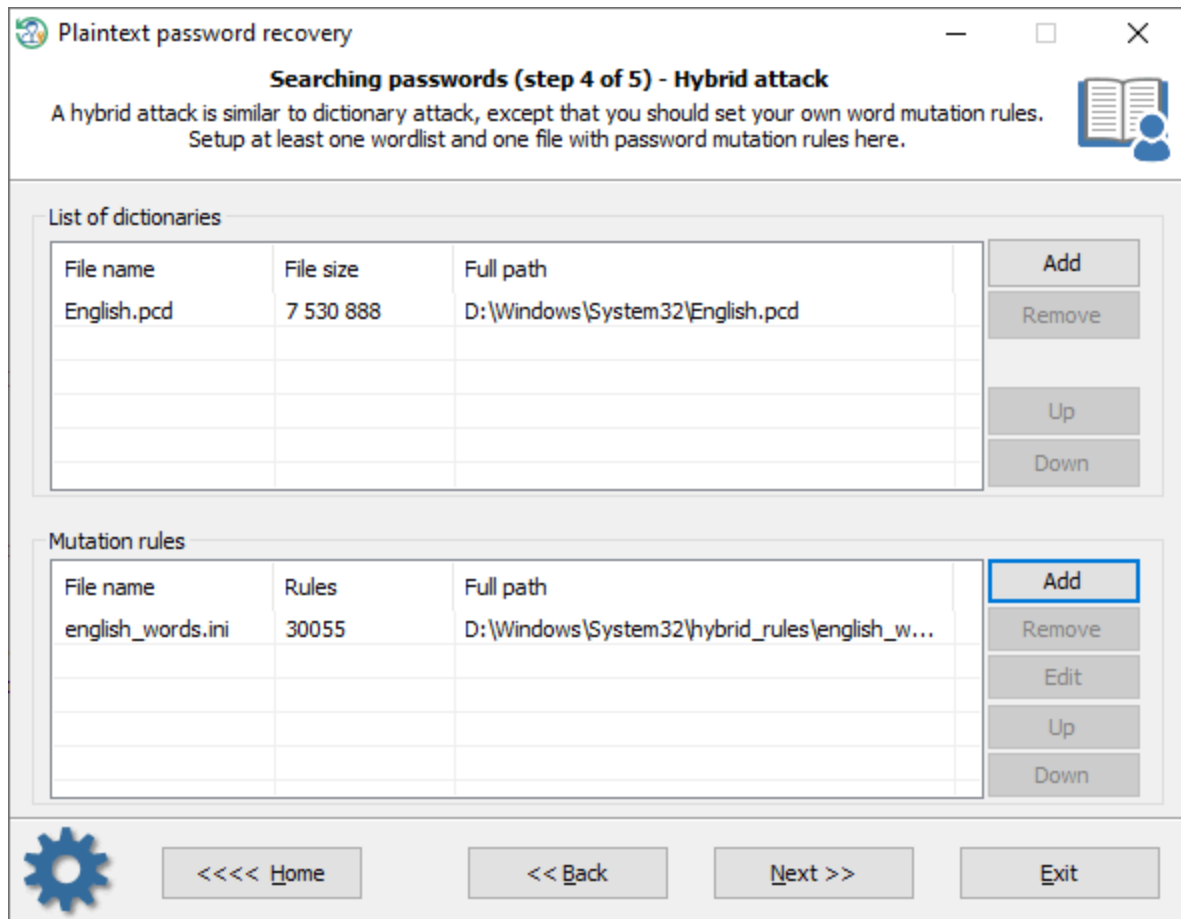
- Dictionary attack
- Hybrid attack
- Mask attack

Dictionary attack



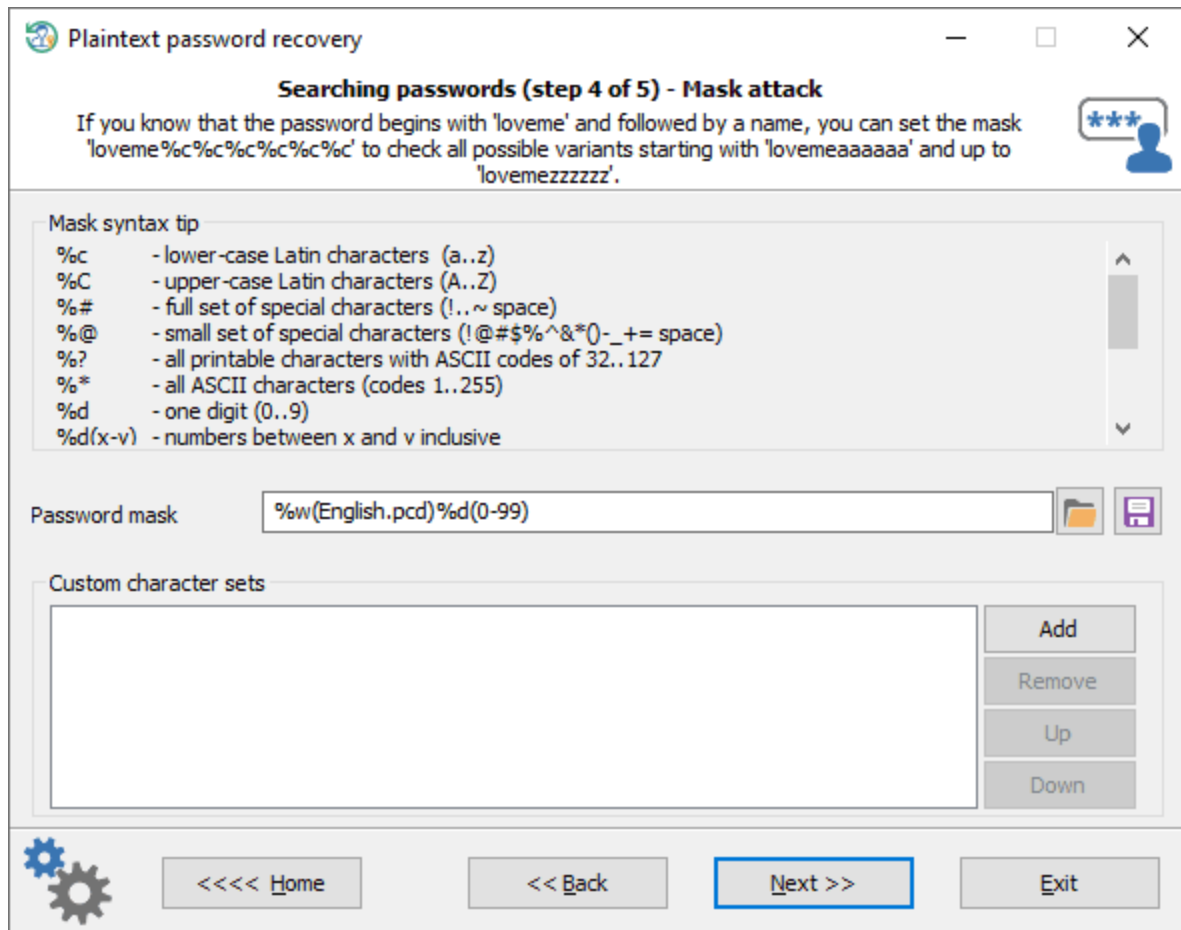
A [dictionary attack](#) tries passwords, which are most likely to succeed, typically derived from a wordlist. RWP supports for different types of dictionaries: ASCII, UNICODE, UTF8, as well as encrypted/compressed dictionaries in the native PCD format. You can use both predefined and custom dictionaries. To add your own wordlist, copy one to a USB drive and attach the drive to the target PC. The mutation level determines how many combinations (based on a social engineering rules) will be generated for every word of the wordlist(s).

Hybrid attack



A [hybrid attack](#) is similar to a dictionary one, except that you can set your own word mutation rules. The program comes with a huge set of rule-files. Just use one that is best for your task. The good thing in a Hybrid attack is that you can additionally create, edit and modify password mutation rules according to your needs.

[Mask attack](#)

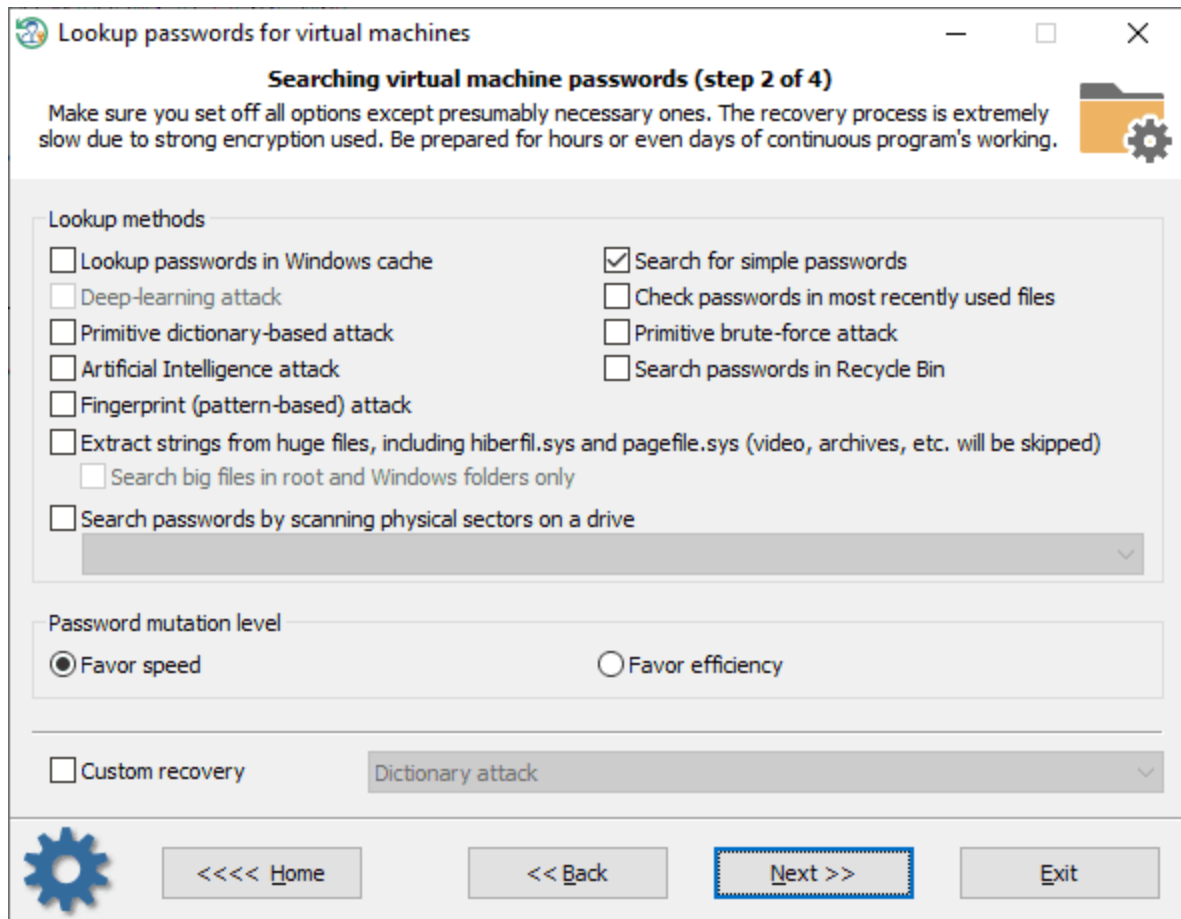


A [Mask attack](#) is an irreplaceable tool when you know a part of the password or have any specific details about it. For example, if you know that the password consists of 12 characters and starts with 'loveme', obviously it's just enough to guess the last 6 characters of the password. That is what the mask attack is for. In our example, you can set the following mask: loveme%c%c%c%c%c%c%c. To get more information about how the mask works, please refer to our [online documentation](#).

3.16.4 Search for virtual machine passwords

Once a password for Virtual Machine is forgotten, you can use this RWP feature to get back access to your locked VM. The current version of the program supports VmWare and Oracle VirtualBox virtual machines. Both virtualization programs have very strong protection, thus password recovery for these VMs has some peculiarities described below.

[Setting up password recovery methods](#)



At the very beginning, determine what search methods fit best for your task. Password recovery for Virtual Machines is an extremely slow process, so it is highly recommended to disable the most time-expensive items. The '[Custom recovery](#)' checkbox switches between custom and predefined attack templates. If the first is selected, you will be asked to configure some options for the selected attack during the next Wizard steps. If certain information about the password is known, a custom attack would be your choice.

Selecting data source

Lookup passwords for virtual machines

Searching passwords (step 3 of 4)

You should provide files and folders required for successful recovery. Typical location for profiles directory: C:\Users. Typical location for program files folder: C:\Program Files.

Files and folders required for successful recovery

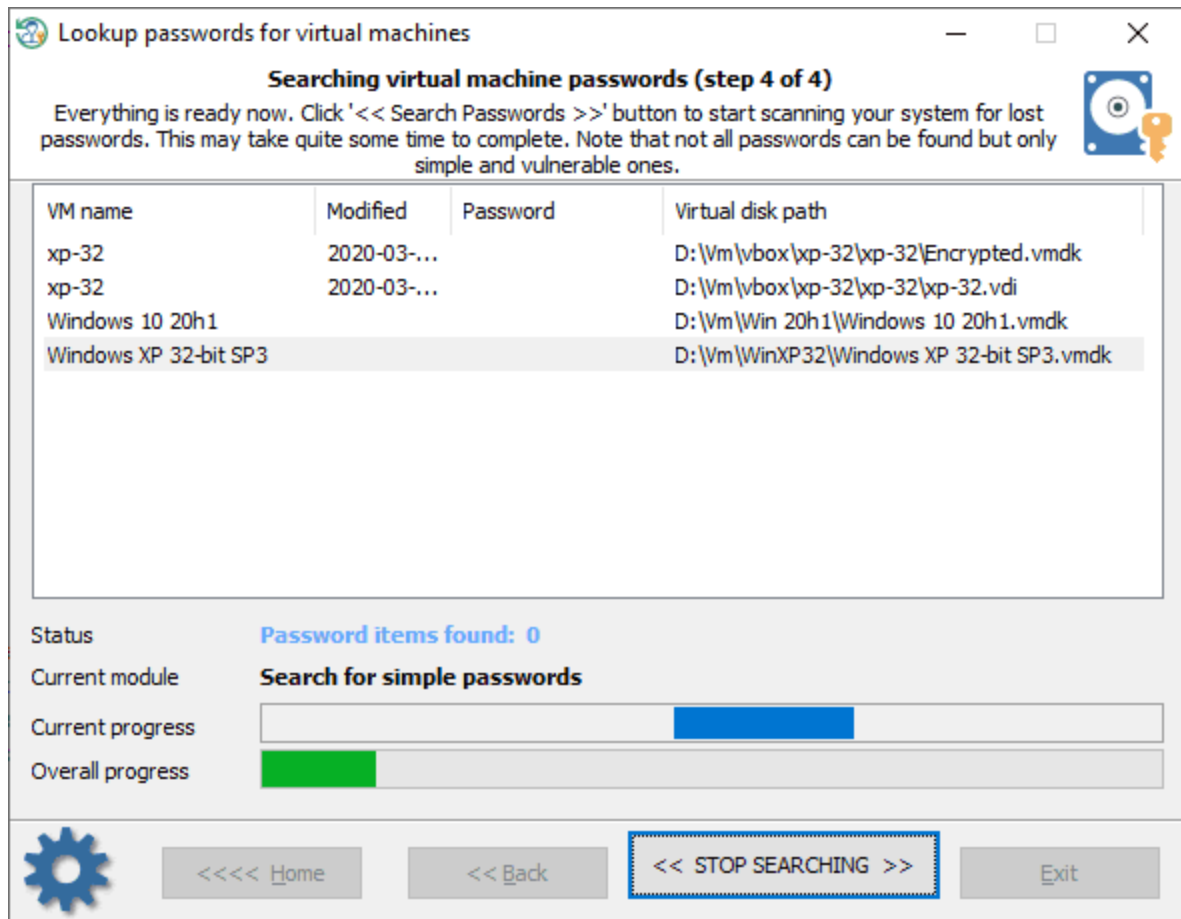
Path to Active Directory database		
SAM registry file	C:\Windows\System32\Config\SAM	
SYSTEM registry file	C:\Windows\System32\Config\SYSTEM	
SECURITY registry file		
SOFTWARE registry file		
Profiles directory	D:\Users	
Program files directory		

Settings <<<< Home << Back Next >> Exit

Please, pay special attention to setting up all folders required for further system analysis. Otherwise, the program will be able neither to detect Virtual Machines nor to search for passwords properly. In most cases, RWP automatically fills up all fields with required files and folders.

Keep in mind that the disk letters may differ from ones on the original system!

Searching for virtual machine passwords



Searching for VM passwords usually takes a really long time. All virtual machines have very strong protection and in some cases, the password search speed is as low as only a few passwords per second. Therefore, to optimize and increase the process, just exclude unnecessary virtual machines from the search list and leave active the only one you need. Use the context menu for that.

3.16.5 Search passwords for encrypted documents

Modern documents have extremely strong password protection that makes common recovery methods like a brute-force or a dictionary attack useless in most cases. Therefore, once the encryption password for such a document was not recovered using any other program applying the common recovery methods, then the Reset Windows Password is your last chance to find the password.

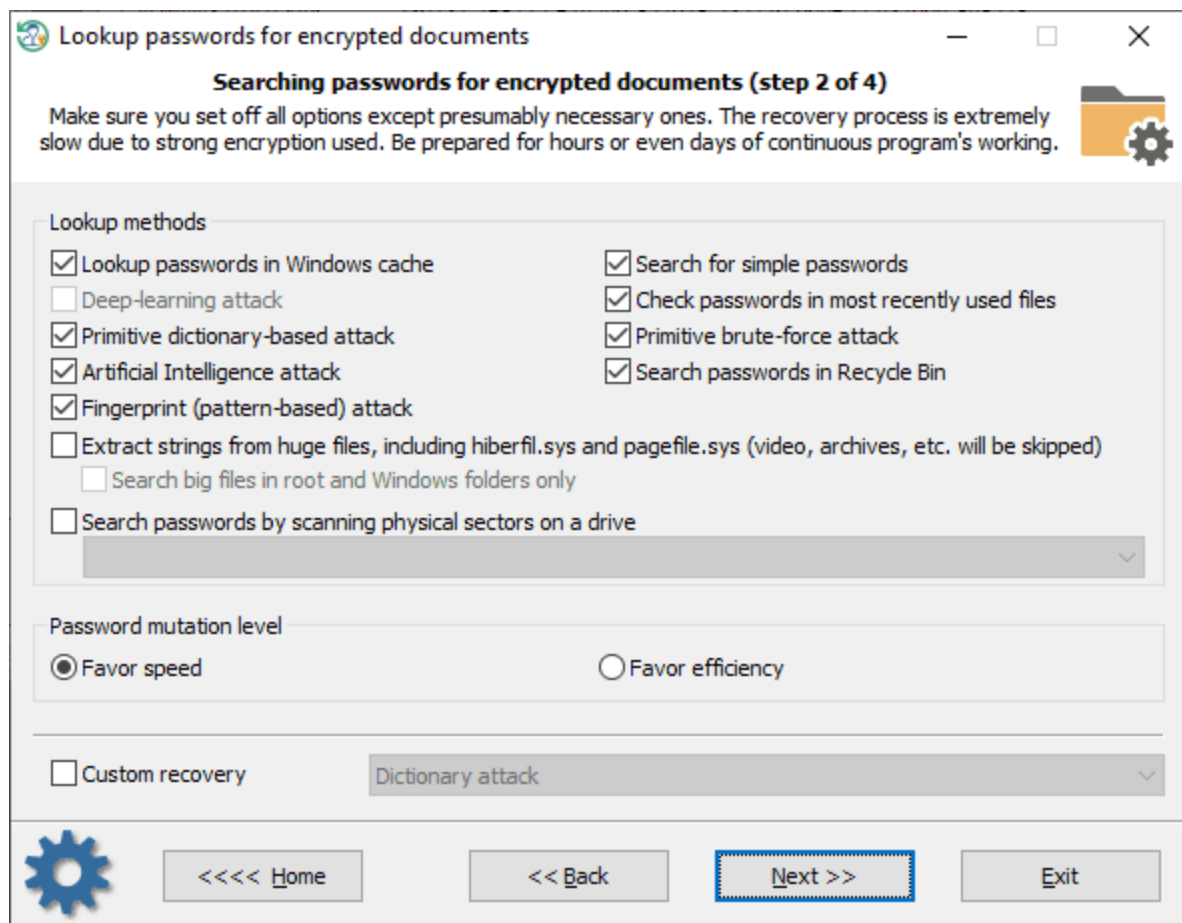
A well-known secret that uncovers password weakness is that many users often reuse their passwords or use slightly modified variations when creating Internet accounts, encrypting documents, creating wireless networks, etc. RWP utilizes the weakness in its powerful built-in engine to increase the recovery percentage for algorithms that cannot be broken using common methods. If you do not go into details, then everything is quite trivial at first glance: the program scans the system, enumerates every found password, as well as some password candidates, for every found item it makes all possible

mutations and modifications, and at the final stage, tries to guess the original password using the huge variety of the generated items. Despite its apparent simplicity, the internal algorithms are quite complex. For example, the general password lookup module consists of several dozen sub-modules. This also applies to other modules and groups of modules such as mutation, artificial intelligence, etc.

The current version of the program supports the following file formats:

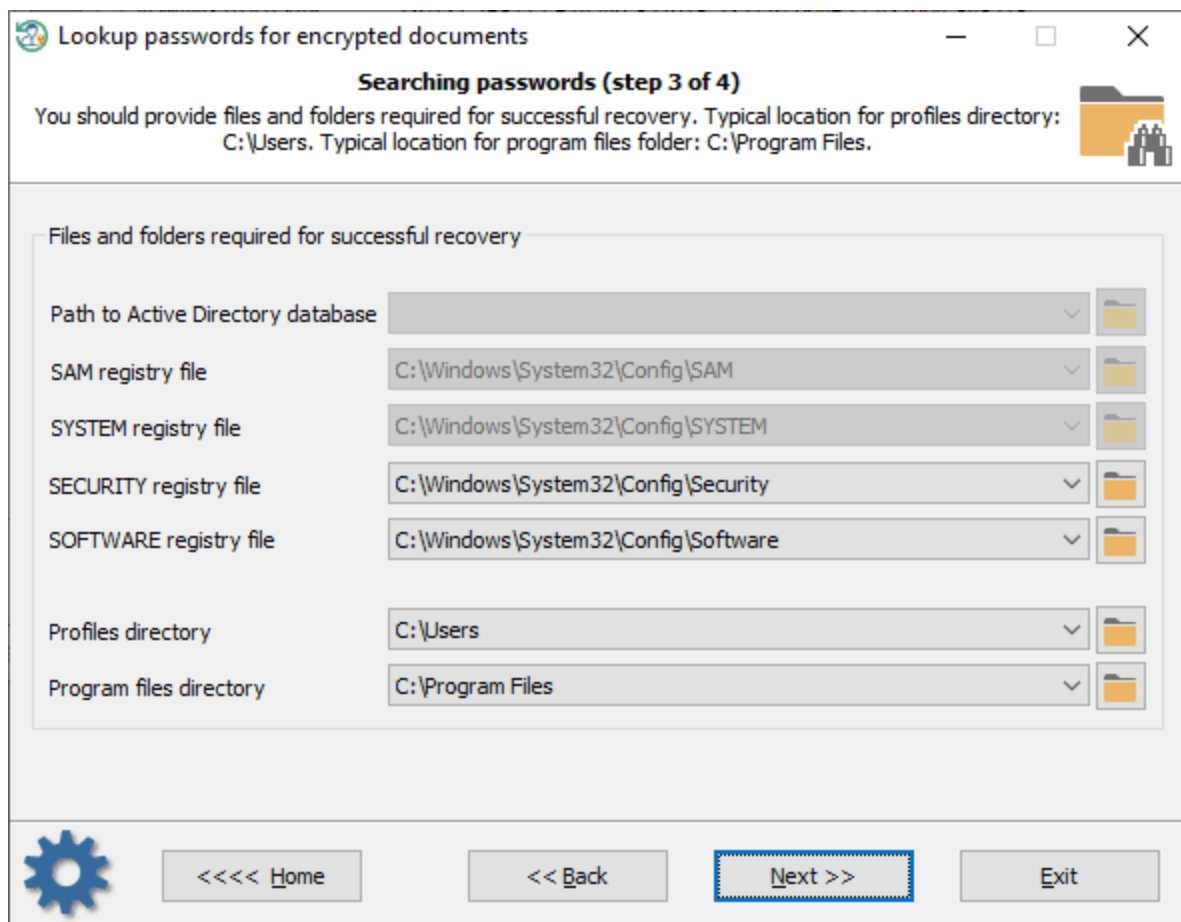
- Microsoft Office 97 and newer documents
- Files in OpenDocument format: OpenOffice, LibreOffice, MyOffice.
- PDF documents (both user and owner passwords).

Setting up password recovery methods



At the very beginning, determine what search methods would fit best for your task. Password recovery for encrypted documents is an extremely slow process, especially if you have more than one file to decrypt. Thus it is highly recommended to turn off the most time-consuming methods. If certain information about the password is known then it would not be unreasonable to switch to a custom attack. Just click the '[Custom recovery](#)' checkbox and choose one of the available methods. For example, a Mask attack. Otherwise, the default parameters is your best choice.

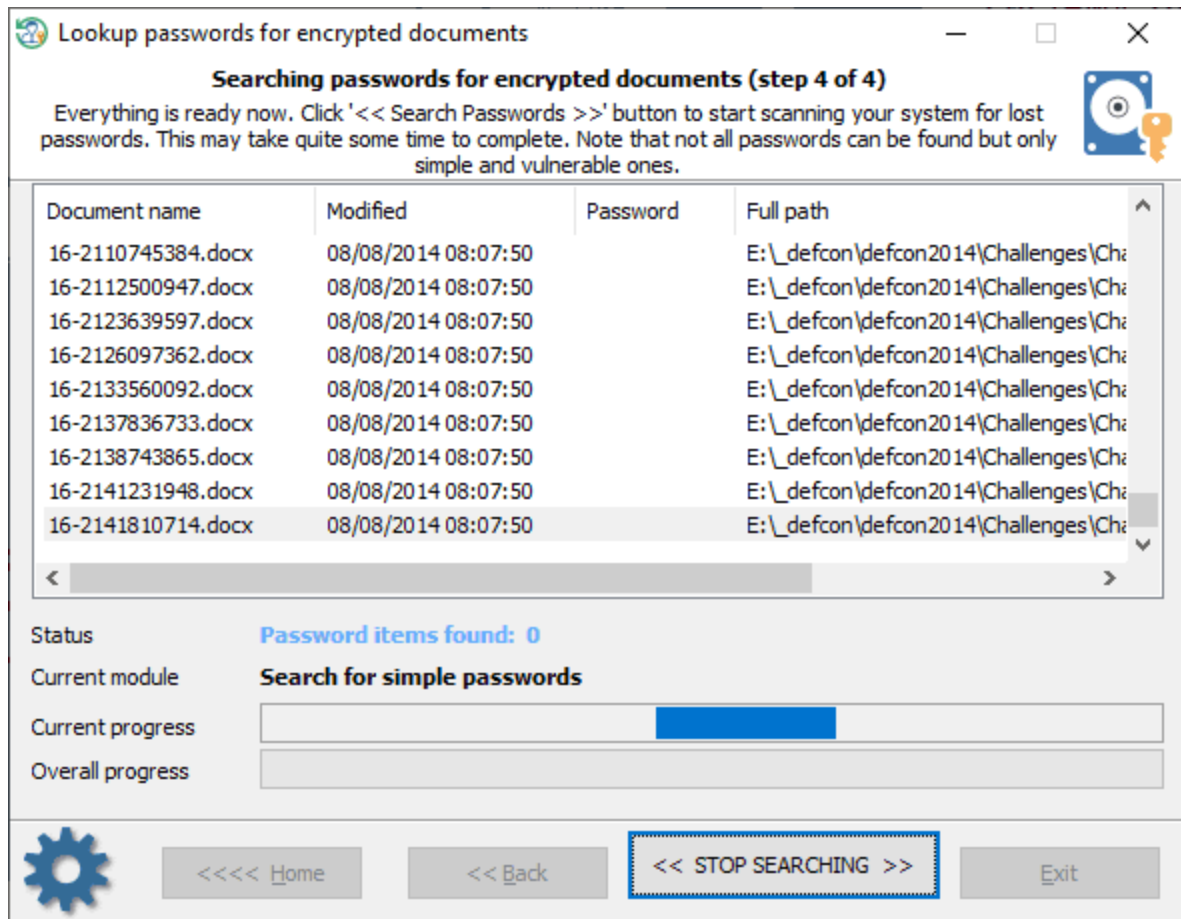
Setting up folders



All you need here is to set up all the required folders properly. Some of them are vital when analyzing files and password candidates. In most cases, the program sets them up automatically.

Keep in mind, the the drive letters may differ from the original system!

Searching password for encrypted documents



The program guesses passwords for all found documents simultaneously (unless you mark some of them to be skipped). The password lookup process usually takes quite some time. For example, guessing passwords for Microsoft Office 2013 and newer documents runs at less than 10 passwords per second for a single document! Therefore, to optimize and increase the search speed, do exclude unnecessary documents from the search list, ideally leaving only the necessary one. You can use the context menu for that.

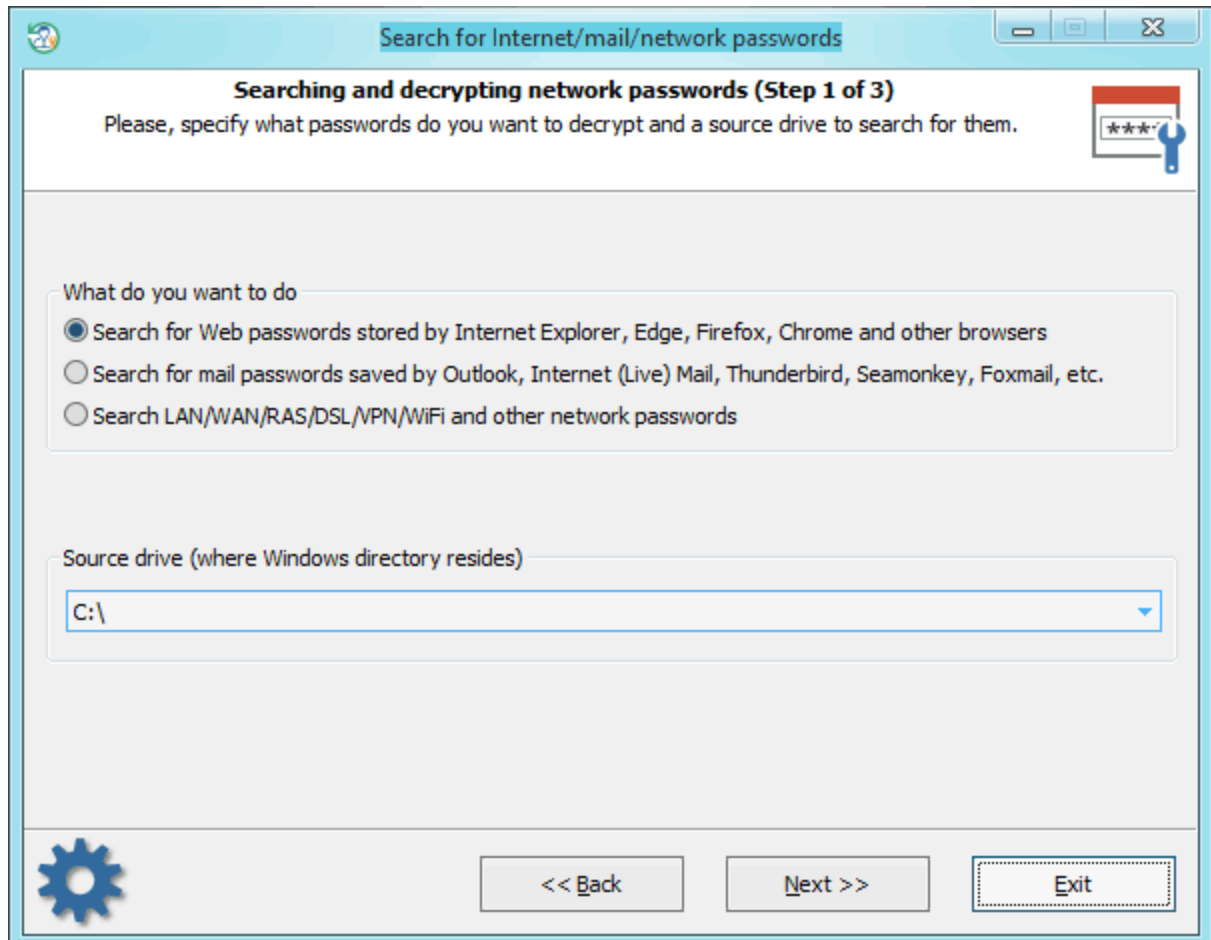
To add a new file, right-click them mouse button and select 'Add new document'.

Starting with version 11 the program has a built-in technic to recover Indian Aadhaar and e-pan cards out-of-the-box. An [Aadhaar card](#) is a pdf file that contains a unique Identification Authority of Indian citizens. An e-pan card is a digital identifier issued by the Indian Income Tax Department..

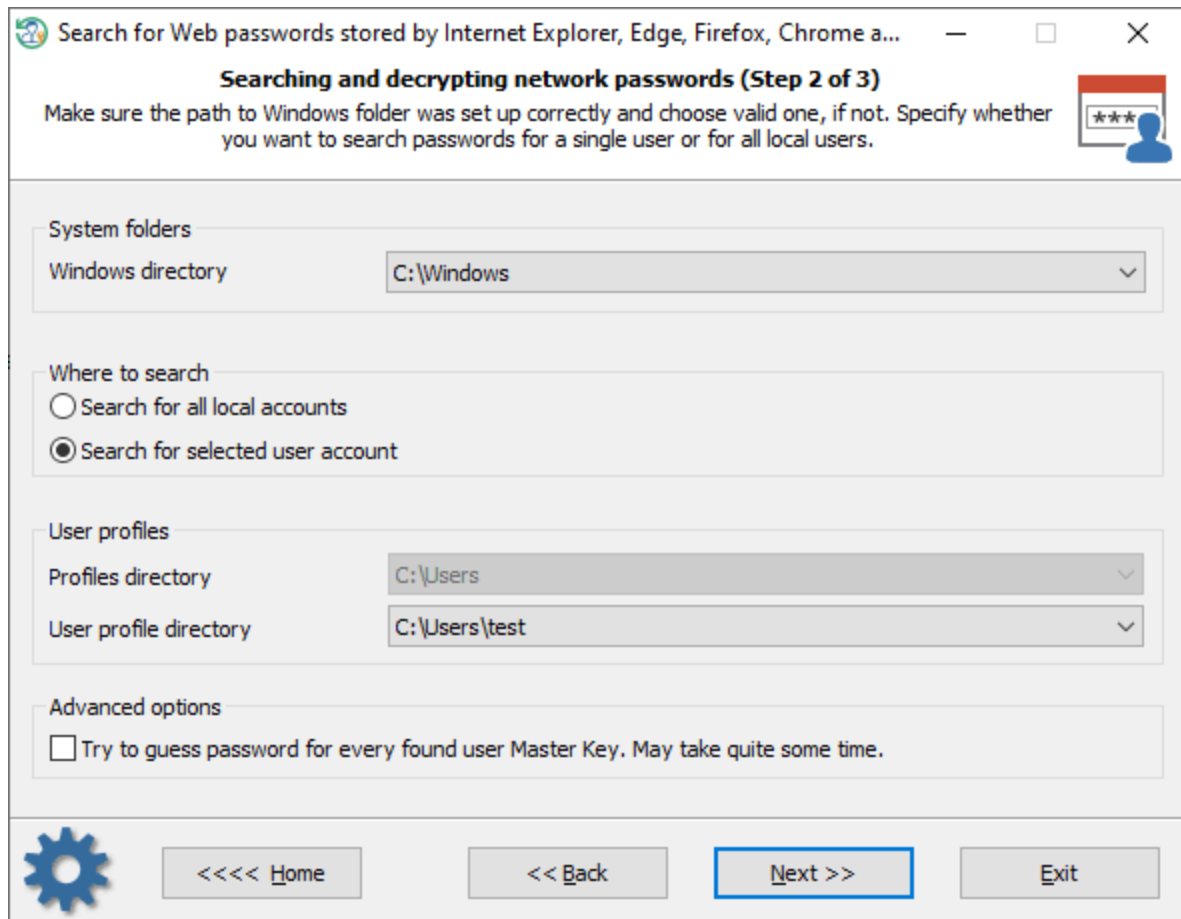
To recover an Aadhaar/e-pan card, right-click the list of found items and deactivate any other documents except those you need to decrypt. Setting active Aadhaar/e-pan pdfs only should increase the recovery speed drastically. Then click the << Start searching >> button to launch the password lookup. The program automatically involves 7 built-in attacks. That allows keeping the success rate close to 100%.

3.16.6 Search for Internet/mail/network passwords

One of the application's most notable features is searching and decrypting PC users' network passwords. Reset Windows Password supports all major popular browsers and email clients. The interface is split into three steps to make the process as easy as possible, and the specific details are left to the program.



On the first step of the Wizard, the program prompts you to select the type of passwords to be searched for and the source drive with the Windows folder. By default, the program selects the first hard drive, where the operating system is installed.



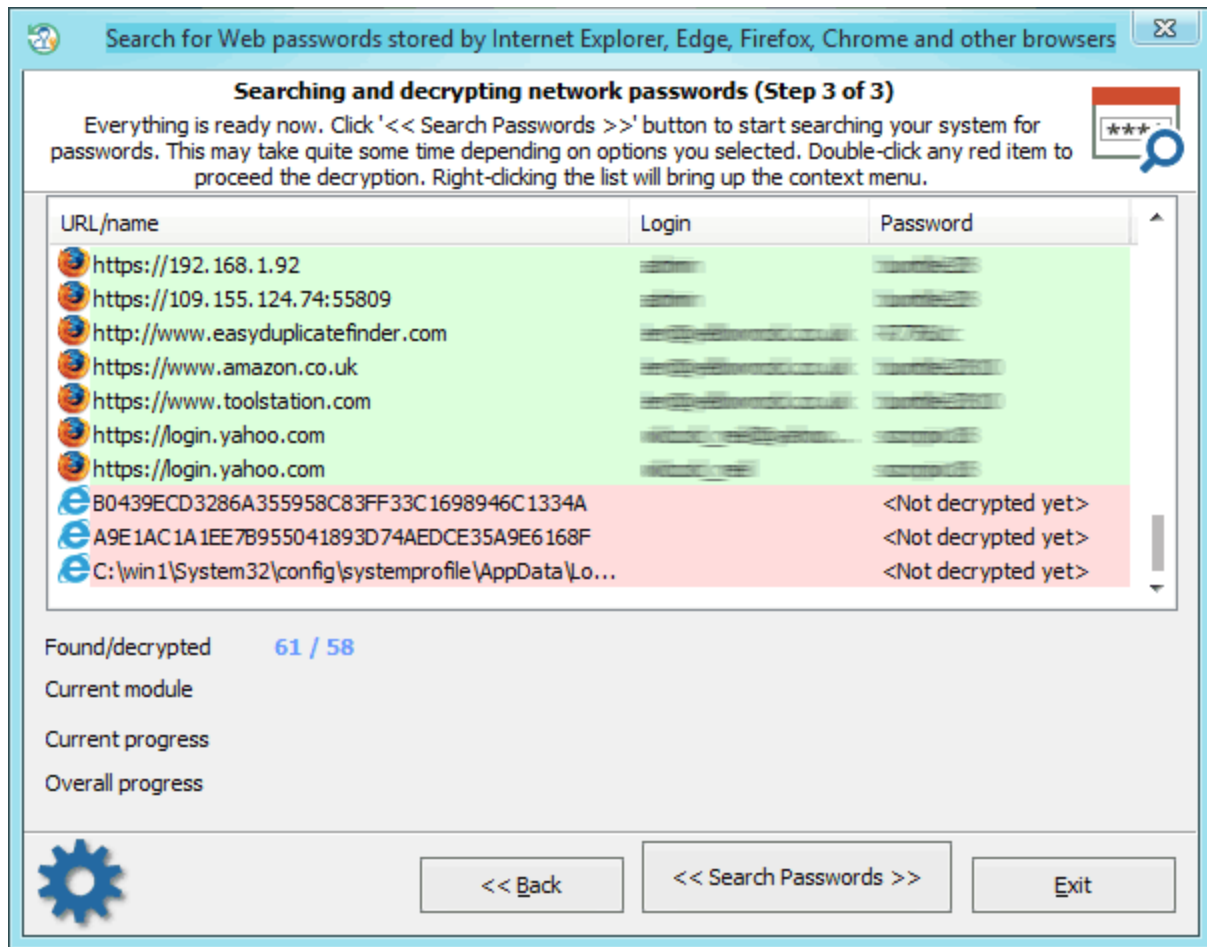
On the next step, specify the location of the Windows folder and the folders where the program will try to find the passwords: all user profiles or only the selected one. In the latter case, select the respective folder.

By default, the program automatically scans the system for any information (for example, [TBAL](#) or [domain secrets](#)) that can be used to decrypt DPAPI data without providing user logon passwords. However, setting the advanced option on, you can force the program to guess DPAPI Master Key passwords using some found items. For example, using cached credentials, LSA secrets, extracted browsers' passwords, wireless/dialup/dls/ras/lan and other network passwords, etc. Once a DPAPI Master Key password is guessed, there's no need to provide user logon credentials. The program uses the decrypted Master Key to decode any data protected with this Key. However, the process may take quite some time depending on the number of found Master Keys and password items to guess.

In the final dialog, clicking the **<< Search Passwords >>** button launches the process of gathering, analyzing, and decrypting data. Please be patient; depending on the selected options and the number of users in the system, the process may take quite some time.

3.16.6.1 Search for Web passwords stored by Internet browsers

Selecting the internet password search opens a screen like this:



The application decrypts passwords from all major Web browsers:

- Internet Explorer
- Edge
- Firefox
- Opera
- Chrome
- Safari
- Majority of Mozilla-based browsers: Flock, Seamonkey, Pale Moon, Waterfox, etc.
- Major browsers based on Chromium sources: 360 Safe Browser, 7Star, Amigo, Brave, Centbrowser, Chedot, Canary, Coccoc, Comodo Dragon, Elements, Kometa, Orbitum, QQ Browser, Sputnik, Torch, UC Browser, Uran, Vivaldi.

Web browsers use different algorithms for protecting users' personal data. Passwords from the following browsers can be decrypted almost instantly:

- Internet Explorer 4-6
- Firefox and other Mozilla-based browsers (unless Master Password is set)
- Old versions of Opera (unless Master Password is set)

Decrypting other data requires additional information. That is usually the Master Password or the user logon password:

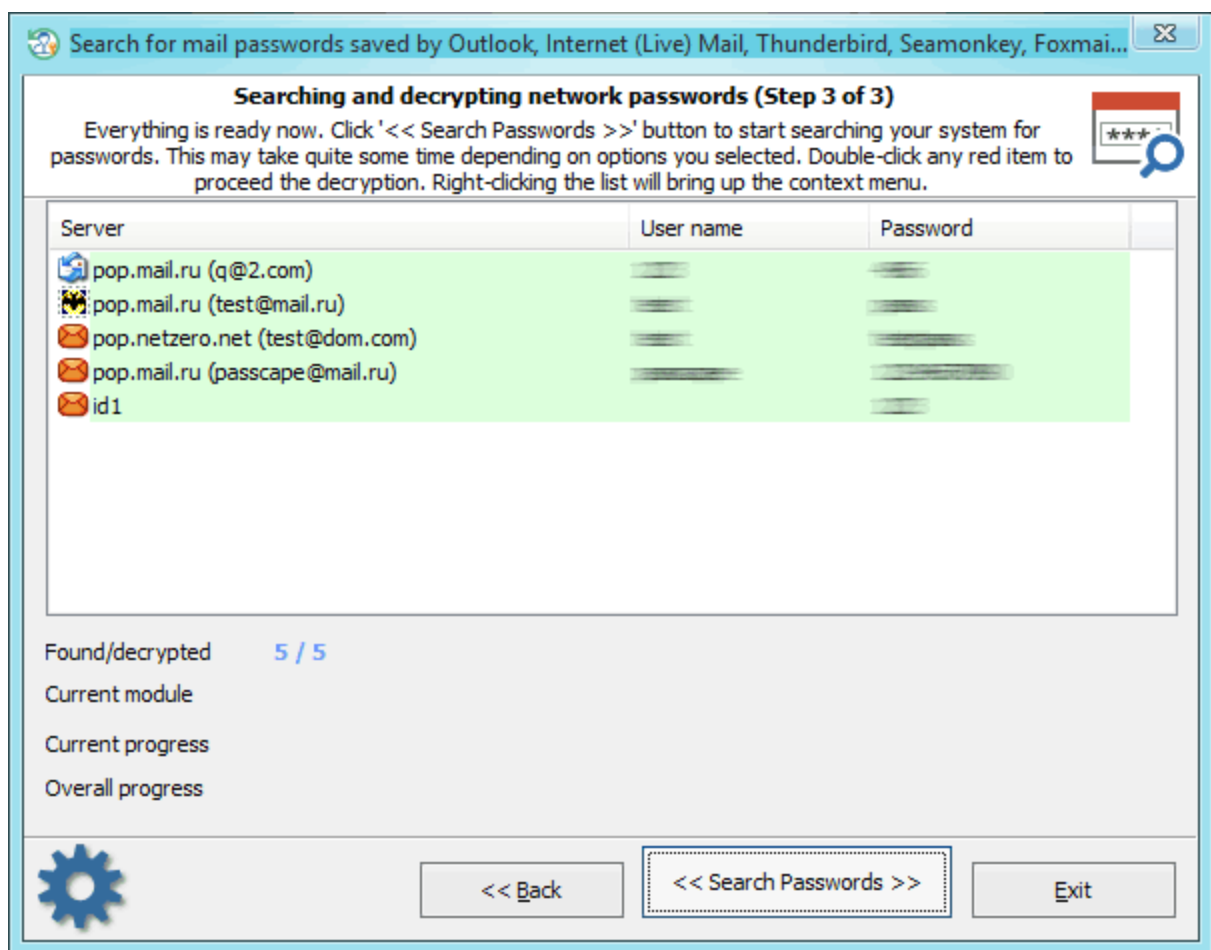
- Internet Explorer 10
- Edge
- Firefox (if Master Password is set)

- Opera (if Master Password is set)
- Chrome
- Safari

To activate the next step of the decryption, simply double-click on the record highlighted in red.

Internet Explorer 7-9 require three-step decryption. First, one should enter the URL where the password was saved, then enter the account password. More information on this tricky kind of protection used in Internet Explorer 7-9 can be found in [our article](#).

3.16.6.2 Search for mail passwords saved by email clients

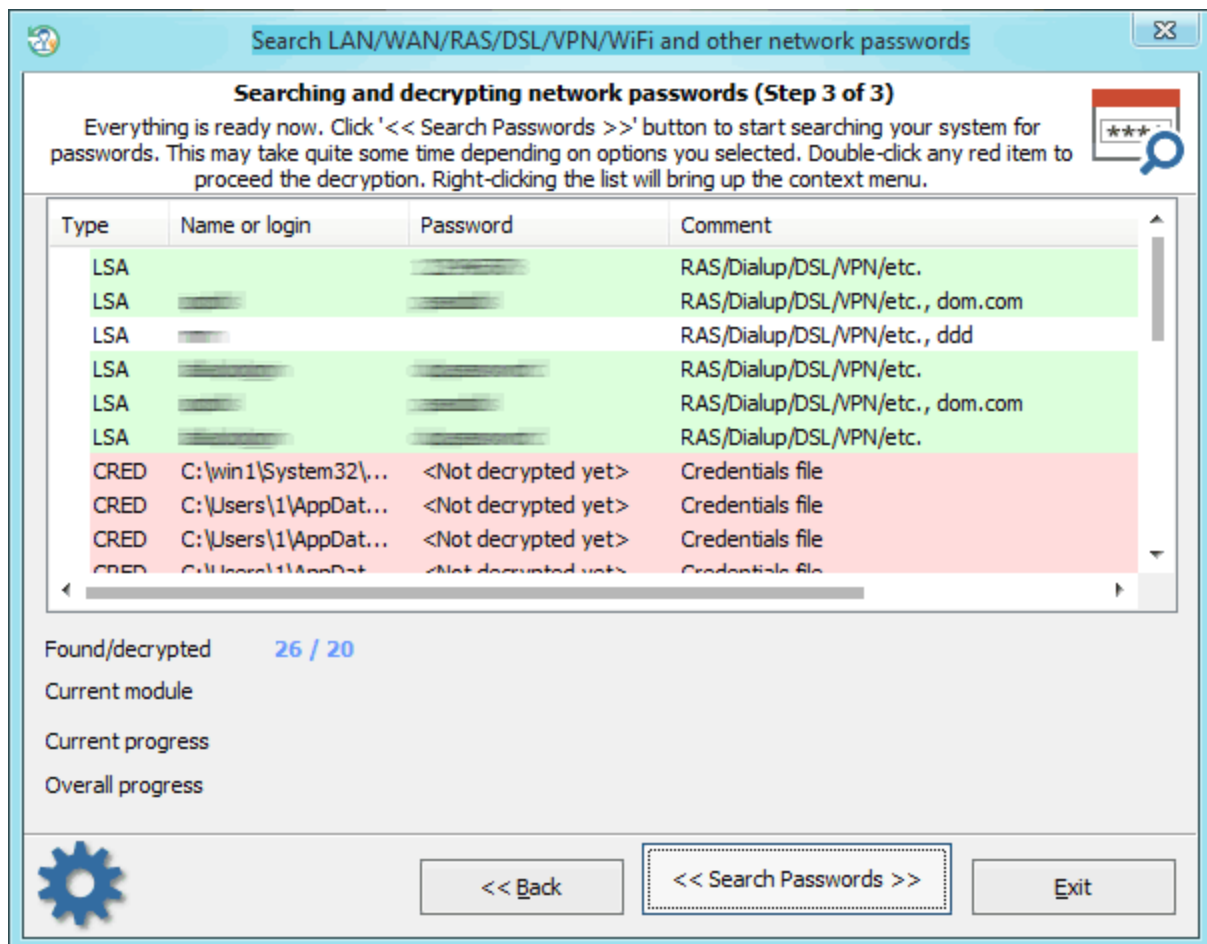


The following email clients are supported:

- Outlook Express
- Microsoft Office Outlook
- Internet Mail
- Internet Live Mail
- Windows Mail
- TheBat!
- Incredimail
- Eudora

Please keep in mind that some email passwords could be stored in browsers. This depends on whether the user used the email client or read their email using a Web browser. Passwords from Outlook Express, TheBat!, Incredimail, Eudora, and some versions of MS Office Outlook can be decrypted almost instantly. Decrypting other data requires the account password. Simply double-click on the record highlighted in red. That activates the second step of analyzing found data. If the entered user password matches the other records, they will be decoded automatically.

3.16.6.3 Search LAN/WAN/RAS/DSL/VPN/WiFi and other network passwords



For gathering network passwords, the program has several modules for reading and decrypting secrets of LSA, protected storage, password manager, Windows Vault, etc.

The decryption of data stored in LSA secrets and in the protected storage is carried out automatically and does not require entering additional parameters. This applies to the following data:

- Cached user passwords
- Passwords of some system accounts, SQL server, remote assistant, etc.
- Passwords of services launched with specific credentials
- Some network passwords stored in server OSes
- Wired connection passwords: RAS, DSL, VPN, etc
- Passwords from old versions of Internet Explorer/Outlook/Outlook Express/FTP, etc.

- Passwords for wireless (WPA/WPA2) connections
- Passwords from domain group policies
- VNC passwords
- Passwords for Tortoise SVN accounts
- Open VPN passwords
- other

For other passwords protected with DPAPI, user account password is required for the successful decryption:

- Passwords stored in Credential manager: passwords for remote computers in your LAN, passwords for some mail accounts (stored by Microsoft Outlook), MSN Messenger passwords, Internet Explorer 7-9 passwords for Web sites that use Basic Authentication or Digest Access Authentication, Remote Desktop, RSS feed credentials, etc.
- Windows Vault records: passwords for some versions of Internet Explorer/Outlook/Windows Mail, account passwords when using PIN/Picture password or biometric authentication (only for Windows 8).

More on DPAPI encryption can be found in our [detailed review](#) that covers this protection method.

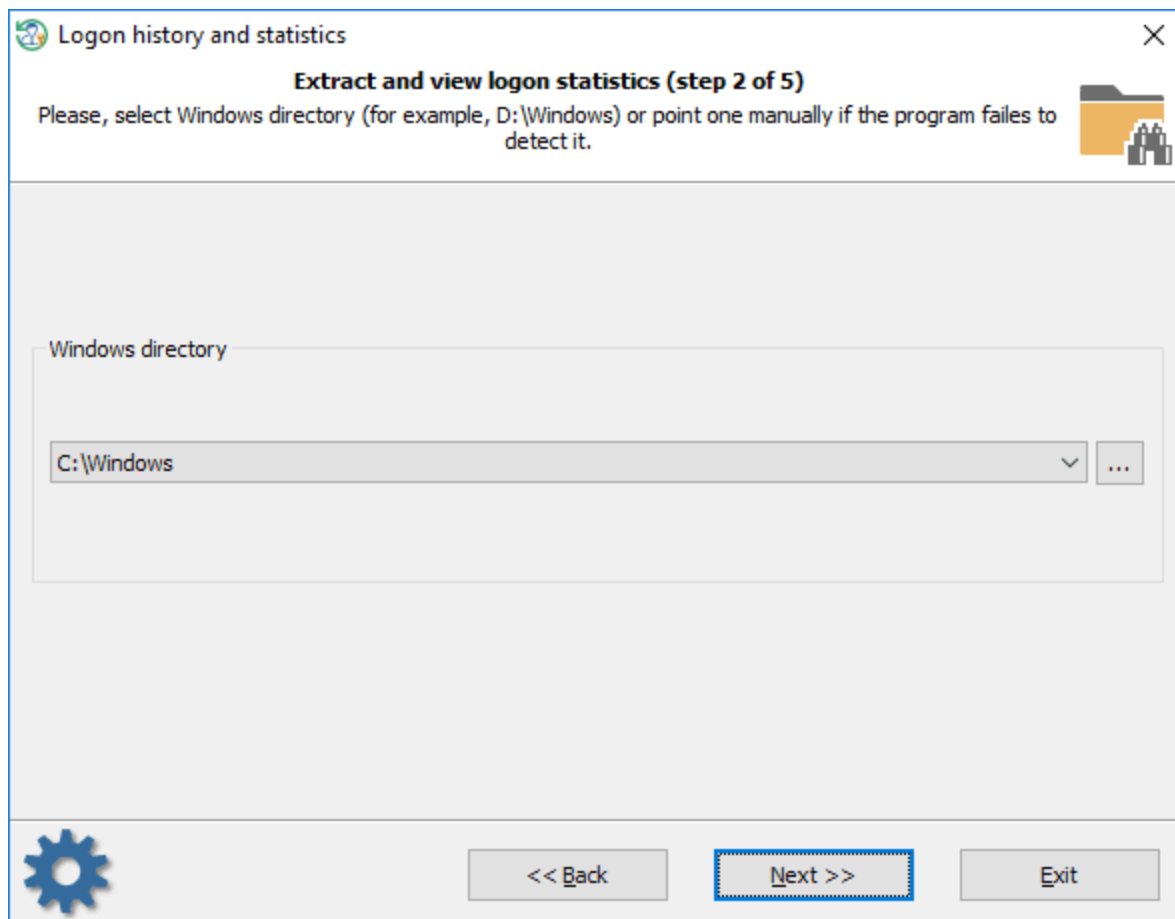
In some server operating systems, the program can successfully exploit the vulnerability we have found, which allows decrypting DPAPI blobs without entering the data owner's account password! More information on this is available in our [article that covers vulnerabilities in server OSes](#).

3.17 FORENSICS

3.17.1 View logon history and statistics

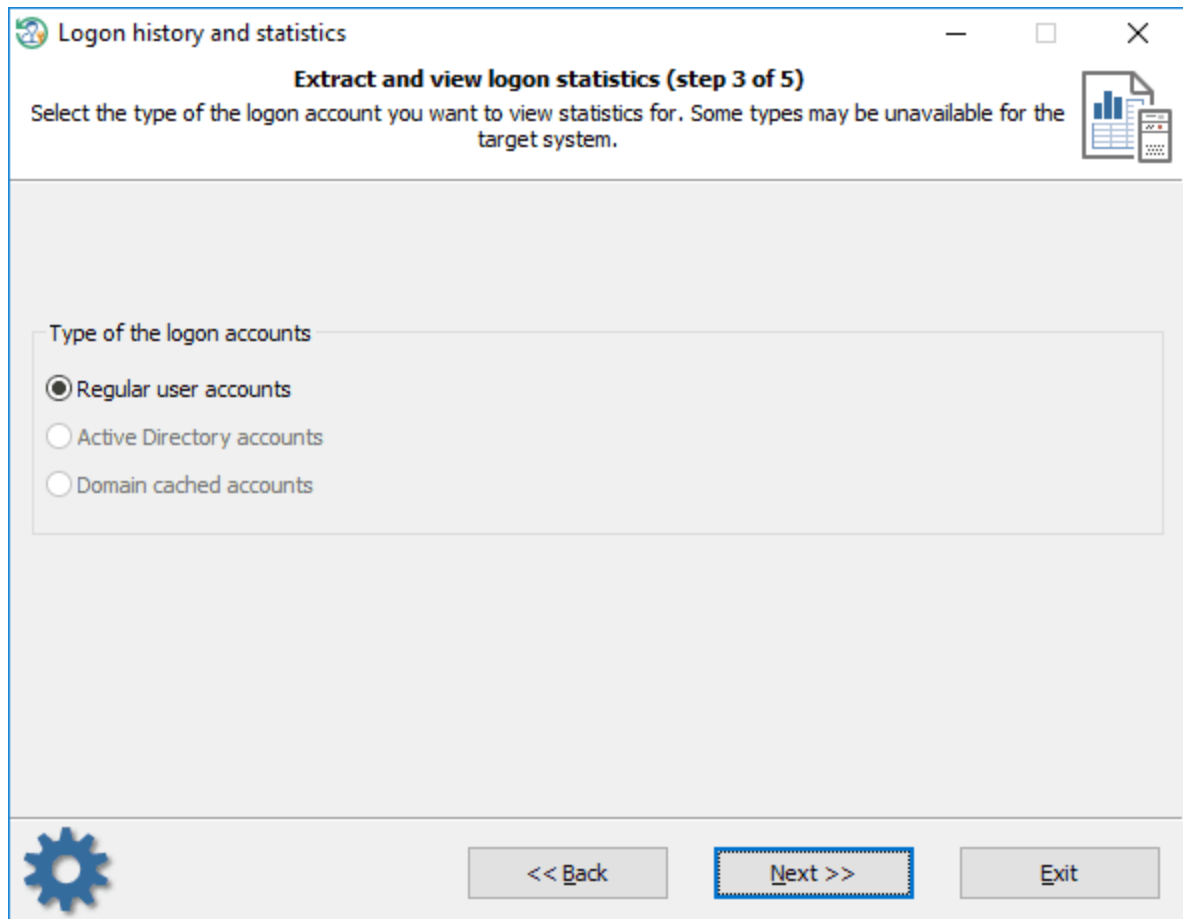
This is a tool to view miscellaneous logon statistics of both regular and domain users.

[Selecting Windows directory](#)



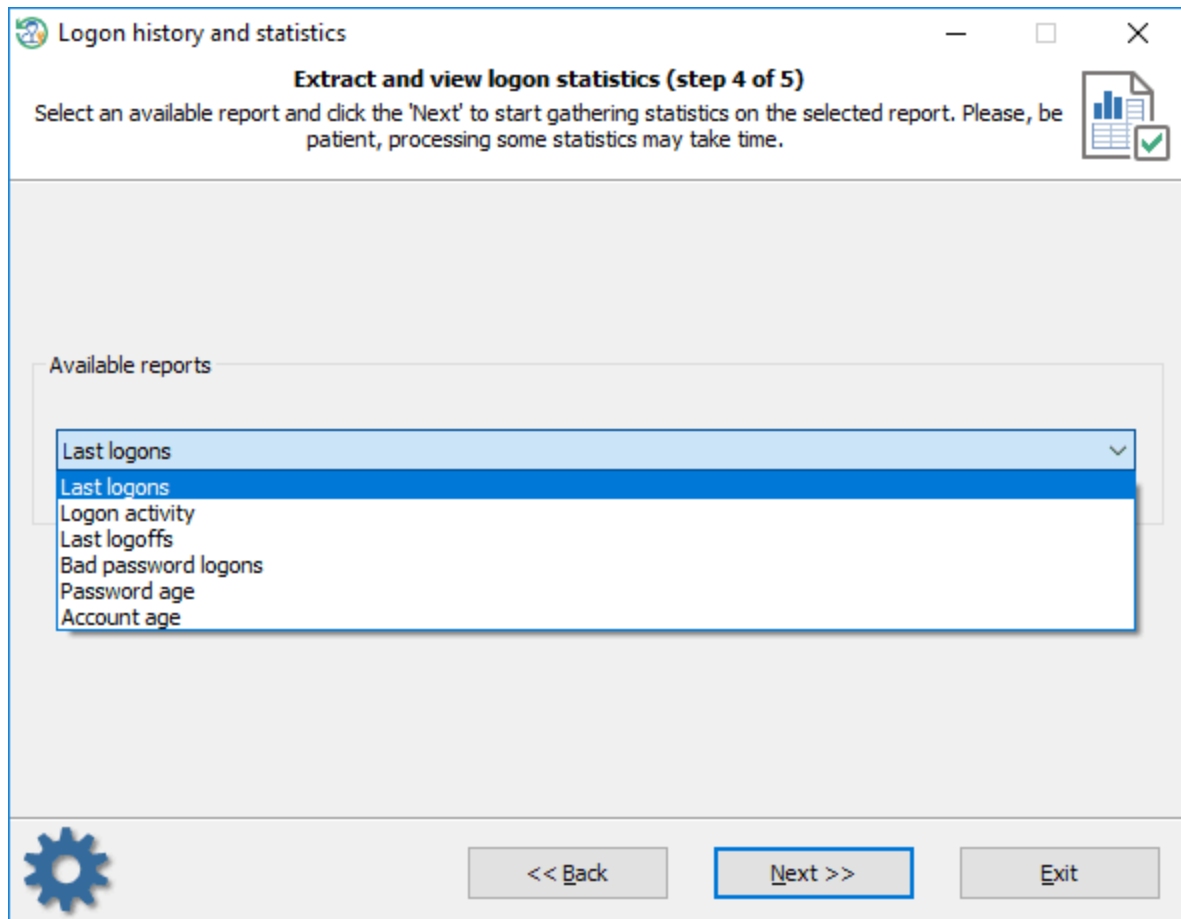
First of all, you should select a target Windows directory or browse for it if the program fails to detect one automatically.

Type of the logon accounts



Once the Windows directory is selected, the program will try to detect if the system contains any domain accounts (in addition to regular ones). Select the type of the logon accounts you want to view the statistics for and proceed to the next step.

Available reports

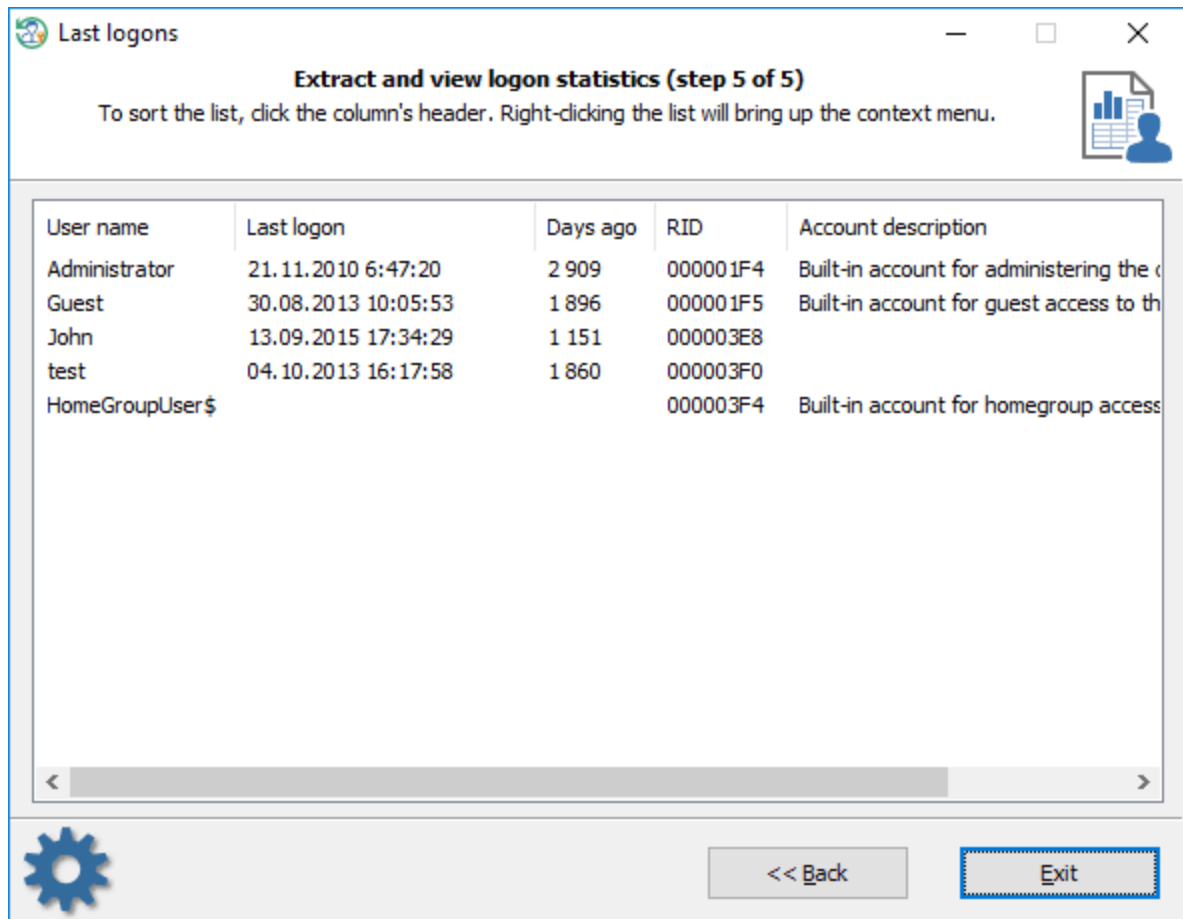


Here you can choose one of the following reports:

- Last logons - displays last logon date of the users
- Logon activity - outputs most active users
- Last logoffs - unfortunately, most versions of Windows stopped saving the logoff date. However, some related information is available in ['User activity'](#).
- Bad password logons - the last time when a user attempted to log on into his/her account with an invalid password.
- Password age - the last time when a user changed his/her password.
- Account age - when the account was created first.

Some of the reports are unavailable for domain cached accounts.

Logon statistics

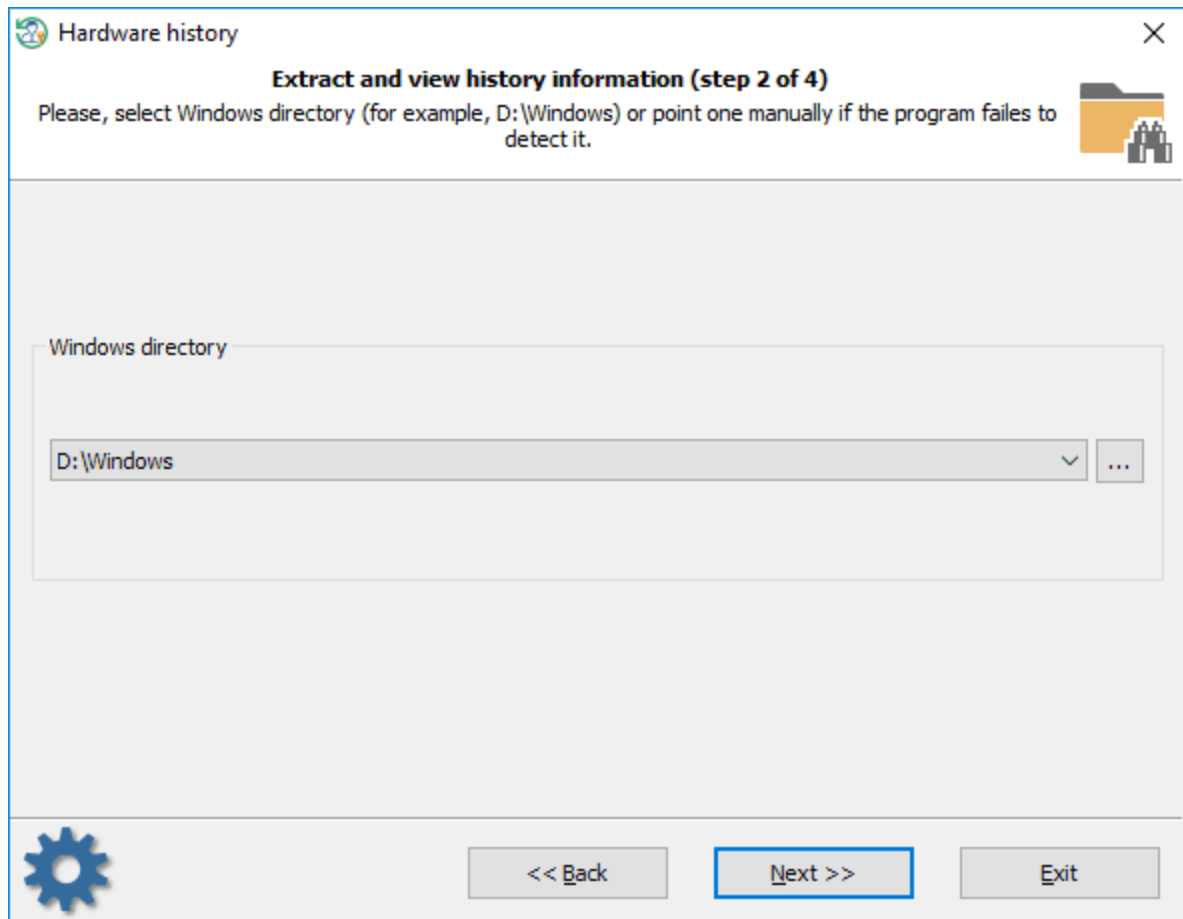


You can copy statistics to the clipboard or save it to file.

3.17.2 View hardware history

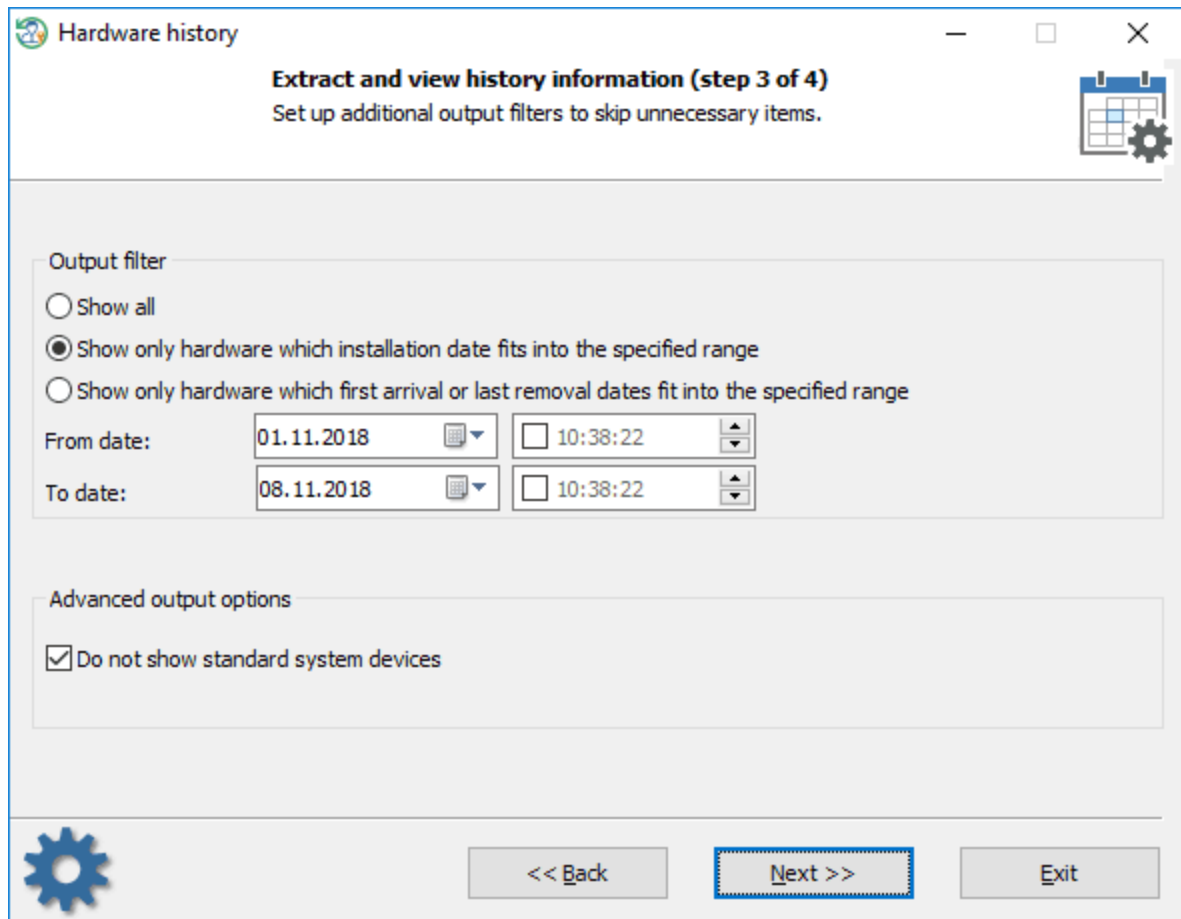
The hardware history enumerates all hardware of the target OS and sorts it by installation or last arrival/removal date.

Selecting Windows directory



Select the target Windows folder first. The program usually does it automatically.

Select output filters



Hardware history

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.

Output filter

☐ Show all

☒ Show only hardware which installation date fits into the specified range

☐ Show only hardware which first arrival or last removal dates fit into the specified range

From date: 01.11.2018 10:38:22

To date: 08.11.2018 10:38:22

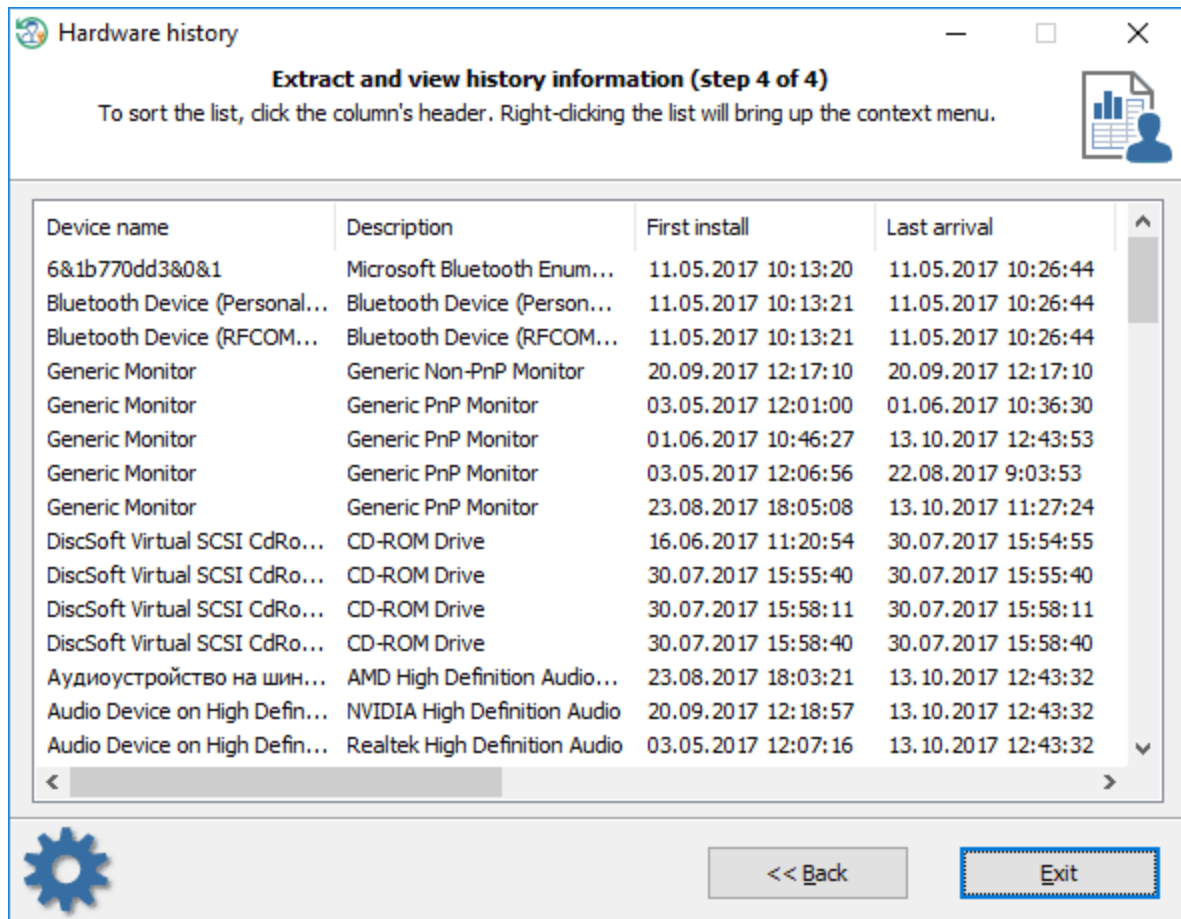
Advanced output options

☒ Do not show standard system devices

<< Back Next >> Exit

Set up additional output filters to skip unnecessary items. You can set the program up so that to display only hardware that was installed or arrived/removed last time on the date you specified.

Hardware history information

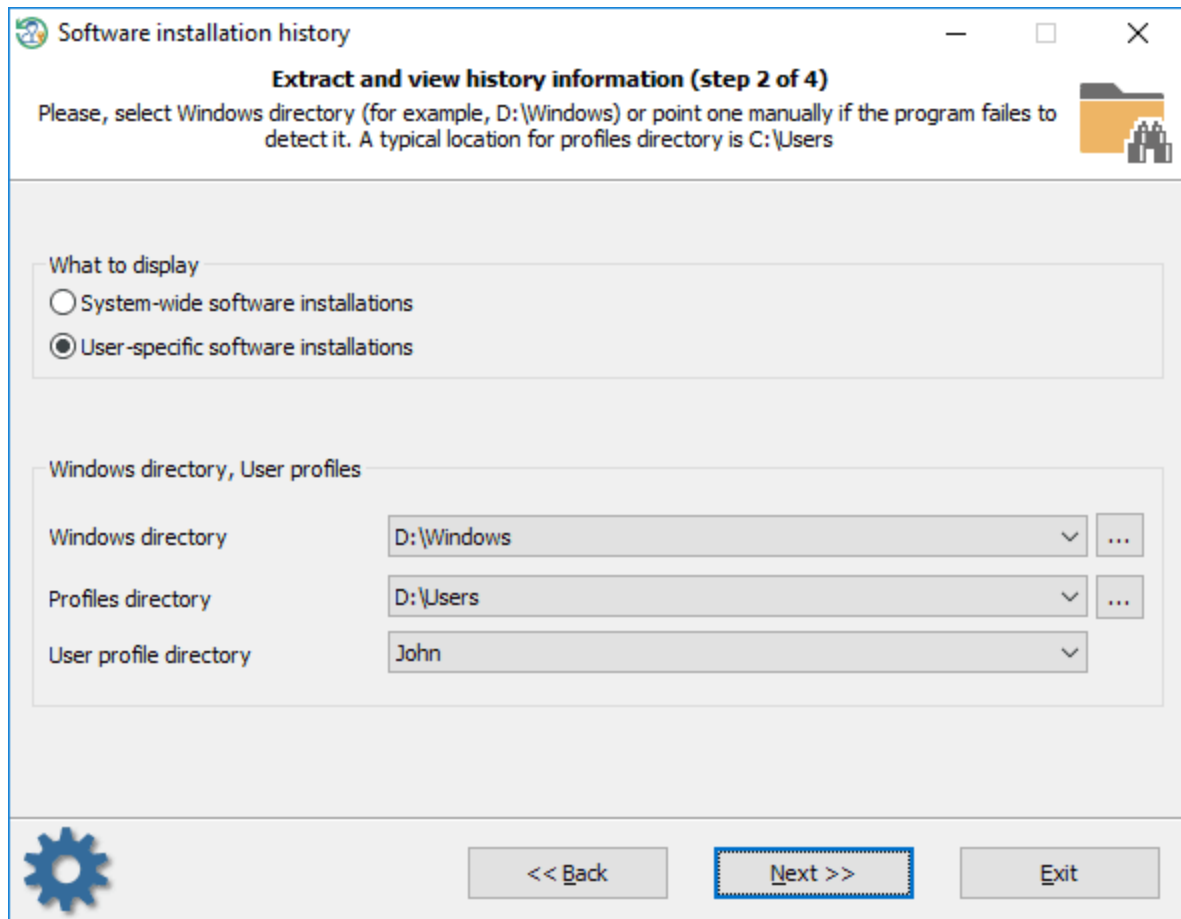


To sort the list, click one of the columns.

3.17.3 View software history

The software history displays all the programs that were installed in the target OS.

Selecting a type of software installations



Select what type of the software installations you want to view. This is either user specific installations (programs installed for a certain user account) or system-wide installations (programs that are available for all users).

Output filters

Software installation history

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.

Output filter

☒ Show all
☐ Show items created between given dates only

From date: 08.11.2018 11:22:44
To date: 08.11.2018 11:22:44

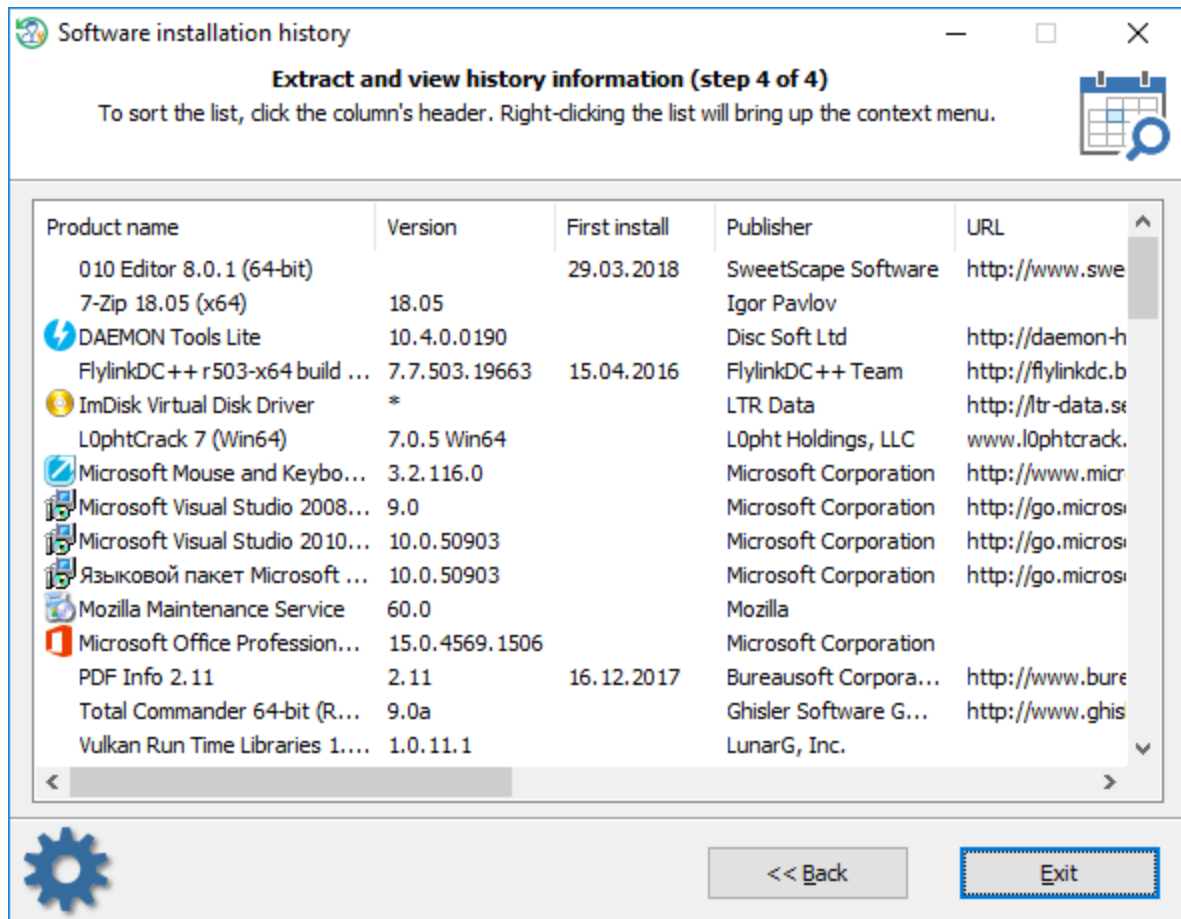
Advanced output options

☒ Do not show system components

<< Back Next >> Exit

You can point the program to display all items or items that were created between given dates only. The additional option is aimed to hide some system components, like system updates, etc.

Software installations

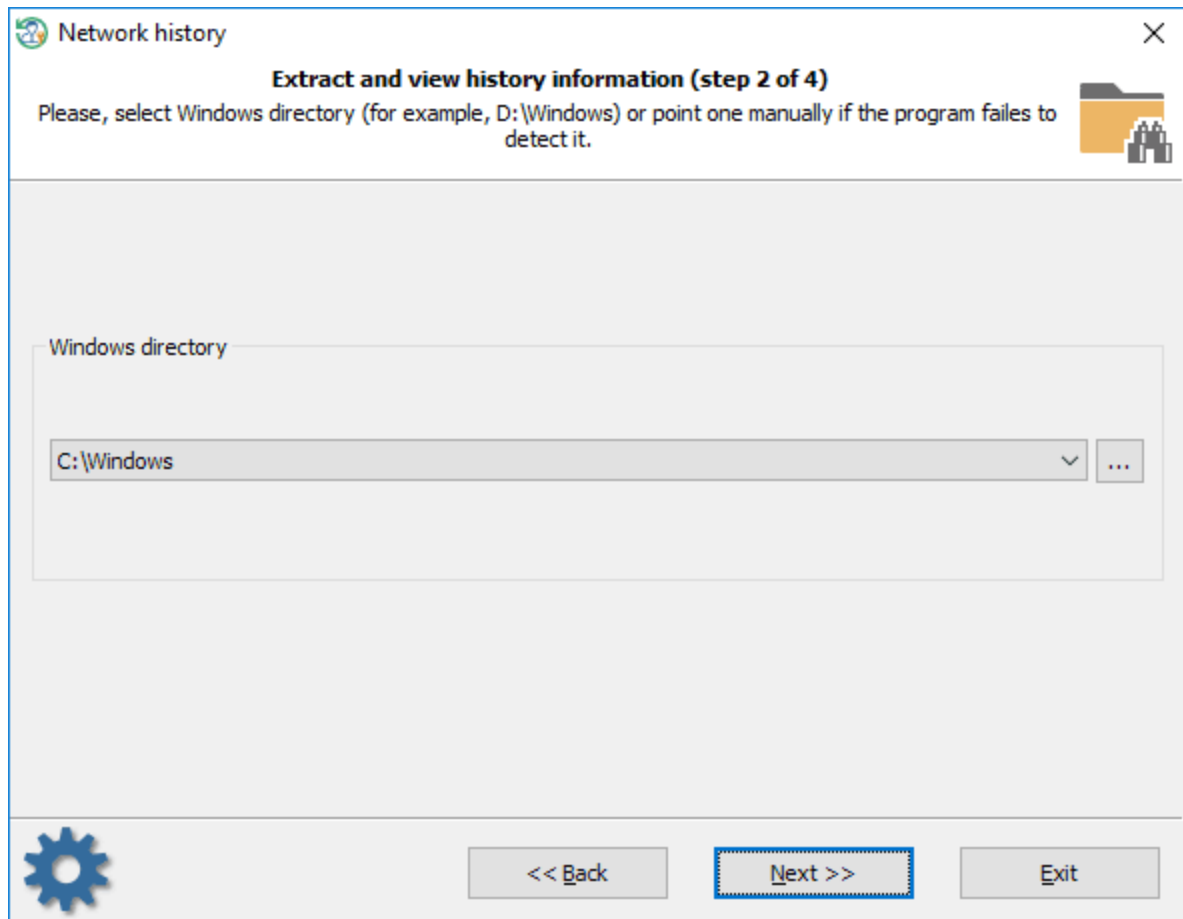


To sort the list click one of the columns.

3.17.4 View network history

The network connection history displays all available networks along with their installation and last connection dates.

Selecting Windows directory



Select the target Windows folder first. The program should do it for you.

Setting output filters

Network history

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.

Output filter

☒ Show all

☐ Show networks which creation date fits into the specified range

☐ Show networks which last connection date fits into the specified range

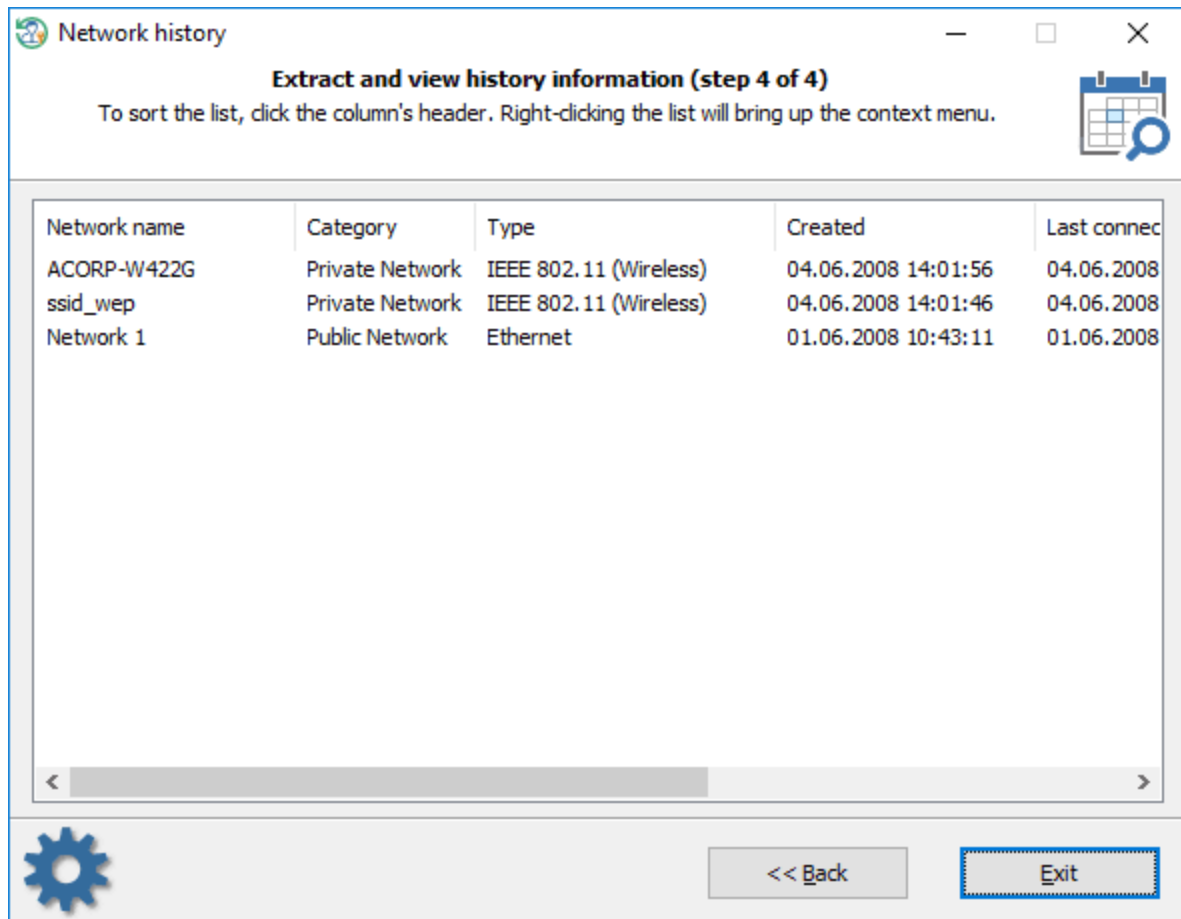
From date: 08.11.2018 11:45:55

To date: 08.11.2018 11:45:55

<< Back Next >> Exit

Set up additional output filters to display only networks of your interest.

Network connection history



The extracted networks usually contain the date they were created at and the last connection date. To sort the list by dates, click one of the correspondent column.

3.17.5 View recent user activity

This tool collects all available information about recent user activity occurred on this computer.

Selecting a type of activity

Recent user activity

Extract and view history information (step 2 of 4)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it. A typical location for profiles directory is C:\Users

What to display

☐ System-wide data

☒ User-specific data

Windows directory, User profiles

Windows directory: D:\Windows

Profiles directory: D:\Users

User profile directory: John

<< Back Next >> Exit

First of all, select if you want to view system-wide or user-specific data.

Setting output filters

Recent user activity

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.

Output filter

☐ Show all

☒ Show items which last modification date fits into the specified range

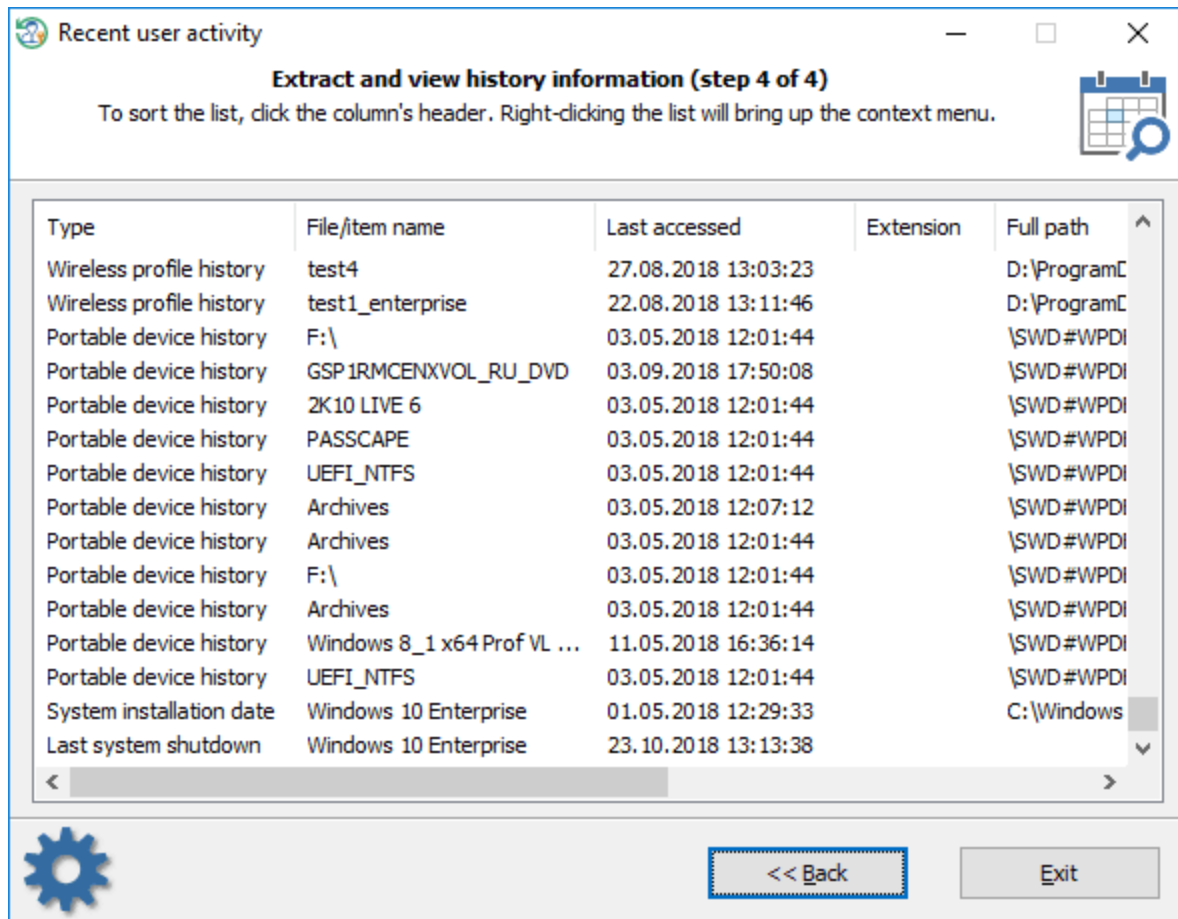
From date: 01.01.2018 16:14:56

To date: 31.10.2018 16:14:56

<< Back Next >> Exit

Then specify if all entries are to be displayed or only ones that fit into specific time frames.

Displaying recent user activity



Be patient, gathering the statistics may take quite some time.

To hide unnecessary record(s), right-click your mouse on the list and select the appropriate menu item.

The current version of the program supports for the following information (some items are not available in old OSes):

- Last items in file open/save dialogs
- Task Run items
- Mapped network drives
- Recent network find items
- Recent file/folder find items
- Recent files of Windows applets
- Last opened Regedit key
- Recently opened documents
- Recently opened MS Office documents
- Recent Outlook accounts and connections
- Recently run applications
- Recent application items
- Recent RDP connections
- Internet Explorer typed URLs
- Explorer typed paths
- Explorer search history
- Explorer User Assist items
- Recent background activity items
- Recent desktop activity items

- Wireless connections
- Bluetooth activity
- Recent portable devices
- Windows installation date
- Last system shutdown date

3.17.6 Search for recently opened documents

Windows OS keeps track of all opened documents and saves links to them to a Microsoft Windows-specific ('Recent') folder in the user profile. 'C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent' is a special folder, where Windows stores the links to recently used documents. You can control the Windows behavior at Start Menu > Settings > Personalization > Start, by toggling the 'Show recently opened items' option.

This program's feature is aimed to browse through the recent file list and view the names of the files that have been opened recently and saved to the Windows 'Recent' folder.

Selecting user profile

Search for recently opened documents

Searching for recent documents (step 2 of 3)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it. A typical location for profiles directory is C:\Users

What to display

☐ System-wide data

☒ User-specific data

Windows directory, User profiles

Windows directory: D:\Windows

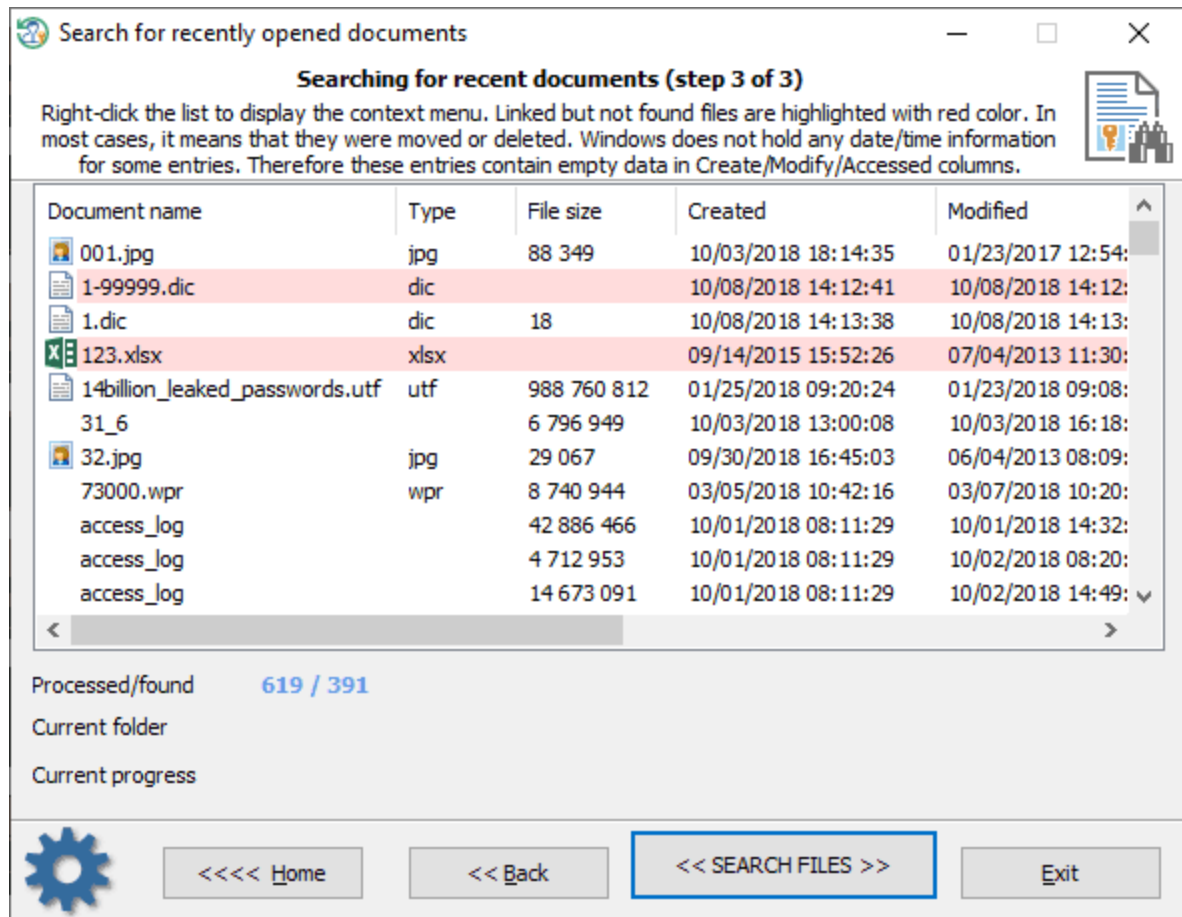
Profiles directory: D:\Users

User profile directory: John

<<<< Home << Back **Next >>** Exit

Select the user profile whose documents you want to analyze.

View recently opened documents



Click the << SEARCH FILES >> button and wait patiently until the program finds the last opened files and fills in the table.

In order to hide the unnecessary items, right-click on the list of found files and select the appropriate menu.

Files that no longer exist (for example, were moved or deleted) but still have links to them are marked with red color.

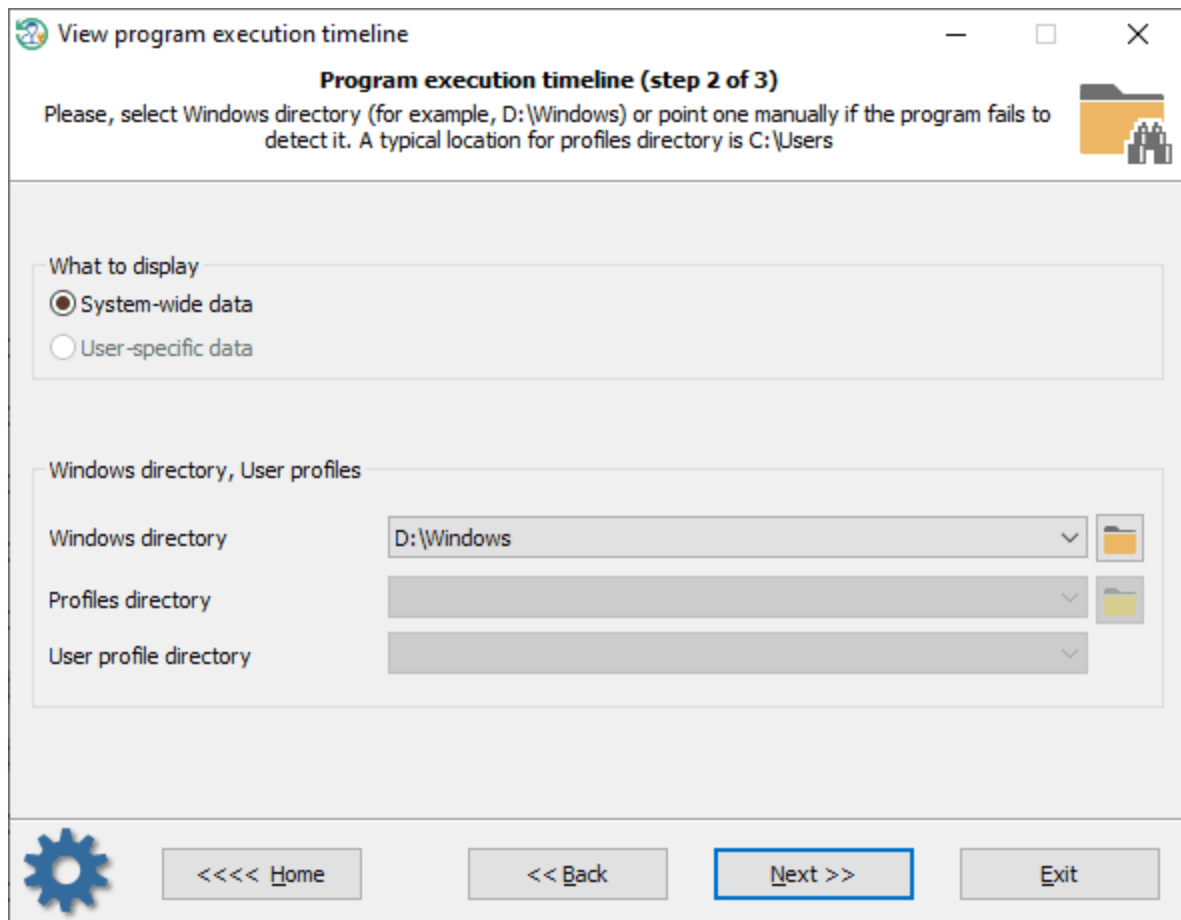
3.17.7 View program execution timeline

It would not be a big surprise to know that there are a lot of artifacts that contain information about recently opened documents or launched files in Windows. The AmCache is one of them which stores data about every program that has been started or installed in the system earlier. The AmCache is available starting with Windows 7. Older operating systems use a BCF format to save data about

executed programs. Physically, both formats are simple files located in the %WINDIR%\appcompat\Programs folder. The AmCache.hve is a registry hive that provides a timeline of which program was executed and when, while the RecentFileCache.bcf stands for a simple Binary Cache File.

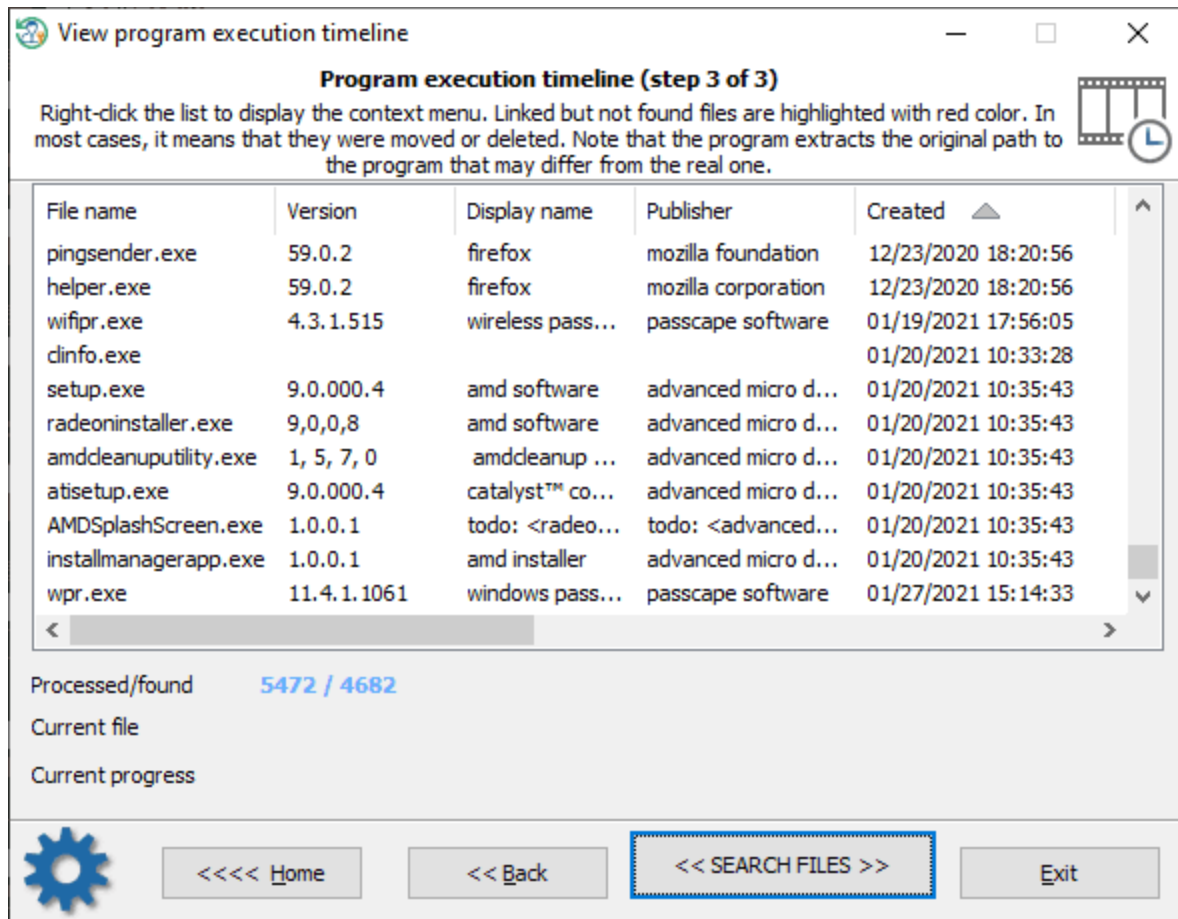
The program supports both formats, however the old BCF format contains no information about the execution time.

Choosing Windows directory



Select the Windows directory detected by the program.

View program execution timeline



Now it's time to hit the << SEARCH FILES >> button and wait for the program to locate the files to fill in the table.

In order to wipe out any unnecessary file from the list of found items, right-click the list and select the appropriate menu.

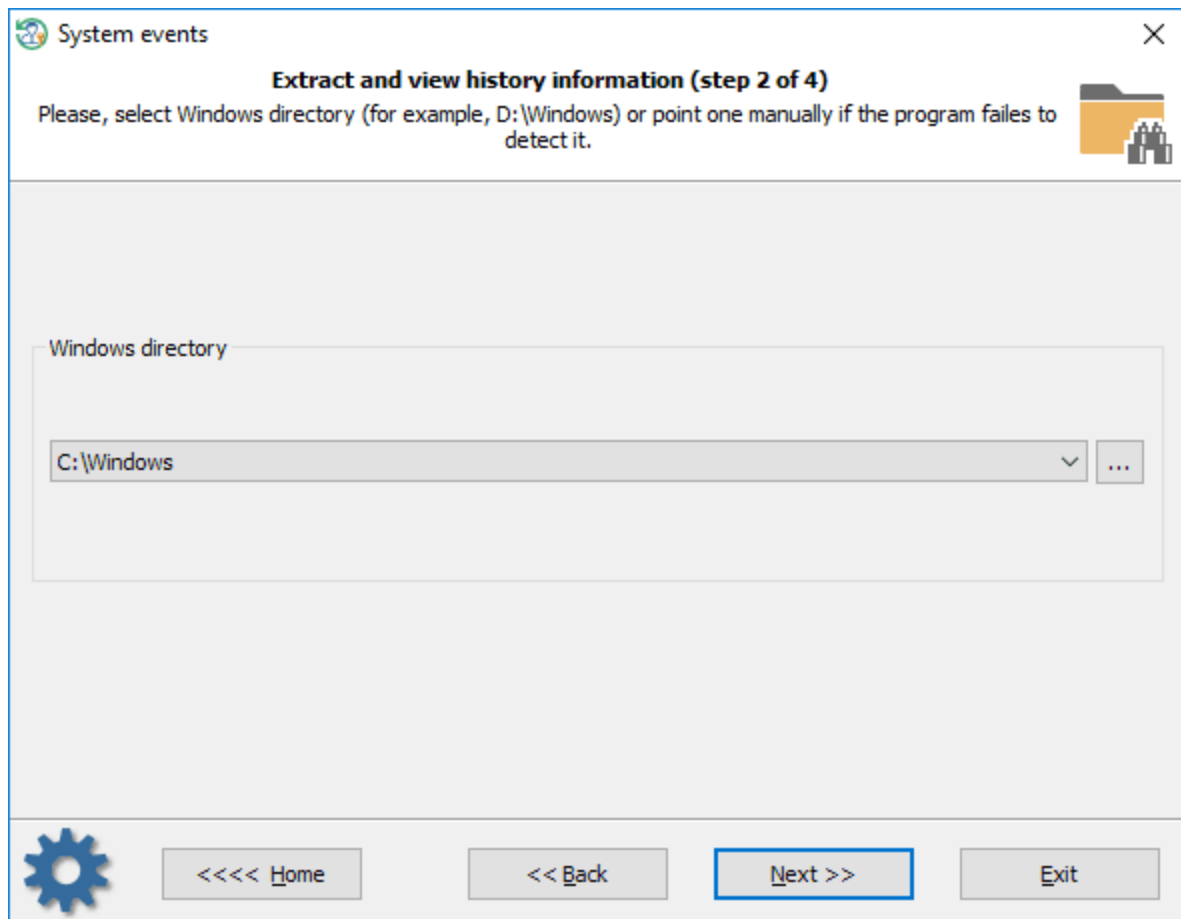
If the program fails to locate files Windows links to from within the AmCache database, it marks the files with red color.

3.17.8 View system events

All Windows OSes log various types of events that occur in the system time to time: errors in device or driver installations, application failures, security notifications, etc. Events help users and administrators to eliminate errors, perform diagnostics and monitoring the system, maintain its security. Events are stored in *.evtx files and are recorded in chronological order. Every evtx file corresponds to a specific event source or to an operating system component. For example, system.evtx keeps tracking of common system notifications. Security.evtx holds all security events. And so on.

The system event viewer is a simple tool allowing to display major events that occur in Windows Vista and later OSes. For example, starting or shutting down the system, logging on/off user accounts, drivers installation, etc.

Selecting Windows directory



First, you must select the Windows directory that holds the event logs. Typically, C:\Windows or D:\Windows.

Setting output filters

System events

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.

Output filter

☒ Show all
☐ Show items which last modification date fits into the specified range

From date: 23.01.2019 11:30:46
To date: 23.01.2019 11:30:46

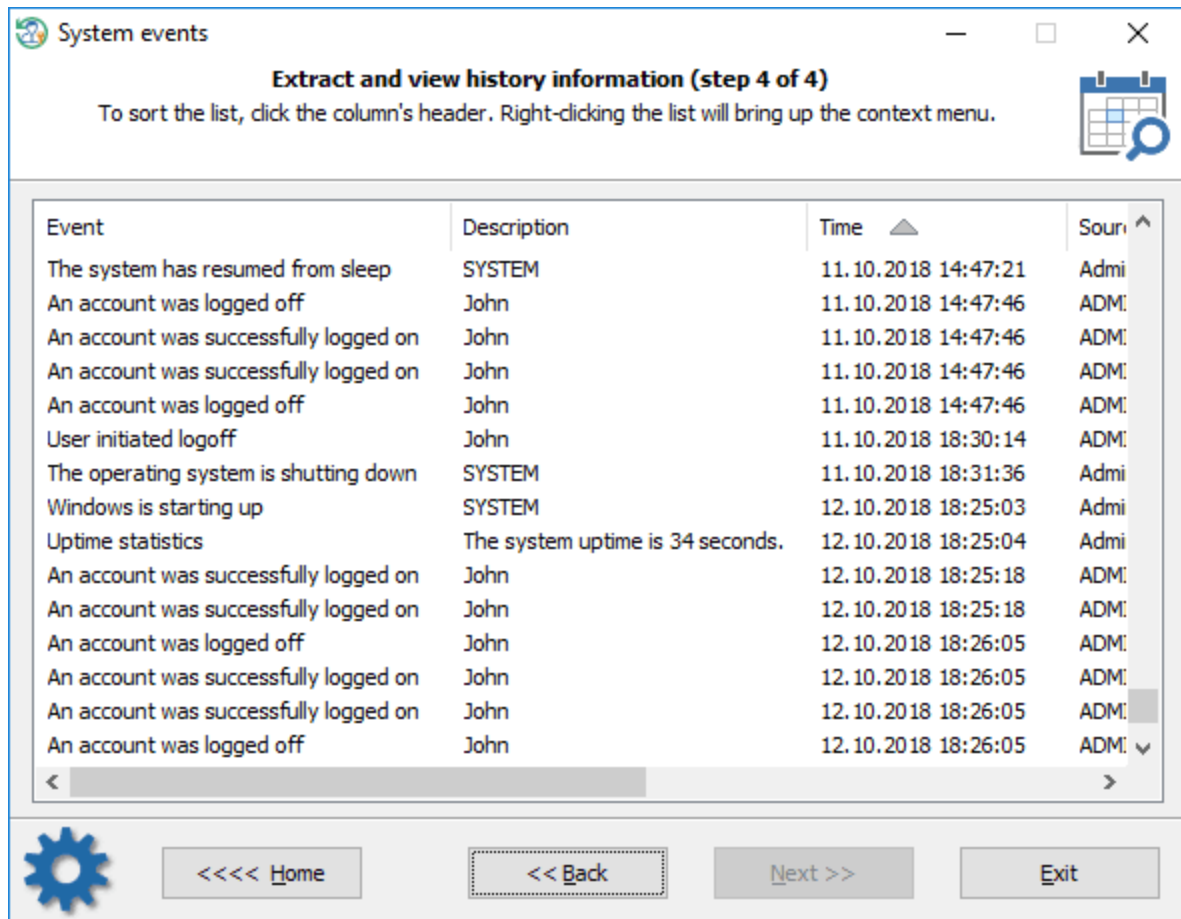
Advanced output options

☒ Show major events only (recommended)

Home <<<< << Back Next >> Exit

On the next step, you can additionally configure output filters to display events that occurred in specific time. There's also an option for displaying all events (even unknown to the program). If the option is set, the program outputs known/major events only, all events otherwise.

Viewing Windows events

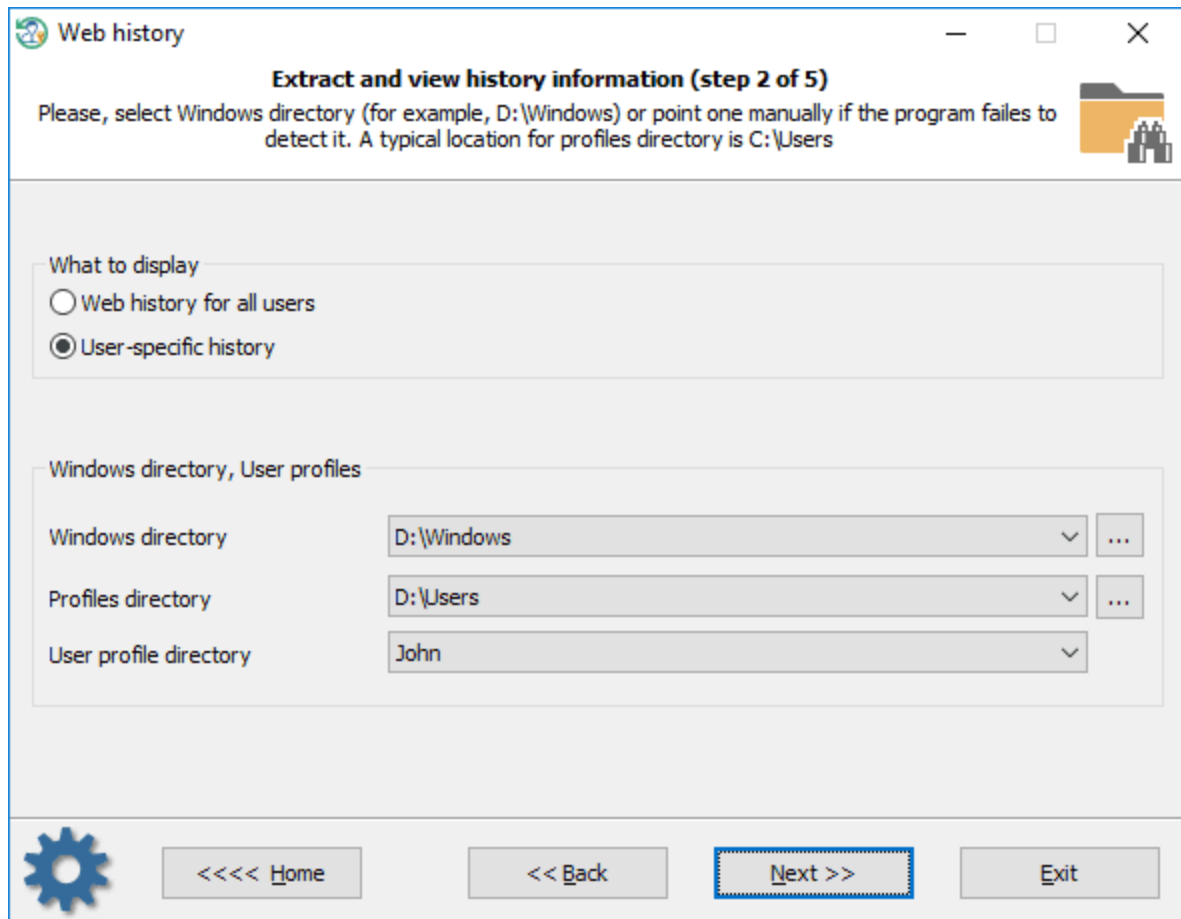


Collecting and processing the information may take considerable time, depending on the size of *.evtx files of the target system. In order to hide some certain records that are of no interest to you, right-click on the list of events and select one of the corresponding menu items. To sort the list, click one of its headers.

3.17.9 View web history

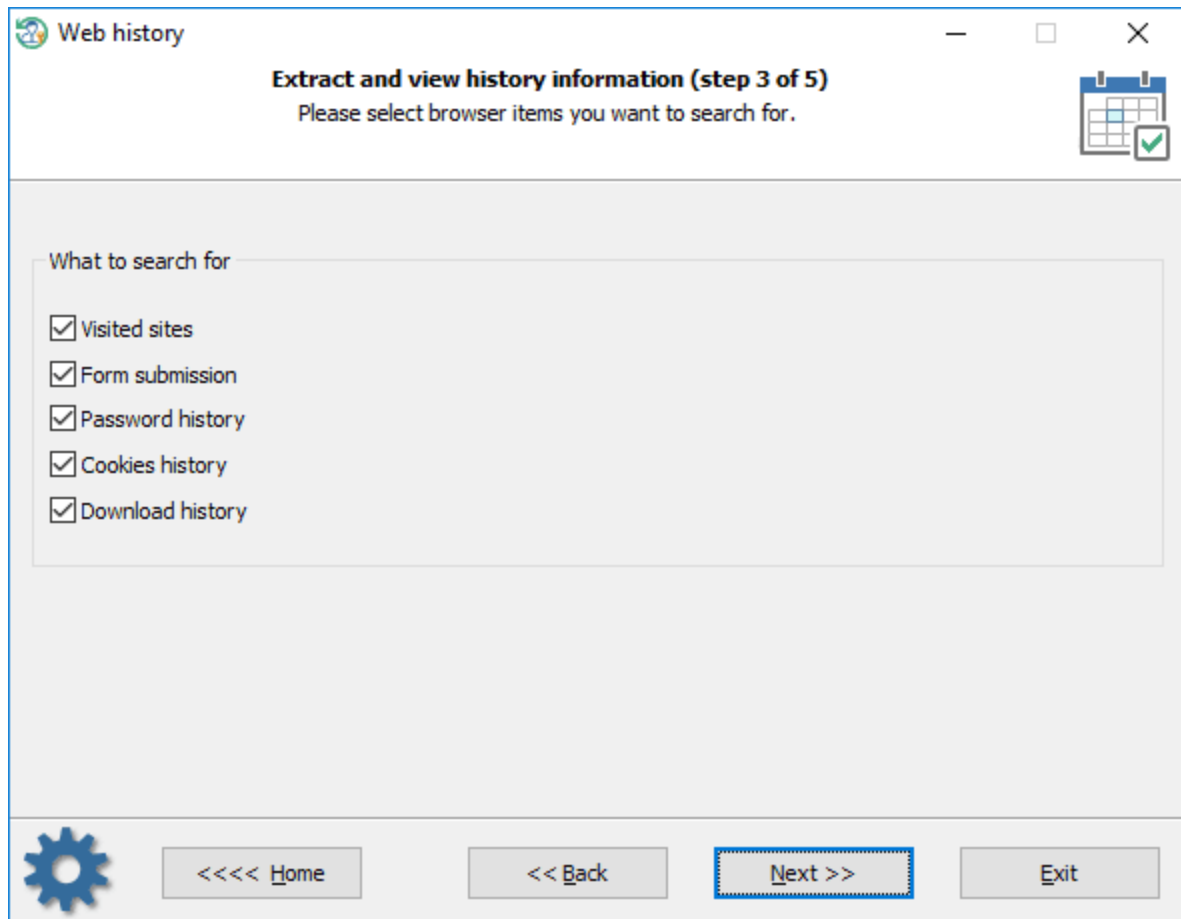
The Web history allows you to extract and collect statistics of visited Web pages, saved cookies, stored form autocompletion data and saved passwords. The program supports all popular browsers: Internet Explorer, Edge, Opera, browsers based on Mozilla source code (Firefox, SeaMonkey, etc.), Chromium (Google Chrome, YandexBrowser, 360 Extreme Explorer, etc.)

Selecting data source



Initially, RWP offers to select the data source where to search. This is either a specific user's profile or profiles for all users.

What to search for



By default, the program tries to search for the following items, you can turn on/off each of them separately:

- The list of visited URLs
- Form auto-completion data
- Logon names and passwords (if ones can be decrypted instantly only)
- Cookies. May be used for determining what sites were visited and when, whether the user was logged in and so on
- Download history. Note that not all browser keep this information

Setting up time filters

Web history

Extract and view history information (step 4 of 5)
Set up additional output filters to skip unnecessary items.

Output filter

☒ Show all

☐ Show items which last modification date fits into the specified range

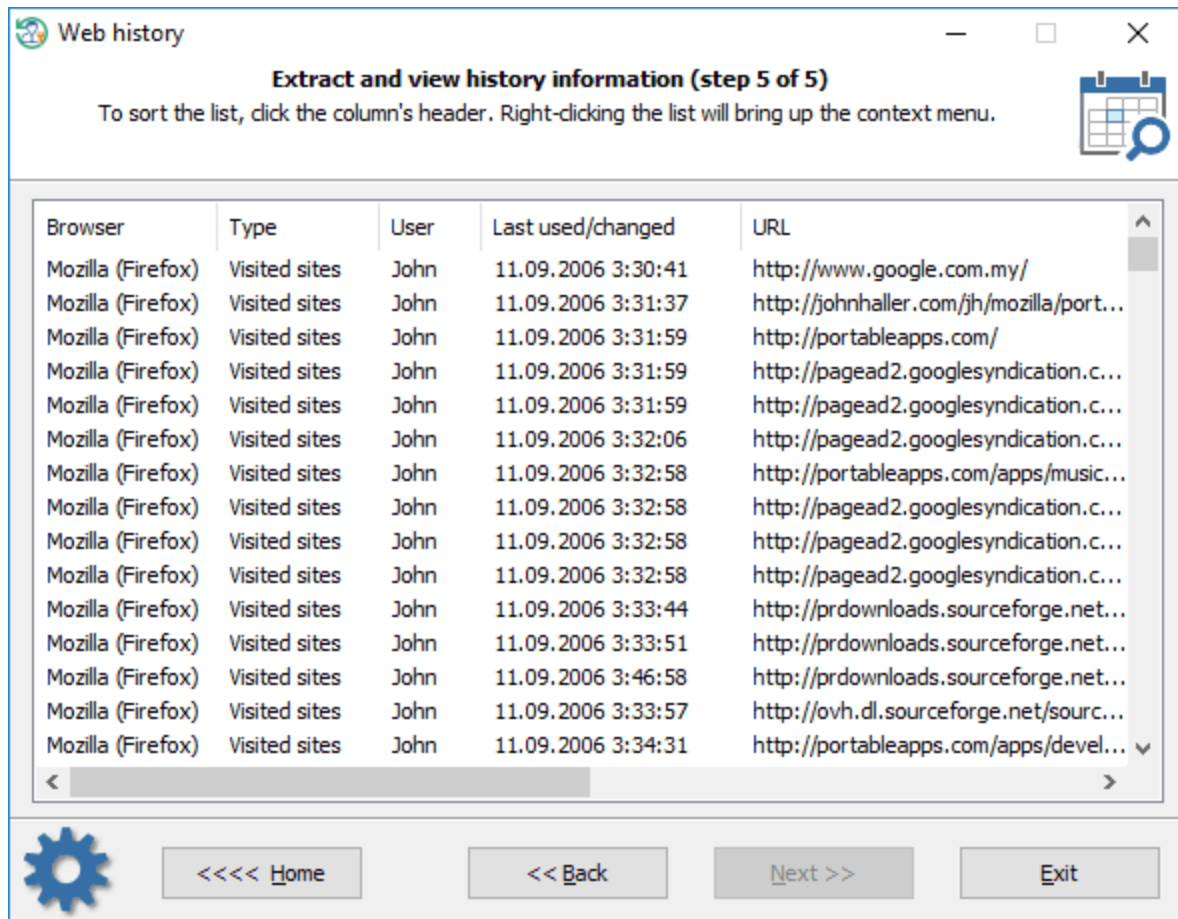
From date: 11.03.2019 16:14:25

To date: 11.03.2019 16:14:25

Home Back Next >> Exit

You can set up an additional time filter to skip out-dated or unnecessary items.

Web history



Browser	Type	User	Last used/changed	URL
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:30:41	http://www.google.com.my/
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:31:37	http://johnhaller.com/jh/mozilla/port...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:31:59	http://portableapps.com/
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:31:59	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:31:59	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:06	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:58	http://portableapps.com/apps/music...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:58	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:58	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:32:58	http://pagead2.googlesyndication.c...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:33:44	http://prdownloads.sourceforge.net...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:33:51	http://prdownloads.sourceforge.net...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:46:58	http://prdownloads.sourceforge.net...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:33:57	http://ovh.dl.sourceforge.net/sourc...
Mozilla (Firefox)	Visited sites	John	11.09.2006 3:34:31	http://portableapps.com/apps/devel...

The statistics can be copied to the clipboard or saved to a file. Using the context menu, you can also hide some items that are not of interest to you.

Where do browsers store their lists of visited URLs?

Internet Explorer

Visited places are stored in index.dat file. The index.dat contains different records: visited URLs and local files, web mail accesses, cookies, etc. The database file has its own format (Client UrlCache MMF) and was first introduced in Internet Explorer 5. The format of index.dat file was not changed much since that time, the physical location, however, may vary:

C:\Users\<USERNAME>\AppData\Local\Microsoft\History

C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\History

C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Internet Explorer\UserData

Older OSes use different paths to keep the file.

Internet Explorer - typed in URLs

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Microsoft Edge

Similar to Internet Explorer, Microsoft Edge keeps the history of the Web browsing, cache, cookies, along with other information in a single file called WebCacheV01.dat which seems to be the successor of the index.dat. The WebCacheV01.dat is located at the following path:
C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\WebCache

Opera (older versions)

The browser history is kept in global_history.dat, global.dat, vlink4.dat files in the current Opera's profile. The files have a different format (depends on browser version).

Chrome (along with Chromium-based browsers)

All visited URLs are kept in SQLite database called history. The location of the history is different and depends on the browser. For example:

C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (along with Mozilla-based browsers)

This is either a history.dat file (a mork format) or a places.sqlite file in newer versions. A typical location is C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles. For example:

C:\Users\<USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default

Where do browsers store the form autocompletion data?

Internet Explorer

Internet Explorer v4-6 keep autocompletion data in a special location of the user registry called protected storage. Even though encrypted, it is [easy to decrypt and view](#) because decryption keys are stored along with encrypted data. The registry location of the storage provider:

HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Internet Explorer v7-9 use a different and interesting technique. Instead of encrypting user-sensitive data with a static secret key (IE 4-6) which can be figured out easily, IE 7-9 use the source URL address as the encryption key to protect the data. Thus without knowing the Web page a certain data belong to, you will not be able to decrypt the data. More details can be found [here](#). RWP does not support extracting IE 7-9 form autocompletion data. Use our PIEPR for that. Here's the registry location where the encrypted data is stored:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\FormData

Internet Explorer v10+ and Microsoft Edge have even better protection. All data entries are kept in [Windows Vault](#) files and protected with [DPAPI](#). There's no chance to decrypt it unless providing the owner logon password and master key file.

A tricky part is that RWP can decrypt the data/passwords instantly if the browser has saved it under the system account. The Vault location for the user data:

C:\Users\<USERNAME>\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Opera (older versions)

The form autocompletion data can be found in the following files:

C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\typed_history.xml

C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\search_field_history.dat

Chrome (and Chromium-based browsers)

The form submission data is kept in history and Web Data files, both have SQLite format. A typical location for the Chrome browser is:

C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (and Mozilla-based browsers)

This is either a formhistory.dat file (older versions of the browser) or formhistory.sqlite file. A typical location is C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles. Like this:

C:\Users\<USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default\formhistory.sqlite

Where do browsers store their passwords?

Internet Explorer

Internet Explorer v4-6 keep Web passwords in the protected storage.

HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Internet Explorer v7-9 passwords are kept in the following registry key:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

Internet Explorer v10 default location for the saved passwords:

C:\Users\<USERNAME>\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Some versions of IE can also save HTTP basic authentication passwords in the 'Credentials store' (Windows Vista and higher OSes). The DPAPI is used to protect the entries there.

C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Credentials

The program is smart enough to extract some extra data stored in other locations. For example, the Reset Windows Password can parse Chrome databases to look for Internet Explorer items that are kept there after data migration.

Opera (older versions)

All passwords are stored in wand.dat file in encrypted form along with decryption keys. The passwords can easily be decrypted unless a Master password is set.

C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\wand.dat

Chrome (and Chromium-based browsers)

Chromium-based browsers protect user passwords with DPAPI in Windows and store them in Login Data file which actually is an SQLite database. A typical database location for Google Chrome:

C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default>Login data

Firefox (and Mozilla-based browsers)

Mozilla had a long way evolving the password storage format. Initially, it was a simple textual file signons.txt. Then in version 2 it came signons2.txt which had the "#2c" prefix at the beginning of the file. Then signons3.txt with the "#2d" prefix in version 3, etc. Next the signons.sqlite database came into a play. But it's not the end of the story. Firefox v32.x and higher has new storage for passwords - logins.json which is actually a JSON format file. In spite of apparent diversity, data protection is almost the same.

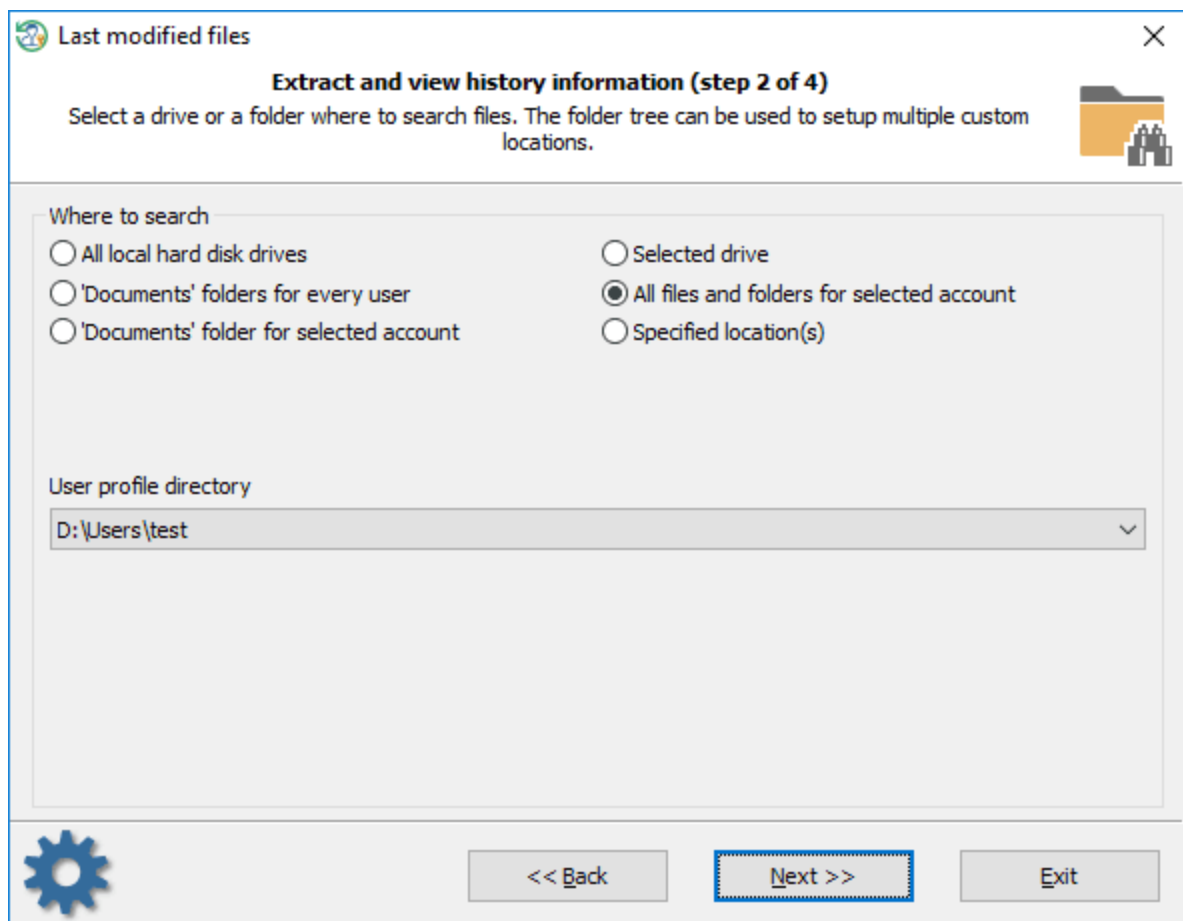
A typical location for the files is:

C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles\<PROFILE>.

3.17.10 View last modified files

Sometimes it is required to figure out what files or folders were created or modified in a certain time. This is what this tool was created for. We tried to make it as simple as possible. All you need is to set the search location and to specify the time range for the sought files/folders.

Setting search location



To point the program the starting point for the files to search, select one of some predefined values like documents folder of a certain user, the whole user's profile, etc. You can also specify your own location by setting a custom path or a hard drive.

Setting the time range

Last modified files

Extract and view history information (step 3 of 4)
Set up additional output filters to skip unnecessary items.

Output filter

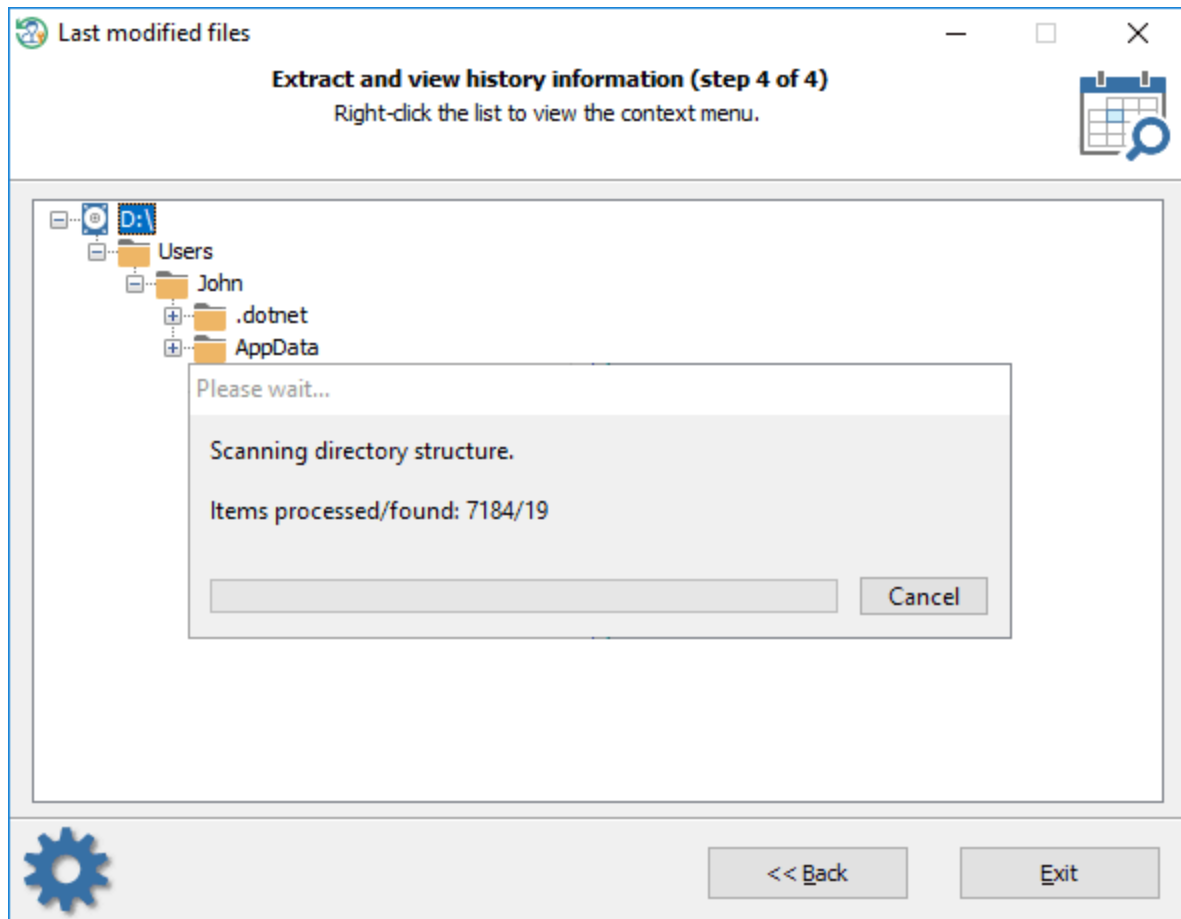
☒ Show files/folders with the creation date that fit into the specified range
☐ Show files/folders with the last modification date that fit into the specified range

From date: 01.10.2018 0:00:00
To date: 05.10.2018 23:59:59

<< Back Next >> Exit

Specify here if you need to search for files/folders with a certain creation date or a modification date. You can set up the time up to seconds or turn the seconds off completely.

Displaying last modified files



Be patient, searching may take quite a lot of time.

3.17.11 View last modified directories

This tool behaves exactly like the previous one except that it searches for the folders instead of files. Please, refer to the [file search tool](#) for more information.

3.18 UTILS

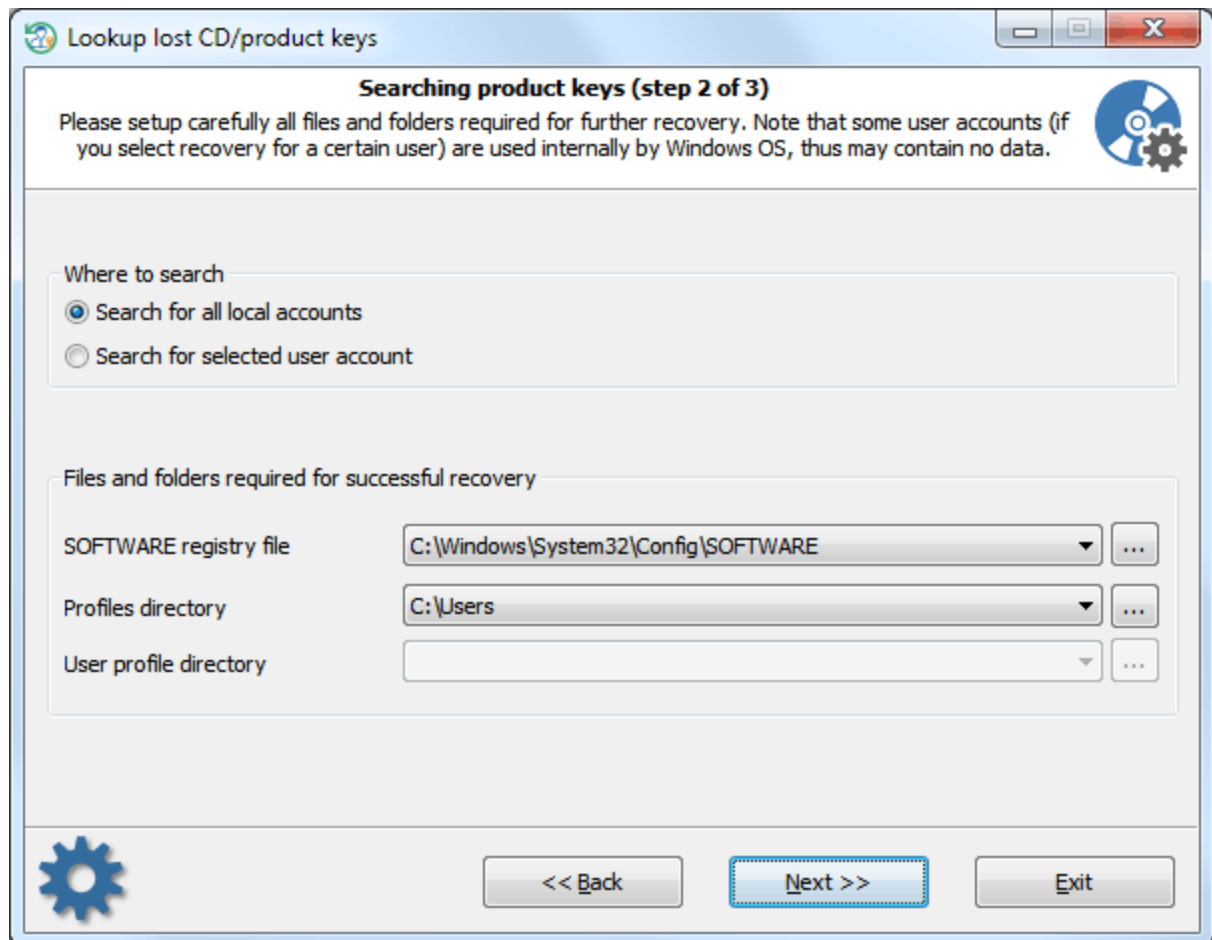
3.18.1 Search for lost product/CD keys

Using this feature, you can easily recover lost product keys and serial numbers, even if the target system is not bootable any longer.

Almost all commercial programs for Windows come with a serial key that binds the program to your PC and makes the software legal or fully featured. By losing this key, you will no longer have access to your own software unless you get the key back. Just imagine that one day you need to reinstall your

operating system. There might be a lot of reasons why you want to do so, from updating to getting rid of viruses, fixing a problem, etc. And after reinstalling, you will find out that you need to reinstall most of your software and supply it with serial codes that you no longer have access to. Without the keys, you cannot reinstall the software.

Luckily, a large proportion of computer programs store their product keys in the Windows registry and thus can easily be extracted. That's what this feature is for. Using a built-in script language, the 'Reset Windows Password' can recover serial keys for more than 1,000 software products. And yet it is very simple to use.



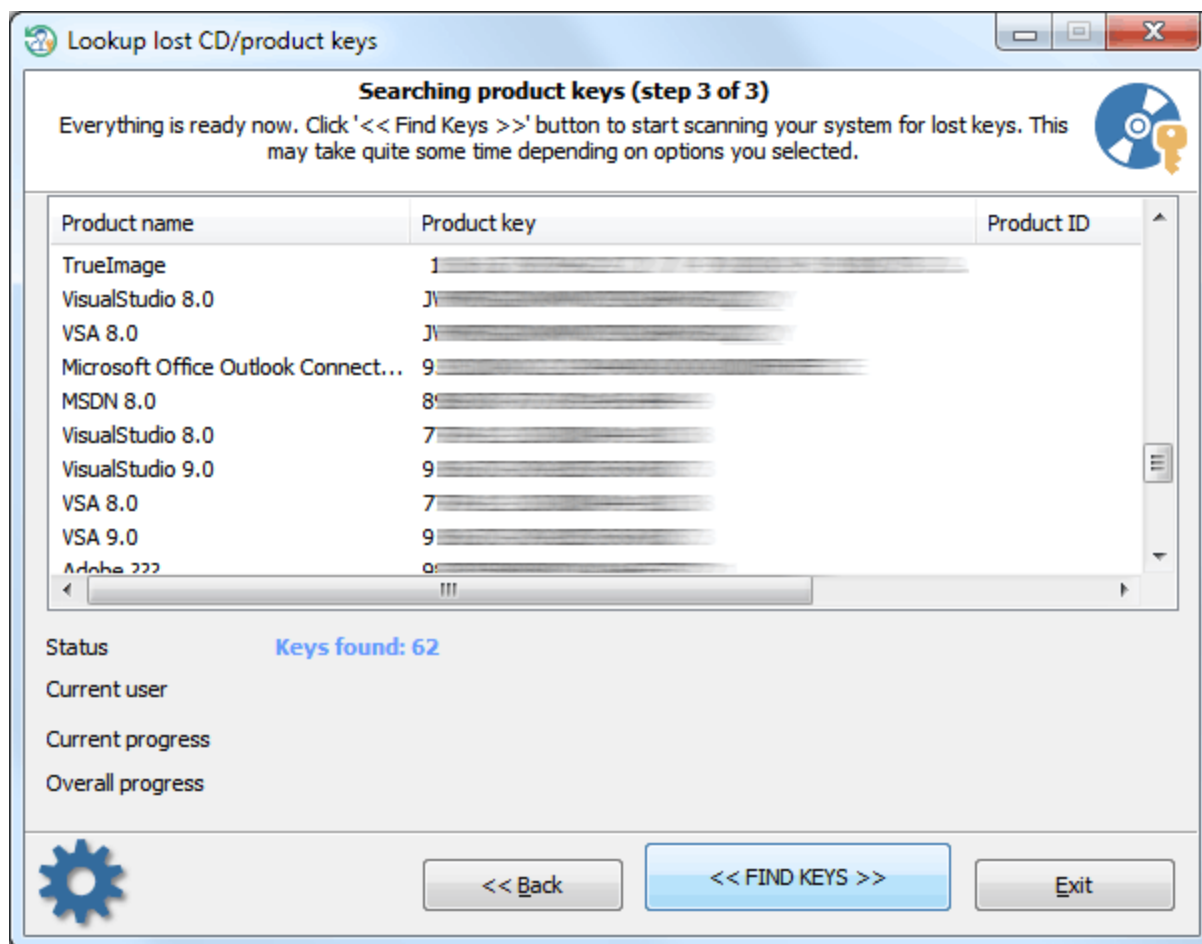
First, indicate to the program whether you need to recover serial keys for all local users or for a selected account only. Recovering keys for all user accounts needs at least two parameters to be set properly:

1. SOFTWARE registry file that is located at the following directory: 'C:\Windows\System32\Config'. Note, the drive letter as well as the Windows folder may be different. For example, 'D:\Windows', 'E:\Win', etc.

2. Profiles folder. That is the directory where all local user accounts are physically stored. For Windows Vista and higher OSs, it is usually 'C:\Users' while Windows XP uses the 'C:\Documents and Settings' folder. Usually, the profiles folder is on the same drive where the Windows directory is located, not always though.

The program will attempt to detect these folders automatically. All you need to do is select one from the drop-down list or specify an alternative path otherwise.

If you need to recover serials for a certain user, just set the appropriate option and additionally select the user from the 'User profile directory' list.

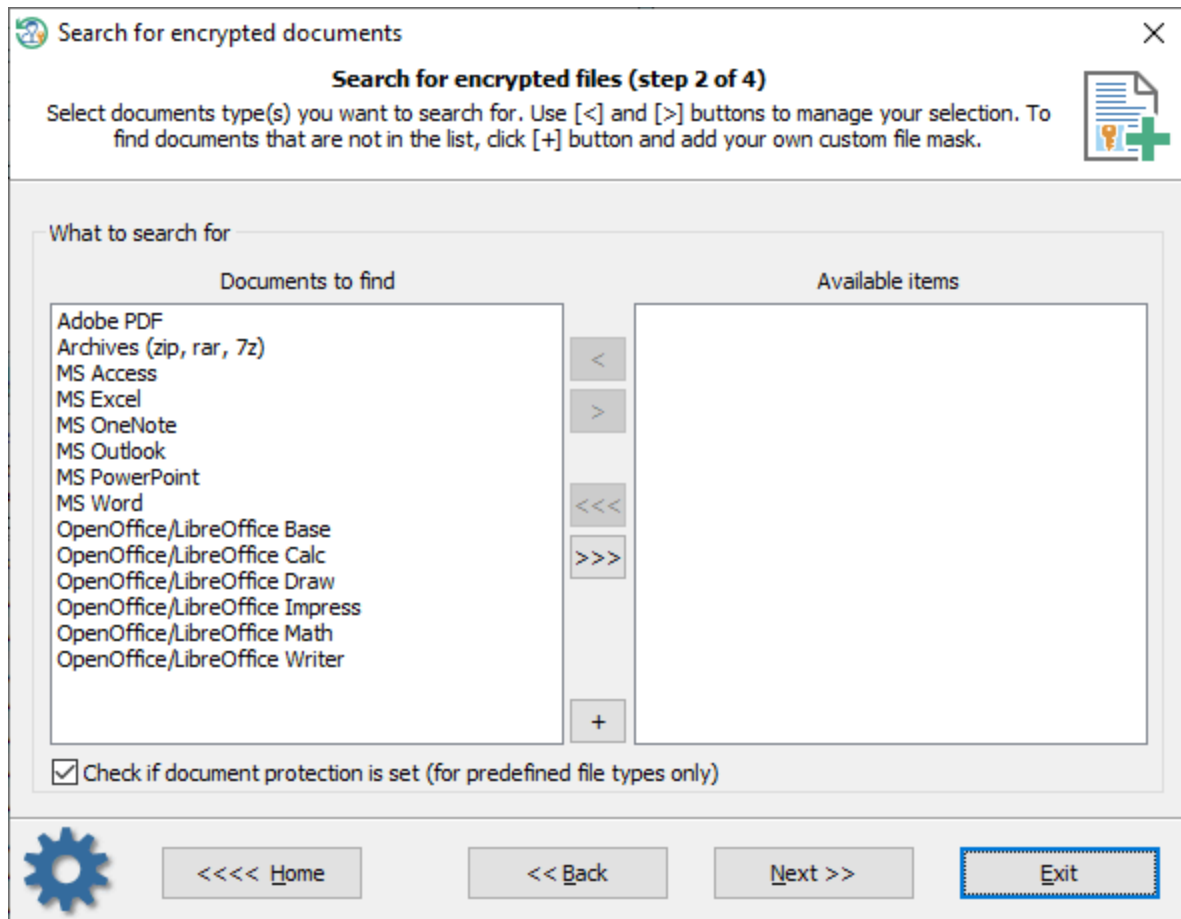


After the required options are set, proceed to the final step and clicking the '<< FIND KEYS >>' button to start the program searching for lost serial keys.

3.18.2 Search for password-protected documents

This program's feature is aimed to scan and search a PC for encrypted documents, password-protected archives and files. It is easy to use, and fast and flexible in its configuration. You can even specify your own file types to look for. The search process is divided into three simple steps:

1 Selecting document type



By default, the program searches for the following pre-defined documents:

- File archives (zip, rar, 7z)
- Adobe PDF documents
- MS Word documents
- MS Excel tables
- MS Access databases
- MS PowerPoint presentations
- MS OneNote notes
- MS Outlook data files
- OpenOffice/LibreOffice Writer documents
- OpenOffice/LibreOffice Calc tables
- OpenOffice/LibreOffice Base databases
- OpenOffice/LibreOffice Impress presentations
- OpenOffice/LibreOffice Draw documents
- OpenOffice/LibreOffice Math documents

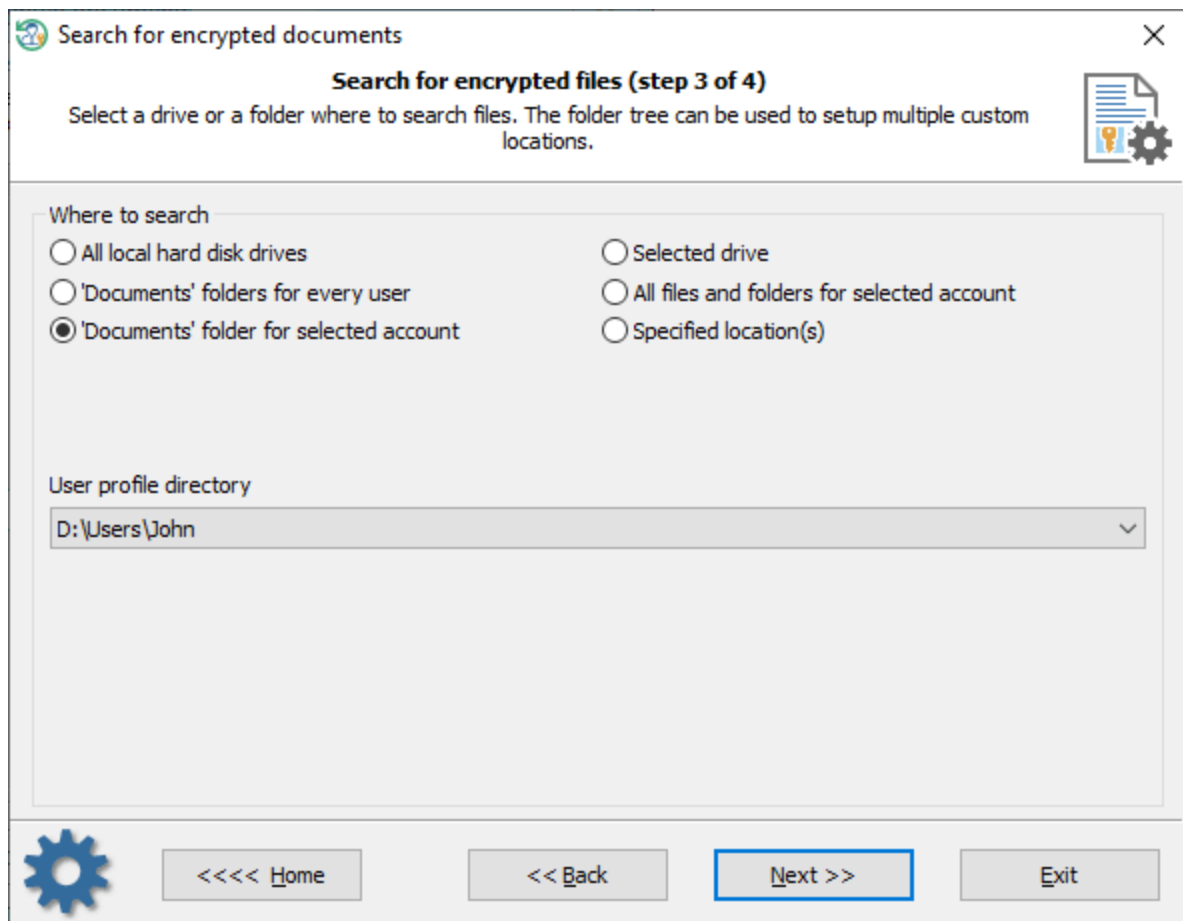
Use the [>] and [<] buttons to include or exclude available documents from the search process. If you want to add your own file types to search for, use the [+] button and specify your description and a search mask. For example, the following mask can be used to search for KeePass data files:

***.kdbx, *.kdb, *.pwd**

Keep in mind that password protection analysis is not used for the custom masks.

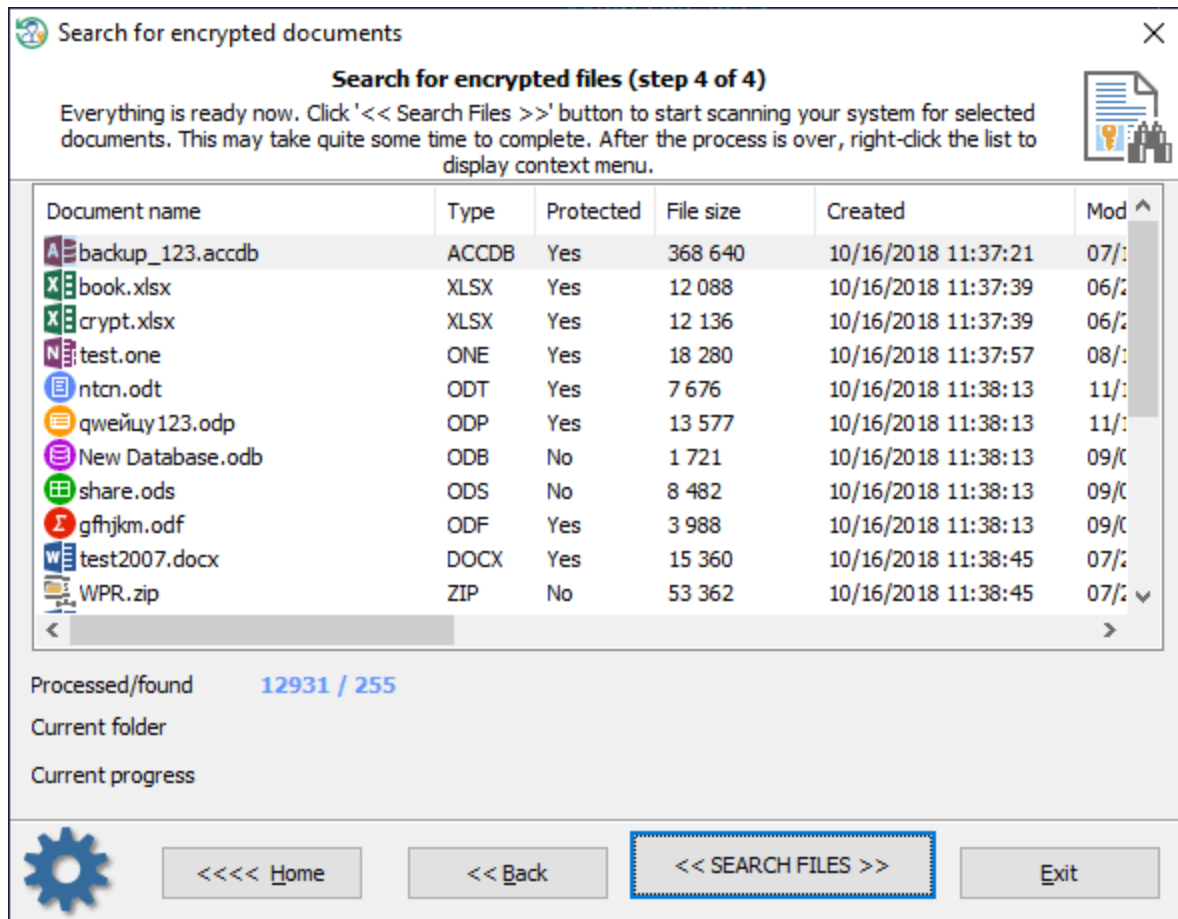
The 'Check if document protection is set...' option is used to completely turn off the password protection analysis. That could significantly speed up the search process in some cases.

2 Selecting where to search



You can narrow down the scanning range by setting up, for example, the 'Documents' folder for a selected account, or choosing a certain directory.

3 Searching for documents

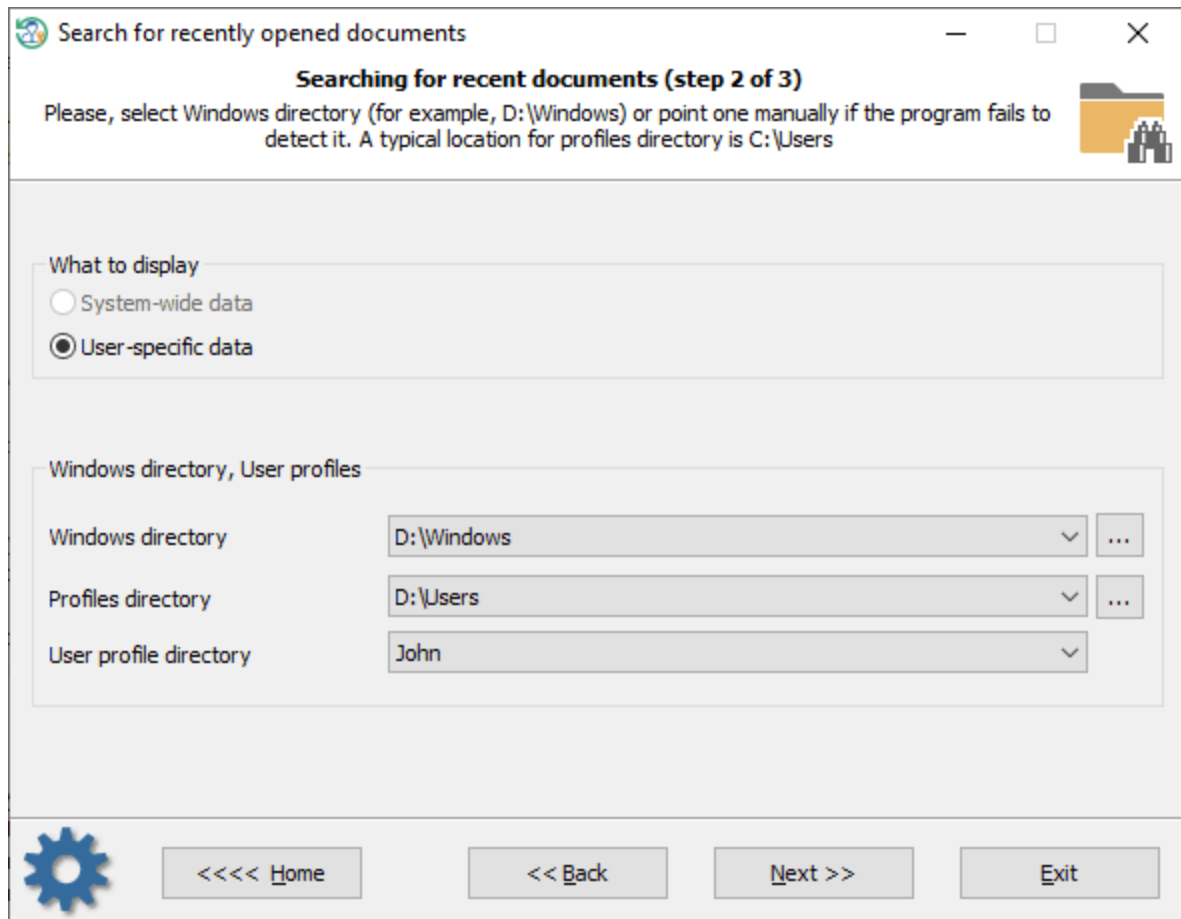


Even though the program was optimized for fast search, scanning hard disks with a lot of files may take a long time. After the search is over, right-click the list of found documents to specify the available operations. For example, you can save the list of files found to a text/ html file, or create a single zip archive for the selected items.

3.18.3 Search for recently opened files

Sometimes it is vital to get a list of the last modified documents for a user account. For example, forensics can use this tool to analyze files accessed by the user during the last login session.

1 Selecting where to search



Search for recently opened documents

Searching for recent documents (step 2 of 3)

Please, select Windows directory (for example, D:\Windows) or point one manually if the program fails to detect it. A typical location for profiles directory is C:\Users

What to display

☐ System-wide data

☒ User-specific data

Windows directory, User profiles

Windows directory: D:\Windows

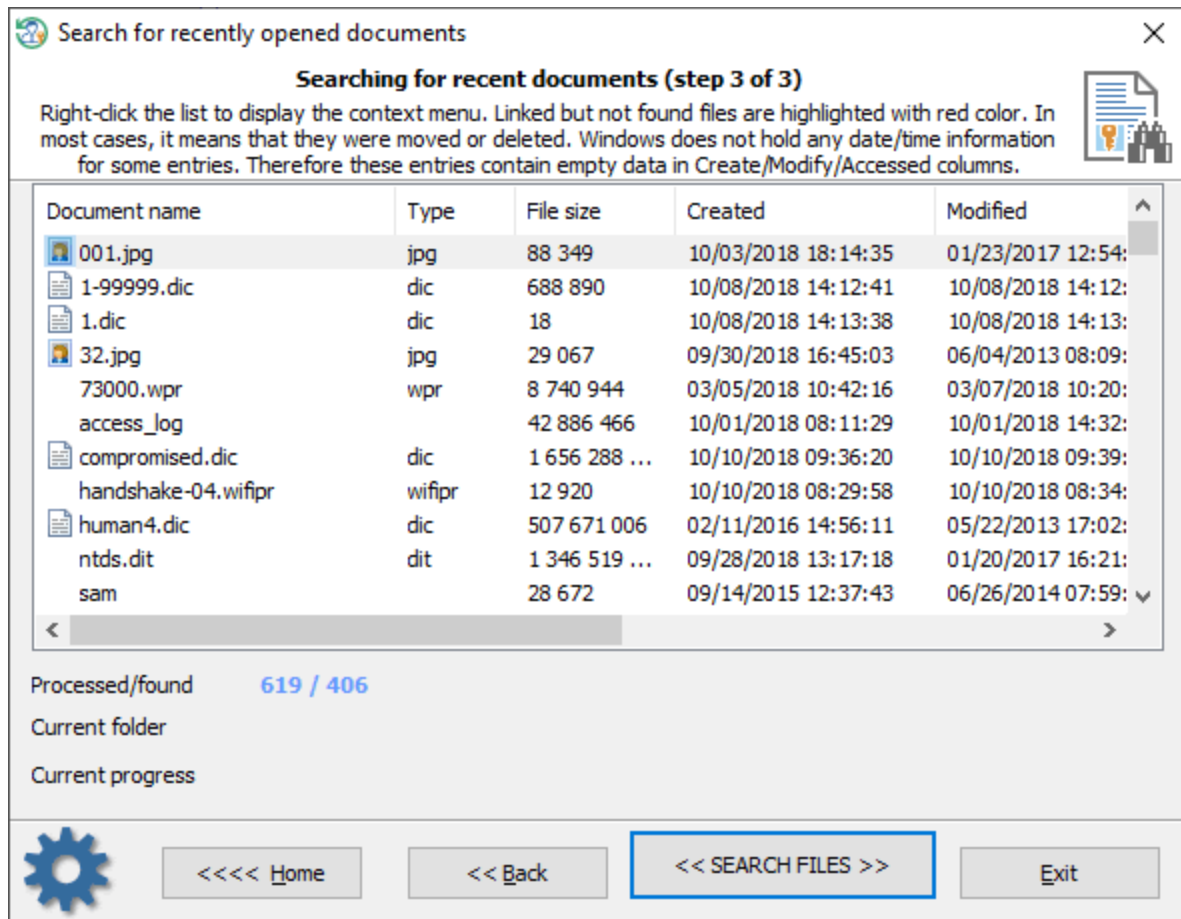
Profiles directory: D:\Users

User profile directory: John

Settings: <<<< Home << Back Next >> Exit

To extract the data, specify the target Windows directory and the user's profile.

2 Searching for recent files

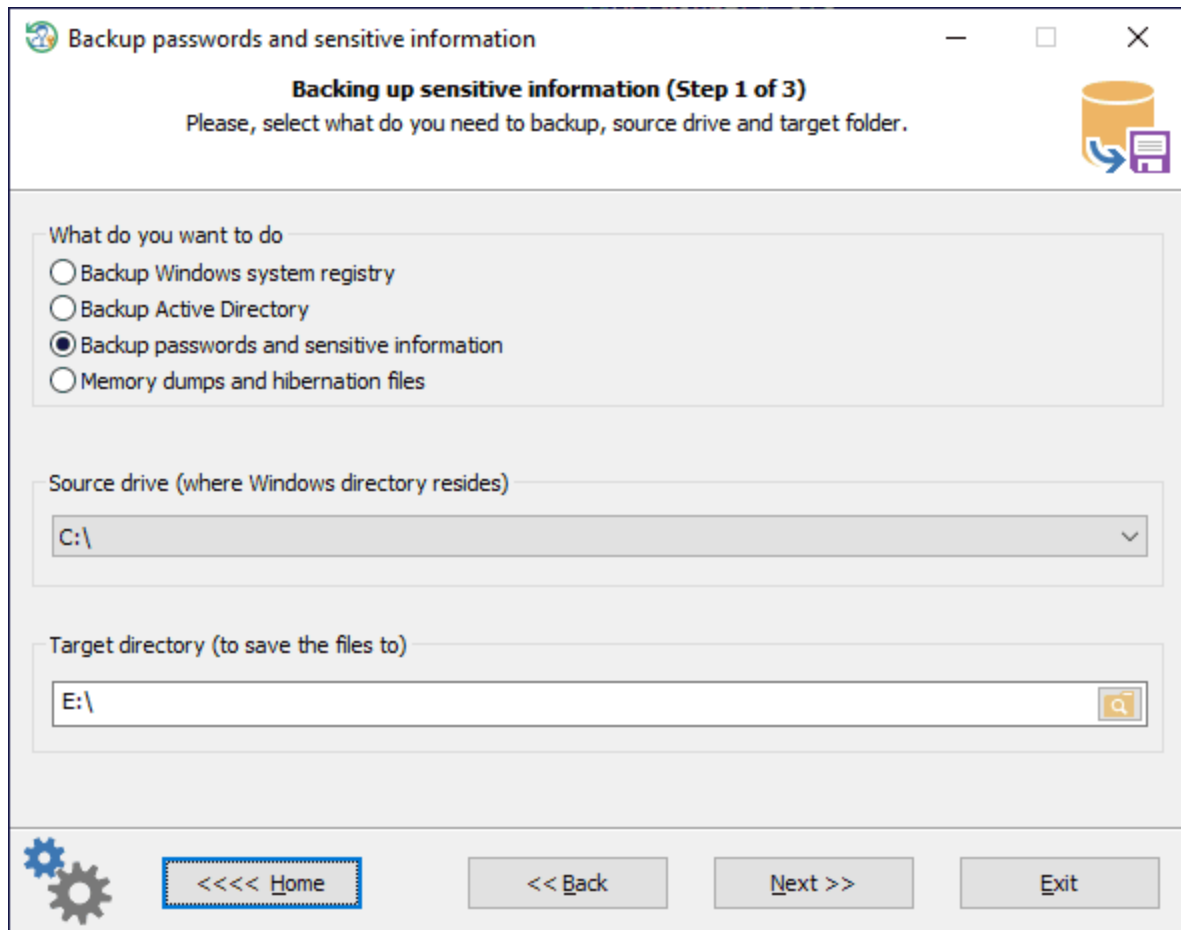


Click the 'Search Files' button to start the process. After the search is over, right-click the table to display the available operations. You can save the list of found items to a text/ html file, or backup the selected files into a zip archive.

3.18.4 Backup passwords and sensitive information

Sometimes it is vital to make a copy of Windows registry or an Active Directory database. **Reset Windows Password** is a lifesaver for those who need to back up the files easily. It can even make a snapshot of all sensitive data of the target PC in just a couple of clicks.

Setting what do you want to backup



First, we need to set up what to backup:

- Windows registry files
- Active Directory database
- All sensitive information including Windows registry, passwords, certificates, etc.
- Found memory dumps and hibernation files

You will have to set a source drive where the target Windows directory resides and a target path. The target path will be used to save the output archived files. By default, the program suggests first hard drive as the source and first removable drive as the target.

Setting Windows directory and user account

Backup passwords and sensitive information

Backing up sensitive information (Step 2 of 3)

Make sure the path to Windows folder was set up correctly and choose valid one, if not. Specify whether you want to backup sensitive data for a single user or for all local users.

System folders

Windows directory: G:\Windows

Active Directory folder:

Where to search

☐ Search for all local accounts

☒ Search for selected user account

User folders

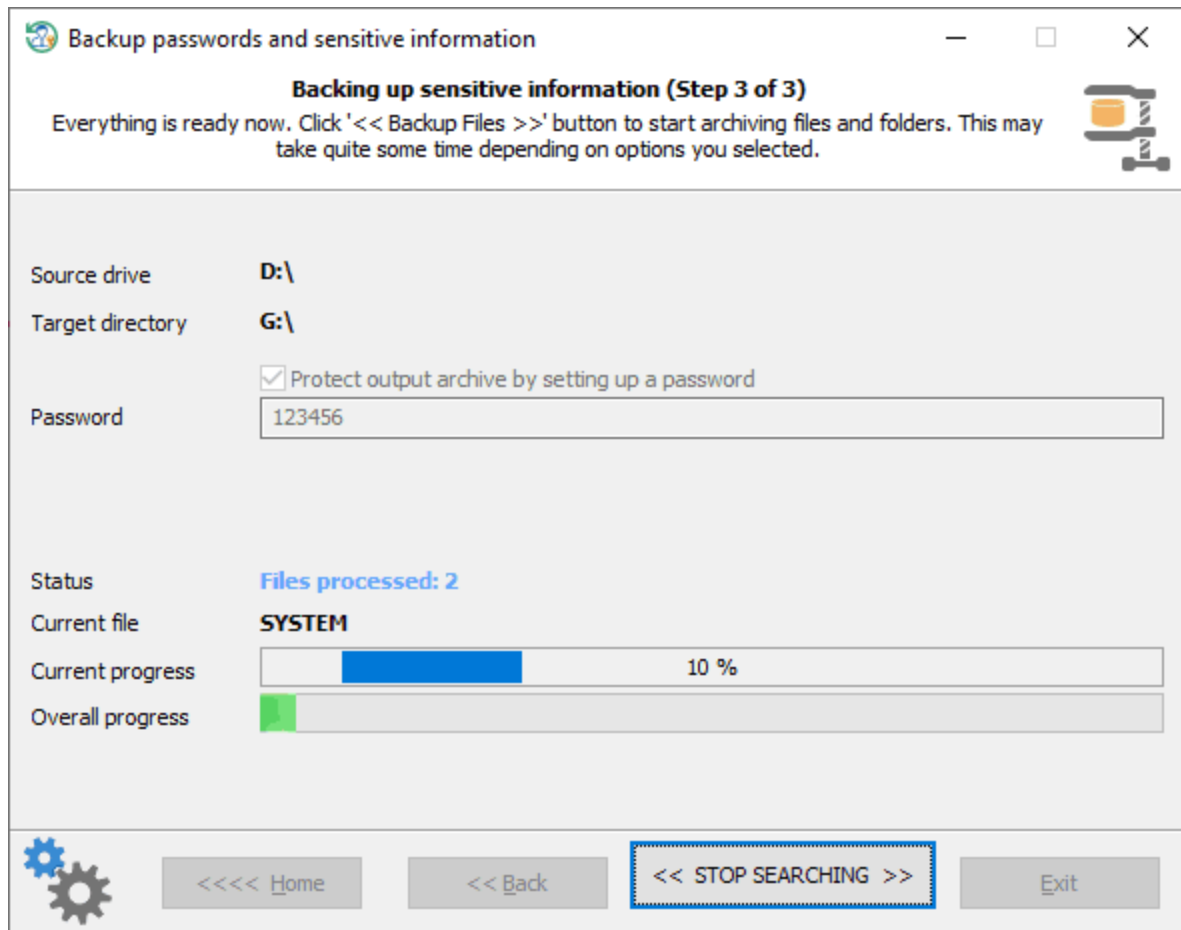
Profiles directory: G:\Users

User profile directory: G:\Users\Administrator

<< Back Next >> Exit

Next step is a bit simpler. In case you selected Registry/Active Directory backup on the previous step, all you need here is to confirm Windows/AD folders. Otherwise, you'll additionally have to select either profiles directory or profile directory for selected user, depending on options you choose.

Locating and backing up the found data

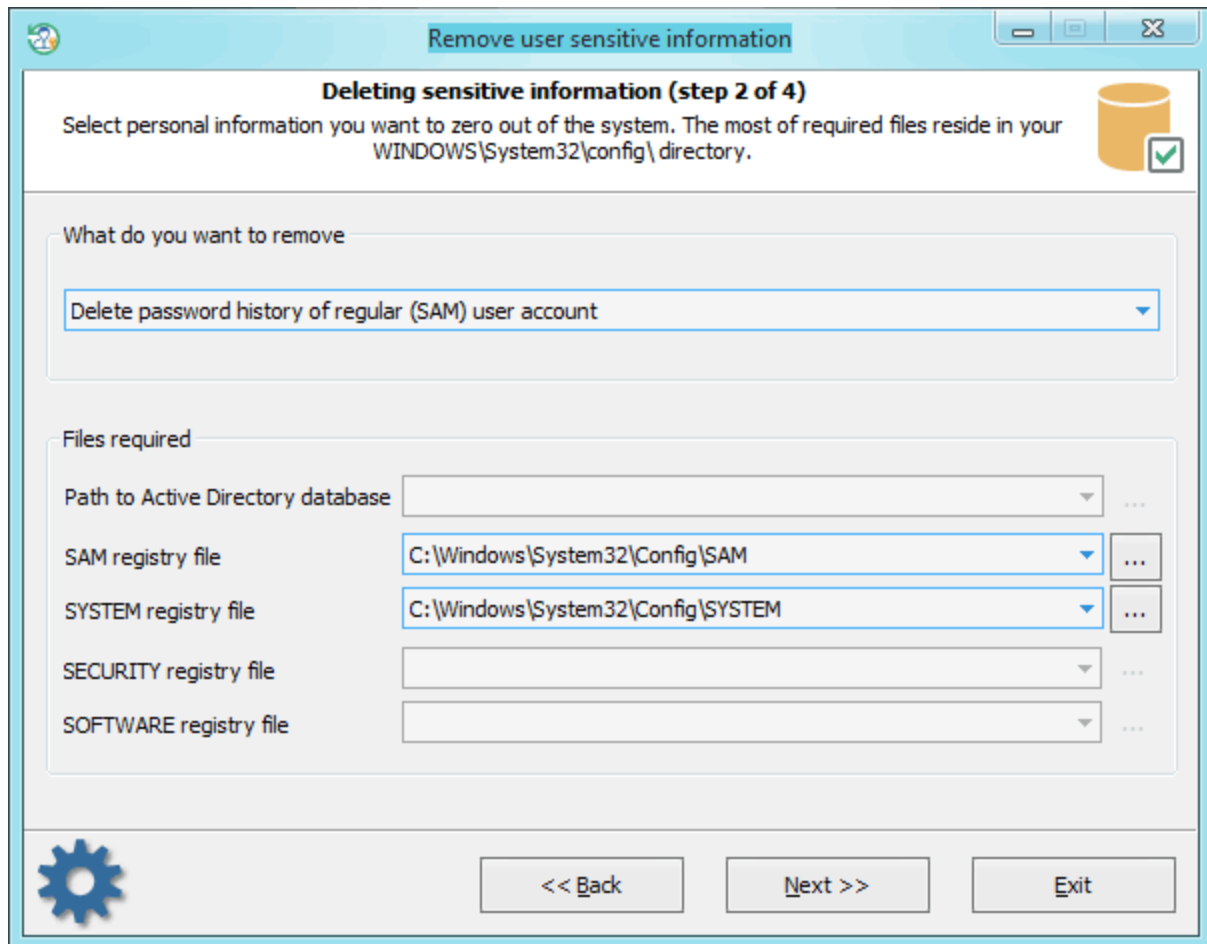


And the final dialog is just a progress for the backup operation. Click **<< Back up files >>** button to start the process. By successful completion, you should get a *.ZIP archive which holds all found files. To protect your private data against unauthorized access, you are free to set a password for the output ZIP archive.

Later you can use the found files to further security analysis, password recovery, and audit in any 3d-party software. For example, using our [Windows Password Recovery](#) tool.

3.18.5 Removing user's private information

Selecting data to be removed



The application has a number of advanced features. One of them is deleting information that can be used by potential malefactors for recovering account passwords on your computer. Be careful; the information will be removed permanently with no chances for recovery. So, it includes the following items:

1. Deleting password history for standard SAM accounts and Active Directory user accounts. SAM password history, for example, is set in the groups policy of the local computer. Start -> Run -> gpedit.msc -> click OK. Under Computer Configuration, drill down under Windows Settings -> Security Settings -> Local Policies -> Security Options. Here look for policy: *Interactive Logon: Number of previous logons to cache*.
2. Deleting domain cached passwords. More on domain cached passwords can be read [here](#).
3. Deleting cached Windows logon password.
4. Deleting password reset diskette information. With that information and the password reset disk, one can recover the original textual password.
5. Deleting password hints.
6. Resetting Syskey

To continue with the application, provide (or select from available) the following files:

- [Deletion of AD password history](#) – **SYSTEM** registry file and Active Directory database file (**ntds.dit**)
- [Deletion of SAM password history](#) – **SAM** and **SYSTEM** registry files
- [Deletion of cached domain passwords](#) – files **SECURITY** and **SYSTEM**
- [Deletion of cached logon passwords](#) – files **SECURITY**, **SOFTWARE** and **SYSTEM**
- [Deletion of password reset information](#) - files **SAM**, **SECURITY** and **SYSTEM**
- [Deletion of password hints](#) - **SAM**, **SOFTWARE** and **SYSTEM**

- [Resetting SYSKEY](#) - **SAM**, **SECURITY** and **SYSTEM**

All registry files, except Active Directory database, are stored in the following directory **%WINDIR%\system32\config**. Where %WINDIR% stands for the Windows folder, by default - C:\Windows.

The location of the AD database is set during installation. By default, that's the **%WINDIR%\NTDS** folder.

3.18.5.1 Removing password history of SAM or Active Directory users

Selecting data source

Remove user sensitive information

Deleting sensitive information (step 2 of 4)

Select personal information you want to zero out of the system. The most of required files reside in your WINDOWS\System32\config\ directory.

What do you want to remove

Delete password history of regular (SAM) user account

Files required

Path to Active Directory database

SAM registry file C:\Windows\System32\Config\SAM

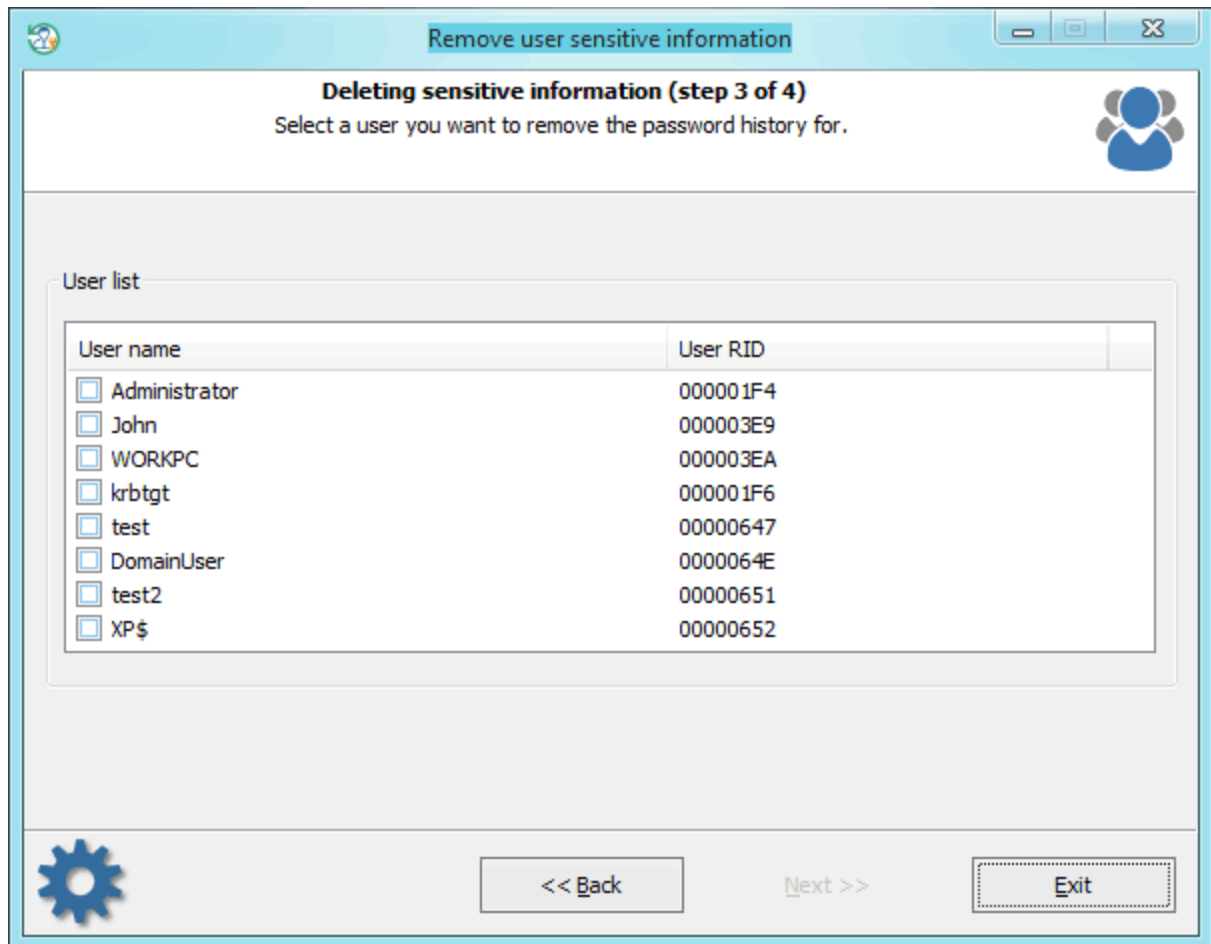
SYSTEM registry file C:\Windows\System32\Config\SYSTEM

SECURITY registry file

SOFTWARE registry file

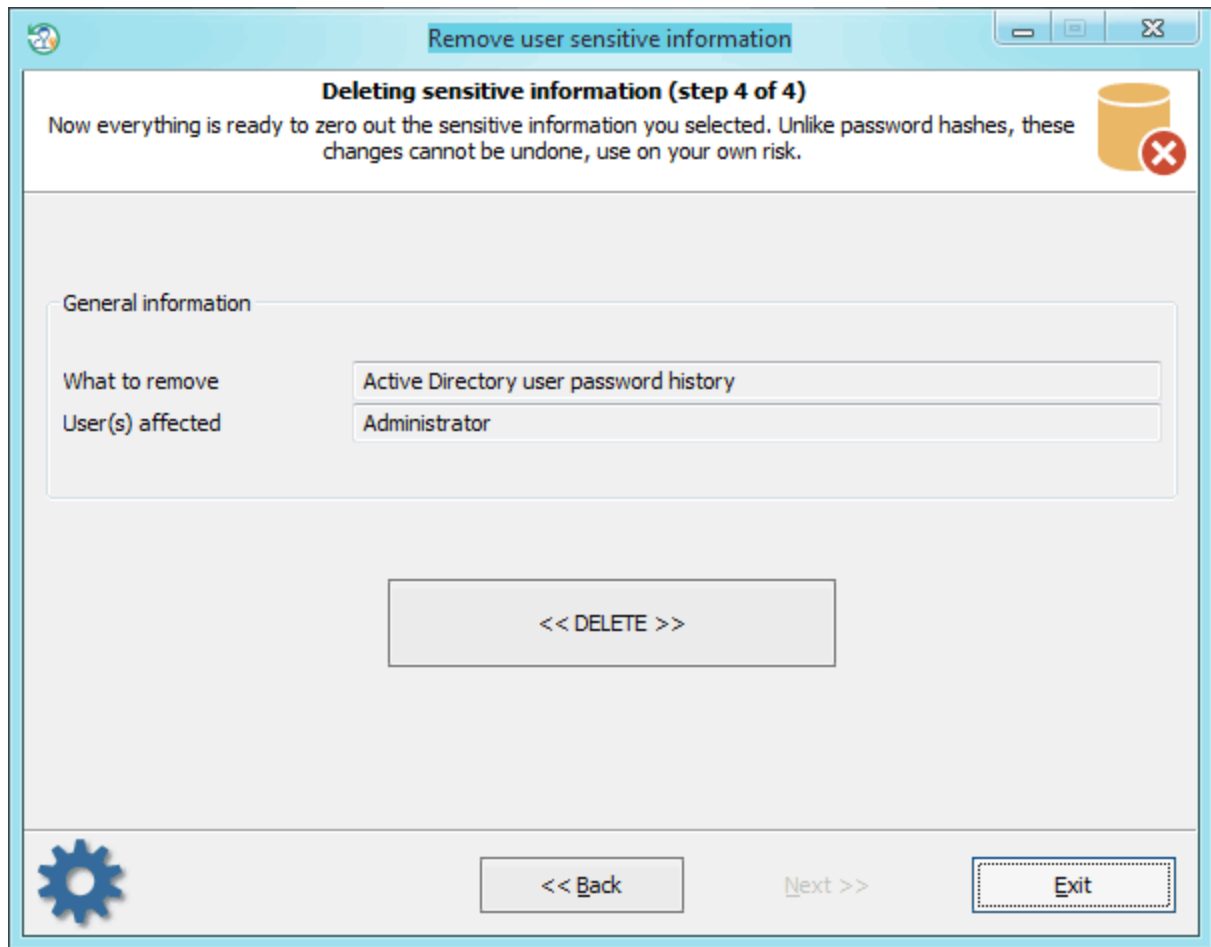
<< Back Next >> Exit

Selecting user account



On the account list, select the one we need to delete password history for. The application displays only users that have history.

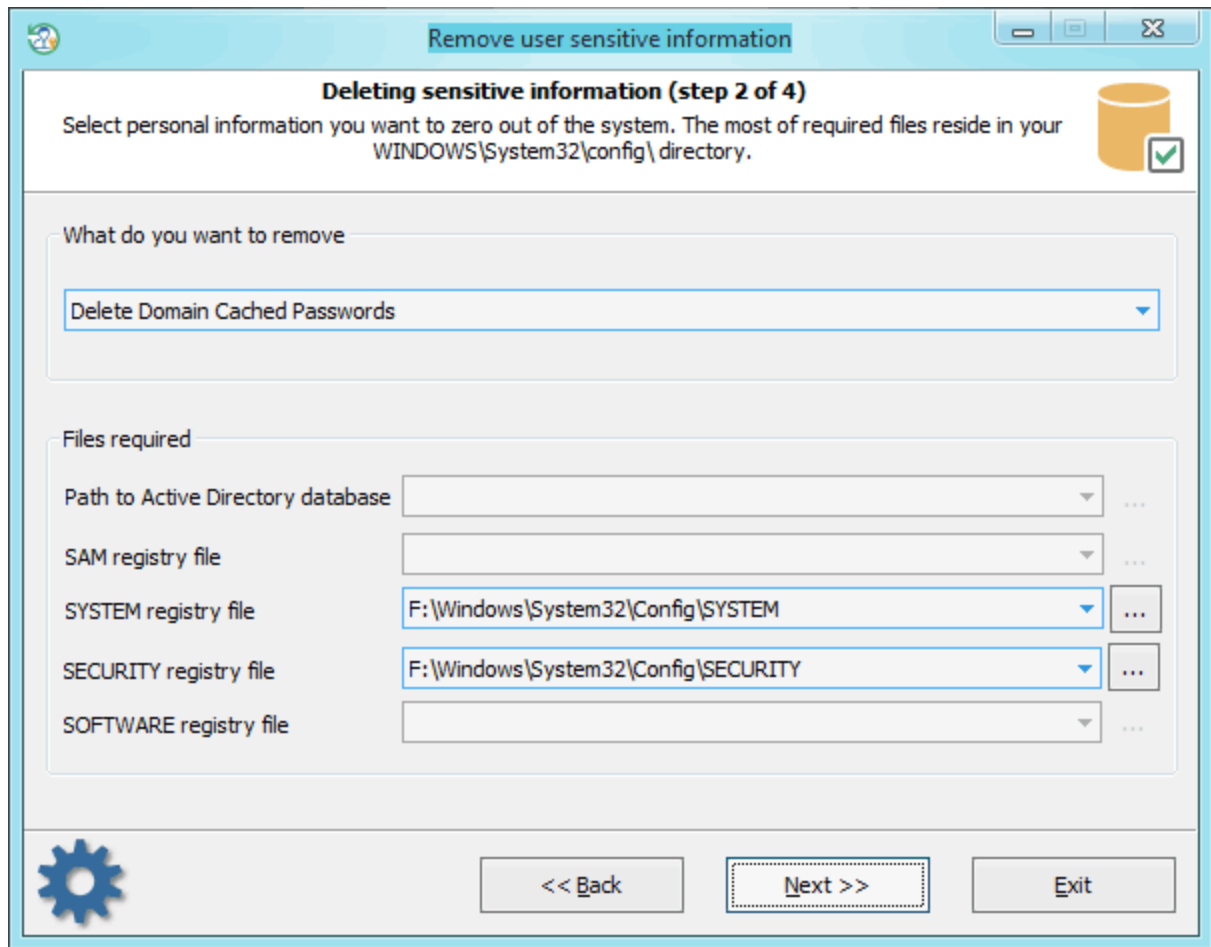
Deleting password history



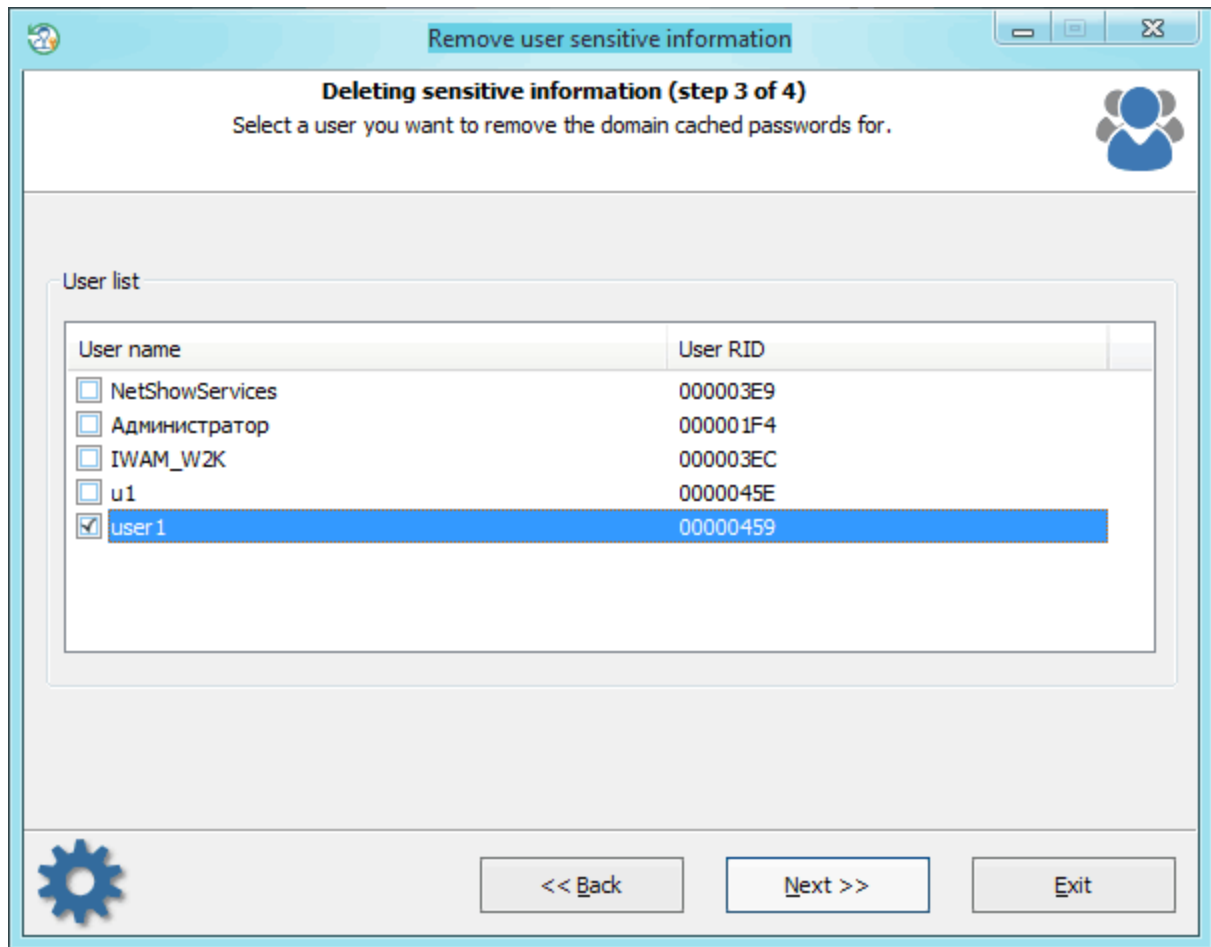
Click <<Delete>> and get rid of the unnecessary information permanently.

3.18.5.2 Removing domain cached passwords

Selecting data source

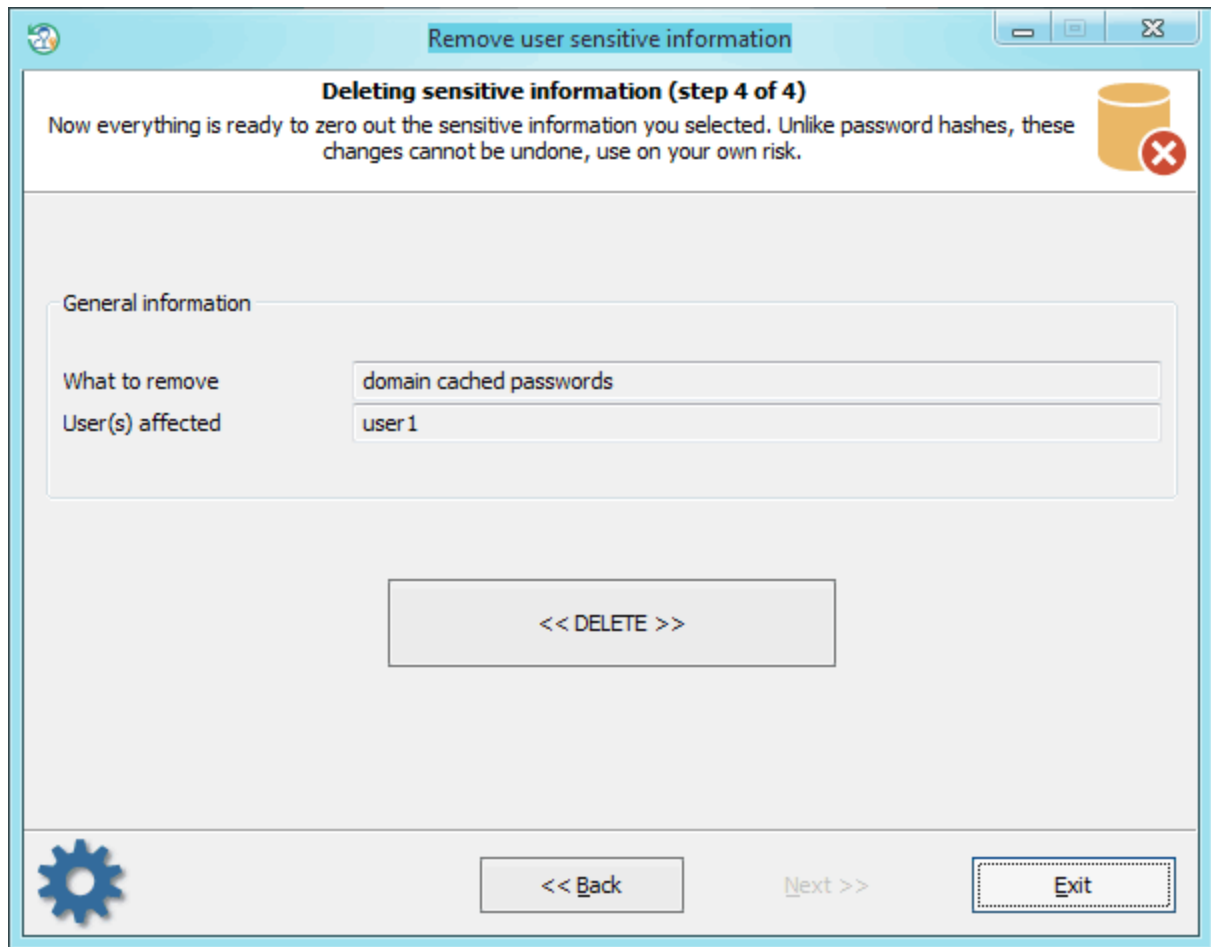


Selecting user account



Choosing the account you want to remove the passwords for.

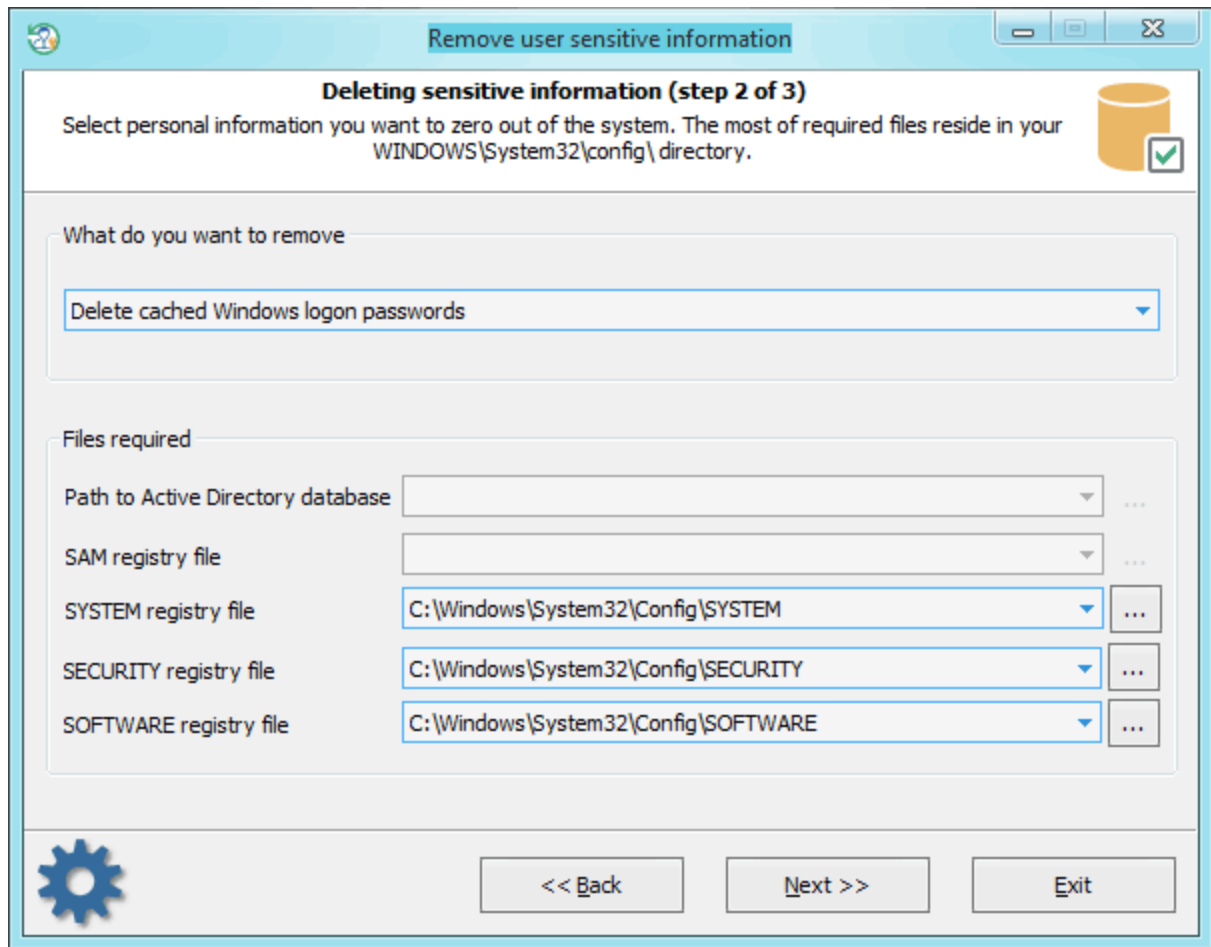
Deleting domain cached passwords



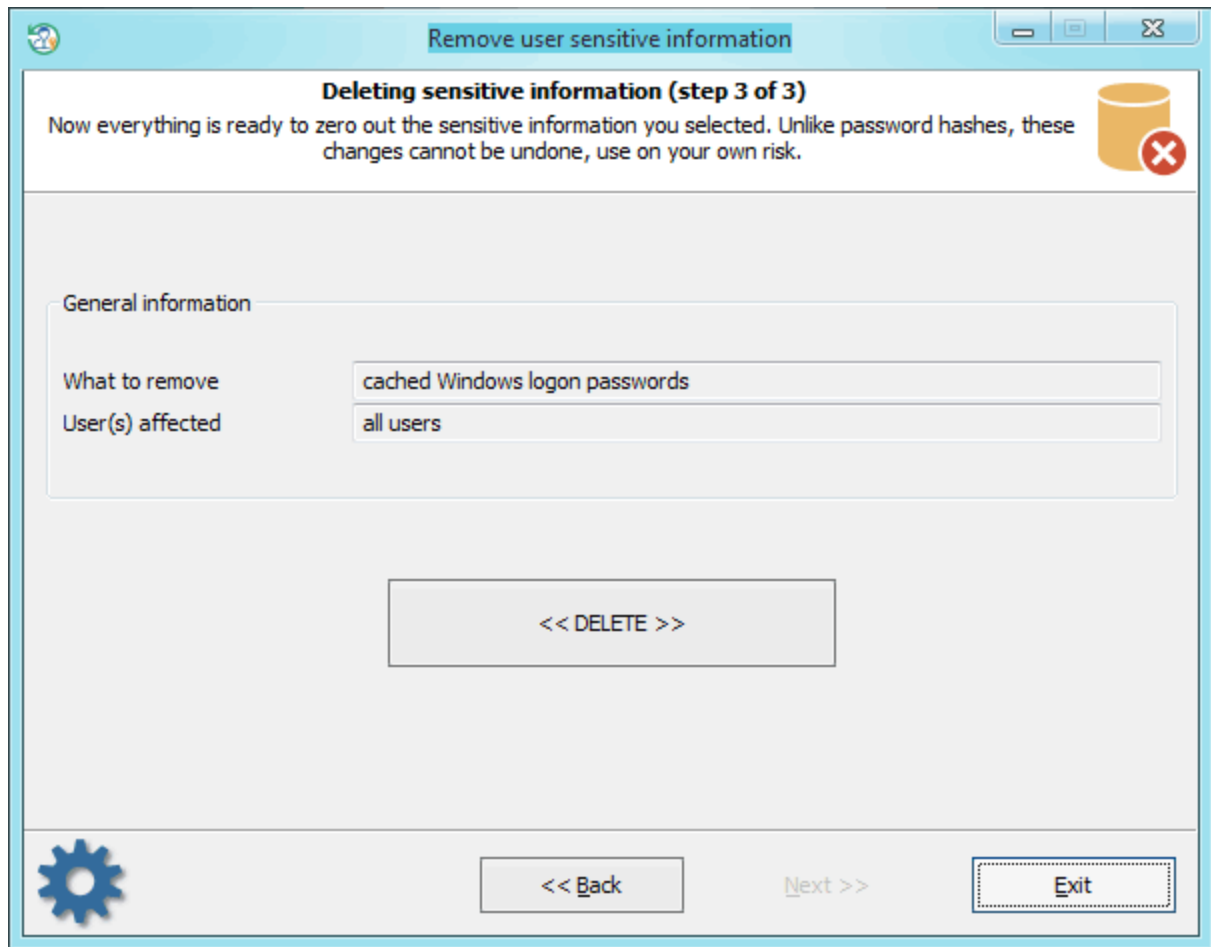
Just confirm deleting all domain cached passwords for user1 account.

3.18.5.3 Removing cached logon password

Selecting data source



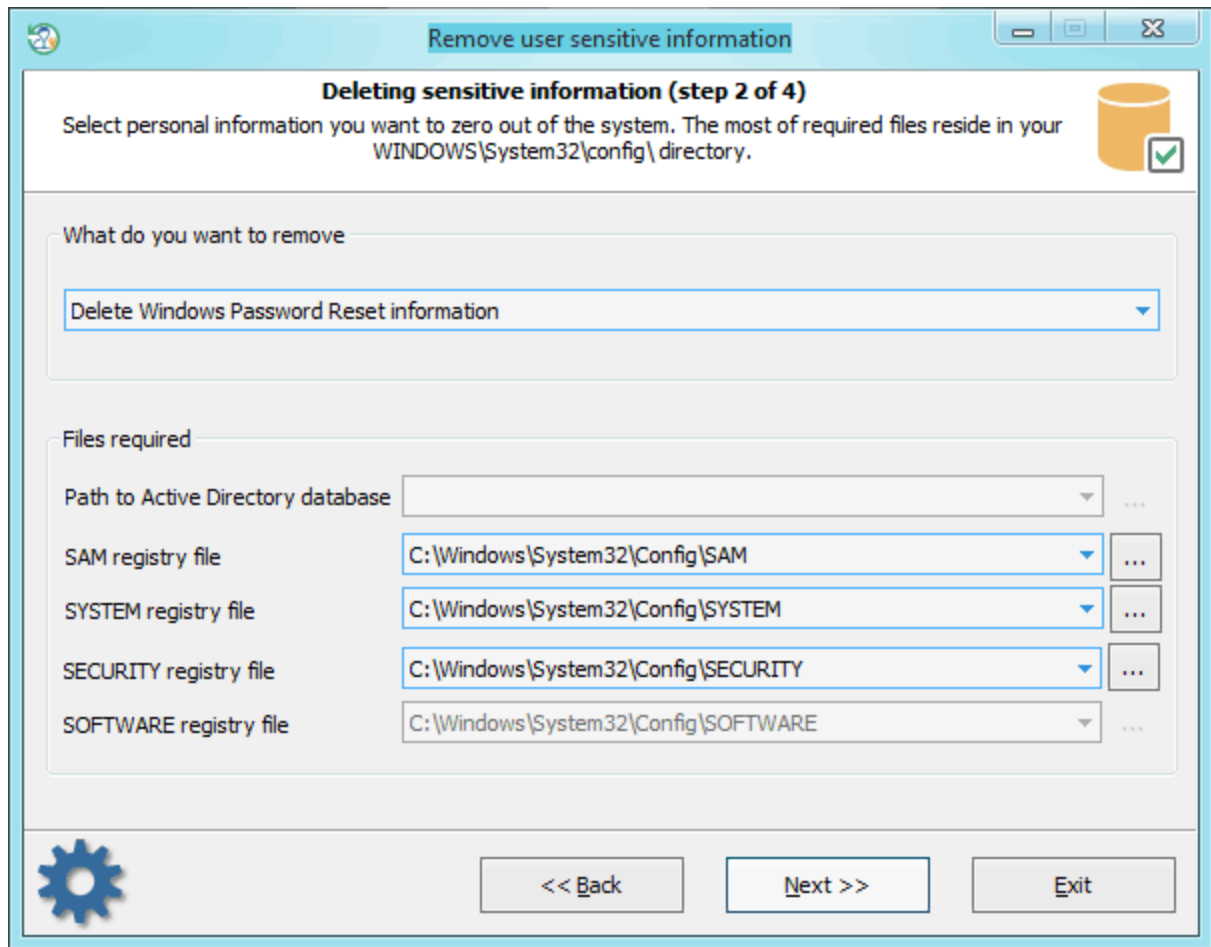
Deleting Windows cached logon password



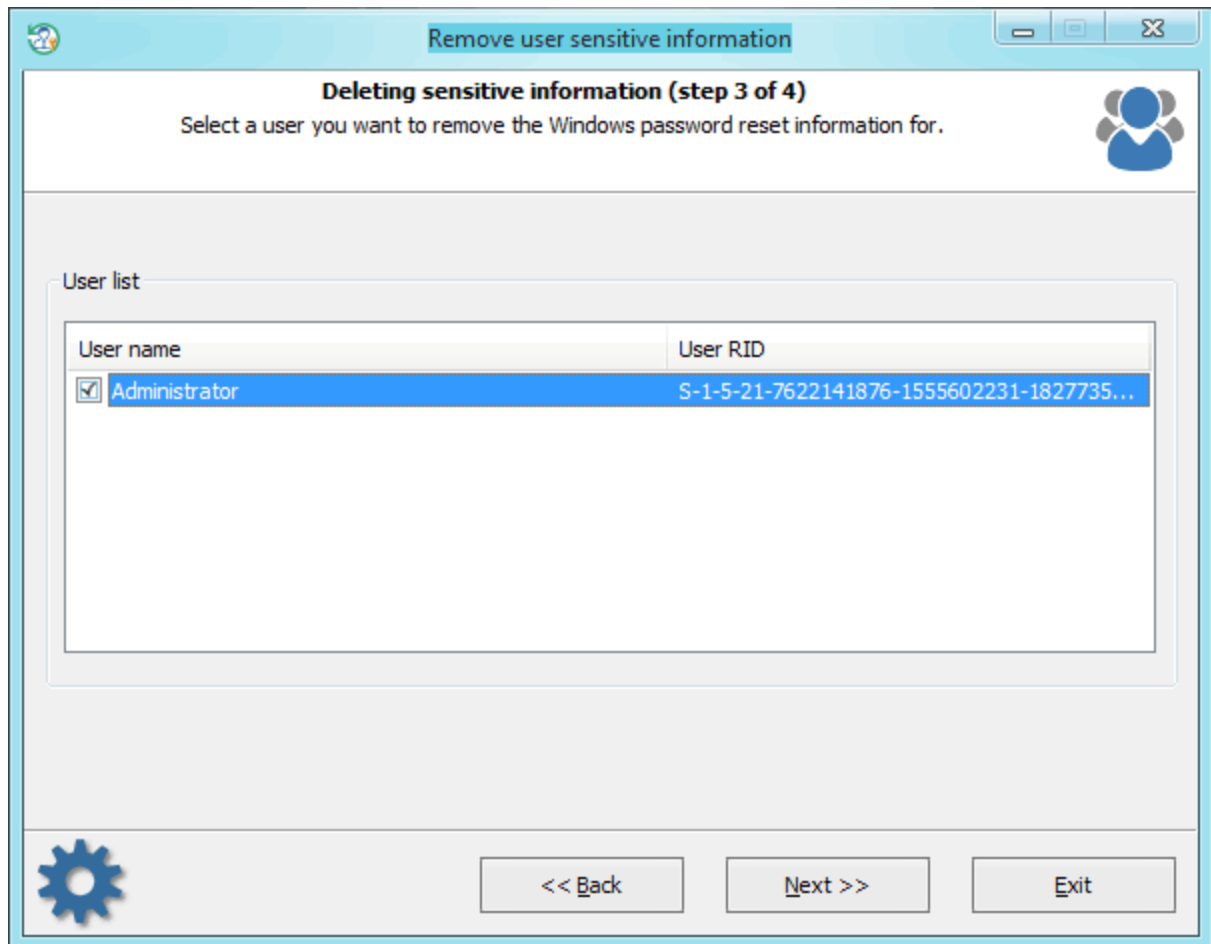
And confirm the permanent removal of cached logon passwords.

3.18.5.4 Removing password reset disk information

Selecting data source

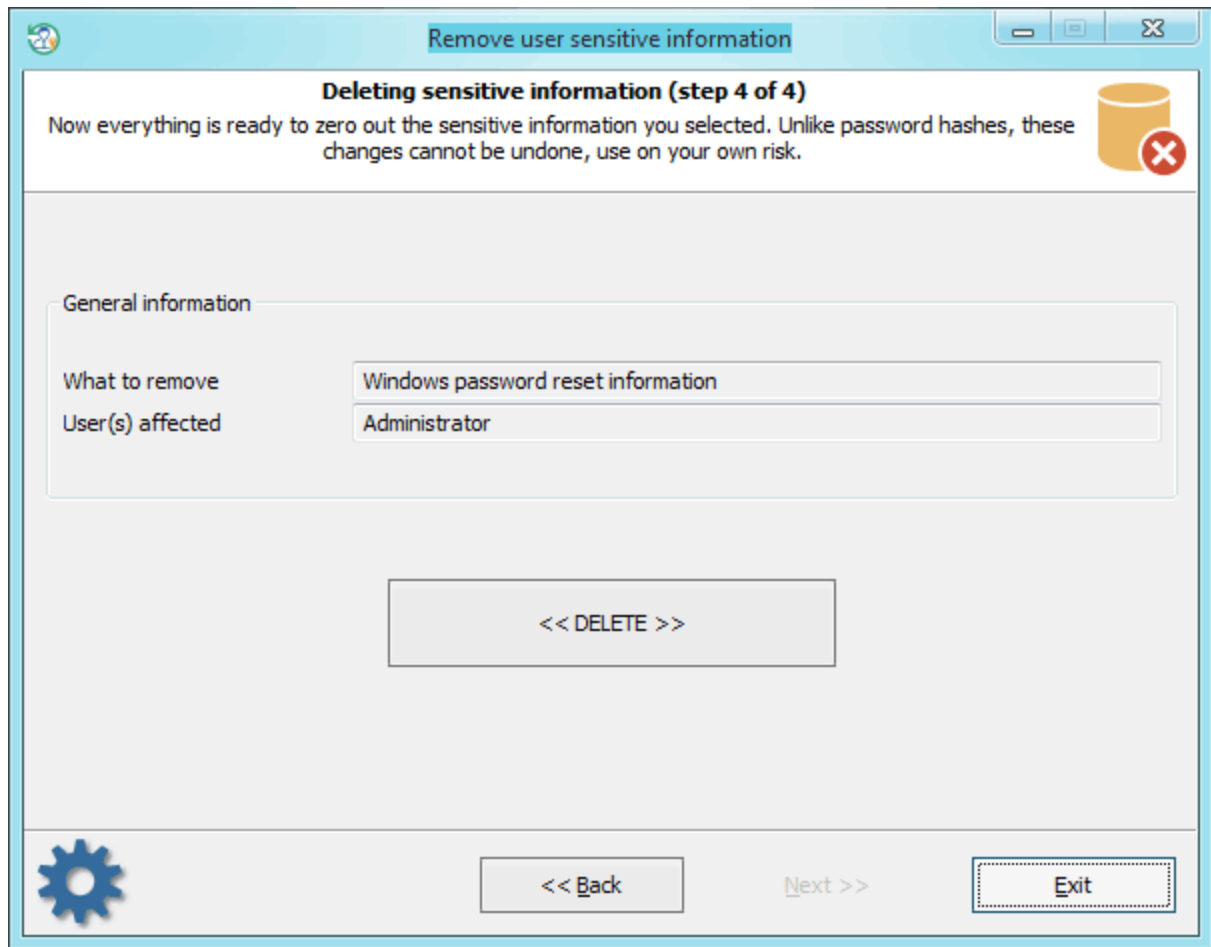


Selecting user account



Check the user whose information we want to delete. When creating a password reset disk, the user's encrypted password is stored in the registry. While the diskette stores the encryption key. Deleting the encrypted password from the registry makes the further existence of the reset password diskette useless.

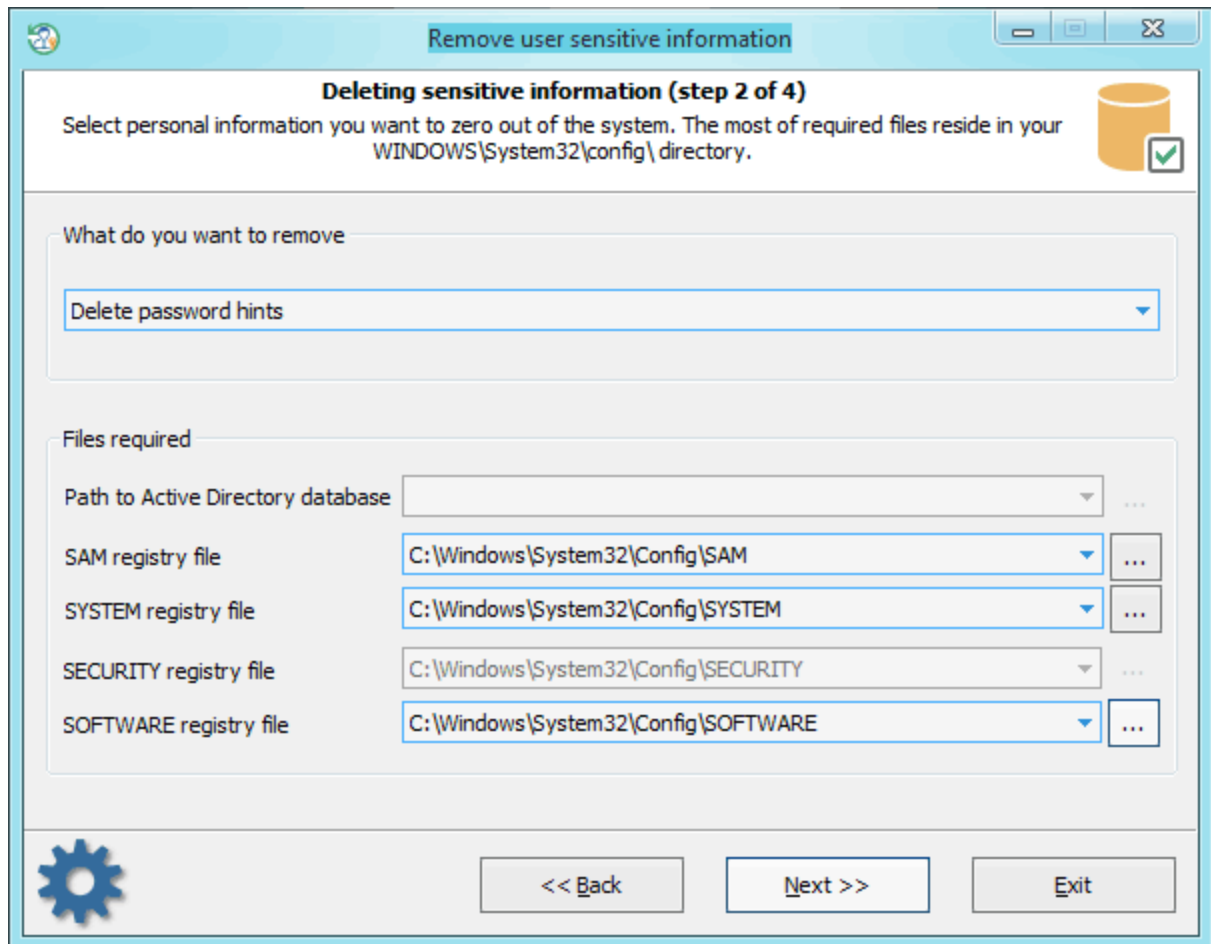
Deleting password reset diskette information



Confirm deletion.

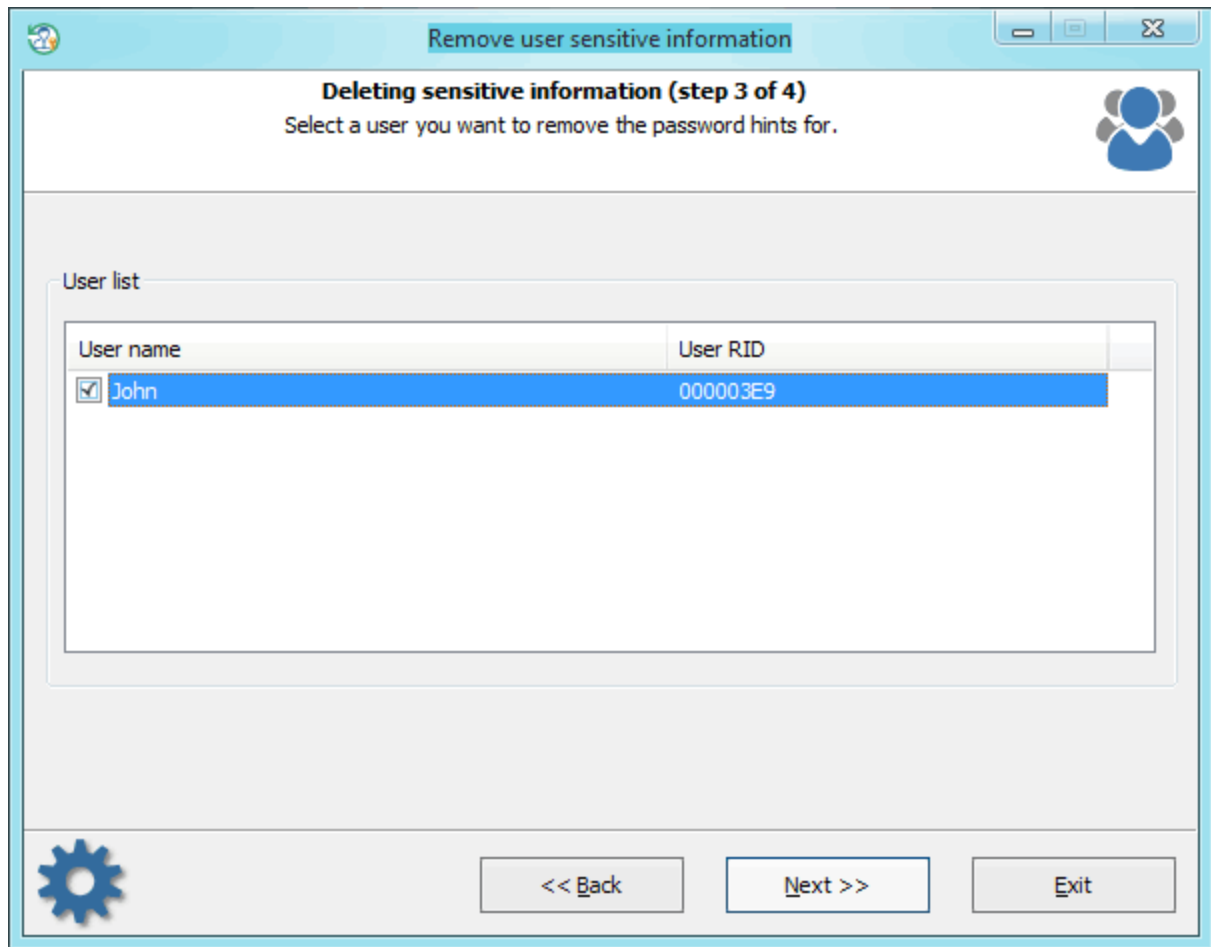
3.18.5.5 Removing password hints

Selecting data source



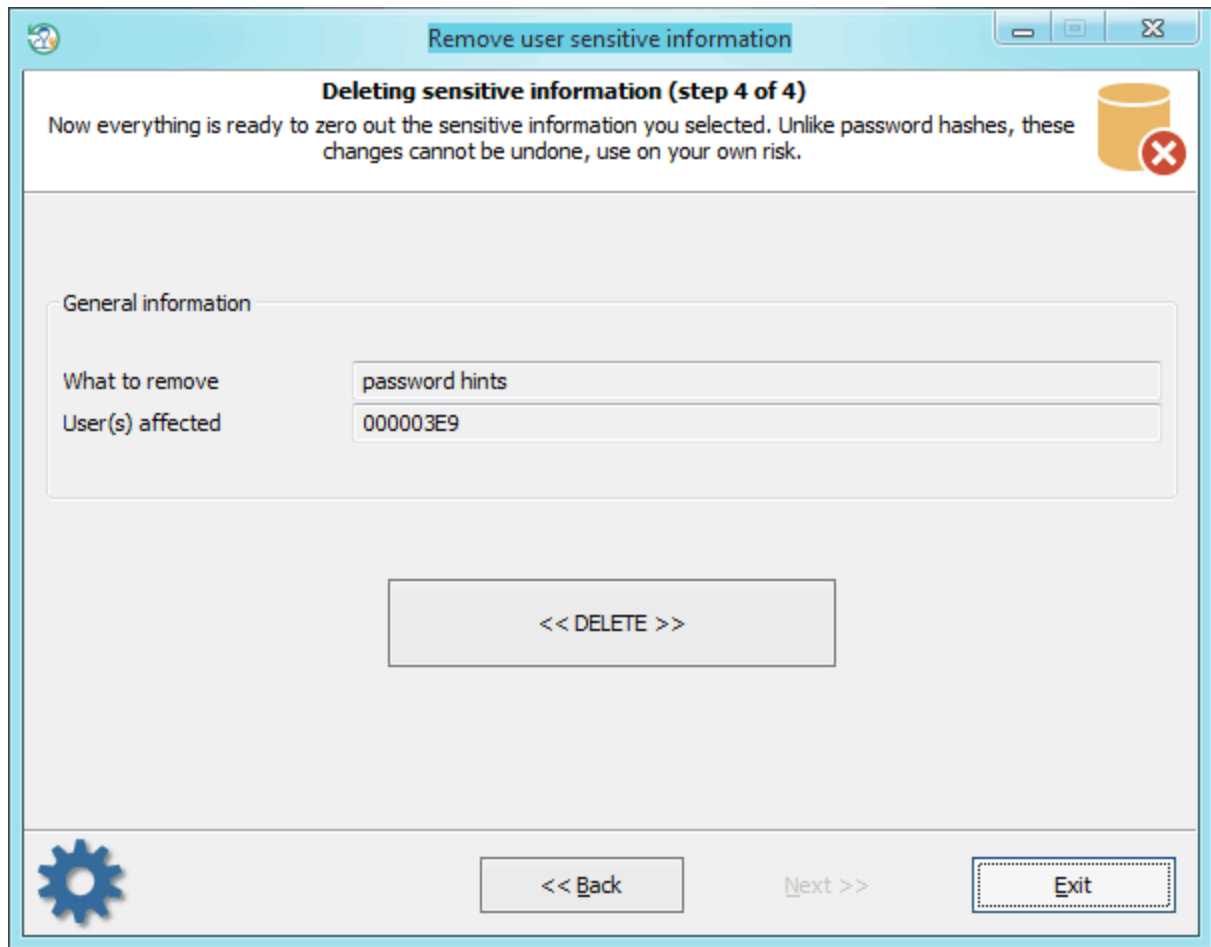
Password hints are stored either in the SOFTWARE registry (Windows XP, Windows 2003) or in the SAM file (Windows Vista and higher OS). The decryption will also require the SYSTEM file.

Selecting user account



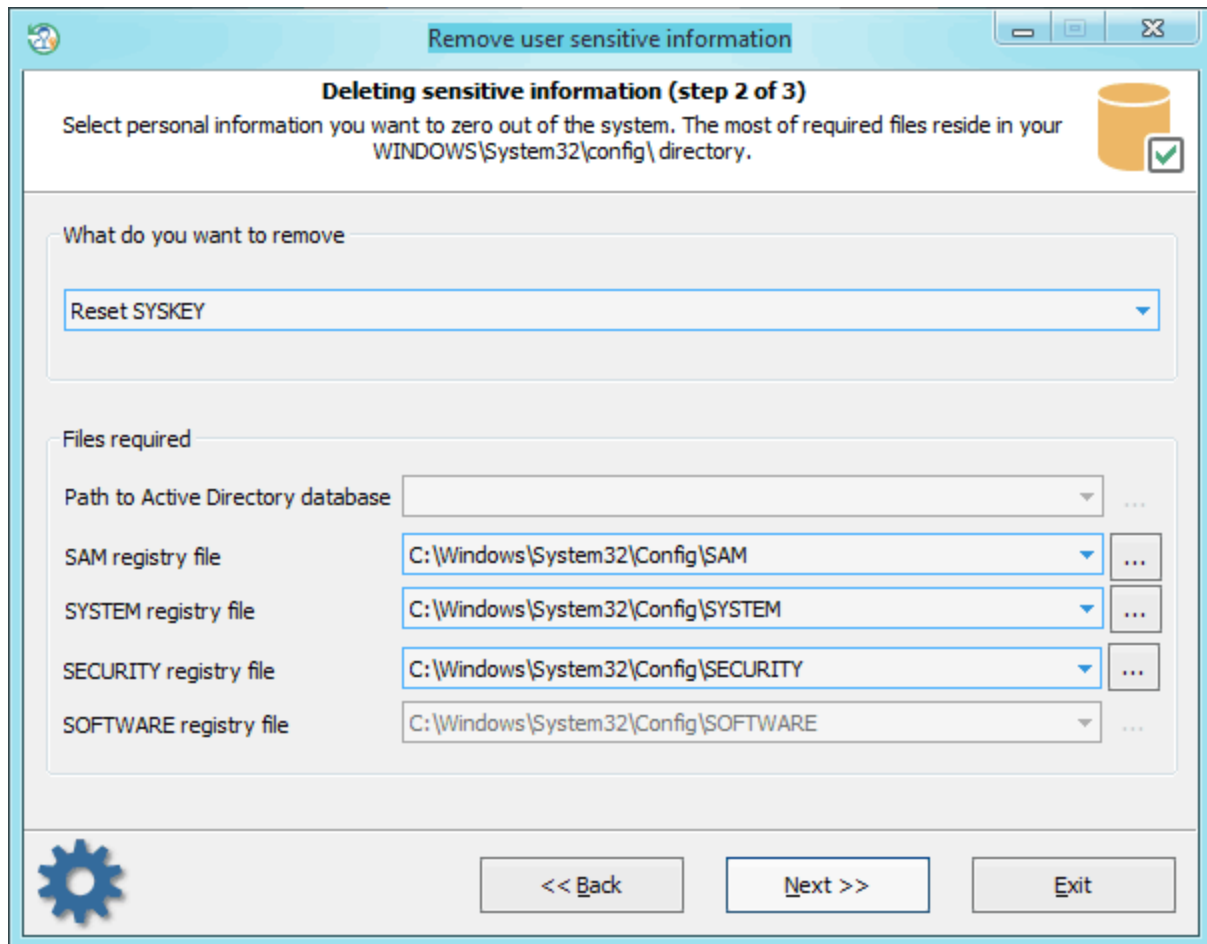
Select the user whose hint is to be cleared from the system and then follow the final removal dialog.

Removing hints



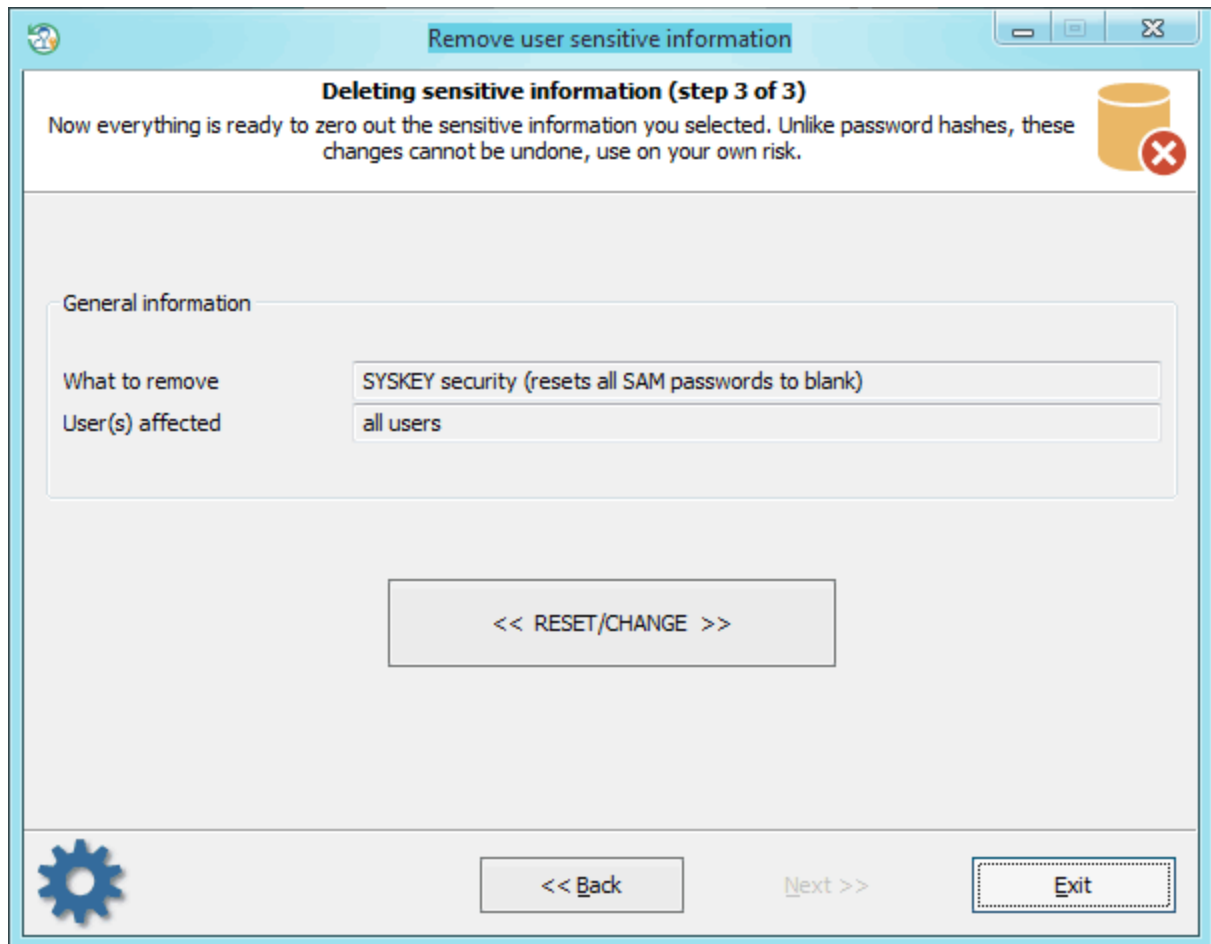
3.18.5.6 Resetting SYSKEY

Selecting data source



First you need to point to 3 registry hives: **SAM**, **SYSTEM** and **SECURITY**. Usually SYSKEY resides in your SYSTEM registry under **HKLM\CurrentControlSet\Control\Lsa** key. But once you set your SYSKEY for example to require a boot startup password and forgot it, there's no chance to boot up your system. Needless to say that SYSKEY is extremely effective tool in the hands of a guru. Setting your SYSKEY option to require a startup password or boot diskette is very effective against ANY(!) Windows password breaker. In that case a password extractor program can not decrypt your password hashes even if it get a full access to your system.

Resetting SYSKEY

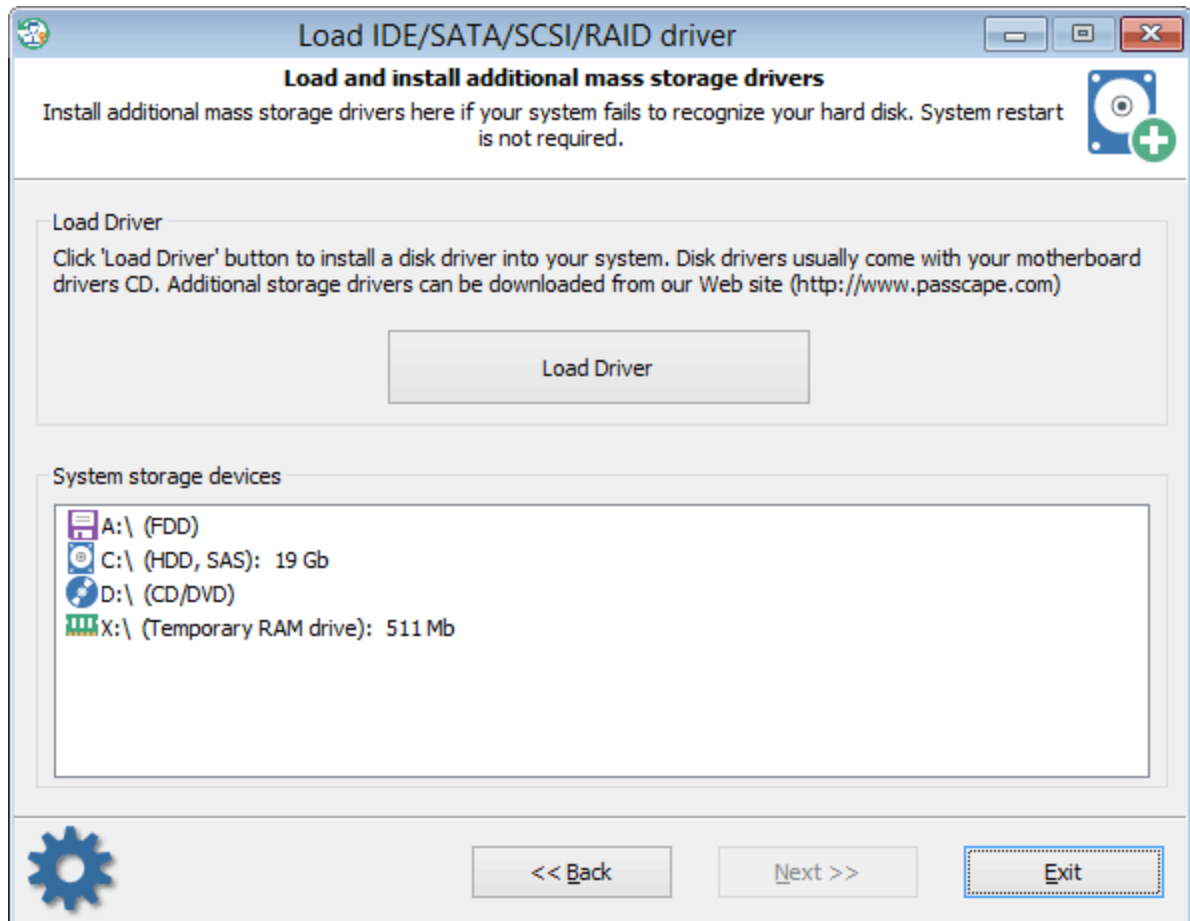


Note! SYSKEY resetting is an unsafe operation that affects the whole system security. For example after SYSKEY is reset, even if you can log on your system, you will not be able to decrypt your EFS protected files, all DPAPI-protected passwords (eg. Outlook saved passwords) will be discarded as well.

There are a number of programs in the Net that proclaim they can reset SYSKEY. But none of them works correctly at the moment. The reason is that SYSKEY resetting requires a lot of additional operations for your system to prevent it from being broken. For example you need also to zero out SAM domain session key(s), re-encrypt and reset local user hashes, LSA secrets, etc. **Reset Windows Password** has 2 algorithms for resetting SYSKEY. Once the primary one fails, another one runs. After SYSKEY is reset, all local user passwords will be set to blank automatically.

Note! After resetting SYSKEY on a Windows 8 and later OSes, you should change password for every LiveID/Microsoft account to a non-empty one. Otherwise you will not be able to log on the system with empty password.

3.18.6 Loading additional hard disk drivers



If when the application started it was unable to detect one or several hard disk drives, you will most likely need to install a driver for that device. In the main window, on the task list, select 'Load IDE/SATA/SCSI/RAID/NVME driver' and go to the driver installation dialog. The software comes with several popular hard drive controller drivers: ATI, Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware.

They all are stored in the folder **X:\Apps\Drivers**. For example, if your HDD controller is built upon the Nvidia chipset, load the corresponding *.INF file from the folder X:\Apps\Drivers\Nvidia.

Normally when you buy a new PC you get loaded with a CD with the motherboard and hard disk drivers. You can, and even are highly encouraged to use that disk for installing drivers for the missing devices. Be careful; the drivers should be compatible with Windows 10 x64 operating system! Please refer to the manual on your motherboard for more information on installing the drivers.

In Reset Windows Password drivers are installed 'on the fly'; therefore, rebooting the system is not required. Upon the completion, the found devices should appear on the list of data storage devices. Once the required driver is installed and the hard disk drive is found, you can go on with the next steps.

3.18.7 Unlock Bitlocker encrypted drives

Unlock BitLocker-encrypted drive

Unlock drives protected by BitLocker

In order to be able to use the BitLocker encrypted drives, you should provide volume password, recovery password, recovery key or certificate file.

Select the drive to unlock

Encrypted drive: F:\

Drive protectors: Volume unlock password, Recovery password

Select unprotection type

☐ I have a volume unlock password

☒ I have a recovery password

☐ I have a recovery key-file

☐ I have a certificate

Password: 092575-981932-611795-310511-854891-953186-117307-446237

Key file: [Browse]

Certificate file: [Browse]

PIN: []

[Extract BitLocker passwords from Active Directory](#)

<<<< Home << Back << UNLOCK >> Exit

BitLocker is a full drive encryption. It was first introduced in Windows Vista and is aimed to protect your data even if someone has physical access to your PC or laptop.

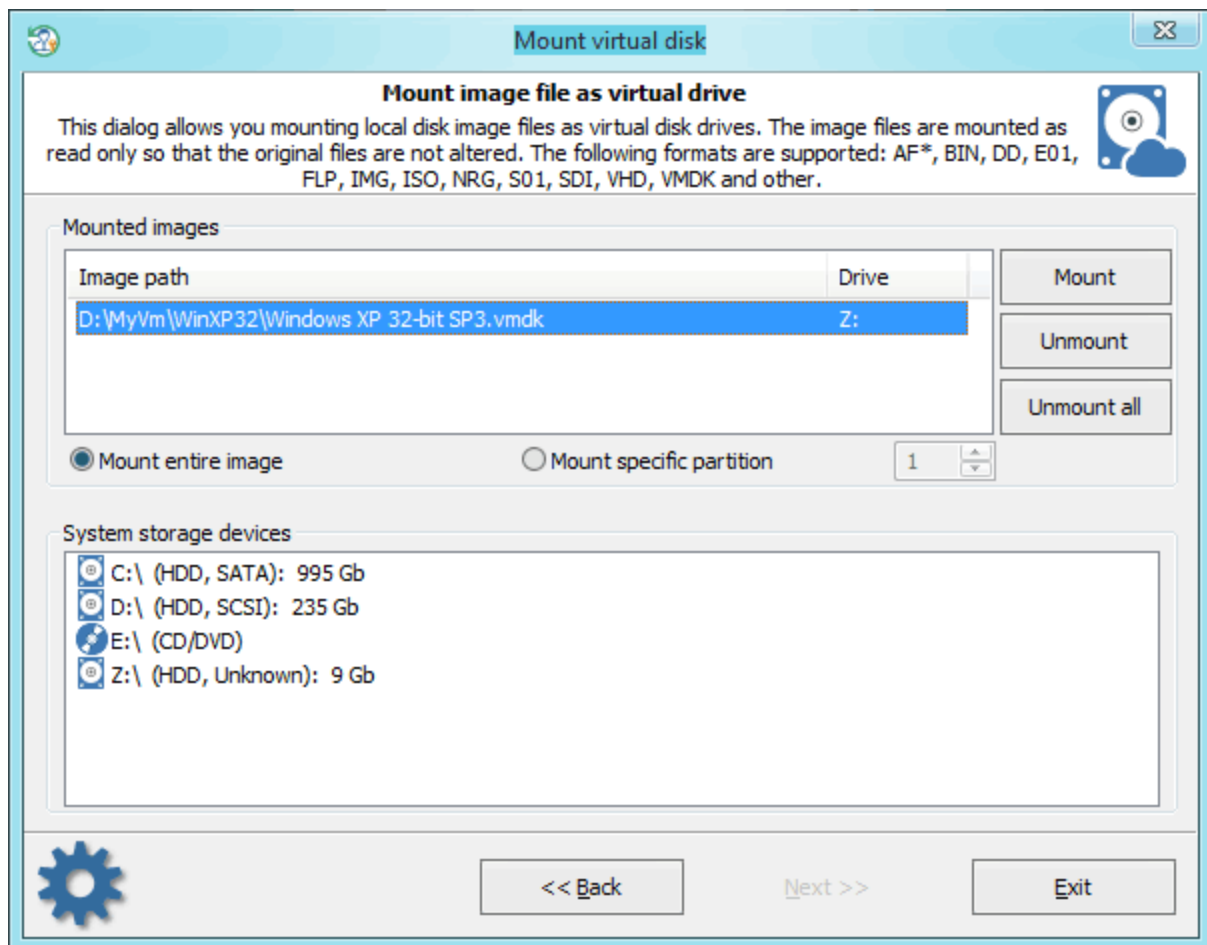
BitLocker encrypts all files on a drive, including those needed for startup. So its content is invisible to system. In order to unlock the drive and get access to its content, you should use one of the following unprotection methods:

- Unlock the drive with volume unlock password
- Unlock using recovery (numerical) password
- Unlock using external recovery key
- Unlock using BitLocker certificate

Just select your BitLocker-encrypted drive along with required unlock type and click << UNLOCK >> button to decrypt it. The operation takes several seconds.

To get a BitLocker recovery password stored in a domain, click the ['Extract BitLocker passwords from Active Directory'](#) link and follow the program's instructions.

3.18.8 Mounting virtual drives



This dialog allows you to mount a disk image to the system as virtual drive. You can then refer to the new drive by it's volume letter. Images are mounted as read-only so that the original file is not altered. The following formats are supported:
AF*, BIN, DD, E01, FLP, IMG, ISO, NRG, S01, SDI, VHD, VMDK and some others.

If you need to attach a BitLocker-encrypted image, first mount the image file and then [unlock it using a known recovery password or key](#).

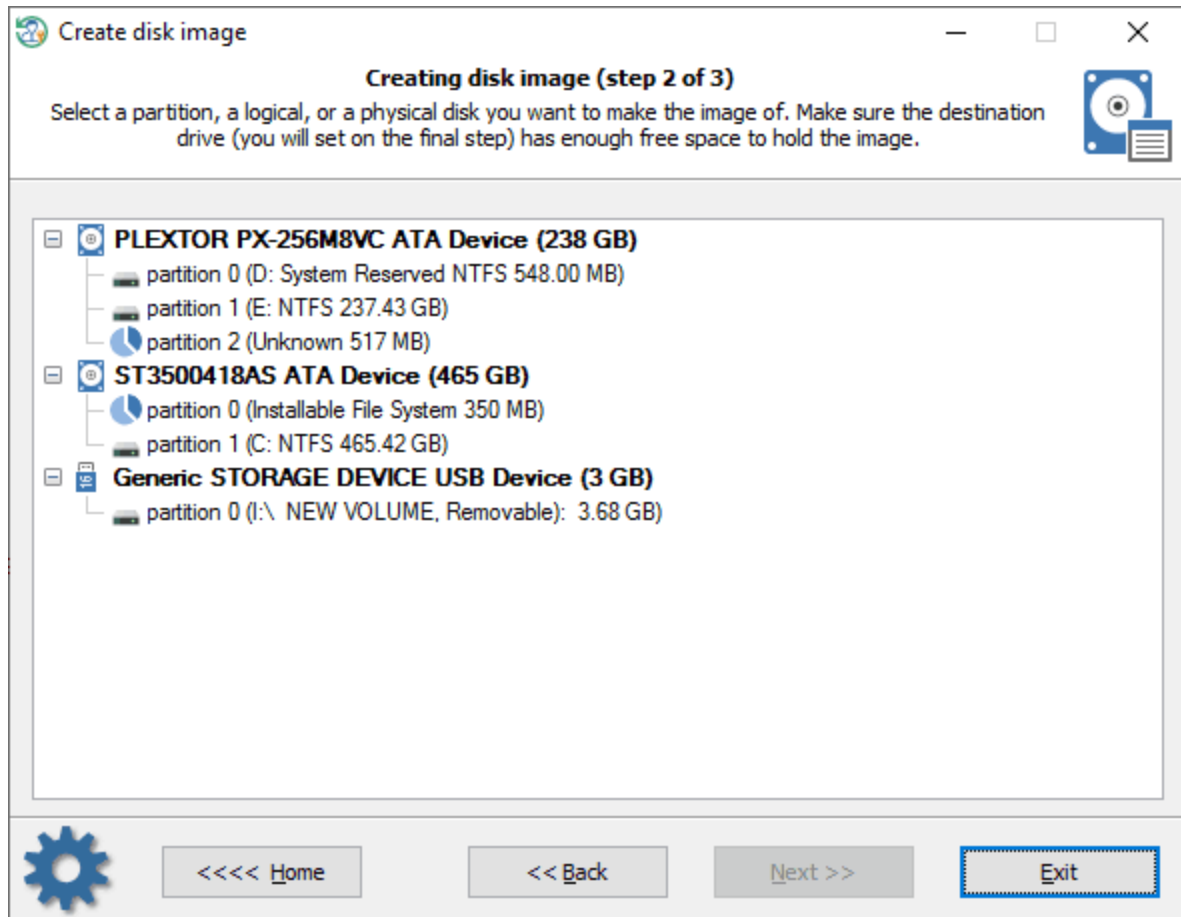
Be patient, mounting some image types may take up to several minutes to complete.

3.18.9 Create disk image

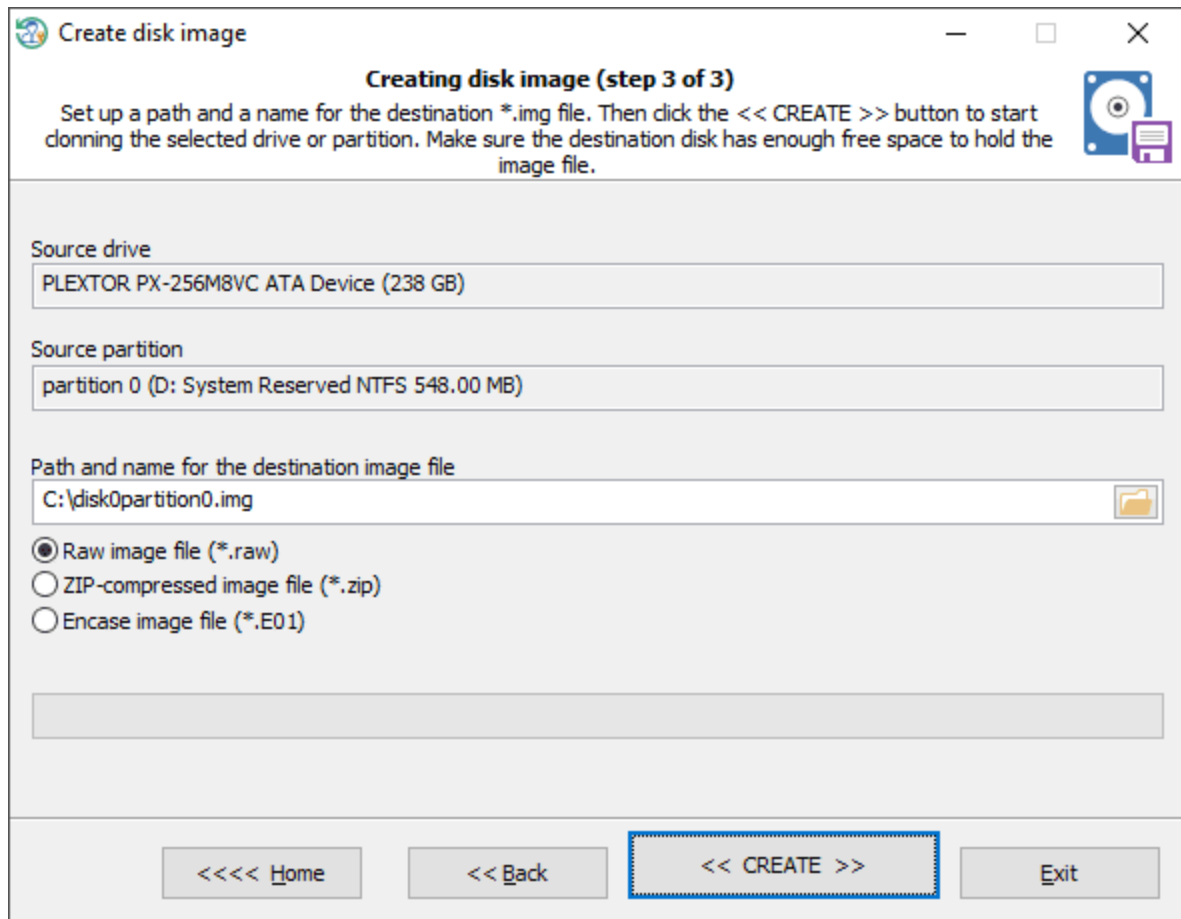
Sometimes when Windows becomes corrupt or your hard drive crashes, it is a nice idea to back up the entire content of your drive including disk encryption, OS state, settings, passwords, installed applications and drivers, all of your personal information, etc. One of the easiest ways to do it is to create an image of the entire hard drive.

In forensics, a disk image is a must-have and allows both saving some time during the initial investigation and ensuring nothing important will be missed during further in-depth analysis.

Creating a disk image in RWP is extremely simple.



At the first dialog, the program displays a list of found partitions and disk drives the partitions belong to. Select a partition or the disk whose image you want to create.



At the final dialog, set the name of the image and the destination path the image to save to. Note that the destination path should be located on another physical drive. Make sure you have enough free space to hold the entire image file. Click the '<< Create >>' button to start the disk image creation. Be patient, it may take some time and depends on the speed of your source and target drives.

Optionally, image compression is available. Once set, the output image file will be compressed to *.ZIP or to *.E01 file.

License and registration

4 License and registration

4.1 License Agreement

=====

SOFTWARE LICENSE AGREEMENT

=====

IMPORTANT-READ CAREFULLY: This is the End User License Agreement (the "Agreement") is a legal agreement between you, the end-user, and Passcape Software, the manufacturer and the copyright owner, for the use of the "Reset Windows Password" software product ("SOFTWARE").

All copyrights to SOFTWARE are exclusively owned by Passcape Software.

The SOFTWARE and any documentation included in the distribution package are protected by national copyright laws and international treaties. Any unauthorized use of the SOFTWARE shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution.

You are granted a non-exclusive license to use the SOFTWARE as set forth herein.

You can use trial version of SOFTWARE as long as you want, but to access all functions you must purchase the fully functional version. Upon payment we provide to you the download link and the registration code to the SOFTWARE .

Once registered, the user is granted a non-exclusive license to use the SOFTWARE on one computer at a time for every single-user license purchased.

With the personal license, you can use the SOFTWARE as set forth in this Agreement for non-commercial purposes in non-business, non-commercial environment. To use the SOFTWARE in a corporate, government or business environment, you should purchase a business license. With the business license you can run the SOFTWARE on multiple computers within a single organization.

The registered SOFTWARE may not be rented or leased, but may be permanently transferred together with the accompanying documentation, if the person receiving it agrees to terms of this license. If the software is an update, the transfer must include the update and all previous versions.

The SOFTWARE unregistered (trial) version may be freely distributed, provided that the distribution package is not modified. No person or company may charge a fee for the distribution of the SOFTWARE without written permission from the copyright holder.

You may not create any copy of the SOFTWARE. You can make one (1) copy the SOFTWARE for backup and archival purposes, provided, however, that the original and each copy is kept in your possession or control, and that your use of the SOFTWARE does not exceed that which is allowed in this Agreement.

You agree not modify, decompile, disassemble, otherwise reverse engineer the SOFTWARE, unless such activity is expressly permitted by applicable law.

Passcape Software does not warrant that the software is fit for any particular purpose. Passcape Software disclaims all other warranties with respect to the SOFTWARE, either express or implied. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, do the above limitations or exclusions may not apply to you.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our SOFTWARE or have permission from the legitimate owner to perform these acts. Any illegal use of our SOFTWARE will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequencial data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

All rights not expressly granted here are reserved by Passcape Software.

4.2 Registration

The software is available in three editions: Light, Standard and Advanced. The detailed list of features is [shown here](#). You can order fully registered version of Reset Windows Password at a cost of \$45 for Light Edition (personal usage), \$145 for Standard Edition (personal usage) or \$345 for Advanced Edition (business license).

Detailed instructions for all kinds of orders are available online at the [program's order page](#). Online orders are fulfilled in just a few minutes 24 hours a day 7 days a week. The ordering pages are on a secure server, ensuring that your confidential information remains confidential.

As soon as your order is processed, you will be provided with the link to the fully-featured version of the program. If you've made a payment, but haven't received a confirmation letter with the link within a reasonable amount of time, please notify us!

Important: when completing the order form, please double-check that your e-mail address is correct. If it will not, we'll be unable to send you the registration code.

To complete the registration process, you should download the program using the link that was sent to you in your registration e-mail and follow the [instructions to create a bootable disk](#).

4.3 Limitation of unregistered version

An unregistered version of the **Reset Windows Password** shows only first 3 characters of recovered passwords and has some functional limitations. In particular, only hashes dump and password backup features are working without any limitations. Registered version eliminates all restrictions.

4.4 Program editions

Reset Windows Password comes in three editions: Light, Standard and Advanced. The detailed list of features is shown below.

FEATURE	Light	Standard	Advanced
Support for Windows NT/2000/XP/Vista/7/8/10 workstations	+	+	+
Support for NT/2000/2003/2008/2012/2016/2019 servers	+	+	+
Windows 64-bit support	+	+	+
Non-US Windows support	+	+	+
Multilingual passwords support	+	+	+
Additional mass storage drivers	+	+	+
Detect multiple Operating Systems	+	+	+
Extended download warranty	+	+	+
14-day money back guarantee	+	+	+
License	personal	personal	business
Support for all types of Windows accounts, including Live ID, Microsoft account, etc.	+	+	+
Create a bootable password reset CD/DVD	+	+	+
Create a bootable password reset USB	+	+	+
Create a bootable password reset HDD	+	+	+
Support booting on UEFI-based computers	+	+	+
Reset local Administrator password	+	+	+
Change local Administrator password	+	+	+
Unlock disabled, locked or expired local Administrator account ⁽¹⁾	+	+	+
Reset Domain Administrator password	-	-	+
Change Domain Administrator password	-	-	+
Unlock disabled, locked or expired Domain Administrator account ⁽¹⁾	-	-	+
Change a desktop account extended properties and flags	+	+	+
Change extended properties and flags of Active Directory accounts	-	-	+
Reset password to regular (SAM) accounts	+	+	+
Change passwords to regular (SAM) accounts	+	+	+
Unlock disabled, locked or expired SAM account ⁽¹⁾	+	+	+
Decrypt secret questions and answers for Windows 10 OS	+	+	+
Reset password to Active Directory accounts	-	-	+
Change passwords to Active Directory accounts	-	-	+
Unlock disabled, locked or expired Active Directory accounts ⁽¹⁾	-	-	+
Reset/Change password to DSRM ⁽²⁾ account	-	-	+
Reset domain cached password	-	+	+
Change domain cached password	-	+	+

FEATURE	Light	Standard	Advanced
Instant load and install any IDE/SATA/SCSI/RAID driver	+	+	+
Roll back changes (restore previously modified passwords)	+	+	+
Support SYSKEY encryption	+	+	+
Support SYSKEY startup password decryption	+	+	+
Support SYSKEY floppy decryption	+	+	+
Show password hints	+	+	+
Dump LM/NTLM password hashes for regular (SAM) accounts	+	+	+
Dump password history hashes	-	+	+
Dump domain cached credentials (MSCACHE)	-	+	+
Dump LM/NTLM password hashes for Active Directory accounts	-	-	+
Password recovery for Active Directory user accounts ⁽³⁾	-	-	+
Password recovery for regular (SAM) user accounts	-	+	+
Password recovery for domain cached accounts	-	-	+
Search for simple passwords	-	+	+
Primitive dictionary analysis	-	+	+
Advanced dictionary analysis ⁽⁴⁾	-	-	+
Primitive brute-force attack against user passwords	-	+	+
Recover passwords using Artificial Intelligence analysis	-	+	+
Password recovery using custom attacks including dictionary, hybrid and mask attacks	-	+	+
Remove password history hashes out of regular (SAM) accounts	-	+	+
Remove password history hashes out of Active Directory accounts	-	+	+
Remove domain cached passwords	-	+	+
Remove cached logon passwords	-	+	+
Remove password reset information	-	+	+
Remove password hints	-	+	+
Reset SYSKEY security (with user passwords re-encryption)	-	+	+
Lookup SYSKEY startup password	-	+	+
Instant plaintext password recovery for accounts with Picture password	-	+	+
Instant plaintext password recovery for accounts with Biometric logon ⁽⁵⁾	-	+	+
PIN recovery	-	+	+
Decrypt PIN history ⁽⁸⁾	-	+	+
Mount virtual drives	+	+	+
Automatic detection and mounting virtual OSes	+	+	+
Search for virtual machines passwords	-	+	+
Search for lost product keys and serial numbers	-	+	+
Convert Microsoft Live ID to local user account	+	+	+
Backup passwords, registry and Active Directory	+	+	+

FEATURE	Light	Standard	Advanced
Search for password-protected documents	+	+	+
Search for recently opened documents ⁽⁷⁾	+	+	+
Password recovery for MS Office, OpenOffice, LibreOffice, MyOffice, and PDF documents	-	+	+
Password lookup and recovery for Indian Aadhaar and e-pan cards	-	+	+
Search and decrypt Internet browser passwords	-	+	+
Search and decrypt passwords for popular e-mail clients	-	+	+
Search and decrypt different network passwords	-	+	+
Create new SAM accounts	-	+	+
Unlock BitLocker drives	+	+	+
Extract BitLocker recovery passwords from Active Directory	-	-	+
Windows logon options	-	+	+
Local password policy editor	-	+	+
Domain password policy editor	-	-	+
Logon policy editor	-	+	+
Interface and system restriction policy editor	-	+	+
Support for passwordless sign-in option	+	+	+
Decrypt Windows Hello credentials ⁽⁸⁾	-	+	+
Logon history and statistics ⁽⁶⁾	+	+	+
Hardware history ⁽⁷⁾	+	+	+
Software history ⁽⁷⁾	+	+	+
Network history ⁽⁷⁾	+	+	+
Recent user activity ⁽⁶⁾	+	+	+
Search for recently opened documents ⁽⁷⁾	+	+	+
View program execution timeline ⁽⁷⁾	+	+	+
System events ⁽⁶⁾	+	+	+
Web history ⁽⁶⁾	+	+	+
Last modified files	-	+	+
Last modified directories	-	+	+
Create disk images in raw format	+	+	+
Create disk images in *.E01 format	-	+	+
Program's access password	+	+	+
Price	\$45	\$145	\$345

Notes:

- (1) If the account is locked, disabled or expired
- (2) Directory Services Restore Mode
- (3) If Reversible Encryption is set. You can find this option in your domain password policy.
- (4) Using Arabian, Chinese, English, French, German, Portuguese, Russian, Spanish dictionaries.
- (5) Not for all accounts
- (6) Data export feature is available in Advanced edition only

- (7) Data export feature is available in Standard and Advanced editions only
- (8) If not protected with TPM

Technical support

5 Technical support

5.1 Reporting problems

If you have a problem, please contact us at support@passcape.com. Please inform us about the following:

- Windows version including service packs and other fixes installed
- Program full version (see **About** dialog)
- Program registration information if any
- Detailed description of your problem (as much information as possible)

If you're reporting an error, please attach **RWPCrash.log** file(s) that was saved during an unhandled exception.

5.2 Suggesting features

If you have any questions, comments or suggestions about the program or would like more information, email us at info@passcape.com. Please don't forget to mention the program name and version. Also make sure you have the latest program version installed. Your feedback helps us to improve our products and work more effective.

5.3 Contacts

Please don't hesitate to send your questions regarding our products to e-mail support@passcape.com. You will get reply during one or two days. Note, that registered users have priority in technical support.

If you experience any problems during registration process, please send a letter to sales@passcape.com. We will be happy to assist you with the registration.

Please write in English!

You can find other password recovery utilities at <https://www.passcape.com>.

© 2021 Passcape Software. All rights reserved.