

## Setting Up Pi-hole with Tailscale

### Install and Configure Pi-hole

1. Open Terminal and SSH into Pi-hole
  - a. ssh <username>@<hostname>
2. Make sure your Raspberry Pi software packages are up to date:
  1. 6. sudo apt update
  - sudo apt upgrade -y
3. Install the Tailscale client:  

```
curl -fsSL https://tailscale.com/install.sh | sh
```
4. Enable Tailscale and disable automatic DNS settings (since the Raspberry Pi is the DNS server):  

```
sudo tailscale up --accept-dns=false
```
5. Copy the Pi-hole's Tailscale IP address

configuration. [Learn more](#)

The screenshot shows the Pi-hole web interface under the 'DNS' settings. It lists several public DNS servers with their IP addresses: Google Public DNS (8.8.8.8), Cloudflare Public DNS (1.1.1.1), Quad9 Public DNS (9.9.9.9), and Mullvad Public DNS (194.242.2.2). Below this is a section titled 'Override DNS servers' with a lock icon. A red arrow labeled '1' points to the 'Add nameserver' dropdown menu. Another red arrow labeled '2' points to the 'Pi-hole IP' entry field. A third red arrow labeled '3' points to the 'Override DNS servers' toggle switch, which is turned on.

Name	IP Address
Google Public DNS	8.8.8.8
Cloudflare Public DNS	1.1.1.1
Quad9 Public DNS	9.9.9.9
Mullvad Public DNS	194.242.2.2
NextDNS	DoH
Control D	DoH
Custom...	

Add nameserver ▾

Pi-hole IP

Override DNS servers

6. In Pi-hole web interface, go to Settings → DNS → change from Basic to Expert

## DNS Settings

Basic

### Jpstream DNS Servers

IPv4	IPv6	Name		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Google (ECS, DNSSEC)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	OpenDNS (ECS, DNSSEC)
<input type="checkbox"/>	<input type="checkbox"/>			Level3
<input type="checkbox"/>	<input type="checkbox"/>			Comodo
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quad9 (filtered, DNSSEC)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quad9 (unfiltered, no DNSSEC)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Quad9 (filtered, ECS, DNSSEC)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cloudflare (DNSSEC)

 Save & Apply

### Interface settings

#### Recommended setting

##### Allow only local requests

Allows only queries from devices that are at most one hop away (local devices)

#### Potentially dangerous options

Make sure your Pi-hole is properly firewalled!

##### Respond only on interface `wlan0`

##### Bind only to interface `wlan0`

##### Permit all origins

These options are dangerous on devices directly connected to the Internet such as cloud instances and are only safe if your Pi-hole is properly firewalled. In a typical at-home setup where your Pi-hole is located within your local network (and you have not forwarded port 53 in your router!) they are safe to use.

 Save & Apply

See our documentation for further technical details.