Matthew Helmke

2021 Edition

Covers 20.04, 20.10, and 21.04

Ubuntu Linux

UNLEASHED

Matthew Helmke

with Andrew Hudson
and Paul Hudson

Ubuntu Linux

UNLEASHED

2021 Edition

SAMS

User Management Tools

As with groups, Ubuntu provides several command-line tools for managing users, and it also provides graphical tools for doing so. As mentioned earlier, most experienced system administrators prefer the command-line tools because they are quick and easy to use, they are always available (even when there is no graphical user interface), and they can be included in scripts that system administrators may want to write to perform repetitive tasks. Here are the most common commands to manage users:

- **`useradd`**—This command adds a new user account to the system. Its options permit the system administrator to specify the user's `/home` directory and initial group or to create the user with the default `/home` directory and group assignments (based on the new account's username).
- **`useradd -D`**—This command sets the system defaults for creating the user's `/home` directory, account expiration date, default group, and command shell. See the specific options in the `useradd` man page. Used without any arguments, the `useradd` command displays the defaults for the system. The default files for a user are in `/etc/skel`.

NOTE

The set of files initially used to populate a new user's home directory is kept in `/etc/skel`. This is convenient for the system administrator because any special files, links, or directories that need to be universally applied can be placed in `/etc/skel` and will be duplicated automatically with appropriate permissions for each new user:

```
matthew@seymour:~$ ls -la /etc/skel
total 32
drwxr-xr-x   2 root root  4096 2010-04-25 12:14 .
drwxr-xr-x 154 root root 12288 2010-07-01 16:30 ..
-rw-r--r--   1 root root   220 2009-09-13 22:08 .bash_logout
-rw-r--r--   1 root root  3103 2010-04-18 19:15 .bashrc
-rw-r--r--   1 root root   179 2010-03-26 05:31 examples.desktop
-rw-r--r--   1 root root   675 2009-09-13 22:08 .profile
```

Each line provides the file permissions, the number of files housed under that file or directory name, the file owner, the file group, the file size, the creation date, and the filename.

As you can see, root owns every file here. The `useradd` command copies everything in `/etc/skel` to the new home directory and resets file ownership and permissions to the new user.

Certain user files might exist that the system administrator doesn't want the user to change; the permissions for those files in `/home/username` can be reset so that the user can read them but can't write to them.

- **deluser**—This command removes a user's account (thereby eliminating that user's home directory and all files it contains). There is an older version of this command, userdel, that previous versions of this book discussed. deluser is preferred because it provides finer control over what is deleted. Whereas userdel automatically removes both the user account and also all the user's files, such as the associated /home directory, deluser deletes only the user account, unless you use a command-line option to tell it to do more. deluser includes options such as --remove-home, --remove-all-files, --backup, and more. See the man page for more information.
- **passwd**—This command updates the authentication tokens used by the password management system.

TIP

To lock a user out of his or her account, use the following command:

```
matthew@seymour:~$ sudo passwd -l username
```

This prepends an ! (exclamation point, also called a bang) to the user's encrypted password; the command to reverse the process uses the -u option.

- **usermod**—This command changes several user attributes. The most commonly used arguments are -s to change the shell and -u to change the UID. No changes can be made while the user is logged in or running a process.
- **chsh**—This command changes the user's default shell. For Ubuntu, the default shell is /bin/bash, known as the Bash, or Bourne Again Shell.

Adding New Users

The command-line approach to adding a user is quite simple and can be accomplished on a single line. In the following example, the system administrator uses the useradd command to add the new user sandra:

```
matthew@seymour:~$ sudo useradd sandra -p c00kieZ4ME -u 1042
```

The command adduser (a variant found on some UNIX systems) and useradd are similar and do the same thing. This example uses the -p option to set the password the user requested and the -u option to specify her UID. (If you create a user with the default settings, you do not need to use these options.) As you can see, all this can be accomplished on one line.

The system administrator can also use the graphical interface that Ubuntu provides to add the same account as shown in the preceding command but with fewer setting options available:

1. From the menu at the upper right of the desktop, select the Settings icon, which looks like a gear (see Figure 13.1). In the Settings application, from the bottom left select Users (see Figure 13.2).

2. Click Unlock at the upper right and enter your password to authorize making changes to user accounts.
3. Click Add User at the upper right, where Unlock was, to open the Add Account window.
4. Fill in the form with the new user's name and desired username, select whether to set a password now or have the new user create a password the first time he or she logs in, and designate whether the new user is a standard user or an administrator, and click Add (see Figure 13.3).

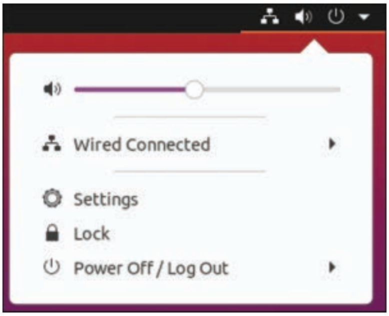
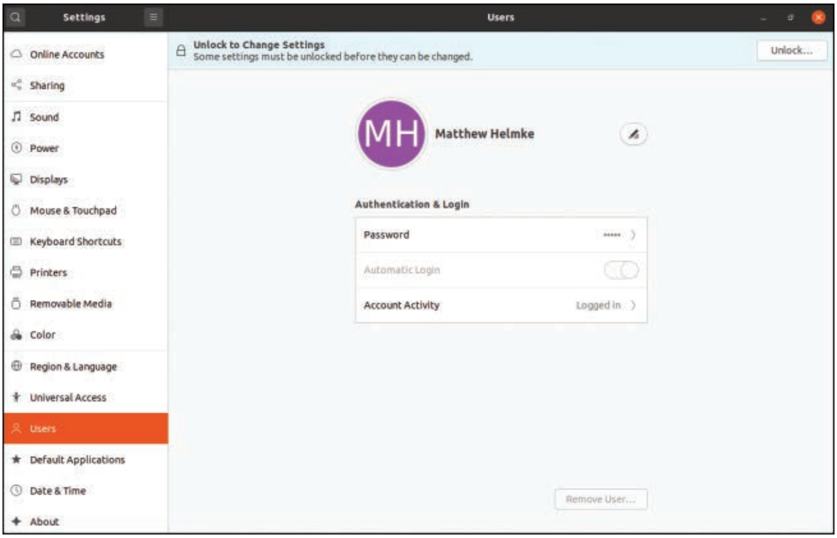


FIGURE 13.1 Open the menu at the upper right to find the Settings icon.



Unlock to Change Settings
Some settings must be unlocked before they can be changed.

Matthew Helmke

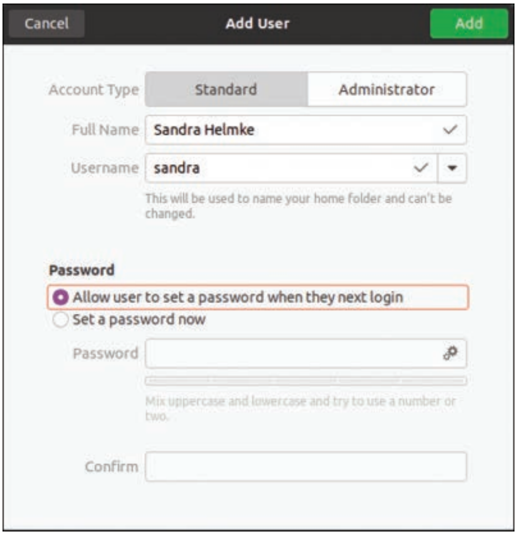
Authentication & Login

Password •••••

Automatic Login

Account Activity Logged in

FIGURE 13.2 Select Users.



Account Type: Standard | Administrator

Full Name: Sandra Helmke ✓

Username: sandra ✓

This will be used to name your home folder and can't be changed.

Password

● Allow user to set a password when they next login

○ Set a password now

Password:

Mix uppercase and lowercase and try to use a number or two.

Confirm:

FIGURE 13.3 Adding a new user is simple. The GUI provides a set of options for user management spread over several screens.

NOTE

A Linux username can be any alphanumeric combination that does not begin with a special character reserved for shell script use (mostly <space> and punctuation characters; see Chapter 14, “Automating Tasks and Shell Scripting,” for disallowed characters). A username is often the user’s first name plus the first initial of her last name or the first initial of the user’s first name and his entire last name. These are common practices on larger systems with many users because it makes life simpler for the system administrator, but neither convention is a rule or a requirement.

Monitoring User Activity on the System

Monitoring user activity is part of a system administrator’s duties and an essential task in tracking how system resources are being used. The `w` command tells the system administrator who is logged in, where he is logged in, and what he is doing. No one can hide from the super user. The `w` command can be followed by a specific user’s name to show only that user.

The `ac` command provides information about the total connect time of a user, measured in hours. It accesses the `/var/log/wtmp` file for the source of its information. The `ac` command is most useful in shell scripts to generate reports on operating system usage for management review. Note that to use the `ac` command, you must install the `acct` package from the Ubuntu repositories.

TIP

Interestingly, a phenomenon known as *time warp* can occur, where an entry in the `wtmp` files jumps back into the past, and `ac` shows unusual amounts of time accounted for users. Although this can be attributed to some innocuous factors having to do with the system clock, it is worthy of investigation by the system administrator because it can also be the result of a security breach.

The `last` command searches through the `/var/log/wtmp` file and lists all the users logged in and out since that file was first created. The user reboot exists so that you might know who has logged in since the last reboot. A companion to `last` is the command `lastb`, which shows all failed, or bad, logins. It is useful for determining whether a legitimate user is having trouble or a hacker is attempting access.

NOTE

The accounting system on your computer keeps track of user usage statistics and is kept in the current `/var/log/wtmp` file. That file is managed by the `systemd` processes. If you want to explore the depths of the accounting system, use the GNU info system: `info accounting`.

Managing Passwords

Passwords are an integral part of Linux security, and they are the most visible part to the user. In this section, you learn how to establish a minimal password policy for your system, where the passwords are stored, and how to manage passwords for your users.

System Password Policy

An effective password policy is a fundamental part of a good system administration plan. The policy should cover the following:

- Allowed and forbidden passwords
- Frequency of mandated password changes
- Retrieval or replacement of lost or forgotten passwords
- Password handling by users

The Password File

The password file is `/etc/passwd`, and it is the database file for all users on the system. The format of each line is as follows:

```
username:password:uid:gid:gecos:homedir:shell
```

The fields are self-explanatory except for the `gecos` field. This field is for miscellaneous information about the user, such as the user's full name, office location, office and home phone numbers, and possibly a brief text note. For security and privacy reasons, this field is little used today, but the system administrator should be aware of its existence because the `gecos` field is used by traditional UNIX programs such as `finger` and `mail`. For that reason, it is commonly referred to as the *finger information field*. The data in this field is comma delimited; you can change the `gecos` field with the `chfn` (`change finger`) command.

Note that colons separate all fields in the `/etc/passwd` file. If no information is available for a field, that field is empty, but all the colons remain.

If an asterisk appears in the `password` field, that user is not permitted to log on. This feature exists so that a user can be easily disabled and (possibly) reinstated later without the need to create the user all over again. The traditional UNIX way of accomplishing this task is for the system administrator to manually edit this field. Ubuntu provides a more elegant method with the `passwd -l` command, mentioned earlier in this chapter.

Several services run as pseudo-users, usually with root permissions. These are the system, or logical, users mentioned previously. You would not want these accounts to be available for general login for security reasons, so they are assigned `/sbin/nologin` or `/bin/false` as their shell, which prohibits any logins from these accounts.

A list of `/etc/passwd` reveals the following (abridged for brevity):

```
matthew@seymour:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
messagebus:x:102:106::/var/run/dbus:/bin/false
avahi:x:105:111:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
couchdb:x:106:113:CouchDB Administrator,,,:/var/lib/couchdb:/bin/bash
haldaemon:x:107:114:Hardware abstraction layer,,,:/var/run/hald:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
gdm:x:112:119:Gnome Display Manager:/var/lib/gdm:/bin/false
matthew:x:1000:1000:Matthew Helmke,,,,:/home/matthew:/bin/bash
sshd:x:114:65534::/var/run/sshd:/usr/sbin/nologin
ntp:x:115:122::/home/ntp:/bin/false
pulse:x:111:117:PulseAudio daemon,,,:/var/run/pulse:/bin/false
```