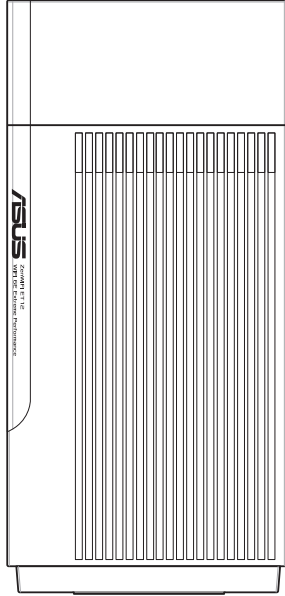


# دليل المستخدم

## ZenWiFi Pro ET12

جهاز توجيه لاسلكي نطاق ثلاثي AXE11000



**ASUS**  
IN SEARCH OF INCREDIBLE

ARB22785

الإصدار الأول

يناير 2024

#### حقوق النشر © لعام 2024 لصالح شركة ASUSTeK COMPUTER INC. جميع الحقوق محفوظة.

لا تجوز إعادة إنتاج أي جزء من هذا الدليل، بما في ذلك المنتجات والبرامج الواردة ذكرها به، أو نقله أو نسخه أو تخزينه في نظام استعادة، أو ترجمته إلى أي لغة بأي شكل أو بأي وسيلة، باستثناء المستندات التي يتم الحصول عليها بواسطة المشتري لأغراض إنشاء نسخة احتياطية، دون الحصول على إذن كتابي صريح من شركة ASUSTeK COMPUTER INC. (المشار إليها باسم "ASUS").

لن يتم تمديد ضمان أو خدمة المنتج في حالة: (١) إصلاح المنتج، أو تعديله أو تغييره، ما لم يتم التصريح بإجراء هذا الإصلاح، أو التعديل أو التغيير كتابة من جانب شركة ASUS؛ أو (٢) تشوّه الرقم التسلسلي للمنتج أو فقده.

توفر ASUS هذا الدليل "كما هو" دون أي ضمان من أي نوع، صريحاً كان أم ضمنياً، ويشمل، لكنه لا يقتصر على، الضمانات الضمنية أو شروط القابلية للتسويق أو الملائمة لغرض معين. لا تتحمل شركة ASUS، أو مديرها، أو موظفها، أو مسؤولوها، أو وكلاؤها، بأي حال من الأحوال، المسؤولية تجاه أي تلف غير مباشر، أو خاص، أو عرضي أو لاحق (بما في ذلك التلف الناجم عن خسائر في الأرباح، أو الأعمال التجارية، أو خسارة الاستخدام أو البيانات، أو مقاطعة الأعمال التجارية وما شابه)، حتى في حالة نصيحة ASUS باحتمالية حدوث مثل هذا التلف الناجم عن أي عيب أو خطأ في هذا الدليل أو المنتج.

تم توفير المواصفات والمعلومات الواردة في هذا الدليل بغرض المعلومات فقط، وهي عرضة للتغيير في أي وقت دون إخطار، ولا يجب اعتبارها التزاماً من ناحية ASUS. ولا تتحمل ASUS أية مسؤولية أو مسؤولية قانونية تجاه أية أخطاء أو حالات عدم دقة قد تظهر في هذا الدليل، بما في ذلك المنتجات والبرامج الواردة فيه.

قد تكون المنتجات وأسماء الشركات الواردة في هذا الدليل أو لا تكون علامات تجارية أو حقوق نشر مسجلة لكل شركة على حده، ولا تستخدم إلا للتعريف أو للتفسير وتكون لصالح أصحابها، بدون وجود نية للانتهاك.

## جدول المحتويات

١	التعرف على جهاز التوجيه اللاسلكي	
1.1	مرحبًا! .....	6
1.2	محتويات العبوة .....	6
1.3	جهاز التوجيه اللاسلكي الخاص بك .....	7
1.4	ضبط موضع جهاز التوجيه اللاسلكي .....	9
1.5	متطلبات الإعداد .....	10
٢	البداء	
2.1	إعداد جهاز التوجيه .....	11
	A. الاتصال السلكي .....	11
	B. الاتصال اللاسلكي .....	12
2.2	إعداد الإنترنت السريع (QIS) مع الاكتشاف التلقائي .....	14
2.3	الاتصال بالشبكة اللاسلكية الخاصة بك .....	17
٣	تكوين الإعدادات العامة و المتقدمة	
3.1	تسجيل الدخول إلى واجهة المستخدم العمومية على الويب (Web GUI) .....	18
3.1.1	إعداد إعدادات الأمان اللاسلكية .....	20
3.1.2	إدارة عملاء الشبكة .....	21
3.2	جودة الخدمة التكيفية .....	22
3.2.1	إدارة عرض نطاق QoS (جودة الخدمة) .....	22
3.3	الإدارة .....	25
3.3.1	وضع التشغيل .....	25
3.3.2	النظام .....	26
3.3.3	ترقية البرنامج الثابت .....	27
3.3.4	استعادة/حفظ/تحميل الإعداد .....	27
3.4	AiCloud 2.0 .....	28
3.4.1	القرص السحابي .....	29
3.4.2	الوصول الذكي .....	30
3.4.3	مزامنة AiCloud .....	31

## جدول المحتويات

32	.....AiProtection	3.5
32	..... حماية الشبكة	3.5.1
36	..... إعداد التحكم الأبوي	3.5.2
39	..... جدار الحماية	3.6
39	..... عام	3.6.1
40	..... عامل تصفية URL	3.6.2
41	..... عامل تصفية الكلمات الأساسية	3.6.3
42	..... عامل تصفية خدمات الشبكة	3.6.4
44	..... شبكة ضيف	3.7
46	..... IPv6	3.8
47	..... شبكة الاتصال المحلية (LAN)	3.9
47	..... عنوان IP لشبكة الاتصال المحلية (LAN)	3.9.1
48	..... خادم DHCP	3.9.2
50	..... المسار	3.9.3
51	..... التلفزيون عبر الإنترنت (IPTV)	3.9.4
52	..... سجل النظام	3.10
53	..... محلل حركة البيانات	3.11
54	..... الشبكة واسعة النطاق (WAN)	3.12
54	..... اتصال الإنترنت	3.12.1
57	..... الشبكة واسعة النطاق الثنائية	3.12.2
58	..... مشغل المنافذ	3.12.3
60	..... الخادم الافتراضي/إعادة توجيه المنفذ	3.12.4
63	..... المنطقة المنزوعة (DMZ)	3.12.5
64	..... نظام أسماء النطاقات الديناميكي (DDNS)	3.12.6
65	..... اجتياز NAT	3.12.7
66	..... لاسلكي	3.13
66	..... عام	3.13.1
69	..... WPS	3.13.2
71	..... الجسر	3.13.3
73	..... عامل تصفية MAC للشبكة اللاسلكية	3.13.4

## جدول المحتويات

74.....	RADIUS إعداد	3.13.5
75.....	احترافي	3.13.6

### ٤ الأدوات المساعدة

78.....	استكشاف الجهاز	4.1
79.....	استعادة البرنامج الثابت	4.2
81.....	إعداد خادم الطابعة	4.3
81.....	مشاركة طابعة ASUS EZ	4.3.1
85.....	استخدام LPR لمشاركة الطابعة	4.3.2
90.....	مدير التنزيل	4.4
91.....	تكوين إعدادات تنزيل Bit Torrent	4.4.1
92.....	إعدادات NZB	4.4.2

### ٥ استكشاف الأخطاء وإصلاحها

93.....	استكشاف الأخطاء وإصلاحها الأساسي	5.1
96.....	أسئلة شائعة (FAQs)	5.2

### الملحقات

114.....	الخدمة والدعم	
----------	---------------	--

# ١ التعرف على جهاز التوجيه اللاسلكي

## 1.1 مرحبًا!

نشكرك على شراء جهاز التوجيه ZenWiFi Pro ET12 اللاسلكي من ASUS! يتضمن جهاز التوجيه ZenWiFi Pro ET12، الذي يتميز بهيكل أسود ذي تصميم مدهش ولمسات حمراء مستوحاة من عالم الألعاب، نطاقات ثلاثي 2.4 جيجا هرتز، 5 جيجا هرتز و6 جيجا هرتز لتحقيق تجربة بث HD لاسلكي متزامن منقطع النظير؛ إلى جانب خادم SMB وخادم UPnP AV وخادم FTP لمشاركة الملفات على مدار الساعة؛ وإمكانية معالجة 300000 جلسة عمل؛ وتقنية الشبكات الخضراء من ASUS، والتي تحقق توفيرًا في الطاقة يصل إلى 70%.

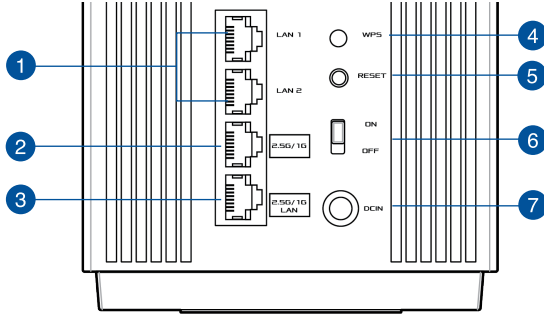
## 1.2 محتويات العبوة

- جهاز توجيه ZenWiFi Pro ET12 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 قائمة الخطوط الساخنة للدعم من ASUS 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 شبكة الاتصال المحلية 1~2 LAN  
وصل الحاسوب الشخصي بمنفذ بواسطة كبل شبكة LAN.

2 منفذ 2.5G/1G WAN  
وصل المودم البصري بهذا المنفذ بواسطة كبل شبكة.

3 منفذ 2.5G/1G LAN  
وصل الحاسوب الشخصي بمنفذ بواسطة كبل شبكة 2.5G / 1G LAN.

4 زر WPS  
يقوم هذا الزر بإطلاق معالج WPS.

5 Reset button (زر إعادة الضبط)  
تسمح لك هذه الميزة باستعادة النظام إلى إعدادات المصنع الافتراضية.

6 Power switch (مفتاح الطاقة)  
اضغط على هذا الزر لتشغيل طاقة النظام أو إيقاف تشغيله.

7 منفذ الطاقة (منفذ تيار متردد)  
أدخل مهبط التيار المتردد المرفق في هذا المنفذ لتوصيل جهاز التوجيه الخاص بك بمصدر للطاقة.

ملاحظات:

- لا تستخدم سوى المهائى المرفق بالعبوة. قد يؤدي استخدام مهائيات أخرى إلى تلف الجهاز.

المواصفات:

مهاين طاقة التيار المتردد		خرج التيار المتردد: +19 فولت مع تيار 2.37 أمبير
مهاين طاقة التيار المتردد		خرج التيار المتردد: +19.5 فولت مع تيار 2.31 أمبير
درجة حرارة التشغيل	40°C~0	التخزين 70°C~0
نسبة الرطوبة المسموح بها أثناء التشغيل	90%~50	التخزين 90%~20



## 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 بتردد 2.4 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 IEEE 802.11a/b/g/n/ac/ax WLAN في الكمبيوتر للاتصال بالشبكة.
- بفضل تقنية النطاق ثلاثي، يدعم جهاز التوجيه اللاسلكي إشارات لاسلكية 2.4 جيجا هرتز، 5 جيجا هرتز و6 جيجا هرتز في وقت واحد. هذا يسمح لك بالقيام بأنشطة متعلقة بالإنترنت مثل تصفح الإنترنت أو قراءة/كتابة رسائل البريد الإلكتروني باستخدام النطاق 2.4 جيجا هرتز في حين الاستمتاع في نفس الوقت ببث ملفات صوت/فيديو بجودة عالية مثل الأفلام أو الموسيقى باستخدام نطاق 5 جيجا هرتز.
- قد تدعم بعض أجهزة IEEE 802.11n التي تريد توصيلها بالشبكة الخاصة بك أو قد لا تدعم نطاق 5 جيجا هرتز. 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

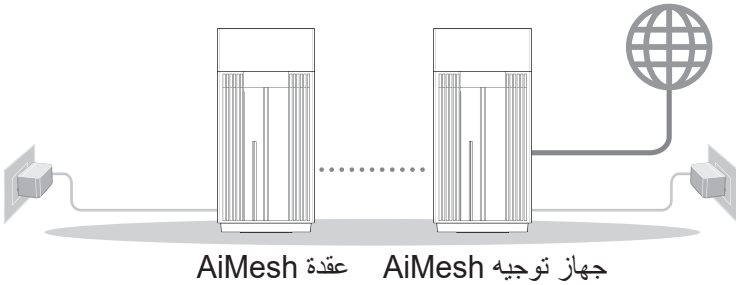
### 2.1 إعداد جهاز التوجيه

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 أيضاً.
- أعد تمهيد مودم الكابل والكمبيوتر الخاص بك (موصى به).

#### A. الاتصال السلكي

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



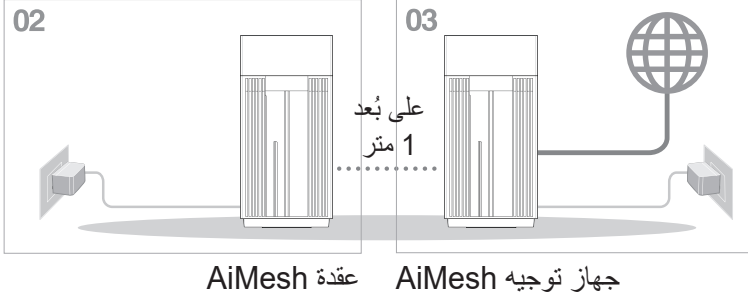
إعداد جهاز التوجيه اللاسلكي الخاص بك باستخدام اتصال سلكي:

1. أدخل مهائئ التيار المتردد الخاص بجهاز التوجيه اللاسلكي بمنفذ DCIN ووصله بمأخذ طاقة.
2. استخدام كبل الشبكة المرفق، ووصل حاسوبك بمنفذ LAN الخاص بجهاز التوجيه اللاسلكي.
3. استخدام كبل شبكة آخر، ووصل المودم بمنفذ WAN الخاص بجهاز التوجيه اللاسلكي.
4. أدخل مهائئ التيار المتردد الخاص بالمودم بمنفذ DCIN ووصله بمأخذ طاقة.

## B. الاتصال اللاسلكي

إعداد 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 و قم بتعيين كلمة المرور.

اسم (SSID) :Wi-Fi	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.

### Login Information Setup

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

Router Login Name

New Password

Retype Password

Show password

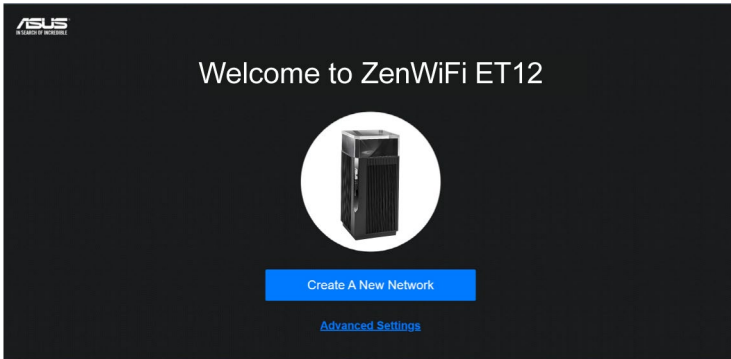
## 2.2 إعداد الإنترنت السريع (QIS) مع الاكتشاف التلقائي

توجيهك 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 توجيهه، 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 2.4 جيجاهرتز و 5 جيجاهرتز اللاسلكي الخاص بك. انقر فوق **Apply (تطبيق)** عند الانتهاء.

**ASUS**  
WIRELESS NETWORKS

## Wireless

Settings

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

2.4GHz Network Name (SSID)

2.4GHz Wireless Security

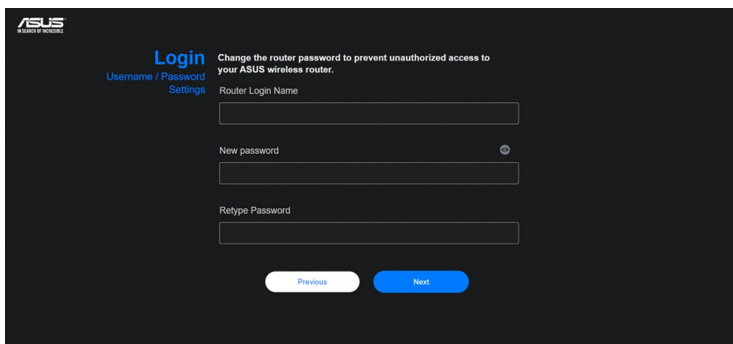
5GHz Network Name (SSID)

5GHz Wireless Security

Separate 2.4GHz and 5GHz

Previous Apply

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





**ملاحظة:** يختلف اسم مستخدم تسجيل الدخول إلى جهاز التوجيه اللاسلكي وكلمة المرور عن اسم شبكة 2.4 جيجا هرتز/5 جيجا هرتز/6 جيجا هرتز (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 2.4 جيجا هرتز/5 جيجا هرتز/6 جيجا هرتز (SSID) ومفتاح الأمان لأجهزة Wi-Fi بتسجيل الدخول والاتصال بشبكة 2.4 جيجا هرتز/5 جيجا هرتز/6 جيجا هرتز 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 من 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.

أزرار الأوامر العليا

معالج - QIS  
الاتصال السريع

جزء التنقل

شريط المعلومات



\* الصورة مرجعية فقط.

**ملاحظة:** إذا كنت تسجل الدخول إلى واجهة المستخدم العمومية على الويب (Web GUI) للمرة الأولى، فسوف يتم توجيهك إلى صفحة (QIS) Quick Internet Setup (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. في شاشة **Network Map** (خريطة الشبكة) تحت **System Status** (حالة النظام)، يمكنك تكوين إعدادات الأمان اللاسلكية مثل SSID، ومستوى الأمان وإعدادات التشفير.

**ملاحظة:** يمكنك إعداد إعدادات أمان لاسلكية مختلفة لنطاقات 2.4 جيجا هرتز و5 جيجا هرتز.

### إعدادات أمان 5/2.4 جيجا هرتز

The screenshot shows the 'System Status' page with two tabs: 'Wireless' and 'Status'. The 'Wireless' tab is active. It displays configuration for two frequency bands: 2.4 GHz and 5 GHz. For each band, the 'Network Name (SSID)' is set to 'ASUS\_2.4GHz' and 'ASUS\_5GHz' respectively. The 'Authentication Method' is set to 'WPA2-Personal' and 'WPA Encryption' is set to 'AES'. The 'WPA-PSK key' field is masked with asterisks. An 'Apply' button is visible at the bottom.

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



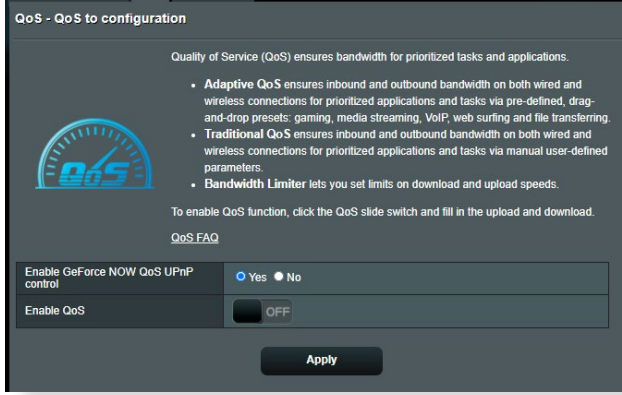
#### إدارة عملاء الشبكة:

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. لاحظ 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. املا 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 أنواع افتراضية للخدمة على الإنترنت - هي تصفح الويب، و HTTPS 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 مرسله 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** و **SYN** و **ICMP** كحزمة عالية الأولوية.

---

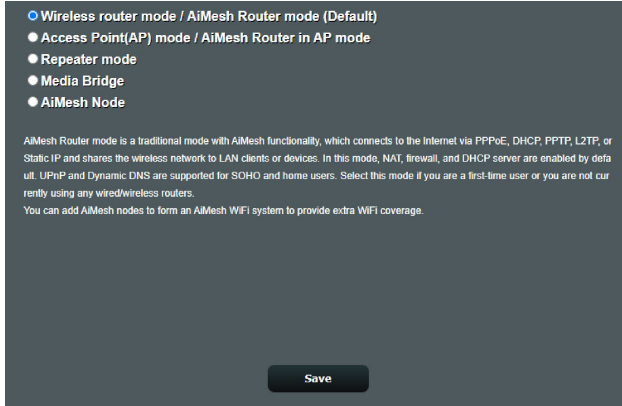
**ملاحظة:** تأكد من تمكين QoS أولاً وإعداد حدود معدلات التحميل والتنزيل.



## 3.3 الإدارة

### 3.3.1 وضع التشغيل

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



#### إعداد 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.
  - **Repeater mode (وضع التكرار):** يعمل هذا الوضع على تحويل جهاز التوجيه إلى جهاز تكرر لاسلكي لتوسعة نطاق الإشارة الخاصة بك.
  - **Media Bridge (جسر الوسائط):** يوفر وضع Media Bridge (جسر الوسائط) أسرع اتصال Wi-Fi لعدة أجهزة وسائط في آن واحد. لإعداد وضع Media Bridge (جسر الوسائط)، يلزمك استخدام جهاز ZenWiFi Pro ET12: إحداهما مكون على أنه محطة وسائط والآخر جهاز توجيه.
  - **AiMesh Node (عقدة AiMesh):** يمكنك تعيين جهاز ZenWiFi Pro ET12 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** (إصدار 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، سوف 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.


## AiCloud 2.0 3.4


AiCloud 2.0 هو تطبيق خدمة سحابية يسمح لك بحفظ ومزامنة ومشاركة الوصول إلى ملفاتك.

**AiCloud 2.0**










ASUS AiCloud 2.0 keeps you connected to your data wherever and whenever you have an Internet connection. It links your home network and online storage service and lets you access your data through the AiCloud mobile app on your iOS or Android mobile device or through a personalized web link in a web browser. Now all your data can go where you go.

- Enter AiCloud 2.0 <https://router.asus.com>
- Find FAQs [GO](#)

 ANDROID APP ON Google play

 Download on the App Store

The wireless router is currently using a private WAN IP address.  
This router may be in a multiple-NAT environment, and accessing AiCloud from WAN does not work.

  	Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device.	<input type="checkbox"/>
Cloud Disk		OFF
  	Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC.	<input type="checkbox"/>
Smart Access		OFF
  	Enables synchronization of USB-attached storage with cloud services like <b>ASUS Webstorage</b> and other AiCloud 2.0-enabled networks.	<input type="button" value="GO"/>
AiCloud Sync		

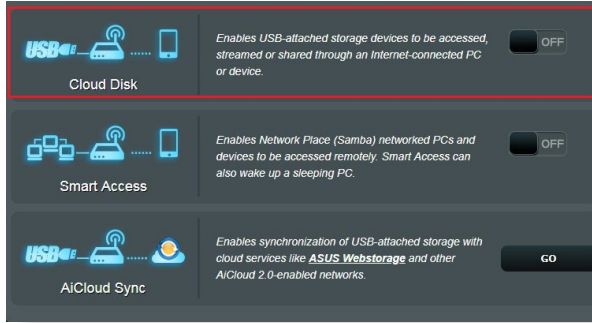
### لاستخدام AiCloud 2.0:

1. من متجر Google Play Store أو Apple Store، قم بتنزيل وتثبيت تطبيق ASUS AiCloud 2.0 إلى الجهاز الذكي الخاص بك.
2. قم بتوصيل الجهاز الذكي بشبكتك. اتبع الإرشادات لاستكمال عملية إعداد AiCloud 2.0.

## 3.4.1 القرص السحابي

لإنشاء قرص سحابي:

1. قم بإدراج جهاز تخزين USB في جهاز التوجيه اللاسلكي.
2. قم بتشغيل **Cloud Disk** (القرص السحابي).

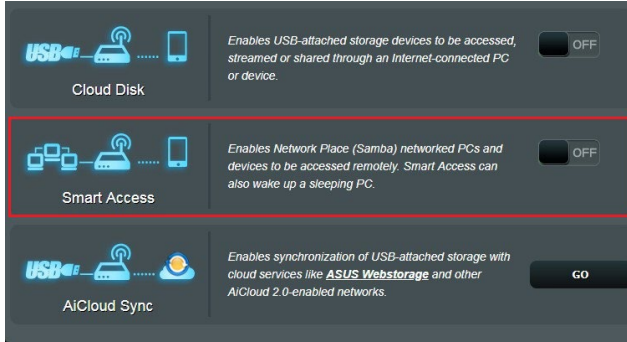


3. انتقل إلى <http://www.asusrouter.com> وأدخل حساب تسجيل الدخول لجهاز التوجيه وكلمة المرور. للحصول على تجربة مستخدم أفضل، نوصي بأن تستخدم **Google Chrome** أو **Firefox**.
4. يمكنك الآن بدء الوصول إلى ملفات القرص السحابي على الأجهزة المتصلة بالشبكة.

**ملاحظة:** عند الوصول إلى الأجهزة المتصلة بالشبكة، يلزمك إدخال اسم المستخدم وكلمة المرور للجهاز يدويًا، والذي لا يتم حفظه في AiCloud 2.0 لأسباب تتعلق بالأمان.

## 3.4.2 الوصول الذكي

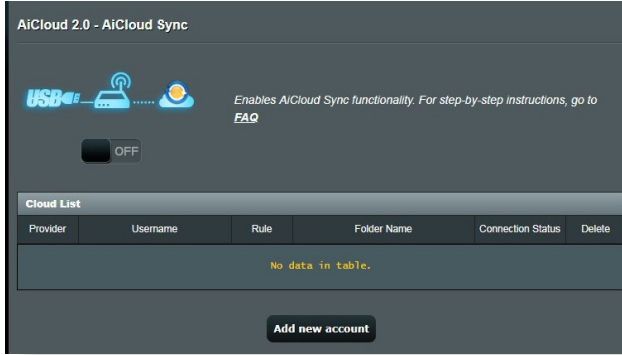
تتيح لك وظيفة الوصول الذكي الوصول بسهولة إلى الشبكة المنزلية الخاصة بك عن طريق اسم المجال لجهاز التوجيه.



### ملاحظات:

- يمكنك إنشاء اسم مجال لجهاز التوجيه من خلال ASUS DDNS. لمزيد من التفاصيل، راجع القسم **DDNS 3.12.6**.
- يوفر AiCloud 2.0 افتراضياً اتصال HTTPS آمن. اكتب [https://\[yourASUSDDNSname\].asuscomm.com](https://[yourASUSDDNSname].asuscomm.com) لكل استخدام آمن للفرص السحابي والوصول الذكي.

## 3.4.3 مزامنة AiCloud



### لاستخدام مزامنة AiCloud:

1. قم بتشغيل AiCloud 2.0، وانقر فوق **AiCloud Sync** (مزامنة AiCloud).
2. حدد **ON** (تشغيل) لتمكين AiCloud Sync (مزامنة AiCloud).
3. انقر فوق **Add new account** (إضافة حساب جديد).
4. أدخل كلمة المرور لحساب ASUS WebStorage الخاص بك وحدد الدليل الذي تريد مزامنته مع WebStorage.
5. انقر فوق **Apply** (تطبيق).

## AiProtection 3.5

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.

### 3.5.1 حماية الشبكة

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

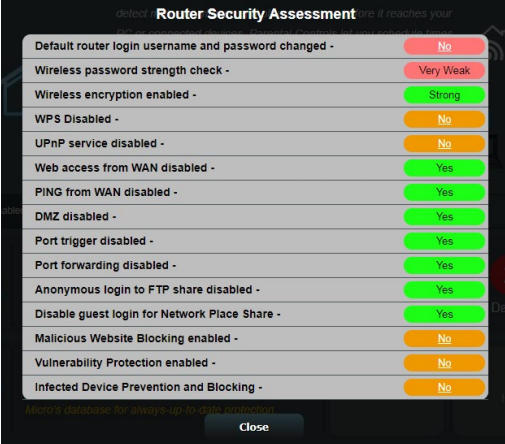
The screenshot displays the AiProtection interface with the following components:

- Header:** AiProtection logo and a description: "Network Protection with Trend Micro protects against network exploits to secure your network from unwanted access." It includes a "Trend Micro SMART HOME NETWORK" logo and an "AiProtection FAQ" link.
- Diagram:** A network diagram showing a globe (2), a router (1), and a smartphone/laptop (3).
- Control Panel:** A toggle switch for "Enabled AiProtection" is currently set to "OFF".
- Router Security Assessment:** A section with a "Scan" button and a "1 Danger" status indicator.
- Malicious Sites Blocking:** A section with a toggle switch set to "ON" and a "0 Protection" status indicator.
- Two-Way IPS:** A section with a toggle switch set to "ON" and a "0 Protection" status indicator.
- Infected Device Prevention and Blocking:** A section with a toggle switch set to "ON" and a "0 Protection" status indicator.
- Alert Preference:** A button located at the bottom right of the interface.



## 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)**.



Security Setting	Status
Default router login username and password changed -	No
Wireless password strength check -	Very Weak
Wireless encryption enabled -	Strong
WPS Disabled -	No
UPnP service disabled -	No
Web access from WAN disabled -	Yes
PING from WAN disabled -	Yes
DMZ disabled -	Yes
Port trigger disabled -	Yes
Port forwarding disabled -	Yes
Anonymous login to FTP share disabled -	Yes
Disable guest login for Network Place Share -	Yes
Malicious Website Blocking enabled -	No
Vulnerability Protection enabled -	No
Infected Device Prevention and Blocking -	No

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)** تبعاً 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

تفيد 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:

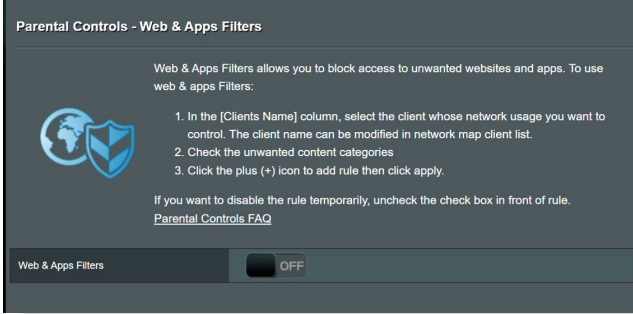
1. من جزء التنقل، انتقل إلى **General** (عام) < **AiProtection**.
  2. من صفحة **AiProtection** الرئيسية، انقر فوق **Network Protection** (حماية الشبكة).
  3. من جزء **Infected Device Prevention and Blocking** (منع الأجهزة المصابة بالفيروسات وحجبها)، انقر فوق **ON** (تشغيل).  
لتكوين تفضيلات التنبيه: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

## 3.5.2 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) (نقل الملفات)**، **Streaming and Entertainment (البث والترفيه)**.

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

### Parental Controls - Web & Apps Filters


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



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

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

Web & Apps Filters
 ON

	Client Name (MAC Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">                     NEW CLIENTS LIST SERVICE                 </div>	<ul style="list-style-type: none"> <li><input type="checkbox"/> <b>Adult</b> Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature.</li> <li><input type="checkbox"/> <b>Instant Message and Communication</b> Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites.</li> <li><input type="checkbox"/> <b>P2P and File Transfer</b> By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission.</li> <li><input type="checkbox"/> <b>Streaming and Entertainment</b> By blocking streaming and entertainment services you can limit the time your children spend online.</li> </ul>	
No data in table.			

Apply

## جدولة الوقت

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


**ملاحظة:** تأكد من مزامنة وقت النظام مع خادم NTP.

### Parental Controls - Time Scheduling

By enabling Block All Devices, all of the connected devices will be blocked from Internet access.

Enable block all devices  OFF

This feature allows you to set up a scheduled time for specific devices' Internet access.



1. In [Client Name] column, select a device you would like to manage. You can also manually key in MAC address in this column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In [Time Management] column, click the edit icon to set a schedule.
4. Click [Apply] to save the configurations.

Enable Time Scheduling  ON

System Time Thu, Sep 21 12:34:41 2023

Client List (Max Limit : 64)

Select all	Client Name (MAC Address)	Time Management	Add / Delete
Time		-	+

No data in table.

Apply

### 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.

## 3.6 جدار الحماية

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

ملاحظة: يتم تمكين ميزة جدار الحماية هذه افتراضياً.

### 3.6.1 عام

#### Firewall

**General**

Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.

[DoS Protection FAQ](#)

Enable Firewall	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable DoS protection	<input checked="" type="radio"/> Yes <input type="radio"/> No
Logged packets type	None
Respond ICMP Echo (ping) Request from WAN	<input type="radio"/> Yes <input checked="" type="radio"/> No

**Basic Config**

Enable IPv4 inbound firewall rules	<input type="radio"/> Yes <input checked="" type="radio"/> No
------------------------------------	---

**Inbound Firewall Rules (Max Limit : 128)**

Source IP	Port Range	Protocol	Add / Delete
		TCP	+
No data in table.			

**IPv6 Firewall**

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified. (2001::1111:2222:3333:64 for example)

**Basic Config**

Enable IPv6 Firewall	<input checked="" type="radio"/> Yes <input type="radio"/> No
Famous Server List	Please select

**Inbound Firewall Rules (Max Limit : 128)**

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
				TCP	+
No data in table.					

**Apply**

إعداد إعدادات جدار الحماية الأساسية:

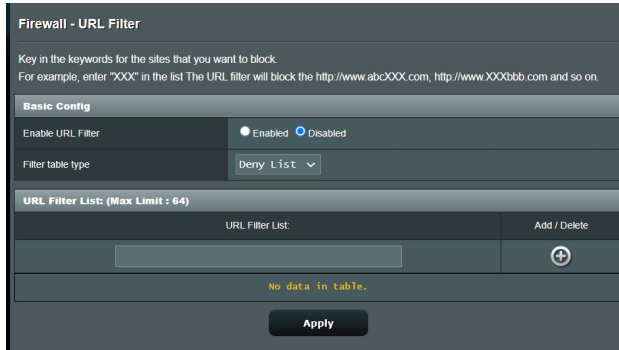
1. من جزء التنقل، انتقل إلى **Advanced Settings** (الإعدادات المتقدمة) < **Firewall** (جدار الحماية) < **General** (عام).
2. في حقل **Enable Firewall** (تمكين جدار الحماية)، حدد **Yes** (نعم).

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 و WAN. في نوع الحزم المسجلة، حدد **Dropped** (مفصولة) أو **Accepted** (مقبولة)، أو **Both** (كليهما).
5. انقر فوق **Apply** (تطبيق).

## 3.6.2 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.



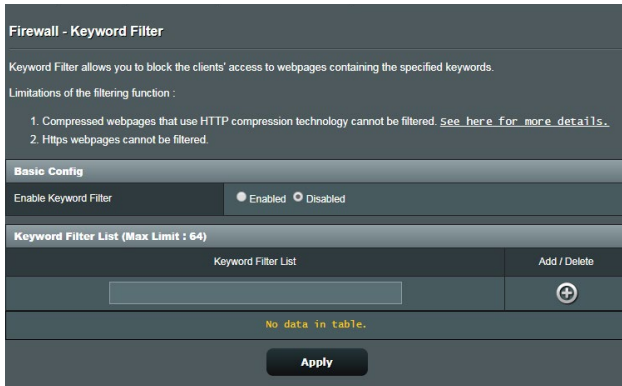
لإعداد عامل تصفية URL:

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).



### 3.6.3 عامل تصفية الكلمات الأساسية

يجب 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 تخزن 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.

## 3.6.4 عامل تصفية خدمات الشبكة

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

### Firewall - Network Services Filter

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

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

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

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

#### Network Services Filter

Enable Network Services Filter	<input checked="" type="radio"/> Yes <input type="radio"/> No
Filter table type	Deny List
Well-Known Applications	User Defined
Date to Enable LAN to WAN Filter	<input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59
Date to Enable LAN to WAN Filter	<input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59
Filtered ICMP packet types	

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

Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
				TCP	+

No data in table.

Apply

## إعداد 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 **Enabled** (ممكّن).
3. حدد نوع جدول عامل التصفية. **Deny** (رفض) تحظر خدمات شبكة معينة. **Allow** (سمّاح) 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).

## 3.7 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 Pro ET12 حتى ست معرفات SSID (ثلاثة لنطاق 2.4 جيجا هرتز وثلاثة لنطاق 5 جيجا هرتز).

### لإنشاء شبكة ضيف:

1. من جزء التنقل، انتقل إلى **General** (عام) < **Guest Network** (شبكة الضيف).
2. في شاشة **Guest Network** (شبكة الضيف)، حدد نطاق التردد 2.4 جيجا هرتز أو 5 جيجا هرتز لشبكة الضيف التي تريد إنشاؤها.
3. انقر فوق **Enable** (تمكين).

#### Guest Network

 The Guest Network provides Internet connection for guests but restricts access to your local network.

---

#### 2.4GHz

Network Name (SSID)  
Authentication  
Method  
Network Key **Enable** **Enable** **Enable**  
Time Remaining **Default setting by Alexa/FTTT**  
Access Intranet


---

#### 5GHz

Network Name (SSID)  
Authentication  
Method  
Network Key **Enable** **Enable** **Enable**  
Time Remaining **Default setting by Alexa/FTTT**  
Access Intranet

4. لتكوين الخيارات الإضافية، انقر فوق **Modify** (تعديل).

### Guest Network

 The Guest Network provides Internet connection for guests but restricts access to your local network.

---

#### 2.4GHz

Network Name (SSID)	ASUS_2G_Guest		
Authentication Method	Open System		
Network Key	None	<b>Enable</b>	<b>Enable</b>
Time Remaining	Unlimited access		Default setting by Alexa/FTTT
Access Intranet	off		
		<b>Remove</b>	

---

#### 5GHz

Network Name (SSID)	ASUS_5G_Guest		
Authentication Method	Open System		
Network Key	None	<b>Enable</b>	<b>Enable</b>
Time Remaining	Unlimited access		Default setting by Alexa/FTTT
Access Intranet	off		
		<b>Remove</b>	

5. انقر فوق **Yes** (نعم) في شاشة **Enable Guest Network** (تمكين شبكة الضيف).

6. قم بتعيين اسم شبكة لاسلكية للشبكة المؤقتة في حقل **Network Name (SSID)** (اسم الشبكة).

7. حدد **Authentication Method** (طريقة المصادقة).

8. حدد طريقة **Encryption** (التشفير).

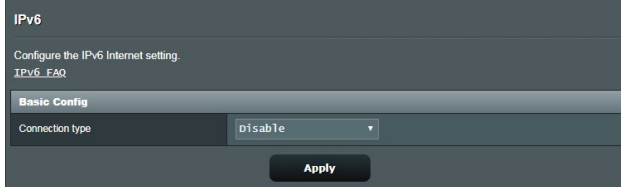
9. حدد **Access time** (وقت الوصول) أو اختر **Limitless** (بلا حدود).

10. حدد **Disable** (تعطيل) أو **Enable** (تمكين) في عنصر **Access Intranet** (الوصول إلى الإنترنت).

11. عند الانتهاء، انقر فوق **Apply** (تطبيق).

## IPv6 3.8

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.



### إعداد 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.

---

## 3.9 شبكة الاتصال المحلية (LAN)

### 3.9.1 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.

LAN - LAN IP

Configure the LAN setting of ASUS Router.

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

Apply

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).

## 3.9.2 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.

### LAN - DHCP Server

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

#### Basic Config

Enable the DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
ASUS Router's Domain Name	<input type="text"/>
IP Pool Starting Address	<input type="text" value="192.168.50.2"/>
IP Pool Ending Address	<input type="text" value="192.168.50.254"/>
Lease time	<input type="text" value="86400"/>
Default Gateway	<input type="text"/>

#### DNS and WINS Server Setting

DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>
Advertise router's IP in addition to user-specified DNS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WINS Server	<input type="text"/>

#### Manual Assignment

Enable Manual Assignment	<input type="radio"/> Yes <input checked="" type="radio"/> No
--------------------------	---

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

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

### 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 Server Settings (DNS وإعدادات 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.

### 3.9.3 المسار

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

**ملاحظة:** نوصي بالآ تغيير إعدادات التوجيه الافتراضية إلا إذا كنت تتمتع بمعرفة متقدمة بجدول جهاز التوجيه.

Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
				LAN	+

No data in table.

Apply

#### 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).

### 3.9.4 التلفزيون عبر الإنترنت (IPTV)

يُدمج جهاز التوجيه اللاسلكي الاتصال بخدمات التلفزيون عبر الإنترنت (IPTV) عن طريق إما مزود خدمة الإنترنت (ISP) أو شبكة اتصال محلية. توفر علامة تبويب IPTV (التلفزيون عبر الإنترنت) إعدادات التكوين اللازمة لإعداد خدمة التلفزيون 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.

**LAN - IPTV**

To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN - Dual WAN](#) to confirm that WAN port is assigned to primary WAN.

LAN Port	
Select ISP Profile	None ▾
Choose IPTV STB Port	None ▾

Special Applications	
Use DHCP routes	Microsoft ▾
Enable multicast routing (IGMP Proxy)	Disable ▾
UDP Proxy (Udpxy)	0

**Apply**

## 3.10 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)

The screenshot displays the 'System Log - General Log' interface. At the top, it states 'This page shows the detailed system's activities.' Below this, the system time is shown as 'Thu, Aug 23 07:15:34 2018' and the uptime as '0 days 1 hours 18 minute(s) 11 seconds'. There is an 'Apply' button for the remote log server. The main area contains a scrollable log of system events, including MiniUPnPd starting, HTTP listening on port 5351, kernel path\_add\_flow ASSERT messages, wan: finish adding multi routes, nps: start NTP update, and nat: apply nat rules. At the bottom, there are 'Clear' and 'Save' buttons.

```
System Log - General Log

This page shows the detailed system's activities.

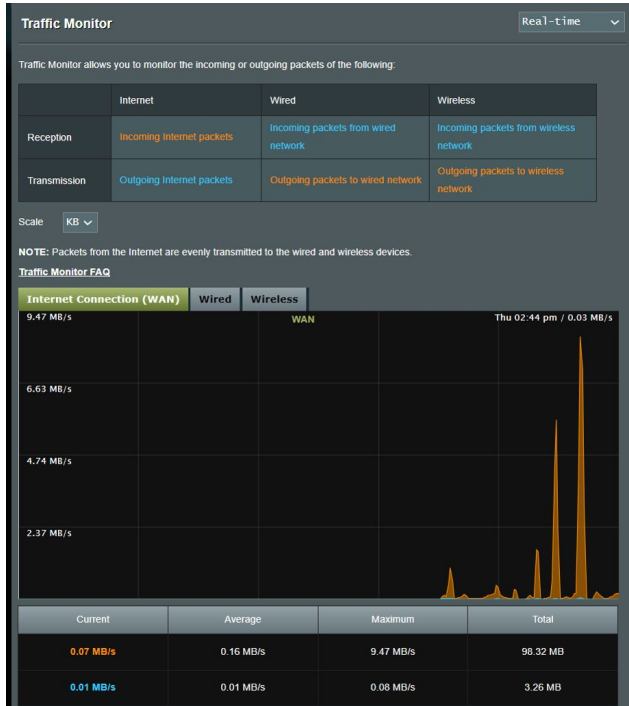
System Time Thu, Aug 23 07:15:34 2018
Uptime 0 days 1 hours 18 minute(s) 11 seconds
Remote Log Server [ ] Apply

Aug 23 06:51:04 miniupnpd(7139): version 1.9 started
Aug 23 06:51:04 miniupnpd(7139): HTTP listening on port 5351
Aug 23 06:58:52 kernel: ~[[0:33:41m][PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVAL
Aug 23 06:58:52 kernel: ~[[0:33:41m][PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVAL
Aug 23 06:58:55 kernel: ~[[0:33:41m][PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVAL
Aug 23 06:58:55 kernel: ~[[0:33:41m][PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVAL
Aug 23 06:58:57 kernel: ~[[0:33:41m][PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVAL
Aug 23 06:58:57 kernel: ~[[0:33:41m][PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVAL
Aug 23 06:58:57 kernel: ~[[0:33:41m][PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVAL
Aug 23 06:58:57 kernel: ~[[0:33:41m][PATHSTAT] path_add_flow ASSERT: (enroute_pathkey != PATH_IX_INVAL
Aug 23 07:07:14 rc_services: httpd 1079:modify rc_start_multipath
Aug 23 07:07:14 miniupnpd(7139): shutting down MiniUPnPd
Aug 23 07:07:14 nat: apply nat rules (/tmp/nat_rules_eth0_eth0)
Aug 23 07:07:14 miniupnpd(7688): version 1.9 started
Aug 23 07:07:14 miniupnpd(7688): HTTP listening on port 60955
Aug 23 07:07:14 miniupnpd(7688): Listening for NAT-PMP/PCP traffic on port 5351
Aug 23 07:07:14 wan: finish adding multi routes
Aug 23 07:07:14 nps: start NTP update
Aug 23 07:07:15 miniupnpd(7688): shutting down MiniUPnPd
Aug 23 07:07:15 miniupnpd(7729): version 1.9 started
Aug 23 07:07:15 miniupnpd(7729): HTTP listening on port 58635
Aug 23 07:07:15 miniupnpd(7729): Listening for NAT-PMP/PCP traffic on port 5351

Clear Save
```

## 3.11 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 أنياً وبصفة منتظمة. وتعرض كذلك خيار عرض حركة بيانات الشبكة خلال آخر 24 ساعة.



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

## 3.12 الشبكة واسعة النطاق (WAN)

### 3.12.1 اتصال الإنترنت

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

#### WAN - Internet Connection

ASUS Router supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of ASUS Router.

##### Basic Config

WAN Connection Type	Automatic IP
Enable WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable NAT	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UPnP	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable WAN Aggregation	<input checked="" type="radio"/> Yes <input type="radio"/> No <small>WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification) <a href="#">WAN Aggregation FAQ</a></small>

##### WAN DNS Setting

DNS Server	Default status: Get the DNS IP from your ISP automatically. Assign a DNS service to improve security, block advertisement and gain faster performance. <span>Assign</span>
Forward local domain queries to upstream DNS	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable DNS Rebind protection	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable DNSSEC support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Prevent client auto DoH	Auto
DNS Privacy Protocol	None

##### DHCP Option

Class Identifier (Option 60)	
Client Identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID
Class Identifier (Option 60)	
Client Identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID

##### Account Settings

Authentication	None
PPP Echo Interval	6
PPP Echo Max Failures	10

##### Special Requirement from ISP

Host Name	
MAC Address	<span>MAC Clone</span>
DHCP query frequency	Aggressive Mode
Extend the TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No
Spoof LAN TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

## 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 عنوان IP 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 والتلفزيون وأنظمة الإستريو ووحدات الألعاب والهاتف الخليوي)، 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 سلسلة 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 وخواص الويب أو خواص 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 4 LAN لجهاز التوجيه الخاص بك بمنفذ 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 وأملأ 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.



## 3.12.2 الشبكة واسعة النطاق الثنائية

تسمح لك Dual WAN (الشبكة واسعة النطاق الثنائية) بتحديد اتصاليين 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)**. يتوفر أمامك الخيارات WAN و USB و Ethernet LAN و 2.5 جيجا WAN.
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>

### WAN - Dual WAN

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

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

<b>Basic Config</b>	
Enable Dual WAN	<input type="checkbox"/> OFF
Primary WAN	1.G. WAN ▾
Auto USB Backup WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
<b>Auto Network Detection</b>	
Detailed explanations are available on the <a href="#">ASUS Support Site FAQ</a> , which may help you use this function effectively.	
Detect Interval	Every 3 seconds
Internet Connection Diagnosis	When the current WAN fails 2 continuous times, it is deemed a disconnection.
Network Monitoring	<input type="checkbox"/> DNS Query <input checked="" type="checkbox"/> Ping
<b>Apply</b>	

### 3.12.3 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.

WAN - Port Trigger

Port Trigger allows you to temporarily open data ports when LAN devices require unrestricted access to the Internet. There are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port.  
Port Trigger FAQ

**Basic Config**

Enable Port Trigger  Yes  No

Well-Known Applications

Trigger Port List ( Max Limit : 32 )

Description	Trigger Port	Protocol	Incoming Port	Protocol	Delete
No data in table					

#### إعداد 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 اتصالاً صادرًا باستخدام نطاق منفذ المشغل 66660-7000. 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.
-

### 3.12.4 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.

#### WAN - Virtual Server / Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.

If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200,10300), the LAN IP address, and leave the Local Port blank.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with ASUS Server's web user interface.
- When you set 2021 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with ASUS Server's native FTP server.

[Virtual Server / Port Forwarding FAQ](#)

#### Basic Config

Enable Port Forwarding  OFF

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

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

[Add profile](#)

#### 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 SIP):** تجنب تعيين نطاق المنفذ 20:21 لخادم FTP الخاص بك نظرًا لأنه يتعارض مع تعيين خادم FTP الأصلي لجهاز 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)، و Port Range (نطاق المنافذ) (على سبيل المثال 10200:10300)، وعنوان LAN IP، و اترك 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 معطلاً 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 يمكنك 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 3.9 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 (يشار 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.

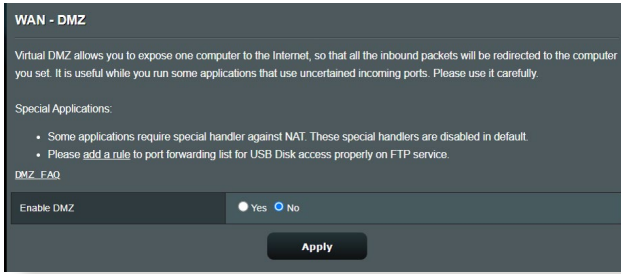
### 3.12.5 المنطقة المنزوعة (DMZ)

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 مفيداً عندما تحتاج إلى فتح المنافذ الواردة أو ترديد استضافة مجال أو خادم ويب أو خادم بريد إلكتروني.

**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).



#### إعداد 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 للعميل الذي سيوفر خدمة DMZ يكون مكشوفاً 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).

## 3.12.6 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.

**WAN - DDNS**

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to <https://iplookup.asus.com/nslookup.php> to reach your internet IP address to use this service.

The wireless router currently uses a private WAN IP address.  
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.

The host name is successfully registered. You can use "[hostname].asuscomm.com" to access the service in home network from WAN. Use "[hostname].asuscomm.com" to remotely access your network.  
Go to Advanced Settings > WAN to configure the port forwarding or DMZ settings to allow other WAN clients to remotely access your network.  
If you want to remotely configure the wireless router, go to [here](#).

Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	www.asus.com <input type="button" value="Deregister"/>
Host Name	A8878A175D46FD54D2E6BD6195D85EF7 .asuscomm.com
DDNS Status	Active
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	<input type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input checked="" type="radio"/> None

## إعداد 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 أولاً. قم بملء اسم المستخدم أو عنوان البريد الإلكتروني وكلمة المرور أو حقول مفتاح DDNS.
- **Enable wildcard (تمكين حرف البديل):** قم بتمكين حرف البديل 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.

### 3.12.7 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)، و IPsec Passthrough (اجتياز IPsec) و RTSP Passthrough (اجتياز RTSP) افتراضياً.

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).

WAN - NAT Passthrough	
Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.	
PPTP Passthrough	Enable ▾
L2TP Passthrough	Enable ▾
IPSec Passthrough	Enable ▾
RTSP Passthrough	Enable ▾
H.323 Passthrough	Enable ▾
SIP Passthrough	Enable ▾
PPPoE Relay	Disable ▾
FTP ALG port	2021
<b>Apply</b>	

## 3.13 لاسلكي

### 3.13.1 عام

تسمح لك علامة التبويب General (عام) بتكوين الإعدادات اللاسلكية الأساسية.

Wireless - General	
Set up the wireless related information below.	
Enable Smart Connect	<input type="checkbox"/> OFF
Band	2.4 GHz
Network Name (SSID)	ASUS Router
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Mode	Auto <input checked="" type="checkbox"/> big Protection
802.11ax / WiFi 6 mode	Enable <small>If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check FAQ</small>
WiFi Agile Multiband	Disable
Target Wake Time	Disable
Channel bandwidth	20/40 MHz
Control Channel	Auto <small>Current Control Channel: 4</small>
Extension Channel	Auto
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	***** Very Strong
Protected Management Frames	Disable
Group Key Rotation Interval	3600

Apply

### لتهيئة الإعدادات اللاسلكية الأساسية:

1. من جزء التنقل، انتقل إلى **Advanced Settings (الإعدادات المتقدمة) < Wireless (اللاسلكي) < General (عام)**.
2. حدد 2.4 جيجا هرتز أو 5 جيجا هرتز كنطاق تردد للشبكة اللاسلكية.
3. قم بتعيين اسم فريد يحتوي على 32 حرفاً لـ SSID (معرف مجموعة الخدمة) أو اسم الشبكة لتحديد الشبكة اللاسلكية الخاصة بك. يمكن تعريف أجهزة Wi-Fi وتوصيلها بشبكة لاسلكية عن طريق معرف SSID المعين. يتم تحديث معرفات SSID على شريط المعلومات بمجرد حفظ معرفات SSID جديدة في الإعدادات.

**ملاحظة:** يمكنك تعيين معرفات SSID جديدة لنطاقات تردد 2.4 GHz و 5 جيجاهرتز.

4. في حقل **Hide SSID (إخفاء SSID)**، حدد **Yes (نعم)** لمنع الأجهزة اللاسلكية من اكتشاف معرف SSID الخاص بك. عند تمكين هذه الوظيفة، سوف تحتاج إلى إدخال SSID يدويًا في الجهاز اللاسلكي للوصول إلى الشبكة اللاسلكية.
5. حدد أي من خيارات الوضع اللاسلكي هذه لتحديد أنواع الأجهزة اللاسلكية التي يمكنك توصيلها بجهاز التوجيه اللاسلكي الخاص بك:
  - **تلقائي: Auto (تلقائي)** للسماح لأجهزة 802.11n و 802.11AC و 802.11g و 802.11b بالاتصال بجهاز التوجيه اللاسلكي.
  - **Legacy (قديم):** حدد **Legacy (قديم)** للسماح بأجهزة 802.11b/g/n للاتصال بجهاز التوجيه اللاسلكي الخاص بك. مع ذلك، فالأجهزة التي تدعم 802.11n بصورة طبيعية، لن تعمل بأقصى سرعة 54 ميجابايت في الثانية.
  - **N only (N فقط):** حدد **only N (N فقط)** لرفع أداء N إلى أقصى حد. يمنع هذا الإعداد أجهزة 802.11g و 802.11b من الاتصال بجهاز التوجيه اللاسلكي.
6. حدد أي عرض نطاق للقناة لاستيعاب سرعات الإرسال العالية:
  - **40MHz (40 ميجاهرتز):** حدد عرض النطاق هذا لرفع الإنتاجية اللاسلكية إلى أقصى حد.
  - **20MHz (20 ميجاهرتز) (الافتراضي):** حدد عرض النطاق هذا إذا واجهت بعض المشكلات في الاتصال اللاسلكي الخاص بك.
7. حدد قناة التشغيل لجهاز التوجيه اللاسلكي الخاص بك. حدد **Auto (تلقائي)** للسماح لجهاز توجيه اللاسلكي بتحديد القناة تلقائيًا والتي تتضمن أقل مقدار من التداخل.
8. حدد أي من طرق المصادقة هذه:
  - **Open System (نظام مفتوح):** هذا الخيار لا يوفر أي أمان.
  - **Shared Key (مفتاح مشترك):** يجب أن تستخدم تشفير WEP وأدخل مفتاح مشترك واحد على الأقل.

- **WPA/WPA2 Personal** (نظام WPA/WPA2 شخصي) **WPA/WPA2 Auto-Personal** (نظام WPA تلقائي شخصي): يوفر هذا الخيار إعداد أمان قوي. يمكنك استخدام إما WPA (مع TKIP) أو WPA2 (مع AES). إذا حددت هذا الخيار، يجب أن تستخدم تشفير TKIP + AES وإدخال عبارة مرور WPA (مفتاح الشبكة).
- **WPA/WPA2 Enterprise** (نظام WPA/WPA2 للمؤسسة) **WPA/WPA2 Auto-Enterprise** (نظام WPA تلقائي للمؤسسة): يوفر هذا الخيار إعداد أمان قوي للغاية. إنه يتكامل مع خادم EAP أو خادم مصادقة RADIUS خلفي خارجي.
- **Radius مع 802.1x**

---

**ملاحظة:** يدعم جهاز التوجيه اللاسلكي الخاص بك أقصى معدل إرسال 54 ميجابايت في الثانية عند تعيين **Wireless Mode** (الوضع اللاسلكي) إلى **Auto** (تلقائي) وتعيين **encryption method** (طريقة التشفير) إلى **WEP** أو **TKIP**.

---

9. حدد أي من خيارات تشفير WEP (الخصوصية المكافئة للشبكات السلكية) للبيانات التي يتم نقلها عن طريق الشبكة اللاسلكية الخاصة بك:
- **Off** (إيقاف): يعطل تشفير WEP
  - **64-bit** (64 بت): يوفر تشفير WEP ضعيف
  - **128-bit** (128 بت): يوفر تشفير WEP محسّن
  - 10. عند الانتهاء، انقر فوق **Apply** (تطبيق).

## WPS 3.13.2

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.

Wireless - WPS

WPS (WiFi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button.

Enable WPS	<input checked="" type="checkbox"/>
Current Frequency	2.4 GHz
Connection Status	Idle
Configured	Enabled <input type="button" value="Reset"/> <small>Pressing the reset button resets the network name (SSID) and WPA encryption key.</small>
AP PIN Code	51246044

You can easily connect a WPS client to the network in either of these two ways:

- Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.
- Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.

WPS Method:  Push button  Client PIN Code

لتمكن 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 افتراضياً نطاق 2.4 جيجا هرتز. إذا أردت تغيير التردد إلى 5 جيجا هرتز، فقم **OFF** (بايقاف) 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 WPA2-الشخصي. لا يدعم WPS الشبكة اللاسلكية التي تستخدم مفتاح مشترك ونظام WPA-للمؤسسة، ونظام WPA2-للمؤسسة، وطريقة تشفير RADIUS.

---

4. في حقل WPS Method (طريقة)، حدد **Push Button (زر ضغط)** أو رمز **Client PIN (التعريف الشخصي للعميل)**. إذا حددت **Push Button (زر ضغط)**، انتقل إلى الخطوة 5. إذا حددت **Client PIN (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 مؤخره 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.

### 3.13.3 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 تكرر لاسلكيًا حيث يتواصل جهاز التوجيه اللاسلكي الخاص بك من ASUS مع نقطة وصول أخرى وأجهزة لاسلكية أخرى.

**Wireless - Bridge**

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

**Note:**

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

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

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

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

Basic Config	
2.4 GHz MAC	<input type="text" value="C8:7F:54:12:69:C8"/>
5 GHz MAC	<input type="text" value="C8:7F:54:12:69:CC"/>
Band	<input type="text" value="2.4 GHz"/>
AP Mode	<input type="text" value="AP Only"/>
Connect to APs in list	<input checked="" type="radio"/> Yes <input type="radio"/> No

Remote AP List (Max Limit : 4)	
Remote AP List	Add / Delete
<input type="text"/>	<input type="button" value="+"/>
No data in table.	

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 وصول 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 تلقائياً بأقل مقدار من التداخل.

---

**ملاحظة:** يختلف توفر القناة حسب الدولة أو المنطقة.

6. في 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)**.



### 3.13.4 عامل تصفية MAC للشبكة اللاسلكية

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

Wireless - Wireless MAC Filter	
Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.	
<b>Basic Config</b>	
Band	2.4GHz
Enable MAC Filter	<input checked="" type="radio"/> Yes <input type="radio"/> No
MAC Filter Mode	Accept
<b>MAC filter list (Max Limit : 64)</b>	
Client Name (MAC Address)	Add / Delete
<input type="text"/>	<input type="button" value="Add"/>
No data in table.	
<input type="button" value="Apply"/>	

إعداد عامل تصفية MAC اللاسلكي:

1. من جزء التنقل، انتقل إلى **Advanced Settings** (الإعدادات المتقدمة) < **Wireless** (لاسلكي) < **Wireless MAC Filter** (عامل تصفية MAC اللاسلكي).
2. اختر **Yes** (نعم) في حقل **Enable Mac Filter** (تمكين عامل تصفية Mac).
3. في القائمة المنسدلة **MAC Filter Mode** (وضع 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.
4. في قائمة عوامل تصفية MAC، انقر فوق زر **Add** (إضافة)  واكتب عنوان MAC للجهاز اللاسلكي.
5. انقر فوق **Apply** (تطبيق).

## 3.13.5 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.

Wireless - RADIUS Setting	
This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".	
Band	2.4Ghz
Server IP Address	
Server Port	1812
Connection Secret	
<b>Apply</b>	

### إعداد 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.

**ملاحظة:** الرجاء مراجعة القسم 3.13.1 عام لتكوين وضع المصادقة لجهاز التوجيه اللاسلكي.

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).**

## 3.13.6 احترافي

توفر شاشة Professional (احترافي) خيارات تكوين متقدمة.

ملاحظة: نوصي بأن تستخدم القيمة الافتراضية بهذه الصفحة.

### Wireless - Professional

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

Band	2.4 GHz
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable wireless scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No
Set AP Isolated	<input type="radio"/> Yes <input checked="" type="radio"/> No
Roaming assistant	Enable Disconnect clients with RSSI lower than: -70 dBm
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Enable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable
Modulation Scheme	Up to MCS 11 (NitroQAM/1024-QAM)
Airtime Fairness	Disable
Multi-User MIMO	Enable
OFDMA/802.11ax MU-MIMO	Disable
Explicit Beamforming	Enable
Universal Beamforming	Enable
Tx power adjustment	<input type="range"/> Performance

Apply

في شاشة Professional Settings (الإعدادات 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.

Wireless - Professional

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

Clock Format: 24-hour  Allow  Deny

Active Schedule

System Time: Thu, Aug 23 06:59:27 2018

Select All	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00 ~ 01							
01 ~ 02							
02 ~ 03							
03 ~ 04							
04 ~ 05							
05 ~ 06							
06 ~ 07							
07 ~ 08							
08 ~ 09							
09 ~ 10							
10 ~ 11							
11 ~ 12							
12 ~ 13							
13 ~ 14							
14 ~ 15							
15 ~ 16							
16 ~ 17							
17 ~ 18							
18 ~ 19							
19 ~ 20							
20 ~ 21							
21 ~ 22							
22 ~ 23							
23 ~ 24							

Cancel OK

- **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 الأني.
- **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 ميلي ثانية.
- **Beacon Interval (فاصل الإشارة):** يشير فاصل الإشارة إلى الفترة الزمنية بين إشارة DTIM والإشارة التي تليها. القيمة الافتراضية هي 100 ميلي 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

ملاحظات:

- قم بتنزيل الأدوات المساعدة لجهاز التوجيه اللاسلكي وتثبيتها من موقع ASUS على الويب:
- [https://dlcdnets.asus.com/pub/ASUS/wireless/ASUSWRT/Discovery\\_1483.zip?model=ZenWiFi%20Pro%20ET12](https://dlcdnets.asus.com/pub/ASUS/wireless/ASUSWRT/Discovery_1483.zip?model=ZenWiFi%20Pro%20ET12) Device Discovery (استكشاف الجهاز) v1.4.7.1 على العنوان
- [https://dlcdnets.asus.com/pub/ASUS/wireless/GT-AX6000/Rescue\\_2103.zip?model=ZenWiFi%20Pro%20ET12](https://dlcdnets.asus.com/pub/ASUS/wireless/GT-AX6000/Rescue_2103.zip?model=ZenWiFi%20Pro%20ET12) Firmware Restoration (استعادة البرنامج الثابت) v1.9.0.4 على العنوان
- <http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip> (الأداة المساعدة لطابعة Windows) Windows Printer Utility v1.0.5.5 على العنوان
- لا يتم دعم هذه الأدوات المساعدة على أنظمة MAC OS.

### 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.

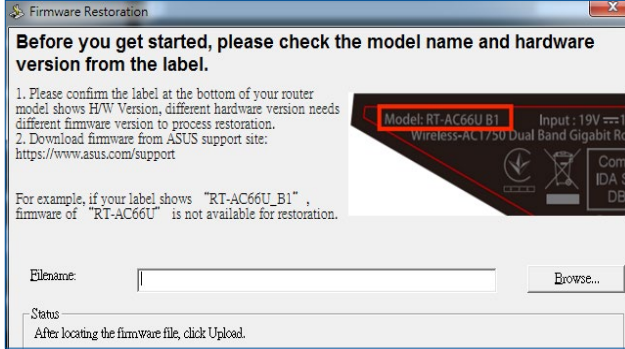
لتشغيل أداة Device Discovery (اكتشاف الجهاز) المساعدة:

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

**ملاحظة:** عندما تقوم بتعيين جهاز التوجيه إلى وضع نقطة وصول، عندئذٍ 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 ببطي، 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.

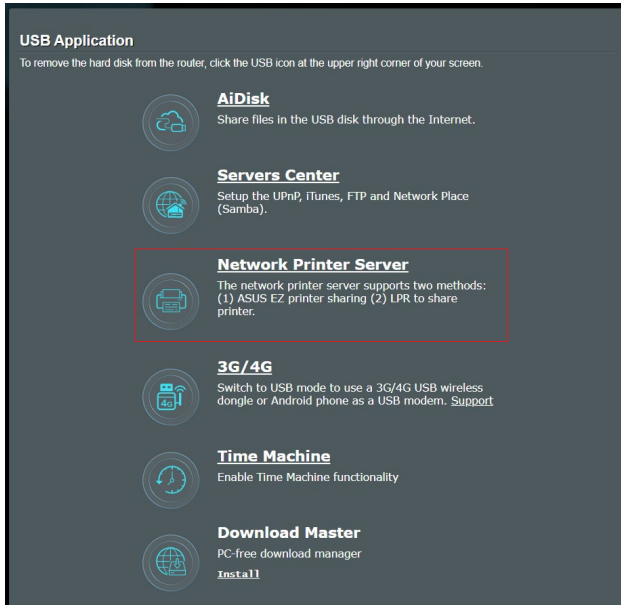
---



## 4.3 إعداد خادم الطباعة

### 4.3.1 ASUS EZ مشاركة طباعة

تسمح أداة مشاركة الطباعة ASUS EZ Printing Sharing لك بتوصيل طباعة USB بمنفذ USB لجهاز التوجيه اللاسلكي وإعداد خادم الطباعة. هذا يسمح لعملاء الشبكة بطباعة الملفات ومسحها ضوئيًا بشكل لاسلكي.

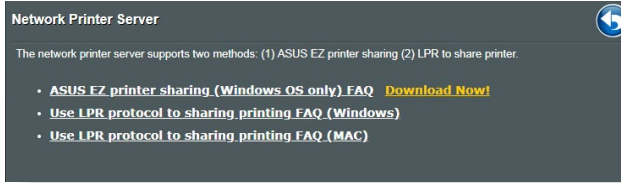


ملاحظة: يتم دعم وظيفة خادم الطباعة على أنظمة تشغيل Windows® 10 و Windows® 11.

## إعداد وضع مشاركة الطابعة EZ:

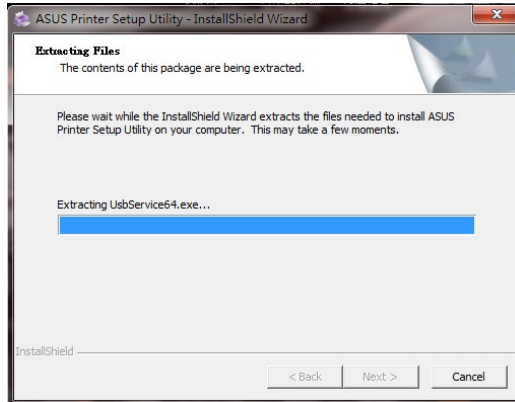
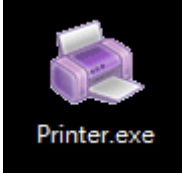
1. من لوحة التحكم، انتقل إلى **General (عام) < USB Application (تطبيق Network Printer Server < (USB خادم طابعة الشبكة).**

2. انقر فوق **Download Now! (تنزيل الآن)** لتنزيل الأداة المساعدة لطابعة الشبكة.



**ملاحظة:** يتم دعم الأداة المساعدة لطابعة الشبكة على أنظمة تشغيل Windows® 10 و Windows® 11 فقط. لتثبيت الأداة المساعدة على نظام Mac OS، حدد **Use LPR protocol for sharing printer (استخدام بروتوكول LPR لمشاركة الطابعة).**

3. قم بفك ضغط الملف الذي تم تنزيله وانقر فوق رمز الطابعة لتشغيل برنامج إعداد طابعة الشبكة.



4. اتبع الإرشادات المعروضة على الشاشة لإعداد الأجهزة، ثم انقر فوق **Next** (التالي).



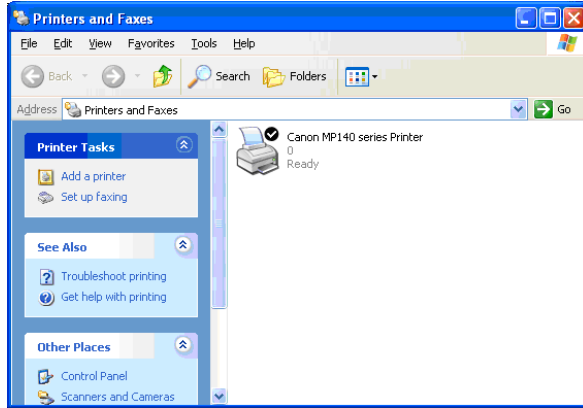
5. انتظر بضع دقائق حتى يتم استكمال الإعداد الأولي. انقر **Next** (التالي).

6. انقر فوق **Finish** (إنهاء) لاستكمال التثبيت.

7. اتبع التعليمات من نظام تشغيل Windows® OS لتثبيت برنامج تشغيل الطابعة.



8. بعد استكمال تثبيت برنامج تشغيل الطابعة، يمكن الآن لعملاء الشبكة استخدام الطابعة.



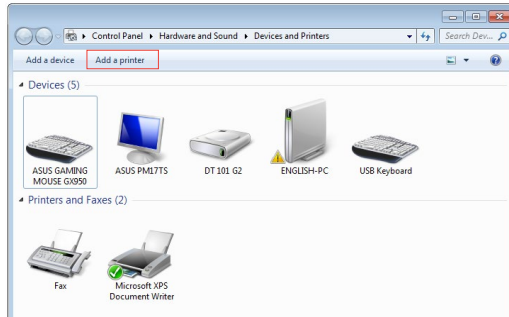
## 4.3.2 استخدام LPR لمشاركة الطابعة

يمكنك مشاركة الطابعة مع أجهزة الكمبيوتر التي تعمل بأنظمة تشغيل Windows® و MAC التي تستخدم LPR/LPD (بروتوكول تلقي مهام الطباعة عن بعد/البرنامج الوسيط للطباعة عن بعد).

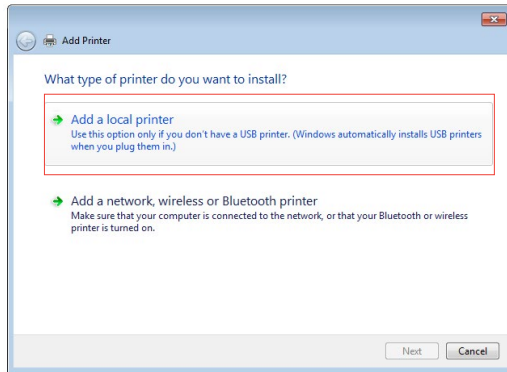
### مشاركة طابعة LPR

#### لمشاركة طابعة LPR:

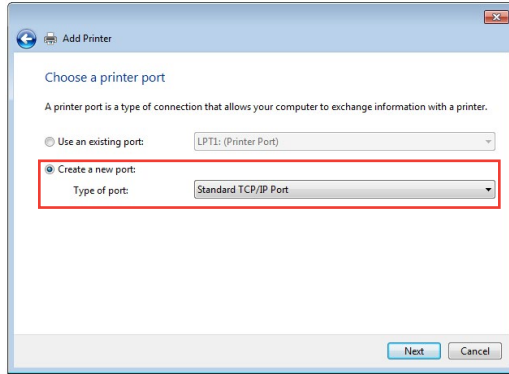
1. من سطح مكتب Windows®، انقر فوق **Start** (بدء) < **Devices and Printers** (الأجهزة والطابعات) < **Add a printer** (إضافة طابعة) لتشغيل **Add Printer Wizard** (معالج إضافة طابعة).



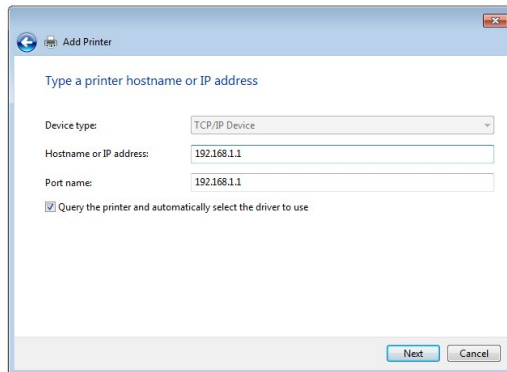
2. حدد **Add a local printer** (إضافة طابعة محلية) ثم انقر فوق **Next** (التالي).



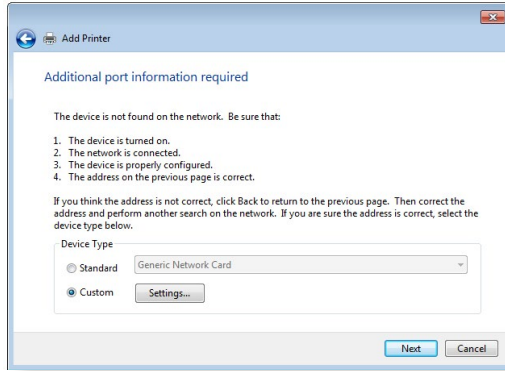
3. حدد **Create a new port** (إنشاء منفذ جديد) ثم قم بتعيين **Type of Port** (نوع المنفذ) إلى **Standard TCP/IP Port** (منفذ TCP/IP قياسي). انقر فوق **Next** (التالي).



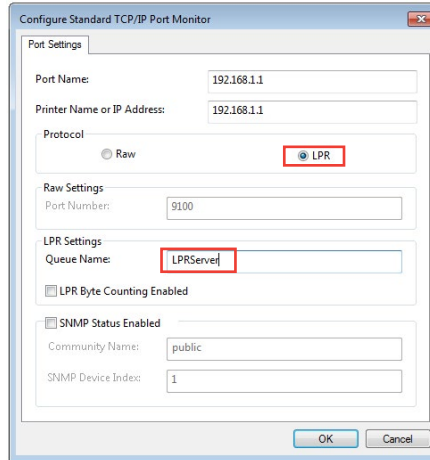
4. في حقل **Hostname or IP address** (اسم المضيف أو عنوان IP)، اكتب عنوان IP لجهاز التوجيه اللاسلكي ثم انقر فوق **Next** (التالي).



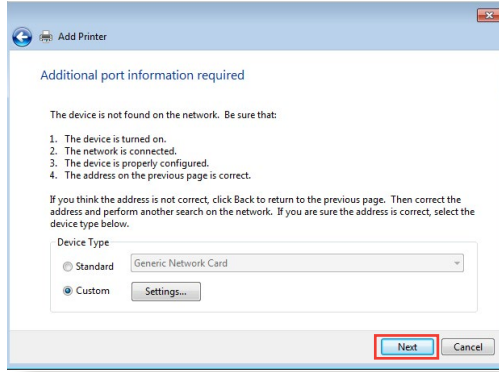
5. حدد Custom (مخصص) ثم انقر فوق Settings (إعدادات).



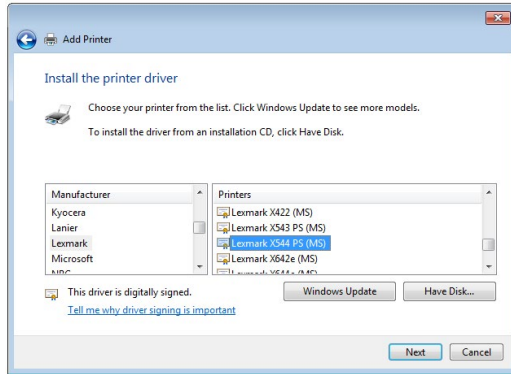
6. قم بتعيين Protocol (البروتوكول) إلى LPR. في حقل Queue Name (اسم القائمة)، اكتب LPRServer ثم انقر فوق OK (موافق) للاستمرار.



7. انقر فوق **Next** (التالي) لإنهاء إعداد منفذ TCP/IP القياسي.

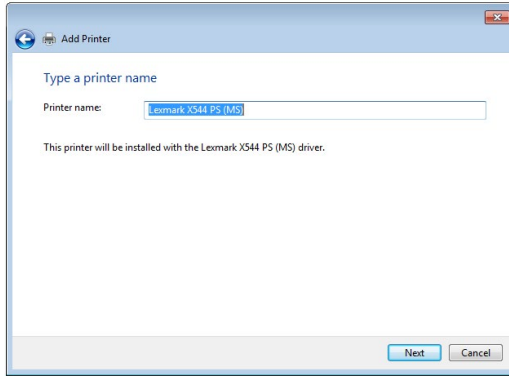


8. قم بتنصيب برنامج تشغيل الطابعة من قائمة طرازات المورد. إذا كانت الطابعة غير مدرجة، فانقر فوق **Have Disk** (قرص خاص) لتنصيب برامج تشغيل الطابعة يدويًا من قرص مضغوط CD-ROM أو ملف.

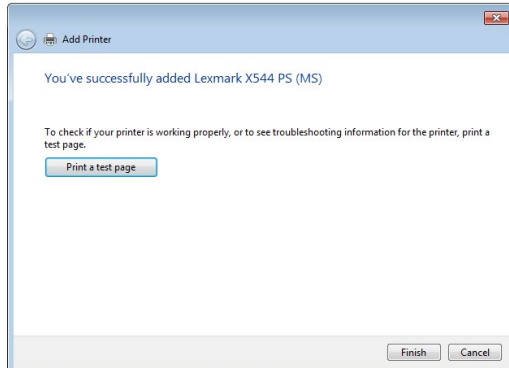




9. انقر فوق **Next** (التالي) لقبول الاسم الافتراضي للطابعة.



10. انقر فوق **Finish** (إنهاء) لاستكمال التثبيت.



## 4.4 مدير التنزيل

يمثل Download Master (مدير التنزيل) أداة مساعدة لمساعدتك في تنزيل الملفات حتى في حالة إيقاف تشغيل أجهزة الكمبيوتر المحمول أو الأجهزة الأخرى.

**ملاحظة:** يلزمك جهاز USB متصل بجهاز التوجيه اللاسلكي لاستخدام Download Master (مدير التنزيل).

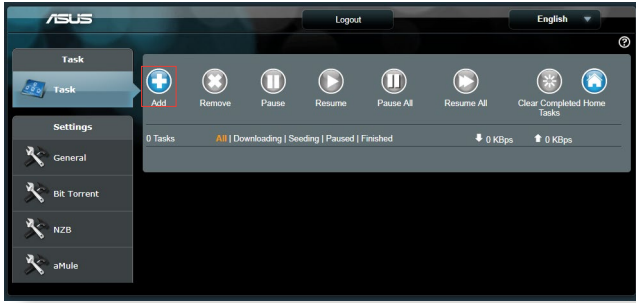
لاستخدام Download Master (مدير التنزيل):

1. انقر فوق **General (عام) < USB application (تطبيق USB) < Download Master (مدير التنزيل)** لتنزيل وتثبيت الأداة المساعدة تلقائياً.

**ملاحظة:** إذا كان لديك أكثر من محرك أقراص USB، فحدد جهاز USB الذي تريد تنزيل الملفات عليه.

2. بعد استكمال عملية التنزيل، انقر فوق رمز Download Master (مدير التنزيل) لبدء استخدام الأداة المساعدة.

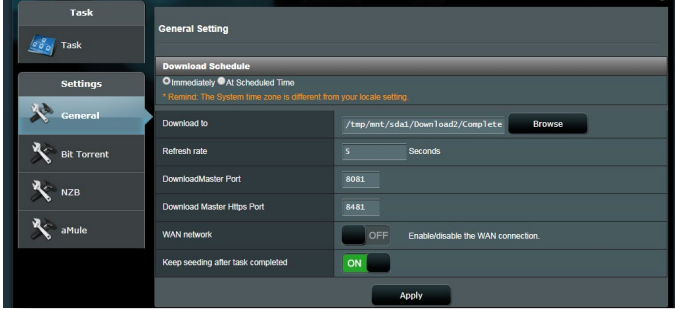
3. انقر فوق **Add (إضافة)** لإضافة مهمة تنزيل.



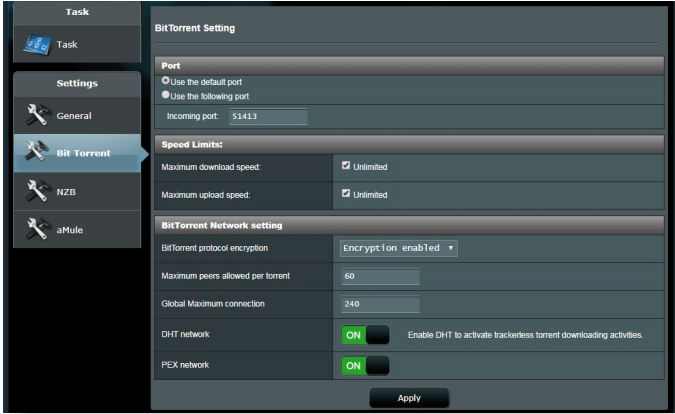
4. حدد نوع تنزيل مثل BitTorrent أو HTTP أو FTP. قم بتوفير ملف torrent أو عنوان URL لبدء التنزيل.

**ملاحظة:** لمعرفة تفاصيل عن Bit Torrent، راجع القسم 4.4.1 تكوين إعدادات تنزيل Bit Torrent.

5. استخدم جزء التنقل لتكوين الإعدادات المتقدمة.



## 4.4.1 تكوين إعدادات تنزيل Bit Torrent

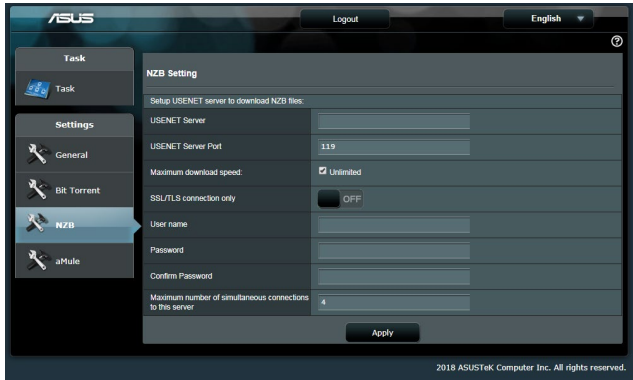


### لتكوين إعدادات تنزيل BitTorrent:

1. من جزء التنقل الخاص بـ Download Master (مدير التنزيل)، انقر فوق **Bit Torrent Setting** لبدء تشغيل صفحة **Bit Torrent** (إعداد BitTorrent).
2. حدد منفذاً معيناً لمهمة التنزيل الخاصة بك.
3. لتجنب تكديس الشبكة، يمكنك تحديد السرعات القصوى للتحميل والتنزيل تحت قسم **Speed Limits** (حدود السرعة).
4. يمكنك تحديد أقصى عدد للنظراء المسموح بها وتمكين أو تعطيل تشفير الملف أثناء عمليات التنزيل.

## 4.4.2 إعدادات NZB

يمكنك إعداد خادم USENET لتنزيل ملفات NZB. بعد إدخال إعدادات USENET، انقر فوق **Apply** (تطبيق).



ASUS

Logout English

Task

Task

Settings

General

Bit Torrent

**NZB**

aMule

NZB Setting

Setup USENET server to download NZB files.

USENET Server

USENET Server Port 119

Maximum download speed:  Unlimited

SSL/TLS connection only  OFF

User name

Password

Confirm Password

Maximum number of simultaneous connections to this server 4

Apply

2018 ASUSTeK Computer Inc. All rights reserved.

## 5 استكشاف الأخطاء وإصلاحها

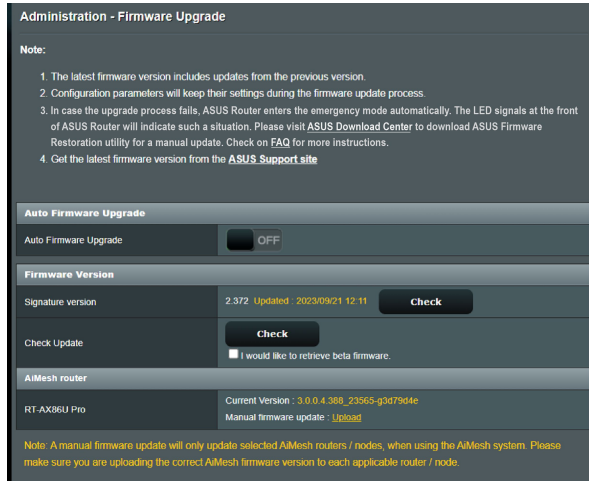
يوفر هذا الفصل الحلول للمشكلات التي قد تصادفها مع جهاز التوجيه. إذا صادفت مشكلات ليست مذكورة في هذا الفصل، فيرجى زيارة موقع دعم ASUS على العنوان: <https://www.asus.com/support> للحصول على مزيد من المعلومات حول المنتج وتفاصيل الاتصال بالدعم الفني لـ ASUS.

### 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 **Administration > Advanced Settings (الإعدادات المتقدمة)** **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-iot-servers/whole-home-mesh-wifi-system/zenwifi-wifi-systems/asus-zenwifi-pro-et12/helpdesk\\_bios/?model2Name=ASUS-ZenWiFi-Pro-ET12](https://www.asus.com/networking-iot-servers/whole-home-mesh-wifi-system/zenwifi-wifi-systems/asus-zenwifi-pro-et12/helpdesk_bios/?model2Name=ASUS-ZenWiFi-Pro-ET12) لتحميل 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 مما إذا تم توصيل كابلات Ethernet (الإيثرنت) بشكل صحيح أم لا.

- عند توصيل كابل إيثرنت الذي يوصل جهاز التوجيه بالمودم بشكل صحيح، فإن مصباح WAN LED يضيء.
- عند توصيل كابل إيثرنت الذي يوصل جهاز الكمبيوتر المتصل بجهاز التوجيه بشكل صحيح، فإن مصباح LAN LED المقابل يضيء.

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

- عندما تقوم بتوصيل الكمبيوتر الخاص بك بجهاز 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 الكابل استخدام عنوان MAC للكمبيوتر المسجل أوليًا في الحساب. يمكنك عرض عنوان MAC في واجهة المستخدم العمومية على الويب GUI، **Network Map** (خريطة الشبكة) < صفحة **Clients** (العملاء)، وحلق بمؤشر الماوس فوق جهازك في **Client Status** (حالة العميل).

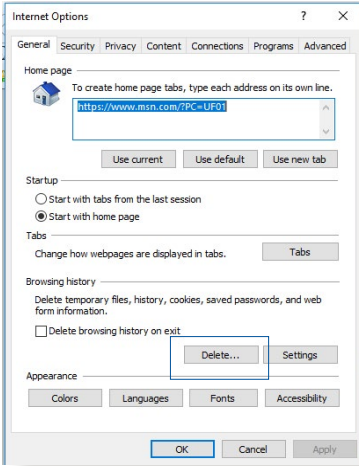


## 5.2 أسئلة شائعة (FAQs)

### 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. اسم تسجيل الدخول وكلمة المرور الافتراضية من المصنع هي "admin/admin". 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. شغل Internet Explorer، ثم انقر على **Tools (أدوات) < Internet Options (خيارات الإنترنت)**.



2. في علامة تبويب **General Browsing (عام)**، تحت **history (تاريخ التصفح)**، انقر فوق **Delete... (حذف...)**، حدد **Temporary Internet files and website files (ملفات الإنترنت المؤقتة وملفات موقع الويب) و 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 تلقائياً. 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:
- قَرَب جهاز التوجيه إلى عميل الشبكة اللاسلكية.
- جرب ضبط هوائيات جهاز التوجيه على أفضل اتجاه كما هو موضح في القسم 1.4 ضبط موضع جهاز التوجيه اللاسلكي.
- 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)**.

### LAN - DHCP Server

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

Basic Config	
Enable the DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
ASUS Router's Domain Name	<input type="text"/>
IP Pool Starting Address	<input type="text" value="192.168.50.2"/>
IP Pool Ending Address	<input type="text" value="192.168.50.254"/>
Lease time	<input type="text" value="86400"/>
Default Gateway	<input type="text"/>

DNS and WINS Server Setting	
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>
Advertise router's IP in addition to user-specified DNS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WINS Server	<input type="text"/>

Manual Assignment	
Enable Manual Assignment	<input type="radio"/> Yes <input checked="" type="radio"/> No

Manually Assigned IP around the DHCP list (Max Limit : 64)				
Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>

No data in table.

- 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، فانقل 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)**.

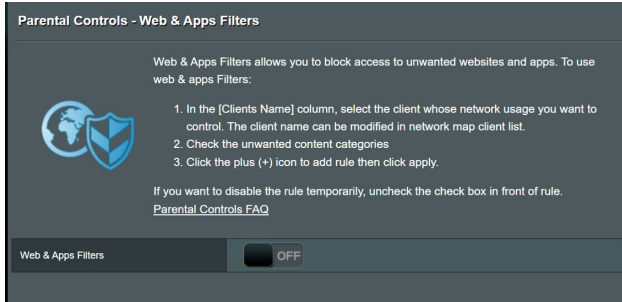
- إذا كنت تستخدم مهائى LAN لاسلكي، فتتحقق من أن القناة اللاسلكية المستخدمة تتوافق مع القنوات المتوفرة في بلدك/منطقتك. إذا لم تكن متوافقة، فاضبط القناة، وعرض نطاق القناة والوضع اللاسلكي.
- إذا كنت ما تزال غير قادر على الاتصال بجهاز التوجيه اللاسلكي، فيمكنك إعادة ضبط جهاز التوجيه على الإعدادات الافتراضية 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.
- تحقق من مؤشرات الحالة على مودم ADSL وجهاز توجيه اللاسلكي. إذا لم يكن مصباح WAN LED على جهاز التوجيه اللاسلكي مضيئاً، فتتحقق من أن جميع الكابلات متصلة بشكل صحيح.

### 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)**. حساب تسجيل الدخول وكلمة المرور الافتراضية هي "admin" لكل منهما.

### كيف تستعيد النظام إلى إعداداته الافتراضية؟

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

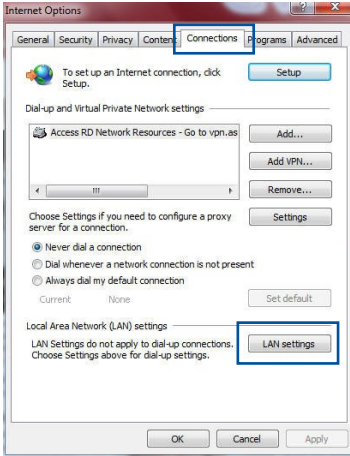
### فشل تحديث البرنامج الثابت.

- 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)

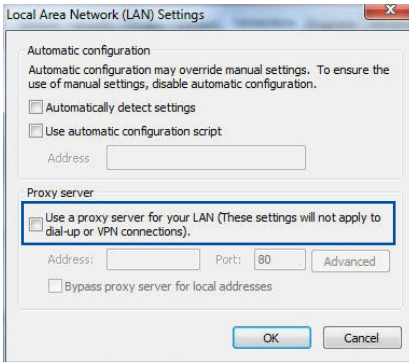
قبل تكوين جهاز التوجيه اللاسلكي، نفذ الخطوات الموضحة في هذا القسم للكمبيوتر المضيف وعملاء الشبكة.

A. تعطيل الخادم الوكيل، في حالة تمكينه.



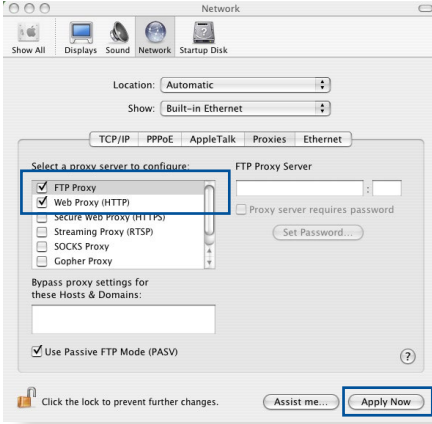
Windows®

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



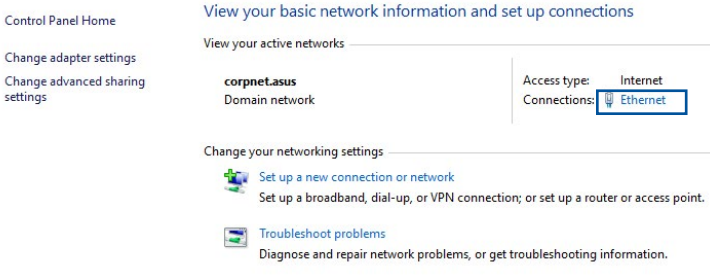
1. من مستعرض Safari، انقر فوق **Preferences < Safari (التفضيلات) < Change (متقدم) Settings (تغيير الإعدادات)...**
2. من شاشة الشبكة، قم بإلغاء تحديد **FTP Proxy (وكيل FTP) و Web Proxy (وكيل الويب) (HTTP)**.
3. انقر فوق **Apply Now (تطبيق الآن)** عند الانتهاء.

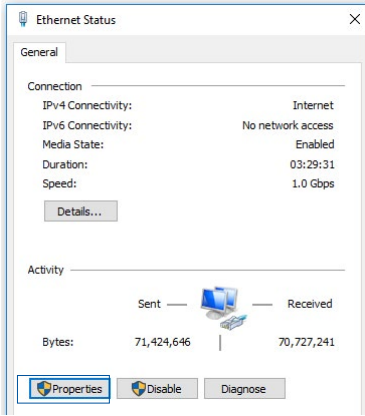
ملاحظة: راجع ميزة المساعدة في المستعرض لمعرفة التفاصيل حول تعطيل الخادم الوكيل.

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

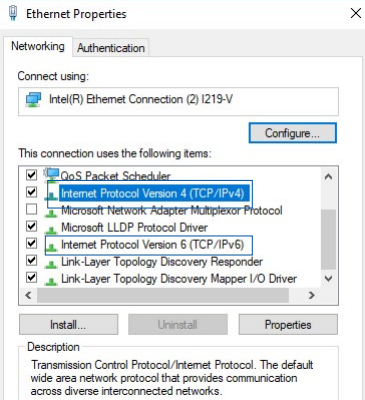
## Windows®

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.

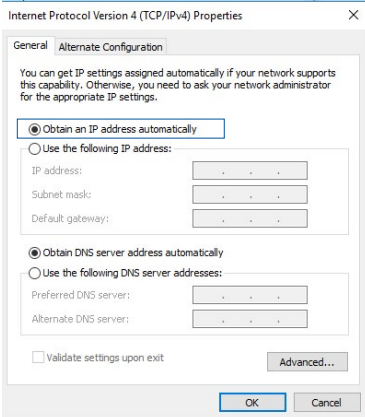




2. انقر فوق **Properties** (خصائص) لعرض نافذة Ethernet Properties (خصائص الإنترنت).



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

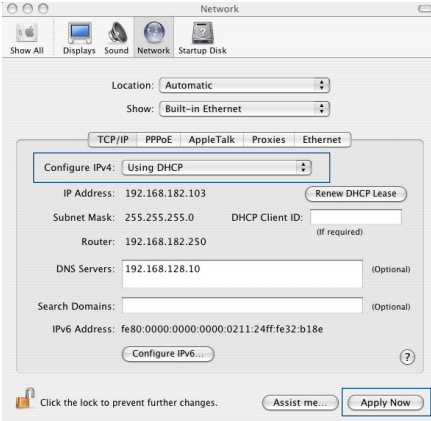


4. للحصول على إعدادات IP IPv4 تلقائياً، اختر **Obtain an IP address automatically** (الحصول على عنوان IP تلقائياً).

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

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

## MAC OS



1. انقر فوق رمز Apple الموجود في القسم العلوي الأيسر للشاشة.

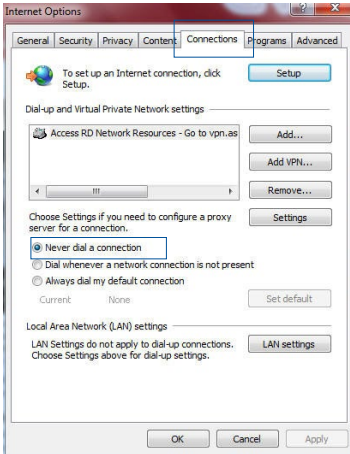
2. انقر فوق **System Preferences** (تفضيلات النظام) < **Network** (الشبكة) < **Configure** (تكوين) ...

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 مطلقاً).

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

## الخدمة والدعم

زر موقع الويب المتعدد اللغات خاصتنا على [.https://www.asus.com/support/](https://www.asus.com/support/)

