10 Managing Users with YaST

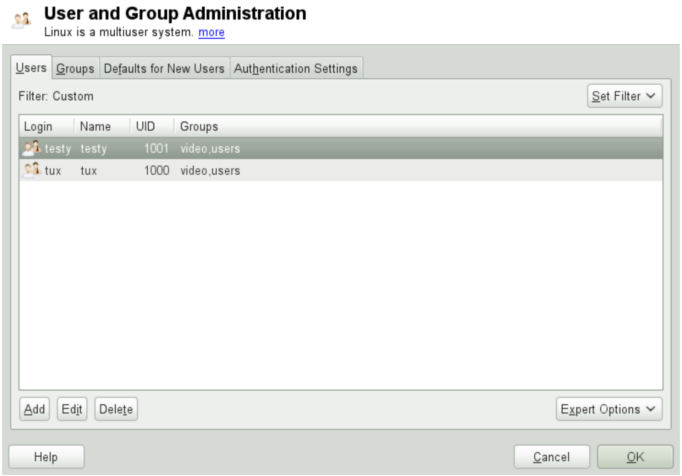
During installation, you chose a method for user authentication. This method is either local (via `/etc/passwd`) or, if a network connection is established, via NIS, LDAP, Kerberos or Samba (see Section “Create New User” (Chapter 1, *Installation with YaST*, ↑Reference)). You can create or modify user accounts and change the authentication method with YaST at any time.

Every user is assigned a system-wide user ID (UID). Apart from the users which can log in to your machine, there are also a number of *system users* for internal use only. Each user is assigned to one or more groups. Similar to *system users*, there are also *system groups* for internal use.

10.1 User and Group Administration Dialog

To administer users or groups, start YaST and click *Security and Users* > *User and Group Management*. Alternatively, start the *User and Group Administration* dialog directly by running **`yast2 users &`** from a command line.

Figure 10.1: *YaST User and Group Administration*



User and Group Administration

Linux is a multiuser system. more

Filter: Custom

Login	Name	UID	Groups
testy	testy	1001	video,users
tux	tux	1000	video,users

Depending on the set of users you choose to view and modify with, the dialog (local users, network users, system users), the main window shows several tabs. These allow you to execute the following tasks:

Managing User Accounts
: From the *Users* tab create, modify, delete or temporarily disable user accounts as described in Section 10.2, "Managing User Accounts" (page 128). Learn about advanced options like enforcing password policies, using encrypted home directories, using fingerprint authentication, or managing disk quotas in Section 10.3, "Additional Options for User Accounts" (page 130).

Changing Default Settings
: Local users accounts are created according to the settings defined on the *Defaults for New Users* tab. Learn how to change the default group assignment, or the default path and access permissions for home directories in Section 10.4, "Changing Default Settings for Local Users" (page 135).

Assigning Users to Groups
: Learn how to change the group assignment for individual users in Section 10.5, "Assigning Users to Groups" (page 136).

Managing Groups
: From the *Groups* tab, you can add, modify or delete existing groups. Refer to Section 10.6, "Managing Groups" (page 137) for information on how to do this.

Changing the User Authentication Method
: When your machine is connected to a network that provides user authentication methods like NIS or LDAP, you can choose between several authentication methods on the *Authentication Settings* tab. For more information, refer to Section 10.7, "Changing the User Authentication Method" (page 138).

For user and group management, the dialog provides similar functionality. You can easily switch between the user and group administration view by choosing the appropriate tab at the top of the dialog.

Filter options allow you to define the set of users or groups you want to modify: On the *Users* or *Group* tab, click *Set Filter* to view and edit users or groups according to certain categories, such as *Local Users* or *LDAP Users*, for instance (if you are part of a network which uses LDAP). With *Set Filter* > *Customize Filter* you can also set up and use a custom filter.

Depending on the filter you choose, not all of the following options and functions will be available from the dialog.

10.2 Managing User Accounts

YaST offers to create, modify, delete or temporarily disable user accounts. Do not modify user accounts unless you are an experienced user or administrator.

NOTE: Changing User IDs of Existing Users

File ownership is bound to the user ID, not to the user name. After a user ID change, the files in the user's home directory are automatically adjusted to reflect this change. However, after an ID change, the user no longer owns the files he created elsewhere in the file system unless the file ownership for those files are manually modified.

In the following, learn how to set up default user accounts. For some further options, such as auto login, login without password, setting up encrypted home directories or managing quotas for users and groups, refer to Section 10.3, "Additional Options for User Accounts" (page 130).

Procedure 10.1: *Adding or Modifying User Accounts*

1 Open the YaST *User and Group Administration* dialog and click the *Users* tab.

2 With *Set Filter* define the set of users you want to manage. The dialog shows a list of users in the system and the groups the users belong to.

3 To modify options for an existing user, select an entry and click *Edit*.

  To create a new user account, click *Add*.

4 Enter the appropriate user data on the first tab, such as *Username* (which is used for login) and *Password*. This data is sufficient to create a new user. If you click *OK* now, the system will automatically assign a user ID and set all other values according to the default.

5 Activate *Receive System Mail* if you want any kind of system notifications to be delivered to this user's mailbox. This creates a mail alias for `root` and the user can read the system mail without having to first log in as `root`.

6 If you want to adjust further details such as the user ID or the path to the user's home directory, do so on the *Details* tab.

  If you need to relocate the home directory of an existing user, enter the path to the new home directory there and move the contents of the current home directory with *Move to New Location*. Otherwise, a new home directory is created without any of the existing data.

7 To force users to regularly change their password or set other password options, switch to *Password Settings* and adjust the options. For more details, refer to Section 10.3.2, "Enforcing Password Policies" (page 131).

8 If all options are set according to your wishes, click *OK*.

9 Click *Expert Options* > *Write Changes Now* to save all changes without exiting the *User and Group Administration* dialog. Click *OK* to close the administration

dialog and to save the changes. A newly added user can now log in to the system using the login name and password you created.

TIP: Matching User IDs

For a new (local) user on a laptop which also needs to integrate into a network environment where this user already has a user ID, it is useful to match the (local) user ID to the ID in the network. This ensures that the file ownership of the files the user creates “offline” is the same as if he had created them directly on the network.

Procedure 10.2: *Disabling or Deleting User Accounts*

1 Open the YaST *User and Group Administration* dialog and click the *Users* tab.

2 To temporarily disable a user account without deleting it, select the user from the list and click *Edit*. Activate *Disable User Login*. The user cannot log into your machine until you enable the account again.

3 To delete a user account, select the user from the list and click *Delete*. Choose if you also want to delete the user's home directory or if you want to retain the data.

10.3 Additional Options for User Accounts

In addition to the settings for a default user account, openSUSE® offers further options, such as options to enforce password policies, use encrypted home directories or define disk quotas for users and groups.

10.3.1 Automatic Login and Passwordless Login

If you use the KDE or GNOME desktop environment you can configure *Auto Login* for a certain user as well as *Passwordless Login* for all users. Auto login causes a user to become automatically logged in to the desktop environment on boot. This functionality can only be activated for one user at a time. Login without password allows all users to log in to the system after they have entered their username in the login manager.

WARNING: Security Risk

Enabling *Auto Login* or *Passwordless Login* on a machine that can be accessed by more than one person is a security risk. Without the need to authenticate, any user can gain access to your system and your data. If your system contains confidential data, do not use this functionality.

If you want to activate auto login or login without password, access these functions in the YaST *User and Group Administration* with *Expert Options* > *Login Settings*.

10.3.2 Enforcing Password Policies

On any system with multiple users, it is a good idea to enforce at least basic password security policies. Users should change their passwords regularly and use strong passwords that cannot easily be exploited. For local users, proceed as follows:

Procedure 10.3: *Configuring Password Settings*

1. Open the YaST *User and Group Administration* dialog and select the *Users* tab.
2. Select the user for which to change the password options and click *Edit*.
3. Switch to the *Password Settings* tab. The user's last password change is displayed on the tab.
4. To make the user change his password at next login, activate *Force Password Change*.
5. To enforce password rotation, set a *Maximum Number of Days for the Same Password* and a *Minimum Number of Days for the Same Password*.
6. To remind the user to change his password before it expires, set a number of *Days before Password Expiration to Issue Warning*.
7. To restrict the period of time the user can log in after his password has expired, change the value in *Days after Password Expires with Usable Login*.
8. You can also specify a certain expiration date for a password. Enter the *Expiration Date* in *`YYYY-MM-DD`* format.
9. For more information about the options and about the default values, click *Help*.
10. Apply your changes with *OK*.

10.3.3 Managing Encrypted Home Directories

To protect data in home directories against theft and hard disk removal, you can create encrypted home directories for users. These are encrypted with LUKS (Linux Unified Key Setup), which results in an image and an image key being generated for the user. The image key is protected with the user's login password. When the user logs into the system, the encrypted home directory is mounted and the contents are made available to the user.

NOTE: Fingerprint Reader Devices and Encrypted Home Directories

If you want to use a fingerprint reader device, you must not use encrypted home directories. Otherwise logging in will fail, because decrypting during login is not possible in combination with an active fingerprint reader device.

With YaST, you can create encrypted home directories for new or existing users. To encrypt or modify encrypted home directories of already existing users, you need to know the user's current login password. By default, all existing user data is copied to the new encrypted home directory, but it is not deleted from the unencrypted directory.

WARNING: Security Restrictions

Encrypting a user's home directory does not provide strong security from other users. If strong security is required, the system should not be physically shared.

Find background information about encrypted home directories and which actions to take for stronger security in Section “Using Encrypted Home Directories” (Chapter 10, *Encrypting Partitions and Files*, ↑Security Guide).

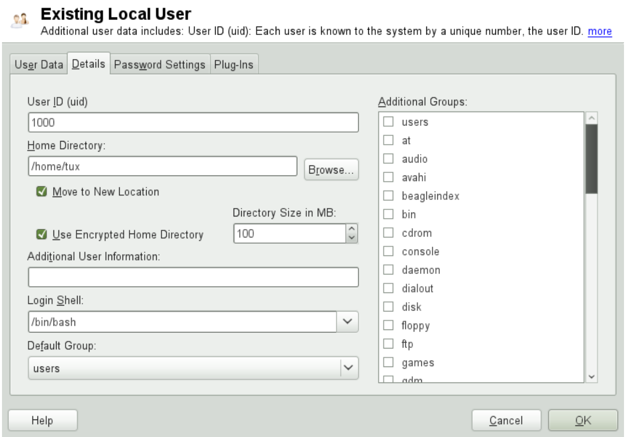
Procedure 10.4: *Creating Encrypted Home Directories*

1 Open the YaST *User and Group Management* dialog and click the *Users* tab.

2 To encrypt the home directory of an existing user, select the user and click *Edit*.

Otherwise, click *Add* to create a new user account and enter the appropriate user data on the first tab.

3 In the *Details* tab, activate *Use Encrypted Home Directory*. With *Directory Size in MB*, specify the size of the encrypted image file to be created for this user.



Existing Local User

Additional user data includes: User ID (uid): Each user is known to the system by a unique number, the user ID. more

User ID (uid): 1000

Home Directory: /home/tux

☑ Move to New Location

Directory Size in MB: 100

☑ Use Encrypted Home Directory

Additional User Information:

Login Shell: /bin/bash

Default Group: users

Additional Groups:

□ users
□ at
□ audio
□ avahi
□ beagleindex
□ bin
□ cdrom
□ console
□ daemon
□ dialout
□ disk
□ floppy
□ ftp
□ games
□ gdm

4 Apply your settings with *OK*.

5. Enter the user's current login password to proceed if YaST prompts for it.

6. Click *Expert Options* > *Write Changes Now* to save all changes without exiting the administration dialog. Click *OK* to close the administration dialog and save the changes.

Procedure 10.5: *Modifying or Disabling Encrypted Home Directories*

Of course, you can also disable the encryption of a home directory or change the size of the image file at any time.

1. Open the YaST *User and Group Administration* dialog in the *Users* view.

2. Select a user from the list and click *Edit*.

3. If you want to disable the encryption, switch to the *Details* tab and disable *Use Encrypted Home Directory*.

   If you need to enlarge or reduce the size of the encrypted image file for this user, change the *Directory Size in MB*.

4. Apply your settings with *OK*.

5. Enter the user's current login password to proceed if YaST prompts for it.

6. Click *Expert Options* > *Write Changes Now* to save all changes without exiting the *User and Group Administration* dialog. Click *OK* to close the administration dialog and to save the changes.

10.3.4 Using Fingerprint Authentication

If your system includes a fingerprint reader you can use biometric authentication in addition to standard authentication via login and password. After registering their fingerprint, users can log into the system either by swiping a finger on the fingerprint reader or by typing in a password.

Fingerprints can be registered with YaST. Find detailed information about configuration and use of fingerprint authentication in Chapter 7, *Using the Fingerprint Reader* (↑Security Guide). For a list of supported devices, refer to `http://www.freedesktop.org/wiki/Software/fprint/libfprint`.

10.3.5 Managing Quotas

To prevent system capacities from being exhausted without notification, system administrators can set up quotas for users or groups. Quotas can be defined for one or more file systems and restrict the amount of disk space that can be used and the number of inodes (index nodes) that can be created there. Inodes are data structures on a file system that store basic information about a regular file, directory, or other file system object. They store all attributes of a file system object (like user and group ownership, read, write, or execute permissions), except file name and contents.

openSUSE allows usage of `soft` and `hard` quotas. Soft quotas usually define a warning level at which users are informed that they are nearing their limit, whereas hard quotas define the limit at which write requests are denied. Additionally, grace intervals can be defined that allow users or groups to temporarily violate their quotas by certain amounts.

Procedure 10.6: *Enabling Quota Support for a Partition*

In order to configure quotas for certain users and groups, you need to enable quota support for the respective partition in the YaST Expert Partitioner first.

1 In YaST, select *System* > *Partitioner* and click *Yes* to proceed.

2 In the *Expert Partitioner*, select the partition for which to enable quotas and click *Edit*.

3 Click *Fstab Options* and activate *Enable Quota Support*. If the `quota` package is not already installed, it will be installed once you confirm the respective message with *Yes*.

4 Confirm your changes and leave the *Expert Partitioner*.

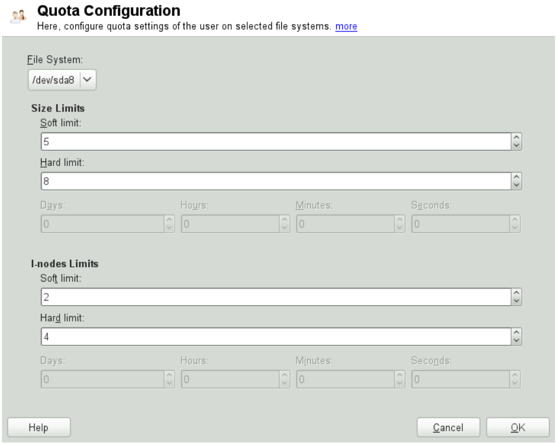
Procedure 10.7: *Setting Up Quotas for Users or Groups*

Now you can define soft or hard quotas for specific users or groups and set time periods as grace intervals.

1 In the YaST *User and Group Administration*, select the user or the group you want to set the quotas for and click *Edit*.

2 On the *Plug-Ins* tab, select the *Manage User Quota* entry and click *Launch* to open the *Quota Configuration* dialog.

3 From *File System*, select the partition to which the quota should apply.



Quota Configuration

Here, configure quota settings of the user on selected file systems. more

File System: /dev/sda8

Size Limits

Soft limit: 5

Hard limit: 8

Days: 0 Hours: 0 Minutes: 0 Seconds: 0

I-nodes Limits

Soft limit: 2

Hard limit: 4

Days: 0 Hours: 0 Minutes: 0 Seconds: 0

4 Below *Size Limits*, restrict the amount of disk space. Enter the number of 1 KB blocks the user or group may have on this partition. Specify a *Soft Limit* and a *Hard Limit* value.

5 Additionally, you can restrict the number of inodes the user or group may have on the partition. Below *Inodes Limits*, enter a *Soft Limit* and *Hard Limit*.

6 You can only define grace intervals if the user or group has already exceeded the soft limit specified for size or inodes. Otherwise, the time-related input fields are not activated. Specify the time period for which the user or group is allowed to exceed the limits set above.

7 Confirm your settings with *OK*.

8 Click *Expert Options* > *Write Changes Now* to save all changes without exiting the *User and Group Administration* dialog. Click *OK* to close the administration dialog and to save the changes.

openSUSE also ships command line tools like `repquota` or `warnquota` with which system administrators can control the disk usage or send e-mail notifications to users exceeding their quota. With **`quota_nld`**, administrators can also forward kernel messages about exceeded quotas to D-BUS. For more information, refer to the `repquota`, the `warnquota` and the **`quota_nld`** man page.

10.4 Changing Default Settings for Local Users

When creating new local users, several default settings are used by YaST. These include, for example, the primary group and the secondary groups the user belongs to, or the access permissions of the user's home directory. You can change these default settings to meet your requirements:

1. Open the YaST *User and Group Administration* dialog and select the *Defaults for New Users* tab.

2. To change the primary group the new users should automatically belong to, select another group from *Default Group*.

3. To modify the secondary groups for new users, add or change groups in *Secondary Groups*. The group names must be separated by commas.

4. If you do not want to use `/home/`*`username`* as default path for new users' home directories, modify the *Path Prefix for Home Directory*.

5. To change the default permission modes for newly created home directories, adjust the umask value in *Umask for Home Directory*. For more information about umask, refer to Chapter 9, *Access Control Lists in Linux* (↑Security Guide) and to the **`umask`** man page.

6. For information about the individual options, click *Help*.

7. Apply your changes with *OK*.

10.5 Assigning Users to Groups

Local users are assigned to several groups according to the default settings which you can access from the *User and Group Administration* dialog on the *Defaults for New Users* tab. In the following, learn how to modify an individual user's group assignment. If you need to change the default group assignments for new users, refer to Section 10.4, "Changing Default Settings for Local Users" (page 135).

Procedure 10.8: *Changing a User's Group Assignment*

1. Open the YaST *User and Group Administration* dialog and click the *Users* tab. It shows a list of users and of the groups the users belong to.

2. Click *Edit* and switch to the *Details* tab.

3. To change the primary group the user belongs to, click *Default Group* and select the group from the list.

4. To assign the user additional secondary groups, activate the corresponding check boxes in the *Additional Groups* list.

5. Click *OK* to apply your changes.

6. Click *Expert Options* > *Write Changes Now* to save all changes without exiting the *User and Group Administration* dialog. Click *OK* to close the administration dialog and save the changes.

10.6 Managing Groups

With YaST you can also easily add, modify or delete groups.

Procedure 10.9: *Creating and Modifying Groups*

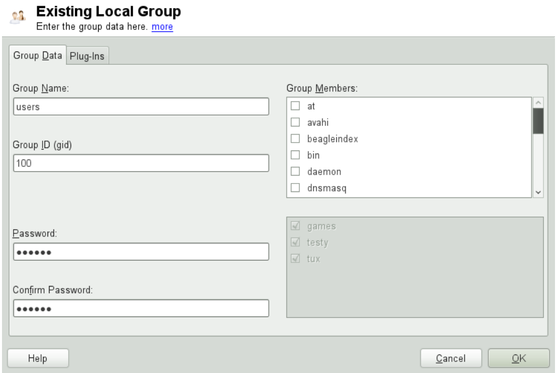
1 Open the YaST *User and Group Management* dialog and click the *Groups* tab.

2 With *Set Filter* define the set of groups you want to manage. The dialog shows a list of groups in the system.

3 To create a new group, click *Add*.

4 To modify an existing group, select the group and click *Edit.*

5 In the following dialog, enter or change the data. The list on the right shows an overview of all available users and system users which can be members of the group.



Existing Local Group

Enter the group data here. more

Group Name: users

Group ID (gid) 100

Password: ••••••

Confirm Password: ••••••

Group Members:

□ at
□ avahi
□ beagleindex
□ bin
□ daemon
□ dnsmasq

☑ games
☑ testy
☑ tux

6 To add existing users to a new group select them from the list of possible *Group Members* by checking the corresponding box. To remove them from the group uncheck the box.

7 Click *OK* to apply your changes.

8 Click *Expert Options* > *Write Changes Now* to save all changes without exiting the *User and Group Administration* dialog.

In order to delete a group, it must not contain any group members. To delete a group, select it from the list and click *Delete*. Click *Expert Options* > *Write Changes Now* to save all changes without exiting the *User and Group Administration* dialog. Click *OK* to close the administration dialog and to save the changes.

10.7 Changing the User Authentication Method

When your machine is connected to a network, you can change the authentication method you set during installation. The following options are available:

NIS
: Users are administered centrally on a NIS server for all systems in the network. For details, see Chapter 3, *Using NIS* (↑Security Guide).

LDAP
: Users are administered centrally on an LDAP server for all systems in the network. For details about LDAP, see Chapter 4, *LDAP—A Directory Service* (↑Security Guide).

  You can manage LDAP users with the YaST user module. All other LDAP settings, including the default settings for LDAP users, have to be defined with the YaST LDAP client module as described in Section "Configuring an LDAP Client with YaST" (Chapter 4, *LDAP—A Directory Service*, ↑Security Guide) .

Kerberos
: With Kerberos, a user registers once and then is trusted in the entire network for the rest of the session.

Samba
: SMB authentication is often used in mixed Linux and Windows networks. For details, see Chapter 19, *Samba* (↑Reference) and Chapter 5, *Active Directory Support* (↑Security Guide).

To change the authentication method, proceed as follows:

1. Open the *User and Group Administration* dialog in YaST.
2. Click the *Authentication Settings* tab to show an overview of the available authentication methods and the current settings.
3. To change the authentication method, click *Configure* and select the authentication method you want to modify. This takes you directly to the client configuration modules in YaST. For information about the configuration of the appropriate client, refer to the following sections:

   NIS: Section "Configuring NIS Clients" (Chapter 3, *Using NIS*, ↑Security Guide)

   LDAP: Section "Configuring an LDAP Client with YaST" (Chapter 4, *LDAP—A Directory Service*, ↑Security Guide)
4. After accepting the configuration, return to the *User and Group Administration* overview.
5. Click *OK* to close the administration dialog.