bProbe Installation and Configuration Guide

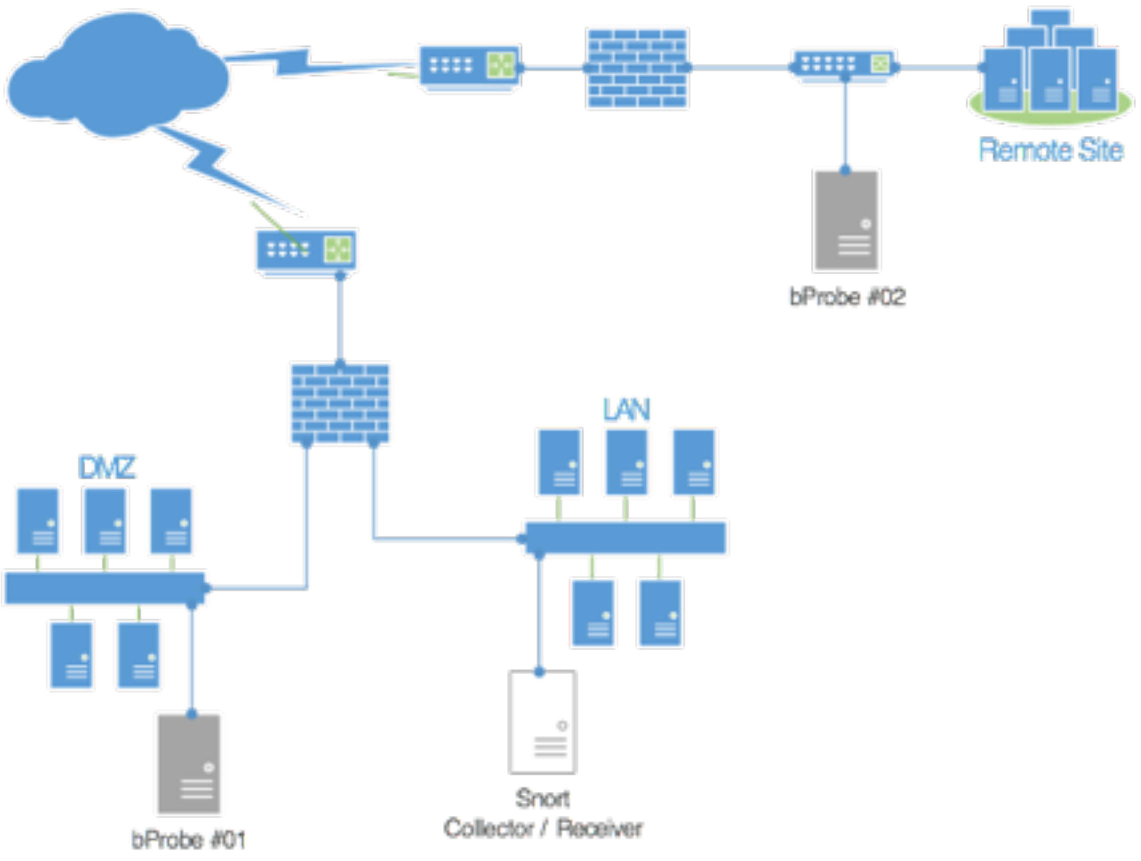
Revision 1.2.4 - (05-02-2015)

Introduction

Thank you for choosing bProbe. This is the installation and configuration guide for the bProbe software version 1.3. Please follow the instructions below to set up the bProbe software.

bProbe is a Snort IDS and Network probe software that is configured to run in packet logger mode. It can be installed on a pc and inserted at a key juncture in a network to monitor and collect network activity data.

The data collected is sent to a central "collector" server, which is any software capable of interpreting IDS and network data, such as BLËSK or its variants.



It should be noted that the installer will delete any existing partitions on your disk in order to install the software required to use bProbe.

Before beginning the installation, please be sure to backup any data that you wish to keep.

System Requirements

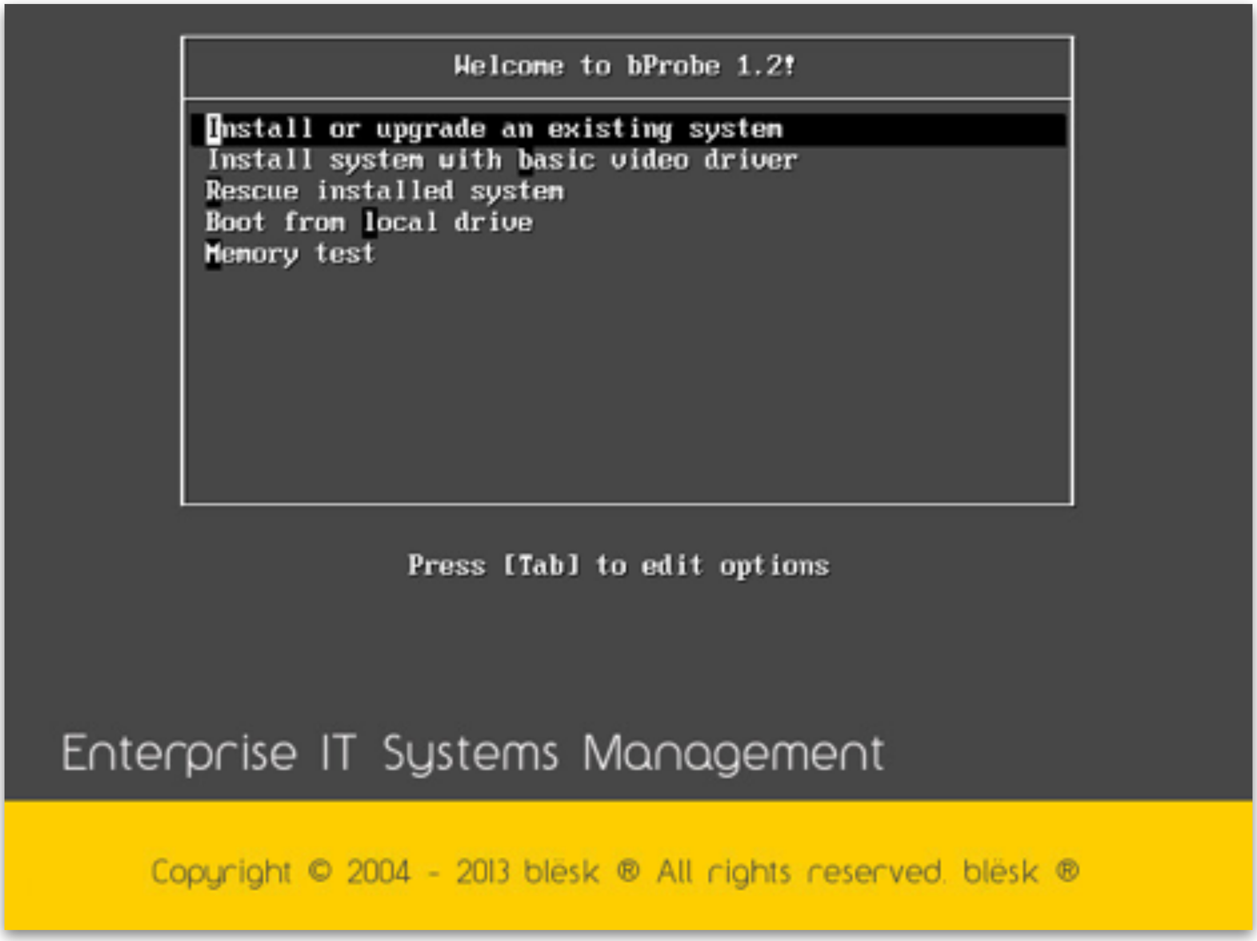
bProbe software is downloaded as an ISO image. The minimum requirements are:

Memory:	512 MB
CPU:	1 Cores
Hard Disk:	>5 GB
NIC:	2 NICs
Guest Operating System:	Select Linux, and choose version CentOS 4/5/6 (64-bit).

Note: Two network interfaces are required for a network probe server to function. The first NIC will be used for access while the second will be used to TAP/capture the data.

1. Press Enter

Once you have burned the ISO file onto a CD and have used it to boot your computer, Highlight the "***Install or upgrade an existing system***" option and press **Enter** to begin the installation.



```
Welcome to bProbe 1.2!

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test

Press [Tab] to edit options
```

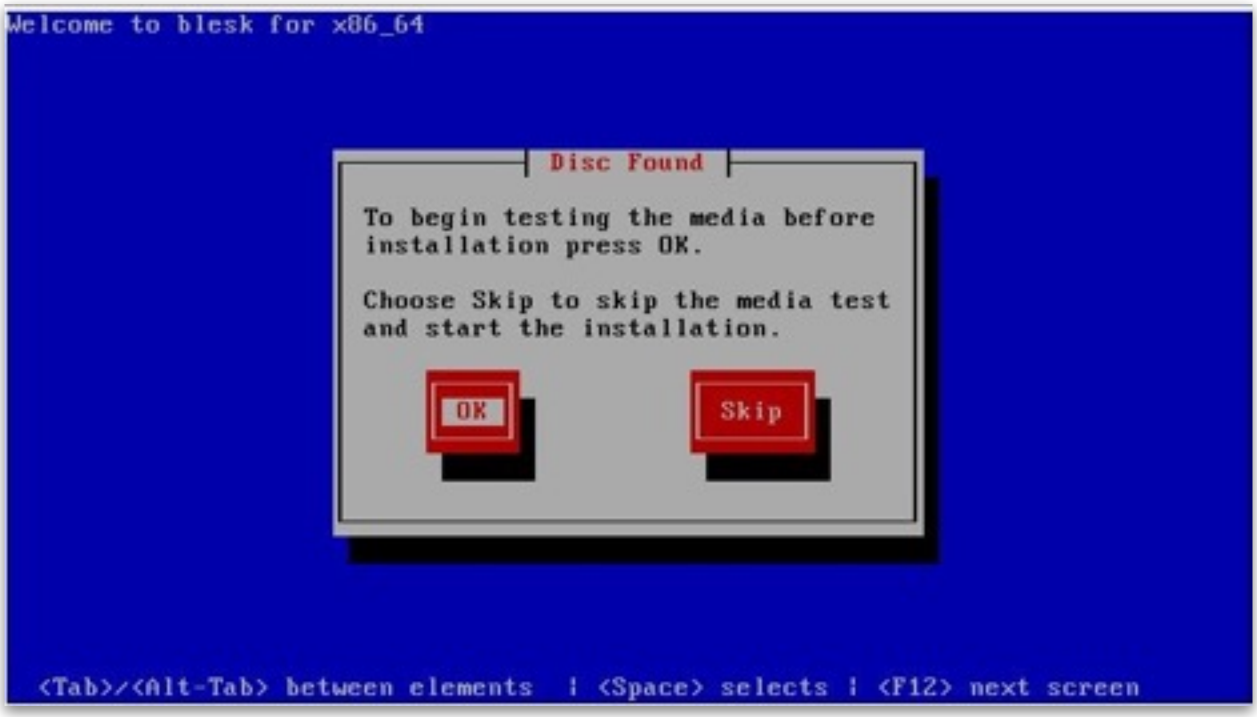
Enterprise IT Systems Management

Copyright © 2004 - 2013 blësk ® All rights reserved. blësk ®

2. Test the media (optional)

The installer will next ask if you would like to test the installation disk. This will check all of the installation files on the cd to make sure that they are readable before continuing.

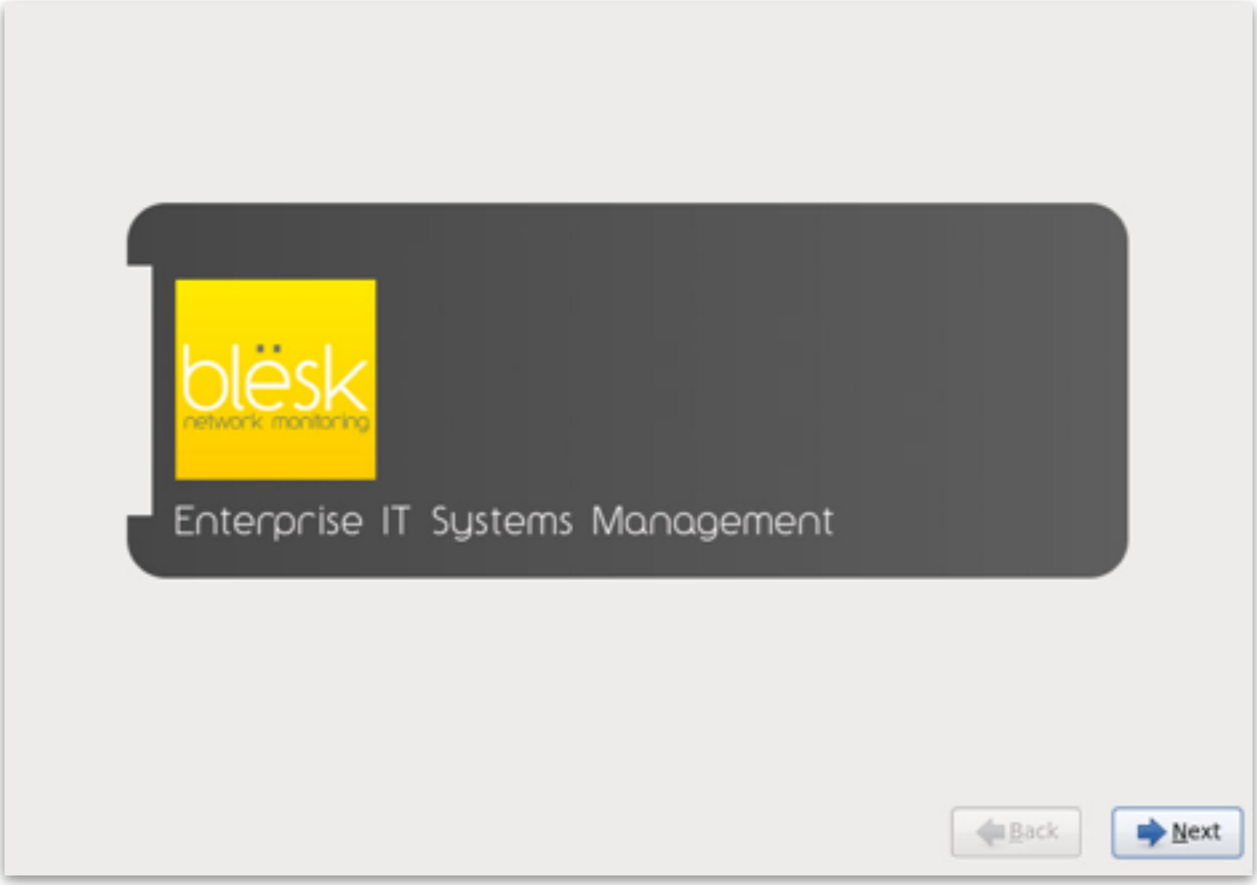
This step is optional.



```
Welcome to blesk for x86_64

Disc Found

To begin testing the media before
installation press OK.

Choose Skip to skip the media test
and start the installation.

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
```

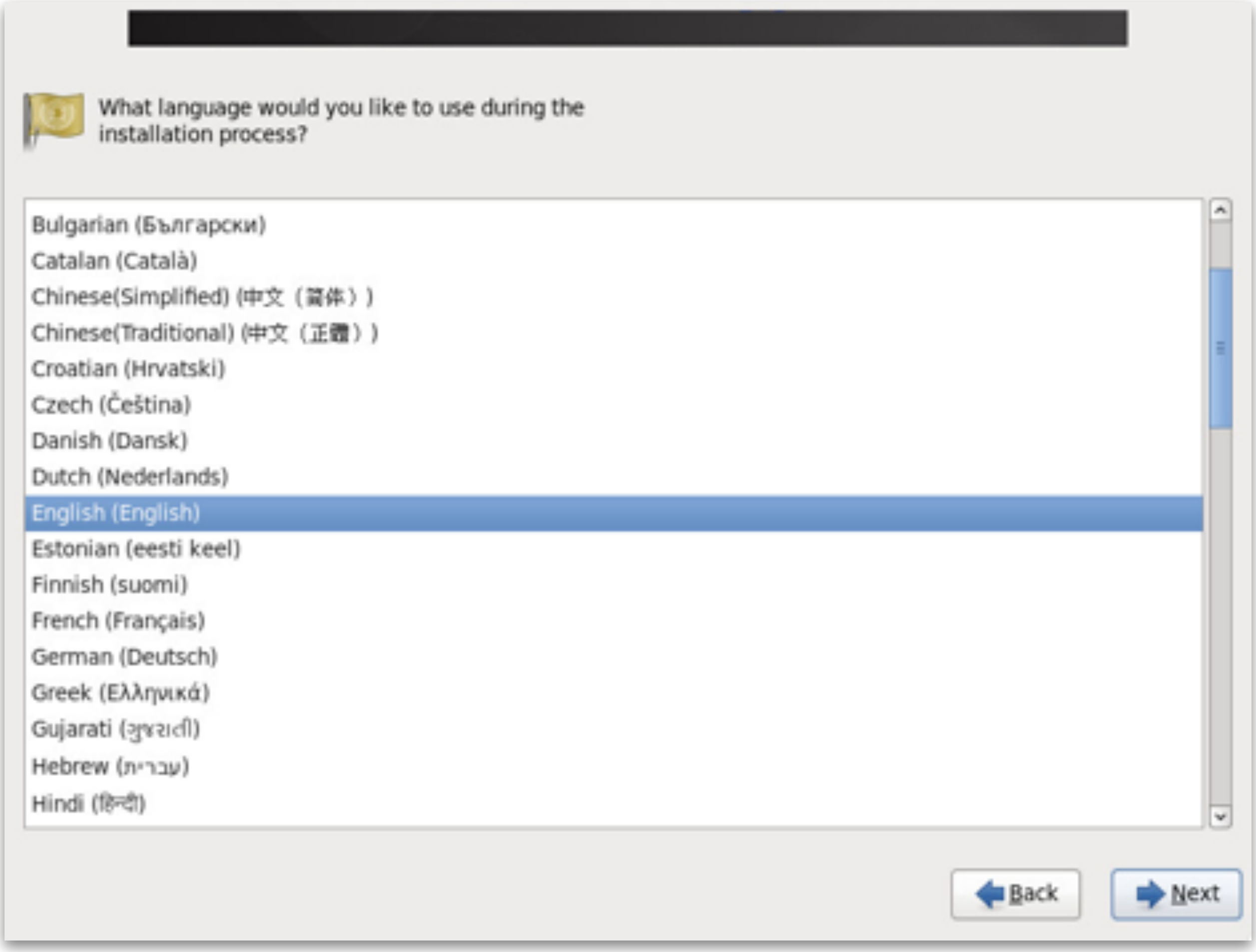
3. Launch the installation

Click « **Next** » to begin the installation.



4. Choose the language

Choose the language to be used during the installation, and click « **Next** ».

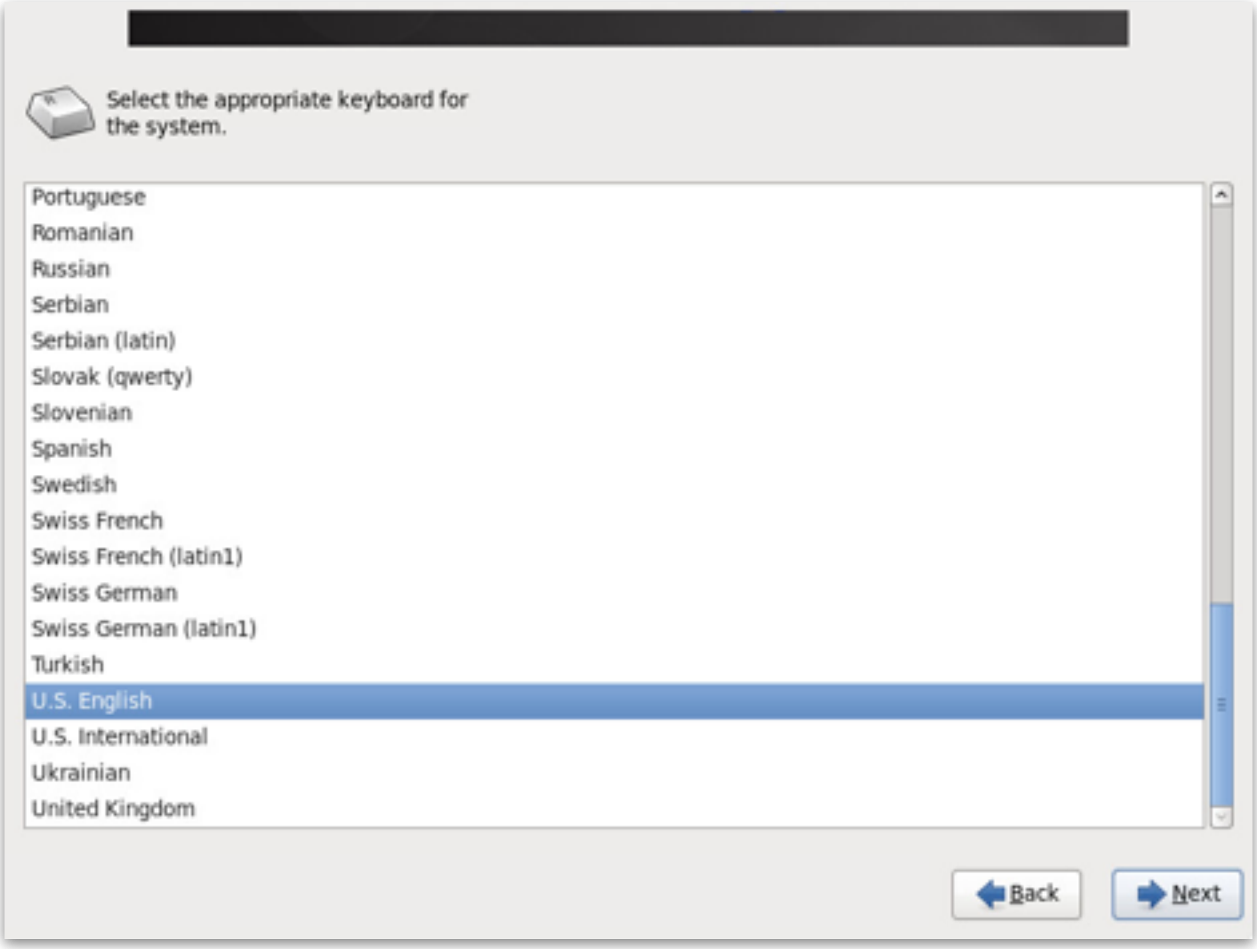


What language would you like to use during the installation process?

Bulgarian (Български)
Catalan (Català)
Chinese(Simplified) (中文（简体）)
Chinese(Traditional) (中文（正體）)
Croatian (Hrvatski)
Czech (Čeština)
Danish (Dansk)
Dutch (Nederlands)
English (English)
Estonian (eesti keel)
Finnish (suomi)
French (Français)
German (Deutsch)
Greek (Ελληνικά)
Gujarati (ગુજરાતી)
Hebrew (עברית)
Hindi (हिन्दी)

5. Select the keyboard

Choose your keyboard from the list. Click « **Next** ».

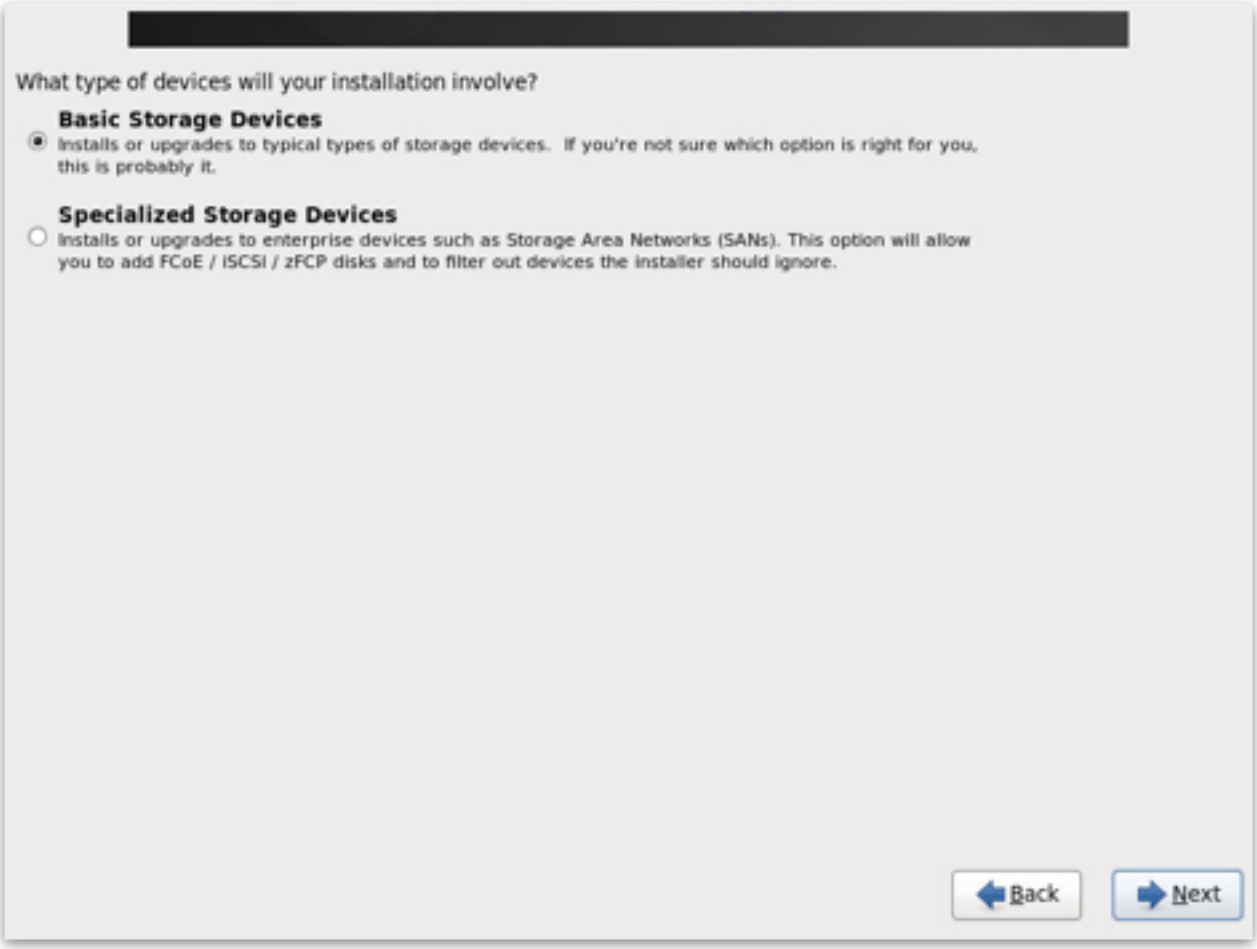


Select the appropriate keyboard for the system.

Portuguese
Romanian
Russian
Serbian
Serbian (latin)
Slovak (qwerty)
Slovenian
Spanish
Swedish
Swiss French
Swiss French (latin1)
Swiss German
Swiss German (latin1)
Turkish
U.S. English
U.S. International
Ukrainian
United Kingdom

6. Choose Disk Type

During this step you will choose the type of hard disk. Choose the first option if using a local hard disk.



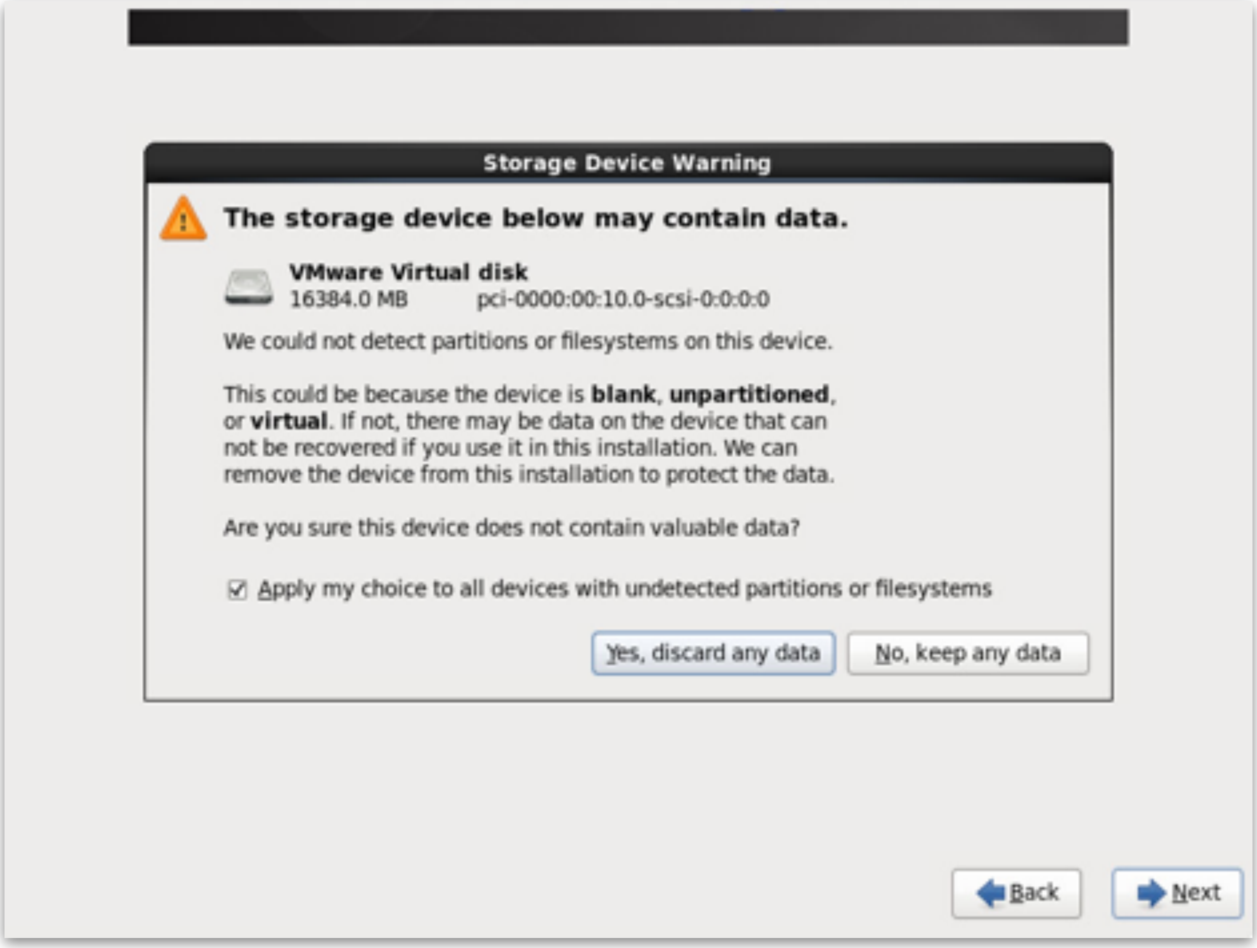
What type of devices will your installation involve?

● **Basic Storage Devices**
Installs or upgrades to typical types of storage devices. If you're not sure which option is right for you, this is probably it.

○ **Specialized Storage Devices**
Installs or upgrades to enterprise devices such as Storage Area Networks (SANs). This option will allow you to add FCoE / iSCSI / zFCP disks and to filter out devices the installer should ignore.

7. Confirm formatting

The installer will now ask for confirmation that you want to format the hard disk.



Storage Device Warning

The storage device below may contain data.

VMware Virtual disk
16384.0 MB pci-0000:00:10.0-scsi-0:0:0:0

We could not detect partitions or filesystems on this device.

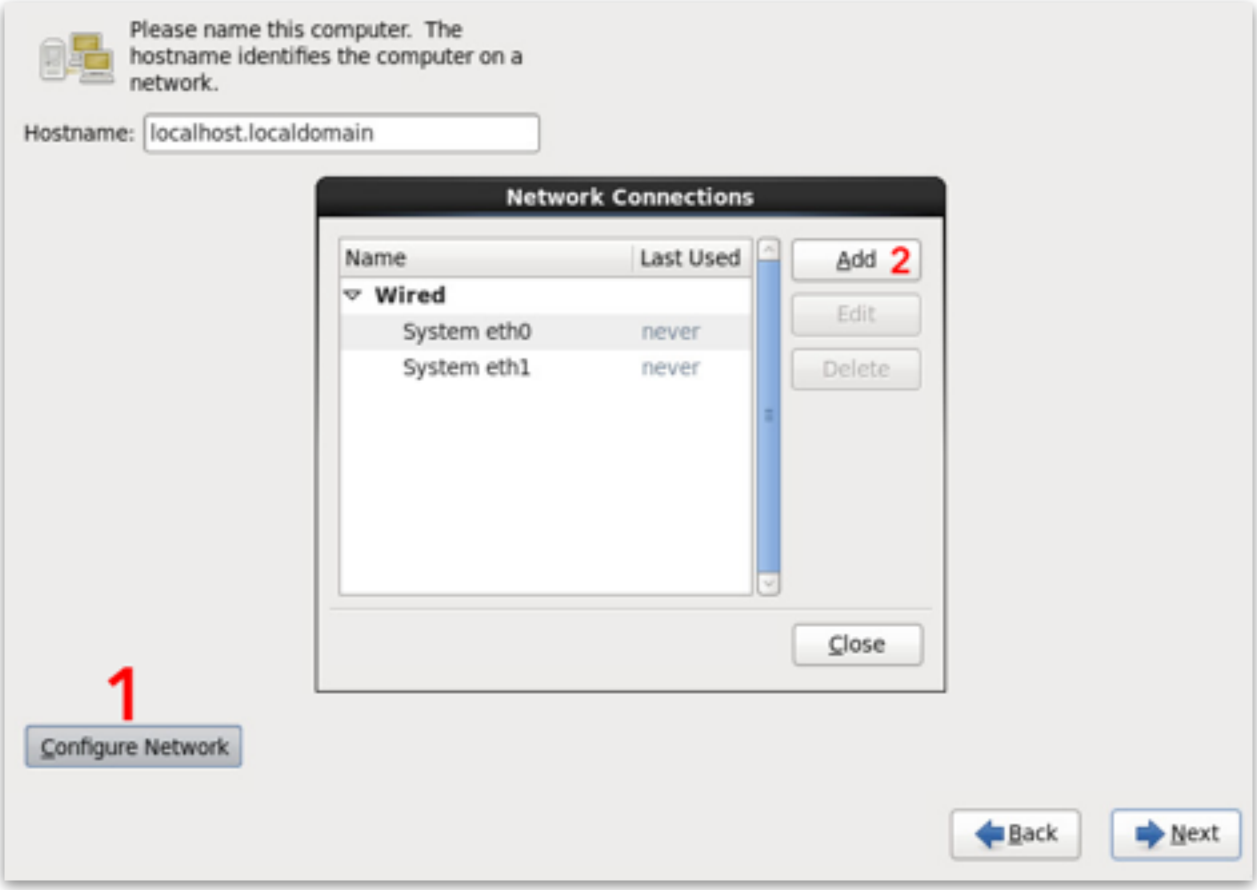
This could be because the device is **blank**, **unpartitioned**, or **virtual**. If not, there may be data on the device that can not be recovered if you use it in this installation. We can remove the device from this installation to protect the data.

Are you sure this device does not contain valuable data?

☑ Apply my choice to all devices with undetected partitions or filesystems

8. Add a network card

Click « **Configure Network** » to add a network connection. In the « *Network Connections* » window, click « **Add** » to add connections. You should at least have two network cards detected and listed. One will be used to access the bProbe server and the other for sniffing the data.



Please name this computer. The hostname identifies the computer on a network.

Hostname: localhost.localdomain

Network Connections

Name	Last Used
Wired	
System eth0	never
System eth1	never

9. Configure the first network card (used for access)

Start with the first NIC which should be detected as **eth0**, **em0**, etc… This one will represent the first physical Network Interface Card attached to your server.

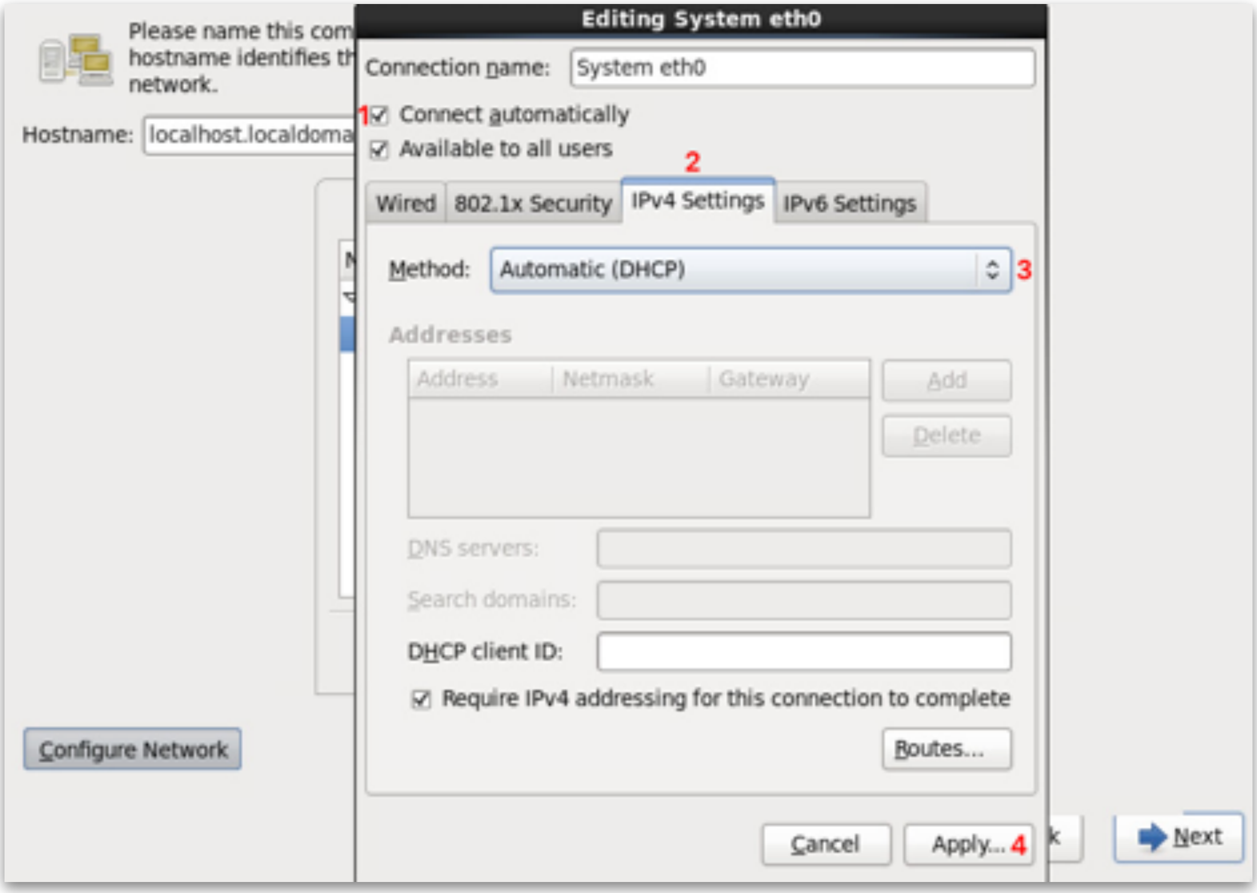
The steps for configuring the first network connection can be seen in the image below.

Step 1 – make sure that « **Connect automatically** » is checked.

Step 2 – click the IPv4 Settings tab to access the IPv4 settings.

Step 3 – it is recommended to use DHCP (you can use manual if you like).

Step 4 – click « **Apply** » to finish.



Editing System eth0

Connection name: System eth0

1 ☑ Connect automatically

☑ Available to all users

Method: Automatic (DHCP) 3

☑ Require IPv4 addressing for this connection to complete

Hostname: localhost.localdoma

10.Configure the second network card (used for sniffing)

The steps for configuring the second network connection can be seen in the image below.

Step 1 – make sure that « **Connect automatically** » is checked.

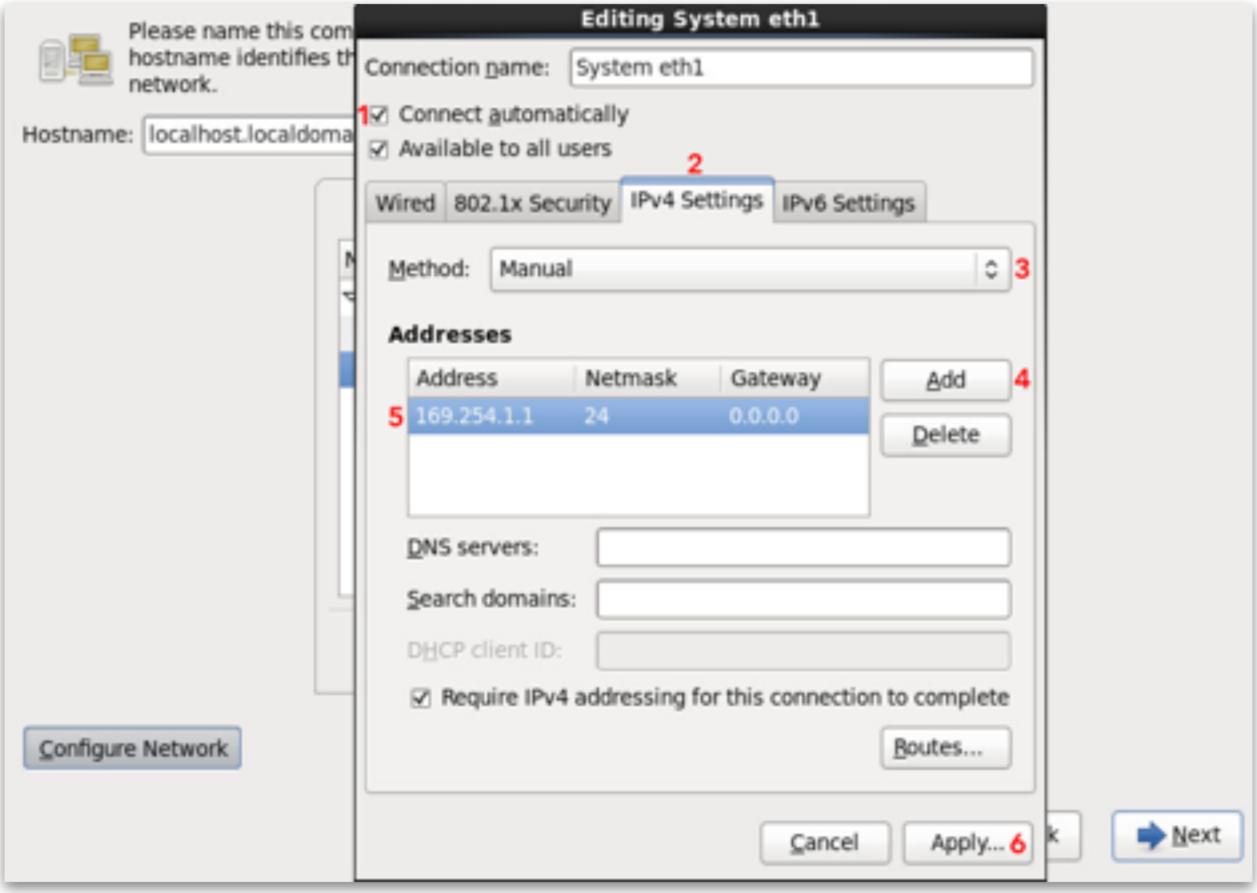
Step 2 - click the IPv4 Settings tab to access the IPv4 settings.

Step 3 - it is recommended to use a **fake** static IP address for your bProbe server. Select Manual from the Method drop down menu.

Step 4 - click the « **Add** » button to add an IP address.

Step 5 - enter the information for the IP address, subnet mask, and default gateway. We recommend **169.254.1.1/24 0.0.0.0** (this is a fake IP that we can use here).

Step 6 - click « **Apply** » to finish.



Please name this com
hostname identifies th
network.

Hostname: localhost.localdoma

Editing System eth1

Connection name: System eth1

1 ☑ Connect automatically

☑ Available to all users

2

Method: Manual 3

Addresses

Address	Netmask	Gateway
169.254.1.1	24	0.0.0.0

4

5

DNS servers:

Search domains:

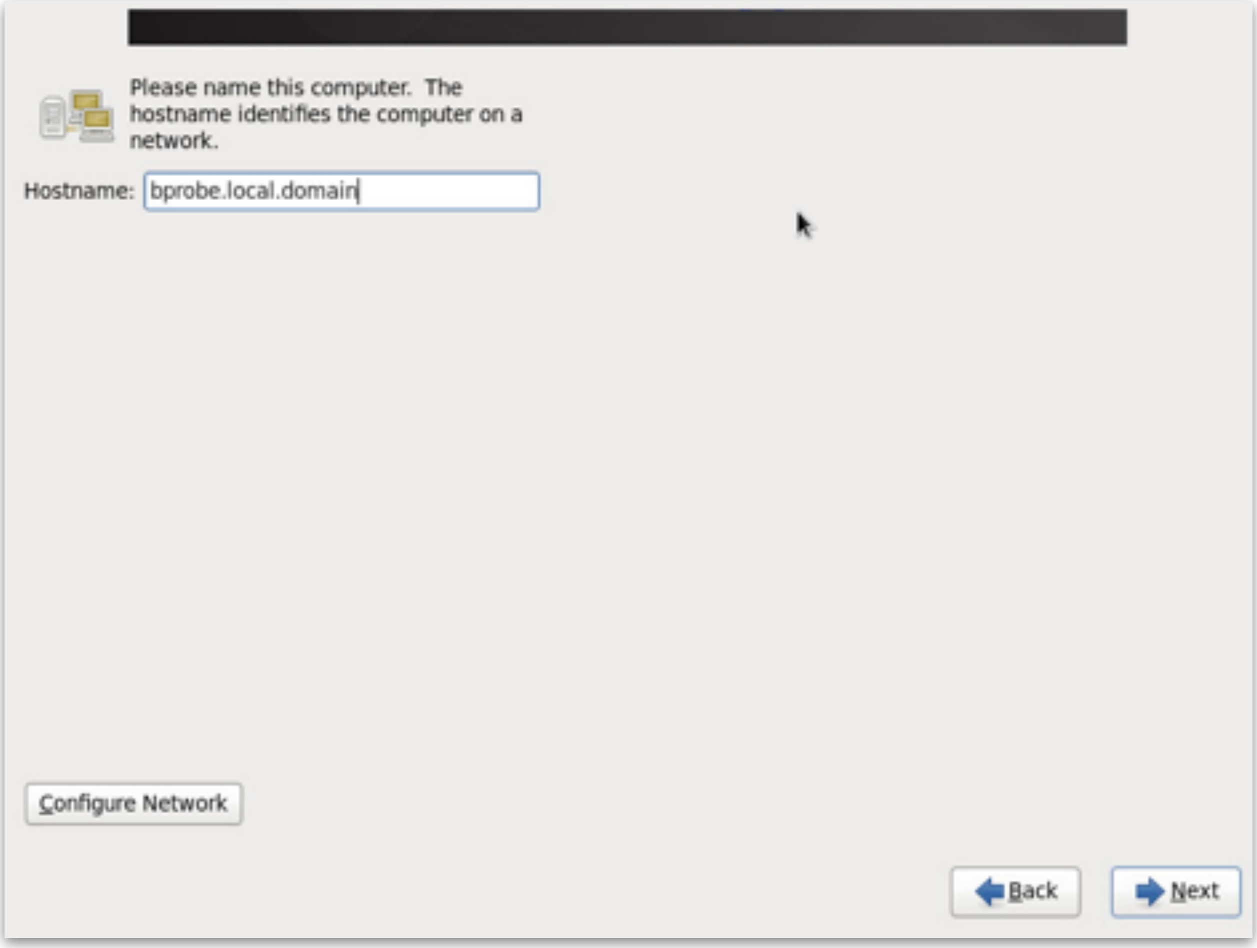
DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

6

11. Define domain name

Once the network connection has been added, specify a name for your server and click « **Next** » (It is preferable to use the fully qualified name, as shown below).

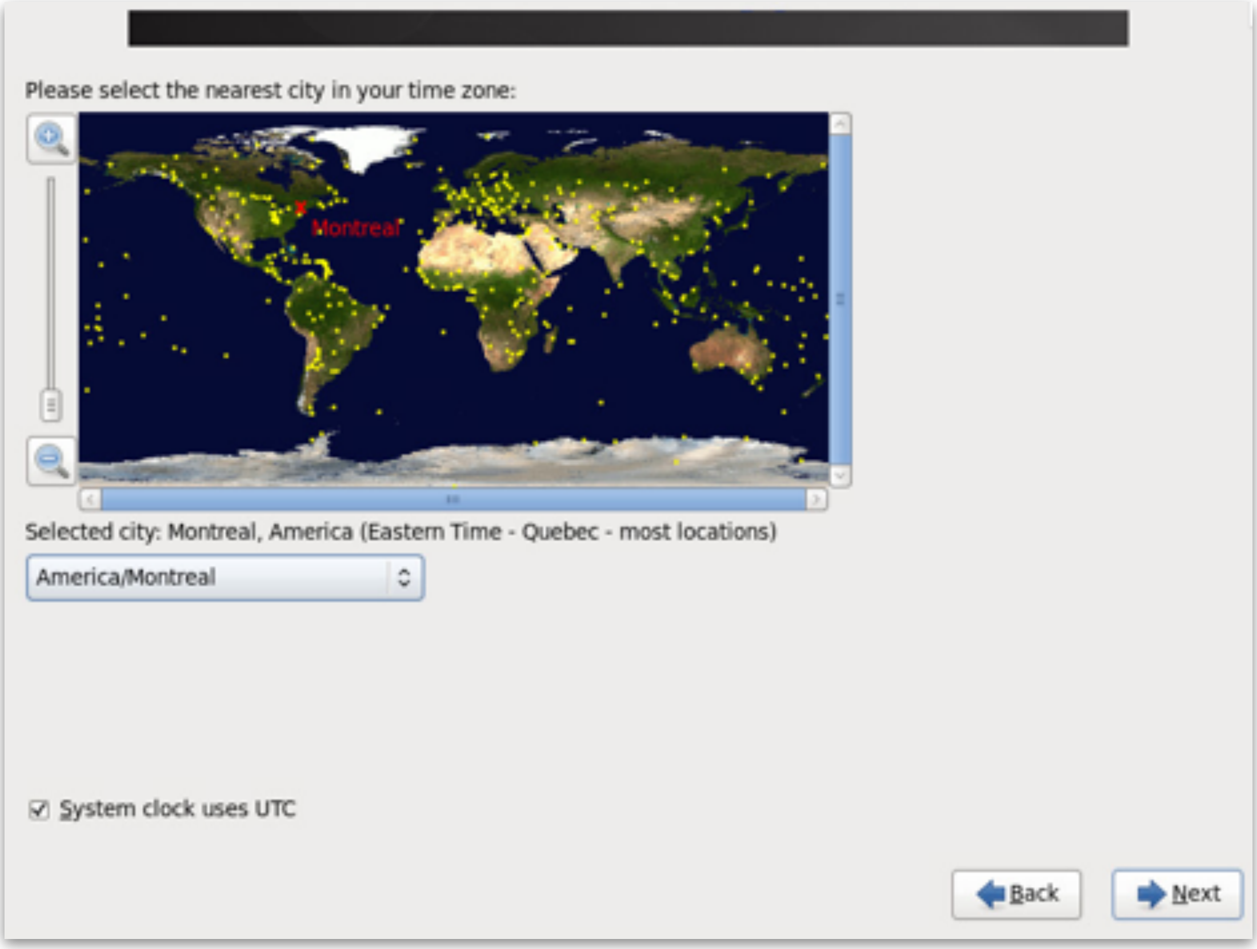


Please name this computer. The hostname identifies the computer on a network.

Hostname: bprobe.local.domain

12.Select the time zone

Select your time zone.



Please select the nearest city in your time zone:

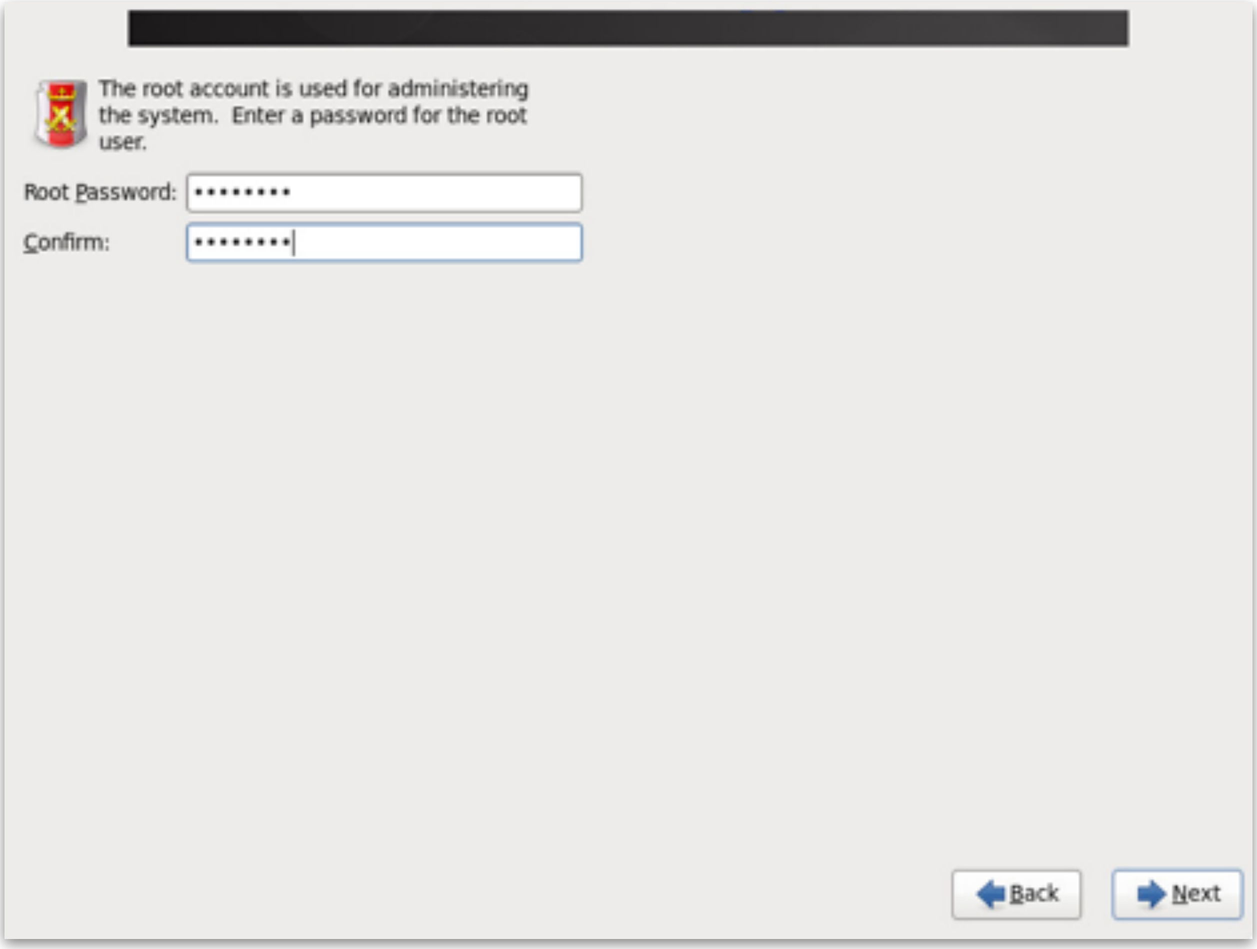
Selected city: Montreal, America (Eastern Time - Quebec - most locations)

America/Montreal

☑ System clock uses UTC

13. Enter administrator password

Choose a password for the « root » account and click « **Next** ».



The root account is used for administering the system. Enter a password for the root user.

Root Password: •••••••••

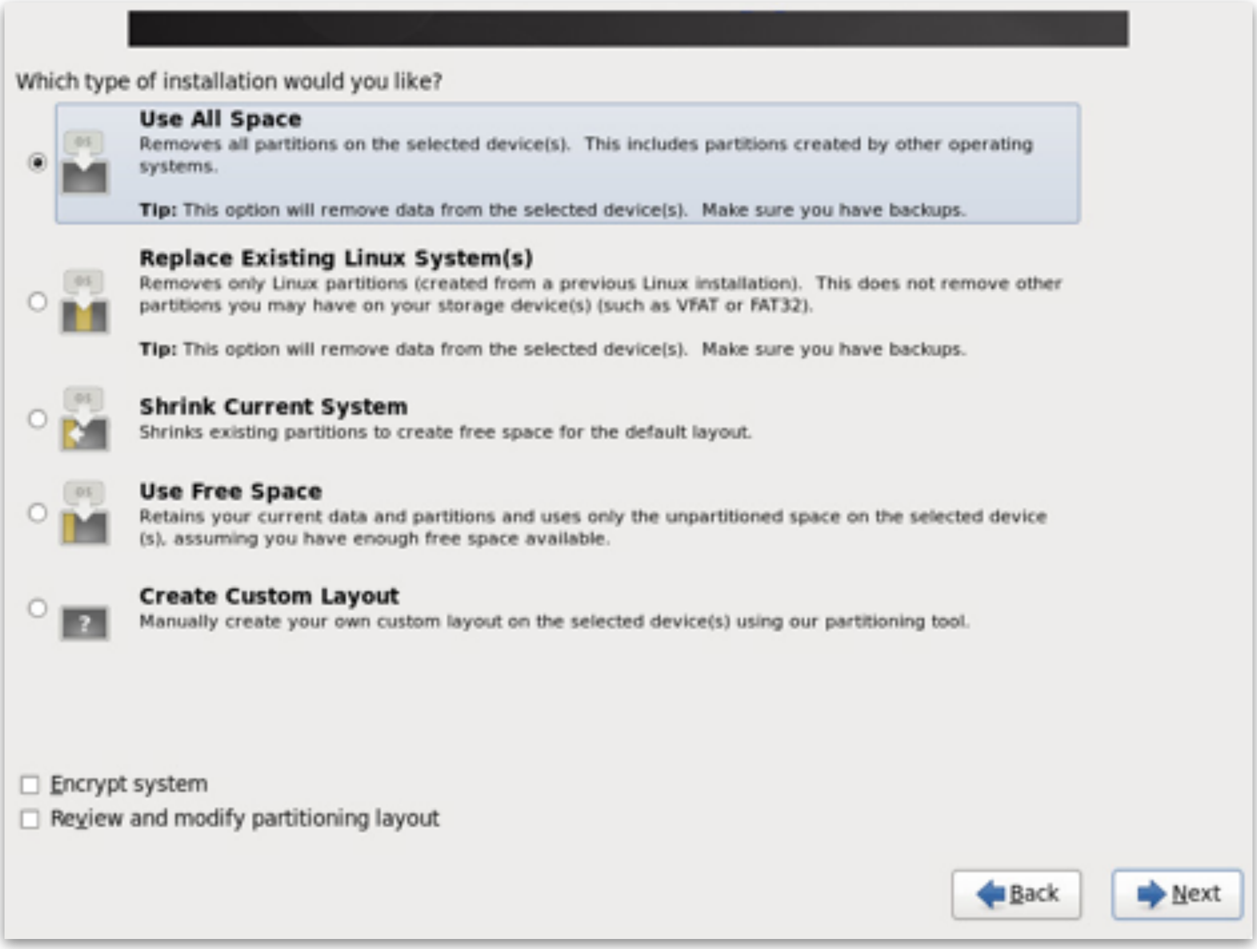
Confirm: •••••••••

14.Define partitions

When partitioning the hard disk, choose the option « **Use all space** ».

Once your selection is made, the installer will ask you to choose the disk to be formatted. If there is more than one disk in the server, you will be asked on which disk you would like to install bProbe.

!!!WARNING!!! During this step all of the partitions on your physical hard disk will be erased and new partitions created. If there is data on this disk that you wish to keep, be sure to make a backup before proceeding.



Which type of installation would you like?

● **Use All Space**
Removes all partitions on the selected device(s). This includes partitions created by other operating systems.

Tip: This option will remove data from the selected device(s). Make sure you have backups.

○ **Replace Existing Linux System(s)**
Removes only Linux partitions (created from a previous Linux installation). This does not remove other partitions you may have on your storage device(s) (such as VFAT or FAT32).

Tip: This option will remove data from the selected device(s). Make sure you have backups.

○ **Shrink Current System**
Shrinks existing partitions to create free space for the default layout.

○ **Use Free Space**
Retains your current data and partitions and uses only the unpartitioned space on the selected device (s), assuming you have enough free space available.

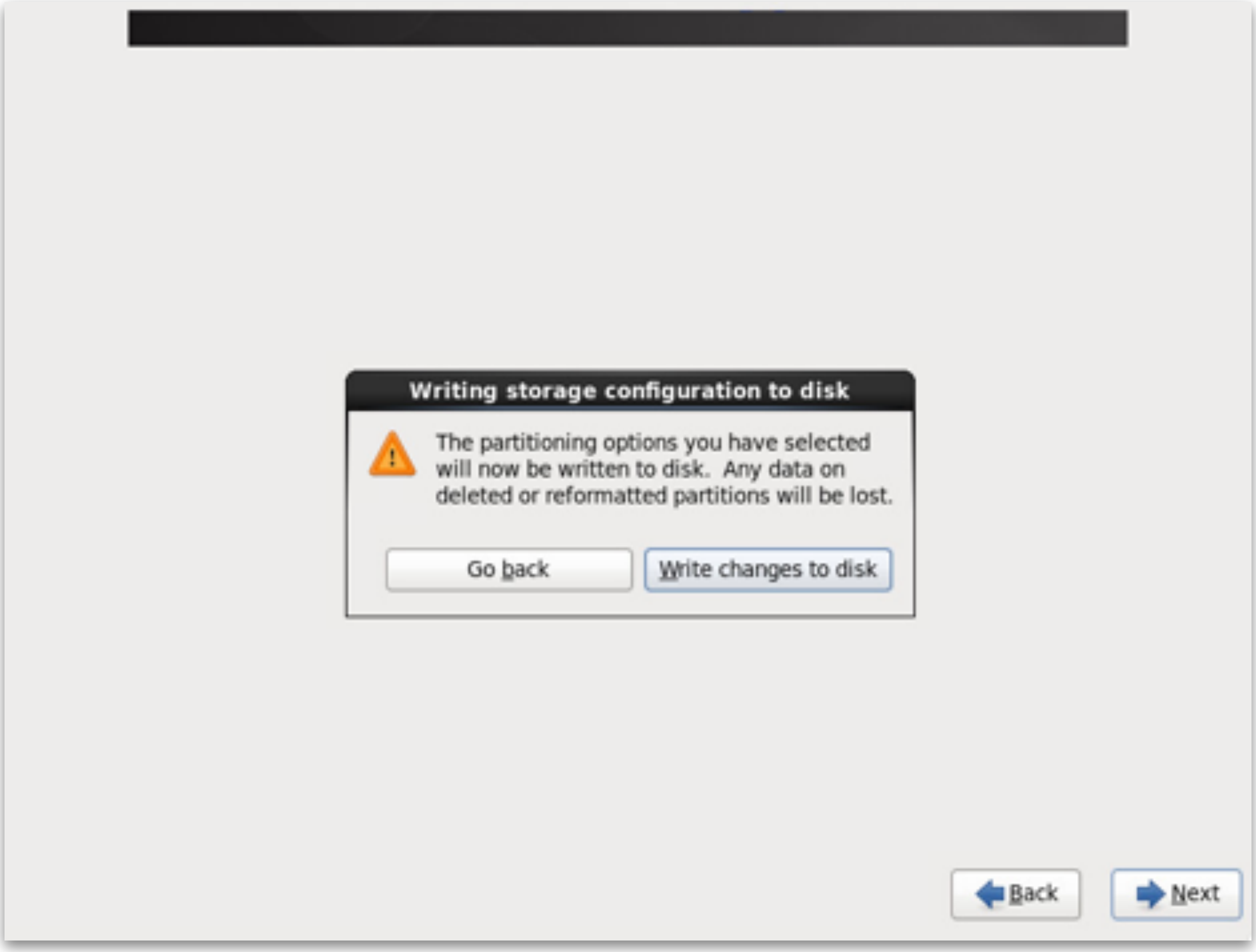
○ **Create Custom Layout**
Manually create your own custom layout on the selected device(s) using our partitioning tool.

□ Encrypt system

□ Review and modify partitioning layout

15.Confirm partition selection

Confirm your choice of partitions by clicking « **Write changes to disk** », then click « **Next** ».

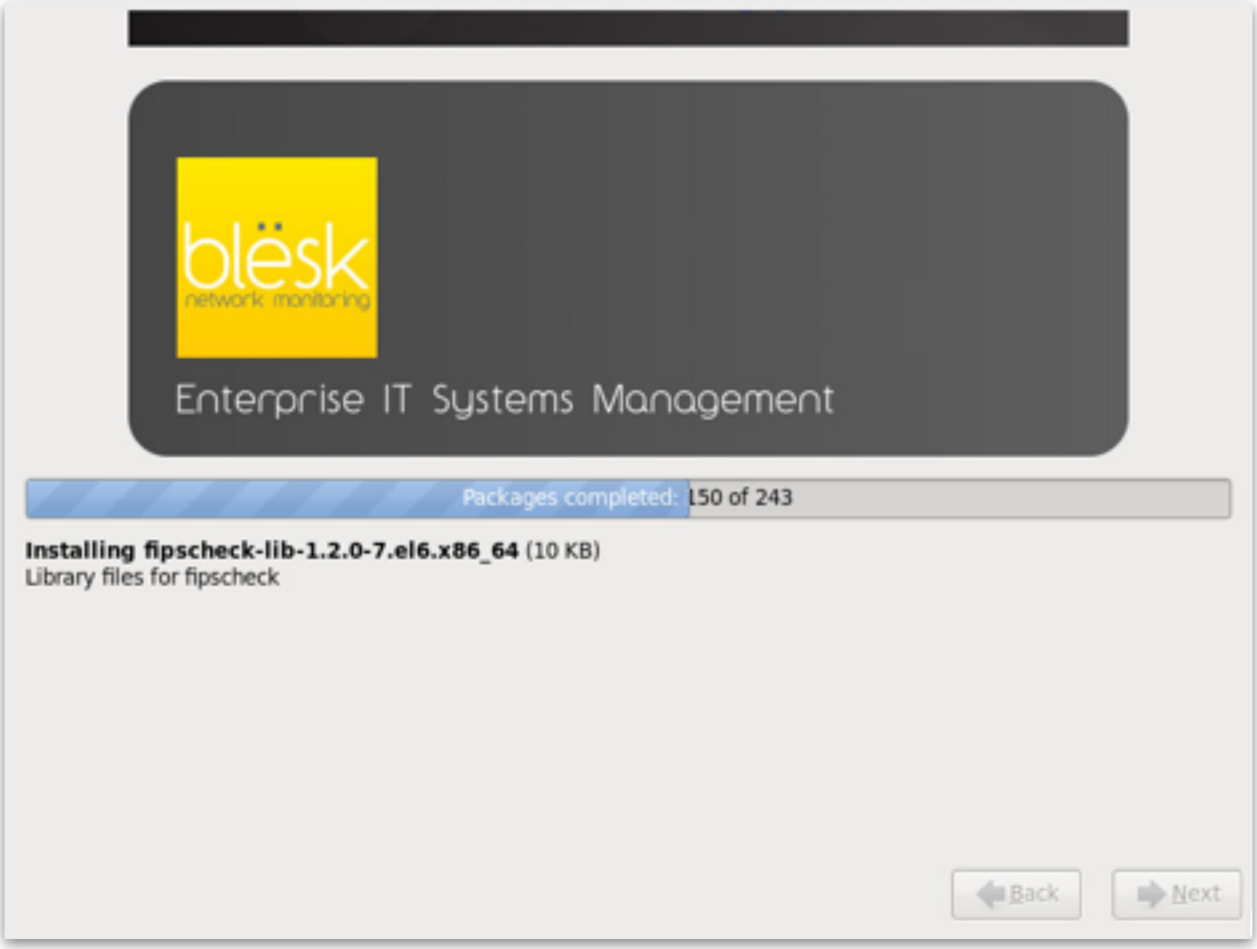


Writing storage configuration to disk

The partitioning options you have selected will now be written to disk. Any data on deleted or reformatted partitions will be lost.

16.Install the software

Once you have confirmed the partitions, package installation will begin automatically.

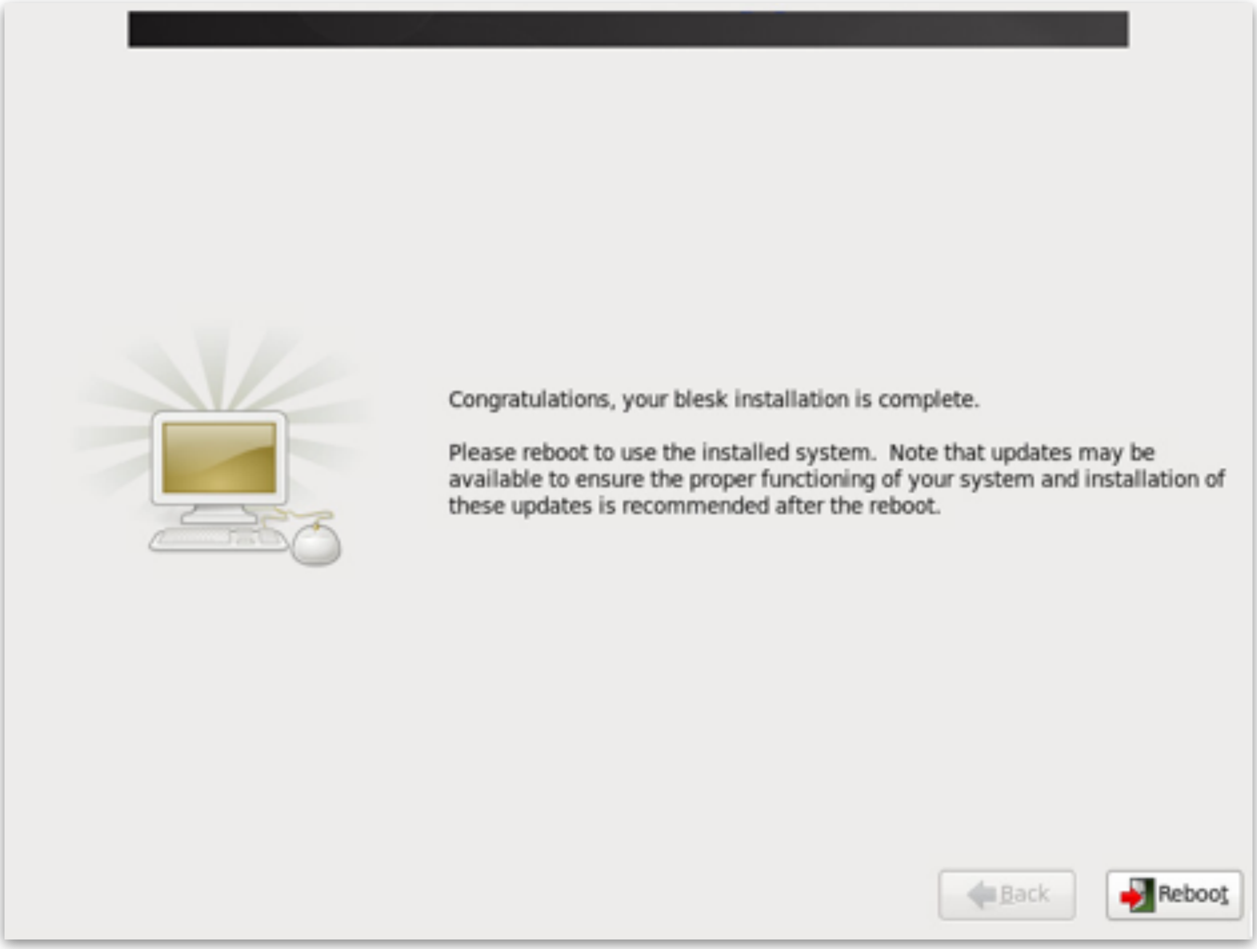


Packages completed: 150 of 243

Installing fipscheck-lib-1.2.0-7.el6.x86_64 (10 KB)
Library files for fipscheck

17.Installation complete

The installation of your bProbe server is now complete. There remain a few additional steps to be done via the web interface to make your server operational.



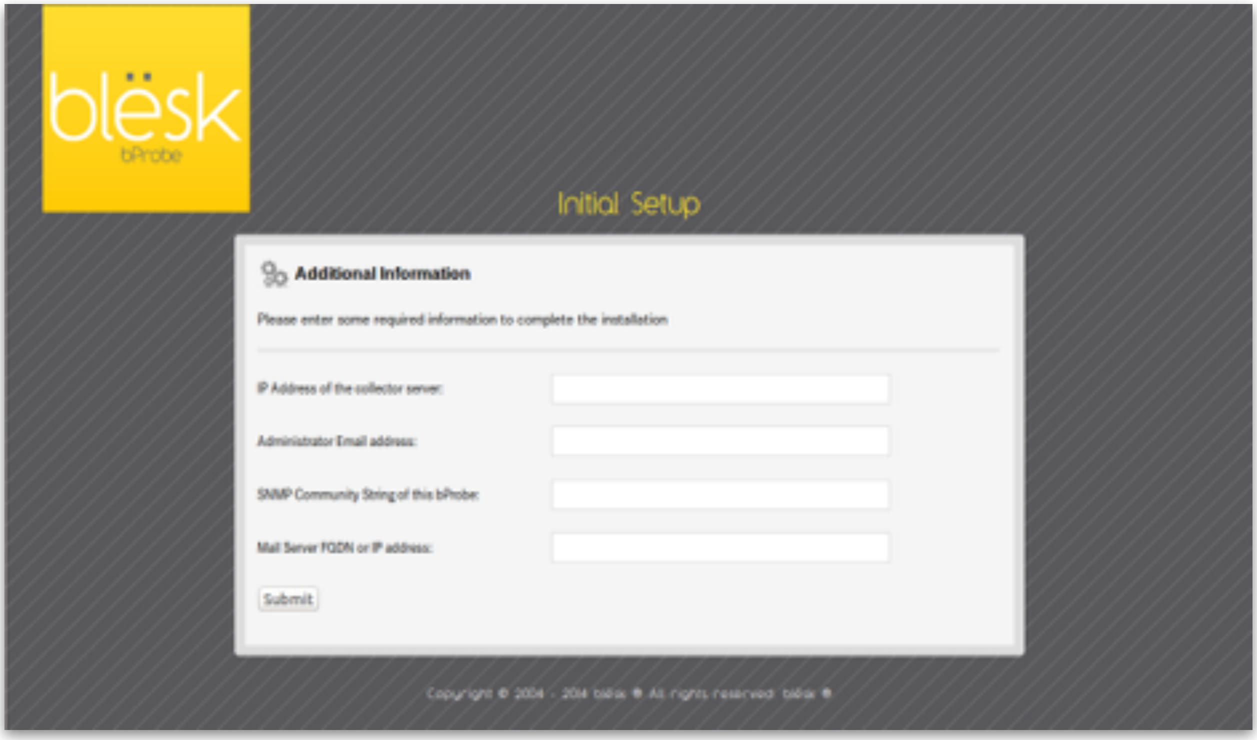
Congratulations, your blesk installation is complete.

Please reboot to use the installed system. Note that updates may be available to ensure the proper functioning of your system and installation of these updates is recommended after the reboot.

18.Finalize the configuration

To access the bProbe web interface, enter the IP address of your server in a web browser. The page you will see will ask you to enter the following:

1. The IP address of the collector / receiver server (BLËSK, etc…).
2. The email address of the system administrator.
3. The « Community string » used by SNMP to let other system monitors this unit.
4. The IP address of the mail server that will be used to send notifications.



Initial Setup

Additional Information

Please enter some required information to complete the installation

IP Address of the collector server:

Administrator Email address:

SNMP Community String of this bProbe:

Mail Server FQDN or IP address:

Copyright © 2004 - 2014 blësk ® All rights reserved. blësk ®