IPS redborder Live 3

Quick installation guide

redborder

IPS redborder Live 3 Quick installation guide

Author *info@redborder.com*

ISBN: No available

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

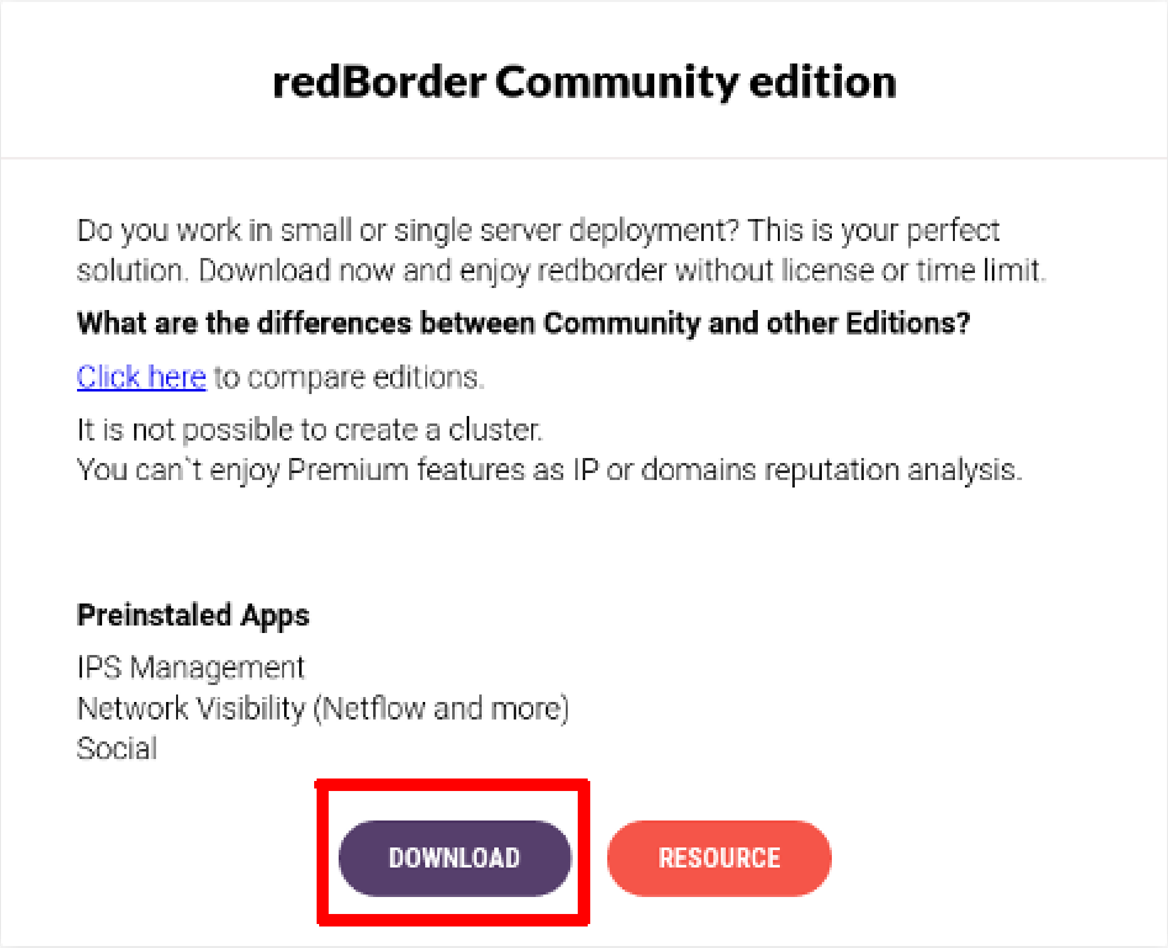
- RAM 32GB
- Processor: 4 cores
- HD 100GB

1.2. Downloading the ISO

In order to download the ISO image, we must be registered on the web. Once we are logged in to the redborder web, we must go to *Community -> Downloads* following this link *https://redborder.com/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

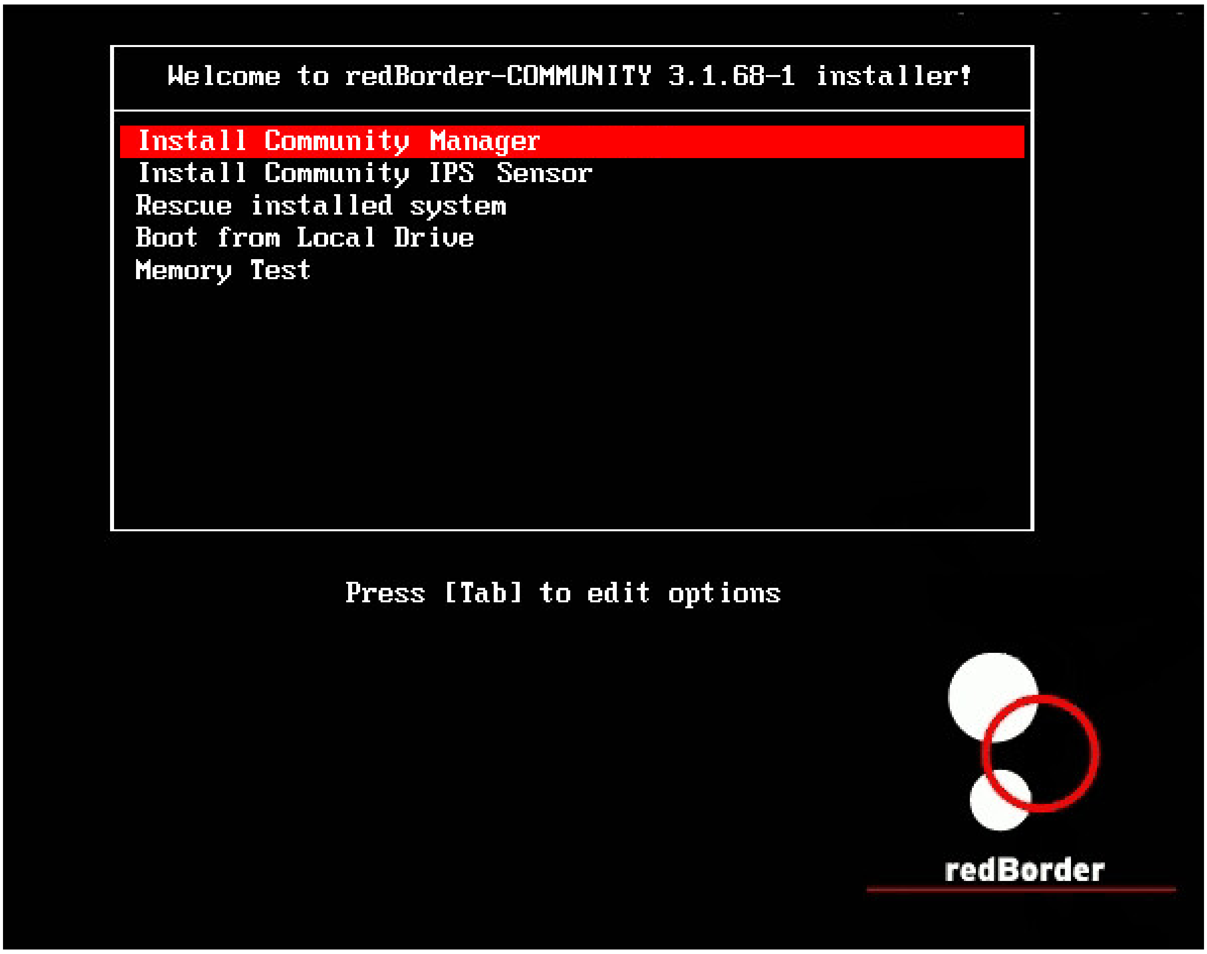
1.3. Burning the ISO Image

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

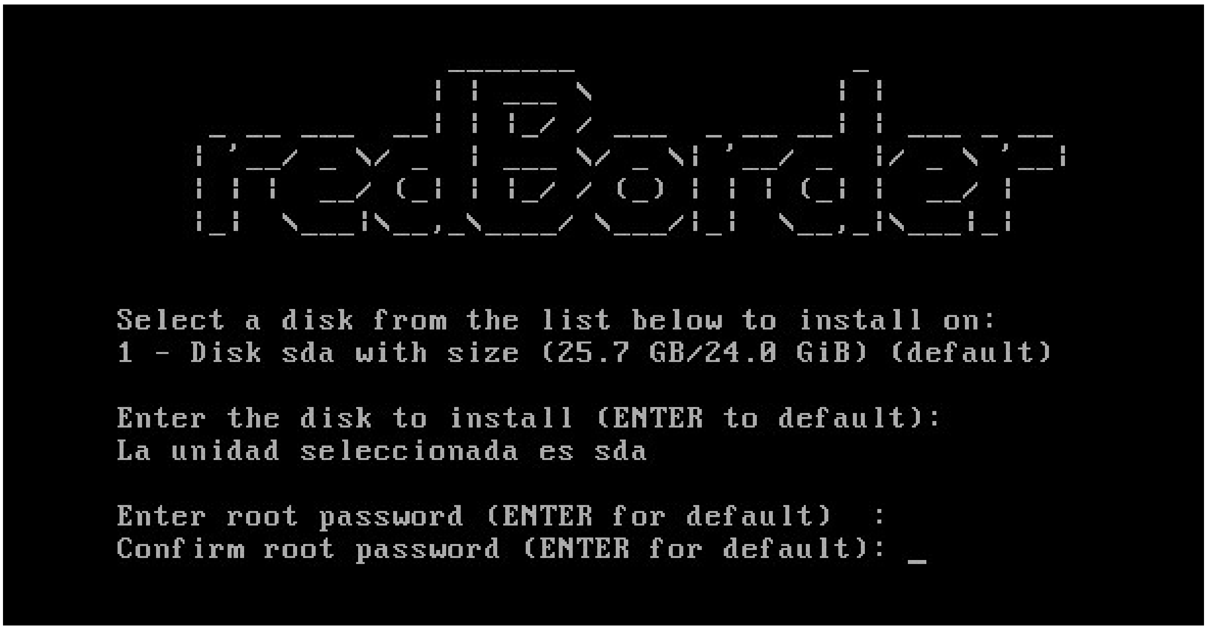
Once we have booted the redborder ISO, we will see the installation menu. To perform the installation, select the option *Install Community Manager:*



```
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

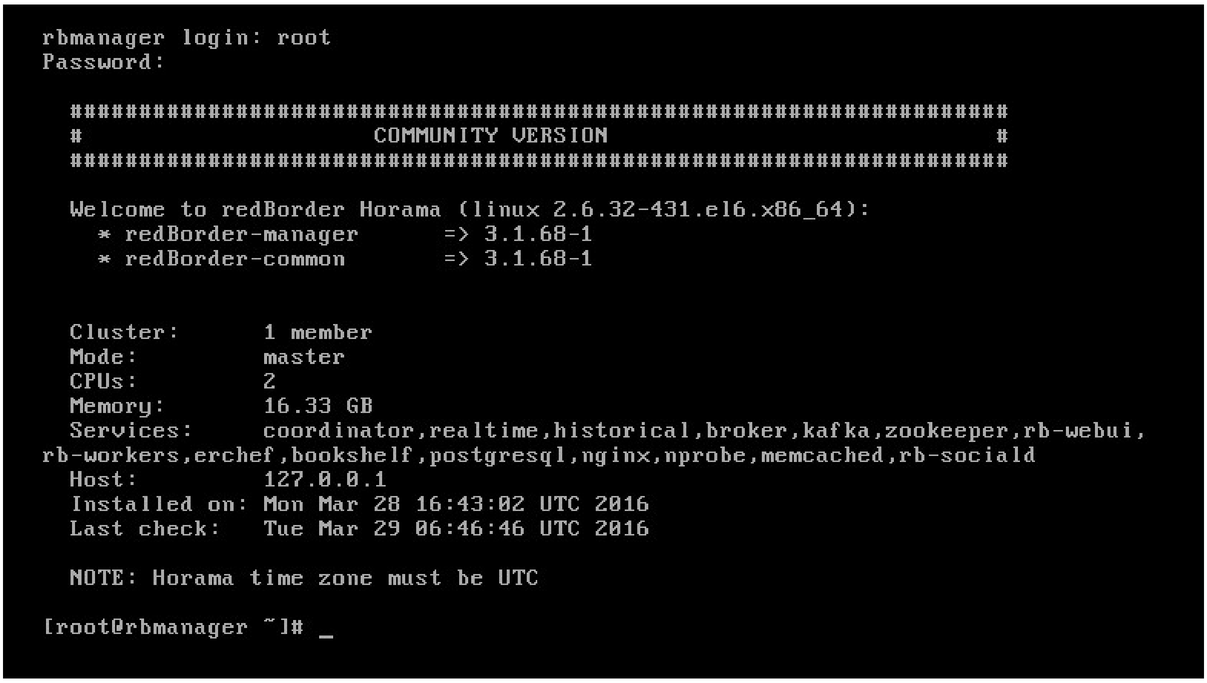
Once this page has been confirmed, the installation will carry out all of the necessary processes to prepare the system for configuration. By default, **the root password will be redborder.**

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.



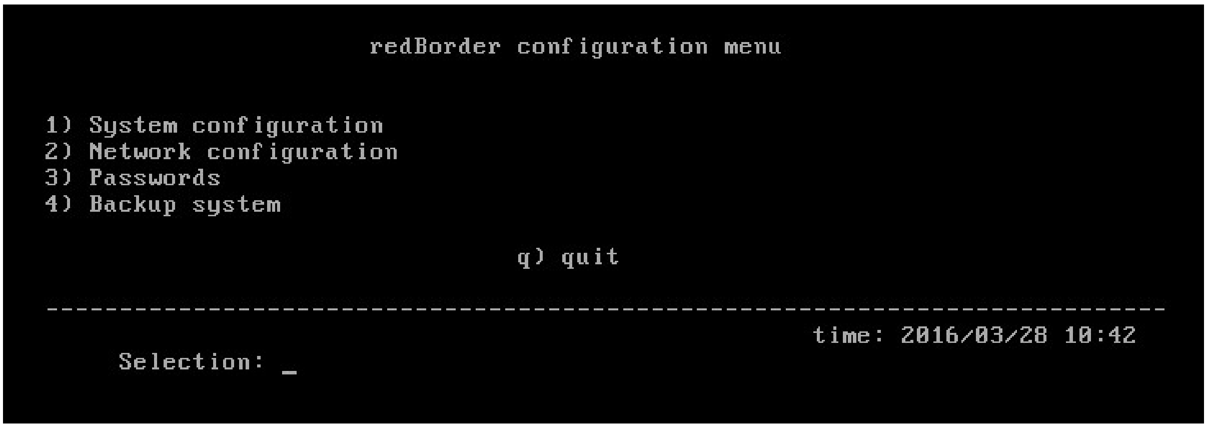
```
rbmanager login: root
Password:

  ####################################################################
  #                      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
```

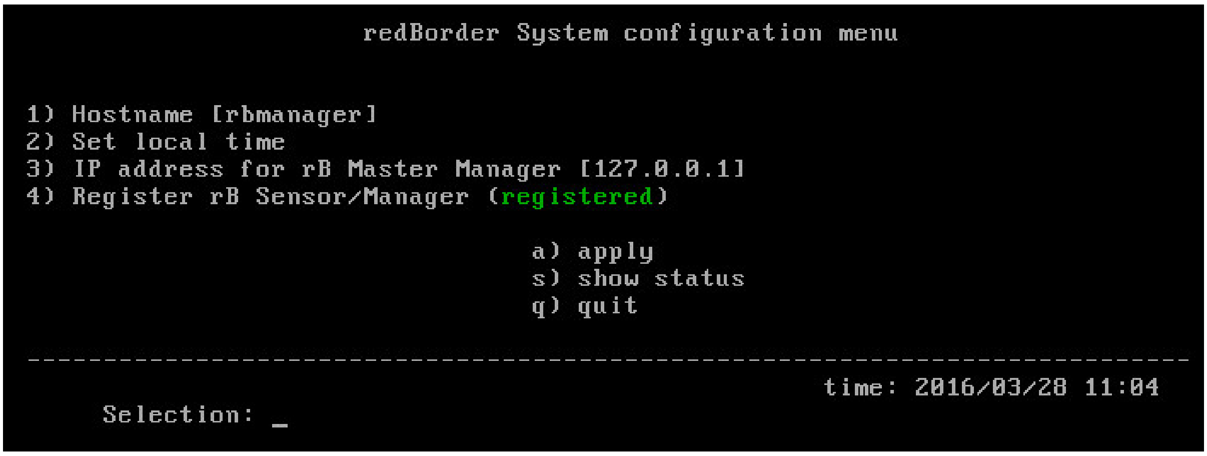
In the configuration we have several options:



```
                        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:`**

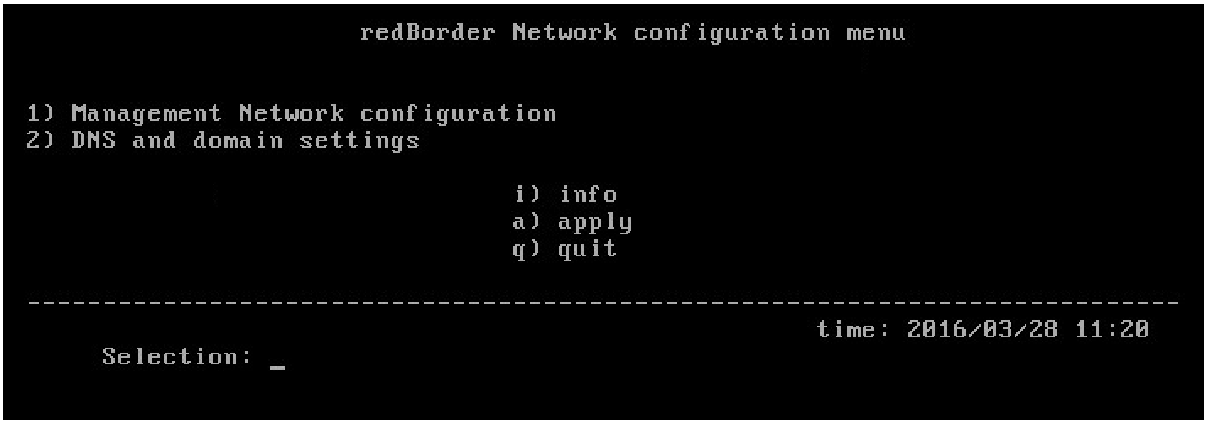


```
                        redBorder System configuration menu


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.

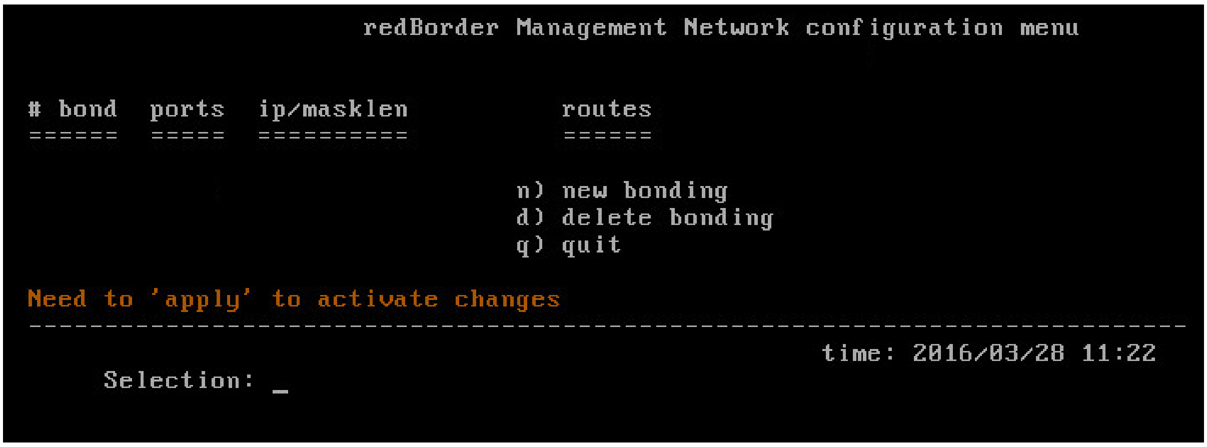
Returning to the main menu, in option **`2 - Network configuration`** we will have to configure everything related to the network environment:



```
                        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:

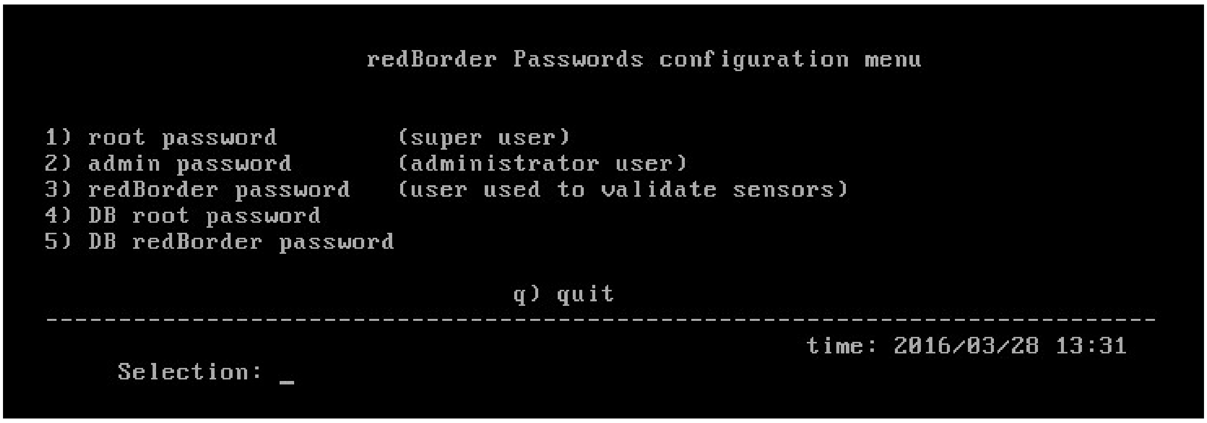
- *Insert Domain [redborder.cluster]:* we are asked to enter the domain which redborder will be integrating.
- *Insert DNS Primary:* we are asked for the DNS server to be used.
- *Insert DNS Secondary (optional):* we are asked for the secondary DNS server to be used. A secondary DNS server is not necessary 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.



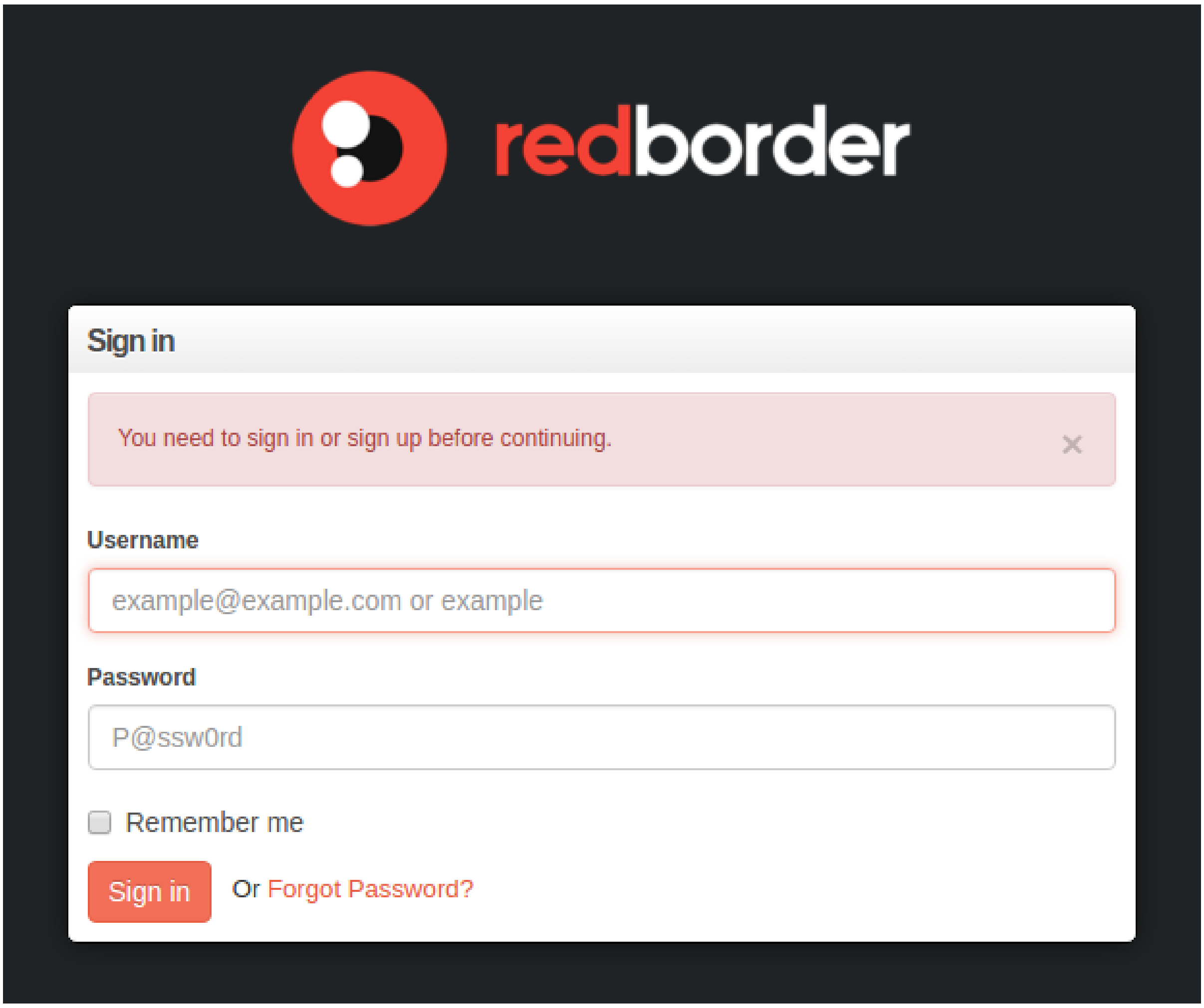
```
                         redBorder Passwords configuration menu


 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.



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

2.1. 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 referenced at every SNORT instance being executed. They are shown in the following chart:

Installation requirements

Minimum per instance

- RAM 2GB
- Processor: 1 core

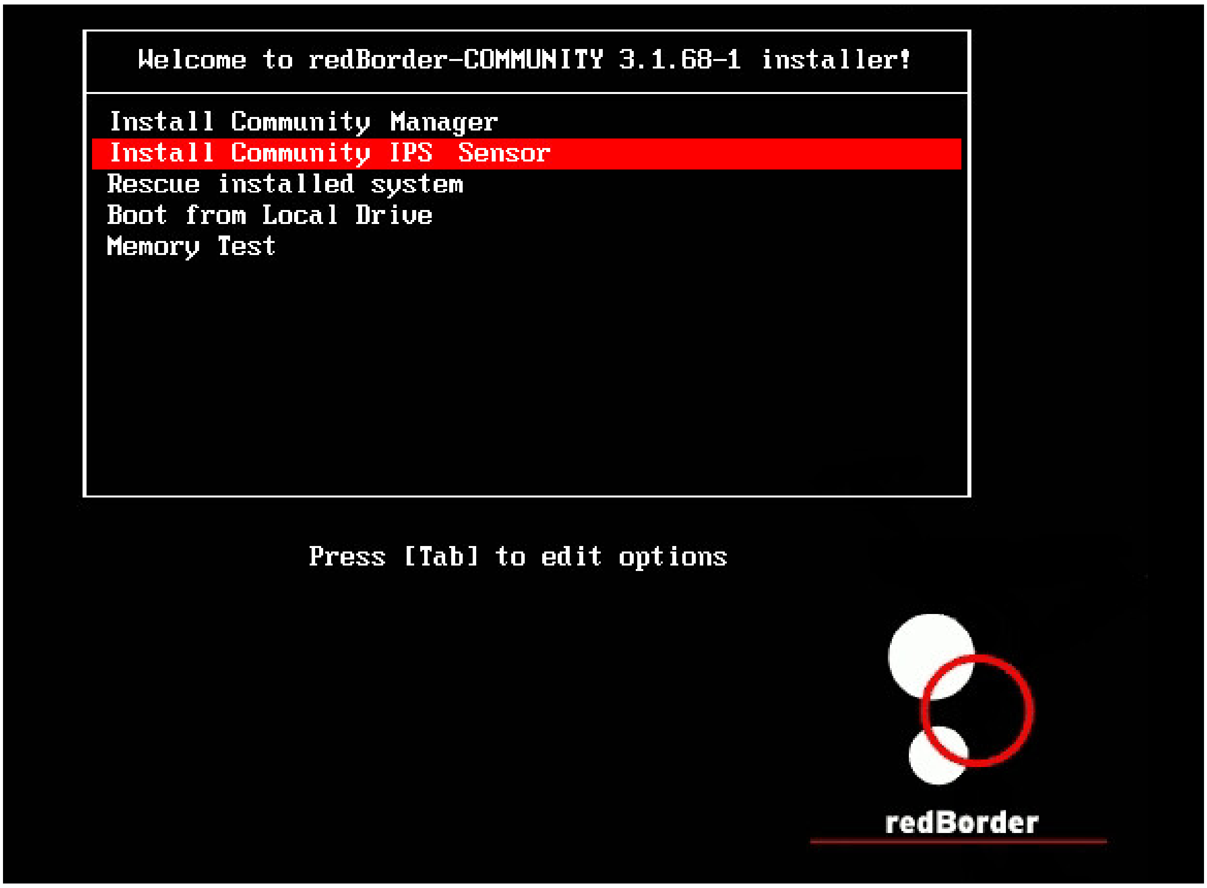
Recommended per instance [1]

- RAM 4GB
- Processor: 1 core

2.2. Installing the sensor in the Manager

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

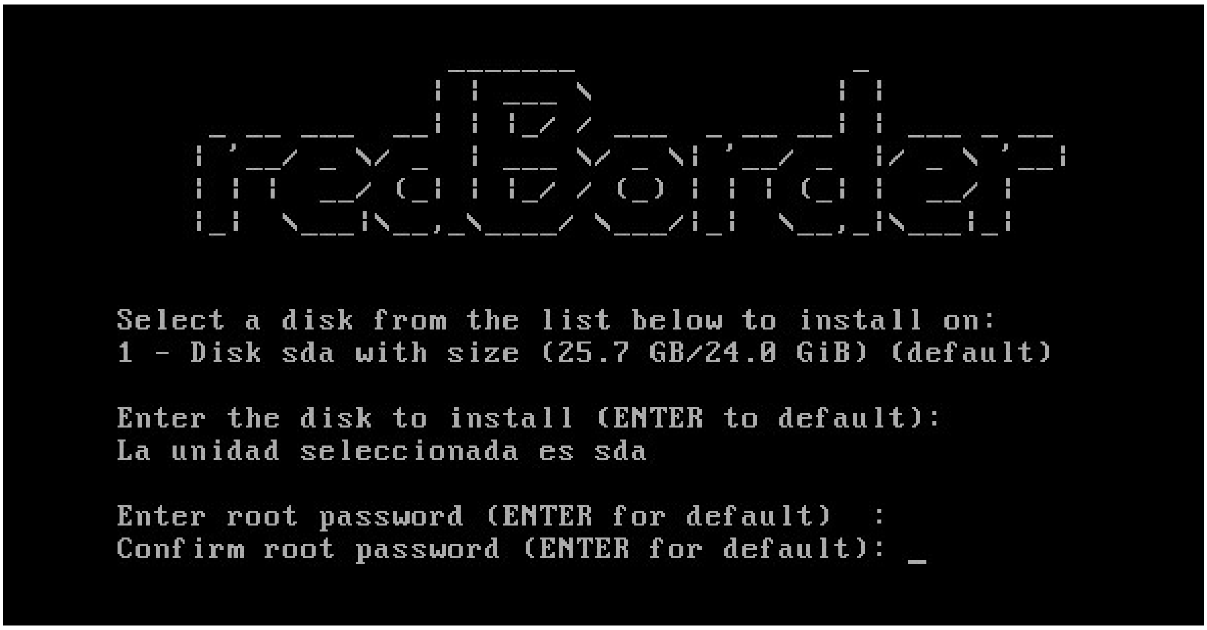
[1] For example, if we want four SNORT instances in the recommended configuration, we need a machine with 16 GB and four cores.



```
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
```

ISO Installation menu: Install Community IPS Sensor

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): _
```

Select the disk in which you want to install the sensor

Once this page has been confirmed, the installation will carry out all of the necessary processes to prepare the system for configuration.

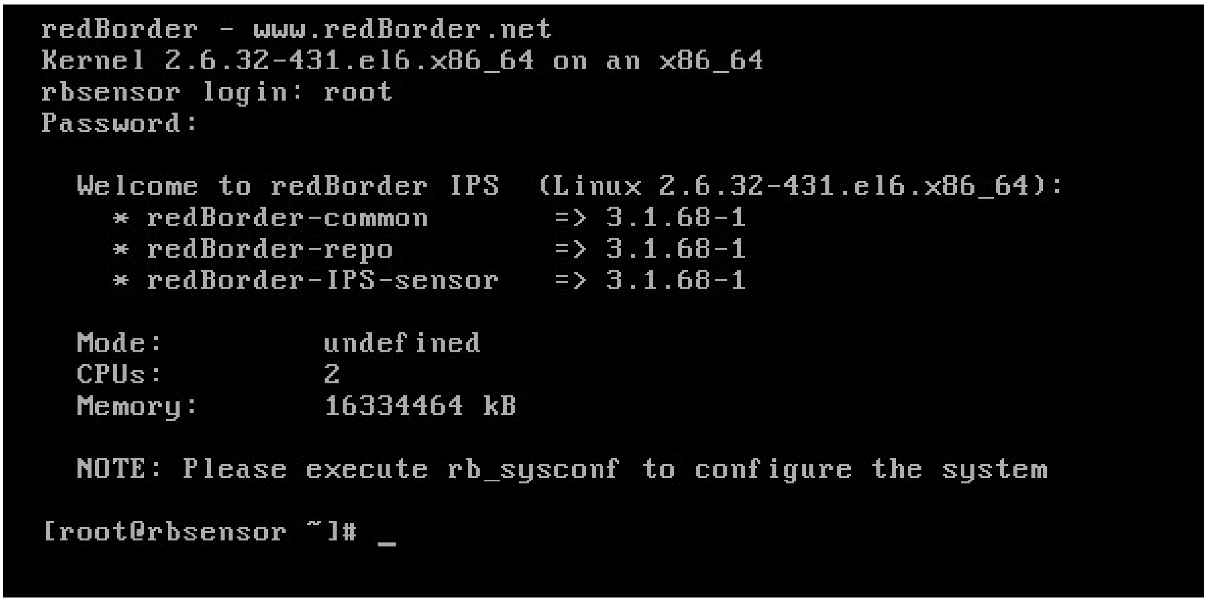
By default, the root password will be *redborder.*

2.3. 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.
2. *Static IP:* in this case redborder will not have any IP assigned.

In both cases we will have to access the system in order to configure and register the sensor in the manager. We will access with the root user and password that was selected during installation.



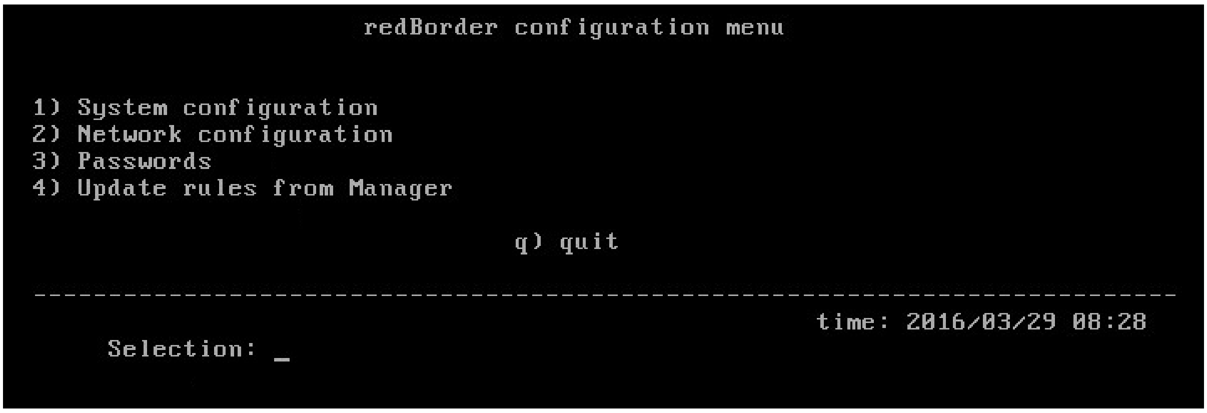
```
redBorder - www.redBorder.net
Kernel 2.6.32-431.el6.x86_64 on an x86_64
rbsensor login: root
Password:

  Welcome to redBorder IPS  (Linux 2.6.32-431.el6.x86_64):
    * redBorder-common        => 3.1.68-1
    * redBorder-repo          => 3.1.68-1
    * redBorder-IPS-sensor    => 3.1.68-1

  Mode:           undefined
  CPUs:           2
  Memory:         16334464 kB

  NOTE: Please execute rb_sysconf to configure the system

[root@rbsensor ~]# _
```

Introducing user/ password

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

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

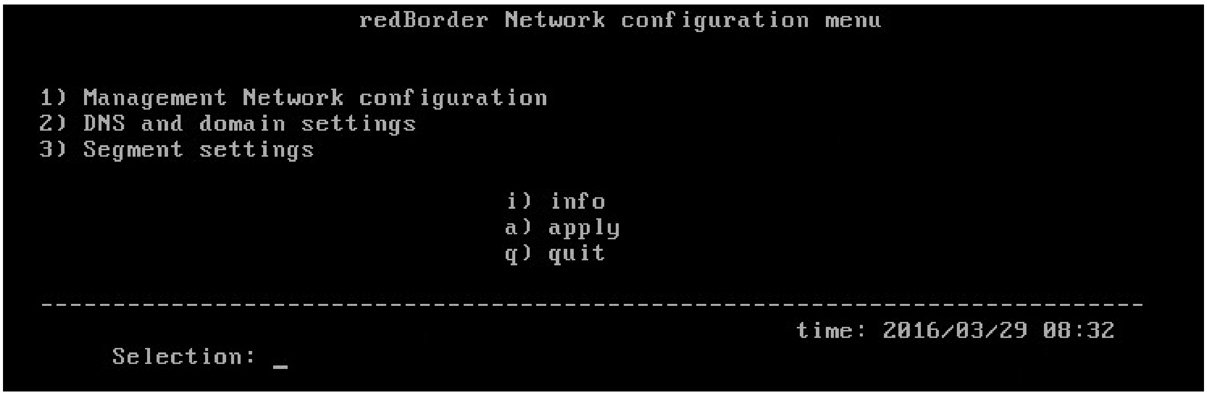
A menu with different options will appear:



```
                    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

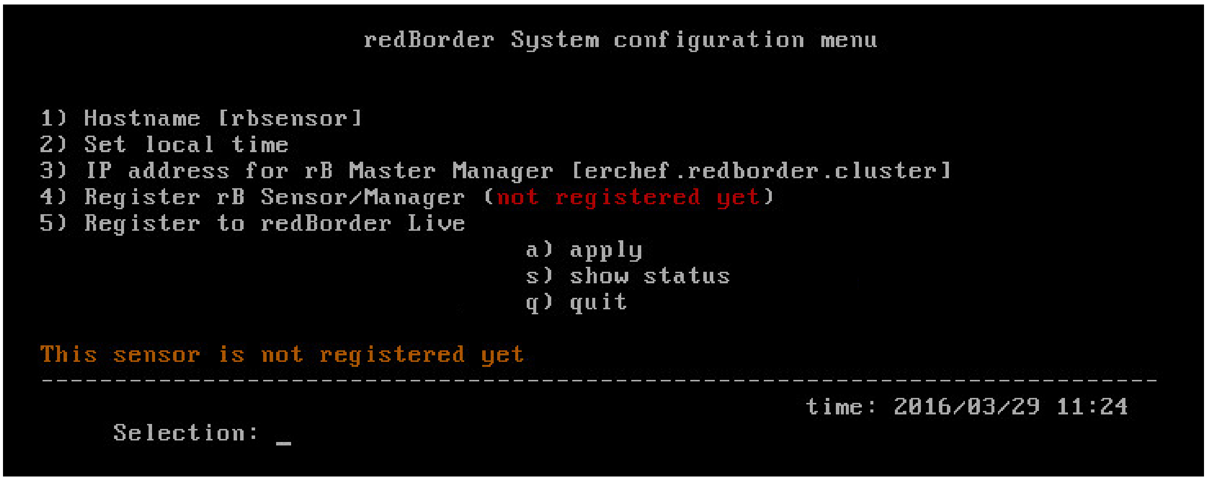
Select option number 2 for Network configuration:



```
                       redBorder Network configuration menu


 1) Management Network configuration
 2) DNS and domain settings
 3) Segment settings

                                 i) info
                                 a) apply
                                 q) quit

 ---------------------------------------------------------------------------
                                                    time: 2016/03/29 08:32
      Selection: _
```

redborder configuration menu

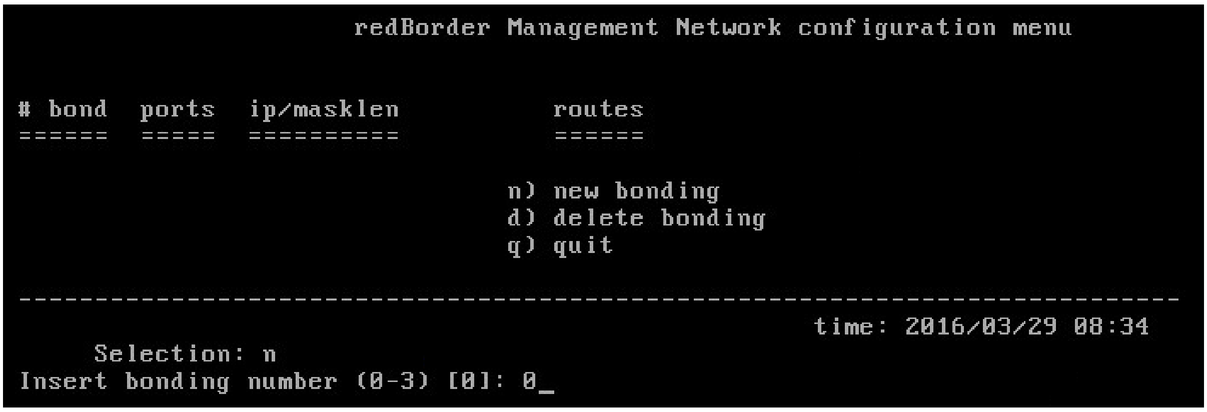
Select option number 1 for Management Network configuration:



```
                       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: _
```

redborder Network configuration menu

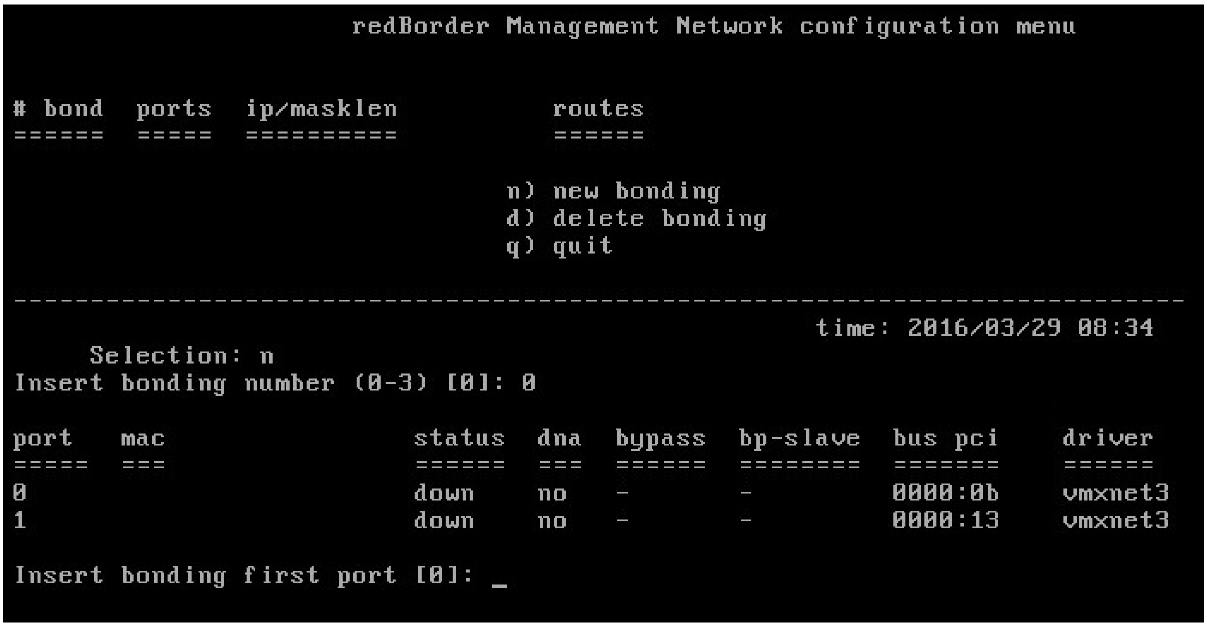
Select option **n** to create a new bonding. We’ll configure the management IP in the first bonding (bond0). We type "0" to create bond0.



```
                        redBorder Management Network configuration menu


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

                                 n) new bonding
                                 d) delete bonding
                                 q) quit

------------------------------------------------------------------------------
                                                      time: 2016/03/29 08:34
     Selection: n
Insert bonding number (0-3) [0]: 0_
```

Bond creation

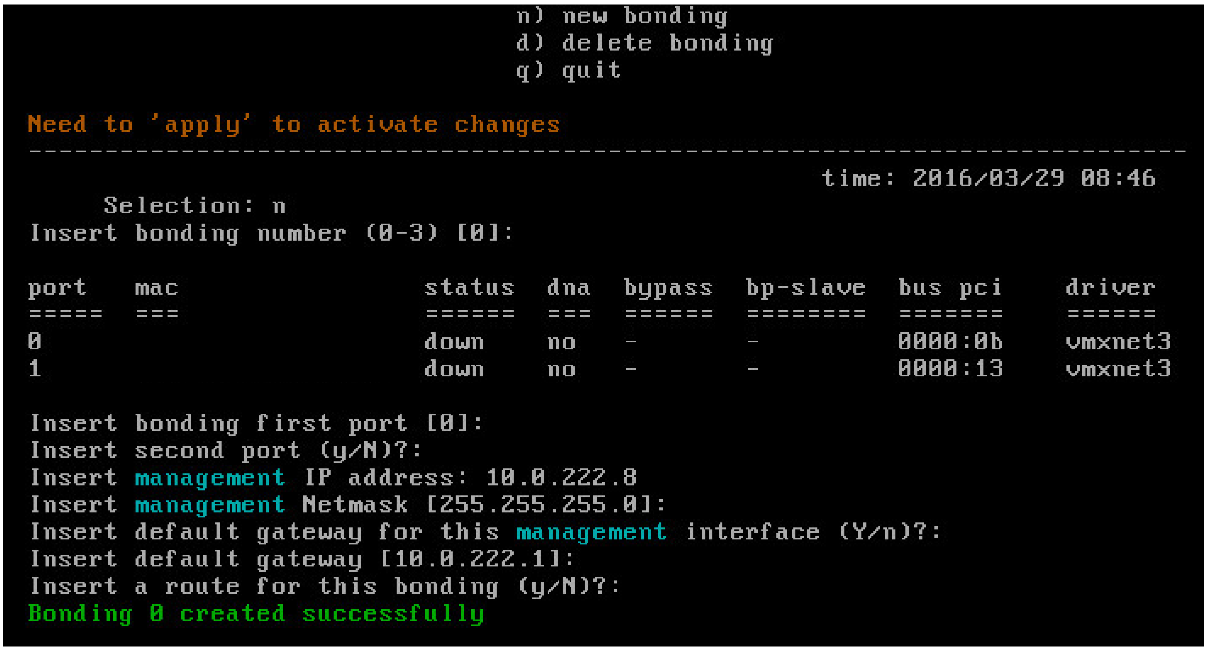
Now we choose the first interface (port) for bond0. The second interface in optional:



```
                  redBorder Management Network configuration menu


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

                                   n) new bonding
                                   d) delete bonding
                                   q) quit

-----------------------------------------------------------------------------
                                                  time: 2016/03/29 08:34
     Selection: n
Insert bonding number (0-3) [0]: 0

port    mac                  status  dna   bypass  bp-slave  bus pci    driver
=====   ===                  ======  ===   ======  ========  =======    ======
0                            down    no    -       -         0000:0b    vmxnet3
1                            down    no    -       -         0000:13    vmxnet3

Insert bonding first port [0]: _
```

Select the interface for bond0

In the next steps we set the IP address, netmask and defaullt gateway. Remember that the sensor requires visibility with the manager. The option **`Insert a route for this bonding`** defines a static route. If you are going to use the default gateway, select **n** for this option.

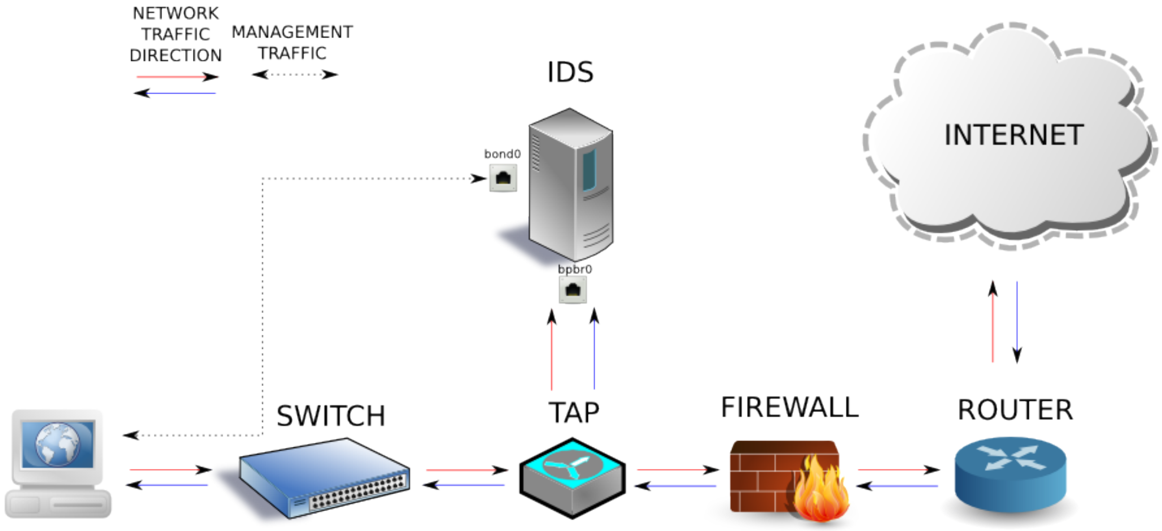


```
                                   n) new bonding
                                   d) delete bonding
                                   q) quit

Need to 'apply' to activate changes
-----------------------------------------------------------------------------
                                                  time: 2016/03/29 08:46
     Selection: n
Insert bonding number (0-3) [0]:

port    mac                  status  dna   bypass  bp-slave  bus pci    driver
=====   ===                  ======  ===   ======  ========  =======    ======
0                            down    no    -       -         0000:0b    vmxnet3
1                            down    no    -       -         0000:13    vmxnet3

Insert bonding first port [0]:
Insert second port (y/N)?:
Insert management IP address: 10.0.222.8
Insert management Netmask [255.255.255.0]:
Insert default gateway for this management interface (Y/n)?:
Insert default gateway [10.0.222.1]:
Insert a route for this bonding (y/N)?:
Bonding 0 created successfully
```

Set IP Address, netmask and gateway

To finish the configuration of the management IP, we need to apply the changes. Then we must return to the previous menu (Network configuration menu) and select option **a**

IDS using Network TAP implementation (SPAN mode)



Select "apply" to save the changes

When the above processes finish, the management interface will be configured.

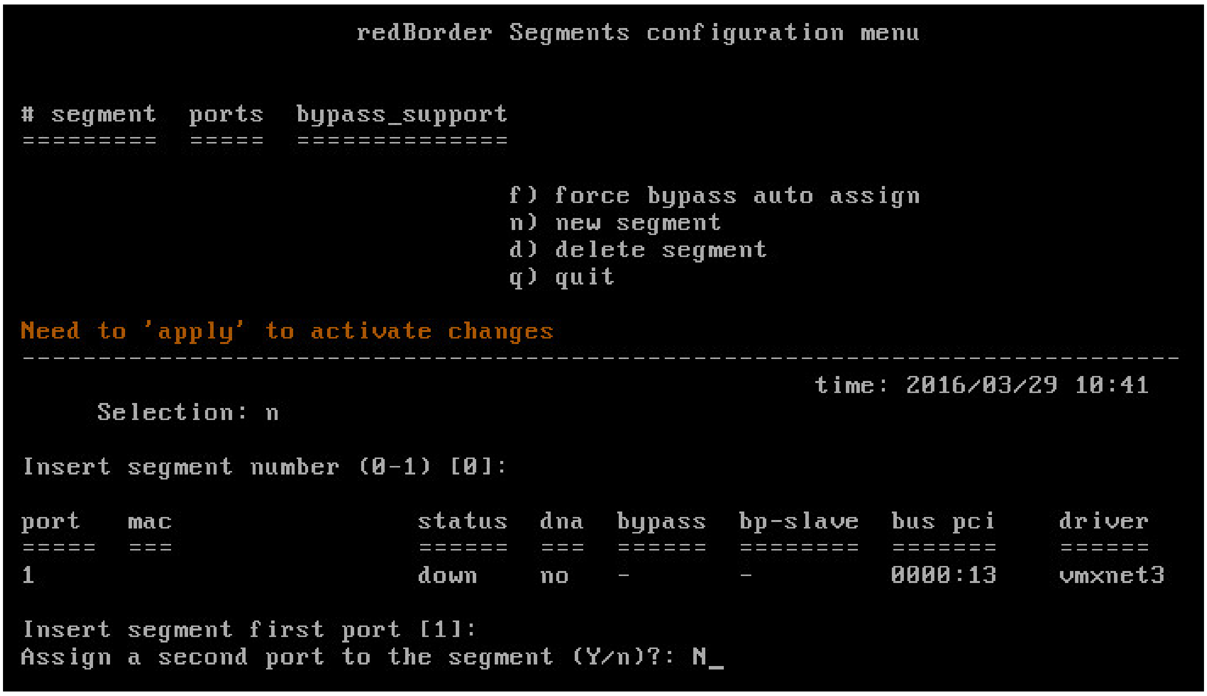
2.3.1. Network interfaces

In this section we must keep in mind whether we want an **Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS).** For the former, we only need a management network interface and another which we will use to analyze traffic. For the latter, in addition to the management interface, we will need **two or more network interfaces.**

In this guide we will assume that there are two network interfaces in our system.

1. *First interface:* We have already configured the first in the previous steps and this is the interface that we will use to communicate with the sensor.

2. *Second interface:*With the second network interface we are going to create a segment with a listening port to analyze the traffic that flows through the said interface. Likewise, we need to send the desired traffic to this second interface. One option is to use a network listening device (Network TAP) which will be configured to resend traffic through the interfaces where it has not received traffic (see image). A diagram is included where the configuration can be seen:



```
                        redBorder Segments configuration menu


# segment  ports  bypass_support
=========  =====  ==============

                                 f) force bypass auto assign
                                 n) new segment
                                 d) delete segment
                                 q) quit

Need to 'apply' to activate changes
-----------------------------------------------------------------------------
                                                       time: 2016/03/29 10:41
     Selection: n

Insert segment number (0-1) [0]:

port   mac                 status  dna  bypass  bp-slave  bus pci    driver
=====  ===                 ======  ===  ======  ========  =======    ======
1                          down    no   -       -         0000:13    vmxnet3

Insert segment first port [1]:
Assign a second port to the segment (Y/n)?: N_
```

IDS (SPAN mode)

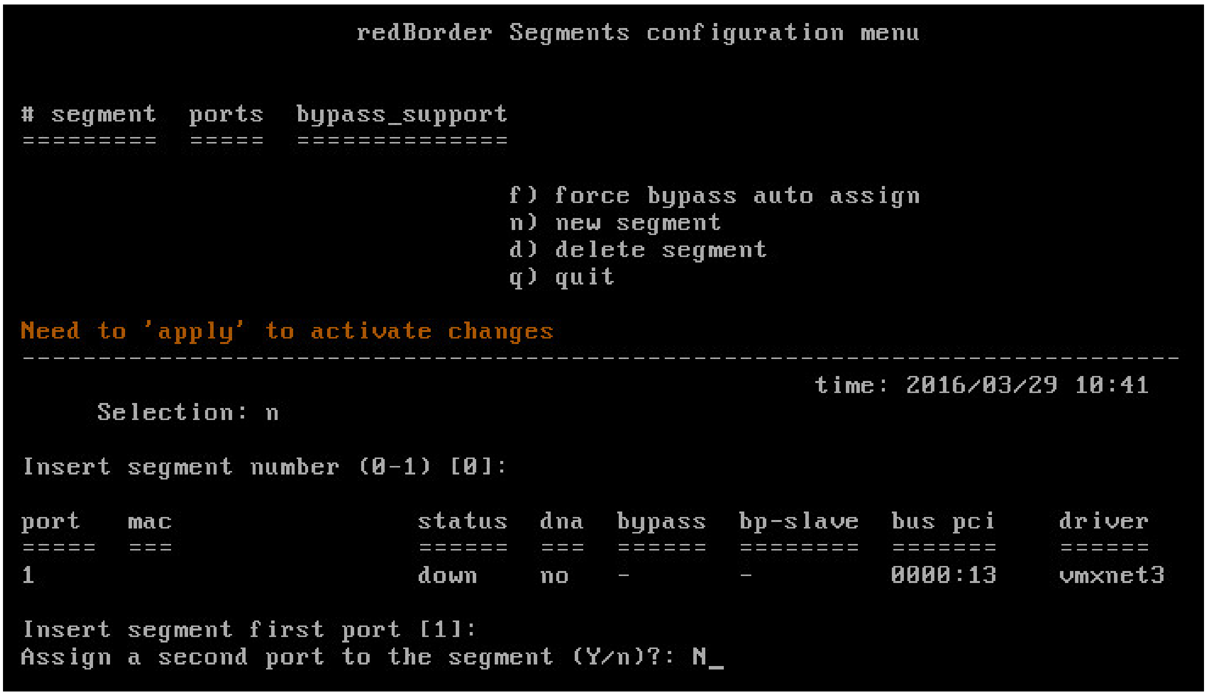
2.3.2. Segment creation

Now select option number **`3 for Segment settings.`** If you have a segment with bypass support, this capability will be auto-configured by default when detected. In our case we are going to assume that we don't have bypass support. So, you must select the option **`n (new segment)`** in order to configure a segment and follow the wizard:

1. Insert segment number (0-1) [0]: Press **`ENTER`** to select 0.

2. Insert segment first port [1]: Press **`ENTER`** to select 1.

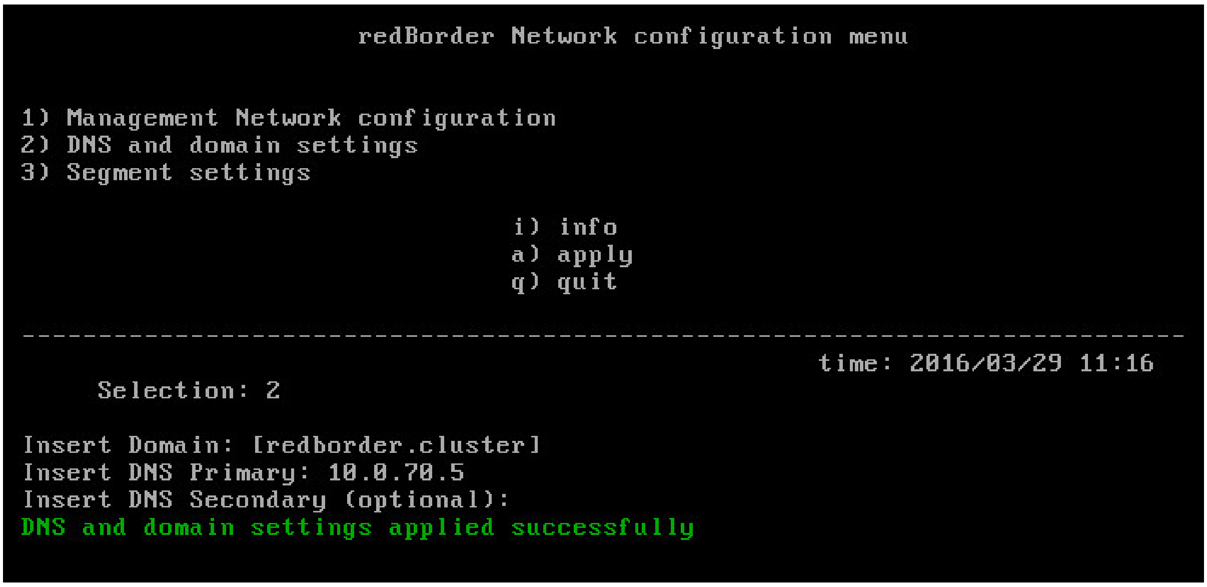
3. Assign a second port to the segment (Y/n): Select N and press **`ENTER`** .



```
                        redBorder Segments configuration menu


# segment  ports  bypass_support
=========  =====  ==============

                                f) force bypass auto assign
                                n) new segment
                                d) delete segment
                                q) quit

Need to 'apply' to activate changes
----------------------------------------------------------------------------
                                                    time: 2016/03/29 10:41
     Selection: n

Insert segment number (0-1) [0]:

port   mac                        status  dna  bypass  bp-slave  bus pci   driver
=====  ===                        ======  ===  ======  ========  =======   ======
1                                 down    no   -       -         0000:13   vmxnet3

Insert segment first port [1]:
Assign a second port to the segment (Y/n)?: N_
```

Assigning ports to each segment

After creating the segment, you must apply the changes. Lastly we can change, in Network Configuration, the DNS configuration and the desired domain. To do this, we select option **`2 - DNS and domain settings.`** We must apply the changes again.

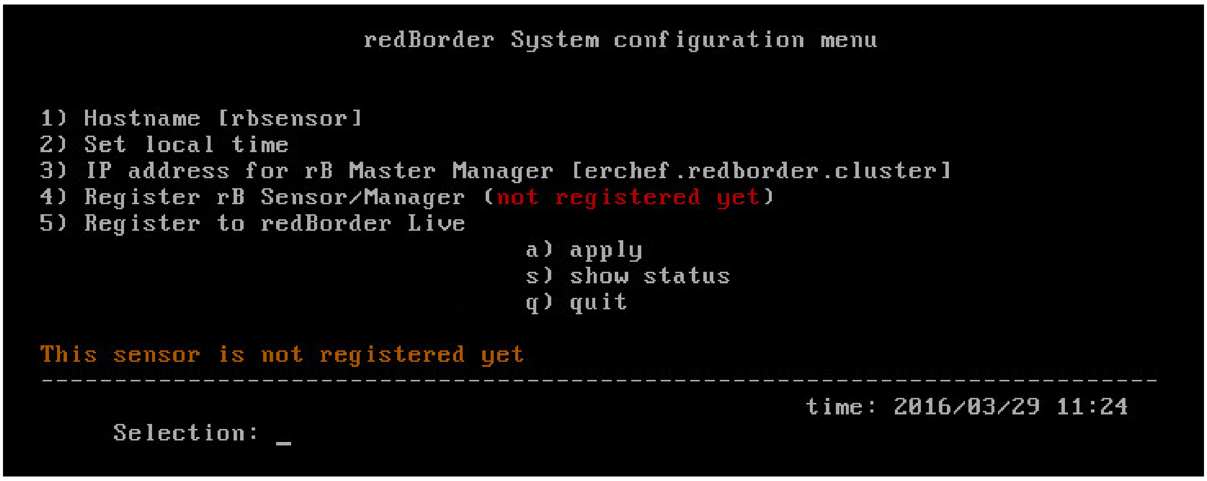


```
                        redBorder Network configuration menu


1) Management Network configuration
2) DNS and domain settings
3) Segment settings

                                i) info
                                a) apply
                                q) quit

----------------------------------------------------------------------------
                                                    time: 2016/03/29 11:16
     Selection: 2

Insert Domain: [redborder.cluster]
Insert DNS Primary: 10.0.70.5
Insert DNS Secondary (optional):
DNS and domain settings applied successfully
```

Adding DNS and domain settings

2.4. Registering the IDS Sensor in the Manager

Now we are going to register the sensor, configured previously, in the Manager. To do this, we must go to the main menu and select option **`1 - System configuration:`**



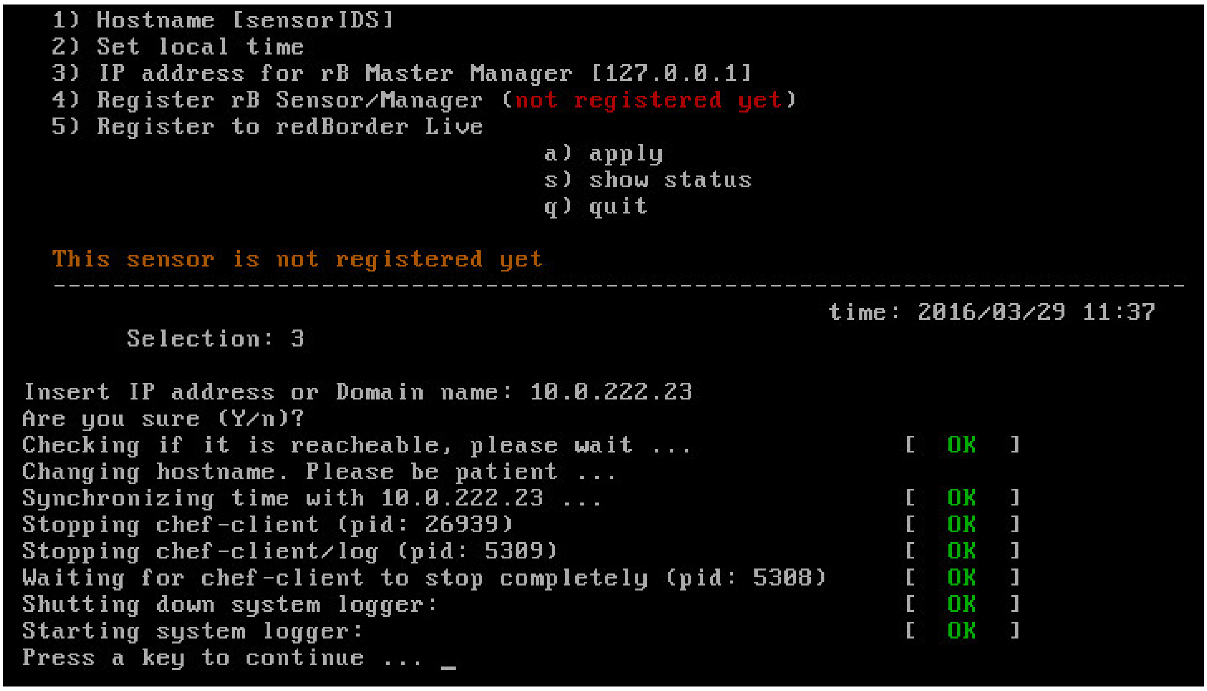
```
                    redBorder System configuration menu


 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: _
```

Registering the IDS Sensor in the Manager

1. Option 1: allows us to create a host name for the IDS/IPS sensor.

2. Option 2: allows us to indicate the local time of the IDS/IPS sensor.

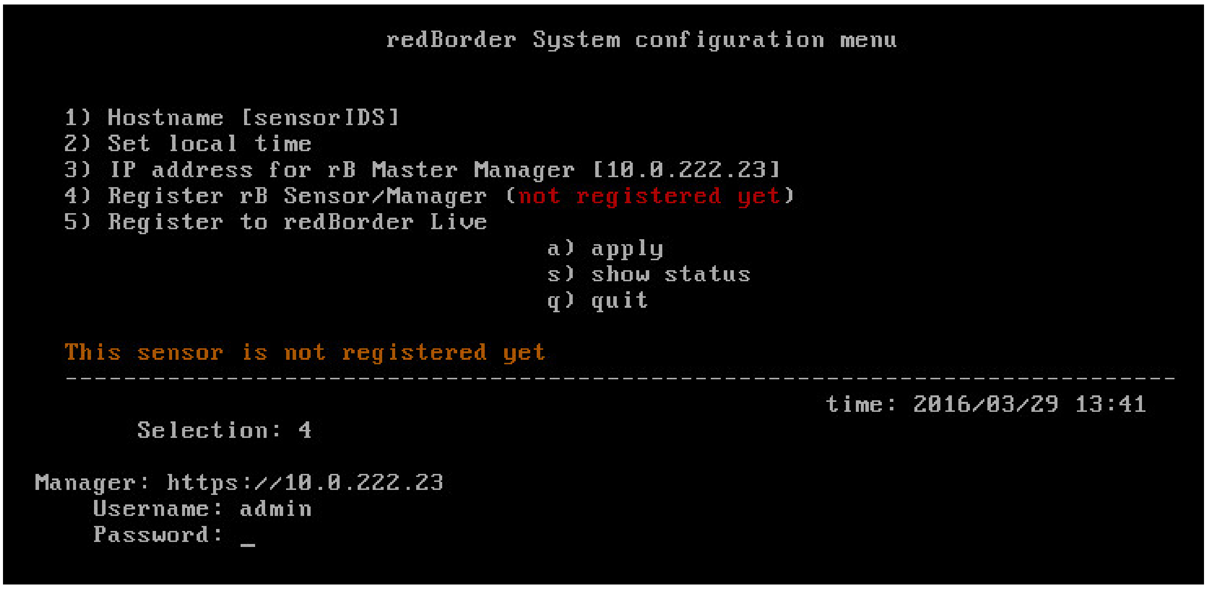
3. Option 3: we must insert the domain or IP that the Manager has in its management interface.



```
   1) Hostname [sensorIDS]
   2) Set local time
   3) IP address for rB Master Manager [127.0.0.1]
   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 11:37
        Selection: 3

 Insert IP address or Domain name: 10.0.222.23
 Are you sure (Y/n)?
 Checking if it is reacheable, please wait ...                [  OK  ]
 Changing hostname. Please be patient ...
 Synchronizing time with 10.0.222.23 ...                      [  OK  ]
 Stopping chef-client (pid: 26939)                            [  OK  ]
 Stopping chef-client/log (pid: 5309)                         [  OK  ]
 Waiting for chef-client to stop completely (pid: 5308)       [  OK  ]
 Shutting down system logger:                                 [  OK  ]
 Starting system logger:                                      [  OK  ]
 Press a key to continue ... _
```

Insert IP Address or domain name

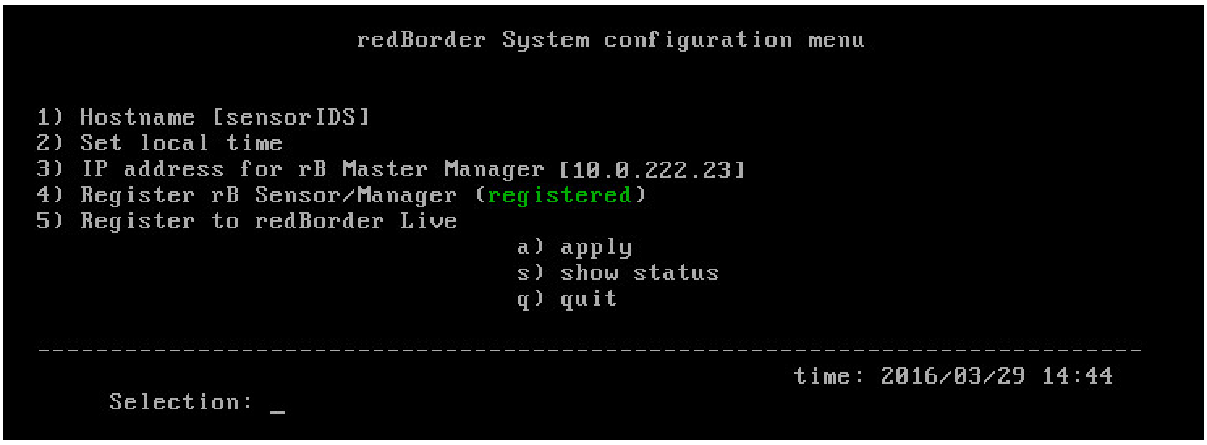
Lastly, we must select option `4 Register rB Sensor/ manager.` This wizard will ask us for the username and password to access the web interface of the Manager (by default, the username is admin and the password is *redborder)*.



```
                          redBorder System configuration menu


    1) Hostname [sensorIDS]
    2) Set local time
    3) IP address for rB Master Manager [10.0.222.23]
    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 13:41
         Selection: 4

  Manager: https://10.0.222.23
      Username: admin
      Password: _
```

Register rB sensor/ manager

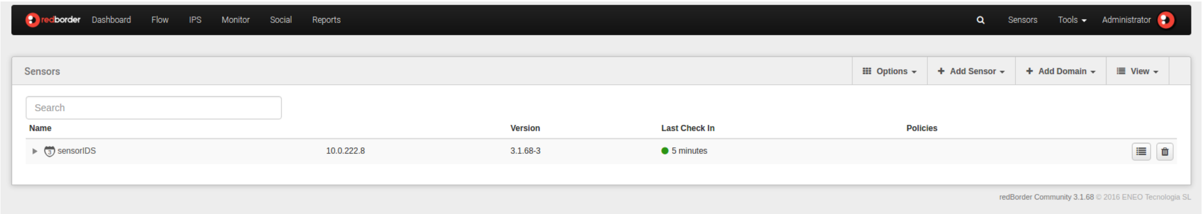
If we have followed these instructions, the sensor will be registered:



```
                        redBorder System configuration menu


  1) Hostname [sensorIDS]
  2) Set local time
  3) IP address for rB Master Manager [10.0.222.23]
  4) Register rB Sensor/Manager (registered)
  5) Register to redBorder Live
                                 a) apply
                                 s) show status
                                 q) quit

  ----------------------------------------------------------------------------
                                                        time: 2016/03/29 14:44
       Selection: _
```

Register rB sensor/ manager

Likewise, it will appear in the web interface of our Manager as configured. 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	

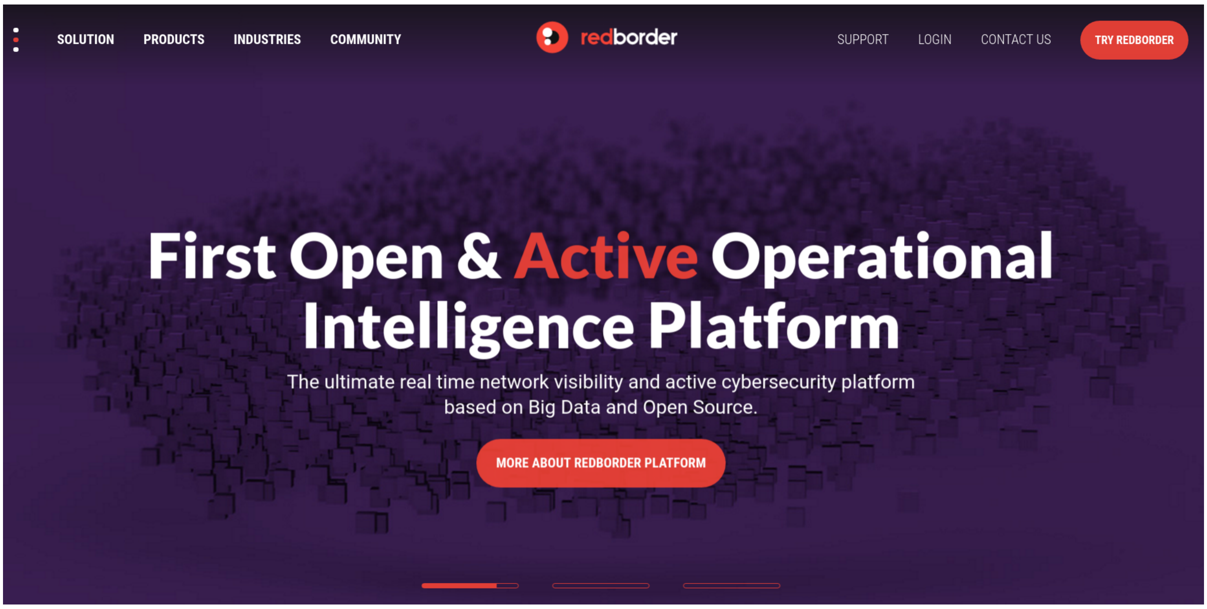
redBorder Community 3.1.68 © 2016 ENEO Tecnologia SL

Sensors interface: checking sensors registration

2.5. Registering the sensor in redborder Live

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.

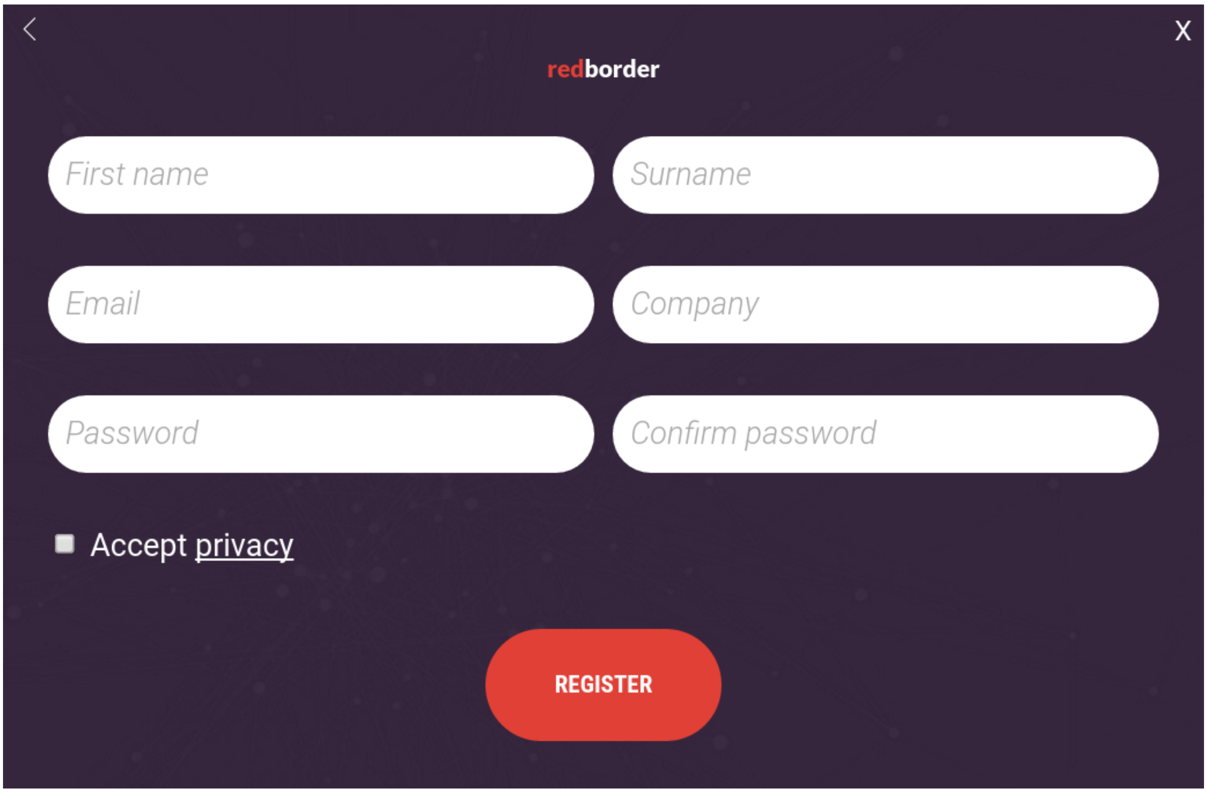


First Open & Active Operational Intelligence Platform

The ultimate real time network visibility and active cybersecurity platform based on Big Data and Open Source.

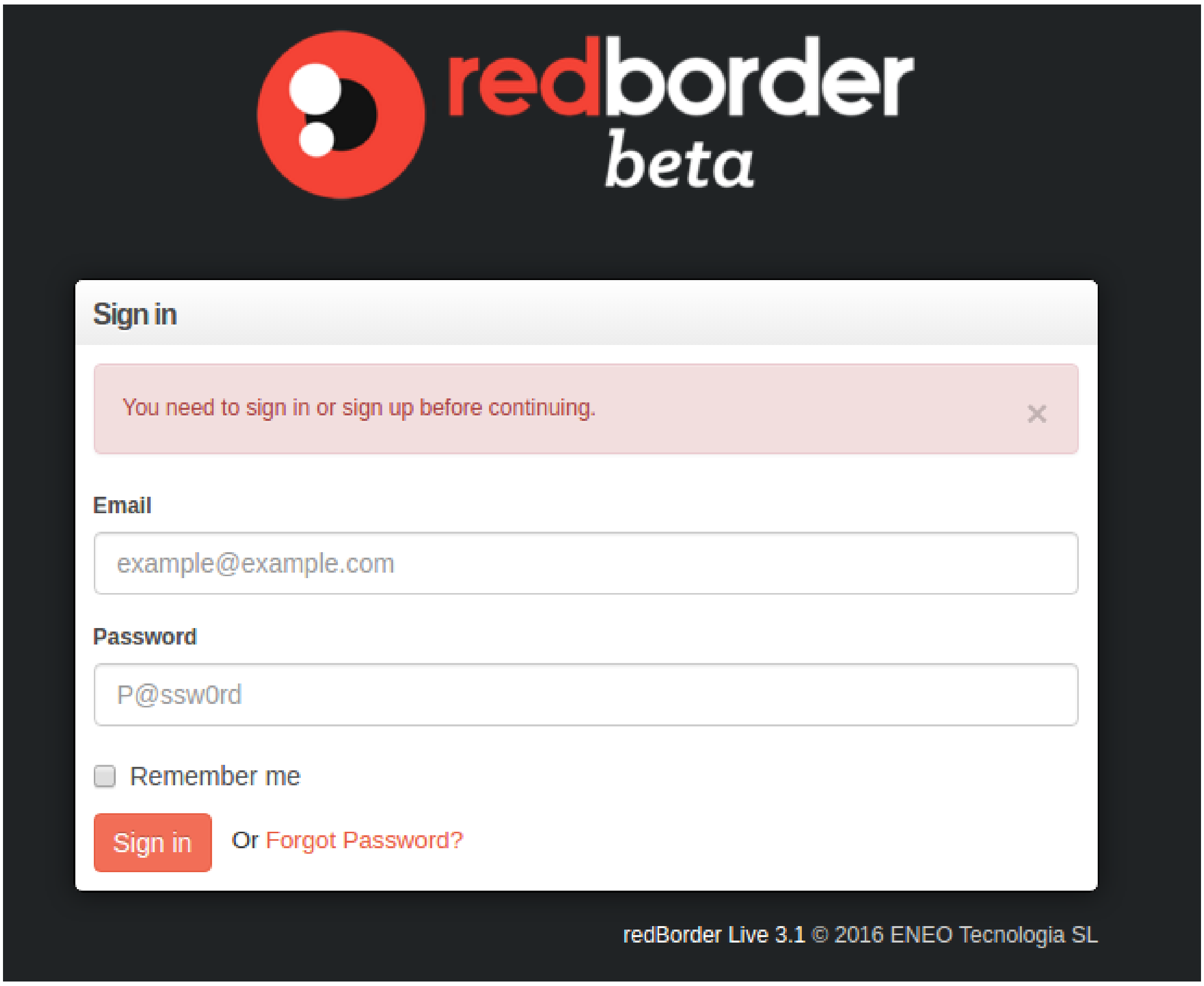
Sign up in redborder Live

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

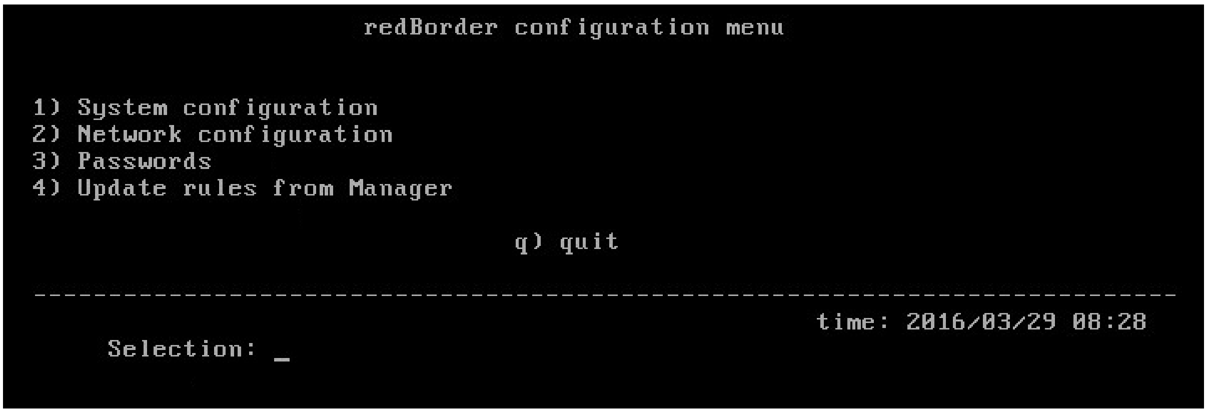
redborder Live login page

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
```

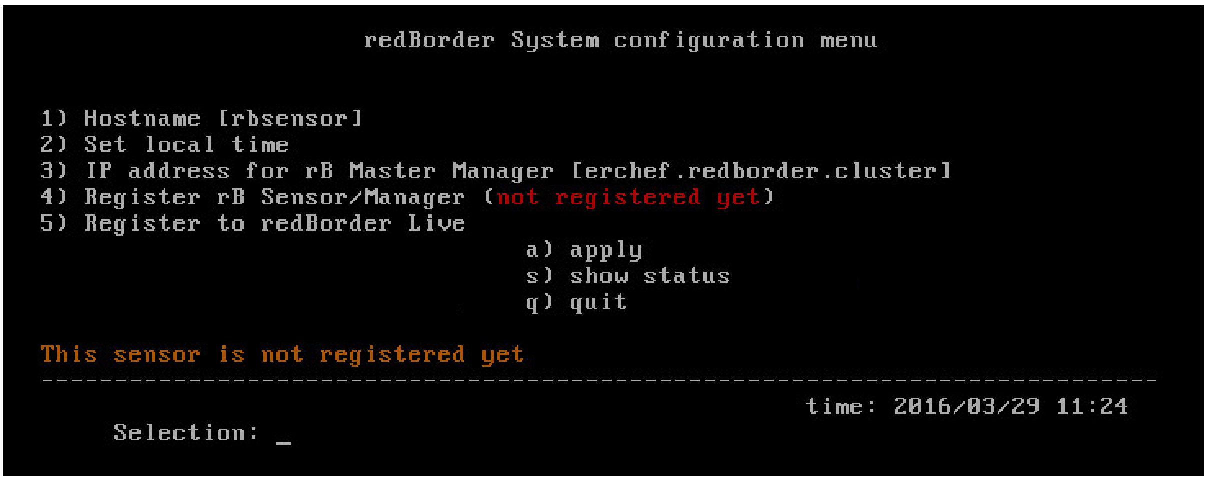
A menu with different options will appear:



```
                        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

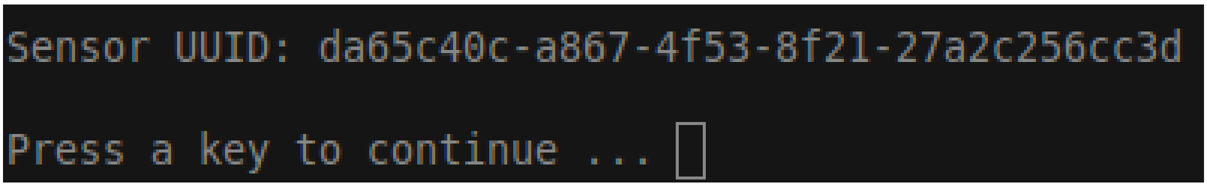
We must select **`option 1 - System configuration`**:



```
                    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

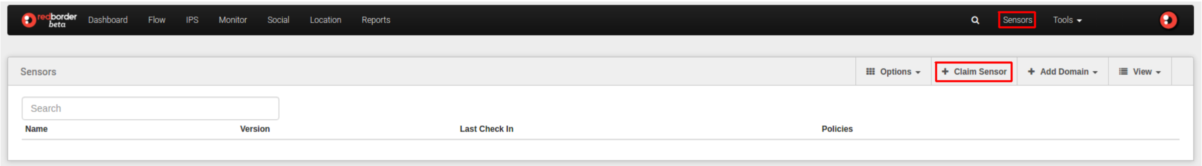
First of all, Option 1 must be selected to create a host name for the IDS/IPS sensor because default hostname rbsensor is not allowed. Then, select Option 5 to start the registration process to redBorder Live. A Sensor UUID will be showed.



```
Sensor UUID: da65c40c-a867-4f53-8f21-27a2c256cc3d

Press a key to continue ...
```

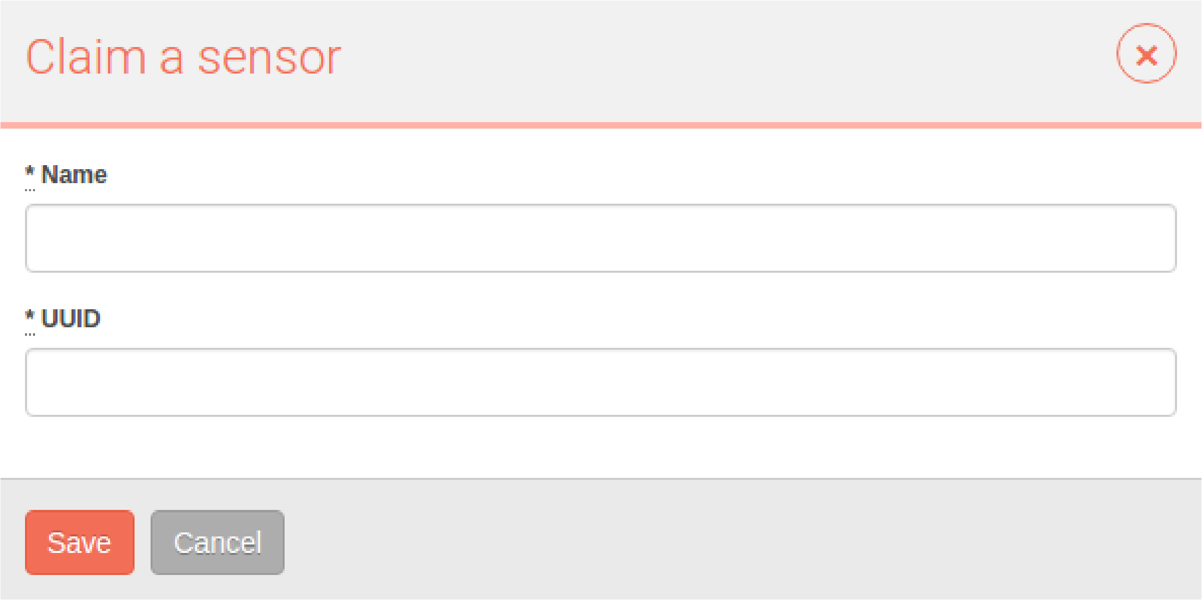
Sensor UUID

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.



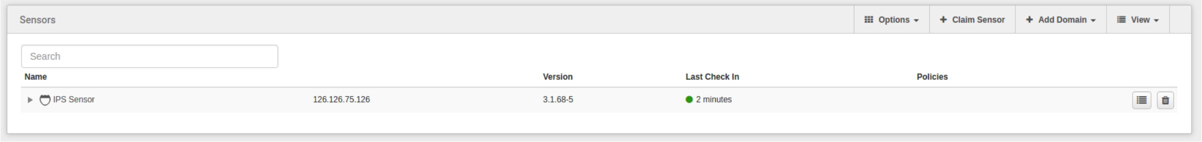
Claim a sensor

* Name

* UUID

Enter the name and UUID of your sensor

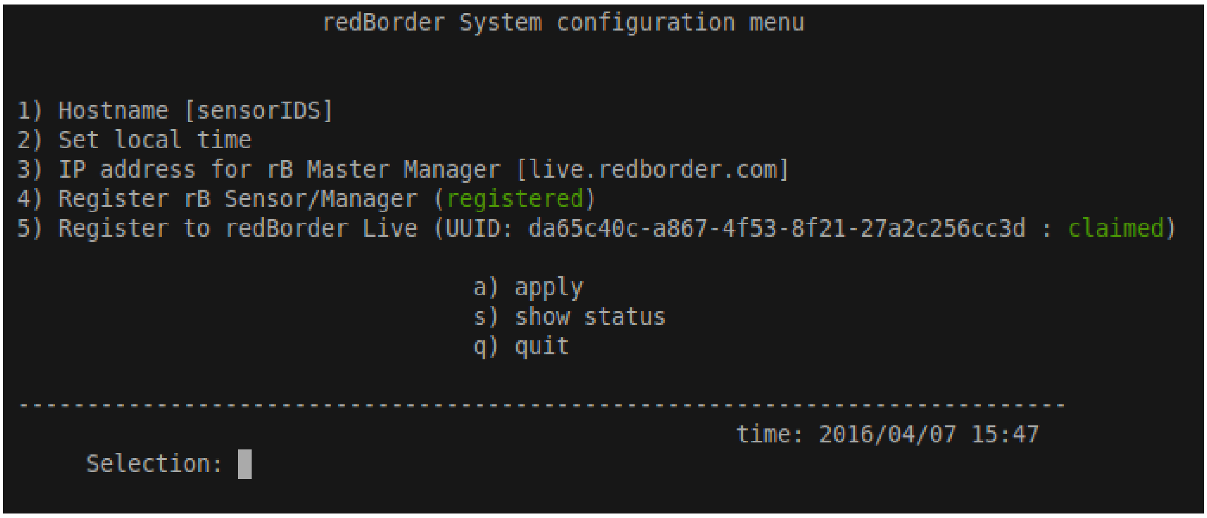
Click on **save** and wait until the sensor is configured correctly. We can then verify that the sensor is working both in redborder Live and by executing the **rb_sysconf** command and selecting option 1 in the menu:



Sensors

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

Sensors interface: claimed sensor

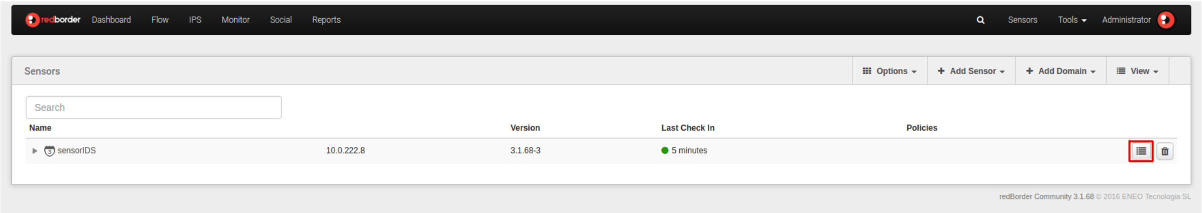


```
                         redBorder System configuration menu


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

2.6. Assigning Resources to Segments

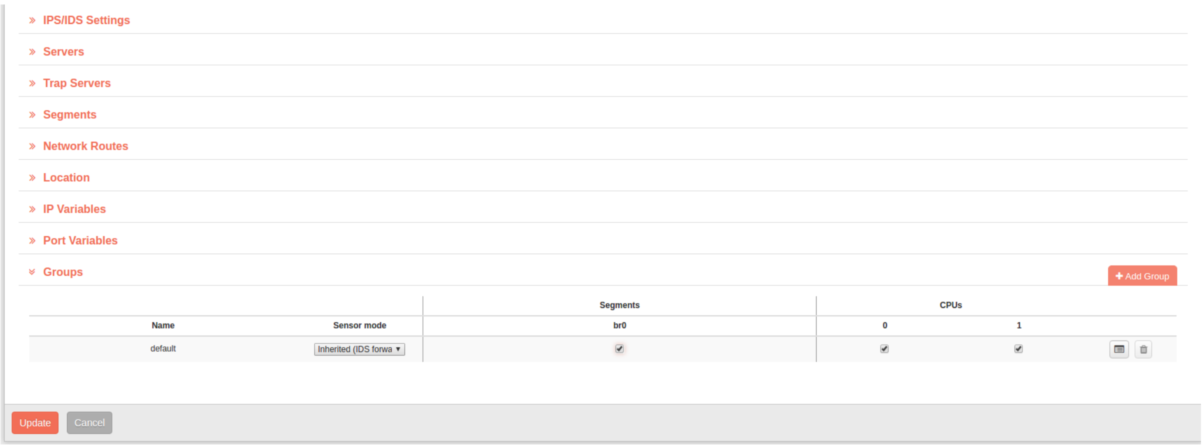
We need to go to Sensor Tab and select **Edit** Option:



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`**.



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

Edit IPS/ IDS settings

Appendix A. Revision History

Revision 0.1-1	**August 2016**	**Eneo Tecnología** *`info@redborder.com`*
IPS Quick Installation Guide for redborder Live		