

# SUSE Linux Enterprise Desktop

11

[www.novell.com](http://www.novell.com)

February 23, 2009

Deployment Guide



# ***Deployment Guide***

All content is copyright © 2006- 2009 Novell, Inc.

## **Legal Notice**

This manual is protected under Novell intellectual property rights. By reproducing, duplicating or distributing this manual you explicitly agree to conform to the terms and conditions of this license agreement.

This manual may be freely reproduced, duplicated and distributed either as such or as part of a bundled package in electronic and/or printed format, provided however that the following conditions are fulfilled:

That this copyright notice and the names of authors and contributors appear clearly and distinctively on all reproduced, duplicated and distributed copies. That this manual, specifically for the printed format, is reproduced and/or distributed for noncommercial use only. The express authorization of Novell, Inc must be obtained prior to any other use of any manual or part thereof.

For Novell trademarks, see the Novell Trademark and Service Mark list <http://www.novell.com/company/legal/trademarks/tmlist.html>. \* Linux is a registered trademark of Linus Torvalds. All other third party trademarks are the property of their respective owners. A trademark symbol (®, ™ etc.) denotes a Novell trademark; an asterisk (\*) denotes a third party trademark.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither Novell, Inc., SUSE LINUX Products GmbH, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.

# Contents

<b>About This Guide</b>	<b>vii</b>
<b>1 Planning for SUSE Linux Enterprise Desktop</b>	<b>1</b>
1.1 Hardware Requirements . . . . .	2
1.2 Reasons to Use SUSE Linux Enterprise Desktop . . . . .	2
<b>Part I Manual Deployment</b>	<b>5</b>
<b>2 Deployment Strategies</b>	<b>7</b>
2.1 Deploying up to 10 Workstations . . . . .	7
2.2 Deploying up to 100 Workstations . . . . .	9
2.3 Deploying More than 100 Workstations . . . . .	16
<b>3 Installation with YaST</b>	<b>17</b>
3.1 Choosing the Installation Method . . . . .	17
3.2 The Installation Workflow . . . . .	20
3.3 System Start-Up for Installation . . . . .	20
3.4 The Boot Screen . . . . .	21
3.5 Welcome . . . . .	25
3.6 Installation Mode . . . . .	26
3.7 Clock and Time Zone . . . . .	29
3.8 Create New User . . . . .	30
3.9 Installation Settings . . . . .	34
3.10 Performing the Installation . . . . .	38
3.11 Configuration of the Installed System . . . . .	38
3.12 Graphical Login . . . . .	46

<b>4</b>	<b>Updating SUSE Linux Enterprise</b>	<b>47</b>
4.1	Updating SUSE Linux Enterprise . . . . .	47
4.2	Installing Service Packs . . . . .	50
4.3	Software Changes from Version 10 to Version 11 . . . . .	50
<b>5</b>	<b>Setting Up Hardware Components with YaST</b>	<b>51</b>
5.1	Probing Your Hardware . . . . .	51
5.2	Setting Up Graphics Card and Monitor . . . . .	52
5.3	Setting Up Keyboard and Mouse . . . . .	53
5.4	Setting Up Sound Cards . . . . .	56
5.5	Setting Up a Printer . . . . .	58
5.6	Setting Up a Scanner . . . . .	62
<b>6</b>	<b>Installing or Removing Software</b>	<b>65</b>
6.1	Definition of Terms . . . . .	65
6.2	Using the Qt Interface . . . . .	66
6.3	Using the GTK+ Interface . . . . .	71
6.4	Managing Software Repositories and Services . . . . .	75
6.5	Keeping the System Up-to-date . . . . .	77
<b>7</b>	<b>Installing Add-On Products</b>	<b>85</b>
7.1	Add-Ons . . . . .	85
7.2	Binary Drivers . . . . .	86
7.3	SUSE Software Development Kit (SDK) 10 . . . . .	86
<b>8</b>	<b>Accessing the Internet</b>	<b>87</b>
8.1	Direct Internet Connection . . . . .	87
8.2	Internet Connection Via Network . . . . .	90
<b>9</b>	<b>Managing Users with YaST</b>	<b>91</b>
9.1	User and Group Administration Dialog . . . . .	91
9.2	Managing User Accounts . . . . .	93
9.3	Additional Options for User Accounts . . . . .	95
9.4	Changing Default Settings for Local Users . . . . .	103
9.5	Assigning Users to Groups . . . . .	104
9.6	Managing Groups . . . . .	104
9.7	Changing the User Authentication Method . . . . .	106

<b>10</b>	<b>Changing Language and Country Settings with YaST</b>	<b>109</b>
10.1	Changing the System Language . . . . .	109
10.2	Changing the Country and Time Settings . . . . .	113
<b>11</b>	<b>Remote Installation</b>	<b>117</b>
11.1	Installation Scenarios for Remote Installation . . . . .	117
11.2	Setting Up the Server Holding the Installation Sources . . . . .	126
11.3	Preparing the Boot of the Target System . . . . .	136
11.4	Booting the Target System for Installation . . . . .	146
11.5	Monitoring the Installation Process . . . . .	150
<b>12</b>	<b>Advanced Disk Setup</b>	<b>155</b>
12.1	Using the YaST Partitioner . . . . .	155
12.2	LVM Configuration . . . . .	163
12.3	Soft RAID Configuration . . . . .	168
<b>13</b>	<b>Subscription Management</b>	<b>173</b>
13.1	Using Kernel Parameters to Access an SMT Server . . . . .	174
13.2	Configuring Clients Using AutoYaST Profile . . . . .	175
13.3	Configuring Clients Using the clientSetup4SMT.sh Script . . . . .	177
13.4	Registering Clients Against SMT Test Environment . . . . .	177
<b>Part II</b>	<b>Imaging and Creating Products</b>	<b>179</b>
<b>14</b>	<b>KIWI</b>	<b>181</b>
14.1	Prerequisites for KIWI . . . . .	181
14.2	Knowing KIWI's Build Process . . . . .	182
14.3	Image Description . . . . .	182
14.4	Creating Appliances with KIWI . . . . .	186
14.5	For More Information . . . . .	188
<b>15</b>	<b>Creating Add-On Products With Add-on Creator</b>	<b>189</b>
15.1	Creating Images . . . . .	189
15.2	Add-On Structure . . . . .	190
15.3	For More Information . . . . .	191
<b>16</b>	<b>Creating Images with YaST Product Creator</b>	<b>193</b>
16.1	Prerequisites for Product Creator . . . . .	193

16.2	Creating Images . . . . .	193
16.3	For More Information . . . . .	195
<b>17</b>	<b>Deploying Customized Preinstallations</b>	<b>197</b>
17.1	Preparing the Master Machine . . . . .	198
17.2	Customizing the Firstboot Installation . . . . .	198
17.3	Cloning the Master Installation . . . . .	207
17.4	Personalizing the Installation . . . . .	207
<b>Part III</b>	<b>Automated Installations</b>	<b>209</b>
<b>18</b>	<b>Automated Installation</b>	<b>211</b>
18.1	Simple Mass Installation . . . . .	211
18.2	Rule-Based Autoinstallation . . . . .	223
18.3	For More Information . . . . .	228
<b>19</b>	<b>Automated Deployment of Preload Images</b>	<b>229</b>
19.1	Deploying system manually from rescue image . . . . .	230
19.2	Automated Deployment with PXE Boot . . . . .	231

# About This Guide

Installations of SUSE Linux Enterprise Desktop are possible in many different ways. It is impossible to cover all combinations of boot, or installation server, automated installations or deploying images. This manual should help with selecting the appropriate method of deployment for your installation.

## Part I, “Manual Deployment” (page 5)

Most tasks that are needed during installations are described here. This includes the manual setup of your computer as well as additional software and remote installations.

## Part II, “Imaging and Creating Products” (page 179)

Mass installations often require to prepare images or products furnished with the features that are needed in this special case. Several options are described that allow the administrator to prepare this deployment methods.

## Part III, “Automated Installations” (page 209)

To do unattended installations, either use the installation with AutoYaST or prepare an image with kiwi or firstboot. This part describes methods to deploy these installations with a minimum of user interaction.

Many chapters in this manual contain links to additional documentation resources. This includes additional documentation that is available on the system as well as documentation available on the Internet.

For an overview of the documentation available for your product and the latest documentation updates, refer to <http://www.novell.com/documentation> or to the following section.

## 1 Available Documentation

We provide HTML and PDF versions of our books in different languages. The following manuals for users and administrators are available on this product:

### GNOME User Guide (↑GNOME User Guide)

Introduces the GNOME desktop of SUSE Linux Enterprise Desktop. It guides you through using and configuring the desktop and helps you perform key tasks. It is

intended mainly for end users who want to make efficient use of GNOME desktop as their default desktop.

#### Application Guide (↑Application Guide)

Learn how to use and configure key desktop applications on SUSE Linux Enterprise Desktop. This guide introduces browsers and e-mail clients as well as office applications and collaboration tools. It also covers graphics and multimedia applications.

#### Deployment Guide (page 1)

Shows how to install single or multiple systems and how to exploit the product inherent capabilities for a deployment infrastructure. Choose from various approaches, ranging from a local installation or a network installation server to a mass deployment using a remote-controlled, highly-customized, and automated installation technique.

#### Administration Guide (↑Administration Guide)

Covers system administration tasks like maintaining, monitoring and customizing an initially installed system.

#### Security Guide (↑Security Guide)

Introduces basic concepts of system security, covering both local and network security aspects. Shows how to make use of the product inherent security software like Novell AppArmor (which lets you specify per program which files the program may read, write, and execute) or the auditing system that reliably collects information about any security-relevant events.

#### System Analysis and Tuning Guide (↑System Analysis and Tuning Guide)

An administrator's guide for problem detection, resolution and optimization. Find how to inspect and optimize your system by means of monitoring tools and how to efficiently manage resources. Also contains an overview of common problems and solutions and of additional help and documentation resources.

#### Virtualization with Xen (↑Virtualization with Xen)

Offers an introduction to virtualization technology of your product. It features an overview of the various fields of application and installation types of each of the platforms supported by SUSE Linux Enterprise Server as well as a short description of the installation procedure.

In addition to the comprehensive manuals, several quick start guides are available:



### Installation Quick Start (↑Installation Quick Start)

Lists the system requirements and guides you step-by-step through the installation of SUSE Linux Enterprise Desktop from DVD, or from an ISO image.

### *Linux Audit Quick Start*

Gives a short overview how to enable and configure the auditing system and how to execute key tasks such as setting up audit rules, generating reports, and analyzing the log files.

### *Novell AppArmor Quick Start*

Helps you understand the main concepts behind Novell® AppArmor.

Find HTML versions of most SUSE Linux Enterprise Desktop manuals in your installed system under `/usr/share/doc/manual` or in the help centers of your desktop.

Find the latest documentation updates at <http://www.novell.com/documentation> where you can download PDF or HTML versions of the manuals for your product.

## 2 Feedback

Several feedback channels are available:

- To report bugs for a product component or to submit enhancements requests, please use <https://bugzilla.novell.com/>. If you are new to Bugzilla, you might find the *Bug Writing FAQs* helpful, available from the Novell Bugzilla home page.
- We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

## 3 Documentation Conventions

The following typographical conventions are used in this manual:

- `/etc/passwd`: filenames and directory names

- *placeholder*: replace *placeholder* with the actual value
- `PATH`: the environment variable `PATH`
- `ls`, `--help`: commands, options, and parameters
- `user`: users or groups
- `Alt`, `Alt + F1`: a key to press or a key combination; keys are shown in uppercase as on a keyboard
- *File*, *File > Save As*: menu items, buttons
- *Dancing Penguins* (Chapter *Penguins*, ↑Another Manual): This is a reference to a chapter in another manual.

# Planning for SUSE Linux Enterprise Desktop

# 1

This chapter is addressed mainly to corporate system administrators who face the task of having to deploy SUSE® Linux Enterprise Desktop at their site. Rolling out SUSE Linux Enterprise Desktop to an entire site should involve careful planning and consideration of the following questions:

For which purpose will the SUSE Linux Enterprise Desktop workstations be used?

Determine the purpose for which SUSE Linux Enterprise Desktop should be used and make sure that hardware and software able to match these requirements are used. Consider testing your setup on a single machine before rolling it out to the entire site.

How many workstations should be installed?

Determine the scope of your deployment of SUSE Linux Enterprise Desktop. Depending on the number of installation planned, consider different approaches to the installation or even a mass installation using SUSE Linux Enterprises unique AutoYaST or KIWI technology. For more information about this subject, refer to *Chapter 2, Deployment Strategies* (page 7).

How do you get software updates for your deployment?

All patches provided by Novell for your product are available for download to registered users. Register and find the patch support database at <http://www.novell.com/linux/suse/portal/index.html>.

Do you need help for your local deployment?

Novell provides training, support, and consulting for all topics around SUSE Linux Enterprise Desktop. Find more information about this at <http://www.novell.com/products/desktop/>.

# 1.1 Hardware Requirements

For a standard installation of SUSE Linux Enterprise Desktop including the desktop environment and a wealth of applications, the following configuration is recommended:

- Intel Pentium IV, 2.4 GHz or higher or any AMD64 or Intel 64 processor
- 1–2 physical CPUs
- 512 MB physical RAM or higher
- 3 GB of available disk space or more
- 1024 x 768 display resolution (or higher)

# 1.2 Reasons to Use SUSE Linux Enterprise Desktop

Let the following items guide you in your selection of SUSE Linux Enterprise Desktop and while determining the purpose of the installed systems:

## Wealth of Applications

SUSE Linux Enterprise Desktop's broad offer of software makes it appeal to both professional users in a corporate environment and to home users or users in smaller networks.

## Ease of Use

SUSE Linux Enterprise Desktop comes with two enterprise-ready desktop environments, GNOME and KDE. Both enable users to comfortably adjust to a Linux system while maintaining their efficiency and productivity. To explore the desktops in detail, refer to the KDE User Guide (↑KDE User Guide) and the GNOME User Guide (↑GNOME User Guide).

## Support for Mobile Users

With the NetworkManager technology fully integrated into SUSE Linux Enterprise Desktop and its two desktop environments, mobile users will enjoy the freedom of easily joining and switching wired and wireless networks.

## Seamless Integration into Existing Networks

SUSE Linux Enterprise Desktop was designed to be a versatile network citizen. It cooperates with various different network types:

**Pure Linux Networks** SUSE Linux Enterprise Desktop is a complete Linux client and supports all the protocols used in traditional Linux and Unix\* environments. It integrates well with networks consisting of other SUSE Linux or SUSE Linux Enterprise machines. LDAP, NIS, and local authentication are supported.

**Windows Networks** SUSE Linux Enterprise Desktop supports Active Directory as an authentication source. It offers you all the advantages of a secure and stable Linux operating system plus convenient interaction with other Windows clients and means to manipulate your Windows user data from a Linux client. Explore this feature in detail in Chapter 5, *Active Directory Support* (↑Security Guide).

**Windows and Novell Networks** Being backed by Novell and their networking expertise, SUSE Linux Enterprise Desktop naturally offers you support for Novell technologies, like GroupWise, Novell Client for Linux, and iPrint, and it also offers authentication support for Novell eDirectory services.

## Application Security with Novell AppArmor

SUSE Linux Enterprise Desktop enables you to secure your applications by enforcing security profiles tailor-made for your applications. To learn more about Novell AppArmor, refer to <http://www.novell.com/documentation/apparmor/>.



# **Part I. Manual Deployment**





# Deployment Strategies

There are several different ways to deploy SUSE Linux Enterprise Desktop. Choose from various approaches ranging from a local installation using physical media or a network installation server to a mass deployment using a remote-controlled, highly-customized, and automated installation technique. Select the method that best matches your requirements.

---

**TIP: Using Xen Virtualization with SLED**

You may use the Xen virtualization technology to test virtual instances of SUSE Linux Enterprise Desktop prior to rolling it out to real hardware. You could also experiment with basic Windows\*-in-SLED setups. For more information about the virtualization technology available with SUSE Linux Enterprise Desktop, refer to [http://www.novell.com/documentation/sles10/xen\\_admin/data/bookinfo.html](http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html).

---

## 2.1 Deploying up to 10 Workstations

If your deployment of SUSE Linux Enterprise Desktop only involves 1 to 10 workstations, the easiest and least complex way of deploying SUSE Linux Enterprise Desktop is a plain manual installation as featured in **Chapter 3, *Installation with YaST*** (page 17). Manual installation can be done in several different ways depending on your requirements:

**Installing from the SUSE Linux Enterprise Desktop Media** (page 8)

Consider this approach if you want to install a single, disconnected workstation.

### Installing from a Network Server Using SLP (page 8)

Consider this approach if you have a single workstation or a small number of workstations and if a network installation server announced via SLP is available.

### Installing from a Network Server (page 9)

Consider this approach if you have a single workstation or a small number of workstations and if a network installation server is available.

**Table 2.1** *Installing from the SUSE Linux Enterprise Desktop Media*

Installation Source	SUSE Linux Enterprise Desktop media kit
Tasks Requiring Manual Interaction	<ul style="list-style-type: none"><li>• Inserting the installation media</li><li>• Booting the installation target</li><li>• Changing media</li><li>• Determining the YaST installation scope</li><li>• Configuring the system with YaST system</li></ul>
Remotely Controlled Tasks	None
Details	<a href="#">Installing from the SUSE Linux Enterprise Desktop Media (page 17)</a>

**Table 2.2** *Installing from a Network Server Using SLP*

Installation Source	Network installation server holding the SUSE Linux Enterprise Desktop installation media
Tasks Requiring Manual Interaction	<ul style="list-style-type: none"><li>• Inserting the boot disk</li><li>• Booting installation target</li><li>• Determining the YaST installation scope</li><li>• Configuring the system with YaST</li></ul>

Remotely Controlled Tasks	None, but this method can be combined with VNC
Details	<a href="#">Section 3.1.1, “Installing from a Network Server Using SLP”</a> (page 19)

---

**Table 2.3** *Installing from a Network Server*

---

Installation Source	Network installation server holding the SUSE Linux Enterprise Desktop installation media
Tasks Requiring Manual Interaction	<ul style="list-style-type: none"> <li>• Inserting the boot disk</li> <li>• Providing boot options</li> <li>• Booting the installation target</li> <li>• Determining the YaST installation scope</li> <li>• Configuring the system with YaST</li> </ul>

Remotely Controlled Tasks	None, but method can be combined with VNC
Details	<a href="#">Section 3.1.2, “Installing from a Network Source without SLP”</a> (page 20)

---

## 2.2 Deploying up to 100 Workstations

With a growing numbers of workstations to install, you certainly do not want to install and configure each one of them manually. There are many automated or semiautomated approaches as well as several options to perform an installation with minimal to no physical user interaction.

Before considering a fully-automated approach, take into account that the more complex the scenario gets the longer it takes to set up. If a time limit is associated with your deployment, it might be a good idea to select a less complex approach that can be carried out much more quickly. Automation makes sense for huge deployments and those that need to be carried out remotely.

Choose from the following options:

**Simple Remote Installation via VNC—Static Network Configuration** (page 11)

Consider this approach in a small to medium scenario with a static network setup. A network, network installation server, and VNC viewer application are required.

**Simple Remote Installation via VNC—Dynamic Network Configuration** (page 11)

Consider this approach in a small to medium scenario with dynamic network setup through DHCP. A network, network installation server, and VNC viewer application are required.

**Remote Installation via VNC—PXE Boot and Wake on LAN** (page 12)

Consider this approach in a small to medium scenario that should be installed via network and without physical interaction with the installation targets. A network, a network installation server, network boot images, network bootable target hardware, and a VNC viewer application are required.

**Simple Remote Installation via SSH—Static Network Configuration** (page 12)

Consider this approach in a small to medium scenario with static network setup. A network, network installation server, and SSH client application are required.

**Remote Installation via SSH—Dynamic Network Configuration** (page 13)

Consider this approach in a small to medium scenario with dynamic network setup through DHCP. A network, network installation server, and SSH client application are required.

**Remote Installation via SSH—PXE Boot and Wake on LAN** (page 14)

Consider this approach in a small to medium scenario that should be installed via network and without physical interaction with the installation targets. A network, a network installation server, network boot images, network bootable target hardware, and an SSH client application are required.

**Simple Mass Installation** (page 14)

Consider this approach for large deployments to identical machines. If configured to use network booting, physical interaction with the target systems is not needed at all. A network, a network installation server, a remote controlling application such as a VNC viewer or an SSH client, and an AutoYaST configuration profile are required. If using network boot, a network boot image and network bootable hardware are required as well.

### Rule-Based Autoinstallation (page 15)

Consider this approach for large deployments to various types of hardware. If configured to use network booting, physical interaction with the target systems is not needed at all. A network, a network installation server, a remote controlling application such as a VNC viewer or an SSH client, and several AutoYaST configuration profiles as well as a rule setup for AutoYaST are required. If using network boot, a network boot image and network bootable hardware are required as well.

**Table 2.4** *Simple Remote Installation via VNC—Static Network Configuration*

Installation Source	Network
Preparations	<ul style="list-style-type: none"><li>• Setting up an installation source</li><li>• Booting from the installation media</li></ul>
Control and Monitoring	Remote: VNC
Best Suited For	small to medium scenarios with varying hardware
Drawbacks	<ul style="list-style-type: none"><li>• Each machine must be set up individually</li><li>• Physical access is needed for booting</li></ul>
Details	<a href="#">Section 11.1.1, “Simple Remote Installation via VNC—Static Network Configuration”</a> (page 118)

**Table 2.5** *Simple Remote Installation via VNC—Dynamic Network Configuration*

Installation Source	Network
Preparations	<ul style="list-style-type: none"><li>• Setting up the installation source</li><li>• Booting from the installation media</li></ul>
Control and Monitoring	Remote: VNC

Best Suited For	Small to medium scenarios with varying hardware
Drawbacks	<ul style="list-style-type: none"> <li>• Each machine must be set up individually</li> <li>• Physical access is needed for booting</li> </ul>
Details	<a href="#">Section 11.1.2, “Simple Remote Installation via VNC—Dynamic Network Configuration”</a> (page 119)

---

**Table 2.6** *Remote Installation via VNC—PXE Boot and Wake on LAN*

---

Installation Source	Network
Preparations	<ul style="list-style-type: none"> <li>• Setting up the installation source</li> <li>• Configuring DHCP, TFTP, PXE boot, and WOL</li> <li>• Booting from the network</li> </ul>
Control and Monitoring	Remote: VNC
Best Suited For	<ul style="list-style-type: none"> <li>• Small to medium scenarios with varying hardware</li> <li>• Completely remote installs; cross-site deployment</li> </ul>
Drawbacks	Each machine must be set up manually
Details	<a href="#">Section 11.1.3, “Remote Installation via VNC—PXE Boot and Wake on LAN”</a> (page 121)

---

**Table 2.7** *Simple Remote Installation via SSH—Static Network Configuration*

---

Installation Source	Network
Preparations	<ul style="list-style-type: none"> <li>• Setting up the installation source</li> </ul>

	<ul style="list-style-type: none"> <li>• Booting from the installation media</li> </ul>
Control and Monitoring	Remote: SSH
Best Suited For	<ul style="list-style-type: none"> <li>• Small to medium scenarios with varying hardware</li> <li>• Low bandwidth connections to target</li> </ul>
Drawbacks	<ul style="list-style-type: none"> <li>• Each machine must be set up individually</li> <li>• Physical access is needed for booting</li> </ul>
Details	Section 11.1.4, “Simple Remote Installation via SSH—Static Network Configuration” (page 122)

---

**Table 2.8** *Remote Installation via SSH—Dynamic Network Configuration*

---

Installation Source	Network
Preparations	<ul style="list-style-type: none"> <li>• Setting up the installation source</li> <li>• Booting from installation media</li> </ul>
Control and Monitoring	Remote: SSH
Best Suited For	<ul style="list-style-type: none"> <li>• Small to medium scenarios with varying hardware</li> <li>• Low bandwidth connections to target</li> </ul>
Drawbacks	<ul style="list-style-type: none"> <li>• Each machine must be set up individually</li> <li>• Physical access is needed for booting</li> </ul>

Details	Section 11.1.5, “Simple Remote Installation via SSH—Dynamic Network Configuration” (page 123)
---------	---

**Table 2.9**    *Remote Installation via SSH—PXE Boot and Wake on LAN*

Installation Source	Network
Preparations	<ul style="list-style-type: none"> <li>• Setting up the installation source</li> <li>• Configuring DHCP, TFTP, PXE boot, and WOL</li> <li>• Booting from the network</li> </ul>
Control and Monitoring	Remote: SSH
Best Suited For	<ul style="list-style-type: none"> <li>• Small to medium scenarios with varying hardware</li> <li>• Completely remote installs; cross-site deployment</li> <li>• Low bandwidth connections to target</li> </ul>
Drawbacks	Each machine must be set up individually
Details	Section 11.1.6, “Remote Installation via SSH—PXE Boot and Wake on LAN” (page 125)

**Table 2.10**    *Simple Mass Installation*

Installation Source	Preferably network
Preparations	<ul style="list-style-type: none"> <li>• Gathering hardware information</li> <li>• Creating AutoYaST profile</li> <li>• Setting up the installation server</li> <li>• Distributing the profile</li> </ul>



	<ul style="list-style-type: none"> <li>• Setting up network boot (DHCP, TFTP, PXE, WOL)</li> </ul> <p><i>or</i></p> <p>Booting the target from installation media</p>
Control and Monitoring	Local or remote through VNC or SSH
Best Suited For	<ul style="list-style-type: none"> <li>• Large scenarios</li> <li>• Identical hardware</li> <li>• No access to system (network boot)</li> </ul>
Drawbacks	Applies only to machines with identical hardware
Details	<b>Section 18.1, “Simple Mass Installation”</b> (page 211)

**Table 2.11** *Rule-Based Autoinstallation*

Installation Source	Preferably network
Preparations	<ul style="list-style-type: none"> <li>• Gathering hardware information</li> <li>• Creating AutoYaST profiles</li> <li>• Creating AutoYaST rules</li> <li>• Setting up the installation server</li> <li>• Distributing the profile</li> <li>• Setting up network boot (DHCP, TFTP, PXE, WOL)</li> </ul> <p><i>or</i></p> <p>Booting the target from installation media</p>

Control and Monitoring	Local or remote through SSH or VNC
Best Suited For	<ul style="list-style-type: none"> <li>• Varying hardware</li> <li>• Cross-site deployments</li> </ul>
Drawbacks	Complex rule setup
Details	<a href="#">Section 18.2, “Rule-Based Autoinstallation”</a> (page 223)

---

## 2.3 Deploying More than 100 Workstations

Most of the considerations brought up for medium installation scenarios in [Section 2.1, “Deploying up to 10 Workstations”](#) (page 7) still hold true for large scale deployments. However, with a growing number of installation targets, the benefits of a fully automated installation method outweigh its disadvantages.

It pays off to invest a considerable amount of time to create a sophisticated rule and class framework in AutoYaST to match the requirements of a huge deployment site. Not having to touch each target separately can save you a tremendous amount of time depending on the scope of your installation project.

As an alternative, and if user settings should be done during the first bootup, create preload images with kiwi and firstboot. Deploying such images could even be done by a PXE boot server specialized for this task. For more details, see [Chapter 14, \*KIWI\*](#) (page 181), [Chapter 18, \*Automated Installation\*](#) (page 211), and [Chapter 17, \*Deploying Customized Preinstallations\*](#) (page 197).

# Installation with YaST

Install your SUSE® Linux Enterprise Desktop system with YaST, the central tool for installation and configuration of your system. YaST guides you through the installation process and the basic configuration of your system. During the installation and configuration process, YaST analyzes both your current system settings and your hardware components and proposes installation settings based on this analysis. By default, YaST displays an overview of all installation steps on the left hand side of the window and provides online help texts for each step. Click *Help* to view the help text.

If you are a first-time user of SUSE Linux Enterprise Desktop, you might want to follow the default YaST proposals in most parts, but you can also adjust the settings as described here to fine-tune your system according to your needs and wishes. Many parts of the basic system configuration, such as user accounts or system language, can also be modified after the installation process.

## 3.1 Choosing the Installation Method

After having selected the installation medium, determine a suitable installation method and boot option that best match your needs:

Installing from the SUSE Linux Enterprise Desktop Media

Choose this option, if you want to perform a stand-alone installation and do not want to rely on a network providing the installation data or the boot infrastructure. The installation proceeds exactly as outlined in [Section 3.2, “The Installation Workflow”](#) (page 20).

### Installing from the LiveDVD

In order to install from a LiveCD, boot the live system from DVD. In the running system, launch the installation routine by clicking on the *Install* icon on the desktop. Phase one of the installation will be carried out in a window on the desktop. It is not possible to update or repair an existing system with a LiveDVD, you can only perform a new installation with automatic configuration.

### Installing from a Network Server

Choose this option, if you have an installation server available in your network or want to use an external server as the source of your installation data. This setup can be configured to use from physical media (Floppy, CD/DVD, or hard disk) for booting or configured to boot via network using PXE/BOOTP. Refer to [Section 3.1.1, “Installing from a Network Server Using SLP”](#) (page 19), [Section 3.1.2, “Installing from a Network Source without SLP”](#) (page 20), or [Chapter 11, \*Remote Installation\*](#) (page 117) for details.

SUSE Linux Enterprise Desktop supports several different boot options from which you can choose depending on the hardware available and on the installation scenario you prefer. Booting from the SUSE Linux Enterprise Desktop media is the most straightforward option, but special requirements might call for special setups:

**Table 3.1** *Boot Options*

Boot Option	Description
DVD	This is the easiest boot option. This option can be used if the system has a local DVD-ROM drive that is supported by Linux.
Floppy	The data for generating boot floppies are located on DVD 1 in the <code>/boot/architecture/</code> directory. A README with instructions on how to create the boot floppies is available in the same directory.
PXE or BOOTP	Bootting over the network must be supported by the system's BIOS or firmware and a boot server must be available in the network. This task can also be handled by another SUSE Linux Enterprise Desktop system. Refer to <a href="#">Chapter 11, <i>Remote Installation</i></a> (page 117) for more information.

Boot Option	Description
Hard Disk	SUSE Linux Enterprise Desktop installation can also be booted from the hard disk. To do this, copy the kernel ( <code>linux</code> ) and the installation system ( <code>initrd</code> ) from the directory <code>/boot/architecture/</code> on the installation media to the hard disk and add an appropriate entry to the existing boot loader of a previous SUSE Linux Enterprise Desktop installation.

---

**TIP: Booting from DVD on UEFI machines**

► **amd64 em64t:** DVD1 can be used as a boot medium for machines equipped with UEFI (Unified Extensible Firmware Interface). Refer to your vendor's documentation for specific information. If booting fails, try to enable CSM (Compatibility Support Module) in your firmware. ◀

---

## 3.1.1 Installing from a Network Server Using SLP

If your network setup supports OpenSLP and your network installation source has been configured to announce itself via SLP (described in [Section 11.2, “Setting Up the Server Holding the Installation Sources”](#) (page 126)), boot the system, press F4 in the boot screen and select *SLP* from the menu.

The installation program configures the network connection with DHCP and retrieves the location of the network installation source from the OpenSLP server. If the automatic DHCP network configuration fails, you are prompted to enter the appropriate parameters manually. The installation then proceeds as described below with the exception of the network configuration step needed prior to adding additional repositories. This step is not needed as the network is already configured and active at this point.

## 3.1.2 Installing from a Network Source without SLP

If your network setup does not support OpenSLP for the retrieval of network installation sources, boot the system and press F4 in the boot screen to select the desired network protocol (NFS, HTTP, FTP, or SMB/CIFS). Provide the server's address and the path to the installation media.

The installation program automatically configures the network connection with DHCP. If this configuration fails, you are prompted to enter the appropriate parameters manually. The installation retrieves the installation data from the source specified. The installation then proceeds as described below with the exception of the network configuration step needed prior to adding additional repositories. This step is not needed as the network is already configured and active at this point.

## 3.2 The Installation Workflow

The SUSE Linux Enterprise Desktop installation is split into three main parts: preparation, installation, configuration. During the preparation phase you configure some basic parameters such as language, time, desktop type, users, passwords, hard disk setup and installation scope. In the non-interactive installation phase the software is installed and the system is prepared for the first boot. Upon finishing the installation the machine reboots into the newly installed system and starts the final system configuration. You can choose whether to do a fully automatic or a manual configuration. In this stage, network and Internet access, as well as hardware components such as printers, are set up.

## 3.3 System Start-Up for Installation

You can install SUSE Linux Enterprise Desktop from local installation sources, such as the SUSE Linux Enterprise Desktop CDs or DVD, or from network source of an FTP, HTTP, NFS, or SMB server. Any of these approaches requires physical access to the system to install and user interaction during the installation. The installation procedure is basically the same regardless of the installation source. Any exceptions are sufficiently highlighted in the following workflow description. For a description on

how to perform non-interactive, automated installations, refer to [Part III, “Automated Installations”](#) (page 209).

## 3.4 The Boot Screen

The boot screen displays a number of options for the installation procedure. *Boot from Hard Disk* boots the installed system and is selected default, because the CD is often left in the drive. Select one of the other options with the arrow keys and press Enter to boot it. The relevant options are:

### *Installation*

The normal installation mode. All modern hardware functions are enabled. In case the installation fails, see [F5Kernel](#) (page 23) for boot options that disable potentially problematic functions.

### *Repair Installed System*

Boots into the graphical repair system. More information on repairing an installed system is available in Section “Recovering a Corrupted System” (Chapter 7, *Common Problems and Their Solutions*, ↑System Analysis and Tuning Guide).

### *Rescue System*

Starts a minimal Linux system without a graphical user interface. For more information, see Section “Using the Rescue System” (Chapter 7, *Common Problems and Their Solutions*, ↑System Analysis and Tuning Guide).

### *Firmware Test*

Starts a BIOS checker that validates ACPI and other parts of your BIOS.

### *Memory Test*

Tests your system RAM using repeated read and write cycles. Terminate the test by rebooting. For more information, see Section “Fails to Boot” (Chapter 7, *Common Problems and Their Solutions*, ↑System Analysis and Tuning Guide). This option is not available with the CD-KDE and CD-GNOME media.

**Figure 3.1** *The Boot Screen*



Use the function keys indicated in the bar at the bottom of the screen to change the language, screen resolution, installation source or to add additional driver from your hardware vendor:

#### **F1***Help*

Get context-sensitive help for the active element of the boot screen. Use the arrow keys to navigate, Enter to follow a link, and Esc to leave the help screen.

#### **F2***Language*

Select the display language and a corresponding keyboard layout for the installation. The default language is English (US).

#### **F3***Video Mode*

Select various graphical display modes for the installation. Select *Text Mode* if the graphical installation causes problems.

#### **F4***Source*

Normally, the installation is performed from the inserted installation medium. Here, select other sources, like FTP or NFS servers. If the installation is carried out in a network with an SLP server, select an installation source available on the server



with this option. Find information about SLP in Chapter 21, *SLP Services in the Network* (↑Administration Guide).

#### F5Kernel

In case you encounter problems with the regular installation, this menu offers to disable a few potentially problematic functions. If your hardware does not support ACPI (advanced configuration and power interface) select *No ACPI* to install without ACPI support. *No local APIC* disables support for APIC (Advanced Programmable Interrupt Controllers) which may cause problems with some hardware. *Safe Settings* boots the system with the DMA mode (for CD/DVD-ROM drives) and power management functions disabled.

If you are not sure, try the following options first: *Installation—ACPI Disabled* or *Installation—Safe Settings*. Experts can also use the command line (*Boot Options*) to enter or change kernel parameters.

#### F6Driver

Press this key to tell the system that you have an optional driver update for SUSE Linux Enterprise Desktop. With *File* or *URL*, load drivers directly before the installation starts. If you select *Yes*, you are prompted to insert the update disk at the appropriate point in the installation process.

---

### TIP: Using IPv6 during the Installation

By default you can only assign IPv4 network addresses to your machine. To enable IPv6 during installation, enter one of the following parameters at the bootprompt: `ipv6=1` (accept IPv4 and IPv6) or `ipv6only=1` (accept IPv6 only).

---

After starting the installation, SUSE Linux Enterprise Desktop loads and configures a minimal Linux system to run the installation procedure. To view the boot messages and copyright notices during this process, press Esc. On completion of this process, the YaST installation program starts and displays the graphical installer.

---

### TIP: Installation without a Mouse

If the installer does not detect your mouse correctly, use Tab for navigation, arrow keys to scroll, and Enter to confirm a selection. Various buttons or selection fields contain a letter with an underscore. Use Alt + Letter to select a button or a selection directly instead of navigating there with Tab.

---

## 3.4.1 Providing Data to Access an SMT Server

By default updates for SUSE Linux Enterprise Desktop are delivered by the Novell Customer Center. If your network provides a so called SMT server to provide a local update source, you need to equip the client with the server's URL. Client and server communicate solely via HTTPS protocol, therefore you also need to enter a path to the server's certificate if the certificate was not issued by a certificate authority. This information can either be entered at the boot prompt as described here, or during the registration process as described in [Section “Local Registration Server”](#) (page 43).

### smturl

URL of the SMT server. The URL has a fixed format

`https://FQN/center/regsvc/` *FQN* has to be full qualified hostname of the SMT server. Example:

```
smturl=https://smt.example.com/center/regsvc/
```

### smtcert

Location of the SMT server's certificate. Specify one of the following locations:

#### URL

Remote location (`http`, `https` or `ftp`) from which the certificate can be downloaded. Example:

```
smtcert=http://smt.example.com/smt-ca.crt
```

#### Floppy

Specifies a location on a floppy. The floppy has to be inserted at boot time, you will not be prompted to insert it if it is missing. The value has to start with the string `floppy` followed by the path to the certificate. Example:

```
smtcert=floppy/smt/smt-ca.crt
```

#### local path

Absolute path to the certificate on the local machine. Example:

```
smtcert=/data/inst/smt/smt-ca.cert
```

#### Interactive

Use `ask` to open a pop-up menu during the installation where you can specify the path to the certificate. Do not use this option with AutoYaST. Example

```
smtcert=ask
```

Deactivate certificate installation

Use `done` if either the certificate will be installed by an add-on product, or if you are using a certificate issued by an official certificate authority. Example:

```
smtcert=done
```

---

### **WARNING: Beware of typing errors**

Make sure the values you enter are correct. If `smturl` has not been specified correctly, the registration of the update source will fail. If a wrong value for `smtcert` has been entered, you will be prompted for a local path to the certificate.

In case `smtcert` is not specified, it will default to `http://FQN/smt.crt` with `FQN` being the name of the SMT server.

---

## **3.4.2 Configuring an alternative data server for supportconfig**

The data `supportconfig` (see Chapter 2, *Gathering System Information for Support* (↑Administration Guide) for more information) gathers is sent to the Novell Customer Center by default. It is also possible to set up a local server collecting this data. If such a server is available on your network, you need to equip the client with the server's URL. This information has to be entered at the boot prompt.

`supporturl`

URL of the server. The URL has the format `http://FQN/Path/` `FQN` has to be full qualified hostname of the server, `Path` has to be replaced with the location on the server. Example:

```
supporturl=http://support.example.com/supportconfig/data/
```

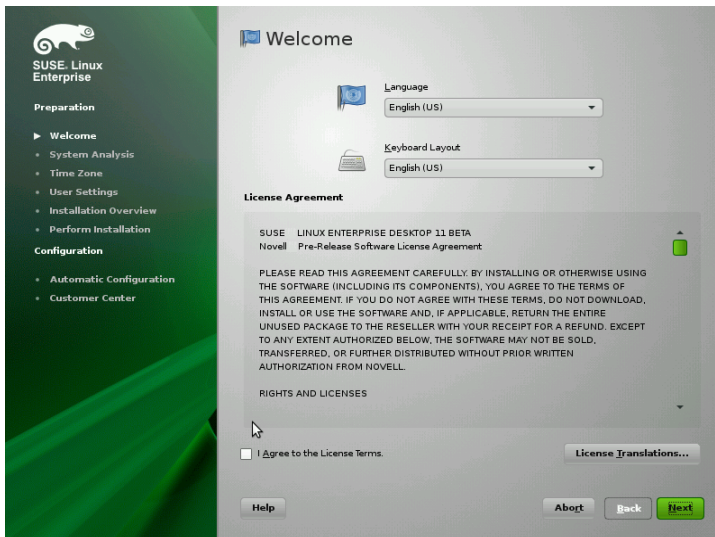
## **3.5 Welcome**

Start the installation of SUSE Linux Enterprise Desktop by choosing your language. Changing the language will automatically preselect a corresponding keyboard layout.

Override this proposal by selecting a different keyboard layout from the drop-down menu. The language selected here is also used to assume a time zone for the system clock. This setting—along with the selection of secondary languages to install on your system—can be modified later in the *Installation Summary*, described in [Section 3.9, “Installation Settings”](#) (page 34). For information about language settings in the installed system, see [Chapter 10, Changing Language and Country Settings with YaST](#) (page 109).

Read the license agreement that is displayed beneath the language and keyboard selection thoroughly. Use *License Translations...* to access translations. If you agree to the terms, check *I Agree to the License Terms* and click *Next* to proceed with the installation. If you do not agree to the license agreement, you cannot install SUSE Linux Enterprise Desktop. Click *Abort* to terminate the installation.

**Figure 3.2** *Welcome*



## 3.6 Installation Mode

After a system analysis where YaST probes for storage devices and tries to find other installed systems on your machine, the installation modes available are displayed.

### *New installation*

Select this option to start a new installation from scratch.

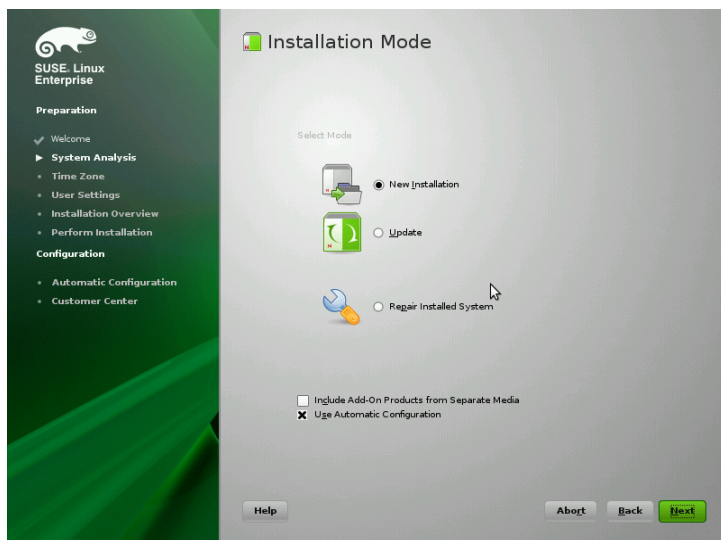
## Update

Select this option to update to a newer version. For more information about system update, see [Chapter 4, \*Updating SUSE Linux Enterprise\*](#) (page 47).

## Repair Installed System

Choose this option to repair a damaged system that is already installed. More information is available in Section “Recovering a Corrupted System” (Chapter 7, *Common Problems and Their Solutions*, ↑System Analysis and Tuning Guide).

**Figure 3.3** *Installation Mode*



By default, the automatic configuration is used when performing a new installation. In this mode the system automatically configures your hardware and the network, so the installation is performed with minimal user interaction. If necessary, you can change every configuration that is set up later in the installed system using YaST. In repair mode the automatic configuration attempts to fix errors automatically. Uncheck *Use Automatic Configuration* if you prefer a manual configuration during the installation or to start the system reparation in expert mode.

This screen also offers to include add-on products during the installation. To include such products, check *Include Add-On Products from Separate Media*. An add-on product can include extensions, third-party products or additional software for your system.

Click *Next* to proceed. If you selected to include an add-on product, proceed with [Section 3.6.1, “Add-On Products”](#) (page 28), otherwise skip the next section and advance to [Section 3.7, “Clock and Time Zone”](#) (page 29).

## 3.6.1 Add-On Products

Add-on products can be installed either from a local source (CD, DVD, or directory) or from a network source (HTTP, FTP, NFS, CIFS,...). When installing from a network source, you need to configure the network first—unless you are performing a network installation anyway. Choose *Yes, Run the Network Setup* and proceed as described in [Section “Network Setup”](#) (page 28). If the add-on product is available locally, select *No, Skip the Network Setup*.

Click *Next* and specify the product source. Source types available are *CD, DVD, Hard Disk, USB Stick or Disk*, a *Local Directory* or a *Local ISO Image*, if no network was configured. If the add-on product is available on removable media, the system automatically mounts the media and reads its contents. If the add-on product is available on hard disk, choose *Hard Disk* to install from an unmounted hard drive, or *Local Directory/Local ISO Image* if it is located in the file system. Add-on products may be delivered as a repository or as a set of rpm files. In the latter case, check *Plain RPM Directory*. While a network is available, you can choose from additional remote sources such as HTTP, SLP, FTP and others. It is also possible to specify a URL directly.

Check *Download Repository Description Files* to download the files describing the repository now. If unchecked, they will be downloaded once the installation starts. Proceed with *Next* and insert a CD or DVD if required. Depending on the product's content it may be necessary to accept additional license agreements.

It is also possible to configure add-on products at any time in the installed systems. Using add-on products in the installed system is described in [Chapter 7, Installing Add-On Products](#) (page 85).

## Network Setup

When invoking the network setup, YaST scans for available network cards. If more than one network card is found, you have to choose the card to configure from the list.

If an ethernet network adapter is not already connected, a warning will open. Make sure the network cable is plugged in and choose *Yes, Use It*. If your network is equipped

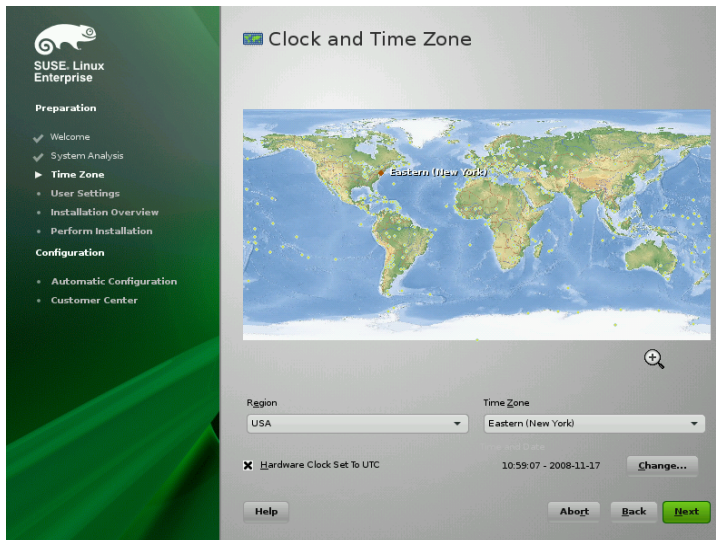
with a DHCP server, choose *Automatic Address Setup (via DHCP)*. To manually set up the network choose *Static Address Setup* and specify *IP Address*, *Netmask*, *Default Gateway IP*, and the *DNS Server IP*.

Some networks require the use of a proxy server to access the Internet. Tick the check box *Use Proxy for Accessing the Internet* and enter the appropriate specifications. Click *Accept* to perform the network setup. The installation procedure will continue with the add-on products or repositories setup as described in [Section 3.6.1, “Add-On Products”](#) (page 28).

## 3.7 Clock and Time Zone

In this dialog, select your region and time zone. Both are preselected according to the selected installation language. To change the preselected values, either use the map or the drop down lists for *Region* and *Time Zone*. When using the map, point the cursor at the rough direction of your region and left-click to zoom. Now choose your country or region by left-clicking. Right-click to return to the world map.

**Figure 3.4** *Clock and Time Zone*



To set up the clock, choose whether the *Hardware Clock is Set to UTC*. If you run another operating system on your machine, such as Microsoft Windows\*, it is likely your

system uses local time instead. If you only run Linux on your machine, set the hardware clock to UTC and have the switch from standard time to daylight saving time performed automatically.

If a network is already configured, you can configure time synchronization with an NTP server. Click *Change* to either alter the NTP settings or to *Manually* set the time. See Chapter 22, *Time Synchronization with NTP* (↑Administration Guide) for more information on configuring the NTP service. When finished, click *Accept* to continue the installation.

## 3.8 Create New User

Create a local user in this step. Administrating local users is a suitable option for stand-alone workstations. If setting up a client on a network with centralized user authentication, click *Change* and proceed with the [Section 3.8.1, “Expert Settings”](#) (page 32).

After entering the first name and last name, either accept the proposal or specify a new *Username* that will be used to log in. Finally, enter a password for the user. Reenter it for confirmation (to ensure that you did not type something else by mistake). To provide effective security, a password should be between five and eight characters long. The maximum length for a password is 72 characters. However, if no special security modules are loaded, only the first eight characters are used to discern the password. Passwords are case-sensitive. Special characters (7-bit ASCII) and the digits 0 to 9 are allowed. Other special characters like umlauts or accented characters are not allowed.

Passwords you enter are checked for weakness. When entering a password that is easy to guess, such as a dictionary word or a name, you will see a warning. It is a good security practice to use strong passwords.

---

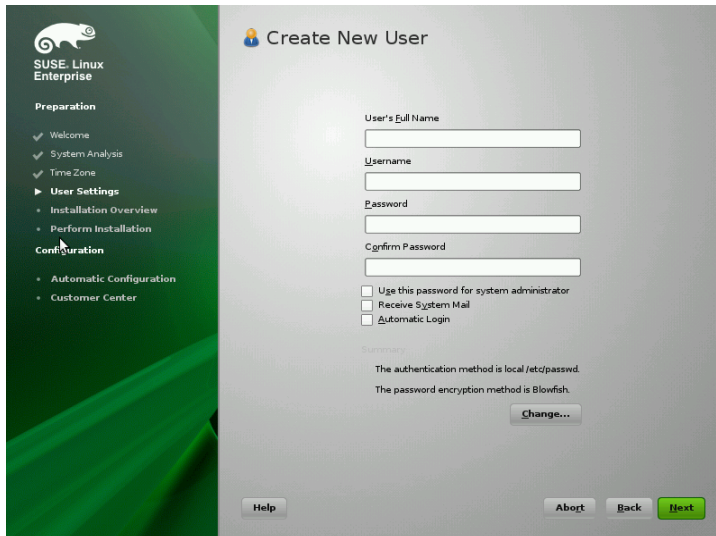
### **IMPORTANT: Username and Password**

Remember both your username and the password because they are needed each time you log in to the system.

---



**Figure 3.5** *Create New User*



Three additional options are available:

#### *Use this Password for the System Administrator*

If checked, the same password you have entered for the user will be used for the system administrator `root`. This option is suitable for stand-alone workstations or machines in a home network that are administrated by a single user. When not checked, you are prompted for a system administrator password in the next step of the installation workflow (see [Section 3.8.2, “Password for the System Administrator root”](#) (page 33)).

#### *Receive System Mail*

Checking this box sends messages created by the system services to the user. These are usually only sent to `root`, the system administrator. This option is useful for the most frequently used account, because it is highly recommended to log in as `root` only in special cases.

The mails sent by system services are stored in the local mailbox `/var/spool/mail/username`, where `username` is the login name of the selected user. To read e-mails after installation, you can use any e-mail client, for example KMail or Evolution.

### *Automatic Login*

This option automatically logs the current user in to the system when it starts. This is mainly useful if the computer is operated by only one user.

---

#### **WARNING: Automatic Login**

With the automatic login enabled, the system boots straight into your desktop with no authentication at all. If you store sensitive data on your system, you should not enable this option if the computer can also be accessed by others.

---

## **3.8.1 Expert Settings**

Click *Change* in the Create User dialog to set up network authentication or, if present, import users from a previous installation. Also change the password encryption type in this dialog.

You can also add additional user accounts or change the user authentication method in the installed system. For detailed information about user management, see [Chapter 9, \*Managing Users with YaST\*](#) (page 91).

The default authentication method is *Local (/etc/passwd)*. If a former version of SUSE Linux Enterprise Desktop or another system using `/etc/passwd` is detected, you may import local users. To do so, check *Read User Data from a Previous Installation* and click *Choose*. In the next dialog, select the users to import and finish with *OK*.

Access to the following network authentication services can be configured:

#### **LDAP**

Users are administered centrally on an LDAP server for all systems in the network. More information is available in Section “Configuring an LDAP Client with YaST” (Chapter 4, *LDAP—A Directory Service*, ↑Security Guide).

#### **NIS**

Users are administered centrally on a NIS server for all systems in the network. See Section “Configuring NIS Clients” (Chapter 3, *Using NIS*, ↑Security Guide) for more information.

Windows Domain

SMB authentication is often used in mixed Linux and Windows networks. and Section “Configuring a Linux Client for Active Directory” (Chapter 5, *Active Directory Support*, ↑Security Guide).

eDirectory LDAP

eDirectory authentication is used in Novell networks.

Along with user administration via *LDAP* and *NIS*, you can use Kerberos authentication. To use it, select *Set Up Kerberos Authentication*. For more information on Kerberos, refer to Chapter 6, *Network Authentication with Kerberos* (↑Security Guide).

## 3.8.2 Password for the System Administrator

### **root**

If you have not chosen *Use this Password for the System Administrator* in the previous step, you will be prompted to enter a Password for the System Administrator `root`. Otherwise this configuration step is skipped.

`root` is the name of the superuser, the administrator of the system. Unlike regular users, who may or may not have permission to do certain things on the system, `root` has unlimited power to do anything: change the system configuration, install programs, and set up new hardware. If users forget their passwords or have other problems with the system, `root` can help. The `root` account should only be used for system administration, maintenance, and repair. Logging in as `root` for daily work is rather risky: a single mistake could lead to irretrievable loss of system files.

For verification purposes, the password for `root` must be entered twice. Do not forget the `root` password. Once entered, this password cannot be retrieved.

The `root` can be changed any time later in the installed system. To do so run YaST and start *Security and Users > User and Group Management*.

---

## WARNING: The root User

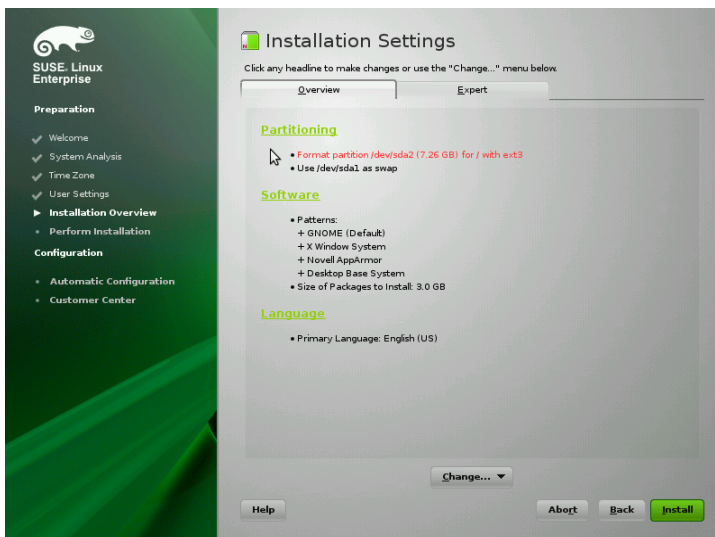
The user `root` has all the permissions needed to make changes to the system. To carry out such tasks, the `root` password is required. You cannot carry out any administrative tasks without this password.

---

## 3.9 Installation Settings

On the last step before the real installation takes place, you can alter installation settings suggested by YaST and also review the settings you made so far. Basic settings can be changed in the *Overview* tab, advanced options are available on the *Experts* tab. To modify the suggestions, either click *Change* and select the category to change or click on one of the headlines. After configuring any of the items presented in these dialogs, you are always returned to the Installation Settings window, which is updated accordingly.

**Figure 3.6** *Installation Settings*



---

**TIP: Restoring the Default Settings**

You can reset all changes to the defaults by clicking *Change > Reset to Defaults*. YaST then shows the original proposal again.

---

## 3.9.1 Partitioning (Overview)

Review and—if necessary—change the partition setup proposed by the system. Changing the partition setup either lets you partition a specific disk or, when choosing *Custom Partitioning*, apply your own partitioning scheme. Modifying the partition setup opens the Expert Partitioner described in [Section 12.1, “Using the YaST Partitioner”](#) (page 155).

## 3.9.2 Booting (Expert)

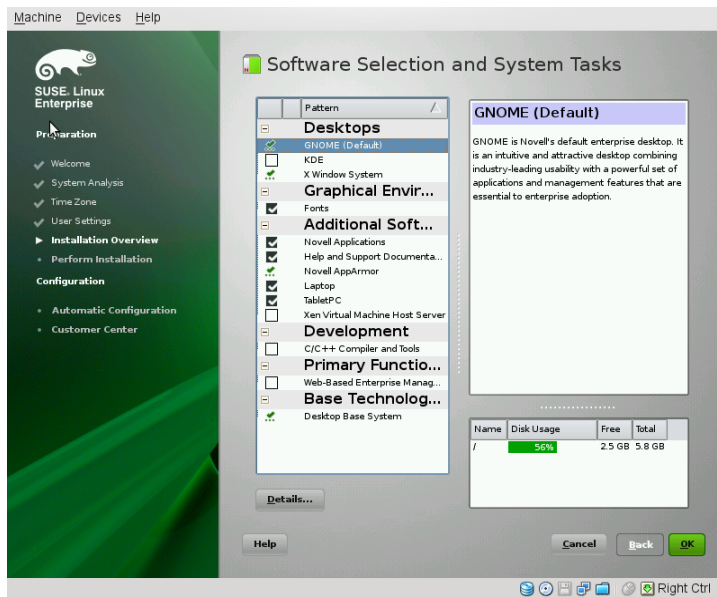
YaST proposes a boot configuration for your system. Other operating systems found on your computer, such as Microsoft Windows or other Linux installations, will automatically be detected and added to the boot loader. However, SUSE Linux Enterprise Desktop will be booted by default. Normally, you can leave these settings unchanged. If you need a custom setup, modify the proposal for your system. For information, see Section “Configuring the Boot Loader with YaST” (Chapter 10, *The Boot Loader GRUB*, ↑Administration Guide).

## 3.9.3 Software (Overview)

SUSE Linux Enterprise Desktop contains a number of software patterns for various application purposes. Click *Software* to start the pattern selection and modify the installation scope according to your needs. Select your pattern from the list and see a pattern description in the right part of the window. Each pattern contains a number of software packages needed for specific functions (e.g. Multimedia or Office software). For a more detailed selection based on software packages to install, select *Details* to switch to the YaST Software Manager.

You can also install additional software packages or remove software packages from your system at any later time with the YaST Software Manager. For more information, refer to [Chapter 6, \*Installing or Removing Software\*](#) (page 65).

**Figure 3.7** *Software Selection and System Tasks*



## 3.9.4 Language (Overview)

Here you can change the system *Language* you defined in the first step of the installation. It is also possible to add additional languages. To adjust the system language settings, select *Language*. Select a language from the list. The primary language is used as the system language. You can also adapt keyboard layout and time zone to the primary language if the current settings differ. *Details* lets you tune language settings for the user `root`, set UTF-8 support, or further specify the language (e.g. select South African English).

Choose secondary languages to be able to switch to one of these languages at any time without having to install additional packages. For more information, see [Chapter 10, Changing Language and Country Settings with YaST](#) (page 109).

### 3.9.5 *Add-On Products* (Expert)

If you added a source for an add-on media earlier, it appears here. Add, remove, or modify add-on products here if needed. This is the same configuration dialog as discussed earlier in [Section 3.6.1, “Add-On Products”](#) (page 28).

### 3.9.6 *Keyboard Layout* (Expert)

To change the keyboard layout, select *Keyboard Layout*. By default, the layout corresponds to the language chosen for installation. Select the keyboard layout from the list. Use the *Test* field at the bottom of the dialog to check if you can enter special characters of that layout correctly. Options to fine-tune various settings are available under *Expert Mode*. Find more information about changing the keyboard layout in [Section 5.3, “Setting Up Keyboard and Mouse”](#) (page 53). When finished, click *Accept* to return to the installation summary.

### 3.9.7 *Time Zone* (Expert)

Adjust time zone and clock settings here. Provided a network is configured, you can also set up a Network Time Protocol (NTP) client that automatically synchronizes your computer with a time server. This is the same configuration as shown earlier in [Section 3.7, “Clock and Time Zone”](#) (page 29).

### 3.9.8 *Default Runlevel* (Expert)

SUSE Linux Enterprise Desktop can boot to different runlevels. Normally, there should be no need to change anything here, but if necessary set the default runlevel with this dialog. Refer to [Section “Configuring System Services \(Runlevel\) with YaST”](#) (Chapter 9, *Booting and Configuring a Linux System*, ↑Administration Guide) for more information about runlevel configuration.

### 3.9.9 *System* (Expert)

This dialog presents all the hardware information YaST could obtain about your computer. When called, the hardware detection routine is started. Depending on your system,

this may take some time. Select any item in the list and click *Details* to see detailed information about the selected item. Use *Save to File* to save a detailed list to either the local file system or a floppy. Advanced users can also change the PCI ID setup and Kernel Settings by choosing *System Settings*.

## 3.10 Performing the Installation

After making all installation settings, click *Install* in the Installation Settings window to start the installation. Some software may require a license confirmation. If your software selection includes such software, license confirmation dialogs are displayed. Click *Accept* to install the software package. When not agreeing to the license, click *I Disagree* and the software package will not be installed. In the dialog that follows, confirm with *Install* again.

The installation usually takes between 15 and 30 minutes, depending on the system performance and the selected software scope. After having prepared the hard disk and having saved and restored the user settings, the software installation starts. During this procedure a slide show introduces the features of SUSE Linux Enterprise Desktop. Choose *Details* to switch to the installation log.

After the software installation has completed, the basic system is set up. Among others, “Finishing the Basic Installation” includes installing the boot manager, initializing fonts and more. Next YaST boots into the new Linux system to start the system configuration.

---

### **TIP: Existing SSH Host Keys**

If you install SUSE Linux Enterprise Desktop on a machine with existing Linux installations, the installation routine automatically imports the SSH host key with the most recent access time from an existing installation.

---

## 3.11 Configuration of the Installed System

The system is now installed, but not yet configured for use. The hardware, the network and other services are not set up, yet. If you follow the default installation path, the



system will be automatically configured. If you have deselected the *Automatic Configuration*, the manual system configuration starts.

### 3.11.1 Automatic System Configuration

Having rebooted, the system starts the Automatic Configuration. This routine attempts to configure your network and Internet access and sets up your hardware. The whole process does not need any interaction. You can change the settings made by the Automatic Configuration at any time in the installed system with YaST. Continue with [Section “Novell Customer Center Configuration”](#) (page 42).

### 3.11.2 Manual System Configuration

Having rebooted, the system starts the manual configuration. If the configuration fails at one of the steps of this stage, it restarts and continues from the last successful step.

#### Hostname and Domain Name

The hostname is the computer's name in the network. The domain name is the name of the network. A hostname and domain are proposed by default. If your system is part of a network, the hostname has to be unique in this network, whereas the domain name has to be common to all hosts on the network.

In many networks, the system receives its name over DHCP. In this case it is not necessary to modify the proposed hostname and domain name. Select *Change Hostname via DHCP* instead. To be able to access your system using this hostname, even when it is not connected to the network, select *Write Hostname to /etc/hosts*. If you often change networks without restarting the desktop environment (e.g. when switching between different WLANs), do not enable this option, because the desktop system may get confused when the hostname in `/etc/hosts` changes.

To change hostname settings at any time after installation, use YaST *Network Devices > Network Settings*. For more information, see Section “Configuring the Network Card with YaST” (Chapter 19, *Basic Networking*, ↑Administration Guide).

# Network Configuration

If you are installing SUSE Linux Enterprise Desktop on a laptop computer, *Interfaces Controlled by NetworkManager* is enabled. NetworkManager is a tool that enables automatic connection with minimal user intervention. It is ideal for WLAN and mobile computing. If you want to use the traditional method without NetworkManager, click *Disable NetworkManager*. Find detailed information about NetworkManager in Chapter 23, *Using NetworkManager* (↑Administration Guide). If you are installing SUSE Linux Enterprise Desktop on any other type of machine, the traditional method without NetworkManager is selected by default. This configuration step also lets you configure the network devices of your system and make security settings, for example, for a firewall or proxy.

The network can also be configured after the system installation has been completed. If you skip it now, your system is left offline unable to retrieve any available updates. To configure your network connection later, select *Skip Configuration* and click *Next*.

The following network settings can be configured in this step:

## *General Network Settings*

Enable or disable the use of NetworkManager as described above. Also change the IPv6 support here. By default the IPv6 support is enabled. To disable it, click *Disable IPv6*. For more information about IPv6, see Section “IPv6—The Next Generation Internet” (Chapter 19, *Basic Networking*, ↑Administration Guide).

## *Firewall*

By default SuSEfirewall2 is enabled on all configured network interfaces. To globally disable the firewall for this computer, click on *Disable*. If the firewall is enabled, you may *Open* the SSH port in order to allow remote connections via secure shell. To open the detailed firewall configuration dialog, click on *Firewall*. See Section “Configuring the Firewall with YaST” (Chapter 15, *Masquerading and Firewalls*, ↑Security Guide) for detailed information.

## *Network Interfaces*

All network cards detected by YaST are listed here. If you have already set up a network connection during the installation (as described in [Section “Network Setup”](#) (page 28)) the card used for this connection is listed as *Configured*. A click on *Network Interfaces* opens the *Network Settings* dialog, where you can change existing configurations, set up networks cards not configured yet, or add and configure additional cards. See [Section 8.2, “Internet Connection Via Network”](#) (page 90)

for checklists of configuration requirements for the various connection types and Section “Configuring the Network Card with YaST” (Chapter 19, *Basic Networking*, ↑Administration Guide) for configuration details.

### *DSL Connections, ISDN Adapters, and Modems*

If your computer is equipped with an internal DSL modem, an internal ADSL Fritz Card, an ISDN card or a modem, clicking on the respective headline opens the configuration dialog. Refer to [Chapter 8, \*Accessing the Internet\*](#) (page 87) for further information.

### VNC Remote Administration

To enable remote administration of your machine via VNC, click *VNC Remote Administration*. Choose *Allow Remote Administration* in the following dialog and adjust your firewall settings accordingly.

### Proxy

If you have a proxy server controlling the Internet access in your network, configure the proxy URLs and authentication details in this dialog.

---

### **TIP: Resetting the Network Configuration to the Default Values**

Reset the network settings to the original proposed values by clicking *Change > Reset to Defaults*. This discards any changes made.

---

## **Test Internet Connection**

After having configured a network connection, you can test it. For this purpose, YaST establishes a connection to the SUSE Linux Enterprise Desktop server and downloads the latest release notes. Read them at the end of the installation process. A successful test is also a prerequisite for registering and updating online.

If you have multiple network interfaces, verify that the desired card is used to connect to the Internet. If not, click *Change Device*.

To start the test, select *Yes, Test Connection to the Internet* and click *Next*. In the next dialog, view the progress of the test and the results. Detailed information about the test process is available via *View Logs*. If the test fails, click *Back* to return to the network configuration to correct your entries.

If you do not want to test the connection at this point, select *No, Skip This Test* then *Next*. This also skips downloading the release notes, configuring the customer center, and updating online. These steps can be performed any time after the system has been initially configured.

## Novell Customer Center Configuration

To get technical support and product updates, you need to register and activate your product with the Novell Customer Center. The *Novell Customer Center Configuration* provides assistance for doing so. Find detailed information about Novell Customer Center at <http://www.novell.com/documentation/ncc/>.

If you are offline or want to skip this step, select *Configure Later*. This also skips SUSE Linux Enterprise Desktop's online update.

In *Include for Convenience*, select whether to send unsolicited additional information, such as your *Hardware Profile* or *Optional Information* when registering. This simplifies the registration process. Click on *Details* to get in-depth information about how the data will be collected. In order to obtain information about which data will be sent for your specific product, the Novell server will be connected. Upon this initial connect no data other than the ID of your product will be send to the Novell servers.

In order to become entitled for support, make sure to check *Registration Code*. You will be prompted to enter the code when proceeding with *Next*. Find more information about the technical support at [http://www.novell.com/products/desktop/services\\_support.html](http://www.novell.com/products/desktop/services_support.html).

---

### NOTE: Data Privacy

No information is passed to anyone outside Novell. The data is used for statistical purposes and to enhancer your convenience regarding driver support and your Web account. Find a link to the detailed privacy policy by clicking on *Details*. View the information transmitted in the log file at `/root/.suse_register.log`.

---

Apart from activating and registering your product, this module also adds the official update repositories to your configuration. These repositories provide fixes for known bugs or security issues which can be installed via an online update.

To keep your repositories valid, select *Regularly Synchronize with Customer Center*. This option checks your repositories and adds newly available catalogs or removes obsolete ones. It does not touch manually added repositories.

In addition to the update repositories, two more catalogs with official drivers for ATI and NVidia graphics cards are added. SUSE Linux Enterprise Desktop ships with open source drivers for these cards, but the official drivers, provided directly by the graphics cards manufacturers, offer additional functionality. In order to add these repositories, you need to import their public GnuPG keys—these keys are used to ensure the repositories is provided by the owner of the catalog. Click *Trust Key* and then *Import* to add the catalog. Click *Skip package* and then *Abort* to prevent this specific repository from being added to your configuration.

To keep your repositories valid, select *Regularly Synchronize with Customer Center*. This option checks your repositories and adds newly available catalogs or removes obsolete ones. It does not touch manually added repositories.

Proceed with *Next*. A connection with the Novell server is established. Follow the on-screen instructions to finish the registration.

## Local Registration Server

If your organization provides a local registration server instead of using the Novell Customer Center, you need to specify the server's URL. Client and server communicate solely via HTTPS protocol, therefore you also need to enter a path to the server's certificate if the certificate was not issued by a certificate authority. Open the dialog with *Advanced > Local Registration Server*

### Registration Server

URL of the registration server. The URL has a fixed format

`https://FQN/center/regsvc/` *FQN* has to be full qualified hostname of the registration server. Example:

`https://smt.example.com/center/regsvc/`

### Server CA certificate location

Location of the registration server's certificate. Specify one of the following locations:

## URL

Remote location (http, https or ftp) from which the certificate can be downloaded. Example:

```
http://smt.example.com/smt-ca.crt
```

## Floppy

Specifies a location on a floppy. The floppy has to be inserted before proceeding. The value has to start with the string `floppy` followed by the path to the certificate. Example:

```
floppy/smt/smt-ca.crt
```

## local path

Absolute path to the certificate on the local machine. Example:

```
/data/inst/smt/smt-ca.crt
```

## Interactive

Use `ask` to open a pop-up menu where you can specify the path to the certificate. Do not use this option with AutoYaST. Example

```
ask
```

## Deactivate certificate installation

Use `done` if either the certificate will be installed by an add-on product, or if you are using a certificate issued by an official certificate authority. Example:

```
done
```

# Online Update

If the *Registration* was successful, and updates are available, select whether to perform a YaST online update. If there are any patched packages available on the servers, download and install them now to fix known bugs or security issues. For detailed instructions see Chapter 1, *YaST Online Update* (↑Administration Guide). Directives on how to perform an online update in the installed system are available at [Section 6.5, “Keeping the System Up-to-date”](#) (page 77) or Chapter 1, *YaST Online Update* (↑Administration Guide). This step is skipped if no updates are available or if you haven't registered.

## New Local User

In addition to the user created in part one of the installation, you can create an additional user in this dialog. To create more users, manage groups, modify defaults for new users and set up network authentication, launch the *User Management*. Refer to [Chapter 9, \*Managing Users with YaST\*](#) (page 91) for more information about user management. To skip this step, just click *Next* without entering any data.

## Release Notes

After completing the user authentication setup, YaST displays the release notes. Reading them is recommended, because they contain important up-to-date information which was not available when the manuals were printed. If you successfully tested the Internet connection, read the most recent version of the release notes, as fetched from SUSE Linux Enterprise Desktop's servers. Use *Miscellaneous > Release Notes* in YaST or start the SUSE Help Center to view the release notes after installation.

## Hardware Configuration

At the end of the installation, YaST opens a dialog for the configuration of the graphics card and other hardware components connected to the system, such as printers or sound cards. Click the individual components to start the hardware configuration. For the most part, YaST detects and configures the devices automatically.

You can skip any peripheral devices and configure them later, as described in [Chapter 5, \*Setting Up Hardware Components with YaST\*](#) (page 51). To skip the configuration, select *Skip Configuration* and click *Next*.

However, when setting up a desktop system you should configure the graphics card right away. Although the display settings as configured by YaST should be generally acceptable, most users have very strong preferences as far as resolution, color depth, and other graphics features are concerned. To change these settings, select the respective item and set the values as desired.

---

### TIP: Resetting Hardware Configuration to the Default Values

You can cancel any changes to the hardware configuration by clicking *Change > Reset to Defaults*. YaST then shows the original proposal again.

---

## Installation Completed

After a successful installation, YaST shows the Installation Completed dialog. In this dialog, select whether to clone your newly installed system for AutoYaST. To clone your system, select *Clone This System for AutoYaST*. The profile of the current system is stored in `/root/autoyast.xml`.

AutoYaST is a system for installing one or more SUSE Linux Enterprise Desktop systems automatically without user intervention. AutoYaST installations are performed using a control file with installation and configuration data. Finish the installation of SUSE Linux Enterprise Desktop with *Finish* in the final dialog.

## 3.12 Graphical Login

SUSE Linux Enterprise Desktop is now fully installed and configured. Unless you enabled the automatic login function or customized the default runlevel, you should see the graphical login on your screen in which to enter a username and password to log in to the system. On single user systems with automatic login enabled, the desktop starts automatically.

For a short introduction to the KDE or GNOME desktop environments, refer to the GNOME Quick Start (↑GNOME Quick Start) and the KDE Quick Start (↑KDE Quick Start). Find detailed information about both desktop environments and about the applications to run on KDE or GNOME in the KDE User Guide (↑KDE User Guide) and the GNOME User Guide (↑GNOME User Guide).



# Updating SUSE Linux Enterprise

SUSE® Linux Enterprise provides the option of updating an existing system to the new version without completely reinstalling it. No new installation is needed. Old data, such as home directories and system configuration, is kept intact. During the life cycle of the product, you can apply Service Packs to increase system security and correct software defects. Install from a local CD or DVD drive or from a central network installation source.

## 4.1 Updating SUSE Linux Enterprise

Follow the steps outlined in this section, if you want to update from SUSE Linux Enterprise Desktop 10 to SUSE Linux Enterprise Desktop 11, for example. Make sure you update the old system to the most recent patch level first—at the moment, that is SP2.

Software tends to “grow” from version to version. Therefore, take a look at the available partition space with `df` before updating. If you suspect you are running short of disk space, secure your data before updating and repartition your system. There is no general rule of thumb regarding how much space each partition should have. Space requirements depend on your particular partitioning profile and the software selected.

### 4.1.1 Preparations

Before updating, copy the old configuration files to a separate medium, such as tape device, removable hard disk, USB stick, or ZIP drive, to secure the data. This primarily applies to files stored in `/etc` as well as some of the directories and files in `/var` and

/opt. You may also want to write the user data in /home (the HOME directories) to a backup medium. Back up this data as root. Only root has read permission for all local files.

Before starting your update, make note of the root partition. The command `df /` lists the device name of the root partition. In [Example 4.1, “List with df -h”](#) (page 48), the root partition to write down is /dev/sda3 (mounted as /).

**Example 4.1** *List with df -h*

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda3	74G	22G	53G	29%	/
tmpfs	506M	0	506M	0%	/dev/shm
/dev/sda5	116G	5.8G	111G	5%	/home
/dev/sda1	39G	1.6G	37G	4%	/windows/C
/dev/sda2	4.6G	2.6G	2.1G	57%	/windows/D

## 4.1.2 Possible Problems

If you update a default system from the previous version to this version, YaST works out necessary changes and performs them. Depending on your customizations, some steps or the entire update procedure may fail and you must resort to copying back your backup data. Check the following issues before starting the system update.

### Checking passwd and group in /etc

Before updating the system, make sure that /etc/passwd and /etc/group do not contain any syntax errors. For this purpose, start the verification utilities `pwck` and `grpck` as root and eliminate any reported errors.

### PostgreSQL

Before updating PostgreSQL (`postgres`), dump the databases. See the manual page of `pg_dump`. This is only necessary if you actually used PostgreSQL prior to your update.

## 4.1.3 Updating with YaST

Following the preparation procedure outlined in [Section 4.1.1, “Preparations”](#) (page 47), you can now update your system:

- 1 Optionally, prepare an installation server. For background information, see [Section 11.2.1, “Setting Up an Installation Server Using YaST”](#) (page 126).
- 2 Boot the system as for the installation, described in [Section 3.3, “System Start-Up for Installation”](#) (page 20). In YaST, choose a language and select *Update* in the *Installation Mode* dialog. Do not select *New Installation*.
- 3 YaST determines whether there are multiple root partitions. If there is only one, continue with the next step. If there are several, select the right partition and confirm with *Next* (`/dev/sda3` was selected in the example in [Section 4.1.1, “Preparations”](#) (page 47)). YaST reads the old `fstab` on this partition to analyze and mount the file systems listed there.
- 4 In the *Installation Settings* dialog, adjust the settings according to your requirements. Normally, you can leave the default settings untouched, but if you intend to enhance your system, check the packages offered in the *Software Selection* submenus or add support for additional languages.
  - 4a Click *Update Options* to update only software that is already installed (*Only Update Installed Packages*) or to add new software and features to the system according to selected patterns. It is advisable to accept the suggestion. You can adjust it later with YaST.
  - 4b You also have the possibility to make backups (*Backup*) of various system components. Selecting backups slows down the update process. Use this option if you do not have a recent system backup.
- 5 Click *Accept* and confirm *Start Update* to start the software installation process.

At the end of the installation read the release notes and then click *Finish* to restart the computer and log in.

## 4.2 Installing Service Packs

Use Service Packs to update a SUSE Linux Enterprise installation. There are several different ways in which you can apply a Service Pack. You can either update the existing installation or start a whole new installation using the Service Pack media. Possible scenarios for updating the system and setting up a central network installation source are described here.

---

**TIP: Installation Changes**

Read the installation instructions on the Service Pack media for further changes.

---

## 4.3 Software Changes from Version 10 to Version 11

---

**NOTE: Software Changes from SLES 10 to SLES 11**

For a detailed list of software and configuration changes from SUSE Linux Enterprise Server 10 to SUSE Linux Enterprise Server 11, refer to the release notes . View them in the installed system using the YaST release notes module.

---

# Setting Up Hardware Components with YaST

YaST allows you to configure hardware items at installation time as well as in the installed system. Configure additional graphics cards and monitors, adjust mouse and keyboard settings and configure sound hardware. If you need printer or scanner support, use the appropriate YaST modules to configure these hardware items. Learn which hardware components are connected to your computer by using the YaST Hardware Information module.

## 5.1 Probing Your Hardware

Use YaST, if you want to know more about your hardware or if you need to find out details like vendor and model of a certain hardware to be able to properly configure it. Here and in the following sections we assume that you already started YaST (for example, by pressing `Alt + F2` and entering `kdesu yast2 (KDE)` or `gnomesu yast2 (GNOME)` followed by the root password, because YaST needs system administrator permissions to change the system files):

- 1 In YaST click *Hardware > Hardware Information*. Hardware probing starts immediately and it will take some time until you see the hardware information tree in a separate window.
- 2 In the hardware information tree recursively click on the plus icons to expand the information about a specific device.
- 3 Click *Close* to leave the hardware information overview.

## 5.2 Setting Up Graphics Card and Monitor

After the installation you can change the configuration of your graphics system (graphics card and monitor) according to your needs. Such a change can be necessary because of accessibility issues or hardware upgrades.

---

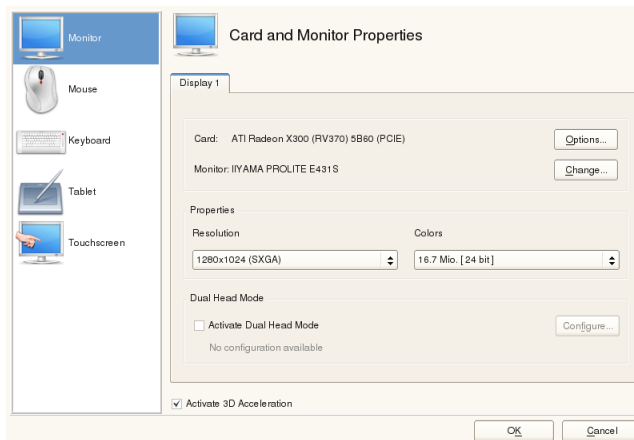
### WARNING: Changing Monitor Frequencies

Although there are safety mechanisms, you should still be very careful when manually changing the allowed monitor frequencies. Incorrect values might destroy your monitor. Always refer to the monitor's manual before changing frequencies.

---

Change the resolution, if fonts are too small or if circles appear misshapen. Proceed as follows:

- 1 In YaST, click *Hardware > Graphics Card and Monitor*. SaX2 checks the system resources and displays a window.
- 2 Make sure the monitor is properly detected. If not, use *Change* to select the appropriate model from the list.
- 3 Select an appropriate *Resolution* and *Colors*, if necessary.



- 4 Test the new configuration before it is applied to the system. Click *Ok* to decide what to do with your configuration (*Test*, *Save*, or *Cancel*.)

To activate a second monitor, proceed as follows:

- 1 In YaST, click *Hardware > Graphics Card and Monitor*. SaX2 checks the system resources and displays the *Card and Monitor Properties* dialog.
- 2 Make sure the monitor is properly detected. If not, use *Change* to select the appropriate model from the list.
- 3 Enable *Activate Dual Head Mode* and click *Configure* for further tuning.
- 4 Make sure the second monitor is properly detected. If not, use *Change* to select the appropriate model from the list.
- 5 Decide whether you want to use the second monitor in *Cloned Multihead* or in *Xinerama Multihead* mode and click *Ok*.
- 6 Test the new configuration before it is applied to the system. Click *Ok* to decide what to do with your configuration (*Test*, *Save*, or *Cancel*.)

---

**NOTE: Restarting the X Server**

Any changes you make here take effect only after you restart the X server. If you want to restart the X server now, log out from the graphical system and log in again.

---

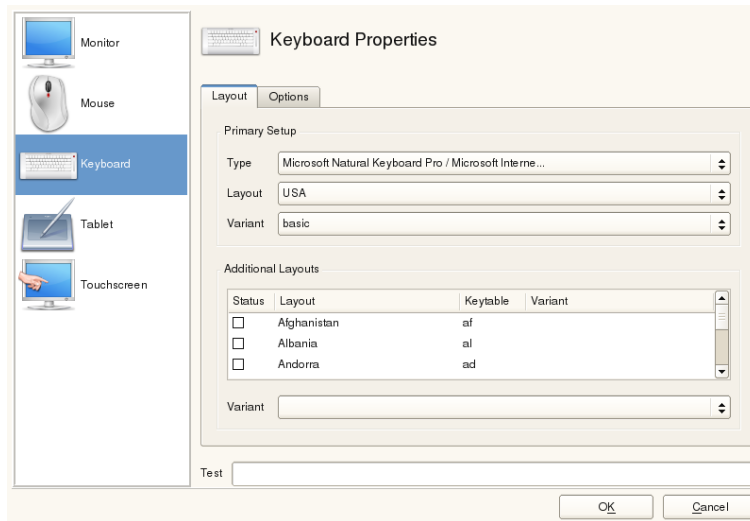
## 5.3 Setting Up Keyboard and Mouse

Reconfigure input devices such as the keyboard or the mouse, or add more than one of these devices using the YaST Keyboard and Mouse modules.

### 5.3.1 Keyboard Layout

In case you want to replace a standard 104-key keyboard with a multimedia keyboard or use a different language or country layout, proceed as follows:

- 1 In YaST, click *Hardware > Keyboard Layout*. The SaX2 configuration tool reads the system resources and displays the *Keyboard Properties* dialog.



- 2 Select your keyboard model from the *Type* list.
- 3 Select the country in the *Layout* list.
- 4 Depending on the country layout, you can choose a certain *Variant*. The selections are applied immediately for testing.
- 5 As an option you can enable *Additional Layouts*. Check one or more boxes in the list. This feature is handy if you want to switch between different languages or scripts in the running system without the need for reconfiguration.
- 6 Before saving the configuration, use the *Test* field at the bottom of the dialog to check if special characters like umlauts and accented characters can be entered and displayed correctly.
- 7 Click *OK* to leave the configuration dialog and in the following message click *Save* to apply your changes.



---

**NOTE: Configuring Console Keyboard Layout**

By clicking the *Save* button as described in **Step 7** (page 54) the setup of the console keyboard layout takes place at the same time. If you want to change the console keyboard layout, either call `yast keyboard` (the text mode interface) or check the `KEYTABLE` and `YAST_KEYBOARD` settings in `/etc/sysconfig/keyboard`.

---

## 5.3.2 Mouse Model

The mouse is usually detected automatically, but you can set up your mouse model manually if the automatic detection fails. Refer to the documentation of your mouse for a description of the model. If you want to modify your mouse configuration, proceed as follows:

- 1 In YaST, click *Hardware > Mouse Model*. The SaX2 configuration tool reads the system resources and displays the *Mouse Properties* dialog.
- 2 Click *Change* and select your mouse model from the list displayed.
- 3 Click *OK* to leave the configuration dialog and apply your changes with *Save*.

In the *Options* part of the dialog, set various options for operating your mouse.

### *Activate 3-Button Emulation*

If your mouse has only two buttons, a third button is emulated whenever you click both buttons simultaneously.

### *Activate Mouse Wheel*

Check this box to use a scroll wheel.

### *Invert X-Axis / Invert Y-Axis*

Check these options if you want to change the direction in which the mouse pointer moves.

### *Activate Left-Hand Button Mapping*

Check this box to make the button mapping suitable for left-hand usage.

### *Emulate Wheel with Mouse Button*

If your mouse does not have a scroll wheel but you want to use a similar functionality, you can assign an additional button for this. Select the button to use. While pressing this button, any movement of the mouse is translated into scroll wheel commands. This feature is especially useful with trackballs.

## 5.4 Setting Up Sound Cards

Most sound cards are detected automatically and configured with reasonable values. In YaST, use *Hardware > Sound* if you want to add a problematic sound card that could not be configured automatically or change the default settings. It is also possible to set up additional sound cards or switch their sequence.

---

### **TIP: Probing for Old Sound Chips**

If you know a legacy sound board is installed in your computer, let YaST probe for old chips, if YaST cannot find a sound board. Within the pop-up click *Yes, probe*.

---

If YaST cannot detect your sound card automatically, proceed as follows:

- 1 Click *Add* to open a dialog in which to select a sound card vendor and model. Refer to your sound card documentation for the information required. Find a reference list of sound cards supported by ALSA with their corresponding sound modules in `/usr/share/doc/packages/alsa/cards.txt` and at <http://www.alsa-project.org/alsa-doc/>.

Make your choice and click *Next*.

- 2 In the *Sound Card Configuration* dialog, choose the configuration level in the first setup screen:

#### *Quick automatic setup*

You are not required to go through any of the further configuration steps and no sound test is performed. The sound card is configured automatically.

#### *Normal setup*

Adjust the output volume and play a test sound.

### *Advanced setup with possibility to change options*

Customize all settings manually.

Click *Next* to continue.

- 3** In *Sound Card Volume*, test your sound configuration and make adjustments to the volume. You should start at about ten percent to avoid damage to your hearing or the speakers. A test sound should be audible when you click *Test*. If you cannot hear anything, increase the volume. Press *Next* > *Finish* to complete the sound configuration.

If you want to change the configuration of a sound card, go to the *Sound Configuration* dialog, select a displayed *Card Model* and click *Edit*. Use *Delete* to remove a sound card altogether.

Click the *Other* popup menu to customize one of the following options manually:

#### *Volume...*

Use this dialog is for setting the volume.

#### *Play Test Sound*

Use this option for testing the sound system.

#### *Start Sequencer*

For playback of MIDI files, check this option.

#### *Set as the Primary Card*

Click *Set as the Primary Card* if you want to adjust the sequence of your sound cards. The sound device with index 0 is the default device and thus used by the system and the applications.

#### *PulseAudio Configuration...*

Enter this dialog if you want to disable the PulseAudio sound system because you want to use something else system-wide.

The volume and configuration of all sound cards installed are saved when you click *Finish*. The mixer settings are saved to the file `/etc/asound.conf` and the ALSA configuration data is appended to the end of the files `/etc/modprobe.d/sound` and `/etc/sysconfig/hardware`.

## 5.5 Setting Up a Printer

YaST can be used to configure a local printer that is directly connected to your machine (normally with USB or parallel port) and to set up printing with network printers. It is also possible to share printers over the network and to add 3rd party “drivers” (PostScript Printer Description (PPD) files). Further information about printing (concepts, technical details, and troubleshooting) is available in Chapter 12, *Printer Operation* (↑Administration Guide).

In YaST, click *Hardware > Printer* to start the printer module. By default it opens in the *Printer Configurations* view, displaying a list of all printers available and configured. This is especially useful when having access to a lot of printers via the network. From here you can also *Print a Test Page* on the selected printer and configure local printers.

### 5.5.1 Configuring Local Printers

If an unconfigured local printer is detected, YaST starts automatically to configure it. YaST can configure the printer automatically if the parallel or USB port can be set up automatically and the connected printer can be detected. The printer model must also be listed in the database used during the automatic hardware detection.

If the printer model is unknown or cannot be automatically detected, configure it manually. There are two possible reasons why a printer is not automatically detected:

- The printer does not identify itself correctly. This may apply to very old devices. Try to configure your printer as described in [Section “Configuring Manually”](#) (page 58).
- If the manual configuration does not work, communication between printer and computer is not possible. Check the cable and the plugs to make sure that the printer is properly connected. If this is the case, the problem may not be printer-related, but rather a USB or parallel port-related problem.

### Configuring Manually

To manually configure the printer, select *Add* in the *Printer Configurations* view. YaST will load a list of printer drivers—this may take some time. Use the *Connection Wizard*

to specify how the printer is connected to the machine. Then choose a suitable driver and specify a unique name for the printer queue in the *Set Name* field.

A printer is never used directly, but always through a printer queue. This ensures that simultaneous jobs can be queued and processed one after the other. Each printer queue is assigned to a specific driver, and a printer can have multiple queues. This makes it possible to set up a second queue on a color printer, that prints black only, for example. Refer to Section “The Workflow of the Printing System” (Chapter 12, *Printer Operation*, ↑Administration Guide) for more information about print queues.

For many printer models, several drivers are available. When configuring the printer, YaST defaults to the one marked `recommended` as a general rule. Normally it is necessary to change the driver—the `recommended` one should produce the best results. However, if you want a color printer to print only in black and white, it is most convenient to use a driver that does not support color printing, for example. If you experience performance problems with a PostScript printer when printing graphics, it may help to switch from a PostScript driver to a PCL driver (provided your printer understands PCL).

If no driver for your printer is listed, you can try to select a generic driver with an appropriate standard language from the list. Refer to your printer's documentation to find out which language (the set of commands controlling the printer) your printer understands. If this does not work, refer to [Section “Adding Drivers with YaST”](#) (page 59) for another possible solution.

The printer is now configured with the default settings and ready to use. Click *Finish Add* to return to the *Printer Configurations* view. The newly configured printer is now visible in the printers list.

## Adding Drivers with YaST

If your printer does not appear in the *Assign Drivers* dialog when adding a new printer, the PPD (PostScript Printer Description) file for your model is not available. For more information about PPD files, refer to Section “Installing the Software” (Chapter 12, *Printer Operation*, ↑Administration Guide). To manually add a PPD file from the local file system or an FTP or HTTP server, choose *Add Driver*.

Get PPD files directly from your printer vendor or from the driver CD of the printer. For details, see Section “No Suitable PPD File Available for a PostScript Printer” (Chapter 12, *Printer Operation*, ↑Administration Guide). Alternatively, you can also

find PPD files at <http://www.linuxfoundation.org/en/OpenPrinting/>, the “OpenPrinting.org printer database”. When downloading PPD files from OpenPrinting.org, keep in mind that it always shows the latest Linux support status, which is not necessarily met by SUSE Linux Enterprise Desktop.

## Fine-tuning a Local Printer Configuration

In order to adjust the default settings for paper size, resolution, media source and others, choose a printer from the list in the *Printer Configurations* view and click *Configure*. In the window for modifying the respective printer queue, you can make detailed adjustments by opening *All options for the Current Driver*. If you have access to more than one printer queue, you can specify whether this should be the *Default Printer*. You may also alter the generic printer *Description* and the *Location* description here.

For many printer models, several drivers are available. When configuring the printer, YaST defaults to the one marked *recommended* as a general rule. See the *Driver* section in the dialog for all drivers available. The one that is currently chosen is marked as *Current Driver*.

Normally it is not necessary to change the driver—the one chosen by YaST should produce the best results. However, if you want a color printer to print only in black and white, it is most convenient to use a driver that does not support color printing, for example. If you experience performance problems with a PostScript printer when printing graphics, it may help to switch from a PostScript driver to a PCL driver (provided your printer understands PCL).

## 5.5.2 Configuring Printing via the Network with YaST

Network printers are not detected automatically. They must be configured manually using the YaST printer module. Depending on your network setup, you can print to a print server (CUPS, LPD, SMB, or IPX) or directly to a network printer (preferably via TCP). Access the configuration view for network printing by choosing *Printing via Network* from the left pane in the YaST printer module.

## Using CUPS

In a Linux environment CUPS is usually used to print via the network. The simplest setup is to only print via a single CUPS server which can directly be accessed by all clients. Check *Do All Your Printing Directly via One Remote CUPS Server* and specify the name or IP address of the server. Click *Test the Server* to make sure you have chosen the correct name/IP address. Leave with *OK*.

If you print via more than one CUPS server, check *Receive Printer Information from remote CUPS Servers*. Specify, whether you want to listen to servers in all networks available, to servers in your local network, or to specific IP addresses. This setup needs a running local CUPS daemon that communicates with the remote CUPS servers. Therefore answer *Yes* when asked to start a local CUPS daemon.

## Using Print Servers other than CUPS

If your network offers print services via print servers other than CUPS, start the *Connection Wizard* and choose the appropriate *Connection* type. Ask your network administrator for details on configuring a network printer in your environment.

### 5.5.3 Sharing Printers Over the Network

Printers managed by a local CUPS daemon can be shared over the network and so turn your machine into a CUPS server. Usually you share a printer by enabling CUPS' so called “browsing mode”. If browsing is enabled, the local printer queues are made available on the network for listening remote CUPS daemons. It is also possible to set up a dedicated CUPS server, that manages all printing queues and can directly be accessed by remote clients. In this case it is not necessary to enable browsing.

To share your printer, open the *Share Printers* view in the YaST printer module. Select *Allow Remote Access* and configure your CUPS daemon to be accessible *For Computers Within the Local Network*. To enable the browsing mode, also check *Publish Printers by Default Within the Local Network*. Then specify the network interface(s) that should be used by the CUPS server. If you enable more than one interface, you can also enable or disable the browsing mode on a per interface base. Apply the settings with *OK* and allow to restart the CUPS server.

## 5.6 Setting Up a Scanner

You can configure a USB or SCSI scanner at any time using YaST. The `sane-backends` package contains hardware drivers and other essentials needed to use a scanner. Scanners connected to a parallel port must be configured manually. If you own a HP All-In-One device, see [Section 5.6.1, “Configuring an HP All-In-One Device”](#) (page 62), instructions on how to configure a network scanner are available at [Section 5.6.3, “Scanning over the Network”](#) (page 63).

Connect your USB or SCSI scanner to your computer and turn it on. Start YaST and select *Hardware > Scanner*. YaST builds the scanner database and tries to detect your scanner model automatically. If your scanner is detected correctly, and can be tested with *Other > Test*. Leave the configuration menu with *Finish*.

If a USB/SCSI scanner is not properly detected, try *Other > Restart Detection* first. If that does not help, or if your scanner is connected to the parallel port, configure it manually by clicking *Add* and choosing a scanner from the list. Use *Other > Test* to make sure you have chosen the correct driver.

### 5.6.1 Configuring an HP All-In-One Device

HP All-In-One device can be configured with YaST even if they are connected to the parallel port or are made available via network. If you own a USB HP All-In-One device, start configuring as described at the beginning of this chapter. If it is detected properly and the *Test* succeeds, it is ready to use.

If your USB device is not properly detected, or your HP All-In-One device is connected to the parallel port or the network, run the HP Device Manager with *Other > Run hp-setup* from the YaST scanner module and follow the on-screen instructions. After having finished the HP Device Manager, the YaST scanner module automatically restarts the auto detection. If your scanner is detected properly, leave with *Finish*, otherwise manually choose a scanner from the list by clicking *Add*.

### 5.6.2 Sharing a Scanner over the Network

SUSE Linux Enterprise Desktop allows to share a scanner over the network. To do so, configure your scanner as described in [Section 5.6, “Setting Up a Scanner”](#) (page 62).



Once the scanner is successfully configured, choose *Other > Scanning via Network* in the YaST scanner module. Enter the hostnames of the clients (separated by a comma) that should be allowed to use the scanner under *Server Settings > Permitted Clients for saned* and leave the configuration dialog with *OK*.

## 5.6.3 Scanning over the Network

To use a scanner that is shared over the network, run the YaST scanner module with *Hardware > Scanner*. Open the network scanner configuration menu by *Other > Scanning via Network* and enter the hostname of the machine the scanner is connected to under *Client Settings > Servers Used for the net Metadriver*. Leave with *OK*. The network scanner is now listed in the Scanner Configuration window and is ready to use.



# Installing or Removing Software

Change the software collection of your system using YaST. This YaST module is available in three toolkit flavors: Qt, GTK+, and ncurses; Qt and GTK+ flavors are described here.

In YaST's software management tool search for software components you want to add or remove. YaST resolves all the dependencies for you. Add additional software repositories to your setup to install packages not shipped with the installation media and let YaST manage them. Keep your system up-to-date by managing software updates with openSUSE Updater.

## 6.1 Definition of Terms

### Repository

A local or remote directory containing packages plus additional information about these packages (package meta-data).

### (Repository) Alias

A short name for a repository used by various zypper commands. The alias can be chosen by the user when adding a repository and has to be unique.

### Product

Represents a whole product, for example SUSE Linux Enterprise Desktop.

### Pattern

A pattern is an installable list of packages needed for a special purpose. Examples are `Base System`, providing the openSUSE basic system, or `GNOME Base System`, containing all packages needed to run the GNOME Desktop environment.

### Package

A package is a compressed file in rpm format that contains the files for a particular program.

### Patch

A patch consists of one or more packages—either full packages or `patchrpm` or `deltarpm` packages—and may also introduce dependencies to packages that are not installed yet.

### Resolvable

An generic term for product, pattern, package or patch. The most commonly used type of resolvable is a package or a patch.

### patchrpm

A `patchrpm` consists only of files that have been updated since it was first released for SUSE Linux Enterprise Desktop 11. Its download size is usually considerably smaller than the size of a package.

### deltarpm

A `deltarpm` consists only of the binary diff between two defined versions of a package and therefore, has the smallest download size. Before being installed, the rpm package has to be rebuilt on the local machine.

## 6.2 Using the Qt Interface

Start the YaST Qt interface on the command line with `yast2 --qt`.

### 6.2.1 Installing Software

Software is available via RPM packages. Each package contains the program itself, the configuration files, and additional documentation. If you want to add more software to the system, proceed as follows:

- 1 Click *Software > Software Management* to start the YaST package manager.
- 2 In the search field enter the name of the software you want to install (for example, *xpdf*, a lightweight PDF viewer) and press *Enter*.
- 3 The package is listed in the right frame. Select it for installation. Once done, you can search for more packages and select them for installation in one go.
- 4 Click *Accept*.
- 5 When all selected packages are installed, YaST asks you whether you want to install or remove additional packages. Press *No* to close YaST.

By specifying various search criteria, you can restrict the search to display a few or even only one package. You can also define special search patterns using wild cards and regular expressions in *Search Mode*.

---

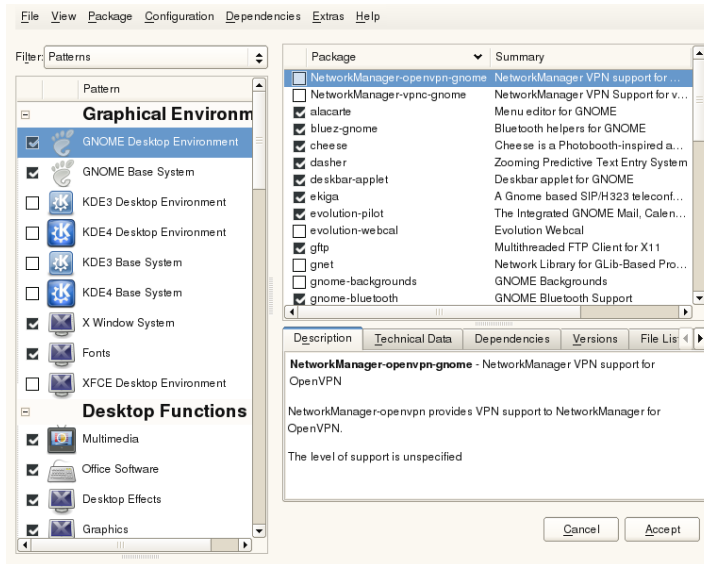
### **TIP: Quick Search**

In addition to the *Search* filter, all lists of the package manager feature a quick search. Click the respective list to gain focus (for example, the *Package* list) and enter a letter to move the cursor to the first package in the list whose name begins with this letter.

---

If you do not know the name of the software you are interested in, you can browse through the software catalog in various ways. For example, you can filter by patterns, package groups, languages, repositories, or installation summary. Filter by patterns, if you are looking for software for a specific task:

- 1 From the filter list in the upper left corner, select *Patterns*. Now you see various pattern sets listed in the area below.



- 2 From the patterns select one or more patterns you are interested in. If you click on the name of a pattern, for example on *Base Development*, you see the packages it contains, in the right frame. If you activate it, the status markers at the beginning of the line will change: all packages get marked either with the status *Keep* or *Install*. The meaning of all the symbols and font color changes is explained in *Help > Symbols*.

- 3 Click *Accept*.

Alternatively, filter by package groups. The package groups feature offers a more detailed view of the software grouped by categories. Often packages depend on other packages; if you select a package, you might be requested to install additional packages to resolve possible package dependencies.

Filtering by languages is similar to filtering by package groups. Using the languages view enables you to select packages like translated program messages, documentation, or special fonts which are needed to support a specific language.

For installing corresponding source packages, use `zypper`. For more information, see Section “Installing and Removing Software with Zypper” (Chapter 5, *Managing Software with Command Line Tools*, ↑Administration Guide).

Using the installation summary filter you see an overview of the packages you have scheduled for installation. It is convenient for double-checking if many packages are pending for installation.

## 6.2.2 Checking Software Dependencies

The software of one package might only work properly if the required package is also installed. If packages with identical or similar functionality use the same system resource, they should not be installed at the same time, because this would cause a package conflict.

When the package manager starts, it examines the system and displays the installed packages. When you select to install and remove packages, the package manager automatically checks the dependencies and selects any other required packages (resolution of dependencies). If you select or deselect conflicting packages, the package manager indicates this and suggests possible solutions to this problem (resolution of conflicts).

*Check Dependencies* and *Autocheck* are located under the information window. If you click *Check Dependencies*, the package manager checks if the current package selection results in any unresolved package dependencies or conflicts. In the event of unresolved dependencies, the required additional packages are selected automatically. For package conflicts, the package manager opens a dialog that shows the conflict and offers various options for solving the problem.

If you activate *Autocheck*, any change of a package status triggers an automatic check. This is a useful feature, because the consistency of the package selection is monitored permanently. However, this process consumes resources and can slow down the package manager. For this reason, *Autocheck* is not activated by default. In either case, a consistency check is performed when you confirm your selection with *Accept*.

For example, `sendmail` and `postfix` may not be installed concurrently. **Figure 6.1, “Conflict Management of the Package Manager”** (page 70) shows the conflict message prompting you to take a decision. `postfix` is already installed. Accordingly, you can refrain from installing `sendmail`, remove `postfix`, or take the risk and ignore the conflict.

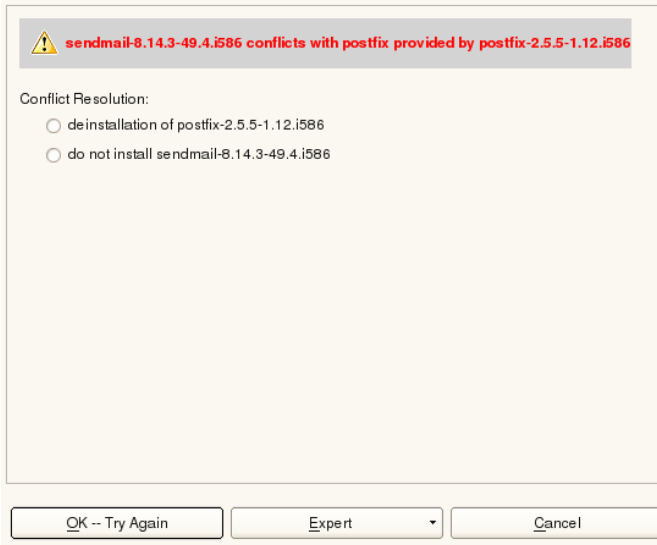
---

## WARNING: Handling Package Conflicts

Unless you are very experienced, follow the suggestions of YaST when handling package conflicts, because otherwise the stability and functionality of your system could be endangered by the existing conflict.

---

**Figure 6.1** *Conflict Management of the Package Manager*



## 6.2.3 Packages and Software Repositories

If you want to search for packages originating from one particular software repository, use the *Repositories* filter. In the default configuration, this filter shows a list of all packages from the selected installation source. To restrict the list, use a secondary filter.

To view a list of the all installed packages from the selected repository, select the filter *Repositories* then select *Installation Summary* from *Secondary Filter* list and deactivate all check boxes except *Keep*.

If you are interested in the opposite and want to detect packages not belonging to any repository, also use the *Repositories* filter and select *Unmaintained Packages* as the *Secondary Filter*.



## 6.2.4 Removing Software

If you want to remove software from the system, proceed as follows:

- 1 Make use of a search strategy explained in [Section 6.2.1, “Installing Software”](#) (page 66).
- 2 Depending on the search strategy, you can either select a complete set or single packages one by one. For patterns, both ways are possible.
- 3 Click *Accept* and either watch the de-installation progress or adjust your selection, if YaST complains about dependency issues.

## 6.3 Using the GTK+ Interface

Change the software collection of your system using YaST. In YaST's software management tool search for software components you want to add or remove. YaST resolves all the dependencies for you. Add additional software repositories to your setup to install packages not shipped with the installation media and let YaST manage them. Keep your system up-to-date by managing software updates with openSUSE Updater.

Start the YaST GTK+ interface on the command line with `yast2 --gtk`.

### 6.3.1 Installing Software

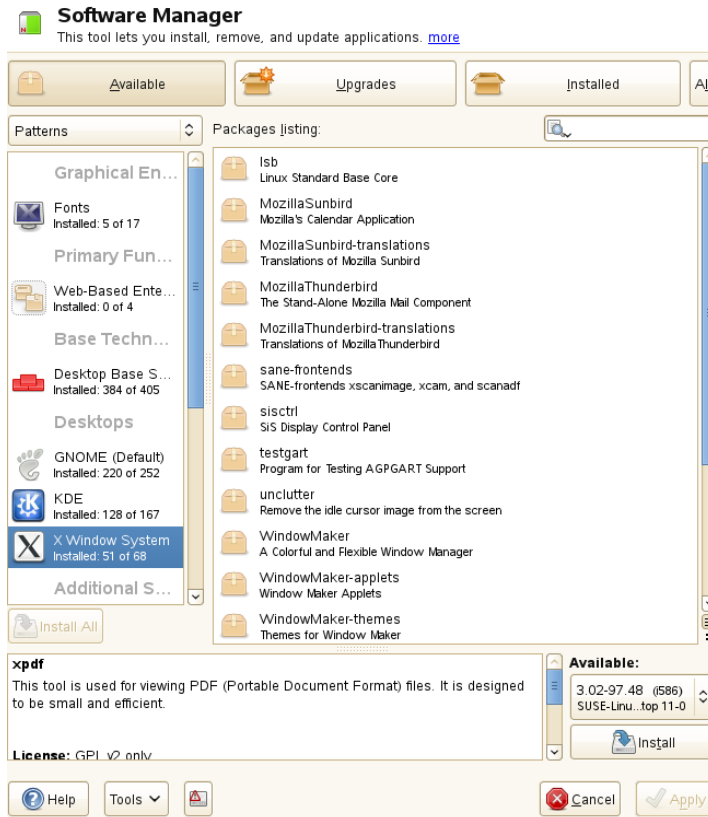
Software is available via RPM packages. Each package contains the program itself, the configuration files, and additional documentation. If you want to add more software to the system, proceed as follows:

- 1 Click *Software > Software Management* to start the YaST package manager.
- 2 In the package search field at the right window border enter the name of the software you want to install (for example, `xpdf`, a lightweight PDF viewer). YaST starts searching for the package while you enter the name. When the search is finished, select the desired package in the main pane and click *Install*.
- 3 You are able to search for more packages and list them the same way.

- 4 When finished, click *Apply* to perform the installation of the listed packages.

If you do not know the name of the software you are interested in, you can browse through the software catalog in various ways. For example, you can group by patterns, package groups, languages, or repositories. Group by patterns, if you are looking for software for a specific task:

- 1 From the grouping menu in the upper left corner, select *Patterns*. Now you see various pattern sets listed in the area below.



- 2 From the patterns select one or more patterns you are interested in. If you click the name of a pattern, for example, *Base Development*, you see the packages it

contains in the right frame. If you activate this pattern by clicking *Install All*, the packages will get listed in the changes overview on the right side.

**3** Click *Apply* to install all selected packages.

Alternatively, group by package groups. The package groups feature offers a more detailed view of the software grouped by categories. Packages often depend on other packages; if you select a package, you might be requested to install additional packages to resolve possible package dependencies.

Grouping by languages is similar to grouping by package groups. Using the languages view enables you to select packages like translated program messages, documentation, or special fonts which are needed to support a specific language.

For installing corresponding source packages, use `zypper`. For more information, see Section “Installing and Removing Software with Zypper” (Chapter 5, *Managing Software with Command Line Tools*, ↑Administration Guide).

## 6.3.2 Checking Software Dependencies

The software of one package might only work properly if the required package is also installed. If packages with identical or similar functionality use the same system resource, they should not be installed at the same time, because this would cause a package conflict.

When the package manager starts, it examines the system and displays the installed packages. When you select a package to install and remove it, the package manager automatically checks the dependencies and selects any other required packages (resolution of dependencies). If you select or deselect conflicting packages, the package manager indicates this and suggests possible solutions to this problem (resolution of conflicts).

For example, `sendmail` and `postfix` should not be installed concurrently. **Figure 6.2, “Conflict Management of the Package Manager”** (page 74) shows a conflict message prompting you to make a decision. `postfix` is already installed. Accordingly, you can decide whether to install `sendmail` or remove `postfix`.

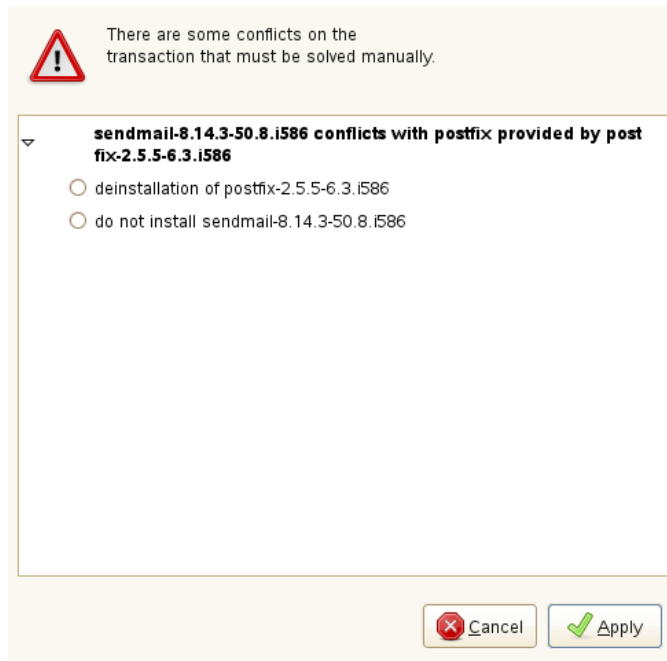
---

## WARNING: Handling Package Conflicts

Unless you are very experienced, follow the suggestions of YaST when handling package conflicts, because otherwise the stability and functionality of your system could be endangered by the existing conflict.

---

**Figure 6.2** *Conflict Management of the Package Manager*



## 6.3.3 Packages and Software Repositories

If you want to search for packages originating from one particular software repository, use grouping by *Repositories*. This view shows a list of all packages from the selected installation source.

To view a list of the all installed packages from the selected repository, click *Installed*. From this listing select packages for removing. To accomplish the opposite action, click *Available* and select packages for installation.

## 6.3.4 Removing Software

If you want to remove software from the system, proceed as follows:

- 1 Make use of a search strategy explained in [Section 6.3.1, “Installing Software”](#) (page 71).
- 2 In the *Packages Listing* mark the packages you want to remove. To mark all of them with one click, right-click in the *Packages Listing* pane and choose *Select All*.
- 3 Click *Remove*.

If you try to remove a package which is required by installed software, the conflict manager will complain about dependency issues and you must resolve the conflicts first as described in [Section 6.3.2, “Checking Software Dependencies”](#) (page 73).

When all conflicts are resolved, the package scheduled for removing is listed in the *Changes* pane on the right side.

- 4 Click *Apply* to perform all actions listed in the *Changes* pane.

## 6.4 Managing Software Repositories and Services

Add additional software repositories to your system to install third-party software. By default, the product repository such as SUSE Linux Enterprise Desktop-DVD 11 and a matching update repository are configured once you registered your system. Depending on the initially selected product, a separate language add-on repository with translations, dictionaries, etc. might also be configured.

Here also manage subscriptions to so-called *Services*. A Service in this context is a *Repository Index Service* (RIS) that can offer one or more software repositories. Such a Service can be changed dynamically by its administrator or vendor.

---

## WARNING: Trusting External Software Sources

Before adding external software repositories to your list of repositories, make sure this repository can be trusted. SUSE Linux Enterprise Desktop is not responsible for any potential problems arising from software installed from third-party software repositories.

---

To ensure the integrity software repositories can be signed with the GPG Key of the repository maintainer. You can manage these keys in YaST—for more information, see [GPG Keys](#) (page 77). Whenever you add a new repository, YaST offers to import its key. Verify it as any other GPG key and pay attention that it does not change. If you detect a key change, something could be wrong with the repository and you should better disable it as an installation source until you know the cause of the key change.

To add product repositories either click *Software Repositories* directly in the *Software* pane of the YaST control center, or from within the *Software Management*, proceed as follows:

- 1 In the *Software Management* start screen, select *Repositories* from the upper left drop-down menu and then click *Edit* to display an overview of configured software repositories.
- 2 Click *Add* to select the media type holding the repository, for example, *DVD* or *USB Mass Storage* with the language add-ons. Then click *Next* and provide additional information about the medium.
- 3 YaST asks to insert the medium.
- 4 Confirm with *Continue*. It takes some moments until YaST has downloaded and parsed the metadata of the repository. Once done you can install software from this repository as described in [Section 6.2.1, “Installing Software”](#) (page 66) resp. [Section 6.3.1, “Installing Software”](#) (page 71).

In the *Configured Software Repositories* overview find several configuration options:

### Properties

By default, after adding a new repository, the repository is *Enabled* and the *Automatically Refresh* is active. This means, YaST will pull in updated meta data automatically and is always aware of new versions.

The *Priority* of a repository is a value between 0 and 99, where 0 is the highest priority. If a package is available in more than one repository the repository with the highest priority wins. This is useful if you want to give a local repository (for example, a DVD) a higher priority to avoid downloading packages unnecessarily from the Internet although they have the same or a higher version number.

#### GPG Keys

Clicking *GPG Keys*, you open the GPG public keys management interface. In the *GPG Keys* subdialog, you can add new keys manually, delete or edit existing keys.

#### Refresh

*Refresh* lets you update the repository meta data in various ways.

## 6.5 Keeping the System Up-to-date

Novell offers a continuous stream of software security patches for your product. The updater applet informs you about the availability of patches and lets you easily install them with just a few clicks.

### 6.5.1 Using the KDE Updater Applet

The updater applet resides in the system tray of your panel depicting the head of the SUSE mascot (Geeko), which changes depending on the availability and relevance of patches and the status of the updater. Whenever the icon changes, a tool tip displaying the current status is shown, too. The applet is started by default. Choose *Applications > System > Desktop Applet > kupdateapplet* from the main menu to manually start it.

#### Green Geeko Head with Green Arrows

No patches available.

#### Green Geeko Head with Yellow Arrows

The updater applet is busy (for example checking for updates, installing software).

#### Red Star with Arrow

Security patches available.

#### Orange Star with Arrow

Important patches are available.

???Blue square with Arrow  
Trivial patches are available.

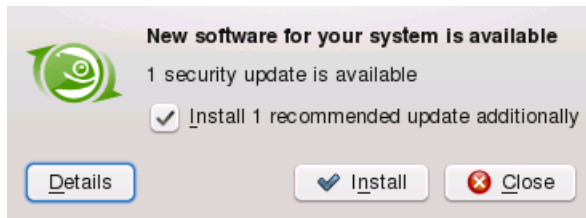
Yellow Triangle with Exclamation Mark  
An error occurred.

Blue Circle with Question Mark  
No update repository is defined. When you click the updater applet in this state, you are asked whether to check for updates. If you agree, the YaST *Online Update Configuration* module is started.

## Installing Patches

Whenever the updater icon shows the availability of patches, left-click to open the software installation window. It lists the number of *Security* and *Recommended* patches available. While the security patches are installed by default, you can choose whether to install the recommended ones as well. Some patches, such as new kernel versions, require to restart your computer. Check *Do not Install Updates that Require a Restart* to skip these updates for now. Start updating your system by clicking *Install*.

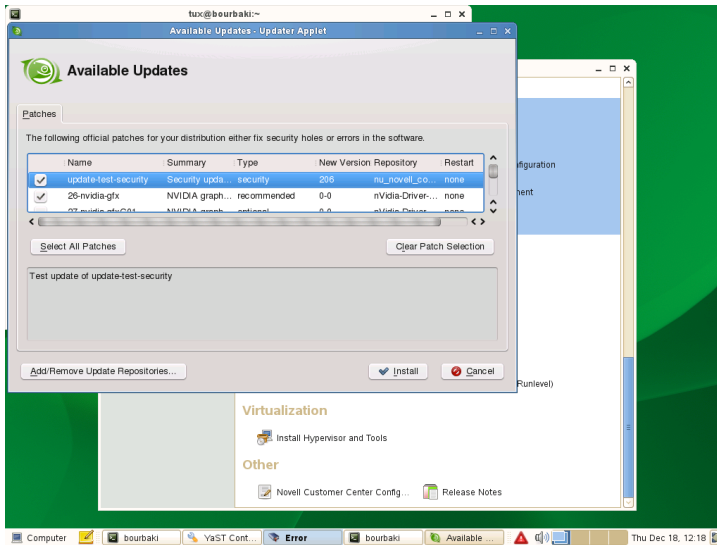
**Figure 6.3** KDE Updater Applet: Simple Update View



A click on *Details* opens the *Available Updates* window which shows a detailed list of all patches and allows you to alter the selection of packages that will be installed. Apart from the patch name the *Type* (Security, Recommended or Optional), a short *Summary* and the patch version number is shown. Patches are sorted alphabetically by default—change this by clicking on a column headline (*Name*, *Summary*, *Type*, *New Version*, *Catalog*, or *Restart*). Click *Install* to proceed.



**Figure 6.4** KDE Updater Applet: Detailed Update View



You will be prompted for the `root` password after having proceeded with *Install*. The updater performs the installation of the patches. See the system tray (KDE) or the notification area (GNOME) for status messages and a progress meter.

The YaST Online Update offers advanced features to customize the patch installation. Please refer to Chapter 1, *YaST Online Update* (↑Administration Guide) for more information.

## Installing New Software Versions

New software versions are available from software repositories provided by the open-SUSE community. By default, no such repositories are preconfigured. To add a repository, right-click on the updater icon and choose *Add/Remove Update Sources*. You need to enter the `root` password to start the *Configured Software Repositories* module.

---

### WARNING: Trusting External Software Sources

Before adding external software repositories to your list of repositories make sure this repository can be trusted. SUSE Linux Enterprise Desktop is not respon-

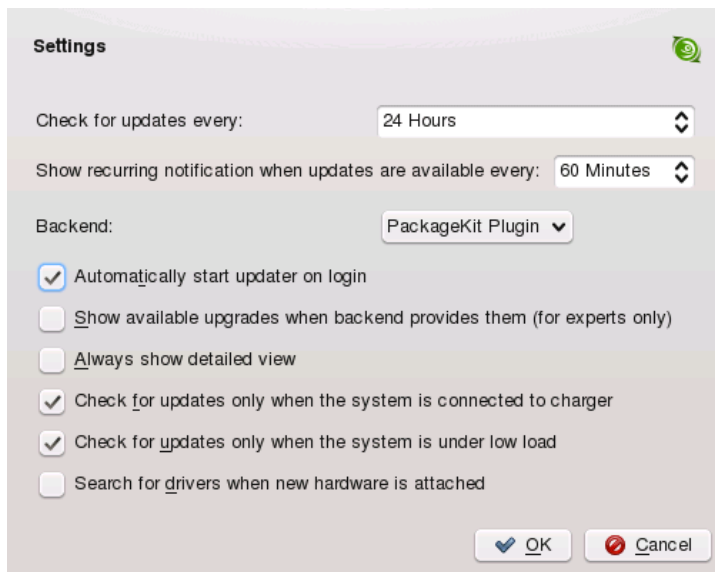
sible for any potential problems arising from software installed from third party software repositories.

The updater applet does not monitor repositories for new software versions by default. To enable this feature, open the configuration window as described in [Section “Configuring the Updater Applet”](#) (page 80) and tick the check box *Show Available Upgrades When Back-End Provides Them* check box. When the updater icon indicates the availability of updates, click on the icon to launch the software installation window. Click on *Details* and then on the *Upgrade* tab to open the list with new software versions. Either select single packages by checking the box in front of an entry, or click *Select All Packages*. *Install* starts the installation of the selected software packages. You will be prompted for the `root` password. See the system tray (KDE) or the notification area (GNOME) for status messages and a progress meter.

## Configuring the Updater Applet

By default the updater is started on login, checks for updates every 24 hours, shows recurring notifications every 60 minutes and only monitors the availability of patches. To change this behavior, right-click the applet icon and choose *Configure Applet*.

**Figure 6.5** KDE Updater Applet: Configuration



The configuration dialog also offers to change the following settings:

#### *Back-End*

Choose between different back-ends. The *Package Kit Plugin* is used by default. If you prefer the *ZYpp Plugin*, make sure the package `kde4-kupdateapplet-zypp` is installed.

#### *Always Show Detailed View*

Activate this option when you prefer the detailed patch view that lists all patches available with short summaries rather than the simple view.

#### *Check for Updates only When System Is Connected to Charger*

Prohibits checking for updates when running on batteries in order to save power. This option is activated by default but only affects mobile computers.

#### *Check for Updates only When System Is under Low Load*

Prohibits checking for updates when the system is under heavy load. This option is activated by default.

#### *Search for Drivers When New Hardware is Attached*

Provided a repository offering appropriate drivers, the updater can automatically install drivers for hardware such as USB devices.

## 6.5.2 Using the GNOME Updater Applet

The updater applet resides in the notification area of your panel. Its icon changes depending on the availability and relevance of patches and the status of the updater. The applet is started by default, choose *Computer > More Applications > System > Update System*.

---

### **NOTE: Icon visibility**

By default, the updater applet icon is only visible in the notification area, if patches are available.

---

Open box with a globe

The updater is busy (for example checking for updates, installing software).

Red Star with Exclamation Mark

Security patches available.

Orange Star with an Up Arrow

Recommended patches are available.

Yellow Star with a Down Arrow

Optional patches are available.

Yellow Triangle with Exclamation Mark

An error occurred.

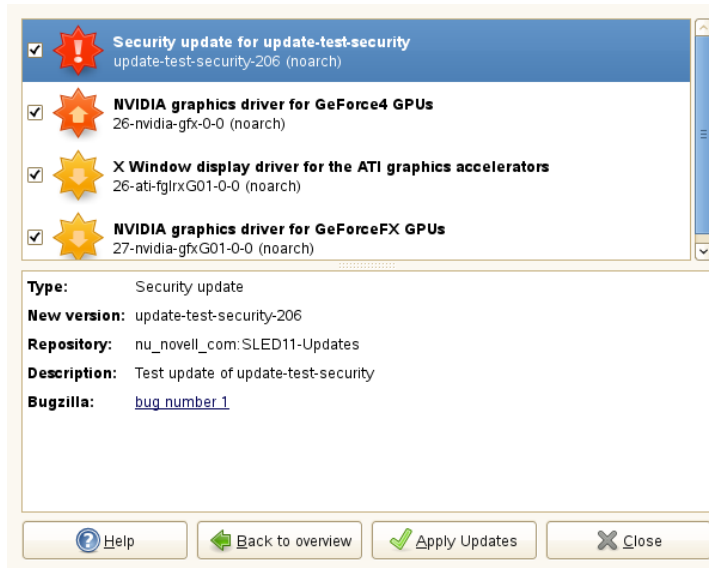
## Installing Patches

Whenever the updater icon shows the availability of patches, left-click the icon and choose *Update System Now*. Provide the `root` password. The patches available will be installed in the background.

Alternatively, left-click the updater icon and choose *Show Updates* to open the Software Update Viewer. In the overview it shows the number of patches available per category. Click on *Review* to open a detailed view where all patches sorted by category are listed. Security patches are displayed first, trivial patches last. Click on a patch to see details, such as a description, version number, repository, and—if available—a link to bugzilla, the Novell bug tracking system.

By default all patches are marked for installation. Uncheck the checkbox in front of a patch to prevent a patch from being installed.

**Figure 6.6** *GNOME Software Update Viewer: Detailed Update View*



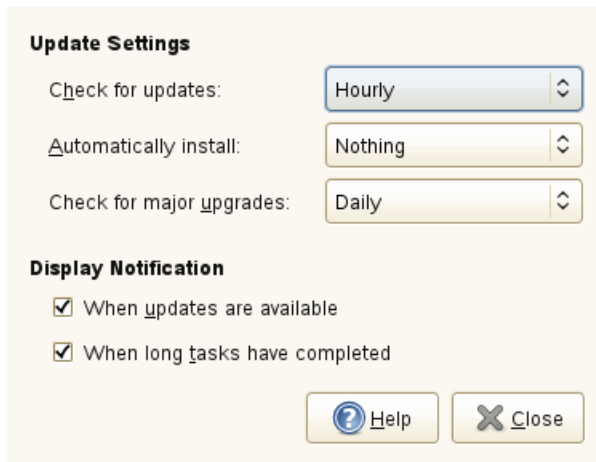
You will be prompted for the `root` password after having proceeded with *Apply Updates* or *Update System*. The updater performs the installation of the patches. After having finished the installation, choose whether to *Install More Updates* or whether to *Close* the Software Update Viewer.

The YaST Online Update offers advanced features to customize the patch installation. Please refer to Chapter 1, *YaST Online Update* (↑Administration Guide) for more information.

## Configuring the Updater Applet

To configure the updater applet, either right-click the updater icon in the panel and choose *Preferences*, or start the configuration dialog with *Computer > Control Center > System > Software Updates* to manually start it.

**Figure 6.7** *GNOME Updater Applet: Configuration*



**Update Settings**

Check for updates: Hourly

Automatically install: Nothing

Check for major upgrades: Daily

**Display Notification**

☒ When updates are available

☒ When long tasks have completed

? Help ✕ Close

The configuration dialog offers to change the following settings:

*Check for Updates*

Choose how often a check for updates is performed: *Hourly*, *Daily*, *Weekly*, or *Never*.

*Automatic Install*

Configure whether patches are installed automatically or not (default). Automatic installation can be chosen for either security patches only or for all patches.

*Check for Major Upgrades*

Choose how often a check for major upgrades is performed: *Daily*, *Weekly*, or *Never*.

**Display Notification Settings**

Determine whether and when to show the updater applet icon in the panel with this options.

# Installing Add-On Products

Add-on products are system extensions. You can install a third-party add-on product or a special system extension of SUSE Linux Enterprise, for example, the SDK add-on or a CD with binary drivers. To install a new add-on, use *Software > Add-On Products*. You can select various types of product media, like CD, FTP, USB mass storage devices (such as USB flash drives or disks) or a local directory. You can also work directly with local ISO files. To add an add-on as ISO file media, select *Local ISO Image* and enter the *Path to ISO Image*. The *Repository Name* is arbitrary.

## 7.1 Add-Ons

To install a new add-on, proceed as follows:

- 1 Click *Software > Add-On Products* to see an overview of installed add-on products.
- 2 Select various types of product media, such as CD, FTP or a local directory, by clicking *Add*. You can also use ISO images instead of CD or DVD media.
- 3 To add an ISO image, select *Local ISO Image* and click *Next*.
- 4 Enter the *Path to ISO Image* and choose a *Repository Name*. Click *Next*.
- 5 After successfully adding the add-on media, the software manager window appears. If the add-on provides a new pattern, see the new item in the *Patterns* filter.

To view the list of all packages from the selected software repository, select the filter *Software Repositories* and choose the repository to view.

## 7.2 Binary Drivers

Some hardware needs binary-only drivers to function properly. If you have such hardware, refer to the release notes for more information about availability of binary drivers for your system. To read the release notes, open YaST and select *Miscellaneous > Release Notes*.

## 7.3 SUSE Software Development Kit (SDK) 10

SUSE Software Development Kit 10 is an add-on for SUSE Linux Enterprise 10. It is a complete tool kit for application development. In fact, to provide a comprehensive build system, SUSE Software Development Kit 10 includes all the open source tools that were used to build the SUSE Linux Enterprise Server product. It provides you as a developer, independent software vendor (ISV), or independent hardware vendor (IHV), with all the tools needed to port applications to all the platforms supported by SUSE Linux Enterprise Desktop and SUSE Linux Enterprise Server.

SUSE Software Development Kit also contains integrated development environments (IDEs), debuggers, code editors, and other related tools. It supports most major programming languages, including C, C++, Java, and most scripting languages. For your convenience, SUSE Software Development Kit includes multiple Perl packages that are not included in SUSE Linux Enterprise.

For detailed information, refer to <http://developer.novell.com/ndk/susesdk.htm>. Use the YaST add-on installer and package manager to install SUSE Software Development Kit 10.



# Accessing the Internet

If you have chosen not to configure Internet access during the installation, you can perform this task at any time using YaST. How to configure your computer to access the Internet depends on your environment. If the computer you are installing is part of a network which already is connected to the Internet, the only thing to do is to link your machine into the network. If you are installing a machine that is directly connected to the Internet, the hardware and the access to the Internet Service Provider (ISP) need to be set up.

Please refer to the checklists below to make sure you have all the data ready to hand when starting to configure the Internet access.

## 8.1 Direct Internet Connection

When your computer is directly connected to the Internet, you first need to configure the hardware that is used for this task. This can either be an internal device (such as an ISDN card) or an external device (for example a modem). In most cases it is detected automatically.

In a second step you need to enter data provided by your ISP, such as login credentials, gateway, or name server, for example. You should have received a data sheet from your ISP where all the necessary data is listed.

If you have successfully configured your hardware and ISP data, use the *NetworkManager* for managing the internet connection. See Chapter 23, *Using NetworkManager* (↑Administration Guide) for details.

## 8.1.1 Checklist DSL

There are different types of DSL devices available that use different point-to-point protocol (PPP) methods:

- a regular ethernet card connected to the external DSL modem uses PPP over Ethernet (PPPoE). In Austria the Point-to-Point Tunneling Protocol (PPTP) is used. With PPTP the external modem also has a static IP address.
- an internal DSL modem uses PPP over ATM (PPPoATM)
- an internal ADSL Fritz Card uses CAPI for ADSL

The DSL configuration module already contains the data for major ISPs in some countries. If your ISP is not listed, you will need to know how name resolving (DNS) and IP allocation is handled (in most cases this data is received automatically when connecting). Regardless whether you choose an ISP from the list or add a custom provider, you need to enter at least your login and password.

For configuration details, refer to Section “DSL” (Chapter 19, *Basic Networking*, ↑Administration Guide).

## 8.1.2 Checklist ISDN

In case your internal ISDN card is not detected automatically you will need to know the vendor and the name of the device.

---

### **NOTE: ISDN Modem or Terminal Adapter**

If you are using an external ISDN modem or terminal adapter, refer to **Section 8.1.3, “Checklist Modem”** (page 89) instead.

---

In order to configure the ISDN device you will need the following data:

- ISDN Protocol (depends on your country)
- Area code and phone number.

- Interface type (SyncPPP or RawIP). If unsure, select SyncPPP, because RawIP is only used in connection with certain telephone systems.
- In case you got a static IP-address from your provider: local and remote IP-addresses for the dial-in server and the gateway.
- The ISDN configuration module already contains the data for major ISPs in some countries. If your ISP is not listed, you will need to know how name resolving (DNS) and IP allocation is handled (in most cases this data is received automatically when connecting). Regardless whether you chose an ISP from the list or added a custom provider, you need to enter at least your login and password.

For configuration details, refer to Section “ISDN” (Chapter 19, *Basic Networking*, ↑Administration Guide).

## 8.1.3 Checklist Modem

In case your modem is not detected automatically, you need to know whether it is connected to a serial port or to an USB port. Please note that not all USB modems and internal modems are supported by SUSE® Linux Enterprise Desktop.

The modem configuration module already contains the data for major ISPs in some countries. If your ISP is not listed, you will need to know its dial-in number and how name resolving (DNS) and IP allocation is handled (in most cases this data is received automatically when connecting). Regardless whether you chose an ISP from the list or added a custom provider, you need to enter at least your login and password.

For configuration details, refer to Section “Modem” (Chapter 19, *Basic Networking*, ↑Administration Guide).

## 8.1.4 Checklist Cable Modem

Accessing the Internet through the TV cable requires a cable modem. Such a modem is connected to the computer via ethernet cable. Therefore it is only necessary to configure your network card accordingly. For details, refer to Section “Cable Modem” (Chapter 19, *Basic Networking*, ↑Administration Guide).

## 8.2 Internet Connection Via Network

If your machine is part of a network which is already connected to the Internet, it is very easy to gain Internet access—just configure your network card and connect your machine to the existing network and you are done. This not only applies to large company networks, but to small home networks as well. Even if the machine you are installing is only connected to a router (e.g. a DSL router) it is already part of a network.

---

### **NOTE: Routing and Name Services**

In the following it is assumed that the network is connected to the Internet and provides routing and name services. In case these services are provided by a router, make sure the router is configured correctly before setting up the client.

---

### 8.2.1 Checklist Network

If your network provides DHCP (Dynamic Host Configuration Protocol) check the appropriate check box when setting up the network card and you are done—all parameters needed will be provided by the DHCP server.

In case DHCP is not available, ask your network administrator for the following details:

- Hostname
- Name server
- Gateway

For configuration details, refer to Section “Configuring the Network Card with YaST” (Chapter 19, *Basic Networking*, ↑Administration Guide).

# Managing Users with YaST

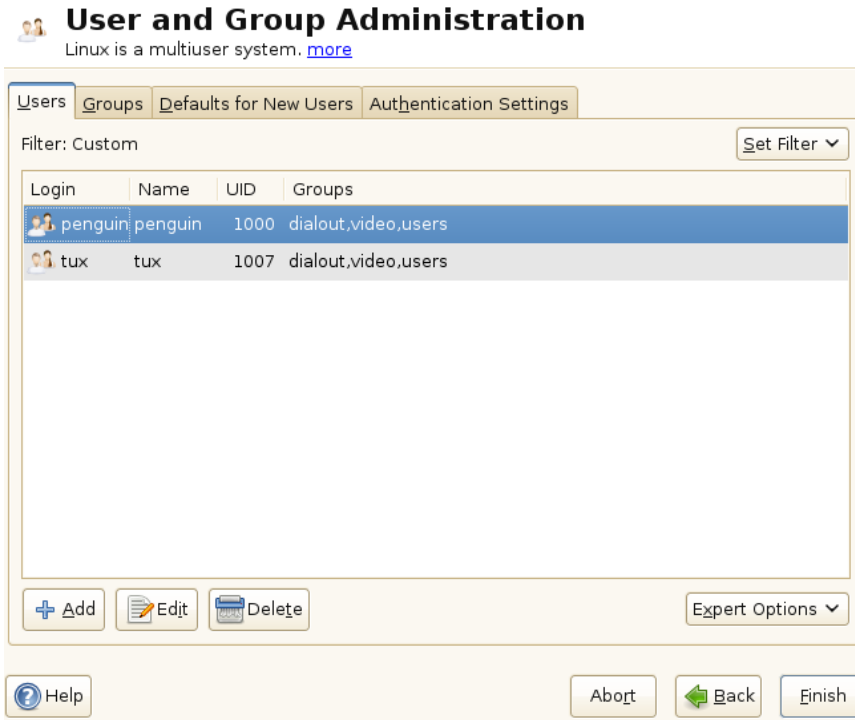
During installation, you have chosen a method for user authentication . This method is either local (via `/etc/passwd`) or, if a network connection is established, via NIS, LDAP, Kerberos or Samba (see [Section 3.8, “Create New User”](#) (page 30)). You can create or modify user accounts and can change the authentication method with YaST at any time.

Every user is assigned a user ID (UID) which identifies him in the system. 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. .

## 9.1 User and Group Administration Dialog

To administrate 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 9.1** *YaST User and Group Administration*



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 9.2, “Managing User Accounts”](#) (page 93). Learn about advanced options like enforcing password policies, using encrypted home directories, using fingerprint authentication, or managing disk quotas in [Section 9.3, “Additional Options for User Accounts”](#) (page 95).

### 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 9.4, “Changing Default Settings for Local Users”](#) (page 103).

### Assigning Users to Groups

Learn how to change the group assignment for individual users in [Section 9.5, “Assigning Users to Groups”](#) (page 104).

### Managing Groups

From the *Groups* tab, you can add, modify or delete existing groups. Refer to [Section 9.6, “Managing Groups”](#) (page 104) for information how to do this.

### Changing the User Authentication Method

When your machine is connected to a network providing 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 9.7, “Changing the User Authentication Method”](#) (page 106).

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 may be available from the dialog.

## 9.2 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 and know about the implications.

---

**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 does no longer own the files he created elsewhere in the file system unless you manually change the file ownership for those files.

---

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 9.3.5, “Managing Quotas”](#) (page 100).

**Procedure 9.1** *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 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.

- 6 To force users to regularly change their password or set other password options, switch to *Password Settings* and adjust the options.
- 7 If all options are set according to your wishes, click *OK*.



- 8 Click *Expert Options > Write Changes Now* to save all changes without exiting the *User and Group Administration* dialog. Or click *Finish* 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 should also integrate in 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 created them directly on the network.

---

**Procedure 9.2** *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 in to 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.

## 9.3 Additional Options for User Accounts

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

## 9.3.1 Automatic Login and Passwordless Login

If you use 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*.

## 9.3.2 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 9.3** *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.
- 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*.

### 9.3.3 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 generated for the user. The image key is protected with the user's login password. When the user logs in to 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 11, *Encrypting Partitions and Files*, ↑Security Guide).

**Procedure 9.4** *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 un... [more](#)

User Data Details Password Settings Plug-Ins

User ID (uid):

Home Directory:

☒ Move to New Location

Directory Size in MB  
☒ Use Encrypted Home Directory

Additional User Information:

Login Shell:

Default Group:

Additional Groups:

- ☐ users
- ☐ at
- ☐ audio
- ☐ avahi
- ☐ beagleindex
- ☐ bin
- ☐ cdrom
- ☐ console
- ☐ daemon
- ☒ dialout
- ☐ disk
- ☐ festival
- ☐ floppy
- ☐ ftp
- ☐ games
- ☐ qdm

- 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. Or click *Finish* to close the administration dialog and to save the changes.

### **Procedure 9.5** *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 users, 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. Or click *Finish* to close the administration dialog and to save the changes.

## **9.3.4 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 in to 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://reactivated.net/fprint/wiki/Supported\\_devices](http://reactivated.net/fprint/wiki/Supported_devices).

## **9.3.5 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 notes) 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.

SUSE Linux Enterprise Desktop allows usage of `soft` and `hard` quotas. Soft quotas usually define a warning level at which users are informed 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 9.6** *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 if you confirm the respective message with *Yes*.
- 4** Confirm your changes and leave the *Expert Partitioner*.

### **Procedure 9.7** *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 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:

**Size Limits**

Soft limit:

Hard limit:

Days:  Hours:  Minutes:  Seconds:

**I-nodes Limits**

Soft limit:

Hard limit:

Days:  Hours:  Minutes:  Seconds:

- 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. Or click *Finish* to close the administration dialog and to save the changes.

SUSE Linux Enterprise Desktop 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 (root password needed).

## 9.4 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 belong 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 10, *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 *Finish*.

## 9.5 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 9.4, “Changing Default Settings for Local Users”](#) (page 103).

### **Procedure 9.8** *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 to 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. Or click *Finish* to close the administration dialog and to save the changes.

## 9.6 Managing Groups

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

### **Procedure 9.9** *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 Data Plug-Ins

Group Name:

Group ID (gid):

Password:

Confirm Password:

Group Members:

- ☐ at
- ☐ avahi
- ☐ beagleindex
- ☐ bin
- ☐ daemon
- ☐ festival
- ☐ ftp
- ☒ games
- ☒ mrxml
- ☒ penguin
- ☒ tux

 Help  

- 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 just 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. Or click *Finish* to close the administration dialog and to save the changes.

## 9.7 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 complete network for the rest of the session.

### Samba

SMB authentication is often used in mixed Linux and Windows networks. For details, see Chapter 24, *Samba* (↑Administration Guide) and Chapter 5, *Active Directory Support* (↑Security Guide).

### eDirectory LDAP

eDirectory authentication is used in Novell networks.

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)

**Samba:** Section “Configuring a Samba Client with YaST” (Chapter 24, *Samba*, ↑Administration Guide)
- 4 After accepting the configuration, return to the *User and Group Administration* overview.
- 5 Click *Finish* to close the administration dialog.



# Changing Language and Country Settings with YaST

# 10

Working in different countries or having to work in a multilingual environment requires your computer to be set up to support this. Use the YaST language and timezone modules to install additional system languages and adjust the country and timezone settings accordingly. The YaST language module also lets you change your system language or determine a primary language that you use most often. Install secondary languages to get optional localizations if you need to start applications or desktops in languages other than the primary one. The YaST timezone module allows you to adjust your country and timezone settings and synchronize your system clock against a time server.

## 10.1 Changing the System Language

Depending on how you use your desktop and whether you want to switch the entire system to another language or just the desktop environment itself, there are several ways to achieve this:

### Change the System Language Globally

Proceed as described in [Section 10.1.1, “Installing Additional System Languages”](#) (page 110) and [Section 10.1.2, “Switching the System Language”](#) (page 112) to install additional localized packages with YaST and set the default language. Changes are effective after relogin. To ensure that the entire system reflects the change, reboot the system or close and restart all running services, applications, and programs.

### Change the Language for the Desktop Only

Provided you have previously installed the desired language packages for your desktop environment with YaST as described below, you can switch the language

of your desktop using the desktop's control center. After X has been restarted, your entire desktop reflects your new choice of language. Applications not belonging to your desktop framework are not affected by this change and may still appear in the language that was set in YaST.

#### Temporarily Switch Languages for One Application Only

To run a single application in another language (that has already been installed with YaST), use one of the following commands:

- `LANG=de_DE application` to start any standard X application or GNOME application in German. For other languages, use the appropriate language code. Get a list of all language codes available using the `locale -av` command.
- `KDE_LANG=de application` to start any KDE application in German. For other languages, use the appropriate language code.

## 10.1.1 Installing Additional System Languages

The main language was selected during installation (see [Section 3.5, “Welcome”](#) (page 25)) and keyboard and time zone settings were adjusted. However, you can install additional languages on your system and determine which of the different languages installed should be taken as the default. Before installing additional languages, determine which of them should be activated after you install it. YaST knows two different language categories:

#### Primary Language

The primary language set in YaST applies to the entire system, including YaST and the desktop environment. This language is used whenever available unless you manually specify another language.

#### Secondary Languages

Secondary languages are languages selected manually for a specific situation. For example, use a secondary language to start an application in a certain language, for example, to do word processing in this language.



**Figure 10.1** *Setting the Language*



To install an additional language, proceed as follows:

- 1 As root, start YaST.
- 2 Select *System > Language*.
- 3 Select the desired languages from the list of languages offered in *Secondary Languages*. When you leave this dialog with *Ok*, YaST installs the additional localized software packages. The system is multilingual, but you need to set the desired language explicitly to start an application in a language other than the primary one.
- 4 To make this language the default (the primary language), select it under *Primary Language*:

- 4a** Adapt the keyboard to the new primary language and adjust the time zone, if appropriate.

---

**TIP**

For advanced keyboard or time zone settings, open the *Hardware > Keyboard Layout* (Section 5.3.1, “Keyboard Layout” (page 53)) or *System > Date and Time* dialog (Section 10.2, “Changing the Country and Time Settings” (page 113)).

---

- 4b** Select *Details* to change language settings specific to `root` and to determine the exact locale:

Locale Settings for User `root`

`ctype` only adjusts the `LC_TYPE` variable in `/etc/sysconfig/language` for `root`, which sets the localization for language-specific function calls. `yes` sets the language for `root` to the same as the language for local users. `no` means the language settings for `root` are not affected by language changes. All `locale` values remain unset.

Use UTF-8 Encoding

Disable this box, if you do not want to use UTF-8 encoding for `root`.

Detailed Locale Setting

If your locale was not included in the list of primary languages available, try explicitly specifying it here. However, some of these localizations may be incomplete.

- 5** Leave this dialog and apply your settings with *Ok*.

## 10.1.2 Switching the System Language

Switching the system language is similar to installing additional languages. Use the YaST language module to change the primary language and to adjust keyboard and time zone. Once YaST has applied your changes and any open X sessions have been restarted, YaST, applications, and the desktop reflect your new language settings.

## 10.2 Changing the Country and Time Settings

Using the YaST date and time module, adjust your system date, clock and time zone information to the area you are working in. First, select a general region, such as *Europe*, for example. Choose an appropriate time zone that matches the one you are working in, for example, *Germany*.

Depending on which operating systems run on your workstation, adjust the hardware clock settings, accordingly:

- If you run another operating system on your machine, such as Microsoft Windows\*, it is likely your system does not use UTC, but local time. In this case, uncheck *Hardware Clock Set To UTC*.
- If you only run Linux on your machine, set the hardware clock to UTC and have the switch from standard time to daylight saving time performed automatically.

You can change the date and time manually or opt for synchronizing your machine against an NTP server, either permanently or just for adjusting your hardware clock. If you want to set date and time manually, proceed as follows:

**Figure 10.2** *Setting Country and Time*

 **Clock and Time Zone**  
To select the time zone to use in your system, first select the Region. [more](#)

---



Region:  Time Zone:


☒ Hardware Clock Set To UTC

**Time and Date (NTP is configured)**  
15:34:12 - 2008-10-22

- 1 Click *Change* to set date and time.
- 2 Select *Manually* and enter date and time values.
- 3 Confirm with *Accept*.

If you want to make use of an NTP server:

**Figure 10.3** *Setting Date and Time With NTP Server*

 **Change Date and Time**  
The current system time and date are displayed. [more](#)

---

☐ Manually

Current Time:  
 :

Current Date:  
 -  -

☒ Synchronize with NTP Server

NTP Server Address:

☒ Save NTP Configuration

- 1 Click *Change* to set date and time.
- 2 Select *Synchronize with NTP Server*.
- 3 Enter the address of an NTP server, if not prefilled.
- 4 Press *Synchronize Now*, to get your system time set correctly. If you want to make use of NTP permanently, enable *Save NTP Configuration*.
- 5 Confirm with *Accept*.

With the *Configure* button, you can also open the advanced NTP configuration. For details, see Section “Configuring an NTP Client with YaST” (Chapter 22, *Time Synchronization with NTP*, ↑Administration Guide).



# Remote Installation

SUSE® Linux Enterprise Desktop can be installed in several different ways. As well as the usual media installation covered in [Chapter 3, \*Installation with YaST\*](#) (page 17), you can choose from various network-based approaches or even take a completely hands-off approach to the installation of SUSE Linux Enterprise Desktop.

Each method is introduced by means of two short check lists: one listing the prerequisites for this method and the other illustrating the basic procedure. More detail is then provided for all the techniques used in these installation scenarios.

---

## NOTE

In the following sections, the system to hold your new SUSE Linux Enterprise Desktop installation is referred to as *target system* or *installation target*. The term *installation source* is used for all sources of installation data. This includes physical media, such as CD and DVD, and network servers distributing the installation data in your network.

---

## 11.1 Installation Scenarios for Remote Installation

This section introduces the most common installation scenarios for remote installations. For each scenario, carefully check the list of prerequisites and follow the procedure outlined for this scenario. If in need of detailed instructions for a particular step, follow the links provided for each one of them.

---

## IMPORTANT

The configuration of the X Window System is not part of any remote installation process. After the installation has finished, log in to the target system as `root`, enter `telinit 3`, and start `SaX2` to configure the graphics hardware.

---

### 11.1.1 Simple Remote Installation via VNC—Static Network Configuration

This type of installation still requires some degree of physical access to the target system to boot for installation. The installation itself is entirely controlled by a remote workstation using VNC to connect to the installation program. User interaction is required as with the manual installation in [Chapter 3, \*Installation with YaST\*](#) (page 17).

For this type of installation, make sure that the following requirements are met:

- Remote installation source: NFS, HTTP, FTP, or SMB with working network connection.
- Target system with working network connection.
- Controlling system with working network connection and VNC viewer software or Java-enabled browser (Firefox, Konqueror, Internet Explorer, or Opera).
- Physical boot medium (CD or DVD) for booting the target system.
- Valid static IP addresses already assigned to the installation source and the controlling system.
- Valid static IP address to assign to the target system.

To perform this kind of installation, proceed as follows:

- 1 Set up the installation source as described in [Section 11.2, “Setting Up the Server Holding the Installation Sources”](#) (page 126). Choose an NFS, HTTP, or FTP network server. For an SMB installation source, refer to [Section 11.2.5, “Managing an SMB Installation Source”](#) (page 134).



- 2 Boot the target system using the first CD or DVD of the SUSE Linux Enterprise Desktop media kit.
- 3 When the boot screen of the target system appears, use the boot options prompt to set the appropriate VNC options and the address of the installation source. This is described in detail in [Section 11.4, “Booting the Target System for Installation”](#) (page 146).

The target system boots to a text-based environment, giving the network address and display number under which the graphical installation environment can be addressed by any VNC viewer application or browser. VNC installations announce themselves over OpenSLP and if the firewall settings permit, they can be found using Konqueror in `service:/` or `slp:/` mode.

- 4 On the controlling workstation, open a VNC viewing application or Web browser and connect to the target system as described in [Section 11.5.1, “VNC Installation”](#) (page 150).
- 5 Perform the installation as described in [Chapter 3, \*Installation with YaST\*](#) (page 17). Reconnect to the target system after it reboots for the final part of the installation.
- 6 Finish the installation.

## 11.1.2 Simple Remote Installation via VNC—Dynamic Network Configuration

This type of installation still requires some degree of physical access to the target system to boot for installation. The network configuration is made with DHCP. The installation itself is entirely controlled from a remote workstation using VNC to connect to the installer, but still requires user interaction for the actual configuration efforts.

For this type of installation, make sure that the following requirements are met:

- Remote installation source: NFS, HTTP, FTP, or SMB with working network connection.

- Target system with working network connection.
- Controlling system with working network connection and VNC viewer software or Java-enabled browser (Firefox, Konqueror, Internet Explorer, or Opera).
- Physical boot medium (CD, DVD, or custom boot disk) for booting the target system.
- Running DHCP server providing IP addresses.

To perform this kind of installation, proceed as follows:

- 1 Set up the installation source as described in [Section 11.2, “Setting Up the Server Holding the Installation Sources”](#) (page 126). Choose an NFS, HTTP, or FTP network server. For an SMB installation source, refer to [Section 11.2.5, “Managing an SMB Installation Source”](#) (page 134).
- 2 Boot the target system using the first CD or DVD of the SUSE Linux Enterprise Desktop media kit.
- 3 When the boot screen of the target system appears, use the boot options prompt to set the appropriate VNC options and the address of the installation source. This is described in detail in [Section 11.4, “Booting the Target System for Installation”](#) (page 146).

The target system boots to a text-based environment, giving the network address and display number under which the graphical installation environment can be addressed by any VNC viewer application or browser. VNC installations announce themselves over OpenSLP and if the firewall settings permit, they can be found using Konqueror in `service:/` or `slp:/` mode.

- 4 On the controlling workstation, open a VNC viewing application or Web browser and connect to the target system as described in [Section 11.5.1, “VNC Installation”](#) (page 150).
- 5 Perform the installation as described in [Chapter 3, \*Installation with YaST\*](#) (page 17). Reconnect to the target system after it reboots for the final part of the installation.
- 6 Finish the installation.

## 11.1.3 Remote Installation via VNC—PXE Boot and Wake on LAN

This type of installation is completely hands-off. The target machine is started and booted remotely. User interaction is only needed for the actual installation. This approach is suitable for cross-site deployments.

To perform this type of installation, make sure that the following requirements are met:

- Remote installation source: NFS, HTTP, FTP, or SMB with working network connection.
- TFTP server.
- Running DHCP server for your network.
- Target system capable of PXE boot, networking, and Wake on LAN, plugged in and connected to the network.
- Controlling system with working network connection and VNC viewer software or Java-enabled browser (Firefox, Konqueror, Internet Explorer, or Opera).

To perform this type of installation, proceed as follows:

- 1 Set up the installation source as described in [Section 11.2, “Setting Up the Server Holding the Installation Sources”](#) (page 126). Choose an NFS, HTTP, or FTP network server or configure an SMB installation source as described in [Section 11.2.5, “Managing an SMB Installation Source”](#) (page 134).
- 2 Set up a TFTP server to hold a boot image that can be pulled by the target system. This is described in [Section 11.3.2, “Setting Up a TFTP Server”](#) (page 139).
- 3 Set up a DHCP server to provide IP addresses to all machines and reveal the location of the TFTP server to the target system. This is described in [Section 11.3.1, “Setting Up a DHCP Server”](#) (page 136).
- 4 Prepare the target system for PXE boot. This is described in further detail in [Section 11.3.5, “Preparing the Target System for PXE Boot”](#) (page 145).

- 5 Initiate the boot process of the target system using Wake on LAN. This is described in [Section 11.3.7, “Wake on LAN”](#) (page 146).
- 6 On the controlling workstation, open a VNC viewing application or Web browser and connect to the target system as described in [Section 11.5.1, “VNC Installation”](#) (page 150).
- 7 Perform the installation as described in [Chapter 3, \*Installation with YaST\*](#) (page 17). Reconnect to the target system after it reboots for the final part of the installation.
- 8 Finish the installation.

## 11.1.4 Simple Remote Installation via SSH—Static Network Configuration

This type of installation still requires some degree of physical access to the target system to boot for installation and to determine the IP address of the installation target. The installation itself is entirely controlled from a remote workstation using SSH to connect to the installer. User interaction is required as with the regular installation described in [Chapter 3, \*Installation with YaST\*](#) (page 17).

For this type of installation, make sure that the following requirements are met:

- Remote installation source: NFS, HTTP, FTP, or SMB with working network connection.
- Target system with working network connection.
- Controlling system with working network connection and working SSH client software.
- Physical boot medium (CD, DVD, or custom boot disk) for the target system.
- Valid static IP addresses already assigned to the installation source and the controlling system.
- Valid static IP address to assign to the target system.

To perform this kind of installation, proceed as follows:

- 1 Set up the installation source as described in [Section 11.2, “Setting Up the Server Holding the Installation Sources”](#) (page 126). Choose an NFS, HTTP, or FTP network server. For an SMB installation source, refer to [Section 11.2.5, “Managing an SMB Installation Source”](#) (page 134).
- 2 Boot the target system using the first CD or DVD of the SUSE Linux Enterprise Desktop media kit.
- 3 When the boot screen of the target system appears, use the boot options prompt to set the appropriate parameters for network connection, address of the installation source, and SSH enablement. This is described in detail in [Section 11.4.2, “Using Custom Boot Options”](#) (page 147).

The target system boots to a text-based environment, giving the network address under which the graphical installation environment can be addressed by any SSH client.

- 4 On the controlling workstation, open a terminal window and connect to the target system as described in [Section “Connecting to the Installation Program”](#) (page 152).
- 5 Perform the installation as described in [Chapter 3, \*Installation with YaST\*](#) (page 17). Reconnect to the target system after it reboots for the final part of the installation.
- 6 Finish the installation.

## 11.1.5 Simple Remote Installation via SSH—Dynamic Network Configuration

This type of installation still requires some degree of physical access to the target system to boot for installation and determine the IP address of the installation target. The installation itself is entirely controlled from a remote workstation using VNC to connect to the installer, but still requires user interaction for the actual configuration efforts.

For this type of installation, make sure that the following requirements are met:

- Remote installation source: NFS, HTTP, FTP, or SMB with working network connection.
- Target system with working network connection.
- Controlling system with working network connection and working SSH client software.
- Physical boot medium (CD or DVD) for booting the target system.
- Running DHCP server providing IP addresses.

To perform this kind of installation, proceed as follows:

- 1 Set up the installation source as described in [Section 11.2, “Setting Up the Server Holding the Installation Sources”](#) (page 126). Choose an NFS, HTTP, or FTP network server. For an SMB installation source, refer to [Section 11.2.5, “Managing an SMB Installation Source”](#) (page 134).
- 2 Boot the target system using the first CD or DVD of the SUSE Linux Enterprise Desktop media kit.
- 3 When the boot screen of the target system appears, use the boot options prompt to pass the appropriate parameters for network connection, location of the installation source, and SSH enablement. See [Section 11.4.2, “Using Custom Boot Options”](#) (page 147) for detailed instructions on the use of these parameters.

The target system boots to a text-based environment, giving you the network address under which the graphical installation environment can be addressed by any SSH client.

- 4 On the controlling workstation, open a terminal window and connect to the target system as described in [Section “Connecting to the Installation Program”](#) (page 152).
- 5 Perform the installation as described in [Chapter 3, \*Installation with YaST\*](#) (page 17). Reconnect to the target system after it reboots for the final part of the installation.
- 6 Finish the installation.

## 11.1.6 Remote Installation via SSH—PXE Boot and Wake on LAN

This type of installation is completely hands-off. The target machine is started and booted remotely.

To perform this type of installation, make sure that the following requirements are met:

- Remote installation source: NFS, HTTP, FTP, or SMB with working network connection.
- TFTP server.
- Running DHCP server for your network, providing a static IP to the host to install.
- Target system capable of PXE boot, networking, and Wake on LAN, plugged in and connected to the network.
- Controlling system with working network connection and SSH client software.

To perform this type of installation, proceed as follows:

- 1 Set up the installation source as described in [Section 11.2, “Setting Up the Server Holding the Installation Sources”](#) (page 126). Choose an NFS, HTTP, or FTP network server. For the configuration of an SMB installation source, refer to [Section 11.2.5, “Managing an SMB Installation Source”](#) (page 134).
- 2 Set up a TFTP server to hold a boot image that can be pulled by the target system. This is described in [Section 11.3.2, “Setting Up a TFTP Server”](#) (page 139).
- 3 Set up a DHCP server to provide IP addresses to all machines and reveal the location of the TFTP server to the target system. This is described in [Section 11.3.1, “Setting Up a DHCP Server”](#) (page 136).
- 4 Prepare the target system for PXE boot. This is described in further detail in [Section 11.3.5, “Preparing the Target System for PXE Boot”](#) (page 145).
- 5 Initiate the boot process of the target system using Wake on LAN. This is described in [Section 11.3.7, “Wake on LAN”](#) (page 146).

- 6 On the controlling workstation, start an SSH client and connect to the target system as described in [Section 11.5.2, “SSH Installation”](#) (page 152).
- 7 Perform the installation as described in [Chapter 3, \*Installation with YaST\*](#) (page 17). Reconnect to the target system after it reboots for the final part of the installation.
- 8 Finish the installation.

## 11.2 Setting Up the Server Holding the Installation Sources

Depending on the operating system running on the machine to use as network installation source for SUSE Linux Enterprise Desktop, there are several options for the server configuration. The easiest way to set up an installation server is to use YaST on SUSE Linux Enterprise Server 11 or SUSE Linux 9.3 and higher.

---

### TIP

You can even use a Microsoft Windows machine as installation server for your Linux deployment. See [Section 11.2.5, “Managing an SMB Installation Source”](#) (page 134) for details.

---

### 11.2.1 Setting Up an Installation Server Using YaST

YaST offers a graphical tool for creating network installation sources. It supports HTTP, FTP, and NFS network installation servers.

- 1 Log in as `root` to the machine that should act as installation server.
- 2 Start *YaST > Miscellaneous > Installation Server*.
- 3 Select the server type (HTTP, FTP, or NFS). The selected server service is started automatically every time the system starts. If a service of the selected



type is already running on your system and you want to configure it manually for the server, deactivate the automatic configuration of the server service with *Do Not Configure Any Network Services*. In both cases, define the directory in which the installation data should be made available on the server.

- 4 Configure the required server type. This step relates to the automatic configuration of server services. It is skipped when automatic configuration is deactivated.

Define an alias for the root directory of the FTP or HTTP server on which the installation data should be found. The installation source will later be located under `ftp://Server-IP/Alias/Name` (FTP) or under `http://Server-IP/Alias/Name` (HTTP). *Name* stands for the name of the installation source, which is defined in the following step. If you selected NFS in the previous step, define wild cards and export options. The NFS server will be accessible under `nfs://Server-IP/Name`. Details of NFS and exports can be found in Chapter 25, *Sharing File Systems with NFS* (↑Administration Guide).

---

### **TIP: Firewall Settings**

Make sure that the firewall settings of your server system allow traffic on the ports for HTTP, NFS, and FTP. If they currently do not, start the YaST firewall module and open the respective ports.

---

- 5 Configure the installation source. Before the installation media are copied to their destination, define the name of the installation source (ideally, an easily remembered abbreviation of the product and version). YaST allows providing ISO images of the media instead of copies of the installation CDs. If you want this, activate the relevant check box and specify the directory path under which the ISO files can be found locally. Depending on the product to distribute using this installation server, it might be that more add-on CDs or service pack CDs are required and should be added as extra installation sources. To announce your installation server in the network via OpenSLP, activate the appropriate option.

---

**TIP**

Consider announcing your installation source via OpenSLP if your network setup supports this option. This saves you from entering the network installation path on every target machine. The target systems are just booted using the SLP boot option and find the network installation source without any further configuration. For details on this option, refer to [Section 11.4, “Booting the Target System for Installation”](#) (page 146).

---

- 6 Upload the installation data. The most lengthy step in configuring an installation server is copying the actual installation CDs. Insert the media in the sequence requested by YaST and wait for the copying procedure to end. When the sources have been fully copied, return to the overview of existing information sources and close the configuration by selecting *Finish*.

Your installation server is now fully configured and ready for service. It is automatically started every time the system is started. No further intervention is required. You only need to configure and start this service correctly by hand if you have deactivated the automatic configuration of the selected network service with YaST as an initial step.

To deactivate an installation source, select the installation source to remove then select *Delete*. The installation data are removed from the system. To deactivate the network service, use the respective YaST module.

If your installation server should provide the installation data for more than one product of product version, start the YaST installation server module and select *Add* in the overview of existing installation sources to configure the new installation source.

## 11.2.2 Setting Up an NFS Installation Source Manually

---

**IMPORTANT**

This assumes that you are using any kind of SUSE Linux-based operating system on the machine that will serve as installation server. If this is not the case, turn to the others vendor's documentation on NFS instead of following these directions.

---

Setting up an NFS source for installation is basically done in two steps. In the first step, create the directory structure holding the installation data and copy the installation media over to this structure. Second, export the directory holding the installation data to the network.

To create a directory holding the installation data, proceed as follows:

- 1** Log in as `root`.
- 2** Create a directory that should later hold all installation data and change into this directory. For example:

```
mkdir install/product/productversion
cd install/product/productversion
```

Replace *product* with an abbreviation of the product name and *productversion* with a string that contains the product name and version.

- 3** For each CD contained in the media kit execute the following commands:

- 3a** Copy the entire content of the installation CD into the installation server directory:

```
cp -a /media/path_to_your_CD-ROM_drive .
```

Replace *path\_to\_your\_CD-ROM\_drive* with the actual path under which your CD or DVD drive is addressed. Depending on the type of drive used in your system, this can be `cdrom`, `cdrecorder`, `dvd`, or `dvdrecorder`.

- 3b** Rename the directory to the CD number:

```
mv path_to_your_CD-ROM_drive CDx
```

Replace *x* with the actual number of your CD.

On SUSE Linux Enterprise Desktop, you can export the installation sources with NFS using YaST. Proceed as follows:

- 1** Log in as `root`.
- 2** Start *YaST > Network Services > NFS Server*.

- 3 Select *Start* and *Open Port in Firewall* and click *Next*.
- 4 Select *Add Directory* and browse for the directory containing the installation sources, in this case, *productversion*.
- 5 Select *Add Host* and enter the hostnames of the machines to which to export the installation data. Instead of specifying hostnames here, you could also use wild cards, ranges of network addresses, or just the domain name of your network. Enter the appropriate export options or leave the default, which works fine in most setups. For more information about the syntax used in exporting NFS shares, read the `exports` man page.
- 6 Click *Finish*. The NFS server holding the SUSE Linux Enterprise Desktop installation sources is automatically started and integrated into the boot process.

If you prefer manually exporting the installation sources via NFS instead of using the YaST NFS Server module, proceed as follows:

- 1 Log in as `root`.
- 2 Open the file `/etc/exports` and enter the following line:

```
productversion *(ro,root_squash,sync)
```

This exports the directory `/productversion` to any host that is part of this network or to any host that can connect to this server. To limit the access to this server, use netmasks or domain names instead of the general wild card `*`. Refer to the `export` man page for details. Save and exit this configuration file.

- 3 To add the NFS service to the list of servers started during system boot, execute the following commands:

```
insserv /etc/init.d/nfsserver
insserv /etc/init.d/portmap
```

- 4 Start the NFS server with `rcnfsserver start`. If you need to change the configuration of your NFS server later, modify the configuration file and restart the NFS daemon with `rcnfsserver restart`.

Announcing the NFS server via OpenSLP makes its address known to all clients in your network.

- 1 Log in as `root`.
- 2 Enter the directory `/etc/slp.reg.d/`.
- 3 Create a configuration file called `install.suse.nfs.reg` containing the following lines:

```
# Register the NFS Installation Server
service:install.suse:nfs://$HOSTNAME/path_to_instsource/CD1,en,65535
description=NFS Installation Source
```

Replace `path_to_instsource` with the actual path to the installation source on your server.

- 4 Save this configuration file and start the OpenSLP daemon with `rcslpd start`.

For more information about OpenSLP, refer to the package documentation located under `/usr/share/doc/packages/openslp/` or refer to Chapter 21, *SLP Services in the Network* (↑Administration Guide). More Information about NFS is found in Chapter 25, *Sharing File Systems with NFS* (↑Administration Guide).

## 11.2.3 Setting Up an FTP Installation Source Manually

Creating an FTP installation source is very similar to creating an NFS installation source. FTP installation sources can be announced over the network using OpenSLP as well.

- 1 Create a directory holding the installation sources as described in [Section 11.2.2, “Setting Up an NFS Installation Source Manually”](#) (page 128).
- 2 Configure the FTP server to distribute the contents of your installation directory:
  - 2a Log in as `root` and install the package `vsftpd` using the YaST package manager.
  - 2b Enter the FTP server root directory:

```
cd /srv/ftp
```

- 2c** Create a subdirectory holding the installation sources in the FTP root directory:

```
mkdir instsource
```

Replace *instsource* with the product name.

- 2d** Mount the contents of the installation repository into the change root environment of the FTP server:

```
mount --bind path_to_instsource /srv/ftp/instsource
```

Replace *path\_to\_instsource* and *instsource* with values matching your setup. If you need to make this permanent, add it to */etc/fstab*.

- 2e** Start vsftpd with vsftpd.

- 3** Announce the installation source via OpenSLP, if this is supported by your network setup:

- 3a** Create a configuration file called *install.suse.ftp.reg* under */etc/slp.reg.d/* that contains the following lines:

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/srv/ftp/instsource/CD1,en,65535
description=FTP Installation Source
```

Replace *instsource* with the actual name to the installation source directory on your server. The *service:* line should be entered as one continuous line.

- 3b** Save this configuration file and start the OpenSLP daemon with *rcslpd start*.

## 11.2.4 Setting Up an HTTP Installation Source Manually

Creating an HTTP installation source is very similar to creating an NFS installation source. HTTP installation sources can be announced over the network using OpenSLP as well.

- 1 Create a directory holding the installation sources as described in [Section 11.2.2, “Setting Up an NFS Installation Source Manually”](#) (page 128).
- 2 Configure the HTTP server to distribute the contents of your installation directory:

**2a** Install the Web server Apache.

**2b** Enter the root directory of the HTTP server (`/srv/www/htdocs`) and create a subdirectory that will hold the installation sources:

```
mkdir instsource
```

Replace *instsource* with the product name.

**2c** Create a symbolic link from the location of the installation sources to the root directory of the Web server (`/srv/www/htdocs`):

```
ln -s /path_instsource /srv/www/htdocs/instsource
```

**2d** Modify the configuration file of the HTTP server (`/etc/apache2/default-server.conf`) to make it follow symbolic links. Replace the following line:

```
Options None
```

with

```
Options Indexes FollowSymLinks
```

**2e** Reload the HTTP server configuration using `rcapache2 reload`.

- 3 Announce the installation source via OpenSLP, if this is supported by your network setup:

- 3a** Create a configuration file called `install.suse.http.reg` under `/etc/slp.reg.d/` that contains the following lines:

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/srv/www/htdocs/instsource/CD1/,en,65535
description=HTTP Installation Source
```

Replace *instsource* with the actual path to the installation source on your server. The `service:` line should be entered as one continuous line.

- 3b** Save this configuration file and start the OpenSLP daemon using `rcslpd restart`.

## 11.2.5 Managing an SMB Installation Source

Using SMB, you can import the installation sources from a Microsoft Windows server and start your Linux deployment even with no Linux machine around.

To set up an exported Windows Share holding your SUSE Linux Enterprise Desktop installation sources, proceed as follows:

- 1** Log in to your Windows machine.
- 2** Start Explorer and create a new folder that will hold the entire installation tree and name it `INSTALL`, for example.
- 3** Export this share according to the procedure outlined in your Windows documentation.
- 4** Enter this share and create a subfolder, called *product*. Replace *product* with the actual product name.
- 5** Enter the `INSTALL/product` folder and copy each CD or DVD to a separate folder, such as `CD1` and `CD2`.



To use a SMB mounted share as installation source, proceed as follows:

- 1 Boot the installation target.
- 2 Select *Installation*.
- 3 Press F4 for a selection of installation sources.
- 4 Choose SMB and enter the Windows machine's name or IP address, the share name (`INSTALL/product/CD1`, in this example), username, and password.

After you hit Enter, YaST starts and you can perform the installation.

## 11.2.6 Using ISO Images of the Installation Media on the Server

Instead of copying physical media into your server directory manually, you can also mount the ISO images of the installation media into your installation server and use them as installation source. To set up an HTTP, NFS or FTP server that uses ISO images instead of media copies, proceed as follows:

- 1 Download the ISO images and save them to the machine to use as the installation server.
- 2 Log in as `root`.
- 3 Choose and create an appropriate location for the installation data, as described in [Section 11.2.2, “Setting Up an NFS Installation Source Manually”](#) (page 128), [Section 11.2.3, “Setting Up an FTP Installation Source Manually”](#) (page 131), or [Section 11.2.4, “Setting Up an HTTP Installation Source Manually”](#) (page 133).
- 4 Create subdirectories for each CD or DVD.
- 5 To mount and unpack each ISO image to the final location, issue the following command:

```
mount -o loop path_to_iso path_to_instsource/product/mediumx
```

Replace *path\_to\_iso* with the path to your local copy of the ISO image, *path\_to\_instsource* with the source directory of your server, *product* with the product name, and *mediumx* with the type (CD or DVD) and number of media you are using.

- 6 Repeat the previous step to mount all ISO images needed for your product.
- 7 Start your installation server as usual, as described in [Section 11.2.2, “Setting Up an NFS Installation Source Manually”](#) (page 128), [Section 11.2.3, “Setting Up an FTP Installation Source Manually”](#) (page 131), or [Section 11.2.4, “Setting Up an HTTP Installation Source Manually”](#) (page 133).

To automatically mount the ISO images at boot time, add the respective mount entries to `/etc/fstab`. An entry according to the previous example would look like the following:

```
path_to_iso path_to_instsource/product
medium auto loop
```

## 11.3 Preparing the Boot of the Target System

This section covers the configuration tasks needed in complex boot scenarios. It contains ready-to-apply configuration examples for DHCP, PXE boot, TFTP, and Wake on LAN.

### 11.3.1 Setting Up a DHCP Server

There are two ways to set up a DHCP server. For SUSE Linux Enterprise Desktop, YaST provides a graphical interface to the process. Users can also manually edit the configuration files.

#### Setting Up a DHCP Server with YaST

To announce the TFTP server's location to the network clients and specify the boot image file the installation target should use, add two declarations to your DHCP server configuration.

- 1 Log in as `root` to the machine hosting the DHCP server.
- 2 Start *YaST* > *Network Services* > *DHCP Server*.
- 3 Complete the setup wizard for basic DHCP server setup.
- 4 Select *Expert Settings* and select *Yes* when warned about leaving the start-up dialog.
- 5 In the *Configured Declarations* dialog, select the subnet in which the new system should be located and click *Edit*.
- 6 In the *Subnet Configuration* dialog select *Add* to add a new option to the subnet's configuration.
- 7 Select `filename` and enter `pxelinux.0` as the value.
- 8 Add another option (`next-server`) and set its value to the address of the TFTP server.
- 9 Select *OK* and *Finish* to complete the DHCP server configuration.

To configure DHCP to provide a static IP address to a specific host, enter the *Expert Settings* of the DHCP server configuration module (**Step 4** (page 137)) and add a new declaration of the host type. Add the options `hardware` and `fixed-address` to this host declaration and provide the appropriate values.

## Setting Up a DHCP Server Manually

All the DHCP server needs to do, apart from providing automatic address allocation to your network clients, is to announce the IP address of the TFTP server and the file that should be pulled in by the installation routines on the target machine.

- 1 Log in as `root` to the machine hosting the DHCP server.
- 2 Append the following lines to a subnet configuration of your DHCP server's configuration file located under `/etc/dhcpd.conf`:

```
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range dynamic-bootp 192.168.1.200 192.168.1.228;  
    # PXE related stuff
```

```
#
# "next-server" defines the tftp server that will be used
next-server ip_tftp_server:
#
# "filename" specifies the pxelinux image on the tftp server
# the server runs in chroot under /srv/tftpboot
filename "pxelinux.0";
}
```

Replace *ip\_of\_the\_tftp\_server* with the actual IP address of the TFTP server. For more information about the options available in `dhcpd.conf`, refer to the `dhcpd.conf` manual page.

### 3 Restart the DHCP server by executing `rcdhcpd restart`.

If you plan on using SSH for the remote control of a PXE and Wake on LAN installation, explicitly specify the IP address DHCP should provide to the installation target. To achieve this, modify the above-mentioned DHCP configuration according to the following example:

```
group {
    # PXE related stuff
    #
    # "next-server" defines the tftp server that will be used
    next-server ip_tftp_server:
    #
    # "filename" specifies the pxelinux image on the tftp server
    # the server runs in chroot under /srv/tftpboot
    filename "pxelinux.0";
    host test {
        hardware ethernet mac_address;
        fixed-address some_ip_address;
    }
}
```

The host statement introduces the hostname of the installation target. To bind the hostname and IP address to a specific host, you must know and specify the system's hardware (MAC) address. Replace all the variables used in this example with the actual values that match your environment.

After restarting the DHCP server, it provides a static IP to the host specified, enabling you to connect to the system via SSH.

## 11.3.2 Setting Up a TFTP Server

Set up a TFTP server with YaST on SUSE Linux Enterprise Server and SUSE Linux Enterprise Desktop or set it up manually on any other Linux operating system that supports `xinetd` and `tftp`. The TFTP server delivers the boot image to the target system once it boots and sends a request for it.

### Setting Up a TFTP Server Using YaST

- 1 Log in as `root`.
- 2 Start *YaST > Network Services > TFTP Server* and install the requested package.
- 3 Click *Enable* to make sure that the server is started and included in the boot routines. No further action from your side is required to secure this. `xinetd` starts `tftpd` at boot time.
- 4 Click *Open Port in Firewall* to open the appropriate port in the firewall running on your machine. If there is no firewall running on your server, this option is not available.
- 5 Click *Browse* to browse for the boot image directory. The default directory `/tftpboot` is created and selected automatically.
- 6 Click *Finish* to apply your settings and start the server.

### Setting Up a TFTP Server Manually

- 1 Log in as `root` and install the packages `tftp` and `xinetd`.
- 2 If unavailable, create `/srv/tftpboot` and `/srv/tftpboot/pxelinux.cfg` directories.
- 3 Add the appropriate files needed for the boot image as described in [Section 11.3.3, “Using PXE Boot”](#) (page 140).
- 4 Modify the configuration of `xinetd` located under `/etc/xinetd.d/` to make sure that the TFTP server is started on boot:

**4a** If it does not exist, create a file called `tftp` under this directory with `touch tftp`. Then run `chmod 755 tftp`.

**4b** Open the file `tftp` and add the following lines:

```
service tftp
{
    socket_type          = dgram
    protocol             = udp
    wait                 = yes
    user                 = root
    server               = /usr/sbin/in.tftpd
    server_args          = -s /srv/tftpboot
    disable              = no
}
```

**4c** Save the file and restart `xinetd` with `rcxinetd restart`.

## 11.3.3 Using PXE Boot

Some technical background information as well as PXE's complete specifications are available in the Preboot Execution Environment (PXE) Specification (<http://www.pix.net/software/pxeboot/archive/pxespec.pdf>).

**1** Change to the directory `boot/<architecture>/loader` of your installation repository and copy the `linux`, `initrd`, `message`, `biostest`, and `memtest` files to the `/srv/tftpboot` directory by entering the following:

```
cp -a linux initrd message biostest memtest /srv/tftpboot
```

**2** Install the `syslinux` package directly from your installation CDs or DVDs with YaST.

**3** Copy the `/usr/share/syslinux/pxelinux.0` file to the `/srv/tftpboot` directory by entering the following:

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

- 4 Change to the directory of your installation repository and copy the `isolinux.cfg` file to `/srv/tftpboot/pxelinux.cfg/default` by entering the following:

```
cp -a boot/<architecture>/loader/isolinux.cfg  
/srv/tftpboot/pxelinux.cfg/default
```

- 5 Edit the `/srv/tftpboot/pxelinux.cfg/default` file and remove the lines beginning with `gfxboot`, `readinfo`, and `framebuffer`.
- 6 Insert the following entries in the append lines of the default `failsafe` and `apic` labels:

```
insmod=kernel module
```

By means of this entry, enter the network kernel module needed to support network installation on the PXE client. Replace *kernel module* with the appropriate module name for your network device.

```
netdevice=interface
```

This entry defines the client's network interface that must be used for the network installation. It is only necessary if the client is equipped with several network cards and must be adapted accordingly. In case of a single network card, this entry can be omitted.

```
install=nfs://ip_instserver/path_instsource/CD1
```

This entry defines the NFS server and the installation source for the client installation. Replace *ip\_instserver* with the actual IP address of your installation server. *path\_instsource* should be replaced with the actual path to the installation sources. HTTP, FTP, or SMB sources are addressed in a similar manner, except for the protocol prefix, which should read `http`, `ftp`, or `smb`.

---

## IMPORTANT

If you need to pass other boot options to the installation routines, such as SSH or VNC boot parameters, append them to the `install` entry. An overview of parameters and some examples are given in [Section 11.4, “Booting the Target System for Installation”](#) (page 146).

---

---

## TIP: Changing Kernel and Initrd Filenames

It is possible to use different filenames for kernel and initrd images. This is useful if you want to provide different operating systems from the same boot server. However, you should be aware, that only one dot is permitted in the filenames that are provided by tftp for the pxe boot.

---

An example `/srv/tftpboot/pxelinux.cfg/default` file follows. Adjust the protocol prefix for the installation source to match your network setup and specify your preferred method of connecting to the installer by adding the `vnc` and `vncpassword` or the `useshh` and `sshpassword` options to the `install` entry. The lines separated by `\` must be entered as one continuous line without a line break and without the `\`.

```
default harddisk

# default
label linux
    kernel linux
    append initrd=initrd ramdisk_size=65536 \
        install=nfs://ip_instserver/path_instsource/product/DVD1

# repair
label repair
    kernel linux
    append initrd=initrd splash=silent repair=1 showopts

# rescue
label rescue
    kernel linux
    append initrd=initrd ramdisk_size=65536 rescue=1

# bios test
label firmware
    kernel linux
    append initrd=biostest,initrd splash=silent
install=exec:/bin/run_biostest showopts

# memory test
label memtest
    kernel memtest

# hard disk
label harddisk
    localboot 0

implicit      0
display       message
```



```
prompt      1
timeout     100
```

Replace *ip\_instserver* and *path\_instsource* with the values used in your setup.

The following section serves as a short reference to the PXELINUX options used in this setup. Find more information about the options available in the documentation of the `syslinux` package located under `/usr/share/doc/packages/syslinux/`.

## 11.3.4 PXELINUX Configuration Options

The options listed here are a subset of all the options available for the PXELINUX configuration file.

`DEFAULT kernel options...`

Sets the default kernel command line. If PXELINUX boots automatically, it acts as if the entries after `DEFAULT` had been typed in at the boot prompt, except the `auto` option is automatically added, indicating an automatic boot.

If no configuration file is present or no `DEFAULT` entry is present in the configuration file, the default is the kernel name “linux” with no options.

`APPEND options...`

Add one or more options to the kernel command line. These are added for both automatic and manual boots. The options are added at the very beginning of the kernel command line, usually permitting explicitly entered kernel options to override them.

`LABEL label KERNEL image APPEND options...`

Indicates that if *label* is entered as the kernel to boot, PXELINUX should instead boot *image* and the specified `APPEND` options should be used instead of the ones specified in the global section of the file (before the first `LABEL` command). The default for *image* is the same as *label* and, if no `APPEND` is given, the default is to use the global entry (if any). Up to 128 `LABEL` entries are permitted.

Note that GRUB uses the following syntax:

```
title mytitle
    kernel my_kernel my_kernel_options
    initrd myinitrd
```

PXELINUX uses the following syntax:

```
label mylabel
    kernel mykernel
    append myoptions
```

Labels are mangled as if they were filenames and they must be unique after mangling. For example, the two labels “v2.1.30” and “v2.1.31” would not be distinguishable under PXELINUX because both mangle to the same DOS filename.

The kernel does not have to be a Linux kernel; it can be a boot sector or a COM-BOOT file.

APPEND -

Append nothing. APPEND with a single hyphen as argument in a LABEL section can be used to override a global APPEND.

LOCALBOOT *type*

On PXELINUX, specifying LOCALBOOT 0 instead of a KERNEL option means invoking this particular label and causes a local disk boot instead of a kernel boot.

Argument	Description
0	Perform a normal boot
4	Perform a local boot with the Universal Network Driver Interface (UNDI) driver still resident in memory
5	Perform a local boot with the entire PXE stack, including the UNDI driver, still resident in memory

All other values are undefined. If you do not know what the UNDI or PXE stacks are, specify 0.

TIMEOUT *time-out*

Indicates how long to wait at the boot prompt until booting automatically, in units of 1/10 second. The time-out is canceled as soon as the user types anything on the

keyboard, assuming the user will complete the command begun. A time-out of zero disables the time-out completely (this is also the default). The maximum possible time-out value is 35996 (just less than one hour).

PROMPT *flag\_val*

If *flag\_val* is 0, displays the boot prompt only if Shift or Alt is pressed or Caps Lock or Scroll Lock is set (this is the default). If *flag\_val* is 1, always displays the boot prompt.

F2 *filename*  
F1 *filename*  
...etc...  
F9 *filename*  
F10 *filename*

Displays the indicated file on the screen when a function key is pressed at the boot prompt. This can be used to implement preboot online help (presumably for the kernel command line options). For backward compatibility with earlier releases, F10 can be also entered as F0. Note that there is currently no way to bind filenames to F11 and F12.

## 11.3.5 Preparing the Target System for PXE Boot

Prepare the system's BIOS for PXE boot by including the PXE option in the BIOS boot order.

---

### WARNING: BIOS Boot Order

Do not place the PXE option ahead of the hard disk boot option in the BIOS. Otherwise this system would try to reinstall itself every time you boot it.

---

## 11.3.6 Preparing the Target System for Wake on LAN

Wake on LAN (WOL) requires the appropriate BIOS option to be enabled prior to the installation. Also, note down the MAC address of the target system. This data is needed to initiate Wake on LAN.

## 11.3.7 Wake on LAN

Wake on LAN allows a machine to be turned on by a special network packet containing the machine's MAC address. Because every machine in the world has a unique MAC identifier, you do not need to worry about accidentally turning on the wrong machine.

---

### IMPORTANT: Wake on LAN across Different Network Segments

If the controlling machine is not located in the same network segment as the installation target that should be awakened, either configure the WOL requests to be sent as multicasts or remotely control a machine on that network segment to act as the sender of these requests.

---

Users of SUSE Linux Enterprise Server can use a YaST module called WOL to easily configure Wake on LAN. Users of other versions of SUSE Linux-based operating systems can use a command line tool.

## 11.3.8 Wake on LAN with YaST

- 1 Log in as `root`.
- 2 Start *YaST > Network Services > WOL*.
- 3 Click *Add* and enter the hostname and MAC address of the target system.
- 4 To turn on this machine, select the appropriate entry and click *Wake up*.

## 11.4 Booting the Target System for Installation

Basically, there are two different ways to customize the boot process for installation apart from those mentioned under [Section 11.3.7, “Wake on LAN”](#) (page 146) and [Section 11.3.3, “Using PXE Boot”](#) (page 140). You can either use the default boot options and function keys or use the boot options prompt of the installation boot screen to pass any boot options that the installation kernel might need on this particular hardware.

## 11.4.1 Using the Default Boot Options

The boot options are described in detail in [Chapter 3, \*Installation with YaST\*](#) (page 17). Generally, just selecting *Installation* starts the installation boot process.

If problems occur, use *Installation—ACPI Disabled* or *Installation—Safe Settings*. For more information about troubleshooting the installation process, refer to Section “Installation Problems” (Chapter 7, *Common Problems and Their Solutions*, ↑System Analysis and Tuning Guide).

The menu bar at the bottom screen offers some advanced functionality needed in some setups. Using the F keys, you can specify additional options to pass to the installation routines without having to know the detailed syntax of these parameters (see [Section 11.4.2, “Using Custom Boot Options”](#) (page 147)). A detailed description of the available function keys is available at [Section 3.4, “The Boot Screen”](#) (page 21).

## 11.4.2 Using Custom Boot Options

Using the appropriate set of boot options helps facilitate your installation procedure. Many parameters can also be configured later using the `linuxrc` routines, but using the boot options is easier. In some automated setups, the boot options can be provided with `initrd` or an `info` file.

The following table lists all installation scenarios mentioned in this chapter with the required parameters for booting and the corresponding boot options. Just append all of them in the order they appear in this table to get one boot option string that is handed to the installation routines. For example (all in one line):

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

Replace all the values `...` in this string with the values appropriate for your setup.

**Table 11.1** *Installation (Boot) Scenarios Used in This Chapter*

Installation Scenario	Parameters Needed for Booting	Boot Options
<i>Chapter 3, <b>Installation with YaST</b></i> (page 17)	None: system boots automatically	None needed
<i>Section 11.1.1, “Simple Remote Installation via VNC—Static Network Configuration”</i> (page 118)	<ul style="list-style-type: none"><li>• Location of the installation server</li><li>• Network device</li><li>• IP address</li><li>• Netmask</li><li>• Gateway</li><li>• VNC enablement</li><li>• VNC password</li></ul>	<ul style="list-style-type: none"><li>• <code>install=(nfs,http,ftp,smb) :///path_to_instmedia</code></li><li>• <code>netdevice=some_netdevice</code> (only needed if several network devices are available)</li><li>• <code>hostip=some_ip</code></li><li>• <code>netmask=some_netmask</code></li><li>• <code>gateway=ip_gateway</code></li><li>• <code>vnc=1</code></li><li>• <code>vncpassword=some_password</code></li></ul>
<i>Section 11.1.2, “Simple Remote Installation via VNC—Dynamic Network Configuration”</i> (page 119)	<ul style="list-style-type: none"><li>• Location of the installation server</li><li>• VNC enablement</li><li>• VNC password</li></ul>	<ul style="list-style-type: none"><li>• <code>install=(nfs,http,ftp,smb) :///path_to_instmedia</code></li><li>• <code>vnc=1</code></li><li>• <code>vncpassword=some_password</code></li></ul>
<i>Section 11.1.3, “Remote Installation via VNC—PXE Boot and Wake on LAN”</i> (page 121)	<ul style="list-style-type: none"><li>• Location of the installation server</li><li>• Location of the TFTP server</li><li>• VNC enablement</li><li>• VNC password</li></ul>	Not applicable; process managed through PXE and DHCP

Installation Scenario	Parameters Needed for Booting	Boot Options
<p>Section 11.1.4, “Simple Remote Installation via SSH—Static Network Configuration” (page 122)</p>	<ul style="list-style-type: none"> <li>• Location of the installation server</li> <li>• Network device</li> <li>• IP address</li> <li>• Netmask</li> <li>• Gateway</li> <li>• SSH enablement</li> <li>• SSH password</li> </ul>	<ul style="list-style-type: none"> <li>• <code>install=(nfs,http,ftp,smb) :///path_to_instmedia</code></li> <li>• <code>netdevice=some_netdevice</code> (only needed if several network devices are available)</li> <li>• <code>hostip=some_ip</code></li> <li>• <code>netmask=some_netmask</code></li> <li>• <code>gateway=ip_gateway</code></li> <li>• <code>usessh=1</code></li> <li>• <code>sshpassword=some_password</code></li> </ul>
<p>Section 11.1.5, “Simple Remote Installation via SSH—Dynamic Network Configuration” (page 123)</p>	<ul style="list-style-type: none"> <li>• Location of the installation server</li> <li>• SSH enablement</li> <li>• SSH password</li> </ul>	<ul style="list-style-type: none"> <li>• <code>install=(nfs,http,ftp,smb) :///path_to_instmedia</code></li> <li>• <code>usessh=1</code></li> <li>• <code>sshpassword=some_password</code></li> </ul>
<p>Section 11.1.6, “Remote Installation via SSH—PXE Boot and Wake on LAN” (page 125)</p>	<ul style="list-style-type: none"> <li>• Location of the installation server</li> <li>• Location of the TFTP server</li> <li>• SSH enablement</li> <li>• SSH password</li> </ul>	<p>Not applicable; process managed through PXE and DHCP</p>

---

**TIP: More Information about linuxrc Boot Options**

Find more information about the linuxrc boot options used for booting a Linux system in `/usr/share/doc/packages/linuxrc/linuxrc.html`.

---

## 11.5 Monitoring the Installation Process

There are several options for remotely monitoring the installation process. If the proper boot options have been specified while booting for installation, either VNC or SSH can be used to control the installation and system configuration from a remote workstation.

### 11.5.1 VNC Installation

Using any VNC viewer software, you can remotely control the installation of SUSE Linux Enterprise Desktop from virtually any operating system. This section introduces the setup using a VNC viewer application or a Web browser.

#### Preparing for VNC Installation

All you need to do on the installation target to prepare for a VNC installation is to provide the appropriate boot options at the initial boot for installation (see [Section 11.4.2, “Using Custom Boot Options”](#) (page 147)). The target system boots into a text-based environment and waits for a VNC client to connect to the installation program.

The installation program announces the IP address and display number needed to connect for installation. If you have physical access to the target system, this information is provided right after the system booted for installation. Enter this data when your VNC client software prompts for it and provide your VNC password.

Because the installation target announces itself via OpenSLP, you can retrieve the address information of the installation target via an SLP browser without the need for any physical contact to the installation itself provided your network setup and all machines support OpenSLP:



- 1 Start the KDE file and Web browser Konqueror.
- 2 Enter `service://yast.installation.suse` in the location bar. The target system then appears as an icon in the Konqueror screen. Clicking this icon launches the KDE VNC viewer in which to perform the installation. Alternatively, run your VNC viewer software with the IP address provided and add `:1` at the end of the IP address for the display the installation is running on.

## Connecting to the Installation Program

Basically, there are two ways to connect to a VNC server (the installation target in this case). You can either start an independent VNC viewer application on any operating system or connect using a Java-enabled Web browser.

Using VNC, you can control the installation of a Linux system from any other operating system, including other Linux flavors, Windows, or Mac OS.

On a Linux machine, make sure that the package `tightvnc` is installed. On a Windows machine, install the Windows port of this application, which can be obtained at the TightVNC home page (<http://www.tightvnc.com/download.html>).

To connect to the installation program running on the target machine, proceed as follows:

- 1 Start the VNC viewer.
- 2 Enter the IP address and display number of the installation target as provided by the SLP browser or the installation program itself:

*ip\_address:display\_number*

A window opens on your desktop displaying the YaST screens as in a normal local installation.

Using a Web browser to connect to the installation program makes you totally independent of any VNC software or the underlying operating system. As long as the browser application has Java support enabled, you can use any browser (Firefox, Internet Explorer, Konqueror, Opera, etc.) to perform the installation of your Linux system.

To perform a VNC installation, proceed as follows:

- 1 Launch your preferred Web browser.

- 2 Enter the following at the address prompt:

```
http://ip_address_of_target:5801
```

- 3 Enter your VNC password when prompted to do so. The browser window now displays the YaST screens as in a normal local installation.

## 11.5.2 SSH Installation

Using SSH, you can remotely control the installation of your Linux machine using any SSH client software.

### Preparing for SSH Installation

Apart from installing the appropriate software package (OpenSSH for Linux and PuTTY for Windows), you just need to pass the appropriate boot options to enable SSH for installation. See [Section 11.4.2, “Using Custom Boot Options”](#) (page 147) for details. OpenSSH is installed by default on any SUSE Linux–based operating system.

### Connecting to the Installation Program

- 1 Retrieve the installation target's IP address. If you have physical access to the target machine, just take the IP address the installation routine provides at the console after the initial boot. Otherwise take the IP address that has been assigned to this particular host in the DHCP server configuration.

- 2 At a command line, enter the following command:

```
ssh -X root@ip_address_of_target
```

Replace *ip\_address\_of\_target* with the actual IP address of the installation target.

- 3 When prompted for a username, enter `root`.

- 4 When prompted for the password, enter the password that has been set with the SSH boot option. After you have successfully authenticated, a command line prompt for the installation target appears.
- 5 Enter `yast` to launch the installation program. A window opens showing the normal YaST screens as described in [Chapter 3, \*Installation with YaST\*](#) (page 17).



# Advanced Disk Setup

Sophisticated system configurations require particular disk setups. All common partitioning tasks can be done with YaST. To get persistent device naming with block devices, use the block devices below `/dev/disk/by-id` or `/dev/disk/by-uuid`. Logical Volume Management (LVM) is a disk partitioning scheme that is designed to be much more flexible than the physical partitioning used in standard setups. Its snapshot functionality enables easy creation of data backups. Redundant Array of Independent Disks (RAID) offers increased data integrity, performance, and fault tolerance.

## 12.1 Using the YaST Partitioner

With the expert partitioner, shown in [Figure 12.1, “The YaST Partitioner”](#) (page 156), manually modify the partitioning of one or several hard disks. Partitions can be added, deleted, resized, and edited. Also access the soft RAID and LVM configuration from this YaST module.

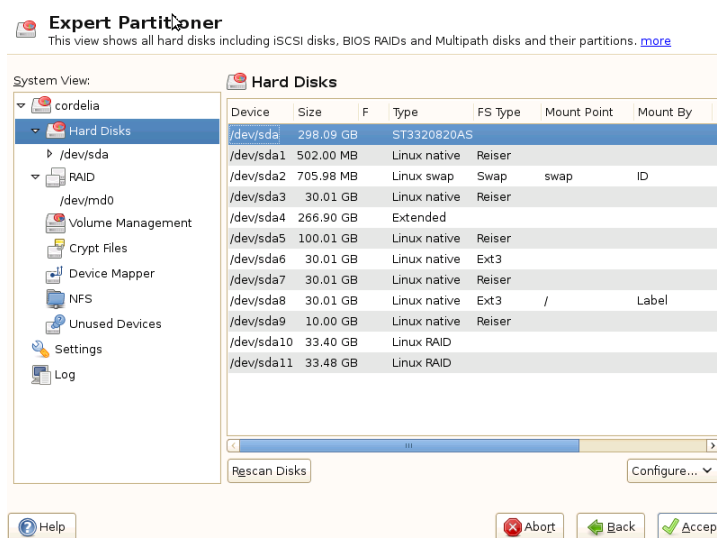
---

**WARNING: Repartitioning the Running System**

Although it is possible to repartition your system while it is running, the risk of making a mistake that causes data loss is very high. Try to avoid repartitioning your installed system and always do a complete backup of your data before attempting to do so.

---

**Figure 12.1** *The YaST Partitioner*



All existing or suggested partitions on all connected hard disks are displayed in the list of *Available Storage* in the YaST *Expert Partitioner* dialog. Entire hard disks are listed as devices without numbers, such as `/dev/sda`. Partitions are listed as parts of these devices, such as `/dev/sda1`. The size, type, file system, and mount point of the hard disks and their partitions are also displayed. The mount point describes where the partition appears in the Linux file system tree.

Several functional views are available on the lefthand *System View*. Use these views to gather information about existing storage configurations, or to configure functions like RAID, Volume Management, Crypt Files, or NFS.

If you run the expert dialog during installation, any free hard disk space is also listed and automatically selected. To provide more disk space to SUSE® Linux Enterprise Desktop, free the needed space starting from the bottom toward the top of the list (starting from the last partition of a hard disk toward the first). For example, if you have three partitions, you cannot use the second exclusively for SUSE Linux Enterprise Desktop and retain the third and first for other operating systems.

## 12.1.1 Partition Types

Every hard disk has a partition table with space for four entries. Every entry in the partition table corresponds to a primary partition or an extended partition. Only one extended partition entry is allowed, however.

A primary partition simply consists of a continuous range of cylinders (physical disk areas) assigned to a particular operating system. With primary partitions only, you would be limited to four partitions per hard disk, because more do not fit in the partition table. This is why extended partitions are used. Extended partitions are also continuous ranges of disk cylinders, but an extended partition may be subdivided into *logical partitions* itself. Logical partitions do not require entries in the partition table. In other words, an extended partition is a container for logical partitions.

If you need more than four partitions, create an extended partition as the fourth partition or earlier. This extended partition should span the entire remaining free cylinder range. Then create multiple logical partitions within the extended partition. The maximum number of logical partitions is 15 on SCSI, SATA, and Firewire disks and 63 on (E)IDE disks. It does not matter which types of partitions are used for Linux. Primary and logical partitions both work fine.

## 12.1.2 Creating a Partition

To create a partition from scratch select *Hard Disks* and then a hard disk with free space. The actual modification can be done in the *Partitions* tab:

- 1 Select *Add*. If several hard disks are connected, a selection dialog appears in which to select a hard disk for the new partition.
- 2 Specify the partition type (primary or extended). Create up to four primary partitions or up to three primary partitions and one extended partition. Within the extended partition, create several logical partitions (see [Section 12.1.1, “Partition Types”](#) (page 157)).
- 3 Select the file system to use and a mount point. YaST suggests a mount point for each partition created. To use a different mount method, like mount by label, select *Fstab Options*.

- 4 Specify additional file system options if your setup requires them. This is necessary, for example, if you need persistent device names. For details on the available options, refer to [Section 12.1.3, “Editing a Partition”](#) (page 158).
- 5 Click *OK > Apply* to apply your partitioning setup and leave the partitioning module.

If you created the partition during installation, you are returned to the installation overview screen.

## 12.1.3 Editing a Partition

When you create a new partition or modify an existing partition, set various parameters. For new partitions, suitable parameters are set by YaST and usually do not require any modification. To edit your partition setup manually, proceed as follows:

- 1 Select the partition.
- 2 Click *Edit* to edit the partition and set the parameters:

### File System ID

Even if you do not want to format the partition at this stage, assign it a file system ID to ensure that the partition is registered correctly. Possible values include *Linux*, *Linux swap*, *Linux LVM*, and *Linux RAID*.

### File System

Change the file system or format the partition here. Changing the file system or reformatting partitions irreversibly deletes all data from the partition.

Ext3 is the default file system for the Linux partitions. ReiserFS, JFS, XFS, and Ext3 are journaling file systems. These file systems are able to restore the system very quickly after a system crash, because write processes are logged during the operation. Furthermore, ReiserFS is very fast in handling lots of small files. Ext2 is not a journaling file system. However, it is rock solid and good for smaller partitions, because it does not require much disk space for management.

### Encrypt File System

If you activate the encryption, all data is written to the hard disk in encrypted form. This increases the security of sensitive data, but slightly reduces the



system speed, because the encryption takes some time. More information about the encryption of file systems is provided in Chapter 11, *Encrypting Partitions and Files* (↑Security Guide).

#### Fstab Options

Specify various parameters contained in the global file system administration file (`/etc/fstab`). The default settings should suffice for most setups. You can, for example, change the file system identification from the device name to a volume label. In the volume label, use all characters except `/` and space.

To get persistent devices names, use the mount option *Device ID*, *UUID* or *LABEL*. In SUSE Linux Enterprise Desktop, persistent device names are enabled by default.

When using the mount option *LABEL* to mount a partition, define an appropriate label for the selected partition. For example, you could use the partition label `HOME` for a partition intended to mount to `/home`.

If you intend to use quota on the file system, use the mount option *Enable Quota Support*. This must be done before you can define quotas for users in the YaST *User Management* module. For further information on how to configure user quota, refer to [Section 9.3.5, “Managing Quotas”](#) (page 100).

#### Mount Point

Specify the directory at which the partition should be mounted in the file system tree. Select from various YaST proposals or enter any other name.

- 3 Select *OK > Apply* to activate the partition.

---

### NOTE: Resize Filesystems

To resize an existing file system, select the partition and use *Resize*. Note, that it is not possible to resize partitions while mounted. To resize partitions, unmount the respective partition before running the partitioner.

---

## 12.1.4 More Partitioning Tips

The following section comprises a few hints and tips on partitioning that should help you in taking the right decisions while setting up your system.

---

### **TIP: Cylinder Numbers**

Note, that different partitioning tools may start counting the cylinders of a partition with 0 or with 1. When calculating the number of cylinders, you should always use the difference between the last and the first cylinder number and add one.

---

## **Using swap**

Swap is used to extend the physically available memory. This makes it possible to use more memory than physical ram available. The memory management system of kernels before 2.4.10 needed swap as a safety measure. In those times, if you did not have twice the size of your ram in swap, the performance of the system suffered. This does not hold true anymore as these limitations no longer exist.

Linux uses a page called “Least Recently Used” (LRU) to select pages that might be moved from memory to disk. Therefore, the running applications have more memory available and even their caching works more smoothly.

If an application tries to allocate as much memory as it can possibly get, there are some problems with swap. There are three major cases to look at:

### **System with no swap**

The application gets all memory that can be freed by any means. All caches are freed, and thus all other applications are slowed down. After a few minutes, the out of memory killer mechanism of the kernel will become active and kill the process.

### **System with medium sized swap (128 MB–512 MB)**

At first, the system is slowed down like a system without swap. After all physical ram has been used up, swap space is used as well. At this point, the system becomes very slow and it becomes impossible to run commands from remote. Depending on the speed of the hard disks that run the swap space, the system stays in this condition for about 10 to 15 minutes until the out of memory killer of the kernel

resolves the issue. Note, that you will need a certain amount of swap if the computer should perform a “suspend to disk”. In that case, the swap size should be reasonably big to contain the necessary data from memory (512 MB–1GB).

#### System with lots of swap (several GB)

It is better to not have an application that is running wild and swapping frantically, in this case. If you do have this problem, the system will need many hours to recover. In the process, it is likely that other processes get timeouts and faults, leaving the system in an undefined state, even if the faulty process is killed. In this case, reboot the machine hard and try to get it running again. Lots of swap is only useful if you have an application that relies on this feature. Such applications (like databases or graphics manipulation programs) often have an option to directly use hard disk space for their needs. It is advisable to use this option instead of using lots of swap space.

If your system does not run wild, but needs more swap after some time, it is possible to extend the swap space online. If you prepared a partition for swap space, just add this partition with YaST. If you do not have a partition available, you may also just use a swap file to extend the swap. Swap files are generally slower than partitions, but compared to physical ram, both are extremely slow and the actual speed difference is not as important as one would think in the first place.

#### **Procedure 12.1** *Adding a Swap File Manually*

To add a swap file in the running system, proceed as follows:

- 1 Create an empty file in your system. For example, if you want to add a swap file with 128 MB swap at `/var/lib/swap/swapfile`, use the commands:

```
mkdir -p /var/lib/swap
dd if=/dev/zero of=/var/lib/swap/swapfile bs=1M count=128
```

- 2 Initialize this swap file with the command

```
mkswap /var/lib/swap/swapfile
```

- 3 Activate the swap with the command

```
swapon /var/lib/swap/swapfile
```

To disable this swap file, use the command

```
swapoff /var/lib/swap/swapfile
```

- 4 Check the current available swap spaces with the command

```
cat /proc/swaps
```

Note, that at this point this is only temporary swap space. After the next reboot, it is not used anymore.

- 5 To enable this swap file permanently, add the following line to `/etc/fstab`:

```
/var/lib/swap/swapfile swap swap defaults 0 0
```

## 12.1.5 Partitioning and LVM

From the expert partitioner, access the LVM configuration with *Volume Management*. However, if a working LVM configuration already exists on your system, it is automatically activated as soon as you enter the LVM configuration for the first time in a session. In this case, any disks containing a partition belonging to an activated volume group cannot be repartitioned because the Linux kernel cannot reread the modified partition table of a hard disk when any partition on this disk is in use. However, if you already have a functioning LVM configuration on your system, physical repartitioning should not be necessary. Instead, change the configuration of the logical volumes.

At the beginning of the physical volumes (PVs), information about the volume is written to the partition. To reuse such a partition for other non-LVM purposes, it is advisable to delete the beginning of this volume. For example, in the VG system and PV `/dev/sda2`, do this with the command `dd if=/dev/zero of=/dev/sda2 bs=512 count=1`.

---

### **WARNING: File System for Booting**

The file system used for booting (the root file system or `/boot`) must not be stored on an LVM logical volume. Instead, store it on a normal physical partition.

---

For more details about LVM, see the *Storage Administration Guide*.

## 12.2 LVM Configuration

This section briefly describes the principles behind the Logical Volume Manager (LVM) and its basic features that make it useful under many circumstances. In [Section 12.2.2, “LVM Configuration with YaST”](#) (page 165), learn how to set up LVM with YaST.

---

### WARNING

Using LVM might be associated with increased risk, such as data loss. Risks also include application crashes, power failures, and faulty commands. Save your data before implementing LVM or reconfiguring volumes. Never work without a backup.

---

### 12.2.1 The Logical Volume Manager

The LVM enables flexible distribution of hard disk space over several file systems. It was developed because sometimes the need to change the segmentation of hard disk space arises only after the initial partitioning during installation has already been done. Because it is difficult to modify partitions on a running system, LVM provides a virtual pool (volume group, VG for short) of memory space from which logical volumes (LVs) can be created as needed. The operating system accesses these LVs instead of the physical partitions. Volume groups can span more than only one disk so that several disks or parts of them may constitute one single VG. This way, LVM provides a kind of abstraction from the physical disk space that allows its segmentation to be changed in a much easier and safer way than physical repartitioning does. Background information regarding physical partitioning can be found in [Section 12.1.1, “Partition Types”](#) (page 157) and [Section 12.1, “Using the YaST Partitioner”](#) (page 155).

**Figure 12.2** *Physical Partitioning versus LVM*

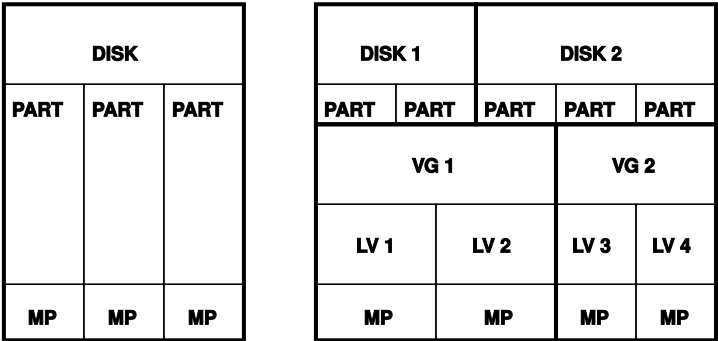


Figure 12.2, “Physical Partitioning versus LVM” (page 164) compares physical partitioning (left) with LVM segmentation (right). On the left side, one single disk has been divided into three physical partitions (PART), each with a mount point (MP) assigned so that the operating system can access them. On the right side, two disks have been divided into two and three physical partitions each. Two LVM volume groups (VG 1 and VG 2) have been defined. VG 1 contains two partitions from DISK 1 and one from DISK 2. VG 2 contains the remaining two partitions from DISK 2. In LVM, the physical disk partitions that are incorporated in a volume group are called physical volumes (PVs). Within the volume groups, four LVs (LV 1 through LV 4) have been defined, which can be used by the operating system via the associated mount points. The border between different LVs need not be aligned with any partition border. See the border between LV 1 and LV 2 in this example.

LVM features:

- Several hard disks or partitions can be combined in a large logical volume.
- Provided the configuration is suitable, an LV (such as `/usr`) can be enlarged when the free space is exhausted.
- Using LVM, it is possible to add hard disks or LVs in a running system. However, this requires hot-swappable hardware that is capable of such actions.
- It is possible to activate a "striping mode" that distributes the data stream of a LV over several PVs. If these PVs reside on different disks, this can improve the reading and writing performance just like RAID 0.

- The snapshot feature enables consistent backups (especially for servers) in the running system.

With these features, using LVM already makes sense for heavily used home PCs or small servers. If you have a growing data stock, as in the case of databases, music archives, or user directories, LVM is just the right thing for you. This would allow file systems that are larger than the physical hard disk. Another advantage of LVM is that up to 256 LVs can be added. However, keep in mind that working with LVM is different from working with conventional partitions. Instructions and further information about configuring LVM is available in the official LVM HOWTO at <http://tldp.org/HOWTO/LVM-HOWTO/>.

Starting from kernel version 2.6, LVM version 2 is available, which is downward-compatible with the previous LVM and enables the continued management of old volume groups. When creating new volume groups, decide whether to use the new format or the downward-compatible version. LVM 2 does not require any kernel patches. It makes use of the device mapper integrated in kernel 2.6. This kernel only supports LVM version 2. Therefore, when talking about LVM, this section always refers to LVM version 2.

## 12.2.2 LVM Configuration with YaST

The YaST LVM configuration can be reached from the YaST Expert Partitioner (see [Section 12.1, “Using the YaST Partitioner”](#) (page 155)) below *Volume Management*. The Expert Partitioner allows you to edit and delete existing partitions and also create new ones that should be used with LVM. The first task is to create PVs that provide space to a volume group:

- 1 Select a hard disk from *Hard Disks*.
- 2 Change to the *Partitions* tab.
- 3 Click *Add* and enter the desired size of the PV on this disk.
- 4 Use *Do not Format the Partition* and change the *File System ID* to *0x8E Linux LVM*. Do not mount this partition.
- 5 Repeat this procedure until you defined all the desired physical volumes on the available disks.

# Creating Volume Groups

If no volume group exists on your system yet, you have to add one (see [Figure 12.3](#), “Creating a Volume Group” (page 166)). It is possible to create additional groups with *Add Volume Group*, but usually one single volume group is sufficient.

- 1 Enter a name for the VG, e.g. `system`.
- 2 Select the desired *Physical Extend Size*. This value defines the size of a physical block in the volume group. All the disk space in a volume group is handled in chunks of this size.

---

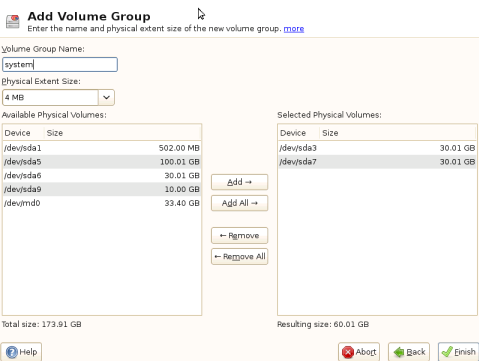
## TIP: Logical Volumes and Block Sizes

The possible size of a LV depends on the block size used in the volume group. The default is 4 MB and allows for a maximum size of 256 GB for physical and LVs. The physical extent size should be increased, for example, to 8, 16, or 32 MB, if you need LVs larger than 256 GB.

---

- 3 Add the prepared PVs to the VG by selecting the device and clicking on *Add*. Selecting several devices is possible by holding *Strg* pressed while selecting the devices.
- 4 Select *Finish* to make the VG available to further configuration steps.

**Figure 12.3** *Creating a Volume Group*



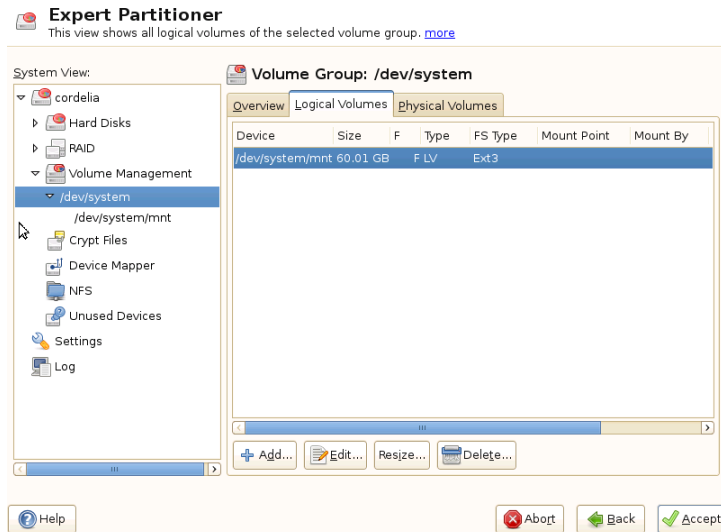


If you have multiple volume groups defined, and want to add or remove PVs, select the volume group in *Volume Management*. Then change to the *Overview* tab and select *Resize*. In the following menu, you can add or remove PVs to the selected volume group.

## Configuring Logical Volumes

After the volume group has been filled with PVs, define the LVs the operating system should use in the next dialog. Choose the current volume group and change to the *Logical Volumes* tab. *Add*, *Edit*, *Resize*, and *Delete* LVs as needed until all space in the volume group has been exhausted. Assign at least one LV to each volume group.

**Figure 12.4** *Logical Volume Management*



Click *Add* and go through the wizard-like popup that opens:

1. Enter the name of the LV. For a partition that should be mounted to `/home`, a selfexplaining name like `HOME` could be used.
2. Select the size and the number of stripes of the LV. If you have only one PV, selecting more than one stripes is not useful.
3. Choose the filesystem to use on the LV as well as the mount point.

By using stripes it is possible to distribute the data stream in the LV among several PVs (striping). If these PVs reside on different hard disks, this generally results in a better reading and writing performance (like RAID 0). However, a striping LV with  $n$  stripes can only be created correctly if the hard disk space required by the LV can be distributed evenly to  $n$  PVs. If, for example, only two PVs are available, a LV with three stripes is impossible.

---

**WARNING: Striping**

YaST has no chance at this point to verify the correctness of your entries concerning striping. Any mistake made here is apparent only later when the LVM is implemented on disk.

---

If you have already configured LVM on your system, the existing logical volumes can also be used. Before continuing, assign appropriate mount points to these LVs, too. With *Next*, return to the YaST Expert Partitioner and finish your work there.

## 12.3 Soft RAID Configuration

The purpose of RAID (redundant array of independent disks) is to combine several hard disk partitions into one large *virtual* hard disk to optimize performance, data security, or both. Most RAID controllers use the SCSI protocol because it can address a larger number of hard disks in a more effective way than the IDE protocol and is more suitable for parallel processing of commands. There are some RAID controllers that support IDE or SATA hard disks. Soft RAID provides the advantages of RAID systems without the additional cost of hardware RAID controllers. However, this requires some CPU time and has memory requirements that make it unsuitable for real high performance computers.

SUSE® Linux Enterprise Desktop offers the option of combining several hard disks into one soft RAID system with the help. RAID implies several strategies for combining several hard disks in a RAID system, each with different goals, advantages, and characteristics. These variations are commonly known as *RAID levels*.

Common RAID levels are:

## RAID 0

This level improves the performance of your data access by spreading out blocks of each file across multiple disk drives. Actually, this is not really a RAID, because it does not provide data backup, but the name *RAID 0* for this type of system has become the norm. With RAID 0, two or more hard disks are pooled together. The performance is very good, but the RAID system is destroyed and your data lost if even one hard disk fails.

## RAID 1

This level provides adequate security for your data, because the data is copied to another hard disk 1:1. This is known as *hard disk mirroring*. If a disk is destroyed, a copy of its contents is available on another one. All of them except one could be damaged without endangering your data. However, if damage is not detected, it also may happen that damaged data is mirrored to the correct disk and data corruption happens that way. The writing performance suffers a little in the copying process compared to when using single disk access (10 to 20 % slower), but read access is significantly faster in comparison to any one of the normal physical hard disks, because the data is duplicated so can be parallel scanned. Generally it can be said that Level 1 provides nearly twice the read transaction rate of single disks and almost the same write transaction rate as single disks.

## RAID 2 and RAID 3

These are not typical RAID implementations. Level 2 stripes data at the bit level rather than the block level. Level 3 provides byte-level striping with a dedicated parity disk and cannot service simultaneous multiple requests. Both levels are only rarely used.

## RAID 4

Level 4 provides block-level striping just like Level 0 combined with a dedicated parity disk. In the case of a data disk failure, the parity data is used to create a replacement disk. However, the parity disk may create a bottleneck for write access. Nevertheless, Level 4 is sometimes used.

## RAID 5

RAID 5 is an optimized compromise between Level 0 and Level 1 in terms of performance and redundancy. The hard disk space equals the number of disks used minus one. The data is distributed over the hard disks as with RAID 0. *Parity blocks*, created on one of the partitions, are there for security reasons. They are linked to each other with XOR, enabling the contents to be reconstructed by the corresponding parity block in case of system failure. With RAID 5, no more than one hard disk

can fail at the same time. If one hard disk fails, it must be replaced as soon as possible to avoid the risk of losing data.

#### Other RAID Levels

Several other RAID levels have been developed (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50, etc.), some of them being proprietary implementations created by hardware vendors. These levels are not very widespread, so are not explained here.

## 12.3.1 Soft RAID Configuration with YaST

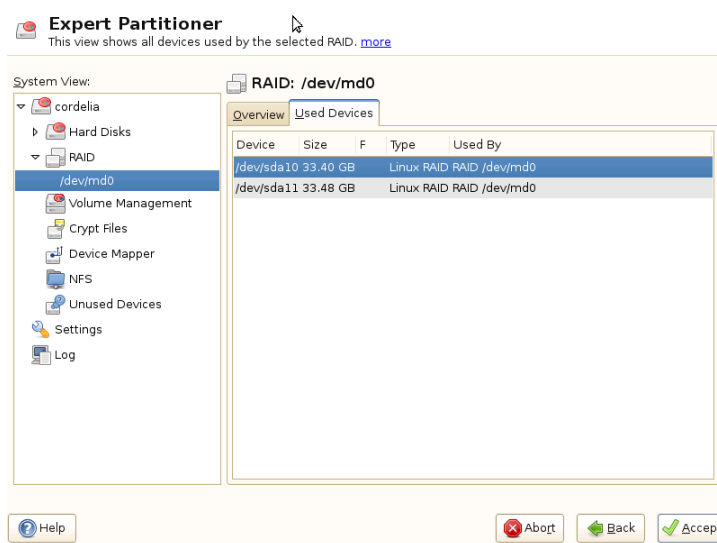
The YaST *RAID* configuration can be reached from the YaST Expert Partitioner, described in [Section 12.1, “Using the YaST Partitioner”](#) (page 155). This partitioning tool enables you to edit and delete existing partitions and create new ones that should be used with soft RAID. There, create RAID partitions:

- 1 Select a hard disk from *Hard Disks*.
- 2 Change to the *Partitions* tab.
- 3 Click *Add* and enter the desired size of the raid partition on this disk.
- 4 Use *Do not Format the Partition* and change the *File System ID* to *0xFD Linux RAID*. Do not mount this partition.
- 5 Repeat this procedure until you defined all the desired physical volumes on the available disks.

For RAID 0 and RAID 1, at least two partitions are needed—for RAID 1, usually exactly two and no more. If RAID 5 is used, at least three partitions are required. It is recommended to take only partitions of the same size. The RAID partitions should be located on different hard disks to decrease the risk of losing data if one is defective (RAID 1 and 5) and to optimize the performance of RAID 0. After creating all the partitions to use with RAID, click *RAID > Add RAID* to start the RAID configuration.

In the next dialog, choose between RAID levels 0, 1, and 5. Then, select all partitions with either the “Linux RAID” or “Linux native” type that should be used by the RAID system. No swap or DOS partitions are shown.

**Figure 12.5** RAID Partitions



To add a previously unassigned partition to the selected RAID volume, first click the partition then *Add*. Assign all partitions reserved for RAID. Otherwise, the space on the partition remains unused. After assigning all partitions, click *Next* to select the available *RAID Options*.

In the last step, set the file system to use as well as encryption and the mount point for the RAID volume. After completing the configuration with *Finish*, see the `/dev/md0` device and others indicated with *RAID* in the expert partitioner.

## 12.3.2 Troubleshooting

Check the file `/proc/mdstat` to find out whether a RAID partition has been damaged. In the event of a system failure, shut down your Linux system and replace the defective hard disk with a new one partitioned the same way. Then restart your system and enter the command `mdadm /dev/mdX --add /dev/sdX`. Replace 'X' with your particular device identifiers. This integrates the hard disk automatically into the RAID system and fully reconstructs it.

Note that although you can access all data during the rebuild, you may encounter some performance issues until the RAID has been fully rebuilt.

## 12.3.3 For More Information

Configuration instructions and more details for soft RAID can be found in the HOWTOs at:

- `/usr/share/doc/packages/mdadm/Software-RAID.HOWTO.html`
- <http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html>

Linux RAID mailing lists are also available, such as <http://marc.theaimsgroup.com/?l=linux-raid>.

# Subscription Management

Any machine running SUSE Linux Enterprise Server 11 or SUSE Linux Enterprise Desktop 11 can be configured to register against local Subscription Management Tool server and download software updates from there instead of communicating directly with the Novell Customer Center and the NU servers. To use an SMT server for client registration and as a local update source, you must configure the SMT server in your network first. The SMT server software is distributed as an add-on for SUSE Linux Enterprise Server and its configuration is described in the *Subscription Management Tool Guide*. There is no need to install any add-on on the clients to be configured to register against an SMT server.

To register a client against an SMT server, you need to equip the client with the server's URL. As client and server communicate via the HTTPS protocol during registration, you also need to make sure the client trusts the server's certificate. In case your SMT server is set up to use the default server certificate, the CA certificate will be available on the SMT server via HTTP protocol at `http://FQDN/smt.crt`. In this case you do not have to care about the certificate: The registration process will automatically download the CA certificate from there, unless configured otherwise. You have to enter a path to the server's CA certificate if the certificate was issued by an external certificate authority.

---

**NOTE: Registering Against \*.novell.com Subdomain**

If you try to register against any \*.novell.com subdomain, the certificate will not be downloaded during registration for security reasons, and certificate handling will not be done. In such a case, use a different domain name or a plain IP address.

---

There are several ways to provide this information and to configure the client machine to use SMT. The first way is to provide the needed information via kernel parameters at boot time. The second way is to configure clients using an AutoYaST profile. There is also a script distributed with Subscription Management Tool, `clientSetup4SMT.sh`, which can be run on a client to make it register against a specified SMT server. These methods are described in the following sections:

## 13.1 Using Kernel Parameters to Access an SMT Server

Any client can be configured to use SMT by providing the following kernel parameters during machine boot: `regurl` and `regcert`. The first parameter is mandatory, the latter is optional.

### `regurl`

URL of the SMT server. The URL needs to be in the following format:

`https://FQDN/center/regsvc/` with *FQDN* being the fully qualified hostname of the SMT server. It must be identical to the FQDN of the server certificate used on the SMT server. Example:

```
regurl=https://smt.example.com/center/regsvc/
```

### `regcert`

Location of the SMT server's CA certificate. Specify one of the following locations:

#### URL

Remote location (http, https or ftp) from which the certificate can be downloaded. Example:

```
regcert=http://smt.example.com/smt.crt
```

#### Floppy

Specifies a location on a floppy. The floppy has to be inserted at boot time—you will not be prompted to insert it if it is missing. The value has to start with the string `floppy`, followed by the path to the certificate. Example:

```
regcert=floppy/smt/smt-ca.crt
```

#### Local Path

Absolute path to the certificate on the local machine. Example:



```
regcert=/data/inst/smt/smt-ca.cert
```

#### Interactive

Use `ask` to open a pop-up menu during installation where you can specify the path to the certificate. Do not use this option with AutoYaST. Example:

```
regcert=ask
```

#### Deactivate Certificate Installation

Use `done` if either the certificate will be installed by an add-on product, or if you are using a certificate issued by an official certificate authority. Example:

```
regcert=done
```

---

### **WARNING: Beware of Typing Errors**

Make sure the values you enter are correct. If `regurl` has not been specified correctly, the registration of the update source will fail.

If a wrong value for `regcert` has been entered, you will be prompted for a local path to the certificate. In case `regcert` is not specified at all, it will default to `http://FQDN/smt.crt` with `FQDN` being the name of the SMT server.

---

### **WARNING: Change of SMT Server Certificate**

If the SMT server gets a new certificate from a new and untrusted CA, the clients need to fetch the new CA certificate file. This is done automatically with the registration process but only if a URL was used at installation time to fetch the certificate, or if the `regcert` parameter was omitted and thus, the default URL is used. If the certificate was loaded using any other method, such as floppy or local path, the CA certificate will not be updated.

---

## **13.2 Configuring Clients Using AutoYaST Profile**

Clients can be configured to register with SMT server via AutoYaST profile. For general information about creating AutoYaST profiles and preparing automatic installation,

refer to [Chapter 18, Automated Installation](#) (page 211). In this section, only SMT specific configuration is described.

To configure SMT specific data using AutoYaST, follow these steps:

- 1 As `root`, start YaST and select *Miscellaneous > Autoinstallation* to start the graphical AutoYaST front-end.

From a command line, you can start the graphical AutoYaST front-end with the `yast2 autoyast` command.

- 2 Open an existing profile using *File > Open*, create a profile based on the current system's configuration using *Tools > Create Reference Profile*, or just work with an empty profile.
- 3 Select *Support > Novell Customer Center Configuration*. An overview of the current configuration is shown.
- 4 Click *Edit*.
- 5 To register while installing automatically, select *Run Product Registration*. You can include information from your system with *Hardware Profile* and *Optional Information*.
- 6 Set the URL of the *SMT Server* and, optionally, the location of the *SMT Certificate*. The possible values are the same as for the kernel parameters `regurl` and `regcert` (see [Section 13.1, “Using Kernel Parameters to Access an SMT Server”](#) (page 174)). The only exception is, that the `ask` value for `regcert` does not work in AutoYaST, because it requires user interaction. If using it, the registration process will be skipped.
- 7 Perform all other configuration needed for the systems to be deployed.
- 8 Select *File > Save As* and enter a filename for the profile, such as `autoinst.xml`.

## 13.3 Configuring Clients Using the `clientSetup4SMT.sh` Script

The `/usr/share/doc/packages/smt/clientSetup4SMT.sh` script is provided with SMT. This script allows to configure a client machine to use a SMT server or to reconfigure it to use a different SMT server.

To configure a client machine to use SMT with the `clientSetup4SMT.sh` script, follow these steps:

- 1 Copy the `/usr/share/doc/packages/smt/clientSetup4SMT.sh` script from your SMT server to the client machine.
- 2 As root, execute the script on the client machine. The script can be executed in two ways. In the first case, the script name is followed by the registration URL: `./clientSetup4SMT.sh registration_URL`, for example, `./clientSetup4SMT.sh https://smt.example.com/center/regsvc`. In the second case, the script name is followed by the `--host` option followed by hostname of the SMT server: `./clientSetup4SMT.sh --host server_hostname`, for example, `./clientSetup4SMT.sh --host smt.example.com`.
- 3 The script downloads the server's CA certificate. Accept it by pressing `y`.
- 4 The script performs all necessary modifications on the client. However, the registration itself is not performed by the script.
- 5 Perform a registration by executing `suse_register` or running `yast2 inst_suse_register` module on the client.

## 13.4 Registering Clients Against SMT Test Environment

To configure a client to register against the test environment instead the production environment, modify `/etc/suseRegister.conf` on the client machine by setting:

```
register = command=register&testenv=1
```

For more information about using SMT with a test environment, refer to the *Subscription Management Tool Guide*.

## **Part II. Imaging and Creating Products**



# KIWI

KIWI is a system for creating operating system images. An image is a directory with a file containing the operating system, its applications and configurations, the filesystem structure of the OS, possible additional metadata, and depending on the image type, also disk geometry and partition table data. With KIWI you can create LiveCDs and LiveDVDs, USB sticks, virtual disk to play in full virtual systems like VMware, XEN images for paravirtualization in a hypervisor, and a PXE environment to boot from network.

## 14.1 Prerequisites for KIWI

To build images with KIWI, you need the following preconditions:

1. Free space, the more the better.
2. KIWI is split into several packages, targeted to different image types. In any case, you need the base package `kiwi`. Depending on your target image, you need the following packages:

Image Type	Package Name
Installation Media	<code>kiwi-desc-oemboot</code>
Virtualization	<code>kiwi-desc-xenboot</code>

Image Type	Package Name
USB Sticks	<code>kiwi-desc-usbboot</code>
Network Client	<code>kiwi-desc-netboot</code>

3. Install the `kiwi-doc` package. You can find some example configurations to get an idea about the structure and its content.
4. Know the KIWI configuration file and its structure. It is based on a RELAX NG schema and documented in the `kiwi` package under `/usr/share/doc/packages/kiwi/kiwi.html`. You need this document, if you want to create the configuration file from scratch or when you want to insert elements or attributes.

## 14.2 Knowing KIWI's Build Process

The building process of KIWI is separated into three steps:

1. **Physical Extend (Preparation)** This stage prepares the content of your new filesystem. During this step, the root directory is created, you determine which packages are installed on your image and which user configuration files are included.
2. **Logical Extend (Creation)** This stage requires a successful preparation step. The logical extend step creates the operating system image based on the first step.
3. **Deployment** The resulting image type can be deployed with different methods like installed on a hard disk or played by a virtualization system (VMware, Qemu, VirtualBox).

## 14.3 Image Description

KIWI needs an image description to build an image type. The image description is a directory which contains at least a file `config.xml`, or alternatively with the extension `*.kiwi`.



## 14.3.1 Contents of Image Description

The following table contains additional optional information. However, most of information is mandatory for the functionality of the later operating system:

**Table 14.1** *Additional Files and Directories For Image Description*

File/Directory	Description
<code>config/</code>	optional subdirectory. Contains Bash scripts which are executed after the installation of all the image packages.
<code>config.sh</code>	optional configuration script while creating the physical extend
<code>config.xml</code>	configuration file for each image description, explained in <a href="#">Section 14.3.2</a> (page 184)
<code>config-cdroot.tgz</code>	archive, only used for ISO images
<code>config-cdroot.sh</code>	manipulate extracted data from <code>config-cdroot.tgz</code>
<code>config-yast-autoyast.xml</code>	configuration file created by AutoYaST
<code>config-yast-firstboot.xml</code>	configuration file for controlling the YaST firstboot service
<code>images.sh</code>	optional configuration script while creating the preparation step
<code>root/</code>	contains other directories, special files, and scripts which are changed <i>after</i> the installation of all image packages

## 14.3.2 The config.xml File

All information about an image description is stored in the central configuration XML file `config.xml`. Each time KIWI is executed, `config.xml` is validated against an RELAX NG schema (see <http://www.relaxng.org> for more information about this schema language). Therefore it is recommended, to use a decent XML editor with RELAX NG support or to use the documentation about the schema in the HTML file `/usr/share/doc/packages/kiwi/schema/kiwi.xsd.html`.

The configuration file consists of several parts:

- some description about the author, contact information, and a short explanation.
- preferences option needed for the logical extent stage.
- information about the users, their name, their home directories, and their passwords.
- links to repositories.
- a list of packages that are used for the defined image type.
- and others, less important information which can be viewed in the above HTML file of the RELAX NG schema documentation.

An skeleton of the file is shown in the following example:

## Example 14.1 KIWI Configuration File

```
<image schemeversion="2.0" name="..."> ❶
  <description type="system"> ❷
    <author>...</author>
    <contact>...</contact>
    <specification>...</specification>
  </description>
  <preferences> ❸
    <type primary="true" boot="..." flags="...">iso</type>
    <type boot="..." filesystem="ext3" format="vmdk">vmx</type>
    <type boot="..." filesystem="ext3">xen</type>
    <type boot="..." filesystem="squashfs" flags="unified">oem</type>
    <version>2.7.0</version>
    <size unit="M">780</size>
    <packagemanager>zypper</packagemanager>
    <rpm-check-signatures>False</rpm-check-signatures>
    <rpm-force>False</rpm-force>
    <locale>en_US.UTF-8</locale>
    <oem-swap>no</oem-swap>
    <oem-boot-title>USB</oem-boot-title>
  </preferences>
  <users group="users"> ❹
    <user name="root" pwd="" home="/root"/>
  </users>
  <repository type="rpm-md"> ❺
    <source path="/home/rpmdir"/>
  </repository>
  <packages type="image" patternPackageType="onlyRequired"> ❻
    <package name="yast2-live-installer"/>
    <package name="pam"/>
    <!-- List of packages reduced -->
  </packages>
```

- ❶ The root element of every KIWI configuration file. Each file requires the version number. An optional `kiwirevision` attribute can be used to specify an SVN revision of KIWI.
- ❷ Contains a mandatory descriptions with information about the creator of this image descriptions, its contact address and some short explanation.
- ❸ Contains a mandatory preferences with information about the version of this image, the used package manager, the supported image types, and other settings.
- ❹ The optional `users` element contains a list of all users which are added to the image. The `user` element contains the name, the path to its home directory, password, and the shell.
- ❺ Contains a mandatory list of repositories used by the package manager.

- ⑥ Contains a mandatory list of packages which are included into the image.

More details about the configuration file is shown in the HTML page above.

## 14.4 Creating Appliances with KIWI

This section describes how to create appliances with KIWI. An appliance is a special designed operating system for a specific task. For example, you can create an appliance with the focus on office programs.

### 14.4.1 Creating a Local Installation Source

All examples in the `kiwi-doc` packages need a valid installation source to create an image. Usually the examples connect to a network resource. The higher the network bandwidth, the faster the image creation. If you do not have a fast network or you do not want to use it, create a local installation resource. Proceed as follows:

- 1 Collect your installation DVD.
- 2 Open a shell and become `root`.
- 3 Create the directory for your local installation directory. The examples use usually the path `/image/CDs/full-VERSION-ARCH`. Replace the placeholders `VERSION` and `ARCH` with the respective values.
- 4 Mount the medium. Replace the `DRIVE` placeholder with the respective device (usually `dvd`, `cdrom`, etc.):

```
mount -o loop /dev/DRIVE /mnt
```

- 5 Copy all the content of the medium into the installation directory:

```
cp -a /mnt/* /image/CDs/full-VERSION-ARCH
```

To use the local installation source, all you need to do is to enable it in the `repository` element:

```
<repository type="...">
  <!-- Remove the comment markers in the next line -->
  <!-- <source path="/image/CDs/full-VERSION-ARCH" -->
  <source path="opensuse://openSUSE:11.0/standard"/>
</repository>
```

## 14.4.2 Creating an Image

An image is a virtual disk image containing all partitions, boot loader information, and packages as it resides on a real disk. To create an ISO image, proceed as follows:

- 1 Install the packages `kiwi` and `kiwi-doc` and resolve any dependencies.
- 2 Open a shell and become `root`.
- 3 Copy the directory `/usr/share/doc/packages/kiwi/examples/suse-11.0/suse-oem-preload` to your current directory.
- 4 Open the file `config.xml` and locate the element `repository`. If you want to use a local installation source, refer to [Section 14.4.1](#) (page 186) for more information.
- 5 Execute KIWI with the following command to prepare the first stage (“physical extend”):

```
kiwi --prepare suse-oem-preload --root oem
```

- 6 Build the ISO image:

```
kiwi --create oem --type iso --destdir /tmp/myoem
```

## 14.4.3 Creating Preload Image with NFS

To create an image with NFS functionality, proceed as follows:

- 1 Open a shell and become `root`.
- 2 Copy the directory `/usr/share/doc/packages/kiwi/examples/suse-11.1/suse-oem-preload` to your current directory.

- 3 Open the file `suse-oem-preload/config.xml` and locate the `packages` element with the attribute `type="image"`.
- 4 Insert the following line between `<packages type="image">` and `</packages>` and save the file:  

```
<package name="nfs-client"/>
```
- 5 Rebuild the image as described in [Step 5](#) (page 187).

## 14.5 For More Information

Find more information about KIWI in the following documents:

- <http://developer.berlios.de/projects/kiwi>—Homepage of KIWI
- <file:///usr/share/doc/packages/kiwi/kiwi.pdf>—Extensive description about the KIWI Image System

# Creating Add-On Products With Add-on Creator

# 15

An Add-On is a special designed media, usually a CD or DVD, to extend your product. The Add-on Creator was developed to support our customers and partners and simplify third-party software distribution for all SUSE products.

## 15.1 Creating Images

To create a Add-On CD, proceed as follows:

- 1 Start YaST and open the *Add-On Creator* module. A window opens.
- 2 If you have not run this module before, click on *Create an Add-On from the Beginning* to start. In case you have already created an Add-On, the window shows a list of all created Add-Ons. Click *Add* to start.
- 3 Enter the product name and version of your Add-On and give some further options:
  - Choose the required product which is based upon.
  - Optionally select the path to additional Add-On packages. You need this, if you need further RPM packages which are not included in your base product.
  - Optionally select the path with the required product packages.

- 4 Correct the product definition and enter a vendor name. Disable *Show Only Required Keywords* to display more keywords.
- 5 Optionally change the package descriptions. Use *Add Language* to insert a new language and add translated descriptions.
- 6 Optionally add new patterns. With patterns you can group your RPM packages. Use *New* to add a new pattern name and change the respective attributes in the list below.
- 7 Modify the output settings. Enter a path to your output directory and optionally change the name of the ISO name. Additionally, you can modify further features:
  - Use *Configure Workflow...* to enter files to customize your product workflow.
  - Use *Optional Files...* to add files to your Add-On product. The first part can be used to insert information about the Add-On in the `info.txt` file. Use the license files to display a window with *Agree* and *Disagree* buttons before the installation starts. More files can be added in the README section.

The second part can be used to store `COPYRIGHT` and `COPYING` files in various languages.
- 8 Sign your Add-On product with your GPG key. Signing your product with your GPG key provides evidence of the origin of your product. If you do not have a key, create one first and enter the respective passphrase twice.
- 9 Check your product in the overview and proceed with *Finish*.
- 10 Use the *Build* button to start the process. *Finish* closes the window.

## 15.2 Add-On Structure

If you create an Add-On product, the following overview contains the structure of the files and directories:



`ARCHIVES.gz`

Contains the gzipped contents of all RPM files. It is actually a listing of the `rpm` command with the options `-qil` for each RPM file.

`Changelog`

Contains all the changes of the RPM files.

`content`

Contains information about your Add-On product.

`content.asc`

Contains the signature file from GnuPG.

`content.key, gpg-pubkey-NUMBER.asc`

The public GPG key.

`INDEX.gz`

Contains a list of all RPM files and packed with `gzip`.

`ls-lR.gz`

Contains a list of all files and directories of your Add-On product medium.

`media.N/`

Contains files with basic information about the Add-On media set. The directory is numbered, so `media.1/` is for the first Add-On medium. Additional media have a consecutive number.

`suse/`

Contains sub directories with architecture specific information. Exceptions are `noarch/` for architecture independent packages, and `src/` for source packages. Proprietary software packages are stored under `nosrc/`.

## 15.3 For More Information

Find more information in the following documents:

- <http://en.opensuse.org/KIWI>—KIWI Project

- [http://en.opensuse.org/Creating\\_YaST\\_Installation\\_Sources](http://en.opensuse.org/Creating_YaST_Installation_Sources)—YaST installation source creation
- <http://en.opensuse.org/Libzypp/Metadata/YaST>—YaST metadata description
- [http://developer.novell.com/wiki/index.php/Creating\\_Add-ons](http://developer.novell.com/wiki/index.php/Creating_Add-ons)—

# Creating Images with YaST Product Creator

# 16

The YaST Product Creator is a unified graphical front-end for KIWI and Add-on Creator. It was developed to provide image creation functionality in one place. All tools integrated in the YaST Product Creator are still available as separate YaST modules or applications.

## 16.1 Prerequisites for Product Creator

Before you can create images with the YaST Product Creator, make sure you meet the following prerequisites:

1. Install the package `yast2-product-creator` from the SDK under <ftp://dist.suse.de/install/SLE-11-SDK>. This package needs other packages. Make sure you fulfill all dependencies.
2. Free space. The more, the better.

## 16.2 Creating Images

The Product Creator uses KIWI to create an image of a product. In case you are interested in manually developing such images, refer to [Chapter 14, KIWI](#) (page 181).

To create an image, proceed as follows:

- 1 If you start the Product Creator for the first time, enter the configuration name and choose the method how packages are added to the ISO image.

If you have been used the Product Creator already before, select *Add* to create a new product definition and enter the configuration name and choose the method.

- 2 Select or deselect package sources. To select a source, select it from the table and click *Select*. With *Create New...* execute the Add-on Creator, see [Chapter 15, Creating Add-On Products With Add-on Creator](#) (page 189) for more information. To add a different kind of source, add the source in the YaST *Installation Sources* module first then run the Product Creator again. After source selection, click *Next*.

---

**NOTE: Unsupported Target Architectures**

Do not change the target architecture. KIWI does not support building of different architectures at the moment.

---

- 3 Enter the path in which to create the skeleton directory. Choose wheather to *Generate ISO Image File* or *Create Directory Tree Only*. Use the other options to insert metadata. Click *Next*.
- 4 Edit the content of the `isolinux.cfg` file, if it is a part of the configuration. In most cases you can leave it as it is. If the file is not part of the configuration, add it now with *Load File*. Click *Next*.
- 5 Select your software. All package dependencies are solved automatically after *Apply* is clicked.
- 6 Sign your product with *Digitally Sign the Product on the Medium*, if needed. Provide a key for your product configuration. Signing your product with your GPG key provides evidence of the origin of your product. After key configuration, click *Next*.
- 7 Review the summary. To change any option, use *Back*. To confirm your new product configuration, click *Finish*.

Your product definition is now completed. The Product Creator allows you to choose from the following actions:

- **Create Product** Creates an ISO image of the selected product. If there is something missing, the process will be aborted. Correct the error and repeat the configuration.

- **Create Image with KIWI...** Use the pull-down menu to choose from different target formats, such as Live media or Xen images.

## 16.3 For More Information

Find more information about creating system images and related topics in the following documents:

- **Chapter 14, KIWI** (page 181)
- <http://en.opensuse.org/KIWI>—The KIWI project
- </usr/share/doc/packages/kiwi/kiwi.pdf>—KIWI documentation



# Deploying Customized Preinstallations

# 17

Rolling out customized preinstallations of SUSE Linux Enterprise Desktop to a large number of identical machines spares you from installing each one of them separately and provides a standardized installation experience for the end users. With YaST firstboot, create customized preinstallation images and determine the workflow for the final personalization steps that involve end user interaction. This is different from AutoYaST that allows completely automated installations; for more information, see [Chapter 18, \*Automated Installation\*](#) (page 211).

Creating a custom installation, rolling it out to your hardware, and personalizing the final product involves the following steps:

- 1 Prepare the master machine whose disk should be cloned to the client machines. For more information, refer to [Section 17.1, “Preparing the Master Machine”](#) (page 198).
- 2 Customize the firstboot workflow. For more information, refer to [Section 17.2, “Customizing the Firstboot Installation”](#) (page 198).
- 3 Clone the master machine's disk and roll this image out to the clients' disks. For more information, refer to [Section 17.3, “Cloning the Master Installation”](#) (page 207).
- 4 Have the end user personalize the instance of SUSE Linux Enterprise Desktop. For more information, refer to [Section 17.4, “Personalizing the Installation”](#) (page 207).

# 17.1 Preparing the Master Machine

To prepare a master machine for a firstboot workflow, proceed as follows:

- 1 Insert the installation media into the master machine.
- 2 Boot the machine.
- 3 Perform a normal installation including all necessary configuration steps and wait for the installed machine to boot. Also install the `yast2-firstboot` package.
- 4 To define your own workflow of YaST configuration steps for the end user or to add your own YaST modules to this workflow, proceed to [Section 17.2, “Customizing the Firstboot Installation”](#) (page 198). Otherwise proceed directly to [Step 5](#) (page 198).
- 5 Enable firstboot as `root`:

Create an empty file `/var/lib/YaST2/reconfig_system` to trigger firstboot's execution. This file will be deleted, once the firstboot configuration has been successfully accomplished. Create this file using the following command:

```
touch /var/lib/YaST2/reconfig_system
```

- 6 Proceed to [Section 17.3, “Cloning the Master Installation”](#) (page 207).

## 17.2 Customizing the Firstboot Installation

Customizing the firstboot installation may involve several different components. Customizing them is optional. If you do not make any changes, firstboot performs the installation using the default settings. The following options are available:

- Customizing messages to the user as described in [Section 17.2.1, “Customizing YaST Messages”](#) (page 199).



- Customizing licenses and license actions as described in [Section 17.2.2, “Customizing the License Action”](#) (page 200).
- Customizing the release notes to display as described in [Section 17.2.3, “Customizing the Release Notes”](#) (page 201).
- Customizing the order and number of components involved in the installation as described in [Section 17.2.4, “Customizing the Workflow”](#) (page 201).
- Configuring additional optional scripts as described in [Section 17.2.5, “Configuring Additional Scripts”](#) (page 206).

To customize any of these components, adjust the following configuration files:

`/etc/sysconfig/firstboot`

Configure various aspects of firstboot, such as release notes, scripts, and license actions.

`/etc/YaST2/firstboot.xml`

Configure the installation workflow by enabling or disabling components or adding custom ones.

## 17.2.1 Customizing YaST Messages

By default, an installation of SUSE Linux Enterprise Desktop contains several default messages that are localized and displayed at certain stages of the installation process. These include a welcome message, a license message, and a congratulatory message at the end of installation. You can replace any of these with your own versions and include localized versions of them in the installation. To include your own welcome message, proceed as follows:

- 1** Log in as `root`.
- 2** Open the `/etc/sysconfig/firstboot` configuration file and apply the following changes:
  - 2a** Set `FIRSTBOOT_WELCOME_DIR` to the directory path where you want to store the files containing the welcome message and the localized versions, for example:

```
FIRSTBOOT_WELCOME_DIR="/usr/share/firstboot/"
```

- 2b** If your welcome message has filenames other than `welcome.txt` and `welcome_locale.txt` (where *locale* matches the ISO 639 language codes such as “cs” or “de”), specify the filename pattern in `FIRSTBOOT_WELCOME_PATTERNS`. For example:

```
FIRSTBOOT_WELCOME_PATTERNS="mywelcome.txt"
```

If unset, the default value of `welcome.txt` is assumed.

- 3** Create the welcome file and the localized versions and place them in the directory specified in the `/etc/sysconfig/firstboot` configuration file.

Proceed in a similar way to configure customized license and finish messages. These variables are `FIRSTBOOT_LICENSE_DIR` and `FIRSTBOOT_FINISH_FILE`.

Change the `SHOW_Y2CC_CHECKBOX` to “yes”, if the user should be able to start YaST directly after performing the installation.

## 17.2.2 Customizing the License Action

You can customize the way the installation system reacts to a user not accepting the license agreement. There are three different ways in which the system could react to a user's failure to accept the license:

`halt`

The firstboot installation is aborted and the entire system shuts down. This is the default setting.

`continue`

The firstboot installation continues.

`abort`

The firstboot installation is aborted, but the system tries to boot.

Make your choice and set `LICENSE_REFUSAL_ACTION` to the appropriate value.

## 17.2.3 Customizing the Release Notes

Depending on whether you have changed the instance of SUSE Linux Enterprise Desktop you are deploying with firstboot, you probably need to educate the end users about important aspects of their new operating system. A standard installation uses release notes, displayed during one of the final stages of the installation, to provide important information to the users. To have your own modified release notes displayed as part of a firstboot installation, proceed as follows:

- 1 Create your own release notes file. Use the RTF format as in the example file in `/usr/share/doc/release-notes` and save the result as `RELEASE-NOTES.en.rtf` (for English).
- 2 Store optional localized versions next to the original version and replace the `en` part of the filename with the actual ISO 639 language code, such as `de` for German.
- 3 Open the firstboot configuration file from `/etc/sysconfig/firstboot` and set `FIRSTBOOT_RELEASE_NOTES_PATH` to the actual directory where the release notes files are stored.

## 17.2.4 Customizing the Workflow

By default, a standard firstboot workflow includes the following components:

- Language Selection
- Welcome
- License Agreement
- Host Name
- Network
- Time and Date
- Desktop

- root Password
- User Authentication Method
- User Management
- Hardware Configuration
- Finish Setup

This standard layout of a firstboot installation workflow is not mandatory. You can enable or disable certain components or hook your own modules into the workflow. To modify the firstboot workflow, manually edit the firstboot configuration file `/etc/YaST2/firstboot.xml`. This XML file is a subset of the standard `control.xml` file that is used by YaST to control the installation workflow.

For an overview about proposals, see [Example 17.1, “Configuring the Proposal Screens”](#) (page 202). This provides you with enough background to modify the firstboot installation workflow. The basic syntax of the firstboot configuration file and how the key elements are configured is explained with this example.

### **Example 17.1** *Configuring the Proposal Screens*

```
...
<proposals config:type="list">❶
  <proposal>❷
    <name>firstboot_hardware</name>❸
    <mode>installation</mode>❹
    <stage>firstboot</stage>❺
    <label>Hardware Configuration</label>❻
    <proposal_modules config:type="list">❼
      <proposal_module>printer</proposal_module>❽
    </proposal_modules>
  </proposal>
</proposal>
...
</proposal>
</proposals>
```

- ❶ The container for all proposals that should be part of the firstboot workflow.
- ❷ The container for an individual proposal.
- ❸ The internal name of the proposal.

- ④ The mode of this proposal. Do not make any changes here. For a firstboot installation, this must be set to `installation`.
- ⑤ The stage of the installation process at which this proposal is invoked. Do not make any changes here. For a firstboot installation, this must be set to `firstboot`.
- ⑥ The label to be displayed on the proposal.
- ⑦ The container for all modules that are part of the proposal screen.
- ⑧ One or more modules that are part of the proposal screen.

The next section of the firstboot configuration file consists of the workflow definition. All modules that should be part of the firstboot installation workflow must be listed here.

### **Example 17.2** *Configuring the Workflow Section*

```
<workflows config:type="list">
  <workflow>
    <defaults>
      <enable_back>yes</enable_back>
      <enable_next>yes</enable_next>
      <archs>all</archs>
    </defaults>
    <stage>firstboot</stage>
    <label>Configuration</label>
    <mode>installation</mode>
    ... <!-- list of modules -->
    </modules>
  </workflow>
</workflows>
...
```

The overall structure of the `workflows` section is very similar to that of the `proposals` section. A container holds the workflow elements and the workflow elements all include stage, label and mode information just as the proposals introduced in [Example 17.1, “Configuring the Proposal Screens”](#) (page 202). The most notable difference is the `defaults` section, which contains basic design information for the workflow components:

`enable_back`

Include the *Back* button in all dialogs.

`enable_next`

Include the *Next* button in all dialogs.

`archs`

Specify the hardware architectures on which this workflow should be used.

### **Example 17.3** *Configuring the List of Workflow Components*

```
<modules config:type="list">❶
  <module>❷
    <label>Language</label>❸
    <enabled config:type="boolean">false</enabled>❹
    <name>firstboot_language</name>❺
  </module>
</modules>
```

- ❶ The container for all components of the workflow.
- ❷ The module definition.
- ❸ The label displayed with the module.
- ❹ The switch to enable or disable this component in the workflow.
- ❺ The module name. The module itself must be located under `/usr/share/YaST2/clients` and have the `.ycp` file suffix.

To make changes to the number or order of proposal screens during the firstboot installation, proceed as follows:

**1** Open the firstboot configuration file at `/etc/YaST2/firstboot.xml`.

**2** Delete or add proposal screens or change the order of the existing ones:

- To delete an entire proposal, remove the `proposal` element including all its subelements from the `proposals` section and remove the respective module element (with subelements) from the workflow.
- To add a new proposal, create a new `proposal` element and fill in all the required subelements. Make sure that the proposal exists as a YaST module in `/usr/share/YaST2/clients`.

- To change the order of proposals, move the respective `module` elements containing the proposal screens around in the workflow. Note that there may be dependencies to other installation steps that require a certain order of proposals and workflow components.

### 3 Apply your changes and close the configuration file.

You can always change the workflow of the configuration steps when the default does not meet your needs. Enable or disable certain modules in the workflow or add your own custom ones.

To toggle the status of a module in the firstboot workflow, proceed as follows:

- 1 Open the `/etc/YaST2/firstboot.xml` configuration file.
- 2 Change the value for the `enabled` element from `true` to `false` to disable the module or from `false` to `true` to enable it again.

```
<module>
  <label>Time and Date</label>
  <enabled config:type="boolean">true</enabled>
  <name>firstboot_timezone</name>
</module>
```

### 3 Apply your changes and close the configuration file.

To add a custom made module to the workflow, proceed as follows:

- 1 Create your own YaST module and store the module file `module_name.ycp` in `/usr/share/YaST2/clients`.
- 2 Open the `/etc/YaST2/firstboot.xml` configuration file.
- 3 Determine at which point of the workflow your new module should be run. In doing so, make sure that possible dependencies to other steps in the workflow are taken into account and resolved.
- 4 Create a new `module` element inside the `modules` container and add the appropriate subelements:

```
<modules config:type="list">
...
  <module>
    <label>my_module</label>
    <enabled config:type="boolean">true</enabled>
    <name>filename_my_module</name>
  </module>
</modules>
```

- 4a** Enter the label to display on your module in the `label` element.
  - 4b** Make sure that `enabled` is set to `true` to have your module included in the workflow.
  - 4c** Enter the filename of your module in the `name` element. Omit the full path and the `.ycp` suffix.
- 5** Apply your settings and close the configuration file.

---

**TIP: For More Information**

For more information about YaST development, refer to <http://developer.novell.com/wiki/index.php/YaST>. Detailed information about YaST firstboot can be found at [http://forgeftp.novell.com/yast/doc/SL11.1/tdg/inst\\_in\\_general\\_chap.html](http://forgeftp.novell.com/yast/doc/SL11.1/tdg/inst_in_general_chap.html).

---

## 17.2.5 Configuring Additional Scripts

firstboot can be configured to execute additional scripts after the firstboot workflow has been completed. To add additional scripts to the firstboot sequence, proceed as follows:

- 1** Open the `/etc/sysconfig/firstboot` configuration file and make sure that the path specified for `SCRIPT_DIR` is correct. The default value is `/usr/share/firstboot/scripts`.
- 2** Create your shell script, store it in the specified directory, and apply the appropriate file permissions.



## 17.3 Cloning the Master Installation

Clone the master machine's disk using any of the imaging mechanisms available to you and roll these images out to the target machines.

## 17.4 Personalizing the Installation

As soon as the cloned disk image is booted, firstboot starts and the installation proceeds exactly as laid out in [Section 17.2.4, “Customizing the Workflow”](#) (page 201). Only the components included in the firstboot workflow configuration are started. Any other installation steps are skipped. The end user adjusts language, keyboard, network, and password settings to personalize the workstation. Once this process is finished, a firstboot installed system behaves as any other instance of SUSE Linux Enterprise Desktop.



## **Part III. Automated Installations**



# Automated Installation

AutoYaST allows you to install SUSE® Linux Enterprise on a large number of machines in parallel. The AutoYaST technology offers great flexibility to adjust deployments to heterogeneous hardware. This chapter tells you how to prepare a simple automated installation and lay out an advanced scenario involving different hardware types and installation purposes.

## 18.1 Simple Mass Installation

---

### IMPORTANT: Identical Hardware

This scenario assumes you are rolling out SUSE Linux Enterprise to a set of machines with exactly the same hardware configuration.

---

To prepare for an AutoYaST mass installation, proceed as follows:

- 1 Create an AutoYaST profile that contains the installation details needed for your deployment as described in [Section 18.1.1, “Creating an AutoYaST Profile”](#) (page 212).
- 2 Determine the source of the AutoYaST profile and the parameter to pass to the installation routines as described in [Section 18.1.2, “Distributing the Profile and Determining the `autoyast` Parameter”](#) (page 214).
- 3 Determine the source of the SUSE Linux Enterprise installation data as described in [Section 18.1.3, “Providing the Installation Data”](#) (page 216).

- 4 Determine and set up the boot scenario for autoinstallation as described in [Section 18.1.4, “Setting Up the Boot Scenario”](#) (page 217).
- 5 Pass the command line to the installation routines by adding the parameters manually or by creating an `info` file as described in [Section 18.1.5, “Creating the info File”](#) (page 219).
- 6 Start the autoinstallation process as described in [Section 18.1.6, “Initiating and Monitoring the Autoinstallation”](#) (page 222).

## 18.1.1 Creating an AutoYaST Profile

An AutoYaST profile tells AutoYaST what to install and how to configure the installed system to get a completely ready-to-use system in the end. It can be created in several different ways:

- Clone a fresh installation from a reference machine to a set of identical machines
- Use the AutoYaST GUI to create and modify a profile to meet your requirements
- Use an XML editor and create a profile from scratch

To clone a fresh reference installation, proceed as follows:

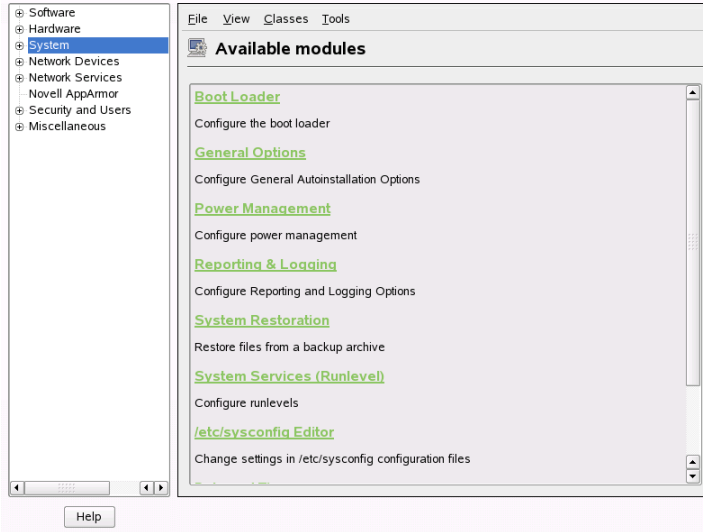
- 1 Perform a normal installation.
- 2 After you complete the hardware configuration and read the release notes, check *Create Profile For AutoYaST*, if it is not yet checked by default. This creates a ready-to-use profile as `/root/autoyast.xml` that can be used to create clones of this particular installation.

To use the AutoYaST GUI to create a profile from an existing system configuration and modify it to your needs, proceed as follows:

- 1 As `root`, start YaST.
- 2 Select *Miscellaneous > Autoinstallation* to start the graphical AutoYaST front-end.

- 3** Select *Tools > Create Reference Control File* to prepare AutoYaST to mirror the current system configuration into an AutoYaST profile.
- 4** As well as the default resources, like boot loader, partitioning, and software selection, you can add various other aspects of your system to the profile by checking the items in the list in *Create a Reference Control File*.
- 5** Click *Create* to have YaST gather all the system information and write it to a new profile.
- 6** To proceed, choose one of the following:
  - If the profile is complete and matches your requirements, select *File > Save as* and enter a filename for the profile, such as `autoyast.xml`.
  - Modify the reference profile by selecting the appropriate configuration aspects (such as “Hardware/Printer”) from the tree view to the left and clicking *Configure*. The respective YaST module starts but your settings are written to the AutoYaST profile instead of applied to your system. When done, select *File > Save as* and enter a suitable name for the profile.
- 7** Leave the AutoYaST module with *File > Exit*.

**Figure 18.1** *Editing an AutoYaST Profile with the AutoYaST Front-End*



## 18.1.2 Distributing the Profile and Determining the autoyast Parameter

The AutoYaST profile can be distributed in several different ways. Depending on the protocol used to distribute the profile data, different AutoYaST parameters are used to make the profile location known to the installation routines on the client. The location of the profile is passed to the installation routines by means of the boot prompt or an `info` file that is loaded upon boot. The following options are available:

Profile Location	Parameter	Description
File	<code>autoyast=file:// /path</code>	Makes the installation routines look for the control file in specified path (relative to source root directory— <code>file:///autoyast.xml</code> if in the top directory of a CD-ROM).



Profile Location	Parameter	Description
Device	<code>autoyast=device:// /path</code>	Makes the installation routines look for the control file on a storage device. Only the device name is needed— <code>/dev/sda1</code> is wrong, use <code>sda1</code> instead.
Floppy	<code>autoyast=floppy:// /path</code>	Makes the installation routines look for the control file on a floppy in the floppy drive. This option is especially useful, if you want to boot from CD-ROM.
NFS	<code>autoyast=nfs:// /server/path</code>	Has the installation routines retrieve the control file from an NFS server.
HTTP	<code>autoyast=http:// /server/path</code>	Has the installation routines retrieve the control file from an HTTP server.
HTTPS	<code>autoyast=https:// /server/path</code>	Has the installation routines retrieve the control file from an HTTPS server.
TFTP	<code>autoyast=tftp:// /server/path</code>	Has the installation routines retrieve the control file from a TFTP server.
FTP	<code>autoyast=ftp:// /server/path</code>	Has the installation routines retrieve the control file from an FTP server.

Replace the *server* and *path* placeholders with values matching your actual setup.

AutoYaST includes a feature that allows binding certain profiles to the client's MAC address. Without having to alter the `autoyast=` parameter, you can have the same setup install several different instances using different profiles.

To use this, proceed as follows:

- 1 Create separate profiles with the MAC address of the client as the filename and put them on the HTTP server that holds your AutoYaST profiles.

- 2 Omit the exact path including the filename when creating the `autoyast=` parameter, for example:

```
autoyast=tftp://192.168.1.115/
```

- 3 Start the autoinstallation.

YaST tries to determine the location of the profile in the following way:

1. YaST searches for the profile using its own IP address in uppercase hexadecimal, for example, `192.0.2.91` is `C000025B`.
2. If this file is not found, YaST removes one hex digit and tries again. This action is repeated eight times until the file with the correct name is found.
3. If that still fails, it tries looking for a file with the MAC address of the clients as the filename. The MAC address of the example client is `0080C8F6484C`.
4. If the MAC address-named file cannot be found, YaST searches for a file named `default` (in lowercase). An example sequence of addresses where YaST searches for the AutoYaST profile looks as follows:

```
C000025B
C000025
C00002
C0000
C000
C00
C00
C0
C
0080C8F6484C
default
```

## 18.1.3 Providing the Installation Data

The installation data can be provided by means of the product CDs or DVDs or using a network installation source. If the product CDs are used as the installation source, physical access to the client to install is needed, because the boot process needs to be initiated manually and the CDs need to be changed.

To provide the installation sources over the network, set up a network installation server (HTTP, NFS, FTP) as described in [Section 11.2.1, “Setting Up an Installation Server Using YaST”](#) (page 126). Use an `info` file to pass the server's location to the installation routines.

## 18.1.4 Setting Up the Boot Scenario

The client can be booted in several different ways:

### Network Boot

As for a normal remote installation, autoinstallation can be initiated with Wake on LAN and PXE, the boot image and control file can be pulled in via TFTP, and the installation sources from any network installation server.

### Bootable CD-ROM

You can use the original SUSE Linux Enterprise media to boot the system for autoinstallation and pull in the control file from a network location or a floppy. Alternatively, create your own custom CD-ROM holding both the installation sources and the AutoYaST profile.

The following sections provide a basic outline of the procedures for network boot or boot from CD-ROM.

## Preparing for Network Boot

Network booting with Wake on LAN, PXE, and TFTP is discussed in [Section 11.1.3, “Remote Installation via VNC—PXE Boot and Wake on LAN”](#) (page 121). To make the setup introduced there work for autoinstallation, modify the featured PXE Linux configuration file (`/srv/tftp/pxelinux.cfg/default`) to contain the `autoyast` parameter pointing to the location of the AutoYaST profile. An example entry for a standard installation looks like this:

```
default linux
# default label linux
  kernel linux
  append initrd=initrd install=http://192.168.1.115/install/suse-enterprise/
```

The same example for autoinstallation looks like this:

```
default linux

# default label linux
  kernel linux
  append initrd=initrd install=http://192.168.1.115/install/suse-enterprise/
  \
    autoyast=nfs://192.168.1.110/profiles/autoyast.xml
```

Replace the example IP addresses and paths with the data used in your setup.

## Preparing to Boot from CD-ROM

There are several ways in which booting from CD-ROM can come into play in AutoYaST installations. Choose from the following scenarios:

### Boot from SUSE Linux Enterprise Media, Get the Profile over the Network

Use this approach if a totally network-based scenario is not possible (for example, if your hardware does not support PXE) and you have physical access to system to install during most of the process.

You need:

- The SUSE Linux Enterprise media
- A network server providing the profile data (see [Section 18.1.2, “Distributing the Profile and Determining the autoyast Parameter”](#) (page 214) for details)
- A floppy containing the `info` file that tells the installation routines where to find the profile

*or*

Access to the boot prompt of the system to install where you manually enter the `autoyast=` parameter

### Boot and Install from SUSE Linux Enterprise Media, Get the Profile from a Floppy

Use this approach if an entirely network-based installation scenario would not work. It requires physical access to the system to install for turning on the target machine, or, in the second case, to enter the profile's location at the boot prompt.

In both cases, you may also need to change media depending on the scope of installation.

You need:

- The SUSE Linux Enterprise media
- A floppy holding both the profile and the `info` file

*or*

Access to the boot prompt of the target to enter the `autoyast=` parameter

Boot and Install from Custom Media, Get the Profile from the Media

If you just need to install a limited number of software packages and the number of targets is relatively low, creating your own custom CD holding both the installation data and the profile itself might prove a good idea, especially if no network is available in your setup.

## 18.1.5 Creating the info File

The installation routines at the target need to be made aware of all the different components of the AutoYaST framework. This is done by creating a command line containing all the parameters needed to locate the AutoYaST components, installation sources, and the parameters needed to control the installation process.

Do this by manually passing these parameters at the boot prompt of the installation or by providing a file called `info` that is read by the installation routines (`linuxrc`). The former requires physical access to any client to install, which makes this approach unsuitable for large deployments. The latter enables you to provide the `info` file on some media that is prepared and inserted into the clients' drives prior to the autoinstallation. Alternatively, use PXE boot and include the `linuxrc` parameters in the `pxelinux.cfg/default` file as shown in [Section “Preparing for Network Boot”](#) (page 217).

The following parameters are commonly used for `linuxrc`. For more information, refer to the AutoYaST package documentation under `/usr/share/doc/packages/autoyast`.

---

## IMPORTANT: Separating Parameters and Values

When passing parameters to `linuxrc` at the boot prompt, use `=` to separate parameter and value. When using an `info` file, separate parameter and value with `:.`

---

Keyword	Value
<code>netdevice</code>	The network device to use for network setup (for BOOTP/DHCP requests). Only needed if several network devices are available.
<code>hostip</code>	When empty, the client sends a BOOTP request. Otherwise the client is configured using the specified data.
<code>netmask</code>	Netmask for the selected network.
<code>gateway</code>	Default gateway.
<code>nameserver</code>	Name server.
<code>autoyast</code>	Location of the the control file to use for the automatic installation, such as <code>autoyast=nfs://192.168.1.110/profiles/.</code>
<code>install</code>	Location of the installation source, such as <code>install=nfs://192.168.1.110/CDs/.</code>
<code>vnc</code>	If set to 1, enables VNC remote controlled installation.
<code>vncpassword</code>	The password for VNC.
<code>usessh</code>	If set to 1, enables SSH remote controlled installation.

---

If your autoinstallation scenario involves client configuration via DHCP and a network installation source and you want to monitor the installation process using VNC, your `info` would look like this:

```
autoyast:profile_source install:install_source vnc:1 vncpassword:some_password
```

If you prefer a static network setup at installation time, your `info` file would look like the following:

```
autoyast:profile_source \  
install:install_source \  
hostip:some_ip \  
netmask:some_netmask \  
gateway:some_gateway
```

The `\` indicate that the line breaks have only been added for the sake of readability. All options must be entered as one continuous string.

The `info` data can be made available to `linuxrc` in various different ways:

- As a file on a floppy or CD Rom that is in the client's drive at installation time. Add the `info` parameter similar to `info=floppy:/info` or `info=cd:/info`.
- As a file in the root directory of the initial RAM disk used for booting the system provided either from custom installation media or via PXE boot.
- As part of the AutoYaST profile. In this case, the AutoYaST file needs to be called `info` to enable `linuxrc` to parse it. An example for this approach is given below.
- By means of an URL that points to the location of the `info` file. The syntax for this looks like `info=http://www.example.com/info`.

`linuxrc` looks for a string (`start_linuxrc_conf`) in the profile that represents the beginning of the file. If it is found, it parses the content starting from that string and finishes when the string `end_linuxrc_conf` is found. The options are stored in the profile as follows:

```
....  
<install>  
....  
    <init>  
        <info_file>  
<![CDATA[  
#  
# Don't remove the following line:  
# start_linuxrc_conf  
#  
install: nfs:server/path
```

```

vnc: 1
vncpassword: test
autoyast: file:///info

# end_linuxrc_conf
# Do not remove the above comment
#
]]>

    </info_file>
  </init>
.....
  </install>
.....

```

linuxrc loads the profile containing the boot parameters instead of the traditional `info` file. The `install:` parameter points to the location of the installation sources. `vnc` and `vncpassword` indicate the use of VNC for installation monitoring. The `autoyast` parameter tells linuxrc to treat `info` as an AutoYaST profile.

## 18.1.6 Initiating and Monitoring the Autoinstallation

After you have provided all the infrastructure mentioned above (profile, installation source, and `info` file), you can go ahead and start the autoinstallation. Depending on the scenario chosen for booting and monitoring the process, physical interaction with the client may be needed:

- If the client system boots from any kind of physical media, either product media or custom CDs, you need to insert these into the client's drives.
- If the client is not switched on via Wake on LAN, you need to at least switch on the client machine.
- If you have not opted for remote controlled autoinstallation, the graphical feedback from AutoYaST is sent to the client's attached monitor or, if you use a headless client, to a serial console.

To enable remote controlled autoinstallation, use the VNC or SSH parameters described in [Section 18.1.5, “Creating the info File”](#) (page 219) and connect to the client from another machine as described in [Section 11.5, “Monitoring the Installation Process”](#) (page 150).



## 18.2 Rule-Based Autoinstallation

The following sections introduce the basic concept of rule-based installation using AutoYaST and provide an example scenario that enables you to create your own custom autoinstallation setup.

### 18.2.1 Understanding Rule-Based Autoinstallation

Rule-based AutoYaST installation allows you to cope with heterogeneous hardware environments:

- Does your site contain hardware of different vendors?
- Are the machines on your site of different hardware configuration (for example, using different devices or using different memory and disk sizes)?
- Do you intend to install across different domains and need to distinguish between them?

What rule-based autoinstallation does is, basically, generate a custom profile to match a heterogeneous scenario by merging several profiles into one. Each rule describes one particular distinctive feature of your setup (such as disk size) and tells AutoYaST which profile to use when the rule matches. Several rules describing different features of your setup are combined in an AutoYaST `rules.xml` file. The rule stack is then processed and AutoYaST generates the final profile by merging the different profiles matching the AutoYaST rules into one. To illustrate this procedure, refer to [Section 18.2.2, “Example Scenario for Rule-Based Autoinstallation”](#) (page 225).

Rule-based AutoYaST offers you great flexibility in planning and executing your SUSE Linux Enterprise deployment. You can:

- Create rules for matching any of the predefined system attributes in AutoYaST
- Combine multiple system attributes (such as disk size and kernel architecture) into one rule by using logical operators

- Create custom rules by running shell scripts and passing their output to the AutoYaST framework. The number of custom rules is limited to five.

---

## NOTE

For more information about rule creation and usage with AutoYaST, refer to the package's documentation under `/usr/share/doc/packages/autoyast2/html/index.html`, Chapter *Rules and Classes*.

---

To prepare for a rule-based AutoYaST mass installation, proceed as follows:

- 1 Create several AutoYaST profiles that contain the installation details needed for your heterogeneous setup as described in [Section 18.1.1, “Creating an AutoYaST Profile”](#) (page 212).
- 2 Define rules to match the system attributes of your hardware setup as shown in [Section 18.2.2, “Example Scenario for Rule-Based Autoinstallation”](#) (page 225).
- 3 Determine the source of the AutoYaST profile and the parameter to pass to the installation routines as described in [Section 18.1.2, “Distributing the Profile and Determining the autoyast Parameter”](#) (page 214).
- 4 Determine the source of the SUSE Linux Enterprise installation data as described in [Section 18.1.3, “Providing the Installation Data”](#) (page 216)
- 5 Pass the command line to the installation routines by adding the parameters manually or by creating an `info` file as described in [Section 18.1.5, “Creating the info File”](#) (page 219).
- 6 Determine and set up the boot scenario for autoinstallation as described in [Section 18.1.4, “Setting Up the Boot Scenario”](#) (page 217).
- 7 Start the autoinstallation process as described in [Section 18.1.6, “Initiating and Monitoring the Autoinstallation”](#) (page 222).

## 18.2.2 Example Scenario for Rule-Based Autoinstallation

To get a basic understanding of how rules are created, think of the following example, depicted in **Figure 18.2, “AutoYaST Rules”** (page 226). One run of AutoYaST installs the following setup:

### A Print Server

This machine just needs a minimal installation without a desktop environment and a limited set of software packages.

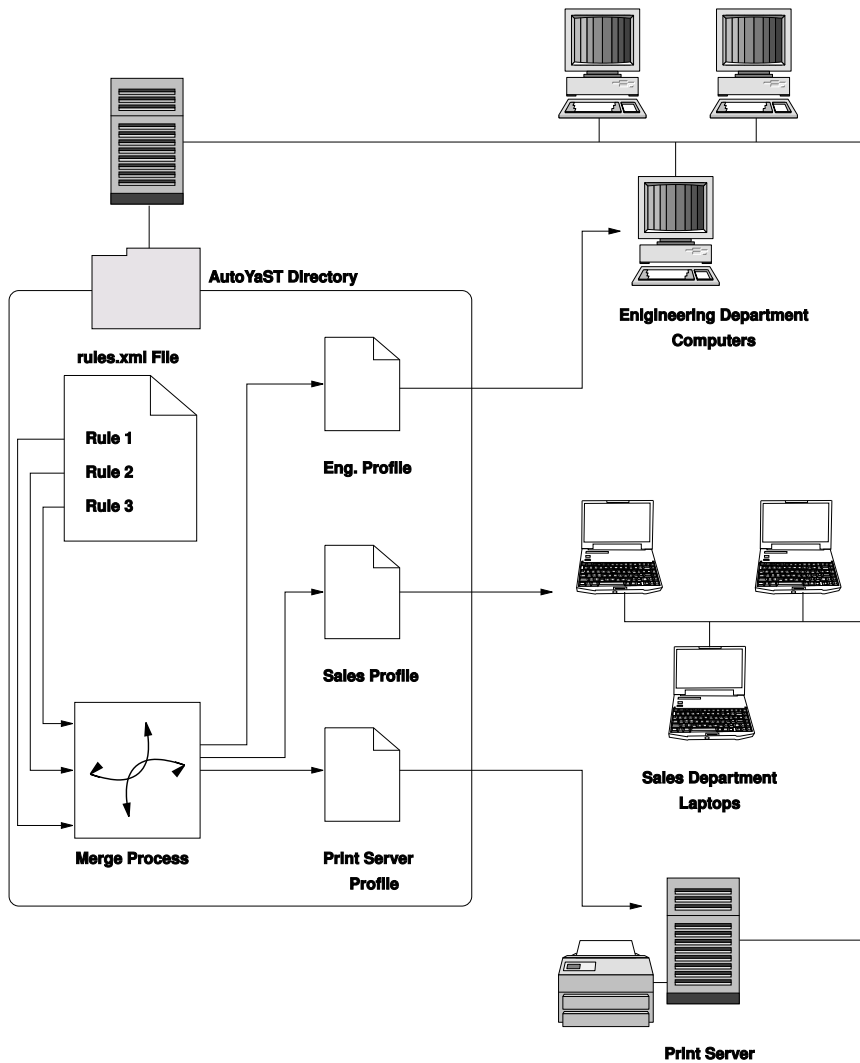
### Workstations in the Engineering Department

These machines need a desktop environment and a broad set of development software.

### Laptops in the Sales Department

These machines need a desktop environment and a limited set of specialized applications, such as office and calendaring software.

**Figure 18.2** *AutoYaST Rules*



In a first step, use one of the methods outlined in [Section 18.1.1, “Creating an AutoYaST Profile”](#) (page 212) to create profiles for each use case. In this example, you would create `print.xml`, `engineering.xml`, and `sales.xml`.

In the second step, create rules to distinguish the three hardware types from one another and to tell AutoYaST which profile to use. Use an algorithm similar to the following to set up the rules:

1. Does the machine have an IP of *192.168.2.253*? Then make it the print server.
2. Does the machine have PCMCIA hardware and feature an Intel chipset? Then consider it an Intel laptop and install the sales department software selection.
3. If none of the above is true, consider the machine a developer workstation and install accordingly.

Roughly sketched, this translates into a `rules.xml` file with the following content:

```
<?xml version="1.0"?>
<!DOCTYPE autoinstall SYSTEM "/usr/share/autoinstall/dtd/rules.dtd">
<autoinstall xmlns="http://www.suse.com/1.0/yast2ns"
xmlns:config="http://www.suse.com/1.0/configs">
  <rules config:type="list">
    <rule>
      <hostaddress>
        <match>192.168.2.253</match>
        <match_type>exact</match_type>
      </hostaddress>
      <result>
        <profile>print.xml</profile>
        <continue config:type="boolean">false</continue>
      </result>
    </rule>
    <rule>
      <haspcmcia>
        <match>1</match>
        <match_type>exact</match_type>
      </haspcmcia>
      <custom1>
        <script>
if grep -i intel /proc/cpuinfo > /dev/null; then
echo -n "intel"
else
echo -n "non_intel"
fi;
        </script>
        <match>*</match>
        <match_type>exact</match_type>
      </custom1>
      <result>
        <profile>sales.xml</profile>
        <continue config:type="boolean">false</continue>
      </result>
    </rule>
  </rules>
</autoinstall>
```

```

        <operator>and</operator>
    </rule>
    <rule>
        <haspcmcia>
            <match>0</match>
            <match_type>exact</match_type>
        </haspcmcia>
    </result>
        <profile>engineering.xml</profile>
        <continue config:type="boolean">>false</continue>
    </result>
</rule>
</rules>
</autoinstall>

```

When distributing the rules file, make sure that the `rules` directory resides under the `profiles` directory specified in the `autoyast=protocol:serverip/profiles/` URL. AutoYaST looks for a `rules` subdirectory containing a file named `rules.xml` first then loads and merges the profiles specified in the rules file.

The rest of the autoinstallation procedure is carried out as usual.

## 18.3 For More Information

For in-depth information about the AutoYaST technology, refer to the documentation installed along with the software. It is located under `/usr/share/doc/packages/autoyast2`. The most recent edition of this documentation can be found at [http://www.suse.de/~ug/autoyast\\_doc/index.html](http://www.suse.de/~ug/autoyast_doc/index.html).

# Automated Deployment of Preload Images

# 19

With KIWI you are able to create operating system images. This chapter handles the process of deploying an system image to an empty machine. For this, you have to create a preload image which contains a bootable RAW image. This file contains two important parts: a partition table and the actual operating system. This RAW image will be written to the empty hard disk and the operating system extends to the remaining disk space at first boot.

To create such a image, see [Section 14.4.2, “Creating an Image”](#) (page 187). When you build the ISO image, you can find the RAW file at the destination folder. There are many possibilities to dump a raw image onto a disk.

- Plug the disk into a deployment server and just copy the image to the raw device.
- Provide the raw image by means of a HTTP or FTP server and dump it on the disk of the client to install.
- Create a netboot image that does nothing but get the image and dump it on the disk. This is a good method for mass deployment.
- Boot a rescue disk and do the dump manually from the rescue image.

For a quick start, it is good to use one of the methods described in [Section 19.1, “Deploying system manually from rescue image”](#) (page 230).

# 19.1 Deploying system manually from rescue image

Deploying with generated ISO file from KIWI:

1. Burn the ISO image you get from the KIWI building process, see [Section 14.4.2, “Creating an Image”](#) (page 187) on CD/DVD
2. Boot from this medium on the machine you want to install the system.
3. Select the hard disk you want to install.
4. Restart the machine and boot from hard disk.

Deploying over rescue system:

1. Boot the client to install with a rescue system. Such systems are available on all SUSE installation CDs or DVDs.
2. Log in as `root`. Leave the password empty, no need to enter anything.
3. Configure your network. If you have DHCP available in your network, this is merely the command `ifup-dhcp eth0`. If you must do this manually, use the command `ip` to configure your network. The output starting DHCP also tells you the IP address of the computer.
4. Listen on an unused port of your network like 1234 and dump the incoming data to disk with the command:

```
netcat -l -p 1234 > /dev/sda
```

5. On the imaging server, send the raw image to the client to install with the command:

```
netcat <IP of client> 1234 < $HOME/preload_image/<image_name>
```

6. When the image is transferred, remove the rescue system from your CD or DVD drive and shutdown the client computer. At the next boot, the boot loader GRUB should be started on the client and the firstboot system will take over.



## 19.2 Automated Deployment with PXE Boot

When doing many installations of a operating system on similar hardware, it is useful to put some effort into preparing a mass deployment of the operating system and to minimize the time needed for the actual deployment. This is what this chapter is about. The goal is to just attach a computer to power and network, start a network boot, and wait until it switches off again.

The following actions have to be performed in order to accomplish this task:

### Setup a boot and install server

A dedicated machine is needed, that should be prepared to offer PXE boot as well as an ftp or web server to provide a preload image. It is a good idea to give the machine enough memory to hold all necessary installation data in memory. For a default installation, you should have at least 4 GByte of memory. All the necessary tasks can be accomplished with a SUSE Linux Enterprise Server. For more details, see [Section 19.2.1, “Setup a Boot and Install Server”](#) (page 232).

### Prepare a preload Image

The actual installation is done by copying a raw image of the operating system to the new harddisk. All features and settings have to be prepared and tested carefully. To provide such an image, KIWI can be used, that is available in the SDK of the SUSE Linux Enterprise operating system. More information about image creation with KIWI is available in [Chapter 14, KIWI](#) (page 181). For more details about the requirements of the preload image, see [Section 19.2.2, “Creating a Preload Image”](#) (page 232).

### Create a initial system for deployment

This is a task that needs some linux expertise. A description about how this can be achieved by means of an example installation is available at [Section 19.2.3, “Creating a Initial System to Deploy a Preload Image”](#) (page 233).

### Configure the boot server to do automatic deployments

Finally, all must be put together. PXE boot must be told to boot the installation system, that in turn will take the preload image from the server and copy it to the harddisk.

## 19.2.1 Setup a Boot and Install Server

There are four steps to accomplish to perform this task after you installed a SUSE Linux Enterprise Server:

To perform this type of installation, proceed as follows:

- 1 Set up the installation source as described in [Section 11.2, “Setting Up the Server Holding the Installation Sources”](#) (page 126). Choose a HTTP, or FTP network server.
- 2 Set up a TFTP server to hold a boot image that will be created in a later step. This is described in [Section 11.3.2, “Setting Up a TFTP Server”](#) (page 139).
- 3 Set up a DHCP server to provide IP addresses to all machines and reveal the location of the TFTP server to the target system. This is described in [Section 11.3.1, “Setting Up a DHCP Server”](#) (page 136).
- 4 Prepare the installation server PXE boot. This is described in further detail in [Section 11.3.3, “Using PXE Boot”](#) (page 140).

Note, that the actual installation process will greatly benefit if you provide enough memory to this machine to hold the preload image in memory. Secondly, using gigabit ethernet will speedup the deployment process considerably compared to slower networks, if the complete network supports this.

## 19.2.2 Creating a Preload Image

The process of creating images with KIWI is described in [Section 14.4.2, “Creating an Image”](#) (page 187). However, to create a useful image for a mass deployment, several considerations should be taken into account:

- A typical preload image will use the following type:

```
<type primary="true" filesystem="ext3" boot="oemboot/suse-SLES11">vmx</type>
```

- During the setup of a preload image, the image creation process is run multiple times. The needed repositories to build the image should be available on the local computer.

- Depending on the desired usage of the preload, some effort should be invested in configuring firstboot. Find more details about firstboot in [Chapter 17, \*Deploying Customized Preinstallations\*](#) (page 197). With this method you can also require the user to do initial configurations at the first bootup of the system.
- Many additional features can be configured into the image like adding update repositories, or doing an update at the first bootup. However, it is impossible to describe all possibilities at this place, and depending on the requirements, the creation of the preload image requires in depth knowledge of the imaging system KIWI as well as several other technologies used in SUSE Linux Enterprise Desktop.

The actual image to be deployed should be available from the ftp or http server you provided on the installation server.

## 19.2.3 Creating a Initial System to Deploy a Preload Image

In order to run an automatic deployment, it is necessary to start a initial linux system on the target computer. During a typical installation, kernel and initial ram filesystem are read from some boot medium and started by the bios. The needed functionality can be implemented in the ram filesystem, which together with the kernel will serve as initial system.

The main features that must be provided by the initial system is to enable access to the harddisk, and to make a network connection available. Both of these functions are depending on the hardware that you want to deploy on. In principle, it is possible to create a initial system from scratch, but to ease this task, it is also possible to modify the initial ram filesystem used by the machine during boot.

The following procedure is just one example how to create the needed initial ram filesystem. There are many different methods to create such a system, however this one is not too complex.

- 1 Do a standard installation of SUSE Linux Enterprise Desktop on the target system.
- 2 Install the package `busybox` on the system.
- 3 Create a new ram filesystem with the following command:

```
mkinitrd -f busybox -D eth0
```

Note that `eth0` represents the ethernet device where your network cable is attached to. The parameter `-f busybox` adds the multi call binary `busybox` to the ram filesystem. After doing this, many standard unix commands are available inside this system.

- 4 Copy the new ram filesystem and the kernel to your boot server with the command:

```
scp /boot/initrd /boot/vmlinuz pxe.example.com:
```

Replace `pxe.example.com` with the name of your local boot server or ip address.

- 5 Log into your bootserver as user `root`, and create a directory where you can modify the ram filesystem:

```
mkdir ~/bootimage
```

- 6 Change your working directory into this directory with the command `cd ~/bootimage`.

- 7 Unpack the previously copied initial ram filesystem with the command:

```
zcat ../initrd | cpio -i
```

- 8 Edit the file `run_all.sh`.

- 9 Search for the following line, delete it and the rest of the file:

```
[ "$debug" ] && echo preping 21-nfs.sh
```

- 10 Add the following lines to the end of the files `run_all.sh`:

```
[ "$debug" ] && echo preping 92-install.sh  
[ "$debug" ] && echo running 92-install.sh  
source boot/92-install.sh  
[ "$modules" ] && load_modules
```

- 11 Create a new script `boot/92-install.sh` with the following content:

```
#!/bin/bash  
if [ "$(get_param rawimage)" ]; then
```

```

rawimage=$(get_param rawimage)
if [ "$(get_param rawdevice)" ]; then
    rawdevice=$(get_param rawdevice)
    echo "wget -O ${rawdevice} ${rawimage}"
    wget -O ${rawdevice} ${rawimage}
    sync
    sleep 5
    echo "DONE"
fi
fi
# /bin/bash
/bin/poweroff -f

```

- 12** If you want to have a debug shell before the computer switches off, remove the comment sign before `/bin/bash`.
- 13** Make this script executable with the command `chmod 755 boot/92-install.sh`.
- 14** Create a new initial ram filesystem with the commands:

```

mkdir -p /srv/tftpboot
find . | cpio --quiet -H newc -o | gzip -9 -n > \
/srv/tftpboot/initrd.boot

```

- 15** Also copy the kernel to this directory:

```

cp ../vmlinuz /srv/tftpboot/linux.boot

```

The initial ram filesystem is now prepared to take two new kernel command line parameters. The parameter `rawimage=<URL>` is used to identify the location of the preload image. Any URL that is understood by `wget` can be used. The parameter `rawdevice=<device>` is used to identify the block device for the harddisk on the target machine.

## 19.2.4 Boot Server Configuration

The configuration of the boot server is covered in detail in several different chapters as listed in [Section 19.2.1, “Setup a Boot and Install Server”](#) (page 232). This section should give a check list that covers steps that are at least necessary to configure the system.

- Setup a dhcp server. The subnet where the machines are installed needs the additional lines:

```
filename "pxelinux.0";  
next-server 192.168.1.115;
```

In this example, 192.168.1.115 is the ip address of the PXE server pxe.example.com.

- Configure a PXE server as described in [Section 11.3.3, “Using PXE Boot”](#) (page 140). When editing `/srv/tftpboot/pxelinux.cfg/default`, add the following entries:

```
default bootinstall  
label bootinstall  
    kernel linux.boot  
    append initrd=initrd.boot \  
    rawimage=ftp://192.168.1.115/preload/preloadimage.raw rawdevice=/dev/sda
```

- Setup a ftp server and copy your prepared preload image to `/srv/ftp/preload/preloadimage.raw`.

Test your setup by booting the target system with PXE network boot. This will automatically copy the prepared preload image to harddisk and switch off the machine when ready.