CHAPTER 4

Users and Groups

This chapter is devoted to the Users and Groups module, which allows you to create and manage UNIX user accounts and UNIX groups.

4.1 Introduction to UNIX Users and Groups

On Linux and other UNIX operating systems, a user is a person who can login to the system via SSH, telnet, FTP or at the console. Users can also receive email and own files on the server's local filesystems. Each user has a login name, a password, and a home directory in which all its files are stored. Users also have several additional attributes, such as a real name, shell (the program that is run when the user logs in), and expiry date.

Each user is a member of at least one group, called a primary group. In addition, a user can be a member of an unlimited number of secondary groups. Group membership can be used to control the files that a user can read and edit. For example, if two users are working on the same project you might put them in the same group so they can both edit a particular file that other users cannot access.

Every system will have several standard user accounts like `root` and `nobody` that are created when the system is installed—although most of these (except for `root`) cannot be used to login. If your server will be used by more than one person, you will need to create an additional user account for each person to keep their files and email separate. Even if you are the only person who uses your machine, it is a good idea to create a user account for yourself that you use to login with instead of using the `root` account.

Depending on your operating system, user and group information will be stored in different files in the `/etc` directory. On modern versions of Linux, `/etc/passwd` and `/etc/shadow` are used to store user details, and `/etc/group` for group details. The Users and Groups module works by directly editing those files, not by calling any external programs or functions. This means that if you are using NIS or storing users in an LDAP server, this module is not for you.

4.2 The Users and Groups Module

The Webmin module Users and Groups that is found under the **System** category (as shown in Figure 4.1) can be used to create, edit, and delete all the UNIX users and groups on your system. You should always be careful when using this module to edit existing system users like `root` and `daemon` because changing or deleting them could stop your system from working. Some users have their home directory set to / (the root directory). Deleting such a user would cause all the files on your system to be deleted!

In addition to managing the UNIX users on your system, this module can also affect user settings in other modules. For example, Samba has its own list of users and passwords that should be kept in sync with the UNIX password list. Webmin can handle this for you automatically using the **other modules** option that appears on the user creation, editing, and deletion forms. You must, however, enable this in every other module that you want automatically updated. The module also

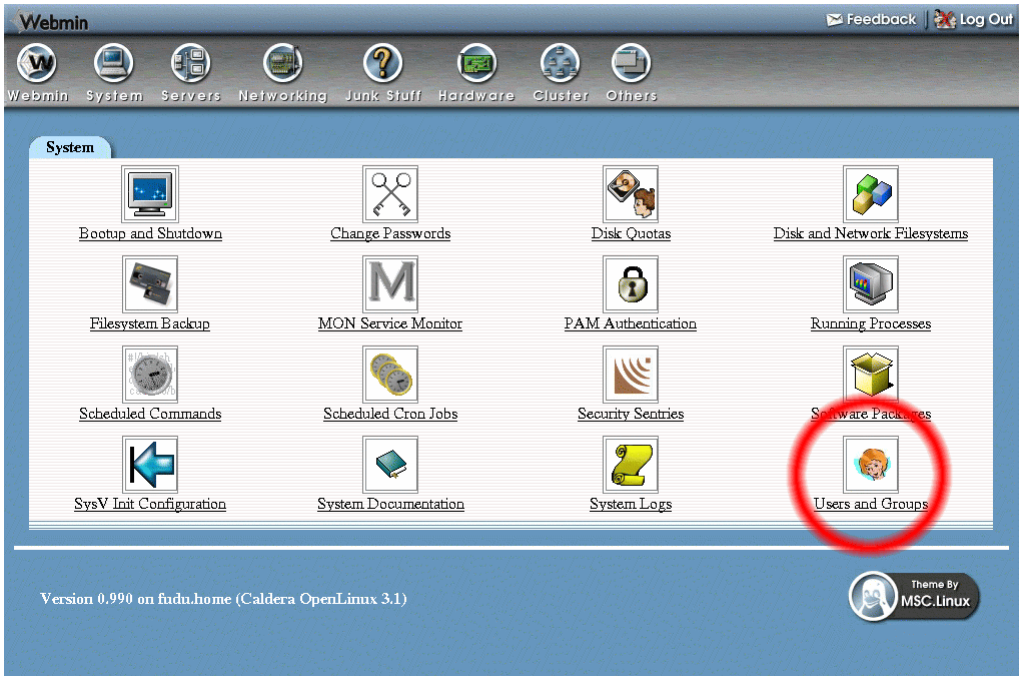


Figure 4.1 The Users and Groups module icon.

has options for synchronizing UNIX groups in a similar way, such as with Samba groups. However, since this feature only works with Samba 3.0, which is still under development, it is not covered in this chapter.

Once you enter the module, the main page lists all the users that currently exist on your system in one table (Figure 4.2), and all the groups in another (Figure 4.3). If there are too many users or groups to sensibly display in a table, then a small form allowing you to search for a user or group will be displayed instead.

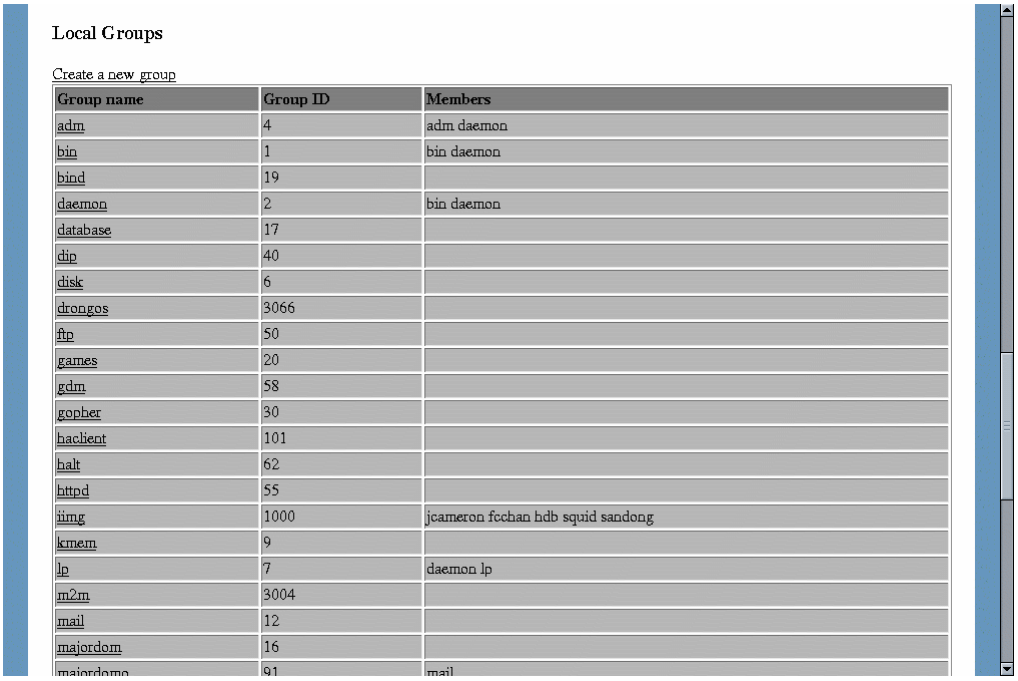
Figure 4.2 List of existing users.

4.3 Creating a New User

To create a new UNIX user, complete the following steps:

1. Click on the **Create a new user link** above or below the table of existing users. A form for entering the details of the new user will appear, as shown in Figure 4.4.
2. At this point you have to decide on a username for the new user, which should be something simple without spaces in it—like *jcameron* or *jamie*—and not used by any other user. If your server is receiving email, the username determines the part of the user's email address to the left of the @. Enter your choice in the **Username** field.
3. The **User ID** field should generally be left unchanged, as it is worked out for you by Webmin. If you set it to the same user ID as another user, they will be able to access each other's files. This is generally not a good idea.
4. In the **Real name** field, you should enter the user's full name, such as *Jamie Cameron*.
5. Every user has a home directory, in which the user stores his personal documents and preference files. In the **Home directory** field, you should enter a directory that does not exist yet, such as */home/jcameron*. When the user is created, this directory will be created and its ownership granted to the new user.

   If Webmin on your system offers an **Automatic** option for the home directory, it is generally best to stick with that.
6. The user's shell is a program that is run when he makes a text mode login of some kind (via SSH, for example), or opens a shell prompt after logging in graphically at the con-



Local Groups

Create a new group

Group name	Group ID	Members
adm	4	adm daemon
bin	1	bin daemon
bind	19	
daemon	2	bin daemon
database	17	
dip	40	
disk	6	
drongos	3066	
ftp	50	
games	20	
gdm	58	
gopher	30	
haclient	101	
halt	62	
httpd	55	
iimg	1000	jcameron fcchan hdb squid sandong
kmem	9	
lp	7	daemon lp
m2m	3004	
mail	12	
majordom	16	
majordomo	91	mail

Figure 4.3 List of existing groups.

sole. The shell is responsible for running the commands that you type (such as `ls` and `cat`), running scripts on login and logout, and providing an interface for command editing. Shells like `bash` and `tcsh` are easier for users to use, because they allow the up and down arrows to be used to scroll through previous commands, and the tab key to autocomplete commands and filenames.

In some cases, you might not want a user to be able to make a shell login at all, as in when the user is only meant to be able to read and send email. In that case, his shell should be set to `/bin/false`, which is a program that does nothing and exits immediately.

You should select whatever shell you want the user to have from the list in the **Shell** field. If your choice is not on the list, select the **Other** option and enter the path to the shell in the field below.

7. For the **Password** field, you have four choices:

No password required The user can login without needing to enter any password.

No login allowed The user can never login.

Normal password You get to enter the user's password.

Pre-encrypted password You must enter a password that is already encrypted, such as one taken from the `/etc/shadow` file on another system.

Generally you will want to use the **Normal password** option. Note that on many operating systems, only the first eight characters of the password are actually used.

8. On most systems, a set of inputs under the heading **Password options** will be available. The first of these is the **Expiry date**—if you want the user to be unable to login after a particular date, fill in this field.
9. The **Minimum days** field is the number of days after the user is created or the password is last changed that the user must wait before changing it again. Leave it blank to allow changing as soon as the user wants.
10. The **Maximum days** field is the number of days after the user is created or the password is last changed that the password will expire and need to be changed. A user with this option set will be forced to change his password periodically, which is good for system security. Leave it blank to prevent the password from ever expiring.
11. The **Warning days** field is the number of days before the password expiry date that the user will be warned at login that his password is about to expire. If left blank, the user will not know that his account has expired until he tries to log in and is forced to choose a new password.
12. The **Inactive days** field is the number of days after the password expires that the entire account will be disabled if the user has not chosen a new password. If left empty, the account will never expire.
13. For the **Primary group**, either select an existing group or enter the name of a new one that Webmin will create for you.
14. If you want the user to be a member of more than one group, select some of the groups from the **Secondary group** list.
15. If you want the user's home directory to be created, select the **Create home directory?** option. If the directory does not already exist, you should select this as well as **Copy files to home directory?** so that the user gets a basic set of preference files like `.profile` and `Desktop`.
16. To create the user in other modules that you have configured for such action, select **Create user in other modules?** It is possible to set up the Samba module to automatically create a user in its user list, and the MySQL module to create a new database user, among others.
17. To create the user, click the **Create** button. After a short delay, you will be returned to the list of existing users, which should include your newly created user.

Once the **Create** button has been clicked, the new user will be able to login via SSH, telnet, or whatever other services you have set up

4.4 Editing an Existing User

You can change any of the details of any user that already exists on your system by following these steps:

1. Click on the user you want to edit from the existing list. A form containing all the details of the user will appear, as shown in Figure 4.5.
2. Change any of the details that you want to modify, including the username. The fields have the same meanings as described inSection 4.3 "Creating a New User".
3. If you have modified the **User ID** or changed the **Primary group**, files owned by the user may need to be updated to use the new IDs. The options at the bottom of the page

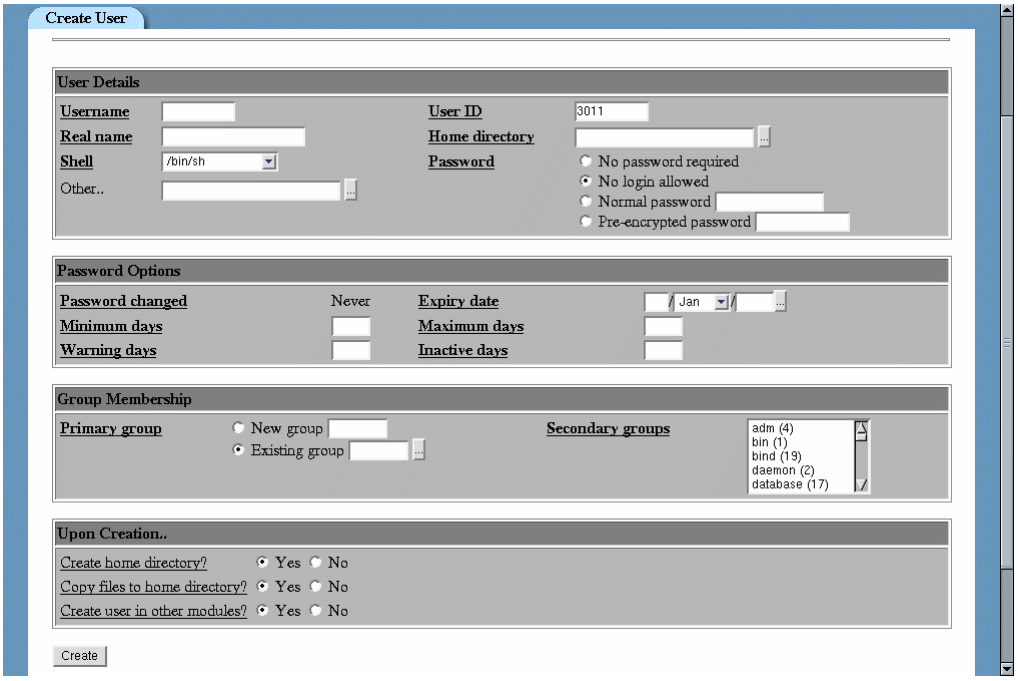


Figure 4.4 The user creation form.

labeled **Change user ID on files?** and **Change group ID on files?** control which directories will be searched for files with the old IDs.

4. If you have changed the user's home directory, you can have Webmin rename it to the new path. However, if the new home directory already exists, this may not always be what you want. The **Move home directory if changed?** option determines if it is moved or not.
5. To have the user updated in other modules where this has been set up, select **Modify user in other modules?** If you are changing the username, this will also rename the user's Sendmail mail file and Cron jobs.
6. Click the **Save** button to have Webmin update the user. Once it is complete, you will be returned to the lists of users and groups.

4.5 Deleting a User

You should always be careful when deleting a user, as important files in the user's home directory may be lost. It is generally never a good idea to delete any of the users that are created when your system is first installed—especially `root`! Even normal users that you have created can be disabled by editing the user and setting the password option to **No login allowed**.

If you still want to go ahead and delete a user, follow these steps:

1. Click on the user you want to edit from the existing list. A form containing all the details of the user will appear, as shown in Figure 4.5.

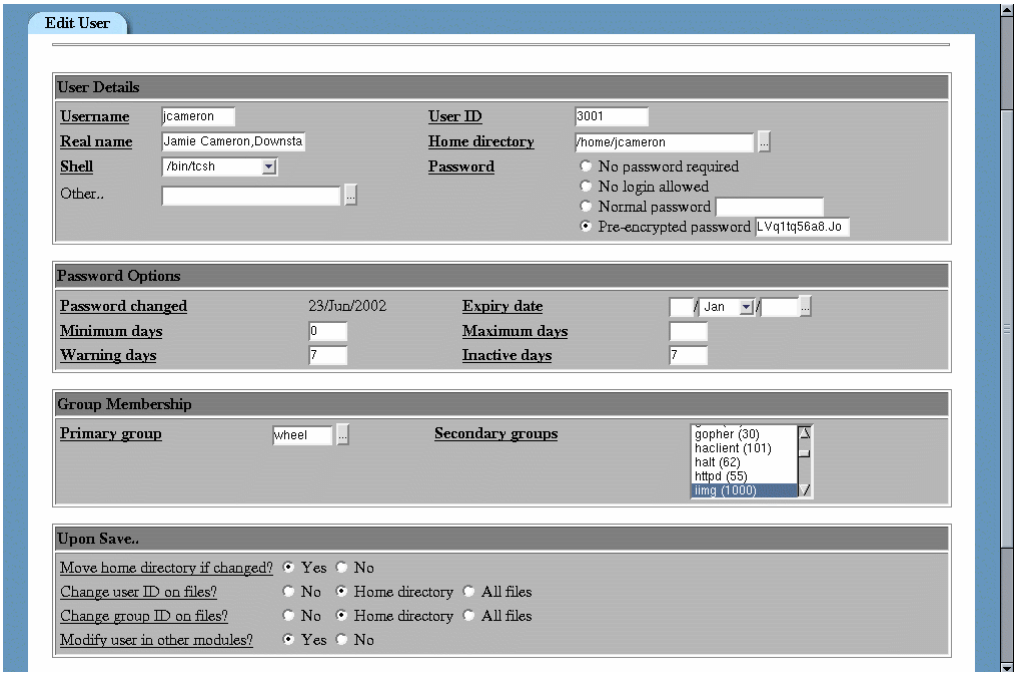


Figure 4.5 The user editing form.

2. Click the **Delete** button at the bottom of the page. This will bring up a form asking you to confirm the deletion, with buttons to delete just the user or his home directory as well. The amount of disk space used by the user's home directory will be shown.
3. Select the **Delete user in other modules?** option if you want the user to be deleted from other modules in which deletion has been set up. Any Cron jobs belonging to the user will be deleted, as will his Sendmail mail file.
4. Click either the **Delete User** or **Delete User and Home Directory** button to delete the user. A page showing the progress of the deletion will be displayed while it is taking place.

4.6 Creating a New Group

A new UNIX group can be added by following these steps:

1. Click on the **Create a new group** link at the top or bottom of the existing list of groups. A form for entering the details of the group will appear, as shown in Figure 4.6.
2. Choose a name for the new group, and enter it into the **Group name** field. The name must not be used by any other group, and should be short and contain no spaces.
3. The **Group ID** field should be left alone, as it is automatically determined by Webmin. If for some reason you change it, make sure that it is not the same as any existing group's ID.
4. The **Password** field can be ignored, as group passwords are never used.

5. In the **Members** field, enter the names of any existing users that you want included in this group. You can use the button to the left of the field to pop up a selection window of all existing users.
6. Click the **Create** button to have Webmin create the new group. Once it is complete, you will be returned to the lists of users and groups.

Once the new group has been created, you can edit users to make it their primary group or one of their secondary groups.

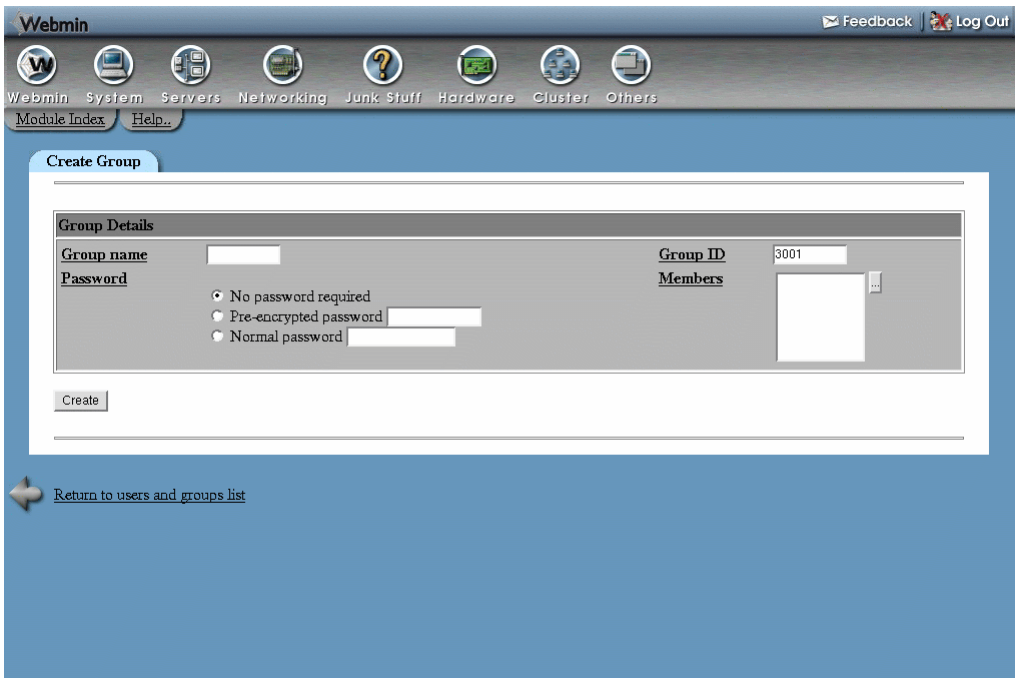


Figure 4.6 The group creation form.

4.7 Editing an Existing Group

You do not often need to edit an existing group, as users can be added to or removed from it by editing them directly. However, if you do want to edit a group, follow these steps:

1. Click on the name of the group that you want to edit from the list of existing groups. This will bring up the group editing form, as shown in Figure 4.7.
2. Change any of the details such as the group ID or member list. It is not possible to change the name of an existing group.
3. If you are changing the group ID, files owned by the group may need to be updated to use the new ID. Use the **Change group ID on files?** option to control which directories will be searched for files that need updating.
4. Click on the **Save** button to make the changes active. Once they are complete, you will be returned to the lists of users and groups.

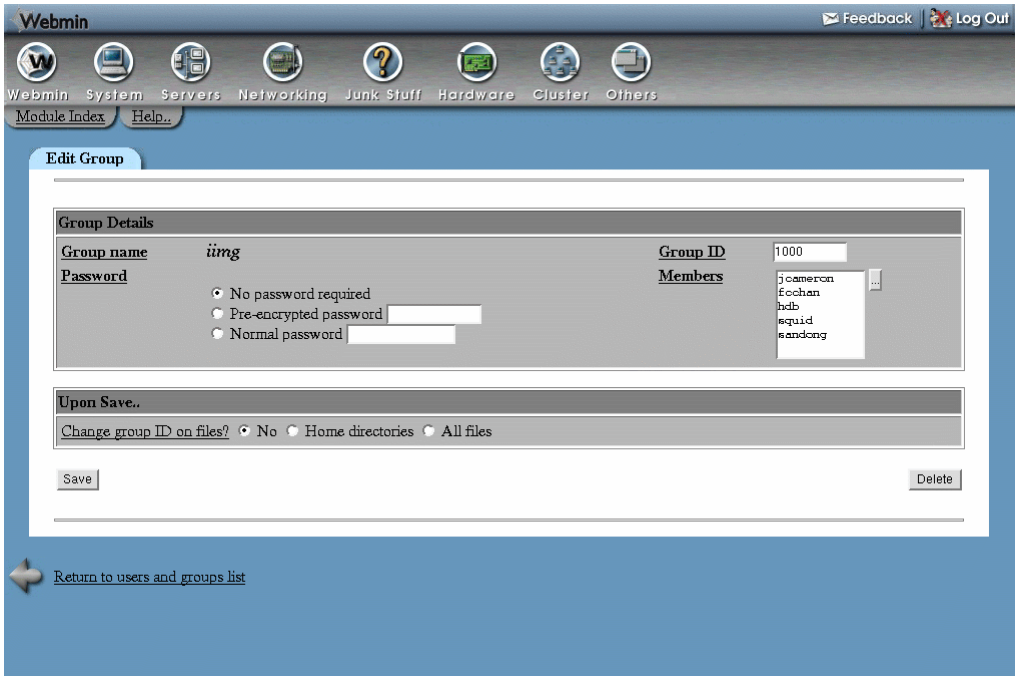


Figure 4.7 The group editing form.

4.8 Deleting a Group

You can safely delete a group at any time, but Webmin will only let you do so if there are no users who have selected it as their primary group. To delete, follow these steps:

1. Click on the name of the group you want to delete from the list of existing groups. This will bring up the group editing form as shown in Figure 4.7.
2. Click the **Delete** button at the bottom of the page. A page asking if you really want to delete the group will appear.
3. Click the **Delete Group** button to confirm the deletion. A page showing the progress of the deletion will be displayed.

4.9 Viewing Recent and Current Logins

All UNIX systems keep track of recent logins made by users using SSH, telnet, or at the console. Some also track FTP logins as well. You can display recent user logins that include the date, time, and source address by following these steps:

1. Below the lists of users and groups, enter the username of the one you want to track into the **Display logins by** field, and click the button. If you want to see logins by ALL users, just leave the field blank.

2. A page listing recent logins by the user or users will be displayed. The list may not cover all logins from the date your system was first installed, as many operating systems automatically truncate the log file periodically in order to save disk space.

It is also possible to display a list of users who are currently logged in by clicking the **Logged In Users** button below the lists of users and groups. If a user is logged in graphically at the console, he may be listed multiple times—once for each shell window he has open.

4.10 Reading Users' Email

When editing a user, you can view mail in the user's mailbox by clicking on the **Read Email** button at the bottom of the page. This will take you directly to the mailbox viewing page of either the Sendmail, Qmail, or Postfix module, depending on what you have chosen for the **Display user email from** option in the module configuration. For more documentation on using the mail interface, see Chapter 37.

4.11 Creating Users from Batch Files

Sometimes you may want to create a large number of users at once without having to go through the process of filling out the user creation form over and over again. You will often have the details of these users in a text file of some kind containing their usernames, passwords, and real names. Fortunately, Webmin has a feature that automates this task for you.

If you click on the **Create, modify and delete users from batch file** link above or below the list of existing users, a form will appear that allows you to upload a file containing the details of users to create, as shown in Figure 4.8. Your file must contain one line of text for each user that you want to create, and the format of each line must match the format shown on the batch file page.

The exact file format depends on what information your system stores about each user, but on most systems each line must follow this format:

`create:`*username:passwd:uid:gid:realname:homedir:shell:min:max:warn:inactive:expire*

An example line to create a user with the user ID automatically assigned by Webmin would be:

```
create:jcameron:mysecret::3001:Jamie Cameron:/home/jcameron:/bin/bash:::::
```

As you can see, the line is made up of a series of fields, each separated by a colon `(:)`. When creating a user, the first field must be the `create` field. The meanings of the other fields are shown in Table 4.1.

Once you have created a file containing the details of users to create, select it using either the **Upload batch file** or **Local batch file** fields, and click the **Execute batch** button. A page displaying each user created and any errors encountered will be displayed. The most common error is a missing field in one of the lines—each must have exactly the right number of fields, and even if a field is blank the colon separator next to it must still be included.

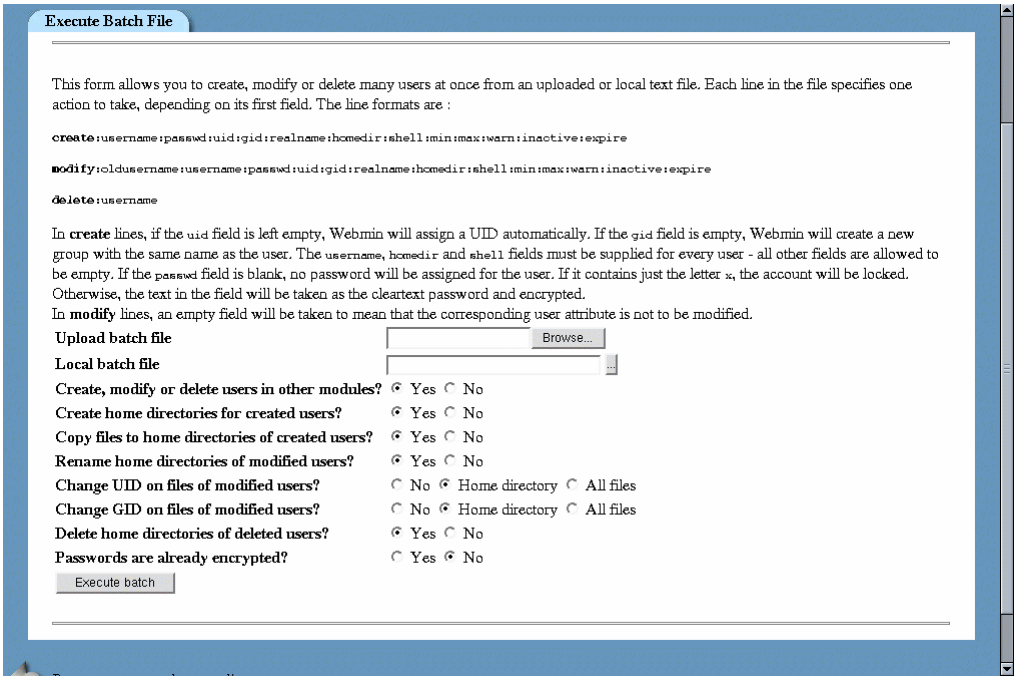


Figure 4.8 The batch file execution form.

Table 4.1 Batch File Fields and Their Meanings

`username`	The user's login name. This cannot be left blank.
`passwd`	The user's password. If this field is left blank, then no password will be needed for the user. If it contains just the letter `x`, then the user will be locked and no login allowed.
`uid`	User ID for the new user. This should be left blank, so Webmin can assign one automatically.
`gid`	ID of the user's primary group. This cannot be a group name, and cannot be left blank. If more than one GID is entered, the user will be added as a secondary member to all of those listed after the first one as well.
`realname`	The user's real name. Not mandatory, but should not be left blank.
`homedir`	A directory that is created with ownership assigned to the user. You can leave this blank if the module has been configured to assign home directories automatically.

Table 4.1 Batch File Fields and Their Meanings (Continued)

`shell`	The user's login shell. This field cannot be left blank.
`min`	The number of days after the user is created or the password is last changed that the user must wait before changing it again. Can be left blank to allow changing as soon as the user likes.
`max`	The number of days after the user is created or the password is last changed that the password expires and must be changed again. If left blank, the password will never expire.
`warn`	The number of days before the password expiry date that the user will be warned at login that his password is about to expire. If left blank, the user will not know that his password has expired until it happens.
`inactive`	The number of days after the password expires that the entire account will be disabled, if the user has not chosen a new password. If left empty, the account will never expire.
`expire`	The date on which this account will expire. Unfortunately, you must enter this as a number of days since January 1, 1970!

4.12 Configuring the Users and Groups Module

Like other Webmin modules, Users and Groups has several options that can be configured by clicking on the **Module Config** link above the lists of users and groups, as shown in Figure 4.9. The options that you can safely change and their meanings are shown in Table 4.2.

Table 4.2 Module Configuration Options

Command to run before making changes	Whatever shell command you enter into this field will be run just before any action is performed, such as adding, deleting, or modifying a user or group. It can be useful for doing things like making a backup copy of the `/etc/passwd` file before Webmin makes any changes. The command can determine exactly what Webmin is about to do by checking environment variables, as explained in the Section 4.13 "Before and After Commands".
Command to run after making changes	Like the above option, but this command is run *after* any action is performed. It can be very useful if you want to have a command run after a user is created in order to setup additional files for that user.
Permissions on new home directories	The octal file permissions on newly created home directories, in the same format as used by the `chmod` command.

Table 4.2 Module Configuration Options (Continued)

Copy files into new home directories from	Directories or files to copy into the home directory of newly created users, assuming the **Copy files to home directory?** option is turned on. If any of the paths you enter is a directory, all files and subdirectories in that directory will be copied. This option is usually set to `/etc/skel` by default, which is a system directory containing files like `.cshrc` and `.profile`.
Automatic home directory base	The directory under which users' home directories are usually created. If this option is set, an **Automatic** option will appear for the **Home directory** field in the user creation form. If chosen, the home directory will be determined by this option and the **Automatic home directory style** below.
Automatic home directory style	This option controls the path to a new user's home directory under the base. The most common default option of `home/username` will make it just a subdirectory under the base, with the same name as the username. So if you were creating a user called *jcameron* and the home directory base was set to `/home`, then the resulting home directory would be `/home/jcameron`. Other options create subdirectories using the first one or two letters of the username. They can be useful if you have a very large number of users on your system, and want to avoid having thousands of entries in `/home`.
Lowest UID for new users	When Webmin automatically chooses a user ID for a new user, it will never pick one that is lower than specified in this option. On most systems, normal users have user IDs above 500, and system users have IDs below that.
Lowest GID for new groups	Like the option above, but for group IDs.
Create new group for new users?	If this option is set to **Yes** when creating a new user, the default action is to create a group of the same name and make it the user's primary group.
Assign same ID to new user and group?	This option only works if the previous one is enabled. If set to **Yes** when a new group is created for a new user, Webmin will make sure that their UID and GID are the same. This doesn't actually make any difference, but some administrators like it.
Don't use MD5 passwords if missing perl MD5 module?	This option should only be changed to **Yes** if you run into an error when creating a new user caused by a missing `MD5` Perl module.
Check for sendmail alias clashes?	If set to **Yes** when creating or renaming a user, Webmin will check if there is a Sendmail alias of the same name. This can be useful to prevent the creation of users who would be unable to receive mail due to an alias redirecting it all to another address.
Only delete files owned by user?	If set to **Yes** when deleting a user, files in the user's home directory that do not belong to him will not be deleted.

Table 4.2 Module Configuration Options (Continued)

Maximum user and group name length	The maximum allowed length for a user or group name. If this is set by default, it is not a good idea to adjust it because your operating system will not recognize longer usernames.
Default group for new users	The default primary group on the new user creation form.
Default secondary groups for new users	A space separated list of secondary groups that will be selected by default on the new user creation form.
Default shell for new users	The default shell on the new user creation form.
Default minimum days for new users	The default number of days before which password changing is not allowed.
Default maximum days for new users	The default number of days after which the password must be changed.
Default warning days for new users	The default number of days before password expiry that the user is warned.
Default inactive days for new users	The default number of days after password expiry that the user is disabled.
Maximum number of users to display	If the number of users or groups on the module's main page exceeds this number, the table of users or groups will be replaced by a search form. You may want to adjust this if the number of users on your system is just over the default limit.
Sort users and groups by	This option controls the ordering of users and groups on the module's main page.
Number of previous logins to display	This option limits the number of recorded logins to display so the table does not become too large on systems that keep an unlimited login history.
Display users and groups by	By default, users and groups are shown on the module's main page in a table with one row per user or group. However, if you change this option to **Name only** then only the username of each appears, saving a lot of screen space if you have a large number of users. Changing to **Primary group categorized** also displays users by username only, but categorized by their primary group.
Conceal plain-text password?	If set to **Yes** when editing or creating a user, the **Normal password** field will show only stars instead of the actual password that you enter. Useful if you are worried about people looking over your shoulder when creating users.

Table 4.2 Module Configuration Options (Continued)

Get user and group info from	Even though the module reads and edits system user, group, and password files directly, there will in some cases be users and groups on your system that come from another source, such as NIS. When displaying a user's primary group or the users who are members of a group, Webmin will use the `getpw` family of system calls by default to get a list of users and groups, instead of reading the user and group files directly. This is normally the right thing to do, but in some cases it will not work properly or will be very slow. You should only change this option to **Files** if you are sure that you want the module to never use the `getpw` functions.
Generate password for new users?	If this option is set to **Yes** when creating a new user, Webmin will generate a random password for you by default.
Show office and phone details?	Normally, a user's **Real name** field only contains his name. However, it can also contain additional information such as his office location, home phone, and work phone. These extra fields are displayed by the `finger` command, and are stored by the system in the real name field of the **/etc/passwd** file separated by commas. If you want to be able to edit this additional information separately, set this option to **Yes**. It will not work well if usernames on your system contain commas in them—like *Cameron, Jamie*.
Display user email from	This option controls which module is used when the **Read Email** button is clicked on the user editing page. You should make sure it is set appropriately depending on the mail system you are using because Sendmail and Qmail use different locations and file formats for user mailboxes.
Minimum password length	If set, you will not be able to create or edit users whose plain-text passwords are shorter than this length. This option and the three below also effect the Change Passwords and Cluster Users and Groups modules. They can be useful if you want to delegate user management to someone else, and don't trust the quality of his passwords.
Prevent dictionary word passwords?	If this option is set, passwords that exactly match any word from the dictionary will not be allowed.
Perl regexp to check password against	If set, passwords must match this Perl regular expression. For example, you could enter *[0-9]* for this option to force all passwords to contain at least one digit.
Prevent passwords containing username?	When this option is set to **Yes**, passwords that exactly match or contain the user's username will not be allowed.

The other options under the **System configuration** heading control the files Webmin reads and writes user and group information from and to. Because they are set automatically based on the type of operating system you use, they should not be changed unless you know what you are doing.

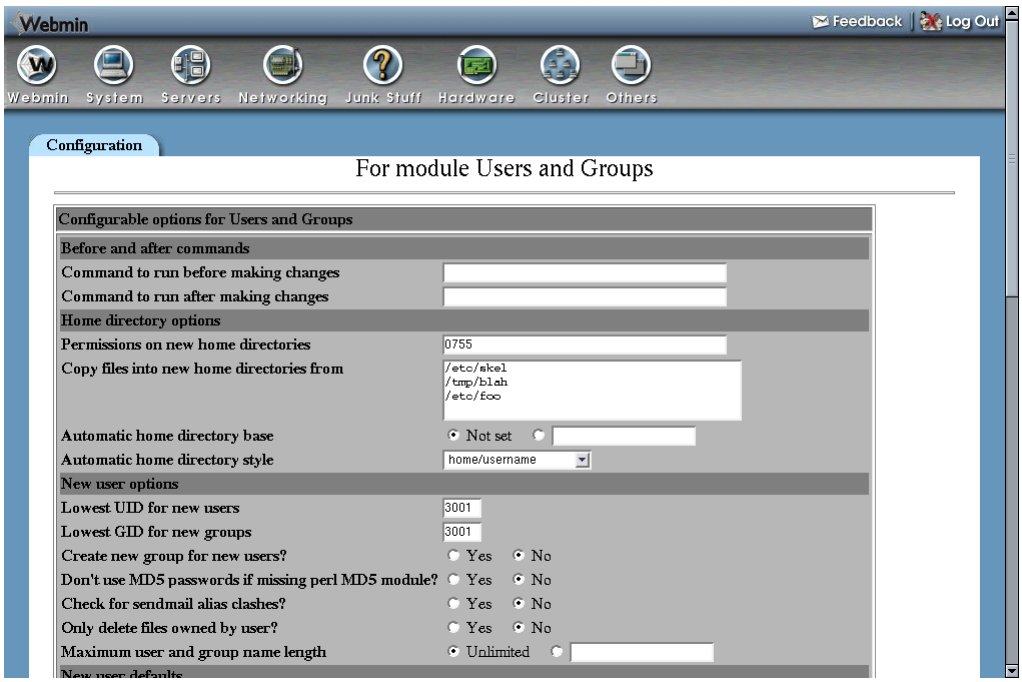


Figure 4.9 Configuration options for Users and Groups.

4.13 Before and After Commands

As Section 4.12 “Configuring the Users and Groups Module” explains, you can specify shell commands to be run before and after any action is taken in the module. Because these commands are called for every addition, modification, or deletion of a user or group, they need some way of telling exactly what action is being performed. They can do this using environment variables that are set before the command is run. The available environment variables are shown in Table 4.3.

If you wanted to send out email when a user is created, for example, you could set the **Command to run after making changes** option to:

```
[ "$USERADMIN_ACTION" = "CREATE_USER" ] && echo "Added user
$USERADMIN_USER ($USERADMIN_REAL)" | mail -s "Added new user"
you@yourdomain.com
```

4.14 Module Access Control

It is possible to grant a Webmin user or group access to only a subset of features in the Users and Groups module. This is most commonly used to allow a subadministrator the right to edit only

Table 4.3 Environment Variables for Before and After Commands

USERADMIN_ACTION	Indicates which action is being taken. Possible values are: CREATE_USER MODIFY_USER DELETE_USER CREATE_GROUP MODIFY_GROUP DELETE_GROUP
USERADMIN_USER	The username of the user being created, modified, or deleted. Not set when a group action is being performed.
USERADMIN_UID	The user ID of the user being created, modified, or deleted.
USERADMIN_GID	The group ID of the user.
USERADMIN_REAL	The real name of the user, including any office and phone information.
USERADMIN_SHELL	The shell of the user.
USERADMIN_HOME	The home directory of the user.
USERADMIN_PASS	The plain text password of the user, if available.
USERADMIN_SECONDARY	A comma-separated list of any secondary groups to which the user belongs.
USERADMIN_GROUP	The name of the group being added, modified, or deleted. Not set when a user action is being performed.

selected users and groups on the system, and to change their attributes in only limited ways. In a virtual hosting environment, for example, you may want to give a Webmin user the ability to create and edit up to 10 users with UIDs in a limited range, and home directories under a fixed directory. These privileges give the user no way to gain **root** access and affect users that do not belong to him.

Chapter 52 explains how to create additional Webmin users and edit their module access control in more detail. The following steps cover just the parts of the process that grant the kind of limited access that is specific to the Users and Groups module:

1. In the Webmin Users module, click on **Users and Groups** next to the name of the user that you want to edit. This will take you to the access control form shown in Figure 52.3.
2. Change the **Can edit module configuration?** field to **No**.

3. The **UNIX users who can be edited** field controls the users that can be changed by this Webmin user. You would typically set it to **Users with UIDs in range** and enter maximum and minimum UIDs into the fields next to it, such as *5000* and *5010*.
4. To allow the addition of new UNIX users, set the **Can create new users?** field to **Yes**.
5. Set the **Can view batch file form?** option to **No**. This will prevent the Webmin user from creating and editing users from a batch script, which is not normally necessary. Allowing it, however, does not grant the user any additional privileges and is not a security risk.
6. For the **UIDs for new and modified users** fields, enter the same UIDs as in Step 4.
7. Deselect the **More than one user can have the same UID** option, but leave the **UIDs of existing users can be changed** option selected. An untrusted subadministrator should not normally be allowed to create multiple users with the same UID due to the problems that this can cause.

   When UID clashes are prevented, the Webmin user will not be able to create any more UNIX users than fit in his allowed UID range.
8. In the **Allowed groups for new or modified users** field, you would typically select the **Only groups** option and enter the names of any groups of which new users can be primary or secondary members. Normally you would just enter a single group like *users*. Leaving this field set to **All groups** is a very bad idea, because it would allow the creation of users who are members of the `root` or `bin` groups, and who can thus edit important system files and executables. The **Groups with GIDs in range** option can be useful if this Webmin user is allowed to create multiple groups of his own within the same GID range.
9. To restrict the shells that a new user can be assigned, set the **Allowed shells for new or modifed users** to **Listed** and enter their paths into the text box below. This can be useful to allow the creation of only mail-only users who always have the shell `/bin/false`.
10. Set the **Home directories must be under** field to a directory that will only be used for accounts created by this Webmin user. Setting it to `/home` is a bad idea, because this would allow the subadministrator to rename or delete directories belonging to other users that are under /home. Instead, enter something like `/home/`*subadmin*.

    To force every user's home directory to be based on his username (such as `/home/subadmin/`*username*), check the **Home directory is always same as username** box.
11. To stop the Webmin user from deselecting some of the options at the bottom of the user creation, editing and deletion forms, deselect the matching **Allowed on save options**. Any that are not chosen will effectively always be turned on.
12. Assuming you just want the Webmin user to create and edit UNIX users, set the U**NIX groups who can be edited** field to **No groups**.
13. If you want to restrict the user from viewing recent logins, change the **Can display logins by** field. Any user who can login with telnet or SSH can run the last command anyway to display logins, so setting this option to **No users** does not usually make your system any more secure.
14. Finally, click **Save**. You will be returned to the module's main page and the new access control restrictions will be immediately applied to the Webmin user.

Be careful when granting a Webmin user access to certain UNIX users, as a mistake may allow him to edit the `root` user or create a new user who is equivalent to `root`. There are also many

other users like `bin`, `uucp`, and `httpd` that own important system files or are used for running server and daemon processes. Someone who can edit or login as one of these users could gain **root** privileges on your system or access files that he is not supposed to.

Often the access control in the Disk Quotas and Scheduled Cron Jobs module is set up to allow editing of the quotas and Cron jobs of the same UNIX users as those that can be edited and created in this module. All modules support the UID range and primary group access control options, which can be set in the same way.

It is also possible to use the Users and Groups access control form to allow a user to edit or create selected UNIX groups, though this is not generally as useful. Granting an untrusted user the rights to edit all groups on the system is a bad idea, as he would make himself a member of the `root` or `bin` group and so be able to read or write critical files.

4.15 Other Operating Systems

Different operating systems store different information about users than Linux does. This is due to the different files and file formats used for storing user information. Some, for example, do not have an `/etc/shadow` file, meaning that information about password change and expiry times does not exist. The list below explains the major differences between other supported operating systems and Linux:

FreeBSD, OpenBSD and NetBSD All these operating systems use the `/etc/master.passwd` file for storing user information, which combines `/etc/passwd` with some fields from `/etc/shadow`. When editing or creating a user, you can enter a **Password change time** which is the date and time after which the password must be next changed, and an **Account expiry time** after which an account can no longer be used. Each user can also have a **Login class**, which is used in conjunction with the `/etc/login.conf` file to determine memory, CPU, and other limits.

Sun Solaris and SCO UnixWare Both these operating systems use the same files and formats as Linux, and so have all the same options.

HP/UX, SGI Irix, and Compaq Tru64/OSF1 Because none of these systems use an `/etc/shadow` file by default, none of the options related to password and account expiration are available when editing or creating a user.

Apple MacOS X OSX does not store user and group information in files at all—instead, it uses a network database called NetInfo, which Webmin manipulates using the `nidump` and `niutil` commands. This database, however, stores the same information as the BSD `master.passwd` file, so when editing or creating a user the same fields are available as for FreeBSD.

IBM AIX AIX uses the files `/etc/passwd` and `/etc/security/passwd` for storing user information. Therefore, when editing or creating users on AIX there are some options that do not exist on other operating systems. The **Expiry date** field can be used to set the date and time after which the account cannot be used. The **Minimum weeks** and **Maximum weeks** fields are very similar to the **Maximum days** and **Minimum days** fields on Linux, but deal with weeks instead of days. The **Warning days** field has exactly the same meaning as on Linux, and deals with days

not weeks. The unique **Account flags** field sets special options whose meanings are explained on the form.

SCO OpenServer OpenServer uses `/etc/passwd` and `/etc/shadow` files, but the `shadow` file stores slightly different information than on Linux. This means that when editing a user, the **Expiry date** field is replaced with an option to control whether the user is prompted for a password at their next login, and the **Warning days** and **Inactive days** fields are not available.

Those few operating systems that are not listed above cannot use the Users and Groups module, as their file formats are not currently know to Webmin.

4.16 Summary

This chapter has explained how to create and manage users and groups on a UNIX system. Because they are used to enforce file security, to protect processes from each other, and as mailboxes, user management is one of the most important tasks on a multi-user server system. This means that the module covered in this chapter is one of the most commonly used in Webmin, and also one of the most powerful.