



SW22795

TUF GAMING

USER MANUAL

Trådlös TUF AX3000 V2 spelrouter

ASUS

SW22795

Första Utgåvan

November 2023

Upphovsrätt © 2023 ASUSTeK Computer Inc. Alla rättigheter förbehållna.

Ingen del av den här manualen, inräknat produkter och programvara som beskrivs i den, får reproduceras, överföras, kopieras, sparas i ett återvinningssystem eller översättas till något språk i någon form eller på något sätt, förutom dokumentation som behålls av köparen i uppbackningssyfte, utan skriftlig tillåtelse från ASUSTeK Computer Inc. ("ASUS").

Produktgaranti eller service kommer inte att förlängas om: (1) produkten är reparerad, modifierad eller ändrad, såvida inte sådan reparation, modifikation eller ändring skriftligt godkänts av ASUS; eller (2) serienumret på produkten gjorts oläsligt eller saknas.

ASUS TILLHANDAHÅLLER DEN HÄR MANUALEN I "BEFINTLIGT SKICK" UTAN NÅGON SLAGS GARANTI, VARE SIG UTTRYCKLIGEN ELLER TILLÄMPBART, INRÄKNAT MEN INTE BEGRÄNSAT TILL TILLÄMPBARA GARANTIER ELLER VILLKOR FÖR KÖPSKAP ELLER TILLPASSNING TILL SÄRSKILT SYFTE. UNDER INGA OMSTÄNDIGHETER SKALL ASUS, DESS DIREKTÖRER, TJÄNSTEMÄN, ANSTÄLLDA ELLER REPRESENTANTER HÅLLAS ANSVARIGA FÖR NÅGRA INDIREKTA, SÄRSKILDA, TILLFÄLLIGA ELLER HÄRAV FÖLJANDE SKADOR (INKLUSIVE SKADOR AVSEENDE FÖRLUST AV FÖRTJÄNST, AFFÄRSFÖRLUSTER, FÖRLUST AV ANVÄNDNING ELLER DATA, AVBROTT AV AFFÄRSVERKSAMHET ELLER LIKNADE) ÄVEN OM ASUS HAR AVISERAT OM MÖJLIGHETEN AV ATT SÅDANA SKADOR KAN UPPSTÅ FRÅN NÅGRA DEFEKTER ELLER FEL I DENNA MANUAL ELLER PRODUKT.

SPECIFIKATIONER OCH INFORMATION I DENNA MANUAL LÄMNAS ENDAST SOM INFORMATION OCH KAN ÄNDRAS NÄR SOM HELST UTAN MEDDELANDE OCH SKALL INTE TOLKAS SOM ETT ÅTAGANDE AV ASUS. ASUS PÅTAR SIG INGET ANSVAR ELLER SKYLDIGHET FÖR NÅGRA FEL ELLER BRISTER SOM KAN VISA SIG I DENNA MANUAL INKLUSIVE PRODUKTER OCH PROGRAM SOM BESKRIVS DÄRI.

Produkter och företagsnamn som visas i denna manual kan eller kan inte vara registrerade varumärken eller upphovsrättsligt skyddade av respektive företag och används endast för identifiering eller förklaring och till ägarens fördel utan intrångsavsikt.

Innehållsförteckning

1	Lär känna din trådlösa router	
1.1	Välkommen!	7
1.2	Paketinnehåll	7
1.3	Din trådlösa router.....	8
1.4	Placering av din router	10
1.5	Installationskrav.....	11
2.	Komma igång	
2.1	Routerinstallation.....	12
	A. Kabelanslutning	12
	B. Trådlös anslutning	13
2.2	Snabb internetinställning (QIS) med autodetektering.....	15
2.3	Ansluta till ditt trådlösa nätverk	18
3	Konfigurera de Allmänna och Avancerade inställningar	
3.1	Inloggning till Web GUI.....	19
3.2	Anpassad tjänst kvalitet - QoS.....	21
3.3	Administration	22
	3.3.1 Driftläge.....	22
	3.3.2 System.....	23
	3.3.3 Uppgradering av fast programvara	24
	3.3.4 Återställ/Spara/Överför inställning	24
3.4	AiCloud 2.0	25
	3.4.1 Molndisk.....	26
	3.4.2 Smart Access.....	28
	3.4.3 AiCloud synkronisering.....	29
3.5	AiMesh	30
	3.5.1 Före inställning	30

Innehållsförteckning

3.5.2	Inställningssteg för AiMesh	30
3.5.3	Felsökning	33
3.5.4	Omplacering	34
3.5.5	FAQs (Vanliga Frågor)	35
3.6	Aiprotection	36
3.6.1	Konfigurering av Aiprotection	37
3.6.2	Blockering av skadliga webbplatser.....	39
3.6.3	Tvåvägs-IPS.....	40
3.6.4	Skydd och blockering av infekterad enhet.....	41
3.7	Brandvägg	42
3.7.1	Allmänt	42
3.7.2	URL-filter.....	42
3.7.3	Nyckelordsfilter.....	43
3.7.4	Nätverkstjänstfilter	44
3.8	Spel.....	45
3.8.1	Växelgas.....	46
3.8.2	Öppen NAT	47
3.9	Gästnätverk	48
3.10	IPv6.....	50
3.11	LAN.....	51
3.11.1	LAN IP	51
3.11.2	DHCP-server	52
3.11.3	Route	54
3.11.4	IPTV	55
3.12	Nätverkskartan	56
3.12.1	Inställning av de trådlösa säkerhetsinställningarna	57
3.12.2	Hantera dina nätverksklienter	58
3.12.3	Övervaka din USB-enhet	59

Innehållsförteckning

3.13	Klassificeringskontroll	61
3.14	Smart anslutning.....	64
	3.14.1 Konfigurera Smart anslutning	64
3.15	Systemlogg.....	65
3.16	Trafkanalys.....	66
3.17	USB-applikation	67
	3.17.1 Använda AiDisk.....	68
	3.17.2 Använda Servers Center	70
	3.17.3 3G/4G	75
3.18	VPN.....	76
	3.18.1 VPN-server	76
	3.18.2 VPN-fusion.....	77
	3.18.3 Instant Guard.....	79
3.19	WAN	80
	3.19.1 Internetanslutning.....	80
	3.19.2 Dubbel WAN.....	83
	3.19.3 Portutlösning.....	84
	3.19.4 Virtuell server/Portvidarebefordran	86
	3.19.5 DMZ.....	89
	3.19.6 DDNS	90
	3.19.7 NAT-genomströmning	91
3.20	Trådlös anslutning	92
	3.20.1 Allmänt	92
	3.20.2 WPS	94
	3.20.3 Brygga.....	96

3.20.4	Trådlöst MAC-filter	98
3.20.5	RADIUS-inställning	99
3.20.6	Professionell	100
4	Verktyg	
4.1	Enhetsidentifiering	103
4.2	Återställning av fast programvara	104
4.3	Installera din skrivarserver	105
4.3.1	Delning av EZ-skrivare	105
4.3.2	Använd LPR för att dela skrivare	109
4.4	Hämtningsadministratör	114
4.4.1	Konfigurera hämtningsinställningar för Bit Torrent	115
4.4.2	NZB-inställningar	116
5	Felsökning	
5.1	Grundläggande felsökning	117
5.2	Vanliga frågor (FAQs)	119
	Bilagor	
	Service och support	137

1 Lär känna din trådlösa router

1.1 Välkommen!

Tack för ditt köp av en trådlös Trådlös TUF spelrouter!

Den designade router har 2,4 GHz och 5 GHz dubbla band för en oöverträffad jämlöpande trådlös HD-strömning: SMB-server, UPnP AV-server och FTP-server för fildelning dygnet runt; en möjlighet att hantera 300 000 sessioner och ASUS gröna nätverksteknologi, vilken ger en lösning för energibesparing på upp till 70 %.

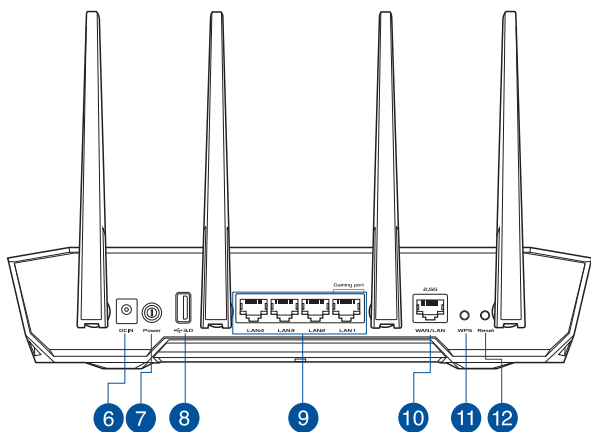
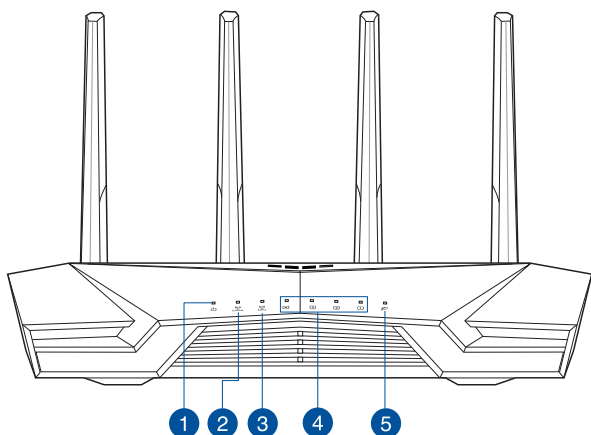
1.2 Paketinnehåll

- | | |
|--|--|
| <input checked="" type="checkbox"/> Trådlös TUF spelrouter | <input checked="" type="checkbox"/> Strömadapter |
| <input checked="" type="checkbox"/> Nätverkskabel (RJ-45) | <input checked="" type="checkbox"/> Snabbstartshandbok |

NOTER:

- Om någon av artiklarna är skadad eller saknas, kontakta ASUS för tekniska frågor och support, se listan över direkttelefonnummer till ASUS Support på baksidan av denna bruksanvisning.
 - Spara originalförpackningsmaterialet ifall du i framtiden behöver garantiservice såsom reparation eller utbyte.
-

1.3 Din trådlösa router



1

Strömlysdiod

Av: Ingen ström.

På: Enheten är klar.

Blinkar sakt: Räddningsläge.

2

2,4 GHz LED

Av: Ingen 2,4 GHz signal.

På: Trådlöst system är redo.

Blinkar snabbt: Sänder eller tar emot data via trådlös anslutning.

-
- 3 5 GHz LED**
Av: Ingen 5 GHz signal.
På: Tråslöst system är redo.
Blinkar snabbt: Sänder eller tar emot data via trådlös anslutning.

 - 4 Lysdiod LAN 1~4**
Av: Ingen ström eller fysisk anslutning.
På: Har fysisk anslutning till ett LAN (Local Area Network).

 - 5 2,5G/1G WAN (Internet) LED**
Av: Ingen 2,5G/1G WAN anslutning.
På: Har fysisk anslutning till 2,5G/1G WAN port.

 - 6 Strömingång (DCIN)**
Sätt in den medföljande strömadaptern i denna port för att ansluta din router till en strömkälla.

 - 7 Strömbrytare**
Tryck på denna knapp för att starta eller stänga av systemet.

 - 8 USB 3.2 Gen 1-port**
Sätt in en USB 3.2 Gen 1-kompatibel enhet som en USB-hårddisk eller ett USB-minne i denna port.

 - 9 LAN 1~4 portar**
Anslut nätverkskablar i dessa portar för att etablera LAN-anslutning.

 - 10 2,5G/1G WAN (Internet) port**
Anslut en nätverkskabel i denna port för att etablera 2,5G/1G WAN-anslutning.

 - 11 WPS knapp**
Håll knappen intryckt för att starta WPS-guiden.

 - 12 Återställningsknapp**
Denna knapp återställer systemet till fabrikenes förinställningar.
-

NOTER:

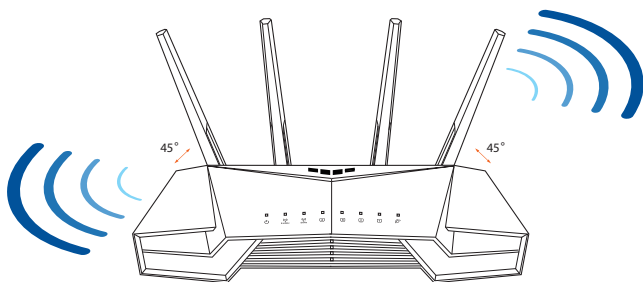
- Använd endast adaptern som följer med i ditt paket. Användning av andra adaptrar kan skada enheten.
- **Specifikationer:**

DC-strömadapter	DC-uteffekt: +12V med max 1,5A ström		
Driftstemperatur	0~40°C	Förvaring	0~70°C
Luftfuktighet vid drift	50~90%	Förvaring	20~90%

1.4 Placering av din router

För bästa trådlösa signalsändning mellan den trådlösa routern och nätverksenheterna som är anslutna till den, se till att du:

- Placerar den trådlösa routern på en central plats för maximal trådlös täckning för nätverksenheterna.
- Håll enheten undan från metallhinder och undan från direkt solljus.
- Håll enheten borta från 802.11g eller 20 MHz endast Wi-Fi-enheter, 2,4 GHz datorutrustning, Bluetooth-enheter, sladdlösa telefoner, transformatorer, kraftiga motorer, fluorescerande ljus, mikrovågsugnar, kylskåp och andra industriella utrustningar, för att förhindra signalstörningar eller signalförluster.
- Uppdatera alltid till senaste inbyggda programvara. Besök ASUS webbplats på: <http://www.asus.com> för att hämta senaste uppdateringar för den inbyggda programvaran.
- För att säkerställa bästa trådlösa signal, rikta de fyra avtagbara antennerna som på bilden nedan.



1.5 Installationskrav

För att installera ditt trådlösa nätverk behöver du en dator som uppfyller följande sytemkrav:

- Ethernet RJ-45-port (LAN) (10Base-T / 100Base-TX / 1000Base-TX)
- IEEE 802.11a/b/g/n/ac/ax trådlös kapacitet
- En installerad TCP/IP-tjänst
- Webbbläsare såsom Internet Explorer, Firefox, Safari eller Google Chrome

NOTER:

- Om din dator inte har inbyggd trådlös anslutningsmöjlighet kan du installera en IEEE 802.11a/b/g/n/ac/ax WLAN-adapter till din dator för att ansluta till nätverket.
- Med dess dubbla bandteknologi stöder din trådlösa router 2,4 GHz och 5 GHz trådlösa signaler samtidigt. Detta gör att du kan utföra internetrelaterade aktiviteter eller läsa/skriva e-postmeddelanden med 2,4 GHz-bandet medan du samtidigt kan strömma högdefinitions ljud/-videofiler såsom filer eller musik med 5 GHz-bandet.
- Vissa IEEE 802.11 n-enheter som du vill ansluta till ditt nätverk kanske inte stödjer 5 GHz-band. Se enhetens bruksanvisning för specifikationer.
- Ethernet RJ-45-kabeln som du kommer att använda för att ansluta nätverksenheter bör inte översiga 100 meter.

VIKTIGT!

- Vissa trådlösa adaptrar kan anslutningsproblem med 802.11ax WiFi-anslutningspunkter.
- Om du har den typen av problem, måste du uppdatera drivrutinen till den senaste versionen. iver to the latest version. Kontrollera att tillverkarens officiella supportwebbplats med drivrutiner och uppdateringar för programvaran, och annan relaterad information finns.
 - Realtek: <https://www.realtek.com/en/downloads>
 - Mediatek: <https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi>
 - Intel: <https://downloadcenter.intel.com/>

2. Komma igång

2.1 Routerinstallation

VIKTIGT!

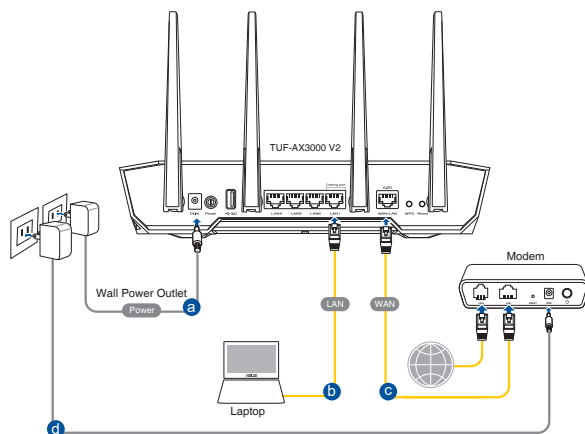
- Använd en kabelanslutning när du installerar din trådlösa router för att förhindra eventuella installationsproblem.
- Innan du ställer in din trådlösa ASUS-router, gör följande:
- Om du byter ut en existerande router, ska den kopplas ifrån ditt nätverk.
- Koppla ifrån alla kablas/sladdar från din nuvarande modeminstallation. Om ditt modem har ett reservbatteri, ta även bort detta.
- Starta om kabelmodem och dator (rekommenderas).

A. Kabelanslutning

NOTERA: Du kan använda antingen en rak eller en korsad kabel för kabelanslutning.

För att ställa in din trådlösa router via kabelanslutning:

1. Anslut din router till ett strömuttag och slå på den. Anslut nätverkskabeln från din dator till en LAN-port på din router.



2. Webb GUI startar automatiskt när du öppnar en webbläsare. Om den inte startar automatiskt, öppna <http://www.asusrouter.com>.
3. Ställ in ett lösenord för din router för att undvika obehörig åtkomst.

Login Information Setup

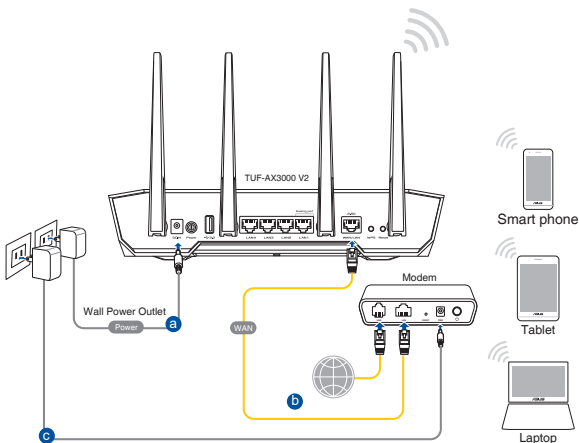
Change the router password to prevent unauthorized access to your ASUS wireless router.

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

B. Trådlös anslutning

Ställ in din trådlösa router via trådlös anslutning:

1. Anslut din router till ett strömuttag och slå på den.



2. Anslut till nätverkets namn (SSID) som står på produktens etikett på baksidan av routern. För bättre nätverkssäkerhet, byt till ett unikt SSID och tilldela ett lösenord.



2,4 G Wi-Fi-namn (SSID):	ASUS_XX_2G
5G Wi-Fi-namn (SSID):	ASUS_XX_5G

* **XX** syftar på de två sista siffrorna på 2,4 GHz MAC-adress. Du kan hitta den på etiketten på baksidan av din ASUS.

3. När du är ansluten startar webb GUI automatiskt när du öppnar en webbläsare. Om den inte startar automatiskt, öppna <http://www.asusrouter.com>.
4. Ställ in ett lösenord för din router för att undvika obehörig åtkomst.

NOTER:

- För detaljer om anslutning till ett trådlöst nätverk, se WLAN-adaptrar i bruksanvisningen.
 - För inställning av säkerhetsinställningarna för ditt nätverk se avsnitt 3 **Setting up the wireless security settings (Inställning av de trådlösa säkerhetsinställningarna)** i denna bruksanvisning.
-

Login Information Setup

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

Router Login Name: admin

New Password: [Empty field]

Retype Password: [Empty field] Show password

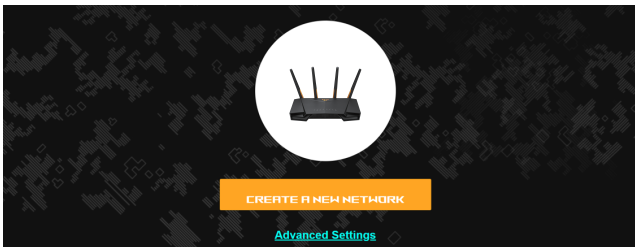
2.2 Snabb internetinställning (QIS) med autodetektering

Quick Internet Setup (QIS) funktionen vägleder dig i snabbinställningen av din Internetanslutning.

NOTERA: Vid inställning av Internetanslutningen för första gången, tryck på Reset-knappen på din trådlösa router, för att återställa den till tillverkarens standardinställning.

Använda QIS med autodetektering:

1. Starta en webbläsare. du kommer att bli omdirigerad till ASUS installationsguide [Quick Internet Setup (Snabb Internetinställning)]. Om inte, ange <http://www.asusrouter.com> manuellt.

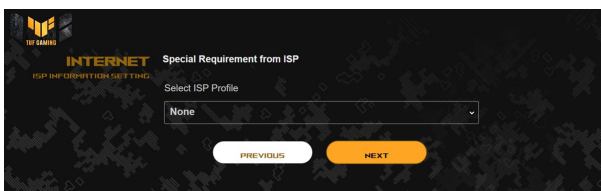
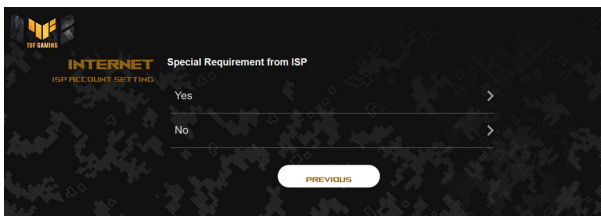


2. Den trådlösa routern upptäcker automatiskt om din ISP-anslutningstyp är **Dynamic IP (Dynamisk IP)**, **PPPoE**, **PPTP**, och **L2TP**. Knappa in den nödvändiga informationen för din ISP-anslutningstyp.

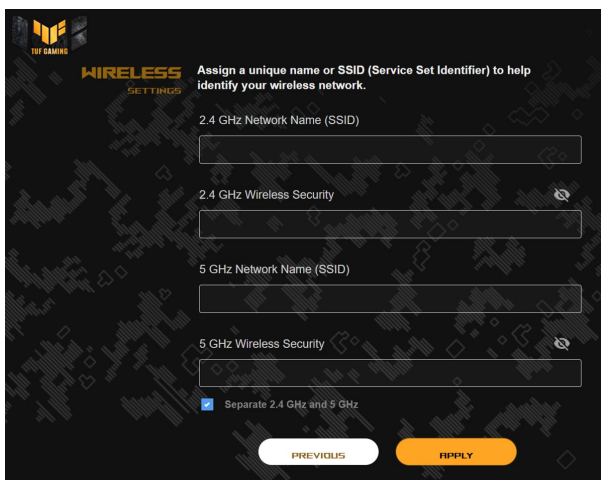
VIKTIGT! Skaffa den nödvändiga informationen om din Internetanslutningstyp från din ISP (internetleverantör).

NOTER:

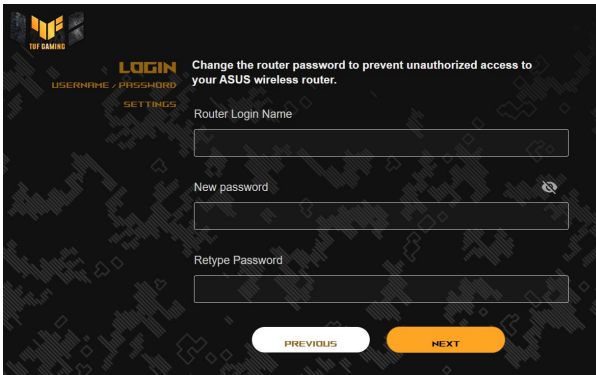
- Auto-detection (Autodetektering) av din ISP-anslutning sker när du konfigurerar den trådlösa routern första gången eller när din trådlösa router återställs till dess standardinställning.
 - Om QIS misslyckas att detektera din Internetanslutningstyp klicka på **Skip to manual setting (Hoppa över till manuell inställning)** och konfigurera din anslutningsinställning manuellt.
-



3. Tilldela det trådlösa nätverksnamnet (SSID) och säkerhetsnyckeln för din 2,4 GHz och 5 GHz trådlösa anslutning. Klicka på **APPLY (VERKSTÄLL)** när du är klar.



4. På sidan **Login Information Setup (Inställning av inloggningsinformation)**, ändra routerns inloggningslösenord för att förhindra otillåten åtkomst till din trådlösa router.



LOGIN
USERNAME / PASSWORD
SETTINGS

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

Router Login Name

New password

Retype Password



PREVIOUS NEXT

NOTER: Den trådlösa routerns användarnamn och lösenord skiljer sig från 2,4 GHz/5 GHz nätverksnamn (SSID) och säkerhetsnyckel. Den trådlösa routerns användarnamn och lösenord ger dig möjlighet att logga in på din trådlösa routers Web GUI för att konfigurera inställningarna för den trådlösa routern. 2,4 GHz/5 GHz nätverksnamn (SSID) och säkerhetsnyckel ger Wi-Fi-enheter möjlighet att logga in och ansluta till ditt 2,4 GHz/5 GHz nätverk.

2.3 Ansluta till ditt trådlösa nätverk

När den trådlösa routern installerats via QIS, kan du ansluta datorn eller andra smarta enheter till det trådlösa nätverket.

Anslutning till ditt nätverk:

1. Klicka på nätverksikonen  i meddelandefältet på datorn för att visa tillgängliga trådlösa nätverk.
2. Välj det trådlösa nätverk som du vill ansluta till, klicka sedan på **Connect (Anslut)**.
3. Du kan behöva knappa in nätverkets säkerhetsnyckel för ett säkert trådlöst nätverk, klicka sedan på **OK**.
4. Vänta medan din dator etablerar en anslutning till det trådlösa nätverket. Anslutningens status visas och nätverksikonen visar den anslutna  statusen.

NOTER:

- Se nästa avsnitt för fler detaljer om hur man konfigurerar inställningarna för det trådlösa nätverket.
 - Se enheternas bruksanvisningar för fler detaljer för hur man ansluter till det trådlösa nätverket.
-

3 Konfigurera de Allmänna och Avancerade inställningar

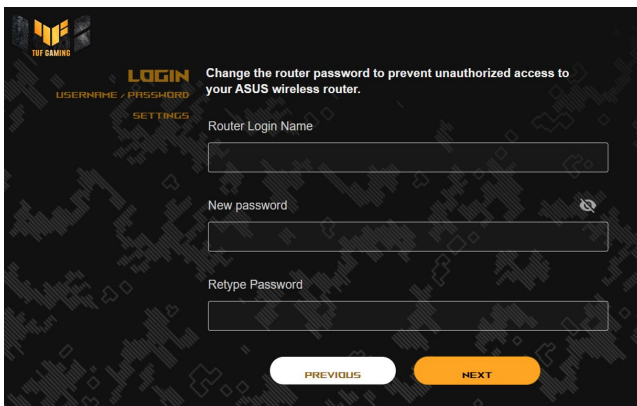
3.1 Inloggning till Web GUI

Din trådlösa TUF spelrouter levereras med ett intuitivt grafiskt webbgränssnitt (GUI) - TUF Gaming Center, som ger dig fullständig nätverkskontroll, med nödvändig information som status för ansluten enhet och ping-värden för spelservrar i hela världen, och direkt åtkomst till alla fantastiska spelfunktioner.

NOTERA: Funktionerna kan variera mellan olika versioner av fasta program.

Inloggning till Web GUI:

1. Skriv manuellt in den trådlösa routerns standard IP-adress i webbläsaren: <http://www.asusrouter.com>.
2. Nyckel i standardanvändarnamnet (**admin**) och lösenorder som du har ställt in i **2.2 Quick Internet Setup (QIS) with Auto-dection (Snabb Internetkonfiguration (QIS) med autodetektering)** på inloggningsidan.



3. Nu kan du använda Web GUI för att konfigurera olika inställningar för din trådlösa ASUS-router.

Översta kommandoknapparna

The screenshot displays the TUF Gaming web GUI interface. At the top, there are 'Logout' and 'English' buttons. The main content area is divided into several sections:

- General:** Includes 'Quick Internet Setup' (QIS), 'Network Map', 'AiMesh', 'Guest Network', 'AiProtection', 'Parental Controls', 'Game Boost', 'Open NAT', 'Adaptive QoS', 'Traffic Analyzer', 'USB Application', and 'AiCloud 2.0'.
- Advanced Settings:** Includes 'Wireless', 'LAN', 'WAN', and 'Amazon Alexa'.
- System Status:** Shows 'Wireless' status for 2.4 GHz and 5 GHz bands, including Network Name (SSID), Authentication Method, WPA Encryption, and WPA-PSK key.
- WPA2-Personal:** Shows 'Internet status: Connected' with IP address 192.168.123.36 and gateway 192.168.1.1. It also displays 'WPA2-Personal' security settings.
- USB 3.0:** Shows 'Clients: 1' and 'USB 3.0: No Device'.
- AI Mesh Node:** Shows 'AI Mesh Node: 0'.

Annotations on the image point to specific features:

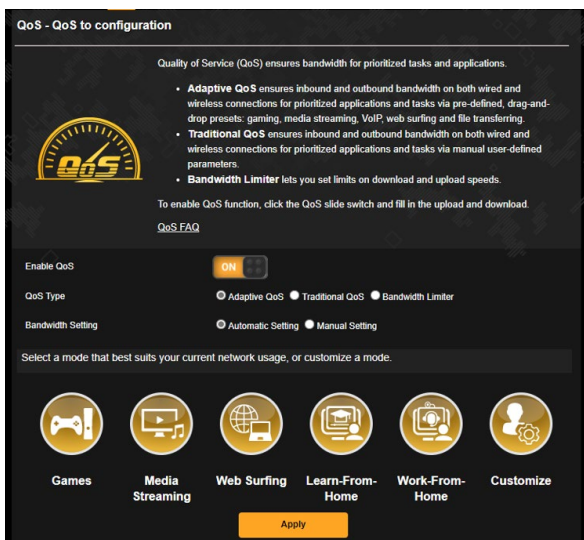
- QIS:** Points to the 'Quick Internet Setup' button.
- Informationsbanderoll:** Points to the top status bar.
- Navigering panel:** Points to the left-hand menu.

* Bilden är endast som referens.

NOTERA: Om du loggar in på Web GUI för första gången, kommer du automatiskt att bli hänvisad till sidan Quick Internet Setup (QIS/ snabb internetinställning).

3.2 Anpassad tjänst kvalitet - QoS

Denna funktion säkerställer bandbredd för prioriterade uppgifter och applikationer.



Konfigurera Anpassad tjänst kvalitet - QoS:

1. Från navigeringsfältet, gå till **General (Allmänt) > Adaptive QoS (Anpassad tjänst kvalitet - QoS) > QoS (Tjänst kvalitet)**.
2. Från fältet **Enable QoS (Aktivera tjänst kvalitet)**, klicka på **ON (PÅ)**.
3. Välj Typ av tjänst kvalitet (Anpassad Tjänst kvalitet - QoS, Traditionell Tjänst kvalitet - QoS eller Bandbreddbegränsare) för din konfiguration.

NOTERA: Se fliken QoS (Tjänst kvalitet) för definitionen av QoS Type (Typ av tjänst kvalitet).

4. Klicka på **Automatic Setting (Automatisk inställning)** för optimal bandbredd automatiskt eller **Manual Setting (Manuell inställning)** för att ställa in bandbredden för upp och nedladdning manuellt.

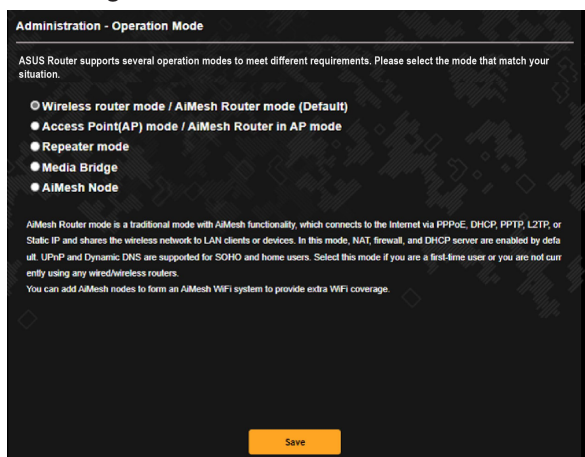
NOTERA: Hämta bandbredds information från din ISP. Du kan även gå till <http://speedtest.net> för att kontrollera och hämta din bandbredd.

5. Klicka på **Apply (Verkställ)**.

3.3 Administration

3.3.1 Driftläge

Sidan Operation Mode (Driftläge) ger dig möjlighet att välja passande läge för ditt nätverk.



Ställa in driftläget:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Administration > Operation Mode (Driftläge)**.
2. Välj något av dessa driftlägen:
 - **Läge för trådlös router / AiMesh Router-läge (standard):** I trådlös router-läge ansluter den trådlösa routern till Internet och ger Internetåtkomst till tillgängliga enheter i det lokala nätverket.
 - **Access Point (AP)-läge / AiMesh Router i AP-läge:** I detta läge skapar routern ett nytt trådlöst nätverk på ett befintligt nätverk.
 - **Repeater mode (Repeterarläge):** I Repetitionsläge ansluter TUF-AX3000 V2 trådlöst till ett befintligt trådlöst nätverk för att utvidga den trådlösa täckningen. I detta läge inaktiveras brandväggs-, IP-delnings- och NAT-funktionerna.
 - **Mediebrygga:** Denna installation kräver två trådlösa routrar. Den andra router fungerar som en brygga där flera enheter som Smart-TVs och spelkonsoler kan anslutas via Ethernet.
 - **AiMesh-Nod:** Denna inställning kräver minst två ASUS-routrar med stöd för AiMesh. Aktivera AiMesh-noden och logga in på AiMesh-routerns webbgränssnitt för att söka efter tillgängliga AiMesh-noder i närheten av ditt AiMesh-system. AiMesh-systemet ger en täckning i hela hemmet och centraliserad hantering.

3. Klicka på **Apply (Verkställ)**.

NOTERA: Routern kommer att starta om när du ändrar lägena.

3.3.2 System

System-sidan ger dig möjlighet att konfigurera dina trådlösa routerinställningar.

Ställ in systeminställningarna:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Administration > System**.
2. Du kan konfigurera dessa inställningar:
 - **Change router login password (Ändra lösenord för routerinloggning):** Du kan ändra lösenordet och inloggningsnamnet för den trådlösa routern genom att ange ett nytt namn och ett lösenord.
 - **Time Zone (Tidszon):** Välj tidszon för ditt nätverk.
 - **NTP Server:** Den trådlösa routern kan komma åt en NTP-server (Network time Protocol) för att synkronisera tiden.
 - **Enable Telnet (Aktivera Telnet):** Klicka på **Yes (Ja)** för att aktivera Telnet-tjänster i nätverket. Klicka på **No (Nej)** för att inaktivera Telnet.
 - **Authentication Method (Verifieringsmetod):** Du kan välja HTTP, HTTPS, eller båda protokollen för att säkra routeråtkomst.
 - **Enable Web Access from WAN (Aktivera webbåtkomst från WAN):** Välj **Yes (Ja)** för att tillåta enheter utanför nätverket åtkomst till den trådlösa routerns gränssnittsinställningar. Välj **No (Nej)** för att hindra åtkomst.
 - **Only allow specific IP (Tillåt enbart specifik IP):** Klicka på **Yes (Ja)** om du vill specificera IP-adresser för enheter som tillåts få åtkomst till den trådlösa routerns gränssnittsinställningar från WAN.
 - **Client List (Klientlista):** Ange WAN IP-adresserna för nätverksenheter som tillåts få åtkomst till den trådlösa routerns gränssnittsinställningar. Listan används om du klickat på **Yes (Ja)** under punkten **Only allow specific IP (Tillåt enbart specifik IP)**.
3. Klicka på **Apply (Verkställ)**.

3.3.3 Uppgradering av fast programvara

NOTERA: Ladda ned den senaste fasta programvaran från ASUS webbsida på <http://www.asus.com>

Uppgradering av det fasta programmet:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Administration > Firmware Upgrade (Uppgradering av fast programvara)**.
2. I fältet **New Firmware File (Ny fast programvarufil)**, klicka på **Browse (Bläddra)** för att lokalisera den hämtade filen.
3. Klicka på **Upload (Överför)**.

NOTER:

- När uppgraderingsproceduren är klar, vänta en stund tills systemet har startat om.
 - Om uppgraderingsprocessen misslyckas går routern automatiskt in i räddningsläge och strömlysdioden på frontpanelen börjar blinka långsamt. För att återställa systemet, se avsnitt **4.2 Återställning av fast programvara**.
-

3.3.4 Återställ/Spara/Överför inställning

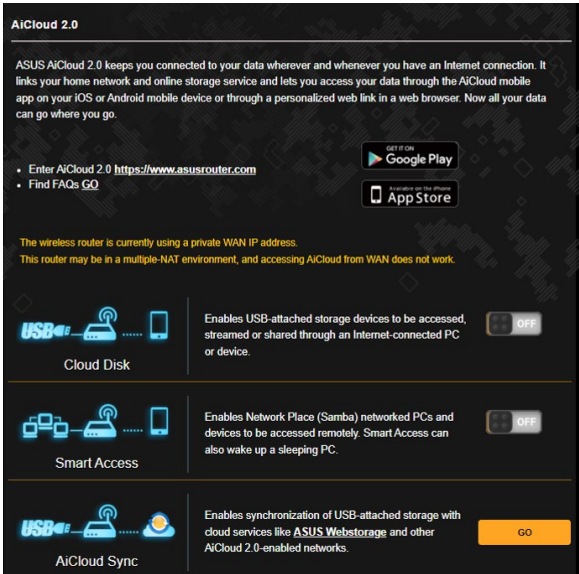
Återställ/Spara/Överför routerinställningarna:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Administration > Restore/Save/Upload Setting (Återställ/Spara/Överför inställning)**.
2. Välj den uppgift som du vill genomföra:
 - För att återställa standardinställningarna, klicka på **Restore (Återställ)**, och klicka på **OK** i bekräftelsemeddelandet.
 - För att spara nuvarande systeminställningar, klicka på **Save (Spara)**, navigera till mappen där du vill spara filen och klicka på **Save (Spara)**.
 - För att återställa från en sparad systeminställningsfil, klicka på **Browse (Bläddra)** för att lokalisera filen, och klicka på **Upload (Överför)**.

VIKTIGT! Om det uppstår problem, överför den senaste versionen av den fasta programvaran, och konfigurera nya inställningar. Återställ inte routern till standardinställningarna.

3.4 AiCloud 2.0

AiCloud 2.0 är ett molntjänstprogram som ger dig möjlighet att spara, synkronisera, dela och ge åtkomst till dina filer.



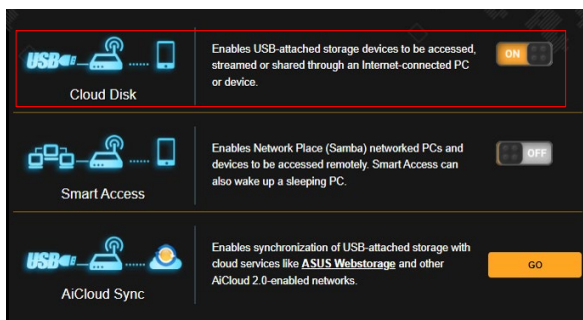
Använda AiCloud:

1. Hämta ASUS AiCloud-appen från Google Play Store eller Apple Store, och installera den på din smarta enhet.
2. Anslut din smarta enhet till ditt nätverk. Följ anvisningarna för att avsluta installationen av AiCloud.

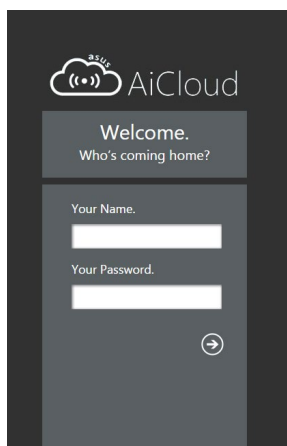
3.4.1 Molndisk

Skapa en molndisk:

1. Sätt i en USB-lagringsenhet i den trådlösa routern.
2. Slå på **Cloud Disk (Molndisk)**.

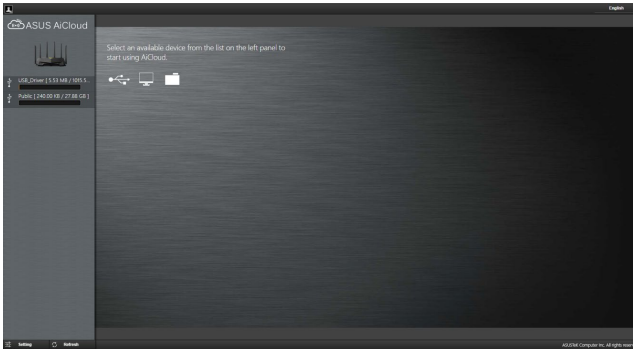


3. Gå till <http://www.asusrouter.com> och ange routerns inloggningskonto och lösenord. För bättre användarerfarenhet rekommenderar vi att du använder **Google Chrome** eller **Firefox**.



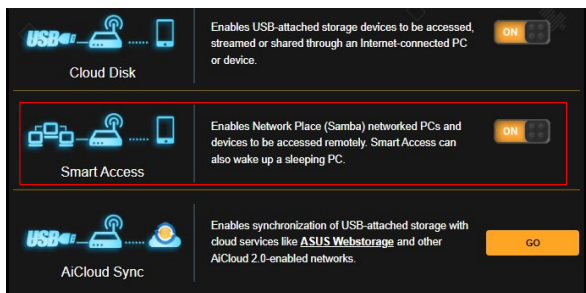
4. Nu kan du börja använda Cloud Disk-filer på enheter som är anslutna till nätverket.

NOTERA: När du använder enheter som är anslutna till nätverket, måste du ange enheternas användarnamn och lösenord manuellt, vilka kommer att sparas av AiCloud av säkerhetsskäl.



3.4.2 Smart Access

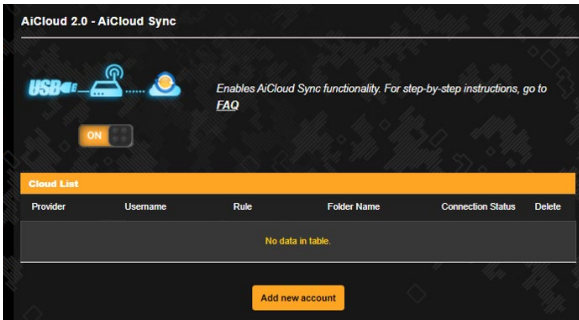
Smart Access-funktionen ger dig möjlighet att enkelt få åtkomst till ditt hemnätverk via routerns domännamn.



NOTER:

- Du kan skapa ett domännamn för routern med ASUS DDNS. För ytterligare detaljer se sektionen **3.19.6 DDNS**.
 - Som standard tillhandahåller AiCloud en säker HTTPS-anslutning. Knappa in [https://\[yourASUSDDNSname\].asuscomm.com](https://[yourASUSDDNSname].asuscomm.com) för en mycket säker Cloud Disk- och Smart Access-användning.
-

3.4.3 AiCloud synkronisering



Använda AiCloud Sync (AiCloud synkronisering):

1. Starta AiCloud, klicka på **AiCloud Sync (AiCloud synkronisering) > Go (Starta)**.
2. Välj **ON (PÅ)** för att aktivera AiCloud Sync.
3. Klicka på **Add new account (Lägg till nytt konto)**.
4. Ange ditt lösenord för ASUS WebStorage-kontot och välj ett arkiv som du vill synkronisera med WebStorage.
5. Klicka på **Apply (Verkställ)**.

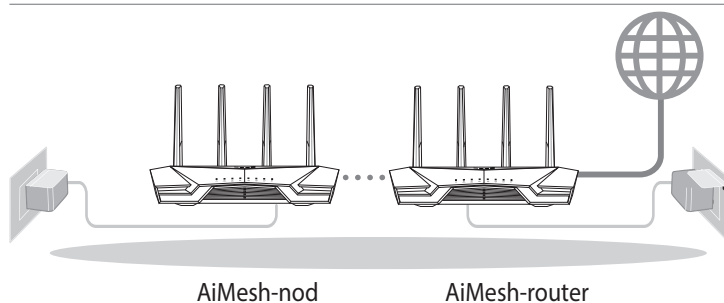
3.5 AiMesh

3.5.1 Före inställning

Förberedelse för inställning av ett AiMesh Wi-Fi-system

1. Två (2) ASUS-routrar (modeller som stödjer AiMesh <https://www.asus.com/AiMesh/>).
2. Tilldela en som AiMesh-router, och en som AiMesh-nod.

NOTERA: Om du har flera AiMesh-routrar rekommenderar vi att du använder den router med de högsta specifikationerna som Aimeshrouter, och de andra som AiMesh-noder.



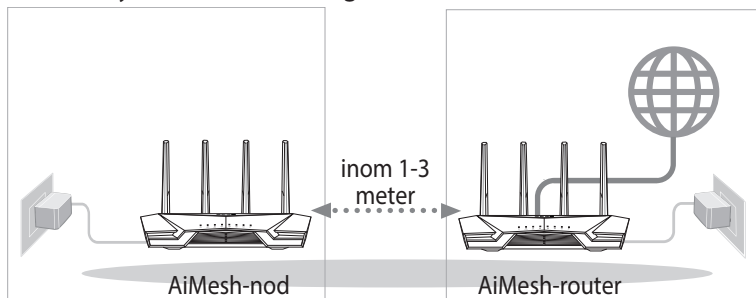
3.5.2 Inställningssteg för AiMesh

Förbered

Placera AiMesh-routern och noden inom 1-3 meter från varandra under inställningsprocessen.

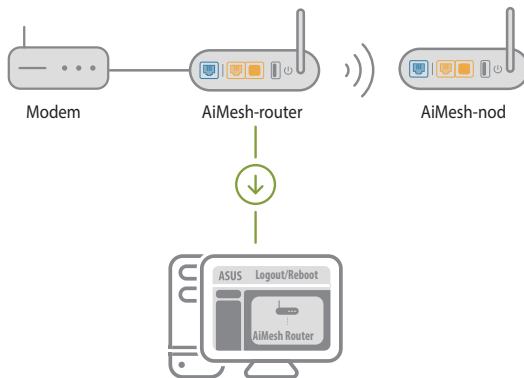
AiMesh-nod

Fabriksinställningsstatus. Låt strömmen vara på och i standby-läge för AiMesh-systemets inställningar.



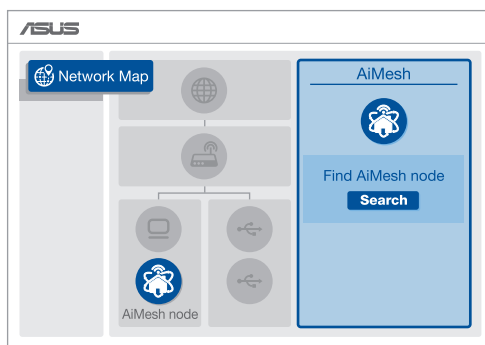
AiMesh-router

- 1) Se den andra routerns **Quick Start Guide (Snabbstartguide)** för att ansluta din AiMesh-router till datorn och modemmet, och logga in på webbanvändargränssnittet.



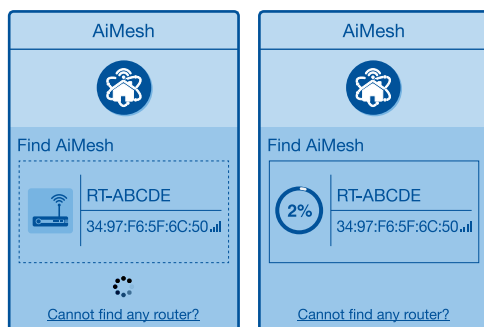
- 2) Gå till sidan Network Map (Nätverkskarta), klicka på AiMesh-ikonen och därefter Search (Sök) för att förlänga AiMesh-noden.

NOTERA: Kan du inte hitta AiMesh-ikonen här, klicka på versionen för den inbyggda programvaran och uppdatera den inbyggda programvaran.

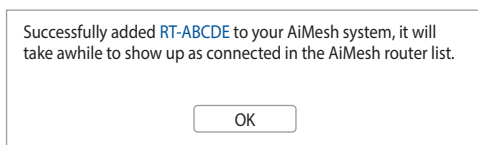


- 3) Klicka på **Search (Sök)**, så kommer den automatiskt att söka upp AiMesh-noden. När AiMesh-noden visas på sidan, klicka på den för att lägga till den i AiMesh-systemet.

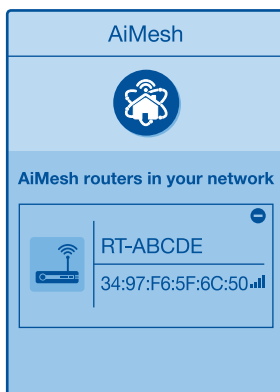
NOTERA: Kan du inte hitta någon AiMesh-nod, gå till **TROUBLE SHOOTING (FELSÖKNING)**.



- 4) Ett meddelande visas när synkroniseringen är klar.



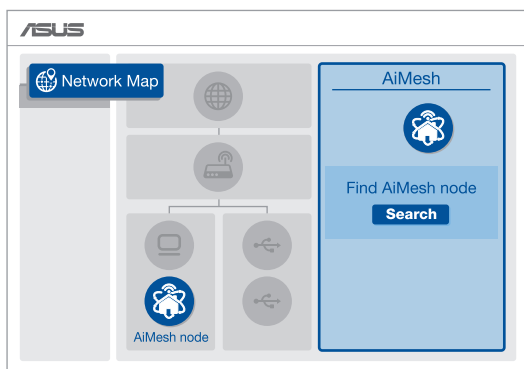
- 5) Grattis! Följande sidor kommer att visas när en AiMesh-nod har lagts till AiMesh-nätverket.



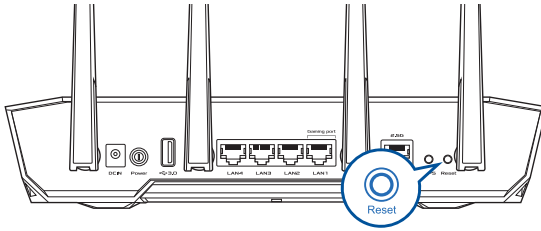
3.5.3 Felsökning

Om AiMesh-routern inte kan hitta någon AiMesh-nod i närheten eller synkroniseringen misslyckas, kontrollera följande och försök igen.

- 1) Flytta helst AiMesh-noden närmare AiMesh-routern. Se till att den är inom 1-3 meter.
- 2) AiMesh-noden startas.
- 3) AiMesh-noden uppgraderas till AiMesh-stödd inbyggd programvara.
 - i. Hämta AiMesh-stödd inbyggd programvara på: <https://www.asus.com/AiMesh/>
 - ii. Starta AiMesh-noden och anslut den till datorn via en nätverkskabel.
 - iii. Starta ett webbanvändargränssnitt. Du kommer att bli omdirigerad till ASUS installationsguide. Om inte, navigera till <http://www.asusrouter.com>
 - iv. Gå till **Administration (Administration) > Firmware Upgrade (Uppgradering av inbyggd programvara)**. Klicka på **Choose File (Välj fil)**, och överför den AiMesh-stödda inbyggda programvaran).
 - v. När den inbyggda programvaran överförs, gå till sidan Network Map (Nätverkskarta) för att kontrollera om AiMesh-ikonen visas.



- vi. Tryck på AiMesh-nodens återställningsknapp i minst 5 sekunder. Släpp knappen när strömindikatorn blinkar långsamt.



3.5.4 Omplacering

Bästa prestandan:

Placera AiMesh-routern och noden på bästa plats.

NOTERA:

- För att minimera störningarna, ska routern inte placeras i närheten av trådlösa telefoner, Bluetooth-enheter och mikrovågsugnar.
 - Vi rekommenderar att du placerar routern på en öppen eller rymlig plats.
-



3.5.5 FAQs (Vanliga Frågor)

F1: Stöds AccessPoint-läget av AiMesh-routern?

S: Ja. Du kan välja att ställa in AiMesh-routern på routerläge eller åtkomstpunktläge. Gå till webbanvändargränssnittet (<http://www.asusrouter.com>), och gå till sidan **Administration (Administration) > Operation Mode (Driftläge)**.

F2: Kan jag installera kabelanslutning mellan AiMesh-routrar (Ethernet-stamnät)?

S: Ja. AiMesh-system stödjer både trådlös och kabelanslutning mellan AiMesh-router och nod för att maximera genomströmning och stabilitet. AiMesh analyserar den trådlösa signalstyrkan för varje tillgängligt frekvensband, och bestämmer sedan automatiskt om en trådlös eller kabelanslutning passar bäst som ryggrad i anslutning mellan routrar.

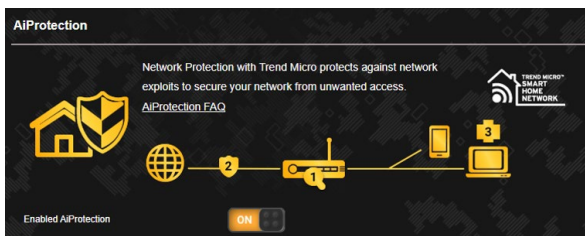
- 1) Följ installationsstegen för att etablera en anslutning mellan AiMesh-routern och noden via Wi-Fi:n först.
- 2) Placera noden på den plats där den har bäst täckning. Dra en Ethernet-kabeln från LAN-porten på AiMesh-routern till WAN-porten på AiMesh-noden.



- 3) AiMesh-systemet kommer att välja bästa väg för dataöverföringen automatiskt, vare sig det är kabelanslutning eller trådlös.

3.6 Aiprotection

Aiprotection erbjuder övervakning i realtid som identifierar skadlig kod, spionprogram och oönskad åtkomst. Det filtrerar även oönskade webbplatser och appar, och ger dig möjlighet att schemalägga en tid då en ansluten enhet kan ha åtkomst till Internet.



3.6.1 Konfigurering av Aiprotection

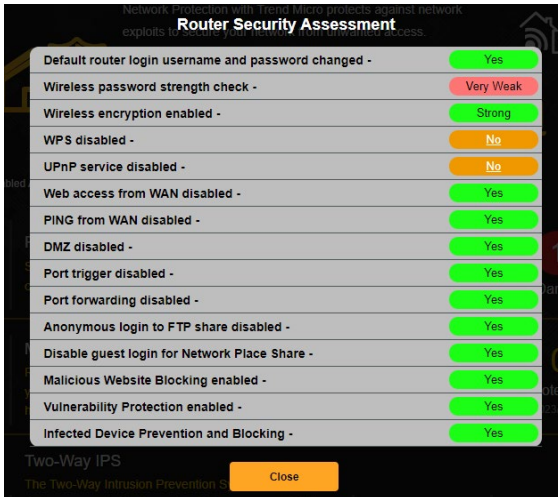
Aiprotection hindrar nätverksexploateringar och säkrar ditt nätverk från oönskad åtkomst.



Konfigurera Aiprotection:

1. Från navigeringsfältet, gå till **General (Allmänt) > Aiprotection**.
2. Från huvudsidan för Aiprotection, klicka på **Network Protection (Nätverksskydd)**.
3. Från fliken Network Protection (Nätverksskydd), klicka på **Scan (Skanna)**.

Sökresultaten visas på sidan **Router Security Assessment (Säkerhetsbedömning för router)**.



VIKTIGT! Objekt markerade med **Yes (Ja)** på sidan **Router Security Assessment (Säkerhetsbedömning för router)** betraktas som säkra.

4. (Valfritt) Från sidan **Router Security Assessment (Säkerhetsbedömning för router)**, konfigurera manuellt objekten som markerats som **No (Nej)**, **Weak (Svag)** eller **Very Weak (Mycket svag)**. Gör följande:
 - a. Klicka på ett objekt för att gå till inställningssidan för objektet.
 - b. Från säkerhetsinställningssidan för objektet, konfigurera och gör de nödvändiga ändringarna och klicka på **Apply (Verkställ)** när det är klart.
 - c. Gå tillbaka till sidan **Router Security Assessment (Säkerhetsbedömning för router)** och klicka på **Close (Stäng)** för att stänga sidan.
5. Klick på **OK** på bekräftelsemeddelandet.

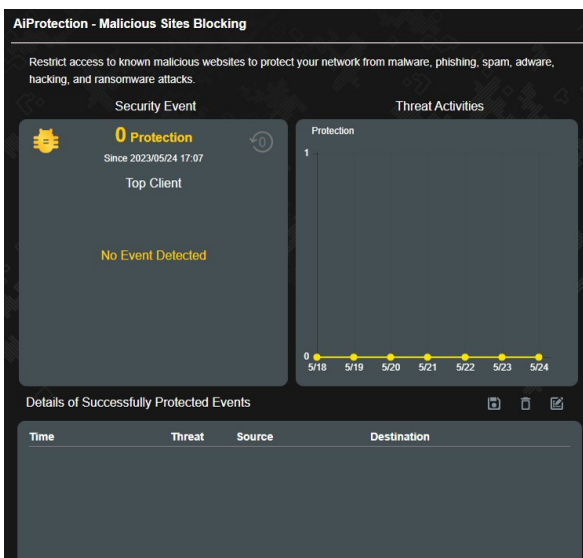
3.6.2 Blockering av skadliga webbplatser

Denna funktion begränsar åtkomst till webbplatser som är skadliga i molndatabasen för ett skydd som alltid är uppdaterat mot hot.

NOTERA: Denna funktion aktiveras automatiskt om du kör Router Weakness Scan (Skanna efter svagheter i router).

Aktivera Blockering av skadliga webbplatser:

1. Från navigeringsfältet, gå till **General (Allmänt) > Aiprotection**.
2. Från huvudsidan för Aiprotection, klicka på **Malicious Sites Blocking (Blockering av skadliga webbplatser)**.



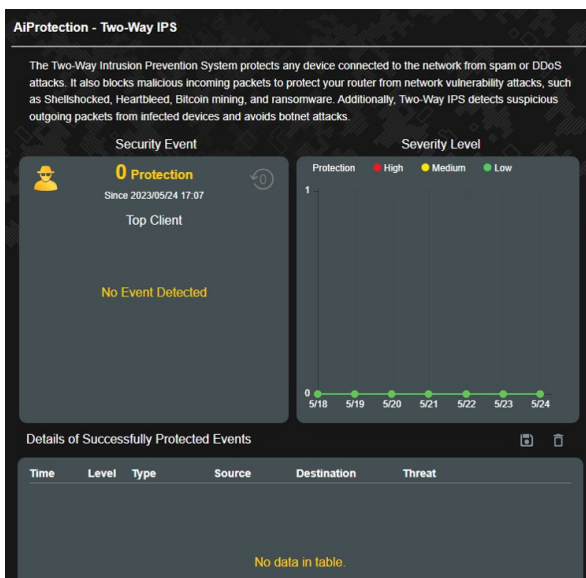
3.6.3 Tvåvägs-IPS

Denna funktion löser vanliga exploateringar inom routerns konfiguration.

NOTERA: Denna funktion aktiveras automatiskt om du kör Router Weakness Scan (Skanna efter svagheter i router).

Aktivera tvåvägs-IPS:

1. Från navigeringsfältet, gå till **General (Allmänt) > Aiprotection**.
2. Från huvudsidan för Aiprotection, klicka på **Two-Way IPS (Tvåvägs-IPS)**.



3.6.4 Skydd och blockering av infekterad enhet

Denna funktion hindrar infekterade enheter från att kommunicera personlig information och/eller infekterad status till externa parter.

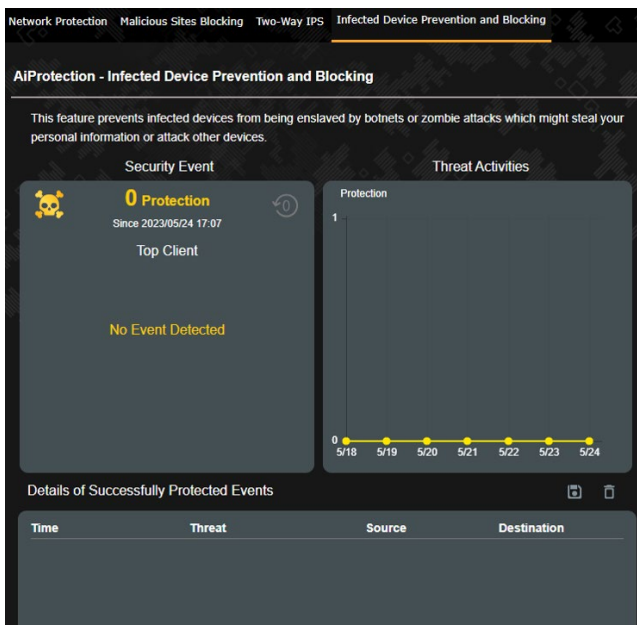
NOTERA: Denna funktion aktiveras automatiskt om du kör Router Weakness Scan (Skanna efter svagheter i router).

Aktivera förebyggande och blockering av infekterad enhet:

1. Från navigeringsfältet, gå till **General (Allmänt) > Aiprotection**.
2. Från huvudsidan för Aiprotection, klicka på **Infected Device Prevention and Blocking (Skydd och blockering av infekterad enhet)**.

Konfigurera Alert Preference (Preferenser för larm):

1. Från fältet Infected Device Prevention and Blocking (Skydd och blockering av infekterad enhet), klicka på **Alert Preference (Preferenser för larm)**.
2. Välj eller ange e-postleverantören, e-postkonto och lösenord, och klicka på **Apply (Verkställ)**.



3.7 Brandvägg

Den trådlösa routern kan fungera som maskinvarubrandvägg för nätverket.

NOTERA: Brandväggsfunktionerna är aktiverade som standard.

3.7.1 Allmänt

Ställa in grundläggande brandväggsinställningar:


1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Firewall (Brandvägg) > General (Allmänt)**.
2. I fältet **Enable Firewall (Aktivera brandvägg)**, välj **Yes (Ja)**.
3. På **Enable DoS protection (Aktivera DoS-skydd)**, välj **Yes (Ja)** för att skydda nätverket från DoS-attacker (Denial of Service) även om det kan påverka din routers prestanda.
4. Du kan även övervaka paket som utväxlas mellan LAN- och WAN-anslutningen. Välj **Dropped (Avbruten)**, **Accepted (Accepterad)** eller **Both (Båda)** på typen Logged packets (Loggade paket).
5. Klicka på **Apply (Verkställ)**.

3.7.2 URL-filer

Du kan specificera nyckelord eller webbadresser för att hindra åtkomst till specifika URL:ar.

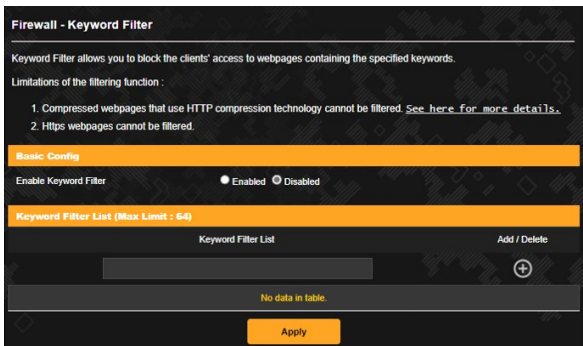
NOTERA: URL-filtret baseras på en DNS-begäran. Om en nätverksklient redan har åtkomst till en webbplats som <http://www.abcxxx.com>, kommer webbplatsen inte att blockeras (en DNS-cache i systemet lagrar tidigare besökta webbplatser). För att lösa problemet, rensa DNS-cacheminnet innan du installerar URL-filtret.

Installera ett URL-filer:


1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Firewall (Brandvägg) > URL Filter**.
2. Välj **Enabled (Aktiverad)** i fältet **Enable URL Filter (Aktivera URL-filer)**.
3. Ange URL:en och klicka på -knappen.
4. Klicka på **Apply (Verkställ)**.

3.7.3 Nyckelordsfilter

Nyckelordsfiltret blockerar åtkomst till webbsidor med specifika nyckelord.



Inställning av ett nyckelordsfilter:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Firewall (Brandvägg) > Keyword Filter (Nyckelordsfilter)**.
2. Välj **Enabled (Aktiverad)** i fältet **Enable Keyword Filter (Aktivera nyckelordsfilter)**.
3. Ange ett ord eller en fras och klicka på knappen .
4. Klicka på **Apply (Verkställ)**.

NOTER:

- Nyckelordsfiltret baseras på en DNS-begäran. Om en nätverksklient redan har åtkomst till en webbplats som `http://www.abcxxx.com`, kommer webbplatsen inte att blockeras (en DNS-cache i systemet lagrar tidigare besökta webbplatser). För att lösa problemet, rensa DNS-cacheminnet innan du ställer in nyckelordsfiltret.
 - Webbsidor som är komprimerade med HTTP-komprimering kan inte filtreras. HTTPS-sidor kan inte heller blockeras med nyckelordsfilter.
-

3.7.4 Nätverkstjänstfilter

Nätverkstjänstfiltret blockerar utbyten av LAN-till-WAN-paket, och begränsar nätverksklienter från att komma åt specifika webbtjänster som Telnet eller FTP.

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.

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

Allow List Duration : During the scheduled duration, clients in the Allow List can ONLY use the specified network.

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

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
				TCP	+

No data in table.

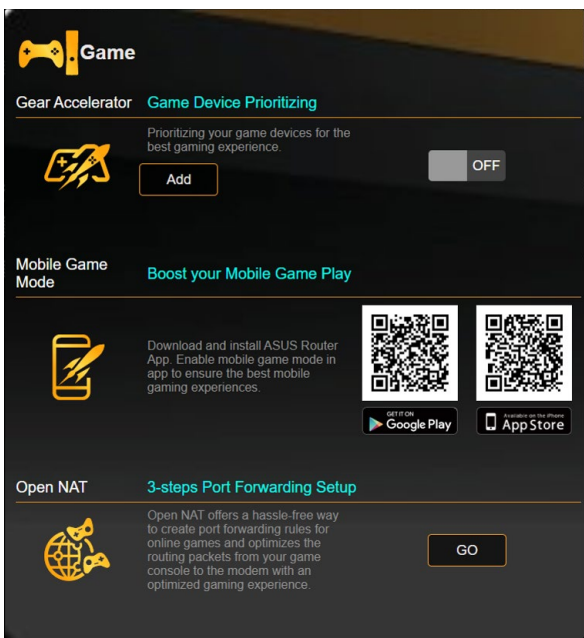
Apply

Ställa in ett nätverksfilter:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Firewall (Brandvägg) > Network Service Filter (Nätverkstjänstfilter)**.
2. Välj **Yes (Ja)** i fältet **Enable Network Service Filter (Aktivera nätverkstjänstfilter)**.
3. Välj typ av filtertabell. **Black List (Svart lista)** blockera specificerade nätverkstjänster. **White List (Vit lista)** begränsar åtkomst enbart till specificerade nätverkstjänster.
4. Specificera dag och tid när filtren ska vara aktiva.
5. Ange Source IP (Käll-IP), Destination IP (Mål-IP), Port Range (Portintervall) och Protocol (Protokoll), för att specificera en nätverkstjänst som ska filtreras. Klicka på knappen **+**.
6. Klicka på **Apply (Verkställ)**.

3.8 Spel

Denna funktion ger dig möjlighet att aktivera Speloptimering med ett klick. När Speloptimering är aktiverad, ger ROG Rapture spelrouter spelpaketet högsta prioritet för att ge dig den bästa spelupplevelsen.

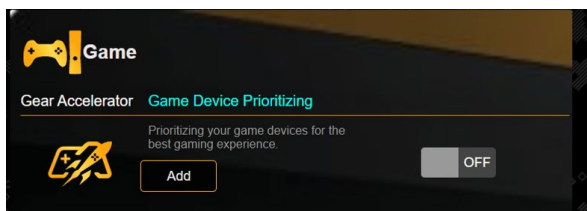


Konfigurera Speloptimering:


Från navigeringsfältet, gå till **General (Allmänt) > Game (Spel)**.

3.8.1 Växelgas

Med Växelgas kan du prioritera spelenheter trådlöst via kontrollpanel online för bästa spelupplevelse.



För att konfigurera Växelgas:

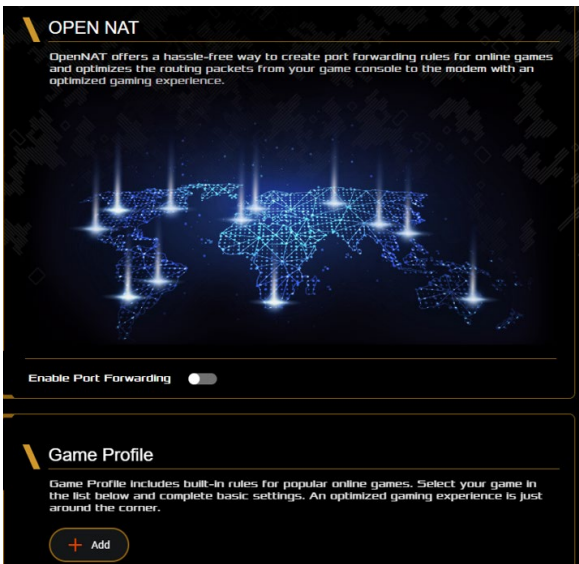
1. Från navigeringsfältet, gå till **General (Allmänt) > Game (Spel)**.
2. Från fältet **Gear Accelerator (Växelgas)**, klicka på **ON (PÅ)**.
3. När inställningen har verkställts, klicka på **Add (Lägg till)** för att välja klientnamn.
4. Klicka på  för att lägga till klientens profil.
5. Klicka på **Apply (Verkställ)** för att spara inställningarna.

NOTERA: Om du vill ta bort klientens profil, klicka på .

3.8.2 Öppen NAT

Open NAT erbjuder ett problemfritt sätt att skapa regler för portvidarebefordran för onlinespel och optimerar routningpkaketen från spelkonsolen till modemmet för en optimerad spelupplevelse.

När du spelar dator- eller konsolspel, kan det finnas en del anslutningsproblem på grund av ISP:en eller routerinställningarna i din miljö, t. ex. NAT och portblockeringar. Öppen NAT hjälper till att säkerställa att Trådlös TUF spelrouter inte blockerar spelanslutningen.



Konfigurera Öppen NAT:

1. Från navigeringspanelen, gå till **General (Allmänt) > Open NAT (Öppen NAT)**.
2. Slå på **Enable Port Forwarding (Aktivera portvidarebefordran)**.
3. Från **Game Profile**, klicka på **Add (Lägg till)** för att välja ett spel och slutför grundinställningarna.
4. Kliccka på **OK**.

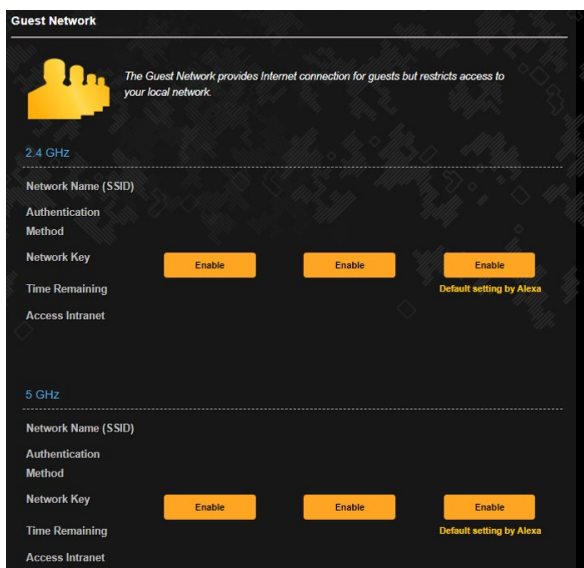
3.9 Gästnätverk

Gästnätverket erbjuder tillfälliga besökare Internetanslutning via åtkomst till separata SSID eller nätverk utan att tillhandahålla åtkomst till ditt privata nätverk.

NOTERA: TUF-AX3000 V2 stöder upp till sex SSID (tre 2,4 GHz och tre 5 GHz).

Skapa ett gästnätverk:

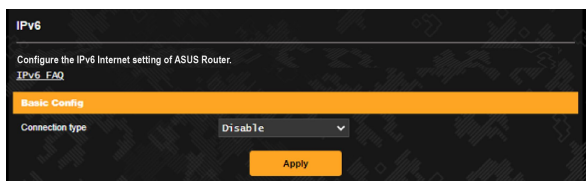
1. Från navigeringsfältet, gå till **General (Allmänt) > Guest network (Gästnätverk)**.
2. På skärmen Guest Network (Gästnätverk), välj frekvensbandet 2,4GHz eller 5GHz för gästnätverket som du vill skapa.
3. Klicka på **Enable (Aktivera)**.



4. För att ändra inställningarna för en gäst, klicka på gästinställningarna du vill ändra. Klicka på **Remove (Ta bort)** för att radera inställningarna för gästen.
5. Tilldela ett namn för det tillfälliga trådlösa nätverket i fältet Network Name (SSID) [Nätverksnamn (SSID)].
6. Välj en verifieringsmetod.
7. Om du väljer en WPA-verifieringsmetod, välj en WPA-kryptering.
8. Specificera Access time (Åtkomsttid) eller välj **Limitless (Obegränsad)**.
9. Välj **Disable (Inaktivera)** eller **Enable (Aktivera)** på Access Intranet (Åtkomst till Intranet).
10. När du är klar, klicka på **Apply (Verkställ)**.

3.10 IPv6

Denna trådlösa router stödjer IPv6-adressering, ett system som stödjer fler IP-adresser. Denna standard finns inte överallt ännu. Kontakta din ISP om din Internet-tjänst stödjer IPv6.



Installera IPv6:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > IPv6**.
2. Välj din **Connection type (Anslutningstyp)**. Konfigureringsalternativen varierar efter vilken anslutningstyp du valt.
3. Ange dina inställningar för IPv6 LAN och DNS.
4. Klicka på **Apply (Verkställ)**.

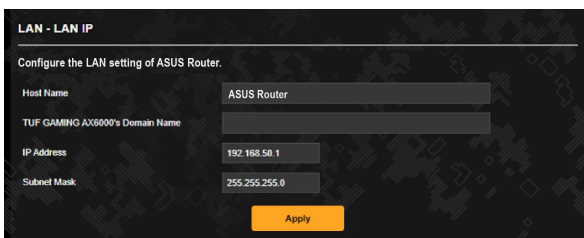
NOTERA: Kontakta din ISP beträffande specifik IPv6-information för din Internet-tjänst.

3.11 LAN

3.11.1 LAN IP

LAN IP-skärmen ger dig möjlighet att modifiera LAN IP-inställningarna för den trådlösa routern.

NOTERA: Alla ändringar av LAN IP-adressen påverkar dina DHCP-inställningar.



LAN - LAN IP

Configure the LAN setting of ASUS Router.

Host Name	ASUS Router
TUF GAMING AX6000's Domain Name	
IP Address	192.168.50.1
Subnet Mask	255.255.255.0

Apply

Ändra LAN IP-inställningarna:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > LAN > LAN IP**.
2. Modifiera **IP address (IP-adress)** och **Subnet Mask (Nätmask)**.
3. När du är klar, klicka på **Apply (Verkställ)**.

3.11.2 DHCP-server

Den trådlösa routern använder DHCP för att automatiskt tilldela IP-adresser på nätverket. Du kan specificera IP-adressintervallet och lånetiden för klienterna på nätverket.

The screenshot shows the 'LAN - DHCP Server' configuration page. It includes a description of DHCP, a link to a FAQ, and several configuration sections: 'Basic Config' with options to enable the server and set domain name, IP pool, lease time, and gateway; 'DNS and WINS Server Setting' with fields for DNS and WINS servers and an option to advertise the router's IP; 'Manual Assignment' with an option to enable manual IP assignment; and a table for 'Manually Assigned IP around the DHCP list' with columns for Client Name, IP Address, DNS Server, and Host Name. An 'Apply' button is at the bottom.

Konfigurera DHCP-servern:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > LAN > DHCP Server**.
2. I fältet **Enable the DHCP Server (Aktivera DHCP-servern)** markera **Yes (Ja)**.
3. Ange ett domännamn för den trådlösa routern i textrutan **Domain Name (Domännamn) för ASUS Router**.
4. I fältet **IP Pool Starting Address (IP pool startadress)** knappa in start-IP-adressen.

5. I fältet **IP Pool Ending Address (IP pool slutadress)** knappa in slut-IP-adressen.
6. Specificera sekunderna när en tilldelad IP-adress går ut i fältet **Lease Time (seconds) (Lånetid (sekunder))**. När tidsgränsen nås, kommer DHCP-servern att tilldela en ny IP-adress.

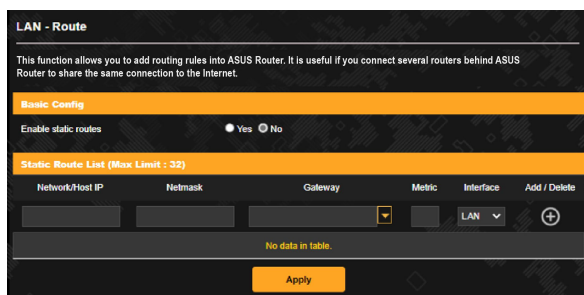
NOTER:

- Vi rekommenderar att du använder IP-adressformatet 192.168.1.xxx (där xxx kan vara vilket nummer som helt mellan 2 och 254) när ett IP-adressintervall specificeras.
 - IP Pool Starting Address (IP Pool-startadress) bör inte vara större än IP Pool Ending Address (IP Pool-slutadress).
-
7. Knappa in din DNS-servers och WINS-servers IP-adress i avsnittet **DNS and WINS Server Settings (DNS och WINS serverinställningar)** vid behov.
 8. Den trådlösa router kan även tilldela IP-adresser manuellt till enheter i nätverket. I fältet **Enable Manual Assignment (Aktivera manuell tilldelning)**, välj **Yes (Ja)** för att tilldela en IP-adress till specifika MAC-adresser på nätverket. Upp till 32 MAC-adresser kan läggas till DHCP-listan för manuell tilldelning.



3.11.3 Route

Om ditt nätverk använder mer än en trådlös router, kan du konfigurera en routningstabell för att dela samma Internettjänst.

NOTERA: Vi rekommenderar att du inte ändrar standardflödesinställningarna, om du inte har djupgående kunskaper om routningstabeller.



Konfigurera LAN-routningstabell:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > LAN > Route**.
2. I fältet **Enable static routes (Aktivera statiska vägar)**, välj **Yes (Ja)**.
3. På listan **Static Route List (Lista över statiska vägar)**, ange nätverksinformationen för åtkomstpunkter och noder. Klicka på knappen **Add (Lägg till)**  eller **Delete (Ta bort)** , för att lägga till eller ta bort en enhet i listan.
4. Klicka på **Apply (Verkställ)**.

3.11.4 IPTV

Den trådlösa routern stödjer anslutning till IPTV-tjänster genom en ISP eller en LAN. IPTV-fliken erbjuder konfigurationsinställningarna som krävs för att ställa in IPTV, VoIP, multicasting och UDP för din tjänst. Kontakta din ISP för specifik information för din tjänst.

The screenshot shows the 'LAN - IPTV' configuration page. At the top, there is a warning: '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, there are two main sections: 'LAN Port' and 'Special Applications'. The 'LAN Port' section contains two dropdown menus: 'Select ISP Profile' set to 'None' and 'Choose IPTV STB Port' set to 'None'. The 'Special Applications' section contains four settings: 'Use DHCP routes' set to 'Microsoft', 'Enable multicast routing' set to 'Disable', 'Enable efficient multicast forwarding (IGMP Snooping)' set to 'Disable', and 'UDP Proxy (Udpxy)' set to '0'. An 'Apply' button is located at the bottom right of the form.

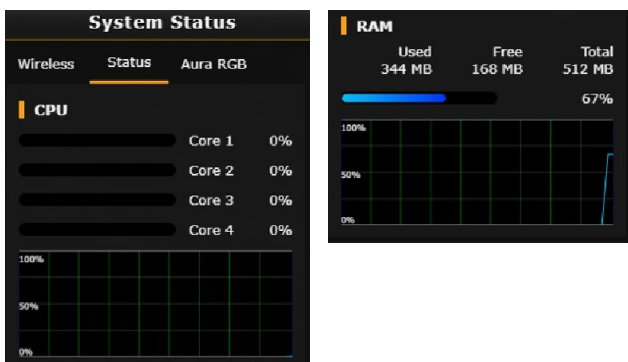
LAN - IPTV	
To watch IPTV, the WAN port must be connected to the Internet. Please go to WAN - Dual WAN to confirm that WAN port is assigned to primary WAN.	
LAN Port	
Select ISP Profile	None
Choose IPTV STB Port	None
Special Applications	
Use DHCP routes	Microsoft
Enable multicast routing	Disable
Enable efficient multicast forwarding (IGMP Snooping)	Disable
UDP Proxy (Udpxy)	0
Apply	

3.12 Nätverkskartan

Nätverkskartan ger dig möjlighet att konfigurera nätverksinställningarna, hantera nätverksklienter och övervaka USB-enheten på ett säkert sätt.



Du kan övervaka CPU-enhetens status för varje kärna, RAM-användningsstatus och Ethernet-portarnas status. Följande är ett exempel på användningsstatusen för CPU, RAM och Ethernet-portarna.



3.12.1 Inställning av de trådlösa säkerhetsinställningarna

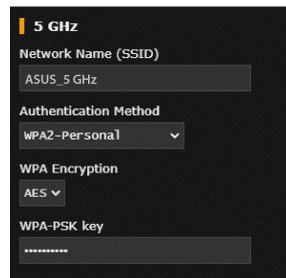
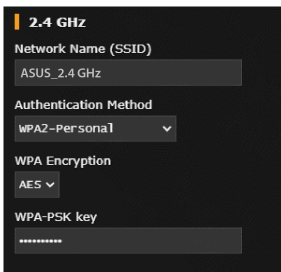
För att skydda ditt trådlösa nätverk från obehörig åtkomst behöver du konfigurera dess säkerhetsinställningar.

Ställa in de trådlösa säkerhetsinställningarna:

1. Från navigeringsfältet, gå till **General (Allmänt) > Network Map (Nätverkskarta)**.
2. På skärmen Network Map (Nätverkskarta) och under **System Status (Systemstatus)** kan du konfigurera de trådlösa säkerhetsinställningarna såsom SSID, säkerhetsnivå och krypteringsinställningar på ett säkert sätt.

NOTERA: Du kan ställa in olika trådlösa säkerhetsinställningar för banden 2,4 GHz och 5 GHz.

2,4 GHz säkerhetsinställningar 5GHz säkerhetsinställningar

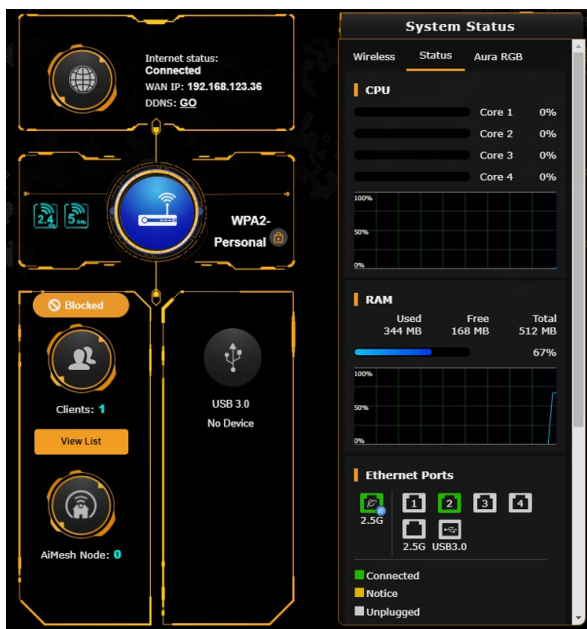


3. I fältet **Network Name (Nätverksnamn, SSID)** knappa in ett unikt namn för ditt trådlösa nätverk.
4. Välj verifieringsmetod för ditt trådlösa nätverk från rullgardinsmenyn **Authentication Method (Verifieringsmetod)**.
Om du väljer WPA-Personal eller WPA-2 Personal som verifieringsmetod, ange WPA-PSK-nyckeln eller säkerhetslösenordet.

VIKTIGT! IEEE 802.11n/ac-standard förbjuder användning av hög genomströmning med WEP eller WPA-TKIP som unikast-kryptering. Om du använder dessa krypteringsmetoder kommer din datahastighet att minska till IEEE 802.11g 54 Mbps anslutning.

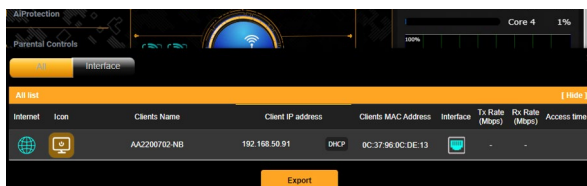
5. Klicka på **Apply (Verkställ)** när du är klar.

3.12.2 Hantera dina nätverksklienter



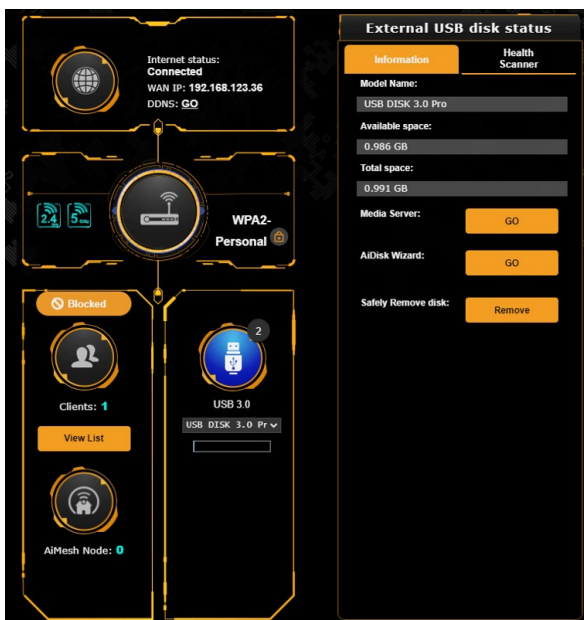
Hantera dina nätverksklienter:

1. Från navigeringsfältet, gå till **General (Allmänt) > Network Map (Nätverkskarta)**.
2. På skärmen **Network Map (Nätverkskarta)**, välj ikonen **Clients (Klienter)** för att visa informationen om dina nätverksklienter.
3. Klicka på **View List (Visa lista)** under **Clients (Klienter)** för att visa alla klienter.
4. För att blockera en klients åtkomst till ditt nätverk välj klienten och klicka på den öppna låsikonen.



3.12.3 Övervaka din USB-enhet

ASUS trådlösa router erbjuder två USB-portar för anslutning av USB-enheter eller USB-skrivare, för att kunna dela filer och skrivare med klienter i nätverket.



NOTER:

- För att använda denna funktion måste du infoga en USB-lagringsenhet såsom en USB-hårddisk eller USB-flashenhet till USB 3.0/2.0 porten på baksidan av din trådlösa router. Se till att USB-lagringsenheten är korrekt formaterad och partitionerad. Se Plug-n-Share Disk Support List (plugga-in-och-dela disk supportlistan) på <http://event.asus.com/networks/disksupport>
- USB-portarna stödjer två USB-enheter eller en skrivare och en USB-enhet samtidigt.

VIKTIGT! Du måste först skapa ett delningskonto och dess tillstånd/åtkomsträttigheter för att tillåta andra nätverksklienter att få åtkomst till USB-enheten via en FTP-plats/tredje parts FTP-klientverktyg, Servers Center, Samba eller AiCloud. För fler detaljer, se avsnitt **3.17 USB-applikationen** och **3.4 AiCloud 2.0** i denna bruksanvisning.

Övervakning av din USB-enhet:

1. Från navigeringsfältet, gå till **General (Allmänt) > Network Map (Nätverksskarta)**.
2. På skärmen Network Map (Nätverksskarta), välj ikonen **USB Disk Status (USB-enhet status)** för att visa informationen om dina USB-enhet.
3. I fältet AiDisk Wizard (AiDisk-guide) **GO (STARTA)** för att ställa in en FTP-server för Internetfildelning.


NOTER:

- För ytterligare detaljer se avsnitt **3.17.2 Using Servers center (Använda Servers Center)** i denna bruksanvisning.
- Den trådlösa routern arbetar mest med USB HDD-/flash-enheter (upp till 2TB i storlek) och stödjer läs-/skrivåtkomst för FAT16, FAT32, EXT2, EXT3 NTFS och HFS+.

Säker borttagning av USB-enhet

VIKTIGT! Felaktig borttagning av USB-enheten kan orsaka skadade data.

Säker borttagning av USB-enhet:

1. Från navigeringsfältet, gå till **General (Allmänt) > Network Map (Nätverksskarta)**.
2. I övre högra hörnet, klicka på  > **Eject USB disk (Mata ut USB-enhet)**. När USB-enheten matas ut, visar USB-statusen **Unmounted (Demonterad)**.

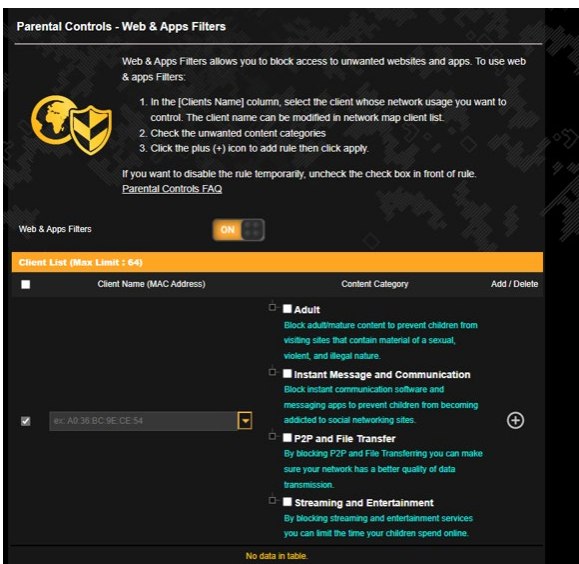


3.13 Klassificeringskontroll

Parental Controls (Klassificeringskontroll) gör dig möjlig att kontrollera Internetåtkomsttiden eller ställa in tidsgränsen för en klients nätverksanvändning.

Konfigurera Klassificeringskontroll:

Från navigeringsfältet, gå till **General (Allmänt) > Parental Controls (Klassificeringskontroll)**.



Parental Controls - Web & Apps Filters

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

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

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

Web & Apps Filters ON

Client List (Max Limit : 64)

Client Name (MAC-Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	<input type="checkbox"/> Adult Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature.	
	<input type="checkbox"/> Instant Message and Communication Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.	
	<input type="checkbox"/> P2P and File Transfer By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.	
	<input type="checkbox"/> Streaming and Entertainment By blocking streaming and entertainment services you can limit the time your children spend online.	

No data in table.

Filter för webb och appar

Web & Apps Filters (Filter för webb och appar) är en funktion i Parental Controls (Klassificeringskontroller) som ger dig möjlighet att blockera åtkomsten till önskade webbplatser eller applikationer.

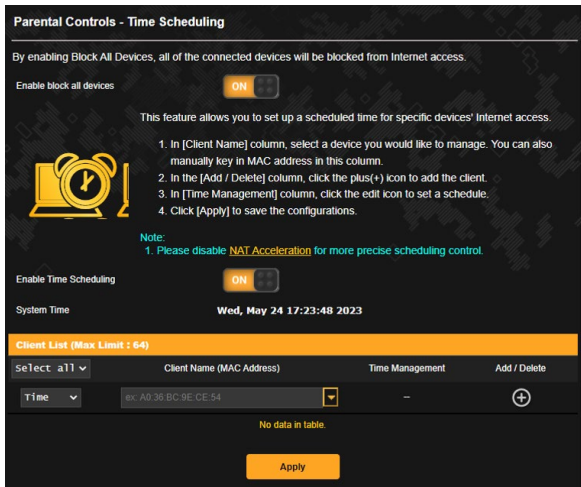
Konfigurera Filter för webb och appar:

1. Från navigeringsfältet, gå till **General (Allmänt) > Parental Controls (Klassificeringskontroll) > Web & Apps Filters (Filter för webb och appar)**.
2. Från fältet **Web & Apps Filters (Filter för webb och appar)**, klicka på **ON (PÅ)**.
3. När meddelandet om licensavtalet (EULA) öppnas, klicka på **I agree (Jag accepterar)** för att fortsätta.
4. Från kolumnen **Client List (Klientlista)** väljer eller anger du klientens namn från den nedrullningsbara listrutan.
5. Från kolumnen **Content Category (Innehållskategori)**, välj filter bland de fyra huvudkategorierna från kolumnen: **Adult (Vuxna)**, **Instant Message and Communication (Snabbmeddelande och kommunikation)**, **P2P and File Transfer (P2P och filöverföring)** och **Streaming and Entertainment (Strömning och underhållning)**.
6. Klicka på  för att lägga till klientens profil.
7. Klicka på **Apply (Verkställ)** för att spara inställningarna.

Schemaläggning av tid

Tidsschemaläggning låter dig ställa in tidsgränsen för en klients nätanvändning.

NOTERA: Kontrollera att tiden på ditt system är synkroniserad med NTP-servern.



Konfigurera Tidsschemaläggning:

1. Från navigeringsfältet, gå till **General (Allmänt) > Parental Controls (Klassificeringskontroller) > Time Scheduling (Schemaläggning av tid)**.
2. Från fältet **Enable Time Scheduling (Aktivera tidsschemaläggning)**, klicka på **ON (PÅ)**.
3. Från kolumnen **Client Name (Klientnamn)** väljer eller anger du klientens namn från den nedrullningsbara listrutan.

NOTERA: Du kan också ange klientens MAC-adress i kolumnen Klientens MAC-adress. Klientens namn får inte innehålla specialtecken eller mellanslag eftersom de kan orsaka att routern fungerar onormalt.

4. Klicka på **+** för att lägga till klientens profil.
5. Klicka på **Apply (Verkställ)** för att spara inställningarna.

3.14 Smart anslutning

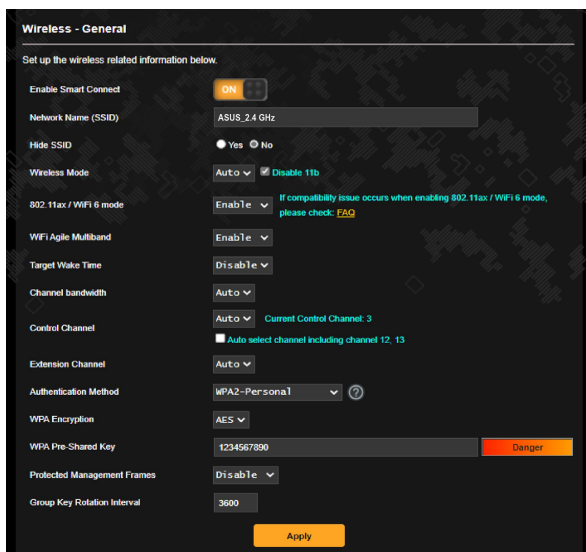
Smart anslutning är utformad för att automatiskt styra klienter till ett av tre radioband (2,4 GHz och 5 GHz) för att maximera den totala trådlösa genomströmningen.

3.14.1 Konfigurera Smart anslutning

Du kan aktivera Smart anslutning från Webb-GUI genom följande två sätt:

- **Via skärmen Wireless (Trådlöst)**

1. Manuellt skriva in den trådlösa routerns standard IP-adress i webbläsaren: <http://www.asusrouter.com>.
2. På inloggningsidan skriver du in standardanvändarnamnet (**admin**) och lösenordet (**admin**) och klickar på **OK**. QIS-sidan startar automatiskt.
3. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Wireless (Trådlöst) > General (Allmänt)**.
4. Flytta skjutreglaget till **ON (PÅ)** i fältet **Enable Smart Connect (Aktivera smart anslutning)**. Denna funktion ansluter automatiskt klienterna i ditt nätverk till rätt band för optimal hastighet.



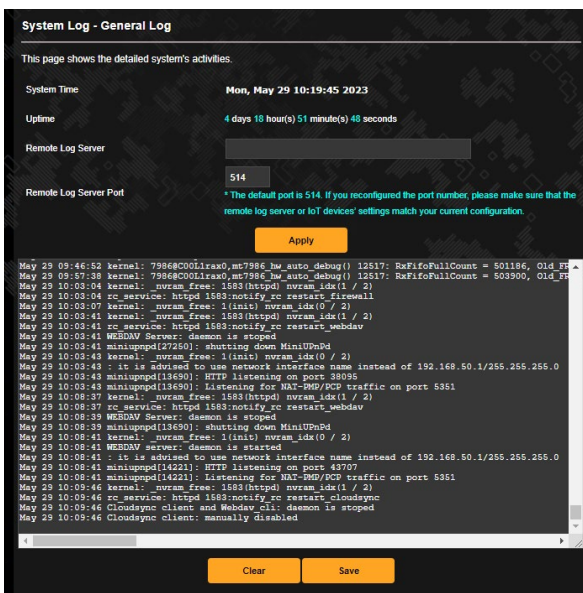
3.15 Systemlogg

System Log (Systemlogg) innehåller dina inspelade nätverksaktiviteter.

NOTERA: Systemloggen återställs när routern startas om eller stängs av.

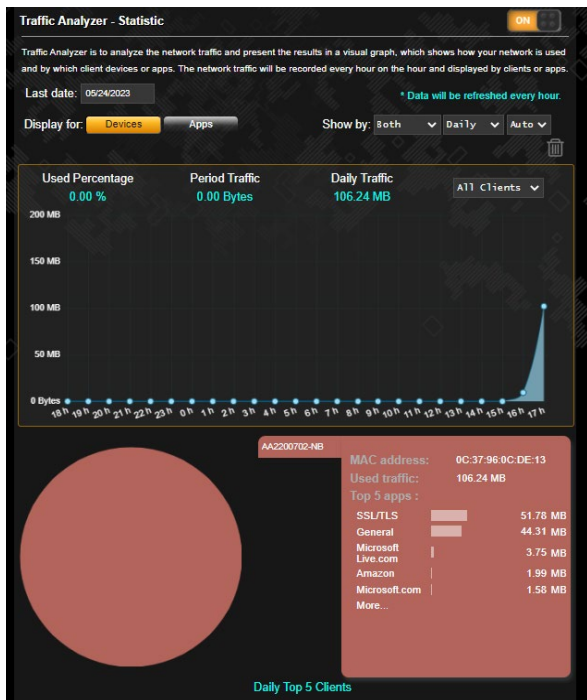
Visa din systemlogg:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > System Log (Systemlogg)**.
2. Du kan visa dina nätverksaktiviteter i någon av följande flikar:
 - General Log (Allmän logg)
 - Wireless Log (Trådlös logg)
 - DHCP Leases (DHCP-lån)
 - IPv6 (IPv6)
 - Routing Table (Routningstabell)
 - Port Forwarding (Portvidarebefordran)
 - Connections (Anslutningar)



3.16 Trafikanalys

Traffic Analyzer (Trafikanalys) ger dig en översikt över vad som händer på nätverket varje dag, vecka eller månad. Det ger dig möjlighet att snabbt se varje användares bandbreddsanvändning eller enheten eller appen som används, och hjälper dig att minska flaskhalsar i din Internet-anslutning. Det är också ett väldigt bra sätt att övervaka användarnas Internet-användning eller -aktiviteter.



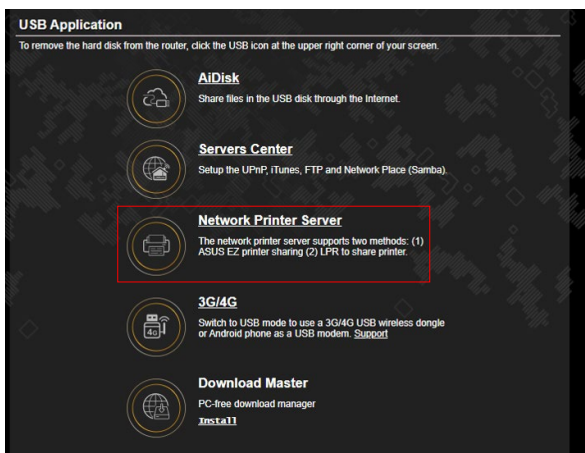
Konfigurera Traffic Analyzer (Trafikanalys):

1. Från navigeringsfältet, gå till **General (Allmänt) > Traffic Analyzer (Trafikanalys)**.
2. Från huvudsidan för **Traffic Analyzer (Trafikanalys)** sätter du på trafikanalysstatistik.
3. Välj datum för vilket du vill visa diagram.
4. På **Display for (Visa för)** fält väljer du Router eller Apps (Appar) för att visa trafikinformation.
5. På Show by field (Visa efter fält) väljer du hur du vill att trafikinformationen ska visas.

3.17 USB-applikation

USB-applikationsfunktioner tillhandahåller undermenyerna AiDisk, Servers Center, Network Printer Server och Download Master.

VIKTIGT! För att använda serverfunktionen måste du sätta i en USB-lagringsenhet, t.ex. en USB-hårddisk eller USB-flashminne, i USB 3.0-porten på baksidan av din trådlösa router. Se till att USB-lagringsenheten är korrekt formaterad och partitionerad. Se ASUS webbsida på <http://event.asus.com/2009/networks/disksupport/> för tabellen över filsystem som stöds.

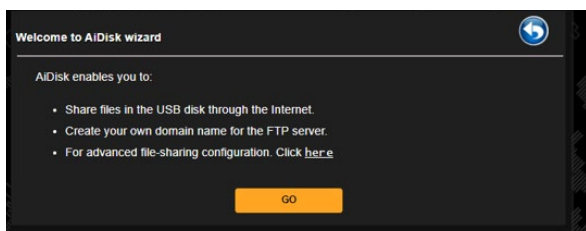


3.17.1 Använda AiDisk

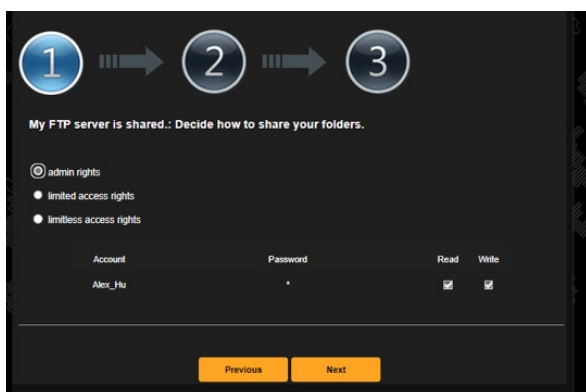
AiDisk ger dig möjlighet att dela filer som är lagrade på en ansluten USB-enhet via Internet. AiDisk hjälper dig också att installera ASUS DDNS och en FTP-server.

Använda AiDisk:

1. Från navigeringsfältet, gå till **General (Allmänt) > USB Application (USB-Applikation)**, och klicka på **AiDisk**-ikonen.
2. Från skärmen Welcome to AiDisk wizard (Välkommen till AiDisk-guiden) klicka på **Go (Starta)**.



3. Välj åtkomsträttigheterna som du vill tilldela klienterna för åtkomst av dina delade data.



4. Skapa ditt domännamn via ASUS DDNS-tjänsten, läs Villkor för användning och välj **I will use the service and accept the Terms of service (Jag ska använda tjänsten och accepterar villkoren för tjänsten)** och knappa in ditt domännamn. När du är klar, klicka på **Next (Nästa)**.



Du kan även välja **Skip ASUS DDNS settings (Hoppa över ASUS DDNS-inställningar)** och klicka på **Next (Nästa)** för att hoppa över DDNS-inställningen.

5. Klicka på **Finish (Slutför)** för att avsluta installationen.
6. För åtkomst till FTP-webbplatsen, starta en webbläsare eller en tredje-parts FTP-klient och knappa in ftp-länken (**ftp://<domain name>.asuscomm.com**), som du har skapat tidigare.

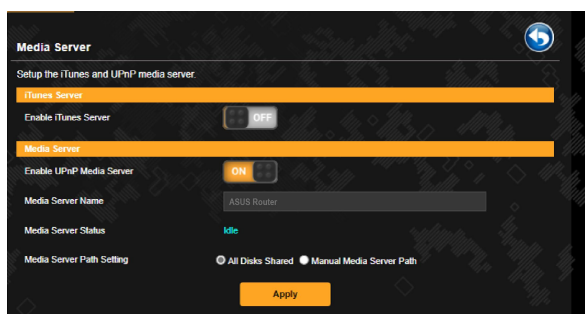
3.17.2 Använda Servers Center

Servers Center ger dig möjlighet att dela mediafilerna från USB-enheten via ett Media Server-arkiv, Samba-delningstjänst eller FTP-delningstjänst. Du kan även konfigurera andra inställningar för USB-enheten i Servers Center.

Använda Media Server

Din trådlösa router tillåter UPnP-stödda enheter åtkomst till multimediafiler från USB-enheten som är ansluten till din trådlösa router.

NOTERA: Innan du använder UPnP Media Server-funktionen, anslut din enhet till TUF-AX3000 V2:s nätverk.

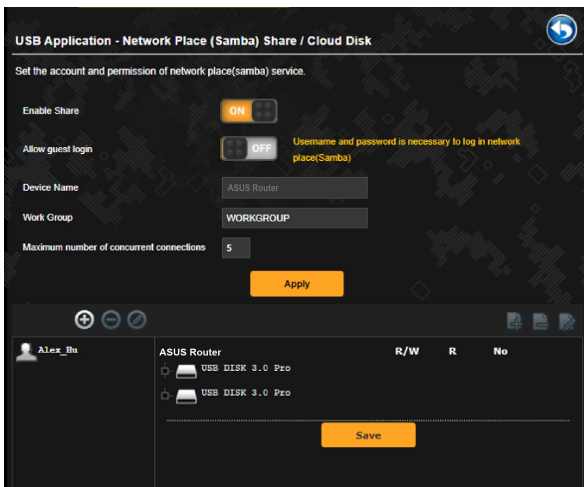


För att starta Media Servers inställningsida, gå till **General (Allmänt) > USB Application (USB-Applikation) > Media Server (Mediaserver)**. Se följande för en beskrivning av fälten:

- **Enable iTunes Server (Aktivera iTunes Server):** Välj ON/OFF (PÅ/AV) för att aktivera/inaktivera iTunes Server.
- **Enable UPnP Media Server (Aktivera UPnP Media Server):** Välj ON/OFF (PÅ/AV) för att aktivera/inaktivera UPnP Media Server.
- **Media Server Status (Mediaserverstatus):** Visar statusen för mediaservern.
- **Media Server Path Setting (Sökvägsinställning för mediaserver):** Välj **All Disks Shared (Alla diskar delas)** eller **Manual Media Server Path (Manuell sökväg för mediaserver)**.

Använda Network Place (Samba) Share-tjänsten

Network Place (Samba) Share ger dig möjlighet att installera konton och tillstånd för Samba-tjänsten.



Använda Samba Share:

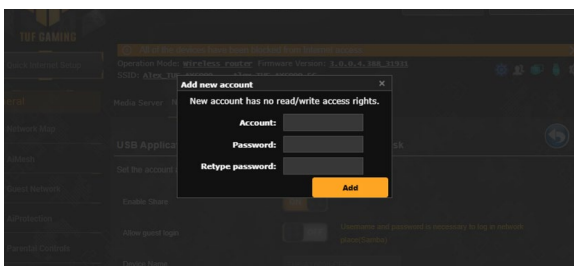
1. Från navigeringsfältet, gå till **General (Allmänt) > USB Application (USB-Applikation) > Network Place (Samba) Share / Cloud Disk**.

NOTERA: Network Place (Samba) Share är aktiverad som standard.


2. Följ nedanstående steg för att lägga till, ta bort eller modifiera ett konto:

Skapa ett nytt konto:


- a) Klicka på **+** för att lägga till ett nytt konto.
- b) I fälten **Account (Konto)** och **Password (Lösenord)** knappar du in namn och lösenord för din nätverksklient. Skriv lösenordet igen för att bekräfta. Klicka på **Add (Lägg till)** för att lägga till kontot i listan.

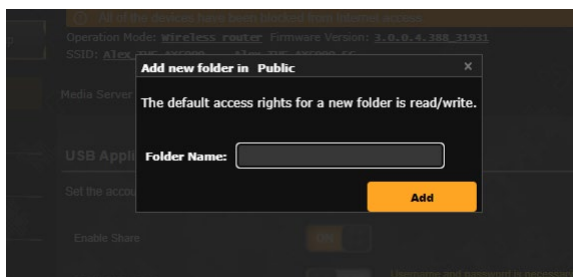


Ta bort ett befintligt konto:

- Välj det konto som du vill ta bort.
- Klicka på .
- Vid uppmaning, klicka på **Delete (Ta bort)** för att bekräfta att du vill ta bort kontot.

Lägga till en mapp:

- Klicka på .
- Ange mappens namn, och klicka på **Add (Lägg till)**. Mappen du skapade kommer att läggas till i mapplistan.



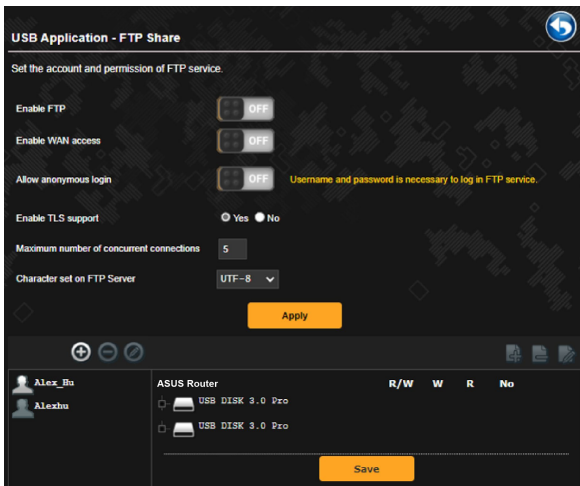
- Från listan med mappar väljer du den typ av åtkomsträttigheter som du vill tilldela för specifika mappar:
 - R/W**: Välj detta alternativ för att tilldela läs-/skrivåtkomst.
 - R**: Välj detta alternativ för att tilldela enbart läsåtkomst.
 - No (Nej)**: Välj detta alternativ om du inte vill dela en specifik filmapp.
- Klicka på **Apply (Verkställ)** för att verkställa ändringarna.

Använda FTP Share-tjänsten

FTP-delning gör det möjligt för en FTP-server att dela filer från USB-enhet till andra enheter via din lokala LAN eller via Internet.

VIKTIGT!

- Se till att ta bort USB-disken på ett säkert sätt. Felaktig borttagning av USB-enheten kan orsaka skadade data.
- För att ta bort USB-enheten säkert, se avsnitt **Säker borttagning av USB-enhet** under **3.12.3 Övervaka din USB-enhet**.



Använda FTP Share-tjänsten:

NOTER: Se till att du ställt in din FTP-server via AiDisk. För mer information, se avsnittet **3.17.1 Använda AiDisk**.

1. Från navigeringsfältet, gå till **General (Allmänt) > USB Application (USB-Applikation) > FTP Share**.
2. Från listan med mappar väljer du den typ av åtkomsträttigheter som du vill tilldela för specifika mappar:
 - **R/W:** Välj för att tilldela läs-/skrivåtkomst till en specifik mapp.
 - **W:** Välj för att tilldela enbart skrivåtkomst till en specifik mapp.
 - **R:** Välj för att tilldela enbart läsåtkomst till en specifik mapp.
 - **No (Nej):** Välj detta alternativ om du inte vill dela en specifik mapp.

3. Om du vill, kan du ställa in fältet **Allow anonymous login (Tillåt anonym inloggning)** på **ON (PÅ)**.
4. I fältet **Maximum number of concurrent connections (Maximalt antal samtidiga anslutningar)** anger du hur många enheter som samtidigt kan ansluta till FTP-delningsservern.
5. Klicka på **Apply (Verkställ)** för att bekräfta ändringarna.
6. För åtkomst till FTP-servern, knappa in ftp-länken **ftp://<hostname>.asuscomm.com** och ditt användarnamn och lösenord i en webbläsare eller tredje-parts FTP-program.

3.17.3 3G/4G

3G/4G USB-modem kan anslutas till TUF-AX4200 för att tillåta Internetåtkomst.

NOTERA: För en lista över verifierade USB-modem, besök:
<http://event.asus.com/2009/networks/3gsupport/>

Installera 3G/4G Internetåtkomst:

1. Från navigeringsfältet, klicka på **General (Allmänt) > USB Application (USB-Applikation) > 3G/4G**.
2. I fältet **Enable USB Modem (Aktivera USB-modem)**, välj **Yes (Ja)**.
3. Ställ in följande:
 - **Plats:** Välj din 3G/4G-tjänstleverantörs plats från rullgardinsmenyn.
 - **ISP:** Välj din Internettjänstleverantör (ISP) från rullgardinsmenyn.
 - **APN-tjänst (Åtkomstpunktens namn) (valfri):** Kontakta din 3G/4G-tjänstleverantör för detaljerad information.
 - **Uppringsnummer och PIN-kod:** 3G/4G-tjänstleverantörens åtkomstnummer och PIN-kod för anslutning.

NOTERA: PIN-kod kan variera mellan olika leverantörer.

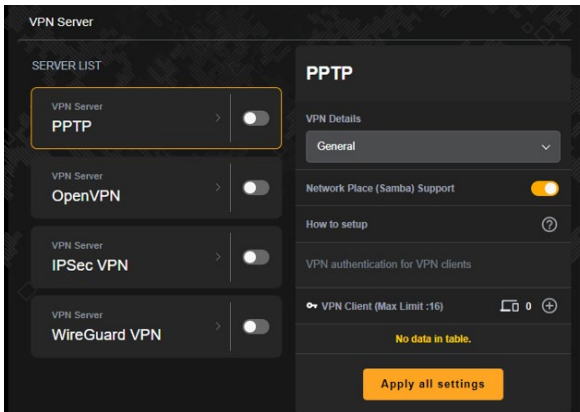
- **Användarnamn/Lösenord:** Användarnamnet och lösenordet tillhandahålls av 3G/4G-nätverksleverantören.
 - **USB Adapter:** Välj din USB 3G/4G-adapter i rullgardinsmenyn. Är du inte säker på vilken modell på USB-adapter du har eller modellen saknas i listan, välj **Auto**.
4. Klicka på **Apply (Verkställ)**.

NOTERA: Routern kommer att starta om för att inställningarna skall träda i kraft.

3.18 VPN


Ett virtuellt privat nätverk (VPN) tillhandahåller en säker kommunikation till en fjärrdator eller fjärrnätverk som använder ett offentligt nätverk som Internet.

NOTERA: Innan du installerar en VPN-anslutning måste du ha IP-adress eller domännamn till VPN-servern.



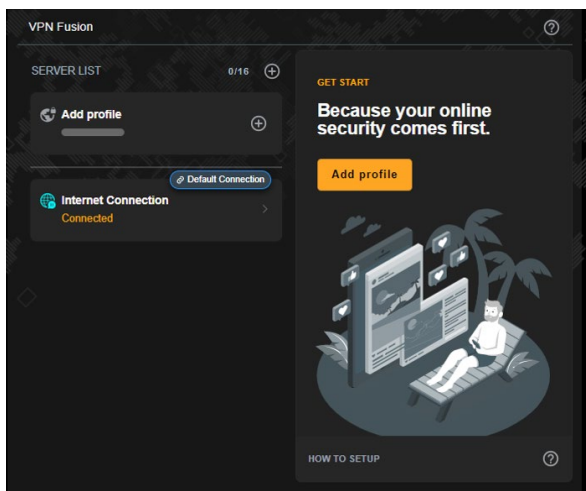
3.18.1 VPN-server

Installera åtkomst till en VPN-server:


1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > VPN**.
2. Klicka på **ON (PÅ)** i fältet **PPTP**.
3. I rullgardinsmenyn **VPN Details (VPN-detaljer)** väljer du **Advanced Settings (Avancerade inställningar)** om du vill konfigurera avancerade VPN-inställningar som sändningsstöd, verifiering, MPPE-kryptering och klient-IP-adressintervall.
4. Klicka på **ON (PÅ)** i fältet **Network Place (Samba) Support [Stöd för nätverksplats (Samba)]**.
5. Ange användarnamnet och lösenordet för åtkomst till VPN-servern. Klicka på .
6. Klicka på **Apply all settings (Verkställ alla inställningar)**.

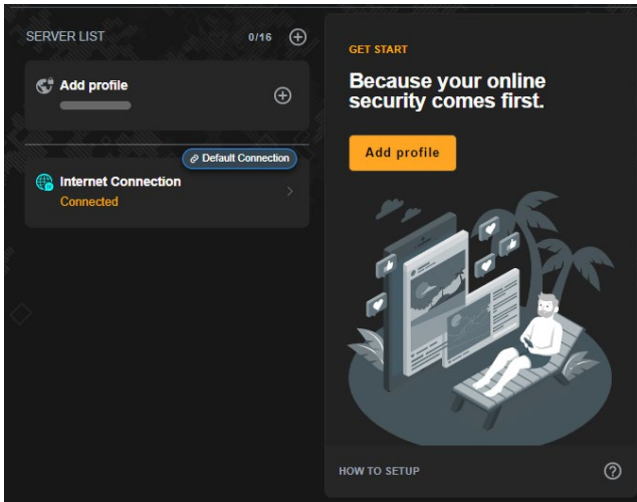
3.18.2 VPN-fusion

VPN Fusion ger dig möjlighet att ansluta till flera VPN-serverar samtidigt, och tilldela dina klientenheter för att ansluta till olika VPN-tunnlar. Vissa enheter som digitalboxar och Blu-ray-spelare stödjer inte VPN-program. Denna funktion tillhandahåller VPN-åtkomst till sådana enheter i ett hemnätverk utan att man behöver installera VPN-program, medan din smarttelefon förblir ansluten till Internet och inte VPN. För spelare motverkar VPN-anslutningen DDoS-attacker för att förhindra ditt datorspel eller din strömning från att kopplas ifrån spelservrarna. Genom att bygga en VPN-anslutning kan du även enkelt ändra din IP-adress till den region där spelservern finns, för att förbättra din ping-tid till spelservrar.



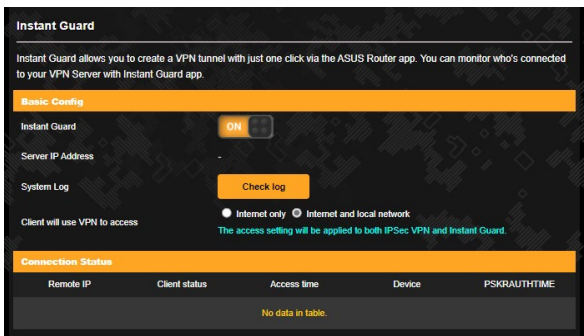
För att starta, följ dessa steg:

1. Klicka på knappen  bredvid **SERVER LIST (SERVERLISTA)** eller **Add profile (Lägg till profil)** för att lägga till en ny VPN-tunnel.
2. Aktivera VPN-anslutningen som du skapade i serverlistan.



3.18.3 Instant Guard

Instant Guard kör din egen privata VPN server på din egen router. När du använder en VPN tunnel passerar alla dina data genom servern. Med Instant Guard har du full kontroll över din egen server, vilket gör det till den säkraste lösningen.



3.19 WAN

3.19.1 Internetanslutning

Skärmen Internet Connection (Internetanslutning) ger dig möjlighet att konfigurera inställningarna för olika WAN-anslutningstyper.

WAN - Internet Connection

ASUS Router 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 of ASUS Router.

Basic Config

WAN Connection Type: Automatic IP ▾

Enable WAN: Yes No

Enable NAT: Yes No

Enable UPnP: [UPnP_FAQ](#) Yes No

Enable WAN Aggregation: Yes No
WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification). [WAN Aggregation FAQ](#)

WAN DNS Setting

Default status: Get the DNS IP from your ISP automatically.

DNS Server: Assign a DNS service to improve security, block advertisement and gain faster performance. [Assign](#)

Forward local domain queries to upstream DNS: Yes No

Enable DNS Rebind protection: Yes No

Enable DNSSEC support: Yes No

Prevent client auto DoH: Auto ▾

DNS Privacy Protocol: None ▾

DHCP Option

Class Identifier (Option 60):

Client Identifier (Option 61): IAID/DUID

Konfigurera WAN-anslutningsinställningarna:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > WAN > Internet Connection (Internetanslutning)**.
2. Konfigurera följande inställningar. När du är klar, klicka på **Apply (Verkställ)**.
 - **WAN Connection Type (WAN-anslutningstyp):** Välj typ av Internettjänstleverantör. Valen är **Automatic IP (Automatisk**

IP), PPPoE, PPTP, L2TP eller **static IP (statisk IP)**. Konsultera din ISP om routern inte kan erhålla en giltig IP-adress eller om du är osäker på typen av WAN-anslutning.

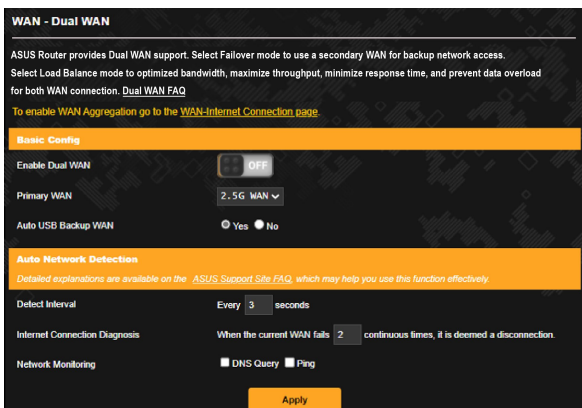
- **Enable WAN (Aktivera WAN):** Välj **Yes (Ja)** för att ge routern Internet-åtkomst. Välj **No (Nej)** för att inaktivera Internet-åtkomsten.
- **Enable NAT (Aktivera NAT):** NAT (Network Address Translation) är ett system där en offentlig IP (WAN IP) används för att tillhandahålla Internet-åtkomst till nätverksklienter med en privat IP-adress på en LAN. Den privata IP-adressen för varje nätverksklient sparas i en NAT-tabell och används för att cirkulera inkommande datapaket.
- **Enable UPnP (Aktivera UPnP):** UPnP (Universal Plug and Play) tillåter att flera enheter (som routrar, TV-apparater, stereosystem, spelkonsoler och mobiltelefon), kontrolleras via ett IP-baserat nätverk med eller utan en central kontroll genom en gateway. UPnP ansluter datorer av alla formfaktorer, genom att tillhandahålla ett sömlöst nätverk för fjärrkonfiguration och dataöverföring. Med UPnP upptäcks en ny enhet automatiskt. Efter anslutning till nätverket, kan enheter fjärrkonfigureras för att stödja P2P-applikationer, interaktiva spel, videokonferencer och webb- eller proxyservrar. Till skillnad från portvidarebefordra, som involverar manuell konfigurering av portinställningar, konfigurerar UPnP automatiskt router för att acceptera inkommande anslutningar och direkta begäranden till en specifik dator i det lokala nätverket.
- **Connect to DNS Server automatically (Anslut till DNS-server automatiskt):** Tillåt routern att skaffa DNS IP-adressen automatiskt från ISP:en. En DNS är en värd på Internet som översätter Internetnamn till numeriska IP-adresser.
- **Authentication (Verifiering):** Denna punkt kan specificeras av vissa ISP:ar. Kontrollera med din ISP och fyll i dem vid behov.

- **Host Name (Världnamn):** Detta fält ger dig möjlighet att tillhandahålla ett världnamn på din router. Det är ofta ett specialkrav från din ISP. Om din ISP tilldelade din dator ett världnamn, ska världnamnet anges här.
- **MAC Address (MAC-adress):** MAC-adress (Media Access Control) är en unik identifierare för din nätverksenhet. Vissa ISP:ar övervakar MAC-adressen för nätverksenheterna som ansluter till deras tjänst och avvisar oidentifierade enheter om försöker ansluta. För att undvika anslutningsproblem på grund av en oregistrerad MAC-adress kan du:
 - Kontakta din ISP och uppdatera den MAC-adress som är associerad med ISP-tjänsten.
 - Klon eller ändra MAC-adressen för den trådlösa ASUS-routern för att matcha MAC-adressen för den föregående nätverksenheten som identifierats av ISP:en.
- **DHCP query frequency (DHCP-frågefrekvens):** Ändrar intervallinställningarna för DHCP Discovery (DHCP-identifiering) för att undvika att DHCP-server blir överbelastad.

3.19.2 Dubbel WAN

Din trådlösa ASUS-router erbjuder dubbel WAN-support. Du kan ställa in den dubbla WAN-funktionen på något av dessa två lägen:

- **Failover Mode (Redundansläge):** Välj detta läge för att använda den sekundär WAN-funktionen som reservåtkomst till nätverk.
- **Load Balance Mode (Lastbalanseringsläge):** Välj detta läge för att optimera bandbredd, minimera svarstid och förhindra överbelastning av data för både primära och sekundära WAN-anslutningar.



WAN - Dual WAN

ASUS Router provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimized bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connection. [Dual WAN FAQ](#)

To enable WAN Aggregation go to the [WAN-Internet Connection page](#).

Basic Config

Enable Dual WAN OFF

Primary WAN 2.5G WAN

Auto USB Backup WAN Yes No

Auto Network Detection

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

Detect Interval Every 3 seconds

Internet Connection Diagnosis When the current WAN fails 2 continuous times, it is deemed a disconnection.

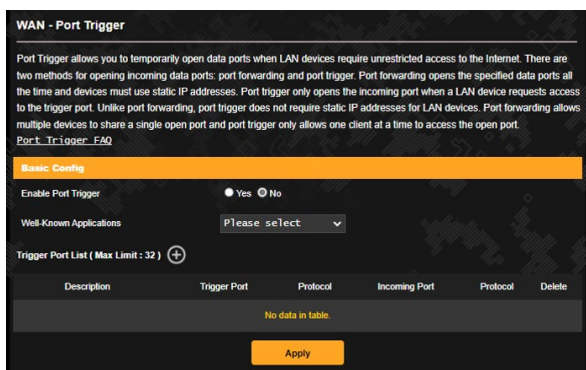
Network Monitoring DNS Query Ping

Apply

3.19.3 Portutlösning

Portintervallutlösning öppnar en förbestämd inkommande port under en begränsad tid när en klient på LAN:en gör en utgående anslutning till en specificerad port. Portutlösning används i följande scenarier:

- Mer än en lokal klient behöver portvidarebefordran för samma applikation vid en annan tidpunkt.
- En applikation kräver specifika inkommande portar som skiljer sig från de utgående portarna.



Installera Port Trigger:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > WAN > Port Trigger (Portutlösning)**.
2. I fältet **Enable Port Trigger (Aktivera portutlösning)**, markera **Yes (Ja)**.
3. Välj populära spel och webbtjänster som ska läggas till Port Trigger List (Portutlösningslista) i fältet **Well-Known Applications (Välkända applikationer)**.
4. I tabellen **Trigger Port List (Portutlösningslista)** anges följande information:

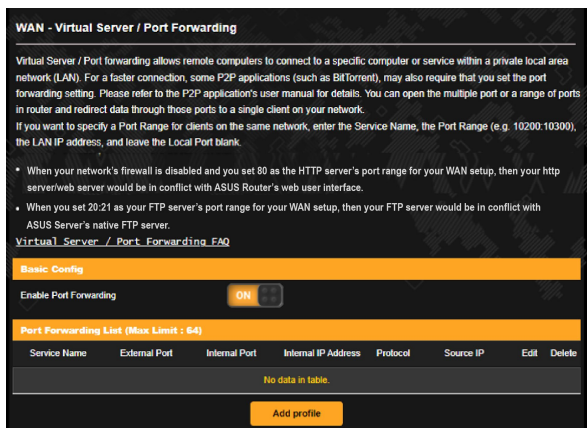
- **Description (Beskrivning):** Ange ett kort namn eller beskrivning för tjänsten.
 - **Trigger Port (Utlösningssport):** Specificera en utlösningssport för att öppna den inkommande porten.
 - **Incoming Port (Inkommande port):** Specificera en inkommande port för att ta emot ingående data från Internet.
 - **Protocol (Protokoll):** Välj protokoll, TCP eller UDP.
5. Klicka på **Add (Lägg till)**  för att ange portutlösningssinformation i listan. Klicka på knappen **Delete (Ta bort)**  för att ta bort en portutlösningsspost från listan.
 6. När du är klar, klicka på **Apply (Verkställ)**.

NOTER:

- Vid anslutning till en IRC-server, gör en klientdator en utgående anslutning med utlösningssportintervallet 66660-7000. IRC-servern svarar genom att verifiera användarnamnet och skapa en ny anslutning till klientdatorn med en inkommande port.
 - Routern avbryter anslutningen om Port Trigger är inaktiverad, eftersom den inte kan bestämma vilken dator som begär IRC-åtkomst. När Port Trigger är aktiverad tilldelas routern en ingångsport som ska ta emot inkommande data. Denna ingångsport stängs efter en bestämd tid eftersom routern är osäker på när applikationen har avslutats.
 - Portutlösning tillåter enbart att en klient i nätverket använder en specifik tjänst och en specifik ingångsport samtidigt.
 - Du kan inte använda samma applikation för att utlösa en port på mer än en dator åt gången. Routern kommer bara att vidarebefordra porten tillbaka till den senaste datorn för att skicka routern en begäran/utlösning.
-

3.19.4 Virtuellt server/Portvidarebefordran

Portvidarebefordran är en metod för att dirigera nätverkstrafik från Internet till en specifik port eller portintervall för att bestämma antalet enheter i ditt lokala nätverk. Inställning av portvidarebefordran på din router ger datorer utanför nätverket möjlighet att komma åt specifika tjänster från en dator i nätverket.



Installera Port Forwarding:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > WAN > Virtual Server/Port Forwarding (Virtuellt server/portvidarebefordran)**.
2. I fältet **Enable Port Forwarding (Aktivera portvidarebefordran)**, flytta skjutreglaget till **Yes (Ja)**.
3. Klicka på **Add profile (Lägg till profil)** och ange följande information i tabellen **Port Forwarding List (Lista över portvidarebefordran)**:
 - **Service Name (Tjänstnamn)**: Ange ett tjänstnamn.
 - **Protocol (Protokoll)**: Välj protokoll. Om du är osäker, välj **BOTH (BÅDA)**.
 - **Extern port**: Den externa porten accepterar följande format:
 - 1) Portintervall som använder ett kolon ":" mellan start- och ändporten, som 300:350.

- 2) Enstaka portar använder ett komma "," mellan individuella portar, t. ex. 566, 789.
- 3) En blandning av portintervall och enskilda portar använder kolon ":" Och komman "," som 1015:1024, 3021.

- **IP-adress på internet:** Knappa in klientens LAN IP-adress.

NOTERA: Använd en statisk IP-adress för den lokala klienten för att få portvidarebefordran att fungera riktigt. Se avsnitt **3.11 LAN** för information.

- **Internetport:** Ange en specifik port som ska ta emot vidarebefordrade paket. Lämna fältet tomt om du vill att inkommande paket ska omdirigeras till det specifika portintervallet.
 - **Käll-IP:** Om du vill öppna din port för en specifik IP-adress från internet, ange IP-adressen som du vill specificera i fältet Käll-IP.
4. Klicka på **Add (Lägg till)**  för att ange portutlösningssinformationen i listan. Klicka på knappen **Delete (Ta bort)**  för att ta bort en portutlösningsspost från listan.
 5. När du är klar, klicka på Apply (Verkställ).

Kontrollera om portvidarebefordran har konfigurerats:

- Kontrollera att servern eller applikationen är inställd och kör.
- Du kommer att behöva en klient utanför din LAN, men ha Internet-åtkomst (s.k. "Internet client"). Denna klient ska inte anslutas till ASUS-routern.
- Använd routerns WAN IP på Internet-klienten för åtkomst till servern. Om portvidarebefordran har fungerat, ska du kunna få åtkomst till filerna eller applikationerna.

Skillnader mellan portutlösning och portvidarebefordran:

- Portutlösning fungerar även om man inte ställer in en specifik LAN IP-adress. Till skillnad från portvidarebefordran, som kräver en statisk LAN IP-adress, tillåter portutlösning dynamisk portvidarebefordran med routern. Förinställda portintervall konfigureras för att acceptera inkommande anslutningar under en begränsad tid. Portutlösning tillåter att flera datorer kör applikationer som normalt skulle kräva manuell vidarebefordran av samma portar till varje dator i nätverket.
- Portutlösning är säkrare än portvidarebefordran eftersom de inkommande portarna inte är öppna hela tiden. De öppnas bara när en applikation gör en utgående anslutning genom utlösningporten.

3.19.5 DMZ

Virtuell DMZ exponerar en klient för Internet, och tillåter klienten att ta emot alla inkommande paket som dirigeras till din LAN.

Ingående trafik från Internet aviseras normalt och cirkuleras bara till en specifik klient om portvidarebefordran eller portutlösning har konfigurerats på nätverket. I en DMZ-konfiguration får en nätverksklient alla inkommande paket.

Det är praktiskt att installera DMZ på ett nätverk när du behöver att inkommande portar är öppna, eller du vill vara värd för en domän, webb eller e-postserver.

WARNING: Att öppna alla portar mot Internet på en klient gör nätverket sårbart för attacker utifrån. Tänk på säkerhetsriskerna som det innebär att använda DMZ.

Installera DMZ:

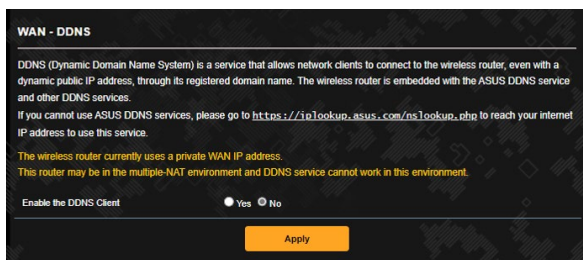
1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > WAN > DMZ**.
2. Konfigurera följande inställning: När du är klar, klicka på **Apply (Verkställ)**.
 - **IP address of Exposed Station (IP-adress för exponerad station):** Knappa in klientens LAN IP-adress som ska tillhandahålla DMZ-tjänsten och exponeras på Internet. Serverklienten måste ha en statisk IP-adress.

Ta bort DMZ:

1. Ta bort klientens LAN IP-adress från textrutan **IP Address of Exposed Station (IP-adress för exponerad station)**.
2. När du är klar, klicka på **Apply (Verkställ)**.

3.19.6 DDNS

Inställning av DDNS (Dynamic DNS) ger dig möjlighet att komma åt routern utifrån ditt nätverk genom den tillhandahållna ASUS DDNS-tjänsten eller annan DDNS-tjänst.



Ställa in DDNS:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > WAN > DDNS**.
2. Konfigurera följande inställningar: När du är klar, klicka på **Apply (Verkställ)**.
 - **Enable the DDNS Client (Aktivera DDNS-klient):** Aktivera DDNS för att få åtkomst till ASUS router via DNS-namnet istället för WAN IP-adressen.
 - **Server and Host Name (Server- och värddamn):** Välj ASUS DDNS eller annan DDNS. Om du vill använda ASUS DDNS, fyll i värddamnet i formatet xxx.asuscomm.com (xxx är ditt värddamn).
 - Om du vill använda en annan DDNS-tjänst, klicka först på FREE TRIAL (PROVA GRATIS) och registrera online. Fyll i User Name or E-mail Address (användarnamn eller e-postadress) och Password or DDNS key (lösenord eller DDNS-nyckel).
 - **Enable wildcard (Aktivera wildcard):** Aktivera wildcard om din DDNS-tjänst kräver det.

NOTER:

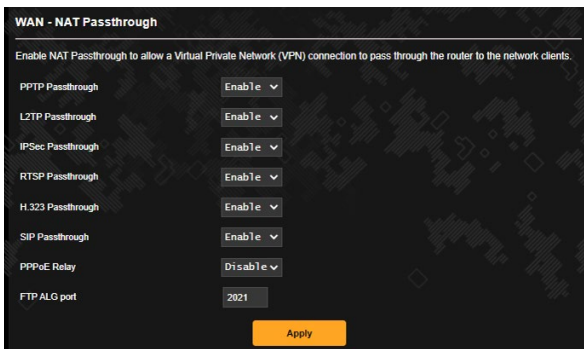
DDNS-tjänst fungerar inte under följande förhållanden:

- När en trådlös router använder en privat WAN IP-adress (192.168.x.x, 10.x.x.x eller 172.16.x.x), som indikeras med gul text.
 - Routern kan vara i ett nätverk som använder flera NAT-tabeller.
-

3.19.7 NAT-genomströmning

NAT Passthrough (NAT-genomströmning) tillåter att ett VPN (Virtuellt privat nätverk) ansluter för att passera igenom routern till nätverksklienterna. PPTP Passthrough, L2TP Passthrough, IPsec Passthrough och RTSP Passthrough är aktiverade som standard.

För att aktivera/inaktivera NAT-genomströmningsinställningarna, gå till **Advanced Settings (Avancerade inställningar) > WAN > NAT Passthrough (NAT-genomströmning)**. När du är klar, klicka på **Apply (Verkställ)**.



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
PPPoE Relay	Disable
FTP ALG port	2021
Apply	

3.20 Trådlös anslutning

3.20.1 Allmänt

Fliken General (Allmänt) ger dig möjlighet att konfigurera grundinställningarna för trådlös anslutning.

The screenshot shows the 'Wireless - General' configuration page. At the top, it says 'Set up the wireless related information below.' The settings are as follows:

- Enable Smart Connect: OFF (toggle)
- Band: 2.4 GHz (dropdown)
- Network Name (SSID): ASUS_2.4G (text input)
- Hide SSID: No (radio button selected)
- Wireless Mode: Auto (dropdown), with checkboxes for 'big Protection' and 'Disable 11b' (both checked)
- 802.11ax / WiFi 6 mode: Enable (dropdown), with a note: 'If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: FAQ' (link)
- WiFi Agile Multiband: Enable (dropdown)
- Target Wake Time: Disable (dropdown)
- Channel bandwidth: 20/40 MHz (dropdown)
- Control Channel: Auto (dropdown), with 'Current Control Channel: 3' and a checkbox for 'Auto select channel including channel 12, 13' (unchecked)
- Extension Channel: Auto (dropdown)
- Authentication Method: WPA2-Personal (dropdown)
- WPA Encryption: AES (dropdown)
- WPA Pre-Shared Key: 1234567890 (text input, with a 'Danger' warning icon)
- Protected Management Frames: Disable (dropdown)
- Group Key Rotation Interval: 3600 (text input)

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

Konfigurera grundinställningarna för trådlös anslutning:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Wireless (Trådlös) > General (Allmänt)**.
2. Välj 2,4GHz eller 5GHz som frekvensband för det trådlösa nätverket.
3. Om du vill använda funktionen Smart Connect (Smart anslutning), flytta skjutreglaget till **ON (PÅ)** i fältet **Enable Smart Connect (Aktivera smart anslutning)**. Denna funktion ansluter automatiskt klienterna i ditt nätverk till rätt 2,4GHz eller 5GHz band för optimal hastighet.

4. Tilldela ett unikt namn med högst 32 tecken för ditt SSID (Service Set Identifier) eller nätverksnamn för att identifiera ditt trådlösa nätverk. Wi-Fi-enheter kan identifiera och ansluta till det trådlösa nätverket via ditt tilldelade SSID. SSID på informationsbanderollen uppdateras när nya SSID sparas i inställningarna.

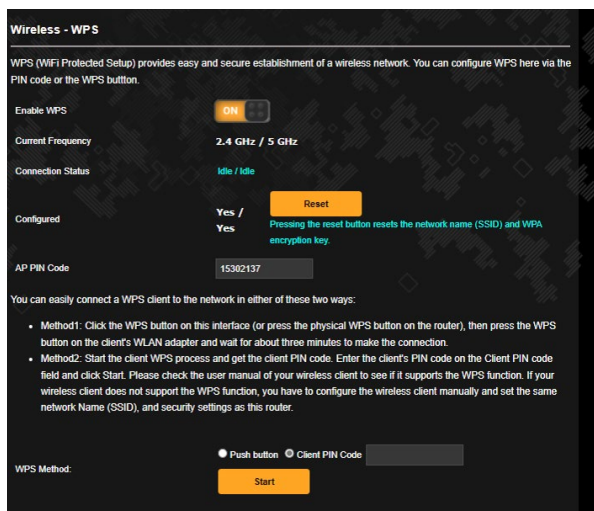
NOTERA: Du kan tilldela unika SSID för 2,4GHz och 5GHz frekvensband.

5. I fältet **Hide SSID (Dölj SSID)**, välj **Yes (Ja)** för att förhindra att trådlösa enheter identifierar din SSID. När funktionen etablerats måste du ange SSID:n manuellt på den trådlösa enheten för att få åtkomst till det trådlösa nätverket.
6. Välj något av dessa trådlösa lägen för att bestämma vilken typ av trådlösa enheter som kan anslutas till din trådlösa router:
 - **Auto:** Välj Auto för att tillåta att 802.11ac-, 802.11n-, 802.11g- och 802.11b-enheter ansluter till den trådlösa routern.
 - **N only (N enbart):** Välj **N only (N enbart)** för att maximera den trådlösa N-prestandan. Denna inställning hindrar 802.11g- och 802.11b-enheter från att ansluta till den trådlösa routern.
 - **Legacy (Bakåtkompatibelt):** Välj **Legacy (Bakåtkompatibelt)** för att tillåta att 802.11b/g/n-enheter ansluter till den trådlösa routern. Men maskinvara som stödjer 802.11n internt kommer bara att köra på högst 54 Mbps hastighet.
7. Välj en operativkanal för den trådlösa routern. Välj **Auto** för att tillåta att den trådlösa routern automatiskt väljer kanalen som har minst störning.
8. Välj kanalbandbredd för att underlätta högre överföringshastigheter.
9. Välj verifieringsmetod.
10. När du är klar, klicka på **Apply (Verkställ)**.

3.20.2 WPS

WPS (WiFi Protected Setup) är en trådlös säkerhetsstandard som tillåter dig att enkelt ansluta enheter till ett trådlöst nätverk. Du kan konfigurera WPS-funktionen via PIN-kod eller WPS-knapp.

NOTERA: Kontrollera att enheten stödjer WPS.



Aktivera WPS på ditt trådlösa nätverk:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Wireless (Trådlös) > WPS**.
2. I fältet **Enable WPS (Aktivera WPS)**, flytta skjutreglaget till **ON (PÅ)**.
3. WPS använder 2,4 GHz som standard. Om du vill ändra frekvensen till 5 GHz, stäng **OFF (AV)** WPS-funktionern, klicka på **Switch Frequency (Växla frekvens)** i fältet **Current Frequency (Aktuell frekvens)**, och sätt **ON (PÅ)** WPS igen.

NOTERA: WPS stödjer autentisering med Open System, WPA/WPA2/WPA3-Personal. WPS stödjer inte ett trådlöst nätverk som använder en krypteringsmetod med Shared Key, WPA-Enterprise, WPA2-Enterprise och RADIUS.

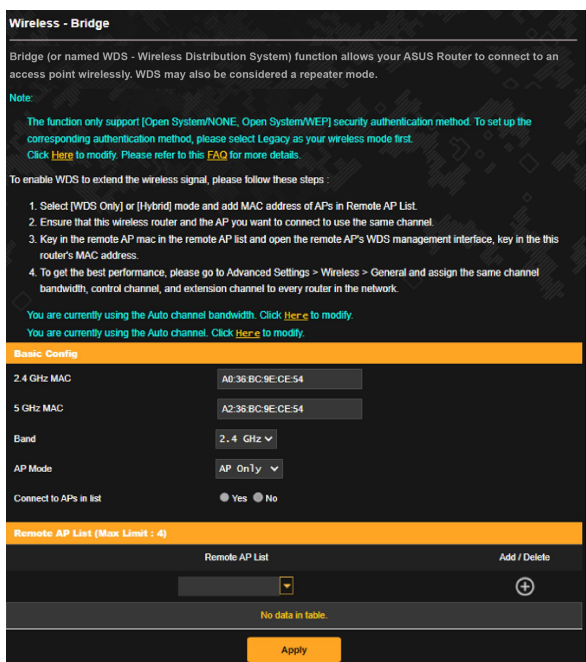
4. I WPS Method-fältet, välj **Push button (Tryckknapp)** eller **Client PIN Code (Klient-Pin Kod)**. Om du väljer **Push button (Tryckknapp)**, gå till steg 5. Om du väljer **Client PIN Code (Klient-Pin Kod)**, gå till steg 6.
5. För att installera WPS med routerns WPS-knapp, följ dessa steg:
 - a. Klicka på **Start** eller tryck på WPS-knappen på baksidan av den trådlösa routern.
 - b. Tryck på WPS-knappen på den trådlösa routern. Den identifieras normalt med WPS-logotyp.

NOTERA: Kontrollera din trådlösa enhet eller bruksanvisningen för WPS-knappens placering.

- c. Den trådlösa routern kommer att söka efter tillgängliga WPS-enheter. Om den trådlösa routern inte hittar några WPS-enheter, kommer den att växla till standby-läge.
6. För att installera WPS med routerns klient-PIN-kod, följ dessa steg:
 - a. Leta reda på WPS PIN-koden i den trådlösa routerns bruksanvisning eller på själva enheten.
 - b. Knappa in klient-PIN-koden i textrutan.
 - c. Klicka på **Start** för att ställa in den trådlösa routern i WPS-övervakningsläge. Routerns lysdioder blinkar snabbt tre gånger tills WPS-installationen är klar.

3.20.3 Brygga

Bridge (Brygga) eller WDS (Wireless Distribution System) ger din trådlösa ASUS-router möjlighet att enbart ansluta trådlöst till en annan åtkomstpunkt, och hindra andra trådlösa enheter eller stationer att komma åt din trådlösa ASUS-router. Den kan även betraktas som en trådlös repeterare där ASUS trådlösa router kommunicerar med en annan åtkomstpunkt och andra trådlösa enheter.



Ställ in den trådlösa bryggan:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Wireless (Trådlös) > WDS**.
2. Välj frekvensband för den trådlösa bryggan.
3. Välj något av dessa alternativ i fältet **AP Mode (AP-läge)**:


- **AP Only (Enbart AP):** Inaktiverar den trådlösa bryggfunktionen.
- **WDS Only (Enbart WDS):** Aktiverar den trådlösa bryggfunktionen men hindrar andra trådlösa enheter/stationer från att ansluta till routern.
- **HYBRID:** Aktiverar den trådlösa bryggfunktionen och tillåter andra trådlösa enheter/stationer att ansluta till routern.

NOTERA: I Hybrid-läget kan trådlösa enheter som är anslutna till den trådlösa ASUS-routern enbart ta emot halva anslutningshastigheten för åtkomstpunkten.

4. I fältet **Connect to APs in list (Anslut till AP:er i listan)**, klicka på **Yes (Ja)** om du vill ansluta till en annan åtkomstpunkt i Remote AP List (Fjärr-AP-lista).
5. Som standard är den operativa/kontrollkanalen för trådlös brygga inställd på **Auto** för att router automatiskt ska kunna välja den kanal som har minst störningar.

Du kan ändra **Control Channel (Kontrollkanal)** från fliken **Advanced Settings (Avancerade inställningar) > Wireless (Trådlös) > General (Allmänt)**.

NOTERA: Tillgängliga kanaler varierar i olika länder och regioner.

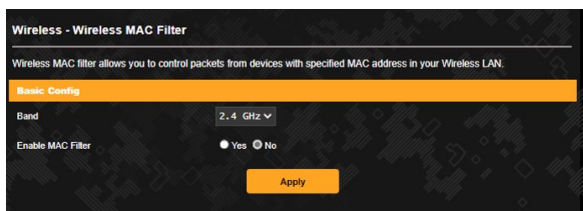
6. I Remote AP List (Fjärr-AP-lista), knappa in en MAC-adress och klicka på knappen **Add (Lägg till)**  för att ange MAC-adressen för andra tillgängliga åtkomstpunkter.

NOTERA: Åtkomstpunkter som läggs till listan ska vara på samma kontrollkanal som den trådlösa ASUS-routern.


7. Klicka på **Apply (Verkställ)**.

3.20.4 Trådlöst MAC-filter

Wireless MAC filter (Trådlöst MAC-filter) ger kontroll över paket som sänds till en specificerad MAC- (Media Access Control) adress på den trådlösa routernätverket.

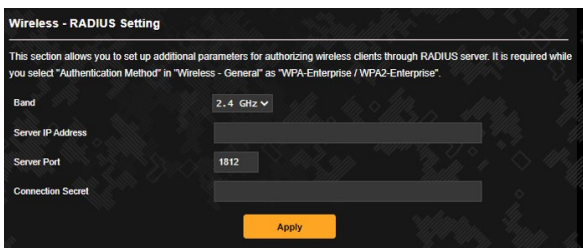


Ställ in det trådlösa MAC-filtret:

1. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Wireless (Trådlös) > Wireless MAC Filter (Trådlöst MAC-filter)**.
2. Välj ett frekvensband.
3. Markera **Yes (Ja)** i fältet **Enable Mac Filter (Aktivera MAC-filter)**.
4. I rullgardinsmenyn **MAC Filter Mode (MAC-filterläge)**, välj **Accept (Acceptera)** eller **Reject (Avvisa)**.
 - Välj **Accept (Acceptera)** för att tillåta åtkomst till det trådlösa nätverket för enheter i MAC-filterlistan.
 - Välj **Reject (Avvisa)** för att neka åtkomst till det trådlösa nätverket för enheter i MAC-filterlistan.
5. I MAC-filterlistan, klicka på knappen **Add (Lägg till)**  och knappa in MAC-adressen för den trådlösa enheten.
6. Klicka på **Apply (Verkställ)**.

3.20.5 RADIUS-inställning

RADIUS-inställning (Remote Authentication Dial In User Service) ger ett extra säkerhetslager när du väljer WPA-Enterprise, WPA2-Enterprise eller Radius med 802.1x som ditt autentiseringsläge.



Ställ in trådlösa RADIUS-inställningar:

1. Den trådlösa routerns autentiseringsläge måste vara inställt på WPA-Enterprise, WPA2-Enterprise eller Radius med 802.1x.

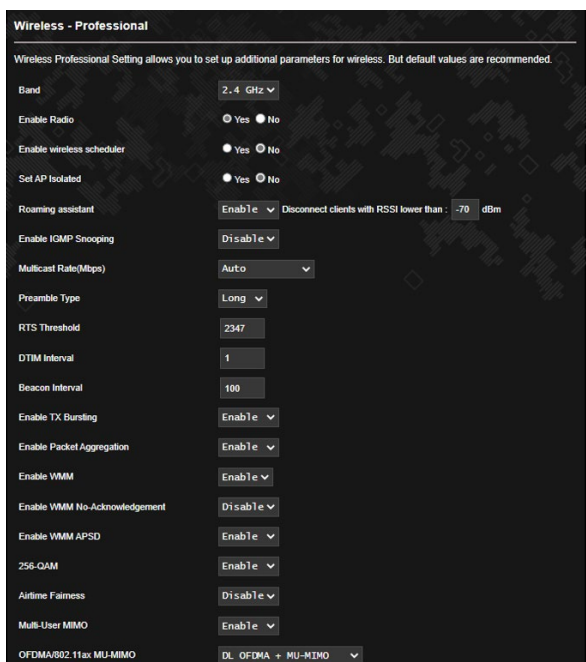
NOTERA: Se avsnittet **3.20.1 Allmänt** för configuration av den trådlösa routerns autentiseringsläge.

2. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Wireless (Trådlös) > RADIUS Setting (RADIUS-inställning)**.
3. Välj ett frekvensband.
4. Knappa in din RADIUS-servers IP-adress i fältet **Server IP Address (Server-IP-adress)**.
5. I fältet **Server Port (Serverport)** anger du serverporten.
6. Tilldela lösenordet för åtkomst till din RADIUS-server i fältet **Connection Secret (Anslutning secret)**.
7. Klicka på **Apply (Verkställ)**.

3.20.6 Professionell

Skärmen Professional (Professionell) ger möjlighet till avancerade konfigurationer.

NOTERA: Vi rekommenderar att du använder standardvärdena på denna sida.



Wireless - Professional

Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.

Band: 2.4 GHz

Enable Radio: Yes No

Enable wireless scheduler: Yes No

Set AP Isolated: Yes No

Roaming assistant: Enable Disconnect clients with RSSI lower than: -70 dBm

Enable IGMP Snooping: Disable

Multicast Rate(Mbps): Auto

Preamble Type: Long

RTS Threshold: 2347

DTIM Interval: 1

Beacon Interval: 100

Enable TX Bursting: Enable

Enable Packet Aggregation: Enable

Enable WMM: Enable

Enable WMM No-Acknowledgement: Disable

Enable WMM APSD: Enable

256-QAM: Enable

Airtime Fairness: Disable

Multi-User MIMO: Enable

OFDMA/802.11ax MU-MIMO: DL OFDMA + MU-MIMO

Följande kan konfigureras på skärmen **Professional (Professionella)** inställningar:

- **Band:** Välj vilket frekvensband de professionella inställningarna ska tillämpas på.
- **Aktivera Radio:** Välj **Yes (Ja)** för att aktivera trådlöst nätverk. Välj **No (Nej)** för att inaktivera trådlöst nätverk.
- **Aktivera trådlös schemaläggare:** Välj **Yes (Ja)** för att aktivera och konfigurera den trådlösa schemaläggaren. Välj **No (Nej)** för att inaktivera den trådlösa schemaläggaren.

- **Datum för aktivering av radio (vardagar):** Du kan specificera vilka veckodagar det trådlösa nätverket ska vara aktivt.
- **Tidpunkt för aktivering av radio:** Du kan specificera tidsintervallet då det trådlösa nätverket är aktivt under veckan.
- **Datum för aktivering av radio (helg):** Du kan specificera vilka helgdagar det trådlösa nätverket ska vara aktivt.
- **Tidpunkt för aktivering av radio:** Du kan specificera tidsintervallet då det trådlösa nätverket är aktivt under helgen.
- **Ställ in AP Isolerat:** Set AP isolated (ställ in AP isolerat) hindrar trådlösa enheter på ditt nätverk att kommunicera med varandra. Funktionen är användbar om många gäster går med eller lämnar ditt nätverk. Välj **Yes (Ja)** för att aktivera funktionen eller **No (Nej)** för att inaktivera.
- **Roaming-assistent:** I nätverkskonfigurationer som involverar flera åtkomstpunkter eller trådlösa repeterare kan trådlösa klienter ibland inte ansluta automatiskt till bästa tillgängliga AP, eftersom de fortfarande är anslutna till den trådlösa huvudroutern. Aktivera denna inställning så att klienten kopplas ifrån den trådlösa huvudroutern om signalstyrkan är under en specifik tröskel, och anslut till en starkare signal.
- **Aktivera IGMP snooping:** Aktivering av den här funktionen gör så att IGMP (Internet Group Management Protocol) kan övervakas mellan enheter och optimerar trådlös multicast-trafik.
- **Multisändningshastighet (Mbps):** Välj multisändningshastigheten eller klicka på **Disable (Inaktivera)** för att stänga av samtidig singelsändning.
- **Inledningstyp:** Preamble Type definierar hur lång tid routern spenderar på CRC (Cyclic Redundancy Check). CRC är en metod för att identifiera fel under dataöverföring. Välj **Short (Kort)** för ett upptaget trådlöst nätverk med hög nätverkstrafik. Välj **Long (Lång)** om ditt trådlösa nätverk består av äldre eller bakåtkompatibla trådlösa enheter.
- **AMPDU RTS:** Aktivera den här funktionen för att skapa en grupp rutor innan de överförs och använda RTS för varje AMPDU för kommunikation mellan 802.11g och 802.11b-enheter.

- **Tröskelvärde:** Välj det lägre värdet för RTS (Request to Send) Threshold för att förbättra den trådlösa kommunikationen i ett upptaget eller med mycket störning, med hög nätverkstrafik och flera trådlösa enheter.
- **DTM-Intervall:** DTIM (Delivery Traffic Indication Message) Interval eller Data Beacon Rate (Datasingleringsintervall) är tidsintervallet innan en signal skickas till en trådlös enhet i viloläge som indikerar att ett datapaket väntar på leverans. Standardvärdet är 3 millisekunder.
- **Signaleringsintervall:** Beacon Interval är tiden mellan en DTIM och nästa. Standardvärdet är 100 millisekunder. Sänk Beacon Interval-värdet för en ostadig trådlös anslutning eller för roaming-enheter.
- **Aktivera TX Bursting:** Enable TX Bursting förbättrar överföringshastigheten mellan den trådlösa routern och 802.11g-enheter.
- **Aktivera WMM APSD:** Aktivera WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) för att förbättra energisparfunktionerna mellan trådlösa enheter. Välj **Disable (Inaktivera)** för att stänga av WMM APSD.
- **Optimera AMPDU-mängd:** Optimera max antal MPDUs i en AMPDU och undvik att paket tappas eller skadas under överföring i felbenägna trådlösa kanaler
- **Turbo QAM:** Aktivera den här funktionen för att stödja 256-QAM (MCS 8/9) på 2,4 GHz-bandet för att uppnå bättre räckvidd och kapacitet på den frekvensen.
- **Reducerad bandbredd:** Med reducerad bandbredd bestäms inte hastigheten på nätverket av den långsammaste trafiken. Genom att fördela tiden rättvist mellan klienter, medger reducerad bandbredd att varje överföring kan förflyttas i sin högsta möjliga hastighet.
- **Explicit strålformning:** Klientens WLAN-adaptör och router stödjer strålformningsteknik. Denna teknik tillåter att dessa enheter kommunicerar kanaluppskattningen och styrriktningen till varandra för att förbättra hämtnings- och upplänkshastigheten.
- **Universal Beamforming (Universell strålformning):** För gamla trådlösa nätverksadaptörer som inte stödjer strålformning, beräknar routern kanalen och bestämmer styrriktningen för att förbättra nedlänkshastigheten.

4 Verktyg

NOTER:

- Hämta och installera den trådlösa routerns verktyg från ASUS webbplats:
 - Device Discovery v1.4.8.3 (Enhetsidentifiering) på <https://www.asus.com/networking-iot-servers/wifi-routers/asus-gaming-routers/tuf-gaming-ax3000-v2/helpdesk/download/?model2Name=TUF-Gaming-AX3000-V2>
 - Firmware Restoration v1.9.0.4 (Återställning av inbyggd programvara) på: <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip>
 - Windows Printer Utility v2.1.0.3 (Skrivarverktyg) på: <https://www.asus.com/networking-iot-servers/wifi-routers/asus-gaming-routers/tuf-gaming-ax3000-v2/helpdesk/download/?model2Name=TUF-Gaming-AX3000-V2>
 - Verktögen stöds inte på MAC OS.
-

4.1 Enhetsidentifiering

Device Discovery (Enhetsidentifiering) är ett ASUS WLAN-verktyg som identifierar en trådlös ASUS-routerenhet, och ger dig möjlighet att konfigurera de trådlösa nätverksinställningarna.

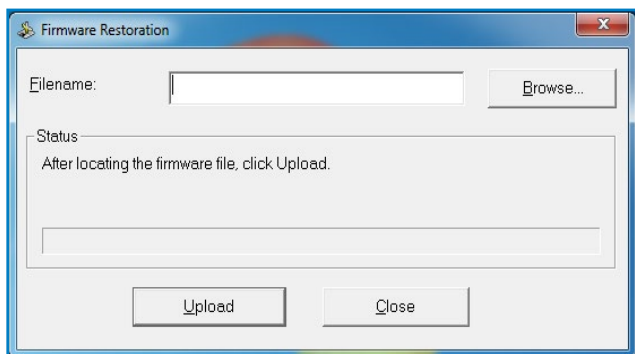
Starta Device Discovery-verktyget:

- Från din dators skrivbord klickar du på **Start > All Programs (Alla program) > ASUS Utility (ASUS verktyg) > ASUS Wireless Router (ASUS Trådlös Router) > Device Discovery (Enhetsidentifiering)**.

NOTERA: När du ställer in routern på åtkomstpunktläge behöver du använda Device Discovery för att få routerns IP-adress.

4.2 Återställning av fast programvara

Firmware Restoration (Återställning av fast programvara) används på en trådlös ASUS-router som misslyckas under uppgraderingsprocessen av den fasta programvaran. Den överför den fasta programvara som du specificerar. Processen tar ungefär tre till fyra minuter.



VIKTIGT! Starta räddningsläget på routern innan återställningsverktyget för det fasta programvaran används.

NOTERA: Denna funktion stöds inte på MAC OS.

För att starta räddningsläget och använda återställningsverktyget för den fasta programvaran:

1. Koppla bort den trådlösa routern från strömkällan.
2. Håll in knappen Reset (Återställning) på baksidan, och koppla samtidigt in den trådlösa routern till strömkällan. Släpp återställningsknappen när strömlysdioden på framsidan blinkar sakta, vilket indikerar att den trådlösa routern är i räddningsläget.
3. Ställ in en statisk IP på datorn, och använd följande för att ställa in dina TCP/IP-inställningar:

IP address (IP-adress): 192.168.1.x

Subnet mask (Nätmask): 255.255.255.0

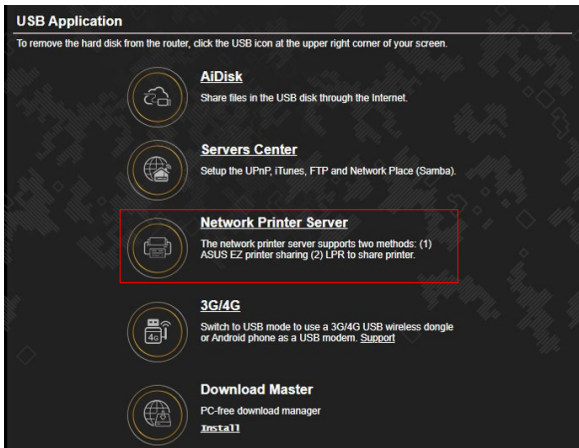
4. Från din dators skrivbord klickar du på **Start > All Programs (Alla program) > ASUS Utility TUF-AX3000 V2 Wireless Router (ASUS verktyg TUF-AX3000 V2 trådlös router) > Firmware Restoration (Återställning av fast programvara)**.
5. Specificera en fast programfil klicka sedan på **Upload (Överför)**.

NOTERA: Detta är inte en uppgraderingsfunktion för fast program och kan inte användas på en fungerande trådlös ASUS-router. Normal uppgradering av fast programvara måste göras genom webbgränssnittet. Se **Kapitel 3: Konfigurera de Allmänna och Avancerade inställningar** för ytterligare detaljer.

4.3 Installera din skrivarserver

4.3.1 Delning av EZ-skrivare

Verktöget ASUS EZ Printing Sharing (Delning av EZ-skrivare) ger dig möjlighet att ansluta en USB-skrivare till din trådlösa routers USB-port och installera skrivarservern. Detta ger dina nätverksklienter möjlighet att skriva ut och skanna filer trådlöst.



NOTERA: Skrivarserverfunktionen stöds på Windows® 7/8/8.1/10/11.

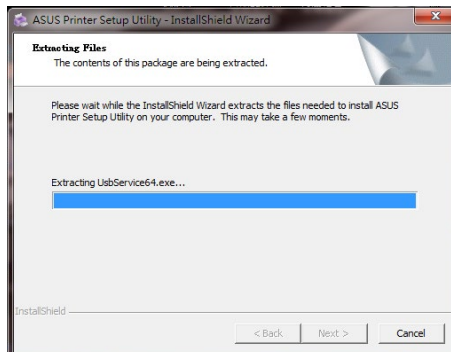
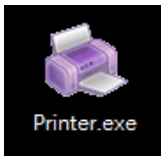
Ställa in delningsläge för EZ-skrivare:

1. Från navigeringsfältet, gå till **General (Allmänt) > USB Application (USB-Applikation) > Network Printer Server (Nätverksskrivarserver)**.
2. Klicka på **Download Now! (Hämta nu!)** för att hämta nätverksskrivarverktöget.

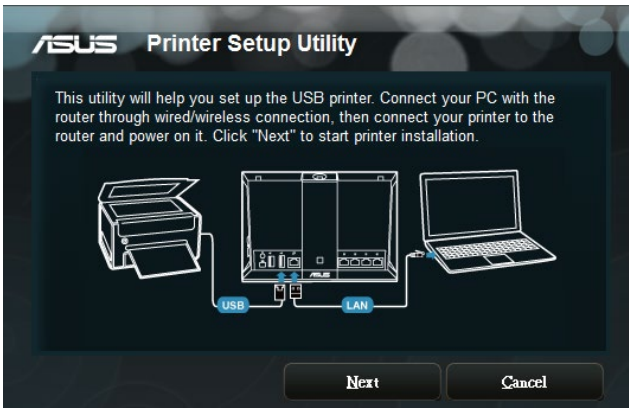


NOTERA: Nätverksskrivarverktöget stöds enbart på Windows® 7/8/8.1/10/11. För att installera verktöget på Mac OS, välj **Use LPR protocol for sharing printer (Använd LPR-protokoll för delning av skrivare)**.

3. Packa upp den hämtade filen och klicka på skrivarikonen för att köra installationsprogrammet för nätverksskrivaren.



4. Följ instruktionerna på skärmen för att ställa in din maskinvara, klicka sedan på **Next (Nästa)**.

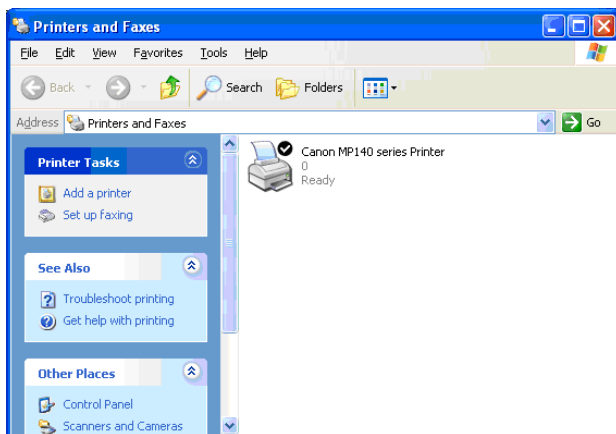


5. Vänta några minuter tills den första installationen avslutas. Klicka på **Next (Nästa)**.
6. Klicka på **Finish (Slutför)**, för att fullborda installationen.

7. Följ Windows® OS-instruktionerna för att installera skrivarens drivrutiner.



8. När installationen av skrivarens drivrutiner är klar kan nätverkets klienter använda skrivaren.



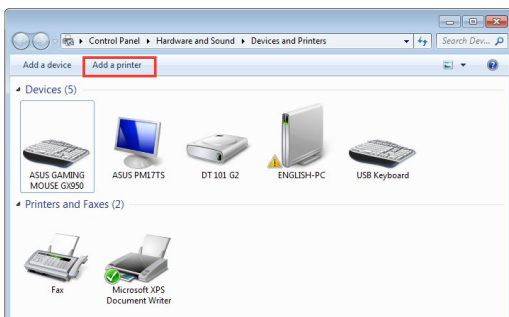
4.3.2 Använd LPR för att dela skrivare

Du kan dela din skrivare med datorer som kör på Windows®- och MAC-operativsystem med LPR/LPD (Line Printer Remote/Line Printer Daemon).

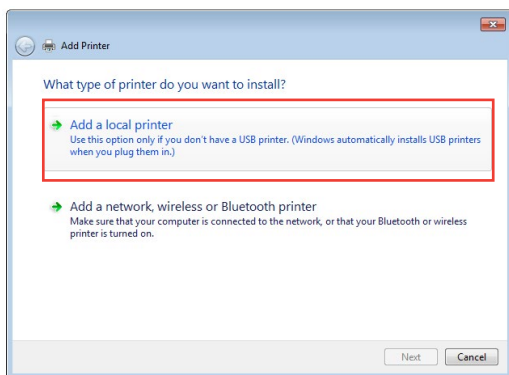
Dela din LPR-skrivare

Dela din LPR-skrivare:

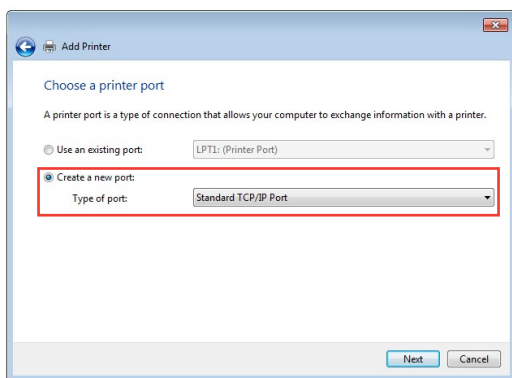
1. Från Windows® skrivbord, klicka på **Start > Devices and Printers (Enheter och skrivare) > Add a printer (Lägg till en skrivare)** för att köra **Add Printer Wizard (Guiden Lägg till skrivare)**.



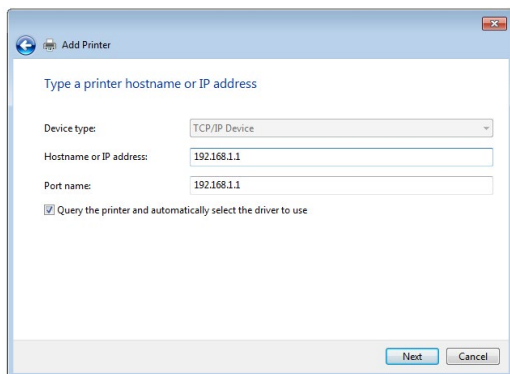
2. Välj **Add a local printer (Lägg till en lokal skrivare)** och klicka på **Next (Nästa)**.



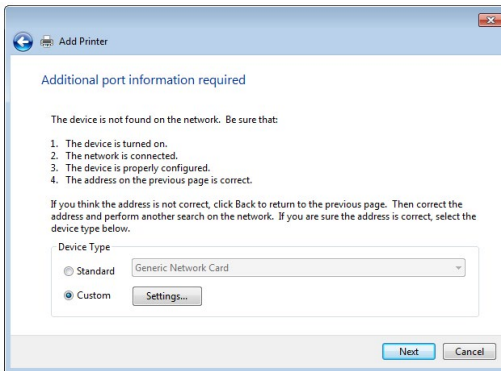
3. Välj **Create a new port (Skapa en ny port)** och ställ in **Type of Port (Typ av ny port)** på **Standard TCP/IP Port**. Klicka på **Next (Nästa)**.



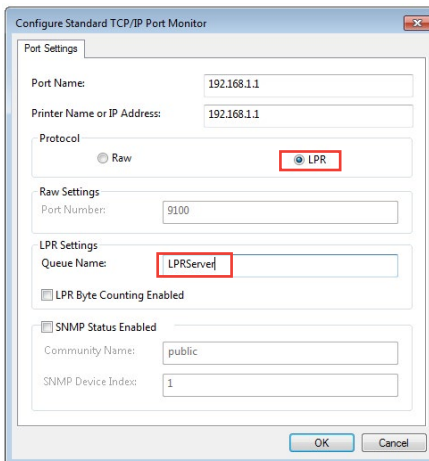
4. Knappa in den trådlösa routerns IP-adress i fältet **Hostname or IP address (Värnamn eller IP-adress)**, och klicka på **Next (Nästa)**.



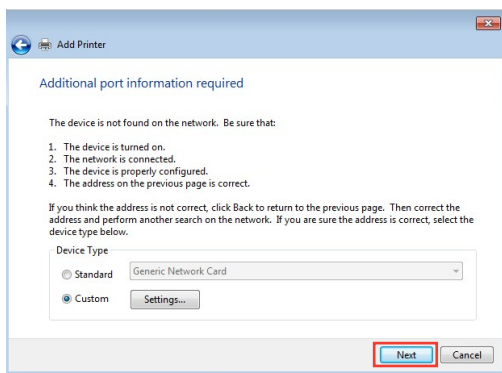
5. Välj **Custom (Anpassa)** och klicka på **Settings (Inställningar)**.



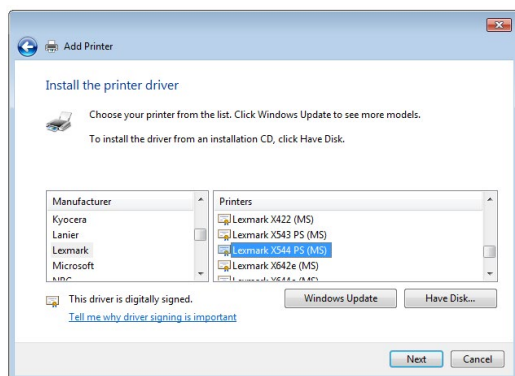
6. Ställ in **Protocol (Protokoll)** på **LPR**. I fältet **Queue Name (Könamn)**, knappa in **LPRServer**, och klicka på **OK** för att fortsätta.



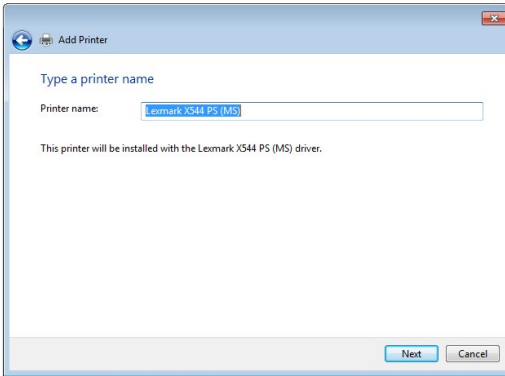
7. Klicka på **Next (Nästa)** för att avsluta inställningen av standard-TCP/IP-porten.



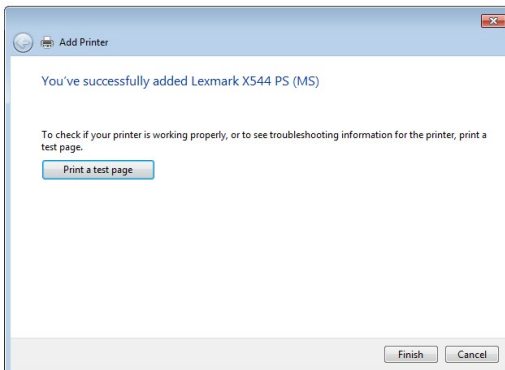
8. Installera skrivarenheten från säljare-modellistan. Om skrivaren saknas i listan, klicka på **Have Disk (Har disk)** för att manuellt installera skrivarens drivrutiner från en CD-ROM eller fil.



9. Klicka på **Next (Nästa)** för att acceptera standardnamnet för skrivaren.



10. Klicka på **Finish (Slutför)**, för att fullborda installationen.



4.4 Hämtningsadministratör

Download Master (Hämtningsadministratör) är ett verktyg som hjälper dig att hämta filer, även när din bärbara dator eller andra enheter är avstängda.

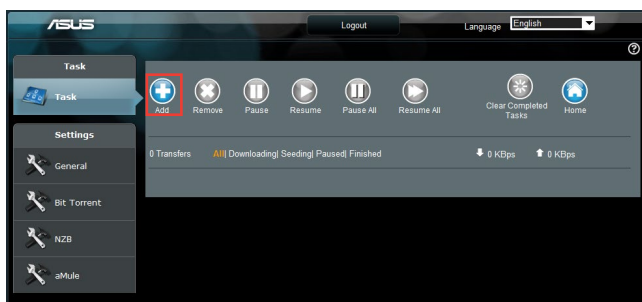
NOTERA: Du behöver en USB-enhet som är ansluten till den trådlösa routern för att använda Download Master.

Använd Download Master:

1. Klicka på **General (Allmänt) > USB Application (USB-Applikation) > Download Master (Hämtningsadministratör)** för att hämta och installera verktyget automatiskt.

NOTERA: Om du har mer än en USB-enhet, välj den USB-enhet som du vill hämta filerna till.

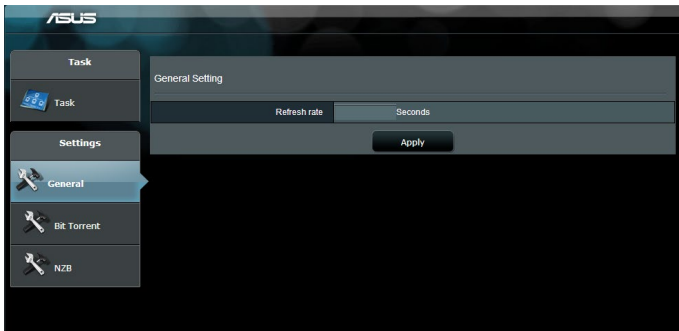
2. När hämtningen är klar, klicka på ikonen för Download Master för att börja använda verktyget.
3. Klicka på **Add (Lägg till)** för att lägga till en hämtningsuppgift.



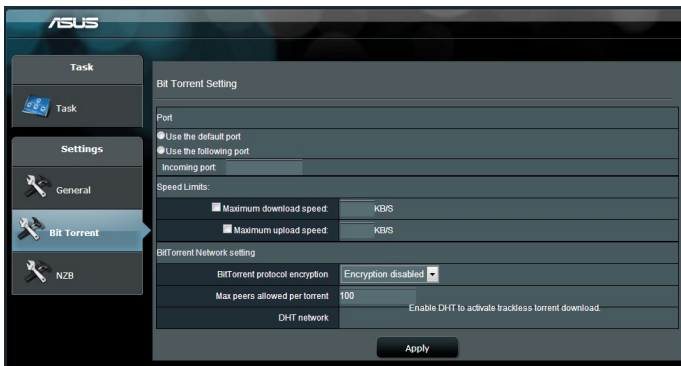
4. Välj en hämtningstyp som Bit Torrent, HTTP eller FTP. Tillhandahåll en torrentfil eller URL för att starta hämtningen.

NOTERA: För detaljer om Bit Torrent, se avsnittet **4.4.1 Konfigurera hämtningsinställningarna för Bit Torrent**.

5. Använd navigeringsfältet för att konfigurera de avancerade inställningarna.



4.4.1 Konfigurera hämtningsinställningar för Bit Torrent

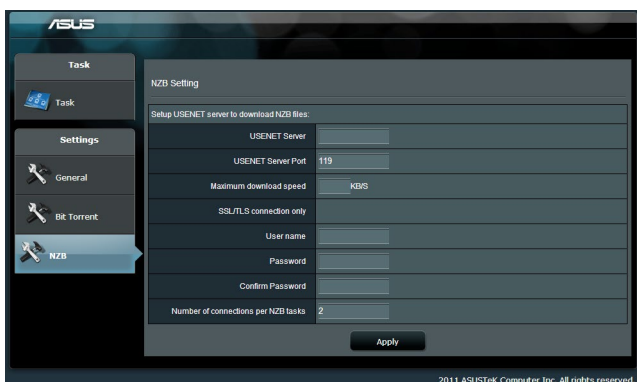


Konfigurera hämtningsinställningarna för Bit Torrent:

1. Från Download Masters navigeringsfält, klicka på **Bit Torrent** för att starta sidan **Bit Torrent Setting (Inställning av Bit Torrent)**.
2. Välj en specifik port för din hämtningsuppgift.
3. För att förhindra nätverksproblem kan du begränsa de maximala överförings- och hämtningshastigheterna under **Speed Limits (Hastighetsgränser)**.
4. Du kan begränsa det maximala antalet tillåtna peer-datorer, och aktivera eller inaktivera filkryptering under hämtningar.

4.4.2 NZB-inställningar

Du kan installera en USENET-server för att hämta NZB-filer. När du angett USENET-inställningar, **Apply (Verkställ)**.



5 Felsökning

Detta kapitel tillhandahåller lösningar på problem som du kan stöta på med routern. Om du stöter på problem som inte tas upp i detta kapitel, kontakta ASUS supportwebbplats på:

<https://www.asus.com/support> för mer produktinformation och kontaktdetaljer för ASUS tekniska support.

5.1 Grundläggande felsökning

Om du har problem med routern, prova de grundläggande stegen i detta avsnitt innan du söker ytterligare lösningar.

Uppgradera den fasta programvaran till den senaste versionen.

1. Starta Web GUI. Från navigeringsfältet, gå till **Advanced Settings (Avancerade inställningar) > Administration > Firmware Upgrade (Uppgradering av fast programvara)**. Klicka på **Check (Kontrollera)** för att verifiera att du har den senaste fasta programvaran.
2. Om den senaste fasta programvaran är tillgänglig, besök ASUS globala webbplats på https://www.asus.com/networking-iot-servers/wifi-routers/asus-gaming-routers/tuf-gaming-ax3000-v2/helpdesk_bios/?model2Name=TUF-Gaming-AX3000-V2 för att hämta den senaste fasta programvaran.
3. Från sidan **Firmware Upgrade (Uppgradering av fast programvara)**, klicka på **Browse (Bläddra)** för att lokalisera filen med den fasta programvaran.
4. Klicka på **Upload (Överför)** för att uppgradera den fasta programvaran.

Starta om nätverket i följande ordning:

1. Stäng av modemmet.
2. Dra ur sladden till modemmet.
3. Stäng av routern och datorerna.
4. Anslut modemmet.
5. Slå på modemmet och vänta i två (2) minuter.
6. Slå på routern och vänta i två (2) minuter.
7. Slå på datorerna.

Kontrollera att Ethernet-kablarna är riktigt anslutna.

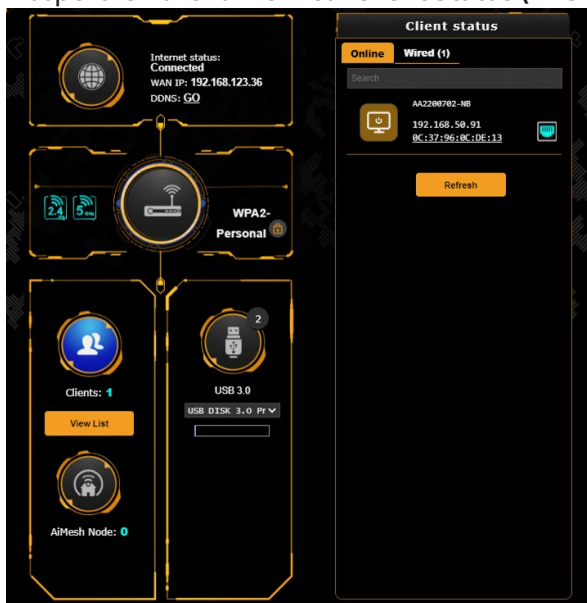
- När Ethernet-kabeln som ansluter routern med modemet är riktigt ansluten, kommer WAN-lysdioden att vara tänd.
- När Ethernet-kabeln mellan den påslagna datorn och router är riktigt ansluten, kommer motsvarande LAN-lysdiod att vara tänd.

Kontrollera om den trådlösa inställningen på din dator matchar den på routern.

- När du ansluter din dator trådlöst till routern, se till att SSID (trådlöst nätverksnamn), krypteringsmetod och lösenord stämmer.

Kontrollera om dina nätverksinställningar stämmer.

- Varje klient på nätverket ska ha en giltig IP-adress. ASUS rekommenderar att du använder den trådlösa routerns DHCP-server för att tilldela IP-adresser till datorer i nätverket.
- Vissa leverantörer av kabelmodemtjänster kräver att du använder MAC-adresserna för datorn som först registrerades på kontot. Du kan visa MAC-adressen i Web GUI, sidan **Network Map (Nätverkskarta) > Clients (Klienter)**, och hovra muspekaren över din enhet i **Client Status (Klientstatus)**.

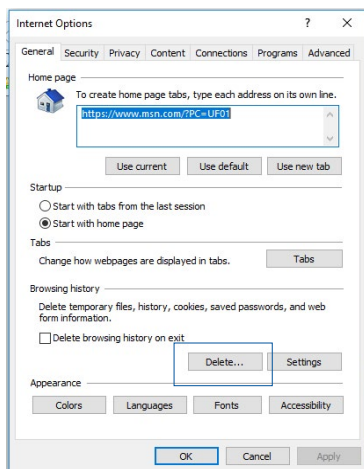


5.2 Vanliga frågor (FAQs)

Jag kan inte komma åt routerns gränssnitt med webbläsaren.

- Om datorn är kabelansluten, kontrollera anslutningen av Ethernet-kabeln och lysdiodens status enligt beskrivning i föregående avsnitt.
- Kontrollera att du använder rätt inloggningsinformation. Standardinloggningsnamn och -lösenord som är "admin/admin". Kontrollera att Caps Lock-tangenten är inaktiverad när du anger inloggningsinformationen.
- Radera cookies och filer i din webbläsare. För Internet Explorer, följ dessa steg:

1. Starta Internet Explorer, klicka på **Tools (Verktyg)** > **Internet Options (Internetalternativ)**.
2. I fliken **General (Allmänt)**, under **Browsing history (Webbhistorik)**, klicka på **Delete... (Ta bort...)**, välj **Temporary Internet Files (Tillfälliga Internet-filer)** och **Cookies and website data (Kakor och webbplatsdata)** och klicka på **Delete (Ta bort)**.



NOTER:

- Kommandona för att ta bort cookies och filer varierar mellan olika webbläsare.
- Inaktivera proxyserverinställningarna, avbryt uppringningsanslutningen och ställ in TCP/IP-inställningarna för att automatiskt erhålla en IP-adress. Se kapitel 1 i bruksanvisningen för ytterligare detaljer.
- Du måste använda CAT5e eller CAT6 Ethernetkablar.

Klienten kan inte etablera en trådlös anslutning med routern.

NOTERA: Om du har problem med att ansluta till 5 GHz nätverk, se till att din trådlösa enhet stödjer 5 GHz eller har dualbandskapacitet.

- **Out of Range (Utanför täckningsområde):**
 - Flytta routern närmare den trådlösa klienten.
 - Prova att justera routerns antenn till bästa riktning enligt beskrivning i avsnitt **1.4 Placera din router.**
- **DHCP server has been disabled (DHCP-servern har inaktiverats):**
 1. Starta Web GUI. Gå till **General (Allmänt) > Network Map (Nätverkskarta) > Clients (Klienter)** och sök efter enheten som du vill ansluta till routern.
 2. Om du inte hittar enheten i listan **Network Map (Nätverkskarta)**, gå till **Advanced Settings (Avancerade inställningar) > LAN > DHCP Server, Basic Config (Grundläggande konfiguration)**, välj **Yes (Ja)** på **Enable the DHCP Server (Aktivera DHCP-servern).**

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. ASUS Router supports up to 253 IP address for your local network.

[Manually Assigned IP around the DHCP list FAQ](#)

Basic Config

Enable the DHCP Server Yes No

ASUS Router's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time (seconds)

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS Yes No

WINS Server

Manual Assignment

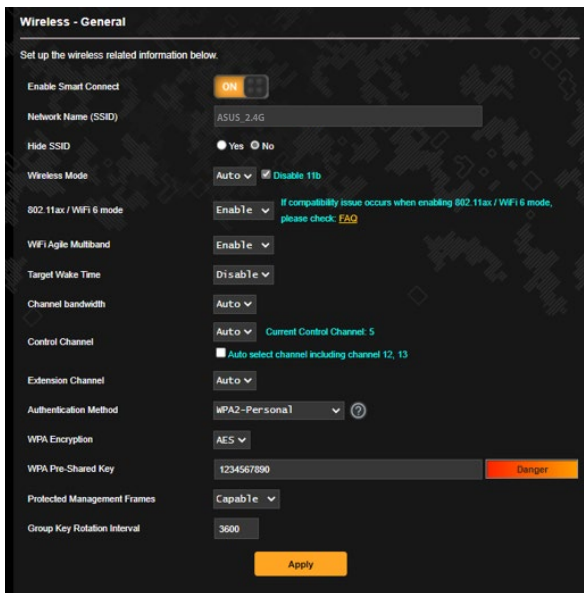
Enable Manual Assignment Yes No

Manually Assigned IP around the DHCP list (Max Limit : 128)

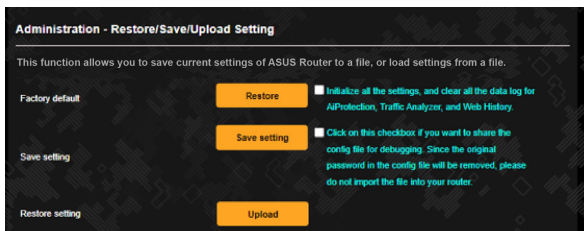
Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
xx:aa:35:bc:9e:ce:54	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

- SSID har dolts. Om din enhet hittar SSID från andra routrar, men inte hittar din routers SSID, gå till **Advanced Settings (Avancerade inställningar) > Wireless (Trådlöst) > General (Allmänt)**, välj **No (Nej)** på **Hide SSID (Dölj SSID)**, och välj **Auto** på **Control Channel (Kontrollkanal)**.



- Om du använder en trådlös LAN-adapter, kontrollera om den trådlösa kanalen som används överensstämmer med de tillgängliga kanalerna där du befinner dig. Om inte, justera kanalen, kanalbandbredden och det trådlösa läget.
- Om du fortfarande inte kan ansluta routern trådlöst, kan du återställa router till fabriken standardinställningar. I routers gränssnitt, klicka på **Administration > Restore/Save/Upload Setting (Återställ/Spara/Överför inställning)** och klicka på **Restore (Återställ)**.



Internet är inte åtkomligt.

- Kontrollera om din router kan ansluta till din ISP:s WAN IP-adress. Det gör du genom att starta Web GUI och gå till **General (Allmänt) > Network Map (Nätverkskarta)**, och kontrollera **Internet Status**.
- Om routern inte kan ansluta till din ISP:s WAN IP-adress, försök att starta om nätverket enligt beskrivning i avsnittet **Restart your network in following sequence (Starta om nätverket i följande ordning)** under **Basic Troubleshooting (Grundläggande felsökning)**.



- Enheten har blockerats via klassificeringskontrollen. Gå till **General (Allmänt) > Parental Controls (Klassificeringskontroll)** och se om enheten finns i listan. Finns enheten i listan under **Client Name (Klientnamn)**, ta bort enheten med knappen **Delete (Ta bort)** eller justera inställningarna för Time Management (Tidshantering).
- Finns det fortfarande ingen Internetåtkomst, försök att starta om datorn och verifiera nätverkets IP-adress och gateway-adress.
- Kontrollera statusindikatorerna på ADSL-modemet och den trådlösa routern. Om WAN-lysdioden på den trådlösa routern inte är PÅ, kontrollera om alla kablar är riktigt isatta.

Du har glömt SSID (nätverksnamn) eller nätverkslösenord.

- Installera en ny SSID och kryperingsnyckel via en kabelanslutning (Ethernet-kabel). Starta Web GUI, gå till **Network Map (Nätverkskarta)**, klicka på routerikonen, ange ett nytt SSID och kryperingsnyckel, och klicka på **Apply (Verkställ)**.
- Återställ routern till standardinställningarna. Starta Web GUI, klicka på **Administration > Restore/Save/Upload Setting (Återställ/Spara/Överför inställning)** och klicka på **Restore (Återställ)**. Standardinloggningskontot och lösenordet är båda "admin".

Hur återställs systemet till dess standardinställning?

- Gå till **Administration > Restore/Save/Upload Setting (Återställ/Spara/Överför inställning)** och klicka på **Restore (Återställ)**.

Följande är standardinställning från fabrik:

Användarnamn:	admin
Lösenord:	admin
Aktivera DHCP:	Ja (om WAN-kabeln är ansluten)
IP-adress:	http://www.asusrouter.com (eller 192.168.1.1)
Domännamn:	(Tomt)
Nätmask:	255.255.255.0
DNS Server 1:	192.168.1.1
DNS Server 2:	(Tomt)
SSID (2.4GHz):	ASUS_XX_2G
SSID (5GHz):	ASUS_XX_5G

Uppgradering av fast programvara misslyckades.

Starta räddningsläget innan återställningsverktyget för den fasta programvaran körs. Se avsnitt **4.2 Firmware Restoration (Återställning av fast programvara)** för hur man använder återställningsverktyget för den fasta programvaran.

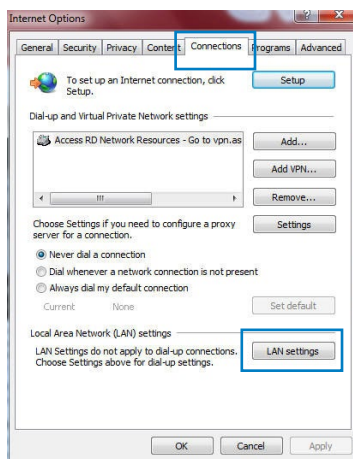
Kan inte komma åt Web GUI

Innan du konfigurerar din trådlösa router, genomför de steg som beskrivs i detta avsnitt för din värddator och nätverksklienter.

A. Inaktivera proxyservern, om den är aktiverad.

Windows®

1. Klicka på **Start > Internet Explorer** för att starta webbläsaren.
2. Klicka på **Tools (Verktyg) > Internet options (Internetalternativ) > Connections (Anslutningar) > LAN settings (LAN-inställningar)**.

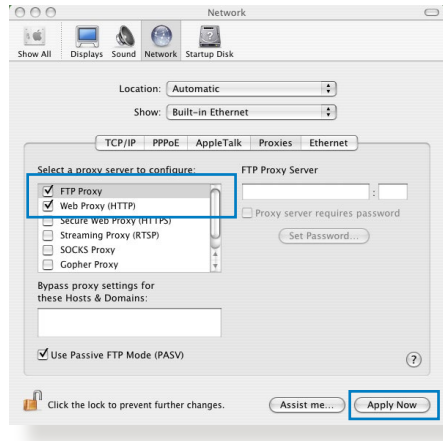


3. Från skärmen Local Area Network (LAN) Settings (Lokala LAN-inställningar), avmarkera **Use a proxy server for your LAN (Använd en proxy-server för din LAN)**.
4. Klicka på **OK** när du är klar.



MAC OS

1. Från din Safari webbläsare, klicka på **Safari > Preferences (Preferenser) > Advanced (Avancerade) > Change Settings... (Ändra inställningar...)**.
2. Avmarkera **FTP Proxy** och **Web Proxy (HTTP)** från nätverksskärmen.
3. Klicka på **Apply Now (Verkställ nu)** när du är klar.

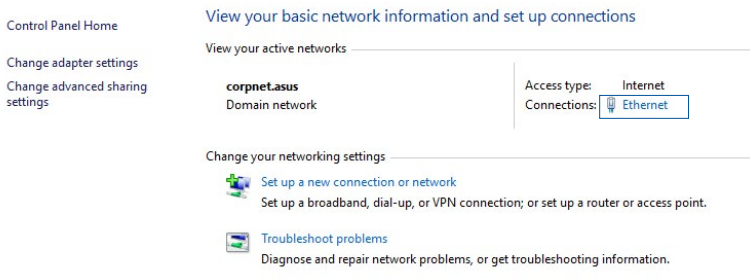


NOTERA: Se din webbläsares hjälpfunktion för detaljer om inaktivering av proxyservern.

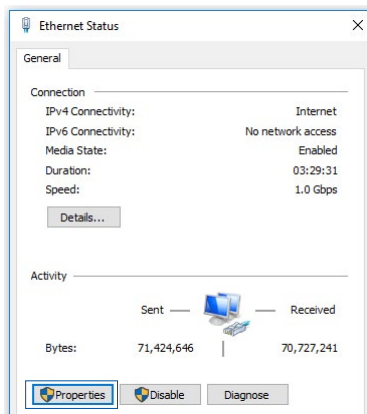
B. Ställ in TCP/IP-inställningarna för att automatiskt erhålla en IP-adress.

Windows®

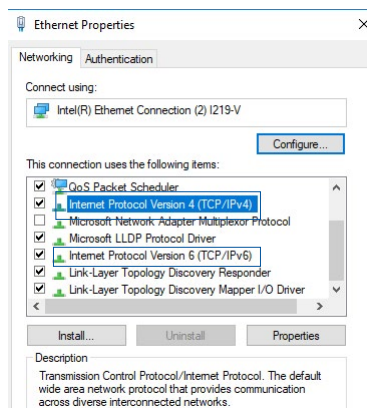
1. Klicka på **Start > Control Panel (Kontrollpanel) > Network and Sharing Center (Nätverks- och delningscenter)**, klicka därefter på nätverksanslutningen för att visa dess statusfönster.



2. Klicka på **Properties** (**Egenskaper**) för att visa fönstret Ethernet-egenskaper.



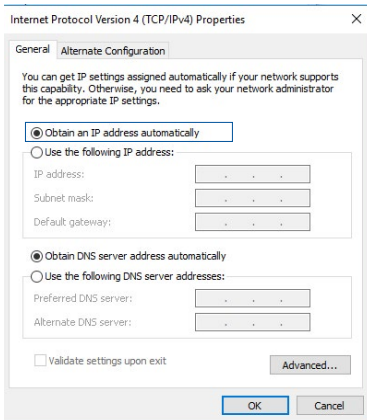
3. Välj **Internet Protocol Version 4 (TCP/IPv4)** eller **Internet Protocol Version 6 (TCP/IPv6)**, klicka sedan på **Properties (Egenskaper)**.




4. För att erhålla IPv4 IP-inställningarna automatiskt, markera **Obtain an IP address automatically (Erhåll en IP-adress automatiskt)**.

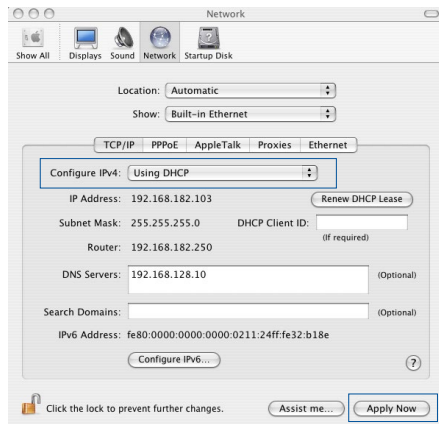
För att erhålla IPv6 IP-inställningarna automatiskt, markera **Obtain an IP address automatically (Erhåll en IP-adress automatiskt)**.

5. Klicka på **OK** när du är klar.



MAC OS

1. Klicka på Apple-ikonen  som är placerad överst till vänster på skärmen.
2. Klicka på **System Preferences (Systempreferenser) > Network (Nätverk) > Configure... (Konfigurera...)**.
3. Från fliken **TCP/IP** välj **Using DHCP (Använd DHCP)** i rullgardinslistan **Configure IPv4 (Konfigurera IPv4)**.



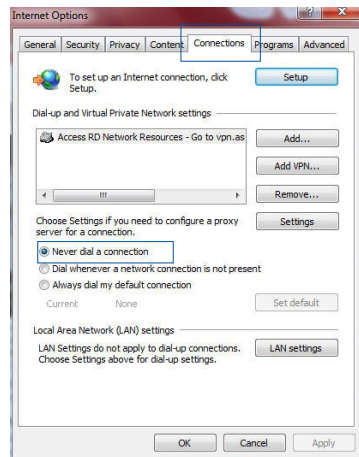
4. Klicka på **Apply Now (Verkställ nu)** när du är klar.

NOTERA: Se ditt operativsystems hjälp och supportfunktion för detaljer om konfiguration av din dators TCP/IP-inställningar.

C. Inaktivera fjärranslutningen, om den är aktiverad.

Windows®

1. Klicka på **Start > Internet Explorer** för att starta webbläsaren.
2. Klicka på **Tools (Verktyg) > Internet options (Internetalternativ) > Connections (Anslutningar)**.
3. Markera **Never dial a connection (Ring aldrig upp en fjärranslutning)**.
4. Klicka på **OK** när du är klar.



NOTERA: Se din webbläsares hjälpfunktion för detaljer om inaktivering av fjärranslutningen.

Bilagor

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

Service och support

Besök vår flerspråkiga webbplats på <https://www.asus.com/support/>.

