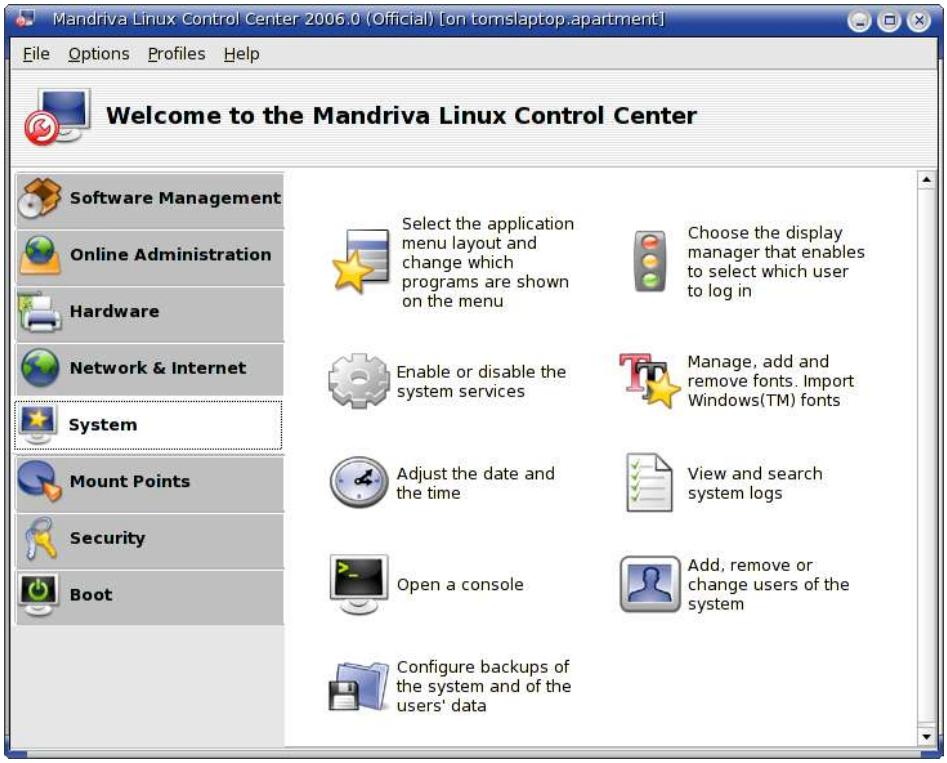
User and Group Administration

When you begin to administer Linux, one of the most important things to know is how to administer users and groups. Scripts, programs, and configuration files use permissions to keep from being used the wrong way and/or from being used by the wrong person/application. Basically, permissions means what user or what group of users are allowed to read, write, and/or execute a file. There are plenty of tutorials and books on Linux security, so I won't go in to depth in explaining this massive topic. Instead, let's look at how to view, add, and delete users and groups.

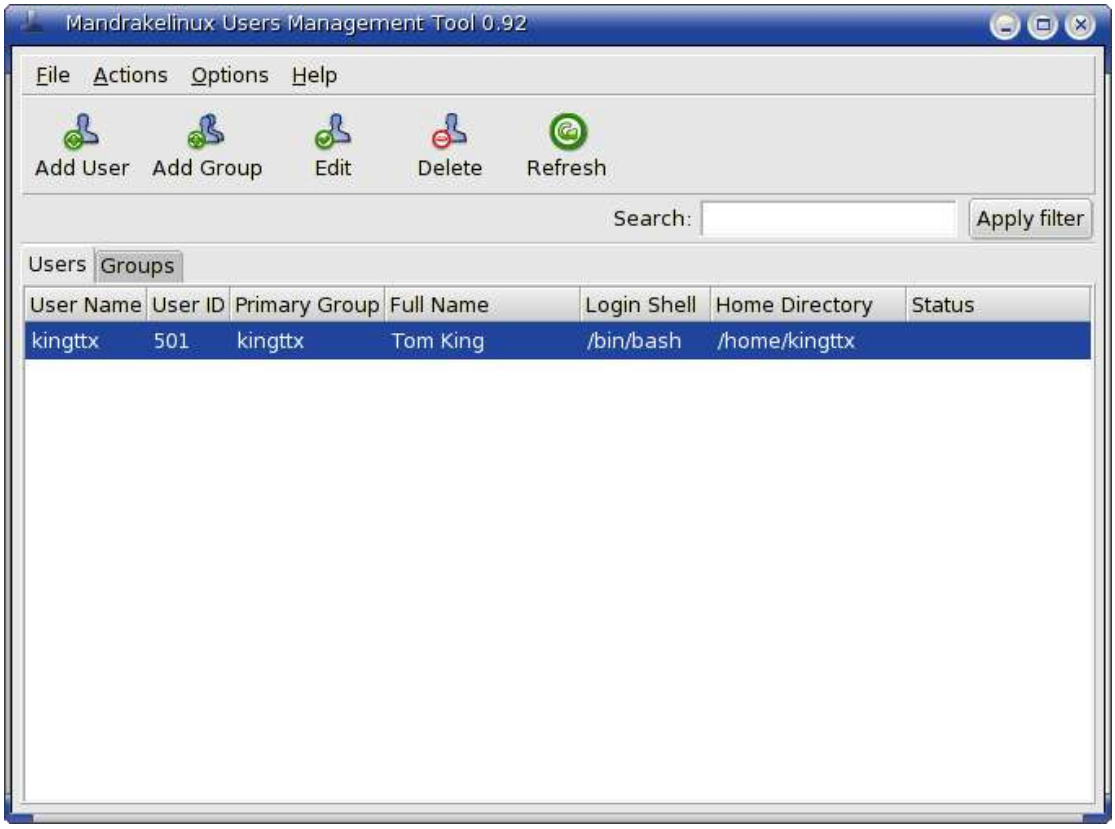
First, access the user/group administration applet by clicking the K-menu > System > Configuration > Other > User Administration.

Alternatively, use the Mandriva Control Center (K-menu > System > Configuration > Configure Your Computer).



The Mandrakelinux Users Management Tool will appear. First, let's go over the tabs.

The **Users** tab, of course, lists all current users, and you use this tab to edit existing users as well.



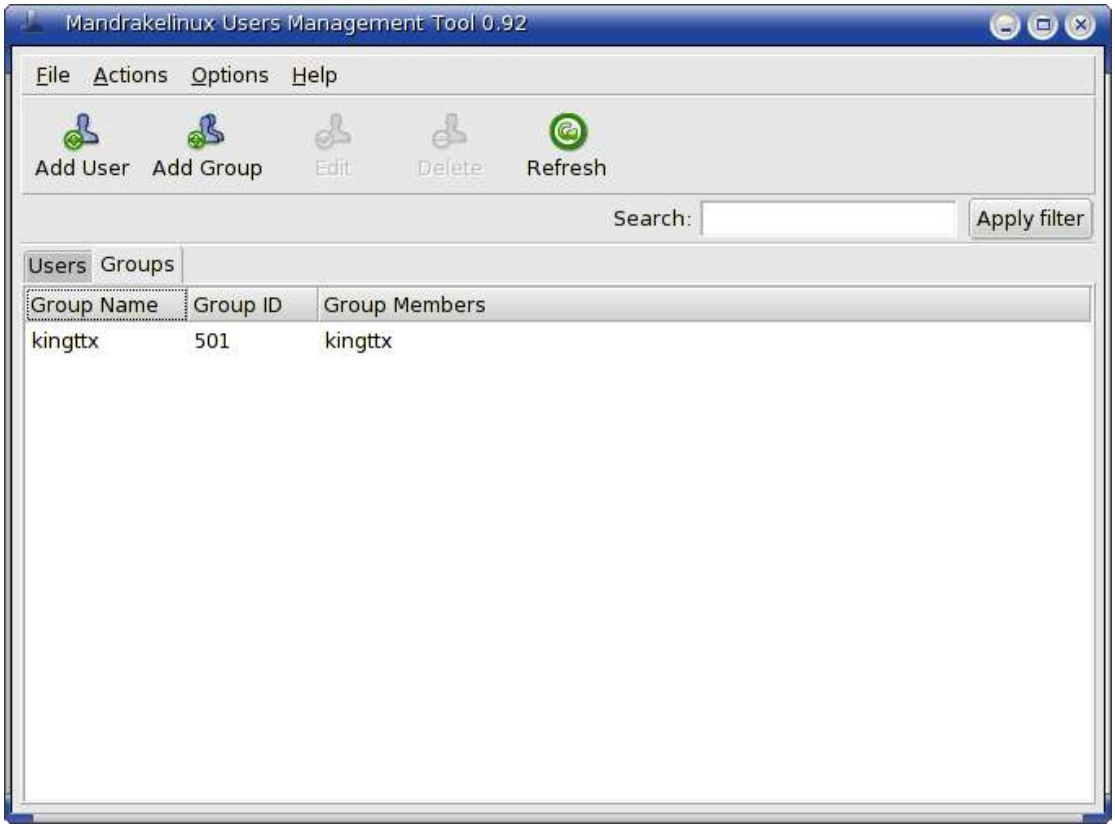
Highlight a use and click “Edit”. A popup will appear with the highlighted user's information ready for editing. The first tab, **User Data**, give the full name, login name, password (with confirmation), the login shell (bash in this case), and the location of the user's home directory if it exists. Note: This information comes from the file /etc/passwd.

The next tab in this popup is **Account Info**, where you can set an account to expire on a certain date (useful for temporary accounts), lock an account, or change the user's icon. It's probably good practice to lock an account instead of deleting one if they have a lot of files. Doing so will allow you to simply change the user login and other information, and the new user takes ownership of the old user's files if need be. For some homework, look up User ID's (UIDs).

The next tab, **Password Info**, allows you to enable password expiration. Once you have enabled this feature, the rest of the areas will open for editing. “Days before change allowed” sets a minimum amount of time before the password can be changed again by the user. “Days before change required” sets the amount of time before the user must change their password. In most environments, it's best to change passwords every 30-45 days. “Days warning before change” sets the amount of time before “Days before change required” where the user will begin to receive prompts that their password is about to expire. Finally, “Days before account inactive” sets the amount of time after a password has expired that an account will be locked if it is inactive. Once locked, the user must check with the system administrator to unlock the account.

The last tab in this popup is **Groups**, which lists all groups this use is a member of. Users should not be members of daemon groups, such as haldaemon shown in this figure.

Back on the main page, the next tab is **Groups**, not to be confused with the **Groups** tab from the user's edit. This tab lists all current user groups. In most cases, user group ID's start at 500, same as user accounts.



Highlight a group, and then press Edit. Here, you receive the popup to edit group information. The first tab, **Group Data**, has a single field, the group name.

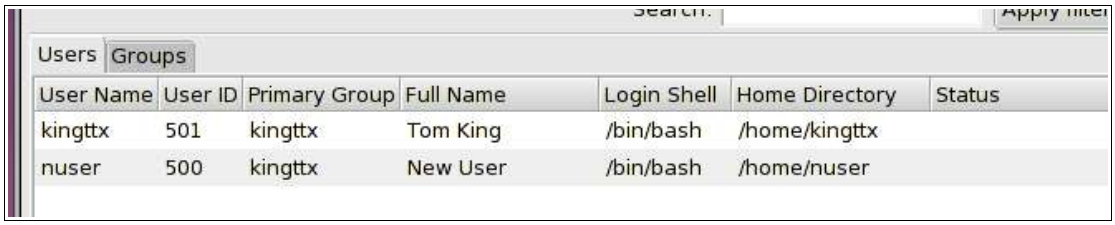
The **Group Users** tab lists all users that are a member of this group. You can add users to this group as well from this tab. Again, don't add daemons, such as haldaemon, to a user group. If you are not sure, add only users listed in the **Users** tab to a user group.

Let's add a user, “New User”, with a login “nuser”, a password of abc123abc, use the bash shell, have a home directory under /home/nuser, its own private group, and specify UID 502. Under any tab, click “Add User”. Here you will find that information in the following figure.

If you do not select “Create Home Directory”, one will not be created. If you do not select “Create a private group for this user”, the user will be added to the “users” group, although you can change that by editing this user which we will do for this example. Not selecting “Specify user ID manually” will give this user the next higher UID. There are cases each of these would or would not be used. For example, if you want all users in Accounting to be part of the accounting group, you'd de-select “Create a private group for this user”, then change their primary group by editing the user information.

You could also keep them in the users primary group, but add them in the Accounting group edit. Assuming you have an Accounting group, go to the **Groups** main tab, then click on Edit.

In this case, I've added nuser to the kingttx group instead. See the information below in the **Users** tab.



Now, any file or directory for which the “kingttx” group has permissions, nuser will also have permissions. Remember that permissions under the user can be different than permissions under the group. For example, I could have a script that has read, write, and execute permissions under the user kingttx, but only read under the kingttx group. Therefore, nuser would only have read permissions.

In addition to the user (owner) and group permissions, there is the “others” permissions, which are the permissions for any user or group that is not the owner or is not a member of the group.

You will want to research Linux security, especially user and group permissions, to fully understand what can/should be done or not done.

Now that we have finished with this introduction to the user applet, I'm going to delete the New User account. The applet will give you a popup with a couple of options you'll want to know about. You have the options to delete the home directory for this user, and/or to delete the user's mailbox (/var/spool/mail/nuser). Be sure you do not select either of these if you might have files or emails that are needed by anyone else. Once you hit delete, the user will be deleted, along with either of the two locations you enable from this popup.