

# Handbuch für Hotspot-Router mit Firmware ab 3.0-6009



Stand der Firmware: HOTSPLOTS 3.0-6009  
Stand: 29.10.2021

## Inhaltsverzeichnis

Handbuch für Hotspot-Router mit Firmware ab 3.0-6009.....	1
Einleitung.....	2
Wesentliche Änderungen in der Firmware-Version 3.0-6009.....	2
1 Installation der Firmware.....	2
1.1 TP-LINK C7 v5.....	2
1.2 Edge Router X.....	2
2 Anschließen des Hotspot-Routers.....	4
2.1 Anschluss des Admin-PCs zur Konfiguration.....	4
2.2 Anschluss an DSL-Modem.....	5
2.3 Anschluss hinter (DSL-)Router.....	6
2.4 Überprüfen der Internet-Verbindung.....	7
3 Erweiterung mit Hotspot-Repeatern oder Access Points.....	8
3.1 Konfiguration als Access-Point zum Anschluss per Netzkabel.....	8
3.2 Konfiguration als WLAN-Repeater.....	9
4 Die Firmware-Menüpunkte im Überblick.....	11
4.1 Die Status-Seite.....	11
4.2 Netzwerk.....	11
WAN / Internetanbindung.....	11
LAN / lokales Ethernet.....	12
WLAN / Funknetz.....	13
HOTSPLOTS Hotspot.....	15
4.3 Sicherheit.....	16
Firewall.....	17
4.4 Administration.....	17
Firmware Update.....	17
Konfiguration sichern.....	17
Neustart.....	18
System-Log.....	18
Prozesse.....	18
Diagnose.....	18
System Information.....	18
5 Administration über ssh.....	18
5.1 Nützliche Linux-Befehle.....	18
6 Troubleshooting / Fehlersuche.....	19
6.1 Die Administrationsoberfläche lässt sich nicht aufrufen.....	19
6.2 Man sieht das WLAN, aber die Loginseite wird nicht angezeigt.....	19
6.3 Man kommt ohne Loginseite ins Internet.....	19
7 Richtlinien zur Hotspot-Installation.....	19
7.1 IT-Sicherheit.....	19
Schutz des Hotspots vor unberechtigtem Zugriff.....	19
Schutz der Nutzer durch netzweite Client-Isolierung.....	20
Schutz des vorhandenen Netzes vor Hotspot-Nutzern.....	20

Idle-Timeout für Terminals.....	20
7.2 Physikalische Sicherheit.....	20
7.3 Entdecken von Störungen.....	20
7.4 Beheben von Störungen.....	21
7.5 Maßnahmen zum Beenden des Hotspot-Angebotes.....	21
8 Anhang 1: Trennung von Clients via VLAN.....	21
9 Impressum/Support/Kontakt.....	21

## 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 zur Zeit folgende Hardware:

- Edge Router X
- TP-Link C7 v5

## Wesentliche Änderungen in der Firmware-Version 3.0-6009

- Hotspot Netzwerk auf /22 erweitert.
- Jugendschutzfilter wurde auf neue Server umgestellt

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

## 1 Installation der Firmware

### 1.1 TP-LINK C7 v5

Der Router kann momentan über tftp(bei Original Firmware) als auch über HOTSPLOTS Webinterface bei Firmware unter 6009 geflasht werden:

1. Vorbereitung: Für das Flashen über TFTP muss ein squashfs-factory Image verwendet werden
2. Die Firmware Dateien müssen unter Linux in das Verzeichnis /srv/tftp geschoben werden
3. Für den TP-Link C7 v5 muss der Dateiname auf ArcherC7v5\_tp\_recovery.bin geändert werden
4. Nun muss die IP Adresse der LAN-Schnittstelle des Computers auf die IP 192.168.0.66 eingestellt werden
5. Unter Linux wäre dies mit folgendem Befehl möglich:  

```
sudo atftp --bind-address 192.168.0.66 --port 69 --daemon /srv/tftp/
```
6. Im Anschluss wird beim Router die WPS/Reset Taste während des Starts gehalten, bis die Sync LED leuchtet.
7. Sobald der Router sich die neue Firmware installiert hat, ist er wieder betriebsbereit. Er ist nun unter der Webadresse <http://192.168.1.1:8080> erreichbar. Die Benutzerdaten lauten wie folgt:

Benutzer: **root**

Passwort: **admin**

### 1.2 Edge Router X

Der Router kann sowohl über SSH als auch über Webinterface mit der Firmware von HOTSPLOTS geflasht werden:

## 1. Flashen über SSH

1. Vorbereitung: Für das Flashen über SSH muss ein squashfs-factory Image verwendet werden.
2. Schließen Sie den Router mithilfe eines LAN-Kabels an den Computer an.
3. Weisen Sie auf ihrem Computer der Netzwerkschnittstelle, die mit dem Router verbunden ist, eine statische IP im Bereich 192.168.1.x/24 zu, da sich der Router im Default unter der IP 192.168.1.1/24 auffinden lässt (Beispiel 192.168.1.2).
4. Testen Sie ob eine Verbindung möglich wäre, indem sie das Kommando „ping“ benutzen.

```
~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) Bytes Daten.
64 Bytes von 192.168.1.1: icmp_seq=1 ttl=64 Zeit=0.271 ms
64 Bytes von 192.168.1.1: icmp_seq=2 ttl=64 Zeit=0.366 ms
64 Bytes von 192.168.1.1: icmp_seq=3 ttl=64 Zeit=0.351 ms
64 Bytes von 192.168.1.1: icmp_seq=4 ttl=64 Zeit=0.337 ms
```

Abbildung 1: Ping als Test ob man den Router sieht

5. Kopieren Sie das Firmware Image per scp-Befehl auf den Router.  
Beispiel-Befehl für die Version 6009 (Hinweis: Es ist nur eine Zeile):  
`scp /path/to/Firmware/hotspots-3.0-6009-ramips-mt7621-ubnt-erx-squashfs-factory-compat.tar ubnt@192.168.1.1:/tmp/`  
Syntax: `scp Pfad_zur_Firmware Hostname@IP:/Pfad_in_dem_abgelegt_werden_soll`
6. Ist das Firmware Image auf den Router geladen, so begeben sie sich via ssh-Befehl auf den Router:  
`ssh ubnt@192.168.1.1`  
Das Passwort für ubnt ist ebenfalls „ubnt“.
7. Auf dem Router angekommen, begeben sie sich mittels des Befehls `cd` in den Ordner `/tmp`.  
Befehl: `cd /tmp`
8. Nun sollte die Konsole „ubnt@ubnt:/tmp“ anzeigen. Fügen sie nun das Firmware-Image hinzu.  
Befehl: `add system image hotspots-3.0-6009-ramips-mt7621-ubnt-erx-squashfs-factory-compat.tar`  
Syntax: `add system image Firmware_Name`
9. Überprüfen Sie, ob das Firmware Image korrekt installiert wurde.  
Befehl: `show system image`

## 2. Flash über Webinterface

1. Schließen sie den Router mithilfe eines LAN-Kabels an den Computer an.
2. Weisen Sie auf ihrem Computer der Netzwerkschnittstelle, die mit dem Router verbunden ist, eine statische IP im Bereich 192.168.1.x/24 zu, da sich der Router im Default unter der IP 192.168.1.1/24 auffinden lässt (Beispiel 192.168.1.2).
3. Testen sie ob eine Verbindung möglich wäre indem sie das Kommando „ping“ benutzen.

```
~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) Bytes Daten.
64 Bytes von 192.168.1.1: icmp_seq=1 ttl=64 Zeit=0.271 ms
64 Bytes von 192.168.1.1: icmp_seq=2 ttl=64 Zeit=0.366 ms
64 Bytes von 192.168.1.1: icmp_seq=3 ttl=64 Zeit=0.351 ms
64 Bytes von 192.168.1.1: icmp_seq=4 ttl=64 Zeit=0.337 ms
```

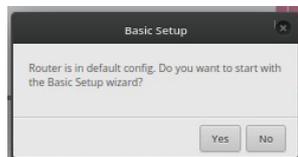
Abbildung 2: Ping als Test ob man den Router sieht

4. Ist dies erfolgreich , starten Sie einen Webbrowser ihrer Wahl. Es wird keine zusätzlich mitgelieferte Software benötigt.
5. Rufen Sie die IP 192.168.1.1 auf, indem Sie diese Adresse in Ihre Adress-Leiste schreiben.
6. Auf der Seite angekommen, loggen sie sich mit dem Default User und Passwort ein:  
 Username: **ubnt**  
 Passwort: **ubnt**



*Abbildung 3: Login Edge Router*

7. Setzen sie einen Haken zum akzeptieren der ToS
8. Brechen Sie den sogenannten Wizard mit einem Klick auf Nein(No) ab



*Abbildung 4: Abbruch Installations-Wizard*

9. In der Leiste am unteren Bildschirmrand finden sie den Reiter „System“, öffnen Sie diesen und wählen Sie Punkt aus: „Upgrade System Image“  
 Laden sie die Firmware, welche sie von unserer Webseite heruntergeladen haben, dort hoch und lassen sie den Router den Rest erledigen.
10. Nach einem Neustart ist der Router mit der HOTSPLOTS Firmware unter der Webadresse <http://192.168.1.1:8080/> erreichbar und kann weiter konfiguriert werden. Die Zugangsdaten sind wie folgt:

Benutzer: **root**  
 Passwort: **admin**

## 2 Anschließen des Hotspot-Routers

Mit Hotspot-Router wird der (WLAN-)Router bezeichnet, auf dem das Hotspot-Portal (chilli), die eigentliche Hotspot-Funktion, läuft. Dieser Router verteilt die IP-Adressen an die Funk-Clients und überwacht den Zugriff auf das Internet.

Es gibt keinen Router mit integriertem DSL-Modem, auf dem eine passende Firmware stabil läuft (Stand Oktober 2021). Bei VDSL-, ADSL- oder auch Kabel-Anschlüssen ist für die Verbindung zum Internet ist daher entweder ein weiterer Router mit eingebautem Modem (z. B. eine Fritz!Box) oder ein Modem notwendig.

### 2.1 Anschluss des Admin-PCs zur Konfiguration

Stellen Sie die Netzwerkverbindung Ihres PCs auf die IP-Adresse 192.168.1.2 ein und verbinden Sie die so konfigurierte Netzwerkkarte per Netzwerkkabel mit einem der LAN-Ports „1-4“ des Routers.

Die Administrationsoberfläche erreichen Sie mit Ihrem Webbrowser über die URL <http://192.168.1.1:8080/>. Anschließend werden Sie nach Nutzernamen und Passwort gefragt. Der Standardwert für den Nutzernamen ist **root** und für das Passwort **admin**.

Dann sollten Sie die Startseite der Administrationsoberfläche sehen.

Firmware Version 3.0-6009



Router Status	
Router Hardware	TP-LINK Archer C7 v5
Zeit	Thu Oct 14 10:02:17 CEST 2021
Uptime	00h 55min 18s
Firmware	hotsplotsWrt-3.0-6009
Webinterface Version	1.0
Betriebsart	Hotspot Router (ohne APs)
WAN / Internet	28:EE:52:62:6F:D0 eth0.2 dhcp 192.168.3.136
LAN / Ethernet	28:EE:52:62:6F:D0 eth0.1 static 192.168.1.1
WLAN SSID	HOTSPLOTS_test HOTSPLOTS_test
Hotspotname	musterGateway (eingeloggte Nutzer: 0)
VPN-Routing	ja
VPN-Routing aktiv.	

Abbildung 5: Status-Seite des Webinterfaces

## 2.2 Anschluss an DSL-Modem

Zum Internet erfolgt der Anschluss des Hotspot-Routers über den WAN-Port, der sich auf der Rückseite des Routers befindet (TP-LINK: blaue Buchse, Edge Router X: ETH 1)

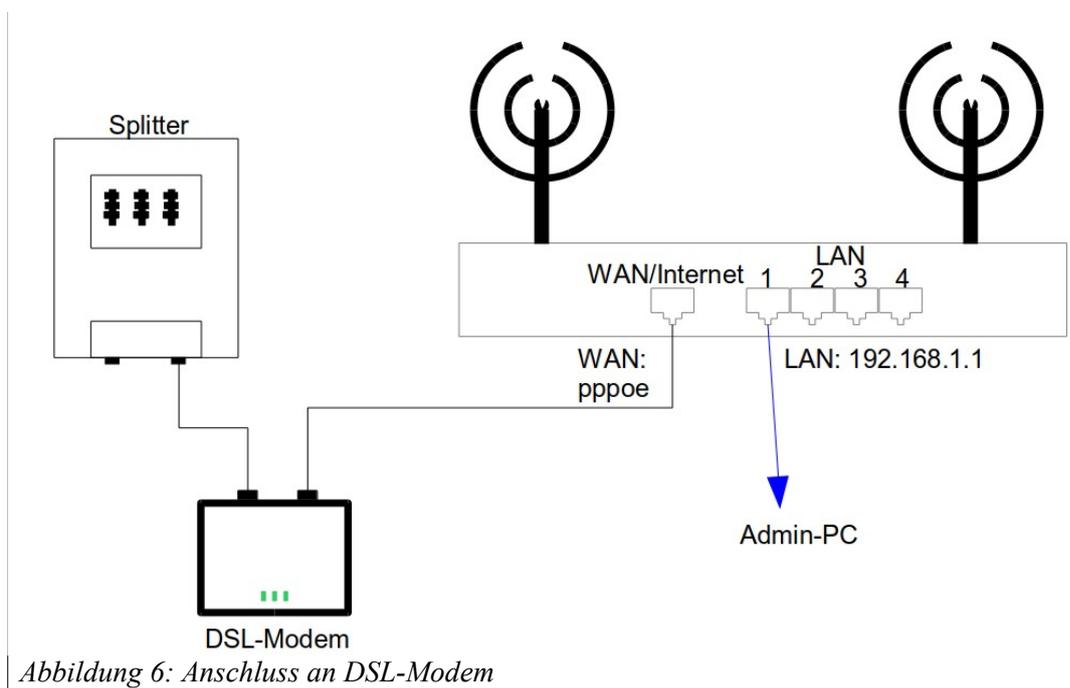


Abbildung 6: Anschluss an DSL-Modem

Wenn der Router per Netzkabel an ein DSL-Modem angeschlossen wird, müssen auf dem Hotspot-Router die DSL-Zugangsdaten hinterlegt werden. Gehen Sie dafür auf den Menüpunkt Netzwerk >> WAN / Internetanbindung (siehe Abb. 7) . Wählen Sie dort „PPPoE (über DSL-Modem)“ aus. Die Seite wird dann neu aufgebaut und Eingabefelder für DSL-Nutzername und DSL-Passwort erscheinen.

Tragen Sie dort die Daten ein, die Sie von Ihrem DSL-Provider bekommen haben. Falls Ihr Anbieter Ihnen zwar einen Nutzernamen (z. B. Ihre Telefonnummer) aber kein Passwort mitgeteilt hat, kann es sein, dass die Einwahl nicht funktioniert, wenn Sie das Feld leer lassen; tragen Sie in dem Fall irgendetwas ein.

Defaultmäßig ist als Verbindungsart „permanent“ ausgewählt. Dies ist zu empfehlen, da der Router so eine kontinuierliche Verbindung zum Internet und zu unseren VPN-Servern aufrechterhalten kann. Sollten Sie eine Internetanbindung haben, die zeitbasiert abgerechnet wird, achten Sie bitte darauf, dass Ihnen durch die permanente Anbindung Kosten entstehen können.



Abbildung 7: Eingabe der DSL-Zugangsdaten

## 2.3 Anschluss hinter (DSL-)Router

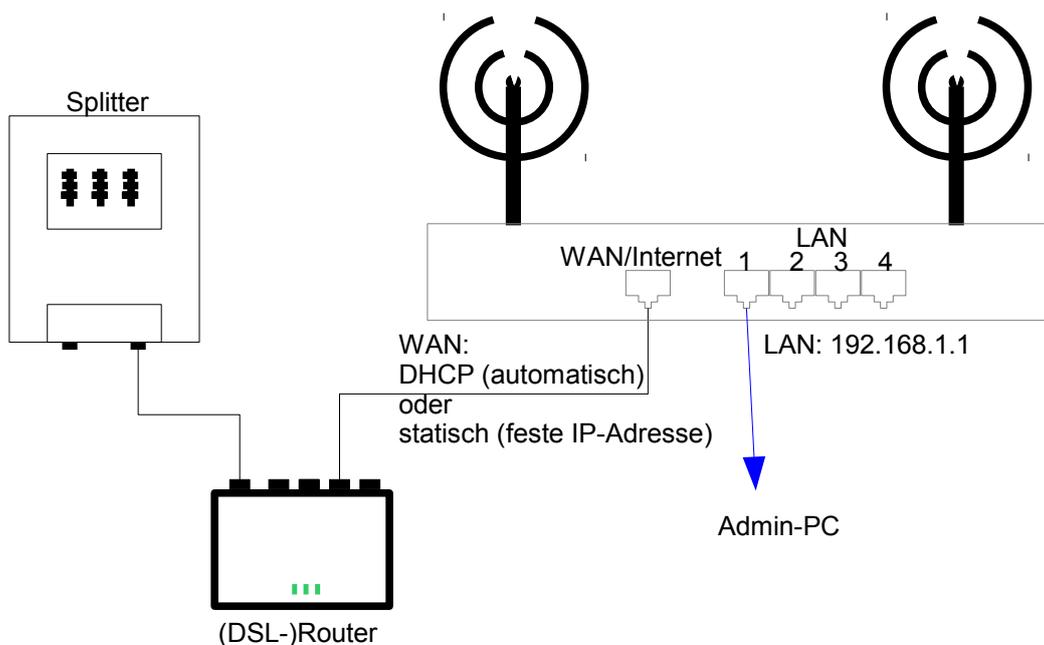


Abbildung 8: Anschluss an (DSL-)Router

Zum Internet erfolgt der Anschluss des Hotspot-Routers über den WAN-Port, der sich auf der Rückseite des Routers befindet (TP-LINK: blaue Buchse, Edge Router X: ETH 1).

Wenn der Hotspot-Router in ein bestehendes LAN integriert oder an einen Internet-Router angeschlossen werden soll, so verbinden Sie den WAN-Port des Hotspot-Routers mit einem LAN-Port Ihres Internet-Routers bzw. mit einem damit verbundenen Switch, siehe 8.



Abbildung 9: Standardeinstellung für den WAN-Port: DHCP (automatisch)

Wenn Ihr Internet-Router per DHCP automatisch IP-Adressen zuweist, dann können Sie die Standardeinstellung für Internet (WAN) „DHCP (automatisch)“ stehen lassen und müssen nichts weiteres eintragen, siehe Abb. 9.

Dabei ist jedoch darauf zu achten, dass die per DHCP bezogene IP-Adresse des WAN-Ports in einem anderen Subnetz liegen muss als die IP-Adresse des LAN-Ports. Sonst funktioniert das Routing nicht, der Router kommt nicht ins Internet und kann auch keine IP-Adressen an WLAN-Clients verteilen. Sollte dieser Fehler auftreten, kann er leicht durch Ändern der LAN-IP-Adresse beseitigt werden, etwa durch Ersetzen von 192.168.1.1 durch 192.168.43.1.

## 2.4 Überprüfen der Internet-Verbindung

Die Internetverbindung kann auf der Status-Seite mit dem Button „Internetverbindung prüfen“ geprüft werden. Es wird nur die Internetverbindung über den WAN-Port geprüft. Bei Repeatern, die per WLAN angebunden sind oder kabelgebundenen Access Points funktioniert die Prüfung über das Webinterface nicht.



Abbildung 10: Kontaktierung eines HOTSPLOTS Servers zum Überprüfen von Internetzugang und Einstellungen

Alternativ geht es unter dem Menüpunkt Netzwerk >> HOTSPLOTS Hotspot: Wenn der Hotspot funktioniert und das kann er nur, wenn die Internetverbindung in Ordnung ist, dann steht dort unten auf der Seite in grüner Schrift „Der Hotspot ist korrekt bei unseren Servern registriert und kann mit diesen Einstellungen verwendet werden.“. Durch Anklicken des Buttons „Name & Schlüssel prüfen“ können Sie eine Verbindung mit einem Server von HOTSPLOTS herstellen und nebenbei die Angaben unter Hotspot-Name und Schlüssel überprüfen. Wenn der Router keine Internetverbindung hat, kommt nach einiger Zeit die Meldung „... Der Hotspot ist nicht korrekt registriert. Entweder ist kein Hotspot unter diesem Namen bei uns angemeldet, oder der Schlüssel ist falsch eingetragen.“

### 3 Erweiterung mit Hotspot-Repeatern oder Access Points

Es ist möglich, das vorhandene Netzwerk durch Hinzunahme weiterer Router zu erweitern:

1. Empfehlenswert ist der Anschluss sog. Access Points per Netzwerkkabel an den LAN-Ports des Hotspot-Routers.
2. Die Funkbereiche von WLAN-Router und Access Points können durch Einsatz weiterer Access Points im Repeater-Modus vergrößert werden.

Alle notwendigen Einstellungen können auf der Admin-Oberfläche der HOTSPLOTS Firmware vorgenommen werden.

**WICHTIG:** Wenn das Netzwerk um zusätzliche Accesspoints oder Repeater erweitert werden soll, stellen Sie bitte unter dem Menüpunkt Netzwerk den Betriebsmodus des Hotspot-Routers auf den Wert „Hotspot Router (mit APs/Repeater)“. Hierdurch werden das WLAN-Interface und das LAN-Interface miteinander gebrückt. Um an den Hotspot-Router weitere APs oder Repeater anzuschließen, ist dieser Betriebsmodus erforderlich. Des Weiteren empfehlen wir, allen Access Points und Repeatern im Netzwerk eine LAN-IP im selben Subnetz zu geben, um diese später über das Netzwerk administrieren zu können. Alle notwendigen Einstellungen können auf der Administrationsoberfläche der HOTSPLOTS Firmware vorgenommen werden.

#### 3.1 Konfiguration als Access-Point zum Anschluss per Netzwerkkabel

Grundsätzlich kann jeder standardkonforme Access Point an den Hotspot-Router angeschlossen werden. Wichtig ist, dass es sich wirklich um einen Access Point also eine Brücke (Bridge) zwischen WLAN und LAN handelt und nicht um einen Router, der selbst die Funktion des NAT (Network Address Translation) übernimmt. Anleitung und Support können wir natürlich nur für Geräte mit der HOTSPLOTS eigenen Firmware oder anderen bei HOTSPLOTS gekauften Access Points leisten.

Um den Router als Access Point zu betreiben, muss der Betriebsmodus umgestellt werden. Dazu wird auf der Netzwerk-Status-Seite (Netzwerk) der Betriebsmodus „Access Point“ gewählt. Nach dem automatischen Neustart arbeitet der Router als Access Point.

Netzwerk Status	
Betriebsart [?]	Access Point
WAN / Internet	28:EE:52:62:6F:D0 eth0.2 dhcp 192.168.3.136
LAN / Ethernet	28:EE:52:62:6F:D0 eth0.1 static 192.168.1.1
WLAN SSID	HOTSPLLOTS_test HOTSPLLOTS_test
Hotspotname	musterGateway
VPN-Routing	ja

Abbildung 11: Einstellung für kabelgebundene Access Points (APs)

**HINWEIS:** Die Verbindung zum Router per Netzwerkkabel muss wie in 12 skizziert über einen der **LAN-Ports** erfolgen! Der WAN-Port ist in dieser Konfiguration vollkommen irrelevant. Am besten stellen Sie ihn auf "DHCP (automatisch)" oder auf "nicht genutzt (aus)", dann kann es nicht zu Konflikten mit den IP-Bereichen von LAN und WLAN kommen.

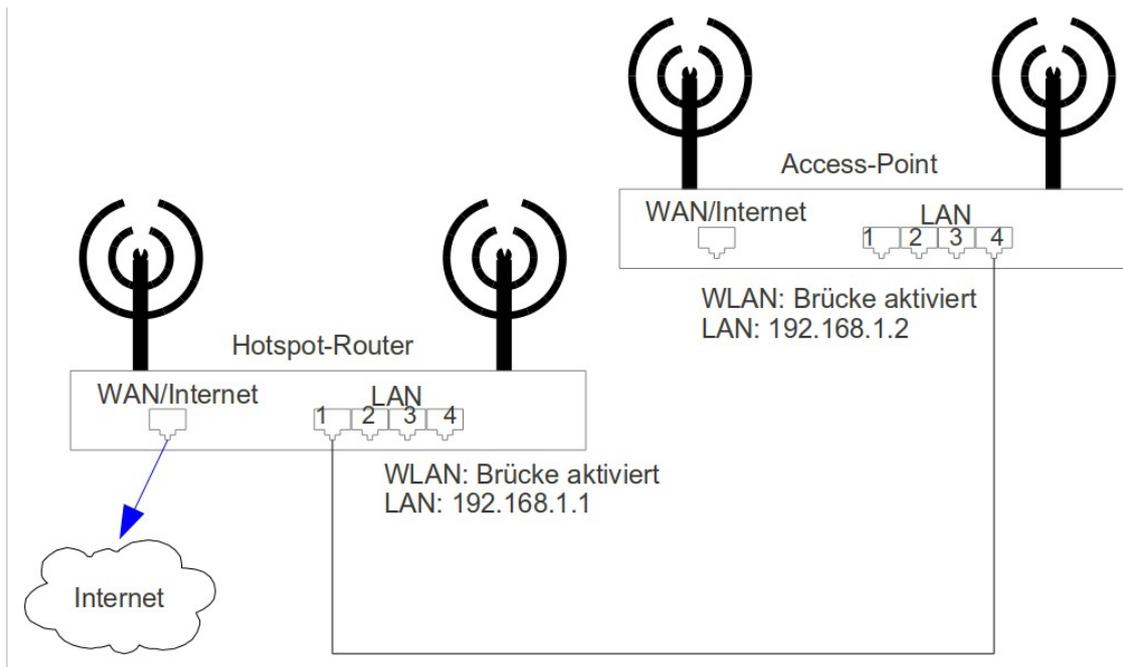


Abbildung 12: Anschluss an (DSL-)Router

**TIPP:** Wenn Sie für den Access-Point dieselbe SSID eintragen wie für den Hotspot-Router, dann können Sie sich ohne Verbindungsabbruch mit dem Notebook vom Empfangsbereich des einen in den des anderen bewegen.

**TIPP:** Zu Wartungszwecken wird die LAN-Adresse statisch konfiguriert. Dann können Sie sich vom Hotspot-Router per ssh darauf einloggen. Eine Fernwartung ist möglich, indem man sich per ssh zuerst auf dem Hotspot-Router einloggt und von dort aus auf den weiteren Access Points bzw. Repeatern.

**Achtung:** Beim Aktivieren des Betriebsmodus „Access Point“ wird automatisch der DHCP-Server unter LAN deaktiviert. Dieser darf nicht manuell wieder angeschaltet werden!

### 3.2 Konfiguration als WLAN-Repeater

Repeater reduzieren die effektive Bandbreite in WLANs! Daher ist es vorteilhafter, mit Access Points zu arbeiten. Um den Router als Repeater zu betreiben, muss der Betriebsmodus umgestellt werden. Dazu wird auf der Netzwerk-Status-Seite (Netzwerk) der Betriebsmodus „Repeater“ gewählt. Bitte beachten Sie, dass sich Hotspot-Router als auch der Repeater im selben WLAN-Netzwerk befinden müssen. Nach dem automatischen Neustart arbeitet der Router als Repeater.

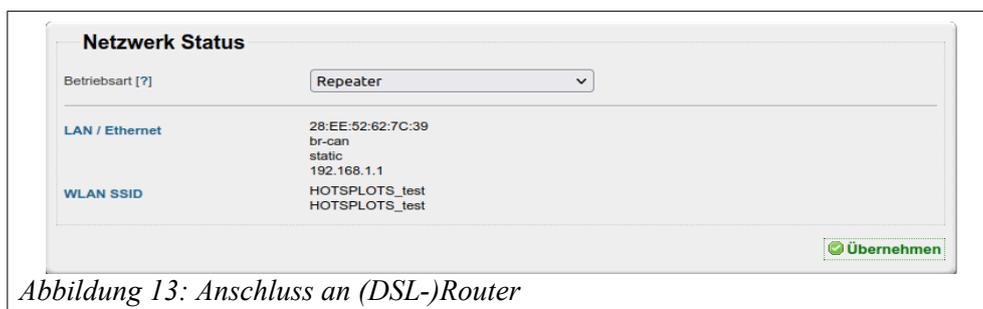


Abbildung 13: Anschluss an (DSL-)Router

Um den Repeater auf das Funknetz einzustellen, wählen Sie die Seite „Netzwerk >> WLAN / Funknetz“. Tragen Sie dort im oberen Feld „Funkeinstellungen Repeater“ die Einstellungen für das Funknetz ein, das der Repeater erweitern soll. Achten Sie bitte darauf, dass SSID und Kanal identisch mit den Funkeinstellungen des Access Points bzw. Hotspot-Routers sind. Andernfalls kann das Funknetz nicht erweitert werden.

### Funkeinstellungen Repeater

Tragen Sie hier die Daten des Funknetzes ein, dessen Reichweite dieser Repeater vergrößern soll.

5 Ghz 2.4 Ghz

Kanal [?]	Kanal 36 - 5.18 GHz ▾
Bandbreite [?]	20 MHz ▾
Modus [?]	802.11 a/n ▾
802.11ac	-- deaktiviert -- ▾
Sendeleistung [?]	17.00 dBm (50 mW) ▾
Eigene MAC-Adresse [?]	28:EE:52:62:7C:38

---

MAC-Adresse der Gegenstelle [?]	<input style="width: 90%;" type="text"/>
SSID der Gegenstelle [?]	<input style="width: 90%;" type="text" value="HOTSPLOTS"/>
Wählen Sie hier das Frequenzband aus, in dem dieser Repeater eine Verbindung herstellen soll. [?]	<span style="border: 1px solid gray; padding: 2px;">nur 5 GHz ▾</span>

Funknetz scannen
 Übernehmen

### HOTSPLOTS WLAN

Alle Clients, die über das HOTSPLOTS WLAN verbunden sind, müssen sich zunächst über die HOTSPLOTS Login-Seite anmelden, bevor sie das Internet nutzen können.

SSID [?]	<input style="width: 90%;" type="text" value="HOTSPLOTS_test"/>	<input checked="" type="checkbox"/> HOTSPLOTS SSID
WLAN-Clients isolieren [?]	<input checked="" type="radio"/> ja <input type="radio"/> nein	
Repeater erlauben [?]	<input type="radio"/> ja <input checked="" type="radio"/> nein	
Frequenzband [?]	<span style="border: 1px solid gray; padding: 2px;">2.4 und 5 GHz (zusammengelegt) ▾</span>	

Übernehmen

*Abbildung 14: Beispiel-Konfiguration eines Routers mit Repeaterfunktion*

Im zweiten Feld „HOTSPLOTS WLAN“ können Sie die SSID des Repeaters selbst einstellen. Mit dieser SSID können sich Hotspot-Gäste mit dem Hotspot verbinden. Ein Screenshot für diese Einstellungen sehen Sie in 14.

**Achtung:** Beim Aktivieren der Betriebsart „Repeater“ wird automatisch der DHCP-Server unter LAN deaktiviert. Dieser darf nicht manuell wieder angeschaltet werden!

Zu Wartungszwecken wird die LAN-Adresse statisch konfiguriert. Bei Fernwartung können Sie sich vom Hotspot-Router per SSH darauf einloggen oder bei entsprechend gesetzter Port-Weiterleitung auch auf das Web-Interface zugreifen.

**Wichtig:** Damit ein Repeater angebunden werden kann, muss beim Router die Option Repeater erlauben eingeschaltet sein. (Näheres siehe Abb. 15)

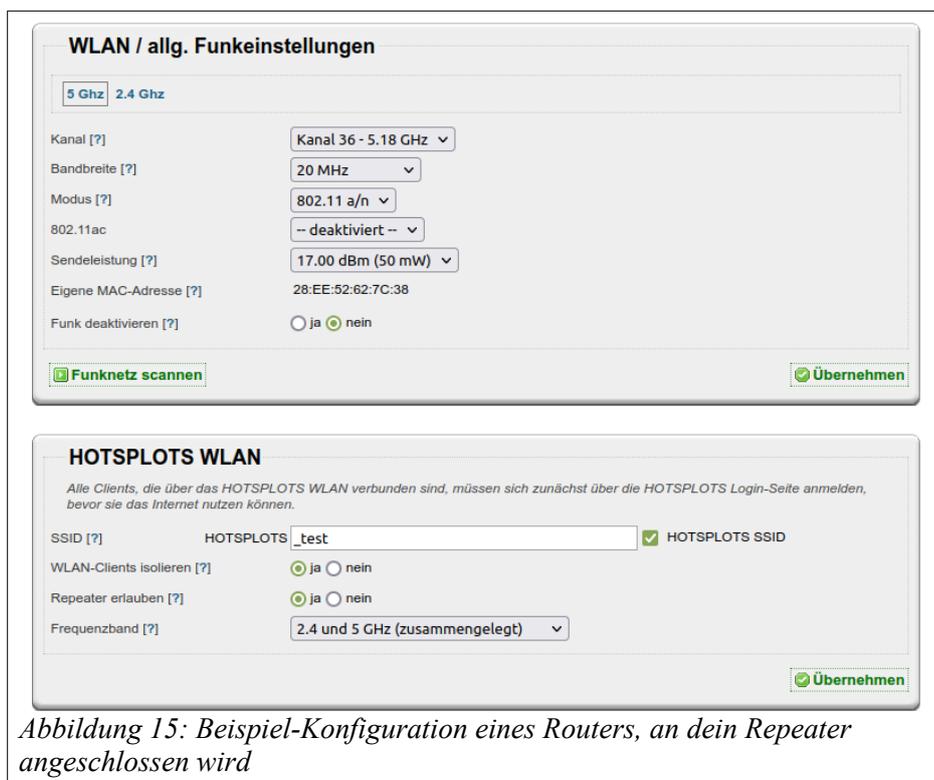


Abbildung 15: Beispiel-Konfiguration eines Routers, an dein Repeater angeschlossen wird

## 4 Die Firmware-Menüpunkte im Überblick

### 4.1 Die Status-Seite

Die Status-Seite gibt eine Übersicht über die verwendete Hardware, die Version der Firmware und eben den Status.

Um zu den einzelnen Menüpunkten zu gelangen, reicht es aus, auf den jeweiligen Bezeichner zu klicken.

Die Zeit holt sich das Gerät bei jedem Neustart von einem NTP-Server im Internet. Für die Basisfunktion des Hotspots ist eine korrekte Zeit nicht zwingend notwendig, allerdings für die Nutzung des optionalen VPN-Routings.

Von den Netzwerkkarten für WAN und LAN werden IP-Adressen und MAC-Adresse angezeigt.

Wenn VPN-Routing aktiv ist, werden alle Verbindungen des Hotspots nicht direkt in das Internet geroutet sondern über einen Server von HOTSPLOTS.

„Hotspot-Name“ gibt den Namen des Hotspots an so wie er zuvor im Kundenbereich generiert wurde.

### 4.2 Netzwerk

#### WAN / Internetanbindung

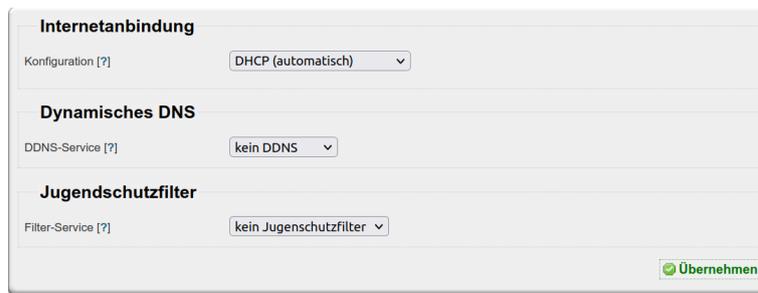


Abbildung 16: WAN / Internetanbindung

Auf der Seite WAN / Internetanbindung werden die Einstellungen für die Netzwerkbuchse zum WAN (Wide Area Network, typischerweise das Internet) vorgenommen. Diese Einstellungen müssen Sie nur am ersten Gerät, dem Hotspot-Router, vornehmen. Wenn Sie noch weitere Geräte als Repeater oder Access Points betreiben, können Sie bei diesen diese Seite ignorieren und auf den Standardeinstellungen lassen oder die oberste Einstellung auf „keine (ausgeschaltet)“ setzen.

Im obersten Pulldown-Menü, *Internetanbindung*, gibt es 4 Betriebsmodi:

1. *PPPoE (DSL-Modem)* ist richtig, wenn der Router direkt an ein DSL-Modem angeschlossen ist.
2. *DHCP (automatisch)* ist richtig, wenn der Hotspot-Router an einen (DSL-)Router angeschlossen wird, der per DHCP-Server automatisch IP-Adressen vergibt. Näheres in Kap. 2.3.
3. *Statisch (feste IP-Adresse)* ist richtig, wenn der Hotspot-Router an einen (DSL-)Router angeschlossen wird, dessen LAN manuell konfiguriert ist. Näheres ebenfalls in Kap. 2.3.
4. *nicht genutzt (aus)* ist nur sinnvoll für Repeater oder kabelgebundene Access Points. Hotspot-Router, die den Zugang zum Hotspot und damit zum Internet regeln sollen, können mit dieser Einstellung nicht funktionieren.

#### Dynamisches DNS

*Dynamisches DNS* brauchen Sie nur, wenn es sich um einen direkt ans Internet - also in aller Regel per PPPoE an ein DSL-Modem angeschlossen - Hotspot-Router handelt und dieser aus dem Internet erreichbar sein soll. Das kann etwa zur Fernwartung nützlich sein oder wenn Sie lokal Serverdienste betreiben. Portweiterleitungen zu diesen Serverdiensten können Sie unter Sicherheit >> Firewall einrichten. Als Anbieter für den Service sind dyndns.com, easydns.com und zoneedit.com vorgesehen.

Die IP-Adresse des Internetanschlusses wird übrigens im Kundenbereich unter dem Menüpunkt Meine Hotspots angezeigt. Damit kann man auch ohne DynDNS Standorte mit dynamischer IP-Adresse fernwarten.

#### Jugendschutzfilter

Für spezielle Standorte wie Schulen und Kinderbibliotheken bieten wir die Möglichkeit, einen Jugendschutzfilter einzuschalten.

Näheres siehe:

[https://www.hotspots.de/fileadmin/Daten/Downloads/Whitepaper/Whitepaper\\_Jugendschutzfilter\\_DE.pdf](https://www.hotspots.de/fileadmin/Daten/Downloads/Whitepaper/Whitepaper_Jugendschutzfilter_DE.pdf)

## LAN / lokales Ethernet

### Für Router ohne APs

Für *LAN / lokales Ethernet* ist die statische Konfiguration voreingestellt. Die LAN-Ports können auch deaktiviert werden, was in der Regel aber nicht gewünscht ist. Typischerweise werden Sie mit der Netzmaske 255.255.255.0 gut bedient sein. In dieses Subnetz können neben dem Router noch bis zu 253 Geräte eingebunden werden.

Die Standardeinstellung für die IP-Adresse ist 192.168.1.1. Wenn der Hotspot-Router in ein bereits vorhandenes LAN integriert werden soll, das auch Adressen im Bereich 192.168.1.xxx benutzt und der WAN-Anschluss in diesem Bereich liegen soll, dann müssen Sie hier eine andere IP-Adresse wie etwa 192.168.43.2 auswählen. Alles mit 192.168.44.1 bis 192.168.47.254 ist tabu, denn in dem Bereich werden IP-Adressen an die Hotspot-Clients verteilt.

Der DHCP-Server hat nichts mit dem Verteilen von IP-Adressen an WLAN-Clients des Hotspots zu tun, sondern betrifft nur Rechner, die per Kabel mit dem LAN-Port verbunden sind und auch das nur dann, wenn die Betriebsart „Hotspot Router (ohne APs)“ ist. Es betrifft also nur Rechner, die über den integrierten Switch an das Internet angeschlossen werden sollen und sich nicht am Hotspot authentifizieren müssen. Wenn der DHCP-Server aktiv ist, können Sie mit einem Handy, Tablet oder Notebook, das die IP-Adresse automatisch bezieht (so, wie es bei allen Systemen voreingestellt ist) das Webinterface aufrufen ohne die Netzwerkkarte konfigurieren zu müssen. (Siehe 17)

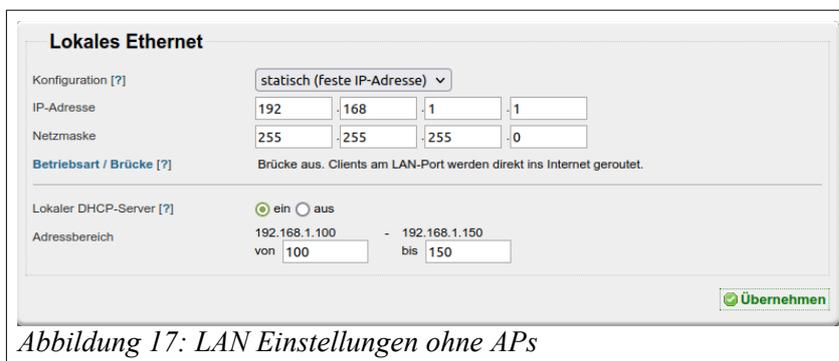


Abbildung 17: LAN Einstellungen ohne APs

## Für Router mit APs

Für *LAN / lokales Ethernet* ist die statische Konfiguration voreingestellt. Die LAN-Ports können auch deaktiviert werden, was in der Regel aber nicht gewünscht ist. Typischerweise werden Sie mit der Netzmaske 255.255.255.0 gut bedient sein. In dieses Subnetz können neben dem Router noch bis zu 253 Geräte eingebunden werden.

Die Standardeinstellung für die IP-Adresse ist **192.168.1.1**. Wenn der Hotspot-Router in ein bereits vorhandenes LAN integriert werden soll, das auch Adressen im Bereich 192.168.1.xxx benutzt und der WAN-Anschluss in diesem Bereich liegen soll, dann müssen Sie hier eine andere IP-Adresse wie etwa 192.168.43.2 auswählen. Alles mit 192.168.44.1 bis 192.168.47.254 ist tabu, denn in dem Bereich werden IP-Adressen an die Hotspot-Clients verteilt.

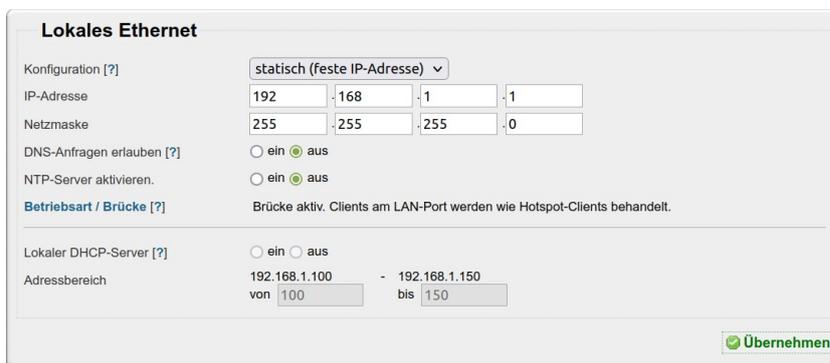


Abbildung 18: LAN Einstellungen mit APs

Der Unterschied zu Routern ohne APs ist, dass die LAN-Brücke aktiv ist. D.h. man beim Anschließen von Geräten eine IP im Managementnetz bekommt. Dies sollte verwendet werden, um wie der Name schon sagt APs anzuschließen. Diese leiten den einkommenden Datenverkehr über den Router an unsere HOTSPLOTS Server (insofern die Option des VPN Routings aktiv ist)

## WLAN / Funknetz

The image shows two screenshots of a web-based configuration interface for a WLAN router. The top screenshot is titled "WLAN / allg. Funkeinstellungen" and shows settings for the 5 GHz band, including channel selection (Kanal 36 - 5.18 GHz), bandwidth (20 MHz), mode (802.11 a/n), and power level (17.00 dBm (50 mW)). It also includes a MAC address and a checkbox for "Funk deaktivieren". The bottom screenshot is titled "HOTSPLOTS WLAN" and shows settings for the hotspot, including SSID (HOTSPLOTS\_test), isolation of WLAN clients, repeater permission, and frequency band (2.4 und 5 GHz (zusammengelegt)).

Abbildung 19: WLAN Einstellungen

Auf der Seite **WLAN / Funknetz** können allgemeine Funkeinstellungen festgelegt werden. Den Kanal sollten Sie so wählen, dass möglichst wenig weitere Sender auf demselben Kanal oder den unmittelbaren Nachbarkanälen stören können. Welche anderen WLAN-Sender aktiv sind, können Sie über den Link „Funknetz scannen“ einsehen.

Die **Bandbreite** steuert die Übertragungsrate des WLAN-Netzes. Bei einer Bandbreite von 40 MHz können Sie eine max. Übertragungsrate von 450 Mbps / 1350Mbps erreichen, wenn die Funkumgebung des Hotspots dies zulässt. Da die Übertragung bei 40MHz empfindlicher gegenüber Störungen ist, empfehlen wir diesen Wert auf 20 MHz belassen.

Die **Sendeleistung** kann zwischen 10 und 100 mW eingestellt werden. Dabei gilt, dass mehr nicht unbedingt besser ist, denn mit steigender Leistung nimmt auch das Rauschen zu und es bringt nichts, wenn der Sender zwar sehr stark sendet, die Gegenstellen aber nicht ebenso stark zurücksenden können. Außerdem ist in Deutschland die maximal erlaubte Sendeleistung auf 100 mW (entspricht 20 dBm) EIRP beschränkt. Bei Bedarf kann der Funk über die Option **Funk deaktivieren** ganz ausgeschaltet werden. Dies ist nur in speziellen Fällen sinnvoll, in denen die Hotspot-Funktionalität nur an den LAN-Anschlüssen gewünscht wird.

Der **Modus** legt fest, in welchem Funkstandard das Gerät operieren soll. Die Standardeinstellung ist 802.11 a/n.

Die **SSID** ist der Name des Drahtlosnetzwerkes, den Nutzer auswählen müssen, bevor sie die Login-Seite sehen können. Die SSID beginnt in der Regel mit „HOTSPLOTS“. Am besten tragen Sie dahinter den Namen ein, den Sie beim Anlegen des Hotspots im Kundenbereich der Website angegeben haben. Dann ist den Nutzern die Verbindung zwischen Daten auf der Hotspot-Karte, ggf. auf Location Tickets und der SSID ersichtlich. In Ausnahmefällen kann die Standardoption HOTSPLOTS SSID ausgeschaltet werden. Das ist vor allem für Hotspots mit dem Tarif V.I.P. /Nur Tickets gedacht.

The image shows a screenshot of the "Privates WLAN anlegen" configuration page. It includes fields for SSID, a checkbox for "Versteckt", a dropdown for "Verschlüsselung" (set to "keine Verschlüsselung"), a warning message in red, a checkbox for "WLAN-Clients isolieren", a dropdown for "Frequenzband" (set to "nur 5 GHz"), radio buttons for "Netzwerk" (selected "mit LAN verbinden"), and input fields for "Private IP-Adresse" (192.168.55.1) and "Privater DHCP Bereich" (100-200).

Abbildung 20: Neues Netzwerk anlegen

Des Weiteren besteht die Möglichkeit, ein **privates WLAN** anzulegen. Clients, die sich in diesem Funknetz einbuchen, werden direkt ohne Anmeldung und VPN-Routing ins Internet geroutet. Alternativ kann für das private WLAN ein **eigenes privates Netz** mit einer eigenen IP-Adresse angelegt werden. In diesem Fall bekommen WLAN-Clients im privaten Netz per DHCP eine IP-Adresse im ausgewählten Bereich zugewiesen und werden direkt ohne Anmeldung und VPN-Routing ins Internet geroutet. Mit der Option **Versteckt** können Sie die SSID des privaten WLANs unsichtbar machen. Unter **Verschlüsselung** können Sie eine Verschlüsselung für Ihr privates WLAN auswählen.

**Achtung:** Ein verstecktes Funknetzwerk, das nicht durch eine Verschlüsselung geschützt ist, bietet keinen Schutz. Es ist für andere Personen weiterhin möglich eine Verbindung aufzubauen, auch wenn der Name nicht sichtbar ist.

## HOTSPLOTS Hotspot

Die Felder Hotspot-Name und Schlüssel sind genau mit den Daten auszufüllen, die Sie im Kundenbereich auf [www.hotspots.de](http://www.hotspots.de) beim Anlegen des Hotspots angegeben haben. Anhand dieser Daten authentifiziert sich der Hotspot gegenüber dem HOTSPLOTS-Server. Diese Authentifizierung kann mit dem Button „Name & Schlüssel prüfen“ getestet werden. Damit wird gleichzeitig die Internetverbindung überprüft.

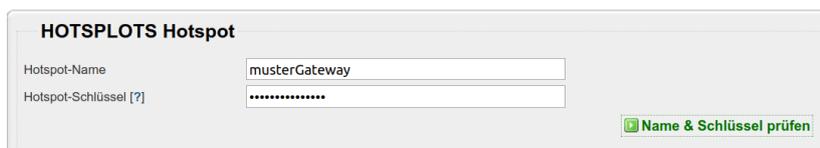


Abbildung 21: HOTSPLOTS spezifische Einstellungen

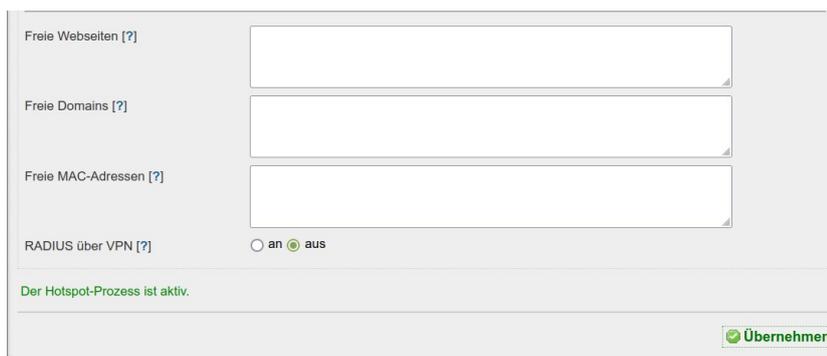


Abbildung 22: Freischaltung von Nutzung ohne Login

In das Feld **Freie Web-Adressen** können Seiten eingegeben werden, die ohne Login am Hotspot erreichbar sein sollen. Diese Funktion von Hotspots wird häufig als Walled Garden bezeichnet. Die Sites [www.hotspots.de](http://www.hotspots.de), [shop.hotspots.de](http://shop.hotspots.de) und [www.paypal.de](http://www.paypal.de) sind immer freigeschaltet. Die maximal mögliche Anzahl an Sites ist nur durch die Feldlänge von maximal 512 Zeichen begrenzt.

Mit dem Feld **Freie MAC-Adressen** können Netzwerkkarten freigeschaltet werden, so dass deren Nutzer nicht auf die Loginseite umgelenkt werden. Wenn es sich dabei um WLAN-Karten handelt, beinhaltet diese Option ein gewisses Risiko: Jeder Nutzer, der sich ein wenig auskennt, kann die MAC-Adressen weiterer laufender Funkverbindungen mitlesen (sniffen), anschließend seiner eigenen Netzwerkkarte eine dieser MAC-Adressen zuweisen und sich so gegebenenfalls unberechtigten Zugang zum Internet verschaffen. Eingeführt wurde diese Option als Notlösung für mobile Geräte ohne Webbrowser, wie etwa eine Playstation, genutzt wird sie aber auch gern für Geräte wie z. B. Handys und Tablets von Mitarbeitern, kabelgebundene Rechner an der Rezeption oder SmartScreens.

## VPN Routing

Wenn die Option **VPN-Routing** aktiviert ist, wird der gesamte Traffic der Hotspot-Clients über einen Server von HOTSPLOTS geroutet. Diese Option ist eine Schutzfunktion für Hotspot-Betreiber. Wenn das VPN-Routing aktiviert ist, ist aus dem Internet nicht die IP-Adresse des Hotspots sondern die Adresse eines Servers von HOTSPLOTS zu sehen.

Die Nutzung dieses Service ist kostenfrei.

Die Pingzeiten erhöhen sich dabei zwangsläufig ein wenig. HOTSPLOTS verfügt aber über ein leistungsstarkes, geografisch redundantes Netz an VPN-Servern, insbesondere bei den beiden wichtigsten deutschen Internetknoten in Frankfurt und Berlin, und kann dort über ein direktes Peering mit geringer Latenz in das Netz der Deutschen Telekom routen.

## 4.3 Sicherheit

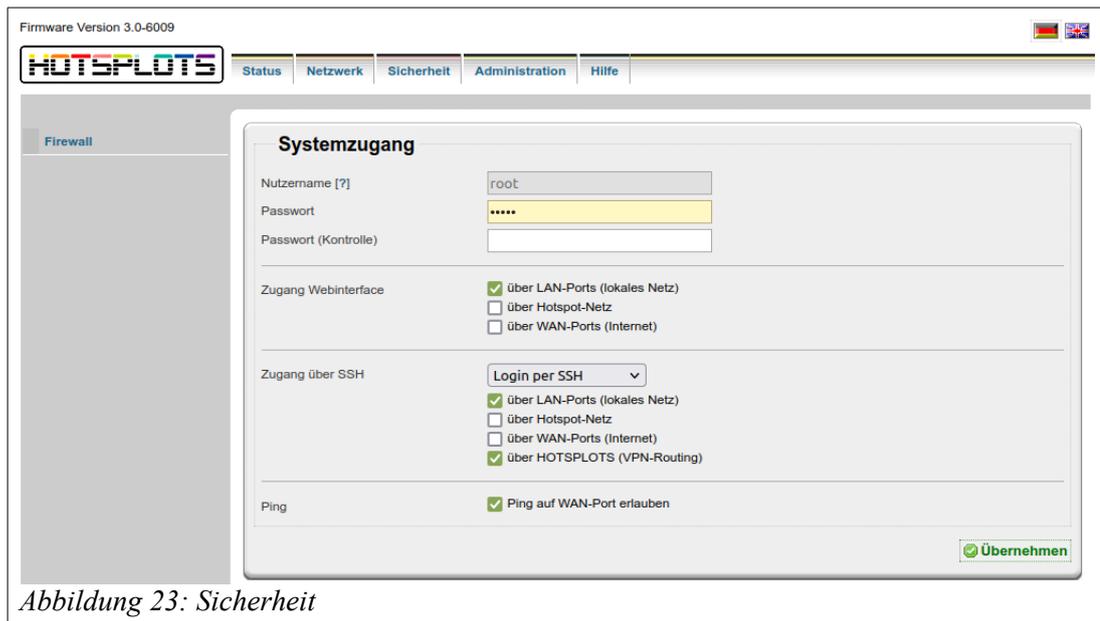


Abbildung 23: Sicherheit

Hier werden die möglichen Wege zur Administration des Gerätes und die Passwörter dafür gesetzt.

Im Auslieferungszustand ist der Zugriff auf das Webinterface nur über einen der LAN-Ports möglich. Username und Passwort sind **root** und **admin**. Aus Sicherheitsgründen sollte das Passwort geändert werden. Zusätzlich kann der Zugriff auf das Webinterface über WLAN und über WAN, sprich aus dem Internet erlaubt werden. Beides ist auch mit einem schwierig zu erratendem Passwort nicht wirklich sicher, weil die Übertragung dieser Daten unverschlüsselt erfolgt. Einen sicheren, weil verschlüsselten Weg bietet eine Administration per ssh. 23 zeigt die Einstellmöglichkeit unter dem Menüpunkt Sicherheit. Dies ist allerdings nur Nutzern mit Grundkenntnissen in Linux zu empfehlen.

## Firewall

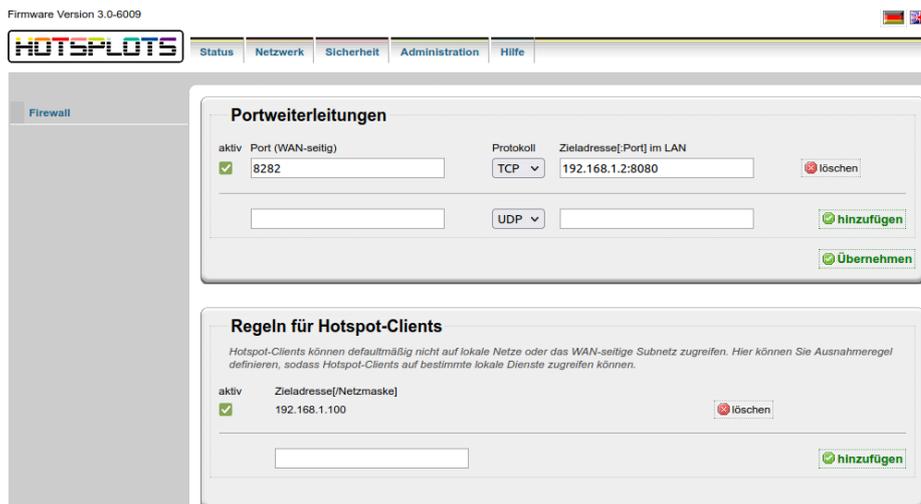


Abbildung 24: Firewall

Mit den Einstellungen zu den **Portweiterleitungen** können Portweiterleitungen gesetzt werden. Dies ist z.B. für den Hotspot-Router sinnvoll um dahinter liegende Access-Points erreichen zu können.

Wenn Sie etwa die Regel **8282 TCP 192.168.1.2:8080** gesetzt haben und der Hotspot-Router am WAN-Port die IP-Adresse 1.2.3.4 und ein kabelgebundener Access Point die LAN-Adresse 192.168.1.2 hat, dann können Sie unter <http://1.2.3.4:8282> das Webinterface des APs auf der 192.168.1.2 erreichen.

Im Fenster **Regeln für Hotspot-Clients** können Sie einzelne IP-Adressen, wie z.B. 192.168.1.100 oder ganze Netzwerke wie z.B. 192.168.1.0/24 eingeben. Diese IP-Adressen (oder Netzwerke) sind dann vom Hotspot-Netz aus erreichbar.

## 4.4 Administration

### Firmware Update



Abbildung 25: Firmware-Update des Hotspot-Routers direkt über das Internet

Der einfachste Weg für ein Update der Firmware geht über den Button „von [www.hotspots.de](http://www.hotspots.de) flashen“. Dann verbindet sich der Router direkt mit dem Server von HOTSPLOTS und lädt die ausgewählte Version ohne Umweg über einen PC herunter – siehe 25. Dies geht nur bei Hotspot-Routern, die über den WAN-Port mit dem Internet verbunden sind.

Alternativ können Sie die Firmware von <https://www.hotspots.de/support/downloads/firmware.html> herunterladen, auf Ihrem PC zwischenspeichern und dann über den *Durchsuchen*-Button auf den Router laden.

### Konfiguration sichern

Unter diesem Menüpunkt können Sie über den Button **Konfiguration sichern** eine Datei vom Router herunterladen, die alle Konfigurationseinstellungen enthält. Diese Datei können Sie z. B. auf andere Geräte aufspielen (**Konfiguration wiederherstellen**), um Einstellungen zu duplizieren (z. B. für Access Points, aber Achtung: eindeutige IP-Adressen sind für APs notwendig), oder um Einstellungen im Fall eines „Verbastelns“ wieder herzustellen.



Abbildung 26: Konfiguration sichern

## Neustart

Unter diesem Menüpunkt können Sie einen Neustart des Gerätes durchführen. Gespeicherte Einstellungen des Gerätes bleiben dabei erhalten. Je nach Gerätetyp dauert dieser Vorgang etwa eine Minute.

## System-Log

An dieser Stelle sehen Sie alle Ereignisse, welche in der Logdatei des Routers enthalten sind. Erfahrene Anwender haben anhand des System-Logs die Möglichkeit, eventuelle Fehlerursachen oder Fehlkonfigurationen zu erkennen.

## Prozesse

Alle Systemprozesse werden unter diesem Menüpunkt dargestellt. Außerdem können Sie ablesen, welche CPU- und Speicherauslastung die einzelnen Systemprozesse verursachen.

## Diagnose

Es besteht die Möglichkeit, die Konfigurationseinstellungen des Gerätes an HOTSPLOTS zu senden. Hierbei werden die Konfigurationseinstellungen wie in der Funktion „Konfiguration sichern“ nicht nur lokal exportiert, sondern stehen den Technikern von HOTSPLOTS zur Verfügung. Dies ermöglicht im Fall der Fälle die schnelle Konfiguration eines Austauschgerätes.

## System Information

Netzwerk- und Geräte-relevante Daten sind unter diesem Menüpunkt vermerkt. Unter anderem sehen Sie die im Gerät hinterlegten statischen Routen, die Bridgeinformationen sowie eine Liste aller Interfaces.

## 5 Administration über ssh

Dieser Weg der Administration ist nur für Fachleute mit Linux-Kenntnissen zu empfehlen und auch dann nur unter besonderen Umständen sinnvoll, z. B. Fernwartung komplexer Netzwerke, Skripten. Bevor Sie tief im System herumwerkeln, sprechen Sie mit uns!

Wir empfehlen, nach Möglichkeit die Administration über das HOTSPLOTS-spezifische Web-Interface vorzunehmen.

### 5.1 Nützliche Linux-Befehle:

**ifconfig** gibt eine Liste der aktiven Netzwerkdevices und deren Konfiguration (IP-Adressen, etc.) aus.

**top** gibt die aktuell laufenden Prozesse und die Systemlast aus.

**uptime** gibt aus, wie lange das Gerät schon durchläuft (seit dem letzten Neustart)

**fping -asqg [IP-Adresse]/[Subnet]** scannt das gesamte Subnetz auf aktive Geräte. Dies ist z. B. sinnvoll, wenn das Vorhandensein diverser Accesspoints im Netzwerk überprüft werden muss.

**logread** gibt das System-Log aus.

## 6 Troubleshooting / Fehlersuche

### 6.1 Die Administrationsoberfläche lässt sich nicht aufrufen

1. Überprüfen Sie die Verkabelung. Sind wirklich ein LAN-Port (und nicht der WAN-Port) des Routers mit dem PC verbunden?
2. Überprüfen Sie die Einstellungen der Netzwerkkarte des Admin-PCs (der Rechner, der per Kabel mit dem Router verbunden ist). Die Karte sollte mit einer IP-Adresse statisch konfiguriert sein. Wenn Sie ein LAN mit mehreren Netzwerkkarten, vielen Kabeln und Switches haben, trennen Sie alles bis auf die Stromversorgung, das Netzwerkkabel zwischen Hotspot-Router und Admin-PC und ggf. dem Kabel am WAN-Port des Routers.  
Wenn Sie meinen, es sei alles in Ordnung, Sie aber dennoch nicht das Web-Interface aufrufen können, konfigurieren Sie die Netzwerkkarte des Admin-PCs, die mit dem Router verbunden ist auf die IP-Adresse 192.168.1.2.
3. Drücken Sie im laufenden Betrieb den Resetknopf des Routers für mindestens 8 Sekunden. Daraufhin wird der Router auf Standardeinstellungen zurückgesetzt und erhält am LAN-Port die IP-Adresse 192.168.1.1 (unabhängig vom Hersteller des Routers), so dass Sie das Web-Interface unter <http://192.168.1.1:8080> aufrufen können.

### 6.2 Man sieht das WLAN, aber die Loginseite wird nicht angezeigt.

1. Dann hat vermutlich der Hotspot-Router keine Verbindung ins Internet. Rufen Sie das Web-Interface auf und überprüfen Sie die Einstellungen unter Netzwerk > WAN / Internetanbindung.
2. Eine zweite Ursache kann daran liegen, dass Ihre WLAN-Karte nicht korrekt konfiguriert ist. Die IP-Adresse muss per DHCP-Client, also automatisch bezogen werden. Die Loginseite wird nur dann dargestellt, wenn Sie auch über das Captive Portal (chilli) authentisiert sind. Sie sollten eine IP-Adresse im Bereich 192.168.44.x bis 192.168.47.xxx erhalten haben.

### 6.3 Man kommt ohne Loginseite ins Internet

1. Sind Sie über einen der LAN-Ports mit dem Hotspot-Router verbunden? Dann arbeitet der Router vermutlich in der Betriebsart „Hotspot Router (ohne APs)“. Erkennbar daran, dass der Client keine IP-Adresse hat, die mit 192.168.44. , 192.168.45. , 192.168.46. oder 192.168.47. beginnt.
2. Sind Sie vielleicht noch eingeloggt? Rufen Sie <http://logout.hotspots.de> auf. Wenn da ein Button zum Ausloggen erscheint, war das der Grund, denn dann waren Sie schon am Hotspot eingeloggt.

## 7 Richtlinien zur Hotspot-Installation

### 7.1 IT-Sicherheit

#### Schutz des Hotspots vor unberechtigtem Zugriff

1. Sicheres Passwort für den Hotspot-Router setzen.
2. Sichere Passwörter für Access Points und Repeater setzen. Idealerweise hätte jedes Gerät ein eigenes Passwort. Wem das zu umständlich ist, der sollte zumindest für den Hotspot-Router ein anderes Passwort setzen als für die weiteren Netzknoten. Da auf dem Hotspot-Router das System für die Zugangskontrolle läuft, ist das Schadenspotential beim Hotspot-Router deutlich größer als etwa bei einem von vielen Access Points. Das Passwort für die APs und Repeater kann zudem mangels SSL-Verschlüsselung vergleichsweise einfach ausspioniert werden, wenn die Webadministration über Funkstrecken genutzt wird. Die sichere Alternative ist die Administration über ssh. Darüber lässt sich auch das Webinterface tunneln.
3. Die erlaubten Zugangswege für die Administration einschränken. Wenn der Hotspot-Router an einen DSL-Router und nicht an ein DSL-Modem angeschlossen wird, ist es empfehlenswert, dem Hotspot-Router eine statische WAN-IP zuzuweisen und die Administration über LAN und WLAN zu deaktivieren.

## Schutz der Nutzer durch netzweite Client-Isolierung

Wenn mehrere Nutzer gleichzeitig im Netz angemeldet sind, besteht die Gefahr, dass ein Nutzer etwa auf ungeschützte Windows-Freigaben eines anderen Nutzers zugreifen kann.

Bei Access Points und Repeatern sollte die HOTSPLOTS Firmware ab Version 2.0-33 eingesetzt werden. Dann werden mit der Client-Isolierung, siehe Menüpunkt Netzwerk >> WLAN, alle Pakete mit einer Zieladresse in dem Adressbereich, in dem den Clients vom Hotspot-Router IP-Adressen zugewiesen werden, geblockt.

Wenn Access Points mit fremder Firmware eingesetzt werden, sollten die Geräte über Switches mit portbasierten VLANs isoliert werden.

## Schutz des vorhandenen Netzes vor Hotspot-Nutzern

Idealerweise wird der Hotspot über einen eigenen DSL-Anschluss, z.B. von HOTSPLOTS, versorgt.

Wenn der Hotspot denselben Internetanschluss nutzt wie z.B. das eigene Büronetz des Standortes, dann sollte die Firewall im Hotspot-Router dafür sorgen, dass Hotspot-Clients keinen Zugriff auf Rechner im lokalen Netz des Standortes haben:

Bei der Firmware 2.0 wird dies über vorformulierte Firewallregeln realisiert, die unter dem Menüpunkt Sicherheit >> Firewall / Ports aktiviert sein sollten. Ansonsten steht dort ein roter Warnhinweis.

Bei der Firmware 3.0 ist diese Firewall-Regel immer aktiv, sofern nicht ausdrücklich, manuell eine Regel für den Zugriff in ein lokales Netz definiert wird.

## Idle-Timeout für Terminals

Automatische Logouts erfolgen nur, wenn das Guthaben aufgebraucht oder der Client nicht mehr erreichbar ist. Dies ist z.B. dann ein Problem, wenn vor Ort Terminals angeboten werden und Nutzer nicht daran denken, sich aktiv auszuloggen. Im Extremfall, z.B. eine Reha-Klinik, die Tickets mit einer Gültigkeit von drei Wochen ausgibt, könnte dies dazu führen, dass sich ein Gast mit einem neuen Ticket einloggt und dann drei Wochen lang alle Nutzer ohne erneutes Login mit der Kennung des Ersten surfen. Für solche Szenarien, kann HOTSPLOTS ein sogenanntes Idle-Timeout von z.B. 60 Sekunden eintragen. Dann würde ein Logout initiiert, sobald 60 Sekunden lang keine Daten von dem Client ins Internet übertragen werden. Damit das funktioniert, ist darauf zu achten, dass keine Hintergrundprozesse auf dem Terminal laufen, die zu oft auf das Internet zugreifen, z.B. um nach Updates zu fragen.

## 7.2 Physikalische Sicherheit

Zum einen sollte die Position der WLAN-Stationen unter dem Gesichtspunkt optimaler Funkverbindungen im zu versorgenden Bereich gewählt werden: also meist eine erhöhte Position über Möbeln, Menschen und anderen Absorbern, nicht zu dicht an metallischen Reflektoren oder abgeschirmt durch wasserhaltige Absorber (Holz, Lehm, Aquarien etc.).

Zum anderen sollte darauf geachtet werden, dass die Geräte soweit möglich vor **Diebstahl** und **Vandalismus** geschützt sind und elementare Gefährdungen möglichst reduziert werden. **Blitzschutz** spielt vor allem bei Outdoorgeräten eine wichtige Rolle. Antennen- und Netzkabel, die in Dachnähe verlegt werden, müssen mit Blitzschutz versehen werden. Ggf. ist der vorhandene Blitzschutz von einer Fachfirma durch Fangstangen zu ergänzen.

Vor allem Indoor-Geräte sind gegenüber **Wasser** sehr empfindlich. Daher sollte der Einsatz in Feuchträumen und mögliches Eindringen von Wasser in das Gehäuse unbedingt vermieden werden

## 7.3 Entdecken von Störungen

Das **Monitoring**-System versendet automatisch per E-Mail sowohl Meldungen über eine Störung als auch über die Störungsbehebung. Dazu sollten im Kundenbereich auf hotspots.de in den Eigenschaften des Hotspots im Feld „Admin Kontakt“ E-Mail-Adressen der zuständigen Stellen, z.B. Hotspot-Betreiber und Installationspartner, eingetragen sein und diese regelmäßig geprüft werden.

## 7.4 Beheben von Störungen

Sollte trotz aller Schutzmaßnahmen die Funktion des Hotspots gestört sein, ist es wichtig, dass die Störung so schnell wie möglich behoben wird. Dies ist nur möglich, wenn eine **aktuelle Dokumentation verfügbar** ist. Das heißt die Dokumentation muss erstens angelegt werden und zweitens jederzeit zugänglich hinterlegt werden. Die Person oder Firma, die die Installation des Hotspots vornimmt, sollte auch die Dokumentation anlegen. Im Sinne der Verfügbarkeit ist es optimal, wenn die Dokumentation sowohl **beim Installateur**, als auch **beim Hotspot-Betreiber** sowie **bei HOTSLOTS** hinterlegt ist. Dabei ist allerdings darauf zu achten, dass sichergestellt ist, dass die Dokumentation nicht in falsche Hände gerät.

Ab Firmware 3.0-16 können die Einstellungen des Hotspot-Routers automatisch an HOTSLOTS übermittelt werden. Damit kann jederzeit und sehr schnell ein Ersatzgerät konfiguriert werden.

Ferner sollte die **Fernwartung für HOTSLOTS** ermöglicht sein (Menüpunkt Sicherheit: „Zugang über SSH: über HOTSLOTS (VPN-Routing)).

## 7.5 Maßnahmen zum Beenden des Hotspot-Angebotes

Falls der Hotspot später außer Betrieb genommen werden soll, informieren Sie bitte die Nutzer darüber. Der einfachste Weg ist, auf die Login-Seite einen kleinen Hinweistext zu setzen. Dort sieht es jeder regelmäßige Nutzer und kann sich entsprechend darauf einstellen.

## 8 Anhang 1: Trennung von Clients via VLAN

Access Points mit der Firmware von HOTSLOTS unterstützen die Client-Isolierung. Das bedeutet, dass WLAN-Clients, die mit demselben AP verbunden sind, vor gegenseitigem Zugriff z. B. auf Windows-Freigaben geschützt sind. Das ist jedoch ein Feature des WLAN-Treibers. In größeren Netzwerken mit über Switchen verbundenen APs oder Terminals ist der Treiber machtlos, wenn es darum geht, Clients die an verschiedenen APs bzw. Ports angeschlossen sind, vor gegenseitigem Zugriff zu schützen. Der einfachste Weg, hier für zusätzliche Sicherheit zu sorgen, ist entweder der Einsatz unserer Firmware für APs, die die Firewall zur Trennung von Clients auch für gebrückte Netzwerke unterstützen, die Verwendung von APs welche mit einem Hosted Controller kommunizieren oder der Einsatz von Appliances mit Lokalem Controller. Fragen sie diesbezüglich gern einmal in unserem Vertrieb an.

## 9 Impressum/Support/Kontakt

Offene Fragen oder auch Verbesserungsvorschläge senden Sie am besten per Mail an [support@hotslots.de](mailto:support@hotslots.de)

hotslots GmbH  
Rotherstr. 22  
10245 Berlin

Tel.: +49 (0)30 - 29 77 348-0  
Fax: +49 (0)30 - 29 77 348-99

hotslots GmbH, Berlin, Amtsgericht Charlottenburg HRB 93460B  
Geschäftsführung: Dr. Ulrich Meier, Dr. Jörg Ontrup