Reset Windows Password

Manuel de l'utilisateur

Passcape Software

Traduit le 16/11/2018

Introduction

1 Introduction

1.1 À Propos du programme

Reset Windows Password a été développé pour réinitialiser, modifier et récupérer les mots de passe de session Windows. Par exemple, lorsque le mot de passe administrateur de l'ordinateur a été perdu ou oublié. Reset Windows Password est la solution la plus complète et riche en fonctionnalité dans ce domaine. L'application supporte toutes les versions de Windows (basées sur NT), fonctionne avec l'Active Directory et les identifiants de connexion de Domaine en cache. Elle possède, également, une Intelligence Artificielle capable de récupérer les mots de passe instantanément, pour certains comptes utilisateurs et des fonctionnalités complémentaires uniques.

L'interface de l'application est traditionnellement réalisée sous la forme d'assistant pas à pas. Du coup, Les étapes du processus ne seront pas compliquées, même pour un utilisateur inexpérimenté. Par exemple, réinitialiser un mot de passe administrateur se fait en seulement trois simples étapes:
1. Sélection des fichiers SAM et SYSTEM (l'application recherche automatiquement sur tous les disques durs, les fichiers de la base de registre).
2. Sélection du compte d'un utilisateur.
3. Réinitialisation ou modification du mot de passe.

En utilisant le logiciel est fourni avec Reset Windows Password (IsoBurner), vous pouvez créer facilement un CD, DVD ou un disque USB amorçable (incluant les périphériques comme des supports Compact Flash, SmartMedia, SONY Memory Stick, Secure Digital, lecteurs ZIP, disques durs USB, etc.) en quelques minutes, à partir d'une image ISO fournie avec le programme. Reset Windows Password possède une interface graphique, supporte le chargement de volumes IDE, SATA, SCSI, RAID à la volée, est compatible avec les fichiers systèmes FAT, FAT32, NTFS, NTFS5, et est fourni avec une large collection de pilotes de disques durs provenant de Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware.

1.2 Fonctionnalités et avantages

Intérêts de l'application:
- Support pour toutes les versions de Windows à base de NT.
- Support pour Windows 32 et 64 bits.
- Large collection de pilotes de disques durs. Chargement complémentaires de pilotes à partir de l'application.
- Réinitialise et modifie les mots de passe des utilisateurs locaux, de l'administrateur local et de domaine, des comptes de l'Active Directory.
- Active ou déverrouille les comptes d'utilisateurs, administrateurs locaux et de domaine.
- Désactive l'option d'expiration du mot du passe.
- Détecte la présence de plusieurs systèmes d'exploitation.
- Supporte les versions de Windows autres qu'en Anglais et les mots de passe en code Nationaux.
- Dump les hachages de mots de passe d'utilisateur à partir du fichier SAM, pour une analyse plus approfondie.
- Dump les hachages de mots de passe à partir de l'Active Directory.
- Dump les mots de passe de Domaine en cache.
- Plusieurs modules pour extraire et décrypter les mots de passe en clair de l'Active Directory.
- Permets l'annulation des modifications effectuées au système.
- Supprime les mots de passe et d'autres données sensibles du PC.
- Recherche avancée et algorithme de récupération de mots de passe.
- Réinitialise la sécurité de SYSKEY.
- Récupération du mot de passe de démarrage SYSKEY.
- Recherche des clés de logiciels perdues.
- Recherche des mots de passe réseau.

- Sauvegarde de la base de registre/Active Directory et d'autres informations sensibles.
- Déverrouillage de disques cryptés par Bitlocker.
- Affichage de l'activitté d'utilisateurs, différentes informations forensiques.
- Édition des stratégies de sécurités des mots de passe locaux et de Domaine.

Le logiciel est disponible en trois versions: **Basic (Light)** , **Standard (Standard)** et **Avancé (Advanced)**.
Le détail de la liste des fonctionnalités, pour chaque version, est disponible ici.

1.3 Configuration Système nécessaire

Configuration nécessaire
Microprocesseur x64, un minimum de 1 Go de RAM, un lecteur CD-ROM ou clé USB. La taille de la clé USB doit être au minimum de 512 Mb ou plus (une clé USB de 2-32 Gb est recommandée pour une meilleur compatibilité). Le BIOS de l'ordinateur doit supporter le démarrage à partir de CD, DVD ou de périphériques USB.

Compatibilité
Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7/8/10, Windows Server 2000/2003/2008/2012/2019. Fichiers systèmes: FAT, FAT32, NTFS, NTFS5. Le programme est compatible avec la majorité des graveurs de CD/DVD et les périphériques USB, incluant les supports Memory Stick, Compact Flash, SmartMedia, Secure Digital, les clés USB, les lecteurs USB ZIP, les disques durs USB, etc.

Restrictions
Si votre système utilise un périphérique de stockage non-standard, vous aurez besoin du pilote du périphérique compatible avec Windows 10. Référez-vous au manuel de votre carte mère de votre ordinateur ou de la carte contrôleur des disques, pour plus de détails.

Solutions et bugs connues
- Si vous avez 2 ou un nombre supérieur de disques logiques dans votre système, les lettres des disques peuvent être réassignés/réorganisés.
- Si vous réinitialisez un mot de passe d'un compte administrateur dans des versions de Windows, gardez à l'esprit que pour pouvoir activer le compte administrateur et se connecter au système, vous devrez charger le système en mode "Sans échec (safe mode).
- Le programme supporte tous les types de cryptage de SYSKEY. Dans certains cas, vous devez peut-être fournir un mode passe de démarrage SYSKEY ou de disquette de démarrage. Cependant, le programme permets également de réinitialiser/analyser le mot de passe SYSKEY. Du coup, si vous oubliez votre SYSKEY, cela n'est pas un problème.
- Après avoir réinitialisé le mot de passe d'un compte local, vous pouvez perdre vos mots de passe de page Web, vos informations de connexion pour les réseaux sans fil et les fichiers partagés, les fichiers cryptés EFS et les e-mails cryptés avec des clés privées. Référez-vous à la base de connaissance Microsoft, pour plus de détails.
- Réinitialiser les mots de passe de l'Active Directory pour certains comptes peut avoir aucun effet. Par exemple, pour un RODC.
- Lors de la réinitialisation d'un mot de passe pour un compte Microsoft, vous devez fournir un mot de passe non vide. Sinon, vous ne serez pas capable de vous connecter (logger) au système.

Créer un environnement bootable

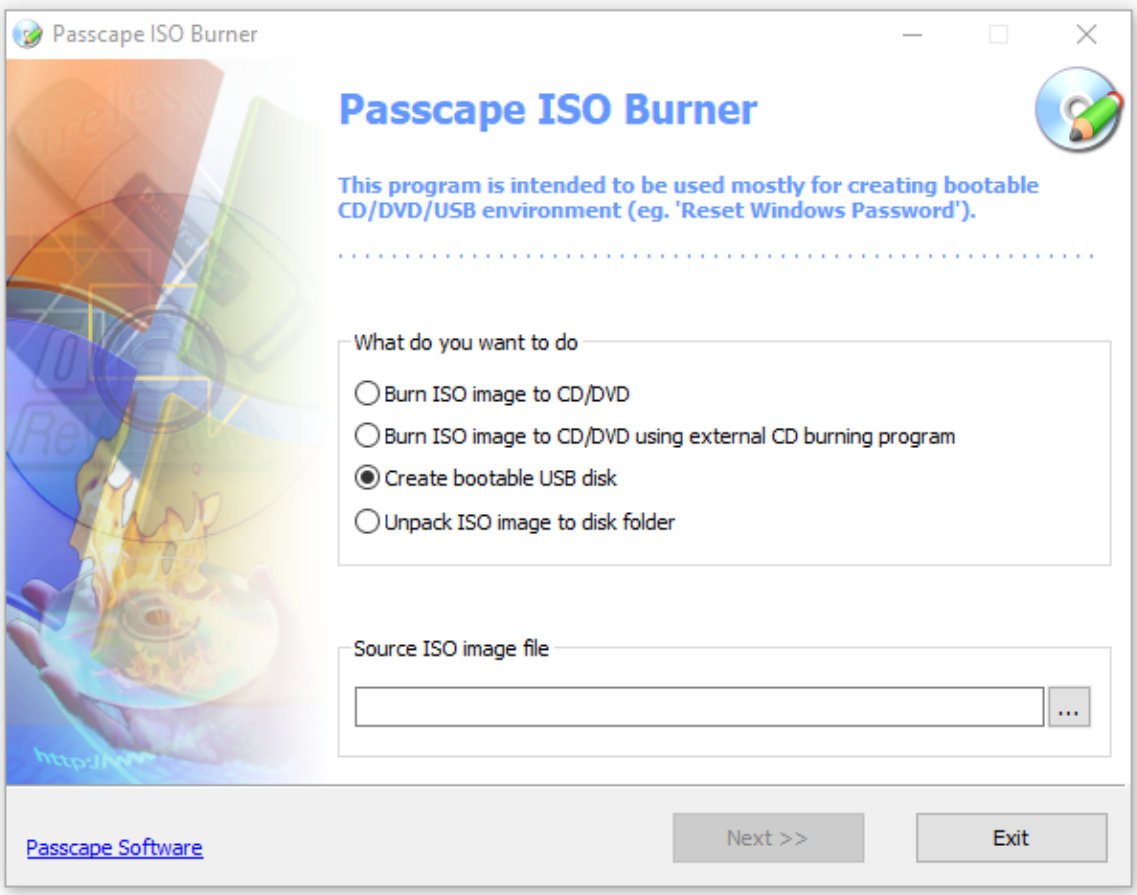
2 Créer un environnement bootable

2.1 3 étapes simples pour lancer le logiciel à partir d'un disque amorçable

1. Télécharger le fichier compressé ZIP, contenant l'image ISO de **Reset Windows Password**, avec le lien suivant: https://www.passcape.com/download/rwp.zip (ou utiliser le lien que vous avez reçu lorsque l'on vous a envoyé votre e-mail d'enregistrement).
2. Créer un disque RWP amorçable: décompacter le fichier RWP.ZIP, lancer le programme IsoBurner.exe, sélectionner l'option pour la création d'un CD/DVD/USB amorçable, afficher le chemin de l'image ISO décompressée et lancer la gravure sur le disque.
3. Démarrer l'ordinateur cible et modifier les paramètres du BIOS/UEFI pour pouvoir démarrer votre ordinateur, sur le premier périphérique de la liste (CD-ROM, DVD-ROM ou disque USB). Enregistrer les paramètres, redémarrer à nouveau l'ordinateur, pour démarrer à partir du CD, DVD ou disque USB amorçable. Vous pouvez utiliser l'option de "Fast boot" si votre BIOS/UEFI supporte le choix du support de démarrage.

2.2 Création du disque RWP amorçable

Passcape ISO Burner

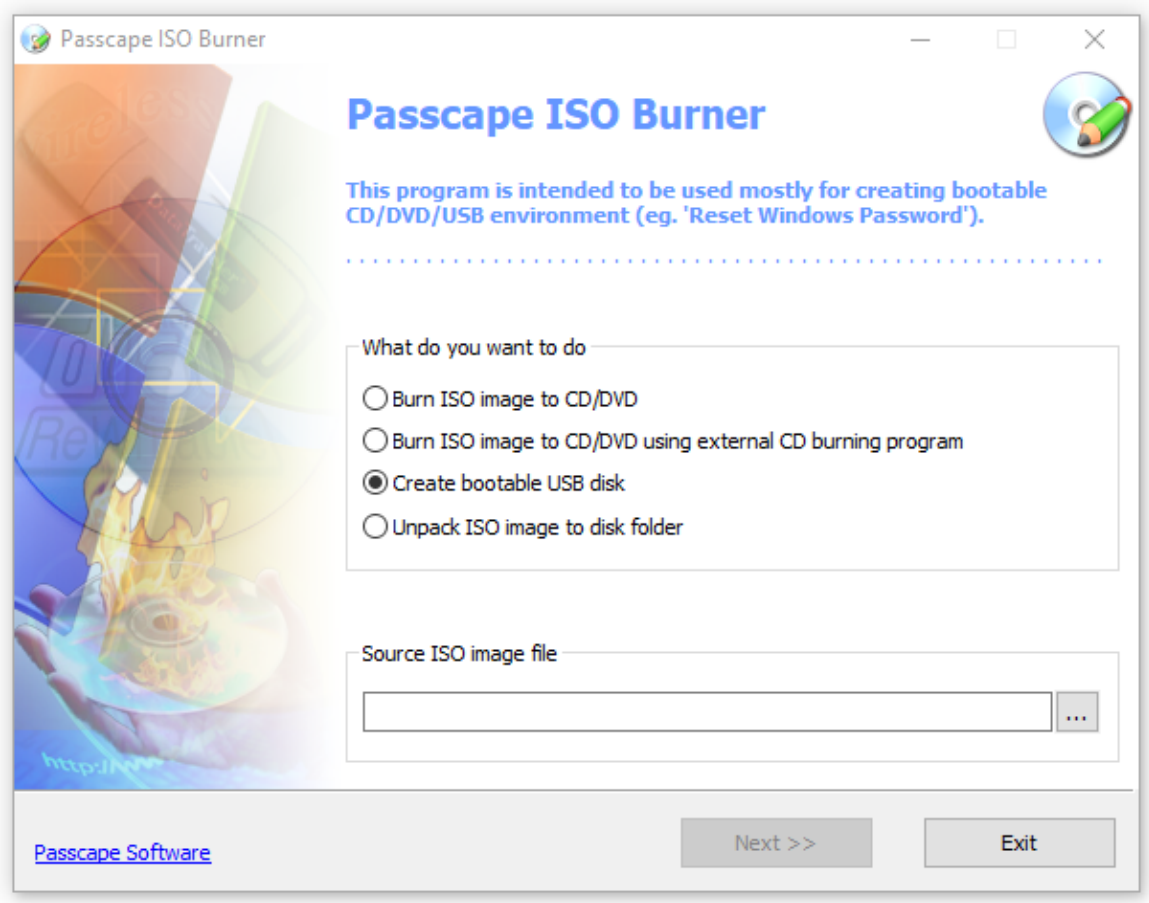


Passcape ISO Burner (PIB) est un utilitaire pour la création de CD, DVD ou de disques USB à partir d'images ISO 9660. **PIB** supporte la création de disques amorçables (par exemple, WinPE, BartPE ou RWP).

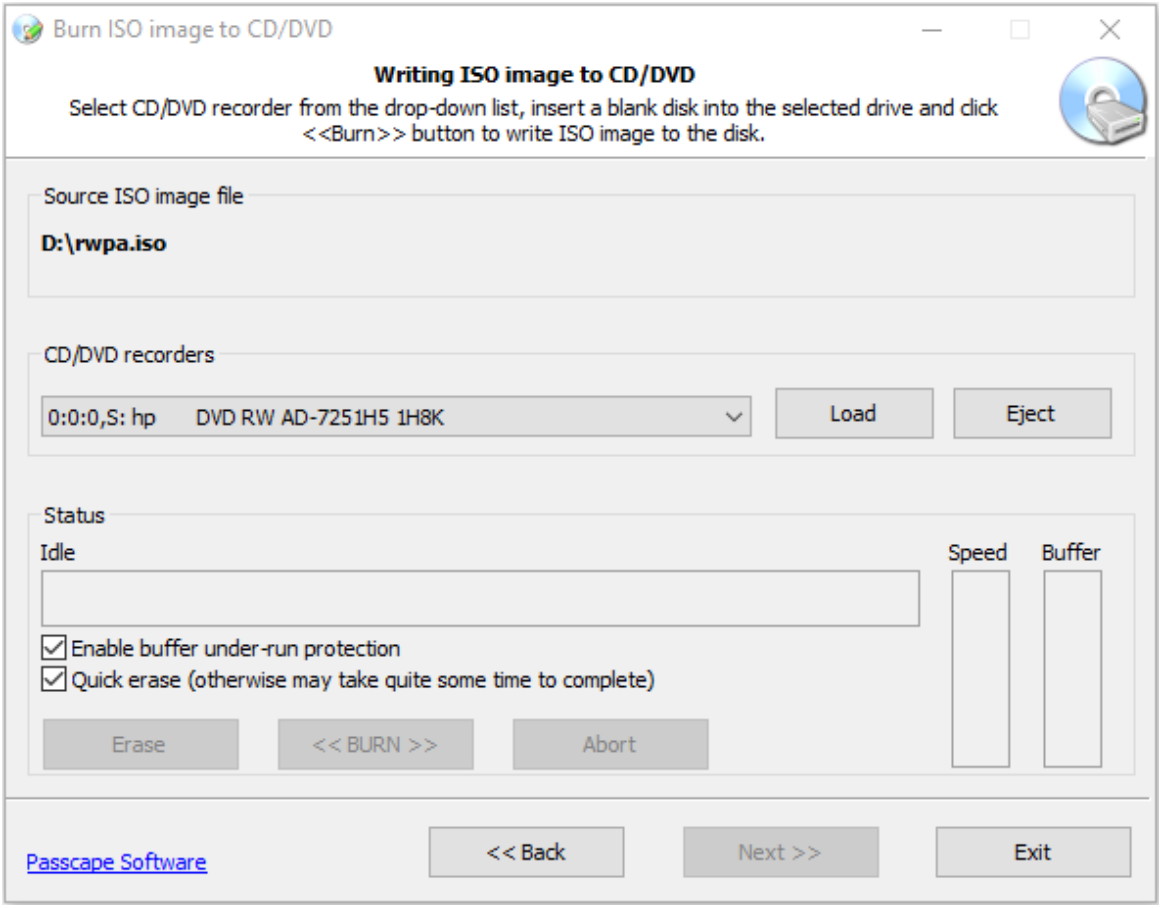
Le logiciel est livré gratuitement avec RWP. Il est aussi possible de le télécharger à partir de notre site sur Internet: https://www.passcape.com/download/pib.zip

L'interface du logicielle est extrêmement simple. Au démarrage, le logiciel vous demande de sélectionner ce que vous voulez faire:
- Burn ISO image to CD/DVD (Graver une image ISO sur un CD/DVD, en utilisant ce logiciel).
- Burn ISO image to CD/DVD using external CD burning program (Graver une image ISO sur un CD/DVD, en utilisant un programme de gravure, comme Nero ou gratuit tel que ImgBurn.
- Create bootable USB disk (Créer un disque USB amorçable avec l'image ISO).
- Unpack Iso image to disk folder (Extraire l'image ISO dans un répertoire du disque). Gardez à l'esprit que cette action peut conduire à la perte des données de démarrage de votre système.

Création d'un CD bootable pour "Reset Windows Password"

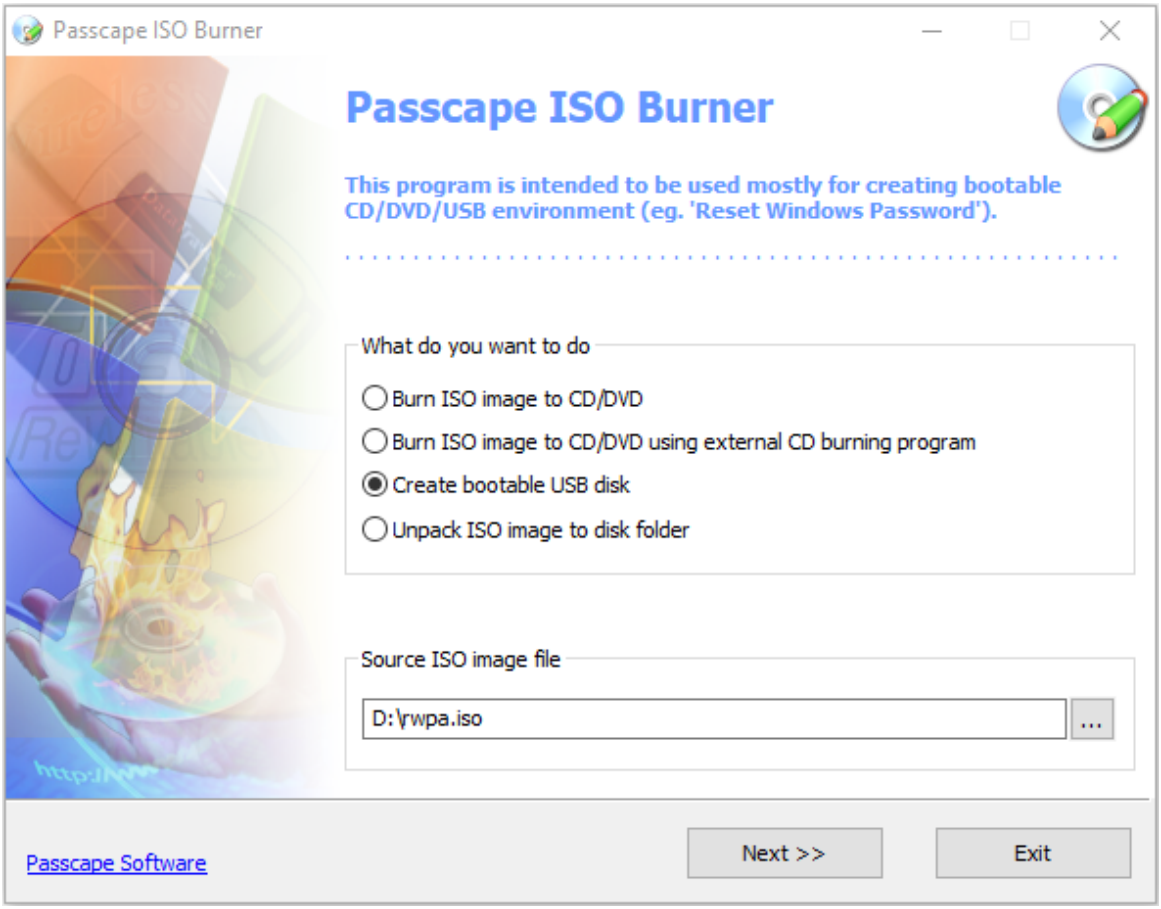


Sélectionner, en premier, l'option de menu: "*Burn ISO image to CD/DVD" (Graver une image ISO sur un CD/DVD)*.
Ensuite, en bas de la fenêtre, entrer le chemin du fichier de l'image ISO, dans le champ réservé pour "*Source ISO image file*".
Cela active le bouton "Next >>", et vous permets de passer à la page suivante de l'assistant de gravure du disque (ci-dessous).

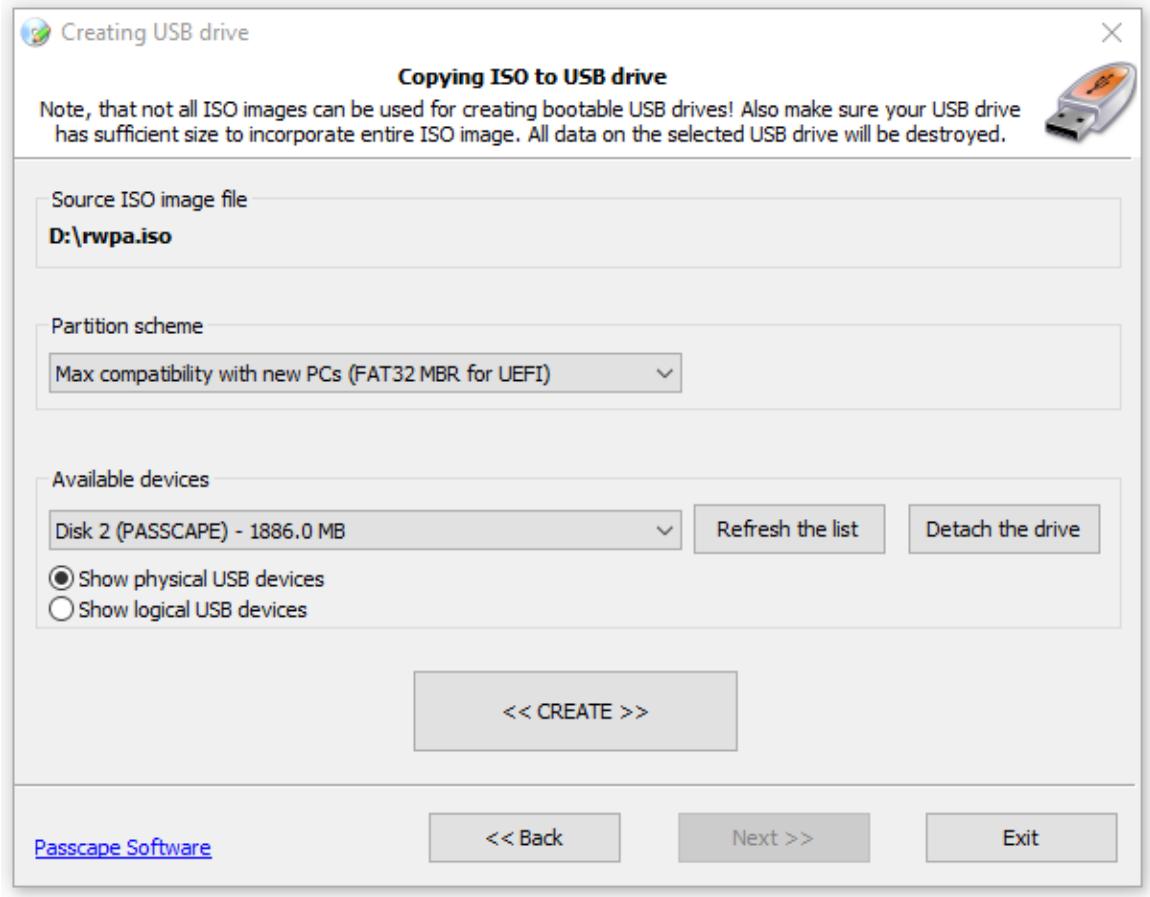


Sélectionner le graveur que vous souhaitez utiliser, insérer un CD/DVD vierge dans le lecteur et cliquer sur le bouton <<BURN>> pour créer et graver un disque à partir de l'image ISO choisie, à l'étape précédente.

Création d'un lecteur USB bootable pour "Reset Windows Password"



Sélectionner l'option "Create bootable USB disk" (Création d'un disque USB bootable).
Sélectionner l'image ISO du logiciel.
Lorsque la fenêtre suivante de l'assistant apparaît, insérer votre lecteur ou clé USB.



Une fois votre disque ou clé USB inséré, une liste des périphériques trouvés apparaît automatiquement.
Cliquer sur le bouton "<< CREATE >>" pour formater et créer le secteur de boot USB. Dans certains cas (par exemple, si le périphérique USB est installé comme un disque dur, et qu'une partition étendue est trouvée sur ce disque) le logiciel va demander un redémarrage de l'ordinateur pour réassigner les lettres des lecteurs.

Le programme dispose au choix, de plusieurs types de partitions (modes de formatage) pour apporter la meilleur compatibilité lors du démarrage à partir de périphériques USB.

Si vous hésitez dans le choix du type de partition, pensez à utiliser l'algorithme suivant:

- Si le PC cible est basé sur une interface UEFI (graphique), sélectionner le mode "*Max compatibility with new PCs (FAT32 MBR for UEFI)*".
  Ce mode créera un support USB pour fonctionner sur les PC où le mode de démarrage sécurisé UEFI est activé.

- Si le PC cible est basé sur une interface BIOS (texte), sélectionner le mode "*Max compatibility with old PCs (FAT32 MBR for BIOS)*".
  Ce mode créera un support USB avec une compatibilité maximum avec les micrologiciels BIOS.

- Si vous ne connaissez pas le type de PC cible, sélectionner le mode "*Max possible compatibility*".
  Ce mode créera un support USB pour fonctionner à la fois sur les PC ayant un BIOS ou UEFI (avec **Compatibility Support Mode** activé).
  Avec certains PC, le mode "Compatibility Support Mode" est aussi appelé "**Legacy Boot Mode**".

Si vous achetez un PC après 2010, la plupart du temps, il possède un UEFI. Les nouveau ordinateurs utilise un micrologiciel UEFI en remplacement du traditionnel BIOS. Les deux sont des

logiciels de "bas niveau" qui s'exécute en premier à l'allumage du PC et qui sont utilisé pour "communiquer" avec les composants matériels. A la différence du BIOS, l'UEFI est une solution moderne avec une interface graphique, supportant les disques de tailles importantes, avec un démarrage plus rapide et d'avantage de fonctionnalités de sécurité.

Attention !!! Toutes les données seront perdues sur le lecteur cible. Si le logiciel est incapable de détecter les fichiers de démarrage dans l'image ISO source, un message d'avertissement sera affiché.

Certains logiciels AntiVirus/AntiMalware bloquent la création de disques amorçables ou la copie de fichiers de démarrage sur le support souvent sans message d'alerte !

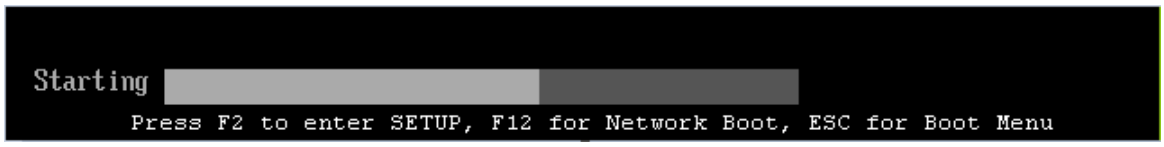
2.3 Modification des paramètres BIOS/UEFI

Information générale

Pour pouvoir charger Reset Windows Password, vous pouvez avoir besoin de régler les paramètres BIOS/UEFI de votre ordinateur, pour démarrer le premier lecteur de la liste des périphériques (CD, DVD, ou USB).

Suivez cette procédure régler votre BIOS/UEFI:

1. Au démarrage de l'ordinateur, appuyer sur la touche "**Suppr**" pour entrer dans le menu du BIOS. Certaines versions de BIOS/UEFI utilise d'autres touches de raccourci; elles peuvent être **F2**, **F10**, **F11**, **ESC**, etc. La touche pour accéder au menu du BIOS est généralement affiché en bas de l'écran au démarrage de l'ordinateur.



2. Entrer dans le BIOS/UEFI, puis dans le menu, trouver la page permettant de gérer l'ordre de démarrage des périphériques. Configurer l'ordre de démarrage pour que le périphérique CD ou USB avec Reset Windows Password soit le premier de la liste.
3. Enregistrer les paramètres, redémarrer à nouveau l'ordinateur pour démarrer votre CD, DVD ou disque USB.

Si votre PC utilise un micrologiciel UEFI, vous pouvez utiliser le démarrage rapide ("Fast boot") sans altérer aucun paramétrages.Pour plus d'informations, référez-vous au manuel de la carte mère de l'ordinateur.

Paramètrage du BIOS, Questions et Réponses

Q: Le BIOS de mon ordinateur possède plusieurs options pour le démarrage à partir d'un périphérique USB: USB FDD, USB ZIP, USB HDD, USB CDROM. Lequel de ces périphériques je dois choisir ?
R: Plusieurs fabricants de BIOS configurent le démarrage initial de différentes façons. Dans la majorité des cas, pour démarrer d'un lecteur USB, sur les anciennes cartes mère vous devez sélectionner l'option - USB ZIP; pour les autres - USB HDD.

Q: Le logiciel prends beaucoup trop de temps (parfois plus de 10 minutes) pour démarrer à partir d'un support USB.
R: C'est le cas lorsque le périphérique fonctionne avec un protocole USB lent: 1.1. En premier, votre périphérique doit supporter la spécification USB 2.0+. En second, le port USB de votre carte mère

où vous branchez votre périphérique USB doit supporter la spécification USB 2.0+. Pour finir, vous devez activer le support USB 2.0 (ou supérieur) dans le BIOS.

Q: L'ordinateur n'arrive pas à démarrer à partir d'un périphérique USB. Lorsqu'il arrive à démarrer – soit un écran noir ou un message d'erreur "'*no operating system* " s'affiche.
R: Essayer de trouver l'option "*Legacy USB storage detect"* et modifier la valeur sur "*Enabled"*. Dans les options de démarrage, vous devez avoir seulement un périphérique USB. Si vous avez deux ou plus de deux périphériques connectés à l'ordinateur (ex: UPS, imprimante, scanner, webcam, etc.), laisser uniquement le disque USB amorçable. Débrancher le périphérique USB de l'ordinateur, éteigner l'ordinateur, brancher le périphérique USB dans un autre port, allumer à nouveau votre ordinateur et attendez qu'il démarre. Si cela ne change rien – mettez à jour le BIOS. Il est aussi possible que votre carte mère ne supporte pas le démarrage à partir d'un périphérique USB ou ne supporte pas le système de fichiers utilisé pour le périphérique USB.

Q: Ecran bleu ou noir, tous les types de pilotes, chargement de la base de registre, etc. des erreurs apparaissent lors du démarrage à partir d'un CD ou d'un support USB.
R: Peut-être que votre ordinateur ne possède pas assez de mémoire. Le taille minimum de RAM nécessaire, est de 1 Go, pour faire fonctionner le programme. Pour un fonctionnement optimal et confortable, 2GB Mb ou plus est conseillé.

Q: Je ne peux pas accéder au BIOS/UEFI. Un mot de passe est nécessaire.
R: Une mauvaise surprise peut arriver lorsque vous essayez de modifier les paramètres de démarrage des périphériques dans le BIOS. Certains fabricants de matériels, distributeurs ou les précédents propriétaires de PC peuvent avoir programmés leur mot de passe personnel pour accéder au BIOS. Du coup, pour pouvoir modifier les paramètres du BIOS/UEFI, vous devrez connaître ce mot de passe, qui généralement est impossible à trouver.
Certaines versions de BIOS/UEFI permettent de réinitialiser leurs paramètres en appuyant sur une touche particulière du clavier; habituellement qui est "**Inser"**. Pour certains types de BIOS/UEFI AMI, c'est la combinaison **Ctrl+Alt+Del+Ins**. Pour les BIOS/UEFI AWARD, la touche doit être appuyée jusqu'a ce que l'ordinateur soit allumé. Ce qui permets de charger les paramètres par défaut. Cependant, cette option doit être utilisé avec beaucoup de précaution, car elle réinitialise tous les autres paramètres du BIOS.
Il existe également, des mots de passe cachés (back-door). Une liste est fournie, plus bas dans cette page, pour la plupart des anciennes versions de BIOS/UEFI connus. Si vous ne connaissez pas votre type ou version de BIOS/UEFI, ces informations sont généralement affichées pendant quelques secondes au démarrage de l'ordinateur, en bas de l'écran.
Si aucun mot de passe ne fonctionne, vous pouvez utilisez la méthode décrite dans beaucoup de manuels de cartes mère: en réinitialisant simplement les paramètres du BIOS/UEFI, en court-circuitant un pont prévu (jumper) à cet effet. Il est habituellement situé près de la pile pour la CMOS. Si la carte mère ne possède pas de pile pour la CMOS, localiser le composant de chez Microchip avec l'inscription "Dallas" ou "Odin"; le pont (jumper) doit être situé à proximité. Le fait de retirer la pile pour la CMOS n'est pas toujours utile, car le BIOS/UEFI microchip peut fonctionner pendant plusieurs heures sans alimentation. Il n'est, également, pas recommandé de court-circuiter la CMOS elle-même pour réinitialiser les paramètres du BIOS, cela ne pouvant que conduire à réduire la durée de vie de la pile.
Sur Internet, vous trouverez des logiciels pour récupérer et réinitialiser les mots de passe de BIOS. Par exemple, cmospwd et killcmos. Il très fortement déconseillé de réinitialiser tous les paramètres BIOS des PC portables. Cela peut complètement bloquer son fonctionnement et le rendre inutilisable.

Q: Un message d'erreur indique que le CPU ne supporte pas le mode 64 bits ou les applications fonctionnant en 64 bits.
A: Reset Windows Password ne supporte plus les CPU en 32 bits (mais le support pour les OS en 32 bits est maintenu). Contacter le support technique de Passcape pour obtenir un lien de téléchargement de la dernière version compatible.

Q: Est-ce que je peux démarrer avec un lecteur CD/USB compatible BIOS en UEFI ?
A: Oui. Entrer dans les paramètres de l'UEFI (appuyer sur ESC, F2 ou Supp). Ouvrer le menu de

"Boot" et activer l'option "Launch CSM". Maintenant, localiser l'onglet "Security" et désactiver le "Secure Boot Control". Enregistrer les modifications et redémarrer votre PC. Entrer à nouveau dans les paramètres de l'UEFI et assurez-vous que le lecteur DVD/USB est disponible dans l'onglet "Boot". Certains UEFI ont aussi un menu de démarrage des périphériques (qui peut est habituellement lancé en appuyant sur la touche F8) où vous pouvez sélectionner votre périphérique de démarrage et son mode.

Q: Est ce que je peux créer un lecteur USB qui sera capable de démarrer avec le BIOS et l'UEFI ?
A: Oui. Exécuter l'outil IsoBurner et sélectionner le type de partition "Max possible compatibility" lors de la création d'un disque USB amorçable. Ce mode crée des disques USB amorçables qui fonctionne pour les ordinateurs à base de BIOS et d'UEFI (avec le "Compatibility Support Mode" activé). Sur certains PC ou portable, le "Compatibility Support Mode" est également connu sous le nom de "Legacy Boot Mode".

Q: L'USB n'est pas listé comme une option de démarrage dans mon UEFI. Comment je peux activer le boot pour une clé USB ?
A: Il est possible que votre clé USB a été formaté soit pour le mode BIOS ou l'UEFI CSM. Votre UEFI ne permets le mode de boot "Secure Boot". Vous devez permettre le démarrage en mode de compatibilité (legacy mode). Dans les paramètres de votre UEFI, désactiver "Boot - Fast Boot' et 'Security - Secure Boot" et activer "Compatibility Support Mode (CSM)" ou les options avec un nom similaire. Une autre possibilité, est de créer simplement un disque USB amorçable avec le modèle "Max compatibility with new PCs (FAT32 MBR for UEFI)". Ce modèle est totalement compatible avec le mode "UEFI Secure Boot".

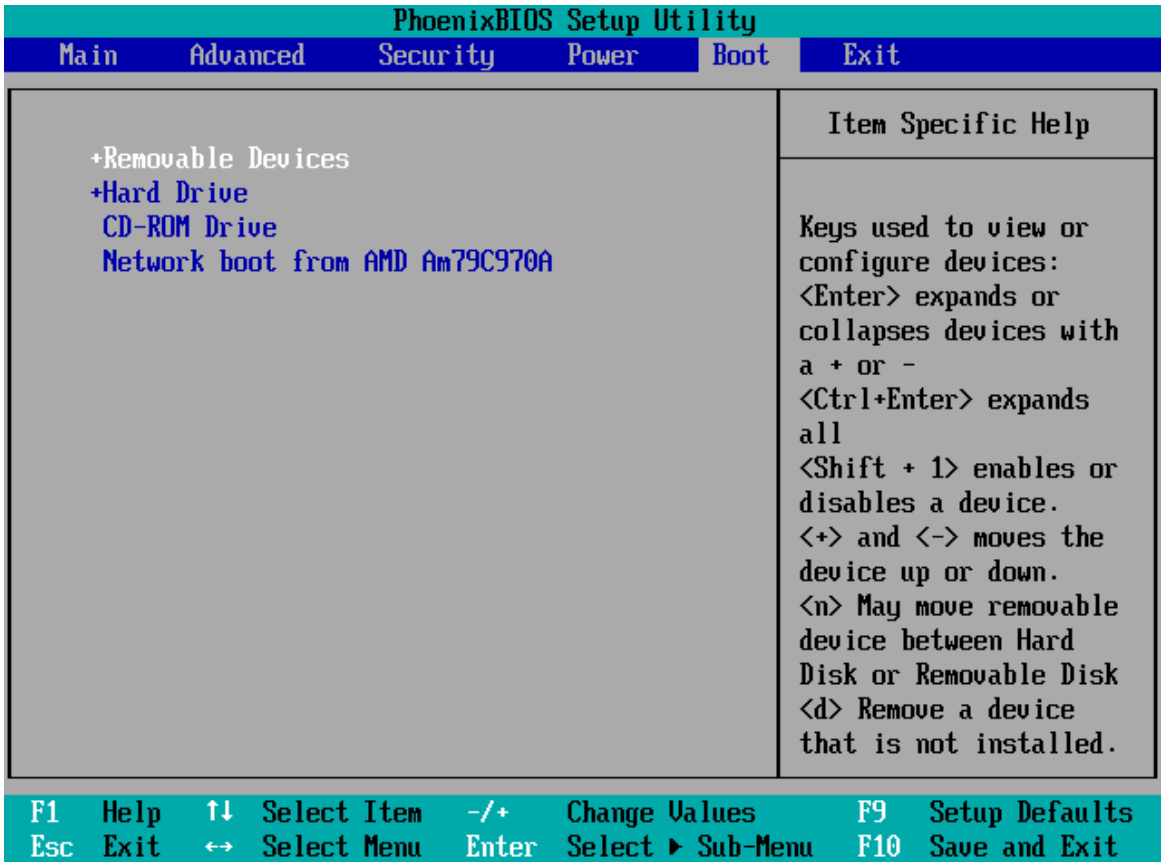
Mots de passe Back-door BIOS/UEFI

Fabricants du BIOS/ UEFI	Mots de passe universel
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

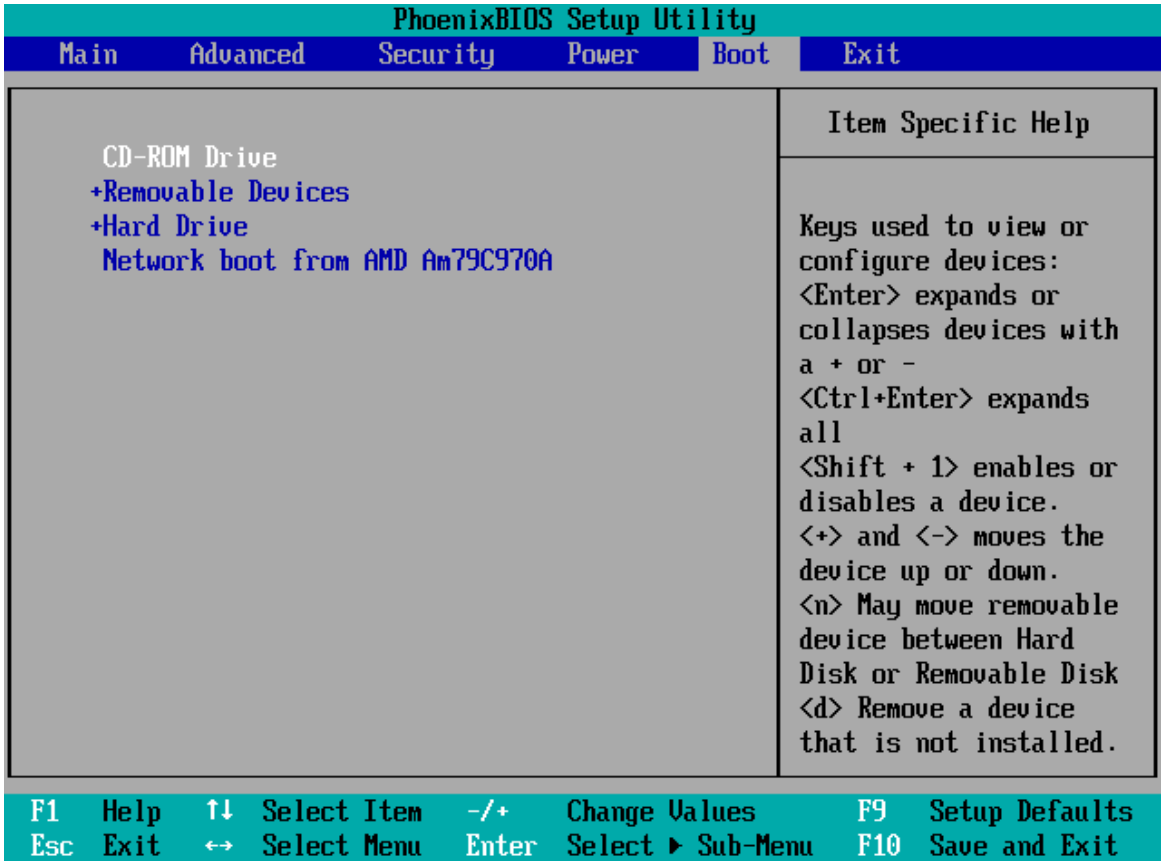
BIOSTAR BIOS	Biostar, Q54arwms
COMPAQ BIOS	Compaq
CONCORD BIOS	last
CTX International BIOS	CTX_123
CyberMax BIOS	Congress
Daewoo BIOS	Daewuu, Daewoo
Daytec BIOS	Daytec
DELL BIOS	Dell
Digital Equipment BIOS	komprie
Enox BIOS	xo11nE
Epox BIOS	Central
Freetech BIOS	Posterie
HP Vectra BIOS	hewlpack
IMB BIOS	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

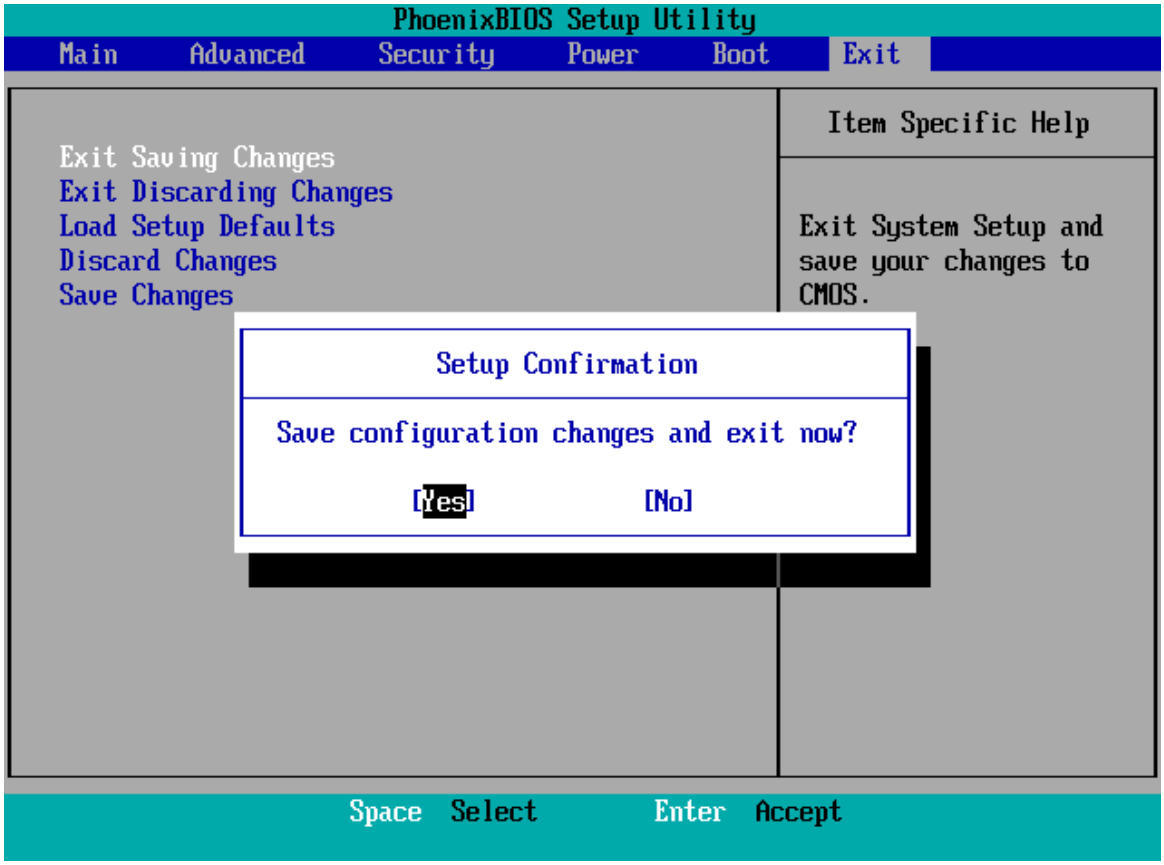
2.4 Démarrer le programme à partir d'un CD/DVD/USB amorçable



Démarrer votre ordinateur. Appuyer sur la touche DEL, pour entrer dans le menu du BIOS. Certaines versions de BIOS utilise d'autres raccourcis de claviers; cela peut être F2, F10, F11, ESC, etc. Un texte indiquant quelle touche est utilisée pour accéder au menu du BIOS est souvent affichée au début du démarrage du BIOS, en bas de l'écran.



Entrer dans le menu de démarrage du BIOS. Modifier l'ordre des périphériques pour permettre au CD ou à la clé USB contenant Reset Windows Password d'être au début de la liste.

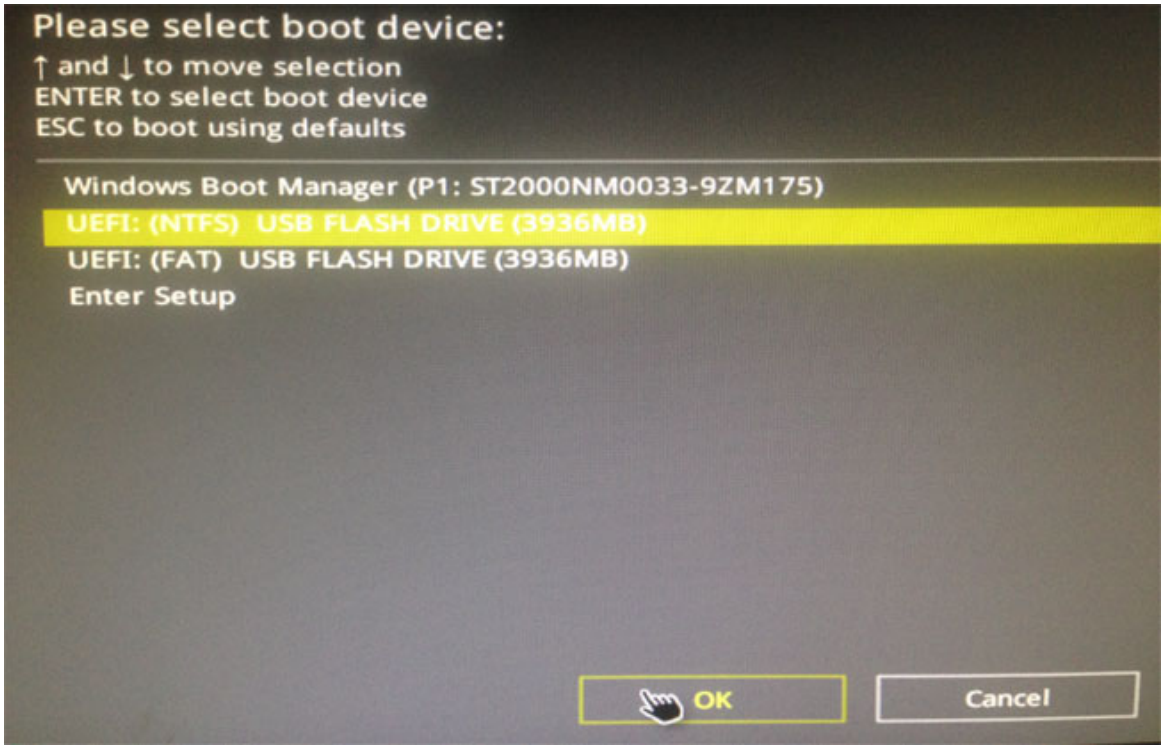


Sauvegarder les modifications effectuées, si c'est le cas. Redémarrer l'ordinateur.
Patienter le temps du démarrage, qui est plus long, avec un périphérique externe (CD/DVD/USB).

RWP a été chargé avec succès et il est prêt à être utilisé.

2.5 Démarrer le programme avec l'option de sélection du support de démarrage UEFI

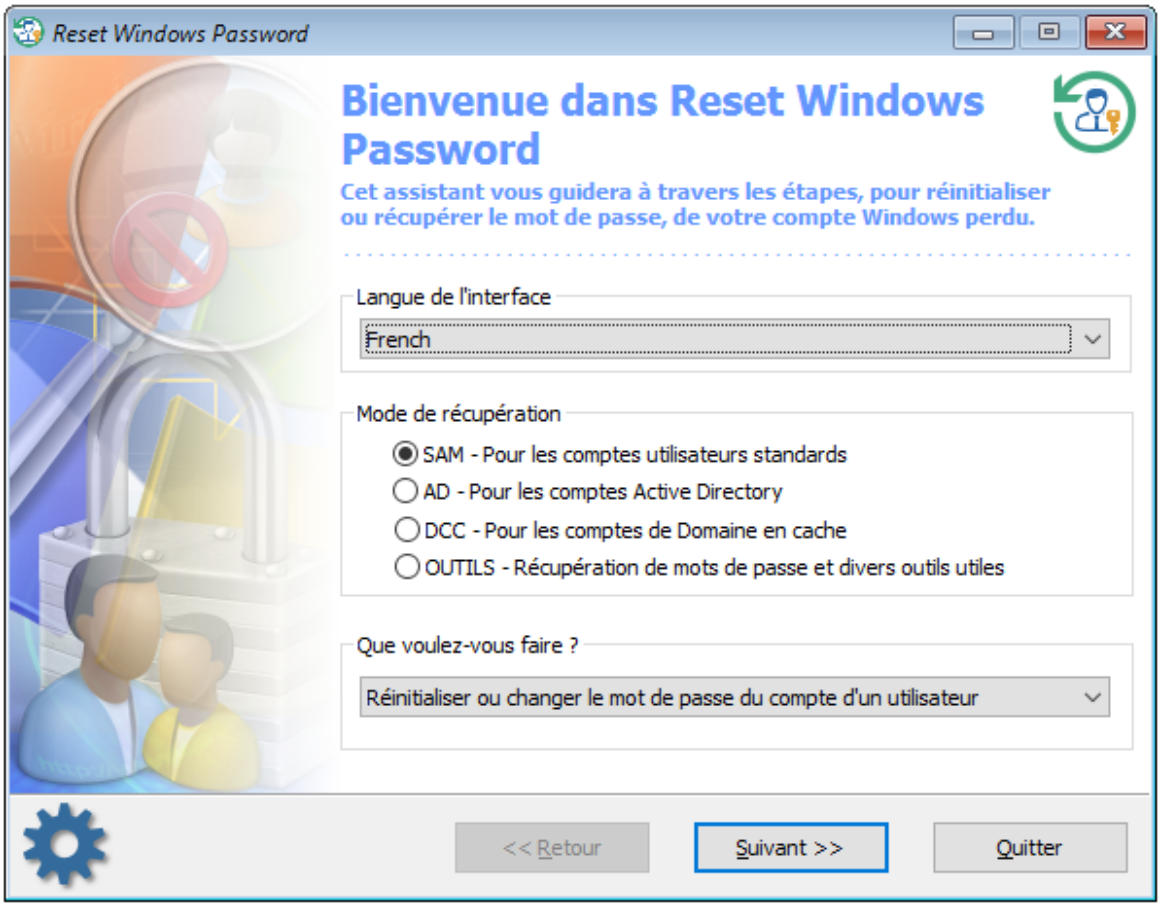
Si votre UEFI supporte la sélection du support de démarrage, vous pouvez l'utiliser pour démarrer le programme facilement. L'option est appelée en maintenant appuyé une touche (habituellement, F8) au démarrage du PC. Dans la plupart des versions d'UEFI, cette option est aussi disponible à partir du menu principal.



Utilisation du logiciel

3 Utilisation du logiciel

3.1 Menu principal



En tout premier, choisissez la langue de votre choix pour le logiciel. Ce qui permets également de sélectionner le clavier, par défaut, en rapport avec la langue.
Ensuite, dans l'assistant, vous devez choisir le mode de fonctionnement: **SAM** – Pour les comptes utilisateurs standards, **AD** – Pour les comptes Active Directory, **DCC** - Pour les comptes de Domaine en cache, **OUTILS** - autres outils et utilitaires, et **FORENSIQUES** - Outils d'investigations système.
Une fois la sélection faite, une liste d'opérations possibles sera disponible.

SAM - Comptes utilisateurs standards

- Réinitialiser ou changer le mot de de passe du compte d'un utilisateur
- Ajouter un nouveau compte utilisateur
- Modifier/Éditer les propriétés du compte d'un utilisateur
- Recherche et récupération du mot de passe de comptes d'utilisateurs
- Dumper (exporter) les hachages de mots de passe
- Restaurer les données et les mots de passe modifiés précédemment

AD - Comptes de Domaine Active Directory

- Réinitialiser ou changer le mot de passe du compte d'un utilisateur
- Réinitialiser ou modifier le mot de passe DSRM (Mode restauration AD)
- Modifier/Éditer les propriétés du compte d'un utilisateur
- Recherche et récupération du mot de passe de comptes d'utilisateurs
- Dumper (exporter) les hachages de mots de passe
- Restaurer les données et les mots de passe modifiés précédemment

DCC - Comptes de Domaine en cache

- Réinitialiser ou changer le mot de passe du compte d'un utilisateur
- Récupération du mot de passe de comptes d'utilisateurs
- Dumper (exporter) les identifiants de Domaine en cache dans un fichier texte
- Restaurer les données et les mots de passe modifiés précédemment

UTILS - miscellaneous tools

- Décrypter les identifiants de connexions Windows Hello
- Rechercher des codes PIN
- Rechercher le mot de passe de démarrage SYSKEY
- Rechercher des clés de CD/logiciels perdues
- Rechercher les mots de passe Internet/e-mail/réseau
- Rechercher les documents cryptés
- Sauvegarder les mots de passe et les informations sensibles
- Supprimer les informations sensibles d'un utilisateur
- Charger un pilote IDE/SATA/SCSI/RAID
- Déverrouiller les disques cryptés par Bitlocker
- Monter un disque virtuel

FORENSIQUES - Outils d'investigations système

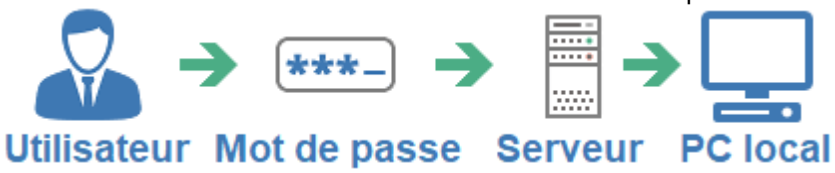
- Historique et statistiques de connexions (Logon)
- Historique matériels
- Historique d'installations de logiciels
- Historique de connexions réseau
- Activités récentes utilisateur
- Derniers fichiers modifiés
- Derniers répertoires modifiés

Descriptions schématiques des différents sortes d'ouvertures de sessions (logon)

SAM
Pour un compte standard pour tous les PC locaux: Les hachages de mots de passe sont stockés dans un fichier de la base de registre, sur le même ordinateur.

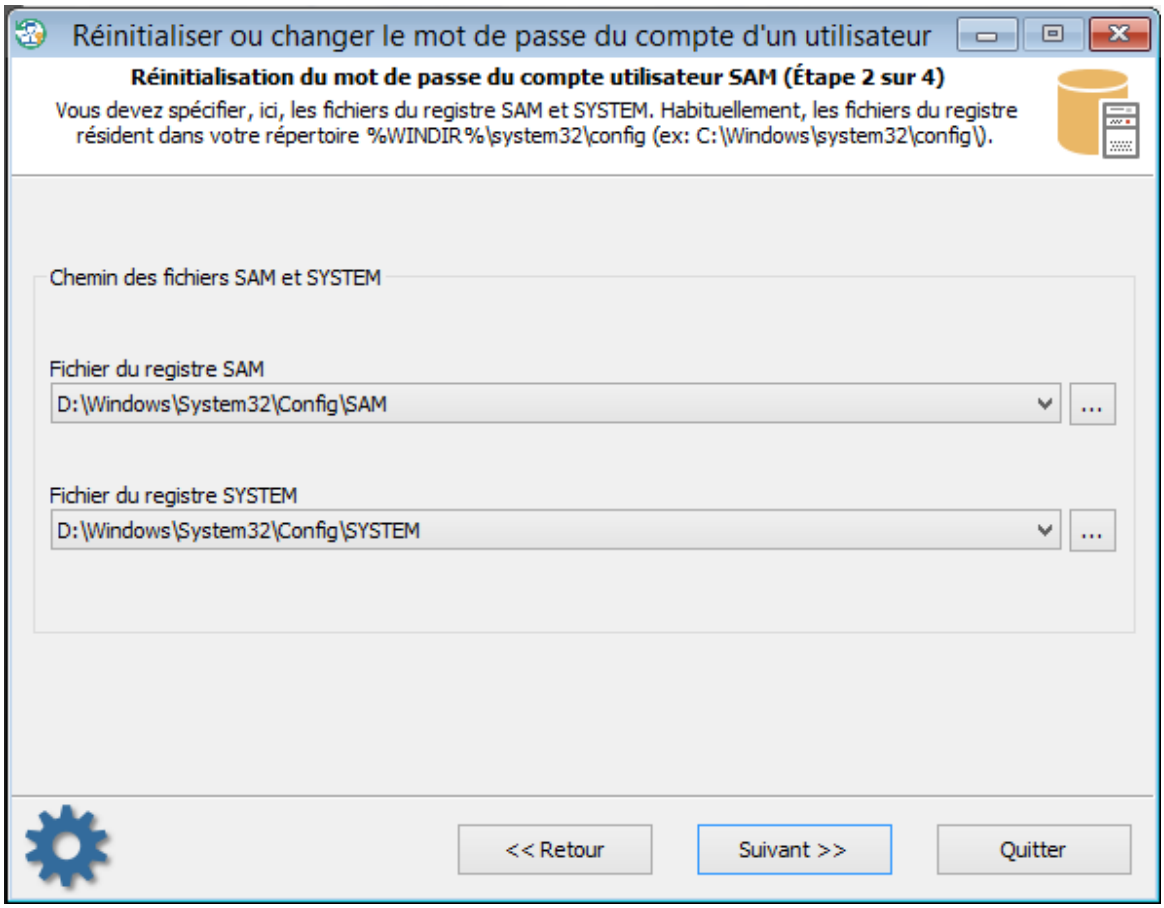
Active Directory
Pour un compte d'utilisateur de Domaine: Les hachages de mots de passe sont stockés dans le fichier NTDS.DIT de la base de données, sur le PC du Domaine.

DCC
Pour les identifiants de connexion des comptes de Domaine en cache: Les hachages de mots de passe (en fonction des stratégies de groupes du Domaine) sur le PC local. Le "login" du compte est réalisé à l'aide du serveur de Domaine ou en en utilisant les paramètres d'identifications en cache.



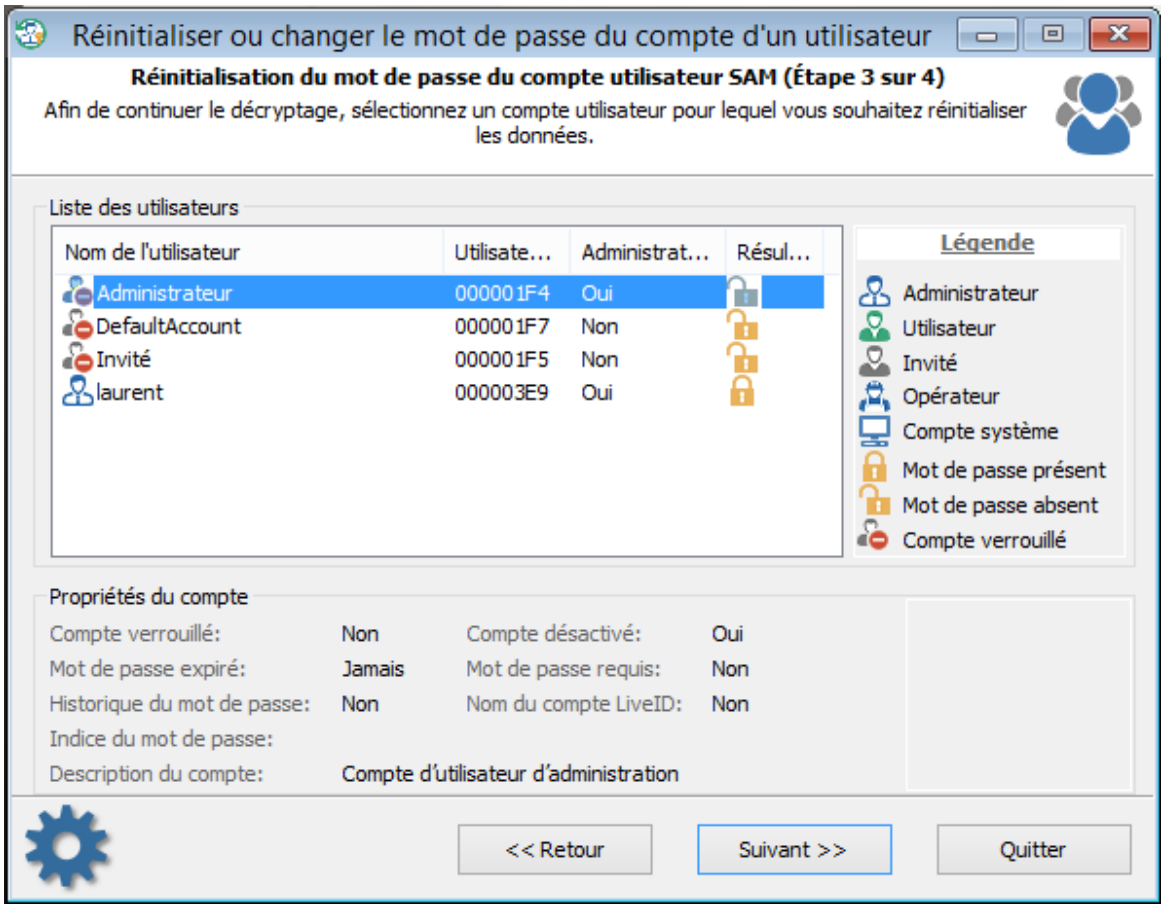
3.2 Réinitialiser ou changer le mode de passe du compte d'un utilisateur

Sélection les données source



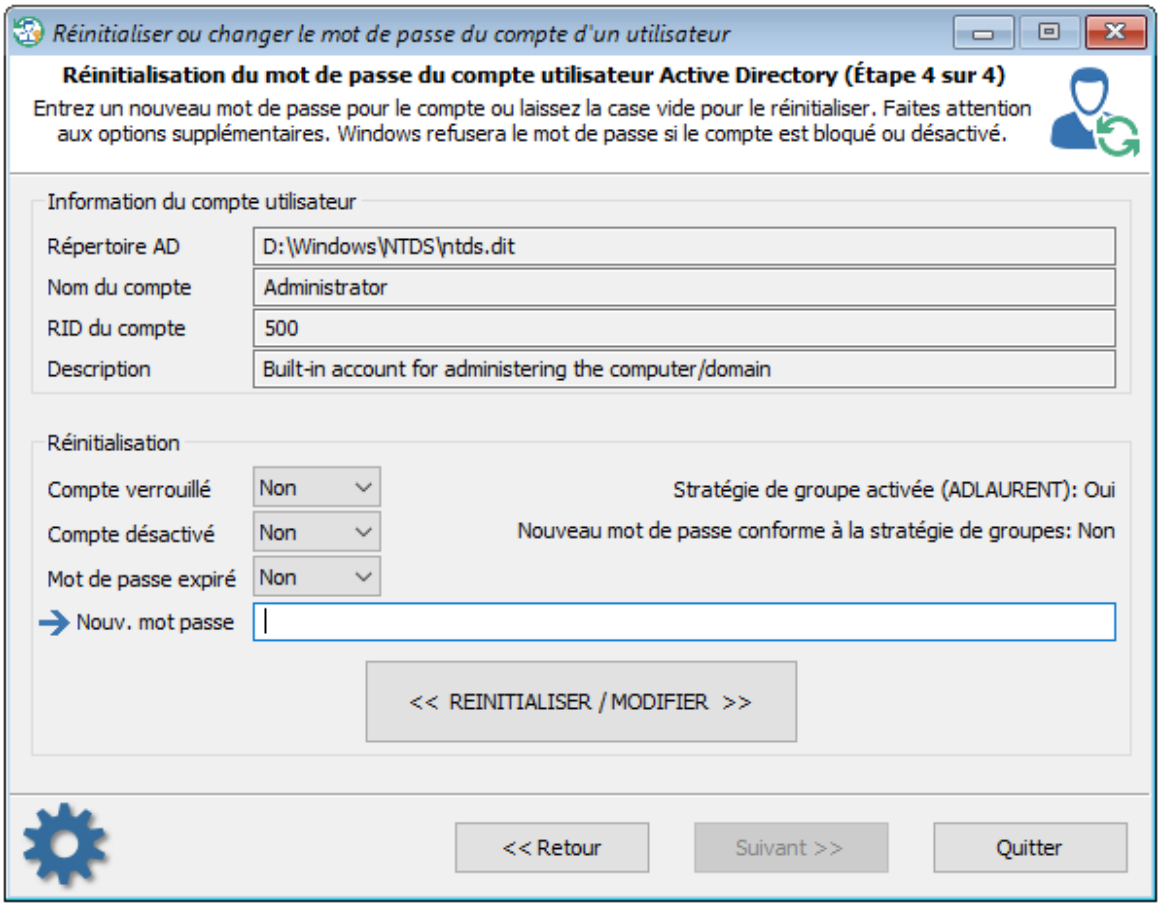
Pour réinitialiser un mot de passe de compte, vous devez sélectionner deux fichiers de la base de registre: **SAM** et **SYSTEM**. Le logiciel recherche automatiquement tous les fichiers et propose ceux trouvés en premier. Les fichiers de la base de registre sont présent dans le répertoire **%WINDIR%\system32\config**. Où %WINDIR% est le répertoire Windows.
Si vous avez sélectionné le mode Active Directory, à l'étape précédente, vous devez indiquer l'emplacement de la base de données de l'Active Directory, à la place du fichier SAM de la base de registre. Par défaut, c'est le répertoire **%WINDIR%\NTDS**. Et le chemin complet pour la base de données de l'AD peut être: C:\Windows\NTDS\ntds.dit

Choix du compte utilisateur Windows



Le haut de la fenêtre affiche la liste des comptes utilisateur trouvés. En cliquant sur l'un d'eux, vous pouvez voir les propriétés du compte, que ce soit, l'état d'un compte (verrouillé ou désactivé), le mot de passe nécessaire pour se connecter au compte, si un historique de mots de passe est disponible, si un indice pour le mot de passe est disponible, etc.

Réinitialiser le mot de passe



Pour réinitialiser le mot de passe, laisser le champ "*Nouv. mot passe*" vide et cliquer sur le bouton "*<< REINITIALISER / MODIFIER >>*".
Attention aux options du mot de passe. Le compte ne doit pas être verrouillé, désactivé ou expiré.

En outre, si les stratégies de sécurités des mots de passe locales ou de domaine sont activées, assurez-vous que le nouveau mot de passe corresponds à la longueur et la complexité définie et n'existe pas dans la liste des mots de passe utilisés précédemment (si un historique de mots de passe existe). Sinon, vous serez incapable de vous connecter au système même si vous réinitialisez le mot de passe avec succès.

Si vous réinitialisez un mot de passe Administrateur Windows, gardez à l'esprit que pour activer ce compte et vous connecter au système. Vous devrez démarrer le système en mode sans échec. Pour réaliser cela, avant que Windows démarre, garder la touche F8 appuyée jusqu'à ce que s'affiche à l'écran le menu de sélection de démarrage texte. Sélectionner dans la liste, le mode sans échec. Après cela, le compte Administrateur Windows sera actif, et il vous sera possible de l'utiliser.

Avec Windows 8 et les systèmes d'exploitation suivants, Appuyer sur le bouton d'alimentation, maintenez appuyé la touche SHIFT de votre clavier et sélectionner "Redémarrer".
Notez que vous devez saisir un mot de passe non vide, pour pouvoir ouvrir la session d'un compte Live ID ou Microsoft.

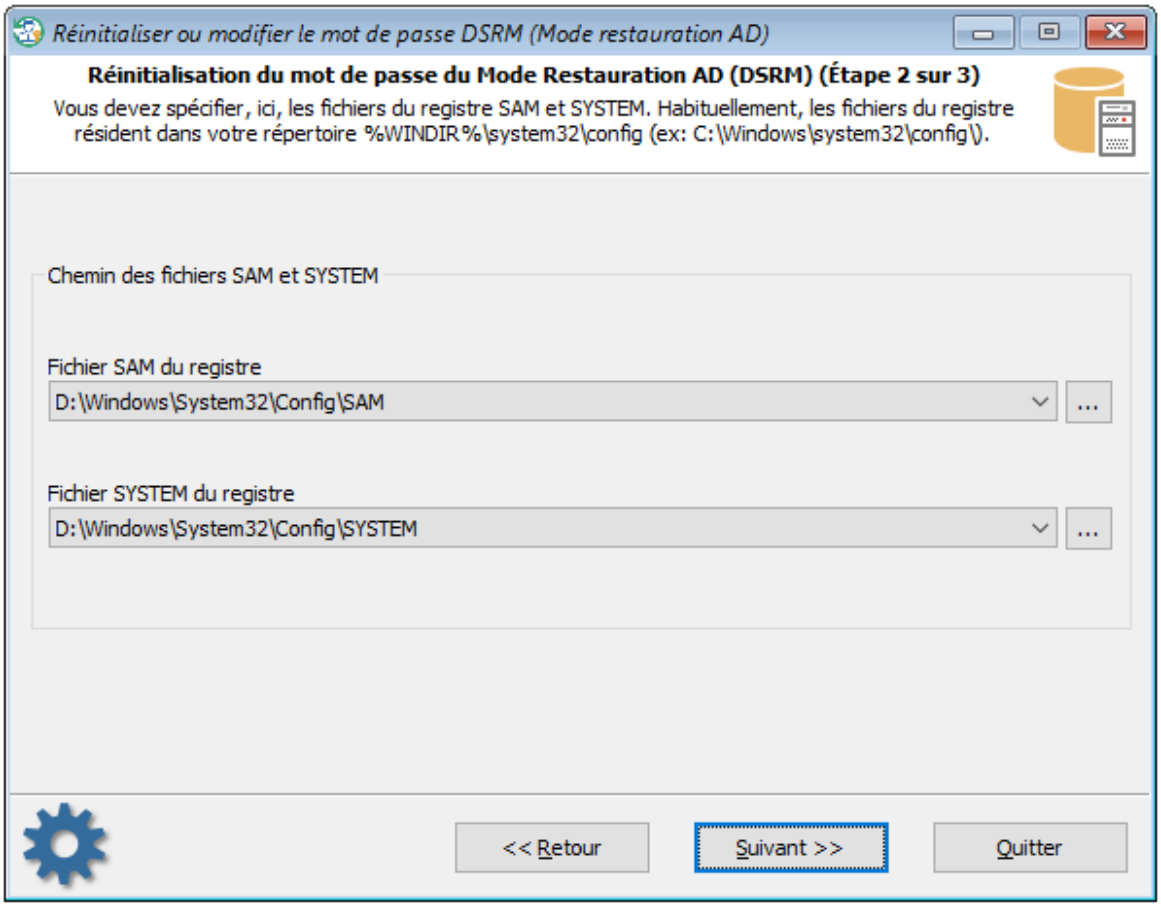
3.3 Réinitialiser le mot de passe DSRM

Qu'est ce que le DSRM

DSRM (connu sous le nom de **Directory Services Repair Mode** ou **Directory Services Restore Mode** dans les versions avant Windows Server 2012) est mode de démarrage spécial du contrôleur de Domaine de Windows Serveur qui est similaire au mode "Sans Échec" avec une connexion réseau, mais sans l'exécution de Active Directory. DSRM est utilisé pour restaurer l'Active Directory à partir d'une sauvegarde. C'est aussi utile dans différentes situations et problèmes avec l'Active Directory.

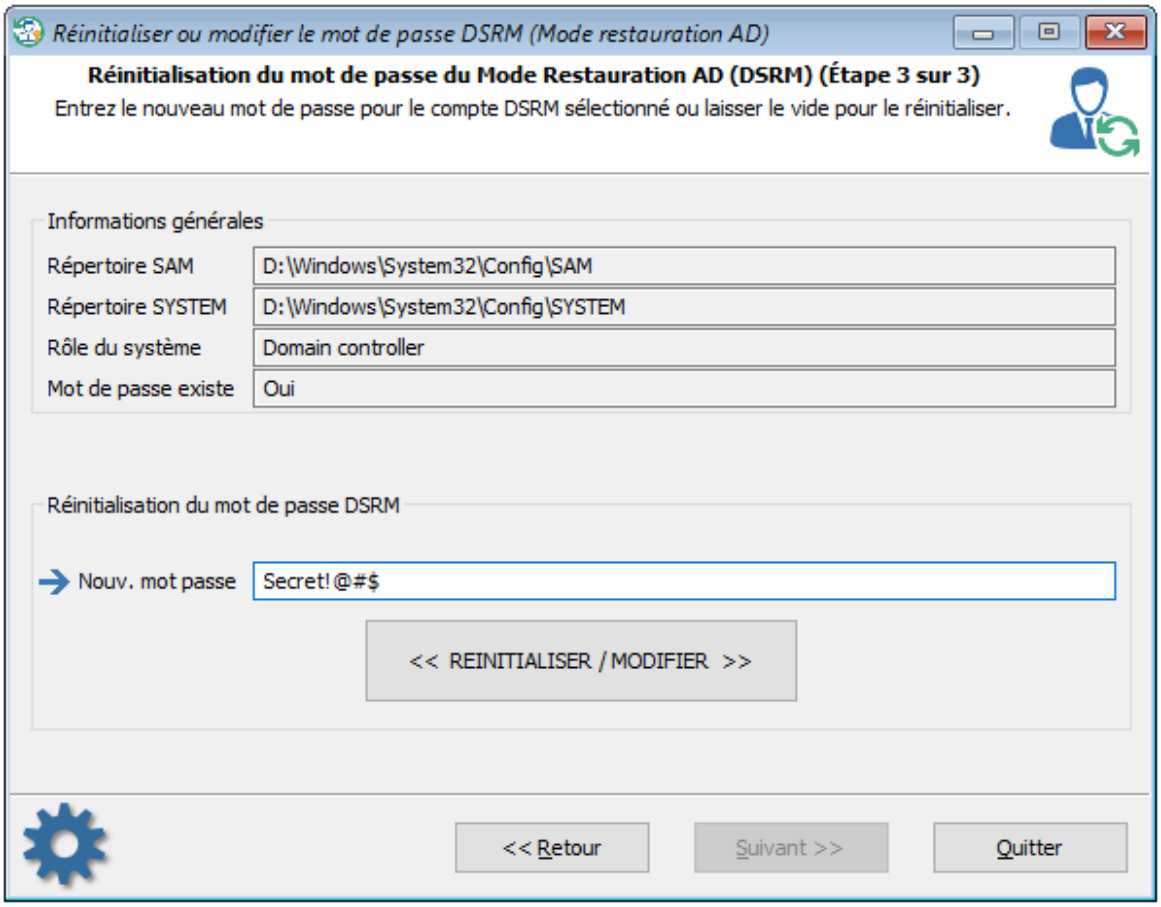
Pour entrer dans le mode DSRM, la première chose à faire est d'appuyer sur la touche F8, immédiatement après l'écran de démarrage BIOS/UEFI, mais avant qu'apparaisse le logo de Windows. Dans Windows Serveur 2012 et les OS plus récent, il y a le menu "**Advanced Boot Options"** ou "**Windows Recovery Environment"** pour cela.

Sélection des données source



Le processus de récupération de mots de passe, pour le compte DSRM, est pratiquement le même que pour un compte d'utilisateur. En premier, vous devez spécifier l'emplacement des fichiers **SAM** et **SYSTEM** de la base de registre.

Réinitialisation du mot de passe

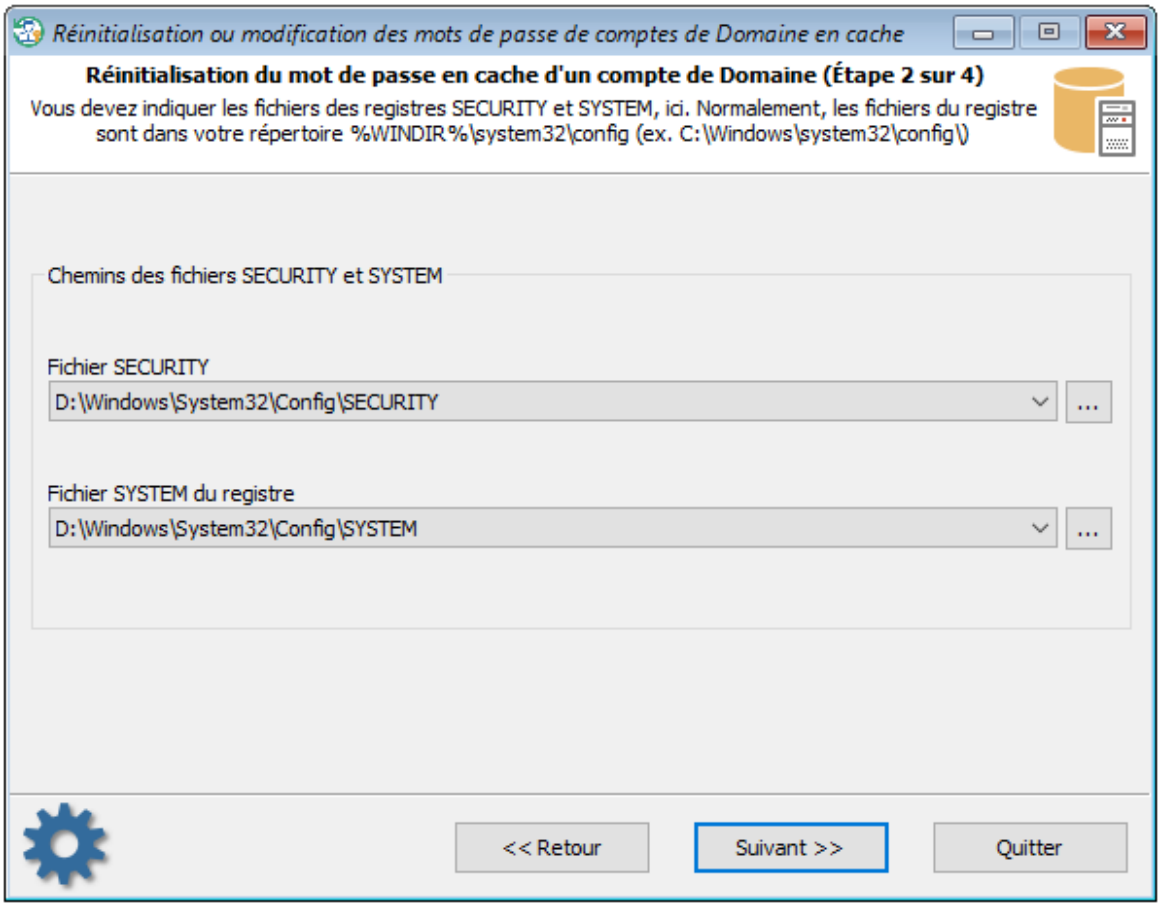


Saisisser un nouveau mode passe ou laisser le champ vide si vous souhaitez le réinitialiser. Puis, confirmer la modification en cliquant sur le bouton << REINITIALISER / MODIFIER >>. Le programme peut vous demander de créer un fichier de sauvegarde. Vous pourrez utiliser ce fichier, plus tard, pour annuler les modifications.

3.4 Réinitialiser du mot de passe en cache d'un compte de Domaine

Lorsqu'un utilisateur se connecte sur un Domaine, les paramètres d'identifications de connexion du Domaine sont sécurisés en cache et sauvegardés dans son PC. Cette fonctionnalité permets aux utilisateurs du Domaine d'ouvrir une session lorsque le réseau est déconnecté ou si le Domaine n'est pas disponible. Pour contourner le problème d'un mot de passe perdu ou oublié, vous pouvez simplement réinitialiser les paramètres d'identifications de connexion de Domaine en cache, en utilisant Reset Windows Password.
Le processus est seulement constitué, de 3 étapes simples.

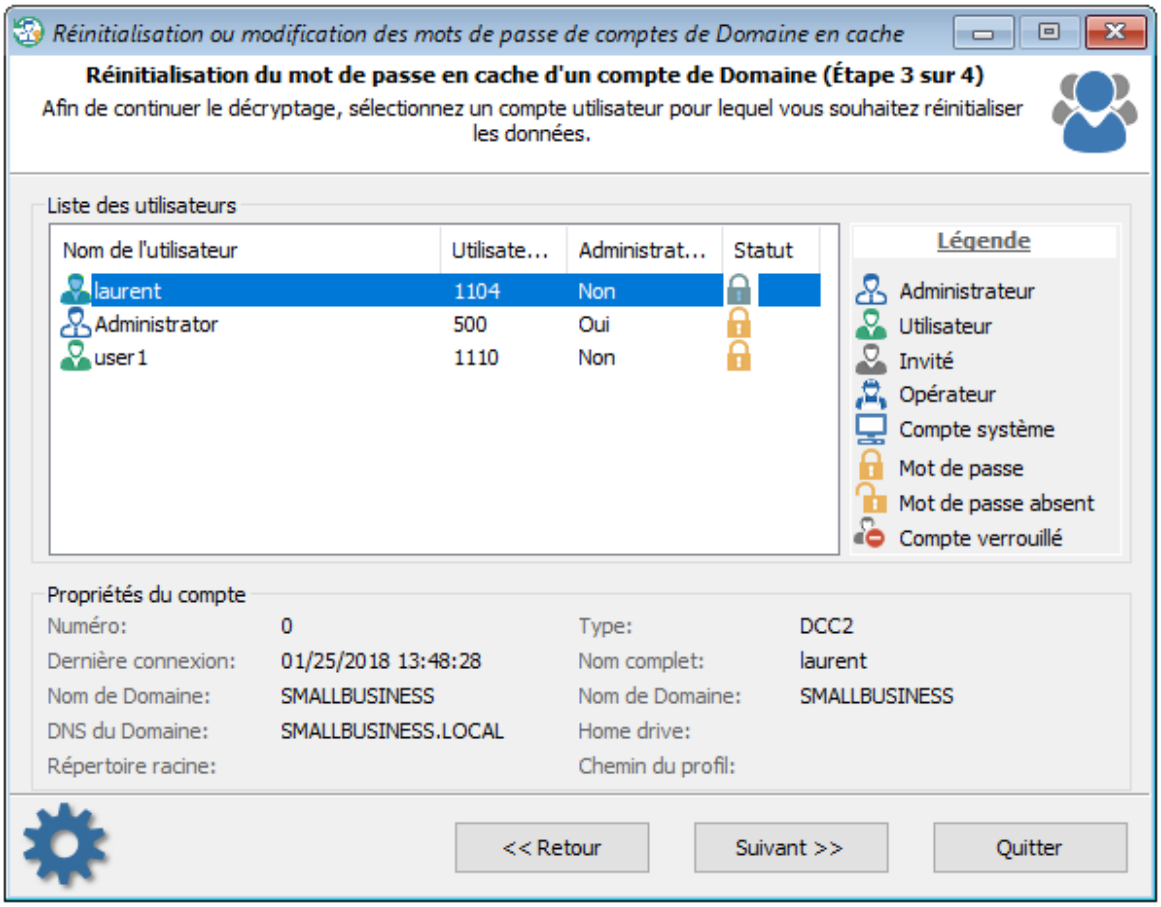
Sélection des fichiers de la base de registre



Pour réinitialiser un mot de passe de Domaine en cache, vous devez avez besoin de deux fichiers de la base de registre: **SECURITY** et **SYSTEM**.
Les deux fichiers sont localisés dans le répertoire **%WINDIR%\system32\config**. Où %WINDIR% est le répertoire Windows. Habituellement, le programme localise les fichiers pour vous et vous suggère leurs emplacements.

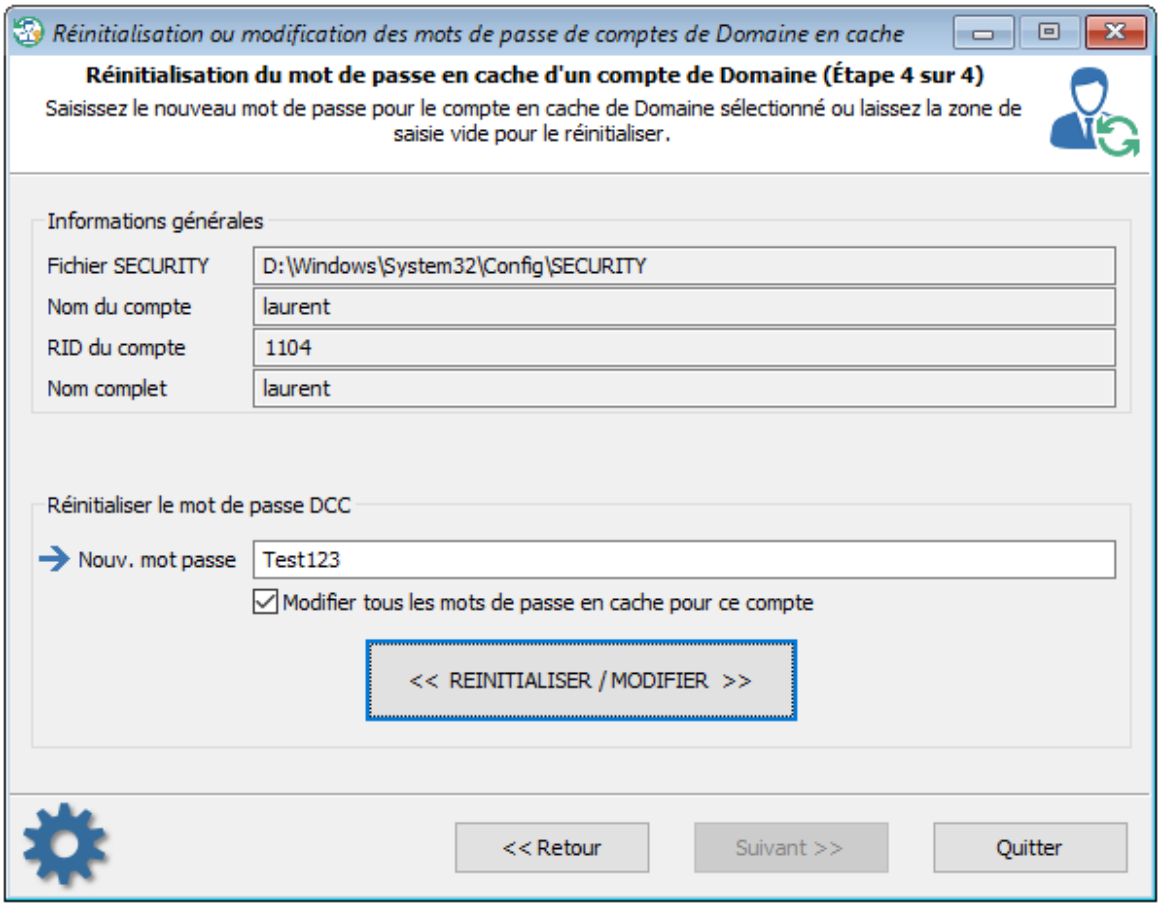
Avant de passer à la prochaine étape, assurez-vous que les fichiers sélectionnés sont ceux dont vous avez besoin.

Sélection du compte du Domaine



La partie supérieure de la boite de dialogue, vous affiche la liste des comptes d'utilisateurs en cache trouvée avec le nom de chaque utilisateur du compte.
Sélectionner un des utilisateurs pour visualiser ses propriétés: Le nom complet de l'utilisateur du compte, la date de la dernière connexion, le nom du Domaine, le répertoire racine, etc.

Réinitialisation du mot de passe



Pour réinitialiser le mot de passe, laisser la zone de saisie "*Nouv. mot de passe*' vide et cliquer sur le bouton "*REINITIALISER/MODIFIER*".

Soyez attentif à l'option complémentaire disponible.
Le cache du Domaine est organisé de telle manière qu'il peut contenir plusieurs entrées pour un même utilisateur. Si l'option "*Modifier tous les mots de passe en cache pour ce compte*' est activée, alors le programme essayera de réinitialiser/modifier les mots de passe de toutes les entrées du compte sélectionnées (spécifié par le RID). Sinon, il réinitialisera le mot de passe, uniquement pour l'entrée sélectionnée. Il est recommandé de laisser cette option activée si vous ne savez pas quoi choisir.

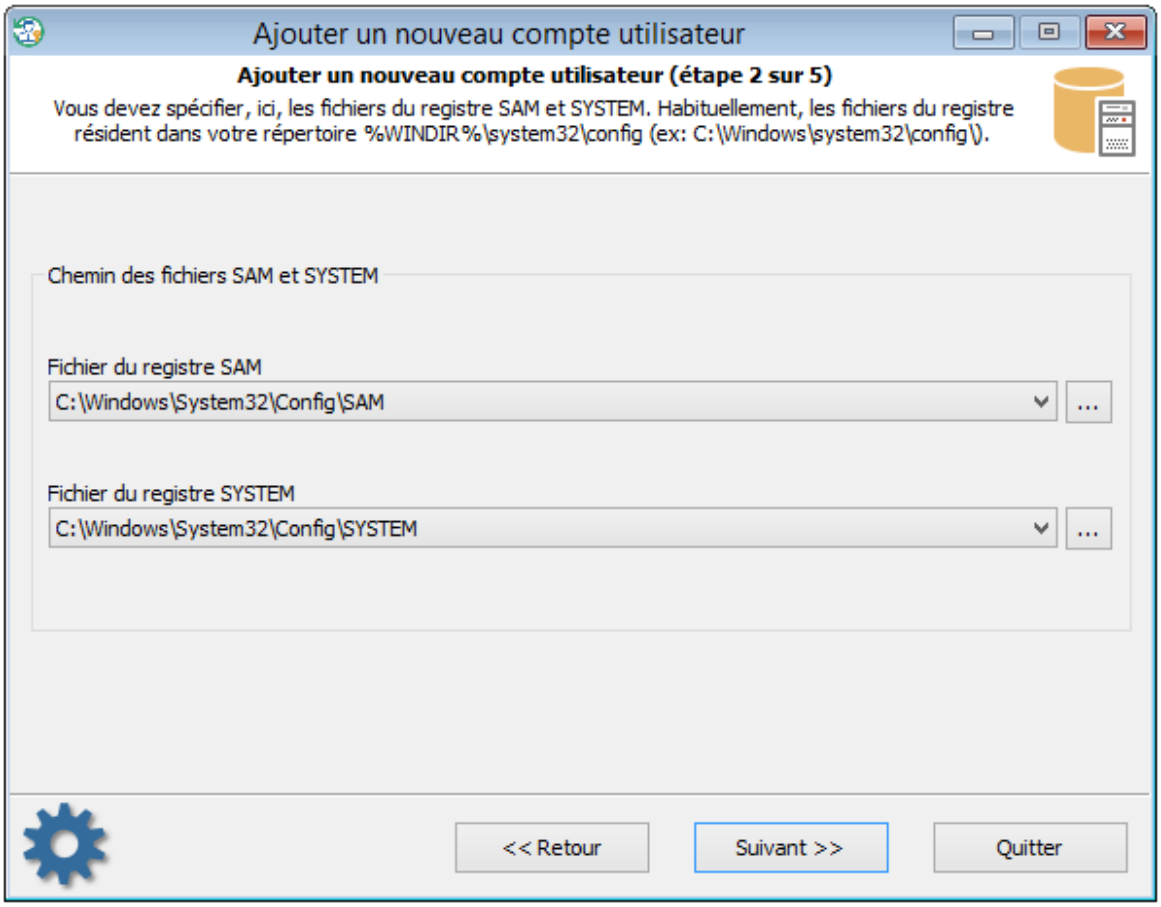
Assurez-vous que le nouveau mot de passe corresponds aux critères de la stratégie de groupes du Domaine (longueur et complexité) et n'est pas identique aux mots de passe précédemment utilisés (si la stratégie de groupe et l'historique des mots de passe est utilisée). Sinon, Windows peut refuser l'accès même si le mot de passe a été changé avec succès.
Notez, que pour ouvrir une session de votre compte de Domaine avec succès après que le mot de passe en cache a été réinitialisé, vous devez temporairement **désactiver la connexion au Domaine** ! Sinon, n'utilisera pas l'entrée en cache locale mais les paramètres d'identifications de connexions de Domaine à la place.

Gardez à l'esprit, que de se connecter avec des paramètres d'identifications en cache, vous donnera uniquement accès aux ressources locales.

3.5 Ajouter un nouveau compte utilisateur

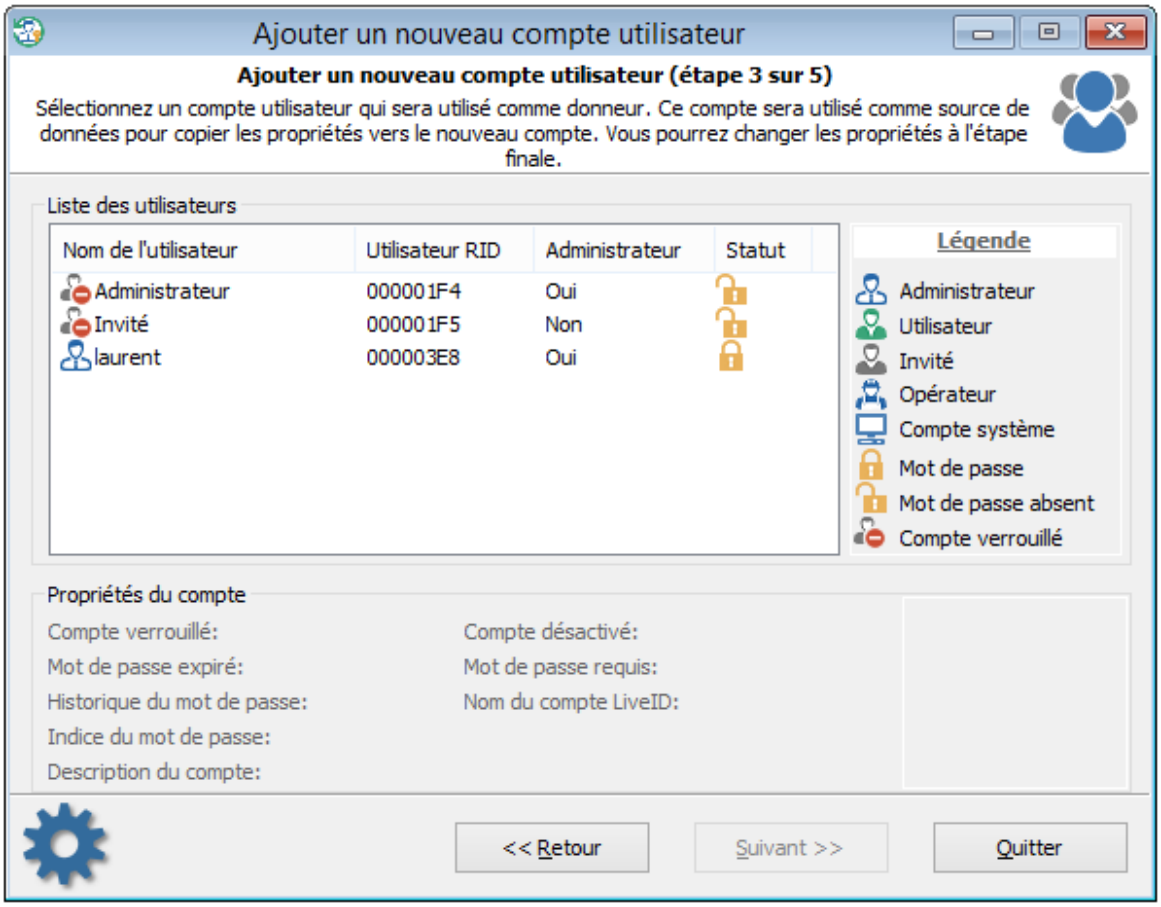
Ajouter un nouveau compte local est très facile. Cela se déroule en trois étapes.

1. Sélectionnez les fichiers sources



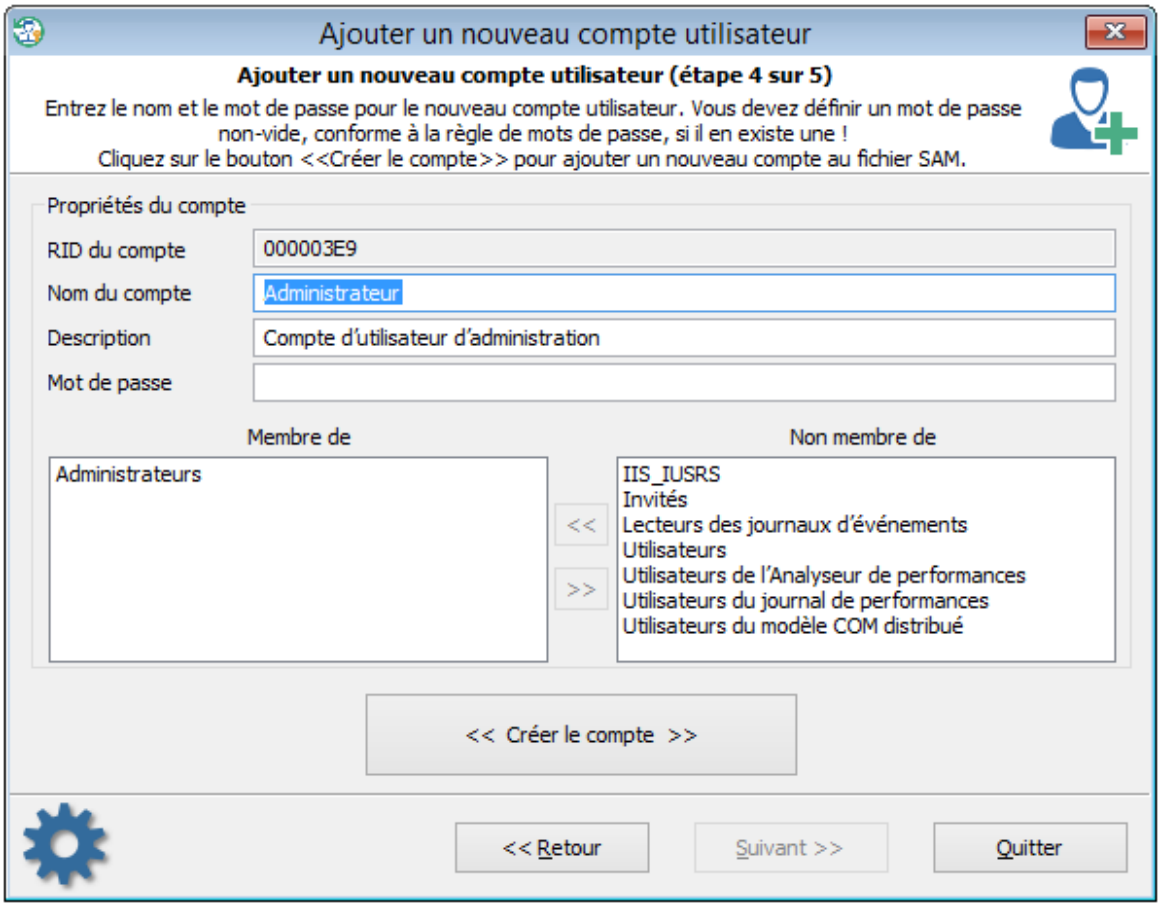
Vous devez sélectionner, d'abord, les fichiers **SAM et SYSTEM**. Le programme effectue une recherche, en général, puis suggère les fichiers automatiquement. Dans le cas où vous avez besoin de définir manuellement les fichiers, sachez qu'ils sont situés dans le répertoire **%WINDIR%\system32\config**.

2. Sélectionnez le compte source



Sélectionner l'utilisateur dont le compte sera utilisé comme compte source. Toutes les propriétés du compte source seront copiés vers le nouveau compte créé. Même si le compte est verrouillé ou désactivé, cela ne pose aucun problème. Le programme corrigera les propriétés importantes du compte et définira les valeurs par défauts. Par exemple, si le compte source est configuré pour permettre de se connecter au système à certaines heures, le programme réinitialisera la restriction.

3. Ajouter le nouveau compte



Maintenant, vous devez définir le nom, la description et le mot de passe du nouveau compte. Laisser le champ du mot de passe vide, pour ne pas configurer le compte avec un mot de passe. Notez que si l'OS a une règle de sécurité définie pour les mots de passe, votre nouveau mot de passe doit être conforme à cette règle.

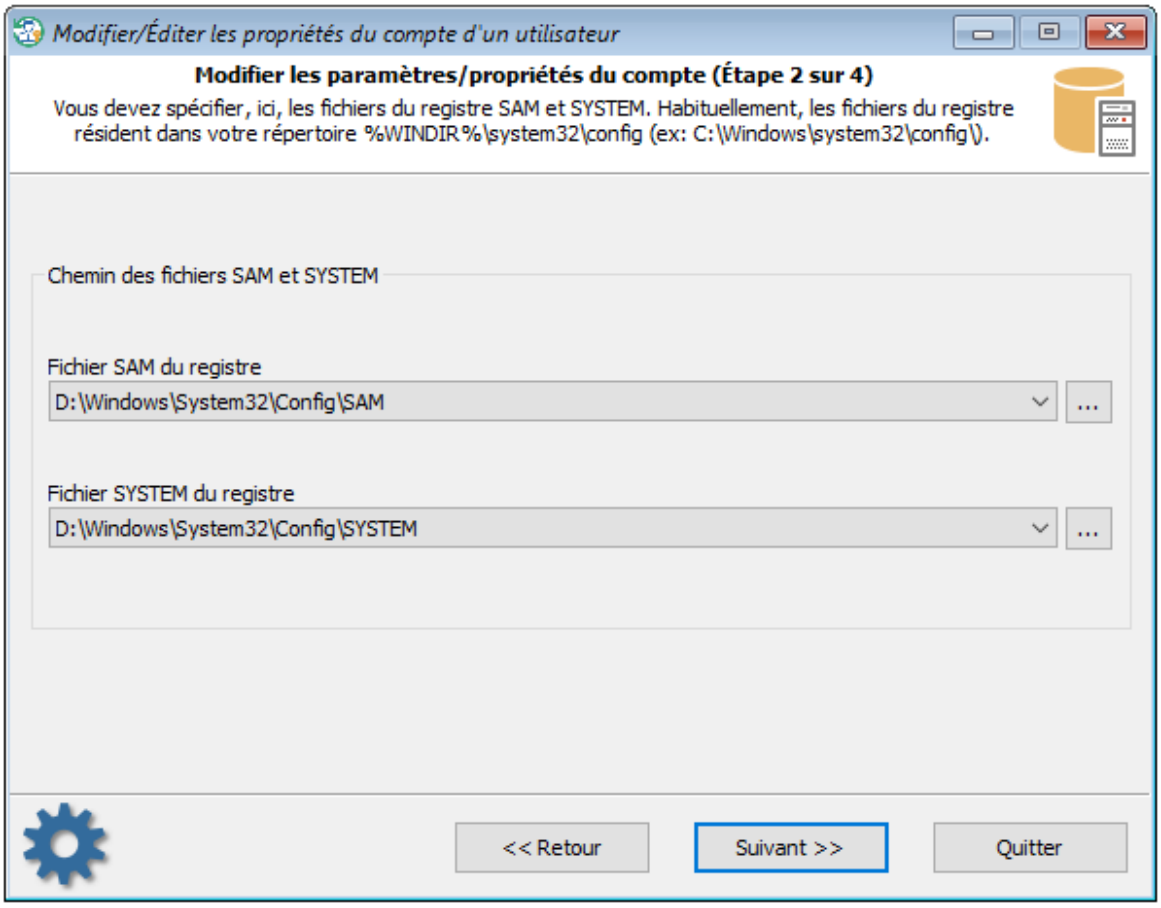
Vous devez apporter une attention spéciale aux paramètres du groupe dont dépends le nouveau compte. Normalement, il doit être membre du groupe "Administrateurs" et/ou "Utilisateurs" pour être capable de vous connecter localement, si cela n'est pas spécifié par votre stratégie de groupe. Si vous ne paramétrez pas correctement le groupe, cela peut causer des problèmes, par exemple, la suppression du compte.

Après la création avec succès du compte, vous pouvez retourner à la fenêtre de dialogue principale, sélectionner le mode "Éditer les propriétés d'un compte" et activer/désactiver les paramètres étendus, si nécessaire.

3.6 Modifier/Editer les propriétés du compte d'un utilisateur

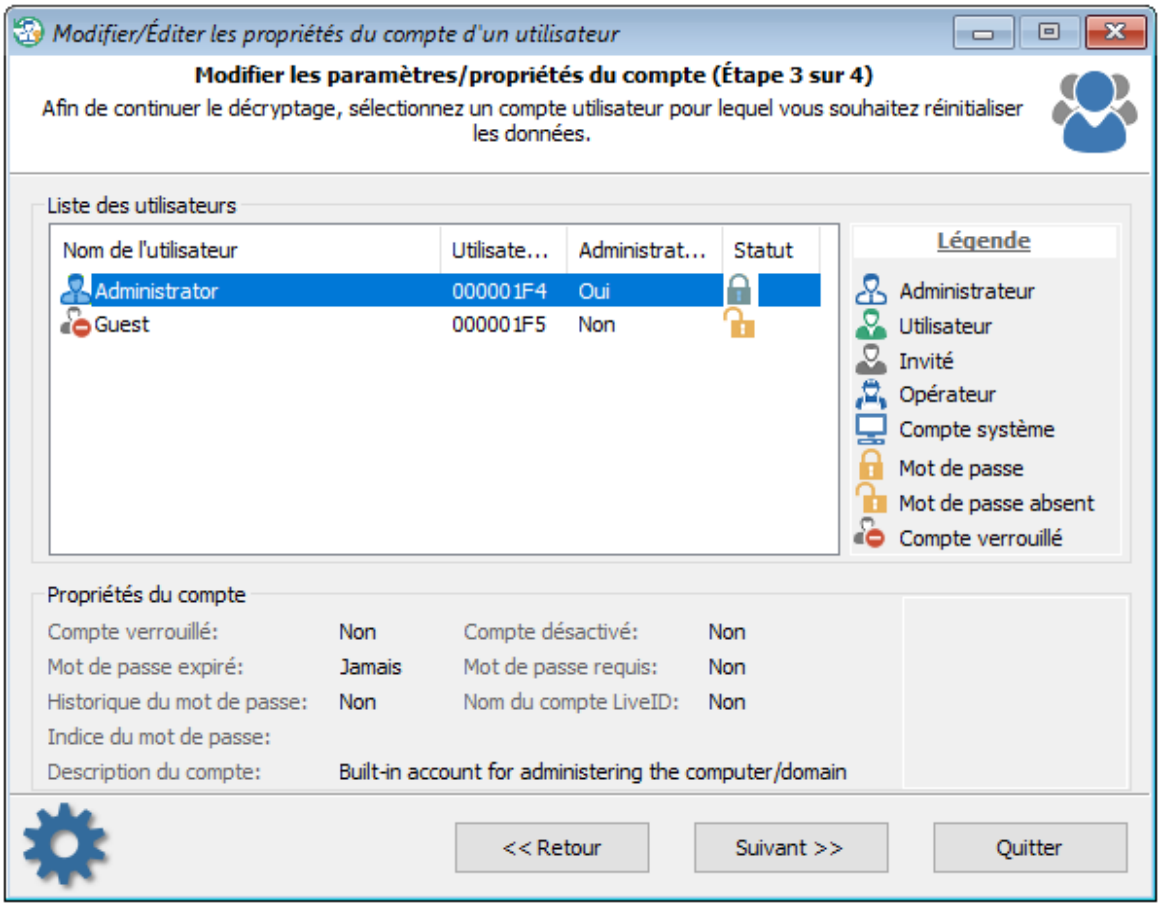
La nouvelle version du programme permets la manipulation des propriétés étendues du compte d'un utilisateur et aussi de changer un compte Live ID Microsoft en un compte local et vice versa.
Cela est extrêmement utile lorsque vous avez besoin de déverrouiller/activer ou verrouiller/désactiver un compte, dévalider le statut du "Mot de passe expiré", désactiver le "Connexion avec une carte à puce" si votre carte à puce a été perdu temporairement, etc.
Modifier les propriétés d'une compte ayant un problème est très facile. En premier, vous devez sélectionner les fichiers du système d'exploitation.

Sélection des données source



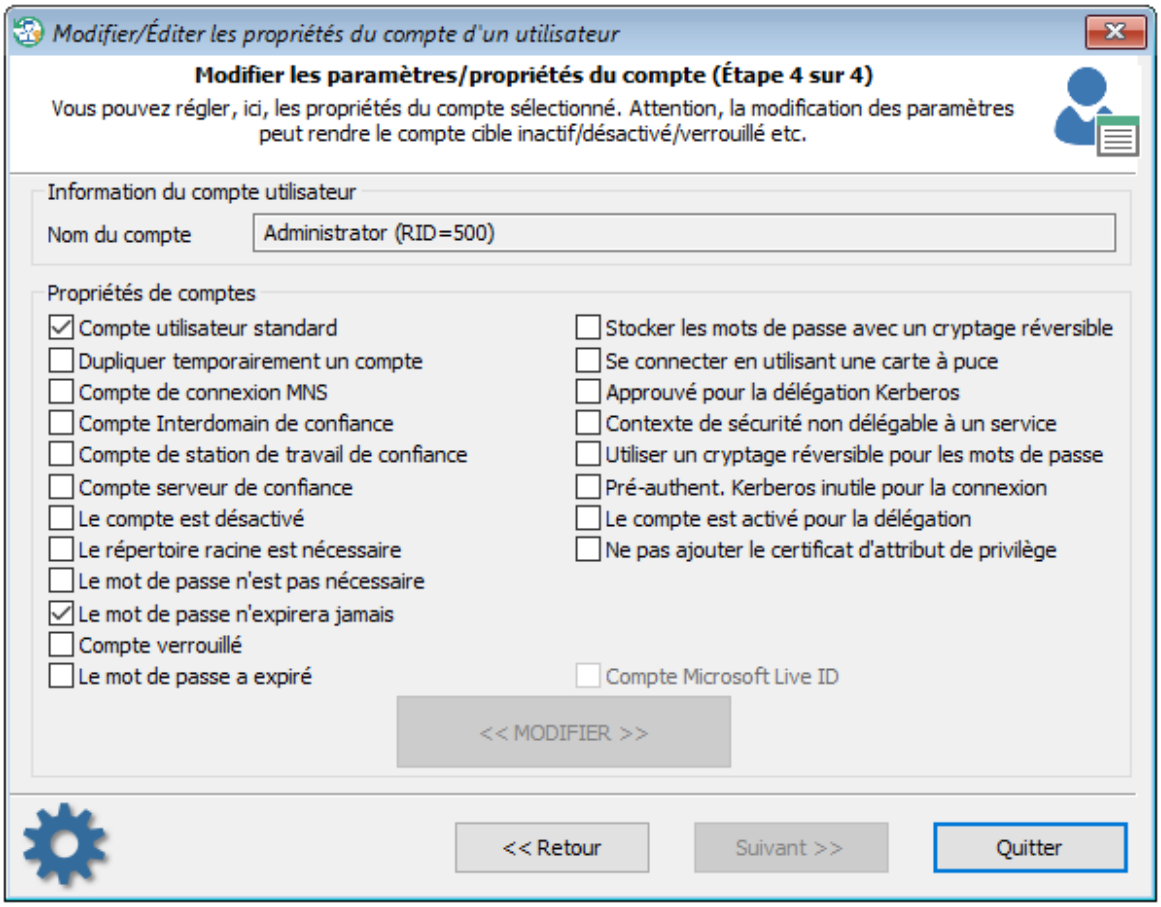
Deux fichiers sont nécessaires. Il s'agit des fichiers **SAM** et **SYSTEM** (dans le cas où vous modifiez un compte local) ou **NTDS.DIT** et **SYSTEM** (lorsque vous devez changer les propriétés d'un utilisateur de domaine). Le programme recherche automatiquement ces fichiers et propose les premiers trouvés. Vous pouvez sélectionner le chemin de ses fichiers manuellement.
Ces fichiers sont localisés dans les répertoires **%WINDIR%\system32\config** et **%WINDIR%\NTDS**. Où %WINDIR% est le répertoire Windows. Du coup, le chemin complet pour la base de données de l'Active Directory ressemblera au chemin suivant: C:\Windows\NTDS\ntds.dit.

Choix d'un compte utilisateur Windows



Une fois que les fichiers sources ont été choisis, le programme liste et affiche tous les comptes utilisateur trouvés. Sélectionner celui que vous souhaitez modifier, puis cliquer sur le bouton "Suivant >>" pour ouvrir la page suivante avec les propriétés des utilisateurs.

Modifier les propriétés d'un compte

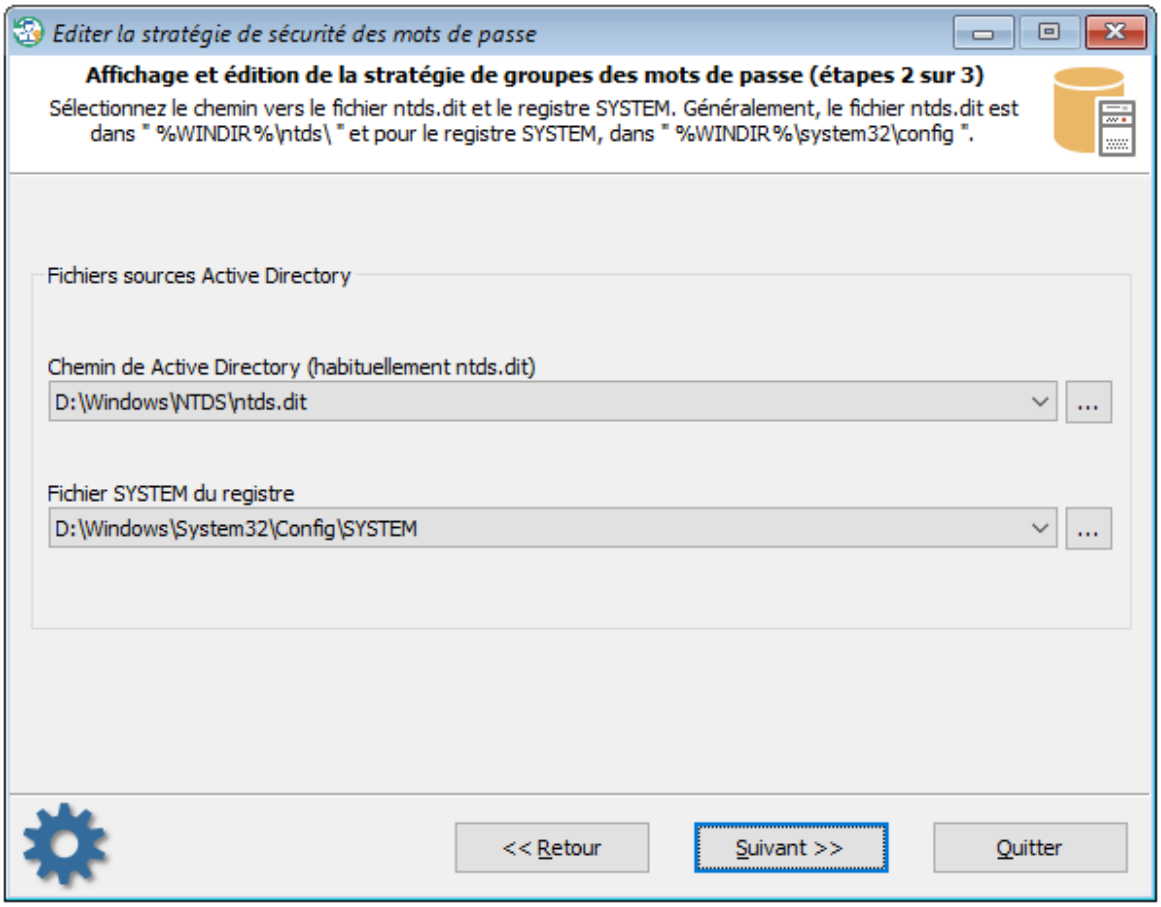


Vous pouvez, ici, activer/désactiver différents paramètres qui contrôle l'ensemble du compte utilisateur.
Attention, la modification de certains paramètres peut verrouiller/désactiver le compte concerné etc.

3.7 Éditer la stratégie de sécurité des mots de passe

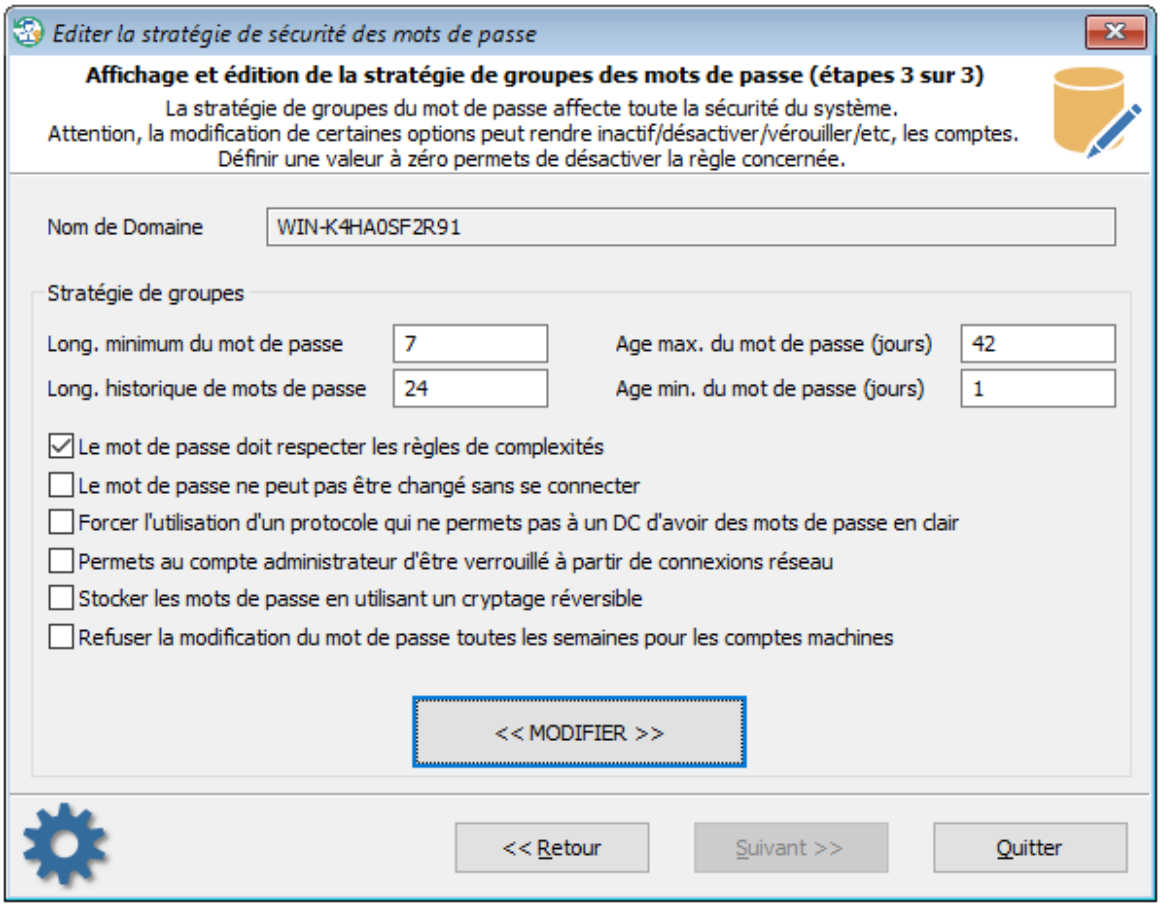
Parfois, pour que les paramètres de sécurité fonctionnent correctement, il est important de configurer les stratégies de sécurité des mots de passe des postes de travail ou du Domaine.
Par exemple, si vous voulez refuser l'accès, à des utilisateurs du Domaine, sans des mots de passe forts, vous devez mettre en place des restrictions à l'aide de stratégies de sécurité de mots de passe de Domaine. Cependant, cela peut être un problème si vous ne pouvez pas vous connecter à un poste de travail ou au Domaine en tant qu'administrateur.
Le nouvel éditeur de stratégie de sécurité de mots de passe de RWP, permets de contourner ce problème et permets de changer différents paramètres de la stratégie de sécurité de mots de passe, de tous les systèmes Windows sans se connecter au système.

Sélection des données source



En tout premier, vous devez fournir au programme deux fichiers systèmes:
- Soit **SAM** et **SYSTEM,** dans le cas où vous voulez modifier la stratégie de sécurité de mots de passe d'une station de travail ou d'un PC local (hors Domaine);
- ou **NTDS.DIT** et **SYSTEM,** lorsque vous devez changer les propriétés de la stratégie de sécurité de mots de passe d'un Domaine.
Le programme essayera de localiser les fichiers automatiquement. Vous pouvez, cependant, fournir les chemins de l'emplacement des fichiers manuellement.

Modifier la stratégie de sécurité de mots de passe



Descriptions des modifications possibles dans les stratégies de sécurité de mots de passe du système cible:

- Long. minimum du mot de passe - longueur minimum d'un mot de passe valide, nombre de caractères.
- Long. historique de mots de passe - nombre de mots de passe précédemment sauvegardés dans la liste de l'historique de mots de passe. Un utilisateur n'est pas autorisé à réutiliser un mot de passe de la liste.
- Age max. du mot de passe (jours) - temps maximum (en jours) d'utilisation d'un mot de passe. A l'issue de cette durée le système, les mots de passe doivent être changés son mot de passe.
- Age min. du mot de passe (jours) - temps minimum (en jours) avant que le mot de passe puisse être changé.

- Les mots de passe doivent respecter les règles de complexités - Les mots de passe doivent respecter les minimum requis: ne pas contenir de nom de compte d'utilisateur ou une partie, avoir une longueur d'au moins six caractères de long (sinon il n'est pas pris en compte), contenir des caractères à au moins trois sortes de caractères (une majuscule et/ou une minuscule et/ou un chiffre et/ou un caractère non alphabétique), ne pas avoir été utilisé précédemment (si l'historique de mots de passe est activé).
- Les mots de passe ne peuvent pas être changés sans se connecter - Les mots de passe ne peuvent pas être changés sans se connecter. Sinon, si il a expiré, vous pouvez le changer et ensuite ouvrir la session.
- Forcer l'utilisation d'un protocole qui ne permets pas à un DC d'avoir des mots de passe en clair - force le client a utiliser un protocole qui ne permets au contrôleur de Domaine d'avoir des mots de passe en clair.
- Permets au compte administrateur d'être verrouillé à partir de connexions réseau

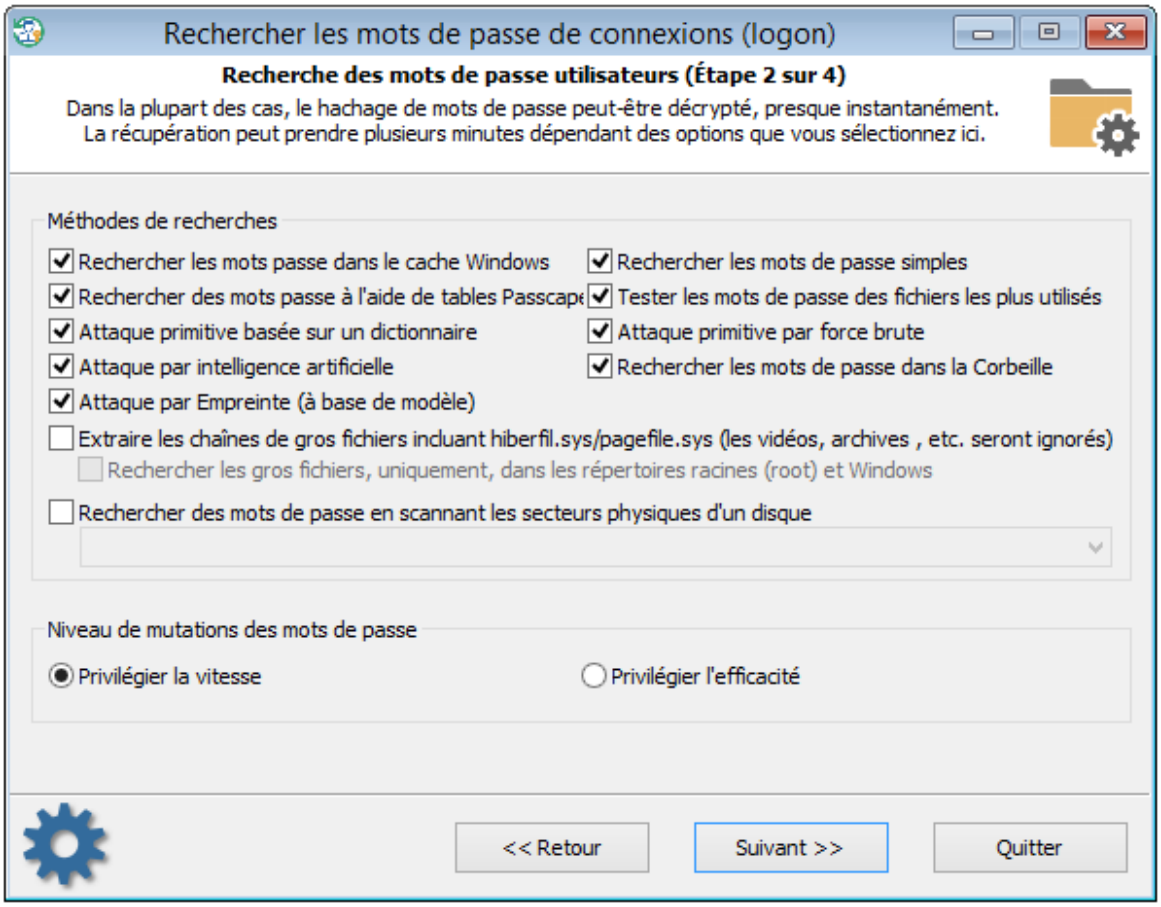
- Stocker les mots de passe en utilisant un cryptage réversible - force les mots de passe a être en clair pour tous les utilisateurs au lieu de hachages de mots de passe.
- Refuser la modification du mot de passe toutes les semaines pour les comptes machines - supprime la nécessité pour tous les comptes machine de changer automatiquement leur mot de passe toutes les semaines.

Pour désactiver un paramètre éditable, entrer une valeur à zéro dans la zone de saisie.

Attention, modifier un des paramètres de la stratégie de sécurités de mots de passe peut avoir un effet sur toute la sécurité système de Windows !

3.8 Recherche et récupération de mots de passe de connexions (logon)

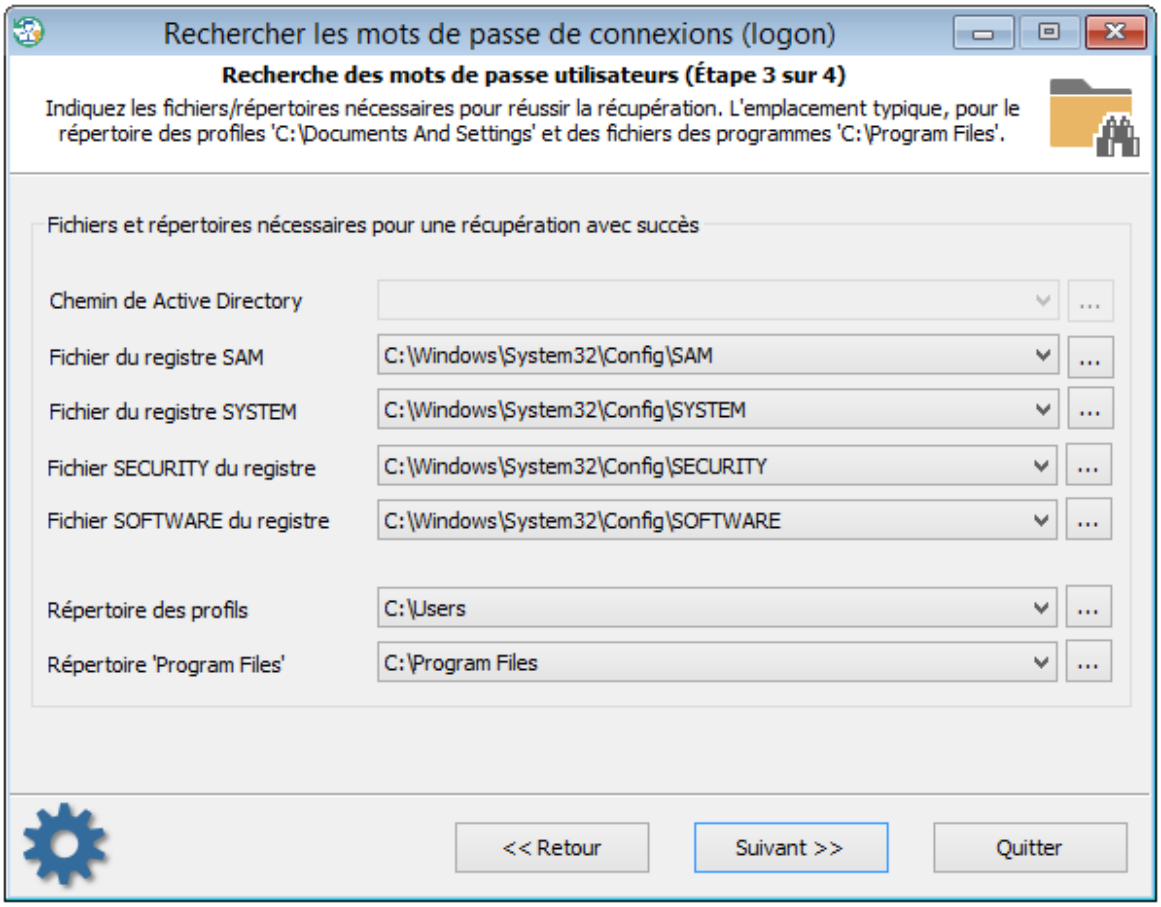
Paramétrage de la recherche et méthodes de récupérations



La recherche des mots de passe d'utilisateurs se réalise en 11 étapes:

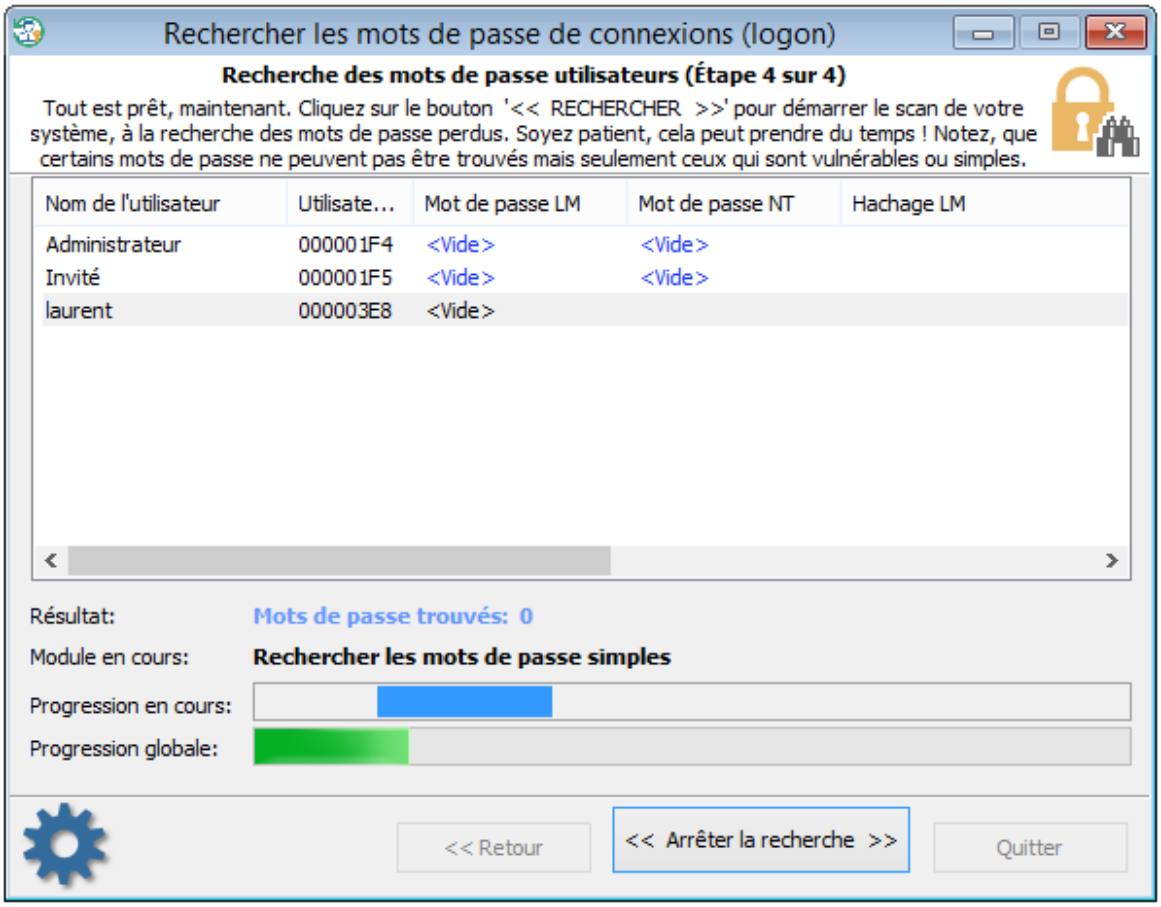
1. La recherche d'informations dans le cache système de Windows. Cette méthode est constituée de plus d'une douzaine de mini-attaques durant lesquelles, le programme analyse toutes les sortes de mots de passe, allant des secrets jusqu'au mots de passe DSL, FTP, IM, etc.
2. Une analyse simple, et courte des mots de passe, des raccourcis claviers, etc.
3. La recherche de mots de passe utilise les tables Arc-en-ciel. Le programme est fourni avec un jeu de 8 tables NTLM simples. Même si la taille de la table générale (52 Mo) est trop petite pour attaquer les mots de passe complexes, cela n'est pas suffisant pour décrypter les plus courant. Cette fonctionnalité n'est pas disponible dans le mode de démonstration.
4. Le scan, la recherche et l'analyse des fichiers les plus récemment utilisés du système cible.
5. Une attaque primitive par dictionnaire. L'application teste tous les mots de passe à partir d'un dictionnaire fourni pour les versions de base et standard du programme ou à partir de plusieurs dictionnaires (Arabe, Chinois, Anglais, Français, Allemand, Portugais, Russe, Espagnol) pour la version avancée du programme. Si la recherche approfondie est activée, les mutations simples de mots seront aussi faites dans le compte pendant la recherche.
6. Une attaque primitive par force-brute.
7. L'attaque par Intelligence Artificielle. C'est notre petit "savoir-faire". L'attaque analyse l'activité réseau d'un utilisateur sur l'ordinateur, à l'aide de 30 mini-modules qui ont en charge cette tâche. Avec les résultats de l'analyse, l'application génère des préférences utilisateurs et un dictionnaire sémantique pour l'attaque, qui sera utilisé plus tard pour rechercher le mot de passe.
8. La recherche des mots de passe dans les fichiers supprimés.
9. L'attaque primitive par empreinte pour les mots de passe Anglais complexes.
10. L'extraction de chaînes à partir des fichiers de tailles importants: Images en RAM, hiberfil.sys, pagefile.sys et ainsi de suite. Lorsque cette option est activée, le programme essayera d'ignorer les fichiers inutiles dans l'analyse du mot de passe comme les vidéos, les archives, les fichiers audio (ex: mp3), etc.
11. La recherche de mots de passe est réalisé en lisant et analysant les secteurs bruts (RAW data) du lecteur sélectionné. Cette fonctionnalité s'applique pour les hachages LM ainsi que les NTLM et la recherche pour les mots de passe ASCII et UNICODE. Si le "*Niveau de mutations des mots de passe*" est sur "*Privilégier l'efficacité*", le programme essayera, en plus, de muter tous les mots de passe trouvés, sachant que le parcours de tous les secteurs du lecteur cible peut prendre beaucoup de temps. Notez que l'algorithme qui scanne les secteurs n'est pas utilisable avec les lecteurs dont le cryptage natif du disque est actif, comme Bitlocker ou TrueCrypt, par exemple.

Sélection des données source



Lors de la recherche des mots de passe, apporter une attention toute particulière aux fichiers et répertoires nécessaires pour le processus d'analyse. Sans cela, la recherche de mots de passe ne sera pas efficace. L'application trouve les fichiers automatiquement, mais parfois, lorsque l'ordinateur possède plusieurs systèmes d'exploitation installés, vous devez utiliser le "mode manuel", en sélectionnant vous-même les répertoires. Gardez aussi à l'esprit, que si l'ordinateur possèdent 2 disques durs ou plus, l'ordre des lettres sur ces disques peut-être complètement différent que dans le système original.

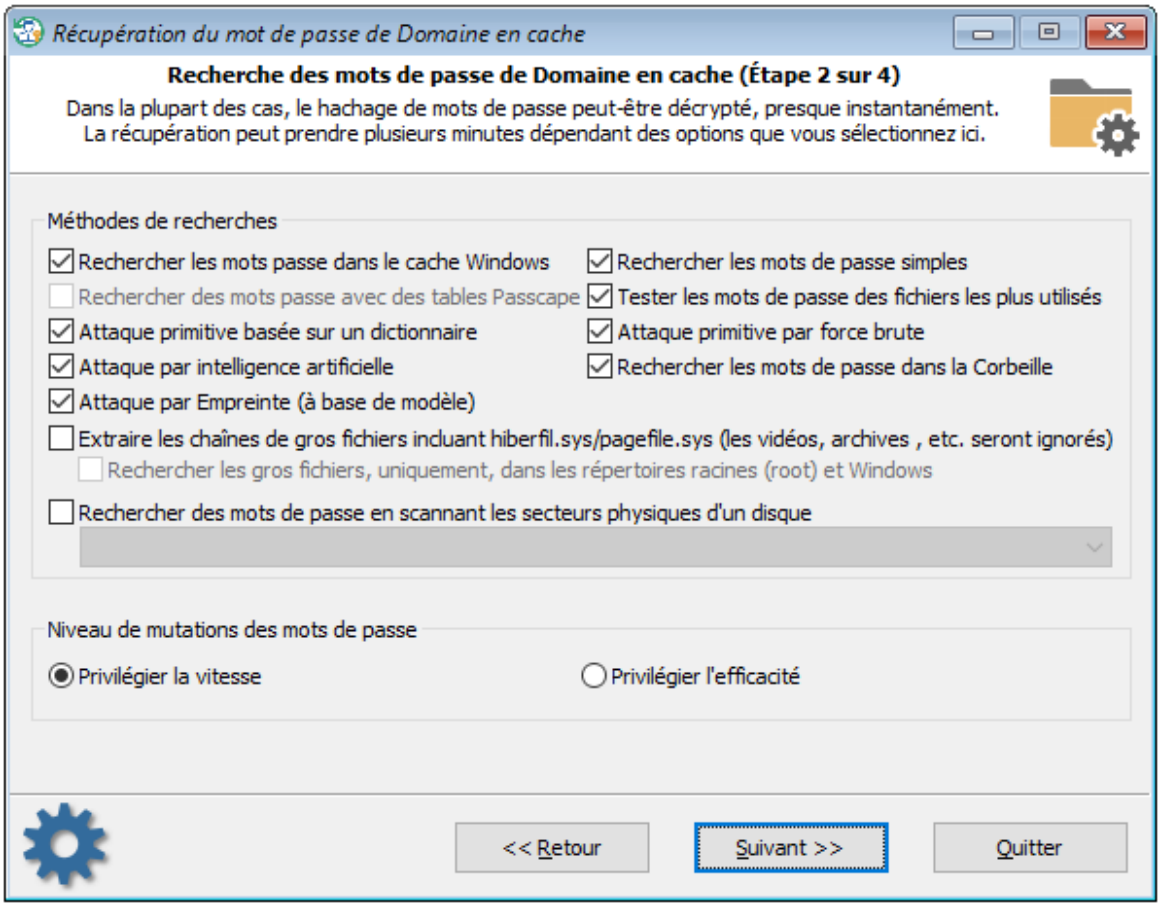
Rechercher et décrypter les mots de passe



La recherche et l'analyse de mots de passe peut prendre beaucoup de temps, en fonction des paramètres d'attaque et des particularités de votre système. Terminer la recherche prends, habituellement, 10-15 minutes sans tables Passcape et des attaques de recherches sur les disques. L'attaque à base de tables Passcape prends beaucoup plus de temps et dépends de votre CPU et du nombre de hachages à récupérer. Par exemple, sur un CPU à 2 cœurs cela prends habituellement jusqu'à 3 minutes pour un simple hachage.

3.9 Recherche et récupération de mots de passe de Domaine en cache

Définir les options de recherches et de récupérations



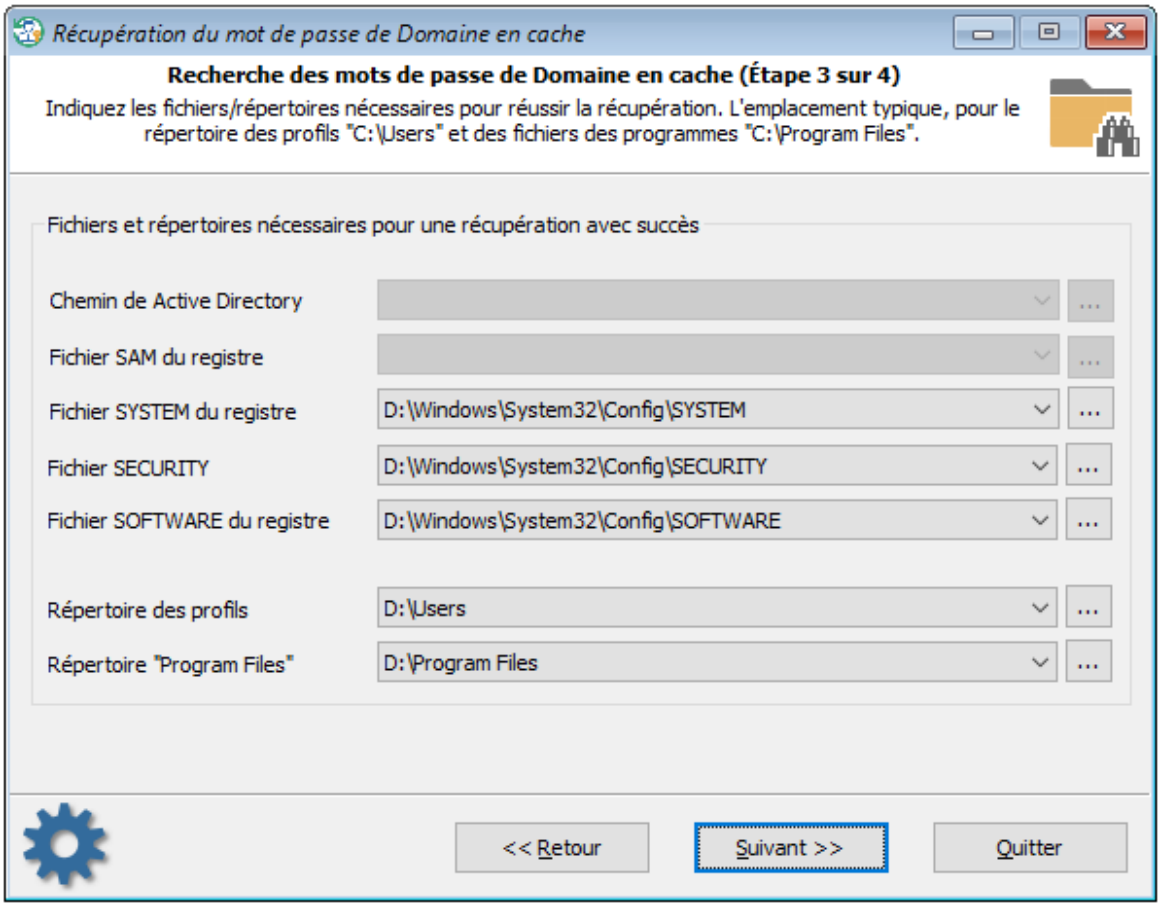
La récupération de mots de passe de Domaine en cache est constitué de plusieurs modules. Chacun d'eux peut être activé/désactivé séparément:

1. La recherche d'informations dans le cache système de Windows. Cette méthode est constituée de plus d'une douzaine de mini-attaques durant lesquelles, le programme analyse toutes les sortes de mots de passe: secrets LSA, DSL, FTP, LAN, mots de passe WAN, Internet et les identifiants de comptes e-mail, etc. Plus tard les mots de passe trouvés seront utilisés par le programme pour terster d'autres mots de passe en générant des variations plus complexes.
2. Une analyse simple, et courte des mots de passe, des raccourcis claviers, etc. A l'ai de 20 mini-modules au total.
3. Le scan, la recherche et l'analyse des fichiers les plus récemment utilisés du système cible. Le programme analyse les fichiers et crée une liste de mots (en générant différentes mutations) à tester comme mots de passe.
4. Une attaque primitive par dictionnaire. L'application teste tous les mots de passe à partir d'un dictionnaire fourni pour les versions de base et standard du programme ou à partir de plusieurs dictionnaires (Arabe, Chinois, Anglais, Français, Allemand, Portugais, Russe, Espagnol) pour la version avancée du programme. Si la recherche approfondie est activée, les mutations simples de mots seront aussi prises en compte pendant la recherche.
5. Le module d'attaque primitive par force-brute est constitué de plusieurs attaques simples pour rechercher les mots de passe courts.
6. Le module d'attaque par Intelligence Artificielle analyse l'activité réseau d'un utilisateur sur l'ordinateur, à l'aide de 30 mini-modules qui ont en charge cette tâche. Avec les résultats de

l'analyse, l'application génère des préférences utilisateurs et un dictionnaire sémantique pour l'attaque, qui sera utilisé plus tard pour rechercher le mot de passe.

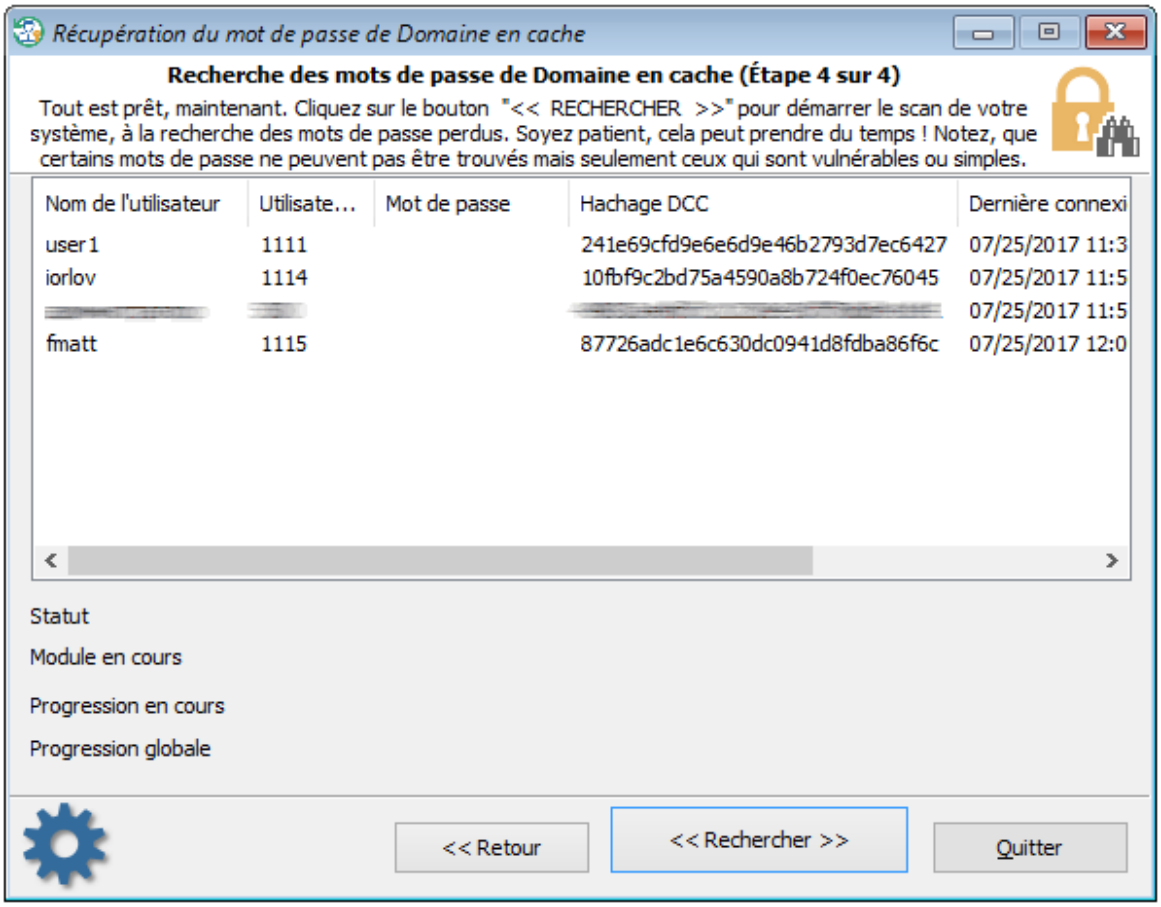
7. La recherche des mots de passe dans les fichiers supprimés.
8. L'attaque primitive par empreinte pour les mots de passe Anglais. L'exécution de ce module peut prendre beaucoup de temps.
9. L'extraction de chaînes à partir des fichiers de tailles importants: Images en RAM, hiberfil.sys, pagefile.sys et ainsi de suite. Lorsque cette option est activée, le programme essayera d'ignorer les fichiers inutiles dans l'analyse du mot de passe comme les vidéos, les archives, les fichiers audio (ex: mp3), etc.
10. La recherche de mots de passe est réalisé en lisant et analysant les secteurs bruts (RAW data) du lecteur sélectionné. Si le "*Niveau de mutations des mots de passe*" est sur "*Privilégier l'efficacité*", le programme essayera, en plus, de muter tous les mots de passe trouvés, sachant que le parcours de tous les secteurs du lecteur cible peut prendre beaucoup de temps. Notez que l'algorithme qui scanne les secteurs n'est pas utilisable avec les lecteurs dont le cryptage natif du disque est actif, comme Bitlocker ou TrueCrypt, par exemple.

Sélection des données source



Lors de la recherche des mots de passe de Domaine en cache, apportez une attention toute particulière aux fichiers et répertoires nécessaires pour le processus d'analyse. RWP trouve les fichiers automatiquement, mais parfois, lorsque l'ordinateur possède plusieurs systèmes d'exploitation installés, vous devez utiliser le "mode manuel", en sélectionnant vous-même les répertoires. Gardez aussi à l'esprit, que si l'ordinateur possèdent 2 disques durs ou plus, l'ordre des lettres sur ces disques peut-être complètement différent que dans le système original.

Recherche des mots de passe de Domaine en cache



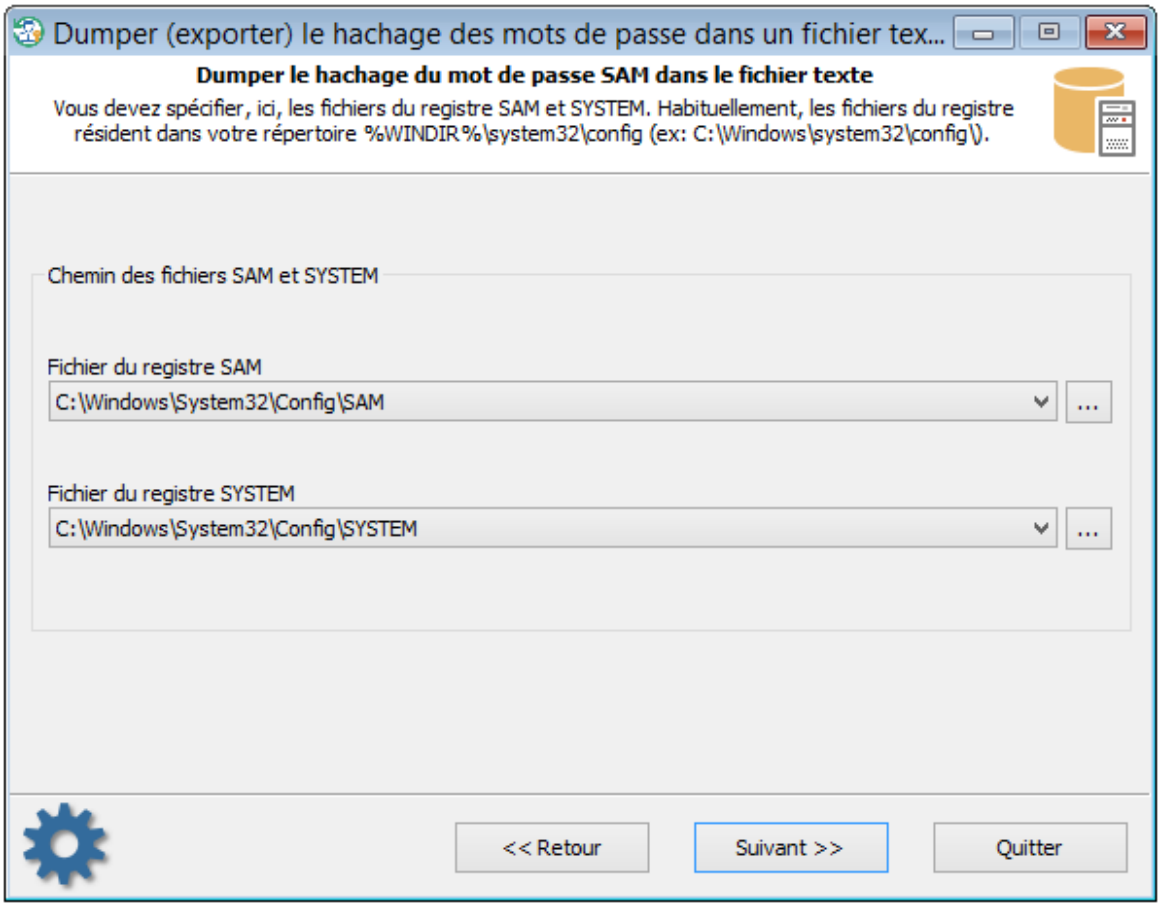
Les identifiants de Domaine en cache sont de deux types. DCC type 1 possède un cryptage très fible et était utilisé dans les systèmes d'exploitation Windows 2000, Windows XP et Windows 2003. Le taux de récupération peut dépasser des millions voir même des milliards de mots de passe par secondes. DCC type 2 est utilisé les systèmes d'exploitation Windows Vista et les générations suivantes plus récentes. Ce cryptage est beaucoup fort et résistant aux attaques de décryptage. La vitesse de l'attaque par Force-brute est seulement de centaines/milliers de mots de passe par secondes. Imaginer deviner un mot de passe de 8 caractères de long constitué de lettres majuscules et minuscules en utilisant l'attaque par Force-brute pourrait prendre plus de 1000 ans !

Vous devez prendre en compte les considérations suivantes:

- Le processus de recherche pour les DCC de type 2 est extrêmement lent. Terminer certains modules (par exemple, l'attaque par Empreinte) peut prendre des heures ou même des jours.
- Pour accélérer la recherche, sélectionner uniquement le compte dont vous recherchez le mot de passe. Faites, seulement, un clic droit sur l'entrée en cache et sélectionner "*Exclure tout hormis ceux sélectionnés*". Sinon, la vitesse de récupération de mots de passe sera réduite par un multiple du nombre de comptes.

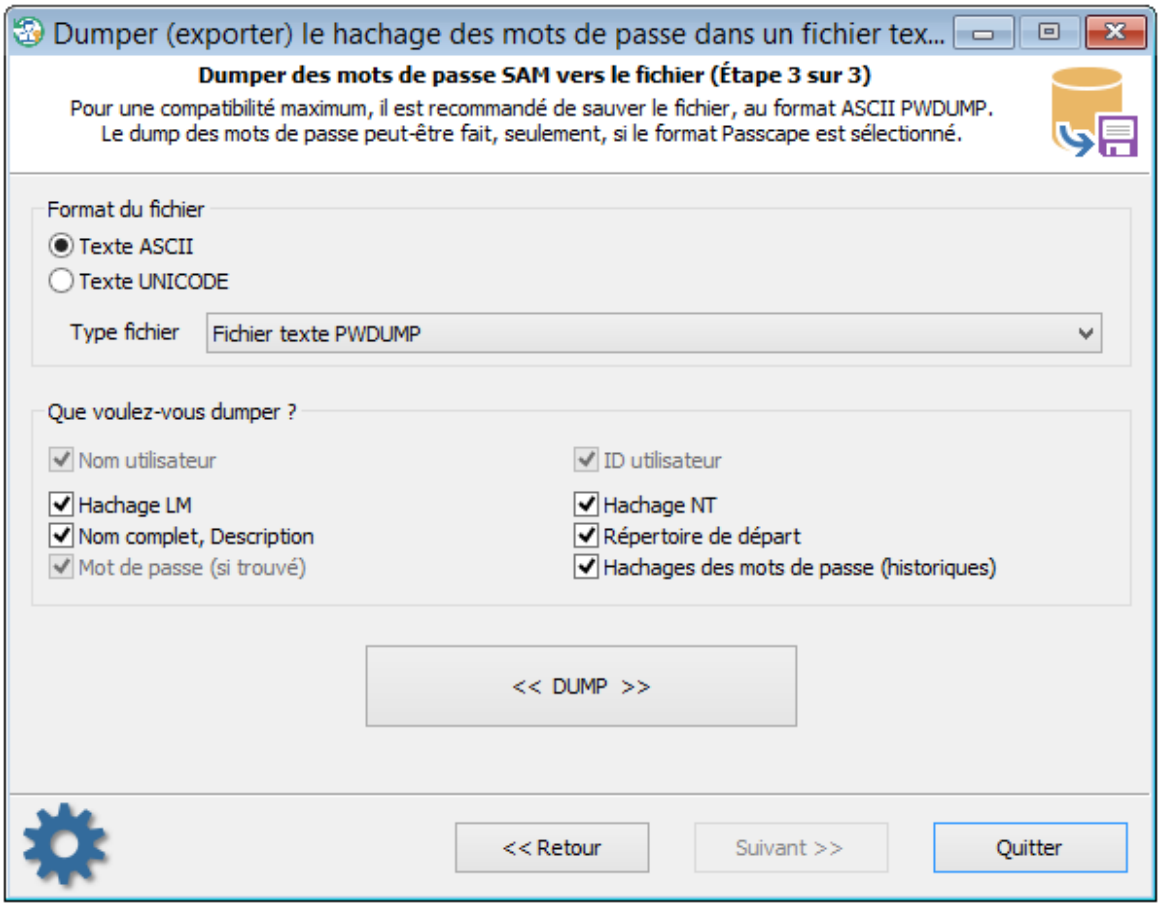
3.10 Dumper (exporter) le hachage des mots de passe

Sélection des données source



A cette étape, vous devez indiquer l'emplacement des fichiers SAM et SYSTEM. Ou dans le cas d'utilisateurs de Domaine, les fichiers ntds.dit et SYSTEM.

Exporter les hachages de mot de passe



Sélectionner le format et le type de fichier à "dumper". Pendant la génération du dump, vous pouvez aussi supprimer, ce qui ne vous est pas utile, comme les paramètres du compte inutile. Si le format Passcape est choisi, vous pouvez aussi dumper les mots de passe en clair (si ils ont été trouvé). Le logiciel scanne votre ordinateur pour en trouver, et si c'est le cas, il les relie aux comptes pendant qu'il sauvegarde le fichier dump.

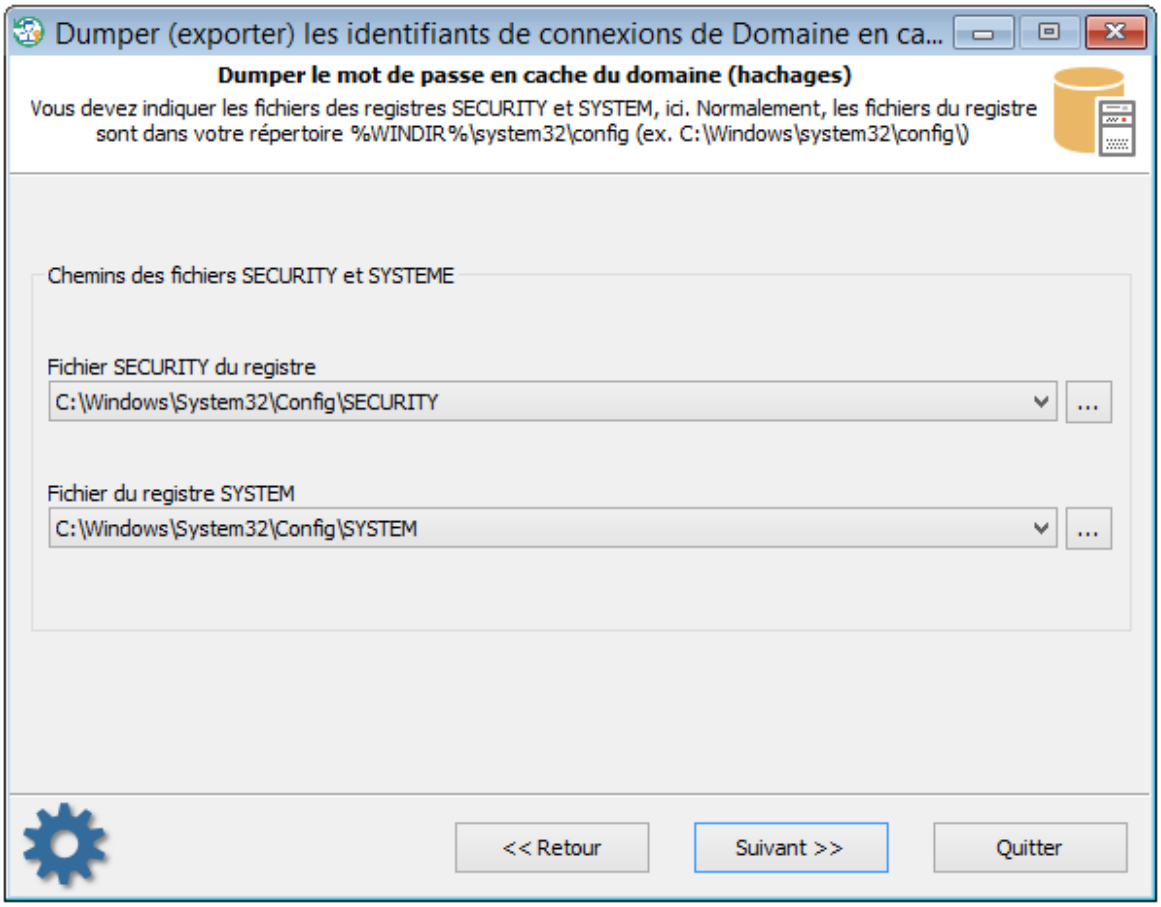
Les mots de passe en clair sont stockés dans le Domaine lorsque l'option "Stocker les mots de passe en utilisant un cryptage réversible pour tous les utilisateurs dans le Domaine" est activée; vous pouvez la trouver dans la console de gestion des stratégies de groupes.

En complément, vous pouvez utiliser le fichier dump avec différents logiciels d'audit et de récupérations de mots de passe.

Veuillez noter également, que Reset Windows Password, en remerciant Passcape Software qui a développé la technologie d'attaque par Intelligence Artificielle, peut décrypter les mots de passe de certains comptes pratiquement instantanément, sans recherche. Pour plus de détails, référez-vous à la section Lookup user passwords.

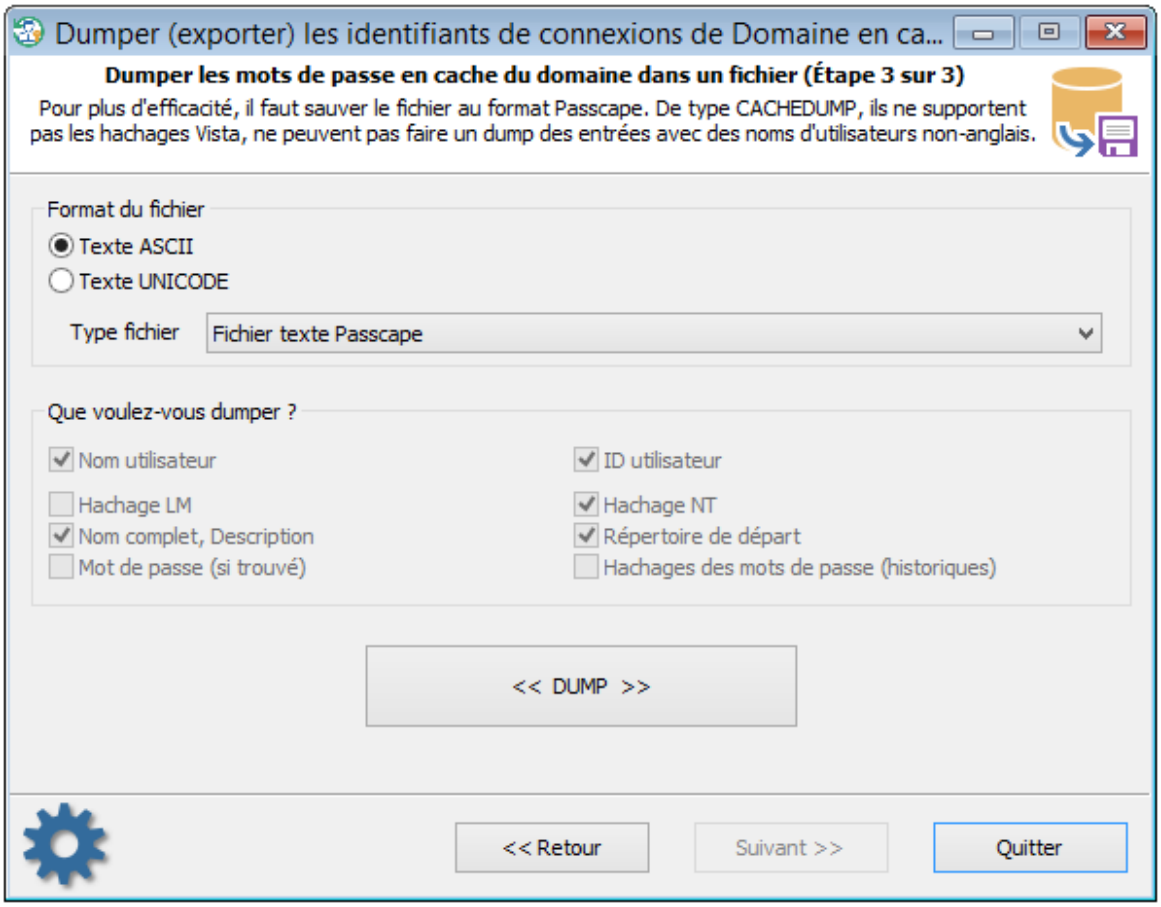
3.11 Dumper les identifiants de connexions de Domaine en cache

Sélection des données source



Pour décrypter les informations d'identifications de domaine en cache (domain cached credentials), le programme a "besoin" de savoir où se trouve les deux fichiers système de la base de registre: SECURITY et SYSTEM. Sélectionner les à partir de la liste ou, si l'application n'arrive pas à les localiser, indiquer manuellement le chemin de leur emplacement.

Dumper les informations d'identification de connexions de Domaine en cache

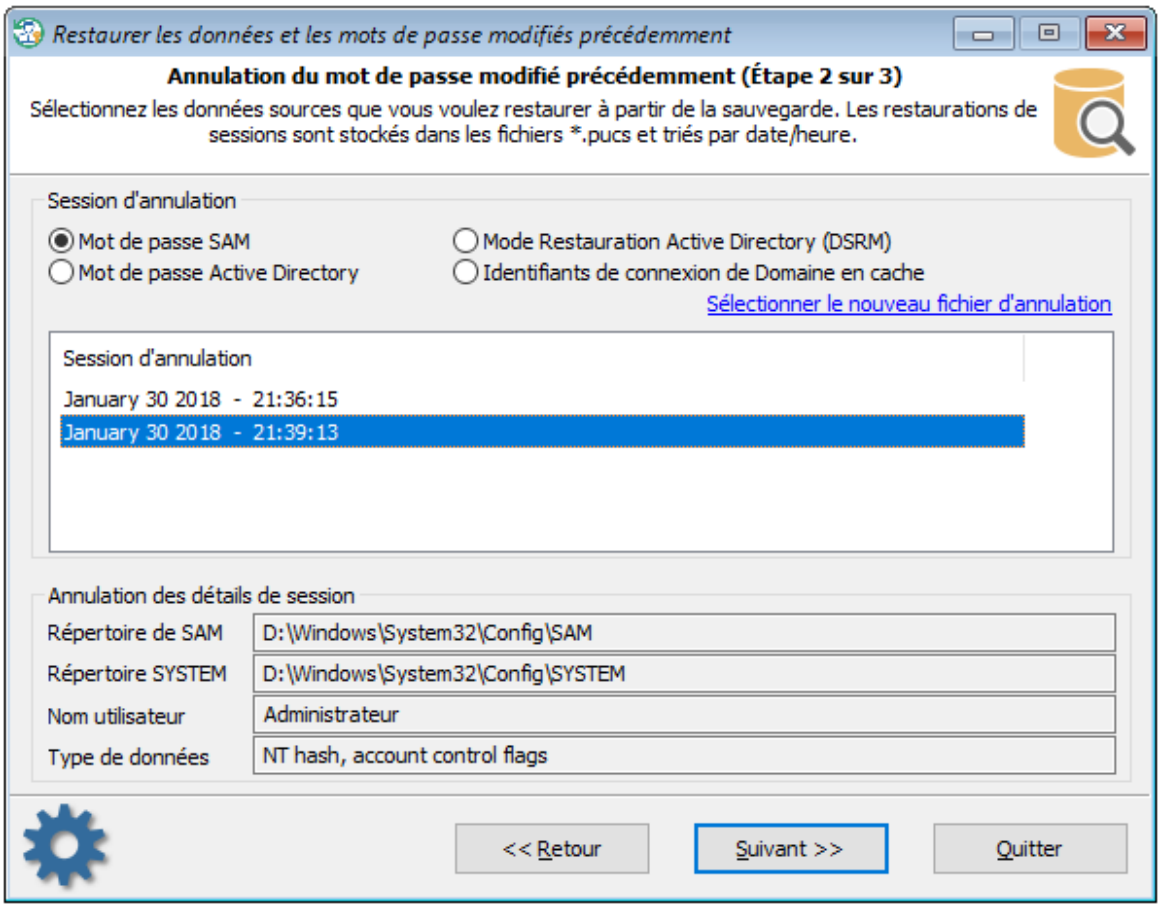


La dernière étape permets de définir deux options:
- Format de fichier de dump: ASCII est idéal pour tous les cas, mais des problèmes peuvent apparaître avec les noms d'utilisateurs non-Anglais et, de la même façon, avec les futures analyses et le décryptage de ces hachages. UNICODE supporte tous les langages, mais des problèmes de compatibilité peuvent apparaître lors de la lecture de ce format dans différents logiciels.

- Type de fichier de dump: Il peut être de type CACHEDUMP – un format simple mais répandu, sans aucun problème de compatibilité.
Cependant, ce format impose certaines restrictions:
- L'absence de support des noms d'utilisateurs non-Anglais. Du coup, vous n'aurez pas la possibilité de décrypter le mot de passe du compte, comme il est lié au nom.
- La version actuelle du format CACHEDUMP ne supporte pas les systèmes d'exploitation Windows Vista et les suivants.
Le format Passcape – n'a pas tous ces désavantages et peut être utilisé avec succès dans les audits de mots de passe et les logiciels de récupérations comme, par exemple, Network Password Recovery.

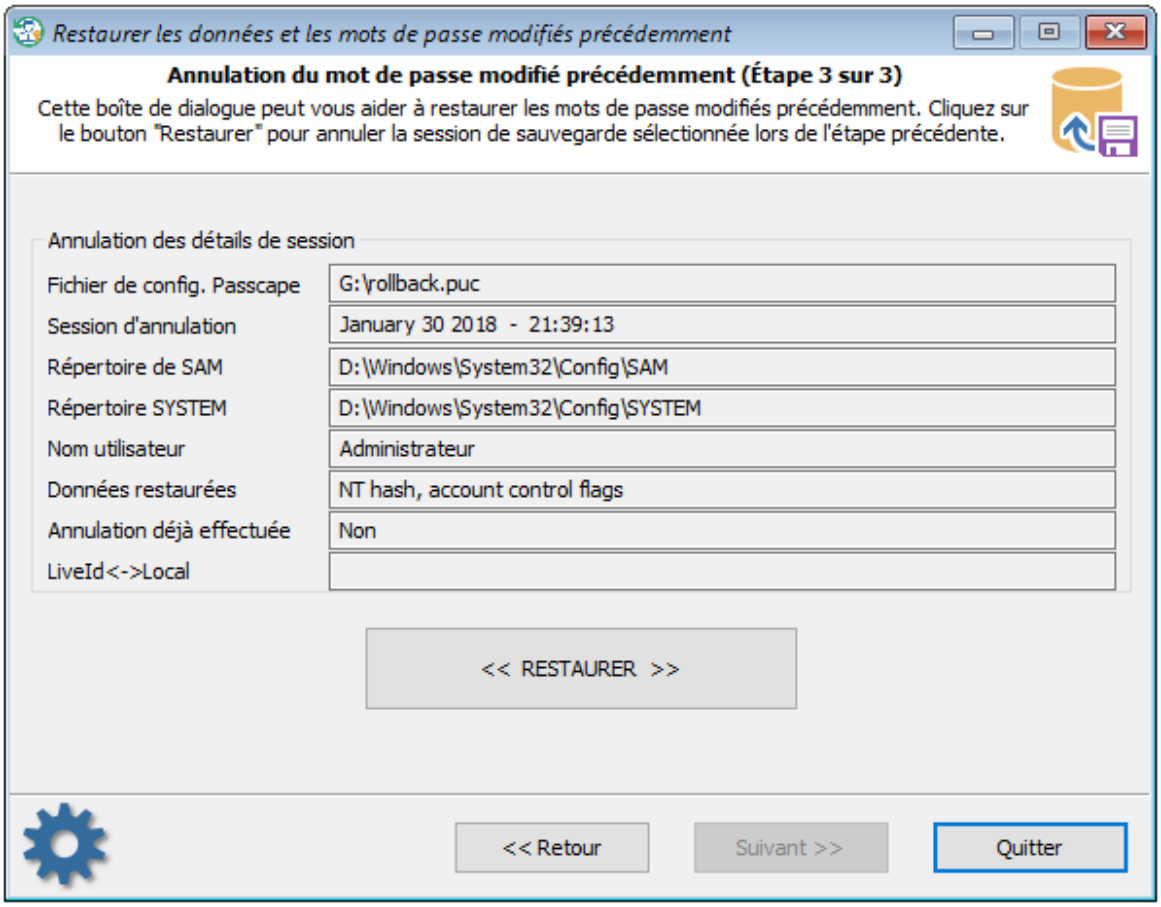
3.12 Restaurer les mots de passe modifiés précedemment

Choix d'un fichier d'annulation



Si quelque soit la raison, vous avez besoin d'annuler (par ex. pour une restauration) le mot de passe que vous avez réinitialisé ou modifié précédemment, à la seconde étape de l'assistant, il faut fournir le fichier "*.puc" contenant les informations d'annulations de sessions.
Ensuite, choisissez le type de mots de passe à restaurer: Mot de passe d'un compte SAM, de Domaine (Active Directory), DSRM, les paramètres d'identifications de Domaine, les paramètres de stratégies de sécurité de mots de passe.
Après cela, sélectionner la date où les modifications ont été faites.

Restaurer un mot de passe modifié



A la dernière étape, l'application vous proposera de voir les détails de la session dont le contenu va être restauré; soyez tout particulièrement attentif au trois derniers éléments:

- Le compte qui va être modifié.
- Les données qui seront restaurées. Ce sont les données qui ont été modifiées à partir de ce point.
- Si ce fichier d'annulation a déjà été utilisé.

Regardons ensemble une exemple de situation:
Un expert en sécurité informatique a besoin de se connecter à Windows à partir d'une certaine session. Le mot de passe pour cette session est inconnu. Sachant que le mot de passe du compte doit rester inchangé.

Voici la séquence d'opération à suivre:

- Lancer "Reset Windows Password", choisissez le compte et réinitialiser le mot de passe. En même temps, sauvegarder les modifications de la session dans un fichier d'annulation "*.puc" (l'application vous le demandera lors de la modification du mot de passe).
- Fermer "Reset Windows Password", relancer l'ordinateur pour démarrer Windows. Connectez-vous sous la session du compte modifié avec le mot de passe vide. Exécuter les opérations que vous souhaiter faire comme opérations dans cette session.
- Maintenant vous devez restaurer l'ancien mot de passe du compte, en effectuant les étapes suivantes:

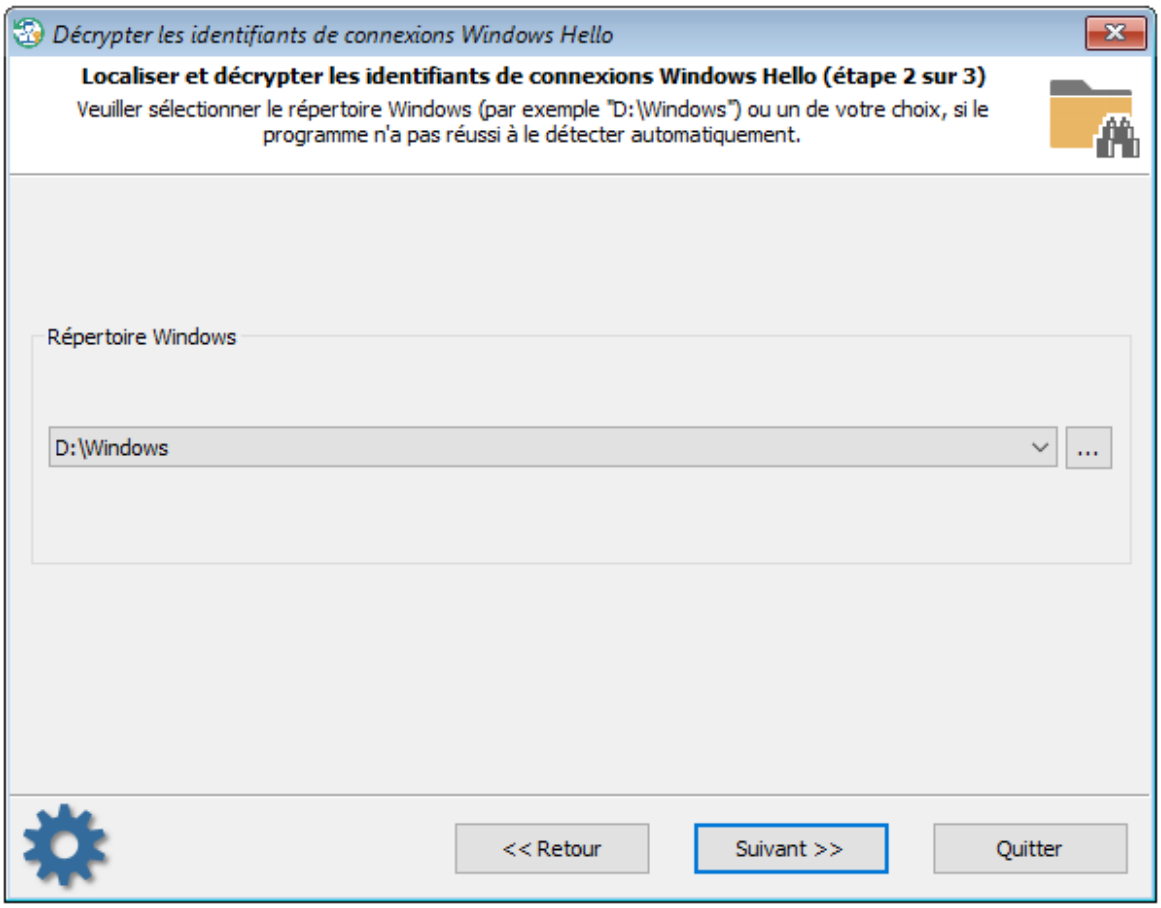
    - Redémarrer une nouvelle fois l'ordinateur en exécutant "Reset Windows Password".
    - Dans le menu principal de "RWP", choisissez "Restaurer le mot de passe et les données modifiées",
    - Saisissez le chemin du fichier d'annulation où vous avez sauvegardé les modifications faites.
    - Poursuivez jusqu'à la troisième étape et vérifier que le compte choisi est correct.
    - Cliquer sur le bouton <<Restaurer>>, et l'ancien mot de passe sera restauré.

3.13 OUTILS - Récupération de mots de passe et divers utilitaires

3.13.1 Décrypter les identifiants de connexions Windows Hello

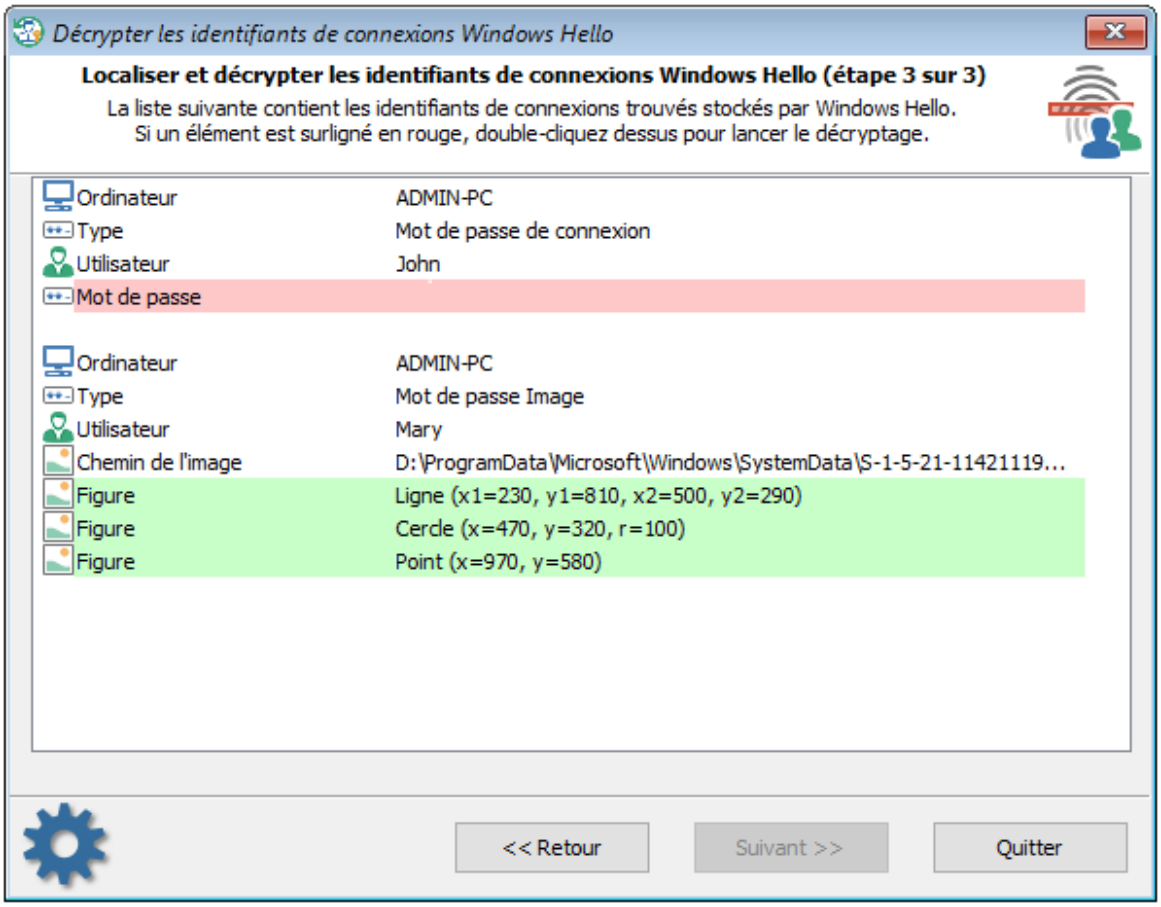
Windows Hello est un système de sécurité qui permets aux utilisateurs de s'identifier dans un OS, des applications ou leurs périphériques sans mots de passe, en utilisant une empreinte digitale, un scan de l'iris de l'œil, un visage ou par reconnaissance vocale.
Windows Hello stocke différents types d'informations personnelles des utilisateurs: les identités digitales, les codes PIN, les mots de passe d'identifications de connexions en clair (non cryptés), etc.

Sélection du répertoire Windows



Reset Windows Password récupère tous les types de données personnelles sauvegardées dans Windows Hello.
Tout d'abord, vous devez indiquer le répertoire Windows du système cible.

Décrypter les mots de passe



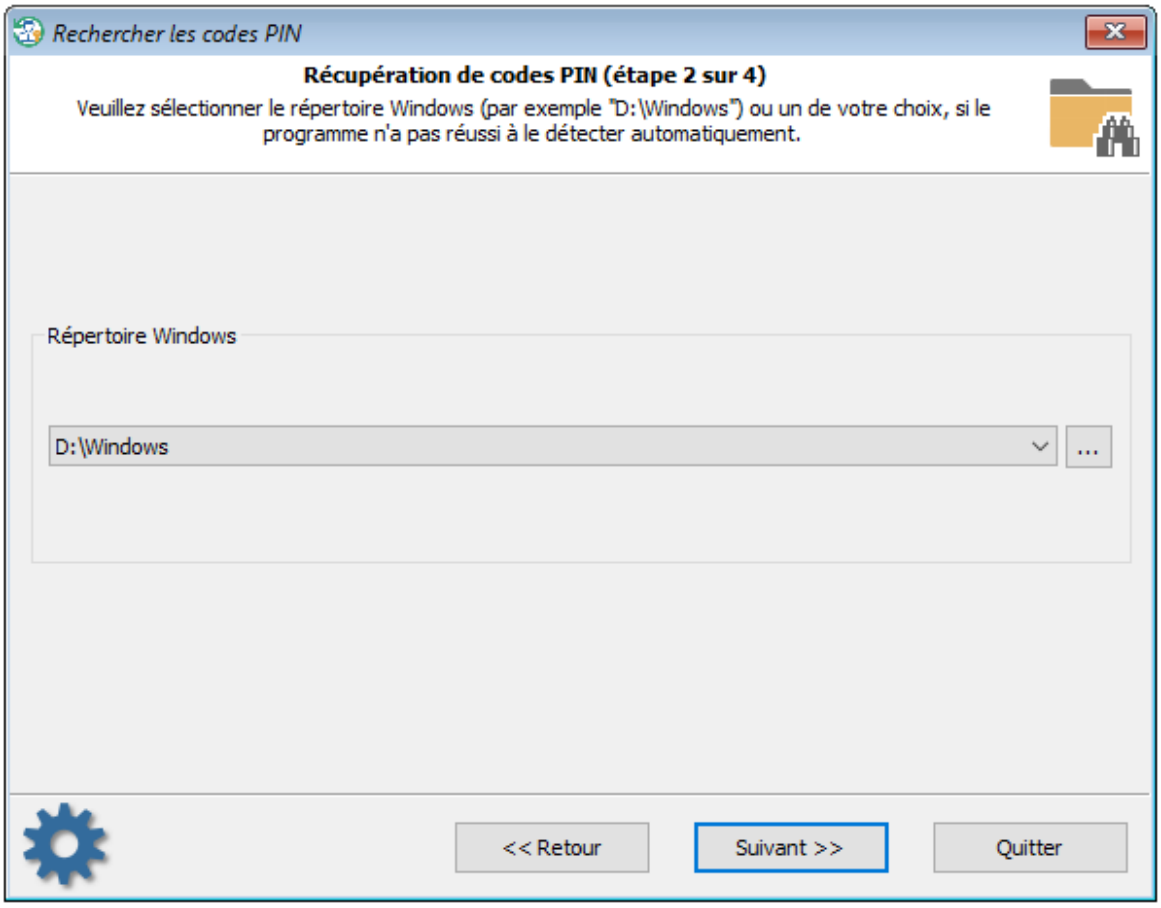
Le programme scanne ensuite le répertoire Windows cible, à la recherche de toutes les données personnelles et les affichent ensuite à l'écran.
Reset Windows Password décrypte automatiquement les mots de passe d'identifications de connexions (logon) si les comptes des utilisateurs ont été configurés pour utiliser une authentification biométrique, par exemple, avec une empreinte digitale ou une reconnaissance faciale.

Certains éléments peuvent être surlignés en rouge. Cela signifie que pour finaliser le décryptage, le programme a besoin du code PIN du compte de l'utilisateur. Double-cliquez sur l'élément et entrez le code PIN qui corresponds au compte de l'utilisateur.
A noter, que les éléments surlignés en vert signifie qu'ils ont été décryptés.

3.13.2 Rechercher les codes PIN

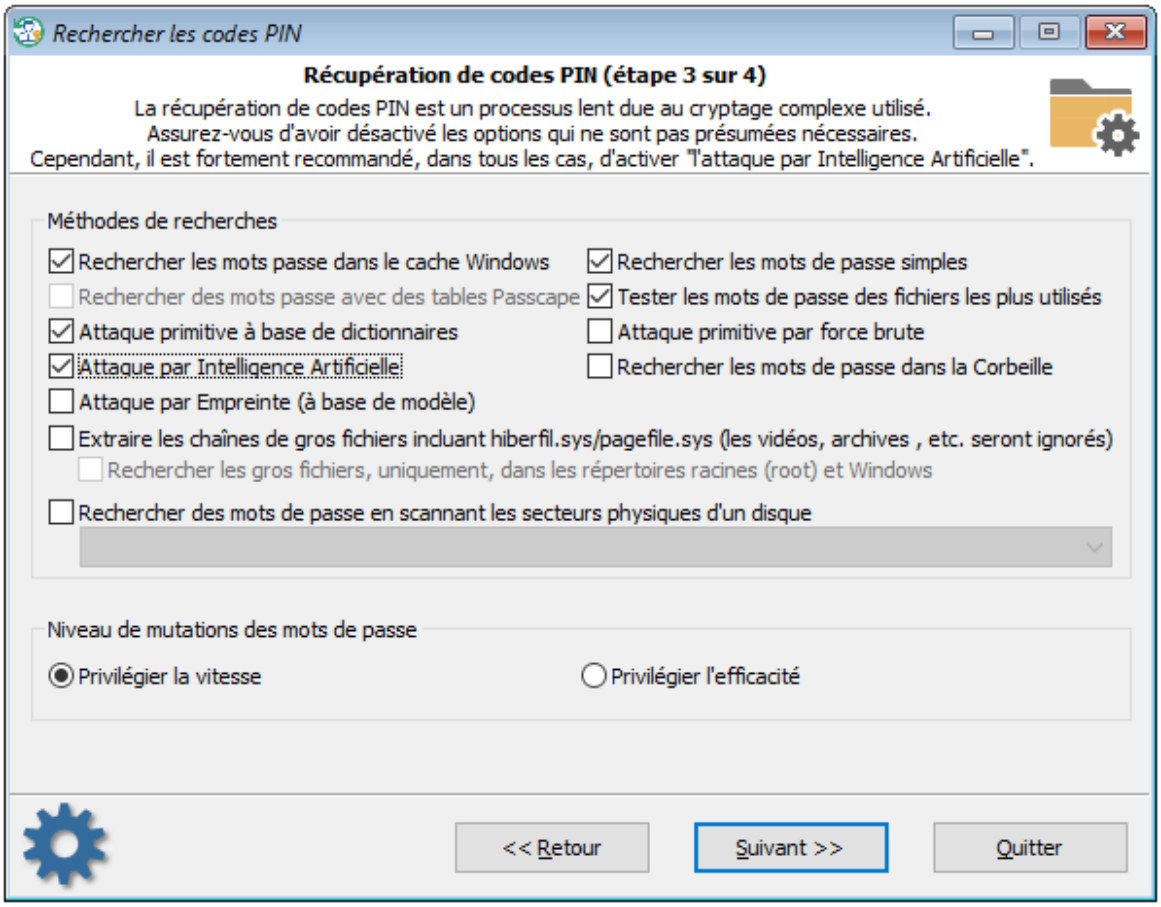
Lorsque vous configurez Windows Hello pour la première fois, il vous est demandé de créer un code PIN.
Le code PIN est utilisé comme alternative à l'authentification biométrique lorsqu'un capteur biométrique n'est pas disponible ou qu'il ne fonctionne pas correctement. A la différence de Windows 8, Windows 10 protège avec un cryptage très complexe les codes PIN (utilisant souvent des fonctionnalités et APIs non documentées). C'est pour cette raison que le problème de la récupération de codes PIN oubliés est extrêmement vital et concerne tous les utilisateurs.

Sélection du répertoire Windows



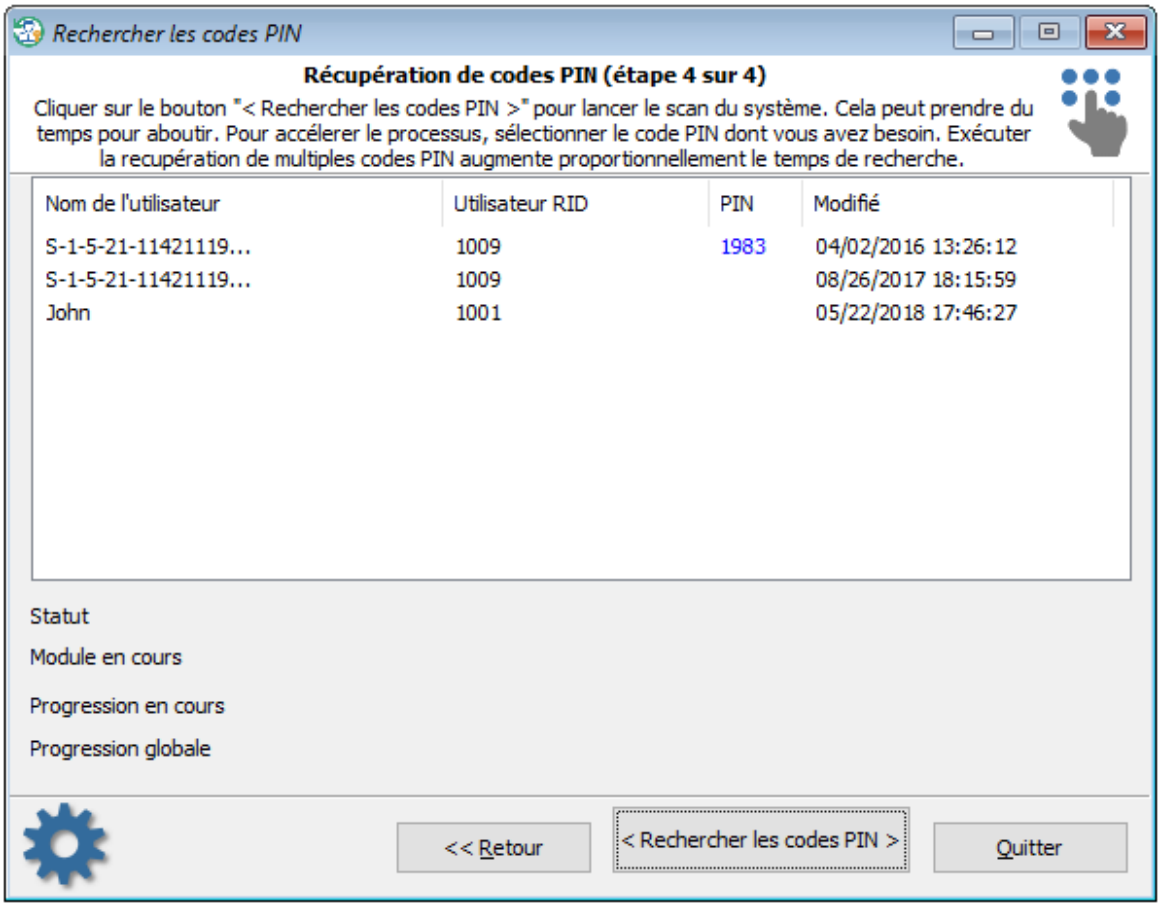
En tout premier, vous devez sélectionner ou rechercher manuellement le répertoire Windows.

Choix des options de recherches et de récupérations



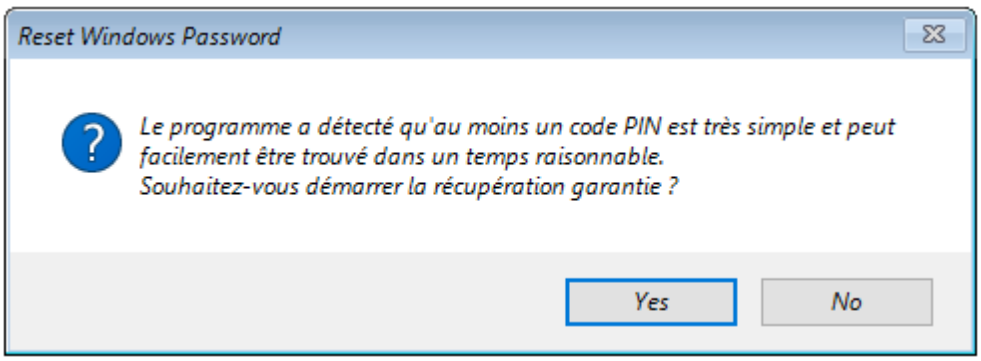
A l'étape suivante, le programme propose les méthodes de récupérations possibles pour rechercher les codes PIN.
Le code du programme est très optimisé pour la vitesse. Malgré cela, le processus de recherche pour un code PIN est extrêment lent. C'est pour cette raison qu'il est fortement recommandé de désactiver les attaques qui prennent le plus de temps, par exemple, comme dans la capture d'écran ci-dessus.

Rechercher les codes PIN



La vitesse de recherche est inversement proportionnelle au nombre de codes PIN recherchés. Plus il y aura de codes PIN recherchés simultanément, plus la vitesse de recherche sera lente. Il est donc recommandé d'exclure de la recherche, les codes PIN inutiles, afin d'optimiser le temps de la récupération et de ne rechercher que ceux dont vous avez besoin. Vous pouvez simplement, avec un clic-droit sur le code PIN que vous souhaitez récupérer, sélectionner "*Exclure tout hormis ceux sélectionnés*".
Pour lancer le processus de recherche, cliquez sur le bouton << Rechercher les codes PIN>>.

Il faut savoir que pour certains codes PIN, le décryptage est garanti, dans un temps raisonnable. Si le programme peut détecter une vulnérabilité du code PIN, il vous offrira de lancer une récupération garantie, comme dans l'exemple de la capture d'écran suivante:

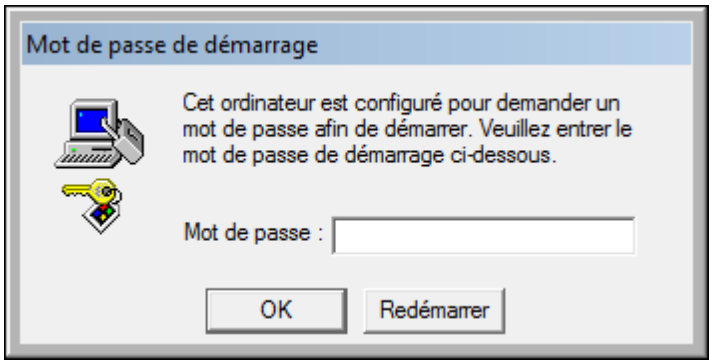


3.13.3 Rechercher le mot de passe de démarrage SYSKEY

Syskey est une couche de sécurité supplémentaire, qui a été introduit la première fois dans Windows 2000. Qui est utilisé par défaut et offre 3 types de protections:

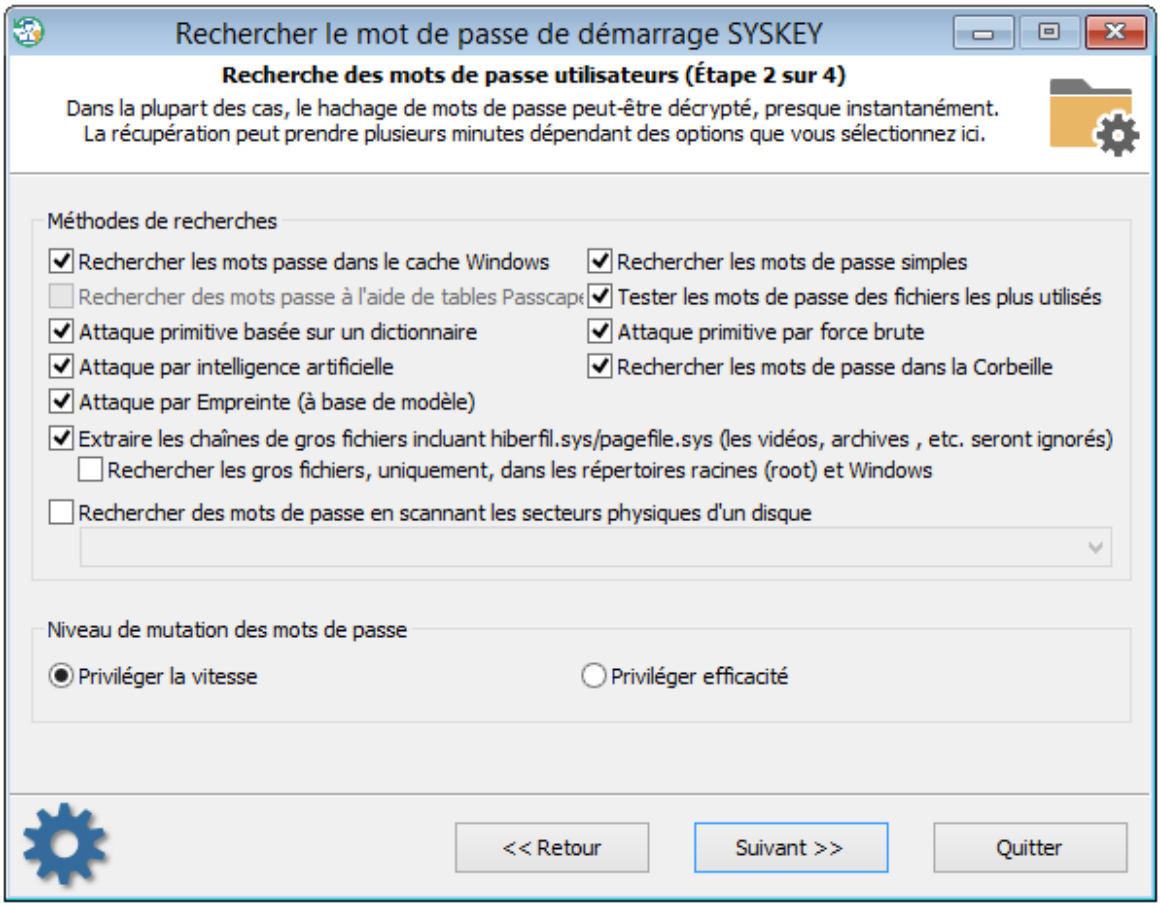
1. **Par défaut** - la clé de cryptage syskey est stockée dans la base de registre de Windows.
2. **Disque de démarrage** - la clé de cryptage syskey est stockée sur une disquette ou une clé USB (vous devez assigner la lettre A à votre clé USB) .
3. **Mot de passe de démarrage** - la clé de cryptage syskey est générée à partir d'un mot de passe saisi par l'utilisateur.

Les personnes malhonnêtes (arnaqueurs) utilise la puissance du SYSKEY souvent pour configurer un mot de passe de démarrage sur le PC de la victime. Habituellement, ils vous contactent avec un petit accent Indien s'identifiant comme des membres du support Microsoft et vous annoncent que votre PC doit être réparé immédiatement parce qu'il a un problème critique. Ils essayent de vous convaincre qu'ils peuvent se connecter à distance pour réparer les problèmes. Si vous faites cette erreur, ils configureront un mot de passe de démarrage SYSKEY. Vu que vous ne connaissez pas le mot de passe, après le redémarrage du système vous verrez cette fenêtre s'ouvrir à l'écran (voir ci-dessous) et vous ne pourrez plus ouvrir votre PC votre session tant que vous n'aurez pas payé pour réparer/supprimer ce message.



Heureusement, dans la plupart des cas les mots de passe sont très simples et peuvent être décryptés en utilisant notre fonction de recherche du mot de passe SYSKEY. Vous devez suivre les trois étapes simples pour lancer la recherche du mot de passe.

Définir les méthodes de récupération du SYSKEY

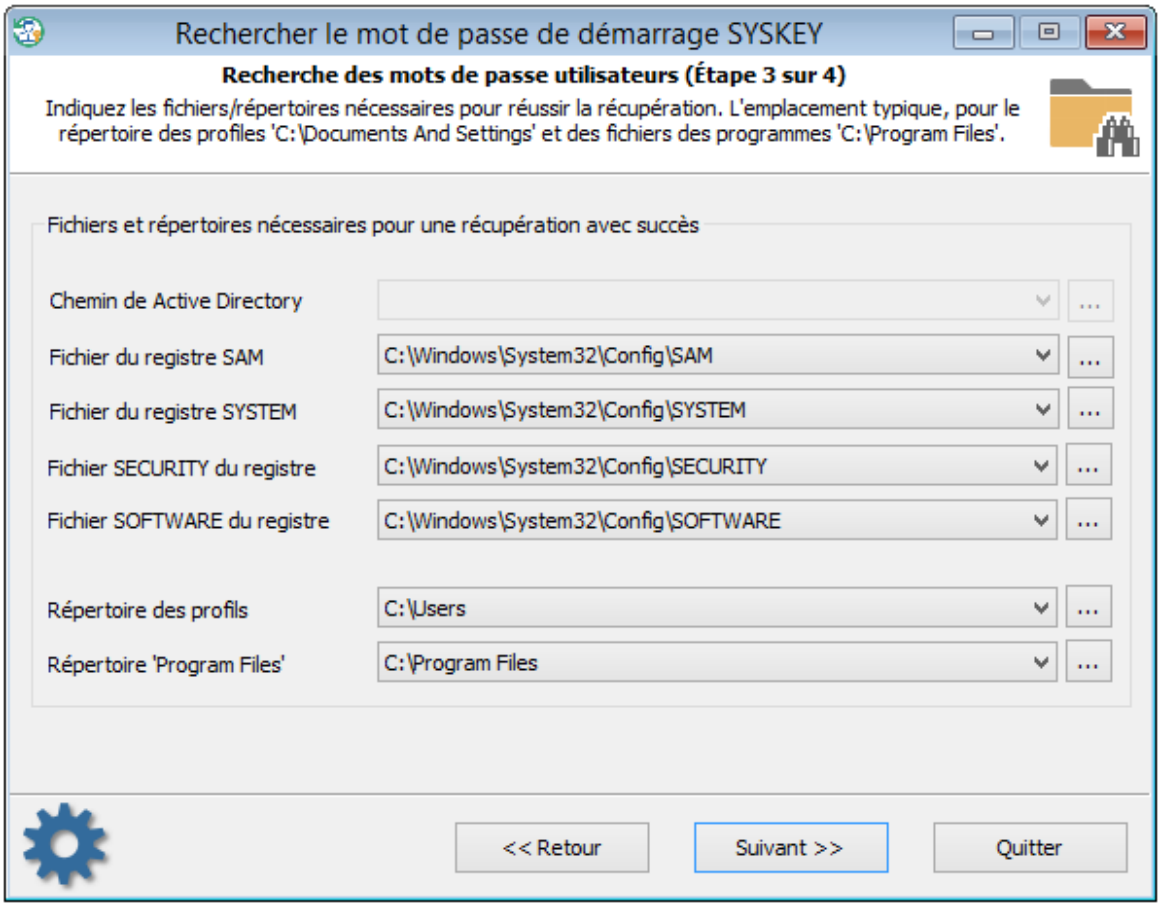


La recherche d'un mot de passe SYSKEY peut prendre du beaucoup de temps et se déroule selon les étapes suivantes:

1. La recherche d'information dans le cache Système de Windows. Cette méthode est constituée de plus d'une douzaine de mini sous-attaques, durant lesquelles le programme analyse tous les types de mots de passe de l'utilisateur: les secrets LSA, DSL, VPN, WiFI, FTP, IM, les mots de passe des navigateurs, etc.
2. Une analyse simple, des mots de passe courts, des combinaisons de clavier, etc.
3. Un scan et une analyse des fichiers les plus récemment utilisés sur le système cible.
4. Une attaque primitive par Dictionnaire. L'application teste tous les mots de passe à partir de dictionnaires inclus dans les versions light et standard ou de plusieurs dictionnaires (Arabe, Chinois, Anglais, Français, Allemand, Portugais, Russe, Espagnol) pour l'édition Avancée. Si l'option de recherche approfondie est activée, de simples mutations de mots sont également prises en compte pendant la recherche.
5. Une récupération Primitive par Force-brute essayera de trouver les mots de passe courts. Les options de la Force-brute sont aussi dépendantes du niveau de mutation.
6. Une attaque par Intelligence artificielle qui analyse l'activité réseau d'un utilisateur sur un ordinateur. A l'aide des résultats de l'analyse, l'application génère les préférences de l'utilisateur et un dictionnaire sémantique pour l'attaque, qui seront utilisés plus tard pour trouver deviner le mot de passe.
7. Une recherche de mots de passe dans les fichiers supprimés.
8. Une recherche de mots de passe Anglais complexes (Attaque par Empreinte).
9. Une extraction de chaînes et de mots à partir de fichiers de tailles importantes: Images RAM, hiberfil.sys, pagefile.sys et ainsi de suite. Quand cette option est activée, le programme ignorera les fichiers inutiles comme les vidéos, les archives, les fichiers audio, etc.
10. Une recherche de mots de passe en lisant et analysant les données brutes des secteurs (raw data) du disque sélectionné. Si le "*Niveau de mutation des mots de passe*" est configuré sur "*Privilégier l'efficacité*", le programme essayera, en plus, de générer différentes combinaisons et

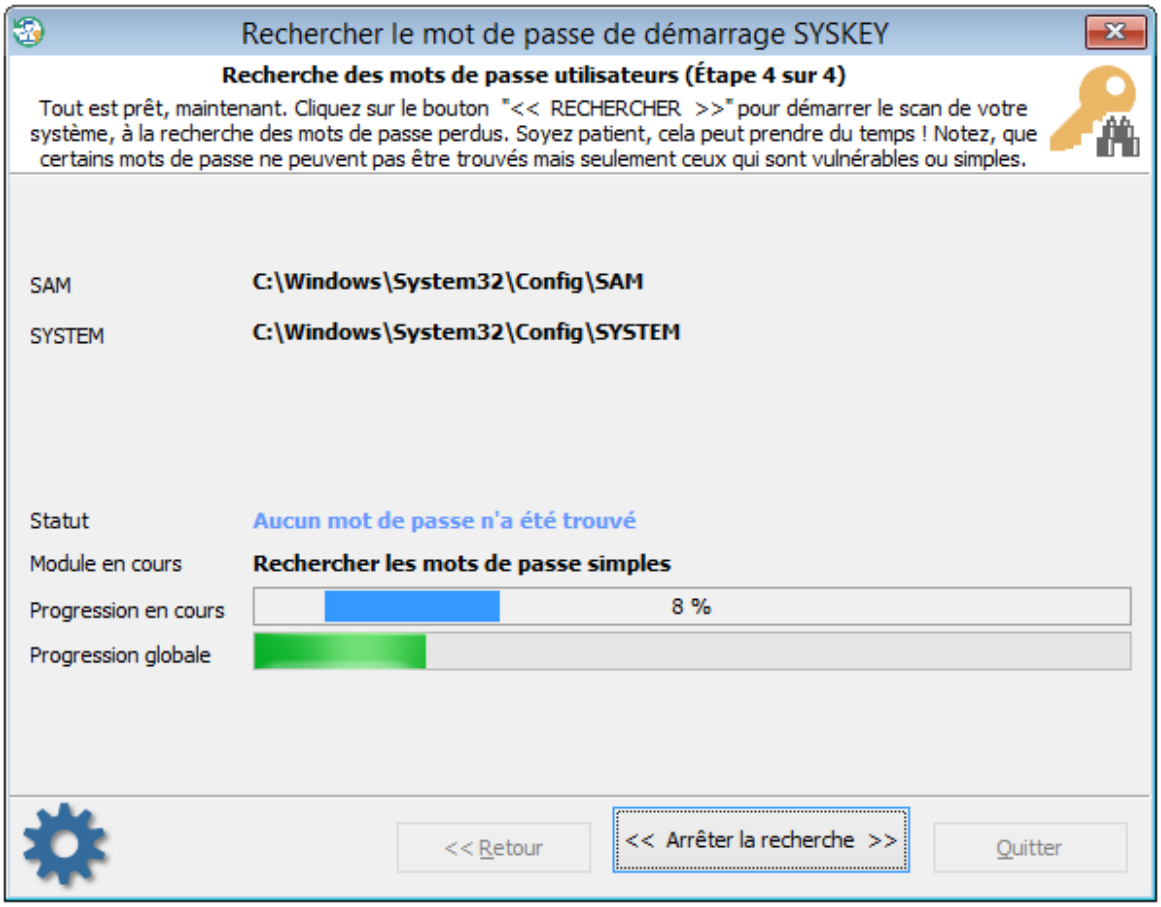
de "*muter*" les mots de passe trouvés, sachant que le parcours de tous les secteurs du lecteur cible peut prendre beaucoup de temps. Notez l'algorithme qui scanne les secteurs n'est pas utilisable avec les lecteurs dont le cryptage natif du disque est actif, comme Bitlocker ou Truecrypt.

Sélectionner les données source



Lors de la recherche d'un mot de passe de démarrage SYSKEY, apportez une attention toute particulière aux fichiers et répertoires nécessaires pour le processus d'analyse. Sinon, la recherche du mot de passe ne sera pas efficace, voire impossible. Le logiciel essayera de localiser les fichiers automatiquement, mais parfois, quand l'ordinateur possède plusieurs systèmes d'exploitation, vous devrez utiliser le "mode manuel". Gardez également à l'esprit que si le PC cible possède 2 disques logiques ou plus, la séquence des lettres de lecteurs pour ces disques peut être totalement différentes que celle du système d'origine.

Recherche du mot de passe SYSKEY

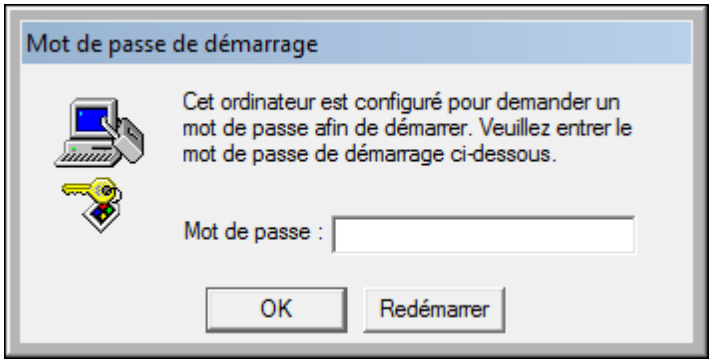


Rechercher/deviner le mot de passe peut prendre du temps, en fonction des paramètres de l'attaque et des particularités de votre système. Veuillez noter que seulement les mots de passe simples et vulnérables peuvent être récupérés !

Une fois que vous avez trouvé le mot de passe SYSKEY, tout ce que vous avez à faire, c'est de désactiver le mode de protection de démarrage SYSKEY, vous demandant un mot de passe et de restaurer votre système dans son mode de démarrage original.

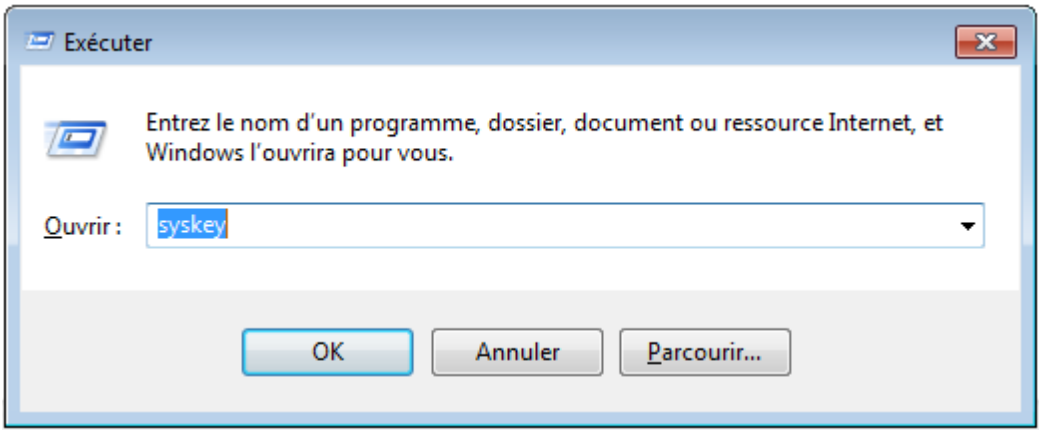
Désactiver le mot de passe de démarrage SYSKEY

Pour désactiver le mot de passe de démarrage SYSKEY, il vous suffit de suivre ces simples étapes

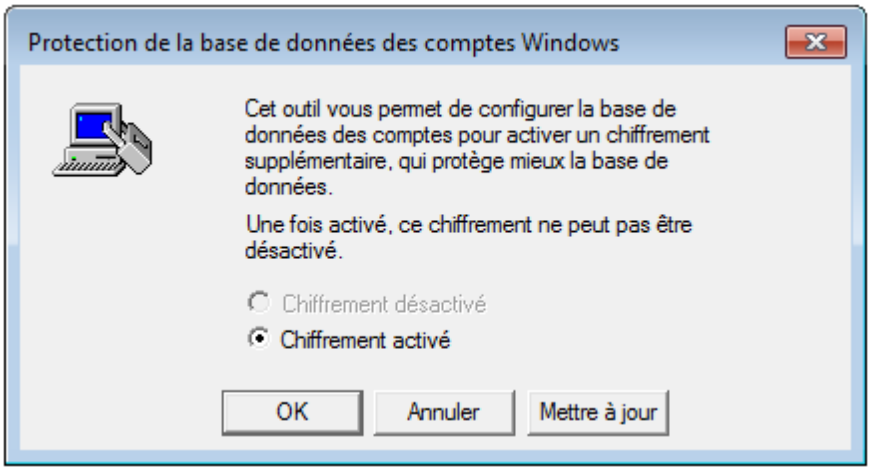


Entrer le mot de passe découvert par RWP. Puis cliquez sur OK.

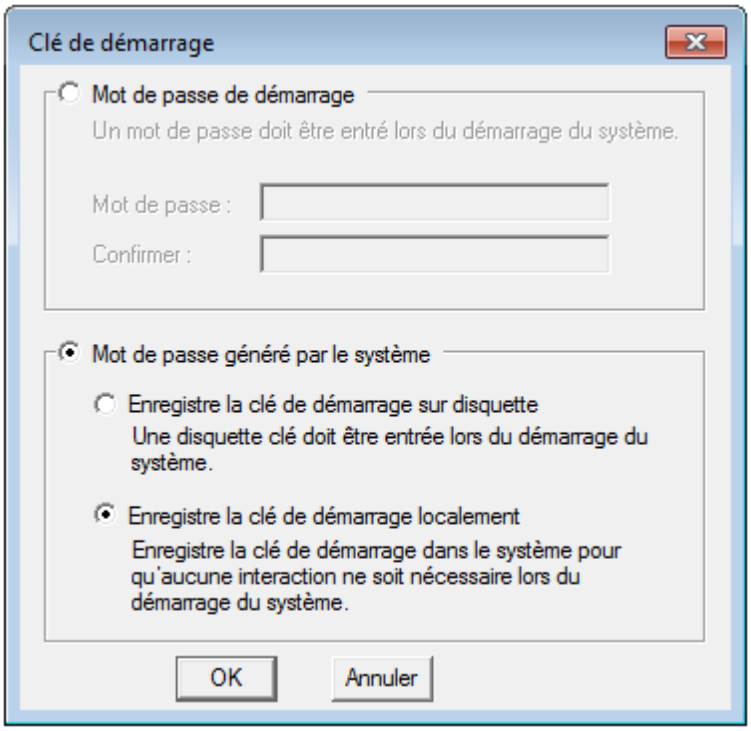
Ouvrer la session de votre compte sur l'ordinateur, avec le mot de passe de votre compte Windows.
Qui peut être différent de celui pour le SYSKEY.
Appuyer sur les touches "**Win+R**", entrer le mot "**SYSKEY**" puis cliquer sur le bouton "**OK**".



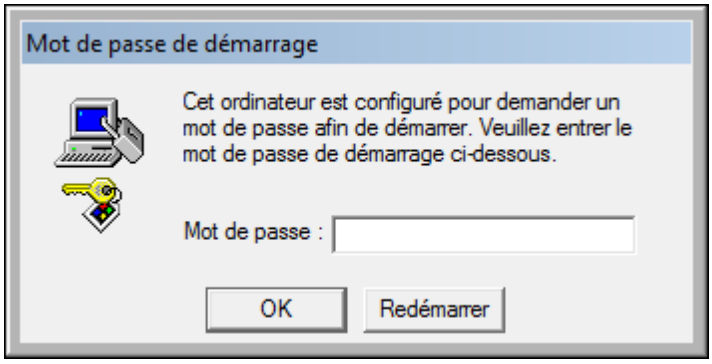
La boite de dialogue d'options de SYSKEY comme ci-dessous va s'ouvrir:



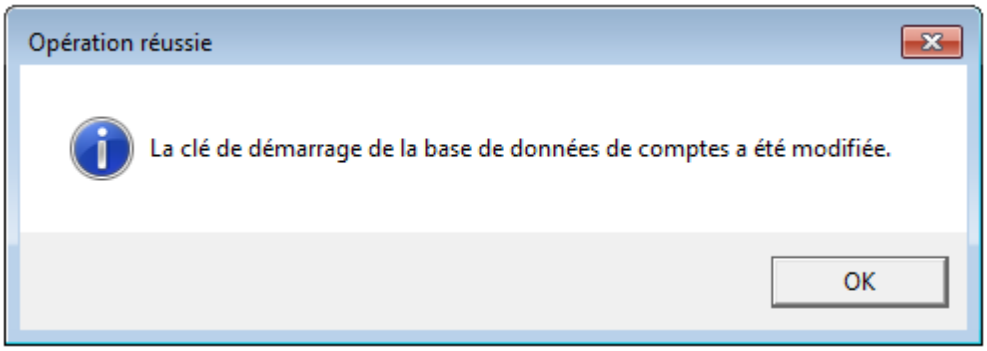
Cliquer sur le bouton "**Mettre à jour**".



Sélectionner maintenant l'option "**Mot de passe généré par le système**" et "**Enregistre la clé de démarrage localement**" pour désactiver la demande d'un mot de passe SYSKEY au démarrage.
Cliquer sur le bouton "**OK**"



Entrer le mot de passe découvert par RWP, puis cliquer sur le bouton "**OK**".



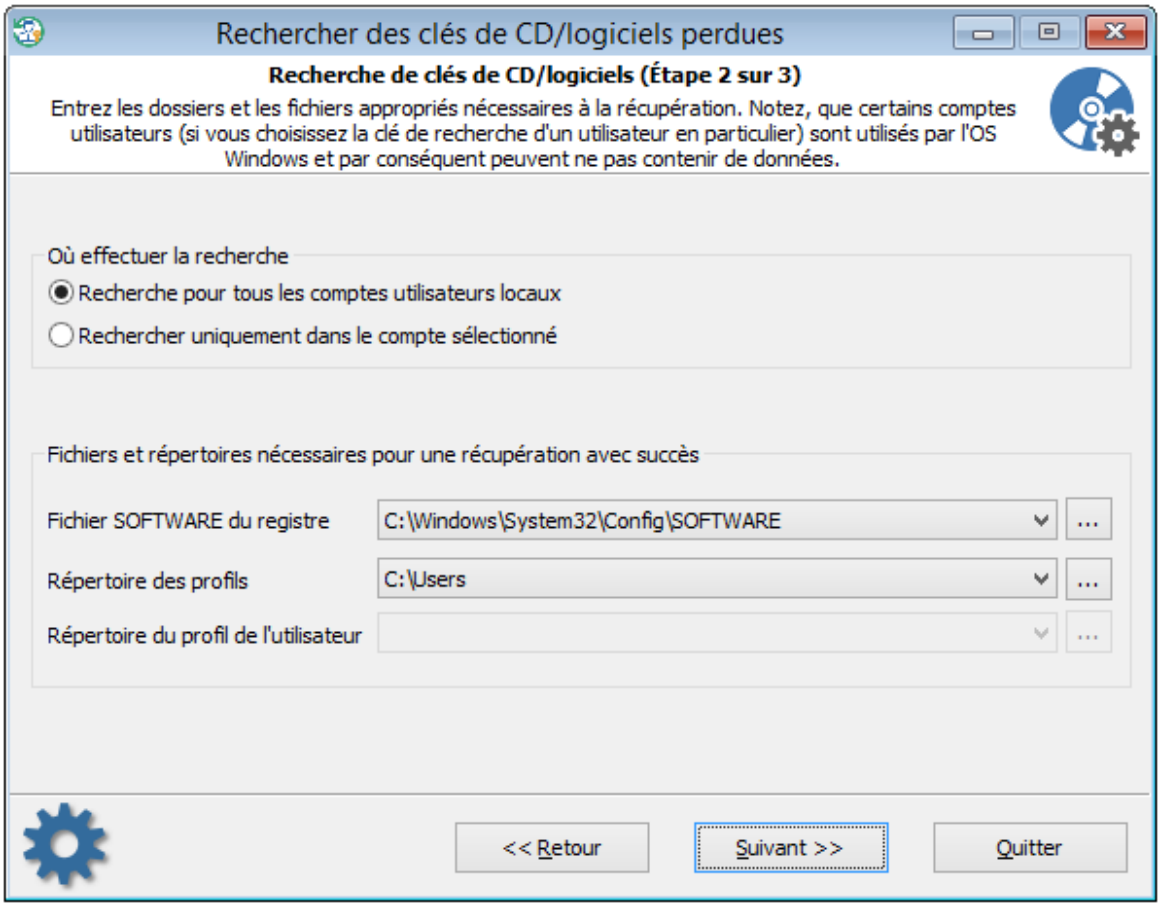
Un message vous confirme que la modification a bien été réalisée.
Il vous suffit, maintenant, de redémarrer votre système pour tester que la demande de mot de passe SYSKEY, au démarrage a bien été supprimée.

3.13.4 Rechercher des clés de CD/Logiciels perdues

En utilisant cette fonctionnalité, vous pouvez facilement récupérer les clés de logiciels perdues et leurs numéros de série, même si le système cible n'est plus amorçable.

La plupart des logiciels du commerce pour Windows sont fournis avec une clé de licence qui lie le logiciel à votre PC et permets de l'utiliser légalement avec toutes ses fonctionnalités. En perdant cette clé, vous ne pourrez plus utiliser le logiciel tant que vous n'aurez pas retrouvé cette clé.
Imaginez juste un instant le jour où vous devez réinstaller votre système d'exploitation. Il y a de nombreuses raisons pour lesquelles vous devriez le faire, de la mise à jour pour éliminer des virus, réparer un problème, etc. Et après la réinstallation, vous devez réinstaller vos logiciels et entrer les clés de licences dont vous n'avez plus l'accès. Sans ces clés, vous ne pouvez pas réinstaller vos logiciels.

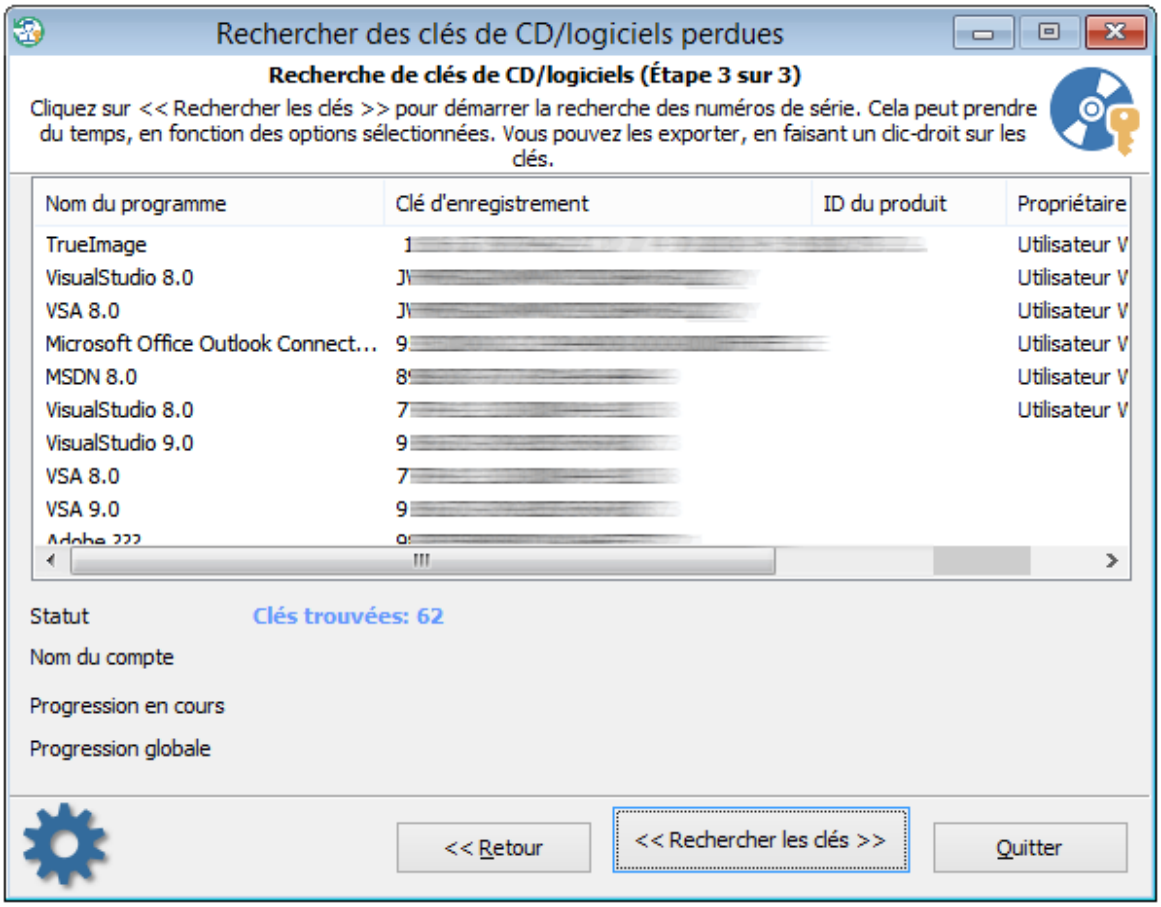
Par chance, un grand nombre de logiciels stockent leurs clés dans la base de registre de Windows et du coup ils sont facile à extraire. A laide de cette fonctionnalité, RWP vous permets cette récupération.
En utilisant le langage script, "Reset Windows Password" peut retrouver les clés pour plus de 1,000 logiciels. Et il est très facile à utiliser.



En premier, vous devez indiquer au programme si vous récupérez les clés de logiciels pour tous les utilisateurs ou pour un compte en particulier.

La récupération de clés pour tous les comptes nécessite au moins deux paramètres pour être configurée correctement:
1. Le fichier de la base de registre " SOFTWARE " qui se trouve dans le répertoire suivant: *'C:\Windows\System32\Config'*.
Notez, que la lettre de lecteur ou le répertoire Windows peut être différent. Par exemple, *'D:\Windows'*, *'E:\Win'*, etc.
2. Le répertoire des profils. C'est le répertoire où sont stockés tous les comptes des utilisateurs locaux qui sont physiquement stockés. Pour Windows Vista et les OS (Windows 7 et Windows 10), le répertoire est généralement "*C:\Users"* alors que Windows XP utilise le répertoire "*C:\Documents and Settings"*. Habituellement, le répertoire des profils est dans le même lecteur que celui où ce trouve Windows, mais ce n'est pas toujours le cas.
Le programme essayera de détecter automatiquement ces répertoires. Tout ce que vous avez besoin de faire, c'est d'en sélectionner un à partir de la liste déroulante ou de regarder les répertoires alternatifs.

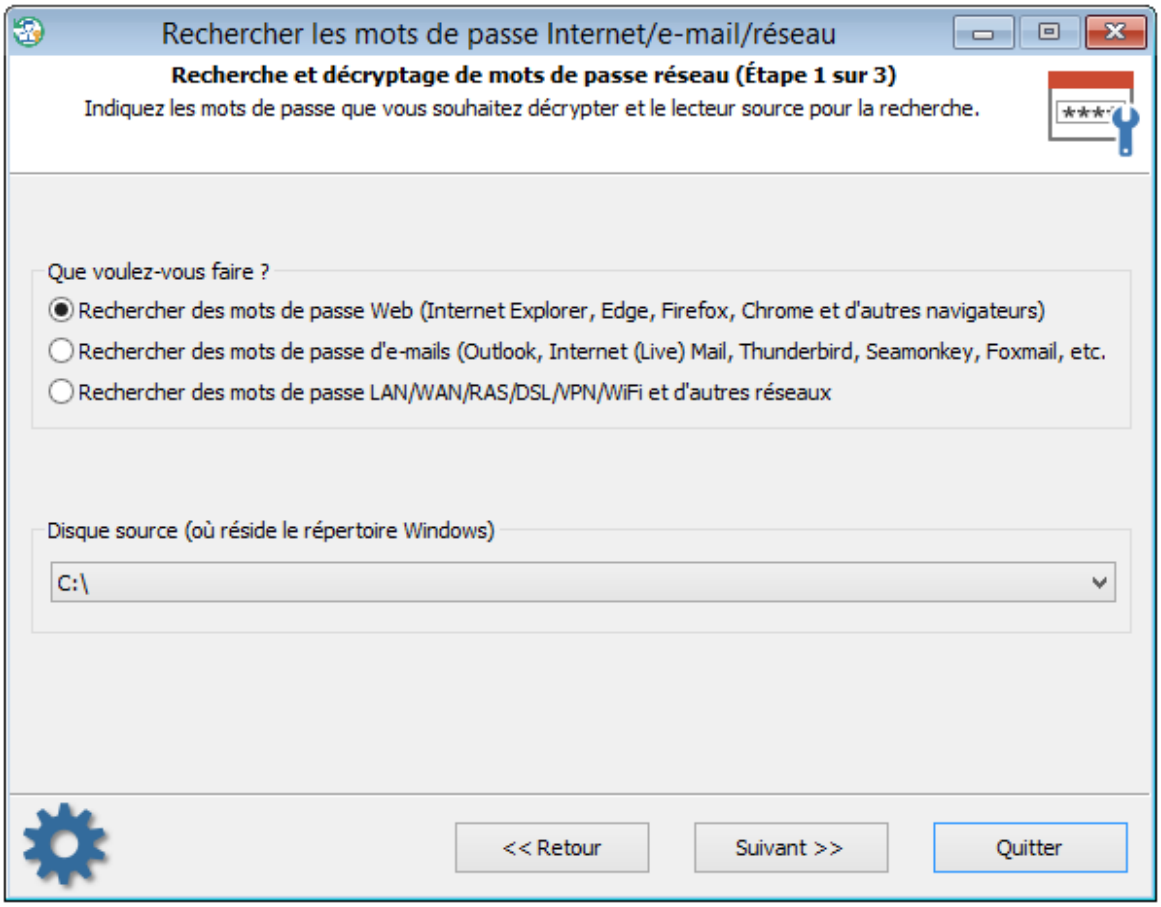
Si vous avez besoin de récupérer des numéros de séries pour un seul utilisateur, sélectionner la première option et choisissez l'utilisateur à partir de la liste dans " Répertoire du profil de l'utilisateur ".



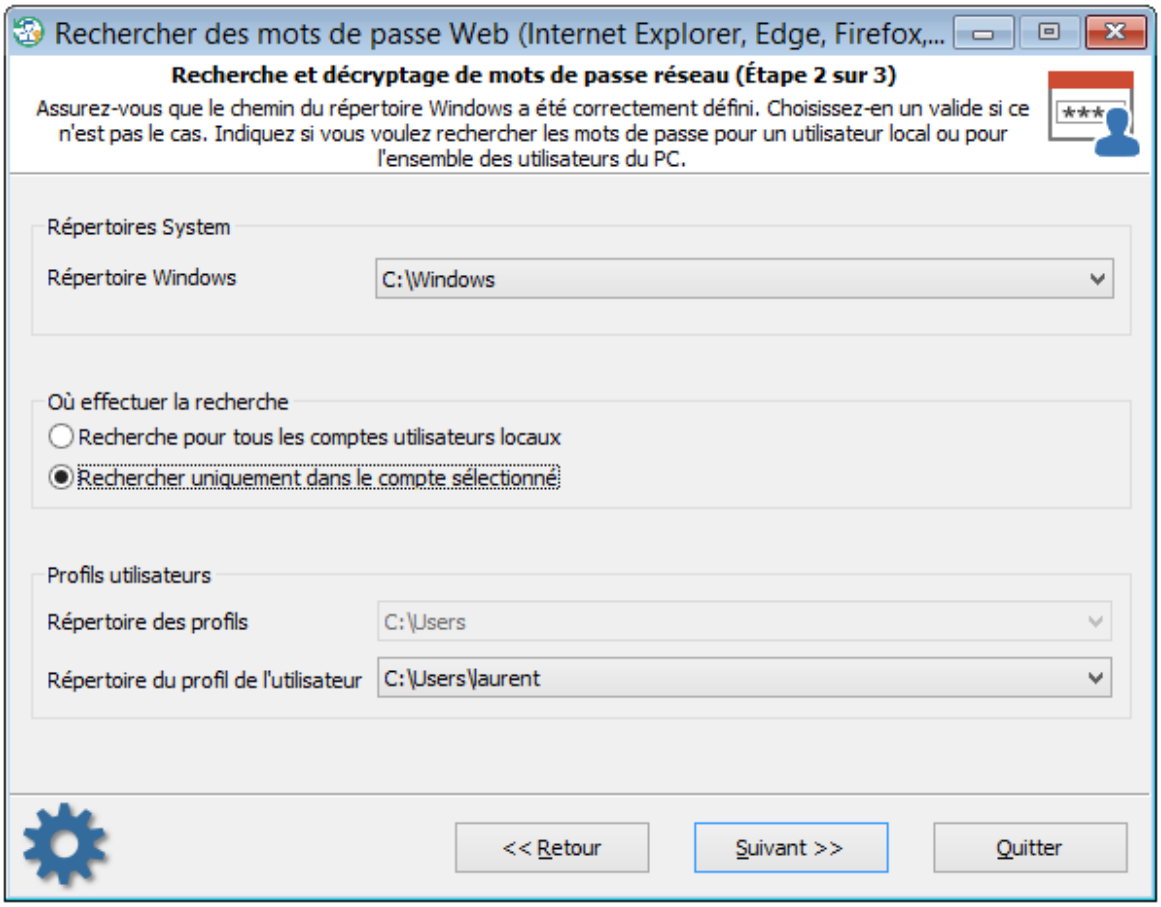
Après avoir configuré les options nécessaires, lancer la dernière étape en cliquant sur le bouton << Rechercher les clés >> pour démarrer la recherche des numéros de série perdus.

3.13.5 Rechercher les mots de passe Internet/e-mail/réseau

Une des fonctionnalité, la plus remarquable, est la recherche et le décryptage des mots de passe réseau des utilisateurs. Reset Windows Password supporte tous les navigateurs les plus populaires et les logiciels de courriels (e-mails). L'interface est divisée en trois étapes pour rendre le processus le plus simple possible, les détails spécifiques étant laissés au programme.



A la première étape de l'assistant, le programme vous demande quels types de mots de passe vous souhaitez rechercher et le lecteur source contenant le répertoire Windows.
Par défaut, le programme sélectionne le premier disque dur, où le système d'exploitation est installé.

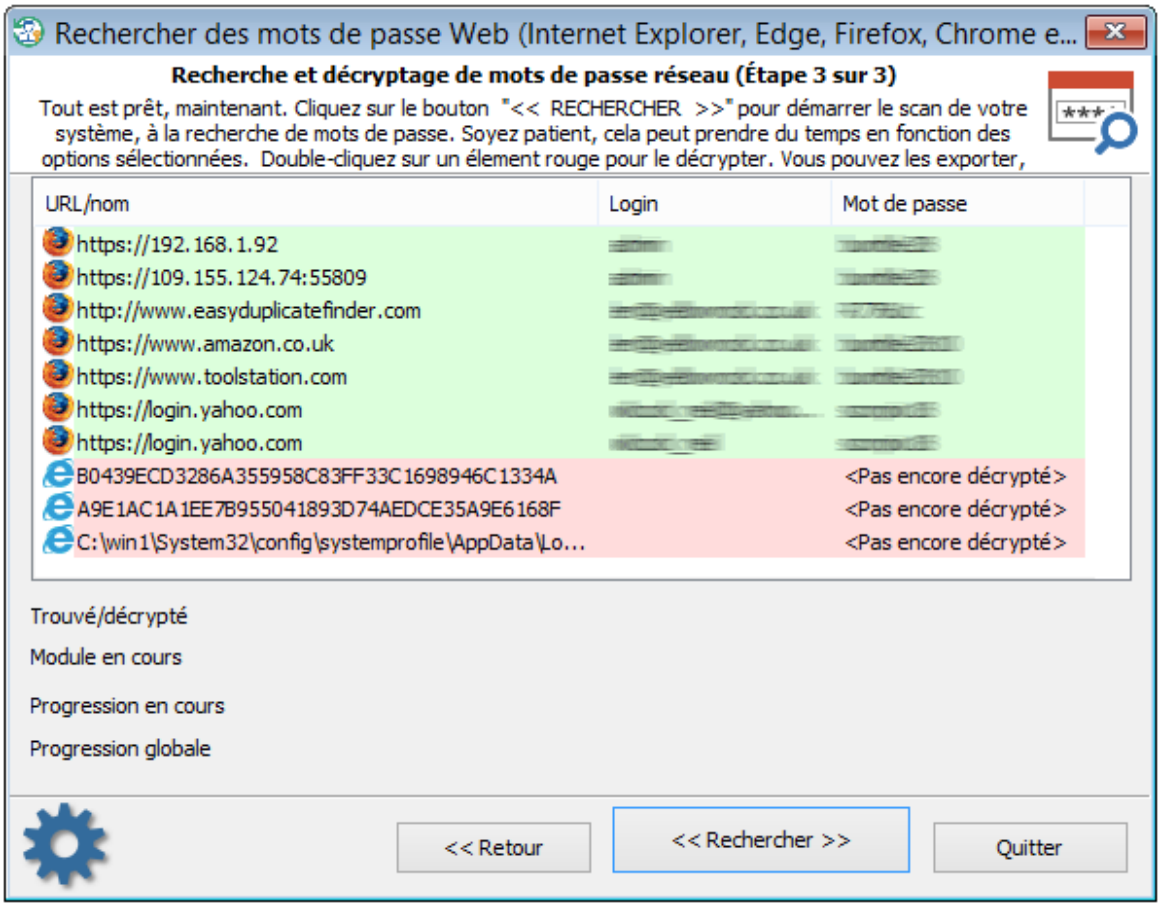


A la deuxième étape, indiquer l'emplacement du répertoire Windows. Ainsi que les répertoires où le programme effectuera la recherche pour trouver les mots de passe: pour tous les utilisateurs ou uniquement un seul. Dans la dernière case, sélectionner le répertoire correspondant.

A la dernière étape, cliquer sur le bouton **<< Rechercher >>** pour lancer le processus de recherche, d'analyse, et de décryptage des données. Soyez patient, en fonction des options choisies et le nombre d'utilisateurs dans le système, le processus peut prendre du temps.

3.13.5.1 Rechercher les mots de passe Web stockés par les navigateurs Internets

En sélectionnant la recherche de mots de passe Internet, la boite de dialogue suivante s'affiche:



Le logiciel décrypte les mots de passe de la plupart des navigateurs Web:

- Internet Explorer
- Edge
- Firefox
- Opera
- Chrome
- Safari
- La majorité des navigateurs basés sur Mozilla: Flock, Seamonkey, Pale Moon, Waterfox, etc.
- La majorité des navigateurs basés sur les sources de Chromium: Comodo Dragon, CoolNovo, Google Chrome, Yandex browser, etc.

Les navigateurs Web utilisent différents algorithmes pour protéger les données personnelles des utilisateurs. Les mots de passe à partir des navigateurs suivants, peuvent être décryptés pratiquement instantanément:

- Internet Explorer 4-6
- Firefox et les autres navigateurs basés sur Mozilla (sans le mot de passe principal activé)
- Les anciennes versions de Opera (sans le mot de passe principal activé)

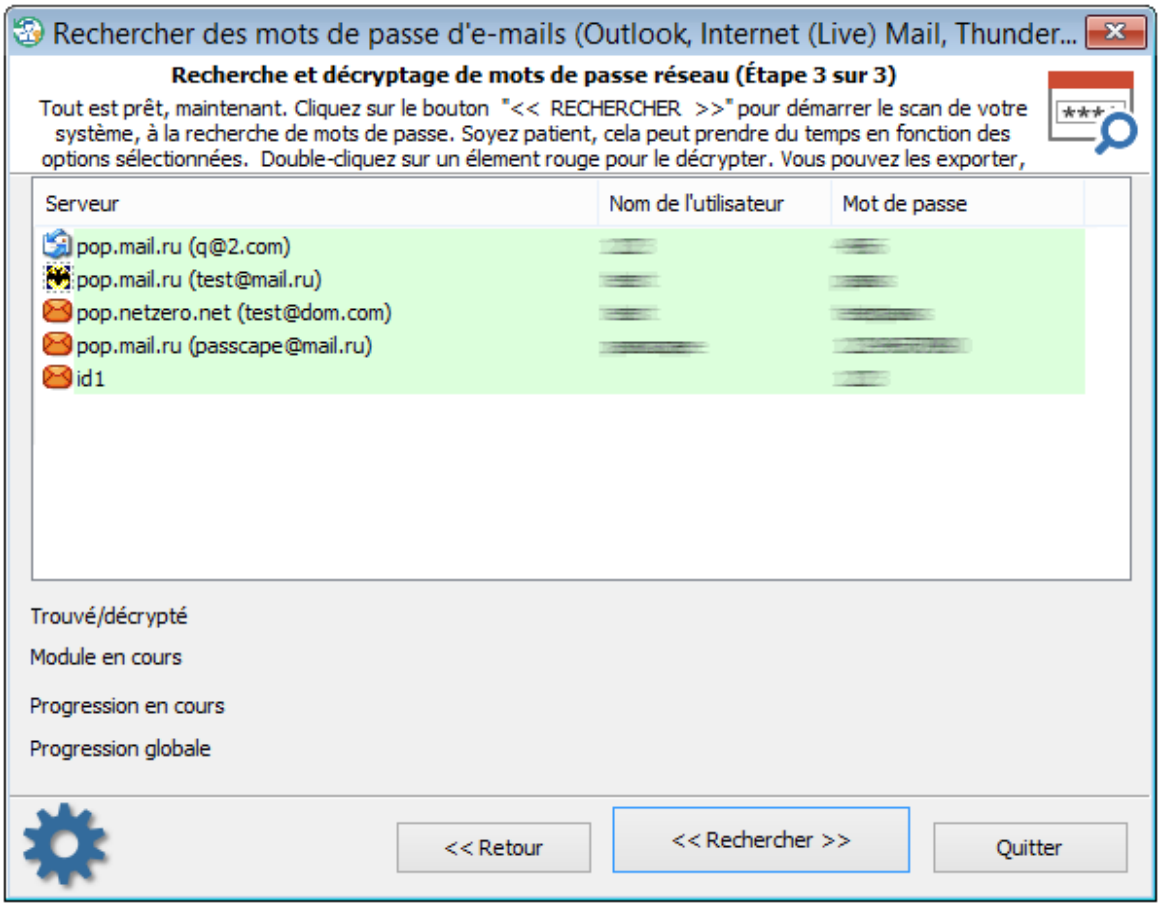
Le décryptage d'autres données nécessite des informations supplémentaires. Comme le mot de passe principal ou le mot de passe de connexion (session Windows) de l'utilisateur:

- Internet Explorer 10
- Edge
- Firefox (si le mot de passe principal est activé)
- Opera (si le mot de passe principal est activé)
- Chrome
- Safari

Pour décrypter les mots de passe, double-cliquer simplement sur la ligne surlignée en rouge.

Internet Explorer 7-9 nécessite trois étapes de décryptage:
En premier, vous devez entrer l'URL où ont été sauvegardé les mots de passe, puis entrer le mot de passe du compte Windows.
Pour plus d'informations, sur cette protection un peu particulière, utilisée dans Internet Explorer 7-9, vous pouvez consulter notre article.

3.13.5.2 Rechercher les mots de passe d'e-mails stockés par les clients d'e-mails

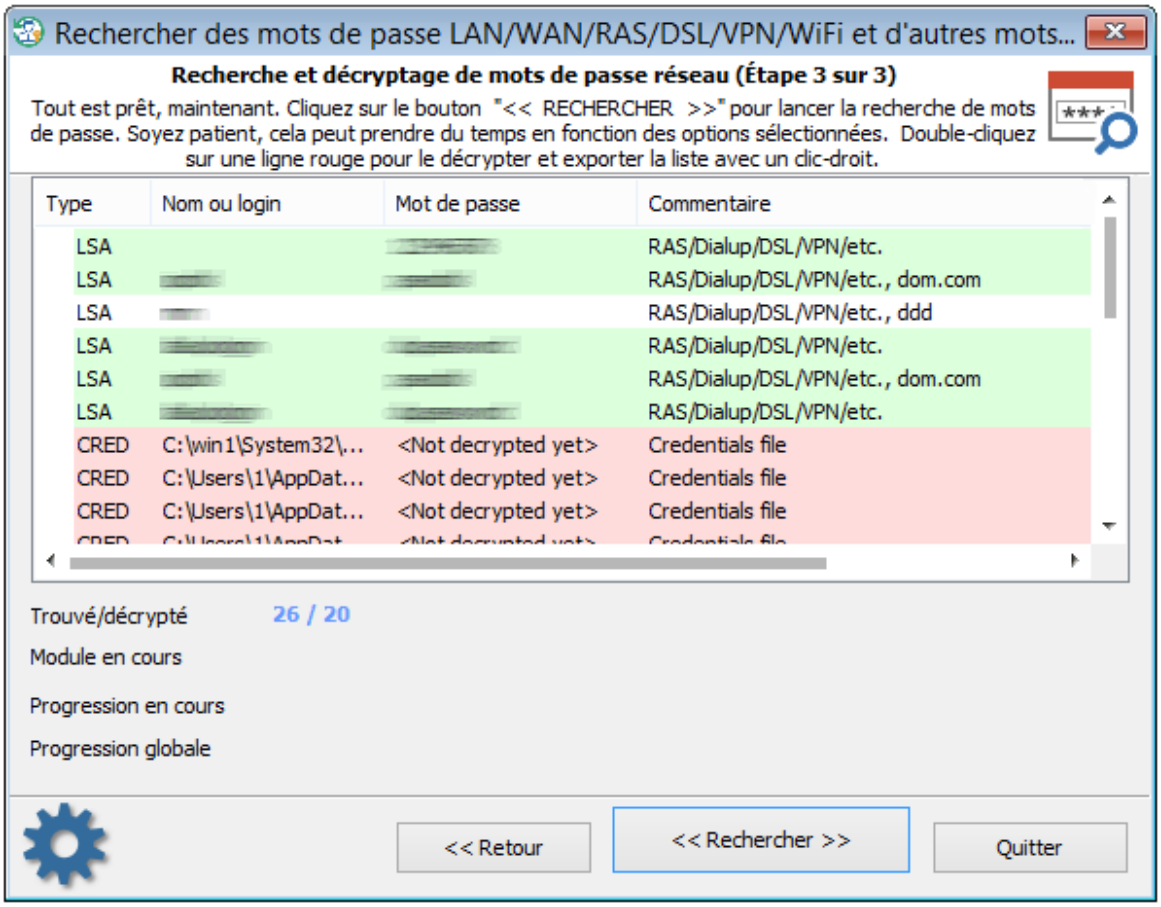


Les logiciels de courriels (e-mails) suivants sont supportés:
- Outlook Express
- Microsoft Office Outlook
- Internet Mail
- Internet Live Mail
- Windows Mail
- TheBat!
- Incredimail
- Eudora

Gardez à l'esprit que les mots de passe des courriels (e-mails) peuvent être stockés dans des navigateurs Internet. Cela dépends si l'utilisateur se sert de son logiciel de courriels (e-mails) ou d'un navigateur Web pour lire ses courriels (e-mails).
Les mots de passe de Outlook Express, TheBat!, Incredimail, Eudora, et certaines versions de MS Office Outlook peuvent être décrypté instantanément.

Le décryptage des autres données nécessite le mot de passe du compte Windows. Double-cliquer simplement sur la ligne surlignée en rouge. Cela activera la deuxième étape pour l'analyse des données trouvées. Si le mot de passe de la session Windows de l'utilisateur corresponds avec les autres données, elles seront également décodées automatiquement.

3.13.5.3 Rechercher les mots de passe de différents types de réseaux



Pour rechercher les mots de passe réseau, le programme possèdent plusieurs modules pour lire et décrypter les secrets LSA, les archives protégées, le gestionnaire de mots de passe, le Coffre Windows, etc.

Le décryptage des données stockées dans les secrets LSA et les archives protégées est réalisé de

manière automatique et ne nécessite pas d'entrer des paramètres complémentaires.

Cela s'applique aux données suivantes:
- Les mots de passe d'utilisateurs en cache
- Les mots de passe de certains comptes système, de serveur SQL, d'assistance à distance, etc.
- Les services de mots de passe exécutés avec des identifications de connexions spécifiques
- Certains mots de passe réseau stockés dans les serveurs d'OS
- Les mots de passe de connexions sans-fils: RAS, DSL, VPN, etc
- Les mots de passe d'anciennes versions de Internet Explorer/Outlook/Outlook Express/FTP, etc.
- Les mots de passe pour les connexions sans-fil (WPA/WPA2)
- Les mots de passe des stratégies de groupes de domaine

Pour les autres mots de passe protégés avec DPAPI, le mot de passe du compte de l'utilisateur est nécessaire pour réussir le décryptage:
- Les mots de passe stockés dans le gestionnaire d'identification (Credential manager): les mots de passe pour les ordinateurs distants du réseau local (LAN), de certains comptes d'e-mails (stockés par Microsoft Outlook), de MSN Messenger, de Internet Explorer 7-9 pour les sites Web qui utilisent l' authentification de base ou Digest Access Authentication, le bureau à distance, les identifiants de connexions pour les flux RSS, etc.
- Les enregistrements du Coffre Windows: les mots de passe de certaines versions de Internet Explorer/Outlook/Windows Mail, les mots de passe de comptes qui utilisent une identification par PIN/image ou une identification biométrique (seulement pour Windows 8).

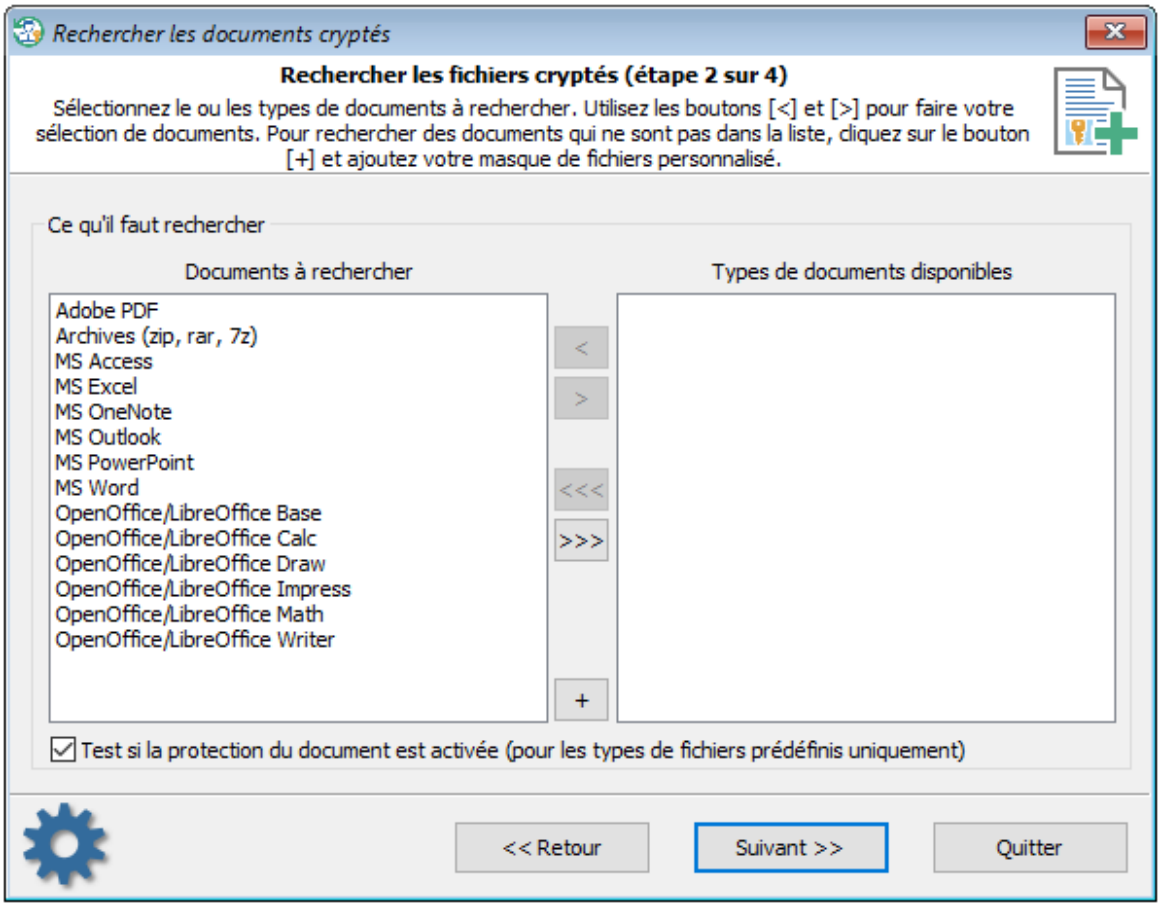
Vous pouvez en savoir plus sur le cryptage DPAPI dans notre article détaillé expliquant cette méthode de protection.

Dans certains serveurs de systèmes d'exploitation, le programme peut exploiter avec succès la vulnérabilité trouvée, avec succès, lui permettant de décrypter les blobs DPAPI sans fournir le mot de passe du propriétaire du compte !
Pour plus d'information à ce propos, vous pouvez consulter notre article détaillant les vulnérabilités des OS de serveurs.

3.13.6 Rechercher les documents cryptés

Cette fonctionnalité du programme permets de scanner un PC à la recherche de documents cryptés, d'archives et de fichiers protégées par un mot de passe. Il est simple à utiliser, rapide et souple dans sa configuration. Vous pouvez même spécifier votre type de fichiers personnalisés que vous souhaitez rechercher.
Le processus de recherche est divisé en trois étapes simples:

1 Sélection des types de documents



Par défaut, le programme recherche les documents prédéfinis suivants:

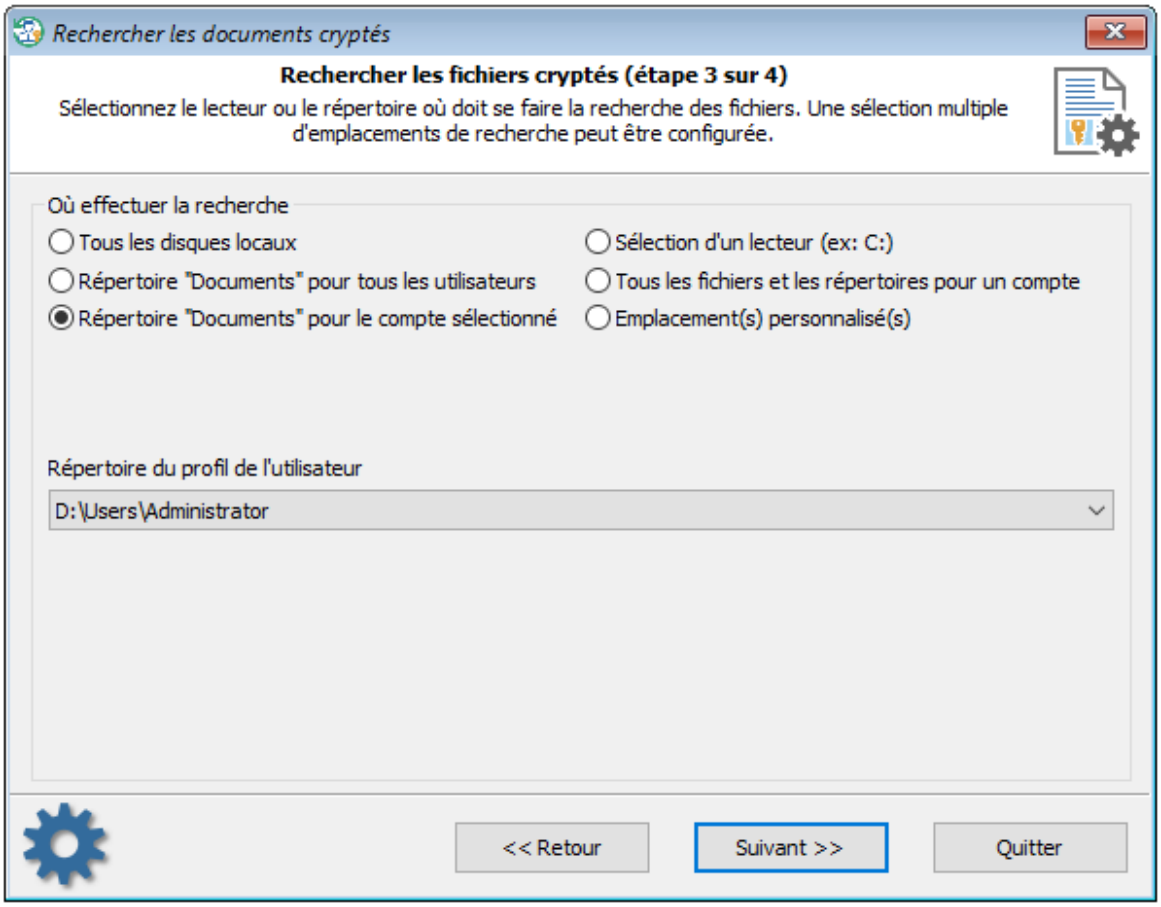
- Les fichiers d'archives (zip, rar, 7z)
- Les documents Adobe PDF
- Les documents MS Word
- Les fichiers MS Excel
- Les bases de données MS Access
- Les présentations MS PowerPoint
- Les notes MS OneNote
- Les fichiers de données MS Outlook
- Les documents OpenOffice/LibreOffice Writer
- Les fichiers OpenOffice/LibreOffice Calc
- Les bases de données OpenOffice/LibreOffice
- Les présentations OpenOffice/LibreOffice Impress
- Les documents OpenOffice/LibreOffice Draw
- Les documents OpenOffice/LibreOffice Math

En utilisant les boutons [>] et [<], vous pouvez inclure ou exclure des types de documents du processus de recherche. Si vous voulez ajouter vos propres types de fichiers à rechercher, utiliser le bouton [+] et compléter la description et le masque de recherche.
Par exemple, le masque suivant peut être utilisé pour rechercher des fichiers de données de KeePass: ***.kdbx, *.kdb, *.pwd**

Gardez à l'esprit, que l'analyse de protection par mots de passe n'est pas utilisée pour les masques personnalisés.
L'option "Test si la protection du document est activé...." est utilisé dans le cas ou l'on souhaite désactiver complètement l'analyse de la protection par mots de passe.

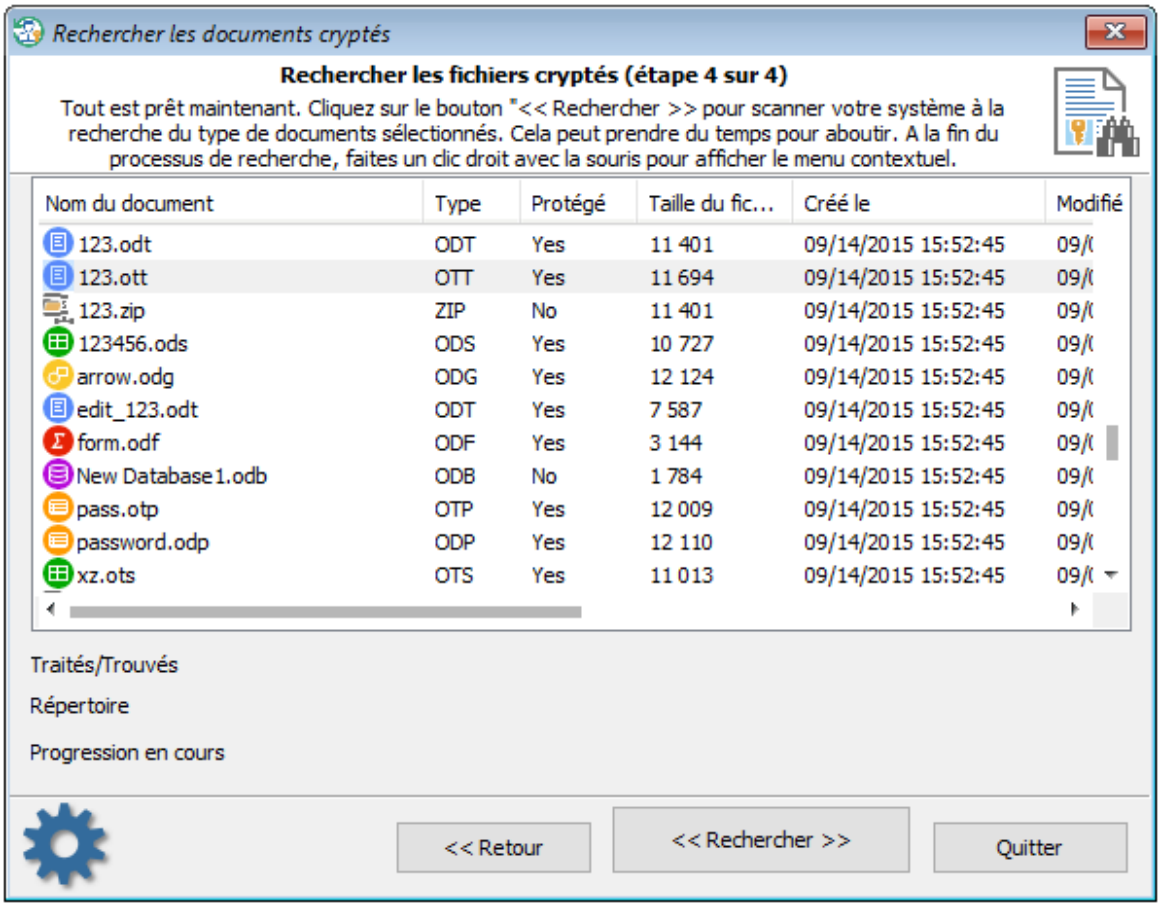
Cela peut accélérer de manière significative le processus de recherche, dans certains cas.

2 Sélection de l'emplacement de recherche



Vous pouvez réduire la plage de recherche en configurant, par exemple, le "Répertoire "Documents" pour le compte sélectionné", ou choisir un répertoire en particulier.

3 Rechercher les documents



Même si le programme a été optimisé pour une recherche rapide, le scan des disques durs avec un grand nombre de fichiers peut prendre beaucoup de temps.
Une fois que la recherche est terminée, Faites un clic droit sur la liste de documents pour afficher les actions possibles.
Par exemple, vous pouvez sauvegarder la liste des fichiers trouvés dans un fichier texte/html, ou créer un fichier d'archive ZIP avec les éléments sélectionnés.

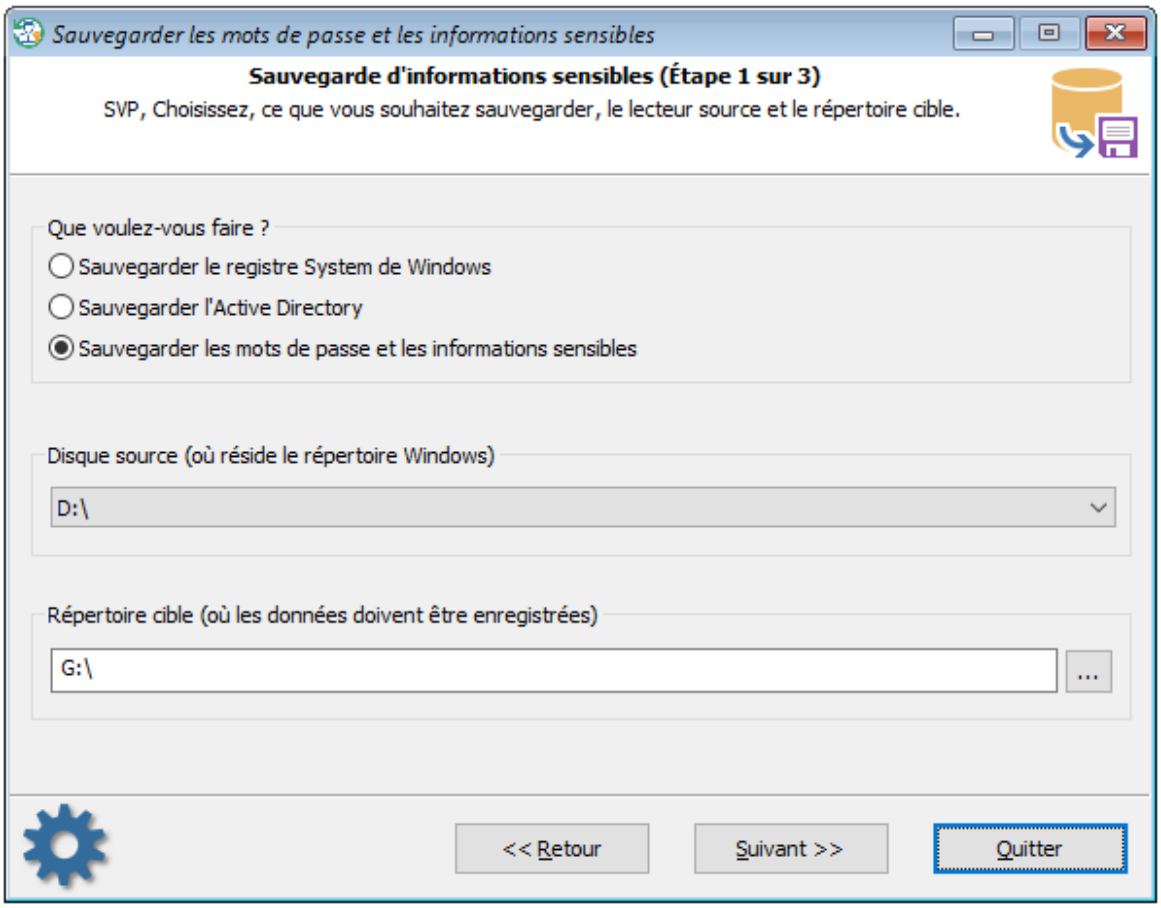
3.13.7 Sauvegarde des mots de passe et des informations sensibles

Dans certains cas, il est vital de faire une copie de la base de registre de Windows ou de la base de données de l'Active Directory.
Reset Windows Password est d'un grand secours pour tous ceux qui souhaite sauvegarder leurs fichiers facilement. Cela permets de faire un instantané des données sensibles du PC cible en quelques clics.

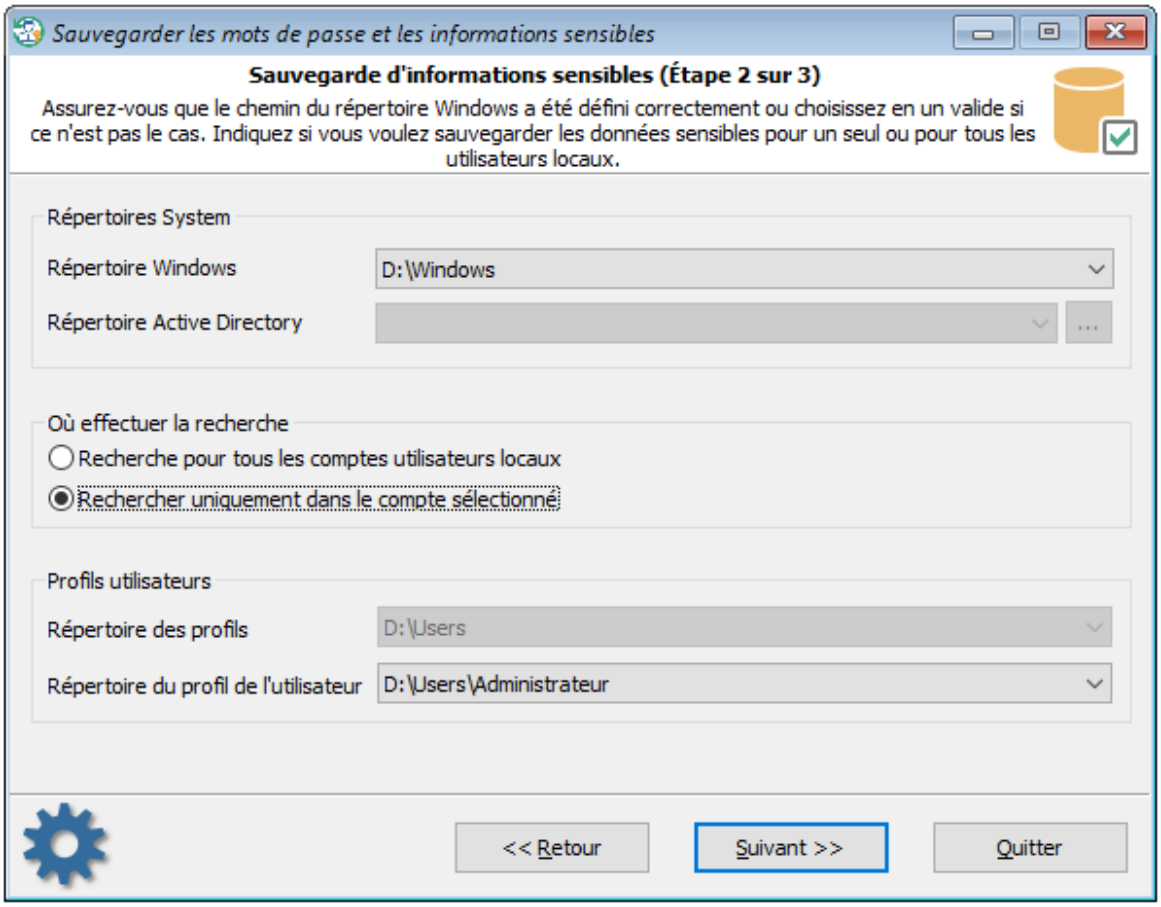
Tout d'abord, vous devez choisir ce que vous souhaitez sauvegarder:
- Les fichiers de la base de registre Windows
- La base de données de l'Active Directory
- Toutes les informations sensibles incluant la base de registre Windows, les mots de passe, les certificats, etc.

Vous devez choisir le lecteur source où se trouve le répertoire Windows et le lecteur/répertoire cible.

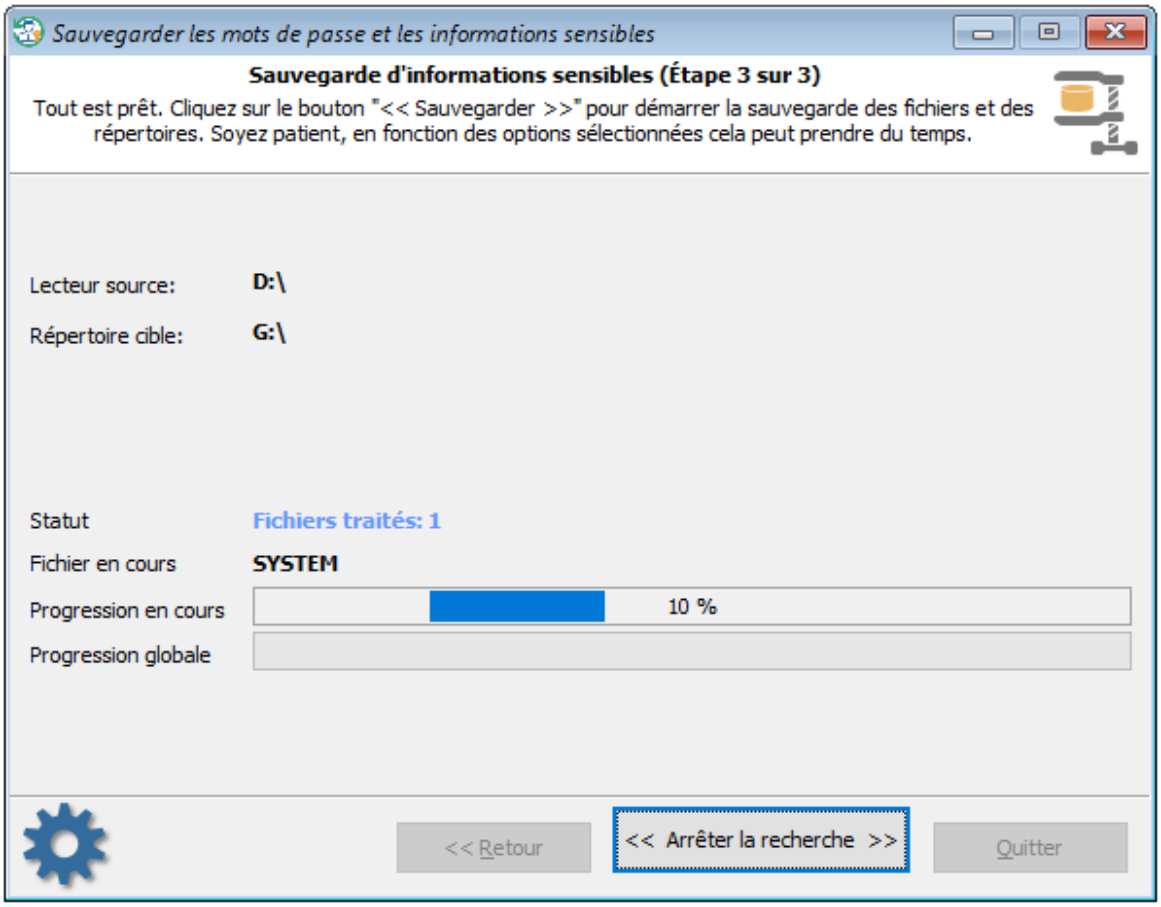
Le répertoire cible sera utilisé pour enregistrer le fichier d'archive de sortie. Par défaut, le programme suggère le premier disque dur comme source et le premier disque amovible comme cible.



L'étape suivante est un peu plus simple.
Dans le cas ou vous avez choisi à l'étape précédente, sauvegarder la base de registre/Active Directory, tout ce que vous avez besoin ici, c'est de confirmer les répertoires Windows/Active Directory. Sinon, vous devez choisir soit le(s) répertoire(s) du ou des profils pour le(s)'utilisateur(s) choisi(s), en fonction des options.

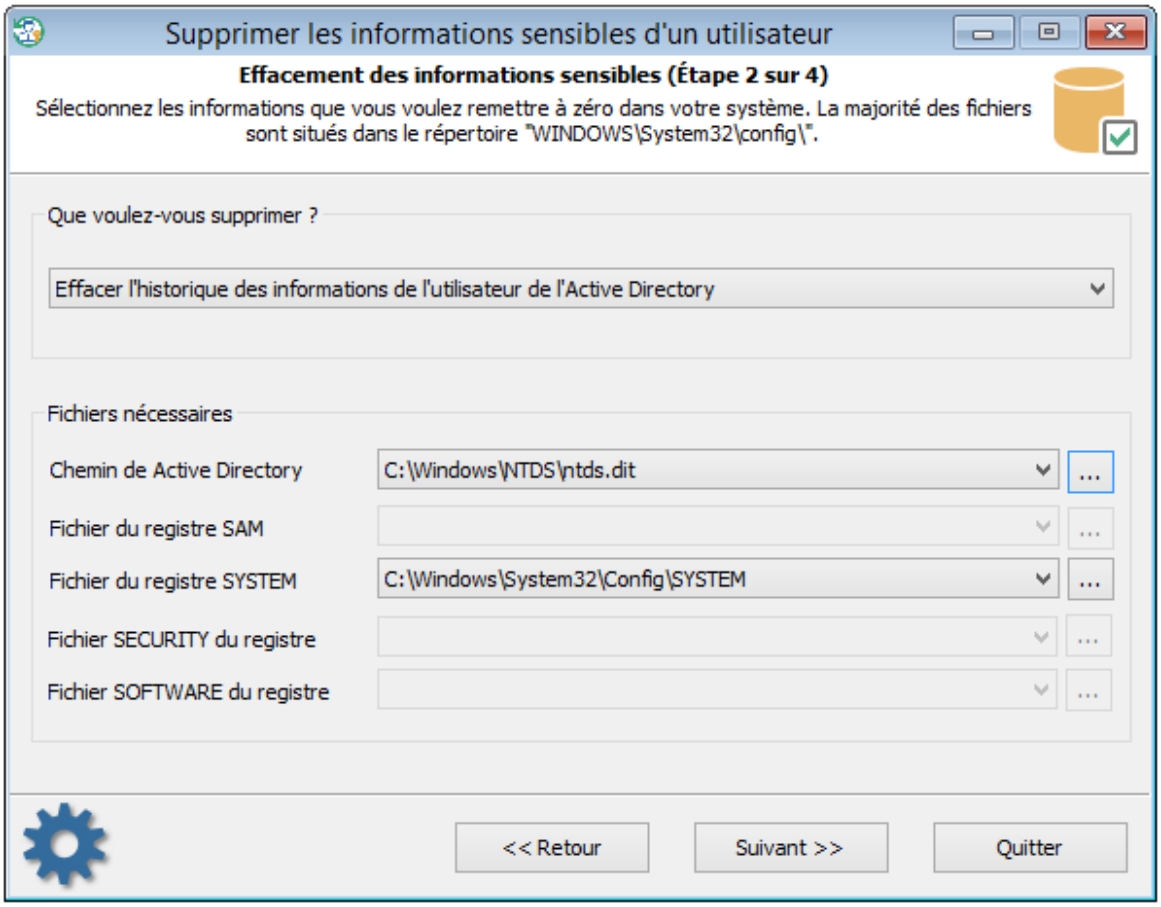


A la dernière fenêtre de dialogue, vous pourrez visualiser la progression des opérations de sauvegardes.
Cliquer sur le bouton **<< Sauvegarder >>** pour lancer le processus. Une fois l'opération terminée, vous devez avoir un fichier d'archive *.ZIP qui contient tous les fichiers souhaités. Ultérieurement, vous pourrez utiliser ces fichiers pour analyser les données secrètes dans un autre logiciel. Par exemple, dans l'outil **Windows Password Recovery**.



3.13.8 Supprimer les informations sensibles d'un utilisateur

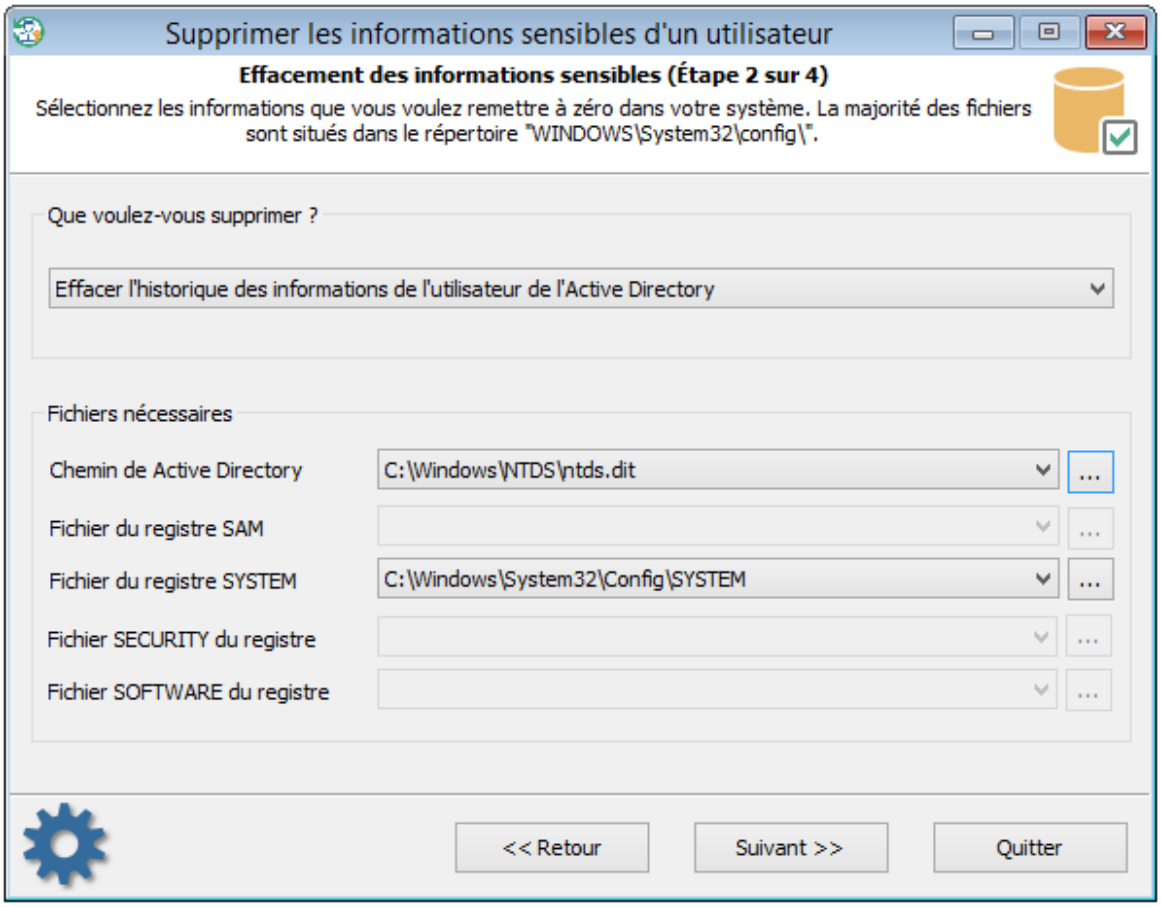
Sélection des données à supprimer



Le logiciel possède un certains nombre de fonctions avancées. L'une d'elle est l'effacement d'informations qui peuvent être utilisées par des personnes mal intentionnées pour récupérer des mots de passe de comptes sur votre ordinateur. Attention, la suppression des informations est permanente sans aucune chances de récupération.

Cela inclus les éléments suivants:

1. La suppression de l'historique de mot de passe pour les comptes SAM standard et les comptes d'utilisateurs d'Active Directory. L'historique de mots de passe SAM, par exemple, configuré dans les stratégies de groupes de l'ordinateur local. Démarrer -> Exécuter -> gpedit.msc -> cliquer sur OK. Sous "Configuration Ordinateur", ouvrer le répertoire sous Paramètres Windows -> Paramètres de sécurité-> Stratégies locales -> Options de sécurité. Rechercher la règle: Ouverture de sessions interactive: Nombre d'ouverture de sessions précédentes en utilisant le cache.
2. La suppression des mots de passe de domaine en cache. Pour en savoir plus sur les mots de passe de domaine en cache, vous pouvez lire cet article.
3. La suppression du mot de passe de sessions Windows en cache.
4. La suppression des informations du mot de passe pour la disquette de réinitialisation. Avec ces informations et le disque de réinitialisation de mot de passe, il est possible de récupérer le mot de passe en clair original.
5. La suppression des indices de mots de passe.
6. La réinitialisation de Syskey



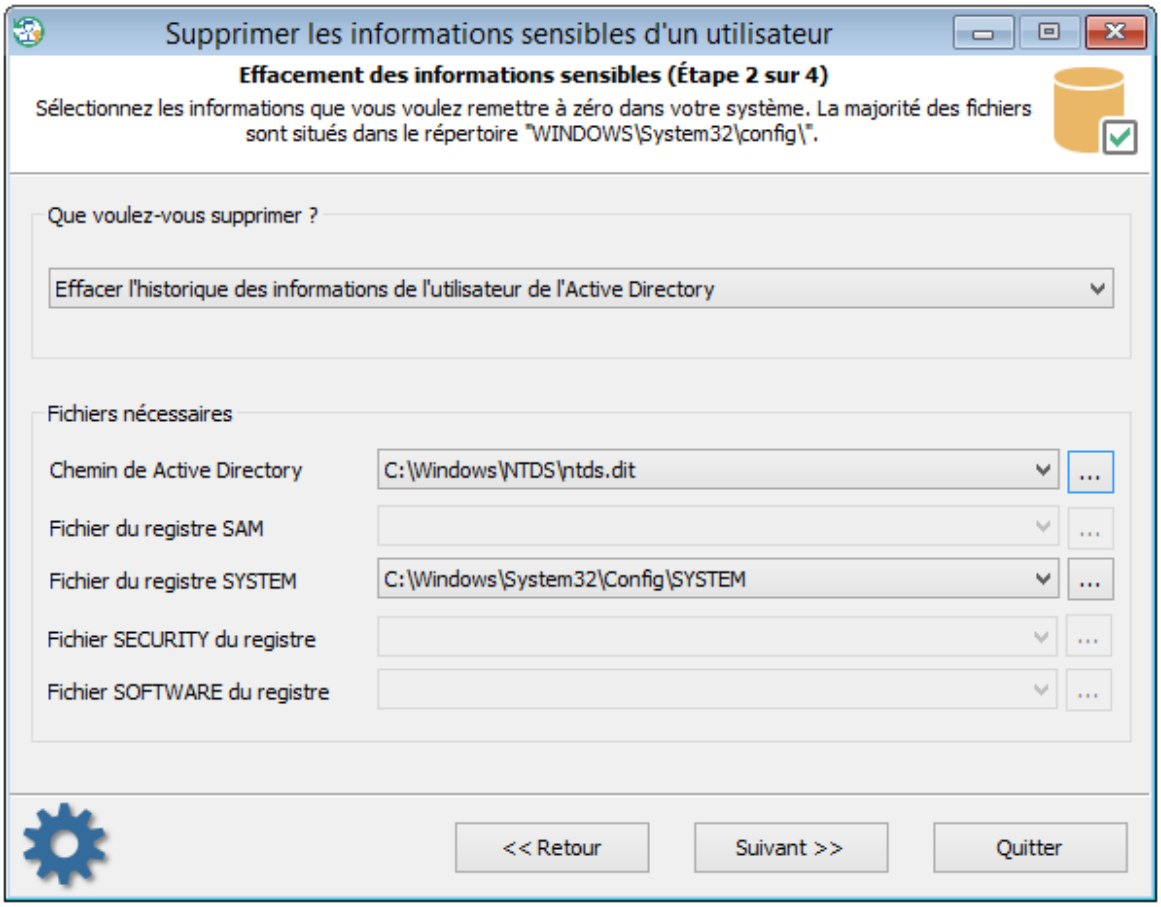
Pour poursuivre avec le logiciel, vous aurez à fournir les fichiers suivants (ou à sélectionner ceux disponibles):
- Effacer l'historique des mots de passe de l'AD – le fichier de la base de registre **SYSTEM** et le fichier de la base de données de l'Active Directory (**ntds.dit**)
- Effacer l'historique des mots de passe SAM du compte de l'utilisateur – les fichiers de la base de registre **SAM** et **SYSTEM**
- Effacer les mots de passe en cache du Domaine – les fichiers de la base de registre **SECURITY** et **SYSTEM**
- Effacer les mots de passe d'ouverture de sessions de Windows en cache – les fichiers de la base de registre **SECURITY**, **SOFTWARE** et **SYSTEM**
- Effacer les informations de réinitialisation des mots de passe Windows - les fichiers de la base de registre **SAM**, **SECURITY** et **SYSTEM**
- Effacer les indices de mots de passe - les fichiers de la base de registre **SAM**, **SOFTWARE** et **SYSTEM**
- Réinitialisation de SYSKEY - les fichiers de la base de registre **SAM**, **SECURITY** et **SYSTEM**

Tous les fichiers de la base de registre sont stockés dans le répertoire suivant: **%WINDIR%\system32\config**. Sachant que %WINDIR% est le répertoire où est installé, par défaut - C:\Windows.

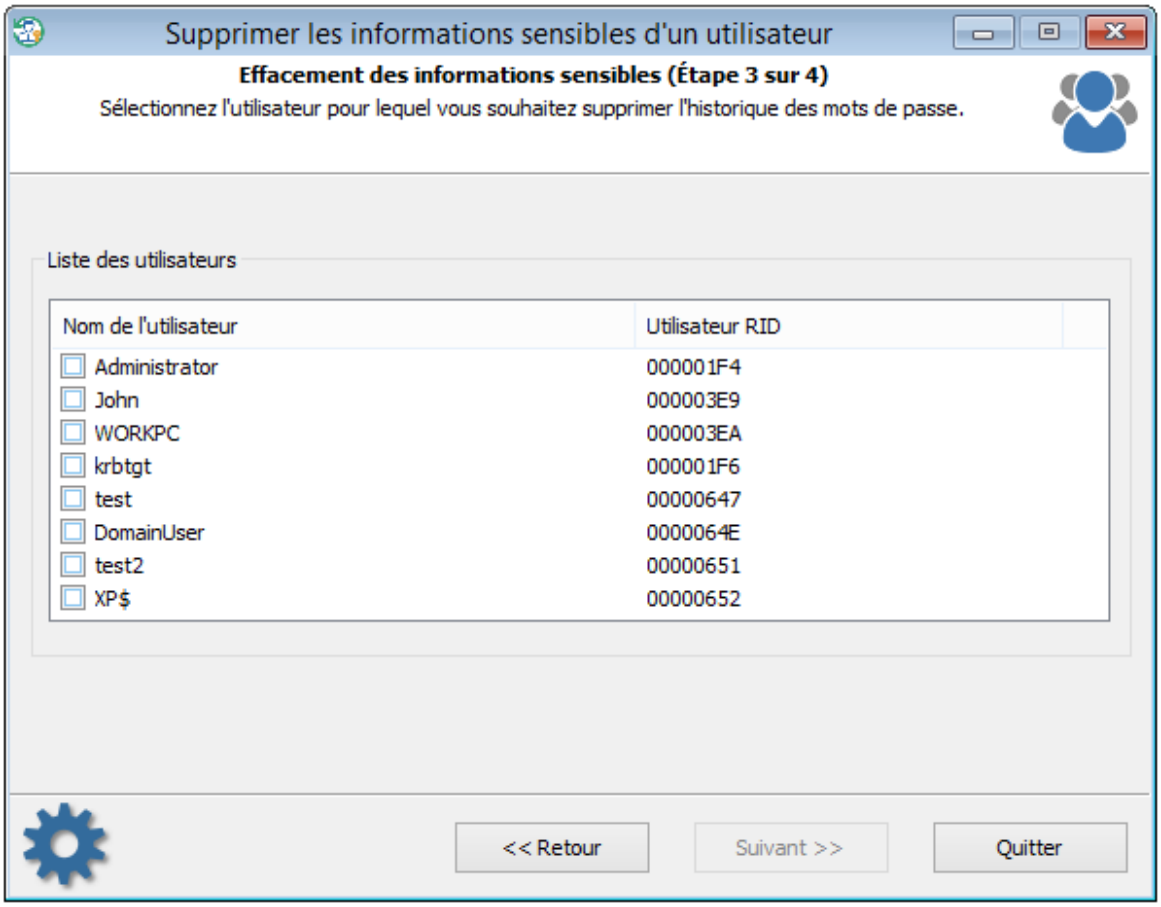
L'emplacement où se situe la base de données de l'AD est défini pendant l'installation de Windows. Par défaut, c'est le répertoire **%WINDIR%\NTDS**.

3.13.8.1 Effacer l'historique des mots de passe SAM/Active Directory des utilisateurs

Sélection des fichiers

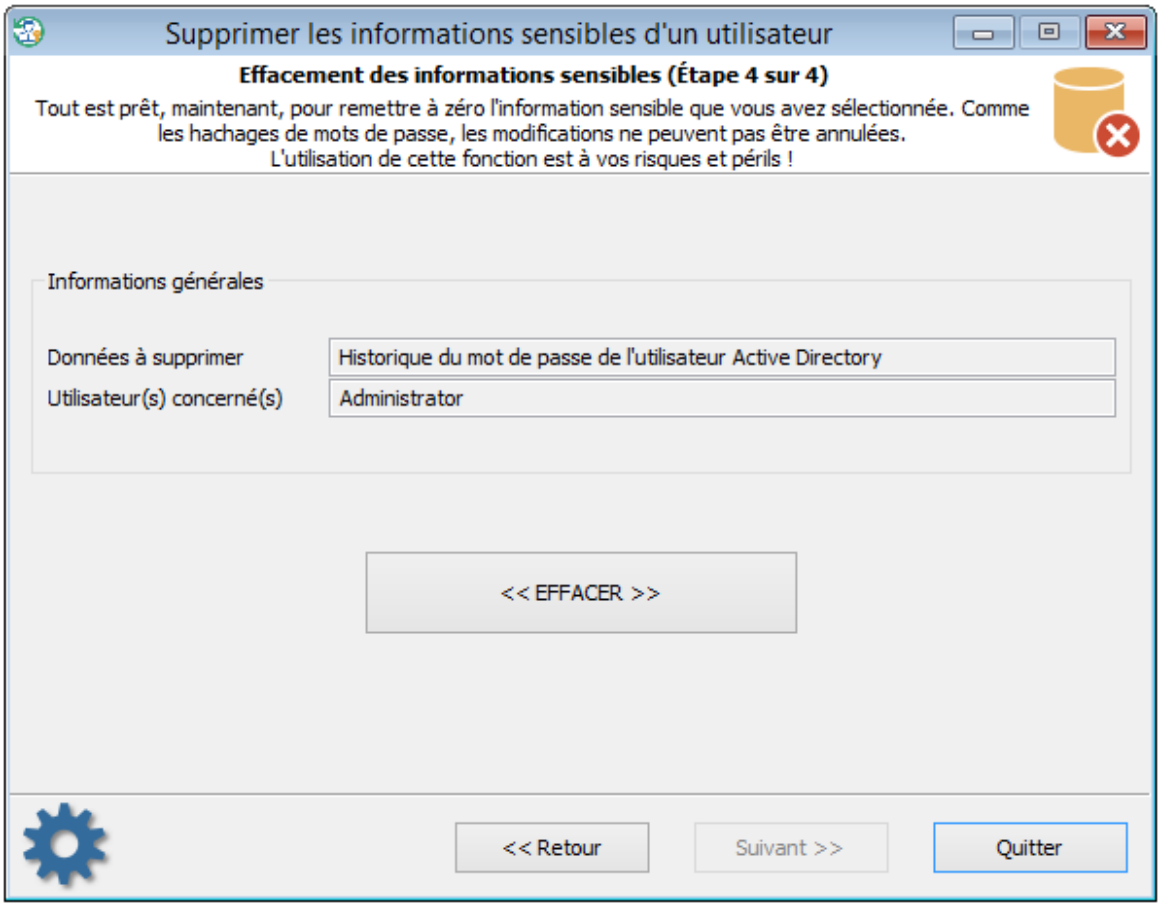


Sélection de l'utilisateur



Dans la liste des comptes, sélectionner celui dont vous voulez supprimer l'historique des mots de passe. L'application affiche uniquement les utilisateurs ayant un historique.

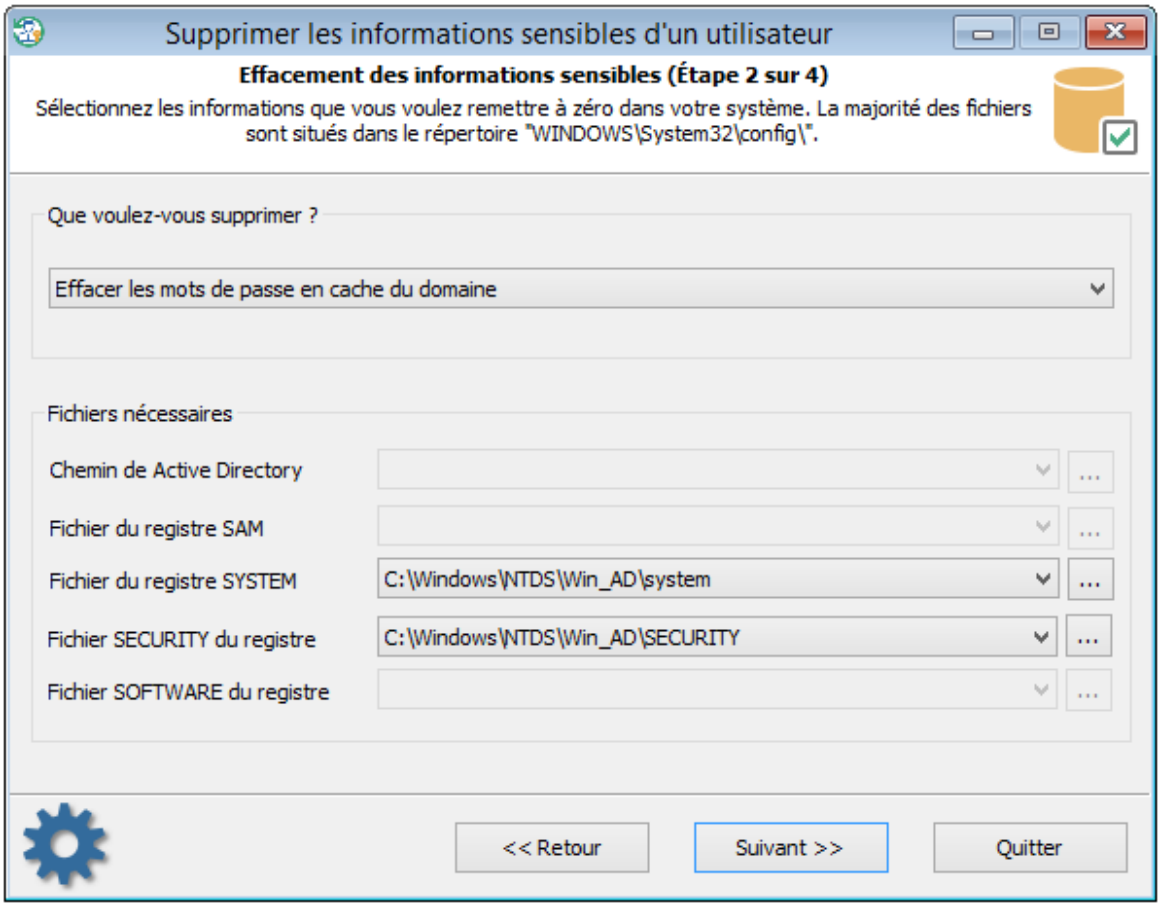
Suppression de l'historique des mots de passe



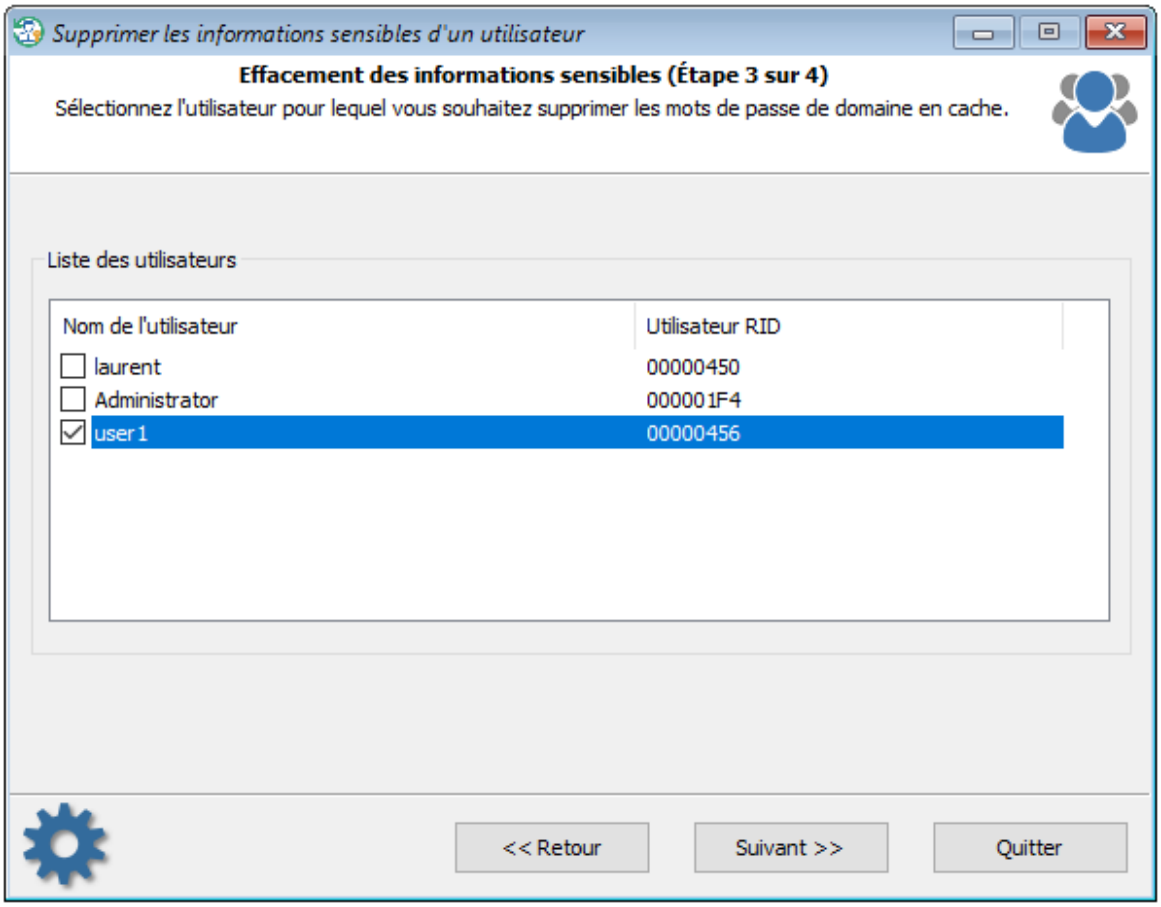
Cliquer sur << EFFACER >> pour supprimer de façon permanente les informations inutiles.

3.13.8.2 Effacer les mots de passe de Domaine en cache

Sélection des données source

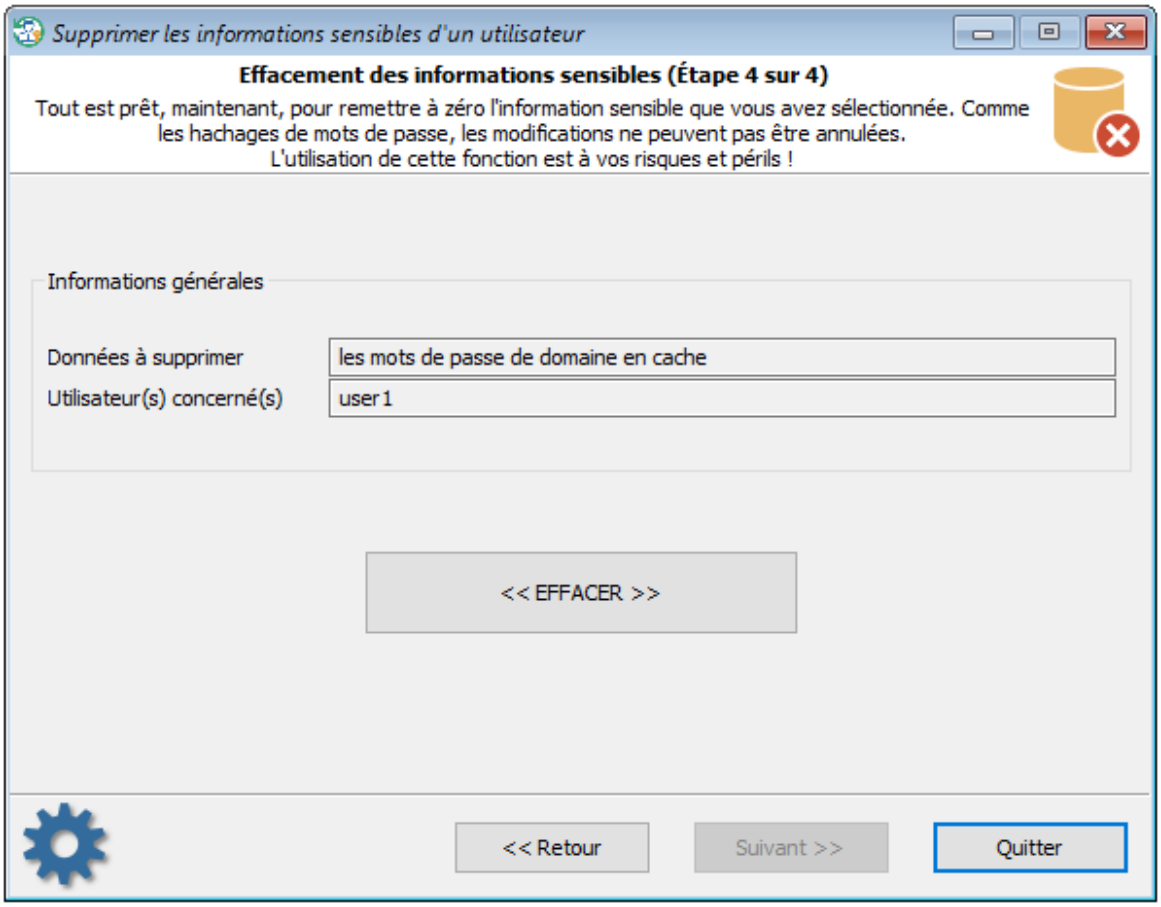


Sélection du compte de l'utilisateur



Sélectionner le compte dont vous voulez supprimer les mots de passe.

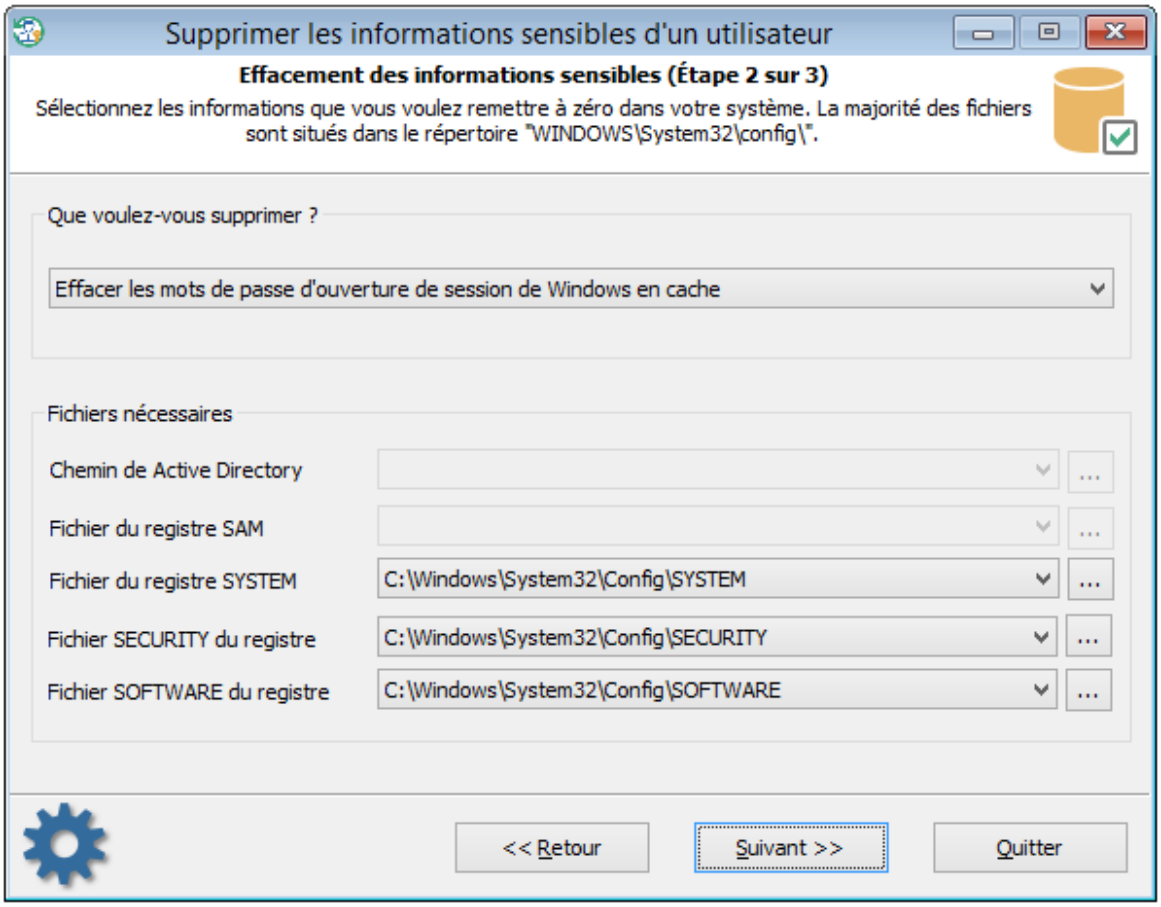
Supprimer les mots de passe de Domaine en cache



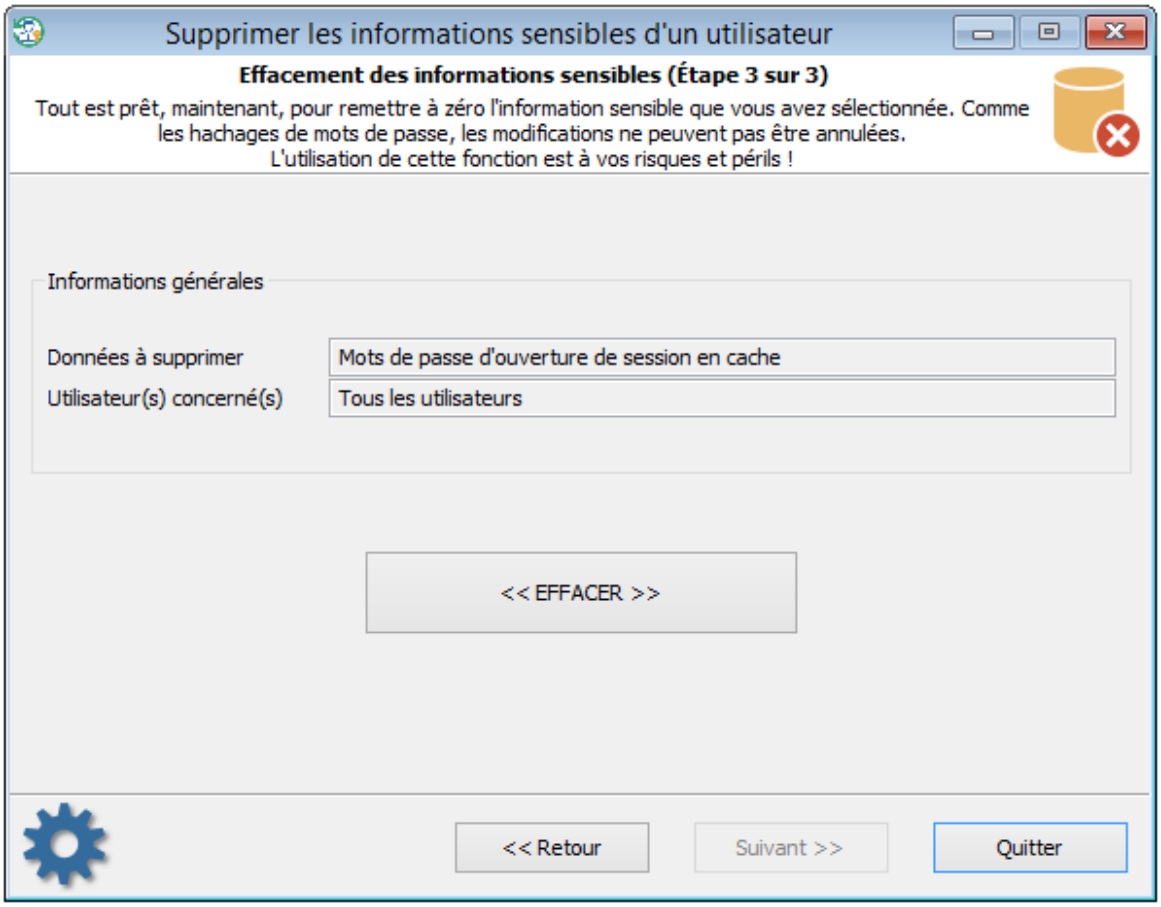
Et pour finir, confirmer la suppression de tous les mots de passe en cache pour le compte, comme ici dans l'exemple, pour user1.

3.13.8.3 Effacer les mots de passe d'ouverture de sessions de Windows en cache

Sélection des données source



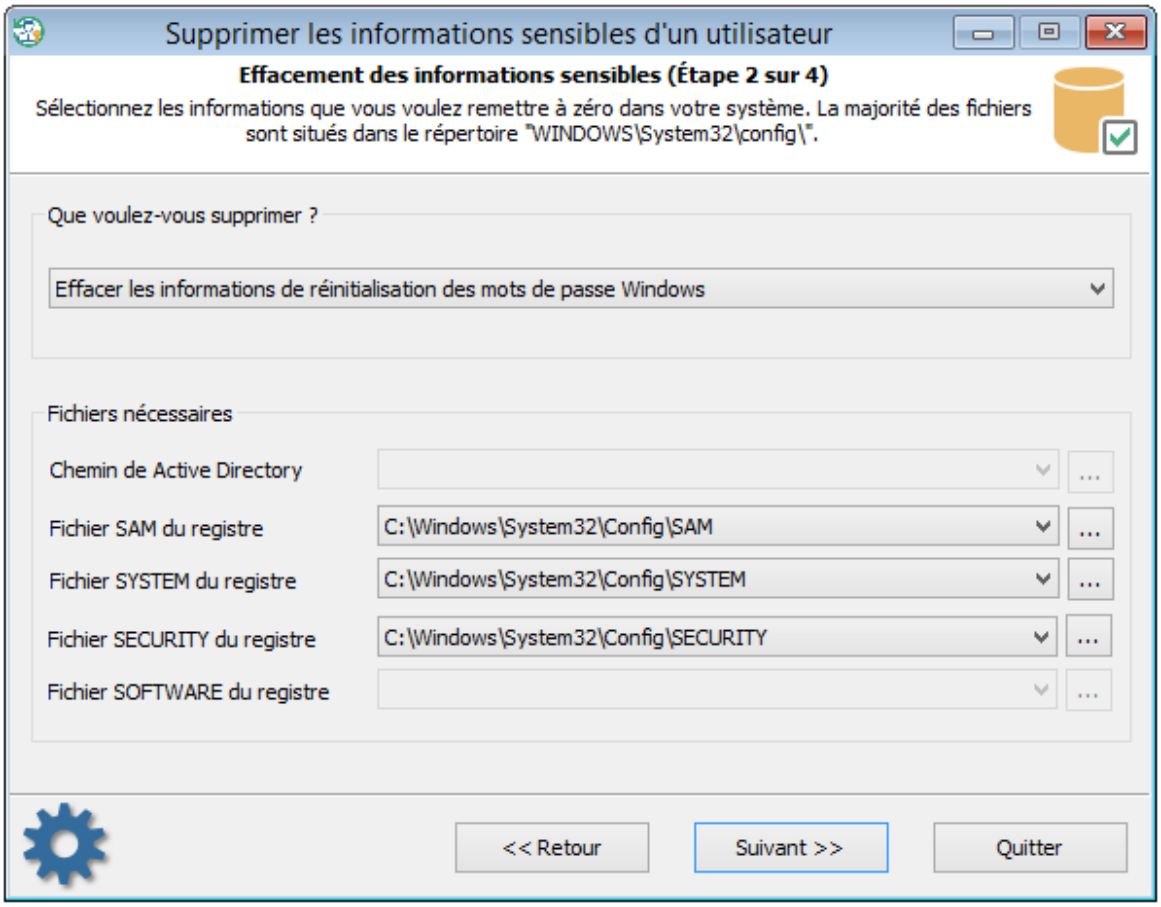
Supprimer les mots de passe d'ouverture de sessions Windows en cache



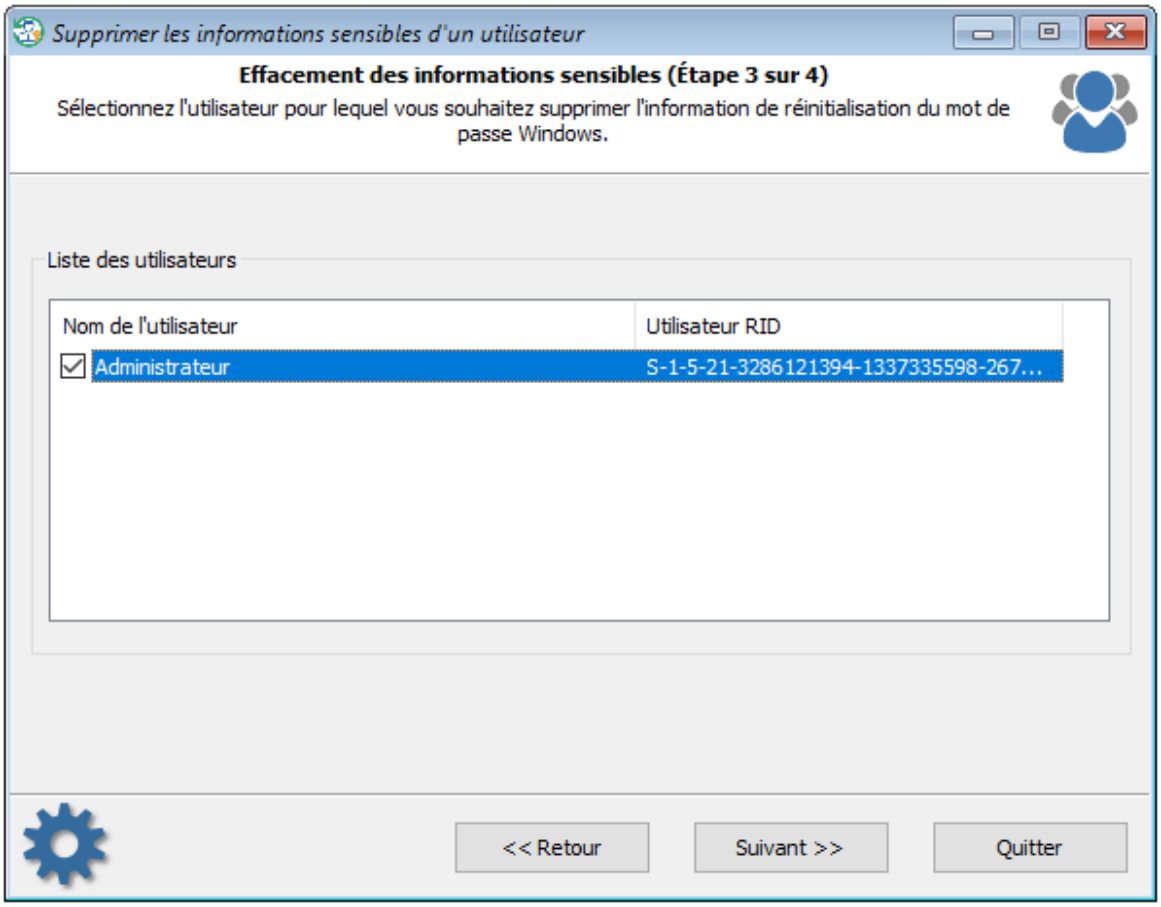
Pour finir, confirmer la suppression permanente des mots de passe de connexions en cache.

3.13.8.4 Effacer les informations du disque de réinitialisation de mot de passe

Sélection des données source

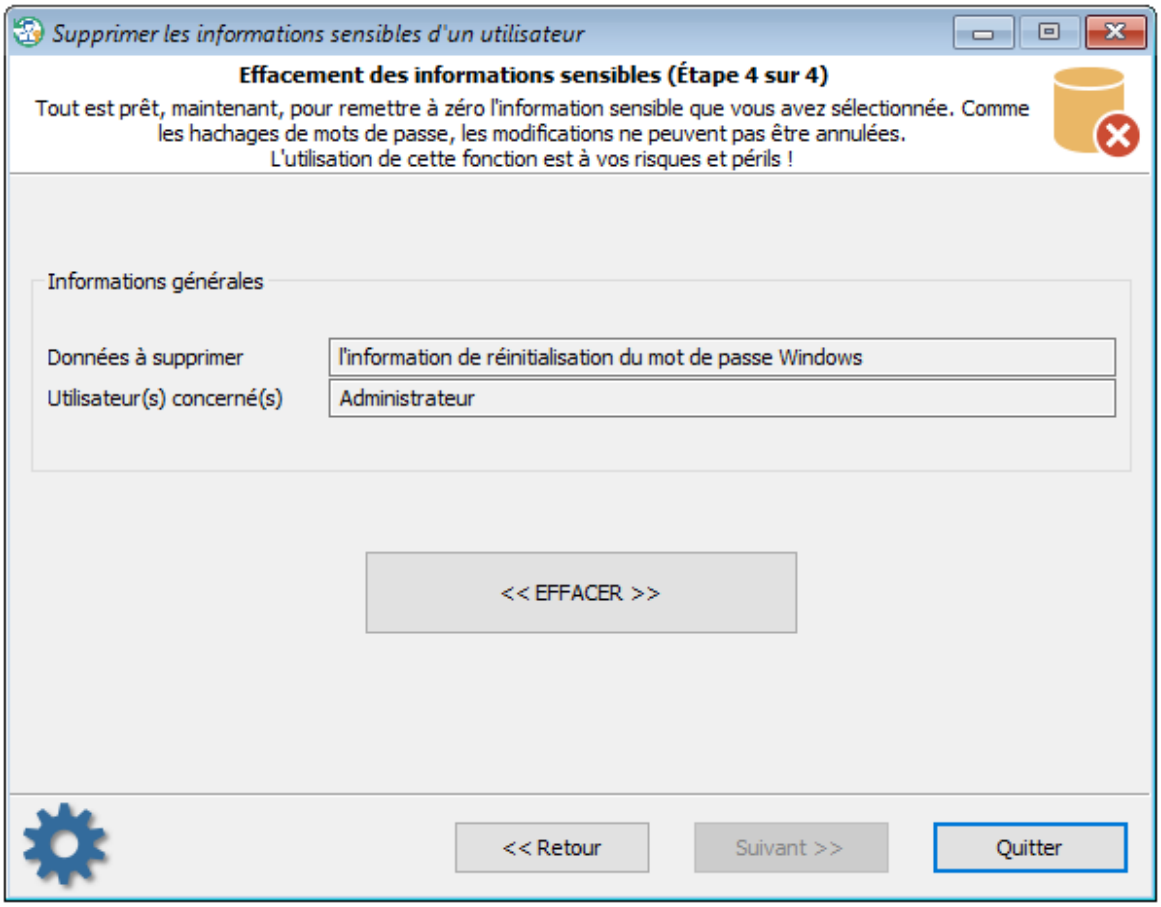


Sélection du compte d'un utilisateur



Choisisse l'utilisateur dont vous souhaitez effacer les informations. Lors de la création du disque de réinitialisation du mot de passe, le mot de passe crypté de l'utilisateur est stocké dans la base de registre. Alors que la disquette/clé USB stocke la clé de cryptage. La suppression de la base de registre du mot de passe crypté, rends l'existence d'une disquette/clé USB de réinitialisation du mot de passe inutile.

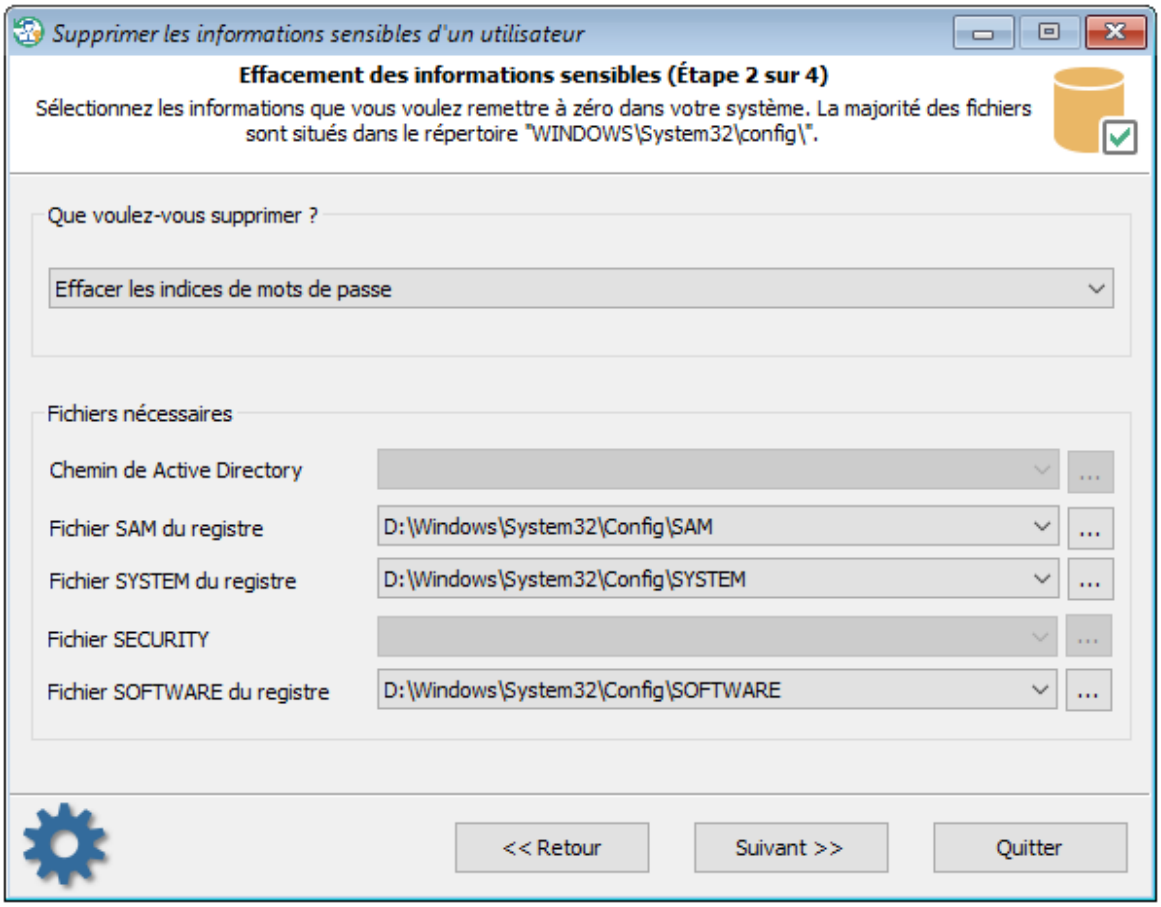
Supprimer les informations de la disque de réinitialisation des mots de passe



Confirmer la suppression des informations en cliquant sur "Effacer".

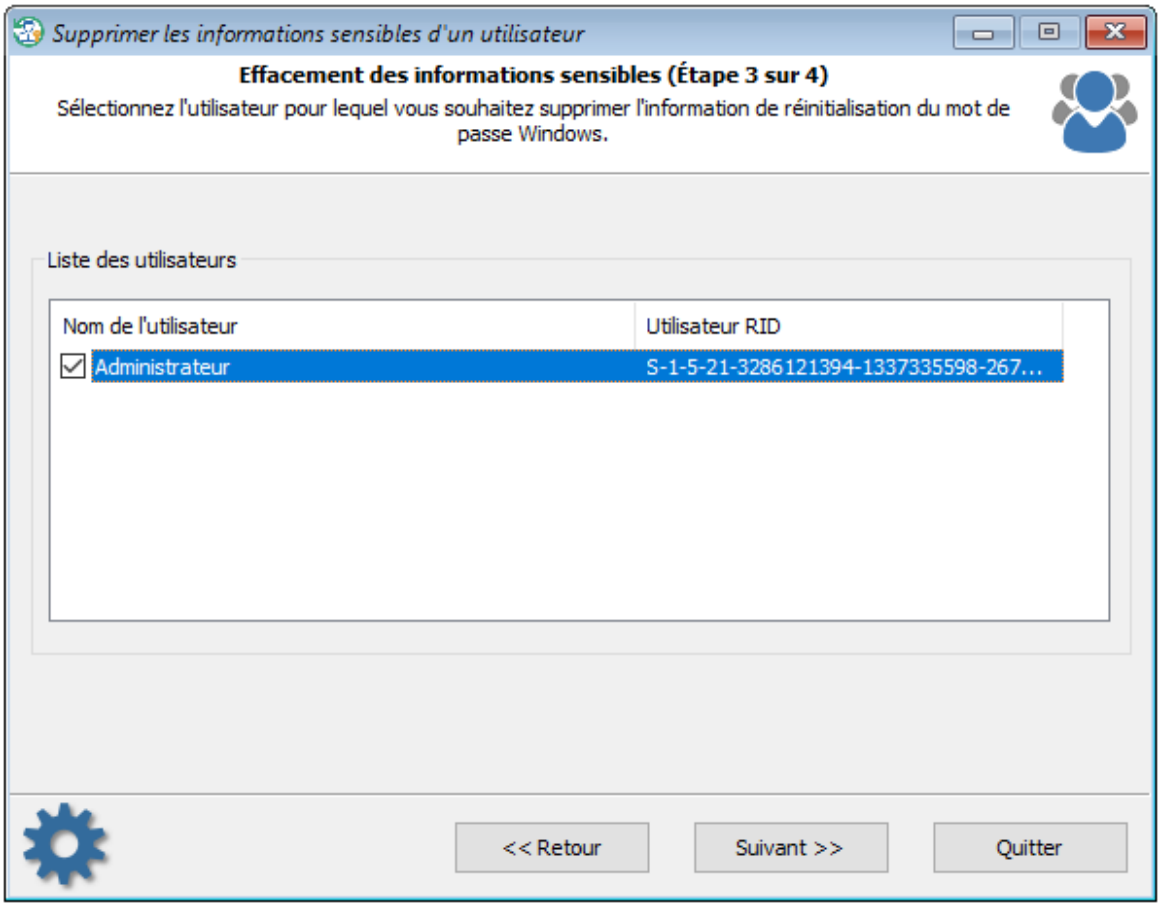
3.13.8.5 Supprimer les indices de mots de passe

Sélection des données source



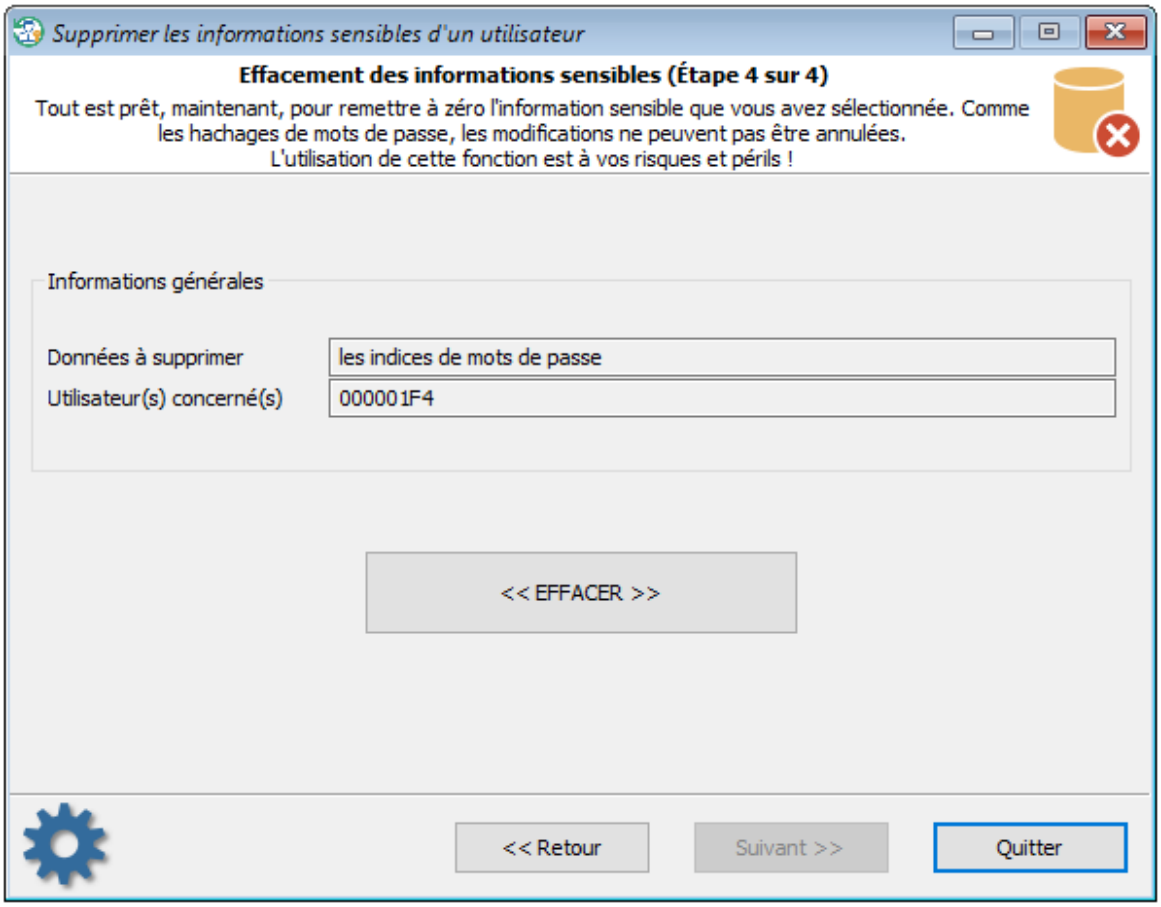
Les astuces de mots de passe sont stockées, soit dans le fichier de la base de registre **SOFTWARE** (pour Windows XP et Windows 2003) ou dans le fichier **SAM** (pour Windows Vista et les OS supérieurs). Le fichier **SYSTEM** est aussi nécessaire pour le décryptage.

Sélection du compte



Sélectionner le compte dont vous souhaitez effacer les indices de mots de passe du système. Passer, ensuite, à l'étape finale.

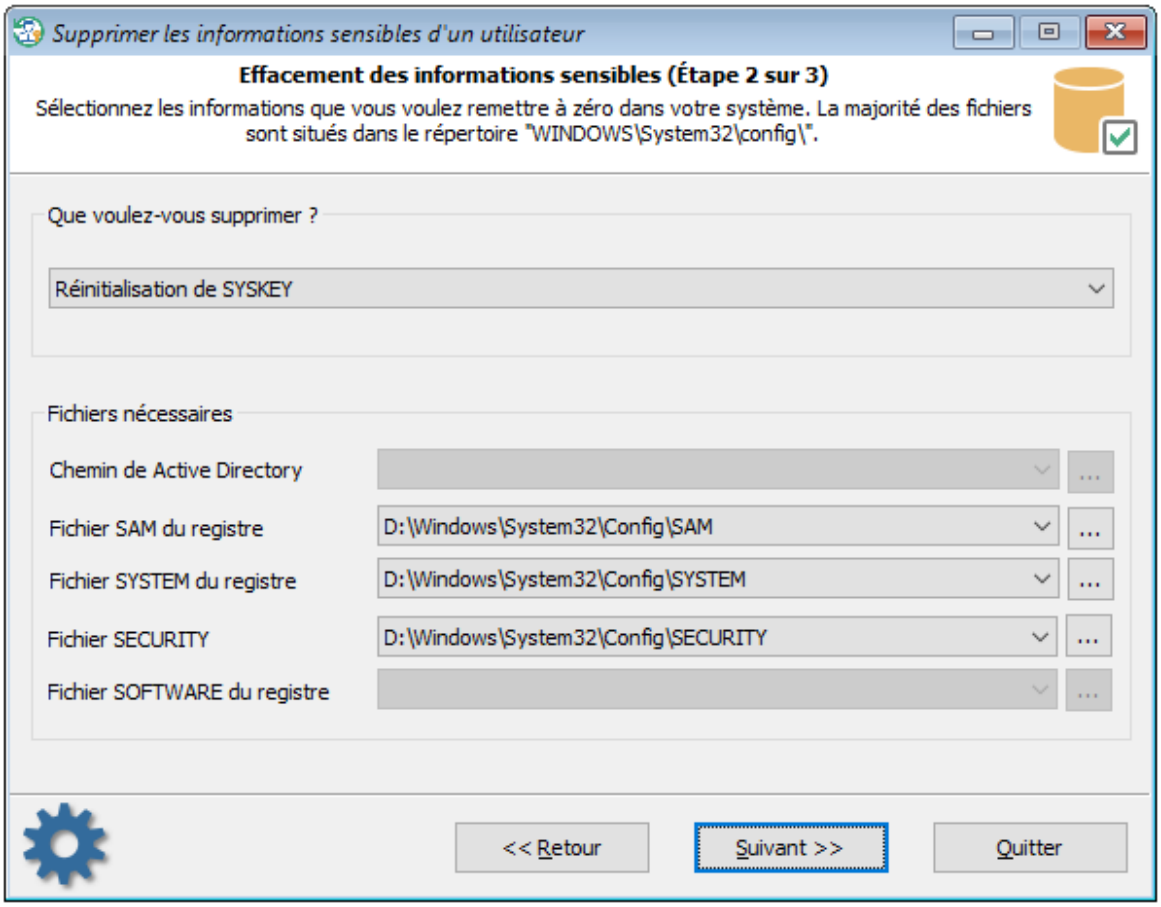
Suppression des indices de mots de passe



Cliquer sur "Supprimer" pour effacer les données.

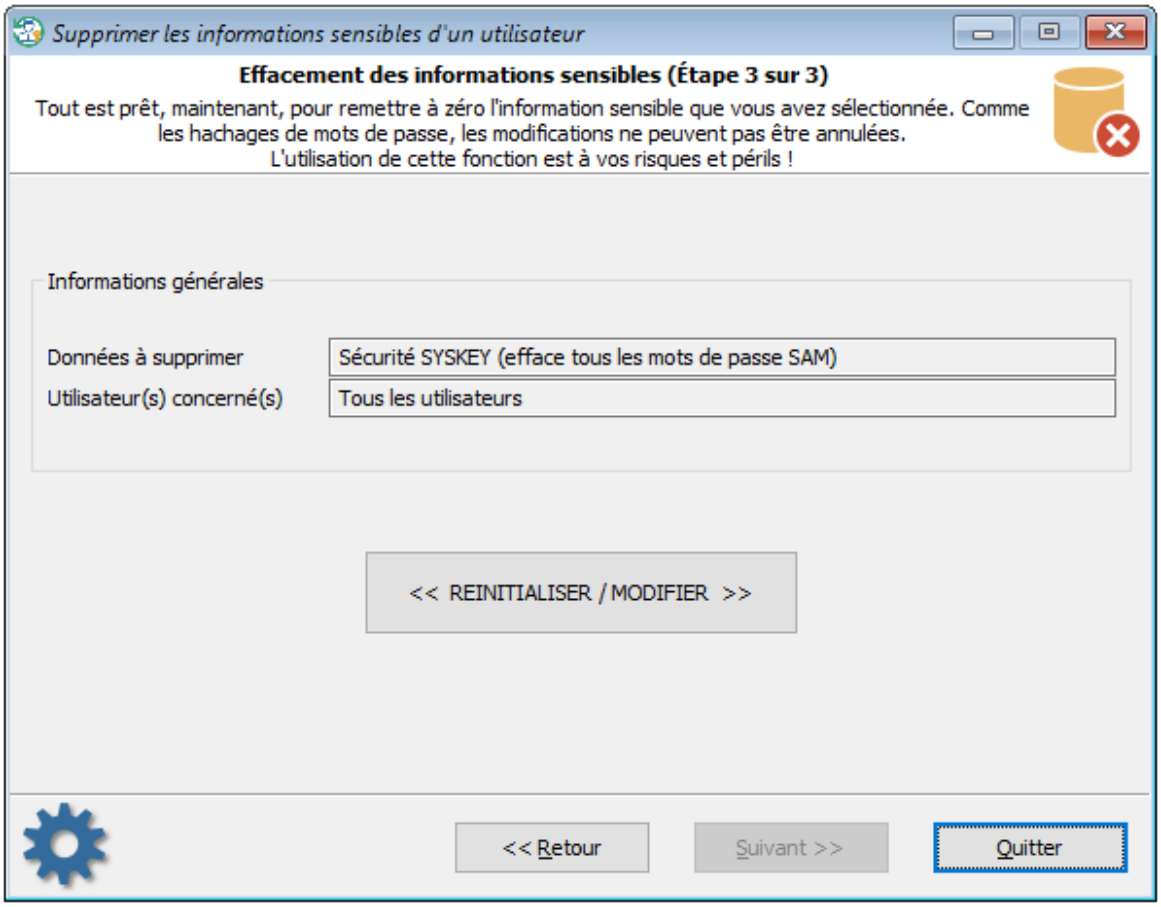
3.13.8.6 Réinitialiser le SYSKEY

Sélection des données source



En premier, vous devez indiquer les 3 fichiers de la base de registre: **SAM**, **SYSTEM** et **SECURITY**. Habituellement, SYSKEY situé dans le fichier **SYSTEM** sous la clé **HKLM\CurrentControlSet\Control\Lsa**.
Mais une fois que vous avez configuré votre SYSKEY, par exemple pour qu'un mot de passe soit nécessaire pour démarrer le système, si vous l'oubliez, il y a aucune possibilité pour démarrer votre système. Cela veut dire que SYSKEY est un outil extrêmement efficace dans les mains d'un spécialiste en PC (Guru). En configurant, votre option SYSKEY avec un mot de passe ou une disquette/clé USB de démarrage, cela est très efficace contre TOUS (!) les programmes de décryptage des mots de passe Windows.
Dans ce cas, un programme d'extraction de mot de passe ne pourra pas décrypter votre hachages du mot de passe même sur cette personne possède tous les accès à votre système.

Réinitialisation de SYSKEY

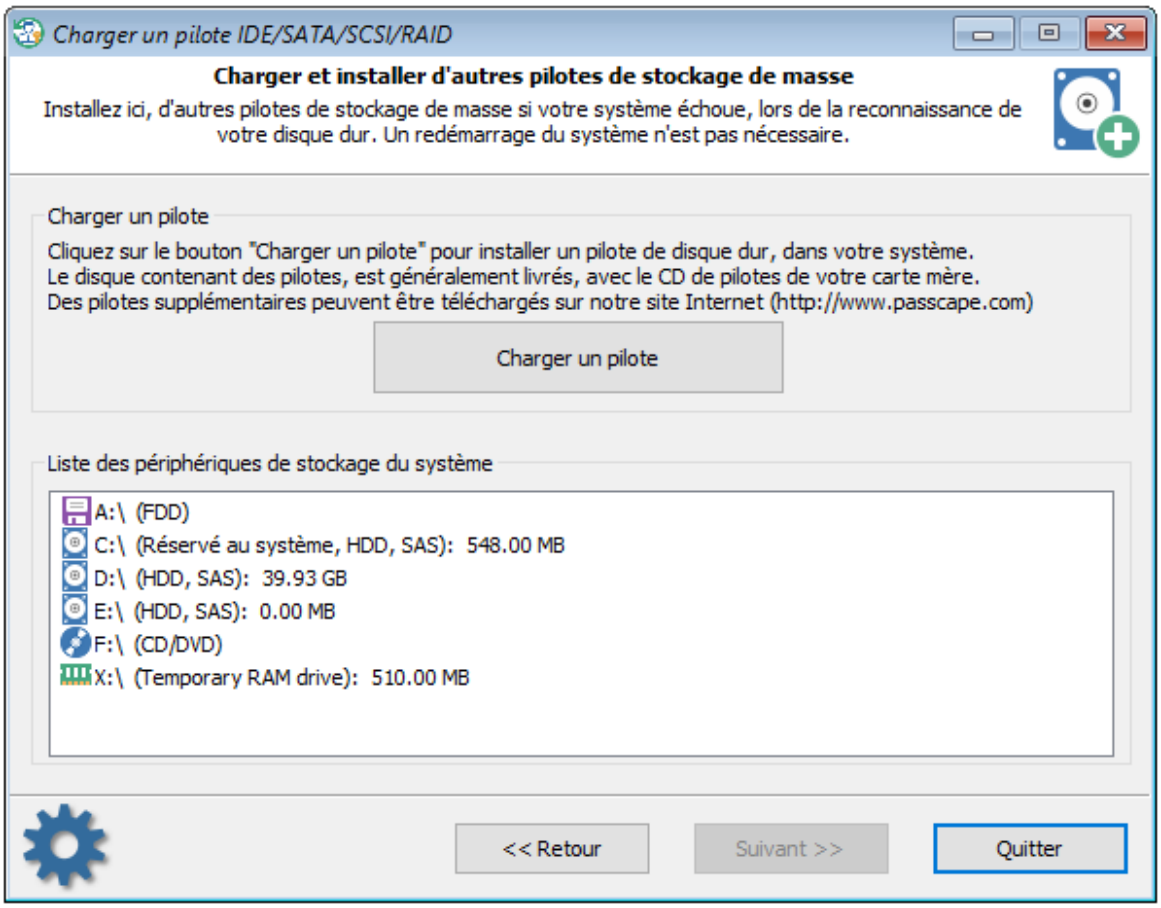


Attention ! La réinitialisation de SYSKEY est une opération à risque qui affecte la sécurité du système complet. Par exemple, après la réinitialisation de SYSKEY, même si vous pouvez ouvrir une session sur votre système, vous pouvez ne plus décrypter les fichiers EFS système, tous les mots de passe protégés DPAPI (ex. les mots de passe sauvegardés de Outlook) seront désactivés également.

Il y a un grand nombre de programmes sur le Net, qui affirme est capable de réinitialiser SYSKEY. Mais aucun d'eux ne fonctionnent correctement actuellement. La raison est que la réinitialisation de SYSKEY nécessite un grand nombre d'opérations supplémentaires pour éviter que le système soit endommagé.
Par exemple, vous avez besoin de remettre à zéro la ou les clés de session de Domaine, crypter à nouveau et réinitialiser les hachages, les secrets LSA, etc.
Reset Windows Password possède 2 algorithmes pour la réinitialisation SYSKEY. Si le premier échoue, un deuxième est exécuté. Après la réinitialisation de SYSKEY, tous les mots de passe des utilisateurs locaux seront effacés automatiquement.

Attention ! Après la réinitialisation SYSKEY sur une machine avec Windows 8, vous devrez changer le mot de passe pour tous les comptes LiveID par un nouveau non vide. Sinon, vous ne serez pas capable d'ouvrir une session avec un mot de passe vide.

3.13.9 Charger des pilotes complémentaires de disques dur



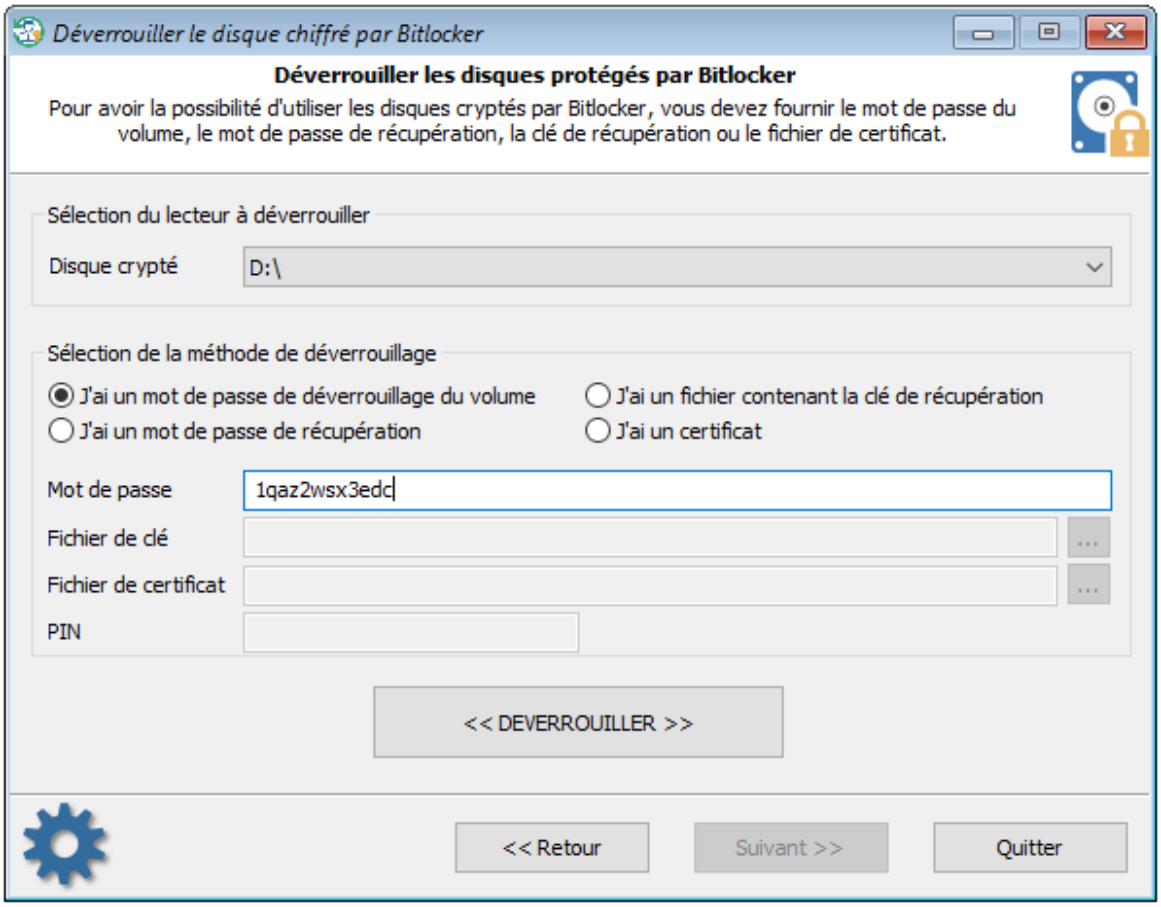
Si lors du démarrage, RWP n'a pas détecté un ou plusieurs disques dur, vous devez probablement installer un pilote pour le périphérique (disque). Dans la fenêtre principale, dans la liste des tâches, sélectionner "Charger un pilote IDE/SATA/SCSI/RAID" et poursuivez avec la boite de dialogue d'installation du pilote. Le logiciel est fourni avec plusieurs pilotes de contrôleurs de disques dur, tel que: ATI, Highpoint, Intel, Jmicron, Marvell, Nvidia, Silicion Image, Sis, Uli, Via, Vmware.

Ils sont tous stockés dans le répertoire **X:\Apps\Drivers**. Par exemple, si votre contrôleur HDD est basé sur un composant de chez Nvidia, chargé le fichier *.INF à partir du répertoire: X:\Apps\Drivers \Nvidia.

Normalement, lorsque vous achetez un nouvel ordinateur, il est fourni avec un CD de pilotes pour la carte mère et le(s) contrôleur(s) de disques dur. Vous pouvez, et souvent c'est fortement recommandé d'utiliser ce répertoire (X:\Apps\Drivers) pour installer les pilotes de périphériques manquants. Attention, les pilotes doivent être compatibles avec le système d'exploitation Windows 10 x64 !
Consultez la documentation de votre carte mère pour plus d'informations concernant l'installation de pilotes.

Dans "Reset Windows Password", les pilotes sont installés "en dynamique"; du coup, le redémarrage du système n'est pas nécessaire. A la fin de l'installation, les périphériques stockage trouvés doivent apparaître dans la liste. Une fois que le pilote est installé et le disque dur trouvé, vous pouvez revenir au menu principal de RWP et choisir une action à réaliser.

3.13.10 Déverrouiller les disques cryptés par Bitlocker



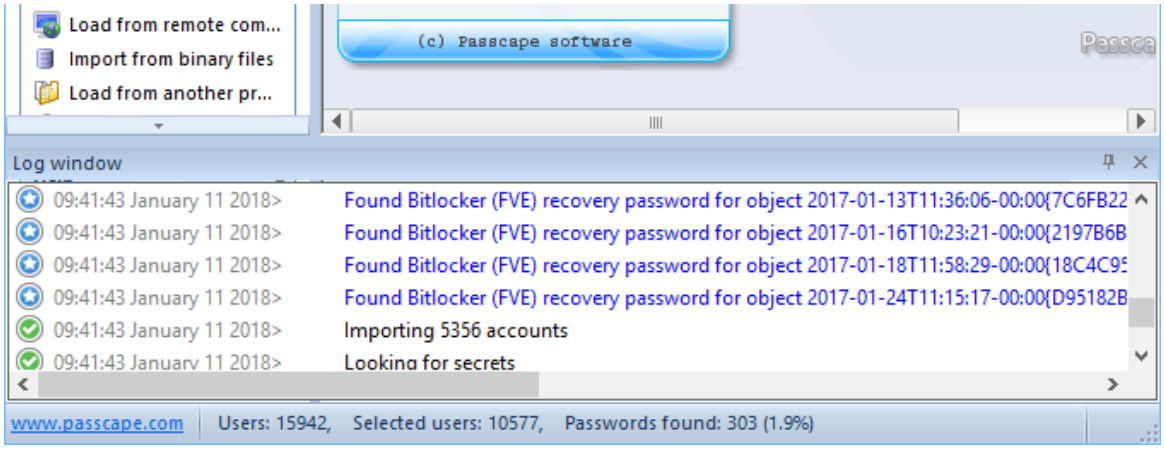
Bitlocker est un cryptage complet du disque ou de la partition. Il a commencé à être utilisé dans Windows Vista et à pour but de protéger vos données même si une personne a un accès physique à votre PC ou votre ordinateur portable.

BitLocker crypte tous les fichiers sur le disque, incluant ceux pour le démarrage du système d'exploitation. Ainsi le contenu est invisible au système. Pour pouvoir déverrouiller le disque et accéder à son contenu, vous devez utiliser une des méthodes de déblocage de la protection suivantes:

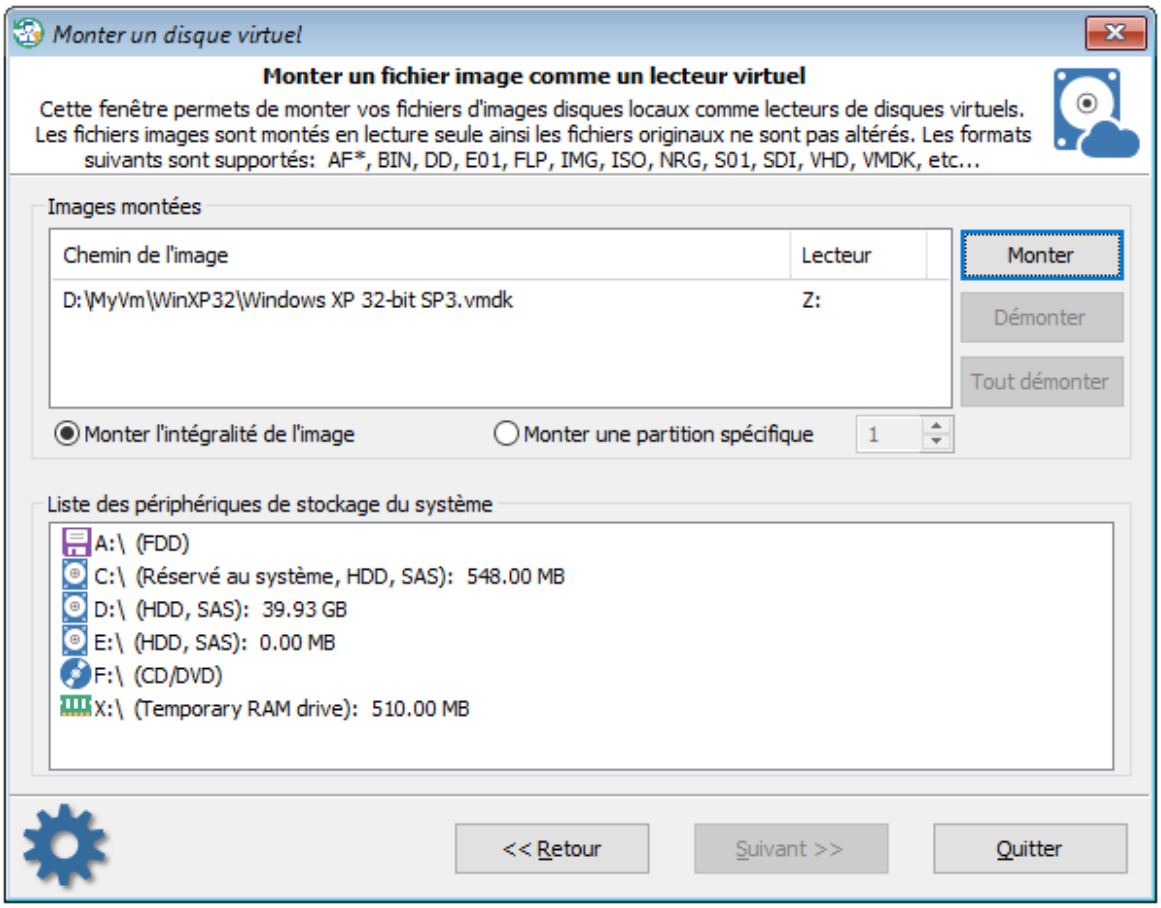
- Déverrouiller le disque avec le mot de passe de déverrouillage du volume
- Déverrouiller en utilisant le mot de passe de récupération (numérique)
- Déverrouiller en utilisant la clé de récupération externe
- Déverrouiller en utilisant le certificat Bitlocker

Sélectionner le lecteur crypté par Bitlocker suivi du type de déverrouillage que vous souhaitez utiliser et cliquer sur le bouton << *DÉVERROUILLER* >> pour le décrypter. L'opération prends quelques secondes.

Pour extraire les mots de passe de récupération Bitlocker de l'Active Directory, vous pouvez utiliser notre logiciel Windows Password Recovery.



3.13.11 Monter des disques virtuels



Cette fonctionnalité permets de monter une image disque dans le système comme disque virtuel.
Vous pouvez ensuite utiliser ce nouveau lecteur sous la lettre où est monté l'image.
Les images sont montées en lecture seule. Du coup, le fichier d'origine n'est pas altéré.
Les formats suivants sont supportés:
AF*, BIN, DD, E01, FLP, IMG, ISO, NRG, S01, SDI, VHD, VMDK et d'autres.

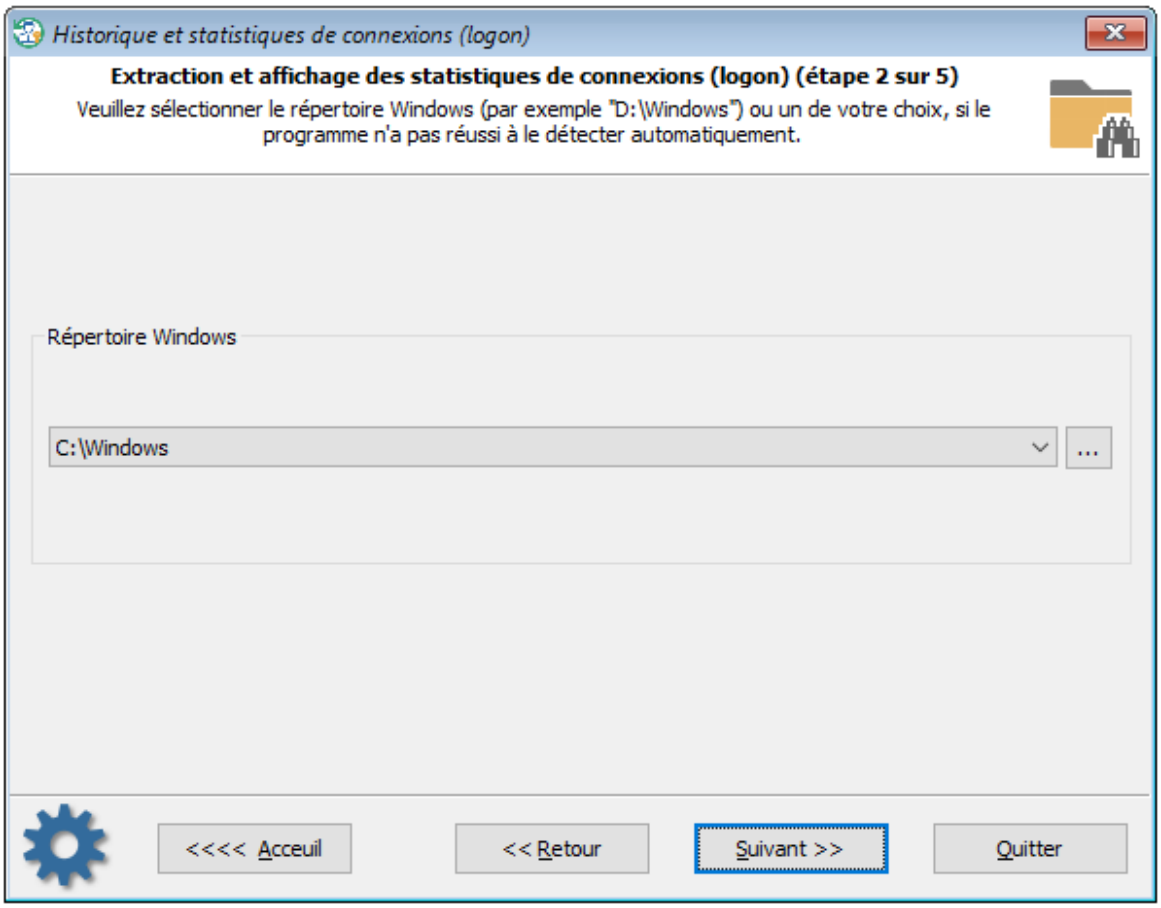
Soyez patient, monter certains types d'images peut prendre parfois jusqu'a plusieurs minutes pour aboutir.

3.14 FORENSIQUES - Outils d'investigations système

3.14.1 Historique et statisques de connexions (Logon)

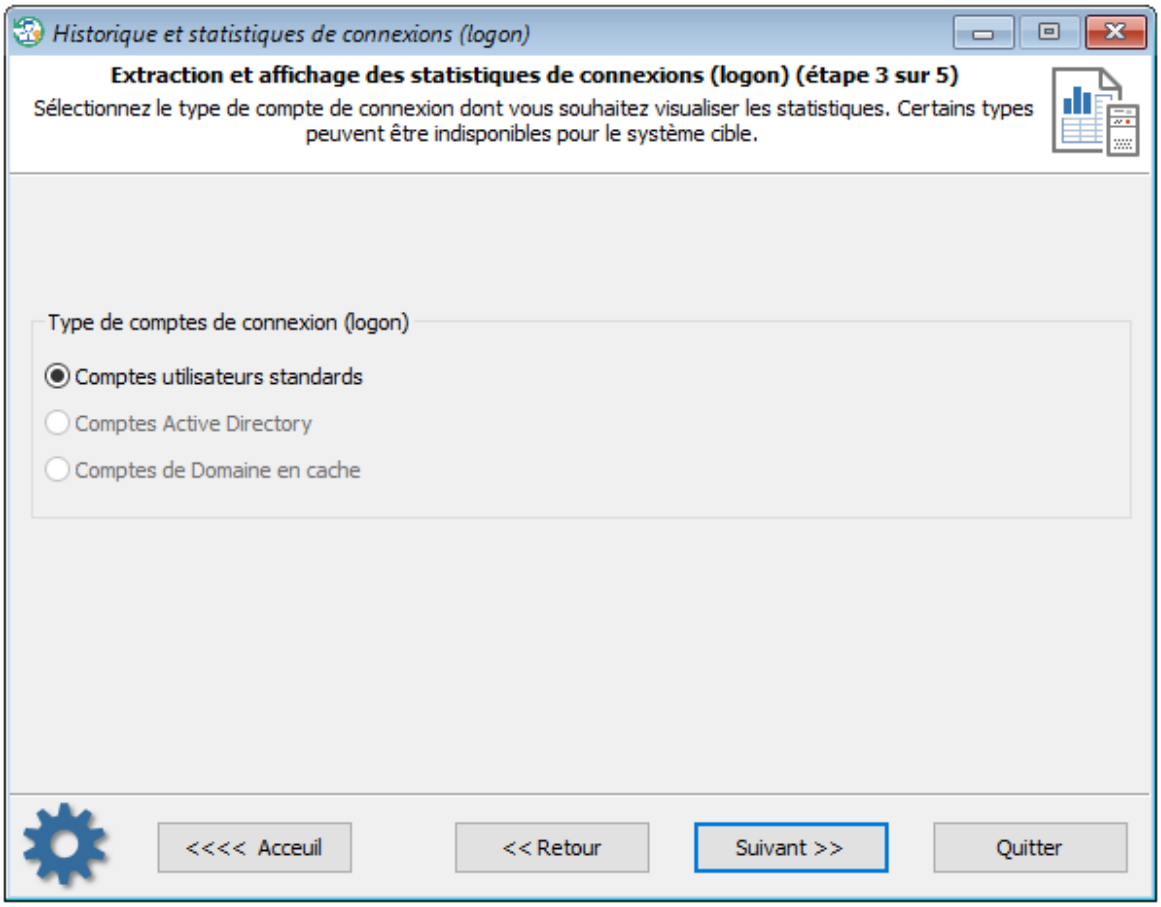
Cet outil permets d'afficher divers statistiques de connexions (logon) pour les utilisateurs classiques et de Domaines.

Sélection du répertoire Windows



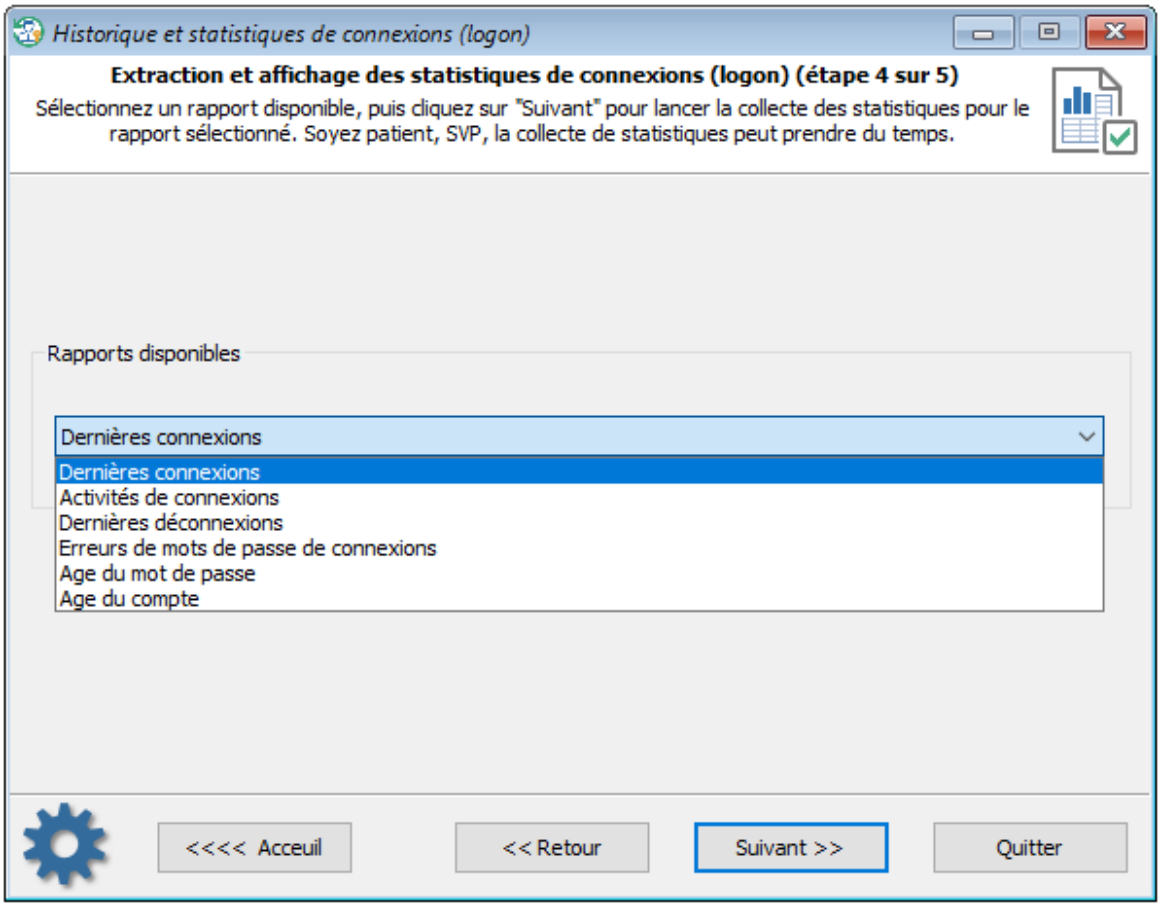
Tout d'abord, vous devez sélectionner le répertoire Windows du système cible ou le rechercher si le programme n'arrive pas à le détecter automatiquement.

Types de comptes de connexion



Une fois que le répertoire Windows est choisi, le programme essayera de détecter si le système contient un compte de Domaine (en compléments des comptes standards).
Sélectionner le type de compte dont vous voulez visualiser les statistiques et passez à l'étapes suivante en cliquant sur le bouton "Suivant >>".

Rapports disponibles

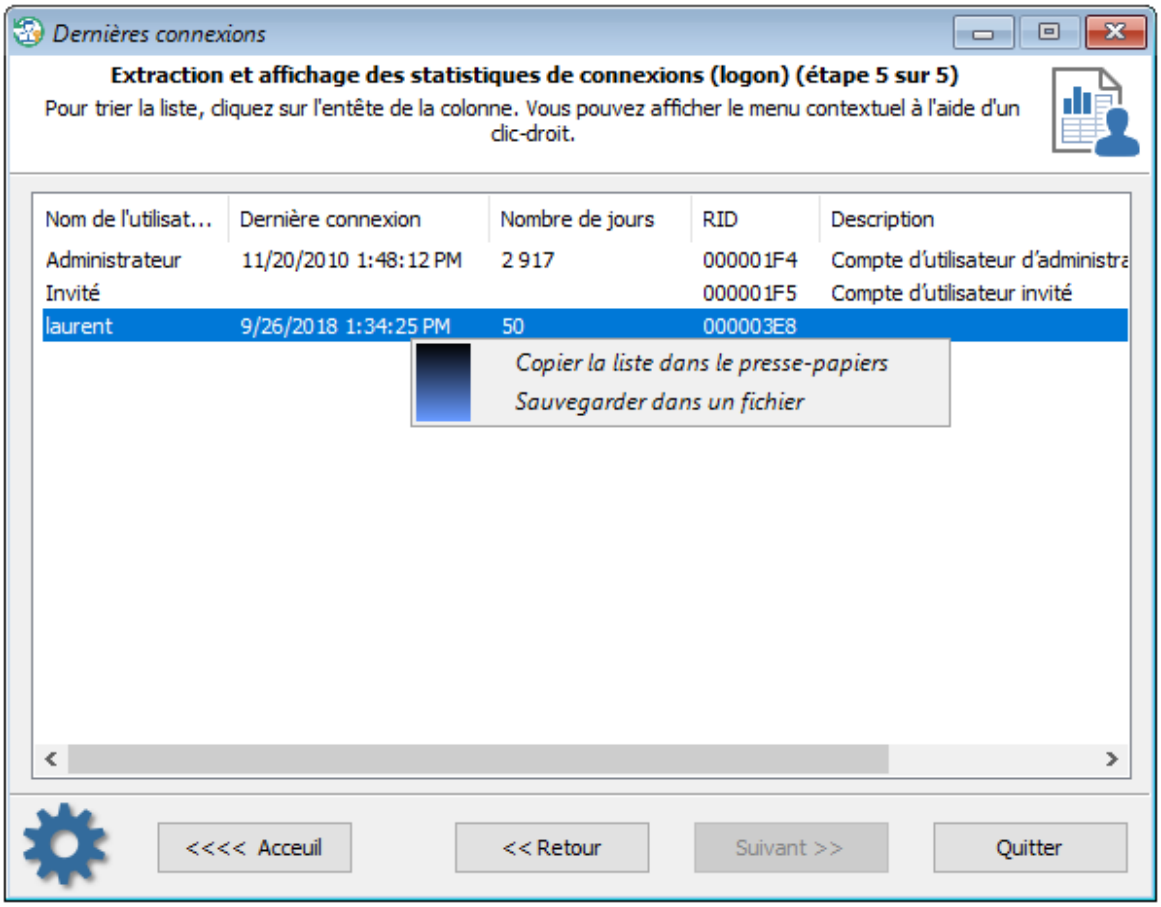


Vous pouvez, ici, choisir un des types de rapports suivants:

- Dernières connexions - affiche la date de la dernière connexion des utilisateurs.
- Activités de connexions - affiche les utilisateurs les plus actifs.
- Dernières déconnexions - malheuresement, la plupart des versions de Windows ont stoppé la sauvegarde de la date de déconnexion. Cependant, certaines informations liées sont disponibles dans "Activités récentes utilisateur".
- Erreurs de mots de passe de connexions - Date et heure du dernier échec d'un utilisateur qui a essayé d'ouvrir son compte avec un mot de passe erroné.
- Age du mot de passe - Date et heure lorsque l'utilisateur a changé son mot de passe.
- Age du compte - lorsque le compte a été créé pour la première fois.

Certains de ces rapports sont indisponibles pour les comptes de Domaine en cache.

Statistiques de connexions (Logon)

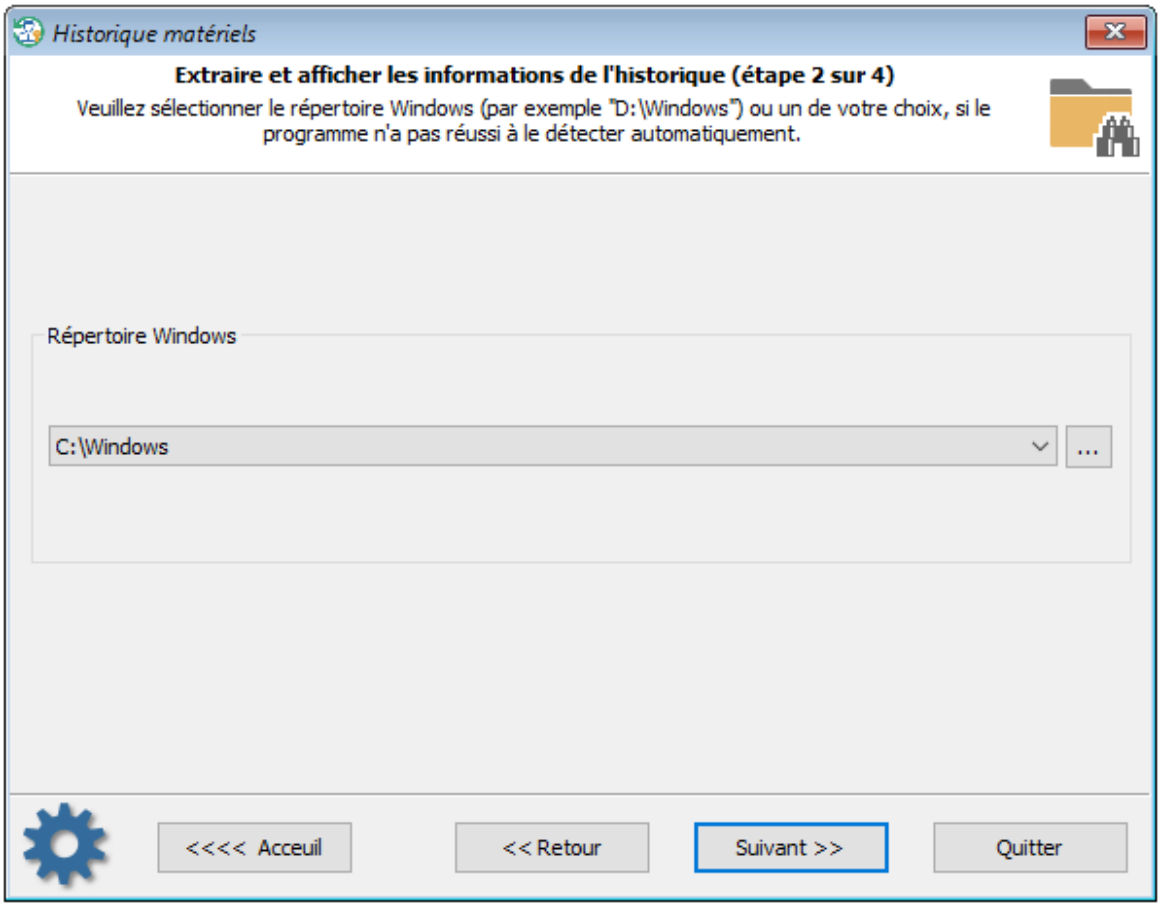


Vous pouvez copier les statistiques dans le Presse-papiers ou les enregistrés dans un fichier, à l'aide du menu contextuel (clic droit).

3.14.2 Historique matériels

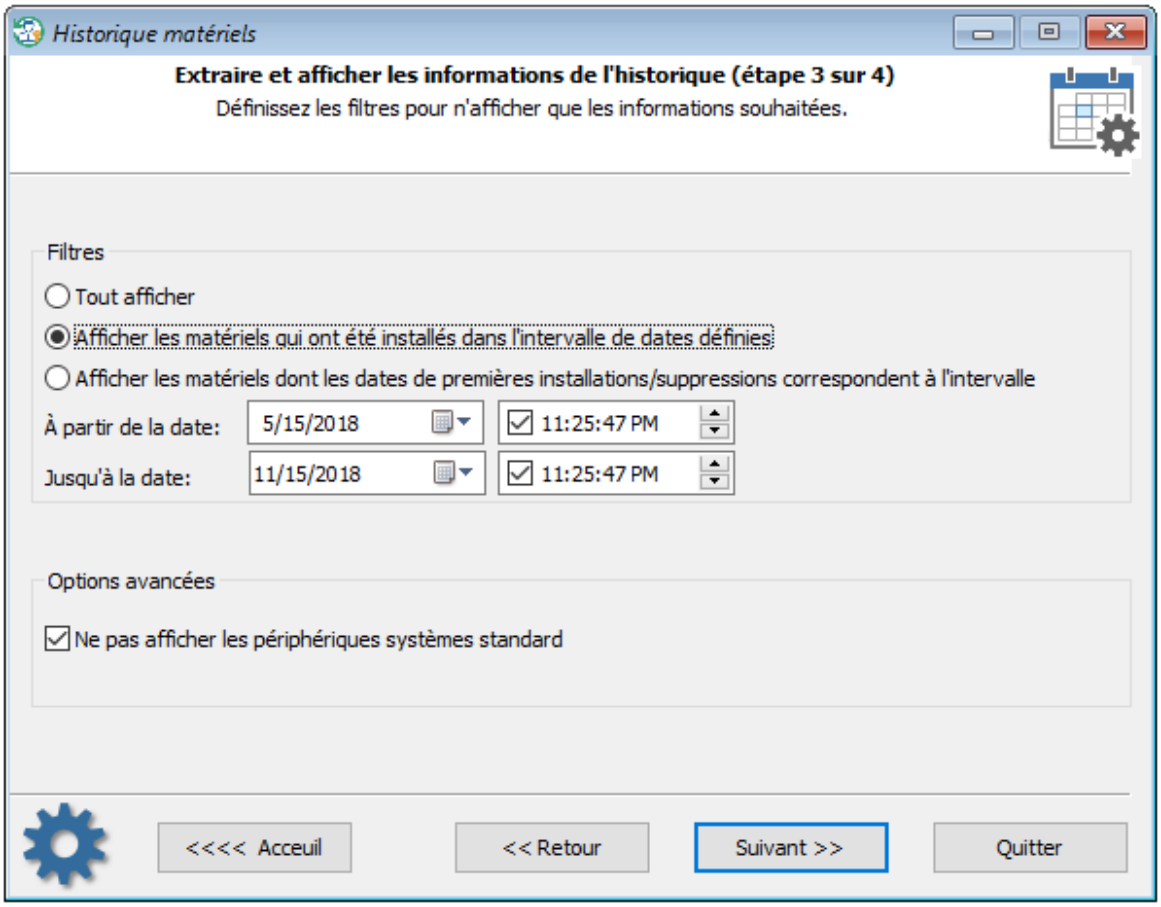
L'historique matériel liste tous les matériels de l'OS cible et les trie par ordre d'installation ou de date d'arrivée/suppression.

Sélection du répertoire Windows



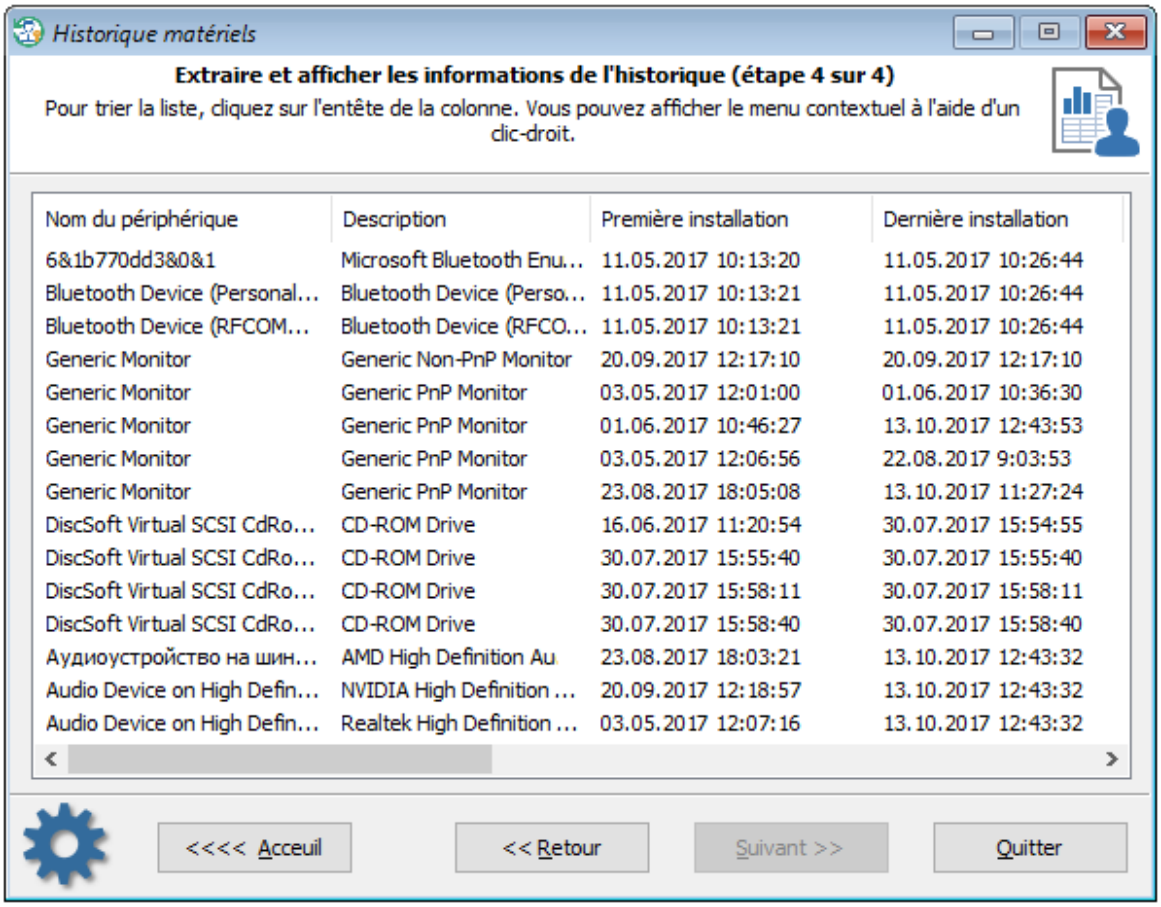
Tout d'abord, vous devez sélectionner le répertoire Windows du système cible ou le rechercher si le programme n'arrive pas à le détecter automatiquement.

Sélection des filtres



Paramétrez les filtres pour exclure les éléments inutiles. Vous pouvez définir comme filtre, uniquement les matériels qui ont été installés ou qui sont arrivés/retirés à l'heure et la date que définie par le filtre.

Informations de l'historique matériel

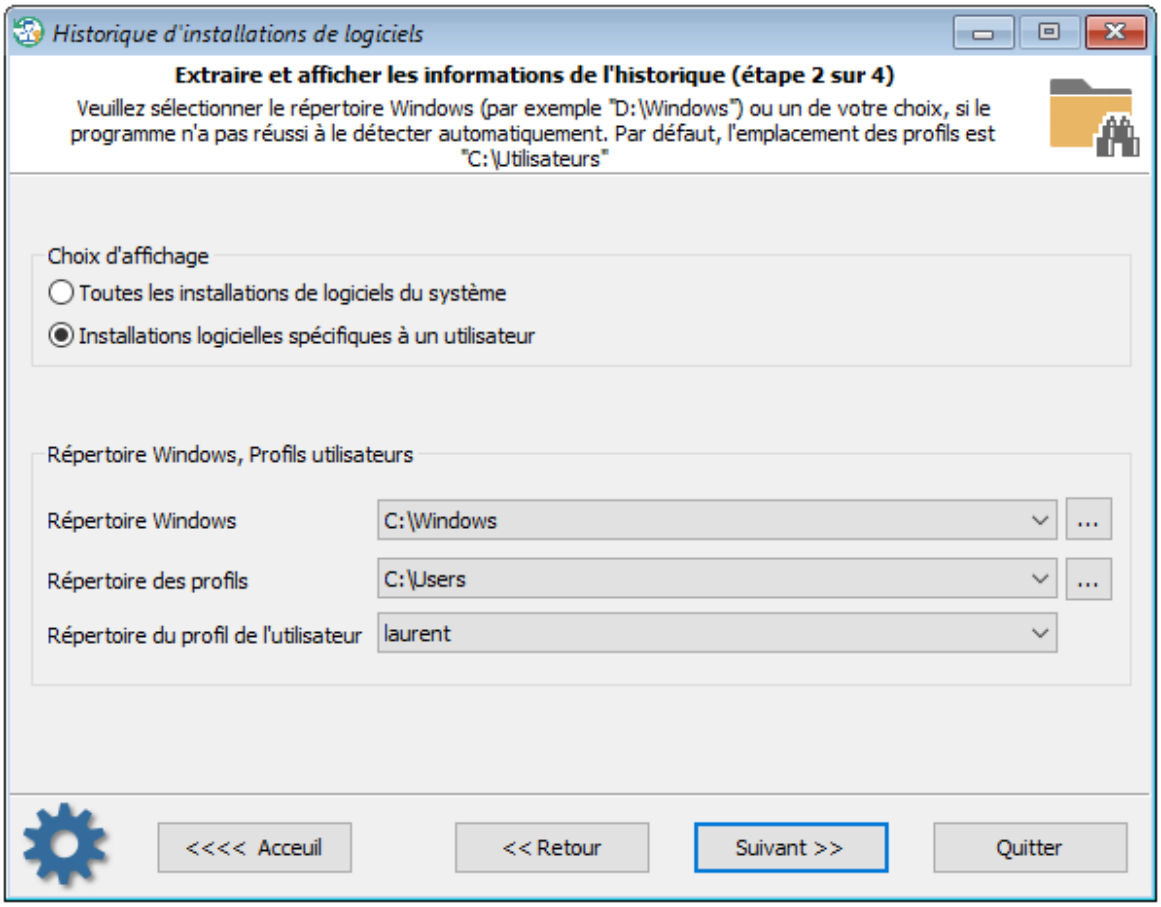


Pour trier la liste, cliquez sur une des entêtes de colonnes.

3.14.3 Historique d'installations de logiciels

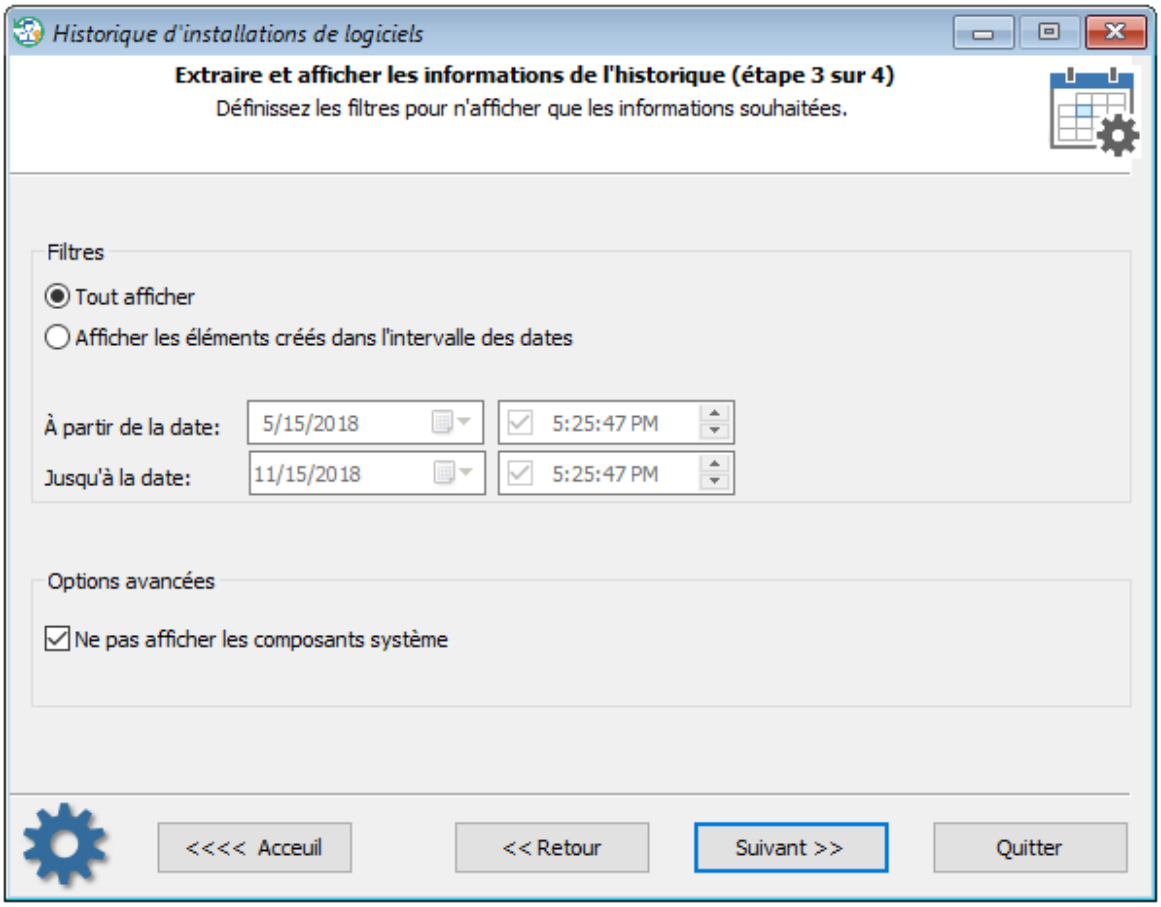
L'historique d'installations de logiciels affiche tous les programmes qui ont été installés dans l'OS cible.

Sélection du type d'installations logicielles



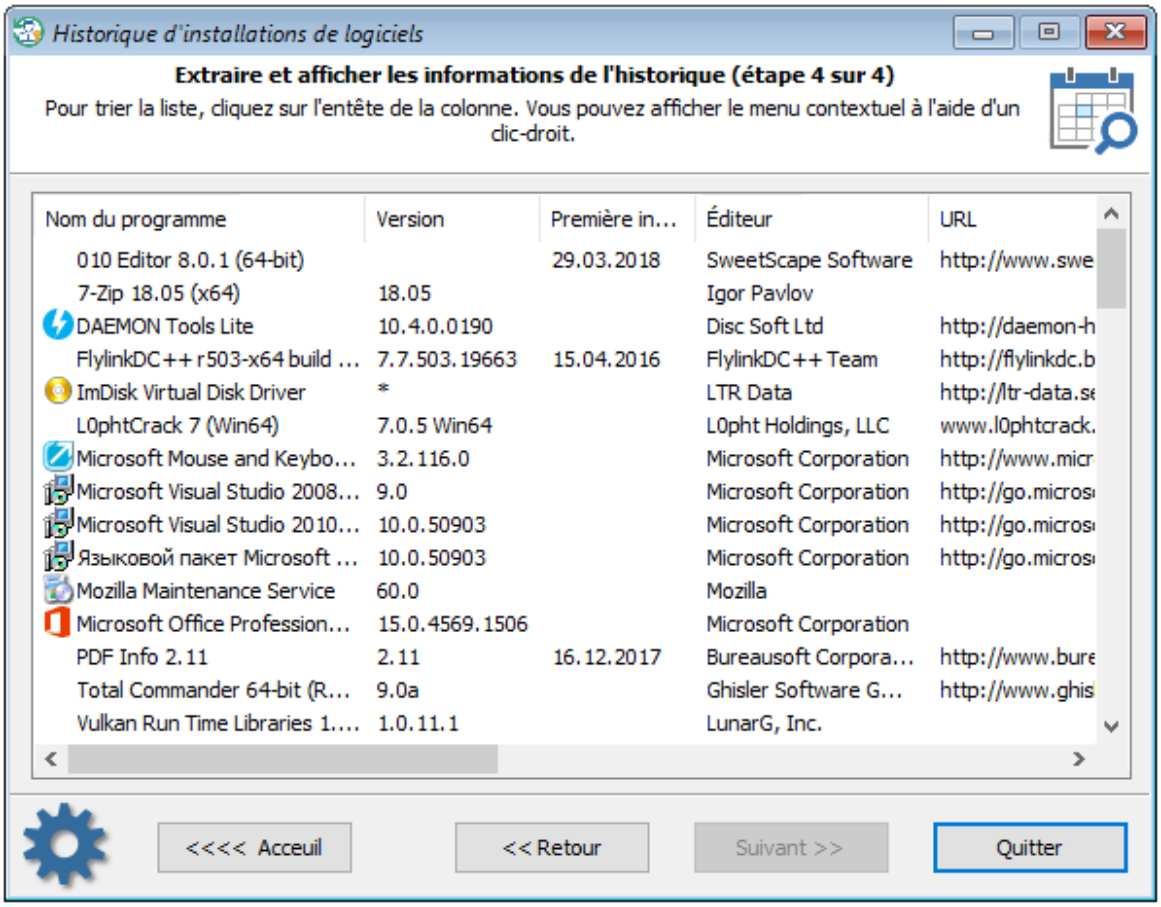
Sélectionnez quel type d'installations logicielles vous voulez afficher. Cela peut être, soit des installations (programmes installés pour un compte d'un utilisateur en particuler) or ou pour des installations disponible pour tous le système (programmes disponibles pour tous les utilisateurs).

Filtres d'affichage



Vous pouvez demander au programme d'afficher tous les éléments ou uniquement que ceux qui ont été créés dans un intervalle de dates. L'option complémentaire permets d'exclure les composants systèmes, comme les mises à jour systèmes, etc.

Installations logicielles

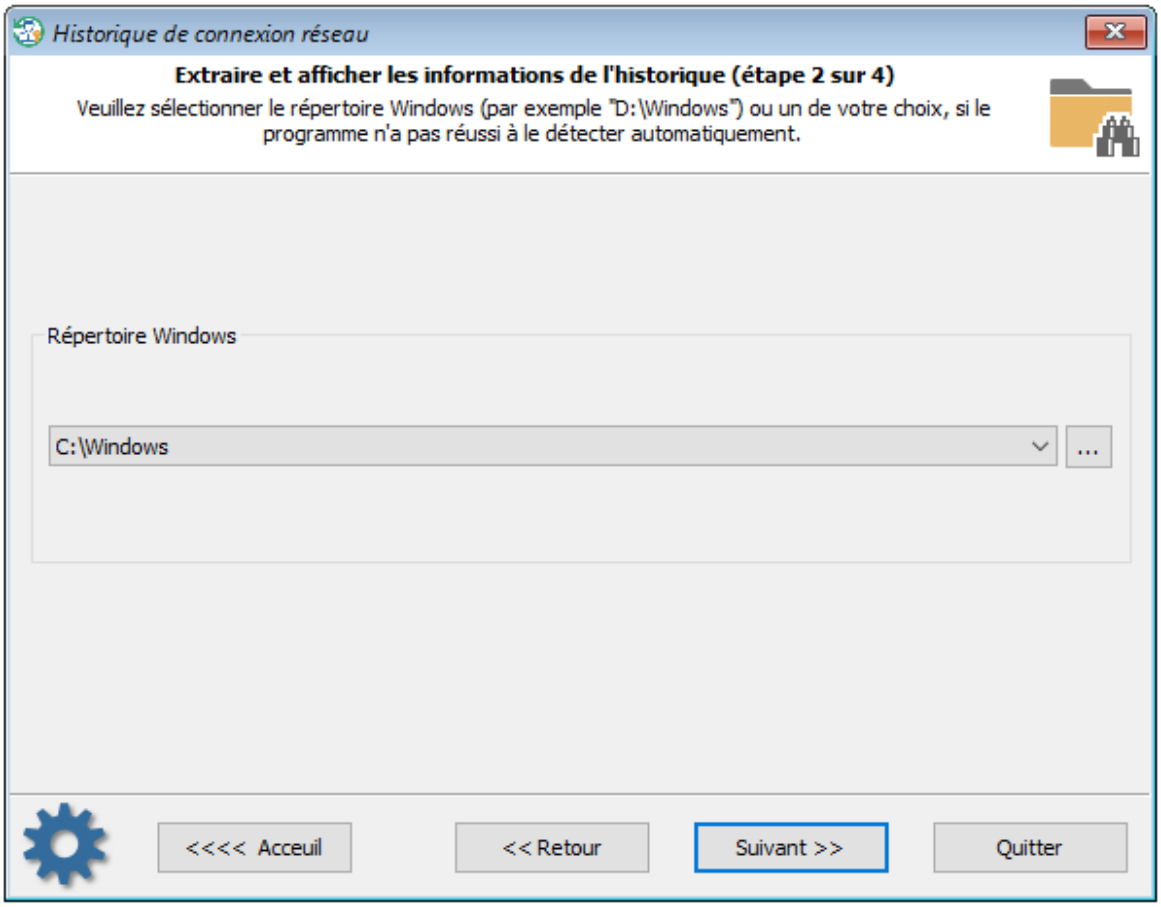


Pour trier la liste, cliquez sur une des entête de colonnes.

3.14.4 Historique de connexions réseau

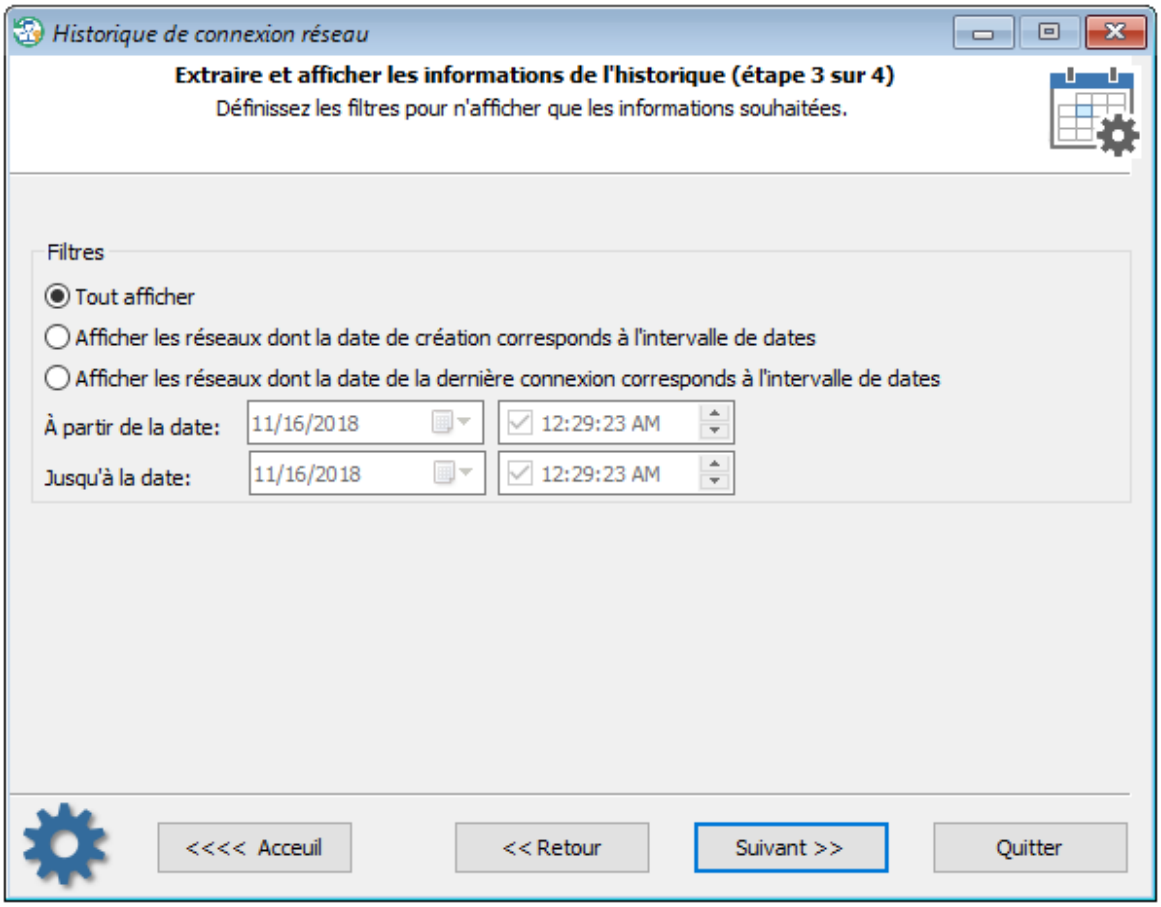
L'historique de connexions réseau affiche tous les réseaux disponibles ainsi que leurs dates d'installations et de la dernière connexion.

Sélection du répertoire Windows



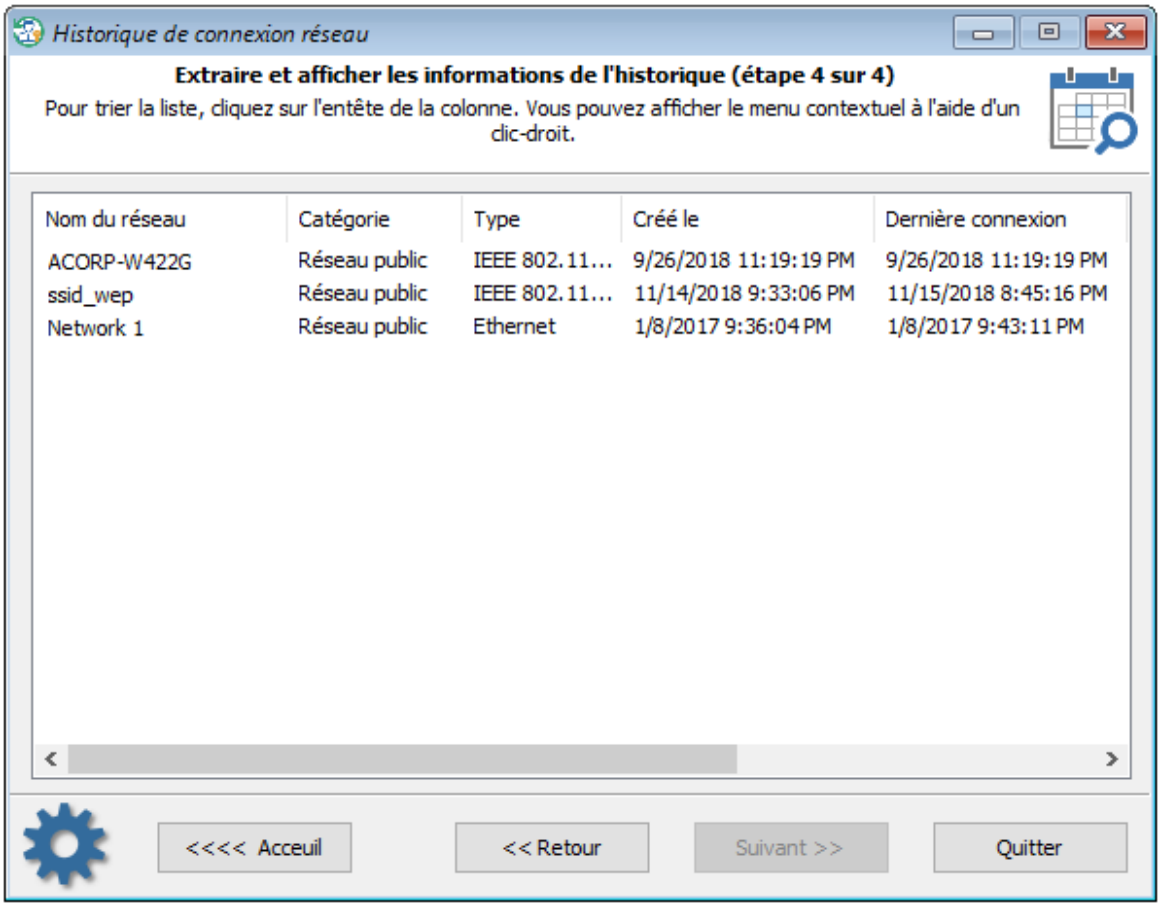
Tout d'abord, vous devez sélectionner le répertoire Windows du système cible ou le rechercher si le programme n'arrive pas à le détecter automatiquement.

Sélection des filtres



Définissez les filtres pour afficher uniquement les réseaux qui vous intéressent

Historique de connexions réseau

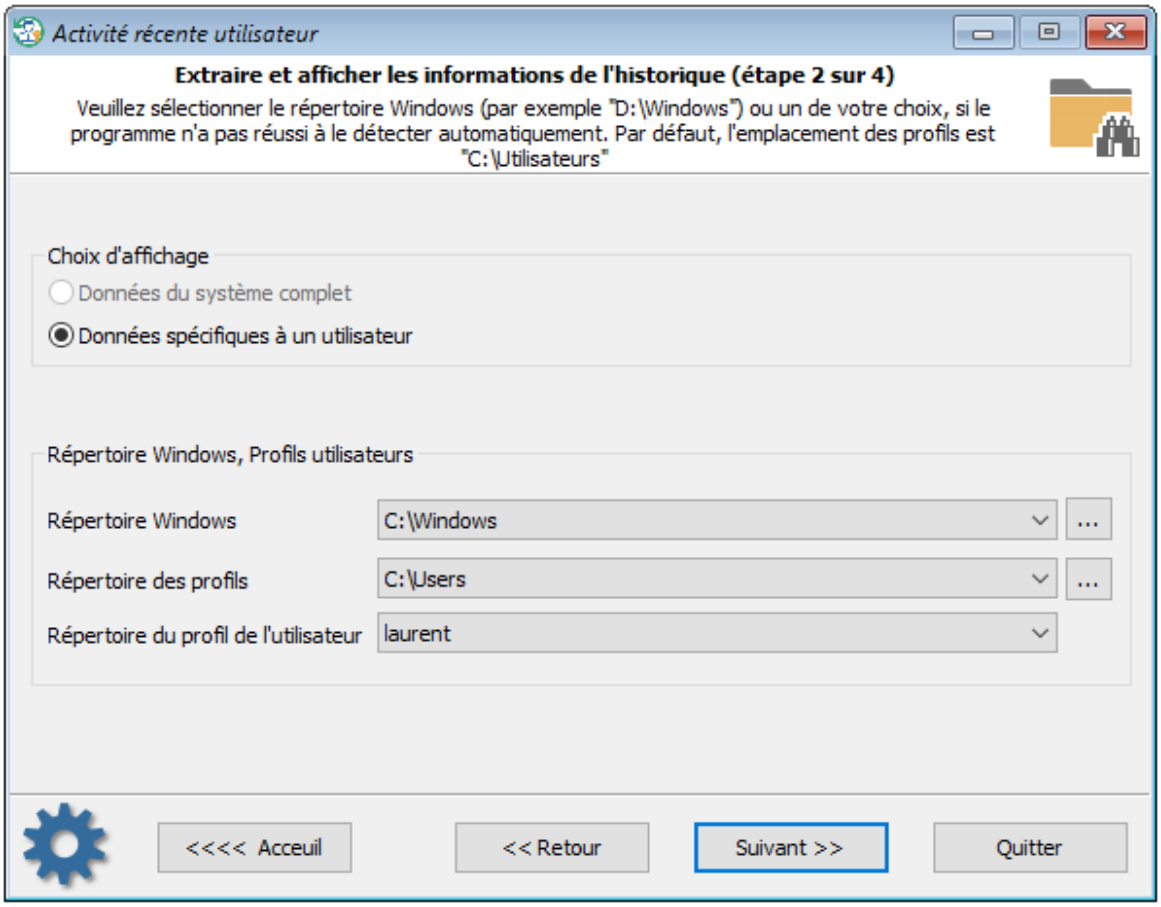


Les réseaux extraits contiennent normalement la date lorsqu'ils ont été créés et de la dernière connexion.
Pour trier la liste, cliquez sur l'entête de la colonne.

3.14.5 Activités récentes utilisateur

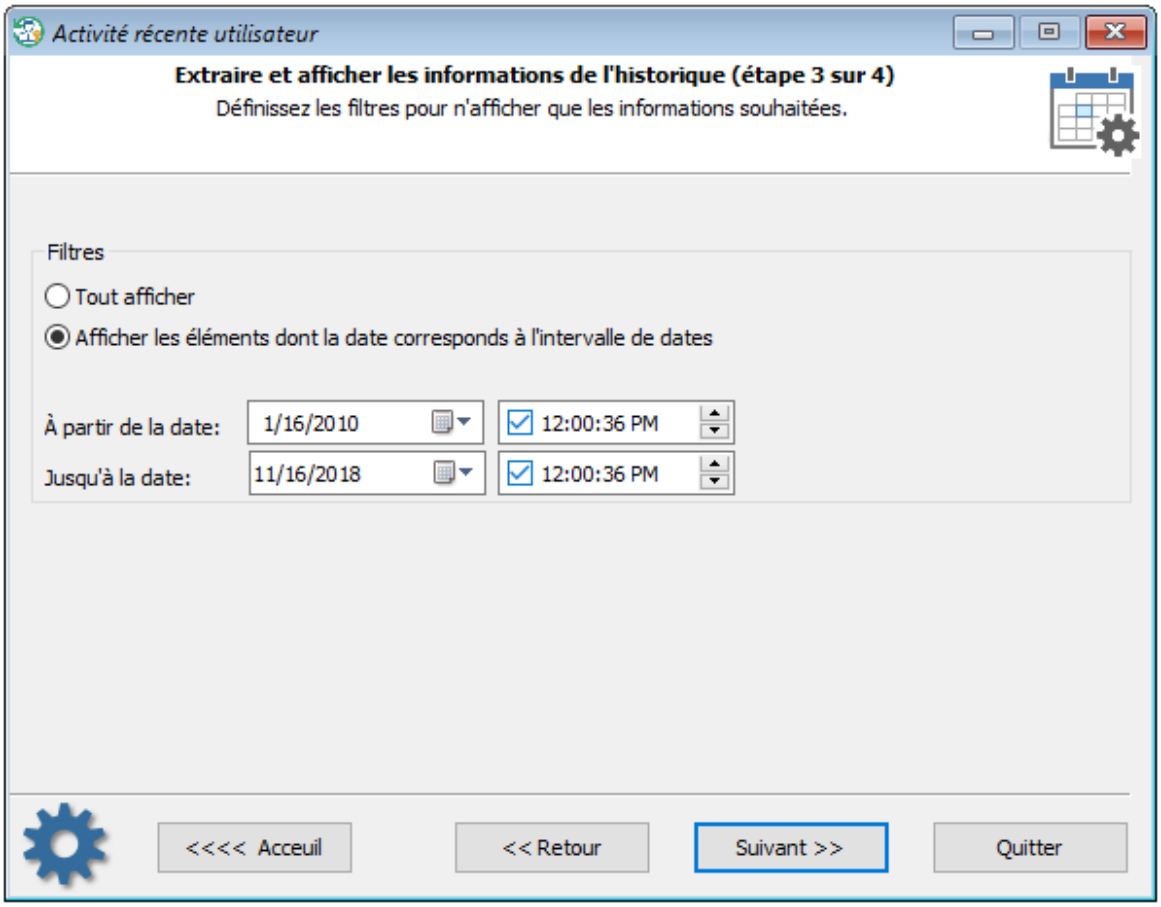
Ce outil collecte toutes les informations concernant l'activité récente d'un utilisateur sur cet ordinateur.

Sélection du type d'activité



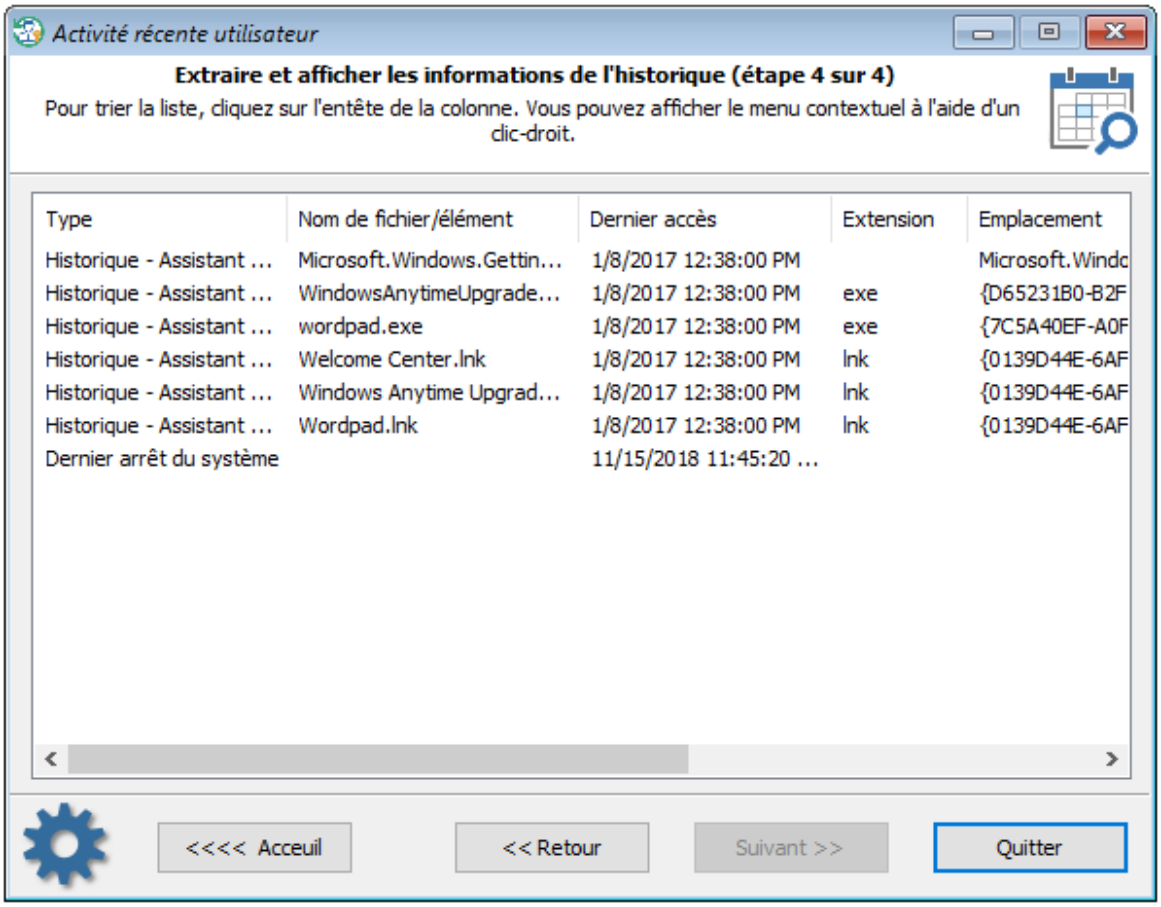
En premier, choisissez si vous voulez voir les données d'un utilisateur en particulier ou tous le système.

Sélection des filtres



Puis indiquez si toutes les éléments doivent être affichés ou seulement ceux qui sont dans l'intervalle de temps.

Affichage de l'activité récente d'un utilisateur



Soyez patient, la collecte des statistiques peut prendre du temps.
Pour masquer le(s) élément(s) a exclure, faites un clic droit sur la liste pour ouvrir le menu contextuel.

La version actuelle du programme supporte les informations suivantes (certains éléments ne sont pas disponibles dans les anciens OS):

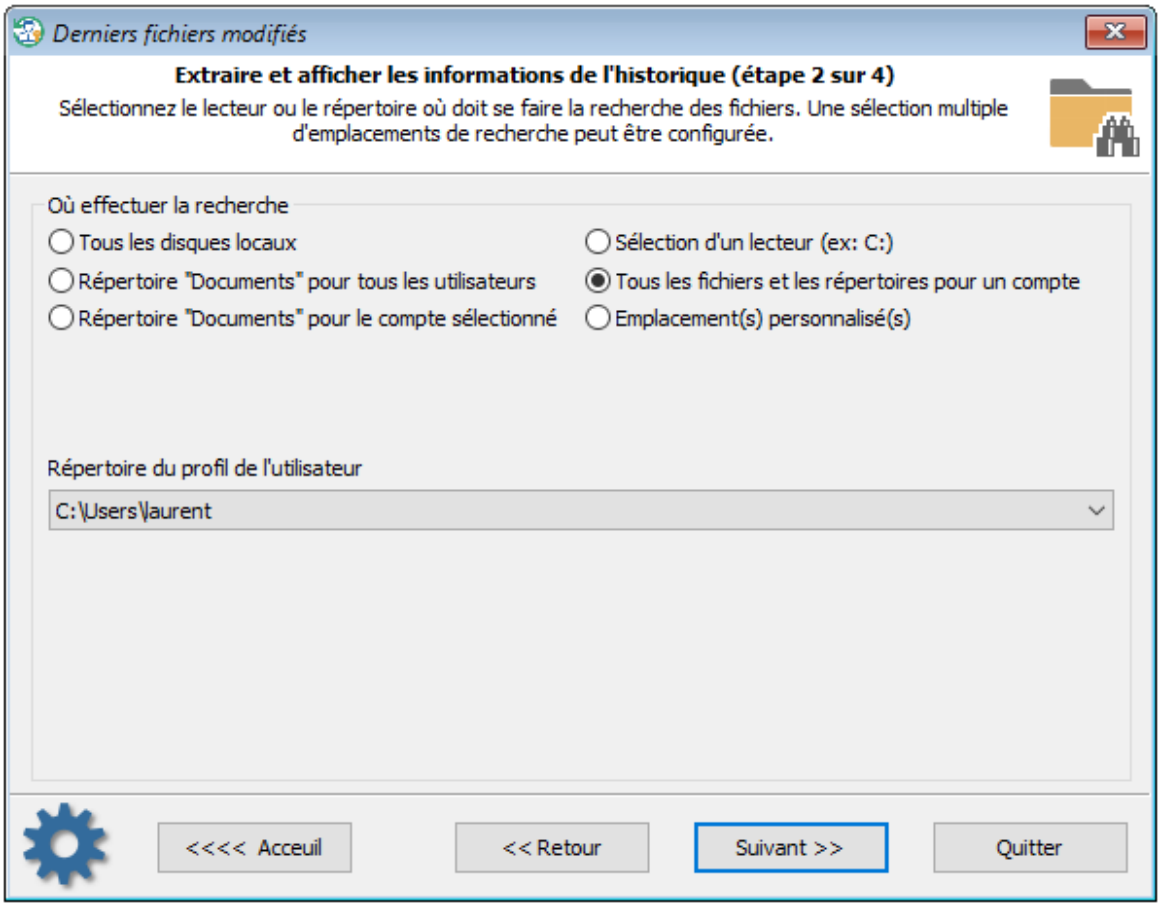
- Derniers éléments dans les dialogues d'ouverture/enregistrement de fichiers
- Les tâches exécutées
- Les lecteurs réseaux connectés
- Les réseaux récemment trouvés
- Les fichiers/répertoires trouvés récemment
- Les fichiers d'applets Windows récents
- La dernière clé de registre ouverte
- Les documents ouverts récemment
- Les documents MS Office ouverts récemment
- Les comptes Outlook et connexions récentes
- Les applications exécutées récemment
- Les éléments d'applications récents
- Les connexions RDP récentes
- Les URL d'Internet Explorer saisies récemment
- Les chemins saisis dans l'explorateur
- L'historique de recherche de l'explorateur
- Les éléments de l'assistant utilisateur de l'explorateur
- L'activité en arrière plan récente
- L'activité du Bureau récente
- Les connexions sans-fil

- L'activité Bluetooth
- Les périphériques portable récents
- La date d'installation de Windows
- La dernière date d'arrêt du système

3.14.6 Derniers fichiers modifiés

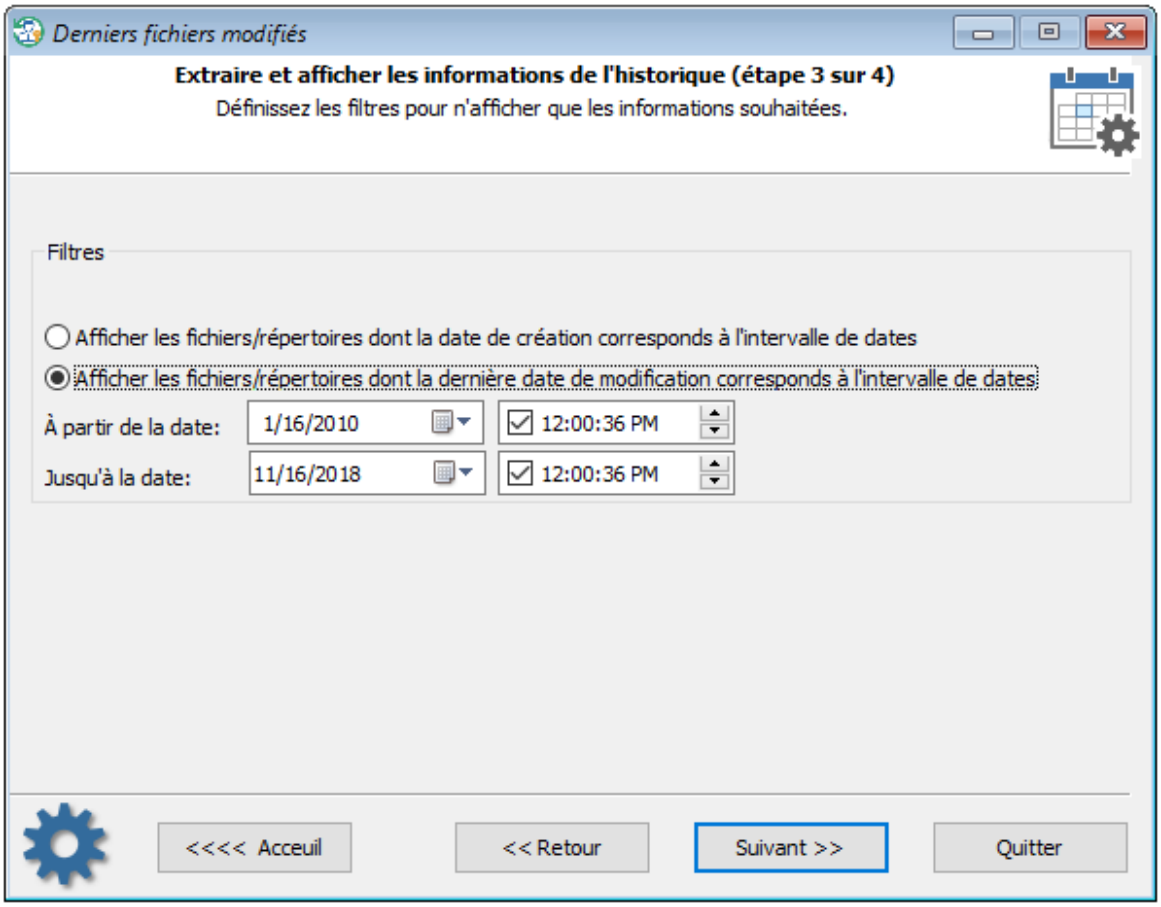
Parfois, Il est utile de savoir quel sont les fichiers ou répertoires qui ont été créés ou modifiés dans un interval de temps. Cet outil est conçu dans ce but.
Nous avons essayé de le faire le plus simple possible. Tout ce dont vous avez besoin est paramétrer l'emplacement de la recherche et l'intervalle de temps pour les fichiers/répertoires recherchés.

Sélection l'emplacement de recherche



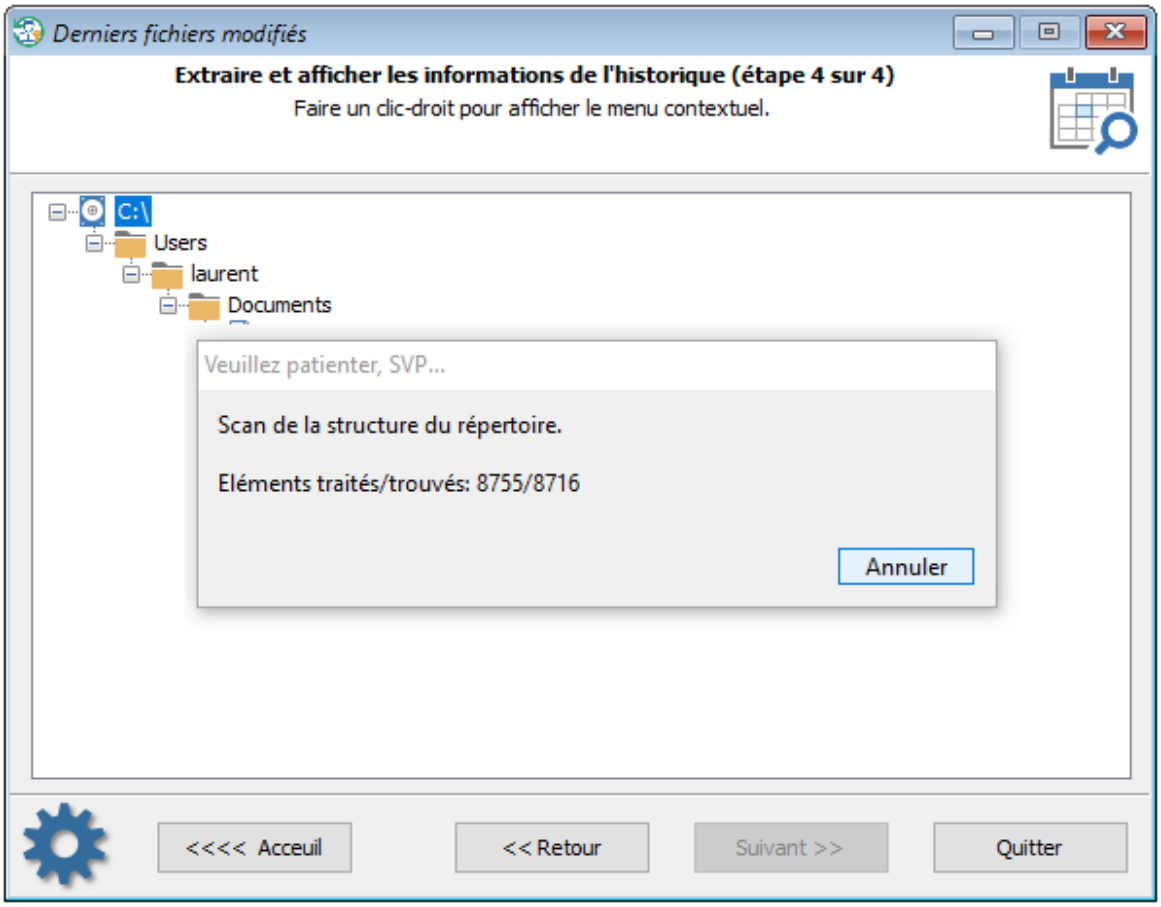
Indiquez au programme le point de départ des fichiers a rechercher, sélectionnez une des valeurs prédéfinies comme le répertoire "Documents" pour un utilisateur en particulier, le profil complet, etc. Vous pouvez aussi choisir un ou plusieurs emplacements de recherches personnalisés en définissant un chemin ou un lecteur.

Choix de l'intervalle de dates/temps



Indiquez ici si vous avez besoin de rechercher des fichiers/répertoires à partir d'une certaine date de création/modification. Vous pouvez définir un intervalle en secondes ou le désactiver complètement.

Affichage des derniers fichiers modifiés



Soyez patient, la recherche peut prendre du temps.

3.14.7 Derniers répertoires modifiés

Cet outil fait exactement la même chose que le précédent excepté qu'il recherche les répertoires au lieu des fichiers.
Veuillez vous référer, à l'outil de recherche de fichiers pour plus d'informations.

Licence et Enregistrement du logiciel

4 Licence et Enregistrement du logiciel

4.1 Contrat de licence

==========
SOFTWARE LICENSE AGREEMENT
==========

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

All copyrights to SOFTWARE are exclusively owned by Passcape Software.

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

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

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

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

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

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

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

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

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

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

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our SOFTWARE or have permission from the legitimate owner to perform these acts. Any illegal use of our SOFTWARE will

be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

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

4.2 Enregistrement du logiciel

Le logiciel est disponible en trois éditions: 'Light', 'Standard' et 'Advanced'. Le détail des fonctionnalités est consultable ici.

Vous pouvez commander une licence pour la version complète de Reset Windows Password, à un tarif en fonction de l'édition choisie:

- 'Light' pour un prix de 45$ (licence et usage personnel)
- 'Standard' pour un prix de 145$ (licence et usage personnel)
- 'Advanced' pour un prix de 345$ (licence et usage professionnelle).

Les informations détaillées pour la commande du logiciel, et les différents moyens de paiement sont disponible en ligne sur la page de commande de WPR. Les commandes en ligne sont traitées en quelques minutes, 24h/24 et 7 jours/7. Les pages de commande sont hébergés sur un serveur sécurisé, vous assurant que les informations restent confidentielles.

Une fois que votre commande a été traitée, vous recevrez un message par e-mail contenant le lien de téléchargement de la version complète du logiciel.

Si vous avez fait un paiement pour le logiciel et que vous n'avez pas reçu le l'e-mail contenant le lien dans un délai raisonnable, merci de nous en informer.

Important: lors de la rédaction du formulaire de commande, s'il vous plaît, vérifiez deux fois que votre adresse e-mail est correcte. Si cela n'était pas le cas, nous serions incapable de vous envoyer à nouveau l'e-mail contenant le lien de téléchargement du logiciel.

Pour compléter le processus d'enregistrement, vous devez télécharger le programme en utilisant le lien que vous avez reçu dans l'e-mail. et suivre les informations pour créer un disque amorçable.

4.3 Limitations de version non enregistrée (démo)

La version non enregistrée de **Reset Windows Password** affiche seulement les 3 premiers caractères des mots de passe récupérés et possède certaines fonctionnalités limitées.
Seul le dump de hachages et la sauvegarde de mots de passe fonctionnent sans limitations.
Une version enregistrée ne possède aucune limitation.

4.4 Versions du logiciel

Reset Windows Password existe en trois éditions: Light, Standard et Advanced.
Le tableau, ci-dessous, affiche la liste détaillée des fonctionnalités et de compatibilités:

FONCTIONNALITÉS	Light	Standard	Advanced
Support de stations de travail sous Windows 2000/XP/ Vista/7/8/10	+	+	+
Support Windows serveur NT/2000/2003/2008/2012/2019	+	+	+
Support de Windows 64-bits	+	+	+
Support de Windows Non-US	+	+	+
Support des mots de passe internationaux	+	+	+
Pilotes complémentaires de périphériques de stockages	+	+	+
Détection de systèmes d'exploitation multiples	+	+	+
Garantie d'une disponibilité du téléchargement étendue	+	+	+
Garantie de remboursement de 14 jours de l'achat d'une licence	+	+	+
Type de licences (utilisation)	Personnelle	Personnelle	Pro.
Support de tous les types de comptes Windows, incluant Live ID, les comptes Microsoft, etc.	+	+	+
Création d'un support CD/DVD de réinitialisation de mots de passe	+	+	+
Création d'un support USB de réinitialisation de mots de passe	+	+	+
Création d'un disque dur de réinitialisation de mots de passe	+	+	+
Support de démarrage pour les ordinateurs à base d'UEFI	+	+	+
Réinitialisation du mot de passe Administrateur local	+	+	+
Modification du mot de passe Administrateur	+	+	+
Déverrouillage du compte Administrateur local désactivé, verrouillé ou expiré (1)	+	+	+
Réinitialisation du mot de passe Administrateur de Domaine	-	-	+
Modification du mot de passe Administrateur de Domaine	-	-	+
Déverrouillage du compte Administrateur de Domaine désactivé, verrouillé ou expiré (1)	-	-	+
Modification des propriétés étendues d'un compte local	+	+	+
Modification des propriétés étendues des comptes d'Active Directory	-	-	+
Réinitialisation du mot de passe de comptes standards (SAM)	+	+	+
Modification des mots de passe de comptes standards (SAM)	+	+	+
Déverrouillage d'un compte SAM désactivé, verrouillé ou expiré (1)	+	+	+
Décryptage des questions et réponses secrètes pour l'OS Windows 10	+	+	+
Réinitialisation du mot de passe de comptes d'Active Directory	-	-	+
Modification de mots de passe de comptes d'Active Directory	-	-	+

FONCTIONNALITÉS	Light	Standard	Advanced
Déverrouillage des comptes d'Active Directory désactivés, verrouillés ou expirés [1]	-	-	+
Réinitialisation/modification du mot de passe de compte DSRM [2]	-	-	+
Chargement et installation instantanée de pilotes IDE/SATA/ SCSI/RAID	+	+	+
Annulation des modifications (mots de passe précédemment modifiés)	+	+	+
Support du cryptage de SYSKEY	+	+	+
Support du décryptage du mot de passe de démarrage SYSKEY	+	+	+
Support du décryptage de la disquette SYSKEY	+	+	+
Affichage des astuces de mots de passe (si elle existe)	+	+	+
Dump des hachages de mots de passe LM/NTLM pour les comptes standards (SAM)	+	+	+
Dump de l'historique des hachages de mots de passe	-	+	+
Dump des identifiants de connexion de Domaine en cache (MSCACHE)	-	+	+
Dump des hachages de mots de passe pour les comptes d'Active Directory	-	-	+
Récupération immédiate du mot de passe pour certains comptes d'utilisateurs d'Active Directory [3]	-	-	+
Récupération immédiate du mot de passe pour certains comptes d'utilisateurs SAM	-	+	+
Recherche pour les mots de passe simples	-	+	+
Analyse à l'aide d'un dictionnaire primitif	-	+	+
Analyse à l'aide de dictionnaires avancés [4]	-	-	+
Attaque primitive par force-brute contre les mots de passe d'utilisateurs	-	+	+
Récupération de mots de passe à l'aide d'une analyse à base d'Intelligence Artificielle	-	+	+
Suppression de l'historique des hachages de mots de passe hors comptes standards (SAM)	-	+	+
Suppression de l'historique des hachages de mots de passe hors comptes d'Active Directory	-	+	+
Suppression des mots de passe de Domaine en cache	-	+	+
Suppression des mots de passe d'identification (logon) en cache	-	+	+
Suppression de l'information de réinitialisation du mot de passe	-	+	+
Suppression des indices de mots de passe	-	+	+
Réinitialisation de la sécurité SYSKEY (avec les mots de passe d'utilisateur qui peuvent être crypté à nouveau)	-	+	+
Recherche du mot de passe de démarrage SYSKEY	-	+	+
Récupération instantanée du mot de passe en clair pour les comptes avec un compte avec un mot de passe de type "Image"	-	+	+
Récupération instantanée du mot de passe en clair pour les comptes avec une identification (logon) biométrique [5]	-	+	+

FONCTIONNALITÉS	Light	Standard	Advanced
Récupération de codes PIN	-	+	+
Montage de disques virtuels	+	+	+
Recherche des clés de licence et de numéros de série de logiciels	-	+	+
Conversion d'un Microsoft Live ID en compte local	+	+	+
Sauvegarde des mots de passe, de la base de registre et de l'Active Directory	+	+	+
Recherche et décryptage des mots de passe de navigateurs Internet	-	+	+
Recherche et décryptage des mots de passe pour les clients les plus populaires d'e-mails	-	+	+
Recherche et décryptage des différents mots de passe réseau	-	+	+
Créer des nouveaux comptes SAM	-	+	+
Déverrouiller les disques cryptés par Bitlocker	+	+	+
Éditer la stratégie de sécurité locales des mots de passe	-	+	+
Éditer la stratégie de sécurité de Domaine des mots de passe	-	-	+
Décrypter les identifiants de connexions Windows Hello	-	+	+
Logon history and statistics (6)	+	+	+
Hardware history (7)	+	+	+
Software history (7)	+	+	+
Network history (7)	+	+	+
Recent user activity (6)	+	+	+
Last modified files	-	+	+
Last modified directories	-	+	+
Prix	$45	$145	$345

Notes:
- Fonctionnalité exclue
+ Fonctionnalité incluse
(1) Si le compte est verrouillé, désactivé ou expiré.
(2) Directory Services Restore Mode (Mode de restauration des Services annuaire).
(3) Si l'option de Cryptage Réversible est activée. Vous pouvez trouver cette option dans votre stratégie de groupes des mots de passe de Domaine.
(4) En utilisant des dictionnaires Arabe, Chinois, Anglais, Français, Allemand, Portugais, Russe et Espagnol.
(5) Pas pour tous les comptes.
(6) L'exportation de données est uniquement disponible dans l'édition "Advanced".
(7) L'exportation de données est uniquement disponible dans les éditions "Standard" et "Advanced".

Support technique

5 Support technique

5.1 Signaler des problèmes

Si vous avez un problème, s'il vous plaît, contactez-nous à l'adresse e-mail support@passcape.com.
Sans oublier de nous communiquer les informations suivantes:

- Nom complet et version du programme (voir "A propos")
- Version de Windows incluant les services packs et autres correctifs installés.
- Information sur votre enregistrement, si vous l'êtes.
- Description détaillé de votre problème, si l'erreur est constante ou intermittente.

Si vous signalez une erreur critique, n'oubliez pas de joindre votre fichier "RWPCrash.log" qui a été sauvegardé pendant la session d'exception non gérée.

5.2 Suggestions de fonctionnalités

Si vous avez des questions, des commentaires ou suggestions à propos du programme ou si vous souhaitez avoir plus d'informations, envoyez-nous un e-mail à l'adresse: info@passcape.com

S'il vous plaît, n'oubliez pas de mentionner le nom du programme et la version. Assurez vous, aussi, que vous avez installé la dernière version du programme.

Votre retour d'informations nous aidera à améliorer nos logiciels et à travailler plus efficacement.

5.3 Contacts

S'il vous plaît, n'hésitez pas à envoyer vos questions concernant nos logiciels, à l'émail suivant: support@passcape.com.
Nous vous répondrons sous un à deux jours. Notez, que les utilisateurs enregistrés ont priorité pour le support technique.

Si vous avez rencontré des problèmes durant le processus d'enregistrement, s'il vous plaît, envoyez un e-mail à l'adresse: sales@passcape.com
Nous serons heureux de vous assister dans votre enregistrement.

S'il vous plaît, écrivez-nous en Anglais !

Vous pouvez trouver d'autres utilitaires de récupération sur notre site Web à l'adresse: https://www.passcape.com

Document d'aide de RWP traduit par Laurent DEBARD - 16/11/2018