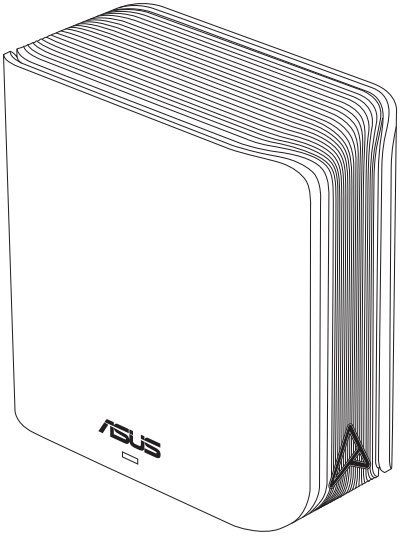
Panduan Pengguna

ZenWiFi BD4

Penghala Dwi Jalur BE3600



IN SEARCH OF INCREDIBLE

MY23951
Edisi Pertama
Ogos 2024

Kandungan

Kandungan

Kandungan

1 Mengenali penghala wayarles anda

1.1 Selamat datang!

Terima kasih kerana membeli Penghala Wayarles ASUS ZenWiFi BD4!

Dengan warna logam monogram A yang menonjol pada casis putih yang minimalis, ZenWiFi BD4 menampilkan jalur dwi 2.4GHz dan 5GHz untuk penstriman HD wayarles serentak yang tiada tandingan; pelayan SMB, pelayan UPnP AV, dan pelayan FTP untuk perkongsian fail 24/7; keupayaan untuk mengendalikan 300,000 sesi; dan Teknologi Rangkaian Hijau ASUS, yang menyediakan sehingga 70% penyelesaian penjimatan kuasa.

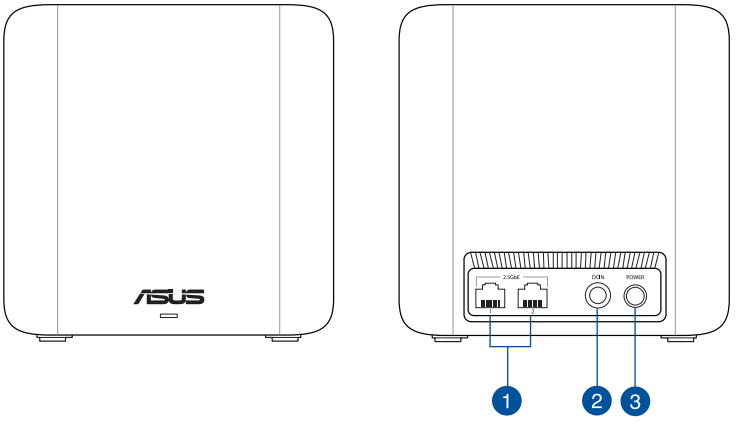
1.2 Kandungan pakej

- ☑ Penghala wayarles ZenWiFi BD4
- ☑ Penyesuai kuasa
- ☑ Kad waranti
- ☑ Kabel rangkaian (RJ-45)
- ☑ Panduan Mula Pantas

NOTA:

- Jika mana-mana daripada item ini rosak atau tiada, hubungi ASUS untuk membuat pertanyaan teknikal dan sokongan. Rujuk **Perkhidmatan dan Sokongan** di bahagian belakang manual pengguna ini.
- Simpan bahan pembungkusan yang asal sekiranya anda inginkan perkhidmatan waranti pada masa hadapan seperti pembaikian atau penggantian.

1.3 Penghala wayarles anda



1	**Port 2.5GbE (Pengesanan auto WAN/LAN)** Sambung kabel rangkaian ke dalam port ini untuk membentuk sambungan 2.5GbE WAN/LAN.
2	**Port Kuasa (DCIN)** Masukkan adapter AC yang diletakkan bersama ke dalam port ini dan sambung penghala anda ke sumber kuasa.
3	**Butang kuasa** Tekan butang ini untuk menghidupkan atau mematikan sistem.

NOTA:

- Hanya guna adapter yang disertakan bersama pakej anda. Menggunakan adapter lain boleh merosa kkan peranti.
- **Spesifikasi:**

Adapter Kuasa DC	Output DC: +12V dengan arus maksimum 1.5A;		
Suhu Pengendalian	0~40°C	Penyimpanan	0~70°C
Kelembapan Operasi	50~90%	Penyimpanan	20~90%

1.4 Meletakkan penghala wayarles anda

Untuk mendapatkan prestasi rangkaian wayarles yang terbaik daripada penghala wayarles anda, ikuti saranan di bawah:

- Letakkan penghala wayarles di tengah-tengah rangkaian anda untuk liputan wayarles yang maksimum.
- Pastikan peranti berada jauh dari sekatan logam dan jauh dari cahaya matahari langsung.
- Pastikan peranti berada jauh dari peranti Wi-Fi 802.11g atau 20MHz sahaja, persisian komputer 2.4GHz, peranti Bluetooth, telefon tanpa kord, pengubah, motor tugas berat, lampu pendarfluor, ketuhar gelombang mikro, peti sejuk, dan peralatan industri lain untuk menghalang gangguan atau kehilangan isyarat.
- Sentiasa kemas kini ke perisian tegar yang terkini. Lawati laman web ASUS di **http://www.asus.com** untuk mendapatkan kemas kini perisian tegar yang terkini.

1.5 Keperluan Penyediaan

Untuk menyediakan rangkaian anda, anda perlukan satu atau dua komputer yang memenuhi keperluan sistem yang berikut:

- Port Ethernet RJ-45 (LAN)(10Base-T/100Base-TX/1000Base-TX)
- Keupayaan wayarles IEEE 802.11a/b/g/n/ac/ax
- Perkhidmatan TCP/IP yang terpasang
- Penyemak imbas Web seperti Microsoft Internet Explorer, Firefox, Safari, atau Google Chrome

NOTA:

- Jika komputer tidak mempunyai keupayaan wayarles terbina dalam, pasang penyesuai IEEE 802.11a/b/g/n/ac/ax WLAN pada komputer anda untuk menyambung kepada rangkaian.
- Dengan teknologi dwi jalur, penghala wayarles anda menyokong isyarat wayarles 2.4GHz dan 5GHz secara serentak. Ini membenarkan anda untuk melakukan aktiviti berkaitan Internet seperti melayari Interet atau membaca/menulis mesej e-mel menggunakan jalur 2.4GHz sementara secara serentak strim fail audio/video berdefinisi tinggi seperti filam atau muzik menggunakan jalur 5GHz.
- Beberapa peranti IEEE 802.11n yang anda ingin sambung ke rangkaian anda mungkin menyokong atau tidak menyokong jalur 5GHz. Rujuk manual peranti untuk spesifikasi.
- Kabel Ethernet RJ-45 yang digunakan untuk menyambungkan peranti rangkaian tidak boleh melebihi 100 meter.

PENTING!

- Sesetengah penyesuai wayarles mungkin menghadapi masalah penyambungan ke AP Wi-Fi 802.11ax.
- Jika anda mengalami masalah sedemikian, sila pastikan anda mengemas kini pemacu ke versi terkini. Semak laman sokongan rasmi pengeluar anda di mana pemacu perisian, kemas kini dan maklumat lain yang berkaitan boleh diperoleh.
    - Realtek: https://www.realtek.com/en/downloads
    - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi
    - Intel: https://downloadcenter.intel.com/

2 Bermula

2.1 Penyediaan Penghala

PENTING!

- Gunakan sambungan berwayar semasa menyediakan penghala wayarles anda untuk mengelakkan isu penyediaan wayarles yang mungkin berlaku.
- Sebelum menyediakan penghala wayarles ASUS anda, lakukan yang berikut:
  - Jika anda sedang menggantikan penghala yang sedia ada, tanggalkannya daripada rangkaian anda.
  - Putuskan sambungan kabel/wayar dari modem anda yang sedia ada. Jika modem anda mempunyai bateri sandaran, tanggalkannya juga.
  - But semua komputer anda (disarankan).

AMARAN!

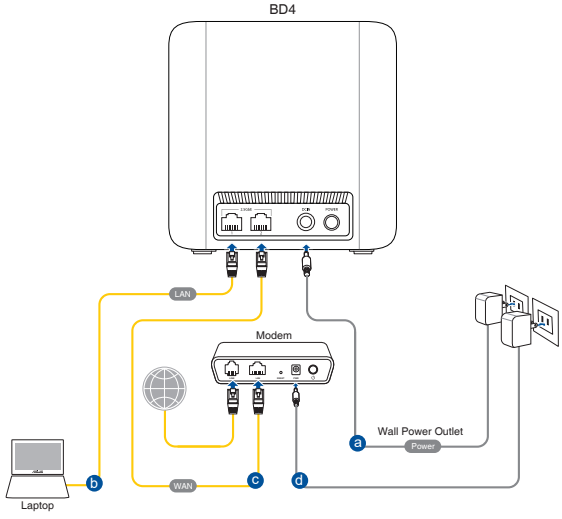
- Kord bekalan kuasa mesti dipalam masuk ke salur keluar soket yang disediakan dengan pembumian yang sesuai. Sambungkan peralatan hanya ke salur keluar soket berdekatan yang mudah diakses.
- Jika Penyesuai, jangan cuba untuk membetulkannya sendiri. Hubungi juruteknik servis bertauliah atau peruncit anda.
- JANGAN guna kord kuasa, aksesori atau persisian lain yang rosak.
- JANGAN pasang peralatan ini lebih tinggi daripada 2 meter.
- Dalam persekitaran dengan suhu ambien antara 0℃(32℉) dan 40℃(104℉).

A. Sambungan berwayar

NOTA: Penghala wayarles anda menyokong kedua-dua kabel tembus lalu atau silang atas semasa menyediakan sambungan berwayar.

Untuk menyediakan rangkaian menggunakan sambungan berwayar:

1. Pasang masuk penghala anda ke sumber kuasa dan hidupkan kuasanya. Sambungkan kabel rangkaian dari komputer anda ke port 2.5GbE pada penghala anda.

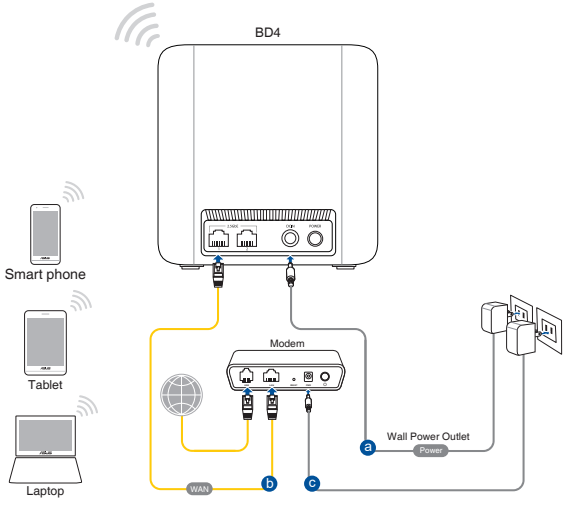


2. GUI web dilancarkan secara automatik apabila anda membuka pelayar web. Jika ia tidak melakukan pelancaran auto, masuki http://www.asusrouter.com.
3. Sediakan kata laluan untuk penghala anda bagi menghalang akses yang tidak dibenarkan.

B. Sambungan wayarles

Untuk menyediakan rangkaian menggunakan sambungan berwayar:

1. Pasang masuk penghala anda ke sumber kuasa dan hidupkan kuasanya.



2. Sambung ke nama rangkaian (SSID) yang ditunjukkan pada label produk di bahagian belakang penghala. Untuk keselamatan rangkaian yang lebih baik, ubah ke SSID unik dan berikan kata laluan.

Nama Wi-Fi (SSID):	ASUS_XX

* **XX** merujuk pada dua digit terakhir alamat MAC 2.4GHz. Anda boleh menemuinya pada label di belakang penghala anda.

3. GUI web dilancarkan secara automatik apabila anda membuka pelayar web. Jika ia tidak melakukan pelancaran auto, masuki http://www.asusrouter.com.
4. Sediakan kata laluan untuk penghala anda bagi menghalang akses yang tidak dibenarkan.

NOTA:

- Untuk mendapatkan butiran mengenai menyambung kepada rangkaian wayarles, rujuk manual pengguna penyesuai WLAN.
- Untuk menyediakan tetapan keselamatan untuk rangkaian anda, rujuk seksyen **3.1.1 Menyediakan keselamatan wayarles**.

2.2 Persediaan Internet Cepat (QIS) dengan pengesanan auto

Ciri Persediaan Internet Cepat (QIS) membimbing anda untuk menyediakan sambungan Internet anda dengan cepat.

NOTA: Semasa menetapkan sambungan Internet buat pertam kali, tekan butang Tetap semula pada penghala wayarles anda untuk menetapkannya ke tetapan lalai kilang.

Untuk menggunakan QIS dengan pengesanan cepat:

1. Lancarkan penyemak imbas web. Anda akan dihalakan semula ke Wizard Penyediaan ASUS (Penyediaan Internet Pantas). Jika tidak, masukkan http://www.asusrouter.com secara manual.
2. Penghala wayarles secara automatik mengesan jika jenis sambungan ISP anda adalah **Dynamic IP (IP Dinamik)**, **PPPoE**, **PPTP**, dan **L2TP**. Masukkan maklumat yang diperlukan untuk jenis sambungan ISP anda.

PENTING! Dapatkan maklumat yang diperlukan dari ISP anda mengenai jenis sambungan Internet.

NOTA:

- Auto-pengesanan jenis sambungan ISP anda berlaku apabila anda mengkonfigurasi penghala wayarles buat kali pertama atau apabila penghala wayarles anda ditetapkan kepada tetapan lalainya.
- Jika QIS gagal untuk mengesan jenis sambungan Internet anda, klik **Skip to manual setting** dan konfigurasi tetapan sambungan anda secara manual.

3. Berikan nama rangkaian (SSID) dan kunci keselamatan untuk sambungan wayarles rangkaian WiFi 7 anda. Klik **Apply (Guna)** setelah selesai.
4. Pada halaman **Login Information Setup (Penyediaan Maklumat Log Masuk)**, ubah kata laluan log masuk penghala untuk menghalang akses tanpa kebenaran ke penghala wayarles anda.

NOTA: Nama pengguna dan kata laluan log masuk adalah berbeza daripada nama rangkaian (SSID) WiFi 7 dan kunci keselamatan. Nama pengguna dan kata laluan log masuk penghala wayarles membolehkan anda untuk log masuk ke GUI Web penghala wayarles anda untuk mengkonfigurasikan tetapan penghala wayarles. Nama rangkaian (SSID) WiFi 7 dan kunci keselamatan membolehkan peranti Wi-Fi log masuk dan bersambung ke rangkaian WiFi 7.

2.3 Menyambung ke rangkaian wayarles anda

Selepas menyediakan penghala wayarles anda melaui QIS, anda boleh menyambungkan komputer anda atau peranti pintar lain ke rangkaian wayarles anda.

Untuk menyambung kepada rangkaian anda:

1. Pada komputer anda, klik ikon rangkaian dalam kawasan pemberitahuan untuk memaparkan rangkaian wayarles tersedia.
2. Pilih rangkaian wayarles yang anda ingin bersambung dengan, kemudian klik **Connect (Sambung)**.
3. Anda mungkin perlu memasukkan kunci keselamatan rangkaian untuk rangkaian wayarles yang selamat, kemudian klik **OK (OK)**.
4. Tunggu sementara komputer anda berjaya membentuk sambungan ke rangkaian wayarles. Status sambungan dipaparkan dan ikon rangkaian memaparkan status yang telah bersambung.

NOTA:

- Rujuk bab seterusnya untuk butiran lanjut mengenai mengkonfigurasi tetapan rangkaian wayarles anda.
- Rujuk manual pengguna peranti anda untuk butiran lanjut mengenai menyambungkannya ke rangkaian wayarles anda.

3 Mengkonfigurasi Tetapan Am dan Lanjutan

3.1 Melog masuk ke GUI web

Penghala Wayarles ASUS anda disertakan dengan antara muka pengguna grafik (GUI) web intuitif yang membolehkan anda mudah mengkonfigurasikan pelbagai cirinya menerusi pelayar web seperti Internet Explorer, Firefox, Safari atau Google Chrome.

NOTA: Ciri mungkin berbeza dengan versi perisian tegar berbeza.

Untuk log masuk ke GUI web:

1. Di penyemak imbas web anda, masukkan alamat IP lalai penghala wayarles secara manual: http://www.asusrouter.com.
2. Pada halaman log masuk, masukkan nama pengguna dan kata laluan yang telah anda tetapkan dalam **2.2 Penyediaan Internet Pantas (QIS) dengan Pengesanan Auto**.
3. Anda sekarang boleh menggunaka GUI Web untuk mengkonfigurasikan pelbagai tetapan Penghala Wayarles ASUS anda.

* Imej adalah untuk rujukan sahaja.

NOTA: Jika anda melog masuk ke dalam GUI Web buat pertama kali, anda akan diarahkan ke halaman Penyediaan Internet Pantas (QIS) secara automatik.

3.1.1 Menyediakan keselamatan wayarles

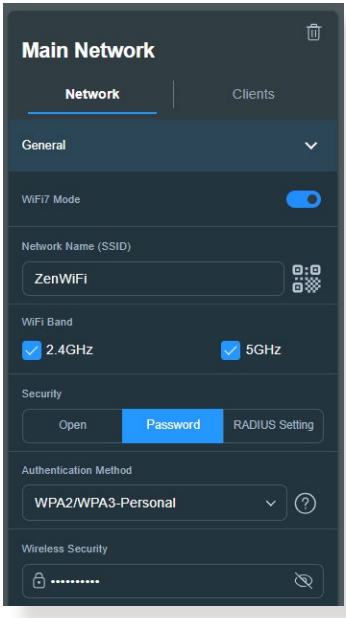
Untuk melindungi rangkaian wayarles anda daripada akses yang tidak dibenarkan, anda perlu mengkonfigurasi tetapan keselamatan penghala anda.

Untuk menyediakan tetapan keselamatan wayarles:

1. Daripada panel navigasi, pergi ke **General (Am)** > **Network Map (Peta Rangkaian)**.
2. Pilih rangkaian dan anda boleh mengkonfigurasikan tetapan keselamatan wayarles seperti SSID, tahap keselamatan, dan tetapan penyulitan.

NOTA: Anda boleh menyediakan beberapa tetapan keselamatan wayarles untuk jalur 2.4GHz dan 5GHz.

Tetapan keselamatan 2.4GHz/5GHz



3. Pada medan **Network Name (SSID) (Nama Rangkaian (SSID))**, masukkan nama unik bagi rangkaian wayarles anda.

4. Dari senarai jatuh bawah **WEP Encryption (Penyulitan WEP)**, pilih kaedah penyulitan untuk rangkaian wayarles anda.

PENTING! IEEE 802.11n/ac/ax standard melarang menggunakan High Throughput (Truhput Tinggi) dengan WEP atau WPA-TKIP sebagai sifer unisiar. Jika anda menggunakan kaedah penyulitan ini, kadar data anda akan merosot kepada sambungan IEEE 802.11g 54Mbps.

5. Masukkan kunci laluan keselamatan anda.
6. Klik **Apply (Guna)** setelah selesai.

3.1.2 Menguruskan klien rangkaian anda

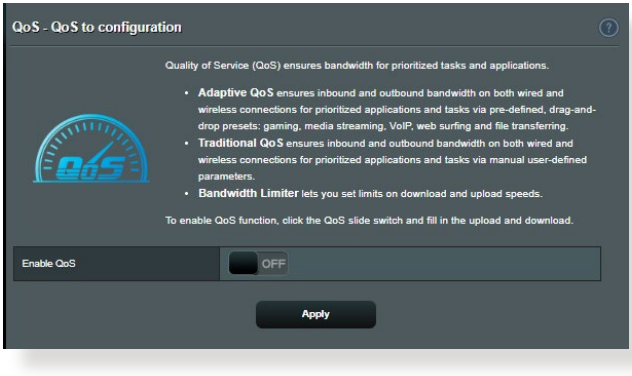
Untuk menguruskan klien rangkaian anda:

1. Daripada panel navigasi, pergi ke **General (Am)** > **Network Map (Peta Rangkaian)**
2. Pada skrin Peta Rangkaian, pilih ikon **Client status (Status Klien)** untuk memaparkan maklumat rangkaian klien anda.
3. Untuk menyekat akses klien ke rangkaian anda, pilih klien dan klik **block (sekat)**.

3.2 Mudah Suai QoS

3.2.1 Menguruskan Jalur Lebar QoS (Kualiti Perkhidmatan)

Ciri Quality of Service (Perkhidmatan Kualiti) membolehkan anda untuk menetapkan keutamaan jalur lebar dan menguruskan trafik rangkaian.



Untuk menyediakan keutamaan lebar jalur:

1. Daripada panel navigasi, pergi ke **General (Am)** > **Adaptive QoS (Mudah Suai QoS)** > **QoS**.
2. Klik **ON (HIDUP)** untuk mendayakan QoS. Isi medan lebar jalur muat naik dan muat turun.

NOTA: Maklumat jalur lebar anda tersedia dari ISP anda.

3. Klik **Apply (Guna)**.

NOTA: Senarai Peraturan Penentuan Pengguna adalah untuk tetapan lanjutan. Jika anda ingin mengutamakan aplikasi rangkaian khusus dan perkhidmatan rangkaian, pilih **User-defined QoS rules (Peraturan QoS bertakrif pengguna)** atau **User-defined Priority (Keutamaan Bertakrif pengguna)** dari senarai jatuh turun di sudut atas sebelah kanan.

4. Pada halaman **user-defined QoS rules (peraturan QoS bertakrif pengguna)**, terdapat empat jenis perkhidmatan dalam talian lalai – layar web, HTTPS dan pemindahan fail. Pilih perkhidmatan yang anda ingini, isi **Source IP or MAC (Sumber IP atau MAC)**, **Destination Port (Port Destinasi)**, **Protocol (Protokol)**, **Transferred (Dipindahkan)** dan **Priority (Keutamaan)**, kemudian klik **Apply (Guna)**. Makluma akan dikonfigurasikan dalam skrin peraturan QoS.

NOTA:

- Untuk mengisi sumber IP atau MAC, anda boleh:

  a) Masukkan alamat IP khusus, seperti "192.168.122.1".

  b) Masukkan alamat IP di dalam satu subnet atau di dalam himpunan IP seperti "192.168.123.*", atau "192.168.*.*"

  c) Masukkan alamat IP seperti "*.*.*.*" atau biarkan medan kosong.

  d) Format untuk alamat MAC adalah enam kumpulan bagi dua digit perenambelasan, diasingkan dengan tanda titik bertindih (:), dalam turutan penghantaran (cth. 12:34:56:aa:bc:ef)

- Untuk sumber atau destinasi julat port, anda boleh :

  a) Masukkan port khusus, seperti "95".

  b) Masukkan port di dalam julat, seperti "103:315", ">100", atau "<65535".

- Lajur **Transferred (Dipindahkan)** mengandungi maklumay mengenai trafik huluan dan hiliran (trafik rangkaian keluar dan masuk) untuk satu bahagian. Dalam lajur ini, anda boleh menetapkan had trafik rangkaian (dalam KB) untuk perkhidmatan tertentu bagi menjanakan keutamaan tertentu untuk perkhidmatan diuntukkan pada port tertentu. Sebagai contoh, jika dua klien rangkaian, PC 1 dan PC 2, kedua-dua mengakses Internet (ditetapkan di port 80), tetapi PC 1 melebihi had trafik rangkaian disebabkan oleh beberapa tugasan memuat turun, PC 1 akan mempunyai keutamaan lebih rendah. Jika anda tidak mahu menetapkan had trafik, biarkannya kosong.

5. Pada halaman**User-defined Priority (Keutamaan Bertakrif pengguna)**, anda boleh mngutamakan aplikasi rangkaian atau peranti ke dalam lima bahagian daripada senarai jatuh bawah **user-defined QoS rules (Peraturan QoS bertakrif pengguna)**. Berdasarkan tahap keutamaan, anda boleh menggunakan kaedah berikut dalam menghantar paket data:
   - Menukar susunan paket rangkaian huluan yang dihantar ke Internet.
   - Di bawah jadual **Upload Bandwidth (Muat Naik Lebar Jalur)**, tetapkan **Minimum Reserved Bandwidth (Lebar Jalur Disimpan Minimum)** dan **Maximum Bandwidth Limit (Had Lebar Jalur Maksimum)** untuk aplikasi rangkaian berbilang dengan tahap keutamaan berbeza. Peratusan menunjukkan julat lebar jalur muat naik yang tersedia untuk aplikasi rangkaian yang dinyatakan.

NOTA:

- Paket keutamaan rendah diabaikan untuk memastikan penghantaran paket keutamaan tinggi.
- Di bawah jadual **Download Bandwidth (Lebar Jalur Muat Turun)**, tetapkan **Maximum Bandwidth Limit (Had Lebar Jalur Maksimum)** untuk aplikasi rangkaian berbilang dalam susunan berkaitan. Paket huluan keutamaan lebih tinggi akan mengakibatkan paket hiliran keutamaan lebih tinggi.
- Jika tiada paket dihantar daripada aplikasi keutamaan tinggi, kadar penghantaran penuh bagi sambungan Internet adalah tersedia untuk paket keutamaan rendah.

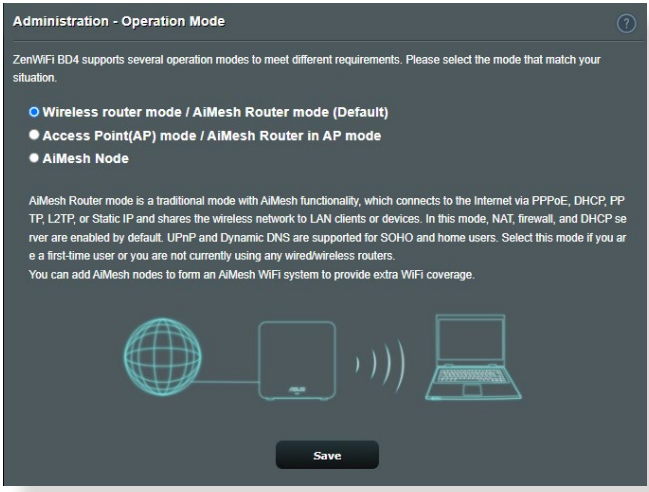
6. Tetapkan paket keutamaan tertinggi. Untuk memastikan pengalaman permainan dalam talian yang lancar, anda boleh menetapkan ACK, SYN, danICMP sebagai paket keutamaan tertinggi.

NOTA: Pastikan untuk mendayakan QoS dahulu dan menyediakan had julat muat naik dan muat turun.

3.3 Pentadbiran

3.3.1 Mod Operasi

Halaman Mod Operasi membolehkan anda memilih mod bersesuaian untuk rangkaian anda.



Untuk menyediakan mod operasi:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Administration (Pentadbiran)** > **Operation Mode (Mod Operasi)**.
2. Pilih mana-mana mod operasi ini:
   - **Mod penghala wayarles (lalai)**: Dalam mod penghala wayarles, penghala wayarles menyambung ka Intternet dan menyediakan akses Internet ke peranti tersedia pada rangkaian setempat sendiri.
   - **Access Point mode (Mod Titik Akses)**: Dalam mod ini, penghalan mencipta rangkaian wayarles baru pada rangkaian sedia ada.
   - **Nod AiMesh:** Anda boleh menetapkan ZenWiFi BD4 sebagai nod AiMesh untuk meluaskan liputan WiFi penghala AiMesh sedia ada.
3. Klik **Save (Simpan)**.

NOTA: Penghalan ini akan but semula bila anda menukar mod.

3.3.2 Sistem

Halaman **System (Sistem)** membolehkan anda mengkonfigurasikan tetapan penghala anda.

Untuk menyediakan tetapan Sistem:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Administration (Pentadbiran)** > **System (Sistem)**.
2. Anda boleh mengkonfigurasi tetapan berikut:
   - **Ubah kata laluan log masuk penghala**: Anda boleh menukar kata laluan dan nama log masuk penghala wayarles dengan memasukkan nama dan kata laluan baru.
   - **Kelakuan butang WPS**: Butang fizikal WPS pada penghala wayarles boleh digunakan untuk mengaktifkan WPS.
   - **Zon Masa**: Pilih zon masa rangkaian anda.
   - **Pelayan NTP**: Penghala wayarles boleh mengakses pelayan NTP (Protokol Masa Rangkaian) untuk menyegerakkan masa.
   - **Dayakan Telnet**: Klik **Yes (Ya)** untuk mendayakan perkhidmatan Telnet pada rangkaian. Klik **No (Tidak)** untuk menyahdayakan Telnet.
   - **Kaedah Pengesahan**: Anda boleh memilih HTTP, HTTPS, atau kedua-dua protokol untuk menjamin akses penghala.
   - **Dayakan Akses Web daripada WAN**: Pilih **Yes (Ya)** untuk membolehkan peranti di luar rangkaian untuk mengakses tetapan GUI penghala wayarles. Pilih **No (Tidak)** untuk menghalang akses.
   - **Hanya benarkan IP tertentu**: Klik **Yes (Ya)** jika anda ingin menentukan alamat IP peranti yang dibenarkan mengakses tetapan GUI penghala wayarles daripada WAN.
3. Klik **Apply (Guna)**.

3.3.3 Menatarkan perisian tegar

NOTA: Muat turun perisian tegar terkini dari laman web ASUS di http://www.asus.com.

Untuk menatarkan perisian tegar:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Administration (Pentadbiran)** > **Firmware Upgrade (Naik Taraf Perisian Tegar)**.
2. Dalam item **Firmware Version (Versi Perisian Tegar)**, klik **Check (Periksa)**. Navigasi ke fail perisian tegar yang dimuat turun.
3. Klik **Upload (Muat naik)**.

NOTA:

- Apabila proses naik taraf selesai, tunggu seketika untuk sistem but semula.
- Jika proses penataran gagal, penghala wayarles secara automatik memasuki mod menyelamat dan penunjuk kuasa LED di panel depan mula berkelip-kelip secara perlahan. Untuk mendapatkan semula atau memulihkan sistem, gunakan utiliti **4.2 Firmware Restoration (Pemulihan Perisian Tegar)**.

3.3.4 Tetapan Pemulihan/Penyimpanan/Memuat Naik

Untuk memulihkan/menyimpan/memuat naik tetapan penghala wayarles:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Administration (Pentadbiran)** > **Restore/Save/Upload Setting (Tetapan Pemulihan/Simpan/Muat Naik)**.
2. Pilih tugasan yang anda ingin lakukan:
   - Untuk memulihkan tetapan kilang lalai, klik **Restore (Pulihkan)**, dan klik **OK** apabila diminta.
   - Untuk menyimpan tetapan sistem semasa, klik **Save setting (Simpan seting)**, navigasi ke folder di mana anda berhasrat untuk menyimpan fail dan klik **Save (Simpan)**.
   - Untuk memulihkan fail tetapan sistem yang disimpan, klik **Upload (Muat naik)** untuk mencari fail anda, kemudian klik **Open (Buka)**.

PENTING! Jika isu berlaku, muat naik versi perisian tegar terkini dan konfigurasi tetapan baru. Jangan pulihkan penghalan ke tetapan lalai.

3.4 AiProtection

AiProtection menyediakan pemantauan masa nyata yang mengesan perisian hasad, perisian pengintip dan akses tidak dikehendaki. Ia juga menapis laman web dan aplikasi yang tidak dikehendaki serta membolehkan anda menjadualkan masa supaya peranti yang bersambung dapat mengakses Internet.

3.4.1 Perlindungan Rangkaian

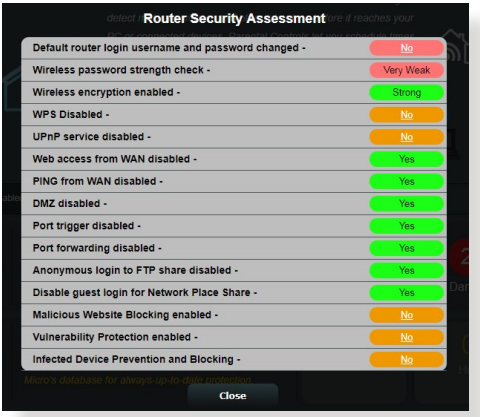
Perlindungan Rangkaian menghalang rangkaian daripada mengeksploitasi dan menjamin keselamatan rangkaian anda daripada akses yang tidak dikehendaki.

Mengkonfigurasi Perlindungan Rangkaian

Untuk mengkonfigurasi Perlindungan Rangkaian:

1. Dari panel navigasi, pergi ke **General (Am)** > **AiProtection**
2. Dari halaman utama **AiProtection**, klik pada **Network Protection (Perlindungan Rangkaian)**.
3. Dari tab **Network Protection (Perlindungan Rangkaian)**, klik **Scan (Imbas)**.

   Apabila selesai mengimbas, utiliti memaparkan hasil pada halaman **Router Security Assessment (Penilaian Keselamatan Penghala)**.



PENTING! Item yang ditandakan sebagai **Yes (Ya)** pada halaman **Router Security Assessment (Penilaian Keselamatan Penghala)** dianggap berada pada status **safe (selamat)**. Item ditandakan sebagai **No (Tidak)**, **Weak (Lemah)**, atau **Very Weak (Sangat Lemah)** amat disyorkan untuk dikonfigurasikan sewajarnya.

4. (Pilihan) Dari halaman **Router Security Assessment (Penilaian Keselamatan Penghala)**, secara manual konfigurasi item ditandakan sebagai **No (Tidak)**, **Weak (Lemah)** atau **Very Weak (Sangat Lemah)**. Untuk melakukan ini:

   a. Klik item.

NOTA: Apabila anda mengklik item, utiliti memajukan anda ke halaman tetapan item.

   b. Dari halaman tetapan keselamatan item, konfigurasi dan buat perubahan yang perlu kemudian klik **Apply (Guna)** apabila selesai.

c. Kembali ke halaman **Router Security Assessment (Penilaian Keselamatan Penghala)** dan klik **Close (Tutup)** untuk keluar halaman.

5. Untuk mengkonfigurasi tetapan keselamatan secara automatik, klik **Secure Your Router (Jamin Keselamatan Penghala Anda).**
6. Apabila gesaan mesej muncul, klik **OK**.

Pemblokan Tapak Hasad

Ciri ini mengehadkan akses ke laman web hasad dalam pangkalan data awan untuk perlindungan terkini setiap masa.

NOTA: Fungsi ini didayakan secara automatik jika anda menjalankan **Router Weakness Scan (Imbasan Kelemahan Penghala)**.

Untuk mendayakan Sekatan Laman Hasad:

1. Dari panel navigasi, pergi ke **General (Am)** > **AiProtection**
2. Dari halaman utama **AiProtection**, klik pada **Network Protection (Perlindungan Rangkaian)**.
3. Dari anak tetingkap **Malicious Sites Blocking (Sekatan Laman Hasad)**, klik **ON (HIDUP)**.

IPS Dua Hala

IPS Dua Hala (Sistem Pencegahan Pencerobohan) melindungi penghala anda daripada serangan rangkaian dengan menyekat paket masuk yang berniat jahat dan mengesan paket keluar yang mencurigakan.

NOTA: Fungsi ini didayakan secara automatik jika anda menjalankan **Router Weakness Scan (Imbasan Kelemahan Penghala)**.

Untuk mendayakan perlindungan Kerentanan:

1. Dari panel navigasi, pergi ke **General (Am)** > **AiProtection**
2. Dari halaman utama **AiProtection**, klik pada **Network Protection (Perlindungan Rangkaian)**.
3. Dari anak tetingkap **Two-Way IPS (IPS Dua Hala)**, klik **ON (HIDUP)**.

Pencegahan Peranti Terjangkit dan Halangan

Ciri ini menghalang peranti terjangkit daripada menyampaikan maklumat peribadi atau status terjangkit kepada pihak luaran.

NOTA: Fungsi ini didayakan secara automatik jika anda menjalankan **Router Weakness Scan (Imbasan Kelemahan Penghala)**.

Untuk mendayakan perlindungan Kerentanan:

1. Dari panel navigasi, pergi ke **General (Am)** > **AiProtection**
2. Dari halaman utama **AiProtection**, klik pada **Network Protection (Perlindungan Rangkaian)**.
3. Dari anak tetingkap **Infected Device Prevention and Blocking (Pencegahan Peranti Terjangkit dan Halangan)**, klik **ON (HIDUP)**.

Untuk mengkonfigurasi Keutamaan Peringatan:

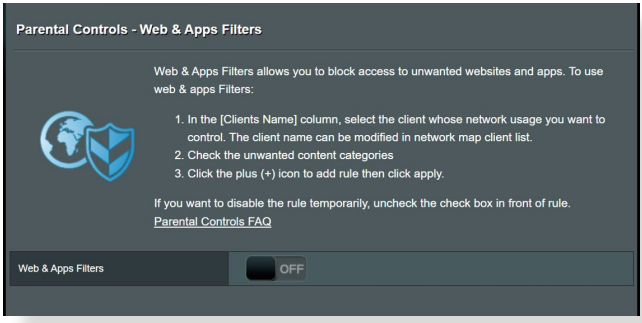
1. Dari anak tetingkap **Infected Device Prevention and Blocking (Pencegahan Peranti Terjangkit dan Halangan)**, klik **Alert Preference (Keutamaan Peringatan)**.
2. Pilih atau masukkan pembekal e-mel, akaun e-mel dan kata laluan, kemudian klik **Apply (Guna)**.

3.4.2 Menyediakan Kawalan Ibu Bapa

Kawalan Ibu Bapa membolehkan anda mengawal masa akses Internet atau menetapkan had masa untuk penggunaan rangkaian klien.

Untuk pergi ke halaman utama Kawalan Ibu Bapa:

Dari panel navigasi, pergi ke **General (Am)** > **Parental Controls (Kawalan Ibu Bapa)**.



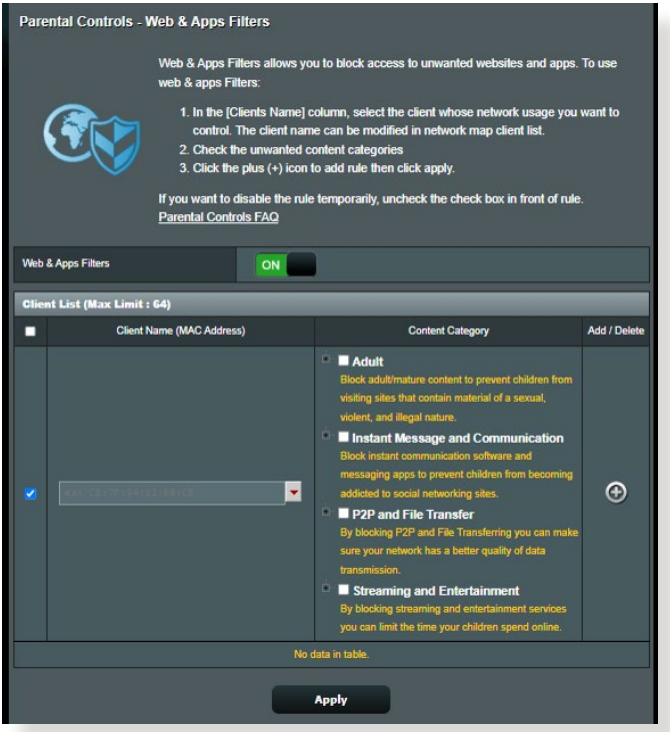
Penapis Web & Aplikasi

Penapis Web & Aplikasi ialah ciri **Parental Controls (Kawalan Ibu Bapa)** yang membolehkan anda menyekat akses ke laman web atau aplikasi yang tidak dikehendaki.

Untuk mengkonfigurasi Penapis Web & Aplikasi:

1. Dari panel navigasi, pergi ke **General (Am)** > **Parental Controls (Kawalan Ibu Bapa)**.
2. Dari anak tetingkap **Web & Apps Filters (Penapis Web & Aplikasi)**, klik **ON (HIDUP)**.
3. Apabila gesaan mesej Perjanjian Lesen Pengguna Akhir (EULA) muncul, klik **I agree (Saya setuju)** untuk teruskan.
4. Dari lajur **Client List (Senarai Klien)** , pilih atau masukkan nama klien daripada kotak senarai juntai bawah.
5. Dari lajur **Content Category (Kategori Kandungan)** , pilih penapis daripada empat kategori utama: **Dewasa, Mesej Segera dan Komunikasi, P2P dan Pemindahan Fail** dan **Penstriman dan Hiburan**.

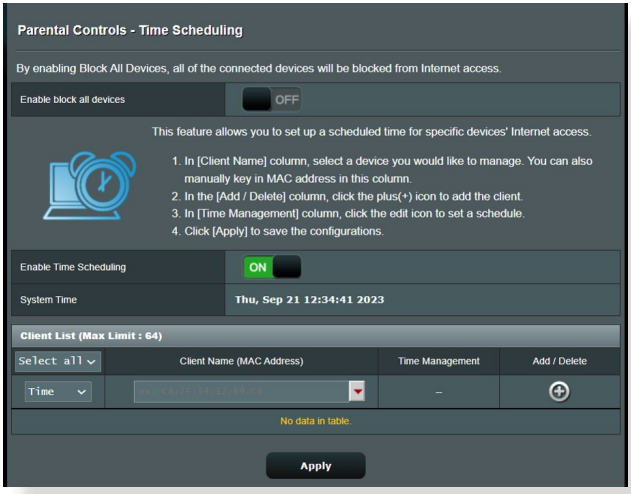
6. Klik untuk menambah profil klien.
7. Klik **Apply (Guna)** untuk menyimpan tetapan.



Penjadualan Waktu

Penjadualan Waktu membolehkan anda menetapkan had masa untuk penggunaan rangkaian klien.

NOTA: Pastikan bahawa waktu sistem anda disegerakkan dengan pelayan NTP.



Untuk mengkonfigurasikan Penjadualan Waktu:

1. Dari panel navigasi, pergi ke **General (Am)** > **Parental Controls (Kawalan Ibu Bapa)** > **Time Scheduling (Penjadualan Waktu)**.
2. Dari anak tetingkap **Enable Time Scheduling (Dayakan Penjadualan Waktu)**, klik **ON (HIDUP)**.
3. Dari lajur **Clients Name (Nama Klien)**, pilih atau masukkan nama klien daripada kotak senarai juntai bawah.

NOTA: Anda juga boleh memasukkan alamat MAC klien dalam lajur **Client MAC Address (Alamat MAC Klien)**. Pastikan bahawa nama klien tidak mengandungi aksara khas atau ruang kerana ini boleh menyebabkan penghala berfungsi secara tidak normal.

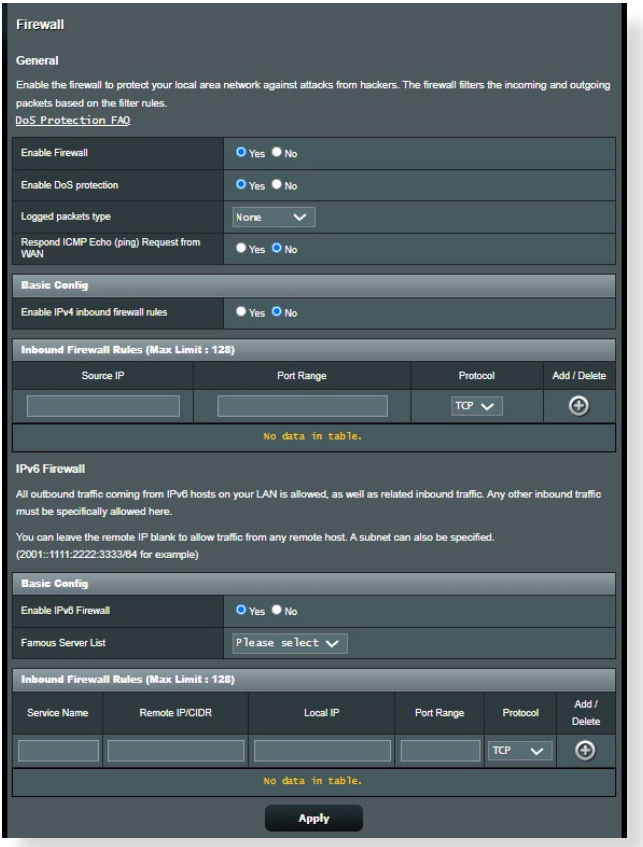
4. Klik untuk menambah profil klien.
5. Klik **Apply (Guna)** untuk menyimpan tetapan.

3.5 Tembok Api

Penghala wayarles boleh menjadi tembok api perkakas untuk rangkaian anda.

NOTA: Ciri Tembok Api didayakan secara lalai.

3.5.1 Umum



Untuk menyediakan tetapan Tembok Api asas:

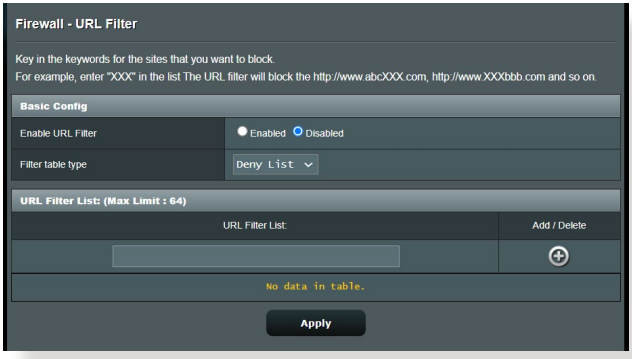
1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Firewall (Tembok Api)** > **General (Am)**.
2. Pada medan **Enable Firewall (Dayakan Tembok Api)**, pilih **Yes (Ya).**

3. Pada perlindungan **Enable DoS (Dayakan DoS)**, pilih **Yes (Ya)** untuk melindungi rangkaian anda daripada serangan DoS (Nafi Khidmat) walaupun ini mungkin menjejaskan prestasi penghala anda.
4. Anda juga boleh memantau pertukaran paket antara sambungan LAN dan WAN. Pada Jenis paket yang dilog, pilih **Dropped (Digugurkan)**, **Accepted (Diterima)**, atau **Both (Kedua-duanya)**.
5. Klik **Apply (Guna)**.

3.5.2 Penapis URL

Anda boleh menentukan kata kerja atau alamat web untuk mengelakkan akses ke URL tertentu.

NOTA: Penapis URL adalah berdasarkan pertanyaan DNS. Jika klien rangkaian telah mengakses tapak web seperti http://www.abcxxx.com, maka tapak web tidak akan disekat (cache DNS dakan sistem menyimpan tapak web yang dilawati sebelum ini). Untuk menyelesaikan isu ini, kososngkan cache DNS sebelum menyediakan Penapis URL.

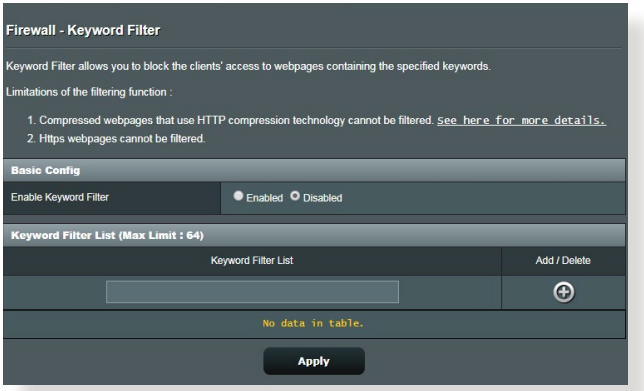


Untuk menyediakan penapis URL:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Firewall (Tembok Api)** > **URL Filter (Penapis URL)**.
2. Pada medan Dayakan Penapis URL, pilih **Enabled (Didayakan)**.
3. Masukkan URL dan klik butang .
4. Klik **Apply (Guna)**.

3.5.3 Penapis kata kunci

Penapis kata kunci menyekat akses ke laman web mengandungi kata kunci yang dinyatakan.



Untuk menyediakan penapis kata kunci:

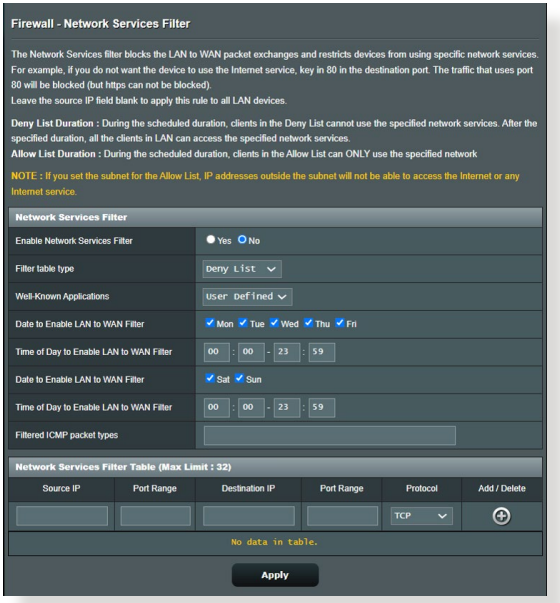
1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Firewall (Tembok Api)** > **Keyword Filter (Penapis Kata Kunci)**.
2. Pada medan Dayakan Penapis Kata Kunci, pilih **Enabled (Didayakan)**.
3. Masukkan perkataan atau frasa dan klik butang **Add (Tambah)**.
4. Klik **Apply (Guna)**.

NOTA:

- Penapis Kata Kunci adalah berdasarkan pertanyaan DNS. Jika klien rangkaian telah mengakses tapak web seperti http://www.abcxxx.com, maka tapak web tidak akan disekat (cache DNS dakan sistem menyimpan tapak web yang dilawati sebelum ini). Untuk menyelesaikan isu ini, kososngkan cache DNS sebelum menyediakan Penapis Kata Kunci.
- Laman web termampat menggunakan pemampatan HTTP tidak boleh ditapis. Halaman HTTPS juga tidak boleh disekat menggunakan penapis kata kunci.

3.5.4 Penapis Perkhidmatan Rangkaian

Penapis Perkhidmatan Rangkaian menyekat pertukaran paket LAN ke WAN dan mengehadkan klien rangkaian daripada mengakses perkhidmatan web khusus seperti Telnet atau FTP.

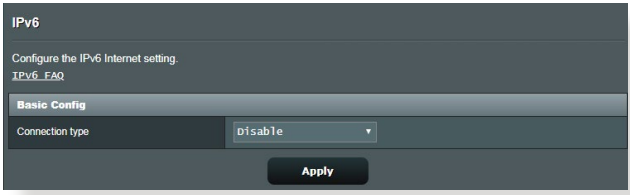


Untuk menyediakan penapis Perkhidmatan Rangkaian:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Firewall (Tembok Api)** > **Network Service Filter (Penapis Perkhidmatan Rangkaian**.
2. Pada medan Dayakan Penapis Perkhidmatan Rangkaian, pilih **Yes (Ya)**.
3. Pilih jenis jadual Penapis. **Deny (Tolak)** menyekat perkhidmatan rangkaian yang ditentukan. **Allow (Benarkan)** mengehadkan akses hanya ke perkhidmatan rangkaian yang ditentukan.
4. Nyatakan hari dan masa apabila penapis akan diaktifkan.
5. Untuk menentukan Perkhidmatan Rangkaian untuk menapis, masukkan IP Sumber, IP Destinasi, Liputan Port, dan Protokol. Klik butang .
6. Klik **Apply (Guna)**.

3.6 IPv6

Penghala wayarles ini menyokong pengalamatan IPv6, sistem yang menyokong lebih alamat IP. Standard ini belum lagi tersedia secara meluas. Hubungi ISP anda jika perkhidmatan Internet anda menyokong IPv6.



Untuk menyediakan IPv6:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **IPv6**.
2. Pilih **Connection type (Jenis sambungan)** anda. Pilih konfigurasi berbeza bergantung pada jenis sambungan terpilih anda.
3. Masukkan tetapan IPv6 LAN dan DNS anda.
4. Klik **Apply (Guna)**.

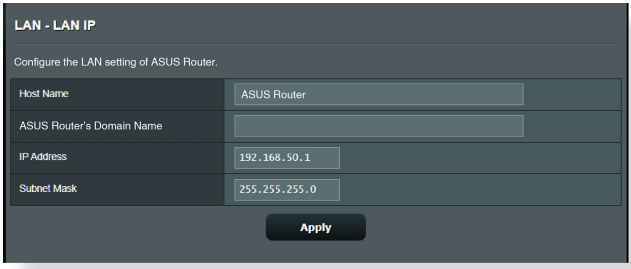
NOTA: Sila rujuk ISP anda berkenaan maklumat khusus IPv6 untuk perkhidmatan Internet anda.

3.7 LAN

3.7.1 IP LAN

Skrin IP LAN membolehkan anda mengubah suai tetapan IP LAN penghala wayarles anda.

NOTA: Apa-apa perubahan kepada alamat IP LAN akan ditunjukkan pada tetapan DHCP anda.

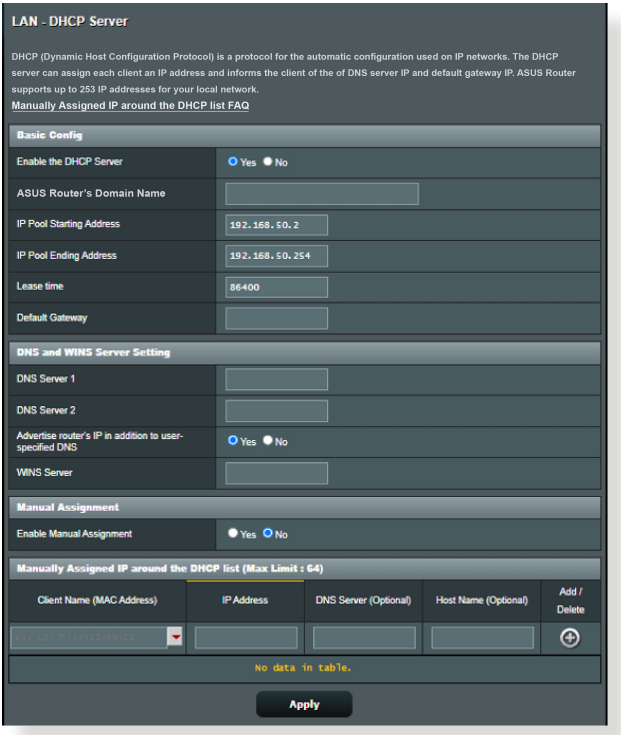


Untuk mengubah suai tetapan IP LAN:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **LAN** > **IP LAN**.
2. mengubah suai **IP address (alamat IP)** dan **Subnet Mask**.
3. Apabila selesai, klik **Apply (Guna)**.

3.7.2 Pelayan DHCP

Penghala wayarles anda menggunakan DHCP untuk menguntukkan alamat IP secara automaik pada rangkaian anda. Anda boleh menyatakan julat alamat IP dan masa pajakan untuk kelian pada rangkaian anda.



Untuk mengkonfigurasi pelayan DHCP:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **LAN** > **DHCP Server (Pelayan DHCP)**.
2. Dalam medan **Enable the DHCP Server (Dayakan Pelayan DHCP)**, tandakan **Yes (Ya)**.
3. Dalam kotak teks **Domain Name (Nama Domain)**, masukkan nama domain untuk penghala wayarles.
4. Dalam medan **IP Pool Starting Address (Alamat Permulaan Kumpulan IP)**, masukkan alamat IP permulaan.

5. Dalam medan **IP Pool Ending Address (Alamat Akhir Kumpulan IP)**, masukkan alamat IP akhir.
6. Dalam medan **Lease Time (Masa Pajakan)**, nyatakan dalam saat bila alamat IP yang diuntukkan akan tamat tempoh. Sebaik sahaja ia mencapai had masa ini, pelayan DHCP kemudiannya akan menguntukkan alamat IP yang baru.

NOTA:

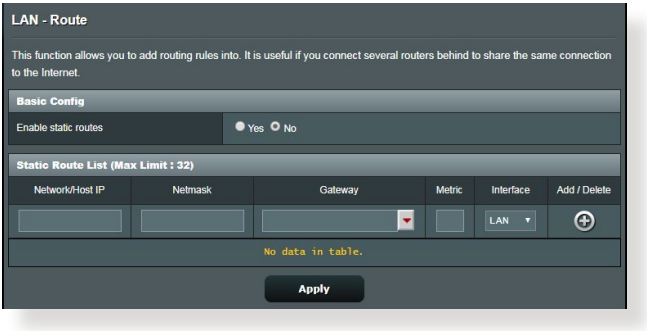
- ASUS menyarankan agar anda menggunakan format alamat IP 192.168.50.xxx (di mana xxx boleh jadi sebarang nombor antara 2 dan 254) apabila menyatakan julat alamat IP.
- IP Pool Starting Address (Alamat Permulaan Kumpulan IP) tidak boleh melebihi Alamat Akhir Kumpulan IP).

7. Dalam bahagian **DNS and WINS Server Settings (Tetapan DNS dan WINS Pelayan)**, masukkan alamat IP Pelayan DNS dan Pelayan WINS jika diperlukan.
8. Penghala wayarles ada juga boleh menugaskan alamat IP kepada peranti pada rangkaian secara manual. Pada medan **Enable Manual Assignment (Dayakan Tugasan Manual)**, pilih **Yes (Ya)** untuk menugaskan alamat IP ke alamat MAC khusus pada rangkaian. Sehingga 32 alamat MAC boleh ditambah pada senarai DHCP untuk penugasan manual.

3.7.3 Hala

Jika rangkaian anda menggunakan lebih daripada satu penghala wayarles, anda boleh mengkonfigurasikan jadual penghalaan untuk berkongsi perkhidmatan Internet yang sama.

NOTA: Kami mengesyorkan anda tidak menukar tetapan hala lalai melainkan anda mempunyai pengetahuan lanjutan mengenai jadual penghalaan.

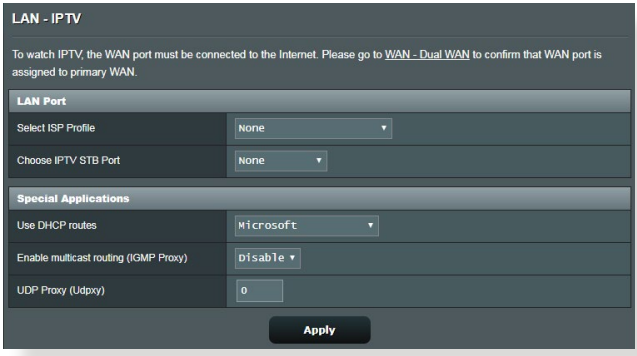


Untuk mengkonfigurasikan jadual Penghalaan LAN:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **LAN** > **Route (Hala)**.
2. Pada medan **Enable static route (Dayakan hala statik)**, pilih **Yes (Ya).**
3. Pada **Static Route List (Senarai Hala Statik)**, masukkan maklumat rangkaian titik akses atau nod lain. Klik butang **Add (Tambah)** atau **Delete (Padam)** untuk menambah atau membuang peranti pada senarai.
4. Klik **Apply (Guna)**.

3.7.4 IPTV

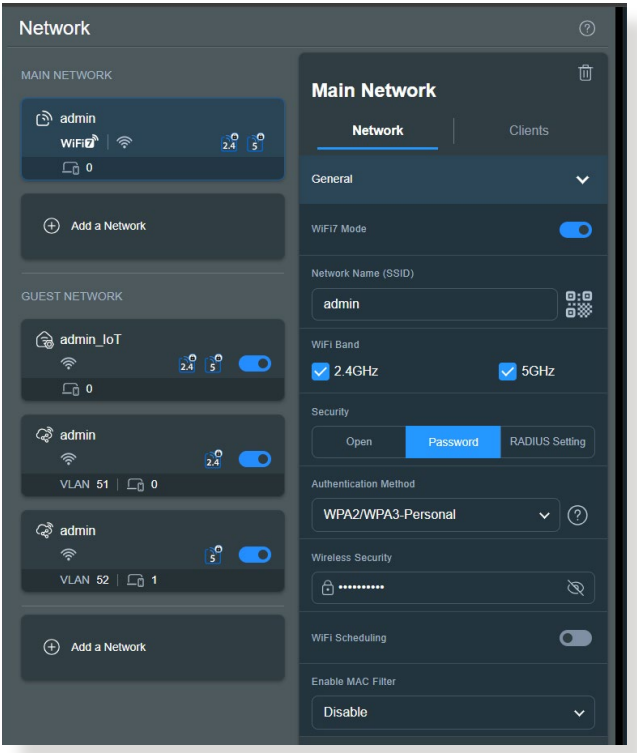
Penghala wayarles menyokong sambungan ke perkhidmatan IPTV melalui ISP atau LAN. Tab IPTV memberikan tetapan konfigurasi yang diperlukan untuk menyediakan IPTV, VoIP, multisiar, dan UDP untuk perkhidmatan anda. Hubungi ISP anda untuk maklumat khusus mengenai perkhidmatan anda.



3.8 Rangkaian

3.8.1 Rangkaian Utama - Penapis MAC

Penapis MAC Wayarles memberikan kawalan ke atas paket yang dihantar ke alamat MAC (Kawalan Akses Media) yang dinyatakan pada rangkaian wayarles anda.



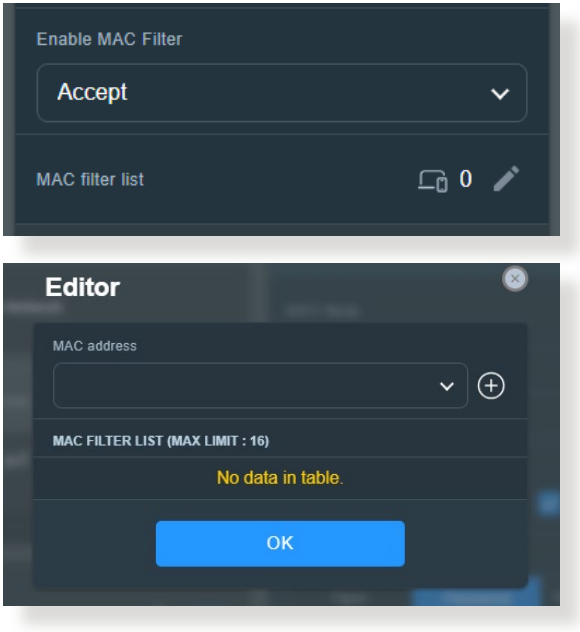
Untuk menyediakan penapis Wayarles MAC:

1. Daripada panel navigasi, pergi ke **General (Umum)** > **Network (Rangkaian)** > **Main Network (Rangkaian Utama)** dan pilih nama rangkaian (SSID) bagi rangkaian utama.
2. Dalam senarai jatuh bawah **Enable Mac Filter (Dayakan Penapis Mac)**, pilih sama ada **Accept (Terima)** atau **Reject (Tolak)**.

- Pilih **Accept (Terima)** untuk membenarkan peranti dalam senarai penapis MAC untuk mengakses rangkaian wayarles.
- Pilih **Reject (Tolak)** untuk menghalang peranti dalam senarai penapis MAC untuk mengakses rangkaian wayarles.

NOTA: Pilih **Disable (Lumpuhkan)** jika anda ingin mematikan **Enable MAC Filter (Dayakan Penapis Mac)**.

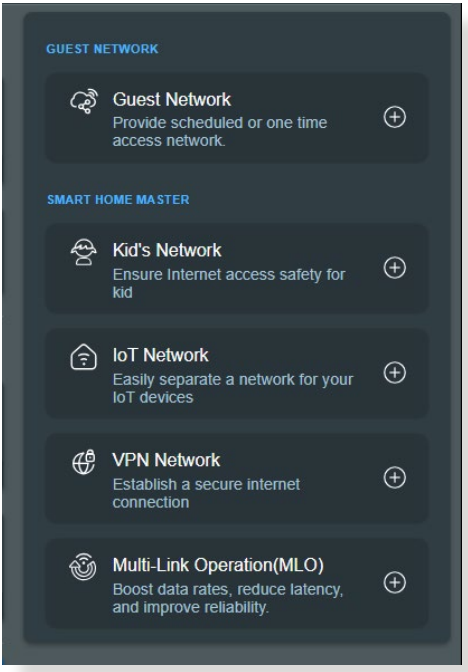
4. Pada senarai penapis MAC, klik untuk mengakses halaman Editor, dan kemudian klik dan masukkan alamat MAC bagi peranti wayarles.
5. Klik **OK**.



3.8.2 Rangkaian Tetamu

3.8.2.1 Rangkaian Tetamu

Guest Network (Rangkaian Tetamu) memberikan sambungan Internet kepada tetamu sementera melalui akses untuk mengasingkan akses SSID atau rangkaian tanpa memberikan akses kepada rangkaian peribadi anda.

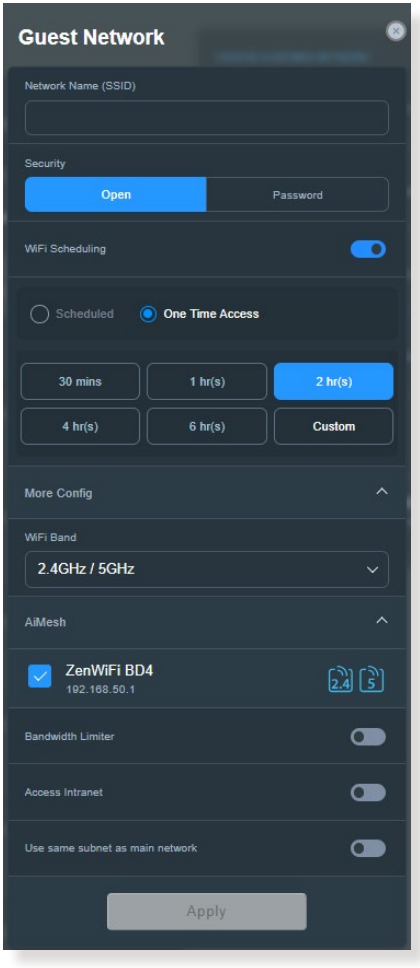


NOTA: ZenWiFi BD4 menyokong sehingga tiga SSID dalam Rangkaian Tetamu.

Mencipta rangkaian tetamu anda:

1. Daripada panel navigasi, pergi ke **General (Am)** > **Network (Rangkaian)** > **Guest Network (Rangkaian Tetamu)** > **Add a Network (Tambah Rangkaian)**.
2. Pilih **Guest Network (Rangkaian Tetamu)** dan tetapkan nama rangkaian untuk rangkaian sementara anda dalam medan **Network Name (Nama Rangkaian) (SSID)**.
3. Pilih kaedah pengesahan di bawah **Security (Keselamatan)**.

4. Tentukan masa akses atau pilih **Scheduled (Dijadualkan)** untuk menambah profil jadual dalam talian.
5. Pilih **WiFi Band** untuk rangkaian tetamu yang ingin anda cipta.
6. Dayakan atau lumpuhkan **Bandwidth Limiter (Penghad Lebar Jalur)**.
7. Dayakan atau lumpuhkan **Access Intranet (Akses Intranet)**.
8. Apabila selesai, klik **Apply (Guna)**.

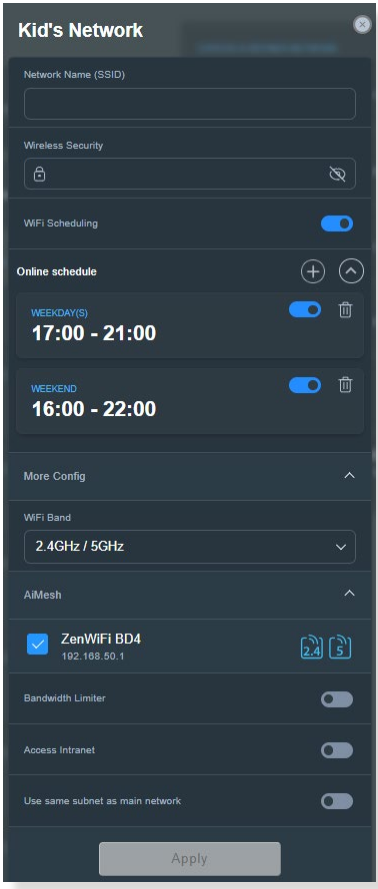


3.8.2.2 Smart Home Master

Smart Home Master merupakan alat yang hebat dan mesra pengguna untuk pensegmenan rangkaian. Ia memudahkan proses mencipta dan mengurus senario subrangkaian lanjutan seperti mencipta SSID khusus untuk peranti anak anda, menyambung ke VPN menerusi subrangkaian khusus, atau malah mencipta satu SSID selamat untuk semua peranti IoT anda.

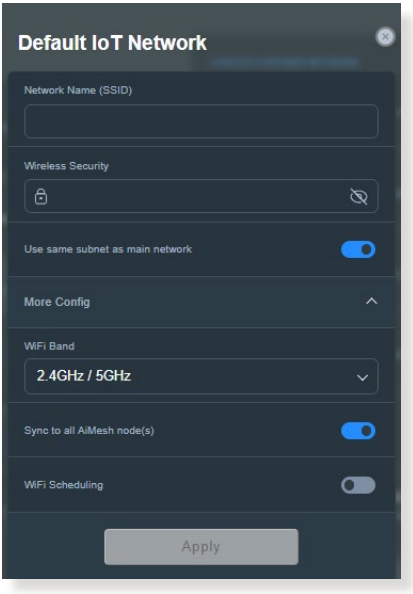
Mencipta Rangkaian Kanak-kanak anda:

1. Daripada panel navigasi, pergi ke **General (Am)** > **Network (Rangkaian)** > **Guest Network (Rangkaian Tetamu)** > **Add a Network (Tambah Rangkaian)**.
2. Pilih **Kid's Network (Rangkaian Kanak-kanak)** dan tetapkan nama rangkaian dan kunci keselamatan dalam medan **Network Name (Nama Rangkaian) (SSID)** dan **Wireless Security (Keselamatan Wayarles)**.
3. Suaikan masa akses Internet dalam medan **Online schedule (Jadual dalam talian)**.
4. Pilih **WiFi Band** untuk rangkaian Kanak-kanak yang ingin anda cipta.
5. Dayakan atau lumpuhkan **Bandwidth Limiter (Penghad Lebar Jalur)**.
6. Dayakan atau lumpuhkan **Access Intranet (Akses Intranet)**.
7. Apabila selesai, klik **Apply (Guna)**.



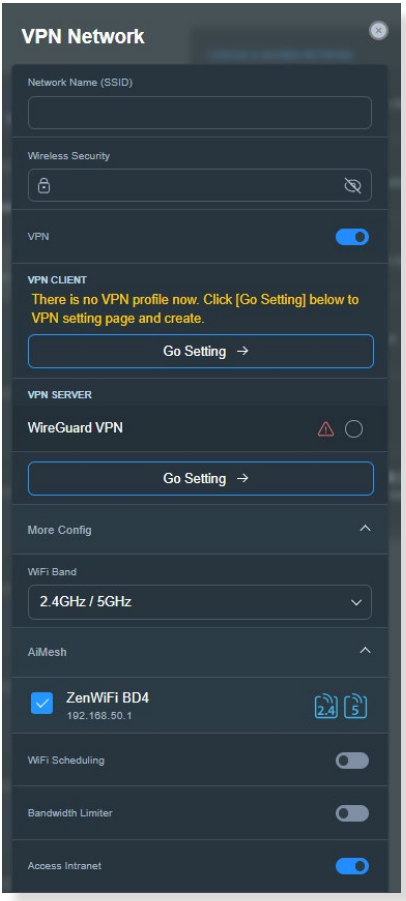
Mencipta Rangkaian IoT anda:

1. Daripada panel navigasi, pergi ke **General (Am)** > **Network (Rangkaian)** > **Guest Network (Rangkaian Tetamu)** > **Add a Network (Tambah Rangkaian)**.
2. Pilih **IoT Network (Rangkaian IoT)** dan tetapkan nama rangkaian dan kunci keselamatan dalam medan **Network Name (Nama Rangkaian) (SSID)** dan **Wireless Security (Keselamatan Wayarles)**.
3. Pilih **WiFi Band** untuk rangkaian IoT yang ingin anda cipta.
4. Suaikan masa akses Internet dengan mendayakan **WiFi Scheduling (Penjadualan WiFi).**
5. Apabila selesai, klik **Apply (Guna)**.



Mencipta Rangkaian VPN anda:

1. Daripada panel navigasi, pergi ke **General (Am)** > **Network (Rangkaian)** > **Guest Network (Rangkaian Tetamu)** > **Add a Network (Tambah Rangkaian)**.
2. Pilih **VPN Network (Rangkaian VPN)** dan tetapkan nama rangkaian dan kunci keselamatan dalam medan **Network Name (Nama Rangkaian) (SSID)** dan **Wireless Security (Keselamatan Wayarles)**.
3. Jika anda belum menyediakan profil VPN untuk pelayan VPN atau klien VPN, klik **Go Setting (Pergi Tetapan)** untuk mencipta profil VPN.
4. Pilih **WiFi Band** untuk rangkaian VPN yang ingin anda cipta.
5. Suaikan masa akses Internet dengan mendayakan **WiFi Scheduling (Penjadualan WiFi).**
6. Dayakan atau lumpuhkan **Bandwidth Limiter (Penghad Lebar Jalur)**.
7. Dayakan atau lumpuhkan **Access Intranet (Akses Intranet)**.
8. Apabila selesai, klik **Apply (Guna)**.


VPN Network
Network Name (SSID)
Wireless Security
VPN
VPN CLIENT
There is no VPN profile now. Click [Go Setting] below to VPN setting page and create.
Go Setting →
VPN SERVER
WireGuard VPN
Go Setting →
More Config
WiFi Band
2.4GHz / 5GHz
AiMesh
ZenWiFi BD4
192.168.50.1
WiFi Scheduling
Bandwidth Limiter
Access Intranet

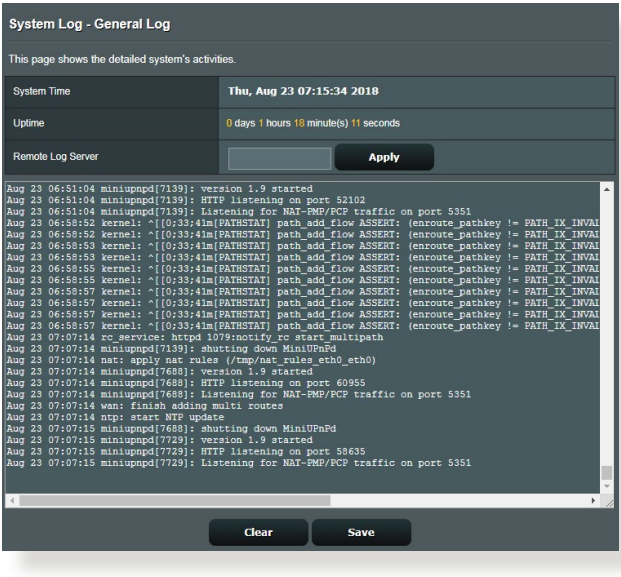
3.9 Log Sistem

Log Sistem mengandungi aktiviti rangkaian terakam anda.

NOTA: Log sistem menetap semula apabila penghala dibut semula atau dimatikan.

Untuk melihat log sistem anda:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **System Log (Log Sistem)**.
2. Anda boleh melihat aktiviti rangkaian anda dalam mana-mana tab ini:
   - Log Am
   - Log Wayarles
   - Pajakan DHCP
   - IPv6
   - Jadual Penghalaan
   - Pemajuan Port
   - Sambungan



3.10 Penganalisis Trafik

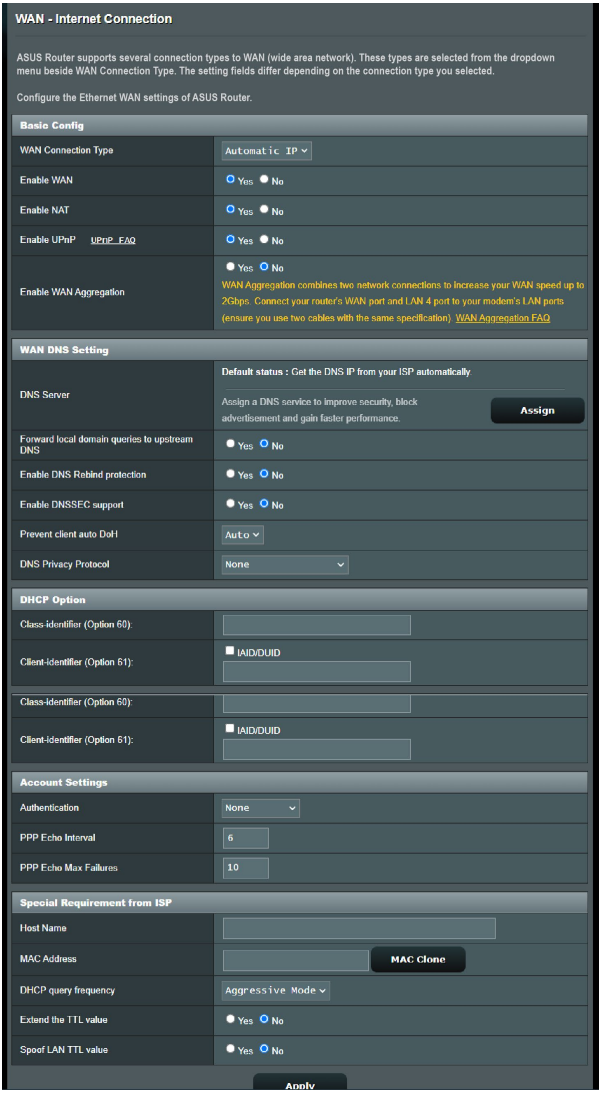
Ciri monitor trafik membolehkan anda mengakses penggunaan lebar jalur dan kelajuan Internet, rangkaian berwayar dan wayarles anda. Ia membolehkan anda memantau trafik rangkaian dalam masa nyata atau berasaskan harian. Ia juga menawarkan pilihan untuk menawarkan trafik rangkaian dalam masa 24 jam terakhir.

NOTA: Paket daripada Internet dihantar dengan sekata ke peranti terdawai dan wayarles.

3.11 WAN

3.11.1 Sambungan Internet

Skrin Sambungan Internet membolehkan anda mengkonfigurasikan tetapan pelbagai jenis sambungan WAN.



Untuk mengkonfigurasikan tetapan sambungan WAN:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **WAN** > **Internet Connection (Sambungan Internet)**.
2. Konfigurasi tetapan di bawah yang berikut. Apabila selesai, klik **Apply (Guna)**.

- **Jenis Sambungan WAN**: Pilih jenis Pembekal Perkhidmatan Internet anda. Pilihan adalah **Automatic IP (IP Automatik)**, **PPPoE**, **PPTP**, **L2TP** atau **fixed IP (IP tetap)**. Rujuk ISP anda jika penghala tidak boleh mendapatkan alamat IP sah atau jika anda tidak pasti jenis sambungan WAN.
- **Mendayakan WAN**: Pilih **Yes (Ya)** untuk membolehkan akses penghala Internet. Pilih **No (Tidak)** untuk mendayakan akses Internet.
- **Mendayakan NAT**: NAT (Terjemahan Alamat Rangkaian) adalah sistem di mana satu IP awam (IP WAN) digunakan untuk memberikan akses Internet ke klien rangkaian dengan alamat IP peribadi dalam LAN. Alamat IP peribadi setiap klien rangkaian disimpan dalam jadual NAT dan ia digunakan pada paket data masuk penghala.
- **Mendayakan UPnP**: UPnP (Universal Plug and Play) (Palam dan Main Universal) membenarkan beberapa peranti (seperti penghala, televisyen, sistem stereo, konsol permainan, dan telefon selular) untuk dikawal melalui rangkaian berasaskan IP dengan atau tanpa kawalan pusat melalui get laluan. UPnP menyambungkan PC semua betuk faktor, memberikan rangkaian tak berkelim untuk konfigurasi jauh dan pemindahan data. Menggunakan UPnP, peranti rangkaian baru ditemui secara automatik. Apabila bersambung ke rangkaian, peranti boleh dikonfigurasikan untuk menyokong aplikasi P2P, permainan interaktif, persidangan video, dan web atau pelayan proksi. Tidak seperti Pemajuan Port, yang melibatkan konfigurasi tetapan port secara manual, UPnP secara mengkonfigurasikan penghala secara automatik untuk menerima sambungan masuk dan mengarahkan permintaan ke PC khusus pada rangkaian setempat.

- **Dayakan Pengagregatan WAN:** Pengagregatan WAN menggabungkan dua sambungan rangkaian untuk meningkatkan kelajuan WAN anda sehingga 2 Gbps. Sambungkan port WAN dan port LAN 4 penghala anda ke port LAN modem anda.
- **Menyambung kepada Pelayan DNS**: Benarkan penghala ini untuk mendapatkan alamat IP DNS daripada ISP secara automatik. DNS adalah hos pada Internet yang menterjemahkan nama Internet ke alamat IP angka.
- **Pengesahan**: Item ini mungkin ditentukan oleh beberapa ISP. Semak dengan ISP anda dan isikannya jika diperlukan.
- **Nama Hos**: Medan ini membenarkan anda untuk memberikan nama hos untuk penghala anda. Biasanya ia adalah keperluan istimewa daripada ISP anda. Jika ISP anda diberikan nama hos kepada komputer anda, masukkan nama hos di sini.
- **Alamat MAC**: Alamat MAC (Kawalan Capaian Media) adalah pengecam unik untuk peranti perangkaian anda. Beberapa ISP memantau alamat MAC peranti perangkaian yang bersambung ke perkhidmatan mereka dan menolak mana-mana peranti yang tidak dikenali yang mencuba untuk bersambung. Untuk mengelakkan isu sambungan disebabkan alamat MAC yang tidak didaftar, anda boleh:
  - Hubungi ISP anda dan kemas kini alamat MAC berkaitan dengan perkhidmatan ISP anda.
  - Klon atau menukar alamat MAC penghala wayarles ASUS untuk sepadan dengan alamat MAC peranti perangkaian sebelumnya dikenali oleh ISP.

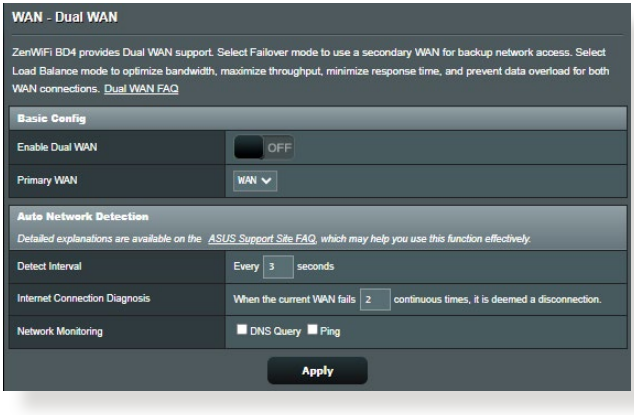
3.11.2 WAN Dual

WAN Dual membolehkan anda memilih dua sambungan ISP ke penghala anda, WAN primer dan WAN sekunder.

Untuk mengkonfigurasikan WAN Dual:

1. Dari panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan) > WAN**.
2. Pergi ke medan **Dual WAN (WAN Dual)**, pilih **ON (HIDUP).**
3. Pilih **Primary WAN (WAN Primer)** dan **Secondary WAN (WAN Sekunder)** anda. Terdapat dua 2.5GbE WAN/LAN untuk pilihan anda.
4. Pilih **Fail Over (Gagal Seluruh)** atau L**oad Balance (Keseimbangan Beban)**.
5. Klik **Apply (Guna)**.

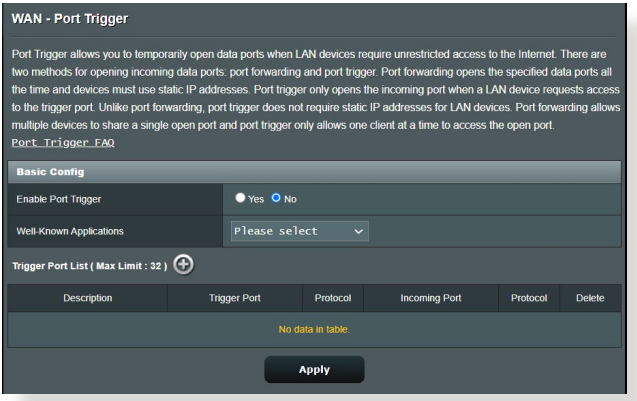
NOTA: Penerangan terperinci boleh didapati pada Soalan Lazim Laman Sokongan **ASUS https://www.asus.com/support/FAQ/1011719**.



3.11.3 Picu Port

Picu julat port membuka port masuk yang ditentukan untuk tempoh masa yang terhad apabila klien di rangkaian kawasan setempat menjadi sambungan keluar ke port yang dinyatakan. Picu port digunakan dalam senario berikut:

- Lebih daripada satu klien setempat memerlukan pemajuan port untuk aplikasi yang sama pada masa yang berbeza.
- Satu aplikasi memerlukan port masuk khusus yang berbeza daripada port keluar.



Untuk menyediakan Picu Port:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **WAN** > **Port Trigger (Picu Port)**.
2. Konfigurasi tetapan di bawah yang berikut. Apabila selesai, klik **Apply (Guna)**.
   - **Mendayakan Pencetus Port**: Pilih **Yes (Ya)** untuk mendayakan Picu Port.
   - **Aplikasi Yang Diketahui**: Pilih permainan dan perkhidmatan web popular untuk menambah ke Senarai Picu Port.
   - **Penerangan**: Masukkan nama pendek atau huraian untuk perkhidmatan ini.

- **Port Picu**: Tentukan port picu untuk membukan port masuk.
- **Protokol**: Pilih protokol, TCP, atau UDP.
- **Port Masuk**: Nyatakan port masuk untuk menerima data masuk daripada Internet.

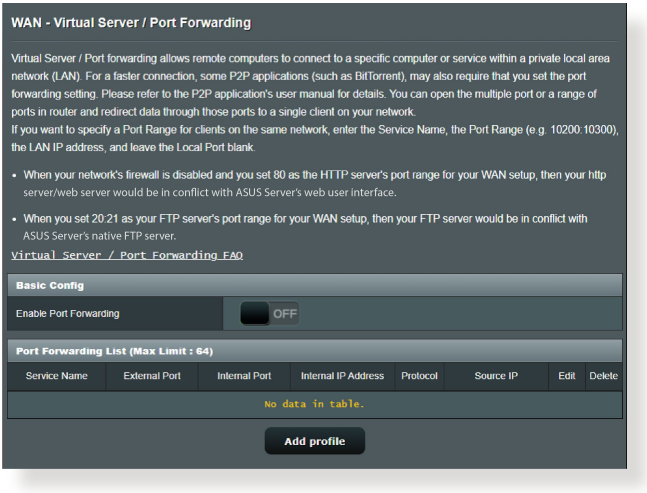
NOTA:

- Apabila menyambung ke pelayan IRC, PC klien membuat sambungan keluar menggunakan julat port picu 66660-7000. Pelayan IRC respons dengan mengesahkan nama pengguna dan mencipta sambungan baru kepada PC klien menggunakan port masuk.
- Jika Picu Port dinyahdayakan, penghala menjatuhkan sambungan kerana ia tidak boleh menentukan PC yang mana yang meminta akses IRC. Apabila Picu Port didayakan, penghala menugaskan port masuk untuk menetapkan data masuk. Port masuk ini ditutup apabila tempoh masa khusus telah berlalu kerana penghala tidak pasti apabila aplikasi telah ditamatkan.
- Picu port hanya membenarkan satu klien dalam rangkaian menggunakan perkhidmatan tertentu dan port masuk khusus pada masa yang sama.
- Anda tidak boleh menggunakan aplikasi yang sama untuk memicu port dalam lebih daripada satu PC pada masa yang sama. Penghala hanya memajukan port semula ke komputer terakhir yang menghantar permintaan/picu penghala.

3.11.4 Pelayan Maya/Pemajuan Port

Pemajuan por adalah kaedah untuk menghala trafik rangkaian dari Internet ke port khusus atau julat port khusus ke satu peranti atau beberapa peranti pada rangkaian tempatan anda. Menyediakan Pemajuan Port pada penghala anda membenarkan PC di luar rangkaian untuk mengakses perkhidmatan khusus yang diberikan oleh PC dalam rangkaian anda.

NOTA: Apabila pemajuan port dinyahdayakan, penghala ASUS menyekat trafik masuk tanpa diminta dari Internet dan hanya membenarkan balasan daripada permintaan luar daripada LAN. Klien rangkaian tidak mempunyai akses kepada Internet secara langsung, dan sebaliknya.



Untuk menyediakan Pemajuan Port:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **WAN** > **Virtual Server / Port Forwarding (Pelayan Maya / Pemajuan Port)**.

2. Konfigurasi tetapan di bawah yang berikut. Apabila selesai, klik **ON (HIDUP)**.

- **Dayakan Pemajuan Port**: Pilih **ON (HIDUP)** untuk mendayakan Pemajuan Port.
- **Senarai Pelayan Terkenal**: Tentukan jenis perkhidmatan yang manakah yang anda ingin akses.
- **Senarai Permainan Terkenal**: Item ini menyenaraikan port yang diperlukan untuk permainan dalam talian popular untuk berfungsi dengan betul.
- **Port Pelayan FTP**: Elakkan menugaskan julat port 20:21 pelayan FTP anda kerana ini akan bercanggah dengan tugasan pelayan FTP asal penghala.
- **Nama Perkhidmatan**: Masukkan nama perkhidmatan.
- **Julat Port**: Jika anda mahu menentukan Liputan Port untuk klien pada rangkaian yang sama, masukkan Nama Perkhidmatan, Liputan Port (cth. 10200:10300), alamat IP LAN dan biarkan Port Setempat kosong. Liputan port menerima pelbagai format seperti Liputan Port (300:350), port individu (566,789) atau Campuran (1015:1024,3021).

NOTA:

- Apabila tembok api rangkaian anda dinyahdayakan dan anda menetapkan 80 sebagai julat port pelayan HTTP untuk penyediaan WAN anda, kemudian pelayan http/pelayan web akan bercanggah dengan antara muka pengguna web penghala.
- Rangkaian menggunakan port untuk menukar data, dengan setiap port ditugaskan nombor port dan tugasan khusus. Sebagai contoh, port 80 digunakan untuk HTTP. Port khusus hanya boleh digunakan oleh satu aplikasi aau perkhidmatan pada satu masa. Oleh itu, dua PC mencuba untuk mengakses data melalui port yang sama pada masa yang sama akan gagal. Sebagai contoh, anda tidak boleh menyediakan Pemajuan Port untuk port 100 untuk dua PC pada masa yang sama.

- **IP Tempatan**: Masukkan alamat IP LAN klien.

NOTA: Gunakan alamat IP statik untuk klien setempat untuk menjadikan pemajuan port berfungsi dengan baik. Rujuk bahagian **3.8 LAN** untuk maklumat.

- **Port Setempat**: Masukkan port khusus untuk menerima paket yang dimajukan. Biarkan medan ini kosong jika anda mahu paket masuk dihalakan semula ke julat port yang dinyatakan.
- **Protokol**: Pilih protokol. Jika anda tidak pasti, pilih **KEDUA-DUANYA**.

Untuk memeriksa jika Pemajuan Port telah berjaya dikonfigurasi:

- Pastikan pelayan atau aplikasi anda disediakan dan berjalan.
- Anda memerlukan klien di luar LAN anda tetapi mempunyai akses Internet (dirujuk sebagai "Klien Internet"). Klien ini tidak boleh disambungkan ke penghala ASUS.
- Pada klien Internet, gunakan IP WAN penghala untuk mengakses pelayan. Jika pemajuan port telah berjaya, anda boleh mengakses fail atau aplikasi.

Perbezaan antara picu port dan pemajuan port:

- Picu port akan berfungsi walaupun tanpa menyediakan alamat IP LAN khusus. Tidak seperti pemajuan port, yang memerlukanalamat IP LAN statik, picu port membolehkan pemajuan port dinamik menggunakan penghala. Julat port yang telah ditetapkan dikonfigurasikan untuk menerima sambungan masuk untuk tempoh masa terhad. Picu port membolehkan berbilang komputer untuk menjalankan aplikasi yang biasanya memerlukan pemajuan secara manual port yang sama ke setiap PC pada rangkaian.
- Picu port adalah lebih selamat daripada pemajuan port memandangkan port masuk tidak dibuka pada setiap masa. Ia dibuka hanya apabila aplikasi membuat sambungan keluar melalui port picu.

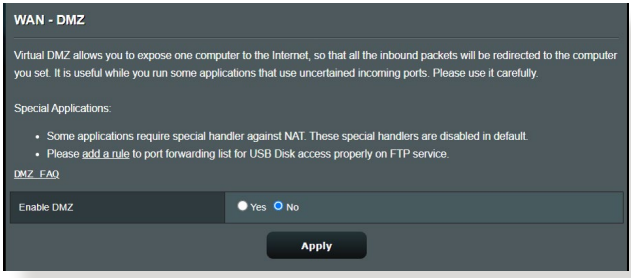
3.11.5 DMZ

DMZ Maya mendedahkan satu klien ke Internet, membolehkan klien ini menerima semua paket masuk diarahkan ke Rangkaian Kawasan Setempat.

Trafik masuk dari Internet biasanya dibuang dan dihalakan ke klien tertentu hanya jika pemajuan port atau picu port telah dikonfigurasikan pada rangkaian. Dalam konfigurasi DMZ, satu klien rangkaian menerima semua paket masuk.

Meyediakan DMZ pada rangkaian adalah berguna bila anda memerlukan port masuk terbuka atau anda ingin mengehos domain, web, atau pelayan e-mel.

PERHATIAN: Membuka semua port pada klien ke Internet menjadikan ragkaian rentan kepada serangan luar. Sila berjaga-jaga akan risiko keselamatan yang terlibat dalam menggunakan DMZ.



Untuk menyediakan DMZ:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **WAN** > **DMZ**.
2. Konfigurasi tetapan di bawah. Apabila selesai, klik **Apply (Guna)**.

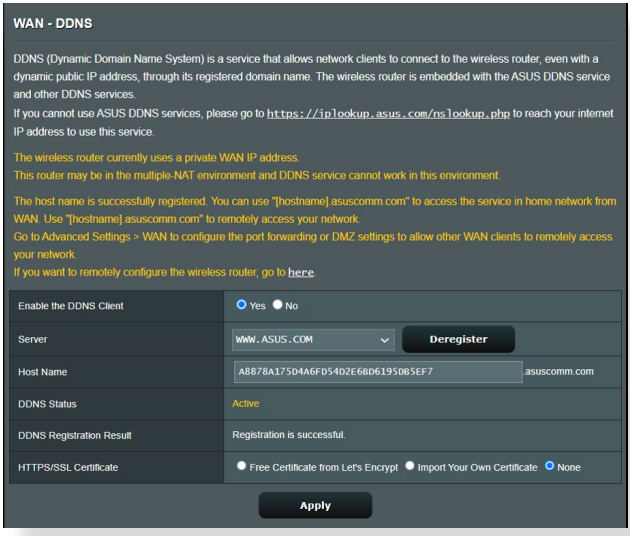
- **Alamat IP bagi Stesen Terdedah:** Masukkan alamat IP LAN klien yang akan menyediakan perkhidmatan DMZ dan terdedah pada Internet. Pastikan klienn pelayan mempunyai alamat IP statik.

Untuk membuang DMZ:

1. Padam alamat IP LAN klien dari kotak teks **IP Address of Exposed Station (Alamat IP Stesen Terdedah)**.
2. Apabila selesai, klik **Apply (Guna)**.

3.11.6 DDNS

Menyediakan DDNS (DNS Dinamik) membolehkan anda mengakses penghala daripada luar rangkaian anda melalui Perkhidmatan DDNS ASUS atau perkhidmatan DDNS lain.



Untuk menyediakan DDNS:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **WAN** > **DDNS**.
2. Konfigurasi tetapan di bawah yang berikut. Apabila selesai, klik **Apply (Guna)**.
   - **Mendayakan Klien DDNS**: Dayakan DDNS untuk mengakses penghala ASUS melalui nama DNS dan bukannya alamat IP WAN.
   - **Pelayan dan Nama Hos**: Pilih DDNS ASUS atau DDNS lain. Jika anda ingin menggunakan DDNS ASUS, isi Nam Hos dalam format xxx.asuscomm.com (xxx adalah nama hos anda).

- Jika anda ingin menggunakan perkhidmatan DDNS berbeza, klik CUBAAN PERCUMA dan mendaftar dalam talian dahulu. Isi Nama Pengguna atau Alamat E-mel dan Kata Laluan atau medan Kunci DDNS.
- **Mendayakan kad bebas**: Dayakan kad bebas jika perkhidmatan DDNS anda memerlukan satu.

NOTA:

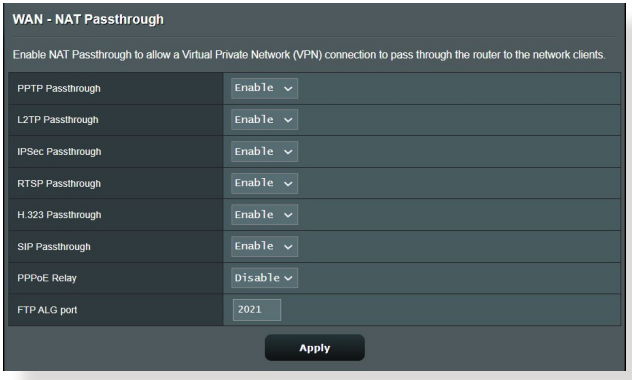
Perkhidmatan DDNS tidak akan berfungsi di bawah keadaan ini:

- Apabila penghala wayarles menggunakan alamat peribadi IP WAN (192.168.x.x, 10.x.x.x, atau 172.16.x.x), seperti yang ditunjukkan oleh teks berwarna kuning.
- Penghala mungkin berada pada rangkaian yang menggunakan jadual NAT berbilang.

3.11.7 Masuk Lalu NAT

Masuk Lalu NAT membolehkan sambungan Rangkaian Peribadi Maya (VPN) untuk melalui penghala ke klien rangkaian. Masuk Lalu PPTP, Masuk Lalu L2TP, Masuk Lalu IPsec dan Masuk Lalu RTSP didayakan secara lalai.

Untuk mendayakan / nyahdaya tetapan Masuk Lalu NAT, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **WAN** > **NAT Passthrough (Masuk Lalu NAT)**. Apabila selesai, klik **Apply (Guna)**.

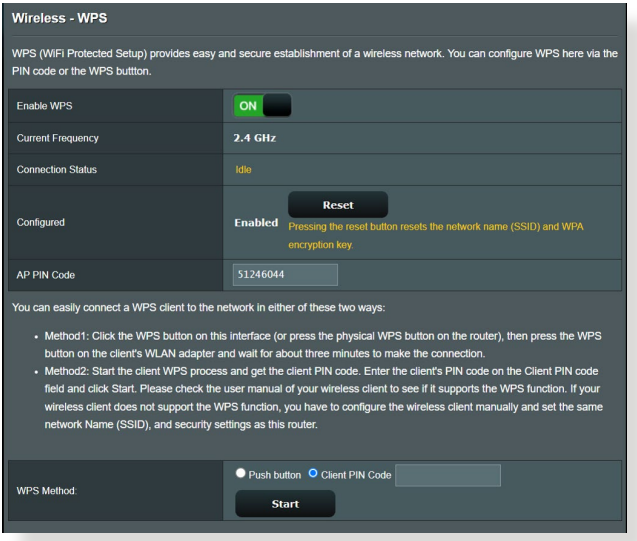


3.12 Wayarles

3.12.1 WPS

WPS (Persediaan Dilindungi Wi-Fi) adalah standard keselamatan wayarles yang membenarkan anda untuk menyambungkan peranti dengan mudah ke rangkaian wayarles. Anda boleh mengkonfigurasi fungsi WPS melalui kod PIN atau butang WPS.

NOTA: Memastikan bahawa peranti menyokong WPS.



Untuk mendayakan WPS pada rangkaian wayarles anda:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Wireless (Wayarles)** > **WPS**.
2. Dalam medan **Dayakan WPS**, gerakkan gelangsar ke **HIDUP**.
3. WPS menggunakan 2.4GHz secara lalai. Jika anda ingin menukar frekuensi ke 5GHz, **OFF (MATIKAN)** fungsi WPS, klik **Switch Frequency (Tukar Frekuensi)** dalam medan **Current Frequency (Frekuensi Semasa)**, dan **ON (HIDUPKAN)** WPS sekali lagi.

NOTA: WPS menyokong pengesahan menggunakan Sistem Terbuka, WPA-Peribadi, dan WPA2-Peribadi. WPS tidak menyokong rangkaian wayarles yang menggunakan Kunci Dikunci, WPA-Enterprise, WPA2-Enterprise, dan kaedaj penyulitan RADIUS.

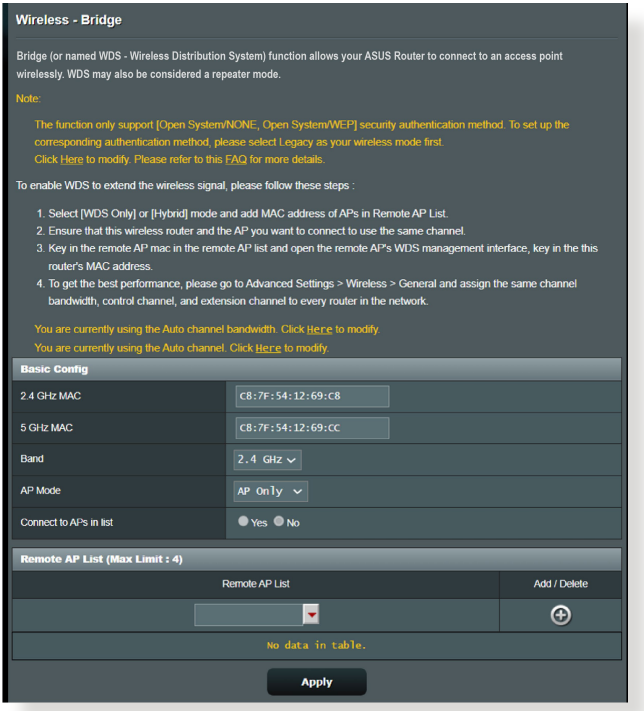
4. Dalam medan Kaedah WPS, pilih kod **Push Button (Butang Tolak)** atau **Client PIN code (Kod PIN Klien)**. Jika anda memilih **Push Button (Butang Tolak)**, pergi ke langkah 5. Jika anda memilih kod **Client PIN code (Kod PIN Klien)**, pergi ke langkah 6.
5. Untuk menyediakan WPS menggunakan butang penghala WPS, ikuti langkah ini:
   a. Klik **Start (Mula)** atau tekan butang WPS yang dijumpai di belakang penghala wayarles.
   b. Tekan butang WPS pada peranti wayarles anda. Ini biasanya dikenal pasti melalui logo WPS.

NOTA: Periksa peranti wayarles anda atau manual pengguna untuk lokasi butang WPS.

   c. Penghala wayarles akan mengimbas mana-mana peranti WPS tersedia. Jika penghala wayarles tidak menjumpai mana-mana peranti WPS, ia akan bertukar ke mod siap sedia.
6. Untuk menyediakan WPS menggunakan kod PIN Klien, ikuti langkah ini:
   a. Cari kod PIN WPS pada manual pengguna peranti wayarles anda atau pada peranti itu sendiri.
   b. Masukkan kod PIN Klien pada kotak teks.
   c. Klik **Start (Mula)** untuk meletakkan penghala wayarles anda ke dalam mod tinjauan WPS. Penunjuk penghala LED berkelip tiga kali dengan pantas sehingga penyediaan WPS lengkap.

3.12.2 Penghubung

Penghubung atau WDS (Sistem Pengedaran Wayarles) membolehkan penghala wayarles ASUS anda untuk bersambung ke titik akses wayarles lain secara eksklusif, mengelakkan peranti wayarles lain atau stesen untuk mengakses penghala wayarles ASUS anda. Ia juga boleh dianggap sebagai pengulang wayarles di mana penghala wayarles ASUS anda berkomunikasi dengan titik akses lain dan peranti wayarles lain.



Untuk menyediakan penghubung wayarles:

1. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Wireless (Wayarles)** > **WDS**.
2. Pilih jalur frekuensi untuk penghubung wayarles.
3. Dalam medan **Mod AP**, pilih mana-mana pilihan ini:
   - **AP Sahaja**: Nyahdaya fungsi Penghubung Wayarles.

- **WDS Sahaja**: Mendayakan ciri Penghubung Wayarles tetapi menghalang peranti/stesen wayarles lain daripada bersambung ke penghala.
- **HIBRID**: Mendayakan ciri Penghubung Wayarles dan membenarkan peranti/stesen wayarles lain bersambung ke penghala.

NOTA: Dalam mod Hibrid, peranti wayarles bersambung dengan penghala wayarles ASUS hanya akan menerima separuh kelajuan sambungan Titik Akses.

4. Dalam medan **Connect to APs in list (Sambung ke AP dalam senarai)** , klik **Yes (Ya)** jika anda ingin bersambung ke Titik Akses yang disenarai dalam Senarai AP Jauh.
5. Dalam medan **Control Channel (Saluran Kawalan)**, pilih saluran operasi untuk penghubung wayarles. Pilih **Auto** untuk membolehkan penghala memilih saluran dengan jumlah yang paling kurang gangguan secara automatik.

NOTA: Ketersediaan saluran berbeza bagi setiap negara atau rantau.

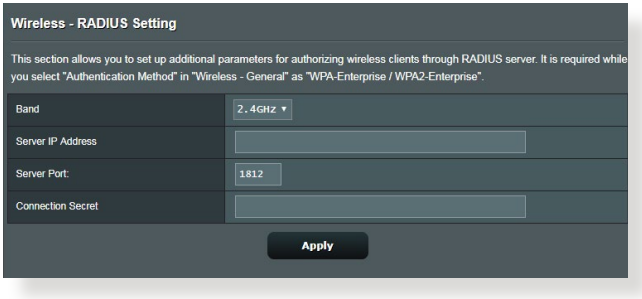
6. Pada **Remote AP List (Senarai AP Jauh)**, masukkan alamat MAC dan klik butang **Add (Tambah)**  untuk memasukkan alamat MAC Titik Akses tersedia lain.

NOTA: Mana-mana Titik Akses ditambah ke senarai perlu berada pada Saluran Kawalan yang sama seperti penghala wayarles ASUS.

7. Klik **Apply (Guna)**.

3.12.3 Seting RADIUS

Tetapan RADIUS (Perkhidmatan Pengguna Dail Pengesahan Jauh) memberikan lapisan tambahan keselamatan semasa anda memilih WPA-Enterprise, WPA2-Enterprise, atau Radius dengan 802.1x sebagai Mod Pengesahan anda.



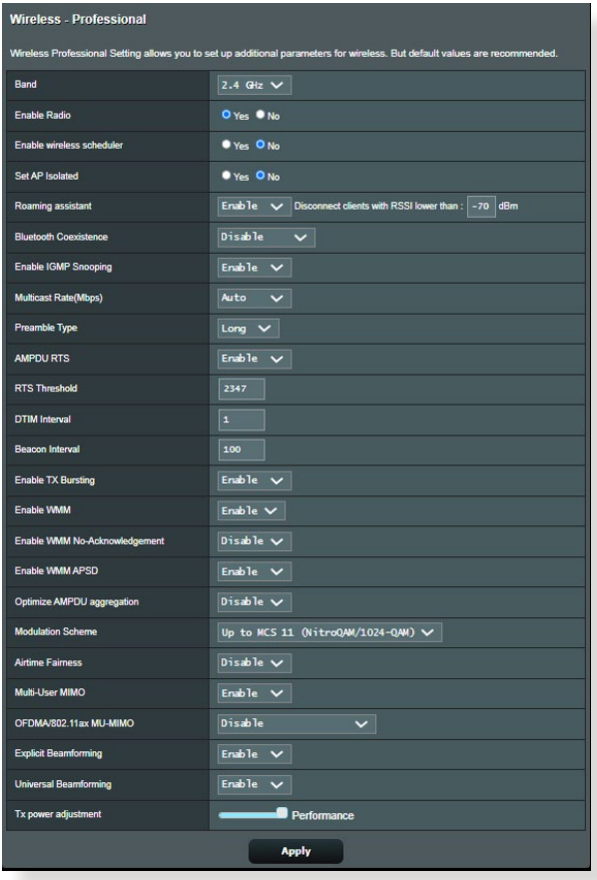
Untuk menyediakan tetapan wayarles RADIUS:

1. Pastikan mod pengesahan penghala wayarles ditetapkan ke WPA-Enterprise, WPA2-Enterprise, atau Radius dengan 802.1x.
2. Daripada panel navigasi, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Wireless (Wayarles)** > **RADIUS Setting (Tetapan RADIUS)**.
3. Pilih jalur frekuensi.
4. Dalam medan **Server IP Address (Alamat IP Pelayan)**, masukkan Alamat IP pelayan RADIUS.
5. Dalam medan **Connection Secret (Rahsia Sambungan)**, tugaskan kata laluan anda untuk mengakses pelayan RADIUS.
6. Klik **Apply (Guna)**.

3.12.4 Profesional

Skrin Profesional memberikan pilihan konfigurasi lanjutan.

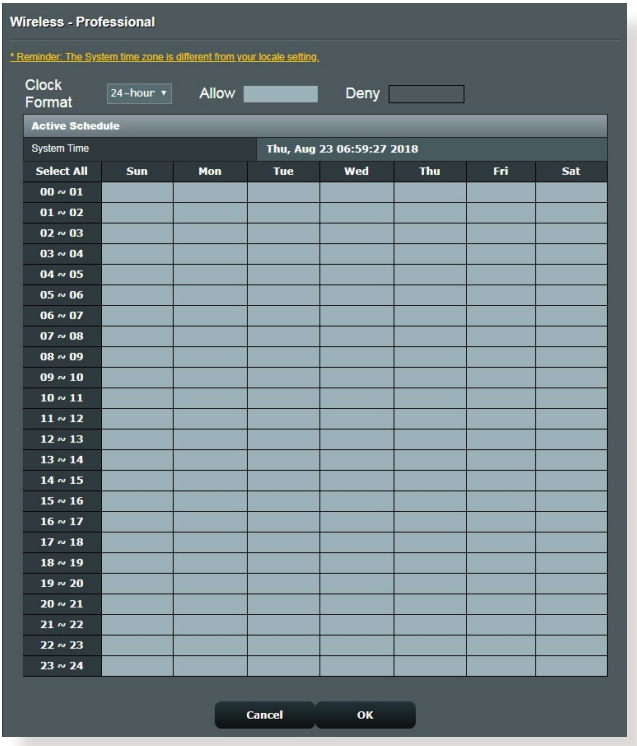
NOTA: Kami mengesyorkan anda menggunakan nilai lalai pada halaman ini.



Dalam skrin **Professional Settings (Tetapan Profesional)**, anda boleh mengkonfigurasikan yang berikut:

- **Jalur**: Pilih jalur frekuensi yang tetapan profesional akan digunakan.
- **Mendayakan Radio**: Pilih **Yes (Ya)** untuk mendayakan perangkaian wayarles. Pilih **No (Tidak)** untuk menyahdayakan perangkaian wayarles.

- **Dayakan penjadual wayarles**: Anda boleh memilih format jam sebagai 24 jam atau 12 jam. Warna dalam jadual menunjukkan Benarkan atau Tolak. Klik setiap bingkai untuk mengubah tetapan waktu bagi hari biasa dan klik **OK** apabila selesai.



- **Tetapkan pengasingan AP**: Item Tetapkan pengasingan Ap menghalang peranti wayarles pada rangkaian anda daripada berkomunikasi dengan antara satu sama lain. Ciri ini berguna jika ramai tetamu menyertai atau meninggalkan rangkaian annda secra kerap. Pilih **Yes (Ya)** untuk mendayakan ciri ini atau pilih **No (Tidak)** untuk menyahdayakan.
- **Julat Berbilang (Mbps)**: Pilih julat penghantaran multisiar atau klik **Disable (Nyahdaya)** untuk mematikan penghantaran tunggal secara serentak.

- **Jenis Mukadimah**: Jenis mukadimah mentakrifkan panjang masa yang penghala luangkan untuk CRC (Semakan Lewahan Kitar). CRC adalah kaedah mengesan ralat semasa penghantaran data. Pilih **Short (Pendek)** untuk rangkaian wayarles sibuk dengan trafik rangkaian tinggi. Pilih **Long (Panjang)** jika rangkaian wayarles anda terdiri daripada peranti wayarles lama atau legasi.
- **Ambang RTS**: Pilih nilai terendah untuk Ambang RTS (Meminta untuk Dihantar) untuk memperbaiki komunikasi wayarles dalam rangkaian wayarles sibuk atau bising dengan trafik rangkaian tinggi dan pelbagai peranti wayarles.
- **Jarak Waktu DTIM**: Jarak Waktu DTIM (Mesej Menunjukkan Lalu Lintas Penghantaran) atau Julat Data Isyarat adalah jarak masa sebelum isyarat dihantar ke peranti wayarles dalam mod tidur menunjukkan bahawa paket data menunggu penghantaran. Nilai lalai adalah tiga milisaat.
- **Jarak Waktu Isyarat**: Jarak Waktu Isyarat adalah masa antara satu DTIM dan seterusnya. Nilai lalai adalah 100 milisaat. Rendahkan nilai Jarak Waktu Isyarat untuk sambungan wayarles tidak stabil atau untuk peranti perayauan.
- **Mendayakan Pecahan TX**: Mendayakan Pecahan TX memperbaiki kelajuan penghantaran di antara penghala wayarles dan peranti 802.11g.
- **Mendayakan WMM APSD**: Mendayakan WMM APSD (Penghantaran Jimat Kuasa Automatik Multimedia Wi-Fi) untuk memperbaiki pengurusan kuasa di antara peranti wayarles. Pilih **Disable (Nyahdaya)** untuk mematikan WMM APSD.

4 Utiliti

4.1 Penemuan Peranti

Device Discovery (Penemuan Peranti) adalah utliti ASUS WLAN yang mengesan sebarang penghala wayarles ASUS yang tersedia pada rangkaian dan membolehkan anda untuk mengkonfigurasi peranti tersebut.

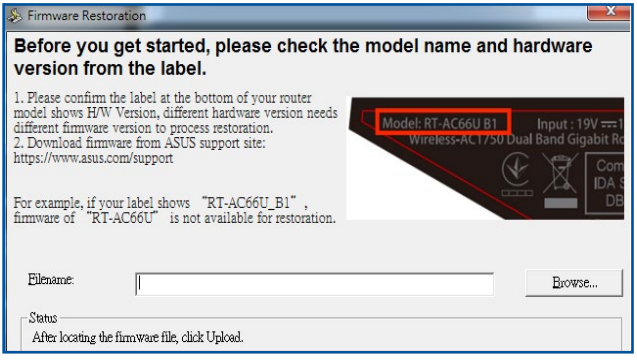
Untuk melancarkan utliti Device Discovery (Penemuan Peranti):

- Dari desktop komputer anda, klik **Start (Mula)** > **All Programs (Semua Program)** > **ASUS Utility (Utiliti ASUS)** > **ASUS Wireless Router (Penghala Wayarles ASUS)** > **Device Discovery (Penemuan Peranti)**.

NOTA: Apabila anda menetapkan penghala kepada mod Titik Akses, anda perlu menggunakan Device Discovery (Penemuan Peranti) untuk mendapatkan alamat IP penghala.

4.2 Pemulihan Perisian Tegar

Firmware Restoration (Pemulihan Perisian Tegar) digunakan pada Penghala Wayarles ASIS selepas penataran perisian tegar yang gagal dijalankan. Utiliti ini memuat naik fail perisian tegar ke penghala wayarles. Proses ini mengambil masa kira-kira tiga hingga empat minit.



PENTING: Lancarkan mod menyelamat sebelum menggunakan utiliti Firmware Restoration (Pemulihan Perisian Tegar).

NOTA: Ciri ini tidak disokong pada MAC OS.

Untuk melancarkan mod menyelamat dan menggunakan utiliti Firmware Restoration (Pemulihan Perisian Tegar):

1. Cabut keluar palam penghala wayarles dari sumber kuasanya.
2. Sambil menekan terus butang Reset (Tetap semula) di bahagian belakang penghala wayarles, pasangkan penghala wayarles ke dalam sumber kuasa. Lepasakan butang Reset (Tetap semula) apabila Power LED (LED Kuasa) di panel hadapan mula berkelip dengan perlahan, yang menandakan bahawa penghala wayarles berada dalam mod menyelamat.
3. Tetapkan IP statik pada komputer anda dan gunakan yang berikut untuk menyediakan tetapan TCP/IP anda:

   Alamat IP: 192.168.1.x

   Subnet mask: 255.255.255.0
4. Dari desktop komputer anda, klik **Start (Mulakan)** > **All Programs (Semua Atur cara)** > **ASUS Utility (Utiliti ASUS)** > **Wireless Router (Penghala Wayarles)** > **Firmware Restoration (Pemulihan Perisian Tegar)**.
5. Untuk menavigasi ke fail perisian tegar, kemudian klik **Upload (Muat naik)**.

NOTA: Utiliti Firmware Restoration (Pemulihan Perisian Tegar) tidak digunakan untuk menatarkan perisian tegar bagi Pengha Wayarles ASUS yang berfungsi. Perisian tegar biasa menatarkan apa yang perlu dilakukan melalui GUI web. Rujuk **3. Mengkonfigurasi Tetapan Am dan Lanjutan** untuk mendapatkan butiran yang lebih lanjut.

5 Menyelesai Masalah

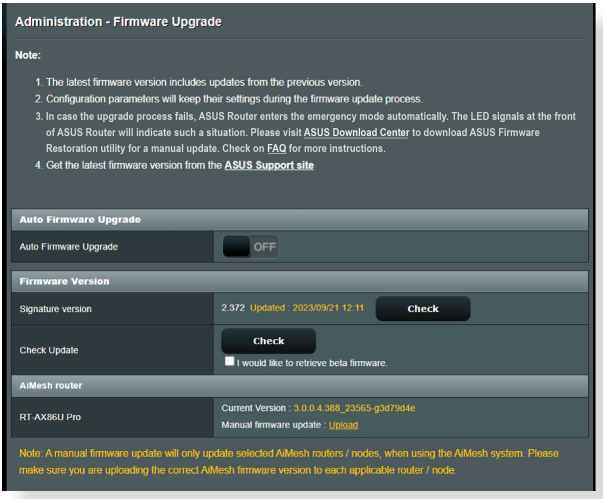
Bab ini memberikan penyelesaian untuk isu yang anda mungkin hadapi dengan penghala anda. Jika anda menghadapi masalah yang tidak disebut dalam bab ini, lawati tapak sokongan ASUS di: http://support.asus.com/ untuk maklumat produk lanjut dan butiran untuk dihubungi Sokongan Teknikal ASUS.

5.1 Penyelesaian Masalah Asas

Jika anda mengalami masalah dengan penghala anda, cuba langkah asas dalam bahagian ini sebelum mencari penyelesaian lanjut.

Naik taraf Perisian Tegar ke versi terkini.

1. Lancarkan Web GUI. Pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Administration (Pentadbiran)** > **Firmware Upgrade (Naik Taraf Perisian Tegar)**. Klik **Check (Periksa)** untuk mengesahkan jika perisian tegar terkini tersedia.



2. Jika perisian tegar tersedia, lawati tapak web global ASUS di https://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/ untuk memuat turun perisian tegar terkini.
3. Daripada halaman **Firmware Version (Versi Perisian Tegar)**, klik **Check (Periksa)** untuk mencari fail perisian tegar.
4. Klik **Upload (Muat Naik)** untuk menaik taraf perisian tegar.

Mula semula rangkaian anda dalam urutan berikut:

1. Matikan modem.
2. Cabut keluar palam.
3. Matikan penghala dan komputer.
4. Palamkan modem.
5. Hidupkan modem dan tunggu selama 2 minit.
6. Hidupkan penghala dan tunggu selama 2 minit.
7. Hidupkan komputer.

Periksa jika tetapan wayarles pada komputer anda sepadan dengan penghala anda.

- Apabila anda menyambungkan komputer anda ke penghala secara wayarles, pastikan SSID (nama rangkaian wayarles), kaedah penyulitan, dan kata laluan adalah betul.

Periksa jika tetapan rangkaian anda betul.

- Setiap klien pada rangkaian perlu mempunyai alamat IP yang sah. ASUS mengesyorkan anda menggunakan pelayan DHCP penghala wayarles untuk menugaskan alamat IP ke komputer pada rangkaian anda.

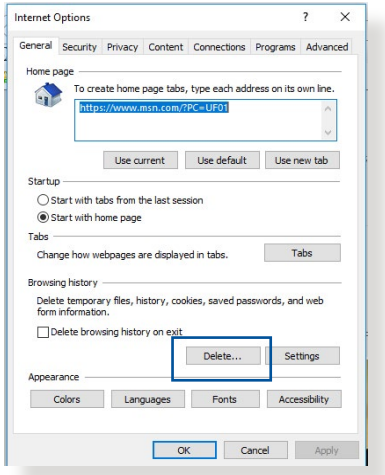
- Beberapa modem kabel pembekal perkhidmatan memerlukan anda menggunakan alamat MAC komputer yang pada mulanya didaftarkan pada akaun. Anda boleh melihat alamat MAC dalam GUI web, halaman **Network Map (Peta Rangkaian)** > **Clients (Klien),** dan layangkan penunjuk tetikus di atas peranti anda dalam **Client status (Status klien)**.

5.2 Soalan Lazim (FAQs)

Saya tidak dapat mengakses GUI penghala menggunakan penyemak imbas web.

- Jika komputer anda diwayarkan, periksa sambungan kabel Ethernet dan status LED seperti yang diterangkan dalam bahagian sebelum ini.
- Pastikan anda menggunakan maklumat log masuk yang betul. Pastikan kunci Huruf Besar dinyahdaya semasa anda memasukkan maklumat log masuk.
- Padam kuki dan fail dalam penyemak imbas anda. Untuk Internet Explorer, ikuti langkah ini:

  1. Lancarkan Internet Explorer anda, kemudian klik **Tools (Alatan)** > **Internet Options (Pilihan Internet)**.
  2. Dalam tab **General (Umum)**, di bawah **Browsing history (Sejarah pelayaran)**, klik **Delete… (Padam...)**, pilih **Fail Internet sementara dan fail laman web** dan **Kuki dan data laman web** kemudian klik **Delete (Padam)**.



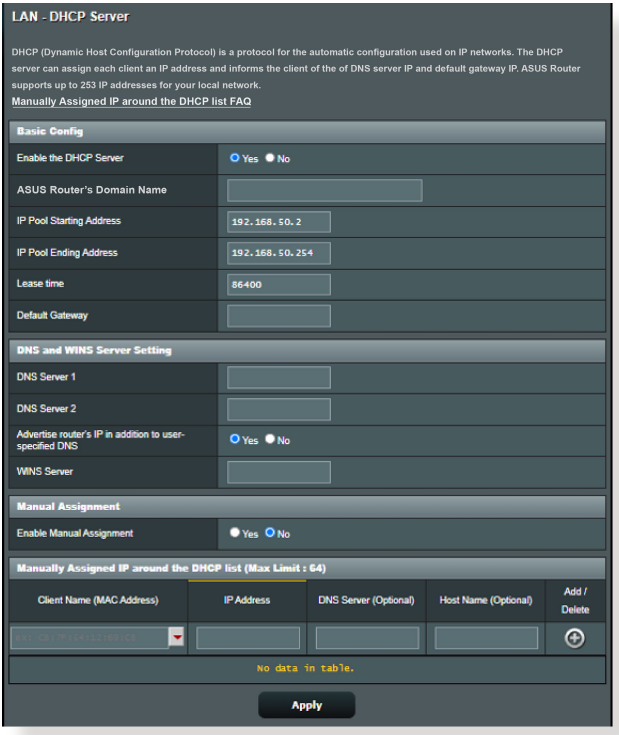
NOTA:

- Arahan untuk memadam kuki dan fail berbeza mengikut penyemak imbas web.
- Nyahdayakan tetapan pelayan proksi, keluarkan sebarang sambungan dail naik, dan tetapkan tetapan TCP/IP untuk menapatkan alamat IP secara automatik. Untuk mendapatkan butiran lanjut. Untuk butiran lanjut, rujuk Bab 1 manual pengguna ini.
- Pastikan anda menggunakan kabel ethernet CAT5e atau CAT6.

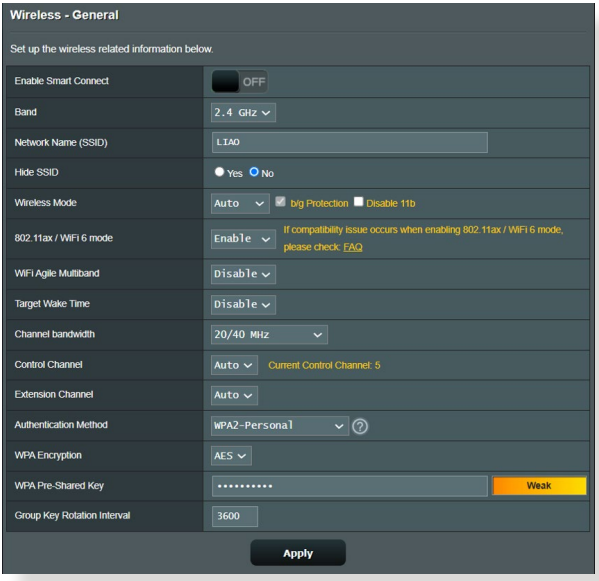
Klien tidak dapat mewujudkan sambungan wayarles dengan penghala.

NOTA: Jika anda mempunyai isu menyambung ke rangkaian 5GHz, pastikan peranti wayarles anda menyokong keupayaan 5GHz atau ciri dwi jalur.

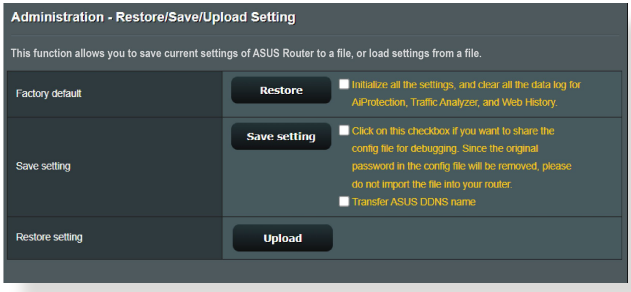
- **Di Luar Jarak Lingkungan**:
  - Letakkan penghala sebih dekat dengan klien wayarles.
- **Pelayan DHCP telah dinyahdayakan:**
  1. Lancarkan Web GUI. Pergi ke **General (Am)** > **Network Map (Peta Rangkaian)** > **Clients (Klien)** dan cari peranti yang anda ingin sambung ke penghala.
  2. Jika anda tidak boleh mencari peranti dalam **Network Map (Peta Rangkaian)**, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **LAN** > senarai **DHCP Server (Pelayan DHCP)**, **Basic Config (Konfigurasi Asas)**, pilih **Ya** pada **Enable the DHCP Server (Dayakan Pelayan DHCP)**.



- SSID telah disembunyikan. Jika peranti anda boleh mencari SSID dari penghala lain tetapi tidak boleh mencari SSID penghala anda, pergi ke **Advanced Settings (Tetapan Lanjutan)** > **Wireless (Wayarles)** > **General (Am)**, pilih **No (Tidak)** pada **Hide SSID (Sembunyi SSID)**, dan pilih **Auto** pada **Control Channel (Saluran Kawalan)**.



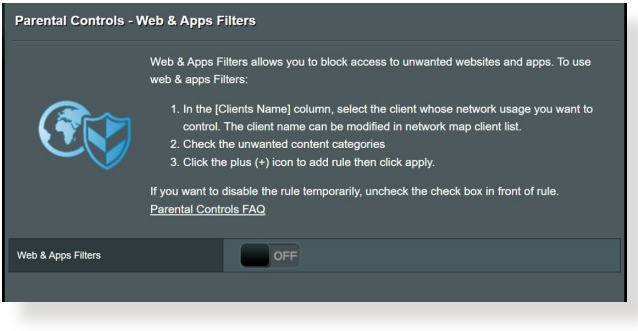
- Jika anda menggunakan adapter LAN wayarles, periksa jika saluran wayarles yang digunakan mengikut saluran tersedia di negara/kawasan anda. Jika tidak, laraskan saluran, lebar jalur saluran, dan mod wayarles.
- Jika anda masih tidak dapat bersambung ke penghala secara wayarles, anda boleh menetap semula tetapan lalai kilang. Dalam GUI penghala, klik **Administration (Pentadbiran)** > **Restore/Save/Upload Setting (Tetapan Pemulihan/Simpan/Muat Naik)**, dan klik **Restore (Pemulihan)**.



Internet tidak dapat diakses.

- Periks jika penghala anda boleh bersambung ke alama IP WAN ISP anda. Untuk melakukannya, lancarkan GUI web dan pergi ke **General (Am)** > **Network Map (Peta Rangkaian)**, dan periksa **Internet Status (Status Internet)**.
- Jika penghala anda tidak boleh bersambung ke alamat IP WAN ISP anda, cuba mula semula rangkaian anda seperti yang diterangkan dalam bahagian **Restart your network in following sequence (Mula semula rangkaian anda dalam urutan berikut)** di bawah **Basic Troubleshooting (Penyelesai Masalah Asas)**.

- Peranti telah disekat melalui fungsi Kawalan Ibu Bapa. Pergi ke **General (Am)** > **Parental Controls (Kawalan Ibu Bapa)** dan lihat jika peranti dalam senarai. Jika peranti disenaraikan di bawah **Client Name (Nama Klien)**, buang peranti menggunakan butang **Delete (Padam)** atau laraskan Tetapan Pengurusan Masa.



- Jika masih tiada akses Internet, cuba but semula komputer anda dan sahkan alamat IP rangkaian dan alamat get laluan.

Anda terlupa SSID (nama rangkaian) atau kata laluan rangkaian

- Sediakan SSID dan kunci penyulitan baru melalui sambungan berwayar (kabel Ethernet). Lancarkan GUI web, pergi ke **Network Map (Peta Rangkaian)**, klik ikon penghala, masukkan SSID dan kunci penyulitan baru, dan kemudian klik **Apply (Guna)**.
- Tetap semula penghala anda ke tetapan lalai. Lancarkan GUI web, pergi ke **Administration (Pentadbiran)** > **Restore/Save/ Upload Setting (Tetapan Pemulihan/Simpan/Muat Naik)**, dan klik **Restore (Pemulihan)**.

Bagaimanakah anda memulihkan sistem kepada tetapan lalainya?

- Pergi ke **Administration (Pentadbiran)** > **Restore/Save/ Upload Setting (Tetapan Pemulihan/Simpan/Muat Naik)**, dan klik **Restore (Pemulihan)**.

Naik taraf perisian tegar gagal.

Lancarkan mod penyelamat dan jalankan utiliti Pemulihan Perisian Tegar. Rujuk bahagian **4.2 Firmware Restoration (Pemulihan Perisian Tegar)** mengenai bagaimana hendak menggunakan uiliti Pemulihan Perisian Tegar.

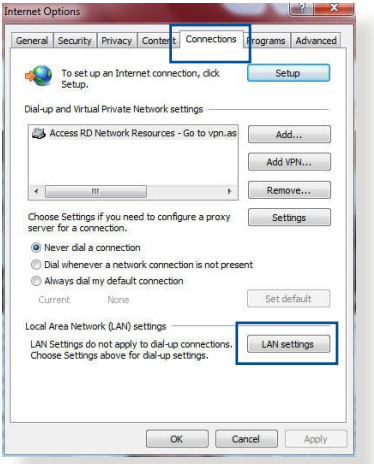
Tidak dapat mengakses GUI Web

Sebelum anda mengkonfigurasikan penghala wayarles anda, lakukan langkah yang diterangkan dalam bahagian ini untuk komputer hos dan klien rangkaian anda.

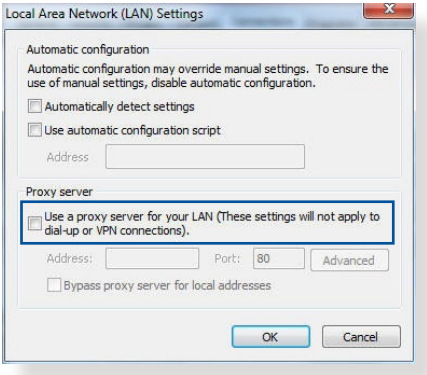
A. Nyahdayakan sebarang pelayan proksi yang dikonfigurasikan.

Windows®

1. Klik **Start (Mula)** > **Internet Explorer** untuk melancarkan penyemak imbas.
2. Klik **Tools (Alatan)** > **Internet options (Pilihan Internet)** > **Connections (Sambungan)** > **LAN settings (Tetapan LAN)**.

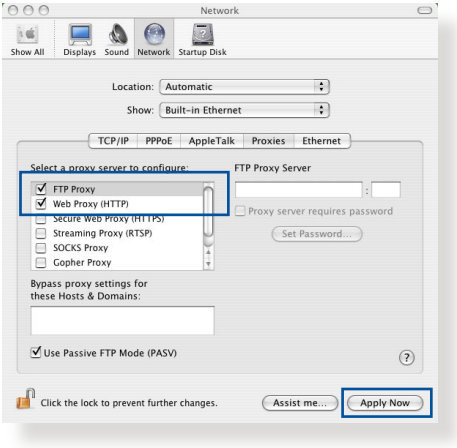


3. Dari tetingkap Local Area Network (LAN) Settings, buang tanda **Use a proxy server for your LAN (Gunakan pelayan proksi untuk LAN anda)**.
4. Klik **OK** setelah selesai.



MAC OS

1. Dari penyemak imbas Safari anda, klik **Safari (Safari)** > **Preferences (Keutamaan)** > **Advanced (Lanjutan)**> **Change Settings... (Tukar Tetapan...)**.
2. Dari skrin Network (Rangkaian), buang tanda **FTP Proxy (FTP Proksi)** dan **Web Proxy (HTTP) (Proksi Web)**.



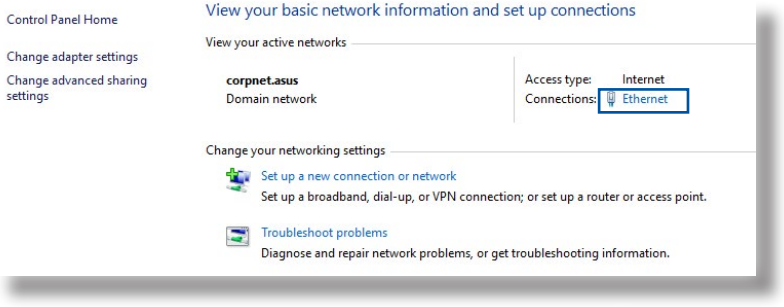
3. Klik **Apply Now (Guna Sekarang)** setelah selesai.

NOTA: Rujuk ciri bantuan penyemak imbas anda untuk butiran mengenai menyahdaya pelayan proksi.

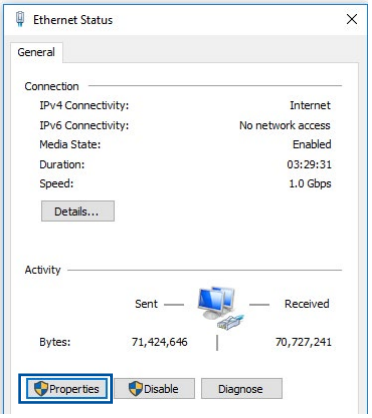
B. Menetapkan tetapan TCP/IP untuk dapatkan alamat IP secara automatik.

Windows®

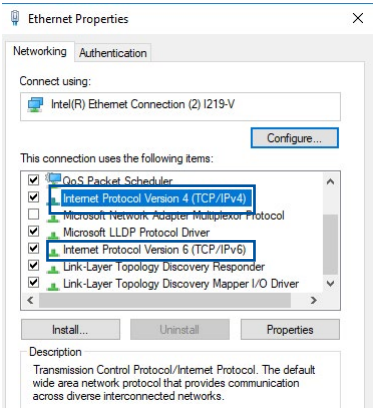
1. Klik **Start (Mula)** > **Control Panel (Panel Kawalan)** > **Network and Sharing Center (Rangkaian dan Pusat Perkongsian)**, kemudian klik sambungan rangkaian untuk memaparkan tetingkap statusnya.



2. Klik **Sifat** untuk memaparkan tetingkap Sifat Ethernet.



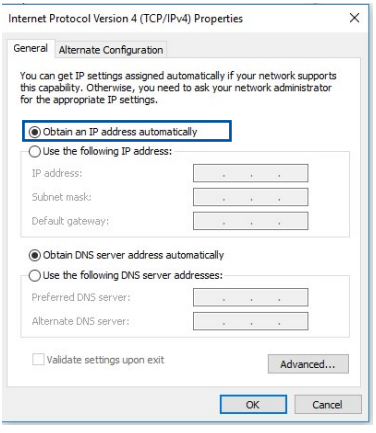
3. Pilih **Protokol Internet Versi 4 (TCP/IPv4)** atau **Protokol Internet Versi 6 (TCP/IPv6)**, kemudian klik **Properties (Ciri-ciri)**.



4. Untuk mendapatkan tetapan IP IPv4 secara automatik, tandakan **Obtain an IP address automatically (Dapatkan alamat IP secara automatik)**.

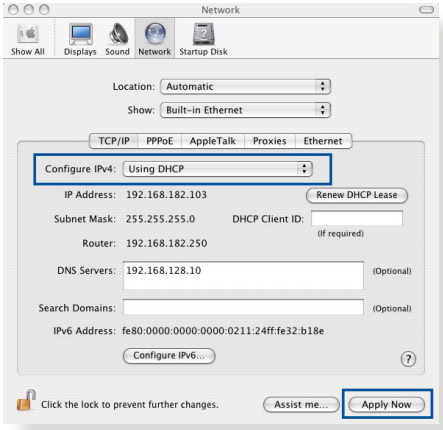
   Untuk mendapatkan tetapan IP IPv6 secara automatik, tandakan **Obtain an IP address automatically (Dapatkan alamat IP secara automatik)**.

5. Klik **OK** setelah selesai.



MAC OS

1. Klik ikon Apple terletak di bahagian atas sebelah kiri skrin anda.
2. Klik **System Preferences (Keutamaan Sistem)** > **Network (Rangkaian)** > **Configure... (Konfigurasi...)**.
3. Dari tab **TCP/IP**, pilih **Using DHCP (Menggunakan DHCP)** dalam senarai jatuh bawah **Configure IPv4 (Konfigurasi IPv4)**.



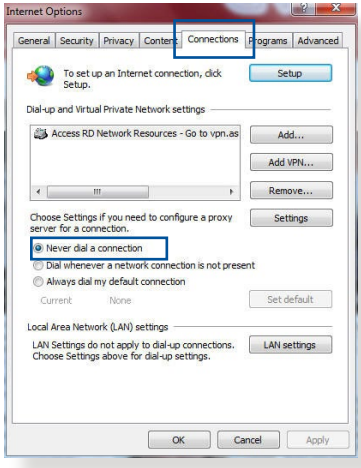
4. Klik **Apply Now (Guna Sekarang)** setelah selesai.

NOTA: Rujuk bantuan dan ciri sokongan sistem operasi anda untuk butiran mengenai mengkonfigurasi tetapan TC/IP komputer anda.

C. Nyahdayakan sambungan dailan, jika didayakan.

Windows®

1. Klik **Start (Mula)** > **Internet Explorer** untuk melancarkan penyemak imbas.
2. Klik tab **Tools (Alatan)** > **Internet options (Pilihan Internet)** > **Connections (Sambungan)**.
3. Tandakan **Never dial a connection**.
4. Klik **OK** setelah selesai.



NOTA: Rujuk ciri bantuan penyemak imbas anda untuk butiran mengenai menyahdaya sambungan dailan.

Lampiran

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

Maklumat keselamatan

Apabila menggunakan produk ini, sentiasa patuhi langkah berjaga-jaga asas, termasuk tetapi tidak terhad pada berikut:

AMARAN!

- Kord bekalan kuasa mesti dipalam masuk ke salur keluar soket yang disediakan dengan pembumian yang sesuai. Sambungkan peralatan hanya ke salur keluar soket berdekatan yang mudah diakses.
- Jika Penyesuai, jangan cuba untuk membetulkannya sendiri. Hubungi juruteknik servis bertauliah atau peruncit anda.
- JANGAN guna kord kuasa, aksesori atau persisian lain yang rosak.
- JANGAN pasang peralatan ini lebih tinggi daripada 2 meter.
- Dalam persekitaran dengan suhu ambien antara 0℃(32℉) dan 40℃(104℉).
- Baca garis panduan operasi dan julat suhu yang diberikan sebelum menggunakan produk.
- Berikan perhatian khusus kepada keselamatan diri semasa menggunakan peranti ini di lapangan terbang, hospital, stesen minyak dan garaj profesional.
- Gangguan peranti perubatan: Kekalkan jarak minimum sekurang-kurangnya 15 cm (6 inci) di antara peranti perubatan yang diimplan dan produk ASUS untuk mengurangkan risiko gangguan.
- Sila gunakan produk ASUS dalam keadaan penerimaan yang baik untuk meminimumkan tahap radiasi.
- Jauhkan peranti daripada wanita hamil dan bahagian bawah abdomen remaja.
- JANGAN gunakan produk ini jika kerosakan jelas boleh diperhatikan atau ia telah basah atau rosak atau diubah suai. Cari perkhidmatan servis untuk mendapatkan bantuan.

AMARAN!

- JANGAN letakkan pada permukaan kerja yang tidak rata atau tidak stabil.
- JANGAN letakkan atau jatuhkan objek di bahagian atas produk. Elakkan produk terdedah kepada kejutan mekanikal seperti penghancuran, pembengkokan, pembocoran atau pencincangan.
- JANGAN tanggalkan, buka, gelombang mikro, bakar, cat, atau sumbat sebarang objek asing ke dalam produk ini.
- Rujuk label perkadaran di bahagian bawah produk anda dan pastikan penyesuai kuasa anda mematuhi perkadaran ini.
- Jauhkan produk daripada api dan sumber haba.
- JANGAN dedahkan kepada atau gunakan berdekatan cecair, hujan atau kelembapan. JANGAN gunakan produk semasa ribut elektrik.
- Sambungkan litar output PoE produk ini secara eksklusif ke rangkaian PoE, tanpa penghalaan ke kemudahan luaran.
- Untuk mengelak bahaya kejutan elektrik, putuskan sambungan kabel kuasa daripada salur keluar elektrik sebelum menempatkan semula sistem.
- Hanya gunakan aksesori yang telah diluluskan oleh pengeluar peranti untuk berfungsi dengan model ini. Penggunaan jenis aksesori lain boleh membatalkan waranti atau melanggar peraturan dan undang-undang tempatan, dan boleh menimbulkan risiko keselamatan. Hubungi penjual tempatan anda untuk ketersediaan aksesori yang dibenarkan.
- Menggunakan produk ini dengan cara yang tidak disyorkan dalam arahan yang diberikan boleh menyebabkan risiko kebakaran atau kecederaan diri.

Perkhidmatan dan Sokongan

Lawati laman web kami yang pelbagai bahasa di https://www.asus.com/support.