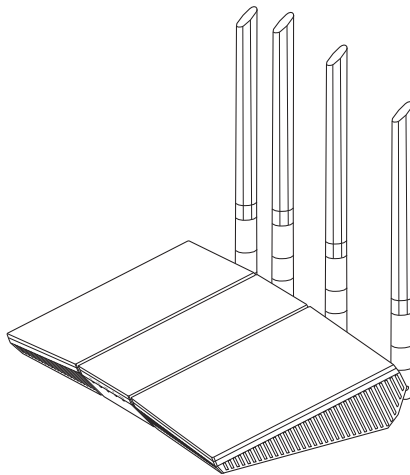


# Benutzerhandbuch

## RT-AX57

### Dualband WLAN-Router



**Copyright © 2024 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

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Kennenlernen Ihres WLAN-Routers</b>                               | <b>6</b>  |
| 1.1      | Willkommen!.....   | 6         |
| 1.2      | Verpackungsinhalt.....   | 6         |
| 1.3      | Ihr WLAN-Router.....   | 7         |
| 1.4      | Ihren Router aufstellen.....   | 9         |
| 1.5      | Installationsanforderungen .....                                     | 10        |
| <b>2</b> | <b>Erste Schritte</b>  | <b>11</b> |
| 2.1      | Router einrichten.....   | 11        |
|          | A. Kabelverbindung.....  | 11        |
|          | B. Drahtlosverbindung.....   | 13        |
| 2.2      | Quick Internet Setup (QIS) mit automatischer Erkennung ...           | 14        |
| 2.3      | Mit Ihrem WLAN verbinden .....                                       | 16        |
| <b>3</b> | <b>Konfigurieren der allgemeinen und erweiterten Einstellungen</b>   | <b>17</b> |
| 3.1      | Anmeldung im Web-GUI.....  | 17        |
| 3.2      | Netzwerkübersicht verwenden .....                                    | 18        |
|          | 3.2.1 Einrichten der WLAN-Sicherheitseinstellungen.....              | 19        |
|          | 3.2.2 Verwalten Ihrer Netzwerk-Clients.....                          | 20        |
| 3.3      | AiProtection.....  | 21        |
|          | 3.3.1 Netzwerkschutz.....  | 22        |
|          | 3.3.2 Jugendschutzeinstellungen festlegen .....                      | 25        |
| 3.4      | Administration.....  | 27        |
|          | 3.4.1 Betriebsmodus .....  | 27        |
|          | 3.4.2 Aktualisieren der Firmware.....                                | 28        |
|          | 3.4.3 Wiederherstellen/Speichern/Hochladen<br>der Einstellungen..... | 28        |
| 3.5      | Firewall.....  | 29        |
|          | 3.5.1 Allgemein.....   | 29        |
|          | 3.5.2 URL-Filter.....  | 29        |
|          | 3.5.3 Schlüsselwortfilter.....                                       | 30        |
|          | 3.5.4 Netzwerkdienstefilter .....                                    | 31        |

# Inhaltsverzeichnis

|      |   |    |
|------|---|----|
| 3.6  | Gast-Netzwerk.....  | 33 |
| 3.7  | IPv6.....   | 35 |
| 3.8  | LAN.....  | 36 |
|      | 3.8.1 LAN-IP.....   | 36 |
|      | 3.8.2 DHCP-Server.....  | 37 |
|      | 3.8.3 Route.....  | 39 |
|      | 3.8.4 IPTV.....   | 40 |
| 3.9  | Systemprotokoll.....  | 41 |
| 3.10 | Traffic Analyzer.....   | 42 |
| 3.11 | Traffic Manager.....  | 43 |
|      | 3.11.1 Verwalten von QoS<br>(Quality of Service - Dienstqualität) Bandbreite..... | 43 |
| 3.12 | WAN.....  | 46 |
|      | 3.12.1 Internetverbindung.....  | 46 |
|      | 3.12.2 Portauslösung.....   | 49 |
|      | 3.12.3 Virtueller Server/Portweiterleitung.....                                   | 51 |
|      | 3.12.4 DMZ.....   | 54 |
|      | 3.12.5 DDNS.....  | 55 |
|      | 3.12.6 NAT-Durchleitung.....  | 56 |
| 3.13 | WLAN.....   | 57 |
|      | 3.13.1 Allgemein.....   | 57 |
|      | 3.13.2 WPS.....   | 60 |
|      | 3.13.3 WDS.....   | 62 |
|      | 3.13.4 WLAN-MAC-Filter.....   | 64 |
|      | 3.13.5 RADIUS-Einstellungen.....  | 65 |
|      | 3.13.6 Professionell.....   | 66 |

# Inhaltsverzeichnis

|          |                                      |           |
|----------|--------------------------------------|-----------|
| <b>4</b> | <b>Dienstprogramme</b>               | <b>69</b> |
| 4.1      | Device Discovery .....               | 69        |
| 4.2      | Firmware Restoration.....            | 70        |
| <b>5</b> | <b>Fehlerbehebung</b>                | <b>72</b> |
| 5.1      | Allgemeine Problemlösung .....       | 72        |
| 5.2      | Häufig gestellte Fragen (FAQs) ..... | 75        |
|          | <b>Anhang</b>                        | <b>84</b> |
|          | Sicherheitshinweise.....             | 93        |
|          | Service und Support .....            | 95        |

# 1 Kennenlernen Ihres WLAN-Routers

## 1.1 Willkommen!

Vielen Dank für den Kauf Ihres WLAN-Routers ASUS RT-AX57! Der extradünne und elegante RT-AX57 bietet 2,4-GHz- und 5-GHz-Dual-Band für unübertroffenes gleichzeitiges HD-WLAN-Streamen. Er verfügt über grüne Netzwerktechnologie von ASUS – eine Lösung für bis zu 70% Energieersparnis.

## 1.2 Verpackungsinhalt

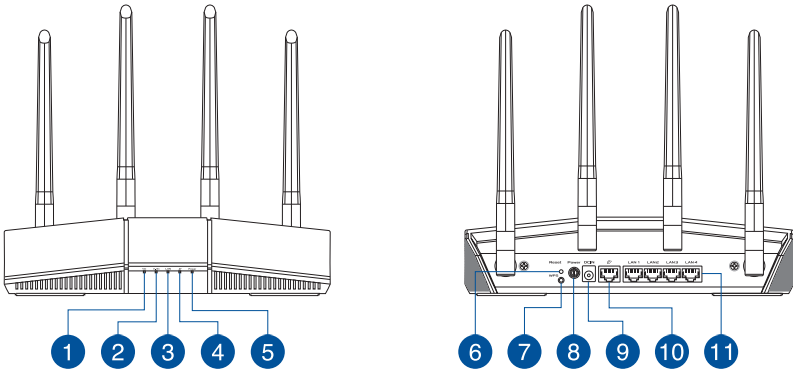
- |   |   |
|---|---|
| <input checked="" type="checkbox"/> RT-AX57 WLAN-Router | <input checked="" type="checkbox"/> Netzwerkkabel (RJ-45) |
| <input checked="" type="checkbox"/> Netzteil            | <input checked="" type="checkbox"/> Schnellstartanleitung |

---

### HINWEISE:

- Falls Artikel beschädigt oder nicht vorhanden sind, wenden Sie sich für technische Anfragen und Support an ASUS. Weitere Informationen finden Sie unter **Service und Support** am Ende dieses Benutzerhandbuchs.
  - Bewahren Sie die Originalverpackung für den Fall eines zukünftigen Garantieanspruchs wie Nachbesserung oder Ersatz gut auf.
-

## 1.3 Ihr WLAN-Router



- 
- 1 5-GHz-LED**  
**Aus:** Kein 5 GHz-Signal.  
**An:** WLAN-System ist bereit.  
**Blinkend:** Datenversand oder -empfang über die WLAN-Verbindung.
- 
- 2 2,4-GHz-LED**  
**Aus:** Kein 2,4 GHz-Signal.  
**An:** WLAN-System ist bereit.  
**Blinkend:** Datenversand oder -empfang über die WLAN-Verbindung.
- 
- 3 LAN-LED**  
**Aus:** Kein Strom oder keine physische Verbindung.  
**An:** Physische Verbindung mit LAN (Lokales Netzwerk).
- 
- 4 WAN-LED (Internet)**  
**Rot:** Keine IP oder keine physische Verbindung.  
**An:** Physische Verbindung mit WAN (Wide Area Network).
- 
- 5 Betriebs-LED**  
**Aus:** Kein Strom.  
**An:** Gerät ist bereit.  
**Langsames Blinken:** Rettungsmodus
- 
- 6 Reset-Taste**  
Mit dieser Taste können Sie das System auf dessen Werkseinstellungen zurücksetzen.
- 
- 7 WPS-Taste**  
Diese Taste startet den WPS-Assistenten.
- 
- 8 Netzschalter**  
Mit diesem Schalter können Sie Ihr System ein-/ausschalten.
-

---

**9****Netzanschluss (DC-In)**

Verbinden Sie das mitgelieferte Netzteil mit diesem Anschluss und schließen Sie Ihren Router an eine Stromversorgung an.

---

**10****WAN-Anschluss (Internet)**

Verbinden Sie ein Netzwerkkabel mit diesem Anschluss, um eine WAN-Verbindung herzustellen.

---

**11****LAN-Anschlüsse 1 ~ 4**

Verbinden Sie ein Netzwerkkabel mit diesen Anschlüssen, um eine LAN-Verbindung herzustellen.

---

---

**HINWEISE:**

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

- **Spezifikationen:**

|                                 |   |          |         |
|---------------------------------|---|----------|---------|
| <b>Netzteil</b>                 | DC Ausgang: +12V mit max. 1A/1,5A Stromstärke |          |         |
| <b>Betriebstemperatur</b>       | 0~40 °C                                       | Lagerung | 0~70 °C |
| <b>Betriebsluftfeuchtigkeit</b> | 50~90%  | Lagerung | 20~90%  |

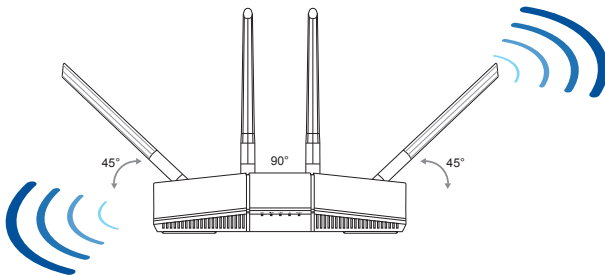
---



## 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.
- Das Gerät von Metallhindernissen oder direktem Sonnenlicht fernhalten.
- Das Gerät 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 fernhalten, 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.



## 1.5 Installationsanforderungen

Zur Netzwerkeinrichtung benötigen Sie einen Computer, der folgende Systemvoraussetzungen erfüllt:

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

---

### HINWEISE:

- Falls Ihr Computer über keine integrierte WLAN-Funktion verfügt, können Sie einen IEEE 802.11a/b/g/n/ac/ax WLAN-Adapter für die Netzwerkverbindung auf Ihrem Computer installieren.
- Mit Dual-Band-Technologie ausgestattet, unterstützt Ihr WLAN-Router 2,4 GHz und 5 GHz WLAN-Signale gleichzeitig. Dies erlaubt die Ausführung normaler Internettätigkeiten wie das Surfen im Internet oder das Lesen/Schreiben von E-Mails im 2,4 GHz-Frequenzbereich und das simultane Streamen von High-Definition Audio-/Videodateien wie Filmen oder Musik im 5 GHz-Frequenzbereich.
- Bestimmte IEEE 802.11n-Geräte, die Sie in Ihr Netzwerk einbinden möchten, unterstützen das 5-GHz-Frequenzband eventuell nicht. Lesen Sie die technischen Daten in der Bedienungsanleitung des jeweiligen Gerätes nach.
- Die für die Verbindung der Netzwerkgeräte verwendeten Ethernet RJ-45-Kabel sollten nicht länger als 100 Meter sein.

---

### WICHTIG!

- Bei einigen WLAN-Adaptoren treten möglicherweise Verbindungsprobleme mit 802.11ax WLAN-APs auf.
- Sollte das bei Ihnen der Fall sein, stellen Sie bitte sicher, dass Sie den Treiber auf die neueste Version aktualisieren. Besuchen Sie die offizielle Support-Webseite des Herstellers, auf der Sie Softwaretreiber, Updates und weitere zugehörige Informationen erhalten können.
  - Realtek: <https://www.realtek.com/en/downloads>
  - Mediatek: <https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi>
  - Intel: <https://downloadcenter.intel.com/>

## 2 Erste Schritte

### 2.1 Router einrichten

---

#### **WICHTIG!**

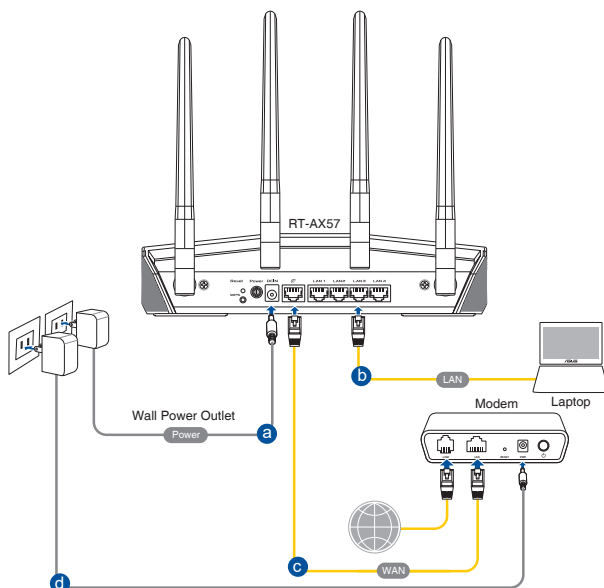
- Nutzen Sie zur Einrichtung Ihres WLAN-Routers eine Kabelverbindung, damit die Einrichtung problemlos vonstatten geht.
  - Bevor Sie Ihren ASUS WLAN-Router einrichten, sollten Sie:
    - Den aktuellen Router vom Netzwerk trennen (falls vorhanden).
    - Alle Kabel/Leitungen der aktuellen Modem-Konfiguration trennen. Falls Ihr Modem über einen Backup-Akku verfügt, entfernen Sie diesen ebenfalls.
    - Starten Sie Ihr Modem und Ihren Computer neu (empfohlen).
- 

#### **WARNUNG!**

- Das Netzkabel muss an eine Steckdose angeschlossen werden, die mit einer geeigneten Erdung versehen ist. Schließen Sie das Gerät nur an eine nahe gelegene Steckdose an, die leicht zugänglich ist.
  - Falls das Netzteil defekt ist, versuchen Sie nicht, es selbst zu reparieren. Wenden Sie sich an den qualifizierten Kundendienst oder Ihre Verkaufsstelle.
  - Benutzen Sie KEINE beschädigten Netzkabel, Zubehörteile oder Peripheriegeräte.
  - Montieren Sie dieses Gerät NICHT in einer Höhe über zwei Metern.
  - Benutzen Sie das Gerät nur in Umgebungen, die eine Temperatur von 0°C (32°F) bis 40°C (104°F) aufweisen.
-

## A. Kabelverbindung

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



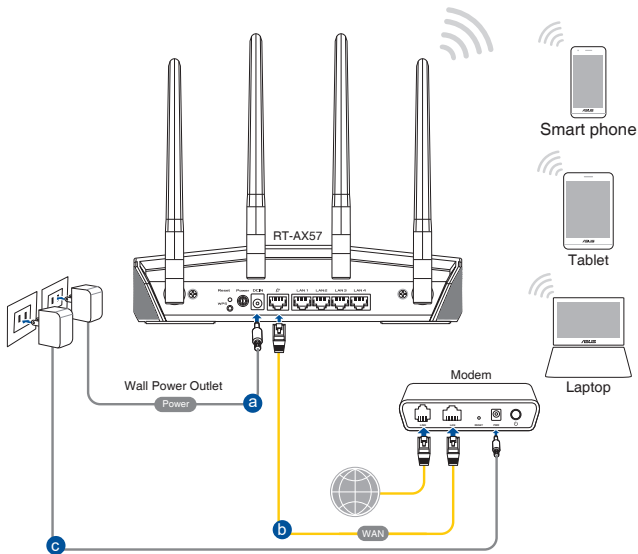
### So richten Sie Ihren WLAN-Router über eine Kabelverbindung ein:

1. Stecken Sie das AC Netzteil Ihres WLAN-Routers in den DC-IN-Anschluss und schließen es an eine Steckdose an.
2. Verbinden Sie Ihren Computer mithilfe des mitgelieferten Netzwerkkabels mit dem LAN-Anschluss Ihres WLAN-Routers.

**WICHTIG!** Die LAN-LED sollte blinken.

3. Schließen Sie Ihr Modem mit einem weiteren Netzwerkkabel an den WAN-Anschluss Ihres WLAN-Routers an.
4. Verbinden Sie das Netzteil des Modems mit dem Stromanschluss (DC-IN) sowie mit der Stromversorgung.

## B. Drahtlosverbindung



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

1. Stecken Sie das AC Netzteil Ihres WLAN-Routers in den DC-IN-Anschluss und schließen es an eine Steckdose an.
2. Verwenden Sie ein anderes Netzkabel, um Ihr Modem mit dem WAN-Anschluss Ihres WLAN-Routers zu verbinden.
3. Verbinden Sie das Netzteil des Modems mit dem Stromanschluss (DC-IN) sowie mit der Stromversorgung.
4. Installieren Sie einen IEEE 802.11a/b/g/n/ac/ax WLAN-Adapter auf Ihrem Computer.

### 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 **3.2.1 Einrichten der WLAN-Sicherheitseinstellungen** in diesem Benutzerhandbuch.

## 2.2 Quick Internet Setup (QIS) mit automatischer Erkennung

Die Quick Internet Setup (QIS)-Funktion leitet Sie dabei an, schnell Ihre Internetverbindung einzurichten.

---

**HINWEIS:** Wenn Sie die Internetverbindung zum ersten Mal einrichten, drücken Sie die Reset-Taste an Ihrem WLAN-Router, um ihn auf seine Standard-Werkseinstellungen zurückzusetzen.

---

### So benutzen Sie QIS mit automatischer Erkennung:

1. Starten Sie einen Webbrowser. Sie werden zum ASUS Setup-Assistenten (Quick Internet Setup) weitergeleitet. Falls nicht, geben Sie bitte <http://www.asusrouter.com> manuell ein.
2. Der WLAN-Router erkennt automatisch, ob Ihr Internetverbindungstyp **Dynamic IP**, **PPPoE**, **PPTP** oder **L2TP** ist. Geben Sie die notwendigen Informationen für Ihre ISP-Verbindungsart ein.

---

**WICHTIG!** Erhalten Sie die notwendigen Informationen über die Art der Internetverbindung von Ihrem ISP (Internetdienstanbieter).

---

### HINWEISE:

- Die automatische Erkennung Ihrer ISP-Verbindungsart findet statt, wenn Sie den WLAN-Router das erste Mal konfigurieren oder wenn Ihr WLAN-Router auf seine Standardeinstellungen zurückgesetzt wird.
  - Falls die Erkennung der Art der Internetverbindung durch QIS fehlgeschlagen ist, klicken Sie auf **Manual setting (Manuelle Einstellung)** und konfigurieren Ihre Verbindungseinstellungen manuell.
- 
3. Weisen Sie den WLAN-Namen (SSID) und Sicherheitsschlüssel für Ihre 2,4 GHz und 5 GHz WLAN-Verbindung zu. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.

**ASUS**  
WIRELESS NETWORKS

## Wireless Settings

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

2.4GHz Network Name (SSID)

2.4GHz Wireless Security

5GHz Network Name (SSID)

5GHz Wireless Security

Separate 2.4GHz and 5GHz

Previous Apply

- Ändern Sie auf der Seite **Login Information Setup (Einrichtung der Anmeldedaten)** das Anmeldekennwort des Routers, um unbefugten Zugriff auf Ihren WLAN-Router zu verhindern.

**ASUS**  
WIRELESS NETWORKS

## Login Settings

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

Router Login Name

New password

Retype Password



Previous Next

**HINWEIS:** Der Benutzername und das Kennwort des WLAN-Routers für die Anmeldung unterscheiden sich vom 2,4 GHz/5 GHz Netzwerknamen (SSID) und Sicherheitsschlüssel. Der Benutzername und das Kennwort des WLAN-Routers ermöglichen Ihnen die Anmeldung auf der Web-Benutzeroberfläche Ihres WLAN-Routers, um die Einstellungen Ihres WLAN-Routers zu konfigurieren. Der 2,4 GHz/5 GHz Netzwerkname (SSID) und Sicherheitsschlüssel ermöglichen es WLAN-Geräten, sich an Ihrem 2,4 GHz/5 GHz Netzwerk anzumelden und sich damit zu verbinden.

## 2.3 Mit Ihrem WLAN verbinden

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

### So verbinden Sie sich mit Ihrem Netzwerk:

1. Auf Ihrem Computer klicken Sie auf das Netzwerksymbol  im Benachrichtigungsbereich: Verfügbare WLANs werden angezeigt.
2. Wählen Sie das drahtlose Netzwerk, mit dem Sie sich verbinden möchten, klicken Sie dann auf **Connect (Verbinden)**.
3. Möglicherweise müssen Sie in den Netzwerksicherheitschlüssel für ein gesichertes drahtloses Netzwerk eingeben. Klicken Sie dann auf **OK**.
4. Warten Sie ab, bis die Verbindung zum WLAN erfolgreich hergestellt wurde. Der Verbindungsstatus wird angezeigt, und das Netzwerksymbol zeigt den Status als verbunden an .

---

### HINWEISE:

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



# 3 Konfigurieren der allgemeinen und erweiterten Einstellungen

## 3.1 Anmeldung im Web-GUI

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

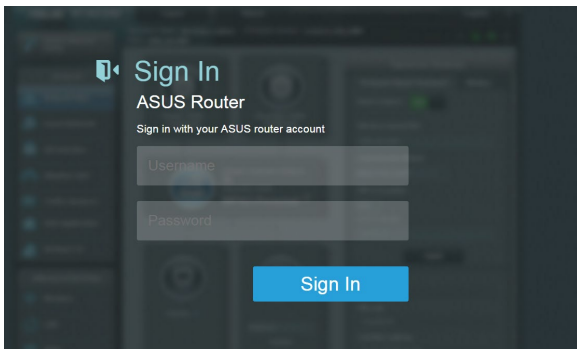
---

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

---

### So melden Sie sich an der Web-Benutzeroberfläche an:

1. Geben Sie in Ihren Browser die Standard-IP-Adresse Ihres WLAN-Routers manuell ein: <http://www.asusrouter.com>.
2. Geben Sie auf der Anmeldeseite den Benutzernamen und das Kennwort ein, die Sie unter **2.2 Quick Internet Setup (QIS) mit automatischer Erkennung** festgelegt haben.



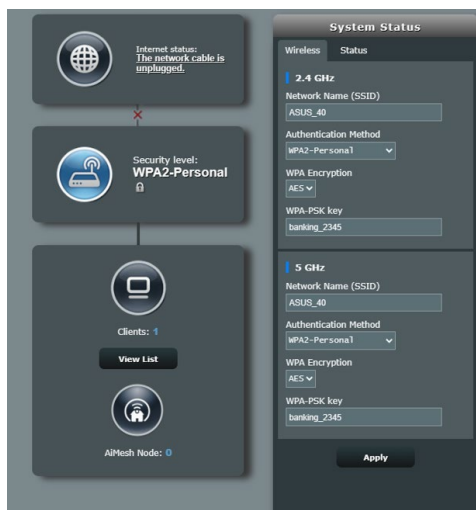
3. Zur Konfiguration der diversen Einstellungen Ihres ASUS WLAN-Routers können Sie nun die grafische Benutzeroberfläche (GUI) verwenden.



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

## 3.2 Netzwerkübersicht verwenden

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



### 3.2.1 Einrichten der WLAN-Sicherheitseinstellungen

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

**So richten Sie die WLAN-Sicherheitseinstellungen ein:**

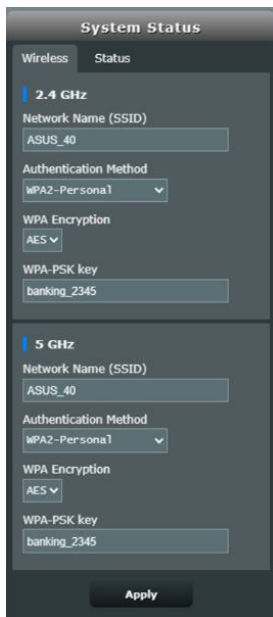
1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Network Map (Netzwerkübersicht)**.
2. Im Bildschirm Network Map (Netzwerkübersicht) wählen Sie **System status (Systemstatus)**, um WLAN-Sicherheitseinstellungen wie SSID, Sicherheitsstufe und Verschlüsselungseinstellungen zu konfigurieren.

---

**HINWEIS:** Sie können für das 2,4 GHz-Frequenzband und 5 GHz-Frequenzband jeweils verschiedene WLAN-Sicherheitseinstellungen einrichten.

---

#### Sicherheitseinstellungen für 2,4 GHz/5 GHz



3. Geben Sie im Feld **Network Name (SSID) (Netzwerkname, SSID)** Ihrem WLAN einen eindeutigen Namen.

4. Wählen Sie aus der **WEP Encryption (WEP-Verschlüsselung)**-Auswahlliste das Verschlüsselungsverfahren für Ihr WLAN aus.

**WICHTIG!** Der IEEE 802.11 n/ac/ax-Standard erkennt die Verwendung eines hohen 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. Geben Sie Ihr Sicherheitskennwort ein.
6. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.

## 3.2.2 Verwalten Ihrer Netzwerk-Clients

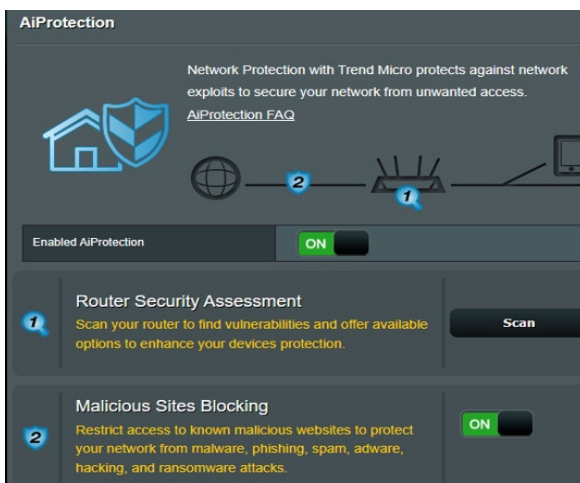


### So verwalten Sie Ihre Netzwerk-Clients:

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

### 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.

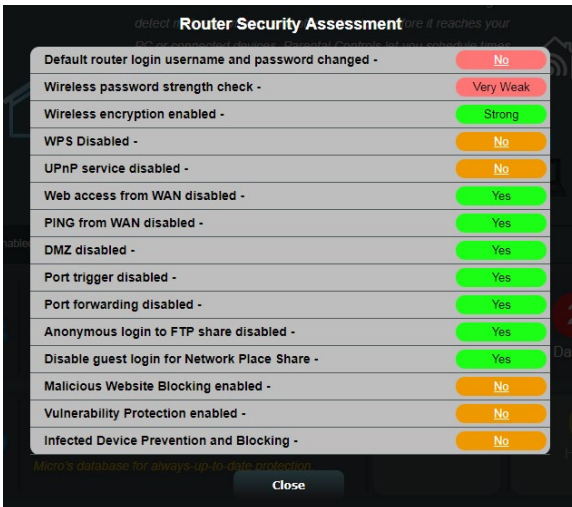


### Netzwerkschutz konfigurieren

**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)**.

## 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)**.

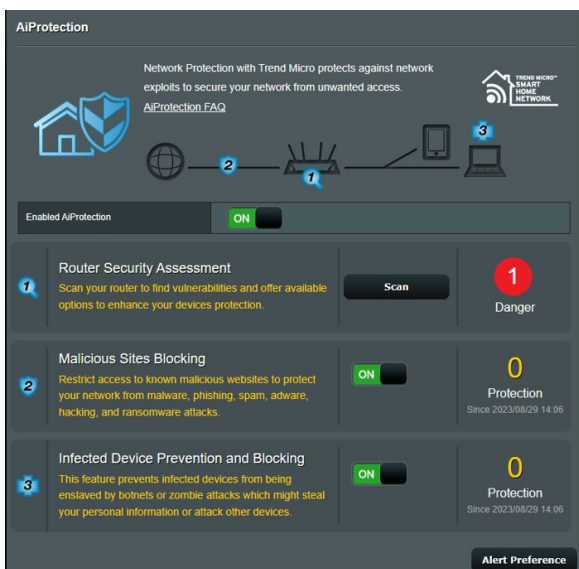


### 3.3.2 Jugendschutzeinstellungen festlegen

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:**

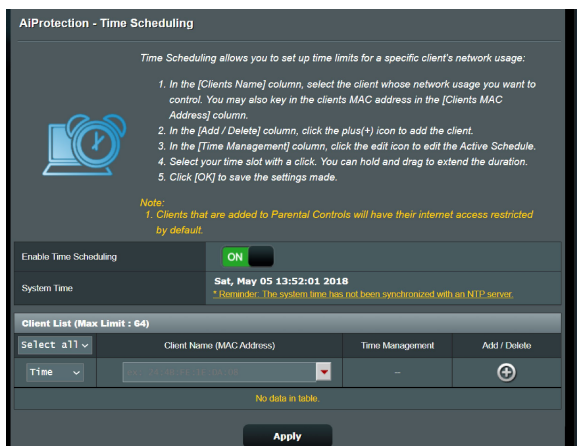
1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > AiProtection**.
2. Klicken Sie in der **AiProtection**-Hauptseite auf das **Parental Controls (Jugendschutzeinstellungen)**-Register.



## 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 **Clients Name (Client-Name)** wählen Sie oder geben Sie den Namen des Clients in der Dropdown-Liste ein.

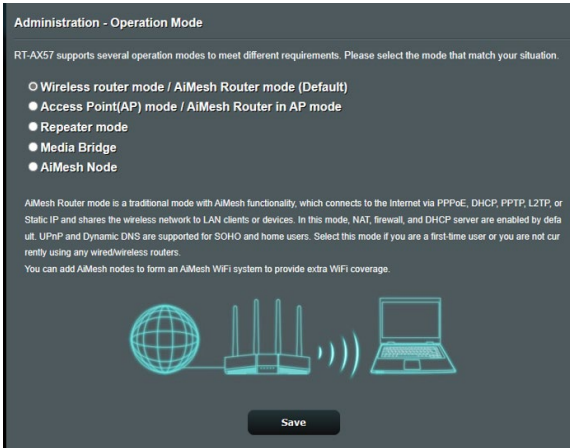
**HINWEIS:** Sie können auch in der **Client MAC Address (Client-MAC-Adresse)**-Spalte die MAC-Adresse des Clients eingeben. Stellen Sie sicher, dass der Name des Clients keine Sonderzeichen oder Leerzeichen enthält, da der Router sonst möglicherweise nicht normal funktioniert.

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

## 3.4 Administration

### 3.4.1 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.
  - **Repeater-Modus:** Dieser Modus verwandelt den Router in einen WLAN-Repeater, um die Reichweite Ihres Signals zu vergrößern.
  - **Access-Point (AP)-Modus:** In diesem Modus erstellt der Router ein neues WLAN im bereits vorhandenen Netzwerk.
3. Klicken Sie auf **Speichern**.

---

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

---

## 3.4.2 Aktualisieren der Firmware

---

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

---

### So aktualisieren Sie die 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)** 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 **4.2 Firmware Restoration (Firmware-Wiederherstellung)**.
- 

## 3.4.3 Wiederherstellen/Speichern/Hochladen der Einstellungen

### 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 (Speichern)**, öffnen den Ordner, in dem Sie die Datei ablegen möchten, anschließend klicken Sie erneut auf **Save (Speichern)**.
    - Um ältere Systemeinstellungen zu laden, klicken Sie auf **Browse (Durchsuchen)**, um die wiederherzustellende Systemdatei zu wählen, 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.

---

## 3.5 Firewall

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

---

**HINWEIS:** Die Firewall-Funktion ist standardmäßig bereits aktiviert.

---

### 3.5.1 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-Attacks (Denial of Service, Überlastung durch übermäßig viele Anfragen) zu schützen, die die Leistung Ihres Routers beeinträchtigen können.
4. Zusätzlich können Sie Pakete überwachen, die zwischen LAN und WAN ausgetauscht werden. Unter **Logged packets type (Protokollierter Pakettyp)** wählen Sie **Dropped (Abgewiesen), Accepted (Angenommen)** oder **Both (Beides)**.
5. Klicken Sie auf **Apply (Übernehmen)**.

### 3.5.2 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.

---

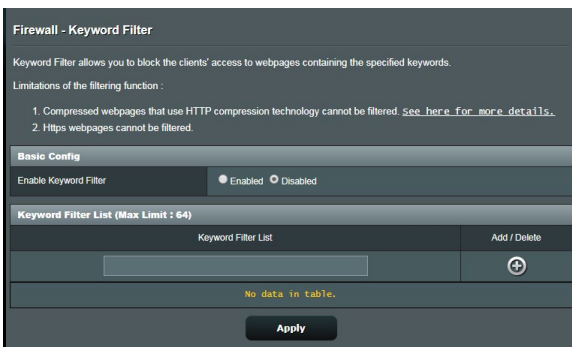
**So richten Sie einen URL-Filter ein:**

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)**.

### 3.5.3 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.

## 3.5.4 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.

**Firewall - Network Services Filter**

The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 80 in the destination port. The traffic that uses port 80 will be blocked (but https can not be blocked).  
Leave the source IP field blank to apply this rule to all LAN devices.

**Black List Duration :** During the scheduled duration, clients in the Black List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.

**White List Duration :** During the scheduled duration, clients in the White List can ONLY use the specified network services. After the specified duration, clients in the White List and other network clients will not be able to access the Internet or any Internet service.

**NOTE :** If you set the subnet for the White List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

\* **Reminder :** The System time zone is different from your locale setting.

**Network Services Filter**

Enable Network Services Filter  Yes  No

Filter table type

Well-Known Applications

Date to Enable LAN to WAN Filter  Mon  Tue  Wed  Thu  Fri

Time of Day to Enable LAN to WAN Filter  :  :  :

Date to Enable LAN to WAN Filter  Sat  Sun

Time of Day to Enable LAN to WAN Filter  :  :  :

Filtered ICMP packet types

**Network Services Filter Table (Max Limit : 32)**

| Source IP            | Port Range           | Destination IP       | Port Range           | Protocol | Add / Delete                     |
|----------------------|----------------------|----------------------|----------------------|----------|----------------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | TCP      | <input type="button" value="⊕"/> |

No data in table.

## 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. **Blacklist** blockiert die angegebenen Netzwerkdienste. **Whitelist** 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)**.



## 3.6 Gast-Netzwerk

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

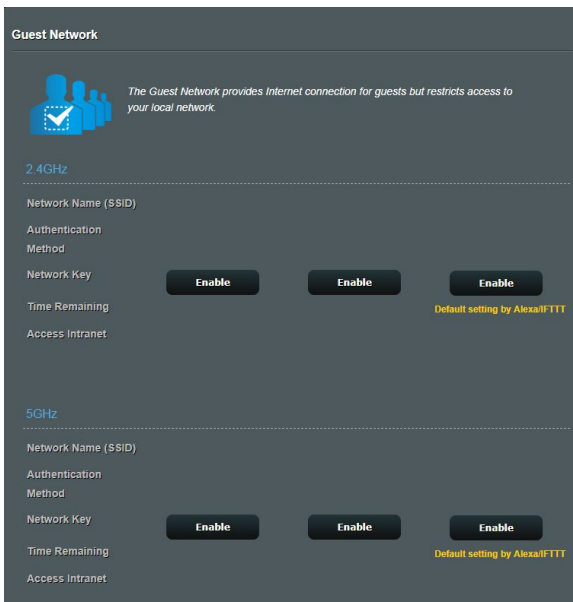
---

**HINWEIS:** Der RT-AX57 unterstützt bis zu sechs SSIDs (drei 2,4-GHz- und drei 5-GHz-SSIDs).

---

### 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)**.



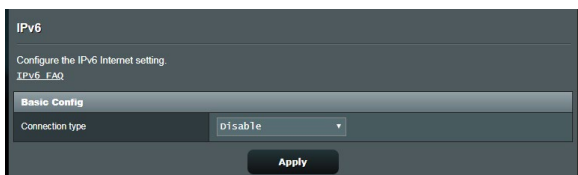
- Um zusätzliche Optionen zu konfigurieren, klicken Sie auf **Modify (Ändern)**.

The screenshot shows the 'Guest Network' configuration page. At the top, there is a blue icon of three people and a checkmark, with the text: 'The Guest Network provides Internet connection for guests but restricts access to your local network.' Below this, there are two sections for configuring networks: 2.4GHz and 5GHz. Each section has a list of settings: Network Name (SSID), Authentication Method, Network Key, Time Remaining, and Access Intranet. For the 2.4GHz network, the settings are: Network Name (SSID) ASUS\_2G\_Guest, Authentication Method Open System, Network Key None, Time Remaining Unlimited access, and Access Intranet off. For the 5GHz network, the settings are: Network Name (SSID) ASUS\_5G\_Guest, Authentication Method Open System, Network Key None, Time Remaining Unlimited access, and Access Intranet off. Each section has an 'Enable' button and a 'Remove' button. A note 'Default setting by AlexaIFTTT' is visible next to the 'Unlimited access' setting in both sections.

- Klicken Sie im Bildschirm **Enable Guest Network (Gastnetzwerk aktivieren)** auf **Yes (Ja)**.
- Legen Sie im Feld **Network Name (SSID) (Netzwerkname (SSID))** einen WLAN-Namen für Ihr temporäres Netzwerk fest.
- Wählen Sie ein **Authentication Method (Authentisierungsverfahren)**.
- Wählen Sie ein **Encryption method (Verschlüsselungsverfahren)**.
- Legen Sie die **Access time (Zugriffszeitdauer)** fest oder wählen Sie **Limitless (Unbegrenzt)**.
- Wählen Sie **Disable (Deaktivieren)** oder **Enable (Aktivieren)** für das Element **Access Intranet (Auf Intranet zugreifen)**.
- Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.

## 3.7 IPv6

Der WLAN-Router unterstützt IPv6-Adressierung, ein System, das weitere 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.

---

## 3.8 LAN

### 3.8.1 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.

---

LAN - LAN IP

Configure the LAN setting of RT-AX57.

|                       |               |
|-----------------------|---------------|
| Host Name             | RT-AX57-7050  |
| RT-AX57's Domain Name |               |
| IP Address            | 192.168.51.1  |
| Subnet Mask           | 255.255.255.0 |

Apply

**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**.

## 3.8.2 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.

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. supports up to 253 IP addresses for your local network.  
Manually Assigned IP around the DHCP list FAQ

**Basic Config**

Enable the DHCP Server  Yes  No

Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

**DNS and WINS Server Setting**

DNS Server

WINS Server

**Manual Assignment**

Enable Manual Assignment  Yes  No

**Manually Assigned IP around the DHCP list (Max Limit : 64)**

| Client Name (MAC Address) | IP Address           | Add / Delete                     |
|---------------------------|----------------------|----------------------------------|
| <input type="text"/>      | <input type="text"/> | <input type="button" value="⊕"/> |

No data in table.

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

### 3.8.3 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.

LAN - Route

This function allows you to add routing rules into. It is useful if you connect several routers behind to share the same connection to the Internet.

Basic Config

Enable static routes  Yes  No

Static Route List (Max Limit : 32)

| 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)**.

### 3.8.4 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 is a note: '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.' Below this, the page is divided into two sections: 'LAN Port' and 'Special Applications'. The 'LAN Port' section contains two rows: 'Select ISP Profile' with a dropdown menu set to 'None', and 'Choose IPTV STB Port' also with a dropdown menu set to 'None'. The 'Special Applications' section contains three rows: 'Use DHCP routes' with a dropdown menu set to 'Microsoft', 'Enable multicast routing (IGMP Proxy)' with a dropdown menu set to 'Disable', and 'UDP Proxy (L4proxy)' with a text input field containing '0'. At the bottom center of the form is an 'Apply' button.

| LAN Port             |      |
|----------------------|------|
| Select ISP Profile   | None |
| Choose IPTV STB Port | None |

| Special Applications                  |           |
|---------------------------------------|-----------|
| Use DHCP routes                       | Microsoft |
| Enable multicast routing (IGMP Proxy) | Disable   |
| UDP Proxy (L4proxy)                   | 0         |

**Apply**



## 3.9 Systemprotokoll

Das 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
  - DHCP-Zuweisungen
  - WLAN-Protokoll
  - Portweiterleitung
  - Routentabelle

```
System Log - General Log
This page shows the detailed system's activities.

System Time Thu, Aug 23 07:15:34 2018
Uptime 0 days 1 hours 18 minute(s) 11 seconds
Remote Log Server [ ] Apply

Aug 23 06:51:04 miniupnpd[7139]: version 1.9 started
Aug 23 06:51:04 miniupnpd[7139]: HTTP listening on port 52102
Aug 23 06:51:04 miniupnpd[7139]: Listening for NAT-PMP/PCP traffic on port 5351
Aug 23 06:58:52 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:52 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:53 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:53 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:55 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 06:58:57 kernel: ^[[0:33:41m[PATHTSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVALID
Aug 23 07:07:14 rc.service: httpd 1079:modify_rc_start_multipath
Aug 23 07:07:14 miniupnpd[7139]: shutting down MiniUPnPd
Aug 23 07:07:14 miniupnpd[7688]: finish adding multi routes (Vcompnat_rules_cho_cho)
Aug 23 07:07:14 miniupnpd[7688]: version 1.9 started
Aug 23 07:07:14 miniupnpd[7688]: HTTP listening on port 60955
Aug 23 07:07:14 miniupnpd[7688]: Listening for NAT-PMP/PCP traffic on port 5351
Aug 23 07:07:14 wan: finish adding multi routes
Aug 23 07:07:14 http: start NAT update
Aug 23 07:07:15 miniupnpd[7688]: shutting down MiniUPnPd
Aug 23 07:07:15 miniupnpd[7729]: version 1.9 started
Aug 23 07:07:15 miniupnpd[7729]: HTTP listening on port 58635
Aug 23 07:07:15 miniupnpd[7729]: Listening for NAT-PMP/PCP traffic on port 5351

Clear Save
```

### 3.10 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.

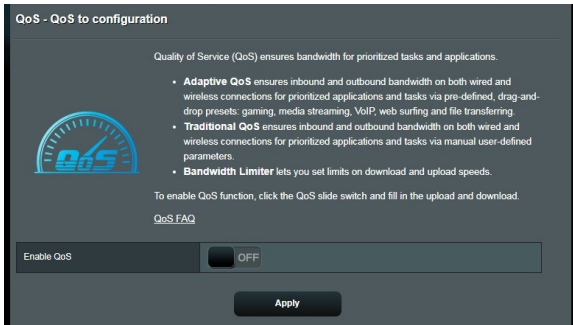


**HINWEIS:** Pakete aus dem Internet werden gleichmäßig an die LAN- und WLAN-Geräte übermittelt.

## 3.11 Traffic Manager

### 3.11.1 Verwalten von QoS (Quality of Service - Dienstqualität) Bandbreite

Mit Quality of Service (QoS) können Sie die Bandbreitenpriorität festlegen und den Netzwerkdatenverkehr verwalten.



**So legen Sie die Bandbreitenpriorität fest:**

1. Wechseln Sie im Navigationspanel zu **General (Allgemein) > Traffic Manager > QoS**.
2. Klicken Sie auf **ON (EIN)**, um QoS zu aktivieren. Füllen Sie die Felder für die Upload- und Download-Bandbreite aus.

---

**HINWEIS:** Informationen über die Bandbreite erhalten Sie von Ihrem Internetanbieter.

---

3. Klicken Sie auf **Speichern**.

---

**HINWEIS:** Die User Specify Rule List (Liste für benutzerdefinierte Regeln) ist für erweiterte Einstellungen. Wenn Sie bestimmten Netzwerkanwendungen und Netzwerkdiensten den Vorrang geben möchten, wählen Sie **User-defined QoS rules (Benutzerdefinierte QoS-Regeln)** oder **User-defined Priority (Benutzerdefinierte Priorität)** aus der Auswahlliste in der rechten oberen Ecke.

---

4. Auf der Seite **User-defined QoS rules (Benutzerdefinierte QoS-Regeln)** gibt es vier Standard-Onlineservicetypen – Web Surfing, HTTPs und Dateiübertragungen. Wählen Sie Ihren bevorzugten Service und füllen die Felder **Source IP or MAC (Quell-IP oder MAC), Destination Port (Zielport), Protocol (Protokoll), Transferred (Übertragen)** und **Priority (Priorität)** aus, klicken Sie dann auf **Apply (Übernehmen)**. Die Informationen werden im QoS-Regeln-Bildschirm konfiguriert.
- 

#### HINWEISE:

- Um Quell-IP oder MAC auszufüllen, können Sie Folgendes tun:
    - a) Geben Sie eine bestimmte IP-Adresse ein, z. B. "192.168.122.1".
    - b) Geben Sie IP-Adressen innerhalb eines Subnetzes oder innerhalb des selben IP-Bereichs ein, z. B. "192.168.123.\*" oder "192.168.\*.\*"
    - c) Geben Sie alle IP-Adressen als "\*.\*.\*.\*" ein oder lassen Sie das Feld leer.
    - d) Das Format für die MAC-Adresse besteht aus sechs Gruppen mit je zwei hexadezimalen Ziffern, getrennt durch Doppelpunkte (:), in der Reihenfolge der Übertragung (z. B. 12:34:56:aa:bc:ef)
  - Für den Quell- oder Zielportbereich haben Sie folgende Möglichkeiten:
    - a) Geben Sie einen bestimmten Port ein, z. B. "95".
    - b) Geben Sie Ports innerhalb eines Bereichs ein, z. B. "103:315", ">100" oder "<65535".
  - Die **Transferred (Übertragen)**-Spalte enthält Informationen über den Upstream- und Downstream-Datenverkehr (ausgehenden und eingehenden Netzwerkdatenverkehr) für einen Abschnitt. In dieser Spalte können Sie ein Limit für den Netzwerkdatenverkehr (in KB) für einen bestimmten Dienst festlegen, um bestimmte Prioritäten für den Dienst, bezogen auf einen bestimmten Port, zu entwickeln. Wenn z. B. zwei Netzwerk-Clients, PC 1 und PC 2, beide auf das Internet zugreifen (festgelegt für Port 80), aber PC 1 das Limit für den Netzwerkdatenverkehr aufgrund einiger Download-Aufgaben überschreitet, dann bekommt PC 1 eine niedrigere Priorität. Wenn Sie kein Limit für den Datenverkehr festlegen möchten, lassen Sie das Feld leer.
-

5. Auf der Seite **User-defined Priority (Benutzerdefinierte Priorität)** können Sie die Netzwerkanwendungen oder -geräte in fünf Ebenen aus der **User-defined QoS rules (Benutzerdefinierte QoS-Regeln)**-Auswahlliste priorisieren. Auf der Grundlage der Prioritätsstufe können Sie die folgenden Methoden zum Versenden von Datenpaketen verwenden:
  - Ändern Sie die Reihenfolge der Upstream-Netzwerkpakete, die an das Internet gesendet werden.
  - Legen Sie in der **Upload Bandwidth (Upload-Bandbreite)**-Tabelle die **Minimum Reserved Bandwidth (Mindestens reservierte Bandbreite)** und das **Maximum Bandwidth Limit (Limit für die maximale Bandbreite)** für mehrere Netzwerkanwendungen mit unterschiedlichen Prioritätsstufen fest. Die Prozentsätze geben die Upload-Bandbreitenraten an, die für die angegebenen Netzwerkanwendungen verfügbar sind.

---

**HINWEISE:**

- Pakete mit niedriger Priorität werden nicht berücksichtigt, um die Übertragung von Paketen mit hoher Priorität sicherzustellen.
- Legen Sie in der **Download Bandwidth (Download-Bandbreite)**-Tabelle das **Maximum Bandwidth Limit (Limit für die maximale Bandbreite)** für mehrere Netzwerkanwendungen in entsprechender Reihenfolge fest. Das Upstream-Paket mit höherer Priorität bedingt das Downstream-Paket mit höherer Priorität.
- Wenn keine Pakete von Anwendungen mit hoher Priorität gesendet werden, ist die volle Übertragungsrate der Internetverbindung für Pakete mit niedriger Priorität verfügbar.

- 
6. Legen Sie die höchste Priorität für Pakete fest. Um ein reibungsloses Online-Gaming-Erlebnis zu gewährleisten, können Sie ACK, SYN und ICMP als Pakete mit höchster Priorität festlegen.

---

**HINWEIS:** Achten Sie darauf, zuerst QoS zu aktivieren und die Limits für die Upload- und Downloadrate festzulegen.

---

## 3.12 WAN

### 3.12.1 Internetverbindung

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

WAN - Internet Connection

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.

Configure the Ethernet WAN settings.

**Basic Config**

WAN Connection Type: Automatic IP ▾

Enable WAN:  Yes  No

Enable NAT:  Yes  No

Enable UPnP: [UPnP\\_FAQ](#)  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 ▾

Extend the TTL value:  Yes  No

Spoof LAN TTL value:  Yes  No

**Apply**

**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 **Fixed 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 Porteinstellungen manuell konfiguriert werden müssen, konfiguriert UPnP den Router automatisch so, dass ankommende Verbindungen und Direktanfragen an einen bestimmten PC im lokalen Netzwerk automatisch angenommen werden.
- **Mit DNS-Server verbinden:** Ermöglicht, die DNS-IP-Adresse 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.

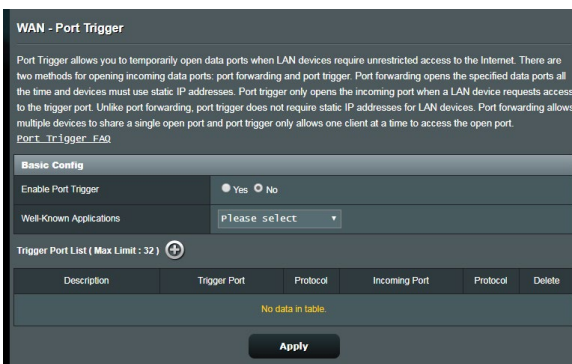
- **Hostname:** In diesem Feld können Sie einen Hostnamen für Ihren Router festlegen. Dieser ist gewöhnlich eine spezielle Vorgabe Ihres Internetanbieters. Sofern Ihrem Computer ein Hostname vom Internetanbieter zugewiesen wurde, tragen Sie diesen Hostnamen hier ein.
- **MAC-Adresse:** Die MAC-Adresse (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.



## 3.12.2 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.



**So richten Sie die Portauslösung ein:**

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > WAN > Port Trigger (Portauslösung)**.
2. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **Übernehmen**.
  - **Portauslösung aktivieren:** Wählen Sie **Yes (Ja)** zur Aktivierung der Portauslösung.
  - **Bekannte Anwendungen:** Wählen Sie beliebige Spiele und Webdienste zum Hinzufügen zur Auslöserportliste.
  - **Beschreibung:** Geben Sie einen kurzen Namen oder eine Beschreibung für den Dienst ein.
  - **Auslösungssport:** Hier legen Sie einen Auslösungssport zum Öffnen des Eingangsports fest.

- **Protokoll:** Wählen Sie das Protokoll, TCP oder UDP.
  - **Eingangsport:** Legen Sie einen Eingangsport zum Empfang ankommender Daten aus dem Internet fest.
  - **Protokoll:** Wählen Sie das Protokoll, TCP oder UDP.
- 

#### **HINWEISE:**

- Wenn Sie sich mit einem IRC-Server verbinden, stellt der Client-PC eine abgehende Verbindung über den Auslösungsbereich 66660 – 7000 her. Der IRC-Server reagiert durch Überprüfung des Benutzernamens und erstellt über einen Eingangsport 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 Eingangsport zum Empfang der ankommenden Daten zu. Dieser Eingangsport 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 Eingangsport 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.
-

### 3.12.3 Virtueller Server/Portweiterleitung

Die Portweiterleitung ist ein Verfahren zum Umleiten von Netzwerkverkehr aus dem Internet an einen bestimmten Port oder bestimmten Portbereich zu einem oder mehreren Geräten im lokalen Netzwerk. Wählen Sie, die Portweiterleitung an Ihrem Router 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.

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 blank.

- 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 RT-AX57'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 RT-AX57's native FTP server.

Virtual Server / Port Forwarding\_FAQ

**Basic Config**

Enable Port Forwarding  OFF

**Port Forwarding List (Max Limit : 64)**

| Service Name      | External Port | Internal Port | Internal IP Address | Protocol | Source IP | Edit | Delete |
|-------------------|---------------|---------------|---------------------|----------|-----------|------|--------|
| No data in table. |               |               |                     |          |           |      |        |

Add profile

**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. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **Übernehmen**.
  - **Portweiterleitung aktivieren:** Wählen Sie **Yes (Ja)** zum Aktivieren der Portweiterleitung.
  - **Liste bekannter Server:** Bestimmen Sie, auf welche Art von Dienst Sie zugreifen möchten.

- **Liste bekannter Spiele:** Dieses Element führt Ports auf, die für das reibungslose Funktionieren beliebter Online-Games benötigt werden.
- **FTP-Server-Port:** Vermeiden Sie es, Ihrem FTP-Server den Portbereich 20:21 zuzuweisen, da dies mit der nativen FTP-Server-Zuweisung des Routers in Konflikt stehen würde.
- **Dienstname:** Geben Sie einen Dienstnamen ein.
- **Portbereich:** Wenn Sie einen Portbereich für Clients im selben Netzwerk festlegen möchten, geben Sie den Dienstnamen, den Portbereich (beispielsweise 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 **3.8 LAN**.

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

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

- Vergewissern Sie sich, dass Ihr Server oder Ihre Anwendung richtig eingerichtet und gestartet wurden.
- Sie benötigen einen Client (Internet-Client genannt), der sich außerhalb Ihres LANs befindet, aber auf das Internet zugreifen kann. Dieser Client sollte nicht 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.

### 3.12.4 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.

---

#### So richten Sie eine DMZ ein:

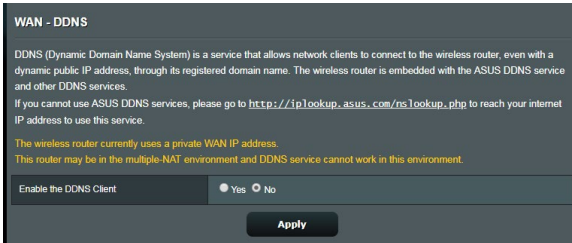
1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > WAN > DMZ**.
2. Konfigurieren Sie die folgenden Einstellungen. Klicken Sie zum Abschluss auf **Übernehmen**.
  - **IP-Adresse der exponierten Station:** Tragen Sie die LAN-IP-Adresse des Clients ein, der den DMZ-Dienst 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**.

### 3.12.5 DDNS

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



#### So richten Sie DDNS ein:

1. Wechseln Sie 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 Hostname:** Wählen Sie ASUS-DDNS oder Anderer DDNS. Wenn Sie den ASUS-DDNS verwenden möchten, tragen Sie den Hostnamen im Format xxx.asuscomm.com ein; das xxx ersetzen Sie durch Ihren Hostnamen.
  - Falls Sie einen anderen DDNS-Dienst nutzen möchten, klicken Sie auf „Kostenlos ausprobieren“ und registrieren sich zunächst online. Tragen Sie Benutzernamen/Email-Adresse und Kennwort oder den DDNS-Schlüssel in die gleichnamigen Felder ein.
  - **Platzhalter aktivieren:** Hier können Sie Platzhalter aktivieren, wenn diese von Ihrem DDNS-Dienst benötigt werden.

---

## HINWEIS:

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.
- 

## 3.12.6 NAT-Durchleitung

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

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

| WAN - NAT Passthrough   |         |
|---|---------|
| Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients. |         |
| PPTP Passthrough  | Enable  |
| L2TP Passthrough  | Enable  |
| IPsec Passthrough   | Enable  |
| RTSP Passthrough  | Enable  |
| H.323 Passthrough   | Enable  |
| SIP Passthrough   | Enable  |
| Enable PPPoE Relay  | Disable |

Apply



## 3.13 WLAN

### 3.13.1 Allgemein

Im Allgemein-Register können Sie WLAN-Grundeinstellungen konfigurieren.

| Wireless - General                             |  |
|--|--|
| Set up the wireless related information below. |  |
| Enable Smart Connect                           | <input type="checkbox"/> OFF   |
| Band   | 2.4GHz   |
| Network Name (SSID)                            | ASUS_2G  |
| Hide SSID                                      | <input type="radio"/> Yes <input checked="" type="radio"/> No                            |
| Wireless Mode                                  | Auto <input type="checkbox"/> Optimized for Xbox <input type="checkbox"/> Big Protection |
| Channel bandwidth                              | 20/40 MHz  |
| Control Channel                                | Auto <input type="checkbox"/> Current Control Channel: 4                                 |
| Extension Channel                              | Auto   |
| Authentication Method                          | WPA2-Personal  |
| WPA Encryption                                 | AES  |
| WPA Pre-Shared Key                             | 12345678   |
| Protected Management Frames                    | Disable  |
| Group Key Rotation Interval                    | 3600   |
| <input type="button" value="Apply"/>           |  |

#### So konfigurieren Sie die WLAN-Grundeinstellungen:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > General (Allgemein)**.
2. Wählen Sie 2,4 GHz oder 5 GHz als Frequenzband Ihres WLANs.
3. 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.

---

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

---

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. Wählen Sie unter den folgenden WLAN-Optionen aus, mit denen Sie festlegen können, welche WLAN-Gerätetypen sich mit Ihrem WLAN-Router verbinden können:
  - **Automatisch:** Wählen Sie **Auto**, um 802.11AX, 802.11AC, 802.11n, 802.11g und 802.11b 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.
  - **Nur N: N only (Nur N)** wählen Sie, wenn Sie maximale N-WLAN-Leistung wünschen. Diese Einstellung verhindert, dass sich 802.11g- und 802.11b-Geräte mit dem WLAN-Router verbinden können.
6. Wählen Sie eine dieser Kanalbandbreiten für höhere Übertragungsgeschwindigkeiten:
  - 40 MHz:** Wählen Sie diese Bandbreite, um den WLAN-Durchsatz zu maximieren.
  - 20 MHz (Standard):** Wählen Sie diese Bandbreite, wenn Sie auf Probleme mit Ihrer WLAN-Verbindung treffen.
7. Wählen Sie den Betriebskanal Ihres WLAN-Routers. Wählen Sie **Auto**, wenn der WLAN-Router automatisch einen besonders störungsfreien Kanal auswählen soll.

8. Wählen Sie eines der folgenden Authentisierungsverfahren:
- **Offenes System:** Diese Option bietet keine Sicherheit.
  - **WPA / WPA2 / WPA3 Personal / WPA Auto-Personal:** Diese Option bietet hohe Sicherheit. Sie können entweder WPA (mit TKIP), WPA2 (mit AES) oder WPA3 verwenden. Wenn Sie diese Option auswählen, müssen Sie TKIP + AES Verschlüsselung verwenden und das WPA-Kennwort (Netzwerkschlüssel) eingeben.
  - **WPA / WPA2 / WPA3 Enterprise / WPA Auto-Enterprise:** Diese Option bietet sehr hohe Sicherheit. Diese Lösung beinhaltet einen integrierten EAP-Server oder einen externen RADIUS Back-End-Authentifizierungserver.
- 

**HINWEIS:** Ihr WLAN-Router unterstützt die maximale Übertragungsrate von 54 Mb/s, wenn der **Wireless Mode (WLAN-Modus)** auf **Auto** und die **Encryption method (Verschlüsselungsverfahren)** auf **WEP** oder **TKIP** gesetzt wurde.

---

9. Wählen Sie eine dieser WEP (Wired Equivalent Privacy)-Verschlüsselungsoptionen für die über Ihr WLAN übertragenen Daten:
- **Aus:** Deaktiviert die WEP-Verschlüsselung
  - **64-bit:** Aktiviert eine unsichere WEP-Verschlüsselung
  - **128-bit:** Aktiviert eine verbesserte WEP-Verschlüsselung
10. Klicken Sie zum Abschluss auf **Apply (Übernehmen)**.

## 3.13.2 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.

---

The screenshot shows the 'Wireless - WPS' configuration page. At the top, there is a title 'Wireless - WPS' and a descriptive paragraph: '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.' Below this are several configuration fields: 'Enable WPS' with a green 'ON' toggle switch; 'Current Frequency' set to '2.4GHz'; 'Connection Status' set to 'Idle'; 'Configured' set to 'Yes' with a 'Reset' button; and 'AP PIN Code' with a text box containing '12345670'. Below these fields is a section titled 'You can easily connect a WPS client to the network in either of these two ways:' followed by two bullet points: 'Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.' and 'Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.' At the bottom, there is a 'WPS Method:' section with radio buttons for 'Push button' (selected) and 'Client PIN Code' (with an empty text box), and a 'Start' button.

### 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 benutzt standardmäßig das 2,4-GHz-Frequenzband. Wenn Sie das 5 GHz-Frequenzband nutzen möchten, schalten Sie die WPS-Funktion **OFF (Aus)**, klicken anschließend im Feld **Current Frequency (Aktuelle Frequenz)** auf **Switch Frequency (Frequenz umschalten)** und schalten dann WPS wieder **ON (Ein)**.

---

**HINWEIS:** WPS unterstützt Authentisierung per Open System, WPA-Personal, WPA2-Personal und WPA3-Personal. WPS unterstützt keine WLANs, die mit den Verschlüsselungsverfahren Shared Key, WPA-Enterprise, WPA2-Enterprise, WPA3-Enterprise oder RADIUS arbeiten.

---

4. Im Feld WPS-Methode wählen Sie **Push Button (Taste)** oder **Client PIN code (Client-PIN-Code)**. Wenn Sie sich für **Push Button (Taste)** entscheiden, fahren Sie mit Schritt 5 fort. Wenn Sie **Client PIN code (Client-PIN-Code)** wählen, machen Sie bei Schritt 6 weiter.
5. Zur WPS-Einrichtung über die WPS-Taste des Routers führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf **Start** oder drücken Sie die WPS-Taste an der Rückwand des WLAN-Routers.
  - b. Drücken Sie die WPS-Taste Ihres WLAN-Gerätes. Diese Taste erkennen Sie normalerweise am WPS-Logo.

---

**HINWEIS:** Schlagen Sie notfalls in der Bedienungsanleitung Ihres WLAN-Gerätes nach, wo sich die WPS-Taste befindet.

---

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

### 3.13.3 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.

**Wireless - Bridge**

Bridge (or named WDS - Wireless Distribution System) function allows your RT-AX55 to connect to an access point wirelessly. WDS may also be considered a repeater mode.

**Note:**

The function only support [Open System/NONE, Open System/WEP] security authentication method. To set up the corresponding authentication method, please select Legacy as your wireless mode first.  
[Click Here to modify.](#) Please refer to this [FAQ](#) for more details.

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.

You are currently using the Auto channel bandwidth. [Click Here to modify.](#)  
You are currently using the Auto channel. [Click Here to modify.](#)

**Basic Config**

|                        |   |
|------------------------|---|
| 2.4GHz MAC             | <input type="text" value="00:90:4C:32:80:00"/>                |
| 5GHz MAC               | <input type="text" value="00:90:4C:30:70:00"/>                |
| 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.    |                                  |

#### So richten Sie die WLAN-Brücke ein:

1. Wechseln Sie im Navigationspanel zu **Advanced Settings (Erweiterte Einstellungen) > Wireless (WLAN) > WDS.**
2. Wählen Sie das Frequenzband der WLAN-Brücke.

3. Wählen Sie im Feld **AP Mode (AP-Modus)** aus den folgenden Optionen:
  - **Nur AP:** Deaktiviert die WLAN-Brückenfunktion.
  - **Nur WDS:** Aktiviert die WLAN-Brückenfunktion, 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.

---

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


---

4. Klicken Sie im Feld **Connect to APs in list (Mit APs in der Liste verbinden)** auf **Yes (Ja)**, wenn Sie sich mit einem in der Externe-AP-Liste aufgeführten Zugangspunkt (AP) verbinden möchten.
5. Wählen Sie im Feld **Control Channel (Steuerungskanal)** den Betriebskanal für die WLAN-Brücke. Wählen Sie **Auto**, wenn der Router automatisch einen besonders störungsfreien Kanal auswählen soll.

---

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

---

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

---

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

---

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

### 3.13.4 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.

Wireless - Wireless MAC Filter

Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.

**Basic Config**

|                   |   |
|-------------------|---|
| Band              | 2.4GHz  |
| Enable MAC Filter | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| MAC Filter Mode   | Accept  |

**MAC filter list (Max Limit : 64)**

| Client Name (MAC Address) | Add / Delete                       |
|---------------------------|------------------------------------|
|                           | <input type="button" value="Add"/> |

No data in table.

#### 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 in der MAC-Filterliste auf die **Add (Hinzufügen)**-Schaltfläche , geben Sie dann die MAC-Adresse des WLAN-Gerätes ein.
5. Klicken Sie auf **Apply (Übernehmen)**.



### 3.13.5 RADIUS-Einstellungen

Die RADIUS-Einstellungen (Remote Authentication Dial In User Service) bieten eine zusätzliche Sicherheitsstufe, wenn Sie WPA-Enterprise, WPA2-Enterprise, WPA3-Enterprise oder Radius mit 802.1x als Authentisierungsverfahren wählen.

| Wireless - RADIUS Setting  |                      |
|--|----------------------|
| 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". |                      |
| Band   | 2.4GHz ▾             |
| Server IP Address  | <input type="text"/> |
| Server Port  | 1812                 |
| Connection Secret  | <input type="text"/> |
| <b>Apply</b>   |                      |

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

1. Vergewissern Sie sich, dass das Authentisierungsverfahren des WLAN-Routers auf WPA-Enterprise, WPA2-Enterprise oder WPA3-Enterprise eingestellt ist.

---

**HINWEIS:** Bitte lesen Sie zur Konfiguration des Authentisierungsverfahrens Ihres WLAN-Routers im Abschnitt **3.13.1 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. Legen Sie im Feld **Connection Secret (Verbindungskennwort)** das Kennwort zum Zugriff auf Ihren RADIUS-Server fest.
6. Klicken Sie auf **Apply (Übernehmen)**.

## 3.13.6 Professionell

Im Professionell-Bildschirm finden Sie erweiterte Konfigurationsoptionen.

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

Wireless - Professional

Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.  
\* Reminder: The System time zone is different from your locale setting.

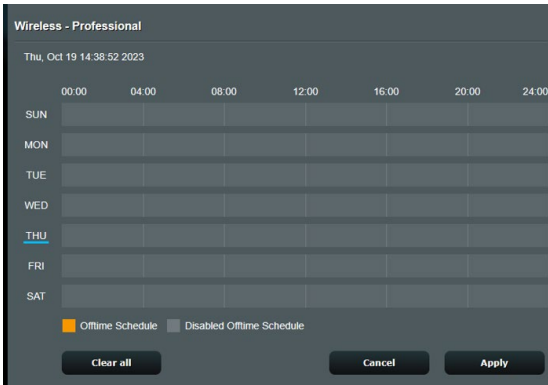
|                               |   |
|-------------------------------|---|
| Band                          | 2.4GHz  |
| Enable Radio                  | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Enable wireless scheduler     | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Set AP Isolated               | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Roaming assistant             | Enable Disconnect clients with RSSI lower than -55 dBm        |
| Bluetooth Coexistence         | Disable   |
| Enable IGMP Snooping          | Disable   |
| Multicast Rate(Mbps)          | Auto  |
| Preamble Type                 | Long  |
| AMPDU RTS                     | Enable  |
| RTS Threshold                 | 2347  |
| DTIM Interval                 | 3   |
| Beacon Interval               | 100   |
| Enable TX Bursting            | Enable  |
| Enable WMM                    | Enable  |
| Enable WMM No-Acknowledgement | Disable   |
| Enable WMM AFSD               | Enable  |
| Modulation Scheme             | Up to MCS 11 (VHT/QAM/1024-QAM)                               |
| Airtime Fairness              | Enable  |
| Multi-User MIMO               | Enable  |
| Explicit Beamforming          | Enable  |
| Universal Beamforming         | Enable  |

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:** Sie können das 24-Stunden- oder 12-Stunden-Uhrzeitformat wählen. Die Farbe in der Tabelle zeigt 'Zulassen' oder 'Verweigern' an. Klicken Sie auf jeden einzelnen Rahmen zum Ändern der Einstellungen der jeweiligen Stunde des Tages und klicken Sie auf **OK**, wenn Sie damit fertig sind.



- **AP isolieren:** Die AP-isolieren-Einstellung verhindert die Kommunikation von WLAN-Geräten im Netzwerk untereinander. Diese Funktion ist dann nützlich, wenn viele Gäste Ihr Netzwerk häufig besuchen oder verlassen. Wählen Sie **Yes (Ja)** zum Aktivieren dieser Funktion, **No (Nein)** zum Abschalten.
- **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.
- **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:** Die aktivierte WMM APSD-Einstellung (Wi-Fi Multimedia Automatic Power Save Delivery, Automatisches WLAN-Energiesparen bei Multimediadaten) verbessert die Energieverwaltung beim Zusammenspiel von WLAN-Geräten. Zum Abschalten der WMM APSD-Funktion wählen Sie **Disable (Deaktivieren)**.

# 4 Dienstprogramme

## HINWEISE:

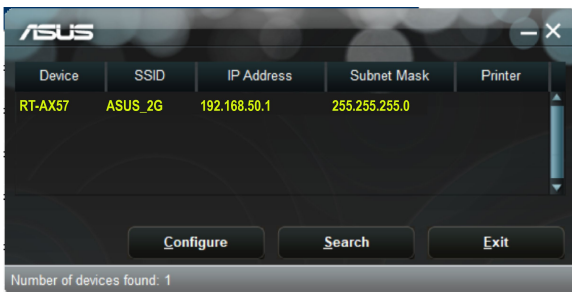
- Laden Sie die Dienstprogramme des WLAN-Routers von der ASUS-Webseite herunter und installieren Sie sie:
  - Device Discovery v1.4.7.1 unter <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip>
  - Firmware Restoration v1.9.0.4 unter <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
- Die Utilities (Dienstprogramme) werden unter MAC OS nicht unterstützt.

## 4.1 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.

### So starten Sie das Dienstprogramm Device Discovery:

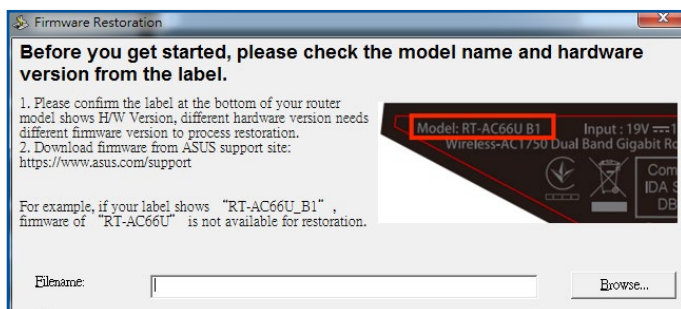
- Klicken Sie auf Ihrem Computer-Desktop auf: **Start > All Programs (Alle Programme) > ASUS Utility (ASUS Dienstprogramm) > Wireless Router (WLAN-Router) > Device Discovery.**



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

## 4.2 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.



---

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

---

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

---

## 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 3: Konfigurieren der allgemeinen und erweiterten Einstellungen.**

---

## 5 Fehlerbehebung

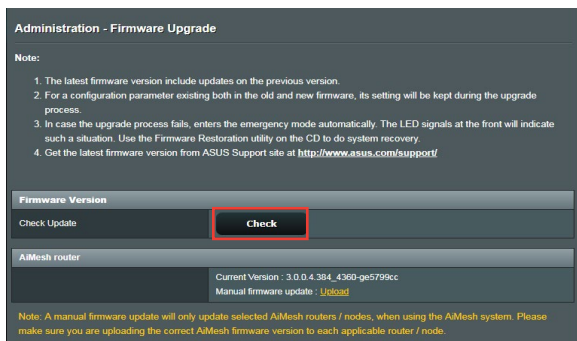
In diesem Kapitel finden Sie Lösungen zu Problemen, die eventuell mit Ihrem Router auftreten können. Falls Sie auf Probleme stoßen sollten, die nicht in diesem Kapitel behandelt werden, besuchen Sie die ASUS-Kundendienstseite: <https://www.asus.com/support/> – Hier finden Sie weitere Produktinformationen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

### 5.1 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 zu **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.



2. Sofern eine aktualisierte Firmware zur Verfügung steht, besuchen Sie die ASUS-Internetseite unter <https://www.asus.com/Networking/RT-AX57/HelpDesk/> und laden Sie die aktuellste Firmware herunter.
3. Klicken Sie auf der **Firmware Upgrade (Firmware-Aktualisierung)**-Seite auf **Browser (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.

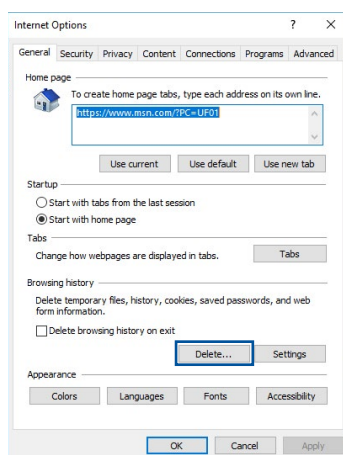
- Einige Kabelmodem-Dienstleister setzen voraus, dass die MAC-Adresse des Computers verwendet wird, der anfangs zur Kontoregistrierung genutzt wurde. Sie können die MAC-Adresse über die grafische Benutzeroberfläche abrufen: Wechseln Sie zur Seite **Network Map (Netzwerkübersicht)** > **Clients**, setzen Sie dann unter **Client Status** den Mauszeiger auf den Namen Ihres Gerätes.



## 5.2 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. 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)**.

The screenshot shows the 'LAN - DHCP Server' configuration page. It includes a description of DHCP, a 'Basic Config' section with fields for enabling the server, domain name, IP pool, lease time, and gateway. Below that is the 'DNS and WINS Server Setting' section, followed by 'Manual Assignment' and a table for manually assigned IP addresses. The table is currently empty, showing 'No data in table.' and an 'Apply' button at the bottom.

LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. supports up to 253 IP addresses for your local network.  
[Manually Assigned IP around the DHCP list FAQ](#)

**Basic Config**

Enable the DHCP Server  Yes  No

Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

**DNS and WINS Server Setting**

DNS Server

WINS Server

**Manual Assignment**

Enable Manual Assignment  Yes  No

**Manually Assigned IP around the DHCP list (Max Limit : 64)**

| Client Name (MAC Address) | IP Address           | Add / Delete                     |
|---------------------------|----------------------|----------------------------------|
| <input type="text"/>      | <input type="text"/> | <input type="button" value="⊕"/> |
| No data in table.         |                      |                                  |

- 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)**.

| Wireless - General                             |   |
|--|---|
| Set up the wireless related information below. |   |
| Enable Smart Connect                           | <input type="checkbox"/> OFF                                  |
| Band   | 2.4GHz  |
| Network Name (SSID)                            | ASUS_2G   |
| Hide SSID                                      | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Wireless Mode                                  | Auto <small>Optimized for Xbox Big Protection</small>         |
| Channel bandwidth                              | 20/40 MHz   |
| Control Channel                                | Auto <small>Current Control Channel: 4</small>                |
| Extension Channel                              | Auto  |
| Authentication Method                          | WPA2-Personal   |
| WPA Encryption                                 | AES   |
| WPA Pre-Shared Key                             | 12345678  |
| Protected Management Frames                    | Disable   |
| Group Key Rotation Interval                    | 3600  |
| <b>Apply</b>                                   |   |

- 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)**.

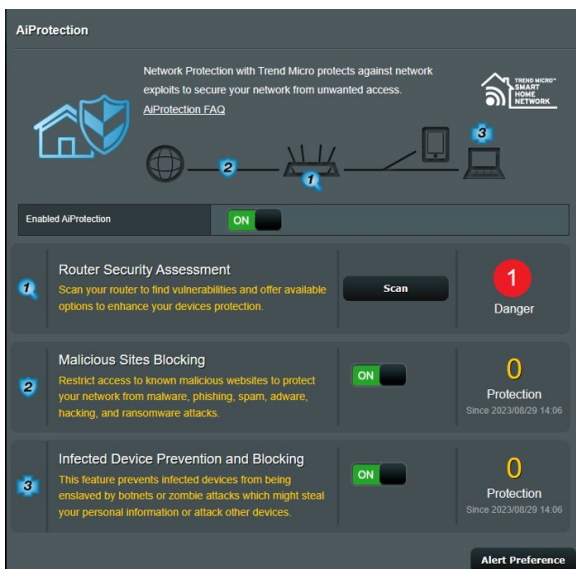
| Administration - Restore/Save/Upload Setting   |                                  |
|--|----------------------------------|
| This function allows you to save current settings to a file, or load settings from a file. |                                  |
| Factory default  | <b>Restore</b> <b>Initialize</b> |
| Save setting   | <b>Save</b>                      |
| Restore setting  | <b>Upload</b> 選擇檔案 上傳擇任何檔案       |

## Das Internet ist nicht zugänglich.

- Vergewissern Sie sich, dass sich Ihr Router mit der WAN-IP-Adresse Ihres Internetanbieters verbinden kann. Dazu rufen Sie die grafische Benutzeroberfläche auf, klicken auf **General (Allgemein) > Network Map (Netzwerkübersicht)** und prüfen den **Internet Status (Internetstatus)**.
- Falls sich Ihr Router nicht mit der WAN-IP-Adresse Ihres Internetanbieters verbinden kann, starten Sie 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. Wechseln Sie zu **General (Allgemein) > AiProtection > Parental Control (Jugendschutzeinstellungen)** und prüfen Sie, ob sich das Gerät in der Liste befindet. 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.

## 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)**.

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

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

Die werkseigenen Standardeinstellungen sind wie folgt:

|                          |   |
|--------------------------|---|
| <b>DHCP-Aktivierung:</b> | Ja (wenn das WAN-Kabel angeschlossen ist) |
| <b>IP-Adresse:</b>       | 192.168.50.1                              |
| <b>Domain-Name:</b>      | (Leer)                                    |
| <b>Subnetzmaske:</b>     | 255.255.255.0                             |
| <b>DNS-Server 1:</b>     | router.asus.com                           |
| <b>DNS-Server 2:</b>     | (Leer)                                    |
| <b>SSID (2,4 GHz):</b>   | ASUS                                      |
| <b>SSID (5 GHz):</b>     | ASUS_5G                                   |

## Firmware-Aktualisierung fehlgeschlagen.

Starten Sie den Rettungsmodus, starten Sie dann das Firmware-Wiederherstellungsprogramm. Hinweise zur Bedienung des Firmware-Wiederherstellungsprogramms finden Sie im Abschnitt **4.2 Firmware Restoration (Firmware-Wiederherstellung)**.

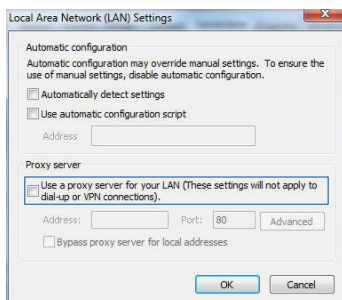
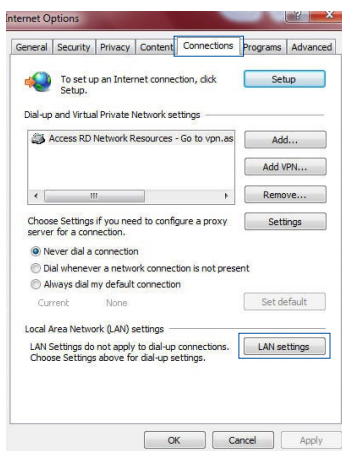
## Grafische Benutzeroberfläche lässt sich nicht aufrufen.

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

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

#### Windows

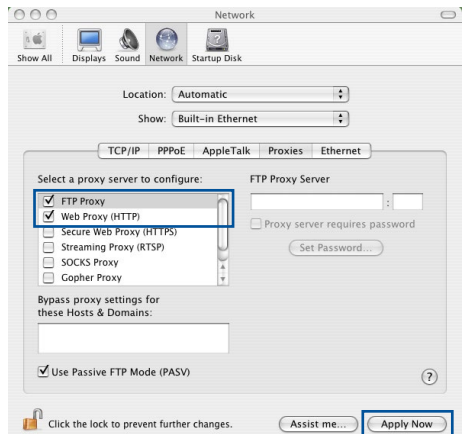
1. Klicken Sie auf **Start > Internet Explorer**, um den Webbrowser zu starten.
2. Klicken Sie auf **Tools (Extras) > Internet options (Internetoptionen) > Connections (Verbindungen) > LAN settings (LAN-Einstellungen)**.
3. Im Einstellungen-Bildschirm für das lokale Netzwerk (LAN) entfernen Sie das Häkchen 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)**.

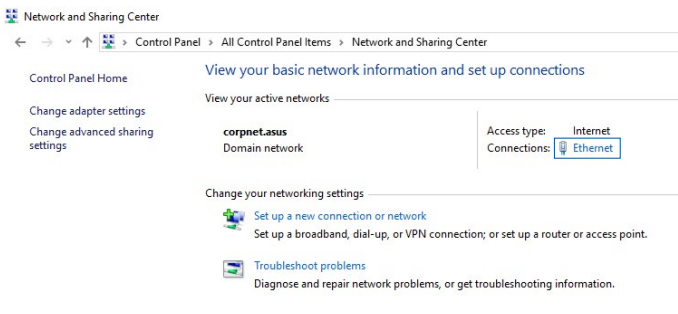


**HINWEIS:** Für Details zur Deaktivierung eines Proxyservers beziehen Sie sich auf die Hilfefunktion Ihres Browsers.

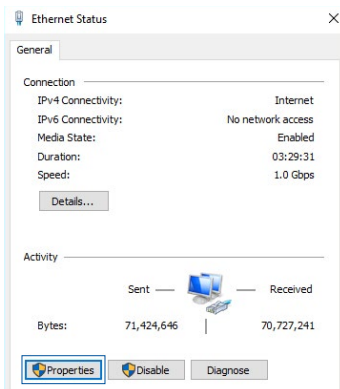
## B. Legen Sie die TCP/IP-Einstellungen so fest, dass Sie automatisch eine IP-Adresse erhalten.

### Windows

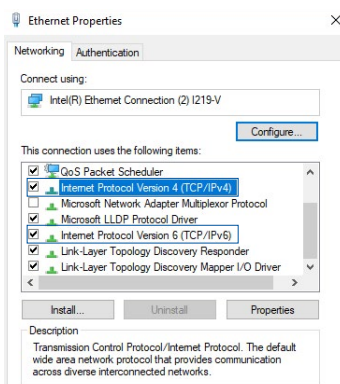
1. Klicken Sie auf **Start > Control Panel (Systemsteuerung) > Network and Sharing Center (Netzwerk- und Freigabecenter)**, klicken Sie dann auf die Netzwerkverbindung, um das Statusfenster anzuzeigen.



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



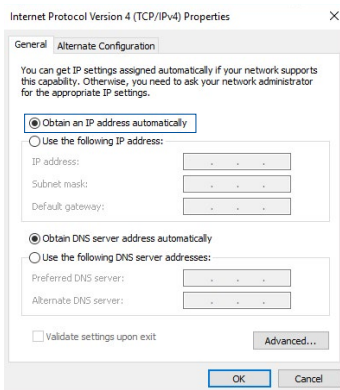
3. Wählen Sie **Internet Protocol Version 4 (TCP/IPv4) (Internetprotokoll Version 4 (TCP/IPv4))** oder **Internet Protocol Version 6 (TCP/IPv6) (Internetprotokoll Version 6 (TCP/IPv6))**, klicken Sie dann auf **Properties (Eigenschaften)**.




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

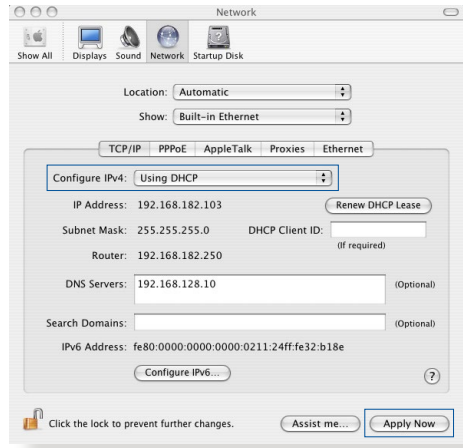
Um die IPv6-IP-Einstellungen automatisch zu beziehen, wählen Sie **Obtain an IPv6 address automatically (IPv6-Adresse automatisch beziehen)**.

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)**.

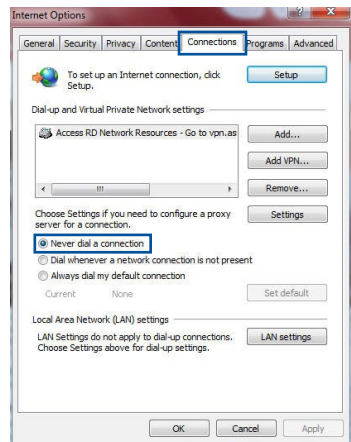


**HINWEIS:** Für Details zur Konfiguration der TCP/IP-Einstellungen beziehen Sie sich auf die Hilfefunktion Ihres Betriebssystems.

## 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

## 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. 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

## Sicherheitshinweise

Befolgen Sie bei der Verwendung dieses Produkts immer die grundlegenden Vorsichtsmaßnahmen, einschließlich, aber nicht beschränkt auf die folgenden:



### **WARNUNG!**

- Das Netzkabel muss an eine Steckdose angeschlossen werden, die mit einer geeigneten Erdung versehen ist. Schließen Sie das Gerät nur an eine nahe gelegene Steckdose an, die leicht zugänglich ist.
  - Falls das Netzteil defekt ist, versuchen Sie nicht, es selbst zu reparieren. Wenden Sie sich an den qualifizierten Kundendienst oder Ihre Verkaufsstelle.
  - Benutzen Sie KEINE beschädigten Netzkabel, Zubehörteile oder Peripheriegeräte.
  - Montieren Sie dieses Gerät NICHT in einer Höhe über zwei Metern.
  - Benutzen Sie das Gerät nur in Umgebungen, die eine Temperatur von 0°C (32°F) bis 40°C (104°F) aufweisen.
  - Lesen Sie die Bedienungsanleitung und halten Sie sich an den angegebenen Temperaturbereich, bevor Sie das Produkt verwenden.
  - Achten Sie besonders auf die Sicherheit von Personen bei der Benutzung dieses Gerätes in Flughäfen, Krankenhäusern, Tankstellen und professionellen Autowerkstätten.
  - Mögliche Störungen bei medizinischen Geräten: Halten Sie einen Mindestabstand von 15 cm (6 Zoll) zwischen implantierten medizinischen Geräten und ASUS Produkten, um die Gefahr von Störungen zu vermindern.
  - Benutzen Sie die ASUS Produkte, wenn es guten Empfang gibt, um die Strahlenbelastung zu minimieren.
  - Halten Sie das Gerät fern von schwangeren Frauen und bei Jugendlichen fern vom Unterleib/den Weichteilen.
  - Verwenden Sie dieses Produkt NICHT, wenn sichtbare Schäden festzustellen sind oder wenn es nass geworden, beeinträchtigt oder modifiziert worden ist. Wenden Sie sich an den Kundendienst, um Unterstützung zu erhalten.
-



## **WARNUNG!**

- Stellen Sie das Gerät NICHT auf schräge oder instabile Arbeitsflächen.
  - Legen Sie KEINE Gegenstände auf das Gerät und lassen Sie keine Gegenstände darauf fallen. Vermeiden Sie es, das Produkt oder Teile des Produkts mechanischen Erschütterungen auszusetzen, z. B. durch Quetschen, Verbiegen, Durchstechen oder Zerkleinern.
  - Dieses Gerät darf NICHT geöffnet, auseinandgebaut, im Mikrowellenherd erhitzt, verbrannt oder bemalt werden und es dürfen KEINE Fremdkörper in dieses Gerät geschoben werden.
  - Prüfen Sie am Aufkleber an der Geräteunterseite, ob Ihr Netzteil den Stromversorgungsanforderungen entspricht.
  - Halten Sie das Produkt von Wärmequellen und offenem Feuer fern.
  - Setzen Sie das Gerät KEINESFALLS Flüssigkeiten, Regen oder Feuchtigkeit aus, verwenden Sie es nicht in der Nähe derartiger Gefahrenquellen. Verwenden Sie das Produkt nicht während eines Gewitters.
  - Verbinden Sie die PoE-Ausgänge dieses Geräts ausschließlich mit PoE-Systemen, ohne Routing zu externen Systemen.
  - Um die Gefahr eines Stromschlags zu verhindern, ziehen Sie das Netzkabel aus der Steckdose, bevor Sie das System an einem anderen Ort aufstellen.
  - Verwenden Sie nur Zubehör, das vom Gerätehersteller für die Benutzung mit diesem Modell zugelassen wurde. Die Verwendung anderer Arten von Zubehör kann zum Erlöschen der Garantie führen oder gegen örtliche Vorschriften und Gesetze verstoßen und ein Sicherheitsrisiko darstellen. Wenden Sie sich an Ihren Händler vor Ort, damit Sie sich über die Verfügbarkeit von autorisiertem Zubehör informieren können.
  - Die Verwendung dieses Produkts in einer Weise, die nicht in der mitgelieferten Anleitung empfohlen wird, kann zu Brand- oder Verletzungsgefahr führen.
-

## Service und Support

Besuchen Sie unsere mehrsprachige Webseite unter <https://www.asus.com/support>.

