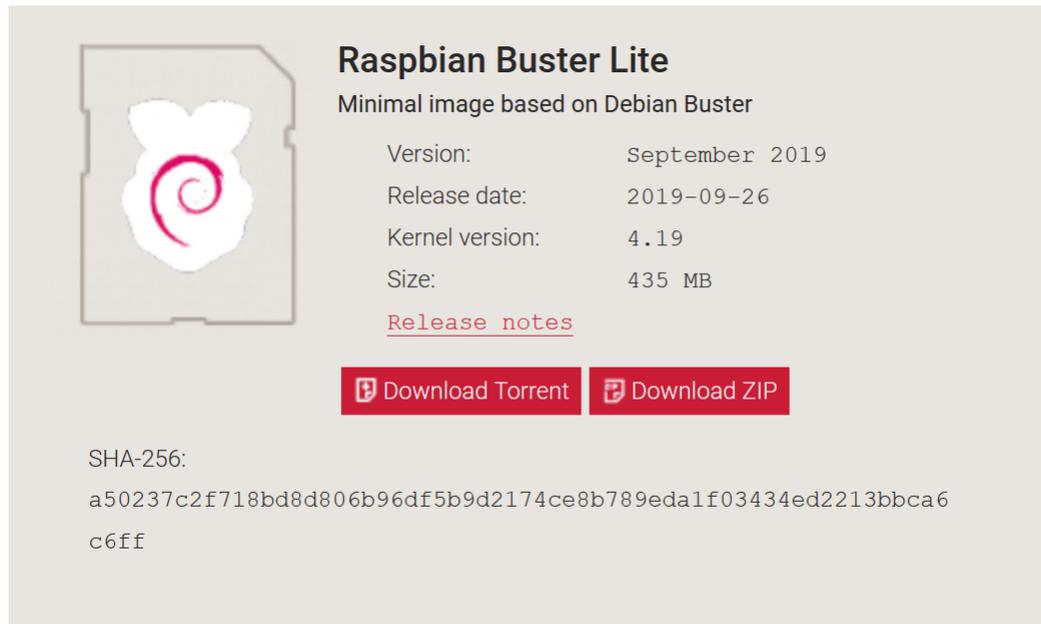


How to set up a Pi-Hole local DNS server w/ DNSSEC and ad-blocking

By Ryan “Techno-Agorist” Burgett



Raspbian Buster Lite
Minimal image based on Debian Buster

Version:	September 2019
Release date:	2019-09-26
Kernel version:	4.19
Size:	435 MB

[Release notes](#)

[Download Torrent](#) [Download ZIP](#)

SHA-256:
a50237c2f718bd8d806b96df5b9d2174ce8b789eda1f03434ed2213bbca6c6ff

1. Download the Raspbian Light image from <https://www.raspberrypi.org/downloads/raspbian/>.

- Download [balenaEtcher](#) and install it.
- Connect an SD card reader with the SD card inside.
- Open balenaEtcher and select from your hard drive the Raspberry Pi `.img` or `.zip` file you wish to write to the SD card.
- Select the SD card you wish to write your image to.
- Review your selections and click 'Flash!' to begin writing data to the SD card.

2. Download and install [balenaEtcher](#) on your computer then follow the above instructions from [Installing operating system images](#) to write the Raspbian Light image to the micro SD card.
3. Once finished, insert the micro SD card into the Raspberry Pi and boot up with the Pi hooked up to a keyboard and monitor.
4. For ``raspberrypi login:`` enter ``pi``.
5. For ``Password:`` enter ``raspberrypi``.
6. Open the Raspberry Pi Software Configuration Tool by entering ``sudo raspi-config``.
7. First, change your password to something unique and record that somewhere.
8. Second, go to ``Network Options`` and change the ``Hostname`` to something recognizable like ``pi-hole`` so that you will be able to recognize the device on your local network.

9. Third, go to `Network Options` and enter your Wi-fi information (if you have a Wi-fi enabled Pi and are going to use Wi-fi rather than a wired connection). A wired connection is generally preferable for something like this.
10. Next, go to `Interfacing Options` and enable the SSH server.
11. Select `Finish` and reboot.

```
pi@pi-hole:~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.123 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::c1e3:5823:9fc1:15a0 prefixlen 64 scopeid 0x20<link>
    ether b8:27:eb:41:eb:53 txqueuelen 1000 (Ethernet)
    RX packets 673 bytes 50276 (49.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 141 bytes 20732 (20.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

12. Once you are logged back in, enter `ifconfig` to see the Pi's network interfaces.
13. Find the device's IP address, usually something like `192.168.x.x`, in the above example, the IP address is 192.168.1.123. Pay attention to the first three numbers.
14. Enter `nano /etc/dhcpd.conf` (or, use `vi` if you are like me).
15. Add the following to the bottom of the file, replacing each line with the appropriate address for your setup. For most people, if their dynamic IP address (what we looked at above) is `192.168.1.x`, their router is `192.168.1.1` and their domain name server is the same as the router. For your static IP, you can choose the current IP address or another one, but you probably make sure that the IP address isn't already in use by another device (you can check this from your router admin control panel). In my case, I already have my network configured to only dynamically give out addresses over 100, which leaves addresses 1-99 free for static IPs, so for my example I chose address 5.

```
...
interface eth0
static ip_address=192.168.1.5
static routers=192.168.1.1
static domain_name_servers=192.168.1.1
...
```

16. Save the file and reboot.
17. Enter `sudo su`.
18. Enter `apt-get update` to update the apt package lists.
19. Enter `apt-get install -y ufw` to install the UFW firewall.
20. Enter the following to configure the firewall to allow SSH and to open the necessary ports for the Pi-Hole:

```
...
ufw allow 22
ufw allow 80/tcp
ufw allow 53/tcp
ufw allow 53/udp
ufw allow 67/tcp
ufw allow 67/udp
...
```

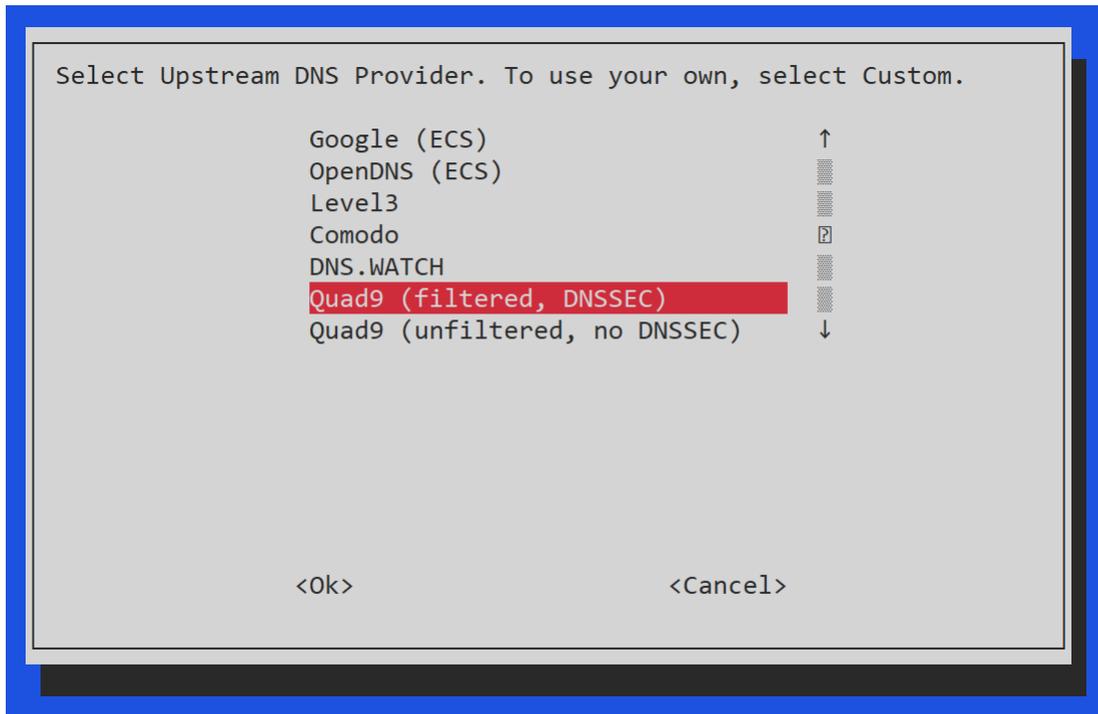
21. Enter `ufw enable` to enable the firewall.

```
root@pi-hole:/home/pi# ufw status
Status: active

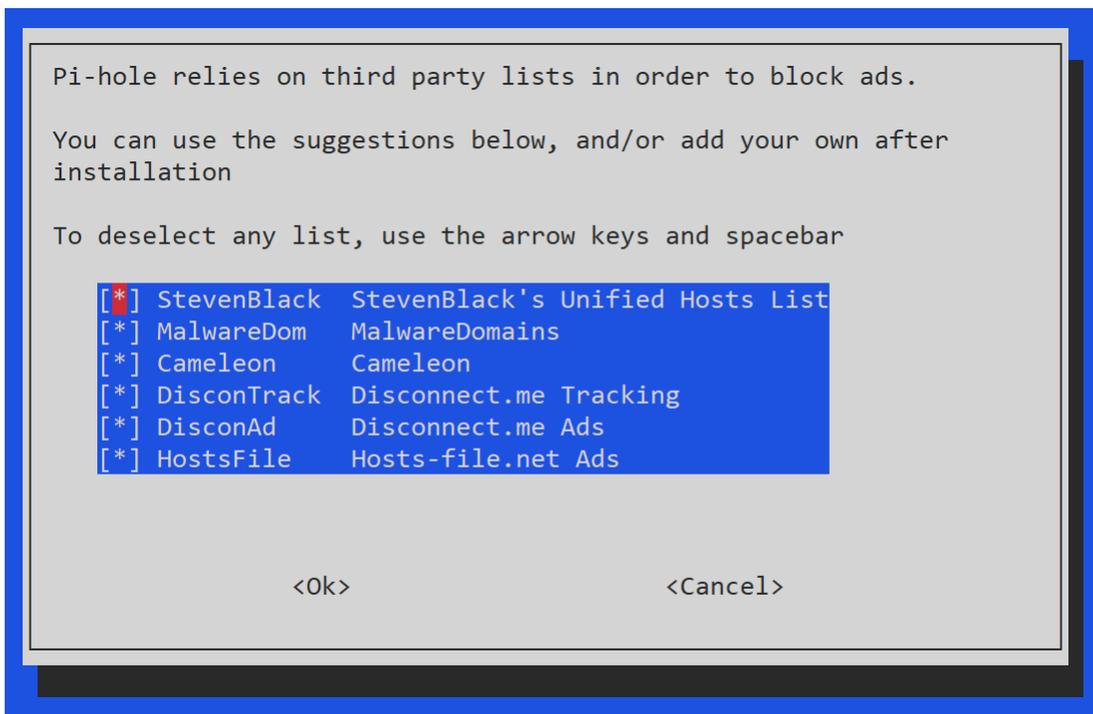
To Action From
-- ---
22 ALLOW Anywhere
80/tcp ALLOW Anywhere
53/tcp ALLOW Anywhere
53/udp ALLOW Anywhere
67/tcp ALLOW Anywhere
67/udp ALLOW Anywhere
22 (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
53/tcp (v6) ALLOW Anywhere (v6)
53/udp (v6) ALLOW Anywhere (v6)
67/tcp (v6) ALLOW Anywhere (v6)
67/udp (v6) ALLOW Anywhere (v6)
```

- 22. Enter `ufw status` to make sure that all the necessary ports were opened.
- 23. Enter `exit` to leave sudo mode.
- 24. Enter the following to run the [One-Step Automated Pi-hole Install](https://install.pi-hole.net):

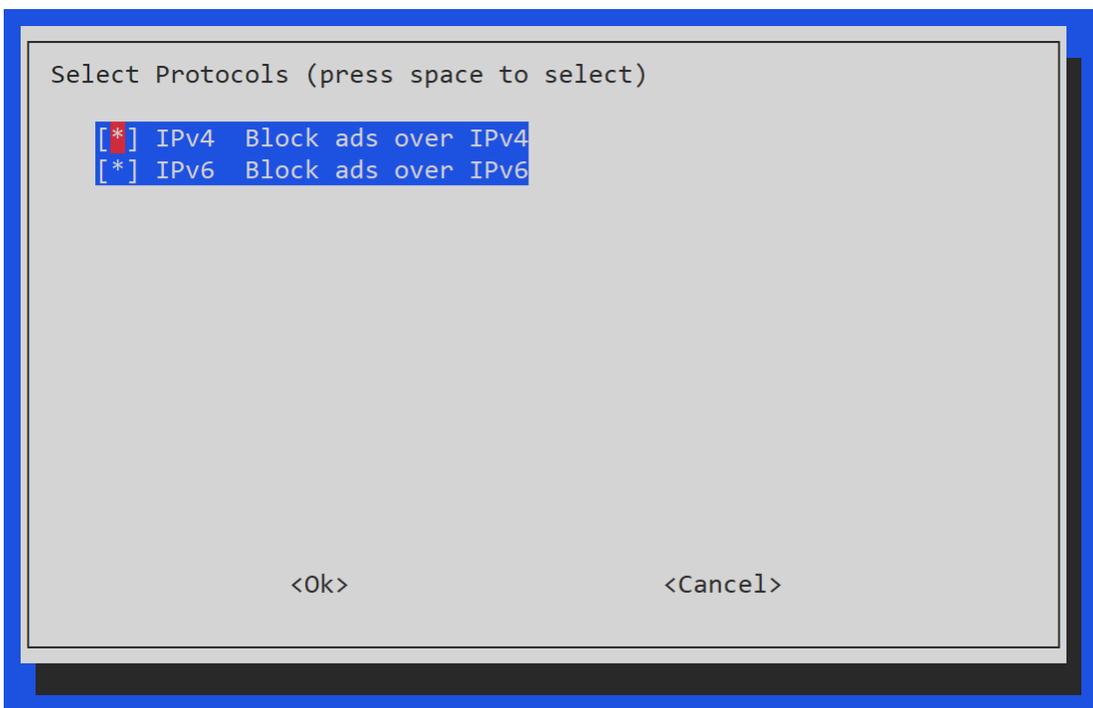
```
`sudo curl -sSL https://install.pi-hole.net | bash`
```



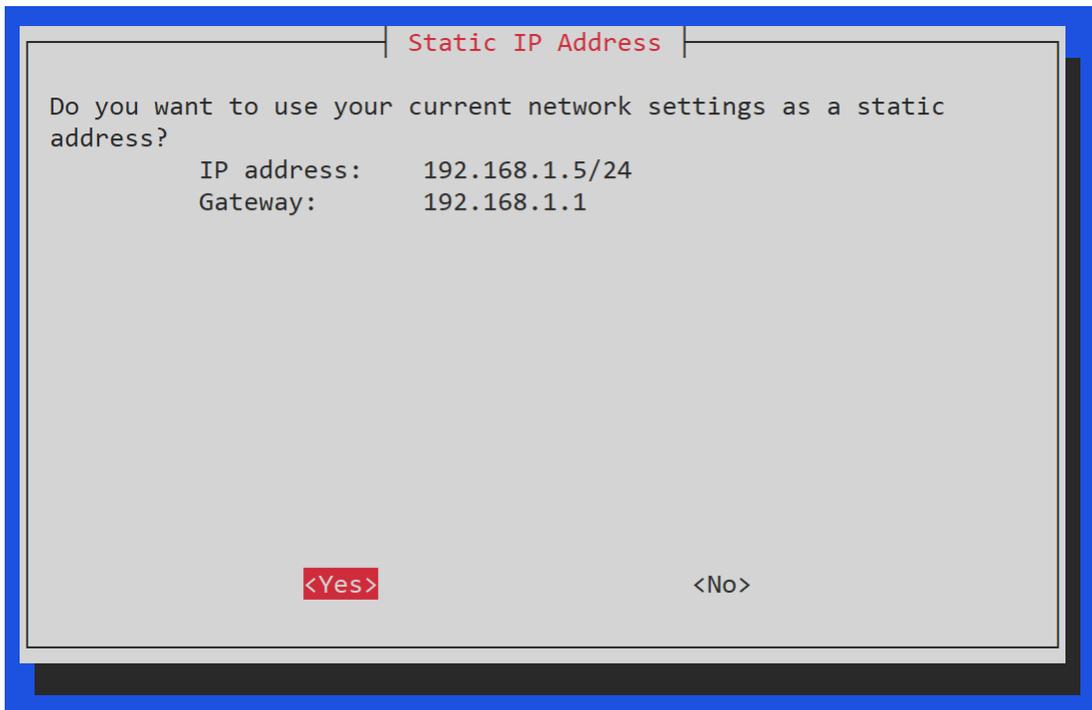
- 25. When asked which DNS Provider to use, select whichever one you would like, but I recommend Quad9 filtered with DNSSEC.



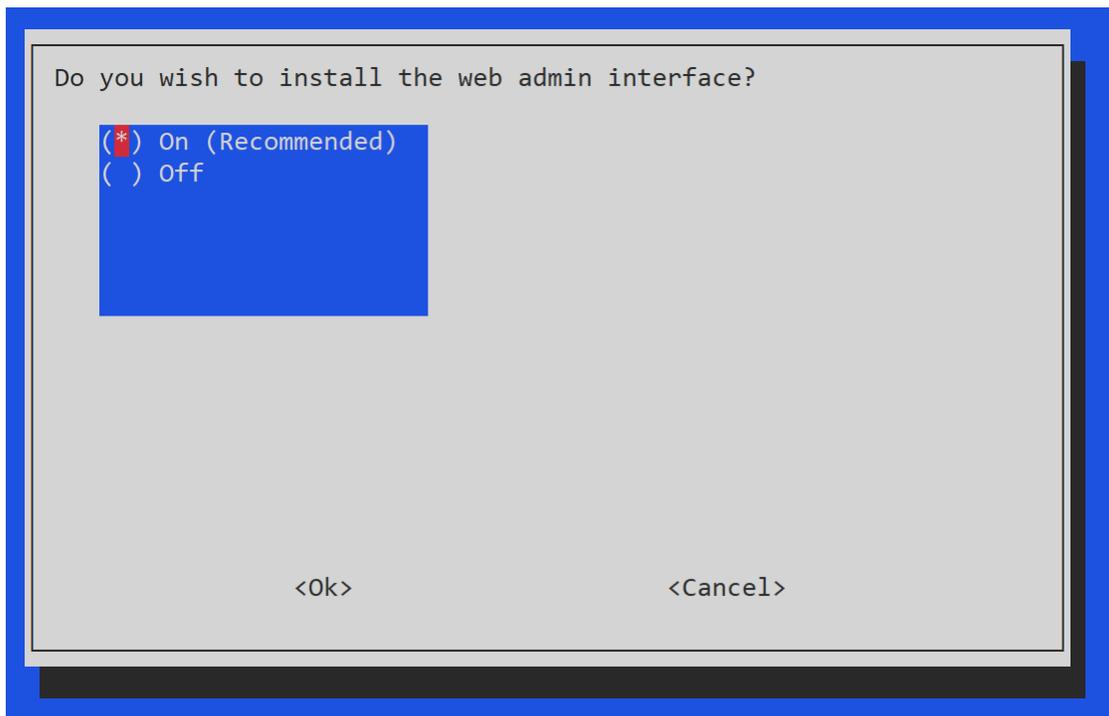
26. When asked which lists to use, I would recommend leaving the default settings as they are and just selecting Ok.



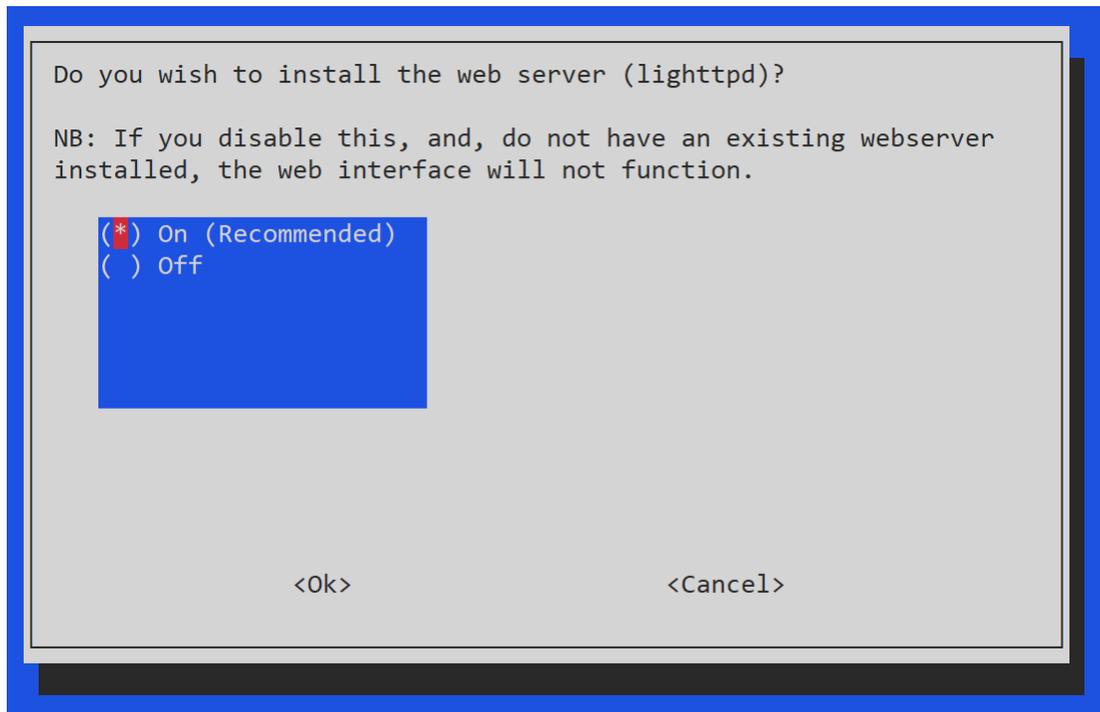
27. Leave the protocols as is.



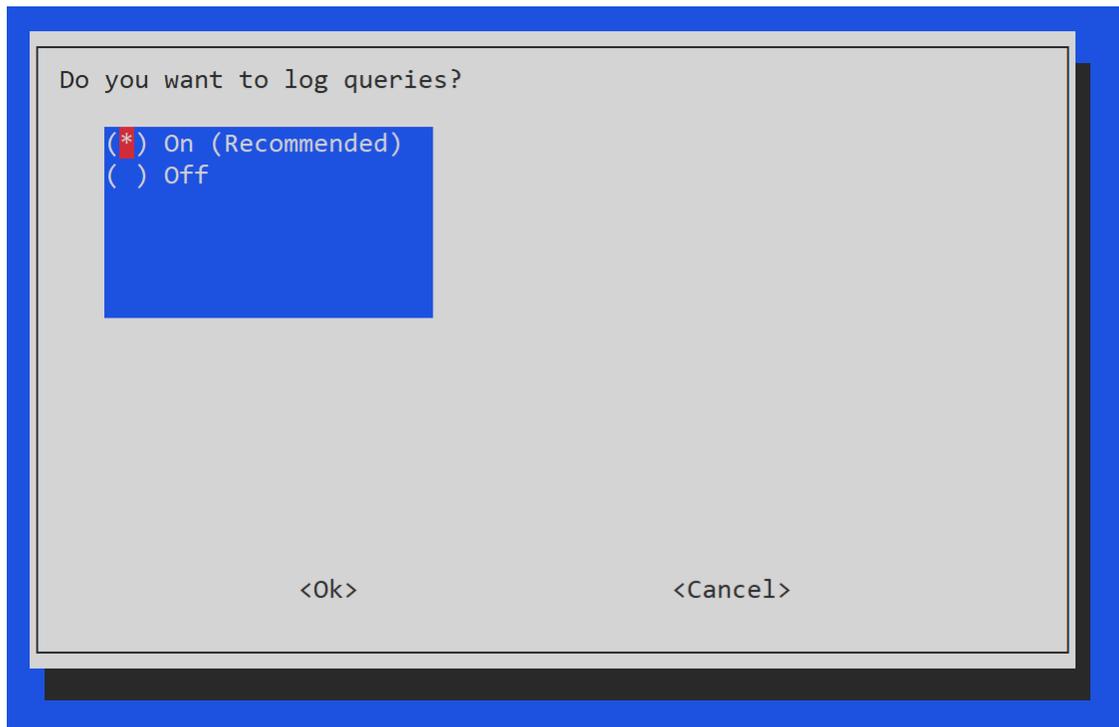
28. Verify that the network settings match what you entered earlier, then select `Yes`.



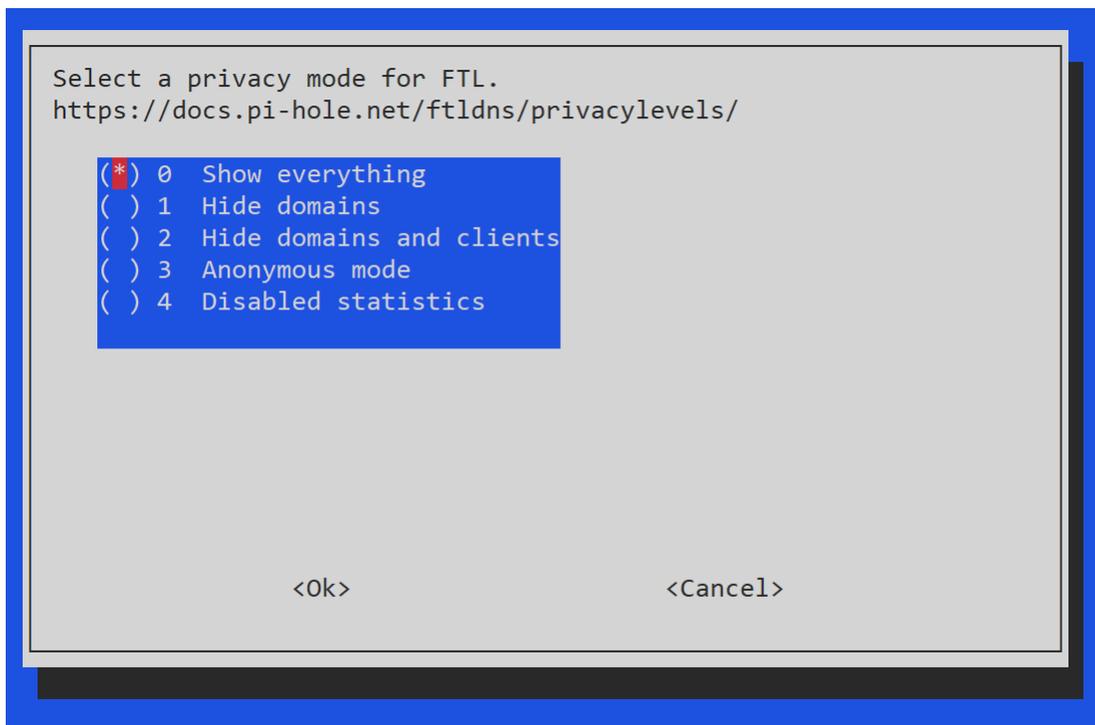
29. Install the web interface.



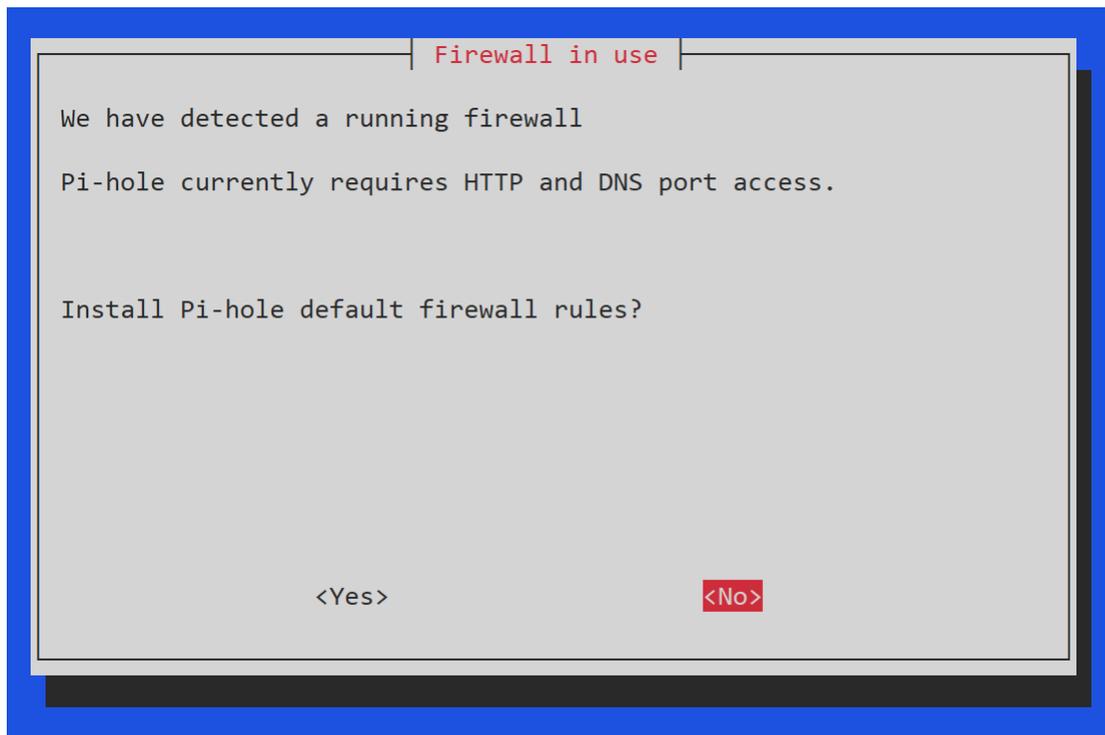
30. Install the web server.



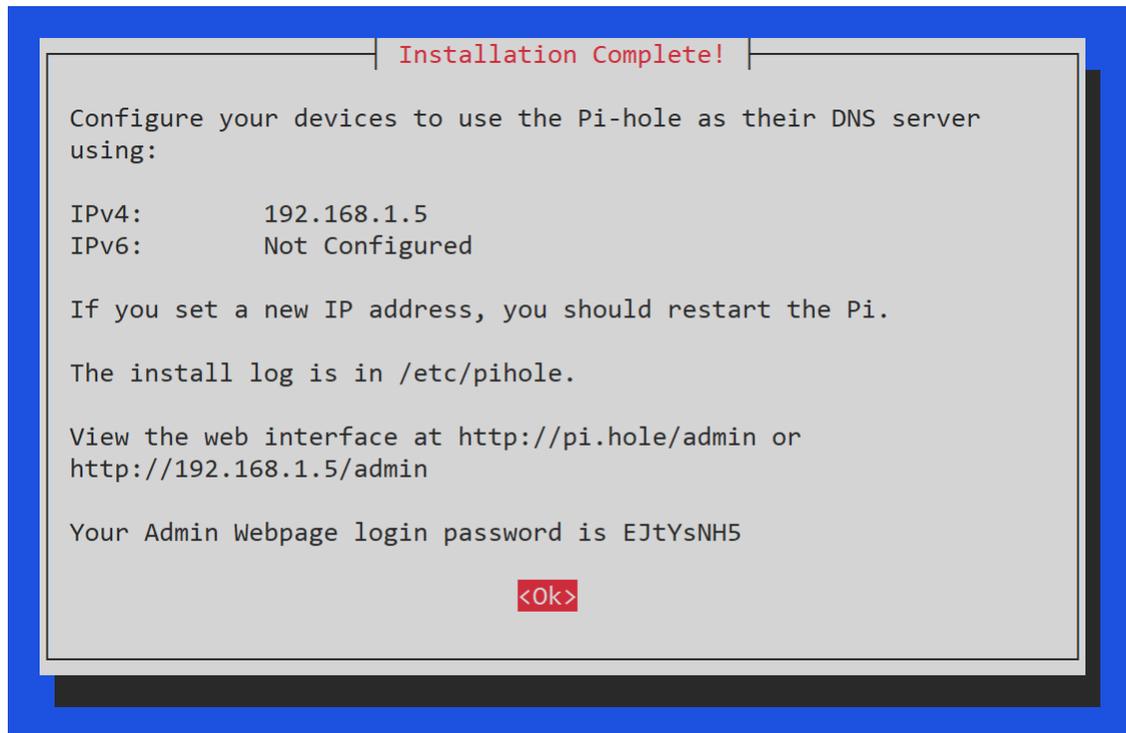
31. Log queries.



32. Select your desired privacy mode (I always select `Show everything`).



33. You already configured the firewall, so select `No` when asked about auto-configuring the firewall.



34. Pay close attention to the Installation Complete screen. The Ipv4 address (the same static IP address that you configured earlier) will be the address for your fancy new Pi-Hole DNS server. You will want to record the admin address (e.g. <http://192.168.1.5/admin>) so that you can log into the admin control panel. Finally, record the admin login password (if you accidentally missed this screen or if you want to change the password, you can set a new password from the command line by entering `pihole -a -p``).
35. Enter the admin control panel address into a web browser on your local network and login.

The screenshot displays the Pi-hole Admin Console interface in a web browser. The browser's address bar shows the URL `192.168.1.5/admin/index.php`. The dashboard features a dark sidebar with navigation options: Dashboard, Query Log, Long term data, Whitelist, Blacklist, Disable, Tools, Network, Settings, Logout, Donate, and Help. The main content area includes a status section with a Raspberry Pi icon and the following metrics: Active (green dot), Temp: 37.9 °C, Load: 0 0.12 0.2, and Memory usage: 11.5%. Below this are four summary cards: 'Total queries (1 clients)' with a value of 28, 'Queries Blocked' with a value of 0, 'Percent Blocked' at 0.0%, and 'Domains on Blocklist' at 113,448. At the bottom, there are two empty line graphs titled 'Queries over last 24 hours' and 'Clients (over time)'.

36. If the status is Active, then congratulations! You have a working Pi-Hole.

Network Setup

Router IP

Local IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 0 . 0 . 0 . 0

Local DNS: 0 . 0 . 0 . 0

Network Address Server Settings (DHCP)

DHCP Type: DHCP Server

DHCP Server: Enable Disable

Start IP Address: 192.168.1. 100

Maximum DHCP Users: 99

Client Lease Expiration: 1440 min

Static DNS 1: 192 . 168 . 1 . 5

Static DNS 2: 1 . 1 . 1 . 1

Static DNS 3: 1 . 0 . 0 . 1

WINS: 0 . 0 . 0 . 0

Use DNSMasq for DNS:

DHCP-Authoritative:

Forced DNS Redirection:

DHCP Server:
Allows the router to manage your IP addresses.

Start IP Address:
The address you would like to start with.

Maximum DHCP Users:
You may limit the number of addresses your router hands out. 0 means only predefined static leases will be handed out.

Time Settings:
Choose the time you are in a summer time (DST) period. The router can use local time or UTC time.

Now that the device is up and running, you can set your internet browser, your operating system, or your network router to use it for all DNS requests. I would recommend that you log into your router and update it to use your Pi-Hole for all DNS requests on the network. This way every device, every browser, every operating system, and every application will use the Pi-Hole for DNS queries.

Enjoy!