



# DuckDNS-Dokumentation

Vier Subdomains, automatisch gepflegt vom DSM auf DS225+. Konfiguration, Update-Mechanismus und Zusammenspiel mit Let's Encrypt.

**Stand:** Mai 2026 | **Dokument:** 2 von 4 · Domain & SSL | **Stack:** 4 Subdomains, DSM-DDNS, Let's Encrypt

Anbieter	DuckDNS (kostenlos)
Subdomains	4 (DSM-DDNS)
SSL	Let's Encrypt pro Subdomain
Update-Methode	DSM-DDNS auf DS225+
Externe Ports	443 + 80 zur DS223

## 1. Was ist DuckDNS?

DuckDNS ist ein kostenloser Dynamic-DNS-Dienst (DDNS). Er löst ein grundlegendes Problem bei Heimnetzwerken: die öffentliche IP-Adresse ist nicht statisch — bei der Telekom z.B. kann sie sich nach jeder Verbindungstrennung ändern. Ohne festen Domain-Eintrag wären die NAS-Tools von außen nicht zuverlässig erreichbar.

### Lösung

- DuckDNS stellt eine feste Subdomain zur Verfügung (z.B. **beeringdokuki.duckdns.org**)
- Hinter dieser Domain steht immer die aktuelle öffentliche IP des Routers
- Ein automatischer Update-Task aktualisiert die IP bei DuckDNS, sobald sie sich ändert
- Der Browser muss nur die Domain kennen — DuckDNS übersetzt sie immer korrekt

Aspekt	Details
Anbieter	<a href="https://www.duckdns.org">https://www.duckdns.org</a>
Kosten	Kostenlos
Anmeldung	via Google, GitHub, Reddit oder Twitter (kein eigenes Passwort)
Domain-Format	SUBDOMAIN.duckdns.org



Max. Subdomains	5 pro Account (kostenlos)
TTL DNS-Eintrag	60 Sekunden — Änderungen propagieren schnell

## 2. Vier aktive Subdomains

Im aktuellen Setup laufen vier Subdomains parallel, jede für einen anderen Dienst:

- **beeringdokuki.duckdns.org** — DMS-Tool (WebSPACE + FileStation-API + OCR), Hauptarbeitsplatz
- **beeringdrive.duckdns.org** — Synology Drive (Cloud-Ersatz)
- **beeringgrafana.duckdns.org** — Grafana-Dashboard für Monitoring
- **beeringds225.duckdns.org** — DSM-Login der DS225+ (Synology-Verwaltung)

Alle vier teilen sich das gleiche DuckDNS-Token — sie gehören zum selben DuckDNS-Account. Bei einer IP-Änderung müssen alle vier Subdomain-Einträge aktualisiert werden, was DSM zentral erledigt.

## 3. Update-Methode: DSM-DDNS auf DS225+

Seit Mai 2026 übernimmt der DSM-eigene DDNS-Updater auf der DS225+ die Aktualisierung. Früher genutzte Methoden (Cron-Skript mit **curl**, FritzBox-DynDNS) sind obsolet — siehe Migration-Hinweis am Ende.

### 3a. Anbieter "DuckDNS" anlegen

DSM unterstützt von Haus aus mehrere DDNS-Anbieter, aber DuckDNS gehört nicht zur Standardliste. Daher zuerst manuell anlegen:

- DSM → Systemsteuerung → Externer Zugriff → DDNS-Tab
- Klick auf "Anbieter anpassen"
- "Hinzufügen" mit folgenden Werten:

Feld	Wert
Dienstanbieter	DuckDNS
Query-URL	https://www.duckdns.org/update?domains=__HOSTNAME__&token=__PASSWORD__&ip=__MYIP__

### 3b. DSM-Limitation: ein Hostname pro Anbieter

**Achtung:** DSM erlaubt pro Anbieter nur einen Hostnamen. Wer mehrere Subdomains hat (wie hier vier), muss den Anbieter mehrfach anlegen.

**Workaround:** Schritt 3a wiederholen mit den Namen **DuckDNS-2**, **DuckDNS-3**, **DuckDNS-4** — die Query-URL bleibt identisch. Die Bezeichnung ist nur intern. Ergebnis: vier separate Anbieter-Einträge, alle DuckDNS-kompatibel.



### 3c. Pro Subdomain ein DDNS-Eintrag

- DSM → Externer Zugriff → DDNS → "Hinzufügen"
- Pro Subdomain einen Eintrag mit:

Feld	Wert
Dienstanbieter	DuckDNS bzw. DuckDNS-2, -3, -4
Hostname	nur die Subdomain, ohne .duckdns.org — z.B. beeringdokuki
Benutzername / Email	frei (z.B. die Login-Mail)
Kennwort	das DuckDNS-Token (36 Zeichen)
Externe Adresse	"Automatisch aus dem WAN ermitteln" lassen

### 3d. Was passiert beim Update?

- DSM ermittelt die aktuelle WAN-IP
- Vergleicht mit der zuletzt gemeldeten IP — wenn unterschiedlich, sendet GET-Request
- DuckDNS empfängt:  
**<https://www.duckdns.org/update?domains=...&token=...&ip=AKTUELL>**
- DuckDNS aktualisiert DNS-Eintrag, antwortet "OK" oder "KO"
- DSM zeigt im Status-Feld "Normal" und die externe Adresse

## 4. Status-Prüfung

In DSM → Externer Zugriff → DDNS sollte für jede Subdomain stehen:

Spalte	Erwarteter Wert
Status	Normal (grün)
Externe Adresse	aktuelle WAN-IP — muss zur Anzeige auf <a href="http://whatismyip.com">whatismyip.com</a> passen
Letzte Aktualisierung	aktueller Zeitstempel

## 5. Zusammenarbeit mit Let's Encrypt

DuckDNS und Let's Encrypt sind eng verzahnt — ohne DuckDNS-Domain gibt es kein SSL-Zertifikat. Der Ablauf bei Erst-Ausstellung oder automatischer Erneuerung:

- DSM beantragt Zertifikat für **beeringdokuki.duckdns.org**
- Let's Encrypt: "Beweise es" — ruft  
**<http://beeringdokuki.duckdns.org/.well-known/acme-challenge/XYZ>** auf
- DuckDNS übersetzt Domain → aktuelle WAN-IP → FritzBox → DS223 Port 80
- DSM antwortet korrekt auf die Challenge



- Let's Encrypt: "Domain verifiziert" → Zertifikat ausgestellt (90 Tage gültig)

**Wichtig:** Damit Let's Encrypt erneuern kann, muss Port 80 dauerhaft erreichbar sein. In der FritzBox ist Port 80 extern auf DS223:80 weitergeleitet (zusätzlich zu Port 443 auf DS223:8080).

## 6. Vollständiger Ablauf von der Domain zur Antwort

Beispiel: `https://beeringdokuki.duckdns.org/posteingang/Posteingang-KI-Tool.php` ruft auf.

### Schritt 1 — DNS-Auflösung

- Browser → "Was ist die IP von beeringdokuki.duckdns.org?"
- DuckDNS → "84.x.y.z" (aktuelle öffentliche IP des Routers)

### Schritt 2 — Verbindung zum Router

- Browser → verbindet sich mit **84.x.y.z:443**
- FritzBox → empfängt auf Port 443 → leitet weiter an **DS223:8080**

### Schritt 3 — SSL-Entschlüsselung

DSM Reverse Proxy auf DS223 empfängt verschlüsselte HTTPS-Anfrage, entschlüsselt mit Let's-Encrypt-Zertifikat und gibt als HTTP weiter an **localhost:8080** (Nginx Docker).

### Schritt 4 — Nginx-Routing

Nginx prüft den Pfad:

- `/webapi/...` → DS225+:5000 (FileStation-API)
- `/ocr/...` → DS223:5050 (Tesseract OCR)
- `/...` → DS225+:80 (Web Station)

### Schritt 5 — Web Station liefert

DS225+:80 → PHP-Engine führt **Posteingang-KI-Tool.php** aus → Antwort zurück durch dieselbe Kette zum Browser.

## 7. Fehlerbehebung

Problem	Mögliche Ursache	Lösung
Domain nicht erreichbar	IP hat sich geändert, DDNS hat nicht aktualisiert	DSM → DDNS → Status prüfen, ggf. "Aktualisieren" klicken
Domain nicht erreichbar	FritzBox-Portweiterleitung fehlt	FritzBox → Internet → Freigaben: Port 443 → DS223:8080 prüfen



HTTPS-Warnung im Browser	Zertifikat abgelaufen oder nicht zugewiesen	DSM → Sicherheit → Zertifikat erneuern bzw. zuordnen
Zertifikat-Erneuerung schlägt fehl	Port 80 nicht durchgeleitet	FritzBox → Port 80 extern → DS223:80 anlegen
DDNS-Status "Fehler"	Token oder Hostname falsch	DSM → DDNS → bearbeiten, Werte prüfen
Nur eine Subdomain aktualisiert sich	nur ein DuckDNS-Anbieter angelegt	Workaround "DuckDNS-2/-3/-4" anlegen (siehe 3b)

## 8. Migration-Hinweis (Mai 2026)

**Vorher (veraltet):** DDNS lief via Cron-Skript mit `curl`-Aufruf alle 5 Minuten oder via FritzBox-DynDNS-Slot. Nachteile: Cron lief versteckt auf einer NAS, FritzBox kann nur einen DDNS-Anbieter (Slot war für eine andere Domain belegt). Beim Wechsel auf Telekom-Glasfaser haben diese Methoden die DuckDNS-Subdomains nicht mehr aktualisiert — Tools waren von außen nicht erreichbar.

**Jetzt (Mai 2026):** Zentral via DSM-DDNS auf DS225+. Alle vier Subdomains in einer Liste sichtbar, Status pro Subdomain auf einen Blick, automatisches Polling, kein manueller Cron nötig.

## 9. Konfiguration im Überblick

Parameter	Wert
DDNS-Anbieter	DuckDNS — manuell in DSM angelegt
DDNS-Updater	DSM-DDNS auf DS225+ (Systemsteuerung → Externer Zugriff → DDNS)
Anzahl Subdomains	4 (dokuki, drive, grafana, ds225)
Workaround DSM-Limit	4 Anbieter-Einträge "DuckDNS", "DuckDNS-2", "DuckDNS-3", "DuckDNS-4"
SSL-Zertifikate	Pro Subdomain ein Let's-Encrypt-Zertifikat
Externe Ports (FritzBox)	443 (HTTPS) → DS223:8080, 80 (HTTP) → DS223:80 (für Renewal)

**Sicherheitshinweis:** Das DuckDNS-Token ist vertraulich — nicht in öffentlichen Repos veröffentlichen, nicht in Screenshots zeigen. Bei Verdacht auf Kompromittierung kann das Token im DuckDNS-Dashboard regeneriert werden — danach in allen vier DSM-DDNS-Einträgen aktualisieren.