Pi-hole

Pi-hole website

Network-wide ad blocking via your own Linux hardware

Pi-hole website | Documentation | Discourse Forum | Donate

Upgrade Notes

> [!CAUTION]
>
> ## !!! THE LATEST VERSION CONTAINS BREAKING CHANGES
>
> **Pi-hole v6 has been entirely redesigned from the ground up and contains many breaking changes.**
>
> Environment variable names have changed, script locations may have changed.
>
> If you are using volumes to persist your configuration, be careful.
> Replacing any `v5` image *(`2024.07.0` and earlier)* with a `v6` image will result in updated configuration files. **These changes are irreversible**.
>
> Please read the README carefully before proceeding.
>
> https://docs.pi-hole.net/docker/

>

> [!NOTE] **Using Watchtower?**
>
> **See the Note on Watchtower at the bottom of this readme.**

> [!TIP] Some users have reported issues with using the `--privileged` flag on `2022.04` and above.
>
> TL;DR, don't use that mode, and be explicit with the permitted caps (if needed) instead.

Quick Start

Using Docker-compose:

1. Copy the below docker compose example and update as needed:

```
# More info at https://github.com/pi-hole/docker-pi-hole/ and https://docs.pi-hole.net/
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    ports:
      # DNS Ports
      - "53:53/tcp"
      - "53:53/udp"
      # Default HTTP Port
      - "80:80/tcp"
      # Default HTTPs Port. FTL will generate a self-signed certificate
      - "443:443/tcp"
      # Uncomment the line below if you are using Pi-hole as your DHCP server
      #- "67:67/udp"
      # Uncomment the line below if you are using Pi-hole as your NTP server
      #- "123:123/udp"
    environment:
      # Set the appropriate timezone for your location
(https://en.wikipedia.org/wiki/List_of_tz_database_time_zones), e.g:
      TZ: 'Europe/London'
      # Set a password to access the web interface. Not setting one will result in a random
```

```
password being assigned
      FTLCONF_webserver_api_password: 'correct horse battery staple'
      # If using Docker's default `bridge` network setting the dns listening mode should be
set to 'all'
      FTLCONF_dns_listeningMode: 'all'
    # Volumes store your data between container upgrades
    volumes:
      # For persisting Pi-hole's databases and common configuration file
      - './etc-pihole:/etc/pihole'
      # Uncomment the below if you have custom dnsmasq config files that you want to persist.
Not needed for most starting fresh with Pi-hole v6. If you're upgrading from v5 you and have
used this directory before, you should keep it enabled for the first v6 container start to
allow for a complete migration. It can be removed afterwards. Needs environment variable
FTLCONF_misc_etc_dnsmasq_d: 'true'
      #- './etc-dnsmasq.d:/etc/dnsmasq.d'
    cap_add:
      # See https://github.com/pi-hole/docker-pi-hole#note-on-capabilities
      # Required if you are using Pi-hole as your DHCP server, else not needed
      - NET_ADMIN
      # Required if you are using Pi-hole as your NTP client to be able to set the host's
system time
      - SYS_TIME
      # Optional, if Pi-hole should get some more processing time
      - SYS_NICE
    restart: unless-stopped
```

2. Run `docker compose up -d` to build and start pi-hole (Syntax may be `docker-compose` on older systems).

> [!NOTE] Volumes are recommended for persisting data across container re-creations for updating images.

Automatic Ad List Updates

`cron` is baked into the container and will grab the newest versions of your lists and flush your logs. This happens once per week in the small hours of Sunday morning.

Running DHCP from Docker Pi-Hole

There are multiple different ways to run DHCP from within your Docker Pi-hole container, but it is slightly more advanced and one size does not fit all.

DHCP and Docker's multiple network modes are covered in detail on our docs site: Docker DHCP and Network Modes.

Configuration

It is recommended that you use environment variables to configure the Pi-hole docker container (more details below), however if you are persisting your `/etc/pihole` directory, you may choose instead to set them via the web interface or by directly editing `pihole.toml`.

> [!WARNING] Settings that are set via environment variables effectively become ***read-only***, meaning that you will not be able to change them in the web interface or CLI. This is to ensure a "single source of truth" on the config.
> If you later unset an environment variable, then FTL will revert to the default value for that setting.

Web interface password

To set a specific password for the web interface, use the environment variable `FTLCONF_webserver_api_password`.

If this variable is not detected and you have not already set one via `pihole setpassword` / `pihole-FTL --config webserver.api.password` inside the container, then a random password will be assigned on startup. This will be printed to the log. Run `docker logs pihole | grep random password` to find it.

To explicitly set no password, set `FTLCONF_webserver_api_password: ''`.

Recommended Environment Variables

Variable	Default	Value	Description
`TZ`	UTC	`<Timezone>`	Set your timezone to make sure logs rotate at local midnight instead of at UTC midnight.

Variable	Default	Value	Description
`FTLCONF_webserver_api_password`	random	`<Admin password>`	http://pi.hole/admin password. Run `docker logs pihole | grep random` to find your random password.
`FTLCONF_dns_upstreams`	`8.8.8.8;8.8.4.4`	IPs delimited by `;`	Upstream DNS server(s) for Pi-hole to forward queries to, separated by a semicolon. Supports non-standard ports with: `#[port number]`, e.g `127.0.0.1#5053;8.8.8.8;8.8.4.4`. Supports Docker service names and links instead of IPs, e.g `upstream0,upstream1` where `upstream0` and `upstream1` are the service names of or links to docker services. **Note:** The existence of this environment variable assumes this as the *sole* management of upstream DNS. Upstream DNS added via the web interface will be overwritten on container restart/recreation.

Optional Variables

Variable	Default	Value	Description
`TAIL_FTL_LOG`	`1`	`<0|1>`	Whether or not to output the FTL log when running the container. Can be disabled by setting the value to 0.

Variable	Default	Value	Description
`FTLCONF_[SETTING]`	unset	As per documentation	Customize pihole.toml with settings described in the API Documentation. Replace `.` with `_`, e.g for `dns.dnssec=true` use `FTLCONF_dns_dnssec: 'true'`. Array type configs should be delimited with `;`.
`PIHOLE_UID`	`1000`	Number	Overrides image's default pihole user id to match a host user id. **IMPORTANT**: id must not already be in use inside the container!
`PIHOLE_GID`	`1000`	Number	Overrides image's default pihole group id to match a host group id. **IMPORTANT**: id must not already be in use inside the container!
`WEBPASSWORD_FILE`	unset	`<Docker secret file>`	Set an Admin password using Docker secrets. If `FTLCONF_webserver_api_password` is set, `WEBPASSWORD_FILE` is ignored. If `FTLCONF_webserver_api_password` is empty, and `WEBPASSWORD_FILE` is set to a valid readable file, then `FTLCONF_webserver_api_password` will be set to the contents of `WEBPASSWORD_FILE`.

Advanced Variables

Variable	Default	Value	Description
`FTL_CMD`	`no-daemon`	`no-daemon -- <dnsmasq option>`	Customize dnsmasq startup options. e.g. `no-daemon --dns-forward-max 300` to increase max. number of concurrent dns queries on high load setups.

Variable	Default	Value	Description
`DNSMASQ_USER`	unset	`<pihole|root>`	Allows changing the user that FTLDNS runs as. Default: `pihole`, some systems such as Synology NAS may require you to change this to `root`. (See #963)
`ADDITIONAL_PACKAGES`	unset	Space separated list of APKs	HERE BE DRAGONS. Mostly for development purposes, this just makes it easier for those of us that always like to have whatever additional tools we need inside the container for debugging.
`FTLCONF_misc_etc_dnsmasq_d`	false	`true|false`	Load custom user configuration files from `/etc/dnsmasq.d/`

Here is a rundown of other arguments for your docker-compose / docker run.

Docker Arguments	Description
`-p <port>:<port>` **Recommended**	Ports to expose (53, 80, 443, 67), the bare minimum ports required for Pi-holes HTTP, HTTPS and DNS services.
`--restart=unless-stopped` **Recommended**	Automatically (re)start your Pi-hole on boot or in the event of a crash.
`-v $(pwd)/etc-pihole:/etc/pihole` **Recommended**	Volumes for your Pi-hole configs help persist changes across docker image updates.
`--net=host` *Optional*	Alternative to `-p <port>:<port>` arguments (Cannot be used at same time as `-p`) if you don't run any other web application. DHCP runs best with `--net=host`, otherwise your router must support dhcp-relay settings.
`--cap-add=NET_ADMIN` *Recommended*	Commonly added capability for DHCP, see Note on Capabilities below for other capabilities.
`--dns=n.n.n.n` *Optional*	Explicitly set container's DNS server. It is ***not recommended*** to set this to `localhost` / `127.0.0.1`.
`--env-file .env` *Optional*	File to store environment variables for docker replacing `-e key=value` settings. Here for convenience.

Tips and Tricks

- A good way to test things are working right is by loading this page: http://pi.hole/admin/

- Port conflicts? Stop your server's existing DNS / Web services.
  - Don't forget to stop your services from auto-starting again after you reboot.
  - Ubuntu users see below for more detailed information.
- Docker's default network mode `bridge` isolates the container from the host's network. This is a more secure setting, but requires setting the Pi-hole DNS option for *Interface listening behavior* to "Listen on all interfaces, permit all origins".
- If you're using a Red Hat based distribution with an SELinux Enforcing policy, add `:z` to line with volumes.

Installing on Ubuntu or Fedora

Modern releases of Ubuntu (17.10+) and Fedora (33+) include `systemd-resolved` which is configured by default to implement a caching DNS stub resolver. This will prevent pi-hole from listening on port 53. The stub resolver should be disabled with: `sudo sed -r -i.orig 's/#?DNSStubListener=yes/DNSStubListener=no/g' /etc/systemd/resolved.conf`.

This will not change the nameserver settings, which point to the stub resolver thus preventing DNS resolution. Change the `/etc/resolv.conf` symlink to point to `/run/systemd/resolve/resolv.conf`, which is automatically updated to follow the system's `netplan`: `sudo sh -c 'rm /etc/resolv.conf && ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf'`. After making these changes, you should restart systemd-resolved using `systemctl restart systemd-resolved`.

Once pi-hole is installed, you'll want to configure your clients to use it (see here). If you used the symlink above, your docker host will either use whatever is served by DHCP, or whatever static setting you've configured. If you want to explicitly set your docker host's nameservers you can edit the netplan(s) found at `/etc/netplan`, then run `sudo netplan apply`.

Example netplan:

```
network:
    ethernets:
        ens160:
            dhcp4: true
            dhcp4-overrides:
                use-dns: false
            nameservers:
                addresses: [127.0.0.1]
    version: 2
```

Note that it is also possible to disable `systemd-resolved` entirely. However, this can cause problems with name resolution in vpns (see bug report).
It also disables the functionality of netplan since systemd-resolved is used as the default renderer (see `man netplan`).

If you choose to disable the service, you will need to manually set the nameservers, for example by creating a new `/etc/resolv.conf`.

Users of older Ubuntu releases (circa 17.04) will need to disable dnsmasq.

Installing on Dokku

@Rikj000 has produced a guide to assist users installing Pi-hole on Dokku.

Docker tags and versioning

The primary docker tags are explained in the following table. Click here to see the full list of tags.

See GitHub Release notes to see the specific version of Pi-hole Core, Web, and FTL included in the release.

The Date-based (including incremented "Patch" versions) do not relate to any kind of semantic version number, rather a date is used to differentiate between the new version and the old version, nothing more.

Release notes will always contain full details of changes in the container, including changes to core Pi-hole components.

tag	description
`latest`	Always latest release
`2022.04.0`	Date-based release
`2022.04.1`	Second release in a given month
`development`	Similar to `latest`, but for the development branch (pushed occasionally)
`*beta`	Early beta releases of upcoming versions - here be dragons
`nightly`	Like `development` but pushed every night and pulls from the latest `development` branches of the core Pi-hole components (Pi-hole, web, FTL)

Upgrading, Persistence, and Customizations

The standard Pi-hole customization abilities apply to this docker, but with docker twists such as using docker volume mounts to map host stored file configurations over the container defaults. However, mounting these configuration files as read-only should be avoided. Volumes are also important to persist the configuration in case you have removed the Pi-hole container which is a typical docker upgrade pattern.

Upgrading / Reconfiguring

Do not attempt to upgrade (`pihole -up`) or reconfigure (`pihole -r`).

New images will be released for upgrades, upgrading by replacing your old container with a fresh upgraded image is the 'docker way'. Long-living docker containers are not the docker way since they aim to be portable and reproducible, why not re-create them often! Just to prove you can.

0. Read the release notes for both this Docker release and the Pi-hole release
    - This will help you avoid common problems due to any known issues with upgrading or newly required arguments or variables
    - We will try to put common break/fixes at the top of this readme too
1. Download the latest version of the image: `docker pull pihole/pihole`
2. Throw away your container: `docker rm -f pihole`
    - **Warning:** When removing your pihole container you may be stuck without DNS until step 3; `docker pull` before `docker rm -f` to avoid DNS interruption.
    - If you care about your data (logs/customizations), make sure you have it volume-mapped or it will be deleted in this step.
3. Start your container with the newer base image: `docker run <args> pihole/pihole` (`<args>` being your preferred run volumes and env vars)

Why is this style of upgrading good?

A couple reasons:

- Everyone is starting from the same base image which has been tested to known it works.
- No worrying about upgrading from A to B, B to C, or A to C is required when rolling out updates, it reduces complexity, and simply allows a 'fresh start' every time while preserving customizations with volumes.
- Basically I'm encouraging phoenix server principles for your containers.

To reconfigure Pi-hole you'll either need to use an existing container environment variables or, if there is no a variable for what you need, use the web UI or CLI commands.

Building the image locally

Occasionally you may need to try an alternative branch of one of the components (`core`, `web`, `ftl`). On bare metal you would run, for example, `pihole checkout core custombranchname`, however in Docker world we have disabled this command as it can cause unpredictable results.

The preferred method is to clone this repository and build the image locally with `./build.sh`.

Usage:

```
./build.sh [-l] [-f <ftl_branch>] [-c <core_branch>] [-w <web_branch>] [-p <padd_branch>] [-t <tag>] [use_cache]
```

Options:

- `-f <branch>` / `--ftlbranch <branch>`: Specify FTL branch (cannot be used in conjunction with `-l`)
- `-c <branch>` / `--corebranch <branch>`: Specify Core branch
- `-w <branch>` / `--webbranch <branch>`: Specify Web branch
- `-p <branch>` / `--paddbranch <branch>`: Specify PADD branch
- `-t <tag>` / `--tag <tag>`: Specify Docker image tag (default: `pihole:local`)
- `-l` / `--local`: Use locally built FTL binary (requires `src/pihole-FTL` file)
- `use_cache`: Enable caching (by default `--no-cache` is used)

If no options are specified, the following command will be executed:

```
docker buildx build src/. --tag pihole:local --no-cache
```

Pi-hole features

Here are some relevant wiki pages from Pi-hole's documentation.

We install all pihole utilities so the the built in pihole commands will work via `docker exec <container> <command>` like so:

- `docker exec pihole_container_name pihole updateGravity`
- `docker exec pihole_container_name pihole -w spclient.wg.spotify.com`
- `docker exec pihole_container_name pihole -wild example.com`

Customizations

The webserver and DNS service inside the container can be customized if necessary. Any configuration files you volume mount into `/etc/dnsmasq.d/` will be loaded by pihole-FTL when the container starts or restarts.

Note on Capabilities

Pi-hole's DNS core (FTL) expects to have the following capabilities available:

- `CAP_NET_BIND_SERVICE`: Allows FTLDNS binding to TCP/UDP sockets below 1024 (specifically DNS service on port 53)
- `CAP_NET_RAW`: use raw and packet sockets (needed for handling DHCPv6 requests, and verifying that an IP is not in use before leasing it)
- `CAP_NET_ADMIN`: modify routing tables and other network-related operations (in particular inserting an entry in the neighbor table to answer DHCP requests using unicast packets)
- `CAP_SYS_NICE`: FTL sets itself as an important process to get some more processing time if the latter is running low
- `CAP_CHOWN`: we need to be able to change ownership of log files and databases in case FTL is started as a different user than `pihole`
- `CAP_SYS_TIME`: FTL needs to be able to set the system time to update it using the Network Time Protocol (NTP) in the background

This image automatically grants those capabilities, if available, to the FTLDNS process, even when run as non-root.
By default, docker does not include the `NET_ADMIN` capability for non-privileged containers, and it is recommended to explicitly add it to the container using `--cap-add=NET_ADMIN`.
However, if DHCP and IPv6 Router Advertisements are not in use, it should be safe to skip it. For the most paranoid, it should even be possible to explicitly drop the `NET_RAW` capability to prevent FTLDNS from automatically gaining it.

Note on Watchtower

We have noticed that a lot of people use Watchtower to keep their Pi-hole containers up to date. For the same reason we don't provide an auto-update feature on a bare metal install, you *should not* have a system automatically update your Pi-hole container. Especially unattended. As much as we try to ensure nothing will go wrong, sometimes things do go wrong - and you need to set aside time to *manually* pull and update to the version of the container you wish to run. The upgrade process should be along the lines of:

- **Important**: Read the release notes. Sometimes you will need to make changes other than just updating the image.
- Pull the new image.
- Stop and *remove* the running Pi-hole container
  - If you care about your data (logs/customizations), make sure you have it volume-mapped or it will be deleted in this step.
- Recreate the container using the new image.

Pi-hole is an integral part of your network, don't let it fall over because of an unattended update in the middle of the night.

Revision #3
Created 2025-03-13 06:02:12 UTC by Johan Odendaal
Updated 2025-03-13 06:45:24 UTC by Johan Odendaal