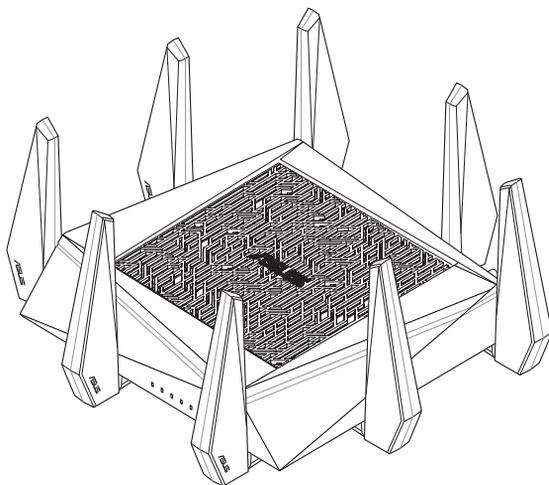


# Benutzerhandbuch

## RT-AC5300

Wireless-AC5300 Tri-band Gigabit Router



**ASUS**<sup>®</sup>  
IN SEARCH OF INCREDIBLE

G10304  
Erste Ausgabe  
Juni 2015

**Copyright © 2015 ASUSTeK Computer Inc. Alle Rechte vorbehalten.**

Kein Teil dieses Handbuchs, einschließlich der darin beschriebenen Produkte und Software, darf ohne ausdrückliche, schriftliche Genehmigung von ASUSTeK COMPUTER INC. ("ASUS") in irgendeiner Form, ganz gleich auf welche Weise, vervielfältigt, übertragen, abgeschrieben, in einem Wiedergewinnungssystem gespeichert oder in eine andere Sprache übersetzt werden.

Produktgarantien oder Service werden nicht geleistet, wenn: (1) das Produkt repariert, modifiziert oder abgewandelt wurde, außer schriftlich von ASUS genehmigte Reparaturen, Modifizierung oder Abwandlungen; oder (2) die Seriennummer des Produkts unkenntlich gemacht wurde oder fehlt.

ASUS STELLT DIESES HANDBUCH "SO, WIE ES IST," OHNE DIREKTE ODER INDIREKTE GARANTIE, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF GARANTIE ODER KLAUSELN DER VERKÄUFLICHKEIT ODER TAUGLICHKEIT FÜR EINEN BESTIMMTEN ZWECK, ZUR VERFÜGBARKEIT. UNTER KEINEN UMSTÄNDEN HAFTET ASUS, SEINE DIREKTOREN, VORSTANDSMITGLIEDER, MITARBEITER ODER AGENTEN FÜR INDIREKTE, BESONDERE, ZUFÄLLIGE ODER SICH ERGEBENDE SCHÄDEN (EINSCHLIESSLICH SCHÄDEN AUF GRUND VON PROFITVERLUST, GESCHÄFTSVERLUST, BEDIENUNGS-AUSFALL ODER DATENVERLUST, GESCHÄFTS-UNTERBRECHUNG UND ÄHNLICHEM), AUCH WENN ASUS VON DER WAHRSCHEINLICHKEIT DERARTIGER SCHÄDEN AUF GRUND VON FEHLERN IN DIESEM HANDBUCH ODER AM PRODUKT UNTERRICHTET WURDE.

SPEZIFIKATIONEN UND INFORMATIONEN IN DIESEM HANDBUCH DIENEN AUSSCHLIESSLICH DER INFORMATION, KÖNNEN JEDERZEIT OHNE ANKÜNDIGUNG GEÄNDERT WERDEN UND DÜRFEN NICHT ALS VERPFLICHTUNG SEITENS ASUS AUSGELEGT WERDEN. ASUS ÜBERNIMMT FÜR EVENTUELLE FEHLER ODER UNGENAUIGKEITEN IN DIESEM HANDBUCH KEINE VERANTWORTUNG ODER HAFTUNG, EINSCHLIESSLICH DER DARIN BESCHRIEBENEN PRODUKTE UND SOFTWARE.

In diesem Handbuch angegebene Produkt- und Firmennamen können u.U. eingetragene Warenzeichen oder Urheberrechte der entsprechenden Firmen sein und dienen nur der Identifizierung oder Erklärung zu Gunsten des Eigentümers, ohne Rechte verletzen zu wollen.

# Inhaltsverzeichnis

<b>1</b>	<b>Kennenlernen Ihres drahtlosen Routers</b>	<b>7</b>
1.1	Willkommen!.....	7
1.2	Packungsinhalt.....	7
1.3	Der drahtlose Router.....	8
1.4	Router Aufstellen.....	10
1.5	Einrichtungsvoraussetzungen.....	11
1.6	Router einrichten .....	12
	1.6.1 Kabelverbindung .....	12
	1.6.2 Drahtlose Verbindung .....	13
<b>2</b>	<b>Erste Schritte</b>	<b>15</b>
2.1	Anmeldung im Web-GUI .....	15
	Quick Internet Setup (QIS) mit autom. Erkennung .....	16
2.3	Mit Ihrem WLAN-Netzwerk verbinden .....	19
<b>3</b>	<b>Allgemeine Einstellungen konfigurieren</b>	<b>20</b>
3.1	Netzwerkübersicht verwenden .....	20
	3.1.1 Einrichten der Drahtlos-Sicherheit .....	21
	3.1.2 Verwalten der Netzwerk-Clients.....	23
	3.1.3 Überwachen der USB-Geräte.....	24
3.2	Erstellen eines Gästernetzwerkes .....	27
3.3	AiProtection .....	29
	3.3.1 Network Protection (Netzwerkschutz).....	30
	3.3.2 Parental Controls (Jugendschutz) einrichten .....	34
3.4	Adaptive QoS.....	38
	3.4.1 Bandwidth Monitor (Bandbreitenüberwachung) .....	38
	3.4.2 QoS .....	39
	3.4.3 Web History (Webverlauf) .....	40
	3.4.4 Traffic Monitor (Datenverkehrsüberwachung).....	41

# Inhaltsverzeichnis

3.5	USB-Anwendungen verwenden.....	42
	3.5.1 AiDisk verwenden.....	42
	3.5.2 Servercenter verwenden.....	44
	3.5.3 3G/4G .....	49
3.6	AiCloud 2.0 verwenden .....	50
	3.6.1 Cloud-Laufwerk .....	51
	3.6.2 Intelligenter Zugriff .....	53
	3.6.3 Intelligente Synchronisierung .....	54
<b>4</b>	<b>Konfigurieren der erweiterten Einstellungen</b>	<b>55</b>
4.1	WLAN.....	55
	4.1.1 General (Allgemein) .....	55
	4.1.2 WPS .....	57
	4.1.3 Brücke.....	59
	4.1.4 WLAN-MAC-Filter .....	61
	4.1.5 RADIUS-Einstellungen.....	62
	4.1.6 Professionell .....	63
4.2	LAN .....	66
	4.2.1 LAN-IP .....	66
	4.2.2 DHCP-Server .....	67
	4.2.3 Route .....	69
	4.2.4 IPTV .....	70
4.3	WAN .....	71
	4.3.1 Internetverbindung .....	71
	4.3.2 Dual-WAN.....	74
	4.3.3 Portauslösung .....	75
	4.3.3 Virtueller Server/Portweiterleitung .....	77
	4.3.4 DMZ.....	80
	4.3.5 DDNS .....	81
	4.3.6 NAT-Durchleitung .....	82

## Inhaltsverzeichnis

4.4	IPv6.....	83
4.5	VPN-Server.....	84
4.6	Firewall.....	85
	4.6.1 Allgemein.....	85
	4.6.2 URL-Filter.....	85
	4.6.3 Schlüsselwortfilter.....	86
	4.6.4 Netzwerkdienstefilter.....	87
	4.6.5 IPv6-Firewall.....	88
4.7	Administration.....	89
	4.7.1 Betriebsmodus.....	89
	4.7.2 System.....	90
	4.7.3 Aktualisieren der Firmware.....	91
	4.7.4 Wiederherstellen/Speichern/Hochladen der Einstellungen 92	
4.8	Systemprotokoll.....	93
4.9	Smart Connect (Schnellverbindung).....	94
	4.9.1 Smart Connect (Schnellverbindung) einrichten.....	94
	4.9.2 Smart Connect Rule (Schnellverbindungsregel).....	97
<b>5</b>	<b>Verwenden der Hilfsprogramme</b>	<b>100</b>
5.1	Device Discovery.....	100
5.2	Firmware Restoration.....	101
5.3	Druckerserver einrichten.....	102
	5.3.1 ASUS EZ Printer Sharing.....	102
	5.3.2 LPR zur Druckerfreigabe verwenden.....	106
5.4	Download Master.....	111
	5.4.1 BitTorrent-Download-Einstellungen konfigurieren.....	112
	5.4.2 NZB-Einstellungen.....	113

<b>6</b>	<b>Fehlerbehebung</b>	<b>114</b>
6.1	Allgemeine Problemlösung.....	114
6.2	Häufig gestellte Fragen (FAQ) .....	116
	<b>Anhänge</b>	<b>125</b>
	Hinweise .....	125
	ASUS Kontaktinformationen .....	139
	Globale Netzwerk-Hotlines.....	140

# 1 Kennenlernen Ihres drahtlosen Routers

## 1.1 Willkommen!

Vielen Dank für den Kauf Ihres neuen WLAN-Routers ASUS RT-AC5300!

Der extradünne und elegante RT-AC5300 bietet 2.4GHz und 5GHz Dual-Bands für ein unvergleichliches drahtloses HD-Streaming; SMB Server, UPnP AV Server und FTOP Server für eine Dateifreigabe rund um die Uhr.; Bearbeitungsfähigkeit von 300,000 Arbeitsvorgängen; und grüne Netzwerktechnologie von ASUS – eine Lösung für bis zu 70% Energieersparnis.

## 1.2 Packungsinhalt

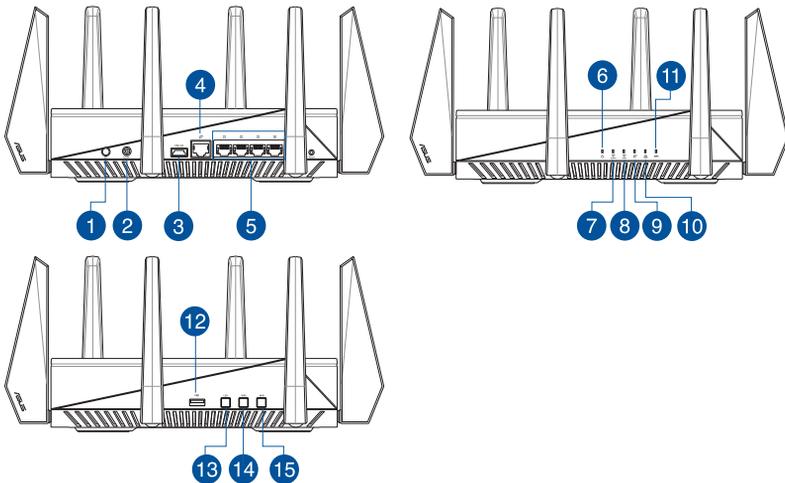
- |   |   |
|---|---|
| <input checked="" type="checkbox"/> RT-AC5300 drahtloser Router | <input checked="" type="checkbox"/> Netzteil          |
| <input checked="" type="checkbox"/> Netzwerkkabel (RJ-45)       | <input checked="" type="checkbox"/> Schnellstarthilfe |
| <input checked="" type="checkbox"/> Support CD ( Handbuch )     |   |

---

### Hinweise:

- Falls Artikel beschädigt oder nicht vorhanden sind, wenden Sie sich für technische Anfragen und Support an ASUS. Eine Liste der ASUS Support Hotlines finden Sie auf der Rückseite dieser Anleitung.
  - Bewahren Sie die Originalverpackung für den Fall eines zukünftigen Garantieanspruchs wie Nachbesserung oder Ersatz gut auf.
-

## 1.3 Der drahtlose Router



- 
- 1 Stromtaste**  
Mit dieser Taste können Sie Ihr System ein-/ausschalten.
- 
- 2 Stromanschluss (DC-IN)**  
Verbinden das mitgelieferte Netzteil mit diesem Anschluss und schließen Sie den Router an eine Stromversorgung an.
- 
- 3 USB 3.0-Anschluss**  
Verbinden Sie USB 3.0-Geräte wie USB-Festplatten oder -Flashlaufwerke mit diesen Anschlüssen.
- 
- 4 WAN-Anschluss (Internet)**  
Verbinden Sie ein Netzkabel mit diesem Anschluss, um eine WAN-Verbindung einzurichten.
- 
- 5 LAN-Anschlüsse 1~8**  
Verbinden Sie Netzkabel mit diesen Anschlüssen, um eine LAN-Verbindung einzurichten.
- 
- 6 Strom LED**  
**Aus:** Kein Strom.  
**An:** Gerät ist bereit.  
**Langsames Blinken:** Rettungsmodus
- 
- 7 2,4 GHz LED**  
**Aus:** Kein 2,4 GHz- oder 5GHz-Signal.  
**An:** Drahtlossystem ist bereit.  
**Blinkend:** Datenversand oder -empfang über die Drahtlosverbindung.
- 
- 8 5 GHz LED**  
**Aus:** Kein 2,4 GHz- oder 5GHz-Signal.  
**An:** Drahtlossystem ist bereit.  
**Blinkend:** Datenversand oder -empfang über die Drahtlosverbindung.
-

---

9

**WAN LED (Internet)**

**Aus:** Kein Strom oder keine physische Verbindung.

**An:** Physische Verbindung mit WAN (Wide Area Network).

---

10

**LAN LED**

**Aus:** Kein Strom oder keine physische Verbindung.

**An:** Physische Verbindung mit LAN (Lokales Netzwerk).

---

11

**WPS-LED**

**Aus:** Keine WPS-Verbindung.

**An:** Die WPS-Verbindung ist hergestellt.

---

12

**USB 2.0 port**

Insert USB 2.0 devices such as USB hard disks or USB flash drives into this port.

---

13

**LED-Einschalttaste**

Drücken Sie die Taste auf dem Panel zum Ein-/Ausschalten der LED.

---

14

**WPS-Taste**

Diese Taste startet den WPS-Assistenten.

---

15

**Wi-Fi-Einschalttaste**

Drücken Sie diese Taste zur De-/Aktivieren der WLAN-Verbindung..

---

---

**HINWEISE:**

- Verwenden Sie nur das mitgelieferte Netzteil. Andere Netzteile könnten das Gerät beschädigen.
- **Spezifikationen:**

<b>Netzteil</b>	Gleichstromausgang: +19V mit max/3.42A Strom;		
<b>Betriebstemperatur</b>	0~40oC	Lagerung	0~70oC
<b>Betriebsluftfeuchtigkeit</b>	50~90%	Lagerung	20~90%

---

## 1.4 Router Aufstellen

Für beste Funksignalübertragung zwischen dem drahtlosen Router und damit verbundenen Netzwerkgeräten sollten Sie:

- Den drahtlosen Router in einem zentralen Bereich für maximale Funkabdeckung der Netzwerkgeräte aufstellen.
- Das Gerät von Metallhindernissen oder direktem Sonnenlicht fernhalten.
- Das Gerät von 802.11g oder nur 20MHz Wi-Fi-Geräten, 2.4GHz Computerperipherie, Bluetooth-Geräten, schnurlosen Telefonen, Transformatoren, Hochleistungsmotoren, Neonlampen, Mikrowellen, Kühlschränken und anderen Industriegeräten fernhalten, um Signalstörungen oder -verlust zu vermeiden.
- Immer die aktuellste Firmware verwenden. Neueste Firmware finden Sie auf der ASUS-Webseite unter <http://www.asus.com>.

## 1.5 Einrichtungsvoraussetzungen

Zur Netzwerkeinrichtung benötigen Sie einen oder zwei Computer, die folgende Systemvoraussetzungen erfüllen:

- Ethernet RJ-45 (LAN)-Anschluss (10Base-T/100Base-TX/1000BaseTX)
- IEEE 802.11a/b/g/n/ac Drahtlosfunktion
- Verfügbarer TCP/IP-Dienst
- Ein Webbrowser wie Internet Explorer, Firefox, Safari, oder Google Chrome

---

### HINWEISE:

- Falls Ihr Computer über keine integrierte Drahtlosfunktion verfügt, können Sie einen IEEE 802.11a/b/g/n/ac WLAN-Adapter für die Netzwerkverbindung auf Ihrem Computer installieren.
  - Mit Dual-Band-Technologie ausgestattet, unterstützt Ihr Drahtlos-Router simultane 2.4GHz und 5GHz Drahtlossignale. Dies erlaubt die Ausführung normaler Internettätigkeiten wie das Surfen im Internet oder das Lesen/Schreiben von E-Mails im 2.4GHz-Frequenzbereich und das simultane Streaming von High-Definition Audio-/Videodateien wie Filme oder Musik im 5GHz-Frequenzbereich.
  - Bestimmte IEEE 802.11n-Geräte, die Sie in Ihr Netzwerk einbinden möchten, unterstützen das 5-GHz-Frequenzband eventuell nicht. Lesen Sie die technischen Daten in der Bedienungsanleitung des jeweiligen Gerätes nach.
  - Die für die Verbindung der Netzwerkgeräte verwendeten Ethernet RJ-45-Kabel sollten nicht länger als 100 Meter sein.
-

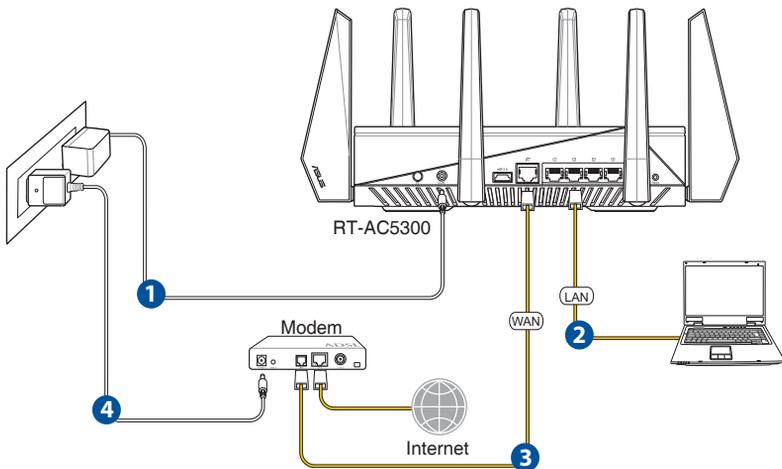
## 1.6 Router einrichten

### WICHTIG!

- Nutzen Sie zur Einrichtung Ihres WLAN-Routers eine Kabelverbindung, damit die Einrichtung problemlos vonstatten geht.
- Bevor Sie den drahtlosen ASUS Router aufbauen, sollten Sie:
  - Den aktuellen Router vom Netzwerk trennen (falls vorhanden).
  - Alle Kabel/Leitungen der aktuellen Modem-Konfiguration trennen. Entfernen Sie auch jegliche Batterien (falls vorhanden).
  - Starten Sie den Computer neu (empfohlen).

### 1.6.1 Kabelverbindung

**HINWEIS:** Bei Kabelverbindungen können Sie entweder ein 1:1-durchkontaktiertes („straight-through“) oder gekreuztes Kabel („crossover“) verwenden.



### So richten Sie die Kabelverbindung ein:

1. Verbinden Sie das Netzteil des Routers mit dem Stromanschluss (DC-IN) sowie mit der Stromversorgung.



3. Verbinden Sie das Netzteil des Modems mit dem Stromanschluss (DC-IN) sowie mit der Stromversorgung.
4. Installieren Sie einen IEEE 802.11a/b/g/n/ac WLAN-Adapter auf Ihrem Computer.

---

**HINWEISE:**

- Für Details zur Verbindung zu einem Drahtlosnetzwerk beziehen Sie sich auf das Handbuch Ihres WLAN-Adapters.
  - Zur Einrichtung der Sicherheitseinstellungen für Ihr Netzwerk beziehen Sie sich auf den Abschnitt **Einrichten der Drahtlos-Sicherheitseinstellungen** im Kapitel 3 in diesem Benutzerhandbuch.
-

## 2 Erste Schritte

### 2.1 Anmeldung im Web-GUI

Ihr drahtloser ASUS Router ist mit einer intuitiven webbasierten grafischen Oberfläche (GUI) ausgerüstet, um Ihnen die Einrichtung seiner vielseitigen Funktion durch einen Webbrowser wie Internet Explorer, Firefox, Safari oder Google Chrome zu erleichtern.

**HINWEIS:** Der Funktionsumfang kann je nach unterschiedlichen Firmware-Versionen variieren.

#### So melden Sie sich bei der Web-GUI an:

1. Geben Sie in Ihren Browser die IP-Adresse **192.168.1.1** manuell ein oder besuchen Sie die Webseite <http://router.asus.com>.
2. Geben Sie auf der Anmeldungsseite den vorgegebenen Benutzernamen (**admin**) und das Kennwort (**admin**) ein.
3. Zur Konfiguration der diversen Einstellungen Ihres ASUS-WLAN-Routers können Sie auch die grafische Benutzeroberfläche (GUI) verwenden.



**HINWEIS:** Wenn Sie sich zum ersten Mal an der grafischen Benutzeroberfläche anmelden, werden Sie automatisch zur Internet-Schnelleinrichtungsseite (ISE) geleitet.

## Quick Internet Setup (QIS) mit autom. Erkennung

Die Funktion Quick Internet Setup (QIS) führt Sie schnell durch die Einrichtung Ihrer Internetverbindung.

---

**HINWEIS:** Wenn Sie das eine Internetverbindung zum ersten Mal einrichten, drücken Sie die Reset-Taste, um den drahtlosen Router auf dessen Werkseinstellungen zurückzusetzen.

---

### So verwenden Sie QIS mit autom. Erkennung:

1. Melden Sie sich an der grafischen Benutzeroberfläche an. Die ISE-Seite öffnet sich automatisch.



---

#### Hinweise:

- Ab Werk sind Benutzername und Kennwort zur Anmeldung an der grafischen Benutzeroberfläche Ihres WLAN-Routers auf **admin** voreingestellt. Detaillierte Hinweise zum Ändern des Benutzernamens und des Kennwortes finden Sie in Abschnitt **4.6.2 System**.
- Benutzername und Kennwort zur Anmeldung am WLAN-Router unterscheiden sich vom 2,4-GHz/5-GHz-Netzwerkname (SSID genannt) und dem Sicherheitsschlüssel. Mit Benutzername und Kennwort können Sie sich an der grafischen Benutzeroberfläche des WLAN-Routers anmelden und die Einstellungen des Routers bequem konfigurieren. 2,4-GHz-/5-GHz-Netzwerkname (SSID) und Sicherheitsschlüssel sorgen dafür, dass sich andere WLAN-Geräte an Ihrem 2,4-GHz-/5-GHz-Netzwerk anmelden und damit verbinden können.

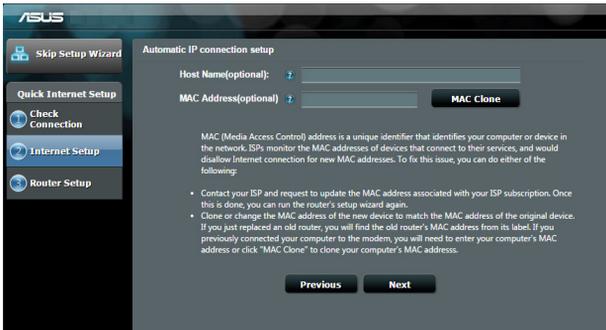
2. Der drahtlose Router erkennt automatisch, ob die Verbindungsart Ihres Internet Dienstanbieters (ISP) **Dynamische IP (Dynamic IP), PPPoE, PPTP, L2TP oder Statische IP (Static IP)** ist. Geben Sie zusätzlich die nötigen Daten Ihrer Verbindung ein.

---

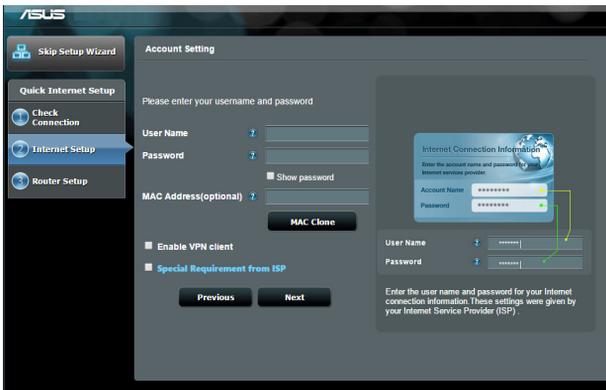
**WICHTIG!** Beziehen Sie die nötigen Informationen zur Ihrer Verbindungsart von Ihrem Internet-Dienstanbieter (ISP).

---

zur automatischen IP-Zuweisung (DHCP)



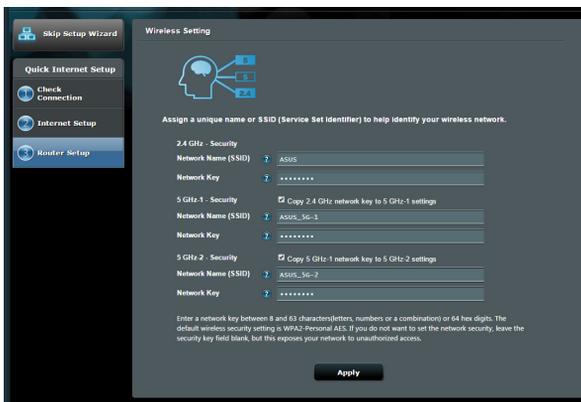
für PPPoE, PPTP und L2TP



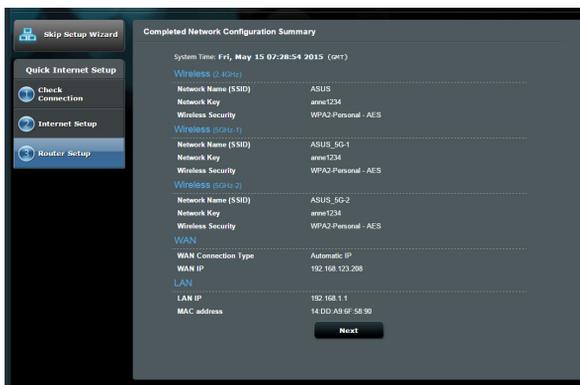
## HINWEISE:

- Die autom. Erkennung der Verbindungsart Ihres ISP wird bei der ersten Konfiguration des drahtlosen Routers oder nach dem Reset (Zurücksetzen) Ihres drahtlosen Routers zu seinen Standardeinstellungen durchgeführt.
- Falls QIS Ihre Verbindungsart nicht erkennt, klicken Sie auf **Manuelle Einstellung (Skip to manual setting)**; Siehe Abbildung in Schritt 1) und konfigurieren Sie die Verbindungseinstellungen manuell.

3. Weisen Sie einen Netzwerknamen (SSID) und einen Sicherheitsschlüssel für Ihre 2.4GHz- und 5 GHz- Drahtlosverbindung zu. Klicken Sie auf **Apply**, wenn Sie fertig sind.



4. Ihre Internet- und Drahtloseinstellungen werden angezeigt. Klicken Sie auf **Next**, um fortzufahren.
5. Lesen Sie die Drahtlosnetzwerk-Verbindungsanleitung und klicken Sie auf **Finish**, wenn Sie fertig sind.



## 2.3 Mit Ihrem WLAN-Netzwerk verbinden

Nachdem Sie Ihren WLAN-Router über ISE eingerichtet haben, können Sie Ihren Computer und andere kompatible Geräte mit Ihrem WLAN-Netzwerk verbinden.

### So verbinden Sie sich mit Ihrem Netzwerk:

1. Am Computer klicken Sie auf das Netzwerksymbol  im Benachrichtigungsbereich: Verfügbare WLAN-Netzwerke werden angezeigt.
2. Wählen Sie das WLAN-Netzwerk aus der Liste, mit dem Sie sich verbinden möchten, klicken Sie dann auf **Connect (Verbinden)**.
3. Bei einem abgesicherten WLAN-Netzwerke müssen Sie eventuell den Netzwerk-Sicherheitsschlüssel eingeben; anschließend klicken Sie auf **OK**.
4. Warten Sie ab, bis die Verbindung zum WLAN-Netzwerk erfolgreich hergestellt wurde. Der Verbindungsstatus wird angezeigt, das Netzwerksymbol signalisiert die Netzwerkverbindung .

---

### HINWEISE:

- In den nächsten Kapiteln finden Sie weitere Hinweise zur Konfiguration der WLAN-Netzwerkeinstellungen.
  - Details zur Verbindung mit Ihrem WLAN-Netzwerk finden Sie in der Bedienungsanleitung Ihres Gerätes.
-

# 3 Allgemeine Einstellungen konfigurieren

## 3.1 Netzwerkübersicht verwenden

Über die Netzwerkübersicht können Sie die Sicherheitseinstellungen Ihres Netzwerks konfigurieren, Ihre Netzwerk-Clients verwalten und Ihre USB-Geräte überwachen.



## 3.1.1 Einrichten der Drahtlos-Sicherheit

Um Ihr Netzwerk vor unautorisiertem Zugriff zu schützen, müssen Sie dessen Sicherheitseinstellungen einrichten.

### So richten Sie die Drahtlos-Sicherheitseinstellungen ein:

1. Wechseln Sie vom Navigationspanel zu **General (Allgemein)** > **Network Map (Netzwerkübersicht)**.
2. Im Fenster Network Map (Netzwerkübersicht) wählen Sie das Symbol **System status (Systemstatus)**, um Drahtlos-Sicherheitseinstellungen wie SSID, Sicherheitsstufe und Verschlüsselungseinstellungen anzuzeigen.

---

**HINWEIS:** Sie können für 2.4GHz-Band, 5GHz- und 5GHz-2-Band jeweils verschiedene Sicherheitseinstellungen einrichten.

---

### Sicherheitseinstellungen für 2.4GHz

System Status

2.4GHz 5GHz-1 5GHz-2 Status

Smart Connect:  OFF

Wireless name(SSID)  
ASUS

Authentication Method  
WPA2-Personal

WPA Encryption  
AES

WPA-PSK key  
\*\*\*\*\*

Apply

### Sicherheitseinstellungen für 5 GHz

System Status

2.4GHz 5GHz-1 5GHz-2 Status

Smart Connect:  OFF

Wireless name(SSID)  
ASUS\_5G-1

Authentication Method  
WPA2-Personal

WPA Encryption  
AES

WPA-PSK key  
\*\*\*\*\*

Apply

### Sicherheitseinstellungen für 5GHz-2

System Status

2.4GHz 5GHz-1 5GHz-2 Status

Smart Connect:  OFF

Wireless name(SSID)  
ASUS\_5G-2

Authentication Method  
WPA2-Personal

WPA Encryption  
AES

WPA-PSK key  
\*\*\*\*\*

Apply

3. Geben Sie im Feld **Wireless name (Drahtlos-Kennung, SSID)** Ihrem drahtlosen Netzwerk einen individuellen Namen.
4. Wählen Sie aus der **Authentication Method (Authentifizierungsverfahren)**-Auswahlliste das Authentifizierungsverfahren für Ihr Drahtlosnetzwerk.  
Falls Sie WPA-Personal oder WPA-2 Personal als Authentifizierungsverfahren wählen, geben Sie den WPA-PSK-Schlüssel oder das Sicherheitskennwort ein.

---

**WICHTIG!** Der IEEE 802.11n/ac-Standard erkennt die Verwendung eines hohen Durchsatzes mit WEP oder WPA-TKIP als Unicastchiffrierung nicht an. Falls Sie diese Verschlüsselungsmethoden verwenden, wird Ihre Datenrate auf die IEEE 802.11g 54Mbps-Verbindung herabgestuft.

---

5. Zum fertigstellen auf **Apply (Übernehmen)** klicken.

## 3.1.2 Verwalten der Netzwerk-Clients



All | By interface

All list - Hide lists...

Icon	Clients Name	Client IP address	Clients MAC Address	Radio	Tx Rate	Rx Rate	Access time
	Anne1_Chen-NB1	192.168.1.80	10:BF:48:6E:35:4E		N/A	N/A	N/A

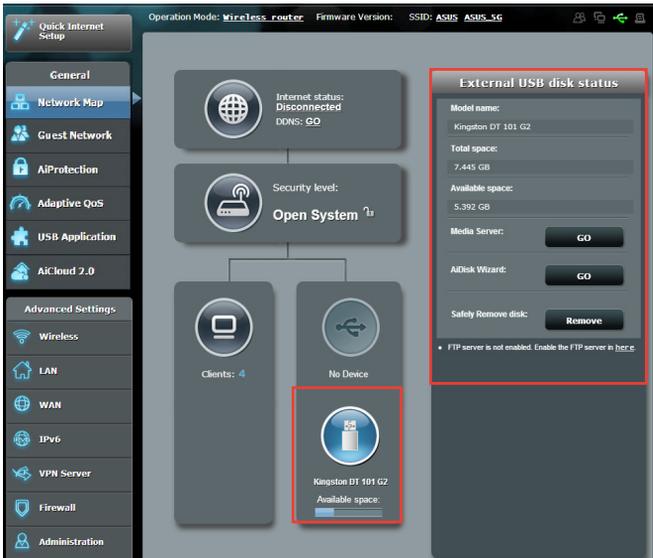
Export

### So verwalten Sie die Netzwerk-Clients:

1. Wechseln Sie vom Navigationspanel zu **General (Allgemein)** > **Network Map tab (Netzwerkübersicht-Register)**.
2. Wählen Sie im Fenster Network Map (Netzwerkübersicht) das Symbol **Client Status (Clientstatus)**, um Informationen über Ihre Netzwerk-Clients anzuzeigen.
3. Wenn Sie den Netzwerkzugriff eines Clients blockieren möchten, wählen Sie den Client aus und klicken anschließend auf **block (blockieren)**.

### 3.1.3 Überwachen der USB-Geräte

Der ASUS-WLAN-Router bietet zwei USB 2.0-Ports zum Anschluss von USB-Geräten oder USB-Druckern; so können Sie Dateien und Drucker mit Clients in Ihrem Netzwerk teilen.



#### HINWEISE:

- Um diese Funktion zu verwenden, müssen Sie einen USB-Datenträger wie ein USB-Laufwerk oder USB-Flashlaufwerk mit dem USB 3.0/2.0-Anschluss auf der Rückseite Ihres drahtlosen Routers verbinden. Stellen Sie sicher, dass der USB-Datenträger richtig formatiert und partitioniert wurde. Für eine Tabelle unterstützter Dateisysteme für Ihre Laufwerke beziehen Sie sich auf die ASUS-Webseite unter <http://event.asus.com/networks/disksupport>
- An die USB-Ports können zwei USB-Laufwerke oder ein Drucker und ein USB-Laufwerk gleichzeitig angeschlossen werden.

---

**WICHTIG!** Wenn Sie anderen Netzwerk-Clients per FTP-Site/ Drittanbieter-FTP-Clients, Servercenter, Samba oder AiCloud Zugriff auf das USB-Gerät gewähren möchten, müssen Sie zunächst ein Freigabekonto und dessen Berechtigungen/Zugriffsrechte einrichten. Weitere Hinweise dazu finden Sie in den Abschnitten **3.5 USB-Anwendungen verwenden** und **3.6 AiCloud verwenden** in dieser Bedienungsanleitung.

---

### **So überwachen Sie die USB-Geräte:**

1. Wechseln Sie vom Navigationspanel zu **General (Allgemein) > Network Map (Netzwerkübersicht)**.
2. Wählen Sie im Fenster Network Map (Netzwerkübersicht) das Symbol **USB Disk Status (USB-Laufwerksstatus)**, um Informationen über Ihre USB-Geräte anzuzeigen.
3. Klicken Sie im Feld AiDisk Wizard (AiDisk-Assistent) auf **GO (Los)**, um einen FTP-Server für die Dateifreigabe im Internet einzurichten.

---

### **HINWEISE:**

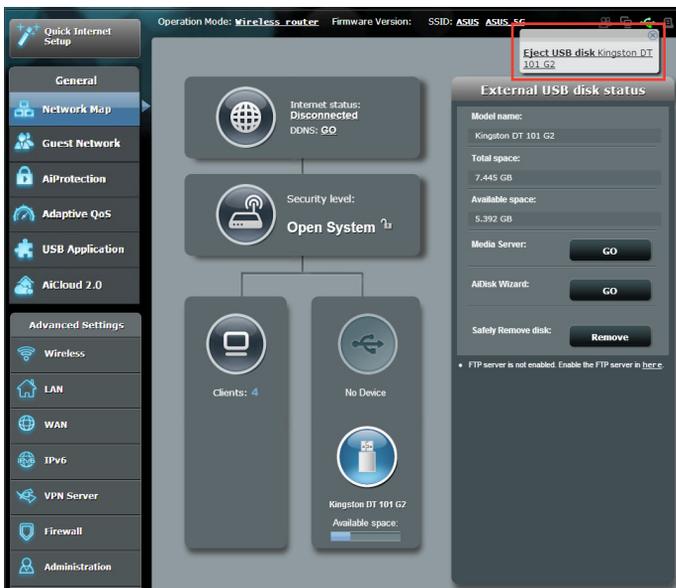
- Weitere Hinweise dazu finden Sie in Abschnitt **3.5.2 Servercenter verwenden** in dieser Anleitung.
  - Der drahtlose Router läuft mit den meisten USB-Festplatten/ Flashlaufwerken (bis zu 2TB) und unterstützt Lese-/Schreibzugriff in FAT16, FAT32, NTFS und HFS+.
-

## USB-Laufwerk sicher trennen

**WICHTIG:** Ein falsches Trennen des USB-Laufwerks kann zu Datenverlusten führen.

### So trennen Sie das USB-Laufwerk auf sichere Weise:

1. Wechseln Sie vom Navigationspanel zu **General (Allgemein)** > **Network Map (Netzwerkübersicht)**.
2. Klicken Sie in der oberen rechten Ecke auf  > **Eject USB disk (USB-Laufwerk trennen)**. Wenn das USB-Laufwerk erfolgreich getrennt wurde, wird als USB-Status **Unmounted (Getrennt)** angezeigt.



## 3.2 Erstellen eines Gästernetzwerkes

Das Gästernetzwerk ermöglicht zeitweiligen Besuchern den Zugriff auf das Internet. Dazu werden separate SSIDs oder Netzwerke verwendet, die keinen Zugang zu Ihrem privaten Netzwerk ermöglichen.

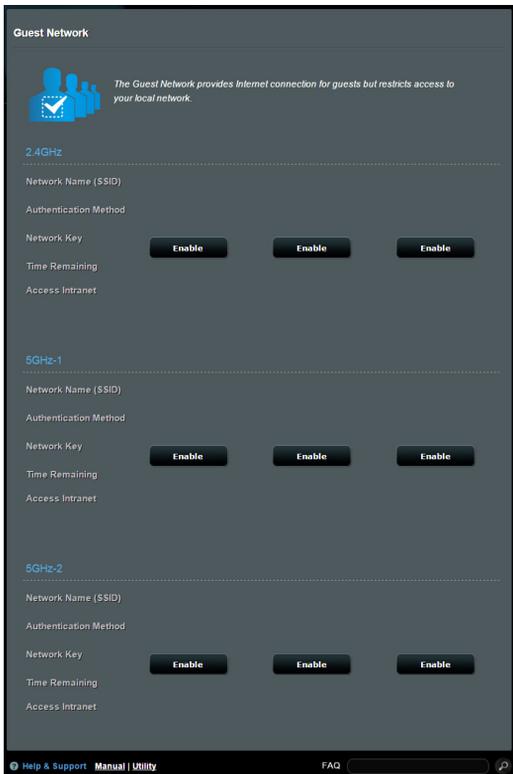
---

**HINWEIS:** Der RT-AC5300 unterstützt bis zu sechs SSIDs (drei 2,4-GHz- und drei 5-GHz-SSIDs).

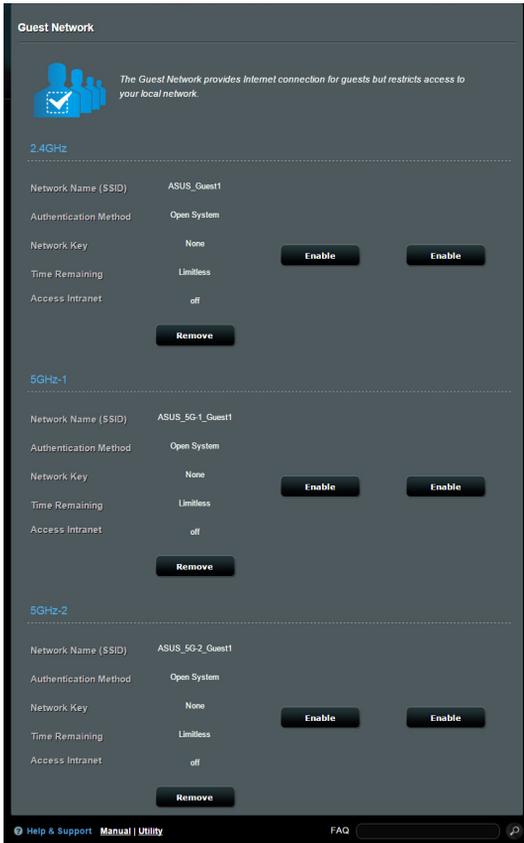
---

### So erstellen Sie ein Gästernetzwerk:

1. Wechseln Sie vom Navigationspanel zu **General (Allgemein) > Guest Network (Gästernetzwerk)**.
2. Im Guest Network (Gästernetzwerk)-Bildschirm wählen Sie, ob Sie das 2,4-GHz- oder 5-GHz-Frequenzband für Ihr Gästernetzwerk verwenden möchten.
3. Klicken Sie auf **Enable (Aktivieren)**.



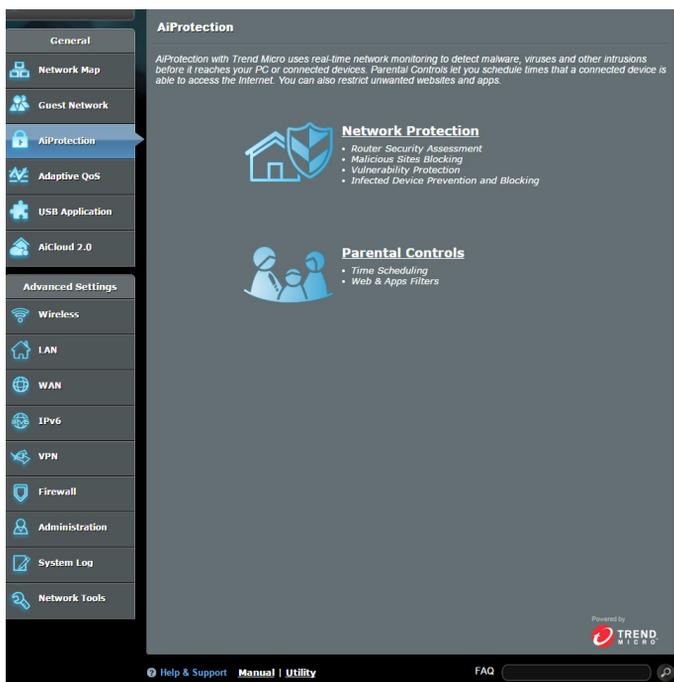
- Wenn Sie zusätzliche Optionen konfigurieren möchten, klicken Sie auf **Modify (Modifizieren)**. Klicken Sie im **Gästenetzwerk-**Bildschirm auf **Entfernen**.
- Legen Sie im Feld **Network Name (SSID) (Netzwerkname (SSID))** einen Namen für Ihr temporäres Netzwerk fest.



- Wählen Sie ein **Authentication Method (Autentisierungsverfahren)**.
- Wählen Sie eine **Verschlüsselungsmethode**.
- Legen Sie die **Access time (Zugangszeiten)** fest oder wählen Sie **Limitless (Unbeschränkt)**.
- Wählen Sie unter **Access Intranet (Intranetzugriff)** zwischen den Optionen **Disable (Deaktivieren)** und **Enable (Aktivieren)**.
- Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.

## 3.3 AiProtection

AiProtection bietet Echtzeitüberwachung, die Malware, Spyware und unerwünschten Zugriff erkennt. Es filtert außerdem unerwünschte Webseiten und Apps und ermöglicht die Festlegen einer Zeit, zu der ein verbundenes Gerät auf das Internet zugreifen kann.



### 3.3.1 Network Protection (Netzwerkschutz)

Network Protection (Netzwerkschutz) verhindert Netzwerksicherheitslücken und schützt Ihr Netzwerk vor unerwünschten Zugriff.

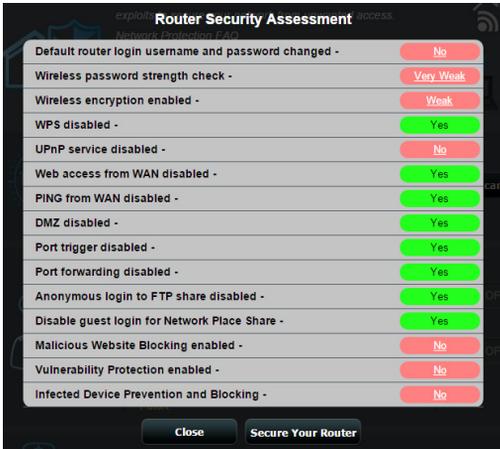


#### Network Protection (Netzwerkschutz) konfigurieren

So konfigurieren Sie Network Protection (Netzwerkschutz):

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **AiProtection**.
2. Klicken Sie auf der **AiProtection**-Hauptseite auf **Network Protection (Netzwerkschutz)**.
3. Klicken Sie im Register **Network Protection (Netzwerkschutz)** auf **Scan (Suchen)**.

Nach der Suche zeigt das Dienstprogramm die Ergebnisse auf der Seite **Router Security Assessment (Router-Sicherheitsbewertung)**.




---

**WICHTIG!** Mit **Yes (Ja)** auf der Seite **Router Security Assessment (Router-Sicherheitsbewertung)** markierte Elemente gelten als **sicher**. Mit **No (Nein)**, **Weak (Schwach)** oder **Very Weak (Sehr schwach)** markierte Elemente sollten unbedingt konfiguriert werden.

---

4. (Optional) Konfigurieren Sie auf der Seite **Router Security Assessment (Router-Sicherheitsbewertung)** manuell die mit **No (Nein)**, **Weak (Schwach)** oder **Very Weak (Sehr schwach)** markierten Elemente. Gehen Sie dazu wie folgt vor:
  - a. Klicken Sie auf ein Element.

---

**HINWEIS:** Wenn Sie ein Element anklicken, führt Sie das Dienstprogramm zur Einstellungsseite des Elements.

---

- b. Nehmen Sie auf der Sicherheitseinstellungsseite des Elements die erforderlichen Änderungen vor; klicken Sie anschließend auf **Apply (Übernehmen)**.
  - c. Kehren Sie auf die Seite **Router Security Assessment (Router-Sicherheitsbewertung)** zurück und klicken Sie zum Verlassen der Seite auf **Close (Schließen)**.
5. Klicken Sie zum automatischen Konfigurieren der Sicherheitseinstellungen auf **Secure Your Router (Ihren Router sichern)**.
6. Wenn eine Mitteilung erscheint, klicken Sie auf **OK**.

## Malicious Sites Blocking (Blockierung schädlicher Seiten)

Diese Funktion beschränkt den Zugriff auf bekannte bedrohliche Webseiten in der Cloud-Datenbank, damit der Schutz immer auf dem neuesten Stand ist.

---

**HINWEIS:** Diese Funktion wird automatisch aktiviert, wenn Sie **Router Weakness Scan (Suche nach Schwächen des Routers)** ausführen.

---

### So aktivieren Sie Malicious Sites Blocking (Blockierung schädlicher Seiten):

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **AiProtection**.
2. Klicken Sie auf der **AiProtection**-Hauptseite auf **Network Protection (Netzwerkschutz)**.
3. Klicken Sie im Bereich **Malicious Sites Blocking (Blockierung schädlicher Seiten)** auf **ON (Ein)**.

## Vulnerability protection (Schutz vor Schwachstellen)

Diese Funktion behebt herkömmliche Schwachstellen innerhalb der Router-Konfiguration.

---

**HINWEIS:** Diese Funktion wird automatisch aktiviert, wenn Sie **Router Weakness Scan (Suche nach Schwächen des Routers)** ausführen.

---

### So aktivieren Sie Vulnerability protection (Schutz vor Schwachstellen):

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **AiProtection**.
2. Klicken Sie auf der **AiProtection**-Hauptseite auf **Network Protection (Netzwerkschutz)**.
3. Klicken Sie im Bereich **Vulnerability protection (Schutz vor Schwachstellen)** auf **ON (Ein)**.

## **Infected Device Prevention and Blocking (Prävention und Blockierung infizierter Geräte)**

Diese Funktion verhindert, dass infizierte Geräte persönliche Informationen oder den infizierten Status an externe Parteien kommunizieren.

---

**HINWEIS:** Diese Funktion wird automatisch aktiviert, wenn Sie **Router Weakness Scan (Suche nach Schwächen des Routers)** ausführen.

---

### **So aktivieren Sie Vulnerability protection (Schutz vor Schwachstellen):**

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **AiProtection**.
2. Klicken Sie auf der **AiProtection**-Hauptseite auf **Network Protection (Netzwerkschutz)**.
3. Klicken Sie im Bereich **Infected Device Prevention and Blocking (Prävention und Blockierung infizierter Geräte)** auf **ON (Ein)**.

### **So aktivieren Sie Alert Preference (Alarmpräferenz):**

1. Klicken Sie im Bereich **Infected Device Prevention and Blocking (Prävention und Blockierung infizierter Geräte)** auf **Alert Preference (Alarmpräferenz)**.
2. Geben Sie durch Auswahl oder Eingabe E-Mail-Anbieter, E-Mail-Konto und Kennwort an, klicken Sie dann auf **Apply (Übernehmen)**.

### 3.3.2 Parental Controls (Jugendschutz) einrichten

Mit Parental Controls (Jugendschutz) können Sie die Zeiten für Internetzugriff oder die Dauer für die Netzwerknutzung eines Clients festlegen.

So rufen Sie die Parental Controls(Jugendschutz)-Hauptseite auf:

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **AiProtection**.
2. Klicken Sie auf der **AiProtection**-Hauptseite auf das Register **Parental Controls (Jugendschutz)**.

ASUS

Logout Reboot English

Operation Mode: **Wireless router** Firmware Version: SSID: ASUS ASUS\_5G

Network Protection Parental Controls

### AiProtection - Web & Apps Filters

Web & Apps Filters Time Scheduling

Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:

1. In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.
2. Check the unwanted content categories
3. Click the plus (+) icon to add rule then click apply.

If you want to disable the rule temporarily, uncheck the check box in front of rule.  
[Parental Controls FAQ](#)

Web & Apps Filters  ON

#### Client List (Max Limit :: 16)

Client name	Content Category	Add / Delete
<input checked="" type="checkbox"/> android-8fcbcbf	<ul style="list-style-type: none"><li><input checked="" type="checkbox"/> <b>Adult</b> Block adult content can prevent child from visiting sexy, violence and illegal related content.</li><li><input checked="" type="checkbox"/> <b>Instant Message and Communication</b> Block IM and communication content can prevent child from addicted to social networking usage.</li><li><input checked="" type="checkbox"/> <b>P2P and File Transfer</b> Block P2P and File Transfer content can keep your network in a better transmission quality.</li><li><input checked="" type="checkbox"/> <b>Streaming and Entertainment</b> Block Streaming and Entertainment content can prevent child from spending long time on internet entertainment.</li></ul>	<input type="checkbox"/>
No data in table		

Apply

Powered by TREND MICRO

Help & Support Manual Utility FAQ

## Web & Apps Filters (Web- und App-Filter)

Web & Apps Filters (Web- und App-Filter) ist eine **Parental Controls (Jugendschutz)**-Funktion, mit der Sie den Zugriff auf unerwünschte Webseiten oder Applikationen blockieren können.

### So konfigurieren Sie Web & Apps Filters (Web- und App-Filter):

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **AiProtection**.
2. Klicken Sie auf der **AiProtection**-Hauptseite auf das Symbol **Parental Controls (Jugendschutz)** und Sie gelangen zum Register **Parental Controls (Jugendschutz)**.
3. Klicken Sie im Bereich **Enable Web & Apps Filters (Web- und App-Filter aktivieren)** auf **ON (Ein)**.
4. Wenn die Meldung zur Endbenutzer-Lizenzvereinbarung angezeigt wird, klicken Sie zum Fortfahren auf **I agree (Ich stimme zu)**.
5. Geben Sie in der Spalte **Client List (Client-Liste)** durch Auswahl aus der Liste oder Eingabe den Client-Namen an.
6. Wählen Sie in der Spalte **Content Category (Inhaltskategorie)** die Filter aus den vier Hauptkategorien: **Adult (Erwachsene)**, **Instant Message and Communication (Sofortmitteilungen und Kommunikation)**, **P2P and File Transfer (P2P und Dateitransfer)** und **Streaming and Entertainment (Streaming und Unterhaltung)**.
7. Klicken Sie zum Hinzufügen des Client-Profiles auf .
8. Klicken Sie zum Speichern der Einstellungen auf **Apply (Übernehmen)**.

## Time Scheduling (Zeitplanung)

Time Scheduling (Zeitplanung) ermöglicht die Festlegung eines Zeitlimits für die Netzwerknutzung eines Clients.

**HINWEIS:** Stellen Sie sicher, dass Ihre Systemzeit mit dem NTP-Server synchronisiert ist.

ASUS

Logout Reboot English

Operation Mode: Wireless router Firmware Version: SSID: ASUS\_ASUS\_5G

Network Protection Parental Controls

AiProtection - Time Scheduling

Web & Apps Filters Time Scheduling

Time Scheduling allows you to set the time limit for a client's network usage. To use Time Scheduling:

1. In the (Clients Name) column, select the client whose network usage you want to control. You may also key in the clients MAC address in the (Clients MAC Address) column.
2. In the (Add / Delete) column, click the plus (+) icon to add the client.
3. In the (Time Management) column, click the edit icon to edit the Active Schedule.
4. Select the desired time slots for allowed access times. Drag and hold to create longer time slots.
5. Click [OK] to save the settings made.

• Click to open the tutorial video.

Note: Clients that are added to Parental Controls will have their internet access restricted by default.

Enable Time Scheduling

System Time Wed, Nov 12 10:11:39 2014  
\* Remind: The System time zone is different from your locale setting.

Client List (Max Limit : 16)

Clients Name	Clients MAC Address	Time Management	Add / Delete
No data in table.			

Apply

Help & Support Manual Utility FAQ

### So konfigurieren Sie Time Scheduling (Zeitplanung):

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **AiProtection** > **Parental Controls (Jugendschutz)** > **Time Scheduling (Zeitplanung)**.
2. Klicken Sie im Bereich **Enable Time Scheduling (Zeitplanung aktivieren)** auf **ON (Ein)**.

3. Geben Sie in der Spalte **Clients Name (Client-Name)** durch Auswahl aus der Liste oder Eingabe den Client-Namen an.

---

**HINWEIS:** Sie können die MAC-Adresse des Clients auch in die **Client MAC Address (Client-MAC-Adresse)**-Spalte eintragen. Achten Sie darauf, dass der Name des Clients keine Sonderzeichen oder Leerzeichen enthält; andernfalls können Fehlfunktionen des Routers auftreten.

---

4. Klicken Sie zum Hinzufügen des Client-Profiles auf .
5. Klicken Sie zum Speichern der Einstellungen auf **Apply (Übernehmen)**.

## 3.4 Adaptive QoS

### 3.4.1 Bandwidth Monitor (Bandbreitenüberwachung)

Diese Funktion ermöglicht Ihnen die Überwachung der WAN/LAN-Bandbreite und zeigt die Upload- und Download-Geschwindigkeit Ihrer Verbindung.



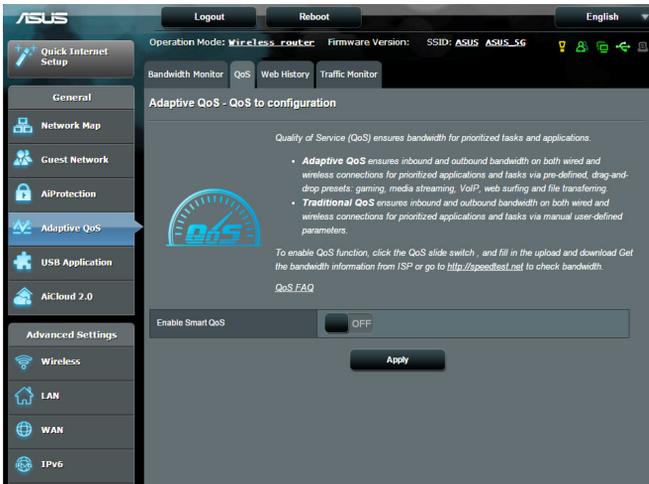
### Apps analysis (App-Analyse)

**So aktivieren Sie Apps analysis (App-Analyse):**

Rufen Sie im Register **Bandwidth Monitor (Bandbreitenüberwachung)** den Bereich **Apps Analysis (App-Analyse)** auf, klicken Sie dann auf **ON (Ein)**.

## 3.4.2 QoS

Diese Funktion sichert Bandbreite für bevorzugte Aufgaben und Applikationen.



### So aktivieren Sie die QoS-Funktion:

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **Adaptive QoS** > **QoS-Register**.
2. Klicken Sie im Bereich **Enable Smart QoS (Intelligente QoS aktivieren)** auf **ON (Ein)**.
3. Füllen Sie die Felder zur Upload- und Download-Bandbreite aus.

---

**HINWEIS:** Sie erhalten die Bandbreiteninformationen von Ihrem Internetanbieter. Alternativ können Sie unter <http://speedtest.net> Ihre Bandbreite prüfen.

---

4. Wählen Sie den QoS Type (QoS-Typ) (Adaptive (Adaptiv) oder Traditional (Traditionell)) für Ihre Konfiguration.

---

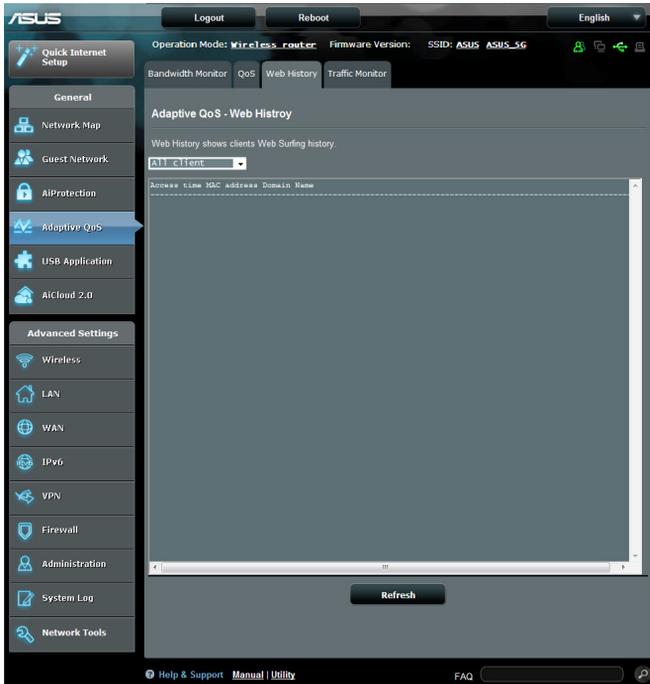
**HINWEIS:** Die Definition zum QoS Type (QoS-Typ) wird als Referenz im QoS-Register angezeigt.

---

5. Klicken Sie auf **Apply (Übernehmen)**.

### 3.4.3 Web History (Webverlauf)

Diese Funktion zeigt Verlauf und Details der Seiten oder URLs, die der Client besucht hat.

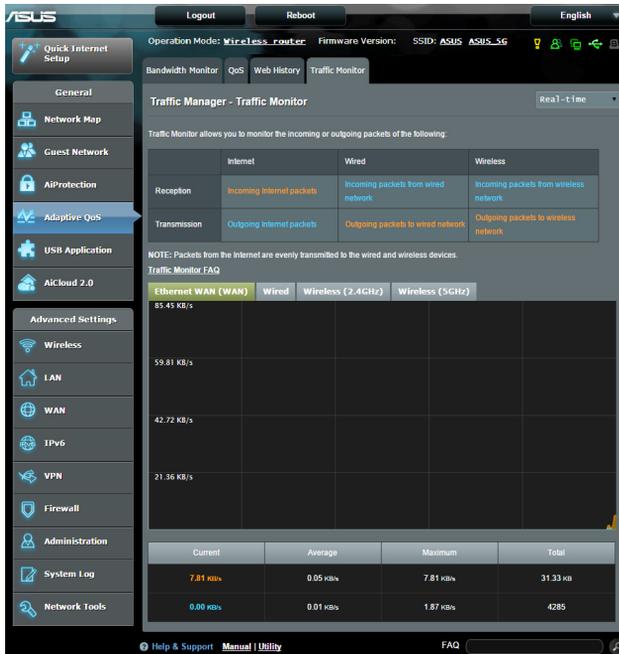


**So rufen Sie Web History (Webverlauf) auf:**

1. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **Adaptive QoS** > **Web History (Webverlauf)**-Register.
2. (Optional) Klicken Sie zum Leeren der Liste auf **Refresh (Aktualisieren)**.

## 3.4.4 Traffic Monitor (Datenverkehrsüberwachung)

Über die Funktion zur Datenverkehrsüberwachung können Sie die Bandbreitennutzung von Internet, Kabel- und WLAN-Netzwerken abrufen. Dabei können Sie den Netzwerkverkehr in Echtzeit oder auf täglicher Basis überwachen. Zudem gibt es eine Option zur Anzeige des Netzwerkverkehrs innerhalb der letzten 24 Stunden.



### So konfigurieren Sie Traffic Monitor (Datenverkehrsüberwachung):

1. Wählen Sie über den Navigationsbereich **General (Allgemein) > Adaptive QoS > Traffic Monitor (Datenverkehrsüberwachung)**-Register.
2. (Optional) Wählen Sie im Bereich **Traffic Manager - Traffic Monitor (Datenverkehrsmanager - Datenverkehrsüberwachung)** eine Option (**Real-Time (Echtzeit)**, **Last 24 Hours (Die letzten 24 Stunden)** oder **Daily (Täglich)**) aus der Auswahlliste.

## 3.5 USB-Anwendungen verwenden

Die USB-Erweiterungsfunktion bietet AiDisk-, Servers Center-, Netzwerkdrucker-Server- und Download Master-Untermenüs an.

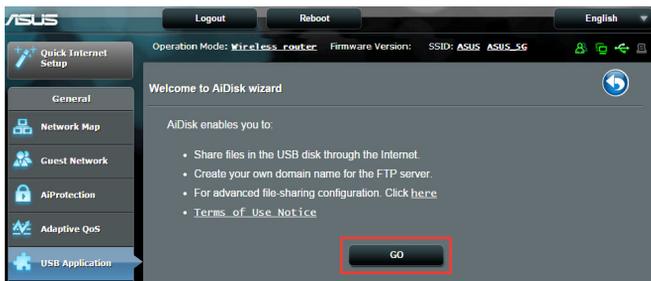
**WICHTIG!** Zum Einsatz der Serverfunktionen müssen Sie ein USB-Speichergerät (beispielsweise USB-Festplatte oder USB-Flash-Laufwerk) an den USB 2.0-Port an der Rückwand Ihres WLAN-Routers anschließen. Sorgen Sie dafür, dass das USB-Speichergerät formatiert und richtig partitioniert ist. Eine Tabelle mit unterstützten Dateisystemen finden Sie auf den ASUS-Internetseiten: <http://event.asus.com/2009/networks/disksupport/>.

### 3.5.1 AiDisk verwenden

AiDisk erlaubt es Ihnen, den Inhalt eines USB-Laufwerks im Internet freizugeben. AiDisk unterstützt Sie bei der Einrichtung von ASUS-DDNS und einem FTP-Server.

#### So verwenden Sie AiDisk:

1. Wechseln Sie vom Navigationspanel zu **General (Allgemein) > USB application (USB-Anwendungen)**, klicken Sie dann auf das **AiDisk**-Symbol.
2. Klicken Sie im Willkommen-Bildschirm des AiDisk-Assistenten auf **Go**.



3. Wählen Sie die Zugriffsrechte, die Sie den Clients, welche auf Ihre freigegebenen Daten zugreifen, zuweisen wollen.



4. Um mit dem ASUS DDNS-Dienst eine eigene Domäne für Ihre FTP-Seite einzurichten, wählen Sie **I will use the service and accept the Terms of service (Ich werde den Dienst nutzen und die Nutzungsbedingungen akzeptieren)** und geben Sie den Domännennamen ein. Klicken Sie dann auf **Next**.



Zum Überspringen der DDNS-Einstellungen können Sie auch **Skip ASUS DDNS settings (ASUS-DDNS-Einstellungen überspringen)** wählen und anschließend auf **Next (Weiter)** klicken.

5. Klicken Sie auf **Finish**, um die Einrichtung abzuschließen.
6. Um auf die von Ihnen erstellte FTP-Seite zuzugreifen, starten Sie einen Webbrowser oder eine FTP-Anwendung eines Drittanbieters und geben Sie den von Ihnen erstellten FTP-Link ein (**ftp://<domain name>.asuscomm.com**).

## 3.5.2 Servercenter verwenden

Mit dem Servercenter können Sie Mediendateien des USB-Laufwerks über einen Medienserver-Ordner, den Samba- oder FTP-Freigabedienst teilen. Außerdem können Sie im Servercenter auch weitere Einstellungen des USB-Laufwerks konfigurieren.

### Medienserver verwenden

Ihr WLAN-Router ermöglicht DLNA-kompatiblen Geräten den Zugriff auf Multimediadateien, die auf dem an Ihren WLAN-Router angeschlossenen USB-Laufwerk gespeichert sind.

---

**HINWEIS:** Verbinden Sie Ihr Gerät mit dem RT-AC5300-Netzwerk, bevor Sie die DLNA-Medienserverfunktionen nutzen.

---

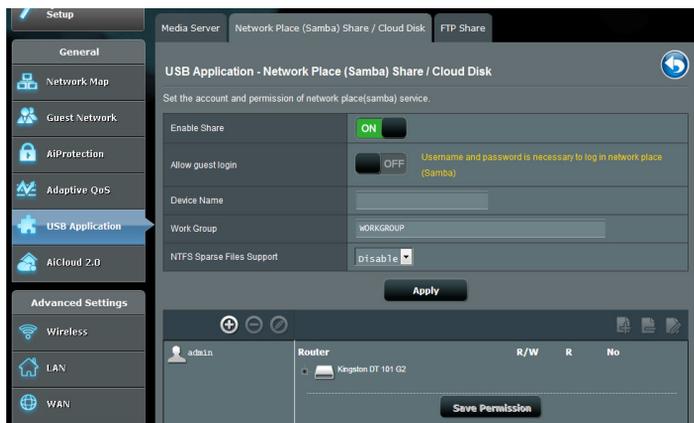


Wechseln Sie zum Aufrufen der Medienserver-Einstellungseite zum Register **General (Allgemein) > USB application (USB-Applikation) > Media Services and Servers (Mediendienste und -server) > Media Servers (Medienserver)**-Register. Hier eine Beschreibung der einzelnen Felder:

- **iTunes-Server aktivieren?:** Mit Ein/Aus aktivieren/deaktivieren Sie den iTunes-Medienserver.
- **DLNA-Medienserver aktivieren:** Mit Ein/Aus aktivieren/deaktivieren Sie den DLNA-Medienserver.
- **Medienserverstatus:** Zeigt den Status des Medienservers.
- **Medienserverordner:** Wählen Sie Ihren Medienserverordner, klicken Sie dann auf **Apply (Übernehmen)**, damit Mediengeräte im Netzwerk auf die Dateien des USB-Laufwerks zugreifen können.

## Netzwerkplatz (Samba) Freigabeservice

Netzwerkplatz (Samba) Freigabe ermöglicht es Ihnen ein Konto und Rechte für den Samba Service einzurichten.



**So verwenden Sie die Samba-Freigabe:**

1. Wechseln Sie vom Navigationspanel zu **GGeneral (Allgemein) > USB application (USB-Applikation) > Media Services and Servers (Mediendienste und -server) > Network Place (Samba) Share / Cloud Disk (Netzwerkumgebungsfreigabe (Samba) / Cloud-Datenträger)**.

---

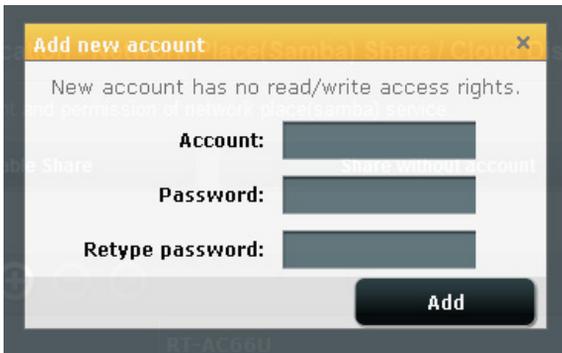
**HINWEIS:** Per Vorgabe ist die Netzwerkumgebung-Freigabe (Samba) aktiv.

---

2. Führen Sie die Schritte zum Zufügen, Löschen oder Modifizieren eines Kontos aus.

### So erstellen Sie ein neues Konto:

- a) Klicken Sie zum Zufügen eines neuen Kontos auf .
- b) Geben Sie Namen und Kennwort Ihres Netzwerk-Clients in die Felder **Account (Konto)** und **Password (Kennwort)** ein. Geben Sie das Kennwort zur Bestätigung noch einmal ein. Klicken Sie zum Zufügen des Kontos zur Liste auf **Add (Zufügen)**.



### So löschen Sie ein vorhandenes Konto:

- a) Wählen Sie das Konto, das Sie löschen möchten.
- b) Klicken Sie auf .
- c) Klicken Sie zum Bestätigen der Kontenlöschung auf **Delete (Löschen)**.

### So fügen Sie einen Ordner hinzu:

- a) Klicken Sie auf .
- b) Geben Sie den Ordernamen ein, klicken Sie dann auf **Add (Zufügen)**. Der soeben angelegte Ordner wird der Ordnerliste zugefügt.



3. Wählen Sie in der Liste der Dateien/Ordner die Art von Zugriffsrechten, die Sie bestimmten Dateien/Ordnern zuweisen möchten:
  - **R/W:** Wählen Sie diese Option, um Lese-/Schreibzugriff für bestimmte Datei/Ordner zuzuweisen.
  - **L:** Diese Option wählen Sie zum schreibgeschützten Zugriff.
  - **No:** Wählen Sie diese Option, wenn Sie bestimmte Datei/ Ordner nicht freigeben möchten.
4. Zum Anwenden klicken Sie auf **Apply (Übernehmen)**.

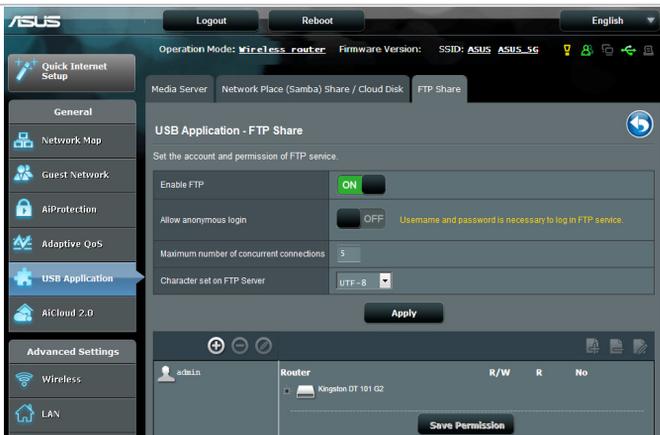
## FTP-Freigabeservice verwenden

Die FTP-Freigabe ermöglicht einem FTP-Server die Freigabe von Dateien eines USB-Laufwerks zur Nutzung mit anderen Geräten; per lokalem Netzwerk oder Internet.

---

### WICHTIG:

- Sie sollten USB-Datenträger immer sicher entfernen. Falsches Entfernen von USB-Datenträgern kann zu Datenverlusten führen.
- Zum sicheren Trennen eines USB-Laufwerks lesen Sie bitte **USB-Laufwerk sicher trennen** im **Abschnitt 3.1.3 USB-Geräte überwachen**.



## So nutzen Sie den FTP-Freigabedienst:

---

**HINWEISE:** Sorgen Sie dafür, dass Sie FTP-Server über AiDisk eingerichtet wurde. Mehr Details dazu finden Sie im Abschnitt **3.5.1 AiDisk verwenden**.

---

1. Wechseln Sie vom Navigationspanel zum Register **General (Allgemein) > USB application (USB-Anwendungen) > edia Services and Servers (Mediendienste und -server) > FTP Share (FTP-Freigabe)**.
2. Wählen Sie in der Liste der Ordner die Art von Zugriffsrechten, die Sie bestimmten Dateien/Ordern zuweisen möchten:
  - **R/W:** Wählen Sie diese Option, um Lese-/Schreibzugriff für bestimmte Ordner zuzuweisen.
  - **W:** Wählen Sie diese Option, um nur einen Schreibzugriff für bestimmte Ordner zuzuweisen.
  - **R:** Wählen Sie diese Option, um nur einen Lesezugriff für bestimmte Ordner zuzuweisen.
  - **No:** Wählen Sie diese Option, wenn Sie bestimmte Ordner nicht freigeben möchten.
3. Wenn Sie möchten, können Sie das Feld **Allow anonymous login (Anonyme Anmeldung erlauben)** auf **ON (Ein)** einstellen.
4. Geben Sie im Feld **Maximum number of concurrent connections (Maximale Anzahl gleichzeitiger Verbindungen)** die Anzahl Geräte an, die gleichzeitig eine Verbindung zum FTP-Freigabeserver herstellen können.
5. Zum Anwenden klicken Sie auf **Apply (Übernehmen)**.
6. Um auf den FTP-Server zuzugreifen, geben Sie den FTP-Link **ftp://<hostname>.asuscomm.com** sowie Ihren Benutzernamen und Kennwort in einen Webbrowser oder eine FTP-Anwendung eines Drittanbieters ein.

### 3.5.3 3G/4G

3G/4G-USB-Modems lassen sich zum Internetzugriff mit dem RT-AC5300 verbinden.

---

HINWEIS: Eine Liste nachweislich funktionierender USB-Modems finden Sie hier:

<http://event.asus.com/2009/networks/3gsupport/>

---

#### So richten Sie den 3G/4G-Internetzugriff ein:

1. Klicken Sie im Navigationspanel auf **General (Allgemein)**> **USB application (USB-Anwendungen)**> **3G/4G (3G/4G)**.
2. Im Feld **Enable USB Modem (USB-Modem aktivieren)** wählen Sie **Yes (Ja)** aus.
3. Richten Sie Folgendes ein:
  - **Standort:** Wählen Sie den Standort Ihres 3G/4G-Anbieters aus der Auswahlliste.
  - **Internetanbieter:** Wählen Sie Ihren Internetanbieter aus der Auswahlliste.
  - **APN- (Zugangspunktname)-Service (optional):** Entsprechende Informationen erhalten Sie von Ihrem 3G/4G-Anbieter.
  - **Einwahlnummer und PIN-Code:** Einwahlnummer und PIN-Code zur Verbindung mit Ihrem 3G/4G-Anbieter.

---

**HINWEIS:** Der PIN-Code kann je nach Anbieter unterschiedlich ausfallen.

---

- **Benutzername/Kennwort:** Benutzernamen und Kennwort erhalten Sie von Ihrem 3G/4G-Anbieter.
  - **USB-Adapter:** Wählen Sie Ihren USB-3G/4G-Adapter aus der Auswahlliste. Falls Sie Ihr USB-Adaptermodell nicht kennen oder das Modell nicht aufgelistet werden sollte, wählen Sie **Auto**.
4. Klicken Sie auf **Apply (Übernehmen)**.

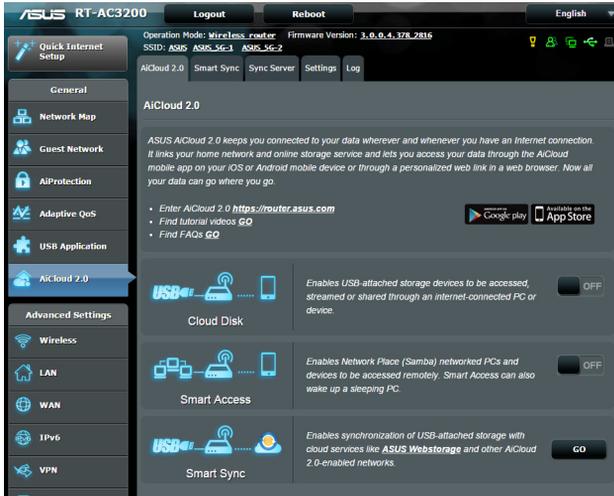
---

**HINWEIS:** Der Router startet neu, damit die Einstellungen in Kraft treten können.

---

## 3.6 AiCloud 2.0 verwenden

AiCloud2.0 ist eine Cloud-Anwendung, mit der Sie Ihre Dateien speichern, synchronisieren teilen und abrufen können.



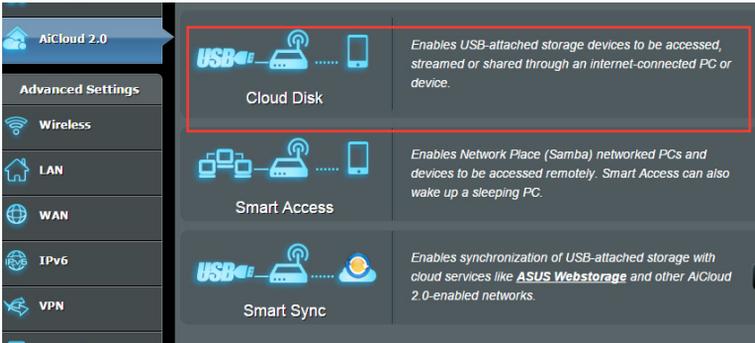
### So nutzen Sie AiCloud:

1. Laden Sie die ASUS AiCloud-App vom Google Play Store oder Apple Store auf Ihr kompatibles Gerät herunter, installieren Sie die Anwendung.
2. Verbinden Sie ihr kompatibles Gerät mit dem Netzwerk. Schließen Sie die AiCloud-Einrichtung gemäß den Hinweisen auf dem Bildschirm ab.

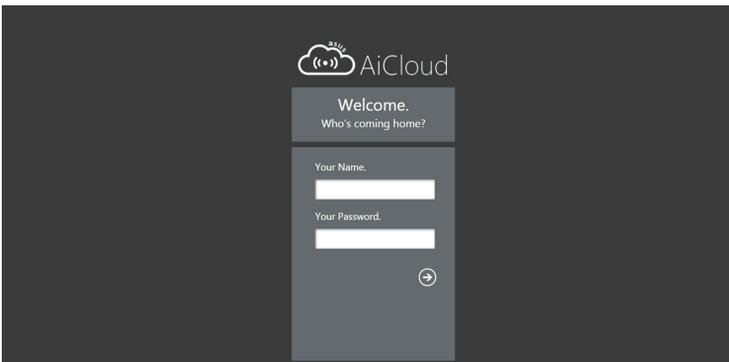
## 3.6.1 Cloud-Laufwerk

### So erstellen Sie ein Cloud-Laufwerk:

1. Schließen Sie ein USB-Speichergerät an den WLAN-Router an.
2. Schalten Sie **Cloud Disk (Cloud-Laufwerk)** ein.

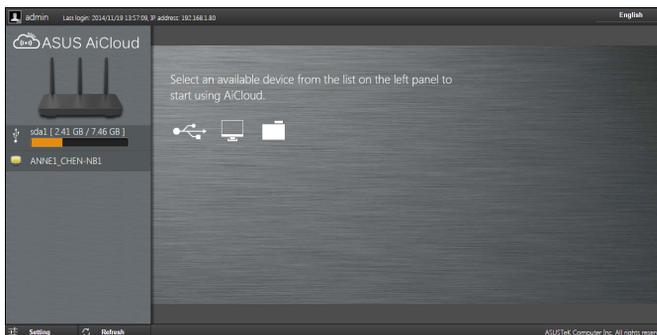


3. Rufen Sie die Internetseite <https://router.asus.com> auf, geben Sie Router-Anmeldekonto und Kennwort ein. Damit alles reibungslos funktioniert, empfehlen wir die Internetbrowser **Google Chrome** oder **Firefox**.



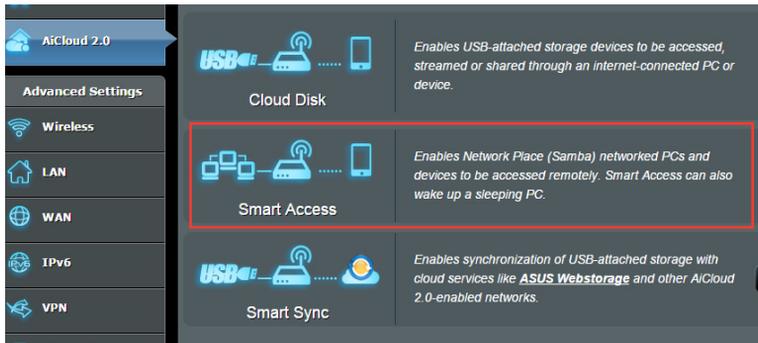
#### 4. Nun können Sie mit Geräten im Netzwerk auf die Dateien des Cloud-Laufwerks zugreifen.

**HINWEIS:** Wenn Sie auf Netzwerkgeräte zugreifen möchten, müssen Sie den Gerätenamen und das Kennwort manuell eingeben, da diese Daten aus Sicherheitsgründen nicht von AiCloud gespeichert werden.



## 3.6.2 Intelligenter Zugriff

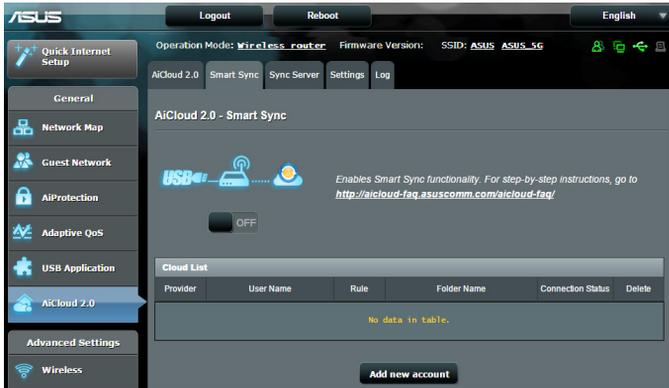
Die Intelligenter-Zugriff-Funktion ermöglicht Ihnen, über den Domännennamen Ihres Routers problemlos auf Ihr Heimnetzwerk zuzugreifen.



### HINWEISE:

- Einen Domännennamen Ihres Routers können Sie mit ASUS DDNS erstellen. Weitere Informationen dazu finden Sie im Abschnitt **4.3.5 DDNS**.
- Per Vorgabe arbeitet AiCloud mit einer sicheren HTTPS-Verbindung. Geben Sie zur besonders sicheren Nutzung mit Cloud-Laufwerk und intelligentem Zugriff [https://\[Ihr-ASUS-DDNS-Name\].asuscomm.com](https://[Ihr-ASUS-DDNS-Name].asuscomm.com) ein.

## 3.6.3 Intelligente Synchronisierung



### So nutzen Sie die intelligente Synchronisierung:

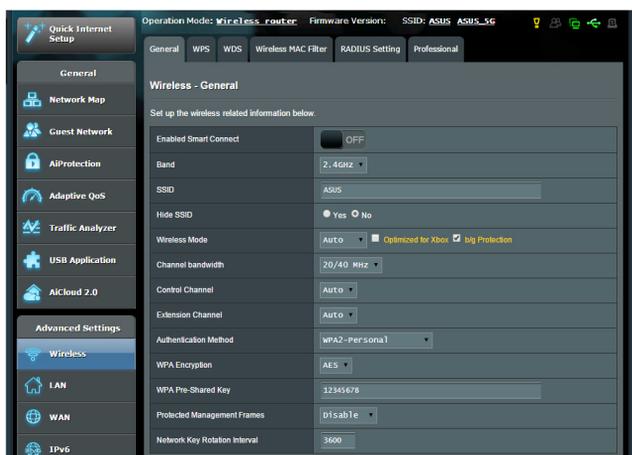
1. Starten Sie AiCloud, klicken Sie auf **Smart Sync (Intelligente Synchronisierung)**> **Go (Los)**.
2. Wählen Sie **ON (Ein)** zum Aktivieren der intelligenten Synchronisierung.
3. Klicken Sie auf **Add new account (Neues Konto hinzufügen)**.
4. Geben Sie das Kennwort Ihres ASUS WebStorage-Kontos ein, wählen Sie den Ordner, den Sie mit WebStorage synchronisieren möchten.
5. Klicken Sie auf **Apply (Übernehmen)**.

# 4 Konfigurieren der erweiterten Einstellungen

## 4.1 WLAN

### 4.1.1 General (Allgemein)

Im Allgemein-Register können Sie WLAN-Grundeinstellungen konfigurieren.



### So konfigurieren Sie die WLAN-Grundeinstellungen:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > General (Allgemein)**.
2. Wählen Sie 2,4 GHz oder 5 GHz als Frequenzband Ihres WLAN-Netzwerks.
3. Wenn Sie die Funktion Smart Connect (Intelligente Verbindung) nutzen möchten, bewegen Sie den Regler im Feld **Enable Smart Connect (Intelligente Verbindung aktivieren)** auf **ON (Ein)**. Diese Funktion verbindet die Clients in Ihrem Netzwerk für optimale Geschwindigkeit automatisch mit dem geeigneten Band 2,4 GHz, 5 GHz-1 oder 5 GHz-2.

4. Weisen Sie einen eindeutigen Namen zu, der aus bis zu 32 Zeichen bestehen darf. Dieser Name ist die SSID oder der Netzwerkname Ihres WLAN-Netzwerks. WLAN-Geräte können das WLAN-Netzwerk über die von Ihnen zugewiesene SSID identifizieren und sich damit verbinden. Die SSIDs im Infobanner werden aktualisiert, sobald eine neue SSID gespeichert wird.

---

**HINWEIS:** Sie können den 2,4-GHz- und 5-GHz-Frequenzbändern unterschiedliche SSIDs zuweisen.

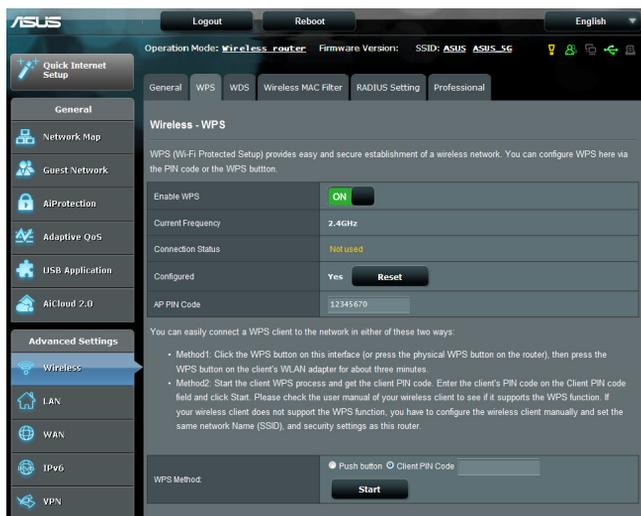
---

5. Wählen Sie im **Hide SSID (SSID verbergen)**-Feld **Yes (Ja)** aus, wenn WLAN-Geräte Ihre SSID nicht ermitteln sollen. Wenn diese Funktion aktiv ist, müssen Sie die SSID manuell an WLAN-Geräten eingeben, wenn Sie auf das WLAN-Netzwerk zugreifen möchten.
6. Wählen Sie unter den folgenden WLAN-Optionen aus, mit denen Sie festlegen können, welche WLAN-Gerätetypen auf Ihren WLAN-Router zugreifen können:
  - **Auto:** Wählen Sie **Auto**, wenn sich 802.11AC-, 802.11n-, 802.11g- und 802.11b-Geräte mit dem WLAN-Router verbinden sollen.
  - **Altgeräte:** Wählen Sie **Legacy (Altgeräte)**, wenn 802.11b/g/n-Geräte auf den WLAN-Router zugreifen dürfen. Allerdings ermöglicht Hardware, die 802.11n physikalisch unterstützt, lediglich eine maximale Übertragungsgeschwindigkeit von 54 Mb/s.
  - **Nur N: N only (Nur N)** wählen Sie, wenn Sie maximale N-Leistung wünschen. Diese Einstellung verhindert, dass 802.11g- und 802.11b-Geräte auf den WLAN-Router zugreifen können.
7. Wählen Sie den Betriebskanal Ihres WLAN-Routers. Wählen Sie **Auto**, wenn der WLAN-Router automatisch einen besonders störungsfreien Kanal auswählen soll.
8. Wählen Sie die Kanalbandbreite für höhere Übertragungsgeschwindigkeiten.
9. Wählen Sie das Authentifizierungsverfahren.
10. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.

## 4.1.2 WPS

WPS (Wi-Fi Protected Setup) ist ein WLAN-Sicherheitsstandard, der einfache Geräteverbindungen zu einem WLAN-Netzwerk ermöglicht. Sie können die WPS-Funktion über den PIN-Code oder die WPS-Taste konfigurieren.

**HINWEIS:** Überzeugen Sie sich davon, dass die Geräte WPS unterstützen.



### So aktivieren Sie WPS in Ihrem WLAN-Netzwerk:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > WPS (WPS)**.
2. Stellen Sie den Schieber im **Enable WPS (WPS aktivieren)**-Feld auf **ON (Ein)** ein.
3. WPS nutzt per Vorgabe das 2,4-GHz-Frequenzband. Wenn Sie das 5GHz-1 oder 5GHz-2-GHz-Frequenzband nutzen möchten, schalten Sie die WPS-Funktion **OFF (Aus)**, klicken anschließend im Feld **Switch Frequency ((Frequenz umschalten)** auf **Current Frequency (Aktuelle Frequenz)**, anschließend schalten Sie WPS wieder **ON (Ein)**.

---

**Hinweis:** WPS unterstützt Authentisierung per Open System, WPA-Personal und WPA2-Personal. WPS unterstützt keine WLAN-Netzwerke, die mit den Verschlüsselungsverfahren Shared Key, WPA-Enterprise, WPA2-Enterprise oder RADIUS arbeiten.

---

3. Im WPS Method (WPS-Methode)-Feld wählen Sie **Push Button (Taste)** oder **Client PIN code (Client-PIN-Code)**. Wenn Sie sich für **Push Button (Taste)** entscheiden, fahren Sie mit Schritt 4 fort. Wenn Sie **Client PIN code (Client-PIN-Code)** wählen, machen Sie bei Schritt 5 weiter.
4. Zur WPS-Einrichtung über die WPS-Taste des Routers führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf **Start** oder drücken Sie die WPS-Taste an der Rückwand des WLAN-Routers.
  - b. Drücken Sie die WPS-Taste Ihres WLAN-Gerätes. Diese Taste erkennen Sie normalerweise am WPS-Logo.

---

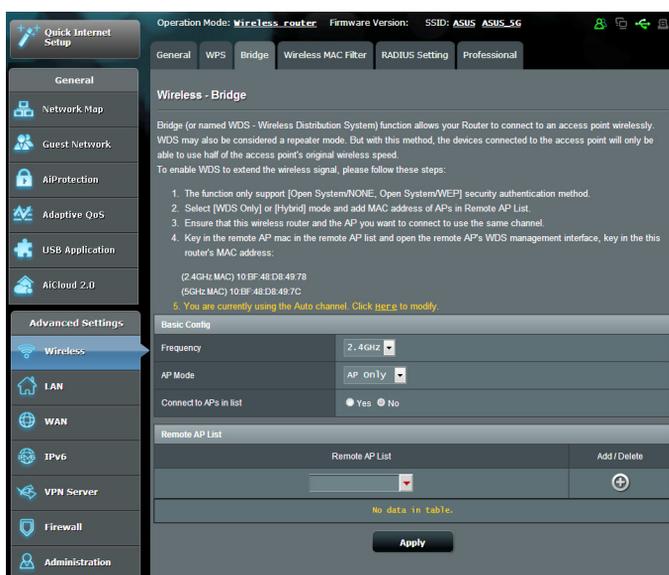
**Hinweis:** Schauen Sie zur Not in der Bedienungsanleitung Ihres WLAN-Gerätes nach, wo sich die WPS-Taste befindet.

---

- c. Der WLAN-Router sucht nach erreichbaren WPS-Geräten. Falls der WLAN-Router keine WPS-Geräte finden kann, schaltet er in den Bereitschaftsmodus um.
5. Zur WPS-Einrichtung über den Client-PIN-Code führen Sie diese Schritte aus:
  - a. Suchen Sie den WPS-PIN-Code in der Bedienungsanleitung oder am WLAN-Gerät selbst.
  - b. Geben Sie den Client-PIN-Code in das Textfeld ein.
  - c. Klicken Sie auf **Start**; damit versetzen Sie Ihren WLAN-Router in den WPS-Suchmodus. Bis zum Abschluss der WPS-Einrichtung blinken die Router-LEDs schnell dreimal hintereinander.

### 4.1.3 Brücke

Eine Brücke oder WDS (Wireless Distribution System) ermöglicht Ihrem ASUS-WLAN-Router exklusive Verbindungen zu anderen WLAN-APs; dabei verhindert das System, dass andere WLAN-Geräte oder -Stationen auf Ihren ASUS-WLAN-Router zugreifen können. Diese Funktion lässt sich auch mit einem WLAN-Repeater (Reichweitenverstärker) vergleichen, wobei Ihr ASUS-WLAN-Router als Vermittlungsstelle zwischen einem anderen AP und anderen WLAN-Geräten auftritt.



So richten Sie die WLAN-Brücke ein:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > Bridge (Brücke)**.
2. Wählen Sie das Frequenzband der WLAN-Brücke.

3. Wählen Sie im Feld **AP Mode (AP-Modus)** aus den folgenden Optionen:
  - **Nur AP:** Deaktiviert die WLAN-Brückenfunktion.
  - **Nur WDS:** Aktiviert die WLAN-Brücke, verhindert jedoch, dass sich andere WLAN-Geräte/-Stationen mit dem Router verbinden können.
  - **HYBRID:** Aktiviert die WLAN-Brücke und ermöglicht, dass sich andere WLAN-Geräte/-Stationen mit dem Router verbinden können.

---

**HINWEIS:** Im Hybridmodus erhalten mit dem ASUS-WLAN-Router verbundene WLAN-Geräte lediglich die halbe Übertragungsgeschwindigkeit des APs.

---

4. Klicken Sie im Feld **Connect to APs in list (mit APs in der Liste verbinden)** auf **Yes (Ja)**, wenn Sie sich mit einem in der Externe-AP-Liste aufgeführten Zugangspunkt (AP) verbinden möchten.
5. Standardmäßig ist der Betriebs-/Steuerungskanal für die WLAN-Bridge auf **Auto** eingestellt, damit der Router automatisch den Kanal mit den geringsten Störungen wählen kann.

Sie können den **Control Channel (Steuerungskanal)** unter **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > General (Allgemein)**-Register ändern.

---

**HINWEIS:** Die nutzbaren Kanäle variieren nach Land oder Region.

---

6. Geben Sie in der Externe-AP-Liste eine MAC-Adresse ein, klicken Sie dann zur Eingabe der MAC-Adresse weiterer verfügbarer APs auf die **Add (Hinzufügen)**-Schaltfläche .

---

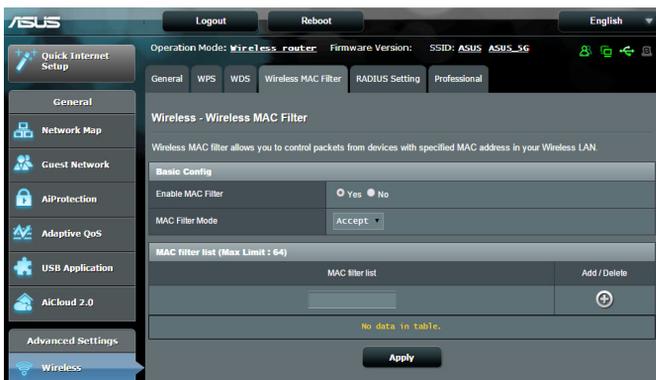
**HINWEIS:** Sämtliche zur Liste zugefügten APs sollten denselben Steuerkanal wie Ihr ASUS-WLAN-Router nutzen.

---

7. Klicken Sie auf **Apply (Übernehmen)**.

## 4.1.4 WLAN-MAC-Filter

Der WLAN-MAC-Filter ermöglicht die Kontrolle über Pakete, die an eine bestimmte MAC-Adresse in Ihrem WLAN-Netzwerk gesendet werden.



### So richten Sie den WLAN-MAC-Filter ein:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > Wireless MAC Filter (WLAN-MAC-Filter)**.
2. Wählen Sie im Feld **Frequency (Frequenz)** das Frequenzband aus, das Sie für die WLAN-MAC-Filterfunktion nutzen möchten.
3. Wählen Sie aus der **MAC Filter Mode (Mac-Filtermodus)**-Auswahlliste entweder **Accept (Annehmen)** oder **Reject (Abweisen)**.
  - Wählen Sie **Accept (Annehmen)**, um Geräten in der MAC-Filterliste Zugriff auf das WLAN-Netzwerk zu gewähren.
  - Wählen Sie **Reject (Abweisen)**, um Geräten in der MAC-Filterliste den Zugriff auf das WLAN-Netzwerk zu verweigern.
4. Klicken Sie in der MAC-Filterliste auf die **Add (Hinzufügen)**-Schaltfläche , geben Sie dann die MAC-Adresse des WLAN-Gerätes ein.
5. Klicken Sie auf **Apply (Übernehmen)**.

## 4.1.5 RADIUS-Einstellungen

Die RADIUS-Einstellungen (Remote Authentication Dial In User Service) bieten eine zusätzliche Sicherheitsschicht, wenn Sie WPA-Enterprise, WPA2-Enterprise oder Radius mit 802.1x als Authentisierungsverfahren wählen.



### So richten Sie die WLAN-RADIUS-Einstellungen ein:

1. Vergewissern Sie sich, dass das Authentisierungsverfahren des WLAN-Routers auf WPA-Enterprise, WPA2-Enterprise oder Radius mit 802.1x eingestellt ist.

---

**HINWEIS:** Bitte lesen Sie zur Konfiguration des Authentisierungsverfahrens Ihres WLAN-Routers im Abschnitt **4.1.1 Allgemein** nach.

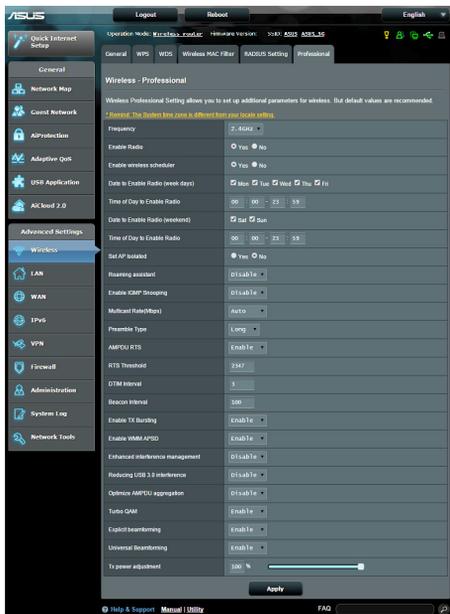
---

2. Wechseln Sie vom Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > RADIUS Setting (RADIUS-Einstellungen)**.
3. Wählen Sie das Frequenzband.
4. Tragen Sie unter **Server IP Address (Server-IP-Adresse)** die IP-Adresse Ihres RADIUS-Servers ein.
5. Geben Sie im Feld **Server Port (Serverport)** den Serverport ein.
6. Legen Sie im Feld **Connection Secret (Verbindungskennwort)** das Kennwort zum Zugriff auf Ihren RADIUS-Server fest.
7. Klicken Sie auf **Apply (Übernehmen)**.

## 4.1.6 Professionell

Im Professionell-Bildschirm finden Sie erweiterte Konfigurationsoptionen.

**HINWEIS:** Wir empfehlen, die Standardeinstellungen auf dieser Seite möglichst nicht zu verändern.



Im Bildschirm **Professional Settings (Professionelle Einstellungen)** können Sie Folgendes konfigurieren:

- **Frequenz:** Hier wählen Sie das Frequenzband, auf das die professionellen Einstellungen angewendet werden sollen.
- **Sender aktivieren:** Wählen Sie **Yes (Ja)** zum Aktivieren des WLAN-Netzwerks. Wählen Sie **No (Nein)**, wenn Sie das WLAN-Netzwerk deaktivieren möchten.
- **Senderaktivität-Tage (wochentags):** Hier können Sie festlegen, an welchen Wochentagen das WLAN-Netzwerk aktiv sein soll.
- **Senderaktivität-Uhrzeiten:** Hier geben Sie einen Zeitraum zur Senderaktivität an.

- **Senderaktivität-Tage (Wochenende):** Hier können Sie festlegen, an welchen Tagen des Wochenendes das WLAN-Netzwerk aktiv sein soll.
- **Senderaktivität-Uhrzeiten:** Hier geben Sie einen Zeitraum zur Senderaktivität am Wochenende an.
- **AP isolieren:** Die AP-isolieren-Einstellung verhindert die Kommunikation von WLAN-Geräten im Netzwerk untereinander. Diese Funktion ist zum Beispiel dann nützlich, wenn viele Gäste Ihr Netzwerk besuchen oder verlassen. Wählen Sie **Yes (Ja)** zum Aktivieren dieser Funktion, **No (Nein)** zum Abschalten.
- **Roaming Assistant (Roaming-Assistent):** In Netzwerkkonfigurationen, die mehrere Zugangspunkte oder WLAN-Repeater beinhalten, können sich WLAN-Clients manchmal nicht mit verfügbaren Zugangspunkten verbinden, da sie immer noch mit dem Haupt-WLAN-Router verbunden sind. Aktivieren Sie diese Einstellung, damit der Client die Verbindung zum Haupt-WLAN-Router trennt, wenn die Signalstärke unter einen spezifischen Schwellwert fällt; stellen Sie dann eine Verbindung zu einem stärkeren Signal her.
- **Enable IGMP Snooping (IGMP-Snooping aktivieren):** Durch Aktivierung dieser Funktion können das IGMP (Internet Group Management Protocol) zwischen Geräten überwacht und der WLAN-Multicast-Datenverkehr optimiert werden.
- **Multicast-Rate (Mb/s):** Hier wählen Sie die Multicast-Übertragungsratenrate oder schalten die gleichzeitige Einzelübertragung mit **Disable (Deaktivieren)** ab.
- **Präambeltyp:** Der Präambeltyp definiert die Zeitspanne, die der Router für CRC-Prüfungen (zyklische Redundanzprüfungen) aufwendet. CRC ist ein Verfahren zur Fehlererkennung bei Datenübertragungen. Die Einstellung **Short (Kurz)** eignet sich für stark frequentierten Netzwerke mit hohem Datenaufkommen. Wählen Sie **Long (Lang)**, wenn sich Ihr WLAN-Netzwerk vornehmlich aus älteren WLAN-Geräten zusammensetzt.
- **AMPDU RTS (A-MPDU-RTS):** Durch Aktivieren dieser Funktion kann vor dem Übertragen eine Gruppe von Frames aufgebaut und für jede A-MPDU für die Kommunikation zwischen 802.11g- und 802.11b-Geräten RTS genutzt werden.
- **RTS Threshold (RTS-Schwellenwert):** Wählen Sie einen niedrigeren RTS-Schwellenwert (RTS steht für „Request to Send“, also Sendeanfrage), wenn Sie die WLAN-Kommunikation in stark frequentierten Netzwerken mit hohem Datenaufkommen und zahlreichen WLAN-Geräten verbessern möchten.

- **DTIM-Intervall:** Das DTIM-Intervall („Delivery Traffic Indication Message“ oder Meldung über anliegenden Datenverkehr) oder die „Data Beacon Rate“, also Datenbakenrate, definieren die Zeit, die vergeht, bevor ein WLAN-Gerät im Schlafmodus über ein zur Abholung bereitstehendes Datenpaket informiert wird. Der Standardwert liegt bei 3 ms.
- **Bakenintervall:** Das Bakenintervall definiert die Zeitspanne zwischen den einzelnen DTIMs. Der Standardwert liegt bei 100 ms. Vermindern Sie das Bakenintervall bei instabilen WLAN-Verbindungen oder beim Einsatz von Roaming-Geräten.
- **Sendebündelung aktivieren:** Diese Einstellung erhöht die Übertragungsgeschwindigkeit zwischen WLAN-Router und 802.11g-Geräten.
- **WMM APSD aktivieren:** Die aktive WMM APSD-Einstellung (Wi-Fi Multimedia Automatic Power Save Delivery, Automatisches WLAN-Energiesparen bei Multimediadaten) verbessert die Energieverwaltung beim Zusammenspiel von WLAN-Geräten. Zum Abschalten der WMM APSD-Funktion wählen Sie **Disable (Deaktivieren)**.
- **Reducing USB 3.0 interference (USB 3.0-Störungen reduzieren):** Die Aktivierung dieser Funktion gewährleistet beste WLAN-Leistung im 2,4-GHz-Band. Durch Deaktivieren dieser Funktion erhöht sich die Übertragungsgeschwindigkeit des USB 3.0-Ports, die 2,4-GHz-WLAN-Reichweite kann beeinträchtigt werden.
- **Optimize AMPDU aggregation (A-MPDU-Aggregation optimieren):** Optimieren Sie die maximale Anzahl MPDUs in einer A-MPDU und verhindern Sie, dass Pakete während der Übertragung in fehleranfälligen WLAN-Kanälen verlorengehen oder beschädigt werden.
- **Optimize ack suppression (ACK-Unterdrückung optimieren):** Optimieren Sie die maximale Anzahl ACK zur Unterdrückung in einer Zeile.
- **Turbo QAM (Turbo-QAM):** Durch Aktivierung dieser Funktion wird zur Erzielung einer besseren Reichweite und eines höheren Durchsatzes in diesem Frequenzbereich 256-QAM (MCS 8/9) im 2,4-GHz-Band unterstützt.
- **Airtime Fairness:** Mit Airtime Fairness wird die Netzwerkgeschwindigkeit nicht über den langsamsten Datenverkehr ermittelt. Durch gleichmäßige Zuteilung von Zeit zwischen den Clients ermöglicht Airtime Fairness jeder Übertragung ihre höchstmögliche Geschwindigkeit.
- **Explicit Beamforming (Explizites Beamforming):** Der WLAN-Adapter des Clients und der Router unterstützen beide Beamforming-Technologie. Diese Technologie ermöglicht diesen Geräten die gegenseitige Kommunikation der Kanalschätzung und Steuerungsrichtung zur Verbesserung der Downlink- und Uplink-Geschwindigkeit.

- **Universal Beamforming (Universal-Beamforming):** Bei alten WLAN-Netzwerkadaptern, die Beamforming nicht unterstützen, schätzt der Router den Kanal und ermittelt die Steuerungsrichtung zur Verbesserung der Downlink-Geschwindigkeit.
- **Sendeleistung anpassen:** Sie können die Sendeleistung des WLAN-Routers in gewissen Grenzen anpassen; die Angabe erfolgt in Milliwatt (mW). Geben Sie einen Wert zwischen 0 und 100 ein.

---

**HINWEIS:** Eine Erhöhung der Sendeleistung kann sich negativ auf die Stabilität des WLAN-Netzwerks auswirken.

---

## 4.2 LAN

### 4.2.1 LAN-IP

Im LAN-IP-Bildschirm können Sie die LAN-IP-Einstellungen Ihres WLAN-Routers verändern.

---

**HINWEIS:** Sämtliche Änderungen der LAN-IP-Adresse spiegeln sich in Ihren DHCP-Einstellungen wieder.

---

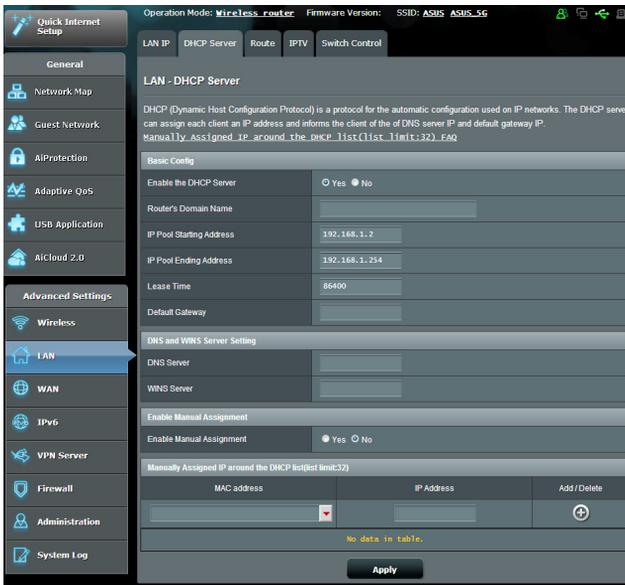


**So ändern Sie die LAN-IP-Einstellungen:**

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > LAN > LAN IP (LAN-IP)**.
2. Ändern Sie **IP address (IP-Adresse)** und **Subnet Mask (Subnetzmaske)**.
3. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.

## 4.2.2 DHCP-Server

Ihr WLAN-Router nutzt DHCP zur automatischen Zuweisung von IP-Adressen im Netzwerk. Sie können den IP-Adressbereich festlegen und bestimmen, wie lange Clients im Netzwerk eine IP-Adresse zugewiesen bleibt.



### So richten Sie einen DHCP-Server ein:

1. Vom Navigationspanel gehen Sie zu **Advanced Settings>LAN>DHCP Server**.
2. Klicken Sie im Feld **Enable the DHCP Server? (DHCP-Server aktivieren?)** auf die Auswahl **Yes (Ja)**.

3. Geben Sie in das **Domain Name (Domänenname)**-Textfeld einen Domännennamen für Ihren WLAN-Router ein.
4. Geben Sie im Feld **IP Pool Starting Address (IP-Pool Startadresse)** die IP-Startadresse ein.
5. Geben Sie im Feld **IP Pool Ending Address (IP-Pool Endadresse)** die IP-Endadresse ein.
6. Geben Sie im Feld **Lease Time (Lease-Zeitraum)** die Ablaufzeit für die IP-Adressen ein, damit der drahtlose Router Ihren Clients im Netzwerk automatisch neue IP-Adressen zuweisen kann.

---

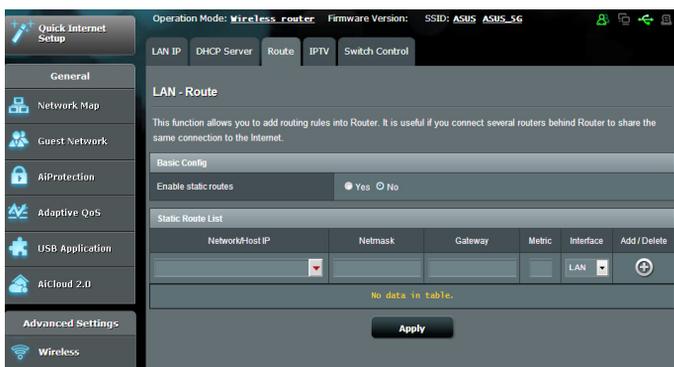
#### **HINWEISE:**

- Wir empfehlen, beim Festlegen eines IP-Adressbereiches eine IP-Adresse im Format 192.168.1.xxx (xxx steht für eine beliebige Zahl zwischen 2 und 254) zu verwenden.
  - Die Startadresse eines IP-Kontingents darf nicht größer als die Endadresse des Kontingents sein.
- 
7. Geben Sie im Bereich **DNS and Server Settings (DNS- und Servereinstellungen)** bei Bedarf die IP-Adressen Ihres DNS- und WINS-Servers ein.
  8. Ihr WLAN-Router kann Geräten im Netzwerk auch manuell IP-Adressen zuweisen. Wenn Sie bestimmten MAC-Adressen im Netzwerk eine IP-Adresse zuweisen möchten, wählen Sie im Feld **Enable Manual Assignment (Manuelle Zuweisung aktivieren)** die Option **Yes (Ja)**. Der DHCP-Liste können bis zu 32 MAC-Adressen manuell zugefügt werden.

## 4.2.3 Route

Falls Sie mehr als einen WLAN-Router in Ihrem Netzwerk einsetzen, können Sie eine Routentabelle konfigurieren und so dieselbe Internetverbindung nutzen.

**HINWEIS:** Wir empfehlen, die Standard-Routeneinstellungen nicht zu verändern, sofern Sie nicht über umfassendes Wissen über Routentabellen verfügen.

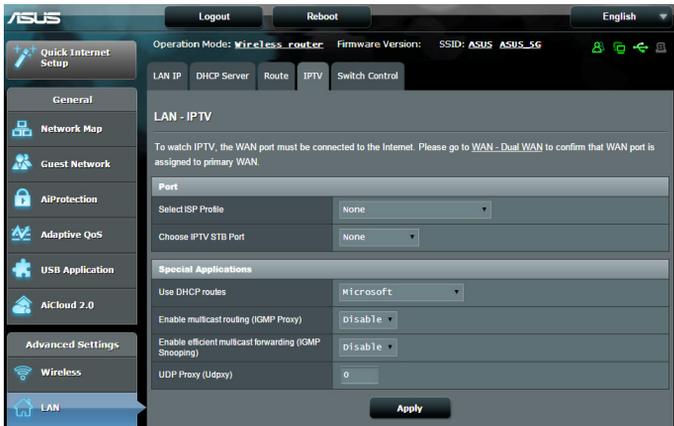


### So konfigurieren Sie die LAN-Routentabelle:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > LAN > Route (Route)**.
2. Im Feld **Enable static routes (Statische Routen aktivieren)** wählen Sie **Yes (Ja)** aus.
3. Geben Sie Netzwerkinformationen zu weiteren APs oder Knoten in die **Static Route List (Statische Routenliste)** ein. Klicken Sie zum Hinzufügen zum Entfernen eines Gerätes zur/ aus der Liste auf die Schaltflächen **Add (Hinzufügen)**  oder **Delete (Löschen)** .
4. Klicken Sie auf **Apply (Übernehmen)**.

## 4.2.4 IPTV

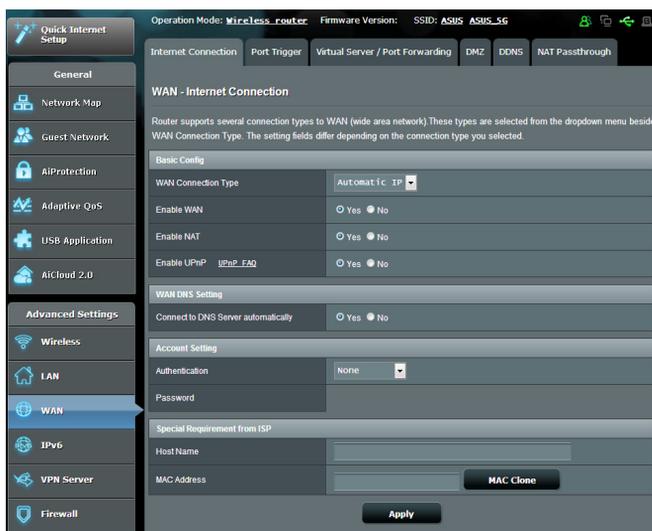
Der WLAN-Router kann sich per Internet oder LAN mit IPTV-Diensten verbinden. Im IPTV-Register finden Sie Konfigurationseinstellungen, die Sie zum Einrichten von IPTV, VoIP, Multicasting und UDP benötigen. Weitere Details erhalten Sie von Ihrem Internetanbieter.



## 4.3 WAN

### 4.3.1 Internetverbindung

Der Internetverbindung-Bildschirm ermöglicht Ihnen die Konfiguration von Einstellungen unterschiedlicher WAN-Verbindungstypen.



**So konfigurieren Sie die WAN-Verbindungseinstellungen:**

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > WAN > Internet Connection (Internetverbindung)**.
2. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.
  - **WAN-Verbindungstyp:** Wählen Sie den Typ Ihrer Internetverbindung. Zur Auswahl stehen **Automatic IP (Automatische IP)**, **PPPoE**, **PPTP**, **L2TP** und **fixed IP (Feste IP)**. Wenden Sie sich an Ihrem Internetanbieter, falls der Router keine gültige IP-Adresse beziehen kann oder Sie nicht sicher sind, welcher WAN-Verbindungstyp eingesetzt wird.
  - **WAN aktivieren:** Wählen Sie **Yes (Ja)**, wenn der Router auf das Internet zugreifen soll. Wählen Sie **No (Nein)**, wenn Sie den Internetzugriff unterbinden möchten.

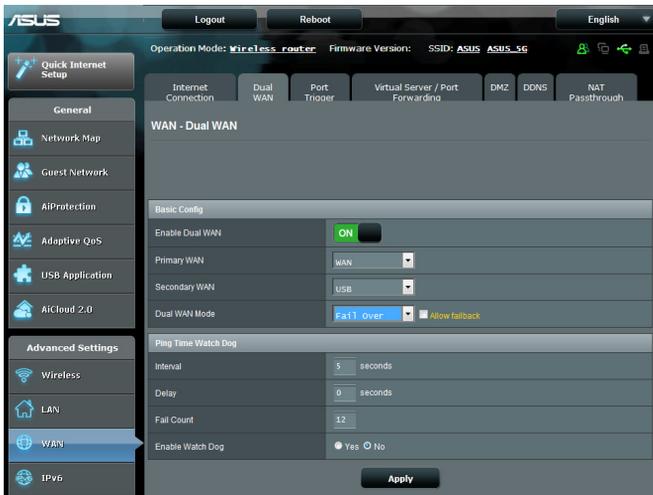
- **NAT aktivieren:** NAT (Network Address Translation, Netzwerkadressenumsetzung) ist ein System, bei dem eine öffentliche IP (WAN-IP) eingesetzt wird, um Netzwerk-Clients mit einer privaten-IP-Adresse im LAN Internetzugriff zu ermöglichen. Die private IP-Adresse der einzelnen Netzwerk-Clients wird in einer NAT-Tabelle gespeichert und zum Umleiten ankommender Datenpakete eingesetzt.
- **UPnP aktivieren:** UPnP (Universal Plug and Play) ermöglicht die Steuerung diverser Geräte (wie Routern, Fernsehgeräten, Stereoanlagen, Spielkonsolen und Mobiltelefonen) über ein IP-basiertes Netzwerk mit oder ohne zentrale Steuerung durch ein Gateway. UPnP verbindet PCs sämtlicher Varianten und ermöglicht ein nahtloses Netzwerk zur Fernkonfiguration und zum Datentransfer. Beim UPnP-Einsatz werden neue Netzwerkgeräte automatisch erkannt. Nachdem Geräte vom Netzwerk erkannt wurden, können diese manuell zur Unterstützung von P2P-Anwendungen, interaktiven Spielen, Videokonferenzen, Web- oder Proxyservern konfiguriert werden. Anders als bei der Portweiterleitung, bei der Porteingstellungen manuell konfiguriert werden müssen, konfiguriert UPnP den Router automatisch so, dass ankommende Verbindungen und Direktanfragen an einen bestimmten PC im lokalen Netzwerk automatisch angenommen werden.
- **Mit DNS-Server verbinden:** Ermöglicht, die DNS-IP-Adresse des Routers automatisch vom Internetanbieter zuweisen zu lassen. Ein DNS ist ein Host im Internet, der Namen von Internetseiten (URLs) in numerische IP-Adressen umsetzt.
- **Autentisierung:** Dieses Element wird eventuell von bestimmten Internetanbietern vorgegeben. Fragen Sie bei Ihrem Internetanbieter nach, füllen Sie dieses Feld bei Bedarf aus.
- **Hostname:** In diesem Feld können Sie einen Hostnamen für Ihren Router festlegen. Dieser ist gewöhnlich eine spezielle Vorgabe Ihres Internetanbieters. Sofern Ihrem Computer ein Hostname vom Internetanbieter zugewiesen wurde, tragen Sie diesen Hostnamen hier ein.

- **MAC-Adresse:** Die MAC-Adresse (Media Access Control, Medienzugriffssteuerung) ist eine eindeutige Kennung Ihres Netzwerkgerätes. Einige Internetanbieter überwachen die MAC-Adressen von Netzwerkgeräten, die Verbindungen zu Ihren Diensten herstellen, und weisen Verbindungsversuche unbekannter Geräte ab. Damit es nicht zu Verbindungsproblemen durch nicht registrierte MAC-Adressen kommt, können Sie Folgendes unternehmen:
  - Nehmen Sie Kontakt zu Ihrem Internetanbieter auf, aktualisieren Sie die mit Ihrem Internetzugang verknüpfte MAC-Adresse.
  - Duplizieren oder ändern Sie die MAC-Adresse des ASUS-WLAN Routers so, dass diese der MAC-Adresse des zuvor beim Internetanbieter registrierten Netzwerkgerätes entspricht.
- **DHCP query frequency (DHCP-Anfragefrequenz):** Ändert die Intervalleinstellungen der DHCP-Erkennung zur Vermeidung einer Überlastung des DHCP-Servers.

## 4.3.2 Dual-WAN

Ihr WLAN-Router von ASUS bietet Dual-WAN-Unterstützung. Sie können die Dual-WAN-Funktion auf einen dieser beiden Modi einstellen:

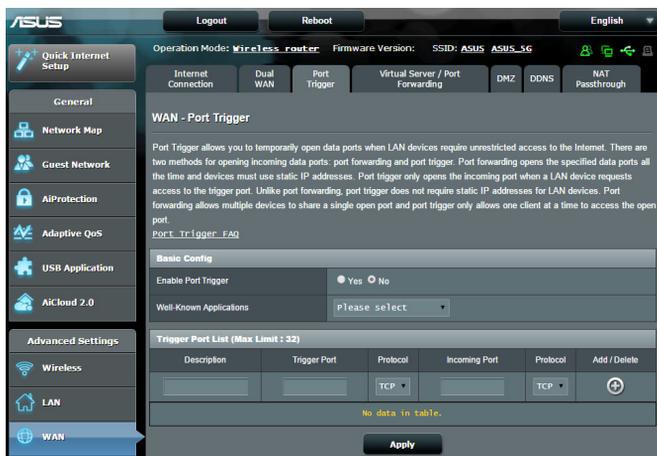
- **Failover Mode (Ausfallschutz-Modus):** Wählen Sie diesen Modus zur Nutzung des zweiten WAN als Reservernetzwerkzugriff.
- **Load Balance Mode (Lastausgleich-Modus):** Wählen Sie diesen Modus zum Optimieren der Bandbreite, zum Minimieren der Reaktionszeit und zur Verhinderung einer Datenüberlastung für primäre und sekundäre WAN-Verbindungen.



### 4.3.3 Portauslösung

Die Portbereichsauslösung öffnet eine begrenzte Zeit lang einen zuvor festgelegten Eingangsport, wenn ein Client im lokalen Netzwerk eine abgehende Verbindung über einen bestimmten Port aufbaut. Die Portauslösung wird in folgenden Szenarien genutzt:

- Mehr als ein lokaler Client benötigt eine Portweiterleitung für dieselbe Anwendung zu einem unterschiedlichen Zeitpunkt.
- Eine Anwendung benötigt spezielle Eingangsport, die nicht mit den Ausgangsports übereinstimmen.



**So richten Sie die Portauslösung ein:**

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > WAN > Port Trigger (Portauslösung)**.
2. Setzen Sie im Feld **Enable Port Trigger (Portauslöser aktivieren)** ein Häkchen bei **Yes (Ja)**.
3. Wählen Sie im Feld **Well-Known Applications (Bekannte Applikationen)** beliebte Spiele und Webdienste zum Hinzufügen zur Port Trigger List (Auslöserportliste).

4. Geben Sie in der Tabelle **Trigger Port List (Auslöserportliste)** die folgenden Informationen ein:
  - **Auslösungspport:** Hier legen Sie einen Auslösungspport zum Öffnen des Eingangspports fest.
  - **Protokoll:** Wählen Sie das Protokoll, TCP oder UDP.
  - **Eingangspport:** Legen Sie einen Eingangspport zum Empfang ankommender Daten aus dem Internet fest.
  - **Protokoll:** Wählen Sie das Protokoll, TCP oder UDP.
5. Klicken Sie zur Eingabe der Portauslöserinformationen in der Liste auf **Add (Hinzufügen)**  Klicken Sie zum Entfernen eines Portauslösereintrags aus der Liste auf **Delete (Löschen)**  .
6. Klicken Sie anschließend auf **Apply (Übernehmen)**.

---

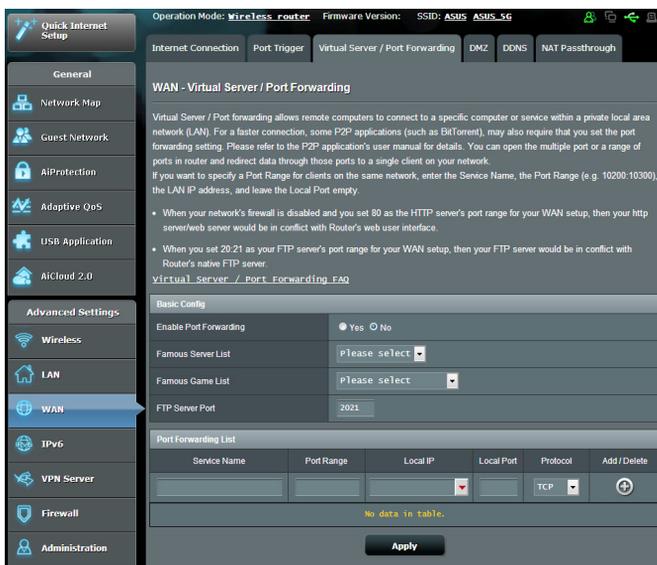
#### HINWEISE:

- Wenn Sie sich mit einem IRC-Server verbinden, stellt der Client-PC eine abgehende Verbindung über den Auslösungspportbereich 66660 – 7000 her. Der IRC-Server reagiert durch Überprüfung des Benutzernamens und erstellt über einen Eingangspport eine neue Verbindung zum Client-PC.
  - Wenn die Portauslösung deaktiviert wurde, trennt der Router die Verbindung, da er nicht feststellen kann, welcher PC den IRC-Zugriff anforderte. Wenn die Portauslösung aktiv ist, weist der Router einen Eingangspport zum Empfang der ankommenden Daten zu. Dieser Eingangspport wird nach einer bestimmten Zeit geschlossen, da der Router nicht feststellen kann, ob die zugehörige Anwendung nach wie vor aktiv ist.
  - Die Portauslösung ermöglicht lediglich einem Client im Netzwerk, einen bestimmten Dienst und einen bestimmten Eingangspport gleichzeitig zu nutzen.
  - Es ist nicht möglich, einen Port mit ein und derselben Anwendung an mehreren PCs gleichzeitig auszulösen. Der Router leitet den Port lediglich zu dem Computer weiter, der zuletzt eine Anfrage/einen Auslöser an den Router sandte.
-

## 4.3.3 Virtueller Server/Portweiterleitung

Die Portweiterleitung ist ein Verfahren zum Umleiten von Netzwerkverkehr aus dem Internet an einen bestimmten Port oder bestimmten Portbereich zu einem oder mehreren Geräten im lokalen Netzwerk. Wählen Sie die Portweiterleitung an Ihrem Router einrichten, können PCs außerhalb des Netzwerks auf bestimmte Dienste zugreifen, die von einem PC in Ihrem eigenen Netzwerk bereitgestellt werden.

**HINWEIS:** Wenn die Portweiterleitung aktiv ist, blockiert der ASUS-Router unaufgefordert eingehenden Datenverkehr aus dem Internet und lässt lediglich Antworten auf abgehende Anfragen aus dem LAN zu. Der Netzwerk-Client kann nicht direkt auf das Internet zugreifen und umgekehrt.



### So richten Sie die Portweiterleitung ein:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > WAN > Virtual Server / Port Forwarding (Virtueller Server/Portweiterleitung)**.
2. Setzen Sie im Feld **Enable Port Forwarding (Portweiterleitung aktivieren)** ein Häkchen bei **Yes (Ja)**.

3. Wählen Sie im Feld **Famous Server List (Liste bekannter Server)** den Servicetyp, auf den Sie zugreifen möchten.
4. Wählen Sie im Feld **Famous Game List (Liste bekannter Spiele)** die bekannten Spiele, auf die Sie zugreifen möchten. Dieses Element listet den erforderlichen Port auf, der zur Ausführung Ihres ausgewählten Online-Spiels erforderlich ist.
5. Geben Sie in der Tabelle **Port Forwarding List (Portweiterleitungsliste)** die folgenden Informationen ein:
  - **Dienstname:** Geben Sie einen Dienstnamen ein.
  - **Portbereich:** Wenn Sie einen Portbereich für Clients im selben Netzwerk festlegen möchten, geben Sie den Dienstnamen, den Portbereich (beispielsweise 100200:10300) und die LAN-IP-Adresse an. Tragen Sie nichts unter Lokaler Port ein. In das Portbereich-Feld können Sie unterschiedliche Formate eingeben; beispielsweise einen Portbereich (wie 300:350), einzelne Ports (wie 566,789), auch gemischte Eingaben (wie 1015:1024,3021) sind möglich.

---

#### **HINWEISE:**

- Wenn die Firewall Ihres Netzwerks deaktiviert ist und Sie 80 als HTTP-Serverportbereich Ihres WAN festlegen, würde Ihr HTTP-Server/ Webserver mit der Web-Benutzeroberfläche des Routers kollidieren.
- Netzwerke nutzen Ports zum Datenaustausch, wobei jedem einzelnen Port eine Portnummer und eine bestimmte Aufgabe zugewiesen werden. Beispielsweise wird Port 80 für HTTP genutzt. Ein bestimmter Port kann lediglich von einer einzigen Anwendung oder einem einzigen Dienst genutzt werden, nicht von mehreren gleichzeitig. Daher ist es nicht möglich, mit zwei PCs gleichzeitig über denselben Port auf Daten zuzugreifen. Beispielsweise können Sie die Portweiterleitung von Port 100 nicht für zwei PCs gleichzeitig festlegen.

---

**Lokale IP:** Hier geben Sie die LAN-IP-Adresse des Clients ein.

---

**HINWEIS:** Verwenden Sie eine statische IP-Adresse für den lokalen Client, damit die Portweiterleitung richtig funktioniert. Weitere Informationen finden Sie im Abschnitt **4.2 LAN**.

---

- **Lokaler Port:** Tragen Sie einen bestimmten Port zum Empfang weitergeleiteter Pakete ein. Lassen Sie dieses Feld leer, wenn die ankommenden Pakete zu einem bestimmten Portbereich umgeleitet werden sollen.
- **Protokoll:** Wählen Sie das Protokoll. Falls Sie unsicher sein sollten, wählen Sie **BOTH (Beide)**.

#### **So prüfen Sie, ob die Portweiterleitung erfolgreich konfiguriert wurde:**

- Vergewissern Sie sich, dass Ihr Server oder Ihre Anwendung richtig eingerichtet und gestartet wurden.
- Sie benötigen einen Client (Internet-Client genannt), der sich außerhalb Ihres LANs befindet, aber auf das Internet zugreifen kann. Dieser Client sollte nicht an den ASUS-Router angeschlossen sein.
- Vom Internet-Client aus nutzen Sie die WAN-IP zum Zugriff auf den Server. Sofern die Portweiterleitung erfolgreich war, sollten Sie auf die Dateien oder Anwendungen zugreifen können.

#### **Unterschiede zwischen Portauslösung und Portweiterleitung:**

- Die Portauslösung funktioniert auch dann, wenn keine spezifische LAN-IP Adresse eingerichtet wurde. Anders als bei der Portweiterleitung, bei der eine statische LAN-IP-Adresse benötigt wird, ermöglicht die Portauslösung dynamische Portweiterleitung über den Router. Vordefinierte Portbereiche werden eine begrenzte Zeit lang zur Annahme ankommender Verbindungen konfiguriert. Die Portauslösung ermöglicht mehreren Computern die Ausführung von Anwendungen, bei denen normalerweise eine manuelle Weiterleitung derselben Ports zu jedem einzelnen PC im Netzwerk erforderlich wäre.
- Die Portauslösung ist sicherer als die Portweiterleitung, da die Eingangsport nicht ständig geöffnet bleiben. Die Ports werden nur dann geöffnet, wenn eine Anwendung eine abgehende Verbindung über den Auslösungsport aufbaut.

### 4.3.4 DMZ

Die virtuelle DMZ (DMZ steht für demilitarisierte Zone) ermöglicht einem Client, sämtliche eingehenden Pakete zu empfangen, die an Ihr lokales Netzwerk gerichtet sind.

Ankommender Datenverkehr aus dem Internet wird gewöhnlich verworfen und nur dann zu einem bestimmten Client geleitet, wenn eine Portweiterleitung oder Portauslösung im Netzwerk konfiguriert wurde. Bei einer DMZ-Konfiguration empfängt ein Netzwerk-Client sämtliche ankommenden Pakete.

Die Einrichtung einer DMZ im Netzwerk ist nützlich, wenn Sie offene Eingangsports benötigen oder einen Domänen-, Web- oder eMail-Server betreiben möchten.

---

**Achtung:** Das Öffnen sämtlicher Ports eines Clients für den Internetdatenverkehr macht das Netzwerk gegenüber Angriffen von außen anfällig. Bitte behalten Sie die Sicherheitsrisiken im Auge, die mit einer DMZ-Konfiguration einhergehen.

---

#### So richten Sie eine DMZ ein:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > WAN > DMZ**.
2. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.
  - **IP-Adresse der exponierten Station:** Tragen Sie die LAN-IP-Adresse des Clients ein, der den DMZ-Dienst nutzen und dem Internetdatenverkehr ausgesetzt werden soll. Achten Sie darauf, dass der Server-Client über eine statische IP-Adresse verfügt.

#### So entfernen Sie eine DMZ:

1. Löschen Sie die LAN-IP-Adresse des Clients aus dem Textfeld **IP Address of Exposed Station (IP-Adresse der exponierten Station)**.
2. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.

## 4.3.5 DDNS

Durch die Einrichtung eines DDNS (dynamischer DNS) können Sie von außerhalb auf den Router im Netzwerk zugreifen; dies geschieht beispielsweise über den ASUS-DDNS-Dienst oder einen anderen DDNS-Anbieter.



### So richten Sie DDNS ein:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > WAN > DDNS**.
2. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.
  - **DDNS-Client aktivieren:** Aktivieren Sie DDNS, wenn Sie statt über die WAN-IP-Adresse über den DNS-Namen auf den ASUS-Router zugreifen möchten.
  - **Server und Hostname:** Wählen Sie ASUS-DDNS oder Anderer DDNS. Wenn Sie den ASUS-DDNS verwenden möchten, tragen Sie den Hostnamen im Format xxx.asuscomm.com ein; das xxx ersetzen Sie durch Ihren Hostnamen.
  - Falls Sie einen anderen DDNS-Dienst nutzen möchten, klicken Sie auf „Kostenlos ausprobieren“ und registrieren sich zunächst online. Tragen Sie Benutzernamen/eMail-Adresse und Kennwort oder den DDNS-Schlüssel in die gleichnamigen Felder ein.

- **Platzhalter aktivieren:** Hier können Sie Platzhalter aktivieren, wenn diese von Ihrem DDNS-Dienst benötigt werden.

---

## HINWEISE:

Unter folgenden Bedingungen funktioniert der DDNS-Dienst nicht:

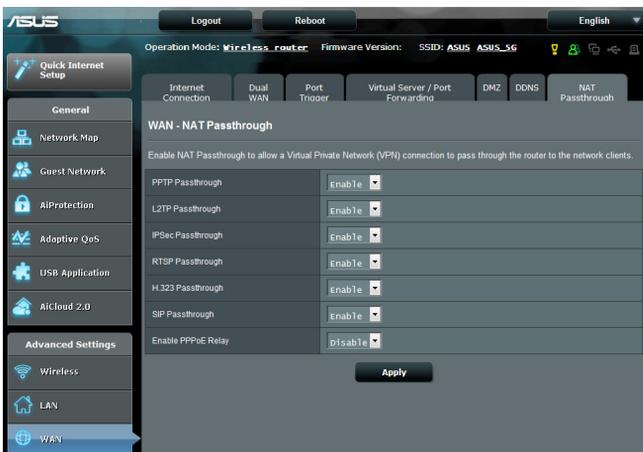
- Der WLAN-Router nutzt eine private WAN-IP-Adresse (192.168.x.x, 10.x.x.x oder 172.16.x.x); dies wird durch gelben Text signalisiert.
- Der Router befindet sich in einem Netzwerk, das mit mehreren NAT-Tabellen arbeitet.

---

## 4.3.6 NAT-Durchleitung

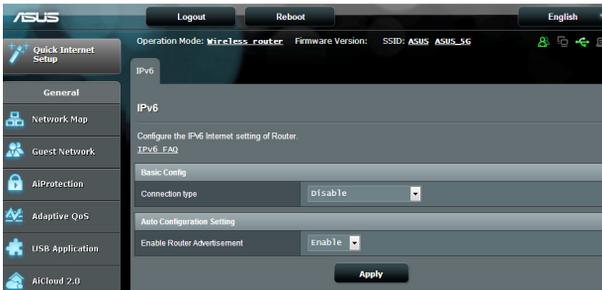
Die NAT-Durchleitung ermöglicht, dass VPN-Verbindungen (VPN steht für virtuelles privates Netzwerk) durch den Router zu den Netzwerk-Clients geleitet werden. PPTP-Durchleitung, L2TP-Durchleitung, IPsec-Durchleitung und RTSP-Durchleitung sind per Vorgabe aktiviert.

Zum Aktivieren/Deaktivieren der NAT-Durchleitungseinstellungen wechseln Sie zum Register **Advanced Settings (Erweiterte Einstellungen) > WAN > NAT Passthrough (NAT-Durchleitung)**. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.



## 4.4 IPv6

Der WLAN-Router unterstützt IPv6-Adressierung; ein System, das mehr IP-Adresse als zuvor ermöglicht. Dieser Standard wird noch nicht flächendeckend eingesetzt. Fragen Sie bei Ihrem Internetanbieter nach, ob Ihr Internetzugang IPv6 unterstützt.



### So richten Sie IPv6 ein:

1. Wechseln Sie vom Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen)**.
2. Wählen Sie Ihren **Connection Type (Verbindungstyp)**. Die Konfigurationsoptionen variieren je nach ausgewähltem Verbindungstyp.
3. Legen Sie Ihre IPv6-LAN- und DNS-Einstellungen fest.
4. Klicken Sie auf **Apply (Übernehmen)**.

---

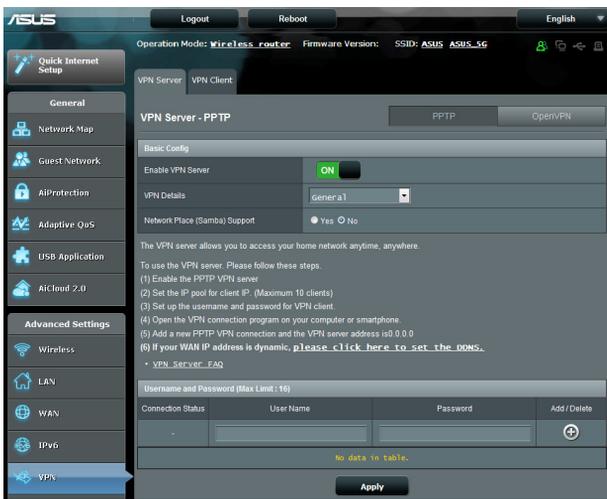
**HINWEIS:** Bitte informieren Sie sich bei Ihrem Internetanbieter über spezielle IPv6-Möglichkeiten Ihres Internetzugangs.

---

## 4.5 VPN-Server

Ein VPN (virtuelles privates Netzwerk) ermöglicht sichere Kommunikation mit externen Computern oder Netzwerken über öffentliche Netzwerke wie dem Internet.

**HINWEIS:** Bevor Sie eine VPN-Verbindung einrichten, benötigen Sie die IP-Adresse oder den Domännennamen des VPN-Servers, auf den Sie zugreifen möchten.



**So richten Sie den Zugriff auf einen VPN-Server ein:**

1. Wechseln Sie vom Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > VPN Server (VPN-Server)**.
2. Wählen Sie im Feld **Enable VPN Server (VPN-Server aktivieren)** die Option **Yes (Ja)**.
3. Wählen Sie aus der **VPN Details (VPN-Details)**-Auswahlliste die Option **Advanced Settings (Erweiterte Einstellungen)**, falls Sie erweiterte VPN-Einstellungen, wie Broadcast-Unterstützung, Authentifizierung, MPPE-Verschlüsselung und Client-IP-Adressbereich, konfigurieren möchten.
4. Wählen Sie im Feld **Network Place (Samba) Support (Netzwerkumgebungsunterstützung (Samba))** die Option **Yes (Ja)**.
5. Geben Sie Benutzername und Kennwort zum Zugriff auf den VPN-Server ein. Klicken Sie auf die Schaltfläche .
6. Klicken Sie auf **Apply (Übernehmen)**.

## 4.6 Firewall

Sie können den WLAN-Router als Hardware-Firewall in Ihrem Netzwerk einsetzen.

---

**HINWEIS:** Die Firewall-Funktion ist per Vorgabe bereits aktiv.

---

### 4.6.1 Allgemein

**So richten Sie grundlegende Firewall-Einstellungen ein:**

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen)** > **Firewall** > **General (Allgemein)**.
2. Im Feld **Enable Firewall (Firewall aktivieren)** wählen Sie **Yes (Ja)**.
3. Unter **Enable DoS protection (DoS-Schutz aktivieren)** wählen Sie **Yes (Ja)**, um Ihr Netzwerk vor DoS-Attacks (Denial of Service, Überlastung durch übermäßig viele Anfragen) zu schützen, die die Leistung Ihres Routers beeinträchtigen können.
4. Zusätzlich können Sie Pakete überwachen, die zwischen LAN und WAN ausgetauscht werden. Unter **Logged packets type (Protokollierter Pakettyp)** wählen Sie **Dropped (Abgewiesen)**, **Accepted (Angenommen)** oder **Both (Beides)**.
5. Klicken Sie auf **Apply (Übernehmen)**.

### 4.6.2 URL-Filter

Sie können Schlüsselwörter oder Internetadressen festlegen, um den Zugriff auf bestimmte URLs zu verhindern.

---

**HINWEIS:** Der URL-Filter basiert auf einer DNS-Abfrage. Falls ein Netzwerk-Client zuvor bereits auf eine Internetseite wie <http://www.abcxxx.com> zugriff, wird die jeweilige Internetseite nicht blockiert (ein DNS-Puffer im System speichert zuvor besuchte Seiten). Zur Lösung dieses Problems (sofern es ein solches sein sollte) löschen Sie den DNS-Puffer, bevor Sie den URL-Filter einrichten.

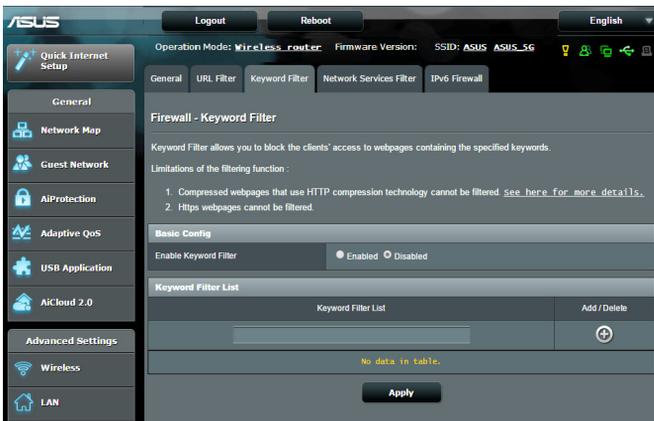
---

## So richten Sie einen URL-Filter ein:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Firewall > URL Filter (URL-Filter)**.
2. Wählen Sie im Feld Enable URL Filter (URL-Filter aktivieren) die Option **Enabled (Aktiviert)**.
3. Geben Sie eine URL ein, klicken Sie anschließend auf die Schaltfläche .
4. Klicken Sie auf **Apply (Übernehmen)**.

## 4.6.3 Schlüsselwortfilter

Der Schlüsselwortfilter blockiert Internetseiten, die bestimmte Ausdrücke enthalten.



## So richten Sie einen Schlüsselwortfilter ein:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Firewall > Keyword Filter (Schlüsselwortfilter)**.
2. Wählen Sie im Feld Enable Keyword Filter (Schlüsselwortfilter aktivieren) die Option **Enabled (Aktiviert)**.

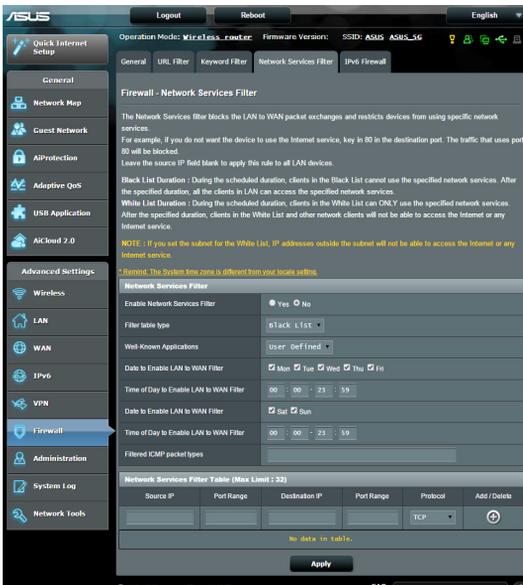
3. Geben Sie ein Wort oder einen Ausdruck ein, klicken Sie dann auf die **Add (Hinzufügen)**- Schaltfläche.
4. Klicken Sie auf **Apply (Übernehmen)**.

## HINWEISE:

- Der Schlüsselwortfilter basiert auf einer DNS-Abfrage. Falls ein Netzwerk-Client zuvor bereits auf eine Internetseite wie <http://www.abcxxx.com> zugriff, wird die jeweilige Internetseite nicht blockiert (ein DNS-Puffer im System speichert zuvor besuchte Seiten). Zur Lösung dieses Problems (sofern es ein solches sein sollte) löschen Sie den DNS-Puffer, bevor Sie den Schlüsselwortfilter einrichten.
- Internetseiten, die per HTTP-Komprimierung komprimiert wurden, können nicht gefiltert werden. Auch HTTPS-Seiten können nicht per Schlüsselwortfilter blockiert werden.

## 4.6.4 Netzwerkdienstefilter

Der Netzwerkdienstefilter blockiert zwischen LAN und WAN ausgetauschte Pakete und verhindert, dass Netzwerk-Clients auf bestimmte Web-Dienste wie Telnet oder FTP zugreifen können.

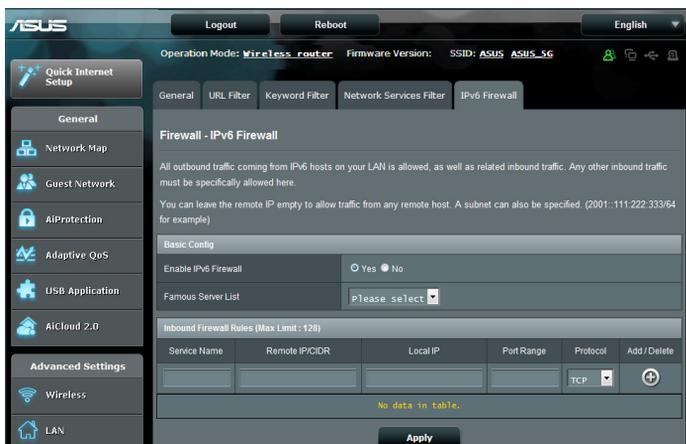


## So richten Sie einen Netzwerkdienstefilter ein:

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Firewall > Network Service Filter (Netzwerkdienstefilter)**.
2. Wählen Sie im Feld Enable Network Services Filter (Netzwerkdienstefilter aktivieren) die Option **Yes (Ja)**.
3. Wählen Sie den Filtertabellentyp. Die **Black List (Schwarze Liste)** blockiert die angegebene Netzwerkdienste. Die **White List (Weiße Liste)** beschränkt den Zugriff auf die angegebene Netzwerkdienste.
4. Legen Sie fest, zu welchen Tagen und Uhrzeiten die Filter aktiv sein sollen.
5. Zum Festlegen eines zu filternden Netzwerkdienstes geben Sie Quell-IP, Ziel-IP, Portbereich und Protokoll an. Klicken Sie auf die Schaltfläche .
6. Klicken Sie auf **Apply (Übernehmen)**.

### 4.6.5 IPv6-Firewall

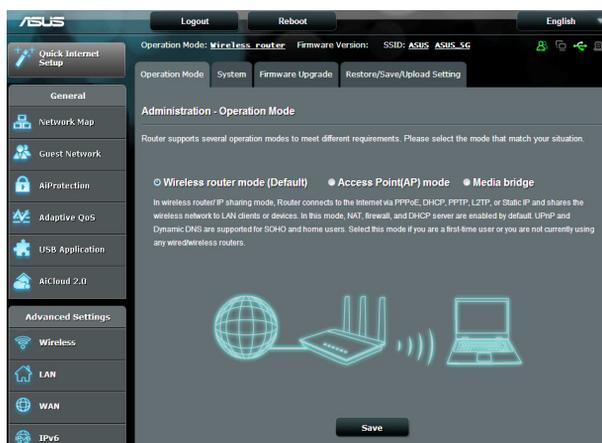
Standardmäßig blockiert Ihr WLAN-Router von ASUS den gesamten unaufgefordert eingehenden Datenverkehr. Die IPv6-Firewall-Funktion erlaubt eingehenden Datenverkehr von bestimmten Diensten das Passieren Ihres Netzwerks.



## 4.7 Administration

### 4.7.1 Betriebsmodus

Auf der Betriebsmodus-Seite können Sie den passenden Betriebsmodus Ihres Netzwerkes festlegen.



**So richten Sie den Betriebsmodus ein:**

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Administration > Operation Mode (Betriebsmodus)**.
2. Wählen Sie eine der folgenden Betriebsmodi:
  - **WLAN-Router (Standardeinstellung):** Im WLAN-Router-Modus verbindet sich der WLAN-Router mit dem Internet und ermöglicht Netzwerkgeräten Internetzugang über das eigene, lokale Netzwerk.
  - **Repeater Mode (Repeater-Modus):** Im Repeater-Modus stellt Ihr WLAN-Router zur Erweiterung der WLAN-Abdeckung kabellos eine Verbindung zu einem bestehenden WLAN-Netzwerk her. In diesem Modus werden Firewall-, IP-Freigabe- und NAT-Funktionen deaktiviert.
  - **AP-Modus:** In diesem Modus erstellt der Router ein neues WLAN-Netzwerk im bereits vorhandene Netzwerk.
3. Klicken Sie auf **Apply (Übernehmen)**.

---

**HINWEIS:** Nach einer Betriebsmodusänderung startet der Router neu.

---

- **Medienbrücke:** Bei dieser Konfiguration werden zwei WLAN-Router benötigt. Der zweite Router dient als Medienbrücke, über die mehrere Geräte wie internetfähige Fernsehgeräte und Spielkonsolen per Ethernet (LAN) verbunden werden können.
3. Klicken Sie auf **Apply (Übernehmen)**.

---

**HINWEIS:** Nach einer Betriebsmodusänderung startet der Router neu.

---

## 4.7.2 System

Auf der **System**-Seite konfigurieren Sie die Einstellungen Ihres WLAN-Routers.

**So nehmen Sie Systemeinstellungen vor:**

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Administration > System**.
2. Sie können folgende Einstellungen konfigurieren:
  - **Router-Anmeldungskennwort ändern:** Hier können Sie Kennwort und Anmeldenamen Ihres WLAN-Routers ändern, indem Sie einen neuen Namen und ein neues Kennwort eingeben.
  - **Zeitzone:** Wählen Sie die Zeitzone, in der sich Ihr Netzwerk befindet.
  - **NTP-Server:** Der WLAN-Router kann zur Synchronisierung der Uhrzeit auf einen NTP-Server (Netzwerkzeitprotokoll-Server) zugreifen.
  - **Telnet aktivieren:** Klicken Sie zum Aktivieren von Telnet-Diensten im Netzwerk auf **Yes (Ja)**. Mit der Auswahl **No (Nein)** deaktivieren Sie Telnet.
  - **Authentisierungsverfahren:** Zum Absichern des Router-Zugriffs können Sie HTTP, HTTPS oder Beides auswählen.
  - **Internetzugriff aus dem WAN aktivieren:** Wählen Sie **Yes (Ja)**, wenn Geräte außerhalb des Netzwerks auf die grafische Benutzeroberfläche des WLAN-Routers zugreifen dürfen. Wählen Sie **No (Nein)**, wenn Sie den Zugriff unterbinden möchten.

- **Nur bestimmte IP zulassen:** Klicken Sie auf **Yes (Ja)**, wenn Sie IP-Adressen von Geräten festlegen möchten, die aus dem WAN auf die grafische Benutzeroberfläche des WLAN-Routers zugreifen dürfen.
- **Client-Liste:** Geben Sie die WAN-IP-Adresse von Netzwerkgeräten ein, die auf die Einstellungen des WLAN-Routers zugreifen dürfen. Diese Liste wird genutzt, wenn Sie unter **Only allow specific IP (Nur bestimmte IP zulassen)** auf **Yes (Ja)** geklickt haben.

3. Klicken Sie auf **Apply (Übernehmen)**.

### 4.7.3 Aktualisieren der Firmware

---

**HINWEIS:** Laden Sie die neueste Firmware von der ASUS-Webseite unter <http://www.asus.com> herunter.

---

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Administration > Firmware Upgrade (Firmware-Aktualisierung)**.
  2. Klicken Sie im Feld **New Firmware File (Neue Firmware-Datei)** auf **Browse (Durchsuchen)**, wählen Sie anschließend die heruntergeladene Datei aus.
  3. Klicken Sie auf **Upload (Hochladen)**.
- 

**HINWEISE:**

- Nach Abschluss der Aktualisierung warten Sie bitte den Neustart des Systems ab.
  - Falls der Aktualisierungsvorgang fehlschlägt, begibt sich der drahtlose Router automatisch in den Rettungsmodus und die Betriebsanzeige-LED auf der Vorderseite blinkt langsam. Um das System wiederherzustellen oder zu bergen, lesen Sie den Abschnitt **5.2 Firmware Restoration (5.2 Firmware-Wiederherstellung)**.
-

## 4.7.4 Wiederherstellen/Speichern/Hochladen der Einstellungen

**So werden die Einstellungen wiederhergestellt/gespeichert/hochgeladen:**

1. Wechseln Sie vom Navigationspanel zum Register **Advanced Settings (Erweiterte Einstellungen) > Administration > Restore/Save/Upload Setting (Einstellungen wiederherstellen/speichern/hochladen)**.
2. Wählen Sie die Aufgaben, die Sie vornehmen möchten:
  - Um die werkseigenen Standardeinstellungen wiederherzustellen, klicken Sie auf **Restore (Wiederherstellen)** und in der Bestätigungsaufforderung dann auf **OK**.
  - Zum Speichern der aktuellen Systemeinstellungen klicken Sie auf **Save (Speichern)**, öffnen den Ordner, in dem Sie die Datei ablegen möchten, anschließend klicken Sie erneut auf **Save (Speichern)**.
  - Um ältere Systemeinstellungen zu laden, klicken Sie auf **Browse (Durchsuchen)**, um die wiederherzustellende Systemdatei zu wählen, und klicken Sie dann auf **Upload (Hochladen)**.

---

Falls Probleme auftreten sollten, aktualisieren Sie auf die neueste Firmware-Version und konfigurieren neue Einstellungen. Setzen Sie den Router nicht auf die Standardeinstellungen (Werksvorgaben) zurück.

---

## 4.8 Systemprotokoll

Das Systemprotokoll enthält Aufzeichnungen der Netzwerkaktivitäten.

**HINWEIS:** Das Systemprotokoll wird bei einem Neustart und beim Abschalten des Routers rückgesetzt.

### So zeigen Sie das Systemprotokoll an:

1. Wechseln Sie vom Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > System Log (Systemprotokoll)**.
2. Sie können sich Netzwerkaktivitäten in folgenden Registern anschauen:
  - Allgemeines Protokoll
  - DHCP-Zuweisungen
  - WLAN-Protokoll
  - Portweiterleitung
  - Routentabelle

The screenshot displays the ASUS router's web interface. At the top, there are buttons for 'Logout' and 'Reboot', and a language dropdown set to 'English'. Below this, the 'Operation Mode' is 'Wireless Router' and the 'Firmware Version' is 'ASUS\_ASUS\_V6'. The main navigation menu on the left includes 'Quick Internet Setup', 'General', 'Network Map', 'Guest Network', 'AiProtection', 'Adaptive QoS', 'USB Application', 'AiCloud 2.0', 'Advanced Settings', 'Wireless', 'LAN', 'WAN', 'IPv6', 'VPN Server', and 'Firewall'. The 'Advanced Settings' section is expanded to show 'System Log - General Log'. The log content shows a series of system events with timestamps and descriptions, such as 'eth1: Broadcom BCM4331 802.11 Wireless Controller 6.30.102.9 (c366174)', 'device eth1 entered promiscuous mode', and 'port 2 (eth2) entering listening state'. At the bottom of the log area, there are 'Clear', 'Save', and 'Refresh' buttons.

## 4.9 Smart Connect (Schnellverbindung)

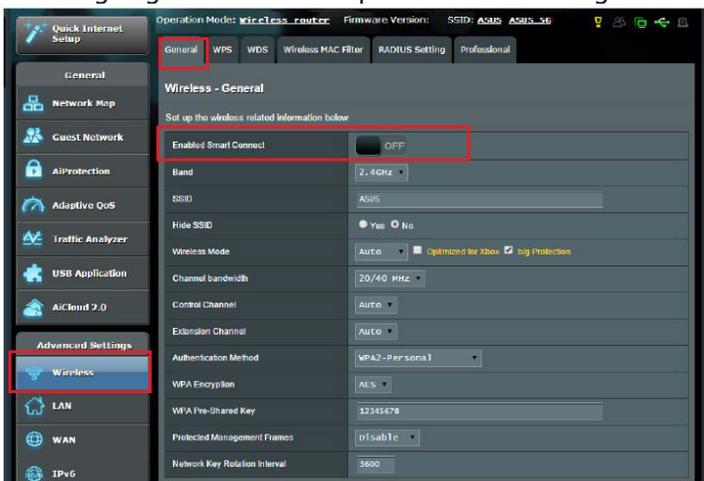
Smart Connect (Schnellverbindung) dient der automatischen Steuerung von Clients an eine von drei Funkverbindungen (2,4 GHz, Low-Band/5 GHz, High-Band/5 GHz) zur Maximierung des gesamten WLAN-Durchsatzes.

### 4.9.1 Smart Connect (Schnellverbindung) einrichten

Sie können Smart Connect (Schnellverbindung) über die Webbenutzeroberfläche aktivieren, indem Sie eine der beiden Methoden befolgen:

#### • Über den Bildschirm Wireless (WLAN)

1. Geben Sie in Ihrem Webbrowser von Hand die Standard-IP-Adresse des WLAN-Routers ein: <http://router.asus.com>.
2. Geben Sie auf der Anmeldeseite den **Standardbenutzernamen (admin)** und das **Standardkennwort (admin)** ein und klicken Sie auf OK. Die QIS-Seite erscheint automatisch.
3. Rufen Sie über den Navigationsbereich das **Register Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > General (Allgemein)** auf.
4. Setzen Sie den Regler im **Enable Smart Connect (Schnellverbindung aktivieren)**-Feld auf **ON (Ein)**. Diese Funktion verbindet automatisch die Clients in Ihrem Netzwerk mit dem geeigneten Band für optimale Geschwindigkeit.



- **Über den Bildschirm Network Map (Netzwerkübersicht)**

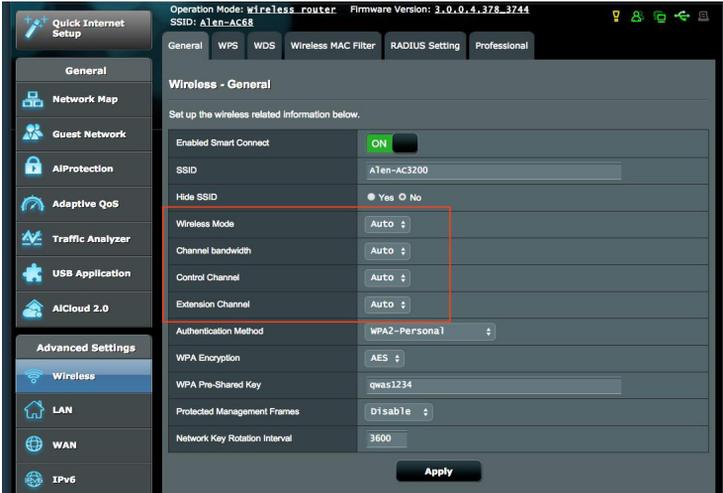
1. Befolgen Sie die ersten beiden Schritte im obigen Abschnitt zur Anmeldung an der Webbenutzeroberfläche.
2. Wählen Sie über den Navigationsbereich **General (Allgemein)** > **Network Map (Netzwerkübersicht)**.
3. Bewegen Sie den Regler am Bildschirm **Network Map (Netzwerkübersicht)** unter **System status (Systemstatus)** im Feld **Smart Connect (Schnellverbindung)** auf **ON (Ein)**.



Nach Aktivierung von Smart Connect (Schnellverbindung) können Sie den Status von **Smart Connect (Schnellverbindung)** am Bildschirm **Network Map (Netzwerkübersicht)** prüfen. Wenn Sie weitere WLAN-Konfigurationen ändern möchten, klicken Sie zum Aufrufen der Einstellungsseite auf **On (Ein)/Off (Aus)**.



Wenn Smart Connect (Schnellverbindung) aktiviert ist, passt Ihr Router WLAN-Modus, Kanalbandbreite, Steuerungskanalbreite und Erweiterungskanaleinstellungen automatisch entsprechend Ihren Netzwerkbedingungen an. Sie können die Änderungen über den Bildschirm Wireless (WLAN) prüfen.



## 4.9.2 Smart Connect Rule (Schnellverbindungsregel)

ASUSWRT bietet Standardbedingungseinstellungen zur Auslösung des Umschaltmechanismus. Sie können die Auslösebedingungen auch entsprechend Ihrer Netzwerkumgebung ändern. Rufen Sie zum Ändern der Einstellungen das Register Smart Connect Rule (Regeln der Schnellverbindung) am Bildschirm Network Tools (Netzwerkwerkzeuge) auf.

Operator Mode: Wireless Router, Firmware Version: 3.0.0.4.376-1129  
SSID: ASUSPN-Public

Network Analysis, Netstat, Wake on LAN, **Smart Connect Rule**

### Wireless - Smart Connect Rule

Set up the Smart Connect related information below.

#### Steering Trigger Condition

	2.4GHz	5GHz-1	5GHz-2
Bandwidth Utilization	0%	80%	0%
Enable Load Balance	Yes No	Yes No	Yes No
RSSI	Greater -58 dBm	Less 0 dBm	Less 0 dBm
PHY Rate Less	Disable	< 54 Mbps	< 433 Mbps
PHY Rate Greater	> 110 Mbps	> 433 Mbps	Disable
VHT	All	All	All

#### STA Selection Policy

RSSI	Greater -58 dBm	Less -76 dBm	Less 0 dBm
PHY Rate Less	Disable	Disable	< 433 Mbps
PHY Rate Greater	> 110 Mbps	> 433 Mbps	Disable
VHT	All	All	All

#### Interface Select and Qualify Procedures

Target Band	1: 5GHz-2 2: 5GHz-1	1: 5GHz-2 2: 2.4GHz	1: 5GHz-1 2: 2.4GHz
Bandwidth Utilization	0%	60%	0%

#### Bounce Detect

Window Time	180 seconds
Counts	4
Dwell Time	1800 seconds

Default Apply

Die Bedienelemente von Smart Connect Rule (Regeln der Schnellverbindung) sind in vier Bereiche unterteilt:

- Steering Trigger Condition (Zustand Steuerungsauslöser)
- STA Selection Policy (STA-Auswahlrichtlinie)
- Interface Select and Qualify Procedures (Schnittstellenauswahl und Qualifizierungsverfahren)
- Bounce Detect (Bounce-Erkennung)

## Steering Trigger Condition (Zustand Steuerungsauslöser)

Diese Auswahl an Bedienelementen legt die Kriterien zur Ausführung der Bandsteuerung fest.

Steering Trigger Condition			
Band	2.4GHz	5GHz-1	5GHz-2
Bandwidth Utilization	<input type="range"/> 0%	<input type="range"/> 80%	<input type="range"/> 0%
Enable Load Balance	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Yes <input type="radio"/> No	<input checked="" type="radio"/> Yes <input type="radio"/> No
RSSI	Greater <input type="text"/> -58 dBm	Less <input type="text"/> 0 dBm	Less <input type="text"/> 0 dBm
PHY Rate Less	<input type="range"/> Disable	<input type="range"/> < 54 Mbps	<input type="range"/> < 433 Mbps
PHY Rate Greater	<input type="range"/> > 110 Mbps	<input type="range"/> > 433 Mbps	<input type="range"/> Disable
VHT	All <input type="text"/>	All <input type="text"/>	All <input type="text"/>

- **Bandwidth Utilization (Bandbreitennutzung)**  
Wenn die Bandbreitennutzung diesen Prozentsatz übersteigt, greift die Steuerung. Die Broadcom-Dokumentation liefert keine Informationen darüber, wie die Nutzung gemessen wird.
- **Enable Load Balance (Lastausgleich aktivieren)**  
Dies steuert den Lastausgleich. Die Broadcom-Dokumentation liefert keine Informationen darüber, wie der Ausgleich durchgeführt wird.
- **RSSI**  
Wenn der Signalpegel eines zugewiesenen Clients dieses Kriterium erfüllt, wird die Steuerung ausgelöst.
- **PHY Rate Less / PHY Rate Greater (PHY-Rate geringer als / PHY-Rate größer als)**  
Diese Bedienelemente ermitteln die STA-Verbindungsraten, welche die Bandsteuerung auslösen.
- **VHT**  
Diese Bedienelemente legen fest, wie 802.11ac- und Nicht-ac-Clients behandelt werden.
  - **ALL (Alle)**(Standard) bedeutet, dass jegliche Clients die Steuerung auslösen können.
  - **AC only** only (Nur AC) bedeutet, dass ein Client zur Auslösung der Steuerung 802.11ac unterstützen muss.
  - **Not-allowed** (Nicht erlaubt) bedeutet, dass nur Nicht-802.11ac-Client die Steuerung auslösen, d. h. 802.11a/b/g/n.

## STA Selection Policy (STA-Auswahlrichtlinie)

Sobald die Steuerung ausgelöst wurde, befolgt ASUSWRT die STA Selection Policy (STA-Auswahlrichtlinie) zur Auswahl eines Clients (STA), der zum geeignetsten Band gesteuert wird.



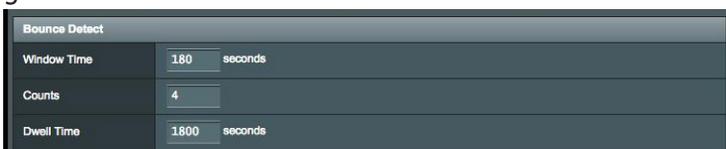
## Interface Select and Qualify Procedures (Schnittstellenauswahl und Qualifizierungsverfahren)

Diese Bedienelemente legen fest, wo der gesteuerte Client landet. Die Bedienelemente Target Band (Zielband) geben die erste und zweite Wahl der Steuerungsziele an. Clients, welche die Funkkriterien der STA-Auswahlrichtlinie erfüllen, werden zum ersten Ziel gesteuert, falls die **Bandwidth Utilization (Bandbreitennutzung)** dieser Funkverbindung unterhalb des eingestellten Wertes liegt. Andernfalls wird der Client an die Funkverbindung von Target **Band (Zielband)** Nummer zwei gesendet.



## Bounce Detect (Bounce-Erkennung)

Diese Bedienelemente legen fest, wie oft ein Client gesteuert werden kann. Dadurch soll verhindert werden, dass Clients konstant umherwandern. Es verhindert jedoch nicht, dass sich Clients selbst trennen oder als Bounces gezählt werden, falls Sie dies tun. Jeder Client kann N-mal (Counts (Anzahl) innerhalb der Angabe unter **Window Time (Zeitfenster)** gesteuert werden. Bei Erreichen des bei Count (Anzahl) festgelegten Limits wird der Client während der Dwell Time (Verweilzeit) nicht erneut gesteuert.



## 5 Verwenden der Hilfsprogramme

---

### HINWEISE:

- Laden Sie die Hilfsprogramme von der ASUS-Webseite herunter und installieren Sie sie:
  - Device Discovery v1.4.7.1 unter <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>.
  - Firmware Restoration v1.9.0.4 unter <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>.
  - Windows Printer Utility v1.0.5.5 unter <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip>.

### 5.1 Device Discovery

Device Discovery (Gerätesuche) ist ein ASUS WLAN-Hilfsprogramm, das einen drahtlosen ASUS Router erkennen kann und Ihnen die Konfiguration des Gerätes ermöglicht.

#### **So starten Sie das Hilfsprogramm Device Discovery:**

- Klicken Sie in Ihrem Computer-Desktop auf: **Start > All Programs (Alle Programme) > ASUS Utility > RT-AC5300 Wireless Router > Device Discovery.**

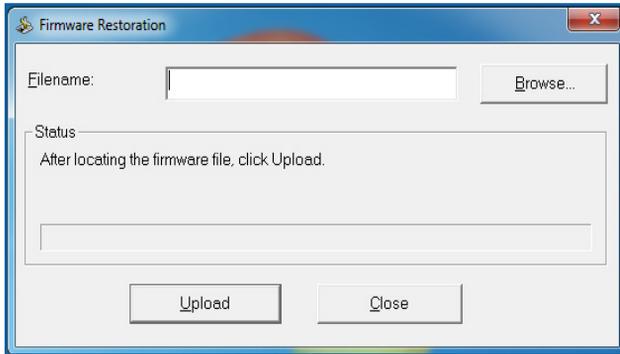
---

**HINWEIS:** Falls Sie den Router auf Access Point-Modus einstellen, verwenden Sie die Gerätesuch (**Device Discovery**), um die IP-Adresse des Routers zu finden.

---

## 5.2 Firmware Restoration

Firmware Restoration (Firmware-Wiederherstellung) wird bei einem drahtlosen ASUS Router verwendet, welches während des Aktualisierungsprozesses ausfällt. Es lädt die von Ihnen angegebenen Firmware hoch. Der Vorgang kann drei bis vier Minuten dauern.



---

**WICHTIG:** Bevor sie die Anwendung Firmware Restoration verwenden, starten Sie den Rettungsmodus.

---

**HINWEIS:** Diese Funktion wird unter Mac OS nicht unterstützt.

---

### **So starten Sie den Rettungsmodus zusammen mit dem Hilfsprogramm Firmware Restoration:**

1. Trennen Sie die Stromversorgung des drahtlosen Routers.
2. Halten Sie die Reset-Taste auf der Rückseite gedrückt und stellen Sie gleichzeitig die Stromversorgung her. Lassen Sie die Reset-Taste wieder los, sobald die Strom-LED auf der Vorderseite mit langsamen Blinken beginnt, was auf den drahtlosen Router im Bergungsmodus hinweist.

3. Legen Sie eine statische IP am Computer fest, nutzen Sie folgende Daten zum Einrichten Ihrer TCP/IP-Einstellungen:

**IP-Adresse:** 192.168.1.x

**Subnetzmaske:** 255.255.255.0

4. Klicken Sie in Ihrem Computer-Desktop auf: **Start > All Programs (Alle Programme) > ASUS Utility RT-N56U Wireless Router > Firmware Restoration.**
5. Geben Sie eine Firmware-Datei an und klicken Sie auf **Upload (Hochladen).**

---

**HINWEIS:** Diese Anwendung ist kein Firmware-Aktualisierungsprogramm und kann nicht auf einem betriebsfähigen drahtlosen ASUS Router verwendet werden. Eine normale Firmwareaktualisierung muss über die Web-GUI ausgeführt werden. Weitere Informationen finden Sie in **Kapitel 4: Konfigurieren der erweiterten Einstellungen.**

---

## 5.3 Druckerserver einrichten

### 5.3.1 ASUS EZ Printer Sharing

Die ASUS EZ Printing Sharing-Software ermöglicht den Anschluss eines USB-Druckers an den USB-Port Ihres WLAN-Routers und die Einrichtung des Drucker-servers. So können Ihre Clients im Netzwerk kabellos drucken und auf Dateien zugreifen.



---

**HINWEIS:** Druckerserverfunktionen werden unter Windows® XP, Windows® Vista und Windows® 7 unterstützt.

---

### So richten Sie die EZ-Druckerfreigabe ein:

1. Wechseln Sie vom Navigationspanel zu **General > USB Application > Network Printer Server (Allgemein > USB-Anwendungen > Netzwerk-Druckerserver)**.
2. Klicken Sie zum Herunterladen der Netzwerkdruckersoftware auf **Download Now! (Jetzt herunterladen!)**.

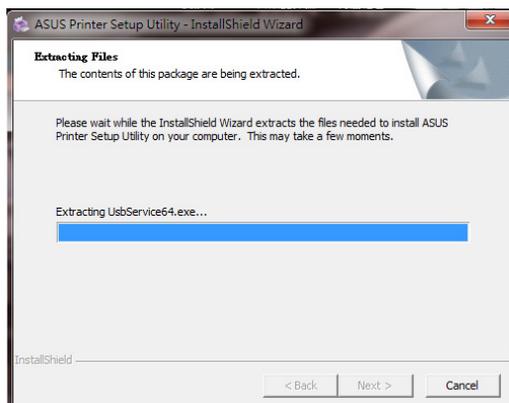
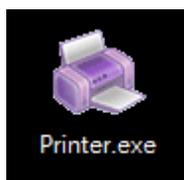


---

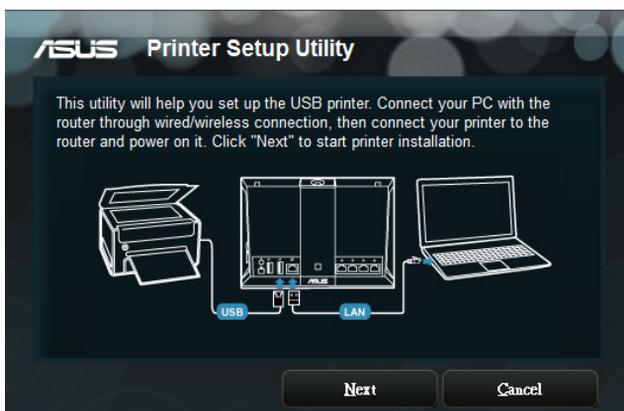
**HINWEIS:** Die Netzwerkdruckersoftware wird nur unter Windows® XP, Windows® Vista und Windows® 7 unterstützt. Zur Installation unter Mac OS wählen Sie **Use LPR protocol for sharing printer (LPR-Protokoll zur Druckerfreigabe verwenden)**.

---

3. Entpacken Sie die heruntergeladene Datei und klicken Sie auf das Druckersymbol, um das Programm auszuführen.



4. Folgen Sie den Bildschirmanweisungen, um Ihre Hardware einzurichten und klicken Sie dann auf **Weiter**.

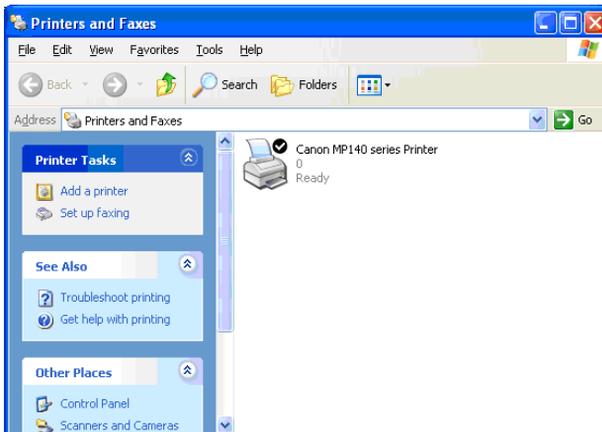


5. Warten Sie ein paar Minuten auf den Abschluss der Basiseinrichtung und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen.

7. Folgen Sie den Anweisungen des Windows® Betriebssystems, um den Druckertreiber zu installieren.



8. Nachdem die Installation der Druckertreiber abgeschlossen ist, können die Netzwerk-Clients darauf zugreifen.



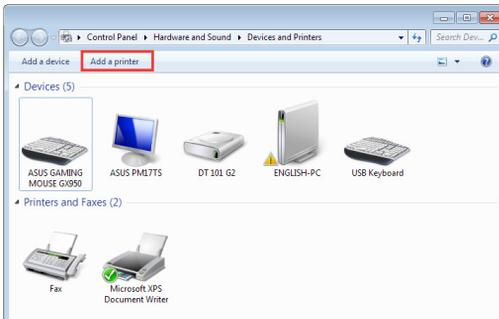
## 5.3.2 LPR zur Druckerfreigabe verwenden

Sie können einen Drucker für Computer mit Windows®- und Mac-Betriebssystemen per LPR/LPD (Line Printer Remote/Line Printer Daemon) freigeben.

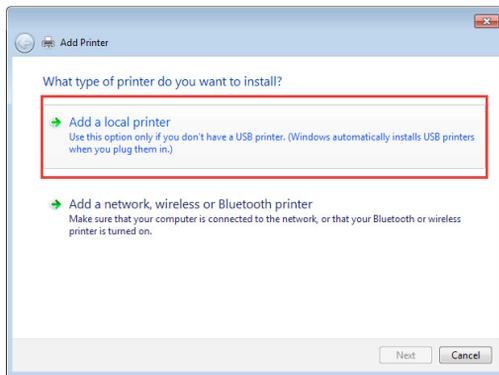
### LPR-Drucker freigeben

So geben Sie einen LPR-Drucker frei:

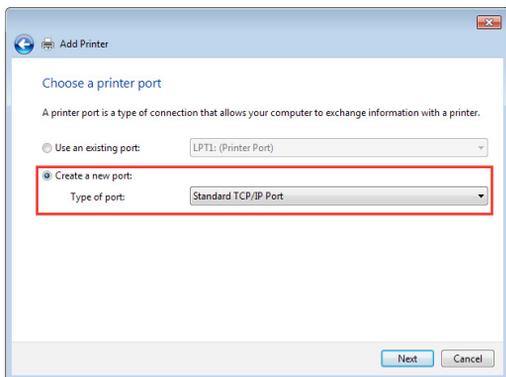
1. Klicken Sie auf dem Windows®-Desktop auf **Start > Geräte und Drucker (Devices and Printers) > Drucker hinzufügen (Add a printer) ; der Drucker hinzufügen (Add Printer Wizard) -Assistent** öffnet sich.



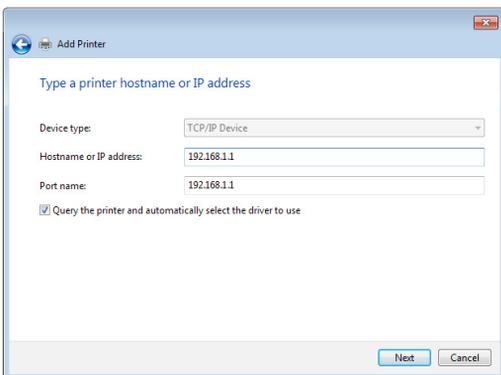
2. Wählen Sie **Einen lokalen Drucker hinzufügen**, klicken Sie dann auf **Weiter**.



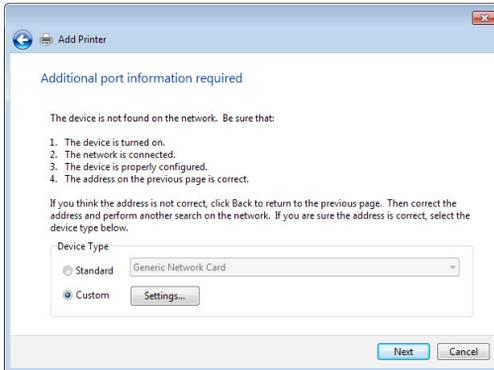
3. Wählen Sie **Create a new port ( Neuen Anschluss ) erstellen**, stellen Sie dann den **Type of Port ( Anschlussstyp )** auf **Standard TCP/IP Port ( Standard TCP/IP Port )** ein. Klicken Sie auf **New Port ( Neuer Anschluss )**.



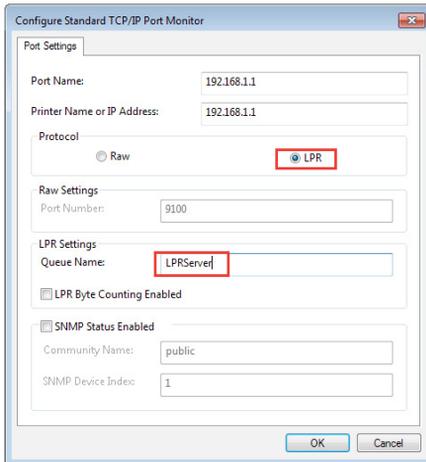
4. Tragen Sie die IP-Adresse des WLAN-Routers in das Feld **Hostname oder IP address ( IP-Adresse )** ein, klicken Sie dann auf **Next ( Weiter )**.



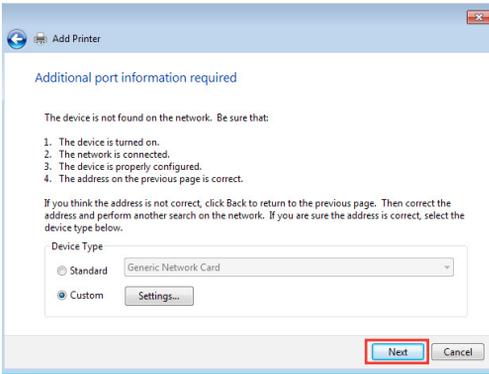
5. Wählen Sie **Custom ( Benutzerdefiniert )**, klicken Sie dann auf **Settings ( Einstellungen )**.



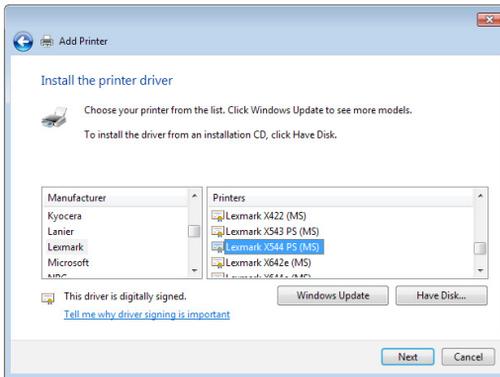
6. Stellen Sie das **Protocol ( Protokoll )** auf **LPR** ein. Tragen Sie **LPRServer** in das Feld **Warteschlangenname** ein, klicken Sie dann zum Fortsetzen auf **OK**.



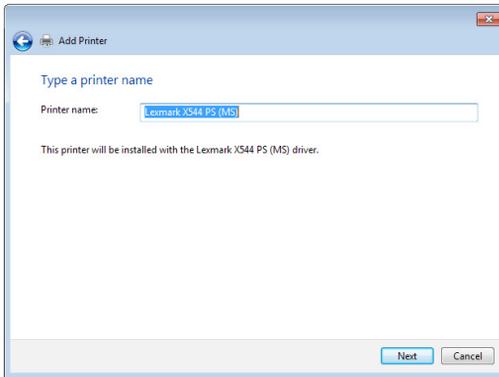
7. Klicken Sie zum Abschluss der Standard-TCP/IP-Porteinstellungen auf **Next (Weiter)**.



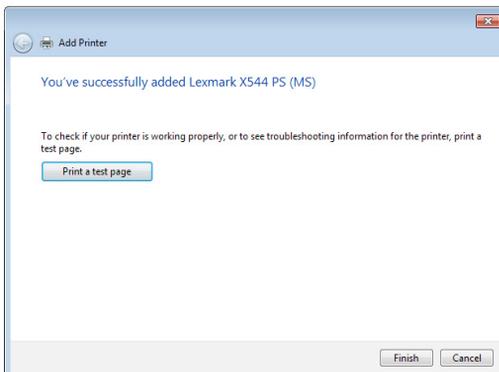
8. Installieren Sie den Druckertreiber aus der Anbieterliste. Falls der Drucker nicht in der Liste aufgeführt wird, klicken Sie zur manuellen Installation der Druckertreiber von CD oder aus einer Datei auf **Have Disk (Datenträger)**.



9. Übernehmen Sie den Standardnamen des Druckers durch einen Klick auf **Next ( Weiter )**.



10. Klicken Sie zum Abschluss der Installation auf **Finish ( Fertig stellen )**.



## 5.4 Download Master

Download Master ist eine Software, die Sie beim Herunterladen von Dateien unterstützt, selbst wenn Ihre Notebooks oder andere Geräte abgeschaltet sind.

---

**HINWEIS:** Um Download Master nutzen zu können, muss ein USB-Gerät an den WLAN-Router angeschlossen sein.

---

### So verwenden Sie Download Master:

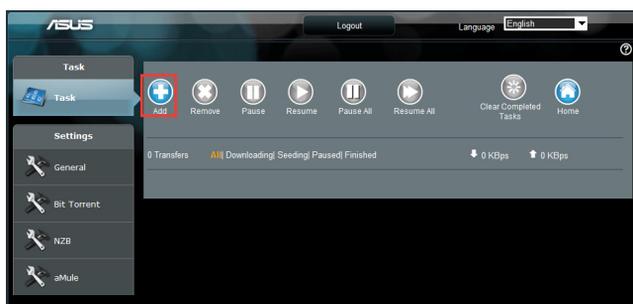
1. Klicken Sie zum automatischen Herunterladen und Installieren auf **General (Allgemein) > USB application (USB-Anwendungen) > Download Master (Download Master)**.

---

**HINWEIS:** Wenn mehrere USB-Geräte angeschlossen sind, wählen Sie das USB-Gerät aus, auf das die Dateien heruntergeladen werden sollen.

---

2. Nach dem Herunterladen starten Sie die Software durch einen Doppelklick auf das Download Master-Symbol.
3. Klicken Sie zum Zufügen einer neuen Download-Aufgabe auf **Add (Hinzufügen)**.



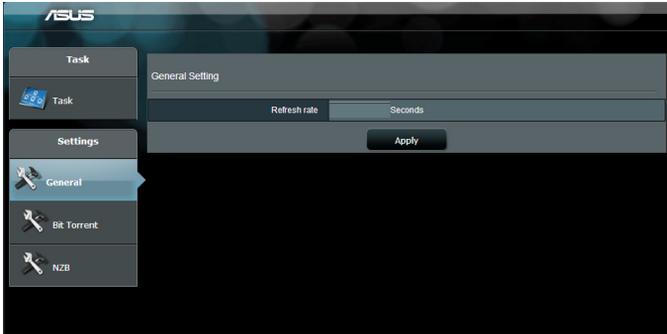
4. Wählen Sie einen Downloadtyp wie BitTorrent, HTTP oder FTP. Geben Sie eine Torrent-Datei oder eine URL zum Starten des Downloads an.

---

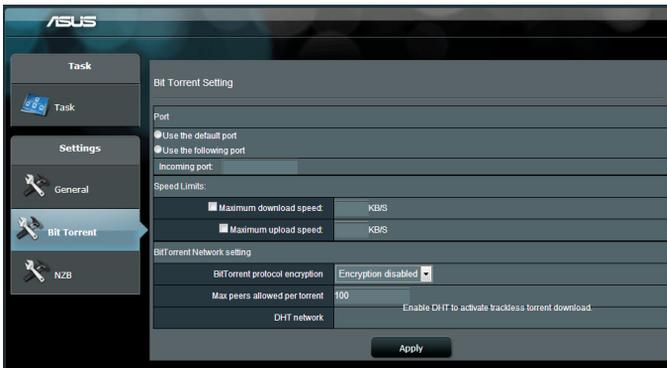
**HINWEIS:** Weiterführende Informationen zu BitTorrent finden Sie im Abschnitt **5.4.1 BitTorrent-Download-Einstellungen konfigurieren**.

---

5. Nutzen Sie das Navigationspanel zur Konfiguration der erweiterten Einstellungen.



### 5.4.1 BitTorrent-Download-Einstellungen konfigurieren

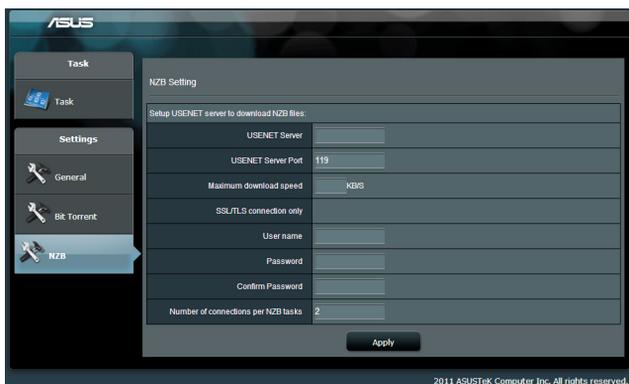


#### So konfigurieren Sie BitTorrent-Download-Einstellungen:

1. Klicken Sie im Download Master-Navigationspanel auf **Bit Torrent (BitTorrent)**; die Seite **Bit Torrent Setting (BitTorrent-Einstellungen)** öffnet sich.
2. Wählen Sie einen spezifischen Port für Ihre Download-Aufgabe.
3. Um Netzwerküberlastungen vorzubeugen, können Sie unter **Speed Limits (Geschwindigkeitslimits)** maximale Upload- und Download-Geschwindigkeiten vorgeben.
4. Sie können die maximale Anzahl zugelassener Peers einschränken und die Dateiverschlüsselung beim Download aktivieren oder deaktivieren.

## 5.4.2 NZB-Einstellungen

Sie können einen USENET-Server zum Herunterladen von NZB-Dateien einrichten. Klicken Sie nach der Eingabe der USENET-Einstellungen auf **Apply (Übernehmen)**.



## 6 Fehlerbehebung

In diesem Kapitel finden Sie Lösungen zu Problemen, die eventuell mit Ihrem Router auftreten können. Falls Sie auf Probleme stoßen sollten, die nicht in diesem Kapitel behandelt werden, besuchen Sie die ASUS-Kundendienstseiten: <http://support.asus.com/> – Hier finden Sie weitere Produktinformationen und Möglichkeiten zur Kontaktaufnahme mit dem technischen ASUS-Kundendienst.

### 6.1 Allgemeine Problemlösung

Falls Schwierigkeiten mit Ihrem Router auftreten sollten, versuchen Sie es zunächst mit den allgemeinen Hinweisen in diesem Abschnitt, bevor Sie nach weiteren Lösungsmöglichkeiten suchen.

#### **Firmware auf die neuste Version aktualisieren.**

1. Starten Sie die grafische Benutzeroberfläche. Wechseln Sie zum Register **Advanced Settings (Allgemeine Einstellungen) > Administration > Firmware Upgrade (Firmware-Aktualisierung)**. Schauen Sie mit einem Klick auf **Check (Prüfen)** nach, ob eine aktualisierte Firmware zum Abruf bereit steht.
2. Sofern eine aktualisierte Firmware zur Verfügung steht, besuchen Sie die ASUS-Internetseiten unter [http://www.asus.com/Networks/Wireless\\_Routers/RTAC87U/#download](http://www.asus.com/Networks/Wireless_Routers/RTAC87U/#download) und laden die aktuellste Firmware herunter.
3. Klicken Sie auf der **Firmware-Aktualisierung**-Seite auf **Browse (Durchsuchen)**, suchen Sie die Firmware-Datei heraus.
4. Klicken Sie zur Aktualisierung der Firmware auf **Upload (Hochladen)**. Starten Sie Ihr Netzwerk in folgender Reihenfolge neu:
  1. Schalten Sie das Modem ab.
  2. Trennen Sie das Modem.
  3. Schalten Sie Router und Computer ab.
  4. Schließen Sie das Modem an.
  5. Schalten Sie das Modem ein, warten Sie dann 2 Minuten lang ab.
  6. Schalten Sie den Router ein, warten Sie weitere 2 Minuten ab.
  7. Schalten Sie die Computer ein.

## Prüfen Sie, ob die Netzkabel richtig angeschlossen sind.

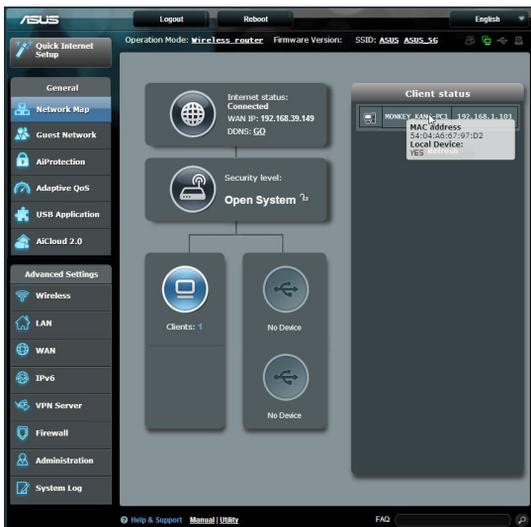
- Wenn das Netzkabel, welches den Router mit dem Modem verbindet, richtig angeschlossen ist, leuchtet die WAN-LED.
- Wenn das Netzkabel, welches den eingeschalteten Computer mit dem Router verbindet, richtig angeschlossen ist, leuchtet die entsprechende LAN-LED.

## Vergewissern Sie sich, dass die WLAN-Einstellungen zu den Einstellungen Ihres Computers passen.

- Wenn Sie den Computer kabellos an den Router anschließen, vergewissern Sie sich, dass SSID (der WLAN-Netzwerkname), Verschlüsselungsverfahren und Kennwort stimmen.

## Prüfen Sie Ihre Netzwerkeinstellungen auf Richtigkeit.

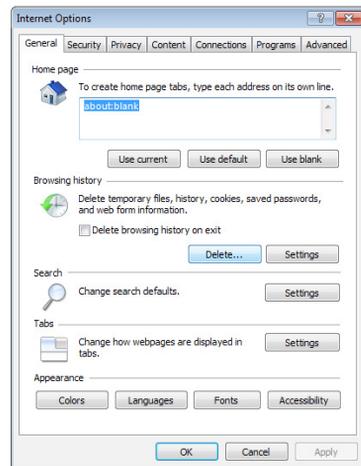
- Jeder Client im Netzwerk muss über eine gültige IP-Adresse verfügen. Wir empfehlen, die IP-Adressen der Computer in Ihrem Netzwerk über den DHCP-Server des WLAN-Routers zuweisen zu lassen.
- Einige Kabelmodem-Serviceanbieter setzen voraus, dass die MAC-Adresse des Computers verwendet wird, die als erste zur Kontoregistrierung genommen wurde.
- Sie können die MAC-Adresse über die grafische Benutzeroberfläche abrufen: Wechseln Sie zur Seite **Network Map (Netzwerkübersicht) > Clients (Clients)**, setzen Sie dann unter **Client Status (Client-Status)** den Mauszeiger auf den Namen Ihres Gerätes.



## 6.2 Häufig gestellte Fragen (FAQ)

### Ich kann per Webbrowser nicht auf die grafische Benutzeroberfläche des Routers zugreifen

- Wenn Ihr Computer per Kabel angeschlossen wurde, überprüfen Sie die Netzkabelverbindung und den LED-Status, wie im vorherigen Abschnitt beschrieben.
- Vergewissern Sie sich, dass Sie die richtigen Anmeldedaten eingeben. Ab Werk wurde als Anmeldename und als Kennwort der Begriff „admin“ eingestellt. Achten Sie darauf, dass die Feststelltaste nicht gedrückt wurde, wenn Sie die Anmeldedaten eingeben.
- Löschen Sie Cookies und temporäre Dateien Ihres Webbrowsers. Beim Internet Explorer 8 führen Sie die folgenden Schritte aus:
  1. Starten Sie den Internet Explorer 8, klicken Sie dann auf **Tools > Internet Options (Extras > Internetoptionen)**.
  2. Klicken Sie auf das **General (Allgemein)**-Register, klicken Sie unter **Browsing history (Browserverlauf)** auf **Löschen...**, wählen Sie **Temporary Internet Files (Temporäre Internetdateien)** und **Cookies**, klicken Sie dann auf **Löschen**.



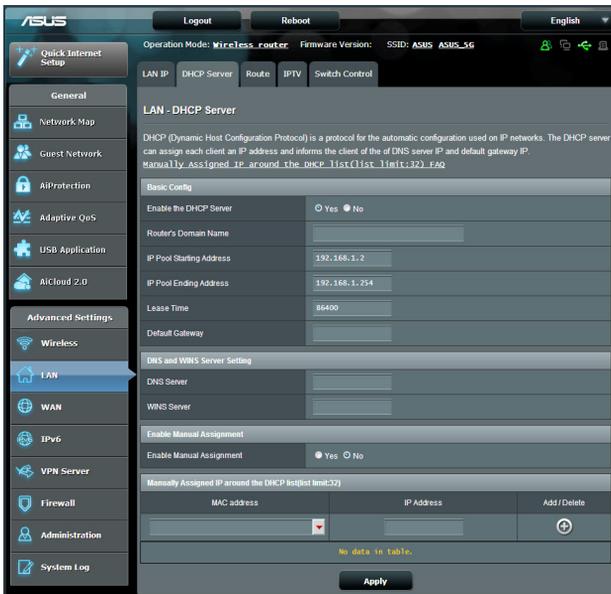
#### HINWEISE:

- Die Schritte zum Löschen von Cookies und temporären Dateien sind von Browser zu Browser unterschiedlich.
- Deaktivieren Sie Proxyservereinstellungen, setzen Sie die Einwahlverbindung außer Kraft, stellen Sie in den TCP/IP-Einstellungen ein, dass IP-Adressen automatisch bezogen werden. Weitere Hinweise dazu finden Sie in Kapitel 1 dieser Anleitung.
- Überzeugen Sie sich davon, dass CAT5e- oder CAT6- Netzkabel eingesetzt werden.

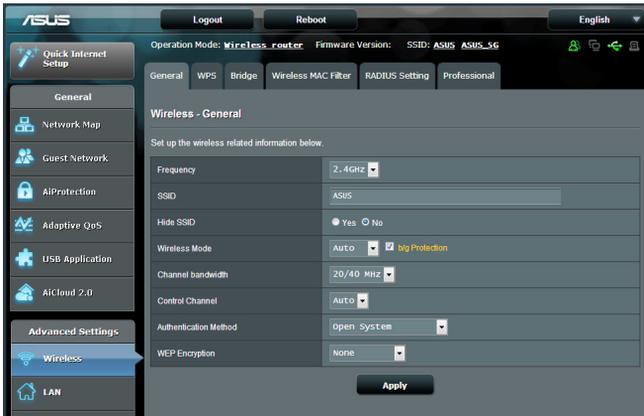
## Der Router lässt sich nicht über einen Webbrowser konfigurieren.

**HINWEIS:**Falls Sie Schwierigkeiten bei der Verbindung mit einem 5-GHz-Netzwerk auftreten, überzeugen Sie sich davon, dass Ihr WLAN-Gerät 5-GHz- oder Dualbandbetrieb unterstützt

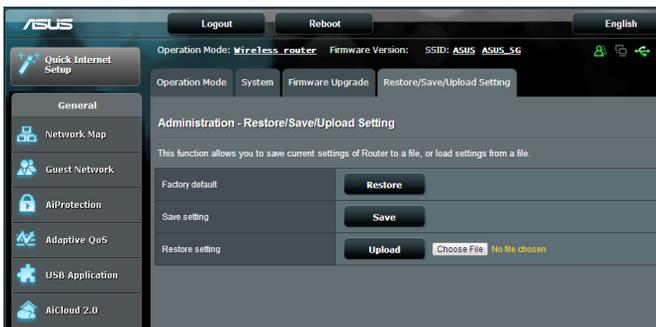
- **Außerhalb der Reichweite:**
  - Stellen Sie den Router näher an den drahtlosen Client.
  - Stellen Sie die Antennen des Routers optimal ein; schauen Sie sich dazu den Abschnitt **1.4 Router aufstellen** an.
- **DHCP-Server wurde deaktiviert:**
  1. Starten Sie die grafische Benutzeroberfläche. Wechseln Sie zu **General (Allgemein) > Network Map (Netzwerkübersicht) > Clients (Clients)**, suchen Sie das Gerät aus, das Sie mit dem Router verbinden möchten.
  2. Falls das Gerät nicht in der **Network Map (Netzwerkübersicht)** angezeigt werden sollte, wechseln Sie zu **Advanced Settings (Erweiterte Einstellungen) > LAN > DHCP Server (DHCP-Server)**, rufen die **Basic Config (Basiskonfiguration)**-Liste auf und wählen **Yes (Ja)** bei **Enable the DHCP Server (DHCP-Server aktivieren)**.



- Die SSID wurde verborgen. Falls Ihr Gerät die SSIDs von anderen Routern, nicht jedoch die SSID Ihres Routers erkennen kann, wechseln Sie zu **Advanced Settings (Erweiterte Einstellungen) > Wireless > General (Allgemein)**, wählen **No** bei **Hide SSID (SSID verbergen)**, anschließend wählen Sie **Auto** bei **Control Channel (Steuerkanal)**.



- Wenn Sie einen WLAN-Adapter verwenden, überzeugen Sie sich davon, dass die genutzten Kanäle mit den in Ihrem Land zulässigen Kanälen übereinstimmen. Falls nicht, passen Sie Kanal, Kanalbandbreite und WLAN-Modus entsprechend an.
- Falls es nach wie vor nicht möglich sein sollte, kabellos auf den Router zuzugreifen, können Sie den Router auf die Werkseinstellungen rücksetzen. Klicken Sie in der grafischen Benutzeroberfläche des Routers auf **Administration > Restore/Save/Upload Setting (Einstellungen wiederherstellen/speichern/hochladen)**, klicken Sie anschließend auf **Restore (Wiederherstellen)**.



## Das Internet ist nicht zugänglich.

- Vergewissern Sie sich, dass sich Ihr Router mit der WAN-IP-Adresse Ihres Internetanbieters verbinden kann. Dazu rufen Sie die grafische Benutzeroberfläche auf, klicken auf **General (Allgemein) > Network Map (Netzwerkübersicht)** und prüfen den **Internet Status (Internetstatus)**.
- Falls sich Ihr Router nicht mit der WAN-IP-Adresse Ihres Internetanbieters verbinden kann, starten Sie den Router wie im Abschnitt **Starten Sie Ihr Netzwerk in folgender Reihenfolge neu**: unter **Allgemeine Problemlösung** beschrieben neu.



- Das Gerät wurde durch die Jugendschutzfunktion blockiert. Rufen Sie **General (Allgemein) > Parental Control (Jugendschutz)** auf, schauen Sie nach, ob das Gerät in der Liste aufgeführt wird. Sollte das Gerät unter **Client Name (Client-Name)** aufgelistet werden, entfernen Sie das Gerät mit der **Delete (Löschen)**-Schaltfläche oder ändern die Zeitmanagement-Einstellungen entsprechend ab. Falls Sie nach wie vor nicht auf das Internet zugreifen können, starten Sie Ihren Computer neu; anschließend überprüfen Sie IP-Adresse und Gateway-Adresse.
- Schauen Sie sich die Statusanzeigen am DSL-Modem und am WLAN-Router an. Falls die WAN-LED am WLAN-Router nicht leuchten sollte, vergewissern Sie sich, dass sämtliche Kabel richtig angeschlossen wurden.

## Sie haben die SSID (den Netzwerknamen) oder das Netzwerkkenntwort vergessen

- Legen Sie per Kabelverbindung (Netzwerkabel) eine neue SSID und ein neues Netzwerkkenntwort fest. Rufen Sie die grafische Benutzeroberfläche auf, wechseln Sie zur **Network Map (Netzwerkübersicht)**, geben Sie eine neue SSID und ein neues Netzwerkkenntwort ein, klicken Sie dann auf **Apply (Übernehmen)**.
- Setzen Sie Ihren Router auf die Werkseinstellungen zurück. Starten Sie die grafische Benutzeroberfläche, wechseln Sie zu **Administration > Restore/Save/Upload Setting (Einstellungen wiederherstellen/speichern/hochladen)**, klicken Sie anschließend auf **Restore (Wiederherstellen)**. Anmeldekonto (Benutzername) und Kennwort sind auf „admin“ voreingestellt.

## Wie stellt man die Standardeinstellungen für das System wieder her?

- Wechseln Sie zu **Administration > Restore/Save/Upload Setting (Einstellungen wiederherstellen/speichern/hochladen)**, klicken Sie anschließend auf **Restore (Wiederherstellen)**.

Die werkseigenen Standardeinstellungen sind wie folgt:

<b>Benutzername:</b>	admin
<b>Kennwort:</b>	admin
<b>DHCP-Aktivierung:</b>	Ja (wenn das WAN-Kabel angeschlossen ist).
<b>IP-Adresse:</b>	http://router.asus.com (or 192.168.1.1)
<b>Domänenname:</b>	(Leer)
<b>Subnetzmaske:</b>	255.255.255.0
<b>DNS-Server 1:</b>	192.168.1.1
<b>DNS-Server 2:</b>	(Leer)
<b>SSID (2.4GHz):</b>	ASUS
<b>SSID (5GHz):</b>	ASUS_5G

### Firmware-Aktualisierung fehlgeschlagen.

Starten Sie den Rettungsmodus, starten Sie dann das Firmware-Wiederherstellungsprogramm. Hinweise zur Bedienung des Firmware-Wiederherstellungsprogramms finden Sie im Abschnitt **5.2 Firmware-Wiederherstellung**.

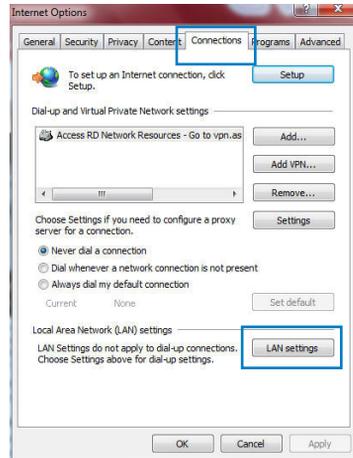
## Grafische Benutzeroberfläche lässt sich nicht aufrufen

Bevor Sie den drahtlosen Router konfigurieren, folgen Sie bei Ihren Host-Computer und Netzwerk-Clients den Anweisungen in diesem Abschnitt.

### A. Proxyserver deaktivieren (falls aktiviert)

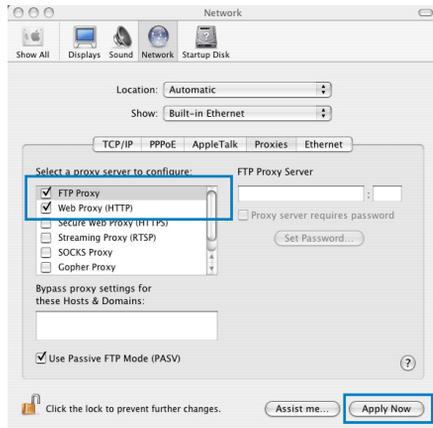
#### Windows® 7

1. Klicken Sie auf **Start > Internet Explorer**, um den Webbrowser zu starten.
2. Klicken Sie auf **Extras (Tools) > Internetoptionen (Internet options) > Auswahl Verbindungen (Connections) > LAN-Einstellungen (LAN settings)**.
3. Im Fenster **Einstellungen für lokales Netzwerk, deaktivieren Sie Proxyserver für LAN verwenden (Use a proxy server for your LAN)**.
4. Wenn abgeschlossen, klicken Sie auf **OK**.



## MAC OS

1. Klicken Sie in der Menüleiste auf **Safari** > **Einstellungen...** (**Preferences...**) > **Erweitert (Advanced) Einstellungen Ändern...** (**Change Settings...**).
2. Deaktivieren Sie in der Protokollliste **FTP Proxy** und **Web Proxy (HTTP)**.
3. Wenn abgeschlossen, klicken Sie auf **Jetzt Anwenden (Apply Now)**.

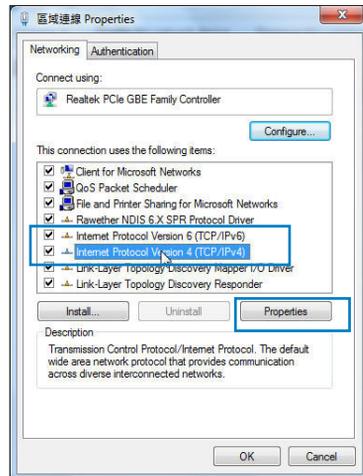


**HINWEIS:**Für Details zur Deaktivierung eines Proxyservers beziehen Sie sich auf die Hilfe Ihres Browsers.

## B. TCP/IP-Einstellungen für automatische IP-Erkennung

### Windows® 7

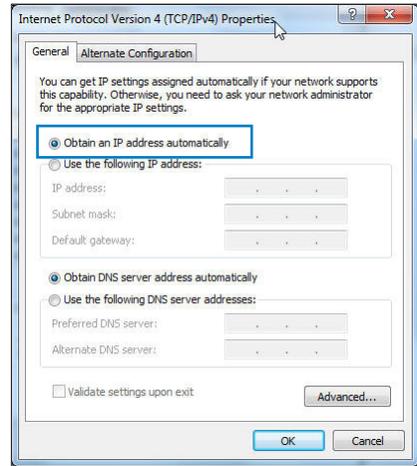
1. Klicken Sie auf **Start** > **Systemsteuerung (Control Panel)** > **Netzwerk und Internet (Network and Internet)** > **Netzwerk- und Freigabecenter (Network and Sharing Center)** > **Netzwerkverbindungen verwalten (Manage network connections)**.
2. Wählen Sie **Internetprotokoll Version 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))** und klicken Sie dann auf **Eigenschaften (Properties)**.



- Um eine IPv4-Adresse automatisch zu beziehen, wählen Sie **IP-Adresse automatisch beziehen (Obtain an IP address automatically)**.

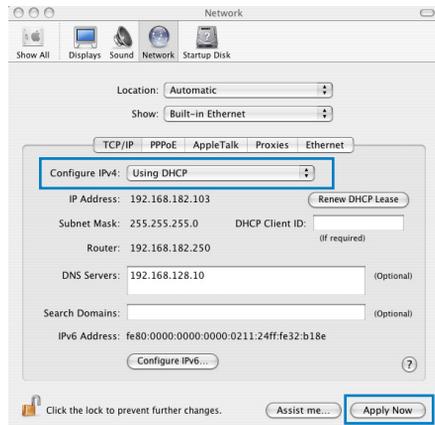
Um eine IPv6-Adresse automatisch zu beziehen, wählen Sie **IPv6-Adresse automatisch beziehen (Obtain an IPv6 address automatically)**.

- Wenn abgeschlossen, klicken Sie auf **OK**.



## MAC OS

- Klicken links oben im Bildschirm sie auf das Apple-Symbol .
- Klicken Sie auf **Systemeinstellungen... (System Preferences) > Netzwerk (Network) Konfigurieren (Configure)**.
- Wählen Sie in der Auswahl **TCP/IP** im Feld **Configure IPv4 (IPv4 konfigurieren)** die Auswahl **DHCP (Using DHCP)**.
- Wenn abgeschlossen, klicken Sie auf **Jetzt Anwenden (Apply Now)**.

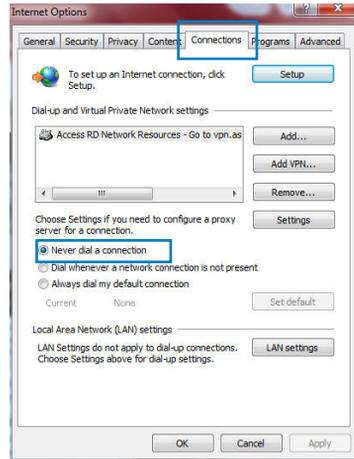


**HINWEIS:**Für Details zur Konfiguration der TCP/IP-Einstellungen beziehen Sie sich auf die Hilfe und Support des jeweiligen Betriebssystems.

## C. DFÜ-Verbindung deaktivieren (falls vorhanden)

### Windows® 7

1. Klicken Sie auf **Start > Internet Explorer**, um den Browser zu starten.
2. Klicken Sie auf **Extras (Tools) > Internetoptionen (Internet options) > Auswahl Verbindungen (Connections)**.
3. Wählen Sie **Keine Verbindung wählen (Never dial a connection)**.
4. Wenn abgeschlossen, klicken Sie auf **OK**.



---

**HINWEIS:** Für Details zur Deaktivierung einer DFÜ-Verbindung beziehen Sie sich auf die Hilfe Ihres Browsers.

---

# Anhänge

## Hinweise

### ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to <http://csr.asus.com/english/Takeback.htm> for the detailed recycling information in different regions.

### REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

<http://csr.asus.com/english/index.aspx>

### Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

---

**IMPORTANT!** This device within the 5.15 ~ 5.25 GHz is restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

---

---

**WARNING!**

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
  - Users must not modify this device. Modifications by anyone other than the party responsible for compliance with the rules of the Federal Communications Commission (FCC) may void the authority granted under FCC regulations to operate this device.
  - For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
-

## **Prohibition of Co-location**

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

## **Safety Information**

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 25 cm between the radiator and your body. Use on the supplied antenna.

## **Declaration of Conformity for R&TTE directive 1999/5/EC**

Essential requirements – Article 3

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 & EN 301 893 have been conducted. These are considered relevant and sufficient.

Operate the device in 5150-5250 MHz frequency band for indoor use only.

## **CE Mark Warning**

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment may be operated in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

### **Canada, Industry Canada (IC) Notices**

This device complies with Industry Canada license-exempt RSS standard(s).

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

### **Radio Frequency (RF) Exposure Information**

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 25 cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 25 cm de distance entre la source de rayonnement et votre corps.

### **Canada, avis d'Industry Canada (IC)**

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

---

**WARNING!**

- Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type should be chosen so that the equivalent isotropically radiated power (e.i.r.p) is not more than that necessary for successful communication.
  - Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.
  - This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.
  - Le présent émetteur radio (identifier le dispositif par son numéro de certification ou son numéro de modèle s'il fait partie du matériel de catégorie I) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.
-

---

## WARNING!

- For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
  - Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
  - This device and its antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.
  - Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionner en association avec une autre antenne ou transmetteur.
  - The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
  - Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.
- 

## NCC 警語

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

## **GNU General Public License**

### **Licensing information**

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. We include a copy of the GPL with every CD shipped with our product. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

### **GNU GENERAL PUBLIC LICENSE**

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### **Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use

pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

### **Terms & conditions for copying, distribution, & modification**

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may

be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
  - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
  - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to

modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide

range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## **NO WARRANTY**

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## ASUS Kontaktinformationen

### ASUSTeK COMPUTER INC.

Adresse 15 Li-Te Road, Peitou, Taipei, Taiwan 11259  
Webseite [www.asus.com.tw](http://www.asus.com.tw)

#### **Technische Unterstützung**

Telefon +886228943447  
Support-Fax +886228907698  
Online-Support [support.asus.com](http://support.asus.com)

### ASUS COMPUTER INTERNATIONAL (Amerika)

Adresse 800 Corporate Way, Fremont, CA 94539, USA  
Telefon +15107393777  
Fax +15106084555  
Webseite [usa.asus.com](http://usa.asus.com)  
Online-Support [support.asus.com](http://support.asus.com)

### ASUS COMPUTER GmbH (Deutschland & Österreich)

Adresse Harkort Str. 25, 40880 Ratingen, Deutschland  
Telefon +49-2102-959931  
Webseite [asus.com/de](http://asus.com/de)  
Online-Kontakt [eu-rma.asus.com/sales](http://eu-rma.asus.com/sales)

#### **Technische Unterstützung**

Telefon (Komponenten) +49-2102-5789555  
Telefon DE +49-2102-5789557  
(System/Notebook/Eee/LCD)  
Telefon AT +43-820-240513  
(System/Notebook/Eee/LCD)  
Support-Fax +49-2102-959911  
Online-Support [support.asus.com](http://support.asus.com)

## Globale Netzwerk-Hotlines

Region	Land	Hotline-Nummer	Servicezeiten	
Europe	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	France	0033-170949400	09:00-18:00 Mon-Fri	
	Germany	0049-1805010920		
		0049-1805010923 ( component support )		09:00-18:00 Mon-Fri 10:00-17:00 Mon-Fri
		0049-2102959911 ( Fax )		
	Hungary	0036-15054561	09:00-17:30 Mon-Fri	
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri	
	Austria	0043-820240513	09:00-18:00 Mon-Fri	
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri	
	Belgium	0032-78150231	09:00-17:00 Mon-Fri	
	Norway	0047-2316-2682	09:00-18:00 Mon-Fri	
	Sweden	0046-858769407	09:00-18:00 Mon-Fri	
	Finland	00358-969379690	10:00-19:00 Mon-Fri	
	Denmark	0045-38322943	09:00-18:00 Mon-Fri	
	Poland	0048-225718040	08:30-17:30 Mon-Fri	
	Spain	0034-902889688	09:00-18:00 Mon-Fri	
	Portugal	00351-707500310	09:00-18:00 Mon-Fri	
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri	
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri	
Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri		
Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri		
Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri		
United Kingdom	0044-8448008340	09:00-17:00 Mon-Fri		
Ireland	0035-31890719918	09:00-17:00 Mon-Fri		
Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri		
Ukraine	0038-0445457727	09:00-18:00 Mon-Fri		

## Globale Netzwerk-Hotlines

Region	Land	Hotline-Nummer	Servicezeiten
Asia-Pacific	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787	09:00-18:00 Mon-Fri
			09:00-17:00 Sat-Sun
	Korea	0081-473905630 ( Non-Toll Free )	09:00-18:00 Mon-Fri
			09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717 1800-8525201	09:00-18:00 Mon-Fri
	Singapore	0065-64157917 0065-67203835 ( Repair Status Only )	11:00-19:00 Mon-Fri
			11:00-13:00 Sat
	Malaysia	0060-320535077	10:00-19:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India	1800-2090365	09:00-18:00 Mon-Sat
	India(WL/NW)		09:00-21:00 Mon-Sun
Indonesia	0062-2129495000 500128 (Local Only)	09:30-17:00 Mon-Fri	
		9:30 – 12:00 Sat	
Vietnam	1900-555581	08:00-12:00	
		13:30-17:30 Mon-Sat	
Hong Kong	00852-35824770	10:00-19:00 Mon-Sat	
Americas	USA	1-812-282-2787	8:30-12:00 EST Mon-Fri
	Canada		9:00-18:00 EST Sat-Sun
	Mexico	001-8008367847	08:00-20:00 CST Mon-Fri
			08:00-15:00 CST Sat

## Globale Netzwerk-Hotlines

Region	Land	Hotline-Nummer	Servicezeiten
<b>Middle East + Africa</b>	Egypt	800-2787349	09:00-18:00 Sun-Thu
	Saudi Arabia	800-1212787	09:00-18:00 Sat-Wed
	UAE	00971-42958941	09:00-18:00 Sun-Thu
	Turkey	0090-2165243000	09:00-18:00 Mon-Fri
	South Africa	0861-278772	08:00-17:00 Mon-Fri
	Israel	*6557/00972-39142800	08:00-17:00 Sun-Thu
		*9770/00972-35598555	08:30-17:30 Sun-Thu
<b>Balkan Countries</b>	Romania	0040-213301786	09:00-18:30 Mon-Fri
	Bosnia Herzegovina	00387-33773163	09:00-17:00 Mon-Fri
		Bulgaria	00359-70014411
	Croatia	00359-29889170	09:30-18:00 Mon-Fri
		00385-16401111	09:00-17:00 Mon-Fri
	Montenegro	00382-20608251	09:00-17:00 Mon-Fri
	Serbia	00381-112070677	09:00-17:00 Mon-Fri
	Slovenia	00368-59045400	08:00-16:00 Mon-Fri
		00368-59045401	08:00-16:00 Mon-Fri
	Estonia	00372-6671796	09:00-18:00 Mon-Fri
	Latvia	00371-67408838	09:00-18:00 Mon-Fri
	Lithuania-Kaunas	00370-37329000	09:00-18:00 Mon-Fri
	Lithuania-Vilnius	00370-522101160	09:00-18:00 Mon-Fri

**HINWEIS:** Besuchen Sie die Webseite <http://support.asus.com> für weitere Informationen.

<b>Hersteller:</b>	<b>ASUSTeK Computer Inc.</b>	
	Tel:	+886-2-2894-3447
	Adresse:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
<b>Autorisierte Niederlassung in Europa:</b>	<b>ASUS Computer GmbH</b>	
	Adresse:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY