

## [Change or Reset Windows Password from a Ubuntu Live CD](#)

If you can't log in even after trying your twelve passwords, or you've inherited a computer complete with password-protected profiles, worry not – you don't have to do a fresh install of Windows. We'll show you how to change or reset your Windows password from a Ubuntu Live CD.

This method works for all of the NT-based version of Windows – anything from Windows 2000 and later, basically. And yes, that includes Windows 7.

*Note: If you have files on your hard disk encrypted using built-in Windows encryption, they may not be available after changing the Windows password using this method. Exercise caution if you have important encrypted files.*

You'll need a Ubuntu 9.10 Live CD, or a bootable Ubuntu 9.10 Flash Drive. If you don't have one, or have forgotten how to boot from the flash drive, check out our article on [creating a bootable Ubuntu 9.10 flash drive](#).

The program that lets us manipulate Windows passwords is called **chntpw**. The steps to install it are different in 32-bit and 64-bit versions of Ubuntu.

### **Installation: 32-bit**

Open up Synaptic Package Manager by clicking on System at the top of the screen, expanding the Administration section, and clicking on Synaptic Package Manager.

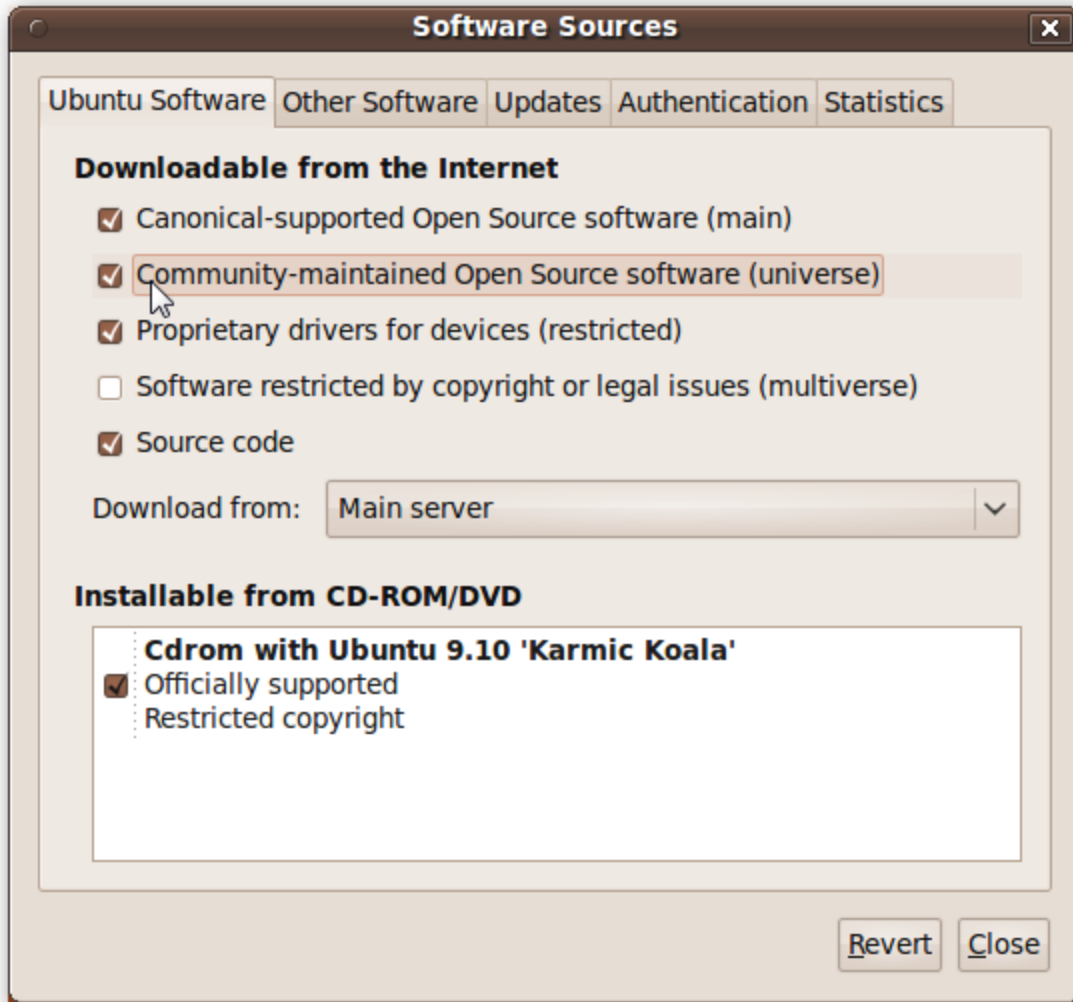


**chntpw** is found in the *universe* repository. Repositories are a way for Ubuntu to group software together so that users are able to choose if they want to use only completely open source software maintained by Ubuntu developers, or branch out and use software with different licenses and maintainers.

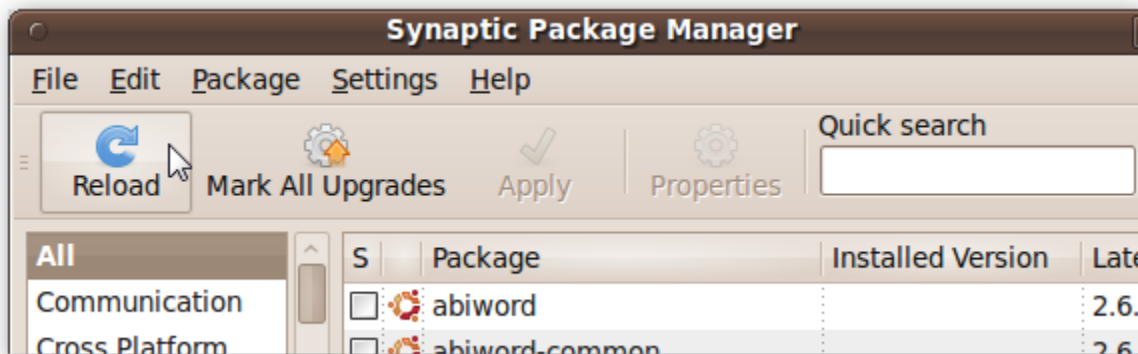
To enable software from the *universe* repository, click on Settings > Repositories in the Synaptic window.



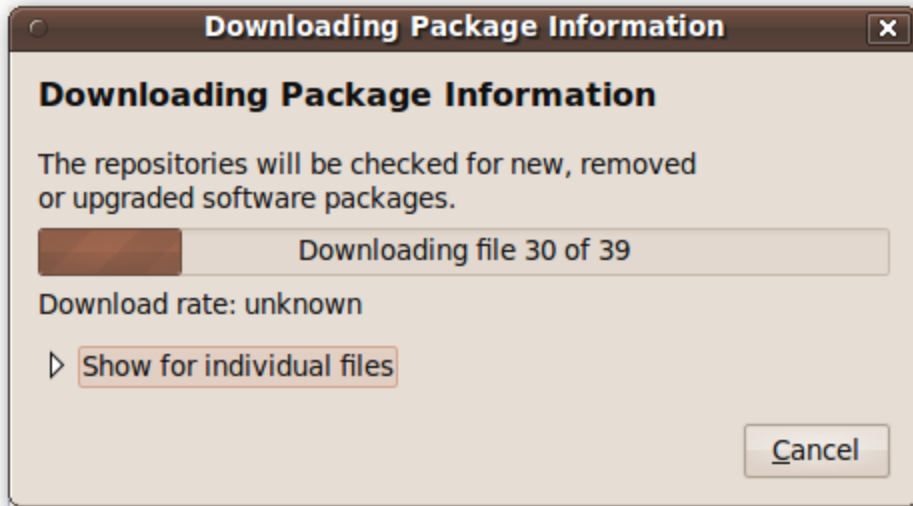
Add a checkmark beside the box labeled “Community-maintained Open Source software (universe)” and then click close.



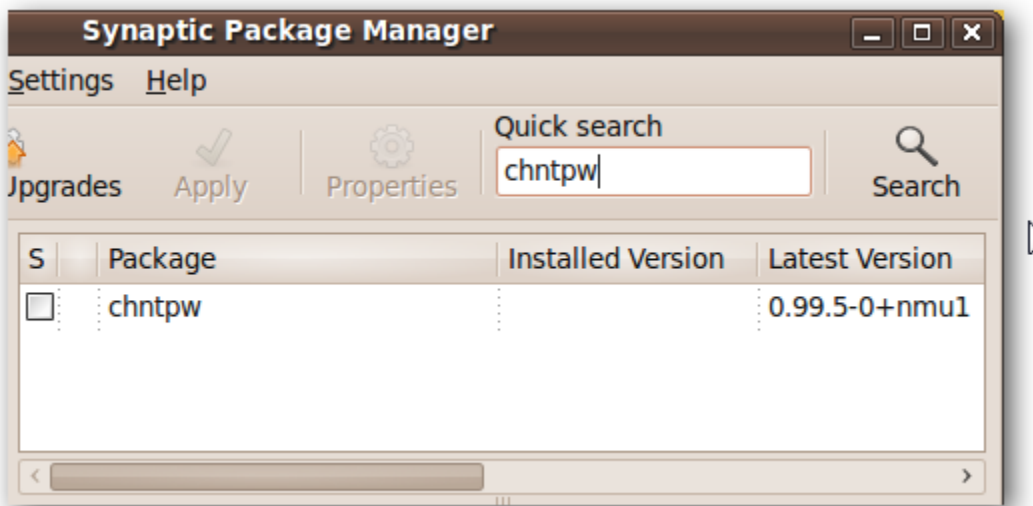
When you change the repositories you are selecting software from, you have to reload the list of available software. In the main Synaptic window, click on the Reload button.



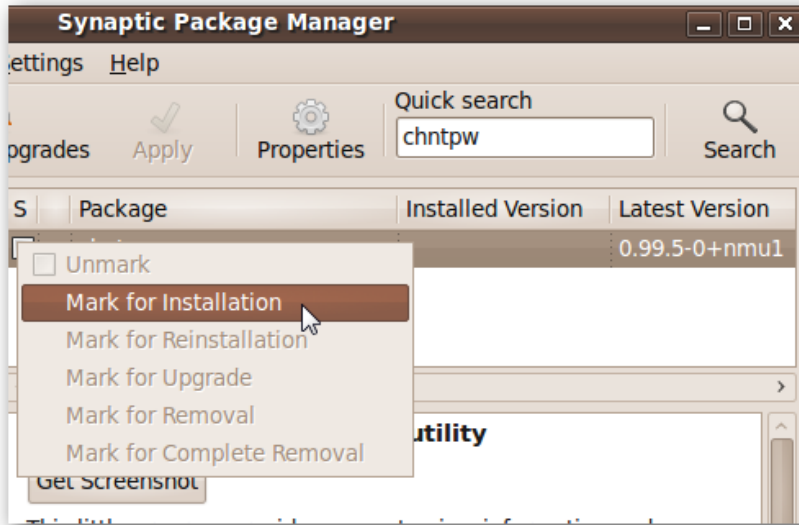
The software lists will be downloaded.



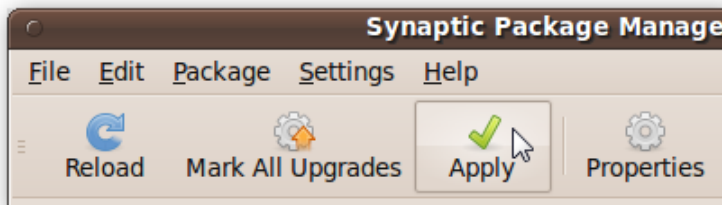
Once downloaded, Synaptic must rebuild its search index. The label over the text field by the Search button will read "Rebuilding search index." When it reads "Quick search," type **chntpw** in the text field. The package will show up in the list.



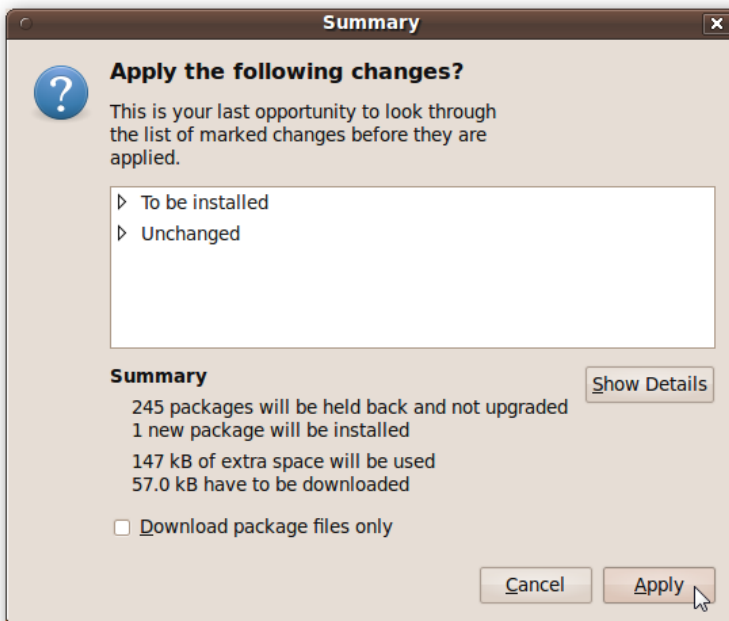
Click on the checkbox near the **chntpw** name. Click on Mark for Installation.



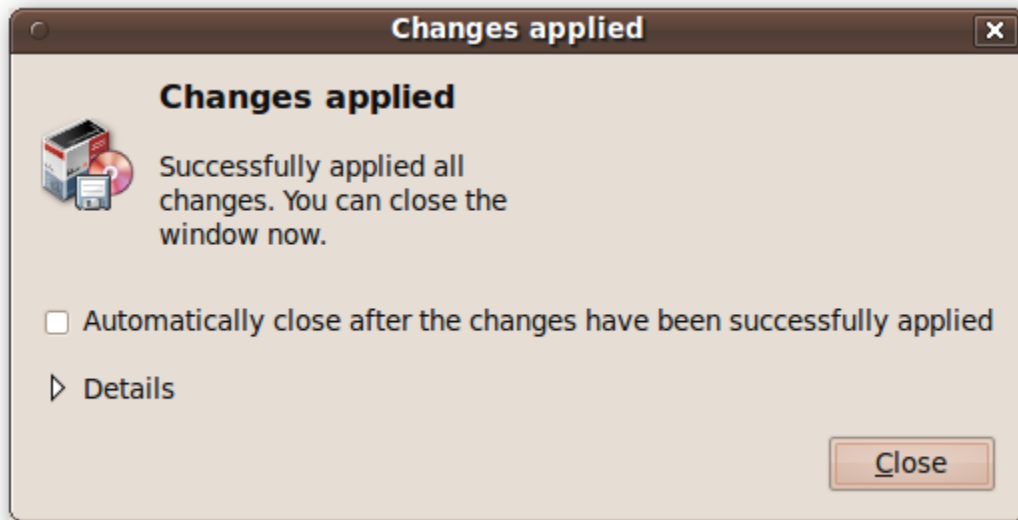
**chntpw** won't actually be installed until you apply the changes you've made, so click on the Apply button in the Synaptic window now.



You will be prompted to accept the changes. Click Apply.



The changes should be applied quickly. When they're done, click Close.

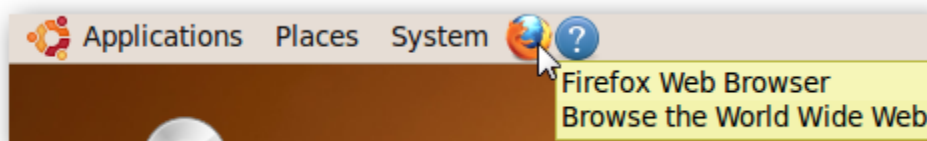


**chntpw** is now installed! You can close Synaptic Package Manager. Skip to the section titled **Using chntpw to reset your password.**

### Installation: 64-bit

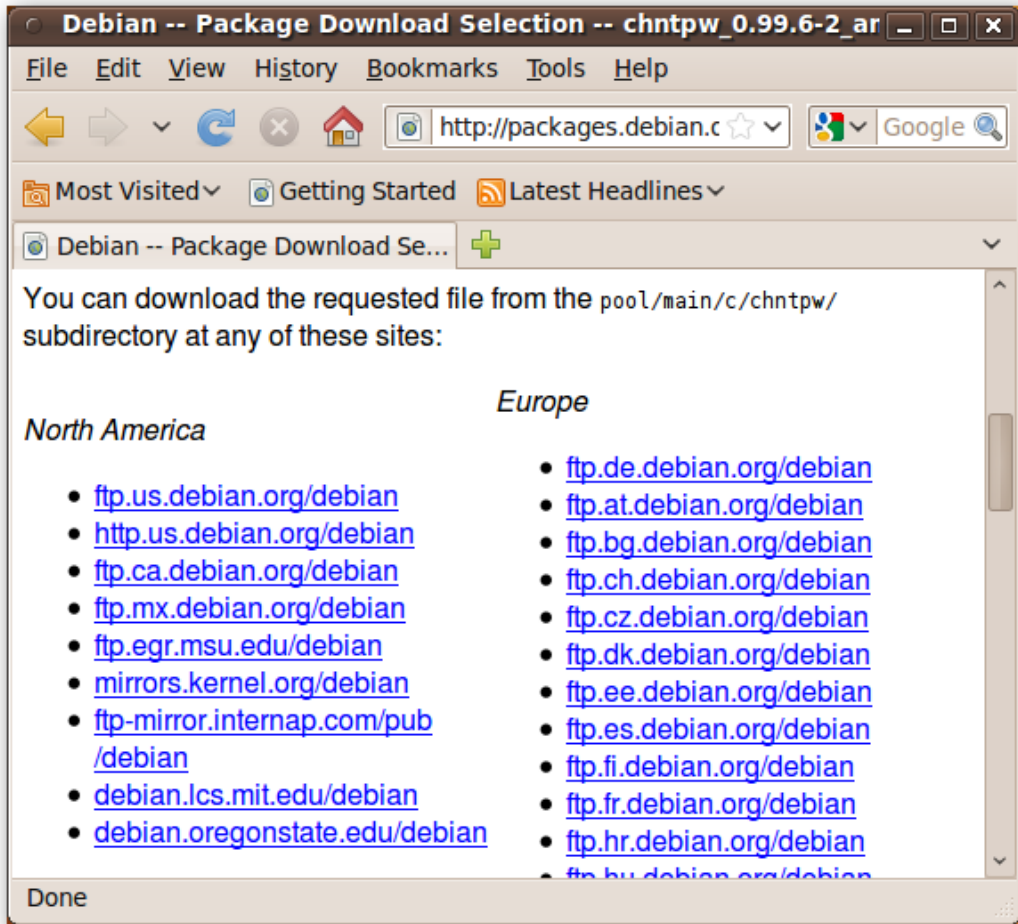
The version of **chntpw** available in Ubuntu's *universe* repository will not work properly on a 64-bit machine. Fortunately, a patched version exists in Debian's Unstable branch, so let's download it from there and install it manually.

Open Firefox. Whether it's your preferred browser or not, it's very readily accessible in the Ubuntu Live CD environment, so it will be the easiest to use. There's a shortcut to Firefox in the top panel.

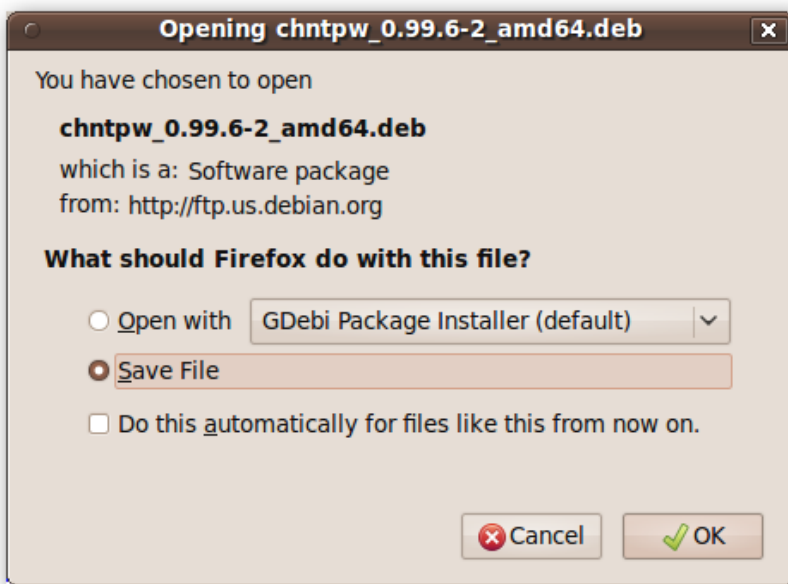


Navigate to <http://packages.debian.org/sid/amd64/chntpw/download> and download the latest version of **chntpw** for 64-bit machines.

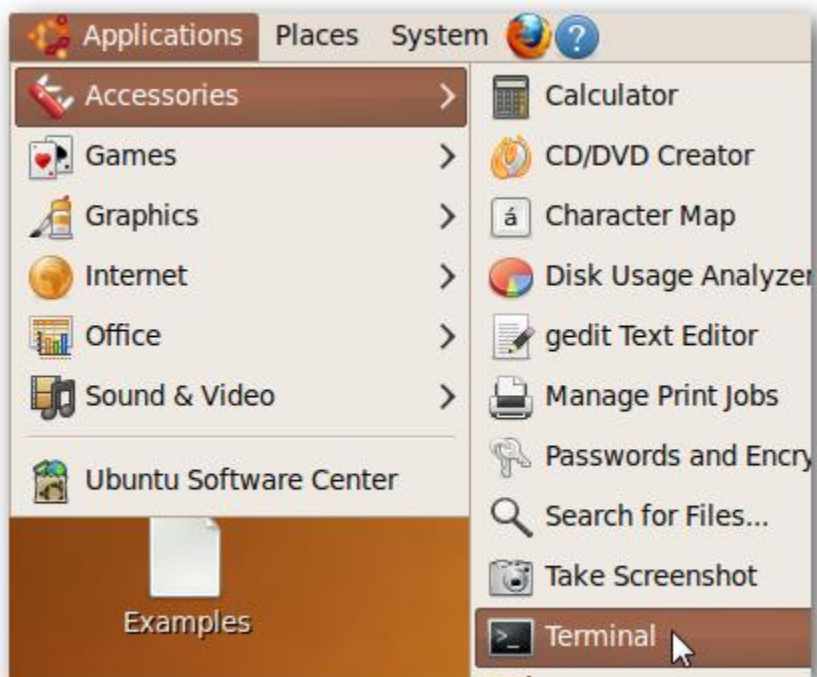
*Note: In most cases it would be best to add the Debian Unstable branch to a package manager, but since the Live CD environment will revert to its original state once you reboot, it'll be faster to just download the .deb file.*



Save the .deb file to the default location.



You can close Firefox if desired. Open a terminal window by clicking on Applications at the top-left of the screen, expanding the Accessories folder, and clicking on Terminal.



In the terminal window, enter the following text, hitting enter after each line:

```
cd Downloads
sudo dpkg -i chntpw*
```

A screenshot of a terminal window titled 'ubuntu@ubuntu: ~/Downloads'. The terminal shows the following commands and output:

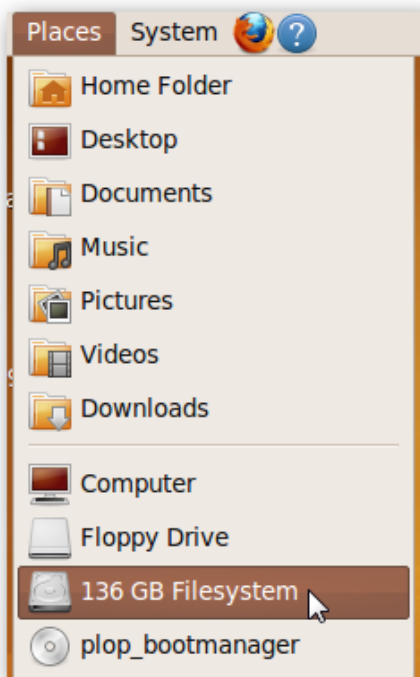
```
ubuntu@ubuntu:~$ cd Downloads
ubuntu@ubuntu:~/Downloads$ sudo dpkg -i chntpw*
Selecting previously deselected package chntpw.
(Reading database ... 118836 files and directories currently installed
.)
Unpacking chntpw (from chntpw_0.99.6-2_amd64.deb) ...
Setting up chntpw (0.99.6-2) ...
Processing triggers for man-db ...
ubuntu@ubuntu:~/Downloads$
```

**chntpw** will now be installed.

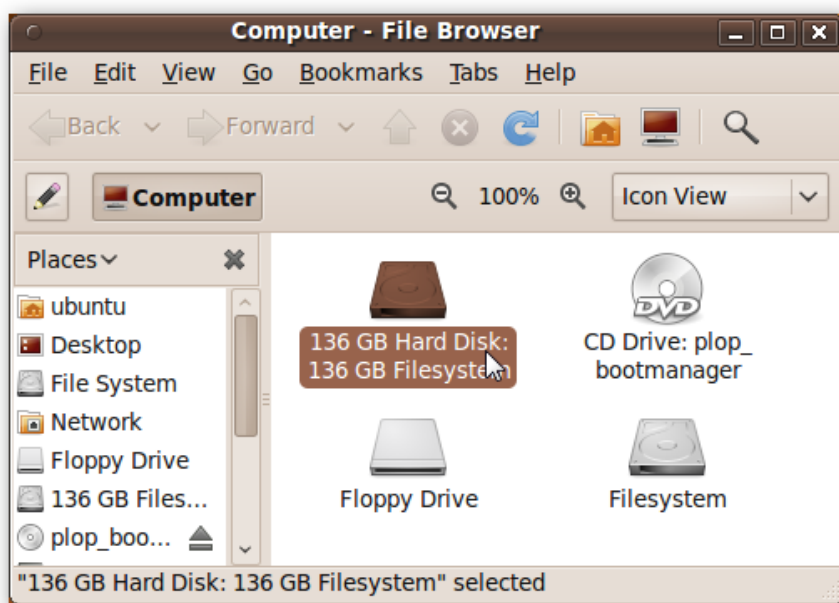
**Using chntpw to reset your password**

Before running **chntpw**, you will have to *mount* the hard drive that contains your Windows installation. In most cases, Ubuntu 9.10 makes this simple.

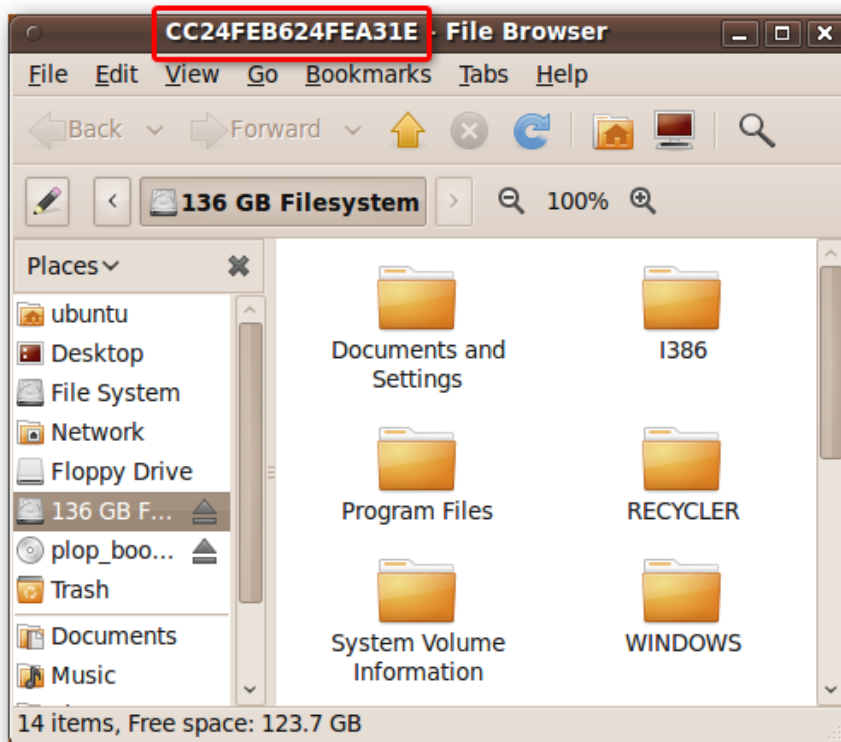
Click on Places at the top-left of the screen. If your Windows drive is easily identifiable – usually by its size – then left click on it.



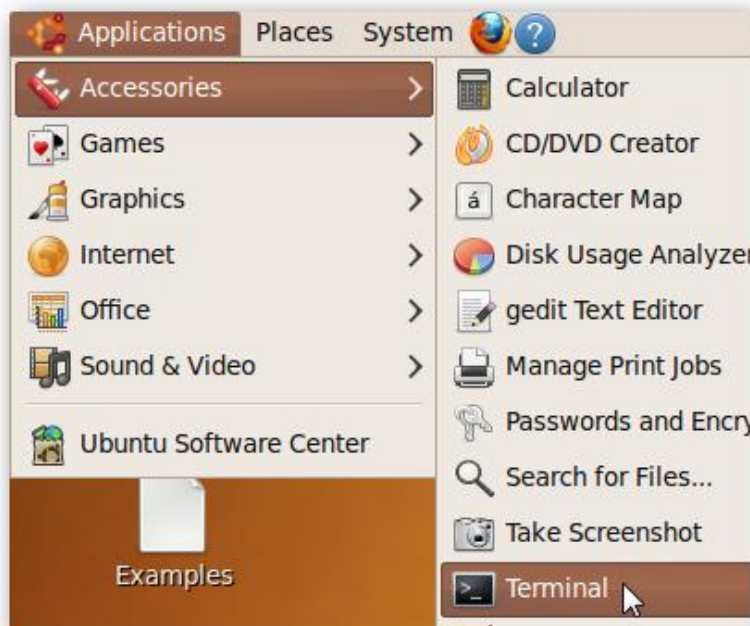
If it is not obvious, then click on Computer and check out each hard drive until you find the correct one.



The correct hard drive will have the WINDOWS folder in it. When you find it, make a note of the drive's label that appears in the menu bar of the file browser.



If you don't already have one open, start a terminal window by going to Applications > Accessories > Terminal.



In the terminal window, enter the commands

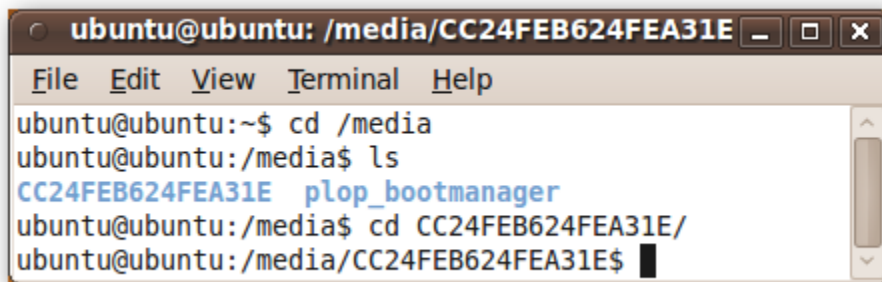
```
cd /media  
ls
```

pressing enter after each line. You should see one or more strings of text appear; one of those strings should correspond with the string that appeared in the title bar of the file browser earlier.

Change to that directory by entering the command

```
cd <hard drive label>
```

Since the hard drive label will be very annoying to type in, you can use a shortcut by typing in the first few letters or numbers of the drive label (capitalization matters) and pressing the Tab key. It will automatically complete the rest of the string (if those first few letters or numbers are unique).

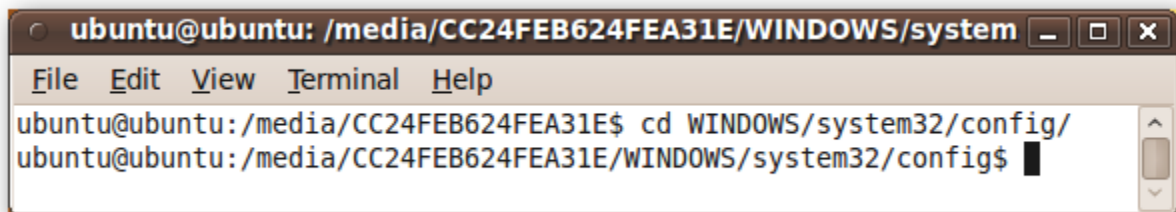
A terminal window titled 'ubuntu@ubuntu: /media/CC24FEB624FEA31E' with a menu bar (File, Edit, View, Terminal, Help). The terminal shows the following commands and output:

```
ubuntu@ubuntu:~$ cd /media  
ubuntu@ubuntu:/media$ ls  
CC24FEB624FEA31E  plop_bootmanager  
ubuntu@ubuntu:/media$ cd CC24FEB624FEA31E/  
ubuntu@ubuntu:/media/CC24FEB624FEA31E$
```

We want to switch to a certain Windows directory. Enter the command:

```
cd WINDOWS/system32/config/
```

Again, you can use tab-completion to speed up entering this command.

A terminal window titled 'ubuntu@ubuntu: /media/CC24FEB624FEA31E/WINDOWS/system' with a menu bar (File, Edit, View, Terminal, Help). The terminal shows the following commands and output:

```
ubuntu@ubuntu:/media/CC24FEB624FEA31E$ cd WINDOWS/system32/config/  
ubuntu@ubuntu:/media/CC24FEB624FEA31E/WINDOWS/system32/config$
```

To change or reset the administrator password, enter:

```
sudo chntpw SAM
```

SAM is the file that contains your Windows registry. You will see some text appear, including a list of all of the users on your system.

```
ubuntu@ubuntu: /media/CC24FEB624FEA31E/WINDOWS/system
File Edit View Terminal Help
ubuntu@ubuntu:/media/CC24FEB624FEA31E/WINDOWS/system32/config$ sudo chntpw SAM
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: 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: 230/18072 blocks/bytes, unused: 12/2248 blocks/bytes.

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

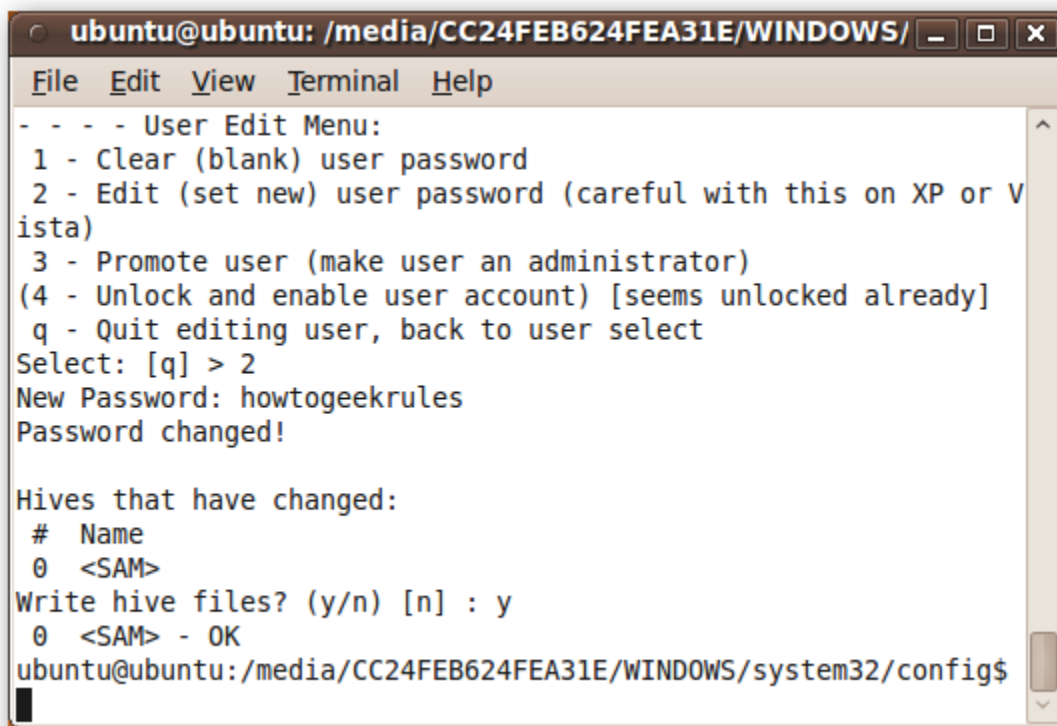
| RID - |----- Username -----| Admin? | - Lock? - |
| 01f4 | Administrator           | ADMIN  |           |
| 01f5 | Guest                   |        | dis/lock  |
| 03ec | HelpAssistant           |        | dis/lock  |
| 03ea | SUPPORT_388945a0        |        | dis/lock  |
| 03eb | XPMUser                 | ADMIN  | dis/lock  |
```

At the bottom of the terminal window, you should see a prompt that begins with “User Edit Menu:” and offers four choices. We recommend that you clear the password to blank (you can always set a new password in Windows once you log in). To do this, enter “1” and then “y” to confirm.

```
ubuntu@ubuntu: /media/CC24FEB624FEA31E/WINDOWS/system
File Edit View Terminal Help
- - - 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

Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
ubuntu@ubuntu:/media/CC24FEB624FEA31E/WINDOWS/system32/config$
```

If you would like to change the password instead, enter “2”, then your desired password, and finally “y” to confirm.

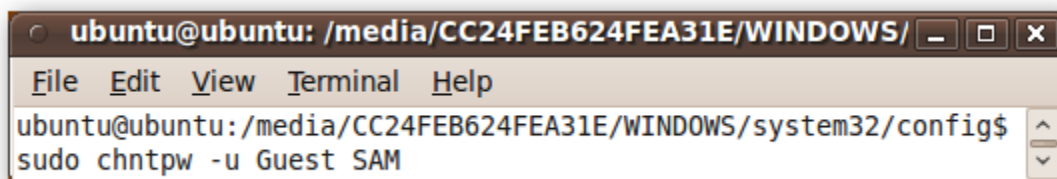


```
ubuntu@ubuntu: /media/CC24FEB624FEA31E/WINDOWS/
File Edit View Terminal Help
- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
q - Quit editing user, back to user select
Select: [q] > 2
New Password: howtogeekrules
Password changed!

Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
ubuntu@ubuntu:/media/CC24FEB624FEA31E/WINDOWS/system32/config$
```

If you would like to reset or change the password of a user other than the administrator, enter:

```
sudo chntpw -u <username> SAM
```



```
ubuntu@ubuntu: /media/CC24FEB624FEA31E/WINDOWS/
File Edit View Terminal Help
ubuntu@ubuntu:/media/CC24FEB624FEA31E/WINDOWS/system32/config$
sudo chntpw -u Guest SAM
```

From here, you can follow the same steps as before: enter “1” to reset the password to blank, or “2” to change it to a value you provide.

```
ubuntu@ubuntu: /media/CC24FEB624FEA31E/WINDOWS/
File Edit View Terminal Help
- - - - 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

Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
ubuntu@ubuntu:/media/CC24FEB624FEA31E/WINDOWS/system32/config$
```

And that's it!