

Managing User Accounts and User Environments in Oracle® Solaris 11.3

ORACLE

Part No: E54800
March 2017

Part No: E54800

Copyright © 1998, 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Référence: E54800

Copyright © 1998, 2017, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou ce matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

Contents

Using This Documentation	9
1 About User Accounts and User Environments	11
What's New in Managing User Accounts in Oracle Solaris 11.3	11
Expanded Login Options During Shutdown	11
Security Changes That Affect User Account Management	12
What Are User Accounts and Groups?	12
User Account Components	13
Guidelines for Assigning User Names, User IDs, and Group IDs	19
Where User Account and Group Information Is Stored	20
Fields in the passwd File	20
Default passwd File	21
Fields in the shadow File	23
Fields in the group File	23
Default group File	24
Commands for Obtaining User Account Information	24
Commands That Are Used for Managing Users, Roles, and Groups	25
About the User Work Environment	26
Using Site Initialization Files	27
Avoiding Local System References	28
Shell Features	28
Bash and ksh93 Shell History	30
Bash and Korn Shell Environment Variables	30
Customizing the Bash Shell	33
MANPATH Environment Variable	33
PATH Environment Variable	33
Guidelines for Setting PATH Variables	34
Locale Variables	34

Default File Permissions (umask)	35
Customizing a User Initialization File	36
Managing Users With Oracle Enterprise Manager Ops Center	37
2 Managing User Accounts by Using the Command-Line Interface	39
Task Map for Setting Up and Managing User Accounts by Using the CLI	39
Setting Up User Accounts by using the CLI	40
Guidelines for Setting Up User Accounts	41
Gathering User Information	42
Identifying Users by Packages	43
▼ How to Customize User Initialization Files	43
▼ How to Change Account Defaults For All Roles	44
Managing User Accounts by Using the CLI	44
▼ How to Add a User	45
▼ How to Modify a User Account	46
▼ How to Unlock a User Account	46
▼ How to Delete a User	47
▼ How to Add a Group	48
▼ How to Create the Home Directory for a User Without Creating a ZFS Dataset	49
Sharing ZFS File Systems	50
▼ How to Share Home Directories That Are Created as ZFS File Systems	50
Manually Mounting a User's Home Directory	51
3 Managing User Accounts by Using the User Manager GUI	53
Introducing the User Manager GUI	53
▼ How to Start the User Manager GUI	54
Organization of the User Manager Dialog Box	54
Filtering the Information Displayed in the GUI	55
Assuming a Role	57
Adding, Modifying, and Deleting Users and Roles by Using the User Manager GUI	57
▼ How to Add a User or Role With the User Manager GUI	58
▼ How to Modify a User or Role With the User Manager GUI	60
▼ How to Delete a User or Role With the User Manager GUI	60
Assigning Advanced Attributes With the User Manager GUI	61
Assigning Groups With the User Manager GUI	62

Assigning Roles With the User Manager GUI	63
Assigning Rights Profiles With the User Manager GUI	64
Assigning Authorizations With the User Manager GUI	65
Index	67

Using This Documentation

- **Overview** – Describes managing user accounts and user environments
- **Audience** – System administrators using the Oracle Solaris 11 release
- **Required knowledge** – Experience administering UNIX systems

Product Documentation Library

Documentation and resources for this product and related products are available at <http://www.oracle.com/pls/topic/lookup?ctx=E53394-01>.

Feedback

Provide feedback about this documentation at <http://www.oracle.com/goto/docfeedback>.

◆◆◆ CHAPTER 1

About User Accounts and User Environments

This chapter covers managing user accounts and user environments, including the following topics:

- [“What's New in Managing User Accounts in Oracle Solaris 11.3” on page 11](#)
- [“What Are User Accounts and Groups?” on page 12](#)
- [“Where User Account and Group Information Is Stored” on page 20](#)
- [“Commands That Are Used for Managing Users, Roles, and Groups” on page 25](#)
- [“About the User Work Environment” on page 26](#)

For task-related information about managing user accounts and user environments, see [Chapter 2, “Managing User Accounts by Using the Command-Line Interface”](#) and [Chapter 3, “Managing User Accounts by Using the User Manager GUI”](#).

What's New in Managing User Accounts in Oracle Solaris 11.3

This section describes new or changed features in this release:

- [“Expanded Login Options During Shutdown” on page 11](#)
- [“Security Changes That Affect User Account Management” on page 12](#)

Expanded Login Options During Shutdown

When the `shutdown` command is shutting down a system, the process creates an `/etc/nologin` file. This file displays a message indicating that the system is being shut down and that logins are not possible. Alternately, superuser can separately create and manage this `/etc/nologin` file.

This type of shutdown does not block the superuser from logging in. Starting in this release, the following additional users are not blocked when the `nologin` file is present on the system:

- Users assigned with the root role
- Users assigned with the `solaris.system.maintenance` authorization

For further information, see the [nologin\(4\)](#) and [shutdown\(1M\)](#) man pages.

Security Changes That Affect User Account Management

System administrators who manage user accounts should note that the following security features that have changed in this release:

- Specific extended rights can be applied to file objects, port numbers, and user IDs. These extended rights replace the set of rights that are otherwise available, except for the basic set.

For a discussion about expanding a user's rights, see [“Expanding a User or Role’s Privileges” in *Securing Users and Processes in Oracle Solaris 11.3*](#).

For instructions, see [Chapter 4, “Assigning Rights to Applications, Scripts, and Resources” in *Securing Users and Processes in Oracle Solaris 11.3*](#). Also, see the [ppriv\(1\)](#) or [privileges\(5\)](#) man pages.

- You can set the `auth_profiles` right so that users must provide a password before executing a command that is assigned through a rights profile. The password is effective for a configurable period of time.

The `AUTH_PROFS_GRANTED` keyword in the `policy.conf` file sets the password requirement for running a privileged command for all users of a system.

For further information, see [“Expanding Users’ Rights” in *Securing Users and Processes in Oracle Solaris 11.3*](#). Also, see the [useradd\(1M\)](#) and [usermod\(1M\)](#) man pages.

What Are User Accounts and Groups?

This section describes the following topics:

- [“User Account Components” on page 13](#)
- [“Guidelines for Assigning User Names, User IDs, and Group IDs” on page 19](#)

A typical user account includes the information a user needs to log in and use a system. User account components are described in [“User Account Components” on page 13](#).

When you set up a user account, you can add the user to a predefined group of users. A typical use of groups is to set up group permissions on a file or directory, which allows access only to those users who are part of that group.

For example, you might have a directory containing confidential files that only a few users should be able to access. You could set up a group called `private` that includes the users that are working on the non-public project. In addition, you could set up the `private` files with `read` permission for the `private` group so that only the users in the `private` group are able to read the files.

A special type of user account, called a *role*, gives special rights to specific users. For more information, see [Chapter 1, “About Using Rights to Control Users and Processes” in *Securing Users and Processes in Oracle Solaris 11.3*](#).

User Account Components

This section describes the various components of a user account.

User (Login) Names

User names, also called *login names*, enable users to access their own local and remote systems that have the appropriate access rights. You must choose a unique user name for each account that you create.

Consider establishing a standard way of assigning user names so that they are easier for you to track. Also, names should be easy for users to remember. A simple scheme when selecting a user name is to use the first name initial and first seven letters of the user's last name. For example, John Smith becomes `jsmith`. If this scheme results in duplicate names, you can use the first initial, middle initial, and the first six characters of the user's last name. For example, John Jay Smith becomes `jjsmith`.

If this scheme still results in duplicate names, consider using the following scheme to create a user name:

- Using the first initial, middle initial, and first five characters of the user's last name
- Adding the number 1, or 2, or 3, and so on, until you have a unique name

Note - User names must be distinct from any mail aliases that are known to the system or to a NIS domain. Otherwise, mail might be delivered to the alias rather than to the actual user.

For detailed guidelines on setting up user (login) names, see [“Guidelines for Assigning User Names, User IDs, and Group IDs” on page 19](#).

User ID Numbers

A unique user identification number (UID) is associated with each user name. The UID number identifies the user name to any system on which the user attempts to log in. It is also used by systems to identify the owners of files and directories. If you create user accounts for an individual on a number of different systems, always use the same user name and ID number. This enables the user to easily move files between systems without ownership problems.

UID numbers must be a whole number that is less than or equal to 2147483647. UID numbers are required for both regular user accounts and special system accounts. The following table lists the UID numbers that are reserved for user accounts and system accounts.

TABLE 1 Reserved UID Numbers

UID Numbers	User or Login Accounts	Description
0 – 99	root, daemon, bin, sys, and so on	Reserved for use by the operating system
100 – 2147483647	Regular users	General purpose accounts
60001 and 65534	nobody and nobody4	NFS Anonymous users
60002	noaccess	Reserved for OS

Do not assign UIDs 0 through 99. These UIDs are reserved for allocation by Oracle Solaris. By definition, root always has UID 0, daemon has UID 1, and pseudo-user bin has UID 2.

For additional guidelines on setting up UIDs, see [“Guidelines for Assigning User Names, User IDs, and Group IDs” on page 19](#).

As with user (login) names, you should adopt a scheme for assigning unique UID numbers. Some companies assign unique employee numbers. Then, administrators add a number to the employee number to create a unique UID number for each employee.

To minimize security risks, you should avoid reusing the UIDs from deleted accounts. If you must reuse a UID, remove the account information completely so that the new user is not affected by attributes set for a former user. For example, a former user might have been included in a printer deny list. However, denying access to that printer might be inappropriate for the new user.

Using Large User IDs and Group IDs

UIDs and group IDs (GIDs) can be assigned up to the maximum value of a signed integer, or 2147483647.

The following table describes UID and GID limitations.

TABLE 2 Large UID and GID Limitation Summary

UID or GID	Limitations
262144 or greater	Users who use the <code>cpio</code> command with the default archive format to copy a file see an error message for each file. The UIDs and GIDs are set to <code>nobody</code> in the archive.
2097152 or greater	Users who use the <code>cpio</code> command with the <code>-H odc</code> format or the <code>pax -x cpio</code> command to copy files see an error message returned for each file. The UIDs and GIDs are set to <code>nobody</code> in the archive.
1000000 or greater	Users who use the <code>ar</code> command have their UIDs and GIDs set to <code>nobody</code> in the archive.
2097152 or greater	Users who use the <code>tar</code> command, the <code>cpio -H ustar</code> command, or the <code>pax -x tar</code> command have their UIDs and GIDs set to <code>nobody</code> .

UNIX Groups

A *group* is a collection of users who can share files and other system resources. For example, users working on the same project can be formed into a group. A group is traditionally known as a UNIX group.

Each group must have a name, a group identification (GID) number, and a list of user names that belong to the group. A GID number identifies the group internally to the system.

The two types of groups that a user can belong to are as follows:

- **Primary group** – Specifies a group that the operating system assigns to files that are created by the user. Each user must belong to a primary group.
- **Secondary groups** – Specifies one or more groups to which a user also belongs. Users can belong to up to 1024 supplemental groups.

For detailed guidelines on setting up group names, see [“Guidelines for Assigning User Names, User IDs, and Group IDs” on page 19](#).

Sometimes, the secondary group of a user is not important. For example, ownership of files reflect the primary group, not secondary groups. Other applications, however, might rely on the secondary group memberships of a user. For example, a user has to be a member of the `sysadmin` group (group 14) to use the `Admintool` software in previous Oracle Solaris releases. However, it does not matter if group 14 is the user's current primary group.

The `groups` command lists the groups that a user belongs to. A user can have only one primary group at a time. However, users can temporarily change their primary group to any other group in which the user is a member by using the `newgrp` command.

When adding a user account, you must assign a primary group for a user or accept the default group, `staff` (group 10). The primary group should already exist. If the primary group does not exist, specify the group by a GID number. User names are not added to primary groups because the list might become too long. Before you can assign users to a new secondary group, you must create the group and assign it a GID number.

Groups can be local to a system or managed through a name service. To simplify group administration, you should use a name service such as NIS or a directory service such as LDAP. These services enable you to centrally manage group memberships.

User Passwords

You can specify a password for a user when you add the user. Or, you can force the user to specify a password when the user first logs in to the system. Although user names are publicly known, passwords must be kept secret and known only to users. Each user account should be assigned a password.

User passwords must comply with the following syntax:

- Password length is defined by the value `PASSLENGTH` in the `/etc/default/password` file.
The default password hashing algorithm is SHA256. As a result, user passwords are no longer limited to eight characters as in previous Oracle Solaris releases. The eight-character limitation applies only to passwords that use the older `crypt_unix(5)` algorithm, which has been preserved for backward compatibility with any existing `passwd` file entries and NIS maps.
New passwords must match the complexity rules within the maximum number of characters that are allowed for the password algorithm. Thus, if you are using the `crypt_unix` algorithm and you type a 20-character password, the password must match the complexity rules within the first 8 characters. If the password algorithm is any of the other algorithms, the password must match the complexity rules within the full password that is entered, which is 20 in this example.
- Each password must meet the configured complexity constraints that are specified in the `/etc/default/passwd` file.
- Each password must not be a member of the configured dictionary as specified in the `/etc/default/passwd` file.
- New passwords must not be present in the password history of the name service.

Your password change policy should follow industry standards. System administration logins, such as `root`, must be carefully controlled. Administration should be through users with appropriate rights profiles, roles, or `sudo`. These administrative methods use least privilege and write administrative events to the audit trail. For password attributes that Oracle Solaris can enforce when a password is changed, see the [passwd\(1\)](#) man page.

Many breaches of computer security involve guessing a legitimate user's password. You should make sure that users avoid using proper nouns, names, login names, and other passwords that a person might guess just by knowing something about the user.

Good choices for passwords include the following:

- Phrases (beameup).
- Words made up of the first letters of every word in a phrase. For example, swotr b for Somewhere Over The RainBow.
- Words with numbers or symbols substituted for letters. For example, sn00py for snoopy.

Do not use these choices for passwords:

- Your name (spelled forwards, backwards, or jumbled)
- Names of family members or pets
- Car license numbers
- Telephone numbers
- Social security numbers
- Employee numbers
- Words related to a hobby or interest
- Seasonal themes, such as Santa in December
- Any word in the dictionary

Home Directories

The home directory is the portion of a file system that is allocated to a user for storing private files. The amount of space you allocate for a home directory depends on the size of the system on which the directory is hosted, the kinds of files the user creates, the file size, and the number of files that are created.

A home directory can be located either on your local system or on a remote file server. In either case, by convention the home directory should be created as `/export/home/username`. For a large site, you should store home directories on a server. Use a separate file system for each user like `/export/home/alice` or `/export/home/bob`. By creating separate file systems for each user, you can set properties or attributes based on the needs of each user.

Regardless of where their home directory is located, users usually access their home directories through a mount point named `/home/username`. When AutoFS is used to mount home directories, you are not permitted to create any directories under the `/home` mount point on any system. The system recognizes the special status of `/home` when AutoFS is active. For more information about auto-mounting home directories, see [“Autofs Administration” in *Managing Network File Systems in Oracle Solaris 11.3*](#).

To use a home directory from anywhere on the network, you should always refer to the home directory as `$HOME`, not as `/export/home/username`. This is because the `/export/home/username` directory is system-specific. In addition, any symbolic links that are created in a user's home directory should use relative paths (for example, `../..../x/y/x`) so that the links are valid irrespective of where the home directory is mounted.

For more information about how home directories are added when you create user accounts by using the command-line interface, see [“Guidelines for Setting Up User Accounts” on page 41](#).

Naming Services

If you are managing user accounts for a large site, you might want to consider using a name or directory service such as LDAP or NIS. A name or directory service enables you to store user account information in a centralized manner instead of storing user account information in the `/etc` files of every system. When you use a name service or a directory service for user accounts, users can move from system to system using the same user account without having their information duplicated on every system. Using a naming service or a directory service also ensures consistent user account information.

User's Work Environment

Besides having a home directory to create and store files, users need an environment that gives them access to the tools and resources they need to do their work. When a user logs in to a system, the user's work environment is determined by initialization files. These files are defined by the user's startup shell, which can vary depending on the release.

A good strategy for managing the user work environment is to provide customized user initialization files, such as `.bash_profile`, `.bash_login`, `.kshrc`, or `.profile`, in the user's home directory.

Note - Do not use system initialization files, such as `/etc/profile` or `/etc/.login`, to manage the work environment of users. These files reside locally on systems and are not centrally administered. For example, if AutoFS is used to mount the home directory from any system on the network, you would have to modify the system initialization files on each system to ensure a consistent environment whenever a user moved from system to system.

For detailed information about customizing user initialization files for users, see [“About the User Work Environment” on page 26](#).

Guidelines for Assigning User Names, User IDs, and Group IDs

User names, UIDs, and GIDs should be unique within your organization, especially if your setup involves multiple domains.

Keep the following guidelines in mind when creating user or role names, UIDs, and GIDs:

- **User names** – Should contain from two to eight letters and numerals. The first character should be a letter. At least one character should be a lowercase letter.

Note - Even though user names can include a period (.), underscore (_), or hyphen (-), using these characters is not recommended because they can cause problems with some software products.

- **System accounts** – Do not use any of the user names, UIDs, or GIDs that are contained in the default `/etc/passwd` and `/etc/group` files. Do not use the UIDs and GIDs, 0-99. These numbers are reserved for allocation by Oracle Solaris and should not be used by anyone. Note that this restriction also applies to numbers not currently in use.

For example, `gdm` is the reserved user name and group name for the GNOME Display Manager daemon and should not be used for another user. For a complete listing of the default `/etc/passwd` and `/etc/group` entries, see [Table 3, “Default passwd File Entries,” on page 22](#) and [Table 4, “Default group File Entries,” on page 24](#).



Caution - The `nobody` and `nobody4` accounts should never be used for running processes. These two accounts are reserved for use by NFS. Use of these accounts for running processes could lead to unexpected security risks. Processes that need to run as non-root should use the `daemon` or `noaccess` accounts.

- **System account configuration** – The configuration of the default system accounts should never be changed, including never changing the login shell of a system account that is currently locked. The only exception to this rule is the setting of a password and password aging parameters for the root account.

Note - Changing a password for a locked user account changes the password but no longer unlocks the account at the same time. A second step to unlock the account by using the `passwd -u` command is now required.

Where User Account and Group Information Is Stored

This section covers the following information:

- [“Fields in the passwd File” on page 20](#)
- [“Default passwd File” on page 21](#)
- [“Fields in the shadow File” on page 23](#)
- [“Fields in the group File” on page 23](#)
- [“Default group File” on page 24](#)
- [“Commands for Obtaining User Account Information” on page 24](#)

Depending on your site policy, user account and group information can be stored in your local system's /etc files or in a name or directory service as follows:

- The NIS name service information is stored in maps
- The LDAP directory service information is stored in indexed database files

Note - To avoid confusion, the location of the user account and group information is generically referred to as a *file* rather than as a *database*, *table*, or *map*.

Most user account information is stored in the passwd file. Password information is stored as follows:

- In the passwd file when you are using NIS
- In the /etc/shadow file when you are using /etc files
- In the people container when you are using LDAP

Password aging is available when you are using LDAP, but not NIS.

Group information is stored in the group file for NIS. For LDAP, group information is stored in the group container.

Fields in the passwd File

The fields in the passwd file are separated by colons and contain the following information:

username:password:UID:GID:comment:home-directory:login-shell

For example:

```
kryten:x:101:100:Kryten Series 4000 Mechanoid:/export/home/kryten:/bin/csh
```

For a complete description of the fields in the passwd file, see the [passwd\(1\)](#) man page.

Default passwd File

The default passwd file contains entries for standard daemons. Daemons are processes that are usually started at boot time to perform some system-wide task, such as printing, network administration, or port monitoring.

Note - Additional users and groups are created and removed when packages are added or removed from the system. These ongoing changes are reflected in the passwd file. Administrators do not need to clean up this file.

The following display shows the contents of a sample passwd file:

```
root:x:0:0:Super-User:/root:/usr/bin/bash
daemon:x:1:1:/:
bin:x:2:2:/:usr/bin:
sys:x:3:3:/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
dladm:x:15:65:Datalink Admin:/:
netadm:x:16:65:Network Admin:/:
netcfg:x:17:65:Network Configuration Admin:/:
smmsp:x:25:25:SendMail Message Submission Program:/:
gdm:x:50:50:GDM Reserved UID:/var/lib/gdm:
zfsnap:x:51:12:ZFS Automatic Snapshots Reserved UID:/usr/bin/pfsh
upnp:x:52:52:UPnP Server Reserved UID:/var/coherence:/bin/ksh
xvm:x:60:60:xVM User:/:
mysql:x:70:70:MySQL Reserved UID:/:
openldap:x:75:75:OpenLDAP User:/:
webservd:x:80:80:WebServer Reserved UID:/:
postgres:x:90:90:PostgreSQL Reserved UID:/usr/bin/pfksh
svctag:x:95:12:Service Tag UID:/:
unknown:x:96:96:Unknown Remote UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
ikeuser:x:67:12:IKE Admin:/:
ftp:x:21:21:FTPD Reserved UID:/:
dhcpcserv:x:18:65:DHCP Configuration Admin:/:
aiuser:x:60003:60001:AI User:/:
```

```
pkg5srv:x:97:97:pkg(5) server UID:/:
```

The display above shows sample passwd file contents without any explanation. The following table provides a description and the source package information for each daemon in a standard passwd file.

TABLE 3 Default passwd File Entries

User Name	User ID	Description	Package
root	0	Reserved for superuser account	system/core-os
daemon	1	Umbrella system daemon associated with routine system tasks	system/core-os
bin	2	Administrative daemon associated with running system binaries to perform some routine system task	system/core-os
sys	3	Administrative daemon associated with system logging or updating files in temporary directories	system/core-os
adm	4	Administrative daemon associated with system logging	system/core-os
lp	71	Reserved for the Line printer daemon	system/core-os
uucp	5	Assigned to the daemon that is associated with uucp functions	system/core-os
nuucp	9	Assigned to another daemon associated with uucp functions	system/core-os
dladm	15	Reserved for datalink administration	system/core-os
netadm	16	Reserved for network administration	system/core-os
netcfg	17	Reserved for network configuration administration	system/core-os
smmsp	25	Assigned to the Sendmail message submission program daemon	system/core-os
gdm	50	Assigned to the GNOME Display Manager daemon	system/core-os
zfsnap	51	Reserved for automatic snapshots	system/core-os
upnp	52	Reserved for UPnP server	system/core-os
xvm	60	Reserved for xVM user	system/core-os
mysql	70	Reserved for MySQL user	system/core-os
openldap	75	Reserved for OpenLDAP user	library/ldap
websrvd	80	Reserved for WebServer access	system/core-os
postgres	90	Reserved for PostgreSQL access	system/core-os
svctag	95	Reserved for Service Tag Registry access	system/core-os

User Name	User ID	Description	Package
unknown	96	Reserved for unmappable remote users in NFSv4 ACLs	system/core-os
nobody	60001	Reserved for NFS Anonymous Access user	system/core-os
noaccess	60002	Reserved for No Access user	system/core-os
nobody4	65534	Reserved for SunOS 4.x NFS Anonymous Access user	system/core-os
ikeuser	67	Reserved for Internet Key Exchange (IKE) access	system/network/ike
ftp	21	Reserved for FTP access	service/network/ftp
dhcpsrv	18	Reserved for DHCP server user	service/network/dhcp/ isc-dhcp
aiuser	60003	Reserved for AI user	system/install/auto-install/ auto-install-common
pkg5srv	97	Reserved for pkg(5) depot server	package/pkg

Fields in the shadow File

The `/etc/shadow` file stores encrypted user passwords and related information. The fields in the shadow file are separated by colons and contain the following information:

username:password:lastchg:min:max:warn:inactive:expire

The default password hashing algorithm is SHA256. The password hash for the user is similar to the following:

`5cgQk2iUy$AhHtVGx5Qd0.W3NCKj1kb8.Kh0iA4DpxsW55sP0UnYD`

For a complete description of the fields in the shadow file, see the [shadow\(4\)](#) man page.

Fields in the group File

The group file is a local source of group information. The fields in the group file are separated by colons and contain the following information:

group-name:group-password:GID:user-list

For example:

```
bin::2:root,bin,daemon
```

For a complete description of the fields in the group file, see the [group\(4\)](#) man page.

Default group File

The default group file contains the following system groups that support some system-wide tasks such as printing, network administration, or electronic mail. Most of these groups have corresponding entries in the `passwd` file.

The following displays the contents of a sample group file.

```
root::0:
other::1:root
bin::2:root,daemon
sys::3:root,bin,adm
adm::4:root,daemon
```

The display above provides sample group file contents without any explanations. The following table provides further information about each group listed in a typical group file.

TABLE 4 Default group File Entries

Group Name	Group ID	Description	pkg(5)
root	0	Superuser group	system/core-os
other	1	Optional group	system/core-os
bin	2	Administrative group associated with running system binaries	system/core-os
sys	3	Administrative group associated with system logging or temporary directories	system/core-os
adm	4	Administrative group associated with system logging	system/core-os

Commands for Obtaining User Account Information

The following table describes the commands that system administrators can use to obtain information about user accounts. This information is stored in various files within the `/etc`

directory. Using these commands to obtain user account information is preferred over using the `cat` command to view similar information.

TABLE 5 Commands to Obtain Information About Users

Command	Description	Man Page Reference
<code>auths</code>	Lists and manages authorizations.	auths(1)
<code>getent</code>	Displays a list of entries from the administrative database. The information generally comes from one or more of the sources that are specified for the <code>/etc/nsswitch.conf</code> database.	getent(1M)
<code>logins</code>	Displays information about users, roles, and system logins. The output is controlled by the command options that are specified and can include user, role, system login, UID, <code>passwd</code> account field value, primary group, primary group ID, multiple group names, multiple group IDs, home directory, login shell, and password-aging parameters.	logins(1M)
<code>profiles</code>	Lists and manages rights profiles.	profiles(1)
<code>roles</code>	Displays the roles that are assigned to a user.	roles(1)
<code>userattr</code>	Displays the first value that is found for <code>attribute_name</code> . If a user is not specified, the user is taken from the real user ID of the process. Attribute names are defined in the user_attr(4) and prof_attr(4) man pages. Note - This command is new in Oracle Solaris 11.	userattr(1)

Commands That Are Used for Managing Users, Roles, and Groups

Note - The Solaris Management Console GUI, and the command-line interface (CLI) that is associated with this GUI, are no longer supported.

The commands described in the following table are used for managing users, roles, and groups.

TABLE 6 Commands Used to Manage Users, Roles, and Groups

Man Page Reference	Description	See Also
useradd(1M)	Creates users locally or in an LDAP repository.	“How to Add a User” on page 45
usermod(1M)	Changes user properties locally or in an LDAP repository. If the user properties are security-relevant, such as role assignment,	“How to Modify a User Account” on page 46 “Creating a Role” in <i>Securing Users and Processes in Oracle Solaris 11.3</i>

Man Page Reference	Description	See Also
	this task might be restricted to your security administrator or to the root role.	
userdel(1M)	Deletes a user from the system or from the LDAP repository. Can involve additional cleanup, such as cron job removal.	“How to Delete a User” on page 47
roleadd(1M) rolemod(1M) roledel(1M)	Manages roles locally or in an LDAP repository. Roles cannot log in. Users assume an assigned role to perform administrative tasks.	“Assigning Rights to Users” in <i>Securing Users and Processes in Oracle Solaris 11.3</i>
groupadd(1M) groupmod(1M) groupdel(1M)	Manages groups locally or in an LDAP repository.	“How to Add a Group” on page 48

About the User Work Environment

This section covers the following topics:

- [“Using Site Initialization Files” on page 27](#)
- [“Avoiding Local System References” on page 28](#)
- [“Shell Features” on page 28](#)
- [“Bash and ksh93 Shell History” on page 30](#)
- [“Bash and Korn Shell Environment Variables” on page 30](#)
- [“Customizing the Bash Shell” on page 33](#)
- [“Guidelines for Setting PATH Variables” on page 34](#)
- [“MANPATH Environment Variable” on page 33](#)
- [“PATH Environment Variable” on page 33](#)
- [“Locale Variables” on page 34](#)
- [“Default File Permissions \(umask\)” on page 35](#)
- [“Customizing a User Initialization File” on page 36](#)

Part of setting up the home directory for user is providing user initialization files for the login shell of the user. A *user initialization file* is a shell script that sets up a work environment for a user after the user logs in to a system. Basically, you can perform any task in a user initialization file that you can do in a shell script. However, a user initialization file's primary job is to define the characteristics of user work environment, such as a user's search path, environment variables, and windowing environment. Each login shell has its own user

initialization file or files, which are listed in the following table. Note that the default user initialization file for both the bash and ksh93 shells is `/etc/skel/local.profile`.

TABLE 7 Bash and ksh93 User Initialization Files

Shell	User Initialization File	Purpose
bash	<code>\$HOME/.bash_profile</code>	Defines the user's environment at login
	<code>\$HOME/.bash_login</code>	
	<code>\$HOME/.profile</code>	
ksh93	<code>/etc/profile</code>	Defines the user's environment at login
	<code>\$HOME/.profile</code>	
(Korn)	<code>\$ENV</code>	Defines the user's environment at login within the file and is specified by the Korn shell's <code>ENV</code> environment variable

You can use these files as a starting point and then modify them to create a standard set of files that provide the work environment common to all users. You can also modify these files to provide the working environment for different types of users.

For step-by-step instructions on how to create sets of user initialization files for different types of users, see [“How to Customize User Initialization Files” on page 43](#).

Using Site Initialization Files

The user initialization files can be customized by both the administrator and the user. This important task can be accomplished with centrally located and globally distributed user initialization files that are called *site initialization files*. Site initialization files enable you to continually introduce new functionality to the user's work environment while enabling the user to customize the user's initialization file.

When you reference a site initialization file in a user initialization file, all updates to the site initialization file are automatically reflected when the user logs in to the system or when a user starts a new shell. Site initialization files enable you to distribute site-wide changes to users' work environments that you did not anticipate when you added the users.

You can customize a site initialization file the same way that you customize a user initialization file. These files typically reside on a server, or set of servers, and appear as the first statement in a user initialization file. Also, each site initialization file must be the same type of shell script as the user initialization file that references it.

To reference a site initialization file in a bash or ksh93 user initialization file, place a line at the beginning of the user initialization file similar to the following line:

. /net/machine-name/export/site-files/site-init-file

Avoiding Local System References

Do not add specific references to the local system in the user initialization file. The instructions in a user initialization file should be valid regardless of which system the user logs into.

For example:

- To make a user's home directory available anywhere on the network, always refer to the home directory with the variable `$HOME`. For example, use `$HOME/bin` instead of `/export/home/username/bin`. The `$HOME` variable works when the user logs in to another system, and the home directories are auto-mounted.
- To access files on a local disk, use global path names, such as `/net/system-name/directory-name`. Any directory referenced by `/net/system-name` can be mounted automatically on any system on which the user logs in, assuming the system is running AutoFS.

Shell Features

The following shell features and behavior are supported in the Oracle Solaris OS:

- The user account that is created when you install the Oracle Solaris release is assigned the GNU Bourne-Again Shell (bash) by default.
- The standard system shell (bin/sh) is now the Korn Shell 93 (ksh93).
- The default interactive shell is the Bourne-again (bash) shell (`/usr/bin/bash`).
- Both the bash and ksh93 shells feature command-line editing, which means you can edit commands before executing them.
- You can display default shell and path information in a few different ways. They are as follows:

- Use the `echo $SHELL` and `which` commands

```
$ grep root /etc/passwd
root:x:0:0:Super-User:/root:/usr/bin/bash
```

```
$ echo $SHELL
/usr/bin/bash
```

```
$ which ksh93
/usr/bin/ksh93
```

- Use the `pargs` command

```
~$ pargs -l $$
/usr/bin/i86/ksh93
```

- The ksh93 shell also has a built-in variable called `.sh.version`, which can be displayed as follows:

```
~$ echo ${.sh.version}
Version jM 93u 2011-02-08
```

- To change to a different shell, type the path of the shell that you want to use.
- To exit a shell, type `exit`.

The following table describes the shell options that are supported in Oracle Solaris.

TABLE 8 Basic Shell Features in the Oracle Solaris Release

Shell	Path	Comments
Bourne-Again Shell (bash)	<code>/usr/bin/bash</code>	Default shell for users that are created by an installer, as well as the root role The default (interactive) shell for users that are created with the <code>useradd</code> command as well as the root role is <code>/usr/bin/bash</code> . The default path is <code>/usr/bin:/usr/sbin</code> .
Korn Shell	<code>/usr/bin/ksh</code>	ksh93 is the default shell in the Oracle Solaris OS.
C Shell and enhanced C Shell	<code>/usr/bin/csh</code> and <code>/usr/bin/tcsh</code>	C Shell and enhanced C Shell
POSIX-compliant Shell	<code>/usr/xpg4/bin/sh</code>	POSIX-compliant shell
Z Shell	<code>/usr/bin/zsh</code>	Z Shell

Note - The Z Shell (`zsh`) and the enhanced C Shell (`tcsh`) are not installed on your system by default. To use either of these shells, you must first install the required software packages.

The following table shows the default UNIX[®] system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

TABLE 9 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	<code>\$</code>

Shell	Prompt
Bash shell, Korn shell, and Bourne shell for superuser	#
C shell	machine_name%
C shell for superuser	machine_name#

Bash and ksh93 Shell History

Both the `bash` and `ksh93` shells record a history of all of the commands that you run. This history is kept on a per-user basis, which means the history is persistent between login sessions, as well as representative of all your login sessions.

For example, if you are in a `bash` shell, you can display the complete history of the commands that you have run as follows:

```
$ history
1 ls
2 ls -a
3 pwd
4 whoami
.
.
.
```

To display a number of previous commands, include an integer in the command.

```
$ history 2
12 date
13 history
```

For more information, see the [history\(1\)](#) man page.

Bash and Korn Shell Environment Variables

The `bash` and `ksh93` shells store special variable information that is known to the shell as an *environment variable*. To view a complete list of the current environment variables for the `bash` shell, use the `declare` command.

```
$ declare
BASH=/usr/bin/bash
BASH_ARGC=( )
```

```
BASH_ARGV=(  
BASH_LINEND=(  
BASH_SOURCE=(  
BASH_VERSINFO=( [0]='3' [1]='2' [2]='25' [3]='1'  
[4]='release' [5]'  
.  
.  
.
```

For the ksh93 shell, use the `set` command, which is the equivalent of the `declare` command in bash shell.

```
$ set  
  COLUMNS=80  
  ENV='$HOME/.kshrc'  
  FCEDIT=/bin/ed  
  HISTCMD=3  
  HZ=''  
  IFS=$' \t\n'  
  KSH_VERSION=.sh.version  
  LANG=C  
  LINENO=1  
.  
.  
.
```

To print environment variables for either shell, use the `echo` or `printf` command. For example:

```
$ echo $SHELL  
/usr/bin/bash  
$ printf "$PATH\n"  
/usr/bin:/usr/sbin
```

Note - Environment variables do not persist between sessions. To set up persistent environment variable values, set the values in the `.bashrc` file.

A shell can have two types of variables:

Environment variables

Specifies variables that are exported to all processes that are spawned by the shell. The `export` command is used to export a variable. For example:

```
export VARIABLE=value
```

These settings can be displayed by using the `env` command. A subset of environment variables, such as `PATH`, affects the behavior of the shell itself.

Shell (local) variables

Specifies variables that affect only the current shell.

In a user initialization file, you can customize a user's shell environment by changing the values of the predefined variables or by specifying additional variables.

The following table provides more details about the shell and environment variables that are available in the Oracle Solaris OS.

TABLE 10 Shell and Environment Variable Descriptions

Variable	Description
CDPATH	Sets a variable that is used by the <code>cd</code> command. If the target directory of the <code>cd</code> command is specified as a relative path name, the <code>cd</code> command first searches for the target directory in the current directory (<code>.</code>). If the target is not found, the path names that are listed in the <code>CDPATH</code> variable are searched consecutively until the target directory is found and the directory change is completed. If the target directory is not found, the current working directory is left unmodified. For example, suppose the <code>CDPATH</code> variable is set to <code>/home/jean</code> , and two directories exist under <code>/home/jean</code> , <code>bin</code> and <code>doc</code> . If you are in the <code>/home/jean/bin</code> directory and type <code>cd doc</code> , you change directories to <code>/home/jean/doc</code> , even though you do not specify a full path.
HOME	Sets the path to the user's home directory.
LANG	Sets the locale.
LOGNAME	Defines the name of the user that is currently logged in. The default value of <code>LOGNAME</code> is automatically set by the login program to the user name that is specified in the <code>passwd</code> file. You should only use the variable for a reference, and not reset it.
MAIL	Sets the path to the user's mailbox.
MANPATH	Sets the hierarchies of man pages that are available. Note - Starting with Oracle Solaris 11, the <code>MANPATH</code> environment variable is no longer required. The <code>man</code> command determines the appropriate <code>MANPATH</code> based on the <code>PATH</code> environment variable setting.
PATH	Specifies, in order, the directories that the shell searches to find the program to run when the user types a command. If the directory is not in the search path, users must type the complete path name of a command. As part of the login process, the default <code>PATH</code> is automatically defined and set as specified in <code>.profile</code> . The order of the search path is important. When identical commands exist in different locations, the first command that is found with that name is used. For example, suppose that <code>PATH</code> is defined in the shell syntax as <code>PATH=/usr/bin:/usr/sbin:\$HOME/bin</code> and a file named <code>sample</code> resides in both <code>/usr/bin</code> and <code>/home/jean/bin</code> . If the user types the command <code>sample</code> without specifying its full path name, the version that is found in <code>/usr/bin</code> is used.
PS1	Defines the shell prompt for the <code>bash</code> or <code>ksh93</code> shell.
SHELL	Sets the default shell used by <code>make</code> , <code>vi</code> , and other tools.
TERMINFO	Names a directory where an alternate <code>terminfo</code> database is stored. Use the <code>TERMINFO</code> variable in either the <code>/etc/profile</code> or <code>/etc/.login</code> file. For more information, see the terminfo(4) man page.

Variable	Description
	When the <code>TERMINFO</code> environment variable is set, the system first checks the <code>TERMINFO</code> path defined by the user. If the system does not find a definition for a terminal in the <code>TERMINFO</code> directory defined by the user, it searches the default directory, <code>/usr/share/lib/terminfo</code> , for a definition. If the system does not find a definition in either location, the terminal is identified as "dumb".
<code>TERM</code>	Defines the terminal. This variable should be reset in either the <code>/etc/profile</code> or <code>/etc/.login</code> file. When the user invokes an editor, the system looks for a file with the same name that is defined in this environment variable. The system searches the directory referenced by <code>TERMINFO</code> to determine the terminal characteristics.
<code>TZ</code>	Sets the time zone. The time zone is used to display dates, for example, in the <code>ls -l</code> command. If <code>TZ</code> is not set in the user's environment, the system setting is used. Otherwise, Greenwich Mean Time is used.

Customizing the Bash Shell

To customize your bash shell, add to or change the information in the `.bashrc` file that is located in your home directory. The initial user that is created when you install Oracle Solaris has a `.bashrc` file that sets the `PATH`, `MANPATH`, and command prompt. For more information, see the [bash\(1\)](#) man page.

MANPATH Environment Variable

The `MANPATH` environment variable specifies where the `man` command looks for reference manual (`man`) pages. The `MANPATH` is set automatically based on a user's `PATH` value, but it generally includes `/usr/share/man` and `usr/gnu/share/man`.

Note that a user's `MANPATH` environment variable can be modified independent of the `PATH` environment variable. A one-to-one equivalent of the associated man page locations with directories in the user's `$PATH` is not required.

PATH Environment Variable

When the user executes a command by using the full path, the shell uses that path to find the command. However, when users specify only a command name, the shell searches the directories for the command in the order specified by the `PATH` variable. If the command is found in one of the directories, the shell executes the command.

A default path is set by the system. However, most users modify it to add other command directories. Many user problems related to setting up the environment and accessing the correct version of a command or a tool can be traced to incorrectly defined paths.

Guidelines for Setting PATH Variables

The guidelines for setting up PATH variables are as follows:

- If you must include the current directory (.) in your path, place it last. Including the current directory in your path is a security risk because some malicious person could hide a compromised script or executable in the current directory. Consider using absolute path names instead.
- Keep the search path as short as possible. The shell searches each directory in the path. If a command is not found, long searches can slow down system performance.
- The search path is read from left to right, so you should put directories for commonly used commands at the beginning of the path.
- Make sure that directories are not duplicated in the path.
- Avoid searching large directories, if possible. Put large directories at the end of the path.
- Put local directories before NFS mounted directories to lessen the chance of the system becoming nonresponsive when the NFS server does not respond. This strategy also reduces unnecessary network traffic.

Locale Variables

The LANG and LC environment variables specify the locale-specific conversions and conventions for the shell. These conversions and conventions include time zones, collation orders, and formats of dates, time, currency, and numbers. In addition, you can use the `stty` command in a user initialization file to indicate whether the terminal session will support multibyte characters.

The LANG variable sets all possible conversions and conventions for the given locale. You can set various aspects of localization separately through the LC variables LC_COLLATE, LC_CTYPE, LC_MESSAGES, LC_NUMERIC, LC_MONETARY, and LC_TIME.

Note - By default, Oracle Solaris 11 installs UTF-8 based locales only.

The following table describes the environment variable values for the core Oracle Solaris 11 locales.

TABLE 11 Values for Locale Variables

Value	Locale
en_US.UTF-8	English, United States (UTF-8)
fr_FR.UTF-8	French, France (UTF-8)
de_DE.UTF-8	German, Germany (UTF-8)
it_IT.UTF-8	Italian, Italy (UTF-8)
ja_JP.UTF-8	Japanese, Japan (UTF-8)
ko_KR.UTF-8	Korean, Korea (UTF-8)
pt_BR.UTF-8	Portuguese, Brazil (UTF-8)
zh_CN.UTF-8	Simplified Chinese, China (UTF-8)
es_ES.UTF-8	Spanish, Spain (UTF-8)
zh_TW.UTF-8	Traditional Chinese, Taiwan (UTF-8)

EXAMPLE 1 Setting the Locale

In an `sh` or `ksh` shell user initialization file, you would add the following:

```
LANG=de_DE.ISO8859-1; export LANG
```

Default File Permissions (umask)

When you create a file or directory, the default file permissions assigned to the file or directory are controlled by the *user mask*. The user mask is set by the `umask` command in a user initialization file. You can display the current value of the user mask by typing `umask` and pressing Return.

The user mask contains the following octal values:

- The first digit sets permissions for the user
- The second digit sets permissions for group
- The third digit sets permissions for other, also referred to as `world`

Note that if the first digit is zero, it is not displayed. For example, if the user mask is set to 022, 22 is displayed.

To determine the `umask` value that you want to set, subtract the value of the permissions you want from 666 (for a file) or 777 (for a directory). The remainder is the value to use with the `umask` command. For example, suppose you want to change the default mode for files to 644 (`rw-r--r--`). The difference between 666 and 644 is 022, which is the value you would use as an argument to the `umask` command.

The following table provides `umask` values . It shows the file and directory permissions that are created for each of the octal values of `umask`.

TABLE 12 Permissions for `umask` Values

<code>umask</code> Octal Value	File Permissions	Directory Permissions
0	<code>rw-</code>	<code>rwx</code>
1	<code>rw-</code>	<code>rw-</code>
2	<code>r--</code>	<code>r-x</code>
3	<code>r--</code>	<code>r--</code>
4	<code>-w-</code>	<code>-wx</code>
5	<code>-w-</code>	<code>-w-</code>
6	<code>--x</code>	<code>--x</code>
7	<code>---</code> (none)	<code>---</code> (none)

The following line in a user initialization file sets the default file permissions to `rw-rw-rw-`.

```
umask 000
```

Customizing a User Initialization File

The following example shows a sample of the `.profile` user initialization file. You can use this sample file as a template to customize your own user initialization files. This example uses system names and paths that you will need to modify for your particular site.

EXAMPLE 2 `.profile` File

```
PATH=$PATH:$HOME/bin:/usr/local/bin:/usr/gnu/bin:      User's shell search path
MAIL=/var/mail/$LOGNAME      Path to user's mail file
NNTPSERVER=server1      User's time/clock server
MANPATH=/usr/share/man:/usr/local/man      User's search path for man pages
PRINTER=printer1      User's default printer
umask 022      User's default file creation permissions
export PATH MAIL NNTPSERVER MANPATH PRINTER      Sets the listed environment variables
```

Managing Users With Oracle Enterprise Manager Ops Center

If you are managing physical and virtual operating systems, servers, and storage devices within a large deployment, rather than just managing individual systems, you can use the management solutions available in the Oracle Enterprise Manager Ops Center.

With the Enterprise Manager Ops Center you can manage users and roles for the overall data center. You can add existing local users from your individual systems as users in the Ops Center, and you can control what assets and features these users are authorized to use.

For information, see <http://www.oracle.com/pls/topic/lookup?ctx=oc122>.

◆◆◆ CHAPTER 2

Managing User Accounts by Using the Command-Line Interface

This chapter provides basic information for setting up and managing user accounts by using the command-line interface (CLI).

For overview information about managing user accounts and user environments, see [Chapter 1, “About User Accounts and User Environments”](#).

For information about managing users and roles by using the User Manager graphical user interface (GUI), see [Chapter 3, “Managing User Accounts by Using the User Manager GUI”](#).

Task Map for Setting Up and Managing User Accounts by Using the CLI

The following tasks describe how to set up and manage user accounts by using the command-line interface (CLI).

Task	Description	For Instructions
Gather user information	Use a standard form to gather user information to help you keep user information organized.	“Gathering User Information” on page 42
Customize user initialization files	Set up user initialization files to provide new users with consistent environments.	“How to Customize User Initialization Files” on page 43
Change account defaults for all roles	Change the default home directory and skeleton directory for all roles.	“How to Change Account Defaults For All Roles” on page 44
Create a user account	Create a local user by using the <code>useradd</code> command with the account defaults that you have set up.	“How to Add a User” on page 45
Modify a user account	Modify the login information of a user on the system.	“How to Modify a User Account” on page 46

Task	Description	For Instructions
Unlock a user account	Unlock a user account using the <code>passwd -u</code> command.	“How to Unlock a User Account” on page 46
Delete a user account	Delete a user account by using the <code>userdel</code> command.	“How to Delete a User” on page 47
Create, then assign a role to perform an administrative task.	Create a local role to enable the user to perform specific administrative commands or tasks with the account defaults that you have set up.	“Creating a Role” in <i>Securing Users and Processes in Oracle Solaris 11.3</i>
Create a group	Create a new group by using the <code>groupadd</code> command.	“How to Add a Group” on page 48
Create home directories for users without creating a ZFS dataset.	Create the home directory for users without creating a ZFS dataset for each user.	“How to Create the Home Directory for a User Without Creating a ZFS Dataset” on page 49
Add security attributes to a user account	Add the required security attributes after setting up the local user accounts.	“Creating a Role” in <i>Securing Users and Processes in Oracle Solaris 11.3</i>
Share a user's home directory	Share the home directory of the user in order to remotely mount the directory from the system of the user.	“How to Share Home Directories That Are Created as ZFS File Systems” on page 50
Manually mount a user's home directory	Typically, you do not need to manually mount user home directories that are created as a ZFS file system. The home directory is mounted automatically when it is created and also at boot time from the SMF local file system service.	“Manually Mounting a User's Home Directory” on page 51

Setting Up User Accounts by using the CLI

This section describes the following topics:

- [“Guidelines for Setting Up User Accounts” on page 41](#)
- [“Gathering User Information” on page 42](#)
- [“Identifying Users by Packages” on page 43](#)
- [“How to Customize User Initialization Files” on page 43](#)
- [“How to Change Account Defaults For All Roles” on page 44](#)

Guidelines for Setting Up User Accounts

Note the following guidelines for setting up user accounts by using the CLI:

- In the Oracle Solaris OS, user accounts are created as Oracle Solaris ZFS file systems. As an administrator, when you create user accounts, you are giving users their own file system and their own ZFS dataset. Every home directory that is created by using the `useradd` and `roleadd` commands places the home directory of the user on the `/export/home` file system as an *individual* ZFS file system. As a result, users have the ability to back up their home directories, create ZFS snapshots of their home directories, and replace files in their current home directory from the ZFS snapshots that they created.
- To set up user accounts, you must assume the root role or a role that has the appropriate rights profile, for example, the User Management rights profile. For more information, see [“Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3*](#).
- When you create a user account with the `useradd` command, you must specify the `-m` option to create a home directory for the user.

For example, the following command will create a home directory for the user `jdoe`:

```
# useradd -m jdoe
```

But, the following syntax will *not* create a home directory for the user:

```
# useradd jdoe
```

Note - If you want the `pam_zfs_key` module to create an encrypted home directory for the user, do *not* specify the `-m` option with the `useradd` command. See the [`pam_zfs_key\(5\)`](#) and [`zfs_encrypt\(1M\)`](#) man pages.

- The `useradd` command creates entries in the `auto_home` map *only* if the `-d` option is specified with `hostname:/pathname`. Otherwise, the path name that is specified is updated as the home directory for the user in the `passwd` database, and no `auto_home` map entry is created. Home directories that are specified in the `auto_home` automounter map are only mounted if the `autofs` service is enabled.

For example, if you specify the `-d` option to create a user as follows, the user is created without an `auto_home` entry, and the `passwd` entry specifies `/export/home/user1` as the user's home directory:

```
# useradd -d /export/home/user1 user1
```

If you use the `-d` option to create the user as follows, the user will have an `auto_home` entry, and the `passwd` database will contain `/home/user1`, indicating a dependency on the `autofs` service.

```
# useradd -d localhost:/export/home/user1 user1
```

- If the pathname of the home directory includes a remote host specification, for example, `foobar:/export/home/jdoe`, then the home directory for `jdoe` must be created on the system `foobar`. The default pathname is `localhost:/export/home/username`.
- When the file system is a ZFS dataset, which is the case for all of Oracle Solaris 11, the user's home directory is created as a child ZFS dataset, with the ZFS permission to take snapshots delegated to the user. If a pathname is specified that does not correspond to a ZFS dataset, then a regular directory is created. If the `-S ldap` option is specified, then the `auto_home` map entry is updated on the LDAP server instead of the local `auto_home` map.

Gathering User Information

When setting up user accounts, you can create a form similar to the following form to gather information about users before setting up their accounts.

Item	Description
User Name	
Role Name	
Profiles or Authorizations	
UID	
Primary Group	
Secondary Groups	
Comment	
Default Shell	
Password Status and Aging	
Home Directory Path Name	
Mounting Method	
Permissions on Home Directory	
Mail Server	
Add to These Mail Aliases	
Desktop System Name	

Identifying Users by Packages

To find all the users that were delivered by a package (do not represent humans) on this system, you must specify the `--l` option. Note that this search excludes user packages created manually by the `useradd` command.

```
:$ pkg search -l username, pkg.name user::
```



Caution - Do not try to change the users' output with the `pkg search` command.

▼ How to Customize User Initialization Files

The following task describes how to set up customized initialization files for the user on your system.

1. **Become an administrator or a user with the User Management rights profile.**

```
$ su -
Password:
#
```

For more information, see [“Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3*](#).

2. **Create a skeleton directory for each type of user.**

```
# mkdir /shared-dir/skel/user-type
```

shared-dir The name of a directory that is available to other systems on the network

user-type The name of a directory to store initialization files for a type of user

3. **Copy the default user initialization files into the directories that you created for different types of users.**

4. **Customize the user initialization files for each user type.**

For a detailed description on how to customize the user initialization files, see [“About the User Work Environment” on page 26](#).

5. **Set the permissions for the user initialization files.**

```
# chmod 744 /shared-dir/skel/user-type/*
```

6. **Verify that the permissions for the user initialization files are correct.**

```
# ls -la /shared-dir/skel/*
```

▼ How to Change Account Defaults For All Roles

In the following procedure, the administrator has customized a `roles` directory. The administrator changes the default home directory and skeleton directory for all roles.

1. **Become an administrator or a user with the User Management rights profile.**
See [“Using Your Assigned Administrative Rights”](#) in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Create a custom roles directory.**

For example:

```
# roleadd -D
group=other,1 project=default,3 basedir=/home
skel=/etc/skel shell=/bin/pfsh inactive=0
expire= auths= profiles=All limitpriv=
defaultpriv= lock_after_retries=
```

3. **Change the default home directory and skeleton directory for all roles.**

For example:

```
# roleadd -D -b /export/home -k /etc/skel/roles
# roleadd -D
group=staff,10 project=default,3 basedir=/export/home
skel=/etc/skel/roles shell=/bin/sh inactive=0
expire= auths= profiles= roles= limitpriv=
defaultpriv= lock_after_retries=
```

Further use of the `roleadd` command will now create home directories in the `/export/home` directory, and will populate the roles' environment from the `/etc/skel/roles` directory.

Managing User Accounts by Using the CLI

This section covers the following:

- “How to Add a User” on page 45
- “How to Modify a User Account” on page 46
- “How to Unlock a User Account” on page 46
- “How to Delete a User” on page 47
- “How to Add a Group” on page 48
- “How to Create the Home Directory for a User Without Creating a ZFS Dataset” on page 49
- “Sharing ZFS File Systems” on page 50
- “How to Share Home Directories That Are Created as ZFS File Systems” on page 50
- “Manually Mounting a User's Home Directory” on page 51

▼ How to Add a User

1. Become an administrator or a user with the User Management rights profile.

See “Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3*.

2. Create a local user.

By default, the user is created locally. If you include the `-S ldap` option, the user is created in an existing LDAP repository.

```
# useradd -d dir -m username
```

`-d` Specifies the location of the home directory of the user
Use the `-d localhost:/export/home/username` instead of `-d /export/home/username` to force the entry to be written to `auto_home`.

`-m` Creates a local home directory on the system for the user.

For a detailed description of all of the options and arguments that you can specify with the `useradd` command, see the [useradd\(1M\)](#) man page.

Note - The account is locked until you assign the user a password.

3. Assign the user a password.

```
# passwd username
New password:      Type user password
Re-enter new password:  Retype password
```

For more command options, see the [useradd\(1M\)](#) and [passwd\(1\)](#) man pages.

See Also After creating a user, you might need to perform some additional tasks, including adding and assigning roles to a user, and displaying or changing the rights profiles of a user. For more information, see [“Creating a Role” in *Securing Users and Processes in Oracle Solaris 11.3*](#).

▼ How to Modify a User Account

The `usermod` command is used to change the definition of a user's login and make appropriate login-related file system changes for the user.

1. **Become an administrator or log in as a user who has the User Management rights profile.**

See [“Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3*](#).

2. **Modify the user account, as required.**

See the [usermod\(1M\)](#) man page for details about the arguments and options that you can specify with the `usermod` command.

For example, to add a role to a user, you would type:

```
# usermod -R role username
```

Example 3 Setting Per-User PAM Policy by Modifying a User's Account

The following example shows how to modify a user to set PAM policy. This particular modification specifies that user `jdoe` should only be authenticated with the Kerberos V5 protocol for all PAM services. For more information, see the [pam_user_policy\(5\)](#) man page.

```
# usermod -K pam_policy=krb5_only jdoe
```

See Also For additional information, see [“Creating a Role” in *Securing Users and Processes in Oracle Solaris 11.3*](#).

▼ How to Unlock a User Account

1. **Become an administrator or log in as a user who has the User Security rights profile.**

See “Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3* in *Securing Users and Processes in Oracle Solaris 11.3*.

2. Check the status of the user account that you need to unlock.

```
$ passwd -s username
username    LK
```

3. Unlock the user account.

```
$ passwd -u username
passwd: password information changed for username
```

4. Check if the desired user account has been unlocked.

```
$ passwd -s
username    PS
```

Note - For more information about unlocking a user account, see “Guidelines for Assigning User Names, User IDs, and Group IDs” on page 19 and the `passwd(1)` man page.

▼ How to Delete a User

1. Become an administrator.

```
$ su -
Password:
#
```

Note - This method works whether `root` is a user account or a role.

2. Archive the home directory of the user.

3. Delete the user.

```
# userdel -r username
```

The `-r` option removes the account from the system.

The preferred method for removing a local home directory for a deleted user is to specify the `-r` option with the `userdel` command. This method is preferred because user home directories are now ZFS datasets.

4. **If the user's home directory is on a remote server, manually delete it.**

```
# userdel username
```

For a full list of command options, see the [userdel\(1M\)](#) man page.

Next Steps Additional cleanup might be required if the user that you deleted had administrative responsibilities, for example creating cron jobs, or if the user had additional accounts in non-global zones.

▼ How to Add a Group

When an administrator creates a group, the system assigns the `solaris.group.assign/groupname` to that administrator, giving the administrator complete control over that group. If another administrator who has the same authorization creates a group, that administrator has the control over that group. An administrator who has control of one group cannot administer the group of the other administrator. For more information, see the [groupadd\(1M\)](#) and [groupmod\(1M\)](#) man pages.

1. **Become an administrator or a user who has the `solaris.group.manage` authorization.**

See “Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **List the existing groups.**

```
# cat /etc/group
```

3. **Create a new group.**

```
$ groupadd -g group-id group-name
```

-g Assigns the group ID for the new group

For more information, see the [groupadd\(1M\)](#) man page.

Example 4 Setting Up a Group and User With the `groupadd` and `useradd` Commands

The following example shows how to use the `groupadd` and `useradd` commands to add the group `scutters` and the user `scutter1` to files on the local system.

```
# groupadd -g 102 scutters
```



```
# useradd -u 1003 -g 102 -d /export/home/scutter1 -s /bin/csh \  
-c "Scutter 1" -m -k /etc/skel scutter1  
64 blocks
```

For more information, see the [groupadd\(1M\)](#) and [useradd\(1M\)](#) man pages.

▼ How to Create the Home Directory for a User Without Creating a ZFS Dataset

1. Become an administrator.

See “Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3*.

2. Create a local directory under the /export/home path.

```
# mkdir /export/home/local
```

3. Add a new user account and specify the base directory for the same.

```
# useradd -d /export/home/local/username -m username  
80 blocks
```

4. Assign a password to the new user account.

```
# passwd username  
New Password:  
Re-enter new Password:  
passwd: password successfully changed for username
```

Note - Make sure you have the User Security rights profile assigned in order to assign passwords.

5. The home directory of the user account is created in the /export/home directory.

```
# cat /etc/passwd  
root:x:0:0:Super-User:/root:/usr/bin/bash  
daemon:x:1:1:/:/bin/sh  
bin:x:2:2:/:/bin/sh  
sys:x:3:3:/:/bin/sh  
adm:x:4:4:Admin:/var/adm:/bin/sh  
dladm:x:15:65:DataLink Admin:/:  
netadm:x:16:65:Network Admin:/:  
netcfg:x:17:65:Network Configuration Admin:/:
```

```
sshd:x:22:22:sshd privsep:/var/empty:/bin/false
smmsp:x:25:25:SendMail Message Submission Program:/:
username:x:167:10:./export/home/local/username:/usr/bin/bash
```

Sharing ZFS File Systems

You can share a ZFS file system by setting the `share.nfs` property or the `share.smb` property. Or, you can create a file system share by using the `zfs share` command. By default, all file systems are unshared.

By default, the `pool/export/home` dataset is already mounted on `/export/home`. The `useradd` command automatically creates per-user datasets as children of this dataset. As an administrator, you can choose to create a new pool for user home directories.

For more information about sharing and unsharing file systems, see [“Autofs Administration” in *Managing Network File Systems in Oracle Solaris 11.3*](#).

▼ How to Share Home Directories That Are Created as ZFS File Systems

1. **Become an administrator or log in as a user who is assigned the User Management rights profile.**

See [“Using Your Assigned Administrative Rights” in *Securing Users and Processes in Oracle Solaris 11.3*](#).

2. **Create a separate pool for the user home directories.**

```
# zpool create pool mirror disk 1 disk 2 mirror disk 3 disk 4
```

For example:

```
# zpool create users mirror c1t1d0 c1t2d0 mirror c2t1d0 c2t2d0
```

3. **Create a container for the home directories.**

```
# zfs create filesystem
```

For example:

```
# zfs create users/home
```

4. Set the share properties for the home directory.

For example, to create an NFS share and set the `share.nfs` property for `users/home`, you would type:

```
# zfs set share.nfs=on users/home
```

When using this new syntax, each file system contains an "auto share" that is created as soon as the `share.nfs` property (or the `share.smb` property) is set to on for that file system. The previous command shares a file system named `users/home` and all of its children.

5. Confirm that the descendent file system shares are also published.

For example:

```
# zfs get -r share.nfs users/home
```

The `-r` option displays all of the descendent file systems.

Manually Mounting a User's Home Directory

Typically, the user accounts that are created as ZFS file systems do not need to be manually mounted. With ZFS, file systems are automounted when they are created and then mounted at boot time from the SMF local file system service.

When creating user accounts, make sure home directories are set up as they are in the name service, at `/home/username`. Then, make sure that the `auto_home` map indicates the NFS path to the user's home directory. For task-related information, see [“Autofs Administration” in *Managing Network File Systems in Oracle Solaris 11.3*](#).

If you need to manually mount a user's home directory, use the `zfs mount` command. For example:

```
# zfs mount users/home/jdoe
```

Note - Make sure that the user's home directory is shared. For more information, see [“How to Share Home Directories That Are Created as ZFS File Systems” on page 50](#).

Managing User Accounts by Using the User Manager GUI

This chapter provides overview and task-related information for setting up and managing users by using the Oracle Solaris User Manager Graphical User Interface (GUI). You can use the User Manager GUI to perform most of the tasks that can be performed by using the equivalent commands (such as `useradd`, `usermod`, and `userdel`). However, note that you cannot use those commands to modify accounts that you did not create. For more information about the User Manager GUI, refer to the online help in the GUI.

This chapter covers the following topics:

- [“Introducing the User Manager GUI” on page 53](#)
- [“Adding, Modifying, and Deleting Users and Roles by Using the User Manager GUI” on page 57](#)
- [“Assigning Advanced Attributes With the User Manager GUI” on page 61](#)

For overview information about managing user accounts, see [Chapter 1, “About User Accounts and User Environments”](#).

For information about managing user accounts by using the CLI, see [Chapter 2, “Managing User Accounts by Using the Command-Line Interface”](#).

Introducing the User Manager GUI

This section provides the following information:

- [“How to Start the User Manager GUI” on page 54](#)
- [“Organization of the User Manager Dialog Box” on page 54](#)
- [“Filtering the Information Displayed in the GUI” on page 55](#)
- [“Assuming a Role” on page 57](#)

The User Manager GUI is based on the Visual Panels framework and is provided as a Visual Panels interface. User authentication and role assumption is provided by the Visual Panels

framework itself and is available to all of the panels, including the User Manager GUI. The User Manager GUI replaces the Solaris Management Console's legacy User and Roles tool. Although not identical to the Solaris Management Console, the GUI has some of the same functionality.

Note - The Solaris Management Console is *not* supported in this release.

The User Manager GUI presents a simple, clear interface that is easy to use. To minimize the possibility of errors, the GUI presents only those choices that are valid based on the authorizations and rights profiles of the authenticated user or role.

The User Manager GUI is delivered by the `pkg:/system/management/visual-panels/panel-usermgr` IPS package.

▼ How to Start the User Manager GUI

1. **Become an administrator or log in as a user who is assigned the User Management rights profile.**

See [“Using Your Assigned Administrative Rights”](#) in *Securing Users and Processes in Oracle Solaris 11.3*.

2. **Start the User Manager GUI.**

- **Desktop: Choose System → Administration → User Manager.**

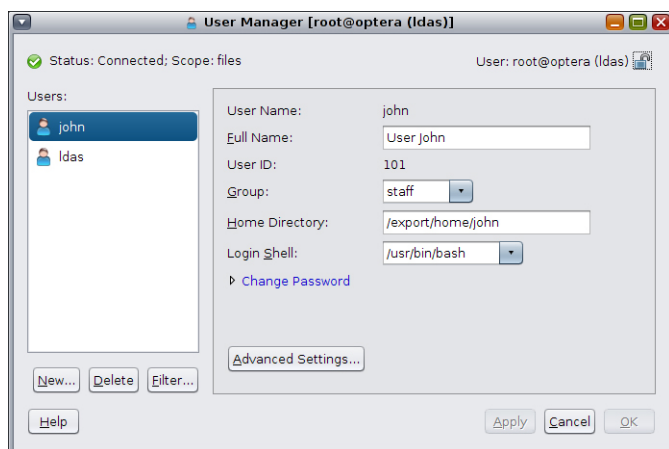
- **Command line:**

```
# vp usermgr &
```

Organization of the User Manager Dialog Box

When you start the User Manager GUI, the main User Manager dialog box is displayed. The User Manager dialog box is used to administer users and roles. The Status field at the top left of the dialog box displays the status of services that are currently running on the local system. At the top right of the dialog box is a User field that displays the credential that is currently being used by the User Manager GUI. To find out how to change credentials, see [“Assuming a Role”](#) on page 57.

The following figure shows the main User Manager dialog box with the user, john, selected.



The User Manager dialog box includes the following components:

- Users and Roles list – A list of users from which you can select to administer
- Basic Settings – The basic settings for a user, such as user name and full name

To view or modify information for an existing user, select the user from the list of users that is displayed. After you select a user, that user's information is displayed on the right side of the dialog box.

The following actions are available to you from within the User Manager dialog box:

- Create a new user or role – See [“How to Add a User or Role With the User Manager GUI” on page 58.](#)
- Delete an existing user or role – See [“How to Delete a User or Role With the User Manager GUI” on page 60](#)
- Filter a user's information – See [“Filtering the Information Displayed in the GUI” on page 55.](#)
- Administer advanced settings for an existing user – See [“How to Modify a User or Role With the User Manager GUI” on page 60.](#)

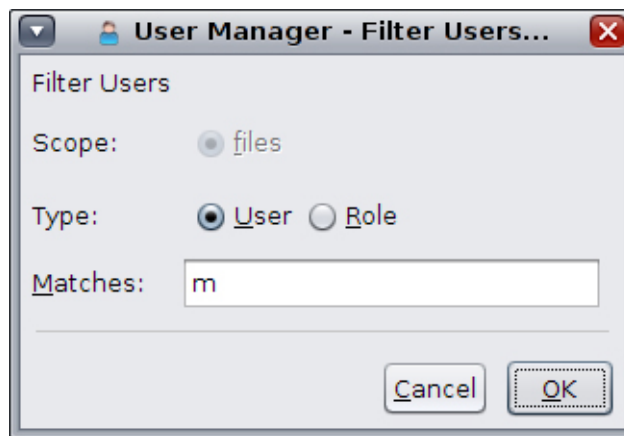
Filtering the Information Displayed in the GUI

You can filter the information that is displayed in the User Manager GUI. You can choose to display only users, or you can choose to display only roles. And, you can limit the scope to display either file information or LDAP information if the system is configured as an LDAP client.

The default settings are User and Files. These settings display users instead of roles, and display users' file information instead of displaying the LDAP specifications for a user.

In the filter dialog box, you also have the option to search for user names or role names that match any search criteria that you enter.

In the following dialog box, the system is not configured for LDAP, so that scope option is not available. The type is filtered to display users instead of roles. And, a search is specified to find user names that start with "m".



▼ How to Set Filters for Default Name Service Type and Scope

1. **Start the User Manager GUI.**
See [“How to Start the User Manager GUI”](#) on page 54.
2. **Click the Filter button.**
3. **Set the Scope option to either file or, if available, to LDAP.**
4. **Set the Type option to either User or Role.**
5. **Optionally, to filter for specific role names or user names, enter text that you want to search by.**
6. **Click OK.**

Assuming a Role

If you have a User Management rights profile, you can create new users and new roles as long as the advanced attributes of the user or role to be created are a subset of those of your own authority. If you do not have sufficient authorization but you have an administrative role with sufficient authorizations, you can assume that role to perform the necessary administration by clicking the Lock button in the main User Manager dialog box as described in this procedure.

▼ How to Assume a Role

1. Start the User Manager GUI.

See [“How to Start the User Manager GUI” on page 54.](#)

2. In the main User Manager dialog box, click the Lock icon next to your user name in the upper right section of the dialog box.

A submenu displays that contains the following options:

- Change Role
- Change User
- Administer New Host
- Clear History

3. Select the Change Role option.

An authentication dialog box is displayed. The authentication dialog box contains a drop-down menu that lists the roles that are available for you.

4. Select the appropriate role.

5. Click Log In to assume that role.

After assuming the role, you can perform the required administrative tasks.

Adding, Modifying, and Deleting Users and Roles by Using the User Manager GUI

Adding, modifying, and deleting users by using the User Manager GUI is equivalent to using the `useradd`, `usermod`, and `userdel` commands, respectively. For more information about

adding users from the command line, see [Chapter 2, “Managing User Accounts by Using the Command-Line Interface”](#).

This section describes the following information:

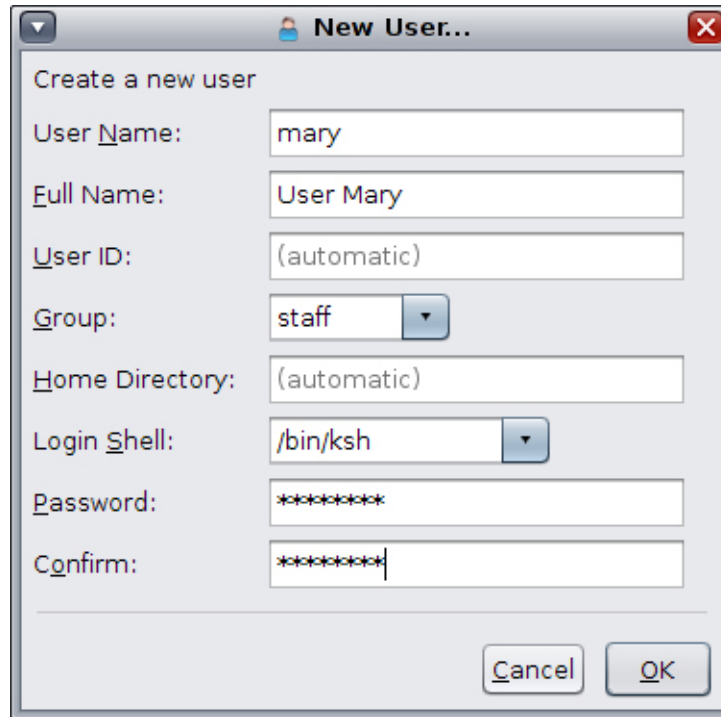
- [“How to Add a User or Role With the User Manager GUI” on page 58](#)
- [“How to Modify a User or Role With the User Manager GUI” on page 60](#)
- [“How to Delete a User or Role With the User Manager GUI” on page 60](#)

▼ **How to Add a User or Role With the User Manager GUI**

This procedure adds a new user or role within the scope of the filter that is currently being used by the GUI.

1. **Start the User Manager GUI.**
See [“How to Start the User Manager GUI” on page 54](#).
2. **Click the New button in the main User Manager dialog box.**

The New User dialog box is displayed.



The screenshot shows a dialog box titled "New User...". It contains the following fields and values:

- User Name: mary
- Full Name: User Mary
- User ID: (automatic)
- Group: staff
- Home Directory: (automatic)
- Login Shell: /bin/ksh
- Password: masked with asterisks
- Confirm: masked with asterisks

Buttons: Cancel, OK

3. Provide the user account information.

- User Name
- Full Name
- User ID – This information is optional. If you don't provide any information, the system automatically assigns a default value.
- Group – Available choices for the Group field vary depending on your system's configuration.
- Home Directory – This information is optional. If you don't provide any information, the system automatically assigns a default value.
If you want the home directory of the user to be automounted, precede the path name with a host name or a local host. For example, localhost:/export/home/test1.
- Login Shell – Choices for the Login Shell field vary, depending on your system's configuration.

- Password – Assign a temporary password to the user.
 - Confirm – Confirm the temporary password that you assigned to the user.
4. **Click OK.**

The user or role is added to the list of users that is displayed in the main User Manager dialog box, click OK.

▼ How to Modify a User or Role With the User Manager GUI

1. **Start the User Manager GUI.**

See [“How to Start the User Manager GUI” on page 54.](#)
2. **Select the user or role that you want to modify from the list that is displayed.**

After selecting the user, the right side of the dialog box is populated with information about the current user.
3. **Modify any or all of the information for the current user or role.**

Note - If a field is modified, an indicator is displayed next to the field.

4. **Click Apply to save the changes.**
5. **(Optional) Click the Advanced Settings button to modify additional security attributes for the user or role.**

See [“Assigning Advanced Attributes With the User Manager GUI” on page 61.](#)
6. **Click OK to save the changes and close the dialog box.**

▼ How to Delete a User or Role With the User Manager GUI

This procedure deletes a user or role within the scope of the filter that is currently being used by the User Manager GUI.

1. **Select the user or role in the main User Manager dialog box.**
2. **Click the Delete button.**
3. **Click OK in the confirmation dialog box.**

Assigning Advanced Attributes With the User Manager GUI

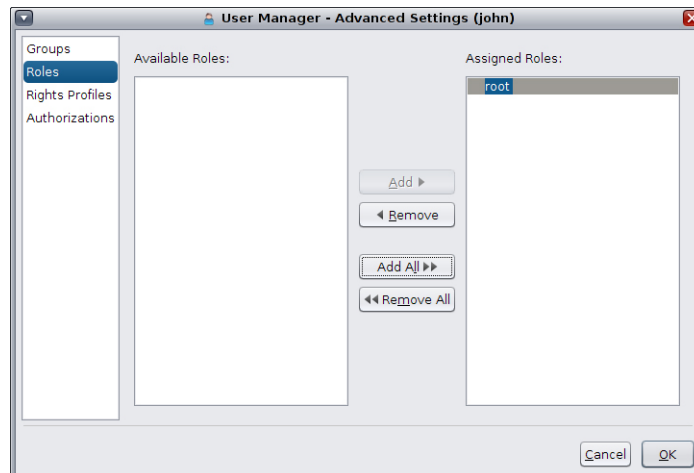
This section describes the following information:

- [“Assigning Groups With the User Manager GUI” on page 62](#)
- [“Assigning Roles With the User Manager GUI” on page 63](#)
- [“Assigning Rights Profiles With the User Manager GUI” on page 64](#)
- [“Assigning Authorizations With the User Manager GUI” on page 65](#)

Use the Advanced Settings dialog box of the User Manager GUI to assign additional security attributes to a user, for example, rights profiles, roles, and authorizations.

For an overview, see [Chapter 1, “About Using Rights to Control Users and Processes” in *Securing Users and Processes in Oracle Solaris 11.3*](#).

The following figure shows the Advanced Settings dialog box, with the Roles security attribute of the user john selected. The selected user's name appears in parentheses in the title bar of the dialog box.



The Advanced Settings dialog box enables you to assign the following security attributes:

- Groups
- Roles
- Rights Profiles
- Authorizations

Assigning Groups With the User Manager GUI

Groups are assigned through the Advanced Settings of the User Manager GUI.

▼ How to Assign Groups

1. Start the User Manager GUI.

See [“How to Start the User Manager GUI” on page 54.](#)

2. Select a user in the main User Manager dialog box, then click the Advanced Settings button.

The Advanced Settings dialog box is displayed.

3. Click the Groups attribute on the left side of the dialog box.

A list of the available groups and a list of the groups that the current user belongs to are displayed.

- **To assign a group (or multiple groups) to a user, select the group (or groups) from the Available Groups list, then click Add.**

The added group is displayed in the Assigned Groups list.

- **To remove a group from the Assigned Groups list, select the group (or groups) from the list, then click Remove.**

- **To add or remove all of the groups for the current user, click the Add All or Remove All button.**

4. Click OK to save the settings.

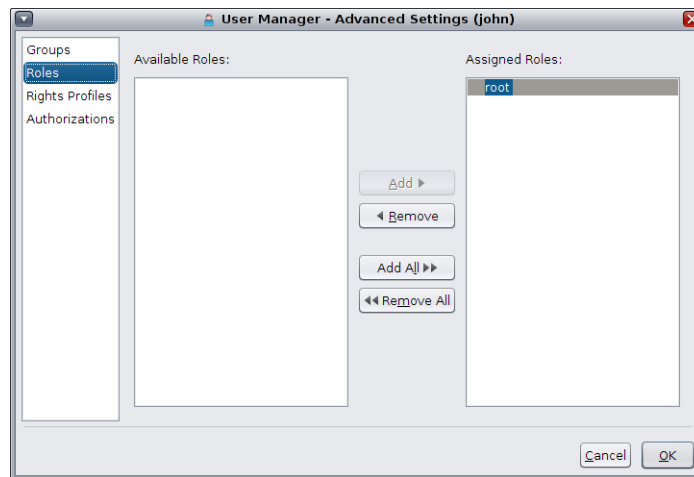
The changes are not applied until you click Apply or OK in the main User Manager dialog box.

Assigning Roles With the User Manager GUI

Roles are assigned through the Advanced Settings of the User Manager GUI.

Note - The Roles attribute is available only for a user, not for a role, because roles can only be assigned to users.

The following figure shows the Advanced Settings dialog box with the Roles security attribute of the user john selected.



▼ How to Assign Roles With the User Manager GUI

1. **Start the User Manager GUI.**
See [“How to Start the User Manager GUI”](#) on page 54.
2. **Select a user in the main User Manager dialog box, then click the Advanced Settings button.**
The Advanced Settings dialog box is displayed.
3. **Click the Roles attribute on the left side of the dialog box.**
A list of the available roles and a list of the roles that are assigned to the current user are displayed.

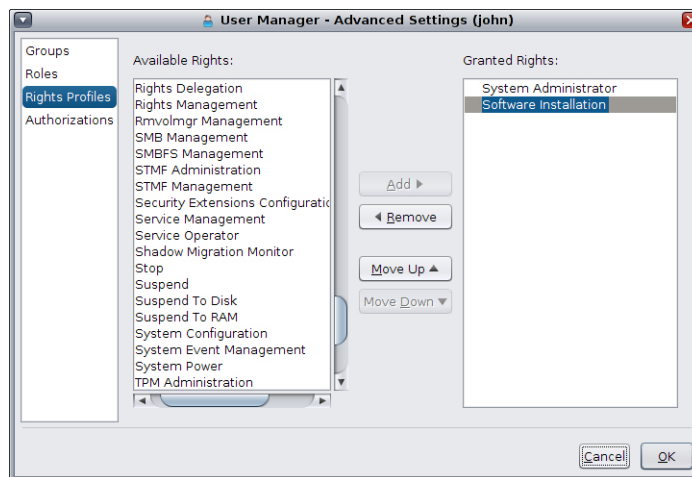
- **To assign a role (or multiple roles) to a user, select the role (or roles) from the Available Roles list, then click Add.**
The added role is displayed in the Assigned Roles list.
 - **To remove a role from the Assigned Roles list, select the role (or roles) from the list, then click Remove.**
 - **To add or remove all of the roles for the current user, click the Add All or Remove All button.**
4. **Click OK to save the settings.**

The changes are not applied until you click Apply or OK in the main User Manager dialog box.

Assigning Rights Profiles With the User Manager GUI

Rights profiles are assigned through the Advanced Settings User Manager GUI.

The following figure shows the Advanced Settings dialog box with the Rights Profile security attribute of the user john selected.



Note - The assignment of rights profiles has an order precedence. Use the Move Up and Move Down buttons to change the order of the rights profiles that are granted to the current user.

▼ How to Administer Rights Profiles With the User Manager GUI

1. Start the User Manager GUI.

See [“How to Start the User Manager GUI” on page 54](#).

2. Select a user in the main User Manager dialog box, then click the Advanced Settings button.

The Advanced Settings dialog box is displayed.

3. Click the Rights Profile attribute on the left side of the dialog box.

A list of the available rights profiles and a list of the rights profiles that are granted to the current user are displayed.

- **To assign a rights profile (or multiple rights profiles) to a user, select the rights profile (or rights profiles) from the Available Rights Profiles list, then click Add.**

The added rights profile is displayed in the Granted Rights Profiles list.

- **To remove a rights profile from the Granted Rights Profiles list, select the rights profile (or rights profiles) from the list, then click Remove.**

- **To add or remove all rights profiles for the current user, click the Add All or Remove All button.**

4. Click OK to save the settings.

The changes are not applied until you click Apply or OK in the main User Manager dialog box.

Assigning Authorizations With the User Manager GUI

A user generally is granted authorizations indirectly through a rights profile. Authorization settings can be used to grant a specific authorization to a user or role. Some authorizations might have additional attributes, such as an object name. For example, when an administrator

creates the group `games`, the administrator is granted an implicit authorization: `solaris.group.manage/games`. The object names are then displayed in the Granted Authorizations list.

▼ How to Assign Authorizations With the User Manager GUI

1. Start the User Manager GUI.

See [“How to Start the User Manager GUI” on page 54](#).

2. Select a user in the main User Manager dialog box, then click the Advanced Settings button.

The Advanced Settings dialog box is displayed.

3. Click the Authorization attribute on the left side of the dialog box.

A list of the available authorizations and a list of the authorizations that are granted to the current user are displayed.

- **To assign an authorization (or multiple authorizations) to a user, select the authorization (or authorizations) from the Available Authorizations list, then click Add.**

The added authorization is displayed in the Granted Authorizations list.

- **To remove an authorization from the Granted Authorizations list, select the authorization (or authorizations) from the list, then click Remove.**

- **To add or remove all authorizations for the current user, click the Add All or Remove All button.**

4. Click OK to save the settings.

The changes are not applied until you click Apply or OK in the main User Manager dialog box.

Index

A

- adding
 - groups
 - through the CLI, 48
 - roles
 - through the CLI, 45
 - with the User Manager GUI, 57, 60
 - user initialization files, 27
 - users
 - through the CLI, 45
 - with the User Manager GUI, 57, 60
- administering
 - accounts, 44
 - groups, 48
 - users, 45, 47
- advanced settings
 - administering with the User Manager GUI, 61
- aging user passwords, 20
- aliases
 - not using user login names for, 13
- assigning
 - with the User Manager GUI
 - authorizations, 65
 - groups, 62
 - rights profiles, 64
 - roles, 63
- authorizations
 - assigning with the User Manager GUI, 65
- automounting user home directories, 18

B

- bash shells
 - customizing, 33

- displaying
 - environment variables in, 30
 - user command history, 30
- bin group, 14

C

- C shell
 - user initialization files and, 36
- CDPATH environment variable, 32
- changing
 - account defaults, 44
- changing credentials with the User Manager GUI, 57
- controlling file and directory access, 35
- .cshrc file
 - customizing, 36
- customizing
 - bash shell, 33

D

- daemon group, 14
- defaults
 - file permissions, 35
 - name service scope and filter, 55
 - setting for users and roles, 44
- deleting
 - roles
 - with the User Manager GUI, 57
 - users
 - using the CLI, 47
 - with the User Manager GUI, 57

directories
controlling access to, 35
home, 17
changing default, 44
sharing a ZFS file system, 50
PATH environment variable and, 32, 33
skeleton, 27
displaying the user mask, 35

E

encryption, 20
environment variables, 30
See also variables
displaying in bash shell, 30
displaying in ksh93 shell, 30
establishing persistent, 31
LOGNAME, 32
PATH, 32
SHELL, 32
TZ, 33
/etc files
user account information and, 18, 18
/etc/passwd file, 20, 20
description, 20
user ID number assignment and, 14
/etc/shadow file
description, 20
/export/home file system, 17

F

file permissions
default, 35
files
controlling access to, 35

G

group file
description, 20

fields in, 23
group ID numbers, 14, 14, 15, 16
groupadd command, 26, 48
groupdel command, 26
groupmod command, 26
groups
adding, 48
assigning with the User Manager GUI, 62
changing primary, 15
default, 16
description, 15
displaying groups a user belongs to, 15
guidelines for managing, 15, 16
ID numbers, 14, 15, 16
names, 15
naming services and, 16
primary, 15, 16
secondary, 15, 16
storage of information for, 20, 23
UNIX, 15
groups command, 15

H

home directories *See* user home directories
HOME environment variable, 32
/home file system
user home directories and, 17

I

ID numbers
group, 14, 15, 16
user, 14, 14
initialization files
system, 18

K

ksh93 shells
displaying

- environment variables in, 30
- user command history, 30
- user initialization files and, 27

L

- LANG environment variable, 32, 34
- LC environment variables, 34
- LDAP
 - filter users by their name service scope and type using User Manager GUI, 55
- locale environment variable, 32
- login
 - options during shutdown, 11
 - .login file
 - customizing, 36
 - login names (user)
 - description, 13
- LOGNAME environment variable, 32

M

- mail aliases
 - not using user login names for, 13
- MAIL environment variable, 32
- MANPATH environment variable, 32, 33
- maximums
 - secondary groups users can belong to, 15
 - user ID number, 14
 - user login name length, 19
- minimums
 - user login name length, 19
- mounting
 - user home directories, 18, 51

N

- name service scope and type
 - User Manager GUI, 55
- names
 - group, 15

- user login, 13
- naming services
 - filtering users by scope and type using User Manager GUI, 55
 - groups and, 16
 - user accounts and, 18, 18, 20
- newgrp command, 15
- NIS
 - user accounts and, 18, 20
- NIS and user accounts, 18
- noaccess user/group, 14
- nobody user/group, 14

P

- passwd command
 - assigning user password with, 45
 - unlocking user, 46
- passwd file
 - fields in, 20, 22
 - user ID number assignment and, 14
- passwords (user)
 - aging, 20
 - assigning to users, 45
 - encryption, 20
 - precautions, 17
- PATH environment variable, 32, 33
- permissions
 - file defaults, 35
- primary groups, 15, 16
- .profile file
 - customizing, 36
- PS1 environment variable, 32
- pseudo user logins, 14
- pseudo-ttys, 14

R

- removing
 - user's home directory, 47
 - with the User Manager GUI
 - authorizations, 65

- groups, 62
- rights profiles, 64
- roles, 63

rights profiles

- assigning with the User Manager GUI, 64

roleadd command, 26

- setting account defaults, 44

roledel command, 26

rolemod command, 26

roles

- assigning with the User Manager GUI, 63

S

secondary groups, 15, 16

security

- recent changes, 12
- user ID number reuse and, 14

settings

- administering with the User Manager GUI, 61

shadow file

- description, 20
- fields in, 23

SHELL environment variable, 32

shells

- displaying environment variables in, 30
- user initialization files and, 36

site initialization files, 27

skeleton directories (/etc/skel), 27

staff group, 16

starting the User Manager GUI, 54

stty command, 34

system accounts, 14

system initialization files, 18

T

TERM environment variable, 33

TERMINFO environment variable, 32

time zone environment variable, 33

ttys (pseudo), 14

ttytype pseudo user logins, 14

TZ environment variable, 33

U

UIDs

- assigning, 14
- definition, 14
- large, 14

umask command, 35

UNIX groups, 15

unlocking

- users

- using the CLI, 46

user accounts, 12

- description, 12, 13
- gathering information for, 42
- guidelines for, 18
- ID numbers, 14, 14
- login names, 13
- naming services and, 18, 18, 20
- storage of information for, 18, 18

user home directories

- automounting, 18
- customized initialization files in, 27
- description, 17
- mounting, 51
- nonlocal reference to (\$HOME), 18, 28
- removing, 47, 47

user ID numbers, 14, 14

user initialization files

- customizing, 26, 36
- adding customized files, 27
- avoiding local system references, 28
- overview, 27
- shell variables, 33
- site initialization files, 27
- user mask setting, 35

description, 18, 18

shells and, 36

user login names

- description, 13

user logins (pseudo), 14

User Manager GUI

- adding roles with, 57
- adding users with, 57
- as Visual Panels interface, 53
- assigning advanced settings with, 61
- assigning authorizations with, 65
- assigning groups with, 62
- assigning rights profiles with, 64
- assigning roles with, 63
- changing credentials with, 57
- deleting users or roles with, 60
- displaying default name service scope and type with, 55
- how to start, 54
- main panel in, 54
- modifying users or roles with, 60
- panel components in, 54
- user mask, 35
- user packages
 - identifying users, 43
- useradd command, 25
 - adding user, 45
 - setting account defaults, 44
- userdel command, 26
 - deleting user, 47
- usermod command, 25
- users
 - adding, 45, 47
 - assigning authorizations for, 65
 - assigning rights profiles for, 64
 - assigning roles to, 63
 - assigning to groups, 62
 - managing in Ops Center, 37
 - removing, 60
 - removing home directories, 47
 - setting account defaults, 44
 - unlocking, 46
- uucp group, 14

V

- variables, 30
 - See also* environment variables
 - in Oracle Solaris, 32

- shell (local) variables, 30
- types of, 30
- Visual Panels
 - User Manager GUI based on, 53

Z

- ZFS file systems
 - sharing, 50
 - user accounts as, 41
 - user home directory as a child ZFS dataset, 42

