Setting the wireless AP mikrotik RB951Ui-2HnD for working with the system of captive portal SiCat.

Author: Ing. Msc. Armando Baños Pascual.

Content:

[1. Introduction. 3](#__RefHeading___Toc6283_5733773)

[2. Brief description of the SOHO Wireless AP Devices RB951Ui-2HnD. 4](#__RefHeading___Toc6285_5733773)

[3. Saving the license of the SOHO Wireless AP Device RB951Ui-2HnD. 4](#__RefHeading___Toc6287_5733773)

[4. Preparation of the necessary environment for the reconfiguration of the Wireless AP Device RB951Ui-2HnD. 4](#__RefHeading___Toc6289_5733773)

[4.1. Windows OS. 4](#__RefHeading___Toc6291_5733773)

[4.1.1. Configuration of the network interface that will be used for the connection with the device during programming with the OpenWrt operating system. 4](#__RefHeading___Toc6293_5733773)

[4.1.2. Installation and configuration of tftpd32 software. 5](#__RefHeading___Toc6295_5733773)

[4.2. Linux / macOS OS. 8](#__RefHeading___Toc6346_5733773)

[5. Copy and running of the OpenWrt operating system to the RAM of the device. 8](#__RefHeading___Toc6297_5733773)

[6. Programming the flash memory of the device with the OpenWrt operating system. 10](#__RefHeading___Toc6299_5733773)

[7. Initial configuration of the device. 12](#__RefHeading___Toc6301_5733773)

1. Introduction.

The SiCat captive portal system with social network authentication is a system aimed at providing Internet access to Wi-Fi users at access points such as coffee shops, nightclubs, etc.

To access the Internet, users of the system must connect via Wi-Fi to one of the access points designed for this purpose, authenticate in a social network and post a message related to a sponsor of the system. From that point on, and for a period of time established in the configuration of the system, the user will have free access to the Internet. When that period of time has been completed, the user must authenticate again to continue enjoying the service.

From the technical point of view, the system is composed of the following elements:

* Wireless AP device SOHO RB951Ui-2HnD.

This device is responsible for providing wireless access to users. The operating system of the device is based on the Linux OpenWrt distribution, specifically designed for working with low-performance devices such as wireless routers. The default configuration that is provided will be the minimum necessary for the work as a captive portal of the device.

* SiCat firmware.

It is the main component of the system within the wireless AP device, being the one that provides the necessary functions for the use of this as a captive portal with authentication in social networks.

* Authentication Server.

This component is external to the wireless AP device, and is responsible for providing the user with the necessary means to interact with the social network, allowing him to perform the authentication process to access the Internet once it has been completed.

The work of the wireless AP device is closely related to the authentication server, and the first can not authorize the client if there is no connection to the server.

The objective of this manual is to instruct the technical personnel in charge of the preparation of wireless AP devices mikrotik RB951Ui-2HnD, regarding its reconfiguration with the OpenWrt operating system for wireless routers devices.

1. Brief description of the SOHO Wireless AP Devices RB951Ui-2HnD.

To be done.

1. Saving the license of the SOHO Wireless AP Device RB951Ui-2HnD.

To be done.

1. Preparation of the necessary environment for the reconfiguration of the Wireless AP Device RB951Ui-2HnD.
   1. Windows OS.

In the Windows operating system, the software packages that will be used to prepare the device are:

* DHCP and TFTP protocol server software, tftpd32.

*Important note: The provided version of the tftp32 software should always be used because even when more current versions are available on the official website of this software, the version provided contains specific arrangements to work with the mikrotiks devices that do not have the official versions.*

* Terminal emulation software for remote connections by telnet and ssh.

*Note: For the preparation of this guide, the SecureCRT software was used, but any other application with functionality to use the telnet and ssh protocols can serve this purpose.*

These programs work in any version of the Windows operating system superior or equal to Windows XP, although for the realization of this guide they were only tested in Windows 8 edition 64 bits.

* + 1. Configuration of the network interface that will be used for the connection with the device during programming with the OpenWrt operating system.

For the device programming process you must configure the network interface that will be used for this purpose with the IPv4 address: 192.168.88.10/24.

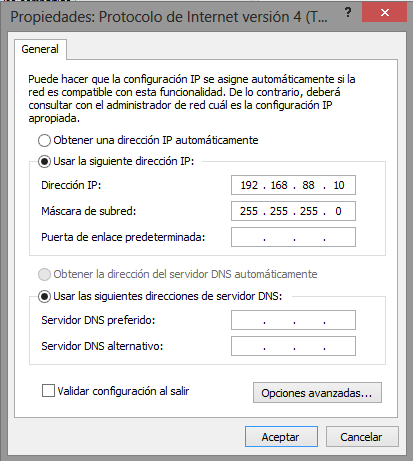


Figure 1: Configuration of the network interface.

* + 1. Installation and configuration of tftpd32 software.

For the installation of the tftpd32 software the only required action is to copy the files: "tftpd32.amd64.exe" and "tftpd32.ini" to any folder on the hard disk of the Windows system. In that same folder we will have to copy the OpenWrt image files that we are going to program in the device:

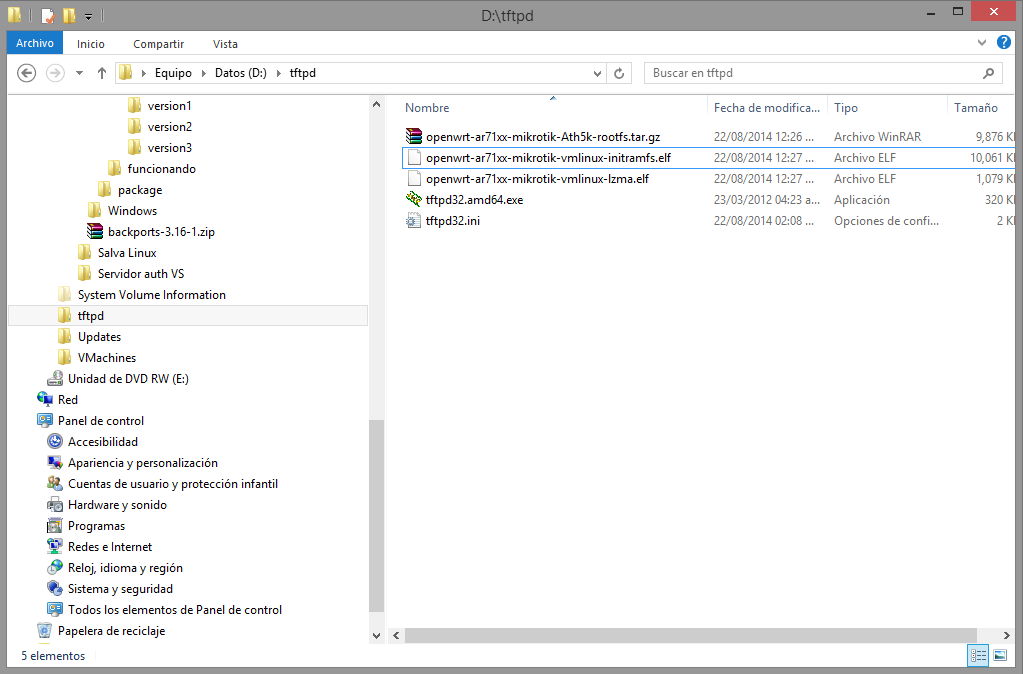


Figure 2: Folder of the tftp32 software and the images to be programmed in the device.

The configuration of the tftpd32 software is done by executing the software as such (file tftpd32.amd64.exe) and pressing the button: "Settings".

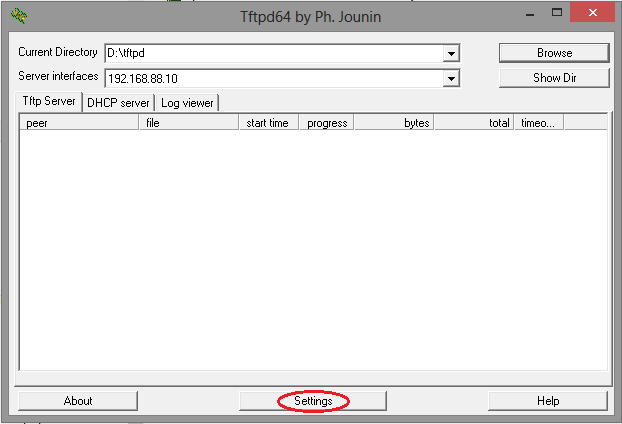


Figure 3: Access to the tftpd32 software configuration.

The tftpd32 software provides other services in addition to those of interest, so those services must be deselected: TFTP client, SNTP server, Syslog server and DNS server. Likewise, support for IPv6 will be disabled, which will not be necessary.

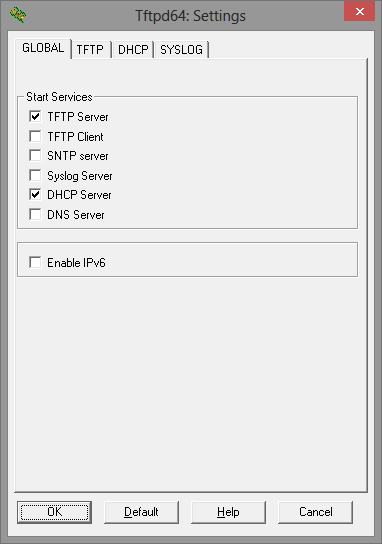


Figure 4: Selection of services.

The configuration of the tftp service is done as shown in Figure 5 of this guide.

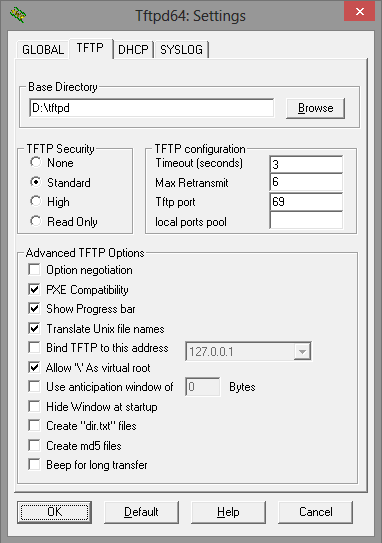
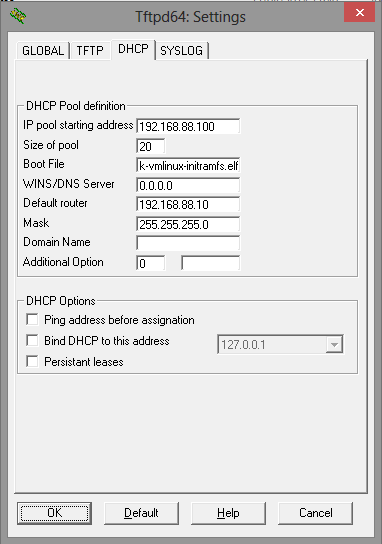


Figure 5: Configuration of the tftp service

The configuration of the DHCP service as shown in the next Figure:



* 1. Linux / macOS OS.

To be done.

1. Copy and running of the OpenWrt operating system to the RAM of the device.

This is the first step in the process of preparing the device. To do this it will be necessary to activate the tftp and dhcp server services provided by the tftpd32 software if the process is being performed from Windows or by the dnsmasq package if it is done from Linux.

Once these services are active, proceed with the following sequence of actions:

* Connect the device to the PC using a network cable between the ethernet port of this and the ethernet port 1 of the device.
* Press and hold the "RES" button on the right side of the device's power connector with a thin clip.
* Turn on the device's holding the RES button pressed.
* The device turns on the PWR LED and in a few seconds it will start flashing the ACT LED, while this happens keep RES pressed.
* When the ACT LED stops flashing release the RES button, at this moment the device will request the tftpd32 server for the boot file.

In Windows, a progress window loading the file to the device should be displayed.

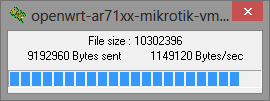


Figure 6: Boot file upload progress window.

* Once the loading is complete, the tftpd32 server window should show us the following messages in the log panel:

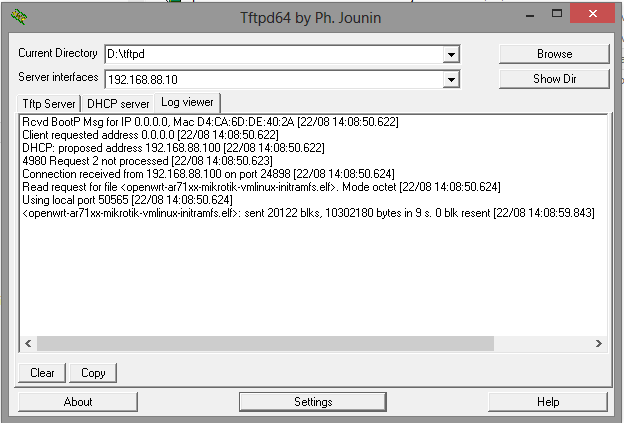


Figure 7: Successful completion of the ram firmware loading process.

* The device restarts by loading the new operating system. This process starts with a beep and ends when the ACT LED stops flashing.

En estos momentos ya el dispositivo tiene cargado como sistema operativo OpenWrt, aunque aún no está grabado en la flash por lo que cuando se desconecte de la alimentación vuelve a cargar el sistema original.

At this time, the device has already loaded as OS OpenWrt, although it is not yet stored in flash, so when it is disconnected from the power it will reload the original system.

OpenWrt, together with other softwares installed on the device (including SiCat) is fully functional, so the relevant tests can be performed to check its operation.

1. Programming the flash memory of the device with the OpenWrt operating system.

To program the OpenWrt operating system in the flash memory of the device, we must connect by telnet to it using the IPv4 address: 192.168.88.1, which is the default one already programmed.

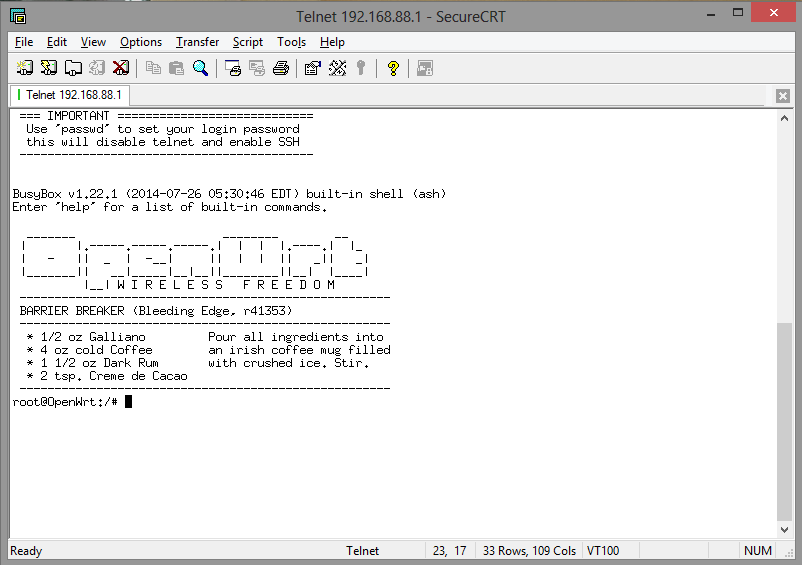


Figure 8: Connection by telnet to the device.

Once connected to the device, the following commands are executed:

* cd /tmp
* atftp
* connect 192.168.88.10
* get openwrt-ar71xx-mikrotik-vmlinux-lzma.elf
* get openwrt-ar71xx-mikrotik-Ath5k-rootfs.tar.gz
* quit

Everything needed to proceed with the programming of the OpenWrt operating system is inside the device, which we can check by listing the /tmp directory:

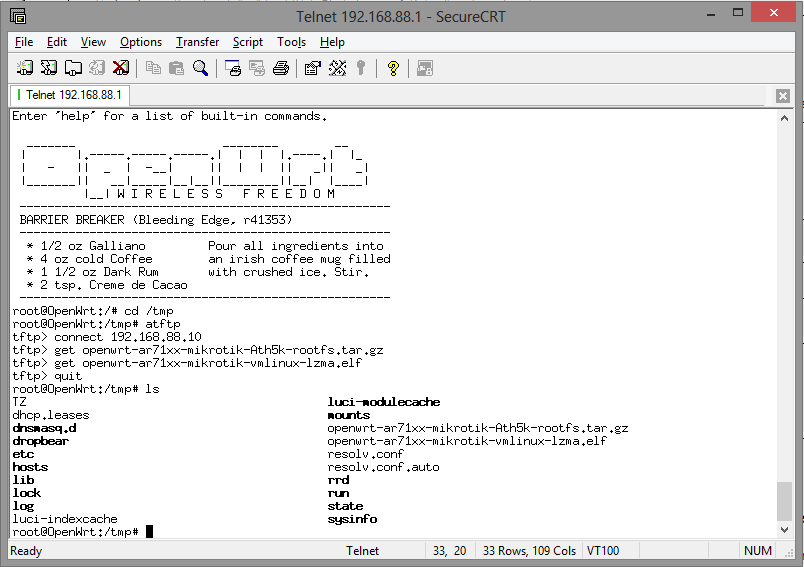


Figure 9: Preparation to definitively program the device with OpenWrt.

Final steps for programming the device:

* mtd erase /dev/mtd1
* mtd erase /dev/mtd2
* mkdir /mnt/kernel
* mkdir /mnt/rootfs
* mount /dev/mtdblock1 /mnt/kernel
* mount /dev/mtdblock2 /mnt/rootfs
* mv /tmp/openwrt-ar71xx-mikrotik-vmlinux-lzma.elf /mnt/kernel/kernel
* chmod +x /mnt/kernel/kernel
* umount /mnt/kernel
* cd /mnt/rootfs
* tar -xvzf /tmp/openwrt-ar71xx-mikrotik-Ath5k-rootfs.tar.gz
* cd /
* umount /mnt/rootfs
* restart.

1. Initial configuration of the device.

After rebooting the device, it will be properly programmed for installation. It will only be necessary to enter the password by default of the system, for which you will access the configuration of the device through the web interface LuCI from a browser, invoking the address http://192.168.88.1.

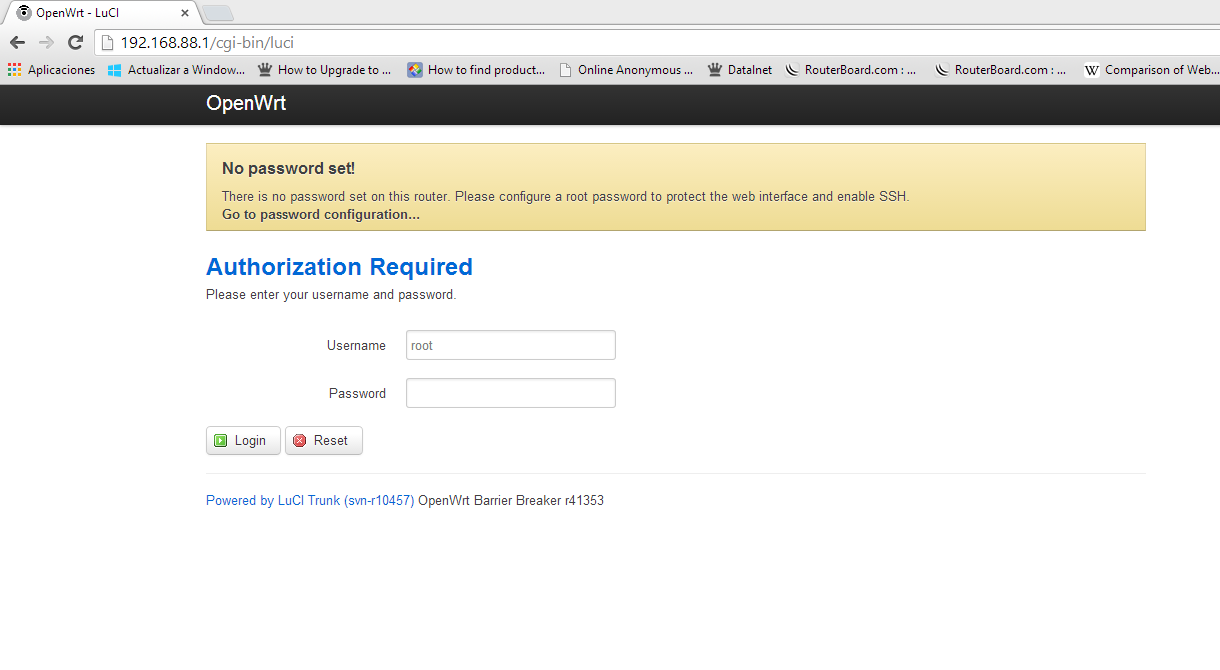


Figure 10: First access to device configuration.

The device is configured without a password, which is indicated in the warning message. To enter just press the "Login" button.

The password is configured in the menu: System / Administration as shown in the figures below.

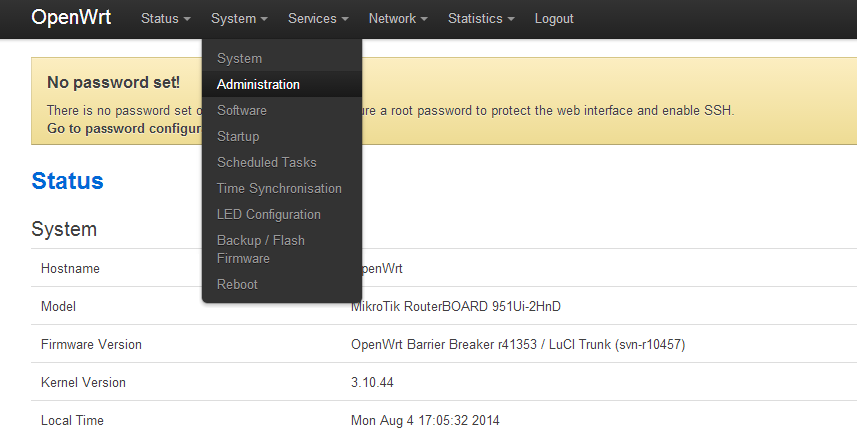


Figure 11: Selection of the Administration menu.

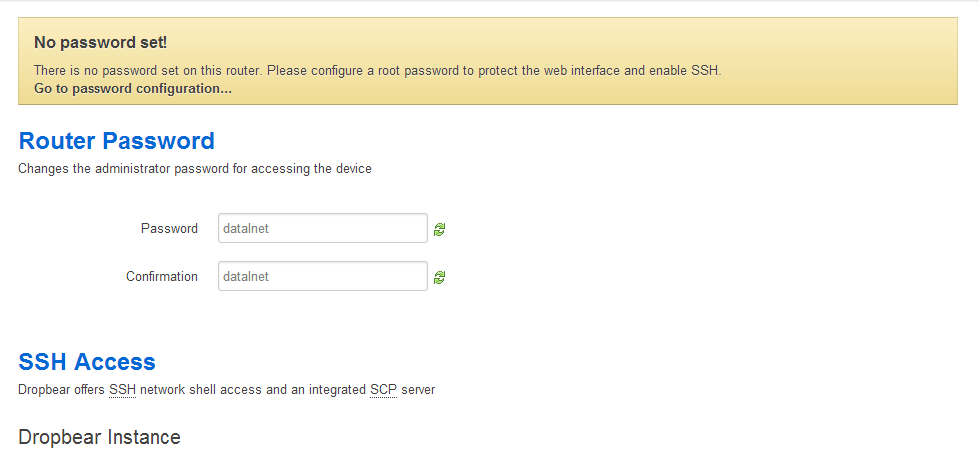


Figure 12: Enter the password by default of the system.

Finally we go down to the bottom of the page and click on the "Save & Apply" button to save the changes.

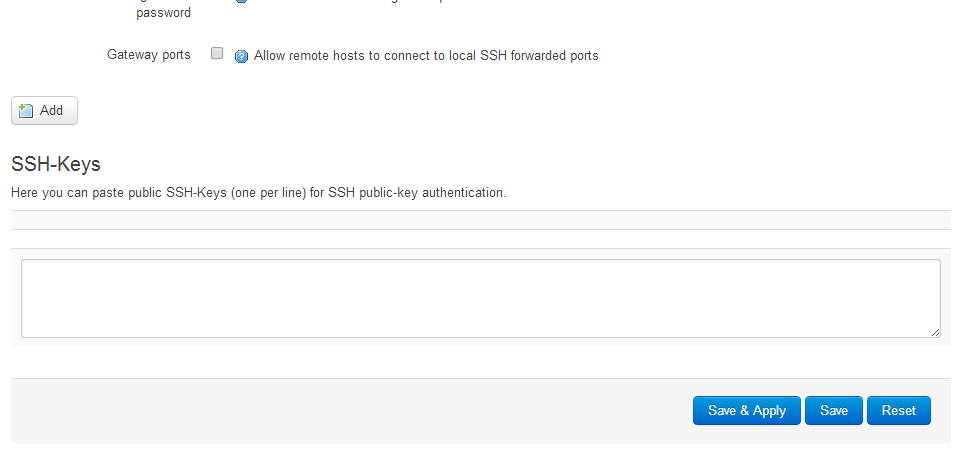


Figure 13: Saved the changes.

The device is properly configured for installation.