



Wifirst Group

Handbuch für Hotspot-Router

*HOTSPLOTS Firmware ab Version 0.9.5-6023 | Stand:
01.08.2026*

Hersteller / System:

HOTSPLOTS GmbH, Berlin

Firmware-Stand:

HOTSPLOTS 0.9.5-6023

Unterstützte Hardware:

Asus RT-AX53U

Einleitung

Dieses Handbuch erläutert die Einrichtung eines WLAN-Hotspots mit einem WLAN-Router bzw. die Erweiterung eines WLAN-Hotspots durch Access Points oder Repeater. Voraussetzung ist ein Gerät, für das eine spezielle Firmware von HOTSPLOTS vorliegt. Das Handbuch behandelt zurzeit folgende Hardware:

- Asus RT-AX53U

Änderungen in der Firmware-Version HOTSPLOTS 0.9.5-6023

- PPoE-Konfigurationsoptionen aus der Benutzeroberfläche entfernt
- Dynamic-DNS-Konfigurationsoptionen aus der Benutzeroberfläche entfernt
- WLAN-Client-Isolierung standardmäßig aktiviert



Die vollständige Änderungshistorie kann unter <https://www.hotspots.de/support/downloads/firmware/changelog.html> eingesehen werden.

1. Anschließen und Einrichtung

Der Hotspot-Router betreibt das Hotspot-Portal, verteilt IP-Adressen an Clients und steuert den Internetzugriff. Der Hotspot Router verfügt über kein Modem. Es ist erforderlich das Gerät an ein Modem oder Router mit bestehender Verbindung ins Internet anzuschließen.

1.1 Anschluss des Admin-PCs zur Konfiguration

Stellen Sie die IP-Adresse Ihres PCs auf 192.168.1.2 ein und verbinden Sie ihn mit einem der LAN-Ports (1-3) des Routers. Die Administrationsoberfläche ist unter <http://192.168.1.1:8080/> erreichbar.

1.2 Anschluss hinter einem bestehenden (DSL-)Router

Verbinden Sie den WAN-Port des Hotspot-Routers mit einem LAN-Port Ihres Hauptrouters. Wenn der Hauptrouter IP-Adressen per DHCP vergibt, wählen Sie als WAN-Konfiguration 'DHCP (automatisch)'.

Achtung möglicher Subnetz-Konflikt

Die per DHCP bezogene IP-Adresse am WAN-Port muss in einem anderen Subnetz liegen als die LAN-IP (192.168.1.1). Zudem dürfen die Bereiche 192.168.44.1 bis 192.168.47.254 nicht für das WAN/LAN verwendet werden, da diese für Hotspot-Clients reserviert sind.

1.3 Überprüfen der Internet-Verbindung

Klicken Sie auf der Status-Seite auf den Button 'Internetverbindung überprüfen'. Bei korrekter Anbindung wird eine grüne Bestätigungsmeldung angezeigt.

1.4 Konfiguration als Hotspot-Router

- **1. Betriebsmodus:** Stellen Sie die Betriebsart auf 'Hotspot Router (ohne APs)' oder auf 'Hotspot Router (mit Aps/Repeater)'.
ACHTUNG: Bei der Betriebsart 'Hotspot Router (ohne APs)' ist eine Internetverbindung ohne VPN und Captive Portal über die LAN - Ports möglich. Wir raten zur Verwendung des Betriebsmodus 'Hotspot Router (mit Aps/Repeater)'.
- **2. Hotspot einrichten:** Unter dem Menüpunkt Netzwerk → HOTSPLOTS Hotspot muss der Hotspotname und der im Kundenbereich hinterlegt Schlüssel eingetragen werden. Durch 'Name und Schlüssel prüfen' wird überprüft ob diese Eingaben korrekt sind. Abschlossen wird der Vorgang durch 'Übernehmen'. Der Router ist nun mit unseren VPN Servern verbunden und kann benutzt werden.
- **3. SSID anpassen:** Unter Netzwerk → WLAN / Funknetz wird die SSID eingerichtet.

2. Erweiterung mit Hotspot-Repeatern oder Access Points

Das Netz lässt sich durch Access Points (per Netzkabel) oder Repeater (per WLAN) erweitern.

Wichtige Systemkonfiguration

Setzen Sie den Betriebsmodus des Haupt-Hotspot-Routers unter 'Netzwerk' auf 'Hotspot Router (mit APs/Repeater)'. Dadurch werden WLAN- und LAN-Interface gebrückt, was den Anschluss weiterer Access Points ermöglicht.

2.2 Konfiguration als Access Point (kabelgebunden)

- **1. Betriebsmodus:** Stellen Sie die Betriebsart auf der Netzwerk-Status-Seite auf 'Access Point'.
- **2. Verkabelung:** Schließen Sie das Netzkabel an einen der LAN-Ports an (der WAN-Port bleibt ungenutzt).
- **3. SSID-Roaming:** Vergeben Sie für den AP dieselbe SSID wie am Hotspot-Router, um nahtloses Roaming zu ermöglichen.
- **4. DHCP:** Der DHCP-Server am LAN-Port wird im AP-Modus automatisch deaktiviert und darf nicht manuell aktiviert werden.

2.3 Konfiguration als WLAN-Repeater

- **1. Betriebsmodus:** Stellen Sie die Betriebsart auf 'Repeater'.
- **2. Funkeinstellungen:** Unter Netzwerk >> WLAN / Funknetz stellen Sie Kanal, Bandbreite und SSID exakt auf die Daten des abzudeckenden Funknetzes ein. Alternativ kann der Repeater an die MAC - Adresse der SSID des Hotspot Routers verbunden werden.
- **3. Voraussetzung:** Beim Haupt-Hotspot-Router muss die Option 'Repeater erlauben' aktiviert sein.

3. Firmware-Menüpunkte im Überblick

3.1 Status-Seite

Zeigt Hardware-Modell, Firmware-Version, Systemzeit (via NTP), Betriebsart, IP/MAC-Adressen von WAN/LAN sowie den Hotspot-Status und VPN-Routing-Zustand an.

3.2 Netzwerk

- **WAN:** WAN / Internetanbindung: Auswahl zwischen DHCP (automatisch), Statisch oder Aus. Enthält zudem Einstellungen den Jugendschutzfilter.
- **LAN:** LAN / Lokales Ethernet: Einstellung der statischen IP (Standard 192.168.1.1). Ermöglicht die Konfiguration des lokalen DHCP-Servers für LAN-Clients.

- **WLAN:** WLAN / Funknetz: Einstellung von Kanal, Bandbreite (20 MHz empfohlen), Sendeleistung (10-100 mW, max. 20 dBm EIRP) und Hotspot-SSID. Zudem kann ein zusätzliches 'Privates WLAN' eingerichtet werden.
- **Hotspot:** HOTSPLOTS Hotspot: Eingabe von Hotspot-Name und -Schlüssel zur Authentifizierung am Server. Konfiguration von 'Freien Webseiten' (Walled Garden), 'Freien Domains' und 'Freien MAC-Adressen'.
- **VPN:** VPN-Routing: Leitet den gesamten Hotspot-Datenverkehr verschlüsselt über HOTSPLOTS-Server in Frankfurt/Berlin um. Bietet Rechtssicherheit und Betreiberschutz.

3.3 Sicherheit & Firewall

- **Zugang:** Systemzugang: Verwaltung von Admin-Passwort sowie Freigabe der Zugangswege für Webinterface und SSH (über LAN, WLAN, WAN oder VPN-Routing).
- **Firewall:** Firewall & Portweiterleitungen: Konfiguration von Port-Forwarding (z.B. Port 8282 auf IP 192.168.1.2:8080 für Fernwartung von APs) sowie Definieren von Zugriffsausnahmen für Hotspot-Clients.

3.4 Administration

- **Update:** Firmware Update: Direktes Online-Update über HOTSPLOTS-Server oder manueller Upload einer Firmware-Datei.
- **Sicherung:** Konfiguration sichern / wiederherstellen: Export und Import aller Systemeinstellungen als Sicherungsdatei.
- **Diagnose:** System-Log & Prozesse: Einsicht in Systemmeldungen, CPU- und Speicherauslastung.

4. Administration über SSH

Für fortgeschrittene Anwender stehen auf der Befehlszeile nützliche Diagnose-Tools zur Verfügung:

- **ifconfig:** Zeigt aktive Netzwerk-Schnittstellen und Konfigurationen an.
- **top:** Zeigt laufende Prozesse und Systemlast in Echtzeit an.
- **uptime:** Gibt die Systemlaufzeit seit dem letzten Neustart aus.
- **fping:** Scannt ein Subnetz nach aktiven IP-Adressen (z.B. `fping -asqq 192.168.1.0/24`).
- **logread:** Gibt das aktuelle System-Log aus.

5. Troubleshooting / Fehlersuche

5.1 Administrationsoberfläche lässt sich nicht aufrufen

- **1.** Verkabelung prüfen: Ist der PC an einen LAN-Port (1-4) angeschlossen?
- **2.** Netzwerkkarte prüfen: Auf statische IP 192.168.1.2 einstellen.
- **3.** Reset durchführen: Reset-Knopf im laufenden Betrieb 8 Sekunden gedrückt halten, um das Gerät auf Werkseinstellungen (192.168.1.1:8080) zurückzusetzen.

5.2 WLAN sichtbar, aber keine Loginseite

- **1.** Prüfen Sie, ob der Hotspot-Router eine funktionierende Internetverbindung hat.
- **2.** Stellen Sie sicher, dass die WLAN-Karte des Endgeräts auf automatischen IP-Bezug (DHCP) eingestellt ist. Der Client muss eine IP im Bereich 192.168.44.x - 192.168.47.x erhalten.

5.3 Internetzugriff ohne Loginseite

- **1.** Falls per LAN verbunden: Prüfen, ob der Router in der Betriebsart 'Hotspot Router (ohne APs)' läuft.
- **2.** Prüfen, ob der Client noch eingeloggt ist (Logout-Seite aufrufen unter <http://logout.hotspots.de>).

6. Richtlinien zur Hotspot-Installation

6.1 IT-Sicherheit

- **Passwortschutz:** Ändern Sie Standard-Passwörter unverzüglich. Verwenden Sie für den Hotspot-Router ein anderes Passwort als für nachgelagerte APs.
- **Client-Isolierung:** Die netzweite Client-Isolierung verhindert den direkten Zugriff von Gast-Geräten untereinander.
- **Netztrennung:** Das lokale Firmen-/Büronetz wird durch automatische Firewall-Regeln vor Zugriffen aus dem Hotspot-Netz geschützt.
- **Idle-Timeout:** Für öffentlich zugängliche Terminals kann ein Idle-Timeout (z.B. 60 Sekunden ohne Traffic) eingerichtet werden.

6.2 Physikalische Sicherheit & Entstörung

- **Aufstellung:** Positionieren Sie Access Points erhöht und geschützt vor Vandalismus, Feuchtigkeit und Diebstahl. Outdoor-Antennen benötigen entsprechenden Blitzschutz.
- **Monitoring:** Tragen Sie im Kundenbereich unter 'Admin Kontakt' eine aktuelle E-Mail-Adresse ein, um automatische Störungsmeldungen des Monitoring-Systems zu erhalten.

7. Impressum & Support

hotspots GmbH, Köpenicker Str. 154A (Aufgang B), 10997 Berlin
Amtsgericht Charlottenburg HRB 93460B
Geschäftsführung: Sascha Schaub, Pierre Fau