OpenWrt Wiki

OpenWrt – First Login

	There is no preset password in OpenWrt! You need to set one at your first login per ssh, telnet or the WebUI.
	**Pre-built trunk images do not come with any web interface or GUI**. You will only be able to login using the CLI, unless you install one yourself: LuCI Essentials
	**Telnet was removed from trunk by 46809. In a newer trunk build, only ssh is available. Note : As of 30/04/2016, Telnet is still available in OpenWrt 15.05.1**

Command-line Interface(CLI)

- Via Telnet: Only if you are using Chaos Calmer 15.05.1 (or earlier) and you have NOT already SET UP a password. After setting a password for the root account, telnet connection is disabled and you must use a ssh connection for CLI.
- Via SSH: Use PuTTY [https://en.wikipedia.org/wiki/PuTTY] , WinSCP [https://en.wikipedia.org/wiki/WinSCP] or HotSSH [https://wiki.gnome.org/Apps/HotSSH]. For OpenWrt builds *prior* to 15.05.1, SSH connection is only available after setting a password for the root account.

HTTP (using your web browser)

- If there is no WebUI (Web user interface) in the image, you can swiftly install one following this HowTo: **LuCI**
- For other WebUIs have a look at the webinterface.overview

*Please note: (HTTP**S** access is only available after First Login)*

OpenWrt System Default

Any freshly installed "vanilla [https://en.wikipedia.org/wiki/Vanilla_software]" OpenWrt Image, will start with these defaults:

- The internal interface **`lan`** and the wireless interface/interfaces **`wlan0`** / **`wlan1`** are bridged together to **`br-lan`**
- wifi is disabled
- the IP address of the internal interface/bridge of the OpenWrt-device is **`192.168.1.1`**`/24`
- dnsmasq [https://en.wikipedia.org/wiki/dnsmasq] is running; it allocates IP addresses in the range of `192.168.1.100 to .250` on the internal interface to connected hosts
- dropbear [https://en.wikipedia.org/wiki/dropbear_(software)] does *not* accept connections (releases up to Chaos Calmer 15.05 and trunk builds before r46809)
- telnet daemon is running on standard port 23 (releases up to Chaos Calmer 15.05 and trunk builds before r46809)
- ssh daemon is running on standard port 22 (trunk builds after r46809)

	**OpenWrt will keep booting into this state until you set a password:**

Login with telnet

- login to your router via **`telnet`**:

```
telnet> open 192.168.1.1 23
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
 === IMPORTANT ============================
  Use 'passwd' to set your login password
  this will disable telnet and enable SSH
 ------------------------------------------
```

```
BusyBox v1.23.2 (2016-01-02 10:46:55 CET) built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 CHAOS CALMER (15.05.1, r48532)
 -----------------------------------------------------
  * 1 1/2 oz Gin            Shake with a glassful
  * 1/4 oz Triple Sec       of broken ice and pour
  * 3/4 oz Lime Juice       unstrained into a goblet.
  * 1 1/2 oz Orange Juice
  * 1 tsp. Grenadine Syrup
 -----------------------------------------------------
root@OpenWrt:/#
```

Note : DO NOT USE the command line "telnet 192.168.1.1" because this connection does not work, you will have this message "Encryption could not be enabled." and next telnet connection is closed by OpenWrt device.

- type **`passwd`** into the prompt. You will be prompted to set a new password for the user root:

```
root@OpenWrt:/# passwd
Changing password for root
New password:
Retype password:
Password for root changed by root
root@OpenWrt:/#
```

- please **choose** a ***secure password***, (consult e.g password strength [http://xkcd.com/936/]) else the passwd tool will say to you "Bad password: too weak" after the line "New password: "
- after you set a password the telnet daemon will be disabled, type `exit` into the prompt
- without reboot, SSH is now available; so is HTTP*S* if the WebUI (LuCI) is installed with it's TLS [https://en.wikipedia.org/wiki/Transport Layer Security]-modules
- login again with `ssh root@192.168.1.1` or use ***signature.authentication***
- proceed with basic.config

Login to WebUI

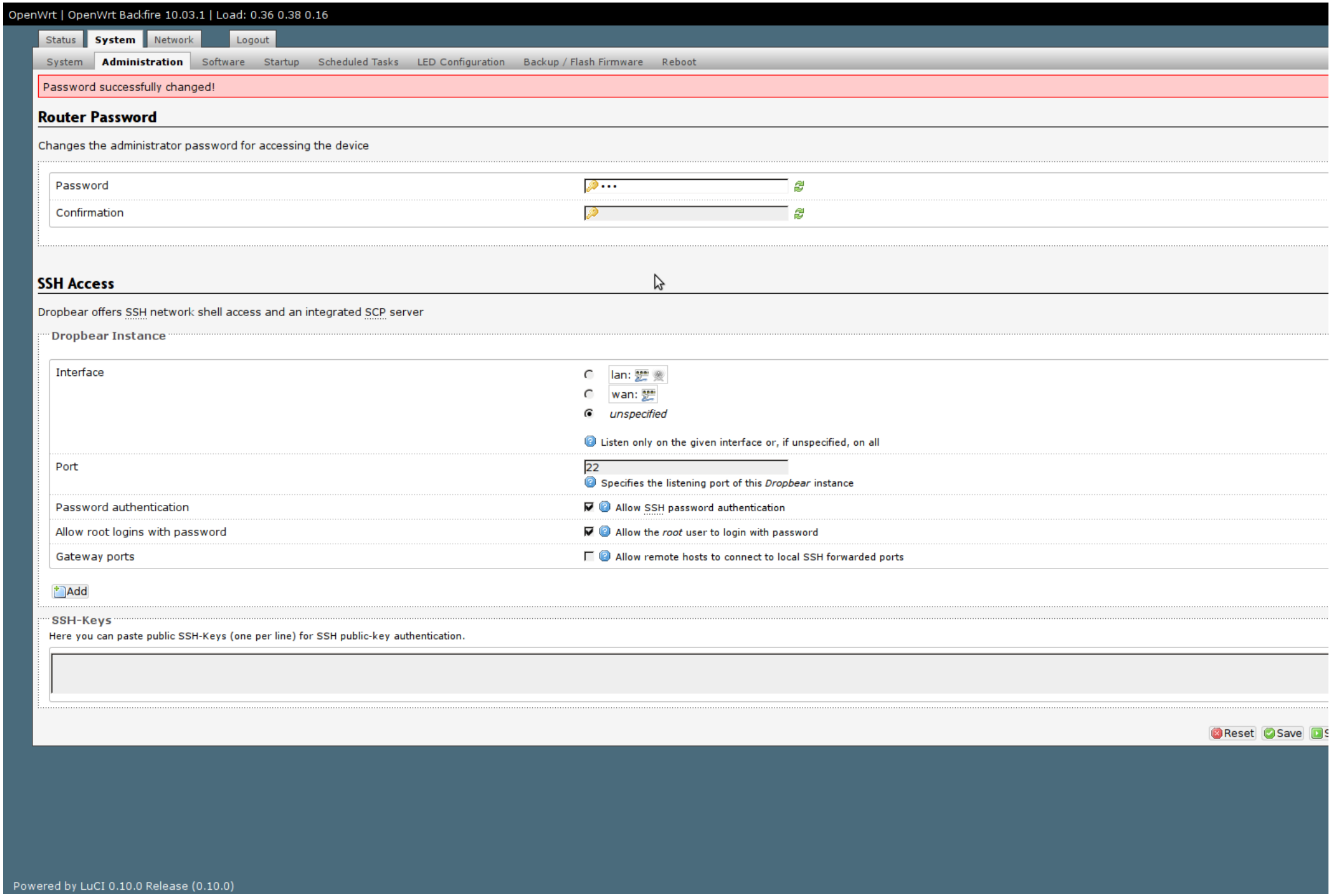
LuCI

First connection to Luci to set up password for root account by GUI

Open your browser and connect to the router at its default address (usually 192.168.1.1). Login using username `root` with an `empty password`.

Make sure your browser accepts (session) cookies. LuCI login fails if password is set and session cookies cannot be accessed.

Then click on the left in the top bar on *Administration*, then go to *System* in the bar underneath. A page to change the password is displayed.


OpenWrt | OpenWrt Backfire 10.03.1 | Load: 0.36 0.38 0.16
Status
System
Network
Logout
System
Administration
Software
Startup
Scheduled Tasks
LED Configuration
Backup / Flash Firmware
Reboot
Password successfully changed!
Router Password
Changes the administrator password for accessing the device
Password
Confirmation
SSH Access
Dropbear offers SSH network shell access and an integrated SCP server
Dropbear Instance
Interface
lan:
wan:
unspecified
Listen only on the given interface or, if unspecified, on all
Port
22
Specifies the listening port of this Dropbear instance
Password authentication
Allow SSH password authentication
Allow root logins with password
Allow the root user to login with password
Gateway ports
Allow remote hosts to connect to local SSH forwarded ports
Add
SSH-Keys
Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.
Reset
Save
Powered by LuCI 0.10.0 Release (0.10.0)

Write your desired password into the field *Password* and repeat it in the field *Confirmation*. Finally click on *Save & Apply*.

- This is the **ADMIN** password for the router, **NOT** your *WiFi* password to connect devices.
  - This password should be a ***minimum 15 characters*** & contain ***at least***:
    - ***two*** **uppercase letters**
    - ***two*** **lowercase letters**
    - ***two*** **numbers**
    - ***two*** **symbols**

Your password is now set.

First connection to Luci after set up password for root account by CLI

Open your browser and connect to the router at its default address (usually http://192.168.1.1 [http://192.168.1.1] or https://192.168.1.1 [https://192.168.1.1]). Login using username `root` and with the password that you have previously set up by CLI (follow the steps in "Login with telnet" part in this web page).

Gargoyle

Open your browser and connect to the Web Interface at its default address (192.168.1.1) the username is ***admin*** OR ***root*** and the password is ***password***. You can ssh to the router at the default address (192.168.1.1) the username is ***root*** the password is ***password***. Unlike OpenWrt the telnet port is not open.

Login Problems

If you encounter problems with login, i.d. you can't login, this may very well be a problem with your firewall settings in Linux or Windows. If you have any firewalls, you may disable them. Also, once you set a password in OpenWrt, telnet will no longer functions (see above).

No SSH access after Setting Password

Try again after a minute or two. On the first bootup OpenWrt will be busy setting up the filesystem and generating SSH keys; the SSH server won't start until after the keys have been generated.

Telnet connection immediately closes

Once you've set a password new telnet connections are immediately terminated. You must SSH at that point.
