

**TUTORIAL
OFFLINE NT PASSWORD
&**

REGISTRY EDITOR

**Utilitaire pour réinitialiser les
mots de passe des comptes
administrateur et locaux**

Description

Offline NT Password & Registry Editor est un utilitaire pour réinitialiser le mot de passe des comptes locaux utilisateur sous Windows NT, Windows 2000, Windows XP, Windows 2003 et Windows Vista 32 et 64 bits. Vous n'avez pas besoin de connaître l'ancien mot de passe pour en mettre un nouveau. Pour cela, vous devez arrêter votre ordinateur et redémarrer sur le CD de l'utilitaire. Le CD inclut l'accès aux partitions NTFS, FAT et FAT32. L'utilitaire détectera les comptes utilisateur et permettra de les déverrouiller ou de les désactiver. Il permet également d'éditer la base de registre. Vous pouvez maintenant ajouter un utilisateur dans le group local Administrateur pour devenir administrateur.

Pourquoi l'utiliser

Le système Windows NT stocke les informations de l'utilisateur, en incluant les versions cryptées des mots de passe, dans un fichier appelé 'SAM ', habituellement sous %systemroot%\winnt\system32\config. Microsoft ne fournit pas le moyen de changer le mot de passe si vous ne pouvez pas ouvrir une session avec les droits de le faire, excepté depuis la disquette de secours Microsoft si vous l'avez générée. C'est pourquoi cet utilitaire permet de le faire.

Comment faire le CD

Dézipper le fichier cd070927.zip, il doit contenir le fichier image ISO : cd070927.iso. Il peut être gravé avec n'importe quel programme de gravure à condition que l'option Graver une image ISO soit prise en compte. Une fois gravé sur le CD, il doit seulement contenir les fichiers suivants :

BOOT.CAT, BOOT.MSG, INITRD.CGZ, ISOLINUX.BIN, ISOLINUX.CFG, README.TXT, SCSI.CGZ, SYSLINUX.CFG, SYSLINUX.EXE et VMLINUX

Le PC devra ensuite démarrer sur le CD.

Fonctionnement

Le programme fonctionne pour : NT 3.51, NT 4 (toutes les versions et Service Pack), Windows 2000 (toutes les versions et Service Pack), Windows XP (toutes les versions, même avec le SP2), Windows Server 2003 (tous les Service Packs) et Windows Vista 32 et 64 bits.

Utilisation

- Redémarrer sur le CD

- **Au boot: attendre ou valider par la touche Entrée**

```
*****
*
* Windows NT/2k/XP/Vista Change Password / Registry Editor / Boot CD
*
* (c) 1998-2007 Petter Nordahl-Hagen. Distributed under GNU GPL v2
*
* DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!
*             THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE
*             CAUSED BY THE (MIS)USE OF THIS SOFTWARE
*
* More info at: http://home.eunet.no/~pnordahl/ntpasswd/
* Email       : pnordahl@eunet.no
*
* CD build date: Thu Sep 27 20:57:41 CEST 2007
*****

Press enter to boot, or give linux kernel boot options first if needed.
Some that I have to use once in a while:
boot nousb          - to turn off USB if not used and it causes problems
boot irqpoll       - if some drivers hang with irq problem messages
boot nodrivers     - skip automatic disk driver loading

boot: _
```

- Sélectionner la version de boot. Dans la plus part des cas laisser le choix 1 pour sélectionner la partition NT trouvée et valider par la touche Entrée

```
* Windows Registry Edit Utility Floppy / chntpw *
* (c) 1997 - 2007 Petter N Hagen - pnoordahl@eunet.no *
* GNU GPL v2 license, see files on CD *
*
* This utility will enable you to change or blank the password of
* any user (incl. administrator) on an Windows NT/2k/XP/Vista
* WITHOUT knowing the old password.
* Unlocking locked/disabled accounts also supported.
*
* It also has a registry editor, and there is now support for
* adding and deleting keys and values.
*
* Tested on: NT3.51 & NT4: Workstation, Server, PDC.
* Win2k Prof & Server to SP4. Cannot change AD.
* XP Home & Prof: up to SP2
* Win 2003 Server (cannot change AD passwords)
* Vista 32 and 64 bit
*
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...
*****
=====
There are several steps to go through:
- Disk select with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File-select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk

DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions

=====
n Step ONE: Select disk where the Windows installation is
=====

Disks:
Disk /dev/sda: 68.7 GB, 68718428160 bytes

Candidate Windows partitions found:
1 : /dev/sda1 65522MB BOOT

Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show propbable Windows (NTFS) partitions only
Select: [1]
```

- Laisser le choix du chemin du dossier de registre de Windows et valider par la touche Entrée

```

* Tested on: NT3.51 & NT4: Workstation, Server, PDC.
* Win2k Prof & Server to SP4. Cannot change AD.
* XP Home & Prof: up to SP2
* Win 2003 Server (cannot change AD passwords)
* Vista 32 and 64 bit
*
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...
*****
=====
There are several steps to go through:
- Disk select with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File-select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk

DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions

=====
Step ONE: Select disk where the Windows installation is
=====

Disks:
Disk /dev/sda: 68.7 GB, 68718428160 bytes

Candidate Windows partitions found:
 1 : /dev/sda1 65522MB BOOT

Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show probable Windows (NTFS) partitions only
Select: [1]

Selected 1

Mounting from /dev/sda1, with filesystem type NTFS
NTFS volume version 3.1.

=====
Step TWO: Select PATH and registry files
=====
What is the path to the registry directory? (relative to windows disk)
[WINDOWS/system32/config] :

```

- Laisser le choix 1 pour changer le mot de passe et valider par la touche
- Entrée

```

- Then finally the password change or registry edit itself
- If changes were made, write them back to disk

DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions

=====
n Step ONE: Select disk where the Windows installation is
=====

Disks:
Disk /dev/sda: 68.7 GB, 68718428160 bytes

Candidate Windows partitions found:
 1 : /dev/sda1 65522MB BOOT

Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show propbable Windows (NTFS) partitions only
Select: [1]

Selected 1

Mounting from /dev/sda1, with filesystem type NTFS
NTFS volume version 3.1.

=====
n Step TWO: Select PATH and registry files
=====
What is the path to the registry directory? (relative to windows disk)
[WINDOWS/system32/config] :
-rw----- 1 0 0 262144 Sep 30 19:07 SAM
-rw----- 1 0 0 262144 Sep 30 19:07 SECURITY
-rw----- 1 0 0 262144 Sep 30 19:07 default
-rw----- 1 0 0 9961472 Sep 30 19:07 software
-rw----- 1 0 0 2621440 Sep 30 19:07 system
drwx----- 1 0 0 4096 May 20 14:08 systemprofile
-rw----- 1 0 0 262144 May 20 15:47 userdiff

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] :

```

- Laisser le choix 1 pour éditer le compte et valider par la touche Entrée

```

or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] :
Selected files: sam system security
Copying sam system security to /tmp

=====
n Step THREE: Password or registry edit
=====
chntpw version 0.99.5 070923 (decade), (c) Petter N Hagen
Hive <sam> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x6000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 230/18888 blocks/bytes, unused: 4/1432 blocks/bytes.

Hive <system> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0x27b000 is not 'hbin', assuming file contains garbage at end
File size 2621440 [280000] bytes, containing 603 pages (+ 1 headerpage)
Used for data: 45406/2514968 blocks/bytes, unused: 1143/62600 blocks/bytes.

Hive <security> name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0xb000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 10 pages (+ 1 headerpage)
Used for data: 776/34856 blocks/bytes, unused: 9/5784 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length      : 0
Password history count       : 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>

 1 - Edit user data and passwords
 2 - Syskey status & change
 3 - RecoveryConsole settings
  - - -
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] ->

```

- Laisser le compte **Administrateur** par défaut et valider par la touche **Entrée**
- Vous pouvez aussi sélectionner d'autres comptes
- Il peut arriver que le compte soit désactivé (dis=disabled) ou verrouillé (lock=locked), il vous sera proposer de le réactiver ou le déverrouiller

```

ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x6000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 230/18888 blocks/bytes, unused: 4/1432 blocks/bytes.

Hive <system> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0x27b000 is not 'hbin', assuming file contains garbage at end
File size 2621440 [280000] bytes, containing 603 pages (+ 1 headerpage)
Used for data: 45406/2514968 blocks/bytes, unused: 1143/62600 blocks/bytes.

Hive <security> name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0xb000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 10 pages (+ 1 headerpage)
Used for data: 776/34856 blocks/bytes, unused: 9/5784 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length      : 0
Password history count       : 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>

 1 - Edit user data and passwords
 2 - Syskey status & change
 3 - RecoveryConsole settings
  _ _ _
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1

===== chntpw Edit User Info & Passwords =====
| RID |----- Username -----| Admin? | Lock? |
| 01f4 | Administrator          | ADMIN | dis/lock |
| 03e8 | HelpAssistant         |       | *BLANK* |
| 01f5 | Invite                 |       |         |
| 03eb | PCMAXDATA1            | ADMIN | dis/lock |
| 03ea | SUPPORT_388945a0      |       |         |

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur]

```


- Taper **1** pour mettre le mot de passe à blanc (clavier français : Touche Verr. Num 1) et valider par la touche Entrée
- Vous pouvez aussi ajouter un nouveau mot de passe (choix 2), promouvoir un autre compte en administrateur (choix 3) ou déverrouiller et activer le compte (choix 4)

```

 1 - Edit user data and passwords
 2 - Syskey status & change
 3 - RecoveryConsole settings
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1

===== chntpw Edit User Info & Passwords =====

RID  Username  Admin?  Lock?
01f4  Administrateur  ADMIN  dis/lock
03e8  HelpAssistant  dis/lock
01f5  Invite  *BLANK*
03eb  PCMAXDATA1  ADMIN  dis/lock
03ea  SUPPORT_388945a0  dis/lock

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur]

RID      : 0500 [01f4]
Username: Administrateur
fullname:
comment  : Compte d'utilisateur d'administration
homedir  :

User is member of 1 groups:
00000220 = Administrateurs (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled           [ ] Homedir req.           [ ] Passwd not req.
[ ] Temp. duplicate    [X] Normal account       [ ] NMS account
[ ] Domain trust ac    [ ] Wks trust act.       [ ] Srv trust act
[X] Pwd don't expir    [ ] Auto lockout         [ ] (unknown 0x08)
[ ] (unknown 0x10)     [ ] (unknown 0x20)       [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] >

```

- Taper ! pour quitter (clavier français : Touches Maj+&) et valider par la touche Entrée

```

 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1

===== chntpw Edit User Info & Passwords =====
| RID |----- Username -----| Admin? |-- Lock? --|
| 01f4 | Administrateur          | ADMIN | dis/lock   |
| 03e8 | HelpAssistant          |       | *BLANK*   |
| 01f5 | Invite                 |       |           |
| 03eb | PCMAXDATA1            | ADMIN | dis/lock   |
| 03ea | SUPPORT_388945a0      |       |           |
Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur]

RID      : 0500 [01f4]
Username : Administrateur
fullname :
comment  : Compte d'utilisateur d'administration
homedir  :

User is member of 1 groups:
00000220 = Administrateurs (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled           [ ] Homedir req.           [ ] Passwd not req.
[ ] Temp. duplicate   [X] Normal account       [ ] NMS account
[ ] Domain trust ac   [ ] Wks trust act.       [ ] Srv trust act
[X] Pwd don't expir   [ ] Auto lockout        [ ] (unknown 0x08)
[ ] (unknown 0x10)    [ ] (unknown 0x20)      [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur]

```

- Taper q pour quitter (clavier français : Touche a) et valider par la touche Entrée

```

! 03ea ! SUPPORT_388945a0 ! dis/lock !
Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur]

RID      : 0500 [01f4]
Username : Administrateur
fullname :
comment  : Compte d'utilisateur d'administration
homedir  :

User is member of 1 groups:
00000220 = Administrateurs (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled           [ ] Homedir req.           [ ] Passwd not req.
[ ] Temp. duplicate   [X] Normal account       [ ] NMS account
[ ] Domain trust ac  [ ] Wks trust act.       [ ] Srv trust act
[X] Pwd don't expir   [ ] Auto lockout        [ ] (unknown 0x08)
[ ] (unknown 0x10)   [ ] (unknown 0x20)      [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0

- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur] ?

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>

1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
- - -
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] ->

```

- Taper y pour valider les changements et valider par la touche Entrée

```

homedir :
User is member of 1 groups:
00000220 = Administrateurs (which has 2 members)

Account bits: 0x0210 =
[ ] Disabled                [ ] Homedir req.           [ ] Passwd not req.
[ ] Temp. duplicate         [X] Normal account       [ ] NMS account
[ ] Domain trust ac        [ ] Wks trust act.       [ ] Srv trust act
[X] Pwd don't expir        [ ] Auto lockout         [ ] (unknown 0x08)
[ ] (unknown 0x10)         [ ] (unknown 0x20)       [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0

- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur] ?

<>=====<> chntpw Main Interactive Menu <>=====<>

Loaded hives: <sam> <system> <security>

1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
- - -
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q

Hives that have changed:
# Name
0 <sam> - OK

=====
Step FOUR: Writing back changes
=====
About to write file(s) back? Do it? [n] :

```

- Vous pouvez recommencer dans le menu sinon accepter le choix par défaut n et valider par la touche Entrée

```

[ ] Temp. duplicate      [X] Normal account      [ ] NMS account
[ ] Domain trust ac    [ ] Wks trust act.     [ ] Srv trust act
[X] Pwd don't expir    [ ] Auto lockout      [ ] (unknown 0x08)
[ ] (unknown 0x10)     [ ] (unknown 0x20)    [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0

- - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrateur] ?

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>

 1 - Edit user data and passwords
 2 - Syskey status & change
 3 - RecoveryConsole settings
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
0 <sam> - OK

=====
n Step FOUR: Writing back changes
=====
About to write file(s) back! Do it? [n] : y
Writing sam

***** EDIT COMPLETE *****

You can try again if it somehow failed, or you selected wrong
New run? [n] :

```

- Retirer le CD
- Redémarrer la machine depuis la combinaison de touche **Ctrl+Alt+Suppr**
- Se connecter sous Windows avec le compte **Administrateur** sans mot de passe

```

or simply enter the username to change: [Administrateur] ?

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
  _ _ _
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
0 <sam> - OK

=====
n Step FOUR: Writing back changes
=====
About to write file(s) back! Do it? [n] : y
Writing sam

***** EDIT COMPLETE *****

You can try again if it somehow failed, or you selected wrong
New run? [n] :

=====
* end of scripts.. returning to the shell..
* Press CTRL-ALT-DEL to reboot now (remove floppy first)
* or do whatever you want from the shell..
* However, if you mount something, remember to umount before reboot
* You may also restart the script procedure with 'sh /scripts/main.sh'

(Please ignore the message about job control, it is not relevant)

BusyBox v1.1.0-pre1 (2005.12.30-19:45+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

sh: can't access tty; job control turned off
$ Clocksource tsc unstable (delta = 965361288 ns)
Time: pit clocksource has been installed.

```