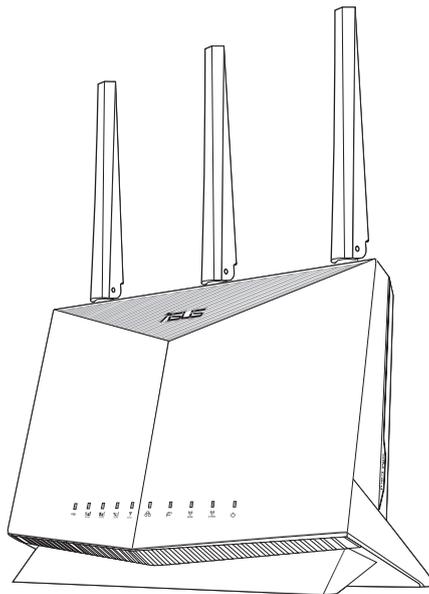


Benutzerhandbuch

4G-AC86U

Wireless-AC2600 Cat.12 LTE Router



ASUS
IN SEARCH OF INCREDIBLE

G18231

Erste Ausgabe

April 2021

Copyright © 2021 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") mit jeglichen Mitteln in jeglicher Form reproduziert, übertragen, transkribiert, in Wiederaufrufsystemen gespeichert oder in jegliche Sprache übersetzt werden, abgesehen von vom Käufer als Sicherungskopie angelegter Dokumentation.

Die Produktgarantie erlischt, wenn (1) das Produkt ohne schriftliche Genehmigung von ASUS repariert, modifiziert oder geändert wird und wenn (2) die Seriennummer des Produkts unkenntlich gemacht wurde oder fehlt.

ASUS BIETET DIESES HANDBUCH IN SEINER VORLIEGENDEN FORM AN, OHNE JEDLICHE GARANTIE, SEI SIE DIREKT ODER INDIREKT, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF INDIREKTE GARANTIEN ODER BEDINGUNGEN BEZÜGLICH DER VERKÄUFLICHKEIT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. IN KEINEM FALL IST ASUS, SEINE DIREKTOREN, LEITENDEN ANGESTELLTEN, ANGESTELLTEN ODER AGENTEN HAFTBAR FÜR JEDLICHE INDIREKTEN, SPEZIELLEN, ZUFÄLLIGEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH SCHÄDEN AUFGRUND VON PROFITVERLUSTEN, GESCHÄFTSVERLUSTEN, NUTZUNGS- ODER DATENVERLUSTEN, UNTERBRECHUNG VON GESCHÄFTSABLÄUFEN ET CETERA), SELBST WENN ASUS VON DER MÖGLICHKEIT SOLCHER SCHÄDEN UNTERRICHTET WURDE, DIE VON DEFEKTEN ODER FEHLERN IN DIESEM HANDBUCH ODER AN DIESEM PRODUKT HERRÜHREN.

DIE TECHNISCHEN DATEN UND INFORMATIONEN IN DIESEM HANDBUCH SIND NUR ZU INFORMATIONSZWECKEN GEDACHT, SIE KÖNNEN JEDERZEIT OHNE VORANKÜNDIGUNG GEÄNDERT WERDEN UND SOLLTEN NICHT ALS VERPFLICHTUNG SEITENS ASUS ANGESEHEN WERDEN. ASUS ÜBERNIMMT KEINE VERANTWORTUNG ODER HAFTUNG FÜR JEDLICHE FEHLER ODER UNGENAUIGKEITEN, DIE IN DIESEM HANDBUCH AUFTRETEN KÖNNTEN, EINSCHLIESSLICH DER DARIN BESCHRIEBENEN PRODUKTE UND SOFTWARE.

In diesem Handbuch erscheinende Produkte und Firmennamen könnten eingetragene Warenzeichen oder Copyrights der betreffenden Firmen sein und dienen ausschließlich zur Identifikation oder Erklärung und zum Vorteil des jeweiligen Eigentümers, ohne Rechtsverletzungen zu beabsichtigen.

Inhaltsverzeichnis

1	Kennenlernen Ihres WLAN-Routers	
1.1	Willkommen!.....	7
1.2	Verpackungsinhalt.....	7
1.3	Ihr WLAN-Router.....	8
1.4	Ihren Router aufstellen.....	10
1.5	Installieren einer Nano-SIM-Karte in Ihren Router.....	11
2	Erste Schritte	
2.1	Router einrichten	12
	A. Kabelverbindung.....	13
	B. Drahtlosverbindung.....	14
2.2	Quick Internet Setup (QIS) mit automatischer Erkennung....	16
3	Allgemeine Einstellungen konfigurieren	
3.1	Netzwerkübersicht verwenden	21
	3.1.1 Einrichten der WLAN-Sicherheitseinstellungen.....	22
	3.1.2 Systemstatus	23
	3.1.3 Verwalten Ihrer Netzwerk-Clients.....	24
	3.1.4 Überwachung des Internetstatus.....	26
	3.1.5 Überwachen der USB-Geräte	27
3.2	Gast-Netzwerk.....	28
3.3	AiProtection.....	30
	3.3.1 Netzwerkschutz.....	31
	3.3.2 Jugendschutzeinstellungen festlegen	35
3.4	Adaptive QoS (Quality of Service)	39
	3.4.1 Bandbreitenüberwachung.....	39
	3.4.2 QoS (Quality of Service)	40
	3.4.3 Webseitenverlauf.....	41

Inhaltsverzeichnis

3.5	Traffic Analyzer	42
3.6	USB-Anwendungen verwenden	43
3.6.1	AiDisk verwenden	43
3.6.2	Servercenter verwenden	46
3.7	AiCloud 2.0 verwenden	51
3.7.1	Cloud-Laufwerk	51
3.7.2	Intelligenter Zugriff	53
3.7.3	Intelligente Synchronisierung	53
3.7.4	Synchronisierungsserver	55
3.7.5	Einstellungen	58
3.8	SMS verwenden	59
3.8.1	Mitteilungen senden	59
3.8.2	Posteingang	60
4	Konfigurieren der erweiterten Einstellungen	
4.1	WLAN	61
4.1.1	Allgemein	61
4.1.2	WPS	63
4.1.3	WDS	65
4.1.4	WLAN-MAC-Filter	67
4.1.5	RADIUS-Einstellungen	68
4.1.6	Professionell	69
4.2	LAN	72
4.2.1	LAN-IP	72
4.2.2	DHCP-Server	73
4.2.3	Route	75
4.2.4	IPTV	76
4.2.5	Switch Control	76

Inhaltsverzeichnis

4.3	WAN	77
4.3.1	Internetverbindung.....	77
4.3.2	IPv6 (Inteneteinstellungen)	85
4.3.3	Dual-WAN	86
4.3.4	Portauslösung.....	88
4.3.5	Virtueller Server/Portweiterleitung.....	90
4.3.6	DMZ.....	93
4.3.7	DDNS	94
4.3.8	NAT-Durchleitung.....	95
4.4	IPv6.....	96
4.5	VPN-Server	97
4.6	Firewall.....	98
4.6.1	Allgemein.....	98
4.6.2	URL-Filter.....	98
4.6.3	Schlüsselwortfilter.....	99
4.6.4	Netzwerkdienstefilter	100
4.6.5	IPv6-Firewall.....	100
4.7	Administration.....	101
4.7.1	Betriebsmodus	101
4.7.2	System.....	102
4.7.3	Aktualisieren der Firmware.....	104
4.7.4	Wiederherstellen/Speichern/Hochladen der Einstellungen.....	105
4.8	Systemprotokoll.....	106
4.9	Liste unterstützter Funktionen für Ethernet, WAN, mobiles Breitband	107
5	Dienstprogramme	
5.1	Device Discovery	109
5.2	Firmware Restoration	110
5.3	Druckerserver einrichten	112
5.3.1	ASUS EZ Printer Sharing.....	112
5.3.2	LPR zur Druckerfreigabe verwenden	115

5.4	Download Master.....	120
5.4.1	Bit Torrent-Download-Einstellungen konfigurieren...	122
5.4.2	NZB Einstellungen.....	123
5.4.3	eMule Einstellungen.....	123

6 Fehlerbehebung

6.1	Allgemeine Problemlösung.....	124
6.2	Häufig gestellte Fragen (FAQs)	127

Anhang

	Hinweise.....	136
	ASUS Kontaktinformation.....	150

1 Kennenlernen Ihres WLAN-Routers

1.1 Willkommen!

Vielen Dank für den Kauf Ihres WLAN-Routers ASUS 4G-AC86U! Der leistungsstarke und elegante 4G-AC86U bietet 2,4-GHz- und 5-GHz-Dual-Band für unübertroffenes gleichzeitiges HD-WLAN-Streamen. Er nutzt SMB-Server, UPnP AV-Server und FTP-Server zum File Sharing rund um die Uhr; hat das Leistungsvermögen zum Bearbeiten von 300.000 Arbeitsvorgängen; und grüne Netzwerktechnologie von ASUS – eine Lösung für bis zu 70% Energieersparnis.

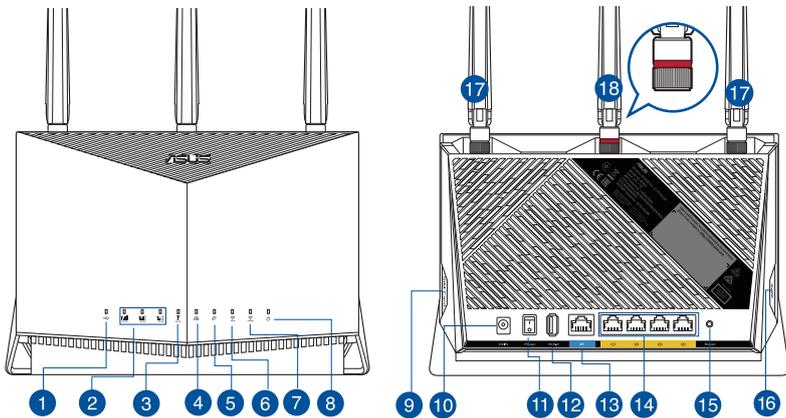
1.2 Verpackungsinhalt

- | | |
|---|---|
| <input checked="" type="checkbox"/> 4G-AC86U WLAN-Router | <input checked="" type="checkbox"/> Netzteil |
| <input checked="" type="checkbox"/> Netzwerkkabel (RJ-45) | <input checked="" type="checkbox"/> Schnellstartanleitung |
| <input checked="" type="checkbox"/> 2 x 3G/4G-Antennen | <input checked="" type="checkbox"/> 1 x WLAN-Antenne
(mit einem roten Kreis) |

HINWEISE:

- Falls Artikel beschädigt oder nicht vorhanden sind, wenden Sie sich für technische Anfragen und Support an Ihren Händler oder 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 Ihr WLAN-Router



-
- 1** USB-LED
Aus: Kein Strom oder keine physische Verbindung.
An: Physische Verbindung mit USB-Geräten.
-
- 2** **3G/4G Signalstärken-LED**
1 beleuchtete LED: Schwaches Signal
2 beleuchtete LEDs: Normales Signal
3 beleuchtete LEDs: Starkes Signal
-
- 3** **LED für mobiles Breitband**
Weiß: 4G-Verbindung ist hergestellt.
Blau: 3G-Verbindung ist hergestellt.
Rot: Keine mobile Breitbandverbindung.
Aus: Keine SIM-Karte erkannt.
-
- 4** **LAN-LED**
Aus: Keine Datenaktivität oder keine physische Verbindung.
An: Ethernetverbindung ist hergestellt.
-
- 5** **WAN-LED (Internet)**
Aus: Keine Datenaktivität oder keine physische Verbindung.
An: Physische Verbindung mit WAN (Wide Area Network).
-
- 6** **5 GHz WLAN-LED**
Aus: Kein 5 GHz-Signal.
An: 5 GHz-WLAN ist bereit.
Blinkend: Datenversand oder -empfang über die WLAN-Verbindung.
-
- 7** **2,4 GHz WLAN-LED**
Aus: Kein 2,4 GHz-Signal.
An: 2,4 GHz-WLAN ist bereit.
Blinkend: Datenversand oder -empfang über die WLAN-Verbindung.
-

-
- 8 Betriebs-LED**
 Aus: Kein Strom.
 An: Gerät ist bereit.
 Langsames Blinken: Rettungsmodus
 Schnelles Blinken: WPS arbeitet.

 - 9 Nano-SIM-Kartensteckplatz**
 Installieren Sie eine Nano-SIM-Karte in diesen Steckplatz, um eine mobile Breitband-Internetverbindung herzustellen.

 - 10 Netzanschluss (DC-In)**
 Verbinden Sie das mitgelieferte Netzteil mit diesem Anschluss und schließen Ihren Router an eine Stromversorgung an.

 - 11 Ein-/Austaste**
 Mit dieser Taste können Sie Ihr System ein-/ausschalten.

 - 12 USB 2.0-Anschluss**
 Verbinden Sie USB 2.0-Geräte wie USB-Festplatten oder -Flashlaufwerke mit diesem Anschluss.

 - 13 WAN-Anschluss (Internet)**
 Verbinden Sie ein Netzkabel mit diesem Anschluss, um eine WAN-Verbindung herzustellen.

 - 14 LAN-Anschlüsse 1~4**
 Verbinden Sie ein Netzkabel mit diesen Anschlüssen, um eine LAN-Verbindung herzustellen.

 - 15 Reset-Taste**
 Mit dieser Taste können Sie das System auf dessen Werkseinstellungen zurücksetzen.

 - 16 WPS-Taste**
 Drücken Sie die Taste lange, um den WPS-Assistenten zu starten.

 - 17 Abnehmbare LTE-Antennen**

 - 18 Abnehmbare WLAN-Antenne**
-

HINWEISE:

- Verwenden Sie nur das mitgelieferte Netzteil. Andere Netzteile könnten das Gerät beschädigen.
 - Stellen Sie sicher, dass Sie die Nano-SIM-Karte in den Kartensteckplatz eingesteckt haben, bevor Sie den Router einschalten.
-

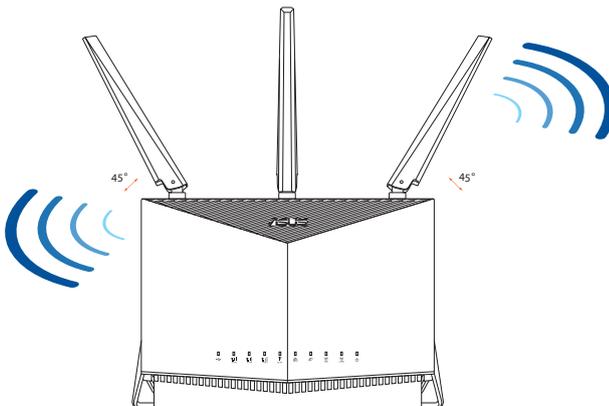
Umgebungsbedingungen:

Netzteil	Gleichstromausgang: +12 V mit 3 A Stromstärke		
Betriebstemperatur	0 ~ 40 °C	Lagertemperatur	-40 ~ 70 °C
Betriebsluftfeuchtigkeit	10 ~ 95%	Lagerluftfeuchtigkeit	5 ~ 95%

1.4 Ihren Router aufstellen

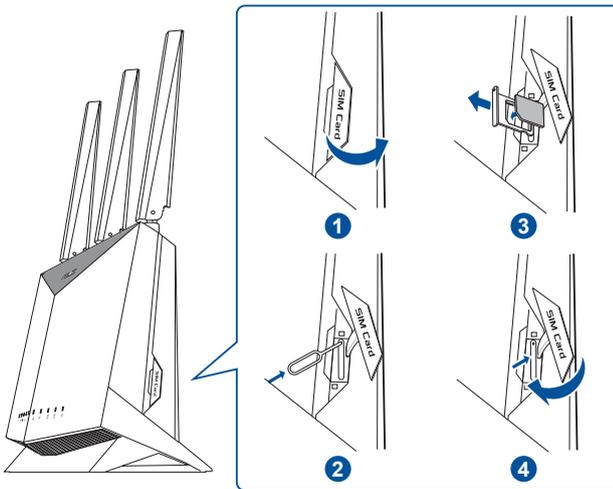
Für beste Funksignalübertragung zwischen dem WLAN-Router und damit verbundenen Netzwerkgeräten sollten Sie Folgendes beachten:

- Platzieren Sie den WLAN-Router in einem zentralen Bereich, um eine maximale WLAN-Reichweite für die Netzwerkgeräte zu erzielen.
- Halten Sie den WLAN-Router entfernt von metallischen Hindernissen und direktem Sonnenlicht.
- Halten Sie den WLAN-Router entfernt von nur 802.11g oder nur 20 MHz WLAN-Geräten, 2,4 GHz Computer-Peripheriegeräten, Bluetooth-Geräten, schnurlosen Telefonen, Transformatoren, Hochleistungsmotoren, fluoreszierendem Licht, Mikrowellenherden, Kühlschränken und anderen gewerblichen Geräten, um Signalstörungen oder Signalverlust zu verhindern.
- Aktualisieren Sie immer auf die neueste Firmware. Besuchen Sie die ASUS-Webseite unter <http://www.asus.com>, um die neuesten Firmware-Aktualisierungen zu erhalten.
- Richten Sie die Antennen wie in der folgenden Abbildung gezeigt aus.



1.5 Installieren einer Nano-SIM-Karte in Ihren Router

1. Entfernen Sie die Abdeckung vom Nano-SIM-Kartensteckplatz auf der rechten Seite Ihres Routers.
2. Stecken Sie eine Nadel in die Öffnung am Nano-SIM-Kartensteckplatz, um das Kartenfach auszuwerfen.
3. Legen Sie eine Nano-SIM-Karte in das Kartenfach ein.
4. Schieben Sie das Kartenfach zu, um es zu schließen.



2 Erste Schritte

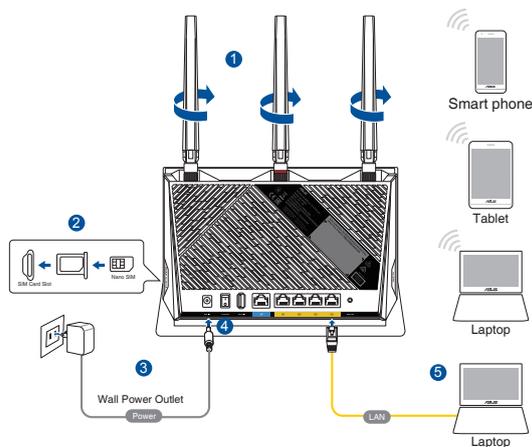
2.1 Router einrichten

WICHTIG!

- Nutzen Sie zur Einrichtung Ihres WLAN-Routers eine Kabelverbindung, damit die Einrichtung problemlos vonstatten geht.
- Wenn Sie den Standort Ihres nächstgelegenen Mobilfunkmasts genau bestimmen, können Sie das stärkste Signal finden.
- Der Standardbenutzername und das Kennwort für die Web-Benutzeroberfläche lauten **admin** und **admin**.

HINWEISE:

- Die LED für das mobile Breitband leuchtet, nachdem Sie Ihren Router mit einer installierten Nano-SIM-Karte eingeschaltet haben.
- Stellen Sie sicher, dass die LED für das mobile Breitband leuchtet, bevor Sie Ihren Router über den QIS-Assistenten (Quick Internet Setup Wizard) einrichten.
- Sie können für den Internetzugang entweder mobiles Breitband oder Ethernet-WAN verwenden.
- Die automatische Erkennung des Verbindungstyps erfolgt bei der erstmaligen Konfiguration Ihres mobilen Breitband-Routers oder bei Rücksetzung Ihres Routers auf seine Standardeinstellungen. Während des QIS (Quick Internet Setup)-Vorgangs müssen Sie möglicherweise den PIN-Code der SIM-Karte eingeben und die APN-Daten (Interneteinstellungen) bereitstellen, die Sie von Ihrem Internetanbieter erhalten haben.



A. Kabelverbindung

So richten Sie Ihren WLAN-Router über eine Kabelverbindung ein:

1. Verbinden Sie zwei 3G/4G-Antennen jeweils mit dem linken und rechten Anschluss und die WLAN-Antenne mit dem Anschluss in der Mitte.
2. Legen Sie eine Nano-SIM-Karte in den Nano-SIM-Kartensteckplatz ein.
3. Schließen Sie das Netzteil Ihres Routers an den Netzanschluss (DC-In) und eine Steckdose an.
4. Drücken Sie den Ein-/Ausshalter, um Ihren mobilen Breitband-Router einzuschalten, und warten Sie einige Minuten, bis die Internetverbindung hergestellt ist.
5. Schließen Sie Ihren Computer über ein Ethernet-Kabel an den Router an.
6. Richten Sie Ihren Router über den QIS-Assistenten (Quick Internet Setup Wizard) ein, nachdem die LED für das mobile Breitband ∇ leuchtet.
 - a. Öffnen Sie einen Webbrowser und geben Sie <http://router.asus.com> ein, um die Web-Benutzeroberfläche aufzurufen. Befolgen Sie die Bildschirmanweisungen, um die Einrichtung fertigzustellen.
 - b. Sie können auch die ASUS Router App zum Einrichten Ihres Routers wählen. Laden Sie die ASUS Router App zum Einrichten Ihres Routers über Ihr Mobilgerät herunter.
7. Richten Sie ein Kennwort für Ihren Router ein, um unbefugten Zugriff zu verhindern.

Login Information Setup

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name

New Password

Retype Password Show password



ASUS
Router

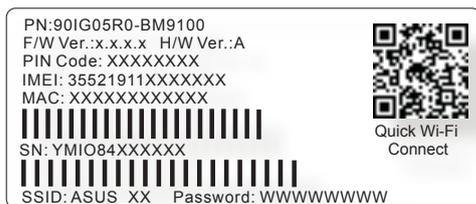


ASUS Router

B. Drahtlosverbindung

So richten Sie Ihren WLAN-Router über eine WLAN-Verbindung ein:

1. Verbinden Sie zwei 3G/4G-Antennen jeweils mit dem linken und rechten Anschluss und die WLAN-Antenne mit dem Anschluss in der Mitte.
2. Legen Sie eine Nano-SIM-Karte in den Nano-SIM-Kartensteckplatz ein.
3. Schließen Sie das Netzteil Ihres Routers an den Netzanschluss (DC-In) und eine Steckdose an.
4. Drücken Sie den Ein-/Ausshalter, um Ihren mobilen Breitband-Router einzuschalten, und warten Sie einige Minuten, bis die Internetverbindung hergestellt ist.
5. Verbinden Sie sich mit dem WLAN mit der SSID, die auf dem Produktaufkleber auf der Rückseite des Routers angegeben ist. Sie können sich verbinden, indem Sie die SSID-Liste durchsuchen oder den QR-Code scannen, um schnell eine Verbindung herzustellen.



- * **XX** bezieht sich auf die letzten zwei Ziffern der 2,4-GHz-MAC-Adresse. Sie finden sie auf dem Etikett auf der Rückseite Ihres Routers.
6. Richten Sie Ihren Router über den QIS-Assistenten (Quick Internet Setup Wizard) ein, nachdem die LED für das mobile Breitband ∇ leuchtet.
 - a. Öffnen Sie einen Webbrowser und geben Sie <http://router.asus.com> ein, um die Web-Benutzeroberfläche aufzurufen. Befolgen Sie die Bildschirmanweisungen, um die Einrichtung fertigzustellen.
 - b. Sie können auch die ASUS Router App zum Einrichten Ihres Routers wählen. Laden Sie die ASUS Router App zum Einrichten Ihres Routers über Ihr Mobilgerät herunter.
 7. Richten Sie ein Kennwort für Ihren Router ein, um unbefugten Zugriff zu verhindern.

HINWEISE:

- Für Details zur Verbindung zu einem WLAN beziehen Sie sich auf das Handbuch Ihres WLAN-Adapters.
 - Zur Einrichtung der Sicherheitseinstellungen für Ihr Netzwerk beziehen Sie sich auf den Abschnitt **3.1.1 Einrichten der WLAN-Sicherheitseinstellungen** in diesem Benutzerhandbuch.
-

Login Information Setup

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name	<input type="text" value="admin"/>
New Password	<input type="password"/>
Retype Password	<input type="password"/> <input type="checkbox"/> Show password



ASUS
Router



GET IT ON
Google Play



Download on the
App Store

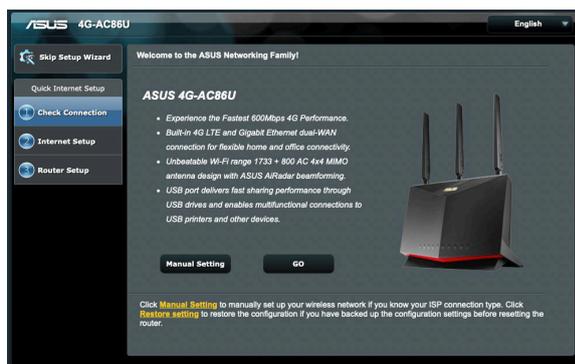
2.2 Quick Internet Setup (QIS) mit automatischer Erkennung

So richten Sie Ihren Router mithilfe von QIS (Quick Internet Setup) ein:

1. Achten Sie darauf, dass die folgenden LEDs leuchten:
 - Betriebs-LED
 - 2,4 GHz WLAN-LED
 - LED für WAN oder mobiles Breitband
 - 5 GHz WLAN-LED
2. Starten Sie Ihren Webbrowser, wie Internet Explorer, Firefox, Google Chrome oder Safari.

HINWEIS: Falls QIS nicht automatisch startet, geben Sie <http://router.asus.com> in die Adresszeile ein und aktualisieren Sie nochmals den Browser.

3. Melden Sie sich auf der Web-Benutzeroberfläche an. Die QIS-Seite wird automatisch gestartet. Standardmäßig lauten der Benutzername und das Kennwort für die Anmeldung auf der Web-Benutzeroberfläche Ihres Routers jeweils "admin".



4. Vergeben Sie den Benutzernamen und das Kennwort für die Routeranmeldung und klicken Sie auf **Next (Weiter)**. Sie benötigen den Benutzernamen und das Kennwort zur Anmeldung am ASUS Router, um die Routereinstellungen anzuzeigen oder zu ändern. Sie können sich Ihren Benutzernamen und Ihr Kennwort zum zukünftigen Gebrauch notieren.

Change the router login password

4G-AC86U is currently not protected and uses an unsafe default username and password. Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name

New password

Retype password

Modify

5. Wenn der WAN-Anschluss aktiv ist, erkennt die Quick Internet Setup (QIS)-Funktion des WLAN-Routers automatisch, ob Ihr Internetverbindungstyp **Dynamic IP (Dynamische IP)**, **PPPoE**, **PPTP**, **L2TP** oder **Static IP (Feste IP)** ist. Bitte beziehen Sie die notwendigen Informationen von Ihrem Internetanbieter. Wenn Ihr Verbindungstyp Dynamic IP (Dynamische IP) (DHCP) ist, leitet Sie der QIS-Assistent automatisch zum nächsten Schritt.

Für automatische IP (DHCP)

Back main page

Quick Internet Setup

Check Connection

Internet Setup

Router Setup

Automatic IP connection setup

Host Name(optional):

MAC Address(optional) **MAC Clone**

MAC (Media Access Control) address is a unique identifier that identifies your computer or device in the network. ISPs monitor the MAC addresses of devices that connect to their services, and would disallow Internet connection for new MAC addresses. To fix this issue, you can do either of the following:

- Contact your ISP and request to update the MAC address associated with your ISP subscription. Once this is done, you can run the router's setup wizard again.
- Clone or change the MAC address of the new device to match the MAC address of the original device. If you just replaced an old router, you will find the old router's MAC address from its label. If you previously connected your computer to the modem, you will need to enter your computer's MAC address or click "MAC Clone" to clone your computer's MAC address.

Previous Next

Für PPPoE, PPTP und L2TP

The screenshot shows the 'Internet Setup' step of a configuration wizard. On the left, a sidebar contains 'Skip Setup Wizard', 'Quick Internet Setup', 'Check Connection', 'Internet Setup' (highlighted), and 'Router Setup'. The main area is titled 'Please refer to your ISP setting, and input the related information.' It features a radio button for 'Connect to DNS Server automatically' with 'Yes' selected. Below are two input fields for 'DNS Server1' and 'DNS Server2'. At the bottom are 'Previous' and 'Next' buttons.

Für feste IP

The screenshot shows the 'Account Settings' screen. It has a sidebar with 'Skip Setup Wizard', 'Quick Internet Setup', 'Check Connection', 'Internet Setup' (highlighted), and 'Router Setup'. The main area is titled 'Account Settings' and contains input fields for 'User Name', 'Password', and 'MAC Address(optional)'. There is a 'Show password' checkbox and a 'MAC Clone' button. Below the fields is the text 'Obtain the account name and password from your ISP.' and 'Previous' and 'Next' buttons.

6. Wenn eine Verbindung mit einem 3G/4G-Netzwerk besteht, erkennt und übernimmt die Quick Internet Setup (QIS)-Funktion des WLAN-Routers automatisch die APN-Einstellung, um eine Verbindung zur WLAN-Basisstation herzustellen. Falls der QIS-Assistent beim automatischen Übernehmen der APN-Einstellung einen Fehler anzeigt oder für die SIM-Karte nach einem PIN-Code gefragt wird, richten Sie die APN-Einstellung manuell ein.

HINWEIS: Der PIN-Code kann je nach Anbieter variieren.

The screenshot shows the 'Detecting your connection type' screen. It has a sidebar with 'Skip Setup Wizard', 'Quick Internet Setup', 'Check Connection' (highlighted), 'Internet Setup', and 'Router Setup'. The main area is titled 'Detecting your connection type' and contains the text 'Please input the PIN code obtained from the Internet service provider.' Below is an input field for 'PIN code' with a 'Save My PIN' checkbox. It also shows 'Remaining Attempts: 3' and an 'OK' button.



7. Das Konfigurationsergebnis der Dual-WAN-Verbindung wird angezeigt. Klicken Sie zum Fortfahren auf **Weiter**.

Die mobile Breitbandverbindung wurde erfolgreich konfiguriert



Die Ethernet-WAN-Verbindung wurde erfolgreich konfiguriert



8. Wenn beide WANs konfiguriert sind, gehen Sie zum nächsten Schritt, um die WLAN-Einstellungen zu konfigurieren.

Wireless Setting

Do you want to use the previous wireless security settings? Yes No

Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.

2.4 GHz - Security

Network Name (SSID)

Password

5 GHz - Security

Network Name (SSID)

Password

Enter a network key between 8 and 63 characters(letters, numbers or a combination) or 64 hex digits. The default wireless security setting is WPA2-Personal - AES. If you do not want to set the network security, leave the security key field blank, but this exposes your network to unauthorized access.

Apply

9. Weisen Sie den Netzwerknamen (SSID) und Sicherheitsschlüssel für Ihre 2,4 GHz WLAN-Verbindung zu. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.
10. Ihre Internet- und WLAN-Einstellungen werden angezeigt. Klicken Sie auf **Next (Weiter)**, um den QIS-Vorgang abzuschließen.

ASUS 4G-AC88U English

Skip Setup Wizard

Quick Internet Setup

Check Connection

Internet Setup

Router Setup

Completed Network Configuration Summary

WAN		
WAN Connection Type	Mobile Broadband	Automatic IP
Status	Standby	Active
WAN IP	0.0.0.0	192.168.2.102
Wireless		
Band	2.4GHz	5GHz
Network Name (SSID)	ASUS_80	ASUS_80
Network Key	brown_4739	brown_4739
Wireless Security	WPA2-Personal - AES	WPA2-Personal - AES
LAN		
LAN IP	192.168.50.1	
MAC address	F0:2F:74:3A:D6:80	

Complete

11. Die LED für die 3G/4G-Signalstärke leuchtet dauerhaft, nachdem die Einrichtung der Einstellungen für das 3G/4G-Netzwerk über QIS abgeschlossen ist und die Internetverbindung erfolgreich hergestellt wurde.

3 Allgemeine Einstellungen konfigurieren

3.1 Netzwerkübersicht verwenden

Network Map (Netzwerkübersicht) ermöglicht Ihnen, den Internetverbindungsstatus zu überprüfen, die Sicherheitseinstellungen Ihres Netzwerks zu konfigurieren, Ihre Netzwerk-Clients zu verwalten und Ihre USB-Geräte zu überwachen.



3.1.1 Einrichten der WLAN-Sicherheitseinstellungen

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

So richten Sie die WLAN-Sicherheitseinstellungen ein:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Network Map (Netzwerkübersicht)**.
2. Klicken Sie im Netzwerkübersicht-Bildschirm auf das Systemstatussymbol . Sie können die WLAN-Sicherheitseinstellungen konfigurieren, z. B. **WLAN-Name (SSID)**, **Authentifizierungsverfahren** und **Verschlüsselungseinstellungen**.

Sicherheitseinstellungen für 2,4 GHz



The screenshot shows the 'System Status' screen for the 2.4GHz band. At the top, there are three tabs: '2.4GHz', '5GHz', and 'Status', with '2.4GHz' selected. The main content area is divided into several sections: 'Network Name (SSID)' with a text field containing 'ASUS_80'; 'Authentication Method' with a dropdown menu set to 'WPA2-Personal'; 'WPA Encryption' with a dropdown menu set to 'AES'; and 'WPA-PSK key' with a text field containing ten asterisks. Below these fields is an 'Apply' button. At the bottom of the screen, there are four more sections: 'LAN IP' (192.168.50.1), 'PIN code' (31257367), 'Yandex.DNS' (Disabled), and 'LAN MAC address' (F0:2F:74:3A:D6:80). A 'Wireless 2.4GHz MAC address' section is also present at the very bottom with the address F0:2F:74:3A:D6:80.

Sicherheitseinstellungen für 5 GHz



The screenshot shows the 'System Status' screen for the 5GHz band. At the top, there are three tabs: '2.4GHz', '5GHz', and 'Status', with '5GHz' selected. The main content area is divided into several sections: 'Network Name (SSID)' with a text field containing 'ASUS_80'; 'Authentication Method' with a dropdown menu set to 'WPA2-Personal'; 'WPA Encryption' with a dropdown menu set to 'AES'; and 'WPA-PSK key' with a text field containing ten asterisks. Below these fields is an 'Apply' button. At the bottom of the screen, there are four more sections: 'LAN IP' (192.168.50.1), 'PIN code' (31257367), 'Yandex.DNS' (Disabled), and 'LAN MAC address' (F0:2F:74:3A:D6:80). A 'Wireless 5GHz MAC address' section is also present at the very bottom with the address F0:2F:74:3A:D6:84.

3. Geben Sie im Feld **Wireless name (SSID) (WLAN-Name, SSID)** Ihrem WLAN einen eindeutigen Namen.
4. Wählen Sie aus der **Authentication Method (Authentifizierungsverfahren)**-Auswahlliste das Authentifizierungsverfahren für Ihr WLAN aus.

Falls Sie **WPA-Personal** oder **WPA-2 Personal** als Authentifizierungsverfahren wählen, geben Sie den WPA-PSK-Schlüssel oder das Sicherheitskennwort ein.

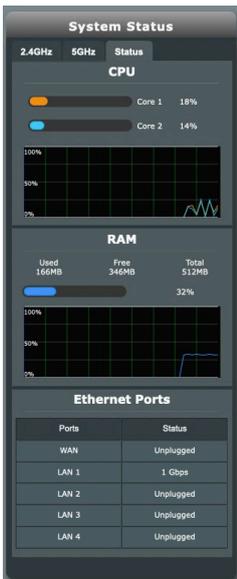
WICHTIG! Der IEEE 802.11n/ac-Standard erkennt die Verwendung eines niedrigen Durchsatzes mit WEP oder WPA-TKIP als Unicast-Chiffrierung nicht an. Falls Sie diese Verschlüsselungsverfahren verwenden, wird Ihre Datenrate auf die IEEE 802.11g 54Mb/s-Verbindung heruntergestuft.

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

3.1.2 Systemstatus

So überwachen Sie die Systemressourcen:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Network Map (Netzwerkübersicht)**.
2. Klicken Sie im Netzwerkübersicht-Bildschirm auf das Systemstatussymbol . Hier finden Sie die Informationen zur CPU- und Speicherauslastung.



3.1.3 Verwalten Ihrer Netzwerk-Clients

So verwalten Sie Ihre Netzwerk-Clients:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Network Map (Netzwerkübersicht)**.
2. Wählen Sie im Netzwerkübersicht-Bildschirm das Client-Statussymbol , um die Informationen Ihrer Netzwerk-Clients anzuzeigen.



3. Klicken Sie in der Client-Statustabelle auf das Gerätesymbol , um das ausführliche Profil des Geräts anzuzeigen.



The screenshot displays a dark-themed user interface for a network management system. At the top left, there are two tabs: "DHCP" and "Logged-in User". A blue icon of a laptop is visible in the top right corner. The main content area shows a profile for a device named "MacBook-Air-M1". To the left of the profile is a placeholder icon of a laptop. The profile details are as follows:

Name	MacBook-Air-M1
IP	192.168.50.209
MAC	00:E0:4C:68:01:A2
Device	REALTEK SEMICONDUCTOR CORP.

Below the profile details, there are two toggle switches:

- Block Internet Access**: OFF
- Time Scheduling**: OFF

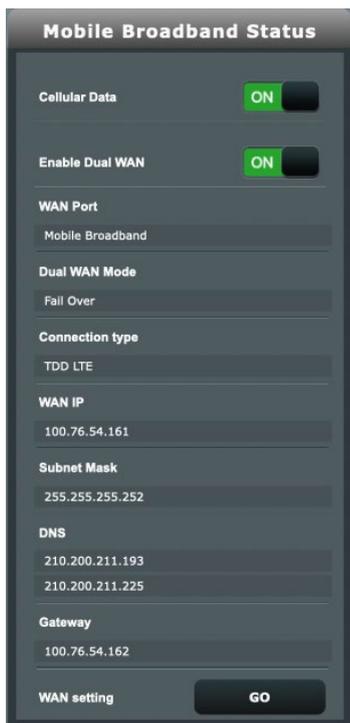
At the bottom left of the profile section, there are two links: [Default](#) and [Change](#).

3.1.4 Überwachung des Internetstatus

So überwachen Sie Ihren Internetstatus:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Network Map (Netzwerkübersicht)**.
2. Wählen Sie im Netzwerkübersicht-Bildschirm das Internetsymbol , um Ihre Internetkonfiguration anzuzeigen. Sie können auch das Symbol für das mobile Breitband  auswählen, um die Konfiguration des mobilen Breitbands anzuzeigen.
3. Um die WAN-Schnittstelle in Ihrem Netzwerk zu deaktivieren, klicken Sie auf die **Switch (Wechsel)**-Schaltfläche bei **Cellular Data (Mobilfunkdaten)** und **Internet Connection (Internetverbindung)**.

Mobiles Breitband



Mobile Broadband Status

Cellular Data

Enable Dual WAN

WAN Port
Mobile Broadband

Dual WAN Mode
Fail Over

Connection type
TDD LTE

WAN IP
100.76.54.161

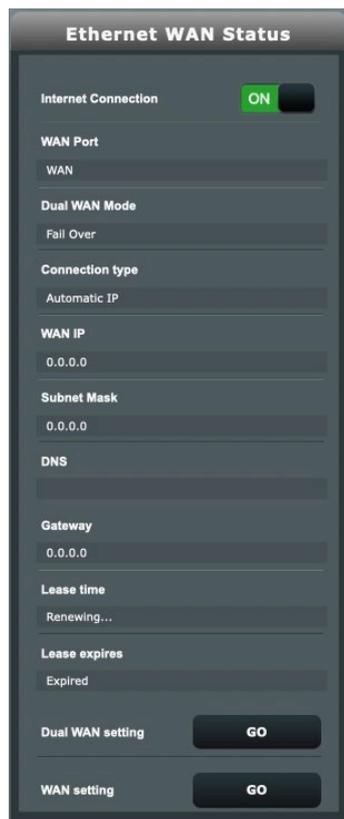
Subnet Mask
255.255.255.252

DNS
210.200.211.193
210.200.211.225

Gateway
100.76.54.162

WAN setting

Ethernet-WAN



Ethernet WAN Status

Internet Connection

WAN Port
WAN

Dual WAN Mode
Fail Over

Connection type
Automatic IP

WAN IP
0.0.0.0

Subnet Mask
0.0.0.0

DNS

Gateway
0.0.0.0

Lease time
Renewing...

Lease expires
Expired

Dual WAN setting

WAN setting

3.1.5 Überwachen der USB-Geräte

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

So überwachen Sie die USB-Geräte:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Network Map (Netzwerkübersicht)**.
2. Wählen Sie im Netzwerkübersicht-Bildschirm das USB-Laufwerksstatussymbol , um Informationen über Ihre USB-Geräte anzuzeigen.
3. Klicken Sie im **Media Server (Medienserver)**-Feld auf **GO (Los)**, um einen iTunes- und DLNA-Server für die lokale Freigabe von Mediendateien einzurichten.

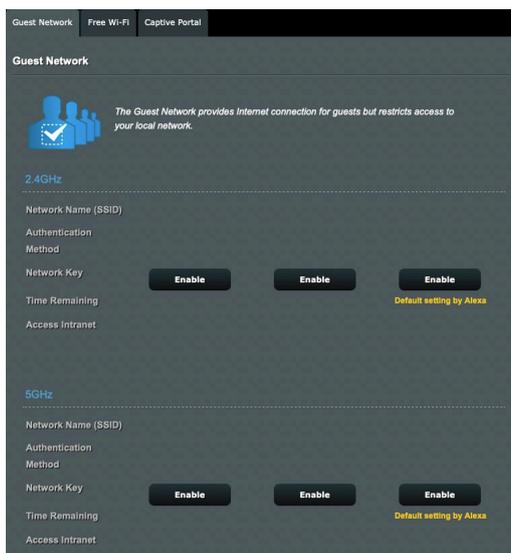
HINWEIS: Der WLAN-Router funktioniert mit den meisten USB Festplatten/Flashlaufwerken (bis zu 2 TB Größe) und unterstützt Lese-/Schreibzugriff für FAT16, FAT32, EXT2, EXT3 und NTFS.

4. Klicken Sie im Feld **AiDisk Wizard (AiDisk-Assistent)** auf **GO (Los)**, um einen FTP-Server für die Dateifreigabe im Internet einzurichten.
5. Um einen USB-Datenträger von der USB-Schnittstelle zu entfernen, klicken Sie auf die **Remove (Entfernen)**-Schaltfläche im **Safely Remove disk (Datenträger sicher entfernen)**-Feld. Wenn das USB-Laufwerk erfolgreich ausgeworfen wurde, wird als USB-Status **Unmounted (Getrennt)** angezeigt.



3.2 Gast-Netzwerk

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



So erstellen Sie ein Gästernetzwerk:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Guest Network (Gästernetzwerk)**.
2. Wählen Sie im **Gastnetzwerk**-Bildschirm das 2,4-GHz- oder 5-GHz-Frequenzband für das zu erstellende Gastnetzwerk.
3. Klicken Sie auf **Enable (Aktivieren)**.
4. Konfigurieren Sie im Popup-Bildschirm die Gasteinstellungen
5. Weisen Sie einen Netzwerknamen (SSID) zu, um Ihr Gastnetzwerk zu identifizieren.
6. Wählen Sie ein Authentifizierungsverfahren.
7. Wenn Sie ein WPA-Authentifizierungsverfahren auswählen, wählen Sie die WPA-Verschlüsselung.
8. Legen Sie die **Access time (Zugriffszeitdauer)** fest oder wählen Sie **Limitless (Unbegrenzt)**.

9. Wählen Sie **Disable (Deaktivieren)** oder **Enable (Aktivieren)** für das Element **Access Intranet (Auf Intranet zugreifen)**.
10. Wählen Sie **Disable (Deaktivieren)** oder **Enable (Aktivieren)** beim **Enable MAC Filter (MAC-Filter aktivieren)**-Element für Ihr Gastnetzwerk.

Guest Network	
Guest Network Index	1
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Network Name (SSID)	ASUS_80_2G_Guest
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	brown_4739
Access time	<input checked="" type="radio"/> 0 days 0 hour(s) 0 minute(s) <input type="radio"/> Unlimited access
Bandwidth Limiter	<input checked="" type="radio"/> Yes <input type="radio"/> No
Access Intranet	Disable
Enable MAC Filter	Disable

Cancel Apply

11. Klicken Sie zum Abschluss auf **Übernehmen**.

HINWEISE:

- Besuchen Sie <https://www.asus.com/support/FAQ/1034977/>, um **Wie Sie das firmeneigene Portal einrichten** zu finden.
 - Besuchen Sie <https://www.asus.com/support/FAQ/1034971/>, um **Wie Sie Free Wi-Fi einrichten** zu finden.
-

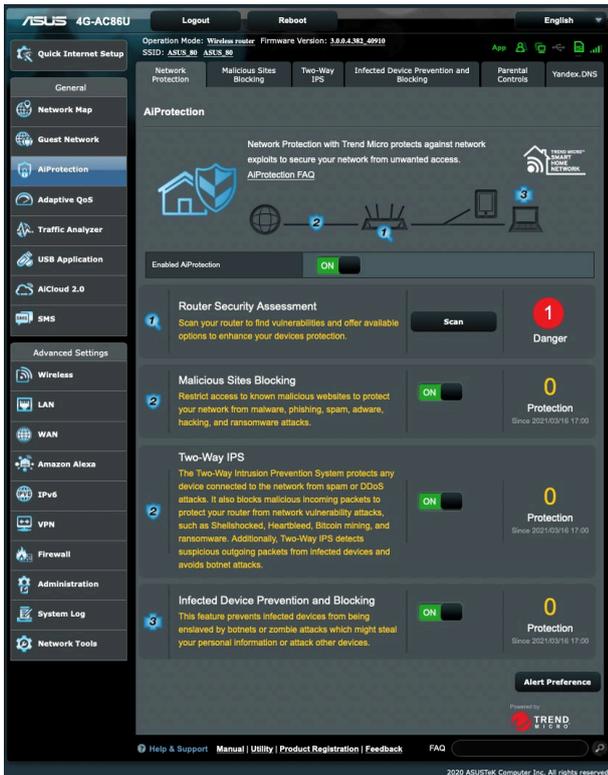
3.3 AiProtection

AiProtection bietet Echtzeitüberwachung, wodurch Malware, Spyware und unbefugter Zugriff erkannt werden. Außerdem werden unerwünschte Webseiten und Apps herausgefiltert und es ist möglich, einen Zeitpunkt festzulegen, ab dem ein verbundenes Gerät auf das Internet zugreifen kann.



3.3.1 Netzwerkschutz

Der Netzwerkschutz verhindert Netzwerk-Exploits und schützt Ihr Netzwerk vor unbefugtem Zugriff.

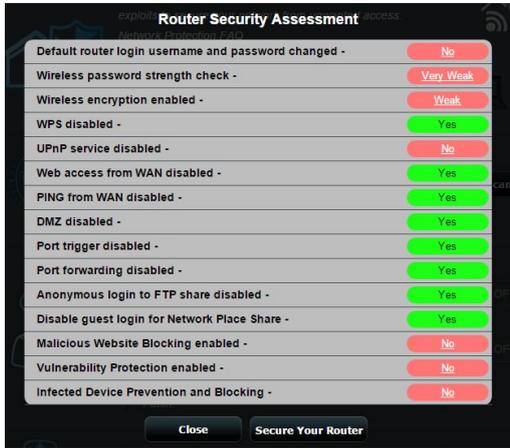


Netzwerkschutz konfigurieren

So konfigurieren Sie den Netzwerkschutz:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein)** > **AiProtection**.
2. Klicken Sie in der **AiProtection**-Hauptseite auf **Network Protection (Netzwerkschutz)**.
3. Im Register **Network Protection (Netzwerkschutz)** klicken Sie auf **Scan (Prüfen)**.

Wenn die Prüfung abgeschlossen ist, zeigt das Dienstprogramm die Ergebnisse auf der Seite **Router Security Assessment (Router Sicherheitsauswertung)** an.



WICHTIG! Mit **Yes (Ja)** markierte Elemente auf der Seite **Router Security Assessment (Router Sicherheitsauswertung)** befinden sich im Status **sicher**. Für mit **No (Nein)**, **Weak (Schwach)** oder **Very Weak (Sehr schwach)** markierte Elemente wird dringend empfohlen, diese ordnungsgemäß zu konfigurieren.

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

HINWEIS: Wenn Sie auf ein Element klicken, leitet Sie das Dienstprogramm zur Einstellungsseite des Elements weiter.

- b. Konfigurieren Sie auf der Seite die Sicherheitseinstellungen des Elements und nehmen Sie die erforderlichen Änderungen vor. Klicken Sie, wenn Sie fertig sind, auf **Apply (Übernehmen)**.
 - c. Gehen Sie zurück zur Seite **Router Security Assessment (Router Sicherheitsauswertung)** und klicken Sie auf **Close (Schließen)**, um die Seite zu verlassen.
5. Um die Sicherheitseinstellungen automatisch zu konfigurieren, klicken Sie auf **Secure Your Router (Machen Sie Ihren Router sicher)**.
6. Wenn eine Aufforderung angezeigt wird, klicken Sie auf **OK**.

Blockieren schädlicher Webseiten

Diese Funktion verhindert den Zugriff auf bekannte schädliche Webseiten aus der Cloud-Datenbank für einen Schutz, der immer auf dem neuesten Stand ist.

HINWEIS: Diese Funktion wird automatisch aktiviert, wenn Sie den **Router Weakness Scan (Routerprüfung auf Schwachstellen)** ausführen.

So aktivieren Sie das Blockieren schädlicher Webseiten:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > AiProtection**.
2. Klicken Sie in der **AiProtection**-Hauptseite auf **Network Protection (Netzwerkschutz)**.
3. Klicken Sie im Feld **Malicious Sites Blocking (Blockieren schädlicher Webseiten)** auf **ON (EIN)**.

Schutz vor Sicherheitsrisiken

Diese Funktion löst gängige Exploits in der Router-Konfiguration.

HINWEIS: Diese Funktion wird automatisch aktiviert, wenn Sie den **Router Weakness Scan (Routerprüfung auf Schwachstellen)** ausführen.

So aktivieren Sie den Schutz vor Sicherheitsrisiken:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > AiProtection**.
2. Klicken Sie in der **AiProtection**-Hauptseite auf **Network Protection (Netzwerkschutz)**.
3. Klicken Sie im Feld **Vulnerability protection (Schutz vor Sicherheitsrisiken)** auf **ON (EIN)**.

Blockieren und Bewahrung vor infizierten Geräten

Diese Funktion verhindert, dass infizierte Geräte persönliche Informationen oder den infizierten Zustand an externe Geräte weitergeben.

HINWEIS: Diese Funktion wird automatisch aktiviert, wenn Sie den **Router Weakness Scan (Routerprüfung auf Schwachstellen)** ausführen.

So aktivieren Sie Infected Device Prevention and Blocking (Blockieren und Bewahrung vor infizierten Geräten):

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > AiProtection**.
2. Klicken Sie in der **AiProtection**-Hauptseite auf **Network Protection (Netzwerkschutz)**.
3. Klicken Sie im Feld **Infected Device Prevention and Blocking (Blockieren und Bewahrung vor infizierten Geräten)** auf **ON (EIN)**.

So konfigurieren Sie die Alarmpräferenz:

1. Klicken Sie im Feld **Infected Device Prevention and Blocking (Blockieren und Bewahrung vor infizierten Geräten)** auf **Alert Preference (Alarmpräferenz)**.
2. Wählen Sie oder geben Sie den Email-Anbieter, das Email-Konto und das Kennwort ein, klicken Sie dann auf **Apply (Übernehmen)**.

3.3.2 Jugendschutzeinstellungen festlegen

Mit den Jugendschutzeinstellungen können Sie die Zugangszeit zum Internet kontrollieren oder ein Zeitlimit für die Netzwerknutzung eines Clients festlegen.

So wechseln Sie zur Hauptseite der Jugendschutzeinstellungen:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein)** > **AiProtection**.
2. Klicken Sie in der **AiProtection**-Hauptseite auf das **Parental Controls (Jugendschutzeinstellungen)**-Register.

The screenshot shows the ASUS AiProtection configuration interface for a 4G-AC86U router. The page is titled "AiProtection - Web & Apps Filters" and includes a navigation sidebar on the left with options like General, Network Map, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer, USB Application, AiCloud 2.0, SMS, Advanced Settings, Wireless, LAN, WAN, Amazon Alexa, IPv6, VPN, Firewall, Administration, System Log, and Network Tools. The main content area is divided into several sections:

- Web & Apps Filters:** A toggle switch is currently set to "ON".
- Client List (Max Limit: 16):** A table with columns for Client Name (MAC Address) and Content Category. One client is listed with the MAC address "08:00:27:2A:5A:26:80".
- Content Category:** A list of categories with checkboxes and descriptions:
 - Adult:** Block adult/mature content to prevent children from viewing sites that contain material of a sexual, violent, and illegal nature.
 - Instant Message and Communication:** Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.
 - P2P and File Transfer:** By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.
 - Streaming and Entertainment:** By blocking streaming and entertainment services you can limit the time your children spend online.

At the bottom of the table, it says "No data in table." and there is an "Apply" button. The footer includes links for Help & Support, Manual, Utility, Product Registration, Feedback, and FAQ, along with the TRENDnet logo and the text "© 2020 ASUSTek Computer Inc. All rights reserved."

Web- und App-Filter

Web- und App-Filter ist eine Funktion der **Parental Controls (Jugendschutzeinstellungen)**, die es Ihnen ermöglicht, den Zugriff auf unerwünschte Webseiten oder Anwendungen zu sperren.

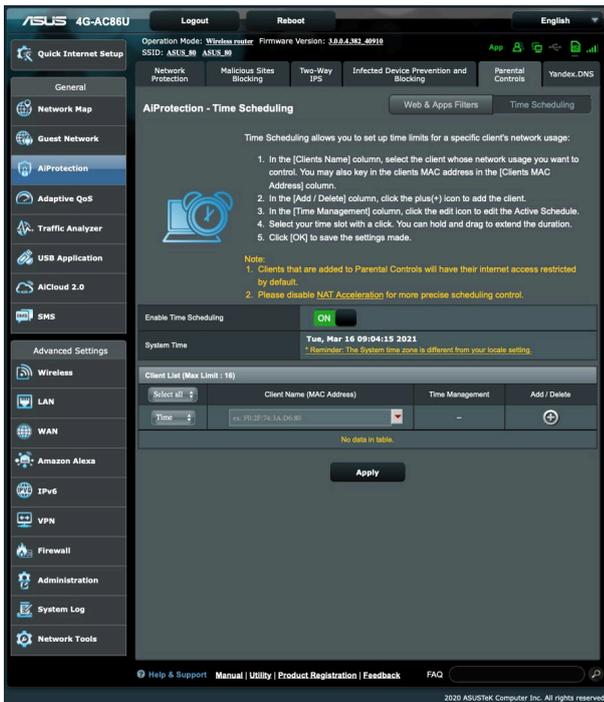
So konfigurieren Sie den Web- und App-Filter:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > AiProtection**.
2. Klicken Sie in der **AiProtection**-Hauptseite auf das **Parental Controls (Jugendschutzeinstellungen)**-Symbol, um zum entsprechenden Register zu gelangen.
3. Klicken Sie im Feld **Web & Apps Filters (Web- und App-Filter)** auf **ON (EIN)**.
4. Wenn die Endnutzer-Lizenzvertrag (EULA)-Aufforderung angezeigt wird, klicken Sie zum Fortfahren auf **I agree (Ich stimme zu)**.
5. In der Spalte **Client List (Client-Liste)** wählen Sie oder geben Sie den Namen des Clients in der Dropdown-Liste ein.
6. Wählen Sie aus der Spalte **Content Category (Inhaltskategorie)** die Filter aus den vier Hauptkategorien aus: **Erwachsener, Instant Messaging und Kommunikation, P2P und Dateiübertragung** und **Streaming und Unterhaltung**.
7. Klicken Sie auf , um das Client-Profil hinzuzufügen.
8. Klicken Sie auf **Apply (Übernehmen)**, um die Einstellungen zu speichern.

Zeitfestlegung

Die Zeitfestlegung ermöglicht es Ihnen, ein Zeitlimit für die Netzwerknutzung eines Clients zu bestimmen.

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



So konfigurieren Sie die Zeitfestlegung:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > AiProtection > Parental Controls (Jugendschutzeinstellungen) > Time Scheduling (Zeitfestlegung)**.
2. Klicken Sie im Feld **Enable Time Scheduling (Zeitfestlegung aktivieren)** auf **ON (EIN)**.
3. In der Spalte **Client Name (MAC Address) (Client-Name (MAC-Adresse))** wählen Sie oder geben Sie den Namen des Clients in der Dropdown-Liste ein.

HINWEIS: Sie können auch in der **Client Name (MAC Address) (Client-Name (MAC-Adresse))**-Spalte die MAC-Adresse des Clients eingeben. Stellen Sie sicher, dass der Name des Clients keine Sonderzeichen oder Leerzeichen enthält, da der Router sonst möglicherweise nicht normal funktioniert.

4. Klicken Sie auf , um das Client-Profil hinzuzufügen.
5. Klicken Sie auf **Apply (Übernehmen)**, um die Einstellungen zu speichern.

3.4 Adaptive QoS (Quality of Service)

3.4.1 Bandbreitenüberwachung

Diese Funktion ermöglicht es Ihnen, die Bandbreite von WAN/LAN zu überwachen und sie zeigt die Upload- und Download-Geschwindigkeit Ihrer Verbindung an.



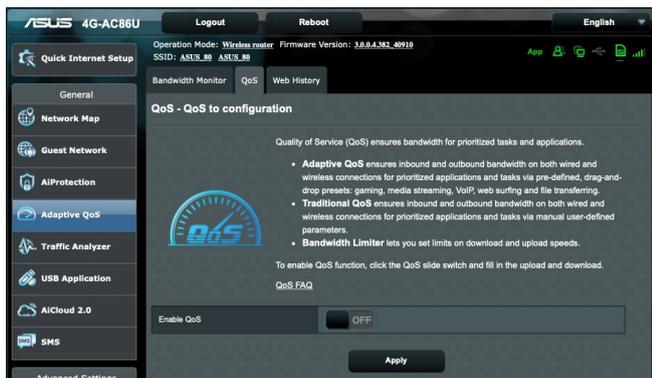
App-Analyse

So aktivieren Sie die App-Analyse-Funktion:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Adaptive QoS > Bandwidth Monitor (Bandbreitenüberwachung)**.
2. Klicken Sie im Feld **Apps Analysis (App-Analyse)** auf **ON (EIN)**.

3.4.2 QoS (Quality of Service)

Diese Funktion sorgt für ausreichend Bandbreite für priorisierte Aufgaben und Anwendungen.



So aktivieren Sie die QoS-Funktion:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Adaptive QoS > QoS**.
2. Klicken Sie im Feld **Enable QoS (QoS aktivieren)** auf **ON (EIN)**.
3. Füllen Sie die Felder für die Upload- und Download-Bandbreite aus.

HINWEIS: Informationen über die Bandbreite erhalten Sie von Ihrem Internetanbieter. Sie können auch <http://speedtest.net> besuchen, um Ihre Bandbreite zu überprüfen.

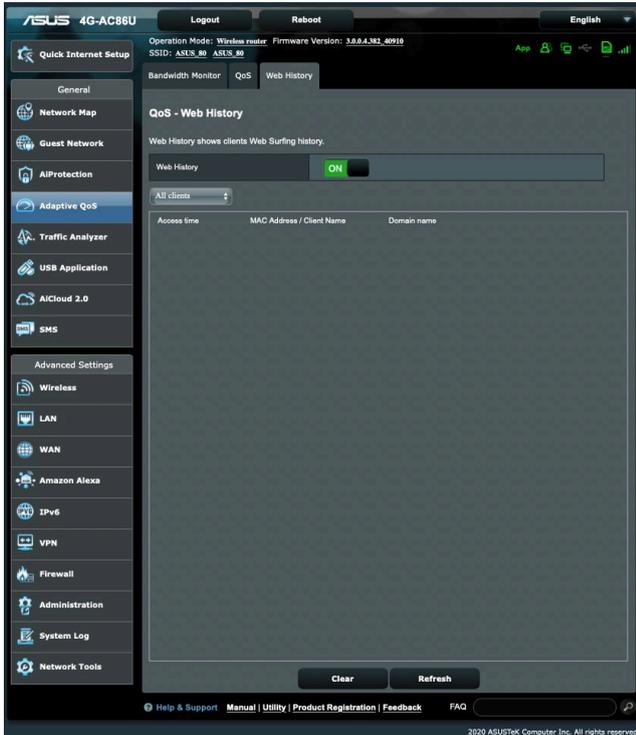
4. Wählen Sie den QoS-Typ (adaptiv oder traditionell) für Ihre Konfiguration.

HINWEIS: Die Definition des QoS-Typs wird auf dem QoS-Register zu Ihrer Referenz angezeigt.

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

3.4.3 Webseitenverlauf

Diese Funktion zeigt den Verlauf und die Einzelheiten der Webseiten oder URLs an, die vom Client besucht wurden.

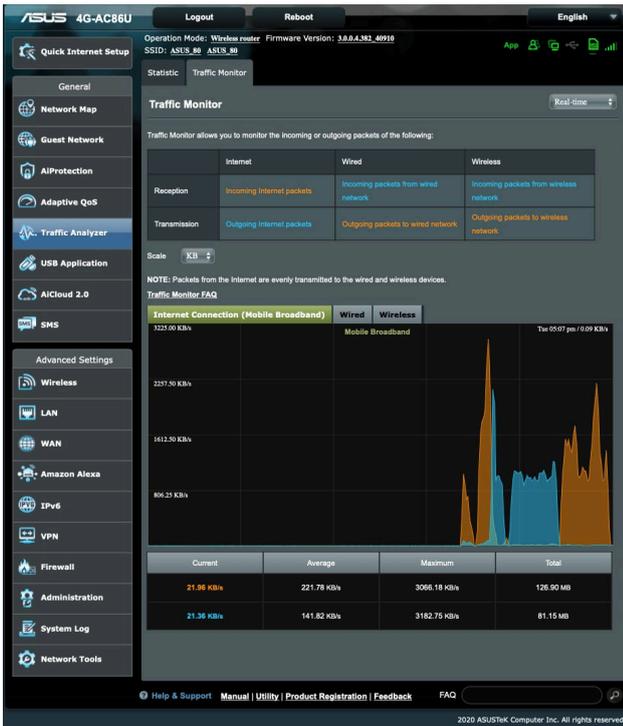


So zeigen Sie den Webseitenverlauf an:

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Adaptive QoS > Web History (Webseitenverlauf)**.
2. (Optional) Klicken Sie auf **Refresh (Aktualisieren)** zum Löschen der Liste.

3.5 Traffic Analyzer

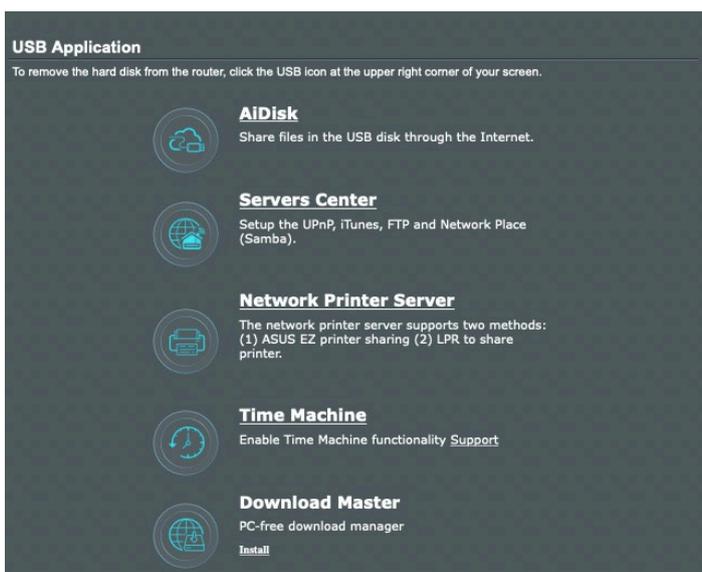
Die Funktion der Überwachung des Datenverkehrs ermöglicht Ihnen das Einsehen der Bandbreitennutzung und der Internetgeschwindigkeit sowie der LANs und WLANs. Damit können Sie den Netzwerkdatenverkehr in Echtzeit oder gleichmäßig über den Tag überwachen. Sie bietet auch die Option, den Netzwerkdatenverkehr der letzten 24 Stunden anzeigen zu lassen.



3.6 USB-Anwendungen verwenden

Die USB-Anwendungen-Funktion bietet AiDisk-, Servers Center-, Netzwerkdruckerserver-, Time Machine- 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. Stellen Sie sicher, dass der USB-Datenträger richtig formatiert und partitioniert wurde. Eine Tabelle mit unterstützten Dateisystemen finden Sie auf der ASUS-Internetseite: <http://event.asus.com/2009/networks/disksupport/>.



3.6.1 AiDisk verwenden

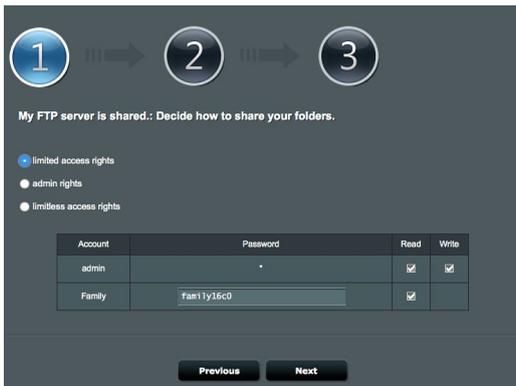
AiDisk erlaubt es Ihnen, den Inhalt eines USB-Laufwerks im Internet freizugeben. AiDisk unterstützt Sie bei der Einrichtung von ASUS-DDNS und einem FTP-Server.

So verwenden Sie AiDisk:

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



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



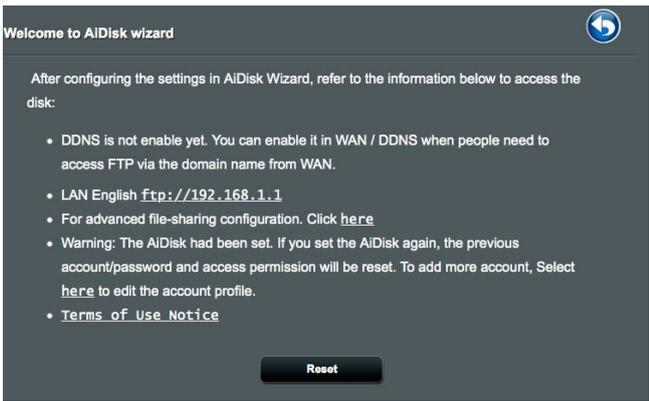
4. Um mit dem ASUS DDNS-Dienst eine eigene Domain einzurichten, lesen Sie die Nutzungsbedingungen, wählen Sie **I will use the service (Ich werde den Dienst nutzen)** und geben Sie Ihren Domain-Namen ein. Klicken Sie dann auf **Next (Weiter)**.





Zum Überspringen der DDNS-Einstellungen können Sie auch **Disable DDNS (DDNS deaktivieren)** wählen und anschließend auf **Next (Weiter)** klicken.

5. Klicken Sie auf **Finish (Fertigstellen)**, 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 den von Ihnen vorher erstellten FTP-Link ein: (**ftp://<domain name>.asuscomm.com**).



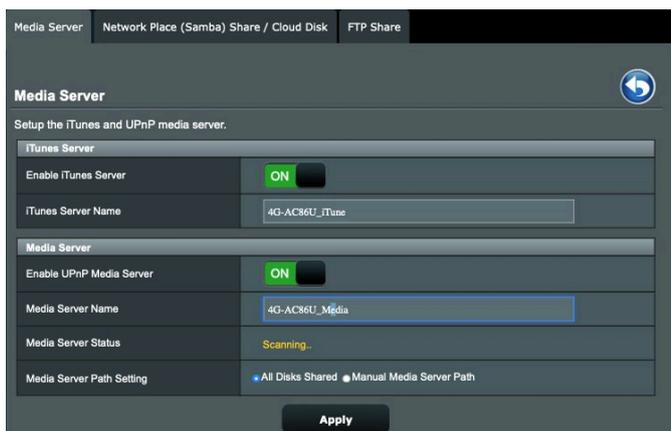
3.6.2 Servercenter verwenden

Mit dem Servercenter können Sie Mediendateien des USB-Laufwerks über ein Medienserver-Verzeichnis, 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 4G-AC86U-Netzwerk, bevor Sie die DLNA-Medienserverfunktionen nutzen.

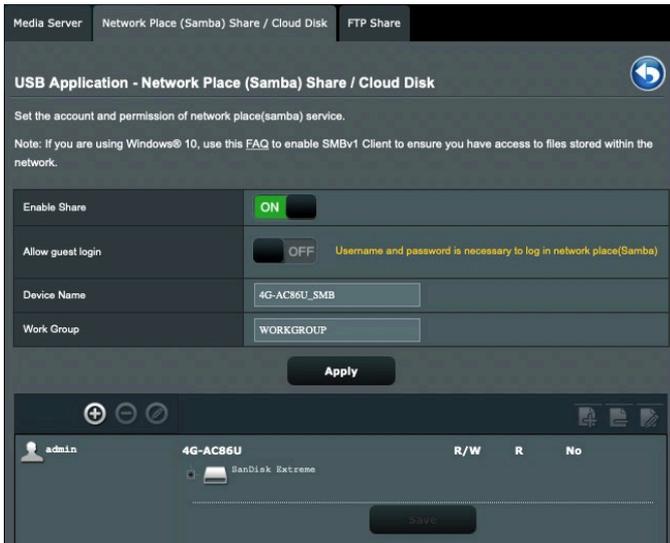


Wechseln Sie zum Aufrufen der Medienserver-Einstellungenseite zum Register **General (Allgemein) > USB Application (USB-Anwendungen) > Media Services and Servers (Mediendienste und -server) > Media Server (Medienserver)**. Hier eine Beschreibung der einzelnen Felder:

- **iTunes-Server aktivieren:** Mit Ein/Aus aktivieren/deaktivieren Sie den iTunes-Medienserver.
- **UPnP-Medienserver aktivieren:** Mit Ein/Aus aktivieren/deaktivieren Sie den UPnP-Medienserver.
- **Medienserverstatus:** Zeigt den Status des Medienservers an.
- **Medienserver-Pfadeinstellungen:** Wählen Sie **All Disks Shared (Alle freigegebenen Laufwerke)** oder **Manual Media Server Path (Manueller Medienserver-Pfad)**.

3.6.3 Netzwerkplatz (Samba) Freigabeservice verwenden

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



So verwenden Sie die Samba-Freigabe:

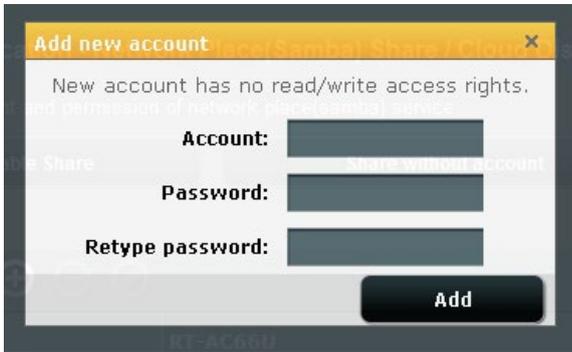
1. Wechseln Sie im Navigationspanel zu **General (Allgemein)** > **USB application (USB-Anwendungen)** > **Media Services and Servers (Medien Dienste und -server)** > **Network Place (Samba) Share / Cloud Disk (Netzwerkumgebungsfreigabe (Samba) / Cloud-Datenträger)**.

HINWEIS: Standardmäßig ist die Netzwerkumgebungsfreigabe (Samba) aktiviert.

2. Führen Sie die Schritte zum Hinzufügen, Löschen oder Ändern eines Kontos aus.

So erstellen Sie ein neues Konto:

- a) Klicken Sie zum Hinzufügen 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 Hinzufügen des Kontos zur Liste auf **Add (Hinzufügen)**.



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 Ordnernamen ein, klicken Sie dann auf **Add (Hinzufügen)**. Der soeben angelegte Ordner wird der Ordnerliste hinzugefügt.



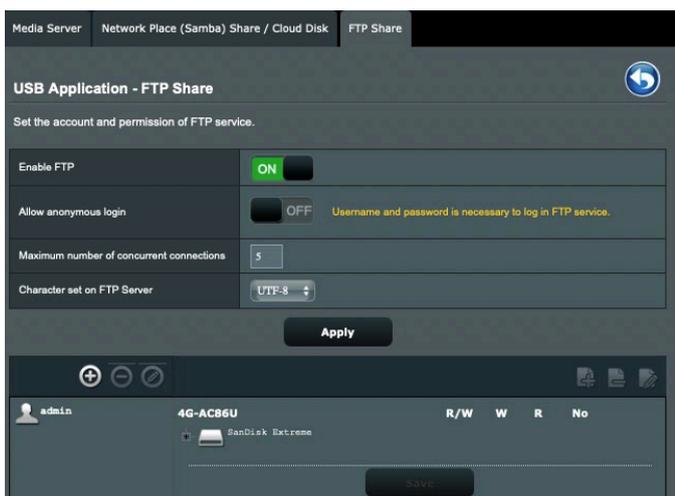
3. Wählen Sie in der Liste der Dateien/Ordner die Art von Zugriffsrechten, die Sie bestimmten Dateien/Ordnern zuweisen möchten:
 - **R/W**: Wählen Sie diese Option, um Lese-/Schreibzugriff zuzuweisen.
 - **R**: Diese Option wählen Sie zum schreibgeschützten Zugriff.
 - **Nein**: Wählen Sie diese Option, wenn Sie eine bestimmte Datei/einen Ordner nicht freigeben möchten.
4. Zum Anwenden klicken Sie auf **Apply (Übernehmen)**.

3.6.4 FTP-Freigabedienst 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 des USB-Datenträgers könnte zur Datenbeschädigung führen.
- Zum sicheren Trennen eines USB-Laufwerks lesen Sie bitte **USB-Laufwerk sicher trennen** im Abschnitt **3.1.5 USB-Geräte überwachen**.



So nutzen Sie den FTP-Freigabedienst:

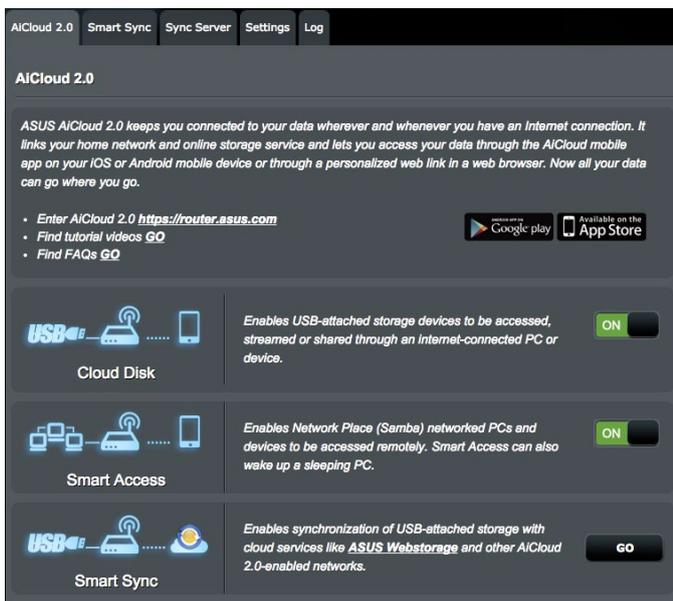
HINWEIS: Sorgen Sie dafür, dass Sie Ihren FTP-Server über AiDisk einrichten. Mehr Details dazu finden Sie im Abschnitt **3.6.1 AiDisk verwenden**.

1. Wechseln Sie im Navigationspanel zu **General (Allgemein)** > **USB application (USB-Anwendungen)** > **Media Services and Servers (Mediendienste und -server)** > **FTP Share (FTP-Freigabe)**.
2. 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 Dateien/Ordner zuzuweisen.
 - **W**: Wählen Sie diese Option, um nur einen Schreibzugriff für bestimmte Dateien/Ordner zuzuweisen.
 - **R**: Diese Option wählen Sie zum schreibgeschützten Zugriff.
 - **Nein**: Wählen Sie diese Option, wenn Sie eine bestimmte Datei/einen 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 der Geräte ein, 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.

3.7 AiCloud 2.0 verwenden

AiCloud 2.0 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 und installieren die Anwendung.
2. Verbinden Sie Ihr kompatibles Gerät mit Ihrem Netzwerk. Schließen Sie die AiCloud-Einrichtung gemäß den Hinweisen auf dem Bildschirm ab.

3.7.1 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 dann Router-Anmeldekontodaten 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.



3.7.2 Intelligenter Zugriff

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



HINWEISE:

- Einen Domain-Namen Ihres Routers können Sie mit ASUS DDNS erstellen. Weitere Informationen dazu finden Sie im Abschnitt **4.3.7 DDNS**.
- Standardmäßig arbeitet AiCloud mit einer sicheren HTTPS-Verbindung. Geben Sie zur besonders sicheren Nutzung mit Cloud-Laufwerk und intelligentem Zugriff [https://\[yourASUSDDNSname\].asuscomm.com](https://[yourASUSDDNSname].asuscomm.com) ein.

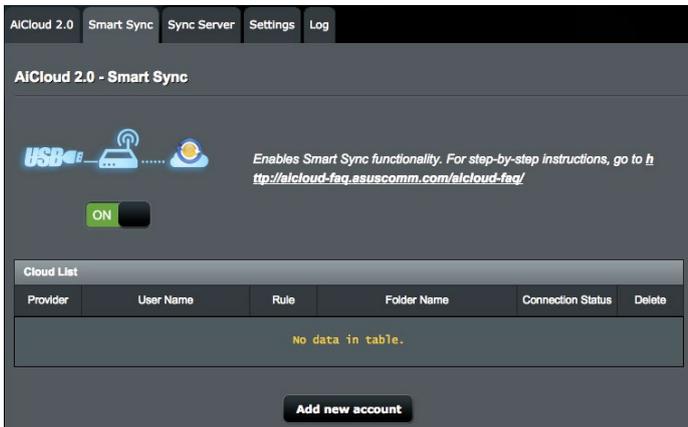
3.7.3 Intelligente Synchronisierung

So nutzen Sie die intelligente Synchronisierung:

1. Wechseln Sie im Navigationspanel zu **AiCloud 2.0 > AiCloud 2.0 > 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- oder Dropbox-Kontos ein, wählen Sie dann den Ordner, den Sie mit WebStorage synchronisieren möchten.
5. Wählen Sie Synchronisierungsregeln für die intelligente Synchronisierung.
 - **Synchronisierung:** Die Auswahl von **Synchronisierung** ermöglicht Ihnen, einen Ordner zwischen zwei Servern zu synchronisieren. Bei dieser Synchronisierungsaufgabe werden im Ordner immer die selben Dateien behalten.
 - **Herunterladen auf USB-Datenträger:** Die Auswahl von **Herunterladen auf USB-Datenträger** ermöglicht es Ihnen, die externen Dateien in den lokalen Ordner auf dem USB-Datenträger zu kopieren.
 - **Hochladen in die Cloud:** Die Auswahl von **Hochladen in die Cloud** ermöglicht es Ihnen, die lokalen Dateien in den externen Ordner auf **ASUS WebStorage** zu kopieren.



6. Klicken Sie auf **Apply (Übernehmen)**, um die Synchronisierungsaufgabe hinzuzufügen

3.7.4 Synchronisierungsserver

AiCloud 2.0 Smart Sync Sync Server Settings Log

AiCloud 2.0 - Sync Server

Smart Sync let you to sync your cloud disk with other AiCloud 2.0 account, fill the forms below then generate an invitation to your friend.

1. Fill the invitation form as below.
2. Select a way to get a security code.
3. Click "Generate" to get a invitation.
4. Copy the contents of invitation and mail to your friends.
5. You might not use smart sync with your friends due to ISP firewall issue, please contact your ISP. For advanced users, please enter a specific "Host name" below to use smart sync with your friends.



Invitation Generator

Description

Host Name

Local sync folder

Rule ?

Security Code

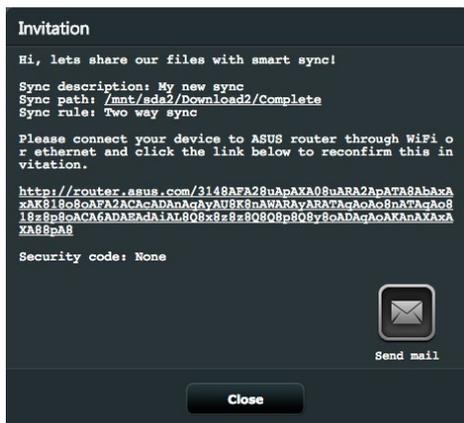


Sync List

Provider	Description	Rule	Local Sync Folder	Invitation	Delete
No data in table.					

So verwenden Sie den Synchronisierungsserver:

1. Wechseln Sie im Navigationspanel zu **AiCloud 2.0 > Sync Server (Synchronisierungsserver)**.
2. Geben Sie die Konfiguration des Synchronisierungsservers im **Invitation Generator (Einladungserstellung)** ein, um **Smart Sync (Intelligente Synchronisierung)** zu aktivieren.
3. Senden Sie an Ihren Freund die Synchronisierungseinladung.



4. Nachdem eine Einladung erstellt wurde, können Sie die Synchronisierungsaufgabe in der Tabelle der **Sync List (Synchronisierungsliste)** überprüfen

Sync List					
Provider	Description	Rule	Local Sync Folder	Invitation	Delete
	My new sync		/sda2/download2/complete	View	



5. Sie können die Löschen-Schaltfläche  anklicken, um die Aufgabe zu beenden, falls Sie den Ordner nicht mehr mit dem externen Client synchronisieren möchten.
6. Sie können außerdem die Aktivitäten des Synchronisierungsservers überprüfen, indem Sie die **Check log (Protokoll überprüfen)**-Schaltfläche oder das **Log (Protokoll)**-Register anklicken.

AiCloud 2.0 Smart Sync Sync Server Settings Log

AiCloud 2.0 - Settings

This page displays a log of AiCloud's activities.

Refresh

3.7.5 Einstellungen

AiCloud 2.0 ermöglicht es Ihnen, eine Zugriffsvorgabe festzulegen, um unbefugten Zugriff, wie z. B. durch einen Wörterbuchangriff, zu verhindern. Wenn ein Host versucht, auf die AiCloud zuzugreifen und die definierte Höchstanzahl fehlgeschlagener Anmeldeversuche in einer bestimmten Zeit überschritten wird, wird der AiCloud-Dienst automatisch deaktiviert.

Secure Socket Layer (SSL) ist ein Protokoll, das eine verschlüsselte Kommunikation zwischen Webserver und Browser für eine sichere Datenübertragung zur Verfügung stellt, einschließlich den Zugang über Kennwörter. Der Benutzerzugriff auf das AiCloud Webportal geschieht über den Standard-Port 443 über https. Die Bereitstellung der Inhalte geschieht über den Standard-Port 8082 über http.

The screenshot shows the 'AiCloud 2.0 - Settings' page. At the top, there is a navigation bar with 'AiCloud 2.0', 'Smart Sync', 'Sync Server', 'Settings', and 'Log'. The main heading is 'AiCloud 2.0 - Settings'. Below this, there is a section for 'Password Protection feature:' with a description: 'The Password Protection feature prevents unauthorized access to AiCloud. You can set a limited number of account/password login attempts. For example, a setting of 3 times / 2 mins indicates that the user has three attempts to input the account and password in 2 minutes. Once the specified number of attempts has been exceeded, the AiCloud account will be locked and administrator access is needed to unlock it.' Below the text is a toggle switch for 'Enable Password Protection Feature.' which is currently turned 'ON'. Underneath, there are two input fields: 'Maximum number of failed login attempts' set to '3' and 'Duration' set to '2 minutes'. Below these is the 'Account Status' section, which shows a user icon and the name 'admin'. At the bottom, there are two more input fields: 'AiCloud Web access port' set to '443' and 'AiCloud content streaming port' set to '8082'. An 'Apply' button is located at the very bottom of the settings area.

3.8 SMS verwenden

Short Message Service (SMS) ist ein Textnachrichten-Dienst, mit dem Sie Nachrichten von oder auf Ihrem WLAN-Router senden oder empfangen können.

3.8.1 Mitteilungen senden

Mit dieser Funktion können Sie Kurznachrichten von Ihrem WLAN-Router senden.

So senden Sie eine neue SMS-Nachricht:

1. Klicken Sie auf die Schaltfläche **New (Neu)** .
2. Geben Sie die Telefonnummer des Empfängers ein.
3. Verfassen Sie Ihre Nachricht.
4. Klicken Sie auf **Send (Senden)**, um die Nachricht abzuschicken.



Phone Number: 0988487210

Message (Max Limit : 70): Comment est ta journée, doux robot?

Buttons: Send, Save

So speichern Sie einen Nachrichtentwurf:

1. Sie können den Nachrichtentwurf speichern, indem Sie auf **Save (Speichern)** klicken.
2. Sie finden die Nachricht aufgelistet in der Tabelle unter **Draft (Entwurf)**.
3. Klicken Sie auf das Bearbeiten-Symbol , um die Nachricht zu bearbeiten und zu senden, oder markieren Sie sie und klicken Sie auf , um den Nachrichtentwurf zu löschen.



SMS - Send Message

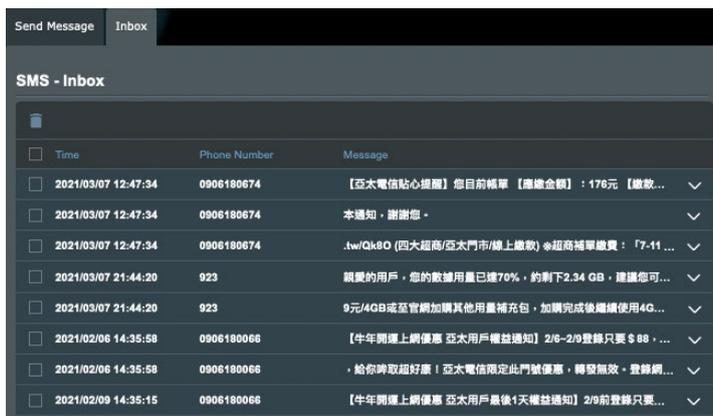
Draft (Max Limit : 5) 

<input type="checkbox"/>	Phone Number	Message	
<input type="checkbox"/>	0988487210	Comment est ta journée, doux robot?	

3.8.2 Posteingang

Im Posteingang können Sie die empfangenen Kurznachrichten anzeigen, die auf Ihrem Gerät gespeichert sind.

Klicken Sie auf , um weitere Informationen anzuzeigen, oder markieren Sie eine Nachricht und klicken Sie auf , um sie zu löschen.



<input type="checkbox"/>	Time	Phone Number	Message	
<input type="checkbox"/>	2021/03/07 12:47:34	0906180674	【亞太電信貼心提醒】您目前帳單【應繳金額】：176元【繳款...	▼
<input type="checkbox"/>	2021/03/07 12:47:34	0906180674	本通知，謝謝您。	▼
<input type="checkbox"/>	2021/03/07 12:47:34	0906180674	.tw/Qk8O (四大超商/亞太門市/線上繳款) 超商補單繳費：「7-11 ...	▼
<input type="checkbox"/>	2021/03/07 21:44:20	923	親愛的用戶，您的數據用量已達70%，約剩下2.34 GB，建議您可...	▼
<input type="checkbox"/>	2021/03/07 21:44:20	923	9元/4GB或至官網加購其他用量補充包，加購完成後繼續使用4G...	▼
<input type="checkbox"/>	2021/02/06 14:35:58	0906180066	【牛年開運上網優惠 亞太用戶權益通知】2/6-2/9登錄只要\$ 88，...	▼
<input type="checkbox"/>	2021/02/06 14:35:58	0906180066	，給你啱取超好康！亞太電信限定此門號優惠，轉發無效 - 登錄網...	▼
<input type="checkbox"/>	2021/02/09 14:35:15	0906180066	【牛年開運上網優惠 亞太用戶最後1天權益通知】2/9前登錄只要...	▼

4 Konfigurieren der erweiterten Einstellungen

4.1 WLAN

4.1.1 Allgemein

Im Allgemein-Register können Sie WLAN-Grundeinstellungen konfigurieren.

The screenshot shows the 'Wireless - General' configuration page. At the top, there are tabs for 'General', 'WPS', 'WDS', 'Wireless MAC Filter', 'RADIUS Setting', and 'Professional'. The 'General' tab is selected. Below the tabs, the page title is 'Wireless - General'. A sub-header reads 'Set up the wireless related information below.' The configuration is presented as a table with various settings:

Band	2.4GHz
SSID	ASUS
Hide SSID	<input type="radio"/> Yes <input checked="" type="radio"/> No
Wireless Mode	Auto <input checked="" type="checkbox"/> b/g Protection
Channel bandwidth	40 MHz
Control Channel	3
Extension Channel	Above
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	99999999
Network Key Rotation Interval	3600

At the bottom of the form is an 'Apply' button.

So konfigurieren Sie die WLAN-Grundeinstellungen:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > General (Allgemein)**.
2. Richten Sie die WLAN-Grundkonfiguration für das 2,4 GHz oder 5 GHz Frequenzband ein.
3. Im **SSID**-Feld weisen Sie einen eindeutigen Namen zu, der aus bis zu 32 Zeichen bestehen darf. Dieser Name ist die SSID (Service Set Identifier) oder der Netzwerkname zum Identifizieren Ihres WLANs. WLAN-Geräte können das WLAN über die von Ihnen zugewiesene SSID identifizieren und sich damit verbinden. Die SSIDs im Infobanner werden aktualisiert, sobald eine neue SSID gespeichert wird.

4. Wählen Sie im **Hide SSID (SSID verbergen)**-Feld **Yes (Ja)** aus, wenn WLAN-Geräte Ihre SSID nicht erkennen sollen. Wenn diese Funktion aktiviert ist, müssen Sie die SSID manuell auf WLAN-Geräten eingeben, wenn Sie auf das WLAN zugreifen möchten.
5. Im **Wireless Mode (WLAN-Modus)**-Feld wählen Sie eine der WLAN-Modusoptionen, um die Art der WLAN-Geräte festzulegen, die sich mit Ihrem WLAN-Router verbinden können:
 - **Auto**: Wählen Sie **Auto**, um 802.11ac, 802.11n, 802.11g, 802.11b und 802.11a Geräten zu gestatten, sich mit dem WLAN-Router zu verbinden.
 - **Altgeräte**: Wählen Sie **Legacy (Altgeräte)**, wenn sich 802.11b/g/n-Geräte mit dem WLAN-Router verbinden dürfen. Allerdings ermöglicht Hardware, die 802.11n physikalisch unterstützt, lediglich eine maximale Übertragungsgeschwindigkeit von 54 Mb/s.
 - **b/g Schutz**: Setzen Sie ein Häkchen bei b/g Schutz, damit der WLAN-Router 802.11n Übertragungen von älteren Geräten mit 802.11g, 802.11b Verbindung schützen kann.
6. Wählen Sie im Feld **Control Channel (Steuerungskanal)** den Betriebskanal für Ihren WLAN-Router. Wählen Sie **Auto**, wenn der WLAN-Router automatisch einen besonders störungsfreien Kanal auswählen soll.
7. Wählen Sie im Feld **Channel bandwidth (Kanalbandbreite)** eine der Kanalbandbreiten, um höhere Übertragungsgeschwindigkeiten zu ermöglichen:
 - **20/40MHz** (Standard): Wählen Sie diese Bandbreite, um automatisch die optimale Bandbreite für Ihre WLAN-Umgebung zu aktivieren. Im 5 GHz Band ist die Standardbandbreite **20/40/80MHz** ausgewählt.
 - **80MHz**: Wählen Sie diese Bandbreite, um den WLAN-Durchsatz der 5 GHz Funkübertragung zu maximieren.
 - **40MHz**: Wählen Sie diese Bandbreite, um den WLAN-Durchsatz der 2,4 GHz Funkübertragung zu maximieren.
 - **20MHz**: Wählen Sie diese Bandbreite, wenn Sie auf Probleme mit Ihrer WLAN-Verbindung treffen.
8. Wenn **20/40/80MHz**, **20/40MHz**, **40MHz** oder **80MHz** ausgewählt ist, können Sie einen oberen oder unteren angrenzenden Kanal im Feld **Extension Channel (Erweiterungskanal)** festlegen
9. Wählen Sie im Feld **Authentication Method (Authentifizierungsverfahren)** eines der Authentifizierungsverfahren:

- **Open System:** Diese Option bietet keinen Schutz.
- **WPA2-Personal / WPA Auto-Personal:** Diese Option bietet einen starken Schutz. Sie können entweder WPA2-Personal (mit AES) oder WPA Auto-Personal (mit AES oder TKIP + AES) verwenden. Wenn Sie diese Option auswählen, müssen Sie den gemeinsamen WPA-Schlüssel (Netzwerkschlüssel) eintragen.
- **WPA2 Enterprise / WPA Auto-Enterprise:** Diese Option bietet einen sehr starken Schutz. Diese Lösung beinhaltet einen integrierten EAP-Server oder einen externen RADIUS Back-End-Authentifizierungsserver.

10. Klicken Sie zum Abschluss auf **Übernehmen**.

4.1.2 WPS

WPS (Wi-Fi Protected Setup) ist ein WLAN-Sicherheitsstandard, der einfache Geräteverbindungen zu einem WLAN 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.

General	WPS	WDS	Wireless MAC Filter	RADIUS Setting	Professional
Wireless - WPS					
WPS (Wi-Fi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button.					
Enable WPS	<input type="checkbox"/> OFF				
Current Frequency	2.4GHz Switch Frequency				
Connection Status	Not used				
Configured	Yes				
AP PIN Code	<input type="text" value="31257367"/>				

General	WPS	WDS	Wireless MAC Filter	RADIUS Setting	Professional
Wireless - WPS					
WPS (Wi-Fi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button.					
Enable WPS	<input type="checkbox"/> OFF				
Current Frequency	5GHz Switch Frequency				
Connection Status	Not used				
Configured	Yes				
AP PIN Code	<input type="text" value="31257367"/>				

So aktivieren Sie WPS in Ihrem WLAN:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > WPS**.
2. Stellen Sie den Schieber im **Enable WPS (WPS aktivieren)**-Feld auf **ON (Ein)** ein.
3. WPS verwendet separat die 2,4 GHz und 5 GHz Funkübertragung.
4. Sie können eines der folgenden WPS-Verfahren zur Kopplung für die WLAN-Verbindung nutzen:
 - **PBC (Push Button Configuration) Modus:**
 - Hardware PBC am Router: Drücken Sie die physische WPS-Taste am WLAN-Router und drücken Sie dann die WPS-Taste am WLAN-Client in drei (3) Minuten.
 - Software PBC am Router: Setzen Sie im Feld **WPS Method (WPS-Verfahren)** ein Häkchen bei <Push button> (<Taste drücken>), klicken Sie auf **Start** und drücken Sie dann die WPS-Taste am WLAN-Client in drei (3) Minuten.
 - **PIN-Code Modus:**
 - Kopplung durch den WLAN-Client: Drücken Sie die WPS-Taste am WLAN-Router und führen Sie dann den WPS-Verbindungsvorgang im PIN-Code Modus nebst Eingabe des **AP PIN-Codes** am Client-Gerät durch.
 - Kopplung durch den WLAN-Router: Drücken Sie die WPS-Taste am WLAN-Client und führen Sie dann den WPS-Verbindungsvorgang im PIN-Code Modus nebst Eingabe des **Client PIN-Codes** im Feld **WPS Method (WPS-Verfahren) > Client PIN Code** durch. Überprüfen Sie, ob der PIN-Code richtig ist und klicken Sie dann auf **Start**, um den WLAN-Client zu koppeln.

HINWEISE:

- WPS unterstützt die Authentisierung per Open System und WPA2-Personal. WPS unterstützt keine WLANs, die mit den Verschlüsselungsverfahren Shared Key, WPA-Personal, WPA-Enterprise, WPA2-Enterprise oder RADIUS arbeiten.
 - Schlagen Sie notfalls in der Bedienungsanleitung Ihres WLAN-Gerätes nach, wo sich die WPS-Taste befindet.
 - Während des WPS-Vorgangs sucht der WLAN-Router nach verfügbaren WPS-Geräten. Wenn der WLAN-Router keine WPS-Geräte findet, schaltet er um in den Inaktivitätsmodus.
 - Bis zum Abschluss der WPS-Einrichtung blinken die Betriebs-LEDs des Routers für drei Minuten schnell.
-

4.1.3 WDS

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 im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > WDS**.

General WPS WDS Wireless MAC Filter RADIUS Setting Professional

Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your 4G-AC55U to connect to an access point wirelessly. WDS may also be considered a repeater mode. But with this method, the devices connected to the access point will only be able to use half of the access point's original wireless speed.

Note: The function only support [Open System/NONE, Open System/WEP] security authentication method.

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

Basic Config

2.4GHz MAC	<input type="text" value="AC:9E:17:56:6F:48"/>
5GHz MAC	<input type="text" value="AC:9E:17:56:6F:4C"/>
Band	<input type="text" value="2.4GHz"/>
AP Mode	<input type="text" value="AP Only"/>
Connect to APs in list	<input checked="" type="radio"/> Yes <input type="radio"/> No

Remote AP List (Max Limit : 4)

Remote AP List	Add / Delete
<input type="text"/>	<input type="button" value="⊕"/>
No data in table.	

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 WDS-Funktion.
 - **Nur WDS:** Aktiviert die WDS-Funktion, verhindert jedoch, dass sich andere WLAN-Geräte/-Stationen mit dem Router verbinden können.
 - **HYBRID:** Aktiviert die WLAN-Brückenfunktion und ermöglicht, dass sich andere WLAN-Geräte/-Stationen mit dem Router verbinden können.
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. Geben Sie in der **Remote AP List (Externe-AP-Liste)** eine MAC-Adresse ein, klicken Sie dann zur Eingabe der MAC-Adressen weiterer verfügbarer Access Points auf die **Add (Hinzufügen)**-Schaltfläche
6. Klicken Sie auf **Apply (Übernehmen)**.

HINWEISE:

- Im Hybridmodus erhalten mit dem ASUS WLAN-Router verbundene WLAN-Geräte lediglich die halbe Übertragungsgeschwindigkeit des Access Points.
 - Jeder zur Liste hinzugefügte Access Point muss sich im selben Steuerungskanal und in der selben festen Kanalbandbreite befinden wie der lokale ASUS WLAN-Router. Sie können den Steuerungskanal unter **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > General (Allgemein)** ändern.
-

4.1.4 WLAN-MAC-Filter

Der WLAN-MAC-Filter ermöglicht die Kontrolle über Pakete, die an eine bestimmte MAC (Media Access Control)-Adresse in Ihrem WLAN gesendet werden.

The screenshot shows the 'Wireless - Wireless MAC Filter' configuration page. At the top, there are tabs for 'General', 'WPS', 'WDS', 'Wireless MAC Filter', 'RADIUS Setting', and 'Professional'. The 'Wireless MAC Filter' tab is selected. Below the tabs, the title 'Wireless - Wireless MAC Filter' is displayed. A descriptive text states: 'Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.' Under the 'Basic Config' section, there are three settings: 'Band' set to '2.4GHz', 'Enable MAC Filter' with 'Yes' selected, and 'MAC Filter Mode' set to 'Accept'. Below this is a table for the 'MAC filter list (Max. Limit: 64)'. The table has two columns: 'MAC filter list' and 'Add / Delete'. The table is currently empty, with the text 'No data in table.' displayed below it. An 'Apply' button is located at the bottom of the page.

So richten Sie den WLAN-MAC-Filter ein:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > Wireless MAC Filter (WLAN-MAC-Filter)**.
2. Wählen Sie **Yes (Ja)** im **Enable Mac Filter (Mac Filter aktivieren)**-Feld.
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 zu gewähren.
 - Wählen Sie **Reject (Abweisen)**, um Geräten in der MAC-Filterliste den Zugriff auf das WLAN zu verweigern.
4. Klicken Sie auf die **Add (Hinzufügen)**-Taste in der **MAC filter list (MAC-Filterliste)** und geben Sie die MAC-Adresse des drahtlosen Geräts ein.
5. Klicken Sie auf **Apply (Übernehmen)**.

4.1.5 RADIUS-Einstellungen

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

The screenshot shows the 'RADIUS Setting' tab in a wireless router's configuration interface. The page title is 'Wireless - RADIUS Setting'. Below the title, there is a descriptive paragraph: 'This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise/ WPA2-Enterprise/ Radius with 802.1x".' The configuration area contains four fields: 'Band' set to '2.4GHz', 'Server IP Address' (empty), 'Server Port' set to '1812', and 'Connection Secret' (empty). An 'Apply' button is located at the bottom right of the form.

So richten Sie die WLAN-RADIUS-Einstellungen ein:

1. Vergewissern Sie sich, dass das Authentisierungsverfahren des WLAN-Routers auf **WPA-Auto-Enterprise** oder **WPA2-Enterprise** eingestellt ist.

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

2. Wechseln Sie im 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.

General	WPS	WDS	Wireless MAC Filter	RADIUS Setting	Professional
Wireless - Professional					
Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.					
<i>*Reminder: The System time zone is different from your locale setting.</i>					
Band	5GHz				
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Enable wireless scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Set AP isolated	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Enable IGMP Snooping	Disable				
Multicast Rate(Mbps)	Auto				
Preamble Type	Long				
RTS Threshold	2347				
DTIM Interval	1				
Beacon Interval	100				
Enable TX Buring	Disable				
Enable Packet Aggregation	Enable				
Enable WMM	Enable				
Enable WMM No-Acknowledgement	Disable				
Enable WMM APSD	Enable				
Enable WMM DLS	Disable				
Airtime Fairness	Disable				
Multi-User MIMO	Enable				
802.11ac Beamforming	Enable				
Universal Beamforming	Disable				
Tx power adjustment	<input type="range"/> Performance				
Apply					

Im **Professional Settings (Professionelle Einstellungen)**-Bildschirm 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 WLANs. Wählen Sie **No (Nein)**, wenn Sie das WLAN deaktivieren möchten.

- **WLAN-Planer aktivieren:** Wählen Sie **Yes (Ja)**, um das WLAN nach den folgenden Zeitplanregeln zu aktivieren. Wählen Sie **No (Nein)**, wenn Sie die Zeitplanregeln deaktivieren möchten.
- **Datum der Funkaktivierung (wochentags):** Hier können Sie die Werktage festlegen, wann das WLAN aktiviert sein soll.
- **Tageszeit der Funkaktivierung:** Hier können Sie den Zeitraum festlegen, wann das WLAN während der Woche aktiviert sein soll.
- **Datum der Funkaktivierung (Wochenende):** Hier können Sie die Wochenendtage festlegen, wann das WLAN aktiviert sein soll.
- **Tageszeit der Funkaktivierung:** Hier können Sie den Zeitraum festlegen, wann das WLAN während des Wochenendes aktiviert sein soll.
- **AP isolieren:** Die AP-isolieren-Einstellung verhindert die Kommunikation von WLAN-Geräten im Netzwerk untereinander. Diese Funktion ist nützlich, wenn Sie ein öffentliches WLAN erstellen möchten, das es nur Gästen gestattet, Zugang zum Internet zu erhalten. Wählen Sie **Yes (Ja)** zum Aktivieren dieser Funktion, **No (Nein)** zum Abschalten.
- **Roaming-Assistent:** Dieser dient für WLAN-Umgebungen, die mit mehreren Access Points (APs) oder WLAN-Repeaterern ausgestattet sind, um alle toten Winkel mit dem WLAN zu versorgen. Wenn sich ein Client, der mit dem AP1 verbunden ist, von einem Ort mit besserem Signal zu einem anderen mit schlechtem Signal bewegt, kann ein weiteres Signal vom AP2 vorhanden sein. Um zu verhindern, dass der Client mit dem AP1 verbunden bleibt, können Sie den Roaming-Assistenten aktivieren und einen RSSI-Minimalwert als Grenze festlegen. Wenn die Verbindungsqualität unter die Grenze fällt, wird der WLAN-Client vom AP1 getrennt, damit die WLAN-Umgebung neu bewertet werden kann, um den AP mit der besten Signalqualität auszuwählen, wie den AP2.
- **IGMP Snooping aktivieren:** Wenn IGMP-Snooping aktiviert ist, wird der Multicast-Datenverkehr nur an WLAN-Clients weitergeleitet, die Mitglieder einer spezifischen Multicast-Gruppe sind.
- **Multicast-Rate (Mb/s):** Hier wählen Sie die Multicast-Übertragungsrate oder schalten die gleichzeitige Einzelübertragung mit **Disable (Deaktivieren)** ab.

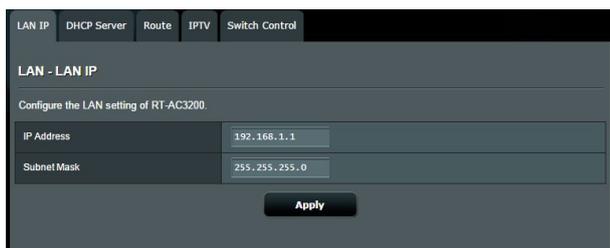
- **Präambeltyp:** Der Präambeltyp definiert die Zeitspanne, die der Router für CRC-Prüfungen (zyklische Redundanzprüfungen) aufwendet. CRC ist ein Verfahren zur Fehlererkennung bei Datenübertragungen. Die Einstellung **Short (Kurz)** eignet sich für stark frequentierte WLANs mit hohem Datenaufkommen. Wählen Sie **Long (Lang)**, wenn sich Ihr WLAN vornehmlich aus älteren WLAN-Geräten zusammensetzt.
- **AMPDU RTS:** Das verwendete Verfahren, A-MPDU, dient dazu, für 802.11n oder 802.11ac kurzfristige Pakete in langfristige Pakete für die selbe MAC-Adresse zu vereinigen. Wenn ein WLAN-Gerät bereit für die Übertragung ist, wird ein RTS (Request to Send) geschickt. Nachdem AMPDU RTS aktiviert ist, wird jeder AMPDU Datenübertragungsblock mit dem RTS-Verfahren versendet.
- **RTS-Schwellenwert:** Wählen Sie einen niedrigeren RTS-Schwellenwert (RTS steht für „Request to Send“, also Sende-anfrage), 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 Millisekunden.
- **Bakenintervall:** Das Bakenintervall definiert die Zeitspanne zwischen den einzelnen DTIMs. Der Standardwert liegt bei 100 Millisekunden. Vermindern Sie das Bakenintervall bei instabilen WLAN-Verbindungen oder beim Einsatz von Roaming-Geräten.
- **Sendebündelung (TX Bursting) aktivieren:** Diese Einstellung erhöht die Übertragungsgeschwindigkeit zwischen WLAN-Router und 802.11g-Geräten.
- **WMM APSD aktivieren:** WMM APSD (Automatic Power Save Delivery) ist die Verbesserung zum älteren Power Saver Modus. Aktivieren Sie WMM APSD und der WLAN-AP verwaltet die Funkauslastung, um die Akkulaufzeit für akkubetriebene WLAN-Clients, wie Smartphones und Laptops, zu verlängern. APSD schaltet automatisch um zur Nutzung eines längeren Bakenintervalls, wenn der Datenverkehr kein kurzes Intervall zum Paketaustausch benötigt.

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 wider.



So ändern Sie die LAN-IP-Einstellungen:

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

The screenshot shows the 'LAN - DHCP Server' configuration page. At the top, there are navigation tabs: LAN IP, DHCP Server (selected), Route, IPTV, and Switch Control. Below the tabs, the page title is 'LAN - DHCP Server'. A descriptive paragraph explains DHCP and mentions '4G-AC55U'. A link for 'Manually Assigned IP around the DHCP list FAQ' is provided. The 'Basic Config' section includes: 'Enable the DHCP Server' (radio buttons for Yes/No, with 'Yes' selected), '4G-AC55U's Domain Name' (empty text field), 'IP Pool Starting Address' (192.168.1.2), 'IP Pool Ending Address' (192.168.1.254), 'Lease time' (86400), and 'Default Gateway' (empty text field). The 'DNS and WINS Server Setting' section has 'DNS Server' and 'WINS Server' (both empty text fields). The 'Enable Manual Assignment' section has 'Enable Manual Assignment' (radio buttons for Yes/No, with 'No' selected). Below this is a table for 'Manually Assigned IP around the DHCP list (Max Limit : 64)'. The table has columns for 'MAC address', 'IP Address', and 'Add / Delete'. The table is currently empty, with a message 'No data in table.' at the bottom. An 'Apply' button is at the bottom of the page.

So konfigurieren Sie einen DHCP-Server:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > 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**-Textfeld einen Domain-Namen 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 eine zugewiesene IP-Adresse in Sekunden ein. Sobald dieses Zeitlimit erreicht wurde, weist der DHCP-Server eine neue IP-Adresse zu.

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 WINS Server Settings (DNS- und WINS-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 hinzugefügt 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.

Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
				LAN	+

No data in table.

Apply

So konfigurieren Sie die LAN-Routentabelle:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > LAN > 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 oder 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.

The screenshot shows the 'LAN - IPTV' configuration page. At the top, there are tabs for 'LAN IP', 'DHCP Server', 'Route', 'IPTV', and 'Switch Control'. Below the tabs, a message states: 'To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN - Dual WAN](#) to confirm that WAN port is assigned to primary WAN.' The configuration options are as follows:

Port	
Select ISP Profile	None
Choose IPTV STB Port	None

Special Applications	
Use DHCP routes	Microsoft
Enable multicast routing (IGMP Proxy)	Disable
Enable efficient multicast forwarding (IGMP Snooping)	Disable
UDP Proxy (Udpxy)	0

An 'Apply' button is located at the bottom right of the configuration area.

4.2.5 Switch Control

Das Switch Control-Register ermöglicht Ihnen, NAT Beschleunigung und Jumbo Frame zu konfigurieren, um die Netzwerkleistung zu verbessern. Wir empfehlen, die Standard-Routeneinstellungen nicht zu verändern, sofern Sie nicht über umfassendes Wissen verfügen.

The screenshot shows the 'LAN - Switch Control' configuration page. At the top, there are tabs for 'LAN IP', 'DHCP Server', 'Route', 'IPTV', and 'Switch Control'. Below the tabs, a message states: 'Setting 4G-AC55U switch control.' The configuration options are as follows:

NAT Acceleration(IPv4 Only)	Enable
Enable Jumbo Frame	Disable

An 'Apply' button is located at the bottom right of the configuration area.

4.3 WAN

4.3.1 Internetverbindung

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

Internet Connection | Dual WAN | Port Trigger | Virtual Server / Port Forwarding | DMZ | DDNS | NAT Passthrough

WAN - Internet Connection

4G-AC55U supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

WAN index

WAN Type: WAN

Basic Config

WAN Connection Type: Automatic IP

Enable WAN: Yes No

Enable NAT: Yes No

Enable UPnP: Yes No

WAN DNS Setting

Connect to DNS Server automatically: Yes No

Account Settings

Authentication: None

Special Requirement from ISP

Host Name:

MAC Address: **MAC Clone**

DHCP query frequency: Aggressive Mode

Apply

4.3.1.1 WAN

So konfigurieren Sie die WAN-Verbindungseinstellungen:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > WAN > Internet Connection (Internetverbindung)**.
2. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **Übernehmen**.
 - **WAN-Verbindungstyp:** Wählen Sie den Typ Ihrer Internetverbindung. Zur Auswahl stehen **Automatic IP (Automatische IP)**, **PPPoE**, **PPTP**, **L2TP** und **Static IP (Feste IP)**. Wenden Sie sich an Ihren 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 einen 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 extern zur Unterstützung von P2P-Anwendungen, interaktiven Spielen, Videokonferenzen, Web- oder Proxyservern konfiguriert werden. Anders als bei der Portweiterleitung, bei der Port Einstellungen 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 automatisch verbinden:** Ermöglicht, die DNS-IP-Adresse für den Router automatisch vom Internetanbieter zuweisen zu lassen. Ein DNS ist ein Host im Internet, der Namen von Internetseiten (URLs) in numerische IP-Adressen umsetzt.
- **Authentifizierung:** Dieses Element wird eventuell von einigen 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-Anfragefrequenz:** Ändert die Intervalleinstellungen der DHCP-Erkennung zur Vermeidung einer Überlastung des DHCP-Servers.

4.3.1.2 Mobiles Breitband

Der 4G-AC86U besitzt ein integriertes 3G/4G Modem, mit dem Sie eine mobile Breitbandverbindung zum Internetzugang nutzen können.

So richten Sie Ihr mobiles Breitband zum Internetzugang ein:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > WAN > Internet Connection (Internetverbindung)** und wählen Sie im Feld **WAN Interface (WAN-Schnittstelle)** die Option **Mobile Broadband (Mobiles Breitband)** aus.

The screenshot shows the 'WAN - Mobile Broadband' configuration page. At the top, there are navigation tabs: Internet Connection, Dual WAN, Port Trigger, Virtual Server / Port Forwarding, DMZ, DDNS, and NAT Passthrough. The main heading is 'WAN - Mobile Broadband'. Below it, a text block explains that the 4G-AC86U can establish an Internet connection via Ethernet WAN, Mobile Broadband, or LAN as WAN, and instructs the user to select the interface from a dropdown list. The configuration area includes a 'WAN Index' section with a 'WAN Interface' dropdown menu set to 'Mobile Broadband' and an 'Enable Mobile Broadband' checkbox set to 'Enable'. Below this is a 'Mobile Broadband Modem Information' section with a table showing the 'Modem software version' as 'EM12QPAR01A18M4G' and the 'IMEI' as '355219110000082'. There are also 'Reset Modem' and 'Reboot Modem' buttons.

WAN Index	
WAN Interface	Mobile Broadband
Enable Mobile Broadband	Enable

Mobile Broadband Modem Information			
Modem software version	EM12QPAR01A18M4G	Reset Modem	Reboot Modem
IMEI	355219110000082		

2. Wählen Sie im Feld **Enable Mobile Broadband (Mobiles Breitband aktivieren)** die Option **Enable (Aktivieren)** aus.
3. Vergewissern Sie sich, dass Sie die SIM-Karte richtig eingelegt haben, und richten Sie die Mobil-Einstellungen Ihres Routers ein.

WAN Index	
WAN Interface	Mobite Broadband ▾
Enable Mobile Broadband	Enable ▾
Mobile Broadband Modem Information	
Modem software version	EM12GPAR01A21M4G Reset Modem Reboot Modem
IMEI	355219110000084
Configure the Mobile Broadband settings of 4G-AC86U.	
Internet Connection	
Connection status	Connected 
Network Type	Auto ▾
PDP Type	IPv4 ▾
LTE Band	Auto ▾
Roaming	Disable ▾

4. Konfiguration der Internetverbindung:
- 1) Wählen Sie im Feld **Network Type (Netzwerktyp)** Ihr bevorzugtes Netzwerk aus:
 - **Automatisch** (Standard): Wählen Sie **Auto**, um dem WLAN-Router zu gestatten, automatisch den Kanal mit einer verfügbaren Verbindung aus dem 4G- oder 3G-Netzwerk auszuwählen.
 - **Nur 4G**: Wählen Sie diese Option, um den WLAN-Router automatisch nur mit dem 4G-Netzwerk zu verbinden.
 - **Nur 3G**: Wählen Sie diese Option, um den WLAN-Router automatisch nur mit dem 3G-Netzwerk zu verbinden.
 - 2) **PDP-Typ**: Der WLAN-Router unterstützt verschiedene PDP-Typen; PPP, IPv4, IPv6, IPv6 zu IPv4.
 - 3) **LTE-Band**: In diesem Feld können Sie das LTE-Band auswählen.
 - 4) **Roaming**: Wenn Sie in ein anderes Land reisen, können Sie die originale SIM-Karte für den Zugang zum lokalen Netzwerk nutzen, falls Ihr Internetanbieter den Roaming-Dienst in diesem Land anbietet. Aktivieren Sie diese Funktion, damit Sie Zugang zum lokalen Netzwerk erhalten können.
 - Klicken Sie auf **Scan (Suche)**, um alle verfügbaren Mobilfunknetze anzuzeigen.
 - Wählen Sie ein verfügbares Mobilfunknetz und klicken Sie auf **Apply (Übernehmen)**, um sich damit zu verbinden.

HINWEISE:

- Der LTE-Router kann Ihren Internetanbieter anhand der IMSI-Informationen Ihrer SIM-Karte erkennen. Falls das Mobilfunknetz Ihres Internetanbieters nicht gefunden werden kann, verbinden Sie sich mit einem Roaming-Netzwerk anderer Internetanbieter.
 - Beachten Sie unbedingt eventuell anfallenden Roaming-Kosten, wenn Sie keine lokale SIM-Karte (fast immer eine gute, da sehr kostensparende Idee) nutzen. Lassen Sie sich von Ihrem Netzanbieter über Roaming-Kosten informieren, bevor Sie Roaming-Dienste nutzen, damit es kein böses Erwachen beim Eintreffen der nächsten Mobilfunkrechnung gibt.
-

The screenshot shows a 'Data Usage Limitation' settings screen. At the top, it displays 'Data Usage' as '9.64 MBytes (Starting Day : 1)' with a 'Clear' button. Below this are several rows of settings:

Data Usage	9.64 MBytes (Starting Day : 1)	Clear
Cycle Start Day	1	
Data Usage Limit	0	Gbytes (Disable : 0)
Data Usage Alert	0	Gbytes (Disable : 0)
Send SMS Notification	Disable	

5. Datennutzungsbeschränkung

- **Datenvolumen:** Zeige das Datenvolumen.
- **Starttag des Zyklus:** Wählen Sie den Tag aus, an dem Sie mit der Zählung des Datenvolumens beginnen möchten. Das Datenvolumen wird am Ende eines jeden Zyklus zurückgesetzt.
- **Begrenzung des Datenvolumens:** Legen Sie für die Internetnutzung eine monatliche Obergrenze des Datenvolumens (in GB) fest. Sobald die Grenze erreicht ist, erscheinen ein Ausrufezeichen und eine Warnmeldung, wenn Sie sich auf der Administratorseite anmelden. Der Internetzugang wird blockiert.
- **Warnmeldung für Datenvolumen:** Legen Sie eine Obergrenze des Datenvolumens fest, bei deren Erreichung ein Ausrufezeichen und eine Warnmeldung erscheinen, wenn Sie sich auf der Administratorseite anmelden. Wenn Ihre Internetnutzung diese Grenze erreicht, wird der Internetzugang nicht blockiert bis die tatsächliche Grenze des Datenvolumens erreicht ist.
- **SMS-Benachrichtigung senden:** Aktivieren Sie diese Funktion, um eine SMS-Benachrichtigung von Ihrem Router auf Ihr Mobilgerät zu senden, sobald die Obergrenze des Datenvolumens für die Internetnutzung erreicht ist.

APN Profile	
APN Configuration	Auto
APN Service(optional)	Gent
Dial Number	*99#
Username	
Password	
Authentication	None

APN Profile	
APN Configuration	Manual Setting
Location	Taiwan
ISP	Far EastOne
APN Service(optional)	Internet
Dial Number	*99#
Username	
Password	
Authentication	None

6. APN-Konfiguration

- 1) **Auto** (Standard): Das System wählt standardmäßig die Einstellung Auto APN.
- 2) **Manuell**: Falls die automatische DFÜ (Dial-Up)-Verbindung fehlschlägt, wählen Sie Manuell aus, um die APN-Einstellung manuell zu konfigurieren.
 - A. **Standort**: Wählen Sie den Standort Ihres 3G/4G-Anbieters aus der Auswahlliste.
 - B. **Internetanbieter**: Wählen Sie Ihren Internetanbieter aus der Auswahlliste.
 - C. **APN (Access Point Name)-Service (optional)**: Entsprechende Informationen erhalten Sie von Ihrem 3G/4G-Anbieter.
 - D. **Einwahlnummer**: Einwahlnummer des 3G/4G-Anbieters
 - E. **Benutzername / Kennwort**: Geben Sie den Benutzernamen und das Kennwort ein, die Ihr 3G/4G-Netzwerkanbieter bereitstellt.

7. PIN-Konfiguration

PIN-Code: Geben Sie für die Verbindung den PIN-Code des 3G/4G-Anbieters im SIM PIN Management ein, falls die SIM-Karte benötigt wird.

- Der standardmäßige PIN-Code kann je nach Anbieter variieren. Wenn Ihr Internetanbieter die PIN-Code-Verifizierung standardmäßig deaktiviert hat, können Sie die Einstellung überspringen.



Screenshot of the SIM PIN Management interface. The 'USIM Card Status' is 'SIM card is ready'. The 'PIN Verification' is set to 'Disable'.

- Wenn Ihr Internetanbieter die PIN-Code-Verifizierung standardmäßig aktiviert hat, sehen Sie das Statussymbol für die SIM-Sperre  im Statussymbolbereich, und Sie müssen den PIN-Code eingeben.



Screenshot of the SIM PIN Management interface. The 'USIM Card Status' is 'PIN code is required'. The 'PIN code' field contains '1234'. There is a 'Save My PIN' checkbox and an 'OK' button. The 'Remaining Attempts' is 3.

- Sie können die PIN-Code-Verifizierung manuell über das Web-Menü Ihres Routers oder Ihr Mobiltelefon aktivieren. Sie müssen auch den PIN-Code eingeben.



Screenshot of the SIM PIN Management interface. The 'USIM Card Status' is 'SIM card is ready'. The 'PIN Verification' is set to 'Enable'. There is a 'Modify' button for PIN Modification.



Screenshot of the SIM PIN Management - PIN Verification dialog box. It prompts the user to input the PIN code obtained from the internet service provider. The 'PIN code' field is empty. The 'PIN Remaining Attempts' is 2. There are 'Cancel' and 'OK' buttons.

Status der Mobilverbindung

So finden Sie Informationen zum mobilen Breitband:

1. Klicken Sie auf  für ausführliche Informationen.

Internet Connection	
Connection status	Connected 
Network Type	Auto
PDP Type	IPv4
LTE Band	Auto
Roaming	Disable

2. Der Bildschirm **Mobile Connection Status (Status der Mobilverbindung)** zeigt den ausführlichen Verbindungsstatus des mobilen Breitbands an.

WAN - Mobile Connection Status	
This page displays basic device information, internet connection status and internet usage.	
Product Information	
Model Name	4G-AC86U
IMSI	466056008449
ICCID	8988605101902049
Phone Number	+88690697
Wireless Status	
Cell ID	1B60134
Connection Type	TDD LTE
Band	LTE BAND 38
RSSI	-58 dBm
SINR	11 dB
RSRP	-94 dBm
RSRQ	-13 dBm
Internet Usage	
Connection Status	 Connected
SIM Provider	KGT-Online
Network Provider	LTE GT
Data Usage	212.514 MBytes
Data Sent	8.841 MBytes
Data Received	203.673 MBytes
Data Sent/Sec	
Data Received/Sec	
Connection Time	0 days 0 hour(s) 28 minute(s) 22 seconds
Close	

4.3.2 IPv6 (Interneteinstellungen)

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

The screenshot shows the IPv6 configuration page for a 4G-AC86U router. The page is titled 'IPv6' and includes a sub-header 'Configure the IPv6 Internet setting of 4G-AC86U.' and a link to 'IPv6_FAQ'. The configuration is organized into several sections:

- Basic Config:** 'Connection type' is set to 'Static IPv6'.
- IPv6 WAN Setting:** Fields for 'WAN IPv6 Address', 'WAN Prefix Length', and 'WAN IPv6 Gateway'.
- IPv6 LAN Setting:** Fields for 'LAN IPv6 Address', 'LAN Prefix Length', and 'LAN IPv6 Prefix'. The 'Auto Configuration Setting' is set to 'Stateless'.
- IPv6 DNS Setting:** Fields for 'IPv6 DNS Server 1', 'IPv6 DNS Server 2', and 'IPv6 DNS Server 3'.
- Auto Configuration Setting:** 'Enable Router Advertisement' is set to 'Enable'.

An 'Apply' button is located at the bottom of the page.

So richten Sie IPv6 ein:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > IPv6**.
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.

4.3.3 Dual-WAN

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

- **Ausfallschutz:** Wählen Sie diesen Modus zur Nutzung des zweiten WAN als Reservenetzwerkzugriff.
- **Lastausgleich:** Wählen Sie diesen Modus, um die gleichzeitige Verwendung von Dual-WAN-Verbindungen für eine verbesserte Bandbreite und Zuverlässigkeit zu ermöglichen.
- **Failback zulassen:** Haken Sie das Kontrollkästchen an, damit die Internetverbindung automatisch zum primären WAN zurückwechseln kann, wenn das primäre WAN verfügbar ist.

Internet Connection | Dual WAN | Port Trigger | Virtual Server / Port Forwarding | DMZ | DDNS | NAT Passthrough

WAN - Dual WAN

4G-AC86U provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. [Dual WAN FAQ](#)

Basic Config

Enable Dual WAN ON

Primary WAN Mobile Broadband

Secondary WAN WAN

Dual WAN Mode **Fail Over** Allow failback

Hot-Standby DISABLE

Auto Network Detection

Detailed explanations are available on the [ASUS Support Site FAQ](#), which may help you use this function effectively.

Detect Interval Every 3 seconds

Failover Trigger Condition When the current WAN fails 12 continuous times, failover to Secondary WAN

Network Monitoring DNS Query Ping

Apply

- **Erkennungsintervall:** Legen Sie das Zeitintervall (in Sekunden) zwischen zwei Ping-Paketen fest.
- **Auslösungsbedingungen für Failover (Ausfallschutz):** Legen Sie die fortlaufenden Verbindungsversuche fest, ab wann das System die Failover/Failback-Aktion auslösen soll, nachdem die Ping-Test-Anzahl erreicht und keine Antwort von der Ziel-IP-Adresse empfangen wurde.

- **Netzwerküberwachung**

- 1) **DNS-Anfrage:** Wählen Sie diese Option aus, wenn Sie den Ziel-FQDN (Fully Qualified Domain Name) regelmäßig auflösen möchten.



- 2) **Ping:** Wählen Sie diese Option aus, wenn Sie eine Testpaket-Domain oder eine IP-Adresse regelmäßig anpingen möchten.



Wenn Schwierigkeiten mit der Internetverbindung aufgrund eines DHCP-Zuweisungsproblems auftreten, z. B. wenn die IP-Adresse abgelaufen ist, können Sie die DNS-Abfrage oder Ping aktivieren, um das Problem zu beheben.

4.3.4 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 Eingangsports, die nicht mit den Ausgangsports übereinstimmen.

The screenshot shows the 'WAN - Port Trigger' configuration page. At the top, there are navigation tabs: Internet Connection, Dual WAN, Port Trigger, Virtual Server / Port Forwarding, DMZ, DDNS, and NAT Passthrough. The 'Port Trigger' tab is selected. Below the tabs, the page title is 'WAN - Port Trigger'. A descriptive paragraph explains that Port Trigger allows temporarily opening data ports when LAN devices require unrestricted access to the Internet. It notes that there are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens specified ports all the time, while port trigger only opens the incoming port when a LAN device requests access. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port, while port trigger only allows one client at a time to access the open port. A link for 'Port Trigger FAQ' is provided.

Below the description is a 'Basic Config' section with two fields: 'Enable Port Trigger' (radio buttons for Yes and No, with 'Yes' selected) and 'Well-Known Applications' (a dropdown menu showing 'Please select').

Below that is a 'Trigger Port List (Max Limit : 32)' section. It contains a table with the following columns: Description, Trigger Port, Protocol, Incoming Port, Protocol, and Add / Delete. The table is currently empty, with the text 'No data in table.' displayed below it. An 'Apply' button is located at the bottom of the page.

Description	Trigger Port	Protocol	Incoming Port	Protocol	Add / Delete
		TCP		TCP	+

So richten Sie die Portauslösung ein:

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

4. Geben Sie in der Tabelle der **Trigger Port List (Auslöserportliste)** die folgenden Informationen ein:
 - **Beschreibung:** Geben Sie einen kurzen Namen oder eine Beschreibung für den Dienst 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 die Liste auf die **Add (Hinzufügen)** -Schaltfläche. Klicken Sie zum Entfernen eines Portauslöserintrags aus der Liste auf **Delete (Löschen)** .
6. Klicken Sie zum Abschluss auf **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 aktiviert 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, wann die zugehörige Anwendung beendet wurde.
 - Die Portauslösung ermöglicht lediglich einem Client im Netzwerk, einen bestimmten Dienst und einen bestimmten Eingangspport gleichzeitig zu nutzen.
 - Sie können nicht die selbe Anwendung benutzen, um einen Port in mehr als einem PC zur gleichen Zeit auszulösen. Der Router wird den Port nur zurück zum vorherigen Computer verweisen, um dem Router eine Anfrage/Auslösung zu senden.
-

4.3.5 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 einzurichten, können PCs außerhalb des Netzwerks auf bestimmte Dienste zugreifen, die von einem PC in Ihrem eigenen Netzwerk bereitgestellt werden.

HINWEIS: Wenn die Portweiterleitung aktiviert 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.

Internet Connection Dual WAN Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough

WAN - Virtual Server / Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.

If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port empty.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with 4G-AC55U's web user interface.
- When you set 20:21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with 4G-AC55U's native FTP server.

[Virtual_Server / Port Forwarding_FAQ](#)

Basic Config

Enable Port Forwarding Yes No

Famous Server List

Famous Game List

FTP Server Port

Port Forwarding List (Max Limit : 32)

Service Name	Port Range	Local IP	Local Port	Protocol	Add / Delete
				TCP	<input type="button" value="⊕"/>

No data in table.

So richten Sie die Portweiterleitung ein:

1. Wechseln Sie im Navigationspanel zu **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 beliebten Spiele, auf die Sie zugreifen möchten. Dieses Element listet den erforderlichen Port auf, der zur Ausführung Ihres ausgewählten Online-Spiels nötig ist.
5. Geben Sie in der Tabelle **Port Forwarding List (Portweiterleitungsliste)** die folgenden Informationen ein:
 - **Dienstname:** Geben Sie einen Dienstenamen ein.
 - **Portbereich:** Wenn Sie einen Portbereich für Clients im selben Netzwerk festlegen möchten, geben Sie den Dienstenamen, den Portbereich (beispielsweise 10200:10300) 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 WANs festlegen, würde Ihr HTTP-Server/ Webserver mit der Web-Benutzeroberfläche des Routers in Konflikt geraten.
- 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)**.

6. Klicken Sie zur Eingabe der Portauslöserinformationen in die Liste auf **Add (Hinzufügen)** . Klicken Sie zum Entfernen eines Portauslöseireintrags aus der Liste auf **Delete (Löschen)** .
7. Klicken Sie zum Abschluss auf **Übernehmen**.

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 mit dem ASUS Router verbunden sein.
- Vom Internet-Client aus nutzen Sie die WAN-IP des Routers 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 Eingangsports nicht ständig geöffnet bleiben. Die Ports werden nur dann geöffnet, wenn eine Anwendung eine abgehende Verbindung über den Auslösungsport aufbaut.

4.3.6 DMZ

Die virtuelle DMZ 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 Domain-, 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.

The screenshot shows the 'WAN - DMZ' configuration page. At the top, there are navigation tabs: Internet Connection, Dual WAN, Port Trigger, Virtual Server / Port Forwarding, DMZ, DDNS, and NAT Passthrough. The 'DMZ' tab is selected. Below the tabs, the page title is 'WAN - DMZ'. The main content area contains the following text: 'Virtual DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set. It is useful while you run some applications that use uncerntained incoming ports. Please use it carefully. Special Applications: Some applications require special handler against NAT. These special handlers are disabled in default. [DMZ_FAQ](#)'. Below this text, there is a section for 'Enable DMZ' with a radio button set to 'Yes' and 'No'. Below that, there is a text input field for 'IP Address of Exposed Station'. At the bottom of the form, there is an 'Apply' button.

So richten Sie eine DMZ ein:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > WAN > DMZ**.
2. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **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 **Übernehmen**.

4.3.7 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.

The screenshot shows the 'WAN - DDNS' configuration page. At the top, there is a navigation bar with tabs: Internet Connection, Dual WAN, Port Trigger, Virtual Server / Port Forwarding, DMZ, DDNS (selected), and NAT Passthrough. Below the navigation bar, the page title is 'WAN - DDNS'. The main content area contains a description of DDNS: 'DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.' Below this, a note states: 'The wireless router currently uses a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x). This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.' The configuration section includes three fields: 'Enable the DDNS Client' with a radio button set to 'Yes', 'Server' with a dropdown menu showing 'WWW.ASUS.COM', and 'Host Name' with a text input field containing 'Key in the name' and a suffix '.asuscomm.com'. An 'Apply' button is located at the bottom of the configuration section.

So richten Sie DDNS ein:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > WAN > DDNS**.
2. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **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 Host-Name:** Wählen Sie ASUS DDNS oder einen anderen 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.
-

4.3.8 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 standardmäßig aktiviert.

So aktivieren/deaktivieren Sie die NAT-Durchleitungseinstellungen:

1. Wechseln Sie zum Register **Advanced Settings (Erweiterte Einstellungen) > WAN > NAT Passthrough (NAT-Durchleitung)**.
2. Wählen Sie **Enable (Aktivieren)** oder **Disable (Deaktivieren)** für einen spezifischen Datenverkehr, der durch die NAT Firewall geleitet wird.
3. Klicken Sie zum Abschluss auf **Übernehmen**.

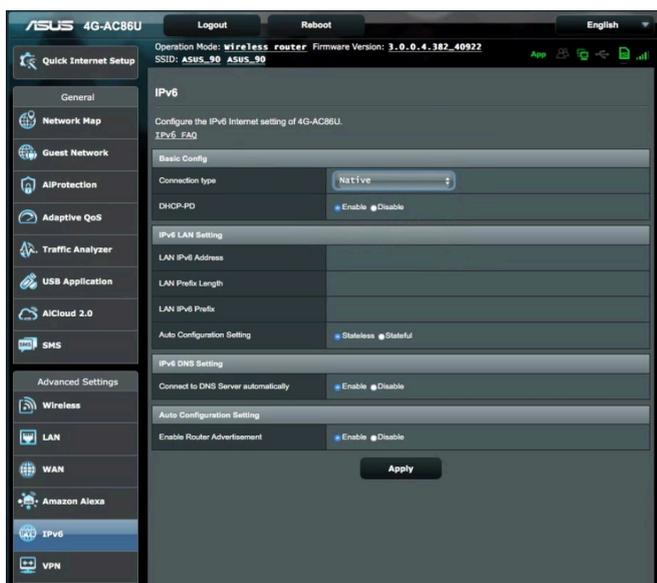
The screenshot shows the 'WAN - NAT Passthrough' configuration page. At the top, there are navigation tabs: 'Internet Connection', 'Dual WAN', 'Port Trigger', 'Virtual Server / Port Forwarding', 'DMZ', 'DDNS', and 'NAT Passthrough'. The main heading is 'WAN - NAT Passthrough'. Below it, a description reads: 'Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.' The configuration table has the following rows:

PPTP Passthrough	Enable
L2TP Passthrough	Enable
IPSec Passthrough	Enable
RTSP Passthrough	Enable
H.323 Passthrough	Enable
SIP Passthrough	Enable
PPPoE Relay	Disable
FTP_ALG Port	2021

An 'Apply' button is located at the bottom center of the page.

4.4 IPv6

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



So richten Sie IPv6 ein:

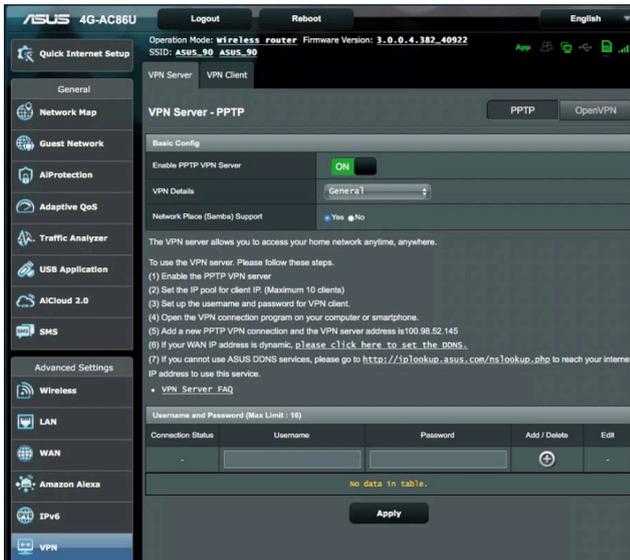
1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > IPv6**.
2. Wählen Sie Ihren **Connection Type (Verbindungstyp)**. Die Konfigurationsoptionen variieren je nach ausgewähltem Verbindungstyp.
3. Legen Sie Ihre IPv6-LAN- und DNS-Einstellungen fest.
4. Klicken Sie auf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

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



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

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > VPN Server**.
2. Wählen Sie im Feld **Enable PPTP VPN Server (PPTP VPN-Server aktivieren)** die Option **ON (Ein)** aus, um den PPTP VPN-Server zu aktivieren.
3. Wählen Sie aus der **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 standardmäßig bereits aktiviert.

4.6.1 Allgemein

So richten Sie grundlegende Firewall-Einstellungen ein:

1. Wechseln Sie im Navigationspanel zu **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-Attacken (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 im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Firewall > 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 im Navigationspanel zu **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 im Navigationspanel zu **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 angegebenen Netzwerkdienste. **Die White List (Weiße Liste)** beschränkt den Zugriff auf die angegebenen Netzwerkdienste.
4. Legen Sie fest, zu welchen Tagen und Uhrzeiten die Filter aktiv sein sollen.
5. Zum Festlegen eines Netzwerkdienstes zum Filtern geben Sie Quell-IP, Ziel-IP, Portbereich und Protokoll an. Klicken Sie auf die Schaltfläche .
6. Klicken Sie auf **Apply (Übernehmen)**.

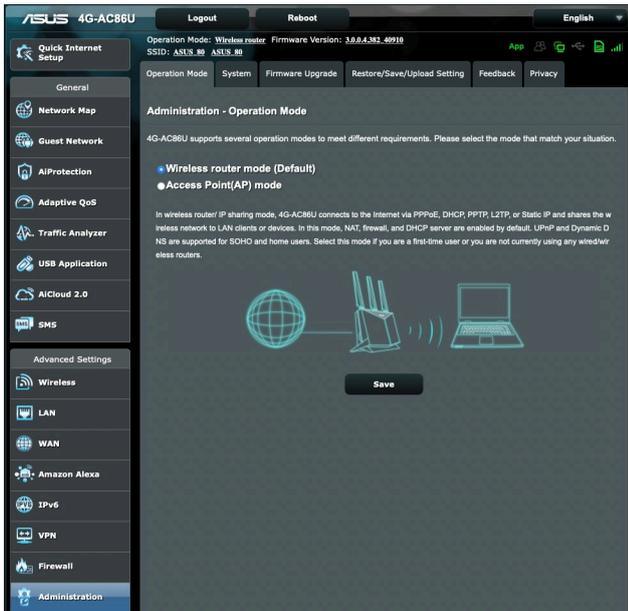
4.6.5 IPv6-Firewall

Standardmäßig blockiert Ihr ASUS WLAN-Router den gesamten unaufgefordert eingehenden Datenverkehr. Die IPv6-Firewall-Funktion erlaubt eingehendem 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 im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Administration > Operation Mode (Betriebsmodus)**.
2. Wählen Sie einen der folgenden Betriebsmodi:
 - **WLAN-Router-Modus (Standardeinstellung)**:: Im WLAN-Router-Modus verbindet sich der WLAN-Router mit dem Internet und ermöglicht Netzwerkgeräten Internetzugang über das eigene, lokale Netzwerk.
 - **Access-Point-Modus (AP-Modus)**: In diesem Modus erstellt der Router ein neues WLAN im bereits vorhandenen Netzwerk.
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.

Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting	Feedback	Privacy
Administration - System					
Change the router login password, time zone, and NTP server settings.					
Change the router login password					
Router Login Name	<input type="text" value="admin"/>				
New password	<input type="password"/>				
Retype Password	<input type="password"/> <input type="checkbox"/> Show password				
Enable Login Captcha	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Basic Config					
Time Zone	<input type="text" value="(GMT) Greenwich Mean Time"/> <input type="button" value="v"/> <small>* Reminder: The System time zone is different from your locale setting.</small>				
NTP Server	<input type="text" value="pool.ntp.org"/>				NTP Link
Network Monitoring	<input checked="" type="checkbox"/> DNS Query <input type="checkbox"/> Ping				
Auto Logout	<input type="text" value="30"/> minute(s) (Disable : 0)				
Enable WAN down browser redirect notice	<input checked="" type="radio"/> Yes <input type="radio"/> No				
WPS Button behavior	<input checked="" type="radio"/> Activate WPS <input type="radio"/> Toggle Radio <input type="radio"/> Turn LED On/Off				
Enable Reboot Scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Service					
Enable Telnet	<input checked="" type="radio"/> Yes <input type="radio"/> No <small>* Due to security concerns, we suggest using SSH instead of Telnet. SSH provides an encrypted network communication.</small>				
Enable SSH	<input type="text" value="No"/> <input type="button" value="v"/>				
Idle Timeout	<input type="text" value="20"/> minute(s) (Disable : 0)				
Local Access Config					
Authentication Method	<input type="text" value="HTTP"/> <input type="button" value="v"/>				
Remote Access Config					
Enable Web Access from WAN	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Enable Access Restrictions	<input type="radio"/> Yes <input checked="" type="radio"/> No				
<input type="button" value="Apply"/>					

So nehmen Sie Systemeinstellungen vor:

1. Wechseln Sie im Navigationspanel zu **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.
 - **Automatisches Abmelden:** Das System meldet automatisch die Administratorseite nach einer Zeit der Inaktivität ab. Um das automatische Abmelden zu deaktivieren, setzen Sie den Wert auf 0.
 - **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 beide Protokolle 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.
 - **Zugriffsbeschränkungen aktivieren:** Wählen Sie **Yes (Ja)**, um eine Whitelist festzulegen, mit der der Administrator den Zugriff nur auf vertrauenswürdige IP-Adressen beschränken und kontrollieren kann.
 - a) **Nur bestimmte IP-Adressen 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.
 - b) **Bestimmte IP-Adressen:** Geben Sie die WAN-IP-Adressen von Netzwerkgeräten ein, die auf die Einstellungen des WLAN-Routers zugreifen dürfen. Auf dieser Client-Liste dürfen maximal 4 IP-Adressen hinzugefügt werden.
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

Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting	Feedback	Privacy
Administration - Firmware Upgrade					
Note:					
1. The latest firmware version includes updates from the previous version.					
2. Configuration parameters will keep their settings during the firmware update process.					
3. In case the upgrade process fails, 4G-AC86U enters the emergency mode automatically. The LED signals at the front of 4G-AC86U will indicate such a situation. Please visit ASUS Download Center to download ASUS Device Discovery utility.					
4. Get the latest firmware version from the ASUS Support site: https://www.asus.com/support/					
Firmware Version					
Product ID	4G-AC86U				
Signature version	2.220 Updated : 2021/03/16 17:01			Check	
Firmware Version	3.0.0.4.382_40910-g755bc74			Check	
New Firmware File	<input type="button" value="選擇檔案"/> 尚未選取檔案			Upload	
4G Modem Firmware					
Modem Firmware version	EM12GPAR01A18M4G				
New Modem Firmware	<input type="button" value="選擇檔案"/> 尚未選取檔案			Upload	

So aktualisieren Sie die Router- oder 4G-Modem-Firmware:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Administration > Firmware Upgrade (Firmware-Aktualisierung)**.
2. Klicken Sie im Feld **New Firmware File (Neue Firmware-Datei)** oder **New Modem Firmware (Neue Modem-Firmware)** 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 WLAN-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 (Firmware-Wiederherstellung)**.

4.7.4 Wiederherstellen/Speichern/Hochladen der Einstellungen

Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting	Feedback	Privacy
Administration - Restore/Save/Upload Setting					
This function allows you to save current settings of 4G-AC86U to a file, or load settings from a file.					
Factory default	Restore	<input type="checkbox"/> Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer, and Web History.			
Save setting	Save setting	<input type="checkbox"/> Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router.			
Restore setting	Upload				

So werden die Einstellungen des WLAN-Routers wiederhergestellt/gespeichert/hochgeladen:

1. Wechseln Sie im Navigationspanel zu **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 setting (Einstellung speichern)**, öffnen den Ordner, in dem Sie die Datei ablegen möchten, anschließend klicken Sie auf **Save (Speichern)**.
 - Um ältere Systemeinstellungen zu laden, klicken Sie auf **Browse (Durchsuchen)**, um die wiederherzustellende Systemdatei zu wählen, klicken Sie dann auf **Upload (Hochladen)**.

WICHTIG! 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.

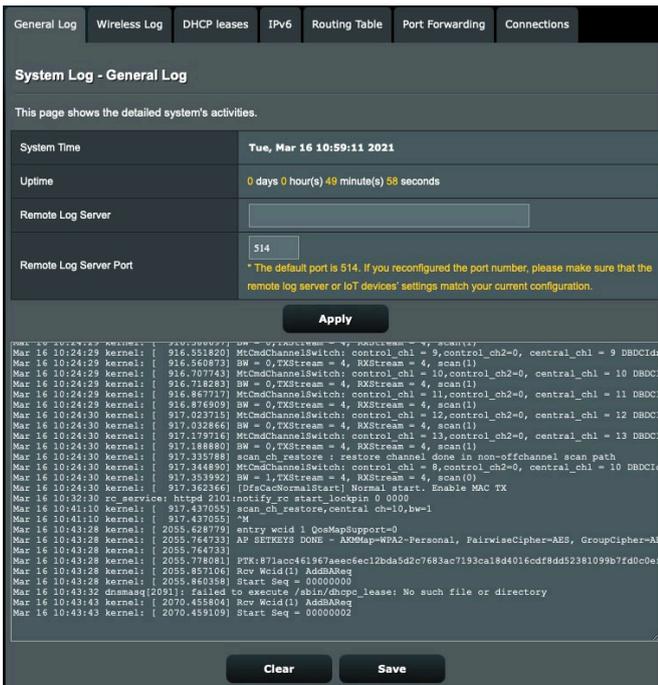
4.8 Systemprotokoll

Systemprotokoll enthält Aufzeichnungen der Netzwerkaktivitäten.

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

So zeigen Sie das Systemprotokoll an:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > System Log (Systemprotokoll)**.
2. Sie können sich Netzwerkaktivitäten in folgenden Registern anschauen:
 - Allgemeines Protokoll
 - WLAN-Protokoll
 - DHCP-Zuweisungen
 - IPv6 (WAN und LAN Netzwerkinformationen)
 - Routentabelle
 - Portweiterleitung
 - Anschlüsse



4.9 Liste unterstützter Funktionen für Ethernet, WAN, mobiles Breitband

Der WLAN-Router unterstützt kabelgebundenes WAN und mobiles Breitband-WAN im Failover und Failback Modus. Das mobile Breitband-WAN wird sowohl zum Internetzugang als auch als WAN-Backup-Schnittstelle verwendet. LAN, WAN, VPN und Firewall unterstützen unterschiedliche Funktionen. Sehen Sie eine Gegenüberstellung in der untenstehenden Tabelle.

	Kabelge- bundenes WAN	LAN als WAN	Mobiles Breitband
LAN			
IPTV	V	N/A	N/A
Switch Control >> NAT-Beschleunigung (nur IPv4)	V	N/A	N/A
Switch Control >> Jumbo Frame	V	N/A	N/A
WAN			
IPv6	V	V	V (1)
Portauslösung	V	V	V (2)
Virtueller Server / Portweiterleitung	V	V	V (2)
DMZ	V	V	V (2)
DDNS	V	V	V (2)
NAT-Durchleitung	V	V	V (2)
Traffic Manager			
QoS (Quality of Service)	V	V	V
Firewall			
Allgemein	V	V	V
URL-Filter	V	V	V
Schlüsselwortfilter	V	V	V
Netzwerkdienstefilter	V	V	V
IPv6-Firewall	V	V	N/A
Administration			
System >> Internetzugriff aus dem WAN aktivieren	V	V	V (2)

Anwendungen			
AiCloud Zugriff vom WAN	V	V	V (2)
VPN-Server	V	V	V (2)
FTP-Server	V	V	V (2)

HINWEISE:

V (1): Das mobile WAN hat eine separate Konfiguration auf seiner Konfigurationsseite.

V (2): In den meisten Fällen sorgt der Internetdienst dafür, dass eine private IP für das mobile Breitband versendet wird, was dazu führt, dass seitens des WANs nicht auf den WAN-Dienst zugegriffen werden kann.

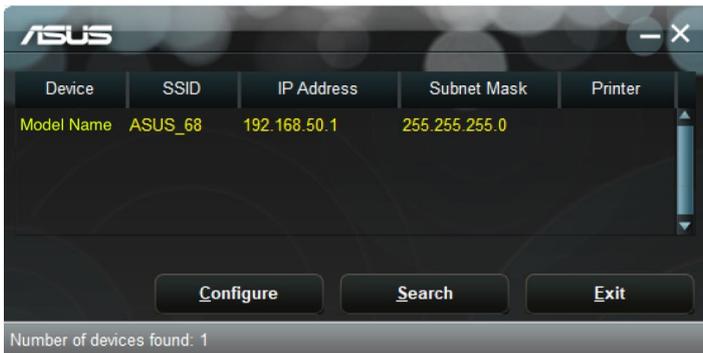
5 Dienstprogramme

HINWEIS: Laden Sie die Dienstprogramme des WLAN-Routers von der ASUS-Webseite unter <https://www.asus.com/support/Download-Center/> herunter und installieren Sie sie.

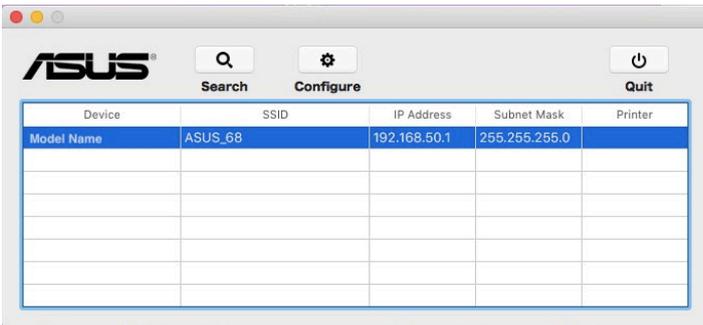
5.1 Device Discovery

Device Discovery (Geräteerkennung) ist ein ASUS WLAN-Dienstprogramm, das einen ASUS WLAN-Router erkennen kann und Ihnen die Konfiguration der WLAN-Einstellungen des Gerätes ermöglicht.

Windows®:



Mac OS:

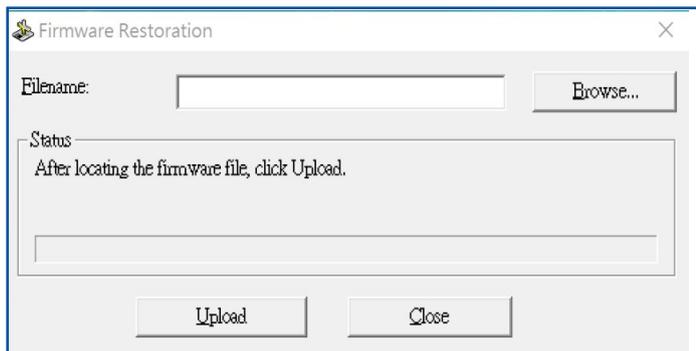


HINWEIS: Wenn Sie beim Router den Access Point (Zugangspunkt)-Modus einstellen, müssen Sie die Device Discovery (Geräteerkennung) verwenden, um die IP-Adresse des Routers zu erhalten.

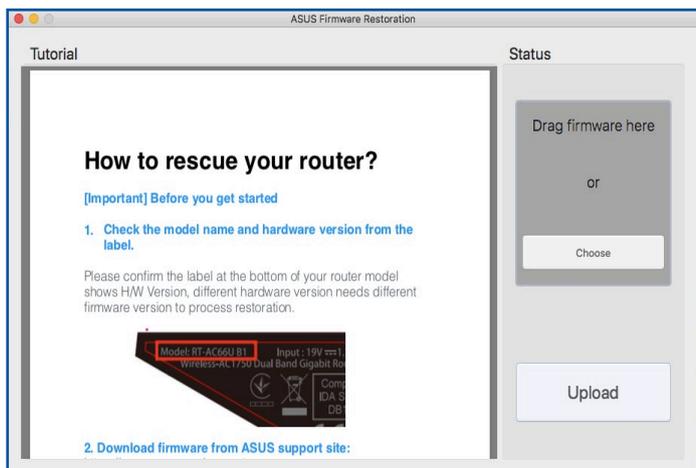
5.2 Firmware Restoration

Firmware Restoration (Firmware-Wiederherstellung) wird bei einem ASUS WLAN-Router verwendet, welcher während der Firmware-Aktualisierung ausgefallen ist. Es lädt die von Ihnen angegebene Firmware hoch. Der Vorgang dauert etwa drei bis vier Minuten.

Windows®:



Mac OS:



WICHTIG! Bevor Sie die Anwendung Firmware Restoration verwenden, starten Sie den Rettungsmodus auf Ihrem Router.

So starten Sie den Rettungsmodus und verwenden das Dienstprogramm Firmware Restoration:

1. Trennen Sie die Stromversorgung vom WLAN-Router.
2. Halten Sie die Reset-Taste auf der Rückseite gedrückt und stellen gleichzeitig die Stromversorgung des WLAN-Routers wieder her. Lassen Sie die Reset-Taste wieder los, sobald die Betriebs-LED auf der Frontseite langsam blinkt. Dies zeigt an, dass sich der WLAN-Router im Rettungsmodus befindet.
3. Legen Sie eine statische IP für Ihren 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 auf Ihrem Computer-Desktop auf: **Start > All Programs (Alle Programme) > ASUS Utility (ASUS Dienstprogramm) > Wireless Router (WLAN-Router) > Firmware Restoration (Firmware-Wiederherstellung)**.
5. Geben Sie eine Firmware-Datei an und klicken auf **Upload (Hochladen)**.

HINWEIS: Diese Anwendung ist kein Firmware-Aktualisierungsprogramm und kann nicht auf einem betriebsfähigen ASUS WLAN-Router verwendet werden. Eine normale Firmwareaktualisierung muss über die grafische Benutzeroberfläche 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 Druckerservers. So können Ihre Clients im Netzwerk kabellos drucken und auf Dateien zugreifen.



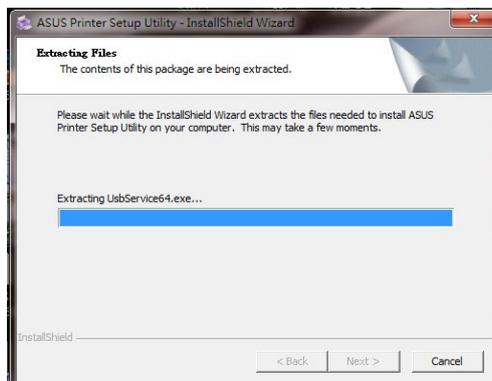
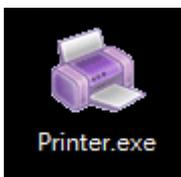
So richten Sie die EZ-Druckerfreigabe ein:

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

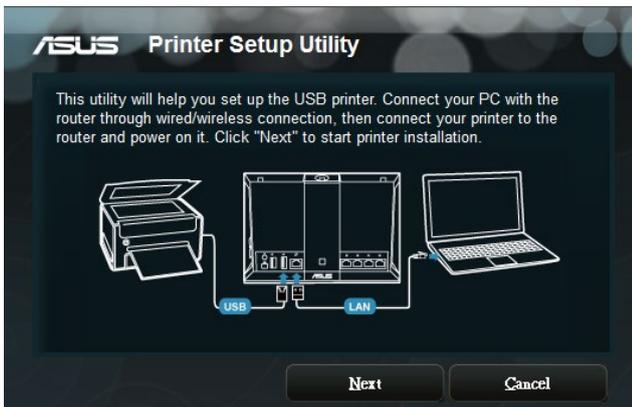


HINWEIS: Die Netzwerkdruckersoftware wird nur unter Windows® XP, Windows® Vista und Windows® 7 unterstützt. Zur Installation unter Mac OS wählen Sie **Use LPR protocol for sharing printer (LPR-Protokoll zur Druckerfreigabe verwenden)**.

3. Entpacken Sie die heruntergeladene Datei und klicken auf das Druckersymbol, um das Netzwerkdrucker-Einrichtungsprogramm auszuführen.



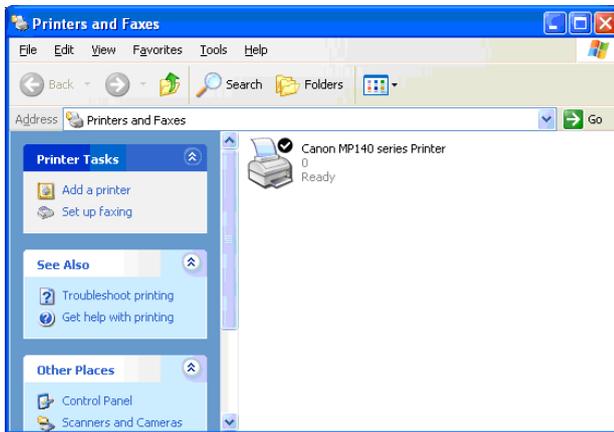
4. Folgen Sie den Bildschirmanweisungen, um Ihre Hardware einzurichten und klicken dann auf **Next (Weiter)**.



5. Warten Sie ein paar Minuten auf den Abschluss der Grundeinrichtung. Klicken Sie auf **Next (Weiter)**.
6. Klicken Sie auf **Finish (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 den Drucker benutzen.



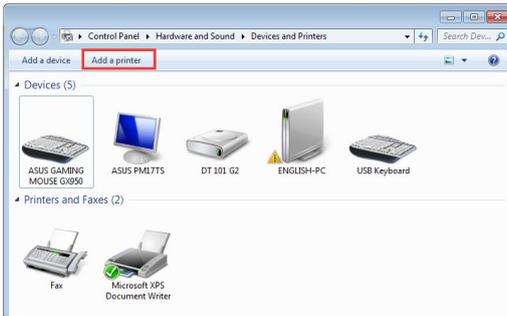
5.3.2 LPR zur Druckerfreigabe verwenden

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

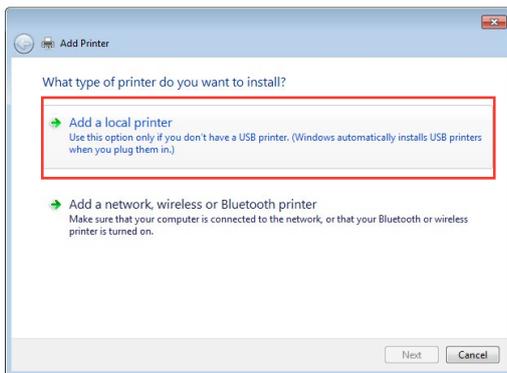
LPR-Drucker freigeben

So geben Sie einen LPR-Drucker frei:

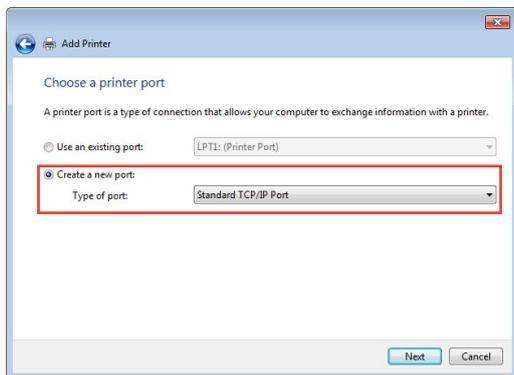
1. Klicken Sie auf dem Windows®-Desktop auf **Start > Devices and Printers (Geräte und Drucker) > Add a printer (Drucker hinzufügen)**, um den **Add Printer Wizard (Druckerhinzufügen-Assistent)** auszuführen.



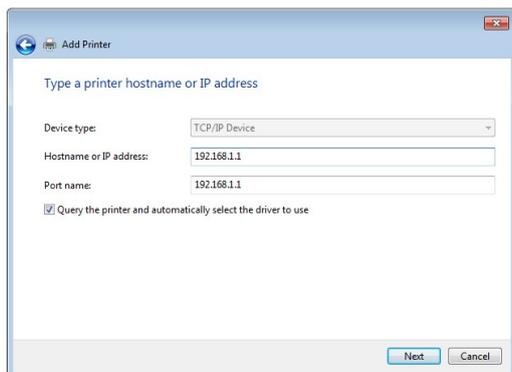
2. Wählen Sie **Add a local printer (Lokalen Drucker hinzufügen)**, klicken Sie dann auf **Next (Weiter)**.



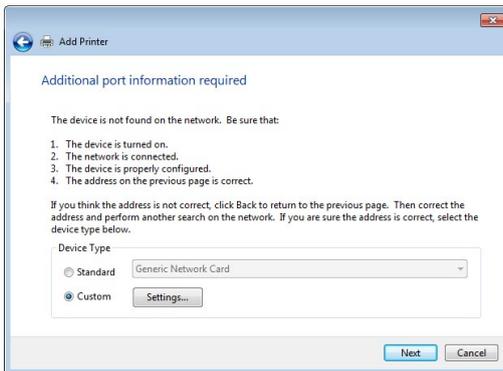
3. Wählen Sie **Create a new port (Neuen Port erstellen)**, stellen Sie dann den **Type of Port (Porttyp)** auf **Standard TCP/IP Port** ein. Klicken Sie auf **New Port (Neuer Port)**.



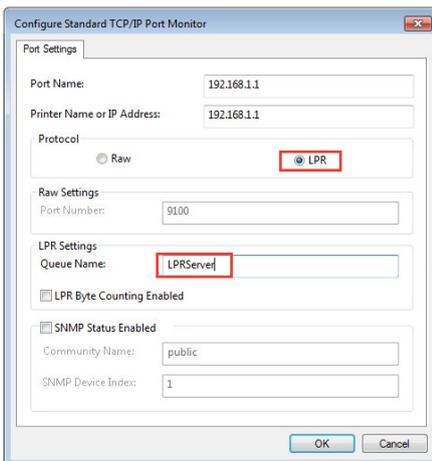
4. Tragen Sie die IP-Adresse des WLAN-Routers in das Feld **Hostname or IP address (Hostname oder IP-Adresse)** ein, klicken Sie dann auf **Next (Weiter)**.



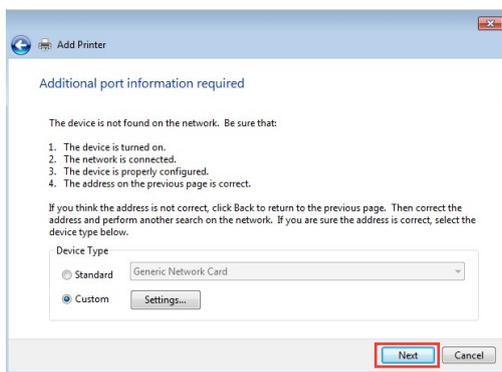
5. Wählen Sie **Custom (Benutzerdefiniert)**, klicken Sie dann auf **Settings (Einstellungen)**.



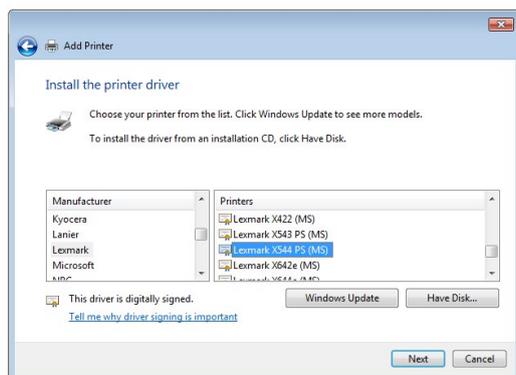
6. Stellen Sie das **Protocol (Protokoll)** auf **LPR** ein. Tragen Sie **LPRServer** in das Feld **Queue Name (Warteschlangenname)** ein, klicken Sie dann zum Fortsetzen auf **OK**.



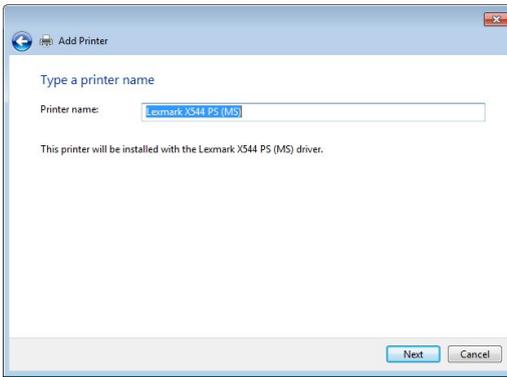
7. Klicken Sie zum Abschluss der Standard-TCP/IP-Porteinstellungen auf **Next (Weiter)**.



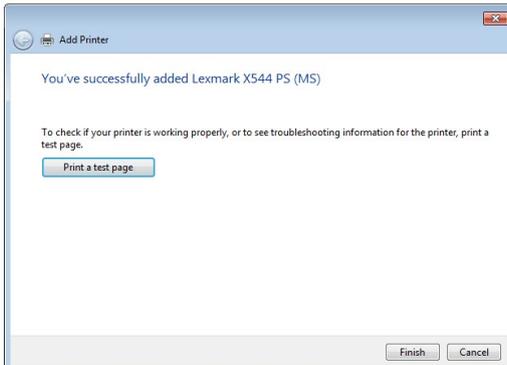
8. Installieren Sie den Druckertreiber aus der Anbieterliste. Falls Ihr Drucker nicht in der Liste aufgeführt wird, klicken Sie zur manuellen Installation der Druckertreiber von CD oder aus einer Datei auf **Have Disk (Datenträger)**.



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



10. Klicken Sie auf **Finish (Fertigstellen)**, um die Installation abzuschließen.



5.4 Download Master

Download Master ist ein Dienstprogramm, mit dem Sie Dateien sogar bei ausgeschalteten Laptops oder sonstigen Geräten herunterladen können.

HINWEIS: Sie benötigen ein an den WLAN-Router angeschlossenes USB-Gerät, um Download Master zu benutzen.

So verwenden Sie Download Master:

1. Klicken Sie auf **General (Allgemein) > USB application (USB-Anwendungen) > Download Master**, um die Anwendung automatisch herunterzuladen und zu installieren.

HINWEIS: Wenn Sie mehr als ein USB-Laufwerk haben, wählen Sie das USB-Gerät, auf das Sie die Dateien herunterladen möchten.



2. Nachdem der Download-Vorgang abgeschlossen ist, klicken Sie auf das Download Master-Symbol, um das Dienstprogramm zu starten.
3. Klicken Sie auf **Add (Hinzufügen)**, um eine Download-Aufgabe hinzuzufügen.



4. Wählen Sie einen Download-Typ, wie BitTorrent, HTTP oder FTP. Stellen Sie eine Torrent-Datei oder eine URL bereit, um mit dem Herunterladen zu beginnen.

HINWEIS: Einzelheiten über Bit Torrent finden Sie im Abschnitt **5.4.1 Bit Torrent-Download-Einstellungen konfigurieren**.

5. Verwenden Sie die Navigationsleiste, um die **Allgemeinen Einstellungen** zu konfigurieren.
 - Sie können den Download-Zeitplan durch Auswahl der Download-Optionen **Immediately (Sofort)** oder **At Scheduled Time (Zum festgelegten Zeitpunkt)** bestimmen.

<input type="radio"/> Immediately <input checked="" type="radio"/> At Scheduled Time	
Date to Enable Download (week days)	<input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri
Time of Day to Enable Download	00 : 00 - 23 : 59
Date to Enable Download (weekend)	<input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun
Time of Day to Enable Download	00 : 00 - 23 : 59

- Standardmäßig werden die Informationen zu den Download-Aufgaben alle 5 Sekunden aktualisiert. Die Option **Refresh rate (Aktualisierungsrate)** ermöglicht es Ihnen, den Zeitraum für die Aktualisierung der Informationen zu ändern.
- Sie können den Verzeichnispfad aus dem **Download to (Herunterladen auf)**-Feld als Ablageort für heruntergeladene Dateien wählen.
- Die standardmäßige Port-Nummer für die **DownloadMaster**-Administratorseite ist 8081. Falls die Port-Nummer mit einer anderen Anwendung in Konflikt steht, können Sie das hier ändern.
- Um den **DownloadMaster** vom Internet aus zu verwalten, können Sie **WAN network (WAN Netzwerk)** auf **ON (Ein)** schieben.
- Falls Ihre Netzwerkressourcen knapp sind, empfehlen wir Ihnen, **Keep seeding after task completed (Nach Beenden der Aufgabe weiter Seeden)** durch Schieben des Reglers auf **OFF (Aus)** zu deaktivieren.

ASUS Logout English

Task

Task

Settings

General

Bit Torrent

NZB

eMule

General Setting

Download Schedule

Immediately At Scheduled Time

Download to /tmp/mnt/sda2/Download2/Complete Browse

Refresh rate 5 Seconds

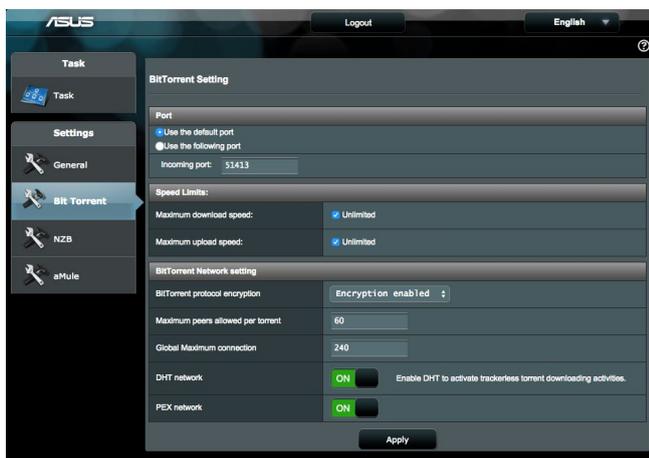
DownloadMaster Port 8081

WAN network OFF Enable/disable the WAN connection.

Keep seeding after task completed ON

Apply

5.4.1 Bit Torrent-Download-Einstellungen konfigurieren

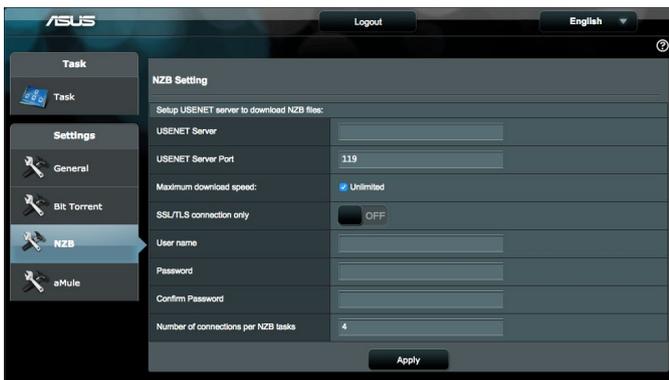


So konfigurieren Sie die Bit Torrent-Download-Einstellungen:

1. Klicken Sie im Download Master-Navigationspanel auf **Bit Torrent**, um die Seite **Bit Torrent Setting (Bit Torrent-Einstellungen)** einzublenden.
2. Wählen Sie einen bestimmten Port oder verwenden Sie den standardmäßigen Port für Ihre Download-Aufgabe.
3. Um eine Überlastung des Netzwerks zu verhindern, können Sie die maximalen Upload- und Download-Geschwindigkeiten unter **Speed Limits (Geschwindigkeitsbegrenzungen)** beschränken.
4. Sie können die maximale Anzahl zulässiger Peers begrenzen und die Dateiverschlüsselung während der Downloads aktivieren oder deaktivieren.
5. Das Aktivieren des DHT (Distributed Hash Table) Netzwerks kann die Download-Geschwindigkeiten und Übertragungsraten verbessern, indem eine Domain zum Teilen von Informationen gemeinsam genutzt wird. Um das DHT Netzwerk zu nutzen, muss Ihr WLAN-Router auch bestimmte Informationen mit anderen Mitgliedern im Netzwerk teilen
6. Das Aktivieren des PEX (Peer Exchange) Netzwerks zum Austausch von Peer-Informationen zwischen zwei verbundenen Peers hilft Ihnen dabei, weitere Peers im Netzwerk zu versammeln.

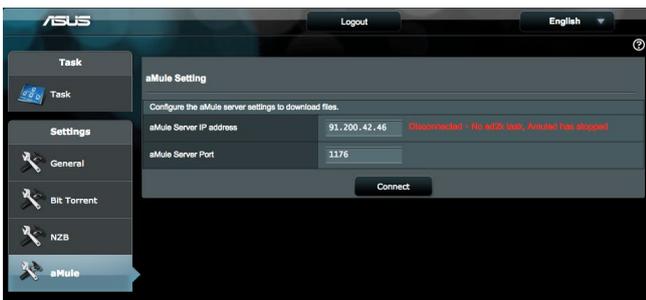
5.4.2 NZB Einstellungen

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



5.4.3 eMule Einstellungen

Sie können einen eMule-Server zum Herunterladen von Dateien von eMule einrichten. Klicken Sie nach der Eingabe der eMule-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-Kundendienstseite: <https://www.asus.com/support> – 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.

Aktualisieren Sie die Firmware auf die neueste Version.

1. Starten Sie die grafische Benutzeroberfläche. Wechseln Sie zum Register **Advanced Settings (Erweiterte Einstellungen)** > **Administration** > **Firmware Upgrade (Firmware-Aktualisierung)**. Schauen Sie mit einem Klick auf **Check (Prüfen)** nach, ob eine aktualisierte Firmware zum Abruf bereit steht.



The screenshot shows the 'Administration - Firmware Upgrade' page. At the top, there are navigation tabs: 'Operation Mode', 'System', 'Firmware Upgrade', 'Restore/Save/Upload Setting', 'Feedback', and 'Privacy'. The main content area has a 'Note' section with four instructions: 1. The latest firmware version includes previous updates. 2. For a configuration parameter existing both in the old and new firmware, its setting will be kept during the upgrade process. 3. When the upgrade fails, ASUS router will enter the emergency mode automatically. The LED in front of router will show corresponding signals. Please visit [ASUS Download Center](#) to download ASUS Device Discovery utility. 4. Get the latest firmware version from ASUS Support site at <https://www.asus.com/support/>. Below the note is a table with the following data:

Firmware Version	
Product ID	Model Name
Firmware Version	3.0.0.4.382_51700-g6b467b5 <input type="button" value="Check"/>
New Firmware File	<input type="button" value="選擇檔案"/> 未選擇任何檔案 <input type="button" value="Upload"/>

2. Sofern eine aktualisierte Firmware zur Verfügung steht, besuchen Sie die ASUS-Internetseite unter <http://www.asus.com/support> und laden Sie die aktuellste Firmware herunter.

3. Klicken Sie auf der **Firmware Upgrade (Firmware-Aktualisierung)**-Seite auf **Browse (Durchsuchen)**, suchen Sie dann 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 Ihres Computers zu den Einstellungen Ihres Routers passen.

- Wenn Sie Ihren Computer kabellos mit dem Router verbinden, vergewissern Sie sich, dass SSID (der WLAN-Name), 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-Dienstleister setzen voraus, dass die MAC-Adresse des Computers verwendet wird, der anfangs zur Kontoregistrierung genutzt wurde. Sie können die MAC-Adresse über die grafische Benutzeroberfläche abrufen: Wechseln Sie zur Seite **Network Map (Netzwerkübersicht)** > **Clients**, setzen Sie dann unter **Client Status** den Mauszeiger auf den Namen Ihres Gerätes.



6.2 Häufig gestellte Fragen (FAQs)

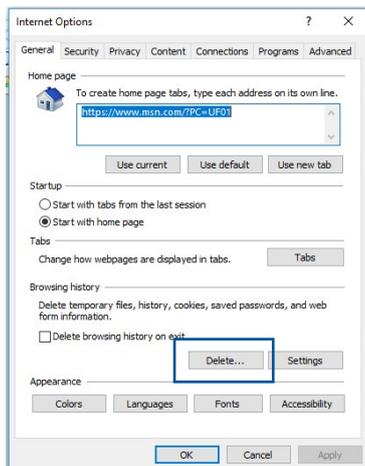
Ich kann per Webbrowser nicht auf die grafische Benutzeroberfläche des Routers zugreifen.

- 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 führen Sie die folgenden Schritte aus:

1. Starten Sie den Internet Explorer, klicken Sie dann auf **Tools (Extras) > Internet Options (Internetoptionen)**.

2. Klicken Sie auf das **General (Allgemein)-Register**, klicken Sie dann unter **Browsing history (Browserverlauf)**

auf **Delete... (Löschen...)**, wählen Sie anschließend **Temporary Internet files and website files (Temporäre Internetdateien und Webseitendateien)** und **Cookies and website data (Cookies und Webseiteninformationen)**, klicken Sie dann auf **Delete (Löschen)**.



HINWEISE:

- Die Schritte zum Löschen von Cookies und temporären Dateien sind von Browser zu Browser verschieden.
- 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 Client kann keine WLAN-Verbindung mit dem Router herstellen.

HINWEIS: Falls 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 WLAN-Client.
 - Stellen Sie die Antennen des Routers optimal ein; schauen Sie sich dazu den Abschnitt **1.4 Ihren Router aufstellen** an.
- **DHCP-Server wurde deaktiviert:**
 1. Starten Sie die grafische Benutzeroberfläche. Wechseln Sie zu **General (Allgemein) > Network Map (Netzwerkübersicht) > Clients**, suchen Sie dann 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**, 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 (WLAN) > General (Allgemein)**, wählen **No (Nein)** 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/Ihrer Region 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 zurücksetzen. 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 kabelgebundene 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 Ihr Netzwerk 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** aufgelistet sein, entfernen Sie das Gerät mit der **Delete (Löschen)**-Schaltfläche oder passen Sie die Zeitmanagement-Einstellungen entsprechend an.
- Falls Sie nach wie vor nicht auf das Internet zugreifen können, starten Sie Ihren Computer neu; anschließend überprüfen Sie IP-Adresse und Gateway-Adresse des Netzwerks.
- Schauen Sie sich die Statusanzeigen am ADSL-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.

Das mobile Breitband-Internet ist nicht zugänglich.

- Stecken Sie eine SIM-Karte mit einem Vertrag für ein Datenabonnement in den USIM-Kartensteckplatz. Die LED für das mobile 3G/4G Breitband leuchtet und zeigt damit an, dass die SIM-Karte richtig installiert ist.
- Die APN-Einstellungen werden nicht automatisch übernommen. Beziehen Sie die APN-Dienst-Einstellungen von Ihrem Internetanbieter, befolgen Sie dann die untenstehenden Schritte, um die APN-Einstellungen manuell zu konfigurieren.
 - Wechseln Sie zum Register **Advanced Settings (Erweiterte Einstellungen) > WAN > Internet Connection (Internetverbindung)**.
 - Wählen Sie im Feld **WAN Type (WAN-Typ)** die Option **Mobile broadband (Mobiles Breitband)**.

- Wenn der APN richtig konfiguriert wurde, aber die Internetverbindung immer noch nicht funktioniert, stellen Sie Folgendes sicher:
 - Das Frequenzband wird von Ihrem Internetanbieter bereitgestellt.
 - Der WLAN-Router wurde in der Nähe eines Fensters aufgestellt, um ein starkes 3G/4G-Signal zu empfangen.
- Die Portauslösung, Portweiterleitung, DDNS- oder DMZ-Dienst funktionieren nicht. Die meisten Internetanbieter stellen eine private IP-Adresse für ein mobiles Breitbandgerät bereit. Daher kann auf einige Dienste, wie iCloud, nicht zugegriffen werden. Kontaktieren Sie bitte Ihren Internetanbieter für weitere Hilfe.

Sie haben die SSID (den Netzwerknamen) oder das Netzwerkennwort vergessen.

- Legen Sie per Kabelverbindung (Netzwerkkabel) eine neue SSID und ein neues Netzwerkennwort fest. Rufen Sie die grafische Benutzeroberfläche auf, wechseln Sie zur **Network Map (Netzwerkübersicht)** und klicken auf das Routersymbol. Geben Sie eine neue SSID und ein neues Netzwerkennwort 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 beide 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:

Benutzername: admin

Kennwort: admin

LAN-IP-Adresse des Routers: 192.168.50.1 / router.asus.com

WLAN-Einstellungen:

SSID (2,4 GHz): ASUS_XX

SSID (5 GHz): ASUS_XX

Standard-WLAN-Schlüssel: Befindet sich auf dem Etikett auf der Rückseite Ihres Routers.

HINWEIS: XX bezieht sich auf die letzten zwei Ziffern der 2,4-GHz-MAC-Adresse. Sie finden sie auf dem Etikett auf der Rückseite Ihres Routers.

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 Restoration (Firmware-Wiederherstellung)**.

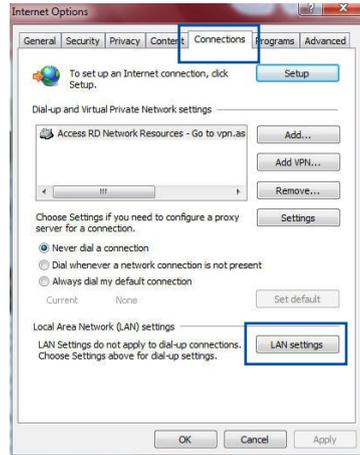
Grafische Benutzeroberfläche lässt sich nicht aufrufen.

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

A. Falls aktiviert, deaktivieren Sie den Proxy-Server.

Windows®

1. Klicken Sie auf **Start > Internet Explorer**, um den Webbrowser zu starten.
2. Klicken Sie auf **Tools (Extras) > Internet options (Internetoptionen) > Connections (Verbindungen) > LAN settings (LAN-Einstellungen)**.

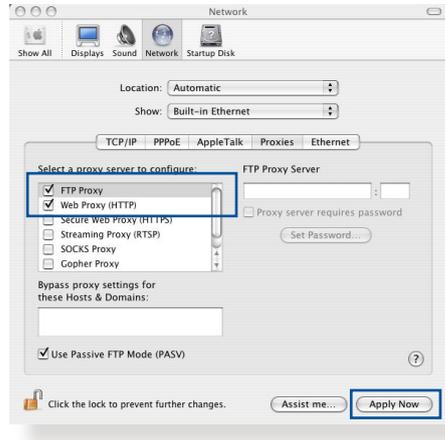


3. Im Einstellungen-Bildschirm für das lokale Netzwerk (LAN) entfernen Sie das Häkchen bei **Use a proxy server for your LAN (Proxyserver für LAN verwenden)**.
4. Klicken Sie zum Abschluss auf **OK**.



MAC OS

1. Klicken Sie in der Menüleiste Ihres Safari Browsers auf **Safari > Preferences (Einstellungen) > Advanced (Erweitert) > Change Settings (Einstellungen ändern)**.
2. Entfernen Sie im Netzwerk-Bildschirm das Häkchen bei **FTP Proxy** und **Web Proxy (HTTP)**.
3. Wenn abgeschlossen, klicken Sie auf **Apply Now (Jetzt übernehmen)**.

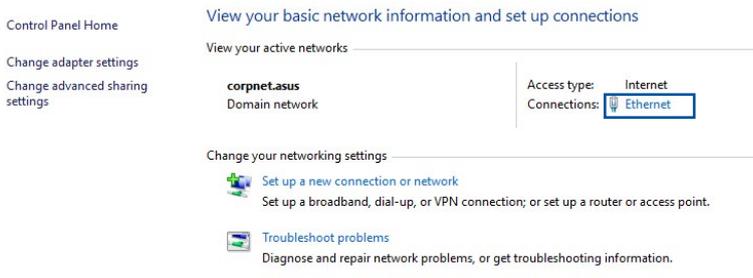


HINWEIS: Für Details zur Deaktivierung eines Proxyserver beziehen Sie sich auf die Hilfefunktion Ihres Browsers.

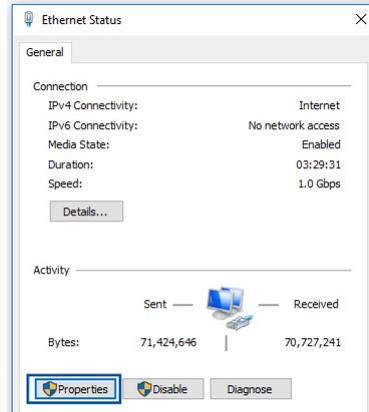
B. Legen Sie die TCP/IP-Einstellungen so fest, dass Sie automatisch eine IP-Adresse erhalten.

Windows®

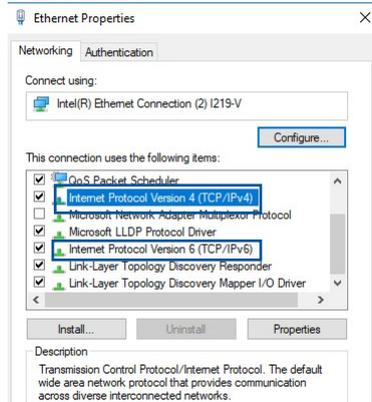
1. Klicken Sie auf **Start > Control Panel (Systemsteuerung) > Network and Sharing Center (Netzwerk- und Freigabecenter)**, klicken Sie dann auf die Netzwerkverbindung, um das Statusfenster anzuzeigen.



2. Klicken Sie auf **Properties (Eigenschaften)**, um das Fenster mit den Ethernet-Eigenschaften anzuzeigen.



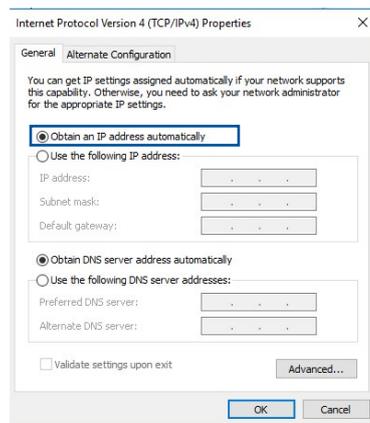
3. Wählen Sie **Internet Protocol Version 4 (TCP/IPv4) (Internetprotokoll Version 4 (TCP/IPv4))** oder **Internet Protocol Version 6 (TCP/IPv6) (Internetprotokoll Version 6 (TCP/IPv6))**, klicken Sie dann auf **Properties (Eigenschaften)**.



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

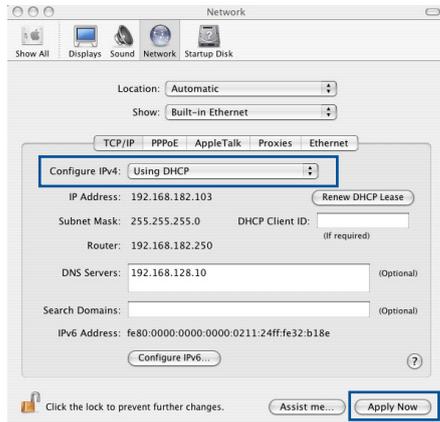
Um die IPv6-IP-Einstellungen automatisch zu beziehen, wählen Sie **Obtain an IPv6 address automatically (IPv6-Adresse automatisch beziehen)**.

5. Klicken Sie zum Abschluss auf **OK**.



MAC OS

1. Klicken Sie links oben im Bildschirm auf das Apple-Symbol .
2. Klicken Sie auf **System Preferences (Systemeinstellungen)** > **Network (Netzwerk)** > **Configure (Konfigurieren)**.
3. Wählen Sie im Register **TCP/IP** in der Auswahlliste **Configure IPv4 (IPv4 konfigurieren)** die Auswahl **Using DHCP (DHCP verwenden)**.
4. Wenn abgeschlossen, klicken Sie auf **Apply Now (Jetzt übernehmen)**.

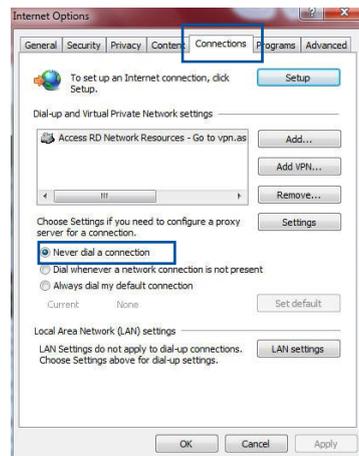


HINWEIS: Für Details zur Konfiguration der TCP/IP-Einstellungen beziehen Sie sich auf die Hilfefunktion Ihres Betriebssystems.

C. Falls aktiviert, deaktivieren Sie die DFÜ (Dial-Up)-Verbindung.

Windows®

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



HINWEIS: Für Details zur Deaktivierung der DFÜ (Dial-Up)-Verbindung beziehen Sie sich auf die Hilfefunktion Ihres Browsers.

Anhang

Hinweise

ASUS Recycling/Rücknahmeservices

Das ASUS-Wiederverwertungs- und Rücknahmeprogramm basiert auf den Bestrebungen, die höchsten Standards zum Schutz der Umwelt anzuwenden. Wir glauben, dass die Bereitstellung einer Lösung für unsere Kunden die Möglichkeit schafft, unsere Produkte, Batterien, andere Komponenten und ebenfalls das Verpackungsmaterial verantwortungsbewußt der Wiederverwertung zuzuführen. Besuchen Sie bitte die Webseite <http://csr.asus.com/english/Takeback.htm> für Details zur Wiederverwertung in verschiedenen Regionen.

REACH

Die rechtlichen Rahmenbedingungen für REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) erfüllend, veröffentlichen wir die chemischen Substanzen in unseren Produkten auf unserer ASUS REACH-Webseite unter

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

Erklärung der Federal Communications Commission

Dieses Gerät entspricht Teil 15 der FCC-Vorschriften. Im Betrieb müssen die folgenden beiden Bedingungen erfüllt werden:

- Dieses Gerät darf keine schädliche Störstrahlung abgeben, und
- Dieses Gerät muss für empfangene Störstrahlung unempfindlich sein, auch für Störstrahlung, die unerwünschte Funktionen hervorrufen kann.

Dieses Gerät wurde geprüft und entspricht den Grenzwerten für digitale Geräte der Klasse B gemäß Teil 15 der FCC-Vorschriften. Diese Grenzwerte wurden für ausreichenden Schutz gegen Radiofrequenzenergie in Wohngebieten aufgestellt.

Dieses Gerät erzeugt und verwendet Radiofrequenzenergie und kann diese ausstrahlen. Wenn es nicht entsprechend der Bedienungsanleitung installiert und verwendet wird, kann es Störungen von Funkübertragungen verursachen. Es kann nicht für alle Installationen gewährleistet werden, dass keine Störungen auftreten. Falls dieses Gerät Störungen des Rundfunk- oder Fernsehempfangs verursacht, was durch Ein- und Ausschalten des Geräts ermittelt werden kann, sollten Sie folgende Maßnahmen ergreifen, um die Störungen zu beheben:

- Ändern Sie die Ausrichtung oder den Standort der Empfangsantenne.
- Vergrößern Sie den Abstand zwischen dem Gerät und dem Empfänger.
- Schließen Sie Gerät und Empfänger an unterschiedliche Netzspannungskreise an.
- Wenden Sie sich an den Fachhändler oder einen erfahrenen Radio-/ Fernsehtechniker.

WICHTIG! Dieses Gerät wird im Frequenzbereich von 5,15~5,25 GHz betrieben und ist auf den Gebrauch in Innenräumen beschränkt.

WARNUNG!

- Änderungen oder Modifizierungen dieses Geräts, die nicht ausdrücklich von der für Übereinstimmung verantwortlichen Partei genehmigt sind, können das Recht des Benutzers, dieses Gerät zu betreiben, annullieren.
 - Benutzer dürfen dieses Gerät nicht modifizieren. Modifikationen, die durch jemand anderen als den Verantwortlichen für die Einhaltung der Vorschriften der Federal Communications Commission (FCC) durchgeführt wurden, können die Berechtigung zum Betrieb dieses Geräts, gewährt nach den FCC-Vorschriften, erlöschen lassen.
 - Bei Produkten auf dem kanadischen bzw. US-Markt können nur die Kanäle 1 bis 11 betrieben werden. Die Auswahl anderer Kanäle ist nicht möglich.
-

CE-Erklärung

Vereinfachte EU-Konformitätserklärung

ASUSTeK Computer Inc. erklärt hiermit, dass dieses Gerät mit den wesentlichen Anforderungen und anderen relevanten Bestimmungen der Richtlinie 2014/53/EU übereinstimmt. Der gesamte Text der EU-Konformitätserklärung ist verfügbar unter: <https://www.asus.com/support/>

Konformitätserklärung für Ökodesign-Richtlinie 2009/125/EC

Die Überprüfung der Ökodesign-Anforderungen nach (EC) Nr. 1275/2008 und (EU) Nr. 801/2013 wurde durchgeführt. Wenn sich das Gerät im Netzwerkbereitschaftsmodus befindet, werden die E/A- und Netzwerkschnittstellen in den Ruhezustand versetzt und arbeiten nicht wie gewöhnlich. Um das Gerät aufzuwecken, drücken Sie die WLAN Ein/Aus-, LED Ein/Aus-, Reset- oder WPS-Taste.

Dieses Gerät erfüllt die EU-Strahlenbelastungsgrenzen für unkontrollierte Umgebungen. Dieses Gerät sollte mit einem Mindestabstand von 20 cm zwischen der Strahlungsquelle und Ihrem Körper installiert und betrieben werden.

Alle Betriebsarten:

2.4GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40)

5GHz: 802.11a, 802.11n (HT20), 802.11n (HT40) , 802.11n (HT80)

Die Frequenz, der Modus und die maximale Sendeleistung in der EU sind nachfolgend aufgeführt:

2412-2472MHz (802.11n HT40 MCS 8): 19.97 dBm

5180-5240MHz (802.11n HT40 MCS 8): 22.43 dBm

5260-5320MHz (802.11n HT40 MCS 8): 22.81 dBm

5500-5700MHz (802.11n HT20 MCS 8): 29.75 dBm

Das Gerät ist auf den Innenbereich beschränkt, wenn es im Frequenzbereich von 5150 MHz bis 5350 MHz betrieben wird.

	AT	BE	BG	CZ	DK	EE	FR
	DE	IS	IE	IT	EL	ES	CY
	LV	LI	LT	LU	HU	MT	NL
	NO	PL	PT	RO	SI	SK	TR
	FI	SE	CH	UK	HR		

Sicherheitshinweise

- Benutzen Sie das Gerät nur in Umgebungen, die eine Temperatur von 0 °C (32 °F) bis 40 °C (104 °F) aufweisen.
- Prüfen Sie am Aufkleber an der Geräteunterseite, ob Ihr Netzteil den Stromversorgungsanforderungen entspricht.
- Stellen Sie das Gerät NICHT auf schräge oder instabile Arbeitsflächen. Wenden Sie sich an das Wartungspersonal, wenn das Gehäuse beschädigt wurde.
- Legen Sie KEINE Gegenstände auf das Gerät, lassen Sie keine Gegenstände darauf fallen und schieben Sie keine Fremdkörper in das Gerät.
- Setzen Sie das Gerät KEINESFALLS Flüssigkeiten, Regen oder Feuchtigkeit aus, verwenden Sie es nicht in der Nähe derartiger Gefahrenquellen. Verwenden Sie das Modem nicht während eines Gewitters.
- Decken Sie die Lüftungsöffnungen am Gerät NICHT ab, um eine Überhitzung des Systems zu vermeiden.
- Benutzen Sie KEINE beschädigten Netzkabel, Zubehörteile oder Peripheriegeräte.
- Falls das Netzteil defekt ist, versuchen Sie nicht, es selbst zu reparieren. Wenden Sie sich an den qualifizierten Kundendienst oder Ihre Verkaufsstelle.
- Um die Gefahr eines Stromschlags zu verhindern, ziehen Sie das Netzkabel aus der Steckdose, bevor Sie das System an einem anderen Ort aufstellen.

CE-Kennzeichen-Warnung

Es handelt sich hier um ein Produkt der Klasse B, das im Hausgebrauch Radiointerferenzen hervorrufen kann.

Dieses Gerät kann betrieben werden 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.

RF-Aussetzungsinformation

Diese Ausrüstung erfüllt die IC RSS-102-Hochfrequenzbelastungsgrenzwerte, die für ein unbeaufsichtigtes Umfeld festgelegt wurden. Dieses Gerät sollte mit einem Mindestabstand von 31 cm zwischen der Strahlungsquelle und Ihrem Körper installiert und betrieben werden.

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 31 cm de distance entre la source de rayonnement et votre corps.

Canada, avis d'Industry Canada (IC)

Le présent appareil est conforme aux normes CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

Son utilisation est sujette aux deux conditions suivantes : (1) cet appareil ne doit pas créer d'interférences et (2) cet appareil doit tolérer tout type d'interférences, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

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

Nur für die Türkei

Autorisierte Händler in der Türkei:

BOGAZICI BİL GİSAYAR SAN. VE TİC. A.S.

Tel. -Nr.: +90 212 3311000

Adresse: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10
AYAZAGA/İSTANBUL

CİZGİ Elektronik San. Tic. Ltd. Sti.

Tel. -Nr.: +90 212 3567070

Adresse: CEMAL SURURI CD. HALİM MERİC İS MERKEZİ
No: 15/C D:5-6 34394 MECİDİYEKOY/İSTANBUL

KOYUNCU ELEKTRONİK BİLGİ İSLEM SİST. SAN. VE DİS TİC. A.S.

Tel. -Nr.: +90 216 5288888

Adresse: EMEK MAH.ORDU CAD. NO:18, SARİGAZİ,
SANCAKTEPE İSTANBUL

ENDEKS BİLİŞİM SAN VE DİŞ TİC LTD ŞTİ

Tel. -Nr.: +90 216 523 35 70 (pbx)

Adresse: Bulgurlu Mahallesi Alemdağ Caddesi No:56 /
B-1 34696 Üsküdar/ İSTANBUL

AEEE Yönetmeliğine Uygundur.

ASUS Kontaktinformation

ASUSTeK COMPUTER INC.

Adresse 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112,
Taiwan
Telefon +886-2-2894-3447
Fax +886-2-2893-1687
Webseite <https://www.asus.com>

Technischer Support

Telefon +86-21-38429911
Online-Support <https://qr.asus.com/techserv>

ASUS COMPUTER INTERNATIONAL (Amerika)

Adresse 48720 Kato Rd., Fremont, CA 94538, USA
Telefon +1-510-739-3777
Fax +1-510-608-4555
Webseite <https://www.asus.com/us/>

Technischer Support

Support-Fax +1-812-284-0883
Telefon +1-812-282-2787
Online-Support <https://qr.asus.com/techserv>

ASUS COMPUTER GmbH (Deutschland und Österreich)

Adresse Harkortstraße 21-23, 40880 Ratingen,
Deutschland
Webseite <https://www.asus.com/de>
Online-Kontakt <https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=de-de>

Technischer Support

Telefon (DE) +49-2102-5789557
Telefon (AT) +43-1360-2775461
Online-Support <https://www.asus.com/de/support>