Sensor Installation Guide

Stealthwatch Cloud

Installation Checklist

To set up a sensor you will need:

- A machine (physical or virtual):
  - Network interfaces: At least 2 (1 control, 1+ data)
  - RAM: At least 2 GiB
  - CPU: At least 2 cores
  - Disk space: At least 32 GiB
- Internet access (**needed during setup**):
  - See the firewall rules on the next page
- Installation media:
  - The ISO file from the web portal
  - A USB drive or CD-R (for physical sensors)

Firewall setup

Configure your firewall to allow the services below before installation. The installation process won't be able to complete properly without them.

After installation the sensor will initiate connections to the monitoring service and send network data for processing.

Service	Domains / IPs	Ports	Direction
Sensor data upload	sensor.ext.obsrvbl.com 107.22.217.211 107.22.210.176 107.22.247.3	443/tcp	Outbound
OS updates	us.archive.ubuntu.com	443/tcp, 80/tcp	Outbound
Hostname resolution	Your local DNS server	53/udp	Outbound
Remote troubleshooting (optional)	54.83.42.41	22/tcp	Inbound

Installation media

For physical machines, you may use the ISO file from the web portal by:

- Writing the image CD or DVD
- Using it to create a bootable USB drive (see the following pages for instructions)

For virtual machines you should be able to boot to the ISO file directly.

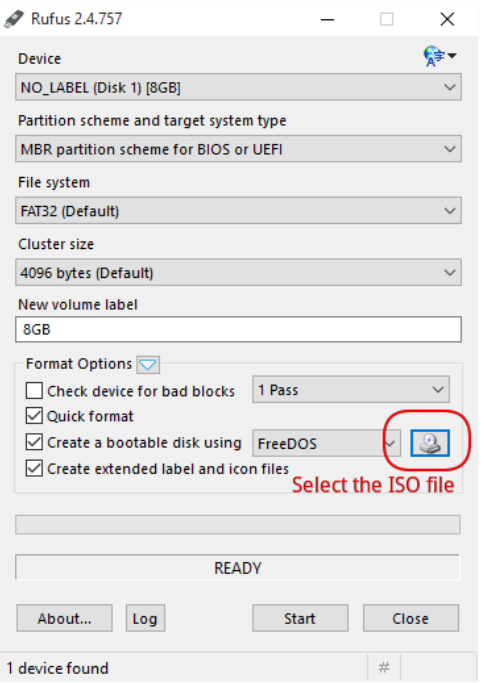
The sensor image is based on Ubuntu Linux. Its source code is available at this URL:
https://github.com/obsrvbl/ona

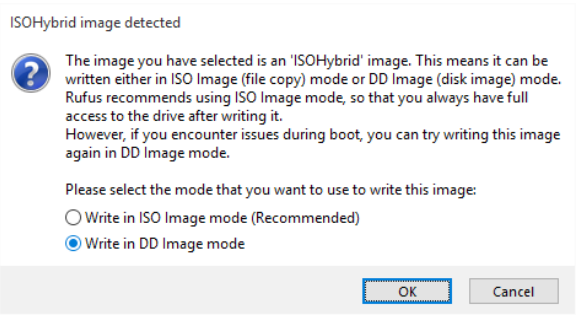
Creating a bootable USB drive (Windows)

After you've downloaded the ISO:

- Go to https://rufus.akeo.ie/
- Download the Rufus utility and open it.
- Insert the target USB drive. Rufus will detect its presence.
- Click the CD-ROM icon and then select the ISO file you downloaded.
- Click the Start button. When prompted, select “Write in DD Image mode.”

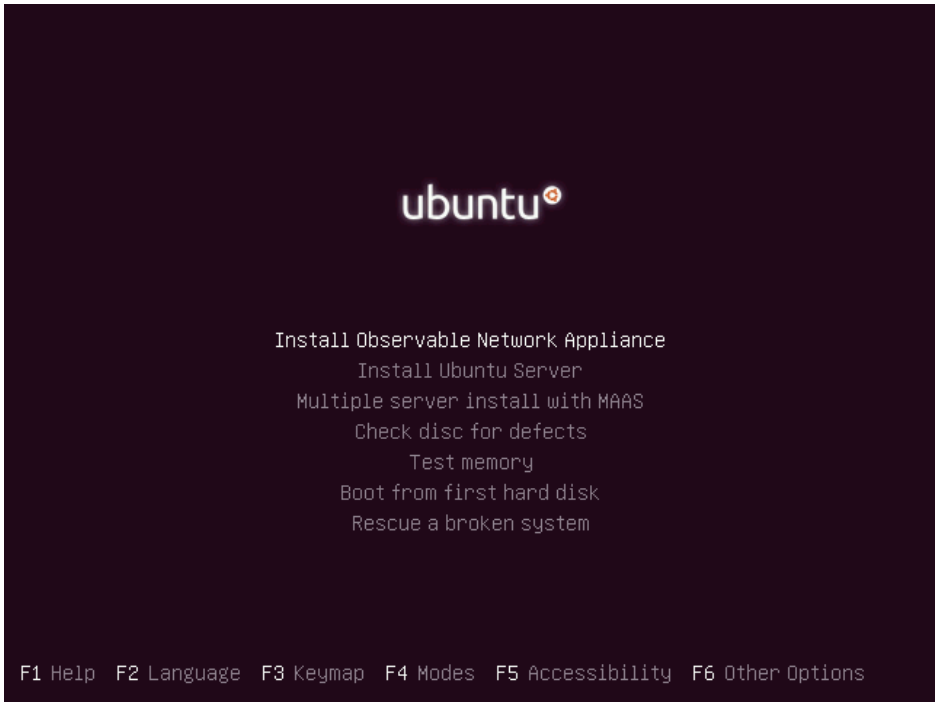
Please make sure you've selected the right ISO and USB drive; this is a destructive operation.





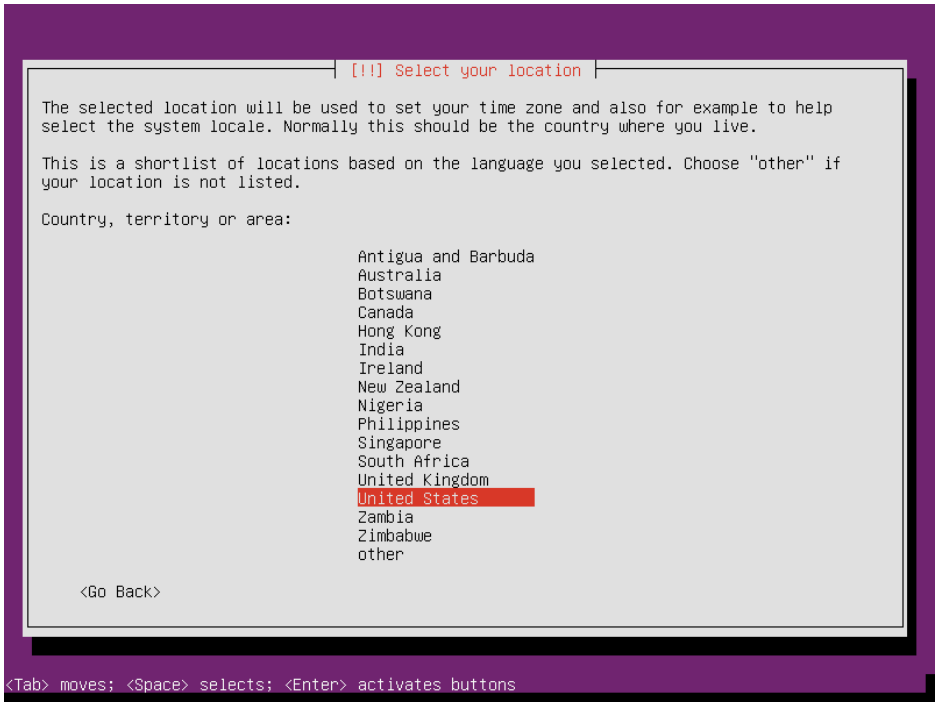
Language settings

When you see a prompt after booting to the CD, select the first option.



Location settings

Select a country. The default is United States.

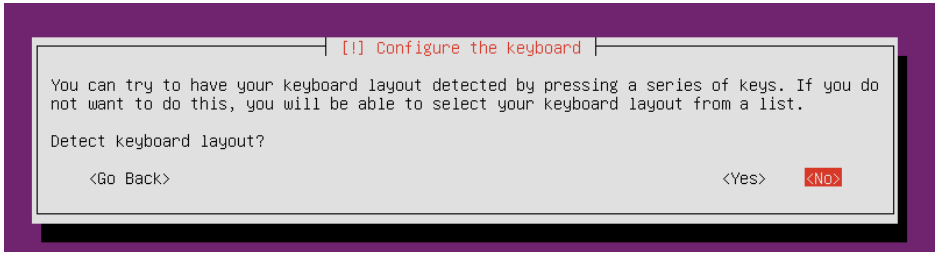


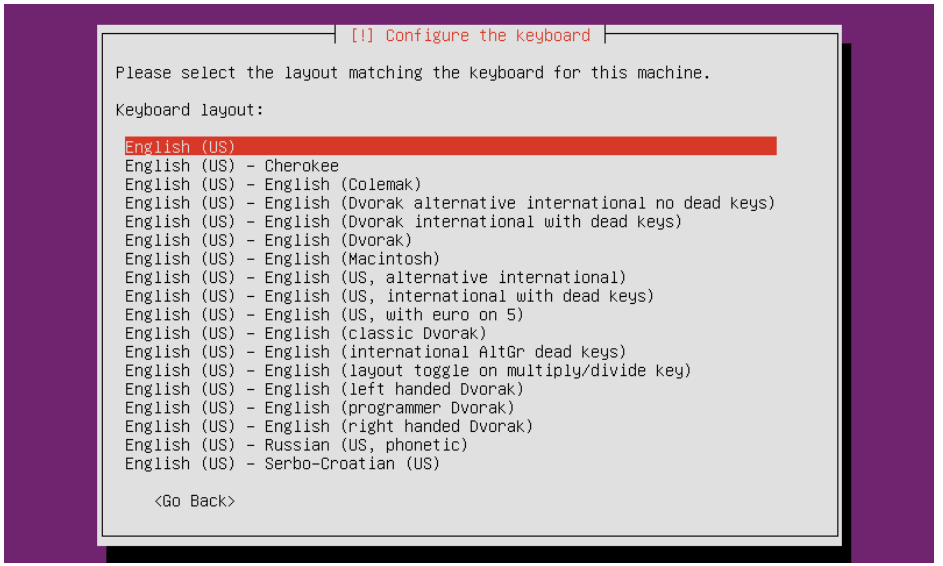
Keyboard settings

You may allow the installer to detect your keyboard layout.

However, if you use a standard US-English keyboard it is faster to select **No** when prompted to detect the layout.

At the next screen select your keyboard layout. The default is *English (US)*.



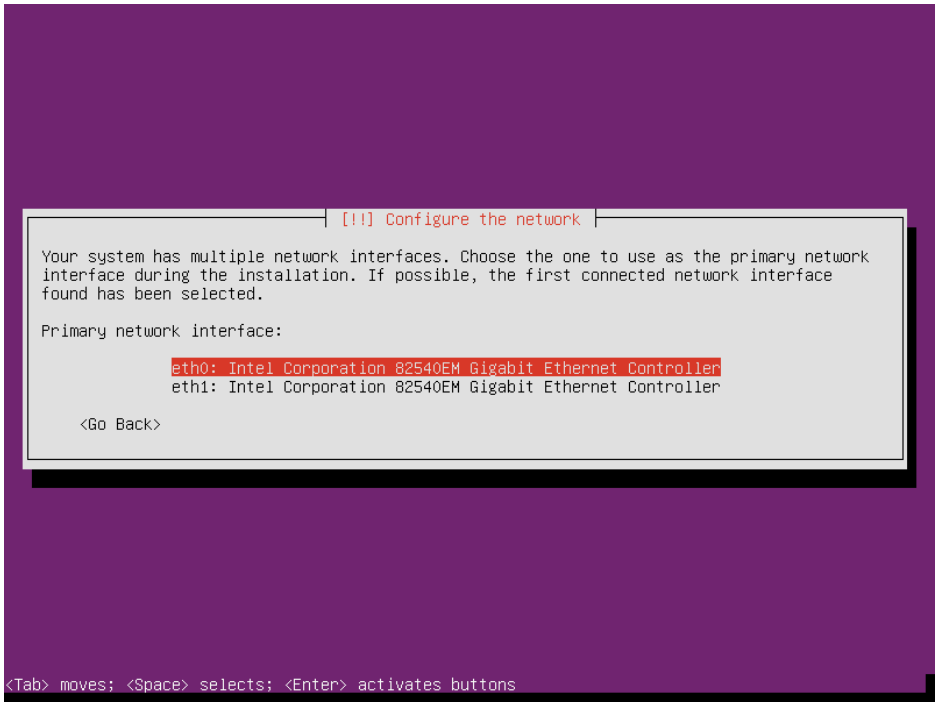


Network settings

If the installer detects multiple network interfaces, then it will prompt you to choose a “primary” one.

Select the interface that you will be using for **control** of the ONA, rather than the one that you will be using for mirroring traffic.

The other NICs will automatically be configured to accept mirrored traffic.



Network settings without DHCP

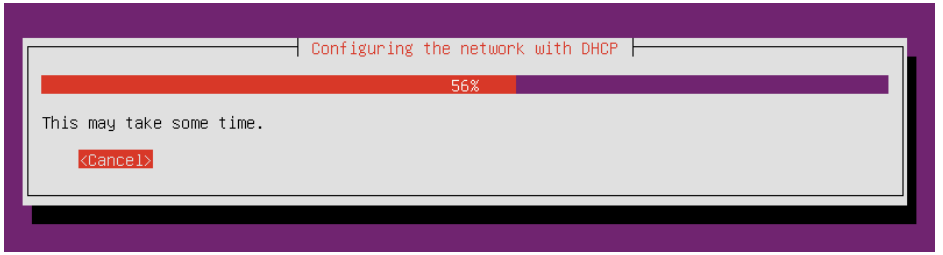
By default the installer will try to use DHCP to configure the interface you selected as the control NIC.

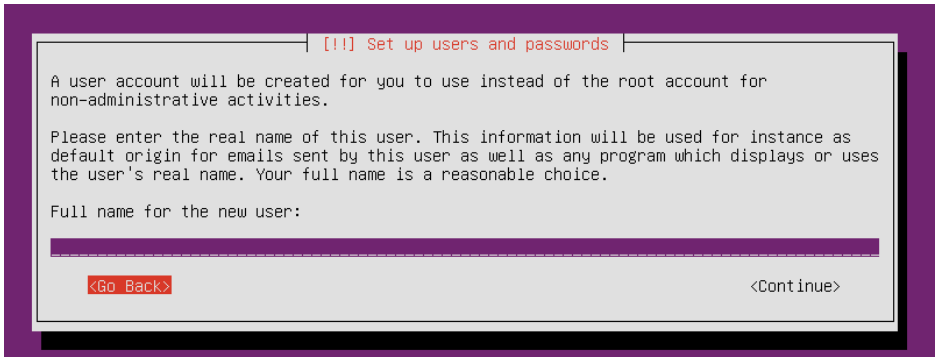
If DHCP is not set up on your network you will be prompted to configure the network manually.

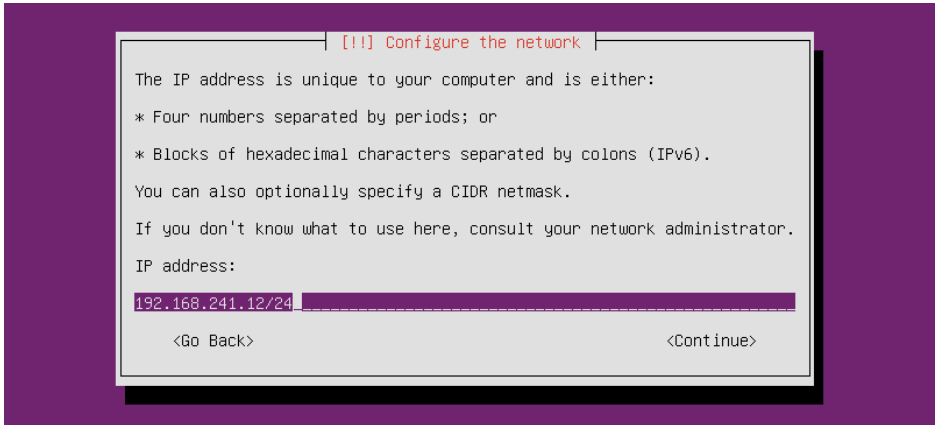
If DHCP is set up on your network, but you don't want to use it, press the Enter key to to **Cancel** while DHCP settings are being detected.

If you miss the chance to cancel, select **Go Back** (with the Tab key) at the next screen. Then select **Configure the Network** to try again.

When configuring the network without DHCP you will need to enter an address, subnet mask, and gateway; and also a DNS server and local domain suffix.





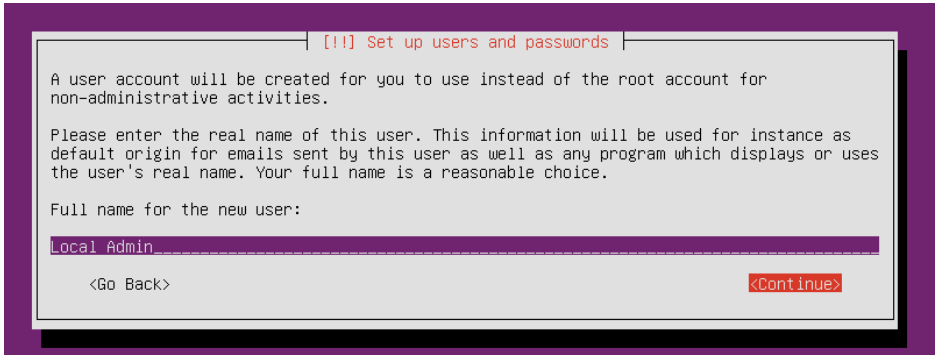


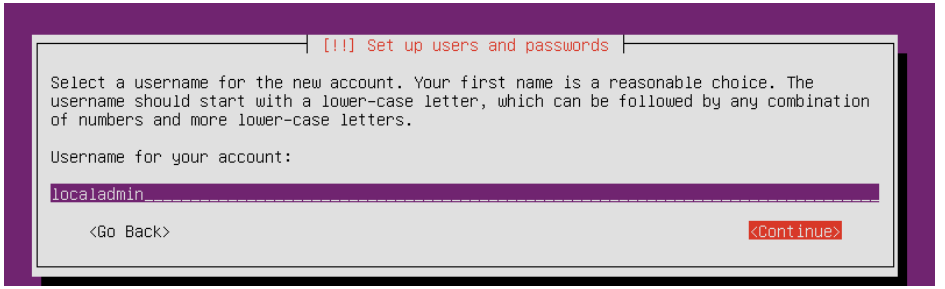
User account

You will be prompted to create a user account for local management of the system.

First, enter the full name of the for the account. This name can have spaces and capital letters (e.g., *Local Admin*).

Next, enter the username for the the account. This name can't have spaces or capital letters. (e.g., *localadmin*).

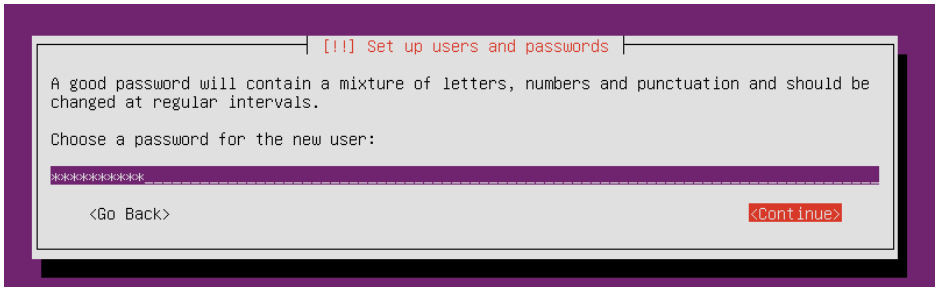


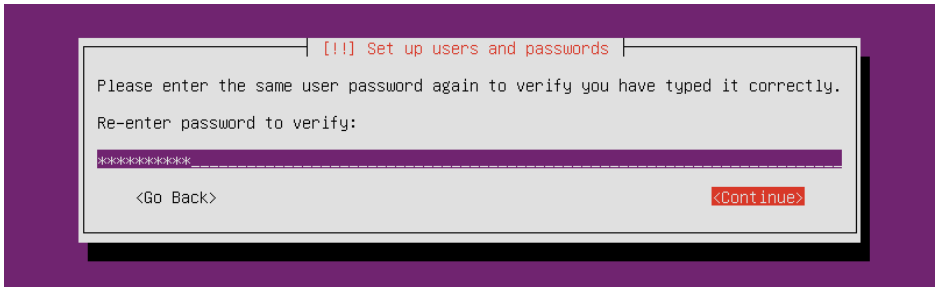


User account password

After you have entered a username you will be prompted to select a password for the local management account.

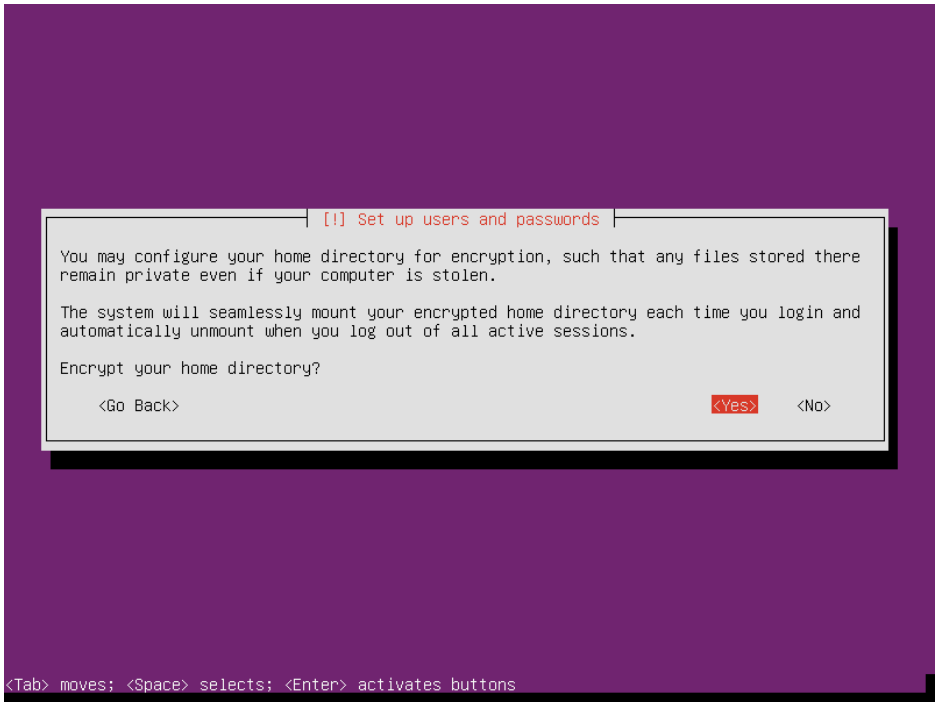
Enter the password into the first prompt and then again into the second verify it.





Encryption settings

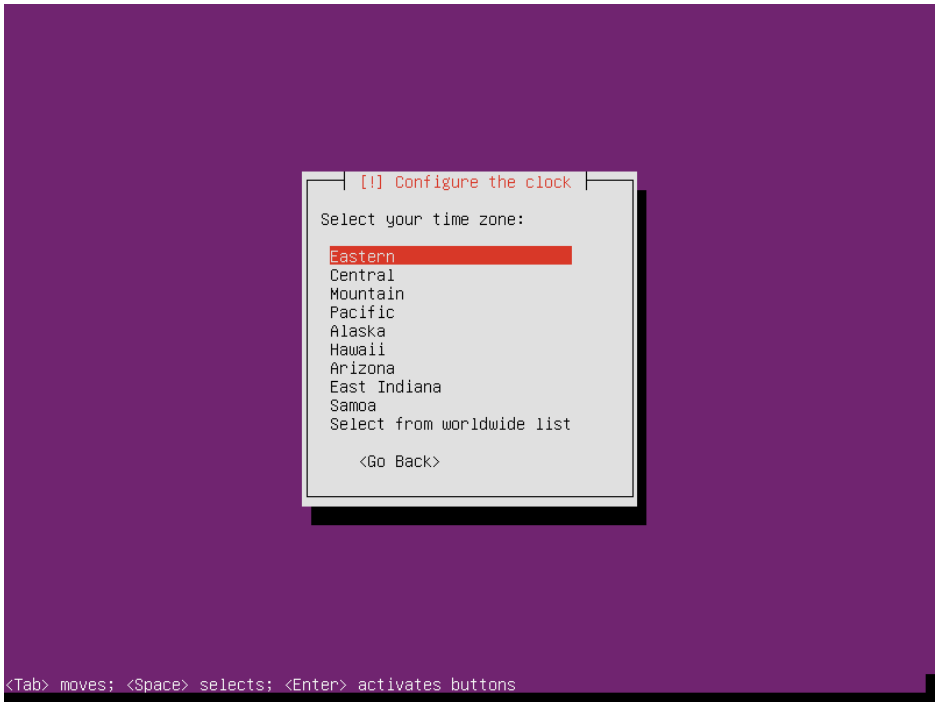
When prompted to encrypt the home directory for the local management user's account, select Yes.



Time zone settings

The installer may be able to detect your time zone automatically.

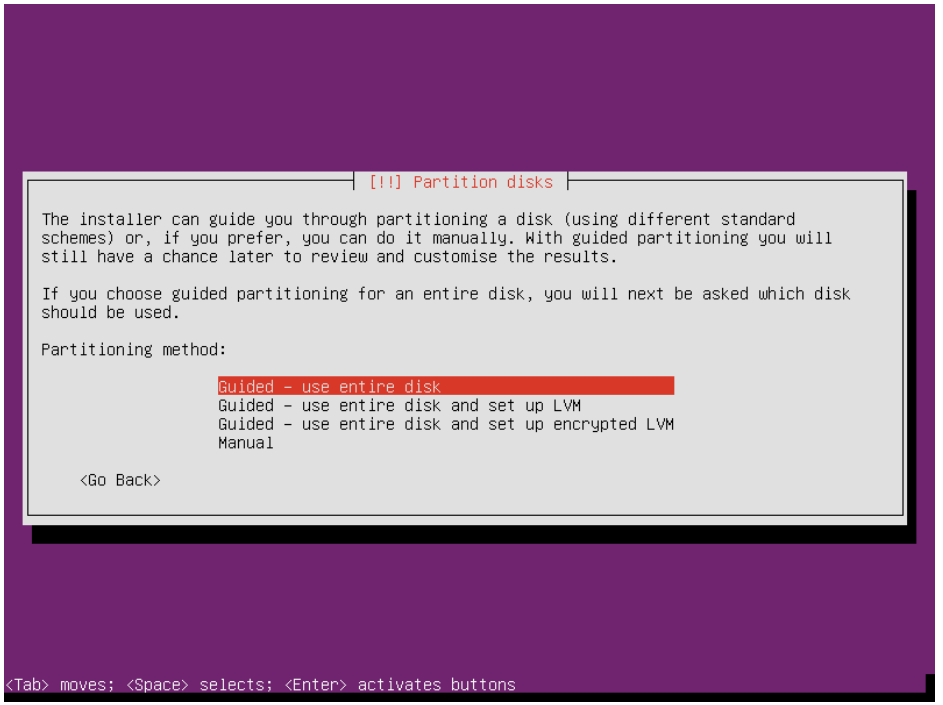
However, if you are prompted to configure the clock, select the correct time zone from the list.



Disk partitioning settings

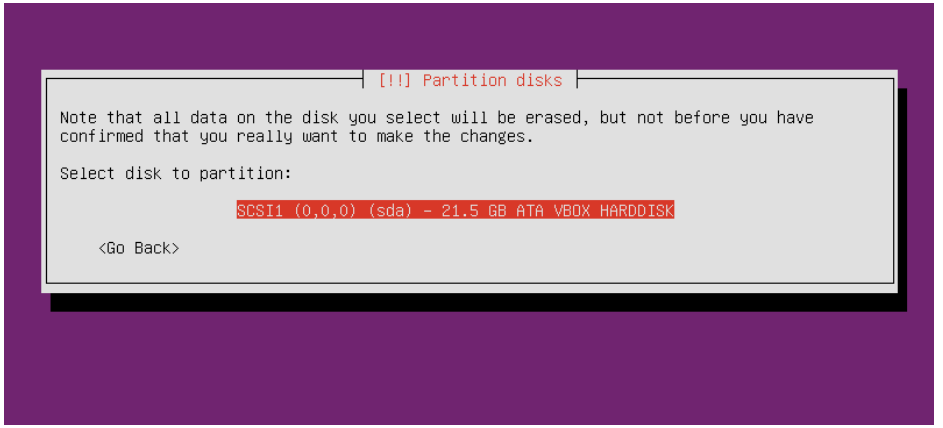
The installer can automatically partition the disk for the operating system.

The simplest option is to select *Guided – use entire disk*.

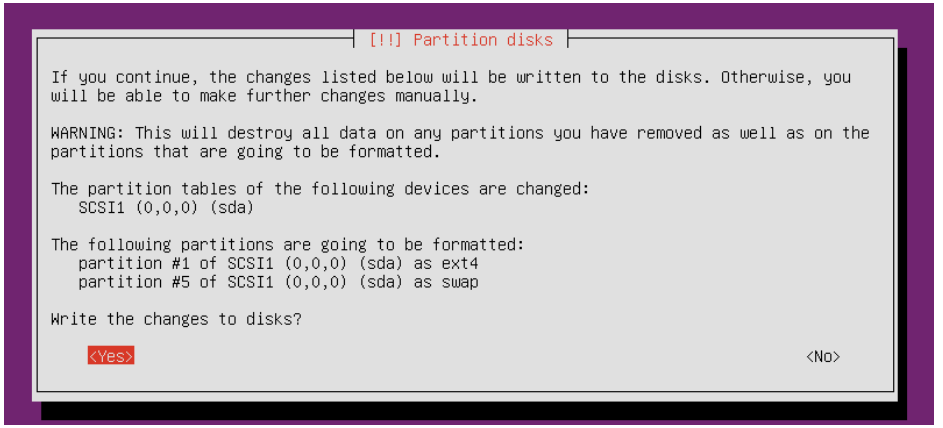


Disk preparation

When prompted, confirm that you are willing to erase the disk and install the operating system.



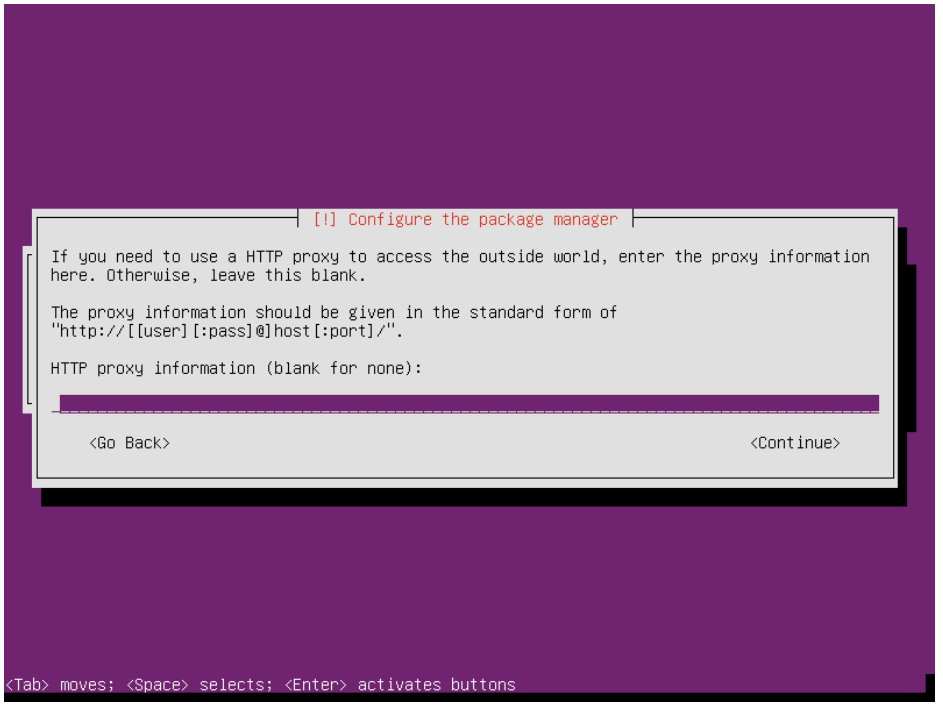
You will have to move the cursor to <*Yes*> and press Enter to start the partitioning.



Internet proxy settings

You will be prompted for HTTP proxy information.

Unless your network requires an HTTP proxy, simply press Enter to Continue.

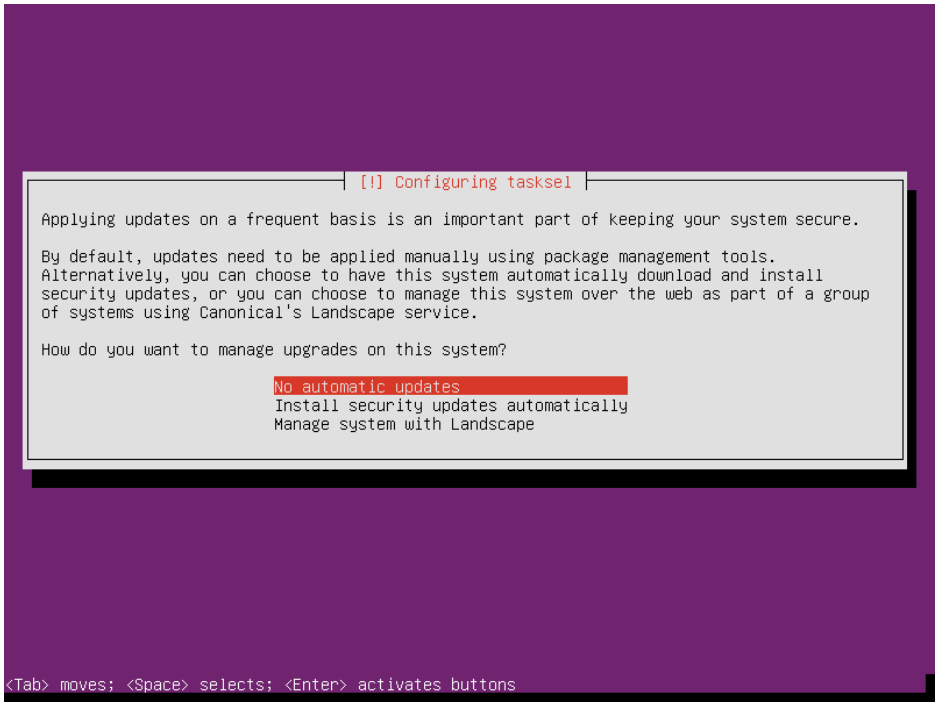


Automatic update settings

You will be prompted to select whether to install updates automatically.

The recommended setting is *Install security updates automatically.*

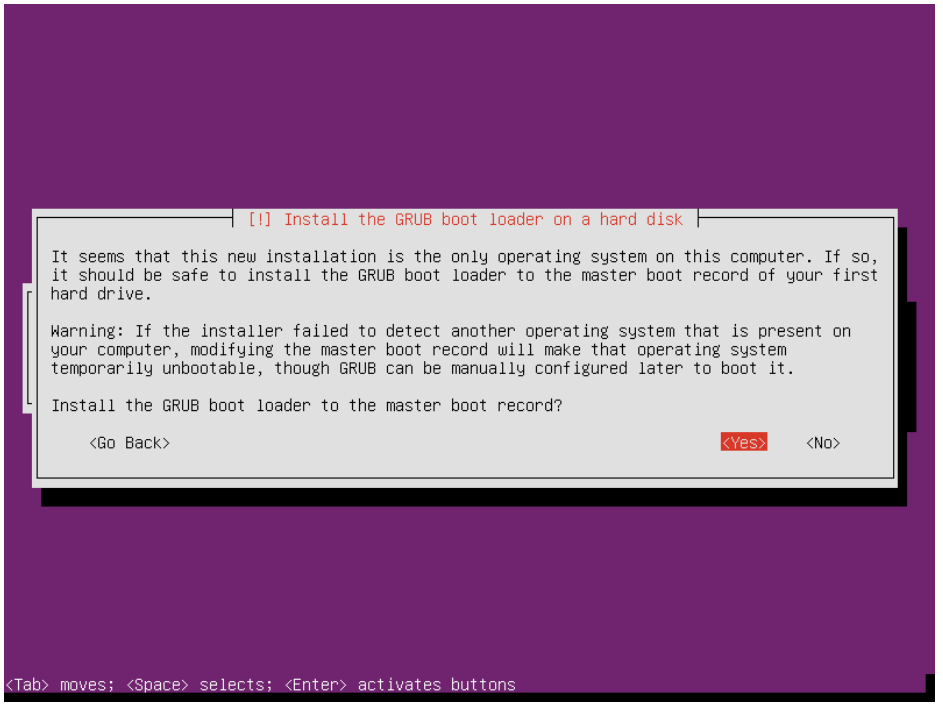
If your organization's policy doesn't allow for automatic updates select *No automatic updates*.



Boot loader installation

You will be prompted whether to install the GRUB boot loader onto the target drive.

Move the cursor to <Yes> and press Enter.



If there are connectivity problems...

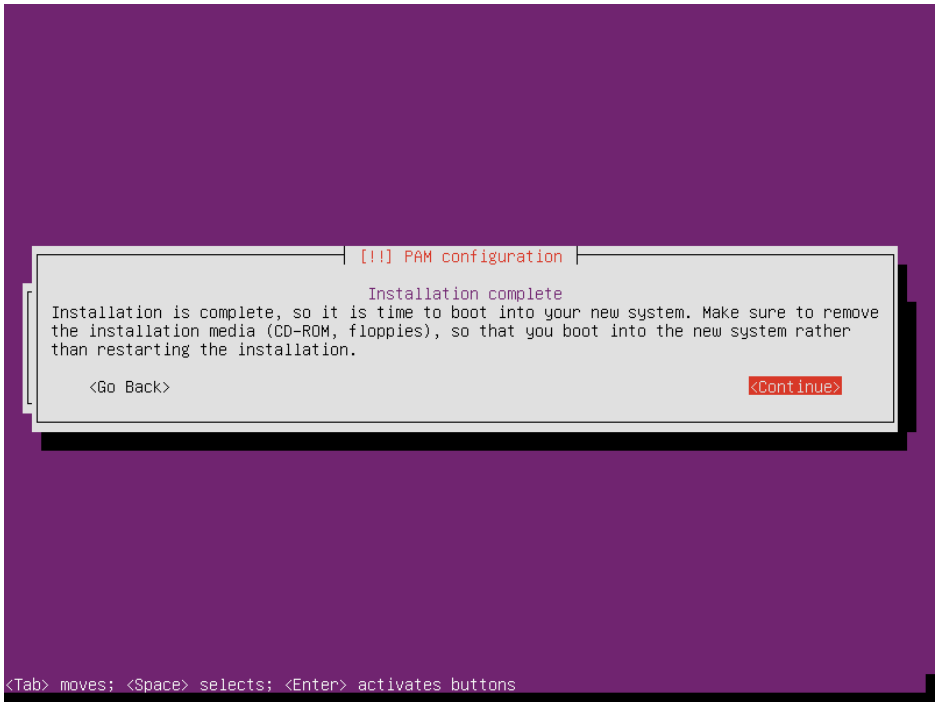
The installer needs to connect to the Internet to retrieve up-to-date packages. If there was an issue with getting to the Internet, you may seen the screen at right.

Double-check that the primary network interface has Internet access (including DNS). You may want to restart the installation once this is in place.

Installation complete

After the installer finishes copying files, eject the boot CD from the drive.

After the boot CD has been removed you may reboot the system.



After the system reboots, you may log in with the user account you set up during the installation.

You may log out (with the *exit* command) and leave the system unattended after verifying that it's working; it will run automatically after installation.

Return to the web portal to complete the setup process.