

Users and Groups

About users and groups

SA4padPointRule2.eps ↗

In this topic

- Local accounts
- Network accounts
- Groups
- Permissions
- Home directories
- Account information

1PointDashedRule3Black.eps ↗

Summary

All users need a *user account* whether they work on a network or a standalone computer. This account provides basic information that the system uses to grant access to the file system and to deliver mail.

In addition, each user account is associated with one or more *groups*. A group can share project files and folders. Groups also provide a way to restrict access to information.

Users in the same group can restrict file permissions to their own group.

96511_paste.eps ↗

Each user also has a *home directory*. This is the user's personal file system. It typically includes any applications the user needs, as well as the **Active.mbox** file, which is necessary to receive e-mail.

Account information is stored in the **/users** and **/groups** directories of a particular domain. You use the UserManager application to add ;AddNetworkUserAccount.rtf;;↗ or change

accounts ;ChangeUserAccount.rtf;;~.

You can use the NetInfoManager application to examine users ;../NetInfo/ExamineUserAccount.rtf;;~ and groups ;../NetInfo/ExamineGroup.rtf;;~.

443536_PointDashedRule3Black.eps ~Local accounts

Local user accounts are stored in the local domain for a particular computer. They give individual users access to that single computer. The computer may be a standalone computer or part of a network.

All NEXTSTEP computers have four local accounts:

- | | |
|---------------|---|
| root | This is a superuser account used for system administration. When you're logged in as root , you can bypass all file and folder permissions. The user ID is 0. |
| me | This a default user account for standalone computers. The user ID is 20. |
| nobody | This is an account for unknown users—that is, those who don't have accounts on the network but may occasionally need access to some network files. The user ID is ±2. |
| uucp | This account is used for uucp mail and file transfer. The user ID is 4. |

A single user working on a standalone computer can use the **me** account as the working account. But if two or more users share a standalone computer, they may want separate local accounts to protect the privacy of their files.

As system administrator, you may want to set up a local account on a computer that's part of a network to restrict access to that computer alone. For example, you can set

up a local account with a single application—such as an on-line visitor's log. Users can log in and fill out the sign-in form, but they can't do or see anything else on the computer or the network.

Local account information is always stored in the **/users** directory of the local domain. You can add a local user with the UserManager application ;AddLocalUserAccount.rtf;;↵.

405019_PointDashedRule3Black.eps ↵

Network accounts;↵Network accounts

Network user accounts are stored in a domain at least one level above the local domain. They give individual users access to several or all of the computers on a network, depending upon the domain in which they're stored.

925255_paste.eps ↵

When you add users to a midlevel domain, you're restricting them to particular computers. You can use groups to further restrict them to particular files and folders.

All account information for network users is stored in the **/users** directory of the domain you choose. If you choose a midlevel domain, make sure the user has access to a computer in that domain.

You can add a network user ;AddNetworkUserAccount.rtf;;↵ or move a local user to the network ;MoveLocalUserToNetwork.rtf;;↵ with the User Manager application.

418335_PointDashedRule3Black.eps ↵**Groups and permissions**

When you set up a group, you give a group of users access to a common set of files

and folders.

Each file in a system is owned by both a user and a group. The users who create the files set the read, write, and execute permissions:

paste.eps ↵

For very secure files, such as financial data, users can limit permissions to the group that owns them. When lots of different groups need access to the files, users may choose to grant complete permissions to everyone.

As system administrator, you can't directly control the permissions for files or folders you don't create. But you can provide the foundation for a secure system by setting up the appropriate groups.

In addition to groups you create, several standard groups are part of each domain:

other This is the default group for new user accounts. It's the only standard group for regular users. The group ID is 20.

wheel Members of this group can use **su** to gain root access. As system administrator, you should belong to this group. This group is also the owner of many system files. The group ID is 0.

nogroup This group is for unknown users—those who need limited access to the system but don't have a user account. The **nobody** user belongs to this group. The group ID is -2.

operator Members of this group have permission to access device files to

perform system backups. The group ID is 9.

Each user must belong to at least one group. For users who belong to more than one group, you can set a default group ;ChangeGroupMembership.rtf;;~. The default group owns any files that the user creates. However, the user can change the group owner of a file with the File Manager's Inspector panel.

Group information is stored in the **/groups** directory of the domain you choose. If you choose a midlevel domain, make sure that all the members of the group have access to a computer in that domain.

You use the UserManager application to add a group to the network ;AddGroup.rtf;;~.

126766_PointDashedRule3Black.eps ~Home directories

Every user needs a home directory. This is where the user stores personal files.

UserManager can automatically create a home directory when you add a new user account. It includes three standard folders.

UserManager creates the **Apps**, **Library**, and **Mailboxes** folders in every new home directory.

197065_paste.eps ~

You can also create the home directory and mailbox file yourself when you set up services for your network.

You typically set up home directories on a home directory server. Before you add a user, space;~make sure you have enough space on the server for the user's file

system. Also, make sure the home directory is available on all computers that the user can log into—that is, to the user's domain. For example, if the user account is in the root domain (*/*), the home directory should also be in the root domain.

409496_PointDashedRule3Black.eps ↗

User account information

Each user account contains the basic information the system needs to provide access to files and deliver mail. It may also contain other information needed by custom applications.

606676__paste.eps ↗

Information in the individual accounts is stored as a set of property keys and values:

Property key	Value
48429_SA1PointRule2.eps ↗	
name	The user's login name (and usually the name of the home directory). The login name may be up to eight lowercase characters—including letters, digits, dashes (-) and underbars (_). Avoid special characters.
passwd	An encrypted representation of the user's password. The password may be up to eight characters, in any combination of upper- and lowercase.
uid	A unique user ID number. Avoid using system UIDs, which are generally in the range from 0 to 100. These are used for initiating system processes.

gid	A unique group ID number that associates a user with a user group. Avoid using system GIDs, which are generally in the range from 0 to 20. These are used for special administrative purposes. See "Group information" below.
real name	The full name of a user, up to 256 characters.
home	The complete pathname for the user's home directory. This directory must be visible in the user's domain.
shell	A file name for the user's default shell program. If you don't specify a shell program, the default is csh . Others, including sh and bash , are available.
_writers_passwd	The name of an user authorized to access the NetInfo data in the user's account under the /users directory.

When a user logs in, **loginwindow** checks the name and password against these NetInfo values. If the login is successful, NEXTSTEP makes the user's specified home directory the current directory in the File Manager.

When the user creates a file, the UNIX operating system uses the UID and GID numbers as part of the file information, setting the permissions according to the **umask** for the user.

When the user starts the Terminal application, the UNIX operating system loads the specified shell program.

You can examine user account information with NetInfoManager

;../NetInfo/ExamineUserAccount.rtf;;~.

916096_PointDashedRule3Black.eps ~Group information

Group information, stored in **/groups** directory of each domain, includes the following property keys and values:

Property key	Value
999553_SA1PointRule2.eps ~ name	The user's login name (and usually the name of the home directory). The login name may be up to eight lowercase characters including letters, digits, dashes (-) and underbars (_). Avoid special characters.
passwd	An encrypted representation of the group password. A group password may be up to eight characters, in any combination of upper- and lowercase.
gid	A unique group ID number. Avoid using system GIDs, which are generally in the range from 0 to 100. These are used for standard system groups.
users	A list of user account names.
description	A description of the group that you create for your own records.

You can examine information about a group with the NetInfoManager application
;../NetInfo/ExamineGroup.rtf;;~.

SA2PointRule2.eps ↗

Related topics (*click a* LinkDiamond.tiff ↗)

161062_SA1pt-Xref-2.eps ↗

Concepts

All NEXTSTEP networks are organized into at least two domains: a local domain and a root domain. You can add one or more midlevel domains.

;../NetInfo/AboutNetInfo.rtf;;↗ **About NetInfo**

In addition to using file permissions and user groups to restrict access to files, you can set up netgroups to restrict file export to a particular group of computers.

;../NetworkComputers/AboutNetworkComputers.rtf;;↗ **About network computers**

SA1pt-XrefDashedRuleBlack.eps ↗

How to

;AddLocalUserAccount.rtf;;↗ Add a local user account

;AddNetworkUserAccount.rtf;;↗ Add a network user account

;AddMultipleUserAccounts.rtf;;↗ Add multiple user accounts

;MoveLocalUserToNetwork.rtf;;↗ Move a local user to the network

;ChangeUserAccount.rtf;;↗ Change a user account

;ChangeGroupMembership.rtf;;↗ Change a user's group membership

;DisableUserAccount.rtf;;↗ Disable a user account

;RemoveUserAccount.rtf;;↗ Remove a user account

;RemoveMultipleUserAccounts.rtf;;↗ Remove multiple user accounts

;AddGroup.rtf;;↗ Add a group

;RemoveGroup.rtf;;↗ Remove a group

;../NetInfo/ExamineUserAccount.rtf;;↗ Examine user accounts

;../NetInfo/ExamineGroup.rtf;;↗ Examine groups