Lastline Enterprise Sensor

Installation and Administration

November 27, 2014

6950 Hollister Avenue, Suite 100
Goleta, CA 93117
lastline.com | 805.456.7076

1 Introduction

This guide describes the process to install the Lastline Enterprise Sensor component.

The Sensor sniffs the network traffic in order to collect artifacts (i.e., executables, documents, emails) that are received or downloaded by the users in the monitored network. These items are then passed to the Manager component, which processes and present them to the user.

2 Prerequisites

2.1 Hardware

The hardware certified for a Lastline Enterprise Sensor installation is a Dell PowerEdge R320 with the following specification:

- Chassis with Hot Plug Hard Drives [1] [2]
- Intel® Xeon® E5-2430 2.20GHz, 15M Cache [3]
- 16 GB ECC RAM [3]
- 500 GB SATA HDD [3]
- Dual Hot Plug Power [1]
- iDRAC7 Enterprise [1] [4]
- ProSupport Service Plan [1]
- Intel Ethernet I350 Quad-Port 1Gb Server Adapter

Note: a Sensor can be identified (among a Manager and an Engine) because it has an additional four-port network card.

2.2 Network Connectivity

The server needs to be able to connect to:

- *log.lastline.com* to TCP port 443.
- *update.lastline.com* to TCP port 443 and optionally to UDP port 123 for time synchronization. The latter can be replaced with a local NTP server.
- *management.lastline.com* to TCP port 443.

All the connections can be optionally routed though an explicit HTTP proxy. Proxy authentication is not supported.

2.3 License

Before starting the installation, the user has to acquire a license for the software. This is done by contacting the Lastline sales team at `sales@lastline.com`.

The sales team sends the user a link to download an ISO image for the installation. The user downloads the ISO image and boot the server from the ISO image (e.g., by burning a DVD, creating a bootable USB stick, or using the Dell iDRAC interface, if available on the server).

[1] Optional.

[2] Lack of Hot Plug chassis will required a server downtime (even for RAID configurations) and opening the chassis for replacing a failed HDD. Also, it will lack the LCD module used for monitoring the status of the server and fast configuration of the iDRAC device.

[3] Or better.

[4] iDRAC Enteprise allows remote control of the server, including remote console redirection.

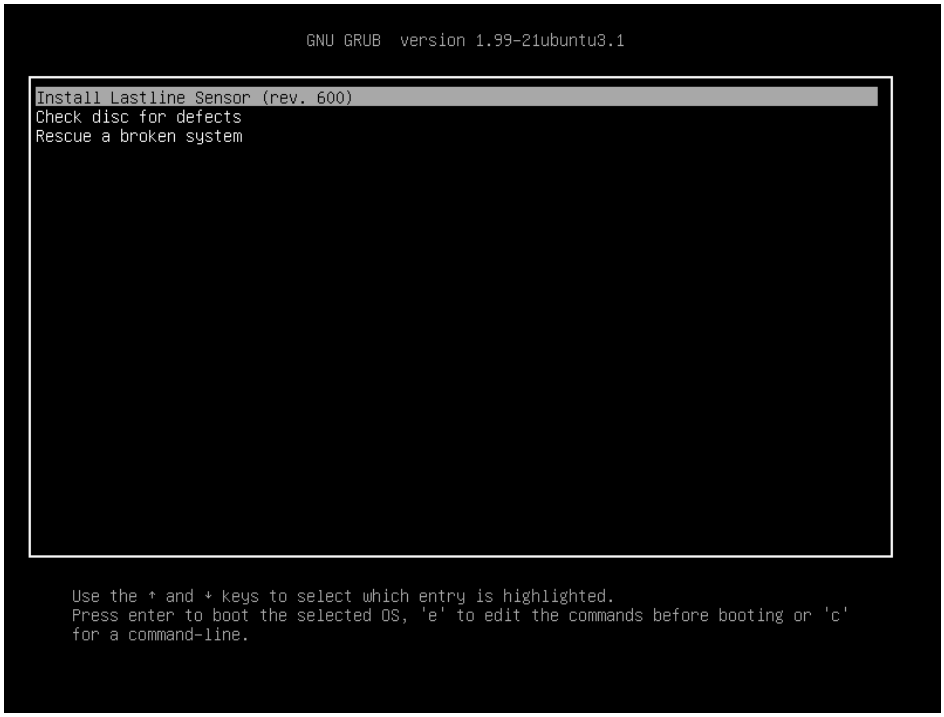
3 Installation Process

The installation process for the Lastline Enterprise Sensor consists of three steps. In the first step, the base system is installed. In the second step, basic configuration information is collected and the configuration is applied to the system. In the final step, required data from the Lastline's servers is retrieved.

3.1 Base System Installation

The Lastline Enterprise Sensor uses as the underlying operating system Ubuntu Server 12.04.05 LTS 64 bit (Precise Pangolin distribution). Therefore, many of the steps of the installation are similar to the ones required to install Ubuntu Server[5].

At the beginning of the booting procedure from the installation medium, the user selects "Install Lastline Enterprise Sensor" from the splash screen (see picture below). The number in parenthesis refers to the revision of the installer program. Depending on whether your system is configured to boot to UEFI or BIOS mode, the boot loader splash screen will be different, as shown below.

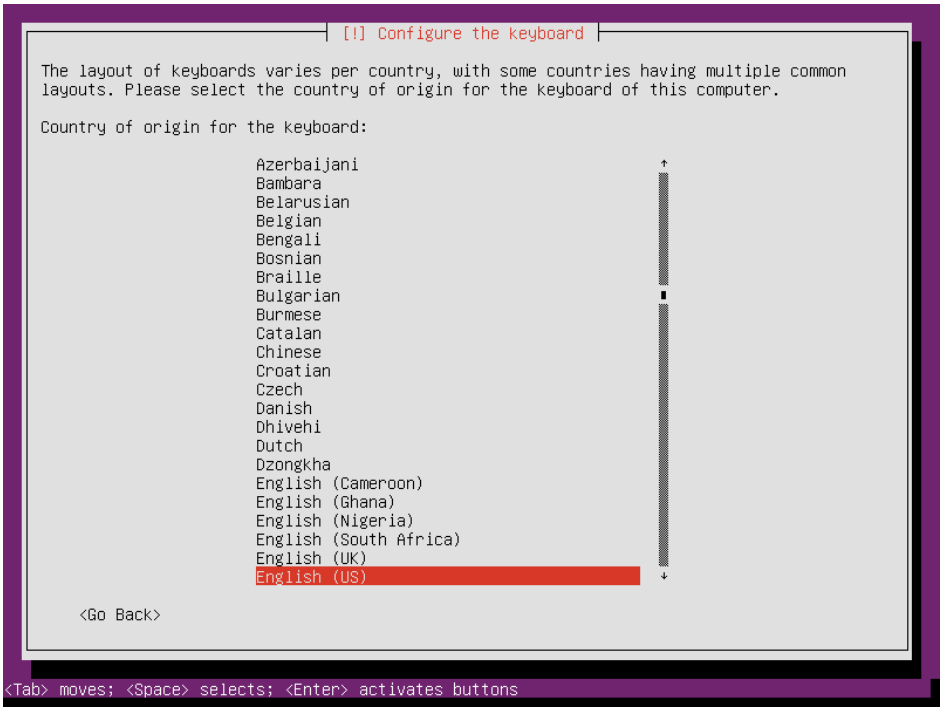


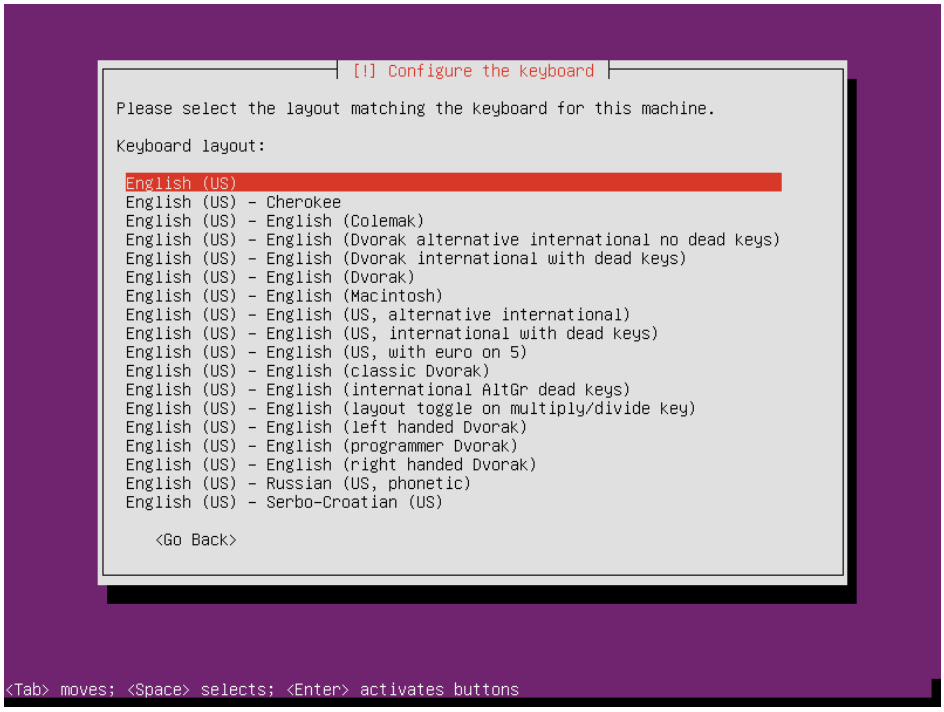
Splash screen in UEFI boot mode.

[5]The Ubuntu Installation guide can be found at https://help.ubuntu.com/12.04/installation-guide/amd64/index.html. Note that many steps of a standard Ubuntu installation have been automated and hidden from the Lastline Enterprise Sensor Installer.

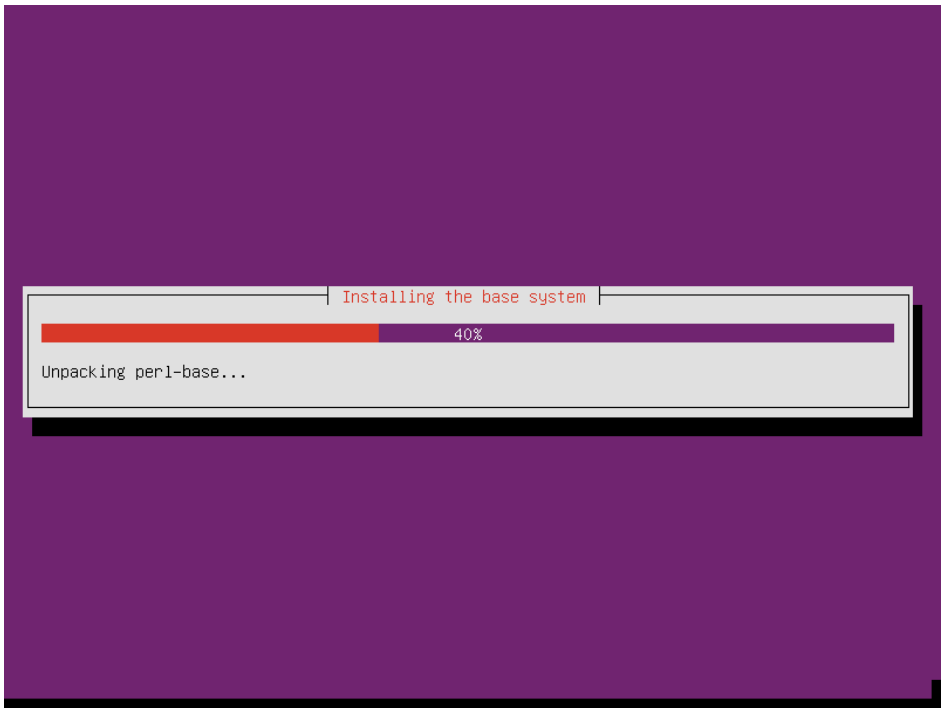
Splash screen in BIOS boot mode.

Then, the user answers questions regarding the localization of the installation (type of keyboard, language, see pictures below).





At this point, the installer proceeds to install the base system. This phase will take a few minutes (see picture below).



After the base system was installed successfully, the system will automatically reboot. After the boot process has completed, a login prompt as in the following screenshot is shown.

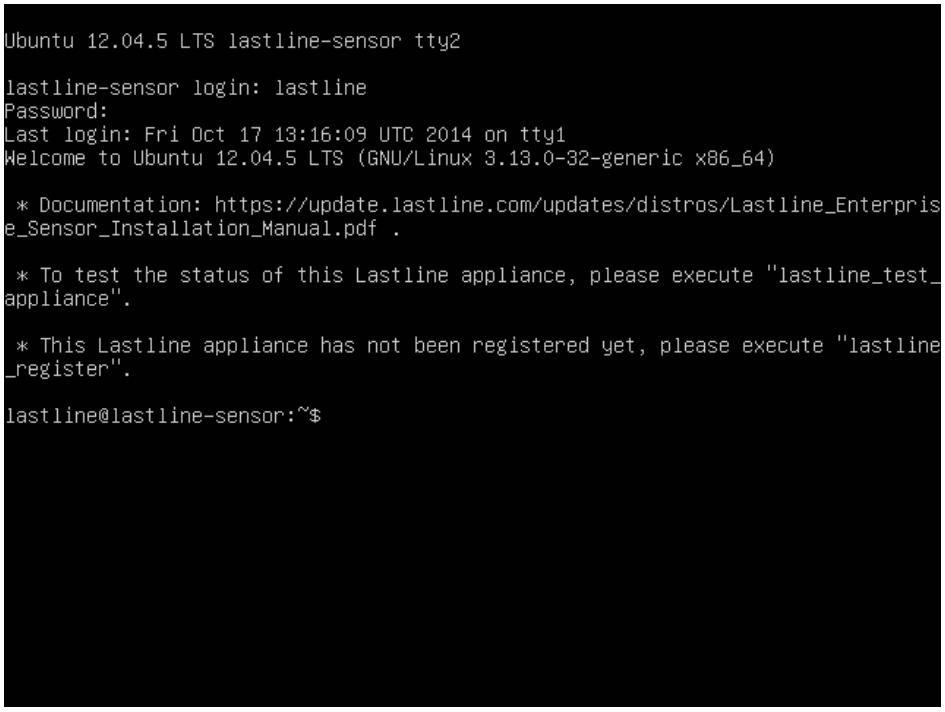
3.2 Registration and Configuration

To register and apply the software configuration to the Lastline Enterprise Sensor, the user logs into the console using

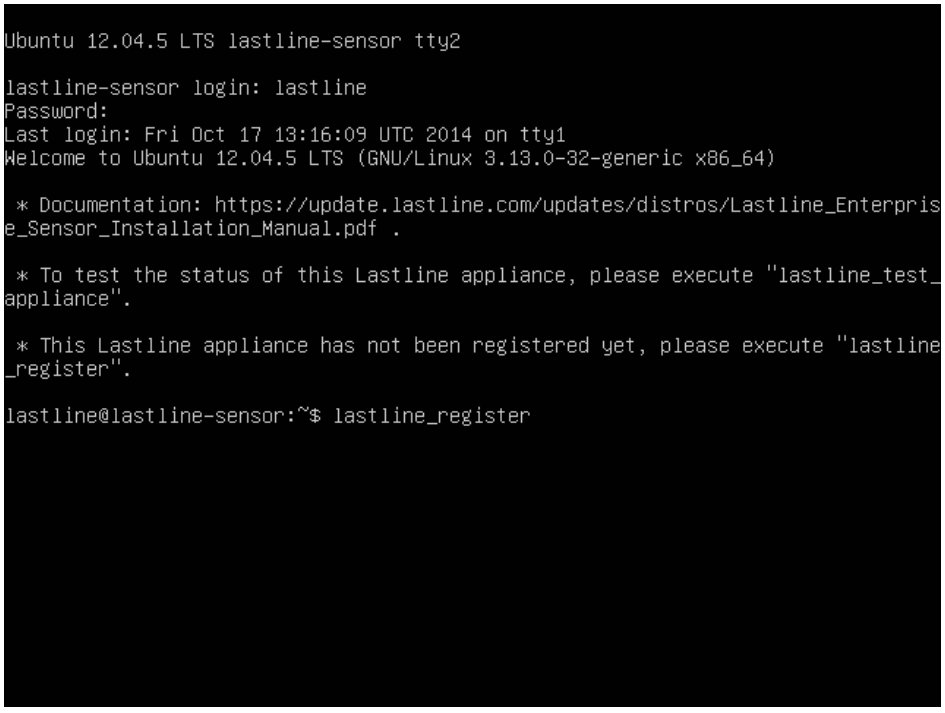
- username `lastline` and
- password `lastline`

as shown in the screenshot below. Note, it is possible to login with username and password only from a console[6].

[6] Remote access requires the use of SSH keys.

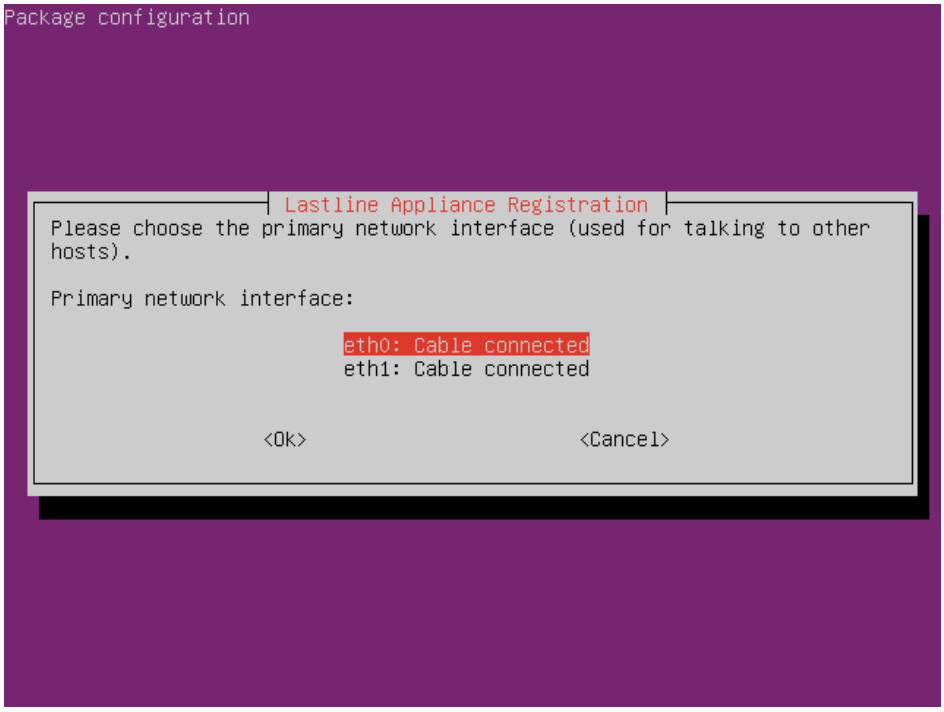


The user executes `lastline_register`, which will start the guided configuration and installation process. Please insert `lastline` as `sudo` password if asked.

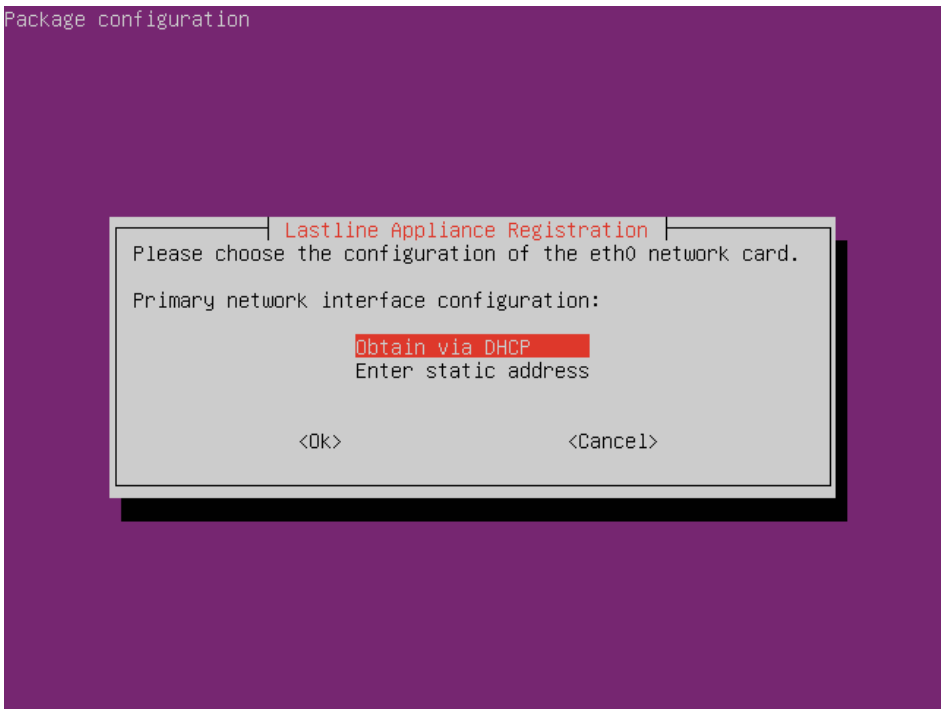


First, the user is asked about the network configuration of the Lastline Enterprise Sensor.

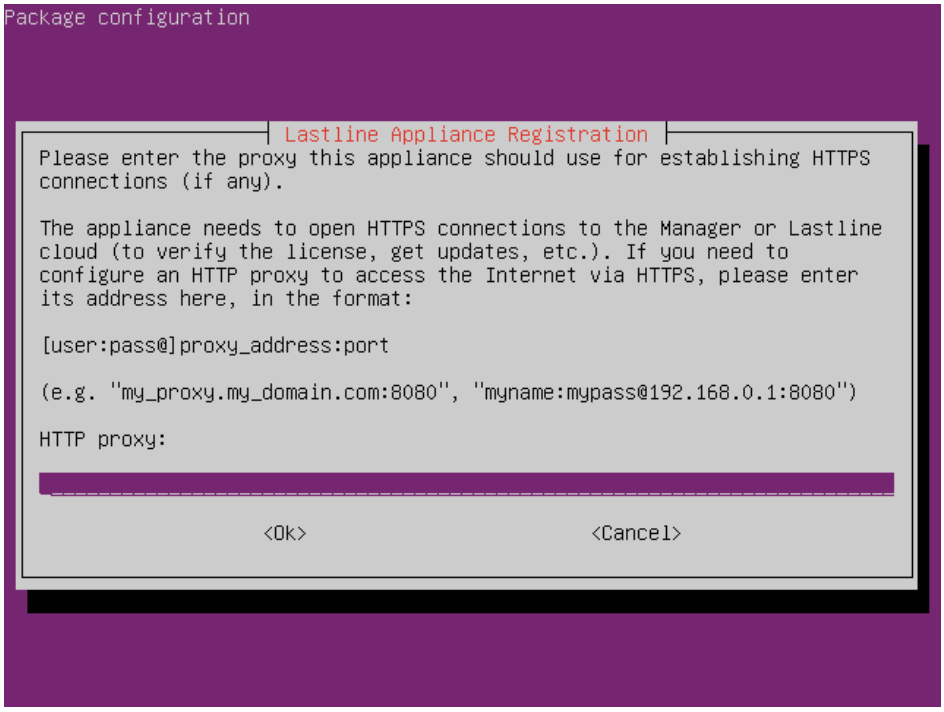
The user will be asked to select the primary network interface, i.e., the interface used by the server to communicate with the other hosts of the network (see the picture below).



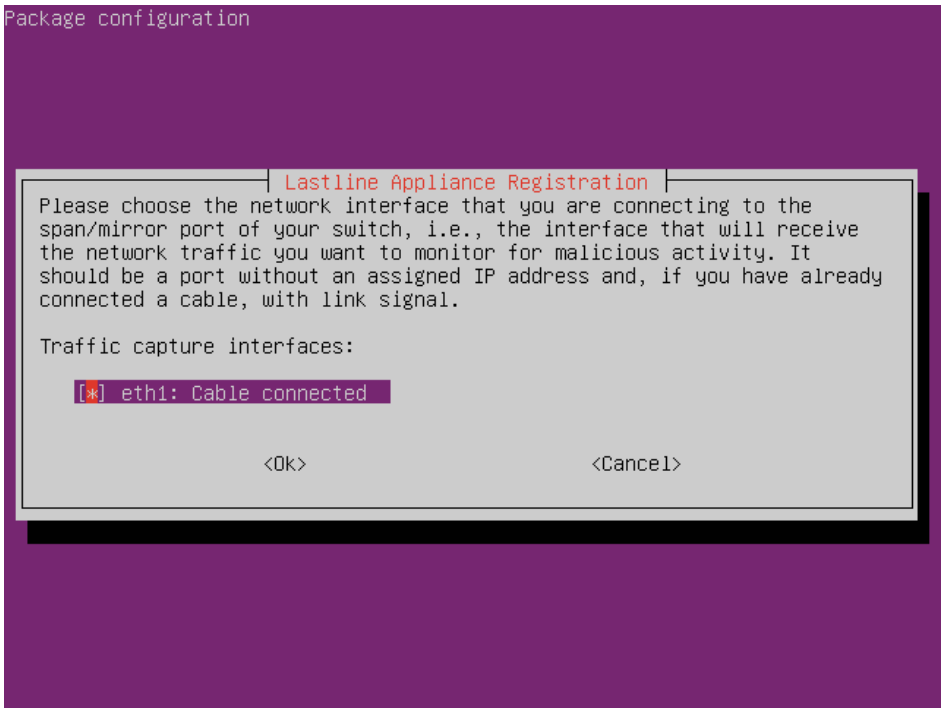
The installation process will then give the user the opportunity to configure the network via DHCP or with a static IP address. In the latter case, the user should select “Enter static address” and, when prompted, input the IP address to be assigned to the interface, the network netmask, as well as the gateway and name server address.



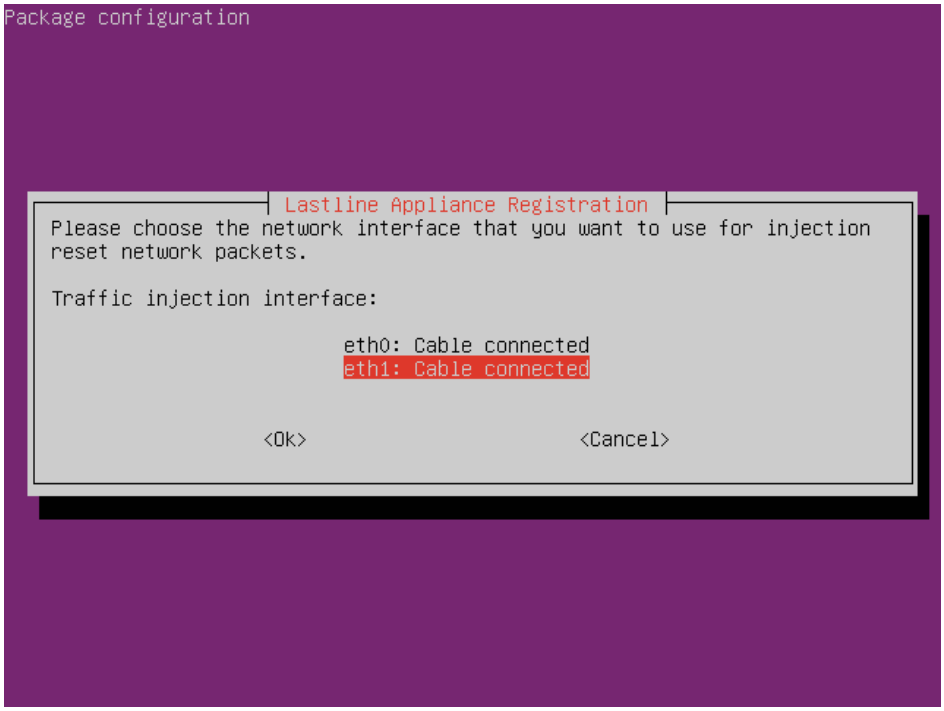
The user then has the option of configuring an HTTP proxy for connecting to Lastline’s servers (see picture below). If no proxy configuration is required to access the Internet via HTTPS, this field should be left empty. Otherwise, if all HTTPS connections need to go through an HTTP proxy, the address of the proxy must be entered here. Optionally, a non-default port of the proxy server can be specified. Valid proxy configurationexamples are: **`my_proxy.my_domain.com:3128`**, **`192.168.0.1:8080`**.



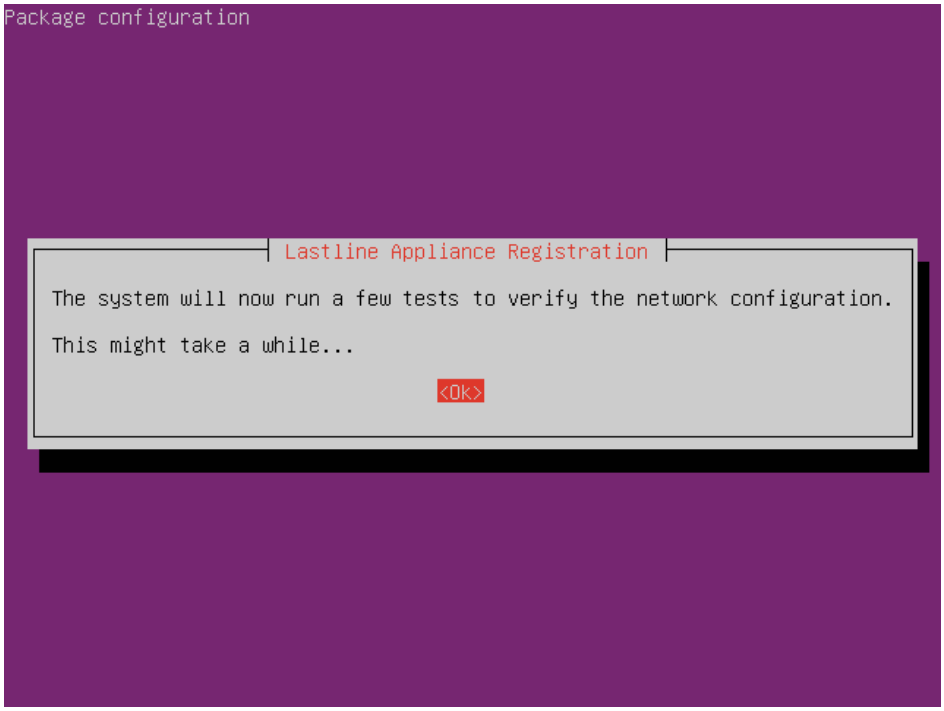
After that, the user will be asked to choose the interface(s) connected to the span/mirror port of the network switch, i.e., the interface(s) that will receive the network traffic to be monitored for malicious activity. A span/mirror interface will not be assigned an IP address



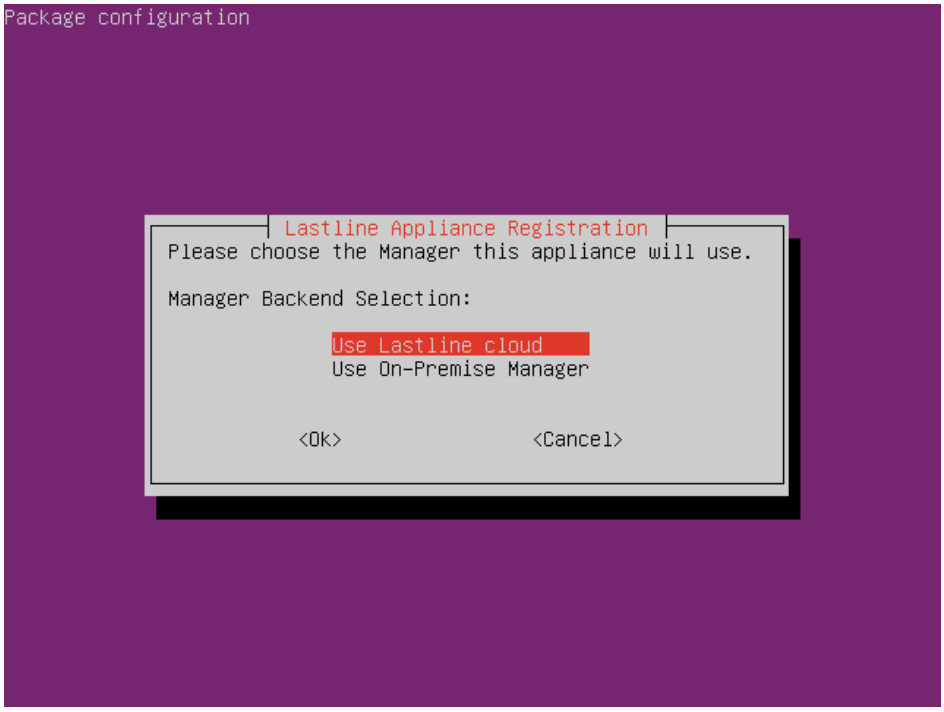
In the next screen the user can chose a network interface to be used for injection of network reset packets. This interface has to be able to communicate with the other hosts of the monitored network.



At this point, the network configuration is applied and further tested to check for sufficient connectivity to the Lastline backend. Further, a set of tests regarding hardware compatibility are executed.

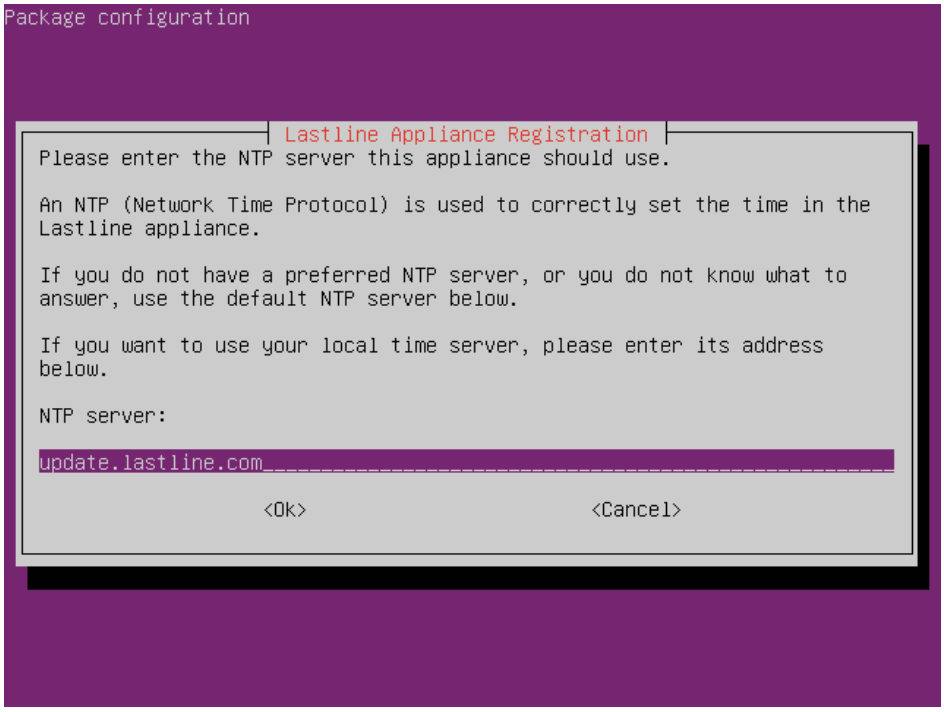


At this point the user is asked to choose the manager backend, as shown below.

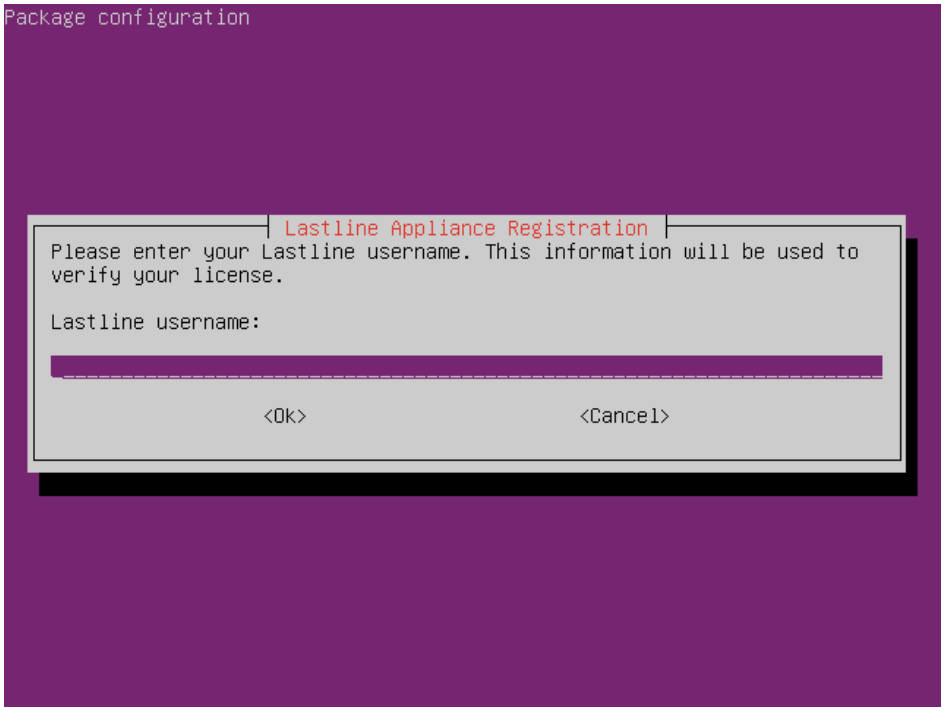


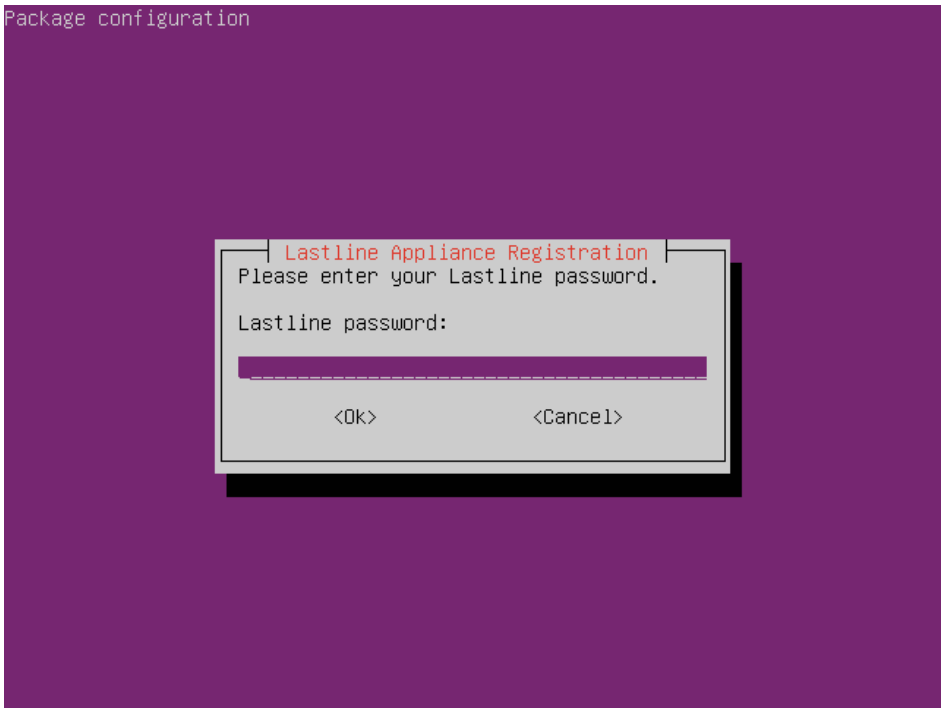
If the Lastline Enterprise Sensor installation is not part of an On Premise deployment, the user should choose ”Use Lastline cloud“.

In the following step, the system will ask for a NTP server (see picture below). Unless the use of a different NTP server is needed, the user can use the default value. The system must be able to reach the chosen NTP server over UDP port 123.



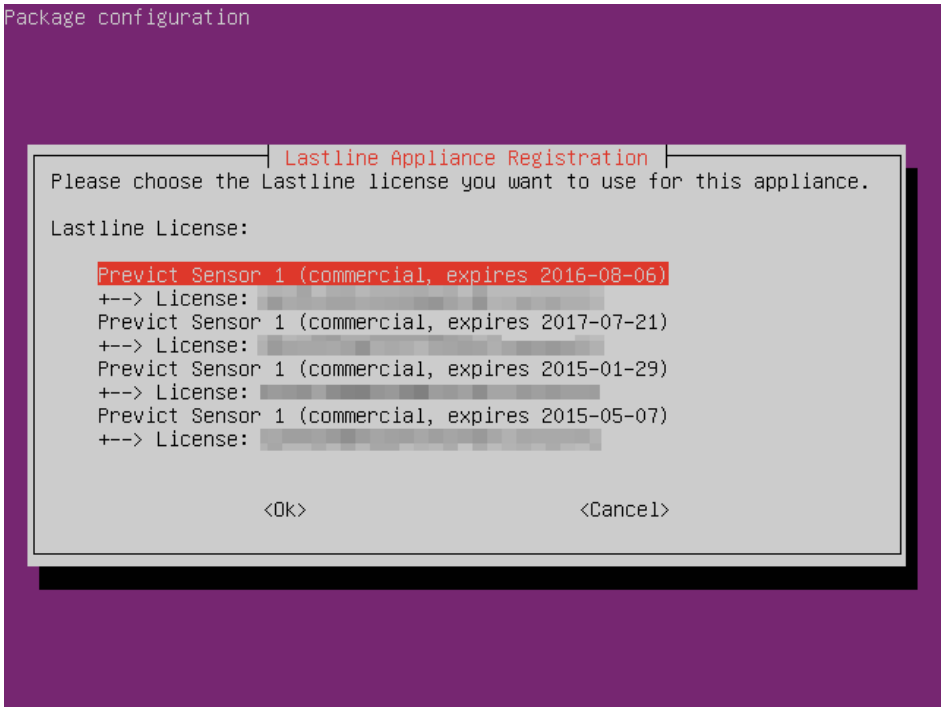
Next, the user must provide the license information associated to this Lastline Enterprise Sensor system. More precisely, the user is required to enter the username and password provided during registration (see pictures below).



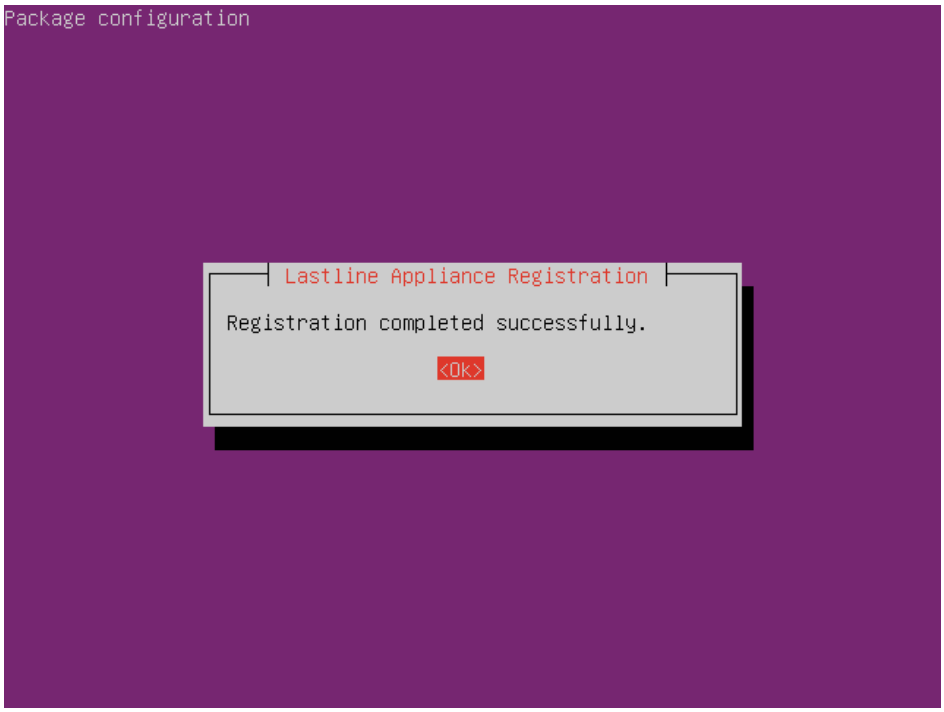


If the provided credentials are valid, the user will be shown the available license keys and will be able to choose or approve a pre-selected choice as shown below[7].

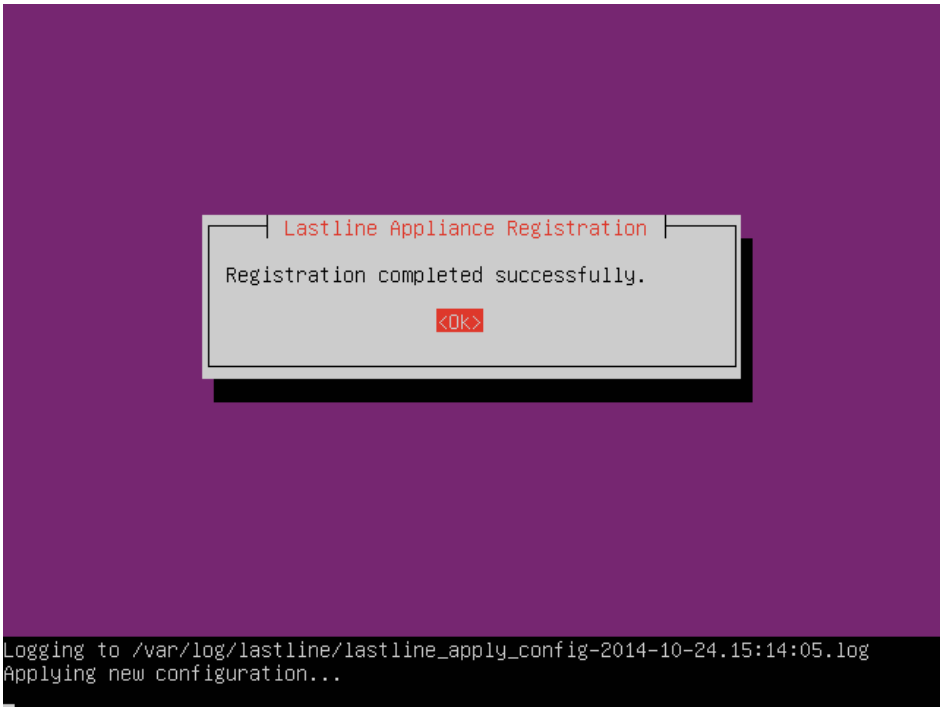
[7] Please contact support@lastline.com mentioning the corresponding error message if the list of license keys is not retrieved correctly.



After fetching the license information and configuration, the registration has completed.



The setup program will now apply the configuration to the machine. This process may take several minutes (20-40) depending on network connectivity and system characteristics.



In case any error message is displayed, please refer to Section 4.2 .

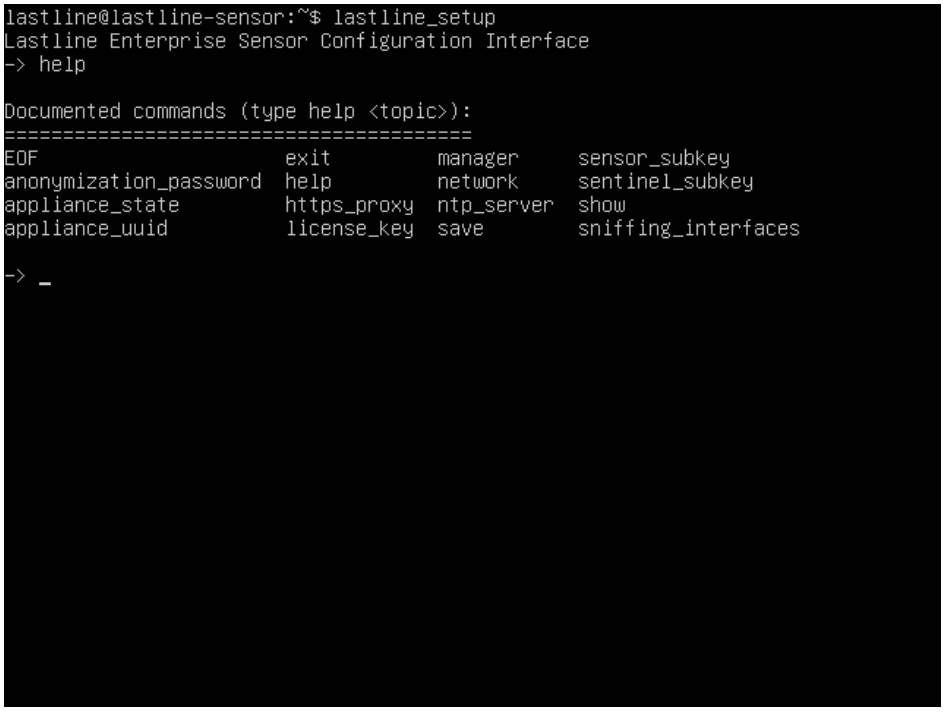
4 System Administration

The Lastline Enterprise Sensor is developed to require as little maintenance and administration as possible. The only action that might be required is to change the system's network configuration, as discussed below. Moreover, we show how to customize and configure some advanced features of the Lastline Enterprise Sensor.

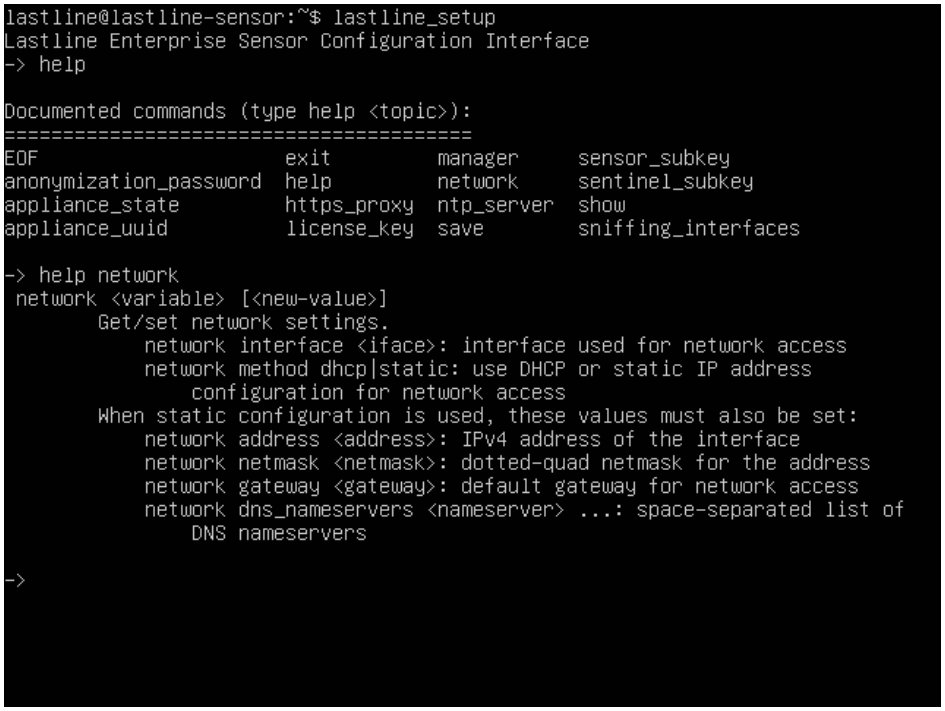
We also provide a troubleshooting guide that allows the administrator to ensure that everything works properly.

4.1 Lastline Configuration Tool

The system comes with the Lastline configuration tool `lastline_setup`, which provides and interface to administrate and manage the Lastline Enterprise Sensor. The tool can be started as shown below.



After starting the tool, to view all the supported commands, issue the `help` command. A detailed description of each command is shown when issuing `help <command>` (e.g. `help network`).



4.2 Error handling

In case any error message is displayed when using `lastline_setup`, please contact support@lastline.com

4.3 Network Configuration

This section shows how modify the network configuration of an Lastline Enterprise Sensor. This may be necessary in case the IP address assigned to the system is modified (e.g., upon a reconfiguration of the DHCP server).

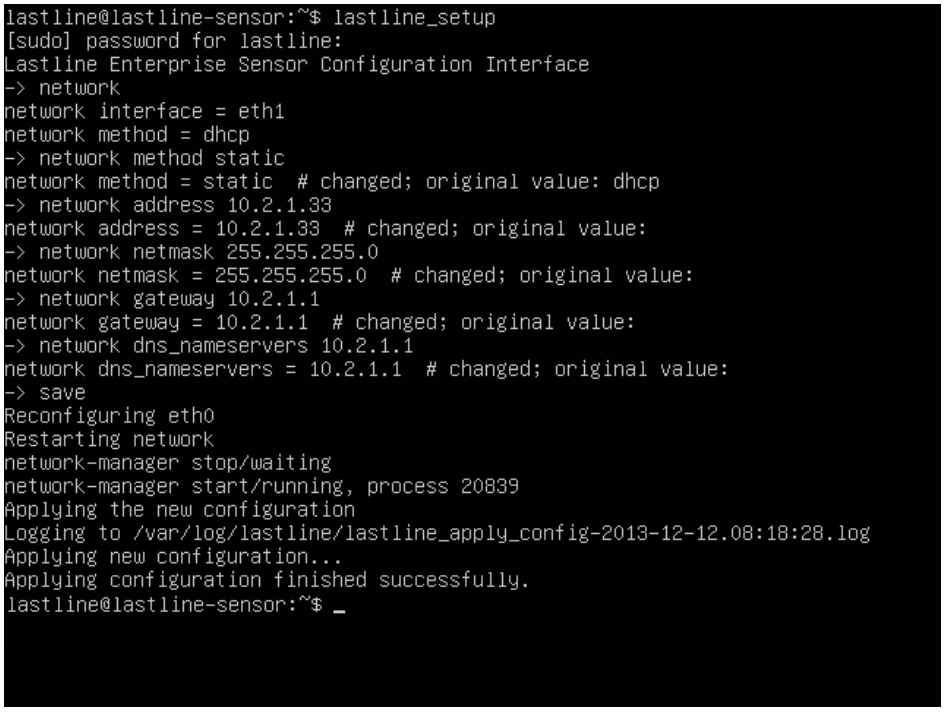
4.3.1 Configuration of Network Address through DHCP

To switch to a DHCP-based network configuration, use the `network` command as outlined below.

```
lastline@lastline-sensor:~$ lastline_setup
Lastline Enterprise Sensor Configuration Interface
-> network
network dns_nameservers = 10.2.1.1
network gateway = 10.2.1.1
network netmask = 255.255.255.0
network address = 10.2.1.33
network interface = eth1
network method = static
-> network method dhcp
network method = dhcp  # changed; original value: static
-> save
Reconfiguring eth0
Restarting network
network-manager stop/waiting
network-manager start/running, process 20839
Applying the new configuration
Logging to /var/log/lastline/lastline_apply_config-2013-12-12.08:18:28.log
Applying new configuration...
Applying configuration finished successfully.
lastline@lastline-sensor:~$ _
```

4.3.2 Configuration of Static Network Address

To enable a network configuration using a static IP, use the `lastline_setup` tool (see Section 4.3.1) as outlined below substituting values for *address*, *netmask*, *gateway*, and *dns-nameservers* accordingly.



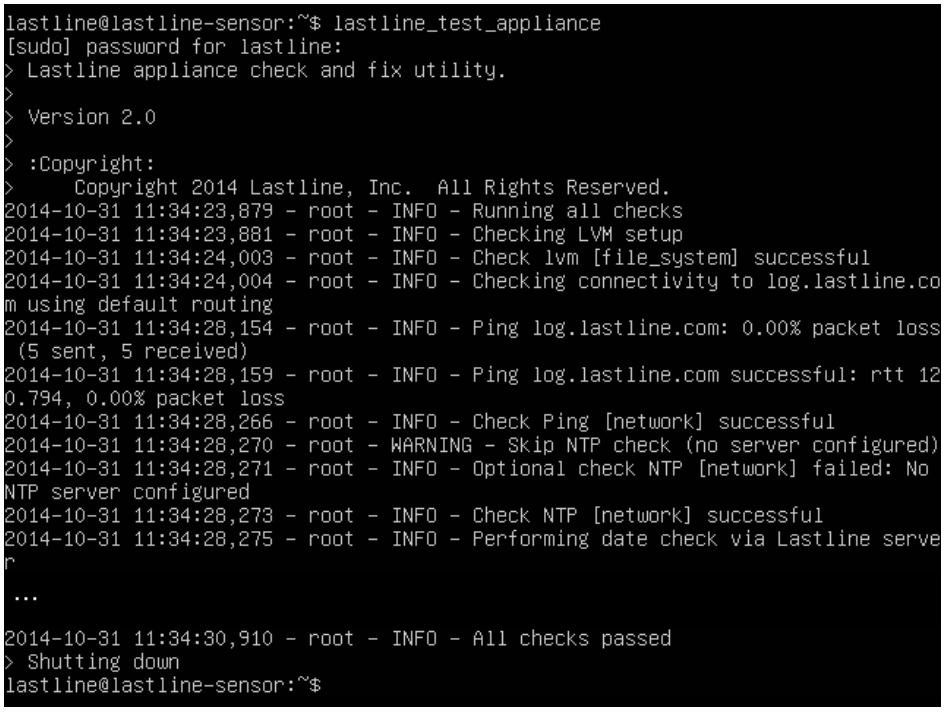
5 Software Upgrades

Lastline periodically releases appliance upgrades or hotfixes. If the appliance has automatic updates enabled, these will transparently be applied to the system.

Automatic updates are enabled by default upon installation. In order to disable automatic upgrades, or to manually upgrade an appliance with automatic updates disabled, the user can log in on https://user.lastline.com and access the appliance configuration page from the Appliance tab.

6 Support

The user can check the state of the system by running the `lastline_test_appliance` tool, as shown below.

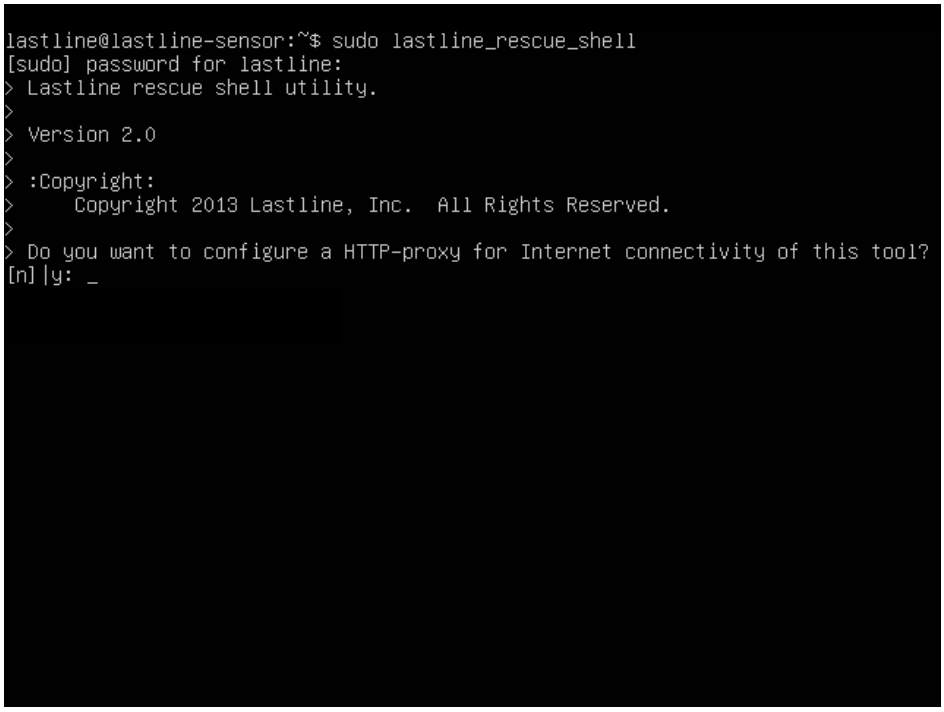


This utility program checks for signs of common configuration errors and can help customers fixing them. For any support request please contact support@lastline.com.

6.1 Rescue Shell

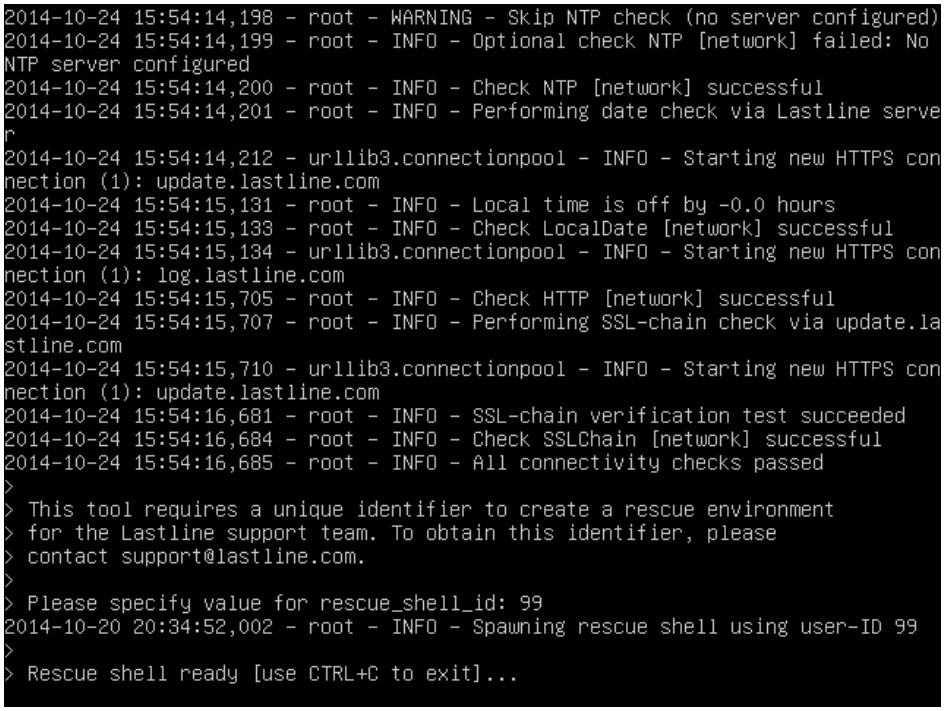
In some situations, it can be valuable to give a member of the Lastline support team remote-access to the Lastline Enterprise Sensor appliance. This is useful to help the customer with configuration problems or recover from unexpected issues.

For this reason, each appliance is shipped with the utility Lastline `lastline_rescue_shell`.



Using a connection-identifier provided by the support team, it provides a secure connection between a member of the support team and the customer appliance, allowing a technician to resolve any issues the utility was unable to handle automatically.

To start the utility, use the steps shown. The secure channel to Lastline can be interrupted at any time by pressing `CTRL+C`.



6.2 License Extensions

To renew an expired license, contact sales@lastline.com.

7 Copyright

The appliance is running on Ubuntu Linux and therefore contains code from a number of open-source projects. For a full list of included open-source packages and attribution of authorship and license/copyright, please refer to https://update.lastline.com/updates/distros/open-source-licenses.txt.