Reset Windows Password

MANUAL DE USUARIO

Passcape Software

Introducción

1 Introducción

1.1 Acerca del Programa

Reset Windows Password fue desarrollado para restablecer, cambiar y recuperar contraseñas de inicio de sesión de Windows. Por ejemplo, cuando se pierde u olvida la contraseña del administrador del equipo. Restablecer contraseña de Windows es la solución más óptima y funcionalmente más rica de su clase. La aplicación es compatible con todas las versiones de Windows (basadas en NT), funciona con Active Directory y credenciales de caché de dominio, posee habilidades de inteligencia artificial para recuperar contraseñas al instante en ciertas cuentas y demuestra una serie de características únicas adicionales.

La interfaz de la aplicación se lleva a cabo tradicionalmente en forma de un asistente paso a paso. Por lo tanto, el proceso de operación no parece complicado incluso para un usuario inexperto. Por ejemplo, restablecer una contraseña de administrador solo requiere tres sencillos pasos:

1. Seleccione los archivos SAM y SYSTEM (la aplicación busca automáticamente los archivos de registro en todos los discos duros).
2. Seleccione la cuenta de usuario.
3. Restablecer o modificar la contraseña.

Utilizando una utilidad incorporada, puede crear fácilmente un CD, DVD o disco USB de arranque (incluidos dispositivos como Compact Flash, SmartMedia, SONY Memory Stick, Secure Digital, unidades ZIP, unidades de disco duro USB, etc.) en unos pocos minutos, a partir de una imagen ISO existente con el programa. Reset Windows Password tiene una interfaz gráfica de usuario, admite la carga de volúmenes IDE, SATA, SCSI, RAID sobre la marcha, es compatible con los sistemas de archivos FAT, FAT32, NTFS, NTFS5, va con una gran colección de controladores de disco duro de Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware.

1.2 Caracteristicas y Beneficios

Application's advantages:

- Compatibilidad con todas las versiones de Windows basado en NT.
- Soporte para Windows de 32/64 bits.
- Gran colección de controladores de disco duro. Carga controladores adicionales desde la aplicación.
- Restablecer y modificar contraseñas de usuarios locales y de dominio, administrador local, administrador de dominio, otras cuentas de Active Directory.
- Habilite y desbloquee cuentas de usuario, tanto administradores locales como de dominio.
- Deshabilite las opciones de caducidad de la contraseña.
- Detectar varios sistemas operativos.
- Soporte para versiones de Windows no inglesas y contraseñas en codificación nacional.
- Volcar hashes de contraseña de usuario de SAM para un análisis más detallado.
- Volcar hashes de contraseña desde Active Directory.
- Volcar contraseñas almacenadas en caché de dominio.
- Varios módulos para extraer y descifrar contraseñas de texto sin formato de Active Directory.
- Permitir deshacer los cambios realizados en el sistema.
- Elimine contraseñas y otros datos confidenciales de la PC.
- Algoritmos avanzados de búsqueda y recuperación de contraseñas.
- Restablecer la seguridad de SYSKEY.

- Recuperación de la contraseña de inicio de SYSKEY.
- Busque claves de serie perdidas.
- Busque contraseñas de red.
- Busque contraseñas de máquinas virtuales.
- Copia de seguridad del registro/Active Directory y otra información confidencial.
- Desbloquear unidades Bitlocker.
- Ver la actividad del usuario, diferente información forense.
- Búsqueda y recuperación de contraseñas para documentos MS Office, OpenOffice, LibreOffice, MyOffice y PDF.
- Edite la política de contraseñas locales o de dominio, así como las restricciones del sistema y la interfaz.

El software está disponible en tres ediciones: **Light**, **Standard** y **Advanced**. La lista detallada de características para cada edición está disponible aquí.

1.3 Requerimientos del Sistema

Requisitos
Microprocesador basado en x64, un mínimo de 1 GB de RAM, CD-ROM o unidad USB. El tamaño de la unidad USB de arranque debe ser de 512 Mb o más (se recomienda una memoria USB de 2-32 Gb para una mejor compatibilidad). El BIOS de la computadora debe admitir el arranque desde un CD, DVD o dispositivo USB.

Compatibilidad
Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7/8/10, Windows Server 2000/2003/2008/2012/2019. Sistemas de archivos: FAT, FAT32, NTFS, NTFS5. El programa es compatible con la mayoría de las grabadoras de CD / DVD y dispositivos USB, incluidos Memory Stick, Compact Flash, SmartMedia, Secure Digital, unidades flash USB, unidades USB ZIP, unidades de disco duro USB, etc.

Restricciones
Una vez que su sistema utiliza un dispositivo de almacenamiento masivo no estándar, es posible que deba especificar un controlador de terceros compatible con Windows 10. Consulte el manual de la placa base para obtener más detalles.

Problemas o errores conocidos
- Si tiene 2 o más discos lógicos en el sistema, las letras de los discos se pueden reasignar/volver a asignar.
- Si está restableciendo una contraseña de la cuenta de administrador integrada en algunas ediciones de Windows, tenga en cuenta que para activar la cuenta de administrador integrada e iniciar sesión en el sistema, deberá cargar el sistema en modo seguro.
- El programa es compatible con todos los tipos de cifrado SYSKEY. En algunos casos, es posible que deba proporcionar la contraseña de inicio de SYSKEY o el disquete de inicio. Sin embargo, el programa también permite restablecer / buscar la contraseña de SYSKEY. Entonces, incluso si olvidó su SYSKEY, no es un problema.
- Después de restablecer la contraseña de una cuenta local, puede perder el acceso a las contraseñas de la página Web, la red inalámbrica y las credenciales de uso compartido de archivos, los archivos cifrados con EFS, los mensajes de correo electrónico cifrados con claves privadas. Consulte la Base de Conocimientos de Microsoft para obtener más información.

- El restablecimiento de las contraseñas de Active Directory para determinadas cuentas puede no tener ningún efecto. Por ejemplo, en un RODC.
- El restablecimiento de contraseña (así como otras características que implican operaciones de escritura en disco) en un sistema operativo virtual no tendrá ningún efecto.
- Al restablecer una contraseña para la cuenta Microsoft, debe proporcionar una contraseña no vacía. De lo contrario, no podrá iniciar sesión en el sistema.

Creando un entorno de arranque

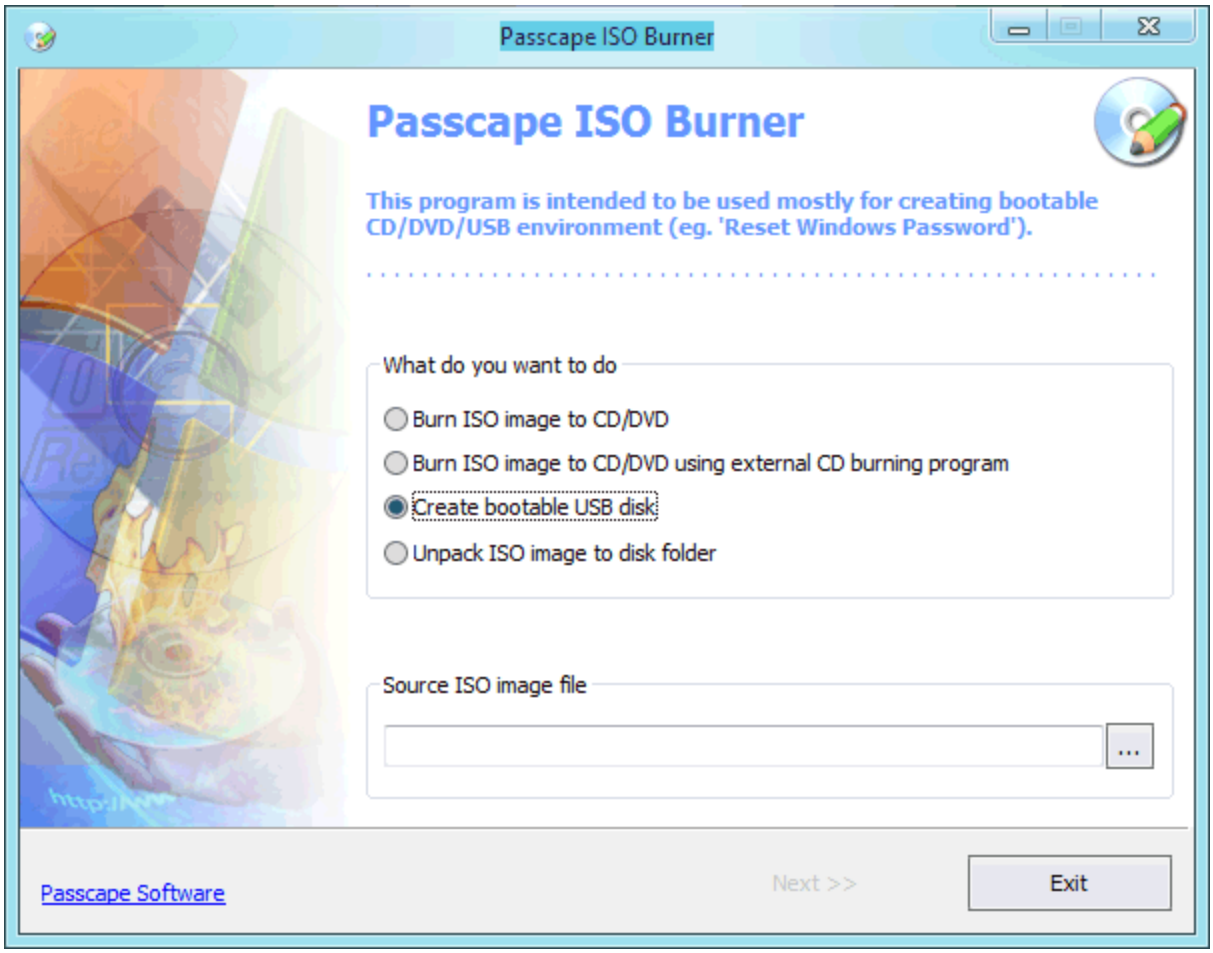
2 Creando un entorno de arranque

2.1 3 simples pasos para lanzar la aplicación desde un disco de arranque

1. Descargue el paquete Reset Windows Password en https://www.passcape.com/download/rwp.zip (o utilizando el enlace que se le envió en el correo electrónico de registro)
2. Crear disco de arranque RWP: descomprima el RWP. ZIP, ejecute IsoBurner.exe, seleccione un elemento para crear CD / DVD / USB de arranque, especifique la ruta a la imagen ISO desempaquetada y grábela en el disco.
3. Inicie el equipo de destino y cambie la configuración del BIOS/UEFI para que el dispositivo de arranque (CD-ROM, DVD-ROM o disco USB) sea el primero en la lista. Guarde la configuración, reinicie una vez más para iniciar el programa desde su CD, DVD o disco USB de arranque. Puede utilizar la opción de arranque rápido si su BIOS/UEFI admite la selección rápida de medios de arranque durante el inicio.

2.2 Creando disco de arranque RWP

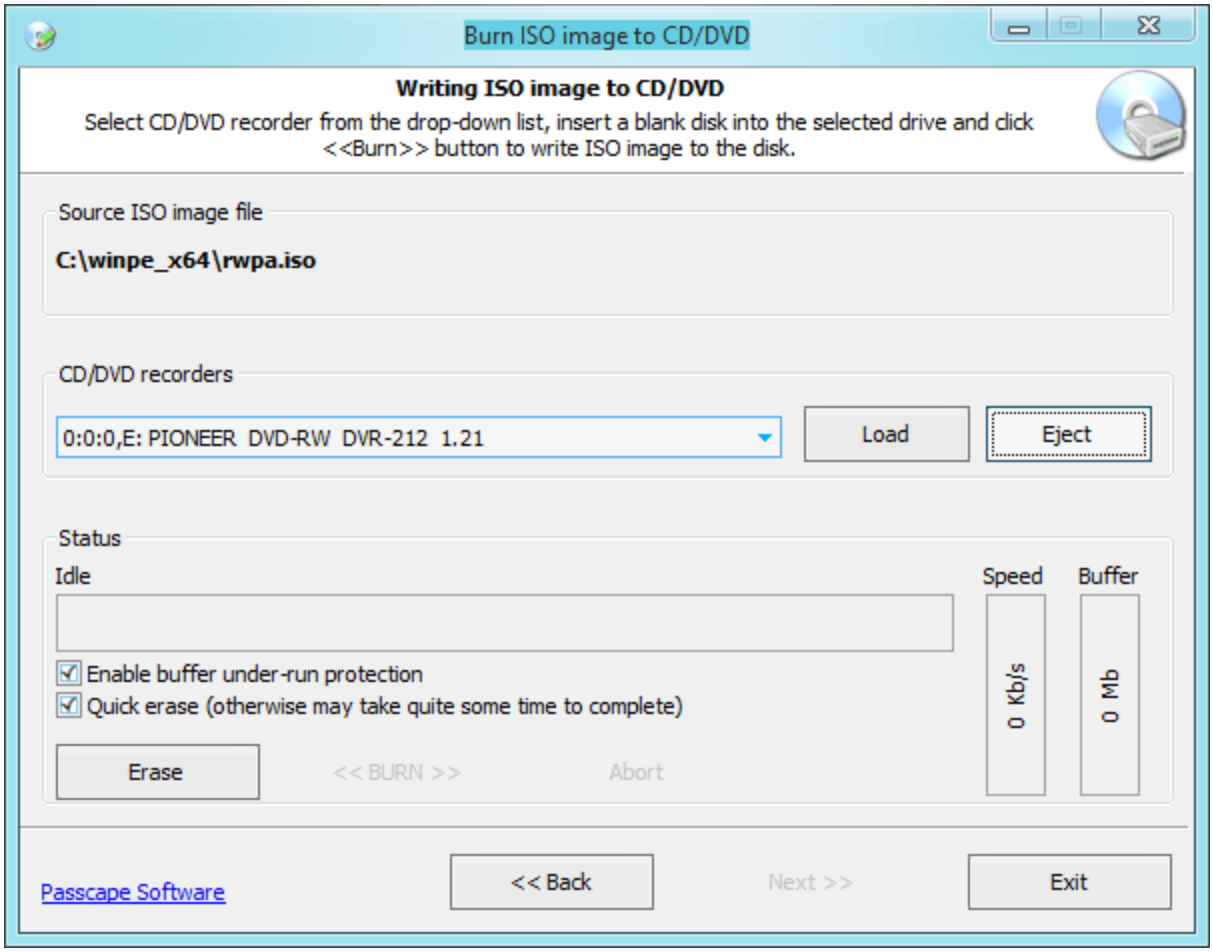
Passcape ISO Burner



Passcape ISO Burner es un programa para crear discos CD, DVD o USB de arranque a partir de imágenes ISO-9660. El programa es gratuito y viene con RWP. también está disponible para su descarga y uso en nuestro sitio web: https://www.passcape.com/download/pib.zip

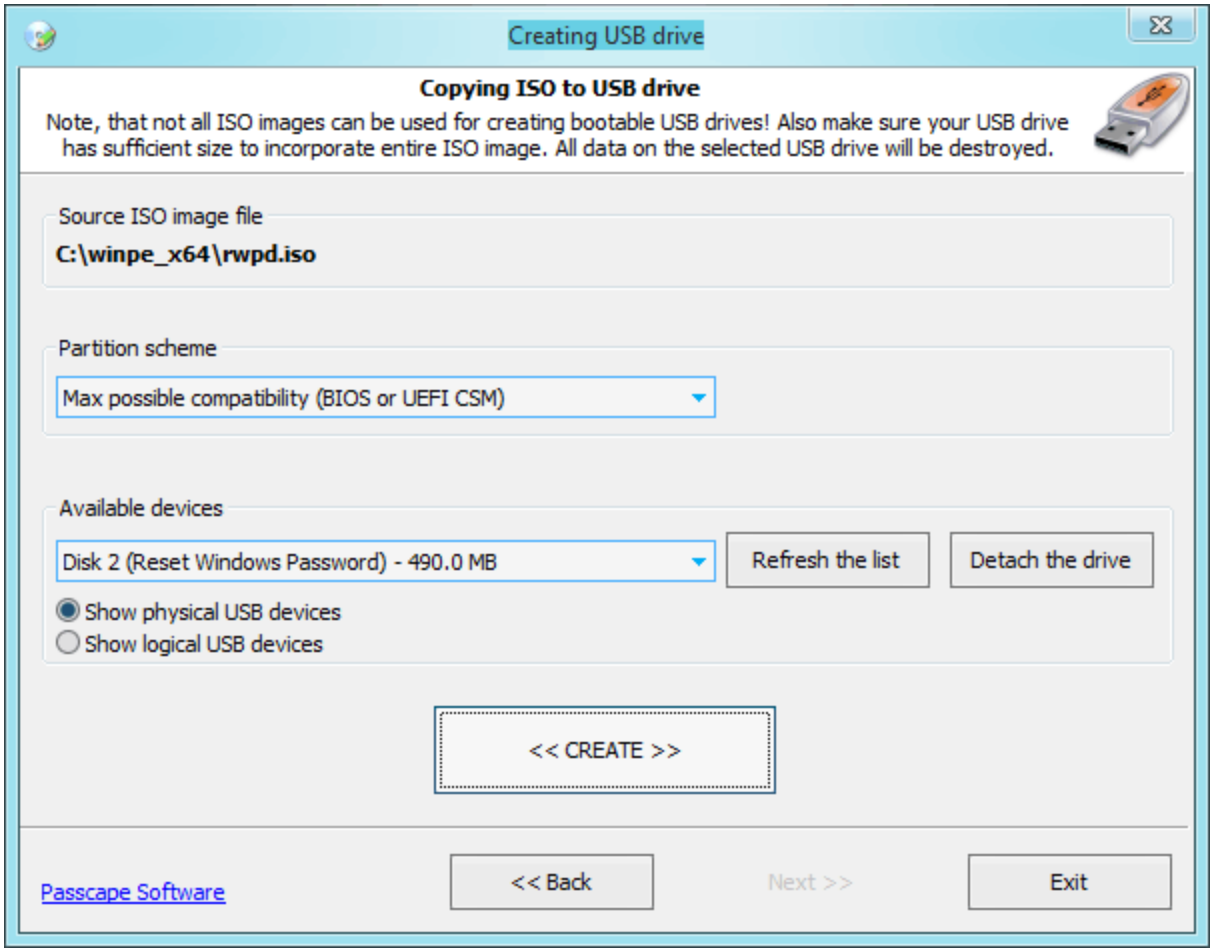
La interfaz de la aplicación es muy simple. Cuando se inicia, la aplicación le pide que seleccione lo que le gustaría hacer:
- Grabar imagen ISO en CD / DVD usando esta aplicación
- Grabe la imagen ISO en CD / DVD utilizando una aplicación de grabación externa instalada en su computadora. Por ejemplo, Nero o su análogo libre ImgBurn.
- Utilice la imagen ISO para crear un disco de arranque USB
- Extraer imagen ISO al disco (tenga en cuenta que esta acción provoca la pérdida de datos de arranque).

Creando disco de arranque de Reset Windows Password



Seleccione el primer elemento del menú: '*Grabar imagen ISO a CD/DVD*'. En la parte inferior de la pantalla, ingrese la ruta al archivo con la imagen ISO. Eso habilita el botón '*Siguiente*', y puede pasar a crear realmente el disco. Todo lo que necesitamos hacer aquí es seleccionar la grabadora que vamos a usar, insertar un CD / DVD en blanco en ella y hacer clic en el botón <<GRABAR>> para crear un disco de inicio a partir de la imagen ISO seleccionada en el paso anterior

Creando USB de arranque de Reset Windows Password



Seleccione la imagen ISO de arranque existente con el programa y marque la opcion '*Crear disco USB de arranque*'. Introduzca el número de serie del producto si tiene uno. Cuando aparezca la siguiente ventana, conecte el dispositivo USB a su computadora; debería aparecer automáticamente en la lista de dispositivos USB encontrados. Haga clic en el botón '*Crear*' para formatear y crear el USB de arranque. En algunos casos (por ejemplo, si el dispositivo USB está instalado como una unidad de disco duro y se encuentra una entrada de partición extendida en ese disco), la aplicación requerirá reiniciarse para reasignar las letras de la unidad.

El programa ofrece varios esquemas de partición (modos de formateo) para proporcionar una mejor compatibilidad al arrancar desde dispositivos USB. Si no está seguro acerca de qué esquema de partición seleccionar, considere usar el siguiente algoritmo simple:
- Si el PC de destino se basa en interfaz UEFI (gráfica), seleccione el modo 'Compatibilidad máxima con nuevos PC (FAT32 MBR para UEFI)'. Este esquema creará un USB para ejecutarse en PC basadas en UEFI donde el modo de arranque seguro está activado.
- Si su PC de destino se basa en interfaz BIOS (textual), seleccione el modo 'Compatibilidad máxima con PC antiguos (FAT32 MBR para BIOS)'. Este modo creará un USB que es totalmente compatible con el firmware del BIOS.
- Si no sabe nada sobre la PC de destino, cambie al esquema 'Máxima posible compatibilidad'. Este modo crea USB de arranque que pueden ejecutarse en equipos basados en BIOS y UEFI (con **Modo de soporte de compatibilidad** seleccionado). En algunos PC o portátiles, el **Modo de soporte de**

compatibilidad también se conoce como modo de arranque heredado.

Si compró su PC después de 2010, lo más probable es que venga con UEFI. Los nuevos equipos utilizan firmware UEFI en lugar del BIOS tradicional. Ambos son software de bajo nivel que se inicia cuando arranca su PC y se utilizan para "comunicarse" con el hardware. A diferencia de BIOS, UEFI es una solución más moderna con interfaz gráfica, que admite discos duros más grandes, tiempos de arranque más rápidos y más funciones de seguridad.

¡Ten cuidado! Se sobrescribirán todos los datos de la unidad de destino. Si la aplicación no puede detectar archivos de arranque en la imagen ISO de origen, mostrará la advertencia respectiva.

¡Algunos programas antivirus / antimalware bloquean la creación de discos de arranque o la copia de algunos archivos de arranque a los medios, incluso sin advertencias en pantalla!

2.3 Cambio de la configuración de BIOS/UEFI

Información general

Para cargar Reset Windows Password, es posible que deba ajustar la configuración de BIOS/UEFI de su computadora para que el dispositivo de arranque (CD, DVD o USB) sea el primero en la lista de dispositivos. Esta es la rutina a seguir para eso:

1. Al arrancar el equipo, presione la tecla Supr para ingresar al menú del BIOS. Algunas versiones del BIOS utilizan otras teclas de acceso rápido; esos podrían ser F2, F10, F11, ESC, etc. La sugerencia se muestra normalmente en la parte inferior de la pantalla de arranque.
2. Ingrese al BIOS/UEFI, luego en el menú busque el elemento que está a cargo de los dispositivos de arranque iniciales. Edítelo para hacer que el CD o USB con Reset Windows Password sea el primero en la lista
3. Asegúrese de haber guardado los cambios y, a continuación, reinicie el equipo.

Si su PC utiliza firmware UEFI, puede usar el interruptor de selección de arranque rápido sin alterar ninguna configuración. Para obtener más información, consulte el manual del usuario de la placa base de su computadora.

Configuración del BIOS, preguntas y respuestas

P: El BIOS de mi computadora tiene varios elementos para arrancar desde dispositivos USB: USB FDD, USB ZIP, USB HDD, USB CDROM. ¿Cuál debe seleccionarse?
R: Diferentes fabricantes de BIOS configuran el arranque inicial de diferentes maneras. En la mayoría de los casos, para arrancar desde un flash normal: en placas base antiguas, deberá seleccionar la opción USB ZIP; en algunos otros - USB HDD.

P: La aplicación tarda demasiado tiempo (a veces hasta 10 minutos) en arrancar desde un medio USB.
R: Eso indica que el dispositivo se ejecuta sobre el protocolo USB lento, 1.1. En primer lugar, el dispositivo de almacenamiento debe ser compatible con la especificación 2.0+. En segundo lugar, el puerto USB de la placa base donde se conecta el dispositivo de almacenamiento debe ser compatible con la especificación 2.0+. Y en tercer lugar, debe habilitar el soporte USB 2.0 (o superior) en el BIOS.

P: La computadora no arrancaría desde dispositivos USB en absoluto. Al intentar arrancar, ya sea en pantalla negra o en el mensaje de error 'sin sistema operativo'.
R: Intente encontrar la opción 'Detección de almacenamiento USB heredado' y haga que esté 'Habilitada'. En las opciones de arranque, solo debe tener un dispositivo USB. Si tiene dos o más dispositivos USB conectados a la computadora (por ejemplo. UPS, impresora, escáner, módem, etc.),

deje solo un disco USB de arranque. Desconecte el dispositivo USB de la computadora, apague la computadora, conecte el dispositivo USB a un puerto USB diferente, encienda su computadora e intente arrancar nuevamente. Si eso no ayudó, actualice su BIOS. También existe la posibilidad de que su placa base no admita el arranque desde dispositivos USB o no admita el sistema de archivos utilizado en este dispositivo de almacenamiento USB.

P: Pantalla azul o negra, todo tipo de controladores, carga de registro, etc. se producen errores al arrancar desde CD o USB.
R: Tal vez su computadora no tiene suficiente memoria. El mínimo requerido por la aplicación es de 1 GB de RAM. Para ejecutarlo con comodidad, necesitaría 2 GB o más.

P: No puedo entrar en mi BIOS. Se requiere una contraseña.
R: Una sorpresa desagradable puede ver por usted cuando intenta modificar la configuración del dispositivo de arranque en el BIOS. El asunto es que algunos fabricantes de hardware, vendedores o propietarios anteriores de la PC pueden haber establecido sus propias contraseñas para acceder al BIOS. En otras palabras, para modificar la configuración del BIOS, tendría que ingresar esa contraseña, que generalmente no es posible averiguar.
Algunas versiones del BIOS permiten restablecer su configuración presionando una determinada tecla en el teclado; normalmente eso es Ins. Para algún tipo de BIOS AMI es una combinación Ctrl+Alt+Supr+Ins. En AWARD BIOS, la tecla debe presionarse y mantenerse presionada hasta que se encienda la computadora. Eso cargará la configuración predeterminada. Sin embargo, esta opción debe usarse con mucho cuidado, ya que restablece todas las demás configuraciones del BIOS. Sin embargo, esta opción debe usarse con mucho cuidado, ya que restablece todas las demás configuraciones del BIOS.
Además, hay contraseñas universales de puerta trasera. Se proporcionan a continuación para muchas versiones antiguas populares de BIOS. Si no lo sabe, el tipo y la versión del BIOS normalmente se muestran durante unos segundos durante el arranque inicial de la computadora en la parte inferior de la pantalla.
Si ninguna de las contraseñas universales ha funcionado, puede aprovechar el método descrito en muchos manuales de usuario de la placa base: simplemente restablezca la configuración del BIOS cortando el puente respectivo. Normalmente se encuentra cerca de la gran batería CMOS. Si la placa base no tiene una batería CMOS, busque el microchip con la marca Dallas u Odin; el saltador debe estar en algún lugar cercano. Simplemente quitar la batería CMOS no siempre ayuda, ya que el microchip BIOS puede vivir durante varias horas sin la energía. Además, se desaconseja encarecidamente que cortocircuite el CMOS en sí para restablecer la configuración del BIOS, ya que eso puede reducir la duración de la batería esencialmente.
En la red, puede encontrar una serie de soluciones de software para recuperar contraseñas y restablecer el BIOS. Por ejemplo, cmospwd y killcmos. Se le desaconseja restablecer todas las configuraciones del BIOS en las computadoras portátiles. Eso puede llevar a la paralización completa del sistema.

P: Aparece un error que indica que la CPU no es compatible con el modo de 64 bits o que ejecuta aplicaciones de 64 bits.
R: Restablecer contraseña de Windows ya no es compatible con CPU de 32 bits (pero sin embargo, es compatible con sistemas operativos de 32 bits). Póngase en contacto con el soporte técnico para obtener un enlace para la última versión compatible con 32 bits.

P: ¿Puedo arrancar una unidad CD/USB compatible con BIOS en UEFI?
R: Sí. Introduzca la configuración de UEFI (pulse ESC, F2 o SUPR). Abra el menú 'Arranque' y habilite la opción 'Iniciar CSM'. Ahora localice la pestaña 'Seguridad' y deshabilite 'Control de arranque seguro'. Guarde los cambios y restablezca su PC. Ingrese a la configuración de UEFI una vez más y asegúrese de que su unidad de DVD / USB esté disponible en la pestaña 'Arranque'. Algunas UEFI también tienen un menú de dispositivo de arranque (generalmente se inicia presionando F8) donde puede seleccionar su dispositivo y modo de arranque.

P: ¿Puedo crear una unidad USB que pueda arrancar tanto en BIOS como en UEFI?
R: Sí. Ejecute la herramienta IsoBurner y seleccione el esquema de partición 'Máxima posible compatibilidad' al crear un USB de arranque. Este modo crea USB de arranque que se pueden ejecutar en equipos basados en BIOS y UEFI (con el modo de compatibilidad activado). En algunos PC o portátiles, el modo de soporte de compatibilidad también se conoce como modo de arranque heredado.

P: USB no aparece como una opción de arranque en mi UEFI. ¿Cómo puedo habilitar el arranque de una memoria USB?
R: Parece que el USB se formateó en modo BIOS o UEFI CSM, pero su UEFI solo permite arrancar en modo de arranque seguro. Tendrá que permitir el arranque en modo heredado. En la configuración de UEFI, deshabilite tanto 'Arranque - Arranque rápido' como 'Seguridad - Arranque seguro' y habilite 'Modo de soporte de compatibilidad (CSM)' u opciones similares. Otra solución sería simplemente crear un USB de arranque utilizando el esquema 'Compatibilidad máxima con nuevas PC (FAT32 MBR para UEFI)'. Este esquema es totalmente compatible con el modo de arranque seguro UEFI.

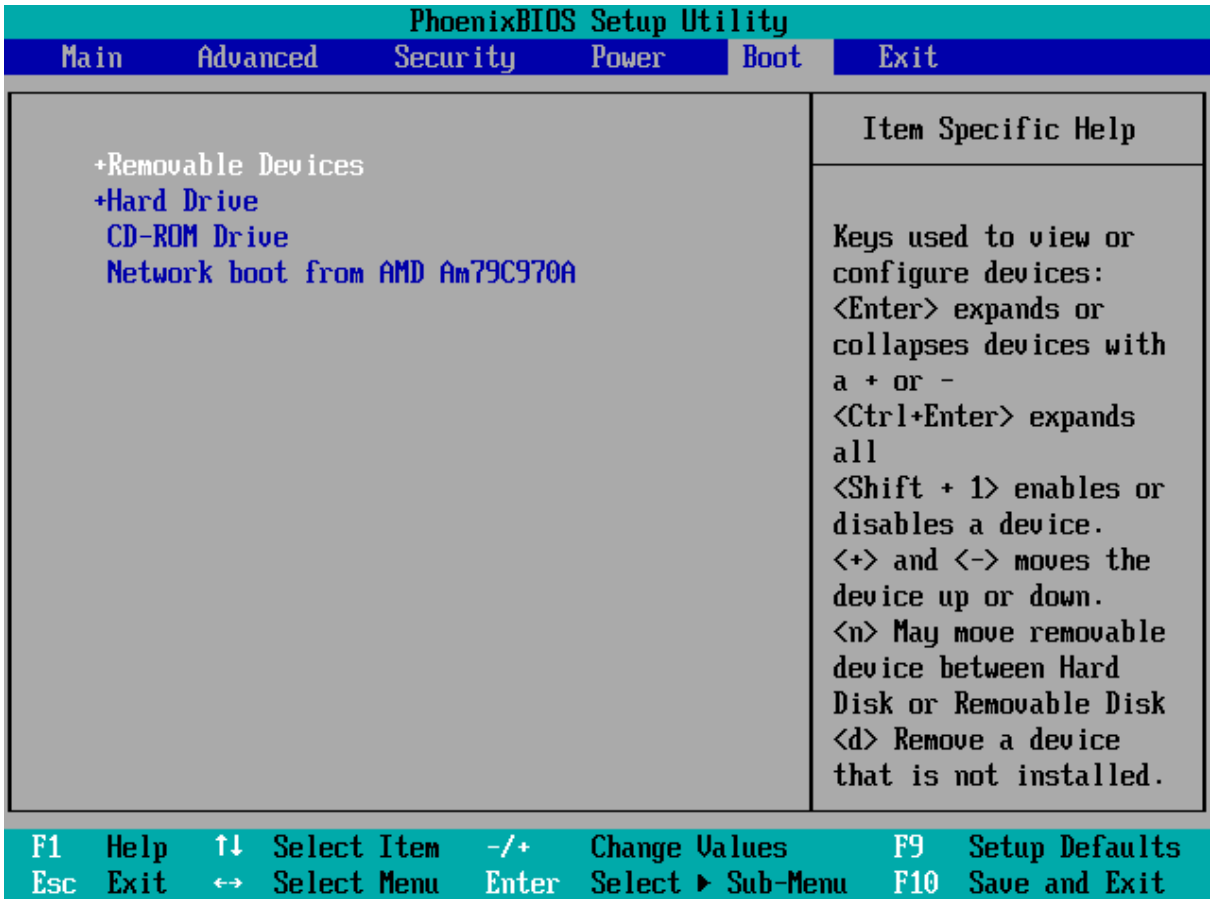
Contraseñas de puerta trasera de Bios

Fabricante del BIOS	Contraseña universal
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	HEWITTRAND, 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, ZJAADC, 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, helgaЯs, 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

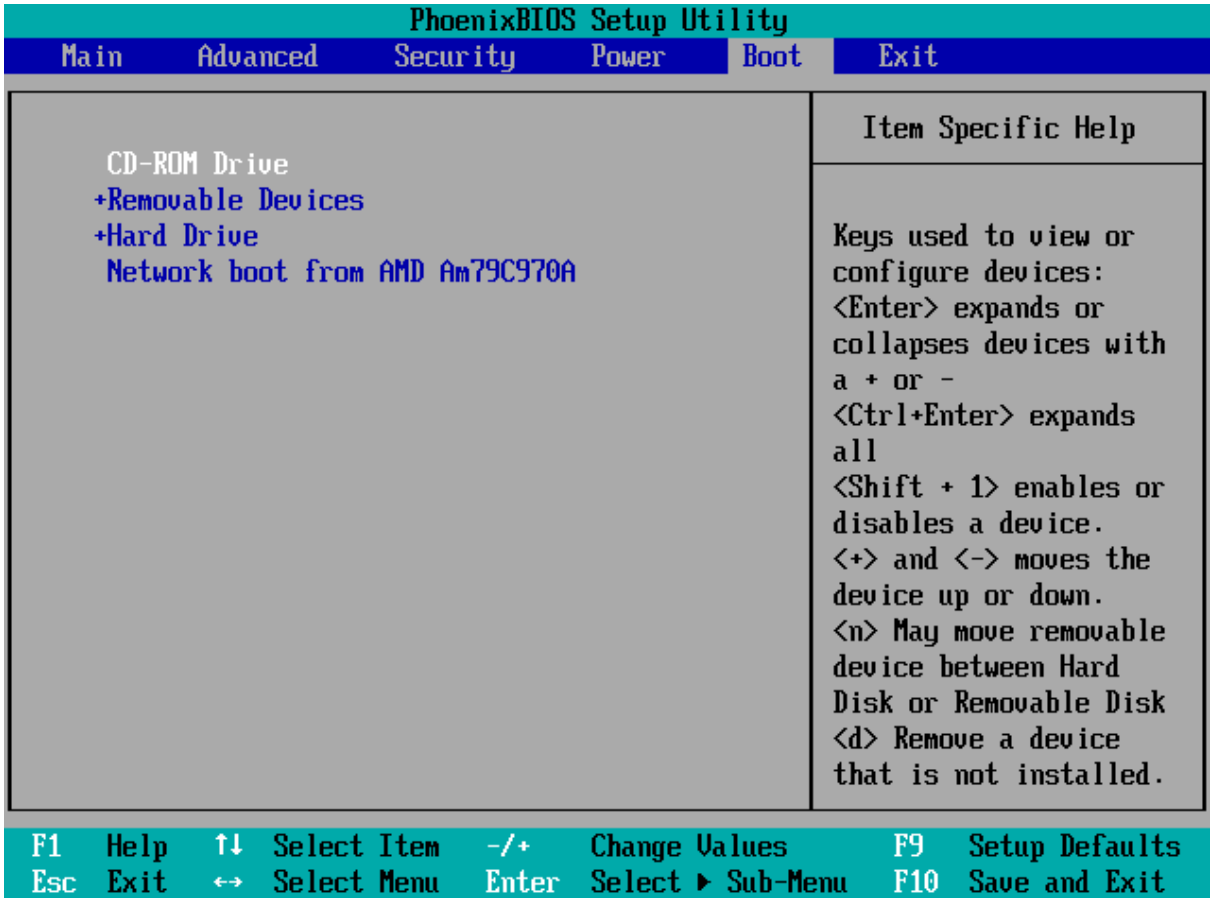
CTX International BIOS	CTX_123
CyberMax BIOS	Congress
Daewoo BIOS	Daewuu, Daewoo
Daytec BIOS	Daytec
DELL BIOS	Dell
Digital Equipment BIOS	komprie
Enox BIOS	xo11nE
Epox BIOS	Central
Freetech BIOS	Posterie
HP Vectra BIOS	hewlpack
IMB BIOS	IBM, MBIUO, sertafu
Iwill BIOS	iwill
JetWay BIOS	spooml
Joss Technology 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, xljlbj
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

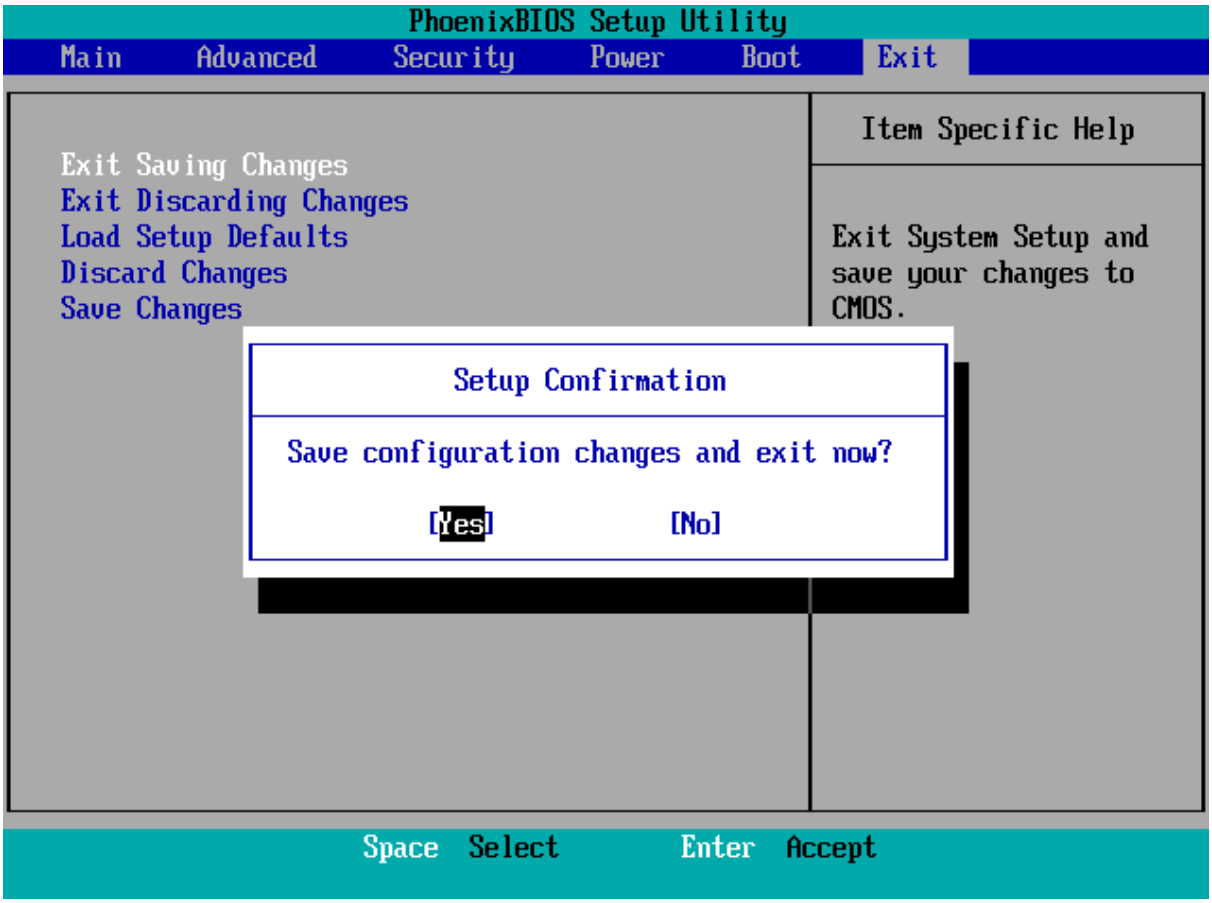
2.4 Ejecución del programa desde el CD/DVD/USB de arranque



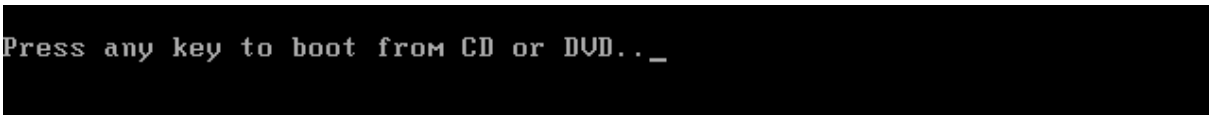
Encienda el equipo. Presione la tecla Supr para ingresar al menú del BIOS. Algunas versiones del BIOS utilizan otras teclas de acceso rápido; esos podrían ser F2, F10, F11, ESC, etc. La sugerencia se muestra normalmente en la parte inferior de la pantalla de arranque.



Editar menú de arranque en la forma de hacer que el CD o disco USB con Reset Windows Password sea el primero en la lista de dispositivos de arranque.



Asegúrese de haber guardado los cambios y, a continuación, reinicie el equipo.

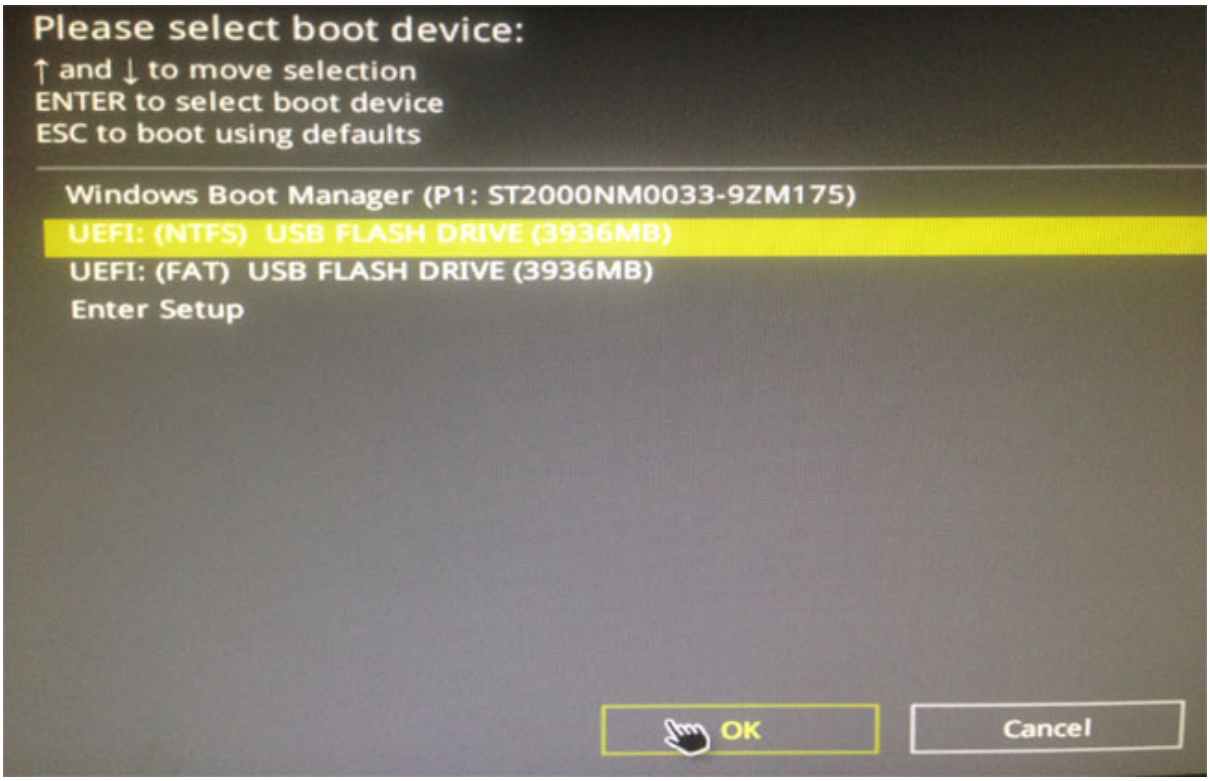


Si todo ha ido bien, verás el siguiente mensaje de texto. Presione cualquier tecla para cargar desde el disco de arranque de Reset Windows Password. De lo contrario, su antiguo sistema operativo se iniciará.

RWP se ha cargado correctamente y está listo para usar.

2.5 Ejecución del programa mediante la opción de selección de medios de arranque de UEFI

Si su UEFI admite la selección de medios de arranque, puede usarlo para iniciar el programa fácilmente desde el disco de arranque. La opción se invoca presionando una tecla de acceso rápido (generalmente, F8) en el inicio de la PC. En la mayoría de las versiones de UEFI esta opción también está disponible en el menú principal.



Trabajando con el programa

3 Trabajando con el programa

3.1 Ventana principal

Primero, el programa sugiere seleccionar uno de los modos de recuperación: **SAM** - cuentas de usuario regulares, **AD** - cuentas de Active Directory, **DCC** - contraseñas en caché de dominio, **PASSWORDS** - herramientas de recuperación de contraseñas, **FORENSICS** - investigación del sistema y herramientas forenses, UTILS - otras utilidades. A medida que realiza la selección, la lista de operaciones disponibles debe estar disponible para el modo.

SAM - cuentas de usuario normales

- Restablecer la contraseña de la cuenta de usuario
- Agregar nueva cuenta de usuario
- Editar propiedades de cuenta
- Opciones de directiva de inicio de sesión
- Editor de políticas de contraseñas
- Editor de políticas de restricción de interfaz y sistema
- Buscar contraseñas de usuario

- Volcar hashes de contraseña
- Restaurar contraseñas modificadas previamente, revertir cambios

AD - Cuentas de dominio de Active Directory

- Restablecer la contraseña de la cuenta de usuario
- Restablecer o cambiar la contraseña de DSRM (Modo de restauración de servicios de directorio)
- Editar propiedades de cuenta
- Editor de políticas de contraseñas
- Buscar contraseñas de usuario
- Extraer contraseñas de recuperación de BitLocker
- Volcar hashes de contraseña
- Restaurar contraseñas modificadas previamente, revertir cambios

DCC - credenciales almacenadas en caché de dominio

- Restablecer contraseña almacenada en caché de dominio
- Buscar contraseñas de DDC
- Volcar las credenciales almacenadas en caché del dominio en el archivo de texto
- Restaurar contraseñas modificadas previamente, revertir cambios

PASSWORDS - herramientas de recuperación de contraseñas

- Descifrar credenciales de Windows Hello
- Búsqueda de PIN
- Buscar contraseña de inicio de SYSKEY
- Contraseñas de búsqueda para máquinas virtuales
- Buscar contraseñas para documentos cifrados
- Buscar contraseñas de Internet/correo/red

FORENSICS - herramientas de investigación del sistema

- Ver el historial de inicio de sesión y las estadísticas
- Ver el historial de hardware
- Ver el historial de software
- Ver el historial de la red
- Ver la actividad reciente del usuario
- Buscar documentos abiertos recientemente
- Ver cronograma de ejecución del programa
- Ver eventos del sistema
- Ver el historial web
- Ver los archivos modificados por última vez
- Ver los directorios modificados por última vez

UTILS - herramientas diversas

- Búsqueda de claves de producto y números de serie perdidos
- Buscar documentos protegidos

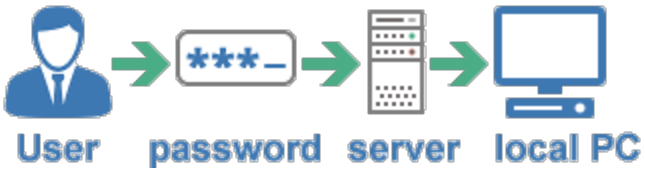
- Buscar documentos abiertos recientemente
- Respaldar Contraseñas e información confidencial
- Eliminar información confidencial del usuario
- Cargar controlador IDE/SATA/SCSI/RAID
- Desbloquear unidades cifradas con Bitlocker
- Montar unidades virtuales
- Crear imagen de disco

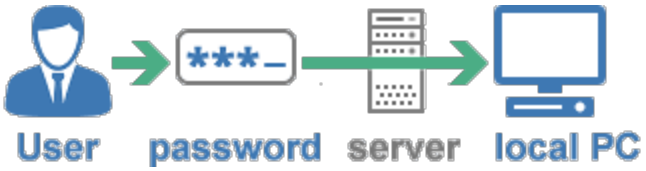
Descripción esquemática de los tipos de inicio de sesión

SAM
Una cuenta de usuario normal de cualquier PC doméstico. Los hashes de contraseña se almacenan en el archivo de registro SAM en el mismo equipo.

Active Directory
Una cuenta de usuario de dominio. Los hashes de contraseña se almacenan en NTDS. Base de datos DIT en PC de dominio.

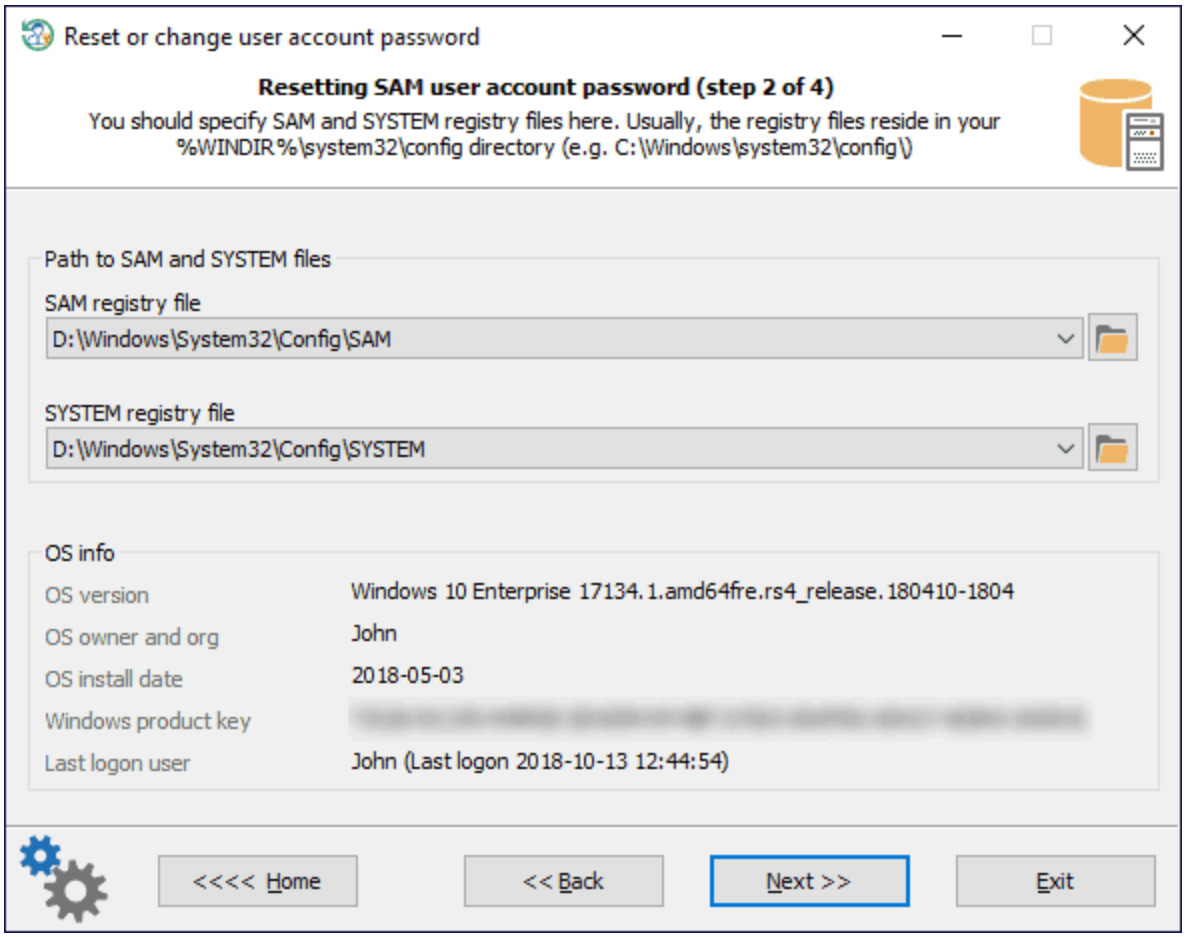
DCC
Credenciales almacenadas en caché de cuentas de dominio. Los hashes de contraseña se pueden almacenar (dependiendo de la política de seguridad del dominio) en el equipo local. El inicio de sesión de la cuenta se realiza a través del dominio o utilizando las credenciales almacenadas en caché.





3.2 Restablecer contraseñas de usuario

Selección del origen de datos

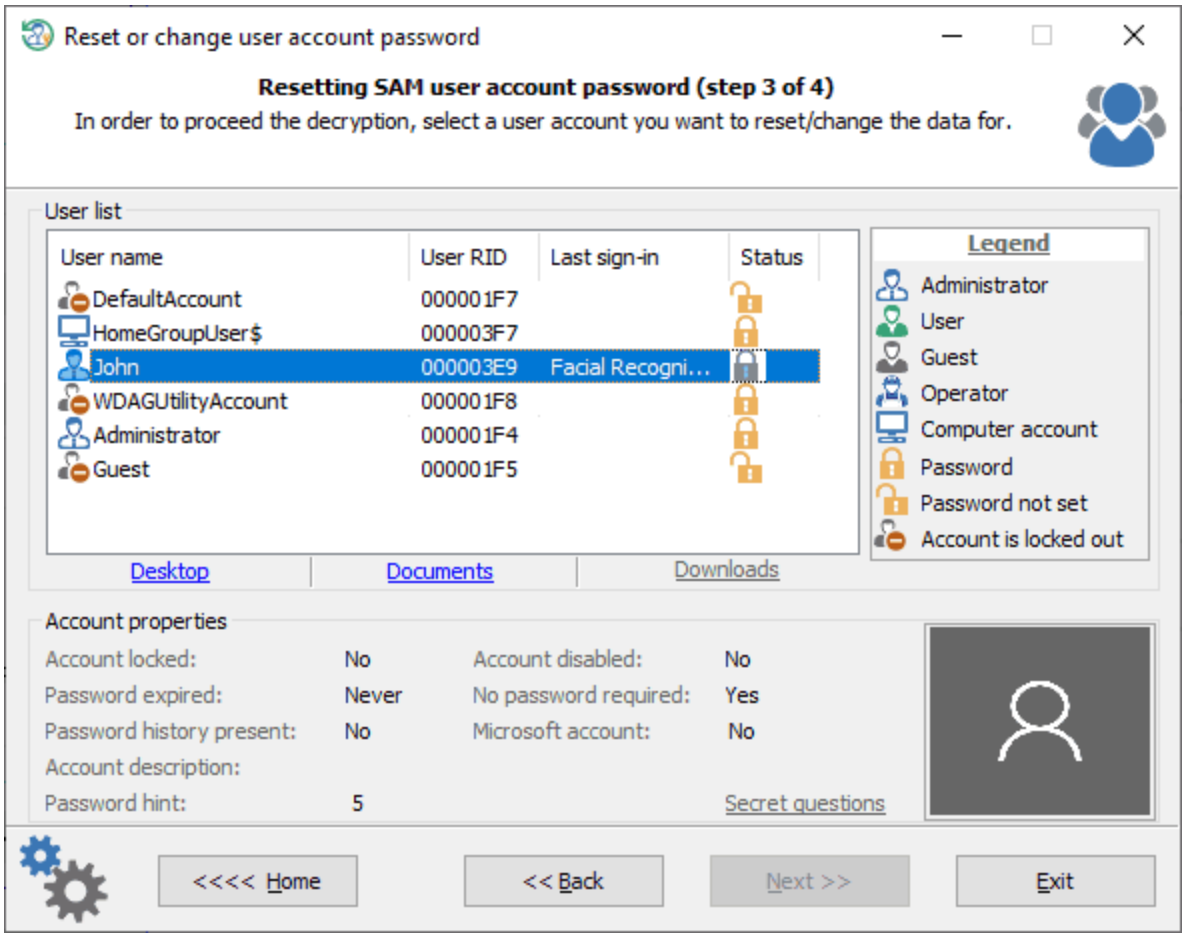


Para restablecer una contraseña de cuenta normal, debe seleccionar dos archivos de registro: SAM y SYSTEM. La aplicación busca automáticamente todos los archivos y sugiere los primeros que encuentra. Los archivos del Registro se encuentran en la carpeta %WINDIR%\system32\config. Donde %WINDIR% es su directorio de Windows.

Si selecciona el modo de Active Directory durante el paso anterior, debe establecer la ubicación de la base de datos de Active Directory en lugar del archivo de registro SAM. De forma predeterminada, esa

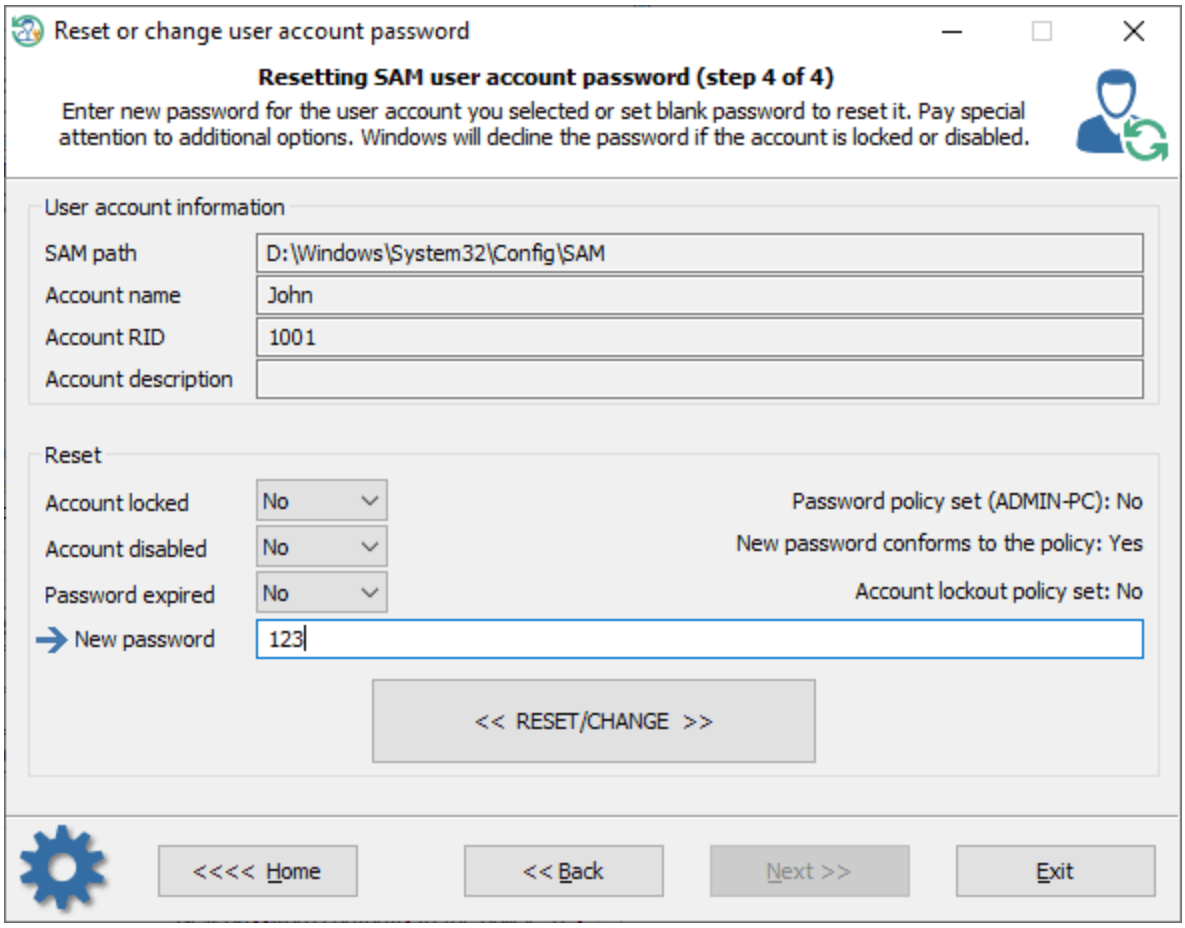
es la carpeta %WINDIR%\NTDS. Por lo tanto, la ruta de acceso completa a la base de datos de AD puede tener este aspecto: C:Windows\NTDS\ntds.dit

Eligiendo una cuenta de Windows



La parte superior del cuadro de diálogo muestra la lista de cuentas de usuario encontradas. Al hacer clic en uno de ellos, puede ver las propiedades de la cuenta; a saber: si la cuenta está bloqueada o deshabilitada, si se requiere la contraseña, si el historial de contraseñas está disponible, si la sugerencia de contraseña está disponible, etc.

Restableciendo contraseña



Para restablecer la contraseña, llene el campo en blanco '*Nueva contraseña*' y haga clic en el botón '*Reestablecer/Cambiar*'. Tome nota de las opciones adicionales. La cuenta no debe estar bloqueada, deshabilitada o caducada.

Además, si se establecen políticas de contraseñas locales o de dominio, asegúrese de que la nueva contraseña cumpla con los requisitos de longitud y complejidad y no coincida con ninguna de las contraseñas utilizadas anteriormente (si existe un historial de contraseñas). De lo contrario, no podrá iniciar sesión en el sistema incluso si restablece la contraseña con éxito.

Si está restableciendo una contraseña del administrador incorporado, tenga en cuenta que para activar esta cuenta e iniciar sesión en el sistema, deberá cargar el sistema en modo seguro. Para hacer eso, antes de que Windows comience a cargarse, siga presionando la tecla F8 hasta que aparezca el cuadro de diálogo de selección de arranque del sistema textual. En ese cuadro de diálogo, seleccione el elemento de modo seguro. Después de eso, la cuenta de administrador incorporada se activará y podrá usarla.

En Windows 8 y sistemas operativos posteriores, haga clic en el botón de *Encendido*, mantén pulsada la tecla MAYÚS del teclado y selecciona *Reiniciar*.

Tenga en cuenta que tendrá que ingresar una contraseña no vacía para poder iniciar sesión en LiveID o cuenta de Microsoft.

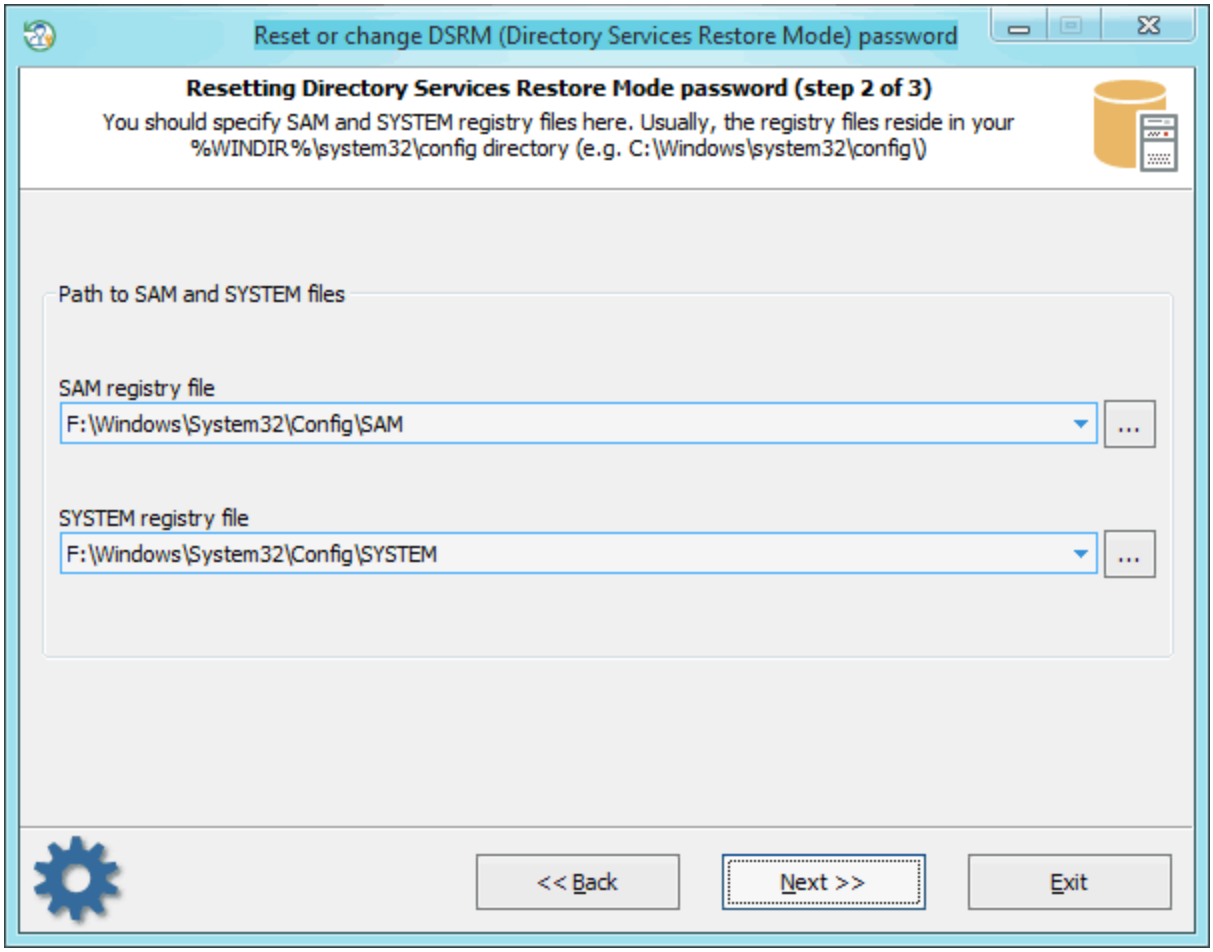
3.3 Restablecer contraseñas DSRM

Que es DSRM

DSRM (conocido como **Modo de reparación de servicios de directorio** o **modo de restauración de servicios de directorio** en versiones anteriores a Windows Server 2012) es un modo de arranque especial de un controlador de dominio de Windows Server que es algo similar al Modo seguro con funciones de red, pero sin Active Directory en ejecución. DSRM se utiliza para restaurar Active Directory desde una copia de seguridad. También es útil en diferentes situaciones y problemas con el AD.

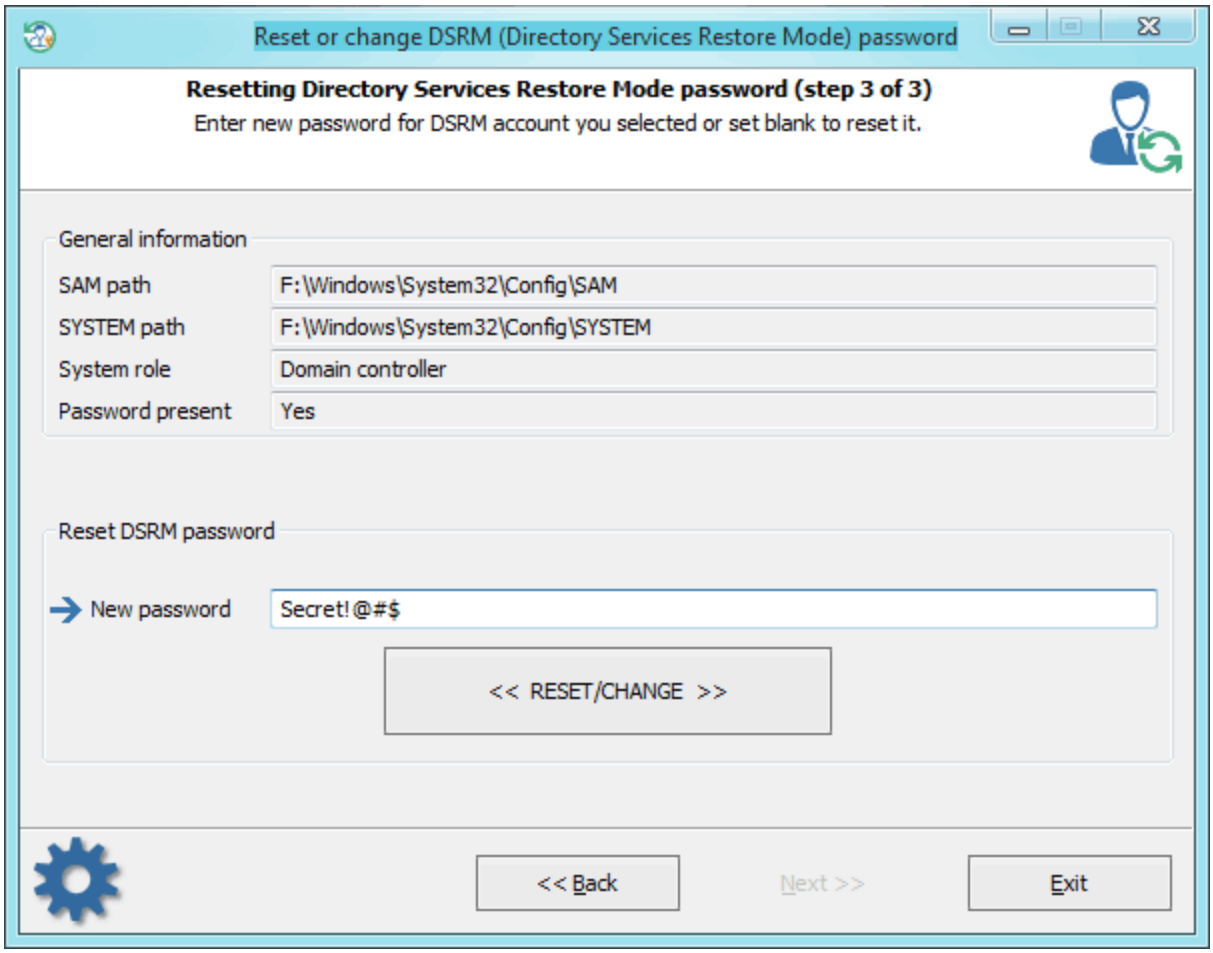
Para entrar en DSRM es necesario presionar la tecla F8 inmediatamente después de la pantalla BIOS/UEFI POST, pero antes de que aparezca el logotipo de Windows. En los sistemas operativos Windows Server 2012 y posteriores hay menú **Opciones de arranque avanzadas** o **Entorno de recuperación de Windows** para eso.

Selección del origen de datos



El proceso de recuperación de contraseña para la cuenta **DSRM** es casi el mismo que para la cuenta de usuario normal. Primero tendrá que especificar la ubicación de los archivos de registro **SAM** y **SYSTEM**.

Resetting password

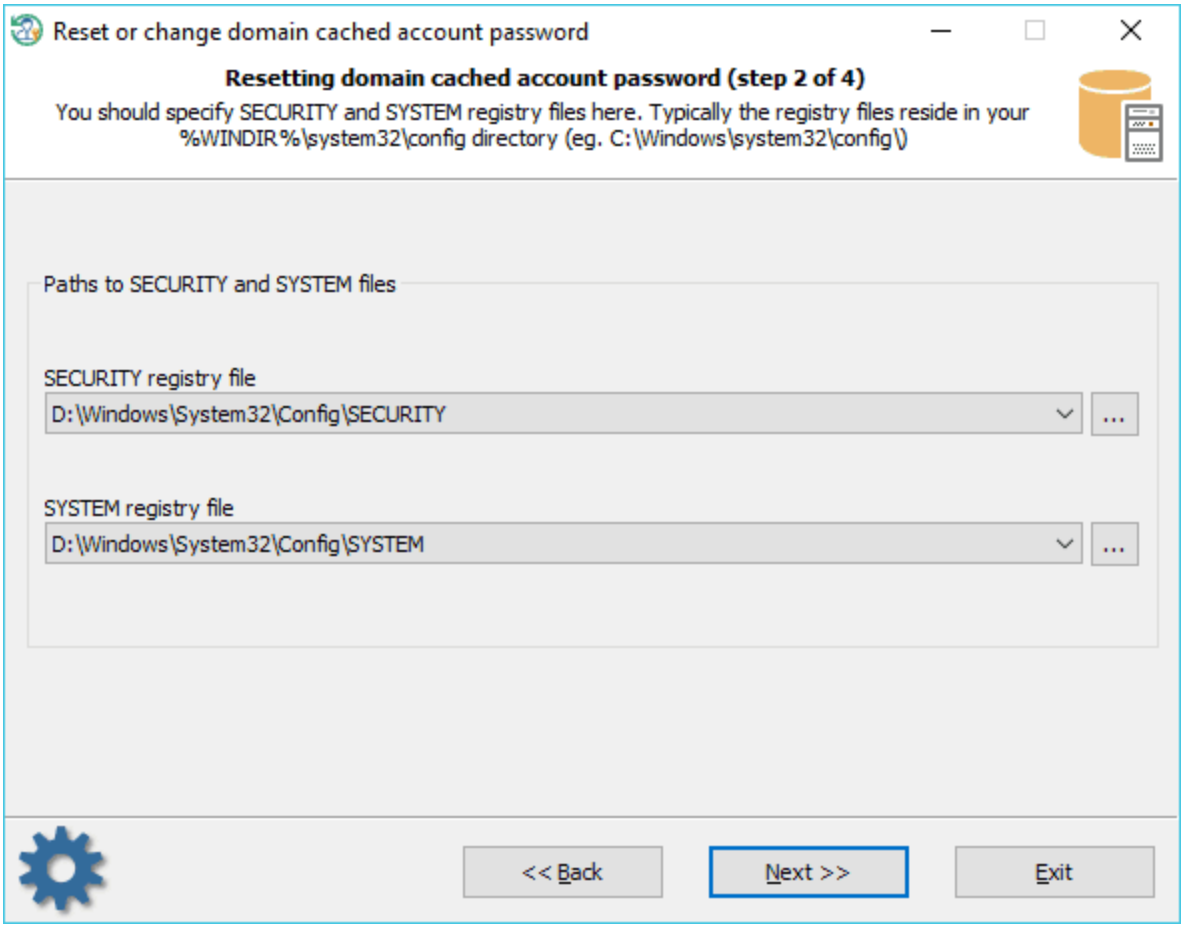


Escriba una nueva contraseña o simplemente establezca el campo de entrada en blanco si desea restablecerla. Luego confirme los cambios haciendo clic en el botón 'REESTABLECER/CAMBIAR'. El programa puede pedirle que cree un archivo de copia de seguridad. Puede utilizar el archivo de copia de seguridad más adelante para revertir los cambios.

3.4 Restablecer contraseña almacenada en caché de dominio

Cuando un usuario inicia sesión en un dominio de Windows, las credenciales de dominio del usuario se almacenan en caché de forma segura y se guardan en su PC. Esta característica permite a los usuarios iniciar sesión en el dominio cuando la estación de trabajo local está desconectada de la red o incluso si no hay ningún controlador de dominio disponible. Para evitar el problema de la contraseña perdida u olvidada para la cuenta de dominio, simplemente puede restablecer las credenciales en caché de su dominio utilizando Reset Windows Password. El proceso consta de 3 sencillos pasos.

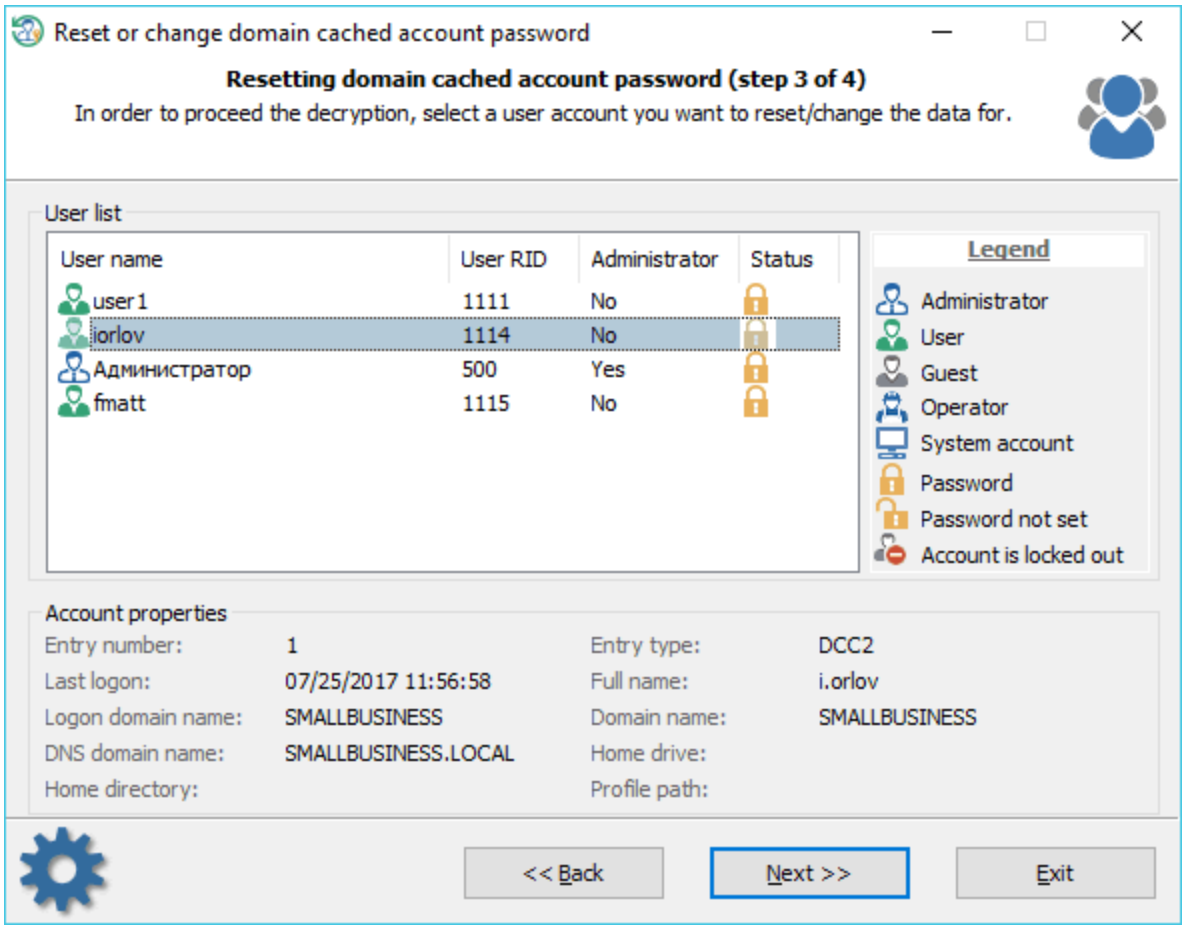
Selección de archivos de registro



Para restablecer una contraseña almacenada en caché de dominio, debe proporcionar dos archivos de registro: **SECURITY** y **SYSTEM**. Ambos archivos se encuentran en la carpeta **%WINDIR%\system32\config**. Dónde %WINDIR% es su directorio de Windows. Por lo general, el programa se encarga de eso y sugiere los archivos que encontró.

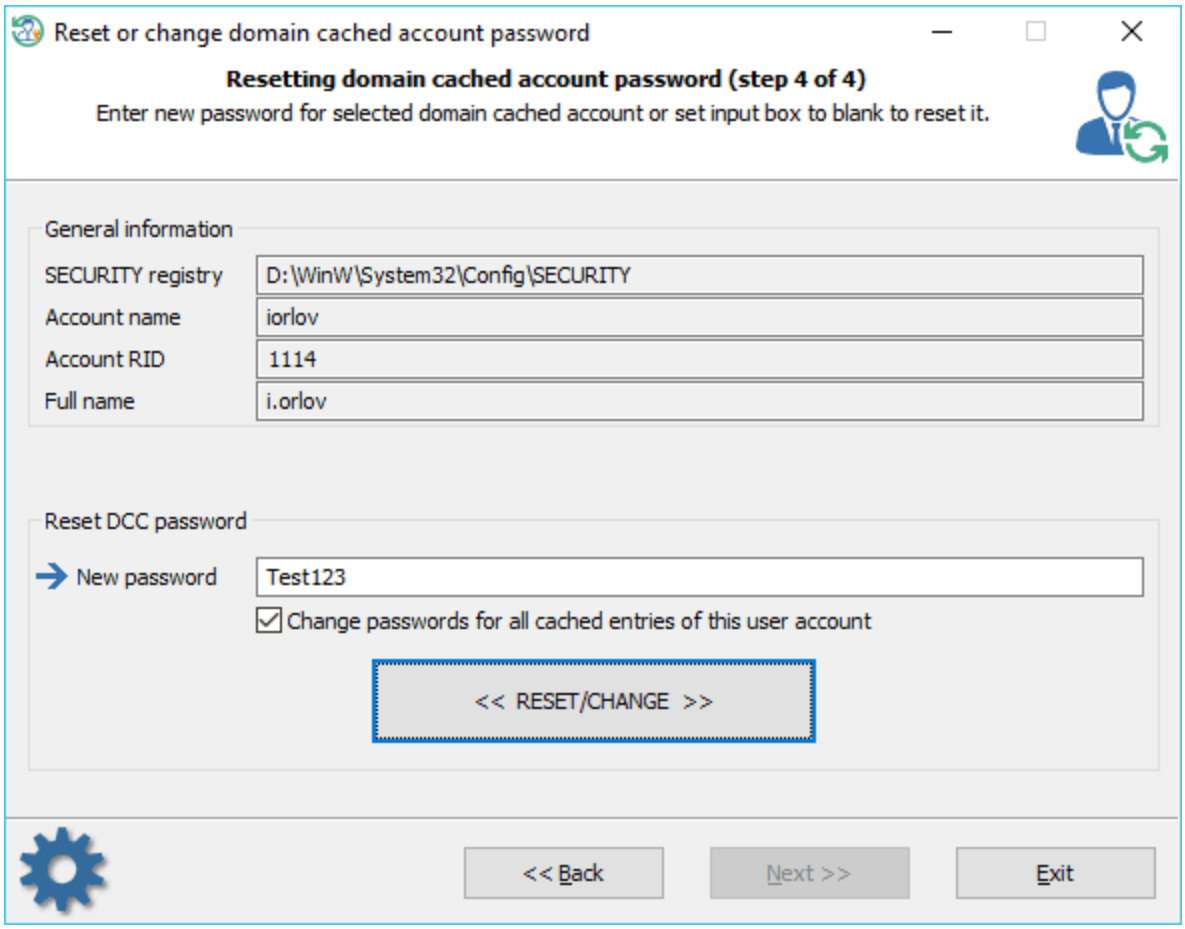
Antes de continuar con el siguiente paso de recuperación, asegúrese de seleccionar exactamente los archivos que necesita.

Selección de la cuenta de dominio



La parte superior del cuadro de diálogo muestra una lista de entradas en caché encontradas con los nombres de las cuentas de usuario. Seleccione una de las entradas para ver sus propiedades: el nombre completo de la cuenta de usuario, la última fecha de inicio de sesión, el dominio de inicio de sesión, el directorio de inicio, etc.

Restablecer contraseña



Para restablecer la contraseña, deje vacío el cuadro de entrada '*Nueva contraseña*' y haga clic en '*REINICIALIZAR/CAMBIAR*'. Preste especial atención a la opción adicional. La caché de dominio está organizada de tal manera que puede contener varias entradas del mismo usuario. Si se establece la opción 'Cambiar contraseña para todas las entradas almacenadas en caché para esta cuenta de usuario', el programa intentará cambiar / restablecer las contraseñas de todas las entradas encontradas de la cuenta seleccionada (con el RID especificado). De lo contrario, restablecerá la contraseña solo para la entrada seleccionada. Se recomienda configurar esta opción a menos que sepa lo que hace.

Asegúrese de que su nueva contraseña cumpla con los requisitos de longitud y complejidad del dominio y no coincida con ninguna de las contraseñas ingresadas anteriormente (si se utilizan la política de seguridad y el historial de contraseñas). De lo contrario, Windows puede denegar el acceso incluso si la contraseña se modifica correctamente.

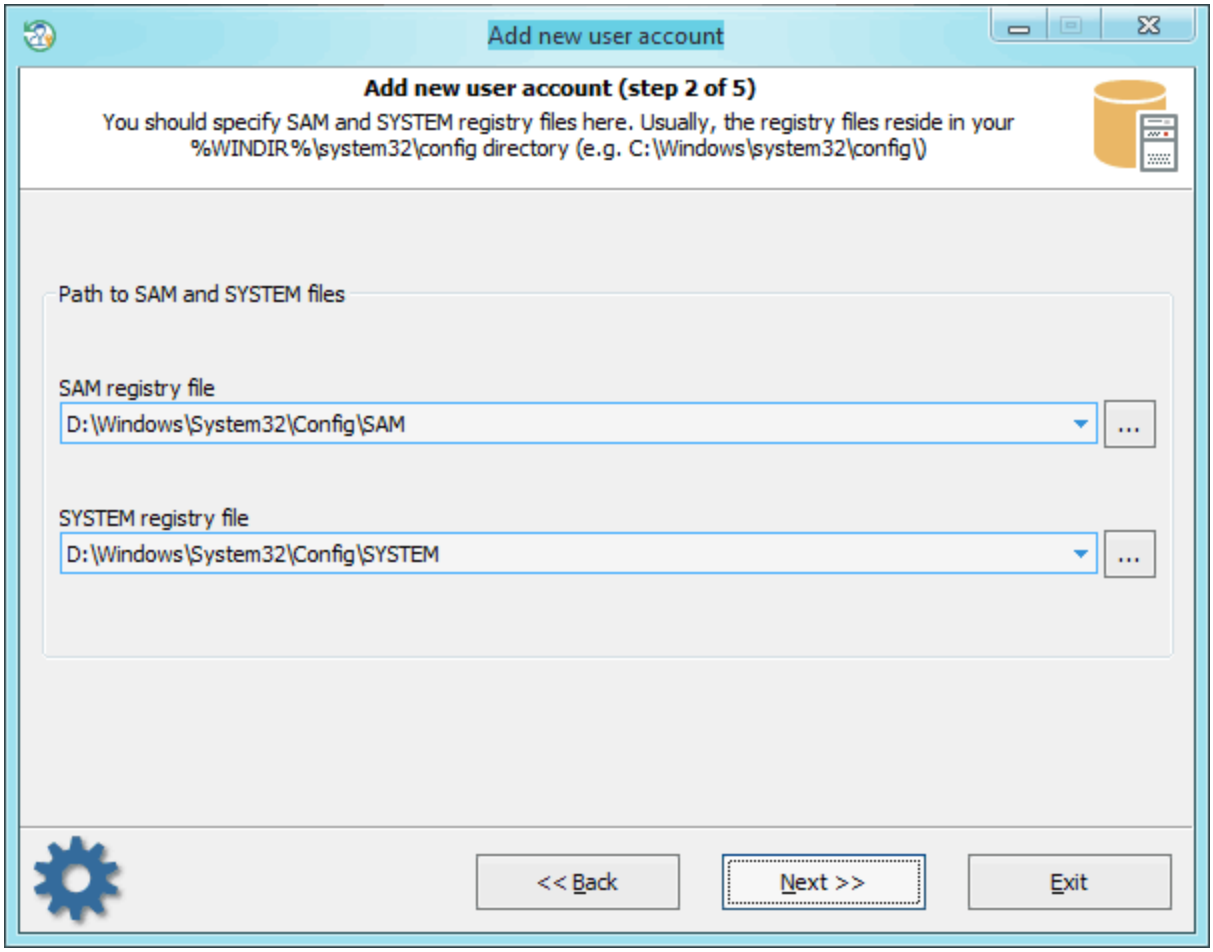
Tenga en cuenta que para iniciar sesión en su cuenta de dominio con éxito después de restablecer la contraseña almacenada en caché, debe iniciar sesión temporalmente **deshabilitar la conexión al dominio!** De lo contrario, Windows no usará la entrada en caché local, sino las credenciales de dominio normales.

Tenga en cuenta que iniciar sesión en el dominio con credenciales almacenadas en caché solo le da acceso a los recursos locales.

3.5 Agregar nueva cuenta de usuario

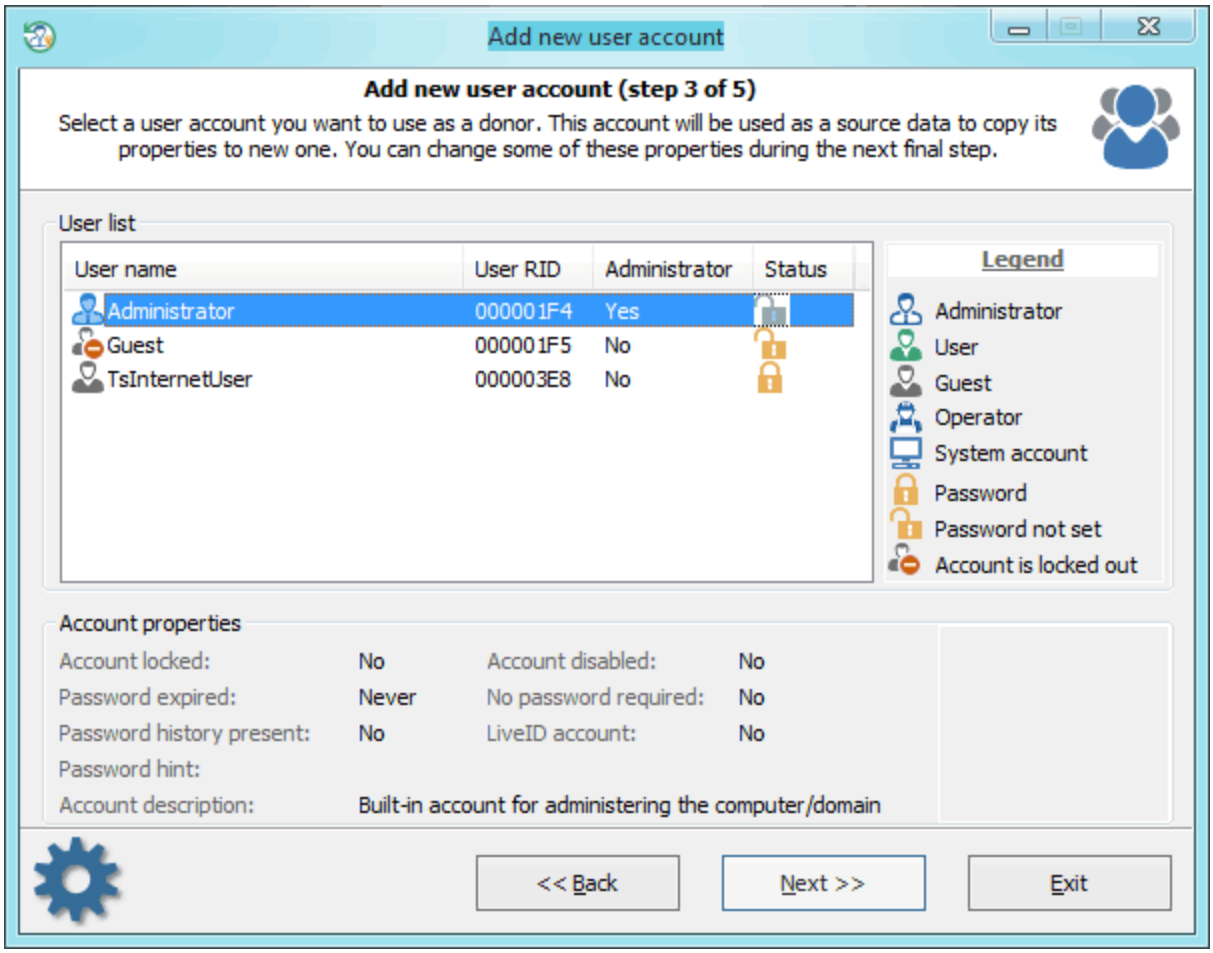
Agregar una nueva cuenta local es simple como es. Intentamos organizarlo en 3 pasos comunes.

1. Selección del origen de datos



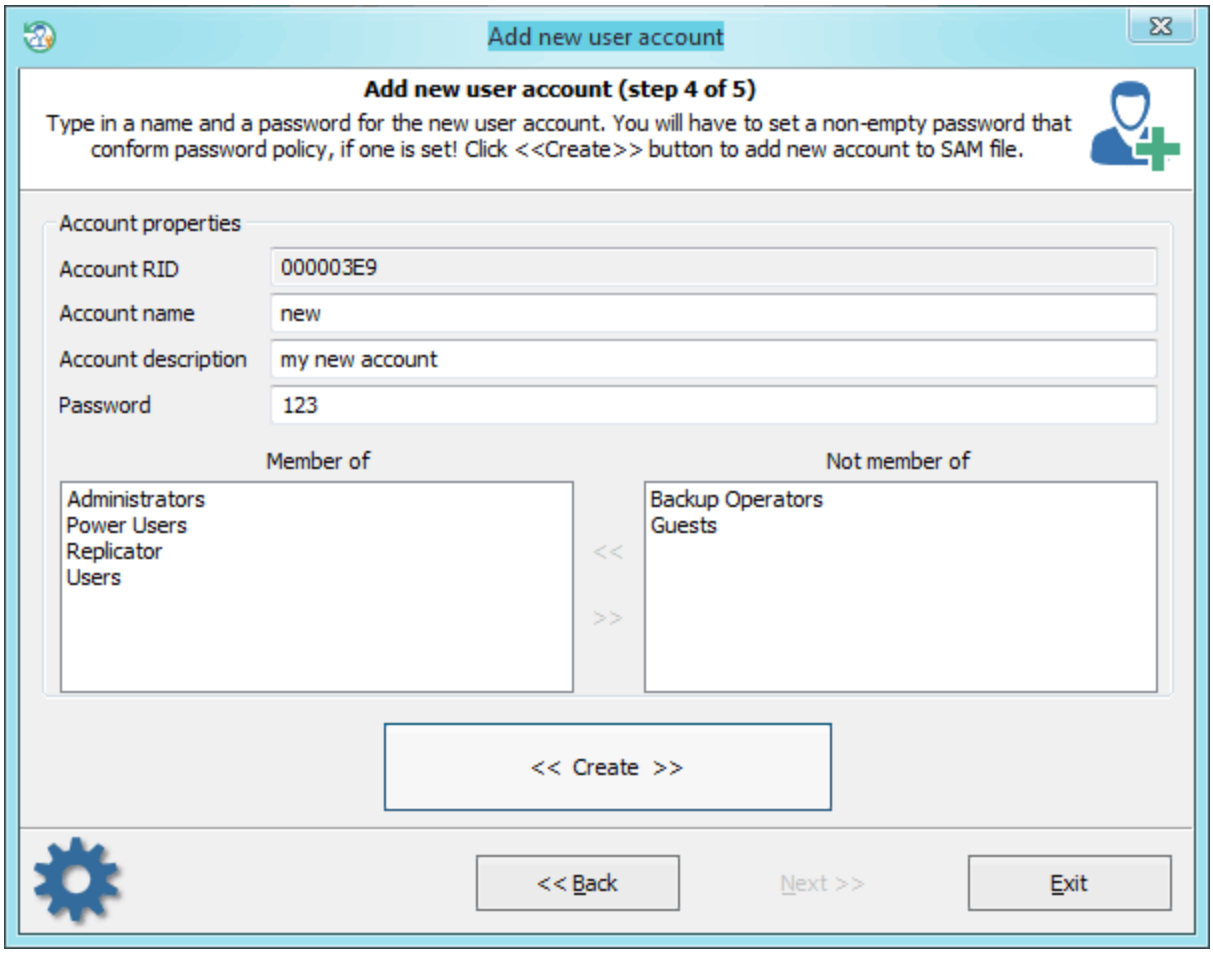
Primero debe seleccionar los archivos **SAM** y **SYSTEM**. El programa generalmente busca y sugiere los archivos automáticamente. En caso de que necesite configurar los archivos manualmente por alguna razón, sepa que los archivos del registro se encuentran en el directorio **%WINDIR%\system32\config**.

2. Elegir una cuenta donante



Seleccione un usuario que desee utilizar como cuenta de donante. Todas las propiedades de la cuenta de origen se copiarán en la recién creada. No hay problema si la cuenta de origen está bloqueada o deshabilitada, el programa debe corregir algunas de sus propiedades críticas y configurar los indicadores predeterminados. Por ejemplo, si la cuenta de origen está configurada para permitir el inicio de sesión en el sistema en ciertas horas, el programa pondrá a cero la restricción.

3. Agregar una nueva cuenta



Ahora todo lo que necesita es establecer un nombre, una descripción y una contraseña para la nueva cuenta. Deje el campo de contraseña en blanco para establecer la contraseña vacía. Tenga en cuenta que si el sistema operativo de destino tiene establecida la directiva de contraseñas, su nueva contraseña debe ajustarse a la directiva.

Debe prestar especial atención a la configuración de la pertenencia a grupos de la nueva cuenta. Por lo general, debe convertirlo en miembro del grupo 'Administradores' y/o 'Usuarios' para poder iniciar sesión localmente, si no se especifica lo contrario en su política de seguridad. Establecer una pertenencia a grupo incorrecta puede causar problemas, por ejemplo, eliminar la cuenta.

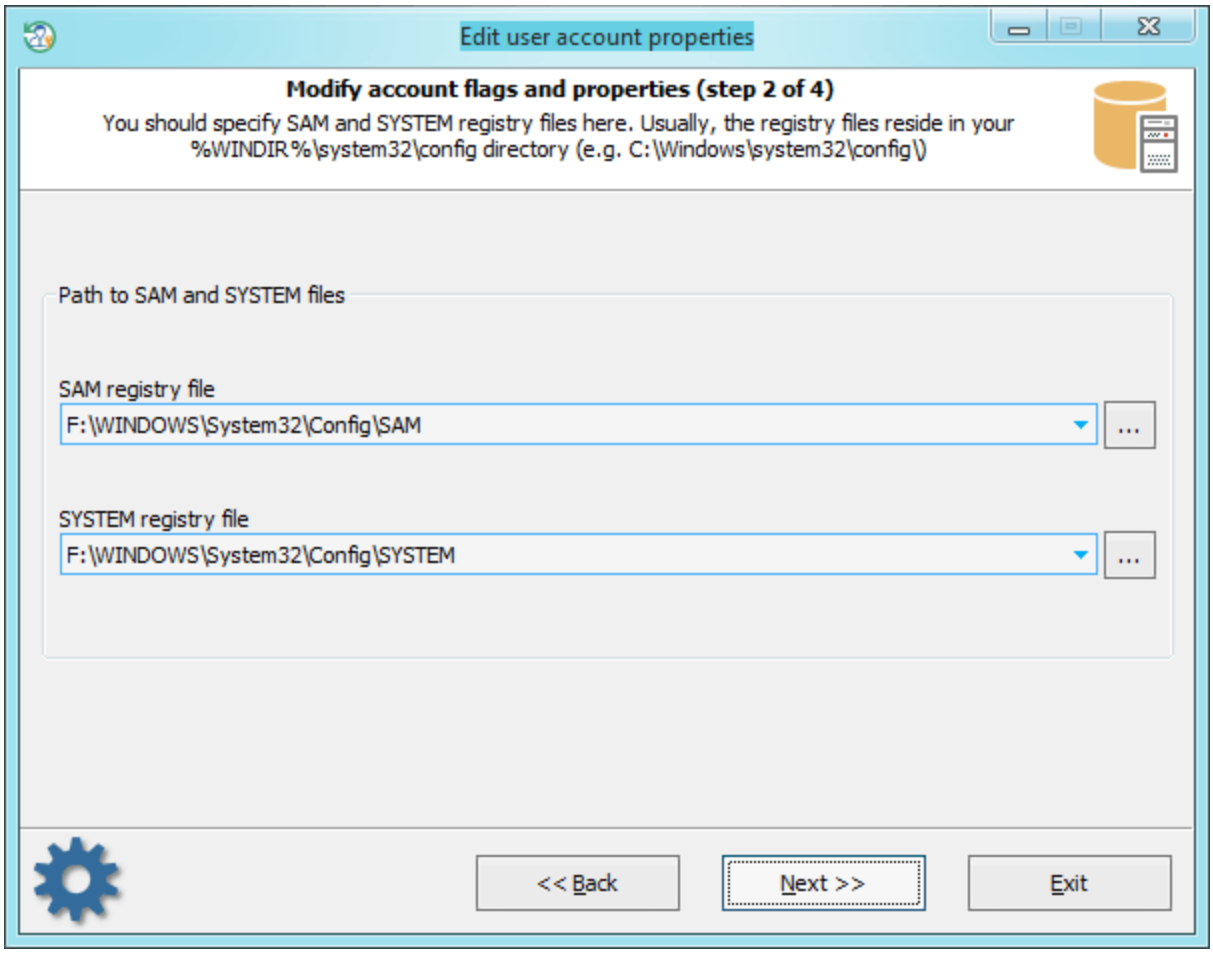
Después de que la cuenta se haya creado correctamente, puede volver al cuadro de diálogo principal, seleccionar el modo 'Editar propiedades de cuenta' y establecer/desestablecer algunos indicadores extendidos, si es necesario.

3.6 Editar propiedades de cuenta de usuario

La nueva versión del programa le permite manipular con propiedades extendidas de la cuenta de usuario de destino, así como cambiar la cuenta de Microsoft Live ID a la cuenta local o viceversa. Esto es

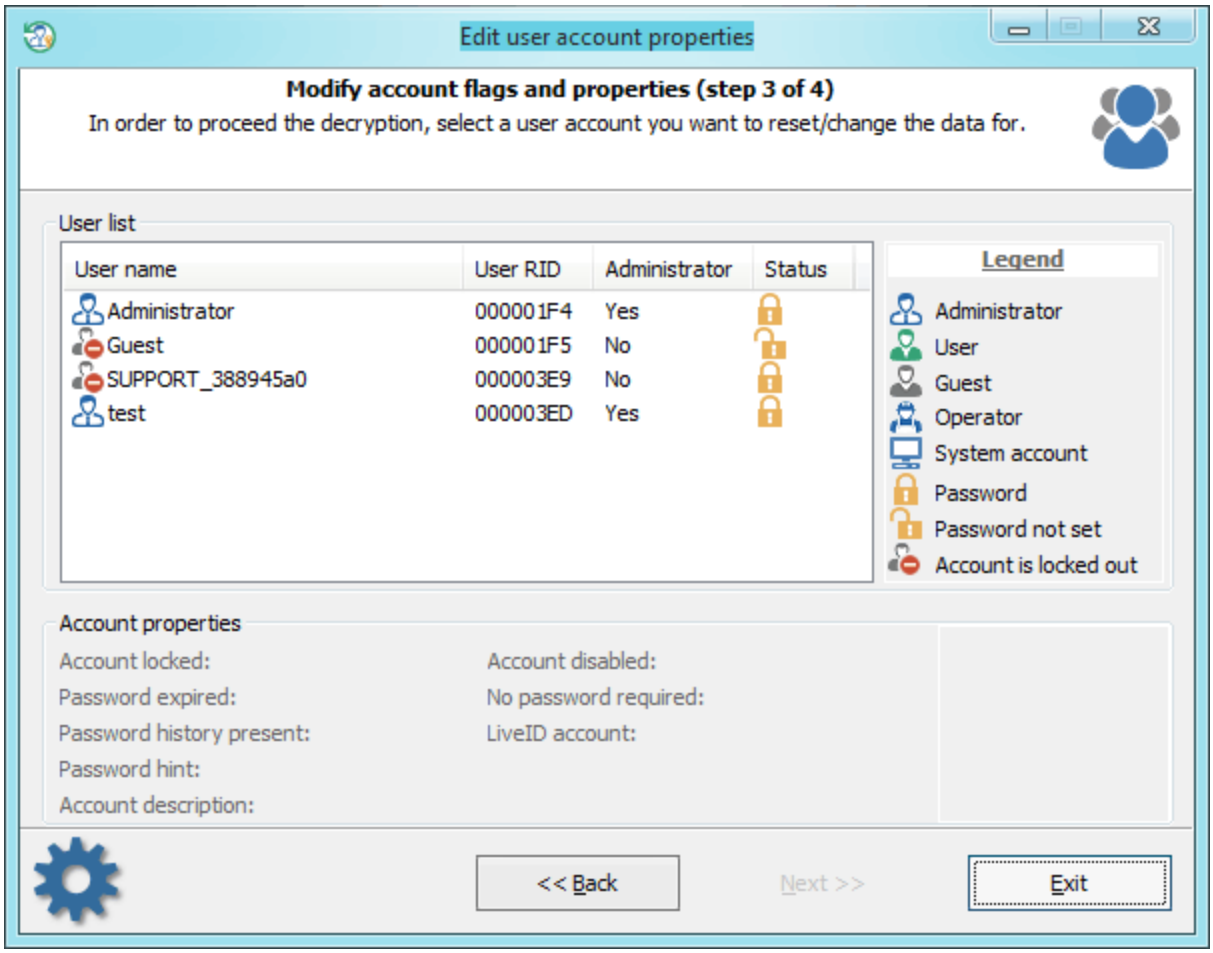
extremadamente útil cuando necesita desbloquear/habilitar una cuenta bloqueada/deshabilitada, desconfigurar la marca 'contraseña caducada', deshabilitar el "Inicio de sesión de la tarjeta inteligente" si su tarjeta inteligente se ha perdido ocasionalmente, etc. Modificar las propiedades de la cuenta problemática es bastante fácil. Primero debe seleccionar los archivos del sistema operativo de destino.

Selección del origen de datos



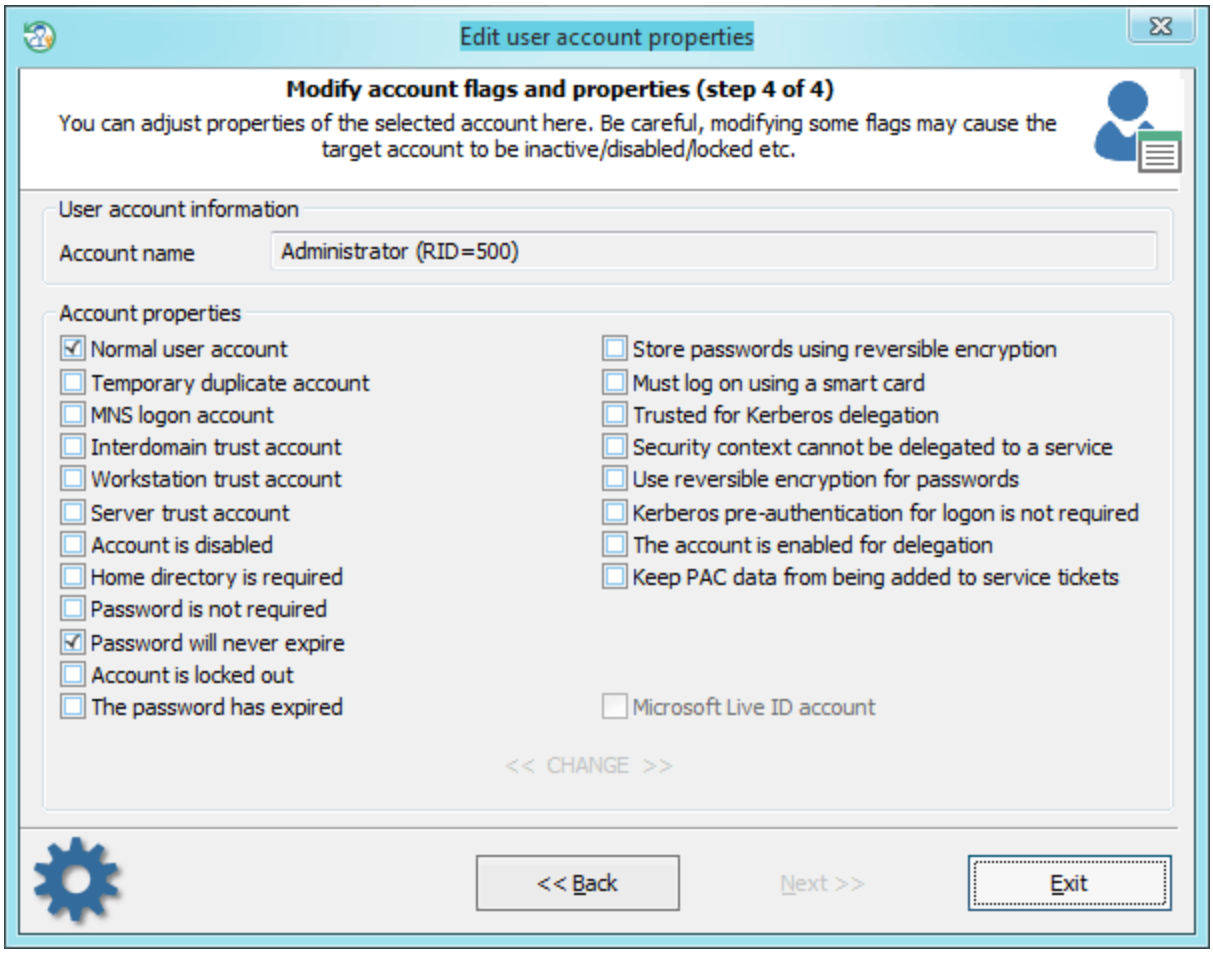
Se necesitan dos archivos. Estos son **SAM** y **SYSTEM** (en caso de que esté modificando una cuenta local) o **NTDS**. **DIT** y **SYSTEM** (cuando necesita cambiar la propiedad de un usuario de dominio). El programa busca automáticamente estos archivos y sugiere los primeros que encuentra. También puede especificar rutas de acceso a estos archivos manualmente. Se encuentran en las carpetas **%WINDIR%\system32\config** y **%WINDIR%\NTDS**. Donde **%WINDIR%** es su directorio de Windows. Por lo tanto, la ruta de acceso completa a la base de datos de Active Directory puede tener este aspecto: **C:\Windows\NTDS\ntds.dit**

Elegir una cuenta de Windows



Una vez seleccionados los archivos de origen, el programa enumera y muestra la lista de todas las cuentas de usuario encontradas. Seleccione uno que necesite y haga clic en el botón 'Siguiente' para abrir el cuadro de diálogo final con las propiedades del usuario.

Changing account properties



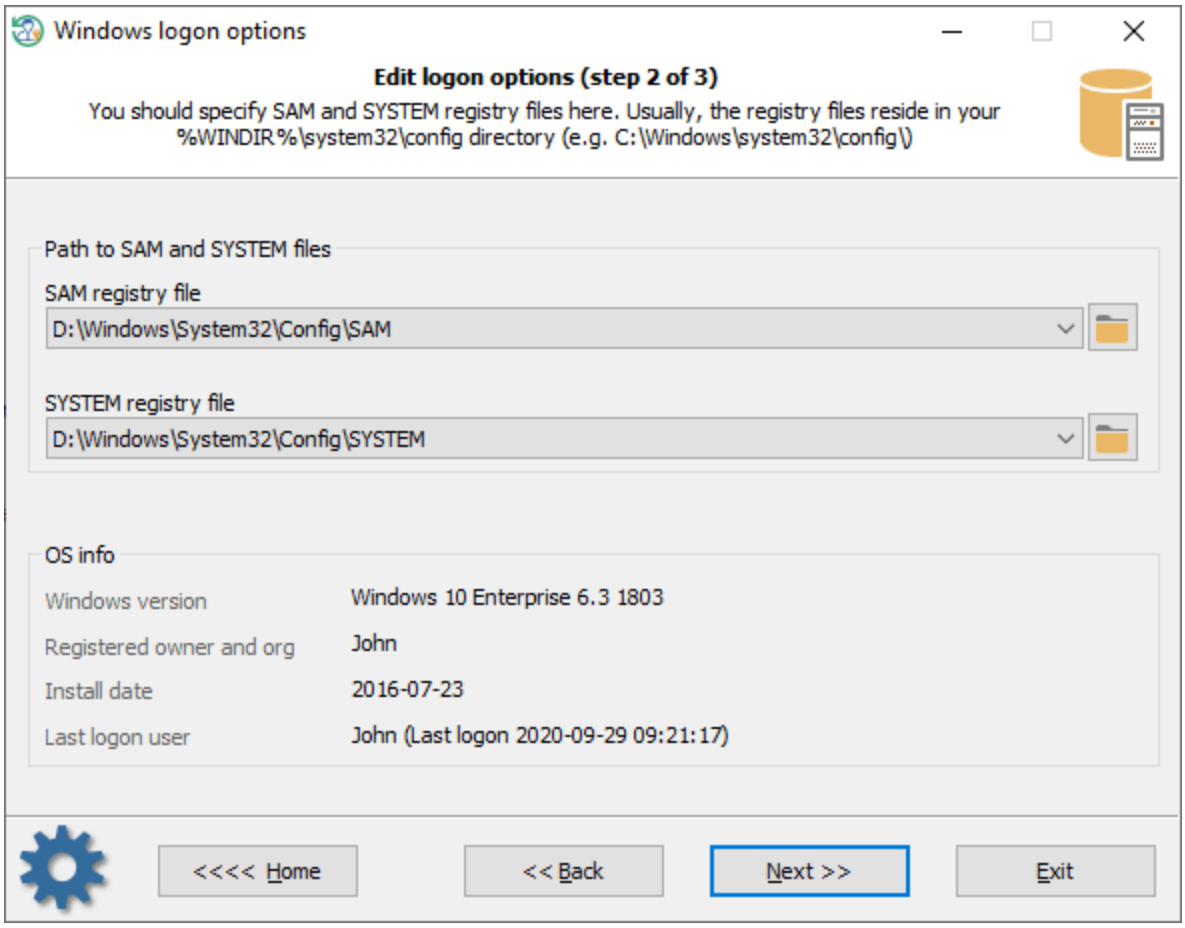
Puede establecer/desestablecer aquí diferentes banderas que controlan el comportamiento de la cuenta de usuario.

Tenga cuidado, cambiar algunas banderas puede hacer que la cuenta de destino se bloquee/deshabilite, etc.

3.7 Opciones de directiva de inicio de sesión

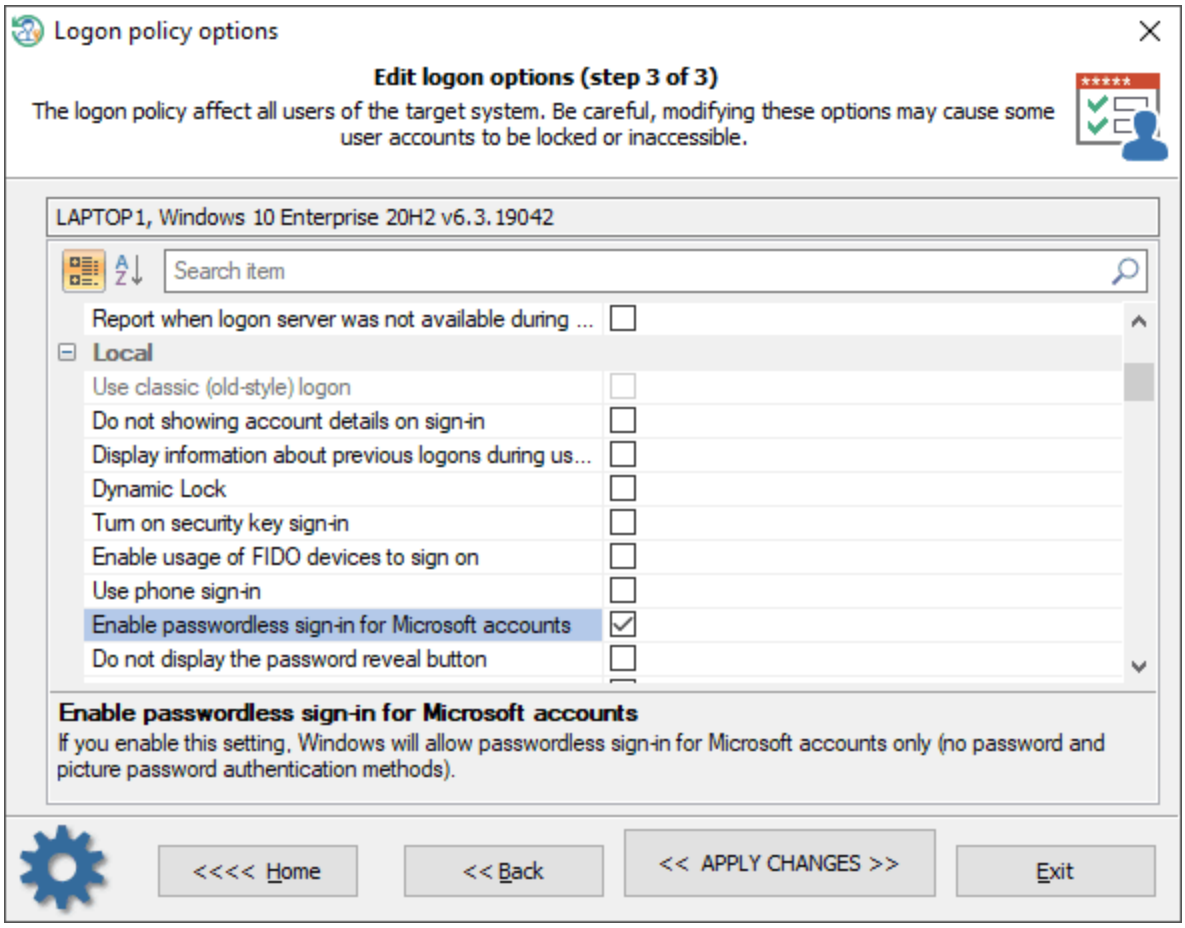
Puede usar la configuración para cambiar la forma en que los usuarios inician sesión en Windows. Por ejemplo, mostrar el nombre de usuario de la última vez que se inició sesión, asignar un dominio predeterminado para el inicio de sesión, activar/desactivar el inicio de sesión sin contraseña, etc.

Selección del origen de datos



Primero, elija los archivos de registro **SAM** y **SYSTEM** que fueron encontrados por el programa o especifique las rutas de acceso a ellos manualmente si RWP no pudo encontrar los que se encuentran.

Cambiar las opciones de directiva de inicio de sesión



Una vez seleccionados los archivos, puede modificar las opciones de inicio de sesión disponibles. Haga clic en el botón << APLICAR CAMBIOS >> para aplicar y guardar los cambios. Las opciones afectan a todos los usuarios locales del sistema de destino.

Tenga cuidado, modificar estas opciones puede hacer que algunas cuentas sean inaccesibles o bloqueadas.

La configuración del grupo **Dominio**:

Nombre	Descripción
Permitir que los usuarios seleccionen cuándo se requiere una contraseña al reanudar desde el modo de espera conectado	Si habilita esta configuración, un usuario en un dispositivo de espera conectado puede cambiar la cantidad de tiempo después de que la pantalla del dispositivo se apague antes de que se requiera una contraseña al activar el dispositivo. Si deshabilita esta configuración, un usuario no puede cambiar la cantidad de tiempo después de que la pantalla del dispositivo se apague antes de que se requiera una contraseña al activar el dispositivo. En su lugar, se requiere una contraseña inmediatamente después de que la pantalla se apague.
Dominio predeterminado para el inicio de sesión	Especifica un dominio de inicio de sesión predeterminado, que puede ser un dominio diferente del dominio al que está unido el equipo.
No enumerar usuarios conectados en equipos unidos a un dominio	Si habilita esta configuración, la interfaz de usuario de inicio de sesión no enumerará ningún usuario conectado en equipos unidos a un dominio.

Enumerar usuarios locales en equipos unidos a un dominio	Si habilita esta configuración, la interfaz de usuario de inicio de sesión enumerará todos los usuarios locales en equipos unidos a un dominio.
Desactivar el inicio de sesión con contraseña de imagen para los usuarios del dominio	Esta configuración le permite controlar si un usuario de dominio puede iniciar sesión con una contraseña de imagen.
Activar el inicio de sesión con PIN de conveniencia para los usuarios del dominio	Si habilita esta configuración, un usuario de dominio puede configurar e iniciar sesión con un PIN de conveniencia. Nota: La contraseña de dominio del usuario se almacenará en caché en el almacén del sistema cuando se utilice esta función.
Informar cuando el servidor de inicio de sesión no estaba disponible durante el inicio de sesión del usuario	Esta configuración controla si se debe notificar al usuario que ha iniciado sesión si no se pudo establecer contacto con el servidor de inicio de sesión durante el inicio de sesión y si ha iniciado sesión con la información de la cuenta almacenada anteriormente.

La configuración del grupo **Local**:

Nombre	Descripción
Usar inicio de sesión clásico (estilo antiguo)	Utilice siempre el esquema de interfaz de inicio de sesión clásico
No mostrar los detalles de la cuenta al iniciar sesión	Si se establece, impide que el usuario muestre los detalles de la cuenta (dirección de correo electrónico o nombre de usuario) en la pantalla de inicio de sesión.
Mostrar información sobre inicios de sesión anteriores durante el inicio de sesión del usuario	Si habilita esta configuración, aparece un mensaje después de que el usuario inicia sesión que muestra la fecha y la hora del último inicio de sesión correcto de ese usuario, la fecha y hora del último inicio de sesión fallido intentado con ese nombre de usuario y el número de inicios de sesión fallidos desde el último inicio de sesión correcto de ese usuario.
Bloqueo dinámico	Si habilita esta configuración, Windows habilitará el bloqueo dinámico para todos los usuarios en dispositivos administrados y los usuarios no podrán deshabilitar el bloqueo dinámico en sus cuentas.
Activar el inicio de sesión de clave de seguridad	Si habilita esta configuración, los usuarios pueden iniciar sesión con claves de seguridad externas.
Habilitar el uso de dispositivos FIDO para iniciar sesión	Esta configuración permite a los usuarios usar un dispositivo FIDO, como un teléfono, una tarjeta NFC, para iniciar sesión en un equipo de escritorio que ejecuta Windows 10.
Usar el inicio de sesión telefónico	Si habilita esta configuración, se habilitará el inicio de sesión telefónico, lo que permitirá el uso de un teléfono como dispositivo complementario para la autenticación de escritorio.
Habilitar el inicio de sesión sin contraseña para cuentas Microsoft	Si habilita esta configuración, Windows solo permitirá el inicio de sesión sin contraseña: los métodos de autenticación de contraseña y contraseña de imagen estarán desactivados. Esta opción solo afecta a las cuentas Microsoft.
No mostrar el botón de revelación de contraseña	Si habilita esta configuración, el botón de revelación de contraseña no se mostrará después de que un usuario escriba una contraseña en el cuadro de texto de entrada de contraseña.
Impedir el uso de preguntas de seguridad para cuentas locales	Si activas esta configuración, los usuarios locales no podrán configurar ni usar preguntas de seguridad para restablecer sus contraseñas.

Permitir dispositivo complementario para la autenticación secundaria	Si habilita o no configura esta opción, los usuarios pueden autenticarse en Windows Hello mediante un dispositivo complementario. Como un teléfono, una banda de fitness o un dispositivo IoT.
Secuencia de atención segura del software	Esta configuración controla si el software puede simular o no la secuencia de atención segura (SAS).
El modo de iniciar sesión automáticamente y bloquear el último usuario interactivo después de un reinicio o arranque en frío	Esta configuración controla la configuración bajo la cual se produce un reinicio automático y el inicio de sesión y el bloqueo después de un reinicio o arranque en frío.
Inicie sesión y bloquee el último usuario interactivo automáticamente después de un reinicio	Esta configuración controla si un dispositivo iniciará sesión y bloqueará automáticamente al último usuario interactivo después de que se reinicie el sistema o después de un apagado y arranque en frío. Esto solo ocurre si el último usuario interactivo no cerró sesión antes del reinicio o apagado.

La configuración del grupo **Misceláneo**:

Nombre	**Descripción**
Utilice siempre un fondo de inicio de sesión personalizado	Si habilita esta configuración de directiva, la pantalla de inicio de sesión siempre intenta cargar un fondo personalizado en lugar del fondo de inicio de sesión con la marca Windows.
Mostrar fondo de inicio de sesión claro	Esta configuración deshabilita el efecto de desenfoque acrílico en la imagen de fondo de inicio de sesión.
No mostrar la pantalla de bienvenida Introducción al iniciar sesión	Si habilita esta configuración, la pantalla de bienvenida se oculta para que el usuario inicie sesión en el sistema.
Desactivar las notificaciones de la aplicación en la pantalla de bloqueo	Esta configuración le permite evitar que las notificaciones de la aplicación aparezcan en la pantalla de bloqueo.
Mostrar la primera animación de inicio de sesión	Esta configuración le permite controlar si los usuarios ven la primera animación de inicio de sesión al iniciar sesión en el equipo por primera vez.
Desactivar el sonido de inicio de Windows	Desactivar los sonidos de Windows durante la autenticación
No procesar la lista de ejecuciones heredada	Esta configuración ignora la lista de ejecución personalizada (programas y servicios que inicia el sistema).
No procesar la lista ejecutar una vez	Si habilita esta configuración, el sistema ignora la lista de programas y documentos adicionales que se inician automáticamente la próxima vez que se inicie el sistema. Las listas personalizadas de ejecución única se almacenan en el Registro en HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\runOnce.
Ocultar puntos de entrada para el cambio rápido de usuario	Esta configuración le permite ocultar la interfaz de usuario de Switch en la interfaz de usuario de inicio de sesión, el menú Inicio y el Administrador de tareas.
Bloquear toda la autenticación de usuario de la cuenta Microsoft del consumidor	Si esta configuración está habilitada, se impide que todas las aplicaciones y servicios del dispositivo usen cuentas Microsoft para la autenticación.

Proveedor de credenciales predeterminado	Asigne un proveedor de credenciales especificado como proveedor de credenciales predeterminado.
Excluir proveedores de credenciales	Esta configuración permite al administrador excluir el uso de los proveedores de credenciales especificados durante la autenticación.

La configuración del grupo **Red**:

Nombre	Descripción
Espere siempre a que la red inicie el equipo e inicie sesión	Determina si los equipos esperan a que la red se inicialice completamente durante el inicio y el inicio de sesión del usuario. De forma predeterminada, los equipos no esperan a que la red se inicialice completamente al iniciar e iniciar sesión.
No mostrar la interfaz de usuario de selección de red	Si habilita esta configuración, el estado de conectividad de red del equipo no se puede cambiar sin iniciar sesión en Wind

La configuración del grupo Biometría:

Nombre	Descripción
Permitir que los usuarios del dominio inicien sesión mediante biometría	Si habilita o no configura esta opción, Windows permite a los usuarios de dominio iniciar sesión en un equipo unido a un dominio mediante la biometría.
Permitir que los usuarios inicien sesión mediante biometría	Si habilita o no configura esta opción, todos los usuarios pueden iniciar sesión en un equipo local basado en Windows y pueden elevar los permisos con UAC mediante la biometría.
Permitir el uso de la biometría	Si habilita o no configura esta opción, el servicio biométrico de Windows está disponible y los usuarios pueden ejecutar aplicaciones que usan biometría en Windows.
Configurar la suplantación de datos mejorada	Si habilita esta configuración, Windows requiere que todos los usuarios de dispositivos administrados usen la suplantación de posición antisono para la autenticación facial de Windows Hello. Esto deshabilita la autenticación facial de Windows Hello en dispositivos que no admiten la suplantación de perfiles mejorada.
Especifique el tiempo de espera para eventos de cambio rápido de usuario	Esta configuración especifica el número de segundos que un evento de cambio rápido de usuario pendiente permanecerá activo antes de que se inicie el conmutador. De forma predeterminada, un evento de cambio de usuario rápido está activo durante 10 segundos antes de quedar inactivo.

La configuración del grupo **PIN**:

Nombre	Descripción
Caducidad del PIN	Esta configuración especifica el período de tiempo en días (entre 1 y 730) que se puede usar un PIN antes de que el sistema requiera que el usuario lo cambie.
Historial de PIN	Esta configuración especifica el número de PIN anteriores que se pueden asociar a una cuenta de usuario que no se pueden reutilizar. El valor debe estar entre 0 y 50 PIN.
Longitud máxima del PIN	La longitud máxima del PIN configura el número máximo de caracteres permitidos para el PIN. El número más grande que puede configurar para esta

	configuración de directiva es 127.
Longitud mínima del PIN	La longitud mínima del PIN configura el número mínimo de caracteres necesarios para el PIN. El número más bajo que puede configurar para esta configuración de directiva es 4.
Requerir dígitos	Si habilita o no configura esta opción, Windows requiere que los usuarios incluyan al menos un dígito en su PIN.
Requerir letras minúsculas	Si habilita esta configuración, Windows requiere que los usuarios incluyan al menos una letra minúscula en su PIN.
Requerir caracteres especiales	Si habilita esta configuración de directiva, Windows requiere que los usuarios incluyan al menos un carácter especial en su PIN.
Requerir letras mayúsculas	Si habilita esta configuración de directiva, Windows requiere que los usuarios incluyan al menos una letra mayúscula en su PIN.

La configuración del grupo de **Windows Hello**:

Nombre	Descripción
Permitir la enumeración de tarjetas inteligentes emuladas para todos los usuarios	Windows impide que los usuarios del mismo equipo enumeren las credenciales aprovisionadas de Windows Hello para empresas para otros usuarios. Si habilita esta configuración, Windows permite que todos los usuarios del equipo enumeren todas las credenciales de Windows Hello para empresas, pero aún así requiere que cada usuario proporcione sus propios factores para la autenticación.
Factores de desbloqueo del dispositivo A	Primeros proveedores de credenciales de factor de desbloqueo
Factores de desbloqueo del dispositivo B	Proveedores de credenciales de segundo factor de desbloqueo
Reglas de desbloqueo de dispositivos	Reglas de señal para el desbloqueo del dispositivo
Factores de bloqueo dinámico	Si habilita esta configuración, estas reglas de señal se evaluarán para detectar la ausencia del usuario y bloquear automáticamente el dispositivo.
Reglas de bloqueo dinámico	Reglas de señal para bloqueo dinámico
Desactivar la emulación de tarjetas inteligentes	Si habilita esta configuración, Windows Hello para empresas aprovisiona las credenciales de Windows Hello para empresas que no son compatibles con las aplicaciones de tarjetas inteligentes.
Usar un dispositivo de seguridad de hardware	Si habilita esta configuración, el aprovisionamiento de Windows Hello para empresas solo se produce en dispositivos con TPM 1.2 o 2.0 utilizables. Opcionalmente, puede excluir los dispositivos de seguridad, lo que impide que el aprovisionamiento de Windows Hello para empresas use esos dispositivos.
No utilice los dispositivos de seguridad TPM 1.2	Excluir dispositivos de seguridad de TPM 1.2.
Usar biometría	Si habilita o no configura esta opción, Windows Hello para empresas permite el uso de gestos biométricos.
Usar certificado para la autenticación local	Si habilita esta configuración, Windows Hello para empresas inscribe un certificado de inicio de sesión que se usa para la autenticación local.
Usar la recuperación de PIN	Si habilita esta configuración, Windows Hello para empresas usa el servicio de recuperación de PIN.
Usar certificados de Windows Hello para empresas como	Si habilita esta configuración, las aplicaciones usan certificados de Windows Hello para empresas como certificados de tarjeta inteligente. Los factores

certificados de tarjeta inteligente	biométricos no están disponibles cuando se solicita a un usuario que autorice el uso de la clave privada del certificado.
Usar Windows Hello para empresas	Si habilita esta configuración, el dispositivo aprovisiona Windows Hello para empresas mediante claves o certificados para todos los usuarios.
No iniciar el aprovisionamiento de Windows Hello después de iniciar sesión	Si habilita esta configuración, Windows Hello para empresas no inicia automáticamente el aprovisionamiento después de que el usuario haya iniciado sesión.

La configuración del grupo **TPM**:

Name	Description
El nivel de información de autorización del propietario de TPM disponible para el sistema operativo	Esta configuración de directiva configura la cantidad de información de autorización del propietario de TPM almacenada en el Registro del equipo local. Dependiendo de la cantidad de información de autorización del propietario de TPM almacenada localmente, el sistema operativo y las aplicaciones basadas en TPM pueden realizar ciertas acciones de TPM que requieren la autorización del propietario de TPM sin requerir que el usuario escriba la contraseña de propietario de TPM. Puede elegir que el sistema operativo almacene el valor completo de autorización del propietario de TPM, el blob de delegación administrativa de TPM más el blob de delegación de usuario de TPM o ninguno. Si habilita esta configuración de directiva, Windows almacenará la autorización del propietario de TPM en el registro del equipo local de acuerdo con la configuración de autenticación de TPM administrada del sistema operativo que elija.
Configure el sistema para borrar el TPM si no está en un estado listo.	Esta configuración de directiva configura el sistema para solicitar al usuario que borre el TPM si se detecta que el TPM se encuentra en cualquier estado que no sea Listo. Esta directiva solo surte efecto si el TPM del sistema se encuentra en un estado distinto de Listo, incluso si el TPM es "Listo, con funcionalidad reducida". El mensaje para borrar el TPM comenzará a ocurrir después del próximo reinicio, al iniciar sesión del usuario solo si el usuario que ha iniciado sesión forma parte del grupo Administradores del sistema. El mensaje se puede descartar, pero volverá a aparecer después de cada reinicio e inicio de sesión hasta que la directiva esté deshabilitada o hasta que el TPM esté en un estado Listo.
Configurar el sistema para que utilice la configuración heredada de parámetros de prevención de ataques de diccionario para TPM 2.0	Esta configuración de directiva configura el TPM para usar los parámetros de prevención de ataques del diccionario (umbral de bloqueo y tiempo de recuperación) a los valores que se usaron para Windows 10 versión 1607 y versiones posteriores. La configuración de esta directiva sólo surte efecto si a) el TPM se preparó originalmente con una versión de Windows posterior a Windows 10 versión 1607 y b) el sistema tiene un TPM 2.0. Tenga en cuenta que habilitar esta directiva solo surte efecto después de que se ejecute la tarea de mantenimiento de TPM (lo que normalmente ocurre después de reiniciar el sistema). Una vez que esta directiva se haya habilitado en un sistema y haya su efecto (después de un reinicio del sistema), deshabilitarla no tendrá ningún impacto y el TPM del sistema permanecerá configurado utilizando los parámetros heredados de Prevención de ataques de diccionario, independientemente del valor de esta directiva de grupo. La única forma de que la configuración deshabilitada de esta directiva surta efecto en un sistema en el que una vez estuvo habilitada es a) deshabilitarla de la directiva de grupo y b) borrar el TPM en el sistema.

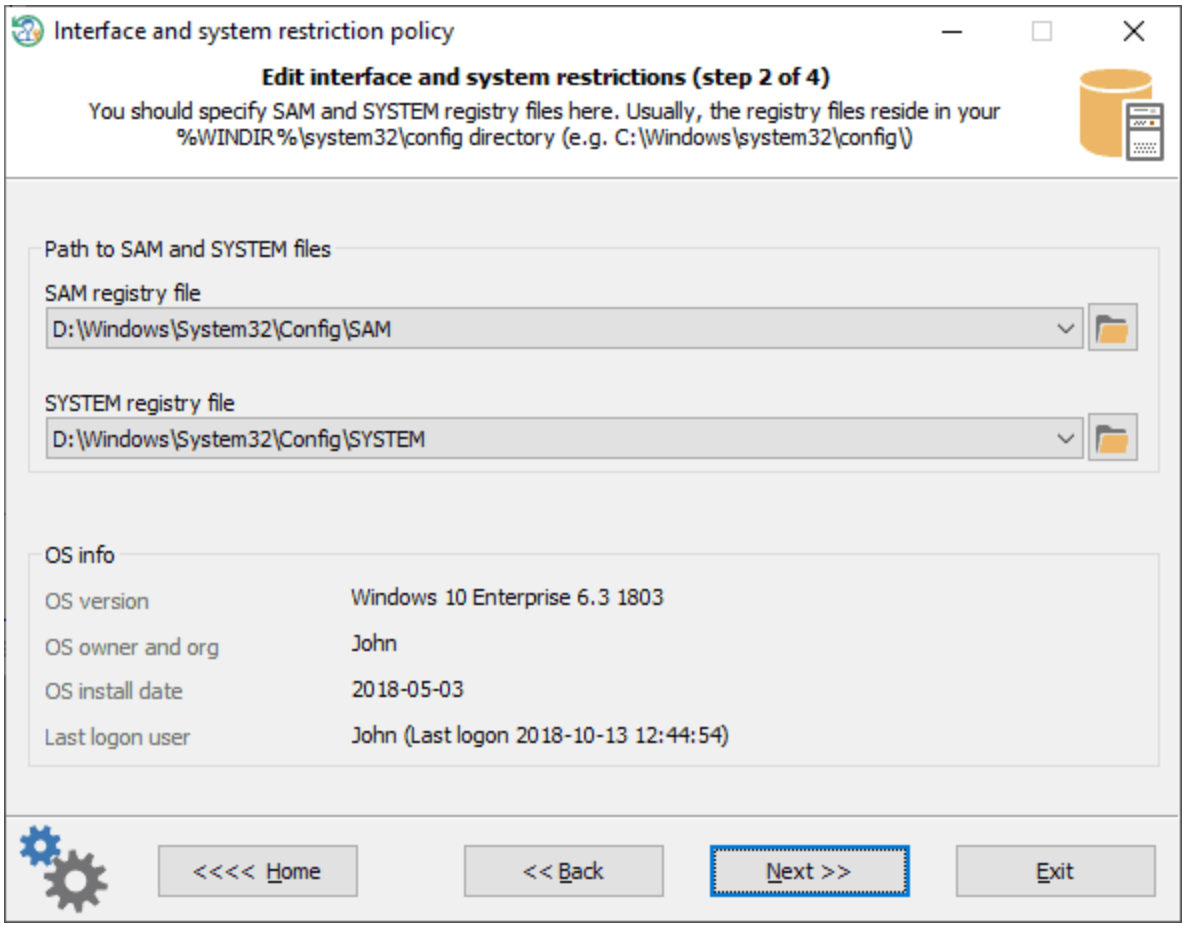
Omitir la lista predeterminada de comandos de TPM bloqueados	Si habilita esta configuración de directiva, Windows omitirá la lista predeterminada del equipo de comandos de TPM bloqueados y solo bloqueará los comandos de TPM especificados por la directiva de grupo o la lista local.
Omitir la lista local de comandos de TPM bloqueados	Si habilita esta configuración de directiva, Windows omitirá la lista local del equipo de comandos de TPM bloqueados y solo bloqueará los comandos de TPM especificados por la directiva de grupo o la lista predeterminada.
Umbral de bloqueo individual de usuario estándar	Esta configuración de directiva le permite administrar el número máximo de errores de autorización para cada usuario estándar para el Módulo de plataforma segura (TPM). Si el número de errores de autorización para el usuario dentro de la duración de la duración del bloqueo de usuario estándar es igual a este valor, se impide que el usuario estándar envíe comandos al Módulo de plataforma segura (TPM) que requieren autorización. Esta configuración ayuda a los administradores a evitar que el hardware de TPM entre en modo de bloqueo porque ralentiza la velocidad a la que los usuarios estándar pueden enviar comandos que requieren autorización al TPM. Si este valor no está configurado, se utiliza un valor predeterminado de 4.
Duración estándar del bloqueo del usuario	Esta configuración de directiva le permite administrar la duración en minutos para contar los errores de autorización de usuario estándar para los comandos del Módulo de plataforma segura (TPM) que requieren autorización. Si el número de comandos de TPM con un error de autorización dentro de la duración es igual a un umbral, se impide que un usuario estándar envíe comandos que requieran autorización al TPM. Si este valor no está configurado, se utiliza un valor predeterminado de 480 minutos (8 horas).
Umbral de bloqueo total del usuario estándar	Esta configuración de directiva le permite administrar el número máximo de errores de autorización para todos los usuarios estándar para el Módulo de plataforma segura (TPM). Si el número total de errores de autorización para todos los usuarios estándar dentro de la duración de la duración del bloqueo de usuario estándar es igual a este valor, se impide que todos los usuarios estándar envíen comandos al Módulo de plataforma segura (TPM) que requieren autorización. Esta configuración ayuda a los administradores a evitar que el hardware de TPM entre en modo de bloqueo porque ralentiza la velocidad a la que los usuarios estándar pueden enviar comandos que requieren autorización al TPM. Si este valor no está configurado, se utiliza un valor predeterminado de 9.
Activar la copia de seguridad de TPM en los Servicios de dominio de Active Directory (1 de 2)|	Si habilita esta opción junto con una anterior, se realizará una copia de seguridad automática y silenciosa de la información del propietario de TPM en AD DS cuando use Windows para establecer o cambiar una contraseña de propietario de TPM.
Activar la copia de seguridad de TPM en servicios de dominio de Active Directory (2 de 2)|	Si habilita esta opción junto con una anterior, se realizará una copia de seguridad automática y silenciosa de la información del propietario de TPM en AD DS cuando use Windows para establecer o cambiar una contraseña de propietario de TPM.

3.8 Política de restricción de interfaz y sistema

Puede utilizar esta función para cambiar o restablecer diferentes restricciones de interfaz y sistema para el usuario seleccionado. Por ejemplo, permitir/no permitir el acceso a aplicaciones específicas de

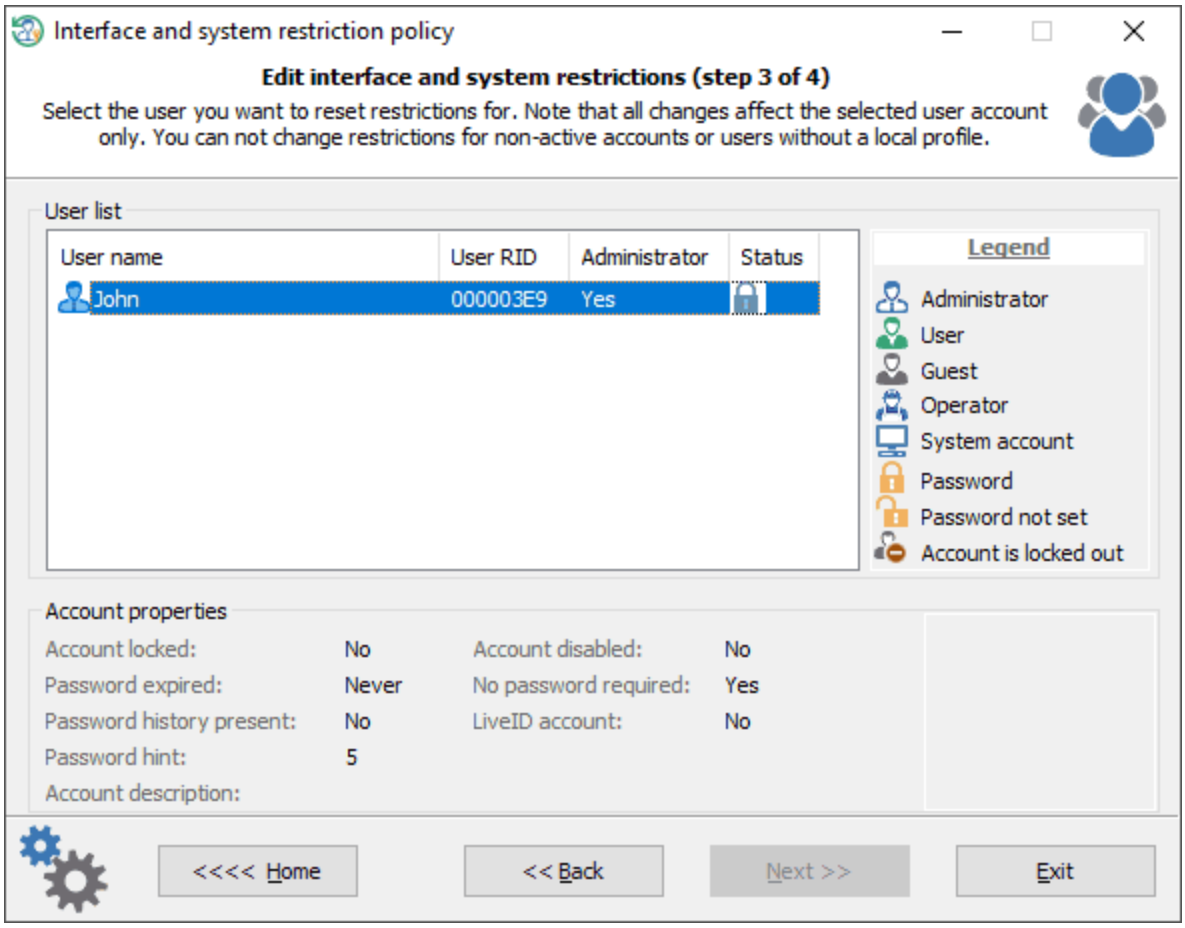
Windows, bloquear/desbloquear el cuadro de diálogo Ejecutar, habilitar/deshabilitar ciertas configuraciones del panel de control, permitir/impedir el acceso al símbolo del sistema o al registro de Windows, permitir/prohibir el acceso a CD-ROM o discos extraíbles, etc.

Elegir archivos de registro de Windows



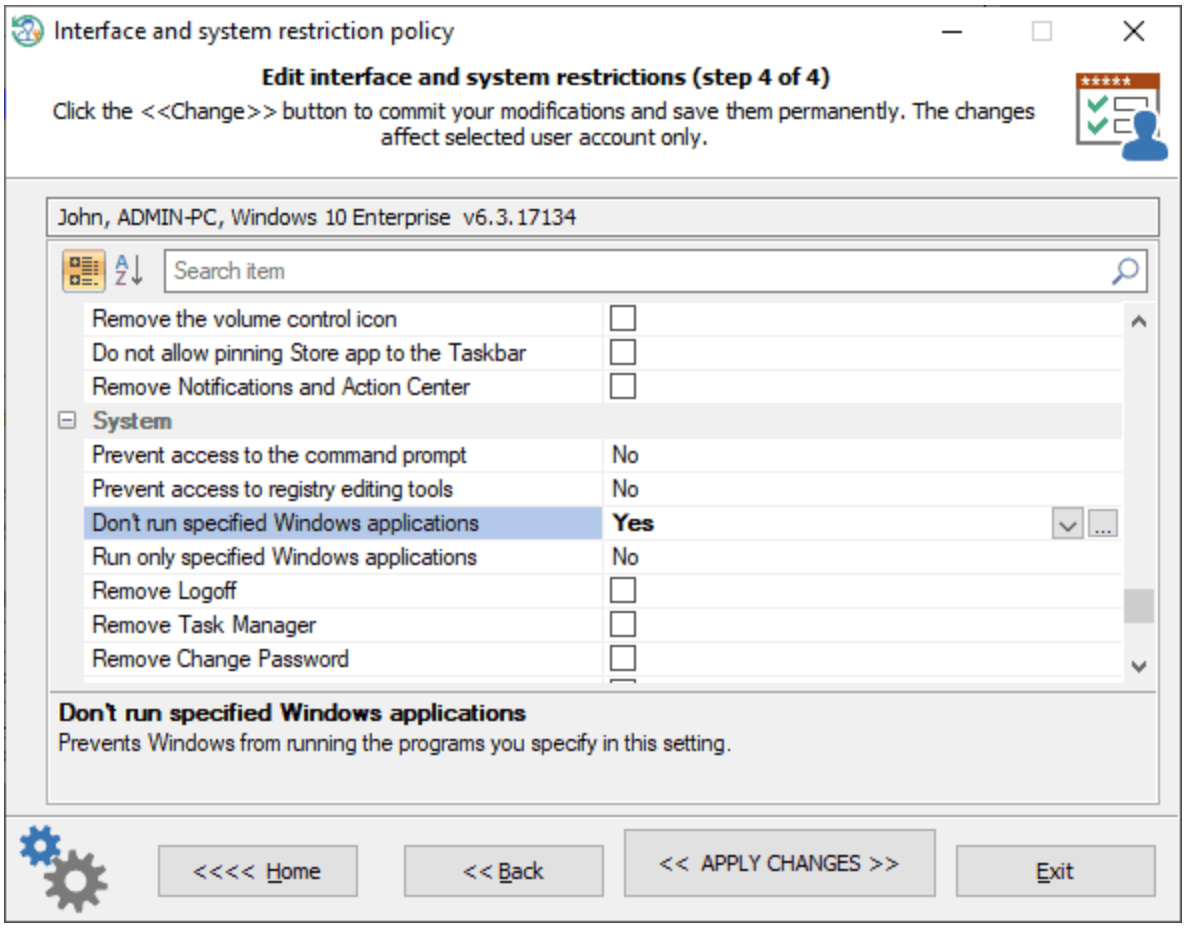
Elija los archivos de registro **SAM** y **SYSTEM** encontrados por el programa, o especifique la ruta a ellos manualmente.

Selección de la cuenta de usuario



Seleccione el usuario para el que desea cambiar o restablecer las restricciones. El programa muestra solo las cuentas activas que tienen un perfil local.

Cambio de las restricciones de la interfaz y del sistema para el usuario seleccionado



Una vez seleccionado el usuario, puede modificar la interfaz y las opciones del sistema disponibles para la cuenta de usuario. Haga clic en el botón << *APLICAR CAMBIOS* >> para confirmar los cambios.

Las opciones solo afectan a la cuenta de usuario seleccionada.

Breve descripción de la interfaz y las opciones del sistema.

Restricciones del **panel de control**:

Nombre	Descripción
Ocultar elementos especificados del Panel de control	Esta opción le permite mostrar u ocultar elementos especificados del Panel de control, como Mouse, Sistema o Personalización, desde la ventana Panel de control y la pantalla Inicio. La opción afecta a la pantalla Inicio y a la ventana panel de control, así como a otras formas de acceder a los elementos del Panel de control, como los accesos directos en Ayuda y soporte técnico o las líneas de comandos que usan control.exe. Esta directiva no tiene ningún efecto en los elementos que se muestran en la configuración de PC. Si habilita esta configuración, puede seleccionar elementos específicos que no se mostrarán en la ventana Panel de control y en la pantalla Inicio.
Mostrar solo los elementos especificados del Panel de control	Esta opción controla qué elementos del Panel de control, como Mouse, Sistema o Personalización, se muestran en la ventana Panel de control y en la pantalla Inicio. Los únicos elementos que se muestran en el Panel de control son los que especifique en esta configuración. Esta opción afecta a la pantalla Inicio y al Panel de control, así como a otras formas de acceder a los

	elementos del Panel de control, como los accesos directos de Ayuda y soporte técnico o las líneas de comandos que utilizan control.exe. Esta directiva no tiene ningún efecto en los elementos que se muestran en la configuración de PC. Por ejemplo, escriba Microsoft.Mouse, Microsoft.System o Microsoft.Personalization.
Prohibir el acceso a la configuración del Panel de control y del PC	Deshabilita todos los programas del Panel de control y la aplicación de configuración de PC. Esta opción impide que se inicie Control.exe y SystemSettings.exe, los archivos de programa para la configuración del Panel de control y pc. Como resultado, los usuarios no pueden iniciar la configuración del Panel de control o del PC, ni ejecutar ninguno de sus elementos.
Visibilidad de la página de configuración	Especifica la lista de páginas que se mostrarán u ocultarán de la aplicación Configuración del sistema. Esta directiva permite a un administrador bloquear un conjunto determinado de páginas desde la aplicación Configuración del sistema. Las páginas bloqueadas no serán visibles en la aplicación, y si todas las páginas de una categoría están bloqueadas, la categoría también se ocultará. Ejemplo: showonly:about,bluetooth hide:bluetooth
Deshabilitar el Panel de control de pantalla	Si habilita esta configuración, el Panel de control de pantalla no se ejecuta. Cuando los usuarios intentan iniciar Display, aparece un mensaje que explica que una configuración impide la acción.
Pestaña Ocultar configuración	Quita la ficha Configuración de la pantalla del Panel de control
Prevent changing theme	Esta opción deshabilita la galería de temas en el Panel de control de personalización.
Prevent changing visual style for windows and buttons	Evita que los usuarios o aplicaciones cambien el estilo visual de las ventanas y botones que se muestran en sus pantallas.
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	Determines whether settings that existed in Windows 2000 Server family will apply to Administrators.

settings for 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	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.

Everywhere link	
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	This option allows you to remove pinned programs from the taskbar.

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.

Restricciones del **sistema**:

Nombre	**Descripción**
Impedir el acceso al símbolo del sistema	Esta opción impide que los usuarios ejecuten el símbolo del sistema interactivo, Cmd.exe. Esta opción también determina si los archivos por lotes (.cmd y .bat) pueden ejecutarse en el equipo. Si habilita esta opción y el usuario intenta abrir una ventana de comandos, el sistema muestra un mensaje que explica que una configuración impide la acción.
Impedir el acceso a las herramientas de edición del Registro	Deshabilita el editor del registro de Windows Regedit.exe. Si habilita esta opción y el usuario intenta iniciar Regedit.exe, aparece un mensaje que explica que una configuración impide la acción.
No ejecutar aplicaciones de Windows especificadas	Impide que Windows ejecute los programas que especifique en esta configuración.
Ejecutar solo aplicaciones de Windows especificadas	Limita los programas de Windows que los usuarios tienen permiso para ejecutar en el equipo.
Eliminar cierre de sesión	Esta opción deshabilita o elimina todos los elementos de menú y botones que cierran la sesión del usuario en el sistema. Si habilita esta configuración, los usuarios no verán el elemento de menú Cerrar sesión cuando presionen Ctrl+Alt+Supr. Esto evitará que cierren la sesión a menos que reinicien o apaguen el equipo, o que hagan clic en Cerrar sesión en el menú Inicio.
Quitar el Administrador de tareas	Esta opción impide que los usuarios inicien el Administrador de tareas. Si habilita esta configuración, los usuarios no podrán acceder al Administrador de tareas. Si los usuarios intentan iniciar el Administrador de tareas, aparece un mensaje que explica que una directiva impide la acción.

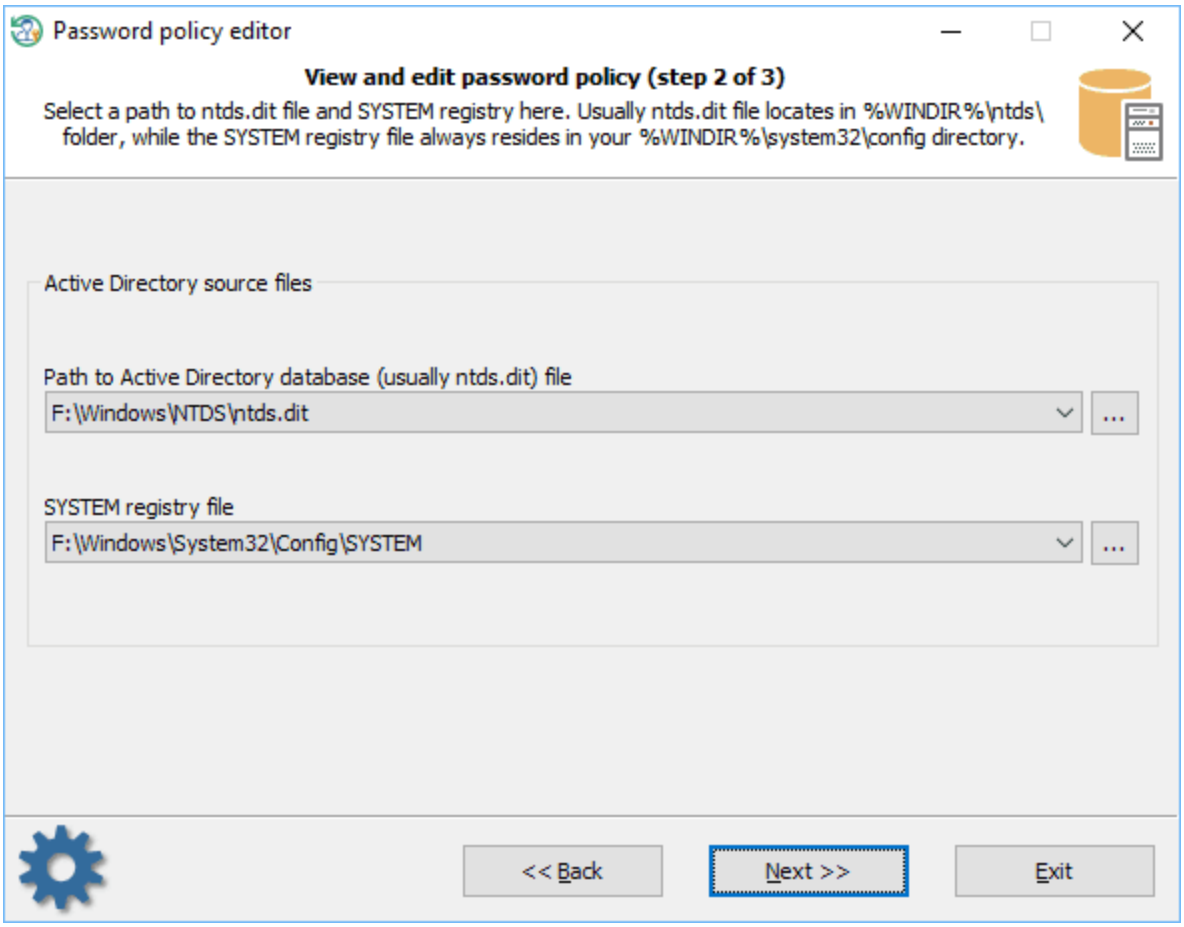
Eliminar Cambiar contraseña	Esta opción impide que los usuarios cambien su contraseña de Windows a petición. Si habilita esta configuración, el botón 'Cambiar contraseña' en el cuadro de diálogo Seguridad de Windows no aparecerá cuando presione Ctrl + Alt + Supr.
Quitar bloquear computadora	Esta opción impide que los usuarios bloqueen el sistema. Si habilita esta configuración, los usuarios no podrán bloquear el equipo desde el teclado mediante Ctrl+Alt+Supr.
Todas las clases de almacenamiento extraíble: denegar todo el acceso	Configure el acceso a todas las clases de almacenamiento extraíbles.
Discos extraíbles: Denegar el acceso de lectura	Esta opción deniega el acceso de lectura a los discos extraíbles.
Discos extraíbles: Denegar el acceso de escritura	Esta opción deniega el acceso de escritura a los discos extraíbles.
CD y DVD: Denegar el acceso de lectura	Esta opción deniega el acceso de lectura a la clase de almacenamiento extraíble de CD y DVD.
CD y DVD: Denegar el acceso de escritura	Esta opción deniega el acceso de escritura a la clase de almacenamiento extraíble de CD y DVD.
Dispositivos WPD: Denegar el acceso de lectura	Esta opción deniega el acceso de lectura a los discos extraíbles, que pueden incluir reproductores multimedia, teléfonos celulares, pantallas auxiliares y dispositivos CE.
Dispositivos WPD: Denegar el acceso de escritura	Esta opción deniega el acceso de escritura a discos extraíbles, que pueden incluir reproductores multimedia, teléfonos celulares, pantallas auxiliares y dispositivos CE.
Unidades de disquete: Denegar el acceso de lectura	Esta opción deniega el acceso de lectura a la clase de almacenamiento extraíble de las unidades de disquete, incluidas las unidades de disquete USB.
Unidades de disquete: Denegar el acceso de escritura	Esta opción deniega el acceso de escritura a la clase de almacenamiento extraíble unidades de disquete, incluidas las unidades de disquete USB.
Unidades de cinta: Denegar el acceso de lectura	Esta opción deniega el acceso de lectura a la clase de almacenamiento extraíble de unidad de cinta.
Unidades de cinta: Denegar el acceso de escritura	Esta opción deniega el acceso de escritura a la clase de almacenamiento extraíble de unidad de cinta.

3.9 Editor de políticas de contraseñas

A veces, para que la configuración de seguridad funcione correctamente, es vitalmente necesario configurar la política de contraseñas de la estación de trabajo o del dominio. Por ejemplo, si desea denegar a los usuarios del dominio que inicien sesión en un sistema sin proporcionar contraseñas seguras, debe restringirlo a través de la directiva de contraseñas de dominio. Sin embargo, eso sería un gran problema si no puede iniciar sesión en la estación de trabajo o en el dominio como administrador. El editor de políticas de contraseñas del nuevo RWP puede evitar el problema y permite cambiar varias

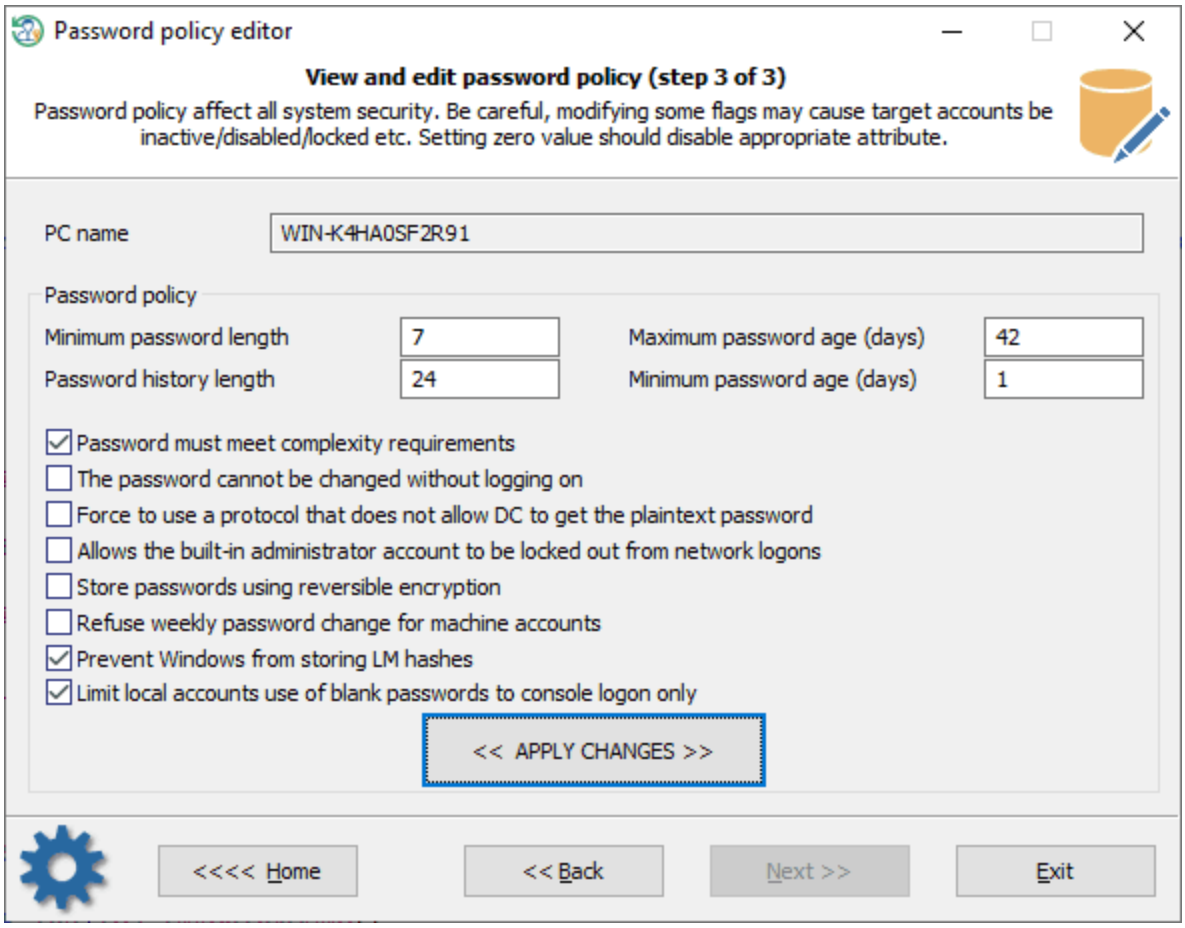
propiedades de la política de contraseñas en cualquier sistema Windows sin iniciar sesión en el sistema.

Selección del origen de datos



En primer lugar, deberá alimentar el programa con dos archivos del sistema:
- SAM y SYSTEM, en caso de que desee modificar la política de contraseñas de una estación de trabajo o de un PC independiente;
- o NTDS. DIT y SYSTEM, cuando necesite cambiar las propiedades de la política de contraseñas de un dominio.
El programa debe tratar de encontrar los archivos automáticamente. Sin embargo, puede proporcionar las rutas manualmente.

Cambio de la política de contraseñas



Aquí está la breve descripción de lo que puede modificar en la política de contraseñas del sistema de destino:

- Longitud mínima de la contraseña: longitud mínima de una contraseña válida, en caracteres.
- Longitud del historial de contraseñas: número de contraseñas anteriores guardadas en la lista de historial. Un usuario no puede reutilizar una contraseña de la lista.
- Antigüedad máxima de la contraseña: longitud máxima (en días) en que una contraseña puede permanecer igual. Las contraseñas anteriores a esta deben cambiarse.
- Antigüedad mínima de la contraseña: período mínimo de tiempo antes de que se pueda cambiar una contraseña.
- La contraseña debe cumplir con los requisitos de complejidad: las contraseñas deben cumplir con los siguientes requisitos mínimos: no contener el nombre de la cuenta del usuario o una parte de él, tener al menos seis caracteres de longitud (si no se establece lo contrario), contener caracteres de al menos tres conjuntos de caracteres, no ser uno utilizado anteriormente (si se establece el historial de contraseñas).
- La contraseña no se puede cambiar sin iniciar sesión: la contraseña no se puede cambiar sin iniciar sesión. De lo contrario, si ha caducado, puede cambiarlo y luego iniciar sesión.
- Forzar el uso de un protocolo que no permite al controlador de dominio obtener la contraseña de texto sin formato: obliga al cliente a usar un protocolo que no permite que el controlador de dominio obtenga contraseñas de texto sin formato.
- Permite bloquear la cuenta de administrador integrada de los inicios de sesión de red
- Almacene contraseñas utilizando cifrado reversible: fuerce el almacenamiento de contraseñas de texto sin formato para todos los usuarios en lugar de hashear las contraseñas.

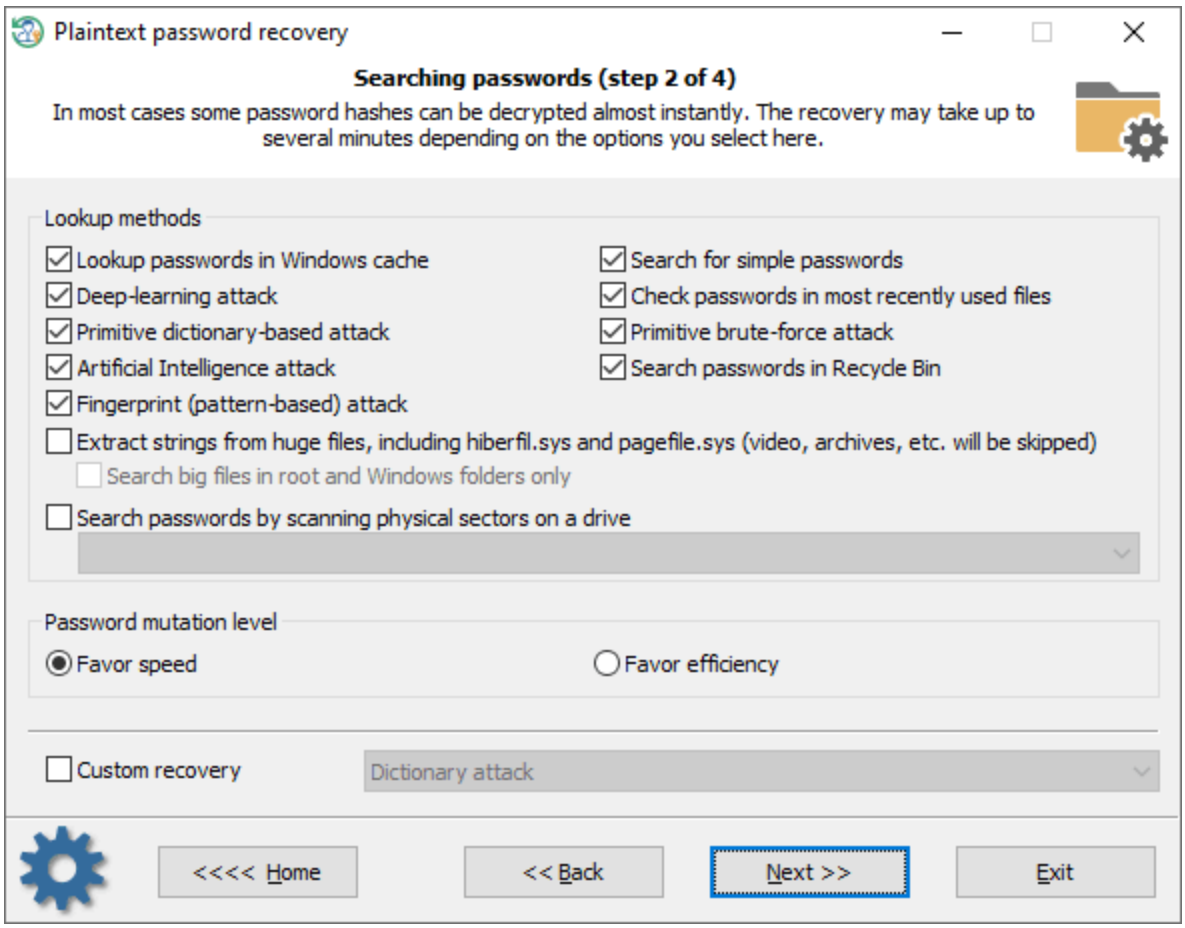
- Rechazar el cambio semanal de contraseña para las cuentas de máquina: elimina el requisito de que cualquier cuenta de máquina cambie automáticamente su contraseña cada semana.
- Impedir que Windows almacene hashes de LM. El hash de LAN Manager utiliza un algoritmo de cifrado extremadamente débil. Esta configuración controla si un hash LM de la contraseña se puede almacenar en Active Directory y en la base de datos SAM local (la próxima vez que se cree un nuevo usuario o se cambie la contraseña). Esta configuración está de forma predeterminada en Windows Vista y sistemas operativos posteriores.
- Limite las cuentas locales para que usen contraseñas en blanco solo para el inicio de sesión de la consola. Evite que existan cuentas con contraseñas en blanco en un sistema. Sin embargo, si existía una cuenta local con una contraseña en blanco, habilitar esta configuración impedirá el acceso a la red, limitando la cuenta solo al inicio de sesión de la consola local.

Para deshabilitar un atributo editable, simplemente establezca el valor cero en su cuadro de edición.

¡Tenga cuidado, alterar cualquier valor de la política de contraseñas afectará toda la seguridad del sistema Windows!

3.10 Buscar contraseñas de inicio de sesión

Configuración de métodos de búsqueda y recuperación

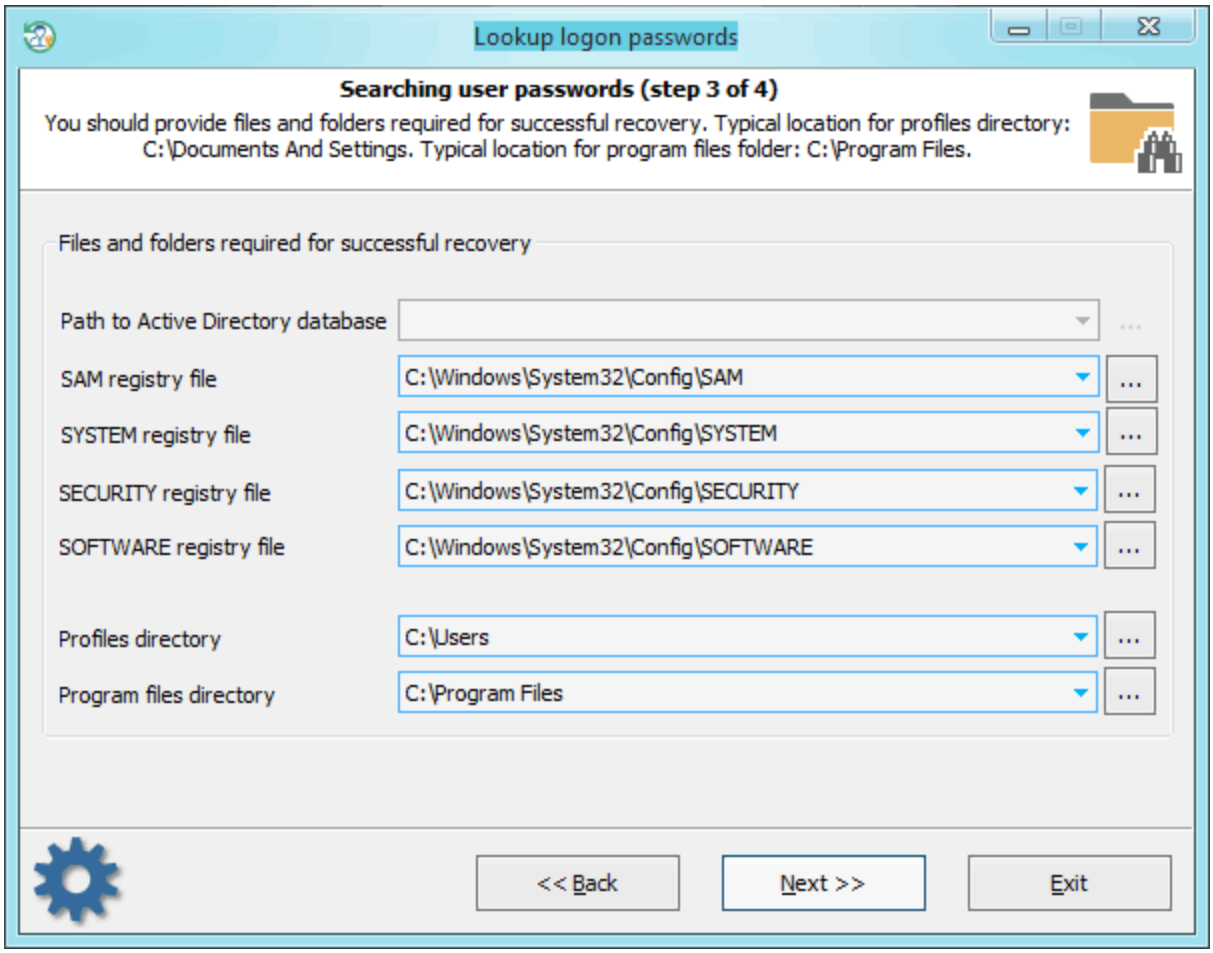


Encontrar las contraseñas de los usuarios requiere 11 pasos:

1. Búsqueda de información en la memoria caché del sistema de Windows. Este método, a su vez, consiste en más de una docena de mini-ataques, durante los cuales el programa analiza todo tipo de contraseñas del sistema, desde secretos pasando por contraseñas DSL, FTP, IM, etc.
2. Análisis de contraseñas simples y cortas, atajos de teclado, etc.
3. Búsqueda de contraseñas mediante algoritmos de aprendizaje profundo. A pesar de que estos algoritmos se reducen significativamente para cumplir con los requisitos de la CPU, funcionan mucho mejor en comparación con los anteriores.
4. Escanee, analice y analice los archivos utilizados más recientemente del sistema de destino.
5. Ataque de diccionario primitivo. La aplicación comprueba todas las contraseñas del diccionario incorporado para las ediciones Light y Standard o de varios diccionarios (árabe, chino, inglés, francés, alemán, portugués, ruso, español) para la edición avanzada. Si la opción de búsqueda profunda está activada, las mutaciones de palabras simples también se tendrán en cuenta durante la búsqueda.
6. Ataque primitivo de fuerza bruta.
7. Ataque de Inteligencia Artificial. Este es nuestro pequeño 'sabes-como'. El ataque analiza la actividad de red de un usuario en el equipo. Más de treinta mini-módulos se encargan de eso. Sobre los resultados del análisis, la aplicación genera preferencias de usuario y genera un diccionario semántico para el ataque, que luego utiliza para encontrar la contraseña.
8. Busque contraseñas en archivos eliminados.
9. Ataque de huellas dactilares primitivas en algunas contraseñas inglesas complicadas.
10. Extraiga cadenas de archivos enormes: imágenes RAM, hiberfil.sys, archivo de página.sys etc. Cuando se establece esta opción, el programa intentará omitir archivos inútiles en el análisis de contraseñas como video, archivos, archivos de audio, etc.
11. Busque contraseñas leyendo y analizando sectores sin procesar de la unidad seleccionada. Esta característica funciona tanto para hashes LM como NTLM, buscando contraseñas ASCII y UNICODE. Si el '*Nivel de mutación de contraseña*' se establece a '*Favorecer eficiencia*', el programa también intenta mutar todas las contraseñas encontradas, por lo que caminar por todos los sectores de la unidad de destino puede llevar bastante tiempo. Tenga en cuenta que el algoritmo de escaneo basado en sectores no es efectivo contra las unidades que tienen un cifrado de disco completo establecido. Como Bitlocker o TrueCrypt, por ejemplo.

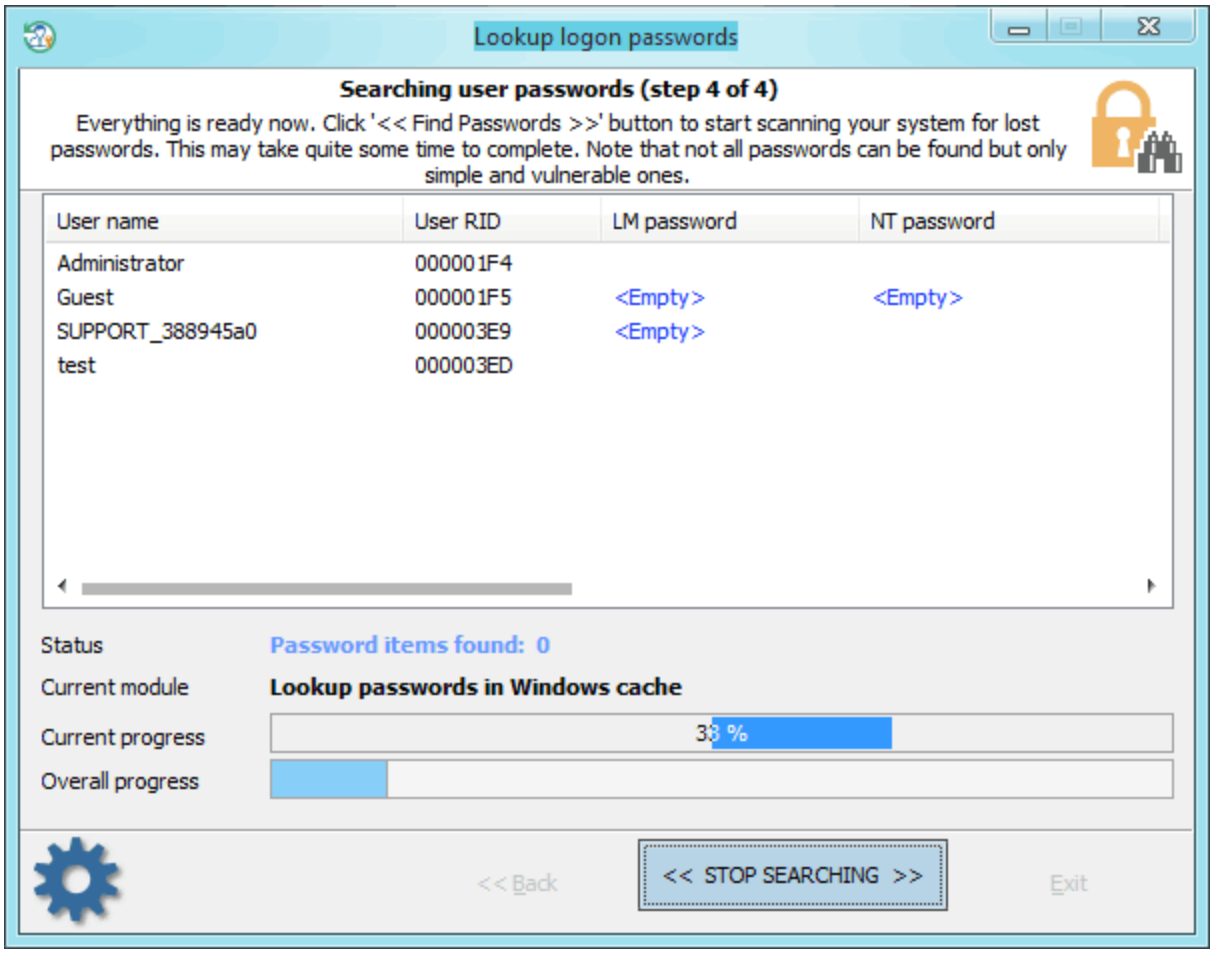
Para aplicar un método de recuperación personalizado, active la opción 'Recuperación personalizada' y seleccione uno de los ataques disponibles. En el siguiente paso, se le pedirá que configure varias opciones relacionadas con el ataque seleccionado.

Selección del origen de datos



Al buscar contraseñas, se debe prestar especial atención a la introducción de archivos y carpetas necesarios para el proceso de análisis. Sin ellos, la búsqueda de contraseñas será ineficiente. La aplicación encuentra los archivos automáticamente, pero a veces, por ejemplo, cuando la computadora tiene varios sistemas operativos instalados, es posible que deba usar el 'control manual'. Tenga en cuenta también que si la computadora tiene 2 o más unidades de disco duro, la secuencia de las letras para estos discos se puede configurar de manera totalmente diferente a la del sistema original.

Búsqueda y descifrado de contraseñas



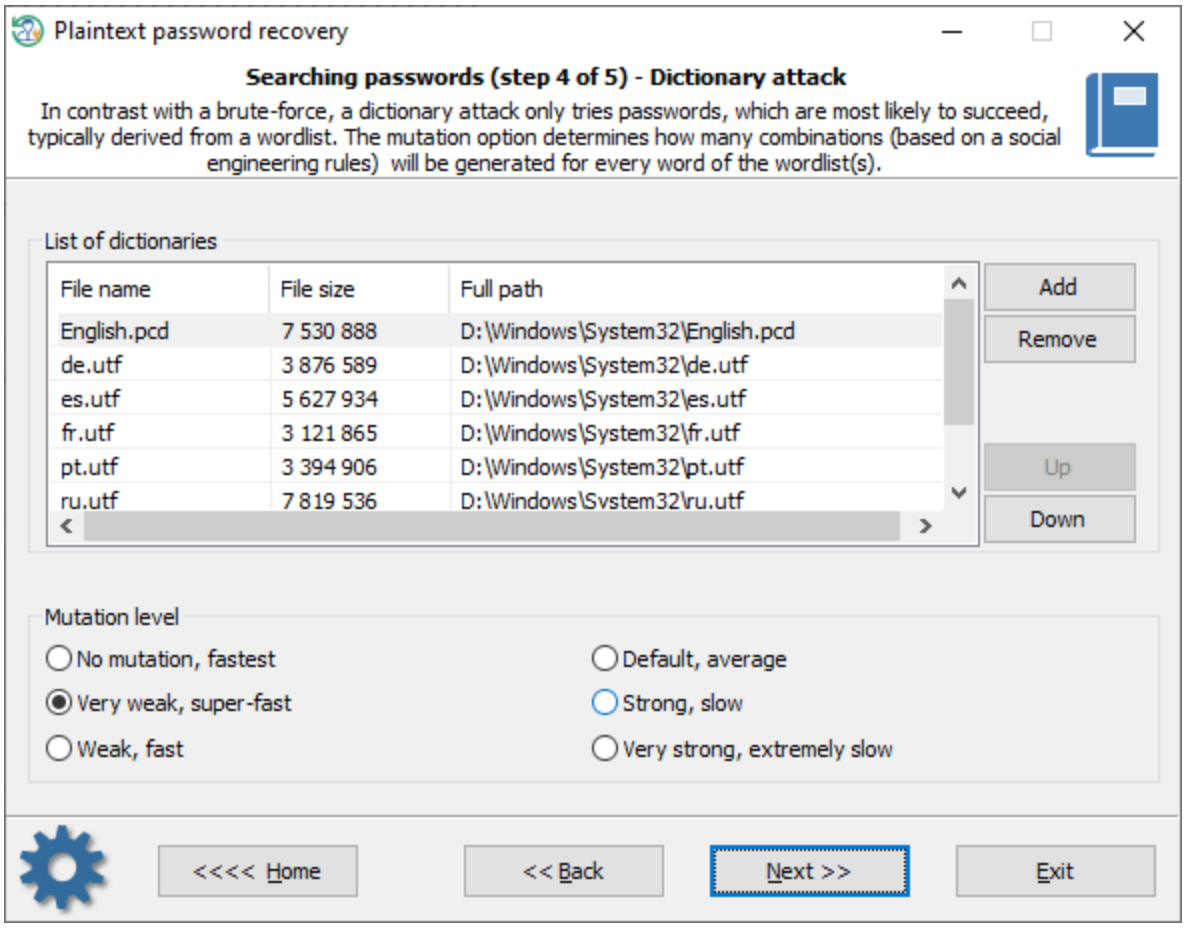
Encontrar/analizar contraseñas puede llevar algún tiempo, lo que depende de la configuración de ataque y las peculiaridades de su sistema. Completar la búsqueda normalmente toma aproximadamente 10-15 minutos sin ataques de búsqueda de tablas y discos de Passcape. El ataque a la tabla Passcape lleva mucho más tiempo y depende de su CPU y del número de hashes que desea recuperar. Por ejemplo, en una CPU de 2 núcleos, generalmente toma hasta 3 minutos para un solo hash.

3.10.1 Recuperación personalizada

Una vez que se establece la opción de recuperación personalizada, el programa también puede ejecutar 3 ataques diferentes para adivinar las contraseñas:

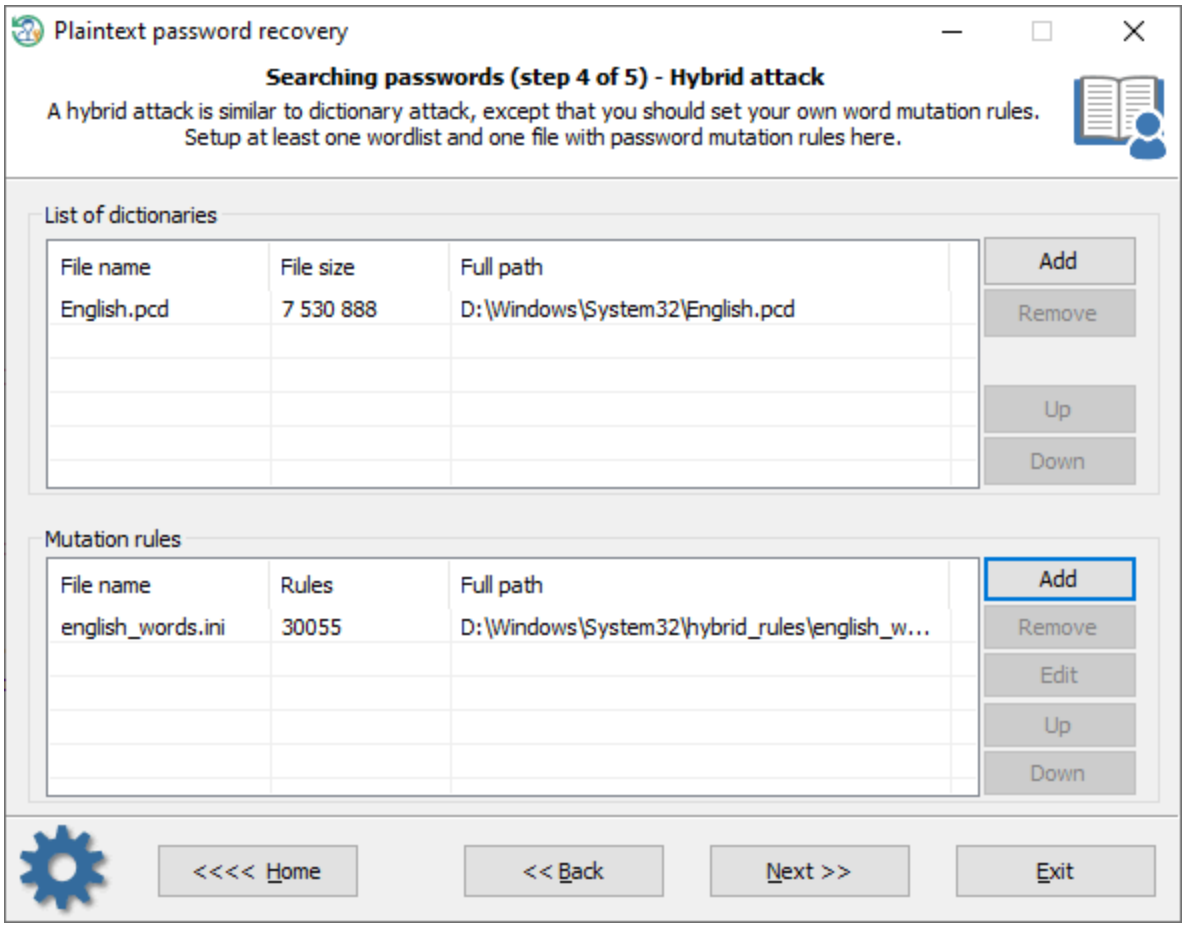
- Ataque de diccionario
- Ataque híbrido
- Ataque de máscara

Ataque de diccionario



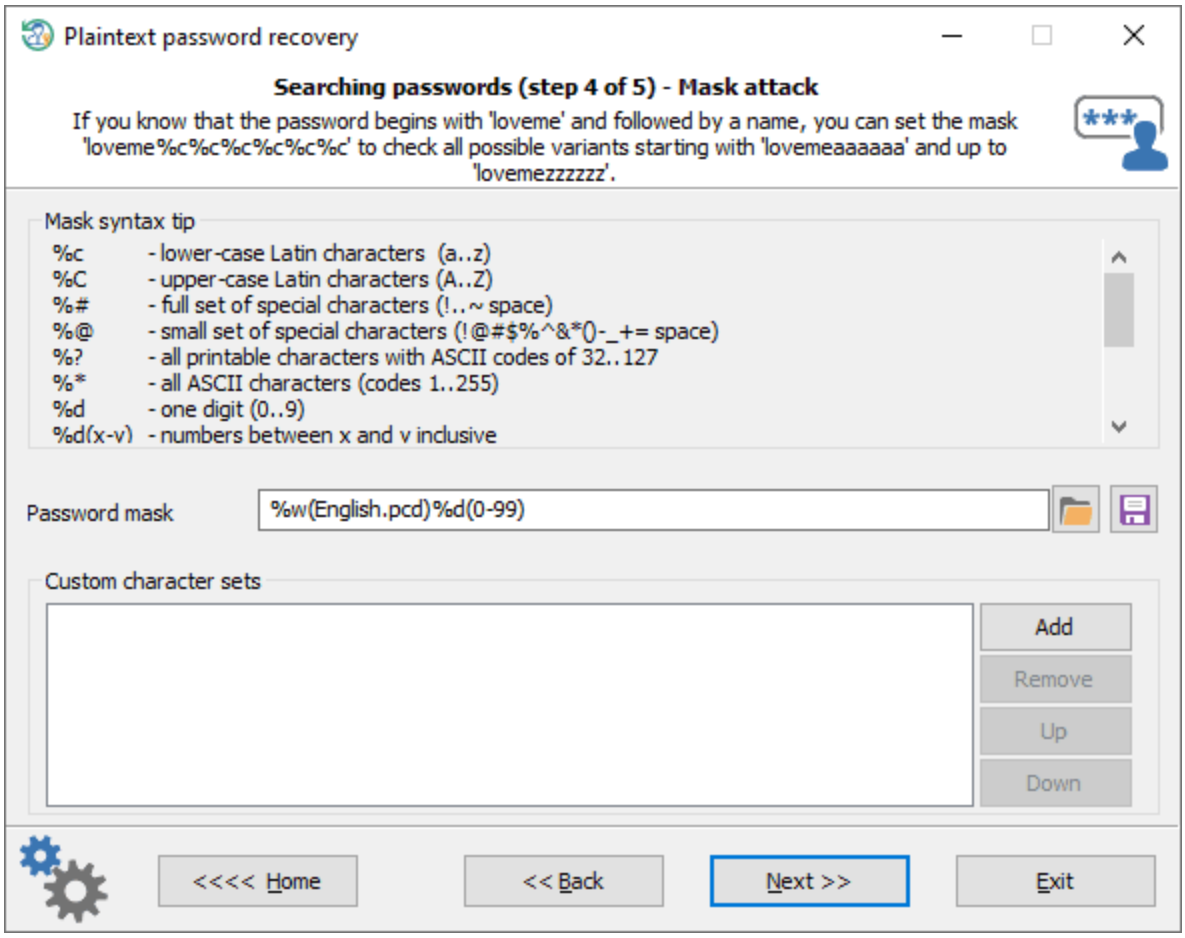
Un ataque de diccionario intenta contraseñas, que tienen más probabilidades de tener éxito, generalmente derivadas de una lista de palabras. RWP soporta diferentes tipos de diccionarios: ASCII, UNICODE, UTF8, así como diccionarios cifrados/comprimidos en formato PCD nativo. Puede utilizar diccionarios predefinidos y personalizados. Para agregar su propia lista de palabras, copie una en una unidad USB y conecte la unidad a la PC de destino. El nivel de mutación determina cuántas combinaciones (basadas en reglas de ingeniería social) se generarán para cada palabra de la(s) lista(s) de palabras.

Ataque híbrido



Un ataque híbrido es similar a uno de diccionario, excepto que puede establecer sus propias reglas de mutación de palabras. El programa viene con un gran conjunto de archivos de reglas. Simplemente use uno que sea mejor para su tarea. Lo bueno de un ataque híbrido es que además puedes crear, editar y modificar reglas de mutación de contraseña según tus necesidades.

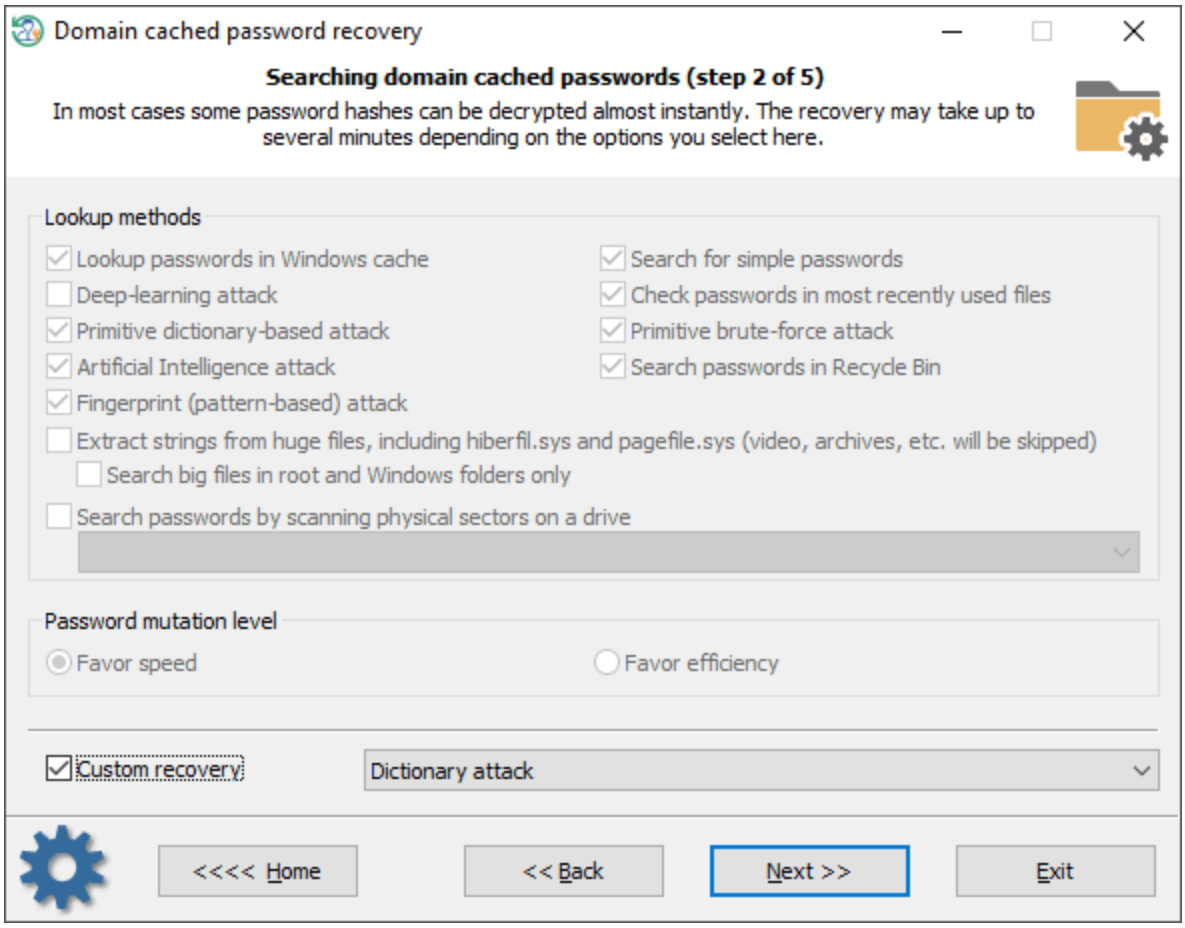
Ataque de máscara



Un Ataque de máscara es una herramienta insustituible cuando conoce una parte de la contraseña o tiene algún detalle específico sobre ella. Por ejemplo, si sabes que la contraseña consta de 12 caracteres y comienza con 'loveme', obviamente basta con adivinar los últimos 6 caracteres de la contraseña. Para eso está el ataque de la máscara. En nuestro ejemplo, puede configurar la siguiente máscara: loveme%c%c%c%c%c%c%c%c
Para obtener más información sobre cómo funciona la máscara, consulte nuestra documentación en línea.

3.11 Buscar contraseñas almacenadas en caché de dominio

Configuración de las opciones de búsqueda y recuperación



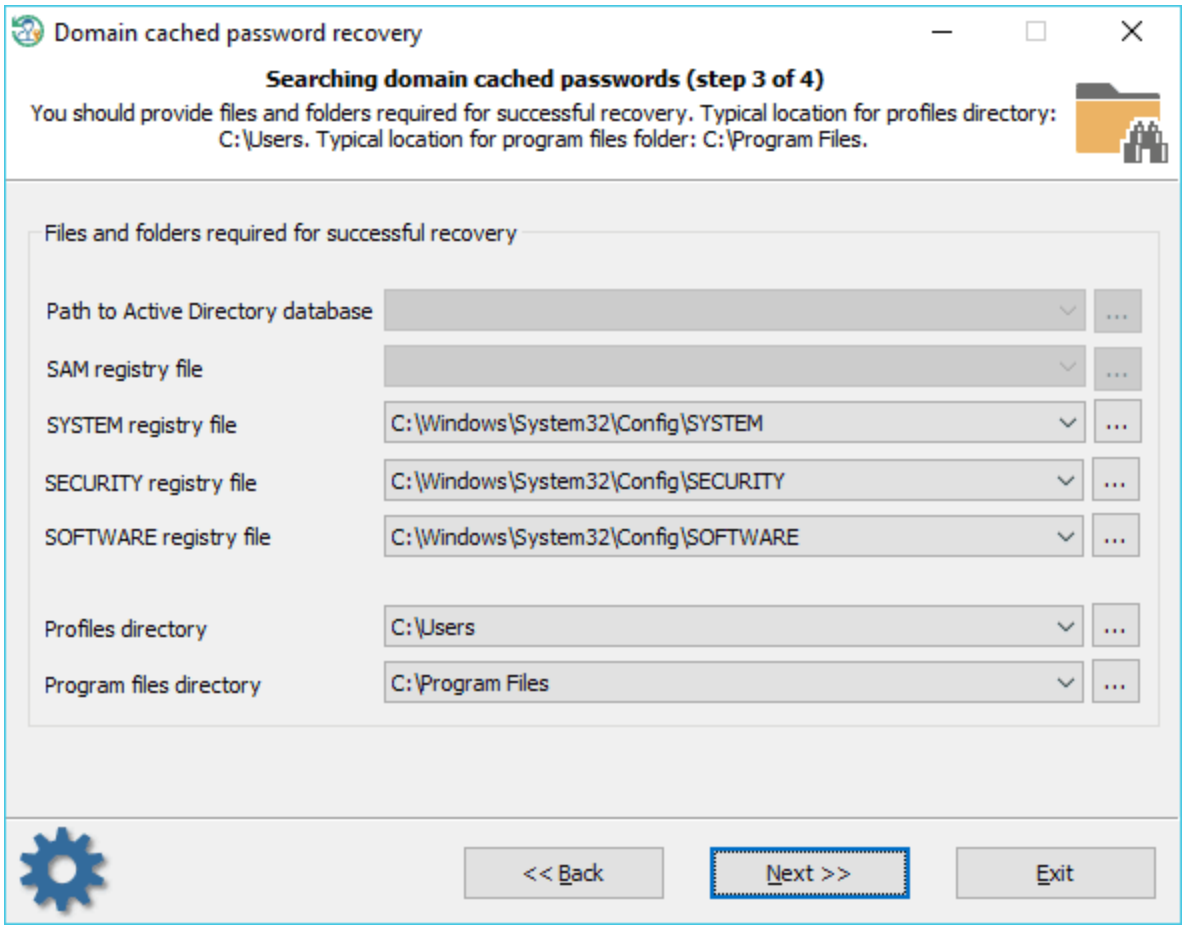
La recuperación de contraseñas almacenadas en caché de dominio consta de varios módulos. Cada uno se puede encender/apagar por separado:

1. Búsqueda de información en la memoria caché del sistema de Windows. Este módulo consta de más de una docena de mini-ataques, durante los cuales el programa analiza todo tipo de contraseñas del sistema: secretos LSA, DSL, FTP, LAN, contraseñas WAN, credenciales de Internet y correo electrónico, etc. Posteriormente las contraseñas encontradas son utilizadas por el programa para comprobar otras contraseñas generando variaciones más complejas.
2. Analizar contraseñas simples, cortas y numéricas, combinaciones de teclado, etc. Más de 20 mini-módulos en total.
3. Escanear, leer y analizar los archivos utilizados más recientemente del sistema de destino. El programa analiza los archivos y crea una lista de palabras (generando varias mutaciones) para ser verificadas como contraseñas.
4. Ataque de diccionario primitivo. La aplicación comprueba todas las contraseñas del diccionario incorporado para las ediciones Light y Standard o de varios diccionarios (árabe, chino, inglés, francés, alemán, portugués, ruso, español) para la edición avanzada. Si la opción de búsqueda profunda está activada, las mutaciones de palabras simples también se tendrán en cuenta durante la búsqueda.
5. Módulo primitivo de fuerza bruta que consiste en varios ataques simples para buscar contraseñas cortas.
6. El módulo de Inteligencia Artificial analiza la actividad de red de los usuarios en la computadora de destino. Más de treinta mini-módulos se encargan de eso. Sobre los resultados del análisis, la aplicación genera preferencias del usuario y crea un diccionario semántico para el ataque. Luego, el diccionario se usa para adivinar contraseñas.

7. Búsqueda de contraseñas en archivos eliminados.
8. Ataque de huellas dactilares primitivas en contraseñas inglesas. Este módulo puede tardar mucho tiempo en completarse.
9. Extraiga cadenas de archivos enormes: imágenes RAM, hiberfil.sys, archivo de página.sys etc. El programa puede omitir archivos inútiles en el análisis de contraseñas como video, archivos, archivos de audio, etc.
10. Búsqueda de contraseñas mediante la lectura y el análisis de sectores sin procesar de la unidad seleccionada. Si el nivel de mutación de la contraseña se establece en '*Favorecer eficiencia*', el programa también intenta mutar todas las contraseñas encontradas, por lo que caminar por todos los sectores de la unidad de destino puede llevar bastante tiempo. Este módulo no es efectivo para unidades que tienen un cifrado de disco completo establecido. Como Bitlocker o TrueCrypt, por ejemplo.

Para aplicar un método de recuperación personalizado, active la opción 'Recuperación personalizada' y seleccione uno de los ataques disponibles. En el siguiente paso, se le pedirá que configure varias opciones relacionadas con el ataque seleccionado.

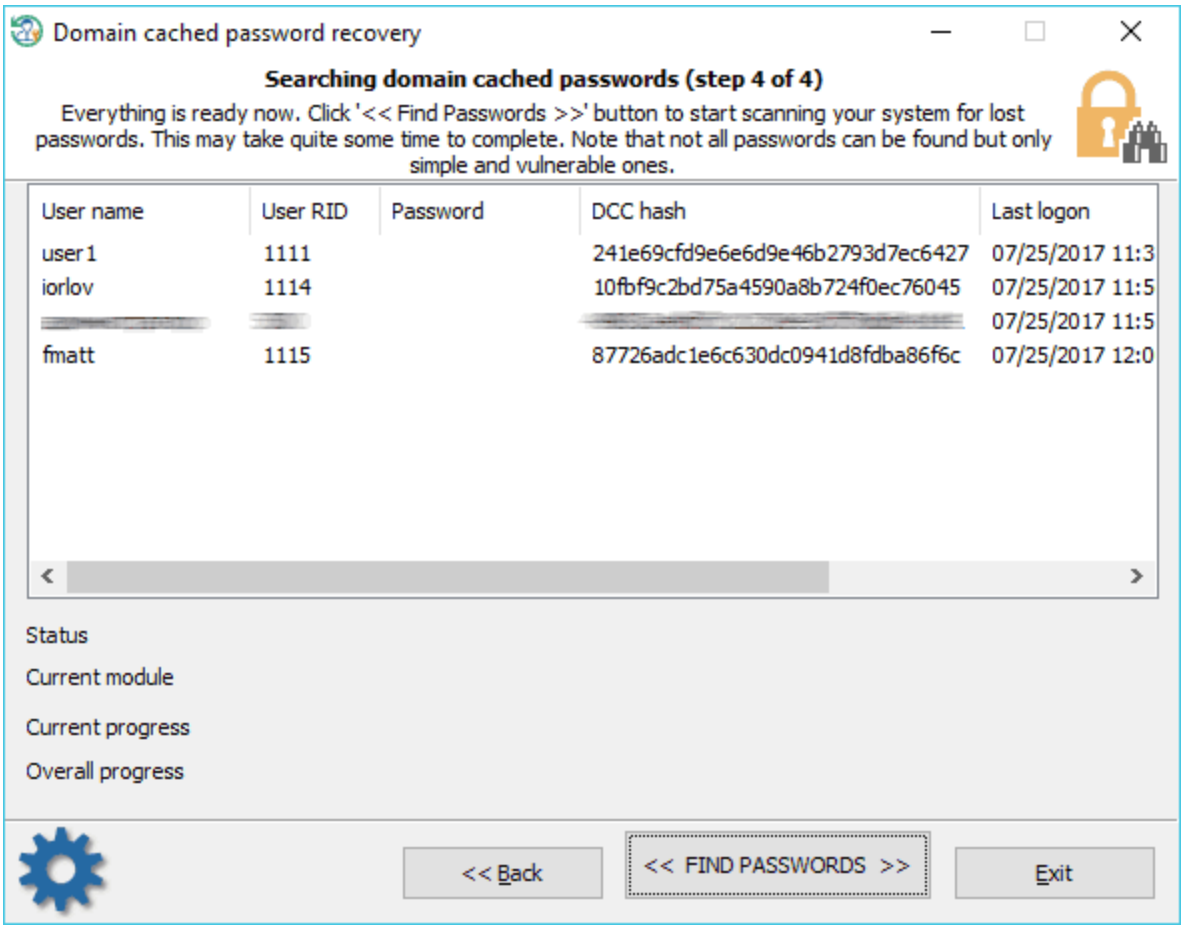
Selección del origen de datos



Al buscar contraseñas almacenadas en caché de dominio, se debe prestar especial atención a la configuración adecuada de los archivos y carpetas necesarios para el proceso. RWP encuentra los archivos automáticamente, pero a veces, por ejemplo, cuando la computadora tiene varios sistemas

operativos instalados, es posible que deba ajustarlo manualmente. También tenga en cuenta que si la PC de destino tiene 2 o más unidades de disco duro, la secuencia de las letras para estos discos se puede configurar de manera totalmente diferente a la del sistema original.

Búsqueda de contraseñas almacenadas en caché de dominio



Las credenciales almacenadas en caché de dominio son de dos tipos. DCC tipo 1 tiene un cifrado muy débil y se utilizó en los sistemas operativos Windows 2000, Windows XP y Windows 2003. La tasa de recuperación puede exceder millones o incluso miles de millones de contraseñas por segundo. DCC tipo 2 se utiliza en Windows Vista y sistemas operativos posteriores. Su cifrado es mucho más fuerte y bastante resistente al agrietamiento. La velocidad de fuerza bruta es de solo cientos / miles de contraseñas por segundo. ¡Imagínese, adivinar una contraseña de 8 caracteres que consiste en letras mayúsculas y minúsculas usando un ataque de fuerza bruta podría llevar más de 1000 años!

Tenga en cuenta las siguientes consideraciones:

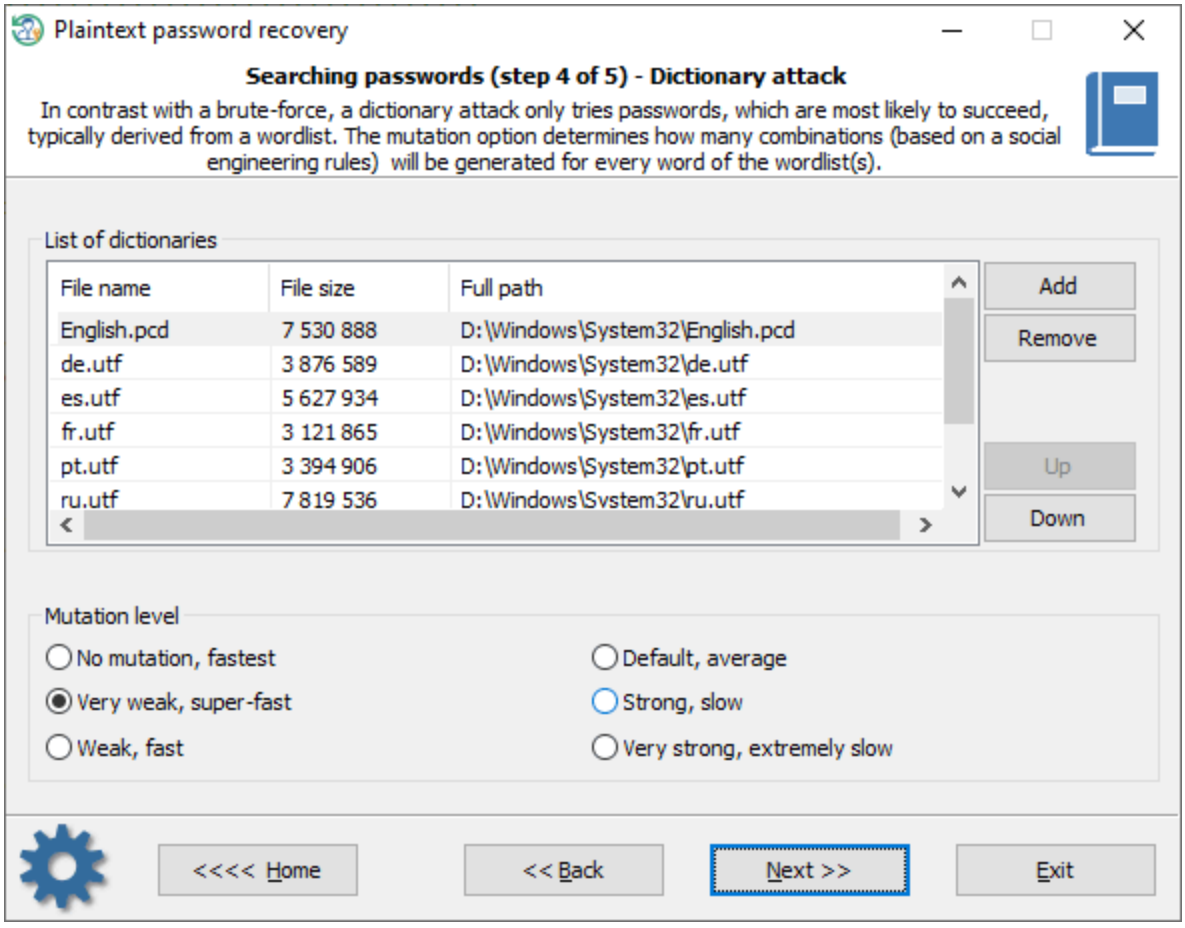
- El proceso de búsqueda de DCC tipo 2 es extremadamente lento. Completar algunos módulos (por ejemplo, el ataque de huellas dactilares) puede llevar horas o incluso días.
- Para acelerar la búsqueda, seleccione solo la cuenta para la que necesita la contraseña. Simplemente haga clic con el botón derecho en la entrada en caché y seleccione '*Excluir de la búsqueda todas las entradas excepto la seleccionada*'. De lo contrario, la velocidad de recuperación de la contraseña disminuirá en un múltiplo del número de cuentas.

3.11.1 Recuperación personalizada

Una vez que se establece la opción de recuperación personalizada, el programa también puede ejecutar 3 ataques diferentes para adivinar las contraseñas:

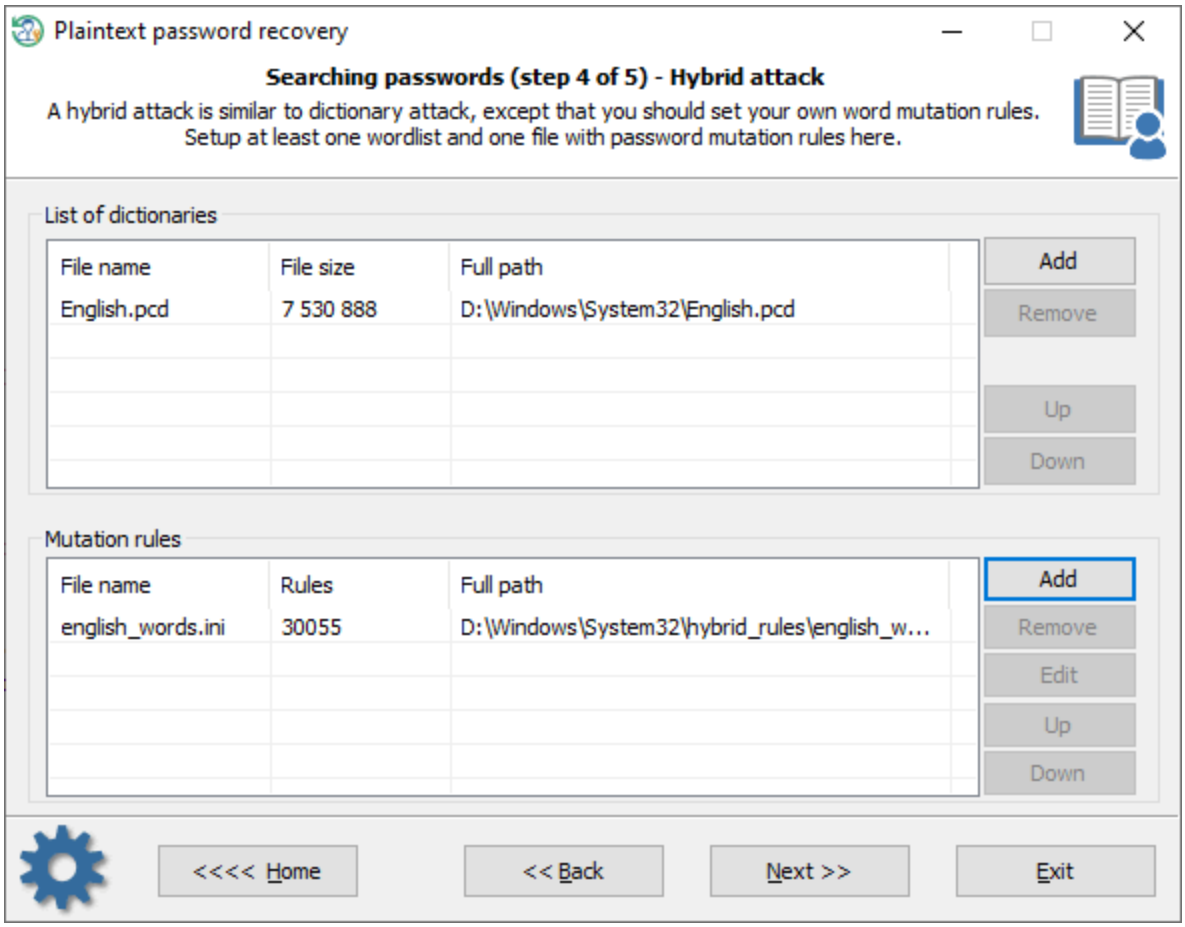
- Ataque de diccionario
- Ataque híbrido
- Ataque de máscara

Ataque de diccionario



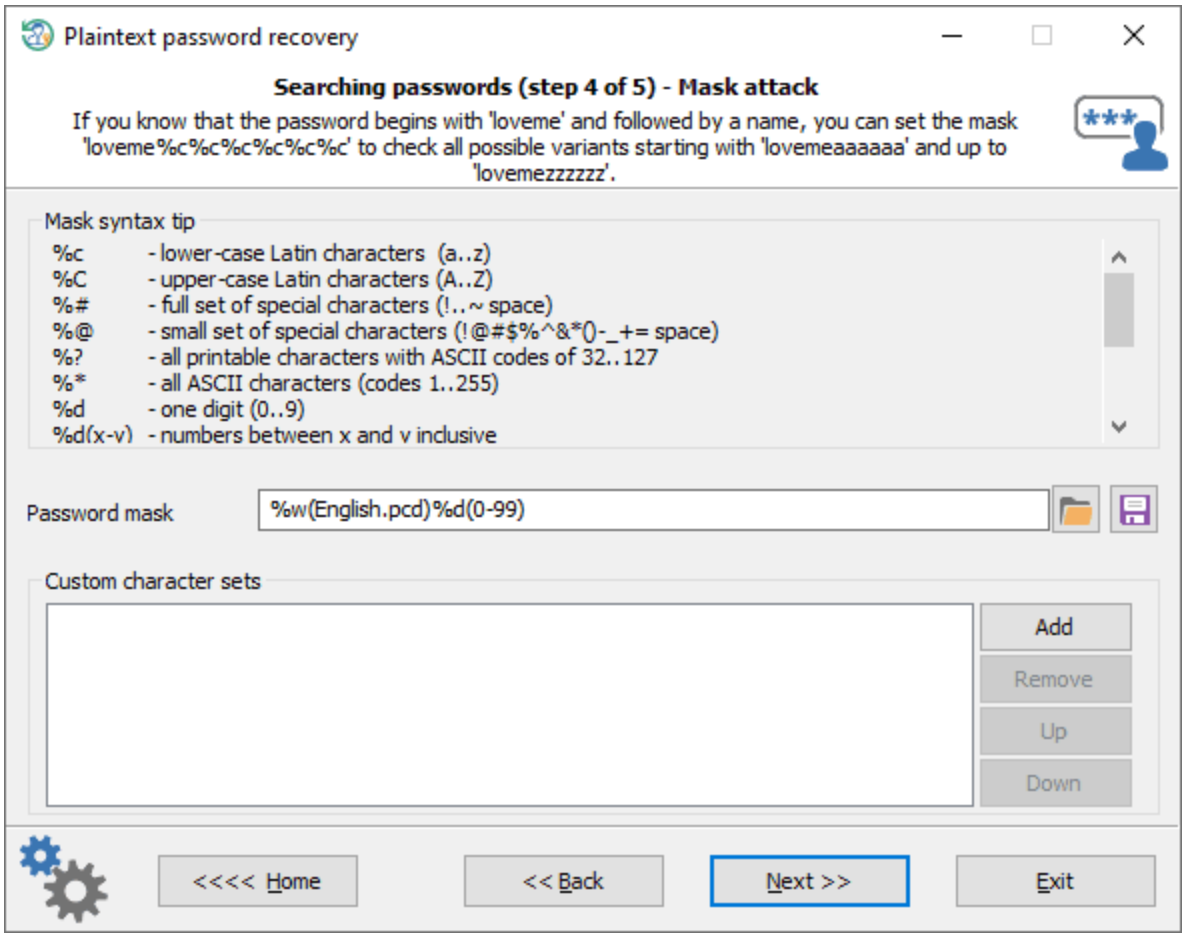
Un ataque de diccionario intenta contraseñas, que tienen más probabilidades de tener éxito, generalmente derivadas de una lista de palabras. RWP soporta diferentes tipos de diccionarios: ASCII, UNICODE, UTF8, así como diccionarios cifrados/comprimidos en formato PCD nativo. Puede utilizar diccionarios predefinidos y personalizados. Para agregar su propia lista de palabras, copie una en una unidad USB y conecte la unidad a la PC de destino. El nivel de mutación determina cuántas combinaciones (basadas en reglas de ingeniería social) se generarán para cada palabra de la(s) lista(s) de palabras.

Ataque híbrido



Un ataque híbrido es similar a uno de diccionario, excepto que puede establecer sus propias reglas de mutación de palabras. El programa viene con un gran conjunto de archivos de reglas. Simplemente use uno que sea mejor para su tarea. Lo bueno de un ataque híbrido es que además puedes crear, editar y modificar reglas de mutación de contraseña según tus necesidades.

Ataque de máscara

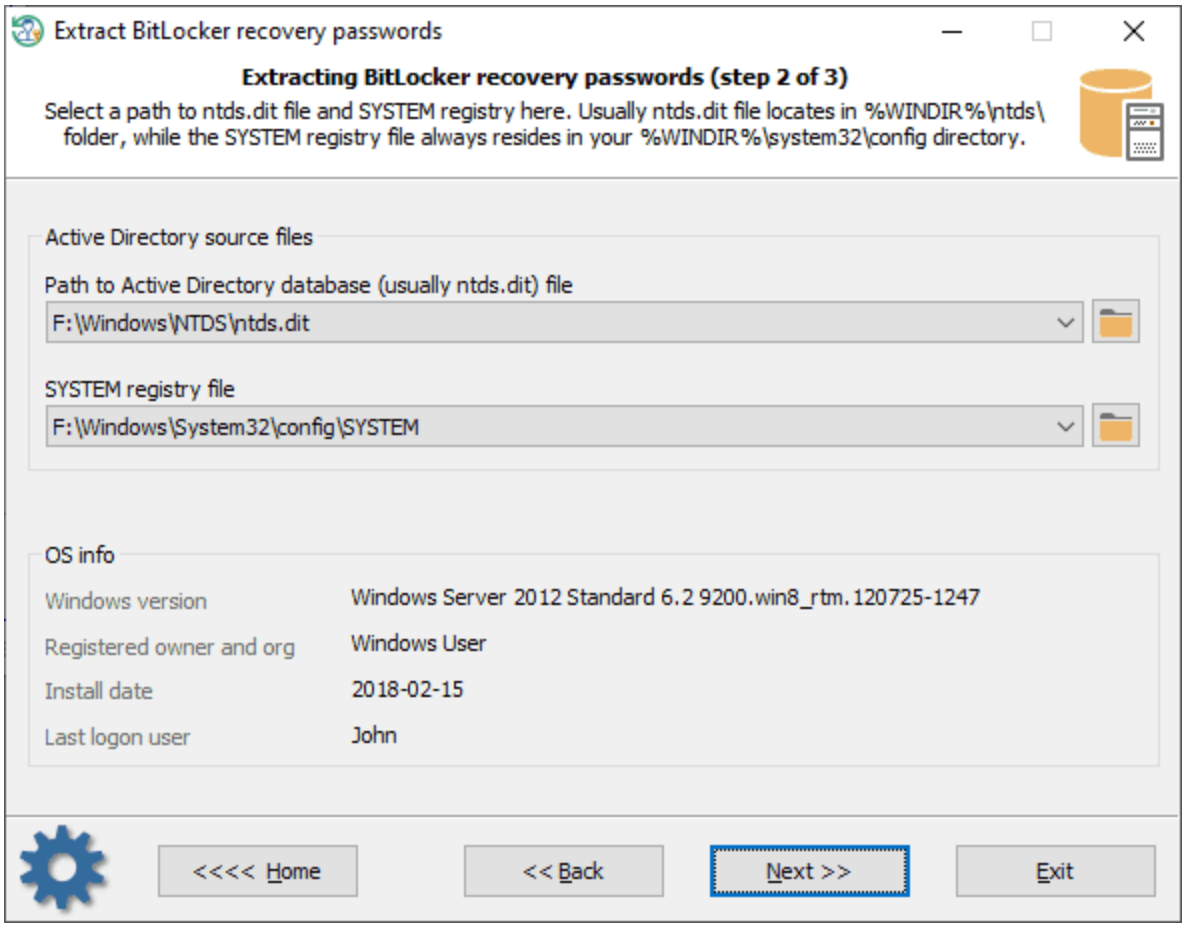


Un Ataque de máscara es una herramienta insustituible cuando conoce una parte de la contraseña o tiene algún detalle específico sobre ella. Por ejemplo, si sabes que la contraseña consta de 12 caracteres y comienza con 'loveme', obviamente basta con adivinar los últimos 6 caracteres de la contraseña. Para eso está el ataque de la máscara. En nuestro ejemplo, puede configurar la siguiente máscara: loveme%c%c%c%c%c%c%c%c
Para obtener más información sobre cómo funciona la máscara, consulte nuestra documentación en línea.

3.12 Extraer contraseñas de recuperación de BitLocker

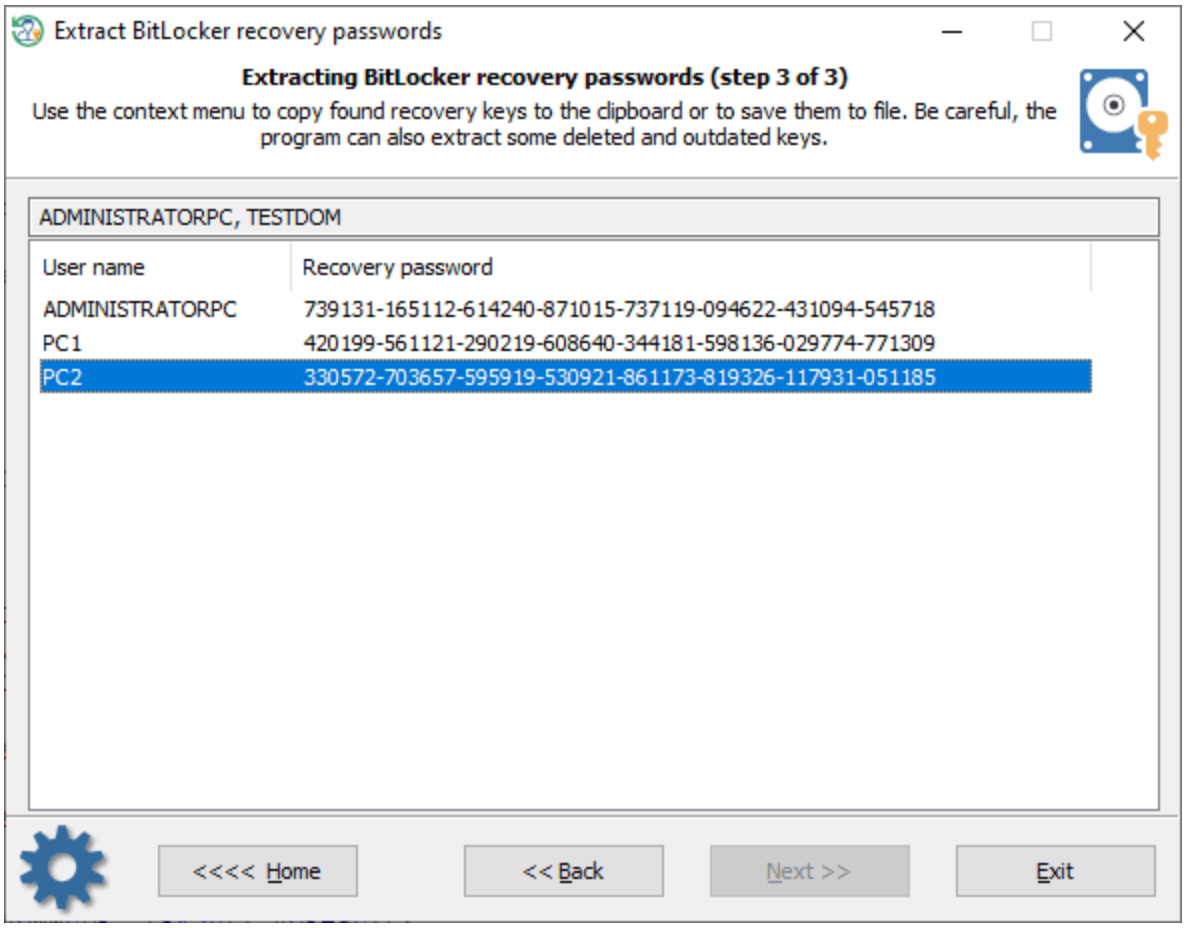
A menudo, se hace una copia de seguridad de las contraseñas de recuperación de BitLocker en una base de datos de Active Directory. Esta función del programa está diseñada para extraer contraseñas de BitLocker incluso de un dominio que no se puede arrancar o que no funciona.

Selección de la base de datos de Active Directory



Al principio, debe configurar rutas para el registro **SYSTEM** y para **NTDS**. Base de datos **DIT**. El programa debe localizar las rutas automáticamente, pero puede seleccionarlas por su cuenta.

Extracción de contraseñas de recuperación de BitLocker

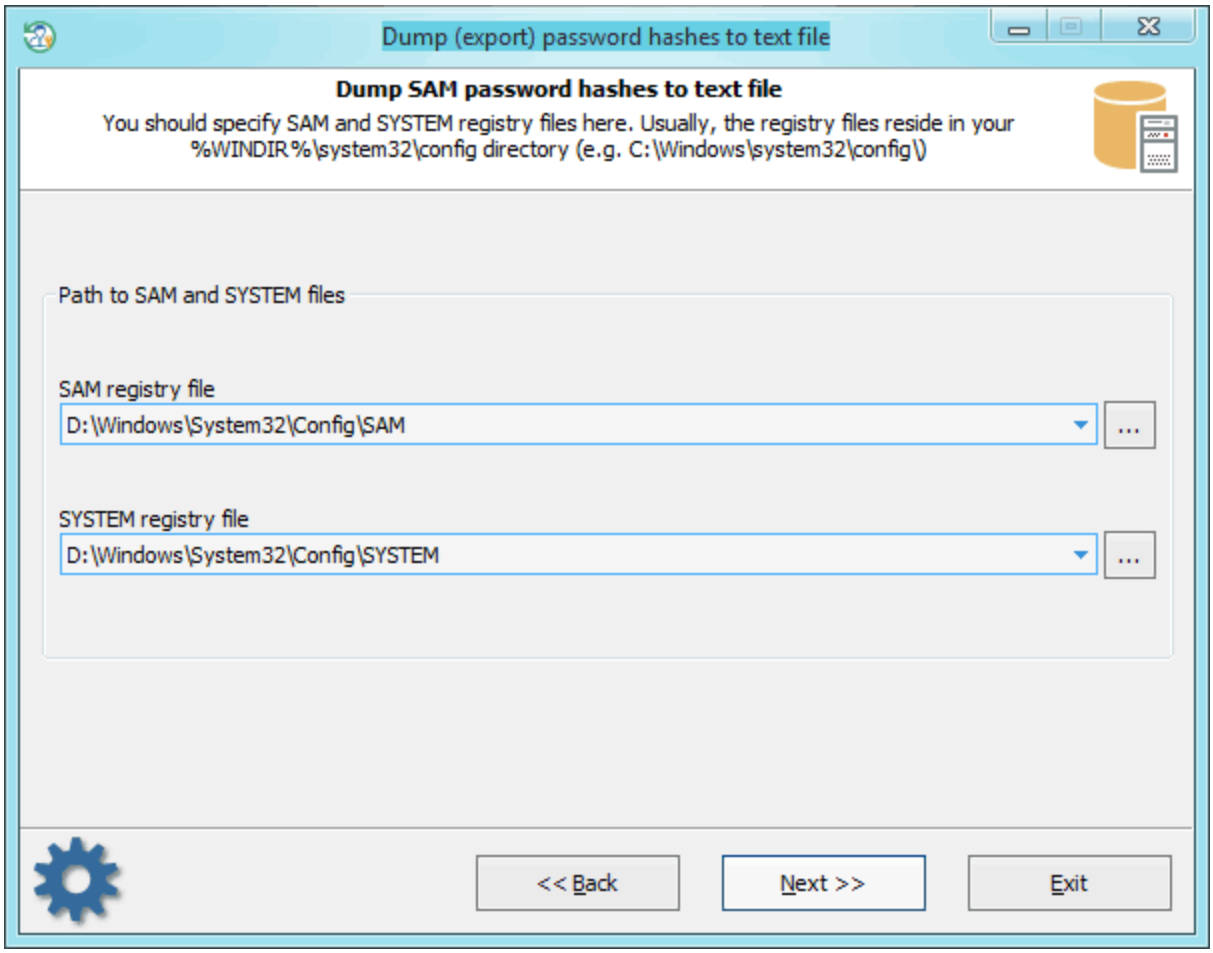


Tenga cuidado, el programa también puede recuperar claves de BitLocker caducadas y eliminadas, y a menudo no hay forma de obtener los nombres reales de los propietarios de las claves.

Puede copiar la clave requerida en el portapapeles o guardarla en un archivo.

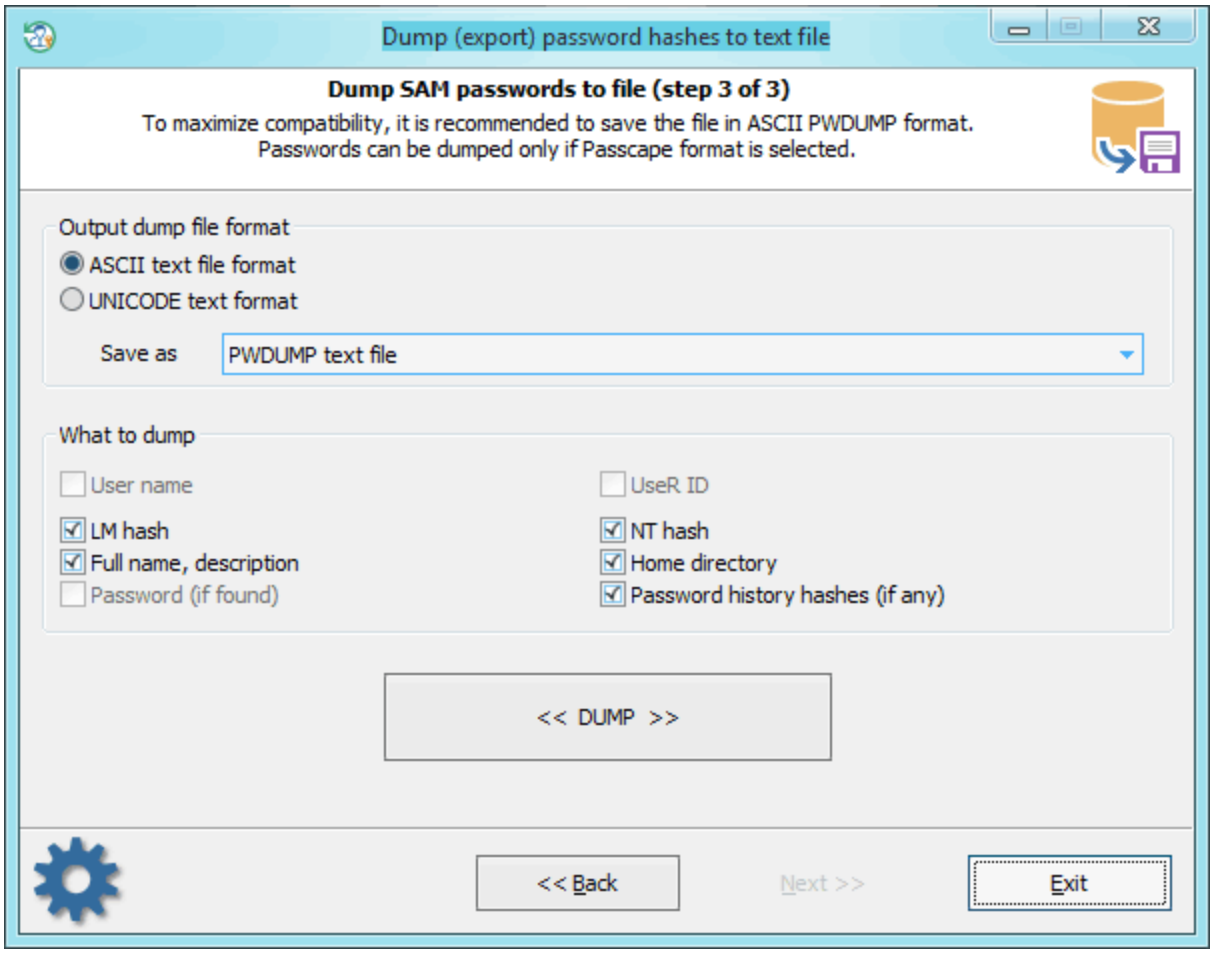
3.13 Volcar hashes de contraseña

Selección del origen de datos



En este paso, especifique la ubicación de los archivos SAM y SYSTEM. O, en el caso de los usuarios de dominio, – ntds.dit y SYSTEM.

Exportar hashes de contraseña



Seleccione el formato y el tipo del archivo de volcado. Al generar el volcado, también puede eliminar, si eso no tiene ningún valor para usted, los atributos innecesarios individuales de la cuenta. Si se selecciona el formato Passcape, también puede volcar contraseñas de texto sin formato (si se encontraron). La aplicación escanea su computadora en busca de la disponibilidad de los mismos y, si están disponibles, los asigna a las cuentas mientras los guarda en el archivo de volcado.

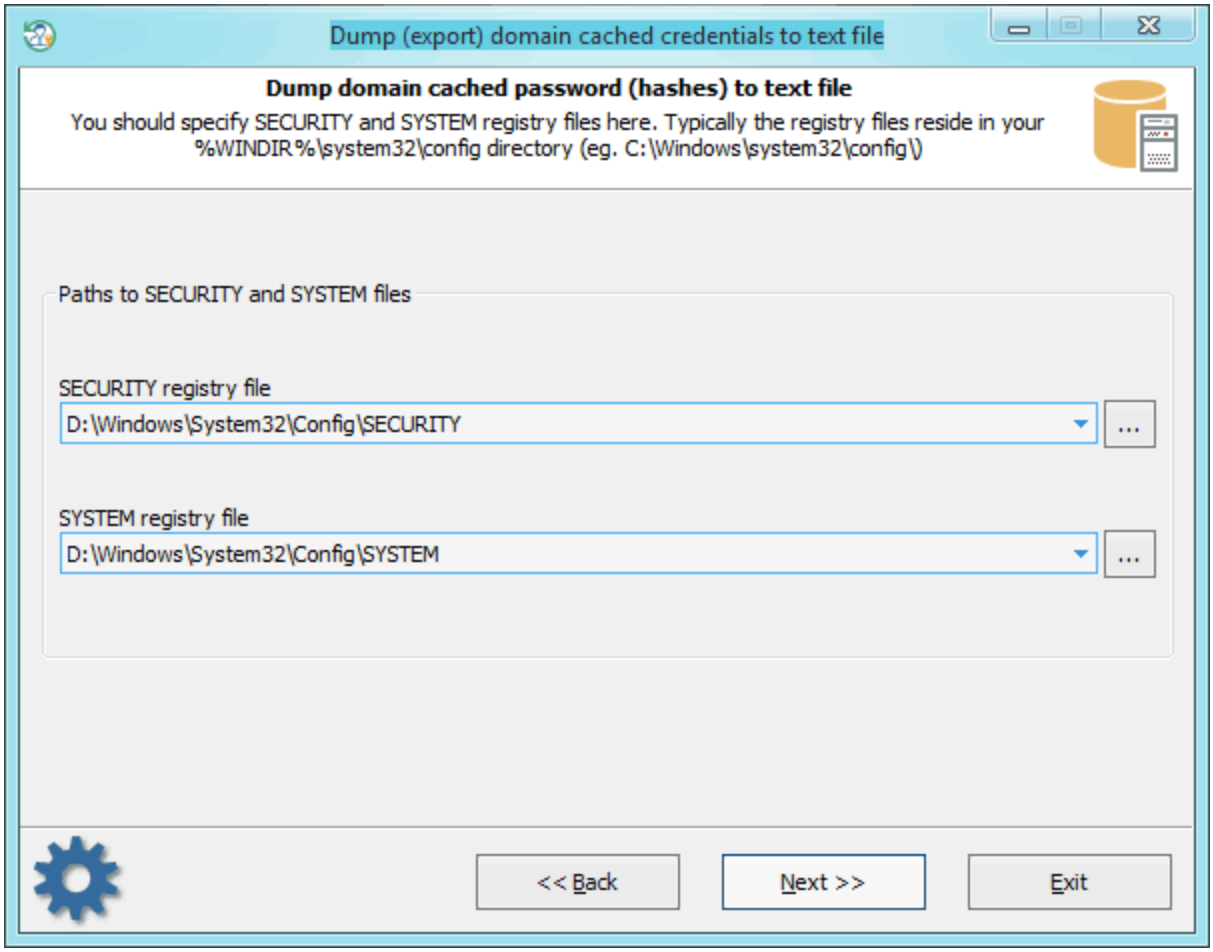
Las contraseñas de texto sin formato se almacenan en el dominio cuando la opción '*Almacenar contraseñas mediante cifrado reversible para todos los usuarios del dominio*' está configurado; Puede encontrarlo en la consola de directivas de grupos.

Más adelante, puede usar el archivo de volcado con diferentes aplicaciones de auditoría y recuperación de contraseñas.

Tenga en cuenta también que Restablecer contraseña de Windows, gracias a la tecnología de ataque de IA desarrollada por Passcape Software, puede descifrar contraseñas de ciertas cuentas literalmente al instante, sin buscar. Para obtener más información, consulte la sección Buscar contraseñas de usuario.

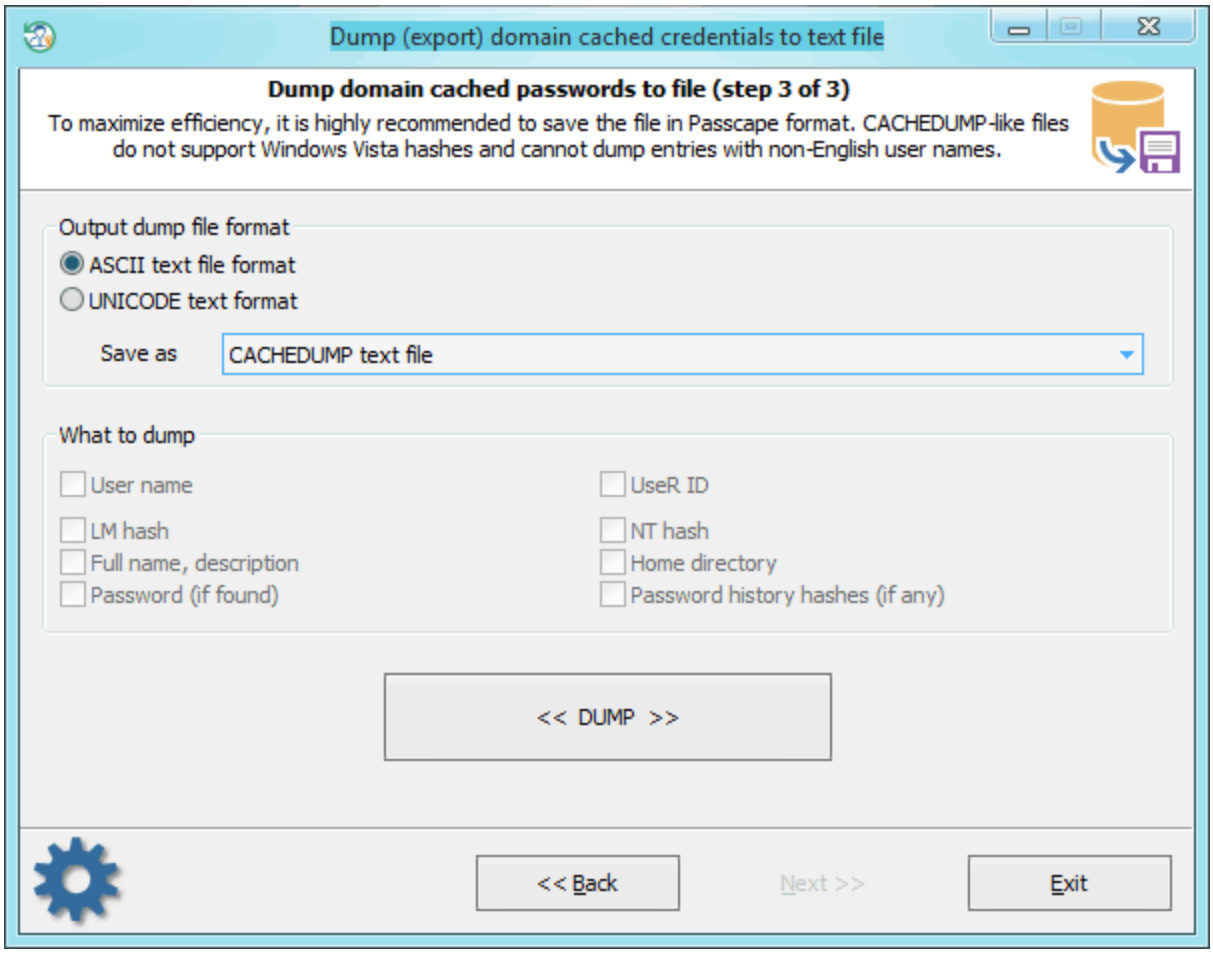
3.14 Volcar contraseñas almacenadas en caché de dominio

Selección del origen de datos



Para descifrar credenciales almacenadas en caché de dominio, el programa necesita 'conocer' la ubicación de dos archivos de registro del sistema: SECURITY y SYSTEM. Selecciónelos de la lista o, si la aplicación no pudo localizarlos, proporcione la ruta de acceso a ellos manualmente.

Volcado de credenciales almacenadas en caché de dominio



El cuadro de diálogo final proporciona solo dos opciones:

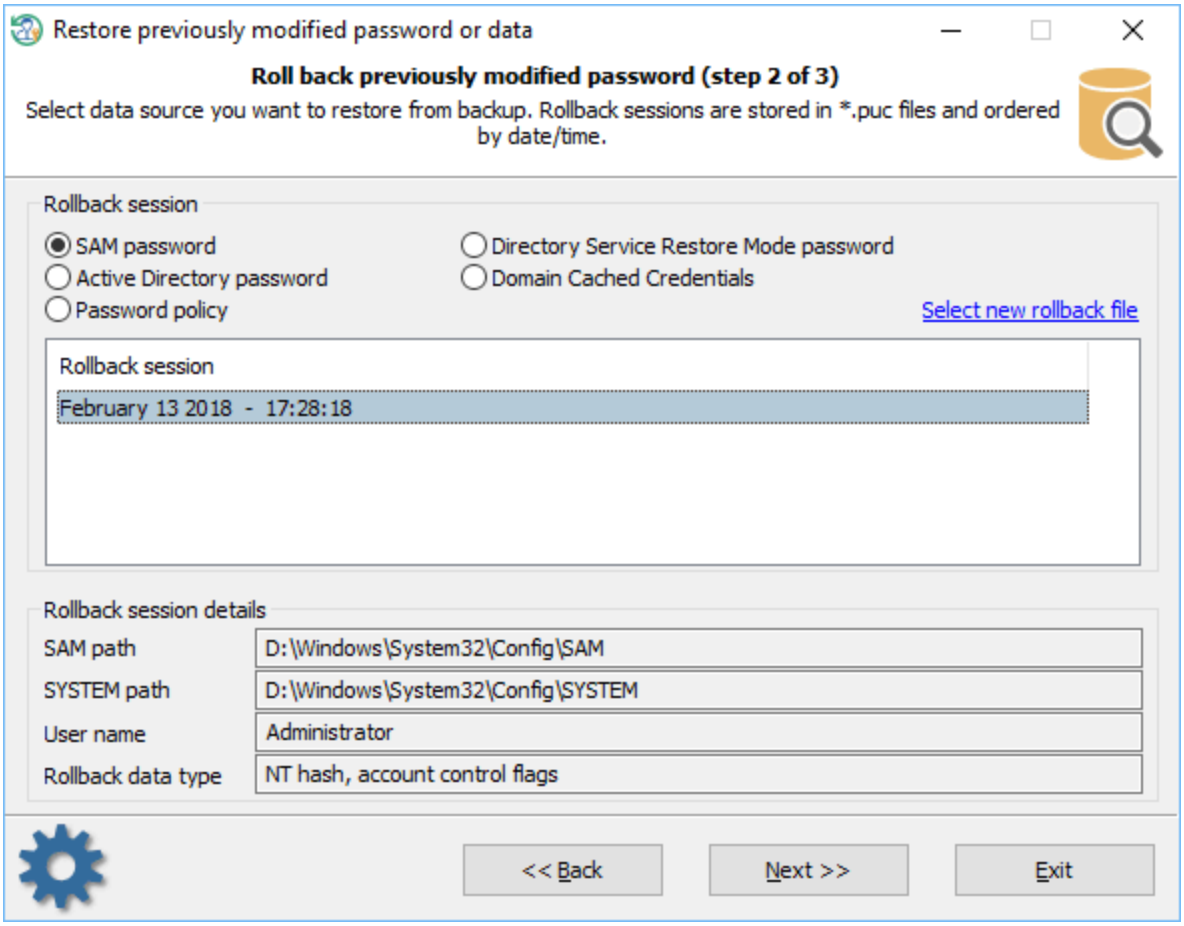
- **Formato de archivo de volcado**. ASCII es bueno para todos los casos, pero pueden ocurrir problemas con nombres de usuario no ingleses y, respectivamente, con un mayor análisis y descifrado de esos hashes. UNICODE es compatible con todos los idiomas, pero pueden producirse problemas de compatibilidad al leer este formato en diferentes aplicaciones.

- **El tipo de archivo de volcado** puede ser CACHEDUMP, un formato simple pero generalizado. No se producirán problemas de compatibilidad. Sin embargo, este formato impone una serie de restricciones. En primer lugar, no admite nombres de usuario que no se den en inglés. Respectivamente, más adelante, no podrá descifrar la contraseña de la cuenta, ya que está vinculada al nombre. En segundo lugar, la versión actual del formato CACHEDUMP no es compatible con los sistemas operativos Windows Vista y superiores.

Formato Passcape - libre de estas desventajas y se puede utilizar con éxito en aplicaciones de auditoría y recuperación de contraseñas como, por ejemplo, Network Password Recovery.

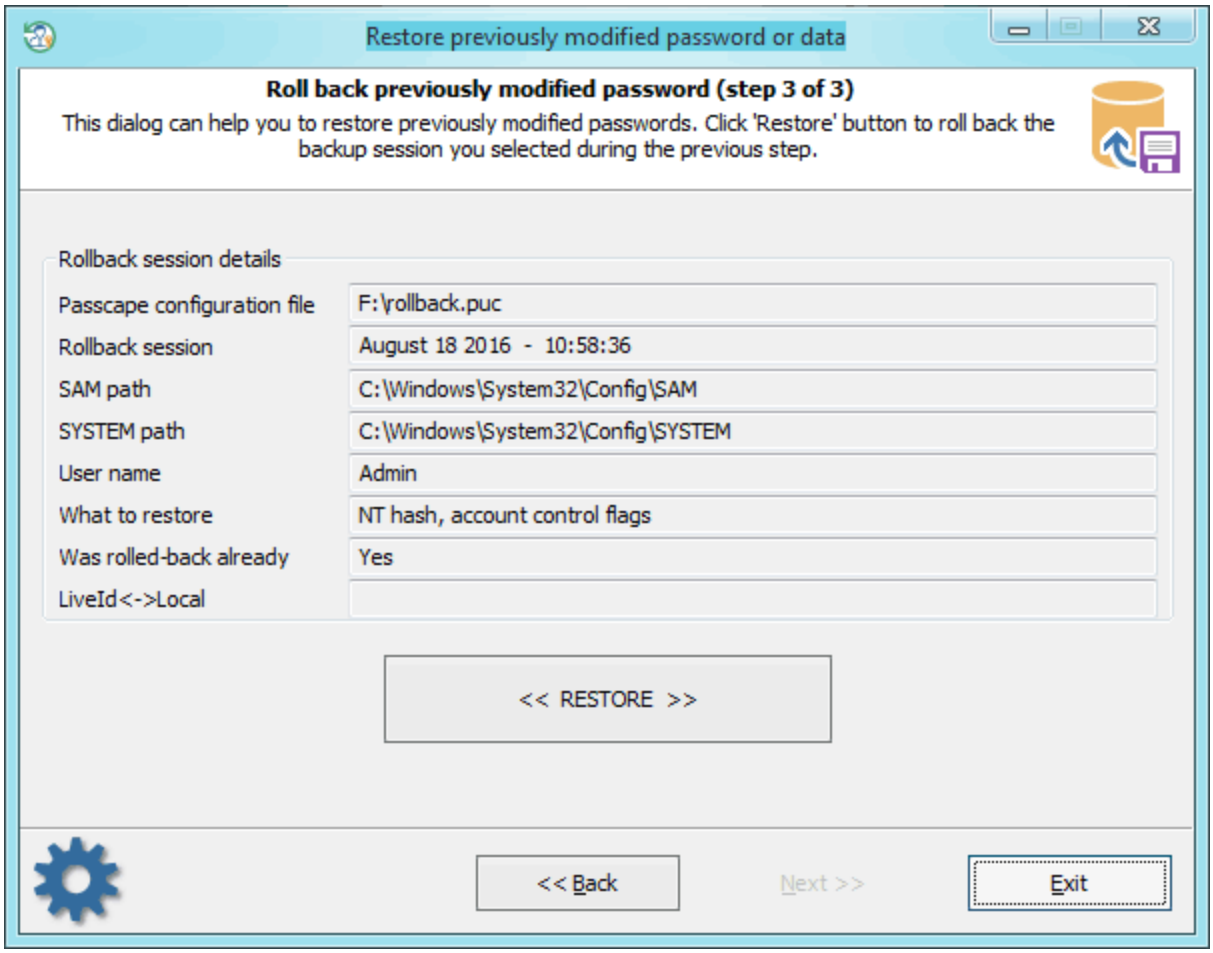
3.15 Restaurar la contraseña modificada anteriormente

Elegir un archivo de reversión



Si por alguna razón necesita deshacer (es decir, restaurar) la contraseña que se restableció o modificó anteriormente, en el segundo paso del Asistente, proporcione a la aplicación el archivo *.puc con las sesiones de reversión (deshacer). Active el tipo de contraseña que se restaurará: contraseña de cuenta SAM normal, Active Directory, contraseña DSRM o credenciales de caché de dominio, marcas de directiva de contraseña. Después de eso, seleccione la fecha en que se realizó el cambio.

Restauración de contraseña modificada previamente



En el último paso, la aplicación le ofrecerá revisar los detalles de la sesión de deshacer; por favor, preste mucha atención a los últimos tres elementos:

- Cuenta a gestionar.
- Datos a restaurar. Esos son los datos que ha modificado en algún momento.
- Si esta sesión de deshacer ya se ha utilizado o no

Repasemos esta situación para un ejemplo:

Un experto en seguridad informática debe iniciar sesión en Windows con una cuenta determinada. La contraseña de esa cuenta es desconocida. Al mismo tiempo, la contraseña de la cuenta debe permanecer sin modificar.

Aquí está la rutina:

- Ejecute Reset Windows Password, seleccione la cuenta correspondiente y restablezca su contraseña. Al mismo tiempo, guarde la sesión de deshacer en un archivo *.puc (la aplicación le pedirá que lo haga cuando modifique la contraseña).
- Cierre Reset Windows Password e inicie Windows. Inicie sesión en la cuenta modificada con la contraseña en blanco. Haga lo que necesite bajo esa cuenta.
- Ahora necesita restaurar la contraseña de la cuenta anterior. Para ese propósito, reinicie una vez más e inicie Restablecer contraseña de Windows. En el menú principal, seleccione '*Restaurar contraseña o datos previamente modificados*', introduzca la ruta de acceso al archivo de deshacer donde ha

guardado los cambios que ha realizado. Pase al tercer paso y asegúrese de que esta sea la cuenta que necesita. Haga clic en el botón <<Restaurar>> y se restaurará la contraseña anterior.

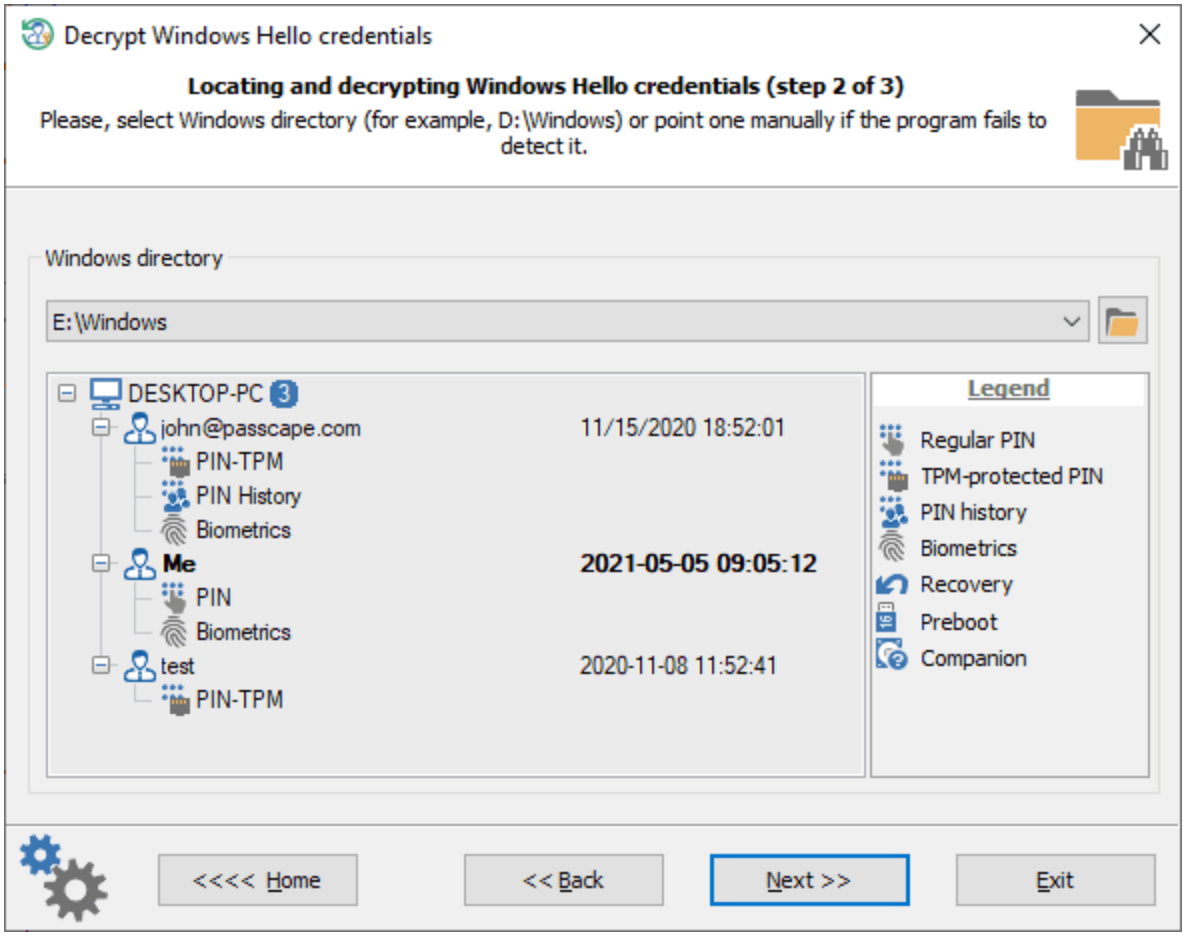
3.16 HERRAMIENTAS DE RECUPERACIÓN DE CONTRASEÑAS

Enter topic text here.

3.16.1 Descifrar credenciales de Windows Hello

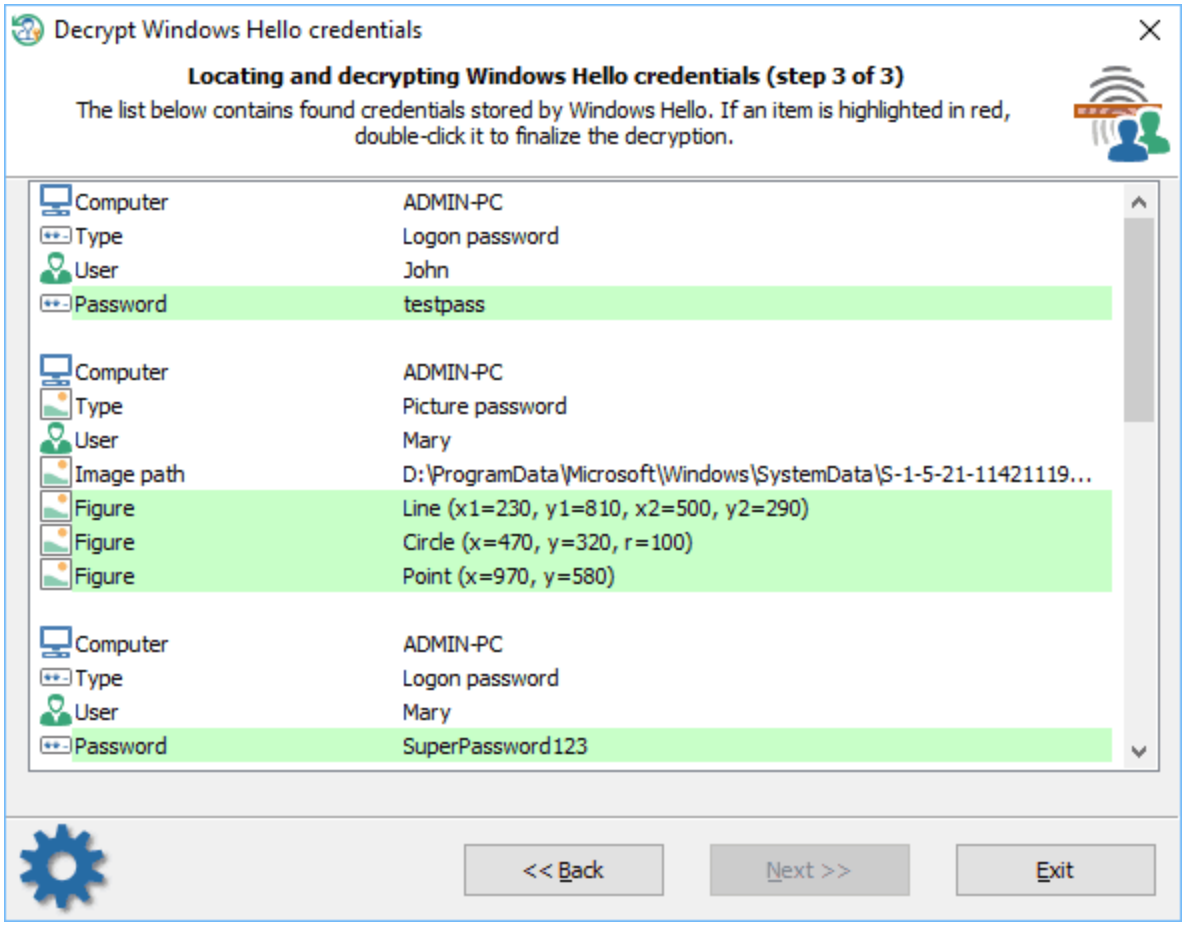
Windows Hello es un sistema de seguridad biométrica que permite a los usuarios de Windows iniciar sesión en el sistema operativo, las aplicaciones y sus dispositivos sin contraseñas, pero utilizando una huella digital, escaneo de iris, reconocimiento facial o de voz. Windows Hello almacena diferentes tipos de información personal de los usuarios: identidades digitales, PIN, contraseñas de inicio de sesión de texto sin formato, etc.

Selección del directorio de Windows



Reset Windows Password recupera todo tipo de datos personales guardados en Windows Hello. En primer lugar, deberá especificar el directorio de Windows del sistema Windows 10 de destino.

Descifrar contraseñas



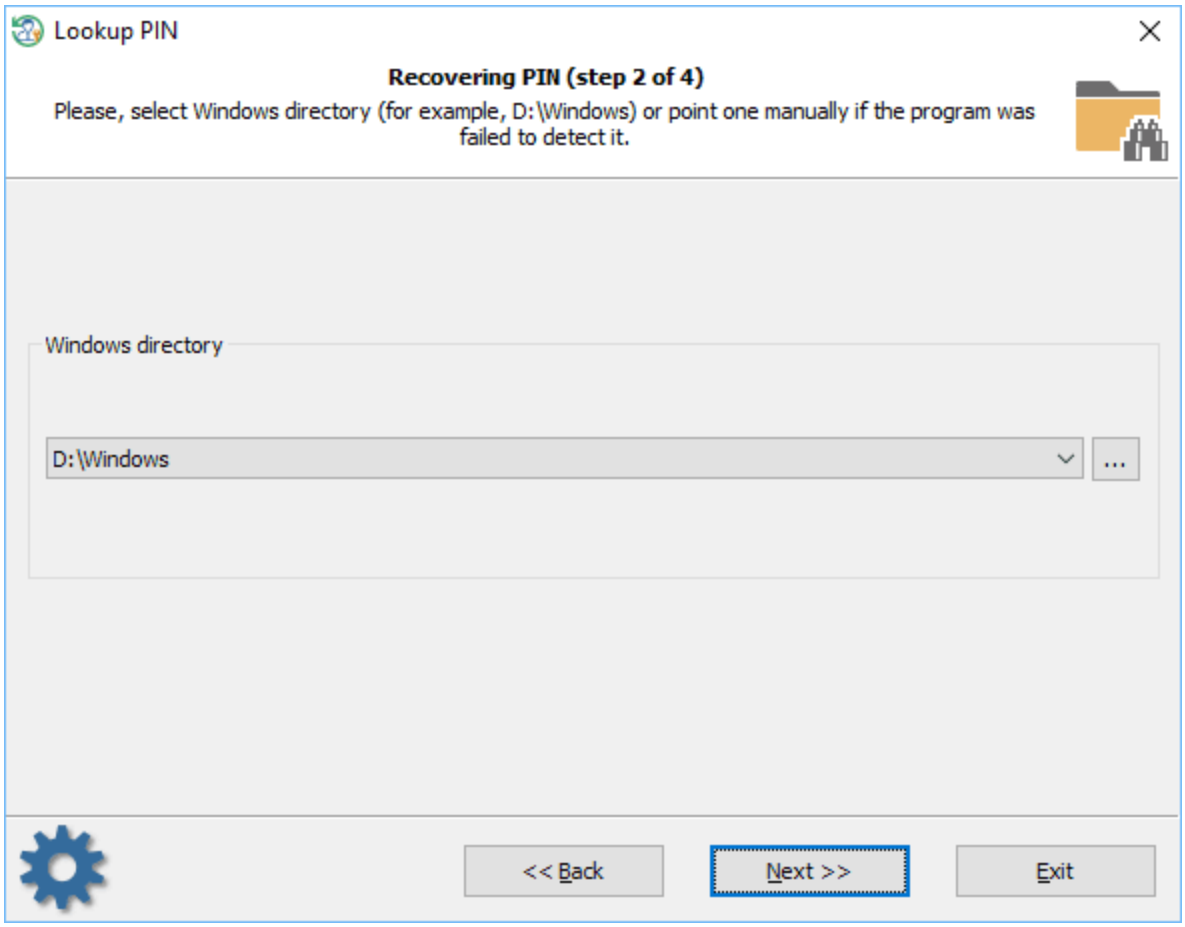
Luego, el programa debe escanear el directorio de Windows de destino en busca de datos personales y enviar la información encontrada a la pantalla. Reset Windows Password descifra automáticamente las contraseñas de inicio de sesión si las cuentas de usuario se configuraron para iniciar sesión mediante biometría, por ejemplo, huella digital o reconocimiento facial.

Algunos elementos de la tabla pueden estar marcados en rojo. Significa que para finalizar el descifrado, el programa necesita conocer el código PIN de la cuenta de usuario. Haga doble clic en el elemento y escriba el PIN que corresponde a la cuenta de usuario.

3.16.2 Búsqueda de PIN

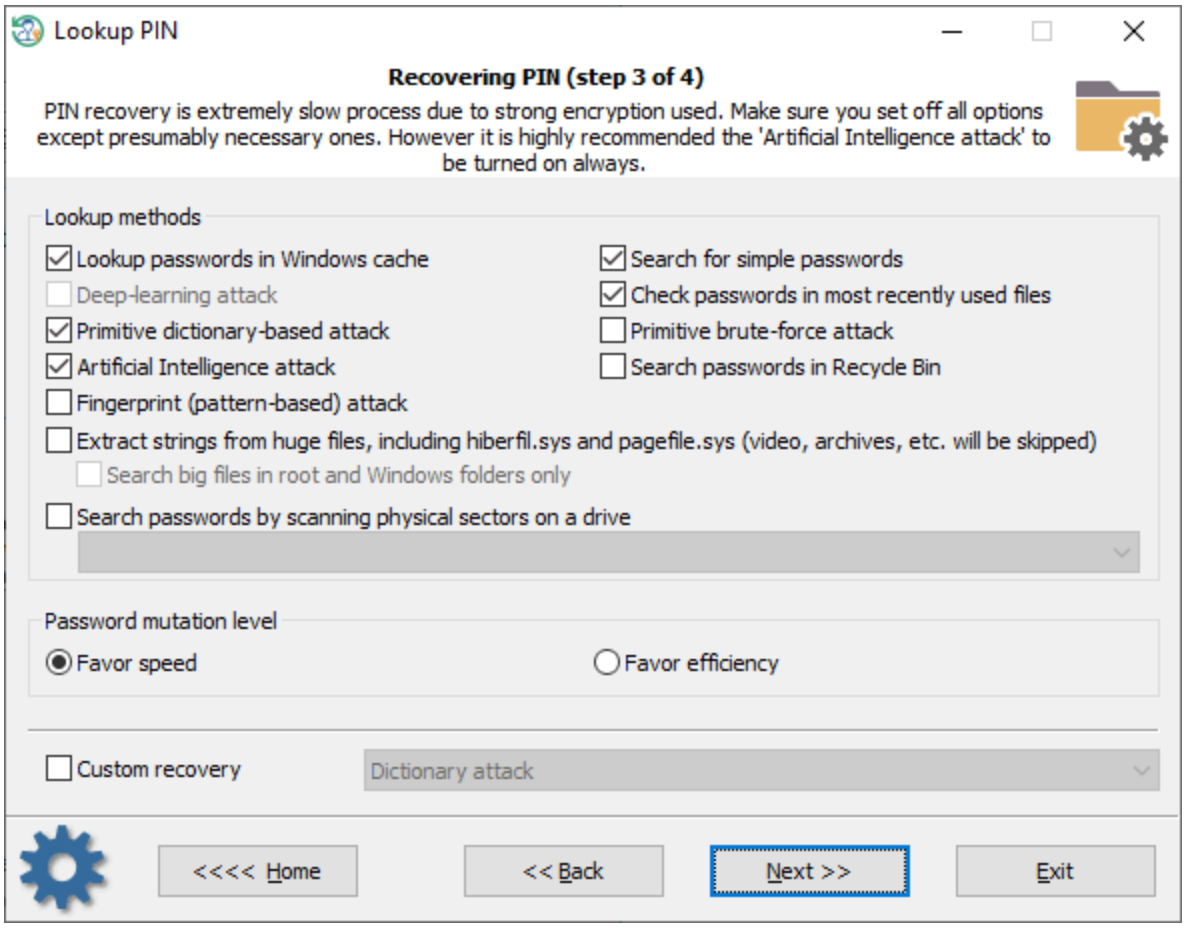
Cuando configuras Windows Hello primero, se te pide que crees un PIN. El PIN se utiliza como alternativa al inicio de sesión biométrico, cuando el sensor biométrico no está disponible o no funciona correctamente. A diferencia de Windows 8, Windows 10 garantiza un cifrado muy fuerte (utilizando incluso características y API no documentadas) para proteger los PIN. Por lo tanto, el problema de la recuperación del PIN olvidado es extremadamente vital y se enfrenta a todos los usuarios.

Selección del directorio de Windows



En primer lugar, debe seleccionar el directorio de Windows o buscarlo manualmente.

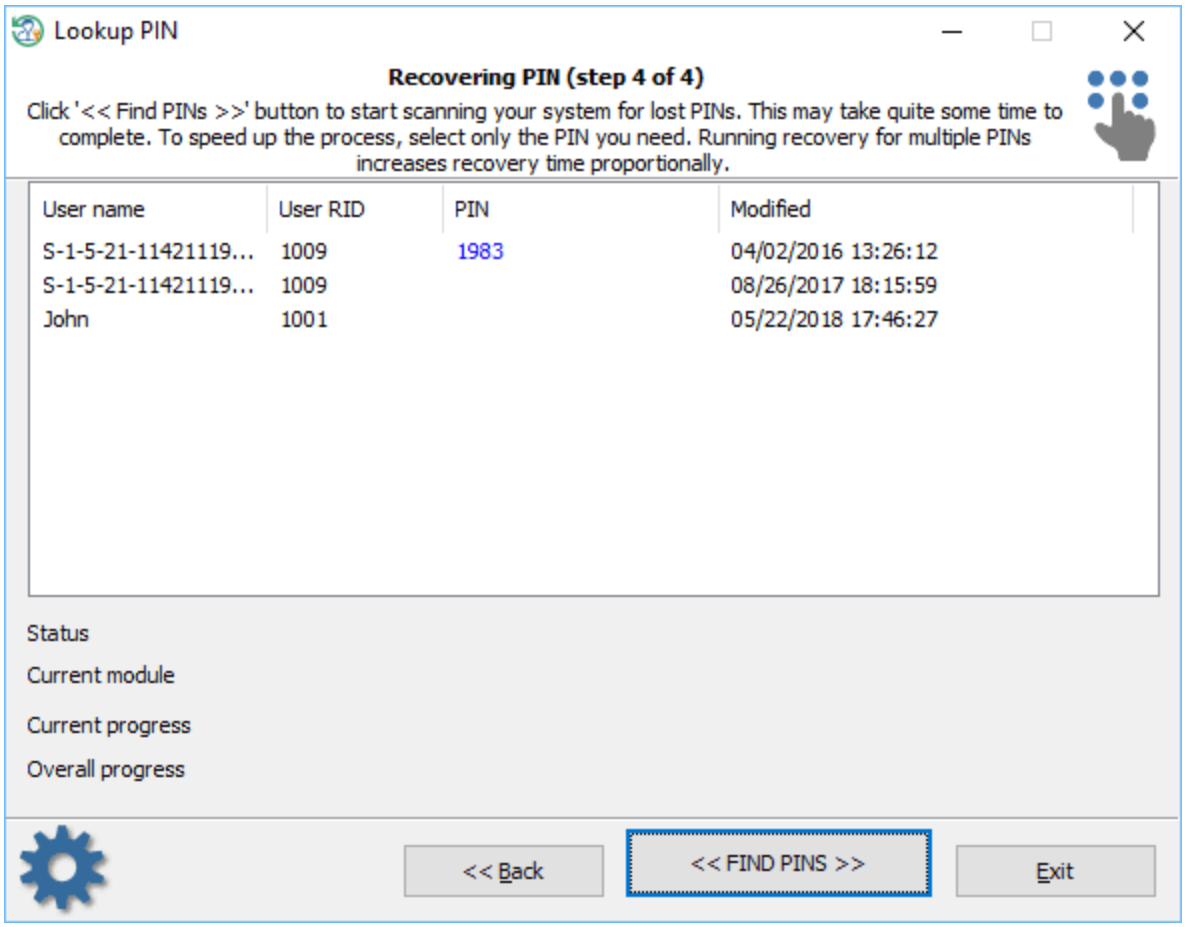
Configuración de las opciones de búsqueda y recuperación



En el siguiente paso, el programa ofrece métodos de recuperación disponibles utilizados para buscar PIN. El código del programa está altamente optimizado para la velocidad. Pero a pesar de esto, el proceso de búsqueda de un PIN es extremadamente lento. Por esta razón, es muy recomendable desactivar la mayoría de los ataques costosos en tiempo, por ejemplo, como en la imagen de arriba.

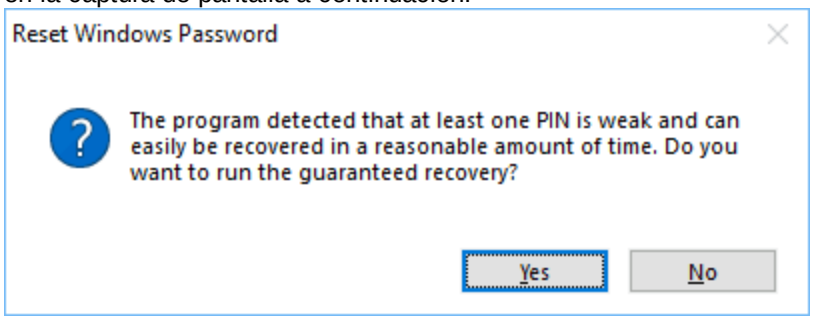
Para aplicar un método de recuperación personalizado, active la opción 'Recuperación personalizada' y seleccione uno de los ataques disponibles. En el siguiente paso, se le pedirá que configure varias opciones relacionadas con el ataque seleccionado.

Búsqueda de PIN



La velocidad de búsqueda es inversamente proporcional al número de pines buscados. Es decir, cuantos más códigos PIN se busquen simultáneamente, menor será la velocidad de búsqueda. Por lo tanto, se recomienda excluir todos los PIN innecesarios de la búsqueda y dejar solo uno necesario. Puede hacerlo simplemente haciendo clic derecho en el PIN que necesita recuperar y seleccionando *'Excluir todos excepto los seleccionados*'. Para iniciar el proceso, presione el botón << BUSCAR PINS >>.

Sepa que se puede garantizar que algunos PIN se descifraran en un período de tiempo razonable. Si el programa puede detectar un PIN tan vulnerable, ofrece iniciar la recuperación garantizada, al igual que en la captura de pantalla a continuación.

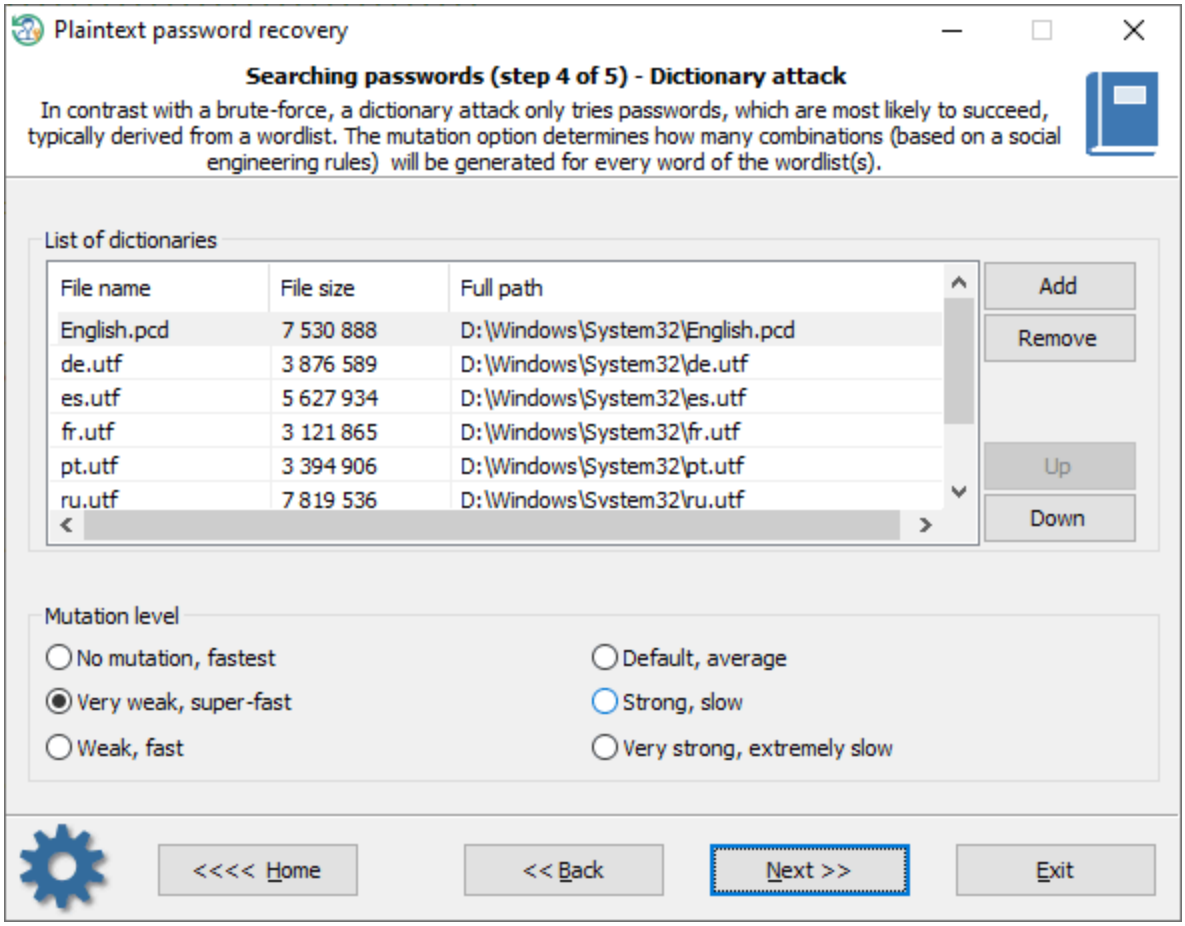


3.16.2.1 Recuperación personalizada

Una vez que se establece la opción de recuperación personalizada, el programa también puede ejecutar 3 ataques diferentes para adivinar las contraseñas:

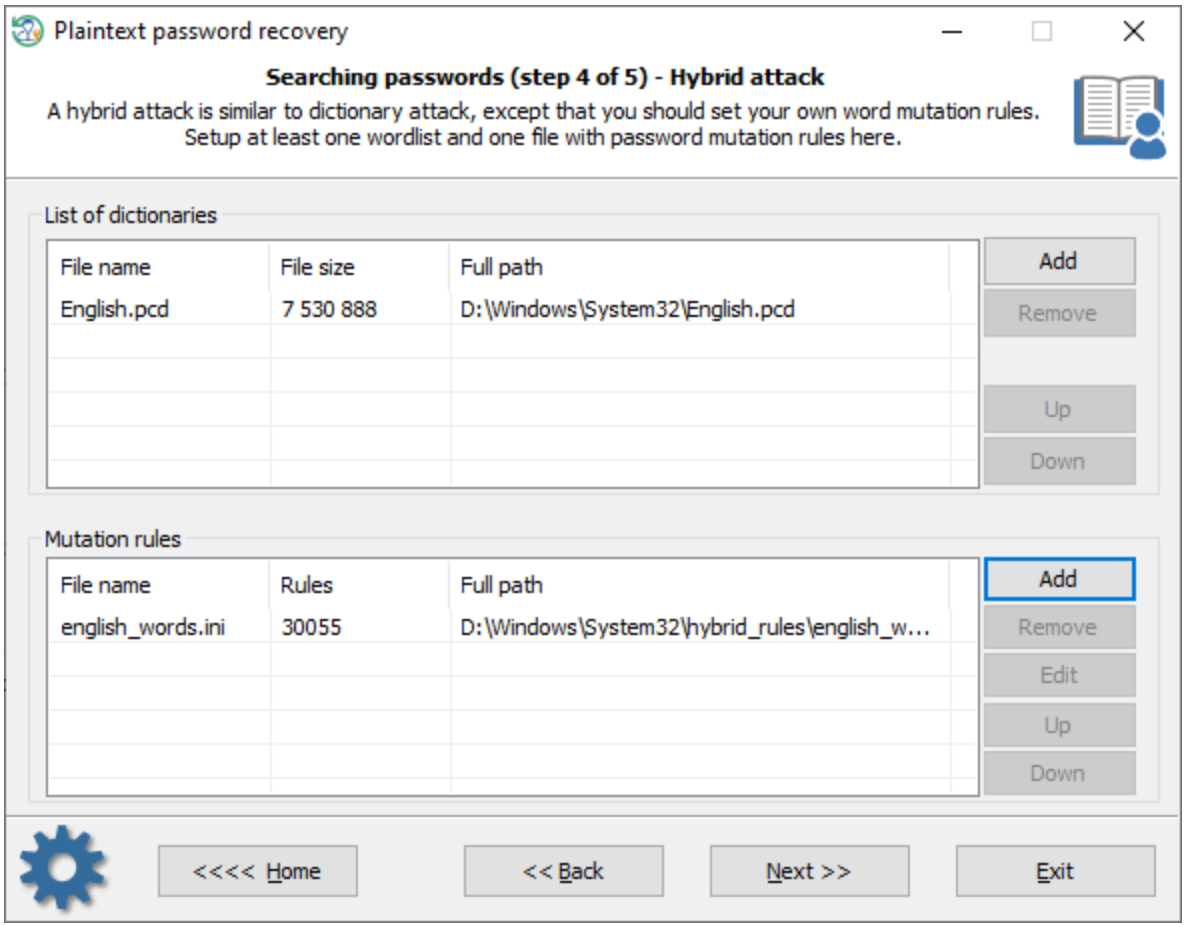
- Ataque de diccionario
- Ataque híbrido
- Ataque de máscara

Ataque de diccionario



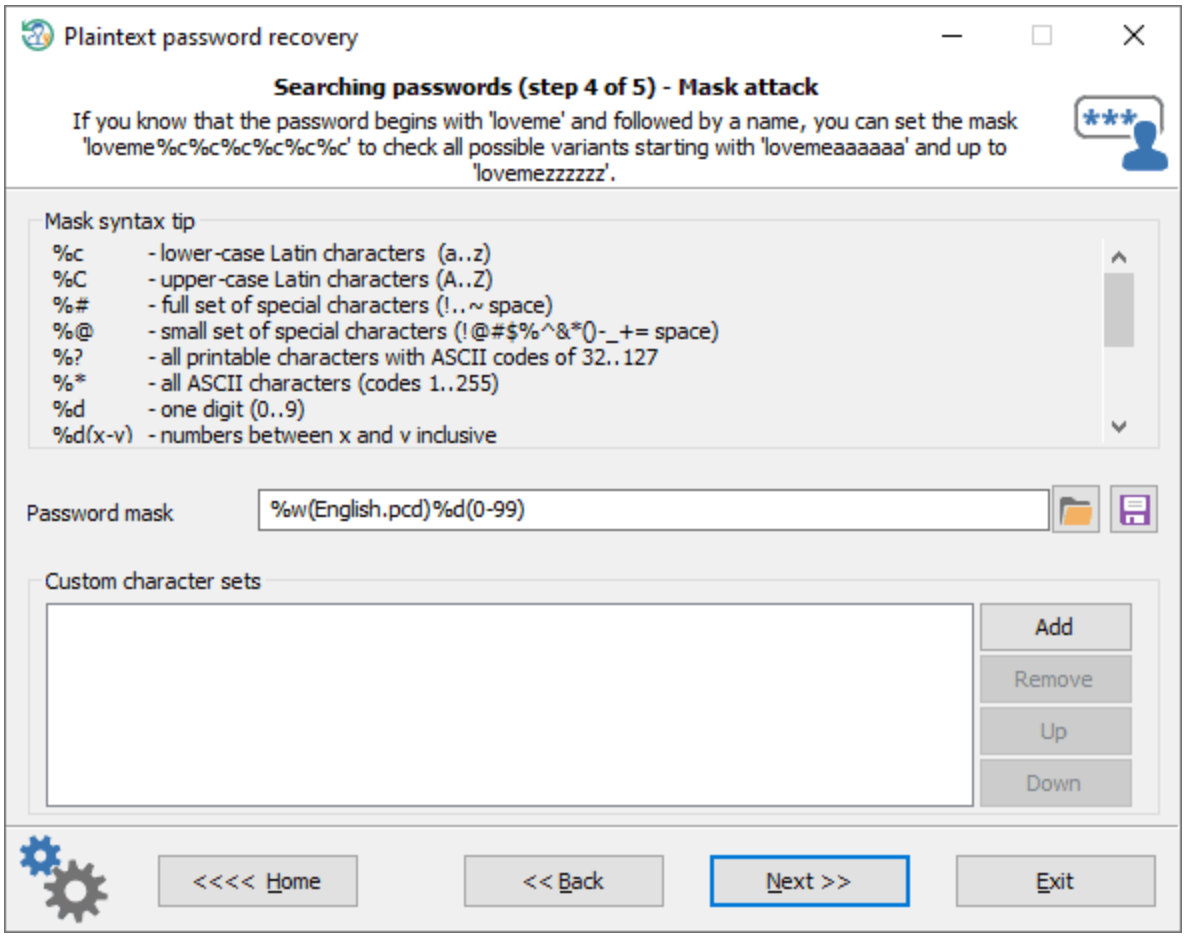
Un ataque de diccionario intenta contraseñas, que tienen más probabilidades de tener éxito, generalmente derivadas de una lista de palabras. RWP soporta diferentes tipos de diccionarios: ASCII, UNICODE, UTF8, así como diccionarios cifrados/comprimidos en formato PCD nativo. Puede utilizar diccionarios predefinidos y personalizados. Para agregar su propia lista de palabras, copie una en una unidad USB y conecte la unidad a la PC de destino. El nivel de mutación determina cuántas combinaciones (basadas en reglas de ingeniería social) se generarán para cada palabra de la(s) lista(s) de palabras.

Ataque híbrido



Un ataque híbrido es similar a uno de diccionario, excepto que puede establecer sus propias reglas de mutación de palabras. El programa viene con un gran conjunto de archivos de reglas. Simplemente use uno que sea mejor para su tarea. Lo bueno de un ataque híbrido es que además puedes crear, editar y modificar reglas de mutación de contraseña según tus necesidades.

Ataque de máscara



Un Ataque de máscara es una herramienta insustituible cuando conoce una parte de la contraseña o tiene algún detalle específico sobre ella. Por ejemplo, si sabes que la contraseña consta de 12 caracteres y comienza con 'loveme', obviamente basta con adivinar los últimos 6 caracteres de la contraseña. Para eso está el ataque de la máscara. En nuestro ejemplo, puede configurar la siguiente máscara: loveme%c%c%c%c%c%c%c%c
Para obtener más información sobre cómo funciona la máscara, consulte nuestra documentación en línea.

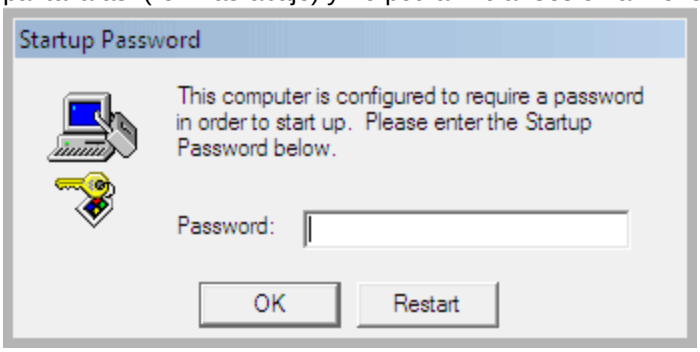
3.16.3 Buscar contraseña de inicio de SYSKEY

Syskey es la capa adicional de seguridad, se introdujo por primera vez en Windows 2000. Se utiliza por defecto y ofrece 3 tipos de protección:

1. **Predeterminado**: cuando la clave de cifrado syskey se almacena en el registro de Windows.
2. **Disco de inicio**: la clave de cifrado syskey se almacena en un disquete.
3. **Contraseña de inicio**: la clave de cifrado syskey se genera a partir de una frase de contraseña de usuario..

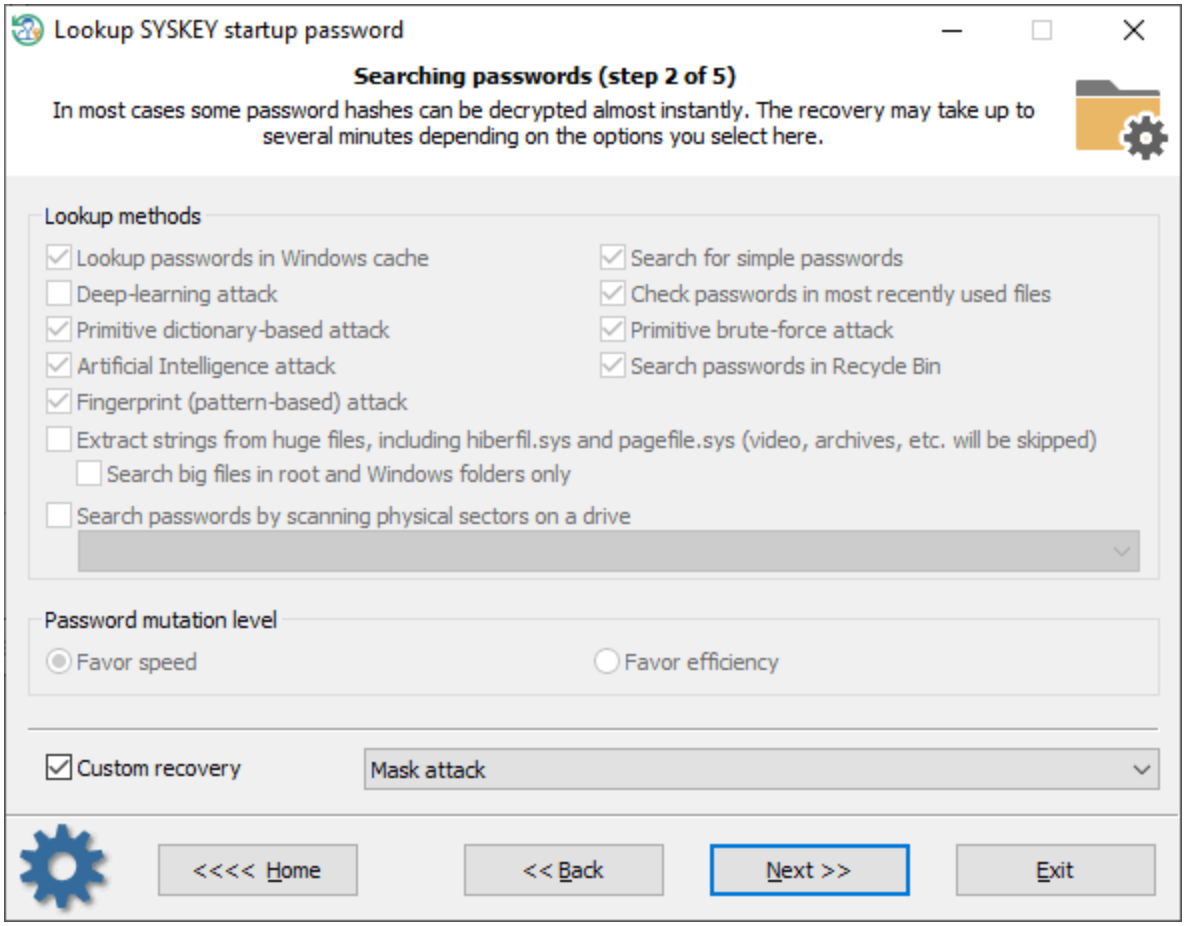
Los estafadores aprovechan el poder de SYSKEY y, a menudo, establecen una contraseña de inicio de syskey en la PC de una víctima. Por lo general, se ponen en contacto con usted con un fuerte acento indio identificándose como miembros del soporte de Microsoft y le dicen que su PC debe repararse de inmediato porque tiene un problema crítico. Intentarán convencerlo de que les permita conectar su

sistema de forma remota y solucionar los problemas. Si comete el error, establecerán una contraseña de inicio syskey. Como no conoce la contraseña, después de volver a cargar el sistema, obtendrá la pantalla así (ver más abajo) y no podrá iniciar sesión a menos que pague por la corrección.



Afortunadamente, en la mayoría de los casos, las contraseñas que utilizan son bastante triviales y se pueden descifrar utilizando nuestra función de búsqueda de contraseñas SYSKEY. Tendrás que pasar por los 3 sencillos pasos para comenzar a buscar la contraseña.

Configuración de los métodos de recuperación de SYSKEY

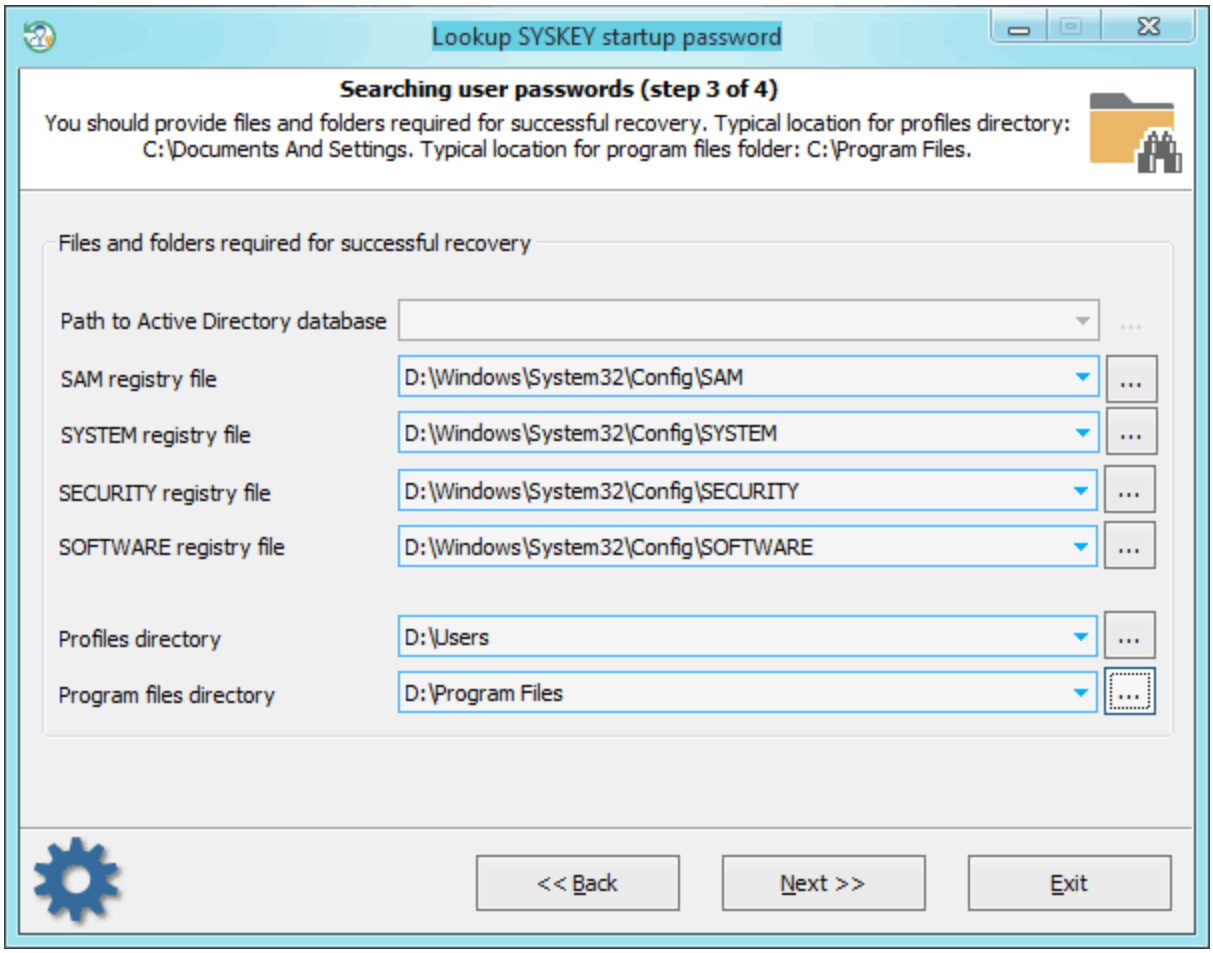


La búsqueda de contraseñas SYSKEY puede llevar bastante tiempo y consta de los siguientes pasos:

1. Búsqueda de información en la memoria caché del sistema de Windows. Este método consiste en más de una docena de mini subataques, durante los cuales el programa analiza todo tipo de contraseñas de usuario: secretos LSA, DSL, VPN, WiFI, FTP, IM, contraseñas del navegador, etc.
2. Análisis de contraseñas simples y cortas, combinaciones de teclado, etc.
3. Escanee, analice y analice los archivos utilizados más recientemente del sistema de destino.
4. Ataque de diccionario primitivo. La aplicación comprueba todas las contraseñas del diccionario incorporado para las ediciones Light y Standard o de varios diccionarios (árabe, chino, inglés, francés, alemán, portugués, ruso, español) para la edición avanzada. Si la opción de búsqueda profunda está activada, las mutaciones de palabras simples también se tendrán en cuenta durante la búsqueda.
5. La recuperación primitiva de fuerza bruta intentará revelar contraseñas cortas. Las opciones de fuerza bruta también dependen del nivel de mutación.
6. El ataque de Inteligencia Artificial analiza la actividad de red de un usuario en la computadora. Sobre los resultados del análisis, la aplicación genera preferencias de usuario y genera un diccionario semántico para el ataque, que luego utiliza para encontrar y adivinar la contraseña.
7. Busque contraseñas en archivos eliminados.
8. Búsqueda de contraseñas complicadas en inglés (ataque de huellas dactilares).
9. Extraiga cadenas y palabras de archivos enormes: imágenes RAM, hiberfil.sys, archivo de página.sys así sucesivamente. Cuando se establece esta opción, el programa intentará omitir archivos inútiles en el análisis de contraseñas como video, archivos, archivos de audio, etc.
10. Busque contraseñas leyendo y analizando sectores sin procesar de la unidad seleccionada. Si el *'Nivel de mutación de contraseña"* se establece en '*Búsqueda profunda*', el programa también intenta generar diferentes combinaciones y 'mutar' las contraseñas encontradas, por lo que caminar por todos los sectores de la unidad de destino puede llevar bastante tiempo. Tenga en cuenta que el algoritmo de escaneo basado en sectores no es efectivo contra las unidades que tienen un cifrado de disco completo establecido.

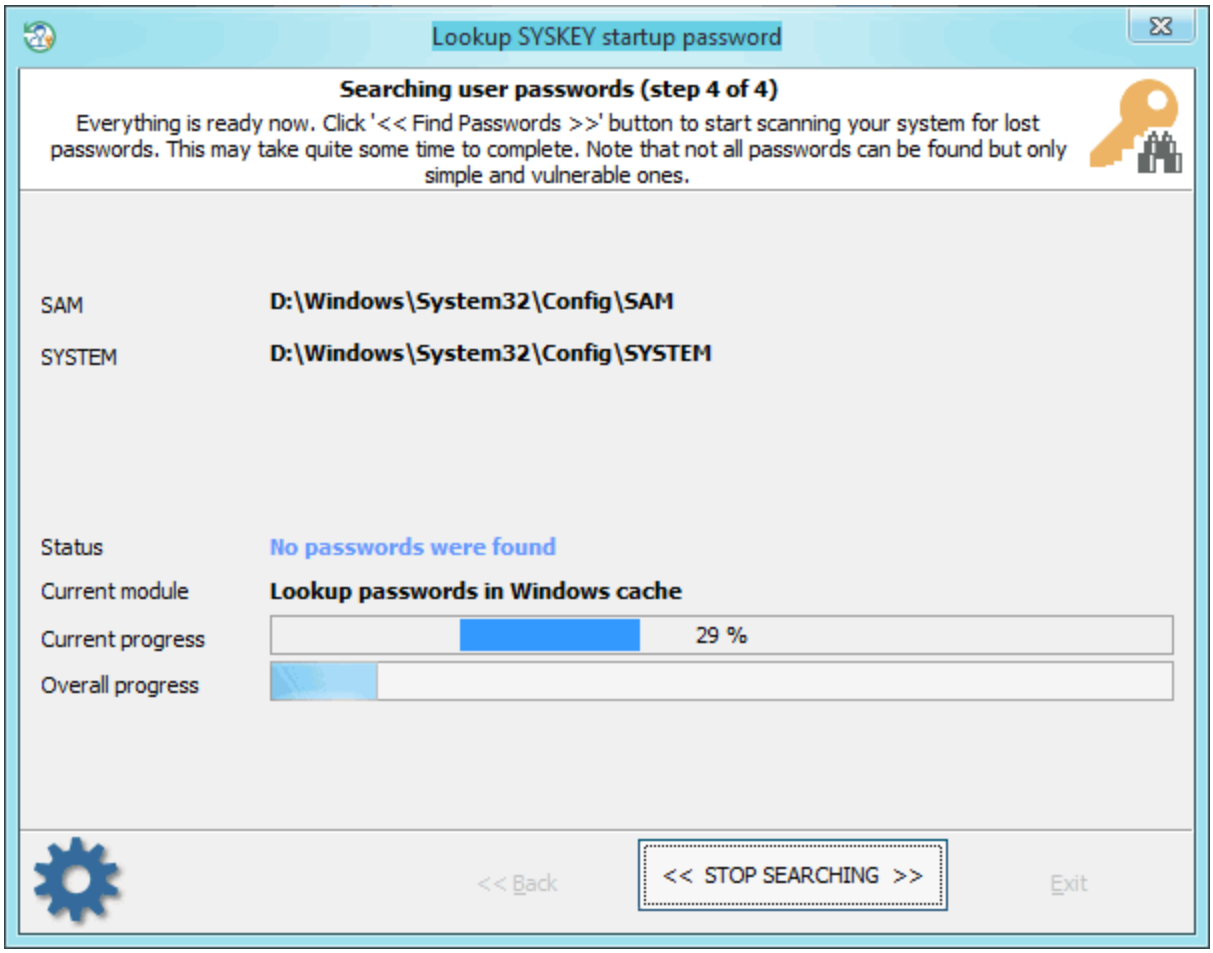
Para aplicar un método de recuperación personalizado, active la opción 'Recuperación personalizada' y seleccione uno de los ataques disponibles. En el siguiente paso, se le pedirá que configure varias opciones relacionadas con el ataque seleccionado.

Selección del origen de datos



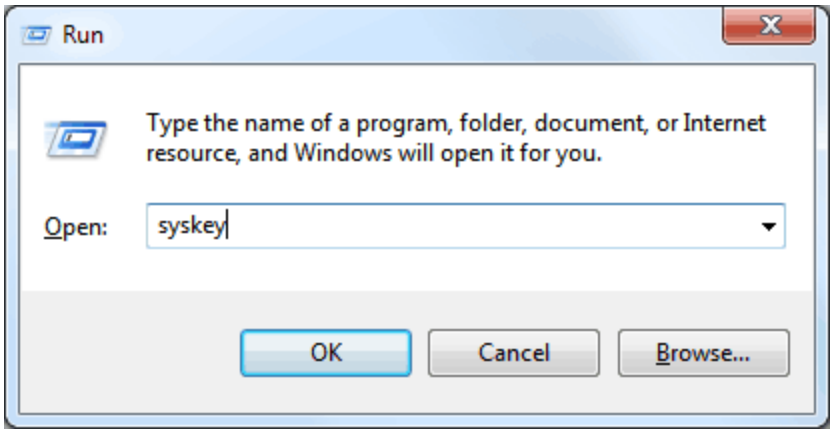
Al buscar la contraseña de inicio de SYSKEY, se debe prestar especial atención al suministro de los archivos y carpetas correctos necesarios para el proceso de análisis. De lo contrario, la búsqueda de contraseñas será ineficiente o incluso no estará disponible. La aplicación intenta localizar los archivos automáticamente, pero a veces, por ejemplo, cuando la computadora tiene varios sistemas operativos instalados, es posible que deba usar el "control manual" sobre ella. Tenga en cuenta también que si el PC problemático tiene 2 o más unidades lógicas, la secuencia de las letras para estos discos puede ser totalmente diferente a la del sistema original.

Búsqueda de contraseña SYSKEY

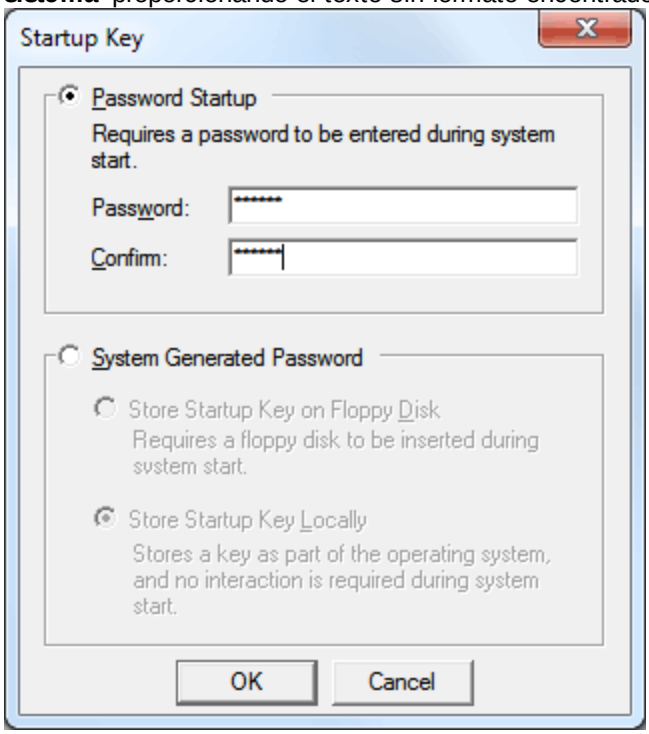


Encontrar / adivinar la contraseña puede llevar algún tiempo, lo que depende de la configuración de ataque y las peculiaridades de su sistema. ¡Tenga en cuenta que solo se pueden recuperar contraseñas simples y vulnerables!

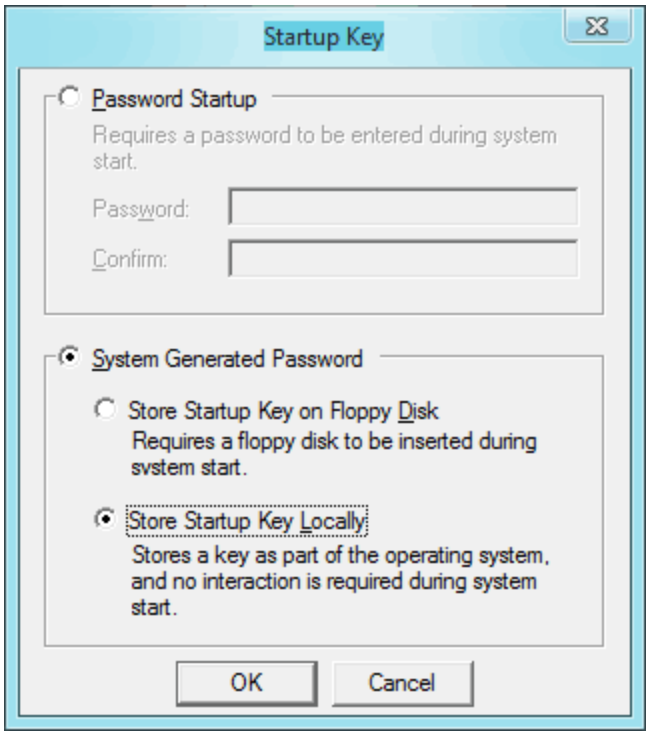
Una vez que recupere la contraseña de texto sin formato de SYSKEY, todo lo que necesita es desactivar el mensaje de inicio de SYSKEY y volver a configurar su sistema a su estado original. Encienda su PC con problemas y use la contraseña encontrada para omitir el cuadro de diálogo de inicio de SYSKEY. Luego inicie sesión en su cuenta de Windows, presione las teclas '**Win + R**', escriba '**SYSKEY**' y haga clic en el botón '**Aceptar**'.



Esto debería abrir el cuadro de diálogo de opciones syskey. Todo lo que necesita aquí es hacer clic en el botón '**Actualizar**' y cambiar la opción '**Inicio de contraseña**' a '**Contraseña generada por el sistema**' proporcionando el texto sin formato encontrado.



Entonces, después de todos los cambios, debe hacer que se vea así:

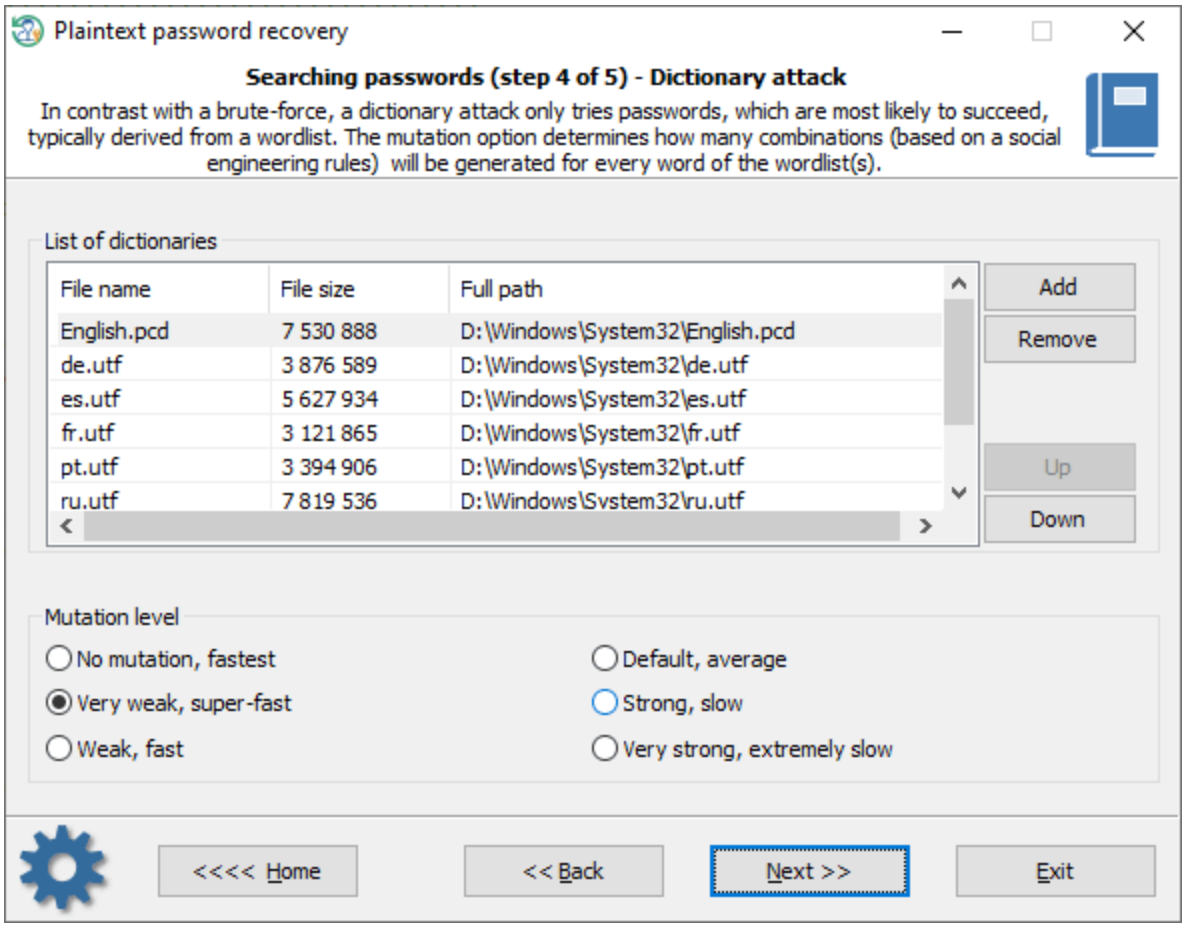


3.16.3.1 Recuperación personalizada

Una vez que se establece la opción de recuperación personalizada, el programa también puede ejecutar 3 ataques diferentes para adivinar las contraseñas:

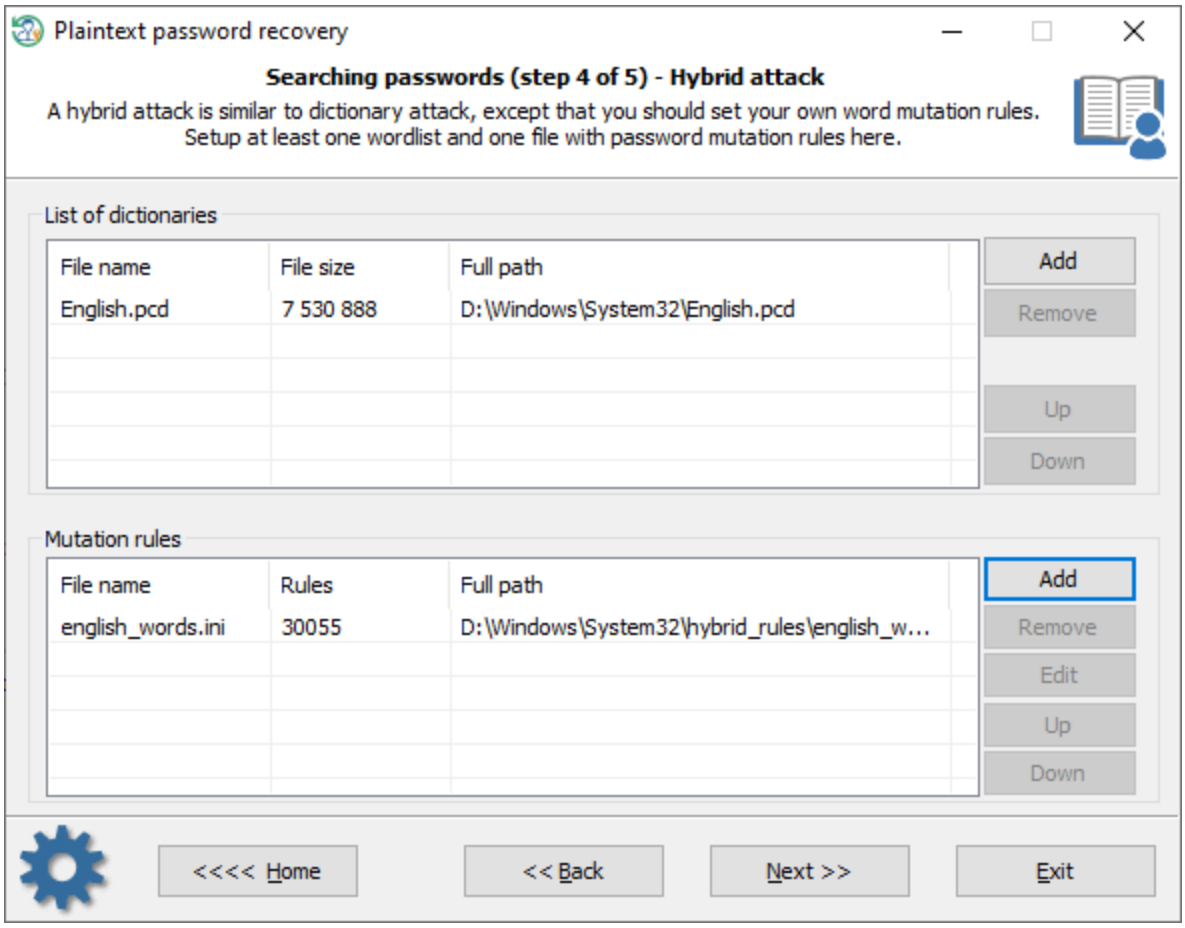
- Ataque de diccionario
- Ataque híbrido
- Ataque de máscara

Ataque de diccionario



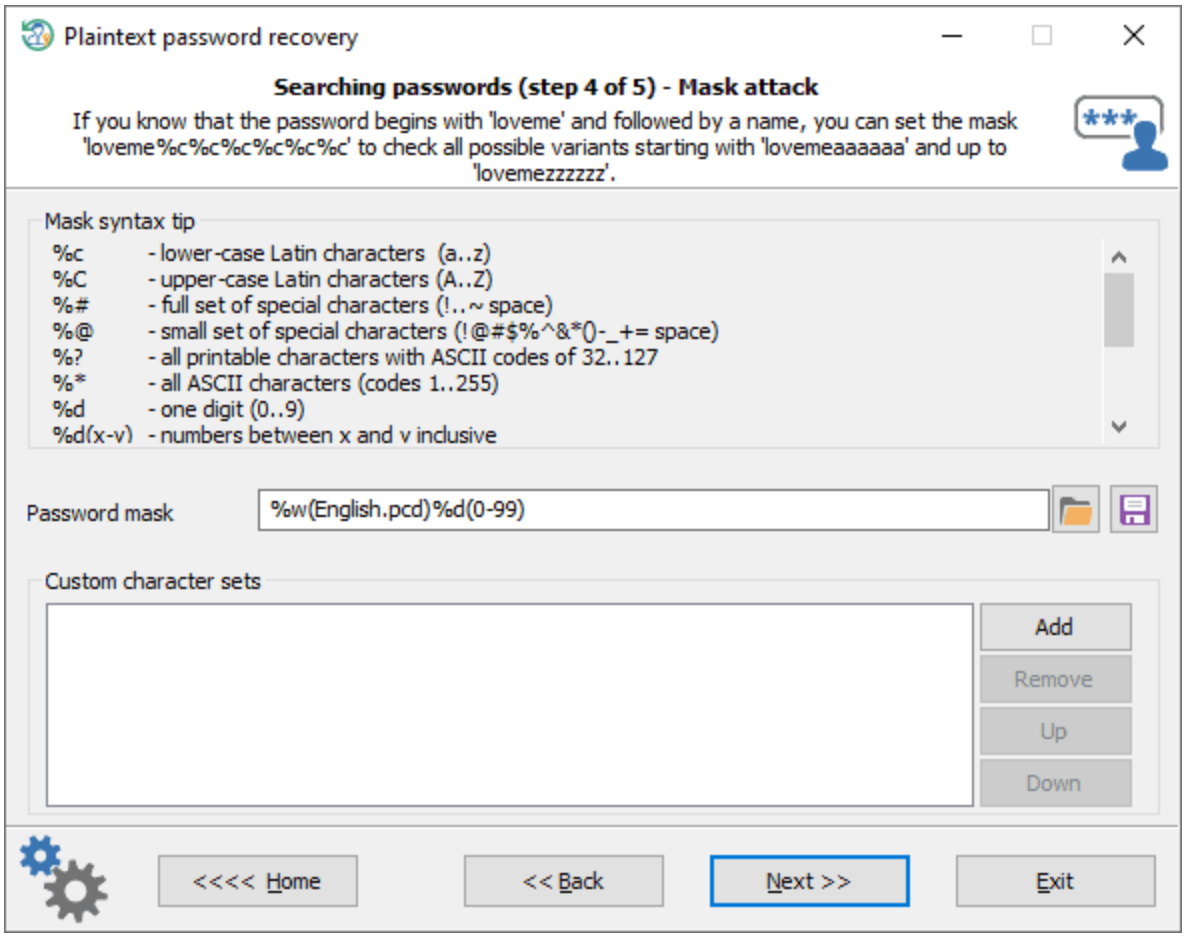
Un ataque de diccionario intenta contraseñas, que tienen más probabilidades de tener éxito, generalmente derivadas de una lista de palabras. RWP soporta diferentes tipos de diccionarios: ASCII, UNICODE, UTF8, así como diccionarios cifrados/comprimidos en formato PCD nativo. Puede utilizar diccionarios predefinidos y personalizados. Para agregar su propia lista de palabras, copie una en una unidad USB y conecte la unidad a la PC de destino. El nivel de mutación determina cuántas combinaciones (basadas en reglas de ingeniería social) se generarán para cada palabra de la(s) lista(s) de palabras.

Ataque híbrido



Un ataque híbrido es similar a uno de diccionario, excepto que puede establecer sus propias reglas de mutación de palabras. El programa viene con un gran conjunto de archivos de reglas. Simplemente use uno que sea mejor para su tarea. Lo bueno de un ataque híbrido es que además puedes crear, editar y modificar reglas de mutación de contraseña según tus necesidades.

Ataque de máscara

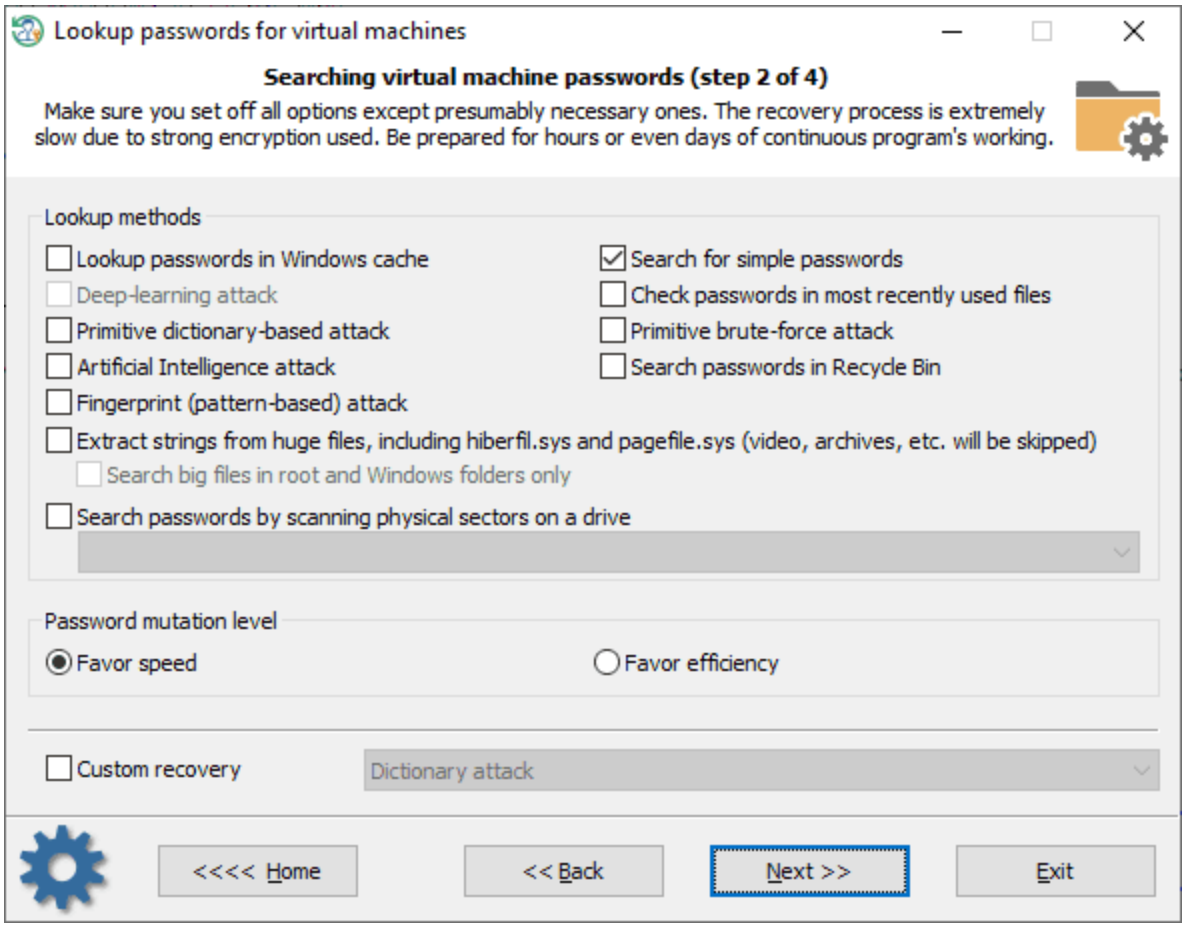


Un Ataque de máscara es una herramienta insustituible cuando conoce una parte de la contraseña o tiene algún detalle específico sobre ella. Por ejemplo, si sabes que la contraseña consta de 12 caracteres y comienza con 'loveme', obviamente basta con adivinar los últimos 6 caracteres de la contraseña. Para eso está el ataque de la máscara. En nuestro ejemplo, puede configurar la siguiente máscara: loveme%c%c%c%c%c%c%c%c
Para obtener más información sobre cómo funciona la máscara, consulte nuestra documentación en línea.

3.16.4 Buscar contraseñas de máquinas virtuales

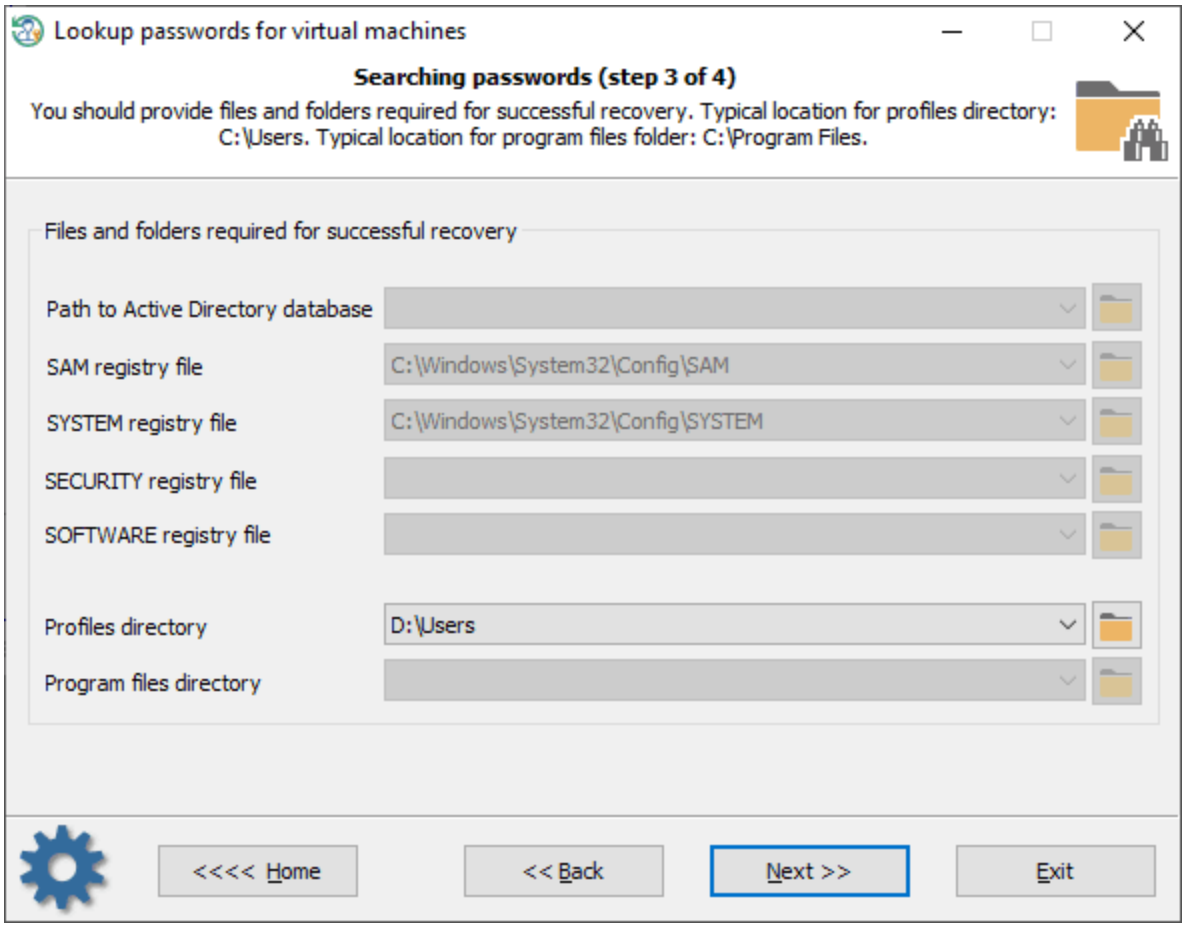
Una vez que se olvida una contraseña para la máquina virtual, puede usar esta característica RWP para recuperar el acceso a la máquina virtual bloqueada. La versión actual del programa es compatible con las máquinas virtuales VmWare y Oracle VirtualBox. Ambos programas de virtualización tienen una protección muy fuerte, por lo que la recuperación de contraseñas para estas máquinas virtuales tiene algunas peculiaridades que se describen a continuación.

Configuración de métodos de recuperación de contraseña



Al principio, determine qué métodos de búsqueda se ajustan mejor a su tarea. La recuperación de contraseñas para máquinas virtuales es un proceso extremadamente lento, por lo que se recomienda encarecidamente deshabilitar los elementos más costosos en tiempo. La casilla de verificación 'Recuperación personalizada' cambia entre plantillas de ataque personalizadas y predefinidas. Si se selecciona el primero, se le pedirá que configure algunas opciones para el ataque seleccionado durante los siguientes pasos del Asistente. Si se conoce cierta información sobre la contraseña, un ataque personalizado sería su elección.

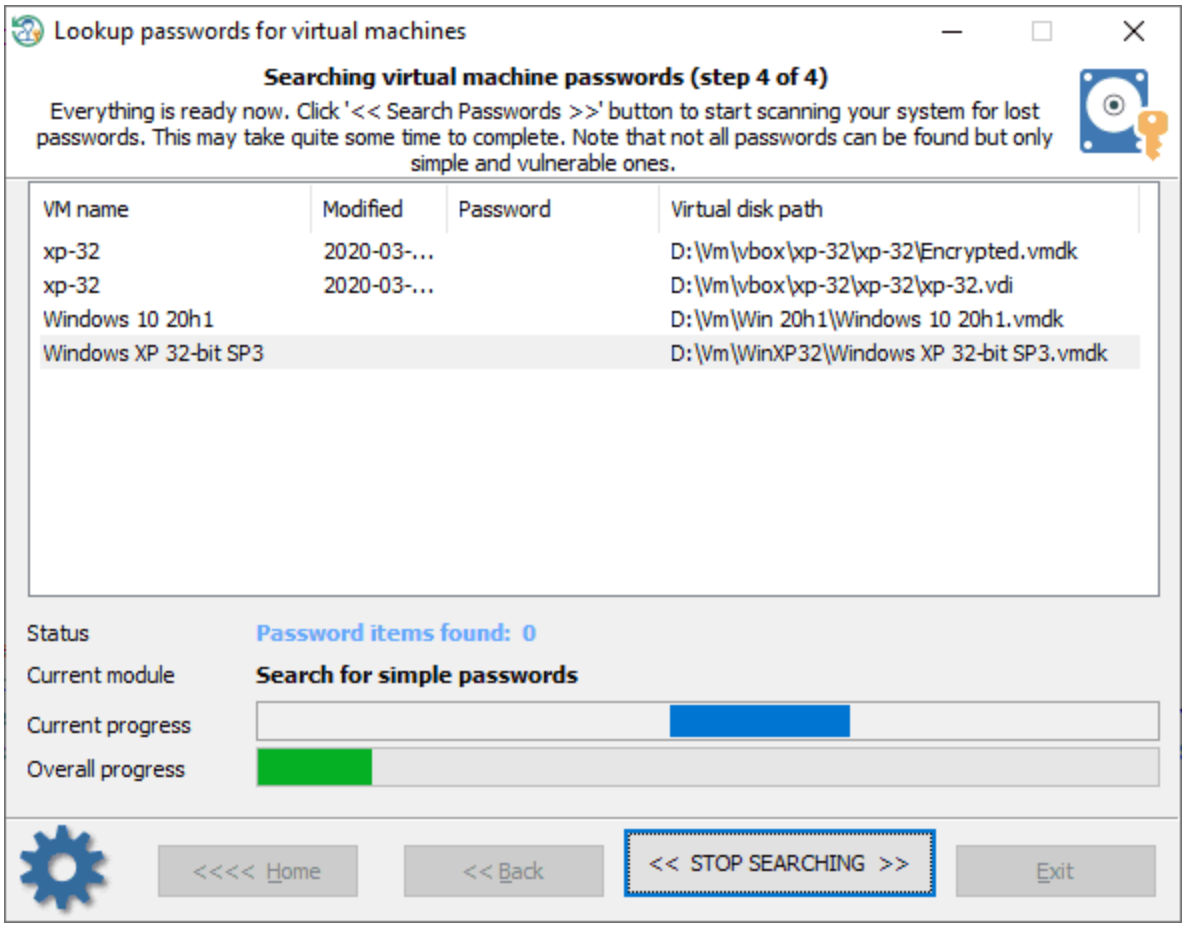
Selección del origen de datos



Por favor, preste especial atención a la configuración de todas las carpetas necesarias para un análisis posterior del sistema. De lo contrario, el programa no podrá detectar máquinas virtuales que no busquen contraseñas correctamente. En la mayoría de los casos, RWP rellena automáticamente todos los campos con los archivos y carpetas necesarios.

¡Tenga en cuenta que las letras del disco pueden diferir de las del sistema original!

Búsqueda de contraseñas de máquinas virtuales



La búsqueda de contraseñas de VM suele tardar mucho tiempo. Todas las máquinas virtuales tienen una protección muy fuerte y, en algunos casos, la velocidad de búsqueda de contraseñas es tan baja como solo unas pocas contraseñas por segundo. Por lo tanto, para optimizar y aumentar el proceso, simplemente excluya las máquinas virtuales innecesarias de la lista de búsqueda y deje activa la única que necesita. Utilice el menú contextual para eso.

3.16.5 Buscar contraseñas para documentos cifrados

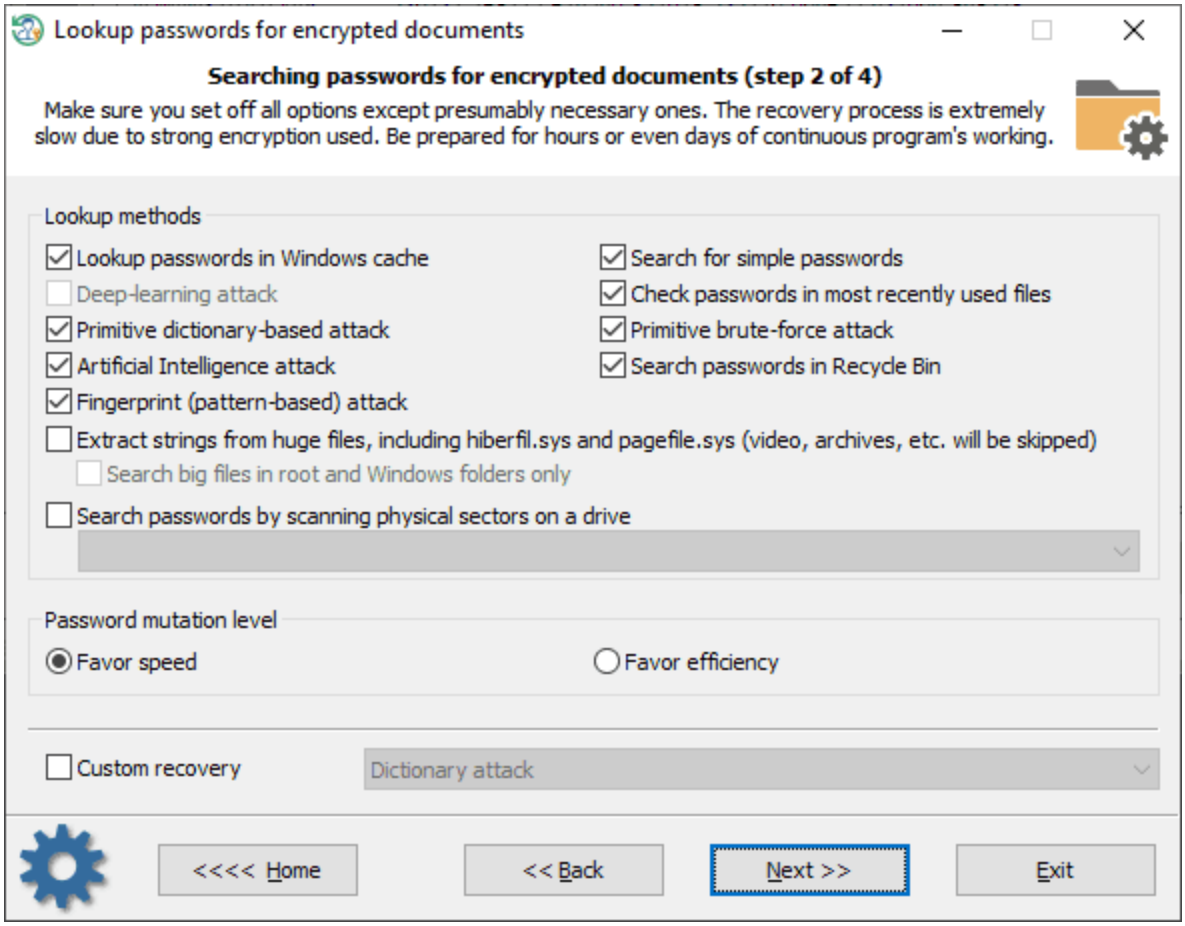
Los documentos modernos tienen una protección de contraseña extremadamente fuerte que hace que los métodos de recuperación comunes como una fuerza bruta o un ataque de diccionario sean inútiles en la mayoría de los casos. Por lo tanto, una vez que la contraseña de cifrado para dicho documento no se recuperó utilizando ningún otro programa que aplique los métodos de recuperación comunes, entonces restablecer contraseña de Windows es su última oportunidad de encontrar la contraseña.

Un secreto bien conocido que descubre la debilidad de las contraseñas es que muchos usuarios a menudo reutilizan sus contraseñas o usan variaciones ligeramente modificadas al crear cuentas de Internet, cifrar documentos, crear redes inalámbricas, etc. RWP utiliza la debilidad en su potente motor incorporado para aumentar el porcentaje de recuperación de algoritmos que no se pueden romper

utilizando métodos comunes. Si no entra en detalles, entonces todo es bastante trivial a primera vista: el programa escanea el sistema, enumera cada contraseña encontrada, así como algunos candidatos a contraseña, para cada elemento encontrado hace todas las mutaciones y modificaciones posibles, y en la etapa final, intenta adivinar la contraseña original utilizando la gran variedad de los elementos generados. A pesar de su aparente simplicidad, los algoritmos internos son bastante complejos. Por ejemplo, el módulo de búsqueda general de contraseñas consta de varias docenas de subóndodos. Esto también se aplica a otros módulos y grupos de módulos como la mutación, la inteligencia artificial, etc.

La versión actual del programa admite los siguientes formatos de archivo:
- Microsoft Office 97 y documentos más recientes
- Archivos en formato OpenDocument: OpenOffice, LibreOffice, MyOffice.
- Documentos PDF (contraseñas de usuario y propietario).

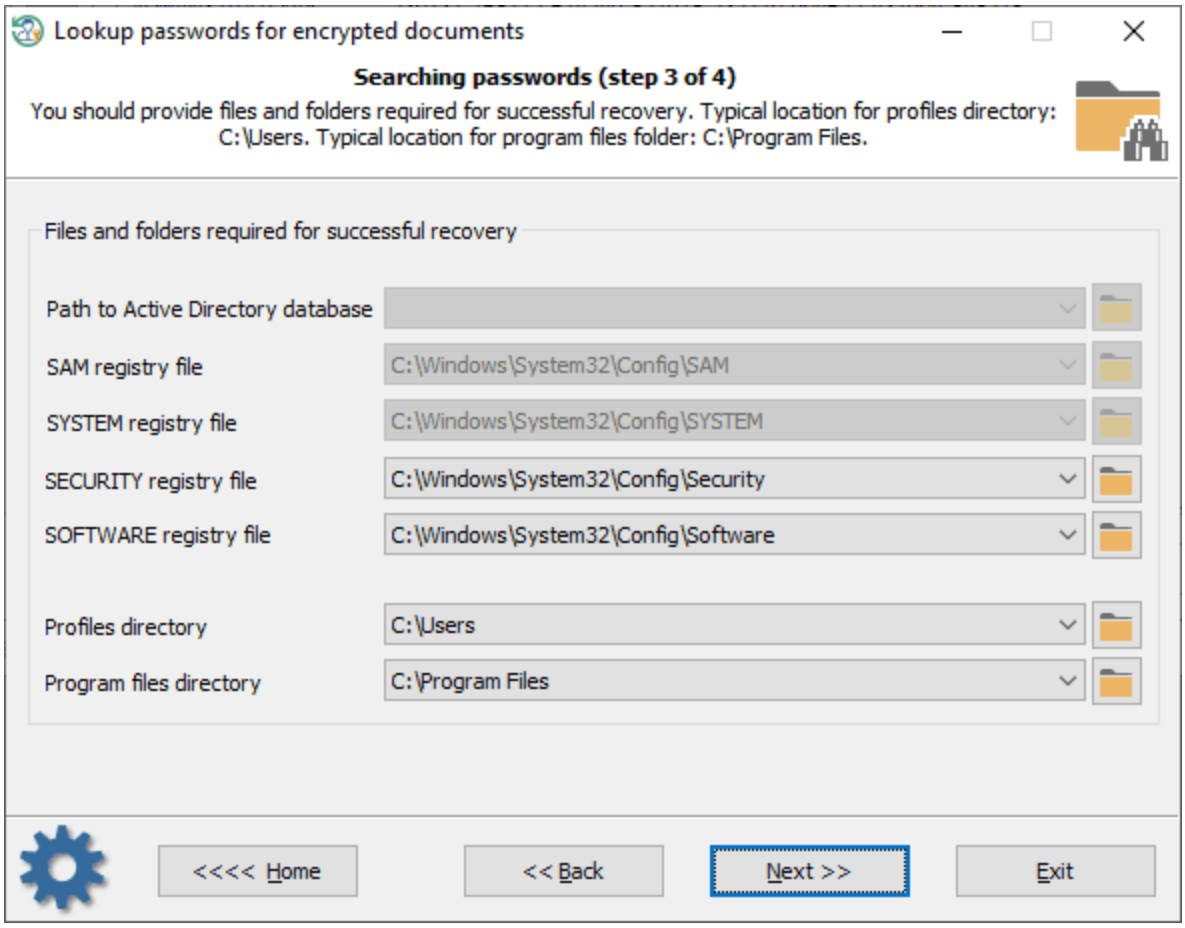
Configuración de métodos de recuperación de contraseña



Al principio, determine qué métodos de búsqueda se ajustarían mejor a su tarea. La recuperación de contraseña para documentos cifrados es un proceso extremadamente lento, especialmente si tiene más de un archivo para descifrar. Por lo tanto, es muy recomendable desactivar los métodos que consumen más tiempo. Si se conoce cierta información sobre la contraseña, entonces no sería irrazonable cambiar a un ataque personalizado. Simplemente haga clic en la opcion 'Recuperación personalizada' y

elija uno de los métodos disponibles. Por ejemplo, un ataque de máscara. De lo contrario, los parámetros predeterminados son su mejor opción.

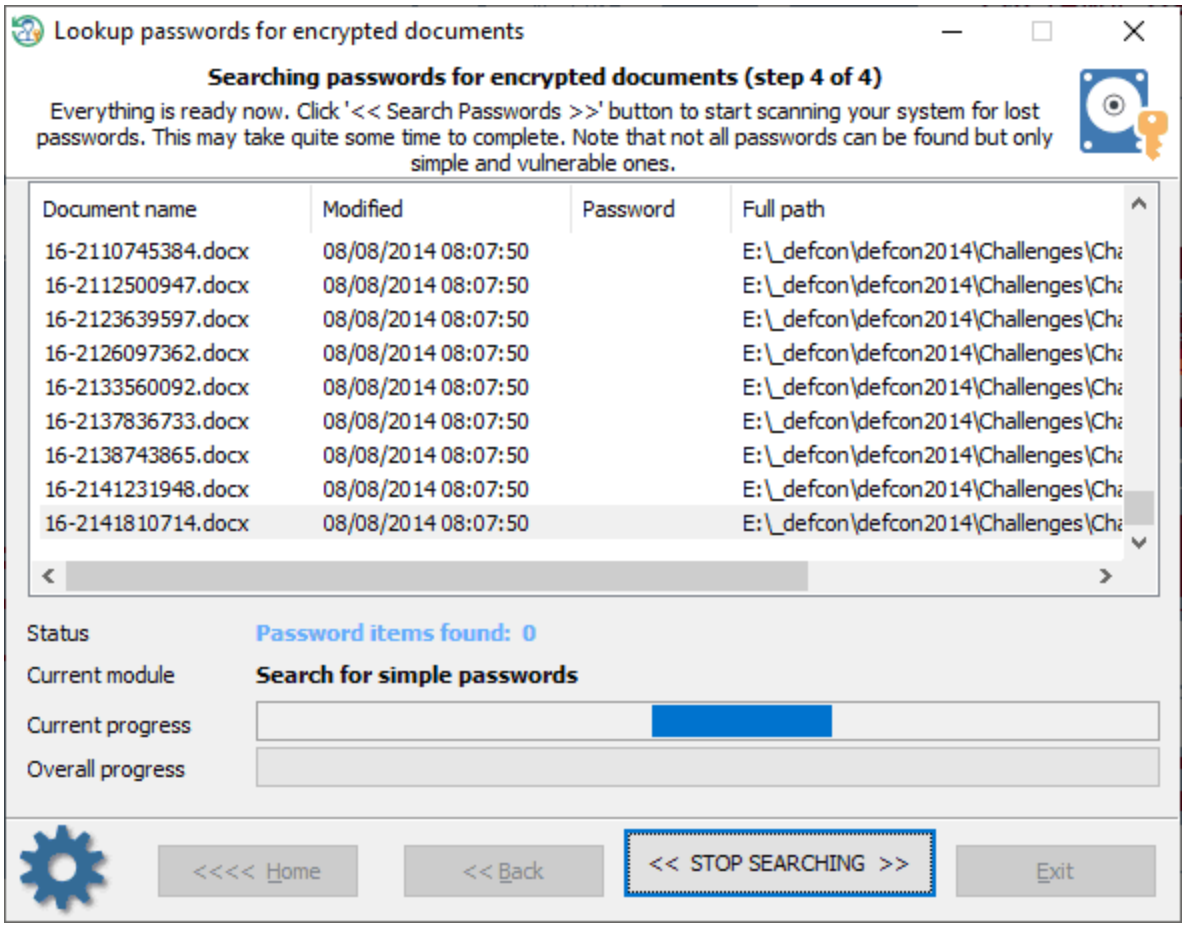
Configuración de carpetas



Todo lo que necesita aquí es configurar todas las carpetas requeridas correctamente. Algunos de ellos son vitales a la hora de analizar archivos y candidatos a contraseñas. En la mayoría de los casos, el programa los configura automáticamente.

Tenga en cuenta que las letras de la unidad pueden diferir del sistema original.

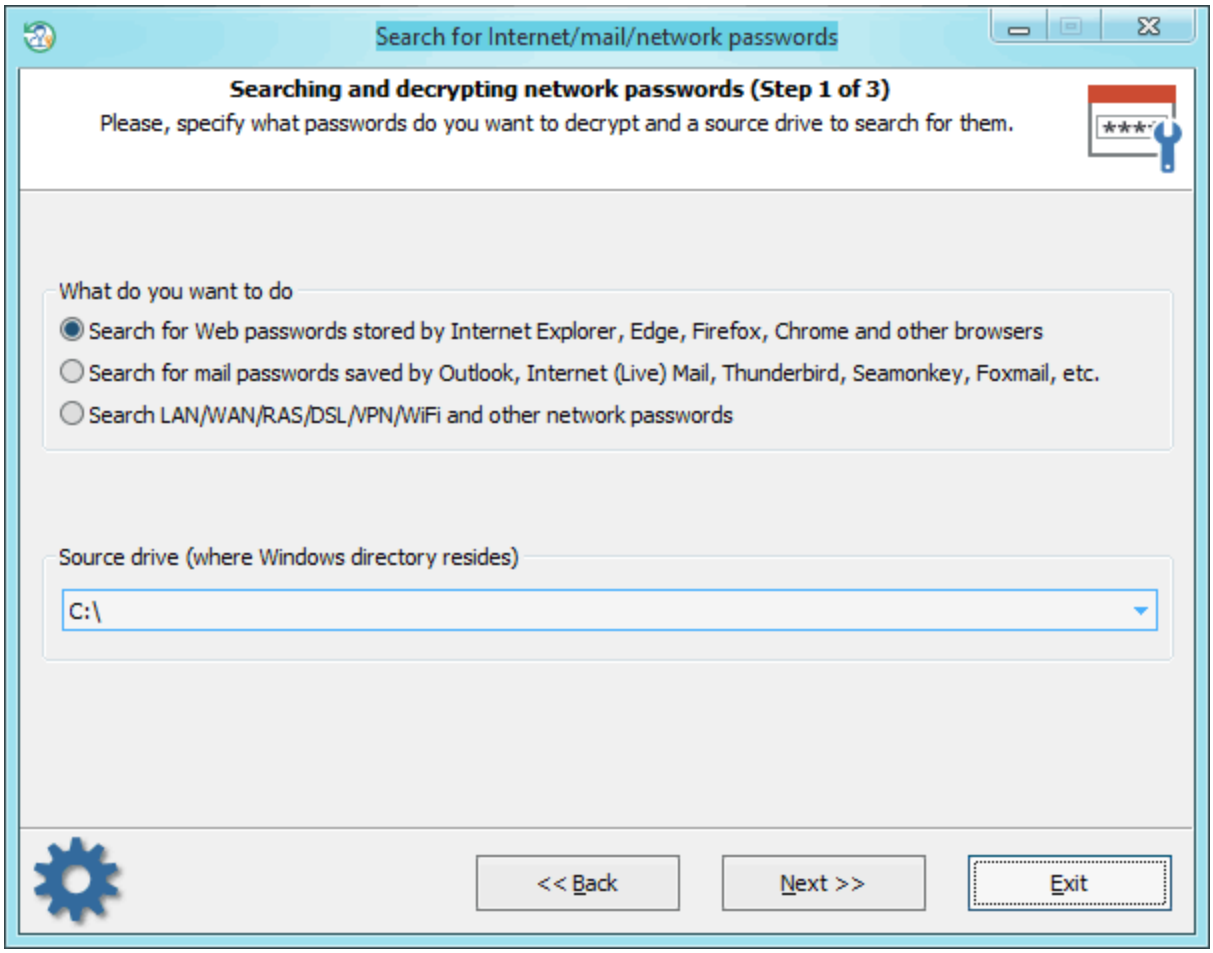
Búsqueda de contraseña para documentos cifrados



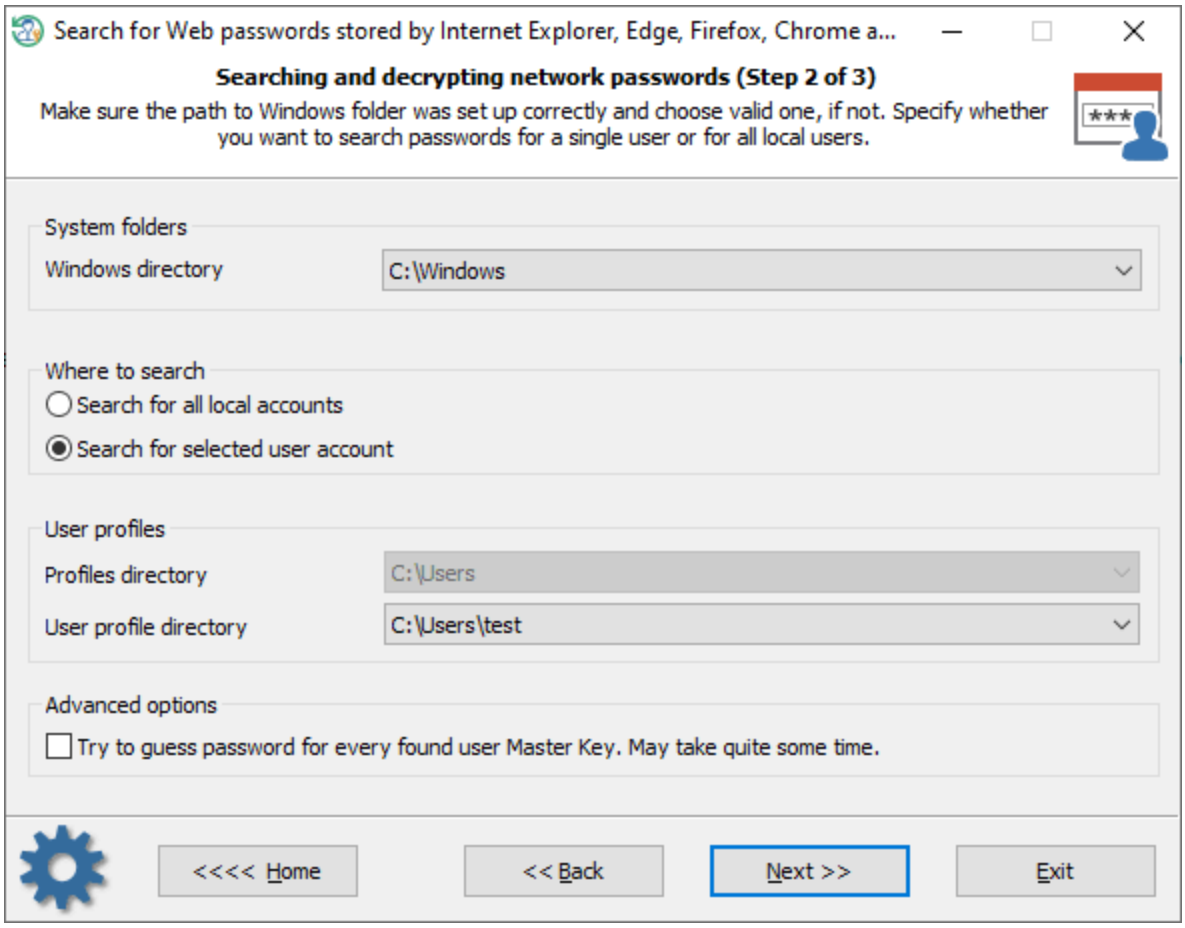
El programa adivina las contraseñas de todos los documentos encontrados simultáneamente (a menos que marque algunos de ellos para omitirlos). El proceso de búsqueda de contraseñas suele tardar bastante tiempo. Por ejemplo, adivinar contraseñas para Microsoft Office 2013 y documentos más recientes se ejecuta a menos de 10 contraseñas por segundo para un solo documento. Por lo tanto, para optimizar y aumentar la velocidad de búsqueda, excluya los documentos innecesarios de la lista de búsqueda, idealmente dejando solo el necesario. Puede usar el menú contextual para eso.
Para agregar un nuevo archivo, haga clic con el botón derecho del mouse y seleccione *'Agregar nuevo documento*'.

3.16.6 Buscar contraseñas de Internet/correo/red

Una de las características más notables de la aplicación es buscar y descifrar las contraseñas de red de los usuarios de PC. Reset Windows Password es compatible con todos los principales navegadores y clientes de correo electrónico populares. La interfaz se divide en tres pasos para que el proceso sea lo más fácil posible, y los detalles específicos se dejan al programa.



En el primer paso del Asistente, el programa le pide que seleccione el tipo de contraseñas que se buscarán y la unidad de origen con la carpeta de Windows. De forma predeterminada, el programa selecciona el primer disco duro, donde está instalado el sistema operativo.



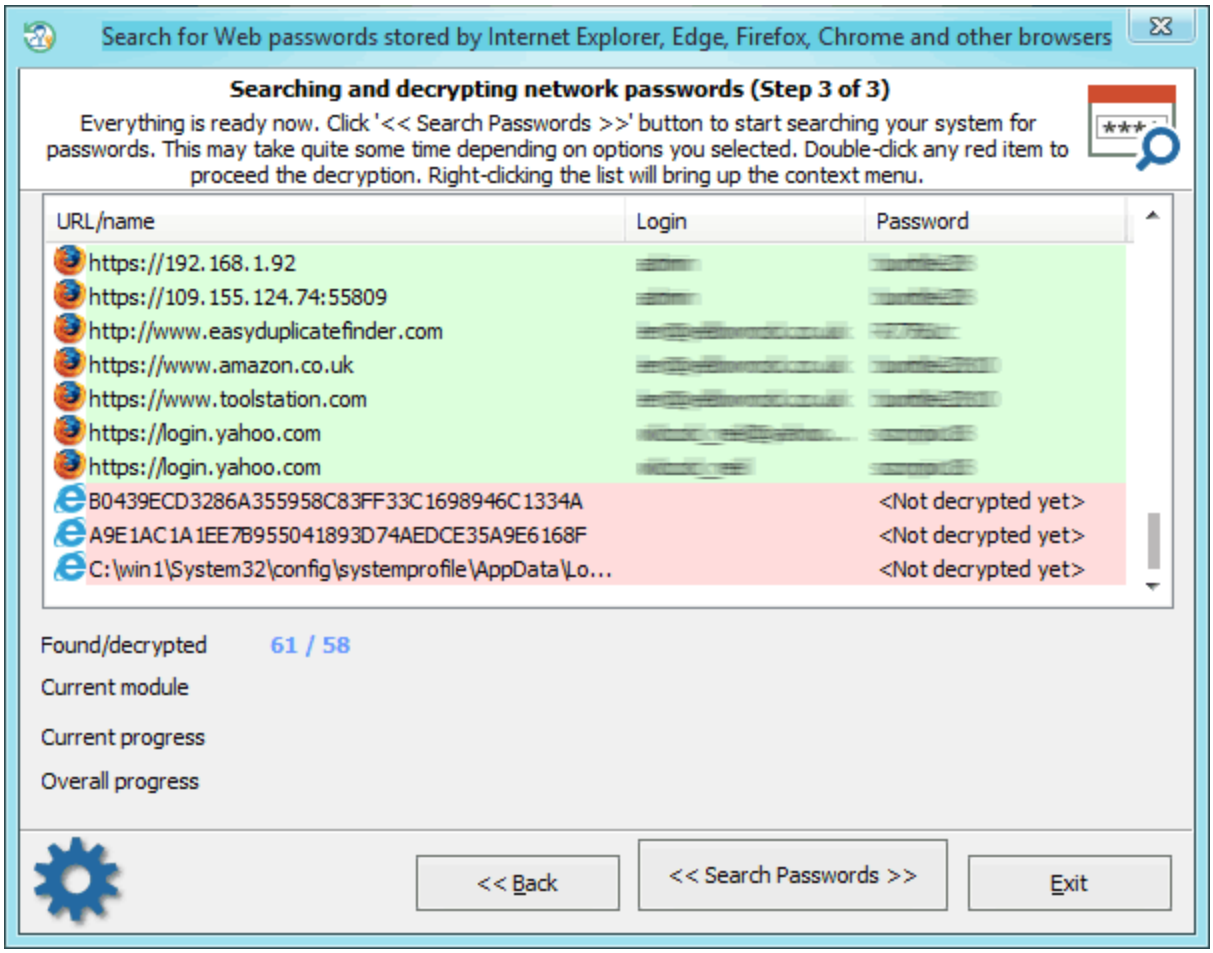
En el siguiente paso, especifique la ubicación de la carpeta de Windows y las carpetas donde el programa intentará encontrar las contraseñas: todos los perfiles de usuario o solo el seleccionado. En este último caso, seleccione la carpeta respectiva.

De forma predeterminada, el programa escanea automáticamente el sistema en busca de cualquier información (por ejemplo, TBAL o secretos de dominio) que se pueden utilizar para descifrar datos DPAPI sin proporcionar contraseñas de inicio de sesión de usuario. Sin embargo, al configurar la opción avanzada activada, puede forzar al programa a adivinar las contraseñas de la clave maestra DPAPI utilizando algunos elementos encontrados. Por ejemplo, utilizando credenciales almacenadas en caché, secretos LSA, contraseñas de navegadores extraídas, wireless/dialup/dls/ras/lan y otras contraseñas de red, etc. Una vez que se adivina una contraseña de clave maestra DPAPI, no es necesario proporcionar credenciales de inicio de sesión de usuario. El programa utiliza la clave maestra descifrada para decodificar cualquier dato protegido con esta clave.
Sin embargo, el proceso puede llevar bastante tiempo dependiendo de la cantidad de claves maestras encontradas y los elementos de contraseña para adivinar.

En el cuadro de diálogo final, al hacer clic en el botón << **Buscar contraseñas** >> se inicia el proceso de recopilación, análisis y descifrado de datos. Por favor, sea paciente; dependiendo de las opciones seleccionadas y el número de usuarios en el sistema, el proceso puede llevar bastante tiempo.

3.16.6.1 Buscar contraseñas Web almacenadas por los navegadores de Internet

Al seleccionar la búsqueda de contraseñas de Internet, se abre una pantalla como esta:



La aplicación descifra las contraseñas de todos los principales navegadores web:

- Internet Explorer
- Edge
- Firefox
- Opera
- Chrome
- Safari
- La mayoría de los navegadores basados en Mozilla: Flock, Seamonkey, Pale Moon, Waterfox, etc.
- Principales navegadores basados en fuentes de Cromo: 360 Safe Browser, 7Star, Amigo, Brave, Centbrowser, Chedot, Canary, Coccoc, Comodo Dragon, Elements, Kometa, Orbitum, QQ Browser, Sputnik, Torch, UC Browser, Uran, Vivaldi.

Los navegadores web utilizan diferentes algoritmos para proteger los datos personales de los usuarios. Las contraseñas de los siguientes navegadores se pueden descifrar casi al instante:

- Internet Explorer 4-6
- Firefox y otros navegadores basados en Mozilla (a menos que se establezca la contraseña maestra)
- Versiones antiguas de Opera (a menos que se establezca la contraseña maestra)

Descifrar otros datos requiere información adicional. Esa suele ser la contraseña maestra o la contraseña de inicio de sesión del usuario:

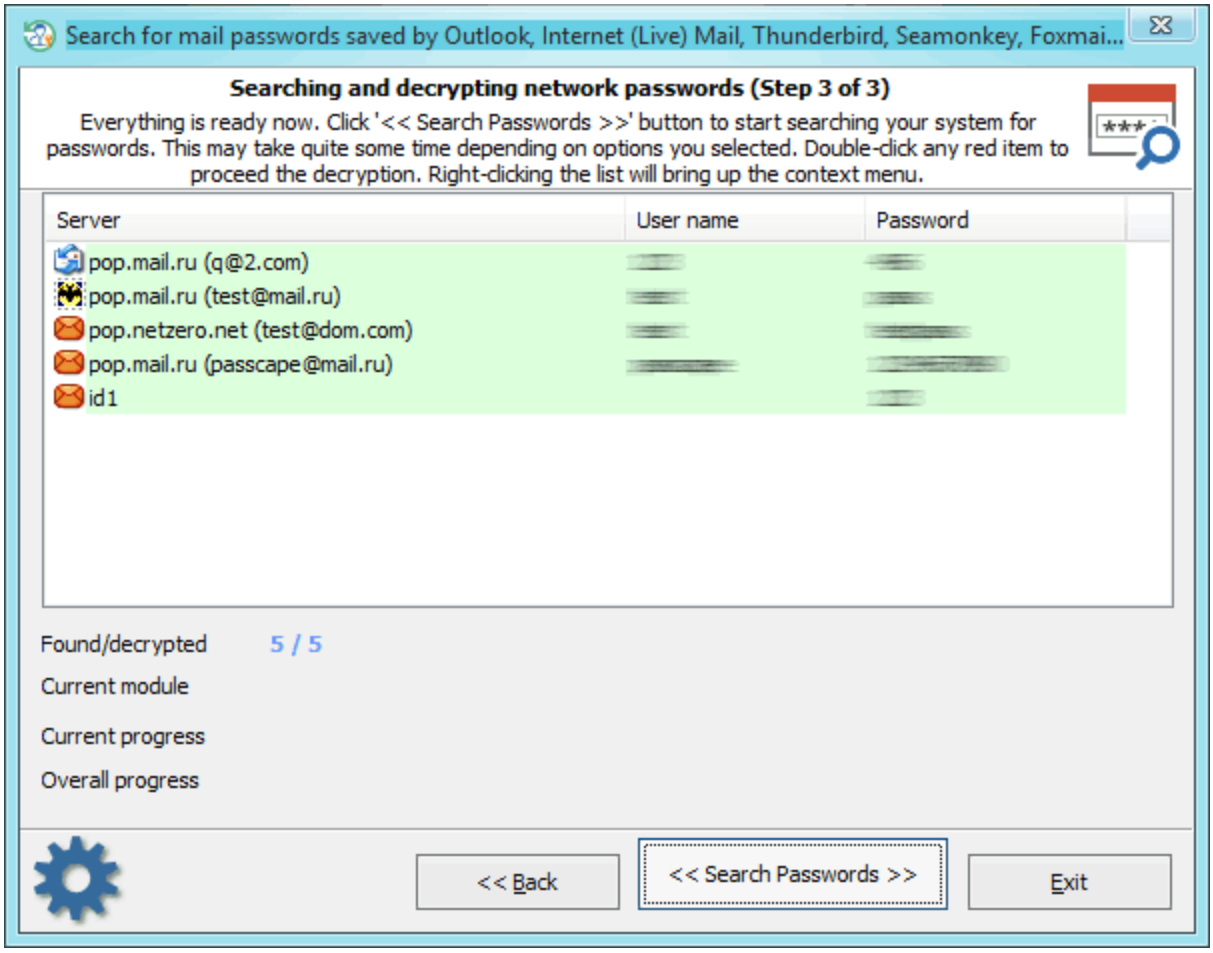
- Internet Explorer 10
- Edge
- Firefox (si se establece la contraseña maestra)

- Opera (si se establece la contraseña maestra)
- Chrome
- Safari

Para activar el siguiente paso del descifrado, simplemente haga doble clic en el registro resaltado en rojo.

Internet Explorer 7-9 requiere un descifrado en tres pasos. Primero, uno debe ingresar la URL donde se guardó la contraseña, luego ingresar la contraseña de la cuenta. Puede encontrar más información sobre este complicado tipo de protección utilizada en Internet Explorer 7-9 en nuestro artículo.

3.16.6.2 Buscar contraseñas de correo guardadas por clientes de correo electrónico



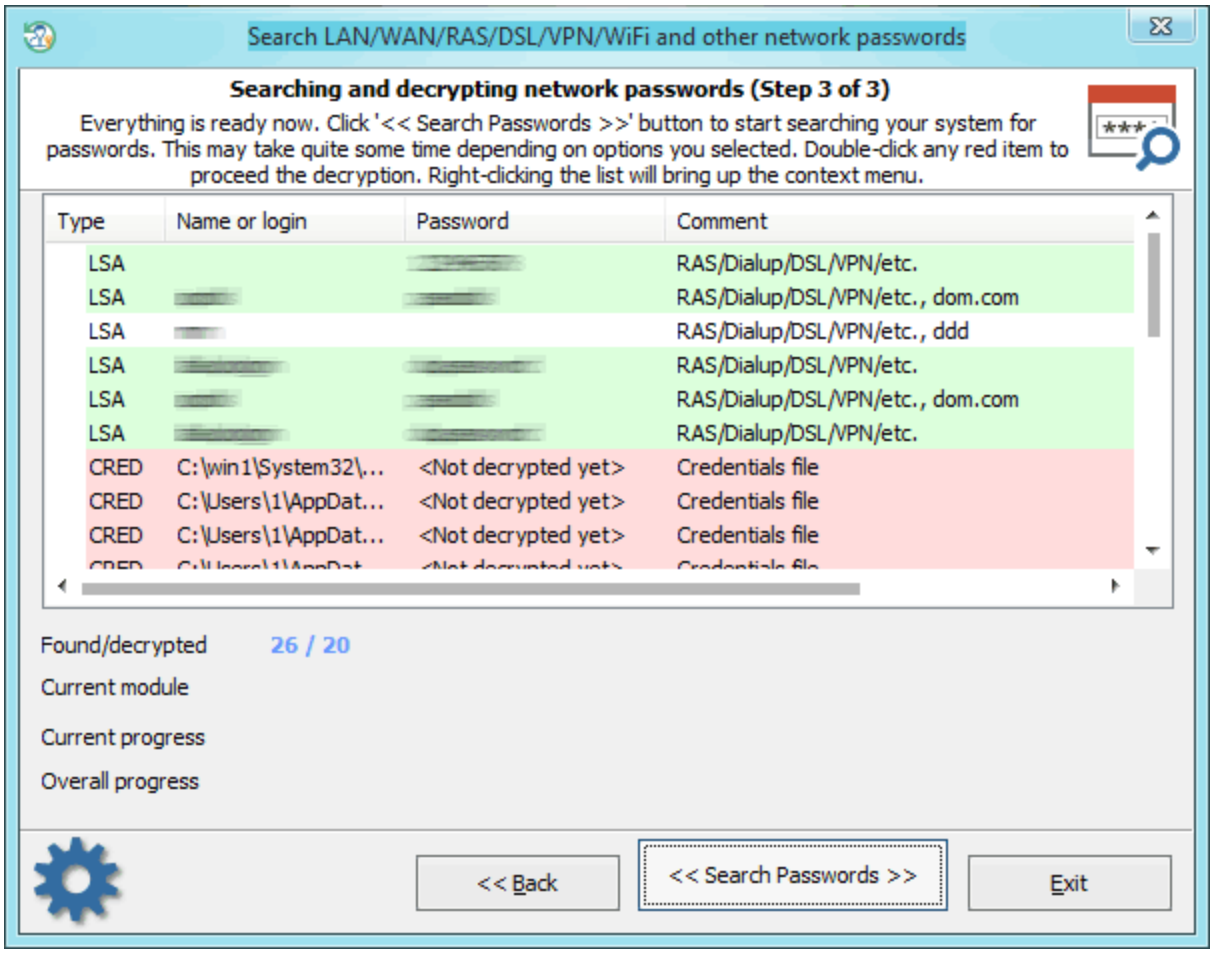
Se admiten los siguientes clientes de correo electrónico:

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

- Eudora

Tenga en cuenta que algunas contraseñas de correo electrónico podrían almacenarse en los navegadores. Esto depende de si el usuario utilizó el cliente de correo electrónico o leyó su correo electrónico mediante un navegador web. Las contraseñas de Outlook Express, TheBat!, Incredimail, Eudora y algunas versiones de MS Office Outlook se pueden descifrar casi al instante. Descifrar otros datos requiere la contraseña de la cuenta. Simplemente haga doble clic en el registro resaltado en rojo. Eso activa el segundo paso de analizar los datos encontrados. Si la contraseña de usuario introducida coincide con los otros registros, se decodificarán automáticamente.

3.16.6.3 Buscar LAN/WAN/RAS/DSL/VPN/WiFi y otras contraseñas de red



Para recopilar contraseñas de red, el programa tiene varios módulos para leer y descifrar secretos de LSA, almacenamiento protegido, administrador de contraseñas, Bóveda de Windows, etc.

El descifrado de los datos almacenados en los secretos LSA y en el almacenamiento protegido se lleva a cabo automáticamente y no requiere la introducción de parámetros adicionales. Esto se aplica a los siguientes datos:

- Contraseñas de usuario almacenadas en caché
- Contraseñas de algunas cuentas del sistema, servidor SQL, asistente remoto, etc.
- Contraseñas de servicios lanzados con credenciales específicas
- Algunas contraseñas de red almacenadas en sistemas operativos de servidor

- Contraseñas de conexión por cable: RAS, DSL, VPN, etc.
- Contraseñas de versiones antiguas de Internet Explorer/Outlook/Outlook Express/FTP, etc.
- Contraseñas para conexiones inalámbricas (WPA/WPA2)
- Contraseñas de directivas de grupo de dominio
- Contraseñas de VNC
- Contraseñas para cuentas SVN de tortuga
- Open VPN passwords
- Otro

Para otras contraseñas protegidas con DPAPI, se requiere la contraseña de la cuenta de usuario para el descifrado correcto:

- Contraseñas almacenadas en el Administrador de credenciales: contraseñas para equipos remotos en su LAN, contraseñas para algunas cuentas de correo (almacenadas por Microsoft Outlook), contraseñas de MSN Messenger, contraseñas de Internet Explorer 7-9 para sitios Web que usan Autenticación básica o Autenticación de acceso implícita, Escritorio remoto, credenciales de fuente RSS, etc.
- Registros del Almacén de Windows: contraseñas para algunas versiones de Internet Explorer/Outlook/Windows Mail, contraseñas de cuenta cuando se usa la contraseña PIN/Imagen o autenticación biométrica (solo para Windows 8).

Puede encontrar más información sobre el cifrado DPAPI en nuestra revisión detallada que cubre este método de protección.

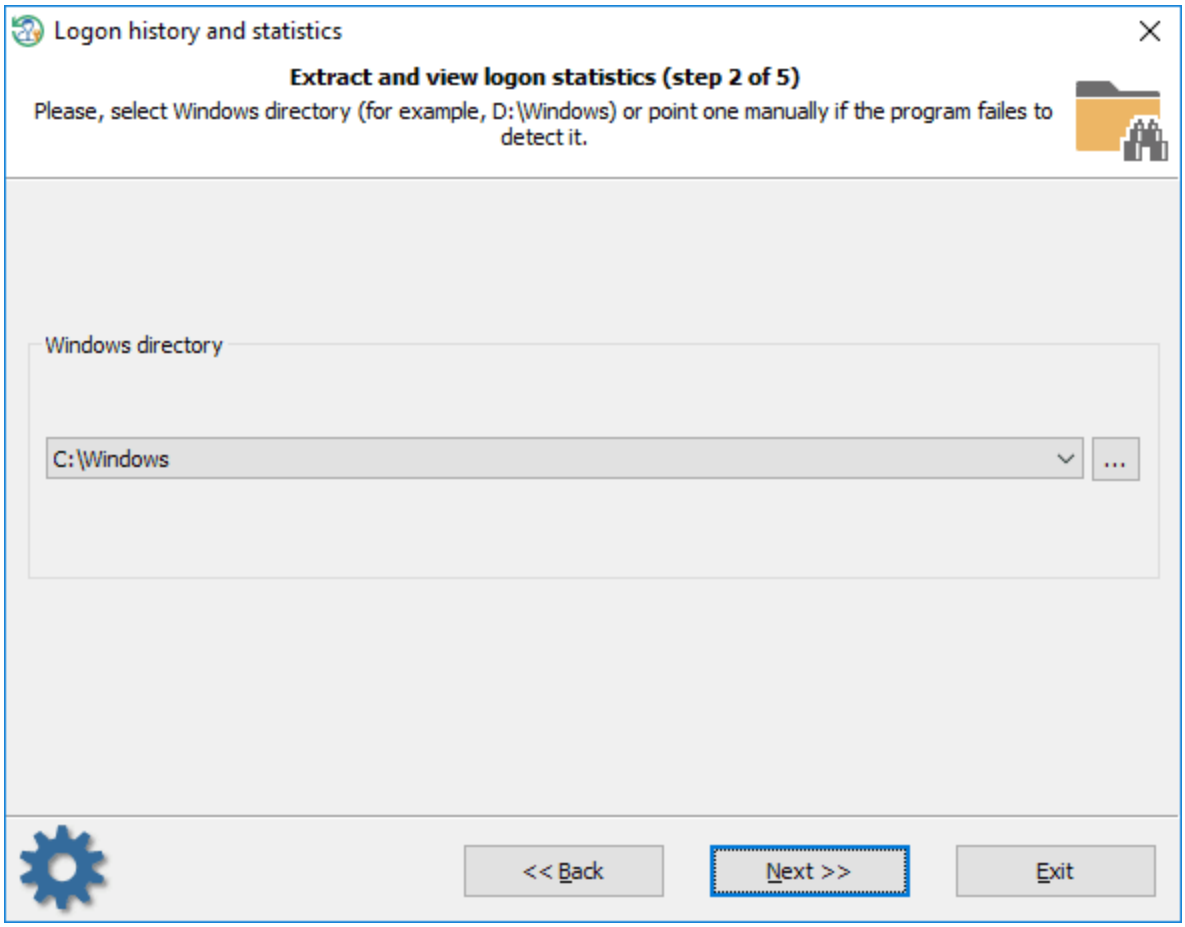
En algunos sistemas operativos de servidor, el programa puede explotar con éxito la vulnerabilidad que hemos encontrado, que permite descifrar blobs DPAPI sin ingresar la contraseña de la cuenta del propietario de los datos. Más información al respecto está disponible en nuestro artículo que cubre vulnerabilidades en los sistemas operativos de servidor.

3.17 FORENSICS

3.17.1 Ver el historial de inicio de sesión y las estadísticas

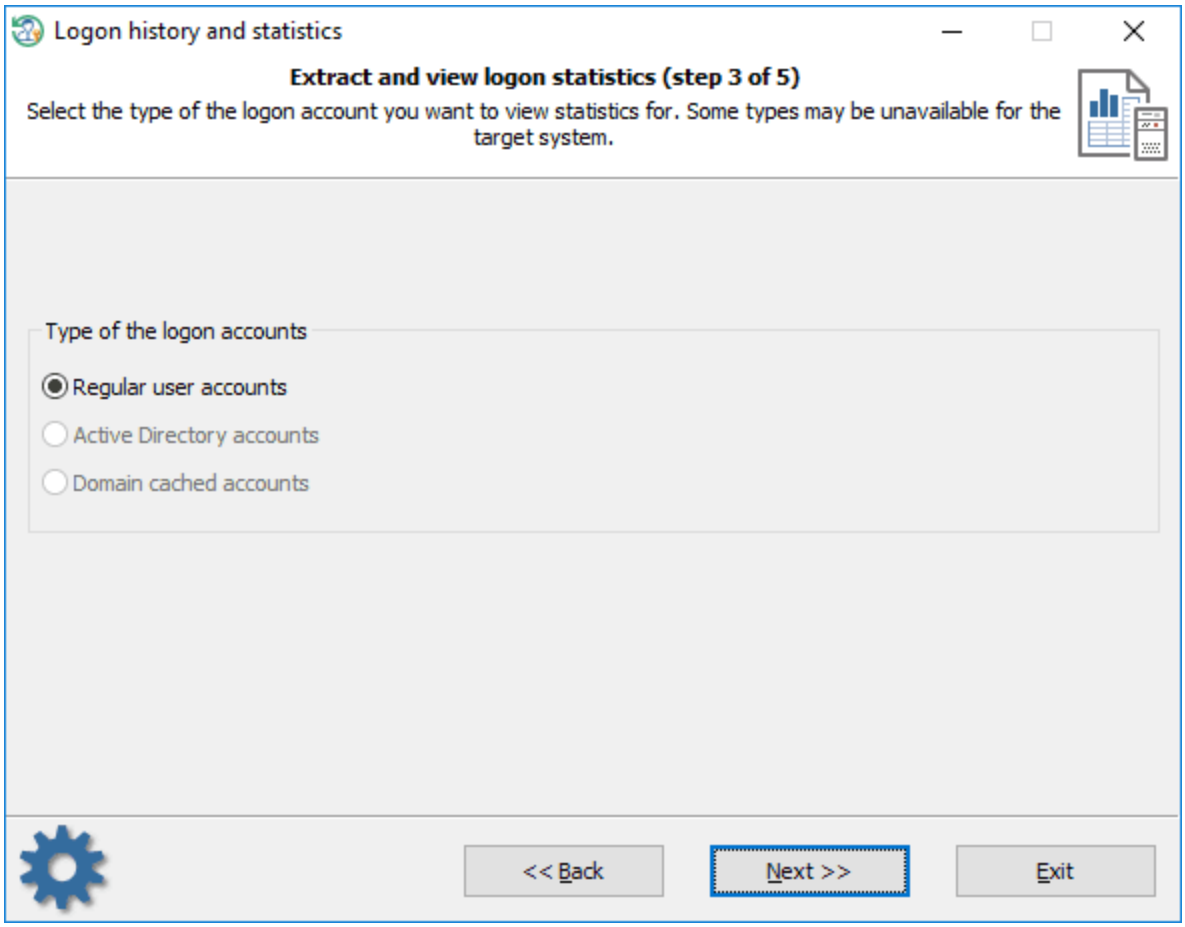
Esta es una herramienta para ver estadísticas de inicio de sesión misceláneas de usuarios regulares y de dominio.

Selección del directorio de Windows



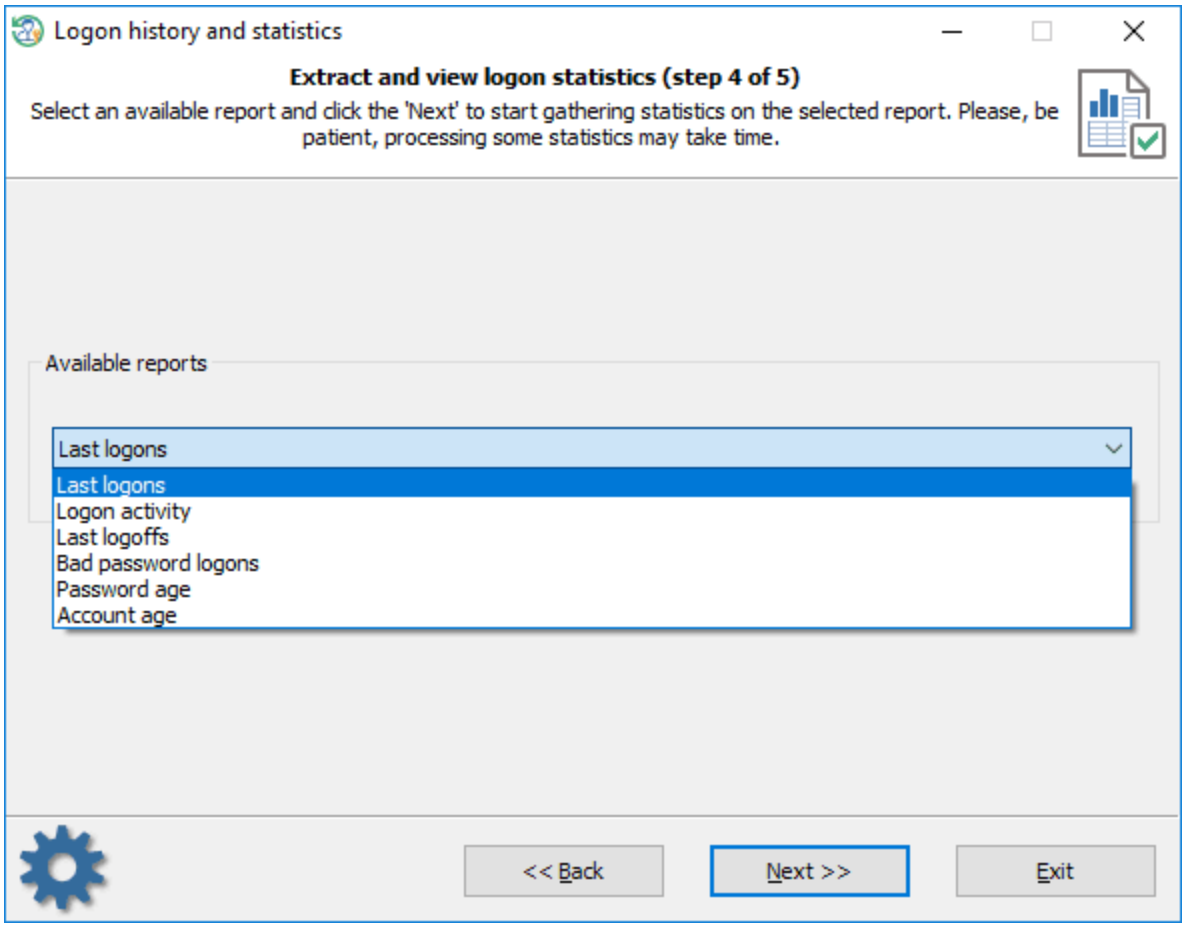
En primer lugar, debe seleccionar un directorio de Windows de destino o buscarlo si el programa no detecta uno automáticamente.

Tipo de cuentas de inicio de sesión



Una vez seleccionado el directorio de Windows, el programa intentará detectar si el sistema contiene alguna cuenta de dominio (además de las normales). Seleccione el tipo de cuentas de inicio de sesión para las que desea ver las estadísticas y continúe con el siguiente paso.

Informes disponibles

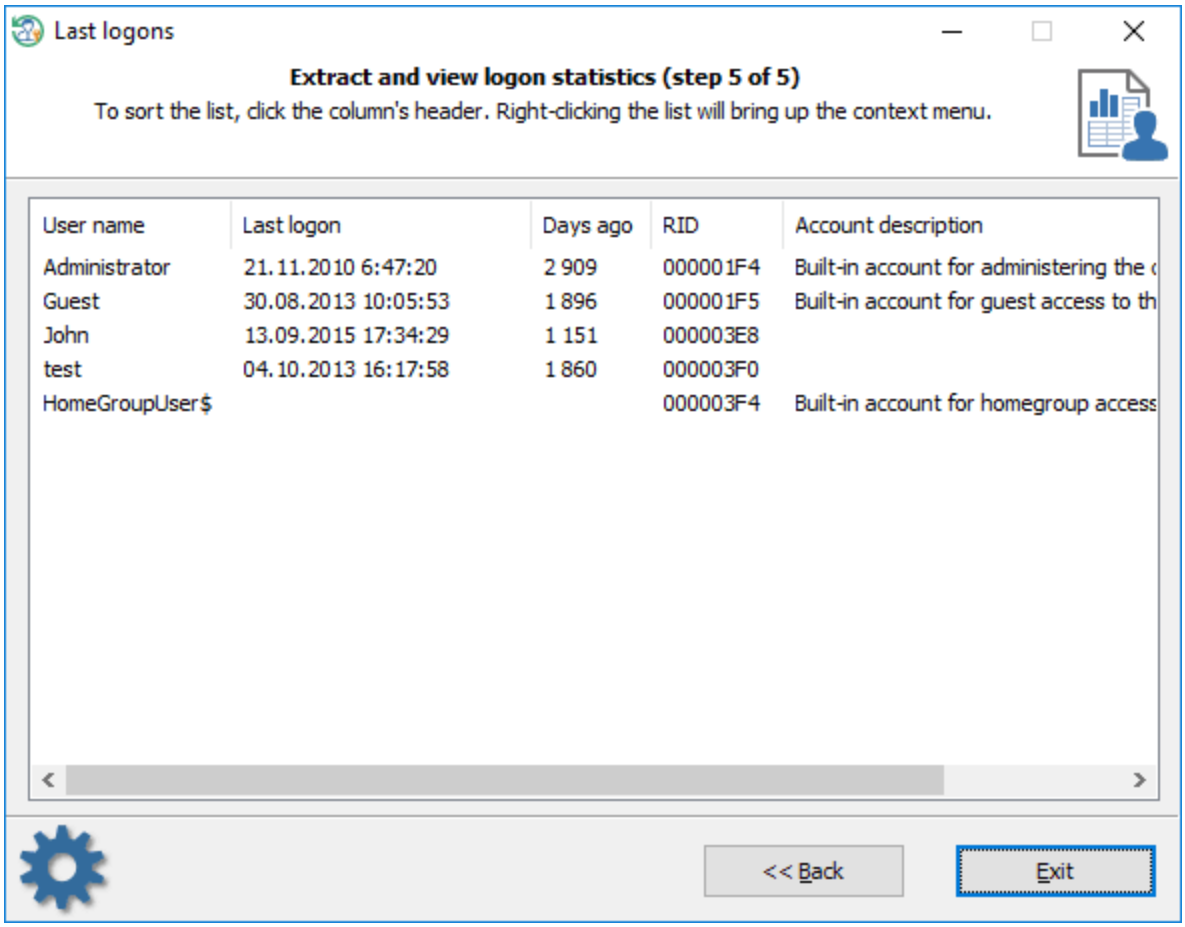


Aquí puede elegir uno de los siguientes informes:

- Últimos inicios de sesión: muestra la fecha de inicio de sesión de los usuarios
- Actividad de inicio de sesión: genera la mayoría de los usuarios activos
- Últimos cierres de sesión: desafortunadamente, la mayoría de las versiones de Windows dejaron de guardar la fecha de cierre de sesión. Sin embargo, cierta información relacionada está disponible en 'Actividad del usuario'.
- Inicio de sesión con contraseña incorrecta: la última vez que un usuario intentó iniciar sesión en su cuenta con una contraseña no válida.
- Antigüedad de la contraseña: la última vez que un usuario cambió su contraseña.
- Antigüedad de la cuenta: cuando se creó la cuenta por primera vez.

Algunos de los informes no están disponibles para las cuentas almacenadas en caché de dominio.

Estadísticas de inicio de sesión

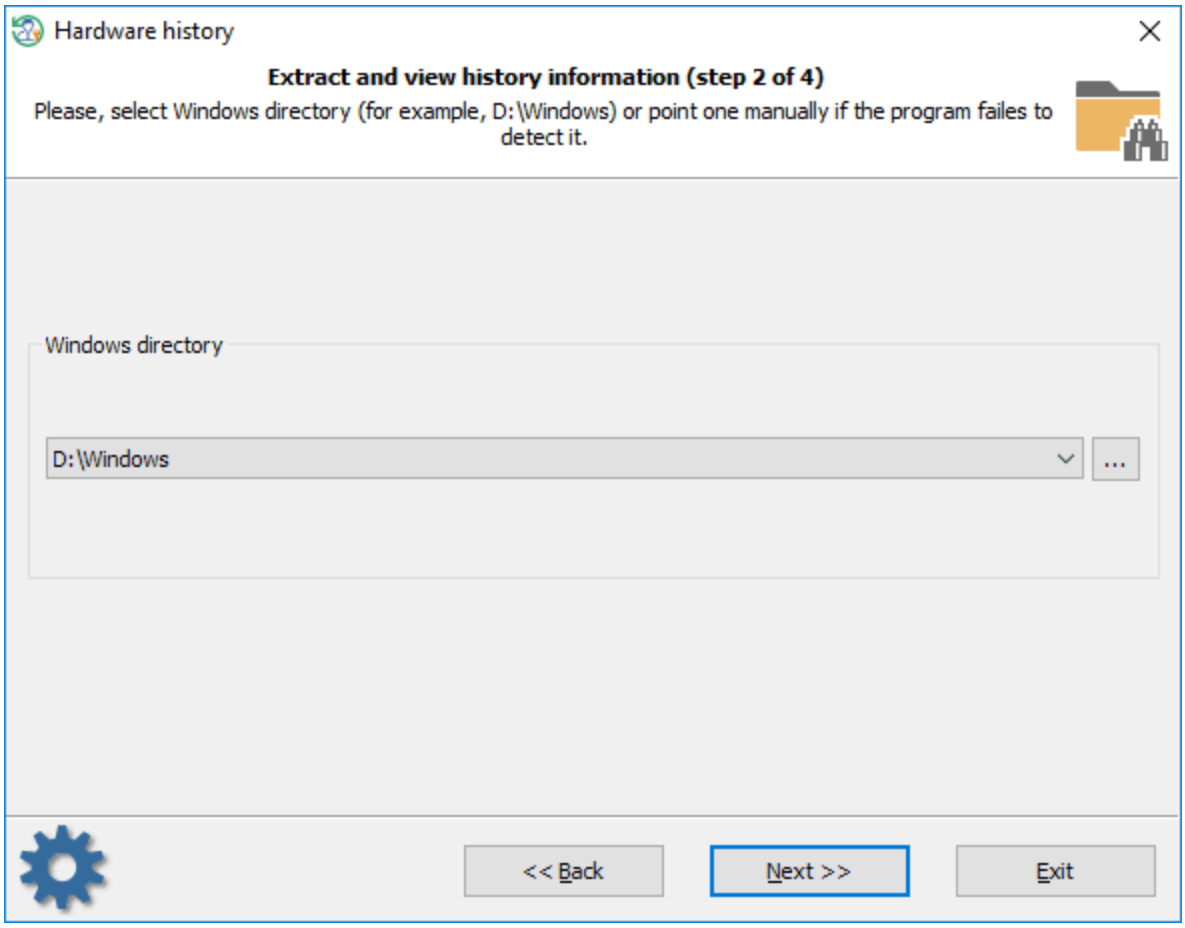


Puede copiar estadísticas en el portapapeles o guardarlo en un archivo.

3.17.2 Ver el historial de hardware

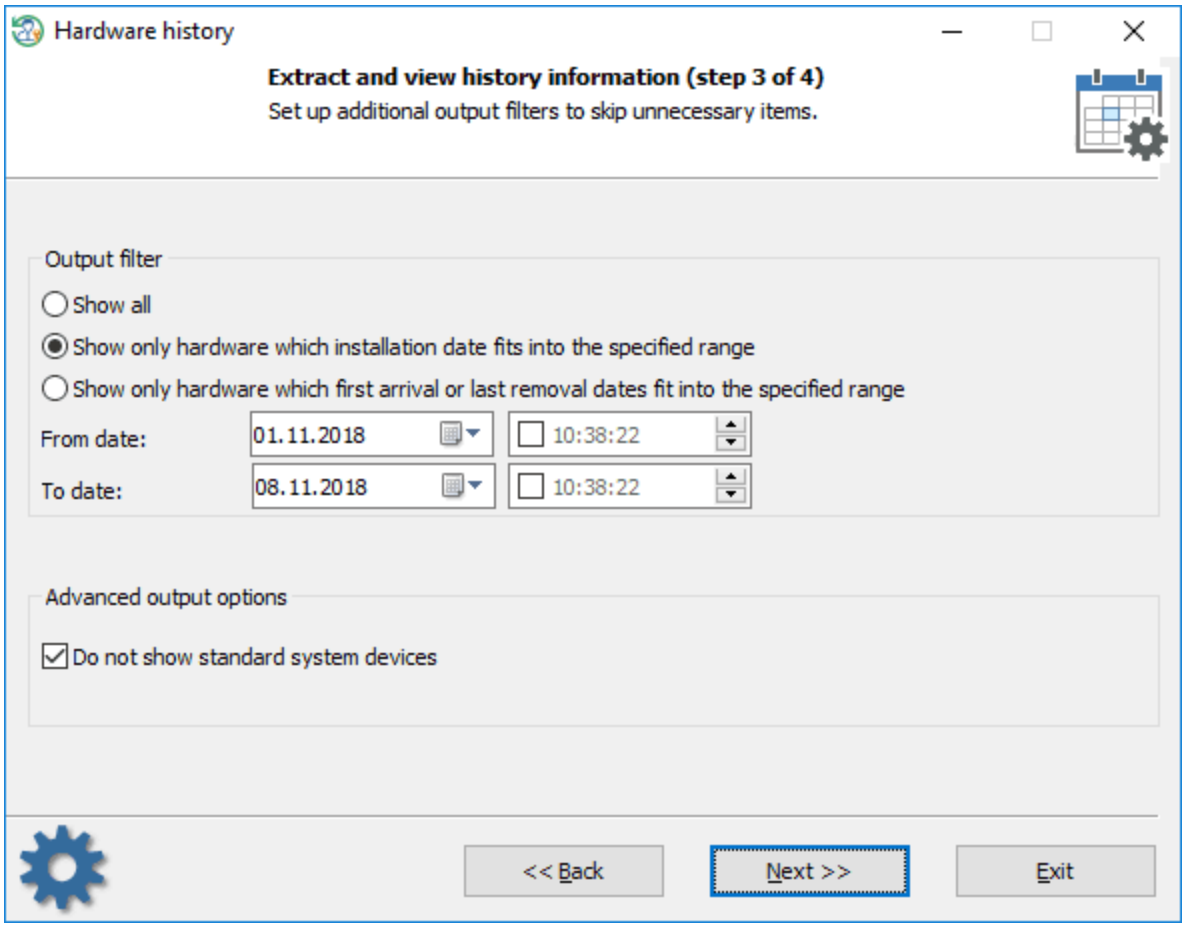
El historial de hardware enumera todo el hardware del sistema operativo de destino y lo ordena por instalación o fecha de última llegada/eliminación.

Selección del directorio de Windows



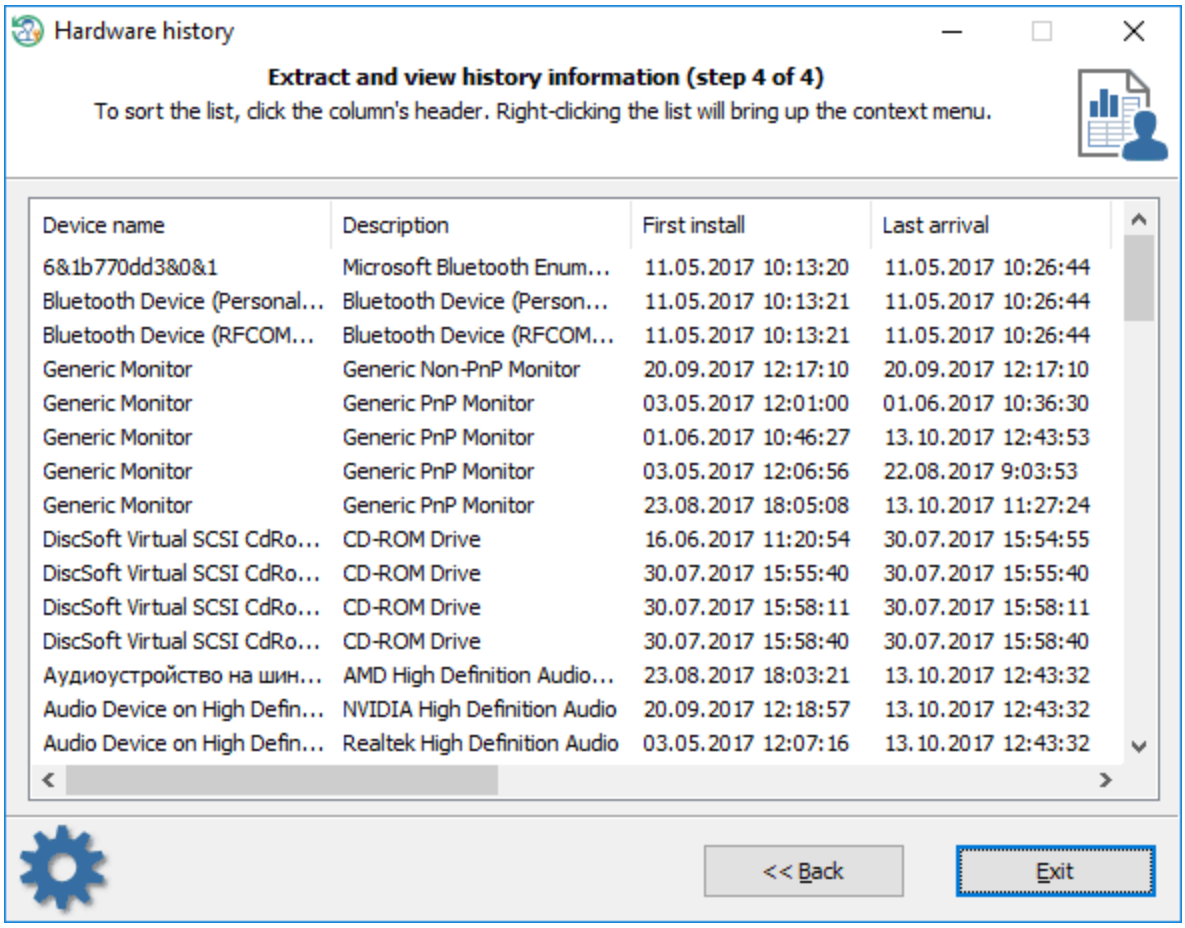
Seleccione primero la carpeta de Windows de destino. El programa suele hacerlo de forma automática.

Seleccionar filtros de salida



Configure filtros de salida adicionales para omitir elementos innecesarios. Puede configurar el programa para que muestre solo el hardware que se instaló o llegó o eliminó la última vez en la fecha especificada.

Información del historial de hardware

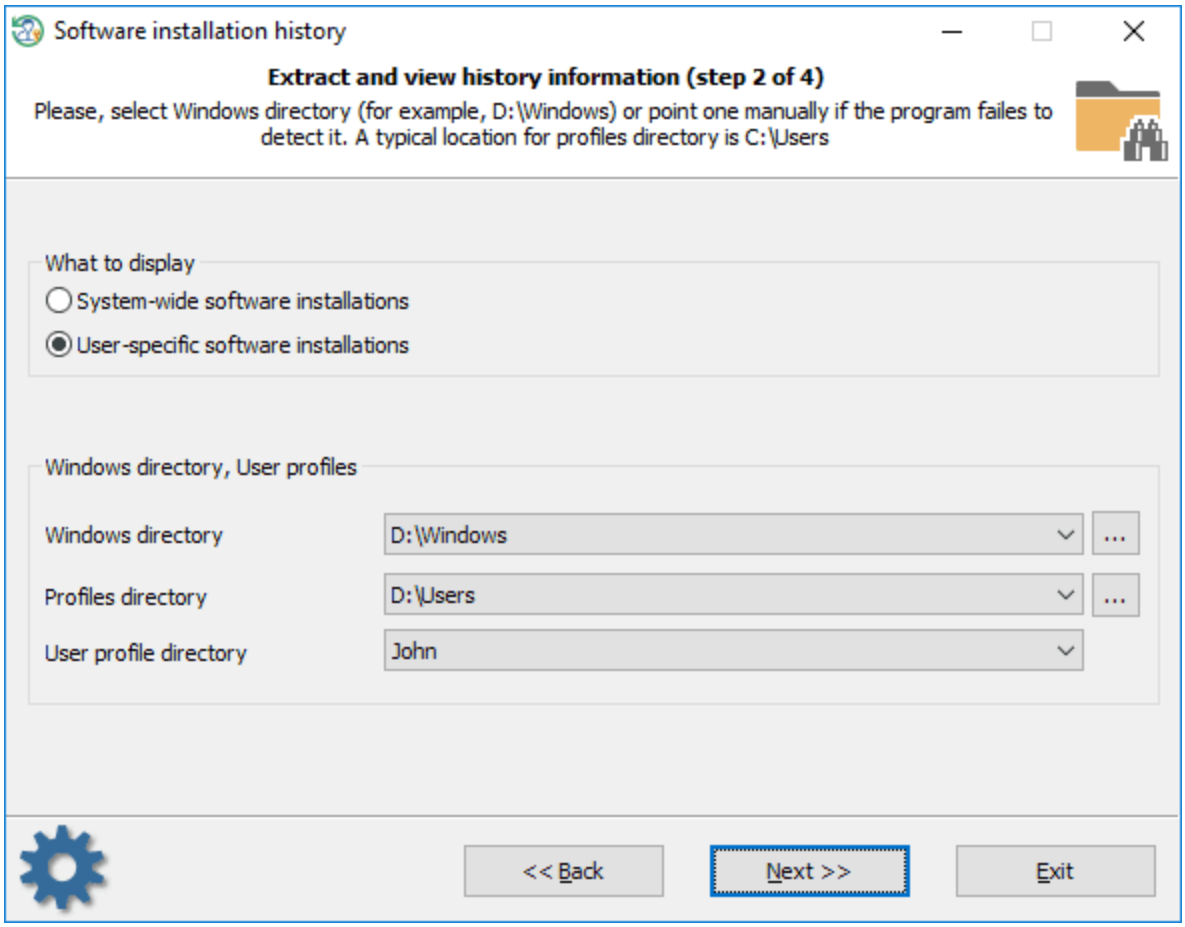


Para ordenar la lista, haga clic en una de las columnas.

3.17.3 Ver el historial de software

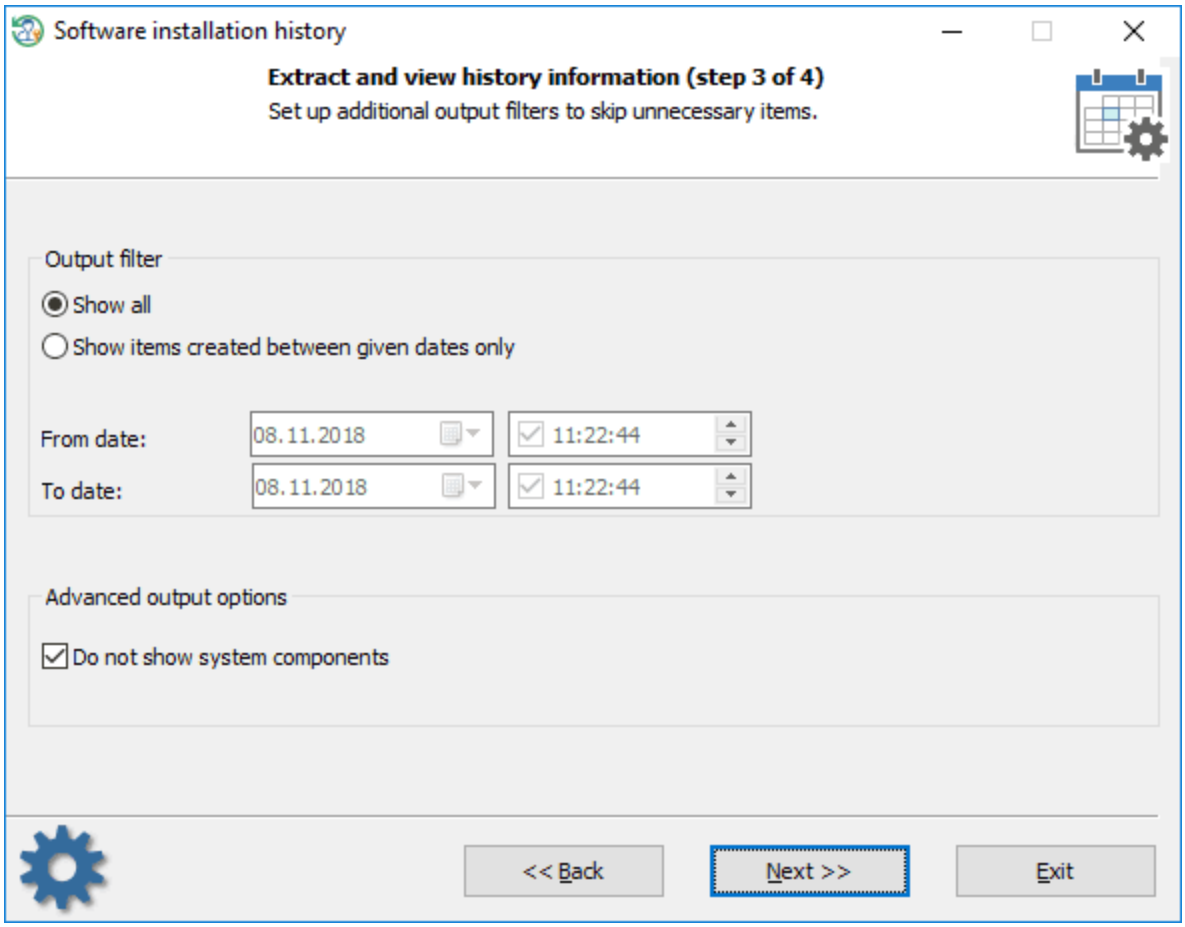
El historial de software muestra todos los programas que se instalaron en el sistema operativo de destino.

Selección de un tipo de instalaciones de software



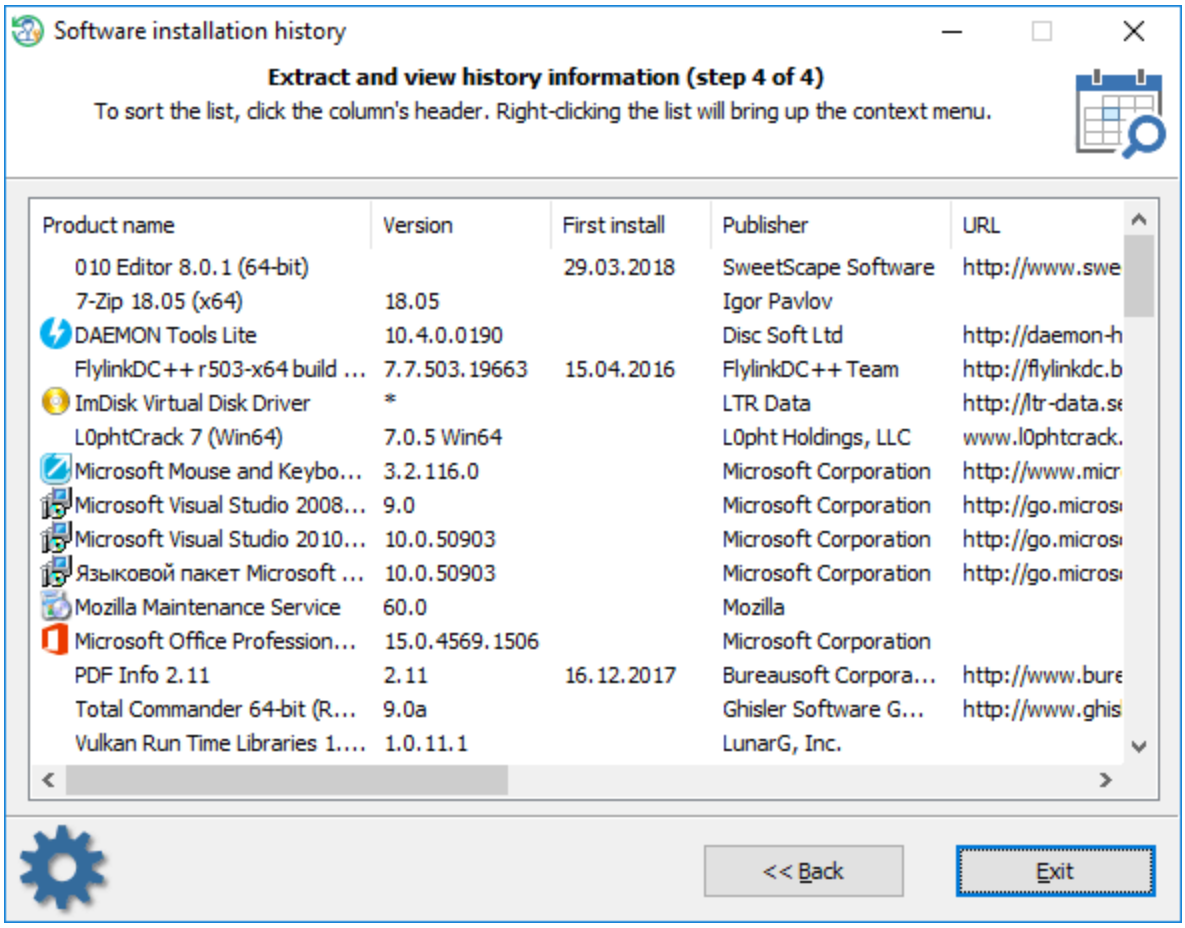
Seleccione el tipo de instalaciones de software que desea ver. Se trata de instalaciones específicas del usuario (programas instalados para una determinada cuenta de usuario) o instalaciones de todo el sistema (programas que están disponibles para todos los usuarios).

Filtros de salida



Puede apuntar al programa para que muestre todos los elementos o elementos que se crearon entre fechas dadas solamente. La opción adicional tiene como objetivo ocultar algunos componentes del sistema, como actualizaciones del sistema, etc.

Instalaciones de software

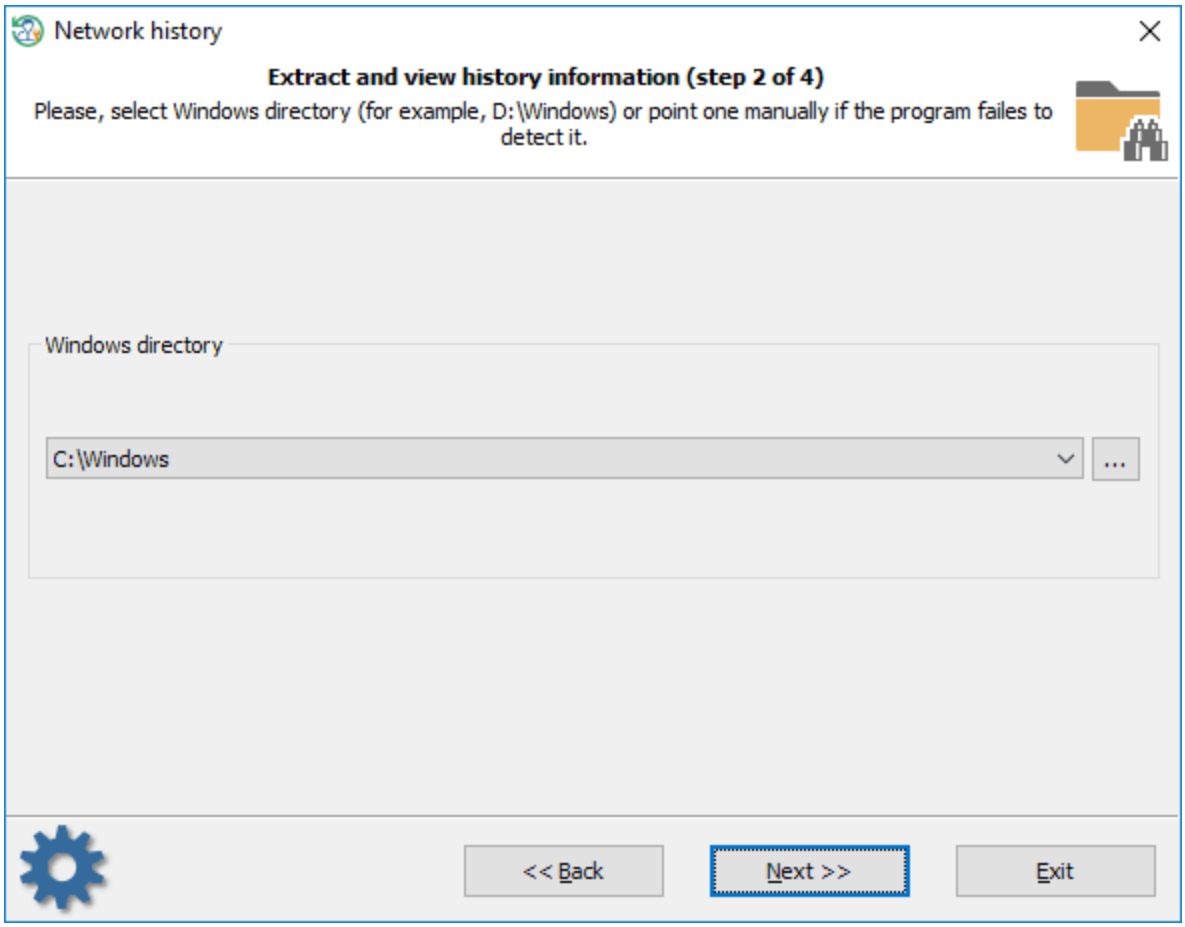


Para ordenar la lista, haga clic en una de las columnas.

3.17.4 Ver el historial de la red

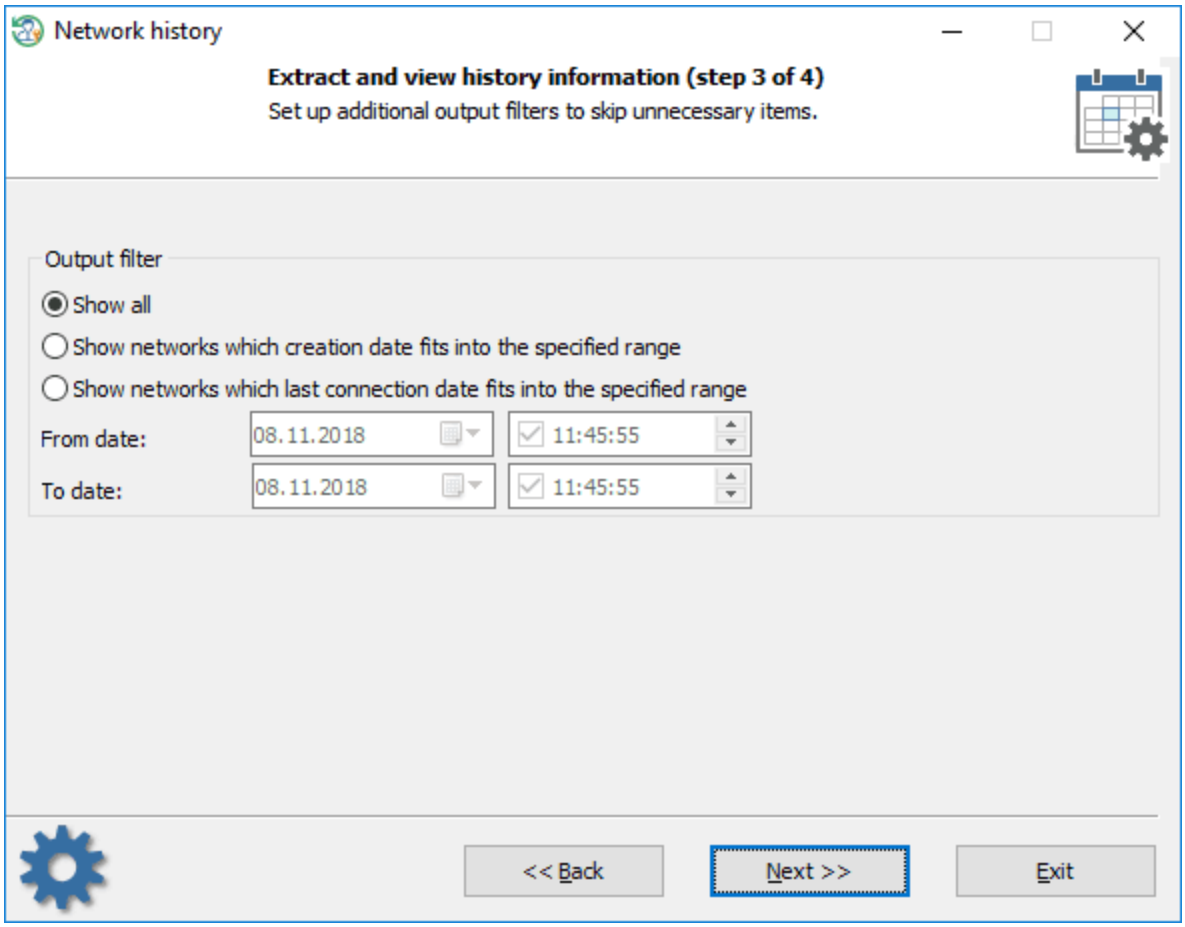
El historial de conexiones de red muestra todas las redes disponibles junto con su instalación y las fechas de última conexión.

Selección del directorio de Windows



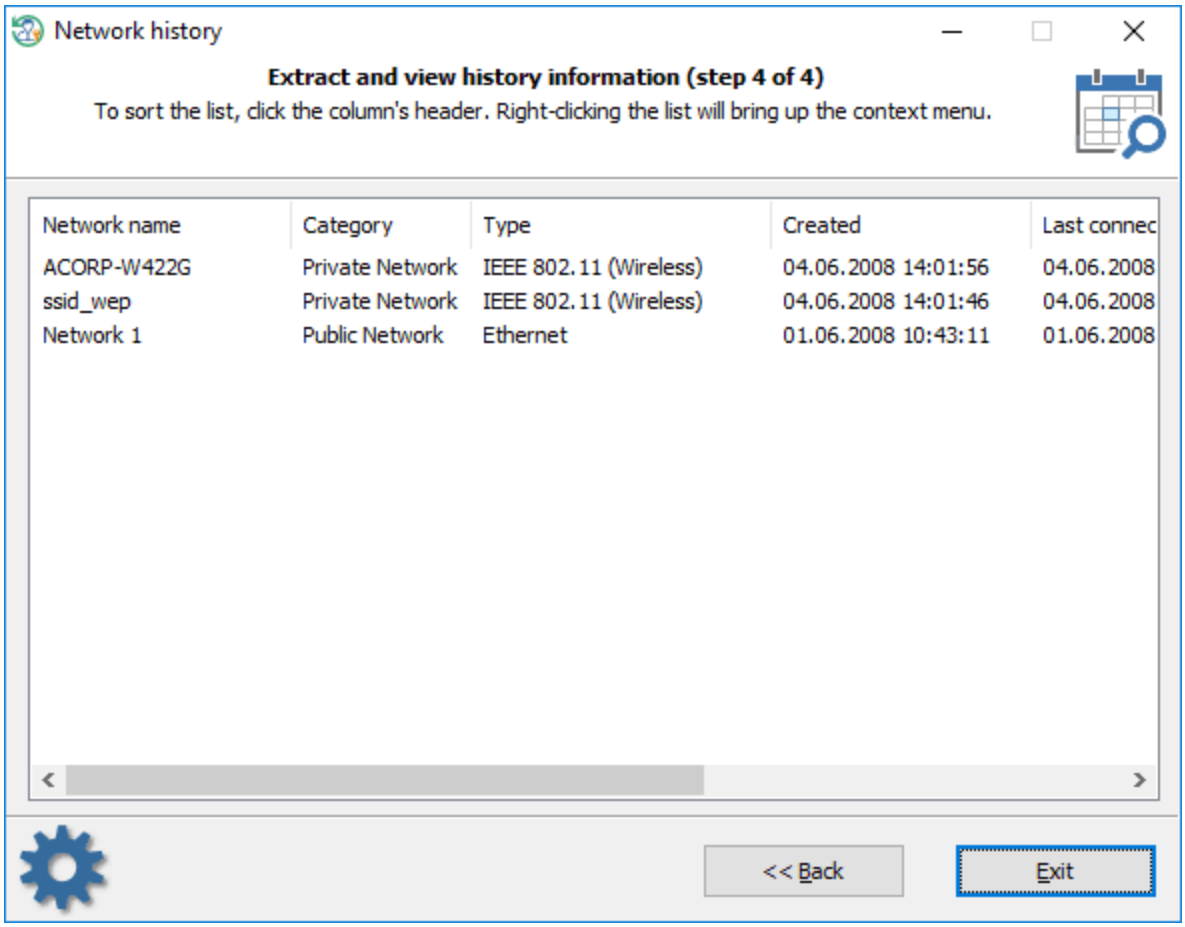
Seleccione primero la carpeta de Windows de destino. El programa debe hacerlo por usted.

Configuración de filtros de salida



Configure filtros de salida adicionales para mostrar solo las redes de su interés.

Historial de conexiones de red

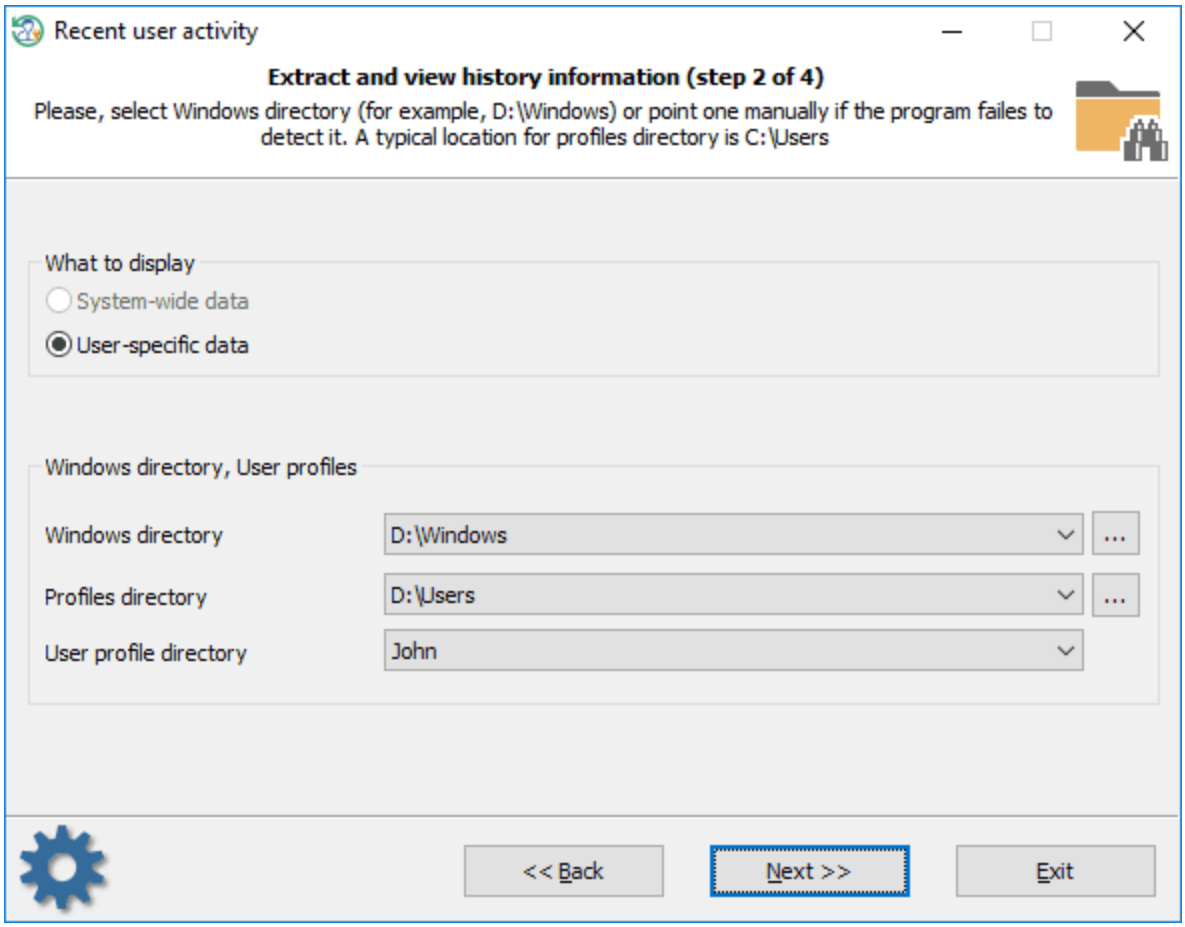


Las redes extraídas generalmente contienen la fecha en que se crearon y la última fecha de conexión. Para ordenar la lista por fechas, haga clic en una de las columnas correspondientes.

3.17.5 Ver la actividad reciente del usuario

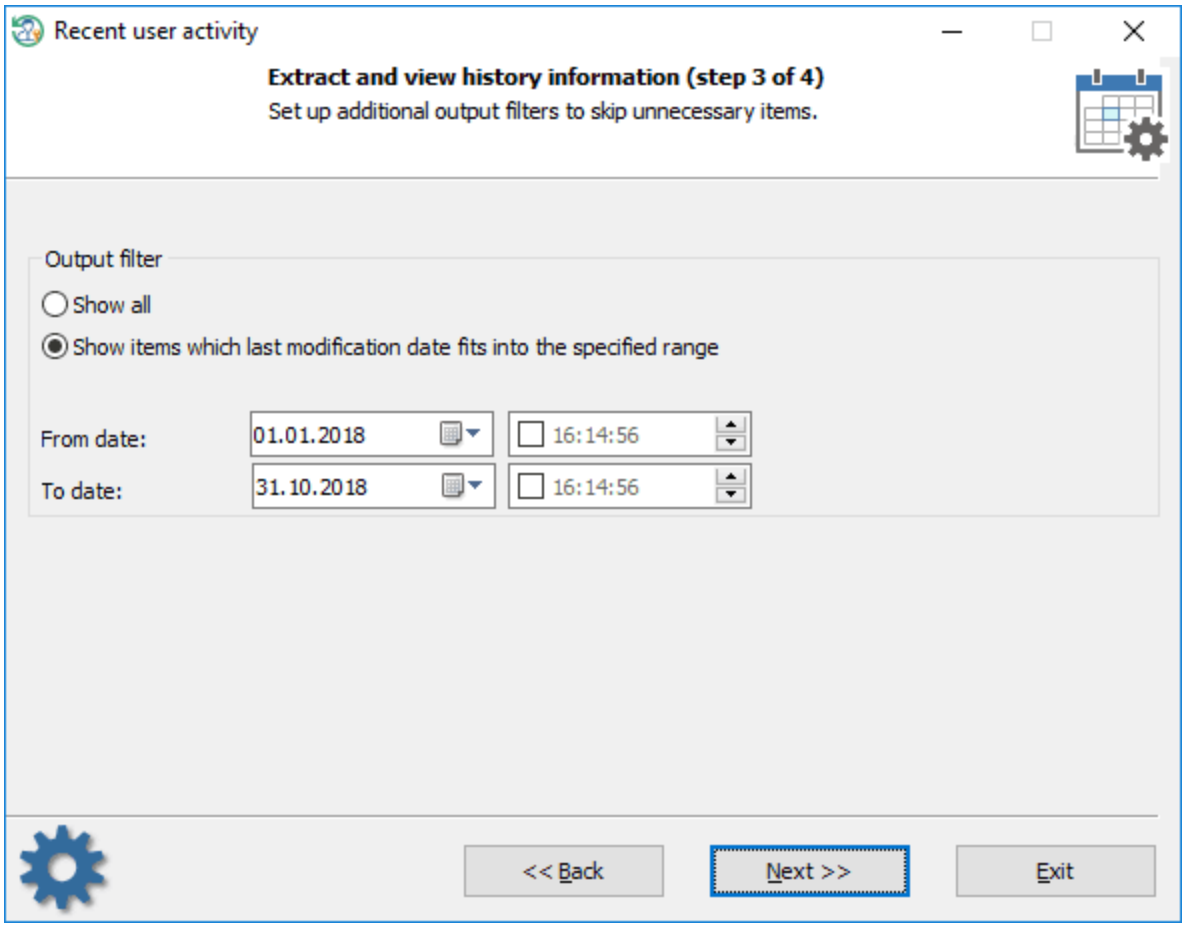
Esta herramienta recopila toda la información disponible sobre la actividad reciente del usuario ocurrida en este equipo.

Selección de un tipo de actividad



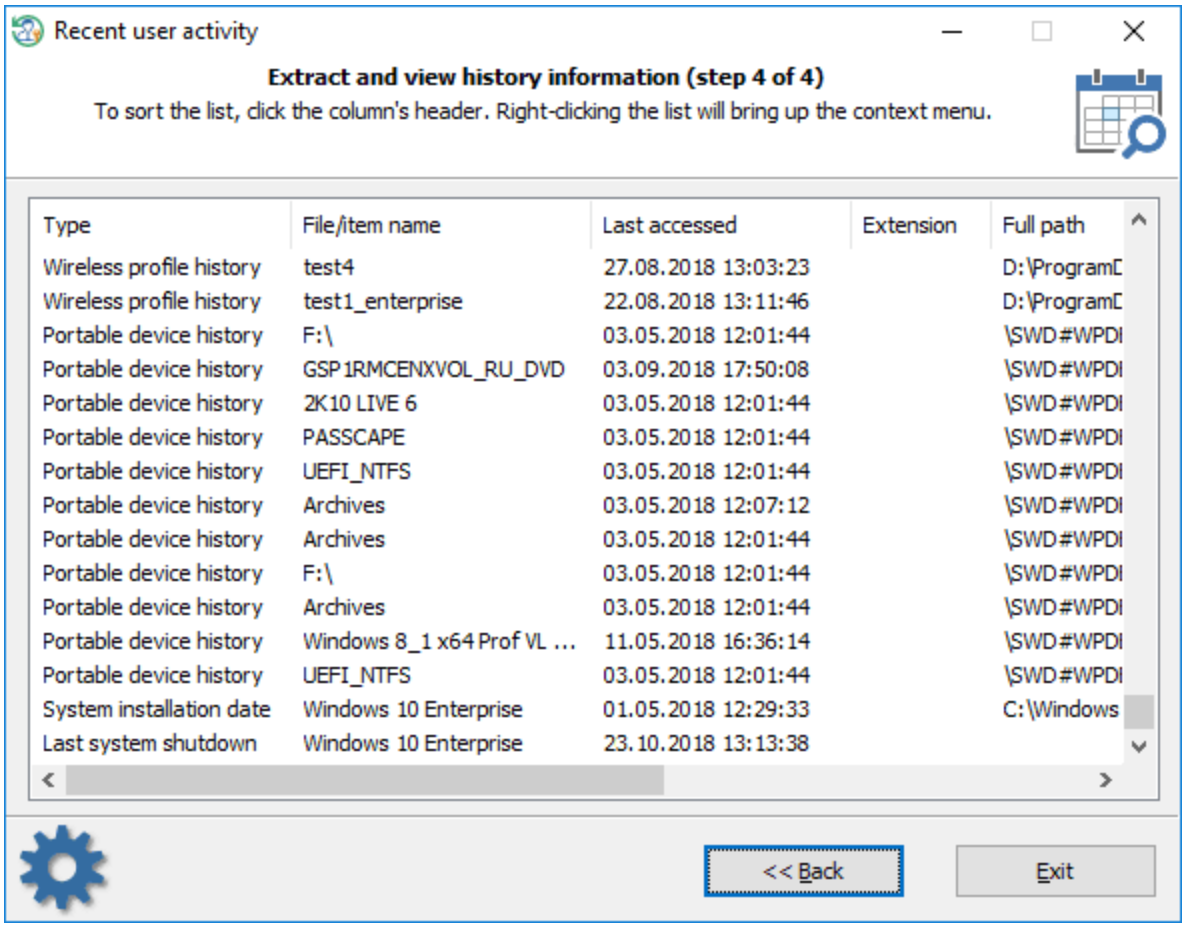
En primer lugar, seleccione si desea ver datos de todo el sistema o específicos del usuario.

Configuración de filtros de salida



A continuación, especifique si se van a mostrar todas las entradas o solo las que se ajustan a marcos de tiempo específicos.

Visualización de la actividad reciente del usuario



Sea paciente, recopilar las estadísticas puede llevar bastante tiempo.
Para ocultar registros innecesarios, haga clic con el botón derecho del ratón en la lista y seleccione el elemento de menú adecuado.

La versión actual del programa admite la siguiente información (algunos elementos no están disponibles en sistemas operativos antiguos):

- Últimos elementos de los cuadros de diálogo abrir/guardar archivos
- Elementos de ejecución de tareas
- Unidades de red asignadas
- Elementos recientes encontrados en red
- Elementos de búsqueda de archivos/carpetas recientes
- Archivos recientes de applets de Windows
- Última clave Regedit abierta
- Documentos abiertos recientemente
- Documentos de MS Office recientemente abiertos
- Cuentas y conexiones recientes de Outlook
- Aplicaciones ejecutadas recientemente
- Elementos de aplicación recientes
- Conexiones RDP recientes
- Direcciones URL de Internet Explorer
- Rutas ingresadas en explorador
- Historial de búsqueda del explorador
- Elementos de Asistencia al usuario del Explorador
- Elementos de actividad de fondo recientes

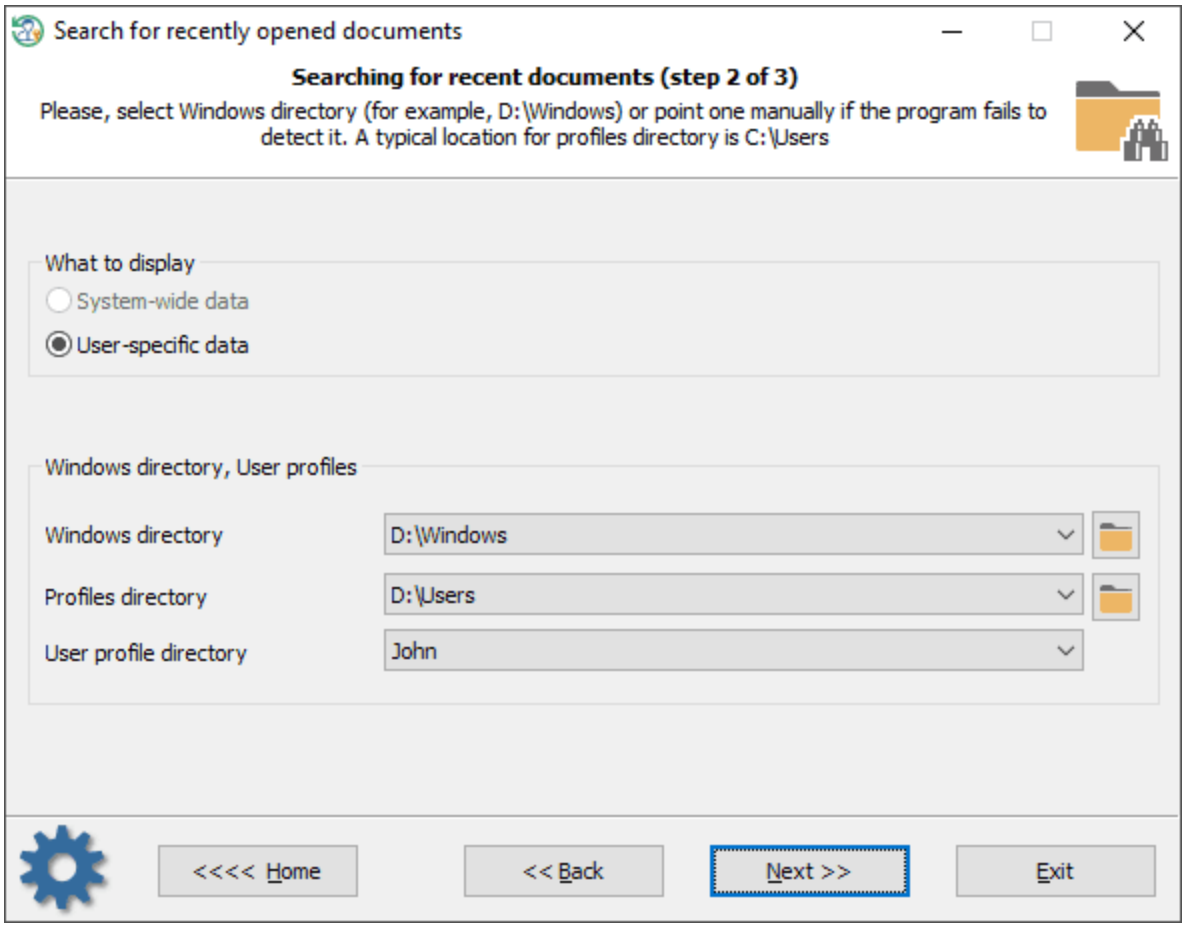
- Elementos de actividad de escritorio recientes
- Conexiones inalámbricas
- Actividad Bluetooth
- Dispositivos portátiles recientes
- Fecha de instalación de Windows
- Última fecha de apagado del sistema

3.17.6 Buscar documentos abiertos recientemente

El sistema operativo Windows realiza un seguimiento de todos los documentos abiertos y guarda los vínculos a ellos a una carpeta específica de Microsoft Windows ('Reciente') en el perfil de usuario. 'C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent' es una carpeta especial, donde Windows almacena los vínculos a documentos usados recientemente. Puede controlar el comportamiento de Windows en el menú Inicio > Configuración > Personalización > Inicio, marcando el botón de opción '*Mostrar elementos abiertos recientemente*'.

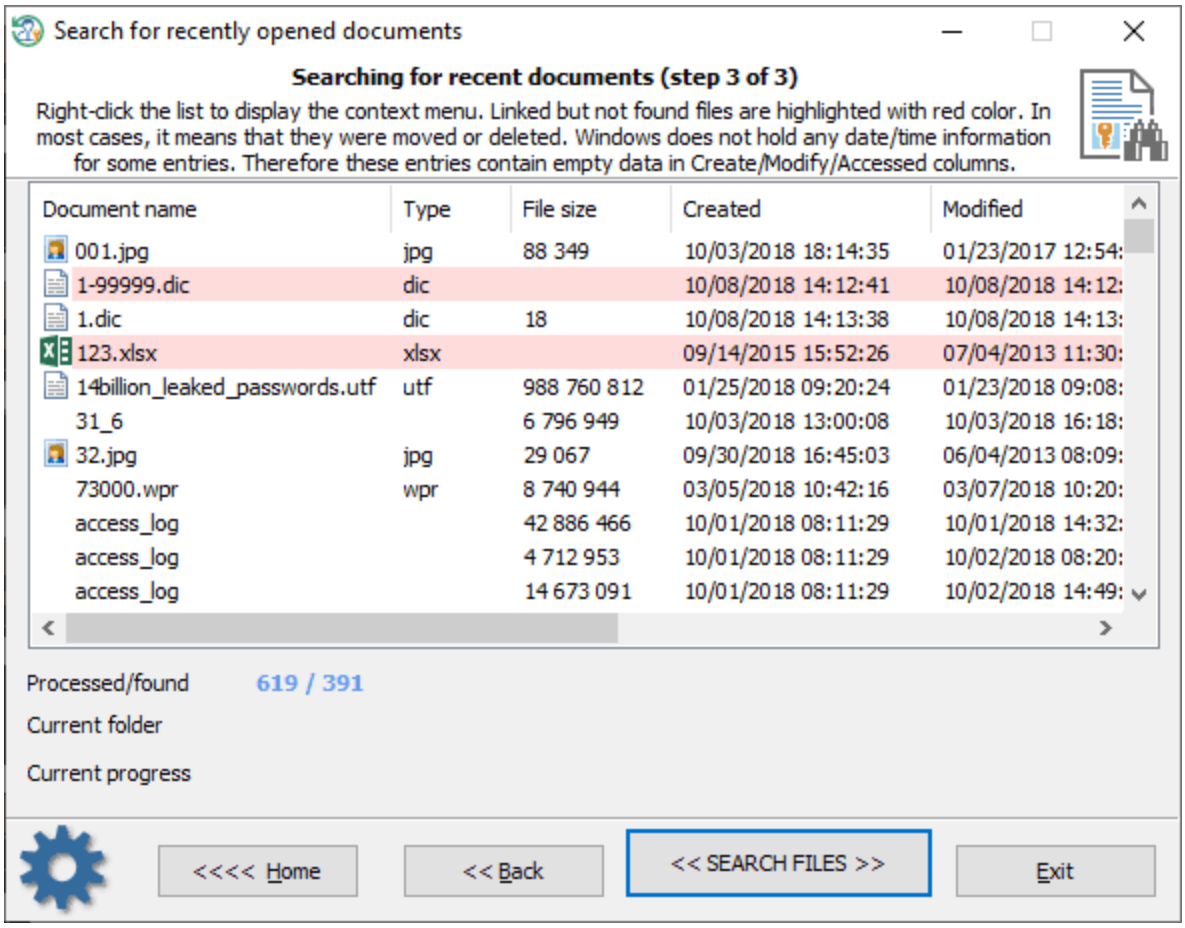
La función de este programa tiene como objetivo navegar a través de la lista de archivos recientes y ver los nombres de los archivos que se han abierto recientemente y se han guardado en la carpeta 'Reciente' de Windows.

Selección del perfil de usuario



Seleccione el perfil de usuario cuyos documentos desea analizar.

Ver documentos abiertos recientemente



Haga clic en el botón << *BUSCAR ARCHIVOS* >> y espere pacientemente hasta que el programa encuentre los últimos archivos abiertos y complete la tabla.

Para ocultar los elementos innecesarios, haga clic con el botón derecho en la lista de archivos encontrados y seleccione el menú apropiado.

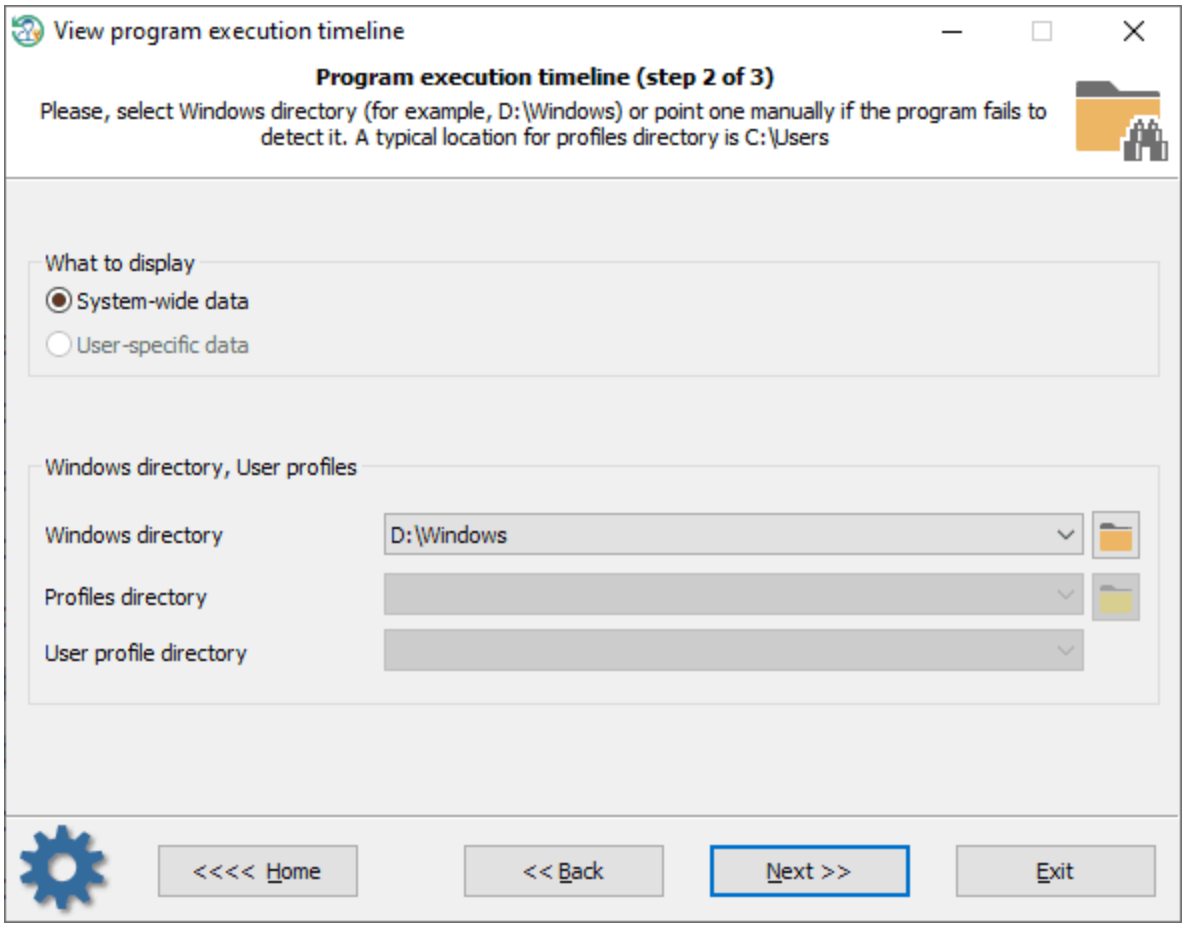
Los archivos que ya no existen (por ejemplo, se movieron o eliminaron) pero que aún tienen enlaces a ellos están marcados con color rojo.

3.17.7 Ver cronograma de ejecución del programa

No sería una gran sorpresa saber que hay muchos artefactos que contienen información sobre documentos abiertos recientemente o archivos lanzados en Windows. El AmCache es uno de ellos que almacena datos sobre cada programa que se ha iniciado o instalado en el sistema anteriormente. El AmCache está disponible a partir de Windows 7. Los sistemas operativos más antiguos utilizan un formato BCF para guardar datos sobre los programas ejecutados. Físicamente, ambos formatos son archivos simples ubicados en la carpeta %WINDIR%\appcompat\Programs. AmCache.hve es un subárbol de registro que proporciona una línea de tiempo de qué programa se ejecutó y cuándo, mientras que RecentFileCache.bcf significa un archivo de caché binario simple.

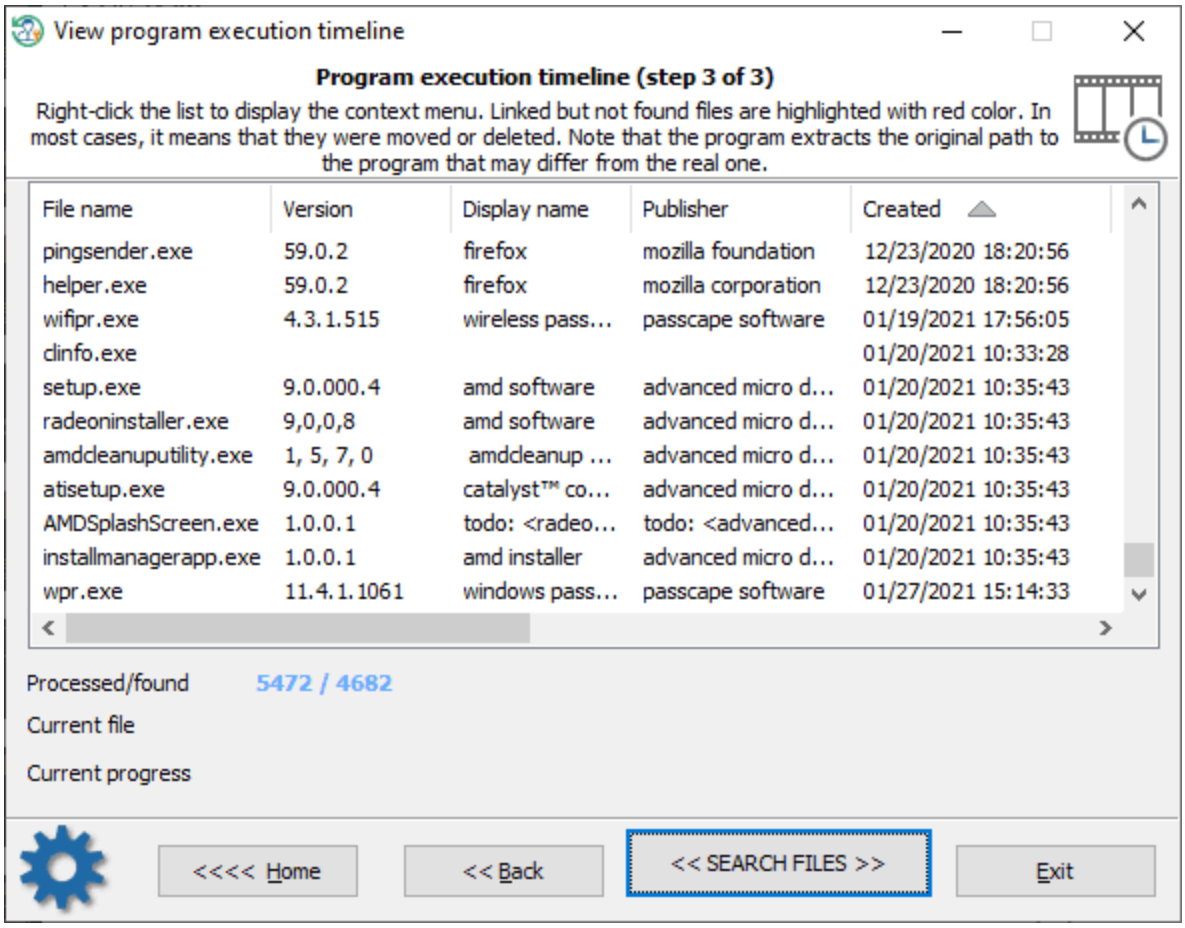
El programa admite ambos formatos, sin embargo, el antiguo formato BCF no contiene información sobre el tiempo de ejecución.

Elegir el directorio de Windows



Seleccione el directorio de Windows detectado por el programa.

Ver cronograma de ejecución del programa



Ahora es el momento de presionar el botón << *SEARCH FILES* >> y espere a que el programa localice los archivos para rellenar la tabla.

Para borrar cualquier archivo innecesario de la lista de elementos encontrados, haga clic con el botón derecho en la lista y seleccione el menú apropiado.

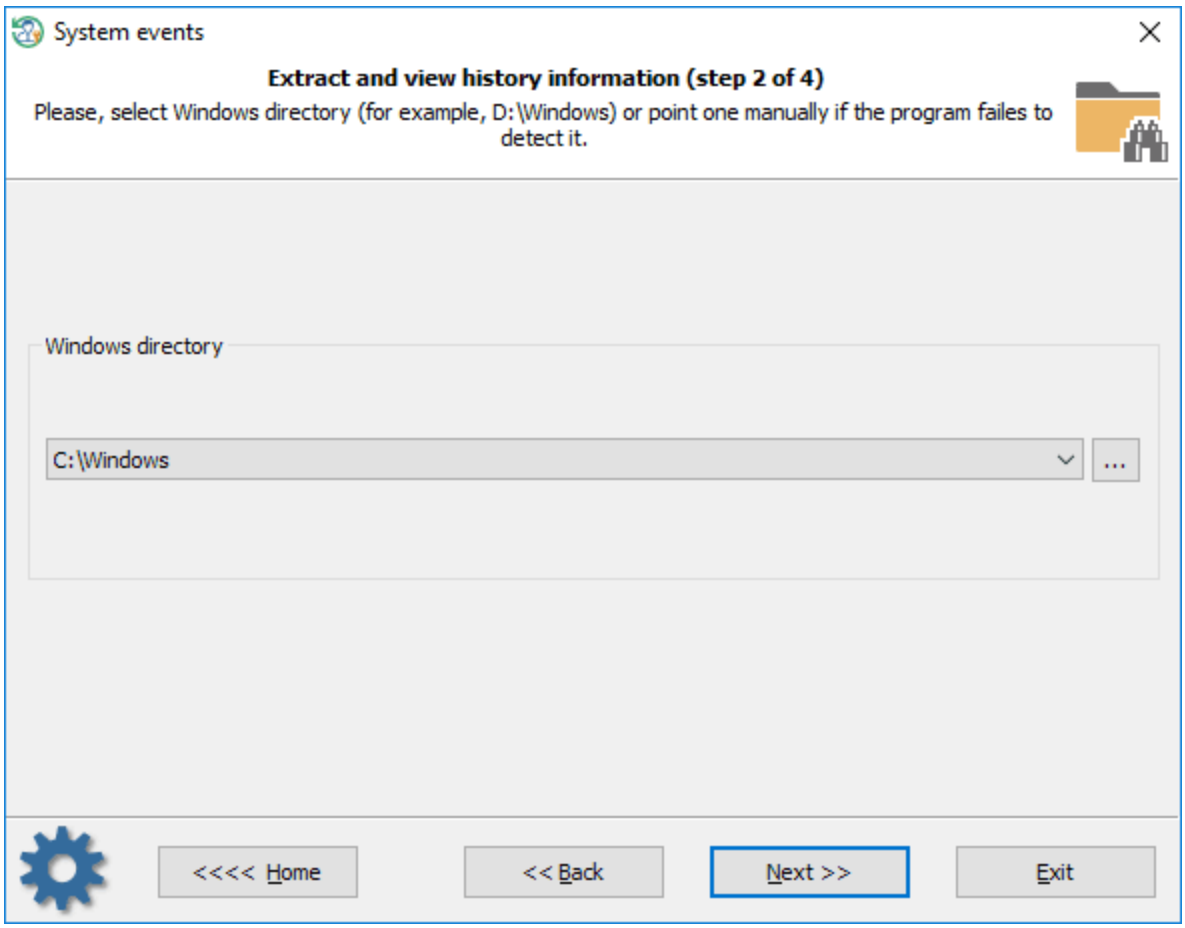
Si el programa no puede localizar los archivos a los que Windows enlaza desde la base de datos amCache, marca los archivos con color rojo.

3.17.8 Ver eventos del sistema

Todos los sistemas operativos Windows registran varios tipos de eventos que ocurren en el sistema de vez en cuando: errores en las instalaciones de dispositivos o controladores, fallas de aplicaciones, notificaciones de seguridad, etc. Los eventos ayudan a los usuarios y administradores a eliminar errores, realizar diagnósticos y monitorear el sistema, mantener su seguridad. Los eventos se almacenan en archivos *.evtx y se registran en orden cronológico. Cada archivo evtx corresponde a un origen de eventos específico o a un componente del sistema operativo. Por ejemplo, system.evtx realiza un seguimiento de las notificaciones comunes del sistema. Security.evtx contiene todos los eventos de seguridad. Y así sucesivamente.

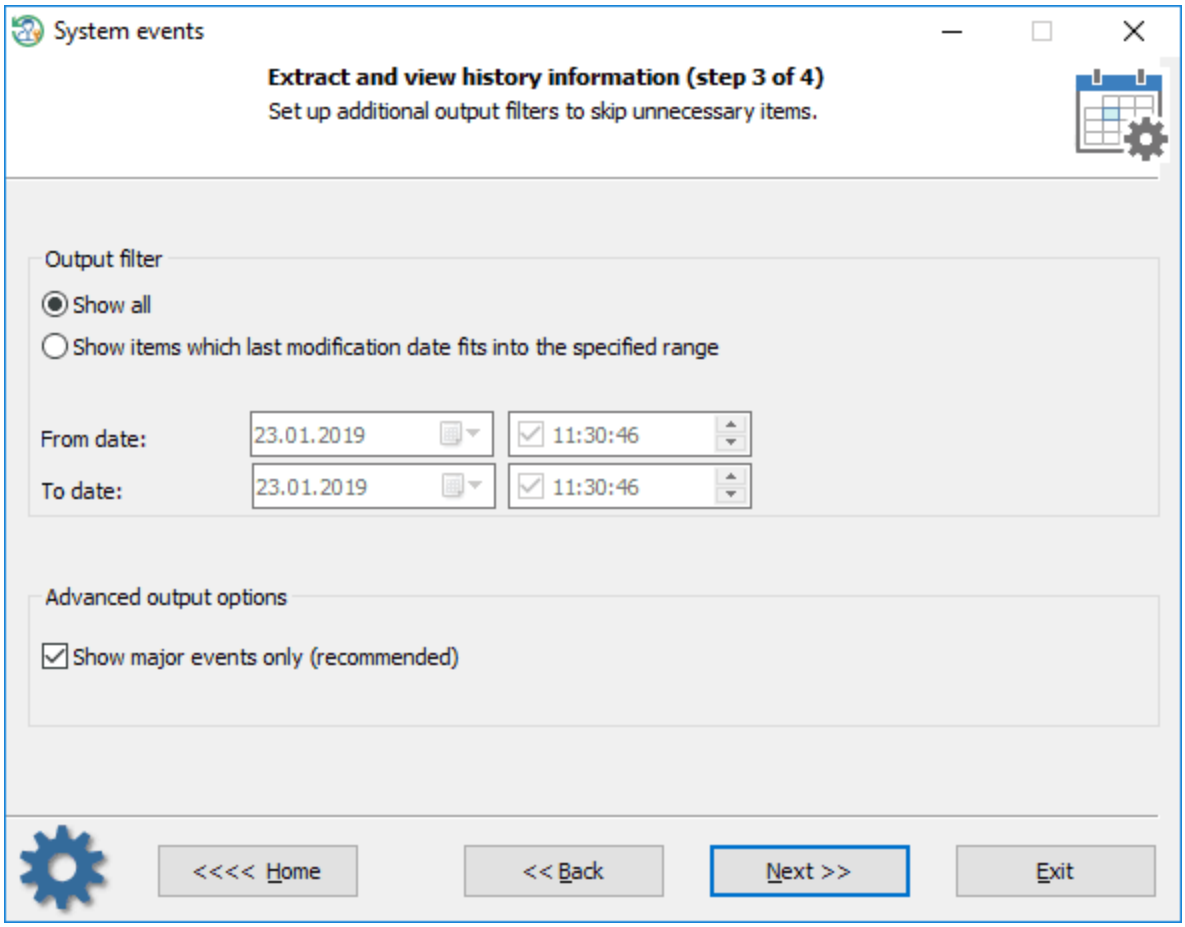
El visor de eventos del sistema es una herramienta simple que permite mostrar eventos importantes que ocurren en Windows Vista y sistemas operativos posteriores. Por ejemplo, iniciar o apagar el sistema, iniciar / desactivar cuentas de usuario, instalación de controladores, etc..

Selección del directorio de Windows



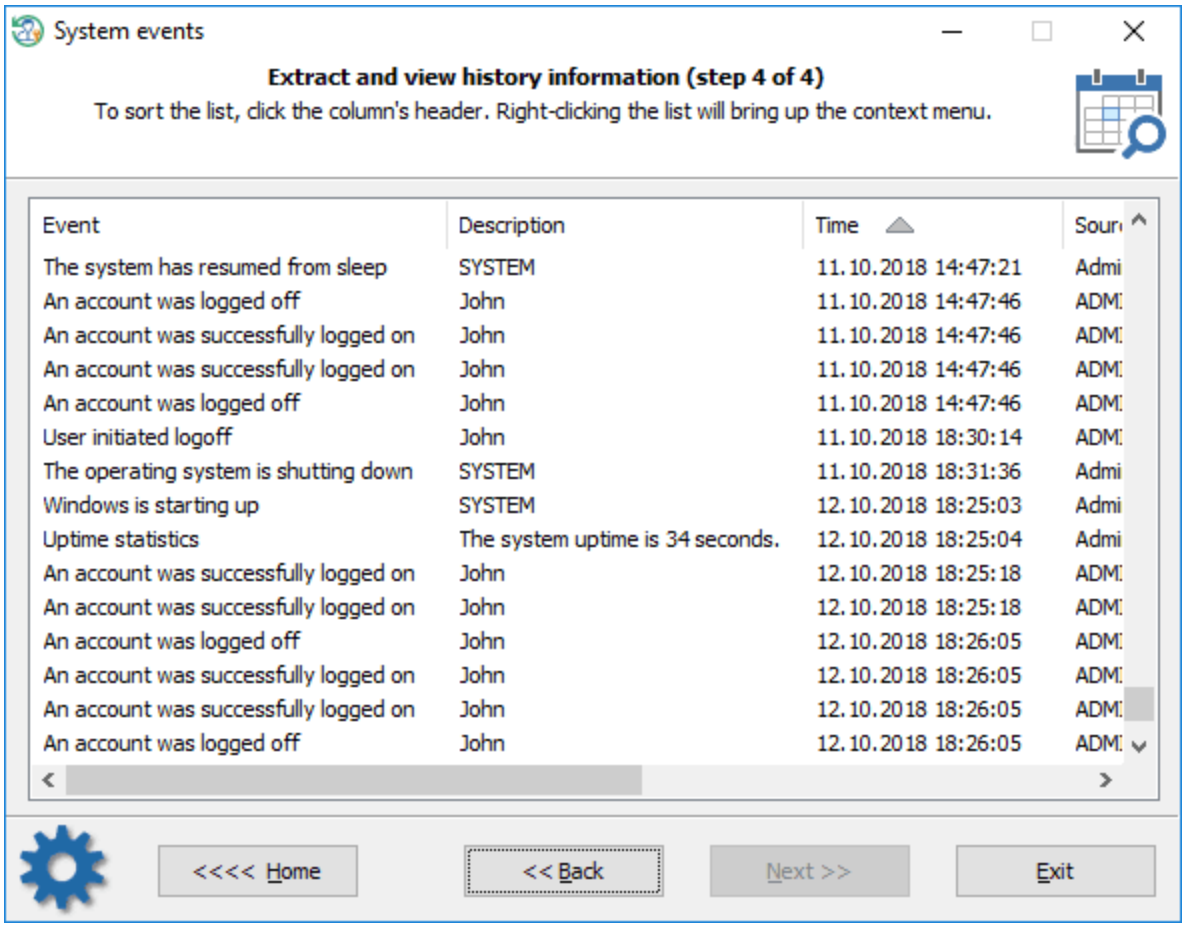
En primer lugar, debe seleccionar el directorio de Windows que contiene los registros de eventos. Típicamente, C:\Windows o D:\Windows.

Configuración de filtros de salida



En el siguiente paso, también puede configurar filtros de salida para mostrar eventos que ocurrieron en un tiempo específico. También hay una opción para mostrar todos los eventos (incluso desconocidos para el programa). Si se establece la opción, el programa solo genera eventos conocidos/principales, todos los eventos de lo contrario.

Visualización de eventos de Windows

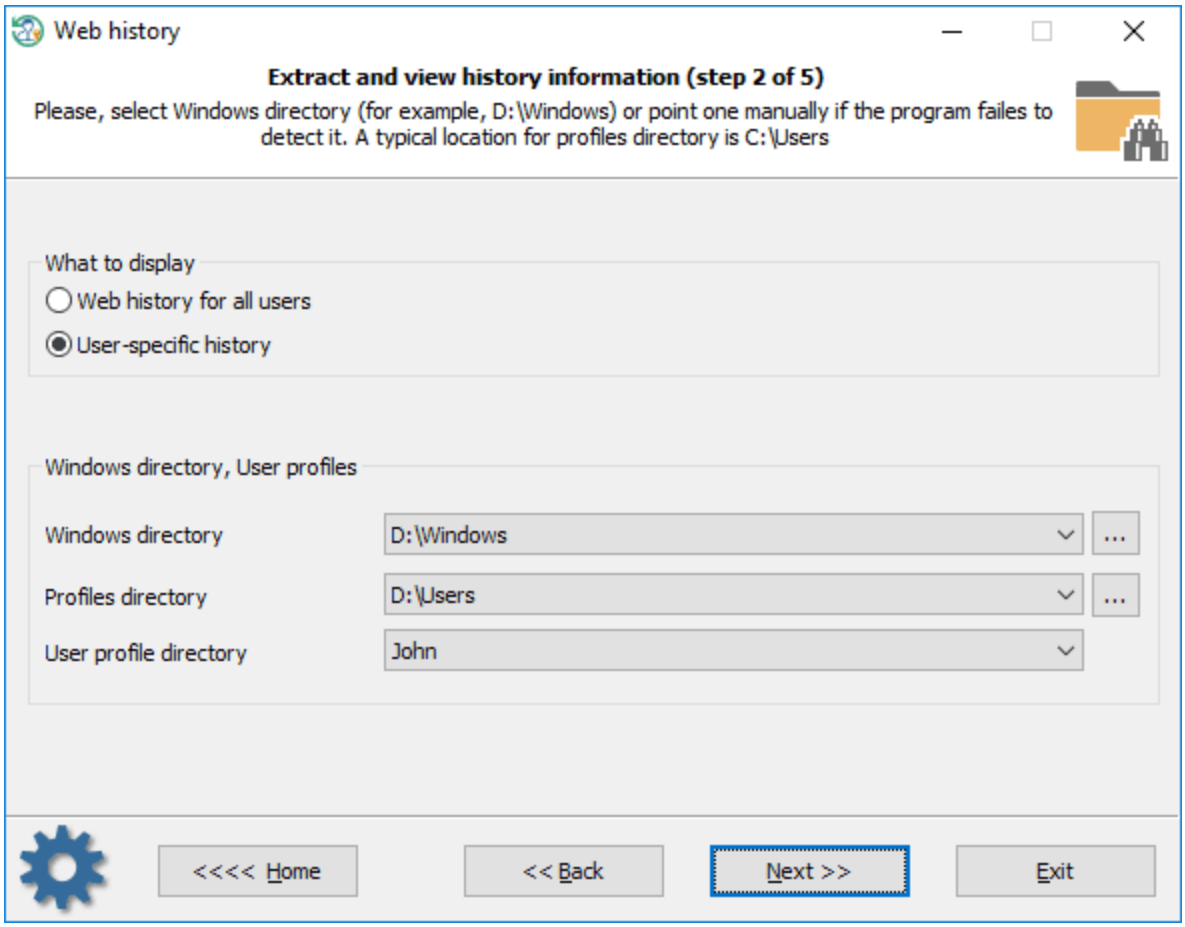


La recopilación y el procesamiento de la información pueden llevar un tiempo considerable, dependiendo del tamaño de los archivos *.evtx del sistema de destino. Para ocultar algunos registros que no le interesan, haga clic con el botón derecho en la lista de eventos y seleccione uno de los elementos de menú correspondientes. Para ordenar la lista, haga clic en uno de sus encabezados.

3.17.9 Ver historial web

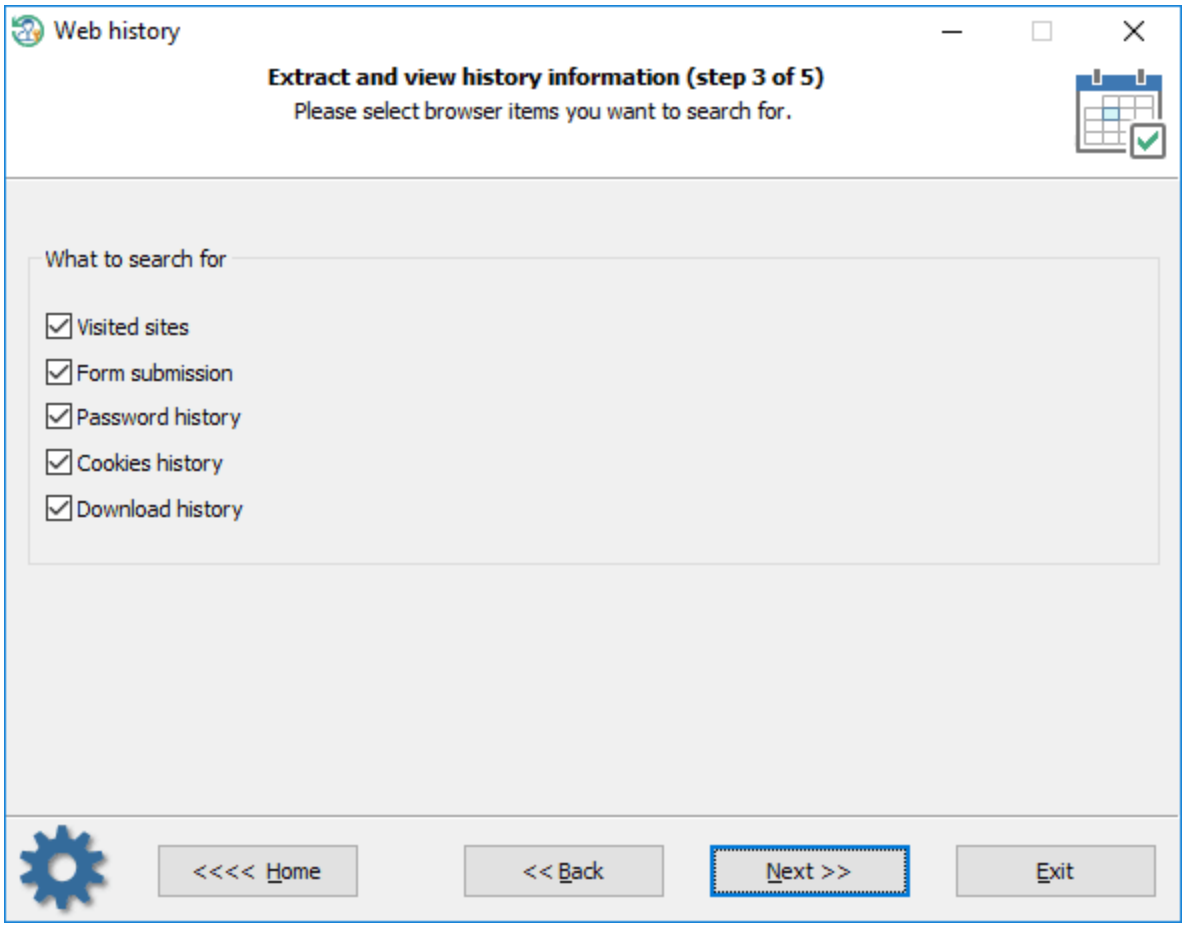
El historial web le permite extraer y recopilar estadísticas de páginas web visitadas, cookies guardadas, datos de autocompletado de formularios almacenados y contraseñas guardadas. El programa es compatible con todos los navegadores populares: Internet Explorer, Edge, Opera, navegadores basados en el código fuente de Mozilla (Firefox, SeaMonkey, etc.), Chromium (Google Chrome, YandexBrowser, 360 Extreme Explorer, etc.)

Selección del origen de datos



Inicialmente, RWP ofrece seleccionar el origen de datos donde buscar. Este es el perfil de un usuario específico o perfiles para todos los usuarios.

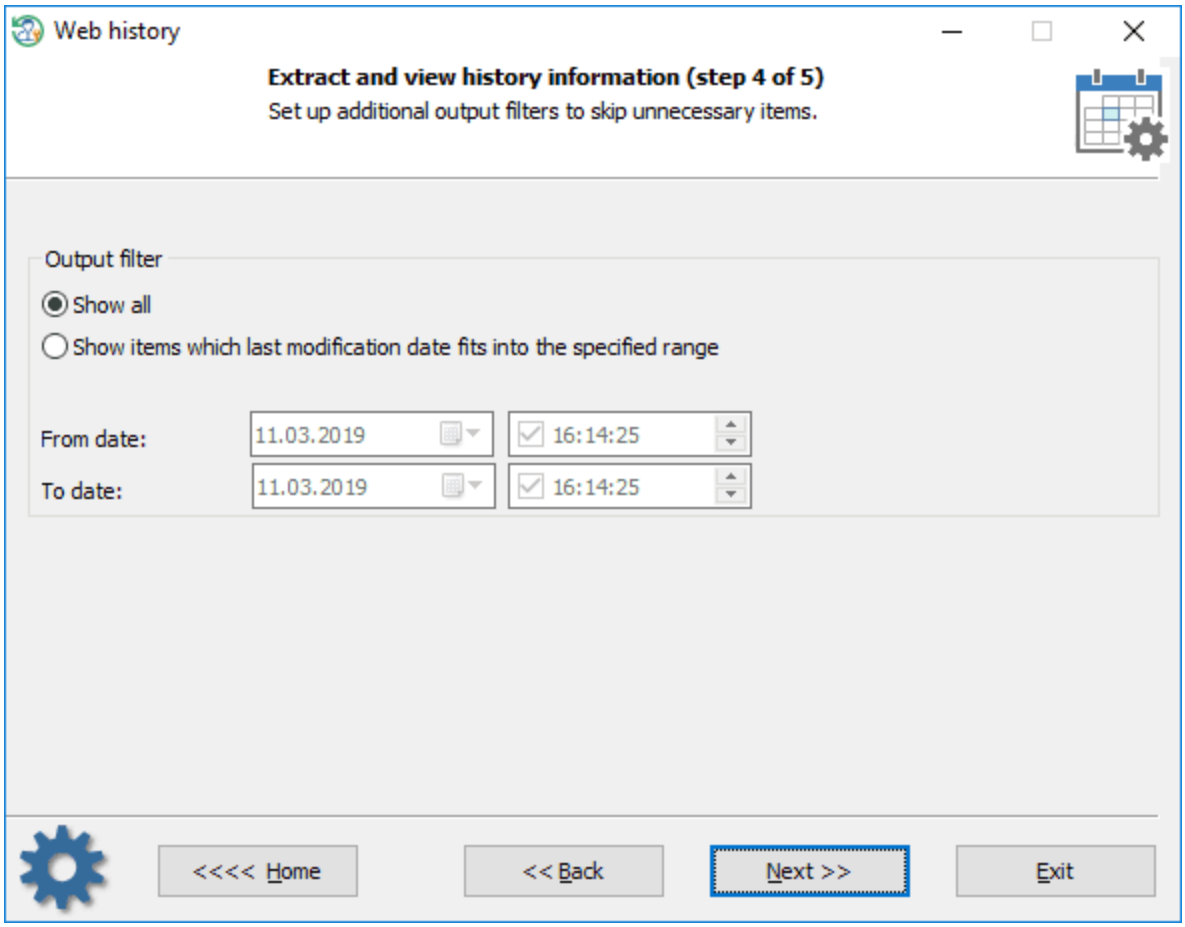
Qué buscar



De forma predeterminada, el programa intenta buscar los siguientes elementos, puede activar / desactivar cada uno de ellos por separado:

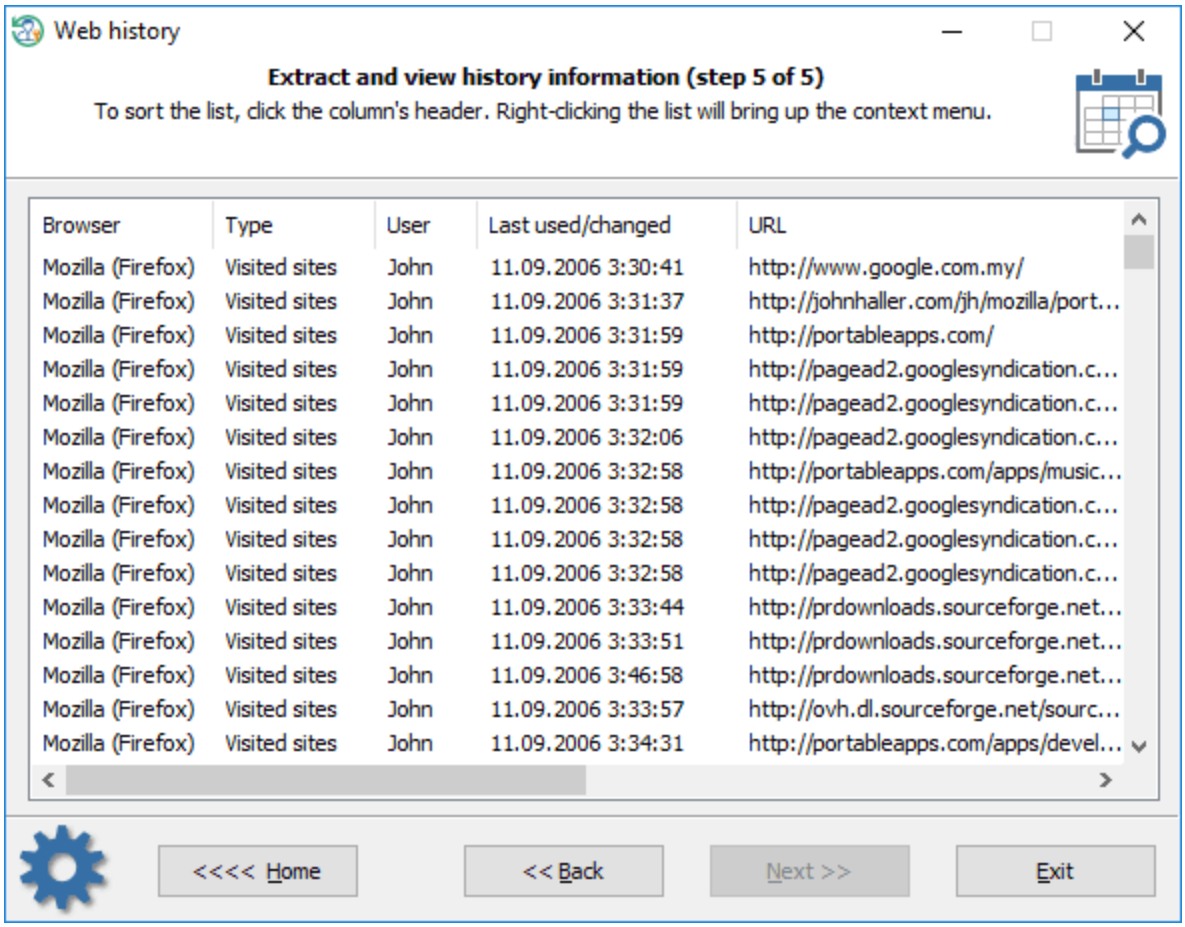
- La lista de URL visitadas
- Datos de autocompletado de formularios
- Nombres de inicio de sesión y contraseñas (si solo se pueden descifrar al instante)
- Galletas. Se puede utilizar para determinar qué sitios se visitaron y cuándo, si el usuario inició sesión, etc.
- Historial de descargas. Tenga en cuenta que no todos los navegadores mantienen esta información

Configuración de filtros de tiempo



Puede configurar un filtro de tiempo adicional para omitir elementos obsoletos o innecesarios.

Historial web



Las estadísticas se pueden copiar en el portapapeles o guardar en un archivo. Usando el menú contextual, también puede ocultar algunos elementos que no son de su interés.

¿Dónde almacenan los navegadores sus listas de URL visitadas?

Internet Explorer
Los lugares visitados se almacenan en el archivo index.dat. El índice.dat contiene diferentes registros: URL visitadas y archivos locales, accesos al correo web, cookies, etc. El archivo de base de datos tiene su propio formato (Client UrlCache MMF) y se introdujo por primera vez en Internet Explorer 5. El formato del archivo index.dat no se cambió mucho desde ese momento, la ubicación física, sin embargo, puede variar:
C:\Users\<USERNAME>\AppData\Local\Microsoft\History
C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\History
C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Internet Explorer\UserData
Los sistemas operativos más antiguos utilizan diferentes rutas para mantener el archivo.

Internet Explorer: direcciones escritas
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

Microsoft Edge

Al igual que Internet Explorer, Microsoft Edge mantiene el historial de la navegación web, caché, cookies, junto con otra información en un solo archivo llamado WebCacheV01.dat que parece ser el sucesor del índice.dat. El .dat WebCacheV01 se encuentra en la siguiente ruta de acceso:
C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\WebCache

Opera (versiones anteriores)
El historial del navegador se mantiene en archivos global_history.dat, global.dat, vlink4.dat en el perfil actual de Opera. Los archivos tienen un formato diferente (depende de la versión del navegador).

Chrome (junto con navegadores basados en Chromium)
Todas las URL visitadas se mantienen en la base de datos SQLite llamada historial. La ubicación del historial es diferente y depende del navegador. Por ejemplo:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (junto con navegadores basados en Mozilla)
Se trata de un archivo de historial.dat (un formato mork) o un archivo places.sqlite en versiones más recientes. Una ubicación típica es C:
\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles. Por ejemplo:
C:\Users\<USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default

¿Dónde almacenan los navegadores los datos de autocompletado de formularios?

Internet Explorer
Internet Explorer v4-6 mantiene los datos de autocompletado en una ubicación especial del registro de usuarios denominada almacenamiento protegido. Aunque está cifrado, es fácil de descifrar y ver porque las claves de descifrado se almacenan junto con los datos cifrados. La ubicación del registro del proveedor de almacenamiento:
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Internet Explorer v7-9 utiliza una técnica diferente e interesante. En lugar de cifrar los datos confidenciales del usuario con una clave secreta estática (IE 4-6) que se puede averiguar fácilmente, IE 7-9 utiliza la dirección URL de origen como clave de cifrado para proteger los datos. Por lo tanto, sin conocer la página web a la que pertenecen ciertos datos, no podrá descifrar los datos. Más detalles se pueden encontrar aquí. RWP no admite la extracción de datos de autocompletado de formularios de IE 7-9. Utilice nuestro PIEPR para eso. Aquí está la ubicación del registro donde se almacenan los datos cifrados:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\FormData

Internet Explorer v10+ y Microsoft Edge tienen una protección aún mejor. Todas las entradas de datos se guardan en Archivos de Bóveda de Windows y protegidos con DPAPI. No hay posibilidad de descifrarlo a menos que proporcione la contraseña de inicio de sesión del propietario y el archivo de clave maestra.
Una parte difícil es que RWP puede descifrar los datos / contraseñas instantáneamente si el navegador los ha guardado en la cuenta del sistema. La ubicación del almacén para los datos de usuario:
C:\Users\<USERNAME>\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Opera (versiones anteriores)
Los datos de autocompletado del formulario se pueden encontrar en los siguientes archivos:
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\typed_history.xml
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\search_field_history.dat

Chrome (y navegadores basados en Chromium)
Los datos de envío del formulario se guardan en el historial y en los archivos de datos web, ambos tienen formato SQLite. Una ubicación típica para el navegador Chrome es:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default

Firefox (y navegadores basados en Mozilla)
Se trata de un archivo formhistory.dat (versiones anteriores del explorador) o un archivo formhistory.sqlite. Una ubicación típica es C:
\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles. Así:
C:\Users\<USERNAME>\AppData\Roaming\Mozilla\Firefox\Profiles\owec6tnk.default\formhistory.sqlite

¿Dónde almacenan los navegadores sus contraseñas?

Internet Explorer
Internet Explorer v4-6 mantiene las contraseñas web en el almacenamiento protegido.
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Las contraseñas de Internet Explorer v7-9 se guardan en la siguiente clave del Registro:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

Ubicación predeterminada de Internet Explorer v10 para las contraseñas guardadas:
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

Algunas versiones de IE también pueden guardar contraseñas de autenticación básica HTTP en el 'Almacén de credenciales' (Windows Vista y sistemas operativos superiores). El DPAPI se utiliza para proteger las entradas allí.
C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Credentials

El programa es lo suficientemente inteligente como para extraer algunos datos adicionales almacenados en otras ubicaciones. Por ejemplo, Reset Windows Password puede analizar las bases de datos de Chrome para buscar elementos de Internet Explorer que se guardan allí después de la migración de datos.

Opera (versiones anteriores)
Todas las contraseñas se almacenan en un archivo wand.dat en forma cifrada junto con las claves de descifrado. Las contraseñas se pueden descifrar fácilmente a menos que se establezca una contraseña maestra.
C:\Users\<USERNAME>\AppData\Roaming\Opera\Profile\wand.dat

Chrome (y navegadores basados en Chromium)
Los navegadores basados en Chromium protegen las contraseñas de usuario con DPAPI en Windows y las almacenan en el archivo de datos de inicio de sesión, que en realidad es una base de datos SQLite. Una ubicación de base de datos típica para Google Chrome:
C:\Users\<USERNAME>\AppData\Local\Google\Chrome\User Data\Default\Login data

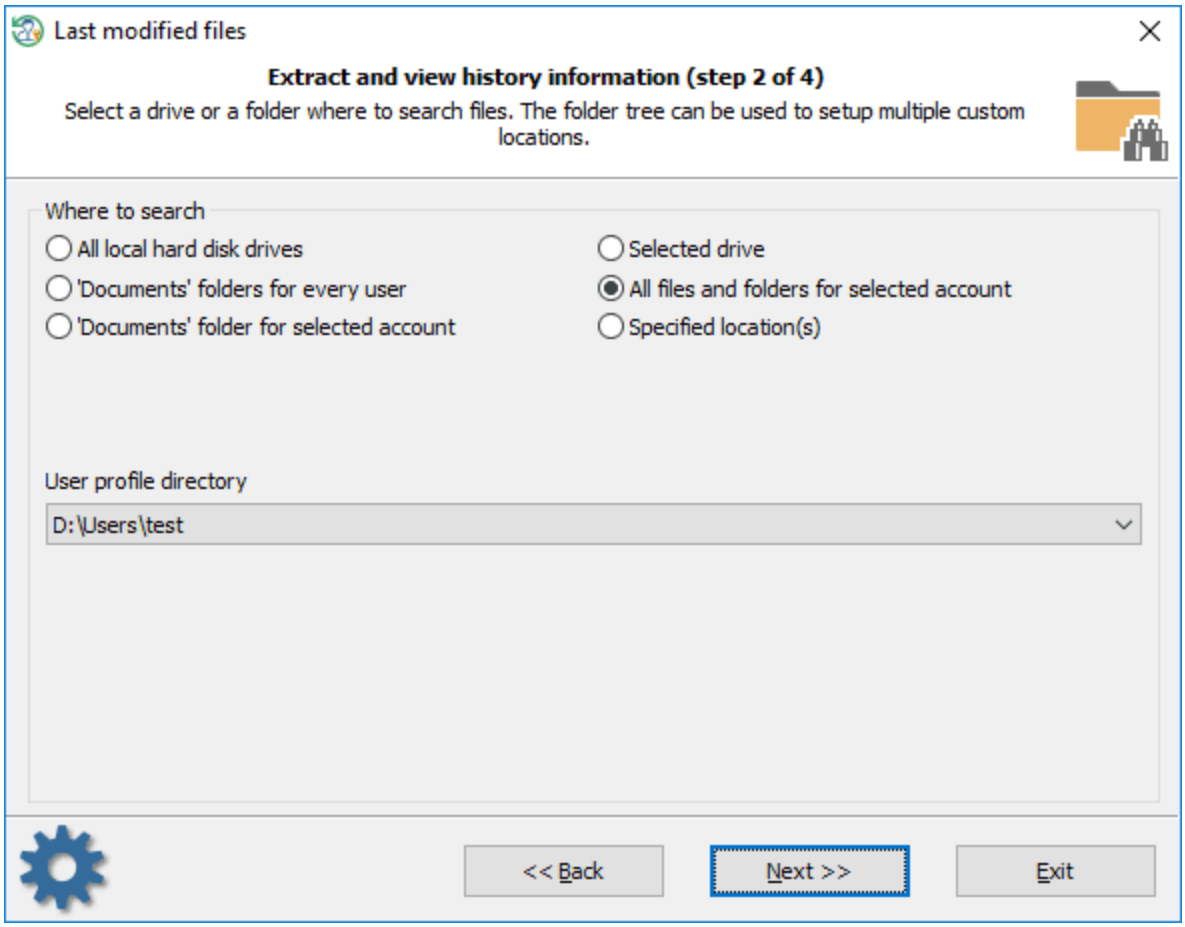
Firefox (y navegadores basados en Mozilla)
Mozilla tuvo un largo camino evolucionando el formato de almacenamiento de contraseñas. Inicialmente, era un simple archivo textual de signons.txt. Luego, en la versión 2, llegó signons2.txt que tenía el

prefijo "#2c" al principio del archivo. Luego signons3.txt con el prefijo "#2d" en la versión 3, etc. A continuación, la base de datos signons.sqlite entró en juego. Pero no es el final de la historia. Firefox v32.x y superior tiene un nuevo almacenamiento para contraseñas: logins.json, que en realidad es un archivo de formato JSON. A pesar de la aparente diversidad, la protección de datos es casi la misma. Una ubicación típica para los archivos es: C:\Users\<USERNAME>\AppData\Roaming\Mozilla\<PROGRAM>\Profiles\<PROFILE>.

3.17.10 Ver los archivos modificados por última vez

A veces se requiere averiguar qué archivos o carpetas se crearon o modificaron en un tiempo determinado. Para eso fue creada esta herramienta. Intentamos hacerlo lo más simple posible. Todo lo que necesita es establecer la ubicación de búsqueda y especificar el intervalo de tiempo para los archivos/carpetas buscados.

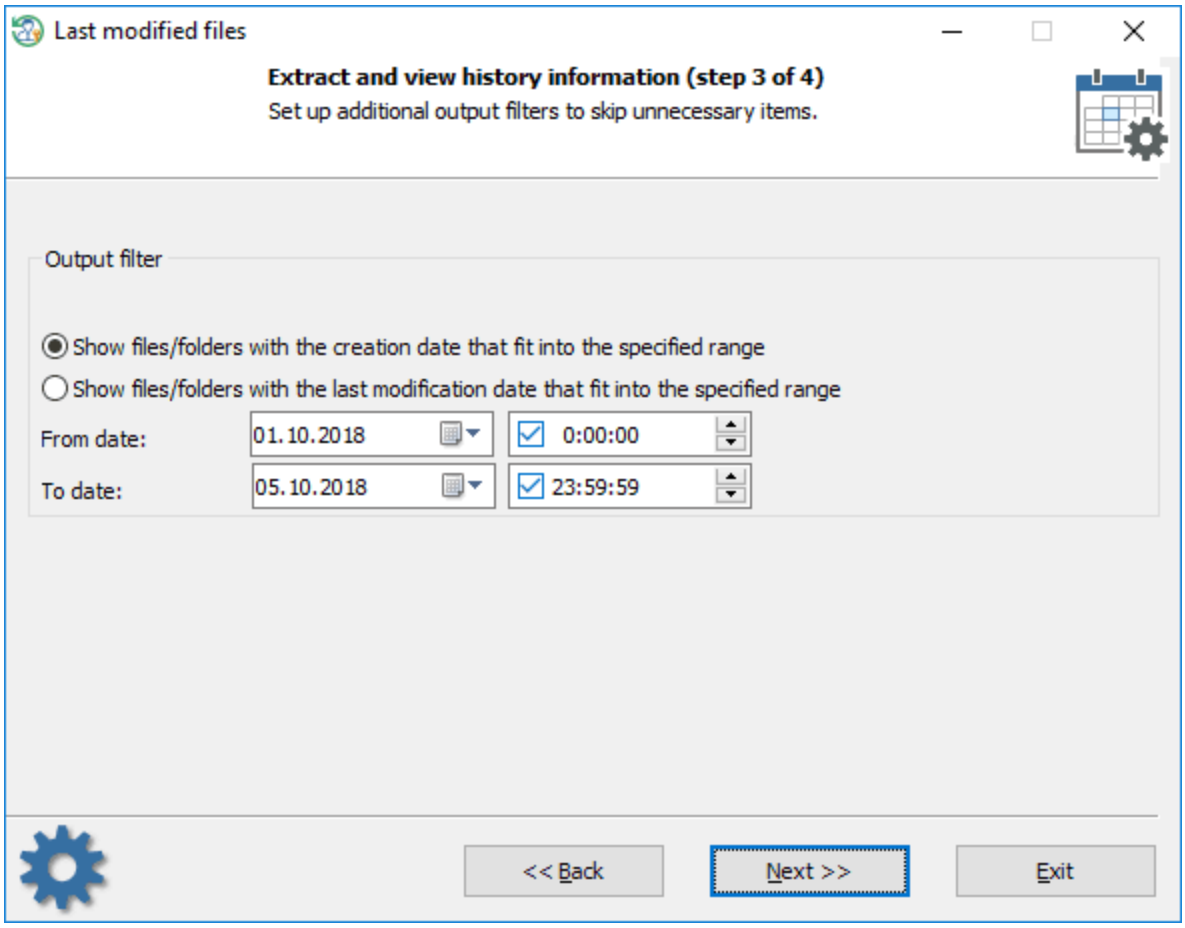
Configuración de la ubicación de búsqueda



Para señalar al programa el punto de partida de los archivos a buscar, seleccione uno de algunos valores predefinidos como la carpeta de documentos de un determinado usuario, el perfil de todo el

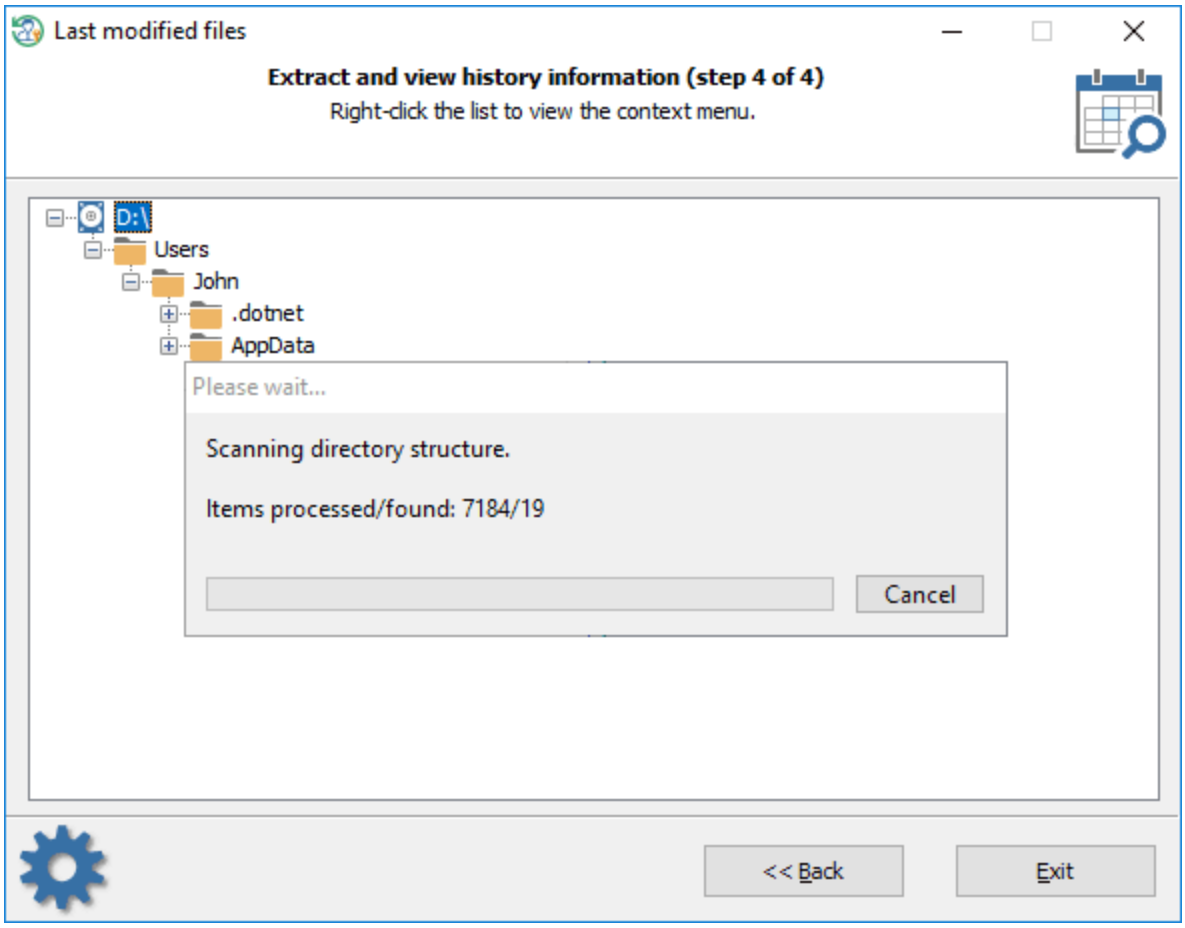
usuario, etc. También puede especificar su propia ubicación estableciendo una ruta personalizada o un disco duro.

Configuración del intervalo de tiempo



Especifique aquí si necesita buscar archivos/carpetas con una fecha de creación determinada o una fecha de modificación. Puede configurar el tiempo hasta segundos o desactivar los segundos por completo.

Visualización de los archivos modificados por última vez



Tenga paciencia, la búsqueda puede llevar bastante tiempo.

3.17.11 Ver directorios modificados por última vez

Esta herramienta se comporta exactamente igual que la anterior, excepto que busca las carpetas en lugar de los archivos. Consulte la herramienta de búsqueda de archivos para obtener más información.

3.18 UTILS

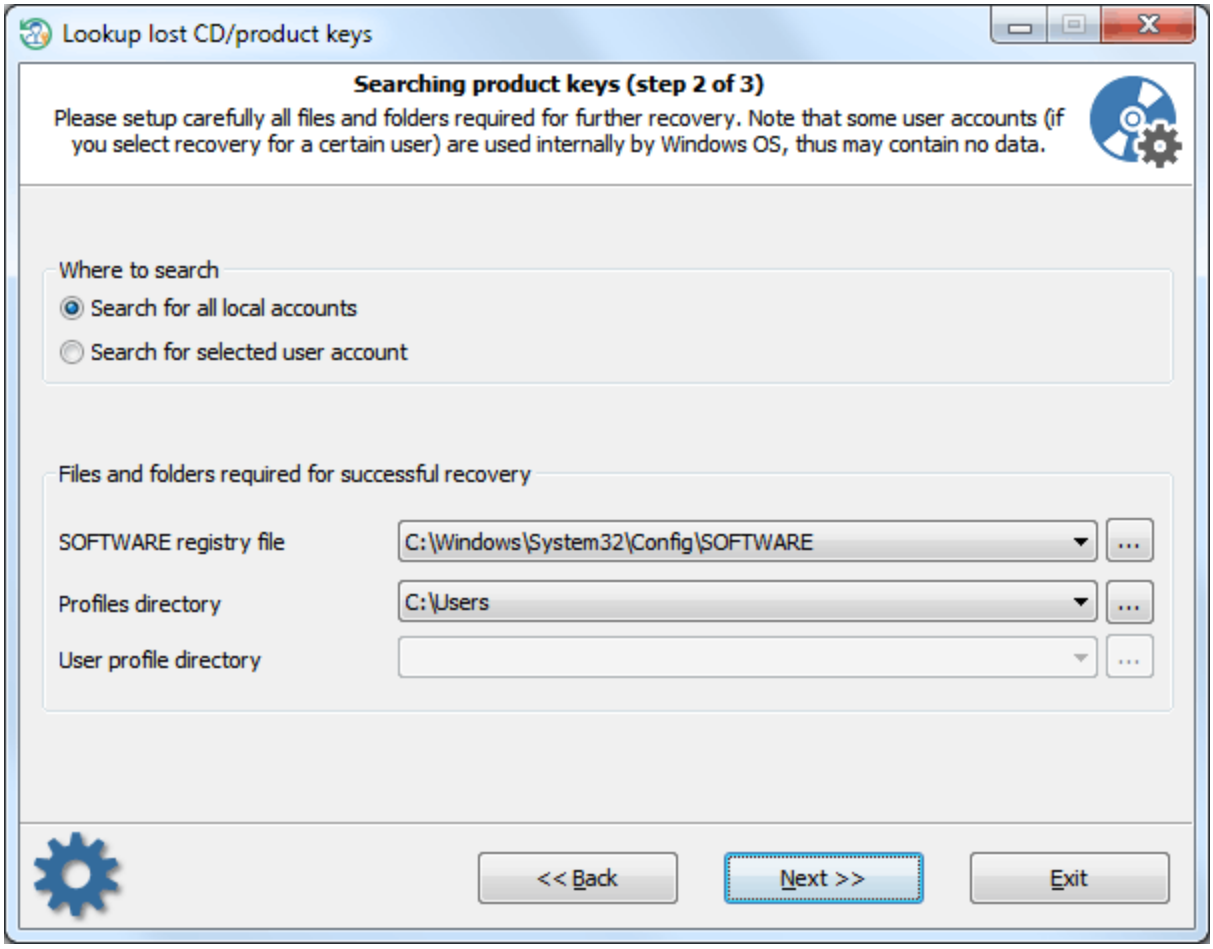
3.18.1 Búsqueda de claves de producto/CD perdidas

Con esta función, puede recuperar fácilmente las claves de producto y los números de serie perdidos, incluso si el sistema de destino ya no se puede arrancar.

Casi todos los programas comerciales para Windows vienen con una clave de serie que une el programa a su PC y hace que el software sea legal o con todas las funciones. Al perder esta clave, ya no tendrá acceso a su propio software a menos que recupere la clave. Imagínese que un día necesita reinstalar su

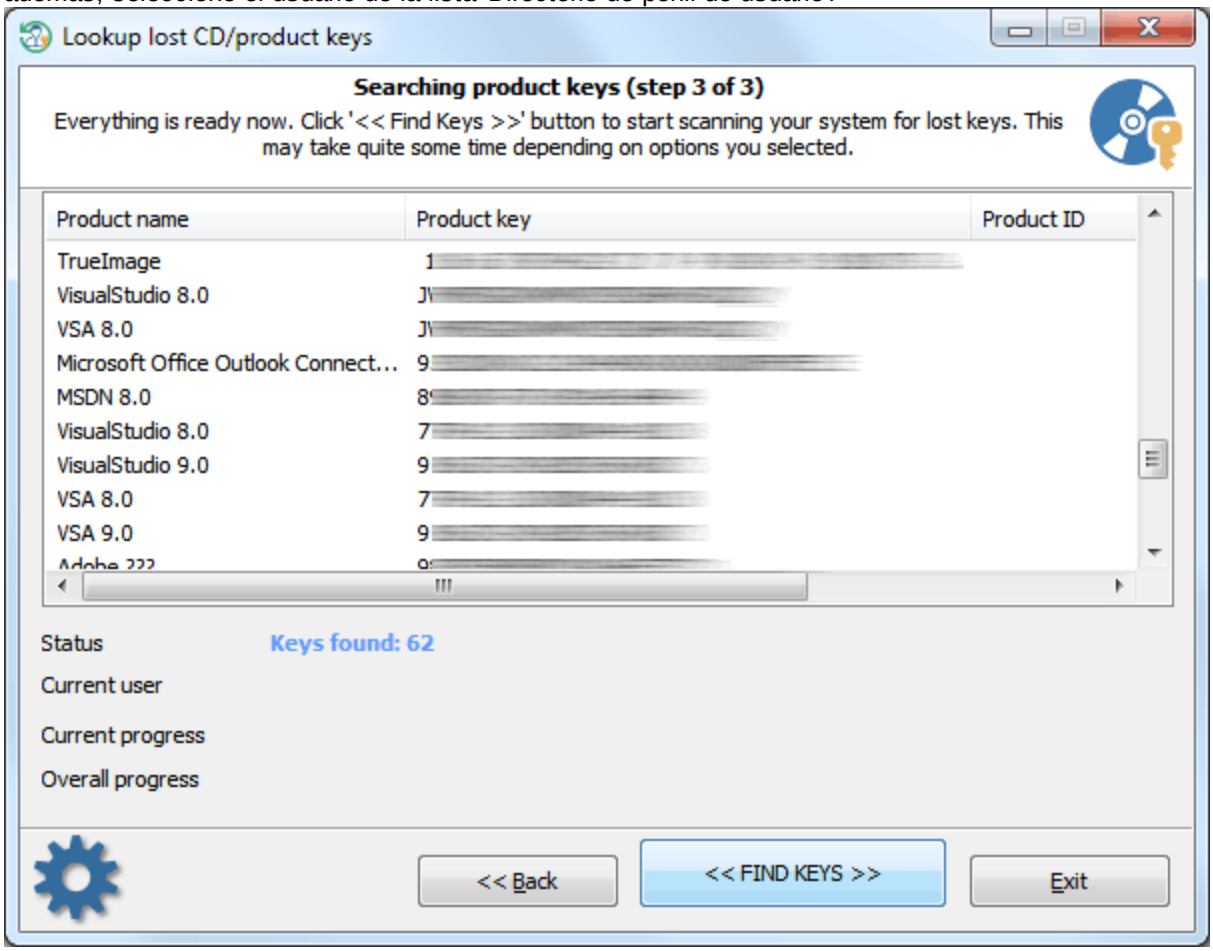
sistema operativo. Puede haber muchas razones por las que desea hacerlo, desde actualizar hasta deshacerse de los virus, solucionar un problema, etc. Y después de reinstalar, descubrirá que necesita reinstalar la mayor parte de su software y suministrarlo con códigos de serie a los que ya no tiene acceso. Sin las claves, no puede reinstalar el software.

Afortunadamente, una gran proporción de programas informáticos almacenan sus claves de producto en el registro de Windows y, por lo tanto, se pueden extraer fácilmente. Para eso está esta característica. Utilizando un lenguaje de script incorporado, el 'Restablecer contraseña de Windows' puede recuperar claves de serie para más de 1,000 productos de software. Y, sin embargo, es muy simple de usar.



Primero, indique al programa si necesita recuperar claves de serie para todos los usuarios locales o solo para una cuenta seleccionada. La recuperación de claves para todas las cuentas de usuario necesita al menos dos parámetros para configurarse correctamente:
1. Archivo de registro de SOFTWARE que se encuentra en el siguiente directorio: *'C:\Windows\System32\Config'*. Tenga en cuenta que la letra de la unidad, así como la carpeta de Windows pueden ser diferentes. Por ejemplo *'D:\Windows'*, *'E:\Win'*, etc.
2. Carpeta Perfiles. Ese es el directorio donde se almacenan físicamente todas las cuentas de usuario locales. Para Windows Vista y sistemas operativos superiores, generalmente es *'C:\Usuarios'* Mientras que Windows XP utiliza *'C:\Documents and Settings'*. Por lo general, la carpeta de perfiles está en la misma unidad donde se encuentra el directorio de Windows, aunque no siempre.
El programa intentará detectar estas carpetas automáticamente. Todo lo que necesita hacer es seleccionar uno de la lista desplegable o especificar una ruta alternativa de lo contrario.

Si necesita recuperar series para un determinado usuario, simplemente configure la opción adecuada y, además, seleccione el usuario de la lista 'Directorio de perfil de usuario'.

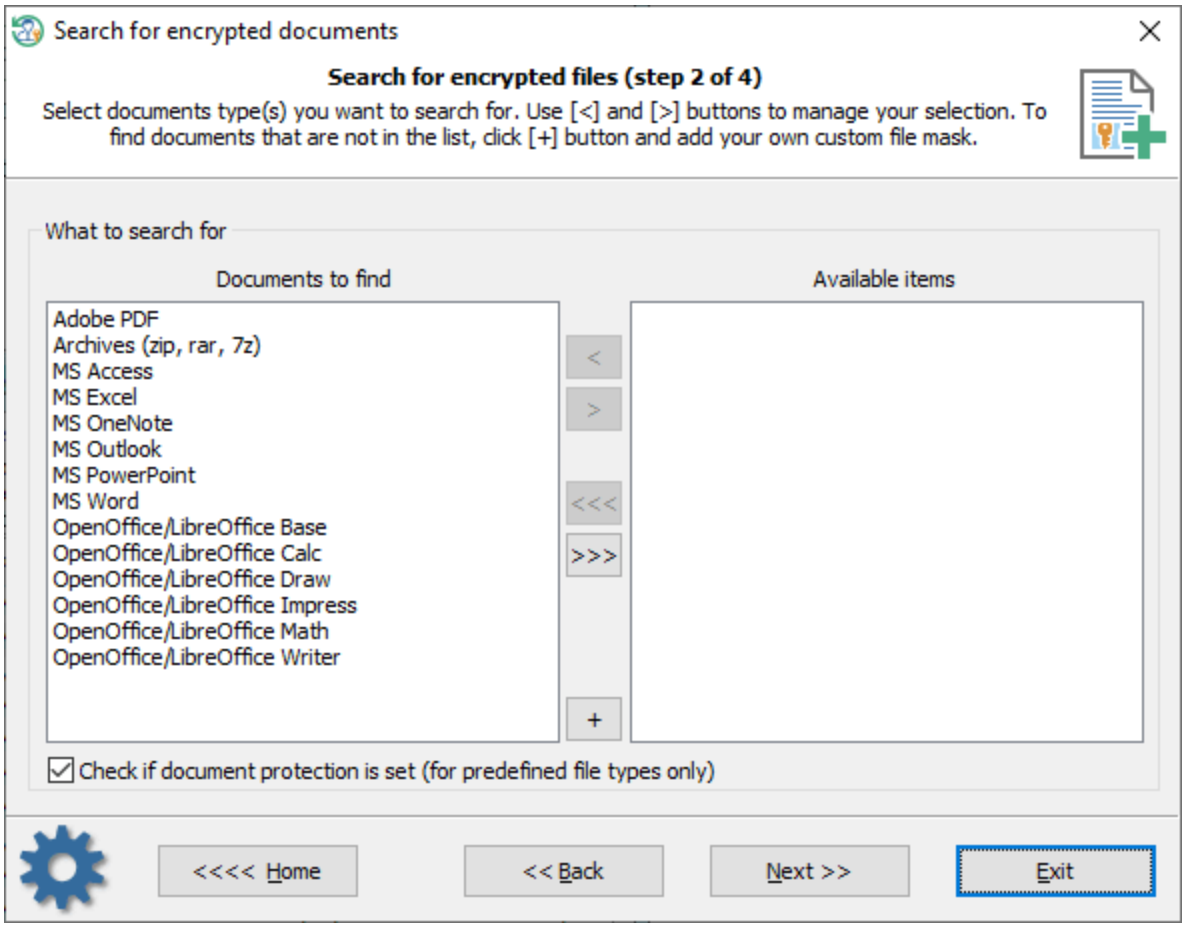


Una vez establecidas las opciones requeridas, continúe con el paso final y haga clic en el botón *'<< ENCONTRAR LLAVES >>'* para iniciar el programa buscando claves de serie perdidas.

3.18.2 Buscar documentos protegidos por contraseña

La función de este programa está destinada a escanear y buscar en una PC documentos cifrados, archivos y archivos protegidos con contraseña. Es fácil de usar, y rápido y flexible en su configuración. Incluso puede especificar sus propios tipos de archivos para buscar. El proceso de búsqueda se divide en tres sencillos pasos:

1 Selección del tipo de documento



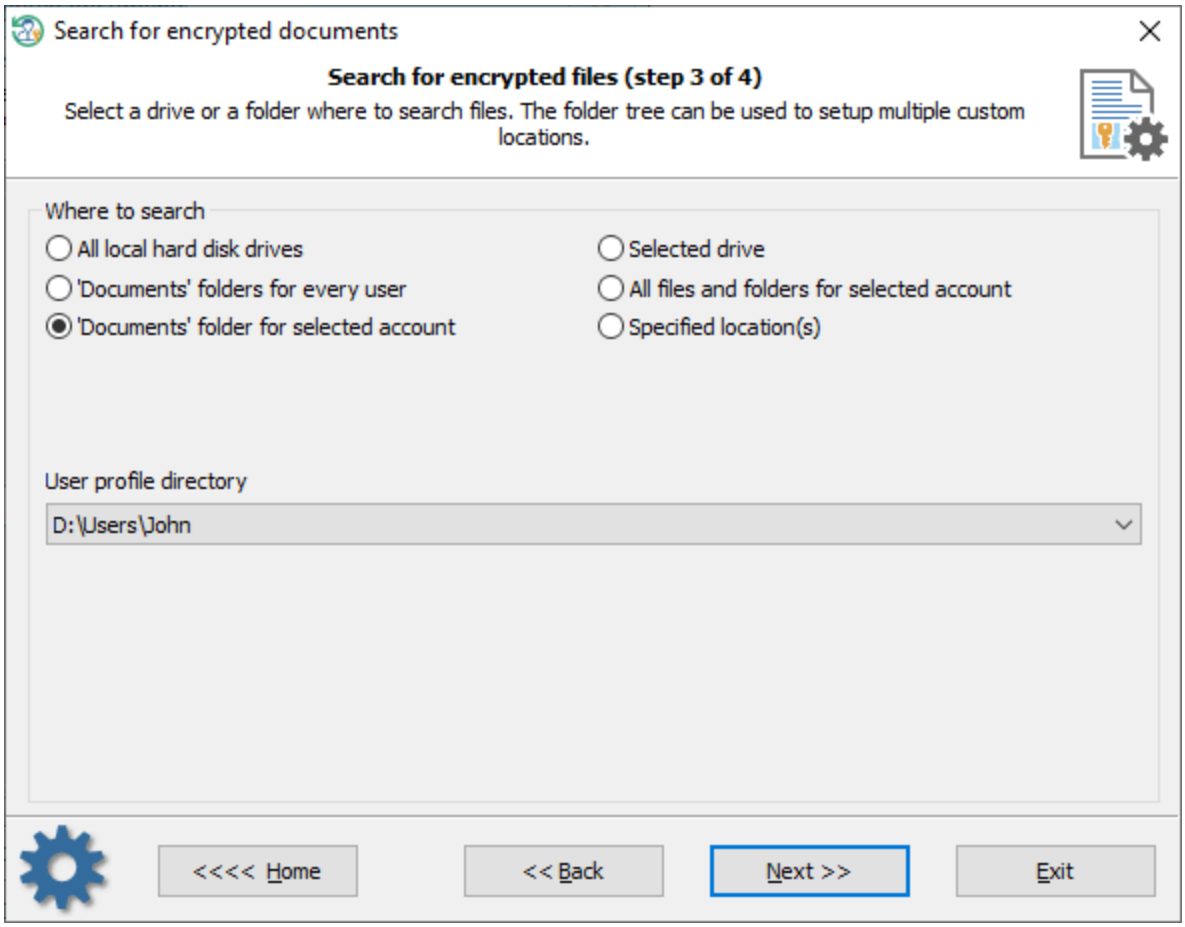
De forma predeterminada, el programa busca los siguientes documentos predefinidos:

- Archivos de archivos (zip, rar, 7z)
- Documentos PDF
- Documentos de MS Word
- Tablas de MS Excel
- Bases de datos de MS Access
- Presentaciones de MS PowerPoint
- Notas de MS OneNote
- Archivos de datos de MS Outlook
- Documentos de OpenOffice/LibreOffice Writer
- Tablas openOffice/LibreOffice Calc
- Bases de datos base de OpenOffice/LibreOffice
- Presentaciones de OpenOffice/LibreOffice Impress
- Documentos de OpenOffice/LibreOffice Draw
- Documentos matemáticos de OpenOffice/LibreOffice

Utilice los botones [>] y [<] para incluir o excluir los documentos disponibles del proceso de búsqueda. Si desea agregar sus propios tipos de archivos para buscar, use el botón [+] y especifique su descripción y una máscara de búsqueda. Por ejemplo, la siguiente máscara se puede utilizar para buscar archivos de datos de KeePass:
***.kdbx, *.kdb, *.pwd**
Tenga en cuenta que el análisis de protección con contraseña no se utiliza para las máscaras personalizadas.

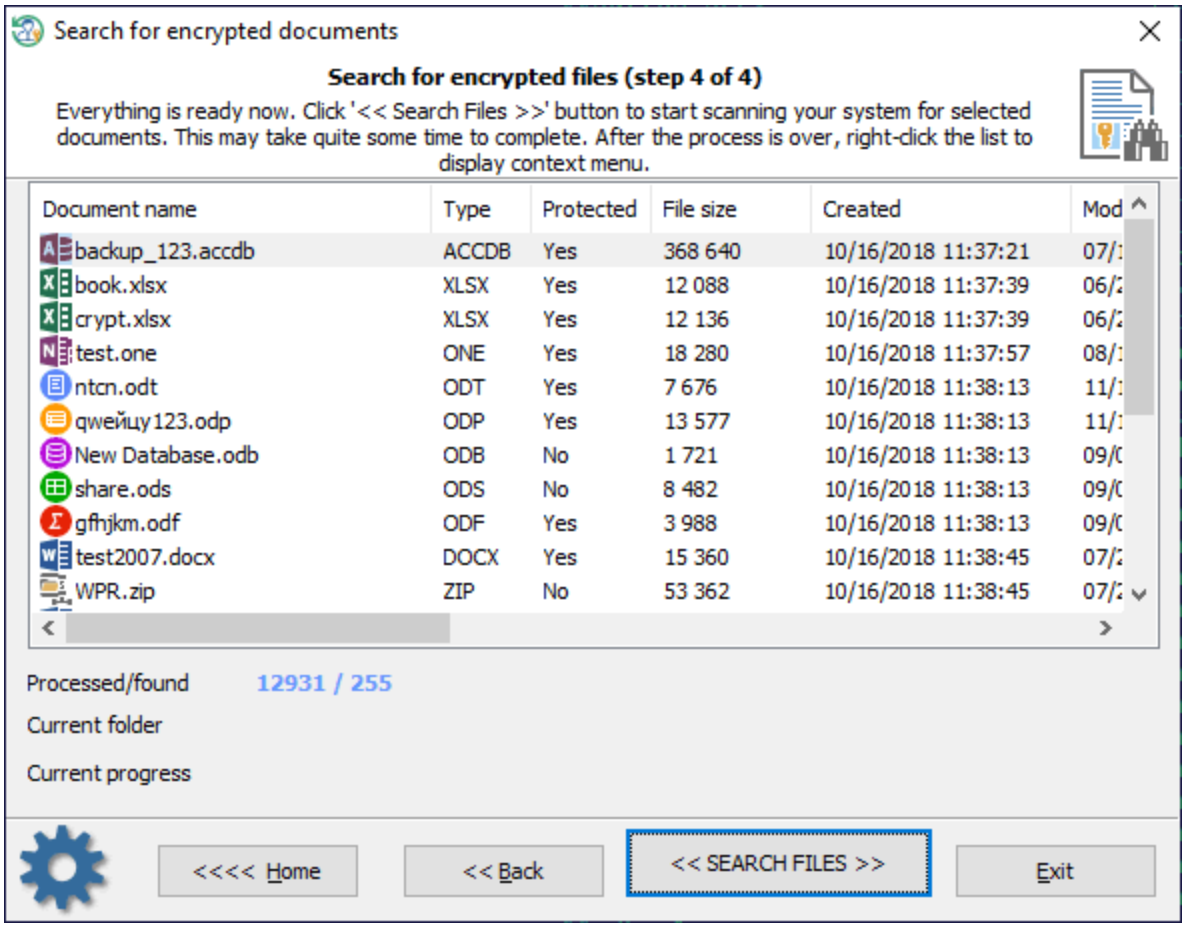
El 'Comprobar si la protección de documentos está configurada...' se utiliza para desactivar completamente el análisis de protección con contraseña. Eso podría acelerar significativamente el proceso de búsqueda en algunos casos.

2 Selección de dónde buscar



Puede reducir el rango de escaneo configurando, por ejemplo, la carpeta 'Documentos' para una cuenta seleccionada o eligiendo un directorio determinado.

3 Búsqueda de documentos

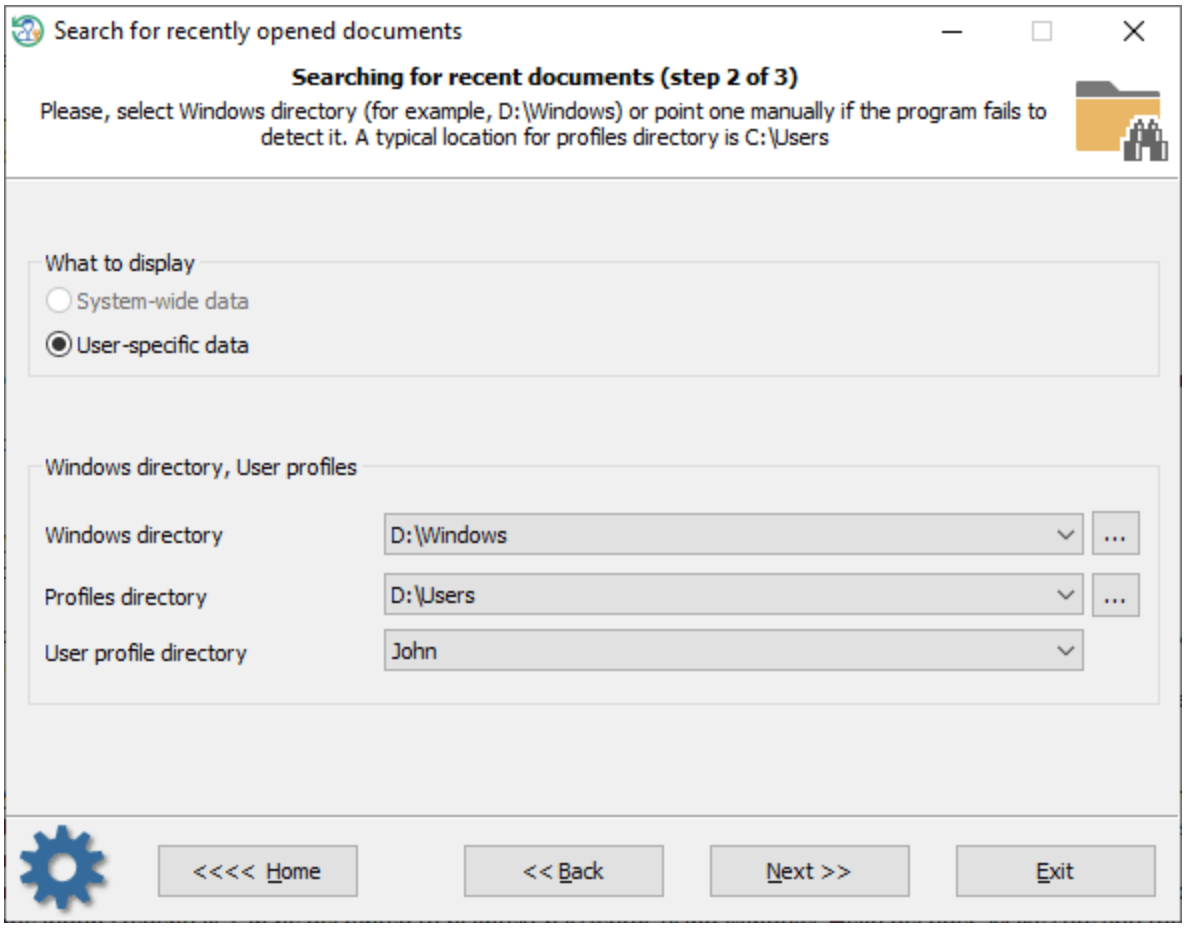


A pesar de que el programa fue optimizado para la búsqueda rápida, escanear discos duros con muchos archivos puede llevar mucho tiempo. Una vez conternó la búsqueda, haga clic con el botón secundario en la lista de documentos encontrados para especificar las operaciones disponibles. Por ejemplo, puede guardar la lista de archivos encontrados en un archivo de texto / html, o crear un solo archivo zip para los elementos seleccionados.

3.18.3 Buscar archivos abiertos recientemente

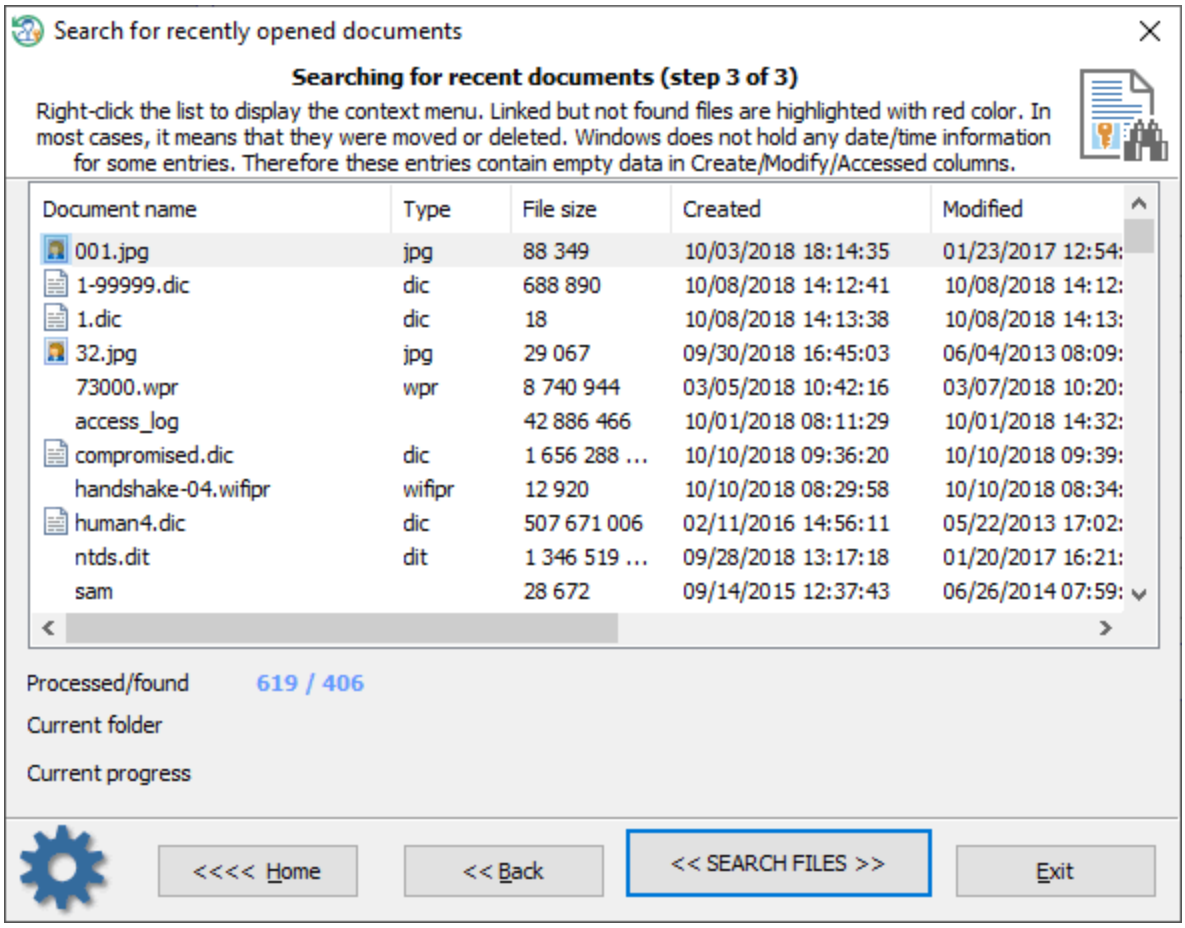
A veces es vital obtener una lista de los últimos documentos modificados para una cuenta de usuario. Por ejemplo, los forenses pueden usar esta herramienta para analizar los archivos a los que accedió el usuario durante la última sesión de inicio de sesión.

1 Selección de dónde buscar



Para extraer los datos, especifique el directorio de Windows de destino y el perfil del usuario.

2 Búsqueda de archivos recientes



Haga clic en el botón 'Buscar archivos' para iniciar el proceso. Una vez conternó la búsqueda, haga clic con el botón secundario en la tabla para mostrar las operaciones disponibles. Puede guardar la lista de elementos encontrados en un archivo de texto/html, o hacer una copia de seguridad de los archivos seleccionados en un archivo zip.

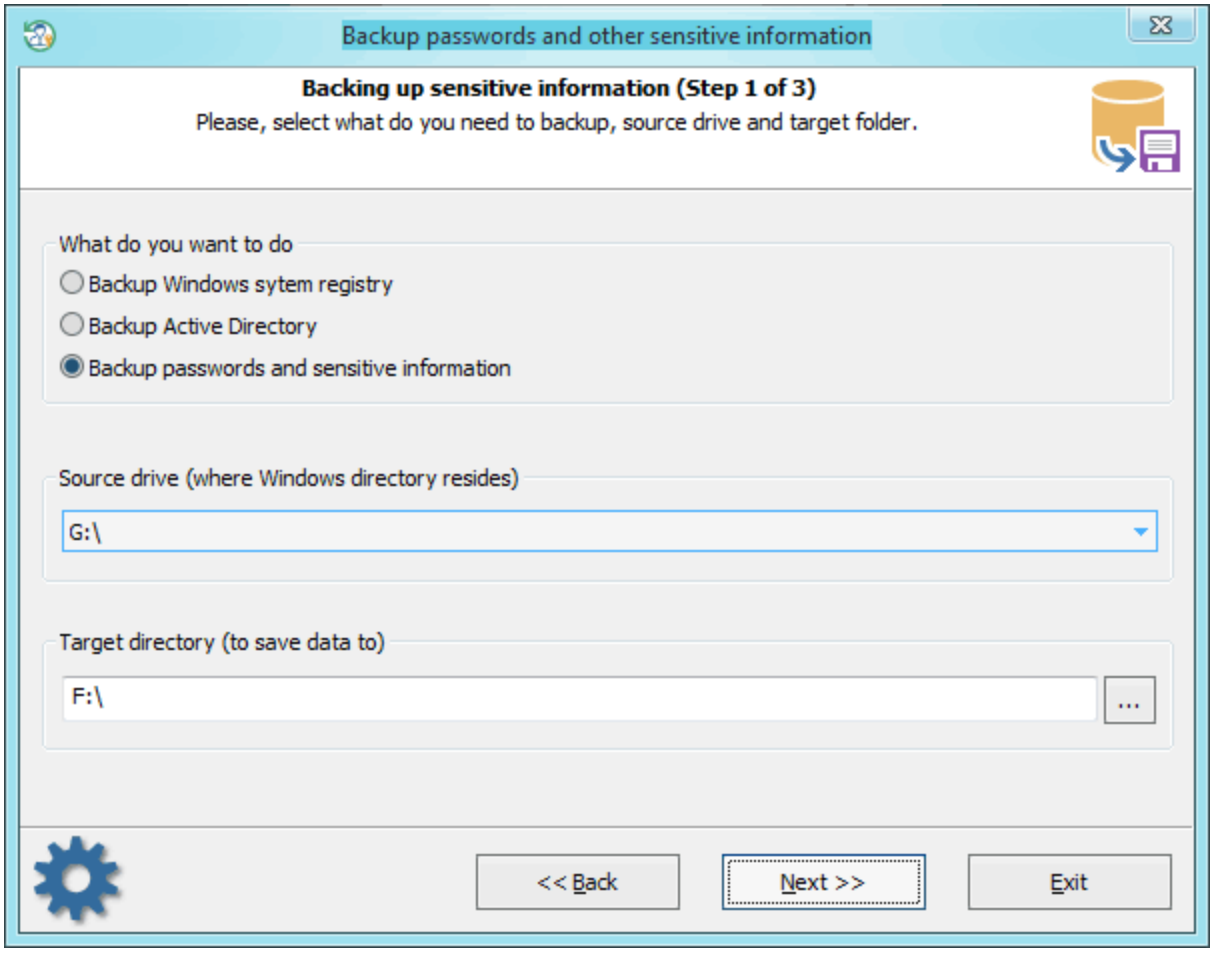
3.18.4 Contraseñas de copia de seguridad e información confidencial

A veces es vital hacer una copia del registro de Windows o una base de datos de Active Directory. **Reset Windows Password** es un salvavidas para aquellos que necesitan hacer una copia de seguridad de los archivos fácilmente. Incluso puede hacer una instantánea de todos los datos confidenciales de la PC de destino en solo un par de clics.

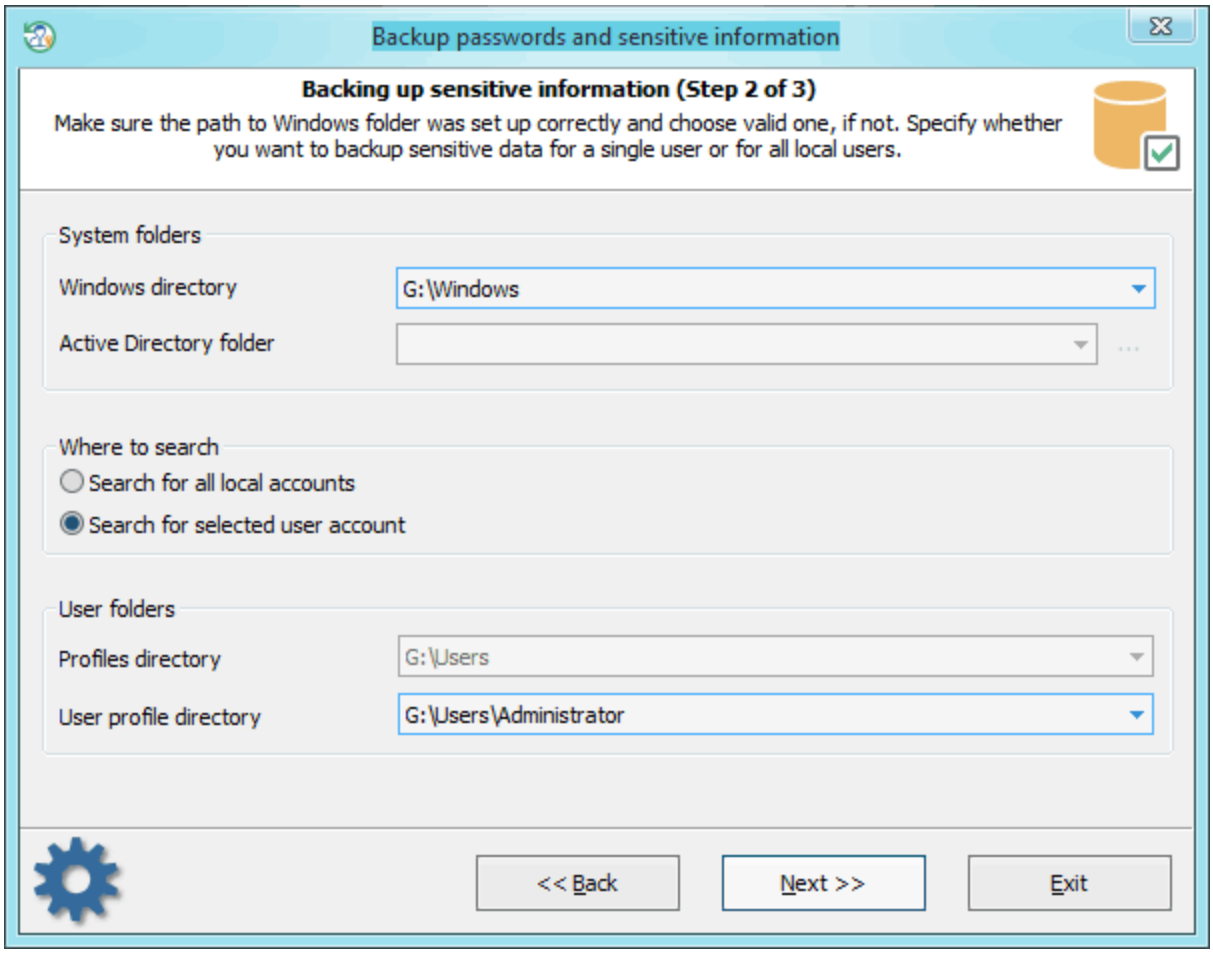
Primero, debemos configurar qué respaldar:
- Archivos de registro de Windows
- Base de datos de Active Directory
- Toda la información confidencial, incluido el registro de Windows, contraseñas, certificados, etc.

Tendrá que establecer una unidad de origen donde reside el directorio de Windows de destino y una ruta de destino. La ruta de destino se utilizará para guardar los archivos archivados de salida. De forma

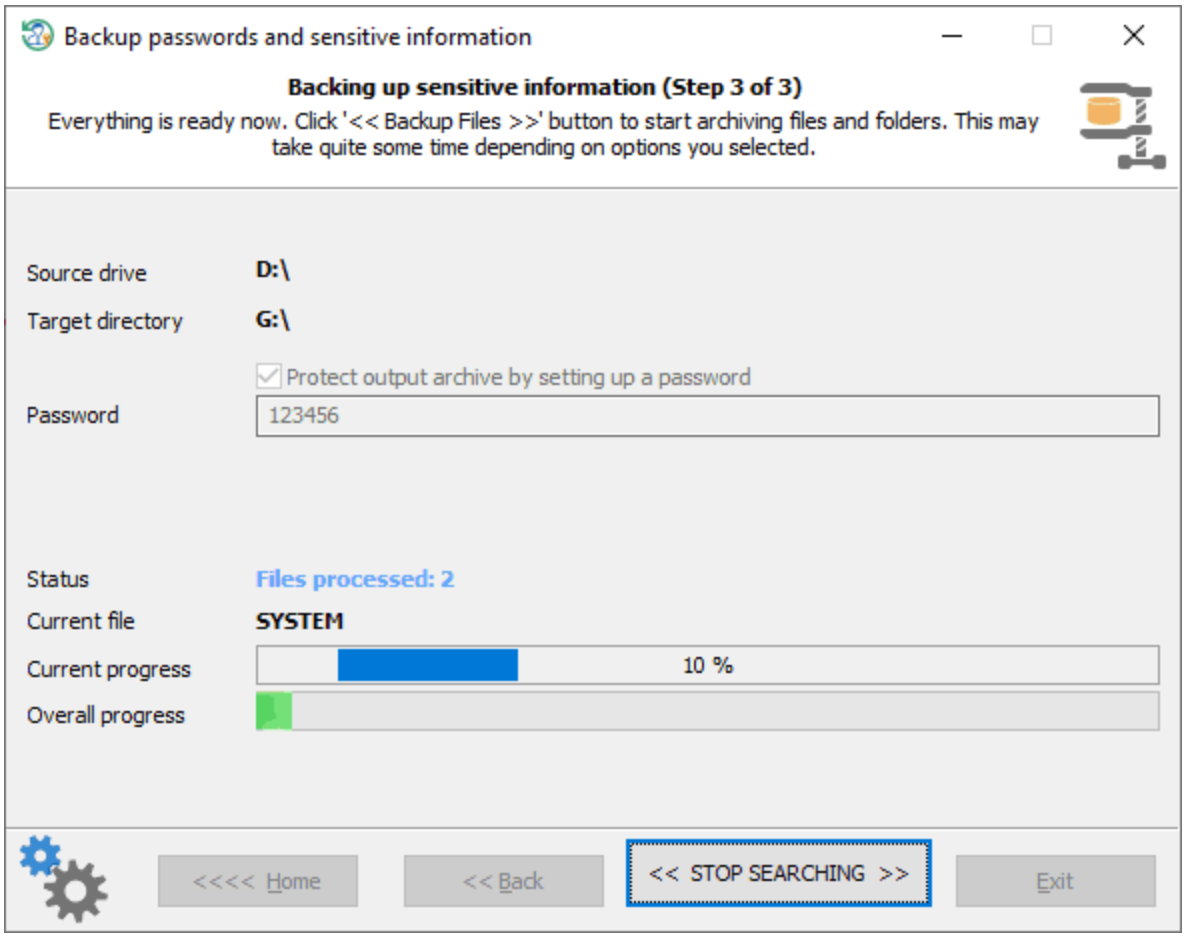
predeterminada, el programa sugiere el primer disco duro como origen y la primera unidad extraíble como destino.



El siguiente paso es un poco más simple. En caso de que haya seleccionado la copia de seguridad de Registro/Active Directory en el paso anterior, todo lo que necesita aquí es confirmar las carpetas de Windows/AD. De lo contrario, también tendrá que seleccionar el directorio de perfiles o el directorio de perfiles para el usuario seleccionado, según las opciones que elija.

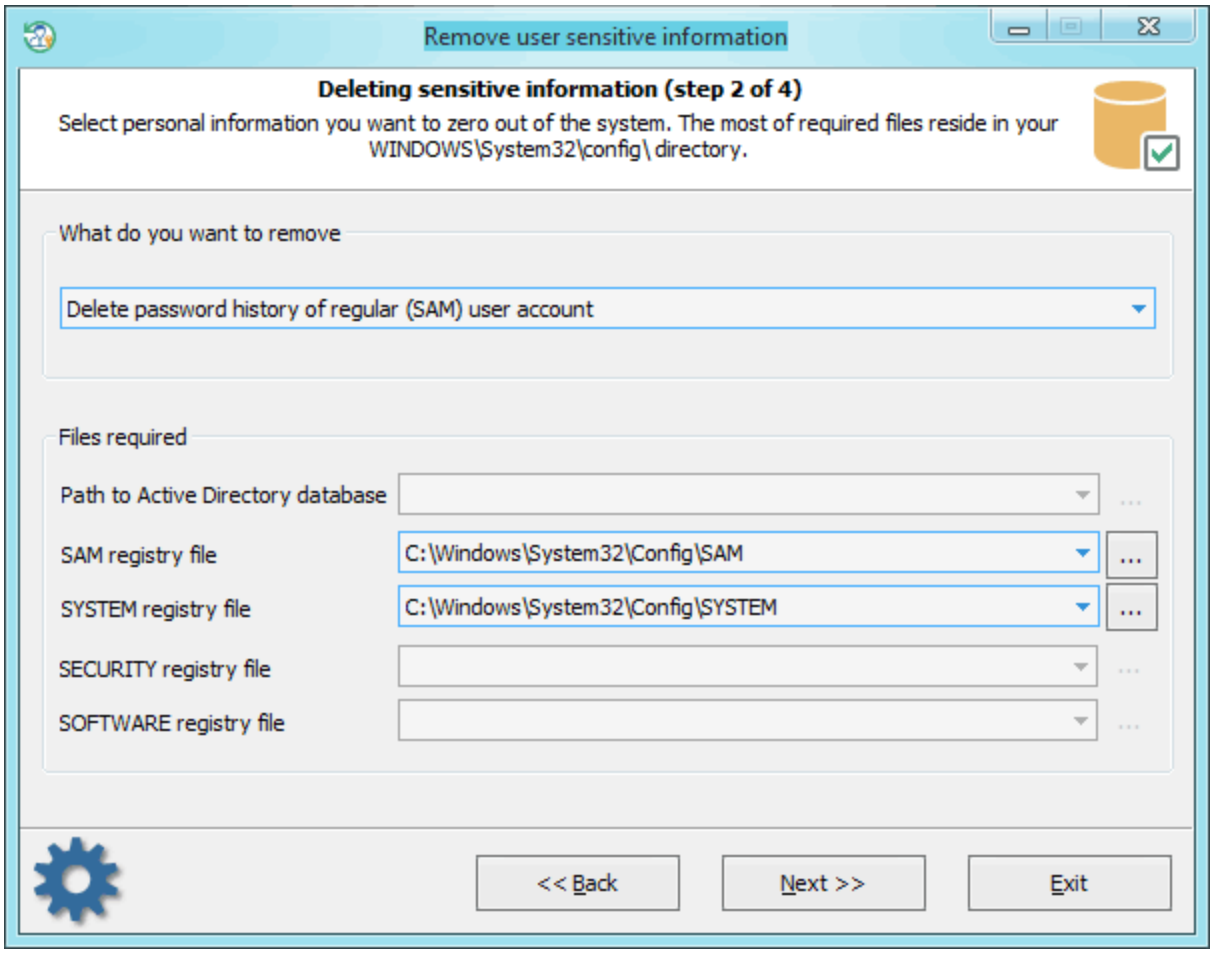


Y el cuadro de diálogo final es solo un progreso para la operación de copia de seguridad. Clic en el botón **<< Respaldar archivos >>** para iniciar el proceso. Al completar con éxito, debe obtener un *. Archivo ZIP que contiene todos los archivos solicitados. Más tarde, puede usar estos archivos para analizar los datos secretos en cualquier software de terceros. Por ejemplo, en la herramienta **Windows Password Recovery**.



3.18.5 Eliminación de la información privada del usuario

Selección de los datos que se eliminarán



La aplicación tiene una serie de características avanzadas. Uno de ellos es eliminar información que puede ser utilizada por posibles malhechores para recuperar contraseñas de cuentas en su computadora. Ten cuidado; la información se eliminará de forma permanente sin posibilidades de recuperación. Por lo tanto, incluye los siguientes elementos:

1. Eliminación del historial de contraseñas de cuentas SAM estándar y cuentas de usuario de Active Directory. El historial de contraseñas de SAM, por ejemplo, se establece en la directiva de grupos del equipo local. Inicio -> Ejecutar -> gpedit.msc -> haga clic en Aceptar. En Configuración del equipo, profundice en Configuración de Windows -> Configuración de seguridad -> Directivas locales -opciones de seguridad >. Aquí busque la política: *Inicio de Sesión Interactivo: Numero de inicios de sesión anteriores en la memoria cache*.
2. Eliminación de contraseñas almacenadas en caché de dominio. Se puede leer más información sobre las contraseñas almacenadas en caché de dominio aquí.
3. Eliminación de la contraseña de inicio de sesión de Windows almacenada en caché.
4. Eliminación de la información del disquete de restablecimiento de contraseña. Con esa información y el disco de restablecimiento de contraseña, se puede recuperar la contraseña original en texto.
5. Eliminación de sugerencias de contraseña.
6. Restablecimiento de Syskey

Para continuar con la aplicación, proporcione (o seleccione entre los disponibles) los siguientes archivos:
- Eliminación del historial de contraseñas de AD – Archivo de registro **SYSTEM** y archivo de base de datos de Active Directory (**ntds.dit**)

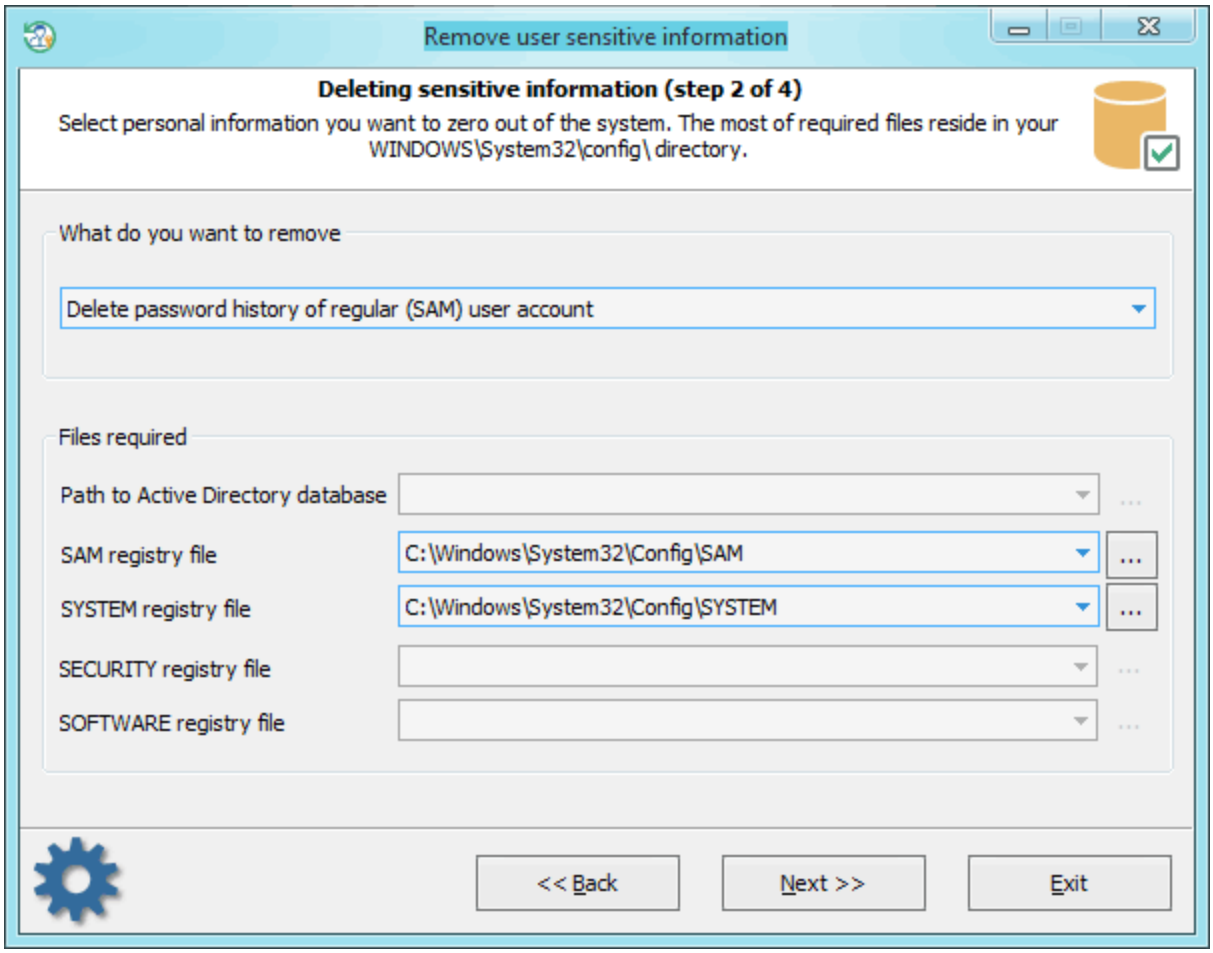
- Eliminación del historial de contraseñas de SAM – Archivos de registro **SAM** y **SYSTEM**
- Eliminación de contraseñas de dominio almacenadas en caché – archivos **SECURITY** y **SYSTEM**
- Eliminación de contraseñas de inicio de sesión almacenadas en caché – archivos **SECURITY**, **SYSTEM** y **SOFTWARE**
- Eliminación de la información de restablecimiento de contraseña - archivos **SAM**, **SECURITY** y **SYSTEM**
- Eliminación de sugerencias de contraseña - **SAM**, **SOFTWARE** y **SYSTEM**
- Restablecimiento de SYSKEY - **SAM**, **SECURITY** y **SYSTEM**

Todos los archivos del Registro, excepto la base de datos de Active Directory, se almacenan en el siguiente directorio **%WINDIR%\system32\config**. Dónde %WINDIR% significa la carpeta Windows, de forma predeterminada - C:\Windows.

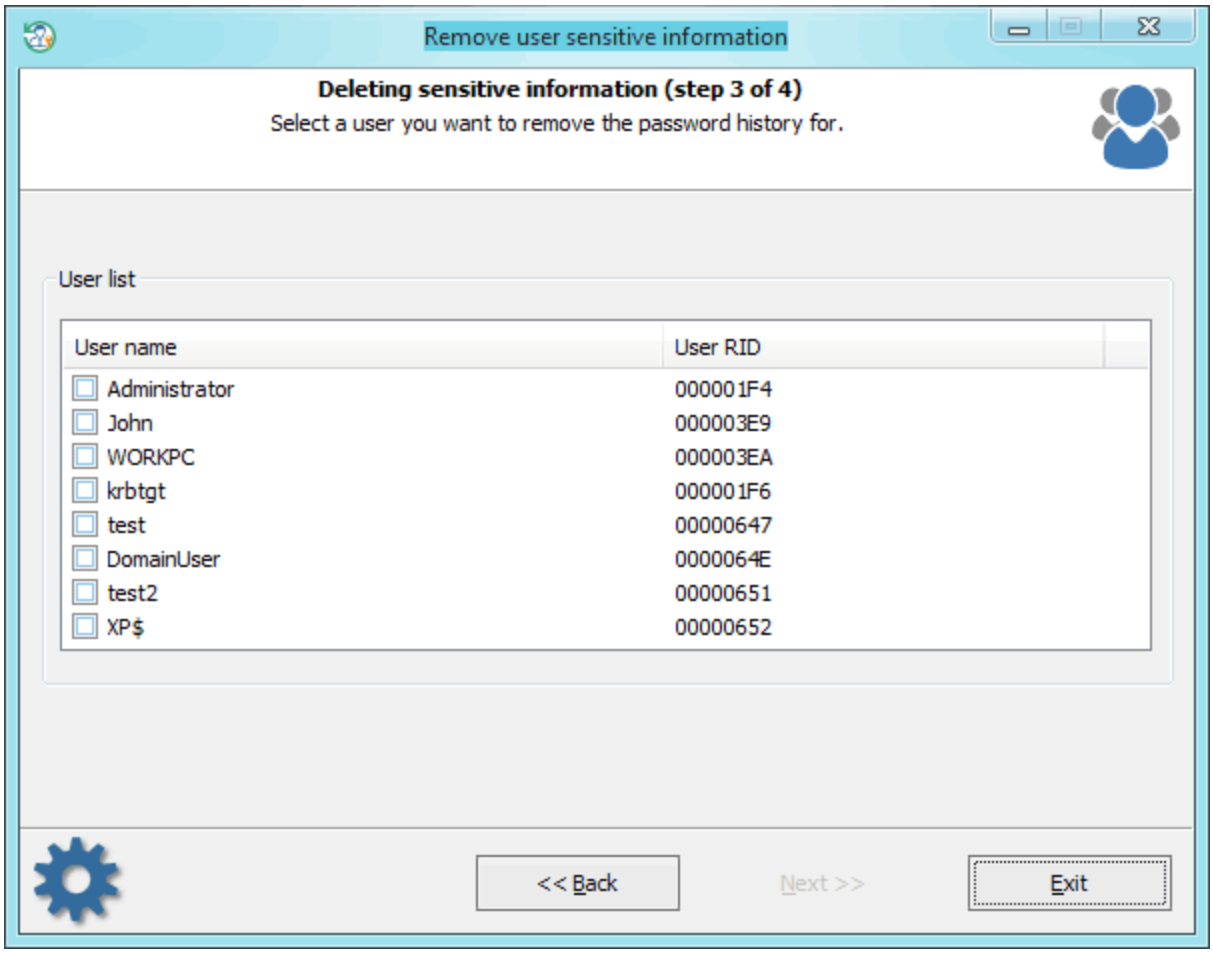
La ubicación de la base de datos de AD se establece durante la instalación. De forma predeterminada, es la carpeta **%WINDIR%\NTDS**.

3.18.5.1 Eliminación del historial de contraseñas de los usuarios de SAM o Active Directory

Selección del origen de datos

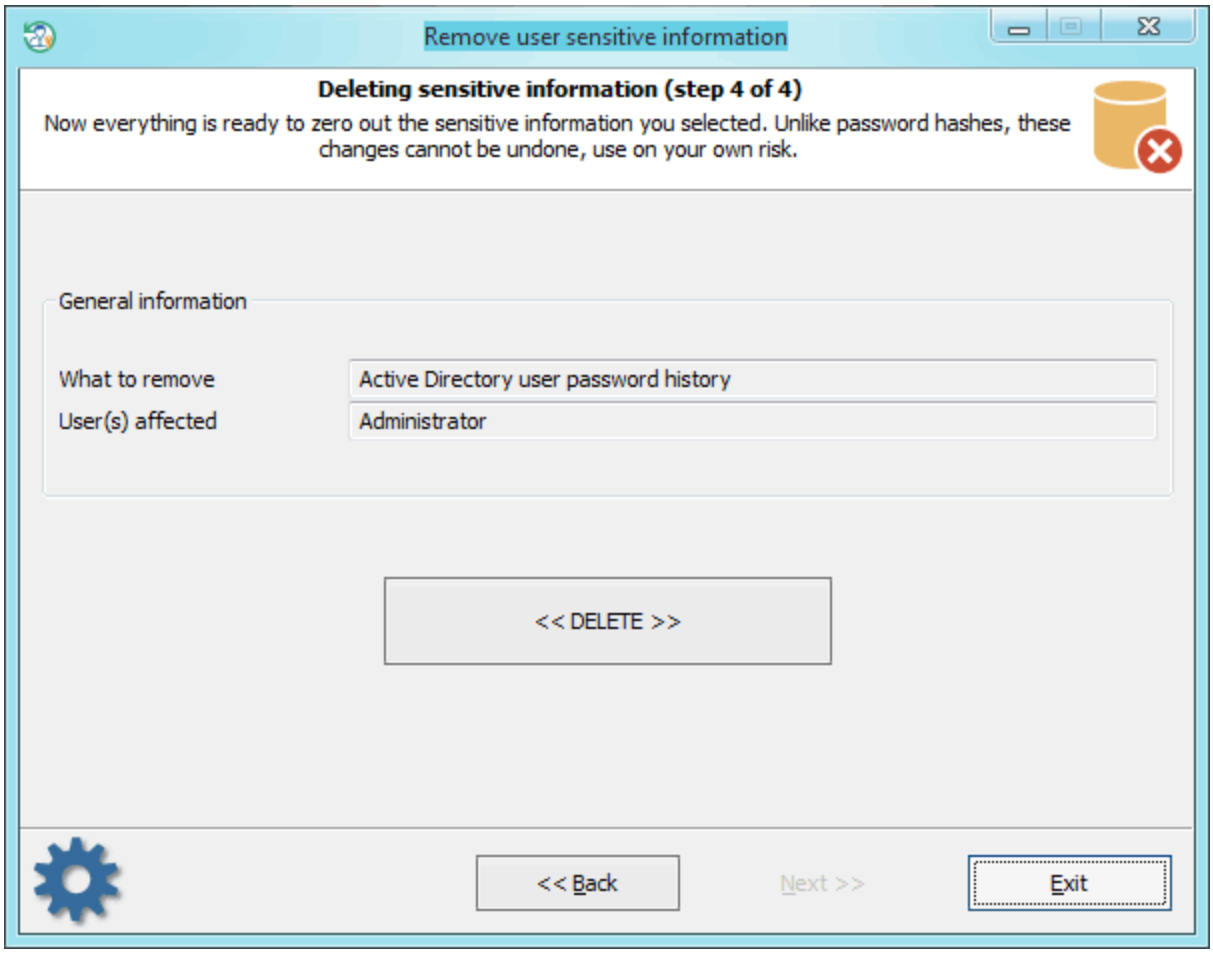


Selección de la cuenta de usuario



En la lista de cuentas, seleccione la que necesitamos para eliminar el historial de contraseñas. La aplicación solo muestra los usuarios que tienen historial.

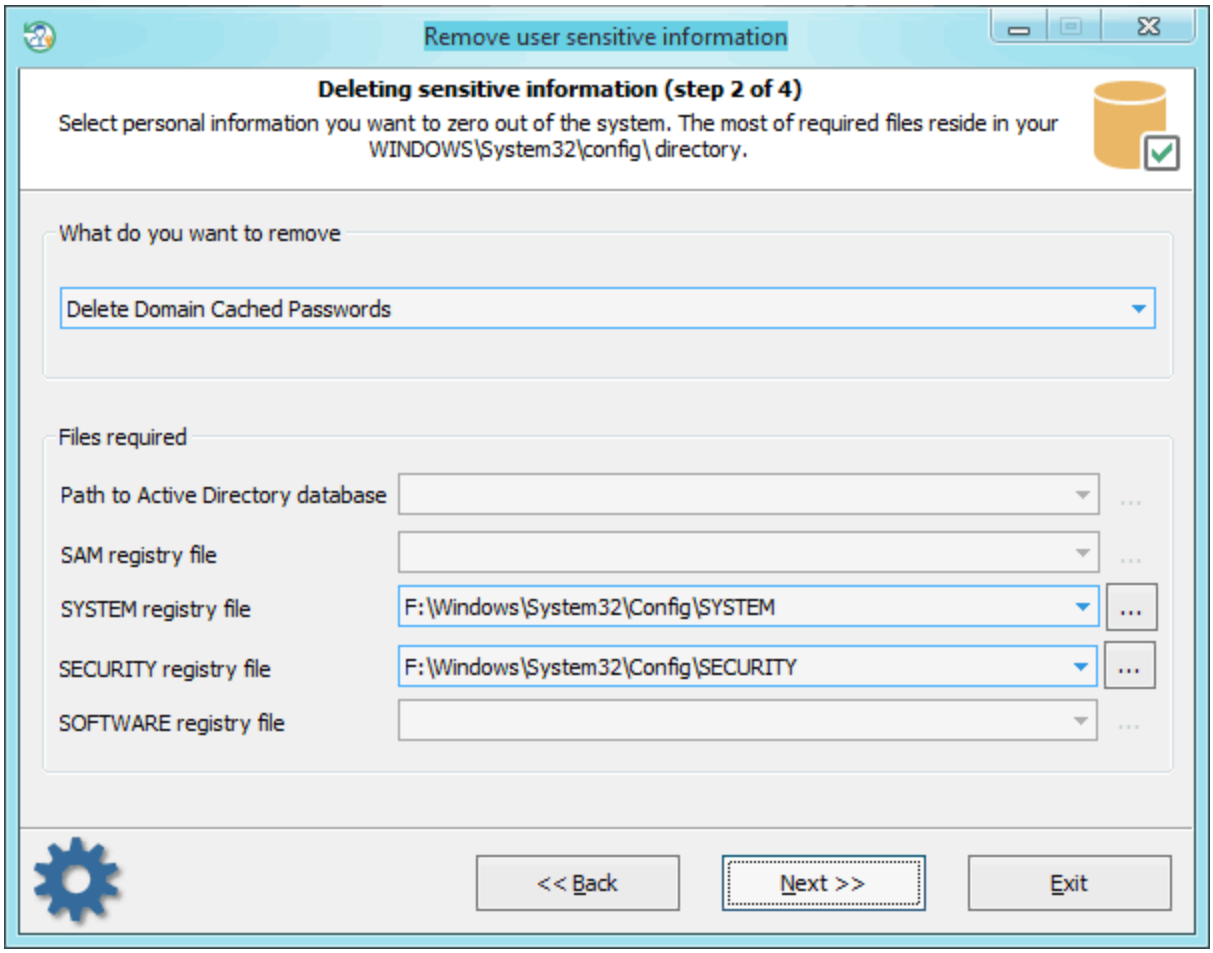
Eliminación del historial de contraseñas



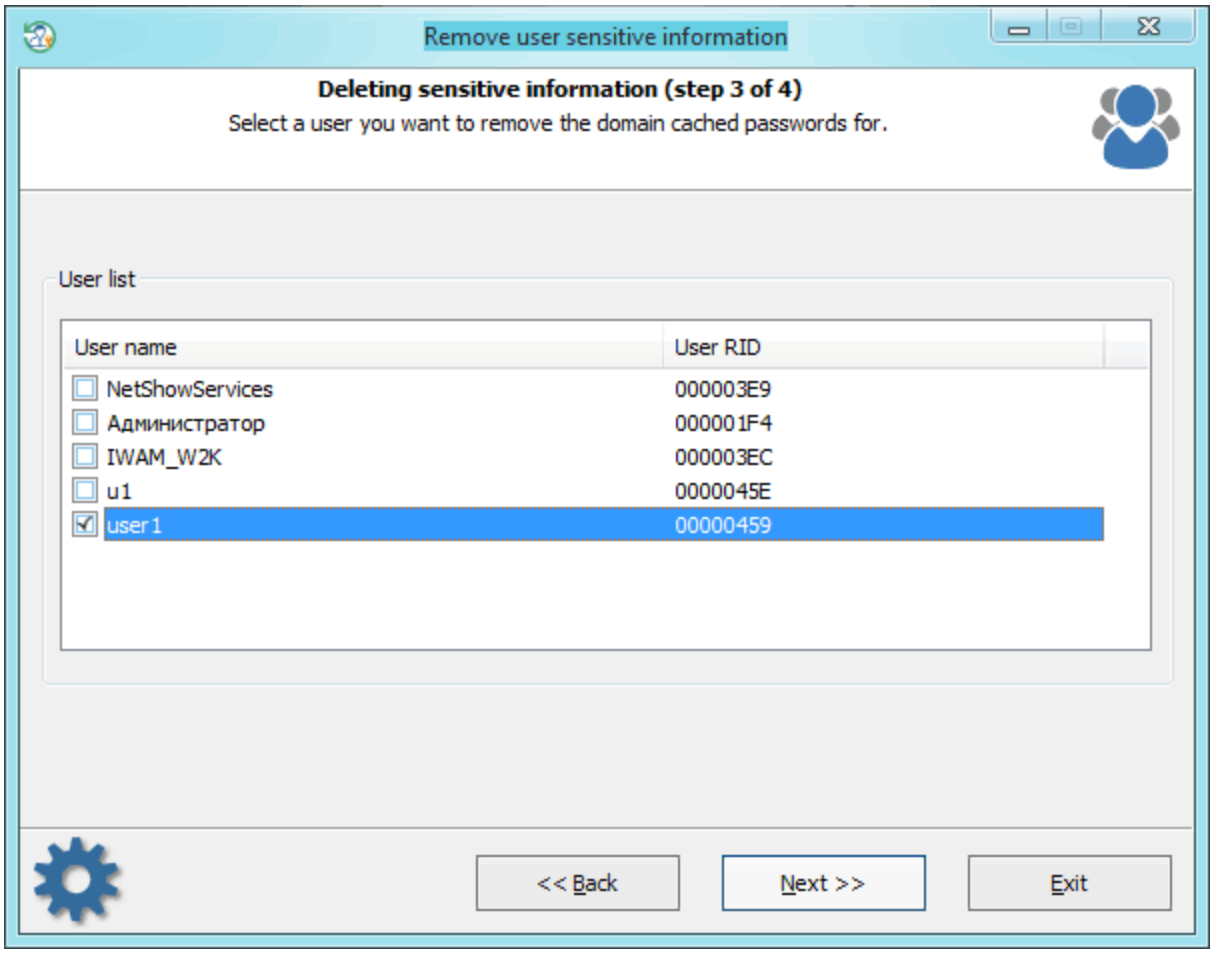
Haga clic en <<Eliminar>> y deshágase de la información innecesaria de forma permanente.

3.18.5.2 Eliminación de contraseñas almacenadas en caché de dominio

Selección del origen de datos

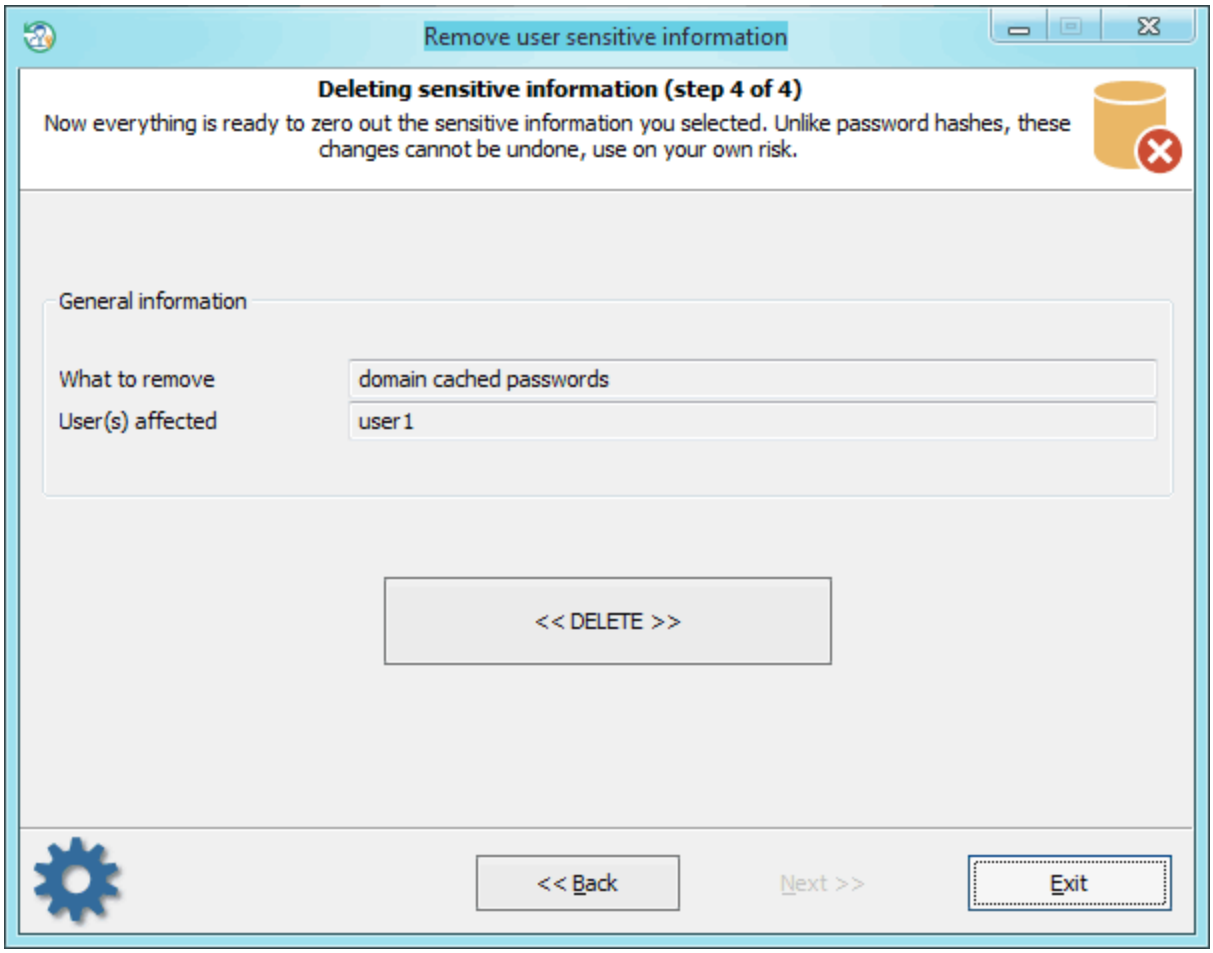


Selección de la cuenta de usuario



Elegir la cuenta para la que desea eliminar las contraseñas.

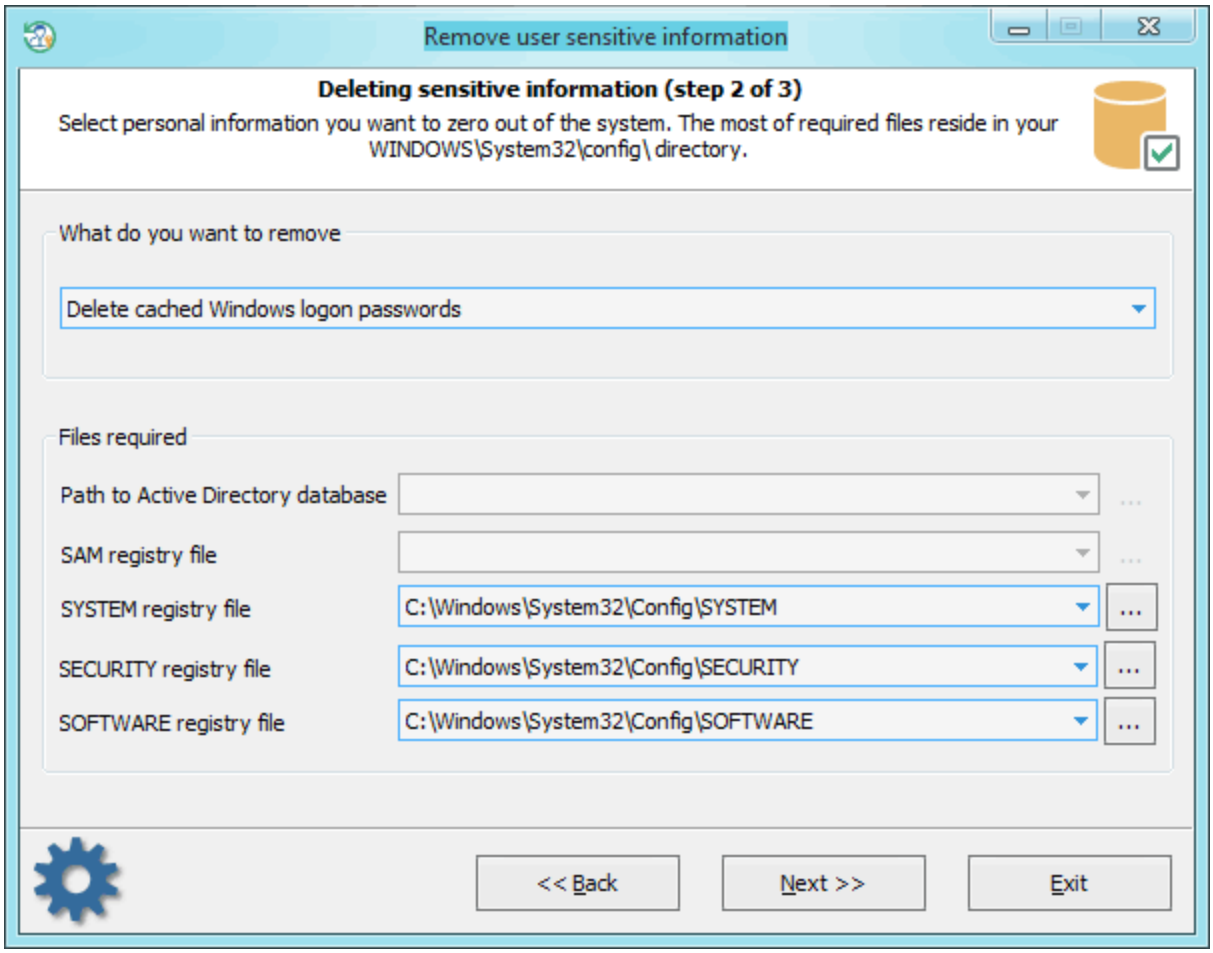
Deleting domain cached passwords



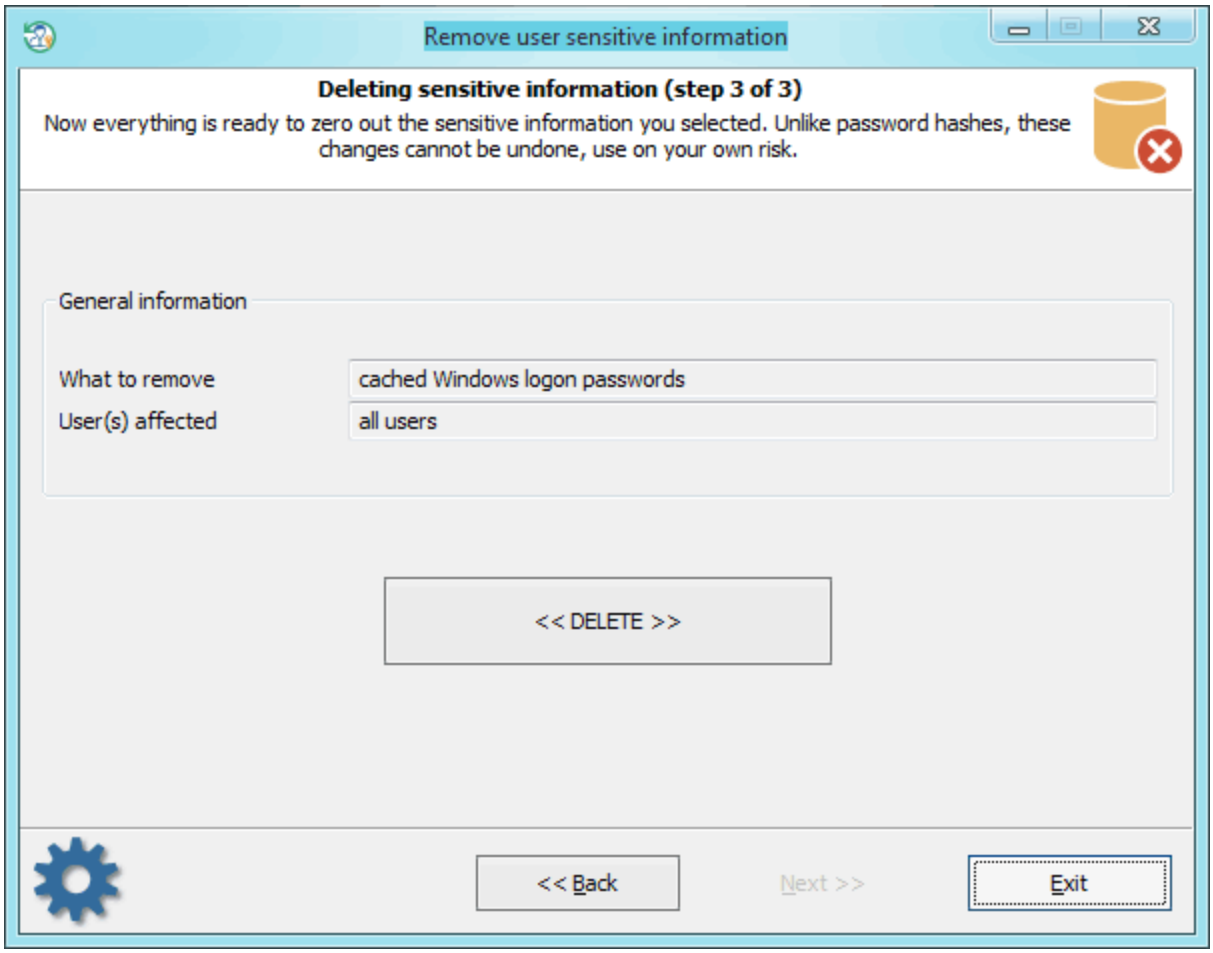
Simplemente confirme la eliminación de todas las contraseñas almacenadas en caché de dominio para la cuenta de usuario1.

3.18.5.3 Eliminación de la contraseña de inicio de sesión almacenada en caché

Selección del origen de datos



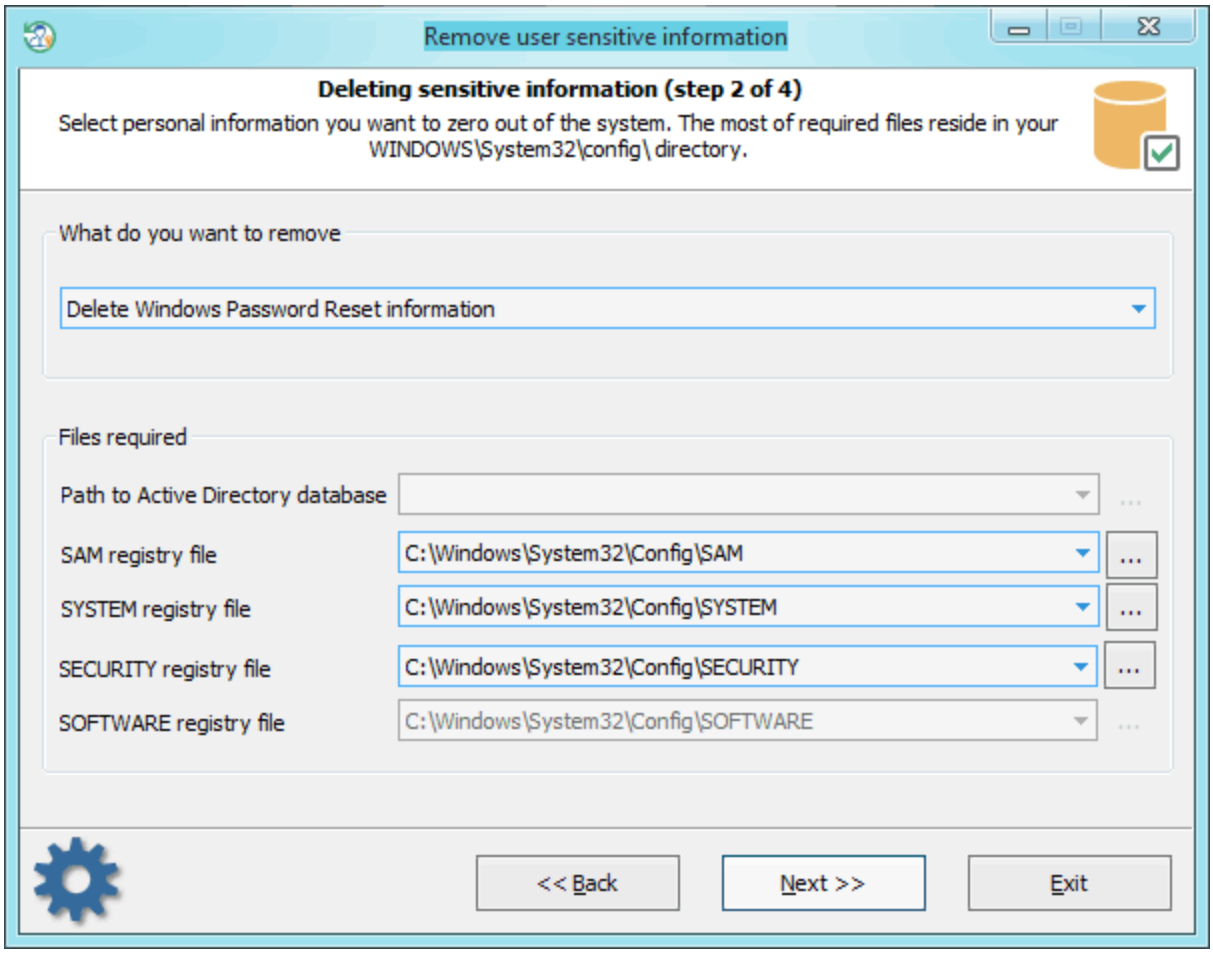
Eliminación de la contraseña de inicio de sesión en caché de Windows



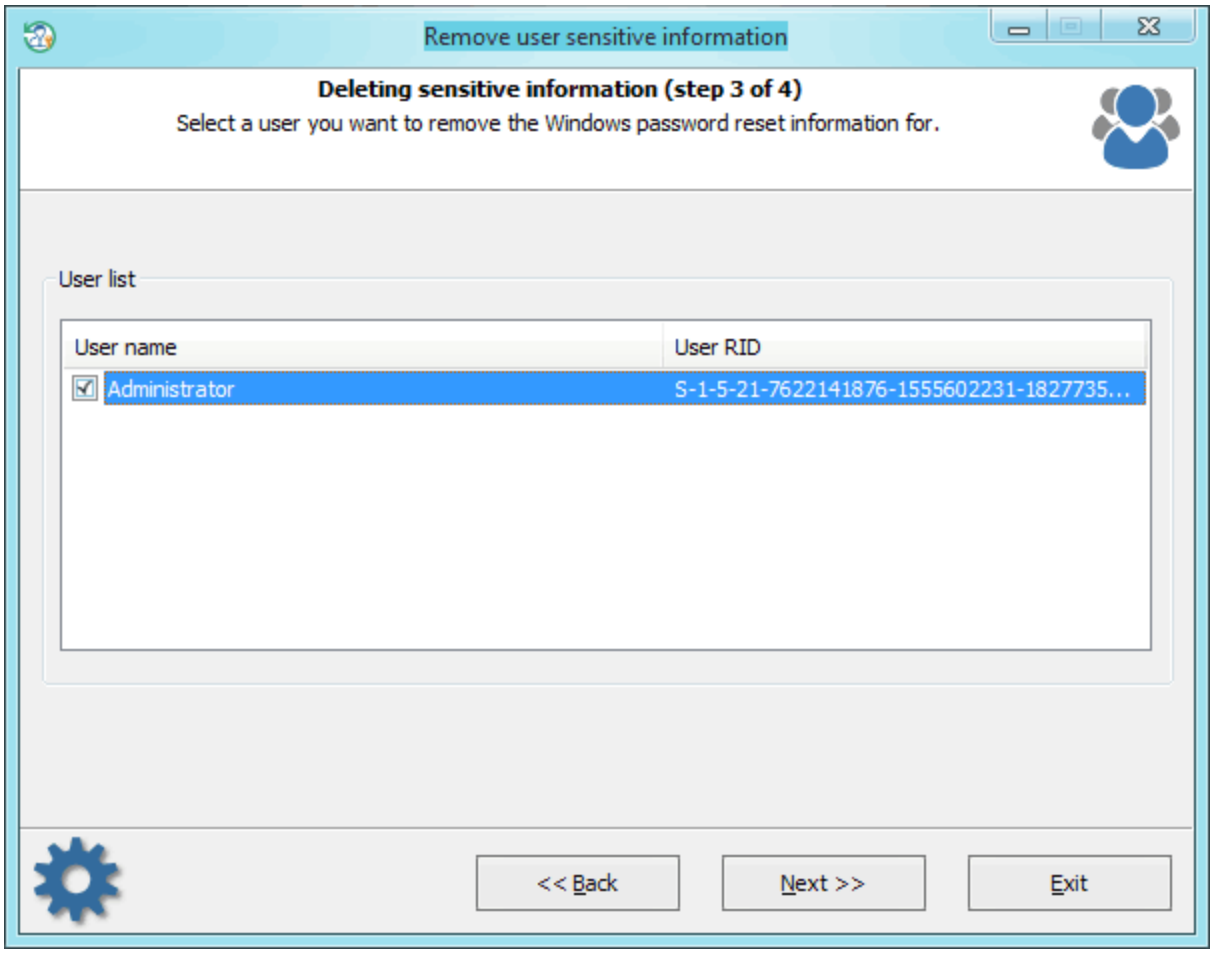
Y confirme la eliminación permanente de las contraseñas de inicio de sesión almacenadas en caché.

3.18.5.4 Eliminación de la información del disco de restablecimiento de contraseña

Selección del origen de datos

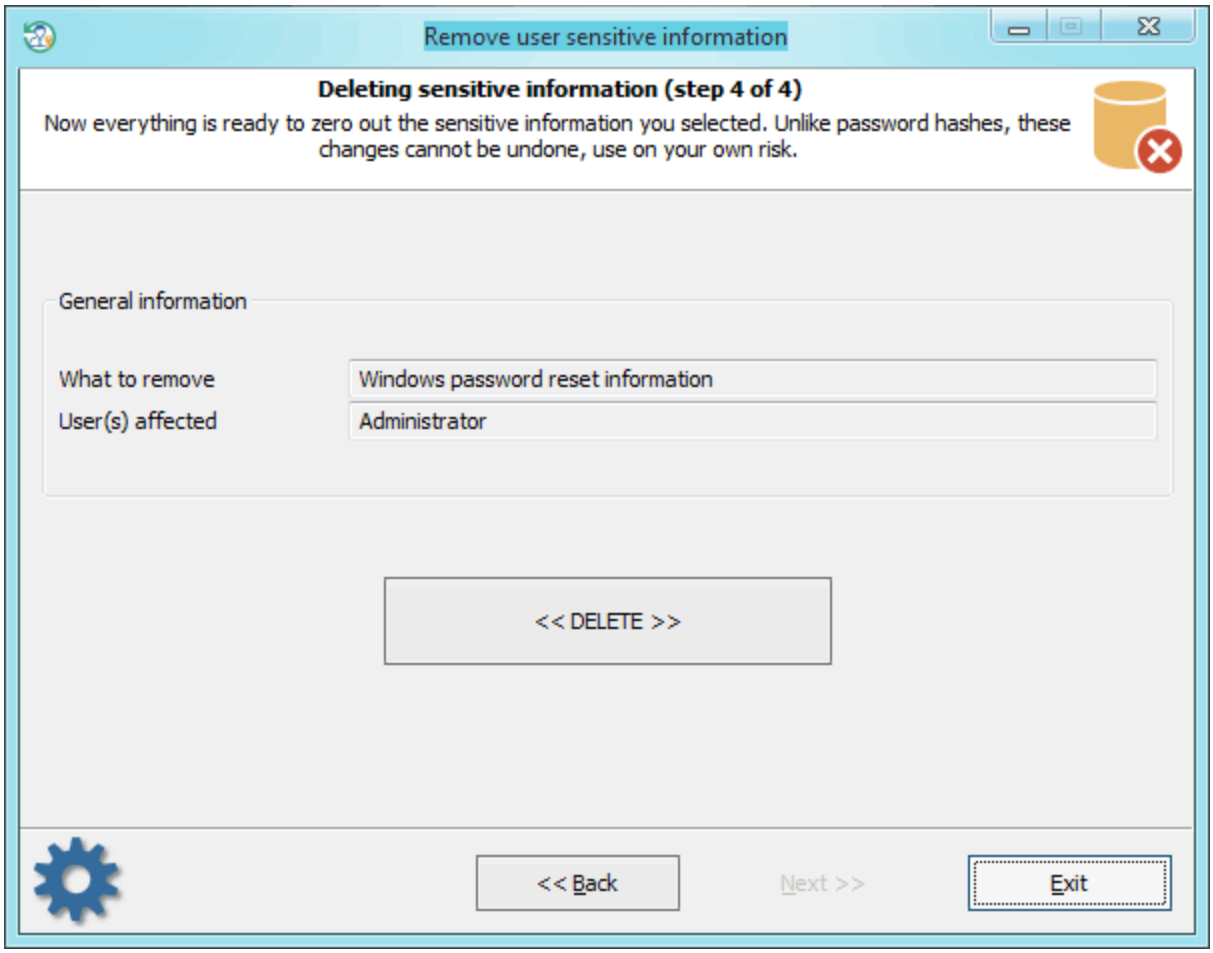


Selección de la cuenta de usuario



Comprobar el usuario cuya información queremos eliminar. Al crear un disco de restablecimiento de contraseña, la contraseña cifrada del usuario se almacena en el registro. Mientras que el disquete almacena la clave de cifrado. Eliminar la contraseña cifrada del registro hace que la existencia adicional del disquete de restablecimiento de contraseña sea inútil.

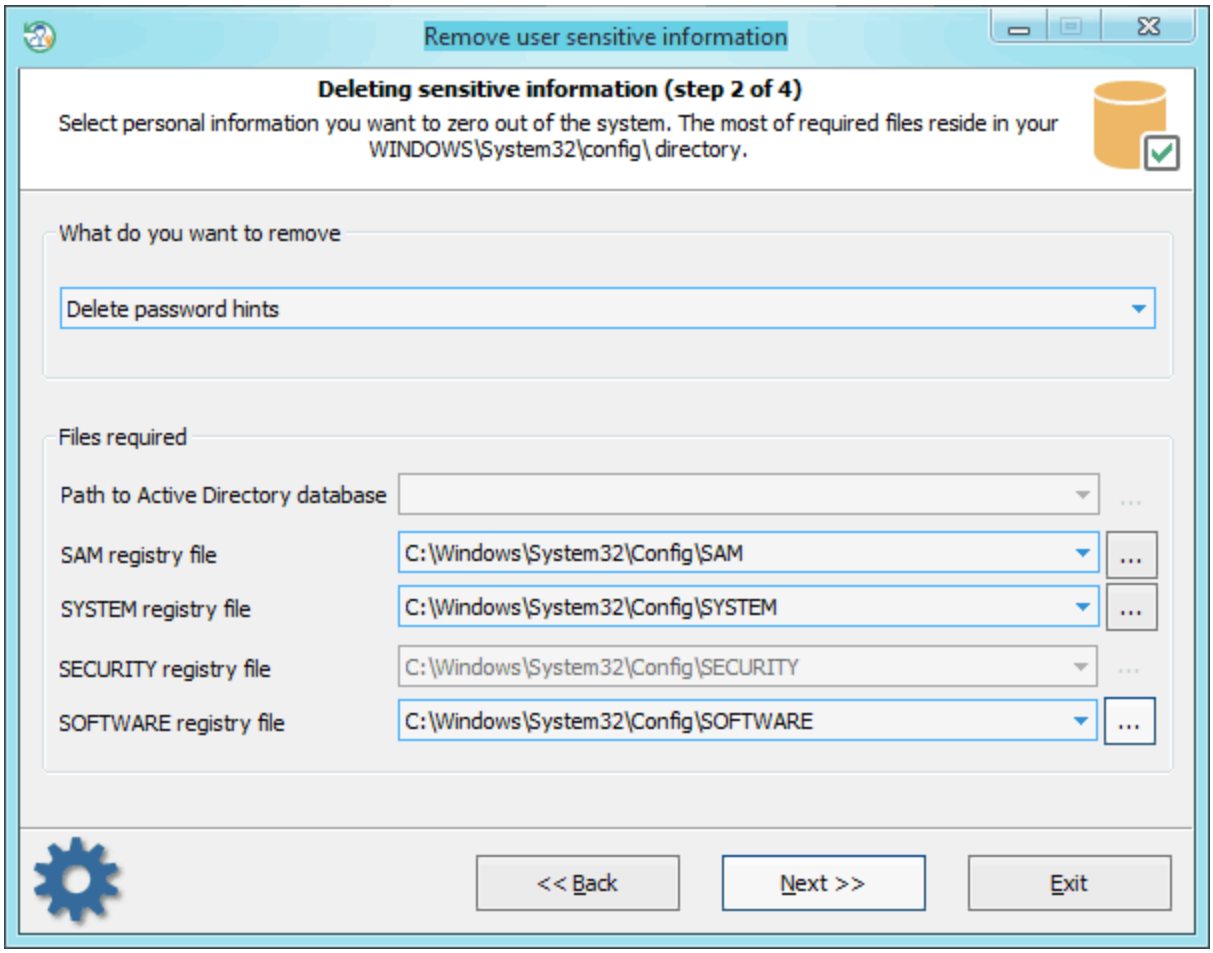
Eliminación de la información del disquete de restablecimiento de contraseña



Confirme la eliminación.

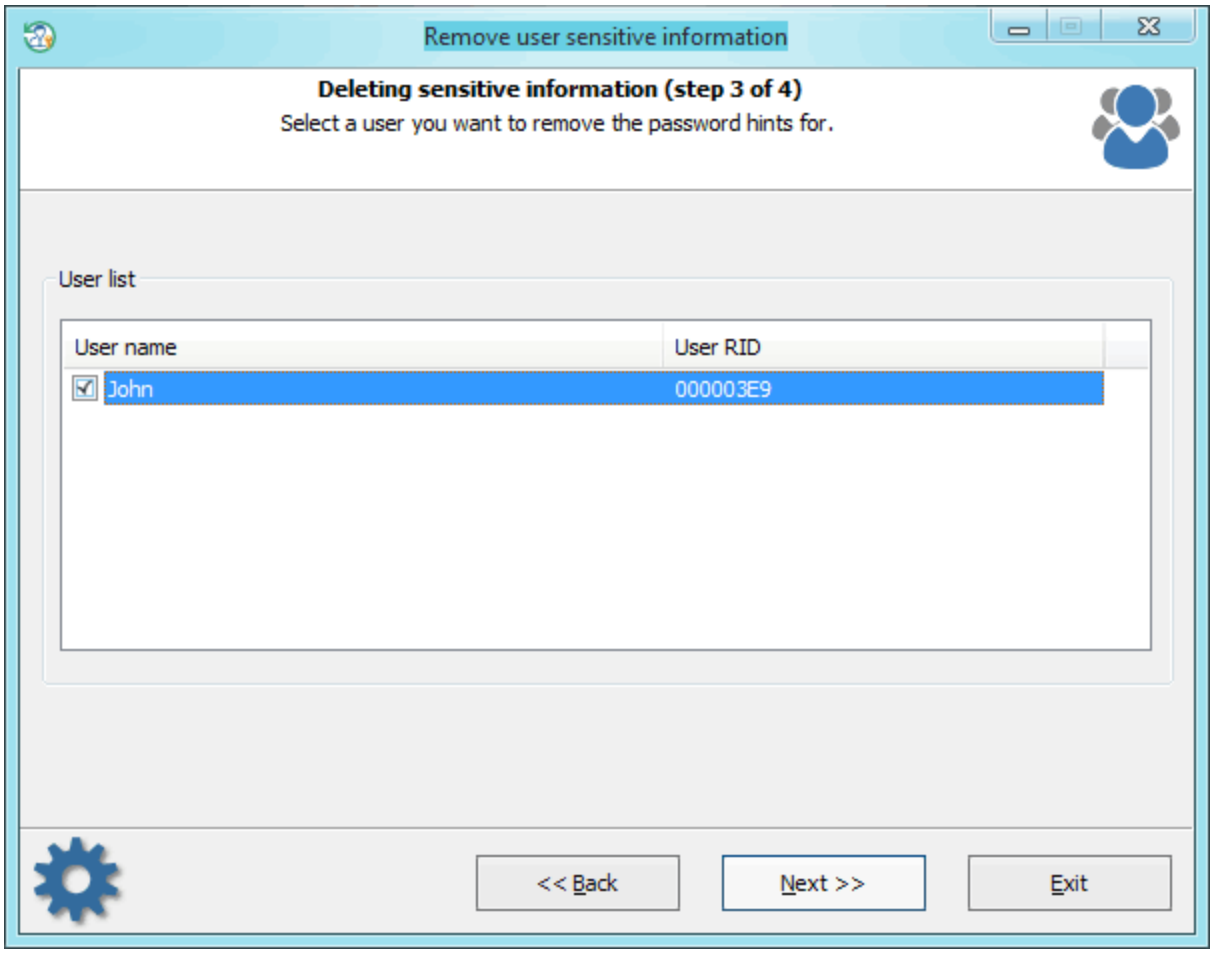
3.18.5.5 Eliminación de sugerencias de contraseña

Selección del origen de datos



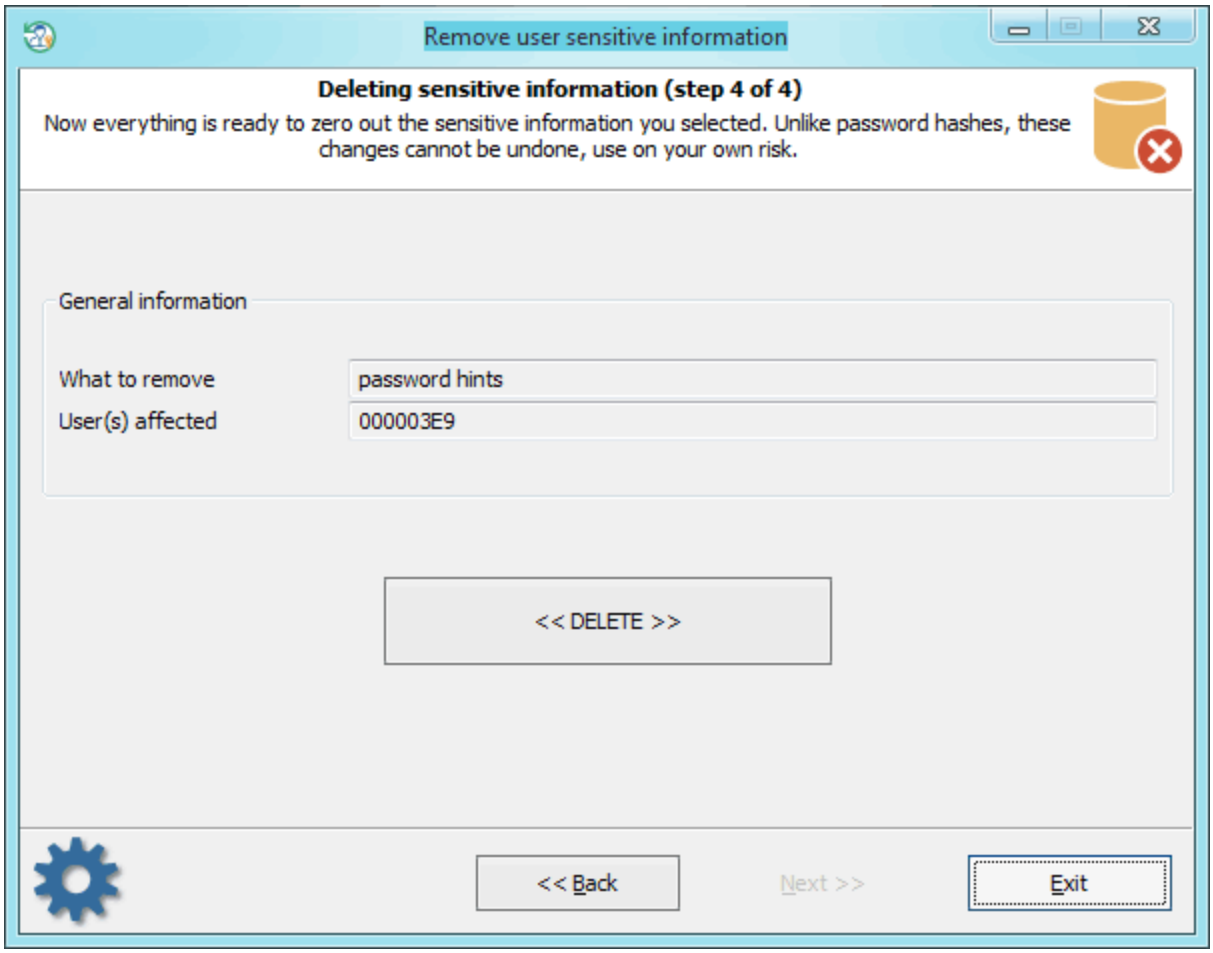
Las sugerencias de contraseña se almacenan en el registro software (Windows XP, Windows 2003) o en el archivo SAM (Windows Vista y sistema operativo superior). El descifrado también requerirá el archivo SYSTEM.

Selección de la cuenta de usuario



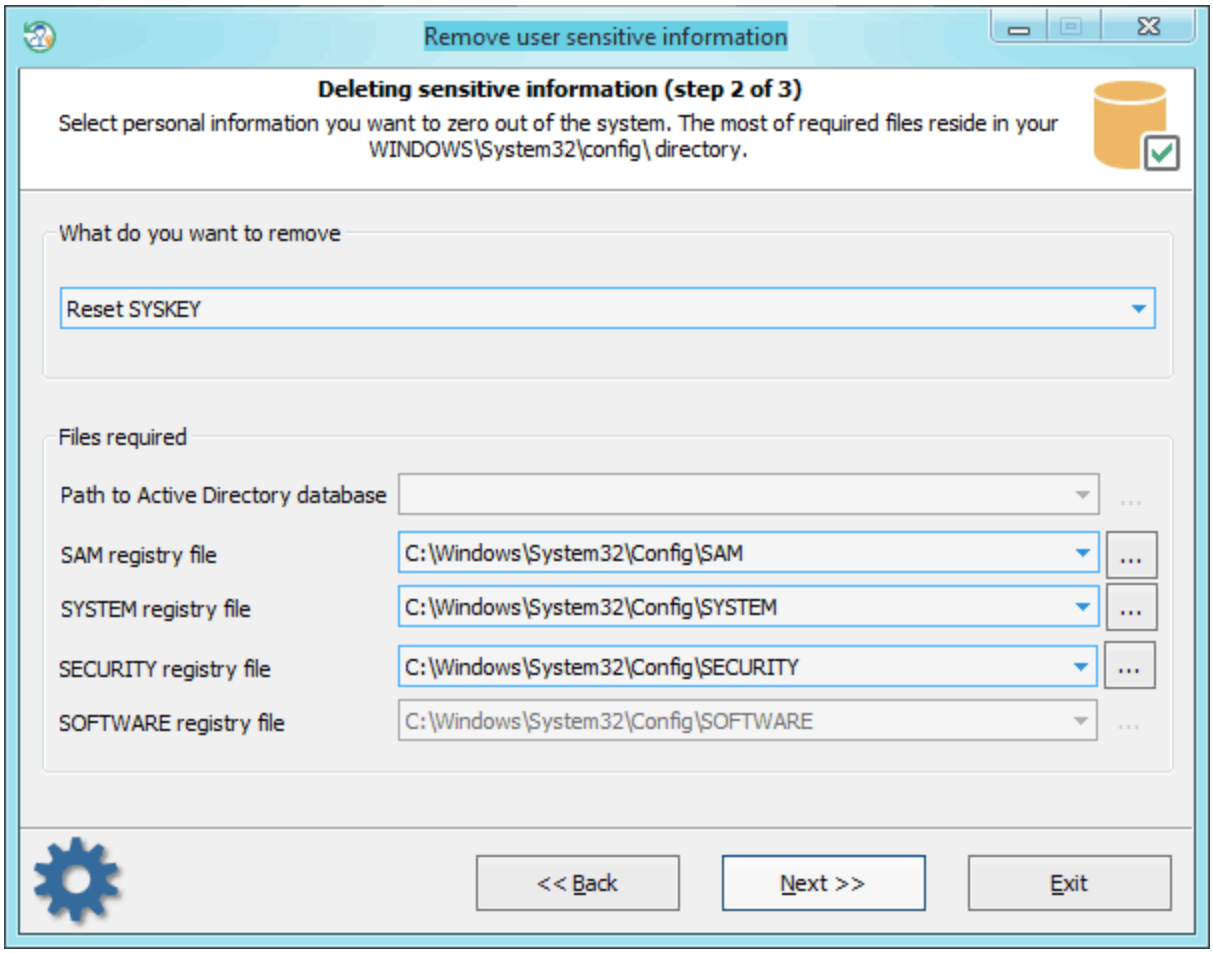
Seleccione el usuario cuya sugerencia se va a borrar del sistema y, a continuación, siga el cuadro de diálogo de eliminación final.

Eliminación de sugerencias



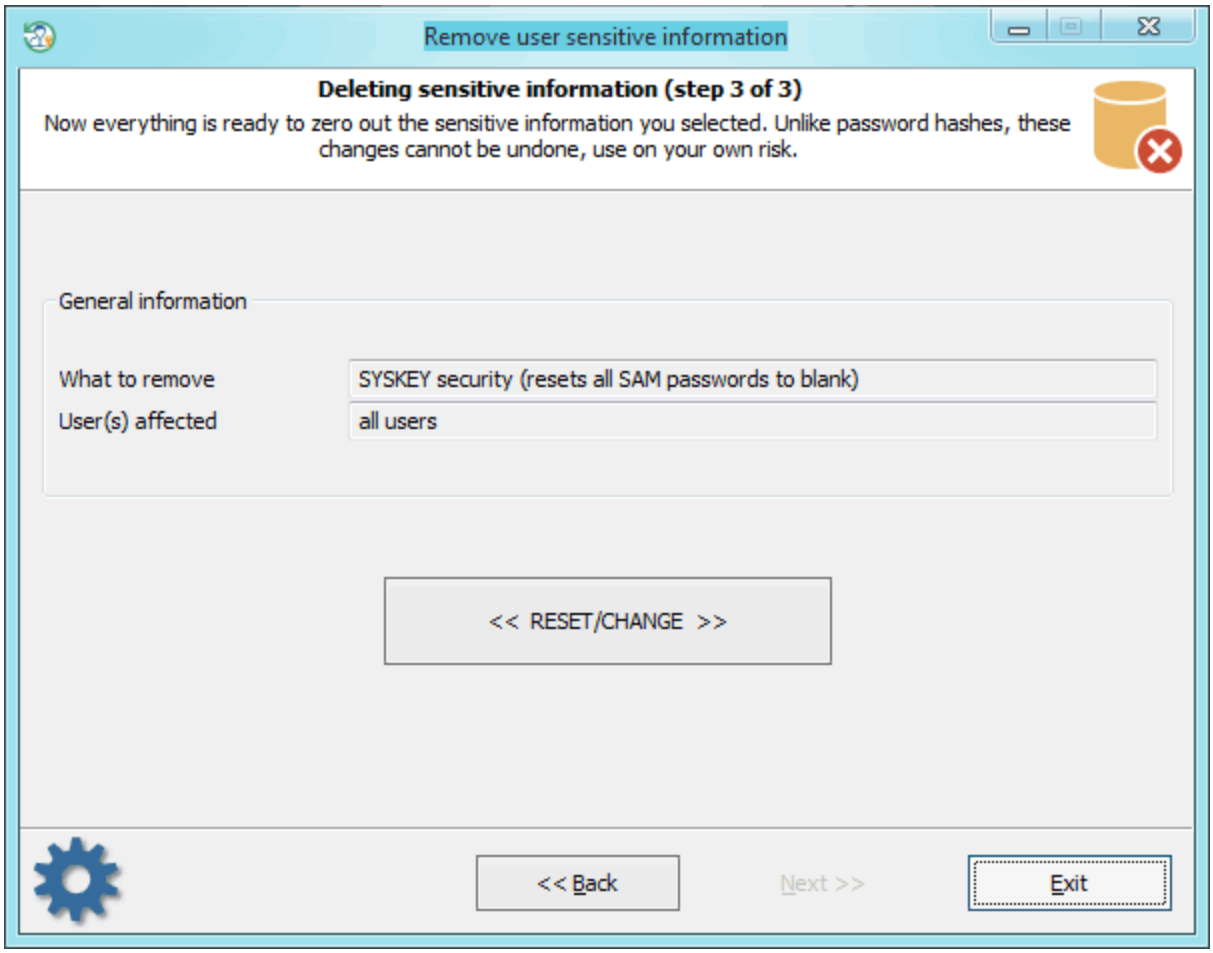
3.18.5.6 Restablecimiento de SYSKEY

Selección del origen de datos



Primero debe seleccionar 3 subárboles de registro: **SAM**, **SYSTEM** y **SECURITY**. Usualmente SYSKEY reside en tu registro SYSTEM debajo de la llave **HKLM\CurrentControlSet\Control\Lsa**. Pero una vez que configuras tu SYSKEY por ejemplo, para requerir una contraseña de inicio de arranque y olvidarla, no hay posibilidad de iniciar su sistema. No hace falta decir que SYSKEY es una herramienta extremadamente efectiva en manos de un gurú. Configurar su SYSKEY para requerir una contraseña de inicio o un disquete de arranque es muy efectivo contra CUALQUIER(!) crackeador de contraseñas de Windows. En ese caso, un programa extractor de contraseñas no puede descifrar los hashes de su contraseña, incluso si obtiene un acceso completo a su sistema.

Restableciemiento de SYSKEY

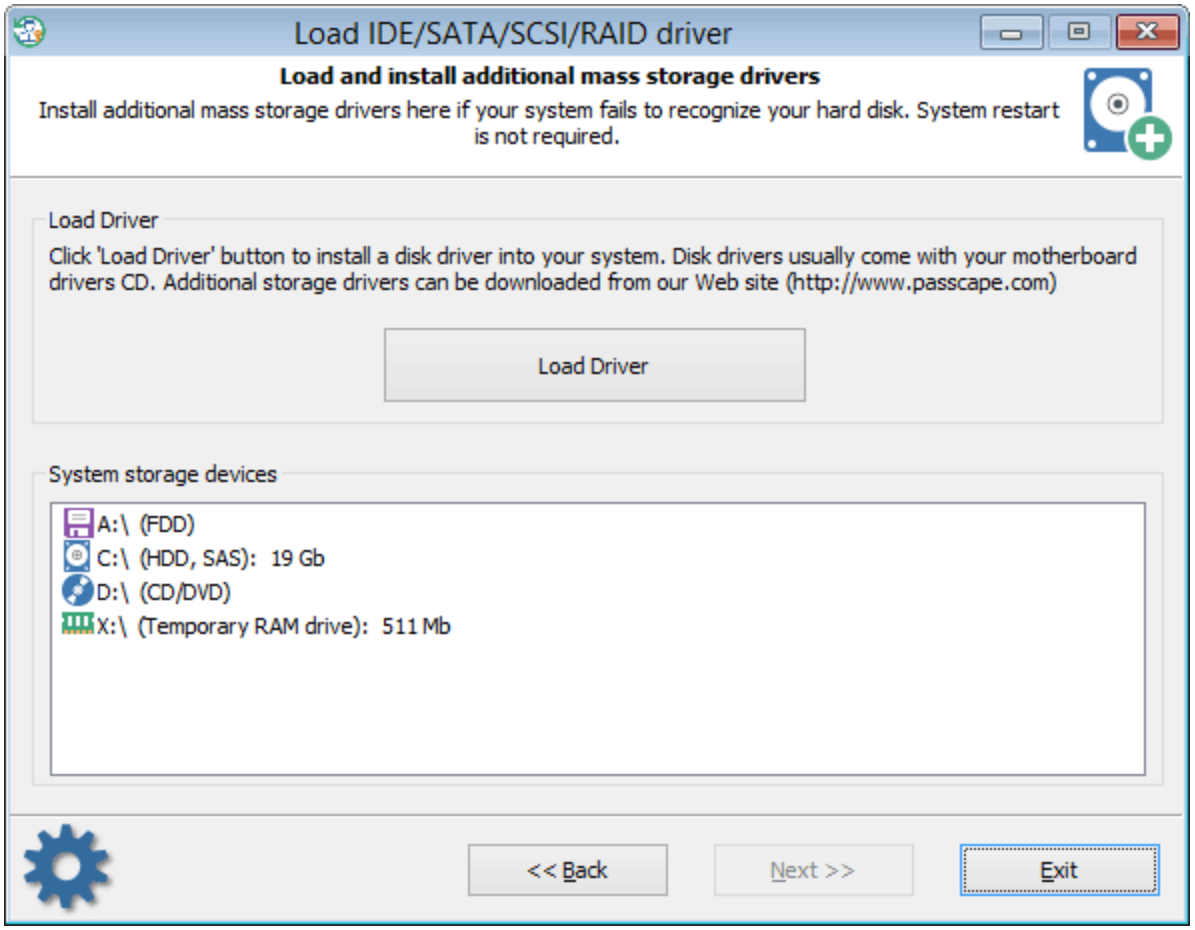


Nota! El restablecimiento de SYSKEY es una operación no segura que afecta a la seguridad de todo el sistema. Por ejemplo, después de restablecer SYSKEY, incluso si puede iniciar sesión en su sistema, no podrá descifrar sus archivos protegidos por EFS, todas las contraseñas protegidas por DPAPI (por ejemplo. Contraseñas guardadas de Outlook) también se descartarán.

Hay una serie de programas en la red que proclaman que pueden restablecer SYSKEY. Pero ninguno de ellos funciona correctamente en este momento. La razón es que el restablecimiento de SYSKEY requiere muchas operaciones adicionales para que su sistema evite que se rompa. Por ejemplo, también debe poner a cero las claves de sesión de dominio SAM, volver a cifrar y restablecer los hashes de usuario locales, los secretos LSA, etc. **Reset Windows Password** tiene 2 algoritmos para restablecer SYSKEY. Una vez que el primario falla, otro se ejecuta. Después de restablecer SYSKEY, todas las contraseñas de usuario locales se establecerán en blanco automáticamente.

Nota! Después de restablecer SYSKEY en un sistema operativo Windows 8 y posteriores, debe cambiar la contraseña de cada cuenta LiveID/Microsoft a una no vacía. De lo contrario, no podrá iniciar sesión en el sistema con la contraseña vacía.

3.18.6 Carga de controladores de disco duro adicionales



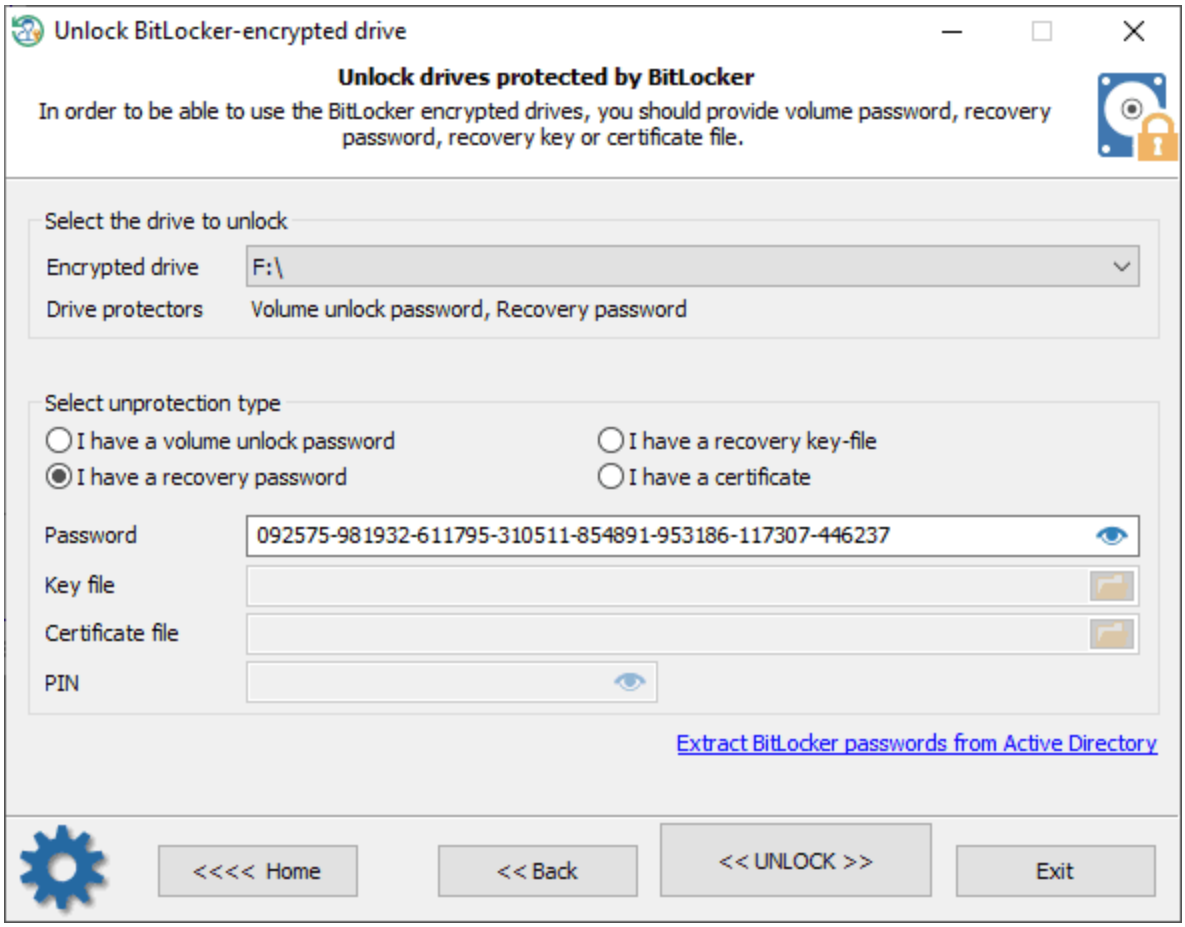
Si cuando se inició la aplicación no pudo detectar una o varias unidades de disco duro, lo más probable es que necesite instalar un controlador para ese dispositivo. En la ventana principal, en la lista de tareas, seleccione '*Cargar controlador IDE/SATA/SCSI/RAID/NVME*' y vaya al cuadro de diálogo de instalación del controlador. El software viene con varios controladores de controlador de disco duro populares: ATI, Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware.

Todos ellos se almacenan en la carpeta **X:\Apps\Drivers**. Por ejemplo, si su controlador de disco duro se basa en el chipset Nvidia, cargue el *correspondiente. Archivo INF de la carpeta X:\Apps\Drivers\Nvidia.

Normalmente, cuando compra una NUEVA PC, se carga con un CD con la placa base y los controladores del disco duro. Puede, e incluso se le recomienda encarecidamente que use ese disco para instalar controladores para los dispositivos que faltan. Ten cuidado; ¡los controladores deben ser compatibles con el sistema operativo Windows 10 x64! Consulte el manual de la placa base para obtener más información sobre la instalación de los controladores.

En Reset Windows Password, los controladores se instalan "sobre la marcha"; por lo tanto, no es necesario reiniciar el sistema. Al finalizar, los dispositivos encontrados deben aparecer en la lista de dispositivos de almacenamiento de datos. Una vez que se instala el controlador requerido y se encuentra la unidad de disco duro, puede continuar con los siguientes pasos.

3.18.7 Desbloquear unidades cifradas de Bitlocker



Bitlocker es un cifrado de unidad completo. Se introdujo por primera vez en Windows Vista y tiene como objetivo proteger sus datos incluso si alguien tiene acceso físico a su PC o computadora portátil.

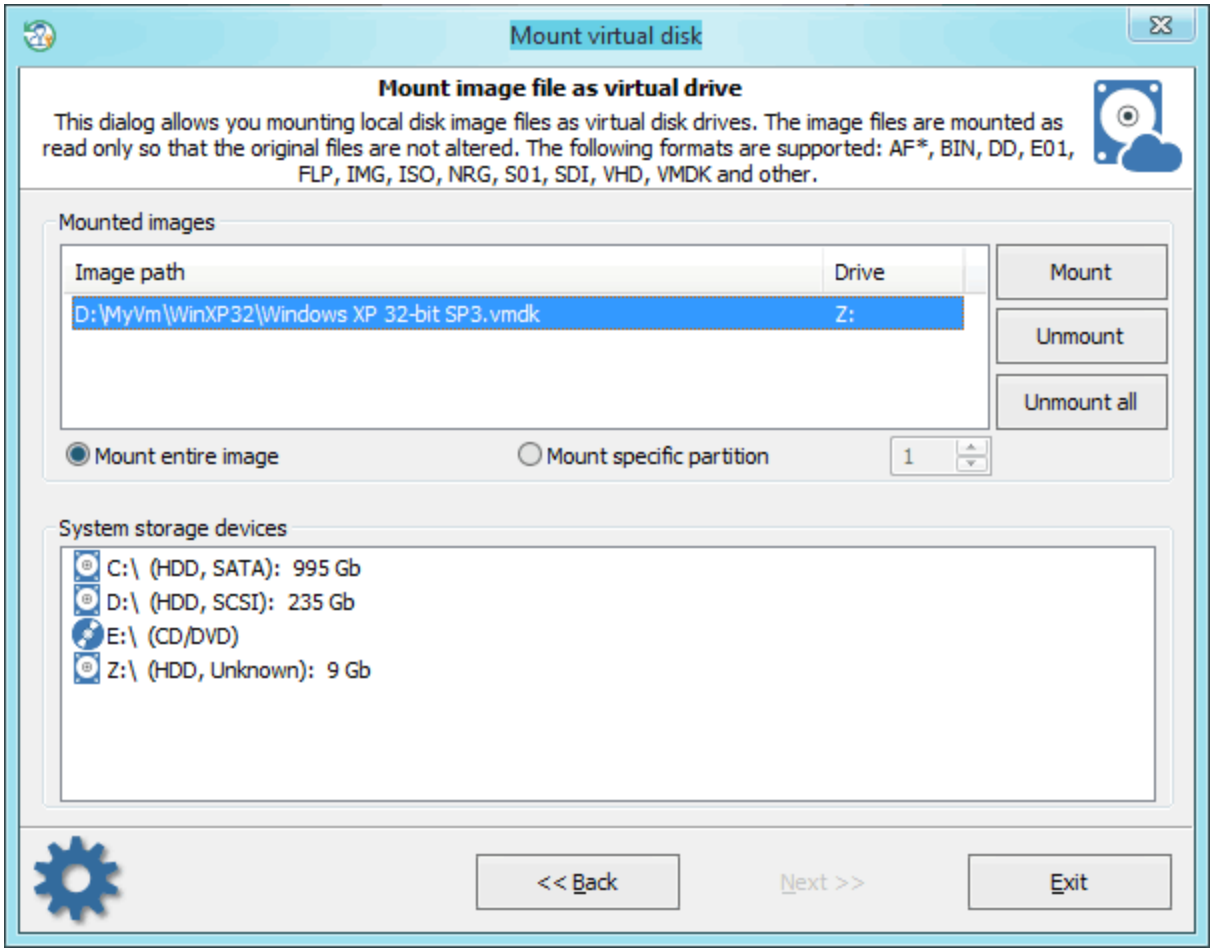
BitLocker cifra todos los archivos de una unidad, incluidos los necesarios para el inicio. Así que su contenido es invisible para el sistema. Para desbloquear la unidad y obtener acceso a su contenido, debe utilizar uno de los siguientes métodos de desprotección:

- Desbloquee la unidad con la contraseña de desbloqueo de volumen
- Desbloqueo mediante contraseña de recuperación (numérica)
- Desbloquear usando la clave de recuperación externa
- Desbloqueo mediante el certificado de Bitlocker

Simplemente seleccione su unidad cifrada con Bitlocker junto con el tipo de desbloqueo requerido y haga clic en el botón << *DESBLOQUEAR* >> para descifrarlo. La operación dura varios segundos.

Para obtener una contraseña de recuperación de BitLocker almacenada en un dominio, haga clic en el link *'Extraer contraseñas de BitLocker de Active Directory'* y siga las instrucciones del programa.

3.18.8 Montaje de unidades virtuales



Este cuadro de diálogo le permite montar una imagen de disco en el sistema como unidad virtual. A continuación, puede hacer referencia a la nueva unidad por su letra de volumen. Las imágenes se montan como de solo lectura para que el archivo original no se altere. Se admiten los siguientes formatos:
AF*, BIN, DD, E01, FLP, IMG, ISO, NRG, S01, SDI, VHD, VMDK y algunos otros.

Si necesita adjuntar una imagen cifrada con BitLocker, primero monte el archivo de imagen y, a continuación, desbloquearlo con una contraseña o clave de recuperación conocida.

Tenga paciencia, el montaje de algunos tipos de imágenes puede tardar hasta varios minutos en completarse.

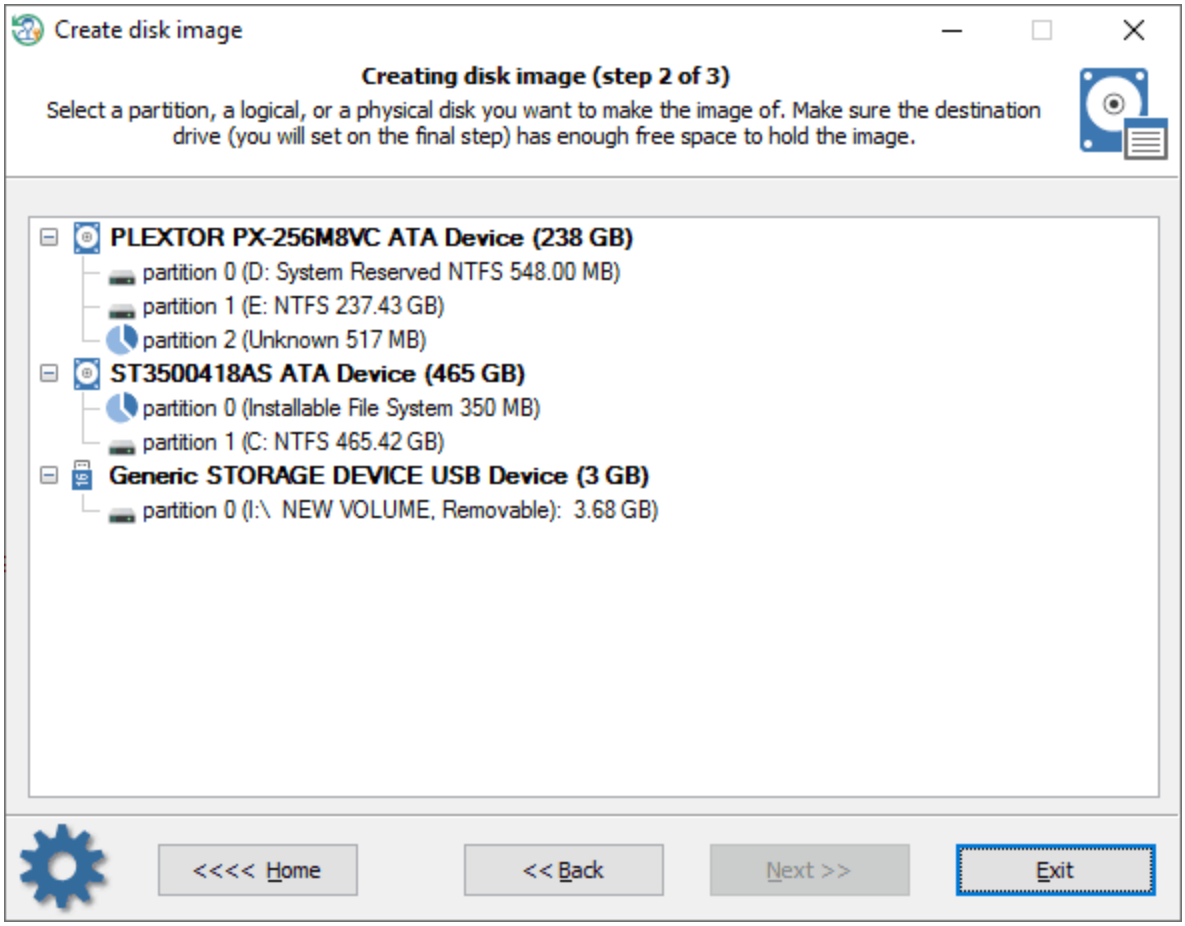
3.18.9 Crear imagen de disco

A veces, cuando Windows se corrompe o su disco duro se bloquea, es una buena idea hacer una copia de seguridad de todo el contenido de su unidad, incluido el cifrado del disco, el estado del sistema operativo, la configuración, las contraseñas, las aplicaciones y controladores instalados, toda su información personal, etc. Una de las formas más fáciles de hacerlo es crear una imagen de todo el disco duro.

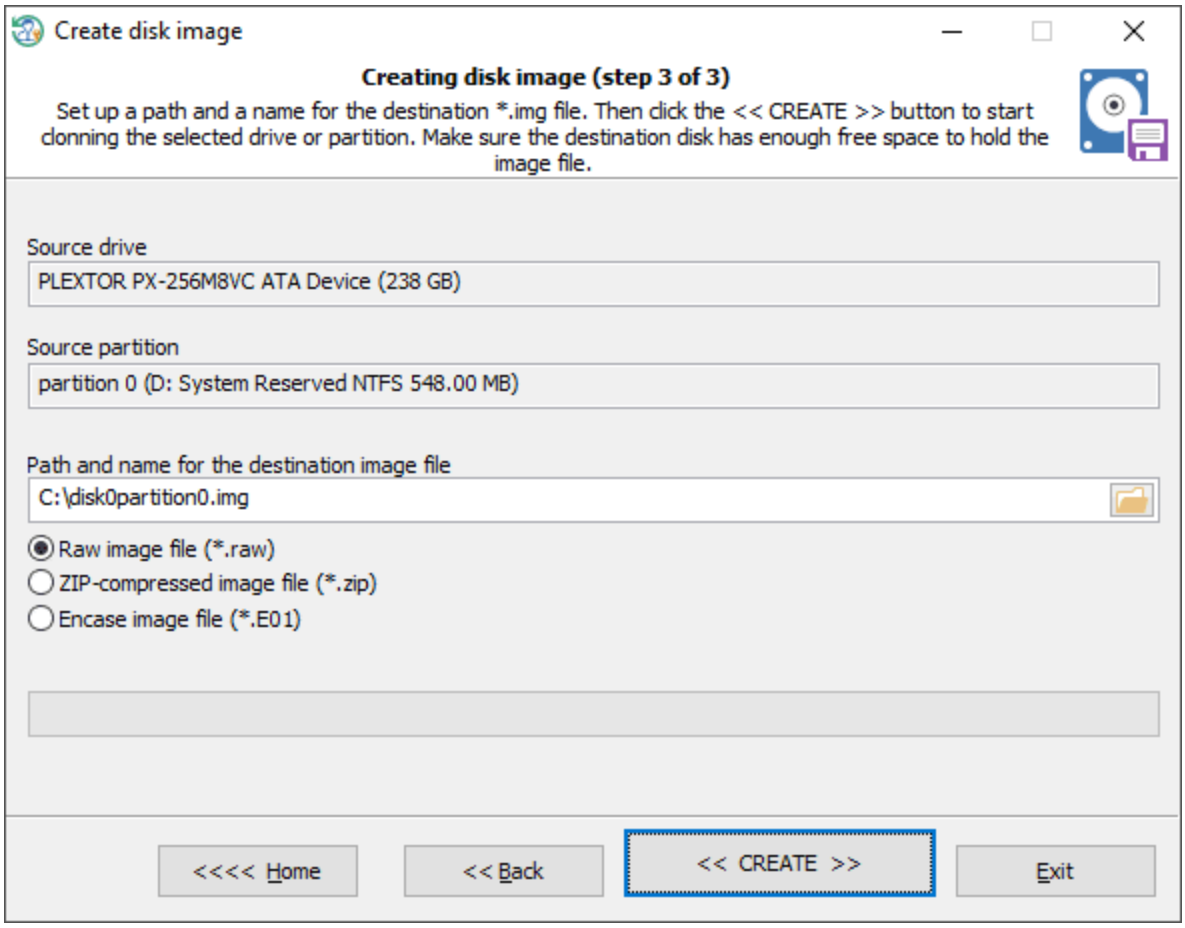
A veces, cuando Windows se corrompe o su disco duro se bloquea, es una buena idea hacer una copia de seguridad de todo el contenido de su unidad, incluido el cifrado del disco, el estado del sistema operativo, la configuración, las contraseñas, las aplicaciones y controladores instalados, toda su información personal, etc. Una de las formas más fáciles de hacerlo es crear una imagen de todo el disco duro.

En forense, una imagen de disco es imprescindible y permite ahorrar algo de tiempo durante la investigación inicial y garantizar que no se pierda nada importante durante un análisis más profundo.

Crear una imagen de disco en RWP es extremadamente simple.



En el primer cuadro de diálogo, el programa muestra una lista de particiones encontradas y unidades de disco a las que pertenecen las particiones. Seleccione una partición o el disco cuya imagen desea crear.



En el cuadro de diálogo final, establezca el nombre de la imagen y la ruta de destino en la que se guardará la imagen. Tenga en cuenta que la ruta de destino debe estar ubicada en otra unidad física. Asegúrese de tener suficiente espacio libre para contener todo el archivo de imagen. Haga clic en el botón '<< Crear >>' para iniciar la creación de la imagen de disco. Tenga paciencia, puede llevar algún tiempo y depende de la velocidad de sus unidades de origen y destino.

Opcionalmente, la compresión de imágenes está disponible. Una vez configurado, el archivo de imagen de salida se comprimirá en un archivo zip.

Licencia y registro

4 Licencia y registro

4.1 Acuerdo de licencia

==========
CONTRATO DE LICENCIA DE SOFTWARE
==========

IMPORTANTE-LEA DETENIDAMENTE: Este es el Acuerdo de licencia de usuario final (el "Acuerdo") es un acuerdo legal entre usted, el usuario final, y Passcape Software, el fabricante y el propietario de los derechos de autor, para el uso del producto de software "Reset Windows Password" software product ("SOFTWARE").

Todos los derechos de autor del SOFTWARE son propiedad exclusiva de Passcape Software.

El SOFTWARE y cualquier documentación incluida en el paquete de distribución están protegidos por las leyes nacionales de derechos de autor y los tratados internacionales. Cualquier uso no autorizado del SOFTWARE dará lugar a la terminación inmediata y automática de esta licencia y puede dar lugar a un proceso penal y/o civil.

Se le concede una licencia no exclusiva para utilizar el SOFTWARE como se establece en este documento.

Puede utilizar la versión de prueba del SOFTWARE todo el tiempo que desee, pero para acceder a todas las funciones debe comprar la versión completamente funcional. Tras el pago, le proporcionamos el enlace de descarga y el código de registro al SOFTWARE.

Una vez registrado, se concede al usuario una licencia no exclusiva para utilizar el SOFTWARE en un ordenador a la vez por cada licencia de usuario único adquirida.

Con la licencia personal, puede utilizar el SOFTWARE como se establece en este Acuerdo para fines no comerciales en entornos no comerciales y no comerciales. Para utilizar el SOFTWARE en un entorno corporativo, gubernamental o empresarial, debe comprar una licencia comercial. Con la licencia comercial puede ejecutar el SOFTWARE en varios equipos dentro de una sola organización.

El SOFTWARE registrado no puede ser alquilado o arrendado, pero puede ser transferido permanentemente junto con la documentación adjunta, si la persona que lo recibe acepta los términos de esta licencia. Si el software es una actualización, la transferencia debe incluir la actualización y todas las versiones anteriores.

La versión no registrada (de prueba) del SOFTWARE puede distribuirse libremente, siempre que el paquete de distribución no se modifique. Ninguna persona o empresa puede cobrar una tarifa por la distribución del SOFTWARE sin el permiso por escrito del titular de los derechos de autor.

No puede crear ninguna copia del SOFTWARE. Puede hacer una (1) copia del SOFTWARE para fines de copia de seguridad y archivo, siempre que, sin embargo, el original y cada copia se mantengan en su posesión o control, y que su uso del SOFTWARE no exceda lo permitido en este Acuerdo.

Usted acepta no modificar, descompilar, desensamblar, realizar ingeniería inversa del SOFTWARE, a menos que dicha actividad esté expresamente permitida por la ley aplicable.

Passcape Software no garantiza que el software sea apto para ningún propósito en particular. Passcape Software renuncia a todas las demás garantías con respecto al SOFTWARE, ya sean expresas o

implícitas. Algunas jurisdicciones no permiten la exclusión de garantías implícitas o limitaciones sobre cuánto tiempo puede durar una garantía implícita, por lo que las limitaciones o exclusiones anteriores pueden no aplicarse a usted.

El programa que se le otorga la licencia es absolutamente legal y puede usarlo siempre que sea el propietario legal de todos los archivos o datos que vaya a recuperar mediante el uso de nuestro SOFTWARE o tenga permiso del propietario legítimo para realizar estos actos. Cualquier uso ilegal de nuestro SOFTWARE será de su exclusiva responsabilidad. En consecuencia, usted afirma que tiene el derecho legal de acceder a todos los datos, información y archivos que han sido ocultados.

Además, usted atestigua que los datos, contraseñas y/o archivos recuperados no se utilizarán para ningún propósito ilegal. Tenga en cuenta que la recuperación de contraseñas y el descifrado de datos secuente de archivos no autorizados u obtenidos ilegalmente pueden constituir un robo u otra acción ilícita y pueden resultar en su enjuiciamiento civil y (o) penal.

4.2 Registro

El software está disponible en tres ediciones: Light, Standard y Advanced. La lista detallada de características es mostrado aquí. Puede solicitar la versión completamente registrada de Reset Windows Password a un costo de $ 45 para Light Edition (uso personal), $ 145 para Standard Edition (uso personal) o $ 345 para Advanced Edition (licencia comercial).

Las instrucciones detalladas para todo tipo de pedidos están disponibles en línea en Página de pedidos de Passcape. Los pedidos en línea se adquieren en solo unos minutos las 24 horas del día, los 7 días de la semana. Las páginas de pedidos se encuentran en un servidor seguro, lo que garantiza que su información privada permanezca confidencial.

Tan pronto como se procese su pedido, se le proporcionará el enlace a la versión completa del programa. Si ha realizado un pago, pero no ha recibido una carta de confirmación con el enlace dentro de un período de tiempo razonable, ¡notifíquenoslo!

Importante: al completar el formulario de pedido, verifique que su dirección de correo electrónico sea correcta. Si no es así, no podremos enviarle el código de registro.

Para completar el proceso de registro, debe descargar el programa utilizando el enlace que se le envió en su correo electrónico de registro y seguir las instrucciones para crear un disco de arranque.

4.3 Limitación de la versión no registrada

Una versión no registrada de **Reset Windows Password** muestra solo los primeros 3 caracteres de las contraseñas recuperadas y tiene algunas limitaciones funcionales. En particular, solo las funciones de volcado de hashes y copia de seguridad de contraseña funcionan sin ninguna limitación. La versión registrada elimina todas las restricciones.

4.4 Ediciones del programa

Reset Windows Password viene en tres ediciones: Light, Standard y Advanced. La lista detallada de características se muestra a continuación.

CARACTERÍSTICA	Light	Stan-dard	Advan-ced
Compatibilidad con estaciones de trabajo Windows NT/2000/XP/Vista/7/8/10	+	+	+
Soporte para servidores NT/2000/2003/2008/2012/2016/2019	+	+	+
Compatibilidad con Windows de 64 bits	+	+	+
Compatibilidad con Windows fuera de EE. UU.	+	+	+
Compatibilidad con contraseñas multilingües	+	+	+
Controladores de almacenamiento masivo adicionales	+	+	+
Detectar múltiples sistemas operativos	+	+	+
Detectar múltiples sistemas operativos	+	+	+
Garantía de devolución de dinero de 14 días	+	+	+
Licencia	personal	personal	business
Soporte para todo tipo de cuentas de Windows, incluyendo Live ID, cuenta de Microsoft, etc.	+	+	+
Crear un CD/DVD de restablecimiento de contraseña de arranque	+	+	+
Crear un USB de arranque de restablecimiento de contraseña	+	+	+
Crear un disco duro de arranque de restablecimiento de contraseña.	.+	+	+
Compatibilidad con el arranque en equipos basados en UEFI	+	+	+
Restablecer contraseña de administrador local	+	+	+
Cambiar la contraseña del administrador local	+	+	+
Desbloquear cuenta de administrador local deshabilitada, bloqueada o caducada (1)	+	+	+
Restablecer contraseña de administrador de dominio.	-	-	+
Cambiar la contraseña del administrador de dominio	-	-	+
Desbloquear cuenta de administrador de dominio deshabilitada, bloqueada o caducada (1)	-	-	+
Cambiar las propiedades extendidas de una cuenta de escritorio and flags	+	+	+
Cambiar las propiedades extendidas y los indicadores de las cuentas de Active Directory.	-	-	+
Restablecer contraseña a cuentas normales (SAM)	+	+	+
Cambiar contraseñas a cuentas normales (SAM)	+	+	+
Desbloquear cuenta SAM deshabilitada, bloqueada o caducada (1)	+	+	+
Descifrar preguntas y respuestas secretas para el sistema operativo Windows 10	+	+	+
Restablecer contraseña a cuentas de Active Directory	-	-	+
Cambiar contraseñas a cuentas de Active Directory	-	-	+

CARACTERÍSTICA	Light	Stan-dard	Advan-ced
Desbloquear cuentas de Active Directory deshabilitadas, bloqueadas o caducadas (1)	-	-	+
Restablecer/Cambiar contraseña a la cuenta DSRM (2)	-	-	+
Restablecer contraseña almacenada en caché de dominio	-	+	+
Cambiar la contraseña almacenada en caché del dominio	-	+	+
Carga e instalación instantáneas de cualquier controlador IDE/SATA/SCSI/RAID	+	+	+
Revertir cambios (restaurar contraseñas modificadas anteriormente)	+	+	+
Soporte de cifrado SYSKEY	+	+	+
Soporte de descifrado de contraseña de inicio SYSKEY	+	+	+
Soporte de descifrado de disquete SYSKEY	+	+	+
Mostrar sugerencias de contraseña	+	+	+
Volcar hashes de contraseña LM/NTLM para cuentas normales (SAM)	+	+	+
Volcar hashes del historial de contraseñas	-	+	+
Volcar credenciales de dominio en caché (MSCACHE)	-	+	+
Volcar hashes de contraseña LM/NTLM para cuentas de Active Directory	-	-	+
Recuperación de contraseña para cuentas de usuario de Active Directory (3)	-	-	+
Recuperación de contraseña para cuentas de usuario normales (SAM)	-	+	+
Recuperación de contraseña para cuentas de dominio almacenadas en caché	-	-	+
Buscar contraseñas sencillas	-	+	+
Análisis de diccionario primitivo	-	+	+
Análisis avanzado de diccionarios (4)	-	-	+
Ataque primitivo de fuerza bruta contra contraseñas de usuario	-	+	+
Recuperar contraseñas mediante análisis de Inteligencia Artificial	-	+	+
Recuperación de contraseñas mediante ataques personalizados, incluidos ataques de diccionario, híbridos y máscaras	-	+	+
Eliminar hashes del historial de contraseñas de las cuentas normales (SAM)	-	+	+
Quitar hashes del historial de contraseñas de las cuentas de Active Directory	-	+	+
Eliminar contraseñas almacenadas en caché de dominio	-	+	+
Eliminar contraseñas de inicio de sesión almacenadas en caché	-	+	+
Eliminar información de restablecimiento de contraseña	-	+	+
Eliminar sugerencias de contraseña	-	+	+
Restablecer la seguridad de SYSKEY (con re-cifrado de contraseñas de usuario)	-	+	+
Buscar contraseña de inicio de SYSKEY	-	+	+

CARACTERÍSTICA	Light	Stan-dard	Advan-ced
Recuperación instantánea de contraseña de texto sin formato para cuentas con contraseña de Imagen	-	+	+
Recuperación instantánea de contraseña de texto sin formato para cuentas con inicio de sesión biométrico (5)	-	+	+
Recuperación de PIN	-	+	+
Descifrar el historial de PIN (8)	-	+	+
Montar unidades virtuales	+	+	+
Detección automática y montaje de SO virtuales	+	+	+
Buscar contraseñas de máquinas virtuales	-	+	+
Buscar claves de producto y números de serie perdidos	-	+	+
Convertir Microsoft Live ID en una cuenta de usuario local	+	+	+
Contraseñas de copia de seguridad, registro y Active Directory	+	+	+
Buscar documentos protegidos por contraseña	+	+	+
Buscar documentos abiertos recientemente (7)	+	+	+
Recuperación de contraseña para MS Office, OpenOffice, LibreOffice, MyOffice y documentos PDF	-	+	+
Buscar y descifrar contraseñas de navegadores de Internet	-	+	+
Buscar y descifrar contraseñas para clientes de correo electrónico populares	-	+	+
Buscar y descifrar diferentes contraseñas de red	-	+	+
Crear nuevas cuentas SAM	-	+	+
Desbloquear unidades BitLocker	+	+	+
Extraer contraseñas de recuperación de BitLocker de Active Directory	-	-	+
Opciones de inicio de sesión de Windows	-	+	+
Editor de directivas de contraseñas local	-	+	+
Editor de directivas de contraseñas de dominio	-	-	+
Editor de directivas de inicio de sesión	-	+	+
Editor de políticas de restricción de interfaz y sistema	-	+	+
Compatibilidad con la opción de inicio de sesión sin contraseña	+	+	+
Descifrar credenciales de Windows Hello (8)	-	+	+
Historial y estadísticas de inicio de sesión (6)	+	+	+
Historial de hardware (7)	+	+	+
Historial de software (7)	+	+	+
Historial de red (7)	+	+	+
Actividad reciente del usuario (6)	+	+	+
Buscar documentos abiertos recientemente (7)	+	+	+
Ver cronograma de ejecución del programa (7)	+	+	+
Eventos del sistema (6)	+	+	+
Historial web (6)	+	+	+

CARACTERÍSTICA	Light	Stan-dard	Advan-ced
Archivos modificados por última vez	-	+	+
Directorios modificados por última vez	-	+	+
Crear imágenes de disco	+	+	+
Contraseña de acceso al programa	+	+	+
Precio	**$45**	**$145**	**$345**

Notas:
(1) Si la cuenta está bloqueada, deshabilitada o caducada
(2) Modo de restauración de servicios de directorio
(3) Si se establece el cifrado reversible. Puede encontrar esta opción en la directiva de contraseñas de su dominio.
(4) Uso de diccionarios de árabe, chino, inglés, francés, alemán, portugués, ruso, español.
(5) No para todas las cuentas
(6) La función de exportación de datos solo está disponible en la edición Advanced
(7) La función de exportación de datos solo está disponible en las ediciones Standard y Advanced
(8) Si no está protegido con TPM

Soporte técnico

5 Soporte técnico

5.1 Reporte de fallos

Si tiene algún problema, póngase en contacto con nosotros en support@passcape.com. Por favor, infórmenos sobre lo siguiente:

- Versión de Windows, incluidos los Service Pack y otras correcciones instaladas
- Versión completa del programa (consulte el cuadro de diálogo **Acerca de**)
- Información de registro del programa, si la hubiera.
- Descripción detallada de su problema (tanta información como sea posible)

Si estás reportando un error, por favor adjunta el(los) archivo(s) **RWPCrash.log** que se han guardado durante una excepción no controlada

5.2 Sugerir nuevas funciones

Si tiene alguna pregunta, comentario o sugerencia sobre el programa o desea obtener más información, envíenos un correo electrónico a info@passcape.com. Por favor, no olvide mencionar el nombre y la versión del programa. También asegúrese de tener instalada la última versión del programa. Sus comentarios nos ayudan a mejorar nuestros productos y trabajar de manera más efectiva.

5.3 Contactos

Por favor, no dude en enviar sus preguntas sobre nuestros productos al correo electrónico support@passcape.com.
Recibirá respuesta durante uno o dos días. Tenga en cuenta que los usuarios registrados tienen prioridad en el soporte técnico.

Si experimenta algún problema durante el proceso de registro, envíe un mensaje a sales@passcape.com
Estaremos encantados de ayudarle con el registro.

¡Por favor, escriba en inglés!

Puede encontrar otras utilidades de recuperación de contraseña en https://www.passcape.com.