FA22958

REPUBLIC OF GAMERS

USER MANUAL

ROG Rapture GT6

ROG Rapture AX10000 سه‌بانده روتر شبکه باز‌ی

FA22958
وي راش اول
دسامبر 2023

فهرست مطالب

فهرست مطالب

فهرست مطالب

فهرست مطالب

1 آشنایی با روتر بی سیم خود

1.1 خوش آمدید!

به خاطر خرید روتر بی سیم ROG Rapture از شما متشکریم!

زیبای روتر دارای باند 2.4 گیگاهرتز, 5 گیگاهرتز-1 و 5 گیگاهرتز-2 برای پخش همزمان اچ دی بی سیم به طور بی همتا؛ سرور SMB، سرور UPnP AV، و سرور FTP برای اشتراک گذاری 24 ساعت و هر روزه فایل ها؛ قابلیت اداره 300,000 جلسه؛ و فناوری شبکه سبز ASUS است، که راهکاری برای صرفه جویی در انرژی تا 70% ارائه می دهد.

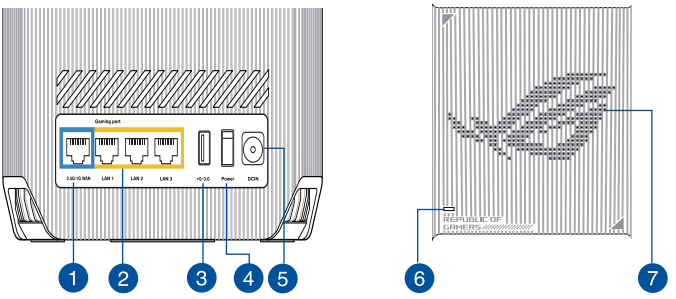
1.2 محتویات بسته

☑ روتر بی سیم ROG Rapture
☑ آداپتور برق متناوب
☑ کابل شبکه (RJ-45)
☑ راهنمای شروع سریع

:ادرکذت

- اگر هر یک از اقلام آسیب دیده یا مفقود شده، برای سؤالات فنی و پشتیبانی با ASUS تماس بگیرید، به فهرست خط مستقیم پشتیبانی ASUS در پشت این دفترچه راهنمای کاربر مراجعه کنید.
- در صورت نیاز آتی به سرویس های ضمانت، از قبیل تعمیر یا تعویض، مواد بسته‌بندی اصلی را نگهداری کنید.

1.3 روتر بی سیم شما



1 **پورت 1GE WAN/2.5 (اینترنت)**
برای برقراری اتصال 1GE WAN/2.5، یک کابل شبکه را داخل این پورت قرار دهید.

2 **پورت های LAN 1 ~ 4**
برای برقراری اتصال LAN، کابل های شبکه را داخل این پورت ها قرار دهید.

3 **پورت USB 3.2 Gen 1x1**
دستگاه سازگار USB 3.2 Gen 1x1 مانند هارد دیسک USB یا درایو فلش USB را در این پورت وارد کنید.

4 **سوییچ روشن/خاموش**
این سوییچ را فشار دهید تا سیستم روشن یا خاموش شود.

5 **پورت برق (ورودی برق مستقیم)**
آداپتور برق متناوب موجود را داخل این پورت قرار دهید و روتر خود را به یک منبع برق وصل کنید.

6 **نشانگر LED**

- آبی ثابت: ROG Rapture GT6 برای اندازه‌گیری سرعت اینترنت مناسب است
- سفید ثابت: ROG Rapture GT6 آنلاین است و به درستی کار می کند
- قرمز ثابت: ROG Rapture GT6 به اینترنت وصل نیست
  تا اتصال مجدد از روتر قطع شده است
- زرد ثابت: سیگنال بین روتر ROG Rapture GT6 و مجدد ضعیف است

7 **Aura RGB**
به کاربر امکان می دهد Aura RGB را از داشبورد روشن یا خاموش کنند.

تذکرها:

- فقط از آداپتوری که در بسته‌بندی قرار دارد استفاده کنید. استفاده از سایر آداپتورها ممکن است به دستگاه آسیب برساند.

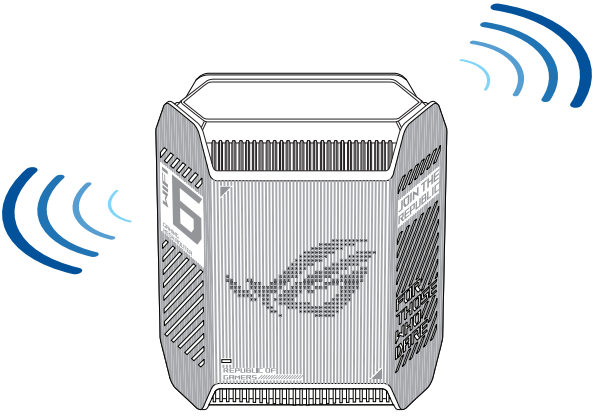
- **مشخصات:**

آداپتور برق مستقیم	خروجی برق مستقیم: +19 ولت با جریان حداکثر 2.37 آمپر +19.5 ولت با جریان حداکثر 2.31 آمپر		
دمای کارکرد	0~40°C	نگهداری	0~70°C
رطوبت کارکرد	50~90%	نگهداری	20~90%

1.4 محل قرارگیری روتر

برای بهترین انتقال سیگنال بی سیم بین روتر بی سیم و دستگاه های شبکه متصل به آن، مطمئن شوید که:

- روتر بی سیم را جهت ایجاد حداکثر پوشش بی سیم برای دستگاه های شبکه در مرکز محل قرار دهید.
- دستگاه را دور از موانع فلزی و همچنین دور از نور مستقیم خورشید نگه دارید.
- دستگاه را دور از دستگاه‌های 802.11g یا دستگاه‌های Wi-Fi فقط 20 مگاهرتز، لوازم رایانه‌ای 2.4 گیگاهرتز، دستگاه‌های بلوتوث، تلفن های بی سیم، مبدل ها، موتورهای قوی، لامپ های فلورسنت، مایکروفر، یخچال و سایر تجهیزات صنعتی نگه دارید تا از تداخل یا افت سیگنال جلوگیری شود.
- همیشه به جدیدترین نرم افزار ثابت به روزرسانی کنید. به وبسایت ASUS به نشانی **http://www.asus.com** مراجعه کنید تا جدیدترین به روزرسانی های نرم افزار ثابت را دریافت کنید.



1.5 الزامات نصب

برای راه‌اندازی شبکه بی سیم خود، به یک رایانه با الزامات زیر نیاز دارید:

- پورت اترنت RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- IEEE 802.11a/b/g/n/ac/ax قابلیت بی‌سیم
- نصب بودن سرویس TCP/IP
- مرورگر وب نظیر Internet Explorer، Firefox، Safari یا Google Chrome

---

تذکرها:

- اگر رایانه شما دارای قابلیت بی‌سیم نیست، می توانید یک آداپتور IEEE 802.11a/b/g/n/ac/ax به رایانه خود وصل کنید تا بتوانید به شبکه متصل شوید.
- با فن آوری باند سه گانه، روتر بی سیم همزمان از سیگنال های 2.4 گیگاهرتز, 5 گیگاهرتز-1و 5 گیگاهرتز-2 پشتیبانی می کند. این به شما امکان می دهد فعالیتهای مربوط به اینترنت را مانند جستجو در اینترنت یا خواندن/ نوشتن ایمیل با استفاده از باند 2.4 گیگاهرتز انجام دهید و در عین حال فایلهای با کیفیت صوتی/تصویری را مانند فیلم یا موسیقی با استفاده از باندهای 5 گیگاهرتز پخش کنید.
- برخی دستگاههای IEEE 802.11n که می خواهید به شبکه خود وصل کنید ممکن است از باند 5 گیگاهرتز پشتیبانی نکنند. برای اطلاع از مشخصات به دفترچه راهنمای دستگاه مراجعه کنید.
- طول کابل های اترنت RJ-45 که برای متصل کردن دستگاه‌های شبکه استفاده خواهند شد، نباید از 100 متر بیشتر باشد.

مهم!

- بعضی از آداپتورهای بی سیم ممکن است مشکل اتصال به 802.11ax WiFi APs داشته باشند.
- اگر با چنین مشکلی مواجه هستید، لطفاً درایور را به جدیدترین نسخه به روز رسانی کنید. به سایت پشتیبانی رسمی سازنده مراجعه کنید که درایورهای نرم افزار، به روزرسانی ها، و سایر اطلاعات مرتبط موجود است.
  - Realtek: https://www.realtek.com/en/downloads
  - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi
  - Intel: https://downloadcenter.intel.com/

---

2 شروع به کار

2.1 راه اندازی روتر

مهم!

- برای جلوگیری از بروز اشکالات احتمالی راه اندازی، هنگام راه‌اندازی روتر بی‌سیم، از یک اتصال باسیم استفاده کنید.
- پیش از راه اندازی روتر بی‌سیم ASUS خود، موارد زیر را انجام دهید:
- اگر یک روتر موجود را تعویض می کنید، اتصال آن را از شبکه قطع کنید.
- کابل ها/سیم ها را از مودم تنظیم شده کنونی جدا کنید. اگر مودم شما دارای باتری پشتیبان است، آن را نیز جدا کنید.
- مودم کابلی و رایانه خود را مجدداً راه اندازی کنید (توصیه می شود).

هشدار!

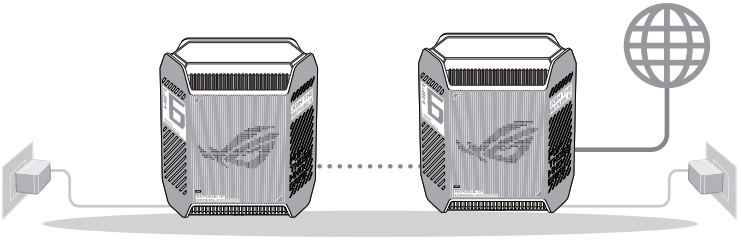
- سیم برق باید به پریزی که دارای اتصال مناسب به زمین باشد وصل شود. دستگاه را فقط به پریزی در نزدیک خودتان وصل کنید که به راحتی قابل دسترسی باشد.
- اگر آداپتور شکسته است، خودتان آن را تعمیر نکنید. با تکنیسین مجرب خدمات یا فروشنده خود تماس بگیرید.
- از سیم برق، وسیله های جانبی، یا سایر وسیله های خراب استفاده نکنید.
- این دستگاه را در ارتفاع بیشتر از 2 متر نصب نکنید.
- از این دستگاه در محیط هایی که دمای بین 0 درجه سانتی گراد (32 درجه فارنهایت) و 40 درجه سانتی گراد (104 درجه فارنهایت) دارند استفاده کنید.

A. اتصال با سیم

نکته: می توانید از کابل مستقیم یا کابل کراس برای اتصال با سیم استفاده کنید.

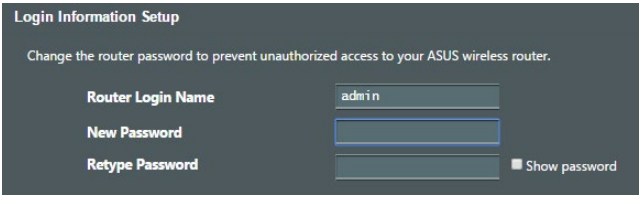
برای راه‌اندازی روتر بی سیم خود با استفاده از یک اتصال با سیم:

1. روتر را به پریز برق وصل کنید و آن را روشن کنید. کابل شبکه را از کامپیوتر به پورت LAN روی روتر وصل کنید.



2. وقتی مرورگر وب را باز می کنید، GUI به صورت خودکار راه اندازی می شود. اگر به صورت خودکار راه اندازی نشد، به سایت http://www.asusrouter.com وارد شوید.

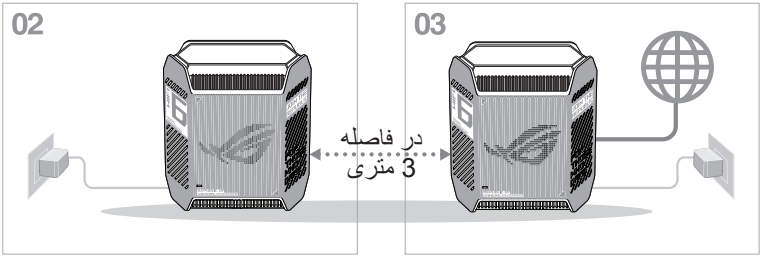
3. یک رمز عبور برای روتر تنظیم کنید تا از دسترسی غیرمجاز جلوگیری شود.



B. اتصال بی سیم

برای راه‌اندازی روتر بی سیم خود با استفاده از یک اتصال بی سیم:

1. روتر را به پریز برق وصل کنید و آن را روشن کنید.



2. به نام شبکه (SSID) نمایش داده شده بر روی برچسب محصول در پشت روتر وصل شوید. برای اینکه ایمنی شبکه بهتری داشته باشید، از یک SSID غیر تکراری استفاده کنید و رمز عبوری را به آن اختصاص دهید.

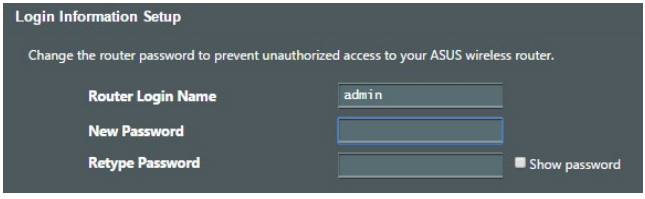
نام Wi-Fi (SSID):	ASUS_XX_GT6

* **XX** دو رقم آخر آدرس MAC 2.4 گیگاهرتز است. آن را می توانید روی برچسب موجود در پشت ROG روتر مشاهده کنید.

3. آبعد از اتصال، وقتی مرورگر وب را باز می کنید، GUI به صورت خودکار راه اندازی می شود. اگر به صورت خودکار راه اندازی نشد، به سایت http://www.asusrouter.com وارد شوید.
4. یک رمز عبور برای روتر تنظیم کنید تا از دسترسی غیرمجاز جلوگیری شود.

تذکرها:

- برای اطلاع از جزئیات اتصال به یک شبکه بی سیم، به دفترچه راهنمای کاربر آداپتور WLAN مراجعه کنید.
- برای تغییر تنظیمات امنیتی شبکه خود، به **بخش تغییر تنظیمات امنیتی بی سیم** در فصل 3 این دفترچه راهنمای کاربر مراجعه کنید.



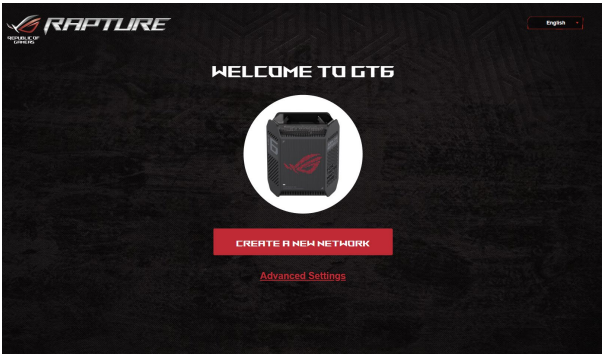
2.2 تنظیم سریع اینترنت با تشخیص خودکار (QIS)

عملکرد تنظیم اینترنت سریع (QIS) شما را راهنمایی می کند تا به سرعت اتصال اینترنت را برقرار کنید.

نکته: وقتی برای اولین بار اتصال اینترنت را برقرار می کنید، دکمه بازنشانی را روی روتر بی سیم فشار دهید تا تنظیمات به موارد پیش فرض کارخانه بازگردد.

برای استفاده از QIS با تشخیص خودکار:

1. یک مرورگر وب را باز کنید. به ASUS Setup Wizard (راه اندازی اینترنتی سریع) هدایت می شوید. در غیر اینصورت به صورت دستی آدرس http://www.asusrouter.com را وارد کنید.



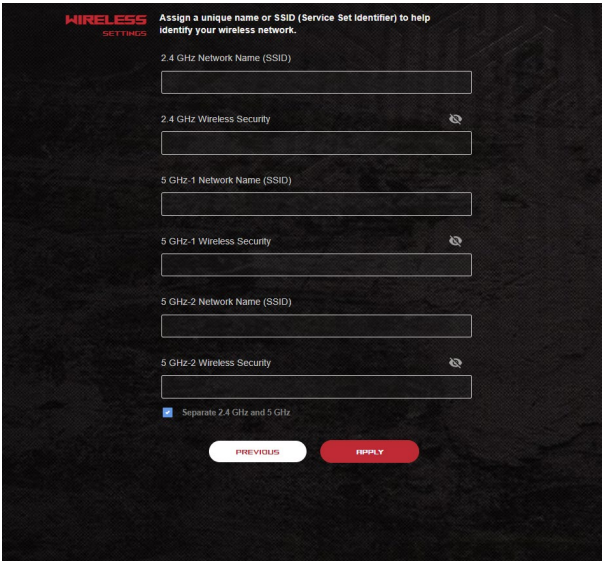
2. روتر بی سیم به صورت خودکار تشخیص می دهد آیا نوع اتصال ISP این موارد است: **PPTP**، **PPPoE**، **Dynamic IP** و **L2TP**. اطلاعات لازم برای نوع اتصال ISP را وارد کنید.

مهم! اطلاعات لازم مربوط به نوع اتصال اینترنتی را از ISP خودتان بپرسید.

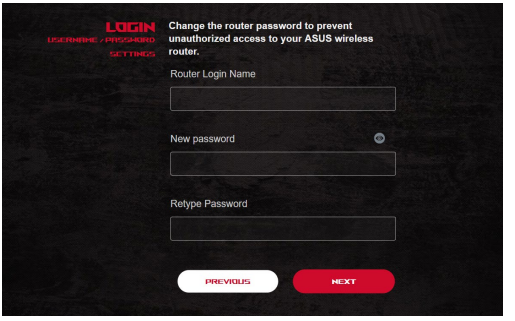
نکته:

- تشخیص خودکار نوع اتصال ISP شما زمانی انجام می شود که روتر بی سیم را برای اولین بار پیکربندی می کنید یا زمانی که روتر بی سیم به تنظیمات پیش فرض خود باز می گردد.
- اگر QIS نتواند نوع اتصال اینترنت شما را شناسایی کند، روی **"Skip to manual setting"** کلیک کنید و به صورت دستی تنظیمات اتصالتان را پیکربندی کنید.

3. نام شبکه بی سیم را اختصاص دهید (SSID) و کلید امنیتی را برای اتصال بی سیم 2.4 گیگاهرتز, 5 گیگاهرتز-1 و 5 گیگاهرتز-2 مشخص کنید. بعد از پایان کار روی **"Apply (اعمال)"** کلیک کنید.



4. در صفحه **Login Information Setup (راه اندازی اطلاعات ورود به سیستم)**، رمز عبور ورود به سیستم روتر را تغییر دهید تا به روتر بی سیم دسترسی غیرمجاز وجود نداشته باشد.



نکته: نام کاربری و رمز عبور ورود به سیستم روتر بی سیم با نام شبکه 2-5/1-5/2.4 (SSID) گیگاهرتز و کلید ایمنی متفاوت است. نام کاربری و رمز عبور ورود به سیستم روتر بی سیم به شما امکان می دهد به Web GUI وارد شوید تا تنظیمات روتر بی سیم را پیکربندی کنید. نام شبکه 2-5/1-5/2.4 گیگاهرتز (SSID) و کلید ایمنی به دستگاه های Wi-Fi اجازه می دهد وارد سیستم شوند و به شبکه 2-5/1-5/2.4 گیگاهرتز شما متصل شوند.

2.3 اتصال به شبکه بی سیم خود

پس از تنظیم روتر بی سیم خود از طریق QIS، می توانید رایانه خود یا سایر دستگاههای هوشمند را به شبکه بی سیم خود وصل کنید.

برای اتصال به شبکه خود:

1. در رایانه خود، روی نماد شبکه در ناحیه اعلان کلیک کنید تا شبکه های بی سیم موجود نمایش داده شود.
2. شبکه بی سیمی که می خواهید به آن وصل شوید را انتخاب کنید، سپس روی **Connect (اتصال)** کلیک کنید.
3. ممکن است لازم باشد کلید امنیتی شبکه را برای یک شبکه بی سیم ایمن وارد کنید، سپس روی **OK (تأیید)** کلیک کنید.
4. صبر کنید تا رایانه شما به طور موفقیت آمیز به شبکه بی سیم متصل شود. وضعیت اتصال نمایش داده می شود و نماد شبکه وضعیت متصل شده را نشان می دهد.

تذکرها:

- برای اطلاع از جزئیات بیشتر درباره پیکربندی تنظیمات شبکه بی سیم خود به فصلهای بعد مراجعه کنید.
- برای اطلاعات بیشتر درباره اتصال آن به شبکه بی سیم خود به دفترچه راهنمای کاربر دستگاه خود مراجعه کنید.

3 پیکربندی تنظیمات کلی و تنظیمات پیشرفته

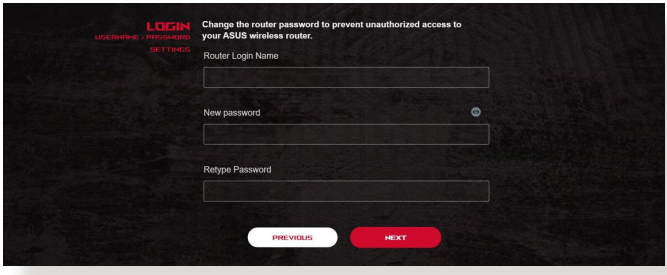
3.1 ورود به رابط گرافیکی کاربر تحت وب

روتر بی سیم بازی TUF شما دارای یک رابط گرافیکی کاربر تحت وب و مستقیم است - مرکز بازی TUF به شما امکان می دهد با استفاده از اطلاعات مفیدی مانند وضعیت دستگاه متصل و مقادیر پینگ سرور-بازی جهانی و همچنین دسترسی سریع به همه ویژگی های جالب بازی، شبکه را به صورت کامل کنترل کنید.

نکته: این ویژگیها ممکن است در نسخه های مختلف نرم افزار ثابت متفاوت باشند.

برای ورود به رابط گرافیکی کاربر تحت وب:

1. مرورگر وب خود را باز کنید، نشانی IP پیش فرض روتر بی سیم خود را به صورت دستی وارد کنید: http://www.asusrouter.com شوید.
2. در صفحه ورود، نام کاربری پیش فرض (**admin**) و رمز عبوری را که در قسمت **Quick Internet Setup (QIS) 2.2 راه اندازی سریع اینترنتی (QIS) with Auto-dection 2.2) با تشخیص خودکار)** تنظیم کرده اید وارد کنید.



3. اکنون می توانید از رابط گرافیکی کاربر تحت وب برای پیکربندی تنظیمات مختلف روتر بی‌سیم ASUS خود استفاده کنید.

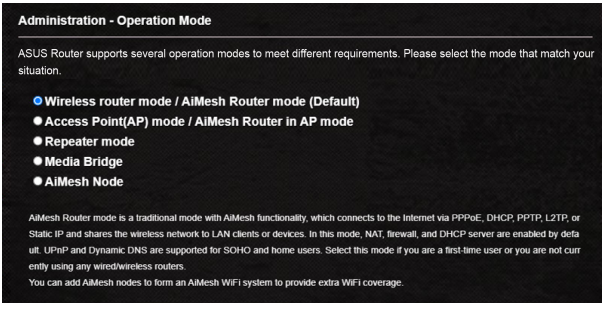
*این تصویر فقط یک مرجع است.

نکته: اگر برای اولین بار به رابط گرافیکی کاربر تحت وب وارد می شوید، به طور خودکار وارد صفحه راه اندازی سریع اینترنت (QIS) می شوید.

3.2 مدیریت

3.2.1 حالت عملکرد

صفحه حالت عملکرد این امکان را به شما می دهد که حالت مناسب شبکه را انتخاب کنید.



برای راه اندازی حالت عملکرد:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Administration (مدیریت)** > زبانه **Operation Mode (حالت عملکرد)** بروید.
2. یکی از این حالت های عملکرد را انتخاب کنید:

- **Wireless router mode / AiMesh Router mode (Default) (حالت روتر بی سیم/حالت روتر AiMesh (به طور پیش فرض)):** در حالت روتر بی سیم، روتر بی سیم به اینترنت متصل می‌شود و دسترسی اینترنتی به دستگاه های موجود در شبکه محلی خود را فراهم می کند.
- **Access Point (AP) mode / AiMesh Router in AP mode (نقطه دسترسی (AP) / حالت حالت AiMesh روتر):** در این حالت روتر، شبکه بی سیم جدیدی روی شبکه موجود ایجاد می‌کند.
- **حالت Repeater (تکرار):** در حالت تکرار GT6 به صورت بی سیم به شبکه بی سیم موجود وصل می شود تا پوشش بی سیم گسترش یابد. در این حالت فایروال، اشتراک گذاری IP، و عملکردهای NAT غیرفعال می شوند.
- **Media Bridge (رابط رسانه):** این تنظیم نیاز به دو روتر بی سیم دارد. دومین روتر به عنوان رابط رسانه عمل می کند تا دستگاه های چندگانه مانند تلویزیون های هوشمند و کنسول های بازی را بتوان از طریق اترنت به آن متصل کرد.

- **AiMesh Node (گره AiMesh)**: برای تنظیم این حالت به حداقل دو روتر ASUS نیاز دارید که از AiMesh پشتیبانی کنند. گره AiMesh را فعال کنید و به سیستم رابط کاربر وب روتر AiMesh وارد شوید تا گره های AiMesh موجود در نزدیکی شما جستجو شود و بتوانید به سیستم AiMesh خودتان ملحق شوید. سیستم AiMesh دارای پوشش کامل خانه و مدیریت متمرکز است

3. روی **Apply (به کارگیری)** کلیک کنید.

نکته: وقتی حالت ها را تغییر دهید روتر دوباره راه اندازی می شود.

3.2.2 سیستم

صفحه **System سیستم** این امکان را به شما می دهد تا تنظیمات روتر بی سیم را پیکربندی کنید.

برای راه اندازی تنظیمات سیستم:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته) > Administration (مدیریت) > System (سیستم)** بروید.
2. می توانید تنظیمات زیر را پیکربندی کنید:

- **Change router login password (رمز عبور ورود روتر را تغییر دهید)**: می توانید رمز عبور و نام ورود روتر بی سیم را با وارد کردن نام و رمز عبور جدید، تغییر دهید.
- **Time Zone (منطقه زمانی)**: برای شبکه خود منطقه زمانی انتخاب کنید.
- **NTP Server (سرور NTP)**: روتر بی سیم برای یکسان کردن زمان به سرور NTP (پروتکل زمان شبکه) دسترسی پیدا می کند.
- **Enable Telnet (فعال کردن تلنت)**: برای فعال کردن خدمات تلنت روی شبکه، روی **Yes (بله)** کلیک کنید. برای غیر فعال کردن تلنت روی **No (خیر)** کلیک کنید.
- **Authentication Method (روش تأیید)**: می توانید برای ایمن کردن دسترسی به روتر HTTP، HTTPS یا هر دو پروتکل را انتخاب کنید.
- **Enable Web Access from WAN (فعال کردن دسترسی به وب از WAN)**: برای اینکه دستگاه های خارج از شبکه بتوانند به تنظیمات GUI روتر بی سیم دسترسی داشته باشند، **Yes (بله)** را انتخاب کنید. برای جلوگیری از دسترسی **No (خیر)** را انتخاب کنید.
- **امکان دسترسی تنها به آدرس IP تعیین شده**: اگر می خواهید آدرس های IP دستگاه هایی که امکان دسترسی به تنظیمات روتر بی سیم GUI از طریق WAN را دارند، تعیین کنید روی **Yes (بله)** کلیک کنید.
- **Client List (فهرست سرویس گیرندگان)**: آدرس های WAN IP دستگاه های شبکه بندی شده که امکان دسترسی به تنظیمات روتر بی سیم را دارند، وارد کنید. همچنین می توانید از این لیست با کلیک کردن **Yes (بله)** در گزینه **Only allow specific IP (فقط اجازه به IP تعیین شده)** استفاده کنید.

3. روی **Apply (به کارگیری)** کلیک کنید.

3.2.3 ارتقای نرم افزار ثابت

نکته: از وب سایت ASUS به نشانی **http://www.asus.com** جدیدترین نرم افزار ثابت را دانلود کنید.

برای ارتقای نرم افزار ثابت:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Administration (مدیریت)** > **Firmware Upgrade (ارتقای نرم افزار ثابت)**.
2. در قسمت **New Firmware File (فایل نرم افزار ثابت جدید)**، روی **Browse (مرور)** کلیک کنید تا فایل دانلود شده را بیابید.
3. روی **Upload (بارگذاری)** کلیک کنید.

تذکرها:

- وقتی فرآیند ارتقا کامل شد، چند لحظه صبر کنید تا سیستم دوباره راه اندازی شود.
- اگر فرآیند ارتقا با مشکل مواجه شد، روتر بی سیم به طور خودکار به حالت نجات می رود و نشانگر LED روی پنل جلو به آهستگی شروع به چشمک زدن می کند. برای بهبود بخشیدن و بازیابی سیستم، به بخش **4.2 بازیابی نرم افزار ثابت مراجعه کنید**.

3.2.4 Restore/Save/Upload Setting (تنظیمات بازیابی/ذخیره/بارگذاری)

برای بازیابی یا ذخیره یا بارگذاری تنظیمات روتر بی سیم:

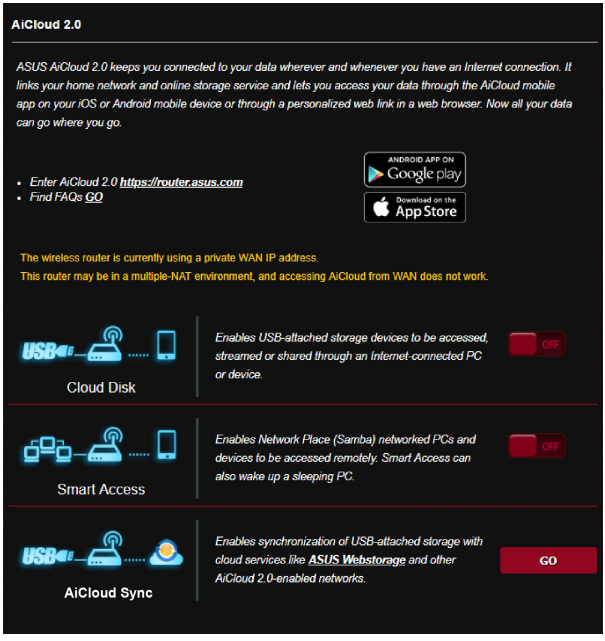
1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Administration (مدیریت)** > **Restore/Save/Upload Setting (بازیابی یا ذخیره یا بارگذاری تنظیمات)** بروید.
2. وظایفی را که می خواهید انجام دهید، انتخاب کنید:

- برای بازیابی تنظیمات کارخانه پیش فرض، روی **Restore (بازیابی)** کلیک کنید سپس در پیام تأیید روی **OK (تأیید)** کلیک کنید.
- برای ذخیره تنظیمات کنونی سیستم، روی **Save (ذخیره)** کلیک کنید، به پوشه‌ای بروید که می‌خواهید فایل را در آنجا ذخیره کنید و روی **Save (ذخیره)** کلیک کنید.
- برای بازیابی از فایل تنظیمات ذخیره شده سیستم، روی **Browse (مرور)** کلیک کنید تا فایل را قرار دهید، سپس روی **Upload (بارگذاری)** کلیک کنید.

مهم! اگر با مشکلی مواجه شدید، جدیدترین نسخه نرم افزار را بارگذاری کنید و تنظیمات جدید را پیکربندی کنید. روتر را به تنظیمات پیش فرض بازیابی نکنید.

AiCloud 2.0 3.3

AiCloud 2.0 نوعی برنامه کاربردی سرویس ابری است که امکان ذخیره، همگام سازی، به اشتراک گذاری و دسترسی به فایل هایتان را به شما می دهد.



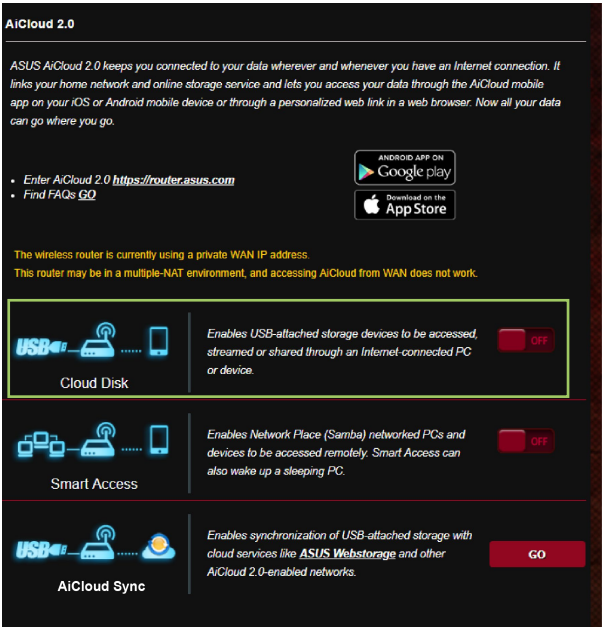
برای استفاده از AiCloud:

1. از فروشگاه Google Play یا Apple، برنامه کاربردی ASUS AiCloud را دانلود کنید و آن را روی دستگاه هوشمند خود نصب کنید.
2. دستگاه هوشمند را به شبکه وصل کنید. دستورالعمل ها را دنبال کنید تا فرآیند تنظیم AiCloud را کامل کنید.

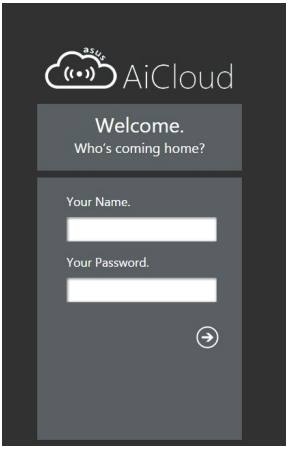
3.3.1 دیسک ابری

برای ایجاد یک دیسک ابری:

1. دستگاه حافظه USB را در روتر بی سیم وارد کنید.
2. **Cloud Disk (دیسک ابری)** را روشن کنید.

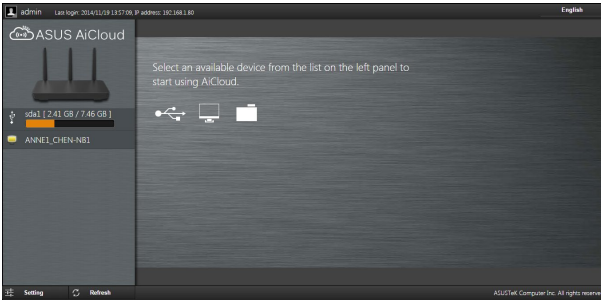


3. به **http://www.asusrouter.com** بروید و حساب کاربری و رمز عبور را وارد کنید. برای داشتن تجربه کاربری بهتر، توصیه می کنیم که از **Google Chrome** یا **Firefox** استفاده کنید.



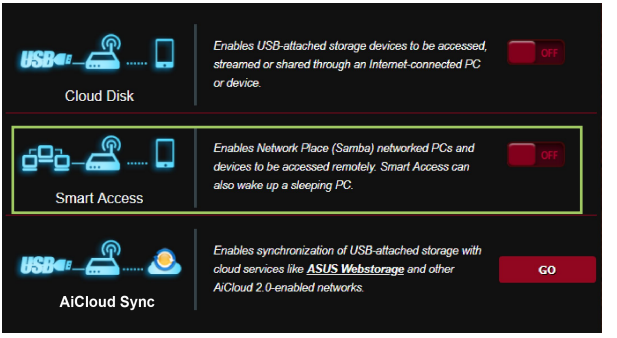
4. اکنون می توانید به فایل های دیسک ابری روی دستگاه های متصل به شبکه دسترسی پیدا کنید.

نکته: هنگام دسترسی به دستگاه های متصل به شبکه، باید نام کاربری و رمز عبور دستگاه را به طور دستی وارد کنید، نام کاربری و رمز عبور به دلایل امنیتی در AiCloud ذخیره نمی شوند.



3.3.2 دسترسی هوشمند

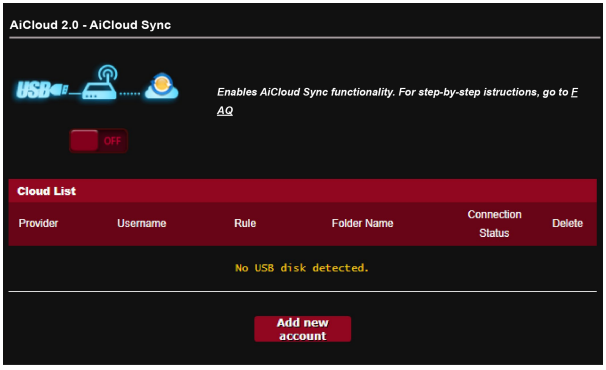
عملکرد دسترسی هوشمند امکان دسترسی آسان تر به شبکه خانگی را از طریق نام دامنه روتر خودتان فراهم می سازد.



تذکرها:

- می توانید برای روتر با ASUS DDNS یک نام دامنه ایجاد کنید. برای اطلاع از جزئیات بیشتر، به بخش **DDNS 3.20.6** مراجعه کنید.
- AiCloud به صورت پیش فرض، اتصال HTTPS امن فراهم می کند. برای استفاده از دیسک ابری و دسترسی هوشمند ایمن https://[yourASUSDDNSname].asuscomm.com را وارد کنید.

3.3.3 یکسان سازی AiCloud

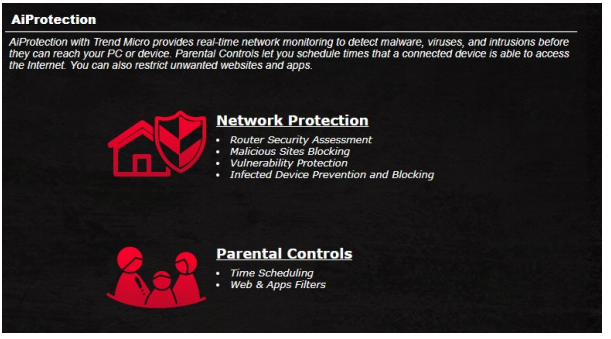


برای استفاده از یکسان سازی AiCloud:

1. AiCloud را راه اندازی کنید، روی **AiCloud Sync (همگام سازی هوشمند) > Go (برو)** کلیک کنید.
2. برای فعال کردن همگام سازی AiCloud، **ON (روشن)** را انتخاب کنید.
3. روی **Add new account (اضافه کردن حساب جدید)** کلیک کنید.
4. رمز عبور حساب ASUS WebStorage را وارد کنید و دایرکتوری مورد نظر برای همگام سازی با WebStorage را انتخاب کنید.
5. روی **Apply (به کارگیری)** کلیک کنید.

AiProtection 3.4

AiProtection امکان نظارت لحظه ای را در اختیارتان قرار می دهد که سبب می شود بتوانید بدافزار، نرم افزارهای جاسوسی و دسترسی ناخواسته راشناسایی کنید. همچنین وبسایت ها و برنامه های ناخواسته را فیلتر می کند و به شما امکان می دهد زمانی را تنظیم کنید که دستگاه متصل بتواند به اینترنت دسترسی داشته باشد.



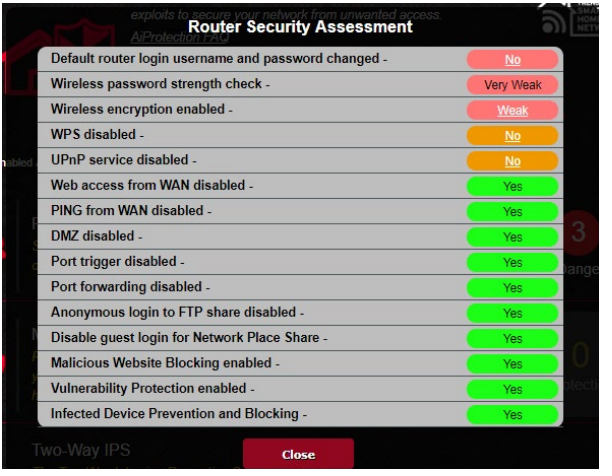
3.4.1 پیکربندی AiProtection

AiProtection مانع از استفاده بدون مجوز از شبکه می شود و شبکه را ایمن سازی می کند تا دسترسی ناخواسته به آن وجود نداشته باشد.

برای پیکربندی AiProtection:

1. از صفحه پیمایش، به زبانه های **General (موارد کلی)** > **AiProtection** بروید.
2. از صفحه اصلی AiProtection، روی **Network Protection (محافظت شبکه)** کلیک کنید.
3. از زبانه محافظت شبکه روی **Scan (اسکن)** کلیک کنید.

نتایج جستجو در صفحه **Router Security Assessment (ارزیابی ایمنی روتر)** نمایش داده می شود.



مهم! مواردی که با **Yes (بله)** در صفحه علامت گذاری **Router Security Assessment (ارزیابی ایمنی روتر)** شده اند، ایمن هستند.

---

4. (اختیاری) از صفحه **Router Security Assessment (ارزیابی ایمنی روتر)** به صورت دستی مواردی را که با **No (خیر)**، **Weak (ضعیف)** یا **Very Weak (خیلی ضعیف)** علامت گذاری شده اند پیکربندی کنید. برای انجام این کار:
   a. روی موردی کلیک کنید تا به صفحه تنظیمات آن مورد بروید.
   b. از صفحه تنظیمات امنیتی آن مورد، تغییرات لازم را پیکربندی کرده و انجام دهید و پس از پایان کار روی **Apply (اعمال)** کلیک کنید.
   c. به صفحه **Router Security Assessment (ارزیابی ایمنی روتر)** برگردید و برای خروج از صفحه روی **Close (بستن)** کلیک کنید.
5. در پیام تأیید روی **OK (تأیید)** کلیک کنید

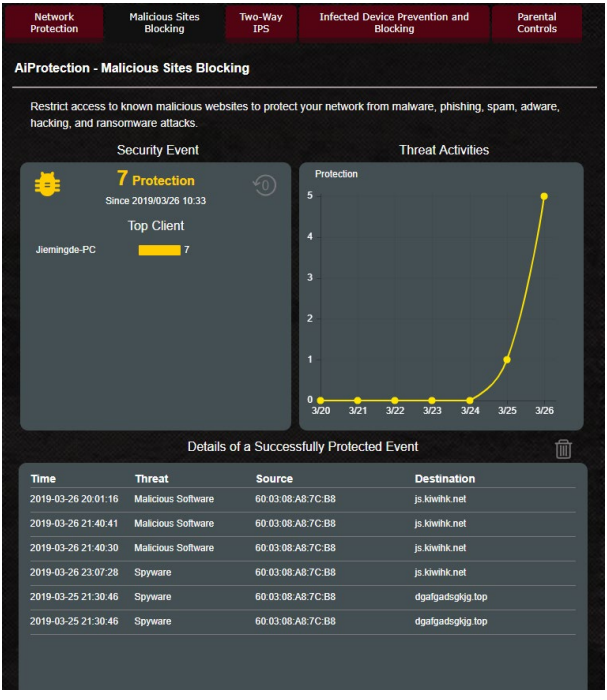
3.4.2 مسدود کردن سایت های مشکوک

این ویژگی دسترسی به وبسایت های مشکوک شناخته شده در پایگاه داده اینترنتی را برای محافظت همیشه به روز محدود می کند.

توجه: اگر Router Weakness Scan (اسکن ضعف روتر) را اجرا کنید، این عملکرد به صورت خودکار فعال می شود.

برای فعال کردن مسدود کردن سایت های مشکوک:

1. از صفحه پیمایش، به زبانه های **General (کلی)** > **AiProtection** بروید.
2. از صفحه اصلی AiProtection، روی **Network Protection (محافظت شبکه)** کلیک کنید.
3. از صفحه مسدود کردن سایت های مشکوک روی **ON (فعال)** کلیک کنید.



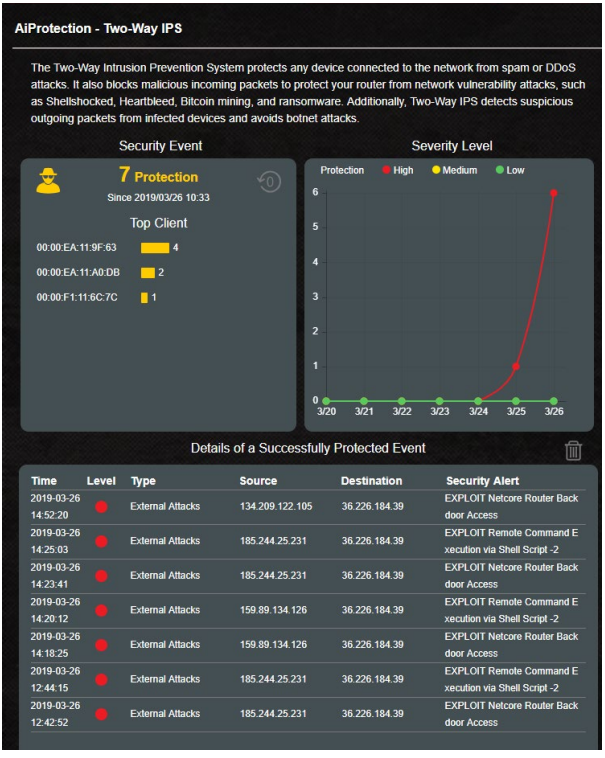
IPS 3.4.3 دوطرفه

این ویژگی موارد استفاده بدون مجوز معمول در پیکربندی روتر را برطرف می کند.

توجه: اگر Router Weakness Scan (اسکن ضعف روتر) را اجرا کنید، این عملکرد به صورت خودکار فعال می شود.

برای فعال کردن IPS دوطرفه:

1. از صفحه پیمایش، به زبانه های **General (کلی)** > **AiProtection** بروید.
2. از صفحه اصلی AiProtection، روی **Network Protection (محافظت شبکه)** کلیک کنید.
3. از صفحه IPS دوطرفه، **ON (فعال)** کلیک کنید.



3.4.4 انسداد و جلوگیری از عملکرد دستگاه ویروسی

این ویژگی مانع از این می شود که دستگاه های ویروسی بتوانند اطلاعات شخصی را رد و بدل کنند یا اینکه وضعیت ویروسی را به شرکای خارجی منتقل کنند.

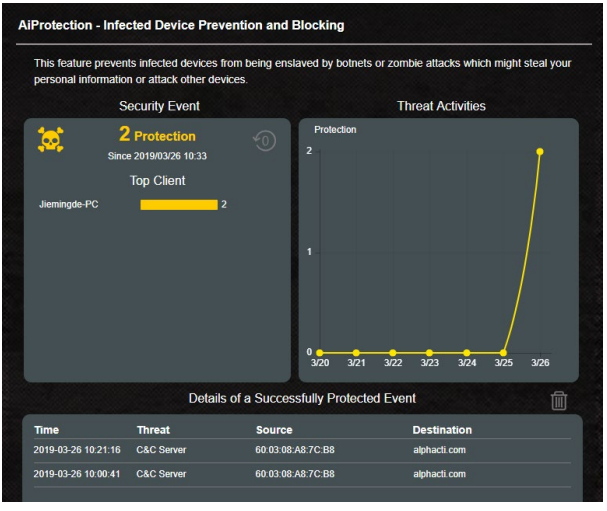
توجه: اگر Router Weakness Scan (اسکن ضعف روتر) را اجرا کنید، این عملکرد به صورت خودکار فعال می شود.

برای فعال کردن ویژگی انسداد و جلوگیری از عملکرد دستگاه ویروسی:

1. از صفحه پیمایش، به زبانه های **General (کلی)** > **AiProtection** بروید.
2. از صفحه اصلی AiProtection، روی Network Protection (محافظت شبکه) کلیک کنید.
3. از صفحه "انسداد و جلوگیری از عملکرد دستگاه ویروسی" روی **ON (فعال)** کلیک کنید.

برای پیکربندی تنظیمات برگزیده هشدار:

1. از صفحه "انسداد و جلوگیری از عملکرد دستگاه ویروسی" روی **Alert Preference (تنظیمات برگزیده هشدار)** کلیک کنید.
2. ارائه دهنده ایمیل، حساب ایمیل و رمز عبور را انتخاب کرده یا وارد کنید و سپس روی **Apply (اعمال)** کلیک کنید.

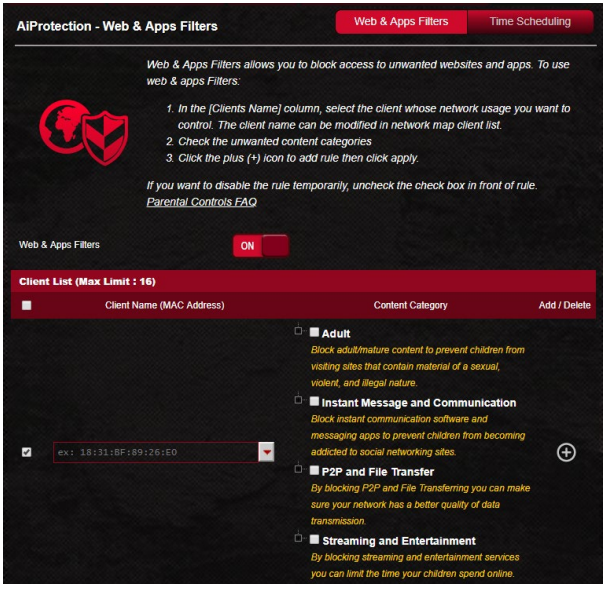


3.4.5 تنظیم Parental Control (کنترل والدین)

کنترل والدین به شما امکان می دهد زمان دسترسی به اینترنت را کنترل کرده یا محدودیت زمانی را برای استفاده شبکه توسط کلاینت تنظیم کنید.

برای فعال کردن IPS دوطرفه:

1. از صفحه پیمایش، به زبانه های **General (کلی)** > **AiProtection** بروید.
2. از صفحه اصلی AiProtection، روی **Parental Controls (کنترل های والدین)** کلیک کنید.



فیلترهای وب و برنامه

"فیلترهای وب و برنامه" ویژگی از کنترل های والدین است که به شما امکان می دهد دسترسی به وبسایت ها یا برنامه های ناخواسته را مسدود کنید.

برای پیکربندی فیلترهای وب و برنامه:

1. از صفحه پیمایش، به زبانه های **General(کلی)** > **AiProtection** بروید.
2. از صفحه اصلی AiProtection روی نماد **Parental Controls (کنترل های والدین)** کلیک کنید تا به زبانه کنترل های والدین بروید.

3. از صفحه **Web & Apps Filters (فیلترهای وب و برنامه)** روی **ON (فعال)** کلیک کنید.

4. بعد از نمایش پیام توافقنامه مجوز کاربر نهایی (EULA) برای ادامه روی **I agree (موافق هستم)** کلیک کنید

5. از ستون **Client List (لیست کلاینت)**، نام کلاینت را از کادر کشویی انتخاب کرده یا آن را وارد کنید.

6. از ستون **Content Category (دسته بندی محتوا)**، فیلترها را از بین چهار دسته اصلی انتخاب کنید: **Adult (بزرگسال)**، **Instant Message and Communication (پیام و ارتباط فوری)**، **P۲P and File Transfer (P۲P و انتقال فایل)** و **Streaming and Entertainment (پخش جریانی و سرگرمی)**.

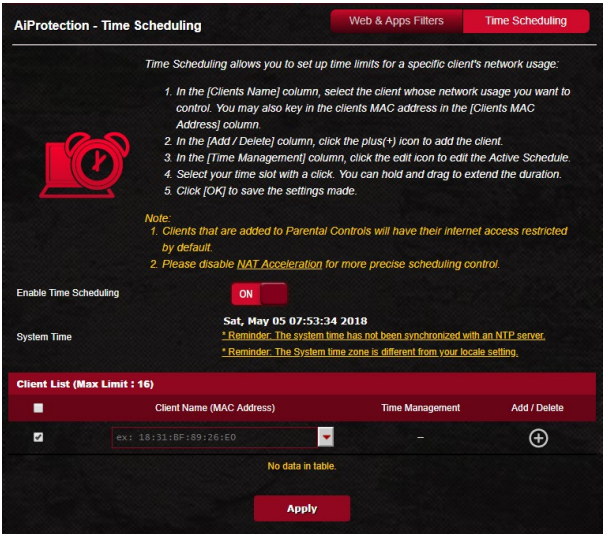
7. برای افزودن نمایه کلاینت روی ⊕ کلیک کنید.

8. برای ذخیره تنظیمات روی **Apply (اعمال)** کلیک کنید.

زمانبندی

"زمانبندی" به شما امکان می دهد محدودیت زمانی را برای مصرف شبکه توسط یک کلاینت تنظیم کنند.

توجه: اطمینان حاصل کنید زمان سیستم با سرور NTP همگامسازی شود.



برای پیکربندی زمانبندی:

1. از صفحه پیمایش، به زبانه های **General(کلی)** > **AiProtection Parental Controls (کنترل های والدین)** > **Time Scheduling (زمانبندی)** بروید.
2. از صفحه **Enable Time Scheduling (فعال کردن زمانبندی)** روی **ON (فعال)** کلیک کنید.
3. از ستون **Clients Name (نام کلاینت ها)**، نام کلاینت را از کادر کشویی انتخاب کرده یا آن را وارد کنید.

توجه: همچنین می توانید آدرس MAC را در ستون Client MAC Address (آدرس MAC کلاینت) وارد کنید. بررسی کنید نام کلاینت نویسه های خاص یا فاصله نداشته باشد زیرا ممکن است باعث عملکرد نادرست روتر شود.

4. برای افزودن نمایه کلاینت روی ⊕ کلیک کنید.
5. برای ذخیره تنظیمات روی **Apply (اعمال)** کلیک کنید.

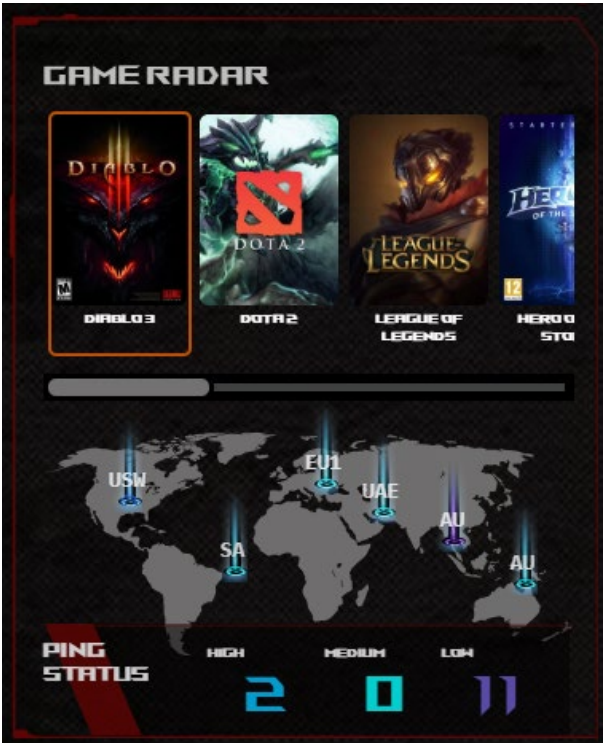
3.5 داشبورد

داشبورد به شما امکان می دهد ترافیک لحظه ای را در محیط شبکه تحت نظارت داشته باشید و پینگ لحظه ای شبکه و انحراف از پینگ را تجزیه و تحلیل کنید.

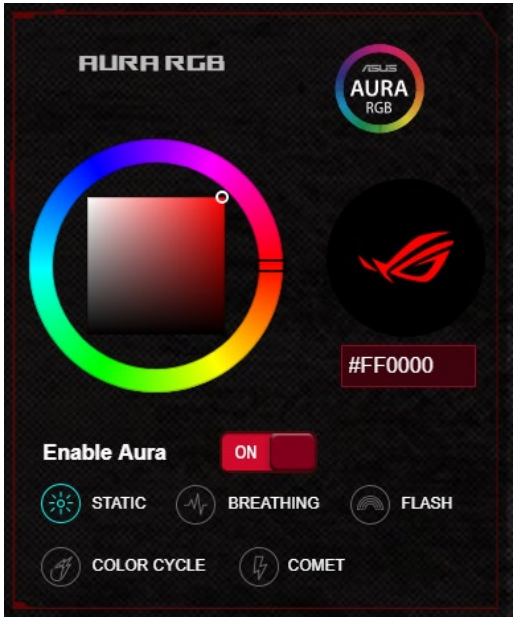
پینگ شبکه به معنای تجربه های بازی آنلاین است. هرچه پینگ بیشتر باشد به این معنا است که زمان تأخیر برای بازی های لحظه ای بالاتر است. برای اکثر بازی های آنلاین اگر پینگ شبکه کمتر از 99 میلی ثانیه باشد، کیفیت

خوب است. اگر پینگ شبکه کمتر از 150 میلی ثانیه باشد، کیفیت قابل قبول است. به طور کلی اگر پینگ شبکه بیشتر از 150 میلی ثانیه باشد، نمی توانید به راحتی بازی کنید.
انحراف پینگ تا حد زیادی به تجربه های بازی آنلاین مرتبط است. هرچه انحراف پینگ بیشتر باشد، احتمال ایجاد جابجایی (تاگل) در حین انجام بازی آنلاین بیشتر است. هیچ معیار پایه ای برای انحراف پینگ وجود ندارد. با این وجود بهتر است انحراف پینگ کمتر باشد.

- **Game Radar (رادار بازی):** با استفاده از رادار بازی در داشبورد می توانید از زمان پینج (تأخیر) سرور خاص یک بازی به سرعت مطلع شوید.



- **Aura RGB:** به کاربر امکان می دهد Aura RGB را از داشبورد روشن یا خاموش کنند. می توانید هر رنگی را تنظیم کنید و هرکدام از پنج الگوی روشنایی را انتخاب کنید.



3.6 دیواره آتش

روتر بی سیم مانند دیواره آتش سخت افزار شبکه عمل می کند.

نکته: ویژگی دیواره آتش به صورت پیش فرض فعال است.

3.6.1 موارد کلی

برای راه اندازی تنظیمات اولیه دیواره آتش:

1. از پنل پیمایش، به زبانه **Advanced Settings (تنظیمات پیشرفته)** > **Firewall (دیوار آتش)** > **General (موارد کلی)** بروید.
2. در قسمت **Enable Firewall (فعال کردن دیوار آتش)**، **Yes (بله)** را انتخاب کنید.
3. در **Enable DoS protection (فعال کردن حفاظت رد سرویس)**، **Yes (بله)** را برای حفاظت از شبکه در برابر حملات رد سرویس انتخاب کنید، اگرچه این کار ممکن است کارایی روتر را تحت تأثیر قرار دهد.
4. همچنین می توانید بسته هایی که بین اتصال LAN و WAN رد و بدل می شوند را باز بینی کنید. در نوع بسته ها، **Dropped (حذف شده)**، **Accepted (پذیرفته شده)** یا **Both (هر دو)** را انتخاب کنید.
5. روی **Apply (به کارگیری)** کلیک کنید.

3.6.2 فیلتر کردن نشانی وب

می توانید کلمات کلیدی یا آدرس های وب را برای جلوگیری از دسترسی به نشانی های خاص وب، مشخص کنید.

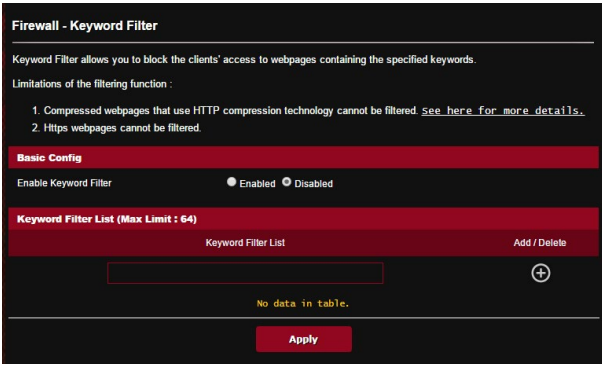
نکته: فیلتر کردن نشانی وب بر اساس جستار DNS است. اگر سرویس گیرنده شبکه قبلاً به وب سایتی مثل سایت http://www.abcxxx.com دسترسی پیدا کرده باشد، وب سایت مسدود نمی شود (حافظه نهان DNS سیستم، بازدیدهای قبلی از وب سایت را ذخیره می کند). برای حل این مشکل، قبل از راه اندازی فیلتر کردن نشانی وب، حافظه نهان DNS را پاک کنید.

برای راه اندازی فیلتر نشانی وب:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Firewall (دیوار آتش)** > **URL Filter (فیلتر نشانی وب)** بروید.
2. در قسمت **Enable URL Filter (فعال کردن فیلتر نشانی وب)**، **Enabled (فعال)** را انتخاب کنید.
3. نشانی وب را وارد کنید و روی دکمه ⊕ کلیک کنید.
4. روی **Apply (به کارگیری)** کلیک کنید.

3.6.3 فیلتر کردن کلمه کلیدی

فیلتر کردن کلمه کلیدی، دسترسی به صفحات وب که حاوی کلمات کلیدی تعیین شده هستند را مسدود می‌کند.



برای راه اندازی فیلتر کلمه کلیدی:

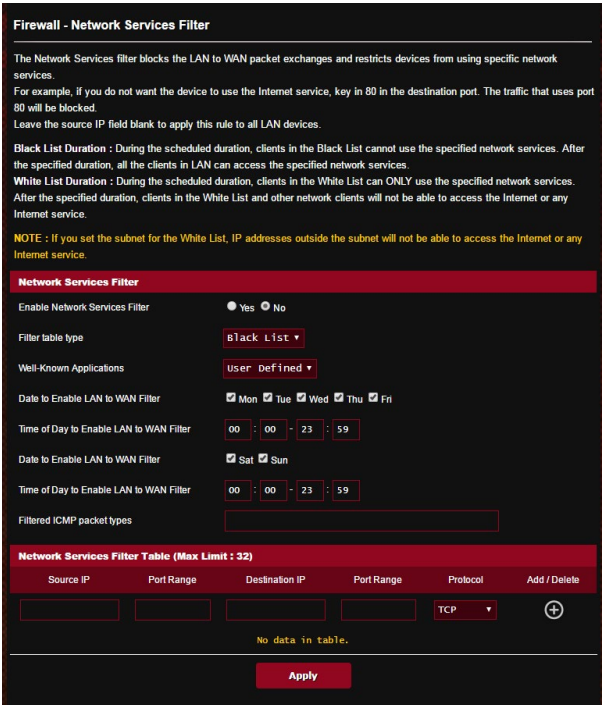
1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Firewall (دیوار آتش)** > **Keyword Filter (فیلتر کلمه کلیدی)**.
2. در قسمت **Enable Keyword Filter (فعال کردن فیلتر کلمه کلیدی)**، **Enabled (فعال)** را انتخاب کنید.
3. کلمه یا عبارت را وارد کنید و روی دکمه ⊕ کلیک کنید.
4. روی **Apply (به کارگیری)** کلیک کنید.

تذکرها:

- فیلتر کردن کلمه کلیدی بر اساس جستار DNS است. اگر سرویس گیرنده شبکه قبلاً به وب سایتی مثل سایت http://www.abcxxx.com دسترسی پیدا کرده باشد، وب سایت مسدود نمی شود (حافظه نهان DNS سیستم، بازدیدهای قبلی از وب سایت را ذخیره می کند). برای حل این مشکل، قبل از راه اندازی فیلتر کردن کلمه کلیدی، حافظه نهان DNS را پاک کنید.
- صفحات وب فشرده شده با استفاده از فشرده سازی HTTP را نمی توان فیلتر کرد. همچنین با استفاده از فیلتر کردن کلمه کلیدی نمی توان صفحات HTTPS را مسدود کرد.

3.6.4 فیلتر سرویس های شبکه

فیلتر سرویس های شبکه، رد و بدل کردن بسته LAN به WAN را مسدود می کند و دسترسی سرویس گیرنده های شبکه به سرویس های وب خاص مانند Telnet یا FTP را محدود می کند.



برای راه اندازی فیلتر سرویس شبکه:

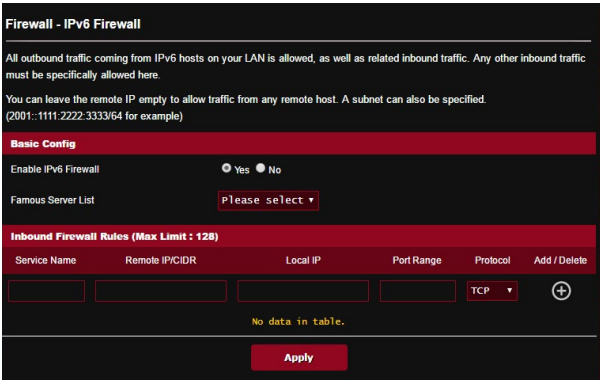
1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Firewall (دیوار آتش)** > **Network Service Filter (فیلتر کردن خدمات شبکه)**.
2. در قسمت **Enable Network Services Filter (فعال کردن فیلتر خدمات شبکه)**، **Yes (بله)** را انتخاب کنید.
3. نوع جدول فیلتر را انتخاب کنید. **Black List (فهرست سیاه)** سرویس های شبکه تعیین شده را مسدود می کند. **White List (فهرست سفید)** دسترسی به سرویس های شبکه تعیین شده را محدود می کند.
4. وقتی فیلتر ها فعال شد، زمان و روز را تعیین کنید.

5. برای تعیین خدمات شبکه و فیلتر کردن آن، IP مبدا، IP مقصد، محدوده درگاه و پروتکل را وارد کنید. روی دکمه ⊕ کلیک کنید.

6. روی **Apply (به کارگیری)** کلیک کنید.

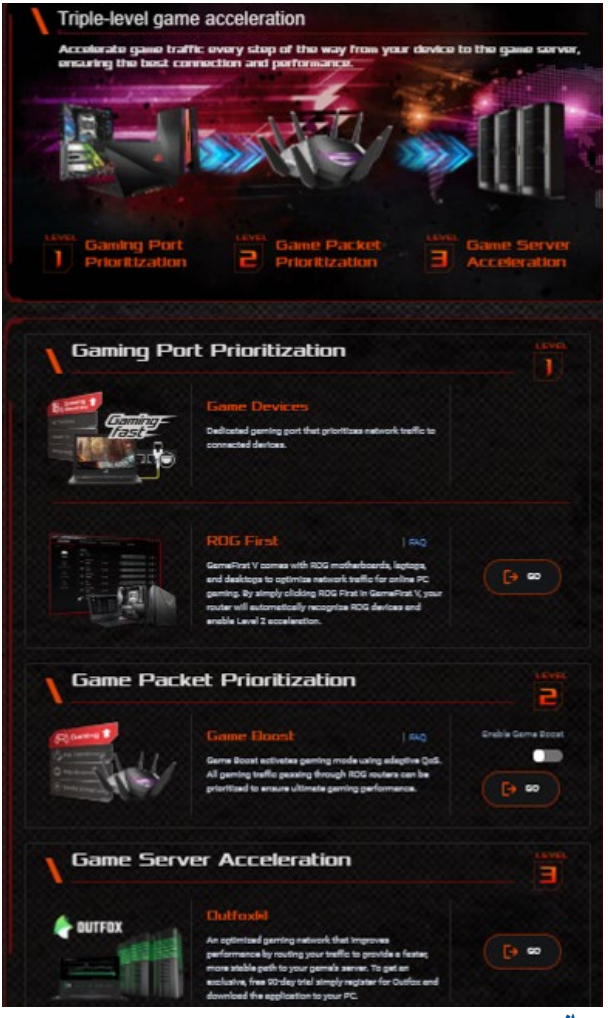
3.6.5 دیواره آتش IPv6

روتر بی سیم ASUS، به صورت پیش فرض، همه ترافیک های ورودی درخواست نشده را مسدود می کند. عملکرد دیواره آتش IPv6 این امکان را می دهد که ترافیک ورودی که از خدمات تعیین شده وارد می شوند از شبکه شما عبور کنند.



3.7 ارتقای بازی

این ویژگی به شما امکان می دهد با یک کلیک، "ارتقای بازی" را فعال کنید. اگر ارتقای بازی فعال باشد، روتر بی سیم ROG Rapture اولویت بالایی را به بسته بازی می دهد تا بهترین تجربه بازی را داشته باشید.



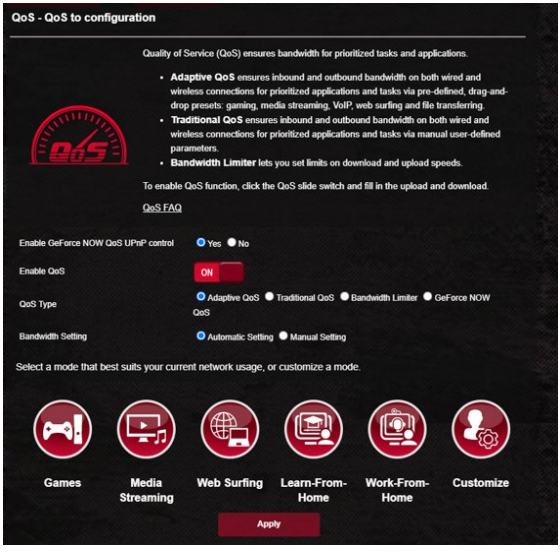
ارتقای بازی

برای فعال کردن ارتقای بازی:

از زبانه **Game Boost (ارتقای بازی)**، اسلایدر **Enable Game Boost (فعال کردن ارتقای بازی)** را روی **ON (روشن)** بگذارید.

QoS 3.7.1

این ویژگی به شما اطمینان می دهد که پهنای باند کارها و برنامه هایی که دارای اولویت هستند در حد خوبی باشند.



برای فعال کردن عملکرد QoS:

1. از صفحه پیمایش، به زبانه های **General(کلی) >** بروید **QoS** > **(ارتقای بازی) Game Acceleration**.
2. از صفحه **Enable QoS (فعال کردن QoS)** روی **ON (فعال)** کلیک کنید.
3. نوع QoS (تطبیقی، سنتی یا محدود کننده پهنای باند) را برای پیکربندی تان انتخاب کنید.

توجه: برای مشاهده تعریف نوع QoS به زبانه QoS بروید.

---

4. برای تنظیم خودکار بهترین پهنای باند روی **Automatic Setting (تنظیم خودکار)** کلیک کنید، یا برای تنظیم دستی پهنای باند آپلود و دانلود روی **Manual Setting (تنظیم دستی)** کلیک کنید.

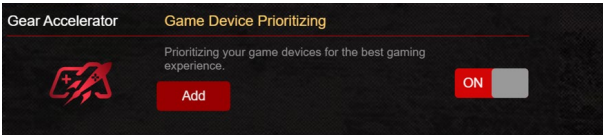
توجه: اطلاعات پهنای باند را از ISP خودتان دریافت کنید. همچنین برای بررسی و دریافت پهنای باند می توانید به سایت http://speedtest.net بروید.

---

5. برای **Apply (اعمال)** کلیک کنید.

Gear Accelerator 3.7.2

با Gear Accelerator می توانید دستگاه های بازی را به صورت بی سیم از طریق صفحه کنترل آنلاین در اولویت قرار دهید تا بهترین تجربه بازی را داشته باشید.



برای تنظیم Gear Accelerator:

1. از صفحه پیمایش به **General (کلی)** > **Game Acceleration (ارتقای بازی)** بروید.
2. در زبانه **Gear Accelerator** روی **ON (فعال)** کلیک کنید.
3. بعد از اجرای تنظیمات، روی **Add (اضافه کردن)** کلیک کنید تا نام مشتری انتخاب شود.
4. برای افزودن پروفایل مشتری، روی کلیک کنید.
5. برای ذخیره تنظیمات روی **Apply (اعمال)** کلیک کنید.

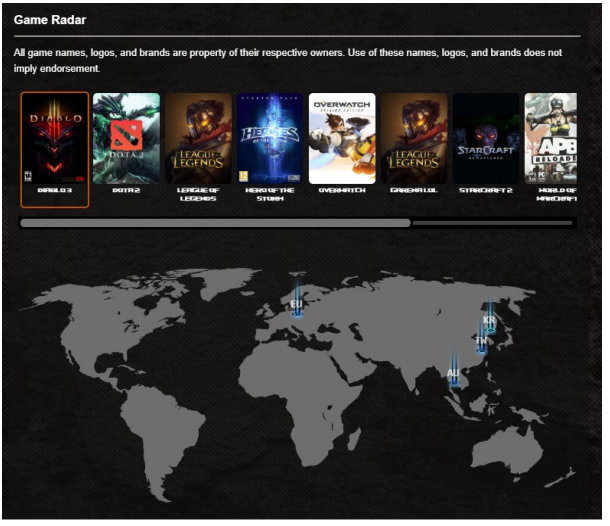
توجه: اگر می خواهید پروفایل مشتری را حذف کنید، روی کلیک کنید.

3.8 رادار بازی

رادار بازی یک ابزار تشخیص عیب است که کیفیت اتصال سرورها را برای بعضی از بازی های خاص شناسایی می کند.

برای استفاده از Game Radar (رادار بازی):

1. از صفحه پیمایش، به **General (موارد کلی)** > **Game Radar (رادار بازی)** بروید و بازی را از لیست بازی ها انتخاب کنید.



2. **Ping Status (وضعیت پینگ)** هر سرور را بررسی کنید.
3. برای اینکه تجربه بازی آنلاین راحتی داشته باشید، یک سرور بازی را انتخاب کنید که وضعیت پینگ پایینی داشته باشد.

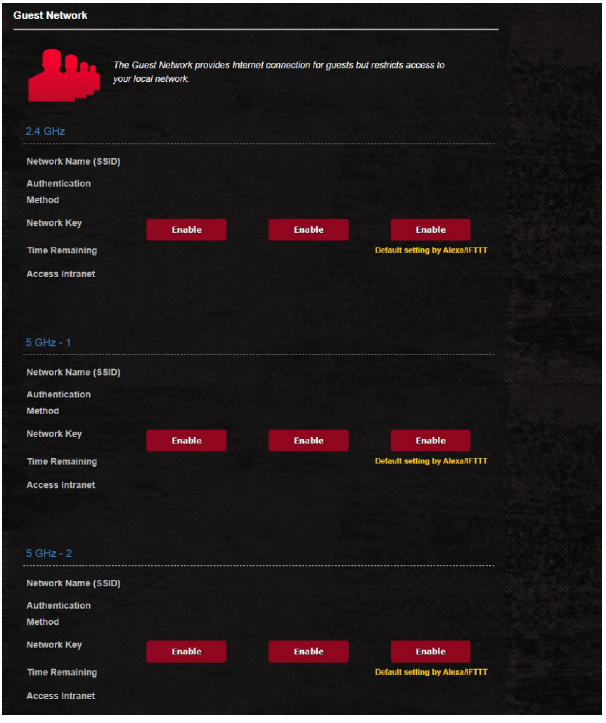
3.9 شبکه مهمان

شبکه مهمان از طریق دسترسی به SSIDها یا شبکه های جداگانه بدون ارائه دسترسی به شبکه خصوصی شما برای بازدیدکنندگان موقت اتصال اینترنتی فراهم می کند.

توجه: GT-AXE16000 از حداکثر شش SSID پشتیبانی می کند (سه 2.4 SSID گیگاهرتز, سه 5 SSID گیگاهرتز-1 و سه 5 SSID گیگاهرتز-2).

برای ایجاد یک شبکه مهمان:

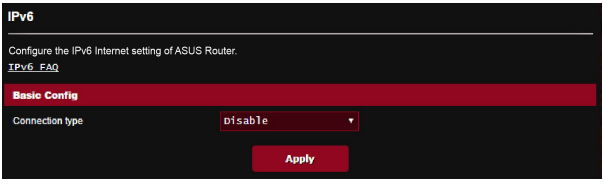
1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Guest Network (شبکه مهمان)** بروید.
2. در صفحه Guest Network (شبکه مهمان) باند فرکانس 2.4 گیگاهرتز, 5 گیگاهرتز-1 تز یا 5 گیگاهرتز-2 را برای شبکه مهمانی که می خواهید ایجاد کنید انتخاب نمایید.
3. روی **Enable (فعال سازی)** کلیک کنید.



4. برای تغییر تنظیمات یک مهمان، روی تنظیمات مهمانی که می خواهید تغییر دهید کلیک کنید. روی **Remove (حذف)** کلیک کنید تا تنظیمات مهمان حذف شود.
5. یک نام بی سیم به شبکه موقت خود در قسمت Network Name (نام شبکه) (SSID) اختصاص دهید.
6. یک روش تأیید اعتبار را انتخاب کنید.
7. اگر یک روش تأیید اعتبار WPA انتخاب کردید، یک رمزگذاری WPA انتخاب کنید.
8. زمان دسترسی را مشخص کنید یا **Limitless (نامحدود)** را انتخاب کنید.
9. **Disable (غیرفعال)** یا **Enable (فعال)** را در قسمت Access Intranet (دسترسی به شبکه داخلی) انتخاب کنید.
10. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.

IPv6 3.10

این روتر بی سیم از آدرس دهی IPv6 پشتیبانی می کند، سیستمی که از سایر آدرس های IP پشتیبانی می‌کند. این استاندارد هنوز به طور گسترده قابل استفاده نیست.
اگر سرویس اینترنت شما از IPv6 پشتیبانی می کند با ارائه دهنده سرویس اینترنت (ISP) خود تماس بگیرید.



برای راه‌اندازی IPv6:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **IPv6** بروید.
2. **Connection type (نوع اتصال)** را انتخاب کنید. گزینه های پیکربندی بسته به نوع اتصالی که انتخاب کرده اید، متفاوت است.
3. تنظیمات IPv6 LAN و DNS را وارد کنید.
4. روی **Apply (به کارگیری)** کلیک کنید.

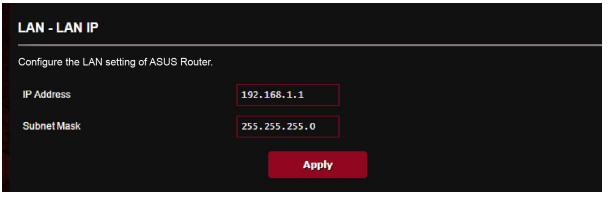
نکته: لطفاً در باره اطلاعات خاص IPv6 سرویس اینترنت به ISP خود مراجعه کنید.

LAN 3.11

LAN IP 3.11.1

صفحه LAN IP این امکان را فراهم می کند که تنظیمات LAN IP روتر شبکه را تغییر دهید.

نکته: هر تغییر در نشانی LAN IP در تنظیمات DHCP منعکس می شود.

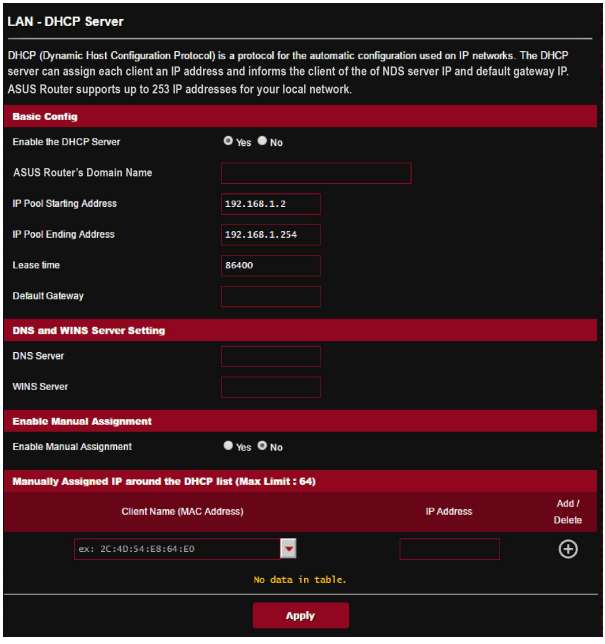


برای تغییر تنظیمات LAN IP:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **LAN** > زبانه **LAN IP**.
2. **IP address (نشانی IP)** و **Subnet Mask (ماسک شبکه فرعی)** را تغییر دهید.
3. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.

3.11.2 سرور DHCP

روتر بی سیم برای اختصاص نشانی IP موجود در شبکه به طور خودکار از DHCP استفاده می کند. می‌توانید محدوده نشانی IP و زمان اجاره به سرویس گیرنده های موجود در شبکه را تعیین کنید.



برای پیکربندی سرور DHCP:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > زبانه **LAN** > **DHCP Server (زبانه DHCP)**.
2. در قسمت **Enable the DHCP Server (فعال کردن سرور DHCP)**، **Yes** (بله) را علامت بزنید.
3. در جعبه متن **Domain Name (نام دامنه)**، نام دامنه برای روتر بی سیم را وارد کنید.
4. در قسمت **IP Pool Starting Address (نشانی شروع منبع IP)**، نشانی IP شروع را وارد کنید.

5. در قسمت **IP Pool Ending Address (نشانی پایان منبع IP)**، نشانی IP پایان را وارد کنید.
6. در قسمت **Lease Time (زمان اشغال) (ثانیه)**، زمان انقضاء نشانی IP اختصاص داده شده را به ثانیه تعیین کنید. زمانی که به این محدوده زمانی رسید، سرور DHCP یک نشانی IP جدید اختصاص می دهد.

تذکرها:

- توصیه می کنیم هنگام تعیین محدوده نشانی IP، از فرمت نشانی 192.168.1.xxx (که xxx می تواند هر عددی بین 2 تا 24 باشد) استفاده کنید.
- نشانی شروع منبع IP نباید از نشانی پایان منبع IP بیشتر باشد.

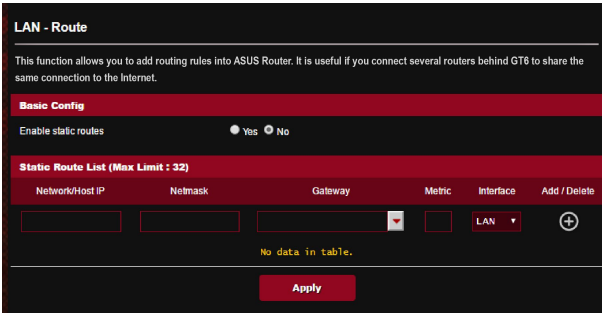
---

7. در بخش **DNS and Server Settings (تنظیمات سرور و DNS)**، در صورت نیاز سرور DNS و نشانی IP سرور WINS را وارد کنید.
8. روتر بی سیم می تواند به صورت دستی نشانی IP را به دستگاه های موجود در شبکه اختصاص دهد. در قسمت **Enable Manual Assignment (فعال کردن اختصاص دستی)**، برای اختصاص دادن نشانی IP به نشانی های خاص MAC موجود در شبکه، **Yes (بله)** را انتخاب کنید. تا 32 نشانی MAC را می توان به فهرست DHCPها برای اختصاص دادن دستی اضافه کرد.

3.11.3 مسیر

اگر شبکه شما از بیشتر از یک روتر بی سیم استفاده می کند، می توانید جدول مسیریابی را پیکربندی کنید تا سرویس اینترنت مشابهی را به اشتراک بگذارید.

نکته: توصیه می کنیم تنظیمات مسیر پیش فرض را تغییر ندهید مگر اینکه درباره جدول مسیریابی اطلاعات کاملی داشته باشید.

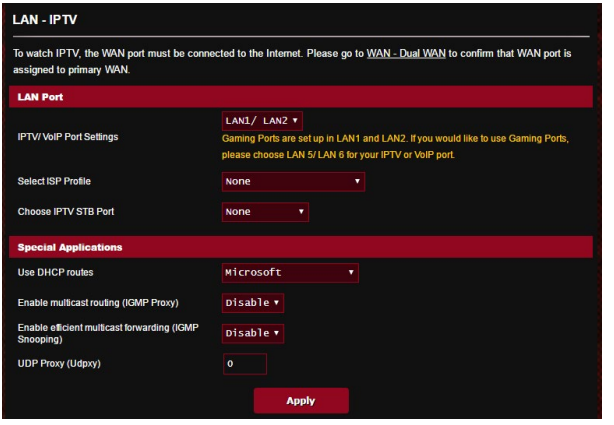


برای پیکربندی جدول مسیریابی LAN:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **LAN** > **Route (مسیر)**.
2. در قسمت **Enable static routes (فعال کردن مسیرهای ثابت)**، **Yes (بله)** را انتخاب کنید.
3. در **Static Route List (فهرست مسیرهای ثابت)**، اطلاعات شبکه نقاط دسترسی یا گره ها را وارد کنید. روی دکمه **Add (اضافه کردن)** یا **Delete (حذف)** کلیک کنید تا یک دستگاه به لیست اضافه شود یا از لیست حذف شود.
4. روی **Apply (به کارگیری)** کلیک کنید.

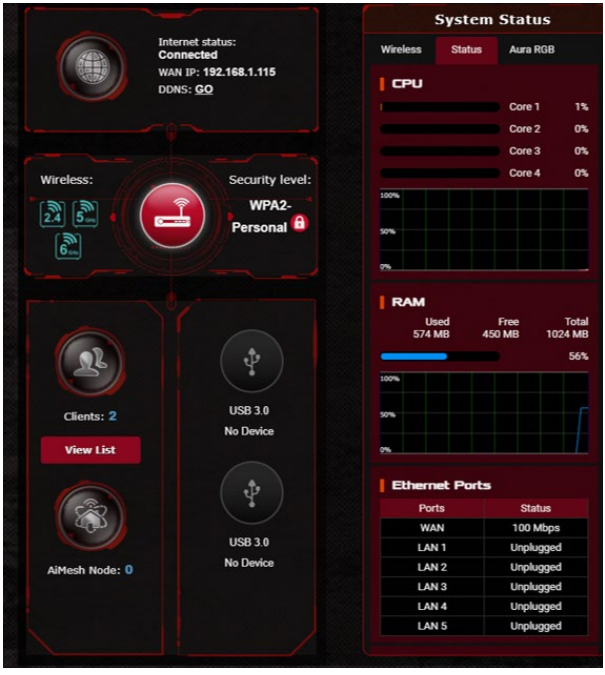
IPTV 3.11.4

روتر بی سیم از اتصال سرویس های IPTV از طریق ISP یا LAN پشتیبانی می کند. زبانه IPTV تنظیمات پیکربندی مورد نیاز برای راه اندازی IPTV، VoIP، پخش چندتایی، و UDP برای سرویس را فراهم می کند. برای کسب اطلاعات خاص درباره سرویس با ISP خود تماس بگیرید.



3.12 نقشه شبکه

نقشه شبکه به شما امکان پیکربندی تنظیمات امنیتی شبکه خود، مدیریت سرویس گیرندگان شبکه خود، و نظارت بر دستگاه USB خود را می دهد.



3.12.1 راه اندازی تنظیمات امنیتی بی سیم

برای محافظت از شبکه بی سیم خود در برابر دسترسی غیرمجاز، باید تنظیمات امنیتی آن را پیکربندی کنید.

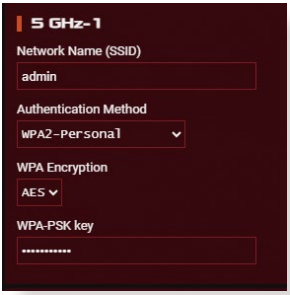
برای راه اندازی تنظیمات امنیتی بی سیم:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Network Map (نقشه شبکه)** بروید.
2. در صفحه نقشه شبکه و زیر **System Status (وضعیت سیستم)**، می توانید تنظیمات امنیتی بی سیم مانند SSID، سطح امنیت، و تنظیمات رمزگذاری را پیکربندی کنید.

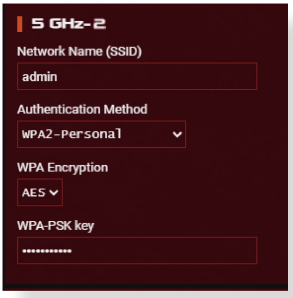
نکته: می توانید تنظیمات امنیتی بی سیم مختلفی را برای باندهای 2.4 گیگاهرتز, 5 گیگاهرتز-1 و 5 گیگاهرتز-2 ایجاد کنید.

تنظیمات امنیتی 2.4 گیگاهرتز

تنظیمات امنیتی 5 گیگاهرتز-1



تنظیمات امنیتی 5 گیگاهرتز-2



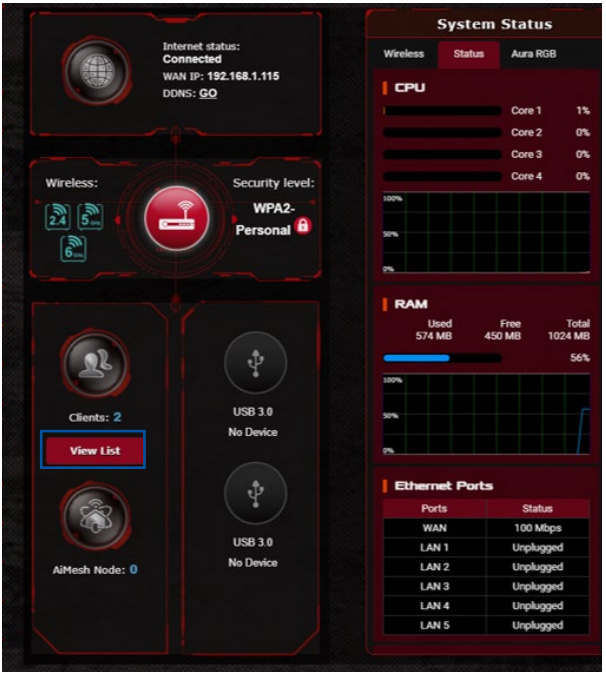
3. در قسمت **Network Name (SSID) (نام شبکه)**، نام خاصی را برای شبکه بی سیم خود وارد کنید.
4. از فهرست بازشوی **Authentication Method (روش تأیید)**، روش تأیید را برای شبکه بی‌سیم خود انتخاب کنید.

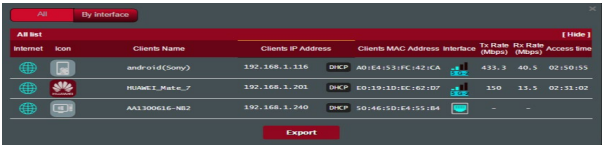
   اگر WPA-Personal یا WPA-2 Personal را به عنوان روش تأیید انتخاب کردید، کلید WPA-PSK یا کلید امنیتی را وارد کنید.

مهم! استاندارد IEEE 802.11n/ac مانع از کاربرد خروجی بالا به عنوان رمز پخش تکی با WEP یا WPA-TKIP می شود. اگر از این روشهای رمزگذاری استفاده کنید، سرعت داده های شما تا حد اتصال IEEE 802.11g تا 54 مگابیت در ثانیه کاهش می یابد.

5. پس از انجام کار روی **Apply (به کارگیری)** کلیک کنید.

3.12.2 مدیریت سرویس گیرندگان شبکه خود



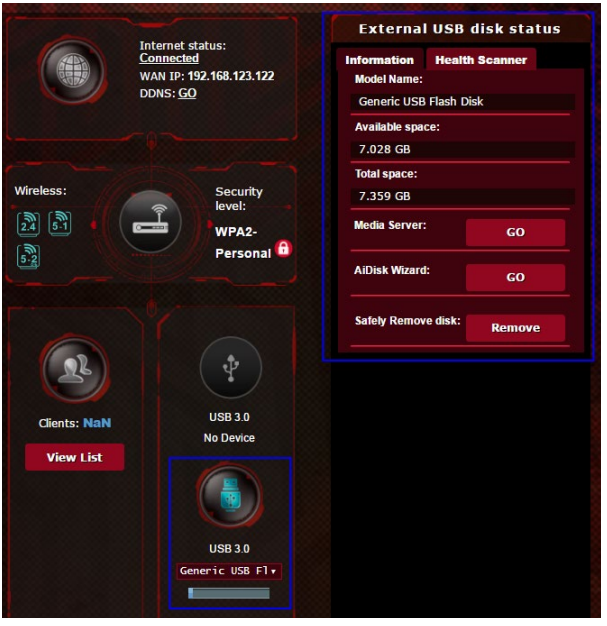


برای مدیریت سرویس گیرندگان شبکه خود:

1. از پنل پیمایش، به زبانه **Advanced Settings (تنظیمات پیشرفته)** > **Network Map (نقشه شبکه)** بروید.
2. در صفحه **Network Map (نقشه شبکه)** نماد **Clients (سرویس گیرندگان)** را برای نمایش اطلاعات سرویس گیرنده شبکه خود انتخاب کنید.
3. برای نمایش همه سرویس گیرندگان، روی View List (مشاهده لیست) در زیر نماد **Clients (سرویس گیرندگان)** کلیک کنید.
4. برای مسدود کردن دسترسی یک سرویس گیرنده به شبکه خود، سرویس گیرنده را انتخاب کنید و روی نماد باز کردن قفل کلیک کنید.

3.12.3 نظارت بر دستگاه USB خود

روتر بی سیم ASUS دو پورت USB برای اتصال دستگاه های USB یا چاپگر USB ارائه می دهد تا به شما امکان دهد فایلها و چاپگر را با سرویس گیرندگان در شبکه خود به اشتراک بگذارید.



تذکرها:

- برای استفاده از این ویژگی، باید یک دستگاه حافظه USB مانند هارد دیسک USB یا درایو فلش USB به پورت های USB 3.0/2.0 در پنل عقب روتر بی سیم خود وصل کنید. مطمئن شوید که دستگاه حافظه USB درست فرمت و پارتیشن بندی شده است. به Plug-n-Share Disk Support List (فهرست پشتیبانی دیسکهای اتصال و اشتراک) در نشانی **http://event.asus.com/networks/disksupport** مراجعه کنید.
- پورت های USB از دو درایو USB یا یک چاپگر و یک درایو USB به طور همزمان پشتیبانی می‌کند.

مهم! ابتدا باید یک حساب مشترک و حقوق مجوز/دسترسی آن را ایجاد کنید تا به سایر سرویس گیرندگان شبکه اجازه دسترسی به دستگاه USB از طریق یک سایت FTP/ برنامه دیگر سرویس گیرنده FTP، مرکز سرورها، Samba، یا AiCloud را بدهید. برای اطلاع از جزئیات بیشتر، به بخش **3.17 برنامه USB** و **3.3 AiCloud 2.0** در این دفترچه راهنمای کاربر مراجعه کنید.

برای نظارت بر دستگاه USB خود:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Network Map (نقشه شبکه)** بروید.
2. در صفحه Network Map (نقشه شبکه) نماد **USB Disk Status (وضعیت دیسک USB)** را برای نمایش اطلاعات دستگاه USB خود انتخاب کنید.
3. در قسمت AiDisk Wizard (راهنمای AiDisk)، روی **GO (برو)** کلیک کنید تا یک سرور FTP برای اشتراک گذاری اینترنتی فایل ایجاد شود.

تذکرها:

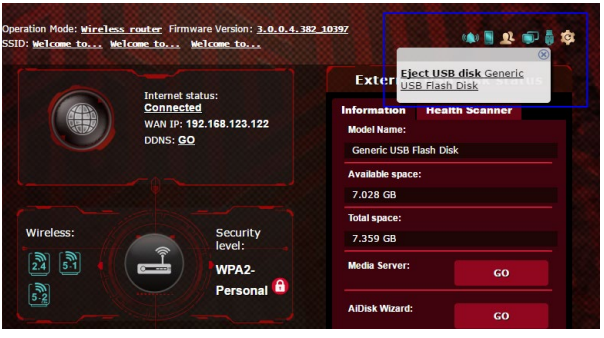
- برای اطلاع از جزئیات بیشتر، به **بخش 3.17.2 استفاده از مرکز سرورها** در این دفترچه راهنمای کاربر مراجعه کنید.
- روتر بی سیم با اکثر هارد دیسک ها/فلش دیسک های USB (تا 4 ترابایت) کار می کند و از دسترسی خواندن-نوشتن برای FAT16، FAT32، NTFS، و HFS+ پشتیبانی می نماید.

جدا کردن دیسک USB به طور ایمن

مهم! جداسازی نادرست دیسک USB ممکن است باعث خراب شدن داده ها شود.

برای جدا کردن دیسک USB به طور ایمن:

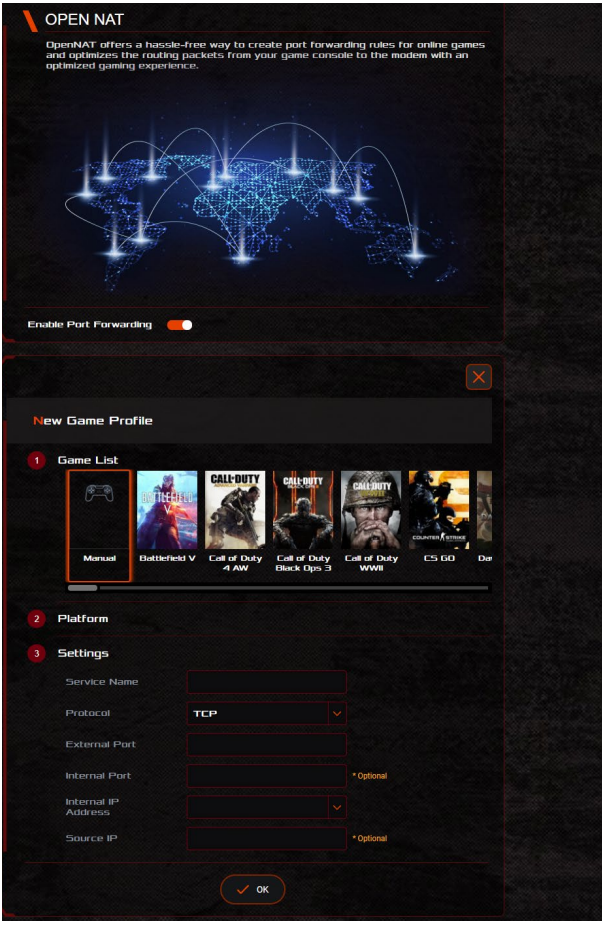
1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Network Map (نقشه شبکه)** بروید.
2. در گوشه بالای سمت راست، روی  > **Eject USB disk (خارج کردن دیسک USB)** کلیک کنید. وقتی دیسک USB به طور موفقیت آمیز خارج شد، وضعیت USB به صورت **Unmounted (پیاده شده)** نشان داده می شود.



3.13 Open NAT & نمایه بازی

Open NAT روش راحتی است برای ایجاد قوانین ارسال پورت برای بازی های آنلاین، که بسته های مسیردهی را از کنسول بازی به مودم بهینه سازی می کند تا تجربه بازی بهتری داشته باشید.

وقتی بازی های کامپیوتری یا کنسول را انجام می دهید ممکن است به دلیل تنظیمات خاص روتر یا ISP در محیطتان مانند NAT یا انسداد پورت، مشکلاتی دراتصال وجود داشته باشد. نمایه بازی این اطمینان را به شما می دهد که روتر بی سیم ROG Rapture اتصال بازی را مسدود نمی کند.



برای تنظیم Open NAT:

1. از صفحه پیمایش به **General (کلی)** > **Open NAT** بروید.
2. به سمت **Enable Port Forwarding (**فعال کردن پورت ارسال**)** بروید
3. از **Game List (**فهرست بازی**)**، بازی تان را انتخاب کنید و تنظیمات اولیه را تکمیل کنید.
4. روی **OK (تأیید)** کلیک کنید.

3.14 Smart Connect (اتصال هوشمند)

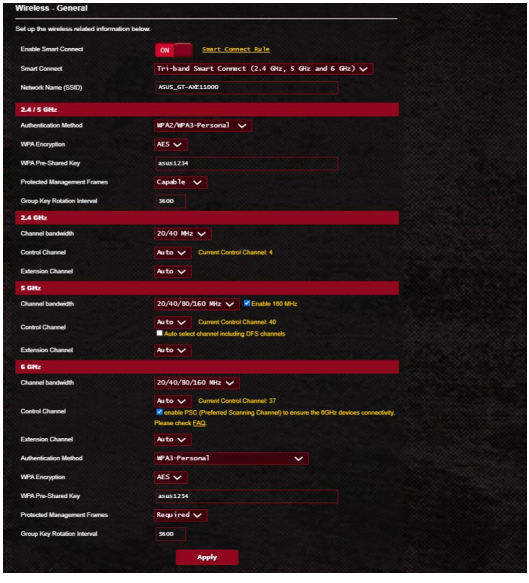
Smart Connect با این هدف طراحی شده است تا به صورت خودکار سرویس گیرندگان را به یکی از این سه رادیو (4.2 گیگاهرتز 5 گیگاهرتز-1 و 5 گیگاهرتز-2) هدایت کند و استفاده کلی از ظرفیت پذیرش را به حداکثر برساند.

3.14.1 تنظیم و راه اندازی Smart Connect

می توانید Smart Connect را از Web GUI به دو روش زیر فعال کنید:

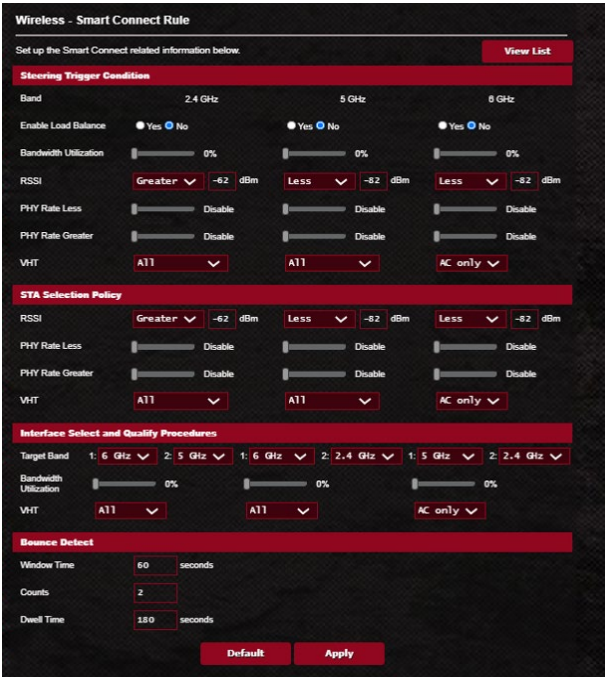
- **از طریق صفحه بی سیم**

1. در مرورگر وب، به صورت دستی آدرس IP پیش فرض روتر را وارد کنید: http://www.asusrouter.com.
2. در صفحه ورود به سیتم، نام کاربری پیش فرض (**admin**) و رمز عبور پیش فرض (**admin**) را وارد کنید و روی **OK (تأیید)** کلیک کنید. صفحه QIS به صورت خودکار راه اندازی می شود.
3. از صفحه پیمایش، به زبانه های **Advanced Settings (تنظیمات پیشرفته)** > **Wireless (بی سیم)** > **General (کلی)**.
4. اسلایدر را روی **ON (روشن)** در قسمت **Enable Smart Connect (فعال کردن Smart Connect)** ببرید. این عملکرد به صورت خودکار سرویس گیرندگان موجود در شبکه تان را به باند مربوطه متصل می کند تا سرعت بهینه سازی شود.



3.14.2 قانون Smart Connect

ASUSWRT تنظیمات شرایط پیش فرضی را برای جابجا کردن مکانیسم ها ارائه می کند. همچنین می توانید شرایط اجرا را با توجه به محیط شبکه تان تغییر دهید. برای تغییر تنظیمات، به زبانه **Smart Connect Rule (قانون Smart Connect)** در صفحه Network Tools (ابزار شبکه) بروید.

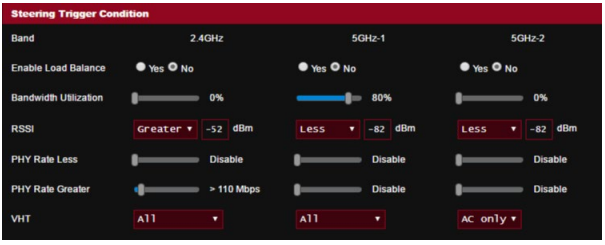


کنترل های قانون Smart Connect به چهار قسمت تقسیم می شوند:

- شرایط اجرای فرمان
- سیاست انتخاب STA
- انتخاب رابط و شرایط تأیید اعتبار
- تشخیص برگشت

Steering Trigger Condition (شرایط اجرای فرمان)

این مجموعه کنترل ها، معیار شروع فرمان باند را تنظیم می کند.



- **Bandwidth Utilization (استفاده از پهنای باند)**

  وقتی میزان استفاده پهنای باند از این درصد بیشتر می شود، فرمان شروع به کار می کند.

- **Enable Load Balance (فعال کردن توازن بار)**

  این قسمت توازن بار را کنترل می کند.

- **RSSI**

  اگر سطح سیگنال دریافتی هر سرویس گیرنده مرتبطی با این شرایط مطابقت داشته باشد، فرمان شروع به کار می کند.

- **PHY Rate Less / PHY Rate Greater (نرخ PHY کمتر/نرخ PHY بیشتر)**

  این موارد نرخ ها (سرعت های) پیوند STA را تعیین می کنند که راه انداز فرمان باند هستند.

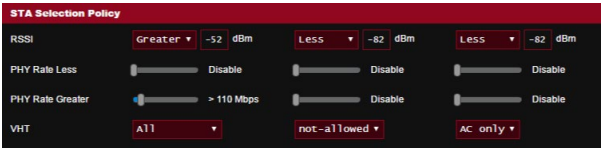
- **VHT**

  این گزینه تعیین می کند که سرویس گیرندگان ۸۰۲,۱۱ac و غیر ac چطور کنترل می شوند.

  - **ALL (همه)** (پیش فرض) به این معنی است که هر نوع سرویس گیرنده ای می تواند فرمان را راه اندازی کند.
  - **AC only (فقط AC)** به این معنی است که سرویس گیرنده باید برای شروع عملکرد فرمان از ۸۰۲,۱۱ac پشتیبانی کند.
  - **Not-allowed (مجاز نیست)** به این معنی است که فقط سرویس گیرندگان غیر 802.11ac فرمان را راه اندازی می کنند، یعنی 802.11a/b/g/n.

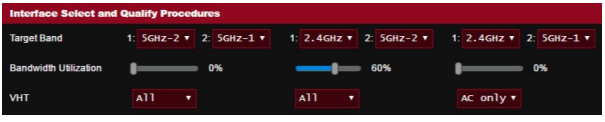
STA Selection Policy (سیاست انتخاب STA)

بعد از شروع به کار فرمان، ASUSWRT از سیاست انتخاب STA پیروی می کند تا یک سرویس گیرنده (STA) را انتخاب کند که به مناسب ترین باند هدایت می شود.



Interface Select and Qualify Procedures (انتخاب رابط و شرایط تأیید اعتبار)

این موارد، تعیین می کنند که سرویس گیرنده هدایت شده در کجا متوقف شود. **Target Band (باند هدف)** کنترل می کند که اولین و دومین انتخاب هدف های فرمان کجا مشخص شوند. اگر **Bandwidth Utilization (استفاده از پهنای باند)** کمتر از مقدار تعیین شده باشد، معیار سرویس گیرندگان برای تبعیت از سیاست انتخاب STA برای رادیو به اولین هدف هدایت می شود. در غیر اینصورت، سرویس گیرنده به دومین رادیوی **Target Band (باند هدف)** ارسال خواهد شد.



Bounce Detect (تشخیص برگشت)

این مجموعه از کنترل ها تعیین می کنند که سرویس گیرنده در چه مواقعی قابل هدایت است. با استفاده از این گزینه، سرویس گیرندگان به صورت مداوم در اطراف جابجا نمی شوند. اما با این حال مانع از این نمی شود که سرویس گیرندگان اتصال خودشان را قطع کنند و در این صورت به عنوان «برگشت» محاسبه نشوند. هر سرویس گیرنده می تواند **Counts N (بار)** در **Window Time (زمان پنجره)** هدایت شود. با رسیدن به حد شمارش تنظیم **Dwell Time (زمان امتحان)** هدایت نمی شده، سرویس گیرنده دوباره برای شود.

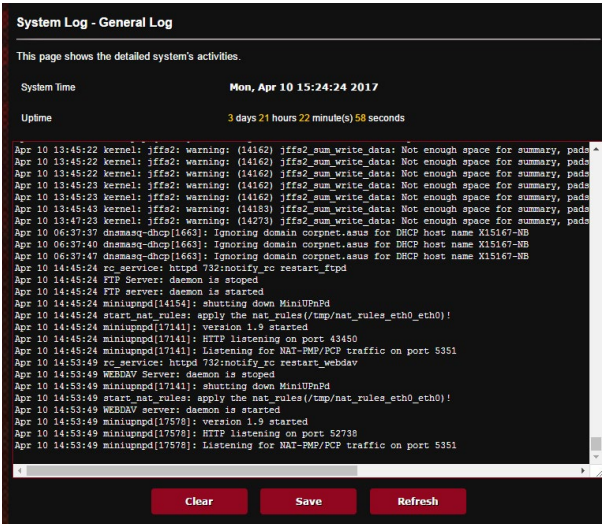
3.15 System Log (گزارش سیستم)

گزارش سیستم حاوی فعالیت‌های ثبت شده شبکه است.

نکته: وقتی روتر راه اندازی می شود یا خاموش می شود، گزارش سیستم بازنشانی می شود.

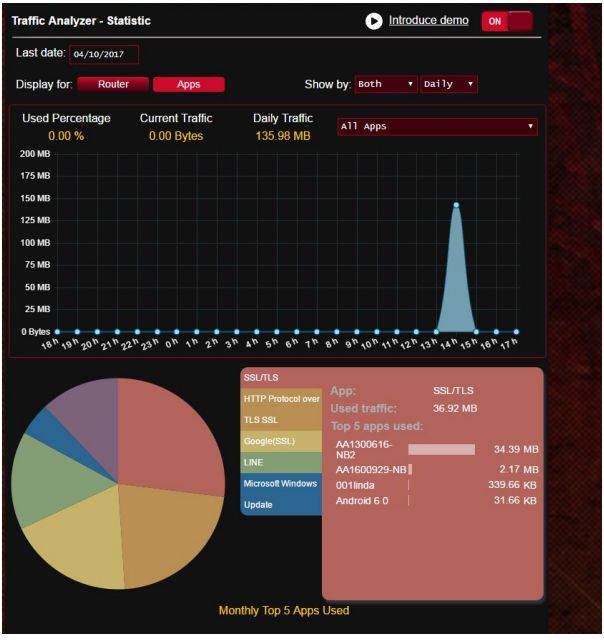
برای مشاهده گزارش سیستم:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **System Log (گزارش سیستم)** بروید.
2. می توانید از هر یک از این زبانه ها، فعالیت های شبکه خود را مشاهده کنید.
   - General Log (گزارش موارد کلی)
   - Wireless Log (گزارش بی سیم)
   - DHCP Leases (اشغال DHCP)
   - IPv6
   - Routing Table (جدول مسیریابی)
   - Port Forwarding (هدایت پورت)
   - Connections (اتصال ها)



3.16 تجزیه کننده ترافیک

Traffic Analyzer(تجزیه کننده ترافیک) نمایی مختصر از آنچه که روزانه، هفتگی یا ماهیانه در شبکه تان روی می دهد نمایش می دهد. این ابزار به شما امکان می دهد به سرعت میزان استفاده از پهنای باند یا دستگاه یا برنامه مورد استفاده را مشاهده کنید و میزان باتلنک اتصال اینترنت را کاهش دهید. همچنین روش فوق العاده ای است برای نظارت بر میزان استفاده از اینترنت یا فعالیت های اینترنتی.



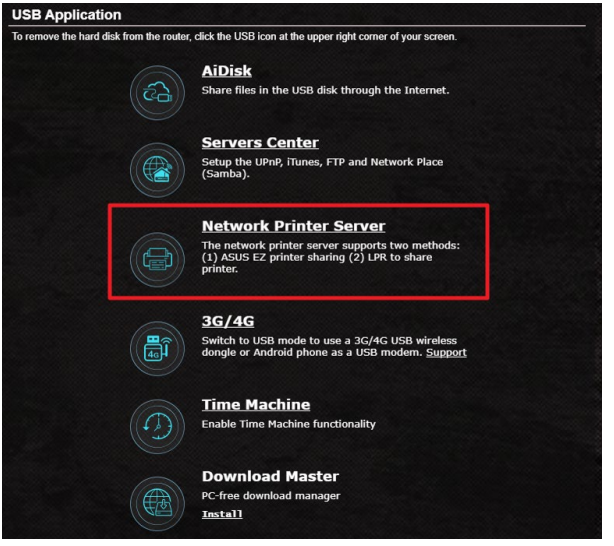
برای پیکربندی Traffic analyzer:

1. از صفحه پیمایش، به زبانه های **General (موارد کلی)** > بروید **Traffic Analyzer(تجزیه کننده ترافیک)**.
2. از صفحه اصلی Traffic Analyzer، اطلاعات آماری تجزیه کننده ترافیک را فعال کنید.
3. تاریخی را انتخاب کنید که می خواهید نمودار برای آن تاریخ نمایش داده شود.
4. روی **Display (صفحه نمایش)** این فیلد، Router (روتر) یا Apps (برنامه ها) را برای نمایش اطلاعات ترافیکی انتخاب کنید.
5. روی قسمت نمایش بر اساس فیلد انتخاب کنید اطلاعات ترافیکی چطور نمایش داده شوند.

3.17 برنامه USB

عملکرد برنامه های USB دارای منوهای فرعی AiDisk، Servers Center، Network Printer Server و Download Master است.

مهم! برای استفاده از عملکردهای سرور، باید یک دستگاه حافظه USB مانند هارد دیسک USB یا درایو فلش USB به پورت USB 3.0 در پنل عقب روتر بی سیم خود وصل کنید. مطمئن شوید که دستگاه حافظه USB درست فرمت و پارتیشن بندی شده است. برای مشاهده جدول پشتیبانی سیستم فایل به وبسایت ASUS به نشانی http://event.asus.com/2009/networks/disksupport مراجعه کنید.

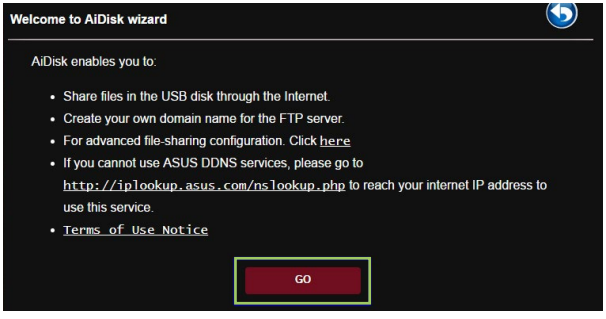


3.17.1 استفاده از AiDisk

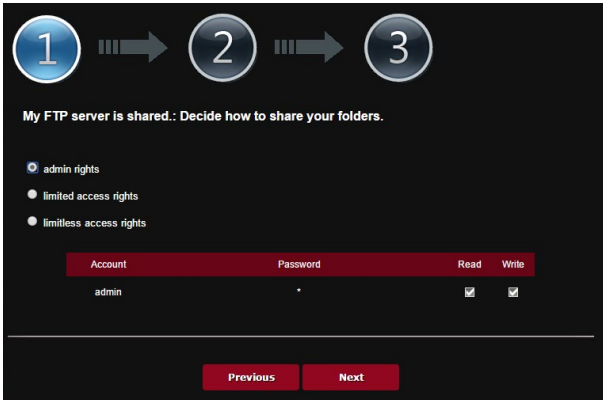
AiDisk به شما امکان می دهد فایل های ذخیره شده روی یک دستگاه USB را از طریق اینترنت به اشتراک بگذارید. AiDisk همچنین به شما در برپایی ASUS DDNS و یک سرور FTP به شما کمک می کند.

برای مشاهده AiDisk:

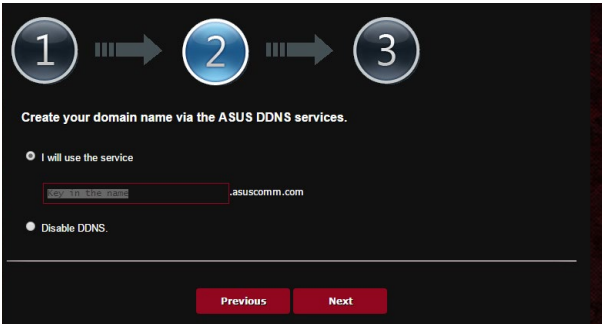
1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **USB Application (برنامه USB)** بروید، سپس روی نماد **AiDisk** کلیک کنید.
2. از صفحه Welcome to AiDisk wizard (به راهنمای AiDisk خوش آمدید) روی **Go (برو)** کلیک کنید.



3. حقوق دسترسی را که می خواهید به سرویس گیرندگانی اعطا کنید که به داده های اشتراک‌گذاری شده شما دسترسی پیدا می کنند انتخاب کنید.



4. نام دامنه خود را از طریق خدمات ASUS DDNS ایجاد کنید، شرایط خدمات را مطالعه کنید و سپس **I will use the service and accept the Terms of service (از این خدمات استفاده خواهم کرد و شرایط خدمات را می پذیرم)** را انتخاب و نام دامنه خود را وارد کنید. وقتی انجام شد، روی **Next (بعدی)** کلیک کنید.



همچنین می توانید **Skip ASUS DDNS settings (رد شدن از تنظیمات ASUS DDNS)** را انتخاب کنید سپس روی **Next (بعدی)** کلیک کنید تا از تنظیم DDNS رد شوید.

5. روی **Finish (پایان)** برای تکمیل تنظیم کلیک کنید.

6. برای دسترسی به سایت FTP که ایجاد کرده اید، یک مرورگر وب یا برنامه سرویس گیرنده FTP دیگر را باز کنید و لینک FTP (**ftp://<domain name>.asuscomm.com**) را که قبلاً ایجاد کرده اید وارد نمایید.

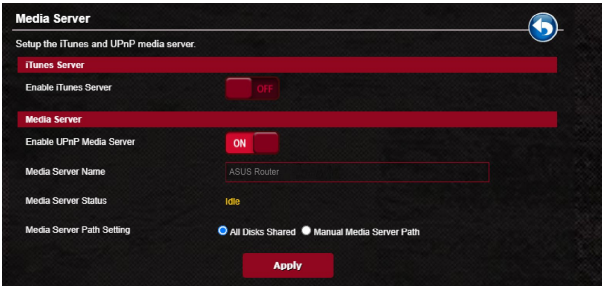
3.17.2 استفاده از مرکز سرورها

مرکز سرورها به شما امکان به اشتراک گذاری فایل های رسانه را از دیسک USB از طریق یک دایرکتوری Media Server، سرویس اشتراک گذاری Samba، یا سرویس اشتراک گذاری FTP می دهد. همچنین می‌توانید سایر تنظیمات را برای دیسک USB در مرکز سرورها پیکربندی کنید.

استفاده از Media Server

روتر بی سیم شما به دستگاه های پشتیبانی کننده از UPnP امکان دسترسی به فایل های چندرسانه ای از دیسک USB متصل شده به روتر بی سیم شما را می دهد.

نکته: قبل از استفاده از عملکرد UPnP Media Server دستگاه خود را به شبکه GT-AXE16000 وصل کنید.

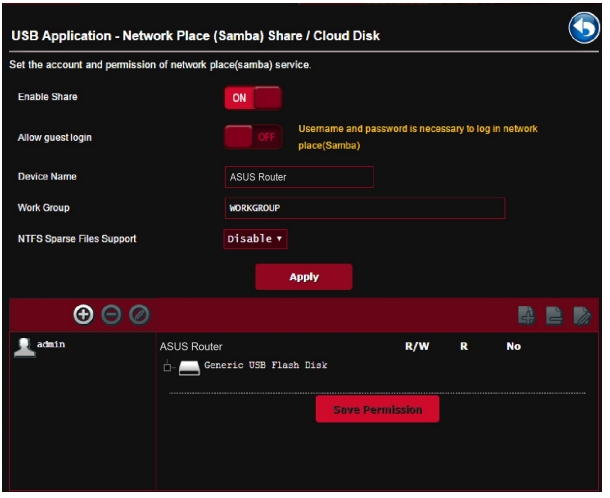


برای باز کردن صفحه تنظیم Media Server، به زبانه **Advanced Settings (تنظیمات پیشرفته) > USB Application (برنامه USB) > Media Server (سرورهای رسانه)**. برای مشاهده توضیحات هر قسمت به موارد زیر مراجعه کنید:

- **Enable iTunes Server (فعال سازی سرور iTunes)**: انتخاب کنید iTunes را برای فعال سازی/غیرفعال سازی سرور ON/OFF.
- **Enable UPnP Media Server (فعال سازی سرور رسانه UPnP)**: انتخاب UPnP سازی/غیرفعال سازی سرور رسانه‌را برای فعال ON/OFF کنید.
- **Media Server Status (وضعیت سرور رسانه)**: وضعیت سرور رسانه را نمایش می دهد.
- **Media Server Path Setting (تنظیم مسیر سرور رسانه)**: **All Disks Shared (همه دیسک‌های اشتراک گذاری شده)** یا **Manual Media Server Path (مسیر دستی سرور رسانه)** را انتخاب کنید.

استفاده از خدمات اشتراک گذاری محل شبکه (Samba)

اشتراک گذاری محل شبکه (Samba) به شما امکان می دهد حساب ها و مجوزها را برای خدمات Samba ایجاد کنید.



برای استفاده از اشتراک گذاری Samba:

1. از پنل پیمایش، به زبانه **Advanced Settings (تنظیمات پیشرفته)** > **USB Application (برنامه USB)** > **Network Place (Samba) Share / Cloud Disk (اشتراک گذاری محل شبکه (Samba)/دیسک ابری)**.

نکته: اشتراک گذاری محل شبکه (Samba) به طور پیش فرض فعال شده است.

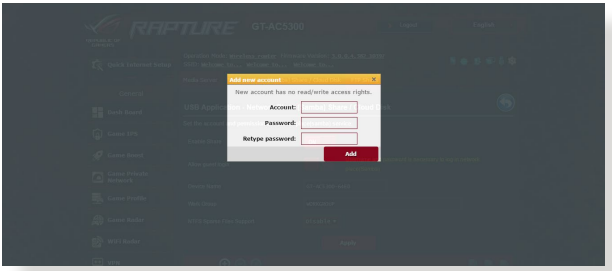
---

2. از مراحل زیر برای اضافه کردن، حذف، یا اصلاح یک حساب پیروی کنید.

برای ایجاد یک حساب جدید:

الف) روی ⊕ جهت اضافه کردن حساب جدید کلیک کنید.

ب) در قسمت های **Account (حساب)** و **Password (رمز عبور)** نام و رمز عبور سرویس گیرنده شبکه خود را وارد کنید. برای تأیید مجدداً رمز عبور را تایپ کنید. برای افزودن حساب به فهرست روی **Add (اضافه کردن)** کلیک کنید.



برای حذف یک حساب موجود:

الف) حسابی را که می خواهید حذف کنید انتخاب کنید.

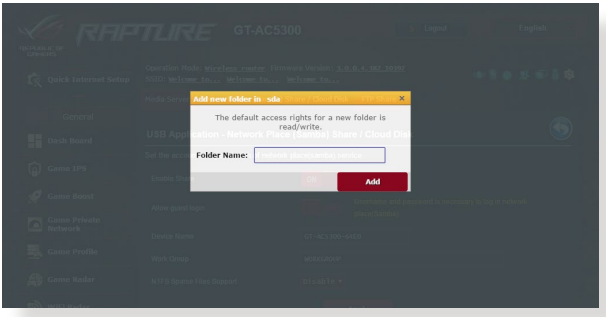
ب) روی ⊖ کلیک کنید.

پ) هنگام پرسش، روی **Delete (حذف)** کلیک کنید تا حذف حساب تأیید شود.

برای افزودن یک پوشه:

الف) روی ⊕ کلیک کنید.

ب) نام پوشه را وارد کنید، و روی **Add (اضافه کردن)** کلیک کنید. پوشه ای که ایجاد کرده اید به فهرست پوشه ها اضافه خواهد شد.



3. از فهرست پوشه ها، نوع اجازه دسترسی که می خواهید به پوشه های خاصی اعطا کنید را انتخاب نمایید:

- **R/W (خواندن/نوشتن):** برای اعطا کردن دسترسی خواندن/نوشتن این گزینه را انتخاب کنید.
- **R (خواندن):** برای اعطا کردن دسترسی فقط خواندنی این گزینه را انتخاب کنید.
- **No (هیچ):** اگر نمی خواهید یک پوشه فایل خاص را به اشتراک بگذارید این گزینه را انتخاب کنید.

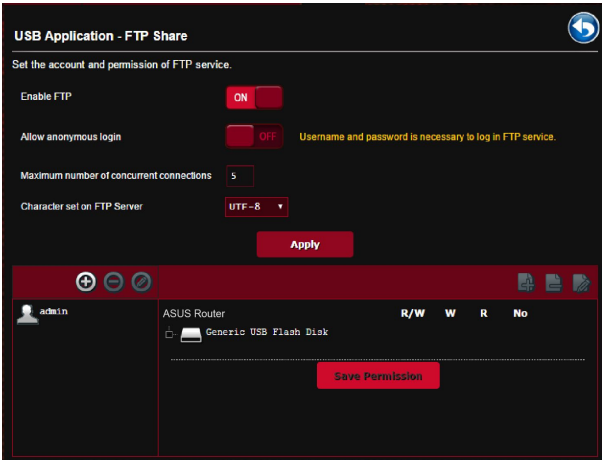
4. برای به کارگیری تغییرات روی **Apply (به کارگیری)** کلیک کنید.

استفاده از خدمات اشتراک گذاری FTP

اشتراک گذاری FTP یک سرور FTP را قادر می سازد فایل ها را از دیسک USB از طریق شبکه محلی شما یا اینترنت برای دستگاههای دیگر به اشتراک بگذارد.

مهم!

- مطمئن شوید که دیسک USB را به طور ایمن جدا کرده اید. جداسازی نادرست دیسک USB ممکن است باعث خراب شدن داده ها شود.
- برای جداسازی ایمن دیسک USB، به بخش **جدا کردن ایمن دیسک (Safely removing the USB disk** خود بروید **USB** در زیر **3.12.3 نظارت بر دستگاه (USB**.



برای استفاده از خدمات اشتراک گذاری FTP:

نکته: مطمئن شوید سرور FTP خود را از طریق AiDisk راه اندازی نموده اید. برای اطلاع از جزئیات بیشتر، به بخش **3.17.1 استفاده از AiDisk** مراجعه کنید.

1. از پنل پیمایش، روی زبانه **Advanced Settings (تنظیمات پیشرفته) > USB Application (برنامه USB) > FTP Share (اشتراک گذاری FTP)** کنید.
2. از فهرست پوشه ها، نوع حقوق دسترسی که می خواهید به پوشه های خاصی اعطا کنید را انتخاب نمایید:

- **R/W (خواندن/نوشتن):** برای اعطای دسترسی خواندن/نوشتن به یک پوشه خاص انتخاب کنید.
- **W (نوشتن)**: برای اعطای دسترسی فقط نوشتنی به یک پوشه خاص انتخاب کنید.

- **R (خواندن)**: برای اعطای دسترسی فقط خواندنی به یک پوشه خاص انتخاب کنید.
- **No (هیچ)**: اگر نمی خواهید یک پوشه خاص را به اشتراک بگذارید این گزینه را انتخاب کنید.

3. اگر مایلید، می توانید قسمت **Allow anonymous login (اجازه به ورود ناشناس)** را روی **ON (روشن)** بگذارید.
4. در قسمت **Maximum number of concurrent connections (حداکثر تعداد اتصالات همزمان)** تعداد دستگاه هایی که می توانند به طور همزمان به سرور اشتراک گذاری FTP متصل شوند را وارد کنید.
5. برای تأیید تغییرات روی **Apply (به کارگیری)** کلیک کنید.
6. برای دسترسی به سرور FTP، لینک **ftp://<hostname>.asuscomm.com** و نام کاربری و رمز وارد کنید FTP عبور خود در مرورگر وب یا برنامه دیگر.

3.17.3 3G/4G

مودم های 3G USB یا 4G را می توان به GT-AXE16000 وصل کرد تا امکان دسترسی به اینترنت را فراهم کند.

نکته: برای مشاهده لیست مودم های USB تأیید شده، لطفاً از سایت زیر را دیدن کنید:
http://event.asus.com/2009/networks/3gsupport/

برای تنظیم دسترسی به اینترنت 3G یا 4G:

1. از پنل پیمایش، روی **Advanced Settings (تنظیمات پیشرفته)** > **USB application (برنامه USB)** > **3G/4G** کلیک کنید.
2. در قسمت **Enable USB Modem (فعالسازی مودم USB)**، **Yes (بله)** را انتخاب کنید.
3. موارد زیر را تنظیم کنید:

- **Location (موقعیت):** موقعیت ارائه دهنده خدمت 3G یا 4G را از فهرست بازشو انتخاب کنید.
- **ISP:** ارائه دهنده خدمت اینترنت (ISP) را از فهرست بازشو انتخاب کنید.
- **خدمات APN (نام نقطه دسترسی) (اختیاری)**: برای آگاهی از جزئیات بیشتر، با ارائه دهنده خدمت 3G یا 4G خود تماس بگیرید.
- **Dial Number and PIN code (شماره دسترسی و پین کد)**: شماره دسترسی ارائه دهنده 3G یا 4G و پین کد برای اتصال.

نکته: پین کد ارائه دهندگان مختلف متفاوت است.

- **Username (نام کاربری) / Password (رمز عبور):** نام کاربری و رمز عبور را را اپراتور شبکه 3G یا 4G در اختیار شما قرار می دهد.
- **USB Adapter (آداپتور USB)**: آداپتور 3G USB یا 4G را از فهرست بازشو انتخاب کنید. اگر از مدل آداپتور USB مطمئن نیستید یا مدل مورد نظر در گزینه ها وجود ندارد، **Auto (خودکار)** را انتخاب کنید.

4. روی **Apply (به کارگیری)** کلیک کنید.

نکته: روتر دوباره راه اندازی می شود تا تنظیمات اجرا شوند.

VPN 3.18

شبکه خصوصی مجازی (VPN) ارتباط ایمنی را با یک کامپیوتر یا شبکه راه دور از طریق شبکه عمومی مانند اینترنت امکان پذیر می سازد.

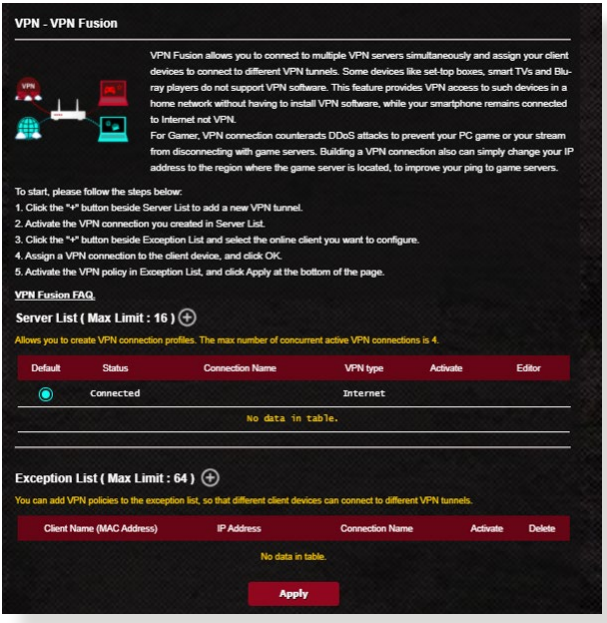
توجه: قبل از راه اندازی اتصال VPN، به آدرس IP یا نام دامنه سرور VPN نیاز دارید.

برای دسترسی به سرور VPN:

1. از صفحه پیمایش، به زبانه های **General(کلی)** > **VPN** بروید.
2. در قسمت **Enable PPTP VPN Server (فعال کردن سرور PPTP VPN)**، **ON(فعال)** کلیک کنید.
3. در لیست کشویی **VPN Details (جزئیات VPN)**، گزینه **Advanced Settings (تنظیمات پیشرفته)** را برای پیکربندی پیشرفته مانند پشتیبانی پخش، تأیید اعتبار، رمزگذاری VPN تنظیمات کلاینت انتخاب کنید IP و محدوده آدرس MPPE.
4. در قسمت **Network Place (Samba) Support (پشتیبانی محل شبکه (Samba)**، گزینه **Yes (بله)** را انتخاب کنید.
5. نام کاربری و رمز عبور را برای دسترسی به سرور VPN وارد کنید. روی ⊕ کلیک کنید.
6. برای **Apply (اعمال)** کلیک کنید.

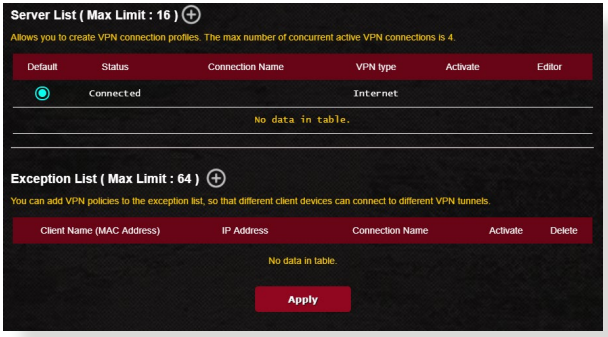
VPN Fusion 3.18.1

با VPN Fusion می توانید همزمان به چند سرور VPN وصل شوید و دستگاه های سرویس گیرنده تان را برای اتصال به تونل های VPN مختلف اختصاص دهید. بعضی از دستگاه ها مثل دستگاه های بازی خانگی، تلویزیون هوشمند و پخش کننده های Blu-ray از نرم افزار VPN پشتیبانی نمی کنند. با این ویژگی می توانید در چنین دستگاه هایی از طریق شبکه خانگی به VPN دسترسی داشته باشید بدون اینکه لازم باشد نرم افزار VPN نصب کنید، تلفن هوشمندتان نیز همچنان به اینترنت وصل است نه به VPN. برای کسانی که بازی می کنند اتصال VPN در برابر حمله های DDoS از آنها محافظت می کند تا بازی کامپیوتری یا پخش مستقیم از سرورهای بازی قطع نشود. با اتصال VPN به سادگی می توانید آدرس IP را به منطقه ای تغییر دهید که سرور بازی در آن واقع شده است، در نتیجه مدت زمان پینج برای آن سرورهای بازی بهتر می شود.



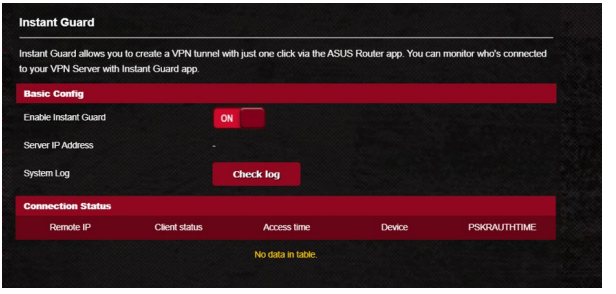
برای شروع به کار، مراحل زیر را دنبال کنید

1. روی ⊕ در کنار **Server List** (فهرست سرور) کلیک کنید تا تونل VPN جدید اضافه شود.
2. اتصال VPN ایجاد شده را در فهرست سرور فعال کنید.
3. روی ⊕ در کنار **Exception List** (فهرست استثنا) کلیک کنید و سرویس گیرنده آنلاین مورد نظر برای پیکربندی را انتخاب کنید.
4. یک اتصال VPN را به دستگاه سرویس گیرنده اختصاص دهید و روی **OK** (تأیید) کلیک کنید.
5. سیاست VPN را در **Exception List** (فهرست استثنا) فعال کنید و روی **Apply** (اعمال) در پایین صفحه کلیک کنید.



Instant Guard 3.18.2

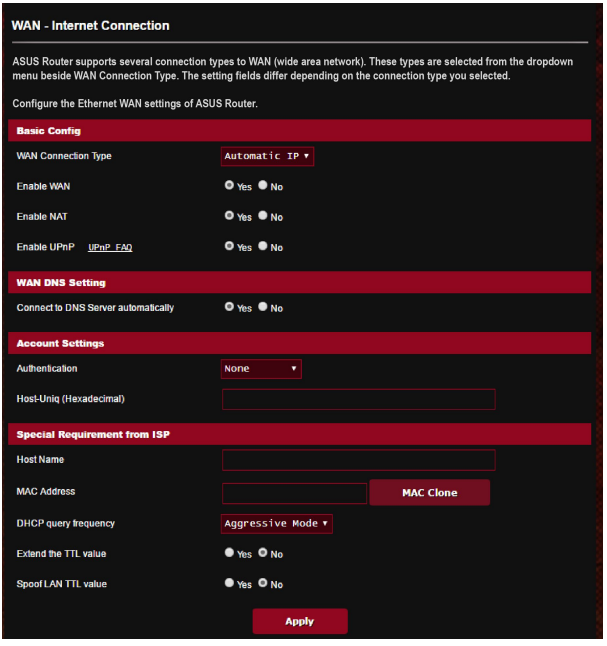
Instant Guard سرور VPN خصوصی شما را در روتر خودتان اجرا می کند. وقتی از تونل VPN استفاده می کنید، همه داده هایتان از سرور عبور می کند. با Instant Guard می توانید به طور کامل سرور خودتان را کنترل کنید و آن را به ایمن ترین راه حل ممکن تبدیل کنید.



3.19 WAN

3.19.1 اتصال به اینترنت

صفحه اتصال به اینترنت به شما این امکان را می دهد که انواع تنظیمات مختلف اتصالات WAN را پیکربندی کنید.



برای پیکربندی تنظیمات اتصال WAN:

1. از پنل پیمایش، به **Advanced Settings** (تنظیمات پیشرفته) > **WAN > Internet Connection (اتصال اینترنت)**.
2. تنظیمات زیر را به ترتیب پیکربندی کنید. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.

- **WAN Connection Type (نوع اتصال WAN)**: نوع ارائه دهنده خدمات اینترنت خود را انتخاب کنید. انتخاب ها عبارت اند از **Automatic IP** (IP خودکار)، **PPPoE**، **PPTP**، **L2TP** یا **static IP (IP ثابت)**. اگر روتر آدرس IP معتبری را پیدا نمی کند یا نوع اتصال WAN را نمی دانید، با ISP خود تماس بگیرید.

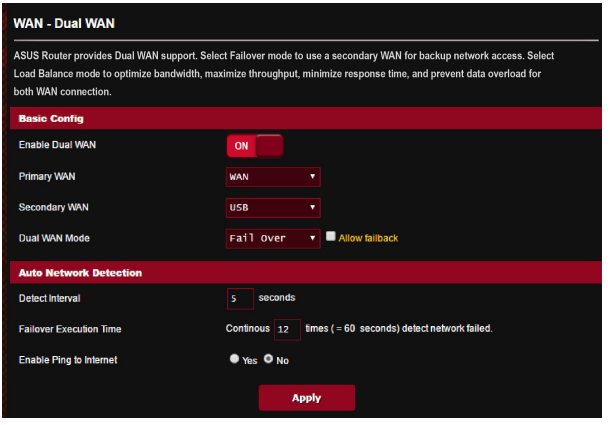
- **Enable WAN (فعال کردن WAN)**: **Yes (بله)** را انتخاب کنید تا امکان دسترسی روتر به اینترنت فراهم شود. برای جلوگیری از دسترسی به اینترنت **No (خیر)** را انتخاب کنید.
- **Enable NAT (فعال کردن NAT)**: NAT (برگردان نشانی شبکه) سیستمی است که در آن یک IP عمومی برای فراهم کردن دسترسی اینترنتی به سرویس گیرندگان شبکه با استفاده از آدرس IP اختصاصی در LAN، استفاده می شود. آدرس IP اختصاصی هر سرویس گیرنده شبکه در جدول NAT ذخیره می شود و برای تعیین مسیر بسته داده های ورودی استفاده می شود.
- **Enable UPnP (فعال کردن UPnP)**: UPnP (اتصال و اجرای سراسری) این امکان را می دهد که چندین دستگاه (مانند روتر ها، تلویزیون ها، سیستم های ضبط و پخش، کنسول های بازی و تلفن های همراه) را بتوان از طریق شبکه مبتنی بر IP با یا بدون کنترل مرکزی از طریق یک دروازه)، کنترل کرد. UPnP انواع رایانه ها را به هم متصل می کند و شبکه یکپارچه ای را برای پیکربندی از راه دور و انتقال داده فراهم می کند. با استفاده از UPnP، دستگاه شبکه ای جدید به طور خودکار شناخته می شود. وقتی دستگاه ها به شبکه متصل شدند، از راه دور برای پشتیبانی از برنامه های P۲P، بازی های تعاملی، کنفرانس ویدئویی و سرورهای وب یا پراکسی، پیکربندی می شوند. بر خلاف هدایت پورت که به طور دستی تنظیمات پورت را پیکربندی می کند، UPnP به طور خودکار روتر را پیکربندی می کند تا اتصالات ورودی و درخواست های مستقیم از رایانه خاص در شبکه محلی را بپذیرد.
- **Connect to DNS Server automatically (اتصال خودکار به سرور DNS)**: این امکان را به روتر می دهد تا به طور خودکار از ISP آدرس DNS IP را دریافت کند. DNS میزبان اینترنتی است که نام های اینترنتی را به آدرس های IP عددی بر می گرداند.
- **Authentication (تأیید اعتبار)**: این مورد ممکن است توسط بعضی از ISP ها تعیین شده باشد. با ISP خود مشورت کنید و در صورت نیاز آنها را پر کنید.
- **Host Name (نام میزبان)**: این قسمت امکان فراهم کردن نام میزبان برای روتر را به شما می دهد. این معمولاً یک الزام خاص از طرف ISP است. اگر ISP یک نام میزبان به رایانه شما اختصاص داده است، نام میزبان را اینجا وارد کنید.

- **MAC Address (نشانی MAC)**: نشانی MAC (کنترل دسترسی رسانه)، شناسه منحصر به فردی برای دستگاه شبکه بندی شده شما است. بعضی از ISP ها نشانی MAC دستگاه های شبکه بندی شده را که به سرویس آنها متصل می شود نظارت می کنند و هر دستگاه ناشناسی که می‌خواهد متصل شود را رد می کنند. برای جلوگیری از مشکلات اتصال به علت نشانی MAC ثبت نشده می توانید:
  - با ISP خود تماس بگیرید و نشانی MAC مرتبط با سرویس ISP را به روز رسانی کنید.
  - نشانی MAC روتر بی سیم ASUS را مطابق با نشانی MAC دستگاه شبکه بندی شده قبلی که ISP آن را می شناخت، مشابه سازی کنید یا تغییر دهید.
- **DHCP query frequency (تناوب جستار DHCP)**: تنظیمات فاصله شناسایی DHCP را برای جلوگیری از اضافه بار سرور DHCP، تغییر دهید.

3.19.2 WAN دوتایی

روتر بی سیم ASUS پشتیبان WAN دوتایی را فراهم می کند. می توانید ویژگی WAN دوتایی را برای هر کدام از این حالت ها تنظیم کنید:

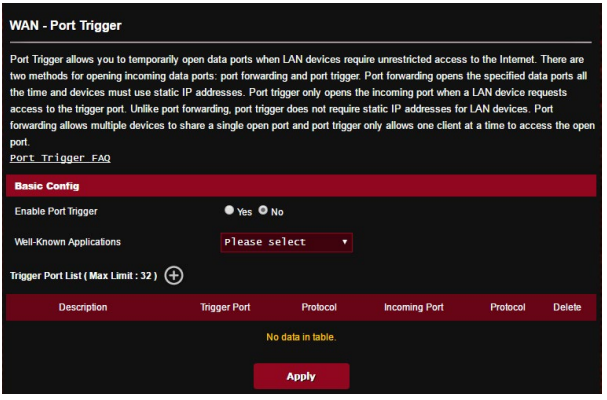
- **Failover Mode (حالت محافظت در برابر خرابی):** این حالت را انتخاب کنید تا بتوانید از WAN ثانویه به عنوان دسترسی شبکه پشتیبان استفاده کنید.
- **Load Balance Mode (حالت تعادل بارگذاری):** این حالت را انتخاب کنید تا پهنای باند را بهینه سازی کنید، زمان پاسخ دهی را به حداقل برسانید و از بارگذاری اضافه داده در اتصالات اولیه و ثانویه WAN جلوگیری کنید.



3.19.3 راه اندازی پورت

راه اندازی محدوده پورت، پورت ورودی مشخصی را برای مدت زمان محدود باز می کند تا وقتی که سرویس گیرنده شبکه محلی اتصال خارجی با یک پورت تعیین شده برقرار کند. راه اندازی پورت در زمینه های زیر استفاده می شود:

- بیش از یک سرویس گیرنده محلی نیاز به هدایت پورت برای برنامه مشابه در زمان متفاوت داشته باشد.
- برنامه نیاز به پورت های ورودی خاص داشته باشد که با پورت های خروجی تفاوت داشته باشد.



برای تنظیم راه اندازی پورت:

1. از پنل پیمایش، به **Advanced Settings** (تنظیمات پیشرفته) > **WAN > Port Trigger** (**راه اندازی پورت**).
2. در قسمت **Enable Port Trigger** (**فعال کردن راه اندازی پورت**) روی **Yes** (**بله**) **کلیک کنید**.
3. در قسمت **Well-Known Applications** (**برنامه های معروف**)، بازی های پرطرفدار و سرویس های وب را انتخاب کنید و به فهرست راه اندازی پورت اضافه کنید.
4. در جدول **Trigger Port List** (**فهرست پورت های راه اندازی**)، اطلاعات زیر را وارد کنید:

- **Description** (**توضیح**): یک نام مختصر یا توضیحی برای سرویس وارد کنید.
- **Trigger Port** (**پورت راه اندازی**): برای باز کردن پورت ورودی، یک پورت راه اندازی تعیین کنید.

- **Protocol (پروتکل)**: پروتکل، TCP یا UDP را انتخاب کنید.
- **Incoming Port (پورت ورودی)**: یک پورت ورودی تعیین کنید تا داده ورودی از اینترنت را دریافت کنید.

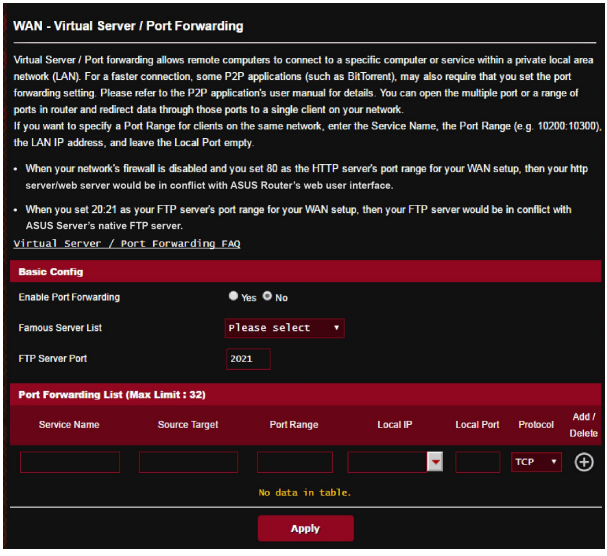
5. روی **Add (اضافه کردن)** کلیک کنید تا اطلاعات راه اندازی پورت را در فهرست وارد کنید. روی دکمه **Delete (حذف کردن)** کلیک کنید تا اطلاعات راه اندازی پورت را از فهرست پاک کنید.
6. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.

تذکرها:

- رایانه سرویس گیرنده هنگام اتصال به سرور IRC با استفاده از محدوده پورت راه اندازی 66660-7000، اتصال خروجی برقرار می کند. سرور IRC با تأیید نام کاربری و ایجاد اتصال جدید با استفاده از پورت ورودی رایانه سرویس گیرنده، پاسخ می دهد.
- اگر راه اندازی پورت غیر فعال شود، روتر اتصال را قطع می کند به این دلیل که نمی تواند تشخیص دهد کدام رایانه برای دسترسی به IRC درخواست فرستاده است. وقتی راه اندازی پورت فعال شود، روتر برای دریافت داده ورودی، یک پورت ورودی انتخاب می کند. وقتی مدت زمان خاص سپری شد، پورت ورودی بسته می شود زیرا روتر نمی تواند زمان متوقف شدن برنامه را تشخیص دهد.
- راه اندازی پورت این امکان را تنها به یک سرویس گیرنده در شبکه می دهد تا از سرویس خاص و پورت ورودی خاص به طور همزمان استفاده کند.
- نمی توانید از یک برنامه برای راه اندازی پورت چندین رایانه به طور همزمان استفاده کنید. روتر فقط پورت را به آخرین رایانه ای که درخواست فرستاده یا راه اندازی شده است، هدایت می کند.

3.19.4 سرور مجازی/هدایت پورت

هدایت پورت روشی است که ترافیک شبکه را از اینترنت به پورت خاص یا محدود خاص پورت یک دستگاه یا چندین دستگاه در شبکه محلی هدایت می کند. راه اندازی هدایت پورت روی روتر این امکان را می دهد که رایانه های خارج از شبکه به سرویس های خاص که توسط رایانه های داخل شبکه فراهم می شود، دسترسی داشته باشند.



برای تنظیم هدایت پورت:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **WAN** > زبانه **Virtual Server / Port Forwarding (سرور مجازی/هدایت پورت)** بروید.
2. در قسمت **Enable Port Forwarding (فعال کردن هدایت پورت)** روی **Yes (بله)** کلیک کنید.
3. در قسمت **Famous Server List (فهرست سرور شناخته شده)**، نوع سرویسی که می‌خواهید به آن دسترسی داشته باشید را انتخاب کنید.
4. در قسمت **Famous Game List (فهرست بازی شناخته شده)**، بازی پرطرفداری که می‌خواهید به آن دسترسی داشته باشید را انتخاب کنید. این مورد پورت مورد نیاز برای بازی آنلاین پرطرفداری که انتخاب کرده اید را نشان می دهد.

5. در جدول **Port Forwarding List (فهرست هدایت پورت)**، اطلاعات زیر را وارد کنید:

- **Service Name (نام خدمات)**: نام خدمات را وارد کنید.
- **Port Range (محدوده پورت)**: اگر می خواهید محدوده پورت را در یک شبکه برای سرویس گیرندگان تعیین کنید، نام خدمات، محدوده پورت (برای مثال 10200:10300)، آدرس LAN IP را وارد کنید و پورت محلی را خالی بگذارید. محدوده پورت قالب های مختلفی از قبیل محدوده پورت (300:350)، پورت های تک (566، 789) یا ترکیبی (1015:1024، 3021) را قبول می کند.

تذکرها:

- وقتی دیواره آتش شبکه غیر فعال شود و شما 80 را به عنوان محدوده پورت سرور HTTP برای راه اندازی WAN تنظیم کرده باشید، سرور http یا سرور وب با رابط کاربر وب روتر ناسازگار می شود.
- شبکه از پورت برای رد و بدل کرده داده استفاده می کند، همراه با هر پورت شماره پورت و وظیفه خاص آن تعیین شده است. برای مثال، پورت 80 برای HTTP استفاده می شود. یک پورت خاص هر دفعه فقط توسط یک برنامه یا سرویس استفاده می شود. بنابراین، وقتی دو رایانه به طور همزمان تلاش می‌کنند که از طریق یک پورت به داده دسترسی داشته باشند، با مشکل مواجه می شوند. برای مثال، نمی توانید به طور هم زمان هدایت پورت را برای پورت 100 در دو رایانه تنظیم کنید.

- **Local IP (IP محلی)**: نشانی LAN IP سرویس گیرنده را وارد کنید.

نکته: از یک آدرس IP برای سرویس گیرنده محلی استفاده کنید تا هدایت پورت به درستی کار کند. برای کسب اطلاعات بیشتر به بخش **LAN 3.11** مراجعه کنید.

- **Local Port (پورت محلی):** یک پورت خاص را وارد کنید تا بسته های ارسال شده را دریافت کنید. اگر می‌خواهید بسته های ورودی به محدوده پورت تعیین شده دوباره ارسال شود، این قسمت را خالی بگذارید.
- **Protocol (پروتکل)**: پروتکل را انتخاب کنید. اگر مطمئن نیستید، **BOTH (هر دو)** را انتخاب کنید.

6. روی **Add (اضافه کردن)** ⊕ کلیک کنید تا اطلاعات راه اندازی پورت را در فهرست وارد کنید. روی دکمه **Delete (حذف کردن)** ⊖ کلیک کنید تا اطلاعات راه اندازی پورت را از فهرست پاک کنید.
7. وقتی انجام شد، روی Apply (به کارگیری) کلیک کنید.

برای بررسی این که هدایت پورت با موفقیت پیکربندی شده است:

- مطمئن شوید که سرور یا برنامه نصب و اجرا شده است.
- به سرویس گیرنده خارج از LAN که به اینترنت دسترسی داشته باشد نیاز دارید (که به آن "سرویس گیرنده اینترنت" می گویند). این سرویس گیرنده نباید به روتر ASUS متصل باشد.
- در سرویس گیرنده اینترنت، از WAN IP روتر استفاده کنید تا به سرور دسترسی پیدا کنید. اگر هدایت پورت موفق باشد، می توانید به فایل ها و برنامه ها دسترسی پیدا کنید.

تفاوت بین راه اندازی پورت و هدایت پورت:

- راه اندازی پورت حتی بدون تنظیم آدرس LAN IP خاص کار می کند. بر عکس هدایت پورت که نیاز به آدرس LAN IP ثابت دارد، راه اندازی پورت این امکان را می دهد که هدایت پورت پویا از روتر استفاده کند. محدوده های پورت مشخص شده پیکربندی می شوند تا برای مدت زمان محدود اتصالات ورودی را امکان پذیر کنند. راه اندازی پورت این امکان را به چند رایانه می دهد تا برنامه هایی را اجرا کنند که به طور طبیعی نیاز به هدایت دستی پورت ها به هر رایانه در شبکه دارند.
- راه اندازی پورت ایمن تر از هدایت پورت است زیرا پورت های ورودی همیشه باز نیستند. پورت های ورودی تنها زمانی باز می شوند که برنامه اتصال خروجی را از طریق پورت راه اندازی شده، برقرار کند.

DMZ 3.19.5

DMZ مجازی اینترنت را در دسترس یک سرویس گیرنده قرار می دهد، و به سرویس گیرنده این امکان را می‌دهد که تمام بسته های ورودی به شبکه محلی را دریافت کند.

ترافیک ورودی اینترنت معمولاً رها می شود و تنها اگر هدایت پورت یا راه اندازی پورت روی شبکه پیکربندی شده باشد به یک سرویس گیرنده خاص انتقال داده می شود. در پیکربندی DMZ، یک سرویس گیرنده شبکه تمام بسته های ورودی را دریافت می کند.

تنظیم DMZ روی شبکه زمانی مفید است که نیاز دارید پورت های ورودی باز باشند یا می خواهید میزبان یک دامنه، وب یا سرور ایمیل باشید.

احتیاط: باز کردن تمام پورت های یک سرویس گیرنده در اینترنت، شبکه را در برابر حملات خارجی آسیب پذیر می‌کند. لطفاً هنگام استفاده از DMZ مراقب خطرات امنیتی باشید.

برای راه‌اندازی DMZ:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته) > WAN > DMZ**.
2. تنظیمات زیر را پیکربندی کنید. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.

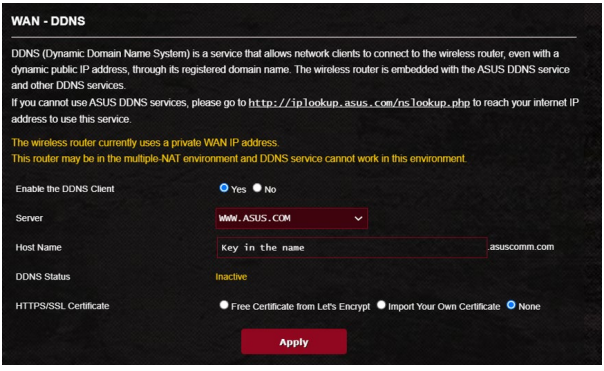
- **IP address of Exposed Station (نشانی IP ایستگاه آشکار):** نشانی LAN IP سرویس گیرنده ای که سرویس DMZ را ایجاد می کند و به اینترنت دسترسی دارد را وارد کنید. مطمئن شوید که سرویس گیرنده سرور دارای نشانی IP ثابت است.

برای حذف DMZ:

1. نشانی LAN IP سرویس گیرنده را از جعبه متن **IP Address of Exposed Station (نشانی IP ایستگاه آشکار)** پاک کنید.
2. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.

DDNS 3.19.6

تنظیم DDNS (DNS پویا) به شما این امکان را می دهد که خارج از شبکه از طریق سرویس ASUS DDNS ایجاد شده یا سرویس دیگر DDNS به روتر دسترسی پیدا کنید.



برای راه اندازی DDNS:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **WAN** > **DDNS**.
2. تنظیمات زیر را به ترتیب پیکربندی کنید. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.

- **Enable the DDNS Client (فعال کردن سرویس گیرنده DDNS)**: DDNS را فعال کنید تا به جای نشانی WAN IP از طریق نام DNS به روتر ASUS دسترسی پیدا کنید.
- **Server and Host Name (نام سرور و میزبان)**: ASUS DDNS یا DDNS را انتخاب کنید. اگر می خواهید از ASUS DDNS استفاده کنید، نام میزبان را با فرمت xxx.asuscomm.com (که xxx نام میزبان شما است) وارد کنید.
- اگر می خواهید از سرویس DDNS متفاوتی استفاده کنید، روی FREE TRIAL کلیک کنید و ابتدا به صورت آنلاین ثبت نام کنید. نام کاربر یا نشانی ایمیل و رمز عبور یا قسمت های کلید DDNS را وارد کنید.
- **فعال کردن فرانویسه:** اگر سرویس DDNS شما به فرانویسه نیاز دارد، آن را فعال کنید.

تذکرها:

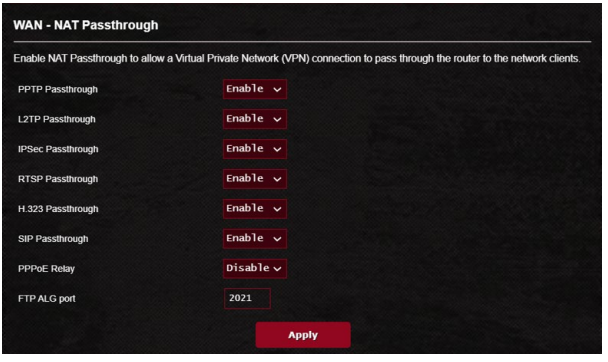
سرویس DDNS تحت این شرایط کار نمی کند:

- وقتی که روتر بی سیم از آدرس WAN IP اختصاصی استفاده می کند (192.168.x.x، 10.x.x.x یا 172.16.x.x)، که با متنی به رنگ زرد نشان داده شده است.
- ممکن است روتر در شبکه ای باشد که از چند جدول NAT استفاده می کند.

3.19.7 گذرگاه NAT

گذرگاه NAT این امکان را می دهد که اتصال شبکه اختصاصی مجازی (VPN) از روتر به سرویس گیرنده‌های شبکه برود. گذرگاه PPTP، گذرگاه L2TP، گذرگاه IPsec و گذرگاه RTSP به صورت پیش فرض فعال هستند.

برای فعال یا غیر فعال کردن تنظیمات گذرگاه NAT، به **Advanced Settings (تنظیمات پیشرفته) > WAN (شبکه گسترده) > NAT Passthrough (گذرگاه NAT)**. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.



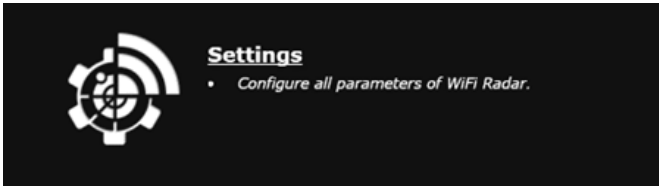
3.20 رادار WiFi

Wi-Fi Radar یک ابزار پیشرفته تجزیه وتحلیل برای شبکه بی سیم است که برای عیب یابی، به دقت کانال ها و داده بسته ای را مورد بررسی قرار می دهد.

توجه: اگر WiFi Radar را فعال کنید ممکن است عملکرد بی سیم قطع شود. فقط در هنگام لزوم WiFi Radar را فعال کنید.

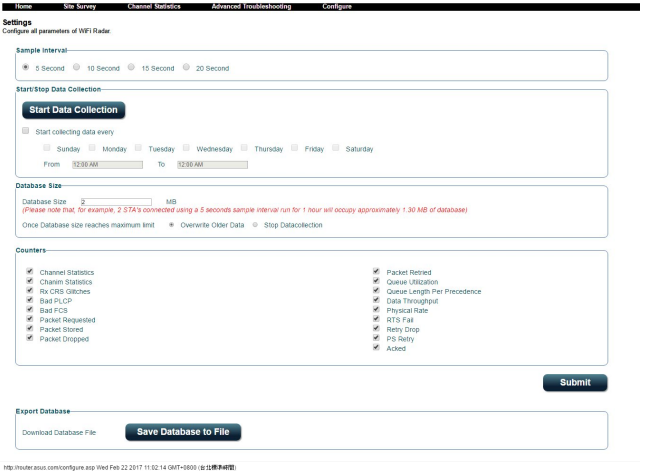
برای استفاده از WiFi Radar:

1. از صفحه پیمایش، به **General (موارد کلی) > WiFi Radar (رادار WiFi)**، به تنظیمات بروید و همه پارامترهای WiFi Radar را پیکربندی کنید.



2. روی **Start Data Collection (شروع جمع آوری داده)** بروید و برنامه زمانی را برای ضبط داده تنظیم کنید.

3. بعد از تنظیم همه پارامترها روی **Submit (ارسال)** کلیک کنید.

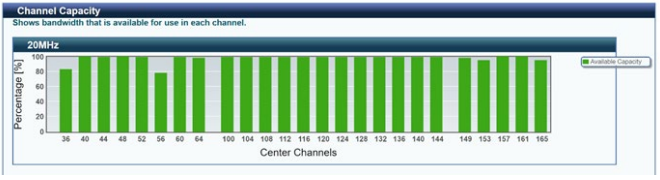


3.20.1 نظرسنجی سایت WiFi

نظرسنجی سایت WiFi به شما امکان می دهد شبکه های بی سیم را در اطرافتان جستجو کنید.

3.20.2 اطلاعات آماری کانال بی سیم

این ویژگی میزان مصرف همه باندها و اطلاعات آماری مربوط به توزیع کانال را در اطرافتان نمایش می دهد.



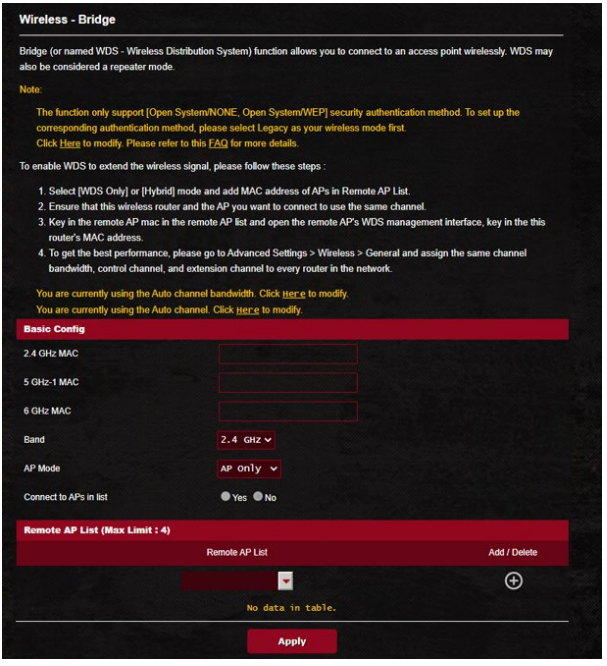
3.20.3 عیب یابی پیشرفته

این ویژگی، اطلاعات آماری مربوط به مشکلات WiFi را در اطرافتان نمایش می دهد.

3.21 بی سیم

3.21.1 موارد کلی

زبانه موارد کلی امکان پیکربندی تنظیمات بی سیم اولیه را به شما می دهد.



برای پیکربندی تنظیمات بی سیم اولیه:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته) > Wireless (بی سیم) > General (موارد کلی)**.
2. برای شبکه بی سیم خود، باند فرکانس 2.4 گیگاهرتزی, 5 گیگاهرتز-1 ی یا 5 گیگاهرتز-2 ی انتخاب کنید.
3. اگر می خواهید از عملکرد اتصال هوشمند استفاده کنید، در قسمت **Enable Smart Connect (فعالسازی اتصال هوشمند)**، لغزانه را روی **ON (روشن)** قرار دهید. این عملکرد به طور خودکار سرویس گیرنده ها در شبکه شما را برای داشتن سرعت بهینه به باند مناسب 2.4 گیگاهرتز, 5 گیگاهرتز-1 ی یا 5 گیگاهرتز-2 متصل می سازد.

4. نام خاصی را که حداکثر 32 نویسه دارد برای SSID (شناسه دستگاه خدمت) یا نام شبکه انتخاب کنید تا شبکه بی سیم خود را تشخیص دهید. دستگاه های Wi-Fi می توانند از طریق SSID اختصاصی، شبکه بی سیم را تشخیص دهند و به آن متصل شوند. زمانی که SSIDهای جدیدی در تنظیمات ذخیره شوند، SSIDها در نشان اطلاعات به روز رسانی می شوند.

نکته: می توانید SSIDهای منحصر به فردی به باندهای فرکانس 2.4 گیگاهرتزی, 5 گیگاهرتز-1ی و 5 گیگاهرتز-2ی اختصاص دهید.

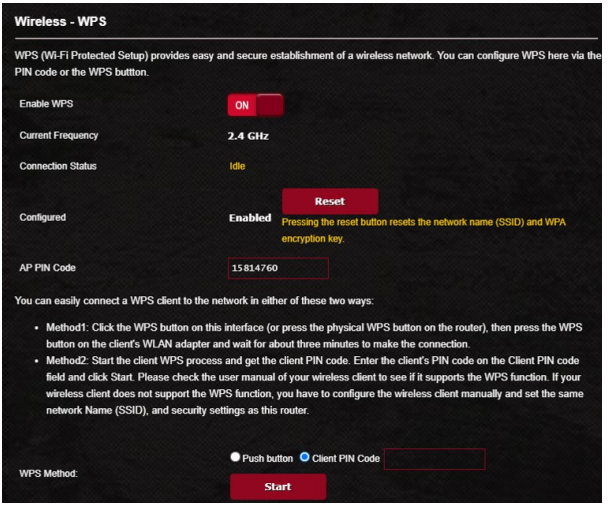
---

5. در قسمت **Hide SSID (پنهان کردن SSID)**، **Yes (بله)** را انتخاب کنید تا دستگاه های بی‌سیم نتوانند SSID شما را تشخیص دهند. زمانی که این عملکرد را فعال کردید، در دستگاه بی‌سیم، SSID را باید به طور دستی وارد کنید تا به شبکه بی سیم متصل شوید.
6. هریک از گزینه های حالت بی سیم را انتخاب کنید تا نوع دستگاه های بی سیم را که می‌توانید به روتر بی سیم متصل کنید مشخص کنید:
   - **Auto (خودکار):** خودکار را انتخاب کنید تا امکان اتصال دستگاه های 802.11ac، 802.11n، 802.11g، 802.11b را به روتر بی سیم فراهم کنید.
   - **N only (فقط N): N only (فقط N)** را انتخاب کنید تا کارایی N بی سیم را به حداکثر برسانید. این تنظیم از اتصال دستگاه های 802.11g و 802.11b به روتر بی سیم جلوگیری می کند.
   - **Legacy (موروثی)**: **Legacy (موروثی)** را انتخاب کنید تا امکان اتصال دستگاه های 802.11b/g/n را به روتر بی سیم فراهم کنید. با این وجود، سخت افزارهایی که به طور طبیعی از 802.11n پشتیبانی می کنند، فقط با سرعت 54 مگابیت در ثانیه کار می کنند.
7. کانال عملکرد یا کنترل را برای روتر بی سیم انتخاب کنید. **Auto (خودکار)** را انتخاب کنید تا به روتر بی سیم اجازه دهید کانالی را با کمترین میزان تداخل به صورت خودکار انتخاب کند.
8. پهنای باند کانال را انتخاب کنید تا سرعت های انتقال بالاتر را تطبیق دهد.
9. روش تأیید اعتبار را انتخاب کنید.
10. وقتی انجام شد، روی **Apply (به کارگیری)** کلیک کنید.

3.21.2 WPS

WPS (تنظیم حفاظت شده WiFi) استاندارد امنیت بی سیم است که امکان اتصال آسان دستگاه ها به شبکه بی سیم را فراهم می کند. عملکرد WPS را از طریق پین کد و دکمه WPS می توانید پیکربندی کنید.

نکته: مطمئن شوید که دستگاه ها از WPS پشتیبانی می کنند.



برای فعالسازی WPS در شبکه بی سیم:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Wireless (بی سیم)** > **WPS**.
2. در قسمت **Enable WPS (فعالسازی WPS)**، لغزانه را روی **ON (روشن)** قرار دهید.
3. WPS به صورت پیش فرض از فرکانس 2.4 گیگاهرتز استفاده می کند. اگر می خواهید فرکانس را به 5 گیگاهرتز تغییر دهید، عملکرد WPS را **OFF (خاموش)** کنید، روی **Switch Frequency (تغییر فرکانس)** در قسمت **Current Frequency (فرکانس فعلی)** کلیک کنید و دوباره WPS را **ON (روشن)** کنید.

نکته: WPS از تأیید اعتباری که از Open System, WPA-Personal و WPA2-Personal استفاده می کند، پشتیبانی می کند. WPS از شبکه بی سیمی که از روش رمزگذاری Shared Key، WPA-Enterprise، WPA2-Enterprise و استفاده می کند، پشتیبانی نمی کند RADIUS.

4. در قسمت روش WPS، **Push button (دکمه فشاری)** یا کد **Client PIN Code (پین سرویس گیرنده)** را انتخاب کنید. اگر **Push button (دکمه فشاری)** را انتخاب کرده اید، به مرحله 5 بروید. اگر **Client PIN Code (پین سرویس گیرنده)** را انتخاب کرده اید، به مرحله 6 بروید.

5. برای تنظیم WPS با استفاده از دکمه WPS روتر، مراحل زیر را دنبال کنید:

الف. روی **Start (شروع)** کلیک کنید یا دکمه WPS را که در پشت روتر بی سیم قرار دارد فشار دهید.

ب. دکمه WPS را روی دستگاه بی سیم فشار دهید. این دکمه را با لوگوی WPS به راحتی می‌توان تشخیص داد.

نکته: برای موقعیت دکمه WPS، دستگاه بی سیم خود یا دفترچه راهنمای کاربر را بررسی کنید.

پ. روتر بی سیم دستگاه های WPS موجود را جستجو می کند. اگر روتر بی سیم هیچ نوع دستگاه WPS را پیدا نکند، به حالت آماده به کار تغییر وضعیت می دهد.

6. برای تنظیم WPS با استفاده از کد پین سرویس گیرنده، مراحل زیر را دنبال کنید:

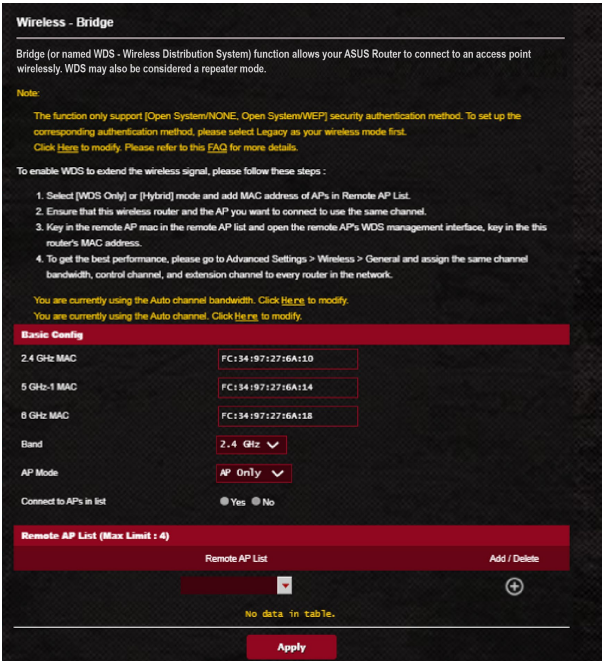
الف. کد پین WPS را در دفترچه راهنمای کاربر دستگاه بی سیم یا در خود دستگاه قرار دهید.

ب. کد پین سرویس گیرنده را در قسمت متن وارد کنید.

پ. روی **Start (شروع)** کلیک کنید تا روتر بی سیم را در حالت بررسی WPS قرار دهید. نشانگرهای LED روتر به سرعت سه بار چشمک می زنند تا زمانی که تنظیم WPS کامل شود.

3.21.3 رابط

رابط یا WDS (سیستم توزیع بی سیم) به شما این امکان را می دهد که روتر بی سیم ASUS را منحصراً به نقطه دسترسی بی سیم دیگری وصل کنید، و از دسترسی سایر دستگاه ها یا ایستگاه های بی سیم به روتر بی‌سیم ASUS جلوگیری می کند. همچنین هنگامی که روتر بی سیم ASUS با نقطه دسترسی یا دستگاه‌های بی سیم دیگری ارتباط برقرار می کند، تکرار کننده بی سیم محسوب می شود.



برای راه اندازی رابط بی سیم:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Wireless (بی سیم)** > **WDS** بروید.
2. باند فرکانس را برای رابط بی سیم انتخاب کنید.

3. در قسمت **AP Mode (حالت AP)**، هر یک از گزینه های زیر را انتخاب کنید:

- **AP Only (فقط AP)**: عملکرد رابط بی سیم را غیر فعال کنید.
- **WDS Only (فقط WDS)**: ویژگی رابط بی سیم را فعال کنید ولی از اتصال سایر دستگاه ها یا ایستگاه ها به روتر جلوگیری می کند.
- **HYBRID (هیبرید)**: ویژگی رابط بی سیم را فعال کنید تا امکان اتصال سایر دستگاه ها یا ایستگاه ها به روتر فراهم شود.

نکته: در حالت هیبرید، دستگاه های بی سیم متصل به روتر بی سیم ASUS فقط نیمی از سرعت اتصال نقطه دسترسی را دریافت می کنند.

---

4. در قسمت **Connect to APs in list (اتصال به APها در فهرست)**، اگر می خواهید به نقطه دسترسی فهرست شده در فهرست APهای راه دور وصل شوید، روی **Yes (بله)** کلیک کنید.

5. به صورت پیش فرض، کانال کنترل و کارکرد رابط بی سیم روی **Auto (خودکار)** تنظیم است تا این امکان را به روتر بدهد که به طور خودکار کانالی را با حداقل میزان تداخل انتخاب کند.

   می توانید **Control Channel (کانال کنترل)** را از **Advanced Settings (تنظیمات پیشرفته) > Wireless (بی سیم) > General (موارد کلی)** تغییر دهید.

نکته: موجود بودن کانال در هر کشور یا منطقه متفاوت است.

---

6. در فهرست APهای راه دور، نشانی MAC را وارد کنید و روی دکمه **Add (اضافه کردن)** ⊕ کلیک کنید تا نشانی MAC سایر نقاط دسترسی موجود وارد شود.

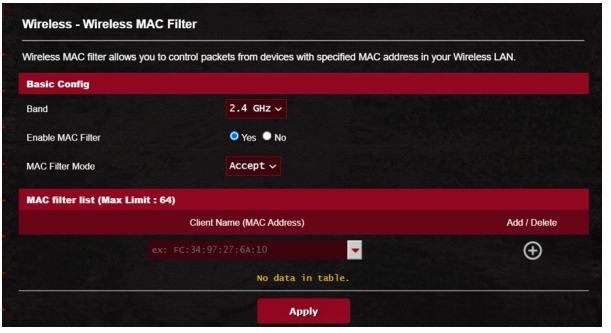
نکته: هر نقطه دسترسی اضافه شده به فهرست باید در همان کانال کنترلی قرار گیرد که روتر بی سیم ASUS قرار دارد.

---

7. روی **Apply (به کارگیری)** کلیک کنید.

3.21.4 فیلتر MAC بی سیم

بسته های انتقال یافته به نشانی MAC (کنترل دسترسی رسانه) تعیین شده را فیلتر MAC بی سیم موجود در شبکه بی سیم کنترل می کند.

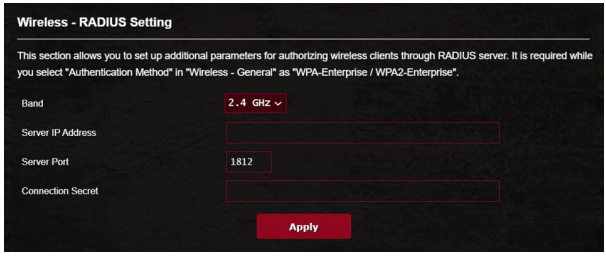


برای راه اندازی فیلتر MAC بی سیم:

1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Wireless (بی سیم)** > **Wireless MAC Filter (فیلتر MAC بی سیم)** بروید.
2. باند فرکانس را انتخاب کنید.
3. در قسمت **Enable Mac Filter (فعال کردن فیلتر Mac)**، **Yes (بله)** را علامت بزنید.
4. در فهرست کشویی **MAC Filter Mode (حالت فیلتر MAC)**، **Accept (پذیرش)** یا **Reject (رد کردن)** را انتخاب کنید.
   - برای ایجاد دسترسی دستگاه ها به شبکه بی سیم در فهرست فیلتر های MAC، **Accept (پذیرش)** را انتخاب کنید.
   - برای عدم ایجاد دسترسی دستگاه ها به شبکه بی سیم در فهرست فیلتر های MAC، **Reject (رد کردن)** را انتخاب کنید.
5. در فهرست فیلترهای MAC، روی دکمه **Add (اضافه کردن)** ⊕ کلیک کنید و نشانی آدرس MAC دستگاه بی سیم را وارد کنید.
6. روی **Apply (به کارگیری)** کلیک کنید.

3.21.5 تنظیمات RADIUS

هنگامی که WPA2-Enterprise، WPA-Enterprise، یا Radius با 802.1x را به عنوان حالت تأیید خود انتخاب می کنید، تنظیمات RADIUS (تماس تأیید راه دور در خدمات کاربر) یک لایه امنیتی اضافی ایجاد می کند.



برای راه اندازی تنظیمات RADIUS بی سیم:

1. مطمئن شوید که حالت تأیید اعتبار روتر بی سیم روی WPA-Enterprise یا WPA2-Enterprise تنظیم است.

نکته: لطفاً برای پیکربندی حالت تأیید روتر بی سیم، به بخش **General 3.21.1 (موارد کلی)** مراجعه کنید.

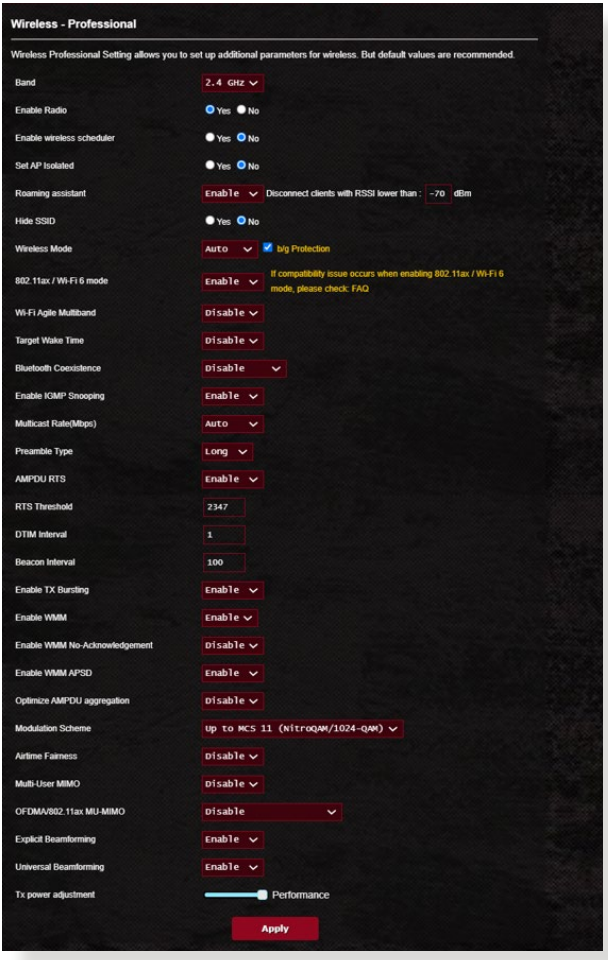
---

2. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **Wireless (بی سیم)** > **RADIUS Setting (تنظیمات RADIUS)** بروید.
3. باند فرکانس را انتخاب کنید.
4. در قسمت **Server IP Address (نشانی IP سرور)**، نشانی IP سرور RADIUS را وارد کنید.
5. در قسمت **Server Port (پورت سرور)**، پورت سرور را وارد کنید.
6. در قسمت **Connection Secret (اتصال مخفی)**، برای دسترسی به سرور رمز عبور وارد کنید.
7. روی **Apply (به کارگیری)** کلیک کنید.

3.21.6 Professional (حرفه ای)

صفحه حرفه ای، گزینه های پیکربندی پیشرفته ای ارائه می دهد.

نکته: توصیه می کنیم که در این صفحه از مقادیر پیش فرض استفاده کنید.



در صفحه **Professional Settings (حرفه ای تنظیمات)**، می توانید موارد زیر را پیکربندی کنید:

- **Band (باند)**: باند فرکانسی که تنظیمات حرفه ای روی آن اعمال خواهد شد را انتخاب کنید.

- **Enable Radio (فعال کردن رادیو)**: برای فعال کردن شبکه بی سیم، **Yes (بله)** را انتخاب کنید. برای غیرفعال کردن شبکه بی سیم، **No (نه)** را انتخاب کنید.
- **Enable wireless scheduler (فعال کردن برنامه ریز بی سیم):** برای فعال کردن برنامه ریز بی سیم و پیکربندی آن گزینه **Yes (بله)** را انتخاب کنید. برای غیرفعال کردن برنامه ریز بی سیم گزینه **No (خیر)** را انتخاب کنید.
- **Date to Enable Radio (weekdays) (تاریخ فعال کردن رادیو (روزهای هفته))**: می توانید روزهای هفته که می خواهید شبکه بی سیم فعال باشد را تعیین کنید.
- **Time of Day to Enable Radio (زمانی از روز که می خواهید رادیو فعال باشد)**: می‌توانید محدوده زمانی که می خواهید شبکه بی سیم فعال باشد را تعیین کنید.
- **Date to Enable Radio (weekend) (تاریخ فعال کردن رادیو (آخر هفته))**: می توانید روزهای آخر هفته ای که می خواهید شبکه بی سیم فعال باشد را تعیین کنید.
- **Time of Day to Enable Radio (زمانی از روز که می خواهید رادیو فعال باشد)**: می‌توانید محدوده زمانی که شبکه بی سیم در آخر هفته فعال است را تعیین کنید.
- **Set AP Isolated (جدا کردن AP)**: گزینه جدا کردن AP از ارتباط دستگاه های بی سیم روی شبکه شما جلوگیری می کند. این ویژگی زمانی مفید است که کاربران مدام به شبکه وصل شوند یا آن را ترک کنند. برای فعال کردن این گزینه، **Yes** (بله) یا برای غیر فعال کردن آن **No** (خیر) را انتخاب کنید.
- **Roaming assistant (دستیار رومینگ):** در پیکربندی های شبکه که چندین نقطه دسترسی یا تکرارکننده بی سیم وجود دارد، سرویس گیرنده های بی سیم بعضی مواقع نمی توانند به صورت خودکار به AP های ناشناس موجود متصل شوند زیرا همچنان به روتر بی سیم اصلی وصل هستند. این تنظیم را فعال کنید تا اگر قدرت سیگنال در آستانه ای خاص است و به یک سیگنال قوی تر وصل می شود، سرویس گیرنده از روتر بی سیم اصلی قطع شود.
- **Enable IGMP Snooping (فعال کردن جستجوی IGMP):** این عملکرد را فعال کنید تا IGMP (پروتکل مدیریت گروه اینترنتی) در بین دستگاه ها تحت بررسی باشد و ترافیک چندپخشی بی سیم بهینه سازی شود.
- **Multicast Rate (Mbps) (سرعت پخش چندگانه (مگا بیت در ثانیه))**: سرعت انتقال چند بخش را انتخاب کنید یا روی **Disable (غیر فعال کردن)** کلیک کنید تا انتقال تکی به طور هم زمان خاموش شود.
- **Preamble Type (نوع پیشایند)**: نوع پیشایند مدت زمانی که روتر برای CRC (بررسی افزونگی چرخه ای) صرف می کند را تعیین می نماید. CRC

روشی برای شناسایی خطاها در حین انتقال داده ها است. برای شبکه بی سیم مشغول با ترافیک شبکه بالا، **Short (کوتاه)** را انتخاب کنید. اگر شبکه بی سیم شما از دستگاه های بی سیم قدیمی تشکیل شده است، **Long (بلند)** را انتخاب کنید.

- **AMPDU RTS:** این عملکرد را فعال کنید تا گروهی از فریم ها قبل از مخابره ایجاد شوند، همچنین از TRS برای هر AMPDU برای ارتباط بین دستگاه های 802.11g و 802.11b استفاده شود.
- **RTS Threshold (آستانه RTS):** مقدار کمتری را برای آستانه RTS (درخواست ارسال) انتخاب کنید تا ارتباطات بی سیم در یک شبکه بی سیم شلوغ با ترافیک شبکه بالا و تعداد زیادی دستگاه بی سیم، بهتر شود.
- **DTIM Interval (فاصله زمانی DTIM)**: فاصله زمانی DTIM (پیام اعلام ترافیک تحویل) یا سرعت هدایت داده، فاصله زمانی قبل از ارسال سیگنال به دستگاه بی سیم در حالت خواب است و نشان می دهد که بسته داده منتظر دریافت شدن است. مقدار پیش فرض 3 میلی ثانیه است.
- **Beacon Interval (فاصله زمانی راهنما)**: فاصله زمانی راهنما، زمان بین یک DTIM و DTIM بعدی است. مقدار پیش فرض 100 میلی ثانیه است. مقدار فاصله زمانی راهنما را برای ارتباط بی سیم ناپایدار یا دستگاه های رومینگ کم کنید.
- **Enable TX Bursting (فعال کردن بیرون ریزی TX)**: فعال کردن بیرون ریزی TX سرعت انتقال بین روتر بی سیم و دستگاه های 802.11g را بهبود می بخشد.
- **Enable WMM APSD (فعال کردن WMM APSD)**: فعال کردن WMM APSD (تحویل ذخیره نیروی خودکار چندرسانه ای Wi-Fi) برای بهبود مدیریت انرژی بین دستگاه های بی سیم است. برای خاموش کردن WMM APSD، **Disable (غیر فعال)** را انتخاب کنید.
- **کم کردن رابط USB 3.0:** اگر این عملکرد را فعال کنید، بهترین عملکرد بی سیم را در باند 2.4 گیگاهرتز خواهید داشت. اگر این ویژگی را غیرفعال کنید، سرعت انتقال پورت USB 3.0 بیشتر می شود و ممکن است روی محدوده بی سیم 2.4 گیگاهرتز تأثیر بگذارد.
- **Optimize AMPDU aggregation (بهینه سازی تجمع AMPDU):** حداکثر تعداد MPDUها را در یک AMPDU بهینه سازی کنید و از گم شدن بسته ها یا خراب شدن آنها در حین مخابره در کانال های بی سیم دارای خطا جلوگیری کنید.
- **Turbo QAM:** این عملکرد را فعال کنید تا از 256-QAM (MCS 8/9) در باند 2.4 گیگاهرتز پشتیبانی شود، در نتیجه محدوده بهتری خواهید داشت و ظرفیت پذیرش آن فرکانس بیشتر می شود.
- **Airtime Fairness:** با استفاده از Airtime Fairness، سرعت شبکه

توسط آهسته ترین ترافیک تعیین نمی شود. Airtime Fairness با تخصیص زمان برابر بین سرویس گیرندگان، این امکان را ایجاد می کند تا هر مخابره ای با بالاترین سرعت ممکن انجام شود.

- **Explicit Beamforming (بیم فرمینگ آشکار):** آداپتر و روتر WLAN سرویس گیرنده هر دو از فن آوری بیم فرمینگ پشتیبانی می کنند. این فن آوری به این دستگاه ها امکان می دهند محاسبات تخمینی و جهت هدایت را به یکدیگر منتقل کنند تا سرعت دانلود و آپلینگ بهبود پیدا کند.
- **Universal Beamforming (بیم فرمینگ جهانی):** برای آداپتورهای شبکه بی سیم قدیمی که از بیم فرمینگ پشتیبانی نمی کنند، روتر کانال را به صورت تخمینی محاسبه می کند و جهت هدایت را تعیین می کند تا سرعت داون لینک بهبود پیدا کند

4 برنامه های کاربردی

تذکرها:

- برنامه های کاربردی روتر بی سیم را از وب سایت ASUS نصب و دانلود کنید.
- Device Discovery (شناسایی دستگاه) نسخه 1.4.7.1 در http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip
- Firmware Restoration (بازیابی نرم افزار) نسخه 1.9.0.4 در http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip
- Windows Printer Utility (برنامه کاربردی چاپگر ویندوز) نسخه 1.0.5.5 در http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip
- این برنامه های کاربردی در MAC OS پشتیبانی نمی شود.

4.1 Device Discovery (شناسایی دستگاه)

شناسایی دستگاه یک برنامه کاربردی ASUS WLAN است که دستگاه روتر بی سیم ASUS را شناسایی می‌کند، و امکان پیکربندی تنظیمات شبکه بی سیم را فراهم می کند.

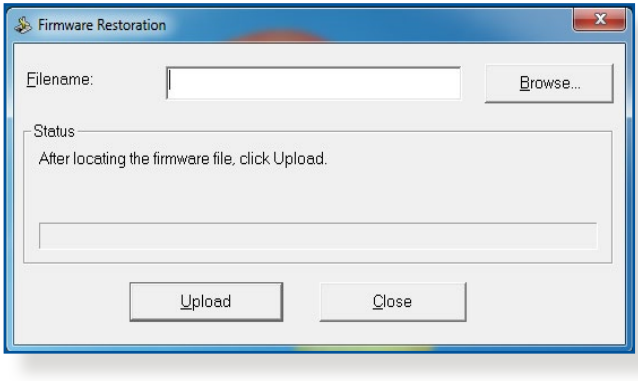
برای راه اندازی برنامه کاربردی شناسایی دستگاه:

- از دسکتاپ کامپیوتر خود، روی **Start (شروع) > All Programs (تمام برنامه‌ها) > ASUS Utility (برنامه کاربردی ASUS) > Device Discovery (روتر بی سیم) Wireless Router (شناسایی دستگاه)** کلیک کنید.

نکته: هنگامی که روتر را روی حالت نقطه دسترسی تنظیم می کنید، برای دریافت آدرس IP روتر باید از Device Discovery (شناسایی دستگاه) استفاده کنید.

4.2 بازیابی نرم افزار

زمانی بازیابی نرم افزار برای روتر بی سیم ASUS استفاده می شود که در طی فرآیند ارتقاء نرم افزار با مشکل مواجه شده باشد. بازیابی، نرم افزار ثابتی را که تعیین کرده اید آپلود می کند. این فرآیند سه تا چهار دقیقه طول می کشد.



مهم! قبل از استفاده از برنامه کاربردی بازیابی نرم افزار، حالت نجات را روی روتر راه اندازی کنید.

نکته: این ویژگی در MAC OS پشتیبانی نمی شود.

برای راه اندازی حالت نجات و استفاده از برنامه کاربردی بازیابی نرم افزار:

1. روتر بی سیم را از منبع برق جدا کنید.
2. دکمه بازنشانی را در پنل پشتی نگه دارید و به طور هم زمان روتر بی سیم را دوباره به منبع برق وصل کنید. هنگانی که LED برق در پنل جلویی به آرامی چشمک زد، دکمه بازنشانی را رها کنید، این حالت نشان می دهد که روتر بی سیم در حالت نجات است.

3. یک IP ثابت روی کامپیوتر خود تنظیم کنید و موارد زیر را برای راه اندازی تنظیمات TCP/IP استفاده کنید.

IP address (نشانی IP): 192.168.1.x

Subnet mask (ماسک شبکه فرعی): 255.255.255.0

4. از دسکتاپ کامپیوتر، روی **Start (شروع) > All Programs (تمام برنامه‌ها) > ASUS Utility GT6 Wireless Router (روتر بی سیم ASUS GT6) > Firmware Restoration (بازیابی نرم افزار)** کلیک کنید.

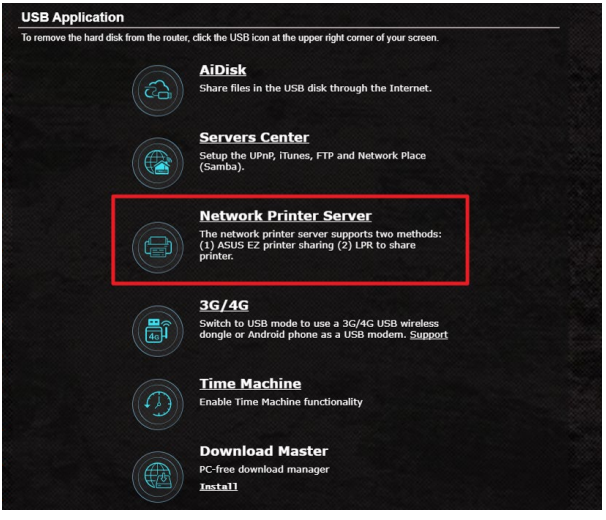
5. یک فایل نرم افزار ثابت را تعیین کنید، سپس روی **Upload (بارگذاری)** کلیک کنید.

نکته: این یک برنامه کمکی ارتقاء دهنده نرم افزار ثابت نیست و نمی توان از آن در روتر بی‌سیم ASUS در حال کار استفاده کرد. ارتقاء دهنده های معمولی نرم افزار باید از طریق رابط وب انجام شود. به **فصل 3** مراجعه کنید: برای اطلاعات بیشتر به **پیکربندی تنظیمات کلی و تنظیمات پیشرفته** مراجعه کنید.

4.3 راه اندازی سرور پرینتر

4.3.1 به اشتراک گذاری پرینتر ASUS EZ

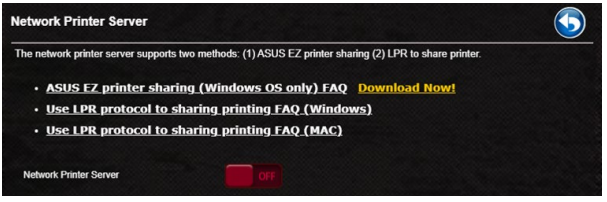
برنامه کاربردی ASUS EZ Printer Sharing (به اشتراک گذاری پرینتر ASUS EZ) به شما این امکان را می‌دهد که پرینتر USB را به پورت روتر بی سیم USB متصل کنید و سرور پرینت را راه اندازی کنید. این به سرویس گیرنده های شبکه شما امکان می‌دهد فایل ها را به طور بی سیم چاپ و اسکن کنند.



نکته: عملکرد سرور پرینت در Windows® 7/8/8.1/10 پشتیبانی می شود.

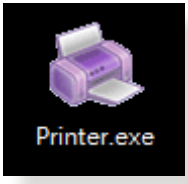
برای راه اندازی حالت اشتراک گذاری پرینتر EZ:

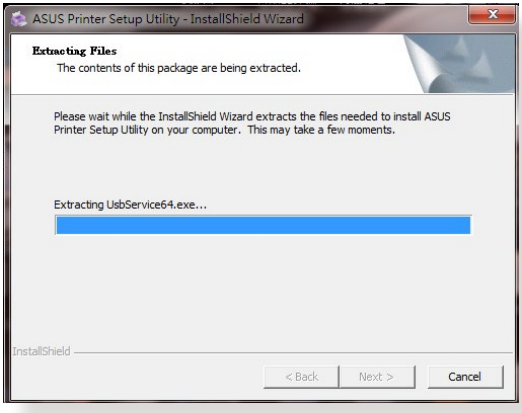
1. از پنل پیمایش، به **Advanced Settings (تنظیمات پیشرفته)** > **USB Application (برنامه کاربردی USB)** > **Network Printer Server (سرور پرینتر شبکه)** بروید.
2. برای دانلود برنامه کاربردی پرینتر شبکه، روی **Download Now! (اکنون دانلود کنید!)** کلیک کنید.



نکته: برنامه کاربردی پرینتر شبکه در Windows® 7/8/8.1/10 پشتیبانی می شود. برای نصب برنامه کاربردی روی Mac OS، **Use LPR protocol for sharing printer (استفاده از پروتکل LPR برای به اشتراک گذاری پرینتر)** را انتخاب کنید.

3. فایل دانلود شده را باز کنید و روی نماد پرینتر کلیک کنید تا برنامه راه اندازی پرینتر شبکه اجرا شود.



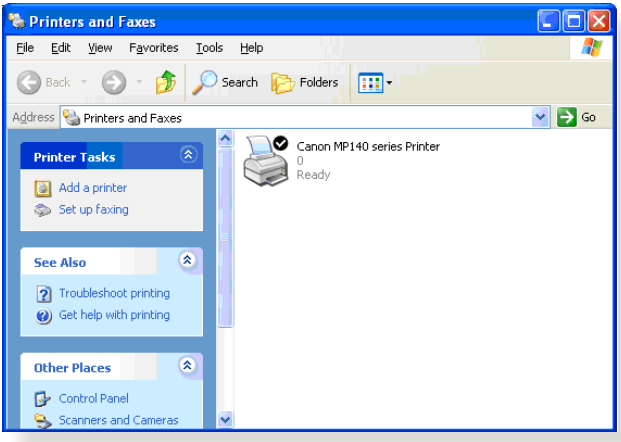


4. دستورالعمل های روی صفحه را دنبال کنید تا سخت افزار شما راه اندازی شود، سپس روی **Next (بعدی)** کلیک کنید.

5. برای اتمام نصب اولیه، چند لحظه صبر کنید. روی **Next (بعدی)** کلیک کنید.
6. برای اتمام نصب، روی **Finish (پایان)** کلیک کنید.

7. برای نصب درایور پرینتر، دستورالعمل های سیستم عامل Windows® را دنبال کنید.

8. بعد از اینکه نصب درایور پرینتر تمام شد، سرویس گیرندگان شبکه می توانند از پرینتر استفاده کنند.



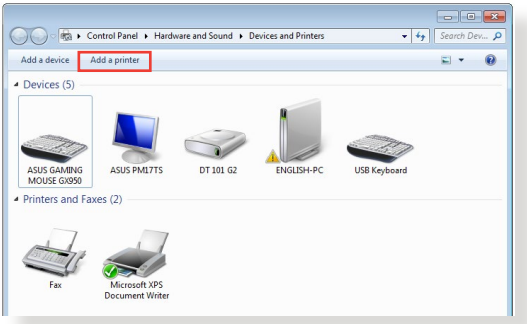
4.3.2 استفاده از LPR برای به اشتراک گذاری پرینتر

می‌توانید پرینتر خود را با کامپیوتر دارای سیستم عامل Windows® و MAC که از LPR/LPD (Line Printer Daemon/Line Printer Remote) استفاده می کنند، به اشتراک بگذارید.

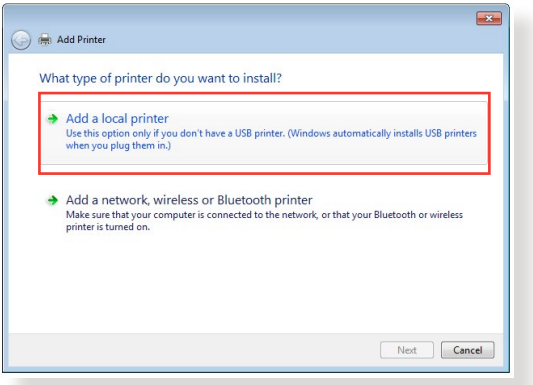
به اشتراک گذاری پرینتر LPR

برای اشتراک گذاری پرینتر LPR:

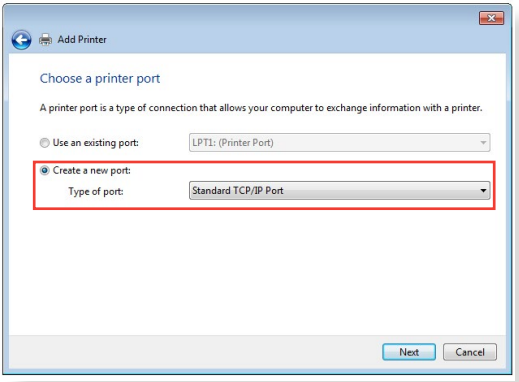
1. از دسکتاپ Windows®، روی **Start (شروع)** > **Devices and Printers (دستگاه‌ها و پرینترها)** > **Add a printer (افزودن پرینتر)** کلیک کنید تا **Add Printer Wizard (راهنمای افزودن پرینتر)** اجرا شود.



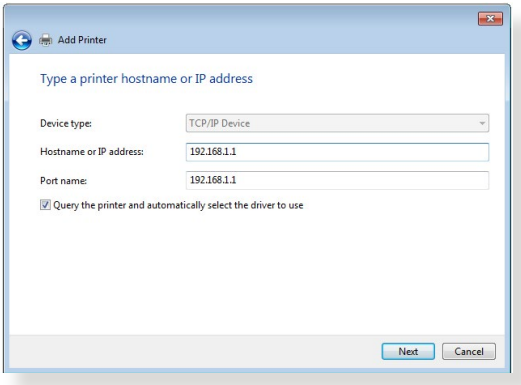
2. **Add a local printer (یک پرینتر محلی اضافه کنید)** انتخاب کنید و سپس روی **Next (بعدی)** کلیک کنید.



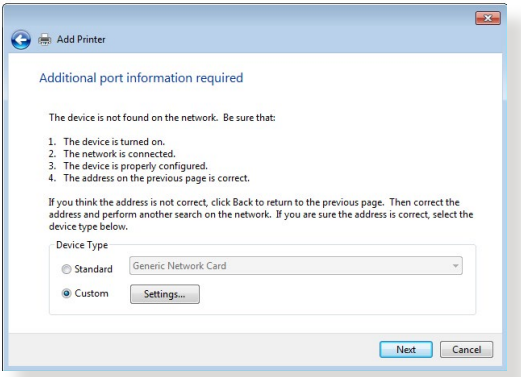
3. **Create a new port (ایجاد یک پورت جدید)** را انتخاب کنید سپس **Type of Port (نوع پورت)** را روی **StandardTCP/IP Port (پورت TCP/IP استاندارد)** تنظیم کنید. روی **Next (بعدی)** کلیک کنید.



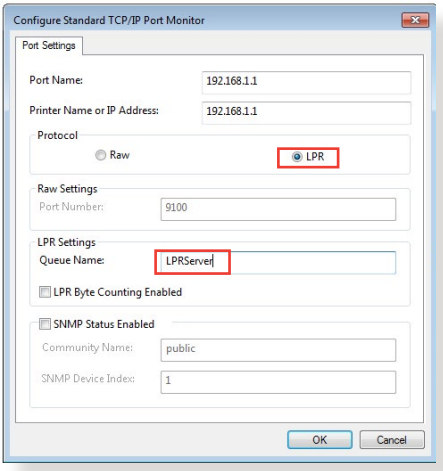
4. در قسمت **Hostname (نام سرور)** یا **IP address (آدرس IP)**، آدرس IP روتر بی سیم را وارد کنید سپس روی **Next (بعدی)** کلیک کنید.



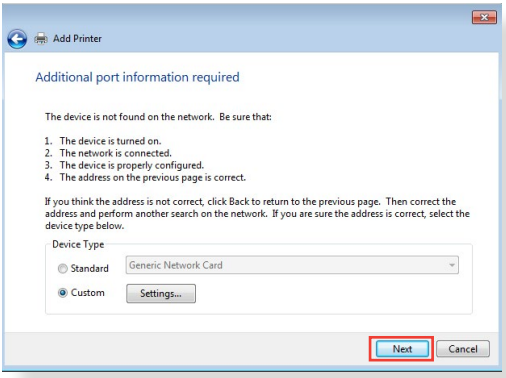
5. **Custom (سفارشی)** را انتخاب کنید سپس روی **Settings (تنظیمات)** کلیک کنید.



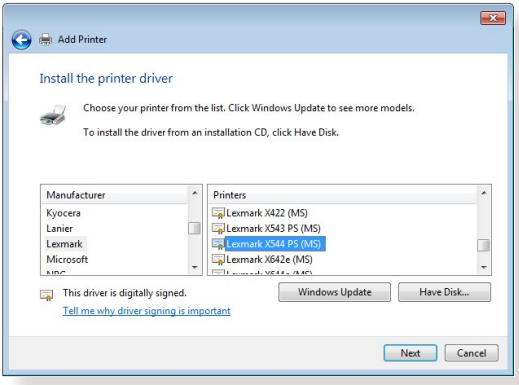
6. **Protocol (پروتکل)** را روی **LPR** تنظیم کنید. در قسمت **Queue Name (نام صف)**، **LPRServer (سرور LPR)** را وارد کنید سپس برای ادامه روی **OK (تأیید)** کلیک کنید.



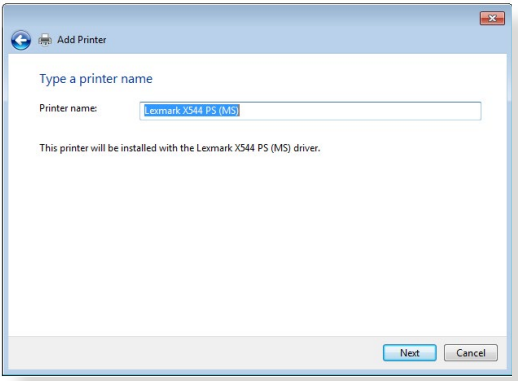
7. برای اتمام راه اندازی پورت استاندارد TCP/IP، روی **Next (بعدی)** کلیک کنید.



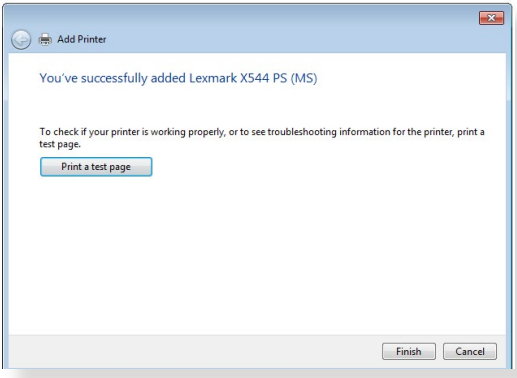
8. درایور پرینتر را از لیست مدل های فروشنده نصب کنید. اگر پرینتر شما در لیست نیست، روی **Have Disk (دارای دیسک)** کلیک کنید تا درایور پرینتر به طور دستی از CD-ROM یا فایل نصب شود.



9. برای پذیرفتن نام پیش فرض پرینتر، روی **Next (بعدی)** کلیک کنید.



10. برای اتمام نصب، روی **Finish (پایان)** کلیک کنید.



4.4 Download Master

Download Master یک برنامه کاربردی است که به شما کمک می‌کند فایل‌ها دانلود شوند حتی زمانی که لپتاپ ها یا سایر دستگاه ها خاموش هستند.

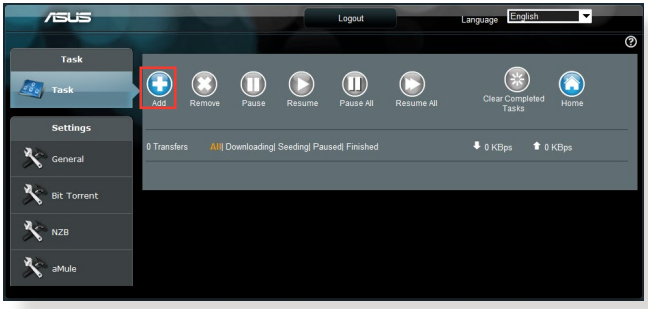
نکته: برای استفاده از Download Master باید دستگاه USB را به روتر بی سیم وصل کنید.

برای استفاده از Download Master:

1. روی **Advanced Settings (تنظیمات پیشرفته) > USB Application (برنامه کاربردی) > Download Master** کلیک کنید تا برنامه کاربردی به طور خودکار نصب و دانلود شود.

نکته: اگر بیش از یک درایو USB دارید، دستگاه USB که می خواهید فایل ها روی آن دانلود شود را انتخاب کنید.

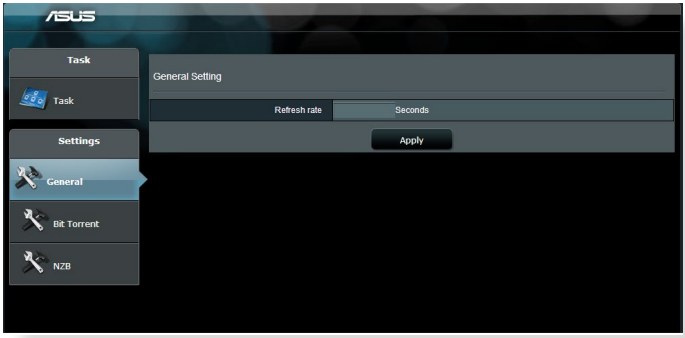
2. بعد از اینکه فرآیند دانلود به اتمام رسید، روی نماد Download Master کلیک کنید تا استفاده از برنامه کاربردی آغاز شود.
3. برای اضافه کردن یک کار دانلود روی **Add (اضافه کردن)** کلیک کنید.



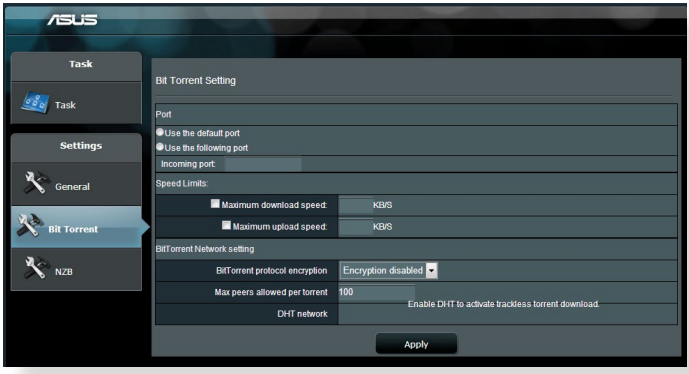
4. نوع دانلود مانند BitTorrent، HTTP یا FTP را انتخاب کنید. برای شروع دانلود، یک فایل torrent یا یک نشانی اینترنتی را معرفی کنید.

نکته: برای اطلاع از جزئیات Bit Torrent، به بخش **4.4.1 پیکربندی تنظیمات دانلود Bit Torrent** مراجعه کنید.

5. برای پیکربندی تنظیمات پیشرفته از پنل پیمایش استفاده کنید.



4.4.1 پیکربندی تنظیمات دانلود Bit Torrent

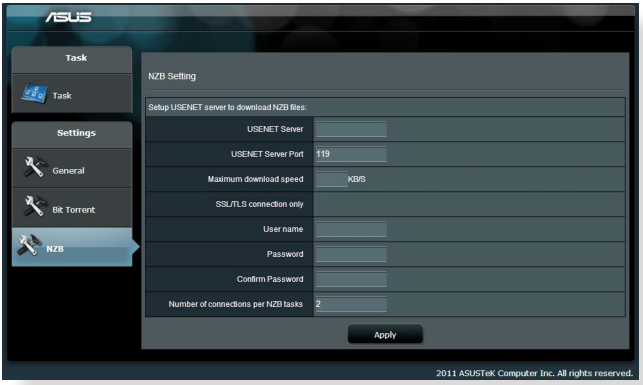


برای پیکربندی تنظیمات دانلود BitTorrent:

1. از پنل پیمایش دانلود اصلی، روی **Bit Torrent** کلیک کنید تا صفحه **Bit Torrent Setting (تنظیمات Bit Torrent)** راه اندازی شود.
2. برای کار دانلود خود یک پورت خاص انتخاب کنید.
3. برای جلوگیری از ازدحام شبکه، می‌توانید حداکثر سرعت بارگذاری و دانلود را در **Speed Limits (محدودیت سرعت)** محدود کنید.
4. می‌توانید حداکثر تعداد مجوزهای هم سطح را محدود کنید و رمزگذاری فایل در حین دانلود را فعال یا غیرفعال کنید.

4.4.2 تنظیمات NZB

برای دانلود فایل های NZB، می توانید سرور یوس نت را راه اندازی کنید. بعد از وارد کردن تنظیمات یوس نت، **Apply (به کارگیری)** کنید.



5 عیب یابی

این فصل راه حل هایی برای مشکلاتی که ممکن است برای روتر شما پیش بیاید، ارائه می دهد. اگر با مشکلاتی مواجه شدید که در این فصل به آنها اشاره نشده است، به سایت پشتیبانی ASUS بروید:https://www.asus.com/support برای اطلاع در مورد محصولات و اطلاعات تماس به پشتیبانی فنی ASUS مراجعه کنید.

5.1 عیب یابی اولیه

اگر با روتر مشکل دارید، پیش از انجام راه حل های بیشتر، مراحل ابتدایی زیر را امتحان کنید.

نرم افزار را به جدیدترین نسخه ارتقا دهید.

1. رابط گرافیکی تحت وب را راه اندازی کنید. به **Advanced Settings (تنظیمات پیشرفته)** > **Administration (مدیریت)** > زبانه **Firmware Upgrade (ارتقای نرم افزار ثابت)** بروید. روی **Check (بررسی)** کلیک کنید تا بررسی کند که آیا نسخه جدید نرم افزار موجود است یا خیر.
2. اگر نسخه جدید موجود بود، از وبسایت ASUS به نشانی https://rog.asus.com/networking/rog-rapture-GT6-model/helpdesk_download دیدن کنید تا جدیدترین نسخه را دانلود کنید.
3. در صفحه **Firmware Upgrade (ارتقای نرم افزار ثابت)**، روی **Browse (مرور)** کلیک کنید تا فایل نرم افزار ثابت را پیدا کنید.
4. روی **Upload (بارگذاری)** کلیک کنید تا نرم افزار ثابت را ارتقا دهید.

شبکه خود را به ترتیب زیر دوباره راه اندازی کنید:

1. مودم را خاموش کنید.
2. مودم را از برق بکشید.
3. روتر و رایانه ها را خاموش کنید.
4. مودم را به برق بزنید.
5. مودم را روشن کنید و 2 دقیقه منتظر بمانید.
6. روتر را روشن کنید و 2 دقیقه منتظر بمانید.
7. رایانه ها را روشن کنید.

بررسی کنید که آیا کابل های اترنت به طور صحیح وصل شده اند یا خیر.

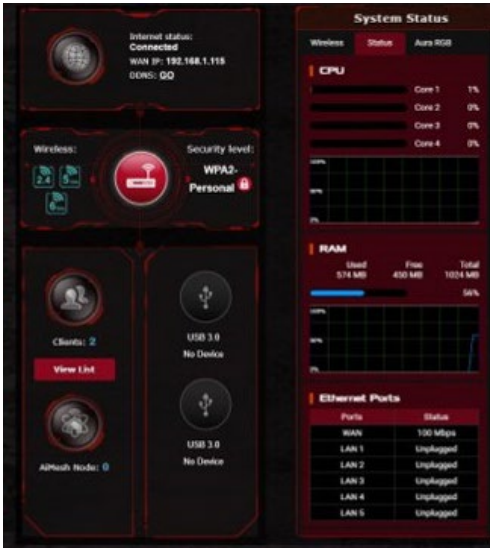
- اگر کابل اترنتی که روتر را به مودم متصل می کند، به طور صحیح وصل شده باشد، WAN LED روشن می شود.
- اگر کابل اترنتی که رایانه روشن را به روتر متصل می کند، به طور صحیح وصل شده باشد، LAN LED مربوط به آن روشن می شود.

بررسی کنید که آیا تنظیم بی سیم درراینه با روترشما مطابقت دارد یا خیر.

- هنگامی که رایانه را به صورت بی سیم به روتر وصل می کنید، مطمئن شوید که SSID (نام شبکه بی سیم)، روش رمزگذاری، و رمز عبور صحیح است.

بررسی کنید که آیا تنظیمات شبکه صحیح است یا خیر.

- هر سرویس گیرنده در شبکه باید نشانی IP معتبری داشته باشد. ASUS توصیه می کند که از سرور DHCP روتر بی سیم برای اختصاص نشانی های IP به رایانه های موجود در شبکه استفاده کنید.
- بعضی ارائه دهندگان خدمات مودم کابلی هنگام ثبت حساب کاربری از شما می خواهند که از نشانی MAC رایانه استفاده کنید. نشانی MAC را می توانید در رابط گرافیکی تحت وب، **Network Map (نقشه شبکه)** > صفحه **Clients (سرویس گیرندگان)** ببینید و نشانگر ماوس را روی دستگاه خود در **Client Status (وضعیت سرویس گیرنده)** قرار دهید.

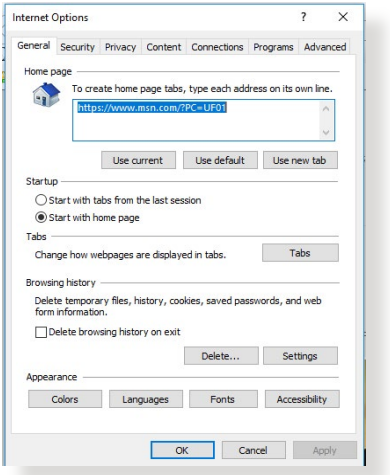


5.2 سؤالات رایج

نمی توانم با استفاده از مرورگر وب به رابط گرافیکی روتر دسترسی پیدا کنم.

- اگر رایانه با کابل وصل شده است، اتصال کابل اترنت و وضعیت LED را همانطور که در بخش قبل توضیح دادیم بررسی کنید.
- مطمئن شوید که از اطلاعات ورود صحیح استفاده کرده اید. نام و رمز عبور ورود به صورت پیش فرض admin/admin است. مطمئن شوید که کلید Caps Lock هنگام وارد کردن اطلاعات ورود غیر فعال است.
- کوکی ها و فایل های مرورگر وب را حذف کنید. برای مرورگر اینترنت اکسپلورر، این مراحل را دنبال کنید:

1. مرورگر اینترنت اکسپلورر را راه‌اندازی کنید، سپس روی **Tools (ابزارها)** > **Internet Options (تنظیمات اینترنت)** کلیک کنید.
2. در زبانه **General (موارد کلی)**، زیر **Browsing history (تاریخچه مرورگر)**، روی **Delete... (حذف...)** کلیک کنید و **Temporary Internet Files (فایل های اینترنتی موقت)** و **Cookies (کوکی ها)** را انتخاب کنید و سپس روی **Delete (حذف)** کلیک کنید.



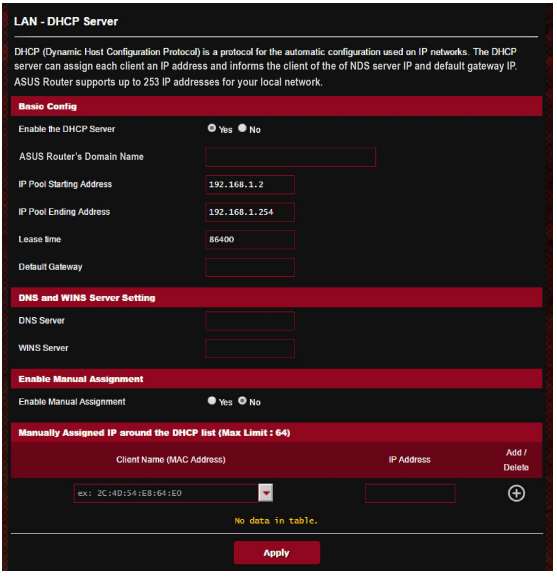
تذکرها:

- فرمان های حذف کوکی ها و فایل ها بسته به مرورگرهای وب متفاوت است.
- تنظیمات سرور پراکسی را غیر فعال کنید، اتصال دایل آپ را لغو کنید و برای دسترسی به نشانی های IP به صورت خودکار، تنظیمات TCP/IP را تنظیم کنید. برای آگاهی از جزئیات بیشتر، به فصل 1 این دفترچه راهنمای کاربر مراجعه کنید.
- مطمئن شوید که از کابل های اترنت CAT5e یا CAT6 استفاده می کنید.

سرویس گیرنده نمی تواند با روتر اتصال بی سیم برقرار کند.

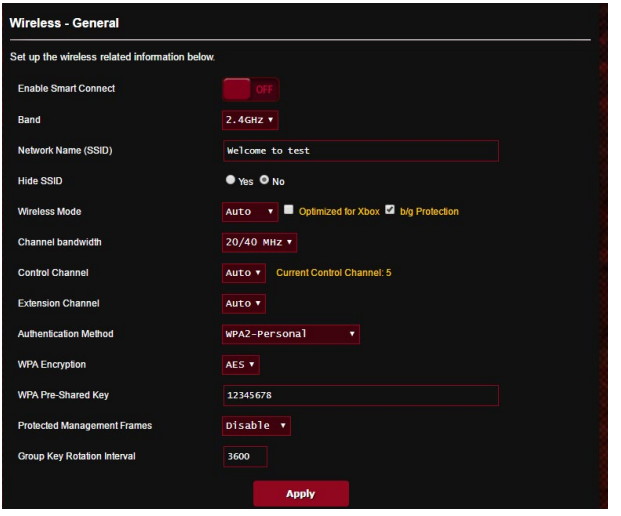
نکته: اگر برای اتصال به شبکه 5 گیگاهرتزی مشکل دارید، مطمئن شوید که دستگاه بی سیم شما از شبکه 5 گیگاهرتزی پشتیبانی می کند یا قابلیت های باند دوتایی را دارد.

- **خارج از محدوده:**
  - روتر را به سرویس گیرنده بی سیم نزدیکتر کنید.
- **سرور DHCP غیر فعال شده است:**
  1. رابط گرافیکی تحت وب را راه اندازی کنید. به **General (موارد کلی) > Network Map (نقشه شبکه)> Clients (سرویس گیرندگان)** بروید و دستگاهی را که می خواهید به روتر وصل شود جستجو کنید.
  2. اگر نمی توانید دستگاه را در **Network Map (نقشه شبکه)** بیابید، به **Advanced Settings (تنظیمات پیشرفته) > LAN >(سرور DHCP) DHCP Server** فهرست **Basic Config (پیکربندی اولیه)** بروید، و **Yes (بله)** را در **Enable the DHCP Server (فعال کردن سرور DHCP)** انتخاب کنید.
- SSID پنهان شده است. اگر دستگاه شما بتواند SSID سایر روتر ها را پیدا کند، ولی نتواند SSID روتر خودتان را پیدا کند، به **Advanced**



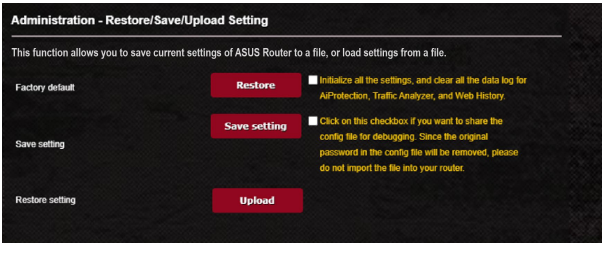
Settings (تنظیمات پیشرفته) > Wireless (بی‌سیم) > General (موارد کلی) بروید، در **Hide SSID (پنهان کردن SSID) No (خیر)** را انتخاب کنید و در **Control Channel (کنترل کانال) Auto (خودکار)** را انتخاب کنید.

- اگر از آداپتور LAN بی سیم استفاده می کنید، بررسی کنید که آیا کانال بی سیم مورد استفاده با کانال های موجود در کشور یا منطقه شما مطابقت دارد یا خیر.



اگر مطابقت ندارد، کانال، پهنای باند کانال و حالت بی سیم را تنظیم کنید.

- اگر هنوز هم نمی توانید به طور بی سیم به روتر وصل شوید، می توانید روتر را به تنظیمات پیش فرض کارخانه بازنشانی کنید. در رابط گرافیکی تحت وب روتر، روی **Administration (مدیریت) > Restore/ Save/Upload Setting (تنظیم بازگردانی/ذخیره/بارگذاری)** کلیک کنید و روی **Restore (بازگردانی)** کلیک کنید.



اینترنت قابل دسترسی نیست.

- بررسی کنید که آیا روتر می تواند به نشانی IP مربوط به ISP WAN متصل شود. برای بررسی آن، رابط گرافیکی تحت وب را راه اندازی کنید و به **Advanced Settings (تنظیمات پیشرفته) > Network Map (نقشه شبکه)** بروید و **Internet status (وضعیت اینترنت)** را بررسی کنید.
- اگر روتر نمی‌تواند به نشانی IP مربوط به ISP WAN متصل شود، شبکه را همانطور که در بخش شبکه خود را به ترتیب زیر دوباره راه اندازی کنید زیر عیب یابی اولیه توضیح داده شده است مجدداً راه اندازی کنید.

- دستگاه از طریق عملکرد کنترل والدین مسدود شده است. به قسمت **General (موارد کلی) > AiProtection > Parental Controls (کنترل والدین)** بروید و ببینید که آیا دستگاه در لیست وجود دارد یا خیر. اگر نام دستگاه زیر **Client Name (نام سرویس گیرنده)** فهرست شده باشد، دستگاه را با استفاده از دکمه **Delete (حذف)** یا تغییر تنظیمات مدیریت زمان حذف کنید.
- اگر هنوز به اینترنت دسترسی ندارید، رایانه را دوباره راه اندازی کنید و نشانی IP شبکه و نشانی دروازه را تأیید کنید.
- نشانگرهای وضعیت روی مودم ADSL و روتر بی سیم را بررسی کنید. اگر WAN LED روی روتر بی سیم روشن نباشد، بررسی کنید که همه کابل‌ها درست وصل شده باشد.

SSID (نام شبکه) یا رمز عبور شبکه را فراموش کرده‌اید.

- از طریق یک اتصال با سیم، یک SSID و کلید رمزگذاری جدید تنظیم کنید (کابل اترنت). رابط گرافیکی تحت وب را راه اندازی کنید، به **Network Map (نقشه شبکه)** بروید، روی نماد روتر کلیک کنید، SSID و کلید رمزگذاری جدید را وارد کنید و سپس روی **Apply (به کارگیری)** کلیک کنید.
- روتر را به تنظیمات پیش فرض بازنشانی کنید. رابط گرافیکی تحت وب را راه اندازی کنید، به **Administration (مدیریت) > Restore/ Save/Upload Setting (تنظیم بازگردانی/ذخیره/بارگذاری)** بروید و روی **Restore (بازگردانی)** کلیک کنید. حساب کاربری ورود پیش فرض و رمز عبور هر دو "admin" است.

چگونه سیستم را به تنظیمات پیش فرض بازگردانیم؟

- به **Administration (مدیریت) > Restore/Save/Upload Setting (تنظیم بازگردانی/ذخیره/بارگذاری)** بروید و روی **Restore (بازگردانی)** کلیک کنید.

تنظیمات پیش فرض کارخانه به صورت زیر است:

User Name (نام کاربری):	admin
Password (رمز عبور):	admin
Enable DHCP (DHCP فعال):	YES (اگر کابل WAN متصل باشد)
IP address (IP نشانی):	http://www.asusrouter.com (یا 192.168.50.1)
Domain Name (نام دامنه):	(خالی)
Subnet Mask (ماسک شبکه فرعی):	255.255.255.0
DNS Server 1 (سرور DNS 1):	192.168.50.1
DNS Server 2 (سرور DNS 2):	(خالی)
SSID (2.4گیگاهرتز):	ASUS_XX_2G
SSID (5گیگاهرتز-1):	ASUS_XX_5GHz-1
SSID (5گیگاهرتز-2):	ASUS_XX_5GHz-2

ارتقاء نرم افزار ثابت انجام نشد.

حالت نجات را راه اندازی کنید و برنامه کاربردی بازیابی نرم افزار ثابت را اجرا کنید. برای اطلاع از نحوه استفاده از برنامه کاربردی بازیابی نرم افزار ثابت، به بخش **4.2 بازیابی نرم افزار** بروید.

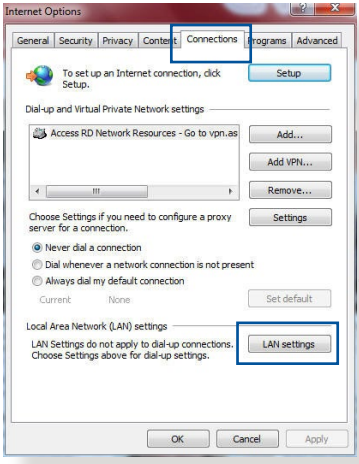
امکان دستیابی به رابط گرافیکی کاربر تحت وب وجود ندارد

پیش از پیکربندی روتر بی سیم، مراحلی که در این بخش توضیح داده شده است را برای رایانه میزبان و سرویس گیرنده های شبکه انجام دهید.

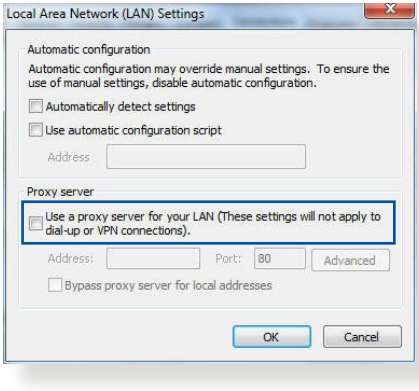
الف. اگر سرور پراکسی فعال است، آن را غیر فعال کنید.

Windows®

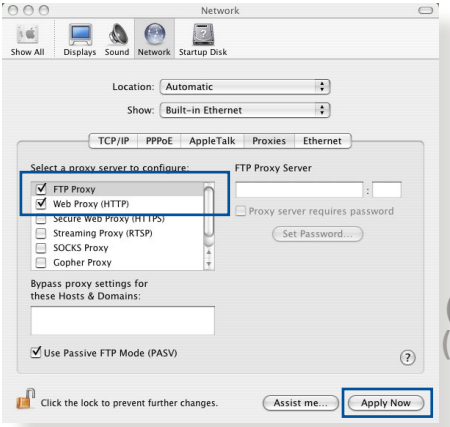
1. روی **Start (شروع)** < **Internet Explorer (اینترنت اکسپلورر)** کلیک کنید تا مرورگر راه اندازی شود.
2. روی **Tools (ابزارها)** < **Internet options (تنظیمات اینترنت)** < زبانه **Connections (اتصال ها)** < **LAN settings (تنظیمات LAN)** کلیک کنید.



3. در صفحه تنظیمات شبکه محلی (LAN)، علامت **Use a proxy server for your LAN (استفاده از سرور پراکسی برای LAN)** را بردارید.
4. زمانی که همه مراحل به پایان رسید، روی **OK (تأیید)** کلیک کنید.



MAC OS



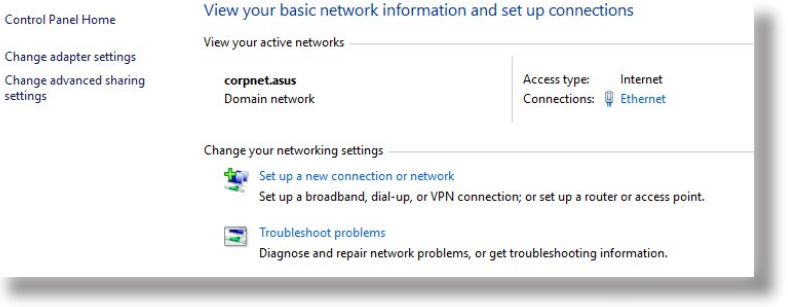
1. در مرورگر Safari، روی **Preferences < Safari** (تنظیمات پیشرفته) **< Advanced < Change Settings... (تغییر تنظیمات...)** کلیک کنید.
2. در صفحه Network، علامت **FTP Proxy (پراکسی FTP)** و **Web Proxy (پراکسی وب) (HTTP)** را بردارید.
3. زمانی که همه مراحل به پایان رسید، روی **Apply Now (اکنون اعمال شود)** کلیک کنید.

نکته: برای آگاهی از جزئیات درباره غیر فعال کردن سرور پراکسی به قسمت کمک مرورگر مراجعه کنید.

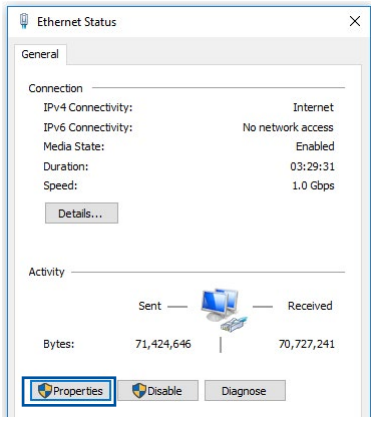
ب. تنظیمات TCP/IP را تغییر دهید تا به صورت خودکار یک آدرس IP به دست آورد.

Windows®

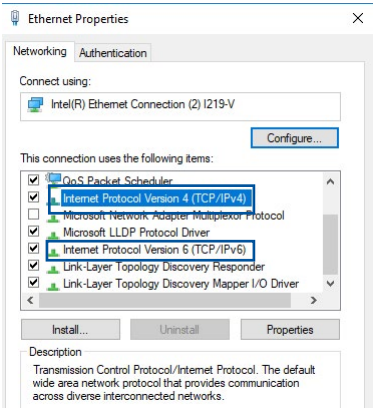
1. روی **Start (شروع) < Control Panel (پنل کنترل) < Network and Sharing Center (شبکه و قسمت اشتراک)** سپس اتصال شبکه را برای نمایش پنجره وضعیت کلیک کنید، **(گذاری**.



2. روی **Properties (ویژگی ها)** کلیک کنید تا پنجره مشخصات اترنت نمایش داده شود.



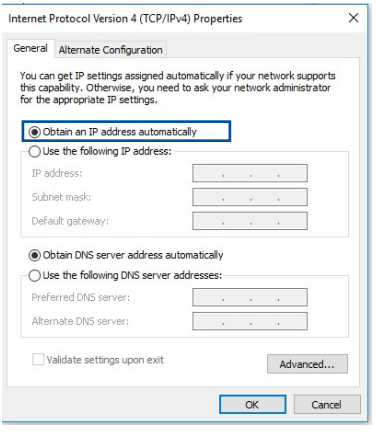
3. **Internet Protocol Version 4 (TCP/IPv4) (پروتکل اینترنتی نسخه 4)** یا **Internet Protocol Version 6 (TCP/IPv6) (پروتکل اینترنتی نسخه 6)** را انتخاب نمایید و سپس روی **Properties (ویژگی ها)** کلیک کنید.



4. برای دستیابی به تنظیمات IP IPv4 به صورت خودکار، **Obtain an IP address automatically (دستیابی به نشانی IP به صورت خودکار)** را علامت بزنید.

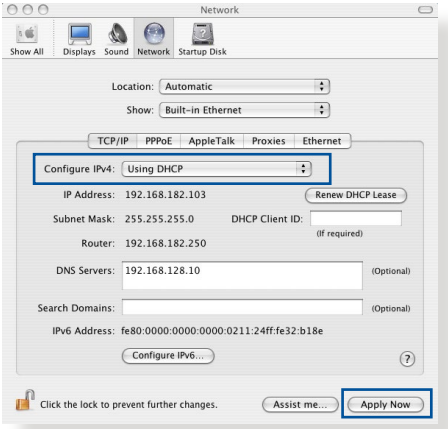
   برای دستیابی به تنظیمات IP IPv6 به صورت خودکار، **Obtain an IPv6 address automatically (دستیابی به نشانی IPv6 به صورت خودکار)** را علامت بزنید.

5. زمانی که همه مراحل به پایان رسید، روی **OK (تأیید)** کلیک کنید.



MAC OS

1. روی نماد Apple در قسمت بالای سمت چپ صفحه کلیک کنید.



2. روی **System Preferences (ترجیحات سیستم)** > **Network (شبکه)** > **Configure (پیکربندی)...** کلیک کنید

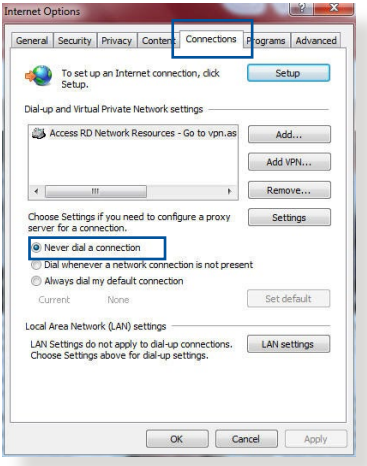
3. در زبانه **TCP/IP**، **Using DHCP (استفاده از DHCP)** را در لیست کشویی **Configure IPv4 (ترکیب بندی IPv4)** انتخاب کنید.

4. زمانی که همه مراحل به پایان رسید، روی **Apply Now (اکنون اعمال شود)** کلیک کنید.

نکته: برای اطلاع از جزئیات پیکربندی تنظیمات TCP/IP رایانه، به قسمت پشتیبانی و راهنمای سیستم عامل مراجعه کنید.

C. اگر گزینه اتصال دایل آپ فعال است، آن را غیر فعال کنید.

Windows®



1. روی **Start (شروع)** > **Internet Explorer (اینترنت اکسپلورر)** کلیک کنید تا مرورگر راه‌اندازی شود.

2. روی **Tools (ابزارها)** > **Internet options (تنظیمات اینترنت)** > **Connections (اتصال ها)** کلیک کنید.

3. **Never dial a connection (هرگز یک اتصال را شماره گیری نکن)** را علامت بزنید.

4. زمانی که همه مراحل به پایان رسید، روی **OK (تأیید)** کلیک کنید.

نکته: برای آگاهی از جزئیات درباره غیر فعال کردن اتصال دایل آپ به قسمت راهنمای مرورگر خود مراجعه کنید.

پیوست ها

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

اعلامیه های ایمنی

هنگام استفاده از این دستگاه همیشه احتیاط های ایمنی را در نظر داشته باشید، ازجمله و نه محدود به این موارد:

هشدار!

- سیم برق باید به پریزی که دارای اتصال مناسب به زمین باشد وصل شود. دستگاه را فقط به پریزی در نزدیک خودتان وصل کنید که به راحتی قابل دسترسی باشد.
- اگر آداپتور شکسته است، خودتان آن را تعمیر نکنید. با تکنیسین مجرب خدمات یا فروشنده خود تماس بگیرید.
- از سیم برق، وسیله های جانبی، یا سایر وسیله های خراب استفاده نکنید.
- این دستگاه را در ارتفاع بیشتر از 2 متر نصب نکنید.
- از این دستگاه در محیط هایی که دمای بین 0 درجه سانتی گراد (32 درجه فارنهایت) و 40 درجه سانتی گراد (104 درجه فارنهایت) دارند استفاده کنید.
- قبل از استفاده از این دستگاه، دستورالعمل های اجرایی را مطالعه کنید و محدوده دما را بررسی کنید.
- هنگام استفاده از این دستگاه در فرودگاه، بیمارستان، پمپ بنزین، و گاراژهای حرفه ای به موارد ایمنی شخصی کاملاً توجه کنید.
- رابط دستگاه پزشکی: حداقل 15 سانتی متر (6 اینچ) بین دستگاه های پزشکی ایمپلنت شده و محصولات ASUS فاصله در نظر بگیرید تا احتمال بروز تداخل کم شود.
- از محصولات ASUS در شرایطی استفاده کنید که دریافت سیگنال به خوبی انجام شود تا سطوح پخش اشعه به حداقل برسد.
- دستگاه را از زنان باردار و قسمت پایین شکم نوجوانان دور نگهدارید.
- اگر نقص قابل مشاهده در دستگاه وجود دارد یا اگر دستگاه آسیب دیده یا تغییری در آن ایجاد شده است از آن استفاده نکنید. برای کمک با متخصص تماس بگیرید.

هشدار!

- دستگاه را روی سطح ناصاف و بدون ثبات نگذارید.
- هیچ وسیله ای را بالای این دستگاه نگذارید یا روی آن نیندازید. دستگاه را در معرض شوک مکانیکی مانند خرد شدن، خمیدگی، سوراخ شدن یا خرد شدن قرار ندهید.
- قطعات دستگاه را از هم باز نکنید، جدا نکنید، در میکروفر نگذارید، نسوزانید، رنگ نکنید، یا هیچ وسیله خارجی را با فشار در این دستگاه وارد نکنید.
- به برچسب درجه بندی در پایین دستگاه مراجعه کنید و اطمینان حاصل کنید که آداپتور با این درجه بندی مطابقت داشته باشد.
- دستگاه را از آتش و منابع گرما دور نگهدارید.
- دستگاه را در معرض مایعات، باران، یا رطوبت قرار ندهید و در نزدیکی این شرایط از آن استفاده نکنید. از دستگاه در شرایط بروز طوفان الکتریکی استفاده نکنید.
- مدارهای خروجی PoE این محصول را فقط به شبکه های PoE محصول وصل کنید و به وسیله های خارجی اتصال برقرار نکنید.
- برای جلوگیری از ایجاد برق گرفتگی، سیم برق را قبل از جابجایی سیستم از پریز جدا کنید.
- فقط از وسیله های جانبی استفاده کنید که توسط سازنده دستگاه برای استفاده با این مدل تأیید شده اند. استفاده از انواع دیگر وسیله جانبی ممکن است باعث نقض ضمانت نامه یا قوانین و مقررات محلی شود و خطرهای ایمنی به همراه داشته باشد. برای اطلاع از وجود وسیله های جانبی مجاز با فروشنده محلی تان تماس بگیرید.
- استفاده از این دستگاه به هر شیوه ای بجز موارد توصیه شده در دستورالعمل های ارائه شده ممکن است باعث آتش سوزی یا جراحت شخصی شود.

سرویس و پشتیبانی

وبسایت چندزبانه ما را در این آدرس مشاهده کنید:
https://www.asus.com/support.