

Windows administrator wachtwoord wijzigen met UBCD4Win

HOWTO:

Het Windows' administrator-wachtwoord wijzigen met de UBCD4Win CD.

Een stap-voor-stap uitleg.

- Start de computer op met de [UBCD4Win-CD](#).

Dit duurt iets langer dan normaal, heb dus geduld tot je het welkomstscherf te zien krijgt.



- Kies in het volgende menu voor **Offline NT Password & Registry Editor** door met de pijltjes-toetsen deze te selecteren en druk dan op <ENTER>

```
----- Welcome to the Ultimate Boot CD! -----
About
see http://www.ubcd4win.com for latest updates & Downloads

Options
Boot from drive C:
Launch "The Ultimate Boot CD for Windows"
REBOOT
... Insert your boot options here ...
Darik's Boot And Nuke v2.0 ~ Submenu
FreeDOS
GOBACK Removal Tool
Memtest86 v3.5 (Standard Version)
NTFS for DOS
Offline NT Password & Registry Editor
Windows(tm) Recovery Console

Help
Runs a pre-installed Windows environment, loaded with diagnostic tools.

----- Please visit the forums at http://www.ubcd4win.com/forum/ -----
```

- Na een hardware-check wordt nu deze editor opgestart, dat duurt even, dus heb geduld.
- Uiteindelijk komt in beeld

Code:

```
=====
STEP ONE: Select Disk where the Windows installation is
=====
```

```

* Windows Registry Edit Utility Floppy / chntpw
* (c) 1997 - 2008 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 SP3
*            Win 2003 Server (cannot change AD passwords)
*            Vista 32 and 64 bit, Server 2008 32+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: 33.5 GB, 33554497536 bytes
Candidate Windows partitions found:
1 : /dev/sda1 31988MB 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] =

```

- Achter **select: [1]:** typ je nu een **a** (show all partitions)
- Type nu het nummer dat is toegekend aan de betreffende partitie. Mocht dit onduidelijk zijn kies dan voor de standaard instelling **1** en druk op <ENTER>.

Dan komt in beeld

Code:

```

=====
STEP TWO: Select Path and registry files
=====

```

- Dit pad is: *Windows/system32/config* en standaard wordt dit al aangegeven.

```
l = show proppable Windows (NTFS) partitions only
Select: [1] Clocksource tsc unstable (delta = 89603479 ns)
d
---- AUTO DISK DRIVER select ----
--- PROBE FOUND THE FOLLOWING DRIVERS:
ata_piix
ata_generic
--- TRYING TO LOAD THE DRIVERS
### Loading ata_piix
### Loading ata_generic
-----
Driver load done, if none loaded, you may try manual instead.
-----
Disks:
Disk /dev/sda: 68.7 GB, 68718428160 bytes
Disk /dev/sdb: 17.1 GB, 17179803648 bytes
Disk /dev/sdb doesn't contain a valid partition table
Candidate Windows partitions found:
 1 : /dev/sdal 65533MB 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 proppable Windows (NTFS) partitions only
Select: [1]
Selected 1
Mounting from /dev/sdal, with assumed filesystem type NTFS
So, let's really check if it is NTFS?
Yes, read-write seems OK.
Mounting it. This may take up to a few minutes:
Success!
=====
■ Step TWO: Select PATH and registry files
=====
What is the path to the registry directory? (relative to windows disk)
[Windows/system32/config] :
```

Tecla Enter

Druk op <ENTER>

- Dan wordt gevraagd welk deel van het register geladen moet worden. Kies **1** (Password reset [sam security system])

Nu volgt stap 3:

```
Code:
=====
Step THREE: Password or registry edit
=====
```

```

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

=====
Step THREE: Password or registry edit
=====
chntpw version 0.99.6 080526 (sixtyfour), (c) Petter N Hagen
hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0x7000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 278/21832 blocks/bytes, unused: 9/2552 blocks/bytes.

hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0xcd0000 is not 'hbin', assuming file contains garbage at end
File size 13631488 [400000] bytes, containing 3077 pages (+ 1 headerpage)
Used for data: 156663/9933728 blocks/bytes, unused: 5818/3398592 blocks/bytes.

hive <SECURITY> name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
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: 341/16248 blocks/bytes, unused: 4/4072 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
 4 -
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] ->

```

- Bij de vraag "what to do?" kies je optie **1** (Edit user data and passwords), gevolgd door een <ENTER>

- En nu begint het allemaal ergens op te lijken.
Je ziet nu een overzicht van alle gebruikers-namen.

Kies nu de gebruiker van wie je het wachtwoord wilt wijzigen. Default staat deze al op Administrator, dus een simpele <ENTER> voldoet.

- Je bent nu bij het moment dat je een nieuw wachtwoord aan de Administrator kunt toekennen. Lees goed de waarschuwing, die IMO nog een understatement is "Blanking is often the best" ofwel: laat het administrator wachtwoord blanco.

Dit voorkomt eventuele foutmeldingen. En later kun je het wachtwoord alsnog wijzigen (belangrijk dit ook te doen!).

Het wachtwoord laat je blanco met * (een asterisk dus).

- Na een <ENTER> vraagt -ie of je dat wel zeker weet en dus bevestig je dat met een **y** en druk <ENTER>

- afsluiten doe je met een **!**, een uitroepteken.

- in het volgende menu kun je afsluiten met een **q**, voor 'quit'. Zoals je ook bij de opties ziet staan.

- Dan wordt gevraagd om de wijzigingen op te slaan:

Code:

=====
Step FOUR: writing back changes
=====

```
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: 40

- - - 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
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] :
```

Je kiest uiteraard voor **y** (yes)

- Na een ******EDIT COMPLETE****** krijg je de mogelijkheid om ook een wachtwoord van een andere gebruiker te wijzigen.

Druk op de **n** of druk simpelweg op <ENTER> bij de vraag **new run? [n] :**

```

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: 40

- - - 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
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] : y
Writing sam
***** EDIT COMPLETE *****
You can try again if it somehow failed, or you selected wrong
New run? [n] :

```

Daarna de computer opnieuw opstarten (wel even de CD uit de lade halen!) en je administrator-wachtwoord is nu blanco.