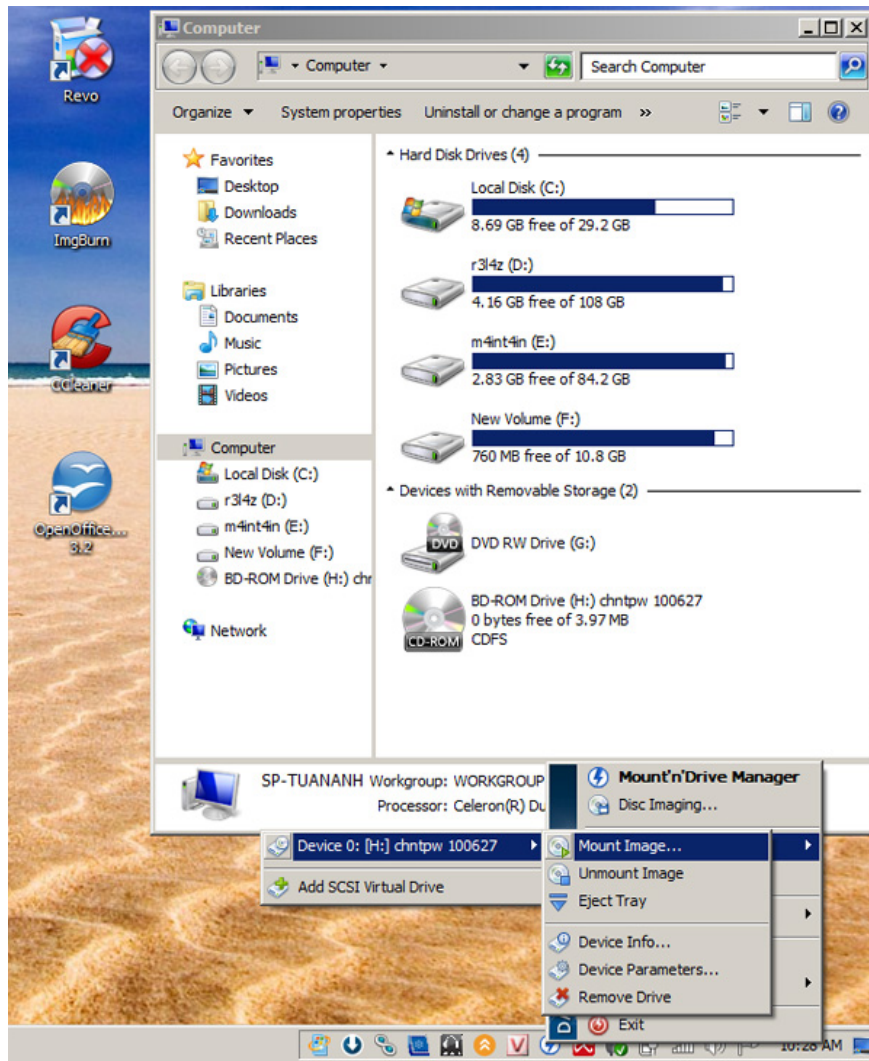


Retrieve password of Windows XP, Vista or 7 account using USB Flash drive

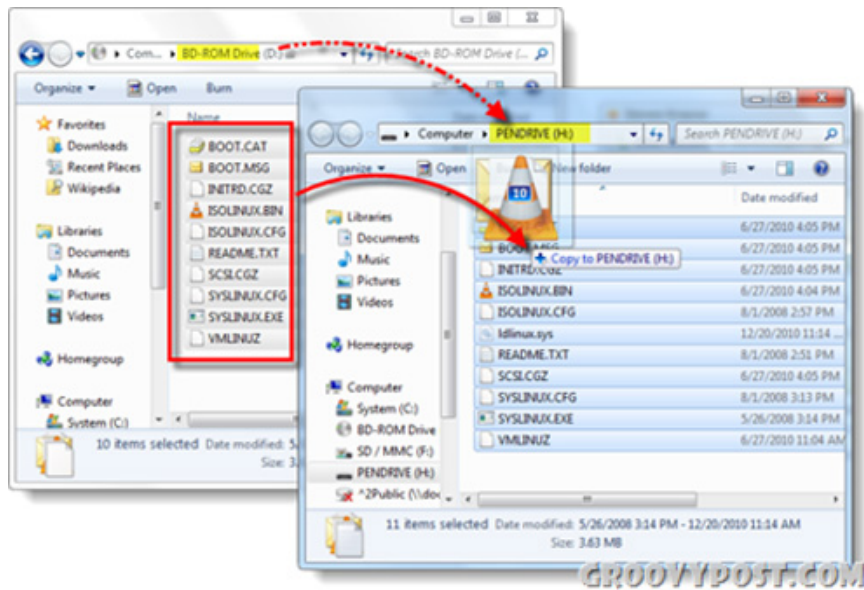
Still the eternal problem of many Windows users: forget the access password? Computer does not have a CD / DVD drive? How will you fix this? And in the following article, TipsMake.com will present the basic steps to get back your account when you forget your password on any computer using Windows operating system with USB Fla device.

QuanTriMang.com - Still a problem for many Windows users: forget your access password? Computer does not have a CD / DVD drive? How will you fix this? And in the following article, TipsMake.com will present the basic steps to get back your account when you forget the password on any computer using Windows operating system with the familiar USB Flash device .

First, you need to download Offline tool NT Password & Registry Editor [here](#) or [here](#). After extracting this file, we will have a single * .iso file: *cd100627.iso* . Next, use a software to create and store virtual drives like Magic ISO or DAEMON Tools Lite to assign that * .iso file to the system:

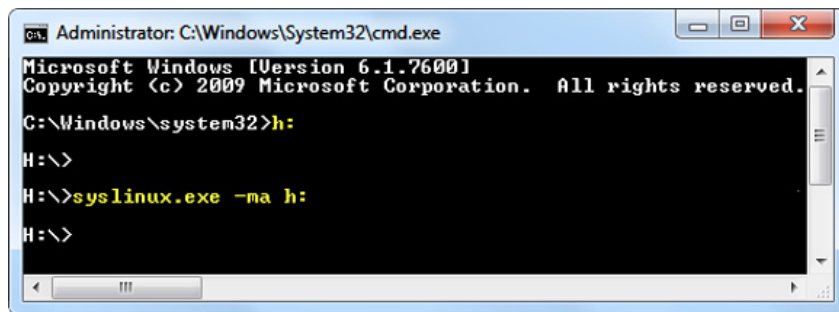


Copy the entire file inside the virtual drive to USB:



Then, use *Command Prompt (Start Menu> Run> cmd and Enter)* , move to the USB drive (here is the H drive) and type the following command:

syslinux.exe -ma h:

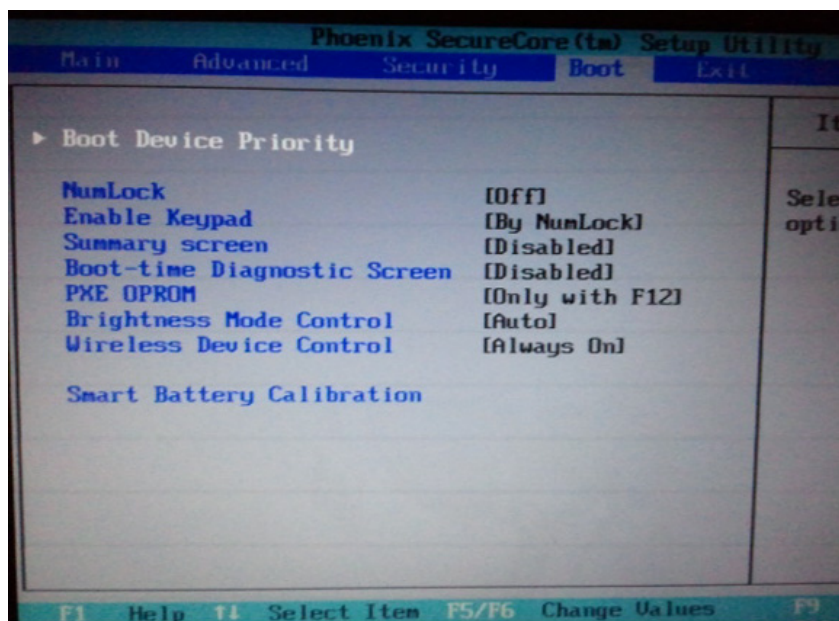


```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>h:
H:\>
H:\>syslinux.exe -ma h:
H:\>
```

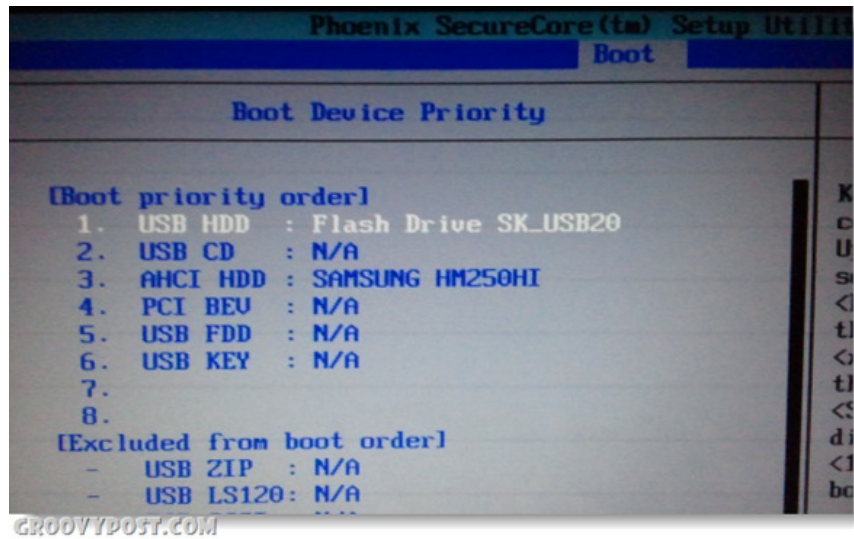
GROOVYP0ST.COM

Then unplug the USB and plug in the computer to retrieve the account. First, we need to change the boot order of the boot device to the USB, boot the computer and press F2, F8 or Delete to access the BIOS, go to the *Boot Order, Boot Device Priority card* or equivalent (depending on different mainboard lines) and change as follows:

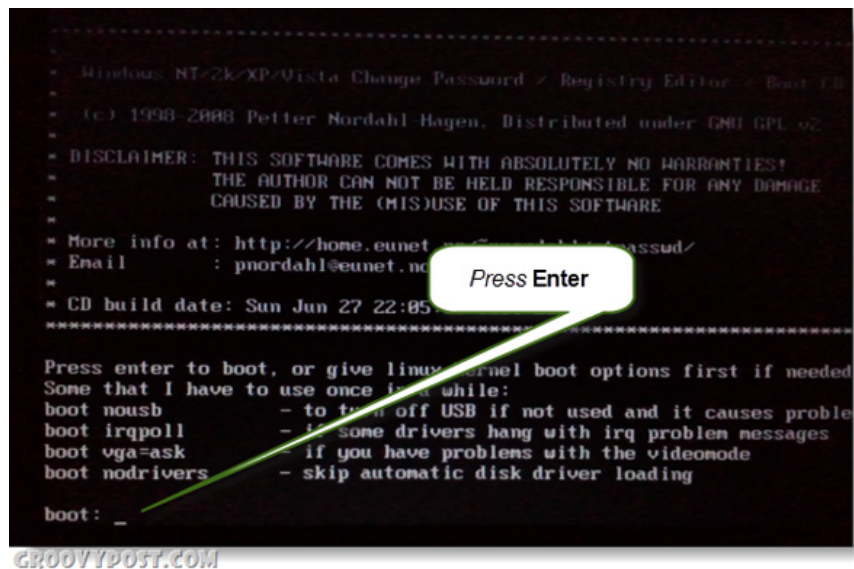


GROOVYP0ST.COM

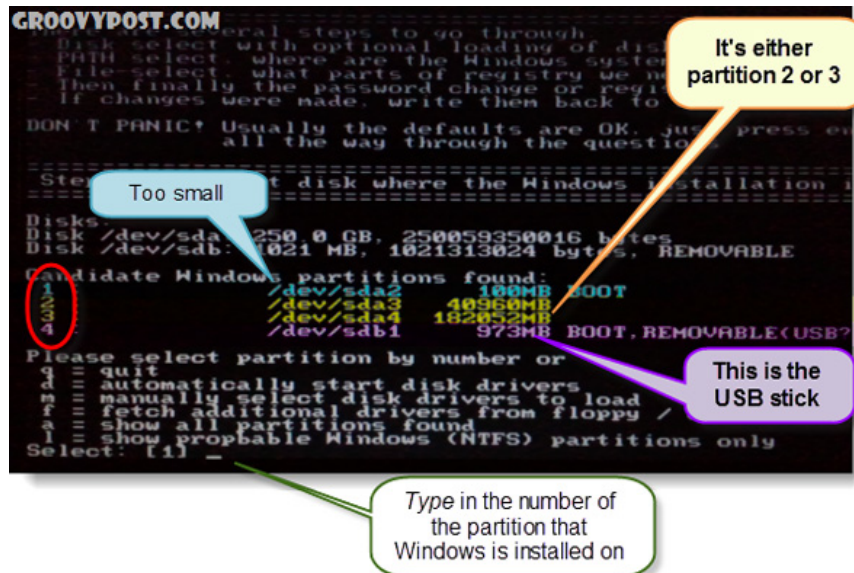
Under the boot device order, set the USB to the first position, then press F10 to save the changes and Enter to restart the computer:



When the system boots from USB, you will see the main interface as follows:



At the current location of the cursor, press Enter. The program will detect the entire hard drive to find the Windows installation partition. In this test, there are 4 partitions, you need to pay attention to the letter corresponding to the drive that installs the operating system, then press Enter:



However, do not worry too much, because if you choose the wrong partition, the program will not work and return to the main screen. If you select the correct partition, the system will display the following information:

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 / System / 32 / config

And press Enter to finish this process. If you choose wrong, press Enter and q to return to the previous screen.

After selecting the right partition and pressing Enter as described above, go to this step and select 1 - *Select Password reset [sam system security]* and Enter :



Select item 1 - *Edit user data and passwords* and Enter :

```
GROOVYPOST.COM
part of registry to load use predefined choices
1 - list the files with space as delimiter
2 - Password reset [san system security]
3 - RecoveryConsole parameters [software]
4 - quit - return to previous
[1]
Selected files san system security
Copying sam system security to /tmp

=====
Step THREE Password or registry edit
=====
chntpw version 0.99.6 100627 (vacation) (c) Petter N Hagen
Hive <SAM> name (from header): (\SystemRoot\System32\Config\SAM)
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c (1)
Page at 0x2000 is not hbin, assuming file contains garbage at
File size 262144 [40000] bytes, containing 4 pages (+ 1 headers)
Used for data: 205/15272 blocks/bytes, unused: 9/984 blocks/bytes

Hive <SYSTEM> name (from header): (\SYSTEM)
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c (1)
Page at 0xdd4000 is not hbin, assuming file contains garbage at
File size 1468800 [10000] bytes, containing 328 pages (+ 1 headers)
Used for data: 210448/13305188 blocks/bytes, unused: 7032/108728 blocks/bytes

Hive <SECURITY> name (from header): (\SystemRoot\System32\Config\SECURITY)
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c (1)
Page at 0x6000 is not hbin, assuming file contains garbage at
File size 262144 [40000] bytes, containing 5 pages (+ 1 headers)
Used for data: 326/15672 blocks/bytes, unused: 10/4648 blocks/bytes

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length: 8
Password history count: 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
2 - Registry editor, now with full write support?
3 - Quit (you will be asked if there is something to save)

What to do? [1] -> 1
```

Type 1 and Press Enter.

Next, you will see the corresponding *RID* and *Username* lines. Depending on which elements are simpler, we will do it that way. For example, if you select *RID* , you must add *0x* in front of the number, for this is *0x03e8* for *RID 03e8*. In this test, we choose *Username Lep*:

```
GROOVYPOST.COM
RID ----- Username ----- Admin? ----- Lock
01f4 Administrator ADMIN dis/lock
01f5 Guest ADMIN dis/lock
03e8 Lep ADMIN *BLANK*

Select: ? - quit, - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] 0x03e8
```

Type in whatever is easier, The Username, or the RID with a 0x in front of it.

Select item 1 - *Clear user password* and Next :

```

GROOVYPOST.COM
Select: ? - quit, ! - enable user account! (seems unlocked already)
or simply enter the username to change: [Administrator]
Select: [q] > q
Select: ? - quit, ! - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
RID      Username      Admin?  Lock?
01f4    Administrator  ADMIN   dis/lock
01f5    Guest          ADMIN   dis/lock
03e8    Lepbarr        ADMIN   *BLANK*
Select: ? - quit, ! - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] 0x03e8
RID      1000 [03e8]
Username Lepbarr
fullname
comment
homedir
User is member of 1 groups:
00000220 = Administrators (which has 2 members)
Account bits: 0x0214 =
Disabled [X] Homedir req. [X] Psswd not req.
Temp duplicate [X] Normal account [X] NMS account
Domain trust ac [X] Nks trust act. [X] Srv trust act
Psd don't expir (unknown 0x10) Auto lockout (unknown 0x08)
(unknown 0x10) (unknown 0x20) (unknown 0x40)
Failed login count: 0, while max tries is: 0
Total login count: 15
-- User Edit Menu:
-- Clear (blank) user password
-- Edit (set new) user password (careful with this on XP or Vista)
-- Promote user (make user an administrator)
-- Unlock and enable user account! (seems unlocked already)
-- Quit editing user, back to user select
Select: [q] > 1

```

Type 1 and Press Enter.

You will see the system appear a small message line as follows: *Password cleared!* Which means we have successfully reset the Administrator account password, now type ! And press Enter:

```

GROOVYPOST.COM
Select: ? - quit, ! - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
RID      Username      Admin?  Lock?
01f4    Administrator  ADMIN   dis/lock
01f5    Guest          ADMIN   dis/lock
03e8    Lep             ADMIN   *BLANK*
Select: ? - quit, ! - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] 0x03e8
RID      1000 [03e8]
Username Lep
fullname
comment
homedir
User is member of 1 groups:
00000220 = Administrators (which has 2 members)
Account bits: 0x0214 =
Disabled [X] Homedir req. [X] Psswd not req.
Temp duplicate [X] Normal account [X] NMS account
Domain trust ac [X] Nks trust act. [X] Srv trust act
Psd don't expir (unknown 0x10) Auto lockout (unknown 0x08)
(unknown 0x10) (unknown 0x20) (unknown 0x40)
Failed login count: 0, while max tries is: 0
-- User Edit Menu:
-- Clear (blank) user password
-- Edit (set new) user password (careful with this on XP or Vi
-- Promote user (make user an administrator)
-- Unlock and enable user account! (seems unlocked already)
-- Quit editing user, back to user select
Password cleared!
Select: [q] > 1

```

Type ! and Press Enter.

Next type Q to exit and Enter:

```

GROOVYPOST.COM
User is member of 1 groups
00000220 - Administrators (which has 2 members)
Account bits 0x0214
[ ] Disabled
[ ] Temp duplicate
[ ] Domain trust ac
[X] Pad don't expir
[ ] (unknown 0x10)
[ ] Homedir req.
[X] Normal account
[ ] Wks trust act.
[ ] Auto lockout
[ ] (unknown 0x20)
[ ] Password
[ ] NMS acc
[ ] Srv tru
[ ] (unknow
[ ] (unknow

Failed login count: 0, while max tries is: 0
Total login count: 15
*** No NT MD4 hash found. This user probably has a BLANK
*** No LANMAN hash found either. Sorry, cannot change. T

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

Select: ? - quit, . - list users, 0x<RID> - User with R
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

What to do? [1] -> q

```

Type q and Press Enter.

Press Y to save changes to the file system, then Enter:

```

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

Select: ? - quit, . - list users, 0x<RID> - User with RID (he
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:
0 <SAM> - OK

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

```

Type y and Press Enter.

If you see a message like this: ***** EDIT COMPLETE ***** means it was really successful. Type N and press Enter:

```

GROOVYPOST.COM
...
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: [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] : n

```

Type n and Press Enter.

In case you have not achieved satisfactory results, type Y and try again. After successful, please unplug the USB from the computer and press *Ctrl + Alt + Delete* to restart the system:

```

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:

(<)=====< 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] : 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 unmount before reboot
# You may also restart the script procedure with 'sh /scripts/main.sh'

```

Unplug the USB Drive and Press Ctrl+Alt+Del to reboot the computer and log in!

After booting up, you will be able to login to the system with Administrator account without a password. So we have completed the process of retrieving the password and admin account with a simple method and familiar USB Flash storage device. Good luck!

You finished reading the article "**Retrieve password of Windows XP, Vista or 7 account using USB Flash drive**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.