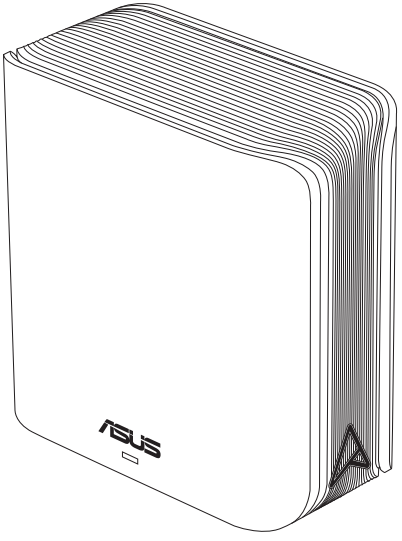
دليل المستخدم

ZenWiFi BD4

جهاز التوجيه BE3600 ثنائي النطاق



IN SEARCH OF INCREDIBLE

ARB23951
الإصدار الأول
أغسطس 2024

جدول المحتويات

جدول المحتويات

جدول المحتويات

١ التعرف على جهاز التوجيه اللاسلكي

1.1 مرحبًا!

نشكرك على شراء جهاز التوجيه ZenWiFi BD4 اللاسلكي من ASUS!

يتميز جهاز ZenWiFi BD4 ثنائي النطاق 2.4 جيجا هرتز و5 جيجا هرتز لبث لاسلكي متزامن عالي الدقة لا مثيل له؛ مع لمسة معدنية بلون حرف A على هيكل أبيض بسيط؛ إلى جانب خادم SMB وخادم UPnP AV وخادمFTP لمشاركة الملفات على مدار الساعة؛ وإمكانية معالجة 300000 جلسة عمل؛ وتقنية الشبكات الخضراء من ASUS، والتي تحقق توفيرًا في الطاقة يصل إلى 70%.

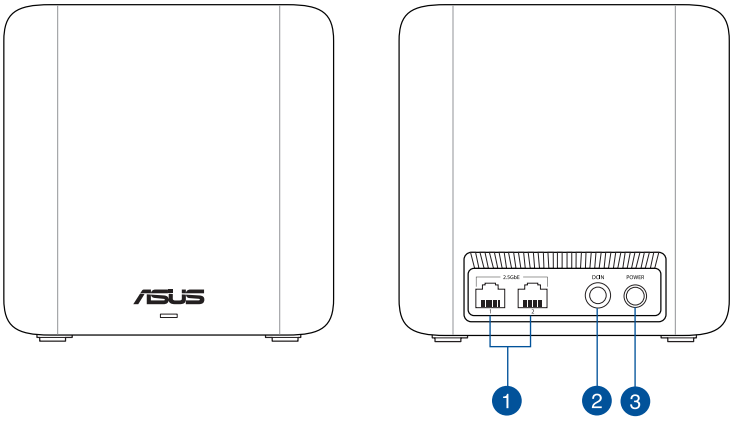
1.2 محتويات العبوة

☑ جهاز توجيه ZenWiFi BD4 لاسلكي
☑ كابل الشبكة (RJ-45)
☑ مهايئ الطاقة
☑ دليل التشغيل السريع
☑ بطاقة الضمان

ملاحظات:

- في حالة تلف أي من العناصر أو فقدانها، اتصل بشركة ASUS بخصوص أي استفسارات تقنية والدعم. راجع **الخدمة والدعم** في مؤخرة دليل المستخدم هذا.
- احتفظ بمواد التغليف الأصلية في حال احتجت إلى أي خدمات ضمان مستقبلية مثل الإصلاح أو الاستبدال.

1.3 جهاز التوجيه اللاسلكي الخاص بك



1	**منافذ 2.5GbE (الكشف التلقائي عن WAN/LAN)** قم بتوصيل كابلات الشبكة بهذه المنافذ لإنشاء اتصال 2.5GbE WAN/LAN.
2	**منفذ الطاقة (منفذ تيار متردد)** أدخل مهايئ التيار المتردد المرفق في هذا المنفذ لتوصيل جهاز التوجيه الخاص بك بمصدر للطاقة.
3	**زر الطاقة** اضغط على هذا الزر لتشغيل طاقة النظام أو إيقاف تشغيله.

ملاحظات:

- لا تستخدم سوى المهايئ المرفق بالعبوة. قد يؤدي استخدام مهايئات أخرى إلى تلف الجهاز.
- **المواصفات:**

مهايئ طاقة التيار المتردد	خرج التيار المتردد: 12+ فولت مع تيار 1.5 أمبير		
درجة حرارة التشغيل	0~40°C	التخزين	0~70°C
نسبة الرطوبة المسموح بها أثناء التشغيل	50%~90%	التخزين	20%~90%

1.4 ضبط موضع جهاز التوجيه اللاسلكي

لتحقيق الإرسال اللاسلكي الأمثل بين جهاز التوجيه اللاسلكي والأجهزة اللاسلكية المتصلة، تأكد من:

- ضع جهاز التوجيه اللاسلكي في منطقة مركزية لتحقيق أقصى تغطية لاسلكية لأجهزة الشبكة.
- أبق جهاز التوجيه اللاسلكي خاليًا من العوائق المعدنية وبعيدًا عن ضوء الشمس المباشر.
- أبق جهاز التوجيه اللاسلكي بعيدًا عن أجهزة Wi-Fi بترددات 802.11g أو 20 ميجاهرتز فقط، والأجهزة الطرفية للكمبيوتر بتردد2.4 جيجاهرتز، وأجهزة Bluetooth، والهواتف اللاسلكية والمحولات، ومواتير المهام الشاقة ومصابيح الفلوريسنت وأفران الميكروويف، والثلاجات والأجهزة الصناعية الأخرى لمنع تداخل الإشارة أو فقدانها.
- احرص دائمًا على تحديث البرنامج الثابت. زر موقع ويب ASUS على العنوان **http://www.asus.com** للحصول على آخر تحديثات البرنامج الثابت.

1.5 متطلبات الإعداد

لإعداد شبكة لاسلكية، يلزم استعمال جهاز كمبيوتر يلبي متطلبات النظام التالية:

- منفذ إيثرنت RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- إمكانية الاتصال اللاسلكي حسب معيار IEEE 802.11a/b/g/n/ac/ax
- جهاز TCP/IP مثبت
- مستعرض ويب مثل Internet Explorer أو Firefox, Safari أو Google Chrome

---

ملاحظات:

- إذا كان الكمبيوتر الخاص بك لا يتضمن إمكانات لاسلكية مضمنة، فيمكنك تثبيت محول WLAN IEEE 802.11a/b/g/n/ac/ax في الكمبيوتر للاتصال بالشبكة.
- بفضل تقنية ثنائي النطاق، يدعم جهاز التوجيه اللاسلكي إشارات لاسلكية 2.4 جيجاهرتز و 5 جيجاهرتز في وقت واحد. هذا يسمح لك بالقيام بأنشطة متعلقة بالإنترنت مثل تصفح الإنترنت أو قراءة/كتابة رسائل البريد الإلكتروني باستخدام النطاق 2.4 جيجاهرتز في حين الاستمتاع في نفس الوقت ببث ملفات صوت/فيديو بجودة عالية مثل الأفلام أو الموسيقى باستخدام نطاق 5 جيجاهرتز.
- قد تدعم بعض أجهزة IEEE 802.11n التي تريد توصيلها بالشبكة الخاصة بك أو قد لا تدعم نطاق 5 جيجاهرتز. ارجع إلى الدليل الكامل للتعرف على المواصفات.
- يجب ألا يتجاوز طول كابل إيثرنت RJ-45 الذي يُستخدم لتوصيل أجهزة الشبكة 100 متر.

هام!

- توجد مشكلات اتصال في بعض المهايئات اللاسلكية لنقاط وصول WiFi بمعيار 802.11ax.
- إذا كنت تعاني من هذه المشكلة، فرجاء التأكد من تحديث برنامج التشغيل إلى أحدث إصدار. افحص موقع الدعم الرسمي لجهة التصنيع حيث يمكن الحصول على برامج تشغيل البرامج والتحديثات والمعلومات ذات الصلة الأخرى.
  - Realtek: https://www.realtek.com/en/downloads
  - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi
  - Intel: https://downloadcenter.intel.com/

---

2 البدء

2.1. إعداد جهاز التوجيه

هام!

- استخدم الاتصال السلكي عند إعداد جهاز التوجيه اللاسلكي لتفادي المشكلات المحتملة في الإعداد.
- قبل إعداد جهاز التوجيه اللاسلكي من ASUS، اتبع ما يلي:
- إذا كنت تستخدم جهاز توجيه موجود، فافصله عن الشبكة الخاصة بك.
- افصل الكابلات/الأسلاك من إعداد المودم الموجود. إذا كان المودم يتضمن بطارية احتياطية، فأزلها أيضًا.
- أعد تمهيد مودم الكابل والكمبيوتر الخاص بك (موصى به).

تحذير!

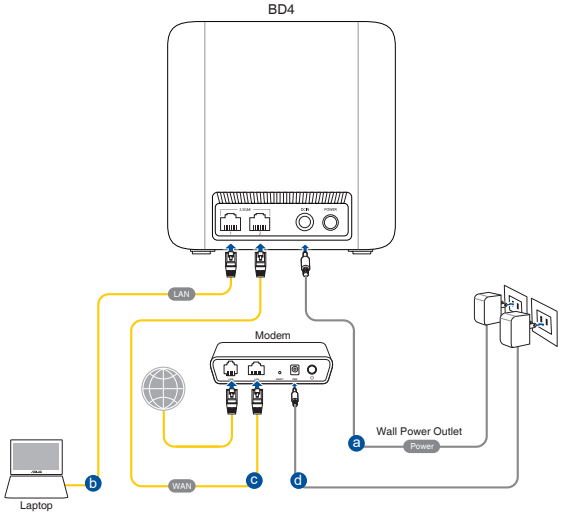
- يجب توصيل سلك (أسلاك) مصدر الإمداد بالطاقة بمأخذ (مآخذ) المقبس المزود بأرضية مناسبة. وصل الجهاز لمقبس كهربي قرب فقط يسهل الوصول إليه.
- في حالة إنكسار المهايئ, لا تحاول إصلاحه بنفسك. اتصل بفني صيانة مؤهل أو ببائع التجزئة لديك.
- يجب عدم استخدام أسلاك الطاقة أو الملحقات أو الوحدات الطرفية الأخرى التالفة.
- لا تركب هذا الجهاز على مسافة أعلى من 2 متر.
- استخدم هذا المنتج في البيئات التي تتراوح درجات الحرارة المنتشرة بها بين 0 درجة مئوية (32 فهرنهايت) و40 درجة مئوية (104 فهرنهايت).

A. الاتصال السلكي

ملاحظة: يمكنك استخدام إما كابل مستقيم أو ملفوف للاتصال السلكي.

لإعداد جهاز التوجيه اللاسلكي الخاص بك باستخدام اتصال سلكي:

1. قم بتوصيل جهاز التوجيه في مخرج الطاقة وشغل الطاقة. قم بتوصيل كبل الشبكة من جهاز الكمبيوتر الخاص بك بمنفذ 2.5GbE على جهاز التوجيه الخاص بك.



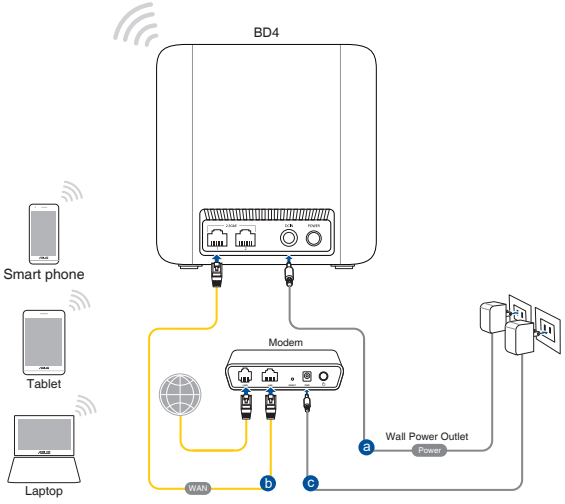
2. يتم تشغيل واجهة المستخدم العمومية على الويب (web GUI) تلقائيًا عندما تفتح مستعرض الويب. إذا لم يتم التشغيل تلقائيًا، فأدخل http://www.asusrouter.com.

3. قم بإعداد كلمة المرور بجهاز التوجيه لمنع الدخول غير المصرح به.

B. الاتصال اللاسلكي

لإعداد جهاز التوجيه اللاسلكي الخاص بك باستخدام اتصال لاسلكي:

1. قم بتوصيل جهاز التوجيه في مخرج الطاقة وشغل الطاقة.



2. اتصل باسم الشبكة (معرف SSID) الموضح على ملصق المنتج في الجانب الخلفي لجهاز التوجيه. لتحقيق أمان أفضل للشبكة، قم بالتغيير إلى اسم SSID فريد وقم بتعيين كلمة المرور.

اسم Wi-Fi (SSID):	ASUS_XX

* يشير **XX** إلى آخر حرفين من عنوان MAC لتردد 2.4 جيجاهرتز. يمكنك العثور عليه على الملصق في مؤخرة جهاز التوجيه.

3. بمجرد الاتصال، يتم تشغيل واجهة المستخدم العمومية على الويب (web GUI) تلقائيًا عندما تفتح مستعرض الويب. إذا لم يتم التشغيل تلقائيًا، فأدخل http://www.asusrouter.com.

4. قم بإعداد كلمة المرور بجهاز التوجيه لمنع الدخول غير المصرح به.

ملاحظات:

- لمعرفة التفاصيل بشأن الاتصال بشبكة لاسلكية، راجع دليل مستخدم مهايئ WLAN.
- لإعداد إعدادات الأمان للشبكة الخاصة بك، راجع **3.1.1 إعداد إعدادات الأمان اللاسلكية** في دليل المستخدم هذا.

2.2 إعداد الإنترنت السريع (QIS) مع الاكتشاف التلقائي

توجهك وظيفة إعداد الإنترنت السريع (QIS) لإعداد اتصال الإنترنت الخاص بك بسرعة.

ملاحظة: عند إعداد اتصال الإنترنت لأول مرة، اضغط على زر Reset (إعادة الضبط)على جهاز التوجيه اللاسلكي الخاص بك لإعادة ضبطه إلى الإعدادات الافتراضية من المصنع.

لاستخدام إعداد QIS مع الاكتشاف السريع:

1. ابدأ تشغيل أحد مستعرضي الويب. ستتم إعادة توجيهك إلى معالج الإعداد ASUS Setup Wizard (إعداد الإنترنت السريع). إذا لم تتم إعادة التوجيه، اكتب http://www.asusrouter.com يدويًا.

2. يكتشف جهاز التوجيه اللاسلكي تلقائيًا ما إذا كان نوع اتصال مزود خدمة الإنترنت (ISP) الخاص بك **Dynamic IP** أم **PPPoE** أم **PPTP** أم **L2TP**. اكتب المعلومات الضرورية لنوع اتصال ISP الخاص بك.

هام! احصل على المعلومات الضرورية من مزود خدمة الإنترنت (ISP) حول نوع اتصال الإنترنت.

ملاحظات:

- يحدث الاكتشاف التلقائي لنوع اتصال ISP الخاص بك عندما تقوم بتكوين جهاز التوجيه اللاسلكي للمرة الأولى أو عند إعادة ضبط جهاز التوجيه اللاسلكي إلى الإعدادات الافتراضية له.
- إذا فشل QIS في اكتشاف نوع اتصال الإنترنت الخاص بك، فانقر فوق **Manual Setting (إعداد يدوي)** وقم بتكوين إعدادات اتصال الإنترنت يدويًا.

3. قم بتعيين اسم الشبكة اللاسلكية (SSID) ومفتاح الأمان لاتصال اللاسلكي شبكة WiFi 7 الخاص بك. انقر فوق **Apply (تطبيق)** عند الانتهاء.

4. في صفحة **Login Information Setup (إعداد معلومات تسجيل الدخول)**، قم بتغيير كلمة مرور تسجيل الدخول إلى جهاز التوجيه لمنع الوصول غير المخوّل إلى جهاز التوجيه اللاسلكي الخاص بك.

ملاحظة: يختلف اسم مستخدم تسجيل الدخول إلى جهاز التوجيه اللاسلكي وكلمة المرور عن اسم شبكة WiFi 7 (SSID) ومفتاح الأمان. يسمح لك اسم مستخدم تسجيل الدخول إلى جهاز التوجيه اللاسلكي وكلمة المرور بتسجيل الدخول إلى واجهة المستخدم العمومية على الويب (Web GUI) لجهاز التوجيه اللاسلكي لتكوين إعدادات جهاز التوجيه اللاسلكي. يسمح اسم شبكة WiFi 7 (SSID) ومفتاح الأمان لأجهزة Wi-Fi بتسجيل الدخول والاتصال بشبكة WiFi 7 الخاصة بك.

2.3 الاتصال بالشبكة اللاسلكية الخاصة بك

بعد إعداد جهاز التوجيه اللاسلكي عن طريق QIS، يمكنك توصيل جهاز الكمبيوتر أو أي جهاز ذكي آخر بالشبكة اللاسلكية الخاصة بك.

للاتصال بالشبكة:

1. من جهاز الكمبيوتر، انقر فوق أيقونة الشبكة في منطقة الإخطارات لعرض الشبكات اللاسلكية المتاحة.
2. حدد الشبكة اللاسلكية التي تريد الاتصال بها، ثم انقر فوق **Connect (اتصال)**.
3. قد تحتاج إلى إدخال مفتاح أمان الشبكة للاتصال بالشبكات اللاسلكية المحمية، ثم انقر فوق **OK (موافق)**.
4. انتظر حتى يقوم الكمبيوتر بإنشاء الاتصال بالشبكة اللاسلكية بنجاح. ويتم عرض حالة الاتصال، وتعرض أيقونة الشبكة حالة قوة إشارة الاتصال.

ملاحظات:

- راجع الفصول التالية لمعرفة مزيد من التفاصيل حول تكوين إعدادات الشبكة اللاسلكية الخاصة بك.
- راجع دليل مستخدم الجهاز الخاص بك لمعرفة مزيد التفاصيل حول توصيله بالشبكة اللاسلكية الخاصة بك.

---

3 تكوين الإعدادات العامة و المتقدمة

3.1 تسجيل الدخول إلى واجهة المستخدم العمومية على الويب (Web GUI)

يجري تزويد جهاز التوجيه اللاسلكي من ASUS بواجهة مستخدم رسومية على الويب (GUI) تتميز بالبديهية وتسمح لك بتكوين الميزات المختلفة للجهاز بسهولة عن طريق مستعرض ويب مثل Internet Explorer أو Firefox أو Safari أو Google Chrome.

ملاحظة: قد تختلف هذه الميزات حسب إصدارات البرنامج الثابت المختلفة.

لتسجيل الدخول إلى واجهة المستخدم العمومية على الويب (web GUI):

1. في مستعرض الويب، اكتب يدويًا عنوان IP الافتراضي لجهاز التوجيه اللاسلكي: http://www.asusrouter.com.
2. في صفحة تسجيل الدخول، اكتب اسم المستخدم وكلمة المرور التي قمت بتعيينها في **2.2 إعداد الإنترنت السريع (QIS) مع الاكتشاف التلقائي**.
3. يمكنك الآن استخدام واجهة المستخدم العمومية على الويب (Web GUI) لتكوين الإعدادات المختلفة لجهاز التوجيه اللاسلكي الخاص بك من ASUS.

* الصورة مرجعية فقط.

ملاحظة: إذا كنت تسجل الدخول إلى واجهة المستخدم العمومية على الويب (Web GUI) للمرة الأولى، فسوف يتم توجيهك إلى صفحة Quick Internet Setup (QIS)) (إعداد الإنترنت السريع) تلقائيًا.

3.1.1 إعداد إعدادات الأمان اللاسلكية

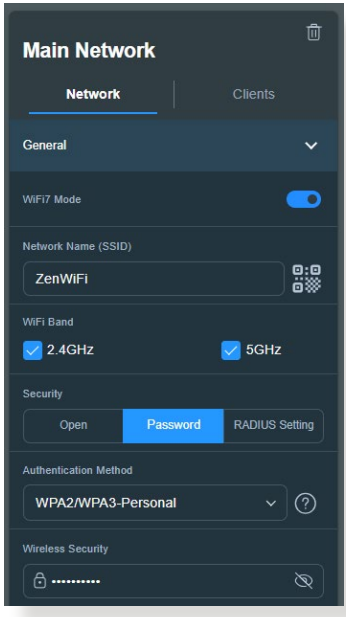
لحماية الشبكة اللاسلكية من الوصول غير المخول، يلزمك تكوين إعدادات الأمان الخاصة بها.

لإعداد إعدادات الأمان اللاسلكية:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Network Map (خريطة الشبكة)**.
2. حدد الشبكة و يمكنك تكوين إعدادات الأمان اللاسلكية مثل SSID، ومستوى الأمان وإعدادات التشفير.

ملاحظة: يمكنك إعداد إعدادات أمان لاسلكية مختلفة لنطاقات 2.4 جيجاهرتز و5 جيجاهرتز.

إعدادات أمان 2.4/5 جيجا هرتز



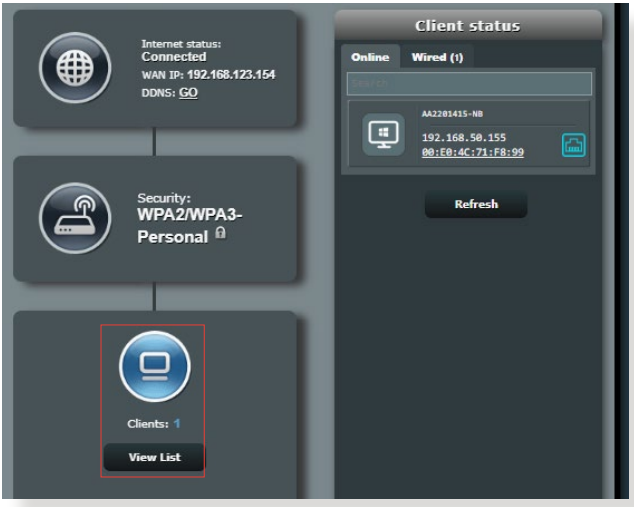
3. في حقل **Network Name (اسم الشبكة) (SSID)**، اكتب اسمًا فريدًا للشبكة اللاسلكية الخاصة بك.

4. من القائمة المنسدلة **WEP Encryption (تشفير WEP)**، حدد طريقة التشفير للشبكة اللاسلكية الخاصة بك.

هام! يحظر معيار IEEE 802.11n/ac/ax استخدام إنتاجية عالية مع WEP أو WPA-TKIP كطريقة تشفير أحادية البث. إذا استخدمت طرق التشفير هذه، فإن معدل نقل البيانات سوف ينخفض إلى اتصال IEEE 802.11g بسرعة 54 ميجابايت في الثانية.

5. اكتب مفتاح مرور الأمان الخاص بك.
6. انقر فوق **Apply (تطبيق)** عند الانتهاء.

3.1.2 إدارة عملاء الشبكة



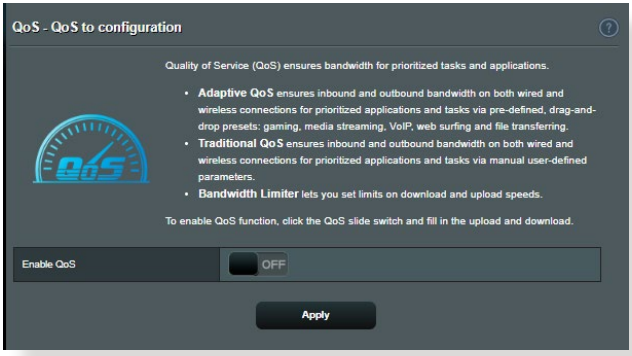
لإدارة عملاء الشبكة:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Network Map (خريطة الشبكة)**.
2. في شاشة Network Map (خريطة الشبكة)، حدد أيقونة **Client status (حالة العميل)** لعرض معلومات عن عميل الشبكة الخاص بك.
3. لحظر وصول العميل إلى الشبكة الخاصة بك، حدد العميل وانقر فوق **block (حظر)**.

3.2 جودة الخدمة التكيفية

3.2.1 إدارة عرض نطاق QoS (جودة الخدمة)

تسمح لك جودة الخدمة (QoS) أن تقوم بضبط أولوية عرض النطاق وإدارة حركة بيانات الشبكة.



لإعداد أولوية عرض النطاق:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Adaptive QoS (جودة الخدمة التكيفية)** > **QoS (جودة الخدمة)**.
2. انقر فوق **ON (تشغيل)** لتمكين جودة الخدمة. املأ حقول عرض نطاق التحميل والتنزيل.

ملاحظة: احصل على معلومات عرض النطاق من مزود خدمة الإنترنت (ISP).

3. انقر فوق **Apply (تطبيق)**.

ملاحظة: تختص User Specify Rule List (قائمة قواعد التحديد للمستخدم) بالإعدادات المتقدمة. إذا أردت تعيين الأولوية لتطبيقات شبكة وخدمات شبكة معينة، فحدد **User-defined QoS rules (قواعد QoS المحددة بواسطة المستخدم)** أو **User-defined Priority (الأولوية المحددة من المستخدم)** من القائمة المنسدلة في الزاوية العلوية اليمنى.

4. في صفحة **User-defined QoS rules (قواعد QoS المحددة بواسطة المستخدم)**، يوجد أربعة أنوع افتراضية للخدمة على الإنترنت - هي تصفح الويب، وHTTPS ونقل الملفات. حدد الخدمة المفضلة، واملأ حقول **Source IP or MAC (عنوان IP أو MAC المصدر)** و**Destination Port (منفذ الوجهة)**، و**Protocol (البروتوكول)** و**Transferred (المنقول)** و**Priority (الأولوية)** ثم انقر فوق **Apply (تطبيق)**. سيتم تكوين المعلومات في شاشة قواعد QoS.

ملاحظات:

- لملء عنوان IP أو MAC المصدر، يمكنك:

a) إدخال عنوان IP خاص، مثل "192.168.122.1".

b) إدخال عنوان IP يتضمن مجموعة فرعية واحدة أو داخل نفس تجمع IP، مثل "192.168.123.*"- أو "192.168.*.*"

c) أدخل جميع عناوين IP على هيئة "*.*.*.*" أو اترك الحقل فارغًا.

d) يتألف تنسيق عنوان MAC من ست مجموعات وكل مجموعة تتضمن رقمين سداسيين عشريين، مفصولين بعلامة العمود (:)، بترتيب الإرسال (مثل aa:bc:ef:12:34:56)

- للحصول على نطاق منفذ الوجهة أو المصدر، يمكنك القيام بأي مما يلي:

a) إدخال منفذ خاص، مثل "95".

b) إدخال المنافذ داخل النطاق، مثل "103:315" أو ">100"، أو "<65535".

- يحتوي عمود **Transferred (المنقول)** على معلومات حول حركة البيانات الصادرة والواردة (حركة البيانات في الشبكة الواردة والصادرة) لأحد الأقسام. في هذا العمود، يمكنك تعيين حد نقل البيانات بالشبكة (بالكيلوبايت) لخدمة معينة لإنشاء أولويات خاصة للخدمة المعينة إلى منفذ خاص. على سبيل المثال، في حالة وصول جهازي عميلين بالشبكة، PC 1 و PC 2، إلى الإنترنت (المعين من المنفذ 80)، ولكن الجهاز PC 1 يتجاوز حد نقل البيانات بالشبكة بسبب بعض مهام التنزيل، فسوف تكون الأولوية منخفضة للجهاز PC 1. إذا كان لا يلزمك تعيين حد نقل بيانات، فاترك هذا الحقل فارغًا.

---

5. في صفحة **User-defined Priority (الأولوية المحددة بواسطة المستخدم)**، يمكنك تعيين الأولوية لتطبيقات الشبكة أو الأجهزة ضمن خمسة مستويات من القائمة المنسدلة لـ **user-defined QoS rules (قواعد QoS المحددة بواسطة المستخدم)**. استنادًا إلى مستوى الأولوية، يمكنك استخدام الطرق التالية لإرسال حزم البيانات:

- تغيير ترتيب حزم الشبكة الصادرة التي يتم إرسالها إلى الإنترنت.
- تحت جدول **Upload Bandwidth (عرض نطاق التحميل)**، قم بتعيين **Minimum Reserved Bandwidth (أدنى عرض نطاق محجوز)** و **Maximum Bandwidth Limit (الحد الأقصى لعرض النطاق)** لتطبيقات الشبكة المتعددة بمستويات أولوية مختلفة. تشير النسبة المئوية إلى معدلات عرض نطاق التحميل المتوفر لتطبيقات الشبكة المحددة.

ملاحظات:

- يتم تجاهل الحزم منخفضة الأولوية لضمان إرسال الحزم مرتفعة الأولوية.
- تحت جدول **Download Bandwidth (عرض نطاق التنزيل)**، قم بتعيين **Maximum Bandwidth Limit (الحد الأقصى لعرض النطاق)** لتطبيقات الشبكة المتعددة بالترتيب المقابل. ستؤدي الحزمة الصادرة عالية الأولوية إلى حزمة واردة منخفضة الأولوية.
- إذا لم يكن هناك أي حزم مرسلة من التطبيقات عالية الأولوية، فسيكون معدل الإرسال الكامل لاتصال الإنترنت متوفرًا للحزم منخفضة الأولوية.

---

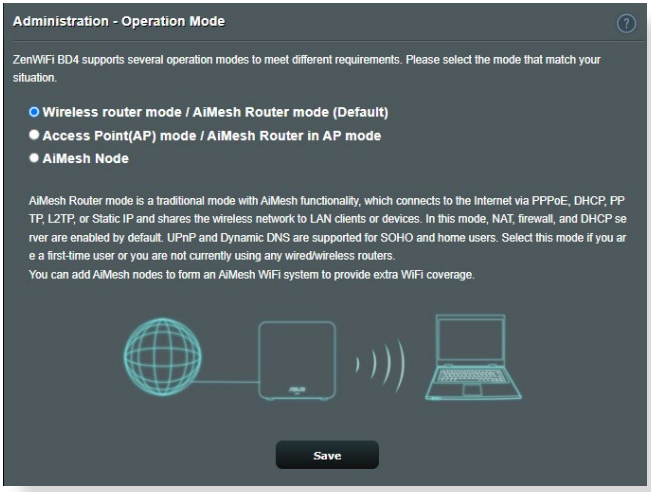
6. قم بتعيين الحزمة الأعلى أولوية. لضمان تجربة ألعاب سلسة على الإنترنت، يمكنك تعيين ACK وSYN وICMP كحزمة عالية الأولوية.

ملاحظة: تأكد من تمكين QoS أولا وإعداد حدود معدلات التحميل والتنزيل.

3.3 الإدارة

3.3.1 وضع التشغيل

تسمح لك صفحة Operation Mode (وضع التشغيل) بتحديد الوضع المناسب لشبكتك.



لإعداد وضع التشغيل:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Administration (الإدارة)** > **Operation Mode (وضع التشغيل)**.
2. حدد أي من أوضاع التشغيل هذه:

- **Wireless router mode (وضع جهاز التوجيه اللاسلكي) (الافتراضي):** في وضع جهاز التوجيه اللاسلكي، يتصل جهاز التوجيه اللاسلكي بالإنترنت ويوفر الوصول إلى الإنترنت للأجهزة المتوفرة على شبكة الاتصال المحلية الخاصة به.
- **Access Point mode (وضع نقطة الوصول):** في هذا الوضع، ينشئ جهاز التوجيه شبكة لاسلكية جديدة على شبكة موجودة.
- **AiMesh Node (عقدة AiMesh):** يمكنك تعيين جهاز ZenWiFi BD4 كعقدة AiMesh لتوسيع تغطية WiFi لأجهزة توجيه AiMesh.

3. انقر فوق **Save (حفظ)**.

ملاحظة: سوف يتم إعادة تمهيد جهاز التوجيه عندما تغير الأوضاع.

3.3.2 النظام

تسمح لك صفحة **System (النظام)** بتكوين إعدادات جهاز التوجيه اللاسلكي الخاص بك.

لإعداد إعدادات النظام:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Administration (الإدارة)** > **System (النظام)**.
2. يمكنك تكوين الإعدادات الآتية:

- **Change router login password (تغيير كلمة المرور لتسجيل الدخول إلى جهاز التوجيه):** يمكنك تغيير كلمة المرور واسم تسجيل الدخول لجهاز التوجيه اللاسلكي بإدخال اسم جديد وكلمة مرور جديدة.
- **WPS button behavior (سلوك زر WPS):** يمكن استخدام زر WPS الفعلي على جهاز التوجيه اللاسلكي لتنشيط WPS.
- **Time Zone (المنطقة الزمنية):** حدد المنطقة الزمنية للشبكة الخاصة بك.
- **NTP Server (خادم NTP):** يمكن لجهاز التوجيه اللاسلكي الوصول إلى خادم NTP (بروتوكول وقت الشبكة) من أجل مزامنة الوقت.
- **Enable Telnet (تمكين Telnet):** انقر فوق **Yes (نعم)** لتمكين خدمات Telnet على الشبكة. انقر فوق **No (لا)** لتعطيل Telnet.
- **Authentication Method (طريقة المصادقة):** يمكنك استخدام بروتوكول HTTP أو HTTPS أو كليهما لتأمين الوصول إلى جهاز التوجيه.
- **Enable Web Access from WAN (تمكين الوصول إلى ويب من WAN):** حدد **Yes (نعم)** للسماح بالأجهزة من خارج الشبكة بالوصول إلى إعدادات GUI لجهاز التوجيه اللاسلكي. حدد **No (لا)** لمنع الوصول.
- **Only allow specific IP (السماح بعنوان IP خاص فقط):** انقر فوق **Yes (نعم)** إذا كنت تريد تحديد عنوان IP للأجهزة المسموح بوصولها إلى إعدادات GUI لجهاز التوجيه اللاسلكي من WAN.

3. انقر فوق **Apply (تطبيق)**.

3.3.3 ترقية البرنامج الثابت

ملاحظة: قم بتنزيل أحدث برنامج ثابت من موقع ASUS على العنوان http://www.asus.com.

لترقية البرنامج الثابت:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Administration (الإدارة)** > **Firmware Upgrade (ترقية البرنامج الثابت)**.
2. في حقل **Firmware Version (اصدار البرنامج الثابت)**، انقر فوق **Check (فحص)** لتحديد مكان الملف الذي تم تنزيله.
3. انقر فوق **Upload (تحميل)**.

ملاحظات:

- عند اكتمال عملية الترقية، انتظر بعض الوقت لكي يتم إعادة تمهيد النظام.
- إذا فشلت عملية الترقية، فسوف يدخل جهاز التوجيه اللاسلكي في وضع الإنقاذ ويبدأ مؤشر LED للطاقة على اللوحة الأمامية في الوميض ببطء. لاستعادة أو استرداد النظام، راجع قسم **4.2 استعادة البرنامج الثابت**.

3.3.4 استعادة/حفظ/تحميل الإعداد

لاستعادة/حفظ/تحميل إعدادات جهاز التوجيه اللاسلكي:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Administration (الإدارة)** > **Restore/Save/Upload Setting (استعادة/حفظ/تحميل الإعداد)**.
2. حدد المهام التي تود القيام بها:

- للاستعادة إلى إعدادات المصنع الافتراضية، انقر على **Restore (استعادة)**، وانقر على **OK (موافق)** في رسالة التأكيد
- لحفظ إعدادات النظام الحالية، انقر فوق **Save setting (حفظ الإعداد)**، وانتقل إلى المجلد الذي تريد أن يتم حفظ الملف فيه وانقر فوق **Save (حفظ)**.
- للاستعادة من ملف إعدادات نظام محفوظ، انقر فوق **Upload (تحميل)**، لتحديد مكان الملف، ثم انقر فوق **Open (فتح)**.

هام! إذا استمرت المشكلات، قم بتحميل أحدث إصدار من البرنامج الثابت وقم بتكوين الإعدادات الجديدة. لا تقم باستعادة جهاز التوجيه إلى الإعدادات الافتراضية له.

AiProtection 3.4

يوفر AiProtection مراقبة آنية لأجل اكتشاف البرامج الضارة وبرامج التجسس والوصول غير المرغوب. كما يقوم أيضًا بتصفية مواقع الويب والتطبيقات غير المرغوبة ويسمح لك بجدولة وقت يمكن فيه للجهاز المتصل الوصول إلى الإنترنت.

3.4.1 حماية الشبكة

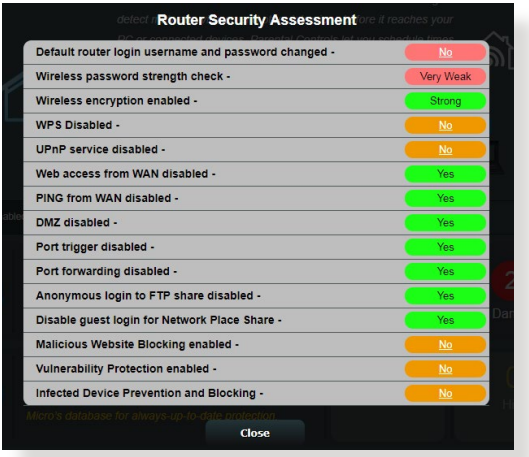
تمنع حماية الشبكة استغلال الشبكة وتحمي الشبكة من الوصول غير المخول.

تكوين حماية الشبكة

تكوين حماية الشبكة:

1. من جزء التنقل، انتقل إلى **General (عام)** > **AiProtection**.
2. من صفحة **AiProtection** الرئيسية، انقر فوق **Network Protection (حماية الشبكة)**.
3. من علامة التبويب **Network Protection (حماية الشبكة)** انقر فوق **Scan (فحص)**.

عند الانتهاء من الفحص، فإن الأداة المساعدة تعرض النتائج في صفحة **Router Security Assessment (تقييم أمان جهاز التوجيه)**.



هام! العناصر المعلمة بـ **Yes (نعم)** في صفحة **Router Security Assessment (تقييم أمان جهاز التوجيه)** تعتبر بالحالة **safe (آمنة)**. يوصى بتكوين العناصر المعلمة بـ **No (لا)** أو **Weak (ضعيف)** أو **Very Weak (ضعيف للغاية)** تبعًا لذلك.

---

4. (اختياري) من صفحة **Router Security Assessment (تقييم أمان جهاز التوجيه)**، قم بتكوين العناصر المعلمة بـ **No (لا)** أو **Weak (ضعيف)** أو **Very Weak (ضعيف للغاية)**. للقيام بذلك:

   a. انقر فوق أحد العناصر.

ملاحظة: عندما تنقر فوق أحد العناصر، فإن الأداة توجهك إلى صفحة إعداد العنصر.

---

   b. من صفحة إعدادات العنصر، قم بتكوين وإجراء التغييرات الضرورية وانقر فوق **Apply (تطبيق)** عند الانتهاء.

c. ارجع إلى صفحة **Router Security Assessment (تقييم أمان جهاز التوجيه)** وانقر فوق **Close (إغلاق)** للخروج من الصفحة.

5. لتكوين إعدادات الأمان تلقائيًا، انقر فوق **Secure Your Router (تأمين جهاز التوجيه)**.

6. عند ظهور رسالة مطالبة، انقر فوق **OK (موافق)**.

حجب مواقع الويب الضارة

تقيد هذه الميزة الوصول إلى مواقع الويب الضارة المعروفة في قاعدة بيانات السحابة للتمتع بالحماية المحدثة دائمًا.

ملاحظة: يتم تمكين هذه الوظيفة تلقائيًا إذا قمت بتشغيل **Router Weakness Scan (فحص ضعف جهاز التوجيه)**.

لتمكين حجب مواقع الويب الضارة:

1. من جزء التنقل، انتقل إلى **General (عام)** > **AiProtection**.

2. من صفحة **AiProtection** الرئيسية، انقر فوق **Network Protection (حماية الشبكة)**.

3. من جزء **Malicious Sites Blocking (حجب مواقع الويب الضارة)**، انقر فوق **ON (تشغيل)**.

IPS ثنائي الاتجاه

يحمي نظام IPS ثنائي الاتجاه (نظام منع التطفل) جهاز التوجيه من هجمات الشبكة من خلال حظر الحزم الواردة الضارة واكتشاف الحزمة الصادرة المشتبه بها.

ملاحظة: يتم تمكين هذه الوظيفة تلقائيًا إذا قمت بتشغيل **Router Weakness Scan (فحص ضعف جهاز التوجيه)**.

لتمكين IPS ثنائي الاتجاه:

1. من جزء التنقل، انتقل إلى **General (عام)** > **AiProtection**.

2. من صفحة **AiProtection** الرئيسية، انقر فوق **Network Protection (حماية الشبكة)**.

3. من جزء **Two-Way IPS (IPS ثنائي الاتجاه)**، انقر فوق **ON (تشغيل)**.

منع الأجهزة المصابة بالفيروسات وحجبها

تمنع هذه الميزة الأجهزة المصابة بالفيروسات من نقل المعلومات الشخصية أو الحالة المصابة بالفيروسات إلى جهات خارجية.

ملاحظة: يتم تمكين هذه الوظيفة تلقائيًا إذا قمت بتشغيل **Router Weakness Scan (فحص ضعف جهاز التوجيه)**.

لتمكين منع الأجهزة المصابة بالفيروسات وحجبها:

1. من جزء التنقل، انتقل إلى **General (عام)** > **AiProtection**.
2. من صفحة **AiProtection** الرئيسية، انقر فوق **Network Protection (حماية الشبكة)**.
3. من جزء **Infected Device Prevention and Blocking (منع الأجهزة المصابة بالفيروسات وحجبها)**، انقر فوق **ON (تشغيل)**.

لتكوين تفضيلات التنبيه:

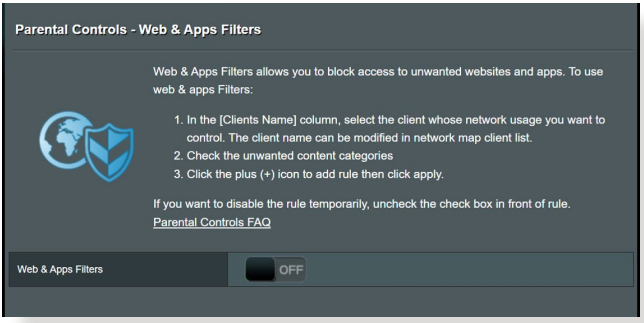
1. من جزء **Infected Device Prevention and Blocking (منع الأجهزة المصابة بالفيروسات وحجبها)**، انقر فوق **Alert Preference (تفضيل التنبيه)**.
2. حدد أو اكتب مزود البريد الإلكتروني، وحساب البريد الإلكتروني وكلمة المرور ثم انقر فوق **Apply (تطبيق)**.

3.4.2 إعداد التحكم الأبوي

يسمح لك التحكم الأبوي بالتحكم في وقت الوصول إلى الإنترنت أو تعيين حد زمني لاستخدام شبكة أحد الأجهزة العميلة.

للذهاب إلى الصفحة الرئيسية لـ Parental Controls (التحكم الأبوي):

من جزء التنقل، انتقل إلى **General (عام)** > **Parental Controls (التحكم الأبوي)**.



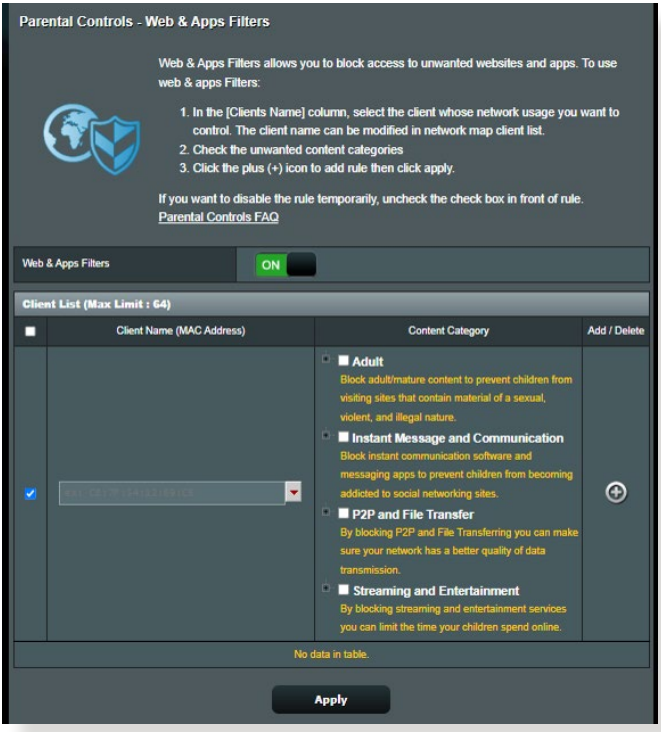
عوامل تصفية الويب والتطبيقات

عوامل تصفية الويب والتطبيقات هي ميزة تابعة لـ **Parental Controls (التحكم الأبوي)** تسمح لك بحظر الوصول إلى مواقع الويب أو التطبيقات غير المرغوبة.

لتكوين عوامل تصفية الويب والتطبيقات:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Parental Controls (التحكم الأبوي)**.
2. من جزء **Web & Apps Filters (عوامل تصفية الويب والتطبيقات)**، وانقر فوق **ON (تشغيل)**.
3. عند ظهور رسالة المطالبة الخاصة باتفاقية ترخيص المستخدم النهائي (EULA) ، انقر فوق **I agree (أوافق)** للاستمرار.
4. من عمود **Client List (قائمة العملاء)**، حدد أو اكتب اسم العميل من مربع القائمة المنسدلة.
5. من عمود **Content Category (فئة المحتوى)**، حدد عوامل التصفية من الفئات الرئيسية الأربعة. **Adult (بالغ)**، **Instant Message and Communication (المراسلة الفورية والاتصالات)**، **P2P and File Transfer (P2P ونقل الملفات)**، **Streaming and Entertainment (البث والترفيه)**.

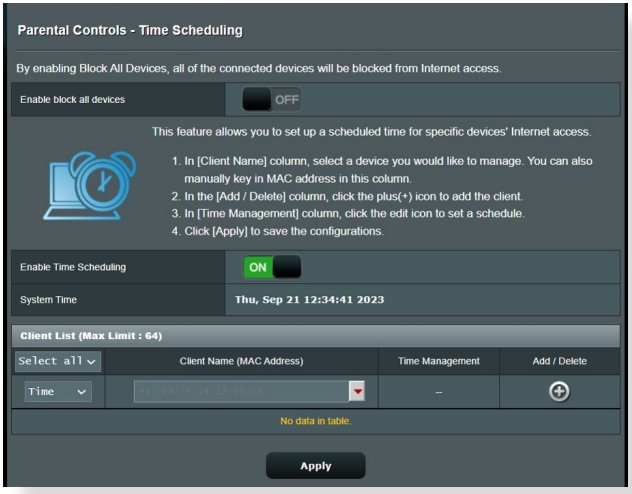
6. انقر فوق ⊕ لإضافة ملف تعريف العميل.
7. انقر فوق **Apply (تطبيق)** لحفظ الإعدادات.



جدولة الوقت

يسمح لك جدولة الوقت بضبط حد زمني لاستخدام شبكة أحد العملاء.

ملاحظة: تأكد من مزامنة وقت النظام مع خادم NTP.



لتكوين جدولة الوقت:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Parental Controls (التحكم الأبوي)** > **Time Scheduling (جدولة الوقت)**.
2. من جزء **Enable Time Scheduling (تمكين جدولة الوقت)**، انقر فوق **ON (تشغيل)**.
3. من عمود **Clients Name (اسم العملاء)**، حدد أو اكتب اسم العميل من مربع القائمة المنسدلة.

ملاحظة: يمكنك أيضًا إدخال عنوان MAC للجهاز العميل في عمود **عنوان MAC الخاص بالجهاز العميل**. تأكد من أن اسم الجهاز العميل لا يحتوي على أحرف خاصة أو مسافات لأنها تؤدي إلى تعطل تشغيل جهاز التوجيه بصورة طبيعية.

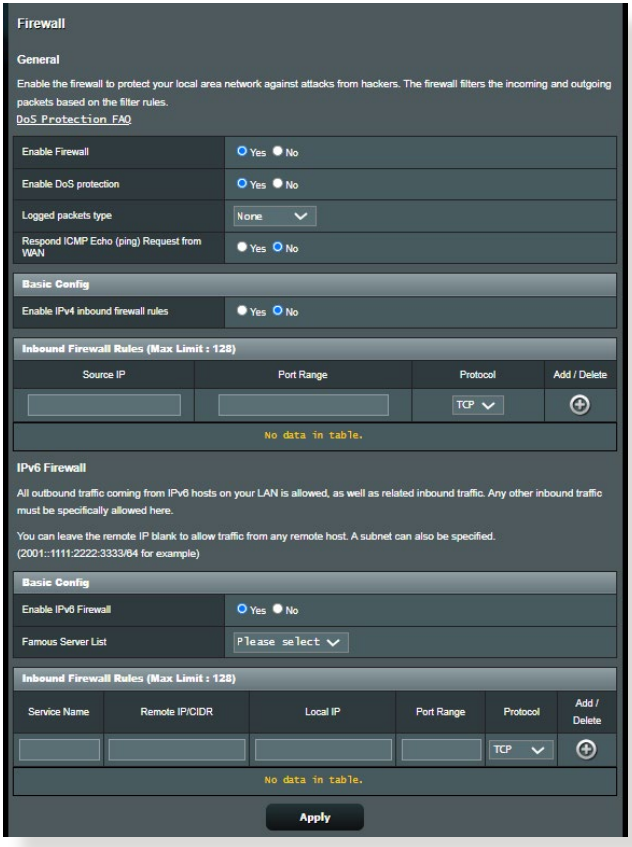
4. انقر فوق ⊕ لإضافة ملف تعريف العميل.
5. انقر فوق **Apply (تطبيق)** لحفظ الإعدادات.

3.5 جدار الحماية

يمكن أن يعمل جهاز التوجيه اللاسلكي كجدار حماية للأجهزة في الشبكة الخاصة بك.

ملاحظة: يتم تمكين ميزة جدار الحماية هذه افتراضيًا.

3.5.1 عام



لإعداد إعدادات جدار الحماية الأساسية:

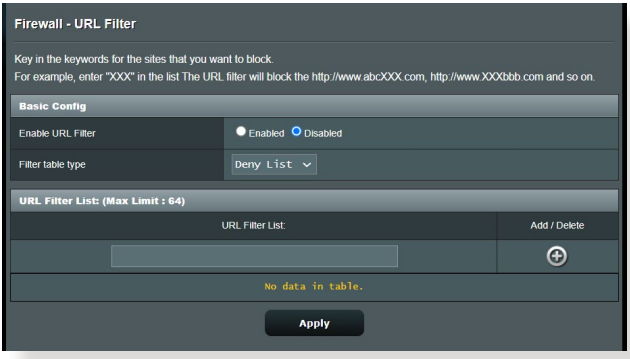
1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Firewall (جدار الحماية)** > **General (عام)**.
2. في حقل **Enable Firewall (تمكين جدار الحماية)**، حدد **Yes (نعم)**.

3. في **Enable DoS protection (تمكين حماية رفض الخدمة)** حدد **Yes (نعم)** لحماية شبكتك من هجمات DoS (رفض الخدمة) بالرغم من أن ذلك قد يؤثر على أداء جهاز التوجيه.
4. يمكنك أيضًا مراقبة الحزم التي يجري تبادلها بين اتصال LAN وWAN. في نوع الحزم المسجلة، حدد **Dropped (مفصولة)** أو **Accepted (مقبولة)**، أو **Both (كليهما)**.
5. انقر فوق **Apply (تطبيق)**.

3.5.2 عامل تصفية URL

يمكنك تحديد كلمات أساسية أو عناوين ويب لمنع الوصول إلى عناوين URL خاصة.

ملاحظة: يعتمد عامل تصفية URL على استعلام DNS. في حالة وصول أحد العملاء على الشبكة بالفعل إلى موقع ويب مثل http://www.abcxxx.com، عندئذ لن يتم حجب موقع الويب (نظرًا لأن ذاكرة التخزين المؤقت لـ DNS في النظام تخزن مواقع الويب التي تمت زيارتها في السابق). لحل هذه المشكلة، امسح ذاكرة التخزين المؤقت لـ DNS قبل إعداد عامل تصفية URL.

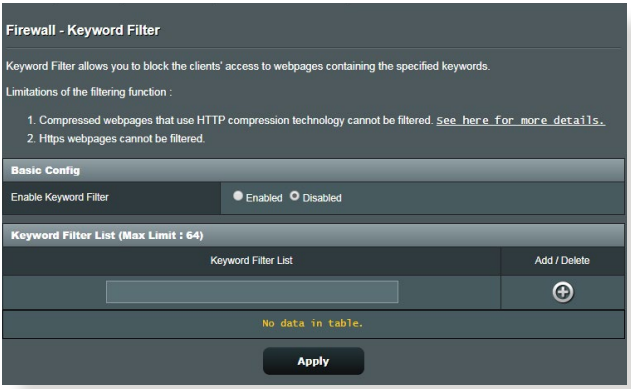


لإعداد عامل تصفية URL:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Firewall (جدار الحماية)** > **URL Filter (عامل تصفية URL)**.
2. في حقل Enable URL Filter (تمكين عامل تصفية URL)، حدد **Enabled (ممكّن)**.
3. أدخل عنوان URL وانقر فوق زر .
4. انقر فوق **Apply (تطبيق)**.

3.5.3 عامل تصفية الكلمات الأساسية

يحجب عامل تصفية الكلمات الأساسية الوصول إلى صفحات الويب التي تحتوي على كلمات أساسية محددة.



لإعداد عامل تصفية كلمات أساسية:

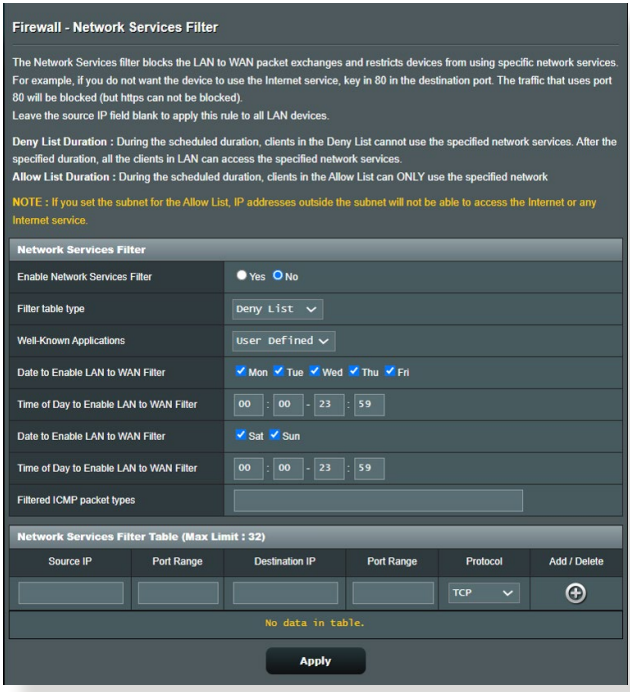
1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Firewall (جدار الحماية)** > **Keyword Filter (عامل تصفية الكلمات الأساسية)**.
2. في حقل Enable Keyword Filter (تمكين عامل تصفية الكلمات الأساسية)، حدد **Enabled (ممكّن)**.
3. أدخل كلمة أو عبارة وانقر فوق زر **Add (إضافة)**.
4. انقر فوق **Apply (تطبيق)**.

ملاحظات:

- يعتمد عامل تصفية الكلمات الأساسية على استعلام DNS. في حالة وصول أحد العملاء على الشبكة بالفعل إلى موقع ويب مثل http://www.abcxxx.com، عندئذ لن يتم حجب موقع الويب (نظرًا لأن ذاكرة التخزين المؤقت لـ DNS في النظام تخزّن مواقع الويب التي تمت زيارتها في السابق). لحل هذه المشكلة، امسح ذاكرة التخزين المؤقت لـ DNS قبل إعداد عامل تصفية الكلمات الأساسية.
- لا يمكن تصفية صفحات الويب التي تم ضغطها باستخدام HTTP. لا يمكن أيضًا حظر صفحات HTTPS باستخدام عامل تصفية الكلمات الأساسية.

3.5.4 عامل تصفية خدمات الشبكة

يحجب عامل تصفية خدمات الشبكة تبادلات حزم LAN إلى WAN ويحظر عملاء الشبكة من الوصول إلى خدمات ويب معينة مثل Telnet أو FTP.



لإعداد عامل تصفية خدمة الشبكة:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Firewall (جدار الحماية)** > **Network Service Filter (عامل تصفية خدمة الشبكة)**.
2. في حقل Enable Network Service Filter (تمكين عامل تصفية خدمة الشبكة)، حدد **Yes (نعم)**.
3. حدد نوع جدول عامل التصفية. **Deny (رفض)** تحظر خدمات شبكة معينة. **Allow (سماح)** تحدد الوصول إلى خدمات شبكة محددة.
4. حدد اليوم والوقت اللذين ستكون فيهما عوامل التصفية نشطة.
5. حدد إحدى خدمات الشبكة المطلوب تصفيتها، وأدخل عنوان IP المصدر وعنوان IP الوجهة ونطاق المنفذ والبروتوكول. انقر على زر ⊕.
6. انقر فوق **Apply (تطبيق)**.

3.6 IPv6

يدعم جهاز التوجيه اللاسلكي هذا عناوين IPv6، وهو نظام يدعم أكثر من عنوان IP. وهذا المعيار ليس متوفرًا على نطاق واسع. اتصل بمزود خدمة الإنترنت الخاص بك إذا كانت خدمة الإنترنت تدعم IPv6.

لإعداد IPv6:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **IPv6**.
2. حدد **Connection type (نوع الاتصال)** الخاص بك. تختلف خيارات التكوين تبعًا لنوع الاتصال المحدد.
3. أدخل إعدادات LAN و DNS لـ IPv6.
4. انقر فوق **Apply (تطبيق)**.

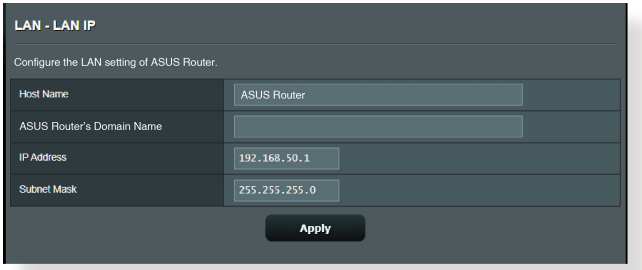
ملاحظة: يرجى مراجعة مزود خدمة الإنترنت الخاص بك (ISP) بشأن معلومات IPv6 الخاصة بخدمة الإنترنت.

3.7 شبكة الاتصال المحلية (LAN)

3.7.1 عنوان IP لشبكة الاتصال المحلية (LAN)

تتيح لك شاشة LAN IP (عنوان IP لشبكة الاتصال المحلي) تعديل إعدادات عنوان IP لشبكة الاتصال المحلية لجهاز التوجيه اللاسلكي.

ملاحظة: سوف تنعكس أي تغييرات في عنوان IP لشبكة الاتصال المحلية على إعدادات DHCP الخاصة بك.

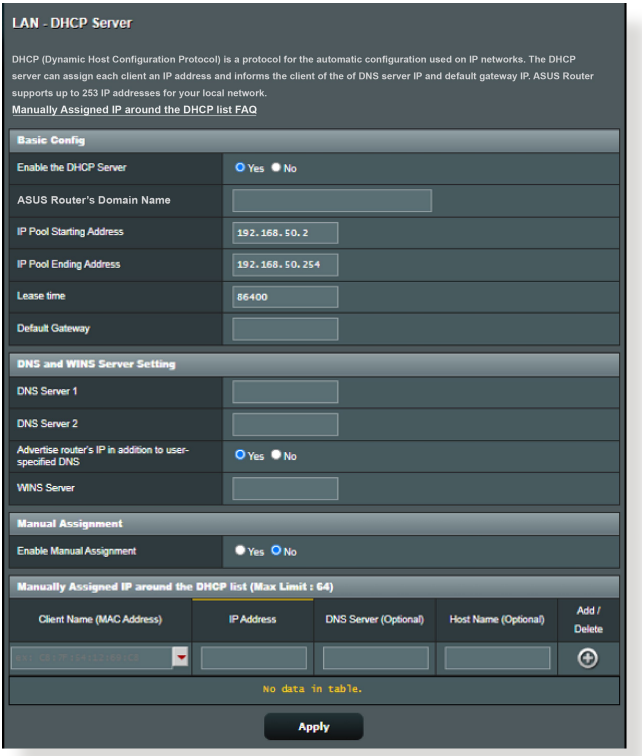


لتعديل إعدادات عنوان IP لشبكة الاتصال المحلية:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة) > LAN (شبكة الاتصال المحلية) > LAN IP (عنوان IP لشبكة الاتصال المحلية)**.
2. قم بتعديل **IP address (عنوان IP)** و**Subnet Mask (وقناع الشبكة الفرعية)**.
3. عند الانتهاء، انقر فوق **Apply (تطبيق)**.

3.7.2 خادم DHCP

يستخدم جهاز التوجيه اللاسلكي الخاص بك DHCP لتعيين عناوين IP تلقائيًا على الشبكة الخاصة بك. يمكنك تحديد نطاق عنوان IP ووقت الإيجار للعملاء على الشبكة الخاصة بك.



لتكوين خادم DHCP:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **LAN (شبكة الاتصال المحلية)** > **DHCP Server (خادم DHCP)**.
2. في حقل **Enable the DHCP Server (تمكين خادم DHCP)**، حدد **Yes (نعم)**.

3. في مربع نص **Domain Name (اسم المجال)**، أدخل اسم المجال لجهاز التوجيه اللاسلكي.
4. في حقل **IP Pool Starting Address (عنوان البدء لمجموعة IP)**، اكتب عنوان IP للبدء.
5. في حقل **IP Pool Ending Address (عنوان النهاية لمجموعة IP)**، اكتب عنوان IP للنهاية.
6. في حقل **Lease Time (وقت الإيجار)**، حدد بالثواني متى تنتهي صلاحية عنوان IP المعين. وبمجرد أن يصل إلى الحد الزمني، سوف يعين خادم DHCP عنوان IP جديد.

ملاحظات:

- نوصي بأن تستخدم عنوان IP بالتنسيق xxx.192.168.50 (حيث تشير حروف xxx إلى أي رقم بين 2 و254) عند تحديد نطاق عنوان IP.
- يجب ألا يكون عنوان البدء لمجموعة IP أكبر من عنوان النهاية لمجموعة IP.

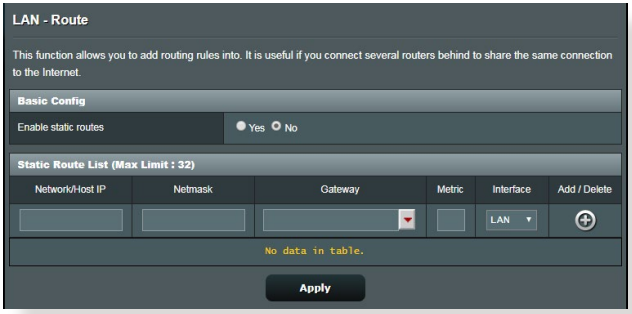
---

7. في قسم **DNS and WINS Server Settings (DNS و WINS إعدادات الخادم)**، اكتب خادم DNS وعنوان IP لخادم WINS حسب الحاجة.
8. يمكن لجهاز التوجيه اللاسلكي الخاص بك كذلك تعيين عناوين IP يدويًا للأجهزة على الشبكة الخاصة بك. في حقل **Enable Manual Assignment (تمكين التعيين اليدوي)**، اختر **Yes (نعم)** لتعيين عنوان IP إلى عناوين MAC الخاصة على الشبكة. يمكن إضافة ما يصل إلى 32 عنوان MAC إلى قائمة DHCP للتعيين اليدوي.

3.7.3 المسار

إذا كانت الشبكة الخاصة بك تستخدم أكثر من جهاز توجيه لاسلكي، فعندئذ يمكنك تكوين جدول توجيه لمشاركة نفس خدمة الإنترنت.

ملاحظة: نوصي بألا تغير إعدادات التوجيه الافتراضية إلا إذا كنت تتمتع بمعرفة متقدمة بجداول جهاز التوجيه.

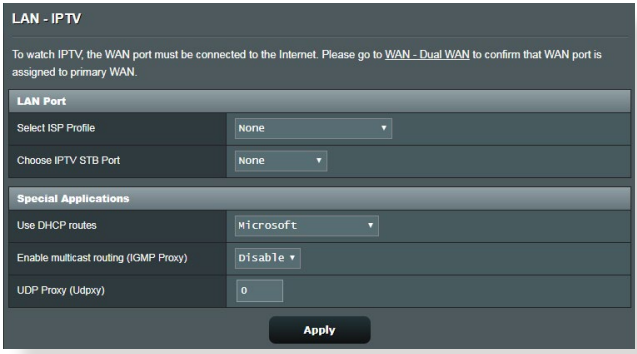


لتكوين جدول توجيه LAN:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **LAN (شبكة الاتصال المحلية)** > **Route (المسار)**.
2. في حقل **Enable static routes (تمكين مسارات ثابتة)**، اختر **Yes (نعم)**.
3. في قائمة **Static Route List (قائمة المسار الثابت)**، أدخل معلومات الشبكة لنقاط الوصول أو العقد الأخرى. انقر فوق زر **Add (إضافة)** أو **Delete (حذف)** لإضافة أو إزالة جهاز على الشبكة.
4. انقر فوق **Apply (تطبيق)**.

3.7.4 التليفزيون عبر الإنترنت (IPTV)

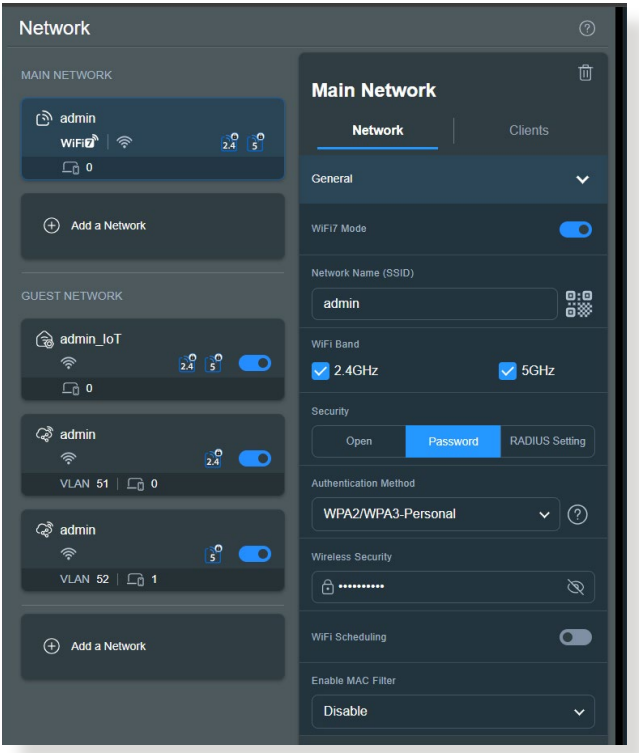
يدعم جهاز التوجيه اللاسلكي الاتصال بخدمات التليفزيون عبر الإنترنت (IPTV)عن طريق إما مزود خدمة الإنترنت (ISP) أو شبكة اتصال محلية. توفر علامة تبويب IPTV (التليفزيون عبر الإنترنت) إعدادات التكوين اللازمة لإعداد خدمة التليفزيون عبر الإنترنت أو الصوت عبر الإنترنت و(VoIP) والبث المتعدد وبروتوكول UDP للخدمة الخاصة بك. اتصل بمزود خدمة الإنترنت (ISP) للحصول على معلومات خاصة بشأن الخدمة.



3.8 شبكة

3.8.1 الشبكة الرئيسية - تصفية MAC

يوفر عامل تصفية MAC اللاسلكي إمكانية التحكم في الحزم المرسلة إلى عنوان MAC محدد (التحكم في وصول الوسائط) على الشبكة اللاسلكية الخاصة بك.



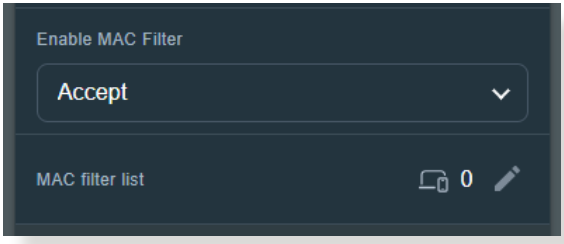
لإعداد عامل تصفية MAC اللاسلكي:

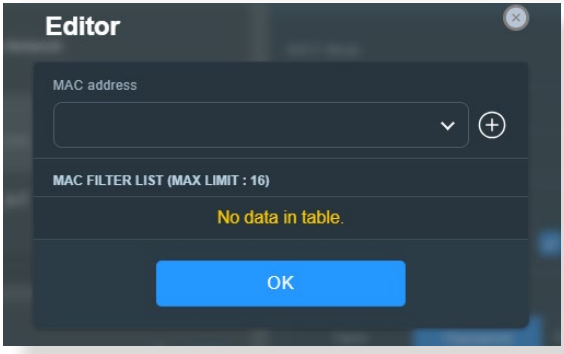
1. من جزء التنقل، انتقل إلى **General (عام)** > **Network (شبكة)** > **Main Network (الشبكة الرئيسية)** واختر اسم الشبكة (SSID) للشبكة الرئيسية.
2. في القائمة المنسدلة **Enable Mac Filter (تمكين عامل تصفية Mac)**، حدد إما **Accept (قبول)** أو **Reject (رفض)**.
   - حدد **Accept (قبول)** للسماح للأجهزة في قائمة عوامل تصفية MAC بالوصول إلى الشبكة اللاسلكية.

- حدد **Reject (رفض)** لمنع الأجهزة في قائمة عوامل تصفية MAC من الوصول إلى الشبكة اللاسلكية.

ملاحظة: حدد **Disable (تعطيل)** إذا كنت تريد إيقاف تشغيل **Enable MAC Filter (تمكين عامل تصفية MAC)**.

3. في قائمة عوامل تصفية MAC، اضغط على علامة للوصول إلى صفحة **Editor (المحرر)**، ثم اضغط على علامة والحقل المُخصص في عنوان MAC للجهاز.
4. انقر فوق **OK (موافق)**.

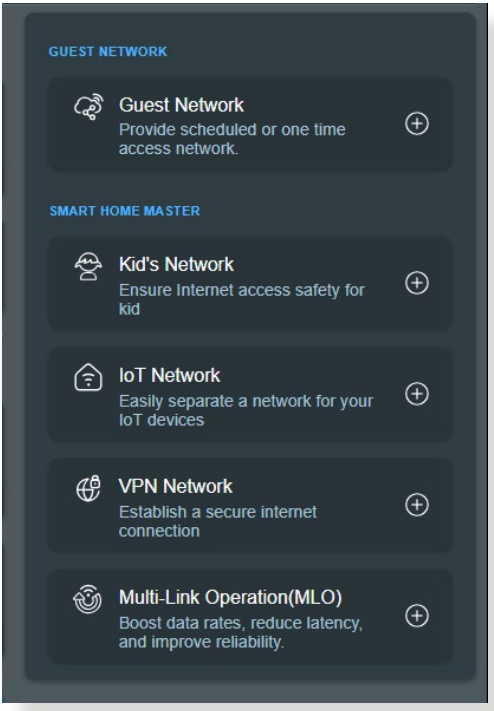




3.8.2 شبكة ضيف

3.8.2.1 شبكة ضيف

توفر شبكة الضيف للزائرين المؤقتين إمكانية الاتصال بالإنترنت عن طريق الوصول إلى معرفات SSID منفصلة أو شبكات بدون توفير الوصول إلى الشبكة الخاصة بك.

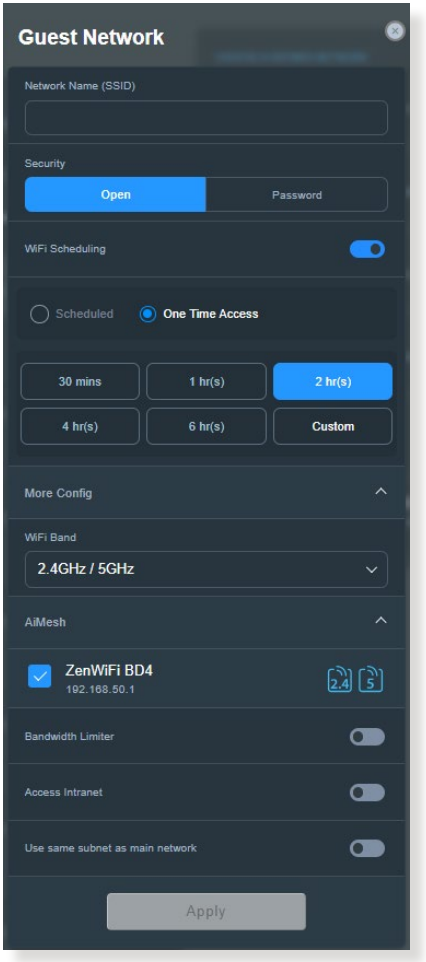


ملاحظة: يدعم ZenWiFi BD4 ما يصل إلى ثلاثة معرفات SSID في شبكة الضيوف.

لإنشاء شبكة ضيف:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Network (شبكة)** > **Guest Network (شبكة الضيف)** > **Add a Network (أضف شبكة)**.
2. حدد **Guest Network (شبكة الضيف)** وقم بتعيين اسم شبكة لشبكتك المؤقتة في حقل **Network Name (SSID) (اسم الشبكة (SSID))**.
3. حدد طريقة المصادقة ضمن **Security (الأمان)**.
4. حدد وقت الوصول أو اختر **Scheduled (مجدول)** لإضافة ملف تعريف جدول عبر الإنترنت.

5. حدد **WiFi Band (نطاق WiFi)** لشبكة الضيف التي تريد إنشاءها.
6. تمكين أو تعطيل **Bandwidth Limiter (محدد النطاق الترددي)**.
7. تمكين أو تعطيل **Access Intranet (الوصول إلى إنترانت)**.
8. عند الانتهاء، انقر فوق **Apply (تطبيق)**.

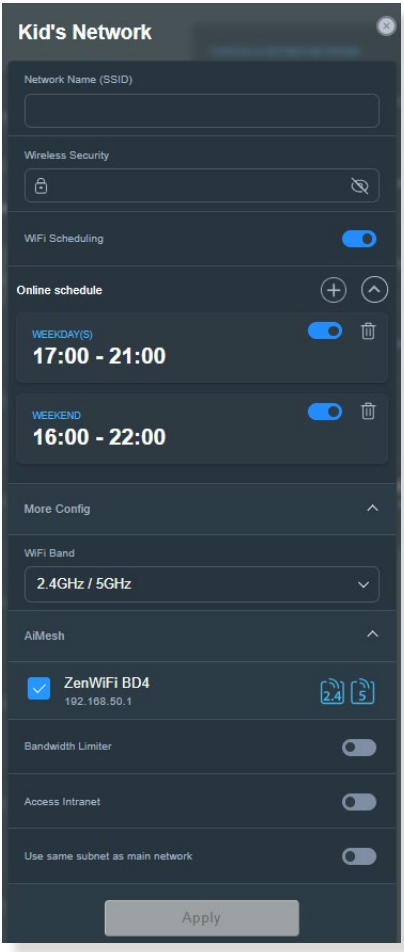


Smart Home Master 3.8.2.2

يعد Smart Home Master أداة قوية وسهلة الاستخدام لتجزئة الشبكة. فهو يبسط عملية إنشاء وإدارة سيناريوهات الشبكات الفرعية المتقدمة مثل إنشاء معرّف مجموعة خدمات الشبكة (SSID) مخصص لأجهزة أطفالك، أو الاتصال بشبكة VPN من خلال شبكة فرعية مخصصة، أو حتى إنشاء معرّف مجموعة خدمات الشبكة (SSID) واحد آمن لجميع أجهزة إنترنت الأشياء الخاصة بك.

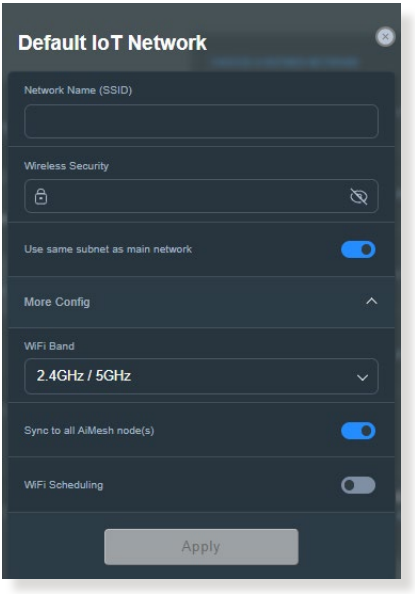
لإنشاء شبكة للأطفال:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Network (شبكة)** > **Guest Network (شبكة الضيف)** > **Add a Network (أضف شبكة)**.
2. حدد **Kid's Network (شبكة الأطفال)** وقم بتعيين اسم الشبكة ومفتاح الأمان في حقلي **Network Name (اسم الشبكة) (SSID)** و **Wireless Security (الأمان اللاسلكي)**.
3. قم بتخصيص وقت الوصول إلى الإنترنت في حقل **Online schedule (الجدول الزمني عبر الإنترنت)**.
4. حدد **WiFi Band (نطاق WiFi)** لشبكة الأطفال التي تريد إنشاءها.
5. تمكين أو تعطيل **Bandwidth Limiter (محدد النطاق الترددي)**.
6. تمكين أو تعطيل **Access Intranet (الوصول إلى إنترانت)**.
7. عند الانتهاء، انقر فوق **Apply (تطبيق)**.



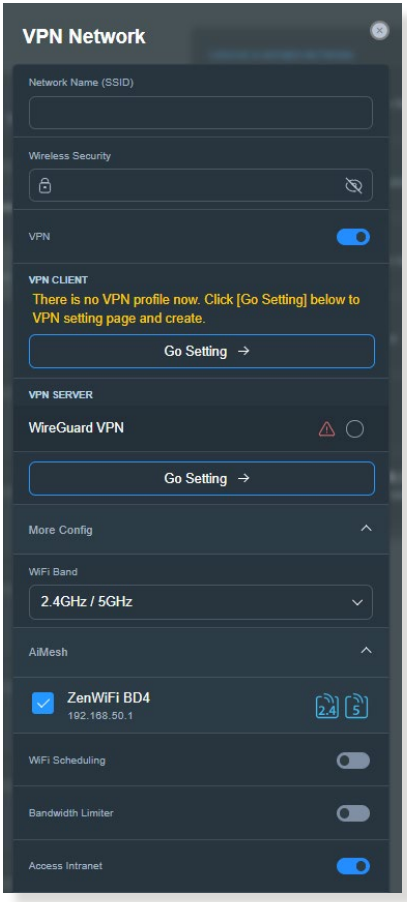
لإنشاء شبكة IoT:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Network (شبكة)** > **Guest Network (شبكة الضيف)** > **Add a Network (أضف شبكة)**.
2. حدد **IoT Network (شبكة IoT)** وقم بتعيين اسم الشبكة ومفتاح الأمان في حقلي **Network Name (اسم الشبكة) (SSID)** و **Wireless Security (الأمان اللاسلكي)**.
3. حدد **WiFi Band (نطاق WiFi)** لشبكة IoT التي تريد إنشاءها.
4. قم بتخصيص وقت الوصول إلى الإنترنت من خلال تمكين **WiFi Scheduling (جدولة WiFi)**.
5. عند الانتهاء، انقر فوق **Apply (تطبيق)**.



لإنشاء شبكة VPN:

1. من جزء التنقل، انتقل إلى **General (عام)** > **Network (شبكة)** > **Guest Network (شبكة الضيف)** > **Add a Network (أضف شبكة)**.
2. حدد **VPN Network (شبكة VPN)** وقم بتعيين اسم الشبكة ومفتاح الأمان في حقلي **Network Name (اسم الشبكة) (SSID)** و **Wireless Security (الأمان اللاسلكي)**.
3. إذا لم تقم بإعداد ملف تعريف VPN لخادم VPN أو عميل VPN، فانقر فوق **Go Setting (انتقال إلى الإعداد)** لإنشاء ملف تعريف VPN.
4. حدد **WiFi Band (نطاق WiFi)** لشبكة VPN التي تريد إنشاءها.
5. قم بتخصيص وقت الوصول إلى الإنترنت من خلال تمكين **WiFi Scheduling (جدولة WiFi)**.
6. تمكين أو تعطيل **Bandwidth Limiter (محدد النطاق الترددي)**.
7. تمكين أو تعطيل **Access Intranet (الوصول إلى إنترانت)**.
8. عند الانتهاء، انقر فوق **Apply (تطبيق)**.


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

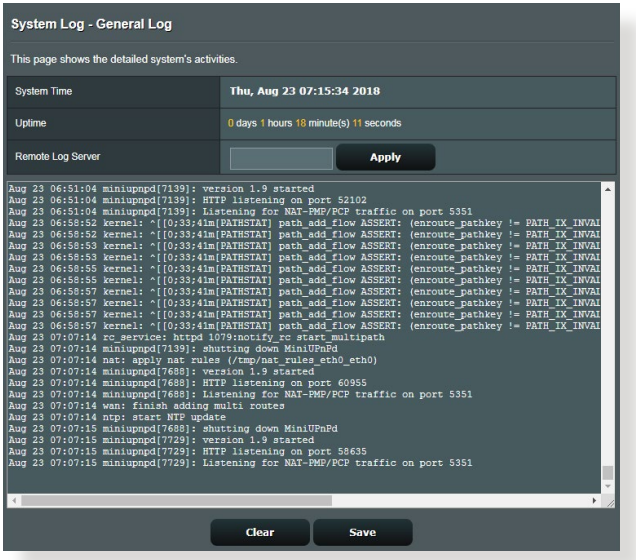
3.9 سجل النظام

يحتوي سجل النظام على أنشطة الشبكة المسجلة.

ملاحظة: تجري إعادة ضبط سجل النظام عند إعادة تمهيد جهاز التوجيه أو فصل الطاقة عنه.

لعرض سجل النظام:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **System Log (سجل النظام)**.
2. يمكنك عرض أنشطة الشبكة الخاصة بك في أي من علامات التبويب هذه:
   - General Log (السجل العام)
   - Wireless Log (سجل اللاسلكي)
   - DHCP Leases (تأجيرات DHCP)
   - IPv6
   - Routing Table (جدول التوجيه)
   - Port Forwarding (إعادة توجيه المنفذ)
   - Connections (الاتصالات)



3.10 محلل حركة البيانات

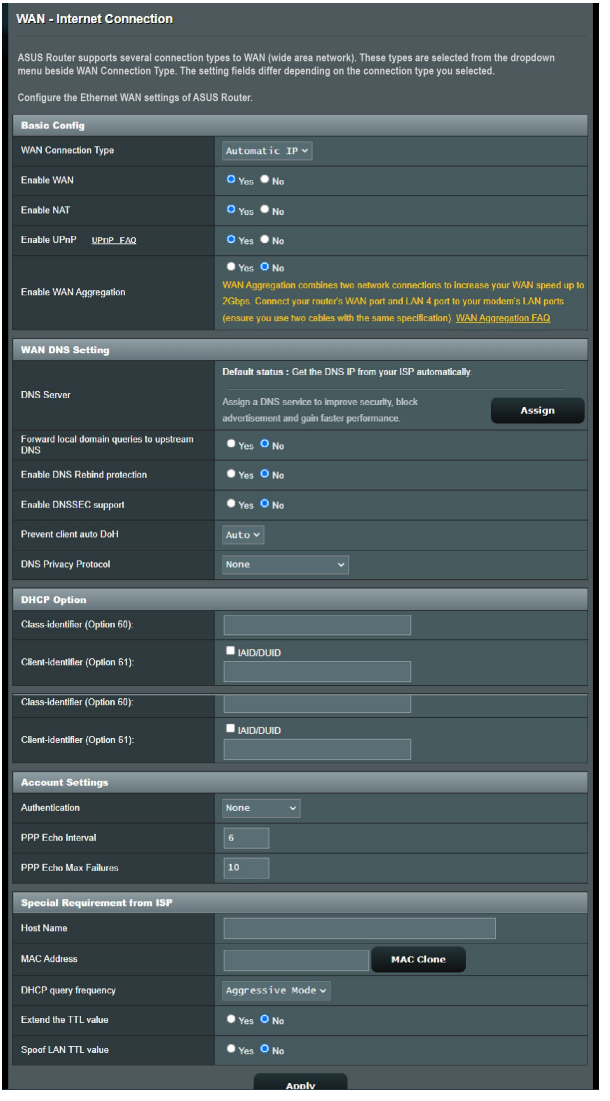
تسمح ميزة مراقبة حركة البيانات لك بالوصول إلى استخدام عرض النطاق وسرعة الإنترنت الخاص بك، والشبكات السلكية أو اللاسلكية. كما يتيح لك مراقبة حركة بيانات الشبكة آنيًا وبصفة منتظمة. وتعرض كذلك خيار عرض حركة بيانات الشبكة خلال آخر 24 ساعة.

ملاحظة: يتم إرسال الحزم من الإنترنت بالتساوي إلى الأجهزة السلكية واللاسلكية.

3.11 الشبكة واسعة النطاق (WAN)

3.11.1 اتصال الإنترنت

تسمح شاشة Internet Connection (اتصال الإنترنت) لك بتكوين إعدادات لأنواع اتصال الشبكة واسعة النطاق (WAN) المتنوعة.



لتكوين إعدادات اتصال شبكة واسعة النطاق (WAN):

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **WAN (الشبكة واسعة النطاق)** > **Internet Connection (اتصال الإنترنت)**.
2. قم بتكوين الإعدادات التالية أدناه. عند الانتهاء، انقر فوق **Apply (تطبيق)**.

- **نوع اتصال WAN**: اختر نوع مزود خدمة الإنترنت. الاختيارات هي **Automatic IP (عنوان IP تلقائي)** أو **PPPoE** أو **PPTP** أو **L2TP** أو **fixed IP (عنوان IP ثابت)**. استشر مزود خدمة الإنترنت (ISP) الخاص بك إذا تعذر على جهاز التوجيه الحصول على عنوانIP صالح أو إذا كنت غير متأكد من نوع اتصال WAN.
- **Enable WAN (تمكين WAN):** حدد **Yes (نعم)** للسماح لجهاز التوجيه بالوصول للإنترنت. حدد **No (لا)** لتعطيل الوصول إلى الإنترنت.
- **Enable NAT (تمكين NAT):** يمثل NAT (ترجمة عنوان الشبكة) نظامًا يتم فيه استخدام عنوان IP عمومي (WAN IP) لتوفير الوصول إلى الإنترنت لعملاء الشبكة باستخدام عنوان IP خاص في شبكة اتصال محلية (LAN). ويتم حفظ عنوان IP الخاص لكل عميل شبكة في جدول NAT ويتم استخدامه لتوجيه حزم البيانات الواردة.
- **Enable UPnP (تمكين UPnP):** يسمح UPnP (التوصيل والتشغيل العمومي) بالتحكم في عدة أجهزة (مثل أجهزة التوجيه والتليفزيون وأنظمة الإستريو ووحدات الألعاب والهاتف الخلوي)، عن طريق شبكة تعتمد على IP باستخدام تحكم مركزي أو بدونه عن طريق بوابة. يعمل UPnP على توصيل أجهزة الكمبيوتر بكافة عوامل النموذج، ما يوفر شبكة سلسة للتكوين عن بعد ونقل البيانات. وباستخدام UPnP، يتم اكتشاف أي جهاز جديد بالشبكة تلقائيًا. وبمجرد توصيل الأجهزة بالشبكة، فمن الممكن تكوينها عن بعد لدعم تطبيقات P2P والألعاب التفاعلية ومؤتمرات الفيديو وخوادم الويب أو خوادم الوكيل. بخلاف ميزة إعادة توجيه المنفذ، التي تتضمن التكوين اليدوي لإعدادات المنفذ، فإن UPnP يقوم تلقائيًا بتكوين جهاز التوجيه لقبول الاتصالات الواردة وتوجيه الطلبات إلى جهاز كمبيوتر معين على الشبكة المحلية.
- **Enable WAN Aggregation (تمكين تجميع WAN):** يعمل تجميع WAN على دمج اتصال شبكتين لزيادة سرعة WAN الخاصة بك إلى 2 جيجابايت في الثانية. قم بتوصيل منفذ WAN ومنفذ LAN 4 لجهاز التوجيه الخاص بك بمنافذ LAN بالمودم.

- **Connect to DNS Server (الاتصال بخادم DNS):** يسمح هذا لجهاز التوجيه بالحصول على عنوان IP الخاص بـ DNS من مزود خدمة الإنترنت تلقائيًا. يمثل DNS مضيف على الإنترنت يترجم أسماء الإنترنت إلى عناوين IP رقمية.
- **Authentication (المصادقة):** هذا العنصر يمكن أن يتم تحديده من قبل بعض مزودي خدمات الإنترنت. تحقق مع مزود خدمة الإنترنت الخاص بك واملأ هذه الحقول عند الحاجة.
- **Host Name (اسم المضيف):** يتيح هذا الحقل لك توفير اسم مضيف لجهاز التوجيه الخاص بك. وهذا في العادة أحد المتطلبات الخاصة من مزود خدمة الإنترنت الخاص بك. إذا قامت شركة مزود خدمة الإنترنت (ISP) بتعيين اسم مضيف للكمبيوتر، فأدخل اسم المضيف هنا.
- **MAC Address (عنوان MAC):** يعد عنوان MAC (التحكم في وصول الوسائط) معرفًا فريدًا لجهاز الشبكة الخاص بك. تراقب بعض شركات مزود خدمة الإنترنت (ISP) عنوان MAC للأجهزة المتصلة بالشبكة التي تتصل بالخدمة وترفض أي جهاز لم يتم التعرف عليه ويحاول الاتصال. لتفادي مشكلات الاتصال بسبب عنوان MAC غير المسجل، يمكنك:
  - اتصل بمزود خدمة الإنترنت وقم بتحديث عنوان MAC المرتبط بخدمة مزود خدمة الإنترنت.
  - استنسخ أو قم بتغيير عنوان MAC لجهاز التوجيه اللاسلكي من ASUS الخاص بك ليطابق عنوان MAC للجهاز المتصل بالشبكة السابق الذي تعرف عليه مزود خدمة الإنترنت.

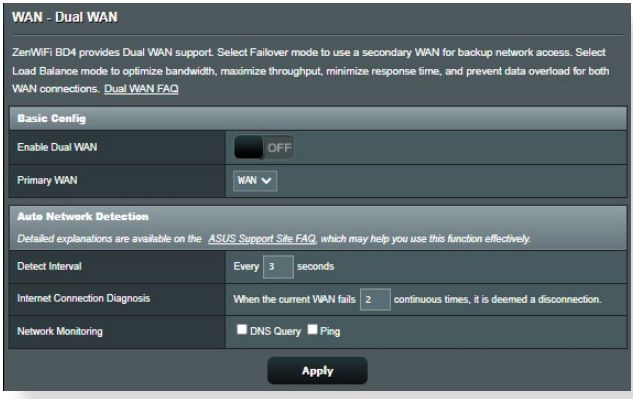
3.11.2 الشبكة واسعة النطاق الثنائية

تسمح لك Dual WAN (الشبكة واسعة النطاق الثنائية) بتحديد اتصالين من مزود خدمة الإنترنت إلى جهاز التوجيه الخاص بك، إحداهما شبكة واسعة النطاق رئيسية والأخرى شبكة واسعة النطاق ثانوية.

لتكوين الشبكة واسعة النطاق الثنائية:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **WAN (الشبكة واسعة النطاق)**.
2. انتقل إلى حقل **Dual WAN (الشبكة واسعة النطاق الثنائية)**، واضبطه على وضع **ON (تشغيل)**.
3. اختر **Primary WAN (الشبكة واسعة النطاق الرئيسية)** و**Secondary WAN (الشبكة واسعة النطاق الثانوية)**. هناك نوعان من شبكات WAN/LAN بسرعة 2.5 جيجابت لخياراتك.
4. اختر **Fail Over (النظام الاحتياطي)** أو **Load Balance (موازنة الحمل)**.
5. انقر فوق **Apply (تطبيق)**.

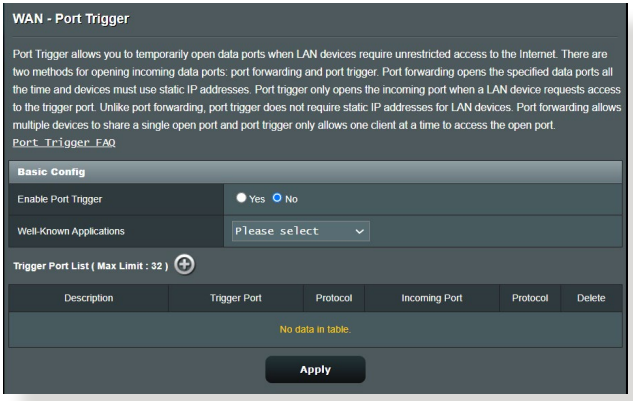
ملاحظة: تتوفر شروحات تفصيلية على موقع دعم ASUS بقسم الأسئلة الشائعة **https://www.asus.com/support/FAQ/1011719**.



3.11.3 مشغل المنافذ

يفتح تشغيل نطاق المنفذ منفذًا واردًا محددًا مسبقًا لفترة محدودة من الوقت عندما يجري أحد العملاء على شبكة الاتصال المحلية اتصالاً صادرًا إلى منفذ معين. يتم استخدام تشغيل المنفذ في السيناريوهات التالية:

- إذا كان هناك أكثر من عميل محلي يحتاج إلى إعادة توجيه المنفذ لنفس التطبيق في وقت مختلف.
- إذا كان التطبيق يتطلب منافذ واردة معينة تختلف عن المنافذ الصادرة.



لإعداد مشغل المنفذ:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **WAN (الشبكة واسعة النطاق)** > **Port Trigger (مشغل المنفذ)**.
2. قم بتكوين الإعدادات التالية أدناه. عند الانتهاء، انقر فوق **Apply (تطبيق)**.

- **Enable Port Trigger (تمكين مشغل المنفذ):** اختر **Yes (نعم)** لتمكين مشغل المنفذ.
- **Well-Known Applications (التطبيقات المعروفة):** حدد الألعاب المشهورة وخدمات الويب لإضافتها إلى Port Trigger List (قائمة مشغلات المنافذ).
- **Description (الوصف):** أدخل اسمًا قصيرًا أو وصفًا للخدمة.

- **Trigger Port (منفذ المشغل):** حدد أحد منافذ المشغل لفتح المنفذ الوارد.
- **Protocol (البروتوكول):** حدد البروتوكول TCP أو UDP.
- **Incoming Port (المنفذ الوارد):** حدد منفذًا واردًا لاستلام البيانات الواردة من الإنترنت.

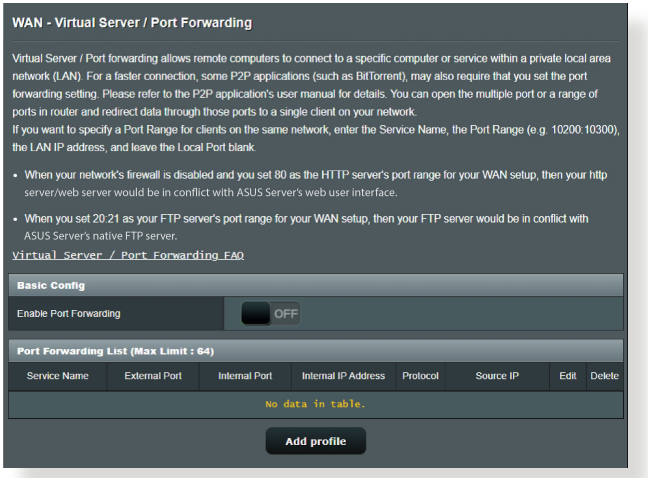
ملاحظات:

- عند الاتصال بخادم IRC، فإن أحد أجهزة الكمبيوتر العميلة يجري اتصالا صادرًا باستخدام نطاق منفذ المشغل 7000-66660. ويستجيب خادم IRC بالتحقق من اسم المستخدم وينشئ اتصالاً جديدًا إلى جهاز الكمبيوتر العميل باستخدام أحد المنافذ الواردة.
- في حالة تعطيل Port Trigger (مشغل المنفذ)، فإن جهاز التوجيه يوقف الاتصال نظرًا لأنه لا يستطيع تمييز أي جهاز كمبيوتر يطلب وصول IRC. عند تمكين Port Trigger (مشغل المنفذ)، فإن جهاز التوجيه يعين منفذًا واردًا لاستلام البيانات الواردة. ويتم إغلاق هذا المنفذ الوارد بمجرد انقضاء فترة زمنية معينة نظرًا لأن جهاز التوجيه يكون غير متأكد من متى سيتم إنهاء التطبيق.
- يسمح تشغيل المنفذ فقط لعميل واحد في الشبكة باستخدام خدمة معينة ومنفذ وارد معين في نفس الوقت.
- لا يمكنك استخدام نفس التطبيق لتشغيل منفذ في أكثر من جهاز كمبيوتر واحد في نفس الوقت. يقوم جهاز التوجيه بتوجيه المنفذ مرة أخرى فقط إلى آخر كمبيوتر لإرسال طلب/مشغل جهاز التوجيه.

3.11.4 الخادم الافتراضي/إعادة توجيه المنفذ

إعادة توجيه المنفذ هي طريقة لتوجيه حركة بيانات الشبكة من الإنترنت إلى منفذ معين أو نطاق منافذ معين إلى جهاز أو عدد من الأجهزة على الشبكة المحلية الخاصة بك.
يسمح إعداد إعادة توجيه المنفذ على جهاز التوجيه للكمبيوتر خارج الشبكة بالوصول إلى خدمات معينة يقدمها جهاز الكمبيوتر في الشبكة الخاصة بك.

ملاحظة: عند تمكين إعادة توجيه المنفذ، فإن جهاز التوجيه من ASUS يحظر حركة البيانات الواردة غير المطلوبة من الإنترنت ويسمح فقط بالردود من الطلبات الصادرة من شبكة الاتصال المحلية. ليس لدى عميل الشبكة حق الوصول إلى الإنترنت مباشرة، والعكس.



لإعداد إعادة توجيه المنفذ:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **WAN (الشبكة واسعة النطاق)** > **Virtual Server / Port Forwarding (الخادم الافتراضي/إعادة توجيه المنفذ)**.

2. قم بتكوين الإعدادات التالية أدناه. عند الانتهاء، انقر فوق **ON (تشغيل)**.

- **Enable Port Forwarding (تمكين إعادة توجيه المنفذ):** اضبط على وضع **ON (تشغيل)** لتمكين إعادة توجيه المنفذ.
- **Famous Server List (قائمة الخوادم المشهورة):** حدد نوع الخدمة الذي تريد الوصول إليه.
- **Famous Game List (قائمة الألعاب المشهورة):** يسرد هذا العنصر المنافذ المطلوبة لألعاب الإنترنت المشهورة لكي تعمل بشكل صحيح.
- **FTP Server Port (منفذ خادم FTP):** تجنب تعيين نطاق المنفذ 20:21 لخادم FTP الخاص بك نظرًا لأنه يتعارض مع تعيين خادم FTP الأصلي بجهاز التوجيه.
- **Service Name (اسم الخدمة):** أدخل اسم الخدمة.
- **Port Range (نطاق المنافذ):** إذا كنت تريد تحديد Port Range (نطاق منافذ) للعملاء على نفس الشبكة، فأدخل Service Name (اسم الخدمة)، وPort Range (نطاق المنافذ) (على سبيل المثال 10200:10300)، وعنوان LAN IP، واترك Local Port (المنفذ المحلي) فارغًا. يقبل نطاق المنافذ التنسيقات المختلفة مثل نطاق المنافذ (300:350)، أو المنافذ الفردية (566,789) أو المزيج منها (1015:1024,3021).

ملاحظات:

- عندما يكون جدار الحماية للشبكة معطلا وقمت بتعيين 80 كنطاق منافذ لخادم HTTP لإعداد الشبكة واسعة النطاق (WAN) الخاصة بك، عندئذ سيكون خادم http/خادم الويب الخاص بك متعارضًا مع واجهة مستخدم الويب لجهاز التوجيه.
- تستخدم الشبكة المنافذ من أجل تبادل البيانات، مع تعيين رقم منفذ ومهمة محددة لكل منفذ. على سبيل المثال، يتم استخدام المنفذ 80 مع HTTP. ويمكن استخدام منفذ معين بواسطة أحد التطبيقات أو الخدمات في المرة. بالتالي، سوف تفشل محاولة وصول جهازي كمبيوتر لإدخال بيانات إلى نفس المنفذ في نفس الوقت. على سبيل المثال، لا يمكك إعداد إعادة توجيه المنفذ للمنفذ 100 لجهازي كمبيوتر في نفس الوقت.

- **Local IP (عنوان IP محلي):** اكتب عنوان IP للشبكة المحلية للعميل.

ملاحظة: استخدم عنوان IP ثابت للعميل المحلي لكي تعمل إعادة توجيه المنفذ بشكل صحيح. راجع قسم **3.8 شبكة الاتصال المحلية (LAN)** لمزيد من المعلومات.

- **Local Port (منفذ محلي):** أدخل منفذًا خاصًا لاستلام الحزم المعادة توجيهها. اترك هذا الحقل فارغًا إذا أردت إعادة توجيه الحزم الواردة إلى نطاق منافذ محدد.
- **Protocol (البروتوكول):** حدد البروتوكول. إذا كنت غير متأكد، حدد **BOTH (كليهما)**.

للتحقق مما إذا تم تعيين إعادة توجيه المنفذ بنجاح أم لا:

- تأكد من أنه تم إعداد الخادم أو التطبيق وأنه يعمل.
- سوف تحتاج إلى جهاز عميل خارج شبكة الاتصال المحلية ولكن لديه وصول إلى الإنترنت (يُشار إليه باسم "عميل الإنترنت"). يجب عدم اتصال هذا العميل بجهاز التوجيه من ASUS.
- في عميل الإنترنت، استخدم عنوان WAN IP لجهاز التوجيه للوصول إلى الخادم. إذا كانت عملية إعادة توجيه المنفذ ناجحة، فيجب أن تكون قادرًا على الوصول إلى الملفات أو التطبيقات.

الاختلافات بين مشغل المنافذ وإعادة توجيه المنفذ:

- يعمل تشغيل المنفذ حتى بدون إعداد عنوان LAN IP محدد. بخلاف إعادة تعيين المنفذ، الذي يتطلب عنوان LAN IP ثابت، فإن تشغيل المنافذ يسمح بإعادة توجيه المنفذ ديناميكيًا باستخدام جهاز التوجيه. يتم تكوين نطاقات المنافذ المحددة مسبقًا لقبول الاتصالات الواردة لفترة محددة من الوقت. يسمح تشغيل المنفذ لعدة أجهزة كمبيوتر بتشغيل التطبيقات التي تتطلب في العادة إعادة توجيه يدوية لنفس المنافذ إلى كل جهاز كمبيوتر على الشبكة.
- يعتبر تشغيل المنفذ أكثر أمانًا من إعادة توجيه المنفذ نظرًا لأن المنافذ الواردة لا تكون مفتوحة طوال الوقت. ويتم فتحها فقط عند يجري أحد التطبيقات اتصالاً صادرًا عبر منفذ المشغل.

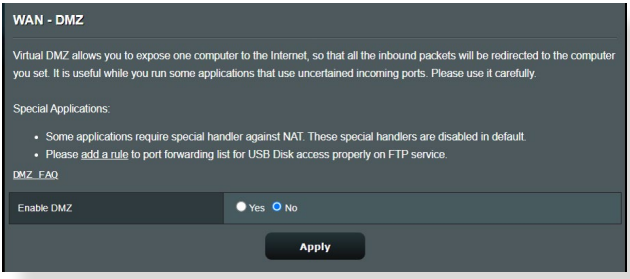
3.11.5 المنطقة المنزوعة (DMZ)

تعمل المنطقة DMZ على تعريض جهاز عميل واحدة للإنترنت، ما يسمح لهذا العميل باستلام جميع الحزم الواردة الموجهة إلى شبكة الاتصال المحلية.

ويتم في العادة تجاهل حركة البيانات الواردة من الإنترنت وتوجيهها إلى عميل محدد فقط في حالة تكوين إعادة توجيه المنفذ أو مشغل المنفذ على الشبكة. في تكوين المنطقة المنزوعة (DMZ)، يستلم عميل شبكة واحدة جميع الحزم الواردة.

يعتبر إعداد منطقة منزوعة (DMZ) على الشبكة مفيدًا عندما تحتاج إلى فتح المنافذ الواردة أو تريد استضافة مجال أو خادم ويب أو خادم بريد الإلكتروني.

تنبيه: إن فتح جميع المنافذ في أحد العملاء إلى الإنترنت يجعل الشبكة معرضة للهجمات الخارجية. يرجى التعرف على مخاطر الأمان المتعلقة باستخدام المنطقة المنزوعة (DMZ).



لإعداد منطقة منزوعة (DMZ):

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة) > WAN (الشبكة واسعة النطاق) > DMZ (المنطقة المنزوعة)**.
2. قم بتكوين الإعدادات التالية. عند الانتهاء، انقر فوق **Apply (تطبيق)**.

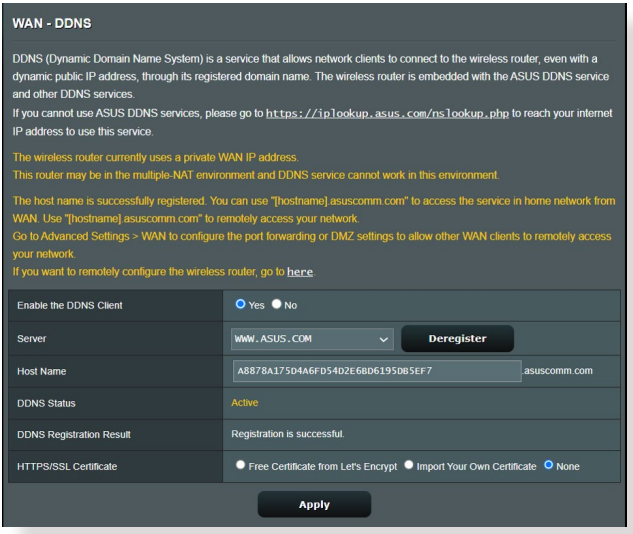
- **IP address of Exposed Station (عنوان IP الخاص بالمحطة المكشوفة):** اكتب عنوان LAN IP للعميل الذي سيوفر خدمة DMZ يكون مكشوفًا على الإنترنت. تأكد من أن عميل الخادم يتضمن عنوان IP ثابت.

لإزالة المنطقة المنزوعة (DMZ):

1. احذف عنوان LAN IP الخاص بالعميل من مربع نص **IP Address of Exposed Station (عنوان IP الخاص بالمحطة المكشوفة)**.
2. عند الانتهاء، انقر فوق **Apply (تطبيق)**.

3.11.6 نظام أسماء النطاقات الديناميكي (DDNS)

يسمح إعداد DDNS (نظام أسماء النطاقات الديناميكي) لك بالوصول إلى جهاز التوجيه من خارج الشبكة عن طريق خدمة DDNS المقدمة من ASUS أو خدمة DDNS أخرى.



لإعداد نظام أسماء النطاقات الديناميكي (DDNS):

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **WAN (الشبكة واسعة النطاق)** > **DDNS (نظام أسماء النطاقات الديناميكي)**.
2. قم بتكوين الإعدادات التالية أدناه. عند الانتهاء، انقر فوق **Apply (تطبيق)**.

- **Enable the DDNS Client (تمكين عميل DDNS):** قم بتمكين DDNS للوصول إلى جهاز توجيه ASUS عن طريق اسم DNS بدلا من عنوان WAN IP.
- **Server and Host Name (اسم الخادم والمضيف):** اختر نظام DDNS من ASUS أو نظام DDNS آخر. إذا أردت استخدام DDNS من ASUS، فقم بملء اسم المضيف بالتنسيق xxx.asuscomm.com (حيث يشير xxx إلى اسم المضيف الخاص بك).

- إذا أردت استخدام خدمة DDNS مختلفة، فانقر فوق FREE TRIAL (تجربة مجانية) وقم بالتسجيل على الإنترنت أولا. قم بملء اسم المستخدم أو عنوان البريد الإلكتروني وكلمة المرور أو حقول مفتاح DDNS.
- **Enable wildcard (تمكين حرف البدل):** قم بتمكين حرف البدل إذا كانت خدمة DDNS تتطلب واحدًا منها.

ملاحظات:

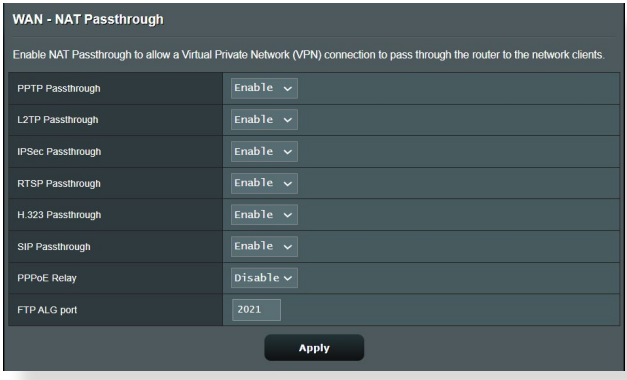
لا تعمل خدمة DDNS في الظروف الآتية:

- عندما يستخدم جهاز التوجيه اللاسلكي عنوان WAN IP خاص (x.x.192.168 أو x.x.x.10 أو x.x.172.16), كما هو مبين بالنص الأصفر.
- جهاز التوجيه ربما يكون على شبكة تستخدم جداول NAT متعددة.

3.11.7 اجتياز NAT

يسمح اجتياز NAT لاتصال الشبكة الخاصة الظاهرية (VPN) باجتياز جهاز التوجيه إلى عملاء الشبكة. يتم تمكين إعدادات PPTP Passthrough (اجتياز PPTP)، و L2TP Passthrough (اجتياز)، وIPsec Passthrough (اجتياز IPsec) و RTSP Passthrough (اجتياز RTSP) افتراضيًا.

لتمكين / تعطيل إعدادات اجتياز NAT، انتقل إلى **Advanced Settings (الإعدادات المتقدمة) > WAN (الشبكة واسعة النطاق) > NAT Passthrough (اجتياز NAT)**. عند الانتهاء، انقر فوق **Apply (تطبيق)**.

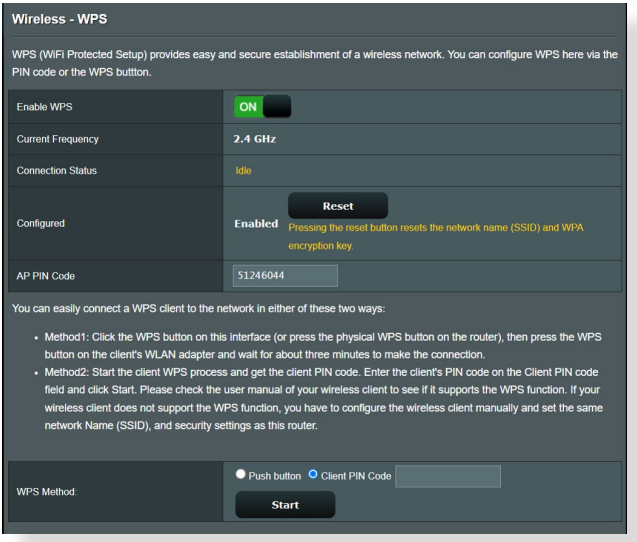


3.12 لاسلكي

3.12.1 WPS

WPS (إعداد Wi-Fi المحمي) هو معيار أمان لاسلكي يسمح لك بالاتصال بسهولة بالأجهزة اللاسلكية. يمكنك تكوين وظيفة WPS هنا باستخدام طريقة رمز التعريف الشخصي أو زر WPS.

ملاحظة: تأكد من أن الأجهزة تدعم WPS.



لتمكين WPS على الشبكة اللاسلكية الخاصة بك:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Wireless (لاسلكي)** > **WPS**.
2. في حقل **Enable WPS (تمكين WPS)**، حرك شريط التمرير إلى وضع **ON (تشغيل)**.
3. يستخدم WPS افتراضيًا نطاق 2.4 جيجا هرتز. إذا أردت تغيير التردد إلى 5 جيجاهرتز، فقم **OFF (بإيقاف)** وظيفة WPS، وانقر فوق **Switch Frequency (تبديل التردد)** في حقل **Current Frequency (التردد الحالي)**، وقم **ON (تشغيل)** وظيفة WPS مرة أخرى.

ملاحظة: يدعم WPS المصادقة باستخدام النظام المفتوح ونظام WPA-الشخصي، ونظام -WPA2الشخصي. لا يدعم WPS الشبكة اللاسلكية التي تستخدم مفتاح مشترك ونظام WPA-للمؤسسة، ونظام -WPA2للمؤسسة، وطريقة تشفير RADIUS.

4. في حقل WPS Method (طريقة)، حدد **Push Button (زر ضغط)** أو **Client PIN Code (رمز التعريف الشخصي للعميل)**. إذا حددت **Push Button (زر ضغط)**، انتقل إلى الخطوة 5. إذا حددت **Client PIN Code (رمز التعريف الشخصي للعميل)**، انتقل إلى الخطوة 6.
5. لإعداد WPS باستخدام زر WPS، اتبع هذه الخطوات:

a. اضغط فوق **Start (ابدأ)** أو اضغط على زر WPS الموجود في مؤخرة جهاز التوجيه اللاسلكي.

b. اضغط زر WPS على جهاز التوجيه الخاص بك. في العادة يتم التعرف على الزر من خلال شعار WPS.

ملاحظة: افحص جهازك اللاسلكي أو دليل المستخدم الخاص به لمعرفة موقع زر WPS.

c. سوف يقوم جهاز التوجيه اللاسلكي بالبحث عن أي أجهزة WPS متوفرة. إذا لم يعثر جهاز التوجيه اللاسلكي على أي أجهزة WPS، فسوف يتم التبديل إلى وضع الاستعداد.

6. لإعداد WPS باستخدام رمز التعريف الشخصي للعميل، اتبع هذه الخطوات:

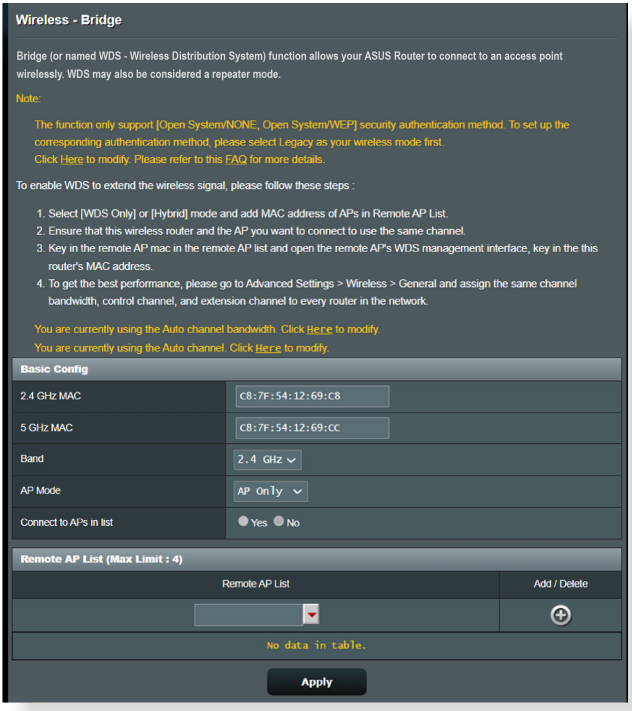
a. حدد موقع رمز التعريف الشخصي لـ WPS في دليل مستخدم الجهاز اللاسلكي الخاص بك أو على الجهاز نفسه.

b. اكتب رمز التعريف الشخصي للعميل في مربع النص.

c. انقر فوق **Start (ابدأ)** لوضع جهاز التوجيه اللاسلكي الخاص بك في وضع استقصاء WPS. تومض مؤشرات LED على جهاز التوجيه بسرعة ثلاث مرات حتى يكتمل إعداد WPS.

3.12.2 الجسر

يسمح الجسر أو WDS (نظام التوزيع اللاسلكي) لجهاز التوجيه اللاسلكي من ASUS الخاص بك بالاتصال بنقطة وصول لاسلكية أخرى بشكل حصري، لمنع الأجهزة أو المحطات اللاسلكية الأخرى من الوصول إلى جهاز التوجيه اللاسلكي ASUS الخاص بك. ويمكن أيضًا اعتباره جهاز تكرار لاسلكيًا حيث يتواصل جهاز التوجيه اللاسلكي الخاص بك من ASUS مع نقطة وصول أخرى وأجهزة لاسلكية أخرى.



لإعداد جسر لاسلكي:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة) > Wireless (لاسلكي) > WDS**.
2. حدد نطاق التردد للجسر اللاسلكي.
3. في حقل **AP Mode (وضع نقطة الوصول)**، حدد أي من هذه الخيارات:
   - **AP Only (نقطة صول فقط):** يعطل وظيفة الجسر اللاسلكي.
   - **WDS Only (WDS فقط):** يتيح ميزة الجسر اللاسلكي ولكن يمنع الأجهزة/المحطات اللاسلكية من الاتصال بجهاز التوجيه.

- **HYBRID (هجين):** يتيح ميزة الجسر اللاسلكي ويسمح للأجهزة/المحطات اللاسلكية الأخرى بالاتصال بجهاز التوجيه.

ملاحظة: في وضع الهجين، تستلم الأجهزة اللاسلكية المتصلة بجهاز التوجيه اللاسلكي من ASUS فقط نصف سرعة الاتصال الخاصة بنقطة الوصول.

4. في حقل **Connect to APs in list (الاتصال بنقاط الوصول في القائمة)**، انقر فوق **Yes (نعم)** إذا كنت تريد الاتصال بنقطة وصول مدرجة في قائمة نقاط الوصول البعيدة.
5. في حقل **Control Channel (قناة التحكم)**، حدد قناة التشغيل للجسر اللاسلكي. حدد **Auto (تلقائي)** للسماح لجهاز التوجيه بتحديد القناة تلقائيًا بأقل مقدار من التداخل.

ملاحظة: يختلف توفر القناة حسب الدولة أو المنطقة.

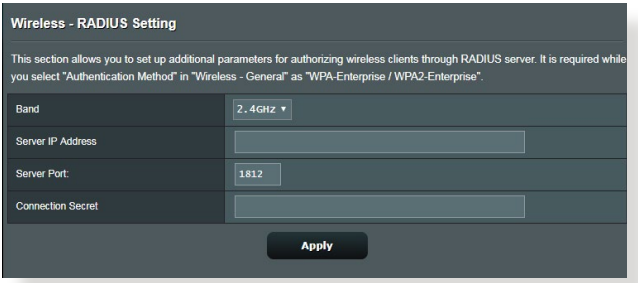
6. في **Remote AP List (قائمة نقاط الوصول البعيدة)**، اكتب عنوان MAC وانقر فوق زر **Add (إضافة)** ⊕ لإدخال عنوان MAC لنقاط الوصول الأخرى المتوفرة.

ملاحظة: أي نقطة وصول مضافة إلى القائمة يجب أن تكون على نفس قناة التحكم مثل جهاز التوجيه اللاسلكي من ASUS.

7. انقر فوق **Apply (تطبيق)**.

3.12.3 إعداد RADIUS

يوفر إعداد RADIUS (خدمة مصادقة عن بعد لمستخدم طلب هاتفي) طبقة إضافية من الأمان عندما تختار نظام WPA-للمؤسسة أو نظام WPA2-للمؤسسة أو Radius مع 802.1x باعتباره وضع المصادقة الخاص بك.



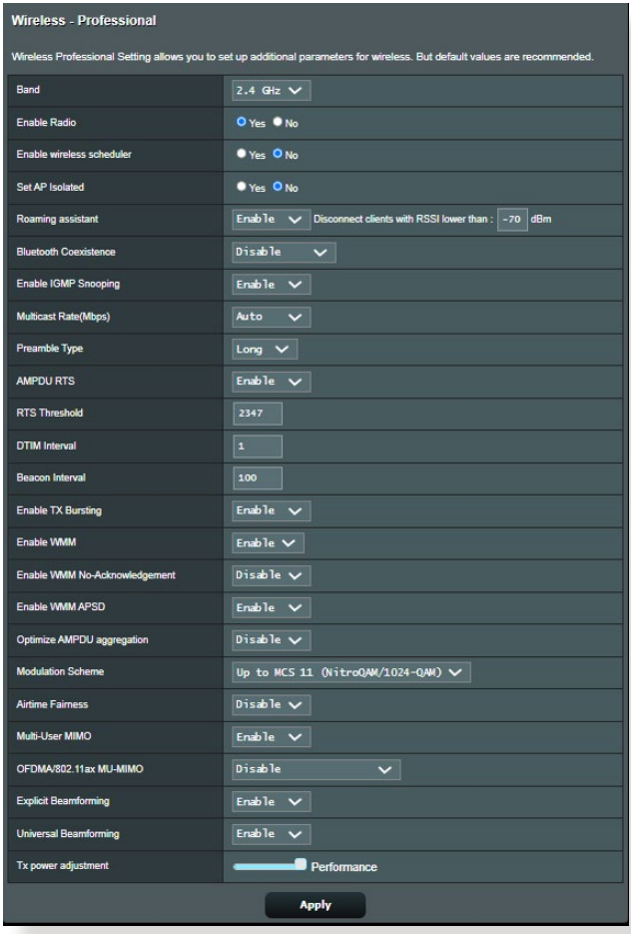
لإعداد إعدادات RADIUS اللاسلكية:

1. تأكد من أنه تم تعيين وضع المصادقة لجهاز التوجيه اللاسلكي على WPA-للمؤسسة أو WPA2-للمؤسسة أو Radius مع 802.1x.
2. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة)** > **Wireless (لاسلكي)** > **RADIUS Setting (إعداد RADIUS)**.
3. حدد نقاط التردد.
4. في حقل **Server IP Address (عنوان IP للخادم)**، اكتب عنوان IP لخادم RADIUS.
5. في حقل **Connection Secret (كلمة سر الاتصال)**، قم بتعيين كلمة المرور للوصول إلى خادم RADIUS.
6. انقر فوق **Apply (تطبيق)**.

3.12.4 احترافي

توفر شاشة Professional (احترافي) خيارات تكوين متقدمة.

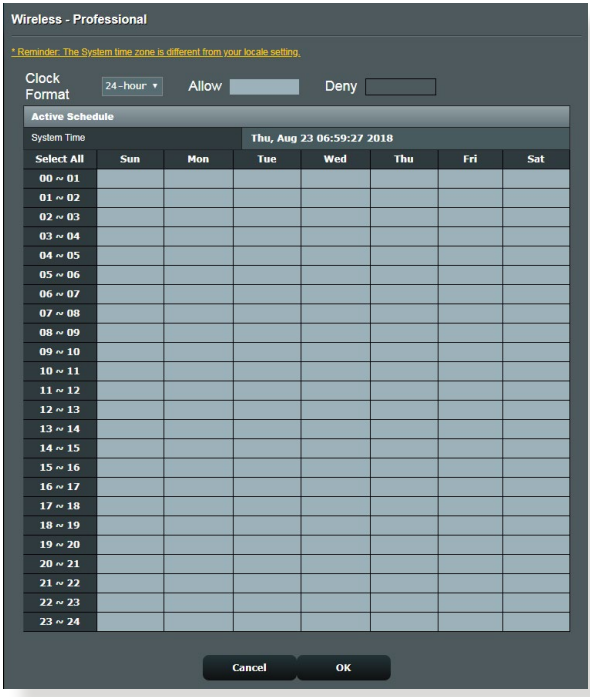
ملاحظة: نوصي بأن تستخدم القيمة الافتراضية بهذه الصفحة.



في شاشة الإعدادات **Professional (الاحترافية)**، يمكنك تكوين ما يلي:

- **Band (فرقة):** حدد نطاق التردد الذي يتم تطبيق الإعدادات الاحترافية عليه.
- **Enable Radio (تمكين الراديو):** حدد **Yes (نعم)** لتمكين الشبكات اللاسلكية. حدد **No (لا)** لتعطيل الشبكات اللاسلكية.

- **Enable wireless scheduler (تمكين المجدول اللاسلكي):** يمكنك اختيار تنسيق الساعة إما 24-ساعة أو 12-ساعة. يشير اللون في الجدول إلى Allow (سماح) أو Deny (رفض). انقر فوق كل إطار لتغيير إعدادات الساعة لأيام الأسبوع وانقر فوق **OK (موافق)** عند الانتهاء.



- **Set AP isolated (تعيين نقطة وصول معزولة):** تمنع عناصر تعيين نقطة الوصول المعزولة الأجهزة اللاسلكية على الشبكة من التواصل مع بعضها البعض. تعتبر هذه الميزة مفيدة في حالة وجود عدة أجهزة ضيوف ينضمون إلى شبكتك أو يغادرونها بصورة متكررة. حدد **Yes (نعم)** لتمكين هذه الميزة أو حدد **No (لا)** لتعطيلها.
- **Multicast rate (Mbps) (معدل الإرسال المتعدد):** حدد معدل الإرسال المتعدد أو انقر فوق **Disable (تعطيل)** لإيقاف تشغيل إرسال الإشارة الآني.
- **Preamble Type (نوع المقدمة):** يحدد Preamble Type (نوع المقدمة) طول الفترة الزمنية التي يقضيها جهاز التوجيه لأجل اختبار التكرار الدوري (CRC). يمثل CRC طريقة لاكتشاف الأخطاء أثناء إرسال البيانات. حدد **Short (قصير)** مع الشبكة اللاسلكية المشغولة التي تتضمن حركة بيانات عالية. حدد **Long (طويل)** إذا كانت الشبكة اللاسلكية تتألف من أجهزة لاسلكية قديمة أو عتيقة.

- **RTS Threshold (حد طلب الإرسال):** حدد قيمة أقل لحد RTS (طلب الإرسال) لتحسين الاتصال اللاسلكي في الشبكة اللاسلكية المشغولة أو المزدحمة التي تتضمن حركة بيانات عالية عبر الشبكة والعديد من الأجهزة اللاسلكية.
- **DTIM Interval (فاصل رسالة الإشارة إلى حركة المرور والتسليم):** يمثل فاصل DTIM (رسالة الإشارة إلى حركة المرور والتسليم) أو معدل إشارة البيانات الفاصل الزمني قبل إرسال إشارة إلى جهاز لاسلكي في وضع السكون والذي يشير إلى أن حزمة البيانات في انتظار التسليم. القيمة الافتراضية هي ثلاثة ميللي ثانية.
- **Beacon Interval (فاصل الإشارة):** يشير فاصل الإشارة إلى الفترة الزمنية بين إشارة DTIM والإشارة التي تليها. القيمة الافتراضية هي 100 ميللي ثانية. قم بخفض قيمة فاصل الإشارة مع الاتصال اللاسلكي غير المستقر أو مع أجهزة التجوال.
- **Enable TX Bursting (تمكين فصل TX):** يعمل تمكين فصل TX على تحسين سرعة النقل بين جهاز التوجيه اللاسلكي وأجهزة 802.11g.
- **Enable WMM APSD (تمكين إيصال حفظ الطاقة التلقائي للوسائط المتعددة اللاسلكية):** قم بتمكين WMM APSD (إيصال حفظ الطاقة التلقائي للوسائط المتعددة اللاسلكية) لتحسين إدارة الطاقة بين الأجهزة اللاسلكية. حدد **Disable (تعطيل)** لإيقاف تشغيل WMM APSD.

4 الأدوات المساعدة

4.1 استكشاف الجهاز

أداة Device Discovery (استكشاف الجهاز) هي أداة مساعدة لشبكة WLAN من ASUS تكتشف جهاز توجيه ASUS اللاسلكي من ASUS، وتسمح لك بتكوين إعدادات الشبكة اللاسلكية.

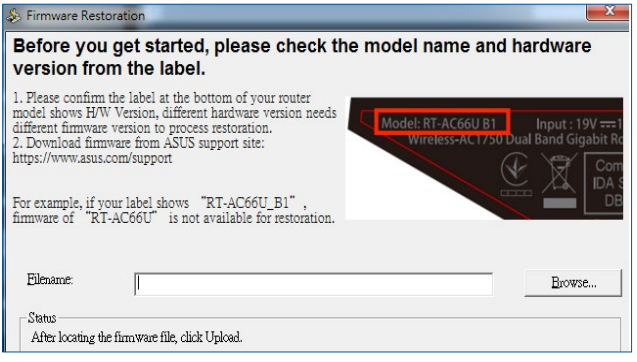
لتشغيل أداة Device Discovery (اكتشاف الجهاز) المساعدة:

- من سطح المكتب على جهاز الكمبيوتر، انقر فوق **Start (ابدأ) > All Programs (كافة البرامج) > ASUS Utility (أداة ASUS المساعدة) > ASUS Wireless Router (ASUS جهاز التوجيه اللاسلكي) > Device Discovery (استكشاف الجهاز).**

ملاحظة: عندما تقوم بتعيين جهاز التوجيه إلى وضع نقطة وصول، عندئذ يلزمك استخدام Device Discovery (استكشاف الجهاز) للحصول على عنوان IP لجهاز التوجيه.

4.2 استعادة البرنامج الثابت

تستخدم أداة Firmware Restoration (استعادة البرنامج الثابت) على جهاز التوجيه من ASUS الذي فشل أثناء عملية تحديث البرنامج الثابت الخاصة به. وهي تقوم بتحميل البرنامج الثابت الذي تحدده. وتستغرق العملية حوالي ثلاث إلى أربع دقائق.



هام! قم بتشغيل وضع الإنقاذ على جهاز التوجيه قبل استخدام أداة استعادة البرنامج الثابت.

ملاحظة: لا يتم دعم هذه الميزة على أنظمة MAC OS.

لتشغيل وضع الإنقاذ واستخدام أداة استعادة البرنامج الثابت:

1. افصل جهاز توجيه اللاسلكي عن مصدر الطاقة.
2. اضغط مع الاستمرار على زر Reset (إعادة ضبط) على اللوحة الخلفية وقم في نفس الوقت بإعادة توصيل جهاز توجيه اللاسلكي بمصدر الطاقة. اترك زر Reset (إعادة ضبط) عندما يومض مؤشر الطاقة LED الموجود على اللوحة الأمامية ببطئ، والذي يدل على أن جهاز توجيه اللاسلكي في وضع الإنقاذ.
3. قم بتعيين عنوان IP ثابت على الكمبيوتر الخاص بك واستخدم ما يلي لإعداد إعدادات TCP/IP:

   IP address (عنوان IP): 192.168.1.x

   Subnet mask (قناع الشبكة الفرعية): 255.255.255.0

4. من سطح المكتب على جهاز الكمبيوتر، انقر فوق**Start (ابدأ) > All Programs (كافة البرامج) > ASUS Utility (أداة ASUS المساعدة) > Wireless Router (جهاز التوجيه اللاسلكي) > Firmware Restoration (تحديث البرنامج الثابت)**.
5. حدد ملف برنامج ثابت، ثم انقر على **Upload (تحميل)**.

ملاحظة: هذه ليست أداة مساعدة لترقية البرنامج الثابت ولا يمكن استخدامها على جهاز التوجيه اللاسلكي من ASUS أثناء عمله. يجب أن يتم إجراء عمليات تحديث البرنامج الثابت العادية من خلال واجهة الويب. راجع **الفصل 3: تكوين الإعدادات العامة و المتقدمة** لمزيد من التفاصيل.

---

5 استكشاف الأخطاء وإصلاحها

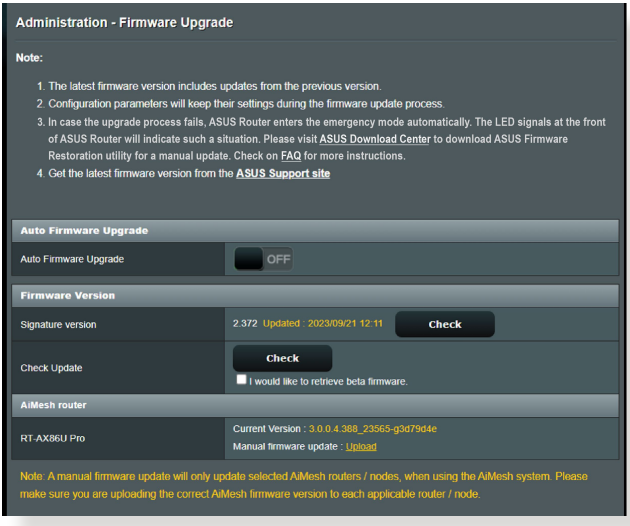
يوفر هذا الفصل الحلول للمشكلات التي قد تصادفها مع جهاز التوجيه. إذا صادفت مشكلات ليست مذكورة في هذا الفصل، فيرجى زيارة موقع دعم ASUS على العنوان: https://www.asus.com/support للحصول على مزيد من المعلومات حول المنتج وتفاصيل الاتصال بالدعم الفني لـ ASUS.

5.1 استكشاف الأخطاء وإصلاحها الأساسي

إذا كان لديك مشكلات في جهاز التوجيه، فجرب هذه الخطوات الأساسية في هذا القسم قبل البحث عن حلول أخرى.

ترقية البرنامج الثابت إلى أحدث إصدار.

1. ابدأ تشغيل واجهة المستخدم العمومية على الويب (Web GUI). انتقل إلى **Advanced Settings (الإعدادات المتقدمة) > Administration (الإدارة) > Firmware Upgrade (ترقية البرنامج الثابت)**. انقر فوق **Check (فحص)** للتحقق من أحدث برنامج ثابت متوفر.



2. في حالة توفر أحدث برنامج ثابت، فقم بزيارة موقع ويب ASUS العالمي على العنوان https://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/ لتنزيل أحدث برنامج ثابت.
3. من صفحة **Firmware Version (إصدار البرنامج الثابت)**، انقر فوق **Check (فحص)** لتحديد مكان ملف البرنامج الثابت.
4. انقر فوق **Upload (تحميل)** لترقية البرنامج الثابت.

أعد بدء الشبكة الخاصة بك باتباع التسلسل التالي:

1. أوقف تشغيل المودم.
2. افصل قابس المودم.
3. أوقف تشغيل جهاز التوجيه وأجهزة الكمبيوتر.
4. قم بتوصيل المودم.
5. شغل المودم ثم انتظر لمدة دقيقتين.
6. شغل جهاز التوجيه ثم انتظر لمدة دقيقتين.
7. شغل أجهزة الكمبيوتر.

تحقق من أن الإعداد اللاسلكي على الكمبيوتر الخاص بك يطابق ذلك الخاص بجهاز التوجيه.

- عندما تقوم بتوصيل الكمبيوتر الخاص بك جهاز توجيه لاسلكيًا، تأكد من أن SSID (اسم الشبكة اللاسلكية)، وطريقة التشفير وكلمة المرور صحيحة.

تحقق مما إذا كانت إعدادات الشبكة الخاصة بك صحيحة أم لا.

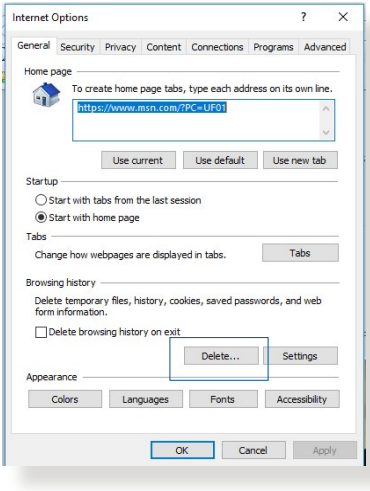
- يجب أن يكون لكل عميل على الشبكة عنوان IP صالح. توصي ASUS بأن تستخدم خادم DHCP بجهاز التوجيه اللاسلكي لتعيين عناوين IP إلى أجهزة الكمبيوتر على الشبكة.

- يتطلب بعض مزودي خدمة مودم االكابل استخدام عنوان MAC للكمبيوتر المسجل أوليًا في الحساب. يمكنك عرض عنوان MAC في واجهة المستخدم العمومية على الويب web GUI، **Network Map (خريطة الشبكة)** > صفحة **Clients (العملاء)**، وحلق بمؤشر الماوس فوق جهازك في **Client status (حالة العميل)**.

5.2 أسئلة شائعة (FAQs)

لا يمكنني الوصول إلى واجهة المستخدم العمومية (GUI) لجهاز التوجيه باستخدام مستعرض ويب

- إذا كان جهاز الكمبيوتر الخاص بك متصلاً بسلك، فافحص اتصال كابل إيثرنت وحالة LED كما هو موضح في القسم السابق.
- تحقق من استخدام معلومات تسجيل الدخول الصحيحة. تأكد من أن مفتاح Caps Lock معطل عند إدخال معلومات تسجيل الدخول.
- احذف ملفات تعريف الارتباط والملفات في مستعرض الويب الخاص بك. في برنامج Internet Explorer، اتبع الخطوات الآتية:



1. شغّل Internet Explorer، ثم انقر على **Tools (أدوات)** > **Internet Options (خيارات الإنترنت)**.
2. في علامة تبويب **General (عام)**، تحت **Browsing history (تاريخ التصفح)**، انقر فوق **Delete... (حذف...)**، حدد **Temporary Internet files and website files (ملفات الإنترنت المؤقتة وملفات موقع الويب)** و **Cookies and website data (ملفات تعريف الارتباط وبيانات موقع الويب)** ثم انقر فوق **Delete (حذف)**.

ملاحظات:

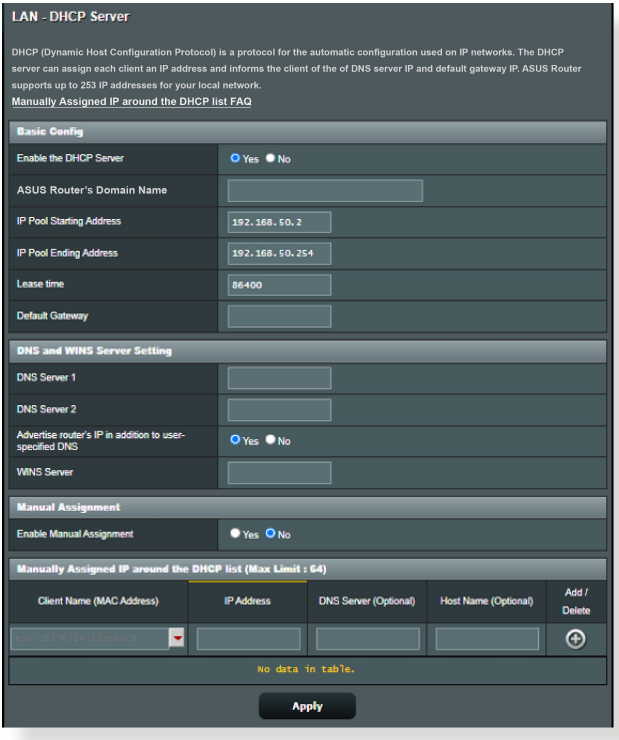
- تختلف أوامر حذف ملفات تعريف الارتباط والملفات حسب مستعرضات الويب.
- قم بتعطيل إعدادات الخادم الوكيل، وإلغاء اتصال الطلب الهاتفي، وقم بتعيين إعدادات TCP/IP للحصول على عناوين IP تلقائيًا. لمزيد من التفاصيل، راجع الفصل 1 من دليل المستخدم هذا.
- تأكد من استخدام كابلات إيثرنت CAT5e أو CAT6.

العميل غير قادر على إنشاء اتصال لاسلكي باستخدام جهاز التوجيه.

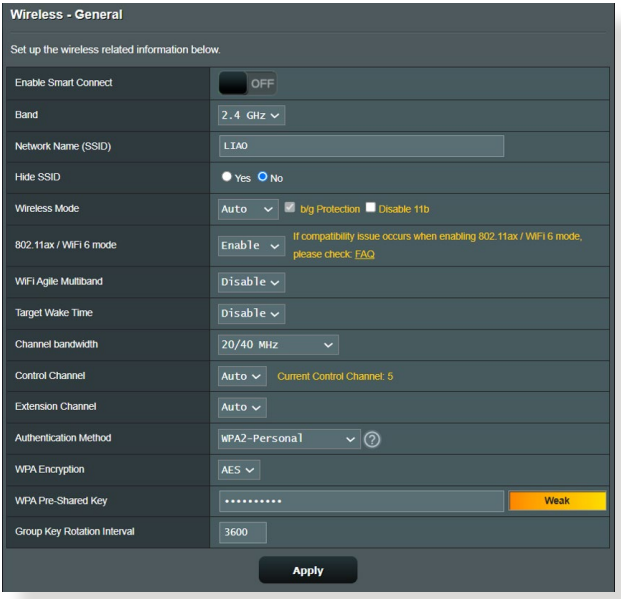
ملاحظة: إذا كنت تصادف مشكلات في الاتصال بشبكة 5 جيجاهرتز ، تأكد من أن الجهاز اللاسلكي الخاص بك يدعم 5 جيجاهرتز أو يتضمن إمكانات النطاق المزدوج.

- **خارج النطاق:**
  - قرّب جهاز التوجيه إلى عميل الشبكة اللاسلكية.
- **تم تعطيل خادم DHCP:**

1. ابدأ تشغيل واجهة المستخدم العمومية على الويب (Web GUI). انتقل إلى **General (عام) > Network Map (خريطة الشبكة) > Clients (العملاء)** وابحث عن الجهاز الذي تريد توصيله بجهاز التوجيه.
2. إذا تعذر عليك العثور على جهاز في **Network Map (خريطة الشبكة)**، انتقل إلى **Advanced Settings (الإعدادات المتقدمة) > LAN (شبكة الاتصال المحلية) > DHCP Server (خادم DHCP)**، قائمة **Basic Config (التكوين الأساسي)**، وحدد **Yes (نعم)** في **Enable the DHCP Server (تمكين خادم DHCP)**.

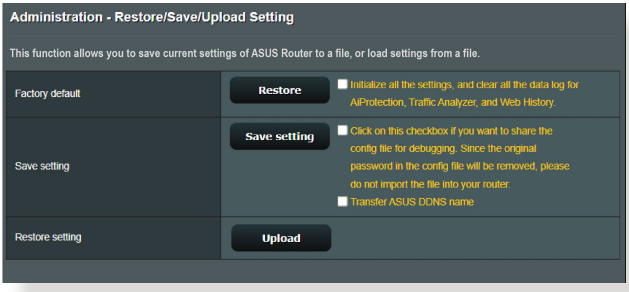


- تم إخفاء SSID. إذا جهازك يستطيع العثور على معرفات SSID من أجهزة التوجيه الأخرى ولكنه لا يمكنه العثور على معرف SSID لجهاز التوجيه الخاص بك، فانتقل إلى **Advanced Settings (الإعدادات المتقدمة) > Wireless (لاسلكي) > General (عام)**، حدد **No (لا)** على **Hide SSID (إخفاء SSID)**، وحدد **Auto (تلقائي)** في **Control Channel (قناة التحكم)**.



- إذ كنت تستخدم مهايئ LAN لاسلكي، فتحقق من أن القناة اللاسلكية المستخدمة تتوافق مع القنوات المتوفرة في بلدك/منطقتك. إذا لم تكن متوافقة، فاضبط القناة، وعرض نطاق القناة والوضع اللاسلكي.

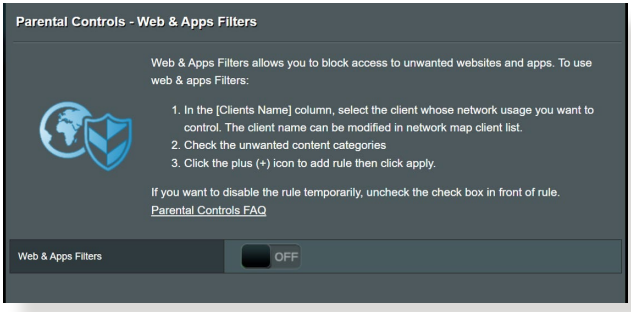
- إذا كنت ما تزال غير قادر على الاتصال بجهاز التوجيه اللاسلكي، فيمكنك إعادة ضبط جهاز التوجيه على الإعدادات الافتراضية من المصنع. في واجهة المستخدم العمومية لجهاز التوجيه، انقر فوق **Administration (الإدارة) > Restore/ Save/Upload Setting (استعادة/حفظ/تحميل الإعداد)** وانقر فوق **Restore (استعادة)**.



لا يمكن الدخول إلى الإنترنت.

- تحقق مما إذا كان جهاز التوجيه لديك يمكنه الاتصال بعنوان WAN IP لمزود خدمة الإنترنت. للقيام بذلك، قم بتشغيل واجهة المستخدم العمومية على الويب (web GUI) وانتقل إلى **General (عام)** > **Network Map (خريطة الشبكة)**، وافحص **Internet status (حالة الإنترنت)**.
- إذا كان جهاز التوجيه لا يمكنه الاتصال بعنوان WAN IP لمزود خدمة الإنترنت، جرب إعادة بدء الشبكة الخاصة بك كما هو موضح في القسم **أعد تشغيل الشبكة في التسلسل التالي** تحت **استكشاف الأخطاء وإصلاحها الأساسي**.

- تم حظر الجهاز عن طريق وظيفة التحكم الأبوي. انتقل إلى **General (عام)** > **Parental Controls (التحكم الأبوي)** وتحقق مما إذا كان الجهاز مدرجًا في القائمة أم لا. إذا كان الجهاز مدرجًا تحت **Client Name (اسم العميل)**، أزل الجهاز باستخدام زر **Delete (أزل)** أو اضبط Time Management Settings (إعدادات إدارة الوقت).



- إذا لم يكن هناك اتصال بالإنترنت، فجرب إعادة تمهيد الكمبيوتر وتحقق من عنوان IP للشبكة وعنوان البوابة.

نسيت معرف SSID (اسم الشبكة) أو كلمة مرور الشبكة.

- قم بإعداد معرف SSID جديد ومفتاح تشفير عن طريق الاتصال السلكي (كابل إيثرنت). ابدأ تشغيل واجهة المستخدم العمومية على الويب (Web GUI)، وانتقل إلى **Network Map (خريطة الشبكة)**، وانقر فوق رمز جهاز التوجيه، وأدخل معرف SSID جديد ومفتاح التشفير، ثم انقر فوق **Apply (تطبيق)**.
- أعد ضبط جهاز التوجيه على الإعدادات الافتراضية. شغل واجهة المستخدم العمومية على الويب (web GUI)، انتقل إلى **Administration (الإدارة) > Restore/Save/Upload Setting (استعادة/حفظ/تحميل الإعداد)** وانقر فوق **Restore (استعادة)**.

كيف تستعيد النظام إلى إعداداته الافتراضية؟

- انتقل إلى **Administration (الإدارة) > Restore/Save/Upload Setting (استعادة/حفظ/تحميل الإعداد)** وانقر فوق **Restore (استعادة)**.

فشل تحديث البرنامج الثابت.

قم بتشغيل وضع الإنقاذ وتشغيل أداة Firmware Restoration (استعادة البرنامج الثابت). راجع القسم **4.2 استعادة البرنامج الثابت** لمعرفة كيفية استخدام أداة Firmware Restoration (استعادة البرنامج الثابت).

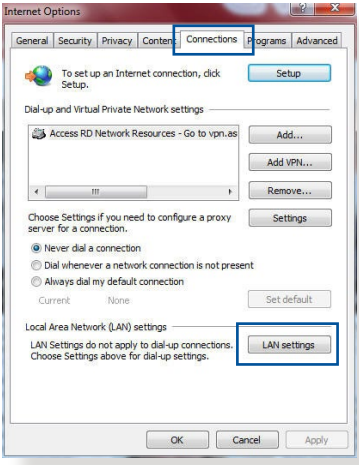
لا يمكن الوصول إلى واجهة المستخدم العمومية على الويب (web GUI)

قبل تكوين جهاز التوجيه اللاسلكي، نفذ الخطوات الموضحة في هذا القسم للكمبيوتر المضيف وعملاء الشبكة.

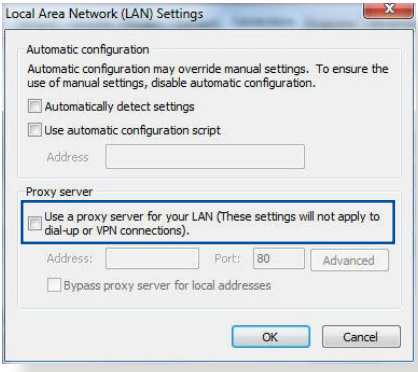
A. تعطيل الخادم الوكيل، في حالة تمكينه.

Windows®

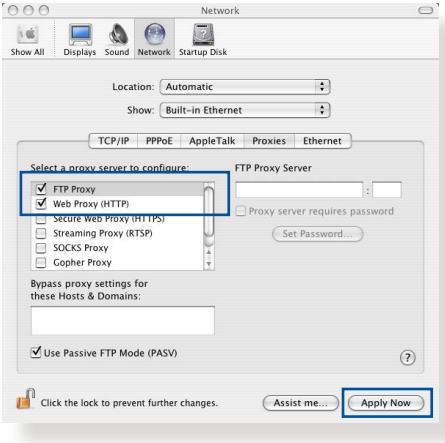
1. انقر فوق **Start (ابدأ)** > **Internet Explorer** لبدء تشغيل مستعرض الويب.
2. انقر فوق **Tools (الأدوات)** > **Internet options (خيارات الإنترنت)** > **Connections (الاتصالات)** > **LAN settings (إعدادات LAN)**.



3. من شاشة إعدادات شبكة الاتصال المحلية (LAN)، قم بإلغاء اختيار **Use a proxy server for your LAN (استخدام خادم وكيل لشبكة LAN الخاصة بك)**.
4. انقر فوق **OK (موافق)** عند الانتهاء.



MAC OS



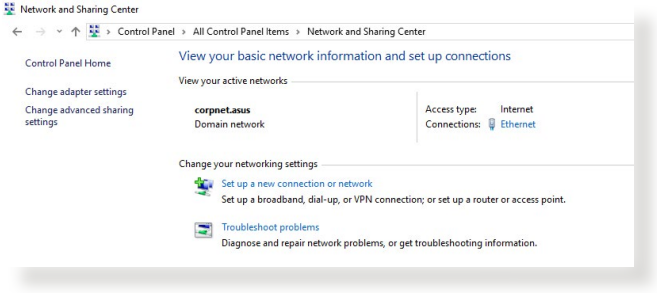
1. من مستعرض Safari، انقر فوق **Safari > Preferences (التفضيلات) > Advanced (متقدم) > Change Settings (تغيير الإعدادات)...**
2. من شاشة الشبكة، قم بإلغاء تحديد **FTP Proxy (وكيل FTP)** و **Web Proxy (وكيل الويب) (HTTP)**.
3. انقر فوق **Apply Now (تطبيق الآن)** عند الانتهاء.

ملاحظة: راجع ميزة المساعدة في المستعرض لمعرفة التفاصيل حول تعطيل الخادم الوكيل.

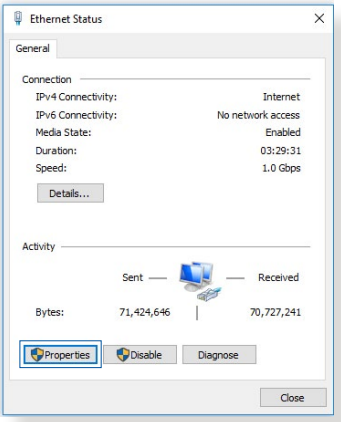
B. تعيين إعدادات TCP/IP للحصول على عنوان IP تلقائيًا

Windows®

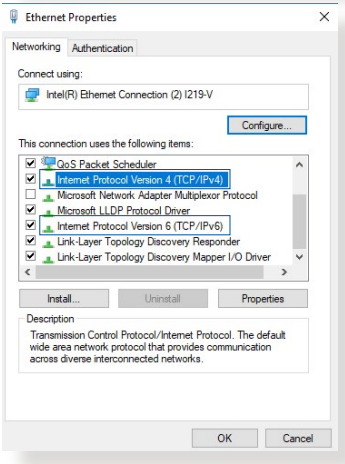
1. انقر فوق **Start (ابدأ) > Control Panel (لوحة التحكم) > Network and Sharing Center (مركز الشبكة والمشاركة)**، ثم انقر فوق اتصال الشبكة لعرض نافذة الحالة الخاصة به.



2. انقر فوق **Properties (خصائص)** لعرض نافذة Ethernet Properties (خصائص الإيثرنت).

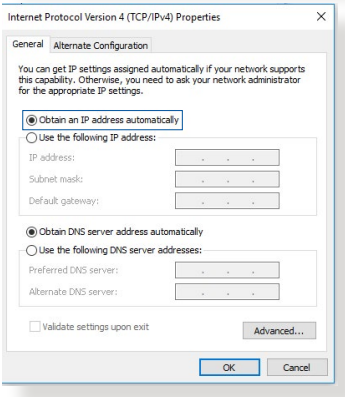


3. حدد **بروتوكول الإنترنت الإصدار 4 (TCP/IPv4)** أو **بروتوكول الإنترنت الإصدار 6 (TCP/IPv6)**، ثم انقر فوق **Properties (الخواص)**.



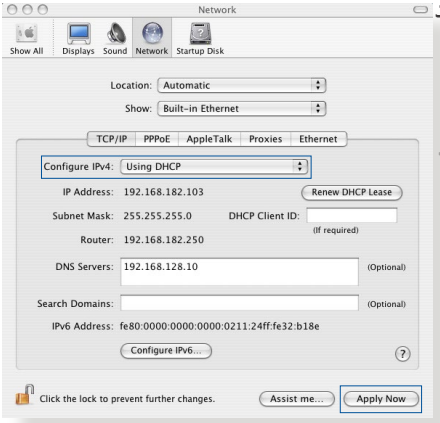
4. للحصول على إعدادات IPv4 IP تلقائيًا، اختر **Obtain an IP address automatically (الحصول على عنوان IP تلقائيًا)**.

   للحصول على إعدادات IPv6 IP تلقائيًا، اختر **Obtain an IPv6 address automatically (الحصول على عنوان IPv6 تلقائيًا)**.



5. انقر فوق **OK (موافق)** عند الانتهاء.

MAC OS

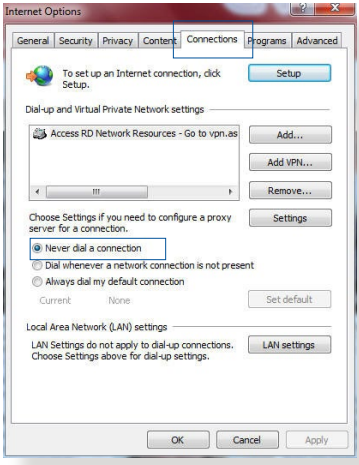


1. انقر فوق رمز Apple الموجود في القسم العلوي الأيسر للشاشة.
2. انقر فوق **System Preferences (تفضيلات النظام)** > **Network (الشبكة)** > **Configure (تكوين)...**
3. من علامة تبويب **TCP/IP**، حدد **Using DHCP (استخدام DHCP)** في القائمة المنسدلة **Configure IPv4 (تكوين IPv4)**.
4. انقر فوق **Apply Now (تطبيق الآن)** عند الانتهاء.

ملاحظة: راجع تعليمات نظام التشغيل وميزة الدعم لمعرفة تفاصيل حول تكوين إعدادات TCP/IP لجهاز الكمبيوتر الخاص بك.

C. تعطيل اتصال الطلب الهاتفي، في حالة تمكينه.

Windows®



1. انقر فوق **Start (ابدأ)** > **Internet Explorer** لبدء تشغيل المستعرض.
2. انقر فوق **Tools (الأدوات)** > **Internet options (خيارات الإنترنت)** > **Connections (الاتصالات)**.
3. اختر **Never dial a connection (عدم إجراء اتصال هاتفي مطلقًا)**.
4. انقر فوق **OK (موافق)** عند الانتهاء.

ملاحظة: راجع ميزة المساعدة في المستعرض لمعرفة التفاصيل حول تعطيل الاتصال الهاتفي.

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

ملاحظات السلامة

عند استخدام المنتج، اتبع دائمًا احتياطات السلامة الأساسية، بما فيها، على سبيل المثال لا الحصر، ما يلي:

تحذير!

- يجب توصيل سلك (أسلاك) مصدر الإمداد بالطاقة بمأخذ (مآخذ) المقبس المزود بأرضية مناسبة. وصل الجهاز لمقبس كهربي قرب فقط يسهل الوصول إليه.
- في حالة إنكسار المهايئ, لا تحاول إصلاحه بنفسك. اتصل بفني صيانة مؤهل أو ببائع التجزئة لديك.
- يجب عدم استخدام أسلاك الطاقة أو الملحقات أو الوحدات الطرفية الأخرى التالفة.
- لا تركب هذا الجهاز على مسافة أعلى من 2 متر.
- استخدم هذا المنتج في البيئات التي تتراوح درجات الحرارة المنتشرة بها بين 0 درجة مئوية (32 فهرنهايت) و40 درجة مئوية (104 فهرنهايت).
- اقرأ إرشادات التشغيل ومعدل درجة الحرارة المقدم قبل استخدام المنتج.
- انتبه بشكل خاص للسلامة الشخصية عند استخدام المنتج في المطارات، المستشفيات، محطات الغاز، والمرائب الاحترافية.
- التداخل الطبي للجهاز: حافظ على مسافة لا تقل عن 15 سم (6 بوصات) بين أجهزة الزرع الطبية ومنتجات ASUS لتقليل خطر التداخل.
- يرجى استخدام منتجات ASUS في ظروف استقبال جيدة لتقليل مستوى الإشعاع.
- إبق الجهاز بعيدًا عن أي أمرأة حامل وعن الجزء السفلي من بطن المراهقين.
- لا تستخدم هذا المنتج في حالة ملاحظة أي عيوب مرئية أو في حالة تعرضه للبلل أو التلف أو التعديل. ابحث عن الصيانة من أجل المساعدة.

تحذير!

- يجب عدم وضع الجهاز على أسطح عمل غير مستوية أو غير مستقرة.
- لا تضع أو تسقط أجسامًا على الجزء العلوي من المنتج. تجنب تعريض المنتج لصدمة ميكانيكية مثل: الكسر أو الثني أو الثقب أو التمزيق.
- لا تفك هذا المنتج أو تفتحه أو تضعه في الميكروويف أو تحرقه أو تدهنه أو تدفع أي أجسام غريبة داخله.
- ارجع إلى ملصق التصنيف الموجود على الجزء السفلي من المنتج وتأكد من أن مهايئ الطاقة متوافق مع هذا التصنيف.
- إبقِ المنتج بعيدًا عن النار ومصادر الحرارة.
- يجب عدم تعرض الجهاز للسوائل أو الأمطار أو الرطوبة. يجب عدم استخدام المنتج أثناء العواصف الكهربية.
- وصل دوائر خرج PoE الخاصة بهذا المنتج بشبكات PoE بشكل حصري بدون التوجيه إلى منشآت خارجية.
- لمنع خطر حدوث صدمة كهربية؛ افصل كبل الطاقة من مأخذ التيار الكهربي قبل تغيير مكان النظام.
- لا تستخدم سوى الملحقات المرفقة من قبل الجهة المصنعة للجهاز للعمل مع هذا الطراز. يبطل استخدام أنواع أخرى من الملحقات الضمان أو يخرق اللوائح والقوانين المحلية، وقد يعرض سلامتك للمخاطر. اتصل ببائع التجزئة المحلي لمعرفة مدى توفر الملحقات المرخصة.
- استخدام هذا المنتج بطريقة غير الموصى بها في التعليمات المقدمة قد يؤدي لخطر نشوب حريق أو إصابة شخصية.

الخدمة والدعم

زر موقع الويب المتعدد اللغات خاصتنا على https://www.asus.com/support/.