# redBorder IPS 3

# Quick installation guide

# redBorder IPS 3 Quick installation guide

Author info@redborder.com

ISBN: No disponible

**ENEO Tecnología S.L.**

Plaza de las Naciones s/n, Torre Norte (Edificio Aljarafe Center). Planta 12.
Mairena del Aljarafe
Sevilla
41927
+34 955 60 11 60
Spain
*info@redborder.com*

# Installing the redborder Manager

## 1.1. Requirements

redBorder is a software which has some minimum requirements in order to function correctly. The minimum essential elements required for installation as well as those recommended for correct performance are shown in the following chart:

### Installation requirements

**Minimum requirements**

RAM 16GB

Processor: 2 cores

HD 24GB

**Recommended requirements**

RAM 32GB

Processor: 4 cores

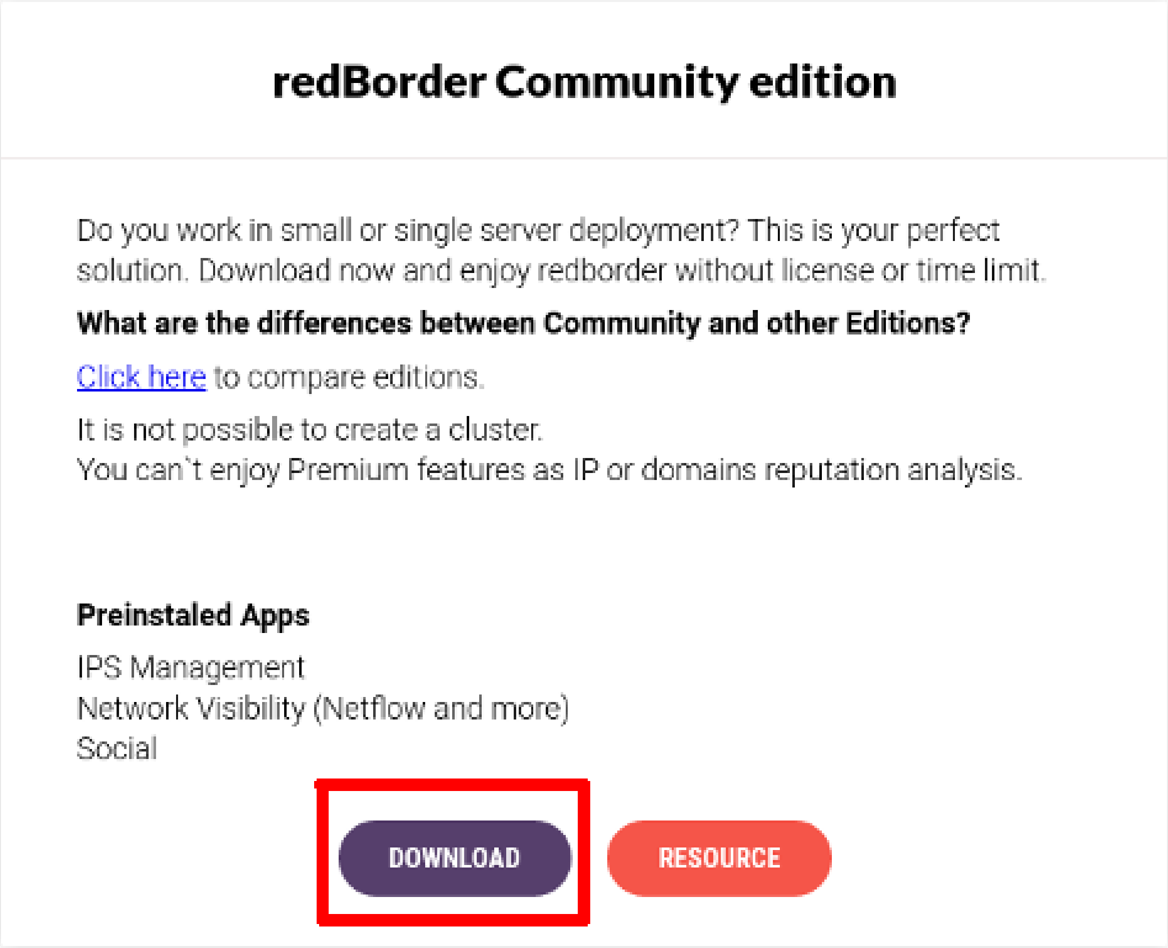
HD 100GB

## 1.2. Downloading the ISO

In order to download the ISO image, we **must be registered.** Once we are logged in to the redborder web, we must go to *Community -> Downloads.*

On this page we will find all of the redborder editions along with their corresponding specifications and characteristics.

To download the Community edition, click on DOWNLOAD in the Community section.



redBorder Community edition

Do you work in small or single server deployment? This is your perfect solution. Download now and enjoy redborder without license or time limit.

**What are the differences between Community and other Editions?**

Click here to compare editions.

It is not possible to create a cluster.
You can`t enjoy Premium features as IP or domains reputation analysis.

**Preinstaled Apps**

IPS Management
Network Visibility (Netflow and more)
Social

Downloading the ISO

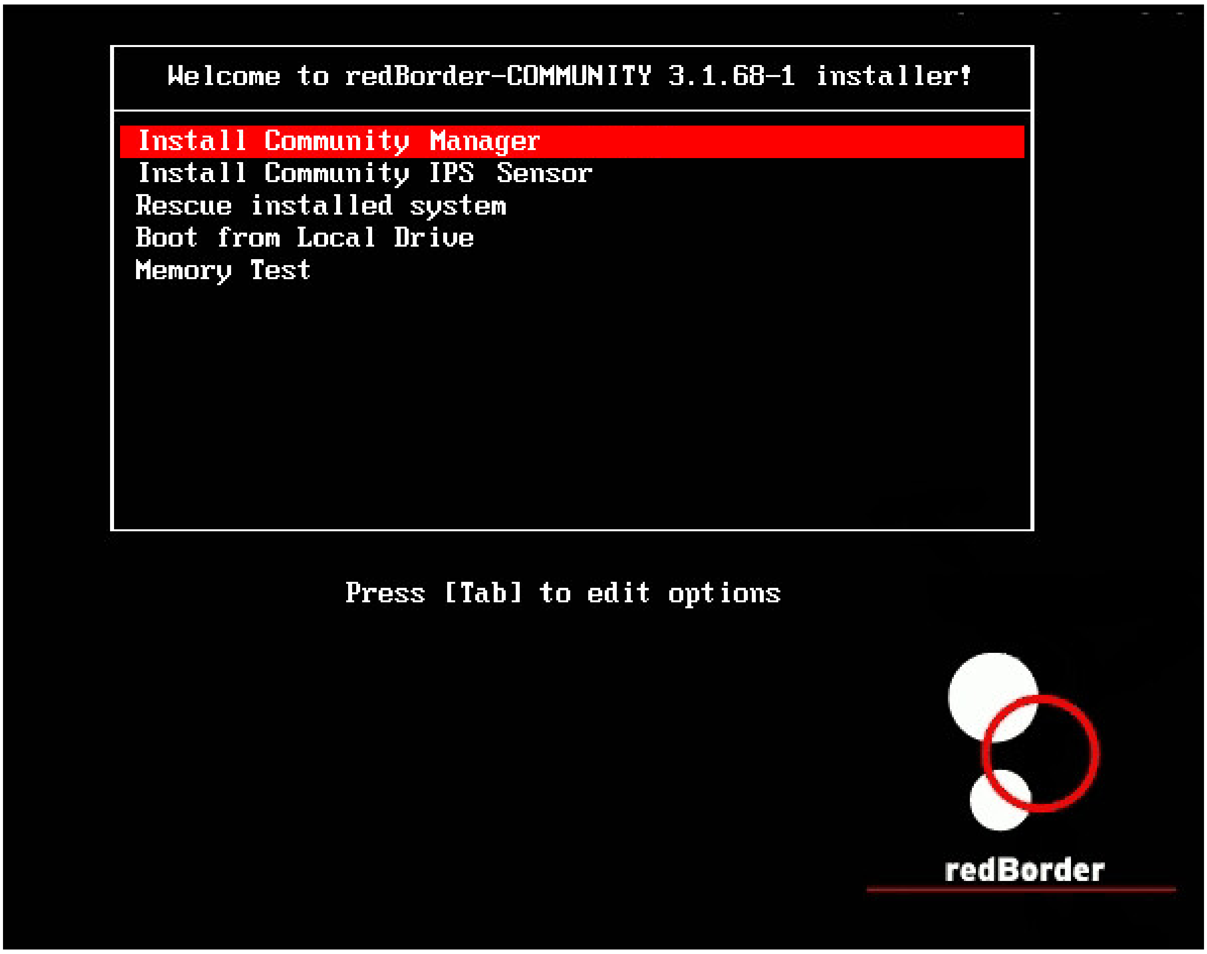
## 1.3. Burning the ISO Image

The ISO image is prepared to perform the boot from a DVD reader, USB device or as an ISO file for a virtual machine. In order to burn the ISO image from a Linux system to a USB device, the following command needs to be used if the USB device is mapped in **`/dev/sdd`**:

```
[root@machine ~]# dd if=redBorder-3.1.68-1-x86_64-6.5-community.iso of=/dev/sdd bs=10M
```

## 1.4. Installing the ISO

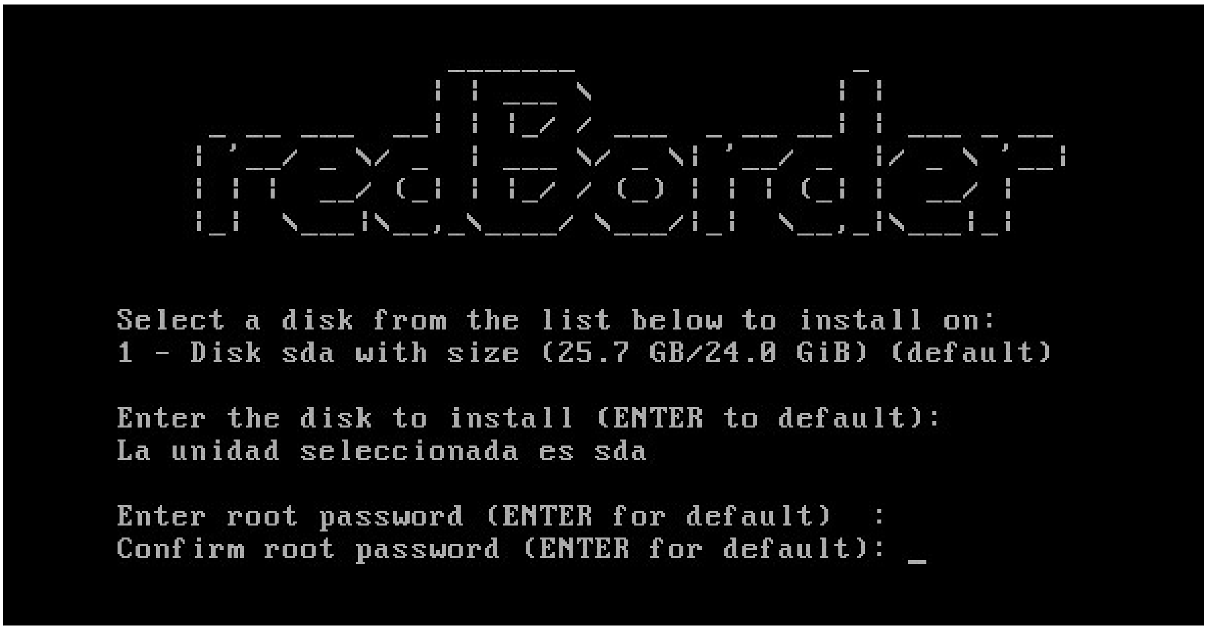
Once we have booted the redborder ISO, we will see the installation menu. To perform the installation, select the option *Install Community Manager:*



```
Welcome to redBorder-COMMUNITY 3.1.68-1 installer!

Install Community Manager
Install Community IPS Sensor
Rescue installed system
Boot from Local Drive
Memory Test

            Press [Tab] to edit options
```

Installing the ISO

Once in the installation process, the user only needs to confirm the installation destination and root password. redborder is prepared for unattended installations and so we should be especially careful with the time we have to respond to these three questions if we wish to modify the default options:



```
              _______               _
             | | ___ \             | |
 _ __ ___  __| | |_/ / ___  _ __ __| | ___ _ __
| '__/ _ \/ _` | ___ \/ _ \| '__/ _` |/ _ \ '__|
| | |  __/ (_| | |_/ / (_) | | | (_| |  __/ |
|_|  \___|\__,_\____/ \___/|_|  \__,_|\___|_|


Select a disk from the list below to install on:
1 - Disk sda with size (25.7 GB/24.0 GiB) (default)

Enter the disk to install (ENTER to default):
La unidad seleccionada es sda

Enter root password (ENTER for default)  :
Confirm root password (ENTER for default): _
```

Selecting the disk to install on

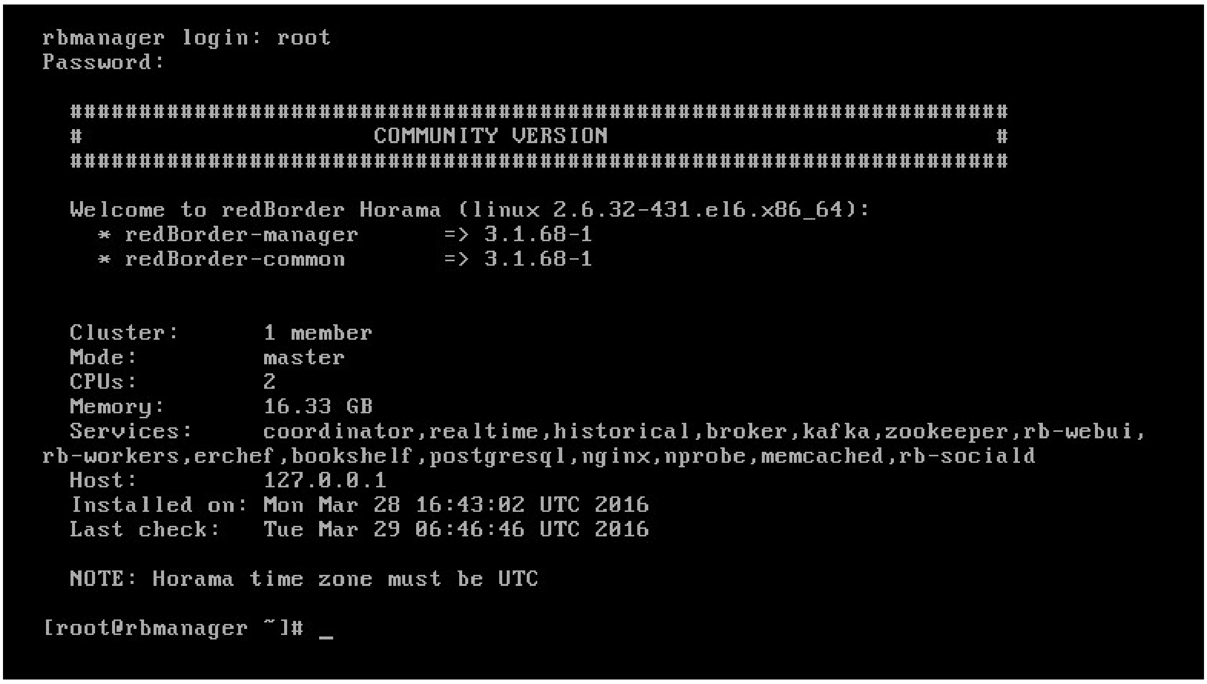
Once this page has been confirmed, the installation will carry out all of the necessary processes to prepare the system for configuration. By default, **the root password will be redborder.**

## 1.5. Basic Configuration

Upon completing the installation process, we have two configuration options depending on whether or not there is a DHCP server.

1. **Dynamic IP (DHCP):** in this case, redborder will have acquired an IP in its network interface and will have auto-configured in order to operate in said address.

2. **Static IP:** in this case redborder will not have configured and we will have to access the system in order to perform the configuration. To gain access we will use the *root user* and the password we selected during the installation.



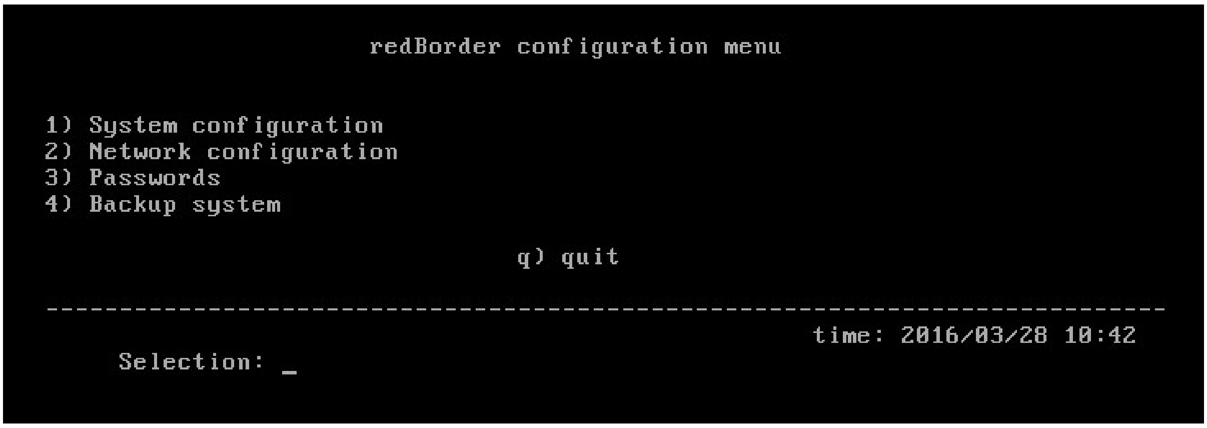
```
rbmanager login: root
Password:

  ######################################################################
  #                      COMMUNITY VERSION                             #
  ######################################################################

  Welcome to redBorder Horama (linux 2.6.32-431.el6.x86_64):
    * redBorder-manager       => 3.1.68-1
    * redBorder-common        => 3.1.68-1


  Cluster:        1 member
  Mode:           master
  CPUs:           2
  Memory:         16.33 GB
  Services:       coordinator,realtime,historical,broker,kafka,zookeeper,rb-webui,
rb-workers,erchef,bookshelf,postgresql,nginx,nprobe,memcached,rb-sociald
  Host:           127.0.0.1
  Installed on:   Mon Mar 28 16:43:02 UTC 2016
  Last check:     Tue Mar 29 06:46:46 UTC 2016

  NOTE: Horama time zone must be UTC

[root@rbmanager ~]# _
```

Choosing the IP for the Manager installation

Once inside the system, we will start the configuration manager. To do this we will execute:

```
[root@rbmanager ~]# rb_sysconf
```

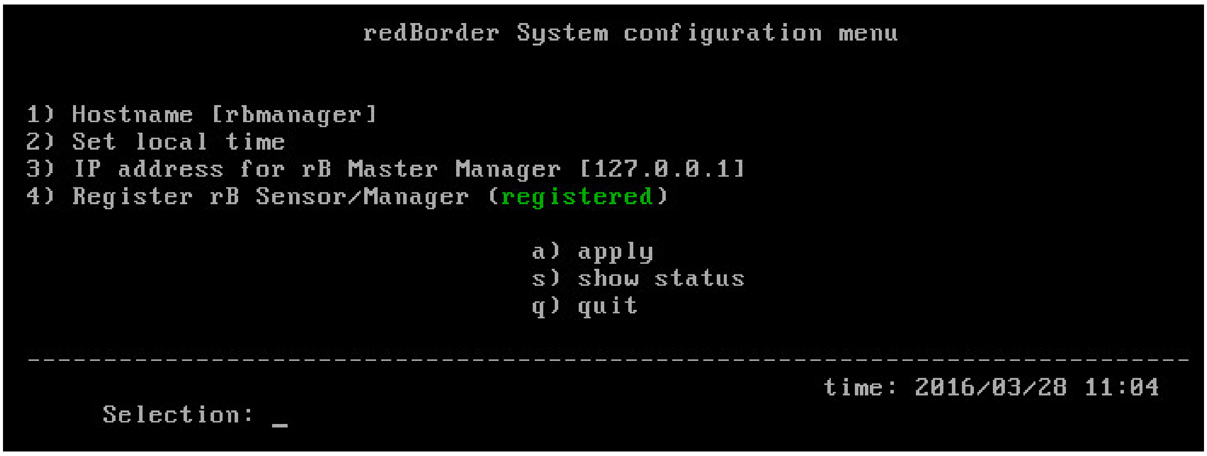
In the configuration we have several options:



```
                         redBorder configuration menu


 1) System configuration
 2) Network configuration
 3) Passwords
 4) Backup system

                                  q) quit

 ---------------------------------------------------------------------------
                                                        time: 2016/03/28 10:42
      Selection: _
```

redborder configuration menu

To start the configuration we begin with **`option 1 - System configuration:`**

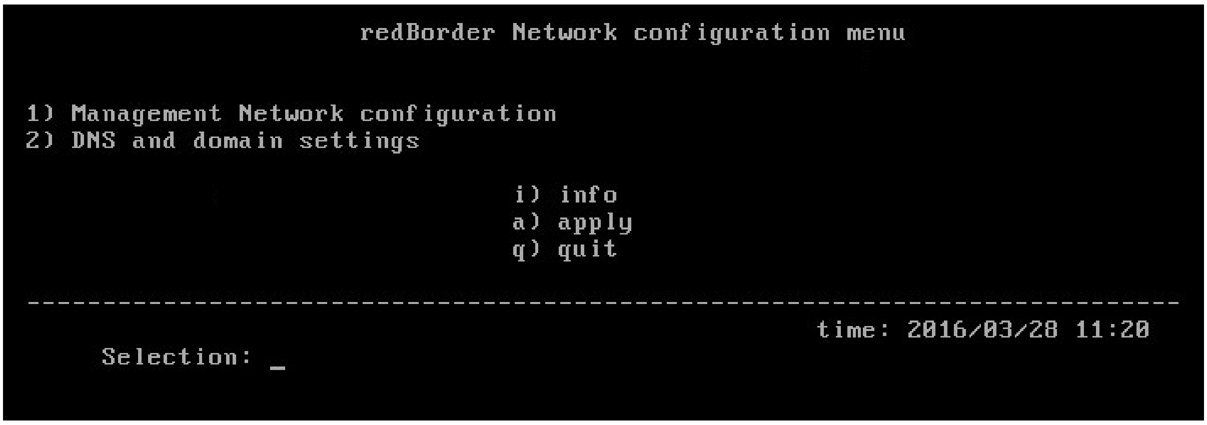


```
                  redBorder System configuration menu


 1) Hostname [rbmanager]
 2) Set local time
 3) IP address for rB Master Manager [127.0.0.1]
 4) Register rB Sensor/Manager (registered)

                            a) apply
                            s) show status
                            q) quit

 ---------------------------------------------------------------------
                                                time: 2016/03/28 11:04
     Selection: _
```

System Configuration

- *Option 1 - Hostname:* we must enter the host name of the machine where redborder has been installed.
- *Option 2 - Set local time:* allows us to indicate a local time for the system.
- *Options 3 y 4:* let us configure parameters not included in this Quick Installation Guide.

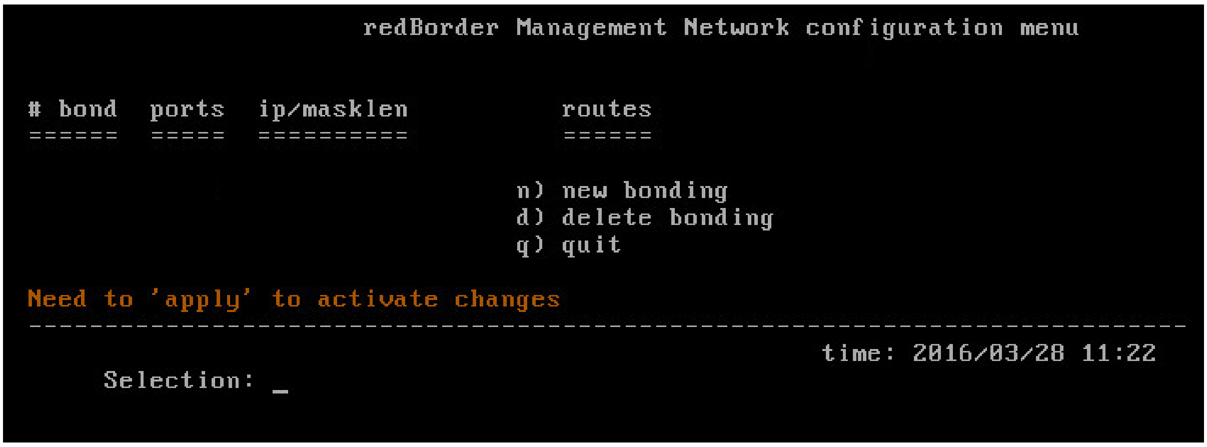
Returning to the main menu, in **`option 2 - Network configuration`** we will have to configure everything related to the network environment:



```
                  redBorder Network configuration menu


 1) Management Network configuration
 2) DNS and domain settings

                           i) info
                           a) apply
                           q) quit

 ---------------------------------------------------------------------
                                                time: 2016/03/28 11:20
     Selection: _
```

Network Configuration

In **`option 1 - Management Network configuration`**we will have the option of creating a link.



```
                  redBorder Management Network configuration menu


# bond   ports   ip/masklen          routes
======   =====   ==========          ======

                                  n) new bonding
                                  d) delete bonding
                                  q) quit

Need to 'apply' to activate changes
--------------------------------------------------------------
                                            time: 2016/03/28 11:22
     Selection: _
```

Management Network Configuration

When we select the option **n** we are asked for:

- *Insert bonding number [0]:* The default value is "0" and indicates the link index (at redBorder we use redundant links called bonding).

- *Insert bonding number [0]:* The default value is "0" and allows us to indicate the network port index to use in the management link.

- *Insert second port (y/N):* If only one port is needed for management, use the default value "N".

- *Insert management IP address:* We will enter the IP that we want to assign to redborder

- *Insert management Netmask:* We will enter the network mask that we want to assign to redborder.

- *Insert default gateway for this management interface (Y/n):* Indicates whether or not we want to assign a link port to redborder. Por defecto indicaremos Y.

- *Insert default gateway []:* We will enter the gateway IP address.

- *Insert a route for this bonding (y/N):* Indicates whether or not we want to indicate a route for the link created. By default we will indicate "N".

Once the link is created, we return to the **`Management Network configuration menu`** and select **`option 2 - DNS and domain settings`** in this option we will be asked to:

- *Insert Domain [redborder.cluster]:* we are asked to enter the domain which redborder will be integrating.

- *Insert DNS Primary:* we are asked for the DNS server to be used.

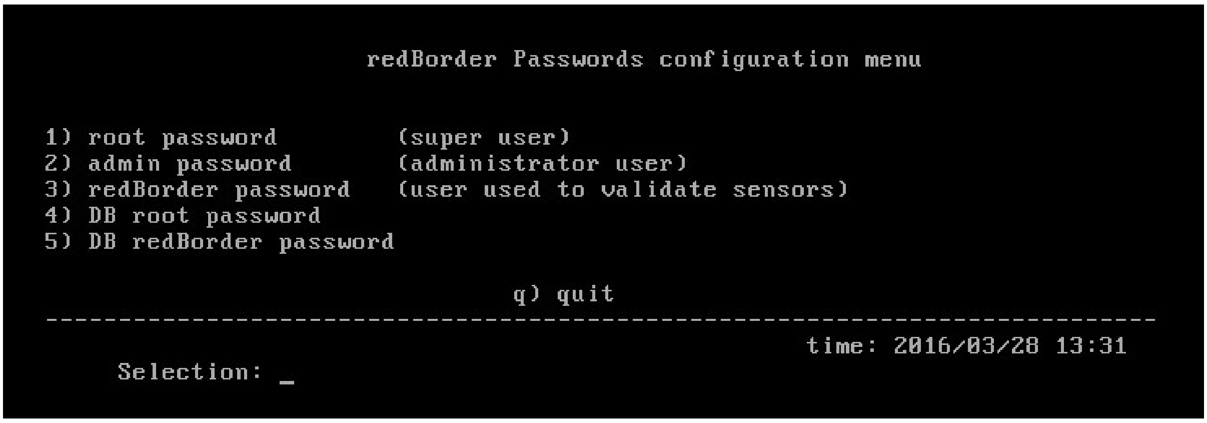
- *Insert DNS Secondary (optional):* we are asked for the secondary DNS server to be used. A secondary DNS server is not necessary by default.

Once the previous steps have been completed, we must apply the configuration with the option **`a - apply.`**

**Note**

At this time we will see that several operations are executed. Please be patient because this process may be lengthy depending on the machine's hardware.

Returning to the main menu, we have **`option 3 - Passwords.`** Within this option we can modify the different passwords used by default for the different users. Remember that the default password is redborder.



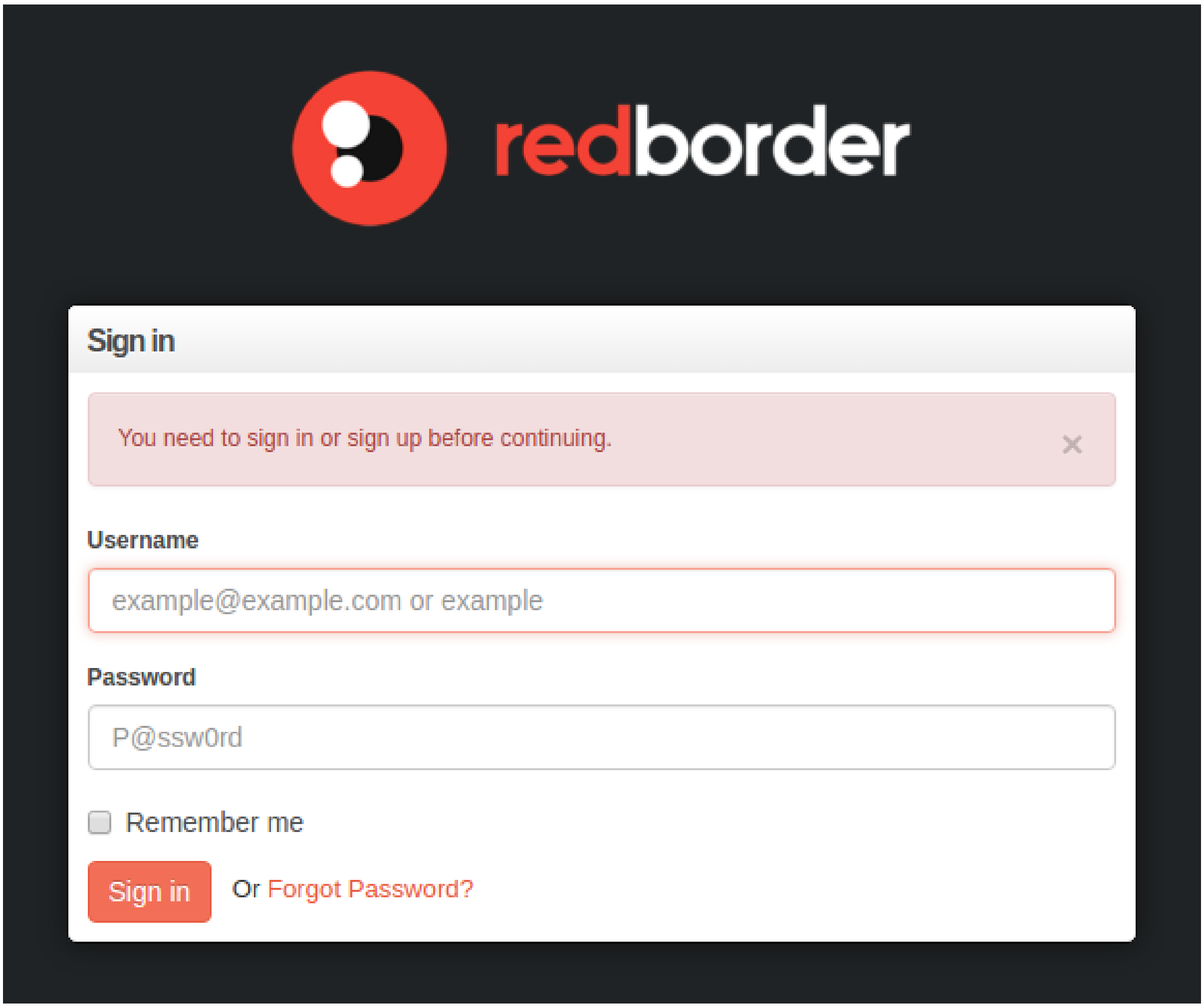
```
                    redBorder Passwords configuration menu


1) root password         (super user)
2) admin password        (administrator user)
3) redBorder password    (user used to validate sensors)
4) DB root password
5) DB redBorder password

                              q) quit
----------------------------------------------------------------------------
                                                    time: 2016/03/28 13:31
     Selection: _
```

Passwords

Lastly, we have **`option 4 - Backup system`** which is outside of the scope of this Quick Installation Guide.

## 1.6. Using redBorder

Once we have carried out all of the previously described configuration steps, we will be able to access the redborder web interface by entering the IP address of the machine where redborder has been installed in a web browser using the admin user and the administration password, which will either be the default password (redborder) or another entered previously in the configuration menu.



Sign in

You need to sign in or sign up before continuing.

Username

example@example.com or example

Password

P@ssw0rd

□ Remember me

redborder web platform

## 1.7. Basic Troubleshooting

To verify the correct functioning of redborder, we can access the system via ssh using root user and execute the command:

```
  [root@rbmanager ~]# rb_get_services.sh all
-----------------------------------------------
Service                  rbmanager
-----------------------------------------------
chef-client:             running
druid_coordinator:       running
druid_realtime:          running
druid_historical:        running
druid_broker:            running
kafka:                   running
zookeeper:               running
rb-monitor:              running
rb-webui:                running
rb-workers:              running
memcached:               running
erchef:                  running
chef-solr:               running
chef-expander:           running
chef-server-webui:       not running
bookshelf:               running
```

```
rabbitmq:               running
postgresql:             running
nginx:                  running
nprobe:                 running
rb-sociald:             running
aerospike:              not running
--------------------------------------------------
Total:                  20
--------------------------------------------------
Running: 20  /  Stopped: 2  /  Errors: 0  /  Unknown: 0
```

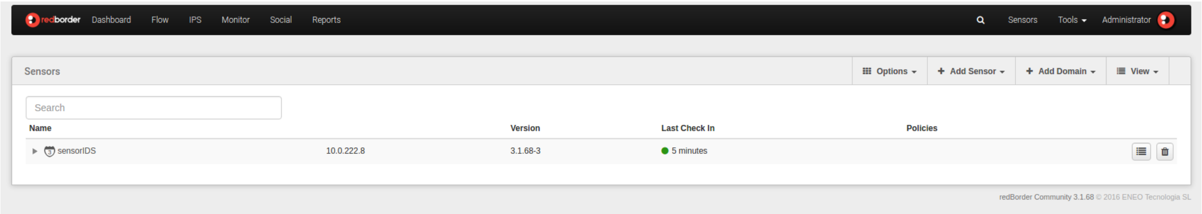
This command should show services in "running" status in green, and services in "not running" status in orange.

If at any time any of the two statuses are shown (running or not running) in red, it means that the service is in the opposite state of that shown. Example: if we see that a status appears as "running" in red, it indicates that the service is running but should be turned off. The same applies to the reverse case, if we see a "not running" status in red, it indicates that the service is not running but in fact should be.

# Registering the IPS/ IDS sensor in redborder Live

## 2.1. Registering the sensor in redborder LIve

Once you have registered the sensors in the Manager you can check it from the redborder platform. To verify this, you can access Sensors in the web interface to see if the last check in was satisfactory:

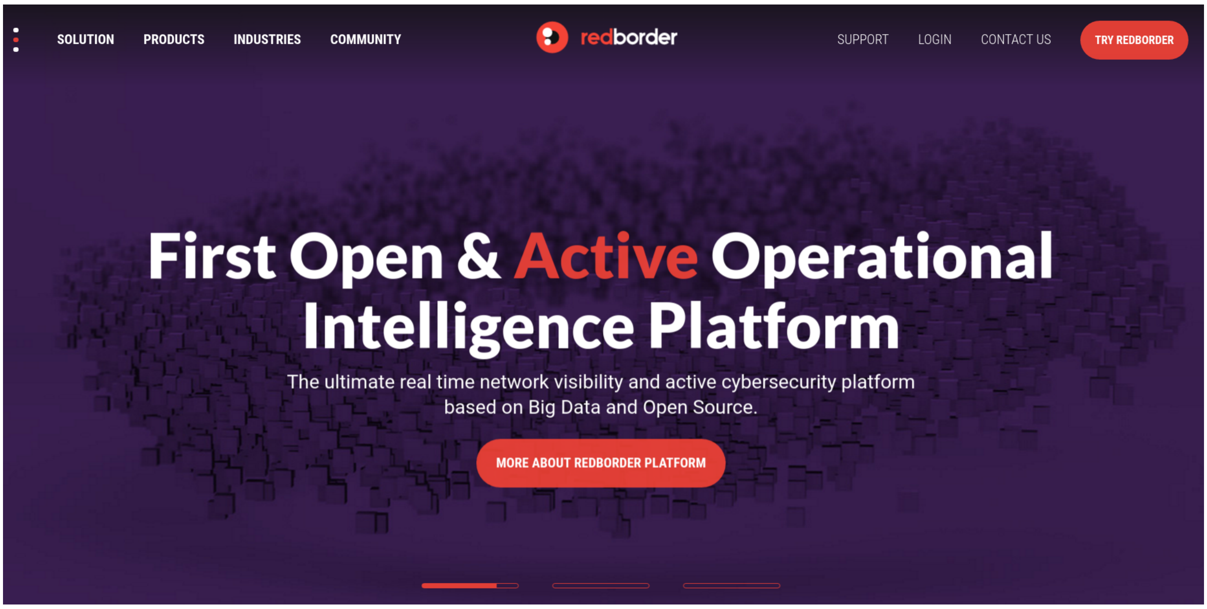


| Name | | Version | Last Check In | Policies |
|---|---|---|---|---|
| sensorIDS | 10.0.222.8 | 3.1.68-3 | ● 5 minutes | |

Sensors interface: checking sensors registration

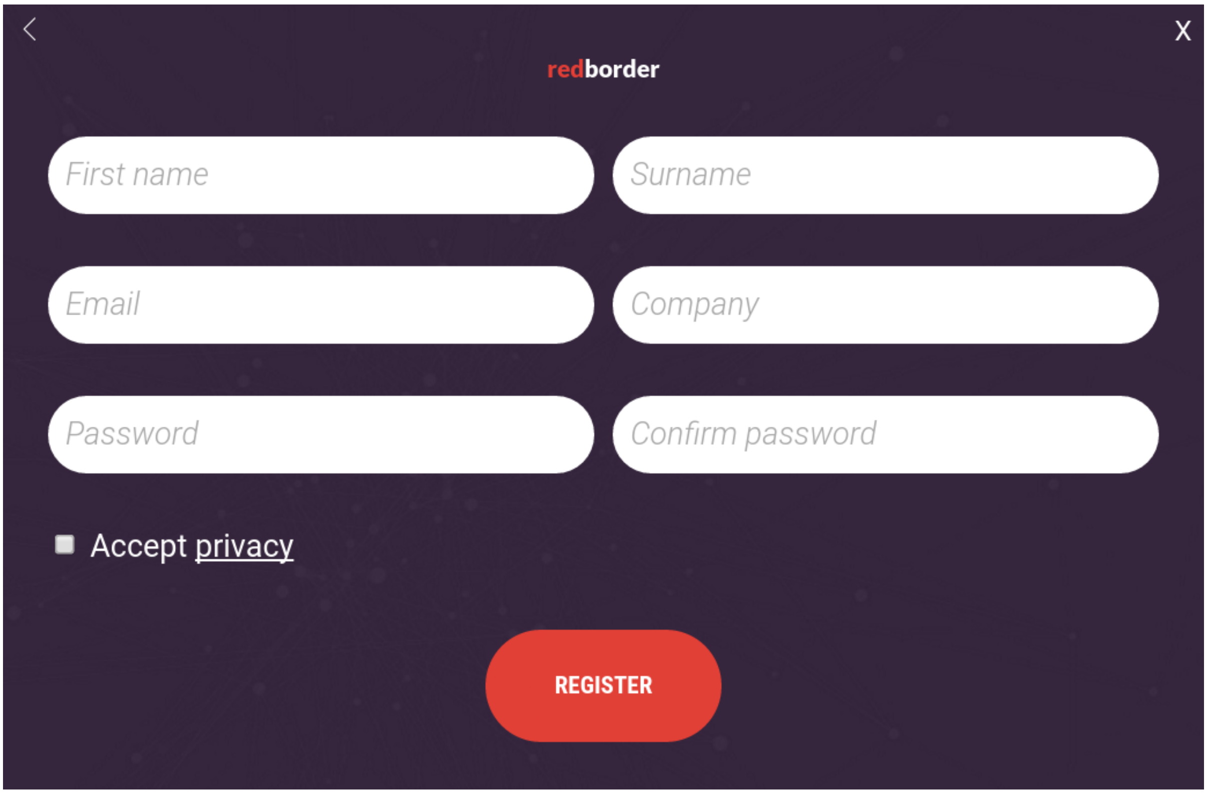
In order to register the sensor in redborder Live, we must have a **redborder account.**

First, sign up in redborder Live, we must access: *https://www.redborder.com/* Click on **`Try redborder`**, in the upper right of the screen.


SOLUTION
PRODUCTS
INDUSTRIES
COMMUNITY
redborder
SUPPORT
LOGIN
CONTACT US
TRY REDBORDER
First Open & Active Operational Intelligence Platform
The ultimate real time network visibility and active cybersecurity platform based on Big Data and Open Source.
MORE ABOUT REDBORDER PLATFORM

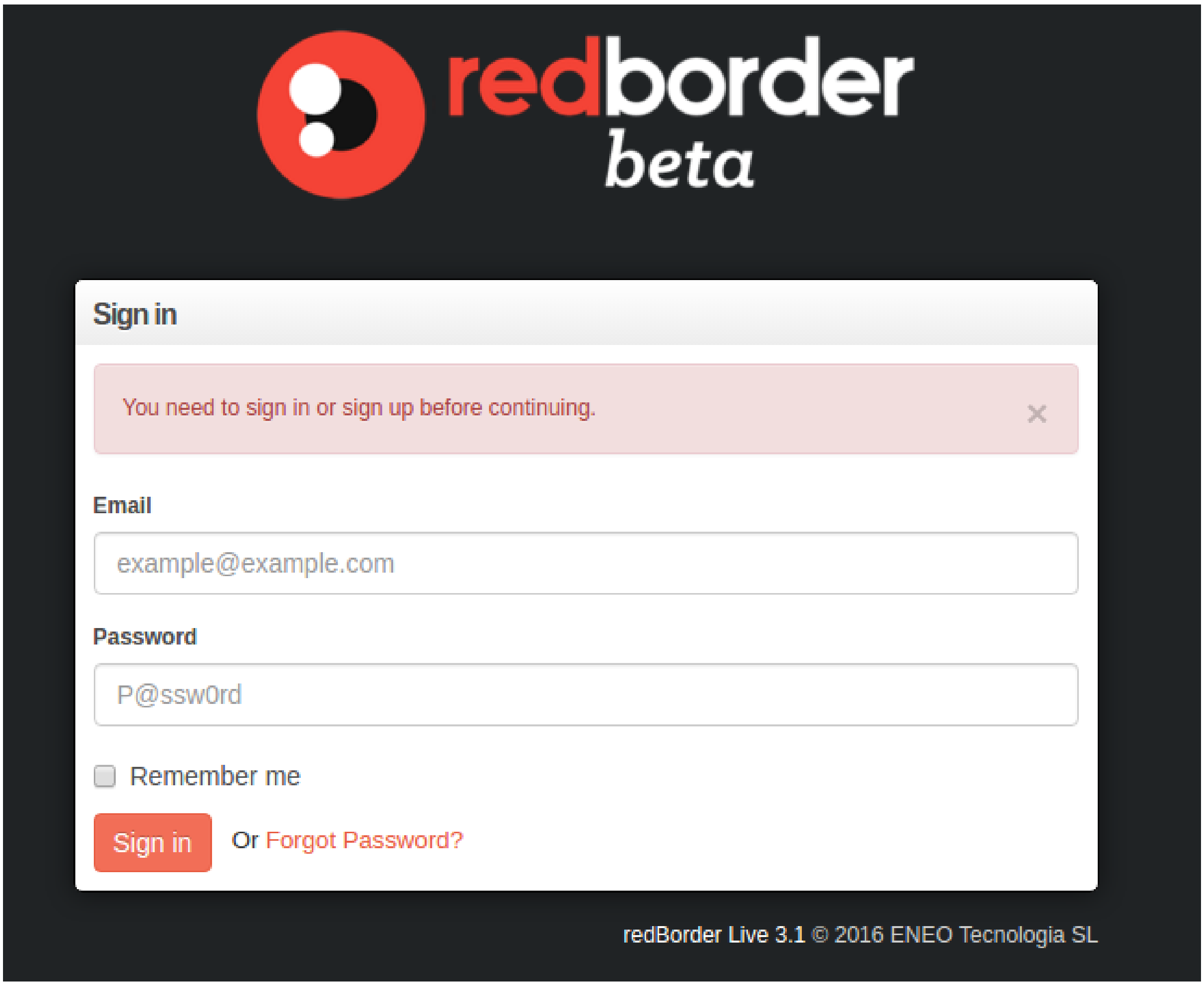
Sign up in redborder Live

Fill out the form and click on **`Register.`** We will need to confirm the email in order to finish the process.



Fill the form with your personal data

Now, we must go the redborder Live login page. The link for this page is: *https://live.redborder.com/*



Sign in

You need to sign in or sign up before continuing. ×

Email

example@example.com

Password

P@ssw0rd

□ Remember me

Sign in  Or Forgot Password?

redBorder Live 3.1 © 2016 ENEO Tecnologia SL

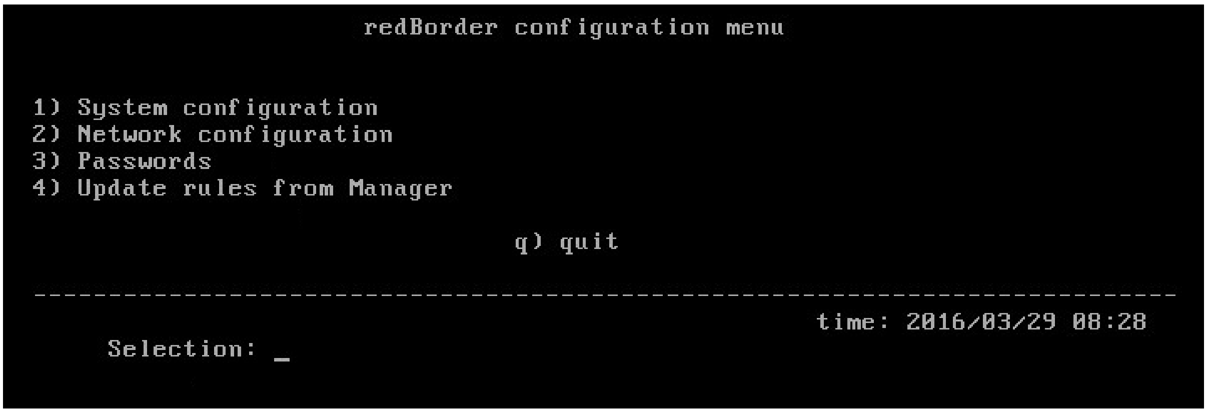
redborder Live login page

We will log in with the same email address and password that we used in the registration.

Now, we will access the sensor as the root user. Once inside the system we will start the configuration manager. To do this, we will execute:

```
[root@rbmanager ~]# rb_sysconf
```

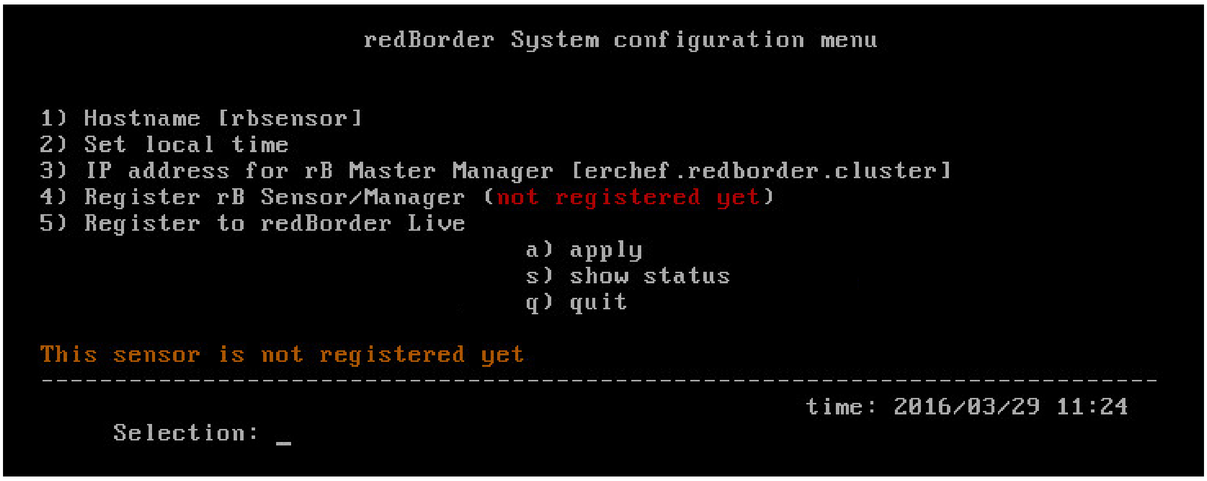
A menu with different options will appear:



```
                    redBorder configuration menu


 1) System configuration
 2) Network configuration
 3) Passwords
 4) Update rules from Manager

                              q) quit

 ----------------------------------------------------------------------------
                                                  time: 2016/03/29 08:28
      Selection: _
```

redborder configuration menu

We must select **`option 1 - System configuration`**:



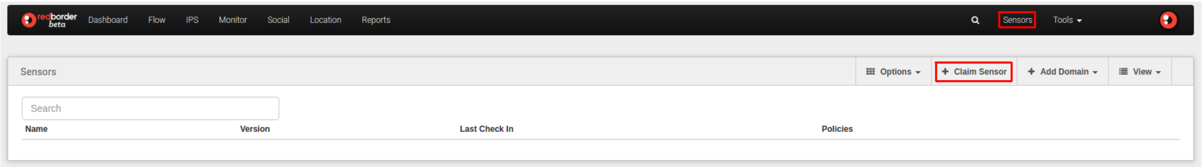
```
                        redBorder System configuration menu


 1) Hostname [rbsensor]
 2) Set local time
 3) IP address for rB Master Manager [erchef.redborder.cluster]
 4) Register rB Sensor/Manager (not registered yet)
 5) Register to redBorder Live
                                a) apply
                                s) show status
                                q) quit

 This sensor is not registered yet
 ----------------------------------------------------------------------------
                                                   time: 2016/03/29 11:24
      Selection: _
```

Select option 1: System configuration

First of all, Option 1 must be selected to create a host name for the IDS/IPS sensor because default hostname rbsensor is not allowed. Then, select Option 5 to start the registration process to redBorder Live. A Sensor UUID will be showed.

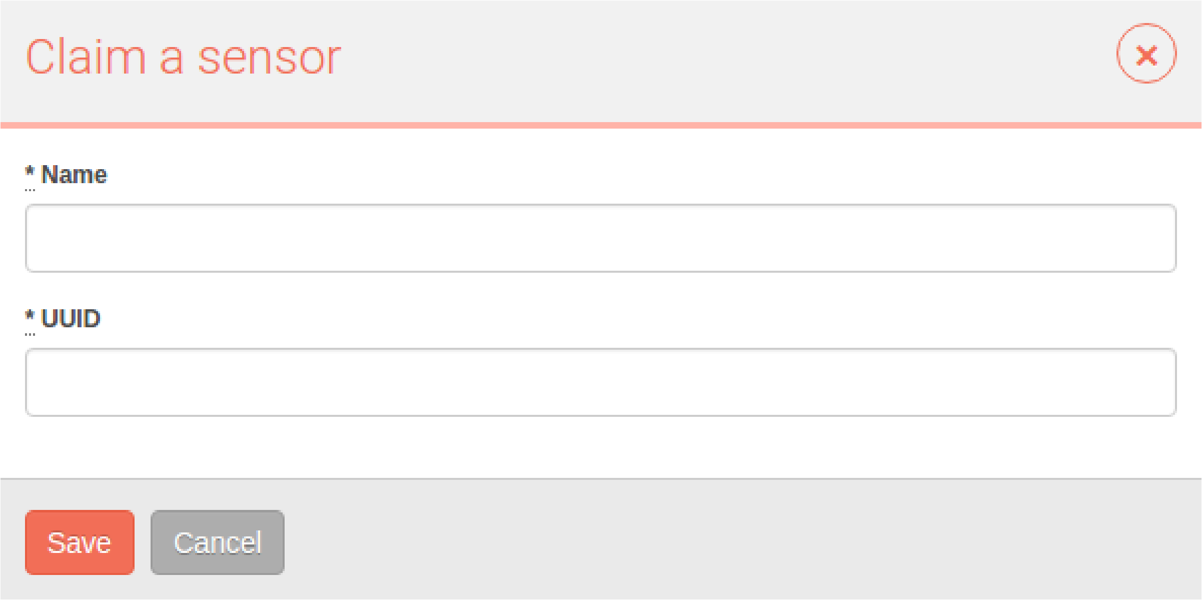
Sensor UUID

Copy the UUID and go to the redborder Live web page. If we are logged in, go to Sensors and press **+ `Claim Sensor`**:



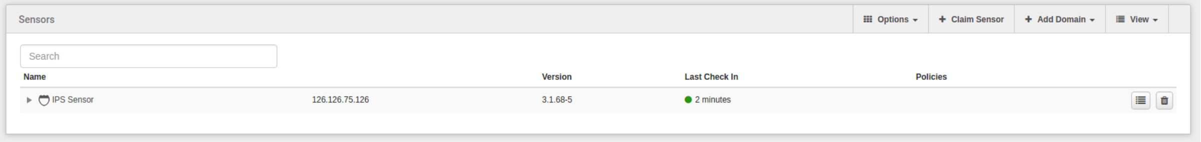
Claim sensor

A pop-up window will appear where we must enter a name for the sensor and paste the UUID that we copied before in the field below.



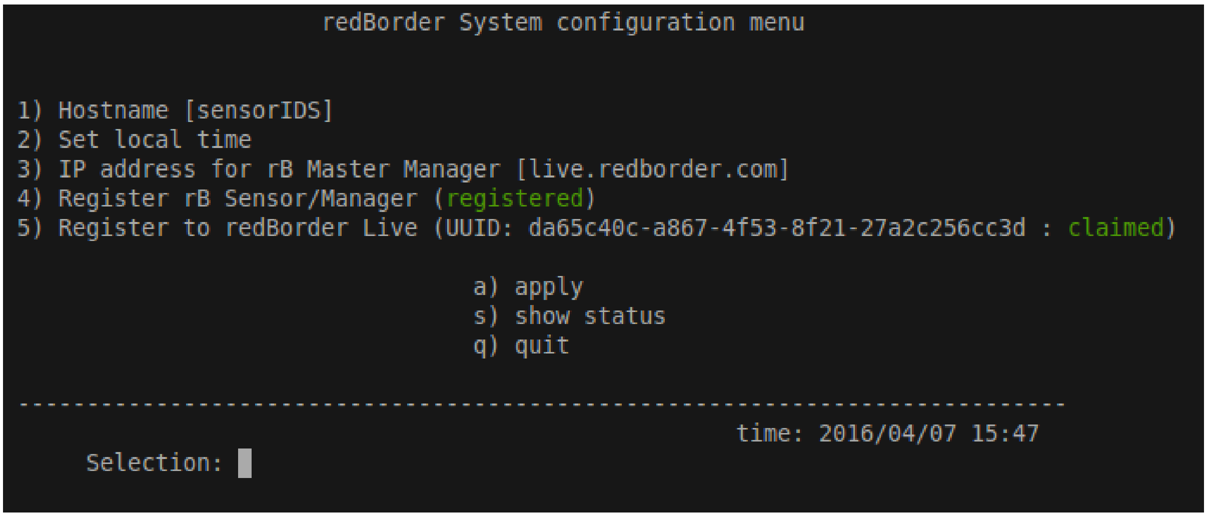
Enter the name and UUID of your sensor

Click on **save** and wait until the sensor is configured correctly. We can then verify that the sensor is working both in redborder Live and by executing the **rb_sysconf** command and selecting option 1 in the menu:



| Name | | Version | Last Check In | Policies |
|---|---|---|---|---|
| IPS Sensor | 126.126.75.126 | 3.1.68-5 | ● 2 minutes | |

Sensors interface: claimed sensor

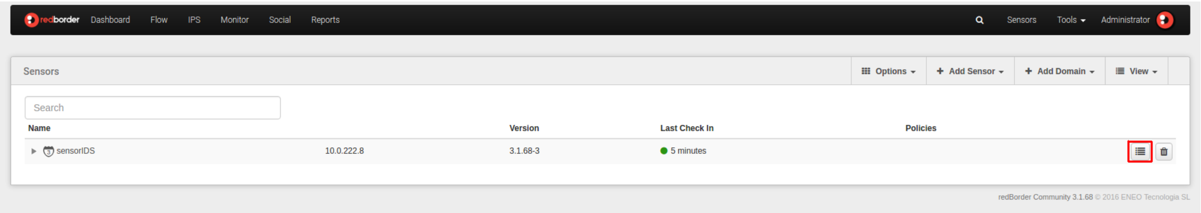


```
                     redBorder System configuration menu


1) Hostname [sensorIDS]
2) Set local time
3) IP address for rB Master Manager [live.redborder.com]
4) Register rB Sensor/Manager (registered)
5) Register to redBorder Live (UUID: da65c40c-a867-4f53-8f21-27a2c256cc3d : claimed)

                                  a) apply
                                  s) show status
                                  q) quit

-----------------------------------------------------------------------------
                                                     time: 2016/04/07 15:47
     Selection: 
```

Sensor registerd and claimed

## 2.2. Assigning Resources to Segments

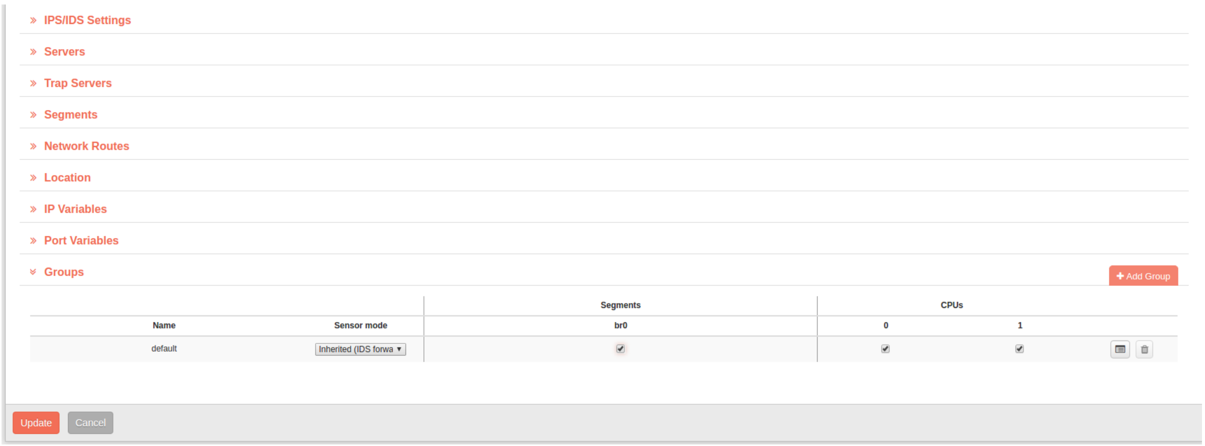
We need to go to Sensor Tab and select **Edit** Option:



| Name | | Version | Last Check In | Policies |
|---|---|---|---|---|
| sensorIDS | 10.0.222.8 | 3.1.68-3 | ● 5 minutes | |

Edit sensor

Go to *Groups* and in this view you can see the number of segments and cores you have. We only need to check the segment and assign the number of cores we want. Then press **Update**.



» IPS/IDS Settings

» Servers

» Trap Servers

» Segments

» Network Routes

» Location

» IP Variables

» Port Variables

» Groups

|  |  | Segments | CPUs |  |  |
|---|---|---|---|---|---|
| Name | Sensor mode | br0 | 0 | 1 |  |
| default | Inherited (IDS forwa ▾ | ☑ | ☑ | ☑ |  |

Edit IPS/ IDS settings

# Appendix A. Histórico de Revisiones

**Revision 0.1-1 Enero 2016** **Eneo Tecnología** *`info@redborder.com`*

Ampliación documentación e inserción de nuevas funcionalidades.