



User manual of [GuardPi]





GuardPi is a micro server designed to protect access to harmful, inappropriate websites or block ads on all devices in the local network such as smart TVs, mobile phones, tablets, computers, laptops and other devices without the need to install any software.

Connecting the model of GuardPi v1:

- on the GuardPi box, you can find the LAN MAC address of the given device
- you need create a reservation on the DHCP server within your SOHO router at the IP address specified by you, which GuardPi will use
- you need set up a DHCP server within your SOHO router where you use the IP address defined by you for the GuardPi as the first DNS server
- you need to connect the GuardPi device anywhere in the local network
- then connect the attached adapter to the electrical outlet
- GuardPi will start up, including all services, within 30 seconds

Control the model of GuardPi v1:

- connect via any browser to the web interface of your chosen GuardPi IP address

HOME	START TOR	STOP TOR (ACTIVE)	UPDATE	SUPPORT	REBOOT	SHUTDOWN
EzMonitor		PHP script which provides a web page containing information such as the operating system, the system load, CPU, memory RAM, available disk space, bandwidth usage, and especially the port monitoring services.				
Monit		Monit is a utility for managing and monitoring processes, programs, files, directories and filesystems on a Unix system. Monit conducts automatic maintenance and repair and can execute meaningful causal actions in error situations.				
VnStat		VnStat is a console-based network traffic monitor for Linux that keeps a log of network traffic for the selected interface.				
PI-Hole		The multi-platform, network-wide ad blocker. Block ads for all your devices without the need to install client-side software. The Pi-hole blocks ads at the DNS-level, so all your devices are protected.				

- The upper field is the buttons for controlling the GuardPi
 - START TOR is for turning on the anonymization network (active means what is active)
 - STOP TOR is for turning off the anonymization network (active means what is active)
 - UPDATE is for updating the GuardPi
 - SUPPORT is for activating remote support for 1 hour
 - REBOOT is for restarting the GuardPi
 - SHUTDOWN is for safely shutting down the GuardPi
- The URLs below are intended for
 - EzMonitor is a web interface for monitoring the workload of the given hardware
 - Monit is a system for autonomous repair of running services
 - VnStat is for the system for generating statistics of transmitted data
 - LAN (eth0) => DNS queries within the local network
 - WIFI (wlan0) => Communication via anonymization network
 - PiHole is a filtering DNS system

<http://guardpi.doit.sk/>

GuardPi v1 credentials:

- Access via SSH
 - name: guardpi
 - password: Passw0rd
- Access to PiHole
 - name: -
 - password: Passw0rd
- Access to Monit
 - name: guardpi
 - password: Passw0rd
- Access to anonymous network (TOR)
 - SSID: GuardPi
 - KEY: Passw0rd

Example configuration of DHCP your SOHO router:

DHCP Server:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Start IP Address:	<input type="text" value="192.168.0.100"/>
End IP Address:	<input type="text" value="192.168.0.199"/>
Address Lease Time:	<input type="text" value="120"/> minutes (1~2880 minutes, the default value is 120)
Default Gateway:	<input type="text" value="192.168.0.1"/> (optional)
Default Domain:	<input type="text"/> (optional)
Primary DNS:	<input type="text" value="GuardPi address"/> (optional)
Secondary DNS:	<input type="text" value="8.8.8.8"/> (optional)

Schema diagram of the GuardPi model v1:

