System Administration

**Automating Tasks**

* Cron is a system daemon that runs tasks in the background according to instructions found in a crontab file. To edit the crontab file for the current user:

crontab -e

Tasks that normally require administrative (sudo) privileges should be added to the root user's crontab:

sudo crontab -e

Add commands using the format specified [here](http://pubs.opengroup.org/onlinepubs/9699919799/utilities/crontab.html) (or see the [Ubuntu Community Help](https://help.ubuntu.com/community/CronHowto)). The crontab command format can also be found using:

man crontab

* Scheduled/automated tasks (cron events) can also be edited using the [GNOME schedule](http://gnome-schedule.sourceforge.net/) GUI interface.

Menu -> System -> Administration -> Task Scheduler

* If the GNOME Schedule task scheduler is not installed, install it:

sudo apt-get install gnome-schedule

**Boot Menu**

**Login Menu settings**

You can change the Login menu settings from the GUI interface:

Menu -> System -> Administration -> Login Manager

You can choose an integrated theme or select individual components of the login screen/process.

**Automating bootup options**

[StartupManager](http://ubuntuguide.org/wiki/Ubuntu:Precise#Use_Startup_Manager_to_change_Grub_settings) is a GUI to manage settings for Grub (Grub Legacy), Grub 2, Usplash, and Splashy.

**GRUB boot manager settings**

**Grub2**

Precise comes with [Grub2](http://www.gnu.org/software/grub/manual/grub.html), a difficult boot manager to customize. (Grub2 is also known as grub-pc.) See the evolving instructions at the [Ubuntu wiki](https://wiki.ubuntu.com/Grub2) or [Ubuntu forums](http://ubuntuforums.org/showthread.php?t=1195275). In brief, some settings can be edited:

sudo nano /etc/default/grub

sudo grub-mkconfig --output=/boot/grub/grub.cfg

Alternatively, use the command:

sudo update-grub

**Grub2 background image, colors, fonts**

* See [this Ubuntu Forums thread](http://ubuntuforums.org/showthread.php?p=10720685#post10720685).
* Any background image can be used for Grub2 by placing the image in the /boot/grub folder and then reconfiguring Grub2:

sudo update-grub

The image ought to be the same size as the Grub2 startup resolution specified in /etc/default/grub (e.g. 1024x768).

* A selection of splashimages can be installed into the /usr/share/images/grub folder:

sudo apt-get install grub2-splashimages

* One of the images can be linked to the /boot/grub folder and used as the splash image. For example:

sudo ln -s /usr/share/images/grub/Plasma-lamp.tga /boot/grub

sudo update-grub

**Change the default menu item**

* There are several ways to [change the default Grub2](https://help.ubuntu.com/community/Grub2#A.2BAC8-etc.2BAC8-grub.d.2BAC8_.28directory.29) menu item, but only one is reliable. The menu items in Grub2 change name and position in the list with every kernel upgrade. However, if you choose the default menu item by name, you can reliably set it as the default. For example, if you wish to boot a Windows OS as the default and the Grub 2 menu lists it as *Microsoft Windows 98SE Ancient Edition (on /dev/sda1)* then edit /etc/default/grub:

sudo kate /etc/default/grub

and change the entry to resemble:

GRUB\_DEFAULT="Microsoft Windows 98SE Ancient Edition (on /dev/sda1)"

then regenerate the Grub2 config file:

sudo update-grub

To find out the names of the menu items, use:

sudo grep menuentry /boot/grub/grub.cfg

* Note: There is a bug in Grub2 v.1.99 such that if the GRUB\_DEFAULT option is used, the Grub2 menu can not be entered (for manually selecting a menu item). If the default option is a non-Linux OS, there will then be no way start a Linux OS (and therefore no way to subsequently change the /etc/default/grub configuration file). Use this option with great care.

**Protecting Grub2 from cracking**

* See [this section of the Grub Manual](http://www.gnu.org/software/grub/manual/grub.html#Security) for important information on securing Grub2.
* To add password protection, in the /etc/grub.d/40\_custom configuration file, add the lines:

set superusers="*user1*"

#password\_pbkdf2 *user1* *grub.pbkdf2.sha512.10000.biglongstring*

password *user1* *insecurecleartextpassword*

and change your password to something other than *insecurecleartextpassword*, or use the pbkdf2-encrypted method described [here](http://www.gnu.org/software/grub/manual/grub.html#Security). You can then password-lock menu items as well. For detailed info see [this blog](http://www.panoet.com/set-grub-2-password-protection-149).

**GRUB Legacy**

The older version of GRUB ("[Grub Legacy](http://www.gnu.org/software/grub/manual/legacy/grub.html)") is available, for use with a boot partition, for example. Install:

sudo apt-get install grub

* If you have [multiple operating systems (OS)](http://ubuntuguide.org/wiki/Multiple_OS_Installation) on your computer, you may be using the GRUB Legacy boot manager (in a boot partition, for example). You can edit the options for GRUB Legacy in the menu.lst configuration file. (See [this detailed info](http://ubuntuguide.org/wiki/Multiple_OS_Installation#Changing_main_Grub_boot_menu_settings).)

sudo nano /boot/grub/menu.lst

(gedit can also be used instead of nano as the text editor.)

**Chainloading Grub2 from Grub Legacy**

* To chainload Grub2 (installed in this example with the OS in the */dev/sda7* partition) from Grub Legacy (stored in a boot partition, for example), use an entry of this format in the Grub Legacy /boot/grub/menu.lst configuration file:

title (K)Ubuntu Precise OS (chainloader)

rootnoverify *(hd0,6)*

chainloader +1

* Grub2 is erratic, however. In many situations I don't bother to chainload it at all. Instead, it is possible to bypass Grub2 entirely and load the OS directly using Grub Legacy (stored in a boot partition, for example) using an entry in /boot/grub/menu.lst of the format:

title (K)Ubuntu Oneiric OS (chainloader)

rootnoverify *(hd0,6)*

kernel /vmlinuz root=*/dev/sda7* ro

initrd /initrd.img

* My old method for chainloading Grub2 (installed in this example in the */dev/sda7* partition) from Grub Legacy used an entry in the Grub Legacy configuration file (/boot/grub/menu.lst) with this format:

title (K)Ubuntu Maverick OS (chainloader)

rootnoverify *(hd0,6)*

kernel /boot/grub/core.img

This method, however, requires a current core.img to have been created with grub-mkimg (part of the grub-install process). When there are substantial changes to the partition or the kernel, the core.img must be re-created by re-installing Grub2 into the OS partition (in this example */dev/sda7* corresponds to *(hd0,6)* ):

sudo grub-install */dev/sda7*

**Protecting Grub Legacy from cracking**

* See [this section of the Grub Manual](http://www.gnu.org/software/grub/manual/legacy/grub.html#Security) for important information on securing Grub Legacy.
* To add password protection, in the /boot/grub/menu.lst configuration file, uncomment (remove the hashmark) from the line:

#password *topsecret*

and change your password to something other than *topsecret*, or use the md5-encrypted method described [here](http://www.gnu.org/software/grub/manual/legacy/grub.html#Security). You can then password-lock menu items by adding the descriptor*lock* below the title of any item menu.