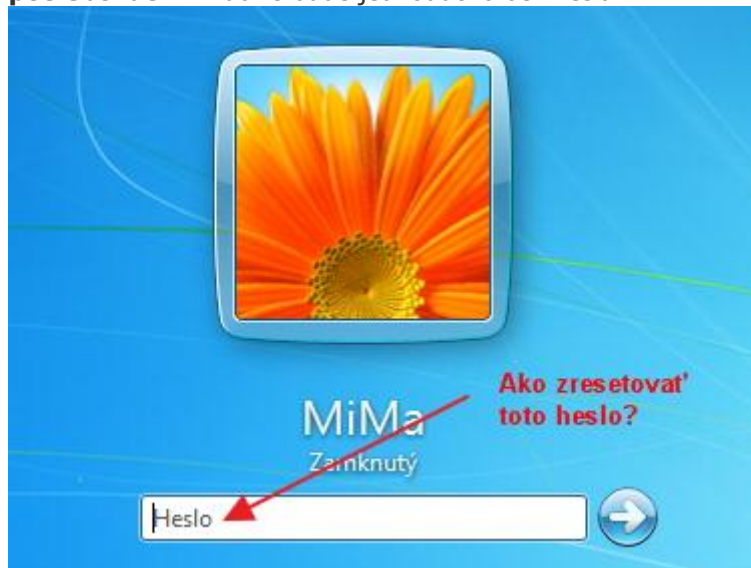


Ako resetovať zabudnuté heslo Windows

Možno sa vám už niekedy stalo že ste zabudli heslo na prihlásenie do Windows a nevedeli ste sa dostať do svojho počítača. V tomto návode ukážem spôsob ako heslo resetovať.

Pomocou tohto návodu docielime to, že **žiadne heslo už nebudete na prihlásenie do počítača potrebovať**. Windows bude jednoducho bez hesla.



Postup na resetovanie hesla Windows:

- 1.) Stiahneme súbor [cd110511.zip](#) zo stránky [pogostick.net](#) a rozbalíme ho niekde na disk.
- 2.) Súbor **cd110511.iso**, ktorý sme rozbalili zo zip archívu v kroku 1. napálime na disk. Ak neviete ako napáliť iso súbor na CD/DVD disk, odporúčam článok [ako napáliť iso súbor](#)
- 3.) Teraz vložíme disk do CD/DVD mechaniky a **reštartujeme počítač**. V biosse **nastavíme bootovanie z CD/DVD mechaniky**, aby sme zabezpečili načítanie napáleného programu.
- 4.) Ak sme správne nastavili bootovanie a obsah CD sa načítal, mali by ste vidieť na obrazovke počítača niečo podobné. Pre pokračovanie **stlačíme klávesu ENTER**.

```
*****
*                               *
*   Windows Reset Password / Registry Editor / Boot CD   *
*                               *
*   (c) 1998-2011 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://pogostick.net/~pnh/ntpasswd/         *
*   Email       : pnh@pogostick.net                          *
*                               *
*   CD build date: Wed May 11 20:16:09 CEST 2011              *
*                               *
*****

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 vga=ask     - if you have problems with the videomode
boot nodrivers  - skip automatic disk driver loading

boot: _
```

5.) Teraz sa nám objavilo okno s oblastami na ktorých sa nachádza **inštalácia systému Windows**. V mojom prípade už mám voľbu 1. prednastavenú a stačí už len stlačiť klávesu **ENTER**.

```
* Windows Registry Edit Utility Floppy / chntpw
* (c) 1997 - 2010 Petter N Hagen - phordahl@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 & Win7 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: 64.4 GB, 64424509440 bytes
Candidate Windows partitions found:
1 : /dev/sda1 61438MB 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] - Stlačíme len klávesu ENTER
```

6.) V tomto kroku nastavíme cestu k priečinkom Windows a registrom. Program nám však **prácu opäť uľahčil a prednastavil** cestu za nás. Stlačíme teda opäť klávesu **Enter** pre pokračovanie.

```
=====
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: 64.4 GB, 64424509440 bytes
Candidate Windows partitions found:
1 : /dev/sda1 61438MB 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 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
=====
DEBUG path: windows found as Windows
DEBUG path: system32 found as System32
DEBUG path: config found as config
DEBUG path: found correct case to be: Windows/System32/config
What is the path to the registry directory? (relative to windo
[Windows/System32/config] _
```

7.) Teraz sa nás program opýta čo chceme urobiť. V našom prípade chceme **resetovať heslo** vo Windows a to je **voľba číslo 1**. Tá už je však opäť prednastavená a stačí len stlačiť na klávesnici


```
Yes, read-write seems OK.  
Mounting it. This may take up to a few minutes:  
  
Success!  
  
=====
```

```
Step TWO: Select PATH and registry files  
=====
```

```
DEBUG path: windows found as Windows  
DEBUG path: system32 found as System32  
DEBUG path: config found as config  
DEBUG path: found correct case to be: Windows/System32/config
```

```
What is the path to the registry directory? (relative to windows)  
[Windows/System32/config]  
DEBUG path: Windows found as Windows  
DEBUG path: System32 found as System32  
DEBUG path: config found as config  
DEBUG path: found correct case to be: Windows/System32/config
```

```
-rwxrwxrwx      0 0 0          28672 May 22 23:08 BCD-Temp  
-rwxrwxrwx      0 0 0    41943040 May 22 12:56 COMPONENT  
-rwxrwxrwx      0 0 0    65536 May 22 16:15 COMPONENT  
-11de-8d1d-001e0bcde3ec}.TM.blf          524288 May 22 19:15 COMPONENT  
-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000000000001 regtrans  
-rwxrwxrwx      0 0 0    524288 Jul 14 2009 COMPONENT  
-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000000000002 regtrans  
-rwxrwxrwx      0 0 0    65536 May 23 12:56 COMPONENT  
-11e2-9e21-000c29d2b59a}.TM.blf          524288 May 23 12:56 COMPONENT  
-11e2-9e21-000c29d2b59a}.TMContainer000000000000000000000001 regtrans  
-rwxrwxrwx      0 0 0    524288 May 23 12:56 COMPONENT  
-11e2-9e21-000c29d2b59a}.TMContainer000000000000000000000002 regtrans  
-rwxrwxrwx      1 0 0    262144 May 23 12:57 DEFAULT  
drwxrwxrwx      1 0 0           0 Jul 14 2009 Journal  
drwxrwxrwx      1 0 0           0 May 23 12:49 RegBack  
-rwxrwxrwx      1 0 0    262144 May 23 12:57 SAM  
-rwxrwxrwx      1 0 0    262144 May 23 12:57 SECURITY  
-rwxrwxrwx      1 0 0   34340864 May 23 12:57 SOFTWARE  
-rwxrwxrwx      1 0 0   11796480 May 23 12:57 SYSTEM  
drwxrwxrwx      1 0 0    4096 May 22 19:10 TxR  
drwxrwxrwx      1 0 0    4096 Nov 21 2010 systempro
```

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

```

-rwxrwxrwx 1 0 0 11796480 May 23 12:57 SYSTEM
drwxrwxrwx 1 0 0 4096 May 22 19:10 TxR
drwxrwxrwx 1 0 0 4096 Nov 21 2010 systemprofi

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
r11 -
Selected files: sam system security
Copying sam system security to /tmp

=====
Step THREE: Password or registry edit
=====
chntpw version 0.99.6 [110511] <C> Petter N. Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [400001] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 246/19480 blocks/bytes, unused: 13/840 blocks/bytes.

Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 11796480 [b400001] bytes, containing 2571 pages (+ 1 headerpage)
Used for data: 188844/11521496 blocks/bytes, unused: 6152/65736 blocks/bytes.

Hive <SECURITY> name (from header): <emRoot\System32\Config\SECURITY
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [400001] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 374/19160 blocks/bytes, unused: 7/1160 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
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> _

```

9.) Teraz **vyberieme názov používateľa zo zoznamu**, ktorého heslo chceme resetovať (vymazať). V mojom prípade je to používateľ MiMa. Vpíšem teda MiMa do programu a stlačím klávesu **ENTER**.

```

Copying sam system security to /tmp
=====
Step THREE: Password or registry edit
=====
chntpw version 0.99.6 110511: (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 246/19480 blocks/bytes, unused: 13/840 blocks/bytes

Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 11796480 [b40000] bytes, containing 2571 pages (+ 1 headerpage)
Used for data: 188844/11521496 blocks/bytes, unused: 6152/65736 blocks/bytes

Hive <SECURITY> name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 374/19160 blocks/bytes, unused: 7/1160 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
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords =====
RID - Username - Admin? - Lock? --
01f4 Administrator ADMIN dis/lock
01f5 Guest dis/lock
03e8 MiMa ADMIN dis/lock

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

Vpíšte do programu meno používateľa ktorého heslo chcete resetovať a stlačte klávesu ENTER.

```

10.) **Pre zmazanie hesla** stlačíme na klávesnici číslo jedna a následne klávesu ENTER pre potvrdenie voľby.

```

<>=====<> 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] ->

===== chntpw Edit User Info & Passwords =====
RID - Username - Admin? - Lock? --
01f4 Administrator ADMIN dis/lock
01f5 Guest dis/lock
03e8 MiMa ADMIN dis/lock

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

RID: 1000 [03e8]
Username: MiMa
fullname:
comment:
homedir:

User is member of 2 groups:
00000221 = Users (which has 3 members)
00000220 = Administrators (which has 2 members)

Account bits: 0x0014 =
[ ] Disabled [ ] Homedir req. [X] Passwd not req.
[ ] Temp duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac [X] Wks trust act [ ] Srv trust act
[ ] Pwd don't expir [ ] Auto lockout [ ] (unknown 0x08)
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)

Failed login count: 1, while max tries is: 0
Total login count: 12

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

Select: [q] > 1

```

napišeme 1 a stlačíme klávesu enter pre zmazanie hesla

11.) Teraz sa nám objavila hláška **Password cleared!**. To znamená že sme heslo úspešne zmazali. Na klávesnici **stlačíme klávesu „!“** a následne **ENTER** pre potvrdenie.

```

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] -> 1

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

RID  Username  Admin?  Lock?
01f4  Administrator  ADMIN   dis/lock
01f5  Guest          ADMIN   dis/lock
03e8  MiMa           ADMIN   dis/lock

Select: ? - quit, - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] MiMa
RID      : 1000 [03e8]
Username : MiMa
fullname :
comment  :
homedir  :

User is member of 2 groups:
00000221 = Users (which has 3 members)
00000220 = Administrators (which has 2 members)

Account bits: 0x0014 =
[ ] Disabled [ ] Homedir req. [X] Passwd not req.
[ ] Temp duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[ ] Pwd don't expir [ ] Auto lockout [ ] (unknown 0x08)
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)

Failed login count: 1, while max tries is: 0
Total login count: 12

- - - 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 [probably locked now]
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: [Administrator] !_

```

12.) Teraz **stlačíme klávesu „q“** a následne **potvrdíme klávesou ENTER**.

```

or simply enter the username to change: [Administrator] MiMa
RID      : 1000 [03e8]
Username : MiMa
fullname :
comment  :
homedir  :

User is member of 2 groups:
00000221 = Users (which has 3 members)
00000220 = Administrators (which has 2 members)

Account bits: 0x0014 =
[ ] Disabled [ ] Homedir req. [X] Passwd not req.
[ ] Temp duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[ ] Pwd don't expir [ ] Auto lockout [ ] (unknown 0x08)
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)

Failed login count: 1, while max tries is: 0
Total login count: 12

- - - 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 [probably locked now]
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: [Administrator] q
Cannot find value <\SAM\Domains\Account\Users\Names\q\>

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

<>=====<> 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_

```

13.) V tomto kroku sa nás program opýta či chceme uložiť všetky zmeny ktoré sme urobili (reset hesla). Preto **stlačíme** na klávesnici **klávesu „y“** ako áno a **následne** potvrdíme klávesou **ENTER**.

```
00000220 = Administrators (which has 2 members)
Account bits: 0x0014 =
[ ] Disabled [ ] Homedir req. [X] Passwd not req.
[ ] Temp. duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[ ] Pwd don't expir [ ] Auto lockout [ ] (unknown 0x08)
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)

Failed login count: 1, while max tries is: 0
Total login count: 12

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vis
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
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: [Administrator] q
Cannot find value <\SAM\Domains\Account\Users\Names\q\@>

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

<>=====<> 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_
```

14.) Mala by sa nám objaviť hláška **EDIT COMPLETE**, ktorá znamená že všetko prebehlo v poriadku. Stačí už len **stlačiť** klávesu **ENTER**, reštartovať počítač a nastaviť bootovanie späť na pevný disk počítača.

```
[ ] Pwd don't expir [ ] Auto lockout [ ] (unknown 0x08) [ ]
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)

Failed login count: 1, while max tries is: 0
Total login count: 12

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vis
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
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: [Administrator] q
Cannot find value <\SAM\Domains\Account\Users\Names\q\@>

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

<>=====<> 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] : - stlačíme klávesu enter
```

Ak ste všetko urobili podľa návodu, počítač by už nemal vyžadovať heslo na prihlásenie.

