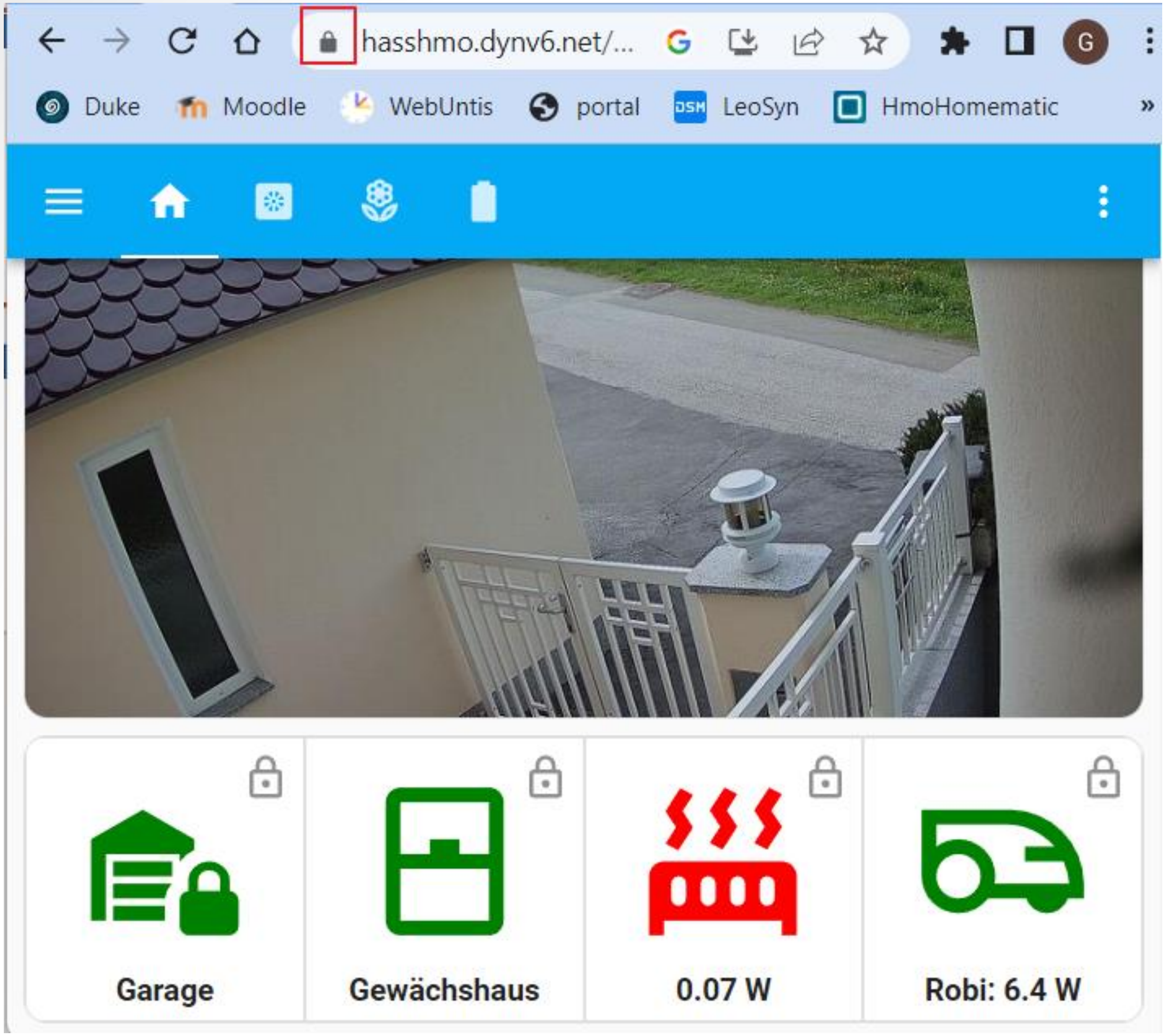


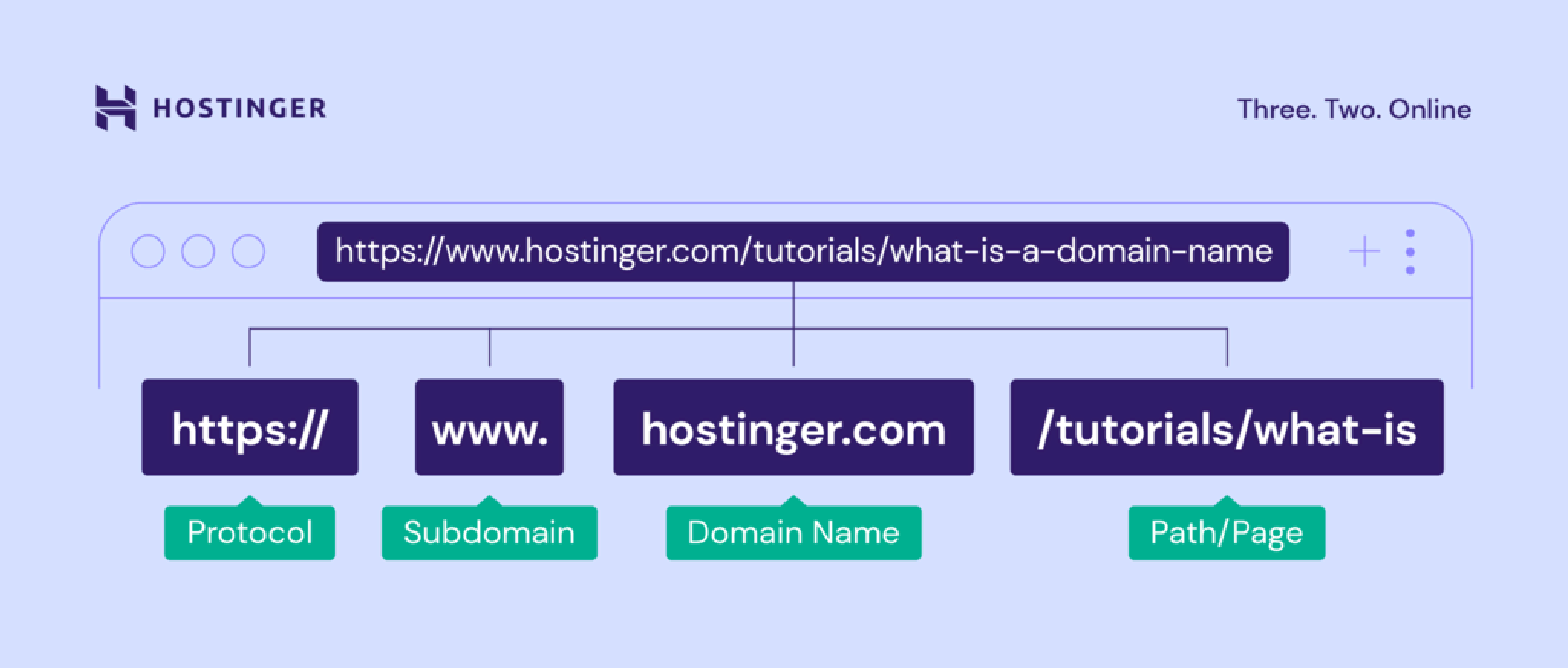
Garage

Gewächshaus

0.07 W

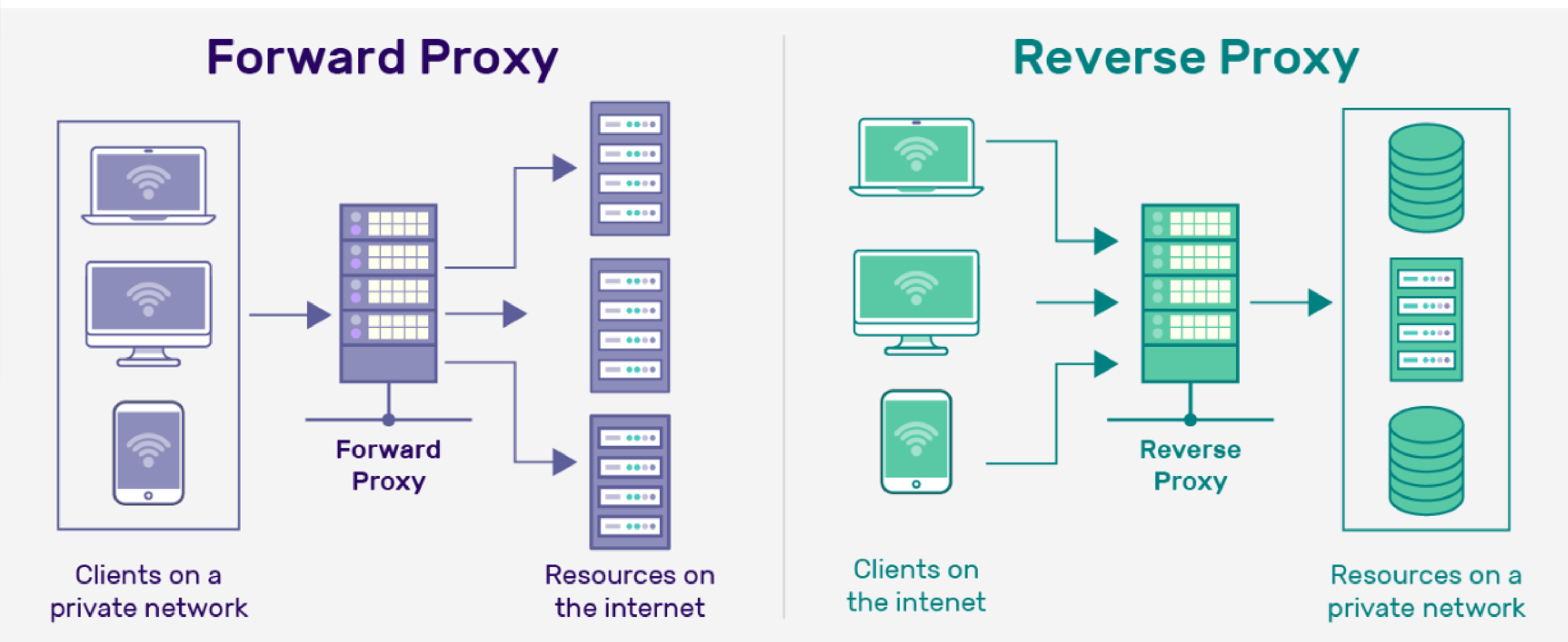
Robi: 6.4 W

Begriffsbestimmungen



Proxies

- https://securityboulevard.com/2023/04/what-is-reverse-proxy-how-does-it-works-and-what-are-its-benefits/

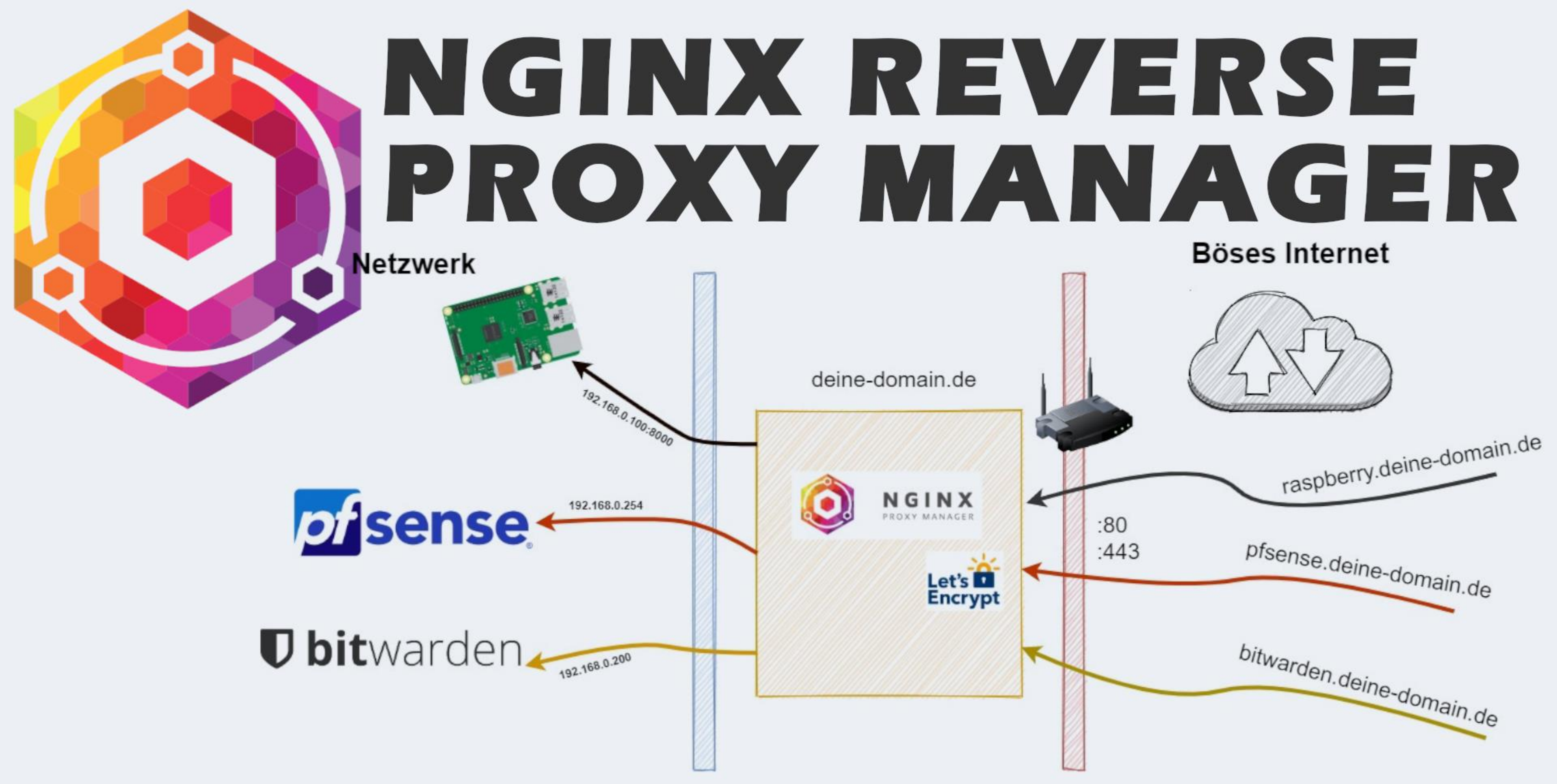

Forward Proxy
Reverse Proxy
Forward Proxy
Clients on a private network
Resources on the internet
Reverse Proxy
Clients on the intenet
Resources on a private network

Möglichkeiten mit Reverse-Proxy

- Https-Verkehr zu Remote-Proxy schicken ➔ verteilt auf die internen Hosts
  - Routing nach
    - Domain
    - Subdomain
    - Port
    - Path
- Einfachste Variante: Eigene Domain für jeden Host
  - Vereinfacht erweiterte Möglichkeiten
    - Websockets, …

Typisches IoT-Szenario

- https://schroederdennis.de/allgemein/nginx-proxy-manager-nginx-reverse-proxy-vorgestellt/

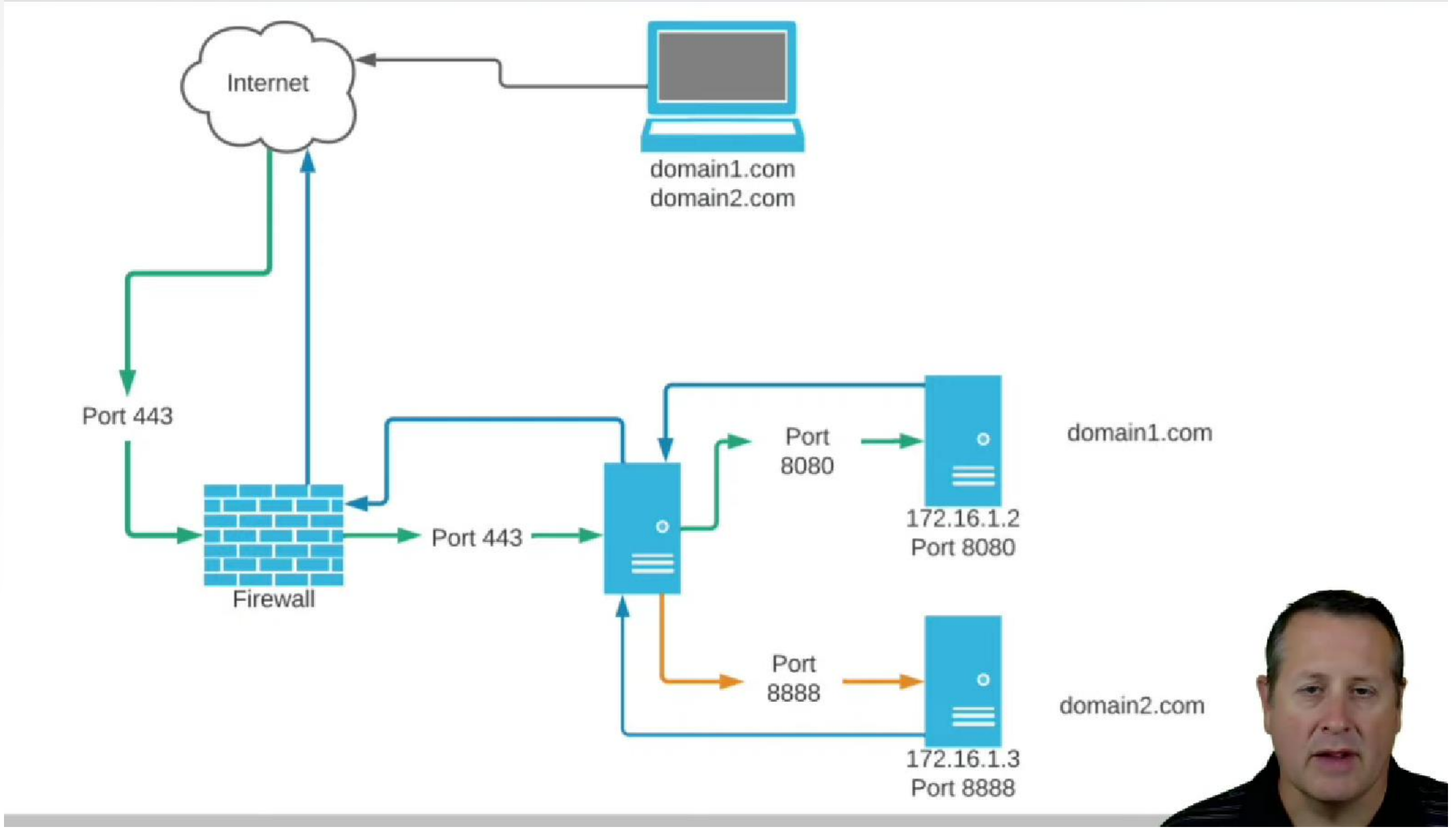


Umsetzung

- Selbst ist der Mann
  - Installation Nginx
  - Installation Certbot
  - Konfiguration über Config-Files
- Bequemer über UI-gestützen Manager
  - Nginx Reverse Proxy Manager
  - Eigenes AddOn in HA

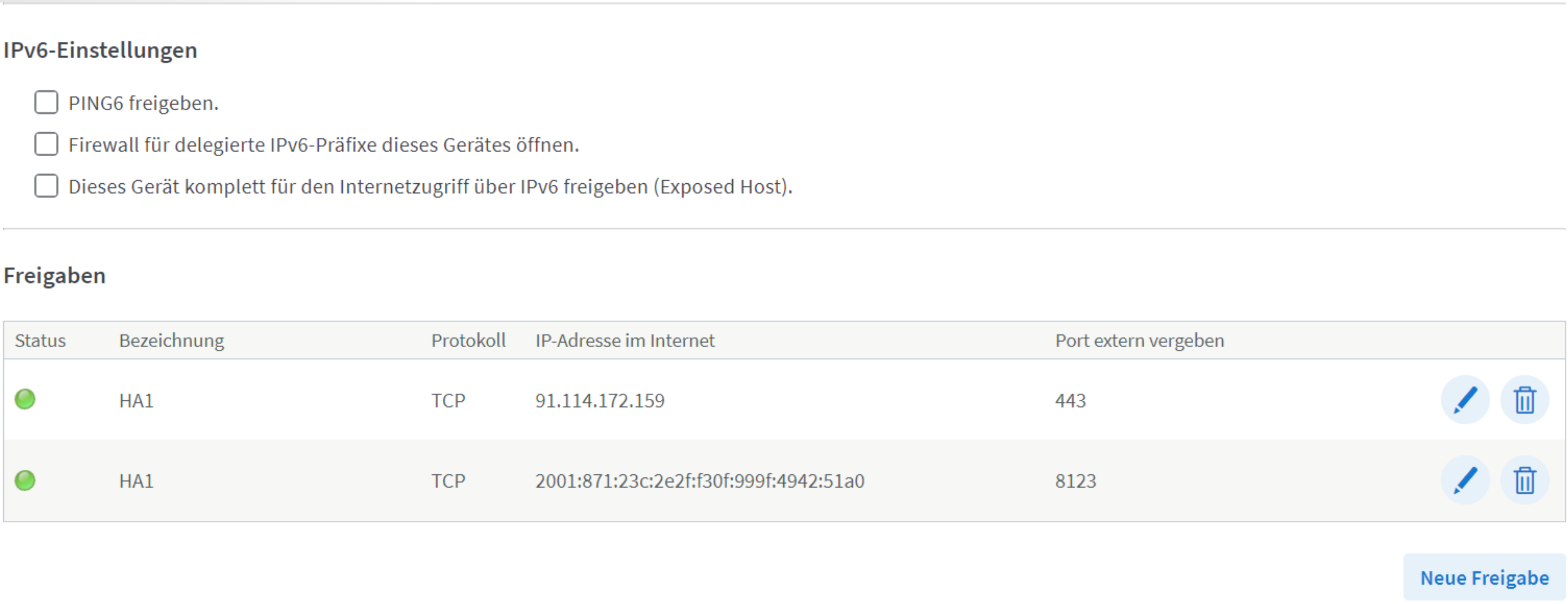
Nginx Reverse Proxy Manager

- https://www.youtube.com/watch?v=CSbgLBcIuwE&ab_channel=mostlychris



In Router Port 80 und 443 umleiten

- Alte Config sichern



IPv6-Einstellungen

□ PING6 freigeben.

□ Firewall für delegierte IPv6-Präfixe dieses Gerätes öffnen.

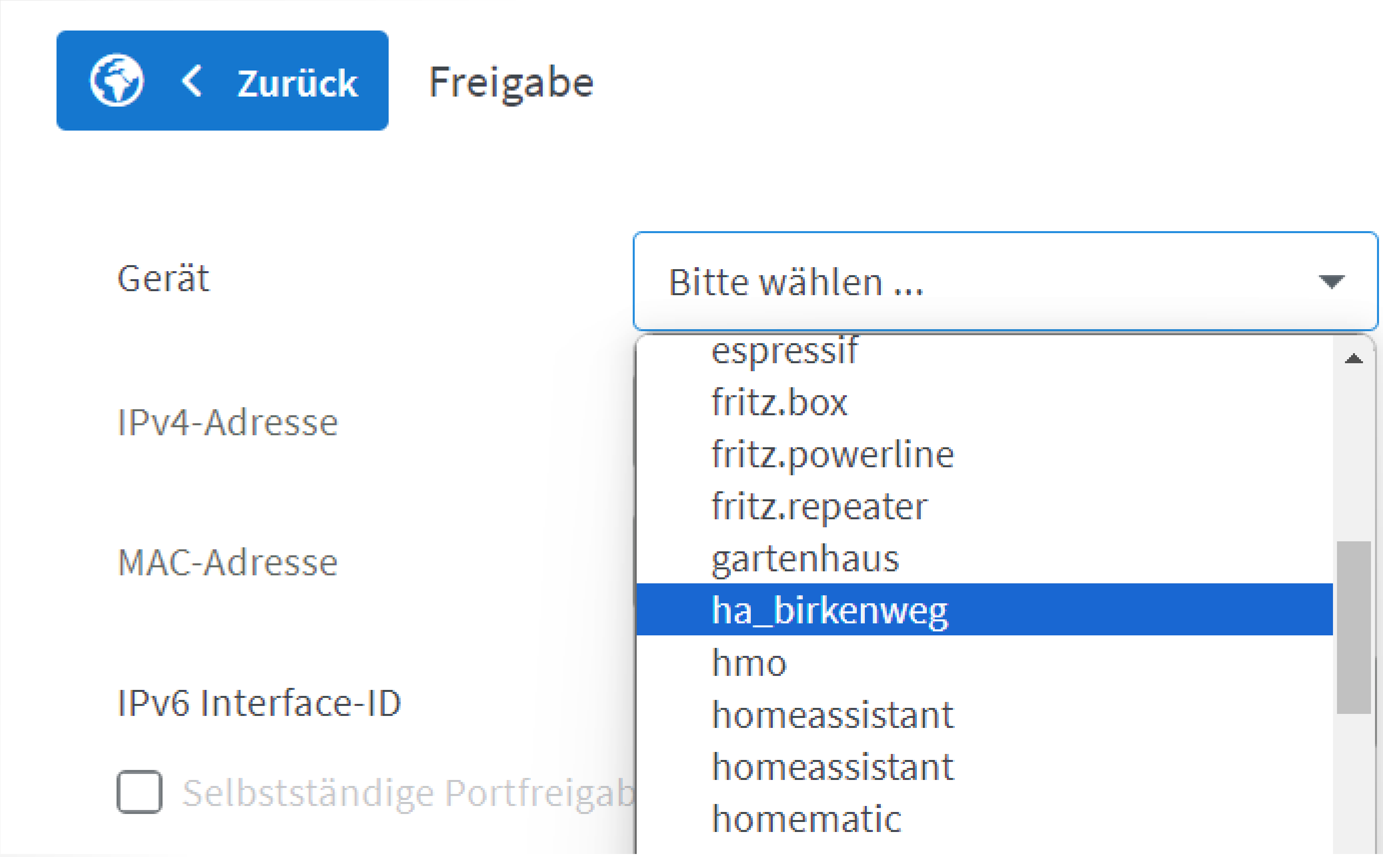
□ Dieses Gerät komplett für den Internetzugriff über IPv6 freigeben (Exposed Host).

Freigaben

Status	Bezeichnung	Protokoll	IP-Adresse im Internet	Port extern vergeben
●	HA1	TCP	91.114.172.159	443
●	HA1	TCP	2001:871:23c:2e2f:f30f:999f:4942:51a0	8123

Gerät sprechend benennen

- In Heimnetz



Freigabe

Gerät: Bitte wählen ...

espressif
fritz.box
fritz.powerline
fritz.repeater
gartenhaus
ha_birkenweg
hmo
homeassistant
homeassistant
homematic

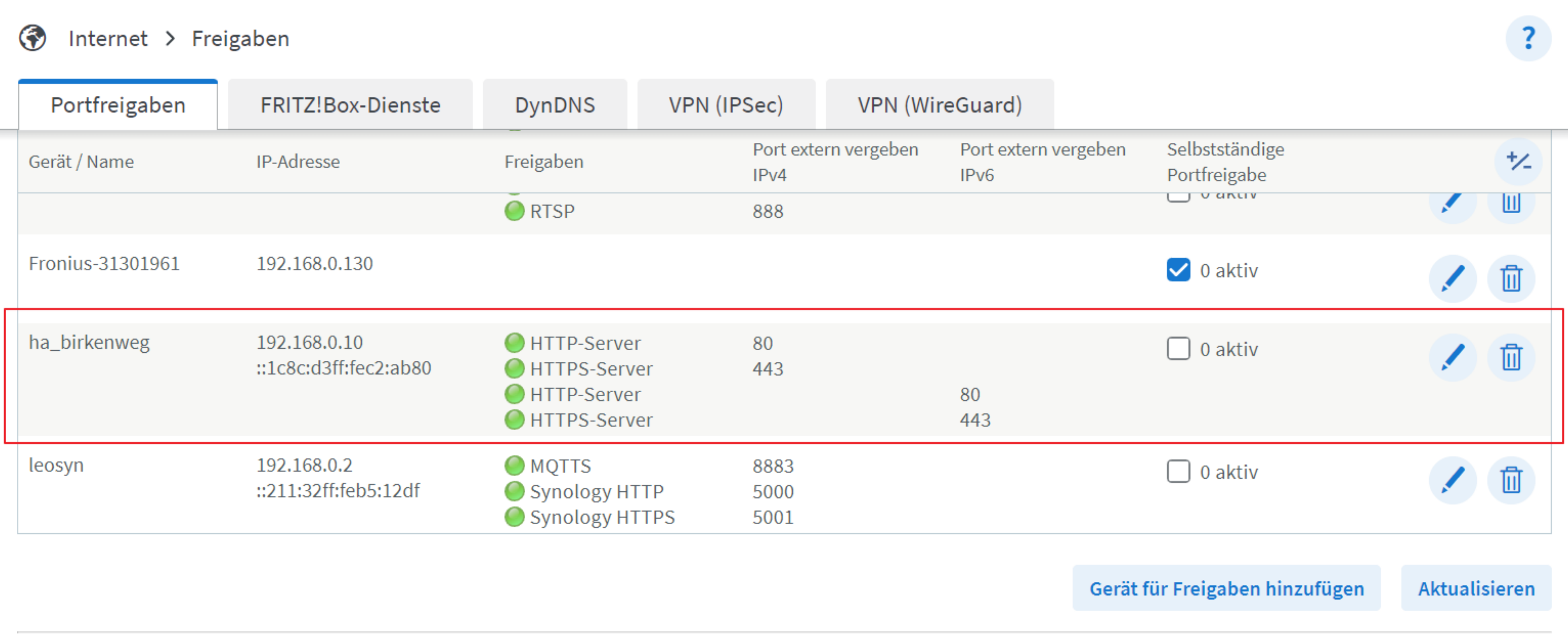
IPv4-Adresse

MAC-Adresse

IPv6 Interface-ID

□ Selbstständige Portfreigab

Kontrolle

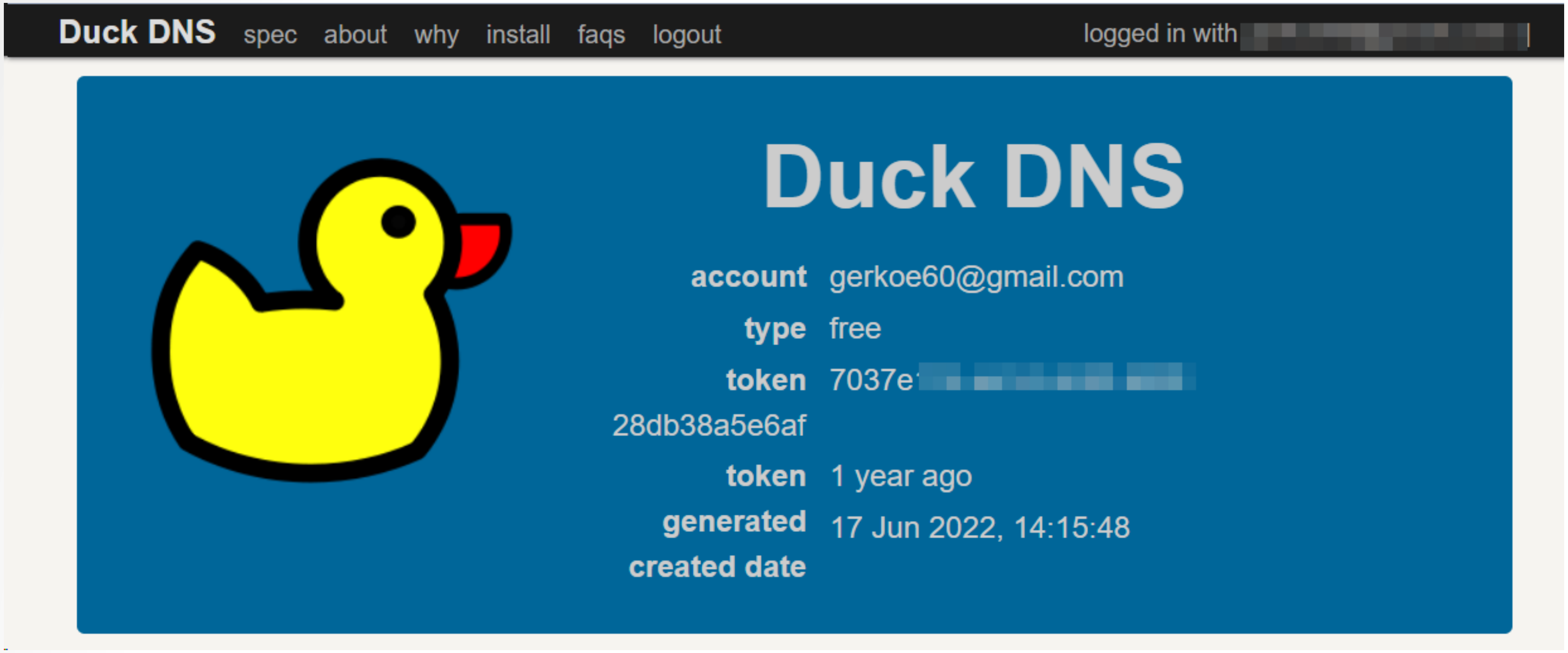


Internet > Freigaben

Gerät / Name	IP-Adresse	Freigaben	Port extern vergeben IPv4	Port extern vergeben IPv6	Selbstständige Portfreigabe
		🟢 RTSP	888		☐ 0 aktiv
Fronius-31301961	192.168.0.130				☑ 0 aktiv
ha_birkenweg	192.168.0.10 ::1c8c:d3ff:fec2:ab80	🟢 HTTP-Server 🟢 HTTPS-Server 🟢 HTTP-Server 🟢 HTTPS-Server	80 443	 80 443	☐ 0 aktiv
leosyn	192.168.0.2 ::211:32ff:feb5:12df	🟢 MQTTS 🟢 Synology HTTP 🟢 Synology HTTPS	8883 5000 5001		☐ 0 aktiv

Domain aus dem Internet erreichbar

- Verfügbares AddOn DuckDns
- Mit Google-Account registrieren/anmelden
- Domain anlegen



account gerkoe60@gmail.com

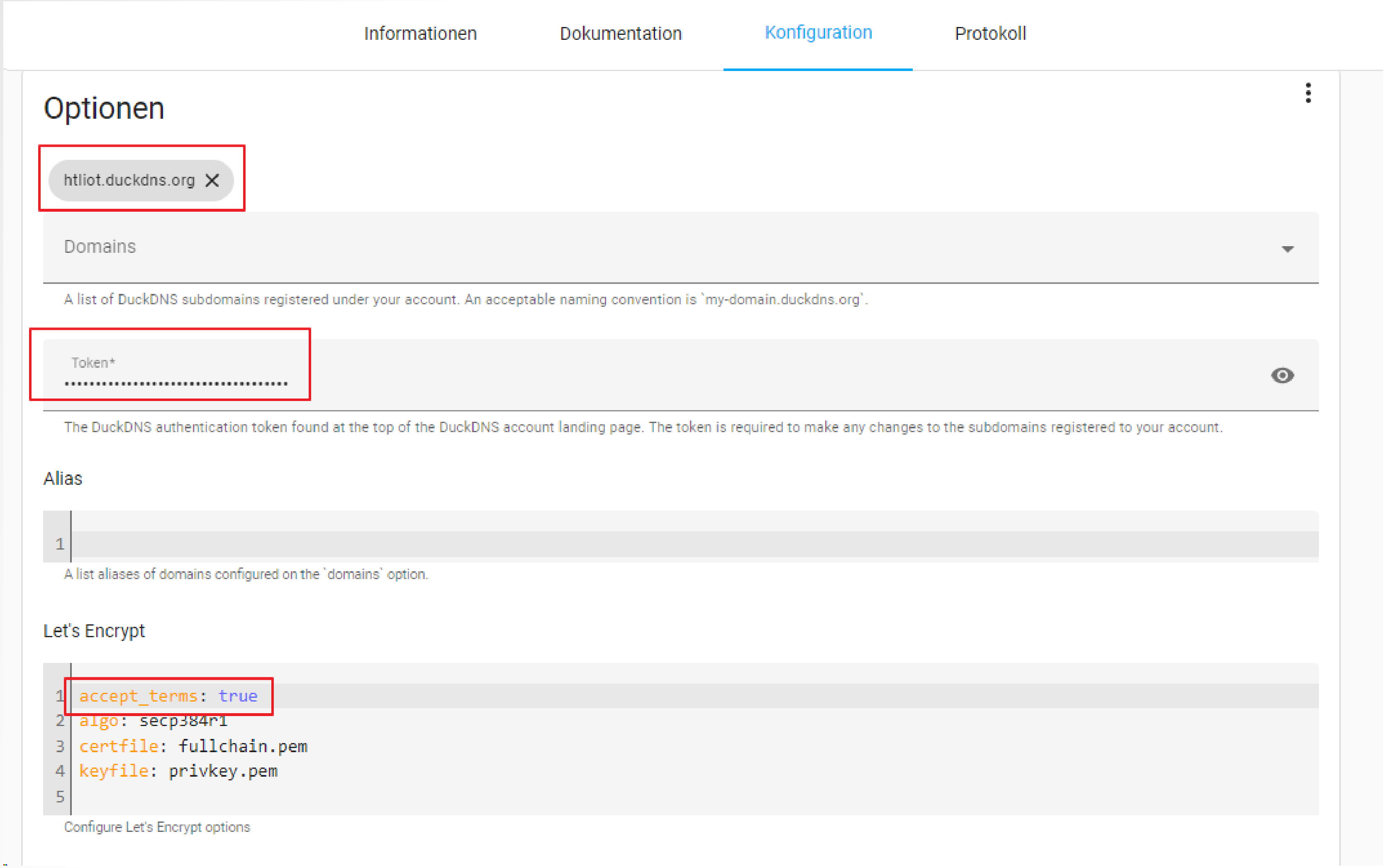
type free

token 7037e[redacted]28db38a5e6af

token generated 1 year ago

created date 17 Jun 2022, 14:15:48

DuckDns konfigurieren



Optionen

htliot.duckdns.org ✕

Domains

A list of DuckDNS subdomains registered under your account. An acceptable naming convention is `my-domain.duckdns.org`.

Token*
••••••••••••••••••••••••••••••••••••••

The DuckDNS authentication token found at the top of the DuckDNS account landing page. The token is required to make any changes to the subdomains registered to your account.

Alias

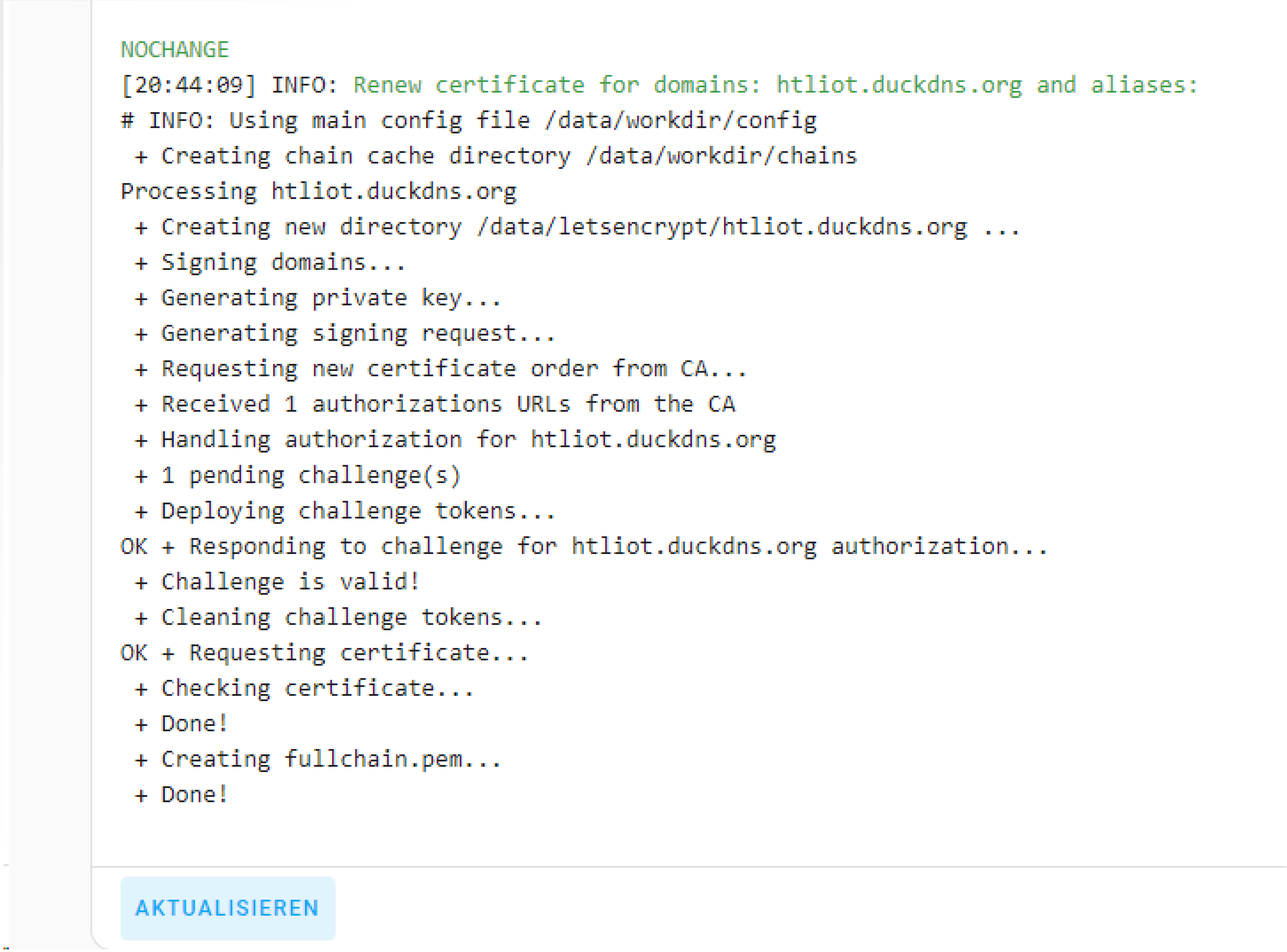
A list aliases of domains configured on the `domains` option.

Let's Encrypt

```
accept_terms: true
algo: secp384r1
certfile: fullchain.pem
keyfile: privkey.pem
```

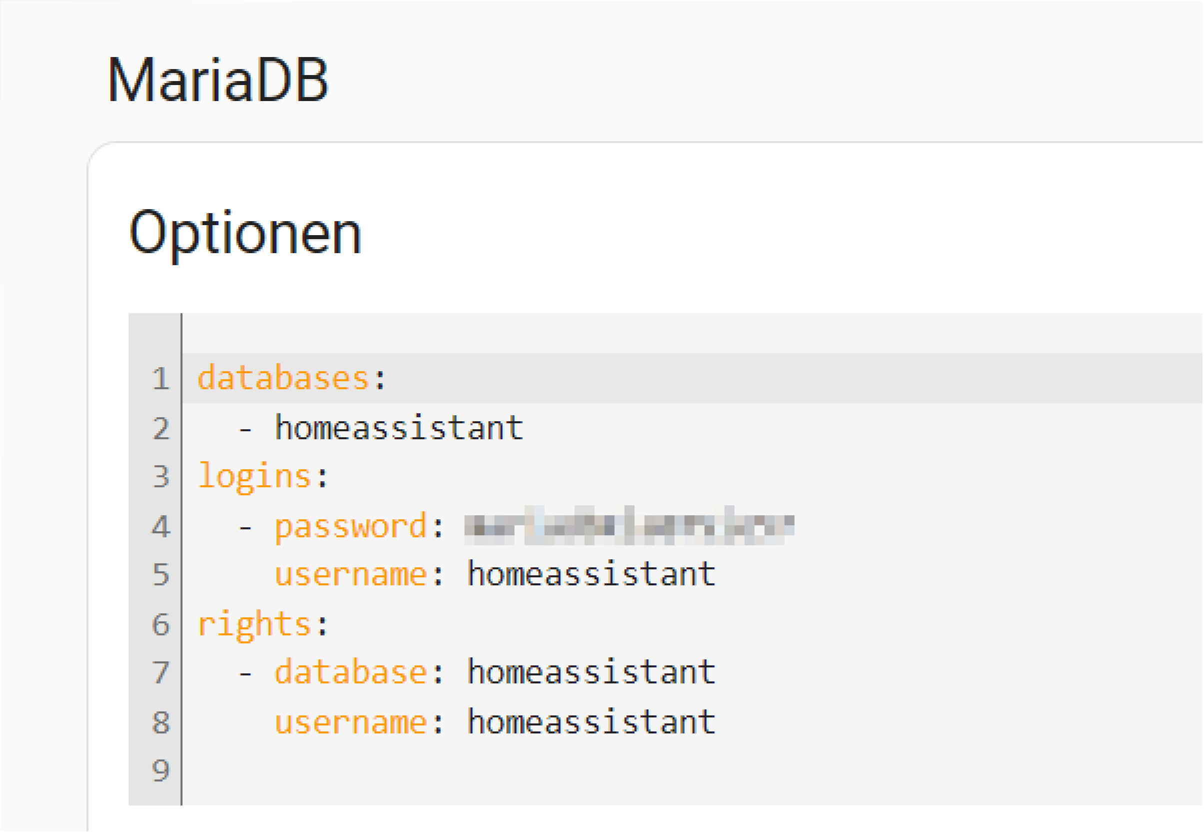
Configure Let's Encrypt options

Kontrolle Log



```
NOCHANGE
[20:44:09] INFO: Renew certificate for domains: htliot.duckdns.org and aliases:
# INFO: Using main config file /data/workdir/config
 + Creating chain cache directory /data/workdir/chains
Processing htliot.duckdns.org
 + Creating new directory /data/letsencrypt/htliot.duckdns.org ...
 + Signing domains...
 + Generating private key...
 + Generating signing request...
 + Requesting new certificate order from CA...
 + Received 1 authorizations URLs from the CA
 + Handling authorization for htliot.duckdns.org
 + 1 pending challenge(s)
 + Deploying challenge tokens...
OK + Responding to challenge for htliot.duckdns.org authorization...
 + Challenge is valid!
 + Cleaning challenge tokens...
OK + Requesting certificate...
 + Checking certificate...
 + Done!
 + Creating fullchain.pem...
 + Done!
```

Vorbedingung: AddOn MariaDB

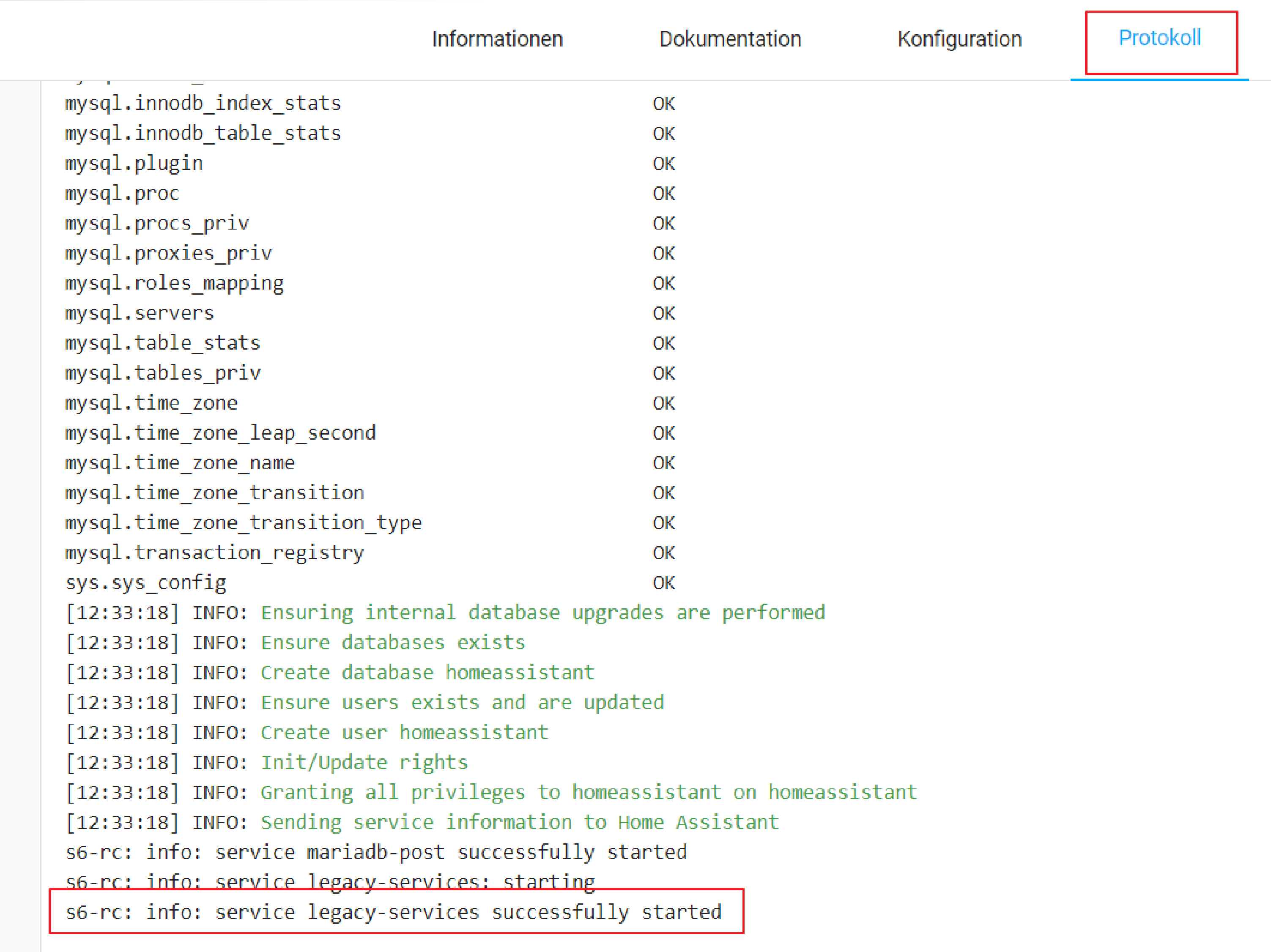


MariaDB

Optionen

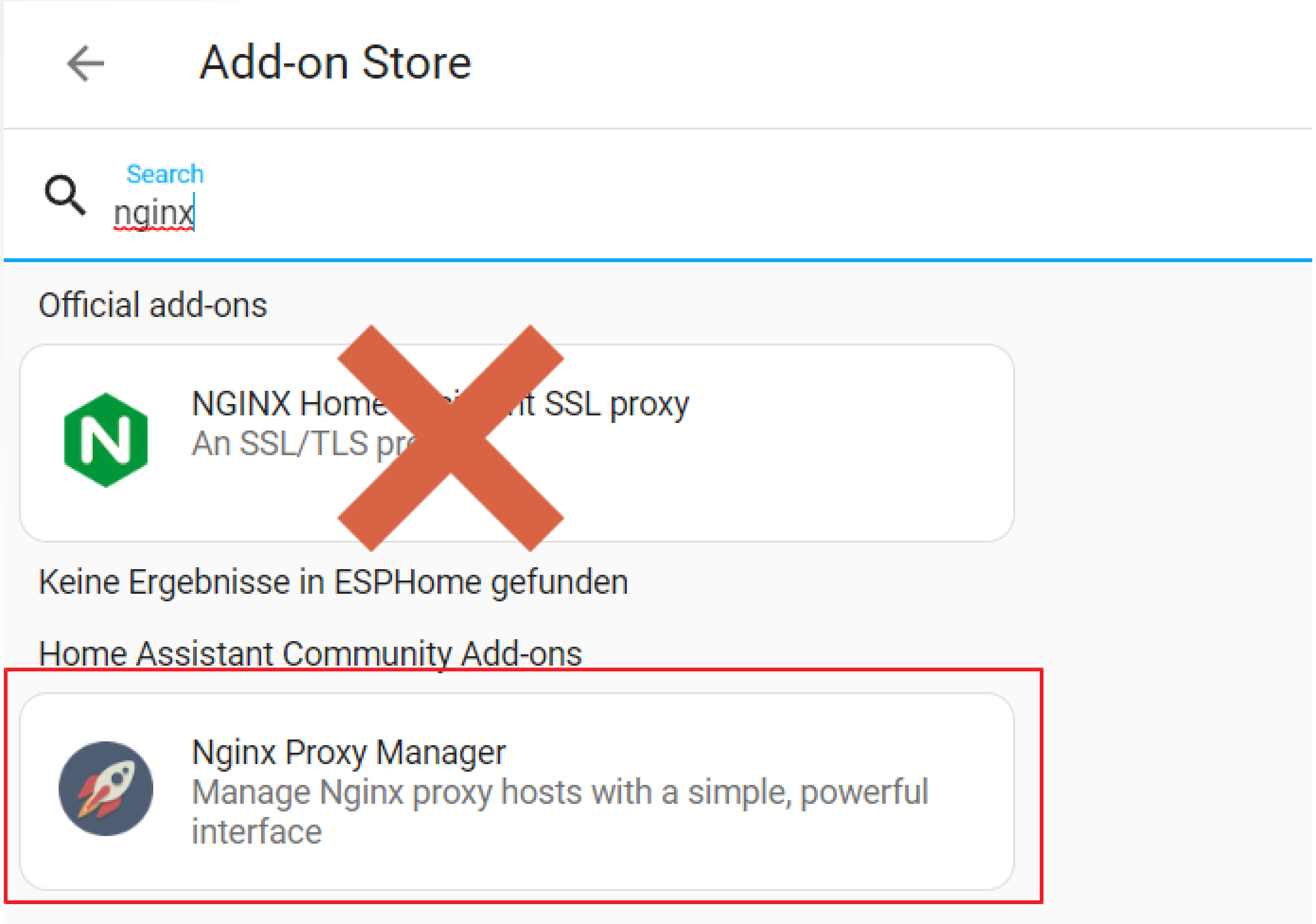
```yaml
databases:
  - homeassistant
logins:
  - password: [redacted]
    username: homeassistant
rights:
  - database: homeassistant
    username: homeassistant

```

Kontrolle



```
mysql.innodb_index_stats                          OK
mysql.innodb_table_stats                          OK
mysql.plugin                                      OK
mysql.proc                                        OK
mysql.procs_priv                                  OK
mysql.proxies_priv                                OK
mysql.roles_mapping                               OK
mysql.servers                                     OK
mysql.table_stats                                 OK
mysql.tables_priv                                 OK
mysql.time_zone                                   OK
mysql.time_zone_leap_second                       OK
mysql.time_zone_name                              OK
mysql.time_zone_transition                        OK
mysql.time_zone_transition_type                   OK
mysql.transaction_registry                        OK
sys.sys_config                                    OK
[12:33:18] INFO: Ensuring internal database upgrades are performed
[12:33:18] INFO: Ensure databases exists
[12:33:18] INFO: Create database homeassistant
[12:33:18] INFO: Ensure users exists and are updated
[12:33:18] INFO: Create user homeassistant
[12:33:18] INFO: Init/Update rights
[12:33:18] INFO: Granting all privileges to homeassistant on homeassistant
[12:33:18] INFO: Sending service information to Home Assistant
s6-rc: info: service mariadb-post successfully started
s6-rc: info: service legacy-services: starting
s6-rc: info: service legacy-services successfully started
```

Nginx Proxy Manager installieren



Add-on Store

Search

nginx

Official add-ons

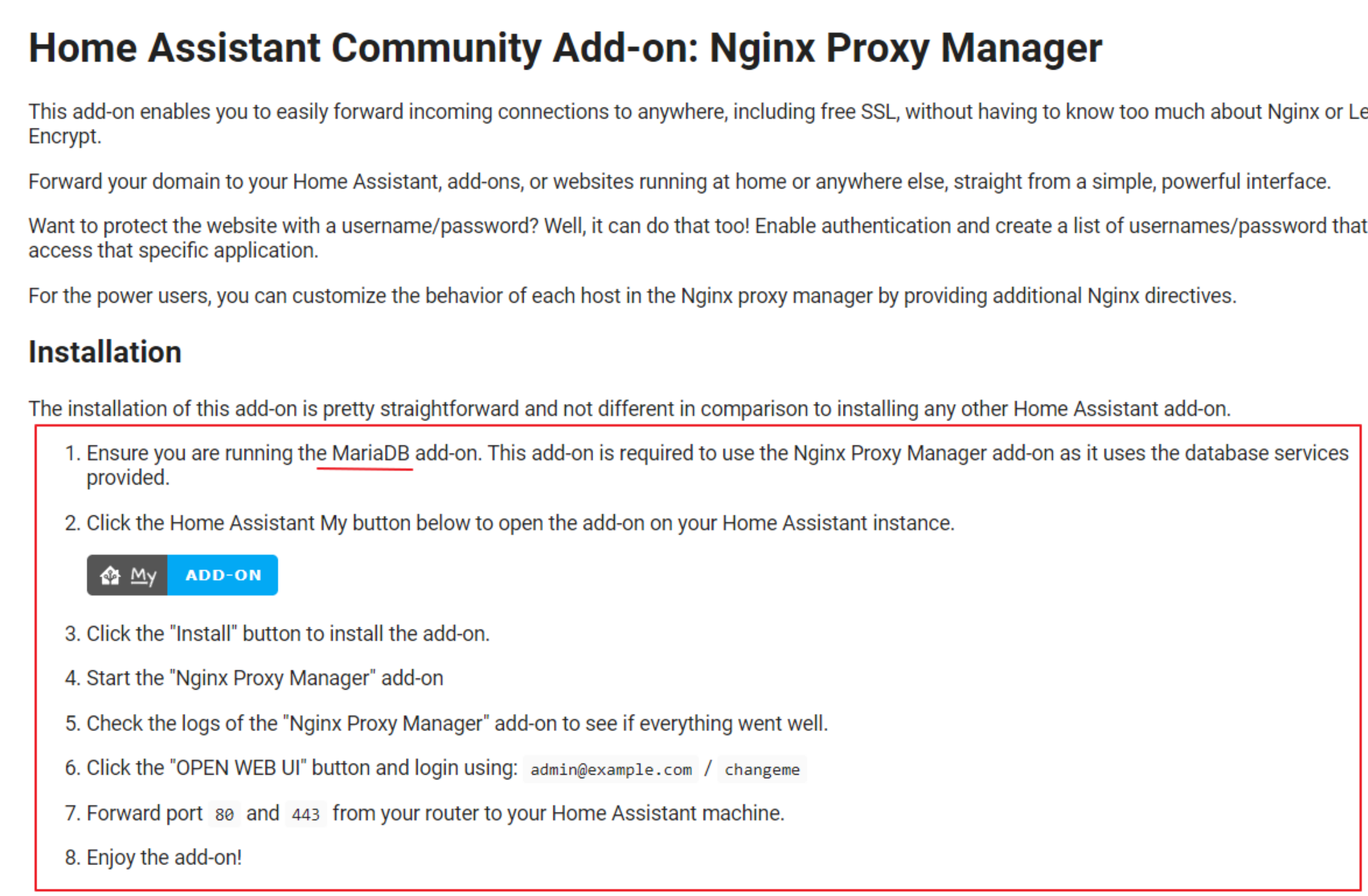
NGINX Home   t SSL proxy
An SSL/TLS pr

Keine Ergebnisse in ESPHome gefunden

Home Assistant Community Add-ons

Nginx Proxy Manager
Manage Nginx proxy hosts with a simple, powerful interface

Dokumentation



Home Assistant Community Add-on: Nginx Proxy Manager

This add-on enables you to easily forward incoming connections to anywhere, including free SSL, without having to know too much about Nginx or Let's Encrypt.

Forward your domain to your Home Assistant, add-ons, or websites running at home or anywhere else, straight from a simple, powerful interface.

Want to protect the website with a username/password? Well, it can do that too! Enable authentication and create a list of usernames/password that can access that specific application.

For the power users, you can customize the behavior of each host in the Nginx proxy manager by providing additional Nginx directives.

Installation

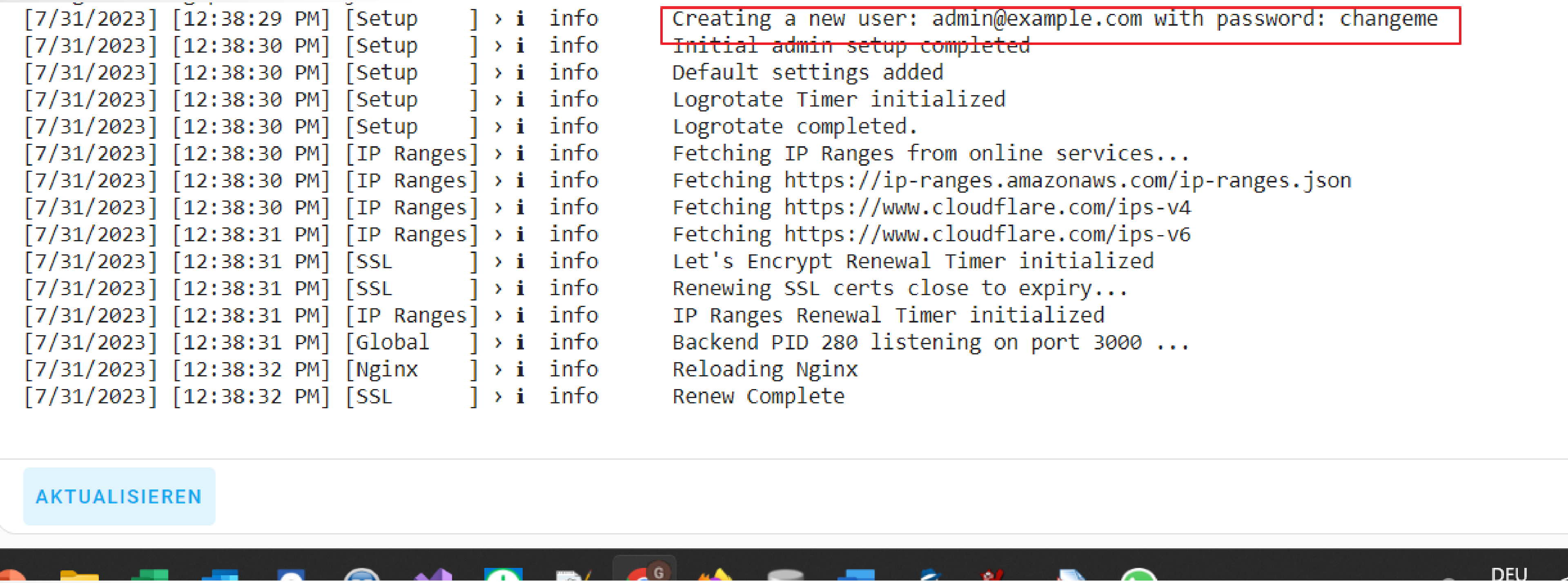
The installation of this add-on is pretty straightforward and not different in comparison to installing any other Home Assistant add-on.

1. Ensure you are running the MariaDB add-on. This add-on is required to use the Nginx Proxy Manager add-on as it uses the database services provided.
2. Click the Home Assistant My button below to open the add-on on your Home Assistant instance.

3. Click the "Install" button to install the add-on.
4. Start the "Nginx Proxy Manager" add-on
5. Check the logs of the "Nginx Proxy Manager" add-on to see if everything went well.
6. Click the "OPEN WEB UI" button and login using: `admin@example.com` / `changeme`
7. Forward port `80` and `443` from your router to your Home Assistant machine.
8. Enjoy the add-on!

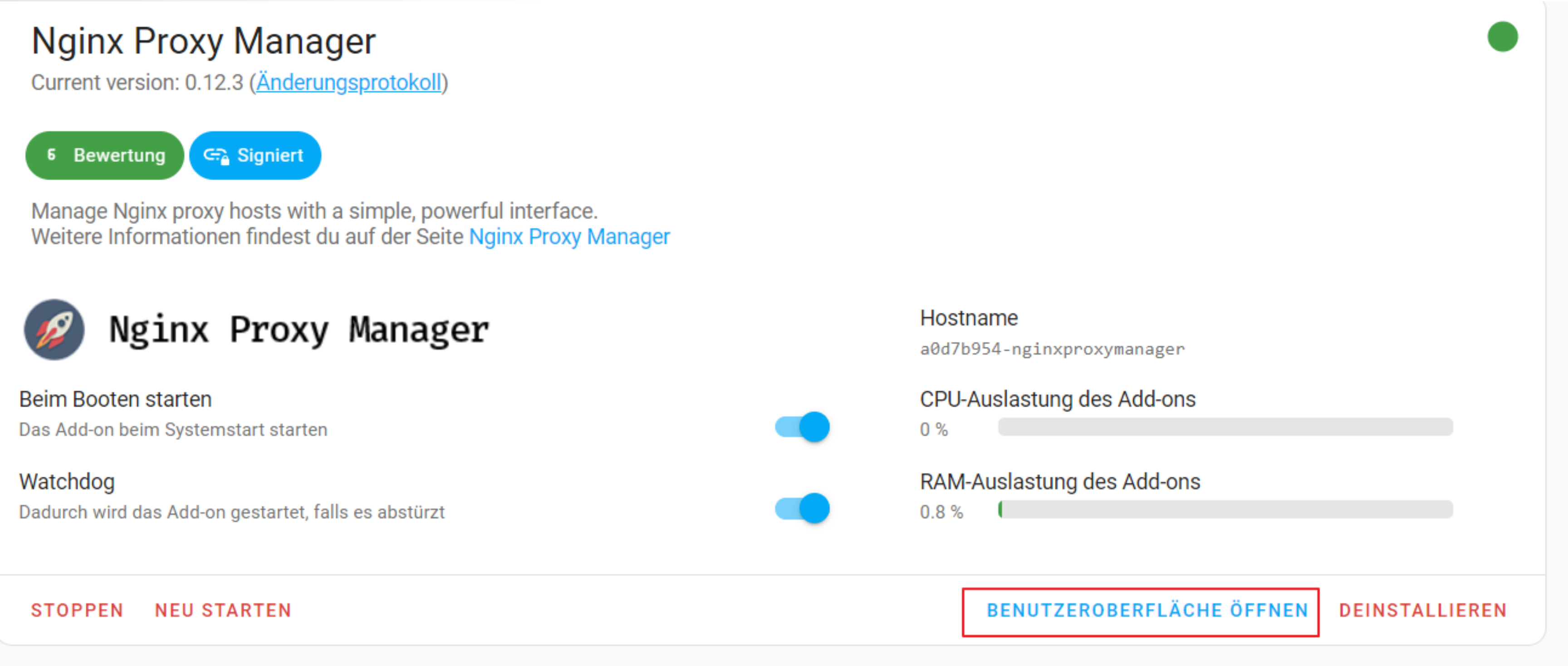
Logs kontrollieren

- Defaultuser: admin@example.com/changeme



```
[7/31/2023] [12:38:29 PM] [Setup    ] › i  info      Creating a new user: admin@example.com with password: changeme
[7/31/2023] [12:38:30 PM] [Setup    ] › i  info      Initial admin setup completed
[7/31/2023] [12:38:30 PM] [Setup    ] › i  info      Default settings added
[7/31/2023] [12:38:30 PM] [Setup    ] › i  info      Logrotate Timer initialized
[7/31/2023] [12:38:30 PM] [Setup    ] › i  info      Logrotate completed.
[7/31/2023] [12:38:30 PM] [IP Ranges] › i  info      Fetching IP Ranges from online services...
[7/31/2023] [12:38:30 PM] [IP Ranges] › i  info      Fetching https://ip-ranges.amazonaws.com/ip-ranges.json
[7/31/2023] [12:38:30 PM] [IP Ranges] › i  info      Fetching https://www.cloudflare.com/ips-v4
[7/31/2023] [12:38:31 PM] [IP Ranges] › i  info      Fetching https://www.cloudflare.com/ips-v6
[7/31/2023] [12:38:31 PM] [SSL      ] › i  info      Let's Encrypt Renewal Timer initialized
[7/31/2023] [12:38:31 PM] [SSL      ] › i  info      Renewing SSL certs close to expiry...
[7/31/2023] [12:38:31 PM] [IP Ranges] › i  info      IP Ranges Renewal Timer initialized
[7/31/2023] [12:38:31 PM] [Global   ] › i  info      Backend PID 280 listening on port 3000 ...
[7/31/2023] [12:38:32 PM] [Nginx    ] › i  info      Reloading Nginx
[7/31/2023] [12:38:32 PM] [SSL      ] › i  info      Renew Complete
```

Nginx ProxyManager hat eigenes UI



Nginx Proxy Manager

Current version: 0.12.3 (Änderungsprotokoll)

6 Bewertung | Signiert

Manage Nginx proxy hosts with a simple, powerful interface.
Weitere Informationen findest du auf der Seite Nginx Proxy Manager

Nginx Proxy Manager

Hostname
a0d7b954-nginxproxymanager

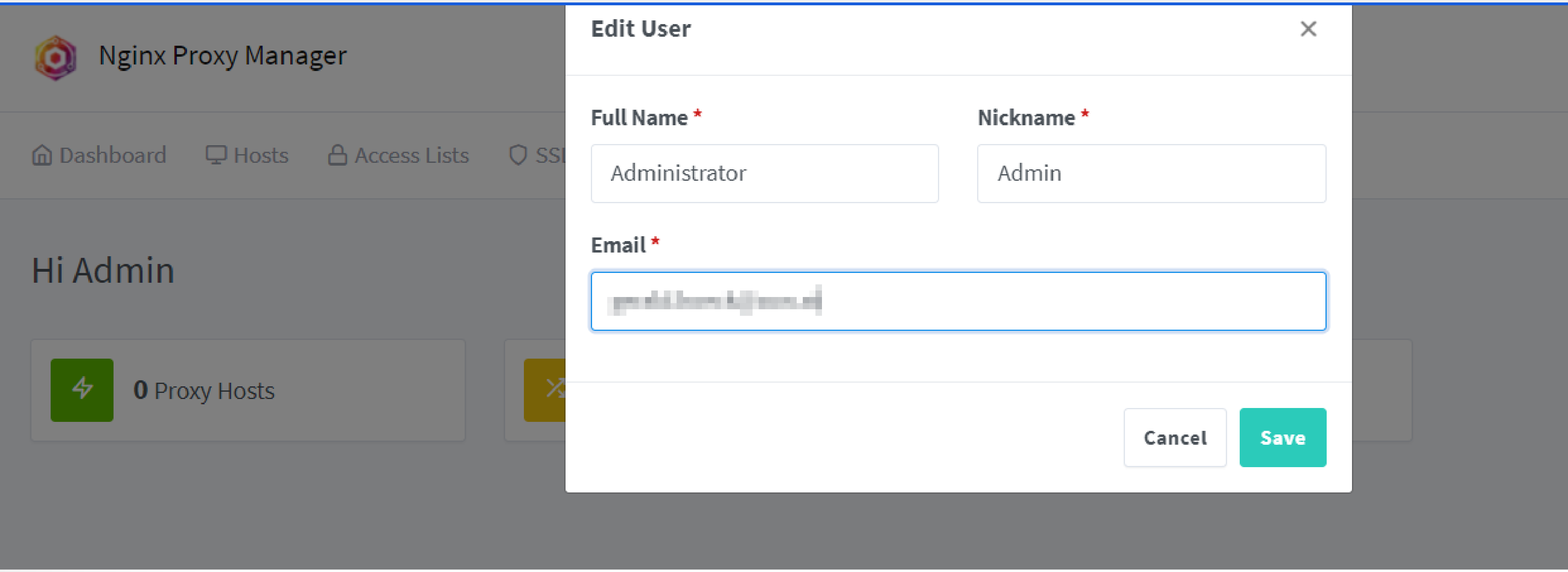
Beim Booten starten
Das Add-on beim Systemstart starten

CPU-Auslastung des Add-ons
0 %

Watchdog
Dadurch wird das Add-on gestartet, falls es abstürzt

RAM-Auslastung des Add-ons
0.8 %

UI starten → admin editieren



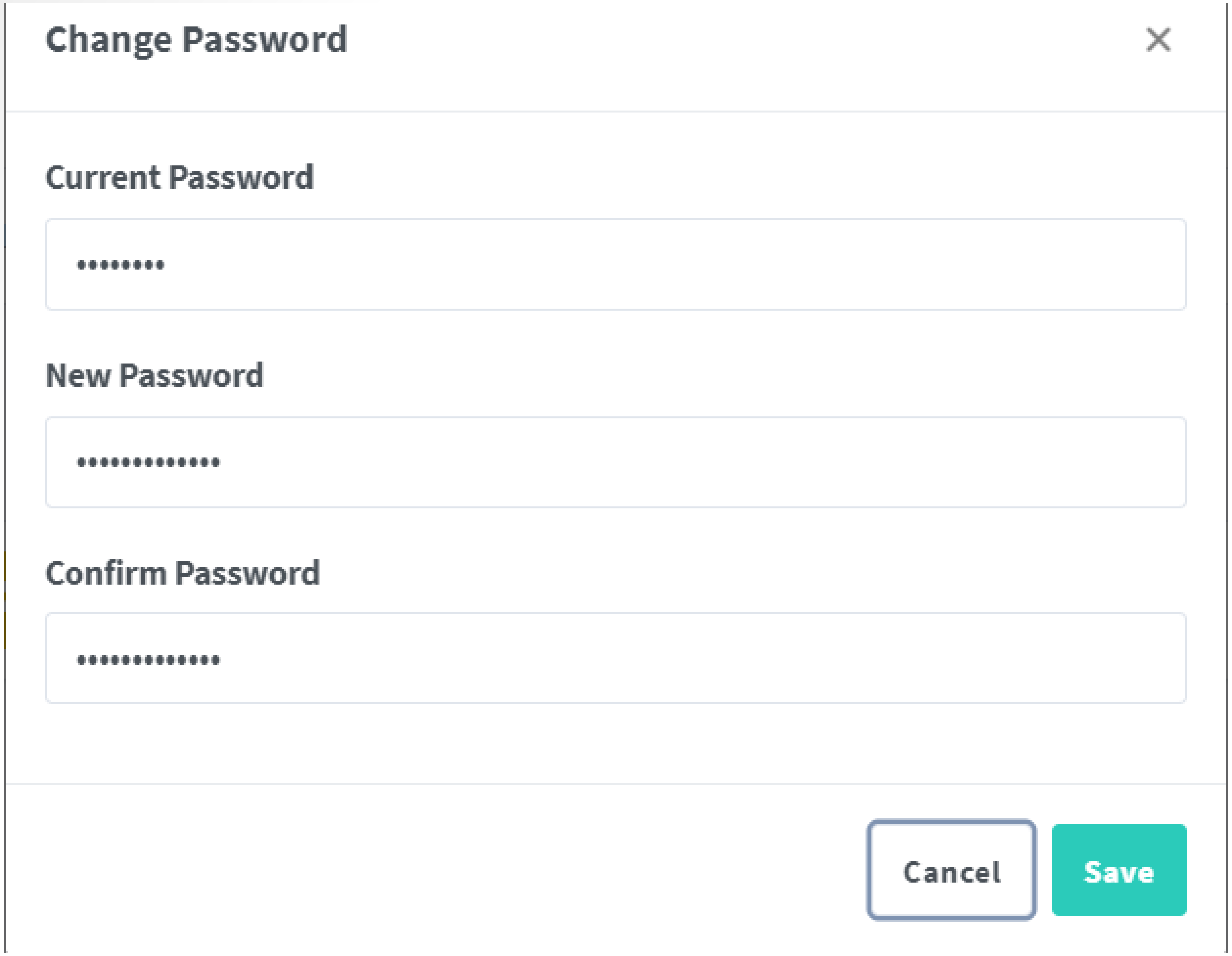
Edit User

Full Name *: Administrator

Nickname *: Admin

Email *: [redacted]

Neues Passwort vergeben (npmK…)



Change Password

Current Password

••••••••

New Password

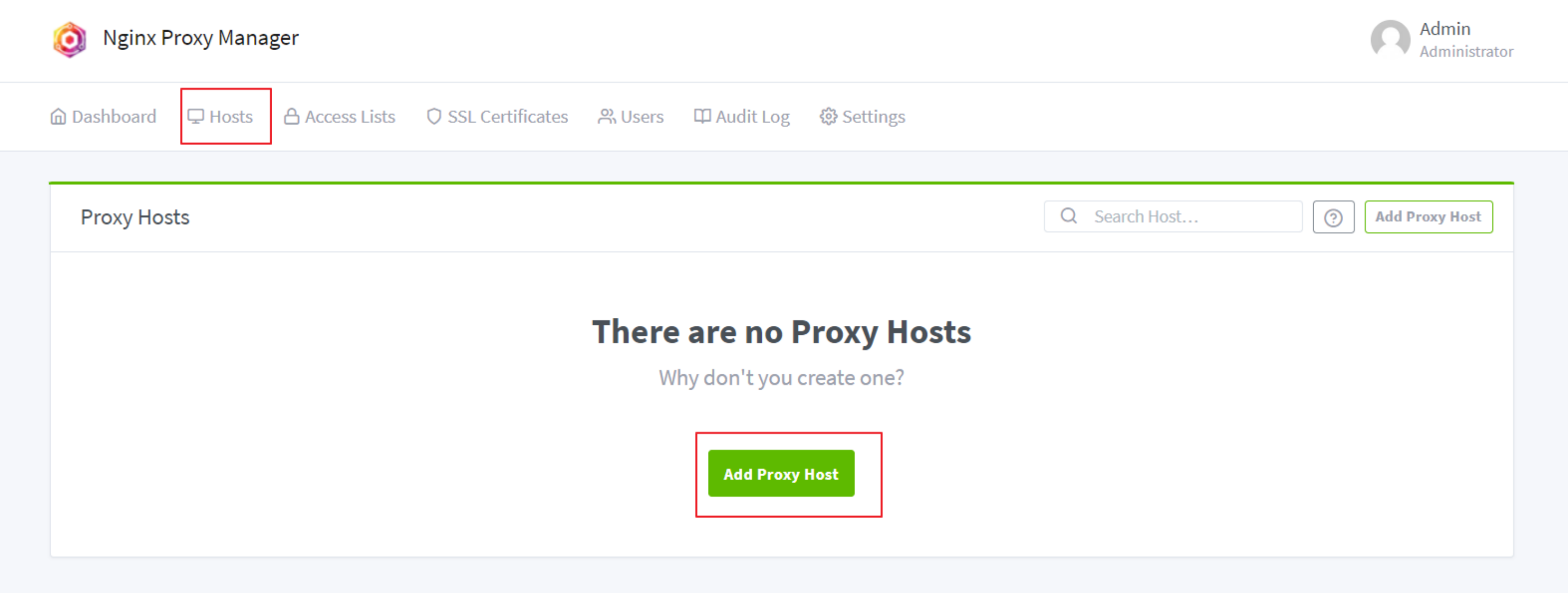
•••••••••••••

Confirm Password

•••••••••••••

Ersten Host hinzufügen

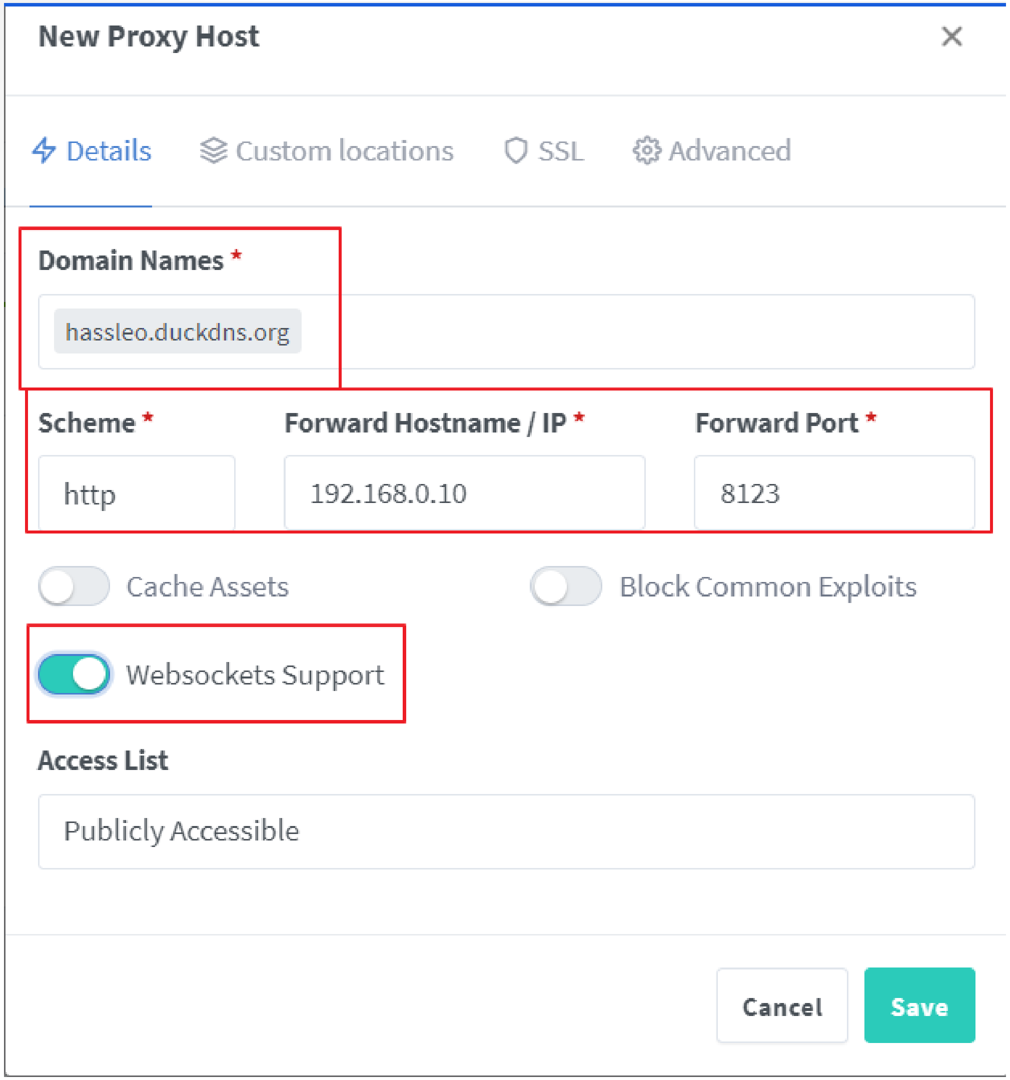
- HA mit Duckdns



There are no Proxy Hosts

Why don't you create one?

Config des Portforwardings



Domain Names *

hassleo.duckdns.org

Scheme *: http

Forward Hostname / IP *: 192.168.0.10

Forward Port *: 8123

○ Cache Assets

○ Block Common Exploits

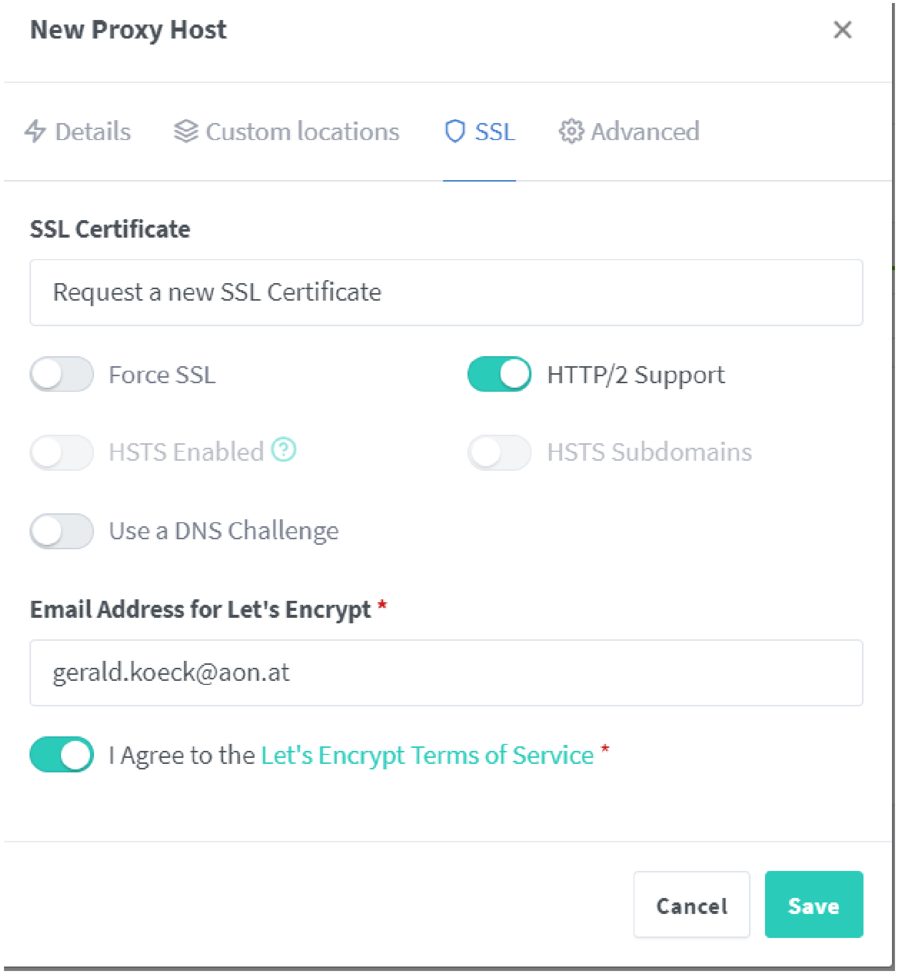
● Websockets Support

Access List

Publicly Accessible

SSL Zertifikat

- LetsEncrypt überprüft die Erreichbarkeit des Hosts per http-Challenge
  - Port 80 muss auf dem Host von Außen erreichbar sein



SSL Certificate

Request a new SSL Certificate

○ Force SSL ● HTTP/2 Support

○ HSTS Enabled ○ HSTS Subdomains

○ Use a DNS Challenge

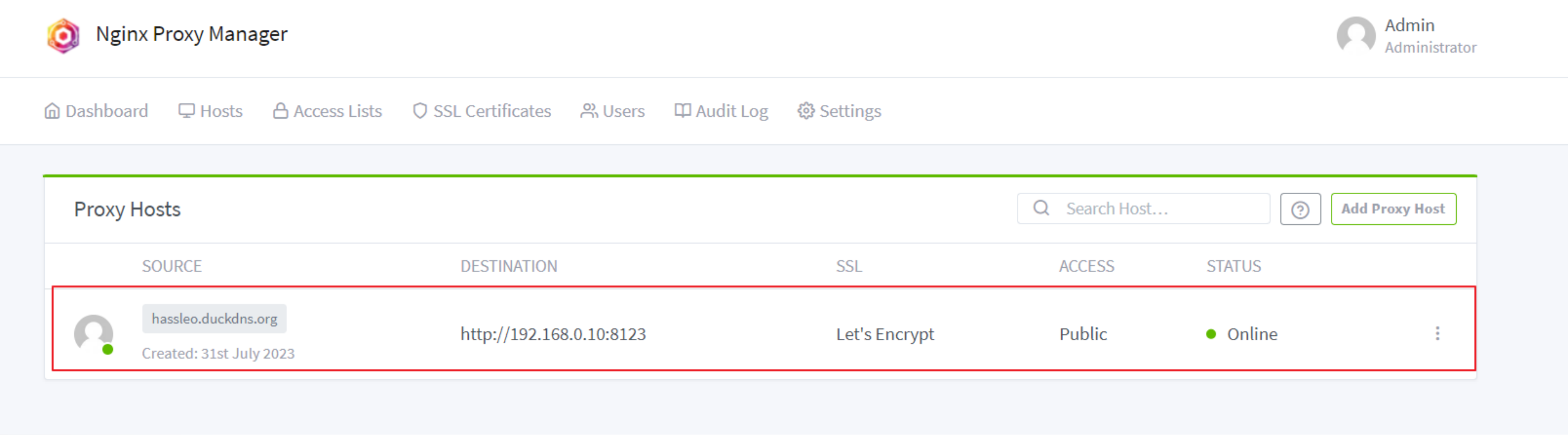
Email Address for Let's Encrypt *

gerald.koeck@aon.at

● I Agree to the Let's Encrypt Terms of Service *

Save → Dauert

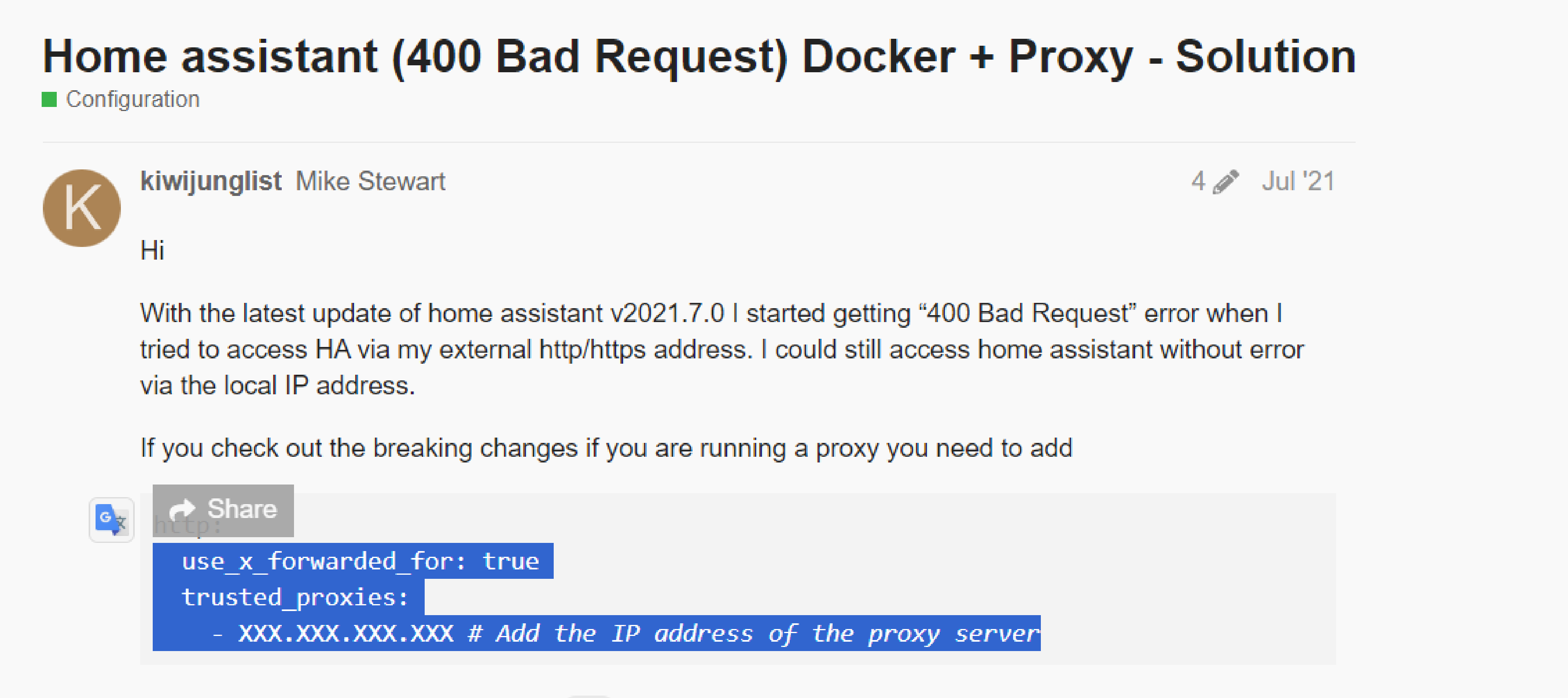
- Erfolg
  - Zertifikat wurde erfolgreich überprüft



SOURCE	DESTINATION	SSL	ACCESS	STATUS
hassleo.duckdns.org Created: 31st July 2023	http://192.168.0.10:8123	Let's Encrypt	Public	● Online

Bad Request ???

- https://community.home-assistant.io/t/home-assistant-400-bad-request-docker-proxy-solution/322163/1



Home assistant (400 Bad Request) Docker + Proxy - Solution

🟩 Configuration

kiwijunglist Mike Stewart 4 ✎ Jul '21

Hi

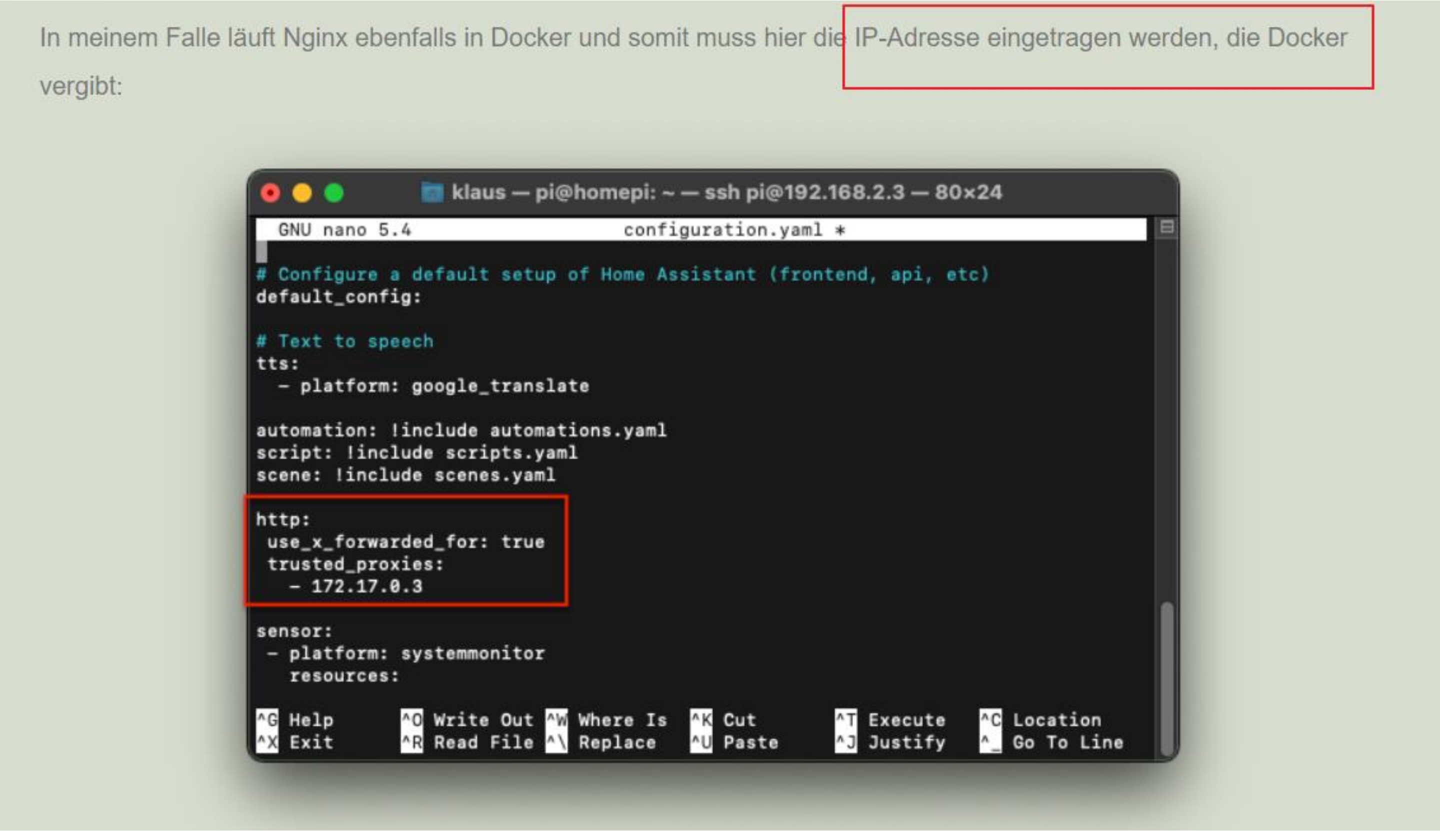
With the latest update of home assistant v2021.7.0 I started getting “400 Bad Request” error when I tried to access HA via my external http/https address. I could still access home assistant without error via the local IP address.

If you check out the breaking changes if you are running a proxy you need to add

```
http:
  use_x_forwarded_for: true
  trusted_proxies:
    - XXX.XXX.XXX.XXX # Add the IP address of the proxy server
```

Geht immer noch nicht

- https://www.klausmoster.de/2022/09/02/home-assistant-und-nginx-proxy-manager/
- Proxy läuft unter Docker ➔ ganz andere IP

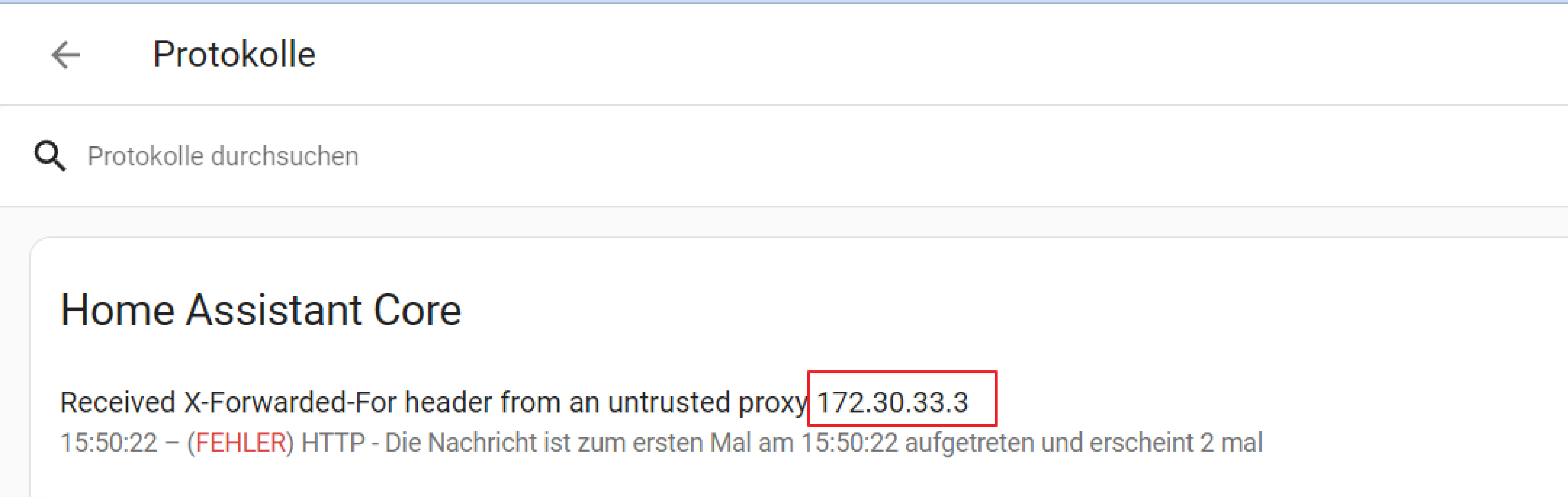


In meinem Falle läuft Nginx ebenfalls in Docker und somit muss hier die IP-Adresse eingetragen werden, die Docker vergibt:

```
  GNU nano 5.4                    configuration.yaml *

# Configure a default setup of Home Assistant (frontend, api, etc)
default_config:

# Text to speech
tts:
  - platform: google_translate

automation: !include automations.yaml
script: !include scripts.yaml
scene: !include scenes.yaml

http:
 use_x_forwarded_for: true
 trusted_proxies:
   - 172.17.0.3

sensor:
 - platform: systemmonitor
   resources:

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Einstellungen – System - Protokolle

- Fehlermeldung: IP von Nginx Reverse Proxy
  - Wurde von Docker vergeben

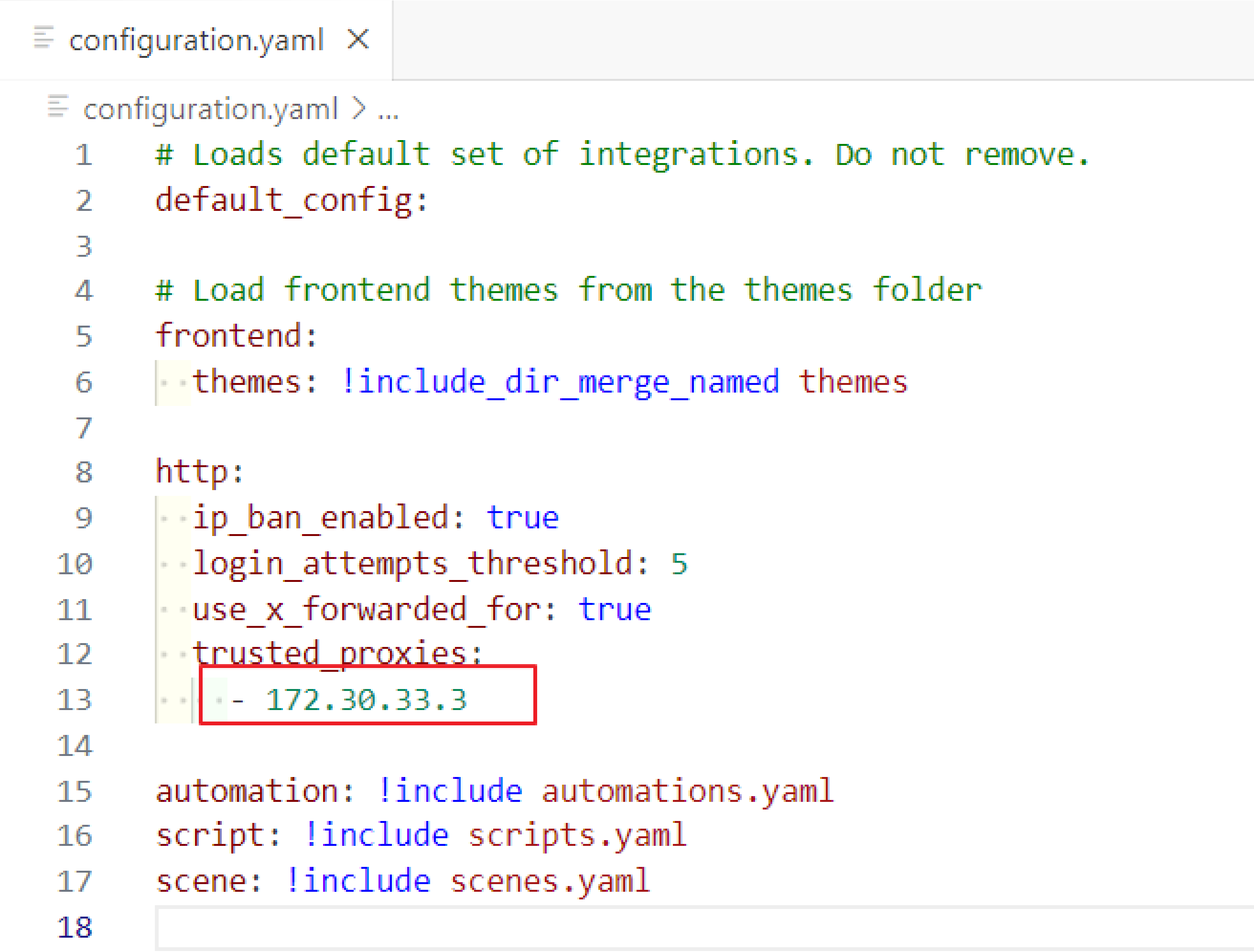


Home Assistant Core

Received X-Forwarded-For header from an untrusted proxy 172.30.33.3

15:50:22 – (FEHLER) HTTP - Die Nachricht ist zum ersten Mal am 15:50:22 aufgetreten und erscheint 2 mal

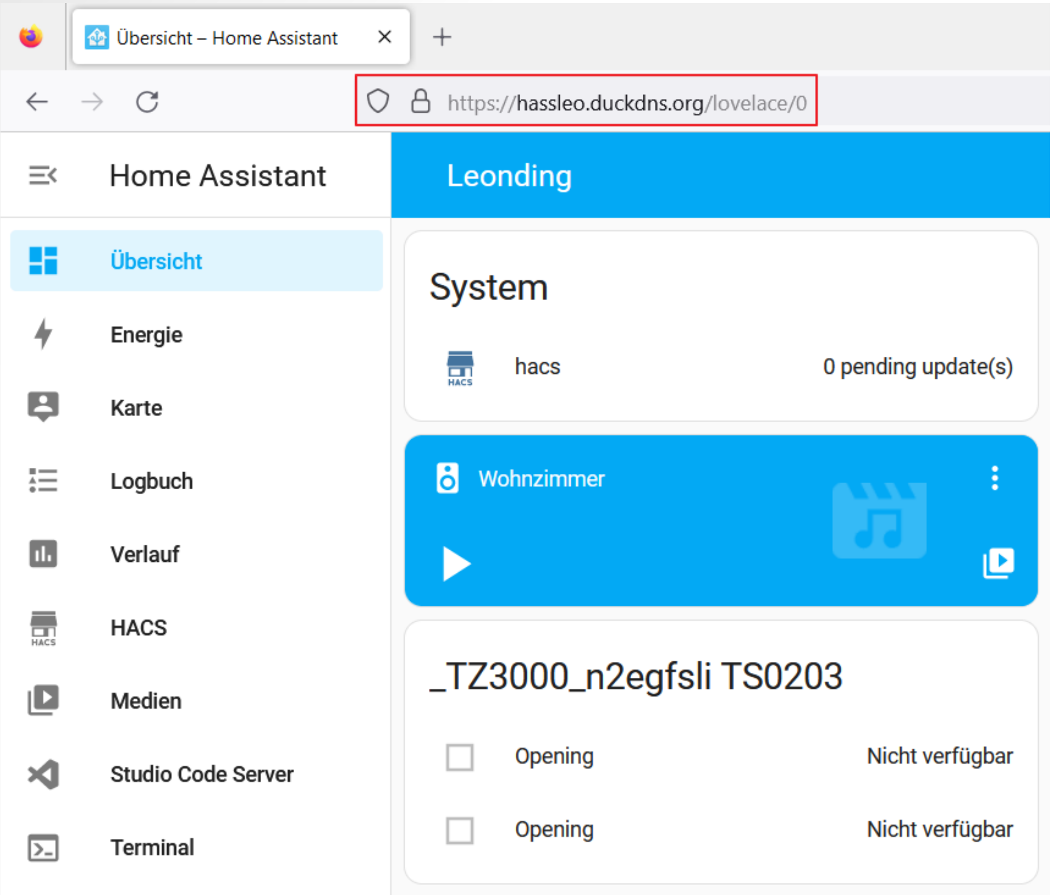
configuration.yaml



```yaml
# Loads default set of integrations. Do not remove.
default_config:

# Load frontend themes from the themes folder
frontend:
  themes: !include_dir_merge_named themes

http:
  ip_ban_enabled: true
  login_attempts_threshold: 5
  use_x_forwarded_for: true
  trusted_proxies:
    - 172.30.33.3

automation: !include automations.yaml
script: !include scripts.yaml
scene: !include scenes.yaml

```

Ergebnis

- Zugriff von Außen verschlüsselt über Https (Dyndns) und vom lokalen LAN über http://xx.xx.xx.xx:8123



https://hassleo.duckdns.org/lovelace/0

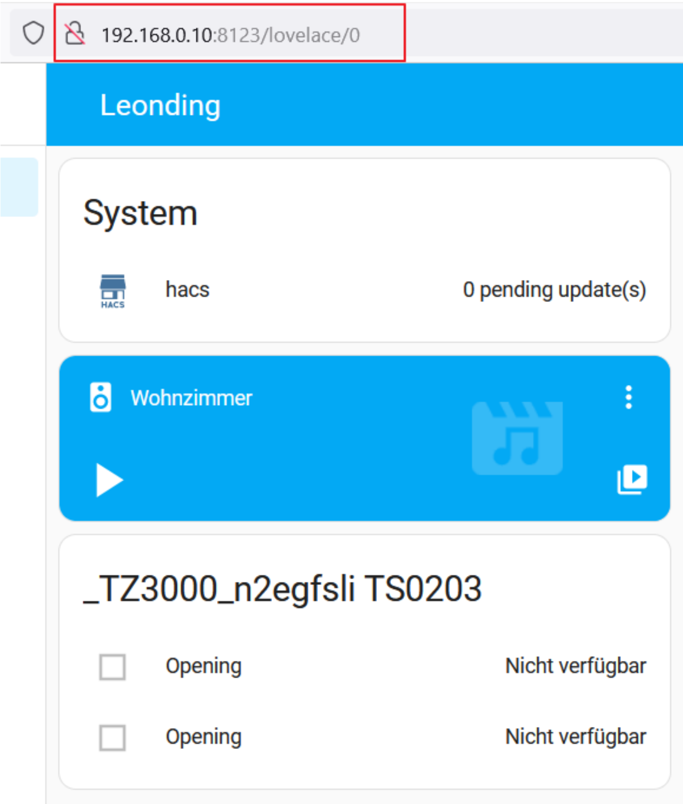
Leonding

System

hacs	0 pending update(s)

_TZ3000_n2egfsli TS0203

□ Opening	Nicht verfügbar
□ Opening	Nicht verfügbar



192.168.0.10:8123/lovelace/0

Leonding

System

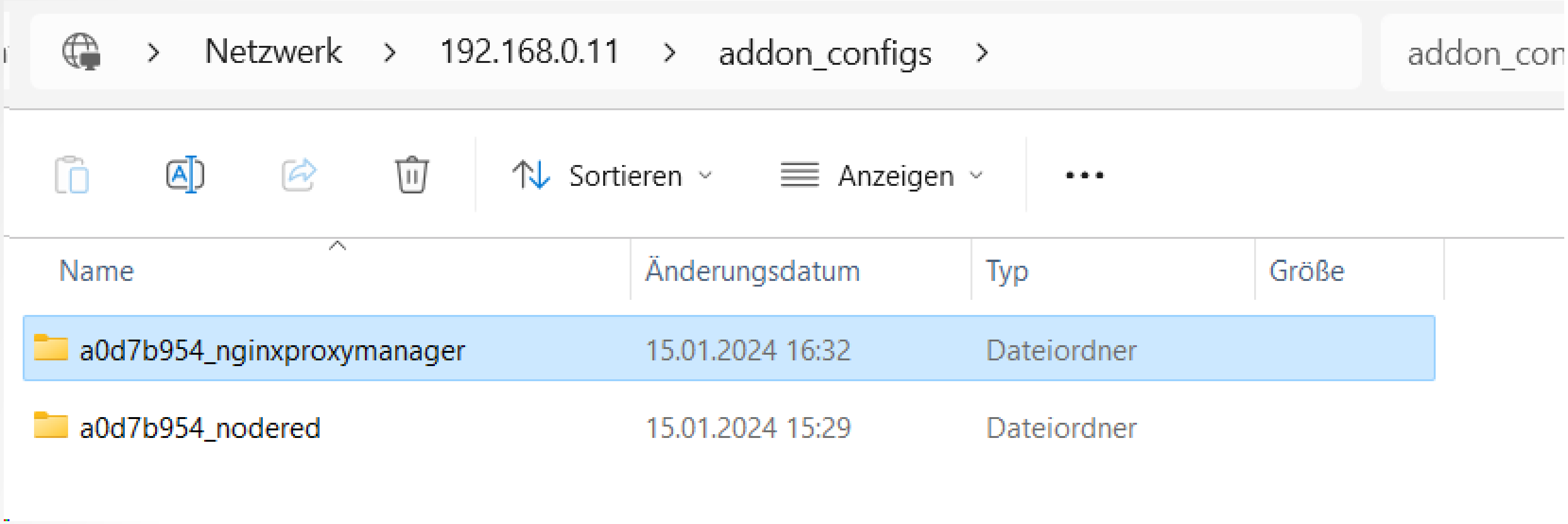
hacs	0 pending update(s)

_TZ3000_n2egfsli TS0203

□ Opening	Nicht verfügbar
□ Opening	Nicht verfügbar

Deinstallation NPM - Config

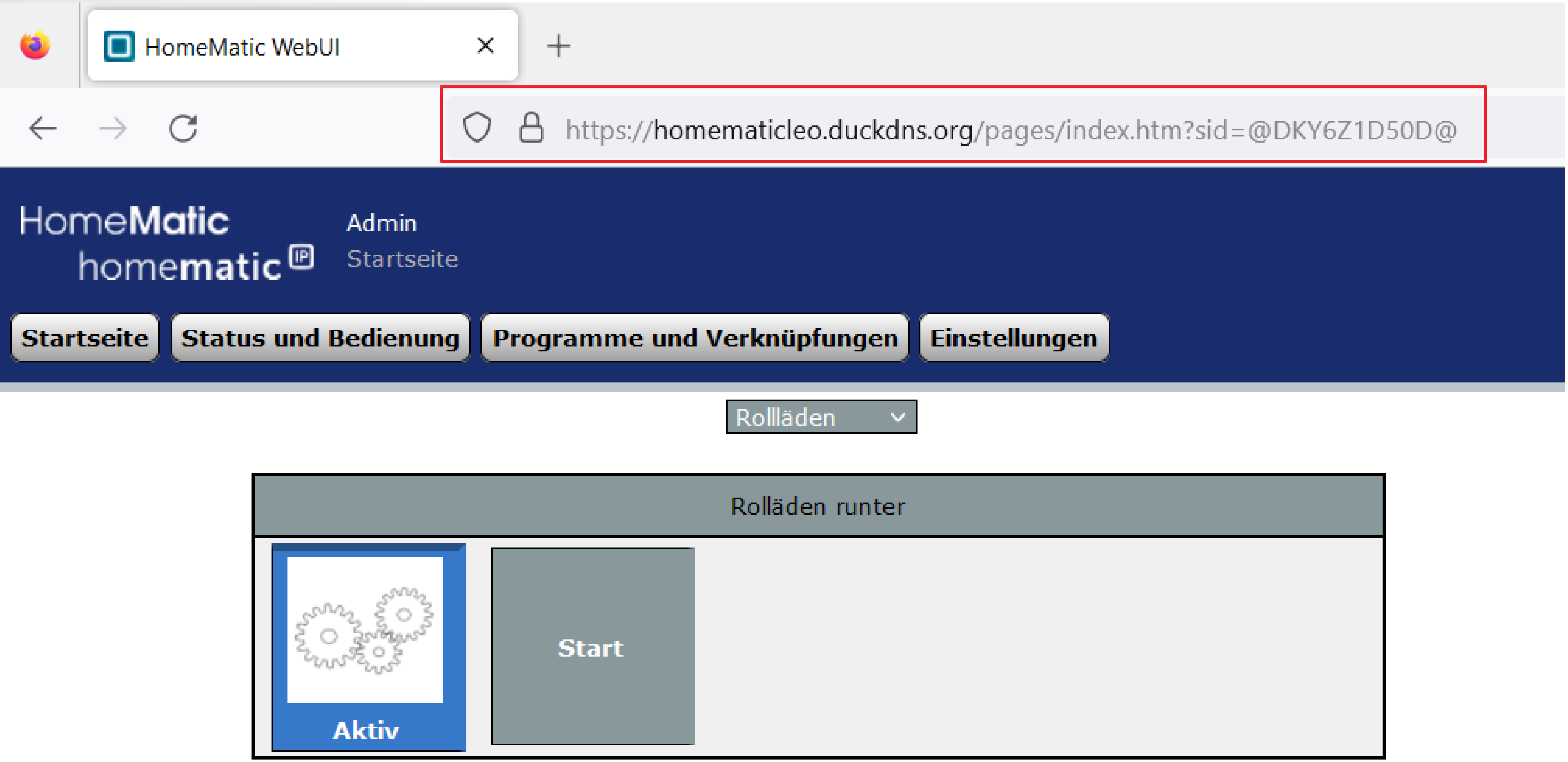
- Config bleibt bei Löschen/Neuinstallation erhalten
- Aus Share addon_configs löschen



Name	Änderungsdatum	Typ	Größe
a0d7b954_nginxproxymanager	15.01.2024 16:32	Dateiordner	
a0d7b954_nodered	15.01.2024 15:29	Dateiordner	

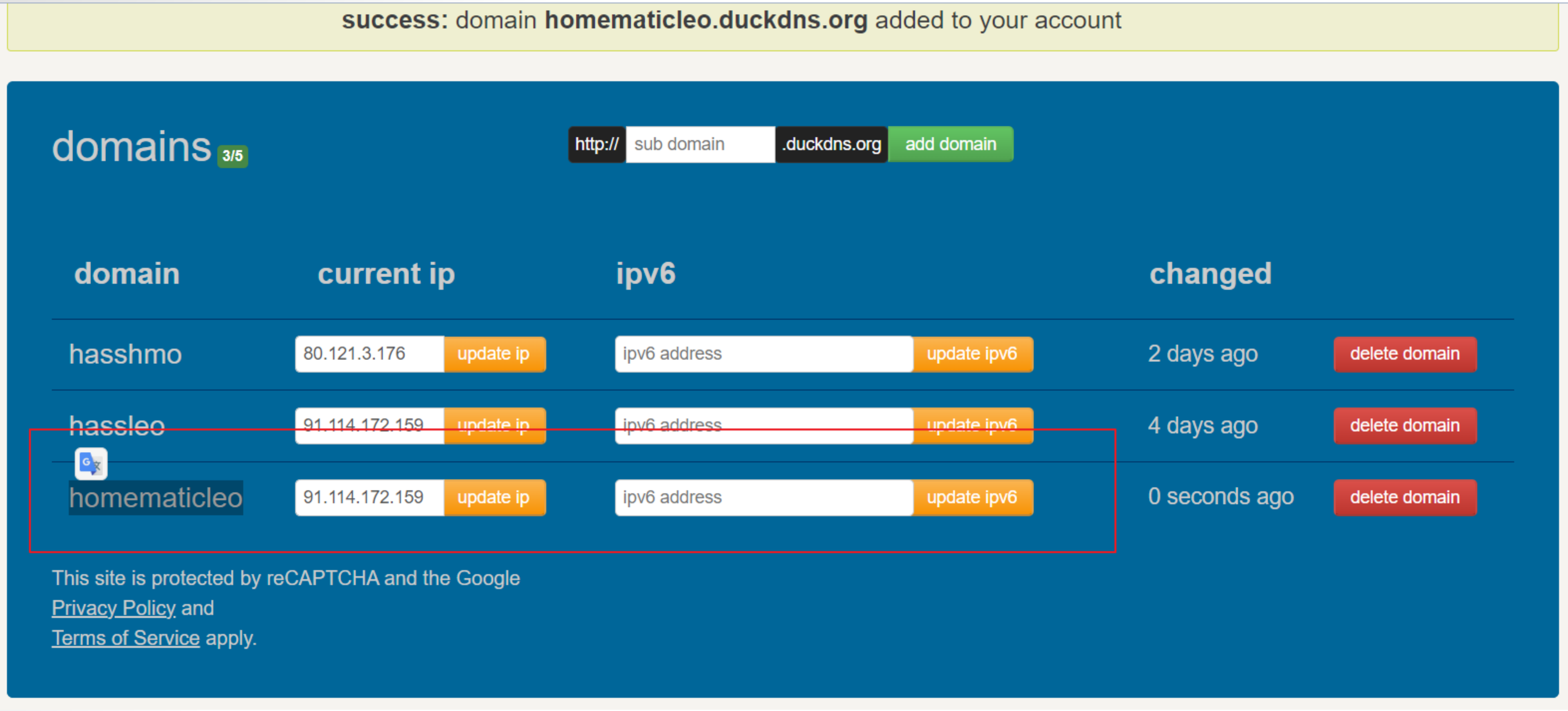
Weiteren Host anlegen

- Homematic mit Basic Authentication



https://homematicleo.duckdns.org/pages/index.htm?sid=@DKY6Z1D50D@

Duckdns – Domain anlegen



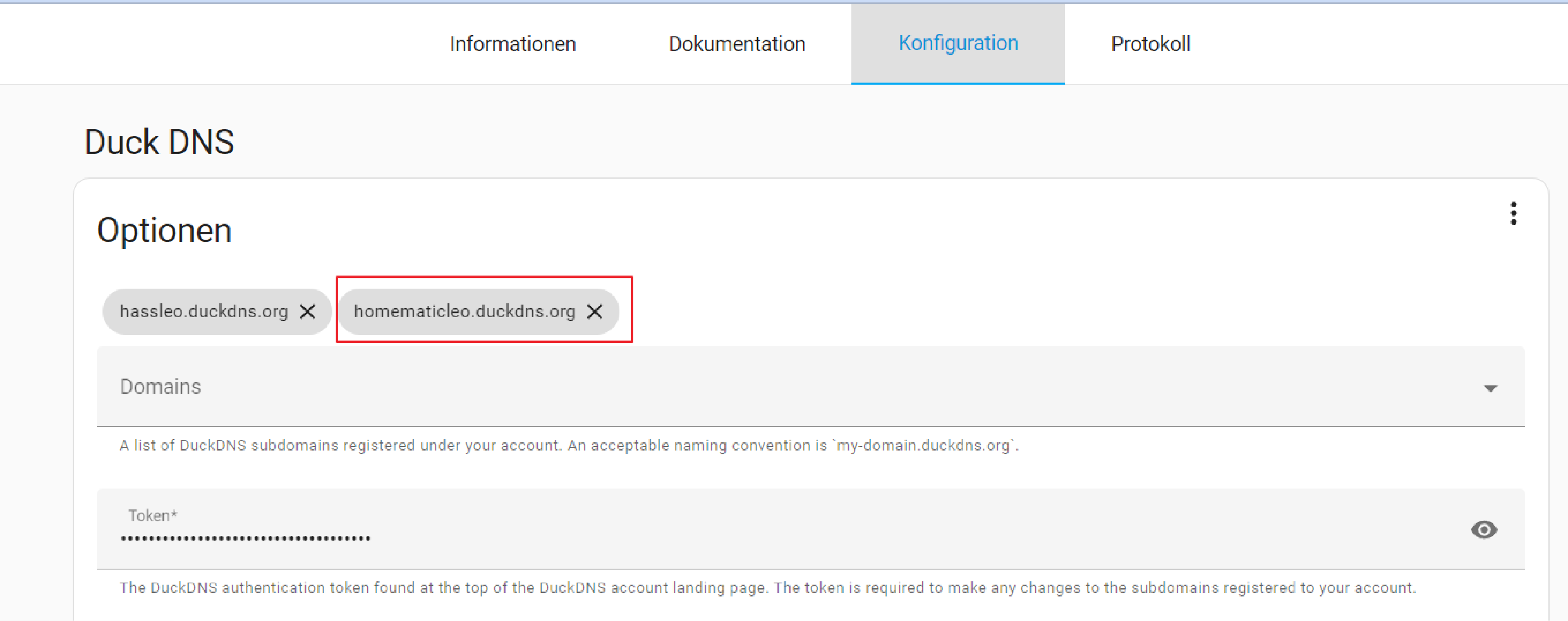
success: domain **homematicleo.duckdns.org** added to your account

domains 3/5

domain	current ip	ipv6	changed	
hasshmo	80.121.3.176 update ip	ipv6 address update ipv6	2 days ago	delete domain
hassleo	91.114.172.159 update ip	ipv6 address update ipv6	4 days ago	delete domain
homematicleo	91.114.172.159 update ip	ipv6 address update ipv6	0 seconds ago	delete domain

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

In AddOn Duckdns Domain anlegen …



Duck DNS

Optionen

hassleo.duckdns.org ✕ homematicleo.duckdns.org ✕

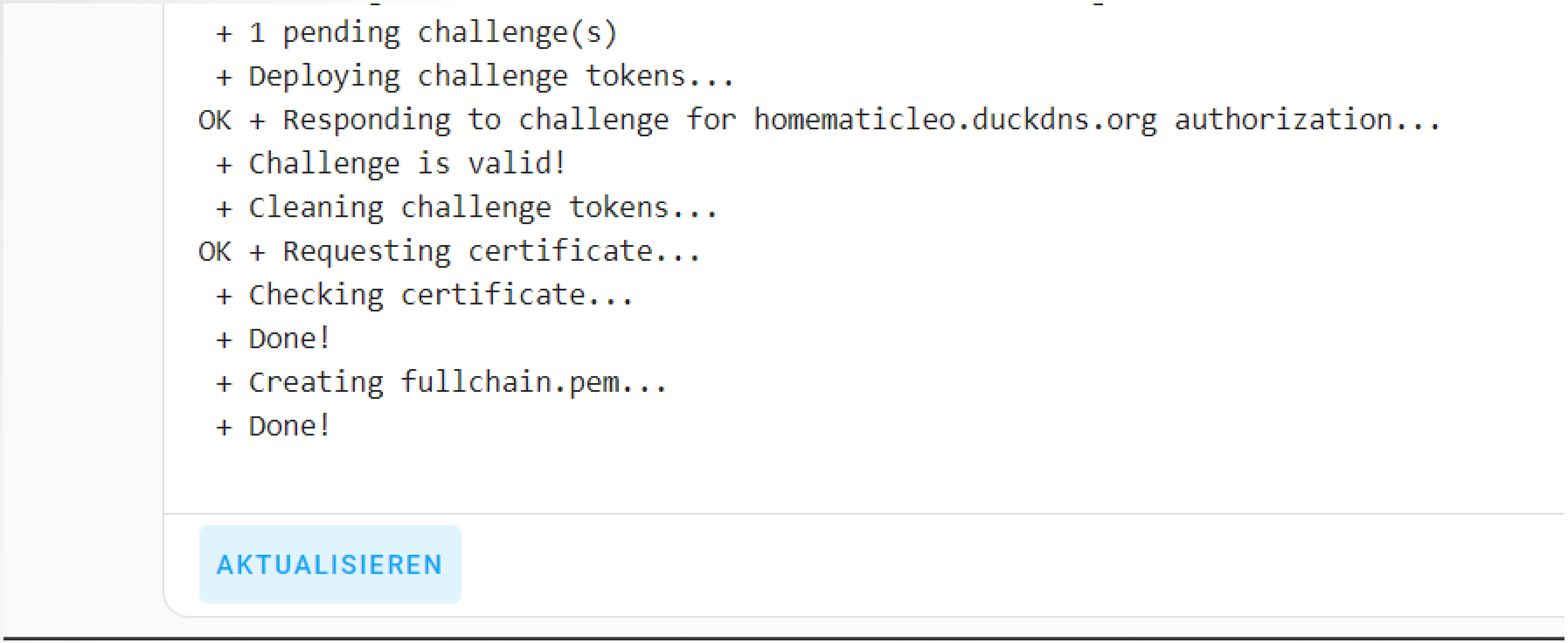
Domains

A list of DuckDNS subdomains registered under your account. An acceptable naming convention is `my-domain.duckdns.org`.

Token*
••••••••••••••••••••••••••••••••

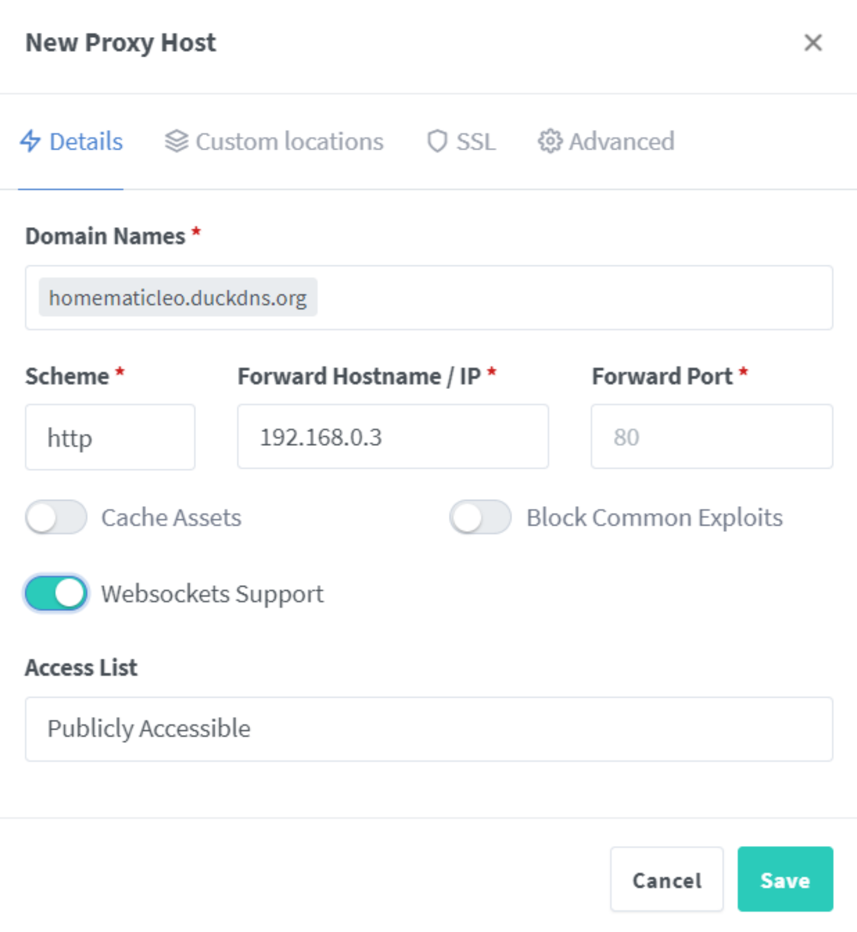
The DuckDNS authentication token found at the top of the DuckDNS account landing page. The token is required to make any changes to the subdomains registered to your account.

… Protokoll überprüfen



```
  + 1 pending challenge(s)
  + Deploying challenge tokens...
OK + Responding to challenge for homematicleo.duckdns.org authorization...
  + Challenge is valid!
  + Cleaning challenge tokens...
OK + Requesting certificate...
  + Checking certificate...
  + Done!
  + Creating fullchain.pem...
  + Done!
```

In Nginx Reverse-Proxy konfigurieren



New Proxy Host ×

Details | Custom locations | SSL | Advanced

Domain Names *

homematicleo.duckdns.org

Scheme *	**Forward Hostname / IP** *	**Forward Port** *
http	192.168.0.3	80

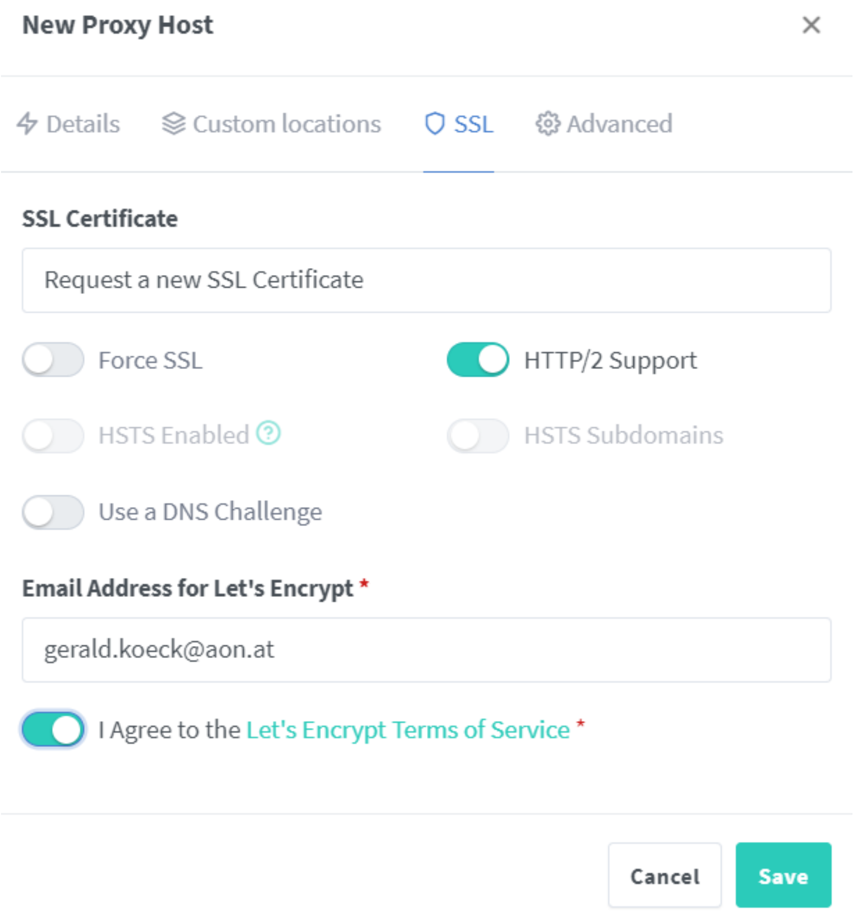
○ Cache Assets   ○ Block Common Exploits

● Websockets Support

Access List

Publicly Accessible

Cancel | Save



New Proxy Host ×

Details | Custom locations | SSL | Advanced

SSL Certificate

Request a new SSL Certificate

○ Force SSL   ● HTTP/2 Support

○ HSTS Enabled ?   ○ HSTS Subdomains

○ Use a DNS Challenge

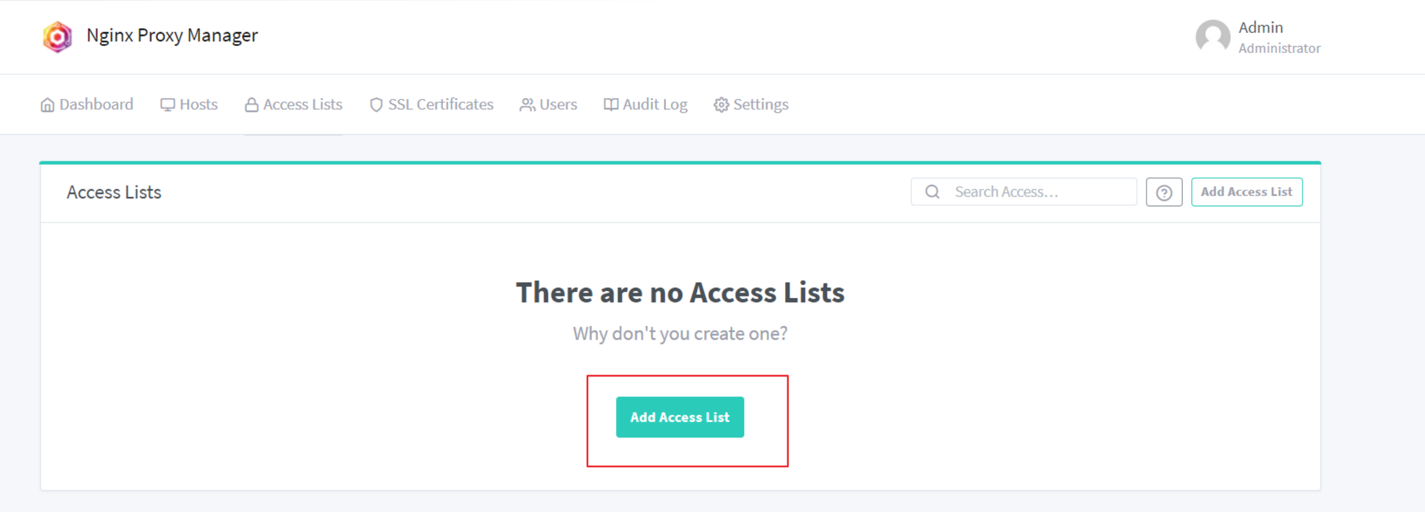
Email Address for Let's Encrypt *

gerald.koeck@aon.at

● I Agree to the Let's Encrypt Terms of Service *

Cancel | Save

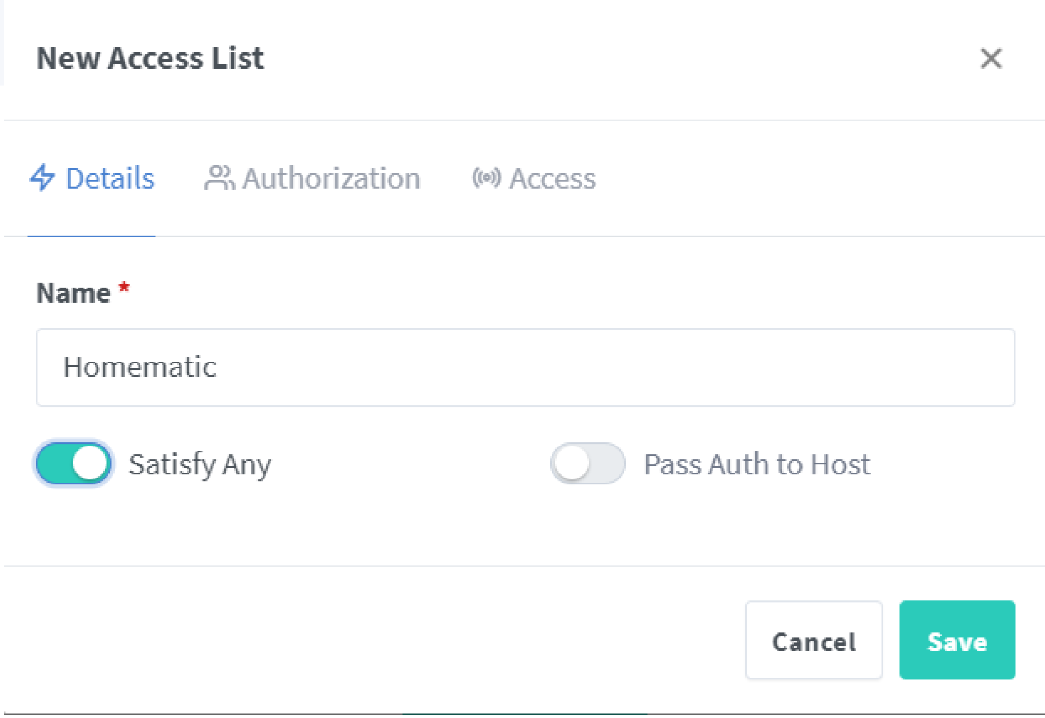
AccessList hinzufügen



Access Lists

There are no Access Lists

Why don't you create one?



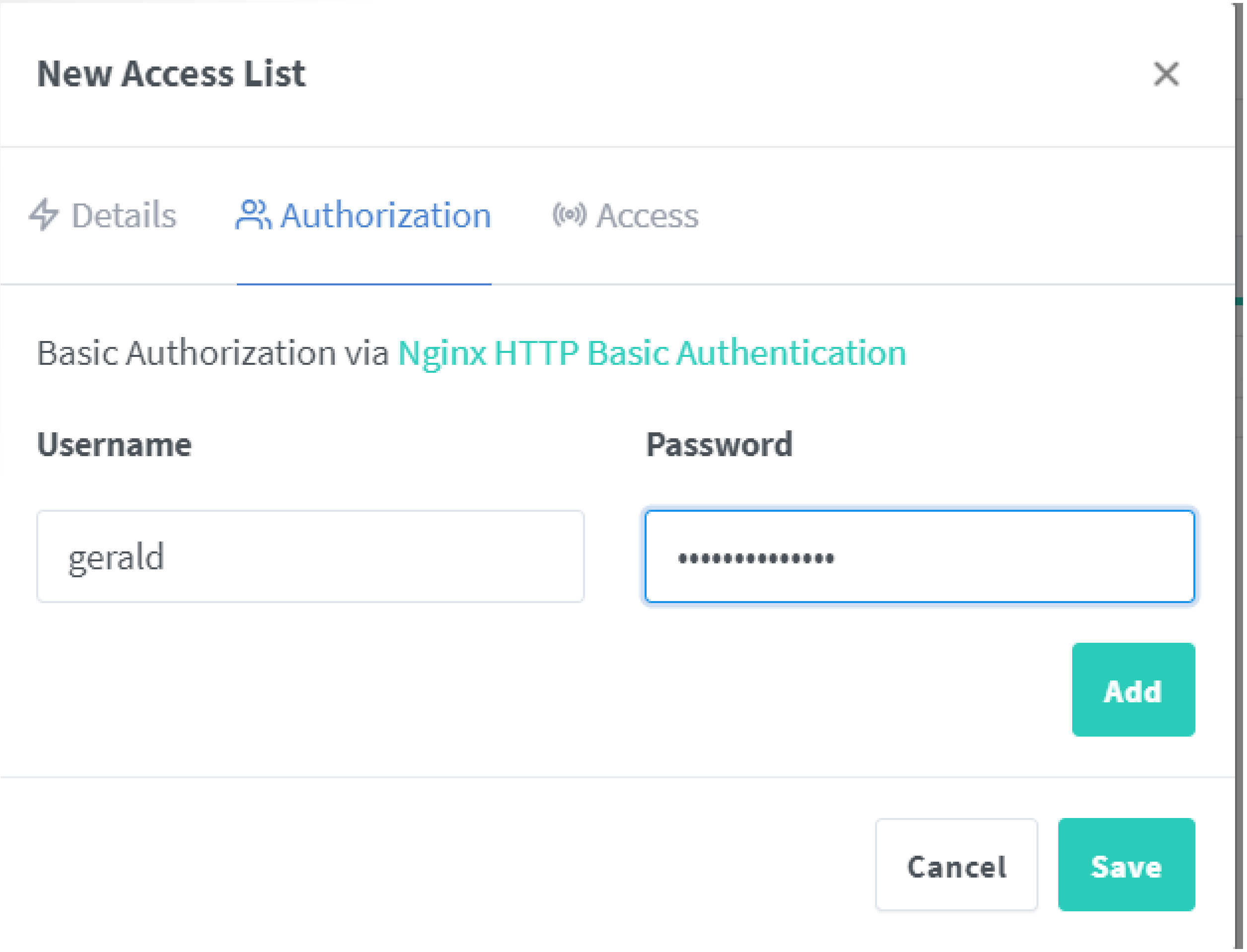
New Access List

Name *: Homematic

● Satisfy Any

○ Pass Auth to Host

Benutzer anlegen

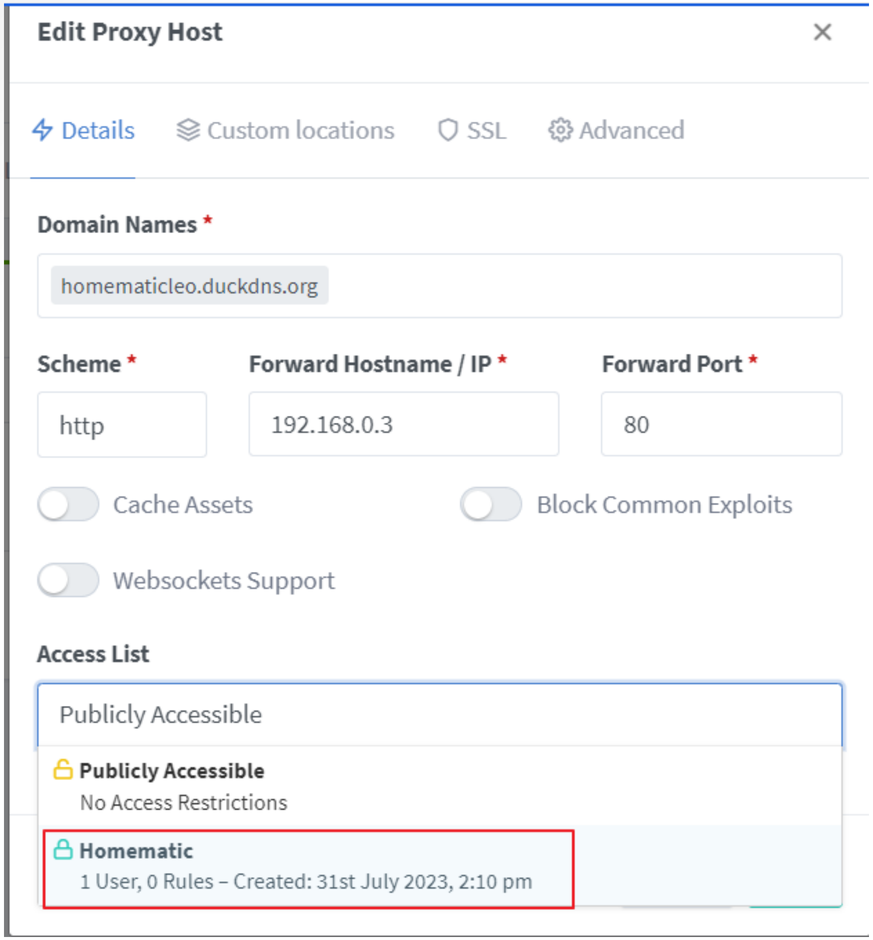

New Access List

Basic Authorization via Nginx HTTP Basic Authentication

Username: gerald

Password: ••••••••••••••

AccessList hinzufügen



Domain Names *

homematicleo.duckdns.org

Scheme *

http

Forward Hostname / IP *

192.168.0.3

Forward Port *

80

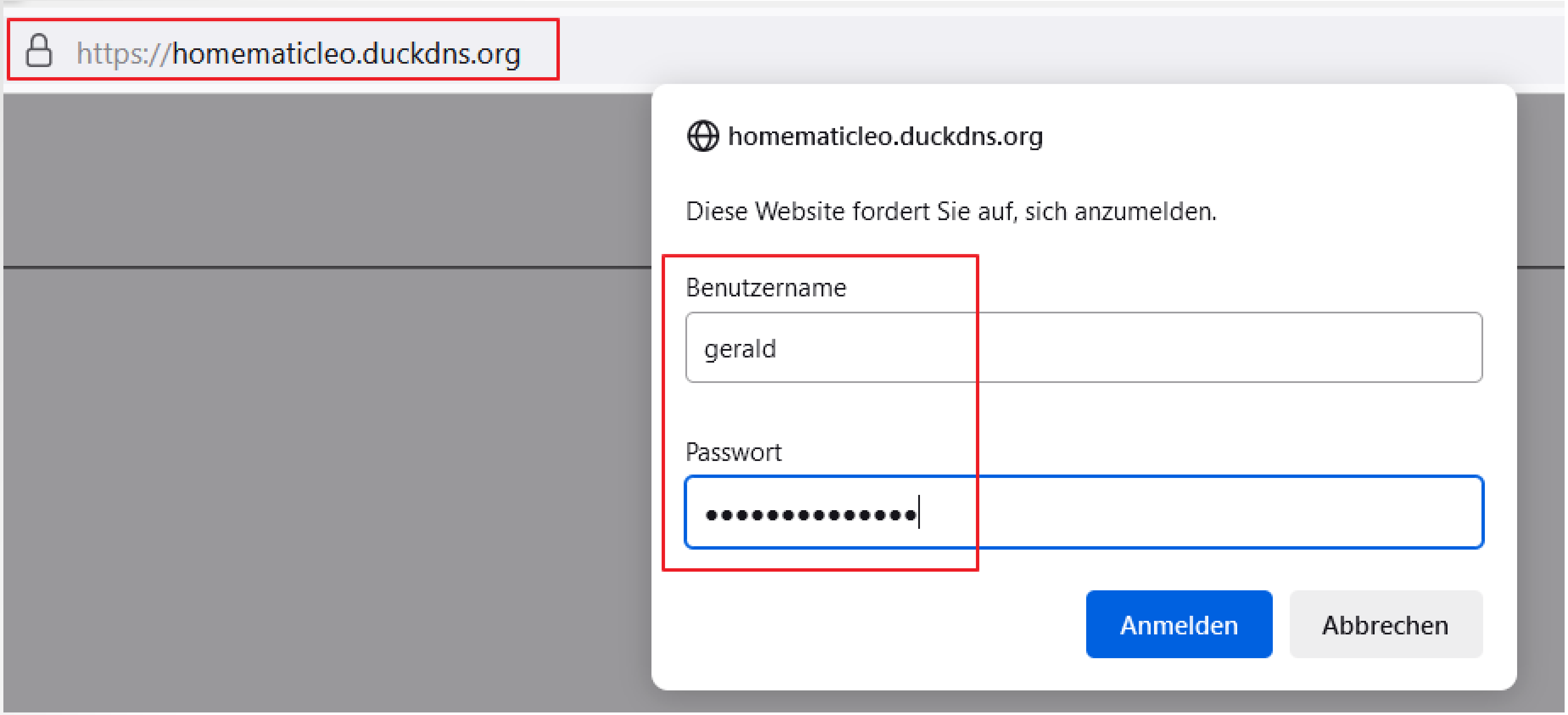
Access List

Publicly Accessible

Publicly Accessible
No Access Restrictions

Homematic
1 User, 0 Rules – Created: 31st July 2023, 2:10 pm

Basic Authentication



https://homematicleo.duckdns.org

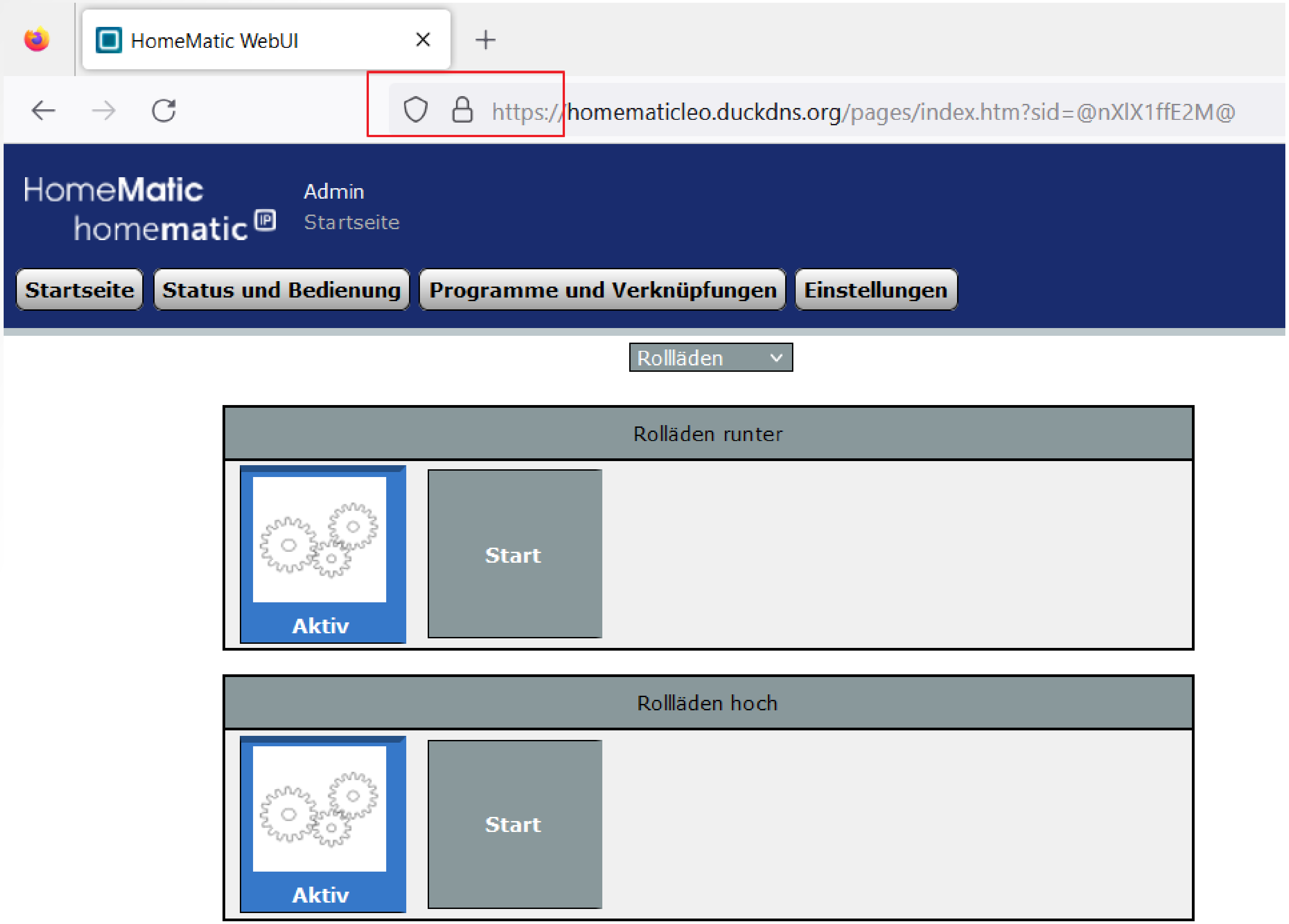
homematicleo.duckdns.org

Diese Website fordert Sie auf, sich anzumelden.

Benutzername: gerald

Passwort: ●●●●●●●●●●●●●●

Verschlüsselt und gesichert

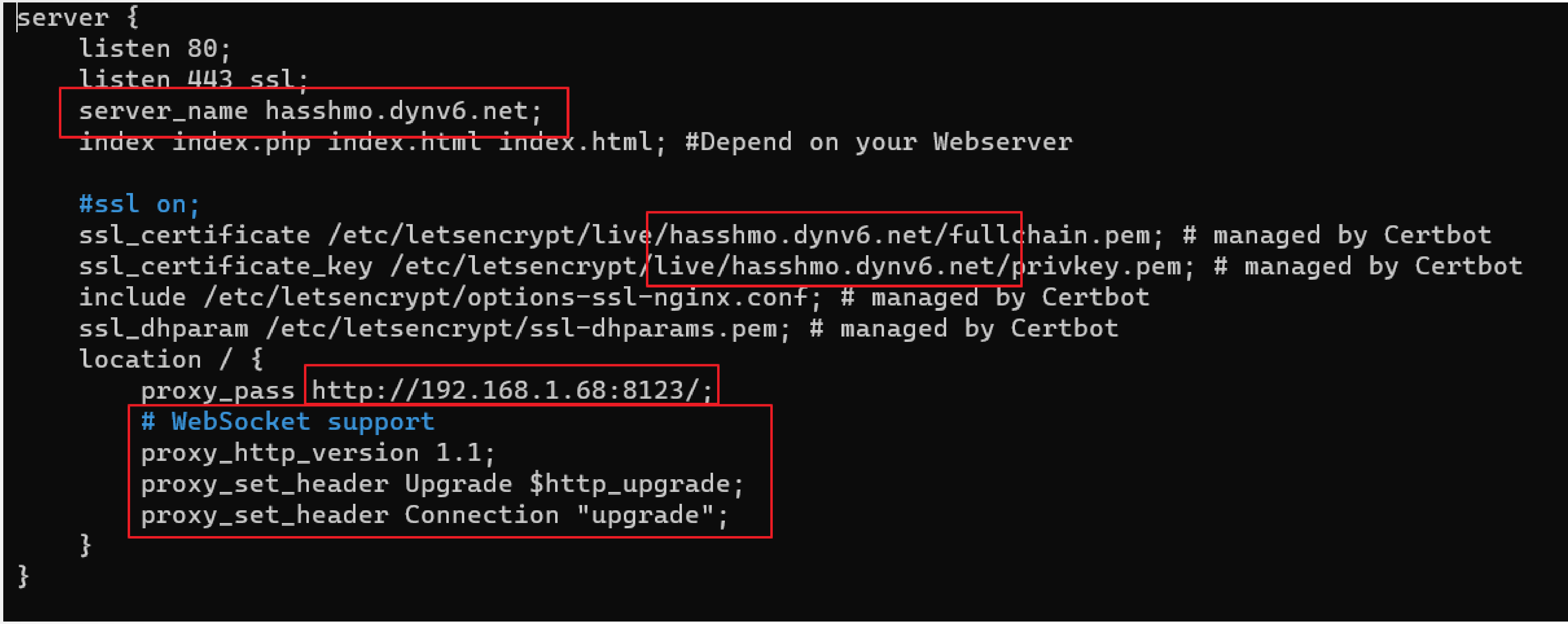


Händisch - Was ist zu tun?

- DynDns: Domain umleiten
- Router: Port 80 und Port 443 auf Raspi umgeleitet
- Raspi mit Nginx konfigurieren
  - Zertifikat anlegen
    - sudo certbot --nginx --domain hasshmo.dynv6.net
  - Config in eigene Dateien auslagern (nächste Folie)
    - /etc/nginx/sites-available
  - Softlink in sites-enabled setzen
    - ln -s /etc/nginx/sites-available/hasshmo.dynv6.net.conf ./hasshmo.dynv6.net.conf
- Nginx restarten
  - nginx -t
  - nginx -s reload

Config-Datei – Home Assistant

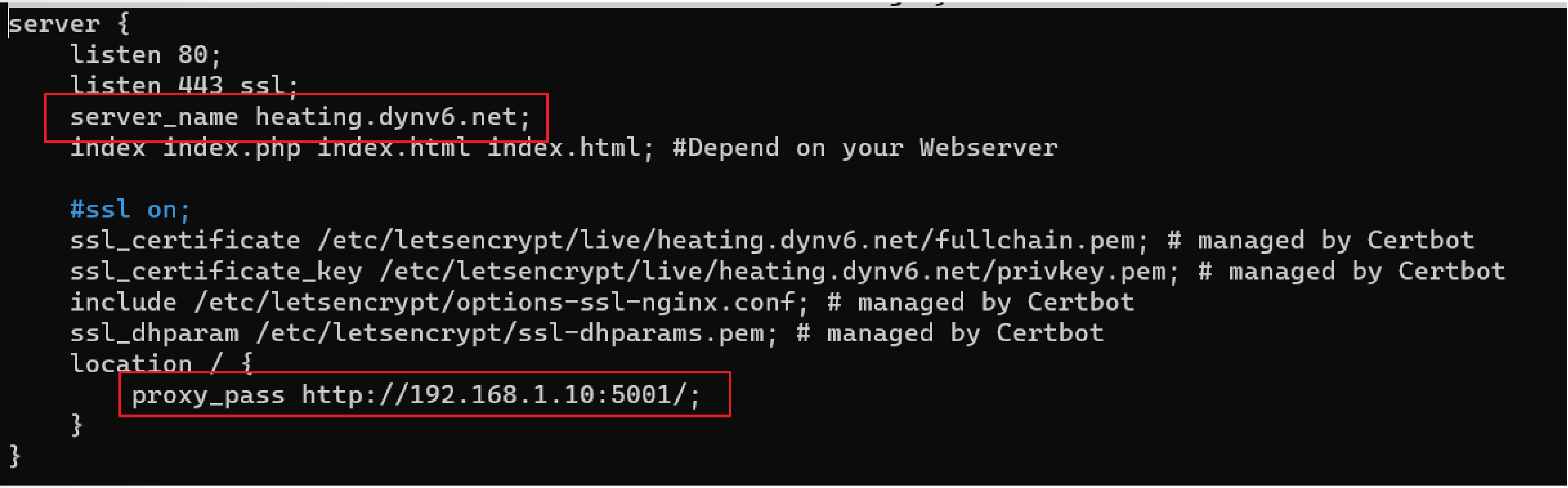
- Umleitung auf Proxmox mit lokalem Port 8123
  - Sowohl per https im Web als auch per http lokal erreichbar
- Achtung: WebSocket Support
- Auch nicht schwierig



```
server {
    listen 80;
    listen 443 ssl;
    server_name hasshmo.dynv6.net;
    index index.php index.html index.html; #Depend on your Webserver

    #ssl on;
    ssl_certificate /etc/letsencrypt/live/hasshmo.dynv6.net/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/hasshmo.dynv6.net/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
    location / {
        proxy_pass http://192.168.1.68:8123/;
        # WebSocket support
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
    }
}
```

Zweiter Host - Heizung

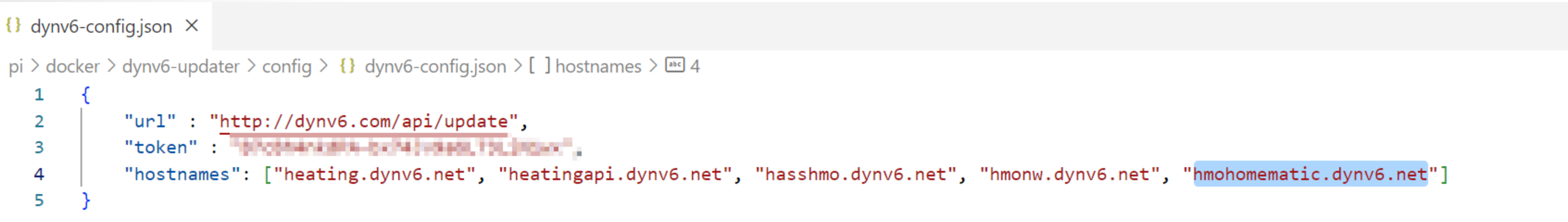
- Andere Domain
- Raspi mit DotNet Service



```
server {
    listen 80;
    listen 443 ssl;
    server_name heating.dynv6.net;
    index index.php index.html index.html; #Depend on your Webserver

    #ssl on;
    ssl_certificate /etc/letsencrypt/live/heating.dynv6.net/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/heating.dynv6.net/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
    location / {
        proxy_pass http://192.168.1.10:5001/;
    }
}
```

DynDns updaten

- Bei Änderung meiner IP-Adresse vom Provider muss dynv6 verständigt werden
  - Kleines Programm läuft gedockert


dynv6-config.json
pi > docker > dynv6-updater > config > dynv6-config.json > [ ] hostnames > 4

```
{
    "url" : "http://dynv6.com/api/update",
    "token" : [redacted],
    "hostnames": ["heating.dynv6.net", "heatingapi.dynv6.net", "hasshmo.dynv6.net", "hmonw.dynv6.net", "hmohomematic.dynv6.net"]
}
```