



Deployment Guide

SUSE Linux Enterprise Desktop 12 SP2



Deployment Guide

SUSE Linux Enterprise Desktop 12 SP2

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.


Publication Date: October 19, 2016

SUSE LLC
10 Canal Park Drive
Suite 200
Cambridge MA 02141
USA

<https://www.suse.com/documentation> 

Copyright © 2006– 2016 SUSE LLC and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled “GNU Free Documentation License”.

For SUSE trademarks, see <http://www.suse.com/company/legal/> . All other third-party trademarks are the property of their respective owners. Trademark symbols (®, ™ etc.) denote trademarks of SUSE and its affiliates. Asterisks (*) denote third-party trademarks.

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

Contents

About This Guide xi

1 Planning for SUSE Linux Enterprise Desktop 1

- 1.1 Hardware Requirements 1
- 1.2 Reasons to Use SUSE Linux Enterprise Desktop 2

I THE INSTALLATION WORKFLOW 4

2 Installation with YaST 5

- 2.1 Choosing the Installation Method 5
- 2.2 System Start-up for Installation 6
 - PC (AMD64/Intel 64/ARM AArch64): System Start-up 7 • Boot Parameters for Advanced Setups 15
- 2.3 Steps of the Installation 18
- 2.4 Installer Self-Update 19
 - Self-Update Process 20 • Networking During Self-Update 21 • Custom self-update repositories 21
- 2.5 Language, Keyboard and License Agreement 22
- 2.6 Network Settings 22
- 2.7 SUSE Customer Center Registration 24
 - Loading Registration Codes from USB Storage 26
- 2.8 Extension Selection 27
- 2.9 Suggested Partitioning 30
- 2.10 Clock and Time Zone 33
- 2.11 Create New User 35
 - Expert Settings 37

- 2.12 Password for the System Administrator root 37
- 2.13 Installation Settings 39
 - Software* 39 • *Booting* 40 • *Firewall and SSH* 41 • *Default systemd Target* 42 • *Import SSH Host Keys and Configuration* 42 • *System* 43
- 2.14 Performing the Installation 44

II SETTING UP AN INSTALLATION SERVER 45

3 Setting Up the Server Holding the Installation Sources 46

- 3.1 Setting Up an Installation Server Using YaST 46
- 3.2 Setting Up an NFS Repository Manually 49
- 3.3 Setting Up an FTP Repository Manually 51
- 3.4 Setting Up an HTTP Repository Manually 52
- 3.5 Managing an SMB Repository 53
- 3.6 Using ISO Images of the Installation Media on the Server 54

4 Preparing the Boot of the Target System 56

- 4.1 Setting Up a DHCP Server 56
 - Setting Up a DHCP Server with YaST 56 • Setting Up a DHCP Server Manually 57
- 4.2 Setting Up a TFTP Server 58
 - Setting Up a TFTP Server Using YaST 59 • Setting Up a TFTP Server Manually 59
- 4.3 Using PXE Boot 60
- 4.4 PXELINUX Configuration Options 62
- 4.5 Preparing the Target System for PXE Boot 65
- 4.6 Preparing the Target System for Wake on LAN 66
- 4.7 Wake on LAN 66

4.8 Wake on LAN with YaST 66

III REMOTE INSTALLATION 68

5 Remote Installation 69

5.1 Installation Scenarios for Remote Installation 69

Simple Remote Installation via VNC—Static Network Configuration 69 • Simple Remote Installation via VNC—Dynamic Network Configuration 71 • Remote Installation via VNC—PXE Boot and Wake on LAN 72 • Simple Remote Installation via SSH—Static Network Configuration 73 • Simple Remote Installation via SSH—Dynamic Network Configuration 74 • Remote Installation via SSH—PXE Boot and Wake on LAN 75

5.2 Booting the Target System for Installation 76

Using the Default Boot Options 77 • Using Custom Boot Options 77

5.3 Monitoring the Installation Process 80

VNC Installation 80 • SSH Installation 82

IV INITIAL SYSTEM CONFIGURATION 84

6 Setting Up Hardware Components with YaST 85

6.1 Setting Up Your System Keyboard Layout 85

6.2 Setting Up Sound Cards 86

6.3 Setting Up a Printer 89

Configuring Printers 89 • Configuring Printing via the Network with YaST 93 • Sharing Printers Over the Network 94

6.4 Setting Up a Scanner 95

Configuring an HP All-In-One Device 95 • Sharing a Scanner over the Network 96 • Scanning over the Network 96

7 Advanced Disk Setup 98

7.1 Using the YaST Partitioner 98

Partition Types 100 • Creating a Partition 100 • Editing a Partition 104 • Expert Options 106 • Advanced Options 107 • More Partitioning Tips 107 • Partitioning and LVM 110

7.2 LVM Configuration 110

LVM Configuration with YaST 111

7.3 Soft RAID Configuration with YaST 114

Soft RAID Configuration with YaST 114 • Troubleshooting 116 • For More Information 116

8 Installing or Removing Software 117

8.1 Definition of Terms 117

8.2 Using the YaST Software Manager 119

Views for Searching Packages or Patterns 119 • Installing and Removing Packages or Patterns 120 • Updating Packages 122 • Checking Software Dependencies 124

8.3 Managing Software Repositories and Services 126

Adding Software Repositories 126 • Managing Repository Properties 128 • Managing Repository Keys 129

8.4 Keeping the System Up-to-date 129

The GNOME Software Updater 130 • Installing Patches and Package Updates 130 • Configuring the GNOME Software Updater 132

9 Installing Modules, Extensions, and Third Party Add-On Products 134

9.1 Installing Modules and Extensions from Online Channels 134

9.2 Installing Extensions and Third Party Add-On Products from Media 137

9.3 SUSE Software Development Kit (SDK) 12 SP2 139

10 Installing Multiple Kernel Versions 140

- 10.1 Enabling and Configuring Multiversion Support 140
 - Automatically Deleting Unused Kernels 141
- 10.2 Installing/Removing Multiple Kernel Versions with YaST 142
- 10.3 Installing/Removing Multiple Kernel Versions with Zypper 143

11 Managing Users with YaST 145

- 11.1 User and Group Administration Dialog 145
- 11.2 Managing User Accounts 147
- 11.3 Additional Options for User Accounts 148
 - Automatic Login and Passwordless Login 149 • Enforcing Password Policies 149 • Managing Encrypted Home Directories 150 • Managing Quotas 152
- 11.4 Changing Default Settings for Local Users 155
- 11.5 Assigning Users to Groups 155
- 11.6 Managing Groups 156
- 11.7 Changing the User Authentication Method 158

12 Changing Language and Country Settings with YaST 160

- 12.1 Changing the System Language 160
 - Modifying System Languages with YaST 161 • Switching the Default System Language 163 • Switching Languages for Standard X and GNOME Applications 164
- 12.2 Changing the Country and Time Settings 164

V UPDATING AND UPGRADING SUSE LINUX ENTERPRISE 167

13 Life Cycle and Support 168

- 13.1 Terminology 168

- 13.2 Product Life Cycle 170
- 13.3 Support Levels 171
- 13.4 Repository Model 174
 - Origin of Packages 176 • Register and Unregister Repositories with SUSEConnect 176 • IBM POWER: Starting an X-Server 177
- 14 Upgrading SUSE Linux Enterprise 178**
 - 14.1 General Preparations 178
 - Temporarily Disable Kernel Multiversion Support 178 • Check the Release Notes 178 • Make a Backup 179 • Migrate your MySQL Database 179 • Migrate your PostgreSQL Database 180 • Create Non-MD5 Server Certificates for Java Applications 182 • Shut Down Virtual Machine Guests 183 • Check the **clientSetup4SMT.sh** script on SMT clients 183
 - 14.2 Disk Space 183
 - Checking Disk Space on Non-Btrfs File Systems 184 • Checking Disk Space on Btrfs Root File Systems 184
 - 14.3 Supported Upgrade Paths for SLE 185
 - 14.4 Supported Methods for Upgrading SUSE Linux Enterprise 186
 - 14.5 Upgrading Manually from SLE 11 SP3 to SLE 12 SP1, Using an Installation Source 186
 - Upgrading from an Installation Medium 187 • Upgrading from a Network Installation Source 188
 - 14.6 Migrating Automatically from SLE 11 SP3 or SP4 to SLE 12 SP1 189
 - 14.7 Starting the Upgrade Process After Booting 190
 - 14.8 Updating via SUSE Manager 192
 - 14.9 Updating Registration Status After Rollback 192
 - 14.10 Registering Your System 193

- 14.11 Retaining Kernel Packages 194
 - Enabling the Multiversion Kernel Feature 194 • Use Case: Deleting an Old Kernel After Reboot Only 195 • Use Case: Keeping Older Kernels as Fall-back 195 • Use Case: Keep a Specific Kernel Version 196

15 Service Pack Migration 197

- 15.1 Conceptual Overview 197
- 15.2 Supported Software Scenarios and Product Versions 197
- 15.3 Service Pack Migration Workflow 198
- 15.4 Canceling Service Pack Migration 199
- 15.5 Migrating with the Online Migration Tool (YaST) 199
- 15.6 Migrating with Zypper 200
- 15.7 Migrating with Plain Zypper 202
- 15.8 Rolling Back a Service Pack 204

16 Backporting Source Code 206

- 16.1 Reasons for Backporting 206
- 16.2 Reasons against Backports 207
- 16.3 The Implications of Backports for Interpreting Version Numbers 208
- 16.4 How to Check Which Bugs are Fixed and Which Features are Backported and Available 208

A Documentation Updates 210

- A.1 November 2016 (Initial Release of SUSE Linux Enterprise Desktop 12 SP2) 210
- A.2 March 2016 (Maintenance Release of SUSE Linux Enterprise Desktop 12 SP1) 211

A.3 December 2015 (Initial Release of SUSE Linux Enterprise Desktop 12 SP1) **212**

A.4 February 2015 (Documentation Maintenance Update) **215**

A.5 October 2014 (Initial Release of SUSE Linux Enterprise Desktop 12) **216**

B GNU Licenses 220

B.1 GNU Free Documentation License **220**

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, "The Installation Workflow"

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

Part II, "Setting up an Installation Server"

SUSE® Linux Enterprise Desktop can be installed in different ways. Apart from the usual media installation, you can choose from various network-based approaches. This part describes setting up an installation server and how to prepare the boot of the target system for installation.

Part III, "Remote Installation"

This part introduces the most common installation scenarios for remote installations. While some still require user interaction or some degree of physical access to the target system, others are completely automated and hands-off. Learn which approach is best for your scenario.


Part IV, "Initial System Configuration"

Learn how to configure your system after installation. This part covers common tasks like setting up hardware components, installing or removing software, managing users, or changing settings with YaST.

Part V, "Updating and Upgrading SUSE Linux Enterprise"

This part will give you some background information on terminology, SUSE product life-cycles and Service Pack releases, and recommended upgrade policies.

Many chapters in this manual contain links to additional documentation resources, including additional documentation that is available on the system and documentation available on the Internet.

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

1 Required Background

To keep the scope of these guidelines manageable, certain technical assumptions have been made:

- You have some computer experience and are familiar with common technical terms.
- You are familiar with the documentation for your system and the network on which it runs.
- You have a basic understanding of Linux systems.

2 Available Documentation

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

Article “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.

Deployment Guide

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.

Book “Administration Guide”

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

Book “Security Guide”

Introduces basic concepts of system security, covering both local and network security aspects. Shows how to use the product inherent security software like AppArmor or the auditing system that reliably collects information about any security-relevant events.

Book “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.

Book “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 as their default desktop.

Find HTML versions of most product manuals in your installed system under `/usr/share/doc/manual`. The latest documentation updates are available at <http://www.suse.com/documentation/> where you can download the documentation for your product in various formats.

3 Feedback

Several feedback channels are available:

Bugs and Enhancement Requests

For services and support options available for your product, refer to <http://www.suse.com/support/>.

To report bugs for a product component, go to <https://scc.suse.com/support/requests>, log in, and click *Create New*.

User Comments



We want to hear your comments about and suggestions for this manual and the other documentation included with this product. Use the User Comments feature at the bottom of each page in the online documentation or go to <http://www.suse.com/documentation/feedback.html> and enter your comments there.

Mail

For feedback on the documentation of this product, you can also send a mail to doc-team@suse.com. Make sure to include the document title, the product version and the publication date of the documentation. To report errors or suggest enhancements, provide a concise description of the problem and refer to the respective section number and page (or URL).

4 Documentation Conventions

The following notices and typographical conventions are used in this documentation:

- /etc/passwd: directory names and file names
- PLACEHOLDER: replace PLACEHOLDER with the actual value
- PATH: the environment variable PATH
- ls, --help: commands, options, and parameters
- user: users or groups
- package name : name of a package
- , : 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.
- Commands that must be run with root privileges. Often you can also prefix these commands with the sudo command to run them.

```
root # command
```

- Commands that can be run by non-privileged users.

```
tux > command
```

- Notices



Warning: Warning Notice

Vital information you must be aware of before proceeding. Warns you about security issues, potential loss of data, damage to hardware, or physical hazards.



Important: Important Notice

Important information you should be aware of before proceeding.



Note: Note Notice

Additional information, for example about differences in software versions.



Tip: Tip Notice

Helpful information, like a guideline or a piece of practical advice.

1 Planning for SUSE Linux Enterprise Desktop

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 with the ability 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 installations planned, consider different approaches to the installation or even a mass installation using SUSE Linux Enterprises unique AutoYaST or KIWI technology.

How do you get software updates for your deployment?

All patches provided by SUSE for your product are available for download to registered users at <http://download.suse.com/> .

Do you need help for your local deployment?

SUSE provides training, support, and consulting for all topics pertaining to SUSE Linux Enterprise Desktop. Find more information about this at <http://www.suse.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 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 the enterprise-ready desktop environment GNOME. It enables users to comfortably adjust to a Linux system while maintaining their efficiency and productivity. To explore GNOME in detail, refer to the *Book "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, as well as the means to

manipulate your Windows user data from a Linux client. Explore this feature in detail in *Book “Security Guide”, Chapter 6 “Active Directory Support”*.

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 AppArmor

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

I The Installation Workflow

2 Installation with YaST 5

2 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 of your system. 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 preferences. Help for each installation step is provided by clicking *Help*.

During the installation process, YaST analyzes both your current system settings and your hardware components. Based on this analysis your system will be set up with a basic configuration including networking (provided the system could be configured using DHCP). To fine-tune the system after the installation has finished, start YaST from the installed system.

2.1 Choosing the Installation Method

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

Installing from the SUSE Linux Enterprise Desktop Media (DVD, USB)

Choose this option if you want to perform a stand-alone installation and do not want to rely on a network to provide the installation data or the boot infrastructure. The installation proceeds exactly as outlined in [Section 2.3, “Steps of the Installation”](#).

Installing from the LiveCD

To install from a LiveCD, boot the live system from CD. In the running system, launch the installation routine by clicking the *Install* icon on the desktop. The installation will be executed in a window on the desktop. It is not possible to update an existing system with a LiveCD, you can only perform an installation from scratch.

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 boot from physical media (flash disk, CD/DVD, or hard disk) or configured to boot via network using PXE/BOOTP. Refer to [Section 2.2, “System Start-up for Installation”](#) for details.

The installation program configures the network connection with DHCP and retrieves the location of the network installation source from the OpenSLP server. If no DHCP is available, choose *F4 Source > Network Config > Manual* and enter the network data. On EFI systems modify the network boot parameters as described in [Section 2.2.1.2, “The Boot Screen on Machines Equipped with UEFI”](#).

Installing from an SLP Server. If your network setup supports OpenSLP and your network installation source has been configured to announce itself via SLP (described in [Chapter 3, Setting Up the Server Holding the Installation Sources](#)), boot the system, press **F4** in the boot screen and select *SLP* from the menu. On EFI systems set the install parameter to install=slp:/ as described in [Section 2.2.1.2, “The Boot Screen on Machines Equipped with UEFI”](#).

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) and provide the server's address and the path to the installation media. On EFI systems modify the boot parameter install= as described in [Section 2.2.1.2, “The Boot Screen on Machines Equipped with UEFI”](#).

Installing as a SUSE Linux Enterprise Server Extension

Choose this option if you want to install SUSE Linux Enterprise Desktop on top of SUSE Linux Enterprise Server. Install SUSE Linux Enterprise Server, register at the SUSE Customer Center and choose the *SUSE Linux Enterprise Workstation Extension* on the *Extension Selection* screen.


2.2 System Start-up for Installation

The way the system is started for the installation depends on the architecture—system start-up is different for PC (AMD64/Intel 64) or mainframe, for example. If you install SUSE Linux Enterprise Desktop as a VM Guest on a KVM or Xen hypervisor, follow the instructions for the AMD64/Intel 64 architecture.

2.2.1 PC (AMD64/Intel 64/ARM AArch64): System Start-up

SUSE Linux Enterprise Desktop supports several 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 2.1: 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. |
| Flash Disks (USB Mass Storage Device) | <p>In case your machine is not equipped with an optical drive, you can boot the installation image from a flash disk. To create a bootable flash disk, you need to copy either the DVD or the Mini CD iso image to the device using the <code>dd</code> command (the flash disk must not be mounted, all data on the device will be erased):</p> <pre>dd if=PATH_TO_ISO_IMAGE of=USB_STORAGE_DEVICE bs=4M</pre> <p> Important: Compatibility</p> <p>Note that booting from a USB Mass Storage Device is <i>not</i> supported on UEFI machines and on the POWER architecture.</p> |
| 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 |

| Boot Option | Description |
|-------------|--|
| | Linux Enterprise Desktop system. Refer to <i>Chapter 5, Remote Installation</i> for more information. |
| 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

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.



Note: Add-on Product Installation Media

Media for add-on products (extensions or third-party products) cannot be used as stand-alone installation media. They can either be embedded as additional installation sources during the installation process (see *Section 2.8, "Extension Selection"*) or be installed from the running system using the YaST Add-on Products module (see *Chapter 9, Installing Modules, Extensions, and Third Party Add-On Products* for details).

2.2.1.1 The Boot Screen on Machines Equipped with Traditional BIOS

The boot screen displays several options for the installation procedure. *Boot from Hard Disk* boots the installed system and is selected by 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 **F5** *Kernel* for boot options that disable potentially problematic functions.

Upgrade

Perform a system upgrade. For more information refer to *Chapter 14, Upgrading SUSE Linux Enterprise*.

Rescue System

Starts a minimal Linux system without a graphical user interface. For more information, see Book “Administration Guide”, Chapter 32 “Common Problems and Their Solutions”, Section 32.6.2 “Using the Rescue System”. This option is not available on LiveCDs.

Check Installation Media

This option is only available when you install from media created from downloaded ISOs. In this case it is recommended to check the integrity of the installation medium. This option starts the installation system before automatically checking the media. In case the check was successful, the normal installation routine starts. If a corrupt media is detected, the installation routine aborts.



Warning: Failure of Media Check

If the media check fails, your medium is damaged. Do not continue the installation because installation may fail or you may lose your data. Replace the broken medium and restart the installation process.

Memory Test

Tests your system RAM using repeated read and write cycles. Terminate the test by re-booting. For more information, see Book “Administration Guide”, Chapter 32 “Common Problems and Their Solutions”, Section 32.2.4 “Fails to Boot”. This option is not available on the LiveCDs.

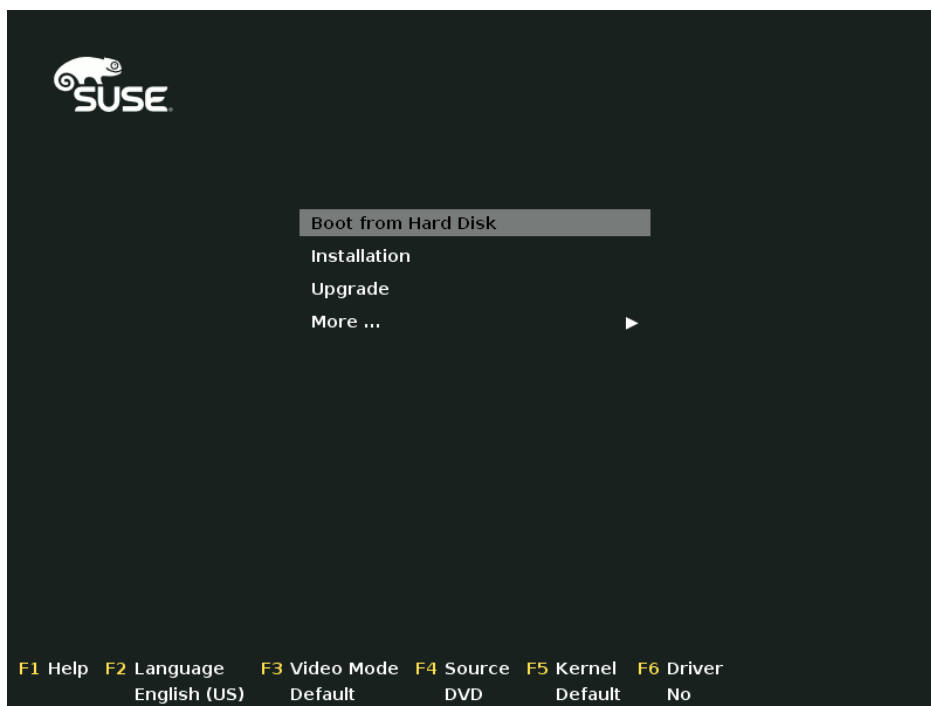


FIGURE 2.1: THE BOOT SCREEN ON MACHINES WITH A TRADITIONAL BIOS

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 an 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. By *Default* the video resolution is automatically determined using KMS (Kernel Mode Settings). If this setting does not work on your system, choose *No KMS* and, optionally, specify vga=ask on the boot command line to get prompted for the video resolution. Choose *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 deployed on a network with an SLP server, select an installation source available on the server with this option. Find information about setting up an installation server with SLP at *Chapter 3, Setting Up the Server Holding the Installation Sources*.

F5 Kernel

If 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.

F6 Driver

Press this key to notify 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: Getting Driver Update Disks

Driver updates for SUSE Linux Enterprise are provided at <http://drivers.suse.com/>. These drivers have been created via the SUSE SolidDriver Program.

2.2.1.2 The Boot Screen on Machines Equipped with UEFI

UEFI (Unified Extensible Firmware Interface) is a new industry standard which replaces and extends the traditional BIOS. The latest UEFI implementations contain the “Secure Boot” extension, which prevents booting malicious code by only allowing signed boot loaders to be executed. See Book “Administration Guide”, *Chapter 13 “UEFI (Unified Extensible Firmware Interface)”* for more information.

The boot manager GRUB 2, used to boot machines with a traditional BIOS, does not support UEFI, therefore GRUB 2 is replaced with GRUB 2 for EFI. If Secure Boot is enabled, YaST will automatically select GRUB 2 for EFI for installation. From an administrative and user perspective, both boot manager implementations behave the same and are called GRUB 2 in the following.



Tip: UEFI and Secure Boot are Supported by Default

The installation routine of SUSE Linux Enterprise automatically detects if the machine is equipped with UEFI. All installation sources also support Secure Boot. If an EFI system partition already exists on dual boot machines (from a Microsoft Windows 8 installation, for example), it will automatically be detected and used. Partition tables will be written as GPT on UEFI systems.



Warning: Using Non-Inbox Drivers with Secure Boot

There is no support for adding non-inbox drivers (that is, drivers that do not come with SLE) during installation with Secure Boot enabled. The signing key used for SolidDriver/PLDP is not trusted by default.

To solve this problem, it is necessary to either add the needed keys to the firmware database via firmware/system management tools before the installation or to use a bootable ISO that will enroll the needed keys in the MOK list at first boot. For more information, see *Book “Administration Guide”, Chapter 13 “UEFI (Unified Extensible Firmware Interface)”, Section 13.1 “Secure Boot”*.

The boot screen displays several options for the installation procedure. Change the selected option with the arrow keys and press to boot it. The relevant options are:

Installation

The normal installation mode.

Upgrade

Perform a system upgrade. For more information refer to [Chapter 14, Upgrading SUSE Linux Enterprise](#).

Rescue System

Starts a minimal Linux system without a graphical user interface. For more information, see *Book “Administration Guide”, Chapter 32 “Common Problems and Their Solutions”, Section 32.6.2 “Using the Rescue System”*. This option is not available on LiveCDs.

Check Installation Media

This option is only available when you install from media created from downloaded ISOs. In this case it is recommended to check the integrity of the installation medium. This option starts the installation system before automatically checking the media. In case the check was successful, the normal installation routine starts. If a corrupt media is detected, the installation routine aborts.

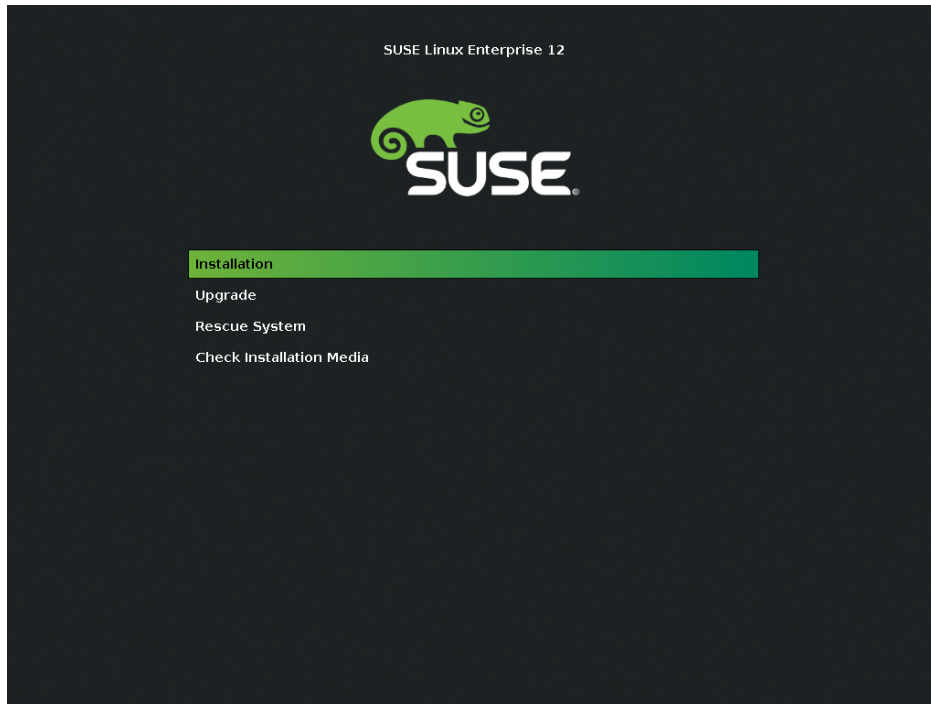


FIGURE 2.2: THE BOOT SCREEN ON MACHINES WITH UEFI

GRUB 2 for EFI on SUSE Linux Enterprise Desktop does not support a boot prompt or function keys for adding boot parameters. By default, the installation will be started with American English and the boot media as the installation source. A DHCP lookup will be performed to configure the network. To change these defaults or to add additional boot parameters you need to edit the respective boot entry. Highlight it using the arrow keys and press **E**. See the on-screen help for editing hints (note that only an English keyboard is available now). The *Installation* entry will look similar to the following:

```
setparams 'Installation'

set gfxpayload=keep
echo 'Loading kernel ...'
linuxefi /boot/x86_64/loader/linux splash=slilent
echo 'Loading initial ramdisk ...'
```

```
initrdefi /boot/x86_64/loader/initrd
```

Add space-separated parameters to the end of the line starting with `linuxefi`. To boot the edited entry, press `F10`. If you access the machine via serial console, press `Esc-0`. A complete list of parameters is available at <http://en.opensuse.org/Linuxrc>. The most important ones are:

TABLE 2.2: INSTALLATION SOURCES

| | |
|------------------|---|
| CD/DVD (default) | <u>install=cd:/</u> |
| Hard disk | <u>install=hd:/?device=sda/PATH_TO_ISO</u> |
| SLP | <u>install=slp:/</u> |
| FTP | <u>install=ftp://ftp.example.com/PATH_TO_ISO</u> |
| HTTP | <u>install=http://www.example.com/PATH_TO_ISO</u> |
| NFS | <u>install=nfs:/PATH_TO_ISO</u> |
| SMB / CIFS | <u>install=smb://PATH_TO_ISO</u> |

TABLE 2.3: NETWORK CONFIGURATION

| | |
|-----------------------|--|
| DHCP (default) | <code>netsetup = dhcp</code> |
| Prompt for Parameters | <u>netsetup=hostip,netmask,gateway,nameserver</u> |
| Host IP address | <u>hostip=192.168.2.100</u> <u>hostip=192.168.2.100/24</u> |
| Netmask | <u>netmask=255.255.255.0</u> |
| Gateway | <u>gateway=192.168.5.1</u> |
| Name Server | <u>nameserver=192.168.1.116</u> <u>nameserver=192.168.1.116,192.168.1.118</u> |
| Domain Search Path | <u>domain=example.com</u> |

TABLE 2.4: MISCELLANEOUS

| | |
|------------------------|--------------|
| Driver Updates: Prompt | <u>dud=1</u> |
|------------------------|--------------|

| | |
|-------------------------------------|---|
| Driver Updates: URL | <u>dud=ftp://ftp.example.com/PATH_TO_DRIVER</u> <u>dud=http://www.example.com/PATH_TO_DRIVER</u> |
| Installation Language | <u>Language=LANGUAGE</u> Supported values for <u>LANGUAGE</u> are, among others, <u>cs_CZ</u> , <u>de_DE</u> , <u>es_ES</u> , <u>fr_FR</u> , <u>ja_JP</u> , <u>pt_BR</u> , <u>pt_PT</u> , <u>ru_RU</u> , <u>zh_CN</u> , and <u>zh_TW</u> . |
| Kernel: No ACPI | <u>acpi=off</u> |
| Kernel: No Local APIC | <u>noapic</u> |
| Video: Disable KMS | <u>nomodeset</u> |
| Video: Start Installer in Text Mode | <u>Textmode=1</u> |

2.2.2 Boot Parameters for Advanced Setups

In case you want to configure access to a local SMT or supportconfig server for the installation, you can specify boot parameters that will be parsed by the installation routine to set up these services. The same is also true if you need IPv6 support during the installation.

2.2.2.1 Providing Data to Access an SMT Server

By default, updates for SUSE Linux Enterprise Desktop are delivered by the SUSE 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.



Note: Non-Interactive Installation Only

Providing parameters for accessing an SMT server is only needed for non-interactive installations. During an interactive installation the data can be provided during the installation (see [Section 2.7, "SUSE Customer Center Registration"](#) for details).

regurl

URL of the SMT server. This URL has a fixed format `https://FQN/center/regsvc/`. *FQN* needs to be a fully qualified host name of the SMT server. Example:

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

regcert

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:

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

local path

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

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

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

```
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, it will default to `http://FQN/smt.crt` with FQN being the name of the SMT server.

2.2.2.2 Configuring an Alternative Data Server for supportconfig

The data that supportconfig (see *Book “Administration Guide”, Chapter 31 “Gathering System Information for Support”* for more information) gathers is sent to the SUSE Customer Center by default. It is also possible to set up a local server to collect this data. If such a server is available on your network, you need to set the server's URL on the client. This information needs to be entered at the boot prompt.

supporturl. URL of the server. The URL has the format http://FQN/Path/, FQN needs to be the fully qualified host name of the server, Path needs to be replaced with the location on the server. Example:

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

2.2.2.3 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 boot prompt:

Accept IPv4 and IPv6

```
ipv6=1
```

Accept IPv6 only

```
ipv6only=1
```

2.2.2.4 Using a Proxy During the Installation

In networks enforcing the usage of a proxy server for accessing remote Web sites, registration during installation is only possible when configuring a proxy server.

To use a proxy during the installation, press **F4** on the boot screen and set the required parameters in the *HTTP Proxy* dialog. Alternatively provide the Kernel parameter proxy at the boot prompt:

```
l>proxy=http://USER:PASSWORD@proxy.example.com:PORT
```

Specifying USER and PASSWORD is optional—if the server allows anonymous access, the following data is sufficient: http://proxy.example.com:PORT.

2.2.2.5 Enabling SELinux Support

Enabling SELinux upon installation start-up enables you to configure it after the installation has been finished without having to reboot. Use the following parameters:

```
security=selinux selinux=1
```

2.2.2.6 Disabling the Installer Self-Update

During installation and upgrade, YaST will try to update itself as described [Section 2.4, “Installer Self-Update”](#) in order to solve potential bugs discovered after release. The `self_update` parameter can be used to modify the behaviour of this feature.

To disable the installer self-update set the parameter to `0`.

```
self_update=0
```

To use a user-defined repository, just specify the URL:

```
self_update=https://updates.example.com/
```

2.3 Steps of the Installation

The interactive installation of SUSE Linux Enterprise Desktop split into several steps is listed below. For a description of how to perform non-interactive, automated installations, refer to https://www.suse.com/documentation/sles-12/book_autoyast/data/book_autoyast.html ↗

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 `[→]` 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 `[→]`.

1. [Section 2.4, “Installer Self-Update”](#)
2. [Section 2.5, “Language, Keyboard and License Agreement”](#)
3. [Section 2.6, “Network Settings”](#)
4. [Section 2.7, “SUSE Customer Center Registration”](#)
5. [Section 2.8, “Extension Selection”](#)
6. [Section 2.9, “Suggested Partitioning”](#)
7. [Section 2.10, “Clock and Time Zone”](#)
8. [Section 2.11, “Create New User”](#)
9. [Section 2.12, “Password for the System Administrator root”](#)
10. [Section 2.13, “Installation Settings”](#)
11. [Section 2.14, “Performing the Installation”](#)

2.4 Installer Self-Update

During the installation or upgrade process, YaST is able to update itself in order to solve bugs in the installer that were discovered after the release. The self-update is performed automatically but it can be disabled if desired. Check out [Section 2.2.2.6, “Disabling the Installer Self-Update”](#) for further information.

Although this feature was designed to run without user intervention, it is worth to know how it works. If you're not interested, you can jump directly into [Section 2.5, “Language, Keyboard and License Agreement”](#) and skip the rest of this section.



Tip: Language Selection

The installer self-update is executed before the language selection step. That means that progress and errors which happens during this process are by default displayed in English.

To use another language for this part of the installer, press **F2** in the DVD boot menu and select the language from the list. Or just use the language boot parameter (e.g. language=de_DE).

2.4.1 Self-Update Process

The process can be broken down into two different parts:

1. Determine updates repository URL.
2. Download and apply the updates to the installation system.

2.4.1.1 Determining the Updates Repository URL

Updates are distributed as regular RPM packages through a dedicated repository, so the first step is to find out the repository URL. YaST will try the following sources of information:

1. self_update boot parameter (check [Section 2.2.2.6, “Disabling the Installer Self-Update”](#) for more details). If you specified some URL, it will take precedence over any other method.
2. /general/self_update_url profile element in case you're using AutoYaST.
3. Registration server. YaST will ask to a registration server for the URL. The server to use is determined in the following order:
 - a. The SMT specified through the regurl boot parameter ([Section 2.2.2.1, “Providing Data to Access an SMT Server”](#)).
 - b. /suse_register/reg_server profile element in case you're using AutoYaST.
 - c. Performing a SLP lookup. If a SLP server is found, YaST will ask the user if it should be used because there's no authentication involved and everybody on the local network could announce a registration server.
 - d. As a last resort, the SUSE Customer Center will be used.
4. A fallback URL defined in the installation media. If none of the previous attempts worked, the fallback URL (defined in the installation media) will be used.

2.4.1.2 Downloading and applying the updates

Once the updates repository is determined, YaST will check whether an update is available. In that case, all the updates will be downloaded and applied to the installation system.

Finally, YaST will be restarted to load the new version and the welcome screen will be shown. If no updates were available, the installation will continue without restarting YaST




Note: Updates Integrity

Updates signatures will be checked to ensure its integrity and authorship. If some signature is not correct (or is missing), the user will be asked whether she/he wants to apply the update.

2.4.2 Networking During Self-Update

Obviously, for downloading the installer updates YaST needs network. By default it tries using DHCP on all network interfaces. If there is a DHCP server in the network, then it will work automatically.

If you need a static IP setup, then you can use the `ifcfg` boot argument. See [linuxrc documentation \(http://en.opensuse.org/Linuxrc\)](http://en.opensuse.org/Linuxrc)  for more details.

2.4.3 Custom self-update repositories

YaST can use a user-defined repository instead of the official one specifying an URL through the `self_update` boot option. However, the following points should be considered:

- Only HTTP/HTTPS and FTP repositories are supported.
- Only RPM-MD repositories are supported (required by SMT).
- Packages are not installed in the usual way: they're just uncompressed and no scripts are executed.
- No dependency checks are performed. Packages are installed in alphabetical order.
- Files from the packages override those files from the original installation media. That means that the update packages might not need to contain all files, just the changed ones. The unchanged files can be omitted to save memory and download bandwidth.



Note: Only One Repository

Currently, it's not possible to use more than one repository as source of updates.

2.5 Language, Keyboard and License Agreement

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 box. The language selected here is also used to assume a time zone for the system clock. This setting can be modified later in the installed system as described in [Chapter 12, Changing Language and Country Settings with YaST](#).

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.

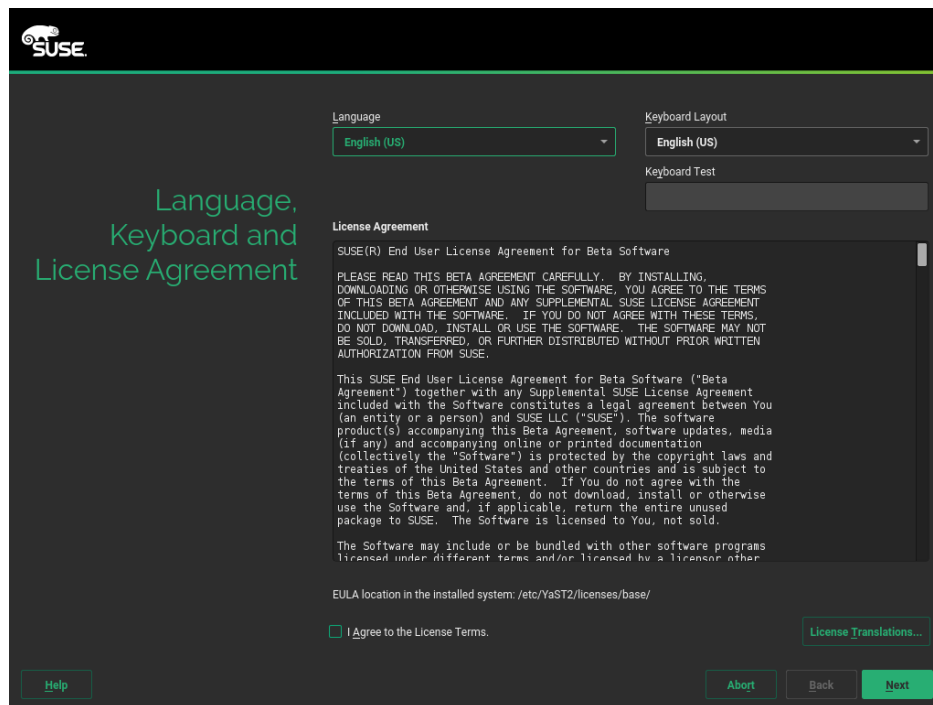


FIGURE 2.3: LANGUAGE, KEYBOARD AND LICENSE AGREEMENT

2.6 Network Settings

After booting into the installation, the installation routine is set up. During this setup, an attempt to configure at least one network interface with DHCP is made. In case this attempt fails, the *Network Settings* dialog launches. Choose a network interface from the list and click *Edit* to

change its settings. Use the tabs to configure DNS and routing. See *Book “Administration Guide”, Chapter 16 “Basic Networking”, Section 16.4 “Configuring a Network Connection with YaST”* for more details.

In case DHCP was successfully configured during installation setup, you can also access this dialog by clicking *Network Configuration* at the *SUSE Customer Center Registration* step. It lets you change the automatically provided settings.



Note: Network Interface Configured via linuxrc

If at least one network interface is configured via linuxrc, automatic DHCP configuration is disabled and configuration from linuxrc is imported and used.

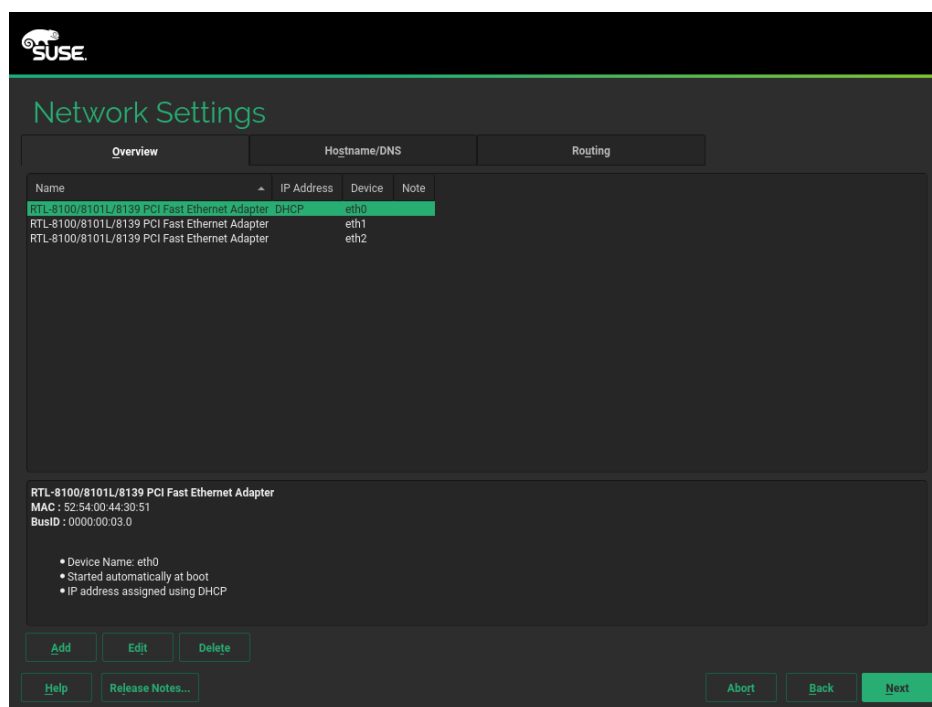


FIGURE 2.4: NETWORK SETTINGS



Tip: Accessing Network Storage or Local RAID

In case you need to access a SAN or a local RAID during the installation, you can use the `libstorage` command line client for this purpose:

1. Switch to a console with `Ctrl-Alt-F2`.

2. Install the libstoragemgmt extension by running `extend libstoragemgmt`.
3. Now you have access to the `lsmcli` command. For more information, run `lsmcli --help`.
4. To return to the installer, press `Alt-F7`

Supported are Netapp Ontap, all SMI-S compatible SAN providers, and LSI MegaRAID.

2.7 SUSE Customer Center Registration

To get technical support and product updates, you need to register and activate your product with the SUSE Customer Center. Registering SUSE Linux Enterprise Desktop now grants you immediate access to the update repository. This enables you to install the system with the latest updates and patches available. If you are offline or want to skip this step, select *Skip Registration*. You can register your system at any time later from the installed system.



Note: Network Configuration

After booting into the installation, the installation routine is set up. During this setup, an attempt to configure all network interfaces with DHCP is made. In case DHCP is not available or if you want to modify the network configuration, click *Network Configuration* in the upper right corner of the *SUSE Customer Center Registration* screen. The YaST module *Network Settings* opens. See Book “Administration Guide”, Chapter 16 “Basic Networking”, Section 16.4 “Configuring a Network Connection with YaST” for details.

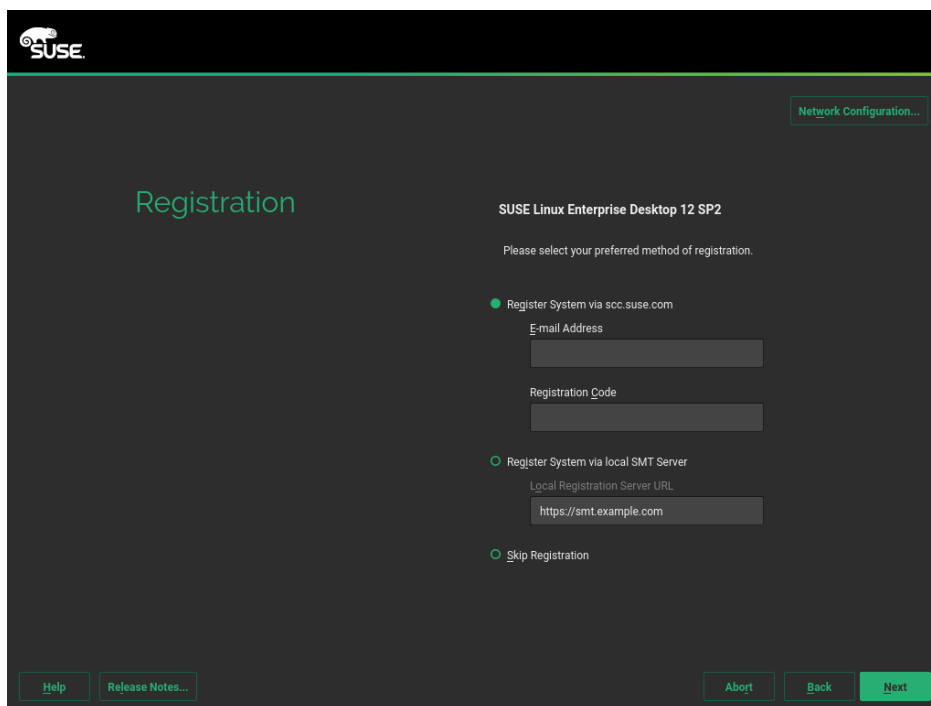


FIGURE 2.5: SUSE CUSTOMER CENTER REGISTRATION

To register your system, provide the *E-mail* address associated with the SUSE account you or your organization uses to manage subscriptions. In case you do not have a SUSE account yet, go to the SUSE Customer Center home page (<https://scc.suse.com/>) to create one.

Enter the *Registration Code* you received with your copy of SUSE Linux Enterprise Desktop. YaST can also read registration codes from a USB storage device such as a flash disk. For details, see [Section 2.7.1, “Loading Registration Codes from USB Storage”](#).

Proceed with *Next* to start the registration process. If one or more local registration servers are available on your network, you can choose one of them from a list—by default SUSE Linux Enterprise Desktop is registered at the SUSE Customer Center. If your local registration server was not discovered automatically, choose *Cancel*, select *Register System via local SMT Server* and enter the URL of the server. Restart the registration by choosing *Next* again.

During the registration, the online update repositories will be added to your installation setup. When finished, you can choose whether to install the latest available package versions from the update repositories. This ensures that SUSE Linux Enterprise Desktop is installed with the latest security updates available. If you choose *No*, all packages will be installed from the installation media. Proceed with *Next*.

If the system was successfully registered during installation, YaST will disable repositories from local installation media such as CD/DVD or flash disks when the installation has been completed. This prevents problems if the installation source is no longer available and ensures that you always get the latest updates from the online repositories.



Tip: Release Notes

From this point on, the Release Notes can be viewed from any screen during the installation process by selecting *Release Notes*.

2.7.1 Loading Registration Codes from USB Storage

To make the registration more convenient, you can also store your registration codes on a USB storage device such as a flash disk. YaST will automatically pre-fill the corresponding text box. This is particularly useful when testing the installation or if you need to register many systems or extensions.



Note: Limitations

Currently flash disks are only scanned during installation or upgrade, but not when registering a running system.

Create a file named `regcodes.txt` or `regcodes.xml` on the USB disk. If both are present, the XML takes precedence.

In that file, identify the product with the name returned by `zypper search --type product` and assign it a registration code as follows:

EXAMPLE 2.1: `regcodes.txt`

```
SLES    cc36aae1
SLED    309105d4

sle-we  5eedd26a
sle-live-patching 8c541494
```

EXAMPLE 2.2: `regcodes.xml`

```
<?xml version="1.0"?>
```

```

<profile xmlns="http://www.suse.com/1.0/yast2ns"
  xmlns:config="http://www.suse.com/1.0/configns">
  <suse_register>
    <addons config:type="list">
      <addon>
        <name>SLES</name>
        <reg_code>cc36aae1</reg_code>
      </addon>
      <addon>
        <name>SLED</name>
        <reg_code>309105d4</reg_code>
      </addon>
      <addon>
        <name>sle-we</name>
        <reg_code>5eedd26a</reg_code>
      </addon>
      <addon>
        <name>sle-live-patching</name>
        <reg_code>8c541494</reg_code>
      </addon>
    </addons>
  </suse_register>
</profile>

```

Note that SLES and SLED are not extensions, but listing them as add-ons allows for combining several base product registration codes in a single file.

2.8 Extension Selection

If you have successfully registered your system in the previous step, a list of available modules and extensions based on SUSE Linux Enterprise Desktop is shown. Otherwise this configuration step is skipped. It is also possible to add modules and extensions from the installed system, see [Chapter 9, Installing Modules, Extensions, and Third Party Add-On Products](#) for details.

The list contains free modules for SUSE Linux Enterprise Desktop, such as the SUSE Linux Enterprise SDK and extensions requiring a registration key that is liable for costs. Click an entry to see its description. Select a module or extension for installation by activating its check mark. This will add its repository from the SUSE Customer Center server to your installation—no additional installation sources are required. Furthermore the installation pattern for the module or extension is added to the default installation to ensure it gets installed automatically.

The amount of available extensions and modules depends on the registration server. A local registration server may only offer update repositories and no additional extensions.



Tip: Modules

Modules are fully supported parts of SUSE Linux Enterprise Desktop with a different life cycle. They have a clearly defined scope and are delivered via online channel only. Registering at the SUSE Customer Center is a prerequisite for being able to subscribe to these channels.



Tip: SUSE Linux Enterprise Desktop

As of SUSE Linux Enterprise 12, SUSE Linux Enterprise Desktop is not only available as a separate product, but also as a workstation extension for SUSE Linux Enterprise Server. If you register at the SUSE Customer Center, the SUSE Linux Enterprise Workstation Extension can be selected for installation. Note that installing it requires a valid registration key.

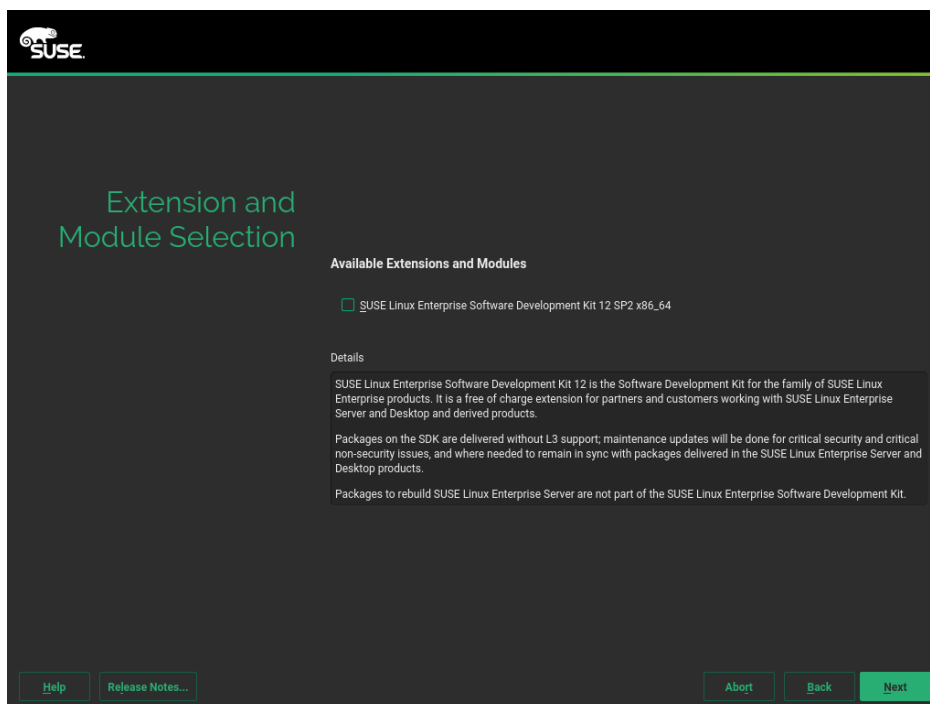


FIGURE 2.6: EXTENSION SELECTION

Proceed with *Next* to the *Add-on Product* dialog, where you can specify sources for additional add-on products not available on the registration server.

If you do not want to install add-ons, proceed with *Next*. Otherwise activate *I would like to install an additional Add-on Product*. Specify the Media Type by choosing from CD, DVD, Hard Disk, USB Mass Storage, a Local Directory or a Local ISO Image. In case network access has been configured you can choose from additional remote sources such as HTTP, SLP, FTP, etc. Alternatively you may directly specify a URL. Check *Download Repository Description Files* to download the files describing the repository now. If deactivated, they will be downloaded after the installation starts. Proceed with *Next* and insert a CD or DVD if required.

Depending on the add-on's content it may be necessary to accept additional license agreements. If you have chosen an add-on product requiring a registration key, you will be asked to enter it at the *Extension and Module Registration Codes* page. Proceed with *Next*.

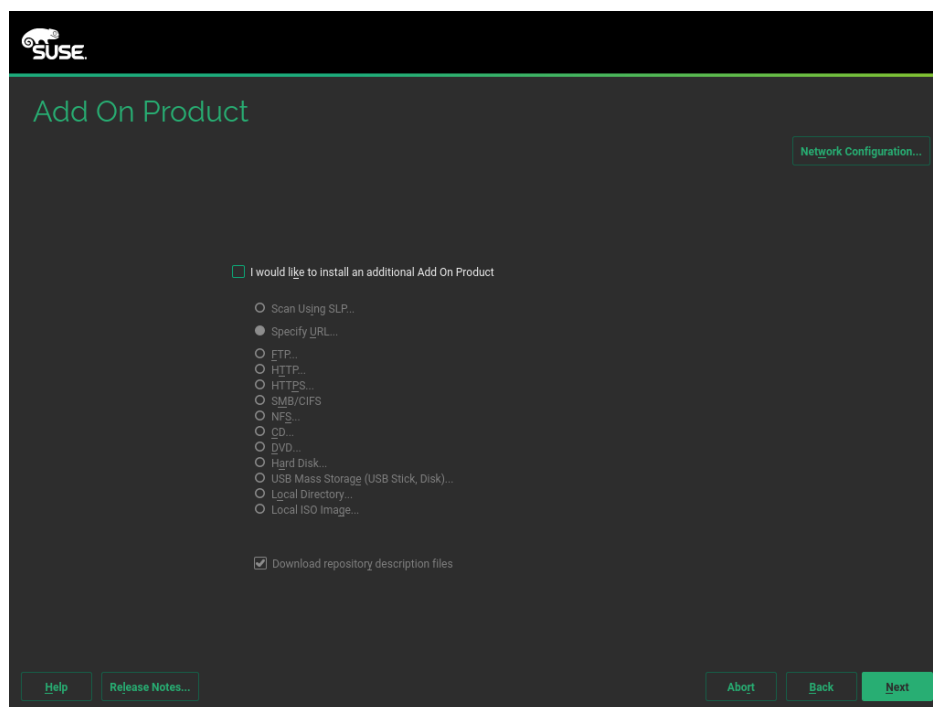


FIGURE 2.7: ADD-ON PRODUCT



Tip: “No Registration Key” Error

In case you have chosen a product in the *Extension Selection* dialog for which you do not have a valid registration key, choose *Back* until you see the *Extension Selection* dialog. Deselect the module or extension and proceed with *Next*. Modules or extensions can also be installed at any time later from the running system as described in [Chapter 9, Installing Modules, Extensions, and Third Party Add-On Products](#).

2.9 Suggested Partitioning

Define a partition setup for SUSE Linux Enterprise Desktop in this step. The installer creates a proposal for one of the available disks containing a root partition formatted with Btrfs, a swap partition, and a home partition formatted with XFS. On hard disks smaller than 25 GB the proposal does not include a separate home partition. If one or more swap partitions have been detected on the available hard disks, these existing ones will be used (rather than proposing a new swap partition). You have several options to proceed:

Next

To accept the proposal without any changes, click *Next* to proceed with the installation workflow.

Edit Proposal Settings

To adjust the proposal choose *Edit Proposal Settings*. The pop-up dialog lets you switch to an *LVM-based Proposal* or an *Encrypted LVM-based Proposal*. You may also adjust file systems for the proposed partitions, create a separate home partition, and enlarge the swap partition (to enable suspend to disk, for example).

If the root file system format is Btrfs, you can also enable Btrfs snapshots here.

Create Partition Setup

Use this option to move the proposal described above to a different disk. Select a specific disk from the list. If the chosen hard disk does not contain any partitions yet, the whole hard disk will be used for the proposal. Otherwise, you can choose which existing partition(s) to use. *Edit Proposal Settings* lets you fine-tune the proposal.

Expert Partitioner

To create a custom partition setup choose *Expert Partitioner*. The Expert Partitioner opens, displaying the current partition setup for all hard disks, including the proposal suggested by the installer. You can *Add*, *Edit*, *Resize*, or *Delete* partitions.

You can also set up Logical Volumes (LVM), configure software RAID and device mapping (DM), encrypt Partitions, mount NFS shares and manage tmpfs volumes with the Expert Partitioner. To fine-tune settings such as the subvolume and snapshot handling for each Btrfs partition, choose *Btrfs*. For more information about custom partitioning and configuring advanced features, refer to [Section 7.1, “Using the YaST Partitioner”](#).



Warning: Custom Partitioning on UEFI machines

A UEFI machine *requires* an EFI system partition that must be mounted to /boot/efi. This partition must be formatted with the FAT file system.

If an EFI system partition is already present on your system (for example from a previous Windows installation) use it by mounting it to /boot/efi without formatting it.



Warning: Custom Partitioning and Snapper

SUSE Linux Enterprise Desktop can be configured to support snapshots which provide the ability to do rollbacks of system changes. SUSE Linux Enterprise Desktop uses Snapper in conjunction with Btrfs for this feature. Btrfs needs to be set up with snapshots enabled for the root partition. Refer to *Book “Administration Guide”, Chapter 6 “System Recovery and Snapshot Management with Snapper”* for details on Snapper.

Being able to create system snapshots that enable rollbacks requires most of the system directories to be mounted on a single partition. Refer to *Book “Administration Guide”, Chapter 6 “System Recovery and Snapshot Management with Snapper”, Section 6.1 “Default Setup”* for more information. This also includes /usr and /var. Only directories that are excluded from snapshots (see *Book “Administration Guide”, Chapter 6 “System Recovery and Snapshot Management with Snapper”, Section 6.1.2 “Directories That Are Excluded from Snapshots”* for a list) may reside on separate partitions. Among others, this list includes /usr/local, /var/log, and /tmp.

If you do not plan to use Snapper for system rollbacks, the partitioning restrictions mentioned above do not apply.

Important: Btrfs on an Encrypted Root Partition

The default partitioning setup suggests the root partition as Btrfs with `/boot` being a directory. If you need to have the root partition encrypted in this setup, make sure to use the GPT partition table type instead of the default MSDOS type. Otherwise the GRUB2 boot loader may not have enough space for the second stage loader.

Note: Supported Software RAID Volumes

Installing to and booting from existing software RAID volumes is supported for Disk Data Format (DDF) volumes and Intel Matrix Storage Manager (IMSM) volumes. IMSM is also known by the following names:

- Intel Rapid Storage Technology
- Intel Matrix Storage Technology
- Intel Application Accelerator / Intel Application Accelerator RAID Edition

Important: Handling of Windows Partitions in Proposals

In case the disk selected for the suggested partitioning proposal contains a large Windows FAT or NTFS partition, it will automatically be resized to make room for the SUSE Linux Enterprise Desktop installation. To avoid data loss it is strongly recommended to

- make sure the partition is not fragmented (run a defragmentation program from Windows prior to the SUSE Linux Enterprise Desktop installation)
- double-check the suggested size for the Windows partition is big enough
- back up your data prior to the SUSE Linux Enterprise Desktop installation

To adjust the proposed size of the Windows partition, use the *Expert Partitioner*.

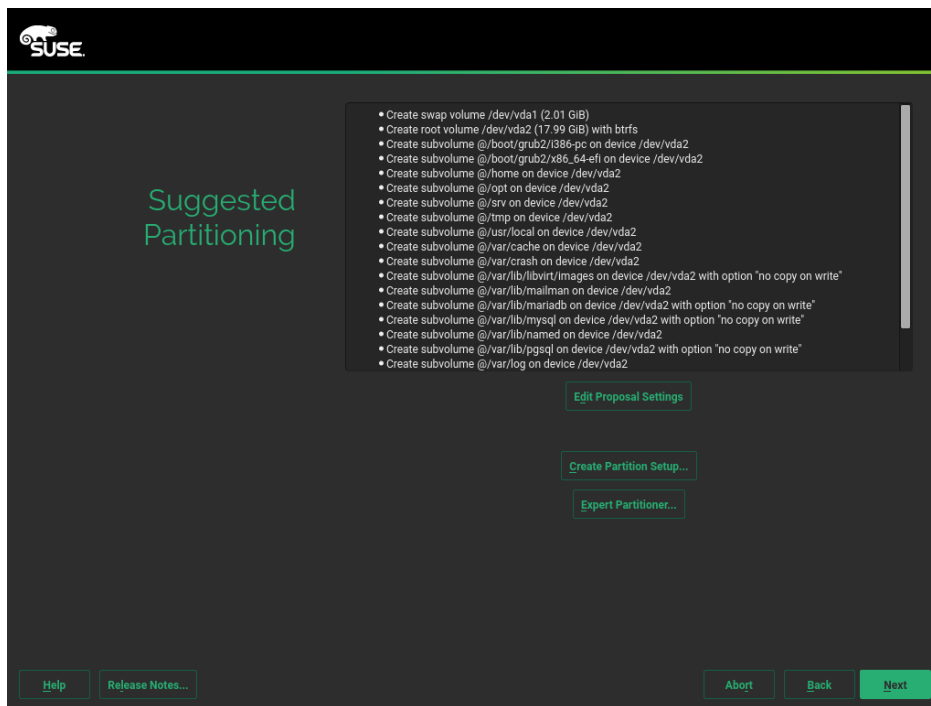


FIGURE 2.8: PARTITIONING

2.10 Clock and Time Zone

In this dialog, select your region and time zone. Both are preselected according to the installation language. To change the preselected values, either use the map or the drop-down boxes 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.

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.

! Important: Set the Hardware Clock to UTC

The switch from standard time to daylight saving time (and vice versa) can only be performed automatically when the hardware clock (CMOS clock) is set to UTC. This also applies if you use automatic time synchronization with NTP, because automatic synchronization will only be performed if the time difference between the hardware and system clock is less than 15 minutes.

Since a wrong system time can cause severe problems (missed backups, dropped mail messages, mount failures on remote file systems, etc.) it is strongly recommended to *always* set the hardware clock to UTC.

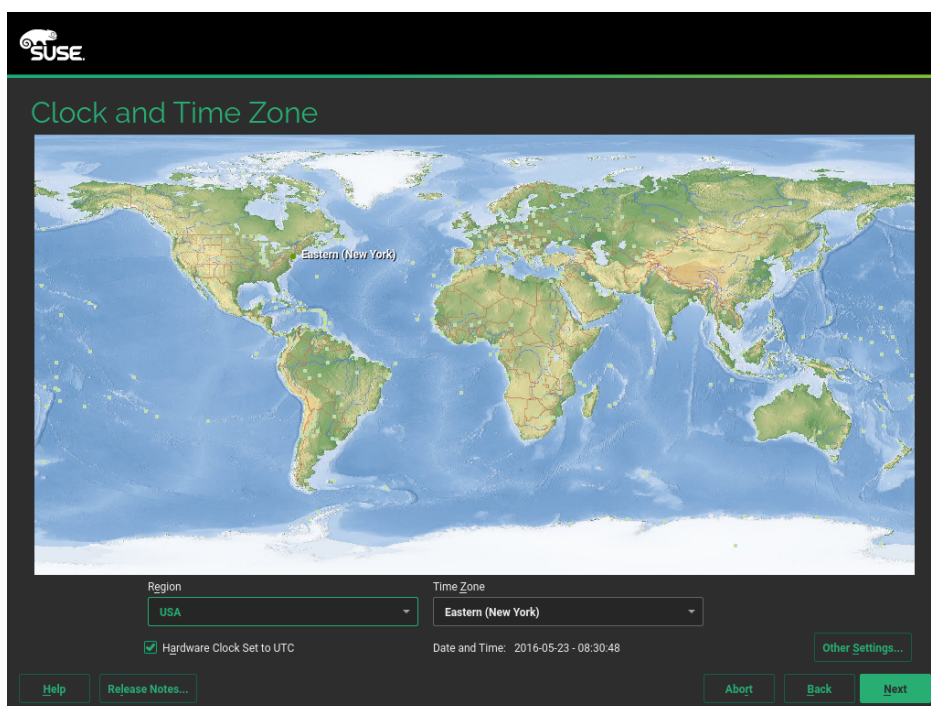


FIGURE 2.9: CLOCK AND TIME ZONE

POWER, x86_64 If a network is already configured, you can configure time synchronization with an NTP server. Click *Other Settings* to either alter the NTP settings or to *Manually* set the time. See *Book “Administration Guide”, Chapter 23 “Time Synchronization with NTP”* for more information on configuring the NTP service. When finished, click *Accept* to continue the installation. ◀

POWER, x86_64 If running without NTP configured, consider setting `SYSTOHC=no` (`sysconfig` variable) to avoid saving unsynchronized time into the hardware clock. ◀

2.11 Create New User

Create a local user in this step. After entering the first name and last name, either accept the proposal or specify a new *User name* that will be used to log in. Only use lowercase letters (a-z), digits (0-9) and the characters `.` (dot), `-` (hyphen) and `_` (underscore). Special characters, umlauts and accented characters are not allowed.

Finally, enter a password for the user. Re-enter it for confirmation (to ensure that you did not type something else by mistake). To provide effective security, a password should be at least six characters long and consist of uppercase and lowercase letters, digits and special characters (7-bit ASCII). 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: User Name and Password

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

If you install SUSE Linux Enterprise Desktop on a machine with one or more existing Linux installations, YaST allows you to import user data such as user names and passwords. Select *Import User Data from a Previous Installation* and then *Choose Users* for import.

In case you do not want to configure any local users, for example when setting up a client on a network with centralized user authentication, skip this step by choosing *Next* and confirming the warning. Network user authentication can be configured at any time later in the installed system, refer to [Chapter 11, Managing Users with YaST](#) for instructions.

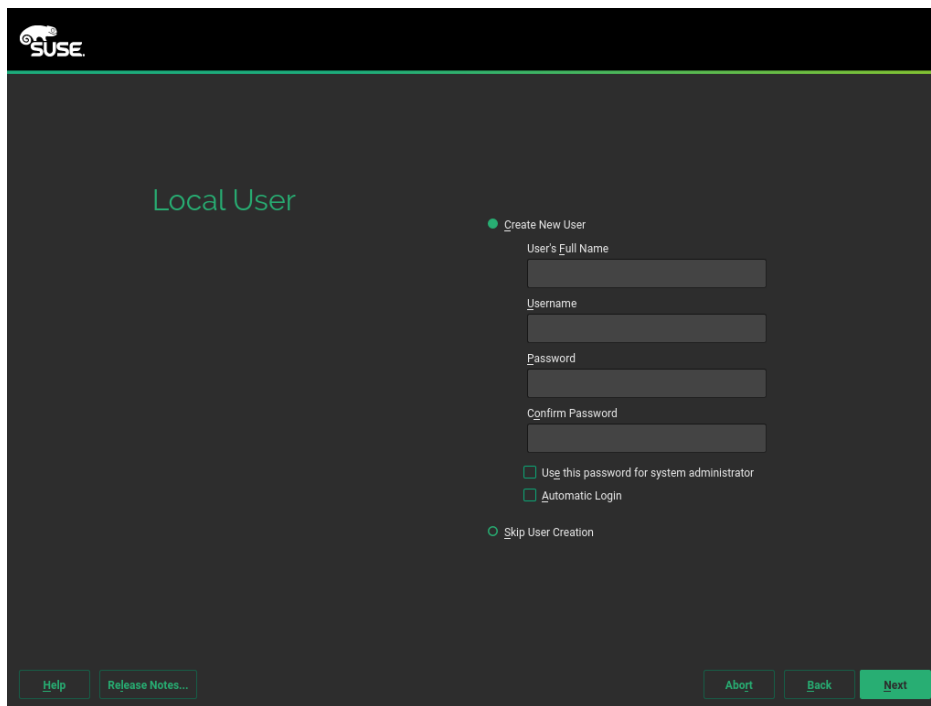


FIGURE 2.10: CREATE NEW USER

Two additional options are available:

Use this Password for 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 2.12, “Password for the System Administrator root”](#)).

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. If you store sensitive data on your system, you should not enable this option if the computer can also be accessed by others.

2.11.1 Expert Settings

Click *Change* in the Create User dialog to import users from a previous installation (if present). Also change the password encryption type in this dialog.

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*.

By default the passwords are encrypted with the SHA-512 hash function. Changing this method is not recommended unless needed for compatibility reasons.

2.12 Password for the System Administrator root

If you have not chosen *Use this Password for 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, or the administrator of the system. Unlike regular users (who may or may not have permission to access certain areas or execute certain commands on the system), root has unlimited access to 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. After having been entered, this password cannot be retrieved.

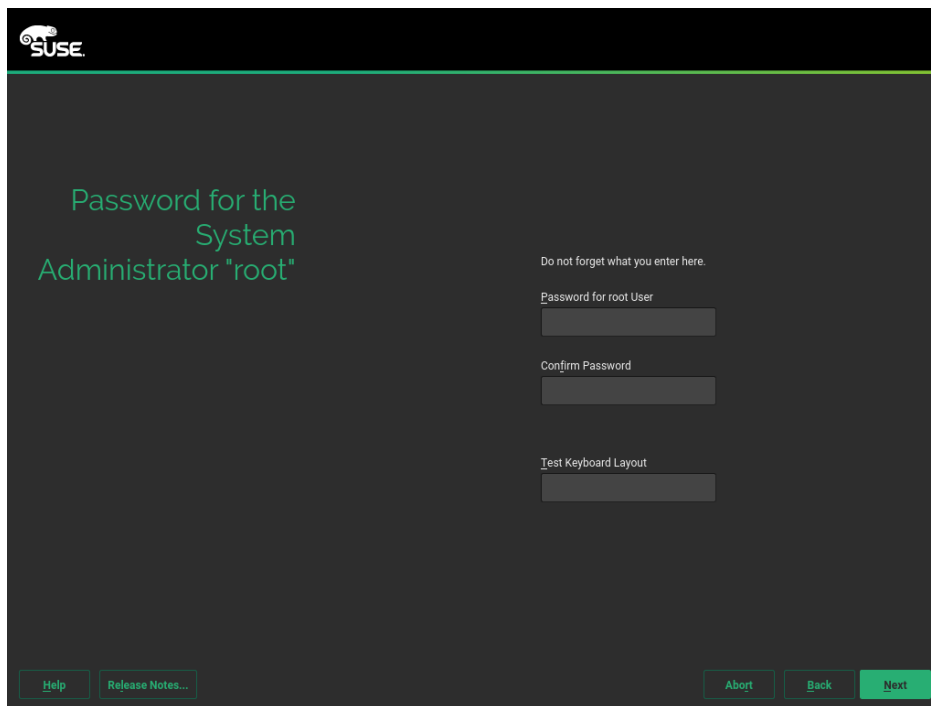


FIGURE 2.11: **PASSWORD FOR THE SYSTEM ADMINISTRATOR** root



Tip: Passwords and Keyboard Layout

It is recommended to only use characters that are available on an English keyboard. In case of a system error or when you need to start your system in rescue mode a localized keyboard might not be available.

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



Important: 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.

2.13 Installation Settings

On the last step before the real installation takes place, you can alter installation settings suggested by the installer. To modify the suggestions, click the respective headline. After having made changes to a particular setting, you are always returned to the Installation Settings window, which is updated accordingly.

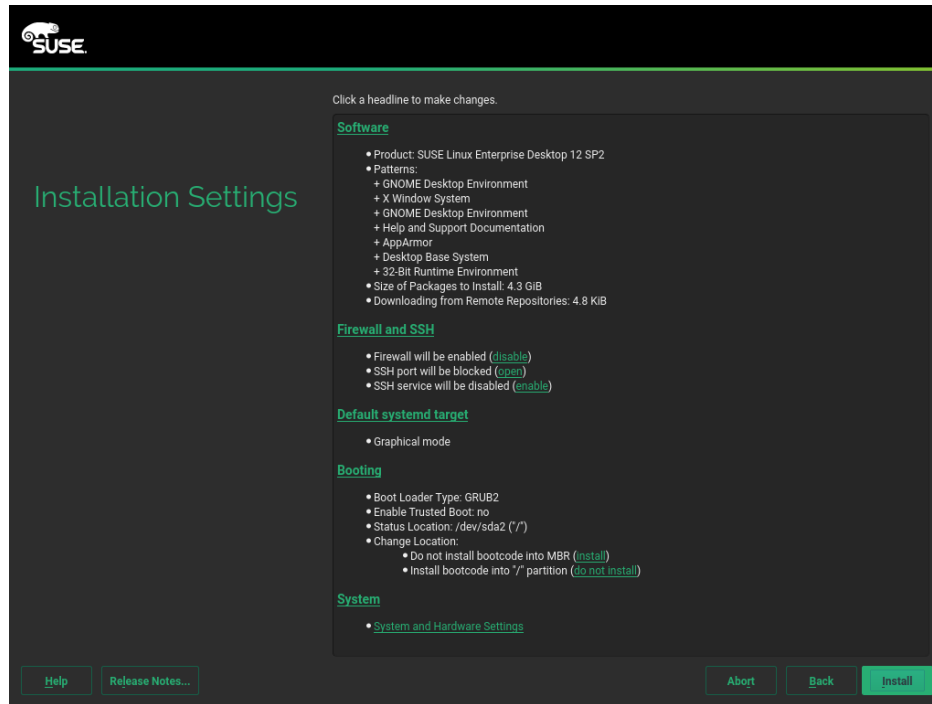


FIGURE 2.12: INSTALLATION SETTINGS

2.13.1 Software

SUSE Linux Enterprise Desktop contains several software patterns for various application purposes. Click *Software* to open the *Software Selection and System Tasks* screen where you can modify the pattern selection according to your needs. Select a pattern from the list and see a description in the right-hand part of the window. Each pattern contains several software packages needed for specific functions (for example 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 8, Installing or Removing Software](#).

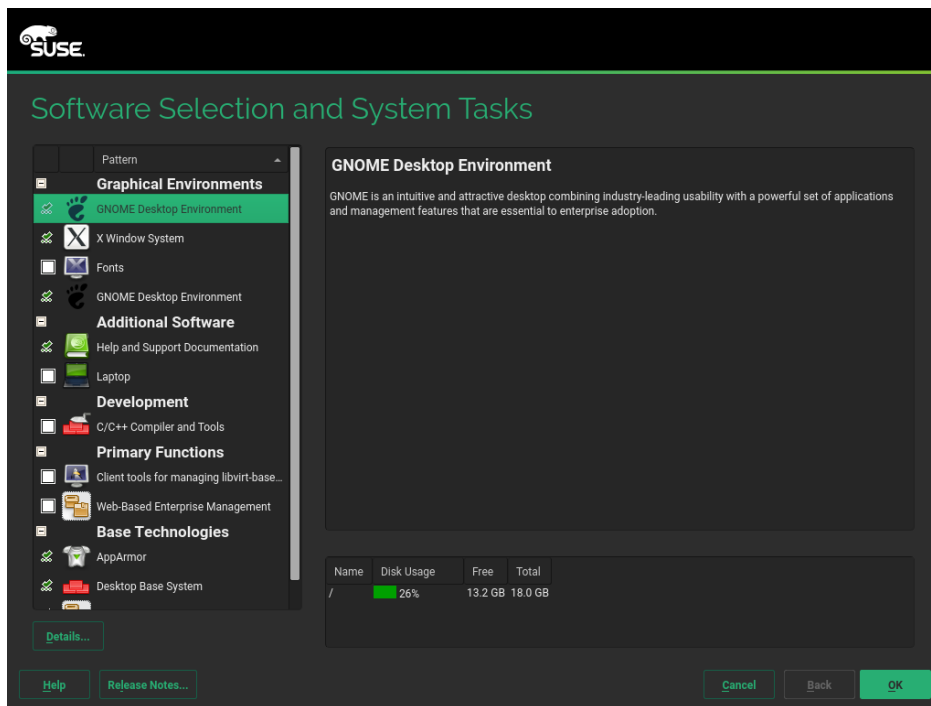


FIGURE 2.13: SOFTWARE SELECTION AND SYSTEM TASKS



Tip: Adding Secondary Languages

The language you selected with the first step of the installation will be used as the primary (default) language for the system. You can add secondary languages from within the *Software* dialog by choosing *Details* > *View* > *Languages*.

2.13.2 Booting

The installer 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 according to your needs. For information, see *Book “Administration Guide”, Chapter 12 “The Boot Loader GRUB 2”, Section 12.3 “Configuring the Boot Loader with YaST”*.

Important: Software RAID 1

Booting a configuration where /boot resides on a software RAID 1 device is supported, but it requires to install the boot loader into the MBR (*Boot Loader Location* > *Boot from Master Boot Record*). Having /boot on software RAID devices with a level other than RAID 1 is not supported.

2.13.3 *Firewall and SSH*

By default SuSEFirewall2 is enabled on all configured network interfaces. To globally disable the firewall for this computer, click *Disable* (not recommended).

Note: Firewall Settings

If the firewall is activated, all interfaces are configured to be in the “External Zone”, where all ports are closed by default, ensuring maximum security. The only port you can open during the installation is port 22 (SSH), to allow remote access. All other services requiring network access (such as FTP, Samba, Web server, etc.) will only work after having adjusted the firewall settings. Refer to *Book “Security Guide”, Chapter 15 “Masquerading and Firewalls”* for more information.

To enable remote access via the secure shell (SSH), make sure the SSH service is enabled and the SSH port is open.

Tip: Existing SSH Host Keys

If you install SUSE Linux Enterprise Desktop on a machine with one or more existing Linux installations, the installation routine imports the SSH host key with the most recent access time from an existing installation by default. See also *Section 2.13.5, “Import SSH Host Keys and Configuration”*.

In case you are performing a remote administration over VNC, you can also configure whether the machine should be accessible via VNC even after the installation. Note that enabling VNC also requires you to set the *Default systemd Target* to *graphical*.

2.13.4 *Default systemd Target*

SUSE Linux Enterprise Desktop can boot into two different targets (formerly known as “run-levels”). The *graphical* target starts a display manager, whereas the *multi-user* target starts the command line interface.

The default target is *graphical*. In case you have not installed the *X Window System* patterns, you need to change it to *multi-user*. If the system should be accessible via VNC, you need to choose *graphical*.

2.13.5 *Import SSH Host Keys and Configuration*

If an existing Linux installation on your computer was detected, YaST will import the most recent SSH host key found in `/etc/ssh` by default, optionally including other files in the directory as well. This makes it possible to reuse the SSH identity of the existing installation, avoiding the `REMOTE HOST IDENTIFICATION HAS CHANGED` warning on the first connection. Note that this item is not shown in the installation summary if YaST has not discovered any other installations.

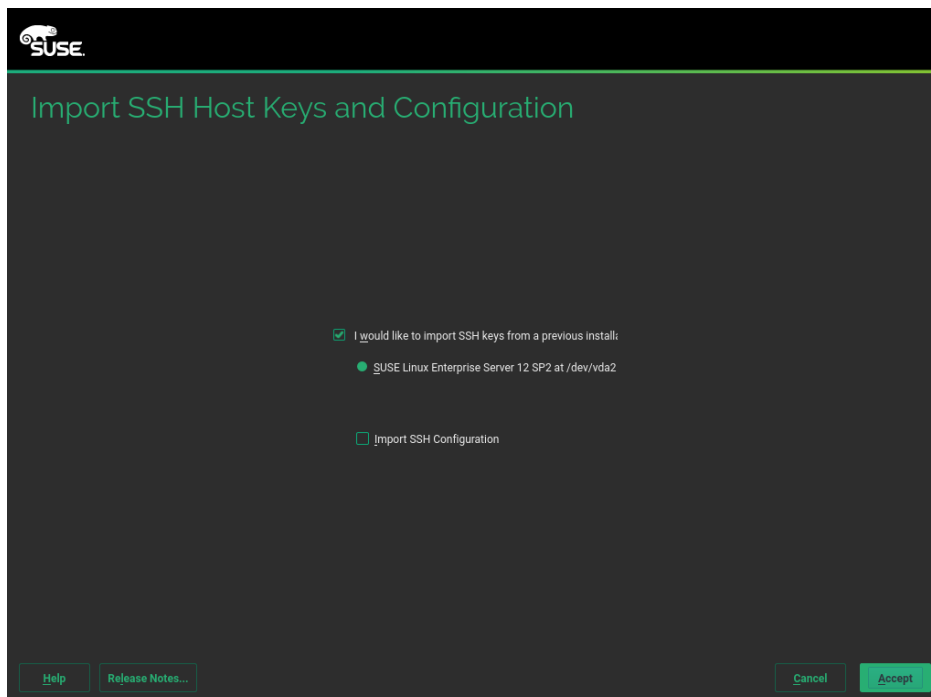


FIGURE 2.14: **IMPORT SSH HOST KEYS AND CONFIGURATION**

I would like to import SSH keys from a previous install:

Select this option if you want to import the SSH host key and optionally the configuration of an installed system. You can select the installation to import from in the option list below.

Import SSH Configuration

Enable this to copy other files in /etc/ssh to the installed system in addition to the host keys.

2.13.6 *System*

This screen lists all the hardware information the installer could obtain about your computer. When opened for the first time, the hardware detection 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 removable device.

Advanced users can also change the *PCI ID Setup* and Kernel Settings by choosing *Kernel Settings*. A screen with two tabs opens:


PCI ID Setup

Each kernel driver contains a list of device IDs of all devices it supports. If a new device is not in any driver's database, the device is treated as unsupported, even if it can be used with an existing driver. You can add PCI IDs to a device driver here. Only advanced users should attempt to do so.

To add an ID, click *Add* and select whether to *Manually* enter the data, or whether to choose from a list. Enter the required data. The *SysFS Dir* is the directory name from /sys/bus/pci/drivers—if empty, the *driver* name is used as the directory name. Existing entries can be managed with *Edit* and *Delete*.

Kernel Settings

Change the *Global I/O Scheduler* here. If *Not Configured* is chosen, the default setting for the respective architecture will be used. This setting can also be changed at any time later from the installed system. Refer to Book “System Analysis and Tuning Guide”, *Chapter 12 “Tuning I/O Performance”* for details on I/O tuning.

Also activate the *Enable SysRq Keys* here. These keys will let you issue basic commands (such as rebooting the system or writing kernel dumps) in case the system crashes. Enabling these keys is recommended when doing kernel development. Refer to <http://www.kernel.org/doc/Documentation/sysrq.txt>  for details.

2.14 Performing the Installation

After configuring 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 or *Release Notes* to read important up-to-date information that was not available when the manuals were printed.

After the software installation has completed, the system reboots into the new installation where you can log in. To customize the system configuration or to install additional software packages, start YaST.



Note: The Second Installation Stage is Gone

SUSE Linux Enterprise versions prior to 12 installed the system in two stages: the base system installation was done in stage one, the system configuration in stage two after having rebooted into the newly installed system. Starting with SUSE Linux Enterprise Desktop 12 the system installation and basic configuration including the network setup is done in a single stage. After having rebooted into the installed system, you can log in and start using the system. To fine-tune the setup, to configure services or to install additional software, start YaST.

II Setting up an Installation Server

3 Setting Up the Server Holding the Installation Sources 46

4 Preparing the Boot of the Target System 56

3 Setting Up the Server Holding the Installation Sources

SUSE® Linux Enterprise Desktop can be installed in different ways. Apart from the usual media installation covered in [Chapter 2, Installation with YaST](#), 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 checklists: 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: Terminology

In the following sections, the system to hold your new SUSE Linux Enterprise Desktop installation is called *target system* or *installation target*. The term *repository* (previously called “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.

Depending on the operating system running on the machine to use as the 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/openSUSE 11.1 or higher.



Tip: Installation Server Operating System

You can even use a Microsoft Windows machine as the installation server for your Linux deployment. See [Section 3.5, “Managing an SMB Repository”](#) for details.

3.1 Setting Up an Installation Server Using YaST

YaST offers a graphical tool for creating network repositories. 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 repository type (HTTP, FTP, or NFS). The selected 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 repository 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 repository 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 repository, 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 Book “Administration Guide”, Chapter 24 “Sharing File Systems with NFS”.



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, enable *Open Port in Firewall* or check *Firewall Details* first.

5. Configure the repository. Before the installation media are copied to their destination, define the name of the repository (ideally, an easily remembered abbreviation of the product and version). YaST allows providing ISO images of the media instead of copies of the installation DVDs. 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 necessary to add additional media, such as service pack DVDs as extra repositories. To announce your installation server in the network via OpenSLP, activate the appropriate option.



Tip: Announcing the Repository

Consider announcing your repository 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 booted using the SLP boot option and find the network repository without any further configuration. For details on this option, refer to [Section 5.2, “Booting the Target System for Installation”](#).

6. Configuring extra repositories. YaST follows a specific naming convention to configure add-on CDs or service pack CDs repositories. Configuration is accepted only if the repository name of the add-on CDs is preceded with the repository name of the installation media. In other words, if you chose SLES12SP1 as repository name for DVD1 then you should chose SLES12SP1addon repository name for DVD2. Same applies to SDK CDs.
7. Upload the installation data. The most lengthy step in configuring an installation server is copying the actual installation media. 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 repositories 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 a repository, select the repository 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 needs to provide the installation data for more than one product of the product version, start the YaST installation server module and select *Add* in the overview of existing repositories to configure the new repository.

3.2 Setting Up an NFS Repository Manually

Important

This assumes that you are using some 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 other vendor's documentation on NFS instead of following these instructions.

Setting up an NFS source for installation is done in two main 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 to hold the installation data, proceed as follows:

1. Log in as root.
2. Create a directory that will 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 product_version with a string that contains the product name and version.

3. For each DVD contained in the media kit execute the following commands:
 - a. Copy the entire content of the installation DVD into the installation server directory:

```
cp -a /media/path_to_your_DVD_drive .
```

Replace path_to_your_DVD_drive with the actual path under which your DVD drive is addressed. Depending on the type of drive used in your system, this can be cdrom, cdrecorder, dvd, or dvdrecorder.

- b. Rename the directory to the DVD number:

```
mv path_to_your_DVD_drive DVDx
```

Replace x with the actual number of your DVD.

On SUSE Linux Enterprise Desktop, you can export the repository 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 host names of the machines to which to export the installation data. Instead of specifying host names here, you could also use wild cards, ranges of network addresses, or 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 repository is automatically started and integrated into the boot process.

If you prefer manually exporting the repository 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:

```
systemctl enable nfsserver
```

4. Start the NFS server with **systemctl start nfsserver**. If you need to change the configuration of your NFS server later, modify the configuration file and restart the NFS daemon with **systemctl restart nfsserver**.

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

1. Log in as root.
2. Create the /etc/slp.reg.d/install.suse.nfs.reg configuration file with the following lines:

```
# Register the NFS Installation Server
service:install.suse:nfs://$HOSTNAME/path_to_repository/DVD1,en,65535
description=NFS Repository
```

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

3. Start the OpenSLP daemon with systemctl start slpd.

3.3 Setting Up an FTP Repository Manually

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

1. Create a directory holding the installation sources as described in *Section 3.2, "Setting Up an NFS Repository Manually"*.
2. Configure the FTP server to distribute the contents of your installation directory:

- a. Log in as root and install the package vsftpd using the YaST software management.

- b. Enter the FTP server root directory:

```
cd /srv/ftp
```

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

```
mkdir repository
```

Replace repository with the product name.

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

```
mount --bind path_to_repository /srv/ftp/repository
```

Replace *path_to_repository* and *repository* with values matching your setup. If you need to make this permanent, add it to */etc/fstab*.

- e. Start vsftpd with ***vsftpd***.

3. Announce the repository via OpenSLP, if this is supported by your network setup:

- a. Create the */etc/slp.reg.d/install.suse.ftp.reg* configuration file with the following lines:

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/repository/DVD1,en,65535
description=FTP Repository
```

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

- b. Start the OpenSLP daemon with ***systemctl start slpd***.

3.4 Setting Up an HTTP Repository Manually

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

1. Create a directory holding the installation sources as described in *Section 3.2, "Setting Up an NFS Repository Manually"*.
2. Configure the HTTP server to distribute the contents of your installation directory:
 - a. Install the Web server Apache.
 - b. Enter the root directory of the HTTP server (*/srv/www/htdocs*) and create the sub-directory that will hold the installation sources:

```
mkdir repository
```

Replace repository with the product name.

- c. 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_to_repository /srv/www/htdocs/repository
```

- d. 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
```

- e. Reload the HTTP server configuration using **systemctl reload apache2**.
3. Announce the repository via OpenSLP, if this is supported by your network setup:

- a. Create the /etc/slp.reg.d/install.suse.http.reg configuration file with the following lines:

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/repository/DVD1/,en,65535
description=HTTP Repository
```

Replace repository with the actual path to the repository on your server. The service: line should be entered as one continuous line.

- b. Start the OpenSLP daemon using **systemctl start slpd**.

3.5 Managing an SMB Repository

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 repository, proceed as follows:

1. Log in to your Windows machine.

2. Create a new directory that will hold the entire installation tree and name it INSTALL, for example.
3. Export this share according the procedure outlined in your Windows documentation.
4. Enter this share and create a subdirectory, called product. Replace product with the actual product name.
5. Enter the INSTALL/product directory and copy each DVD to a separate directory, such as DVD1 and DVD2.

To use an SMB mounted share as a repository, proceed as follows:

1. Boot the installation target.
2. Select *Installation*.
3. Press **F4** for a selection of the repository.
4. Choose SMB and enter the Windows machine's name or IP address, the share name (INSTALL/product/DVD1, in this example), user name, and password. The syntax looks like this:

```
smb://workdomain;user:password@server/INSTALL/DVD1
```

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

3.6 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 a repository. 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 3.2, “Setting Up an NFS Repository Manually”, Section 3.3, “Setting Up an FTP Repository Manually”, or Section 3.4, “Setting Up an HTTP Repository Manually”*.
4. Create subdirectories for each DVD.
5. To mount and unpack each ISO image to the final location, issue the following command:

```
mount -o loop path_to_isopath_to_repository/product/mediumx
```

Replace path_to_iso with the path to your local copy of the ISO image, path_to_repository 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 3.2, “Setting Up an NFS Repository Manually”, Section 3.3, “Setting Up an FTP Repository Manually”, or Section 3.4, “Setting Up an HTTP Repository Manually”*.

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_repository/productmedium auto loop
```

4 Preparing the Boot of the Target System

SUSE® Linux Enterprise Desktop can be installed in different ways. Apart from the usual media installation covered in *Chapter 2, Installation with YaST*, 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 checklists: 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: Terminology

In the following sections, the system to hold your new SUSE Linux Enterprise Desktop installation is called *target system* or *installation target*. The term *repository* (previously called “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.

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.

4.1 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.

4.1.1 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*) 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.

4.1.2 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 needs to 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 settings
    #
    # "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 **`systemctl restart dhcpd`**.

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 settings  
    #  
    # "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 host name of the installation target. To bind the host name 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.

4.2 Setting Up a TFTP Server

If using a SUSE based installation, you may use YaST to set up a TFTP Server. Alternatively, set it up manually. The TFTP server delivers the boot image to the target system after it boots and sends a request for it.

4.2.1 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.

4.2.2 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 4.3, "Using PXE Boot"](#).
4. Modify the configuration of `xinetd` located under `/etc/xinetd.d` to make sure that the TFTP server is started on boot:
 - a. If it does not exist, create a file called `tftp` under this directory with `touch tftp`. Then run `chmod 755 tftp`.
 - b. 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
}
```

- c. Save the file and restart xinetd with **`systemctl restart xinetd`**.

4.3 Using PXE Boot

Some technical background information and PXE's complete specifications are available in the Preboot Execution Environment (PXE) Specification (<http://www.pix.net/software/pxe-boot/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 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 `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_to_repository/DVD1

This entry defines the NFS server and the repository for the client installation. Replace ip_instserver with the actual IP address of your installation server. path_to_repository should be replaced with the actual path to the repository. HTTP, FTP, or SMB repositories are addressed in a similar manner, except for the protocol prefix, which should read http, ftp, or smb.



Important: Adding Boot Options

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 5.2, "Booting the Target System for Installation"](#).



Tip: Changing Kernel and initrd File Names

It is possible to use different file names 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 file names that are provided by TFTP for the PXE boot.

An example /srv/tftpboot/pxelinux.cfg/default file follows. Adjust the protocol prefix for the repository to match your network setup and specify your preferred method of connecting to the installer by adding the vnc and VNCPassword or the ssh and ssh.password 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_to_repository/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 hddisk
    localboot 0

implicit      0
display      message
prompt       1
timeout      100

```

7. Replace *ip_instserver* and *path_to_repository* 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/*.

4.4 PXELINUX Configuration Options

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

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.

APPEND -

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

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 exists or no DEFAULT entry is defined in the configuration file, the default is the Kernel name “linux” with no options.

IFAPPEND FLAG

Adds a specific option to the kernel command line depending on the FLAG value. The IFAPPEND option is available only on PXELINUX. FLAG expects a value, described in *Table 4.1, “Generated and Added Kernel Command Line Options from IFAPPEND”*:

TABLE 4.1: GENERATED AND ADDED KERNEL COMMAND LINE OPTIONS FROM IFAPPEND

| Argument | Generated Kernel Command Line / Description |
|----------|---|
| <u>1</u> | <div>ip=CLIENT_IP:BOOT_SERVER_IP:GW_IP:NETMASK</div> <p>The placeholders are replaced based on the input from the DHCP/BOOTP or PXE boot server.</p> <p>Note, this option is not a substitute for running a DHCP client in the booted system. Without regular renewals, the lease acquired by the PXE BIOS will expire, making the IP address available for reuse by the DHCP server.</p> |
| <u>2</u> | <div>BOOTIF=MAC_ADDRESS_OF_BOOT_INTERFACE</div> |

| Argument | Generated Kernel Command Line / Description |
|----------|---|
| | This option is useful if you want to avoid timeouts when the installation server probes one LAN interface after the other until it gets a reply from a DHCP server. Using this option allows an initrd program to determine from which interface the system has been booted. linuxrc reads this option and uses this network interface. |
| <u>4</u> | <div>SYSUUID=SYSTEM_UUID</div> <p>Adds UUIDs in lowercase hexadecimals, see /usr/share/doc/packages/syslinux/pxelinux.txt</p> |

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.

PXELINUX uses the following syntax:

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

Labels are mangled as if they were file names and they must be unique after mangling. For example, the two labels “v2.6.30” and “v2.6.31” would not be distinguishable under PXELINUX because both mangle to the same DOS file name.

The Kernel does not need to be a Linux Kernel; it can be a boot sector or a COMBOOT file.

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 |
|----------|-----------------------|
| <u>0</u> | Perform a normal boot |

| Argument | Description |
|----------|---|
| <u>4</u> | Perform a local boot with the Universal Network Driver Interface (UNDI) driver still resident in memory |
| <u>5</u> | 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 when 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 file names to **F11** and **F12**.

4.5 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 re-install itself every time you boot it.

4.6 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.

4.7 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.

4.8 Wake on LAN with YaST

1. Log in as root.

2. Start *YaST* > *Network Services* > *WOL*.
3. Click *Add* and enter the host name and MAC address of the target system.
4. To turn on this machine, select the appropriate entry and click *Wake up*.

III Remote Installation

5 Remote Installation 69

5 Remote Installation

SUSE® Linux Enterprise Desktop can be installed in different ways. Apart from the usual media installation covered in *Chapter 2, Installation with YaST*, 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 checklists: one listing the prerequisites for that method and the other illustrating the basic procedure. More detail is then provided for all the techniques used in these installation scenarios.



Note: Terminology

In the following sections, the system to hold your new SUSE Linux Enterprise Desktop installation is called *target system* or *installation target*. The term *repository* (previously called “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.

5.1 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 that scenario. If in need of detailed instructions for a particular step, follow the links provided for each one of them.

5.1.1 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 2, Installation with YaST*.

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

- A repository, either remote or local:
 - Remote repository: NFS, HTTP, FTP, TFTP, or SMB with working network connection.
 - Local repository, for example a DVD.
- Target system with working network connection.
- Controlling system with working network connection and VNC viewer software or Java-enabled browser (Firefox, Chromium, Internet Explorer, Opera, etc.).
- Physical boot medium (CD, DVD, or flash disk) for booting the target system.
- Valid static IP addresses already assigned to the repository 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 repository as described in *Chapter 3, Setting Up the Server Holding the Installation Sources*. Choose an NFS, HTTP, FTP, or TFTP network server. For an SMB repository, refer to *Section 3.5, “Managing an SMB Repository”*.
2. Boot the target system using DVD1 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 repository. This is described in detail in *Section 5.2, “Booting the Target System for Installation”*.

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 **slptool** as described in *Procedure 5.1, “Locating VNC installations via OpenSLP”*.
4. On the controlling workstation, open a VNC viewing application or Web browser and connect to the target system as described in *Section 5.3.1, “VNC Installation”*.
5. Perform the installation as described in *Chapter 2, Installation with YaST*. Reconnect to the target system after it reboots for the final part of the installation.

5.1.2 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 repository: 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, Chromium, Internet Explorer, or Opera).
- Boot the target system using DVD1 of the SUSE Linux Enterprise Desktop media kit.
- Running DHCP server providing IP addresses.

To perform this kind of installation, proceed as follows:

1. Set up the repository as described in *Chapter 3, Setting Up the Server Holding the Installation Sources*. Choose an NFS, HTTP, or FTP network server. For an SMB repository, refer to *Section 3.5, “Managing an SMB Repository”*.
2. Boot the target system using DVD1 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 repository. This is described in detail in *Section 5.2, “Booting the Target System for Installation”*.

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 `slptool` as described in *Procedure 5.1, “Locating VNC installations via OpenSLP”*.

4. On the controlling workstation, open a VNC viewing application or Web browser and connect to the target system as described in *Section 5.3.1, “VNC Installation”*.
5. Perform the installation as described in *Chapter 2, Installation with YaST*. Reconnect to the target system after it reboots for the final part of the installation.
6. Finish the installation.

5.1.3 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 repository: 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, Chromium, Internet Explorer, or Opera).

To perform this type of installation, proceed as follows:

1. Set up the repository as described in *Chapter 3, Setting Up the Server Holding the Installation Sources*. Choose an NFS, HTTP, or FTP network server or configure an SMB repository as described in *Section 3.5, “Managing an SMB Repository”*.
2. Set up a TFTP server to hold a boot image that can be pulled by the target system. This is described in *Section 4.2, “Setting Up a TFTP Server”*.
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 4.1, “Setting Up a DHCP Server”*.

4. Prepare the target system for PXE boot. This is described in further detail in [Section 4.5, “Preparing the Target System for PXE Boot”](#).
5. Initiate the boot process of the target system using Wake on LAN. This is described in [Section 4.7, “Wake on LAN”](#).
6. On the controlling workstation, open a VNC viewing application or Web browser and connect to the target system as described in [Section 5.3.1, “VNC Installation”](#).
7. Perform the installation as described in [Chapter 2, Installation with YaST](#). Reconnect to the target system after it reboots for the final part of the installation.
8. Finish the installation.

5.1.4 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 2, Installation with YaST](#).

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

- Remote repository: 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.
- Boot the target system using DVD1 of the SUSE Linux Enterprise Desktop media kit.
- Valid static IP addresses already assigned to the repository 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 repository as described in [Chapter 3, Setting Up the Server Holding the Installation Sources](#). Choose an NFS, HTTP, or FTP network server. For an SMB repository, refer to [Section 3.5, “Managing an SMB Repository”](#).
2. Boot the target system using DVD1 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 repository, and SSH enablement. This is described in detail in [Section 5.2.2, “Using Custom Boot Options”](#). 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 5.3.2.2, “Connecting to the Installation Program”](#).
5. Perform the installation as described in [Chapter 2, Installation with YaST](#). Reconnect to the target system after it reboots for the final part of the installation.
6. Finish the installation.

5.1.5 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 SSH to connect to the installer, but still requires user interaction for the actual configuration efforts.



Note: Avoid Lost Connections After the Second Step (Installation)

In the network settings dialog, check the *Traditional Method with ifup* and avoid NetworkManager. If not, your SSH connection will be lost during installation. Reset the settings to *User Controlled with NetworkManager* after your installation has finished.

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

- A repository, either remote or local:
 - Remote repository: NFS, HTTP, FTP, TFTP, or SMB with working network connection.
 - Local repository, for example a DVD.
- Target system with working network connection.

- Controlling system with working network connection and working SSH client software.
- Physical boot medium (CD, DVD, or flash 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 repository source as described in *Chapter 3, Setting Up the Server Holding the Installation Sources*. Choose an NFS, HTTP, or FTP network server. For an SMB repository, refer to *Section 3.5, “Managing an SMB Repository”*.
2. Boot the target system using DVD1 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 5.2.2, “Using Custom Boot Options”* 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 5.3.2.2, “Connecting to the Installation Program”*.
5. Perform the installation as described in *Chapter 2, Installation with YaST*. Reconnect to the target system after it reboots for the final part of the installation.
6. Finish the installation.

5.1.6 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 repository: 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 repository as described in *Chapter 3, Setting Up the Server Holding the Installation Sources*. Choose an NFS, HTTP, or FTP network server. For the configuration of an SMB repository, refer to *Section 3.5, "Managing an SMB Repository"*.
2. Set up a TFTP server to hold a boot image that can be pulled by the target system. This is described in *Section 4.2, "Setting Up a TFTP Server"*.
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 4.1, "Setting Up a DHCP Server"*.
4. Prepare the target system for PXE boot. This is described in further detail in *Section 4.5, "Preparing the Target System for PXE Boot"*.
5. Initiate the boot process of the target system using Wake on LAN. This is described in *Section 4.7, "Wake on LAN"*.
6. On the controlling workstation, start an SSH client and connect to the target system as described in *Section 5.3.2, "SSH Installation"*.
7. Perform the installation as described in *Chapter 2, Installation with YaST*. Reconnect to the target system after it reboots for the final part of the installation.
8. Finish the installation.

5.2 Booting the Target System for Installation

There are two different ways to customize the boot process for installation apart from those mentioned under *Section 4.7, "Wake on LAN"* and *Section 4.3, "Using PXE Boot"*. 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.

5.2.1 Using the Default Boot Options

The boot options are described in detail in *Chapter 2, Installation with YaST*. Generally, 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 *Book “Administration Guide”, Chapter 32 “Common Problems and Their Solutions”, Section 32.2 “Installation Problems”*.

The menu bar at the bottom of the 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 5.2.2, “Using Custom Boot Options”*). A detailed description of the available function keys is available in *Section 2.2.1.1, “The Boot Screen on Machines Equipped with Traditional BIOS”*.

5.2.2 Using Custom Boot Options

Using the appropriate set of boot options helps simplify 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. 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=xxx netdevice=xxx hostip=xxx netmask=xxx vnc=xxx VNCPassword=xxx
```

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

Chapter 2, Installation with YaST

Parameters Needed for Booting. None

Boot Options. None needed

Section 5.1.1, “Simple Remote Installation via VNC—Static Network Configuration”

PARAMETERS NEEDED FOR BOOTING

- Location of the installation server
- Network device

- IP address
- Netmask
- Gateway
- VNC enablement
- VNC password

BOOT OPTIONS

- install=(nfs,http,ftp,smb)://path_to_instmedia
- netdevice=some_netdevice (only needed if several network devices are available)
- hostip=some_ip
- netmask=some_netmask
- gateway=ip_gateway
- vnc=1
- VNCPassword=some_password

Section 5.1.2, “Simple Remote Installation via VNC—Dynamic Network Configuration”

PARAMETERS NEEDED FOR BOOTING

- Location of the installation server
- VNC enablement
- VNC password

BOOT OPTIONS

- install=(nfs,http,ftp,smb)://path_to_instmedia
- vnc=1
- VNCPassword=some_password

Section 5.1.3, “Remote Installation via VNC—PXE Boot and Wake on LAN”

PARAMETERS NEEDED FOR BOOTING

- Location of the installation server
- Location of the TFTP server
- VNC enablement
- VNC password

Boot Options. Not applicable; process managed through PXE and DHCP

Section 5.1.4, “Simple Remote Installation via SSH—Static Network Configuration”

PARAMETERS NEEDED FOR BOOTING

- Location of the installation server
- Network device
- IP address
- Netmask
- Gateway
- SSH enablement
- SSH password

BOOT OPTIONS

- install=(nfs,http,ftp,smb)://path_to_instmedia
- netdevice=some_netdevice (only needed if several network devices are available)
- hostip=some_ip
- netmask=some_netmask
- gateway=ip_gateway
- ssh=1
- ssh.password=some_password

Section 5.1.5, “Simple Remote Installation via SSH—Dynamic Network Configuration”

PARAMETERS NEEDED FOR BOOTING

- Location of the installation server
- SSH enablement
- SSH password

BOOT OPTIONS

- install=(nfs,http,ftp,smb)://path_to_instmedia
- ssh=1
- ssh.password=some_password

Section 5.1.6, “Remote Installation via SSH—PXE Boot and Wake on LAN”

- Location of the installation server
- Location of the TFTP server
- SSH enablement
- SSH password

Boot Options. Not applicable; process managed through PXE and DHCP



Tip: More Information about linuxrc Boot Options

Find more information about the linuxrc boot options used for booting a Linux system at <http://en.opensuse.org/SDB:Linuxrc>.

5.2.2.1 Installing Add-On Products and Driver Updates

SUSE Linux Enterprise Desktop supports the installation of add-on products providing extensions (for example the SUSE Linux Enterprise High Availability Extension), third-party products and drivers or additional software. To automatically install an add-on product when deploying SUSE Linux Enterprise Desktop remotely, specify the `addon=REPOSITORY` parameter.

`REPOSITORY` needs to be a hosted repository that can be read by YaST (YaST2 or YUM (rpm-md)). ISO images are currently not supported.



Tip: Driver Updates

Driver Updates can be found at <http://drivers.suse.com/>. Not all driver updates are provided as repositories—some are only available as ISO images and therefore cannot be installed with the `addon` parameter. Instructions on how to install driver updates via ISO image are available at http://drivers.suse.com/doc/SolidDriver/Driver_Kits.html.

5.3 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.

5.3.1 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.

5.3.1.1 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 5.2.2, “Using Custom Boot Options”*). 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:


PROCEDURE 5.1: LOCATING VNC INSTALLATIONS VIA OPENSLLP

1. Run `slptool findsrvtypes | grep vnc` to get a list of all services offering VNC. The VNC installation targets should be available under a service named `YaST.installation.suse`.
2. Run `slptool findsrvs YaST.installation.suse` to get a list of installations available. Use the IP address and the port (usually `5901`) provided with your VNC viewer.

5.3.1.2 Connecting to the Installation Program

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 macOS.

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, Chromium, 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.

5.3.2 SSH Installation

Using SSH, you can remotely control the installation of your Linux machine using any SSH client software.

5.3.2.1 Preparing for SSH Installation

Apart from installing the appropriate software package (OpenSSH for Linux and PuTTY for Windows), you need to pass the appropriate boot options to enable SSH for installation. See [Section 5.2.2, “Using Custom Boot Options”](#) for details. OpenSSH is installed by default on any SUSE Linux-based operating system.

5.3.2.2 Connecting to the Installation Program

1. Retrieve the installation target's IP address. If you have physical access to the target machine, take the IP address the installation routine provides in 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. In 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 user name, 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 2, Installation with YaST*.

IV Initial System Configuration

- 6 Setting Up Hardware Components with YaST **85**
- 7 Advanced Disk Setup **98**
- 8 Installing or Removing Software **117**
- 9 Installing Modules, Extensions, and Third Party Add-On Products **134**
- 10 Installing Multiple Kernel Versions **140**
- 11 Managing Users with YaST **145**
- 12 Changing Language and Country Settings with YaST **160**

6 Setting Up Hardware Components with YaST

YaST allows you to configure hardware items such as audio hardware, your system keyboard layout or printers.



Note: Graphics Card, Monitor, Mouse and Keyboard Settings

Graphics card, monitor, mouse and keyboard can be configured with GNOME tools. See *Book “GNOME User Guide”, Chapter 3 “Customizing Your Settings”, Section 3.3 “Hardware”* for details.

6.1 Setting Up Your System Keyboard Layout

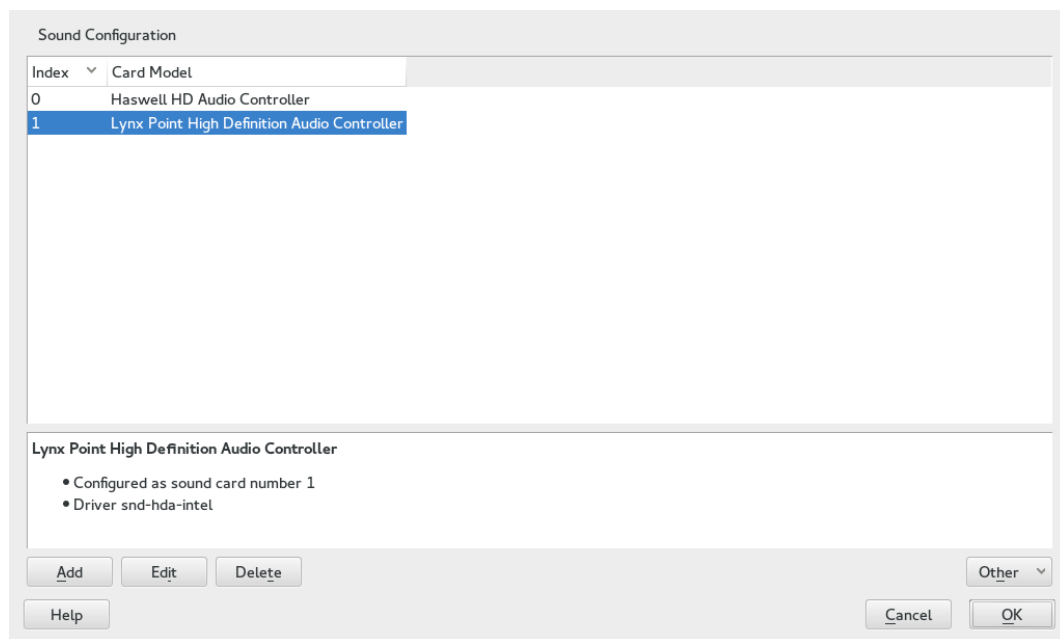
The YaST *System Keyboard Layout* module lets you define the default keyboard layout for the system (also used for the console). Users can modify the keyboard layout in their individual X sessions, using the desktop's tools.

1. Start the YaST *System Keyboard Configuration* dialog by clicking *Hardware > System Keyboard Layout* in YaST. Alternatively, start the module from the command line with **sudo yast2 keyboard**.
2. Select the desired *Keyboard Layout* from the list.
3. Optionally, you can also define the keyboard repeat rate or keyboard delay rate in the *Expert Settings*.
4. Try the selected settings in the *Test* text box.
5. If the result is as expected, confirm your changes and close the dialog. The settings are written to /etc/sysconfig/keyboard.

6.2 Setting Up Sound Cards

YaST detects most sound cards automatically and configures them with the appropriate values. If you want to change the default settings, or need to set up a sound card that could not be configured automatically, use the YaST sound module. There, you can also set up additional sound cards or switch their order.

To start the sound module, start YaST and click *Hardware* > *Sound*. Alternatively, start the *Sound Configuration* dialog directly by running **yast2 sound &** as user root from a command line.



The dialog shows all sound cards that were detected.

PROCEDURE 6.1: CONFIGURING SOUND CARDS

If you have added a new sound card or YaST could not automatically configure an existing sound card, follow the steps below. For configuring a new sound card, you need to know your sound card vendor and model. If in doubt, refer to your sound card documentation for the required information. For a reference list of sound cards supported by ALSA with their corresponding sound modules, see <http://www.alsa-project.org/main/index.php/Matrix:Main>.

During configuration, you can choose between the following setup options:

Quick Automatic Setup

You are not required to go through any of the further configuration steps—the sound card is configured automatically. You can set the volume or any options you want to change later.

Normal Setup

Allows you to adjust the output volume and play a test sound during the configuration.

Advanced setup with possibility to change options

For experts only. Allows you to customize all parameters of the sound card.



Important: Advanced Configuration

Only use this option if you know exactly what you are doing. Otherwise leave the parameters untouched and use the normal or the automatic setup options.

1. Start the YaST sound module.
2. To configure a detected, but *Not Configured* sound card, select the respective entry from the list and click *Edit*.
To configure a new sound card, click *Add*. Select your sound card vendor and model and click *Next*.
3. Choose one of the setup options and click *Next*.
4. If you have chosen *Normal Setup*, you can now *Test* your sound configuration and make adjustments to the volume. You should start at about ten percent volume to avoid damage to your hearing or the speakers.
5. If all options are set according to your wishes, click *Next*.
The *Sound Configuration* dialog shows the newly configured or modified sound card.
6. To remove a sound card configuration that you no longer need, select the respective entry and click *Delete*.
7. Click *OK* to save the changes and leave the YaST sound module.

1. To change the configuration of an individual sound card (for experts only!), select the sound card entry in the *Sound Configuration* dialog and click *Edit*.
This takes you to the *Sound Card Advanced Options* where you can fine-tune several parameters. For more information, click *Help*.
2. To adjust the volume of an already configured sound card or to test the sound card, select the sound card entry in the *Sound Configuration* dialog and click *Other*. Select the respective menu item.



Note: YaST Mixer

The YaST mixer settings provide only basic options. They are intended for troubleshooting (for example, if the test sound is not audible). Access the YaST mixer settings from *Other > Volume*. For everyday use and fine-tuning of sound options, use the mixer applet provided by your desktop or the **alsasound** command line tool.

3. For playback of MIDI files, select *Other > Start Sequencer*.
4. When a supported sound card is detected (like a Creative Soundblaster Live, Audigy or AWE sound card), you can also install SoundFonts for playback of MIDI files:
 - a. Insert the original driver CD-ROM into your CD or DVD drive.
 - b. Select *Other > Install SoundFonts* to copy SF2 SoundFonts™ to your hard disk. The SoundFonts are saved in the directory /usr/share/sfbank/creative/.
5. If you have configured more than one sound card in your system you can adjust the order of your sound cards. To set a sound card as primary device, select the sound card in the *Sound Configuration* and click *Other > Set as the Primary Card*. The sound device with index 0 is the default device and thus used by the system and the applications.
6. By default, SUSE Linux Enterprise Desktop uses the PulseAudio sound system. It is an abstraction layer that helps to mix multiple audio streams, bypassing any restrictions the hardware may have. To enable or disable the PulseAudio sound system, click *Other > PulseAudio Configuration*. If enabled, PulseAudio daemon is used to play sounds. Disable *PulseAudio Support* to use something else system-wide.

The volume and configuration of all sound cards are saved when you click *OK* and leave the YaST sound module. The mixer settings are saved to the file `/etc/asound.state`. The ALSA configuration data is appended to the end of the file `/etc/modprobe.d/sound` and written to `/etc/sysconfig/sound`.

6.3 Setting Up a Printer

YaST can be used to configure a local printer that is directly connected to your machine via USB and to set up printing with network printers. It is also possible to share printers over the network. Further information about printing (general information, technical details, and troubleshooting) is available in *Book “Administration Guide”, Chapter 17 “Printer Operation”*.

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 that are 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* and configure printers.



Note: Starting CUPS

To be able to print from your system, CUPS must run. In case it is not running, you are asked to start it. Answer with *Yes*, or you cannot configure printing. In case CUPS is not started at boot time, you will also be asked to enable this feature. It is recommended to say *Yes*, otherwise CUPS would need to be started manually after each reboot.

6.3.1 Configuring Printers

Usually a USB printer is automatically detected. There are two possible reasons it is not automatically detected:

- The USB printer is switched off.
- The 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-related problem.

Configuring a printer is a three-step process: specify the connection type, choose a driver, and name the print queue for this setup.

For many printer models, several drivers are available. When configuring the printer, YaST defaults to those marked recommended as a general rule. Normally it is not necessary to change the driver. 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, 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 6.3.1.1, "Adding Drivers with YaST"](#) for another possible solution.

A printer is never used directly, but always through a print queue. This ensures that simultaneous jobs can be queued and processed one after the other. Each print 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 and white only, for example. Refer to *Book "Administration Guide", Chapter 17 "Printer Operation", Section 17.1 "The CUPS Workflow"* for more information about print queues.

PROCEDURE 6.3: ADDING A NEW PRINTER

1. Start the YaST printer module with *Hardware > Printer*.
2. In the *Printer Configurations* screen click *Add*.
3. If your printer is already listed under Specify the Connection, proceed with the next step. Otherwise, try to *Detect More* or start the *Connection Wizard*.
4. In the text box under Find and Assign a Driver enter the vendor name and the model name and click *Search for*.
5. Choose a driver that matches your printer. It is recommended to choose the driver listed first. If no suitable driver is displayed:
 - a. Check your search term
 - b. Broaden your search by clicking *Find More*
 - c. Add a driver as described in [Section 6.3.1.1, "Adding Drivers with YaST"](#)
6. Specify the Default paper size.
7. In the *Set Arbitrary Name* field, enter a unique name for the print queue.

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

6.3.1.1 Adding Drivers with YaST

Not all printer drivers available for SUSE Linux Enterprise Desktop are installed by default. If no suitable driver is available in the *Find and Assign a Driver* dialog when adding a new printer install a driver package containing drivers for your printers:

PROCEDURE 6.4: INSTALLING ADDITIONAL DRIVER PACKAGES

1. Start the YaST printer module with *Hardware > Printer*.
2. In the *Printer Configurations* screen, click *Add*.
3. In the Find and Assign a Driver section, click *Driver Packages*.
4. Choose one or more suitable driver packages from the list. Do *not* specify the path to a printer description file.
5. Choose *OK* and confirm the package installation.
6. To directly use these drivers, proceed as described in *Procedure 6.3, "Adding a New Printer"*.

PostScript printers do not need printer driver software. PostScript printers need only a PostScript Printer Description (PPD) file which matches the particular model. PPD files are provided by the printer manufacturer.

If no suitable PPD file is available in the *Find and Assign a Driver* dialog when adding a PostScript printer install a PPD file for your printer:

Several sources for PPD files are available. It is recommended to first try additional driver packages that are shipped with SUSE Linux Enterprise Desktop but not installed by default (see below for installation instructions). If these packages do not contain suitable drivers for your printer, get PPD files directly from your printer vendor or from the driver CD of a PostScript printer. For details, see *Book "Administration Guide", Chapter 17 "Printer Operation", Section 17.8.2 "No Suitable PPD File Available for a PostScript Printer"*. Alternatively, find PPD files at <http://www.linuxfoundation.org/collaborate/workgroups/openprinting/database/databaseintro>, the "OpenPrinting.org printer database". When downloading PPD files from OpenPrinting, keep in mind that it always shows the latest Linux support status, which is not necessarily met by SUSE Linux Enterprise Desktop.

PROCEDURE 6.5: ADDING A PPD FILE FOR POSTSCRIPT PRINTERS

1. Start the YaST printer module with *Hardware > Printer*.
2. In the *Printer Configurations* screen, click *Add*.
3. In the Find and Assign a Driver section, click *Driver Packages*.
4. Enter the full path to the PPD file into the text box under Make a Printer Description File Available.
5. Click *OK* to return to the Add New Printer Configuration screen.
6. To directly use this PPD file, proceed as described in *Procedure 6.3, "Adding a New Printer"*.

6.3.1.2 Editing a Local Printer Configuration

By editing an existing configuration for a printer you can change basic settings such as connection type and driver. It is also possible to adjust the default settings for paper size, resolution, media source, etc. You can change identifiers of the printer by altering the printer description or location.

1. Start the YaST printer module with *Hardware > Printer*.
2. In the *Printer Configurations* screen, choose a local printer configuration from the list and click *Edit*.
3. Change the connection type or the driver as described in *Procedure 6.3, "Adding a New Printer"*. This should only be necessary in case you have problems with the current configuration.
4. Optionally, make this printer the default by checking *Default Printer*.
5. Adjust the default settings by clicking *All Options for the Current Driver*. To change a setting, expand the list of options by clicking the relative + sign. Change the default by clicking an option. Apply your changes with *OK*.

6.3.2 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.

6.3.2.1 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. Printing via more than one CUPS server requires a running local CUPS daemon that communicates with the remote CUPS servers.



Important: Browsing Network Print Queues

CUPS servers announce their print queues over the network either via the traditional CUPS browsing protocol or via Bonjour/DND-SD. Clients need to be able to browse these lists, so users can select specific printers to send their print jobs to. To be able to browse network print queues, the service `cups-browsed` provided by the package `cups-filters-cups-browsed` needs to run on all clients that print via CUPS servers. `cups-browsed` is started automatically when configuring network printing with YaST.

In case browsing does not work after having started `cups-browsed`, the CUPS server(s) probably announce the network print queues via Bonjour/DND-SD. In this case you need to additionally install the package `avahi` and start the associated service with **`sudo systemctl start avahi-daemon`** on all clients.

PROCEDURE 6.6: PRINTING VIA A SINGLE CUPS SERVER

1. Start the YaST printer module with *Hardware > Printer*.
2. From the left pane, launch the *Print via Network* screen.
3. Check *Do All Your Printing Directly via One Single CUPS Server* and specify the name or IP address of the server.
4. Click *Test Server* to make sure you have chosen the correct name or IP address.

5. Click OK to return to the *Printer Configurations* screen. All printers available via the CUPS server are now listed.

PROCEDURE 6.7: PRINTING VIA MULTIPLE CUPS SERVERS

1. Start the YaST printer module with *Hardware > Printer*.
2. From the left pane, launch the *Print via Network* screen.
3. Check *Accept Printer Announcements from CUPS Servers*.
4. Under General Settings specify which servers to use. You may accept connections from all networks available or from specific hosts. If you choose the latter option, you need to specify the host names or IP addresses.
5. Confirm by clicking *OK* and then *Yes* when asked to start a local CUPS server. After the server has started YaST will return to the *Printer Configurations* screen. Click *Refresh list* to see the printers detected by now. Click this button again, in case more printer are to be available.

6.3.2.2 Using Print Servers other than CUPS


If your network offers print services via print servers other than CUPS, start the YaST printer module with *Hardware > Printer* and launch the *Print via Network* screen from the left pane. Start the *Connection Wizard* and choose the appropriate *Connection Type*. Ask your network administrator for details on configuring a network printer in your environment.

6.3.3 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 print queues are made available on the network for listening to remote CUPS daemons. It is also possible to set up a dedicated CUPS server that manages all print queues and can directly be accessed by remote clients. In this case it is not necessary to enable browsing.

PROCEDURE 6.8: SHARING PRINTERS

1. Start the YaST printer module with *Hardware > Printer*.

2. Launch the *Share Printers* screen from the left pane.
3. Select *Allow Remote Access*. Also check *For computers within the local network* and enable browsing mode by also checking *Publish printers by default within the local network*.
4. Click *OK* to restart the CUPS server and to return to the *Printer Configurations* screen.
5. Regarding CUPS and firewall settings, see http://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings .

6.4 Setting Up a Scanner

You can configure a USB or SCSI scanner with YaST. The `sane-backends` package contains hardware drivers and other essentials needed to use a scanner. If you own an HP All-In-One device, see [Section 6.4.1, “Configuring an HP All-In-One Device”](#), instructions on how to configure a network scanner are available at [Section 6.4.3, “Scanning over the Network”](#).

PROCEDURE 6.9: CONFIGURING A USB OR SCSI SCANNER

1. Connect your USB or SCSI scanner to your computer and turn it on.
2. Start YaST and select *Hardware > Scanner*. YaST builds the scanner database and tries to detect your scanner model automatically.
If a USB or SCSI scanner is not properly detected, try *Other > Restart Detection*.
3. To activate the scanner select it from the list of detected scanners and click *Edit*.
4. Choose your model form the list and click *Next* and *Finish*.
5. Use *Other > Test* to make sure you have chosen the correct driver.
6. Leave the configuration screen with *OK*.

6.4.1 Configuring an HP All-In-One Device

An HP All-In-One device can be configured with YaST even if it is made available via the network. If you own a USB HP All-In-One device, start configuring as described in [Procedure 6.9, “Configuring a USB or SCSI Scanner”](#). 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 network, run the HP Device Manager:

1. Start YaST and select *Hardware > Scanner*. YaST loads the scanner database.
2. Start the HP Device Manager with *Other > Run hp-setup* and follow the on-screen instructions. After having finished the HP Device Manager, the YaST scanner module automatically restarts the auto detection.
3. Test it by choosing *Other > Test*.
4. Leave the configuration screen with *OK*.

6.4.2 Sharing a Scanner over the Network

SUSE Linux Enterprise Desktop allows the sharing of a scanner over the network. To do so, configure your scanner as follows:

1. Configure the scanner as described in [Section 6.4, "Setting Up a Scanner"](#).
2. Choose *Other > Scanning via Network*.
3. Enter the host names 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*.

6.4.3 Scanning over the Network

To use a scanner that is shared over the network, proceed as follows:

1. Start YaST and select *Hardware > Scanner*.
2. Open the network scanner configuration menu by *Other > Scanning via Network*.
3. Enter the host name of the machine the scanner is connected to under *Client Settings > Servers Used for the net Metadriver*

4. Leave with *OK*. The network scanner is now listed in the Scanner Configuration window and is ready to use.

7 Advanced Disk Setup

Sophisticated system configurations require specific 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. SUSE Linux Enterprise Desktop also supports multipath I/O , and there is also the option to use iSCSI as a networked disk.

7.1 Using the YaST Partitioner

With the expert partitioner, shown in *Figure 7.1, “The YaST Partitioner”*, manually modify the partitioning of one or several hard disks. You can add, delete, resize, and edit partitions, or access the soft RAID, and LVM configuration.



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.

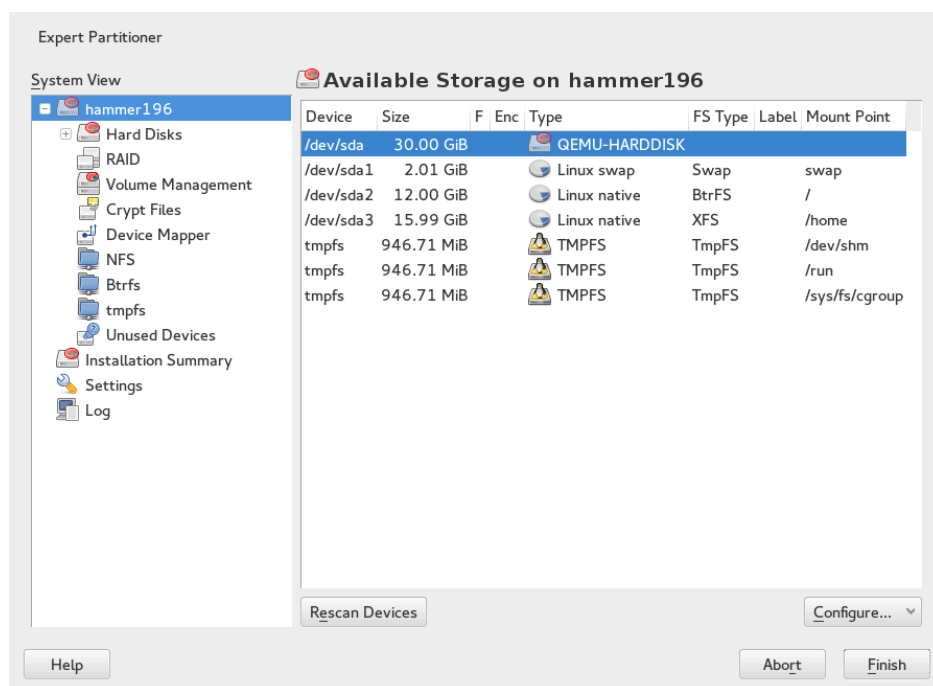


FIGURE 7.1: THE YAST PARTITIONER

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, encryption status, 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 left hand *System View*. Use these views to gather information about existing storage configurations, or to configure functions like RAID, Volume Management, Crypt Files, or view file systems with additional features, such as Btrfs, NFS, or TMPFS.

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).

7.1.1 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 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 divided 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 occupy the entire remaining free cylinder range. Then create multiple logical partitions within the extended partition. The maximum number of logical partitions is 63, independent of the disk type. It does not matter which types of partitions are used for Linux. Primary and logical partitions both function normally.

7.1.2 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* and 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 7.1.1, "Partition Types"](#)).
2. Specify the size of the new partition. You can either choose to occupy all the free unpartitioned space, or enter a custom size.
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*. For more information on supported file systems, see [root](#).
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 7.1.3, "Editing a Partition"](#).

5. Click *Finish* 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.

7.1.2.1 Btrfs Partitioning

The default file system for the root partition is Btrfs (see *Book “Administration Guide”, Chapter 6 “System Recovery and Snapshot Management with Snapper”* for more information on Btrfs). The root file system is the default subvolume and it is not listed in the list of created subvolumes. As a default Btrfs subvolume, it can be mounted as a normal file system.

Important: Btrfs on an Encrypted Root Partition

The default partitioning setup suggests the root partition as Btrfs with /boot being a directory. If you need to have the root partition encrypted in this setup, make sure to use the GPT partition table type instead of the default MSDOS type. Otherwise the GRUB2 boot loader may not have enough space for the second stage loader.

It is possible to create snapshots of Btrfs subvolumes—either manually, or automatically based on system events. For example when making changes to the file system, **zypper** invokes the **snapper** command to create snapshots before and after the change. This is useful if you are not satisfied with the change **zypper** made and want to restore the previous state. As **snapper** invoked by **zypper** snapshots the *root* file system by default, it is reasonable to exclude specific directories from being snapshot, depending on the nature of data they hold. And that is why YaST suggests creating the following separate subvolumes.

/boot/grub2/i386-pc, /boot/grub2/x86_64-efi, /boot/grub2/powerpc-ieee1275, /boot/grub2/s390x-emu

A rollback of the boot loader configuration is not supported. The directories listed above are architecture-specific. The first two directories are present on AMD64/Intel 64 machines, the latter two on IBM POWER and on IBM z Systems, respectively.

/home

If /home does not reside on a separate partition, it is excluded to avoid data loss on rollbacks.

/opt, /var/opt

Third-party products usually get installed to /opt. It is excluded to avoid uninstalling these applications on rollbacks.

/srv

Contains data for Web and FTP servers. It is excluded to avoid data loss on rollbacks.

/tmp, /var/tmp, /var/cache, /var/crash

All directories containing temporary files and caches are excluded from snapshots.

/usr/local

This directory is used when manually installing software. It is excluded to avoid uninstalling these installations on rollbacks.

/var/lib/libvirt/images

The default location for virtual machine images managed with libvirt. Excluded to ensure virtual machine images are not replaced with older versions during a rollback. By default, this subvolume is created with the option no copy on write.

/var/lib/mailman, /var/spool

Directories containing mails or mail queues are excluded to avoid a loss of mails after a rollback.

/var/lib/named

Contains zone data for the DNS server. Excluded from snapshots to ensure a name server can operate after a rollback.

/var/lib/mariadb, /var/lib/mysql, /var/lib/pgsql

These directories contain database data. By default, these subvolumes are created with the option no copy on write.

/var/log

Log file location. Excluded from snapshots to allow log file analysis after the rollback of a broken system.



Tip: Size of Btrfs Partition

Because saved snapshots require more disk space, it is recommended to reserve more space for Btrfs partition than for a partition not capable of snapshotting (such as Ext3). Recommended size for a root Btrfs partition with suggested subvolumes is 20GB.

7.1.2.1.1 Managing Btrfs Subvolumes using YaST

Subvolumes of a Btrfs partition can be now managed with the YaST *Expert partitioner* module. You can add new or remove existing subvolumes.

PROCEDURE 7.1: BTRFS SUBVOLUMES WITH YAST

1. Start the YaST *Expert Partitioner* with *System > Partitioner*.
2. Choose *Btrfs* in the left *System View* pane.
3. Select the Btrfs partition whose subvolumes you need to manage and click *Edit*.
4. Click *Subvolume Handling*. You can see a list of all existing subvolumes of the selected Btrfs partition. You can notice several @/.snapshots/xyz/snapshot entries—each of these subvolumes belongs to one existing snapshot.
5. Depending on whether you want to add or remove subvolumes, do the following:
 - a. To remove a subvolume, select it from the list of *Existing Subvolumes* and click *Remove*.
 - b. To add a new subvolume, enter its name to the *New Subvolume* text box and click *Add new*.

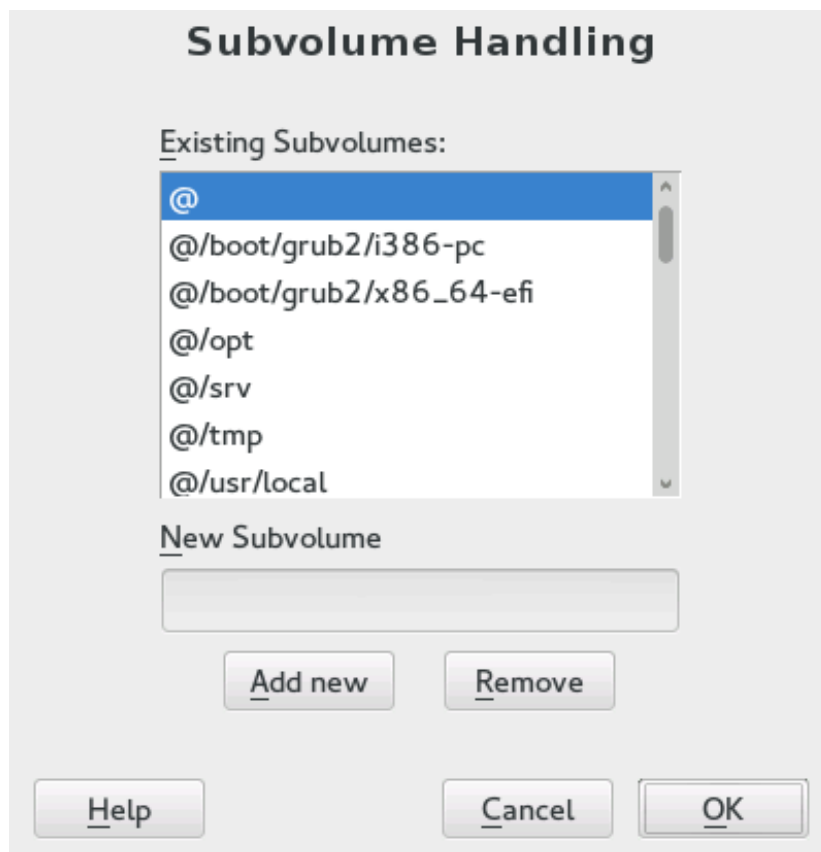


FIGURE 7.2: BTRFS SUBVOLUMES IN YAST PARTITIONER

6. Confirm with *OK* and *Finish*.
7. Leave the partitioner with *Finish*.

7.1.3 Editing a Partition

When you create a new partition or modify an existing partition, you can set various parameters. For new partitions, the default parameters set by YaST are usually sufficient and 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. Typical values are *Linux*, *Linux swap*, *Linux LVM*, and *Linux RAID*.

File System

To change the partition file system, click *Format Partition* and select file system type in the *File System* list.

SUSE Linux Enterprise Desktop supports several types of file systems. Btrfs is the Linux file system of choice for the root partition because of its advanced features. It supports copy-on-write functionality, creating snapshots, multi-device spanning, subvolumes, and other useful techniques. XFS, Ext3 and JFS are journaling file systems. These file systems can restore the system very quickly after a system crash, using write processes logged during the operation. Ext2 is not a journaling file system, but it is adequate for smaller partitions because it does not require much disk space for management.

The default file system for the root partition is Btrfs. The default file system for additional partitions is XFS.

Swap is a special format that allows the partition to be used as a virtual memory. Create a swap partition of at least 256 MB. However, if you use up your swap space, consider adding more memory to your system instead of adding more swap space.



Warning: Changing the File System

Changing the file system and reformatting partitions irreversibly deletes all data from the partition.

For details on the various file systems, refer to *Storage Administration Guide*.

Encrypt Device

If you activate the encryption, all data is written to the hard disk in encrypted form. This increases the security of sensitive data, but reduces the system speed, as the encryption takes some time to process. More information about the encryption of file systems is provided in *Book “Security Guide”, Chapter 11 “Encrypting Partitions and Files”*.

Mount Point

Specify the directory where the partition should be mounted in the file system tree. Select from YaST suggestions or enter any other name.

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 device names, use the mount option *Device ID*, *UUID* or *LABEL*. In SUSE Linux Enterprise Desktop, persistent device names are enabled by default.

If you prefer to mount the partition by its label, you need to define one in the *Volume label* text entry. For example, you could use the partition label `HOME` for a partition intended to mount to `/home`.

If you intend to use quotas 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 11.3.4, "Managing Quotas"](#).

3. Select *Finish* to save the changes.



Note: Resize File Systems

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 relevant partition before running the partitioner.

7.1.4 Expert Options

After you select a hard disk device (like *sda*) in the *System View* pane, you can access the *Expert* menu in the lower right part of the *Expert Partitioner* window. The menu contains the following commands:

Create New Partition Table

This option helps you create a new partition table on the selected device.



Warning: Creating a New Partition Table

Creating a new partition table on a device irreversibly removes all the partitions and their data from that device.

Clone This Disk

This option helps you clone the device partition layout (but not the data) to other available disk devices.

7.1.5 Advanced Options

After you select the host name of the computer (the top-level of the tree in the *System View* pane), you can access the *Configure* menu in the lower right part of the *Expert Partitioner* window. The menu contains the following commands:

Configure iSCSI

To access SCSI over IP block devices, you first need to configure iSCSI. This results in additionally available devices in the main partition list.

Configure Multipath

Selecting this option helps you configure the multipath enhancement to the supported mass storage devices.

7.1.6 More Partitioning Tips

The following section includes a few hints and tips on partitioning that should help you make the right decisions when 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.

7.1.6.1 Using swap

Swap is used to extend the available physical memory. It is then 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. Then, if you did not have twice the size of your RAM in swap, the performance of the system suffered. 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, running applications have more memory available and caching works more smoothly.

If an application tries to allocate the maximum allowed memory, problems with swap can arise. There are three major scenarios to look at:

System with no swap

The application gets the maximum allowed memory. All caches are freed, and thus all other running applications are slowed. After a few minutes, the kernel's out-of-memory kill mechanism activates and kills the process.

System with medium sized swap (128 MB–512 MB)

At first, the system slows like a system without swap. After all physical RAM has been allocated, 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 kill mechanism resolves the issue. Note that you will need a certain amount of swap if the computer needs to perform a “suspend to disk”. In that case, the swap size should be large enough 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 out of control and swapping excessively in this case. If you use such application, 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 after terminating the faulty process. In this case, do a hard machine reboot 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 is not out of control, but needs more swap after some time, it is possible to extend the swap space online. If you prepared a partition for swap space, add this partition with YaST. If you do not have a partition available, you can also use a swap file to extend the swap. Swap files are generally slower than partitions, but compared to physical RAM, both are extremely slow so the actual difference is negligible.

PROCEDURE 7.2: 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
```



Note: Changed UUID for Swap Partitions when Formatting via **mkswap**

Do not reformat existing swap partitions with **mkswap** if possible. Reformatting with **mkswap** will change the UUID value of the swap partition. Either reformat via YaST (will update `/etc/fstab`) or adjust `/etc/fstab` manually.

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, it is only temporary swap space. After the next reboot, it is no longer used.

5. To enable this swap file permanently, add the following line to `/etc/fstab`:

```
/var/lib/swap/swapfile swap swap defaults 0 0
```

7.1.7 Partitioning and LVM

From the *Expert partitioner*, access the LVM configuration by clicking the *Volume Management* item in the *System View* pane. However, if a working LVM configuration already exists on your system, it is automatically activated upon entering the initial LVM configuration of a session. In this case, all disks containing a partition (belonging to an activated volume group) cannot be repartitioned. The Linux kernel cannot reread the modified partition table of a hard disk when any partition on this disk is in use. If you already have a working 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.

In case you want to change your `/usr` or `swap`, refer to , *Updating Init RAM Disk When Switching to Logical Volumes*.

7.2 LVM Configuration

This section explains specific steps to take when configuring LVM.



Warning: Back up Your Data

Using LVM is sometimes 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.

7.2.1 LVM Configuration with YaST

The YaST LVM configuration can be reached from the YaST Expert Partitioner (see [Section 7.1, “Using the YaST Partitioner”](#)) within the *Volume Management* item in the *System View* pane. The Expert Partitioner allows you to edit and delete existing partitions and create new ones that need to 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 partition* and change the *File System ID* to *0x8E Linux LVM*. Do not mount this partition.
5. Repeat this procedure until you have defined all the desired physical volumes on the available disks.

7.2.1.1 Creating Volume Groups

If no volume group exists on your system, you must add one (see [Figure 7.3, “Creating a Volume Group”](#)). It is possible to create additional groups by clicking *Volume Management* in the *System View* pane, and then on *Add Volume Group*. One single volume group is usually sufficient.

1. Enter a name for the VG, for example, 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 blocks of this size.
3. Add the prepared PVs to the VG by selecting the device and clicking *Add*. Selecting several devices is possible by holding `Ctrl` while selecting the devices.

4. Select *Finish* to make the VG available to further configuration steps.

Add Volume Group

Volume Group Name

Physical Extent Size

4 MiB

Available Physical Volumes:

| Device | Size | Enc | Type |
|-----------|-----------|--------------|------|
| /dev/vda1 | 4.00 GiB | Linux native | |
| /dev/vdb2 | 10.24 GiB | Linux native | |
| /dev/vdc1 | 12.00 GiB | Linux native | |
| /dev/vdc2 | 12.41 GiB | Linux native | |

Add ->

Add All ->

<- Remove

<- Remove All

Selected Physical Volumes:

| Device | Size | Enc | Type |
|--------|------|-----|------|
|--------|------|-----|------|

Total size: 38.65 GiB

Resulting size: 0 B

Help

Abort Back Finish

FIGURE 7.3: CREATING A VOLUME GROUP

If you have multiple volume groups defined and want to add or remove PVs, select the volume group in the *Volume Management* list and click *Resize*. In the following window, you can add or remove PVs to the selected volume group.

7.2.1.2 Configuring Logical Volumes

After the volume group has been filled with PVs, define the LVs which 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 occupied. Assign at least one LV to each volume group.

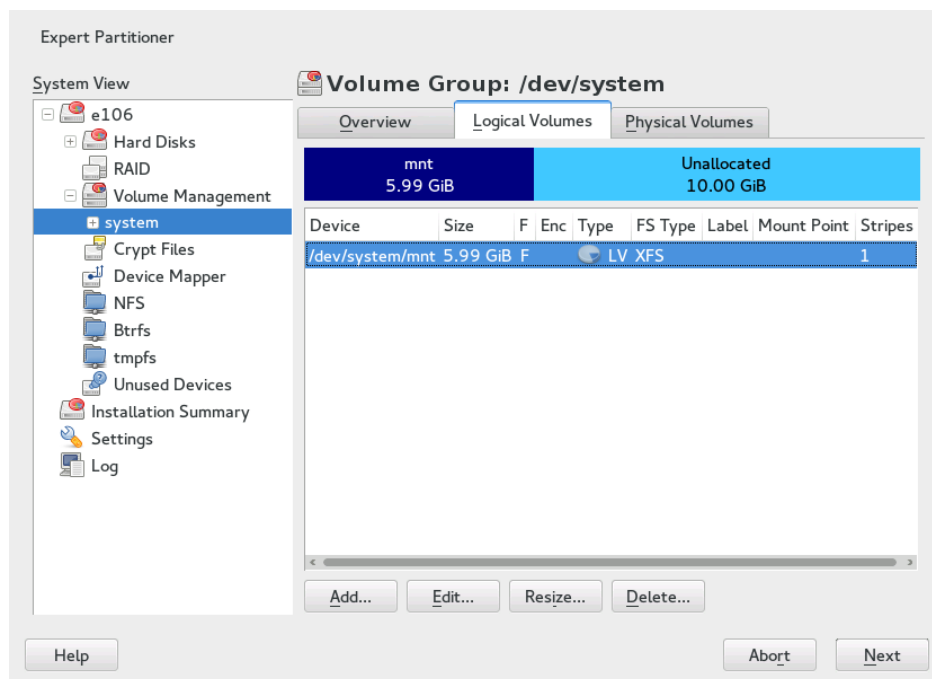


FIGURE 7.4: LOGICAL VOLUME MANAGEMENT

Click *Add* and go through the wizard-like pop-up that opens:

1. Enter the name of the LV. For a partition that should be mounted to /home, a name like HOME could be used.
2. Select the type of the LV. It can be either *Normal Volume*, *Thin Pool*, or *Thin Volume*. Note that you need to create a thin pool first, which can store individual thin volumes. The big advantage of thin provisioning is that the total sum of all thin volumes stored in a thin pool can exceed the size of the pool itself.
3. Select the size and the number of stripes of the LV. If you have only one PV, selecting more than one stripe is not useful.
4. Choose the file system to use on the LV and the mount point.

By using stripes it is possible to distribute the data stream in the LV among several PVs (striping). However, striping a volume can only be done over different PVs, each providing at least the amount of space of the volume. The maximum number of stripes equals to the number of PVs, where Stripe "1" means "no striping". Striping only makes sense with PVs on different hard disks, otherwise performance will decrease.



Warning: Striping

YaST cannot, at this point, 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. With *Finish*, return to the YaST Expert Partitioner and finish your work there.

7.3 Soft RAID Configuration with YaST

This section describes actions required to create and configure various types of RAID. .

7.3.1 Soft RAID Configuration with YaST

The YaST *RAID* configuration can be reached from the YaST Expert Partitioner, described in [Section 7.1, “Using the YaST Partitioner”](#). This partitioning tool enables you to edit and delete existing partitions and create new ones to be used with soft RAID:

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 have 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, RAID 6 and RAID 10 require at least four partitions. It is recommended to use partitions of the same size only. 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, 5, 6 and 10. 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.



Tip: Classify Disks

For RAID types where the order of added disks matters, you can mark individual disks with one of the letters A to E. Click the *Classify* button, select the disk and click of the *Class X* buttons, where X is the letter you want to assign to the disk. Assign all available RAID disks this way, and confirm with *OK*. You can easily sort the classified disks with the *Sorted* or *Interleaved* buttons, or add a sort pattern from a text file with *Pattern File*.

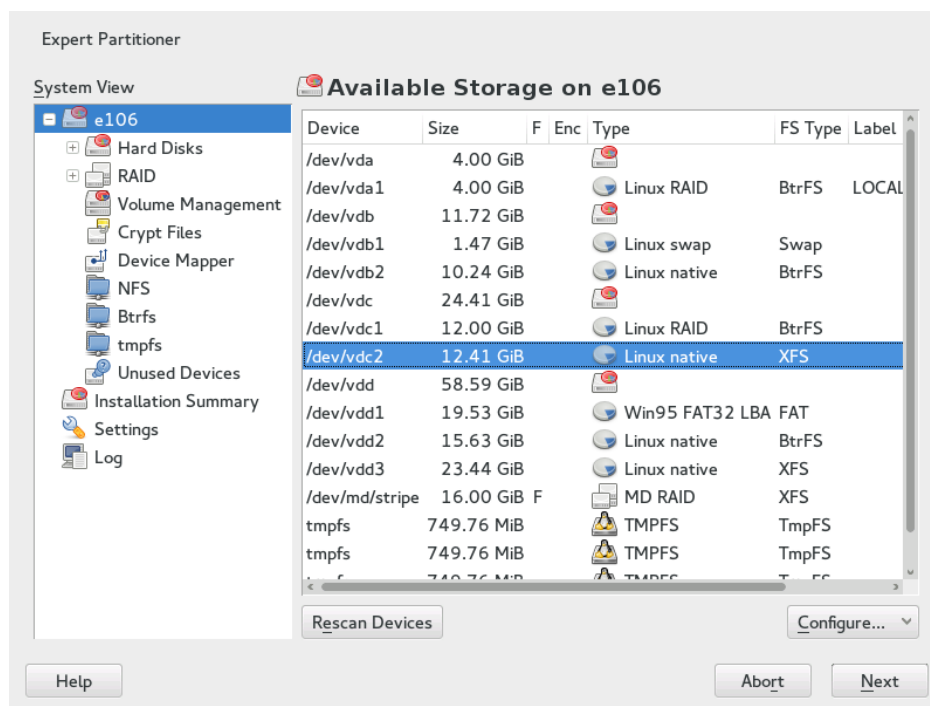


FIGURE 7.5: RAID PARTITIONS

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 this last step, set the file system to use, 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.


7.3.2 Troubleshooting


Check the file `/proc/mdstat` to find out whether a RAID partition has been damaged. If the system fails, 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.

7.3.3 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://raid.wiki.kernel.org> 

Linux RAID mailing lists are available, such as <http://marc.info/?l=linux-raid> .

8 Installing or Removing Software

Use YaST's software management module to search for software components you want to add or remove. YaST resolves all dependencies for you. To install packages not shipped with the installation media, add additional software repositories to your setup and let YaST manage them. Keep your system up-to-date by managing software updates with the update applet.

Change the software collection of your system with the YaST Software Manager. This YaST module is available in two flavors: a graphical variant for X Window and a text-based variant to be used on the command line. The graphical flavor is described here—for details on the text-based YaST, see *Book “Administration Guide”, Chapter 4 “YaST in Text Mode”*.



Note: Confirmation and Review of Changes

When installing, updating or removing packages, any changes in the Software Manager are not applied immediately but only after confirming them with *Accept* or *Apply* respectively. YaST maintains a list with all actions, allowing you to review and modify your changes before applying them to the system.

8.1 Definition of Terms

Repository

A local or remote directory containing packages, plus additional information about these packages (package metadata).

(Repository) Alias/Repository Name

A short name for a repository (called Alias within Zypper and *Repository Name* within YaST). It can be chosen by the user when adding a repository and must be unique.

Repository Description Files

Each repository provides files describing content of the repository (package names, versions, etc.). These repository description files are downloaded to a local cache that is used by YaST.

Product

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

Pattern

A pattern is an installable group of packages dedicated to a certain purpose. For example, the Laptop pattern contains all packages that are needed in a mobile computing environment. Patterns define package dependencies (such as required or recommended packages) and come with a preselection of packages marked for installation. This ensures that the most important packages needed for a certain purpose are available on your system after installation of the pattern. However, not necessarily all packages in a pattern are preselected for installation and you can manually select or deselect packages within a pattern according to your needs and wishes.

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 and may be applied by means of delta RPMs. It may also introduce dependencies to packages that are not installed yet.

Resolvable

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

Delta RPM

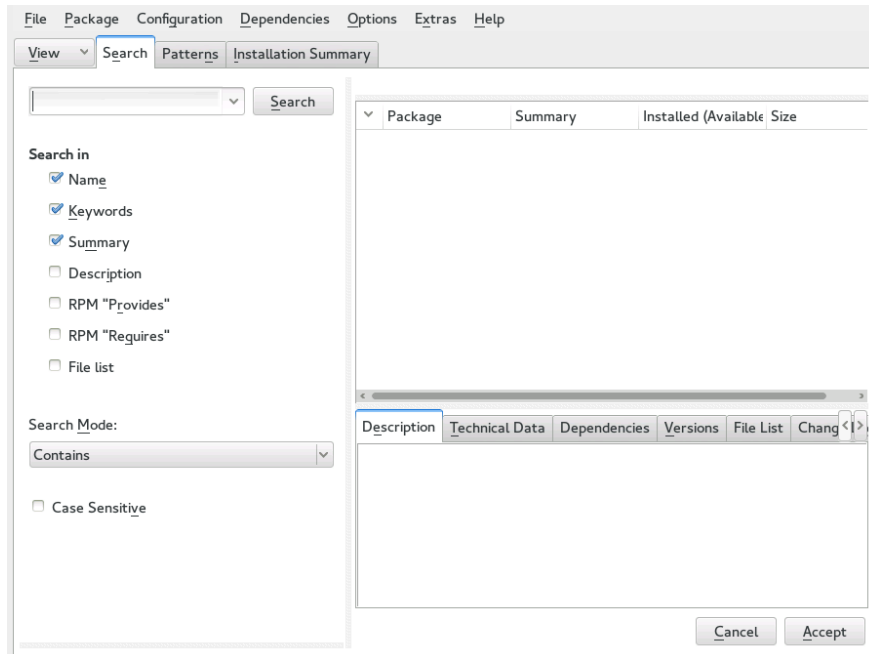
A delta RPM consists only of the binary diff between two defined versions of a package, and therefore has the smallest download size. Before being installed, the full RPM package is rebuilt on the local machine.

Package Dependencies

Certain packages are dependent on other packages, such as shared libraries. In other terms, a package may require other packages—if the required packages are not available, the package cannot be installed. In addition to dependencies (package requirements) that must be fulfilled, some packages recommend other packages. These recommended packages are only installed if they are actually available, otherwise they are ignored and the package recommending them is installed nevertheless.

8.2 Using the YaST Software Manager

Start the software manager from the *YaST Control Center* by choosing *Software > Software Management*.



8.2.1 Views for Searching Packages or Patterns

The YaST software manager can install packages or patterns from all currently enabled repositories. It offers different views and filters to make it easier to find the software you are searching for. The *Search* view is the default view of the window. To change view, click *View* and select one of the following entries from the drop-down box. The selected view opens in a new tab.

Patterns

Lists all patterns available for installation on your system.

Package Groups

Lists all packages sorted by groups such as *Graphics*, *Programming*, or *Security*.

RPM Groups

Lists all packages sorted by functionality with groups and subgroups. For example *Networking > Email > Clients*.

Languages

A filter to list all packages needed to add a new system language.

Repositories

A filter to list packages by repository. To select more than one repository, hold the **Ctrl** key while clicking repository names. The “pseudo repository” *@System* lists all packages currently installed.

Search

Lets you search for a package according to certain criteria. Enter a search term and press **Enter**. Refine your search by specifying where to *Search In* and by changing the *Search Mode*. For example, if you do not know the package name but only the name of the application that you are searching for, try including the package *Description* in the search process.

Installation Summary

If you have already selected packages for installation, update or removal, this view shows the changes that will be applied to your system when you click *Accept*. To filter for packages with a certain status in this view, activate or deactivate the respective check boxes. Press **Shift-F1** for details on the status flags.



Tip: Finding Packages Not Belonging to an Active Repository

To list all packages that do not belong to an active repository, choose *View > Repositories > @System* and then choose *Secondary Filter > Unmaintained Packages*. This is useful, for example, if you have deleted a repository and want to make sure no packages from that repository remain installed.

8.2.2 Installing and Removing Packages or Patterns

Certain packages are dependent on other packages, such as shared libraries. On the other hand, some packages cannot coexist with others on the system. If possible, YaST automatically resolves these dependencies or conflicts. If your choice results in a dependency conflict that cannot be automatically solved, you need to solve it manually as described in [Section 8.2.4, “Checking Software Dependencies”](#).



Note: Removal of Packages

When removing any packages, by default YaST only removes the selected packages. If you want YaST to also remove any other packages that become unneeded after removal of the specified package, select *Options > Cleanup when deleting packages* from the main menu.

1. Search for packages as described in [Section 8.2.1, “Views for Searching Packages or Patterns”](#).
2. The packages found are listed in the right pane. To install a package or remove it, right-click it and choose *Install* or *Delete*. If the relevant option is not available, check the package status indicated by the symbol in front of the package name—press **Shift**–**F1** for help.



Tip: Applying an Action to All Packages Listed

To apply an action to all packages listed in the right pane, go to the main menu and choose an action from *Package > All in This List*.

3. To install a pattern, right-click the pattern name and choose *Install*.
4. It is not possible to remove a pattern per se. Instead, select the packages of a pattern you want to remove and mark them for removal.
5. To select more packages, repeat the steps mentioned above.
6. Before applying your changes, you can review or modify them by clicking *View > Installation Summary*. By default, all packages that will change status, are listed.
7. To revert the status for a package, right-click the package and select one of the following entries: *Keep* if the package was scheduled to be deleted or updated, or *Do Not Install* if it was scheduled for installation. To abandon all changes and quit the Software Manager, click *Cancel* and *Abandon*.
8. When you are finished, click *Accept* to apply your changes.
9. In case YaST found dependencies on other packages, a list of packages that have additionally been chosen for installation, update or removal is presented. Click *Continue* to accept them.

After all selected packages are installed, updated or removed, the YaST Software Manager automatically terminates.



Note: Installing Source Packages

Installing source packages with YaST Software Manager is not possible at the moment. Use the command line tool **zypper** for this purpose. For more information, see *Book “Administration Guide”, Chapter 5 “Managing Software with Command Line Tools”, Section 5.1.2.5 “Installing or Downloading Source Packages”*.

8.2.3 Updating Packages

Instead of updating individual packages, you can also update all installed packages or all packages from a certain repository. When mass updating packages, the following aspects are generally considered:

- priorities of the repositories that provide the package,
- architecture of the package (for example, AMD64/Intel 64),
- version number of the package,
- package vendor.

Which of the aspects has the highest importance for choosing the update candidates depends on the respective update option you choose.

1. To update all installed packages to the latest version, choose *Package > All Packages > Update if Newer Version Available* from the main menu.

All repositories are checked for possible update candidates, using the following policy: YaST first tries to restrict the search to packages with the same architecture and vendor like the installed one. If the search is positive, the “best” update candidate from those is selected according to the process below. However, if no comparable package of the same vendor can be found, the search is expanded to all packages with the same architecture. If still no comparable package can be found, all packages are considered and the “best” update candidate is selected according to the following criteria:

1. Repository priority: Prefer the package from the repository with the highest priority.
2. If more than one package results from this selection, choose the one with the “best” architecture (best choice: matching the architecture of the installed one).

If the resulting package has a higher version number than the installed one, the installed package will be updated and replaced with the selected update candidate.

This option tries to avoid changes in architecture and vendor for the installed packages, but under certain circumstances, they are tolerated.



Note: Update Unconditionally

If you choose *Package > All Packages > Update Unconditionally* instead, the same criteria apply but any candidate package found is installed unconditionally. Thus, choosing this option might actually lead to downgrading some packages.

2. To make sure that the packages for a mass update derive from a certain repository:
 - a. Choose the repository from which to update as described in [Section 8.2.1, “Views for Searching Packages or Patterns”](#).
 - b. On the right hand side of the window, click *Switch system packages to the versions in this repository*. This explicitly allows YaST to change the package vendor when replacing the packages.

When you proceed with *Accept*, all installed packages will be replaced by packages deriving from this repository, if available. This may lead to changes in vendor and architecture and even to downgrading some packages.
 - c. To refrain from this, click *Cancel switching system packages to the versions in this repository*. Note that you can only cancel this until you press the *Accept* button.
3. Before applying your changes, you can review or modify them by clicking *View > Installation Summary*. By default, all packages that will change status, are listed.
4. If all options are set according to your wishes, confirm your changes with *Accept* to start the mass update.

8.2.4 Checking Software Dependencies

Most packages are dependent on other packages. If a package, for example, uses a shared library, it is dependent on the package providing this library. On the other hand some packages cannot coexist with each other, causing a conflict (for example, you can only install one mail transfer agent: sendmail or postfix). When installing or removing software, the Software Manager makes sure no dependencies or conflicts remain unsolved to ensure system integrity.

In case there exists only one solution to resolve a dependency or a conflict, it is resolved automatically. Multiple solutions always cause a conflict which needs to be resolved manually. If solving a conflict involves a vendor or architecture change, it also needs to be solved manually. When clicking *Accept* to apply any changes in the Software Manager, you get an overview of all actions triggered by the automatic resolver which you need to confirm.

By default, dependencies are automatically checked. A check is performed every time you change a package status (for example, by marking a package for installation or removal). This is generally useful, but can become exhausting when manually resolving a dependency conflict. To disable this function, go to the main menu and deactivate *Dependencies > Autocheck*. Manually perform a dependency check with *Dependencies > Check Now*. A consistency check is always performed when you confirm your selection with *Accept*.

To review a package's dependencies, right-click it and choose *Show Solver Information*. A map showing the dependencies opens. Packages that are already installed are displayed in a green frame.



Note: Manually Solving Package Conflicts

Unless you are very experienced, follow the suggestions YaST makes when handling package conflicts, otherwise you may not be able to resolve them. Keep in mind that every change you make, potentially triggers other conflicts, so you can easily end up with a steadily increasing number of conflicts. In case this happens, *Cancel* the Software Manager, *Abandon* all your changes and start again.

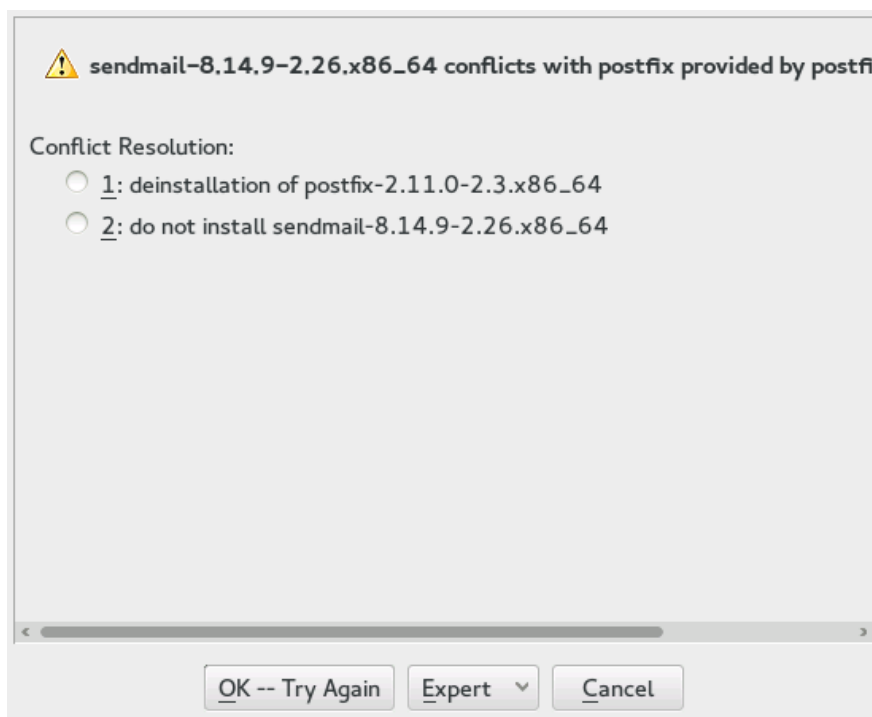


FIGURE 8.1: CONFLICT MANAGEMENT OF THE SOFTWARE MANAGER

8.2.4.1 Handling of Package Recommendations

In addition to the hard dependencies required to run a program (for example a certain library), a package can also have weak dependencies, that add for example extra functionality or translations. These weak dependencies are called package recommendations.

The way package recommendations are handled has slightly changed starting with SUSE Linux Enterprise Desktop 12 SP1. Nothing has changed when installing a new package—recommended packages are still installed by default.

Prior to SLES 12 SP1, missing recommendations for already installed packages were installed automatically. Now these packages will no longer be installed automatically. To switch to the old default, set `PKGMR_REEVALUATE_RECOMMENDED="yes"` in `/etc/sysconfig/yast2`. To install all missing recommendations for already installed packages, start *YaST* > *Software Manager* and choose *Extras* > *Install All Matching Recommended Packages*.

To disable the installation of recommended packages when installing new packages, deactivate *Dependencies* > *Install Recommended Packages* in the YaST Software Manager. If using the command line tool Zypper to install packages, use the option `--no-recommends`.

8.3 Managing Software Repositories and Services

If you want to install third-party software, add additional software repositories to your system. By default, the product repositories such as SUSE Linux Enterprise Desktop-DVD 12 SP2 and a matching update repository are automatically configured after you have registered your system. For more information about registration, see [Section 2.7, “SUSE Customer Center Registration”](#) or [Section 14.10, “Registering Your System”](#). Depending on the initially selected product, an additional repository containing translations, dictionaries, etc. might also be configured.

To manage repositories, start YaST and select *Software > Software Repositories*. The *Configured Software Repositories* dialog opens. Here, you can also manage subscriptions to so-called *Services* by changing the *View* at the right corner of the dialog to *All 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.

Each repository provides files describing content of the repository (package names, versions, etc.). These repository description files are downloaded to a local cache that is used by YaST. To ensure their integrity, software repositories can be signed with the GPG Key of the repository maintainer. Whenever you add a new repository, YaST offers the ability to import its key.



Warning: Trusting External Software Sources

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

8.3.1 Adding Software Repositories

You can either add repositories from DVD/CD, removable mass storage devices (such as flash disks), or a local directory or ISO image.

To add repositories from the *Configured Software Repositories* dialog in YaST proceed as follows:

1. Click *Add*.

2. Select one of the options listed in the dialog:

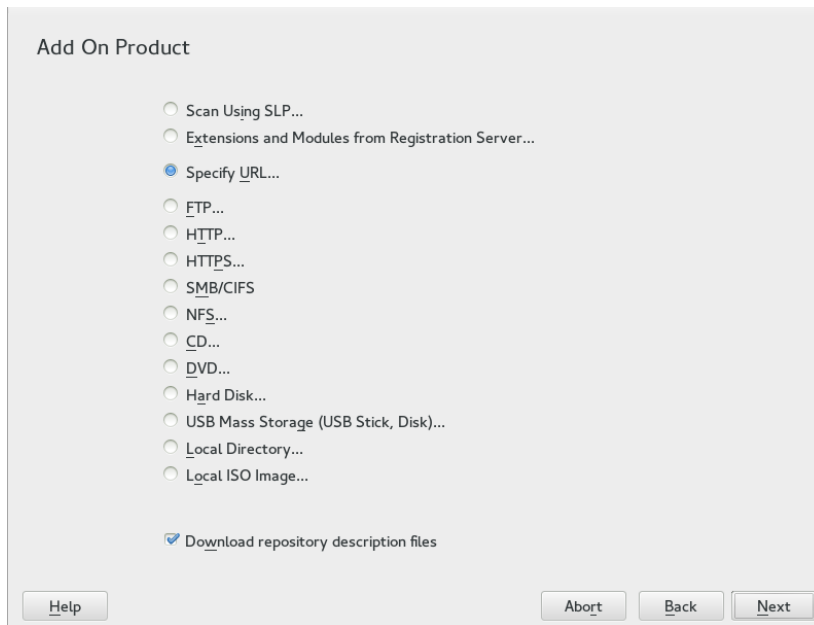


FIGURE 8.2: ADDING A SOFTWARE REPOSITORY

- To scan your network for installation servers announcing their services via SLP, select *Scan Using SLP* and click *Next*.
- To add a repository from a removable medium, choose the relevant option and insert the medium or connect the USB device to the machine, respectively. Click *Next* to start the installation.
- For the majority of repositories, you will be asked to specify the path (or URL) to the media after selecting the respective option and clicking *Next*. Specifying a *Repository Name* is optional. If none is specified, YaST will use the product name or the URL as repository name.

The option *Download Repository Description Files* is activated by default. If you deactivate the option, YaST will automatically download the files later, if needed.

3. Depending on the repository you have added, you may be asked if you want to import the GPG key with which it is signed or asked to agree to a license.
After confirming these messages, YaST will download and parse the metadata. It will add the repository to the list of *Configured Repositories*.

4. If needed, adjust the repository *Properties* as described in [Section 8.3.2, “Managing Repository Properties”](#).
5. Confirm your changes with *OK* to close the configuration dialog.
6. After having successfully added the repository, the software manager starts and you can install packages from this repository. For details, refer to [Chapter 8, Installing or Removing Software](#).

8.3.2 Managing Repository Properties

The *Configured Software Repositories* overview of the *Software Repositories* lets you change the following repository properties:

Status

The repository status can either be *Enabled* or *Disabled*. You can only install packages from repositories that are enabled. To turn a repository off temporarily, select it and deactivate *Enable*. You can also double-click a repository name to toggle its status. If you want to remove a repository completely, click *Delete*.

Refresh

When refreshing a repository, its content description (package names, versions, etc.) is downloaded to a local cache that is used by YaST. It is sufficient to do this once for static repositories such as CDs or DVDs, whereas repositories whose content changes often should be refreshed frequently. The easiest way to keep a repository's cache up-to-date is to choose *Automatically Refresh*. To do a manual refresh click *Refresh* and select one of the options.

Keep Downloaded Packages

Packages from remote repositories are downloaded before being installed. By default, they are deleted upon a successful installation. Activating *Keep Downloaded Packages* prevents the deletion of downloaded packages. The download location is configured in `/etc/zypp/zypp.conf`, by default it is `/var/cache/zypp/packages`.

Priority

The *Priority* of a repository is a value between `1` and `200`, with `1` being the highest priority and `200` the lowest priority. Any new repositories that are added with YaST get a priority of `99` by default. If you do not care about a priority value for a certain repository, you can also set the value to `0` to apply the default priority to that repository (`99`). If a package is

available in more than one repository, then the repository with the highest priority takes precedence. This is useful if you want to avoid downloading packages unnecessarily from the Internet by giving a local repository (for example, a DVD) a higher priority.



Important: Priority Compared to Version

The repository with the highest priority takes precedence in any case. Therefore, make sure that the update repository always has the highest priority, otherwise you might install an outdated version that will not be updated until the next online update.

Name and URL

To change a repository name or its URL, select it from the list with a single-click and then click *Edit*.

8.3.3 Managing Repository Keys

To ensure their integrity, software repositories can be signed with the GPG Key of the repository maintainer. Whenever you add a new repository, YaST offers to import its key. Verify it as you would do with any other GPG key and make sure it does not change. If you detect a key change, something might be wrong with the repository. Disable the repository as an installation source until you know the cause of the key change.

To manage all imported keys, click *GPG Keys* in the *Configured Software Repositories* dialog. Select an entry with the mouse to show the key properties at the bottom of the window. *Add*, *Edit* or *Delete* keys with a click on the respective buttons.

8.4 Keeping the System Up-to-date

SUSE offers a continuous stream of software security patches for your product. They can be installed using the *Book “Administration Guide”, Chapter 3 “YaST Online Update”* module. It also offers advanced features to customize the patch installation.

The GNOME desktop also provides a tool for installing patches and for installing package updates of packages that are already installed. In contrast to a *Patch*, a package update is only related to *one* package and provides a newer version of a package. The GNOME tool lets you install both patches and package updates with a few clicks as described in *Section 8.4.2, “Installing Patches and Package Updates”*.

8.4.1 The GNOME Software Updater

Whenever new patches or package updates are available, GNOME shows a notification about this at the bottom of the desktop (or on the locked screen).

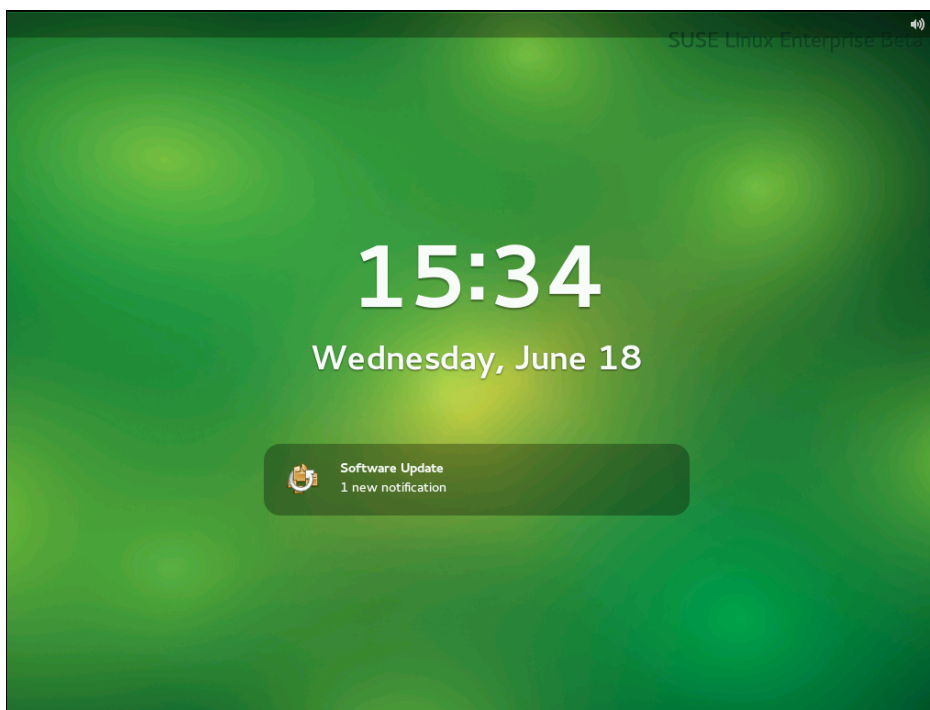


FIGURE 8.3: UPDATE NOTIFICATION ON GNOME LOCK SCREEN

8.4.2 Installing Patches and Package Updates

Whenever new patches or package updates are available, GNOME shows a notification about this at the bottom of the desktop (or on the locked screen).

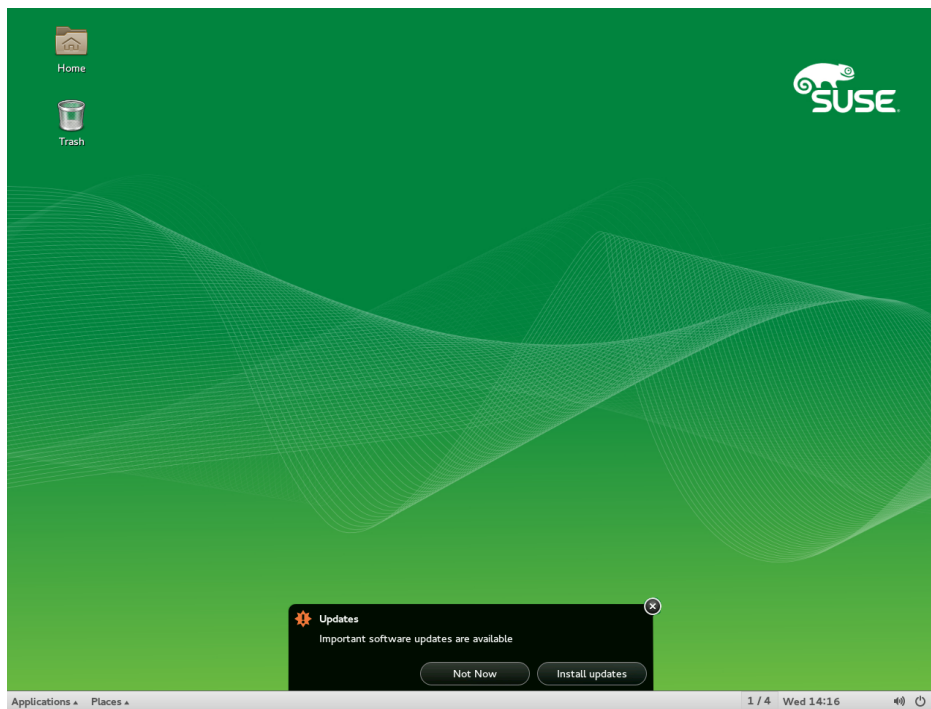


FIGURE 8.4: UPDATE NOTIFICATION ON GNOME DESKTOP

1. To install the patches and updates, click *Install updates* in the notification message. This opens the GNOME update viewer. Alternatively, open the update viewer from *Applications > System Tools > Software Update* or press **Alt-F2** and enter **gpk-update-viewer**.
2. All *Security Updates* and *Important Updates* are preselected. It is strongly recommended to install these patches. *Other Updates* can be manually selected by activating the respective check boxes. Get detailed information on a patch or package update by clicking its title.
3. Click *Install Updates* to start the installation. You will be prompted for the root password.
4. Enter the root password in the authentication dialog and proceed.

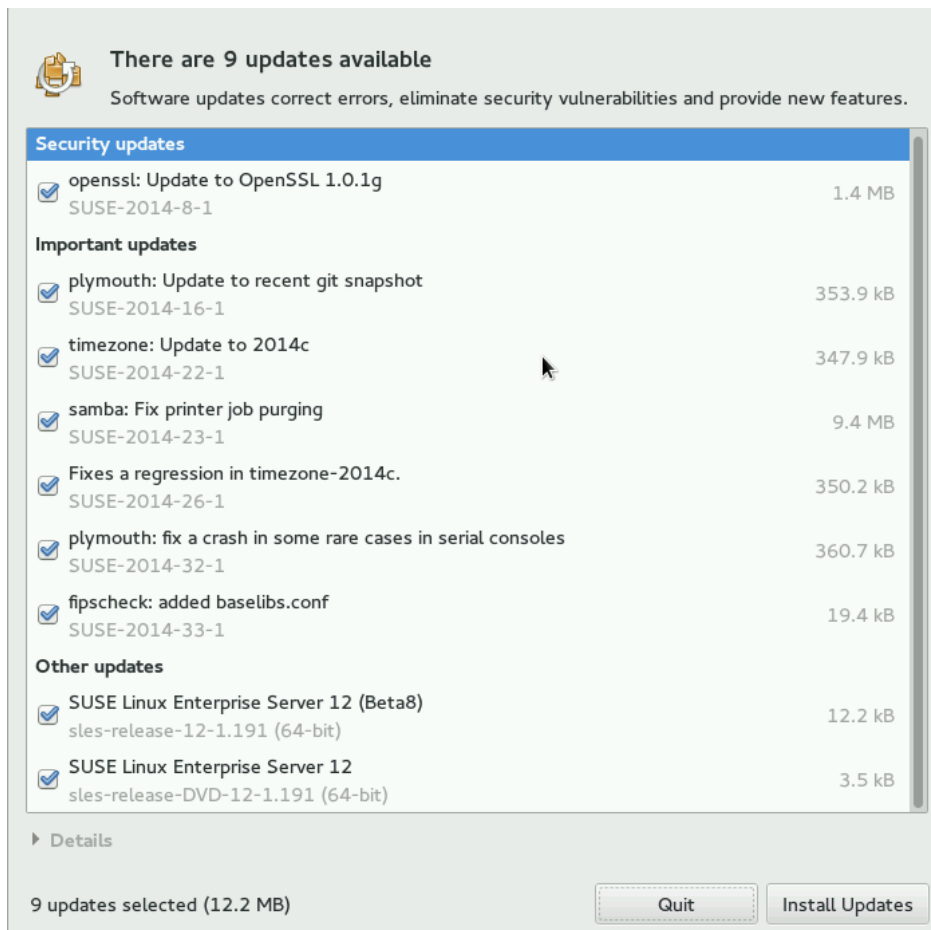


FIGURE 8.5: GNOME UPDATE VIEWER

8.4.3 Configuring the GNOME Software Updater

To define the appearance of the notification (where it appears on the screen, whether to display it on the lock screen), select *Applications > System Settings > Notification > Software Update* and change the settings according to your wishes.

To configure how often to check for updates or to activate or deactivate repositories, select *Applications > System Tools > Settings > Software Settings*. The tabs of the configuration dialog let you modify the following settings:

UPDATE SETTINGS

Check for Updates

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

Check for Major Upgrades

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

Check for updates when using mobile broadband

This configuration option is only available on mobile computers. Turned off by default.

Check for updates on battery power

This configuration option is only available on mobile computers. Turned off by default.

SOFTWARE SOURCES

Repositories

Lists the repositories that will be checked for available patches and package updates. You can enable or disable certain repositories.



Important: Keep Update Repository Enabled

To make sure that you are notified about any patches that are security-relevant, keep the Updates repository for your product enabled.

More options are configurable using **gconf-editor**: *apps > gnome-packagekit*.

9 Installing Modules, Extensions, and Third Party Add-On Products

Modules and extensions add parts or functionality to the system. Modules are fully supported parts of SUSE Linux Enterprise Desktop with a different life cycle and update timeline. They are a set of packages, have a clearly defined scope and are delivered via online channel only.

Extensions, such as the Workstation Extension or the High Availability Extension, add extra functionality to the system and require an own registration key that is liable for costs. Extensions are delivered via online channel or physical media. Registering at the SUSE Customer Center or a local registration server is a prerequisite for being able to subscribe to the online channels.

A list of modules and extensions for your product is available after having registered your system at SUSE Customer Center or a local registration server. If you skipped the registration step during the installation, you can register your system at any time using the *SUSE Customer Center Configuration* module in YaST. For details, refer to [Section 14.10, “Registering Your System”](#).

Some add-on products are also provided by third parties, for example, binary-only drivers that are needed by certain hardware to function properly. If you have such hardware, refer to the release notes for more information about availability of binary drivers for your system. The release notes are available from <http://www.suse.com/releasenotes/>, from YaST or from `/usr/share/doc/release-notes/` in your installed system.

9.1 Installing Modules and Extensions from On-line Channels



Tip: SUSE Linux Enterprise Desktop

As of SUSE Linux Enterprise 12, SUSE Linux Enterprise Desktop is not only available as a separate product, but also as a Workstation Extension for SUSE Linux Enterprise Server. If you register at the SUSE Customer Center, the Workstation Extension can be selected for installation. Note that installing it requires a valid registration key.

The following procedure requires that you have registered your system with SUSE Customer Center, or a local registration server. If you are in the process of registering your system, you will see a list of extensions and modules immediately after having completed *Step 4* of *Section 14.10*, “*Registering Your System*”. In that case, skip the next steps and proceed with *Step 3*.

PROCEDURE 9.1: INSTALLING ADD-ONS AND EXTENSIONS FROM ONLINE CHANNELS WITH YAST

1. Start YaST and select *Software > Add-On Products*. Alternatively, start the YaST *Add-On Products* module from the command line with `sudo yast2 add-on`.

The dialog will show an overview of already installed add-on products, modules and extensions.

2. To add repositories from SUSE Customer Center (or a local registration server), select *Add > Extensions and Modules from Registration Server*.

YaST connects to the registration server and displays a list of *Available Extensions and Modules*.



Note: Available Extensions and Modules

The amount of available extensions and modules depends on the registration server. A local registration server may only offer update repositories and no additional extensions.

3. Click an entry to see its description.
4. Select one or multiple entries for installation by activating their check marks.

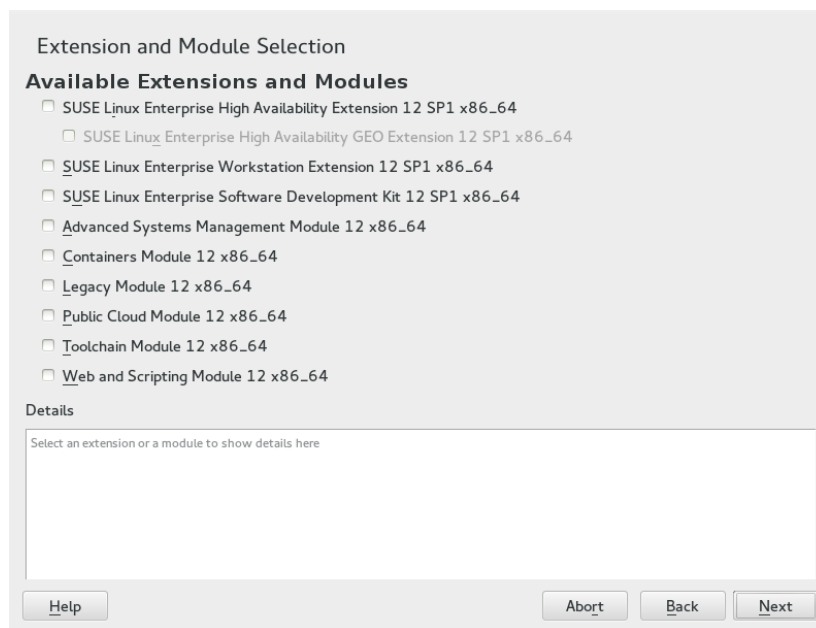


FIGURE 9.1: INSTALLATION OF SYSTEM EXTENSIONS


5. Click *Next* to proceed.
6. Depending on the repositories to be added for the extension or module, you may be asked if you want to import the GPG key with which the repository is signed or asked to agree to a license.

After confirming these messages, YaST will download and parse the metadata. The repositories for the selected extensions will be added to your system—no additional installation sources are required.

7. If needed, adjust the repository *Properties* as described in [Section 8.3.2, “Managing Repository Properties”](#).



Note: For More Information

White paper [SUSE Linux Enterprise Server 12 Modules \(https://www.suse.com/docrep/documents/huz0a6bf9a/suse_linux_enterprise_server_12_modules_white_paper.pdf\)](https://www.suse.com/docrep/documents/huz0a6bf9a/suse_linux_enterprise_server_12_modules_white_paper.pdf) .

9.2 Installing Extensions and Third Party Add-On Products from Media

When installing an extension or add-on product from media, you can select various types of product media, like DVD/CD, removable mass storage devices (such as flash disks), or a local directory or ISO image. The media can also be provided by a network server, for example, via HTTP, FTP, NFS, or Samba.

1. Start YaST and select *Software > Add-On Products*. Alternatively, start the YaST *Add-On Products* module from the command line with **`sudo yast2 add-on`**.
The dialog will show an overview of already installed add-on products, modules and extensions.

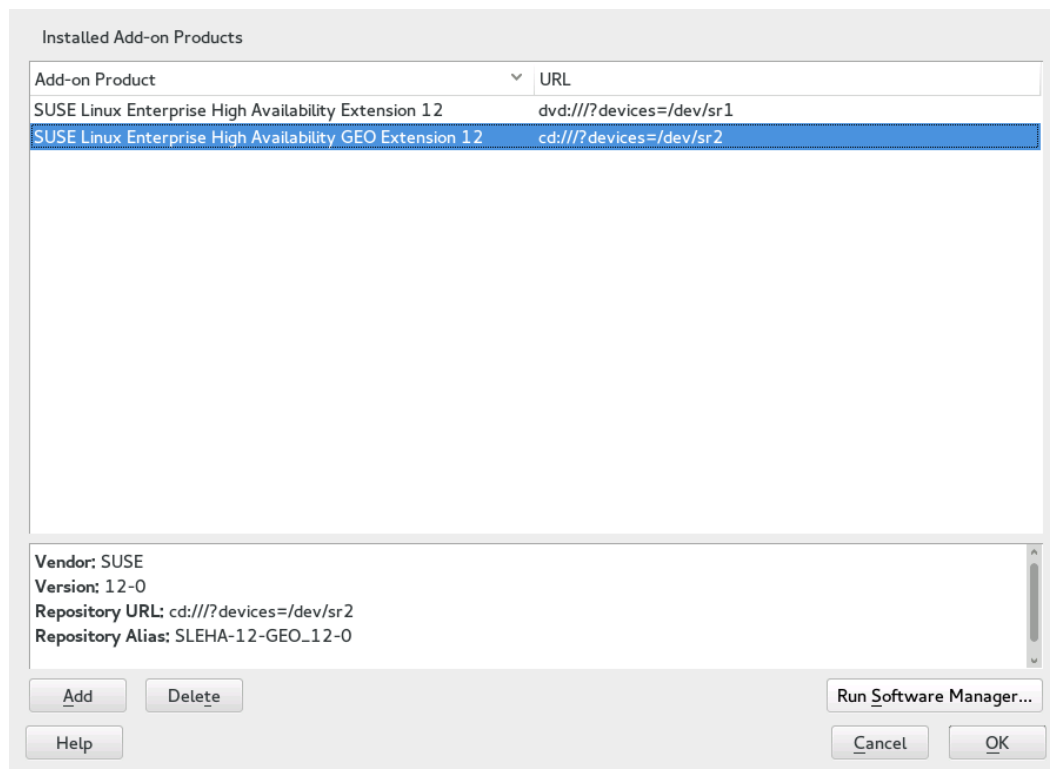


FIGURE 9.2: LIST OF INSTALLED ADD-ON PRODUCTS, MODULES AND EXTENSIONS

2. Choose *Add* to install a new add-on product.

3. In the *Add-On Product* dialog, select the option that matches the type of medium from which you want to install:

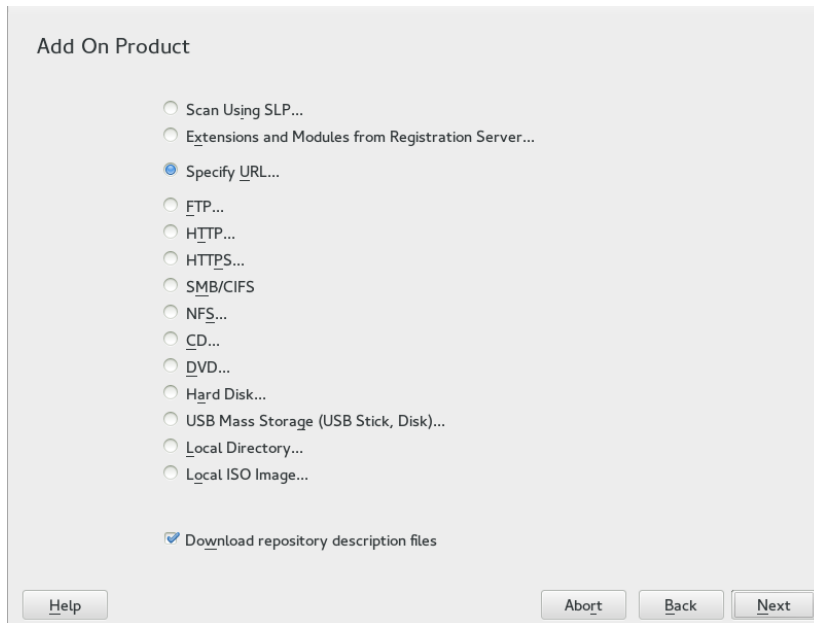


FIGURE 9.3: INSTALLATION OF AN ADD-ON PRODUCT OR AN EXTENSION

- To scan your network for installation servers announcing their services via SLP, select *Scan Using SLP* and click *Next*.
- To add a repository from a removable medium, choose the relevant option and insert the medium or connect the USB device to the machine, respectively. Click *Next* to start the installation.
- For the majority of media types, you will be asked to specify the path (or URL) to the media after selecting the respective option and clicking *Next*. Specifying a *Repository Name* is optional. If none is specified, YaST will use the product name or the URL as the repository name.

The option *Download Repository Description Files* is activated by default. If you deactivate the option, YaST will automatically download the files later, if needed.

4. Depending on the repository you have added, you may be asked if you want to import the GPG key with which it is signed or asked to agree to a license.
After confirming these messages, YaST will download and parse the metadata. It will add the repository to the list of *Configured Repositories*.

5. If needed, adjust the repository *Properties* as described in [Section 8.3.2, “Managing Repository Properties”](#).
6. Confirm your changes with *OK* to close the configuration dialog.
7. After having successfully added the repository for the add-on media, the software manager starts and you can install packages. For details, refer to [Chapter 8, Installing or Removing Software](#).

9.3 SUSE Software Development Kit (SDK) 12 SP2

SUSE Software Development Kit 12 SP2 is a module for SUSE Linux Enterprise 12 SP2. It is a complete tool kit for application development. In fact, to provide a comprehensive build system, SUSE Software Development Kit 12 SP2 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.

The SDK is a module for SUSE Linux Enterprise and is available via an online channel from the SUSE Customer Center. Alternatively, go to <http://download.suse.com/>, search for SUSE Linux Enterprise Software Development Kit and download it from there. Refer to [Chapter 9, Installing Modules, Extensions, and Third Party Add-On Products](#) for details.

10 Installing Multiple Kernel Versions

SUSE Linux Enterprise Desktop supports the parallel installation of multiple kernel versions. When installing a second kernel, a boot entry and an `initrd` are automatically created, so no further manual configuration is needed. When rebooting the machine, the newly added kernel is available as an additional boot option.

Using this functionality, you can safely test kernel updates while being able to always fall back to the proven former kernel. To do so, do not use the update tools (such as the YaST Online Update or the updater applet), but instead follow the process described in this chapter.



Warning: Support Entitlement

Be aware that you lose your entire support entitlement for the machine when installing a self-compiled or a third-party kernel. Only kernels shipped with SUSE Linux Enterprise Desktop and kernels delivered via the official update channels for SUSE Linux Enterprise Desktop are supported.



Tip: Check Your Boot Loader Configuration Kernel

It is recommended to check your boot loader configuration after having installed another kernel to set the default boot entry of your choice. See *Book “Administration Guide”, Chapter 12 “The Boot Loader GRUB 2”, Section 12.3 “Configuring the Boot Loader with YaST”* for more information.

10.1 Enabling and Configuring Multiversion Support

Installing multiple versions of a software package (multiversion support) is enabled by default on SUSE Linux Enterprise 12. To verify this setting, proceed as follows:

1. Open `/etc/zypp/zypp.conf` with the editor of your choice as `root`.

2. Search for the string `multiversion`. If multiversion is enabled for all kernel packages capable of this feature, the following line appears uncommented:

```
multiversion = provides:multiversion(kernel)
```

3. To restrict multiversion support to certain kernel flavors, add the package names as a comma-separated list to the `multiversion` option in `/etc/zypp/zypp.conf`—for example

```
multiversion = kernel-default,kernel-default-base,kernel-source
```

4. Save your changes.



Warning: Kernel Module Packages (KMP)

Make sure that required vendor provided kernel modules (Kernel Module Packages) are also installed for the new updated kernel. The kernel update process will not warn about eventually missing kernel modules because package requirements are still fulfilled by the old kernel that is kept on the system.

10.1.1 Automatically Deleting Unused Kernels

When frequently testing new kernels with multiversion support enabled, the boot menu quickly becomes confusing. Since a `/boot` partition usually has limited space you also might run into trouble with `/boot` overflowing. While you may delete unused kernel versions manually with YaST or Zypper (as described below), you can also configure `libzypp` to automatically delete kernels no longer used. By default no kernels are deleted.

1. Open `/etc/zypp/zypp.conf` with the editor of your choice as `root`.
2. Search for the string `multiversion.kernels` and activate this option by uncommenting the line. This option takes a comma-separated list of the following values:

`3.12.24-7.1`: keep the kernel with the specified version number

`latest`: keep the kernel with the highest version number

`latest-N`: keep the kernel with the Nth highest version number

`running`: keep the running kernel

oldest: keep the kernel with the lowest version number (the one that was originally shipped with SUSE Linux Enterprise Desktop)

oldest+N. keep the kernel with the Nth lowest version number

Here are some examples

multiversion.kernels = latest,running

Keep the latest kernel and the one currently running. This is similar to not enabling the multiversion feature, except that the old kernel is removed *after the next reboot* and not immediately after the installation.

multiversion.kernels = latest,latest-1,running

Keep the last two kernels and the one currently running.

multiversion.kernels = latest,running,3.12.25.rc7-test

Keep the latest kernel, the one currently running, and 3.12.25.rc7-test.



Tip: Keep the running Kernel

Unless using special setups, you probably always want to keep the running Kernel. If not keeping the running Kernel, it will be deleted in case of a Kernel update. This in turn makes it necessary to immediately reboot the system after the update, since modules for the Kernel that is currently running can no longer be loaded since they have been deleted.

10.2 Installing/Removing Multiple Kernel Versions with YaST

1. Start YaST and open the software manager via *Software > Software Management*.
2. List all packages capable of providing multiple versions by choosing *View > Package Groups > Multiversion Packages*.

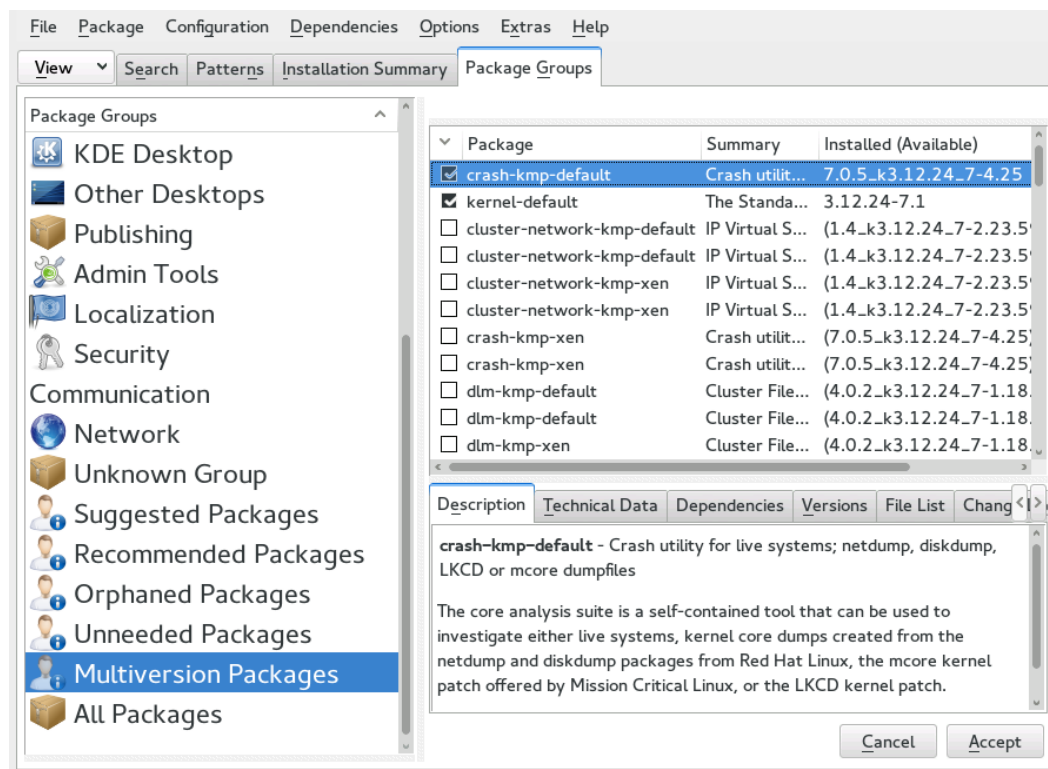


FIGURE 10.1: THE YAST SOFTWARE MANAGER: MULTIVERSION VIEW

3. Select a package and open its *Version* tab in the bottom pane on the left.
4. To install a package, click its check box. A green check mark indicates it is selected for installation.
To remove an already installed package (marked with a white check mark), click its check box until a red X indicates it is selected for removal.
5. Click *Accept* to start the installation.

10.3 Installing/Removing Multiple Kernel Versions with Zypper

1. Use the command `zypper se -s 'kernel*'` to display a list of all kernel packages available:

| S | Name | Type | Version | Arch | Repository |
|----|------|------|---------|------|------------|
| .. | + | + | + | + | + |

| | | | | | | | | | | |
|-----|--|----------------|--|------------|--|-----------------|--|--------|--|--------------------|
| v | | kernel-default | | package | | 2.6.32.10-0.4.1 | | x86_64 | | Alternative Kernel |
| i | | kernel-default | | package | | 2.6.32.9-0.5.1 | | x86_64 | | (System Packages) |
| | | kernel-default | | srcpackage | | 2.6.32.10-0.4.1 | | noarch | | Alternative Kernel |
| i | | kernel-default | | package | | 2.6.32.9-0.5.1 | | x86_64 | | (System Packages) |
| ... | | | | | | | | | | |

2. Specify the exact version when installing:

```
zypper in kernel-default-2.6.32.10-0.4.1
```

3. When uninstalling a kernel, use the commands **zypper se -si 'kernel*'** to list all kernels installed and **zypper rm PACKAGENAME-VERSION** to remove the package.

11 Managing Users with YaST

During installation, you could have created a local user for your system. With the YaST module *User and Group Management* you can add more users or edit existing ones. It also lets you configure your system to authenticate users with a network server.

11.1 User and Group Administration Dialog

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

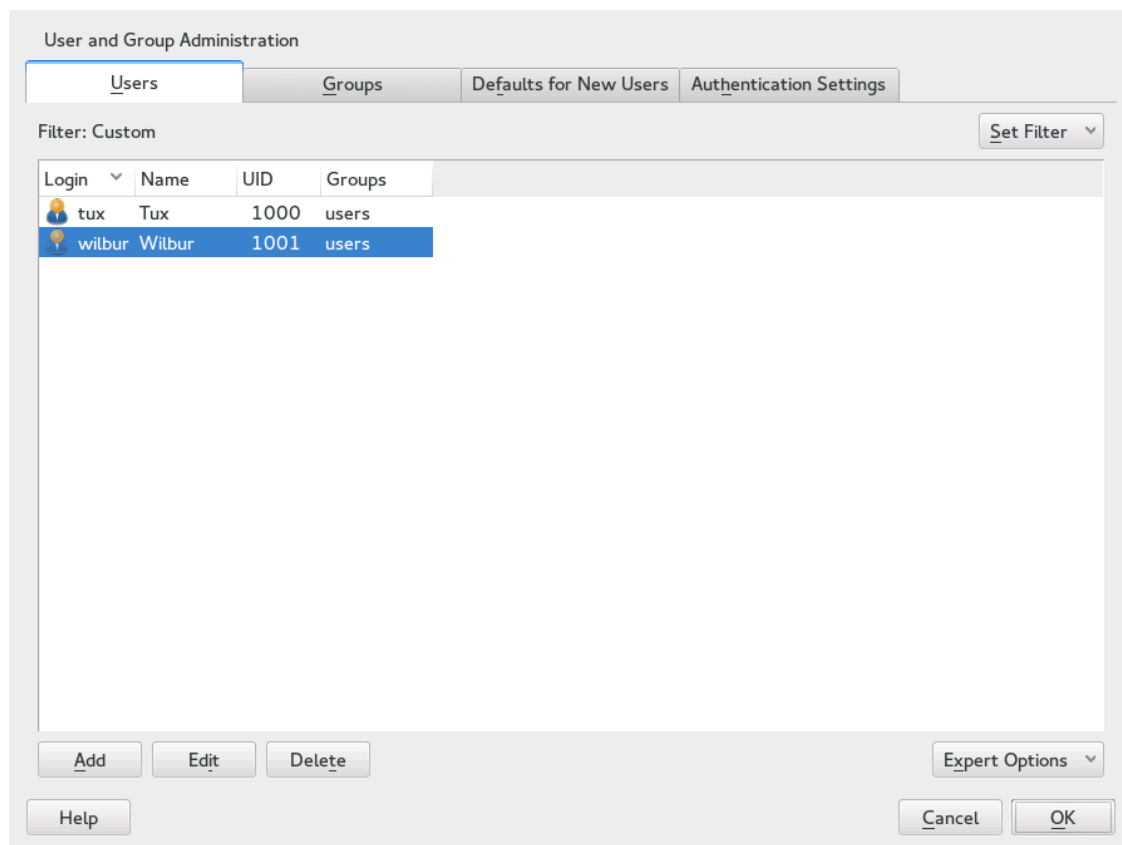


FIGURE 11.1: YAST USER AND GROUP ADMINISTRATION

Every user is assigned a system-wide user ID (UID). Apart from the users which can log in to your machine, there are also several *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.

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 11.2, “Managing User Accounts”](#). Learn about advanced options like enforcing password policies, using encrypted home directories, or managing disk quotas in [Section 11.3, “Additional Options for User Accounts”](#).

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 11.4, “Changing Default Settings for Local Users”](#).

Assigning Users to Groups

Learn how to change the group assignment for individual users in [Section 11.5, “Assigning Users to Groups”](#).

Managing Groups

From the *Groups* tab, you can add, modify or delete existing groups. Refer to [Section 11.6, “Managing Groups”](#) for information on how to do this.

Changing the User Authentication Method

When your machine is connected to a network that provides user authentication methods like NIS or LDAP, you can choose between several authentication methods on the *Authentication Settings* tab. For more information, refer to [Section 11.7, “Changing the User Authentication Method”](#).

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 example (if you are part of a network which uses LDAP). With *Set Filter* > *Customize Filter* you can also set up and use a custom filter.

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

11.2 Managing User Accounts

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



Note: Changing User IDs of Existing Users

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

In the following, learn how to set up default user accounts. For some further options, such as auto login, login without password, setting up encrypted home directories or managing quotas for users and groups, refer to [Section 11.3, "Additional Options for User Accounts"](#).

PROCEDURE 11.1: 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 lists users in the system and the groups the users belong to.
3. To modify options for an existing user, select an entry and click *Edit*.
To create a new user account, click *Add*.
4. Enter the appropriate user data on the first tab, such as *Username* (which is used for login) and *Password*. This data is sufficient to create a new user. If you click *OK* now, the system will automatically assign a user ID and set all other values according to the default.
5. Activate *Receive System Mail* if you want any kind of system notifications to be delivered to this user's mailbox. This creates a mail alias for root and the user can read the system mail without having to first log in as root.
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, you can use the mail command.
6. If you want to adjust further details such as the user ID or the path to the user's home directory, do so on the *Details* tab.

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

7. To force users to regularly change their password or set other password options, switch to *Password Settings* and adjust the options. For more details, refer to [Section 11.3.2, “Enforcing Password Policies”](#).
8. If all options are set according to your wishes, click *OK*.
9. Click *OK* to close the administration dialog and to save the changes. A newly added user can now log in to the system using the login name and password you created. Alternatively, if you want to save all changes without exiting the *User and Group Administration* dialog, click *Expert Options > Write Changes Now*.



Tip: Matching User IDs

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

PROCEDURE 11.2: **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.

11.3 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, use encrypted home directories or define disk quotas for users and groups.

11.3.1 Automatic Login and Passwordless Login

If you use the GNOME desktop environment you can configure *Auto Login* for a certain user and *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 user name 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*.

11.3.2 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 11.3: CONFIGURING PASSWORD SETTINGS

1. Open the YaST *User and Group Administration* dialog and select the *Users* tab.
2. Select the user for which to change the password options and click *Edit*.
3. Switch to the *Password Settings* tab. The user's last password change is displayed on the tab.
4. To make the user change his password at next login, activate *Force Password Change*.
5. To enforce password rotation, set a *Maximum Number of Days for the Same Password* and a *Minimum Number of Days for the Same Password*.
6. To remind the user to change his password before it expires, set the 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 the complete account. Enter the *Expiration Date* in YYYY-MM-DD format. Note that this setting is not password-related but rather applies to the account itself.
9. For more information about the options and about the default values, click *Help*.
10. Apply your changes with *OK*.

11.3.3 Managing Encrypted Home Directories

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

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 *Book “Security Guide”, Chapter 11 “Encrypting Partitions and Files”, Section 11.2 “Using Encrypted Home Directories”*.

PROCEDURE 11.4: 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.

The screenshot shows the 'Existing Local User' dialog box with the 'Details' tab selected. The 'User ID (uid)' field contains '1000'. The 'Home Directory' field contains '/home/tux' with a 'Browse...' button next to it. Below this, the 'Move to New Location' checkbox is checked. The 'Use Encrypted Home Directory' checkbox is also checked, and the 'Directory Size in MB' spinner is set to '100'. To the right, the 'Additional Groups' list is visible, showing various system groups like 'users', 'at', 'audio', etc., with 'users' selected. At the bottom, the 'Login Shell' is set to '/bin/bash' and the 'Default Group' is 'users'. Buttons for 'Help', 'Cancel', and 'OK' are at the bottom.

4. Apply your settings with *OK*.
5. Enter the user's current login password to proceed if YaST prompts for it.
6. Click *OK* to close the administration dialog and save the changes.
Alternatively, if you want to save all changes without exiting the *User and Group Administration* dialog, click *Expert Options > Write Changes Now*.

PROCEDURE 11.5: MODIFYING OR DISABLING ENCRYPTED HOME DIRECTORIES

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

1. Open the YaST *User and Group Administration* dialog in the *Users* view.
2. Select a user from the list and click *Edit*.

3. If you want to disable the encryption, switch to the *Details* tab and disable *Use Encrypted Home Directory*.
If you need to enlarge or reduce the size of the encrypted image file for this user, change the *Directory Size in MB*.
4. Apply your settings with *OK*.
5. Enter the user's current login password to proceed if YaST prompts for it.
6. Click *OK* to close the administration dialog and save the changes.
Alternatively, if you want to save all changes without exiting the *User and Group Administration* dialog, click *Expert Options > Write Changes Now*.

11.3.4 Managing Quotas

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

SUSE Linux Enterprise Desktop allows usage of soft and hard quotas. Additionally, grace intervals can be defined that allow users or groups to temporarily violate their quotas by certain amounts.

Soft Quota

Defines a warning level at which users are informed that they are nearing their limit. Administrators will urge the users to clean up and reduce their data on the partition. The soft quota limit is usually lower than the hard quota limit.

Hard Quota

Defines the limit at which write requests are denied. When the hard quota is reached, no more data can be stored and applications may crash.

Grace Period

Defines the time between the overflow of the soft quota and a warning being issued. Usually set to a rather low value of one or several hours.

PROCEDURE 11.6: ENABLING QUOTA SUPPORT FOR A PARTITION

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

1. In YaST, select *System > Partitioner* and click *Yes* to proceed.
2. In the *Expert Partitioner*, select the partition for which to enable quotas and click *Edit*.
3. Click *Fstab Options* and activate *Enable Quota Support*. If the `quota` package is not already installed, it will be installed once you confirm the respective message with *Yes*.
4. Confirm your changes and leave the *Expert Partitioner*.
5. Make sure the service `quotaon` is running by entering the following command:

```
systemctl status quotaon
```

It should be marked as being active. If this is not the case, start it with the command **`systemctl start quotaon`**.

PROCEDURE 11.7: SETTING UP QUOTAS FOR USERS OR GROUPS

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

1. In the YaST *User and Group Administration*, select the user or the group you want to set the quotas for and click *Edit*.
2. On the *Plug-Ins* tab, select the *Manage User Quota* entry and click *Launch* to open the *Quota Configuration* dialog.
3. From *File System*, select the partition to which the quota should apply.

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 text boxes 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 *OK* to close the administration dialog and save the changes.

Alternatively, if you want to save all changes without exiting the *User and Group Administration* dialog, click *Expert Options* > *Write Changes Now*.

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.

11.4 Changing Default Settings for Local Users

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

1. Open the YaST *User and Group Administration* dialog and select the *Defaults for New Users* tab.
2. To change the primary group the new users should automatically belong to, select another group from *Default Group*.
3. To modify the secondary groups for new users, add or change groups in *Secondary Groups*. The group names must be separated by commas.
4. If you do not want to use `/home/username` as default path for new users' home directories, modify the *Path Prefix for Home Directory*.
5. To change the default permission modes for newly created home directories, adjust the umask value in *Umask for Home Directory*. For more information about umask, refer to Book “Security Guide”, Chapter 10 “Access Control Lists in Linux” and to the `umask` man page.
6. For information about the individual options, click *Help*.
7. Apply your changes with *OK*.

11.5 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 11.4, “Changing Default Settings for Local Users”](#).

PROCEDURE 11.8: CHANGING A USER'S GROUP ASSIGNMENT

1. Open the YaST *User and Group Administration* dialog and click the *Users* tab. It lists users and the groups the users belong to.

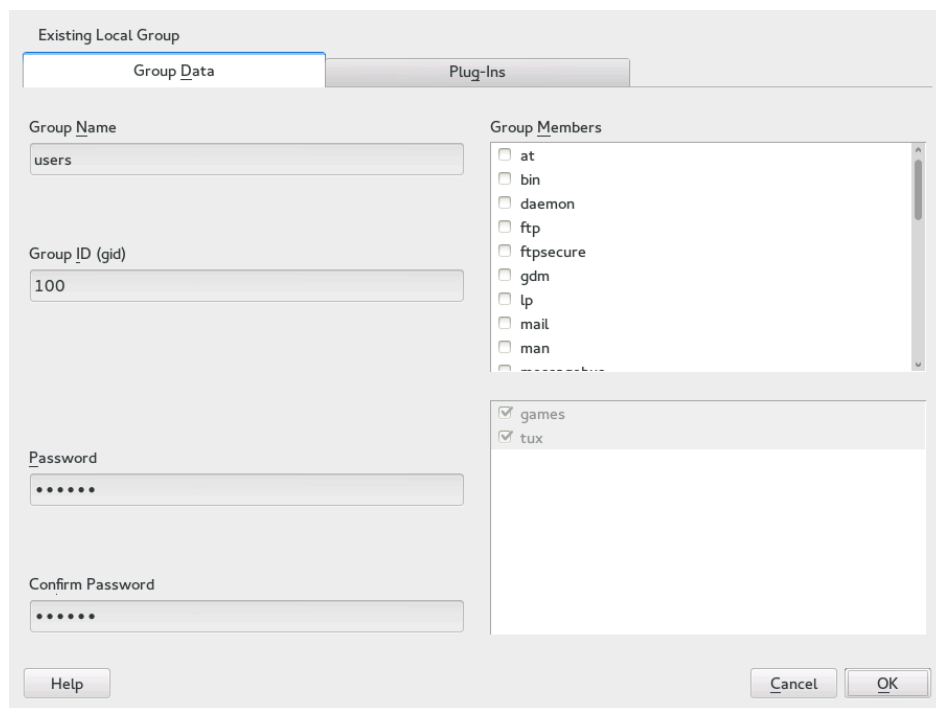
2. Click *Edit* and switch to the *Details* tab.
3. To change the primary group the user belongs to, click *Default Group* and select the group from the list.
4. To assign the user additional secondary groups, activate the corresponding check boxes in the *Additional Groups* list.
5. Click *OK* to apply your changes.
6. Click *OK* to close the administration dialog and save the changes.
Alternatively, if you want to save all changes without exiting the *User and Group Administration* dialog, click *Expert Options* › *Write Changes Now*.

11.6 Managing Groups

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

PROCEDURE 11.9: 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 lists 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.



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 deactivate the box.
7. Click *OK* to apply your changes.
8. Click *OK* to close the administration dialog and save the changes.
Alternatively, if you want to save all changes without exiting the *User and Group Administration* dialog, click *Expert Options > Write Changes Now*.

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

11.7 Changing the User Authentication Method

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

NIS

Users are administered centrally on a NIS server for all systems in the network. For details, see *Book “Security Guide”, Chapter 3 “Using NIS”*.

LDAP

Users are administered centrally on an LDAP server for all systems in the network. For details about LDAP, see *Book “Security Guide”, Chapter 5 “LDAP—A Directory Service”*.

You can manage LDAP users with the YaST user module. All other LDAP settings, including the default settings for LDAP users, need to be defined with the YaST LDAP client module as described in *Book “Security Guide”, Chapter 4 “Setting Up Authentication Servers and Clients Using YaST”, Section 4.1 “Configuring an Authentication Server”*.

Kerberos

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

Samba

SMB authentication is often used in mixed Linux and Windows networks. For details, see *Book “Administration Guide”, Chapter 25 “Samba”* and *Book “Security Guide”, Chapter 6 “Active Directory Support”*.

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: *Book “Security Guide”, Chapter 3 “Using NIS”, Section 3.2 “Configuring NIS Clients”*

LDAP: *Book “Security Guide”, Chapter 4 “Setting Up Authentication Servers and Clients Using YaST”, Section 4.1 “Configuring an Authentication Server”*

Samba: *Book “Administration Guide”, Chapter 25 “Samba”, Section 25.4.1 “Configuring a Samba Client with YaST”*

4. After accepting the configuration, return to the *User and Group Administration* overview.
5. Click *OK* to close the administration dialog.

12 Changing Language and Country Settings with YaST

Working in different countries or having to work in a multilingual environment requires your computer to be set up to support this. SUSE® Linux Enterprise Desktop can handle different locales in parallel. A locale is a set of parameters that defines the language and country settings reflected in the user interface.

The main system language was selected during installation and keyboard and time zone settings were adjusted. However, you can install additional languages on your system and determine which of the installed languages should be the default.

For those tasks, use the YaST language module as described in *Section 12.1, “Changing the System Language”*. Install secondary languages to get optional localization if you need to start applications or desktops in languages other than the primary one.

Apart from that, the YaST timezone module allows you to adjust your country and timezone settings accordingly. It also lets you synchronize your system clock against a time server. For details, refer to *Section 12.2, “Changing the Country and Time Settings”*.

12.1 Changing the System Language

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

Changing the System Language Globally

Proceed as described in *Section 12.1.1, “Modifying System Languages with YaST”* and *Section 12.1.2, “Switching the Default System Language”* to install additional localized packages with YaST and to set the default language. Changes are effective after the next login. To ensure that the entire system reflects the change, reboot the system or close and restart all running services, applications, and programs.

Changing 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. Refer to *Book “GNOME User Guide”, Chapter 3 “Customizing Your Settings”, Section 3.2.2 “Configuring Language Settings”* for details. After the

X server 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 Switching Languages for One Application Only

You can also run a single application in another language (that has already been installed with YaST). To do so, start it from the command line by specifying the language code as described in [Section 12.1.3, “Switching Languages for Standard X and GNOME Applications”](#).

12.1.1 Modifying System Languages with YaST

YaST knows two different language categories:

Primary Language

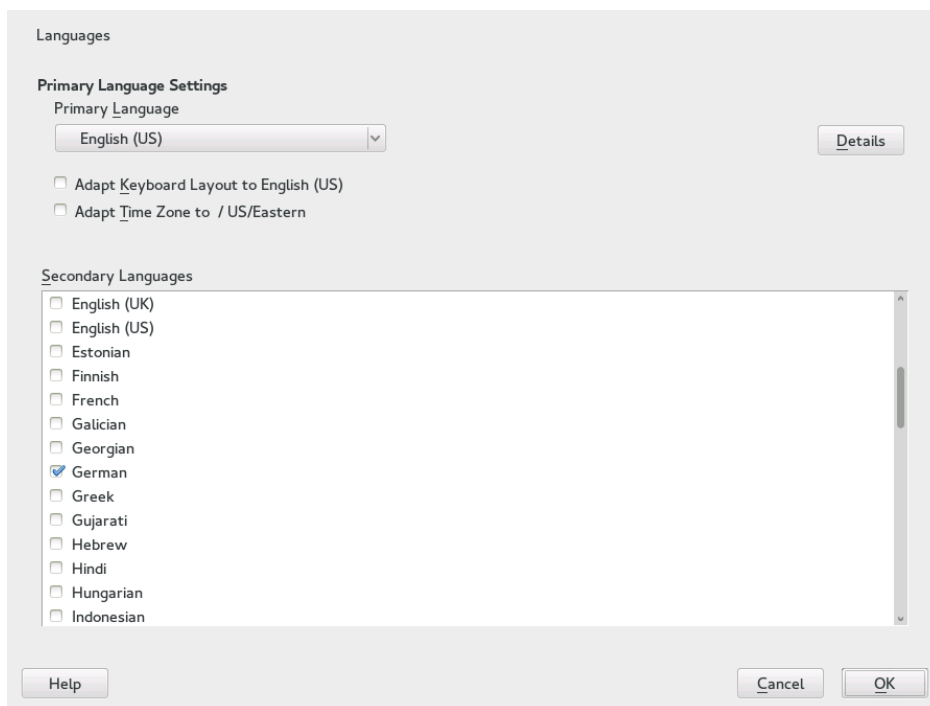
The primary language set in YaST applies to the entire system, including YaST and the desktop environment. This language is used whenever available unless you manually specify another language.

Secondary Languages

Install secondary languages to make your system multilingual. Languages installed as secondary languages can be selected manually for a specific situation. For example, use a secondary language to start an application in a certain language to do word processing in this language.

Before installing additional languages, determine which of them should be the default system language (primary language).

To access the YaST language module, start YaST and click *System > Language*. Alternatively, start the *Languages* dialog directly by running `sudo yast2 language &` from a command line.



PROCEDURE 12.1: INSTALLING ADDITIONAL LANGUAGES

When installing additional languages, YaST also allows you to set different locale settings for the user `root`, see [Step 4](#). The option *Locale Settings for User root* determines how the locale variables (`LC_*`) in the file `/etc/sysconfig/language` are set for `root`. You can either set them to the same locale as for normal users, keep it unaffected by any language changes or only set the variable `LC_CTYPE` to the same values as for the normal users. This variable sets the localization for language-specific function calls.

1. To add additional languages in the YaST language module, select the *Secondary Languages* you want to install.
2. To make a language the default language, set it as *Primary Language*.
3. Additionally, adapt the keyboard to the new primary language and adjust the time zone, if appropriate.



Tip: Advanced Settings

For advanced keyboard or time zone settings, select *Hardware > System Keyboard Layout* or *System > Date and Time* in YaST to start the respective dialogs. For more information, refer to [Section 6.1, “Setting Up Your System Keyboard Layout”](#) and [Section 12.2, “Changing the Country and Time Settings”](#).

4. To change language settings specific to the user `root`, click *Details*.
 - a. Set *Locale Settings for User root* to the desired value. For more information, click *Help*.
 - b. Decide if you want to *Use UTF-8 Encoding* for `root` or not.
5. If your locale was not included in the list of primary languages available, try specifying it with *Detailed Locale Setting*. However, some localization may be incomplete.
6. Confirm your changes in the dialogs with *OK*. If you have selected secondary languages, YaST installs the localized software packages for the additional languages.

The system is now multilingual. However, to start an application in a language other than the primary one, you need to set the desired language explicitly as explained in [Section 12.1.3, “Switching Languages for Standard X and GNOME Applications”](#).

12.1.2 Switching the Default System Language

1. To globally switch the default system language, start the YaST language module.
2. Select the desired new system language as *Primary Language*.



Important: Deleting Former System Languages

If you switch to a different primary language, the localized software packages for the former primary language will be removed from the system. To switch the default system language but keep the former primary language as additional language, add it as *Secondary Language* by enabling the respective check box.

3. Adjust the keyboard and time zone options as desired.
4. Confirm your changes with *OK*.
5. After YaST has applied the changes, restart any X sessions (for example, by logging out and logging in again) to make YaST and the desktop applications reflect your new language settings.

12.1.3 Switching Languages for Standard X and GNOME Applications

After you have installed the respective language with YaST, you can run a single application in another language.

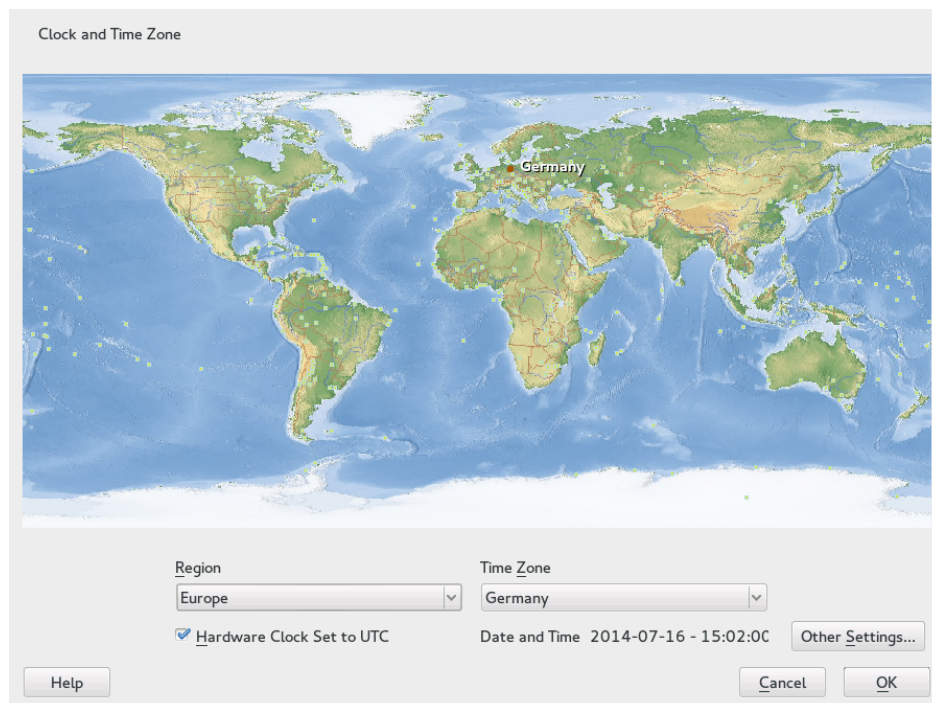
Start the application from the command line by using the following command:

```
LANG=language application
```

For example, to start f-spot in German, run **LANG=de_DE f-spot**. For other languages, use the appropriate language code. Get a list of all language codes available with the **locale -av** command.

12.2 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. To access the YaST module, start YaST and click *System > Date and Time*. Alternatively, start the *Clock and Time Zone* dialog directly by running **sudo yast2 timezone &** from a command line.



First, select a general region, such as *Europe*. Choose an appropriate country 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, deactivate *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.



Important: Set the Hardware Clock to UTC

The switch from standard time to daylight saving time (and vice versa) can only be performed automatically when the hardware clock (CMOS clock) is set to UTC. This also applies if you use automatic time synchronization with NTP, because automatic synchronization will only be performed if the time difference between the hardware and system clock is less than 15 minutes.

Since a wrong system time can cause severe problems (missed backups, dropped mail messages, mount failures on remote file systems, etc.) it is strongly recommended to *always* set the hardware clock to UTC.

You can change the date and time manually or opt for synchronizing your machine against an NTP server, either permanently or only for adjusting your hardware clock.

PROCEDURE 12.2: MANUALLY ADJUSTING TIME AND DATE

1. In the YaST timezone module, click *Other Settings* to set date and time.
2. Select *Manually* and enter date and time values.
3. Confirm your changes.

PROCEDURE 12.3: SETTING DATE AND TIME WITH NTP SERVER

1. Click *Other Settings* to set date and time.
2. Select *Synchronize with NTP Server*.

3. Enter the address of an NTP server, if not already populated.

Change Date and Time

☐ Manually

Current Time
15:02:29

Current Date
2014-07-16

☒ Change the Time Now

☒ Synchronize with NTP Server

NTP Server Address
de.pool.ntp.org

Synchronize now

☐ Run NTP as daemon

☒ Save NTP Configuration

Configure...

Help Cancel Accept

4. Click *Synchronize Now* to get your system time set correctly.
5. To use NTP permanently, enable *Save NTP Configuration*.
6. With the *Configure* button, you can open the advanced NTP configuration. For details, see Book “Administration Guide”, Chapter 23 “Time Synchronization with NTP”, Section 23.1 “Configuring an NTP Client with YaST”.
7. Confirm your changes.

V Updating and Upgrading SUSE Linux Enterprise

- 13 Life Cycle and Support **168**
- 14 Upgrading SUSE Linux Enterprise **178**
- 15 Service Pack Migration **197**
- 16 Backporting Source Code **206**

13 Life Cycle and Support

If you are not familiar with SUSE Linux Enterprise updates, upgrades and service packs in general, this chapter will give you some background information on terminology, SUSE product lifecycles and Service Pack releases, and recommended upgrade policies.

13.1 Terminology

This section uses several terms. To understand the information, read the definitions below:

Backporting

Backporting is the act of adapting specific changes from a newer version of software and applying it to an older version. The most commonly used case is fixing security holes in older software components. Usually it is also part of a maintenance model to supply enhancements or (less commonly) new features.

Delta RPM

A delta RPM consists only of the binary diff between two defined versions of a package, and therefore has the smallest download size. Before being installed, the full RPM package is rebuilt on the local machine.

Downstream

A metaphor of how software is developed in the open source world (compare it with *upstream*). The term *downstream* refers to people or organizations like SUSE who integrate the source code from upstream with other software to build a distribution which is then used by end users. Thus, the software flows downstream from its developers via the integrators to the end users.

Extensions,

Add-On Products

Extensions and third party add-on products provide additional functionality of product value to SUSE Linux Enterprise Desktop. They are provided by SUSE and by SUSE partners, and they are registered and installed on top of the base product SUSE Linux Enterprise Desktop.

Major Release,

General Availability (GA) Version

The Major Release of SUSE Linux Enterprise (or any software product) is a new version which brings new features and tools, decommissions previously deprecated components and comes with backward-incompatible changes.

Migration

Updating to a Service Pack (SP) by using the online update tools or an installation medium to install the respective patches. It updates all packages of the installed system to the latest state.

Migration Targets

Set of compatible products to which a system can be migrated, containing the version of the products/extensions and the URL of the repository. Migration targets can change over time and depend on installed extensions. Multiple migration targets can be selected, for example SLE 12 SP2 and SES2 or SLE 12 SP2 and SES3.

Modules

Modules are fully supported parts of SUSE Linux Enterprise Desktop with a different life cycle. They have a clearly defined scope and are delivered via online channel only. Registering at the SUSE Customer Center, SMT (Subscription Management Tool), or SUSE Manager is a prerequisite for being able to subscribe to these channels.

Package

A package is a compressed file in rpm format that contains all files for a particular program, including optional components like configuration, examples, and documentation.

Patch

A patch consists of one or more packages and may be applied by means of delta RPMs. It may also introduce dependencies to packages that are not installed yet.

Service Packs (SP)

Combines several patches into a form that is easy to install or deploy. Service packs are numbered and usually contain security fixes, updates, upgrades, or enhancements of programs.

Upstream

A metaphor of how software is developed in the open source world (compare it with *downstream*). The term *upstream* refers to the original project, author or maintainer of a software that is distributed as source code. Feedback, patches, feature enhancements, or other improvements flow from end users or contributors to upstream developers. They decide if the request will be integrated or rejected.

If the project members decide to integrate the request, it will show up in newer versions of the software. An accepted request will benefit all parties involved.

If a request is not accepted, it may be for different reasons. Either it is in a state that is not compliant with the project's guidelines, it is invalid, it is already integrated, or it is not in the interest or roadmap of the project. An unaccepted request makes it harder for upstream developers as they need to synchronize their patches with the upstream code. This practice is generally avoided, but sometimes it is still needed.

Update

Installation of a newer *minor* version of a package, which usually contains security or bug fixes.

Upgrade

Installation of a newer *major* version of a package or distribution, which brings *new features*.

13.2 Product Life Cycle

SUSE has the following life cycle for products:

- SUSE Linux Enterprise Server has a 13-year life-cycle: 10 years of general support and 3 years of extended support.
- SUSE Linux Enterprise Desktop has a 10-year life-cycle: 7 years of general support and 3 years of extended support.
- Major releases are made every 4 years. Service packs are made every 12-14 months.

SUSE supports previous service packs for 6 months after the release of the new service pack.

Figure 13.1, "Major Releases and Service Packs" depicts some mentioned aspects.

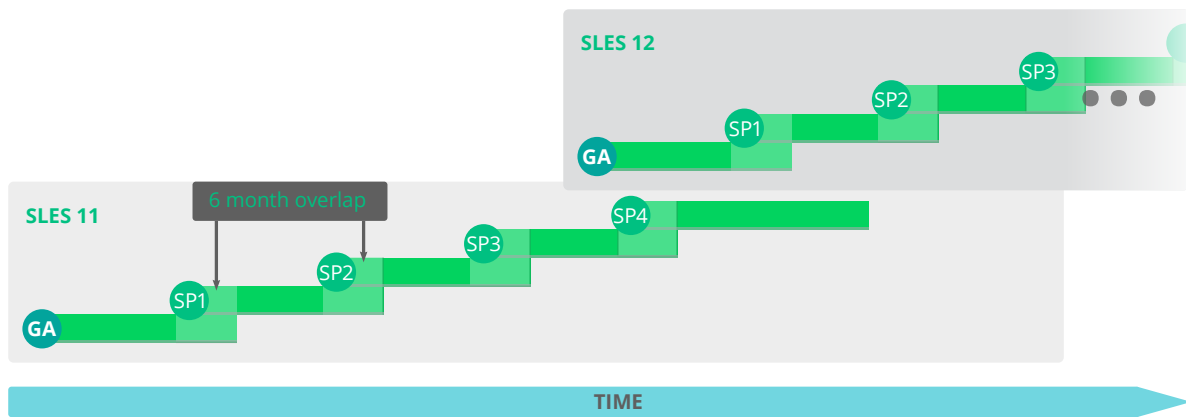


FIGURE 13.1: MAJOR RELEASES AND SERVICE PACKS

If you need additional time to design, validate and test your upgrade plans, Long Term Service Pack Support can extend the support you get by an additional 12 to 36 months in 12-month increments, giving you a total of between 2 and 5 years of support on any service pack (see *Figure 13.2, “Long Term Service Pack Support”*).

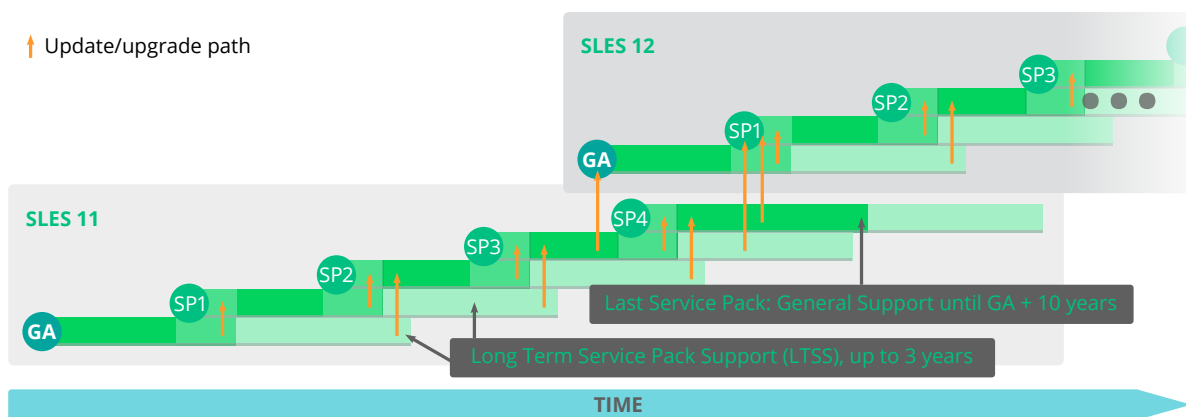


FIGURE 13.2: LONG TERM SERVICE PACK SUPPORT

For more information refer to <https://www.suse.com/products/long-term-service-pack-support/>.

13.3 Support Levels

The range for extended support levels starts from year 10 and ends in year 13. These contain continued L3 engineering level diagnosis and reactive critical bug fixes. These support levels proactively update trivial local root exploits in Kernel or other root exploits directly executable

without user interaction. Furthermore they support existing workloads, software stacks, and hardware with limited package exclusion list. Find an overview in [Table 13.1, “Security Updates and Bug Fixes”](#).

TABLE 13.1: SECURITY UPDATES AND BUG FIXES

| | General Support for Most Recent Service Pack (SP) | | | General Support for Previous SP, with LTSS | Extended Support with LTSS |
|--|---|----------|--|--|----------------------------|
| Feature | Year 1-5 | Year 6-7 | Year 8-10 | Year 4-10 | Year 10-13 |
| Technical Services | Yes | Yes | Yes | Yes | Yes |
| Access to Patches and Fixes | Yes | Yes | Yes | Yes | Yes |
| Access to Documentation and Knowledge Base | Yes | Yes | Yes | Yes | Yes |
| Support for Existing Stacks and Workloads | Yes | Yes | Yes | Yes | Yes |
| Support for New Deployments | Yes | Yes | Limited (Based on partner and customer requests) | Limited (Based on partner and customer requests) | No |

| | General Support for Most Recent Service Pack (SP) | | | General Support for Previous SP, with LTSS | Extended Support with LTSS |
|--|---|---|---|---|----------------------------|
| Feature | Year 1-5 | Year 6-7 | Year 8-10 | Year 4-10 | Year 10-13 |
| Enhancement Requests | Yes | Limited (Based on partner and customer requests) | Limited (Based on partner and customer requests) | No | No |
| Hardware Enablement and Optimization | Yes | Limited (Based on partner and customer requests) | Limited (Based on partner and customer requests) | No | No |
| Driver updates via SUSE Solid-Driver Program (formerly PLDP) | Yes | Yes | Limited (Based on partner and customer requests) | Limited (Based on partner and customer requests) | No |
| Backport of Fixes from recent SP | Yes | Yes | Limited (Based on partner and customer requests) | N/A | N/A |
| Critical Security Updates | Yes | Yes | Yes | Yes | Yes |

| | General Support for Most Recent Service Pack (SP) | | | General Support for Previous SP, with LTSS | Extended Support with LTSS |
|-------------------|---|----------|---|---|---|
| Feature | Year 1-5 | Year 6-7 | Year 8-10 | Year 4-10 | Year 10-13 |
| Defect Resolution | Yes | Yes | Limited (Severity Level 1 and 2 defects only) | Limited (Severity Level 1 and 2 defects only) | Limited (Severity Level 1 and 2 defects only) |

13.4 Repository Model

The repository layout corresponds to the product lifecycles. *Table 13.2, “Repository Layout for SUSE Linux Enterprise 11 SP3/SP4 and for SUSE Linux Enterprise 12 SP1”* contains a list of all relevant repositories.

TABLE 13.2: REPOSITORY LAYOUT FOR SUSE LINUX ENTERPRISE 11 SP3/SP4 AND FOR SUSE LINUX ENTERPRISE 12 SP1

| Type | SLES | SLED |
|-----------------------|---------------------------|---------------------------|
| Required Repositories | 11 SP3 | 11 SP3 |
| | <u>SLES11-SP3-Pool</u> | <u>SLED11-SP3-Pool</u> |
| | <u>SLES11-SP3-Updates</u> | <u>SLED11-SP3-Updates</u> |
| | 11 SP4 | 11 SP4 |
| | <u>SLES11-SP4-Pool</u> | <u>SLED11-SP4-Pool</u> |
| | <u>SLES11-SP4-Updates</u> | <u>SLED11-SP4-Updates</u> |
| | 12 | 12 |
| | <u>SLES12-GA-Pool</u> | <u>SLED12-GA-Pool</u> |
| | <u>SLES12-GA-Updates</u> | <u>SLED12-GA-Updates</u> |
| | 12 SP1 | 12 SP1 |
| | <u>SLES12-SP1-Pool</u> | <u>SLED12-SP1-Pool</u> |

| Type | SLES | SLED |
|------------------------------|--|--|
| | <u>SLES12-SP1-Updates</u> 12 SP2 <u>SLES12-SP2-Pool</u> <u>SLES12-SP2-Updates</u> | <u>SLED12-SP1-Updates</u> 12 SP2 <u>SLED12-SP2-Pool</u> <u>SLED12-SP2-Updates</u> |
| Optional Repositories | 11 SP3 <u>SLES11-SP3-Debuginfo-Core</u> <u>SLES11-SP3-Debuginfo-Updates</u> <u>SLES11-SP3-Extension-Store</u> <u>SLES11-Extra</u> 12 <u>SLES12-GA-Debuginfo-Core</u> <u>SLES12-GA-Debuginfo-Updates</u> 12 SP1 <u>SLES12-SP1-Debuginfo-Core</u> <u>SLES12-SP1-Debuginfo-Updates</u> 12 SP2 <u>SLES12-SP2-Debuginfo-Core</u> <u>SLES12-SP2-Debuginfo-Updates</u> | 11 SP3 <u>SLED11-SP3-Debuginfo-Core</u> <u>SLED11-SP3-Debuginfo-Updates</u> <u>SLED11-SP3-Extension-Store</u> <u>SLED11-Extra</u> 12 <u>SLED12-GA-Debuginfo-Core</u> <u>SLED12-GA-Debuginfo-Updates</u> 12 SP1 <u>SLED12-SP1-Debuginfo-Core</u> <u>SLED12-SP1-Debuginfo-Updates</u> 12 SP2 <u>SLED12-SP2-Debuginfo-Core</u> <u>SLED12-SP2-Debuginfo-Updates</u> |
| Module Specific Repositories | 12/12 SP1/12 SP2 <u>sle-module-adv-systems-management</u> <u>sle-module-certification</u> (<i>Not available on AArch64.</i>) <u>sle-module-containers</u> <u>sle-module-legacy</u> (<i>Not available on AArch64.</i>) <u>sle-module-public-cloud</u> <u>sle-module-web-scripting</u> | 12/12 SP1/12 SP2 Currently, there are no modules for SLED. |

DESCRIPTION OF REQUIRED REPOSITORIES

Updates

Maintenance updates to packages in the corresponding Core or Pool repository.

Pool

Containing all binary RPMs from the installation media, plus pattern information and support status metadata.

DESCRIPTION OF OPTIONAL REPOSITORIES

Debuginfo-Pool,

Debuginfo-Updates

These repositories contain static content. Of these two, only the Debuginfo-Updates repository receives updates. Enable these repositories if you need to install libraries with debug information in case of an issue.

13.4.1 Origin of Packages

SUSE Linux Enterprise 11 SP3/SP4. With the update to SP3 there are only two repositories available: SLED11-SP3-Pool and SLED11-SP3-Updates. Since SP4, any previous repositories are not visible anymore.

SUSE Linux Enterprise 12 and SP1/SP2. With the update to SUSE Linux Enterprise 12 there are only two repositories available: SLED12-GA-Pool and SLED12-GA-Updates. Any previous repositories from SUSE Linux Enterprise 11 are disabled.

13.4.2 Register and Unregister Repositories with SUSEConnect

On registration, the system receives repositories from the SUSE Customer Center (see <https://scc.suse.com/>) or a local registration proxy like SMT. The repository names map to specific URIs in the customer center. To list all available repositories on your system, use zypper as follows:

```
root # zypper repos -u
```

This gives you a list of all available repositories on your system. Each repository is listed by its alias, name and whether it is enabled and will be refreshed. The option `-u` gives you also the URI from where it originated.

To register your machine, run `SUSEConnect`, for example:

```
root # SUSEConnect -r REGCODE
```

If you want to unregister your machine, from SP1 and above you can use `SUSEConnect` too:

```
root # SUSEConnect --de-register
```

To check your locally installed products and their status, use the following command:

```
root # SUSEConnect -s
```

13.4.3 IBM POWER: Starting an X-Server

On SLES 12 for IBM POWER the display manager is configured not to start a local X-Server by default. This setting was reversed on SLES 12 SP1—the display manager now starts an X-Server.

To avoid problems during upgrade, the SLE-12 setting is not changed automatically. If you want the display manager to start an X-Server after the upgrade, change the setting of `DISPLAYMANAGER_STARTS_XSERVER` in `/etc/sysconfig/displaymanager` as follows:

```
DISPLAYMANAGER_STARTS_XSERVER="yes"
```

14 Upgrading SUSE Linux Enterprise

SUSE® Linux Enterprise (SLE) allows to update an existing system to the new version, for example, going from SLE 11 SP4 to SLE 12. No new installation is needed. Existing data, such as home and data directories and system configuration, is kept intact. You can update from a local CD or DVD drive or from a central network installation source.

This chapter explains how to manually upgrade your SUSE Linux Enterprise system, be it by DVD, network, an automated process, or SUSE Manager.

14.1 General Preparations

Before starting the update procedure, make sure your system is properly prepared. Among others, preparation involves backing up data and checking the release notes.

14.1.1 Temporarily Disable Kernel Multiversion Support

SUSE Linux Enterprise Desktop allows to install multiple Kernel versions by enabling the respective settings in `/etc/zypp/zypp.conf`. Support for this feature needs to be temporarily disabled for updating to a service pack. When the update has successfully finished; multiversion support can be re-enabled again. To disable multiversion support, comment the respective lines in `/etc/zypp/zypp.conf`. The result should look like this:


```
#multiversion = provides:multiversion(kernel)
#multiversion.kernels = latest,running
```

To re-activate this feature after a successful update, remove the comment signs. For more information about multiversion support, refer to [Section 10.1, “Enabling and Configuring Multiversion Support”](#).

14.1.2 Check the Release Notes

In the release notes you can find additional information on what has changed since the previous release of SUSE Linux Enterprise. Verify there if your specific hardware or setup needs special considerations, which of your favorite specific software packages have changed significantly,

and which precautions you should take in addition to the general recommendations of this section. The release notes also provide last-minute information and known issues that could not make it to the manual on time.

The current version of the release notes document containing the latest information on SUSE Linux Enterprise Desktop can be read online at <http://www.suse.com/documentation/> .

14.1.3 Make a Backup

Before updating, copy existing configuration files to a separate medium (such as tape device, removable hard disk, etc.) to back up the data. This primarily applies to files stored in /etc and some 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 permissions for all local files.

If you have selected *Update an Existing System* as the installation mode in YaST, you can choose to do a (system) backup at a later point in time. You can choose to include all modified files and files from the /etc/sysconfig directory. However, this is not a complete backup, as all the other important directories mentioned above are missing. Find the backup in the /var/adm/backup directory.


14.1.4 Migrate your MySQL Database

As of SUSE Linux Enterprise 12, SUSE switched from MySQL to MariaDB. Before you start any upgrade, it is highly recommended to back up your database.

To perform the database migration, do the following:

1. Log in to your SUSE Linux Enterprise 11 machine.
2. Create a dump file:

```
root # mysqldump -u root -p --all-databases > mysql_backup.sql
```

By default, mysqldump does not dump the INFORMATION_SCHEMA or performance_schema database. For more details refer to <https://dev.mysql.com/doc/refman/5.5/en/mysqldump.html> .

3. Store your dump file, the configuration file /etc/my.cnf, and the directory /etc/mysql/ for later investigation (*NOT* installation!) in a safe place.
4. Perform your upgrade. After the upgrade, your former configuration file /etc/my.cnf is still intact. You can find the new configuration in the file /etc/my.cnf.rpmnew.
5. Configure your MariaDB database to your needs. Do *NOT* use the former configuration file and directory, but use it as a reminder and adapt it.
6. Make sure you start the MariaDB server:

```
root # systemctl start mysql
```

If you want to start the MariaDB server on every boot, enable the service:

```
root # systemctl enable mysql
```

7. Verify that MariaDB is running properly by connecting to the database:

```
root # mysql -u root -p
```

14.1.5 Migrate your PostgreSQL Database

SLE11 SP3 and SLE12 GA get a newer version of the PostgreSQL database as a maintenance update. Because of the required migration work of the database, there is no automatic upgrade process. As such, the switch from one version to another needs to be done manually.

The migration process is conducted by the pg_upgrade command which is an alternative method of the classic dump and reload. In comparison with the “dump & reload” method, pg_upgrade makes the migration less time-consuming.

Each PostgreSQL version stores its files in different, version-dependent directories. After the update the directories will change to:

SLE11 SP3/SP4

/usr/lib/postgresql91/ to /usr/lib/postgresql94/

SLE12 GA

/usr/lib/postgresql93/ to /usr/lib/postgresql94/

To perform the database migration, do the following:

1. Make sure the following preconditions are fulfilled:

- If not already done, upgrade any package of the old PostgreSQL version to the latest release through a maintenance update.
- Create a backup of your existing database.
- Install the packages of the new PostgreSQL major version. For SLE12 this means to install `postgresql94-server` and all the packages it depends on.
- Install the package `postgresql94-contrib` which contains the command `pg_upgrade`.
- Make sure you have enough free space in your PostgreSQL data area, which is `/var/lib/pgsql/data` by default. If space is tight, try to reduce size with the following SQL command on each database (can take very long!):

```
VACUUM FULL
```

2. Stop the PostgreSQL server:

```
root # /usr/sbin/rcpostgresql stop
```

3. Rename your old data directory:

```
root # mv /var/lib/pgsql/data /var/lib/pgsql/data.old
```

4. Create a new data directory:

```
root # mkdir -p /var/lib/pgsql/data
```

5. If you have changed your configuration files in the old version, copy the files `postgresql.conf` `pg_hba.conf` to your new `data` directory:

```
root # cp /var/lib/pgsql/data.old/*.conf \  
/var/lib/pgsql/data
```

6. Initialize your new database instance either manually with `initdb` or by starting and stopping PostgreSQL, which will do it automatically:

```
root # /usr/sbin/rcpostgresql start  
root # /usr/sbin/rcpostgresql stop
```

7. Start the migration process and replace the OLD placeholder with the older version:

```
root # pg_upgrade \  
  --old-datadir "/var/lib/pgsql/data.old" \  
  --new-datadir "/var/lib/pgsql/data" \  
  --old-bindir "/usr/lib/postgresqlOLD/bin/" \  
  --new-bindir "/usr/lib/postgresql94/bin/"
```

8. Start your new database instance:

```
root # /usr/sbin/rcpostgresql start
```

9. Check if the migration was successful. There is no general tool to automate this step. It depends on your use case how much and what you want to test.

10. Remove any old PostgreSQL packages and your old data directory:

```
root # zypper search -s postgresqlOLD | xargs zypper rm -u  
root # rm -rf /var/lib/pgsql/data.old
```

14.1.6 Create Non-MD5 Server Certificates for Java Applications

During the update from SP1 to SP2, MD5-based certificates were disabled as part of a security fix. If you have certificates created as MD5, recreate your certificates with the following steps:

1. Open a terminal and log in as root.
2. Create a private key:

```
root # openssl genrsa -out server.key 1024
```

If you want a stronger key, exchange 1024 with a higher number, for example, 4096.

3. Create a certificate signing request (CSR):

```
root # openssl req -new -key server.key -out server.csr
```

4. Self-sign the certificate:

```
root # openssl x509 -req -days 365 -in server.csr -signkey server.key -out  
server.crt
```

5. Create the PEM file:

```
root # cat server.key server.crt > server.pem
```

6. Place the files server.crt, server.csr, server.key, and server.pem in the respective directories where the keys can be found. For Tomcat, for example, this directory is /etc/tomcat/ssl/.

14.1.7 Shut Down Virtual Machine Guests

If your machine serves as a VM Host Server for KVM or Xen, make sure to properly shut down all running VM Guests prior to the update. Otherwise you may not be able to access the guests after the update.

14.1.8 Check the **clientSetup4SMT.sh** script on SMT clients

If you are migrating your client OS that is registered against an SMT server, you need to check if the version of the clientSetup4SMT.sh script on your host is up to date. clientSetup4SMT.sh from older versions of SMT cannot manage SMT 12 clients. If you apply software patches regularly on your SMT server, you can always find the latest version of clientSetup4SMT.sh at <SMT_HOSTNAME>/repo/tools/clientSetup4SMT.sh.

14.2 Disk Space

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



Note: Automatic Check for Enough Space in YaST

During the update procedure, YaST will check the free disk space and display a warning to the user if the installation may exceed the available amount. In that case, performing the update may lead to an *unusable system*! Only if you know exactly what you are doing (by testing beforehand), you can skip the warning and continue the update.

14.2.1 Checking Disk Space on Non-Btrfs File Systems

Use the **df** command to list available disk space. For example, in *Example 14.1*, “List with **df -h**”, the root partition is /dev/sda3 (mounted as /).

EXAMPLE 14.1: 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 |

14.2.2 Checking Disk Space on Btrfs Root File Systems

If you use Btrfs as root file systems on your machine, make sure there is enough free space. Getting disk space can be done with these two commands:

```
root # btrfs filesystem df /  
root # df /
```

The results of the two commands show similar numbers of how much disk space is used. However, the problem with Btrfs and free space is that you do not know what is referenced in a snapshot and what is not; you cannot calculate how much disk space a change would need.

In the worst case, an upgrade needs as much disk space as the current root file system (without `/ . snapshot`). Besides any Btrfs file systems, check for free space on other file systems as well. The following recommendation has been proven:

- For all file systems including Btrfs you need enough free disk space to download and install big RPMs. The space of old RPMs are only freed after new RPMs are installed.
- For Btrfs with snapshots, you need at minimum as much free space as your current installation takes. It is recommended to have twice as much free space as the current installation. If you do not have enough free space, you can try to delete old snapshots with **snapper** like this:

```
root # snapper list
root # snapper delete NUMBER
```

However, this may not help in all cases. Before migration, most snapshots occupy only little space.

14.3 Supported Upgrade Paths for SLE

Important: Cross-architecture Upgrades Are Not Supported

Cross-architecture upgrades, such as upgrading from a 32-bit version of SUSE Linux Enterprise Desktop to the 64-bit version, or upgrading from big endian to little endian are *not* supported!

Specifically, SLE 11 on POWER (big endian) to SLE 12 SP1 on POWER (new: little endian!), is *not* supported.

Also, since SUSE Linux Enterprise 12 is 64-bit only, upgrades from any 32-bit SUSE Linux Enterprise 11 systems to SUSE Linux Enterprise 12 and later are *not* supported.

Before you perform any migration, read [Section 14.1, “General Preparations”](#).

Upgrading from SUSE Linux Enterprise 10 (any Service Pack)

There is no supported direct migration path to SUSE Linux Enterprise 12. A fresh installation is recommended instead.

Upgrading from SUSE Linux Enterprise 11 GA, SP1 or SP2

There is no supported direct migration path to SUSE Linux Enterprise 12. You need at least SLE 11 SP3 before you can proceed to SLE 12.

If you cannot do a fresh install, you need to first update from SLE 11 GA to SP1, then from SLE 11 SP1 to SP2, and then from SLE 11 SP2 to SP3. These steps are described in the [SUSE Linux Enterprise 11 Deployment Guide \(https://www.suse.com/documentation/sles11/\)](https://www.suse.com/documentation/sles11/).

Then proceed with *Section 14.4, “Supported Methods for Upgrading SUSE Linux Enterprise”*.

Upgrading from SUSE Linux Enterprise 11 SP3 or SP4

Refer to *Section 14.4, “Supported Methods for Upgrading SUSE Linux Enterprise”* for details.

Upgrading from SUSE Linux Enterprise 12 to SP1

Refer to *Chapter 15, Service Pack Migration* for details.

14.4 Supported Methods for Upgrading SUSE Linux Enterprise

Upgrading from SUSE Linux Enterprise 11 SP3 to SUSE Linux Enterprise 12, SUSE Linux Enterprise 11 SP3 to SUSE Linux Enterprise 12 SP1, or SUSE Linux Enterprise 11 SP4 to SUSE Linux Enterprise 12 SP1 is supported using one of the following methods:

- *Section 14.5, “Upgrading Manually from SLE 11 SP3 to SLE 12 SP1, Using an Installation Source”*
- *Section 14.6, “Migrating Automatically from SLE 11 SP3 or SP4 to SLE 12 SP1”*

14.5 Upgrading Manually from SLE 11 SP3 to SLE 12 SP1, Using an Installation Source

Before you upgrade your system, read *Section 14.1, “General Preparations”* first.

To upgrade your system this way, you need to boot from an installation source, like you would do for a fresh installation. However, when the boot screen appears, you need to select *Upgrade* (instead of *Installation*). The installation source to boot from can be one of the following:

- A local installation medium (like a DVD, or an ISO image on a USB mass storage device). For detailed instructions, see [Section 14.5.1, “Upgrading from an Installation Medium”](#).
- A network installation source. You can either boot from the local medium and then select the respective network installation type, or boot via PXE. For detailed instructions, see [Section 14.5.2, “Upgrading from a Network Installation Source”](#).

14.5.1 Upgrading from an Installation Medium

The procedure below describes booting from a DVD as an example, but you can also use another local installation medium like an ISO image on a USB mass storage device. The way to select the boot method and to start up the system from the medium depends on the system architecture and on whether the machine has a traditional BIOS or UEFI. For details, see the links below.

PROCEDURE 14.1: MANUALLY UPGRADING FROM SLE 11 SP3 TO SLE 12 SP1, USING A DVD

1. Insert DVD 1 of the SUSE Linux Enterprise 12 SP1 installation medium and boot your machine. A *Welcome* screen is displayed, followed by the boot screen.
2. Select the respective boot method to start the system from the medium (see [Section 2.1, “Choosing the Installation Method”](#)).
3. Start up the system from the medium (see [Section 2.2, “System Start-up for Installation”](#)).
4. Proceed with the upgrade process as described in [Section 14.7, “Starting the Upgrade Process After Booting”](#).

14.5.2 Upgrading from a Network Installation Source

If you want to start an upgrade from a network installation source, make sure that the following requirements are met:

REQUIREMENTS FOR UPGRADING FROM A NETWORK INSTALLATION SOURCE

Network Installation Source

A network installation source is set up according to *Chapter 3, Setting Up the Server Holding the Installation Sources*.

Network Connection and Network Services

Both the installation server and the target machine have a functioning network connection. The network must provide the following services: a name service, DHCP (optional, but needed for booting via PXE), and OpenSLP (optional).

Installation Media

You have a SUSE Linux Enterprise DVD 1 (or a local ISO image) at hand to boot the target system or a target system that is set up for booting via PXE according to *Section 4.5, “Preparing the Target System for PXE Boot”*. Refer to *Chapter 5, Remote Installation* for in-depth information on starting the upgrade from a remote server.

When upgrading from network installation source, you can either boot from the local medium and then select the respective network installation type, or boot via PXE. Select the method of your choice and proceed as described in *Procedure 14.2* or *Procedure 14.3*.

PROCEDURE 14.2: MANUALLY UPGRADING FROM SLE 11 SP3 OR SP4 TO SLE 12 SP1 VIA NETWORK INSTALLATION SOURCE—BOOTING FROM DVD

This procedure describes booting from a DVD as an example, but you can also use another local installation medium like an ISO image on a USB mass storage device. The way to select the boot method and to start up the system from the medium depends on the system architecture and on whether the machine has a traditional BIOS or UEFI. For details, see the links below.

1. Insert DVD 1 of the SUSE Linux Enterprise 12 SP1 installation media and boot your machine. A *Welcome* screen is displayed, followed by the boot screen.
2. Select the type of network installation source you want to use (FTP, HTTP, NFS, SMB, or SLP). Usually you get this choice by pressing **F4**, but in case your machine is equipped with UEFI instead of a traditional BIOS, you may need to manually adjust boot parameters. For details, see *Installing from a Network Server* in *Chapter 2, Installation with YaST*.

3. Proceed with the upgrade process as described in *Section 14.7, “Starting the Upgrade Process After Booting”*.

PROCEDURE 14.3: MANUALLY UPGRADING FROM SLE 11 SP3 OR SP4 TO SLE 12 SP1 VIA NETWORK INSTALLATION SOURCE—BOOTING VIA PXE

To perform an upgrade from a network installation source using PXE Boot, proceed as follows:

1. Adjust the setup of your DHCP server to provide the address information needed for booting via PXE. For details, see *Section 4.5, “Preparing the Target System for PXE Boot”*.
2. Set up a TFTP server to hold the boot image needed for booting via PXE. Use DVD 1 of your SUSE Linux Enterprise 12 SP1 installation media for this or follow the instructions in *Section 4.2, “Setting Up a TFTP Server”*.
3. Prepare PXE Boot and Wake-on-LAN on the target machine.
4. Initiate the boot of the target system and use VNC to remotely connect to the installation routine running on this machine. For more information, see *Section 5.3.1, “VNC Installation”*.
5. Proceed with the upgrade process as described in *Section 14.7, “Starting the Upgrade Process After Booting”*.

14.6 Migrating Automatically from SLE 11 SP3 or SP4 to SLE 12 SP1

Before you upgrade your system, read *Section 14.1, “General Preparations”* first. To perform an automated migration, proceed as follows:

PROCEDURE 14.4: AUTOMATED MIGRATION FROM SUSE LINUX ENTERPRISE 11 SP3 TO SUSE LINUX ENTERPRISE 12 SP1


1. Copy the installation Kernel `linux` and the file `initrd` from `/boot/x86_64/loader/` from your first installation DVD to your system's `/boot` directory:

```
cp -vi DVDROOT/boot/x86_64/loader/linux /boot/linux.upgrade
cp -vi DVDROOT/boot/x86_64/loader/initrd /boot/initrd.upgrade
```

`DVDROOT` denotes the path where your system mounts the DVD, usually `/run/media/$USER/$DVDNAME`.

2. Open the GRUB legacy configuration file `/boot/grub/menu.lst` and add another section. For other boot loaders, edit the respective configuration file(s). Adjust device names and the `root` parameter accordingly. For example:

```
title Linux Upgrade Kernel
kernel (hd0,0)/boot/linux.upgrade root=/dev/sda1 upgrade=1 OPTIONAL_PARAMETERS
initrd (hd0,0)/boot/initrd.upgrade
```

`OPTIONAL_PARAMETERS` denote additional boot parameters which you might need to boot your system and perform the upgrade. These may be kernel parameters needed for your system—check if you need to review and copy those from an existing GRUB entry. They also may be SUSE [linuxrc parameters, documented online](http://en.opensuse.org/Linuxrc) (<http://en.opensuse.org/Linuxrc>) .

3. If the upgrade should be done automated, add the `autoupgrade=1` to the end of the `kernel` line in your GRUB configuration.
4. Reboot your machine and select the newly added section from the boot menu (here: *Linux Upgrade Kernel*). You can use `grubonce` to preselect the newly created GRUB entry for an unattended automatic reboot into the newly created entry. You can also use `reboot` to initiate the reboot from the command line.
5. Proceed with the usual upgrade process as described in *Section 14.7, “Starting the Upgrade Process After Booting”*.
6. After the upgrade process was finished successfully, remove the installation Kernel and initrd files (`/boot/linux.upgrade` and `/boot/initrd.upgrade`). They are not needed anymore.

14.7 Starting the Upgrade Process After Booting

1. After you have booted (either from an installation medium or the network), select the *Upgrade* entry on the boot screen.



Warning: Wrong Choice May Lead to Data Loss

If you select *Installation* instead of *Upgrade*, data may be lost later. You need to be extra careful to not destroy your data partitions by doing a fresh installation, for example by repartitioning the disks (which can destroy the existing partitions) or by reformatting the data partitions (which erases all data on them).

Make sure to select *Upgrade* here.

YaST starts the installation system.

2. On the *Welcome* screen choose *Language* and *Keyboard* and accept the license agreement. Proceed with *Next*.
YaST checks your partitions for already installed SUSE Linux Enterprise systems.
3. On the *Select for Upgrade* screen, select the partition to upgrade and click *Next*.
YaST mounts the selected partition and displays all repositories that have been found on the partition that you want to upgrade.
4. On the *Previously Used Repositories* screen, adjust the status of the repositories: enable those you want to include in the upgrade process and disable any repositories that are no longer needed. Proceed with *Next*.
5. On the *Registration* screen, select whether to register the upgraded system now (by entering your registration data and clicking *Next*) or if to *Skip Registration*. For details on registering your system, see [Section 14.10, "Registering Your System"](#).
6. Review the *Installation Settings* for the upgrade, especially the *Update Options*. Choose between the following options:
 - *Only Update Installed Packages*, in which case you might miss new features shipped with the latest SUSE Linux Enterprise version.
 - *Update with Installation of New Software and Features*. Click *Select Patterns* if you want to enable or disable patterns and packages according to your wishes.



Note: Choice of Desktop

If you used KDE before upgrading to SUSE Linux Enterprise 12 (`DEFAULT_WM` in `/etc/sysconfig/windowmanager` was set to `kde*`), your desktop environment will automatically be replaced with GNOME after the upgrade. By default, the KDM display manager will be replaced with GDM.


To change the choice of desktop environment or window manager, adjust the software selection by clicking *Select Patterns*.

7. If all settings are according to your wishes, start the installation and removal procedure by clicking *Update*.
8. After the upgrade process was finished successfully, check for any “orphaned packages”. Orphaned packages are packages which belong to no active repository anymore. The following command gives you a list of these:

```
zypper packages --orphaned
```

With this list, you can decide if a package is still needed or can be uninstalled safely.

14.8 Updating via SUSE Manager

SUSE Manager is a server solution for providing updates, patches, and security fixes for SUSE Linux Enterprise clients. It comes with a set of tools and a Web-based user interface for management tasks. See <https://www.suse.com/products/suse-manager/>  for details.

14.9 Updating Registration Status After Rollback

When performing a service pack migration, it is necessary to change the configuration on the registration server to provide access to the new repositories. If the migration process is interrupted or reverted (via restoring from a backup or snapshot), the information on the registration server is inconsistent with the status of the system. This may lead to you being prevented from accessing update repositories or to wrong repositories being used on the client.

When a rollback is done via Snapper, the system will notify the registration server to ensure access to the correct repositories is set up during the boot process. If the system was restored any other way or the communication with the registration server failed for any reason (for example, because the server was not accessible because of network issues), trigger the rollback on the client manually by calling:

```
snapper rollback
```

We suggest always checking that the correct repositories are set up on the system, especially after refreshing the service using

```
zypper ref -s
```

This functionality is available in the `rollback-helper` package.

14.10 Registering Your System

If you skipped the registration step during the installation, you can register your system at any time using the *Product Registration* module in YaST.

Registering your systems has these advantages:

- Getting support
- Getting security updates and bug fixes
- Access to SUSE Customer Center

1. Start YaST and select *Software > Product Registration* to open the *Registration* dialog.
2. Provide the *E-mail* address associated with the SUSE account you or your organization uses to manage subscriptions. In case you do not have a SUSE account yet, go to the SUSE Customer Center home page (<https://scc.suse.com/>) to create one.
3. Enter the *Registration Code* you received with your copy of SUSE Linux Enterprise Desktop.
4. Proceed with *Next* to start the registration process. If one or more local registration servers are available on your network, you can choose one of them from a list. Alternatively, choose *Cancel* to ignore the local registration servers and register with the default SUSE registration server.

During the registration, the online update repositories will be added to your upgrade setup. When finished, you can choose whether to install the latest available package versions from the update repositories. This provides a clean upgrade path for all packages and ensures that SUSE Linux Enterprise Desktop is upgraded with the latest security updates available. If you choose *No*, all packages will be installed from the installation media. Proceed with *Next*.

After successful registration, YaST lists extensions, add-ons, and modules that are available for your system. To select and install them, proceed with [Section 9.1, “Installing Modules and Extensions from Online Channels”](#).

14.11 Retaining Kernel Packages

When installing a new kernel with YaST or Zypper, SUSE Linux Enterprise preserves the last two kernels and the running one. Usually this is sufficient.

However, there may be situations where you need to preserve more kernel versions, for example, for testing purposes. To enable this, SUSE Linux Enterprise supports the *multiversion kernel feature*. By enabling and configuring this feature the default behavior can be changed and configured to:

- delete an old kernel only after the system has been rebooted successfully with the new kernel
- keep a specified number of older kernels as fallback
- keep a specific kernel version

After the successful reboot, a script will compare the list of installed kernels with the settings in `/etc/zypp/zypp.conf` and delete those kernels that are no longer needed.

14.11.1 Enabling the Multiversion Kernel Feature

The default behavior is defined in the configuration file `/etc/zypp/zypp.conf`:

```
root # grep ^multiversion /etc/zypp/zypp.conf
multiversion = provides:multiversion(kernel)
multiversion.kernels = latest,latest-1,running
```

Remove any hash mark (#) before the line `multiversion` above to enable this feature (which should already be the case). The second line is used to configure *which* kernels need to be preserved. You need to enable both, otherwise the system will keep *all* kernels and it will fill up your hard disk.

The `multiversion.kernels` line can contain several keywords in different combinations and order:

latest

Keep kernel with the highest version number

latest-*N*

Keep kernel with the *N*th highest version number; *N* is a number starting from 1

running

Keep the current running kernel

oldest

Keep kernel with the lowest version number (the kernel on the released product)

oldest-*N*

Keep kernel with the *N*th lowest version number

3.12.28-4.6

Keep this exact kernel version

14.11.2 Use Case: Deleting an Old Kernel After Reboot Only

You want to make sure that an old kernel will only be deleted after the system has rebooted successfully of the new kernel.

Change the following line in `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,running
```

The previous parameters tell the system to keep the latest kernel and the running one only if they differ.

14.11.3 Use Case: Keeping Older Kernels as Fallback

You want to keep one or more kernel versions to have one or more “spare” kernels.

This use case can be useful if you need kernels for testing reasons. In case something goes wrong, for example, your machine does not boot, you still can use one or more kernel versions which are known to be good.

Change the following line in `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,latest-1,latest-2,running
```

When you reboot your system after the installation of a new kernel, the system will keep three kernels: the new and running kernel (configured as `latest,running`), the previous kernel version of the new kernel (configured as `latest-1`), and the predecessor of the previous kernel version (configured as `latest-2`).

14.11.4 Use Case: Keep a Specific Kernel Version

You make regular system updates and install new kernel versions. However, you are also compiling your own kernel version for various reasons and want to make sure that the system will keep it.

Change the following line in `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,3.12.28-4.20,running
```

When you reboot your system after the installation of a new kernel, the system will keep two kernels: the new and running kernel (configured as `latest,running`) and your self-compiled kernel (configured as `3.12.28-4.20`).

15 Service Pack Migration

SUSE offers a graphical and a command line tool to upgrade to a new service pack. These are simple command line tools, an intuitive graphical user interface, support for “rollback” of service packs, and some more. This chapter explains how to do a service pack migration step by step with these tools.

15.1 Conceptual Overview

SUSE releases new service packs for the SUSE Linux Enterprise family at regular intervals. To make it easy for customers to migrate to a new service pack and minimize downtime, SUSE supports to migrate online while the system is running.

Starting with SLE 12 SP2, YaST Wagon has been replaced by the YaST migration (GUI) and Zypper migration (command line). The following features are supported:

- System always in a defined state until the first RPM is updated
- Canceling is possible until the first RPM is updated
- Simple recovery, if there is an error
- “Rollback” via system tools; no backup/restore needed
- Use of all active repositories
- The ability to skip a service pack

15.2 Supported Software Scenarios and Product Versions

SUSE supports the following scenarios, be it offline or online:

Online

Connected through SUSE Customer Center, Subscription Management Tool (SMT), or SUSE Manager

Offline

Boot DVD, flash disk, ISO image, AutoYaST, “plain RPM” and third-party tools

Migration from the following versions are supported:

Online

SUSE Linux Enterprise 12

Offline

SUSE Linux Enterprise 11 SP3/SP4, SUSE Linux Enterprise 12

Manually/Third-Party

SUSE Linux Enterprise 12

Other migration scenarios and versions are currently **NOT** supported.

15.3 Service Pack Migration Workflow

A service pack migration can be executed by either YaST, zypper, or AutoYaST.

Before you can start a service pack migration, your system must be registered at the SUSE Customer Center. It is not possible to perform a migration with self build repositories derived from DVDs.

Regardless of the method, a service pack migration consists of the following steps:

1. Find possible migration targets on your registered systems.
2. Select one migration target.
3. Request and enable new repositories.
4. Run the migration.

The list of migration targets depends on the products you have installed and registered. If you have an extension installed for which the new SP is not yet available, it could be that no migration target is offered to you.

The list of migration targets available for your host will always be retrieved from the SUSE Customer Center and depend on products or extensions installed.

15.4 Canceling Service Pack Migration

A service pack migration can only be cancelled at specific stages during the migration process:

1. Until the package upgrade starts, there are only minimal changes on the system, like for services and repositories. Restore `/etc/zypp/repos.d/*` to revert to the former state.
2. After the package upgrade starts, you can revert to the former state by using a Snapper snapshot (see *Book “Administration Guide”, Chapter 6 “System Recovery and Snapshot Management with Snapper”*).
3. After the migration target was selected, SUSE Customer Center changes the repository data. To revert this state manually, use **SUSEConnect** `--rollback`.

15.5 Migrating with the Online Migration Tool (YaST)

To perform a service pack migration with YaST, use the *Online Migration* tool. By default, YaST does not install any packages from a third-party repository. If a package was installed from a third-party repository, YaST prevents packages from being replaced with the same package coming from SUSE.



Note: Reduce Installation Size

When performing the SP migration, YaST will install all recommended packages. Especially in the case of custom minimal installations, this may increase the installation size of the system significantly.

To change this default behavior and allow only required packages, adjust `/etc/zypp/zypp.conf` and set the following variable:

```
solver.onlyRequires = true
installRecommends=false # or commented
```

This changes the behavior of all package operations, such as the installation of patches or new packages.

To start the service pack migration, do the following:

1. If you are logged into a GNOME session running on the machine you are going to update, switch to a text console. Running the update from within a GNOME session is not recommended. Note that this does not apply when being logged in from a remote machine (unless you are running a VNC session with GNOME).
2. Run YaST online update to get the latest package updates for your system.
3. Install the package `yast2-migration` and its dependencies (in YaST under *Software > Software Management*).
4. Restart YaST, otherwise the newly installed module will not be shown in the control center.
5. Start in YaST *System > Online Migration*. YaST will show possible migration targets and a summary. If more than one migration target is available for your system, select one from the list.
6. Select one migration target from the list and proceed with *Next*.
7. In case the migration tool offers update repositories, it is recommended to proceed with *Yes*.
8. If the Online Migration tool finds obsolete repositories coming from DVD or a local server, it is highly recommended to disable them. Obsolete repositories are from a previous SP. Any old repositories from SCC or SMT are removed automatically.
9. Check the summary and proceed with the migration by clicking *Next*. Confirm with *Start Update*.
10. After the successful migration restart your system.

15.6 Migrating with Zypper

To perform a service pack migration with Zypper, use the command line tool `zypper migration`.



Note: Reduce Installation Size

When performing the SP migration, YaST will install all recommended packages. Especially in the case of custom minimal installations, this may increase the installation size of the system significantly.

To change this default behavior and allow only required packages, adjust `/etc/zypp/zypp.conf` and set the following variable:

```
solver.onlyRequires = true
installRecommends=false # or commented
```

This changes the behavior of all package operations, such as the installation of patches or new packages. To change the behavior of Zypper for a single invocation, add the parameter `--no-recommends` to your command line.

To start the service pack migration, do the following:

1. If you are logged into a GNOME session running on the machine you are going to update, switch to a text console. Running the update from within a GNOME session is not recommended. Note that this does not apply when being logged in from a remote machine (unless you are running a VNC session with GNOME).

2. Register your SUSE Linux Enterprise machine if you have not done so:

```
sudo SUSEConnect --regcode YOUR_REGISTRATION_CODE
```

3. Install the latest updates:

```
sudo zypper patch
```

4. Install the packages `zypper-migration-plugin` and their dependencies:

```
sudo zypper migration
```

5. Run `zypper migration`:

```
tux > sudo zypper migration
Executing 'zypper patch-check'

Refreshing service 'SUSE_Linux_Enterprise_Server_12_x86_64'.
Loading repository data...
Reading installed packages...
0 patches needed (0 security patches)

Available migrations:
```

```
1 | SUSE Linux Enterprise Server 12 SP1 x86_64
2 | SUSE Linux Enterprise Server 12 SP2 x86_64
```

Some notes about the migration process:

- If more than one migration target is available for your system, Zypper allows you to select one SP from the list. This is the same as skipping one or more SPs. Keep in mind, online migration for base products (SLES, SLED) remains available only between the SPs of a major version.
 - By default, Zypper uses the option `--no-allow-vendor-change` which is passed to `zypper dup`. If a package was installed from a third-party repository, this option prevents packages from being replaced with the same package coming from SUSE.
 - If Zypper finds obsolete repositories coming from DVD or a local server, it is highly recommended to disable them. Old SCC or SMT repositories are removed automatically.
6. Review all the changes, especially the packages that are going to be removed. Proceed by typing `y` (the exact number of packages to upgrade can vary on your system):

```
266 packages to upgrade, 54 to downgrade, 17 new, 8 to reinstall, 5 to remove,
1 to change arch.
Overall download size: 285.1 MiB. Already cached: 0 B After the operation,
additional 139.8 MiB will be used.
Continue? [y/n/? shows all options] (y):
```

Use the `Shift+Page ↑` or `Shift+Page ↓` keys to scroll in your shell.

7. After successful migration restart your system.

15.7 Migrating with Plain Zypper

If you cannot use YaST migration or the Zypper migration, you can still migrate with plain Zypper and some manual interactions. To start a service pack migration, do the following:

1. If you are logged into a GNOME session running on the machine you are going to update, switch to a text console. Running the update from within a GNOME session is not recommended. Note that this does not apply when being logged in from a remote machine (unless you are running a VNC session with GNOME).

2. Update the package management tools with the old SUSE Linux Enterprise repositories:

```
sudo zypper patch --updatestack-only
```

3. If the system is registered, it needs to be deregistered:

```
sudo SUSEConnect --de-register
```

4. Remove the old installation sources and repositories and adjust the third-party repositories.

5. Add the new installation sources, be it local or remote sources (for the placeholder *REPOSITORY*, refer to [Table 13.2, “Repository Layout for SUSE Linux Enterprise 11 SP3/SP4 and for SUSE Linux Enterprise 12 SP1”](#)):

```
sudo zypper addrepo REPOSITORY
```

You can also use SUSE Customer Center or Subscription Management Tool. The command for SUSE Linux Enterprise 12 SP1 on x86-64 is:

```
sudo SUSEConnect -p SLES/12.2/x86_64 OPTIONS
```

Keep in mind, cross-architecture upgrades are not supported.

6. Finalize the migration:

```
sudo zypper ref -f -s  
sudo zypper dup --no-allow-vendor-change --no-recommends
```

The first command will update all services and repositories. The second command performs a distribution upgrade. Here, the last two options are important: `--no-allow-vendor-change` ensures that third-party RPMs will not overwrite RPMs from the base system. The option `--no-recommends` ensures that packages deselected during initial installation will not be added again.

15.8 Rolling Back a Service Pack

If a service pack does not work for you, SUSE Linux Enterprise supports reverting the system to the state before the service pack migration was started. Prerequisite is a Btrfs root partition with snapshots enabled (this is the default when installing SLES 12). See *Book “Administration Guide”, Chapter 6 “System Recovery and Snapshot Management with Snapper”* for details.

1. Get a list of all Snapper snapshots:

```
sudo snapper list
```

Review the output to locate the snapshot that was created immediately before the service pack migration was started. The column *Description* contains a corresponding statement and the snapshot is marked as important in the column *Userdata*. Memorize the snapshot number from the column *#* and its date from the column *Date*.

2. Reboot the system. From the boot menu, select *Start boot loader from a read-only snapshot* and then choose the snapshot with the date and number you memorized in the previous step. A second boot menu (the one from the snapshot) is loaded. Select the entry starting with SLES 12 and boot it.
3. The system boots into the previous state with the system partition mounted read-only. Log in as root and check whether you have chosen the correct snapshot. Also make sure everything works as expected. Note that due to the fact that the root file system is mounted read-only restrictions in functionality may apply.

In case of problems or if you have booted the wrong snapshot, reboot and choose a different snapshot to boot from—up to this point no permanent changes have been made. If the snapshot is correct and works as expected, make the change permanent by running the following command:

```
snapper rollback
```

Reboot afterward. On the boot screen, choose the default boot entry to reboot into the reinstated system.

4. Check if the repository configuration and has been properly reset. Furthermore, check if all products are properly registered. If either one is not the case, updating the system at a later point in time may no longer work, or the system may be updated using the wrong package repositories.

Make sure the system can access the Internet before starting this procedure.

- a. Refresh services and repositories by running

```
sudo zypper ref -fs
```

- b. Get a list of active repositories by running

```
sudo zypper lr
```

Carefully check the output of this command. No services and repositories that were added for the update should be listed. If you, for example, are rolling back from a service pack migration from SLES 12 SP1 to SLES 12 SP2, the list must *not* contain the repositories SLES12-SP2-Pool and SLES12-SP2-Updates, but rather the SP1 versions.

In case wrong repositories are listed make sure to delete them and, if necessary, replace them with the versions matching your product or service pack version. For a list of repositories for the supported migration paths refer to [Section 13.4, "Repository Model"](#).

- c. Last, check the registration status for all products installed by running

```
SUSEConnect --status
```

All products should be reported as being Registered. If this is not the case, repair the registration by running

```
SUSEConnect --rollback
```

Now you have successfully reverted the system to the state that was captured immediately before the service pack migration was started.

16 Backporting Source Code

SUSE extensively uses backports, for example for the migration of current software fixes and features into released SUSE Linux Enterprise packages. The information in this chapter helps you understand why it can be deceptive to compare version numbers to judge the capabilities and the security of SUSE Linux Enterprise software packages. You will understand how SUSE keeps the system software secure and current while maintaining compatibility for your application software on top of SUSE Linux Enterprise products. You will also learn how to check which public security issues actually are addressed in your SUSE Linux Enterprise system software, and how current your software really is.

16.1 Reasons for Backporting

Upstream developers are primarily concerned with advancing the software they develop. Often they combine fixing bugs with introducing new features which have not yet received extensive testing and which may introduce new bugs.

For distribution developers, it is important to distinguish between:

- bugfixes with a limited potential for disrupting functionality; and
- changes that may disrupt existing functionality.

Usually, distribution developers do not follow all upstream changes when a package has become part of a released distribution. Usually they stick instead with the upstream version that they initially released and create patches based on upstream changes to fix bugs. This practice is known as *backporting*.

Distribution developers generally will only introduce a newer version of software in two cases:

- when the changes between their packages and the upstream versions have become so large that backporting is no longer feasible, or
- for software that inherently ages badly, like anti-malware software.

SUSE uses backports extensively as we strike a good balance between several concerns for enterprise software. The most important of them are:

- Having stable interfaces (APIs) that software vendors can rely on when building products for use on SUSE's enterprise products.
- Ensuring that packages used in the release of SUSE's enterprise products are of the highest quality and have been thoroughly tested, both in themselves and as part of the whole enterprise product.
- Maintaining the various certifications of SUSE's enterprise products by other vendors, like certifications for Oracle or SAP products.
- Allowing SUSE's developers to focus on making the next version of the product as good as they can make it, rather than them having to spread their focus thinly across a wide range of releases.
- Keeping a clear view of what is in a particular enterprise release, so that our support can provide accurate and timely information about it.

16.2 Reasons against Backports

It is a general policy rule that no new upstream versions of a package are introduced into our enterprise products. This rule is not an absolute rule however. For a limited class of packages, in particular anti-virus software, security concerns weigh heavier than the conservative approach that is preferable from the perspective of quality assurance. For packages in that class, occasionally newer versions are introduced into a released version of an enterprise product line.

Sometimes also for other types of packages the choice is made to introduce a new version rather than a backport. This is done when producing a backport is not economically feasible or when there is a very relevant technical reason to introduce the newer version.

16.3 The Implications of Backports for Interpreting Version Numbers

Because of the practice of backporting, one cannot simply compare version numbers to determine whether a SUSE package contains a fix for a particular issue or has had a particular feature added to it. With backporting, the upstream part of a SUSE package's version number merely indicates what upstream version the SUSE package is based on. It may contain bug fixes and features that are not in the corresponding upstream release, but that have been backported into the SUSE package.

One particular area where this limited value of version numbers when backporting is involved can cause problems is with security scanning tools. Some security vulnerability scanning tools (or particular tests in such tools) operate solely on version information. These tools/tests are thus prone to generating “false positives” (claims that a vulnerable piece of software has been found which in fact is not vulnerable) when backports are involved. When evaluating reports from security scanning tools, one should always investigate whether an entry is based on a version number or on an actual test of whether an actual vulnerability exists.

16.4 How to Check Which Bugs are Fixed and Which Features are Backported and Available




There are several locations where information regarding backported bug fixes and features are stored:

- The package's changelog:

```
rpm -q --changelog name-of-installed-package
rpm -qp --changelog packagefile.rpm
```

The output briefly documents the change history of the package.

- The package changelog may contain entries like bsc#1234 (“Bugzilla Suse.Com”) that refer to bugs in SUSE's Bugzilla tracking system or links to other bugtracking systems. Because of confidentiality policies, not all such information may be accessible to you.
- A package may contain a /usr/share/doc/packagename/README.SUSE file which contains general, high-level information specific to the SUSE package.

- The RPM source package contains the patches that were applied during the building of the regular binary RPMs as separate files that can be interpreted if you are familiar with reading source code. See *Book “Administration Guide”, Chapter 5 “Managing Software with Command Line Tools”, Section 5.1.2.5 “Installing or Downloading Source Packages”* for installing sources of SUSE Linux Enterprise software, see *Book “Administration Guide”, Chapter 5 “Managing Software with Command Line Tools”, Section 5.2.5 “Installing and Compiling Source Packages”* for building packages on SUSE Linux Enterprise and see the [Maximum RPM \(http://www.rpm.org/max-rpm/\)](http://www.rpm.org/max-rpm/)  book for the inner workings of SUSE Linux Enterprise software package builds.
- For security bug fixes, consult the [SUSE security announcements \(http://www.suse.com/support/security/#1\)](http://www.suse.com/support/security/#1) . These often refer to bugs through standardized names like CAN-2005-2495 which are maintained by the [Common Vulnerabilities and Exposures \(CVE\) \(http://cve.mitre.org\)](http://cve.mitre.org)  project.

A Documentation Updates

This chapter lists content changes for this document.

This manual was updated on the following dates:

- *Section A.1, “November 2016 (Initial Release of SUSE Linux Enterprise Desktop 12 SP2)”*
- *Section A.2, “March 2016 (Maintenance Release of SUSE Linux Enterprise Desktop 12 SP1)”*
- *Section A.3, “December 2015 (Initial Release of SUSE Linux Enterprise Desktop 12 SP1)”*
- *Section A.4, “February 2015 (Documentation Maintenance Update)”*
- *Section A.5, “October 2014 (Initial Release of SUSE Linux Enterprise Desktop 12)”*

A.1 November 2016 (Initial Release of SUSE Linux Enterprise Desktop 12 SP2)

General

- The e-mail address for documentation feedback has changed to doc-team@suse.com.
- The documentation for Docker has been enhanced and renamed to *Docker Guide*.

General Changes to this Guide

- The complete guide has been revised, restructured, and flattened (Fate #319115).




Chapter 2, Installation with YaST

- Added a tip on how to access network storage to *Section 2.6, “Network Settings”*.
- Dialog options for creating an encrypted LVM file system (*Section 2.9, “Suggested Partitioning”*) have changed (Fate #320418).
- The *Receive System Mail* has been removed from the *Add User* dialog (Fate #320448).
- Added *Section 2.2.2.6, “Disabling the Installer Self-Update”*.





Chapter 13, Life Cycle and Support

- Updated list of modules *Section 13.4, “Repository Model”* (Fate #320579).

Chapter 15, Service Pack Migration

- Added *Section 14.1.6, “Create Non-MD5 Server Certificates for Java Applications”* (https://bugzilla.suse.com/show_bug.cgi?id=970153 )
- Added a conceptual overview and mentioned additional migration strategies (https://bugzilla.suse.com/show_bug.cgi?id=968195 )
- Added *Section 14.9, “Updating Registration Status After Rollback”* (Fate #319118).
- Added *Section 14.1.8, “Check the `clientSetup4SMT.sh` script on SMT clients”* (https://bugzilla.suse.com/show_bug.cgi?id=944342 )
- Implemented a notice to make sure a service pack migration is not performed with insufficient disk space (Fate #317784, see *Section 14.2, “Disk Space”*).
- Mentioned that during installation, an installation resource is added and removed afterward (Fate #320494).

Bugfixes

- Removed link (https://bugzilla.suse.com/show_bug.cgi?id=972355 )
- Added documentation for installing KVM guests on IBM z Systems (https://bugzilla.suse.com/show_bug.cgi?id=958733 )
- Added note about where to place `/boot` for an LVM root file system (https://bugzilla.suse.com/show_bug.cgi?id=1000631 )
- Added more information about rolling back a service pack (https://bugzilla.suse.com/show_bug.cgi?id=1001070 )
- Added recommendations for the case of running an update from within a GNOME session (https://bugzilla.suse.com/show_bug.cgi?id=1001684 )

A.2 March 2016 (Maintenance Release of SUSE Linux Enterprise Desktop 12 SP1)

- Distinguished between remote and local repository more clearly (https://bugzilla.suse.com/show_bug.cgi?id=956058 ↗).
- Added note about reformatting partitions with **mkswap**, because initrd image cannot boot up when swap partition has changed (https://bugzilla.suse.com/show_bug.cgi?id=955822 ↗).

A.3 December 2015 (Initial Release of SUSE Linux Enterprise Desktop 12 SP1)

General

- Book “*Subscription Management Tool for SLES 12 SP2*” is now part of the documentation for SUSE Linux Enterprise Desktop.
- Add-ons provided by SUSE have been renamed as modules and extensions. The manuals have been updated to reflect this change.
- Numerous small fixes and additions to the documentation, based on technical feedback.
- The registration service has been changed from Novell Customer Center to SUSE Customer Center.
- In YaST, you will now reach *Network Settings* via the *System* group. *Network Devices* is gone (https://bugzilla.suse.com/show_bug.cgi?id=867809 ↗).

Chapter 2, Installation with YaST

- Added *Section 2.2.2.4, “Using a Proxy During the Installation”* (Fate #318488).
- Added a warning on using unsigned drivers in secure boot mode to *Section 2.2.1.2, “The Boot Screen on Machines Equipped with UEFI”* (Fate #317593).

Chapter 8, Installing or Removing Software

- Added *Section 8.2.4.1, “Handling of Package Recommendations”* (Fate #318099).

Chapter 9, Installing Modules, Extensions, and Third Party Add-On Products

- Updated chapter to reflect the software changes to the former YaST *SUSE Customer Center Configuration* dialog (now called *Product Registration*) and the YaST *Add-On Products* module (Fate #318800).

Chapter 7, Advanced Disk Setup

- Mentioned that subvolumes for `/var/lib/mariadb`, `/var/lib/pgsql`, and `/var/lib/libvirt/images` are created with the option `no copy on write` by default to avoid extensive fragmenting with Btrfs.

Subscription Management

- The chapter about registering clients at a Subscription Management Tool server has been replaced by *Book “Subscription Management Tool for SLES 12 SP2”, Chapter 8 “Configuring Clients to Use SMT”*.

Part V, “Updating and Upgrading SUSE Linux Enterprise”

- Split former update chapter into several independent chapters and combined them under this new part.
- Removed YaST Wagon chapter, as YaST Wagon is unsupported for SUSE Linux Enterprise Desktop 12 SP2.
- Added new chapter: *Chapter 15, Service Pack Migration*.
- Added *Section 14.1.4, “Migrate your MySQL Database”* and *Section 14.1.5, “Migrate your PostgreSQL Database”*.
- Integrated various new features: Fate #315161, Fate #318636, Fate #319128, Fate #319129, Fate #319138, Fate #319140.

Bugfixes

- Consistent use of **yast**, **yast2.ssh**, **yast.ssh** for SSH based installation (https://bugzilla.suse.com/show_bug.cgi?id=956060 .
- Consistent spelling of boot parameters (https://bugzilla.suse.com/show_bug.cgi?id=956054 .
- PowerKVM: virt-install does not know about SLES12 (https://bugzilla.suse.com/show_bug.cgi?id=880918 .
- IBM POWER: Starting an X-Server after an Upgrade (https://bugzilla.suse.com/show_bug.cgi?id=948980 .
- Added documentation on the boot process for IBM z Systems (https://bugzilla.suse.com/show_bug.cgi?id=942772 .
- Description of encrypted **/** and **/boot** on Btrfs was missing. Added an important note in *Section 2.9, "Suggested Partitioning"* and *Section 7.1.2.1, "Btrfs Partitioning"* (https://bugzilla.suse.com/show_bug.cgi?id=926951 .
- Zypper multiversion kernels should be mentioned for SP2 Update (https://bugzilla.suse.com/show_bug.cgi?id=753809 .
- SLES 12 Deployment Guide errors for zPXE installations (https://bugzilla.suse.com/show_bug.cgi?id=944384 .
- AutoYaST hangs at "Configuring Bootloader ... 50%" with 512RAM (https://bugzilla.suse.com/show_bug.cgi?id=927237 .
- Netsetup Parameters Wrong (https://bugzilla.suse.com/show_bug.cgi?id=928792 .
- Documentation on not creating **/usr** as separate partition is missing (https://bugzilla.suse.com/show_bug.cgi?id=930267 .
- Document how to enable SELinux during install (https://bugzilla.suse.com/show_bug.cgi?id=928158 .
- YaST boot loader: supported scenarios needs updating clarification (https://bugzilla.suse.com/show_bug.cgi?id=939197 .

A.4 February 2015 (Documentation Maintenance Update)

Section 2.10, "Clock and Time Zone"



With NTP disabled it is recommended to avoid writing system time to the hardware clock. Thus set `SYST0HC=no`.

Bugfixes

- Adjustments for SMT because of the switch from SUSE Customer Center to SUSE Customer Center (https://bugzilla.suse.com/show_bug.cgi?id=857639).
- *Section 11.3.2, "Enforcing Password Policies"*: Password Settings, Expiration Date is expiring user accounts in YaST Users module (https://bugzilla.suse.com/show_bug.cgi?id=743874).
- Various bugfixes for *Chapter 14, Upgrading SUSE Linux Enterprise*:
 - The named upgrade path does not work, there is no working upgrade path from SLES 11 SP3 to SLES 12 on Linux for System z (https://bugzilla.suse.com/show_bug.cgi?id=907648).
 - The Atomic Update (https://bugzilla.suse.com/show_bug.cgi?id=905330).
 - Upgrading to SLE 12 (https://bugzilla.suse.com/show_bug.cgi?id=904188).
 - Intermediate step: Updating SLE 11 SP2 to SLE 11 SP3 (https://bugzilla.suse.com/show_bug.cgi?id=904186).
 - Supported Upgrade Paths to SLE (https://bugzilla.suse.com/show_bug.cgi?id=904182).
 - Potentially misleading info around the 6-month overlap in support (https://bugzilla.suse.com/show_bug.cgi?id=902463).

A.5 October 2014 (Initial Release of SUSE Linux Enterprise Desktop 12)

General

- Removed all KDE documentation and references because KDE is no longer shipped.
- Removed all references to SuSEconfig, which is no longer supported (Fate #100011).
- Move from System V init to systemd (Fate #310421). Updated affected parts of the documentation.
- YaST Runlevel Editor has changed to Services Manager (Fate #312568). Updated affected parts of the documentation.
- Removed all references to ISDN support, as ISDN support has been removed (Fate #314594).
- Removed all references to the YaST DSL module as it is no longer shipped (Fate #316264).
- Removed all references to the YaST Modem module as it is no longer shipped (Fate #316264).
- Btrfs has become the default file system for the root partition (Fate #315901). Updated affected parts of the documentation.
- The **dmesg** now provides human-readable time stamps in `ctime()`-like format (Fate #316056). Updated affected parts of the documentation.
- syslog and syslog-ng have been replaced by rsyslog (Fate #316175). Updated affected parts of the documentation.
- MariaDB is now shipped as the relational database instead of MySQL (Fate #313595). Updated affected parts of the documentation.
- SUSE-related products are no longer available from <http://download.novell.com>  but from <http://download.suse.com> . Adjusted links accordingly.
- Novell Customer Center has been replaced with SUSE Customer Center. Updated affected parts of the documentation.

- /var/run is mounted as tmpfs (Fate #303793). Updated affected parts of the documentation.
- The following architectures are no longer supported: IA64 and x86. Updated affected parts of the documentation.
- The traditional method for setting up the network with ifconfig has been replaced by wicked. Updated affected parts of the documentation.
- A lot of networking commands are deprecated and have been replaced by newer commands (usually ip). Updated affected parts of the documentation.

arp: ip neighbor

ifconfig: ip addr, ip link

iptunnel: ip tunnel

iwconfig: iw

nameif: ip link, ifrename

netstat: ss, ip route, ip -s link, ip maddr

route: ip route

- Numerous small fixes and additions to the documentation, based on technical feedback.

Chapter 2, *Installation with YaST*

- Completely rewrote the chapter because of the new installation workflow.
- The installation routine now supports setting up multiple network devices during the installation (Fate #315680): *Section 2.6, "Network Settings"*.
- The installation proposal contains a separate /home partition formatted with XFS (Fate #316637 and Fate #316624): *Section 2.9, "Suggested Partitioning"*.
- Removed occurrences of the YaST Repair module which has been dropped (Fate #308670).
- Update repositories are added after having registered with SUSE Customer Center and can be used during installation (Fate #312012): *Section 2.8, "Extension Selection"*.
- Extensions and modules can be added to the system during the installation (Fate #316548): *Section 2.7, "SUSE Customer Center Registration"*.

- SUSE Linux Enterprise Desktop can be installed as an add-on on top of SUSE Linux Enterprise Server (Fate #316436): *Section 2.8, "Extension Selection"*.
- Automatically importing SSH keys from a previous installation can be disabled (Fate #314982).

Chapter 14, Upgrading SUSE Linux Enterprise

- Added new section: *Section 14.4, "Supported Methods for Upgrading SUSE Linux Enterprise"*.

Chapter 6, Setting Up Hardware Components with YaST

- Removed the following sections as the respective YaST modules are no longer included: *Hardware Information, Setting Up Graphics Card and Monitor, Mouse Model, and Setting Up a Scanner*.
- Removed content about mouse setup and adjusted *Section 6.1, "Setting Up Your System Keyboard Layout"*.

Chapter 8, Installing or Removing Software

- Completely rewrote *Section 8.4, “Keeping the System Up-to-date”* because of changes in the GNOME software updater.

Chapter 9, Installing Modules, Extensions, and Third Party Add-On Products

- Installing add-on products or software extensions is now also possible without access to physical media. Added the following new sections: *Section 14.10, “Registering Your System”* and *Section 9.1, “Installing Modules and Extensions from Online Channels”*. Modified *Section 9.2, “Installing Extensions and Third Party Add-On Products from Media”* accordingly.

Subscription Management

- For registering clients against an SMT server, suse_register has been replaced with SUSEConnect (Fate #316585).

Bugfixes

- Updated section *Section 8.4, “Keeping the System Up-to-date”* according to http://bugzilla.suse.com/show_bug.cgi?id=839692.
- Removed section *Using Fingerprint Authentication*. Further minor corrections and additions (http://bugzilla.suse.com/show_bug.cgi?id=857680).
- Removed obsolete parameter OsaMedium from `parmfile` and `Cobbler` examples (http://bugzilla.suse.com/show_bug.cgi?id=860404).
- Added instructions on how to add secondary languages during installation (http://bugzilla.suse.com/show_bug.cgi?id=870482).
- Multiversion feature (more than one kernel installed) is enabled by default (http://bugzilla.suse.com/show_bug.cgi?id=891805).
- Warn about incompatible Kernel Module Packages (KPMs) (http://bugzilla.suse.com/show_bug.cgi?id=891805).

B GNU Licenses

This appendix contains the GNU Free Documentation License version 1.2.

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available draw-

ing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from

which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.