

# SUSE Linux Enterprise Point of Service

10

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

March 13, 2008

Installation Guide



# Installation Guide

All content is copyright © Novell, Inc.

## Legal Notice

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

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

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

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

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

# Contents

<b>About This Guide</b>	<b>vii</b>
<b>1 Product Overview</b>	<b>1</b>
1.1 Architecture . . . . .	1
1.2 Images . . . . .	3
1.3 Deployment . . . . .	6
<b>2 System Requirements</b>	<b>11</b>
2.1 Administration Server . . . . .	11
2.2 Image Building Server . . . . .	11
2.3 Branch Server . . . . .	12
2.4 Administration/Branch Server Combination . . . . .	12
<b>3 Installation with YaST</b>	<b>15</b>
3.1 Obtaining the Software . . . . .	15
3.2 Planning Your Installation . . . . .	15
3.3 System Start-Up for Installation . . . . .	16
3.4 The Boot Screen . . . . .	18
3.5 Language . . . . .	20
3.6 License Agreement . . . . .	20
3.7 System Analysis . . . . .	21
3.8 Time Zone . . . . .	22
3.9 Server Selection . . . . .	22
3.10 Installation Summary . . . . .	23
3.11 Performing the Installation . . . . .	26
3.12 Configuration of the Installed System . . . . .	27
3.13 Graphical Login . . . . .	35

<b>4</b>	<b>Securing Your Setup</b>	<b>37</b>
4.1	Physical Server Security . . . . .	38
4.2	Network Security . . . . .	38
4.3	Data Security . . . . .	39
4.4	Application Security . . . . .	41
<b>5</b>	<b>Setting Up the Administration Server</b>	<b>43</b>
5.1	Meeting the System Requirements . . . . .	43
5.2	Installing the Administration Server . . . . .	44
5.3	Initializing the LDAP Directory . . . . .	45
5.4	Creating Point of Service Images . . . . .	48
5.5	Copying the Boot Image Files . . . . .	48
5.6	Copying the System Image Files . . . . .	49
5.7	What's Next . . . . .	50
<b>6</b>	<b>Setting Up a Dedicated Image Building Server</b>	<b>51</b>
6.1	Meeting System Requirements . . . . .	51
6.2	Installing a Dedicated Image Building Server . . . . .	51
6.3	Creating Point of Service Images . . . . .	52
6.4	Copying the System Image Files to the Administration Server . . . . .	53
<b>7</b>	<b>Setting Up a Branch Server</b>	<b>55</b>
7.1	Meeting System Requirements . . . . .	55
7.2	Creating Branch Server Objects in LDAP . . . . .	56
7.3	Installing the Branch Server . . . . .	65
7.4	Configuring the Branch Server . . . . .	65
7.5	Downloading Images from the Administration Server . . . . .	67
7.6	Starting the Core Script . . . . .	68
<b>8</b>	<b>Setting Up an Admin/Branch Server Combo</b>	<b>71</b>
8.1	Meeting System Requirements . . . . .	71
8.2	Installing an Admin/Branch Server Combo . . . . .	72
8.3	Initializing the LDAP Directory . . . . .	73
8.4	Creating the Required LDAP Objects . . . . .	75
8.5	Copying the Default Boot Images . . . . .	77
8.6	Creating Point of Service Images . . . . .	77
8.7	Copying the System Image Files . . . . .	78
8.8	Configuring the Branch Server . . . . .	78

<b>9</b>	<b>Setting Up a POSBranch Server</b>	<b>83</b>
<b>10</b>	<b>Deploying Point of Service Terminals</b>	<b>85</b>
10.1	Creating Point of Service Images . . . . .	85
10.2	Creating the Required LDAP Objects . . . . .	86
10.3	Distributing Images to Point of Service Terminals . . . . .	98
10.4	Booting the Point of Service Terminal . . . . .	102
<b>11</b>	<b>Testing Your SUSE Linux Enterprise Point of Service Environment</b>	<b>109</b>
11.1	Monitoring the Terminal Bootup . . . . .	109
11.2	Troubleshooting Terminal Bootup Problems . . . . .	112
<b>A</b>	<b>Changing the Server Language</b>	<b>113</b>
A.1	Changing the Language Selection . . . . .	113



# About This Guide

This guide contains instructions on how to install and deploy your SUSE Linux Enterprise Point of Service system. Learn which components constitute a SUSE Linux Enterprise Point of Service environment and how to configure the individual servers and terminals.

## 1 Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

## 2 Documentation Updates

For the latest version of this documentation, see the *Novell Documentation Web site* [<http://www.novell.com/documentation/slepos10/>].

## 3 Additional Documentation

For information on managing SUSE Linux Enterprise Point of Service, refer to the *SUSE Linux Enterprise Point of Service Administration Guide* available from <http://www.novell.com/documentation/slepos10>.

For more information on the underlying SUSE Linux Enterprise operating system, refer to the *Installation and Administration* available from <http://www.novell.com/documentation/sles10/>.

For information on securing your applications using AppArmor, refer to the *AppArmor Quick Start* and the *AppArmor Administration Guide* available under <http://www.novell.com/documentation/apparmor/>.

For an introduction to setting up High Availability environments with SUSE Linux Enterprise, refer to the Heartbeat Guide available from <http://www.novell.com/documentation/sles10/>.

## 4 Documentation Conventions

The following typographical conventions are used in this manual:

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

# Product Overview

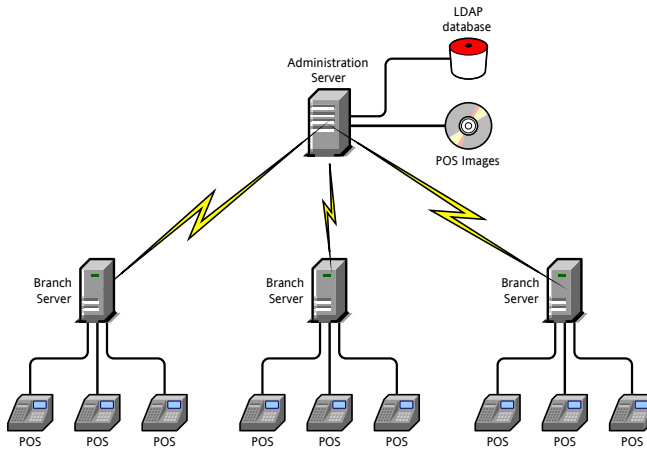
SUSE® Linux Enterprise Point of Service is a secure and reliable Linux platform optimized for enterprise retail organizations. Built on the solid foundation of SUSE® Linux Enterprise, it is the only enterprise-class Linux operating system tailored specifically for retail Point of Service terminals, kiosk and self-service systems, and reverse-vending systems.

This section provides an architectural overview of the SUSE Linux Enterprise Point of Service product, along with an overview of images, and the deployment process.

## 1.1 Architecture

The SUSE Linux Enterprise Point of Service architecture consists of one centralized Administration Server, one or more Branch Servers, and Point of Service terminals, which can be standard PCs running retail check-out applications or specialized point-of-sale machines such as cash registers and customer kiosks (see [Figure 1.1, “SUSE Linux Enterprise Point of Service System Architecture”](#) (page 2)). Find a list of system requirements for the individual components in [Chapter 2, \*System Requirements\*](#) (page 11) and an overview of the different server types and their functions in Chapter 1, *Servers Types in SUSE Linux Enterprise Point of Service* (↑Administration Guide).

**Figure 1.1** *SUSE Linux Enterprise Point of Service System Architecture*



All system information (system structure, the configuration and deployment method for each Branch Server and Point of Service terminal, image information, etc.) is stored in an LDAP database on the Administration Server. The Administration Server usually also holds the master repository for the images required to boot and configure Point of Service terminals and provides the utilities required to build those images.

---

**NOTE: Creating a Dedicated Image Building Server**

However, if you have a large system and want to offload the image building function from the Administration Server, you can also set up a dedicated Image Building Server. For more information, see [Chapter 5, Setting Up the Administration Server](#) (page 43) or [Chapter 6, Setting Up a Dedicated Image Building Server](#) (page 51).

---

Triggered by the `possyncimages.pl` script (see Section “`possyncimages.pl`” (Appendix A, *Point of Service Scripts*, ↑Administration Guide), each Branch Server downloads the system information and images required for its local Point of Service terminals from the Administration Server. The Point of Service terminals, in turn, download their respective images from the Branch Server when they boot.

---

## **WARNING: Protecting the Branch Servers**

Because Branch Servers contain sensitive information, they must be secured against unauthorized access. Close unused ports and allow only the root user to have access to the server console. Refer to [Chapter 4, \*Securing Your Setup\*](#) (page 37) for more details on how to protect your SUSE Linux Enterprise Point of Service setup.

---

SUSE Linux Enterprise Point of Service is broadly scalable so that a small shop with five Point of Service terminals can be managed just as well as a large chain with a thousand branches. For organizations with several Branch Servers, the link between the branch and administrative servers is maintained over WAN links. During execution of administrative tasks, such as installation of new Point of Service terminals in a branch, steps must be taken to ensure that the WAN link to the Administration Server is available.

The SUSE Linux Enterprise Point of Service architecture is highly centralized; however, administrative tasks can also be performed on subunits for role-based administration. Moreover, although the LDAP directory is not replicated on the Branch Server, the Branch Server provides all the services necessary for the operation and management of the Point of Service terminals. Consequently, the Branch Server and Point of Service terminals can function independently of the Administration Server in the event of server failure or a downed connection.

## **1.2 Images**

SUSE Linux Enterprise Point of Service is designed to automate the roll-out of Point of Service terminals as much as possible. To assist this automation, the product makes extensive use of image building technology. For each type of terminal, whether it is a non-graphical system or a full desktop environment, you can create customized images to be downloaded automatically from the Branch Server when the terminal boots.

### **1.2.1 Types of Images**

To help get you started, SUSE Linux Enterprise Point of Service comes with a set of pre-built image files that you can customize to set up your own system. Every Point of Service terminal requires two images: a boot image and a system image. You can also

create your own images using Image Creator or KIWI. For more information, refer to Chapter 6, *Building Images with the Image Creator Tool* (↑Administration Guide) and Chapter 7, *Building Images with KIWI* (↑Administration Guide).

The boot images contain the kernel and a bootstrap image (`initrd`) and thus, provide the minimum your Point of Service terminals need to initially start up from a bootable CD or USB stick, or from the network via remote boot technology. The following boot images templates are available for SUSE Linux Enterprise Point of Service 10:

#### isoboot

This boot image template creates all the files and directories required to boot diskless and preinstalled diskful systems from CD. This boot image must be combined with a system image to create a CD that can be used to boot the Point of Service terminal.

#### usbboot

This boot image template creates all the files and directories required to boot diskless and preinstalled diskful systems from a USB stick.

#### netboot

This boot image template creates all the files and directories (including partitioning and boot loader installation) required to boot diskful and diskless terminals from the network over Preboot Execution Environment (PXE) and DHCP. The kernel and the `initrd` are stored at the Branch Servers and they are downloaded to the terminals using TFTP.

The following system image templates are specially designed for the most common types of retail Point of Service terminals:

#### Minimal

The `Minimal` image contains only the runtime environment for native-code applications (C and C++) and the ncurses library for non-graphical user interface support. The `Minimal` image supports only console-based applications.

Maximum image size: 128 MB (compressed), minimum size of RAM required to boot the image: 64 MB

#### Graphical

The `Graphical` image includes the features of the `Minimal` image and additionally provides essential graphical interface capabilities (the X Window System and a lightweight Window Manager) as well as the ability to run Java programs. It

supports console-based C/C++ applications, Java programs in a Java2 runtime environment, X11 applications, and basic browser-based applications.

Maximum size: 120 MB (compressed), minimum size of RAM required to boot the image: 256 MB

## Desktop

The `Desktop` image is for high-functionality clients with full graphical user interface capabilities. It includes the Firefox Web browser with plug-ins, and a full graphical desktop environment (GNOME or KDE). The `Desktop` image supports console-based C/C++ applications, Java programs in a Java2 runtime environment, X11 applications, browser-based applications, and GNOME-based or KDE-based programs.

Maximum size: 700 MB (compressed), minimum size of RAM required to boot the image: 256 MB

All system images are based on SUSE Linux Enterprise Server. You can extend Point of Service system images to include add-on features such as:

- Advanced Linux Sound Architecture (ALSA) library for audio support
- additional device drivers
- GNOME or KDE desktop environments
- IBM™ Java technology support
- Firefox and other Web browsers
- Samba 3 Client for SMB/CIFS connectivity to Microsoft™ Windows™ servers
- VNC 4 Remote Control Client to allow other computers to remotely control the terminal

System images that you create are initially stored on the Administration Server (or on the Image Building Server, if you chose to set up a dedicated Image Building Server). Before you deploy your Point of Service terminals, you run a script to transmit the system images via the RSYNC to specific directories on the Branch Server where, in turn, they can be downloaded to Point of Service terminals at boot time.

When a Point of Service terminal is started for the first time, it performs a PXE boot (or boots from CD or USB stick) and then registers with the Branch Server to obtain the information it needs to download its system image. The TFTP service on the Branch Server automatically delivers the matching system image to the Point of Service terminal.

To make this work as designed, you must create reference objects in the LDAP directory for the types of Point of Service terminals you intend to deploy in your system. For detailed information, refer to Section “Defining Point of Service Terminal Objects” (Chapter 4, *Using posAdmin to Manage the LDAP Directory*, ↑Administration Guide). Taking the time to correctly create and configure these objects when you install the Branch Servers saves you from separately managing the startup of each Point of Service terminal.

## 1.2.2 KIWI and Image Creator

To create the images for the Point of Service terminals, SUSE Linux Enterprise Point of Service includes both a command line tool (KIWI) and a graphical front-end for KIWI: Image Creator. Install the image building tools by selecting the `SLEPOS Image Server` and the `SLEPOS Images` software patterns in YaST.

When you build images for the Point of Service terminals, all the information required to run a Point of Service terminal—the Linux operating system, drivers, configuration settings, application files, and so forth—can be compiled into a single image file. This file can then be electronically distributed to Point of Service terminals over the network, or you can generate an ISO version of the image file that can be burned to a CD or copied to a USB stick for manual distribution.

For detailed information on KIWI and Image Creator, refer to Chapter 7, *Building Images with KIWI* (↑Administration Guide) and Chapter 6, *Building Images with the Image Creator Tool* (↑Administration Guide).

# 1.3 Deployment

SUSE Linux Enterprise Point of Service requires the following components for a functional system:

- Administration Server

- Image Building Server
- Branch Servers
- Point of Service terminals

The way in which these components are deployed depends on your system requirements. For example, systems that maintain hundreds of system images might require a dedicated Image Building Server, whereas smaller systems can have the image building utilities installed on the Administration Server. Similarly, some customers might install the Administration and Branch Servers on a single box, while others deploy the Branch Server on a Point of Service terminal.

The flexibility of the architecture provides broad scalability so that in large environments components can be distributed to improve system performance, while in smaller environments components can be consolidated to maximize the use of system resources.

## 1.3.1 Design Guidelines for Large Environments

Every retail environment is different in terms of network speed, server hardware, Point of Service terminal hardware, size of images, frequency of updates, etc. This section presents some design guidelines for large environments.

The recommended maximum number of Point of Service terminals being serviced by a single Branch Server is 100. You can adjust this number up or down depending on how frequently the Point of Service terminals are reimaged and whether you can control when the terminals come online.

---

### **NOTE: Time for Booting**

For every 100 terminals coming online at the same time, it can take up to 10 minutes for the terminals to download larger desktop images. If the terminals are simply booting from an existing image, it can take 2-3 minutes per 100 terminals.

---

## 1.3.2 Installation and Setup

The following summary outlines the general steps required to deploy a SUSE Linux Enterprise Point of Service system. It also identifies the configuration options for each system component and notes where you can go to find detailed instructions.

- 1 Install the Administration Server using one of the following configurations:
  - Install an Administration Server that includes the image building utilities (KIWI and Image Creator) and all the files and directories required to create Point of Service images. For detailed instructions, see [Chapter 5, \*Setting Up the Administration Server\*](#) (page 43).
  - Install an Administration Server and a dedicated Image Building Server. For detailed instructions, see [Chapter 6, \*Setting Up a Dedicated Image Building Server\*](#) (page 51).
  - Install an Admin/Branch Server combination. For detailed instructions, see [Chapter 8, \*Setting Up an Admin/Branch Server Combo\*](#) (page 71).
- 2 Create the LDAP directory on your Administration Server. For detailed instructions, see [Section 5.3, “Initializing the LDAP Directory”](#) (page 45).
- 3 Create the Point of Service images required to deploy your Point of Service terminals.
- 4 Copy the image files you have created to the appropriate directories on the Administration Server so they will be ready for the Branch Servers to download.

---

### **IMPORTANT: Location of the System Images**

System images must be located in `/srv/SLEPOS/image/` and boot images must be located in `/srv/SLEPOS/boot/` on the Administration Server before the rsync can transmit the images to the Branch Server.

---

- 5 Create the required LDAP objects for each Branch Server and its Point of Service terminals in the LDAP tree. For detailed instructions, see [Section 7.2, “Creating Branch Server Objects in LDAP”](#) (page 56).

## 6 Install the Branch Servers using one of the following configurations:

---

### **NOTE: Configuring Admin/Branch Server Combinations**

If you install an Admin/Branch Server combination, this step is already completed. For instructions on how to configure the Admin/Branch Server combination, see [Chapter 8, \*Setting Up an Admin/Branch Server Combo\*](#) (page 71).

---

- Install a standard Branch Server. For detailed instructions, see [Chapter 7, \*Setting Up a Branch Server\*](#) (page 55).
  - Install a high availability Branch Server cluster of two nodes in an active/passive setup. For general information on how to set up a high availability environment, refer to the Heartbeat Administration Guide [<http://www.novell.com/documentation/sles10/pdfdoc/heartbeat/heartbeat.pdf>] that is available from <http://www.novell.com/documentation/sles10>.
  - For stores where the Branch Server is only running the Point of Service infrastructure (i.e. the Branch Server is running no additional applications), the Branch Server can be installed as a control terminal running on Point of Service hardware. For more information, see [Chapter 9, \*Setting Up a POS-Branch Server\*](#) (page 83).
- 7** After a Branch Server is installed, you must complete the following steps to initialize the Branch Server before attempting to boot its Point of Service terminals:
- 7a** Run the `posInitBranchserver.sh` script to initialize and configure the Branch Server. For detailed instructions, see [Section 7.4, “Configuring the Branch Server”](#) (page 65).
  - 7b** Run `possyncimages.pl` to download the Point of Service images from the Administration Server to the `/srv/tftpboot` directories on the Branch Server. For detailed instructions, see [Section 7.5, “Downloading Images from the Administration Server”](#) (page 67).

- 7c** Start the core script (`posleases2ldap`) as a daemon process on the Branch Server. This script controls all other scripts. For more information, see [Section 7.6, “Starting the Core Script”](#) (page 68).
- 8** Deploy the Point of Service terminals, following the general instructions in [Chapter 10, \*Deploying Point of Service Terminals\*](#) (page 85).

Depending on your network configuration and terminal hardware, you must prepare the Point of Service terminals to boot using one of the following procedures:

- If the Point of Service terminals have access to the network, the terminals can PXE boot and download their image files from the Branch Server. This method is typically used for diskless workstations. For more information on this process, see [Section 10.4.1, “Network PXE Boot”](#) (page 102).
  - If the Point of Service terminals do not have access to the network, create an isoboot or a usbboot image and deploy the image at the terminal. This method can be used for either diskless or diskful workstations that have a CD drive or a USB port. For information on the isoboot process, see [Section 10.4.2, “ISOBoot”](#) (page 108) .
  - If a Point of Service terminal cannot boot from the network or from a CD, it attempts to boot from the hard drive. For more information, see [Section 10.4, “Booting the Point of Service Terminal”](#) (page 102).
- 9** Test your SUSE Linux Enterprise Point of Service installation to ensure that it is functioning correctly. For detailed instructions, see [Chapter 11, \*Testing Your SUSE Linux Enterprise Point of Service Environment\*](#) (page 109).

# System Requirements

This section provides a list of minimal hardware requirements for SUSE Linux Enterprise Point of Service supported by SUSE® Linux Enterprise Server.

## 2.1 Administration Server

The following list identifies the system requirements for an Administration Server:

- One server with an x86 processor
- A minimum of 4 GB hard disk space; recommended 15 GB

This will vary depending on the size of your images.

- A minimum of 256 MB RAM; recommended 512 MB - 3 GB (at least 256 MB per CPU)
- One network card

## 2.2 Image Building Server

The following list identifies the system requirements for a dedicated image building server:

- One server with an x86 processor

- A minimum of 4 GB hard disk space; recommended 25 GB

This will vary depending on the size of your images.

- A minimum of 512 MB RAM; recommended 512 MB - 3 GB (at least 256 MB per CPU)
- One network card

## 2.3 Branch Server

The following list identifies the system requirements for a Branch Server:

- One server with an x86 processor
- A minimum of 4 GB hard disk space; recommended 10 GB

This will vary depending on the size of the images you distribute to your Point of Service terminals.

- A minimum of 256 MB RAM; recommended 512 MB - 3 GB (at least 256 MB per CPU)
- At least two network cards per server:
  - One network card for the Administration Server's public network
  - One network card for the Branch Server's private network

## 2.4 Administration/Branch Server Combination

The following list identifies the system requirements for an Administration/Branch Server combination:

- One server with an x86 processor
- A minimum of 4 GB hard disk space; recommended 25 GB

This will vary depending on the size of your images.

- A minimum of 512 MB RAM; recommended 512 MB - 3 GB (at least 256 MB per CPU)
- One network card



# Installation with YaST

SUSE® Linux Enterprise Point of Service is distributed as an add-on to SUSE Linux Enterprise. To install it, install the SUSE Linux Enterprise Server base system. Either install SUSE Linux Enterprise Point of Service together with SUSE Linux Enterprise Server or at any later point in time on top of the installed SUSE Linux Enterprise Server system.

## 3.1 Obtaining the Software

To obtain the SUSE Linux Enterprise Point of Service software, go to <http://www.novell.com/download> and select the SUSE Linux Enterprise Point of Service product. Click *Search* and then select *SUSE Linux Enterprise Point of Service* from the results list. Click *Proceed to Download* and log in to your Novell account to access the CD images available for download.

After downloading the `.iso` files, verify the MD5 checksums to ensure that the images have been downloaded completely and without any errors. Burn the `.iso` files to CDs using a CD burning software of your choice. Label the CDs using the names of the `.iso` files.

## 3.2 Planning Your Installation

Before you install SUSE Linux Enterprise Point of Service, decide which system configuration to use. This choice determines how many servers you need and what software packages you need install on each one of them.

For the Administration Server, you have three configuration options:

- Administration Server with Image Building Tools
- Administration Server with separate Image Building Server
- Admin/Branch Server combination

For the Branch Server, you have four configuration options:

- Branch Server
- High Availability Branch Server
- Branch Server running on a Point of Service terminal
- Branch Server as part of the Admin/Branch Server combination

---

### **IMPORTANT: Configuring Admin/Branch Server Combinations**

The Admin/Branch Server combination is supported for single site, self-contained installations only. No additional Branch Servers can connect to the Admin/Branch Server. You can, however, configure an Admin/Branch Server combination in a two-node heartbeat cluster with one server acting as the primary server and the other as the secondary server.

---

The installation process for each type of server is essentially the same. Use YaST for all installations; the main difference is the software you select to install on the server.

## **3.3 System Start-Up for Installation**

You can install SUSE Linux Enterprise from local installation sources, such as the SUSE Linux Enterprise CDs or DVD, or from network source of an FTP, HTTP, or NFS server. Any of these approaches requires physical access to the system to install and user interaction during the installation. The installation procedure is basically the same regardless of the installation source.

## 3.3.1 Boot Options

Boot options other than CD or DVD exist and can be used if problems arise booting from CD or DVD. These options are described in [Table 3.1, “Boot Options”](#) (page 17).

**Table 3.1** *Boot Options*

Boot Option	Description
CD-ROM	This is the easiest boot option. This option can be used if the system has a local CD-ROM drive that is supported by Linux.
Floppy	The images for generating boot floppies are located on CD 1 in the <code>/boot</code> directory. A <code>README</code> is available in the same directory.
PXE or BOOTP	This must be supported by the system's BIOS or firmware and a boot server must be available in the network. This task can also be handled by another SUSE Linux Enterprise system.
Hard Disk	SUSE Linux Enterprise 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/loader</code> on CD 1 to the hard disk and add the appropriate entry to the boot loader.

## 3.3.2 Installing from the SUSE Linux Enterprise Media

To install from the media, insert the first CD or DVD into the appropriate drive of the system to install. Reboot the system to boot from the media and open the boot screen.

### 3.3.3 Installing from a Network Server Using SLP

If your network setup supports OpenSLP and your network installation source has been configured to announce itself via OpenSLP, boot the system from the media or with another boot option. In the boot screen, select the desired installation option. Press F4 then select *SLP*.

The installation program retrieves the location of the network installation source using OpenSLP and configures the network connection with DHCP. If the DHCP network configuration fails, you are prompted to enter the appropriate parameters manually. The installation then proceeds normally.

### 3.3.4 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 from the media or with another boot option. In the boot screen, select the desired installation option. Press F4 then select the desired network protocol (NFS, HTTP, FTP, or SMB). Provide the server's address and the path to the installation media. The installation retrieves the installation data from the source specified. The installation then proceeds normally.

## 3.4 The Boot Screen

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

#### Installation

The normal installation mode. All modern hardware functions are enabled.

### Installation—ACPI Disabled

If the normal installation fails, this might be due to the system hardware not supporting ACPI (advanced configuration and power interface). If this seems to be the case, use this option to install without ACPI support.

### Installation—Local APIC Disabled

If the normal installation fails, this might be due to the system hardware not supporting local APIC (Advanced Programmable Interrupt Controllers). If this seems to be the case, use this option to install without local APIC support.

If you are not sure, try one of the following options first: *Installation—ACPI Disabled* or *Installation—Safe Settings*.

### Installation—Safe Settings

Boots the system with the DMA mode (for CD-ROM drives) and power management functions disabled. Experts can also use the command line to enter or change kernel parameters.

Installation options from the menu disable only the most problematic functions. If you need to disable or set other functions, use the *Boot Options* prompt. Find detailed information about kernel parameters at <http://en.opensuse.org/Linuxrc>.

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

F1

Get context-sensitive help for the active element of the boot screen.

F2

Select the display language for the installation. The default language is English.

F3

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

F4

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

F5

Press this key to tell the system that you have an optional disk with a driver update for SUSE Linux Enterprise. With *File*, load drivers directly from CD before the installation starts. If you select *Yes*, you are prompted to insert the update disk at the appropriate point in the installation process. The default option is *No*—not to load a driver update.

A few seconds after starting the installation, SUSE Linux Enterprise loads a minimal Linux system to run the installation procedure. To see what is going on during the boot process, press Esc to see the messages and copyright notices. At the end of the loading process, the YaST installation program starts. After a few more seconds, the screen should display the graphical installer. The actual installation of SUSE Linux Enterprise begins at this point.

---

**TIP: Installation without a Mouse**

If the installer does not detect your mouse correctly, use Tab for navigation, arrow keys to scroll, and Enter to confirm a selection.

---

## 3.5 Language

YaST and SUSE Linux Enterprise in general can be configured to use different languages according to your needs. The language selected here is also used for the keyboard layout. In addition, YaST uses the language setting to guess a time zone for the system clock. These settings can be modified later along with the selection of secondary languages to install on your system.

You can change the language later during installation in the *Installation Summary*, described in [Section 3.10, “Installation Summary”](#) (page 23). For information about language settings in the installed system, see the SUSE Linux Enterprise Server documentation available at <http://www.novell.com/documentation/sles10>.

## 3.6 License Agreement

Read the license agreement that is displayed on screen thoroughly. If you agree to the terms, choose *Yes, I Agree to the License Agreement* and click *Next* to confirm your

selection. If you do not agree to the license agreement, you cannot install SUSE Linux Enterprise and the installation terminates.

## 3.7 System Analysis

After a system analysis where YaST tries to find other installed systems or an already existing SUSE Linux Enterprise system on your machine, YaST displays the installation modes available:

### *New installation*

Select this option to start a new installation from scratch.

### *Update an existing system*

Select this option to update to a newer version.

### *Other*

This option provides an opportunity to abort installation and boot or repair an installed system instead. To boot an already installed SUSE Linux Enterprise, select *Boot Installed System*.

To repair an installed system that fails to boot, select *Repair Installed System*. Find a description of the system repair options in SUSE Linux Enterprise Server documentation.

---

### **NOTE: Updating an Installed System**

Updating is only possible if an older SUSE Linux Enterprise system is already installed. If no SUSE Linux Enterprise system is installed, you can only perform a new installation.

---

You can choose to install the SUSE Linux Enterprise add-on together with your base system during the initial installation process. To include the SUSE Linux Enterprise Point of Service add-on, select *Include Add-On Products from Separate Media* and click *Next*. In the next dialog, click *Add* and select *CD* as the source type. The added source for add-on media is displayed in the overview.

---

**NOTE: Installing SUSE Linux Enterprise Point of Service**

It is recommended to install SUSE Linux Enterprise Point of Service together with SUSE Linux Enterprise base system. If you want to install the SUSE Linux Enterprise Point of Service add-on on top of an already installed system, use *Software > Add-On Product*.

---

## 3.8 Time Zone

In this dialog, select your region and time zone from the lists. During installation, both are preselected according to the selected installation language. Choose between *Local Time* and *UTC (GMT)* for *Hardware Clock Set To*. The selection depends on how the BIOS hardware clock is set on your machine. If it is set to GMT, which corresponds to UTC, your system can rely on SUSE Linux Enterprise to switch from standard time to daylight saving time and back automatically. Click *Change* to set the current date and time. When finished, click *Next* to continue the installation.

## 3.9 Server Selection

---

**NOTE: Installing the SUSE Linux Enterprise Point of Service Add-On**

This step is available with the SUSE Linux Enterprise Point of Service add-on added during installation as described in [Section 3.7, “System Analysis”](#) (page 21).

---

Select a server type. Choose one of the following:

*Administration Server Installation*

Standalone Administration Server that will not be used to build Point of Service images.

*Branch Server Installation*

All the additional packages needed for a Branch Server.

*Image Server Installation*

Packages needed for image building.

If you want to install more than one server on one system or include other packages, choose *Detailed Selection* and click *Select* for more options.

## 3.10 Installation Summary

After a thorough system analysis, YaST presents reasonable suggestions for all installation settings. The options that sometimes need manual intervention in common installation situations are presented in the *Overview* tab. Find more special options in the *Expert* tab. To modify the suggestions, click *Change* and select the category to change. After configuring any of the items presented in these dialogs, you are always returned to the summary window, which is updated accordingly.

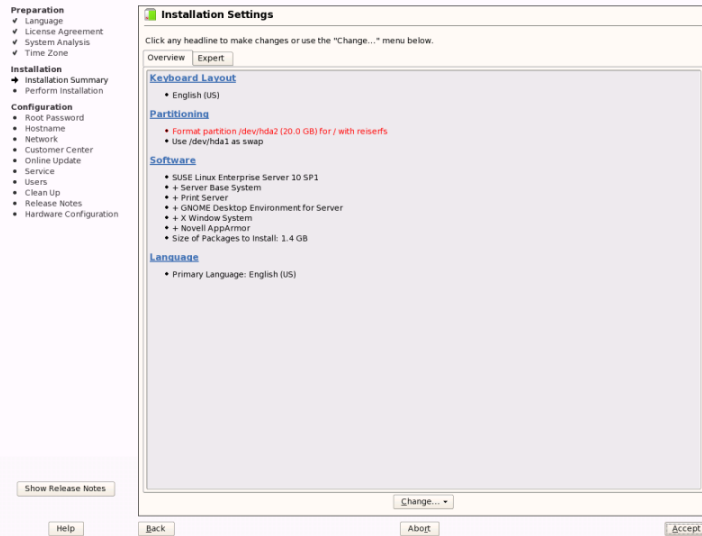
---

### TIP: Resetting the Installation Summary to the Default

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

---

**Figure 3.1** *Installation Settings*



## 3.10.1 Keyboard Layout

To change the keyboard layout, select *Keyboard Layout*. By default, the layout corresponds to the language chosen for installation.

Select the keyboard layout from the list. Use the *Test* field at the bottom of the dialog to check if you can enter special characters of that layout correctly. When finished, click *Accept* to return to the installation summary.

## 3.10.2 Partitioning

In most cases, YaST proposes a reasonable partitioning scheme that can be accepted without change. YaST can also be used to customize the partitioning, but only experienced users should change partitioning.

When you select the partitioning item in the suggestion window for the first time, the YaST partitioning dialog displays the proposed partition settings. To accept these settings, click *Accept Proposal*.

To make small changes in the proposal, select *Base Partition Setup on This Proposal* and adjust partitioning in the next dialog. For completely different partitioning, select *Create Custom Partition Setup*. In the next dialog, choose the disk to partition or *Custom Partitioning*.

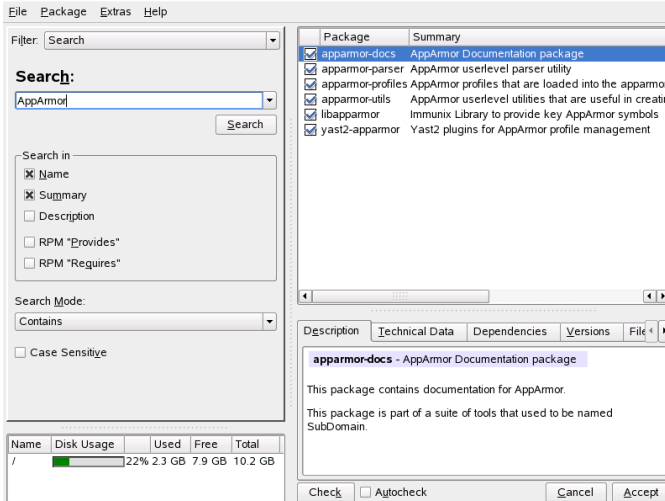
The partitioning scheme proposed should have sufficient disk space. If implementing your own partitioning scheme, consider the following recommendations concerning the requirements for different system types.

## 3.10.3 Software

SUSE Linux Enterprise contains a number of software packages for various application purposes. Click *Software* in the suggestion window to start the software selection and modify the installation scope according to your needs. Select your categories from the list in the middle and see the description in the right window. Each category contains a number of software packages that meet most requirements for that category. For more detailed selection of software packages to install, select *Details* to switch to the YaST Package Manager.

You can also install additional software packages or remove software packages from your system at any time later. For more information, refer to .

**Figure 3.2** *Installing and Removing Software with the YaST Package Manager*



## 3.10.4 Language

To change the system language or to configure support for secondary languages, select *Language*. Select the language from the list. The primary language is used as the system language. To have support for other languages, select these languages as secondary languages. .

## 3.10.5 The Expert Configuration

The *Overview* tab in the *Installation Settings* dialog provides only basic options. If you are an advanced user and want to configure booting or change the time zone or default runlevel, select the *Expert* tab. It shows the following additional entries not contained on the *Overview* tab:

## System

This dialog presents all the hardware information YaST could obtain about your computer. Select any item in the list and click *Details* to see detailed information about the selected item. Also add PCI IDs to device drivers with this dialog.

## Add-On Products

The added source for add-on media appears in the overview. Before you start the installation of the SUSE Linux Enterprise, add, remove, or modify add-on products here if needed.

## Booting

During installation, YaST proposes a boot configuration for your system. Normally, you can leave these settings unchanged. However, if you need a custom setup, modify the proposal for your system.

## Time Zone

This is the same as the configuration shown earlier in installation. See [Section 3.8, “Time Zone”](#) (page 22) for details.

## Default Runlevel

SUSE Linux Enterprise can boot to different runlevels. Normally there should be no need to change anything here, but if necessary set the default runlevel with this dialog.

# 3.11 Performing the Installation

After making all installation settings, click *Accept* in the suggestion window to begin the installation. Confirm with *Install* in the dialog that opens. The installation usually takes between 15 and 30 minutes, depending on the system performance and the software selected. As soon as all packages are installed, YaST boots into the new Linux system, after which you can configure the hardware and set up system services.

Some software can require the license confirmation. If your software selection includes such software, YaST displays a license confirmation dialog after you click *Accept*. To install the software, read the license and click *I Agree*. If you do not agree with the license, click *I Disagree*. The software then is not installed on your system.

# 3.12 Configuration of the Installed System

The system is installed now but not configured for use. No users, hardware, or services are configured. If the installation fails in one of the step of this stage, the configuration part restarts from the beginning. The installation itself is not repeated.

First, provide a password for the account of the system administrator (the `root` user). You can then configure your Internet access and network connection. With a working Internet connection, you can perform an update of the system as part of the installation. You can also configure an authentication server for centralized user administration in a local network. Finally, configure the hardware devices connected to the machine.

## 3.12.1 Root Password

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

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

SUSE Linux Enterprise can use the DES, MD5, or Blowfish encryption types for passwords. The default encryption type is Blowfish. To change the encryption type, click *Expert Options > Encryption Type* and select the new type.

## 3.12.2 Hostname

The hostname is the computer's name in the network. The domain name is the name of the network. A hostname and domain are proposed by default. If your system is part of a local network or should be accessible from the Internet, the domain name used

here must be that expected by the network or Internet. For a system in a local network, the hostname should be unique in the network.

In many networks, the system receives its hostname over DHCP, in which case you should not modify the name. Instead select *Change Hostname via DHCP*.

To be able to access your system using this hostname, select *Write Hostname to /etc/hosts*. This assigns the IP address 127.0.0.2 to the name, both with and without the domain.

To change hostname settings at any time after installation, use YaST *Network Devices > Network Card*.

## 3.12.3 Network

By default, *Traditional Method without NetworkManager Applet* is enabled. If desired, you can also use NetworkManager to manage all your network devices. However, the traditional method is the preferred option for server solutions.

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

As well as device configuration, configure some other network settings in this step:

### Firewall Configuration

When you connect to a network, a firewall is started automatically on the configured interface. The configuration proposal for the firewall is updated automatically every time the configuration of the interfaces or services is modified. To adapt the automatic settings to your own preferences, click *Change > Firewall*. In the dialog that opens, determine whether the firewall should be started. If you do not want the firewall to be started, select the appropriate option and exit the dialog. To start and configure the firewall, click *Next* for a series of dialogs similar to those described in SUSE Linux Enterprise Server documentation.

### IPv6

By default the IPv6 support is enabled. To disable it, click *Disable IPv6*.

## VNC Remote Administration

To administer your machine remotely by VNC, click *Change > VNC Remote Administration*, enable remote administration, and open the port in the firewall. If you have multiple network devices and want to select on which to open the port, click *Firewall Details* and select the network device. You can also use SSH, a more secure option, for remote administration.

## Proxy

If you have a proxy server in your network to control access to the Internet, enter the server name and all other required information to enable access to the Internet.

---

### **TIP: Resetting the Network Configuration to the Defaults**

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

---

After configuring an Internet connection, you can test it. For this purpose, YaST establishes a connection to the SUSE Linux Enterprise server and downloads the latest release notes. Read them at the end of the installation.

To start the test, select *Yes, Test Connection to the Internet* and click *Next*. In the next dialog, view the progress of the test and the results. If the test fails, click *Back* to return in the previous dialog and correct the configuration or skip the test. If you need more information about the test process, click *View Logs*.

If you do not want to test the connection at this point, select *No, Skip This Test* then *Next*. This also skips downloading release notes, configuring the customer center, and updating online.

If you have multiple network interfaces in your system, verify that the the desired card is used to connect to the Internet. To do so, click *Change device*.

## 3.12.4 Customer Center

To get technical support and product updates, first register and activate your product. *Novell Customer Center Configuration* provides assistance for doing so.

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

In *Include for Convenience*, select whether to obtain some of the necessary information from your system. This simplifies the registration process. To keep your installation sources valid, select *Regularly Synchronize with Customer Center*. This option checks your installation sources and adds new available sources or removes obsolete sources. It does not touch manually added sources. Additionally, it resends your hardware information if *Hardware Information* is activated, which can make new hardware-specific sources available. To see what is required to register your system or what happens with your data, use *Details*.

## 3.12.5 Online Update

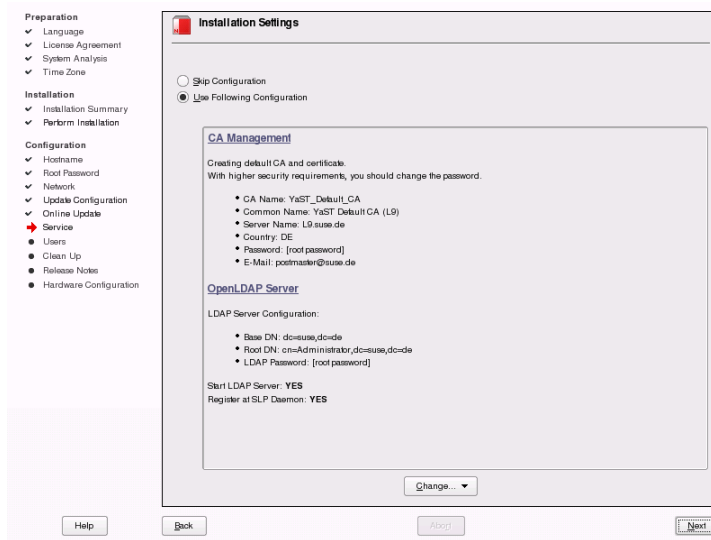
If the Novell Customer Center has not been configured, the next step is the user configuration. See [Section 3.12.7, “Users”](#) (page 32). For detailed instructions for to perform an online update after the installation, see . SUSE Linux Enterprise Server documentation

If YaST was able to connect to the SUSE Linux Enterprise servers, select whether to perform a YaST online update. If there are any patched packages available on the servers, download and install them now to fix known bugs or security issues.

## 3.12.6 Services

After testing the Internet connection and downloading the first updates, a dialog opens in which to enable and configure two important network services. See [Figure 3.3, “Proposed Setup for Network Services”](#) (page 31).

**Figure 3.3** Proposed Setup for Network Services



## CA Management

The purpose of a CA (certificate authority) is to guarantee a trust relationship among all network services communicating with each other. Without a CA, you can secure server communications with SSL and TLS separately for each individual service. By default, a CA is created and enabled during the installation.

## OpenLDAP Server

You can run an LDAP service on your host to have a central facility manage a range of configuration files. Typically, an LDAP server handles user account data, but with SUSE Linux Enterprise it can also be used for mail, DHCP, and DNS data. By default, an LDAP server is set up during the installation. If you decide against the use of an LDAP server, the YaST mail server module does not work because it depends on LDAP functionality. However, you can still set up a mail server on your system with the help of the *Mail Transfer Agent* module.

If preferred, you can skip this configuration proposal for now. After the installation is finished, configure and start the same services with the help of YaST.

---

**TIP: Resetting the Service Configuration to Defaults**

Restore the defaults by clicking *Change > Reset to Defaults*. This discards any changes made.

---

## 3.12.7 Users

If network access was configured successfully during the previous steps of the installation, you now have the following possibilities to manage user administration method on your system:

### Local (/etc/passwd)

Users are administered locally on the installed host. This is a suitable option for stand-alone workstations. User data is managed by the local file `/etc/passwd`. All users who are entered in this file can log in to the system even if no network is available.

If YaST found a former version of SUSE Linux Enterprise or another system using `/etc/passwd`, it offers the possibility to 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 click *OK*.

### LDAP

Users are administered centrally on an LDAP server for all systems in the network.

### NIS

Users are administered centrally on a NIS server for all systems in the network.

### Windows Domain

SMB authentication is often used in mixed Linux and Windows networks.

---

**NOTE: Content of the Authentication Menu**

If you use the custom package selection and one or more authentication methods are missing from the menu, the required packages probably are not installed.

---

You can also add additional user accounts or change the user authentication method in the installed system. For detailed information about user management, see SUSE Linux Enterprise Server documentation.

Along with the selected user administration method, you can use Kerberos authentication. This is essential for integrating your SUSE Linux Enterprise to an Active Directory domain, which is described in SUSE Linux Enterprise Server documentation. To use Kerberos authentication, select *Set Up Kerberos Authentication*.

## 3.12.8 Clean Up

This step does not require any user interaction. The installation program launches the SuSEconfig script to write the system configuration. Depending on the CPU and the amount of memory, this process can take some time.

## 3.12.9 Release Notes

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

## 3.12.10 Hardware Configuration

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

You can skip any peripheral devices and configure them later, as described in SUSE Linux Enterprise Server documentation. To skip the configuration, select *Skip Configuration* and click *Next*.

However, you should configure the graphics card right away. Although the display settings as configured by YaST should be generally acceptable, most users have very strong preferences as far as resolution, color depth, and other graphics features are

concerned. To change these settings, select the respective item and set the values as desired. To test your new configuration, click *Test the Configuration*.

---

### **TIP: Resetting Hardware Configuration to Defaults**

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

---

## **3.12.11 Completing the Installation**

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

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

## 3.13 Graphical Login

SUSE Linux Enterprise is now installed. Unless you enabled the automatic login function or customized the default runlevel, you should see the graphical login on your screen in which to enter a username and password to log in to the system. If automatic login is activated, the desktop starts automatically.



# Securing Your Setup

A SUSE® Linux Enterprise Point of Service setup includes various components that should be secured against intentional and unintentional tampering with the data and against software misbehavior. Securing your setup involves several different aspects:

## Physical Server Security

First and foremost, every server component of the SUSE Linux Enterprise Point of Service setup must be secured against unauthorized access. Physically isolating the servers from other machines is just one aspect of providing physical security. For details, refer to [Section 4.1, “Physical Server Security”](#) (page 38).

## Network Security

All servers connected with each other over potentially insecure networks, take the Admin Server and the Branch Servers for example, need to be secured against unauthorized access via the networks they are connected to. For details, refer to [Section 4.2, “Network Security”](#) (page 38).

## Data Security

Both the Admin and the Branch Server contain vital data that needs to be protected to maintain a fully functional and secure setup. The most important part in this is securing the LDAP directory on the Admin Server that is used to maintain the system structure, configuration and deployment method for all Branch Servers and POS terminals, and other important data. For details on how to achieve this, refer to [Section 4.3, “Data Security”](#) (page 39).

## Application Security

Once physical, network and data security are provided, tighten the security of your setup even further by using AppArmor. AppArmor profiles are used to confine

applications and keep them from performing unnecessary file or directory accesses and this helps to make sure that every profiled application just does what it was designed to and not become a security risk itself. For more details on AppArmor usage on SUSE Linux Enterprise Point of Service, refer to [Section 4.4, “Application Security”](#) (page 41).

## 4.1 Physical Server Security

Your instance of SUSE Linux Enterprise Point of Service is set up in a highly secure corporate environment (using third-party security solutions and various other security measures), but you still need to make sure that nobody gains unauthorized physical access to your servers and can log in to them to tamper with your setups.

The following list provides a few basic security-related things you should bear in mind when creating your setup:

- Keep your servers in a separate server room that is accessible to only a few selected people or ideally just you.
- Separate your server room from the rest of your IT setup by requiring some sort of authentication before people can enter the room. Use any of the following: key cards, key codes, PIN numbers, finger print authentication, etc.
- Use BIOS and boot loader passwords to prevent anyone from manipulating the boot process of your servers.

## 4.2 Network Security

Even if your SUSE Linux Enterprise Point of Service network is secured against the Internet (using third-party security solutions and firewalls), secure your servers against unauthorized access from the inside:

- All servers should just allow (console) access by one account, by `root`, alone.
- Create one single user account through YaST, namely the `root` account.
- Do not export or import any file systems on these servers, i.e. do not allow NFS or Samba shares on your servers.

SUSE Linux Enterprise Point of Service itself provides some security against data manipulation via the network:

- LDAP-related network traffic can be configured via secure SSL/TLS channels.
- Image data is exchanged between servers via rsync and md5sums are calculated and checked to provide data integrity.

## 4.3 Data Security

The most vital data of your SUSE Linux Enterprise Point of Service setup is stored in the LDAP directory on the Administration Server. Whoever gains control over this setup data can manipulate the setup of any server or terminal in your setup. Therefore, limit the list of users with access to the LDAP directory to the bare minimum and make sure they obtain the least possible privileges only. Use LDAP Access Control Lists (ACL) as part of the LDAP server configuration to restrict access to your LDAP data.

The configuration of your OpenLDAP server is located under `/etc/openldap/slapd.conf`. For more information on how this configuration file is generated and maintained, refer to Section “`posInitLdap.sh`” (Appendix A, *Point of Service Scripts*, ↑Administration Guide).

ACLs allow you to specify separate access controls to different parts of the configuration. You can create different ACLs for the user password data, for the server configuration data, for the configuration of different locations and so forth.

Before creating ACLs, perform an analysis of users and privileges needed to run your configuration. These may depend on the type of setup you have chosen and may vary. As an example, let us assume you run the following setup:

- A central Administration Server managed by the global administrator role.
- Independent Branch Servers managed by local administrators.

Thus, you need to make sure that both your user configuration on the Administration Server and the ACLs in the LDAP server configuration reflect these roles and provide suitable privileges to these user roles without providing too many privileges.

The following example includes creating effective ACLs and a user setup as outlined above. Modify both the ACLs and the user configuration to match your own setup:

- 1 Create ACLs similar to the following and make sure you replace the example entries by the ones matching your setup. Ensure the more general rules are specified *after* the more specific ones. The first matching rule is evaluated and the following rules are ignored:

```
access to dn.base="" by * read ❶
access to * attrs=userPassword
    by anonymous auth
    by self write ❷
access to dn.regex="^.*(cn=.*,ou=.*,o=mycorp,c=us)$"
    by dn.regex="^.*, $1$" write
    by users read ❸
access to *
    by self write
    by users read ❹
```

- ❶ Allow read access to the Root-DSE.
  - ❷ Allow unauthenticated clients to use the `userPassword` attribute for authentication. Authenticated clients (users) are allowed to change their own password.
  - ❸ Allow access to any DN matching the regular expression. Using the `$`, you limit the matches to just those strings that contain nothing beyond the last character. All DN's matching the regular expression are granted write access, and authenticated users may read the objects, but not write to them.
  - ❹ Allow access to anything. Entries themselves may write to their entries, authenticated users may read them, but not modify the entries.
- 2 For each location, create a location user. For example, create a user for each branch location. This user is then granted (write) access to all LDAP data concerning his location, but cannot change the data of the other locations.

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
cn=east,ou=boston,o=mycorp,c=us --add --scPOSUser --cn EastBostonUser
--userPassword "secretPassword"
```

- 3 Now the `--user` option can be set to the following in all `posAdmin` commands concerning the `cn=east,ou=boston,o=mycorp,c=us` location:

```
--user cn=EastBostonUser,cn=east,ou=boston,o=mycorp,c=us
```

The default LDAP user can now be replaced by this user, especially for the `posInitBranchserver` command.

```
...
Enter the DN of the LDAP user for administration tasks [default:
cn=admin,o=mycorp,c=us]

cn=EastBostonUser,cn=east,ou=boston,o=mycorp,c=us
```

---

**TIP: For More Information**

For more details on the syntax of the `slapd.conf` configuration file and the ACLs, refer to the manual pages of `slapd.conf(5)`, `slapd.access(5)`, and `slapacl(8)`. The `slapacl` command allows you to verify that your ACLs work as planned.

---

## 4.4 Application Security

Any piece of software used in your setup probably contains some inherent security vulnerabilities which slip by mostly unnoticed as the respective functions may not be used in every day life. To protect your setup from these vulnerabilities, SUSE Linux Enterprise Server and SUSE Linux Enterprise Point of Service come with the AppArmor protection framework. AppArmor provides so-called profiles for some of the most important applications that specify which files these programs are allowed to read, write and execute. Using these profiles, you make sure that a program does what it is supposed to do.

Use AppArmor to protect each of your servers. If you need additional profiles, use the YaST AppArmor tools to generate new profiles. To learn more about AppArmor refer to the *Novell AppArmor Administration Guide* that is part of the SUSE Linux Enterprise documentation under <http://www.novell.com/documentation/sles10/>.



# Setting Up the Administration Server

The Administration Server is the central administration point for SUSE® Linux Enterprise Point of Service. All system information (system structure, the configuration and deployment method for each Branch Server and Point of Service terminal, image information, and so forth) is stored in an LDAP directory on the Administration Server. The Administration Server is also the central distribution point for the images required to boot and configure Point of Service terminals and can run the utilities required to build those images. Set up an Administration Server either with or without the image building software.

---

**NOTE: Creating an Image Building Server**

The utilities required to build Point of Service images can be installed with the Administration Server or you can install them on a dedicated image building server. For more information on creating a dedicated image building server, see [Chapter 6, \*Setting Up a Dedicated Image Building Server\*](#) (page 51).

---

## 5.1 Meeting the System Requirements

For a list of system requirements to set up an Administration Server, refer to [Section 2.1, “Administration Server”](#) (page 11).

## 5.2 Installing the Administration Server

To install the Administration Server, proceed as outlined in [Chapter 3, \*Installation with YaST\*](#) (page 15).

Determine which type of server to install:

- If you want to install a standalone Administration Server that will not be used to build Point of Service images, select the SLEPOS Admin Server software pattern.

This pattern installs all Administration Server packages to the server, but none of the image building packages.

- If you want to use the Administration Server to build Point of Service images, select the above mentioned pattern, the SLEPOS Image Server pattern, and the SLEPOS Images pattern.

This pattern installs all Administration Server packages to the server, plus the image building tools (KIWI and Image Creator) and image templates listed in [Table 5.1, “Image Building Components”](#) (page 44).

**Table 5.1** *Image Building Components*

Description	Location/Command
KIWI Binary	<code>/usr/sbin/kiwi</code>
YaST Image Creator	<code>yast2 image-creator</code>
SUSE Linux Enterprise Point of Service Image Templates	<code>/usr/share/kiwi/image/SLEPOS</code>
Image Description Trees	<code>/var/lib/SLEPOS/system/image _name</code>

Description	Location/Command
config.xml Template	/usr/share/kiwi/image/SLEPOS/image_template/config.xml

Complete the installation as usual and continue with the initialization of the LDAP directory.

## 5.3 Initializing the LDAP Directory

All system information (system structure, the configuration and deployment method for each Branch Server, available system images, and Point of Service terminal types) is stored in an LDAP directory on the Administration Server.

SUSE Linux Enterprise Point of Service uses the OpenLDAP directory service. The `posInitLdap` script defines the LDAP directory schema and the initial records for OpenLDAP.

### 5.3.1 Running `posInitLdap.sh`

The `posInitLdap` script defines the LDAP directory schema and the initial records for OpenLDAP. It cannot add a SUSE Linux Enterprise Point of Service LDAP directory to an existing openLDAP tree; it creates an entirely new LDAP directory tree.

To create the SUSE Linux Enterprise Point of Service LDAP directory for OpenLDAP:

- 1 After you have installed the SUSE Linux Enterprise Point of Service Administration Server, log in as `root` on the Administration Server.
- 2 Configure the firewall running on the Administration Server to allow traffic on the `ldap` and `ldaps` ports, 389 TCP/UDP and 636 TCP/UDP, respectively. Do this by using either the YaST firewall module (`yast2 firewall`) or the YaST command line (`yast firewall services add service=ldap,ldaps zone=EXT`).

3 Run `posInitLdap.sh`.

4 Specify your company name without spaces or special characters.

5 Specify your country abbreviation.

Use `de` for Germany, `us` for United States, `uk` for United Kingdom, and so forth.

6 Specify the LDAP administrator password. The password must be alphanumeric.

You are assigning the password for the LDAP directory administrator account. The Branch Server uses this account to access the LDAP directory and this account is required to use `posAdmin` to add objects to the LDAP directory.

7 Determine if you want to use SSL when the Branch Server connects to the LDAP directory on the Administration Server.

- Select Y to use an SSL connection when the Branch Server connects to the LDAP Directory.
- Select N to disable SSL.

---

### **IMPORTANT: Securing Your Server Communication**

Using SSL/TLS to secure the connections between Administration Server and Branch Servers is highly recommended.

---

`posInitLdap` creates the certificates and keys required to run SSL regardless of whether or not SSL is enabled. This allows you to switch to SSL at a later time if desired.

---

### **IMPORTANT: Regenerating SSL Certificates**

If you need to regenerate your SSL certificates at a later point in time, use the `posInitLdap.sh --r` command. This command generates new certificates and deletes the old ones.

---

The keys and certificates are located in the `/etc/SLEPOS/keys` directory on both the Administration and Branch Servers.

- 8 `posInitLdap` provides a summary of the LDAP directory data based on your input. If all data is correct, press Enter.

If there is something wrong with the input data, abort the installation by pressing Ctrl + C.

- 9 The script initializes the basic LDAP database structure and performs some tests, then displays a summary of the configuration and test results. When the tests are successfully completed, the script displays a success message. To complete the initialization, press Enter.

## 5.3.2 Verifying the LDAP Directory

After you run `posInitLdap`, the LDAP directory has been initialized on the Administration Server and the LDAP service is available. At this point, you should have a basic tree structure with a root, a Country container, and an Organization container.

You can verify that the LDAP structure is accessible using an `ldapsearch` command. Use a syntax similar to the first example when using SSL. For setups without SSL, use a syntax similar to the second example.

```
ldapsearch -x -H ldaps://administration_server_name -b o=mycorp,c=us -s base  
-D cn=admin,o=mycorp,c=us -w password
```

```
ldapsearch -x -H ldap://administration_server_name -b o=mycorp,c=us -s base  
-D cn=admin,o=mycorp,c=us -w password
```

---

### TIP: Setting the LDAP Debugging Level

Turn on a more verbose output for the `ldapsearch` command by enabling the debug option with `-d1`.

---

Before you create a Branch Server, you use the `posAdmin` command to create the LDAP objects required to configure the Branch Server and boot its Point of Service terminals. For detailed instructions on creating these objects, see [Section 7.2, “Creating Branch Server Objects in LDAP”](#) (page 56).

## 5.4 Creating Point of Service Images

Before you can deploy Point of Service terminals, you must first create image files that contain the operating system and application files required to boot the terminals.

SUSE Linux Enterprise Point of Service provides image templates that can be customized and generated using the Image Creator tool. When you select the Image Server during the Administration Server installation, the image creation utilities (Image Creator and KIWI) are installed on the Administration Server along with all the files and directories required to create Point of Service images. For a detailed, step-by-step introduction to building SUSE Linux Enterprise Point of Service images using Image Creator, refer to Chapter 6, *Building Images with the Image Creator Tool* (Administration Guide).

After you have created the images required for your Point of Service terminals, you must copy the images to the appropriate directories on the Administration Server so that the RSYNC service can transmit the images to the Branch Server. Depending on whether the Administration Server and the Image Building Server are on the same machine or whether the images are built on a dedicated Image Building Server, use the different copy procedures outlined in [Section 5.6, “Copying the System Image Files”](#) (page 49).

## 5.5 Copying the Boot Image Files

This section explains how to copy the default boot images (initrd and the Linux kernel file) to the appropriate directories on the Administration Server so they are ready to be transferred to the Branch Servers. If the images have been built on the same machine, use the following `cp` command or your favorite file browser (Konqueror or Nautilus):

- 1 Use the following command to copy the `initrd` file to the `/srv/SLEPOS/boot` directory as `initrd.gz` (type the command all on one line):

```
cp
/var/lib/SLEPOS/system/images/image_name/initrd-netboot-image_name.architecture-version.gz
/srv/SLEPOS/boot/initrd.gz
```

- 2 Use the following command to copy the kernel file to the `/srv/SLEPOS/boot` directory as `linux` (type the command all on one line):

```
cp
/var/lib/SLEPOS/system/images/image_name/initrd-netboot-image_name.architecture-version.kernel.kernel_version
/srv/SLEPOS/boot/linux
```

If the images have been built on a dedicated Image Building Server, use the `scp` command or the remote copy option of your file browser:

- 1 Use the following command to copy the `initrd` file to the `/srv/SLEPOS/boot` directory as `initrd.gz` (type the command all on one line):

```
scp
/var/lib/SLEPOS/system/images/image_name/initrd-netboot-image_name.architecture-version.gz
address_adminserver:/srv/SLEPOS/boot/initrd.gz
```

- 2 Use the following command to copy the kernel file to the `/srv/SLEPOS/boot` directory as `linux` (type the command all on one line):

```
scp
/var/lib/SLEPOS/system/images/image_name/initrd-netboot-image_name.architecture-version.kernel.kernel_version
address_adminserver:/srv/SLEPOS/boot/linux
```

## 5.6 Copying the System Image Files

System images must be located in the `/srv/SLEPOS/image` directory on the Administration Server. The boot image must be located in `/srv/SLEPOS/boot`. The Branch Servers can then download the image files and deploy them on Point of Service terminals. If the images have been built on the same machine, use the following `cp` command or your favorite file browser (Konqueror or Nautilus):

- 1 Use the following command to copy the system images to the `/srv/SLEPOS/image` directory (type the command all on one line):

```
cp
/var/lib/SLEPOS/system/images/image_name/image_name.architecture-version
/srv/SLEPOS/image/image_name.architecture-version
```

- 2 Use the following command to copy the corresponding MD5 checksum files to the `/srv/SLEPOS/image` directory (type the command all on one line):

```
cp
/var/lib/SLEPOS/system/images/image_name/image_name.architecture-version.md5
/srv/SLEPOS/image/image_name.architecture-version.md5
```

If the images have been built on a dedicated Image Building Server, use the `scp` command or the remote copy option of your file browser:

- 1 Use the following command to copy the system images to the `/srv/SLEPOS/image` directory (type the command all on one line):

```
scp
/var/lib/SLEPOS/system/images/image_name/image_name.architecture-version
address_adminserver:/srv/SLEPOS/image/image_name.architecture-version
```

- 2 Use the following command to copy the corresponding MD5 checksum files to the `/srv/SLEPOS/image` directory (type the command all on one line):

```
scp
/var/lib/SLEPOS/system/images/image_name/image_name.architecture-version.md5
address_adminserver:/srv/SLEPOS/image/image_name.architecture-version.md5
```

## 5.7 What's Next

If you need to install a dedicated Image Building Server, follow the instructions in [Chapter 6, \*Setting Up a Dedicated Image Building Server\*](#) (page 51) before you install your Branch Servers.

The next step is to set up your Branch Servers. Refer to the section corresponding to the type of Branch Server you want to install:

- [Chapter 7, \*Setting Up a Branch Server\*](#) (page 55)
- [Chapter 8, \*Setting Up an Admin/Branch Server Combo\*](#) (page 71)
- [Chapter 9, \*Setting Up a POSBranch Server\*](#) (page 83)

# Setting Up a Dedicated Image Building Server

Although a dedicated image building server requires an additional server on your SUSE® Linux Enterprise Point of Service network, it provides several advantages, particularly for large systems that manage a large number of Point of Service images. Providing a dedicated image building server offloads the processor and memory load required to generate images from the Administration Server and it protects the Administration Server and LDAP directory from any possible corruption or user errors that might occur while building Point of Service images.

## 6.1 Meeting System Requirements

For a list of system requirements to set up an Image Building Server, refer to [Section 2.2, “Image Building Server”](#) (page 11).

## 6.2 Installing a Dedicated Image Building Server

To install the Image Building Server, proceed as outlined in [Chapter 3, \*Installation with YaST\*](#) (page 15).

Install the following patterns:

SLEPOS Image Server

This pattern installs all the packages needed for image building.

## SLEPOS Images

This pattern installs the basic image templates for SLEPOS.

**Table 6.1** *Image Building Components*

Description	Location/Command
KIWI Binary	<code>/usr/sbin/kiwi</code>
YaST Image Creator	<code>yast2 image-creator</code>
SUSE Linux Enterprise Point of Service Image Templates	<code>/usr/share/kiwi/image/SLEPOS</code>
Image Description Trees	<code>/var/lib/SLEPOS/system/image _name</code>
<code>config.xml</code> Template	<code>/usr/share/kiwi/image/ SLEPOS/image_template/config .xml</code>

Complete the installation as usual and continue with copying the default boot images to the Administration Server. Set up your network boot images according to Chapter 6, *Building Images with the Image Creator Tool* (↑Administration Guide).

## 6.3 Creating Point of Service Images

With the image building server up and running, you can create system images required for your Point of Service terminals. Before doing so, however, you must copy the image source files from the CDs to the image building server and define their location. For a detailed, step-by-step introduction to building SUSE Linux Enterprise Point of Service images using Image Creator, refer to Chapter 6, *Building Images with the Image Creator Tool* (↑Administration Guide).

## 6.4 Copying the System Image Files to the Administration Server

After you have created the client images you need, you must copy the image files and their corresponding MD5 checksums from the image server to the `/srv/SLEPOS/image` directory on the Administration Server.

For detailed instructions, see [Section 5.6, “Copying the System Image Files”](#) (page 49).



# Setting Up a Branch Server

The Branch Server provides the network boot and system management infrastructure for the SUSE® Linux Enterprise Point of Service terminals as well as a generic system platform for in-store applications, such as database systems and back-ends for the Point of Service applications.

If you intend to set up a high-availability Branch Server, check out the Heartbeat Guide [<http://www.novell.com/documentation/sles10/pdfdoc/heartbeat/heartbeat.pdf>] for general information on Heartbeat.

If you are setting up an Admin/Branch Server combination, follow the instructions in [Chapter 8, \*Setting Up an Admin/Branch Server Combo\*](#) (page 71).

In the NLPOS9, a specialized POSBranch image was needed to setup a Branch Server running on Point of Service hardware. There is no need for such a specialized POSBranch image now. Branch server on POS hardware can be installed as a standard Branch Server.

## 7.1 Meeting System Requirements

For a list of system requirements to set up an Branch Server, refer to [Section 2.3, “Branch Server”](#) (page 12).

# 7.2 Creating Branch Server Objects in LDAP

Before you can configure and deploy a Branch Server, you must first create the necessary objects in the LDAP directory stored on the Administration Server. All `posAdmin.pl` calls must be executed on the Administration Server. These objects include:

- One or more *organizationalUnit* objects (Section 7.2.1, “Creating organizationalUnit Objects” (page 56)) to represent your organizational structure.
- An *scLocation* object (Section 7.2.2, “Creating an scLocation Object” (page 57)) for each site where a Branch Server is located.
- An *scServerContainer* (Section 7.2.3, “Adding an scServerContainer Object” (page 60)) to contain all the Branch Server objects for a given site.
- An *scBranchServer* object (Section 7.2.4, “Adding an scBranchServer Object” (page 61)) and its associated configuration objects for each Branch Server in your system.
- Additional objects (Section 7.2.7, “Creating Point of Service Terminal Objects” (page 65)) for the Point of Service terminals associated with each Branch Server.

---

## NOTE: LDAP Object Attributes

Each LDAP object has two types of attributes: must and may attributes. The must attributes are required for an object; the may attributes are optional. The tables in this section list only those may attributes that are relevant to SUSE Linux Enterprise Point of Service.

---

## 7.2.1 Creating organizationalUnit Objects

In a SUSE Linux Enterprise Point of Service system, Organizational Unit (*organizationalUnit*) objects are containers that typically represent regions, divisions, or branches within a company. These objects can be nested to visually represent the structure or organization of your company. Branch location objects are created in

organizationalUnit containers within the LDAP directory. Use only alphanumeric characters for ou objects.

Here is the posAdmin command syntax for adding an organizationalUnit object in LDAP (type the command all on one line):

```
posAdmin.pl --user dn_of_admin_user --password password --base base_context
--add --organizationalUnit --ou ou_name [--description `string`]
```

**Table 7.1, “Attributes for organizationalUnit Objects”** (page 57) summarizes the organizationalUnit object attributes.

**Table 7.1** *Attributes for organizationalUnit Objects*

Attribute	Type	Explanation
--ou ou_name	must	Specifies the name of the organizational unit. For example, --ou boston.
--description `string`	may	Contains a human-readable description of the object.

For example, the following command adds the boston organizational unit to the LDAP directory and gives it the description “main headquarters”:

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
o=mycorp,c=us --add --organizationalUnit --ou boston --description 'main
headquarters'
```

The LDAP context of the newly created organizationalUnit is the ou=boston,o=mycorp,c=us directory.

## 7.2.2 Creating an scLocation Object

An scLocation object typically is used to represent a branch office; that is, a site where a Branch Server and Point of Service terminals are located. scLocation containers are used to store information about the Branch Servers and the deployed Point of Service terminals. This and all other information that can be modified at the Branch Server should be stored or referenced in the Location containers to limit the need to grant write privileges to subtrees.

Here is the `posAdmin` command syntax to add an `scLocation` object in LDAP (type the command all on one line):

```
posAdmin.pl --user dn_of_admin_user --password password --base base_context
--add --scLocation --cn location_name --ipNetworkNumber network_address
--ipNetmaskNumber subnet_mask --scDhcpRange ip_address,ip_address
--scDhcpFixedRange ip_address,ip_address --scDefaultGw ip_address --scDynamicIp
TRUE | FALSE --scDhcpExtern TRUE | FALSE --scWorkstationBaseName string
--scEnumerationMask number [--associatedDomain ldap_context]
```

**Table 7.2, “Attributes for `scLocation` Objects”** (page 58) summarizes the command options which correspond to the `scLocation` object attributes.

**Table 7.2** *Attributes for `scLocation` Objects*

Attribute	Type	Explanation
<code>--cn location_name</code>	must	Specifies the common name of the location object.
<code>--ipNetworkNumber network_address</code>	must	Identifies the network address of the subnet of the branch. For example, 192.168.1.0.
<code>--ipNetmaskNumber subnet_mask</code>	must	Identifies the netmask of the subnet of the branch. For example, 255.255.255.0.
<code>--scDhcpRange ip_address,ip_address</code>	must	Specifies the dynamic IP address range of the subnet's DHCP server. This is needed to register the Point of Service terminals. It is a comma-separated value pair. For example, 192.168.1.10, 192.168.1.50.
<code>--scDhcpFixedRange ip_address,ip_address</code>	must	Specifies the DHCP server's fixed IP address range reserved for the Point of Service terminals. It is also a comma-separated value pair, such as 192.168.1.51, 192.168.1.150.

<b>Attribute</b>	<b>Type</b>	<b>Explanation</b>
<code>scDhcpExtern</code>	Must	Allow an external DHCP server to be used instead of setting up your own on the Branch Server (TRUE or FALSE).
<code>--scDefaultGw ip_address</code>	must	Identifies the default gateway for this location. This is normally a router to the corporate wide area network.
<code>--scDynamicIp TRUE   FALSE</code>	must	Enables (TRUE) or disables (FALSE) the dynamic IP address range of the DHCP server.
<code>--scWorkstationBaseName string</code>	must	Specifies the base name of the Point of Service terminals of a branch. The base name, in combination with the <code>scEnumerationMask</code> , is used to create a unique name for each terminal, which is then associated with an IP address in the <code>scDhcpFixedRange</code> . For example, if the DHCP fixed range starts at <code>192.168.1.51</code> , the <code>scWorkstationBaseName</code> is <code>CR</code> , and the <code>scEnumerationMask</code> is <code>000</code> , the first terminal to register gets the name <code>CR001</code> and the IP address <code>192.168.1.51</code> , the next terminal is named <code>CR002</code> and gets the IP address <code>192.168.1.52</code> , and so on.
<code>--scEnumerationMask number</code>	must	Specifies the last portion of the Point of Service terminal name. Refer to the explanation of <code>scWorkstationBaseName</code> above.
<code>--associatedDomain ldap_context</code>	may	This optional entry configures the DNS domain and the domain part of the

Attribute	Type	Explanation
		hostnames of the Point of Service terminals to be in the stated domain. If this entry is left empty (the default), the domain is derived from the LDAP structure of the <code>scLocation</code> entry DN. With this entry, a different domain can be chosen.

For example, the following command adds the Harbor `scLocation` to the LDAP directory, sets the IP addresses and DHCP ranges to the indicated values, and specifies a base name of `CR` and an enumeration mask of `000` (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
ou=boston,o=mycorp,c=us --add --scLocation --cn harbor --ipNetworkNumber
192.168.1.0 --ipNetmaskNumber 255.255.255.0 --scDhcpRange
192.168.1.10,192.168.1.50 --scDhcpFixedRange 192.168.1.51,192.168.1.151
--scDefaultGw 192.168.1.254 --scDynamicIp TRUE --scDhcpExtern FALSE
--scWorkstationBaseName CR --scEnumerationMask 000
```

## 7.2.3 Adding an `scServerContainer` Object

Before you can add the `scBranchServer` object to an `scLocation` object, you must define an `scServerContainer`.

Here is the `posAdmin` command syntax for adding an `scServerContainer` object in LDAP (type the command all on one line):

```
posAdmin.pl --user dn_of_admin_user --password password --base base_context
--add --scServerContainer --cn object_name
```

For example, the following command adds an `scBranchServer` object named `server` to the LDAP directory:

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
cn=east,ou=boston,o=mycorp,c=us --add --scServerContainer --cn server
```

## 7.2.4 Adding an scBranchServer Object

The next step is to add an `scBranchServer` object to the new `scServerContainer`. The `scBranchServer` object stores configuration information that is specific to each Branch Server. It is located in the LDAP tree via an `scLocation` object. There must be an `scBranchServer` object for every Branch Server in the SUSE Linux Enterprise Point of Service system.

---

### IMPORTANT: Defining the Branch Server Hostname

The location of the `scBranchServer` object in the LDAP directory must correspond to the hostname defined for the Branch Server during installation. For example, if the hostname is `bs.east.boston.mycorp.us`, the dn of the `scBranchServer` object would be `cn=bs, cn=server, cn=east, ou=boston, o=mycorp, c=us`. You must create the `scBranchServer` object and its supporting organizational structure before you can run `posInitBranchserver` and deploy the Branch Server. For more information on defining the server hostname during installation, see [Section 3.12.3, “Network”](#) (page 28).

---

Here is the `posAdmin` command syntax for adding an `scBranchServer` object in LDAP (type the command all on one line):

```
posAdmin.pl --user dn_of_admin_user --password password --base base_context
--add --scBranchServer --cn branch_server_name
```

As a may attribute, you can define the reference hardware with the `--scRefServerDn` option, specifying a pointer (Distinguished Name) to the global directory.

For example, the following command adds a Branch Server object named `bs1` in the server container:

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
cn=server,cn=east,ou=boston,o=mycorp,c=us --add --scBranchServer --cn bs1
```

## 7.2.5 Defining the Branch Server Hardware

The `scBranchServer` object must contain at least one defined `scNetworkcard` object. You can define other hardware objects as necessary. For a standard Branch Server setup, you would need to configure two network interfaces: one network interface (e.g. `eth0`) facing the Administration Server's public network and a second one (e.g. `eth1`) facing the Branch Server's private network.

Here is the `posAdmin` command syntax for adding a network interface card to the Branch Server object (type the command all on one line):

```
posAdmin.pl --user dn_of_admin_user --password password --base base_context
--add --scNetworkcard --scDevice device_name --ipHostNumber ip_address
```

**Table 7.3, “Attributes for `scNetworkcard` Objects”** (page 62) summarizes the command options which correspond to the `scNetworkcard` object attributes.

**Table 7.3** *Attributes for `scNetworkcard` Objects*

Attribute	Type	Explanation
<code>--scDevice</code> <i>device_name</i>	must	Specifies the name of network device of the card. For example, <code>eth0</code> or <code>eth1</code> . This network card faces the internal network which is used for running the Point of Service machines.
<code>--ipHostNumber</code> <i>ip_address</i>	must	Specifies the IP address assigned to the card. For example, <code>192.168.1.1</code> . This card faces the internal network which is used for running the Point of Service machines.
<code>--macAddress</code>	may	Identifies the MAC address of the network interface card.
<code>--scModul</code>	may	Specifies the name of the Linux kernel module for the network interface card.

Attribute	Type	Explanation
<code>--scModulOption</code>	may	Specifies the module options of the Linux kernel module for the network interface card.
<code>--ipNetmaskNumber</code>	may	Adds the netmask belonging to the IP address assigned to the network interface card, if the <code>ipHostNumber</code> is not inside the defined subnet of the location.

For example, the following command adds a network interface card with a static IP address from the defined subnet (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
cn=bs,cn=server,cn=east,ou=boston,o=mycorp,c=us --add --scNetworkcard
--scDevice eth0 --ipHostNumber 192.168.1.1
```

## 7.2.6 Defining the Branch Server Services

The `scBranchServer` also contains objects representing services such as DHCP and DNS. As a minimum, you should define the required DHCP, DNS, and TFTP.

Here is the `posAdmin` command syntax for defining an `scService` object in LDAP (type the command all on one line):

```
posAdmin.pl --user dn_of_admin_user --password password --base base_context
--add --scService --cn service_name --ipHostNumber ip_address --scDnsName
dns_name --scServiceName string --scServiceStartScript filename
--scServiceStatus TRUE | FALSE
```

**Table 7.4, “Attributes for `scService` Objects”** (page 63) provides a description of `scService` attributes.

**Table 7.4** *Attributes for `scService` Objects*

Attribute	Type	Explanation
<code>--cn service_name</code>	must	Specifies the common name of the service.

Attribute	Type	Explanation
<code>--ipHostNumber</code> <i>ip_address</i>	must	Specifies the IP address of the Branch Server hosting the service. This IP address belongs to the internal network which is used for running the Point of Service machines.
<code>--scDnsName</code> <i>dns_name</i>	must	Specifies the DNS name of the service.
<code>--scServiceName</code> <i>string</i>	must	Specifies the name of the service. For example: dhcp, dns, or tftp.
<code>--scServiceStartScript</code> <i>filename</i>	must	The name of the init script in /etc/init.d. For example, atftpd for the tftp service.
<code>--scServiceStatus</code> TRUE   FALSE	must	The service status. TRUE or FALSE are possible values.

The following examples demonstrate how to add the DHCP, DNS, and TFTP services (type the commands all on one line).

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
cn=bs,cn=server,cn=east,ou=boston,o=mycorp,c=us --add --scService --cn dhcp
--ipHostNumber 192.168.1.1 --scDnsName dhcp --scServiceName dhcp
--scServiceStartScript dhcpd --scServiceStatus TRUE
```

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
cn=bs,cn=server,cn=east,ou=boston,o=mycorp,c=us --add --scService --cn dns
--ipHostNumber 192.168.1.1 --scDnsName dns --scServiceName dns
--scServiceStartScript named --scServiceStatus TRUE
```

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
cn=bs,cn=server,cn=east,ou=boston,o=mycorp,c=us --add --scService --cn tftp
--ipHostNumber 192.168.1.1 --scDnsName tftp --scServiceName tftp
--scServiceStartScript atftpd --scServiceStatus TRUE
```

## 7.2.7 Creating Point of Service Terminal Objects

Before you can boot the Point of Service terminals associated with a Branch Server, you must create additional objects in the branch portion of the LDAP directory. These include an `scCashRegister` object and its associated configuration objects for each type of Point of Service terminal in your system, and `scPosImage` objects for the system image files you want the Branch Server to distribute to Point of Service terminals.

For instructions on how to create these objects, see [Section 10.2, “Creating the Required LDAP Objects”](#) (page 86).

## 7.3 Installing the Branch Server

To install the Branch Server, proceed as outlined in [Chapter 3, \*Installation with YaST\*](#) (page 15) and install the Branch Server pattern.

Complete the installation as usual and continue with the Branch Server configuration.

---

### **WARNING: Securing the Data on the Branch Server**

Protect the sensitive data stored on the Branch Server as outlined in [Chapter 4, \*Securing Your Setup\*](#) (page 37).

---

## 7.4 Configuring the Branch Server

This section describes the Branch Server configuration with the `posInitBranchServer.sh` script.

- 1 Before starting the configuration script, ensure that the Branch Server can find its object in the LDAP directory.

You must have created the `scBranchServer` object and its supporting organizational structure before you can run `posInitBranchserver.sh` to configure the Branch Server. For more information, see [Section 7.2, “Creating Branch Server Objects in LDAP”](#) (page 56).

The Branch Server's hostname must resolve to the IP address defined in the `--ipHostNumber` attribute of the `scNetworkcard` object; for example, `192.168.2.1`. Otherwise, the Branch Server cannot find the `scBranchServer` object in the LDAP directory. To ensure this resolution, add the following line to the Branch Server's `/etc/hosts` file:

```
ip_address_of_scNetworkcard fully_distinguished_name hostname
```

For example,

```
192.168.2.1 bs1.boston.mycorp.com bs1
```

---

### **IMPORTANT: Adjusting the Firewall Configuration**

Check the setup of the Branch Server's network interfaces in the YaST firewall configuration module: make sure all interfaces have a zone selected properly.

---

**2** Execute `posInitBranchserver.sh` at the Branch Server console.

**3** Specify your company name without spaces or special characters.

**4** Specify your country abbreviation.

Use `de` for Germany, `uk` for United Kingdom, `us` for United States, and so forth.

**5** Specify the IP address of the Administration Server.

Set the value according to the IP address you assigned when you configured the Administration Server.

**6** The script attempts to connect to the Administration Server. If it fails, you are prompted again for the company name, country name, and password.

Otherwise, the script tries to determine the Branch Server's IP address, hostname, and domain name as it is defined in the LDAP database. If it fails, you are prompted for the Branch Server's IP address.

If the Branch Server configuration is successful, the script displays the Branch Server's name, IP address, and domain name, along with a success message.

If using LDAP over SSL, proceed as follows:

- 6a** Make sure the following entry is added to the `/etc/hosts` file of your Branch Server:

```
ip_adminserver adminserver_hostname.adminserver_domainname
```

- 6b** When asked to provide the Administration Server's name and IP address, make sure you specify the fully distinguished name of the Administration Server, i.e. *adminserver\_hostname.adminserver\_domainname*

This data can be obtained by running `hostname` and `hostname --domain` on the Administration Server.

- 7** Verify that the necessary LDAP objects have been created by using an `ldapsearch` command. For example (setup without SSL):

```
ldapsearch -x -H ldap://administration_server_name -b base_context -s base -D dn_of_admin_user -w password
```

For setups with SSL, use:

```
ldapsearch -x -H ldaps://administration_server_name -b base_context -s base -D dn_of_admin_user -w password
```

---

**TIP: Setting the LDAP Debugging Level**

Turn on a more verbose output for the `ldapsearch` command by enabling the debug option with `-d1`.

---

## 7.5 Downloading Images from the Administration Server

After the Branch Server is up and running, you can run the `possyncimages.pl` script to download the Point of Service images that have been created from the Administration Server to the `/srv/tftpboot` directories on the Branch Server.

- 1** Verify the `scPosImage` object settings for the Point of Service images in the `/srv/tftpboot/image` directory.

Create the `scPosImage` objects and set the `scPosImageVersion` attribute to `Active` before you boot the Point of Service terminals, so you can keep track of the most recent image version before the images are copied. Manually remove old images from the Administration Server to avoid pulling the same image twice. For more information on setting the `scPosImageVersion` attribute to `Active`, see Section “Activating Images” (Chapter 4, *Using posAdmin to Manage the LDAP Directory*, ↑Administration Guide).

- 2 Run `possyncimages.pl` at the Branch Server console to download the Point of Service images.

The `possyncimages.pl` script can also be used to update Point of Service images on the Branch Server. However, to implement image version changes, you should also activate the version changes inside the corresponding `scPosImage` objects in the LDAP directory to keep track of the most recent image versions and manually remove old images from the Administration Server to avoid pulling the same image twice.

- 3 Verify the result of the `possyncimages.pl` command by checking the contents of the following Branch Server directories:

- `/srv/tftpboot/boot`
- `/srv/tftpboot/image`

For more information on the Administration and Branch Server directory structure, see Appendix B, *SUSE Linux Enterprise Point of Service Files and Directory Structure* (↑Administration Guide).

## 7.6 Starting the Core Script

Start the core script (`posleases2ldap`) as a daemon process on the Branch Server. The core script is responsible for registering any new Point of Service terminals at the LDAP directory and transferring image install notification data to the LDAP directory on the Administration Server.

- To verify that `posleases2ldap` is currently running, execute the following command:

```
rcposleases2ldap status
```

- To manually start the `posleases2ldap` service, execute the following command:

```
rcposleases2ldap start
```

- To ensure the Branch Server automatically starts the core script at boot time, execute the following command:

```
insserv posleases2ldap
```

You are now ready to deploy the Point of Service terminals. For more information on this process, see [Chapter 10, \*Deploying Point of Service Terminals\*](#) (page 85).



# Setting Up an Admin/Branch Server Combo

# 8

For single store installations, the Administration and Branch Servers can be deployed on a single server. The Administration/Branch Server combination provides full SUSE® Linux Enterprise Point of Service system functionality (Administration Server, Branch Server, and Image Building Server) from a single server.

The Admin/Branch Server combination is supported only for self-contained installations. No additional Branch Servers can connect to the Admin/Branch Server. You can, however, create a two-node heartbeat cluster by installing two Admin/Branch Servers and configuring one as the primary and the other as the secondary.

---

## **TIP: High Availability—For More Information**

For more information on High Availability, refer to the Heartbeat Guide [<http://www.novell.com/documentation/sles10/pdfdoc/heartbeat/heartbeat.pdf>] that is available from <http://www.novell.com/documentation/sles10/>.

---

## 8.1 Meeting System Requirements

For a list of system requirements to set up an Administration/Branch Server, refer to [Section 2.4, “Administration/Branch Server Combination”](#) (page 12).

## 8.2 Installing an Admin/Branch Server Combo

To install the Administration Server, proceed as outlined in [Chapter 3, \*Installation with YaST\*](#) (page 15).

Install the following patterns:

### SLEPOS Admin Server

This pattern installs all the packages needed for an Administration Server.

### SLEPOS Branch Server

This pattern installs all the additional packages needed for a Branch Server.

### SLEPOS Image Server and SLEPOS Image

These patterns install all packages needed for an Image Building Server including templates for SLEPOS images.

**Table 8.1** *Image Building Components*

Description	Location/Command
KIWI Binary	<code>/usr/sbin/kiwi</code>
YaST Image Creator	<code>yast2 image-creator</code>
SUSE Linux Enterprise Point of Service Image Templates	<code>/usr/share/kiwi/image/SLEPOS</code>
Image Description Trees	<code>/var/lib/SLEPOS/system/image _name</code>
<code>config.xml</code> Template	<code>/usr/share/kiwi/image/ SLEPOS/image_template/config .xml</code>

You are now ready to initialize the SUSE Linux Enterprise Point of Service LDAP directory.

## 8.3 Initializing the LDAP Directory

All system information (system structure, the configuration and deployment method for the Branch Server, available system images, and Point of Service terminal types) is stored in an LDAP directory on the Admin/Branch Server.

SUSE Linux Enterprise Point of Service uses the OpenLDAP directory service. The `posInitLdap` script defines the LDAP directory schema and the initial records for OpenLDAP.

### 8.3.1 Running `posInitLdap.sh`

The `posInitLdap` script defines the LDAP directory schema and the initial records for OpenLDAP. It cannot add a SUSE Linux Enterprise Point of Service LDAP directory to an existing openLDAP tree; it creates an entirely new LDAP directory tree.

To create the SUSE Linux Enterprise Point of Service LDAP directory for OpenLDAP:

- 1 After you have installed the SUSE Linux Enterprise Point of Service Administration Server, log in as `root` on the Administration Server.
- 2 Configure the firewall running on the Administration Server to allow traffic on the `ldap` and `ldaps` ports, 389 TCP/UDP and 636 TCP/UDP, respectively. Do this by using either the YaST firewall module (`yast2 firewall`) or the YaST command line (`yast firewall services add service=ldap,ldaps zone=EXT`).
- 3 Run `posInitLdap.sh`.
- 4 Specify your company name without spaces or special characters.
- 5 Specify your country abbreviation.  
Use `de` for Germany, `us` for United States, `uk` for United Kingdom, and so forth.
- 6 Specify the LDAP administrator password. The password must be alphanumeric.

You are assigning the password for the LDAP directory administrator account. The Branch Server uses this account to access the LDAP directory and this account is required to use `posAdmin` to add objects to the LDAP directory.

- 7 Determine if you want to use SSL when the Branch Server connects to the LDAP directory on the Administration Server.
  - Select Y to use an SSL connection when the Branch Server connects to the LDAP Directory.
  - Select N to disable SSL.

---

### **IMPORTANT: Securing Your Server Communication**

Using SSL/TLS to secure the connections between Administration Server and Branch Servers is highly recommended.

---

`posInitLdap` creates the certificates and keys required to run SSL regardless of whether or not SSL is enabled. This allows you to switch to SSL at a later time if desired.

---

### **IMPORTANT: Regenerating SSL Certificates**

If you need to regenerate your SSL certificates at a later point in time, use the `posInitLdap.sh --r` command. This command generates new certificates and deletes the old ones.

---

The keys and certificates are located in the `/etc/SLEPOS/keys` directory on both the Administration and Branch Servers.

- 8 `posInitLdap` provides a summary of the LDAP directory data based on your input. If all data is correct, press Enter.

If there is something wrong with the input data, abort the installation by pressing `Ctrl + C`.

- 9 The script initializes the basic LDAP database structure and performs some tests, then displays a summary of the configuration and test results. When the tests are successfully completed, the script displays a success message. To complete the initialization, press Enter.

## 8.3.2 Verifying the LDAP Directory

After you run `posInitLdap` or `posInitEdir`, the LDAP directory has been initialized on the Admin/Branch Server and the LDAP service is available. At this point, you should have a basic tree structure with a root, a Country container, and an Organization container.

You can verify that the LDAP structure is accessible using an `ldapsearch` command. Use a syntax similar to the first example when using SSL. For setups without SSL, use a syntax similar to the second example.

```
ldapsearch -x -H ldaps://administration_server_name -b o=mycorp,c=us -s base  
-D cn=admin,o=mycorp,c=us -w password
```

```
ldapsearch -x -H ldap://administration_server_name -b o=mycorp,c=us -s base  
-D cn=admin,o=mycorp,c=us -w password
```

---

### TIP: Setting the LDAP Debugging Level

Turn on a more verbose output for the `ldapsearch` command by enabling the debug option with `-d1`.

---

## 8.4 Creating the Required LDAP Objects

Next, you must use the `posAdmin` command to create the LDAP objects required to configure the Branch Server and boot its Point of Service terminals.

- Branch Objects
  - One or more `organizationalUnit` objects to represent your organizational structure.
  - An `scLocation` object for the site where the Admin/Branch Server is located.
  - An `scServerContainer` to contain the BranchServer objects.
  - An `scBranchServer` object and its associated configuration objects for the Branch Server.

You must create the `scBranchServer` object and its supporting organizational structure before you can run `posInitBranchserver.sh` to configure the Branch Server.

The Common Name (`cn`) of the `scBranchServer` object in the LDAP directory must match the hostname defined when you installed the Admin/Branch Server. For example, if the hostname is `bs1`, specify that for the `--cn` attribute of the `scBranchServer` object. For more information on defining the Branch Server hostname during installation, see [Section 3.12.3, “Network”](#) (page 28).

- An `scCashRegister` (see [Section 10.2.1, “Creating an scCashRegister Object”](#) (page 87)) object and its associated configuration objects for each type of Point of Service terminal in your system:

You must create `scCashRegister` and its associated objects before you can boot the Point of Service terminals.

- `scHarddisk` or `scRamDisk`
- `scConfigFileTemplate` (optional)
- `scConfigFileSyncTemplate` (optional)
- An `scPosImage` objects for each system image file that you want the Branch Server to distribute to Point of Service terminals.

---

### IMPORTANT

Create the `scPosImage` objects and set the `scPosImageVersion` attribute to `Active` before you boot the Point of Service terminals to keep track of the current image version. For more information on setting the `scPosImageVersion` attribute to `Active`, see [Section 10.2.7, “Activating Images”](#) (page 96).

---

For detailed instructions on creating these objects, see [Section 7.2, “Creating Branch Server Objects in LDAP”](#) (page 56).

## 8.5 Copying the Default Boot Images

This section explains how to copy the default boot images (initrd and the Linux kernel file) to the appropriate directories on the Admin/Branch Server so they are ready to be distributed to the Point of Service terminals.

- 1 Use the following command to copy the default initrd file to the `/srv/SLEPOS/boot` directory as `initrd.gz` (type the command all on one line):

```
cp
/var/lib/SLEPOS/system/image_template-image/initrd-image_type-version-date.gz
/srv/SLEPOS/boot/initrd.gz
```

- 2 Use the following command to copy the default kernel file to the `/srv/SLEPOS/boot/` directory as `linux` (type the command all on one line):

```
cp
/var/lib/SLEPOS/system/image_template-image/initrd-image_type-version-date.kernel.kernel_version
/srv/SLEPOS/boot/linux
```

## 8.6 Creating Point of Service Images

Before you can deploy Point of Service terminals, you must first create image files that contain the operating system and application files required to boot the terminals. Before doing so, however, you must copy the image source files from the CDs to the Admin/Branch Server and define their location.

- 1 Copy the image source files to your Admin/Branch Server using either the `POSCDTool` script or the `POSCopyTool` script.

For detailed instructions, see Chapter 5, *Managing Image Source Files* (↑Administration Guide).

- 2 Define the location of the image source files in the `config.xml` file used by KIWI and Image Creator.

For detailed instructions, see Section “Generating `AdminServer.conf` or `Distribution.xml`” (Chapter 5, *Managing Image Source Files*, ↑Administration Guide).

### 3 Build the Point of Service image files.

For more information on this procedure, see Chapter 6, *Building Images with the Image Creator Tool* (↑Administration Guide).

## 8.7 Copying the System Image Files

After you have created the system images you need, you must copy the image files and their corresponding MD5 checksum files to the `/opt/SLES/POS/rsync/image` directory. The Admin/Branch Server can then distribute the image files to the Point of Service terminals.

---

### IMPORTANT

Both the system image files and their MD5 checksum files must be located in the `/opt/SLES/POS/rsync/image` directory on the Admin/Branch Server before they can be distributed to Point of Service terminals when they are booted up.

---

The boot image files must be located in `/opt/SLES/POS/rsync/boot`, as explained in [Section 8.5, “Copying the Default Boot Images”](#) (page 77).

## 8.8 Configuring the Branch Server

This section describes the Branch Server configuration with the `posInitBranchServer.sh` script.

### 8.8.1 Running the Initialization Script

- 1 Before starting the configuration script, ensure that the Branch Server can find its object in the LDAP directory.

You must have created the `scBranchServer` object and its supporting organizational structure before you can run `posInitBranchserver.sh` to configure the Branch Server. For more information, see [Section 7.2.1, “Creating organizationalUnit Objects”](#) (page 56).

The Branch Server's hostname must resolve to the IP address defined in the `--ipHostNumber` attribute of the `scNetworkcard` object; for example, 192.168.2.1. Otherwise, the Branch Server cannot find the `scBranchServer` object in the LDAP directory. To ensure this resolution, add the following line to the Branch Server's `/etc/hosts` file:

```
ip_address fully_distinguished_name hostname
```

For example,

```
192.168.2.1 bs1.boston.mycorp.com bs1
```

- 2 Execute `posInitBranchserver.sh` at the Branch Server console.
- 3 Specify your company name without spaces or special characters.
- 4 Specify your country abbreviation.

Use `de` for Germany, `uk` for United Kingdom, `us` for United States, and so forth.

- 5 Specify the IP address of the Administration Server.

---

## NOTE

Because in this case the Administration and Branch Server are on the same machine, they have the same IP address. You can specify the machine's actual IP address or use loopback (127.0.0.1) or `localhost`.

---

- 6 The script attempts to connect to the Administration Server. If it fails, you are prompted again for the company name, country name, and password.

Otherwise, the script tries to determine the Branch Server's IP address, hostname, and domain name as it is defined in the LDAP database. If it fails, you are prompted for the Branch Server's IP address.

If the Branch Server configuration is successful, the script displays the Branch Server's name, IP address, and domain name, along with a success message.

If using LDAP over SSL, proceed as follows:

- 6a** Make sure the following entry is added to the `/etc/hosts` file of your Branch Server:

```
ip_adminserver adminserver_hostname.adminserver_domainname
```

- 6b** When asked to provide the Administration Server's name and IP address, make sure you specify the fully distinguished name of the Administration Server, i.e. *adminserver\_hostname.adminserver\_domainname*

This data can be obtained by running `hostname` and `hostname --domain` on the Administration Server.

- 7** Verify that the necessary LDAP objects have been created by using an `ldapsearch` command. For example (setup without SSL):

```
ldapsearch -x -H ldap://administration_server_name -b base_context -s base -D dn_of_admin_user -w password
```

For setups with SSL, use:

```
ldapsearch -x -H ldaps://administration_server_name -b base_context -s base -D dn_of_admin_user -w password
```

## 8.8.2 Copying Images to the tftpboot Directories

After the Branch Server has been configured, you can run the `possyncimages.pl` script to copy the Point of Service images you have created to the `/srv/tftpboot/` directories.

- 1** Verify the `scPosImage` object settings for the Point of Service images in the `/srv/tftpboot/image` directory.

Create `scPosImage` objects and set the `scPosImageVersion` attribute to `Active` before you boot the Point of Service terminals to be able to track the current image versions. Manually remove old images from the Administration Server to avoid pulling the same image twice. For more information on setting the `scPosImageVersion` attribute to `Active`, see Section “Activating Im-

ages” (Chapter 4, *Using posAdmin to Manage the LDAP Directory*, ↑Administration Guide).

- 2 Run `possyncimages.pl` to copy the Point of Service images to the `/srv/tftpboot` directories on the Branch Server.
- 3 Verify the results of running the script by checking the contents of the following directories:
  - `/srv/tftpboot/boot`
  - `/srv/tftpboot/image`

For more information on the Administration and Branch Server directory structure, see Appendix B, *SUSE Linux Enterprise Point of Service Files and Directory Structure* (↑Administration Guide).

The `possyncimages.pl` script can also be used to update Point of Service images on the Branch Server. To keep track of image version changes, activate the version changes inside the corresponding `scPosImage` objects in the LDAP directory. Manually remove old images from the Administration Server to avoid pulling the same image twice.

## 8.8.3 Starting the Core Script

Start the core script (`posleases2ldap`) as a daemon process on the Admin/Branch Server.

- To verify that `posleases2ldap` is currently running, execute the following command:

```
rcposleases2ldap status
```

- To manually start the `posleases2ldap` service, execute the following command:

```
rcposleases2ldap start
```

- To ensure that the Admin/Branch Server automatically starts the core script at boot time, execute the following command:

```
insserv posleases2ldap
```

You are now ready to boot the Point of Service terminals. For more information on this process, see [Section 10.4, “Booting the Point of Service Terminal”](#) (page 102).

# Setting Up a POSBranch Server

For stores where the Branch Server is only running the SUSE® Linux Enterprise Point of Service infrastructure (that is, the Branch Server is running no additional applications), the Branch Server can be deployed as a control terminal running on Point of Service hardware.

In the NLPOS9, a specialized POSBranch image was needed to setup a POSBranch server. There is no need for such a specialized POSBranch image now. Branch server on POS hardware can be installed as a standard Branch Server, by installing SUSE Linux Enterprise Server 10 SP1 and SUSE Linux Enterprise Point of Service 10 add-on directly on a POS Machine. You can install any additional packages you may need to run applications on the POSBranch server (like Java or FireFox) via the YaST Software Manager. For more information about setting up a Branch Server see [Chapter 7, \*Setting Up a Branch Server\*](#) (page 55)

---

## **WARNING: Securing a POSBranch Server**

Because the POSBranch server contains sensitive information, it should be secured. We recommend that you close unused ports and allow only the root user to have access to the server console. For more information on securing your SUSE Linux Enterprise Point of Service setup, refer to [Chapter 4, \*Securing Your Setup\*](#) (page 37).

---



# Deploying Point of Service Terminals

# 10

Point of Service terminals are the end point in the SUSE® Linux Enterprise Point of Service architecture. They provide customer service functions such as Point of Service terminals or bank teller workstations.

## 10.1 Creating Point of Service Images

Before you can deploy Point of Service terminals, you must first create image files that contain the operating system, application files, and system settings required to boot the terminals.

SUSE Linux Enterprise Point of Service provides image templates that can be customized and generated on an Administration Server or a dedicated Image Building Server using Image Creator. For information on the available image templates, see [Section 1.2.1, “Types of Images”](#) (page 3).

To create the Point of Service images required to deploy your Point of Service terminals, you must do the following:

- 1 Copy the image source files to your Image Building Server. For detailed instructions, see Section “Copying the SUSE Linux Enterprise Point of Service CDs” (Chapter 5, *Managing Image Source Files*, ↑Administration Guide).
- 2 Define the location of the image source files. For detailed instructions, see Section “Generating AdminServer.conf or Distribution.xml” (Chapter 5, *Managing Image Source Files*, ↑Administration Guide).

### 3 Build the Point of Service image files.

## 10.2 Creating the Required LDAP Objects

Before you can boot the Point of Service terminals, use `posAdmin.pl` to create the following objects in the LDAP directory (see also Chapter 4, *Using posAdmin to Manage the LDAP Directory* (↑Administration Guide)):

- An `scCashRegister` object and its associated configuration objects for each type of Point of Service terminal in your system:
  - `scHarddisk` or `scRamDisk`
  - `scConfigFileTemplate` (optional)
  - `scConfigFileSyncTemplate` (optional)
- An `scPosImage` object for each client image file that you want the Branch Server to distribute to Point of Service terminals.

Create the `scPosImage` objects and set the `scPosImageVersion` attribute to `Active` before you boot the Point of Service terminals. The Point of Service terminals require an `scPosImage` object with an active `scPosImageVersion` attribute before they can download the corresponding physical image from the Branch Server at boot time. For more information on setting the `scPosImageVersion` attribute to `Active`, see [Section 10.2.7, “Activating Images”](#) (page 96).

With `posAdmin.pl`, you can add, remove, and modify Point of Service terminal hardware assets such as Point of Service terminals, hard disks, network interface cards, and configuration files with the use of reference objects in the LDAP directory. Hardware reference objects are typically located in the global container in the LDAP directory.

---

**NOTE: LDAP Attributes**

Each LDAP object has two types of attributes: must and may attributes. The must attributes are the minimum requirements for an object; the may attributes are optional.

---

## 10.2.1 Creating an `scCashRegister` Object

The first step to register new Point of Service hardware is to define the name and model type of the Point of Service terminal. The `scCashRegister` object stores information about Point of Service hardware. Typically, you should define a `scCashRegister` object for each type of terminal used on the SUSE Linux Enterprise Point of Service system; however, if a Point of Service terminal does not have an `scCashRegister` object for its specific hardware type, it uses the configuration defined in the default `scCashRegister` object.

---

**NOTE: Defining a Default Value**

To create a default `scCashRegister` object, define the object's `scCashRegisterName` attribute as default (see Table “`posAdmin` Options for Creating `scCashRegister` Objects” (↑Administration Guide)).

---

The `scCashRegister` objects are stored in the Global container so they can be accessed by all Branch Servers.

The following list shows the `scCashRegister` attributes:

`--cn` (must)

The common name of the Point of Service terminal.

`--scCashRegisterName` (must)

The model name of the Point of Service terminal; for example, `SurePos500`.

If this field is defined as “default”, the current `scCashRegister` object is used as the default Point of Service configuration. If a Point of Service terminal does not have an `scCashRegister` object for its specific hardware type, it will use the configuration defined in the default `scCashRegister` object.

---

## IMPORTANT: Defining Unique Values

Define only one default `scCashRegister` object in the Global container. Also, `scCashRegisterName` values must be unique; do not create more than one `scCashRegister` object with the same model name.

---

`--scPosImageDn` (may)

The distinguished name of the default system image defined for this Point of Service terminal type.

---

## NOTE: Overriding Default Image

A specific system image can be defined in the `scWorkstation` object. The setting in the `scWorkstation` object overrides the default image defined in the `scCashRegister` object. For information on this procedure, see [Section 10.2.8, “Assigning an Image to a Point of Service Terminal”](#) (page 97).

---

`--scDiskJournal` (may)

A Boolean field that is set to `TRUE` if journaling should be enabled. Journaling is only added on diskful machines. The default is `FALSE`.

`--scPosDeltaImageDN` (may)

The *Distinguished Name* (DN) pointing to the Delta Image associated with this cash register.

The following example adds a default `scCashRegister` object below the global container (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret
--base cn=global,o=mycorp,c=us --add --scCashRegister
--cn crtype3 --scCashRegisterName FlatCR2000
--scPosImageDn cn=browser,cn=global,o=mycorp,c=us --default
```

## 10.2.2 Creating an `scRamDisk` Object

The `scRamDisk` object stores configuration information for a Point of Service terminal RAM disk. If no hard disk is available, you must configure a RAM disk for the Point of Service terminal.

The following list shows the `scRamDisk` attributes:

`--base (must)`

The base distinguished name of the Hardware Reference object. For example, `cn=crtype3, cn=global, o=mycorp, c=us`.

`--cn (must)`

The common name of the device. For example, `ram`.

`--scDevice (must)`

The RAM disk device.

The device `/dev/ram0` cannot be used because it is used for the initial RAM disk. Therefore, we recommend using `/dev/ram1`.

The RAM device should not be confused with the hard disk device, which uses a partition table.

The following example adds an `scRamDisk` object below the Hardware Reference object, `crtype3` (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret
--base cn=crtype3,cn=global,o=mycorp,c=us --add --scRamDisk
--cn ram --scDevice /dev/ram1
```

## 10.2.3 Creating an `scHarddisk` Object

The `scHarddisk` object stores configuration information for a Point of Service terminal hard disk.

The following list shows the `scHarddisk` attributes:

`--base (must)`

The base distinguished name of the Hardware Reference object. For example, `cn=crtype3, cn=global, o=mycorp, c=us`.

`--cn (must)`

The common name of the device. For example, `hda`.

`--scDevice (must)`

The device of the hard disk. For example, `/dev/hda`.

`--scHdSize` (must)

The size of the hard disk in megabytes.

`--scPartitionsTable` (must)

A semicolon-separated (';') list of partition entries. Each entry has four parameters: the size in megabytes, the partition type ID (82 for swap, 83 for a Linux partition), the mount point, and the file system (swap or ext3).

The following example adds an `scHarddisk` object below the `scCashRegister` object, `crtype3` (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret --base
cn=crttype3,cn=global,o=mycorp,c=us --add --scHarddisk --cn hda --scDevice
/dev/hda --scHdSize 9000 --scPartitionsTable "1000 82 swap swap;4000 83 /
ext3;"
```

## 10.2.4 Creating an `scConfigFileTemplate` Object

The `scConfigFileTemplate` is an optional object used when you run services, such as the X Window system, that require hardware-dependent configuration files. An `scConfigFileTemplate` object contains the configuration file data that a Point of Service terminal needs to run a given service.

When you define the `scConfigFileTemplate` object, you designate a source configuration file (`--scConfigFileData`). `posAdmin` extracts the configuration data from the source file and stores it in the `scConfigFileTemplate` object. When a Point of Service terminal registers with a Branch Server (or when you run `posAdmin.pl --updateconfig` or `posldap2crconfig.pl --dumpall`), the Branch Server retrieves the configuration data in the `scConfigFileTemplate` object to create a configuration file in `/srv/tftpboot/CR/MAC_address/` directories on the Branch Server.

Using TFTP, the configuration file is then distributed from the Branch Server to the appropriate Point of Services terminals at boot time.

---

## NOTE

The `scCashRegister` or `scPosImage` object under which the `scConfigFileTemplate` object is created determines which Point of Service terminals receive the configuration file.

If the `scConfigFileTemplate` object is defined under an `scCashRegister` object, all terminals that correspond to the type defined in the `scCashRegister` object receive the configuration file defined in the `scConfigFileTemplate` object.

If the `scConfigFileTemplate` object is defined under an `scPosImage` object, all terminals that load the system image that corresponds to the `scPosImage` object receive the configuration file defined in the `scConfigFileTemplate` object.

---

The following list shows the `scConfigFileTemplate` attributes:

`--cn` (must)

The common name of the configuration file.

`--scMust` (must)

This flag is used to enable or disable the configuration file. Allowed values are `TRUE` to enable or `FALSE` to disable the configuration file.

`--scConfigFile` (must)

Specifies the path where the configuration file is installed on the Point of Service terminal. For example, `/etc/ntp.conf` or `/etc/X11/xorg.conf`.

`--scBsize` (must)

Specifies the block size for the TFTP download.

`--scConfigFileData` (must)

The source path of the configuration file. For example, `/tmp/xorg.conf.mydata`.

`--description` (may)

A short description

`--scConfigFileParser` (may)  
Name of parserFunction to apply

`--scConfigMd5` (may)  
MD5 sum of config file

The following example adds a `scConfigFileTemplate` object below the Hardware Reference object, `crtype3` (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret
--base cn=crtype3,cn=global,o=mycorp,c=us --add --scConfigFileTemplate
--cn XF86Config --scConfigFile /etc/X11/XF86Config --scBsize 1024
--scConfigFileData /mydata/xorg.conf.1234567
```

## 10.2.5 Creating an `scConfigFileSyncTemplate` Object

The `scConfigFileSyncTemplate` is an optional object used when you run services, such as the X Window system, that require hardware-dependent configuration files. This object points to the configuration file that a Point of Service terminal needs to run a given service. This object differs from `scConfigFileTemplate` objects because the configuration data is not stored in the object; rather, the object points to a configuration file outside the LDAP directory.

When a Point of Service terminal registers with a Branch Server (or when you run `posAdmin.pl --updateconfig` or `posldap2crconfig.pl --dumpall`), the Branch Server uses RSYNC to transfer the configuration file designated in the `scConfigFileSyncTemplate` object from the `/srv/SLEPOS/config/` directory on the Administration Server to `/srv/tftpboot/CR/MAC_address/` directories on the Branch Server.

---

### IMPORTANT

Any configuration files referenced in the `scConfigFileSyncTemplate` object must be located in the `/srv/SLEPOS/config/` directory on the Administration Server.

---

Using TFTP, the configuration file is then distributed from the Branch Server to the appropriate Point of Service terminals at boot time.

---

## NOTE

The `scCashRegister` or `scPosImage` object under which the `scConfigFileSyncTemplate` object is created determines which Point of Service terminals receive the configuration file.

If the `scConfigFileSyncTemplate` object is defined under an `scCashRegister` object, all terminals that correspond to the type defined in the `scCashRegister` object receive the configuration file designated in the `scConfigFileSyncTemplate` object.

If the `scConfigFileSyncTemplate` object is defined under an `scPosImage` object, all terminals that load the system image that corresponds to the `scPosImage` object receive the configuration file designated in the `scConfigFileSyncTemplate` object.

---

The following list shows the `scConfigFileSyncTemplate` attributes:

- `--cn`  
The common name of the configuration file.
- `--scMust`  
This flag is used to enable or disable the configuration file. Allowed values are `TRUE` to enable or `FALSE` to disable the configuration file.
- `--scConfigFile`  
Specifies the path where the configuration file is installed on the Point of Service terminal; for example, `/etc/ntp.conf` or `/etc/X11/xorg.conf`.
- `--scBsize`  
Specifies the block size for the TFTP download.
- `--scConfigFileLocalPath`  
The local source path of the configuration file; for example, `/srv/SLEPOS/config/xorg.conf.mydata`.

`--description` (may)

A short description

`--scConfigMd5` (may)

MD5 sum of config file

The following example adds an `scConfigFileSyncTemplate` object below the hardware reference object, `crtype3` (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret \  
  --base cn=crtype3,cn=global,o=mycorp,c=us \  
  --add --scConfigFileSyncTemplate --cn XF86Config \  
  --scConfigFile /etc/X11/XF86Config --scMust TRUE --scBsize 1024 \  
  --scConfigFilePath /srv/SLEPOS/config/xorg.conf.1234567
```

## 10.2.6 Creating `scPosImage` Objects

Images are managed in LDAP with `scPosImage` objects. Each `scPosImage` object stores information about an image stored on the Administration Server. Every system image that you want to distribute to Point of Service terminals must have a corresponding `scPosImage` object in the LDAP directory.

You must create the `scPosImage` objects and set the `scPosImageVersion` attribute to `Active` before you boot the Point of Service terminals. The Point of Service terminals require an `scPosImage` object with an active `scPosImageVersion` attribute before they can download the corresponding physical image from the Branch Server at boot time.

The `scPosImage` objects that correspond to the system images you want to distribute to Point of Service terminals are typically organized within `Distribution Container` objects under the `Global` container in the LDAP tree.

---

### **NOTE: Boot Images and `scPosImage` Objects**

Boot images do not have `scPosImage` objects; they are referenced in the `scInitrName` attribute in the `scDistributionContainer` object.

---

After the installation and configuration of the SUSE Linux Enterprise Point of Service, an `scPosImage` object for the Minimal image is automatically added to the Default `Distribution Container`. This default LDAP entry is intended to serve as an example

and should not be deleted. You must manually add an `scPosImage` object for each system image you want to distribute to Point of Service terminals.

The following list shows the `scPosImage` attributes:

`--base (must)`

The base distinguished name of the `scPosImage` object; for example, `cn=global,o=mycorp,c=us`.

`--cn (must)`

The common name of the system image; for example, `mydesktop`.

`--scImageName (must)`

The name of the system image; for example, `mydesktop`.

`--scPosImageVersion (must)`

The version number of the system image, followed by the flag `passive` or `active`; for example, `2.3.10; active`. The version number and the flag are semicolon-separated (";"). Possible combinations of this attribute are described in [Table 10.1, “Image Version Examples”](#) (page 96).

`--scDhcpOptionsRemote (must)`

The boot option of the Point of Service terminal. The mandatory value is `/boot/pxelinux.0`.

`--scDhcpOptionsLocal (reserved)`

This attribute is reserved for future extension of SUSE Linux Enterprise Point of Service and is not used at this time.

`--scImageFile (must)`

The filename of the image, which the terminal will download from the Branch Server; for example, `mydesktop`.

`--scBsize (must)`

Specifies the block size for the TFTP download of the system image; for example, 8192. Possible values are: 4096 (4 KB) for image sizes less than 128 MB, 8192 (8 KB) for image sizes less than 256MB, 16384 (16 KB) for image sizes less than 512 MB and 32768 (32 KB) for image sizes less than 1GB. You must select a TFTP block size of 32 KB for the full-featured Desktop image, because there is a limitation of the block counter for TFTP.

`--scConfigFile (may)`

Specifies the path where the configuration file is installed on the Point of Service terminal; for example, `/etc/ntp.conf` or `/etc/X11/xorg.conf`.

The following example adds a `scPosImage` object below the global container for a modified Browser system image (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret
--base cn=global,o=mycorp,c=us --add --scPosImage --cn myBrowser
--scImageName myBrowser --scPosImageVersion "2.0.21;active"
--scDhcpOptionsRemote /boot/pxelinux.0 --scDhcpOptionsLocal LOCALBOOT
--scImageFile myBrowser --scBsize 8192 --scConfigFile /etc/X11/xorg.conf
```

## 10.2.7 Activating Images

Each image can be available in several versions, as shown in [Table 10.1, “Image Version Examples”](#) (page 96). The `scPosImageVersion` attribute in each `scPosImage` object must be set to either `active` or `passive`. After images have been downloaded by the Branch Server, the Branch Server selects the highest active version, according to the rules in [Table “Possible Values for the `scPosImageVersion` Attribute”](#) (↑Administration Guide).

**Table 10.1** *Image Version Examples*

Value	Explanation
1.1.2	The version number is set to 1.1.2, but this client image is disabled in LDAP and cannot be used for a new Point of Service terminal, even when the <code>scCashRegister</code> object that corresponds to the Point of Service terminal matches the <code>scPosImageDn</code> attribute entry.
1.1.2;passive	Same behavior as above.
1.1.2;active	This system image with version 1.1.2 is enabled.
1.1.2;active 1.1.3;active 1.1.5;active	All image versions are enabled. The latest image version is used for download to the Point of Service terminal.

Value	Explanation
1.1.2;passive 1.1.3;active 1.1.5;passive	Only image version 1.1.3 is enabled.

To activate a registered image, set its `scPosImageVersion` attribute to active. This is done with `posAdmin` using the `modify` and `multivalued` options as follows (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret \
--modify --scPosImage --multival \
--scPosImageVersion '2.3.10;passive=>2.3.10;active' \
--DN cn=browser,cn=default,cn=global,o=mycorp,c=us
```

To activate the new image version on a Branch Server, run `posldap2crconfig.pl` with the `--dumpall` option and `possyncimages.pl` as follows:

```
posldap2crconfig.pl --dumpall possyncimages.pl
```

## 10.2.8 Assigning an Image to a Point of Service Terminal

You can assign a specific image to a Point of Service terminal through its `scWorkstation` object.

For example, the following command assigns desktop image 2.3.10 to the CR001 `scWorkstation` object in the `boston1` container (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret
--modify --scWorkstation
--scPosImageDn cn=desktop,cn=global,o=mycorp,c=us
--scPosImageVersion 2.3.10
--DN cn=CR001,ou=boston1,ou=boston,o=mycorp,c=us
```

When you explicitly assign an image in the `scWorkstation` entry, the active or passive flag set for the `scPosImage` object in the global container is ignored.

---

**NOTE: Creation of the `scWorkstation` Object**

The `scWorkstation` object is automatically created in the LDAP directory the first time you boot a Point of Service terminal. The `posleases2ldap` daemon automatically triggers `posldap2crconfig.pl` which then creates an `scWorkstation` object and hardware configuration files for each Point of Service terminal that registers on the Branch Server. For more information on this process, see Section “The `hwtype.MAC_address` File” (Chapter 2, *Point of Service Terminals*, ↑Administration Guide).

---

## 10.2.9 Removing an Assigned Image

To remove the image assigned to a workstation, run the following command (type the command all on one line):

```
posAdmin.pl --user cn=admin,o=mycorp,c=us --password secret
--remove --scWorkstation --scPosImageDn --scPosImageVersion
--DN cn=CR001,ou=boston1,ou=boston,o=mycorp,c=us
```

## 10.3 Distributing Images to Point of Service Terminals

To distribute new or updated system images, you must first copy the images into the central RSYNC directory of the Administration Server and then transfer the images to the Branch Servers. From there the images are distributed to the Point of Service terminals when they boot.

---

**NOTE: Manual Distribution of ISOBoot Images**

If you are unable to electronically distribute Point of Service images over your network, you must manually distribute the images using ISOBoot images.

---

## 10.3.1 Copying Images to the Administration Server RSYNC Directory

The first step to distribute new system images is to copy the images from the `/srv/SLEPOS/image` directory to the RSYNC directory, `/srv/SLEPOS`. Before the RSYNC service can transmit the images to the Branch Server, client images must be located in the `/srv/SLEPOS/image` directory on the Administration Server, and the boot image must be located in `/srv/SLEPOS/boot`.

---

### NOTE: Manually Copying System Images

Copying the system images to the RSYNC directory is done manually to control which system image types and versions are distributed to the Branch Servers.

---

### Copying System Images to the Administration Server's RSYNC Directory

The following example demonstrates how to put a previously-extended Desktop system image in the Administration Server's RSYNC directory so it can be received, on request, by the Branch Server:

- 1 Copy the extended Desktop system image:

```
cp /srv/SLEPOS/image/Desktop-2.0.21-2004-12-05 \  
  /srv/SLEPOS/image/browser-2.0.21
```

- 2 Copy the corresponding Browser image MD5 checksum file:

```
cp /srv/SLEPOS/image/Browser-2.0.21-2004-12-05.md5 \  
  /srv/SLEPOS/image/Browser-2.0.21.md5
```

### Copying Boot Images to the Administration Server's RSYNC Directory

The following example demonstrates how to copy the first and second stage boot images to the Administration Server's RSYNC directory so they can be received, on request, by the Branch Server:

---

## NOTE

Point of Service terminals boot two images, a first stage image (`initrd.gz`) and a second stage image (`linux`). For more information, see [Section 10.4, “Booting the Point of Service Terminal”](#) (page 102).

---

- 1 Copy the `initrd-disknetboot` image as `initrd.gz`:

```
cp /srv/SLEPOS/image/initrd-disknetboot-version-date.gz \
   /srv/SLEPOS/boot/initrd.gz
```

- 2 Copy the kernel image as `linux`:

```
cp
/srv/SLEPOS/image/initrd-disknetboot-version-date.kernel.kernel_version
/srv/SLEPOS/boot/linux
```

## 10.3.2 Distributing Images to the Branch Server

If you create a new image or change an image version, you can run the `possyncimages.pl` command at the Branch Server to transfer new or updated images to the Branch Server after the images are in the Administration Server’s RSYNC directory.

---

### IMPORTANT: RSYNC Service and LDAP Objects

The RSYNC service must be properly configured and running on the Administration Server for the `possyncimages.pl` script to run. For more information, see [Section 7.2.4, “Adding an `scBranchServer` Object”](#) (page 61).

Additionally, each system image has an associated `scPosImage` object in LDAP. The object’s `scPosImageVersion` attribute should be set to `active` to keep track of the most recent image version and state before `possyncimages.pl` transfers the images to the Branch Server. For more information, see [Section 10.2.7, “Activating Images”](#) (page 96).

---

The basic process is as follows:

- 1 The `possyncimages.pl` script initially checks via the PID file to determine if an instance is already running.
- 2 The image files are then copied from the Administration Server to the Branch Server. Boot images are copied from the `/srv/SLEPOS/boot/` directory on the Administration Server to the `/srv/tftpboot/boot/` directory on the Branch Server. System images and their associated MD5 checksum files are copied from `/srv/SLEPOS/image/` to `/srv/tftpboot/image`.

During this process, the TFTP server must be stopped or otherwise prevented from transmitting the image files to clients.

For more information on the `possyncimages.pl` script, see Section “`possyncimages.pl`” (Appendix A, *Point of Service Scripts*, ↑Administration Guide).

After executing the `possyncimages.pl` script, verify the result by checking the contents of the following directories:

- `/srv/tftpboot/image`
- `/srv/tftpboot/boot`

### 10.3.3 Distributing Images to Point of Service Terminals

New or updated images are distributed to Point of Service terminals at boot time. For information on this process, see [Section 10.4, “Booting the Point of Service Terminal”](#) (page 102).

### 10.3.4 Image Install Notification

When the Branch Server distributes a new image to a Point of Service terminal, the system provides notification that the image was successfully installed on the Point of Service terminal. The notification is stored in the `scWorkstation` object in the LDAP directory on the Administration Server.

When the image is successfully installed on the Point of Service terminal, the `linuxrc` script running on the Point of Service terminal creates the `bootversion.MAC`

`_Address` file in the `/srv/tftpboot/upload` directory on the Branch Server. The `posleases2ldap` process then transfers the information to the `scNotifiedimage` attribute in the `scWorkstation` object in LDAP and deletes the `bootversion.MAC_address` file.

## 10.4 Booting the Point of Service Terminal

---

### IMPORTANT: Creating LDAP Objects Before Booting

Before you can boot the Point of Service terminals, you must create an `scCashRegister` object and its associated objects. For more information, see [Section 10.2.1, “Creating an `scCashRegister` Object”](#) (page 87).

---

Typically, when you boot a Point of Service terminal, it first tries to boot from CD. If a CD is not available, the terminal attempts a network PXE boot. If the network is not available, it then boots from the hard drive. You can override this order with the BIOS settings.

The first time you boot the Point of Service terminals, the `posleases2ldap` daemon automatically triggers `posldap2crconfig.pl` which then creates a Workstation (`scWorkstation`) object and hardware configuration files for the Point of Service terminals that register on the Branch Server. For more information on this process, see Section “The `hwtype.MAC_address` File” (Chapter 2, *Point of Service Terminals, Administration Guide*).

### 10.4.1 Network PXE Boot

To boot Point of Service terminals from the network, the following conditions must be met:

- The terminal must have a network connection to the Branch Server.
- The TFTP service must be properly configured and running on the Branch Server.

For more information on Branch Server configuration, see [Chapter 7, \*Setting Up a Branch Server\*](#) (page 55).

- The terminal must have an associated `scCashRegister` object in the LDAP directory.

For more information, see [Section 10.2, “Creating the Required LDAP Objects”](#) (page 86).

- The Point of Service boot images must be located in the `/srv/tftpboot/boot/` directory on the Branch Server and the system images must be located in the `/srv/tftpboot/image/` directory.

For more information, see [Section 10.3, “Distributing Images to Point of Service Terminals”](#) (page 98).

- The Point of Service system images must have an associated `scPosImage` object in the LDAP directory and the object’s `scPosImageVersion` attribute must be set to Active.

For more information, see [Section 10.2.6, “Creating `scPosImage` Objects”](#) (page 94).

- The IDE disk modules are not loaded automatically but instead this is done statically. In case you find an issue pxe-booting an image onto an IDE disk, please make sure you have not deleted the kiwi append options on the following line from the Branch Server's config file `/srv/tftpboot/boot/pxelinux.cfg/default`:

```
append kiwkernelmodule=ide-disk
```

If these conditions are met, the Point of Service terminal can successfully boot from the network.

The following is a detailed description of what takes place when a Point of Service terminal boots from the network:

- 1** The Point of Service terminal makes a DHCP request.
- 2** The Point of Service terminal downloads `pxelinux.0`.

The `pxelinux.0` image is the first bootstrap image used to PXE boot the Point of Service terminals.

- 3** The Point of Service terminal downloads the `linux` file.

The `linux` file is actually the `DiskNetboot-version-date.kernel.version-SLRS` image. The Linux image provides the Linux kernel used to PXE boot the Point of Service terminals.

- 4** Using PXE network boot or boot manager (GRUB), the Point of Service terminal boots the `initrd` image (`initrd.gz`) that it receives from the Branch Server.

If no PXE boot is possible, the Point of Service terminal tries to boot via hard disk, if one is accessible.

- 5** The `linuxrc` script begins.

- 6** The file systems required to receive system data are mounted; for example, the `/proc` file system.

- 7** The Point of Service hardware type (`hwtype`) is detected.

The Point of Service hardware manufacturer provides a program to do this. The first time the Point of Service terminal boots, this information is used to register the Point of Service terminal and create the terminal's `config.MAC_address` file. This information is also used to determine which configuration files the terminal should use.

- 8** The Point of Service BIOS version (`hwbios`) is detected.

The Point of Service hardware manufacturer provides a program to do this.

- 9** Network support is activated. The required kernel module is determined from a static table by selecting the entry corresponding to the hardware type. If no known hardware type is detected, a default list of modules is used and types are tried one after the other.

- 10** The module is loaded using `modprobe`. Any dependencies to other modules are cleared at that time.

- 11 The network interface is set up via DHCP.
- 12 After the interface has been established, the DHCP variables are exported into the `/var/lib/dhcpd/dhcpd-eth0.info` file and the contents of DOMAIN and DNS are used to generate a `/etc/resolv.conf` file.
- 13 The TFTP server address is acquired.

During this step, a check is first made to determine whether the hostname `tftp.DOMAIN` can be resolved. If not, the DHCP server is used as the TFTP server.

- 14 The Point of Service configuration file `config.MAC_address` is loaded from the Branch Server's `/srv/tftpbboot/CR` directory over TFTP. For more information about this file, see Section “The `config.MAC_address` File” (Chapter 2, *Point of Service Terminals*, ↑Administration Guide).

If this is the Point of Service terminal's first time booting, the terminal's `config.MAC_address` file does not yet exist. The Point of Service terminal must first register on the system.

A new Point of Service terminal registers as follows:

- 14a An optional alias name can be set for the new Point of Service terminal. During the creation of one of the boot images, you can enable the system alias setting using the `POSSetAlias` feature module. By default, there is no question for the system alias name.
- 14b A Point of Service control file (`hwtype.MAC_address`) is uploaded to the TFTP server's upload directory: `/srv/tftpbboot/upload`.

The `hwtype.MAC_address` file indicates the Point of Service hardware type, the BIOS version, and the Point of Service alias name. The system uses this information to create the terminal's `config.MAC_address` file. For more information on this process, see Section “The `hwtype.MAC_address` File” (Chapter 2, *Point of Service Terminals*, ↑Administration Guide).

- 14c After the upload, the Point of Service terminal renews the DHCP lease (`dhcpd -n`).

- 14d** The Point of Service terminal attempts to load its new `config.MAC_address` file from the TFTP server.
- 14e** If the `config.MAC_address` file is not yet available, the Point of Service terminal waits 60 seconds before repeating **Step 14c** (page 105) and **Step 14d** (page 106).
- 15** When the `config.MAC_address` file loads, the system begins an analysis of its contents.

For more information about the content and file format of the `config.MAC_address` file, refer to Section “The `config.MAC_address` File” (Chapter 2, *Point of Service Terminals*, ↑Administration Guide).

- 16** First, the `PART` line in the `config.MAC_address` file is analyzed (if there is a `PART` line). For more information, refer to Section “The `config.MAC_address` File” (Chapter 2, *Point of Service Terminals*, ↑Administration Guide).

A check is made using the image version to see whether any local system needs to be updated.

- If no system update is required, no image download occurs and the Point of Service terminal boots from the hard drive.
- If a system update is required, the Point of Service hard disk is partitioned according to the parameters specified in the `PART` line.

- 17** Next, the `SYNC` line in the Point of Service configuration file is evaluated. For more information, refer to Section “The `config.MAC_address` File” (Chapter 2, *Point of Service Terminals*, ↑Administration Guide).

The file indicated in the `SYNC` line is downloaded over TFTP. The only value the file contains is the number of seconds to wait (sleep) before the multicast download of the system image starts.

If the file is not present, the boot process proceeds immediately.

- 18** Indicated images are downloaded with multicast TFTP.

**19** If the image is compressed, it is copied then decompressed.

**20** The image checksums are verified.

If they do not match, the images are re-downloaded.

**21** The `CONF` line in the Point of Service configuration file is evaluated. For more information, refer to Section “The `config,MAC_address` File” (Chapter 2, *Point of Service Terminals*, ↑Administration Guide).

All the indicated files are loaded from the TFTP server and stored in a `/config/` path.

**22** All the user-land processes based on the boot image (`dhcpcd -k`) are terminated.

**23** The system image is mounted.

**24** The configuration files stored in the `/config/` path are copied to the mounted system image.

**25** If this is a new image, Image Install Notification occurs.

**25a** The `bootversion.MAC_Address` file is created in `/srv/tftpboot/upload`.

**25b** `posleases2ldap` transfers the information to the `scNotifiedimage` attribute in the `scWorkstation` object in LDAP.

**26** The system switches to the mounted system image.

**27** The root file system is converted to the system image using `pivot_root`.

All the required configuration files are now present because they had been stored in the system image or have been downloaded via TFTP.

The file systems that are mounted read-only can be stored in `cramfs`-compressed RAM file systems to save Point of Service RAM resources.

**28** The boot image is unmounted using an `exec umount` call.

- 29 When `linuxrc` or the `exec` call terminates, the kernel initiates the `init` process, which starts processing the boot scripts as specified in `/etc/inittab`.

## 10.4.2 ISOBoot

Depending on whether network is available or not, there are two possibilities to boot from CD:

If a network connection is available and your computer is not able to boot over PXE/DHCP and you have a PXE boot image, proceed as follows:

- 1 Run the following KIWI command:

```
kiwi --booted initrd-netboot
```

- 2 Burn the resulting ISO image and place the system image into the directory `/srv/tftpboot/`.

If a network connection is not present at all, proceed as follows:

- 1 Build a system image (minimal, desktop or graphical) and an ISO boot image.
- 2 Burn the resulting ISO image.
- 3 Boot from the CD. The system is initialized from this CD.

# Testing Your SUSE Linux Enterprise Point of Service Environment

# 11

To complete the SUSE® Linux Enterprise Point of Service installation process, it is recommended that you verify the installation by booting at least one Point of Service client attached to the Branch Server.

## 11.1 Monitoring the Terminal Bootup

To verify and test your SUSE Linux Enterprise Point of Service installation:

- 1 Attach a Point of Service client to the Branch Server network.
- 2 Verify that the necessary LDAP objects have been created by using an `ldapsearch` command. For example (setup without SSL):

```
ldapsearch -x -H ldap://administration_server_name -b base_context  
-s base -D dn_of_admin_user -w password
```

For setups with SSL, use:

```
ldapsearch -x -H ldaps://administration_server_name -b base_context  
-s base -D dn_of_admin_user -w password
```

- 3 Verify the following LDAP object settings:

- The `scCashRegister` object which matches the model type of the Point of Service client must exist in LDAP; for example, `IBMSurePOS300Series`.
- There must be an `scPosImage` object for each image in the `/srv/tftpboot/image/` directory on the Branch Server. The `scPosImageDn` attribute within each object must correspond to an existing Point of Service image.

For further information how to modify and add LDAP entries for your specific SUSE Linux Enterprise Point of Service system environment, refer to Chapter 4, *Using posAdmin to Manage the LDAP Directory* (↑Administration Guide).

- 4 Verify that the Point of Service system images and their corresponding MD5 checksum files are available in `/srv/tftpboot/image/` directory on the Branch Server.
- 5 Verify that the `initrd.gz` and `linux` images are available in the `/srv/tftpboot/boot/` directory on the Branch Server.
- 6 Power on the Point of Service client.

You can watch the Branch Server log messages using the following command:

```
tail -f /var/log/messages
```

- 7 While the Point of Service client is booting, check if there are `tftpd` entries.

For example:

```
.. bs1 tftpd[31434]: Serving /boot/pxelinux.0 to 192.168.2.15:2070
.. bs1 tftpd[31435]: Serving /boot/pxelinux.cfg/C0A8020F to
192.168.2.15:57217
.. bs1 tftpd[31436]: Serving /boot/pxelinux.cfg/C0A8020 to
192.168.2.15:57090
.. bs1 tftpd[31437]: Serving /boot/pxelinux.cfg/C0A802 to
192.168.2.15:56963
.. bs1 tftpd[31438]: Serving /boot/pxelinux.cfg/C0A80 to
192.168.2.15:56836
.. bs1 tftpd[31439]: Serving /boot/pxelinux.cfg/C0A8 to
192.168.2.15:56709
.. bs1 tftpd[31440]: Serving /boot/pxelinux.cfg/C0A to
192.168.2.15:56582
.. bs1 tftpd[31441]: Serving /boot/pxelinux.cfg/C0 to
```

```

192.168.2.15:56455
.. bs1 tftpd[31442]: Serving /boot/pxelinux.cfg/C to 192.168.2.15:56328
.. bs1 tftpd[31443]: Serving /boot/pxelinux.cfg/default to
192.168.2.15:56201
.. bs1 tftpd[31444]: Serving /boot/linux to 192.168.2.15:56202
.. bs1 tftpd[31445]: Serving /boot/initrd.gz to 192.168.2.15:56203
.. bs1 dhcpd: DHCPDISCOVER from 00:06:29:e3:02:e6 via eth0
.. bs1 dhcpd: DHCP OFFER on 192.168.2.15 to 00:06:29:e3:02:e6 via eth0
.. bs1 dhcpd: DHCPREQUEST for 192.168.2.15 (192.168.2.1) from
00:06:29:e3:02:e6 via eth0
.. bs1 dhcpd: DHCPACK on 192.168.2.15 to 00:06:29:e3:02:e6 via eth0
.. bs1 tftpd[31454]: Serving CR/config.00:06:29:E3:02:E6 to
192.168.2.15:32768
.. bs1 tftpd[31455]: Fetching from 192.168.2.15 to
upload/hwtype.00:06:29:E3:02:E6

```

The Point of Service terminal performs a PXE boot to receive the Linux kernel and its first stage boot image, `initrd.gz`. For detailed information on the Point of Service boot process, see [Section 10.4, “Booting the Point of Service Terminal”](#) (page 102).

- 8 Watch for the `hwtype.MAC_address` file below the `/srv/tftpboot/upload` directory (for example, `hwtype.00:06:29:E3:02:E6`). This file contains the information required to create the terminal's workstation object (`scWorkstation`) in LDAP and determine which image and configuration settings should be included in the terminal's configuration file. For more information, see Section “The `hwtype.MAC_address` File” (Chapter 2, *Point of Service Terminals*, ↑Administration Guide).
- 9 Watch to see if the Point of Service client is able to boot the second stage image. This is the system image configured in LDAP (`scPosImage`) and downloaded from the `/srv/tftpboot/image/` directory on the Branch Server (for example, the `browser-2.0.21` image).
- 10 If everything proceeds normally, the Point of Service terminal boots and you will see the login prompt.

If the boot is successful, the `config.MAC_address` for the terminal is written below the `/srv/tftpboot/CR/` directory on the Branch Server. For example, if a terminal's MAC address is `00:06:29:E3:02:E6`, the `config.00:06:29:E3:02:E6` file will be located in the `/srv/tftpboot/CR/` directory. Additionally, the `scWorkstation` object for the Point of Service terminal is created in the LDAP directory.

# 11.2 Troubleshooting Terminal Bootup Problems

If the Point of Service terminal does not successfully boot, check the following:

- Verify that an `scCashRegister` object exists for the Point of Service terminal. For more information, see [Section 10.2.1, “Creating an `scCashRegister` Object”](#) (page 87).
- Verify the configuration of the `scCashRegister` object for the Point of Service terminal:

There must either be an `scCashRegister` object that corresponds to the `HWTYPE` attribute in the Point of Service terminal's `hwtype.MAC_address` file in the `/srv/tftpboot/upload/hwtypedirectory`, or a default `scCashRegister` object that will work for the Point of Service terminal.

- Verify that the Point of Service image configured in the `scPosImageDn` attribute of the `scCashRegister` object is available in the `/srv/tftpboot/image/` directory on the Branch Server.
- Do not delete any of the default LDAP objects that are created when you install SUSE Linux Enterprise Point of Service. In particular, do not delete the global default minimal `scPosImage` object that is created in the default Distribution Container, even if you do not plan to use the minimal image.
- Each type of Point of Service terminal hardware must have a unique model name defined in the `scCashRegisterName` attribute of the `scCashRegister` object in LDAP.

If two terminals have the same hardware name defined in their `scPosImage` objects, neither of them boots successfully, but a `HWtype` error is displayed on the Branch Server. To resolve the problem, change the `scCashRegisterName` value for one of the Point of Service terminals.



# Changing the Server Language

If you need to change the language that was defined during the initial installation of a SUSE® Linux Enterprise Point of Service Administration Server or Branch Server, you can do so by rerunning YaST and selecting a different system language.

## A.1 Changing the Language Selection

To change the language of your Administration or Branch Server:

- 1 Start YaST.
- 2 In the YaST Control Center, select *System > Choose Language*.
- 3 Select the desired language, then click *Accept*.

The language selected in YaST applies to the operating system, including YaST and the desktop environment. If your system needs additional packages to support the new language, YaST installs them.

